



SECURITY

Cisco Firepower Threat Defense (FTD)

Configuration and Troubleshooting Best Practices
for the Next-Generation Firewall (NGFW),
Next-Generation Intrusion Prevention System (NGIPS),
and Advanced Malware Protection (AMP)

Cisco Firepower Threat Defense (FTD):

Configuration and Troubleshooting Best Practices
for the Next-Generation Firewall (NGFW),
Next-Generation Intrusion Prevention System (NGIPS),
and Advanced Malware Protection (AMP)

Nazmul Rajib

Cisco Press
800 East 96th Street
Indianapolis, Indiana 46240 USA

Copyright© 2018 Cisco Systems, Inc.

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America

First Printing October 2017

Library of Congress Control Number: XXXXXXXXXXX

ISBN-13: 978-1-58714-480-6

ISBN-10: 1-58714-480-8

Warning and Disclaimer

This book is designed to provide information about the Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), and Advanced Malware Protection (AMP) technologies using the Cisco Firepower System. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact international@pearsoned.com.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Editor-in-Chief Mark Taub

Product Line Manager Brett Bartow

Business Operation Manager, Cisco Press

Executive Editor Mary Beth Ray

Managing Editor Sandra Schroeder

Development Editor Ellie C. Bru

Project Editor Tonya Simpson

Copy Editor Kitty Wilson

Technical Editor(s) John Groetzinger, Foster Lipkey

Editorial Assistant Vanessa Evans

Book Designer

Cover Designer

Composition

Indexer

Proofreader

About the Author(s)

Nazmul Rajib is one of the most senior engineers and leaders in the Cisco Global Technical Assistance Center (TAC) for the Next-Generation security technologies. He leads documentation projects, develops internal cybersecurity training program, and trains Cisco engineers worldwide who support Cisco network infrastructures around the world. As an escalation point, Nazmul analyzes complex security deployments, resolves technical issues, and determines the best practices. As an engineering engagement lead, Nazmul reviews design specifications and technical publications, tests the security software and identifies defects. Nazmul has authored numerous publications at Cisco.com and in the Cisco Support Community. He is based in the Research Triangle Park, North Carolina.

Before joining Cisco, Nazmul worked at the Sourcefire Headquarter in Columbia, Maryland. As a Knowledge Manager, he developed the worldwide security knowledge base, and managed corporate training program. He also delivered the partner training, and designed security certification exam. As a Senior Technical Support Engineer, Nazmul supported the network of numerous Fortune 500 companies, security service providers, and U.S. government.

Nazmul has a Master of Science degree in Internetworking. He is a Sourcefire Certified Expert (SFCE) and Sourcefire Certified Security Engineer (SFCSE). He also holds many certifications on information technology, network security, and technical writing.

About the Technical Reviewers

John Groetzinger is a member of the Global TAC Security Technical Leadership team supporting Firepower, FireSIGHT, AMP for endpoints, Threat Grid and 3rd party integrations. He has been a leader in developing tools and procedures for supporting the Cisco Firepower and AMP security software platforms as well as working closely with the various engineering teams in the Cisco security space to improve quality and serviceability. He holds a bachelor's degree in Mechanical Engineering with a minor in Computer Science. John's primary areas of interest are enterprise security, open source software, API development/integration and automation.

Foster Lipkey is a member of the Global TAC Security Technical Leadership team supporting Firepower, FireSIGHT, AMP for endpoints and Threat Grid as well as 3rd party integrations. He has been a leader in developing tools and procedures for supporting the Cisco Firepower and AMP security software platforms. Prior to working for Sourcefire/Cisco, he was an Applications Solutions Specialist as a contractor for the National Cancer Institute (NCI) supporting Java Enterprise applications for NCI Center for Biomedical Informatics and Information Technology (CBIIT). Foster's primary areas of interest are enterprise security and security automation. He served as the technical editor for the most recent edition of Cisco Next-Generation Security Solutions: All-in-one Cisco ASA FirePOWER Services, NGIPS, and AMP.

Dedications

This book is dedicated to...

My parents, whose love and blessings have brought me to where I am today, and...

My wife, whose love and support allow me to persevere every day, and...

My children, whose love and care energize me for the next day...

My teachers, whose wisdom and guidance enlighten me always...

Acknowledgments

Thank you God, for giving me the ability to write this book.

I am grateful to two technical support managers of the Cisco Global TAC —Andrew Firman and Maurice Spencer —for their inspiration, encouragement, and support throughout the project of authoring this book.

I would like to recognize the Technical Leaders of the Firepower Technology — John Groetzinger and Foster Lipkey — who are also the technical editors of this book. Their commitments and thorough reviews are indispensable to this book.

I really appreciate the Principal Engineer Gonzalo Salgueiro taking time to review my proposal for this book. I am thankful to the Senior Vice President Tom Berghoff and Senior Director Marc Holloman for all the encouraging notes about this book.

With gratitude, I want to acknowledge all of my colleagues at Cisco for being so enthusiastic about my progress in writing, and for sharing knowledge nuggets directly and indirectly.

Finally, many thanks to Eleanor Bru, Mary Beth Ray, and everyone at Pearson Education and Cisco Press for keeping me on track until the book is published.

Contents at a Glance

[Introduction](#)

[Chapter 1. Introduction to the Cisco Firepower Technology](#)

[Chapter 2. Firepower Threat Defense \(FTD\) on ASA 5500-X Series Hardware](#)

[Chapter 3. Firepower Threat Defense \(FTD\) on the Firepower eXtensible Operating System](#)

[Chapter 4. Firepower Management Center \(FMC\) Hardware](#)

[Chapter 5. Firepower System \(FMC+FTD\) Virtual on VMware](#)

[Chapter 6. Firepower Management Network](#)

[Chapter 7. Licensing and Registration through SFTunnel](#)

[Chapter 8. Firepower Deployment in Routed Mode](#)

[Chapter 9. Firepower Deployment in Transparent Mode](#)

[Chapter 10. Capture of Traffic for Advance Analysis](#)

[Chapter 11. Blocking of Traffic Using Inline Interface Mode](#)

[Chapter 12. Inspecting Traffic without Blocking Them](#)

[Chapter 13. Handling of Encapsulated Traffic](#)

[Chapter 14. Bypassing Inspection and Trusting Traffic](#)

[Chapter 15. Rate Limiting of Traffic](#)

[Chapter 16. Blacklisting of Suspicious Addresses Using Security Intelligence](#)

[Chapter 17. Blocking of a Domain Name Server \(DNS\) Query](#)

[Chapter 18. Filtering of URL Based on Category, Risk, and Reputation](#)

[Chapter 19. Discovering Network Application and Controlling Application Traffic](#)

[Chapter 20. Controlling a File Transfer and Blocking the Spread of a Malware](#)

[Chapter 21. Preventing Network from an Attack by Blocking an Intrusion Attempt](#)

[Chapter 22. Masquerading the Original IP Address of an Internal Network Host](#)

[Appendix A. Answers to Review Questions](#)

[Appendix B. & C. Generate and Collect Troubleshooting Files Using GUI](#)

[Contents](#)

[Introduction](#)

[Chapter 1. Introduction to the Cisco Firepower Technology](#)

[History of Firepower](#)

[Firepower Threat Defense \(FTD\)](#)

[Summary](#)

[Chapter 2. Firepower Threat Defense \(FTD\) on ASA 5500-X Series Hardware](#)

[Essential Knowledge](#)

[Best Practices](#)

[Configuration](#)

[Verification and Troubleshooting Tools](#)

[Summary](#)

[Review Questions](#)

[Chapter 3. Firepower Threat Defense \(FTD\) on the Firepower eXtensible Operating System \(FXOS\)](#)

[Essential Knowledge](#)

[Best Practices](#)

[Configuration](#)

[Verification and Troubleshooting Tools](#)

[Summary](#)

[Quiz](#)

[Chapter 4. Firepower Management Center \(FMC\) Hardware](#)

[Essential Knowledge](#)

[Best Practices](#)

[Configuration](#)

[Configuration Steps](#)

[Verification and Troubleshooting Tools](#)

[Summary](#)

[Quiz](#)

[Chapter 5. Firepower System \(FMC+FTD\) Virtual on VMware](#)

[Essential Knowledge](#)

[Best Practices](#)

[Configuration](#)

[Verification and Troubleshooting Tools](#)

[Summary](#)

[Quiz](#)

[Chapter 6. Firepower Management Network](#)

[Essential Knowledge](#)

[Best Practices](#)

[On FMC Hardware](#)

[On ASA Hardware](#)

[On Firepower Security Appliance](#)

[Summary](#)

[Quiz](#)

[Chapter 7. Licensing and Registration through SFTunnel](#)

[Essential Knowledge](#)

[Best Practices](#)

[Licensing a Firepower System](#)

[Registration of a Firepower System](#)

[Summary](#)

[Quiz](#)

[Chapter 8. Firepower Deployment in Routed Mode](#)

[Essential Knowledge](#)

[Best Practices](#)

[Configuration](#)

[Verification and Troubleshooting Tools](#)

[Summary](#)

[Quiz](#)

[Answers:](#)

[Chapter 9. Firepower Deployment in Transparent Mode](#)

[Essential Knowledge](#)

[Best Practices](#)

[Configuration](#)

[Summary](#)

[Quiz](#)

[Chapter 10. Capture of Traffic for Advance Analysis](#)

[Essential Knowledge](#)

[Best Practices](#)

[Configuration](#)

[Verification and Troubleshooting Tools](#)

[Summary](#)

[Quiz](#)

[Chapter 11. Blocking of Traffic Using Inline Interface Mode](#)

[Essential Knowledge](#)

[Best Practices](#)

[Configuration](#)

[Summary](#)

[Quiz](#)

[Chapter 12. Inspecting Traffic without Blocking Them](#)

[Essential Knowledge](#)

[Best Practices](#)

[Prerequisites](#)

[Inline-Tap Mode](#)

[Passive Interface Mode](#)

[Analysis of Operation](#)

[Summary](#)

[Quiz](#)

[Chapter 13. Handling of Encapsulated Traffic](#)

[Essential Knowledge](#)

[Best Practices](#)

[Prerequisites](#)

[Scenario 1: Analyzing Encapsulated Traffic](#)

[Scenario 2: Blocking Encapsulated Traffic](#)

[Scenario 3: Bypassing Inspection](#)

[Summary](#)

[Quiz](#)

[Chapter 14. Bypassing Inspection and Trusting Traffic](#)

[Essential Knowledge](#)

[Best Practices](#)

[Prerequisites](#)

[Fastpath through a Prefilter Policy](#)

[Trust through an Access Policy](#)

[Summary](#)

[Quiz](#)

[Answers:](#)

[Chapter 15. Rate Limiting of Traffic](#)

[Essential Knowledge](#)

[Best Practices](#)

[Prerequisites](#)

[Configuration](#)

[Verification of Rate-Limit of a File Transfer](#)

[Analysis of QoS Events and Statistics](#)

[Summary](#)

[Quiz](#)

[Chapter 16. Blacklisting of Suspicious Addresses Using Security Intelligence](#)

[Essential Knowledge](#)

[Best Practices](#)

[Prerequisites](#)

[Configuration](#)

[Verification and Troubleshooting Tools](#)

[Summary](#)

[Quiz](#)

[Chapter 17. Blocking of a Domain Name Server \(DNS\) Query](#)

[Essential Knowledge](#)

[Best Practices](#)

[Prerequisites](#)

[Configuration](#)

[Verification and Troubleshooting Tools](#)

[Summary](#)

[Quiz](#)

[Chapter 18. Filtering of URL Based on Category, Risk, and Reputation](#)

[Essential Knowledge](#)

[Prerequisites](#)

[Best Practices](#)

[Blocking URLs of a Certain Category](#)

[Allowing a Specific URL](#)

[Uncategorized URL](#)

[Summary](#)

[Quiz](#)

[Chapter 19. Discovering Network Application and Controlling Application Traffic](#)

[Essential Knowledge](#)

[Best Practices](#)

[Prerequisite](#)

[Discovery of Application](#)

[Blocking of Application](#)

[Summary](#)

[Quiz](#)

[Chapter 20. Controlling a File Transfer and Blocking the Spread of a Malware](#)

[Essential Knowledge](#)

[Best Practices](#)

[Pre-Requisites](#)

[Configuration](#)

[Verification and Troubleshooting Tools](#)

[Summary](#)

[Quiz](#)

[Chapter 21. Preventing Network from an Attack by Blocking an Intrusion Attempt](#)

[Essential Knowledge](#)

[Best Practices](#)

[Configuration](#)

[Verification and Troubleshooting Tools](#)

[Summary](#)

[Quiz](#)

[Chapter 22. Masquerading the Original IP Address of an Internal Network Host](#)

[Essential Knowledge](#)

[Best Practices](#)

[Pre-Requisites](#)

[Configuration](#)

[Summary](#)

[Quiz](#)

[Appendix A. Answers to Review Questions](#)

[Appendix B. Generate and Collect Troubleshooting Files Using GUI](#)

[Procedures](#)

[Appendix C. Generate and Collect Troubleshooting Files Using CLI](#)

[Introduction](#)

[Procedures](#)

Reader Services

Register your copy at www.ciscopress.com/title/ISBN for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.ciscopress.com/register and log in or create an account*. Enter the product ISBN [provide 13 ISBN for parent title here] and click Submit. Once the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Icons Used in This Book



Laptop



Terminal



WWW Server



Cloud



Attacker



Firepower
Management
Center



Load Balancer



Firepower
Threat Defense



Switch



Router



Satellite Server



Repeater



Third Party



Internet Service
Provider



Server



Server Farms



Database

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

Cisco introduces Next-Generation security technologies in a unified Firepower Threat Defense (FTD) software image. It offers Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), Advanced Malware Protection (AMP) technologies — all in one single software.

This book allows you to learn the best practices, provides configuration examples, and illustrates GUI screenshots from real world deployment scenarios. It empowers you to configure your own Firepower System with confidence. The book describes many diagnostic tools that allow you to investigate any potential technical issues by yourself. In other words, it could serve you as a “Personal Support Engineer”

Who Should Read This Book?

This book demonstrates various real world deployment scenarios of the Cisco Firepower Systems. Any network engineer, system administrator, security engineer, and security analyst who want to configure a Firepower network, and diagnose any technical issues should read this book. The Cisco Global TAC Engineers, Cisco Sales Engineers, Advanced Services Engineers, Field Engineers, Network Consulting Engineers, and Security Engineers use this book everyday, for their references.

This book is very important to the Channel Partners, and Managed Security Service Providers (MSSP) who want to provide technical support to their own customers.

This book is invaluable to the network administrators in a classified environment, such as, U.S. government, who are not allowed to share their sensitive data, and want to troubleshoot their own issues.

Any students or candidates who want to take a Cisco security certification exam will find valuable information on this book. This book covers the Firepower next-Generation security related topics that are available the CCNP Security and CCIE Security exams curriculum.

This book is not a replacement of an official Cisco Firepower publication, such as, User Guide, Installation Guide, etc. It is rather a supplement to the official publications.

How This Book Is Organized

Chapter 1, “Introduction to Cisco Firepower Technology”:

The book begins with the history and evolution of the Cisco Firepower Technology. It introduces various software components that may be installed on a Firepower System. This chapter also provides a quick overview of the supported hardware for the Cisco Firepower Threat Defense (FTD) technology.

Chapter 2, “Firepower Threat Defense (FTD) on ASA 5500-X Series Hardware”:

This chapter describes the differences between various images that may be installed on an ASA 5500-X hardware. It demonstrates the detail process to reimage an ASA 5500-X Series hardware to the Firepower Threat Defense software. In addition, this chapter provides you the command line tools that you can use to verify the status of the hardware and software.

Chapter 3, “FTD on the Firepower eXtensible Operating System (FXOS)”:

This chapter describes the architecture, implementation and installation of FTD on a Firepower Security Appliance running Firepower eXtensible Operating System (FXOS). It demonstrates several command line tools to determine the status of various components of the appliance.

Chapter 4, “Firepower Management Center (FMC) Hardware”:

This chapter discusses and compares various hardware platforms for the FMC. It illustrates the complete reimage (also known as System Restore) process, and describes the best practices for a reimage. By reading this chapter, you can also learn many different commands and tools to determine any issues with an FMC hardware.

Chapter 5, “Firepower System (FMC+FTD) Virtual on VMware”:

This chapter describes various aspects of the Firepower virtual appliance, such as, how to deploy a virtual appliance, how to tune the resources for optimal performance, and how to investigate issues with a new deployment.

Chapter 6, “Firepower Management Network”:

This chapter describes the best practices for designing and configuring a management network for the Firepower system. It also discusses the tools that you could use to verify any communication issues between the management interfaces of an FMC and FTD. Before you begin the registration process which is described in the next chapter, you must ensure that the FMC and FTD are successfully connected through your network.

Chapter 7, “Licensing and Registration through SFTunnel”:

This chapter discusses licensing and registration — two important initial tasks of a Firepower system deployment. It describes the capabilities of different Firepower licenses and the steps to register an FMC with a Smart License Server. It also demonstrates the registration process, and the tools to investigate any communication issues.

Chapter 8, “Firepower Deployment in Routed Mode”:

In this chapter explains the widely deployed firewall mode — the routed mode. It describes the steps to configure the routed interfaces with static IP address as well as dynamic IP address. In addition, this chapter discusses various command line tools that you can use to determine any potential interface related issues.

Chapter 9, “Firepower Deployment in Transparent Mode”:

This chapter discusses the transparent firewall mode — how to configure the physical and virtual interfaces, and how to utilize various command line tools to investigate any potential configuration issues.

Chapter 10, “Capture of Traffic for Advance Analysis”:

This chapter describes the processes to capture live traffic on an FTD using the system-provided capturing tool. To demonstrate the benefit of the tool, this chapter utilizes various tcpdump options and BPF syntaxes to filter and manage a packet capture.

Chapter 11, “Blocking of Traffic Using Inline Interface Mode”:

This chapter demonstrates how to configure an FTD in inline interface mode, how to enable fault tolerance features on an inline set, and how to trace a packet in order to analyze the root cause of a drop. This chapter also describes various command line tools that you can utilize to verify the status of an interface, an inline pair, and an inline set.

Chapter 12, “Inspecting Traffic without Blocking Them”:

This chapter explains the configuration and operation of various detection-only modes of an FTD, such as, passive mode, inline-tap mode, and inline mode with Drop when Inline option disabled. It also provides various command line tools that you can utilize to determine the status of interfaces and traffic.

Chapter 13, “Handling of Encapsulated Traffic”:

This chapter shows you how to analyze and block traffic that are encapsulated with GRE protocol. This chapter also demonstrates the steps to bypass an inspection when the traffic is transferred over a tunnel. Besides configurations, you can learn various tools to analyze an action applied by the Prefilter and Access Control policy of your FTD.

Chapter 14, “Bypassing Inspection and Trusting Traffic”: This chapter discusses the techniques to bypass an inspection. It provides the steps to configure different methods. The chapter also analyzes the flows of bypassed packets to demonstrate how an FTD acts during different bypassing option. You can learn the usage of various debug tools, which helps you to determine if the bypass process is working, as designed.

Chapter 15, “Rate Limiting of Traffic”: This chapter goes through the steps to configure QoS policy on an FTD. It also provides an overview to the common rate-limiting mechanisms, and the QoS implementation on FTD. At the end, this chapter provides the command line tools to verify the operation of QoS policy in an FTD.

Chapter 16, “Blacklisting of Suspicious Addresses Using Security Intelligence”:

This chapter illustrates the detection of a malicious address using the Security Intelligence feature. It describes how to configure an FTD to block, monitor, or whitelist an address, when there is a match. This chapter also discusses the backend file systems for the Security Intelligence feature. You can apply this knowledge to troubleshoot an issue with the Security Intelligence.

Chapter 17, “Blocking of a Domain Name Server (DNS) Query”: This chapter demonstrates various techniques to administer DNS queries using a Firepower DNS policy. Besides traditional access control rule, an FTD can incorporate Cisco intelligence feed and dynamically blacklist suspicious domains. You can learn various ways to configure and deploy a DNS policy. This chapter also demonstrates several command line tools that you can run to verify, analyze and troubleshoot an issue with DNS policy.

Chapter 18, “Filtering of URL Based on Category, Risk, and Reputation”: This chapter describes techniques to filter traffic based on the category and reputation of an URL. It illustrates how a Firepower System performs an URL lookup, and then how an FTD takes an action based on the query result. This chapter explains the connection to an URL through debug messages, which is critical for troubleshooting.

Chapter 19, “Discovering Network Application and Controlling Application Traffic”:

This chapter shows how a Firepower system can make you aware of the applications running on your network, and empowers you to control access to any unwanted applications. You can also learn the techniques to verify if an FTD is able to identify an application properly.

Chapter 20, “Controlling a File Transfer and Blocking the Spread of a Malware”:

Cisco also integrates the Advanced Malware Protection (AMP) technology with the Firepower technology. This chapter explains how both technologies work together, and help you to detect and block the spread of an infected file across your network. You can learn the configurations and operations of a File Policy on a Firepower System. This chapter also demonstrates various logs and debug messages, which are useful to determine any issues with the cloud lookup and file disposition.

Chapter 21, “Preventing Network from an Attack by Blocking an Intrusion Attempt”:

This chapter describes one of the most important and widely used features of a Firepower System — Snort based Next-Generation Intrusion Prevention System (NGIPS). In this chapter, you can learn how to configure an NGIPS, how to apply deploy any associated policies, and how to drill down intrusion events for advanced analysis. This chapter discusses the Firepower Recommendations, and demonstrates how the recommended ruleset can reduce the system overhead by incorporating the discovery data.

Chapter 22, “Masquerading the Original IP Address of an Internal Network Host”:

This chapter discusses various types of NAT on an FTD. It shows the steps to configure a NAT rule, and demonstrate how FTD can leverage NAT technology to masquerade internal IP addresses, in a real world scenario.

Chapter 1. Introduction to the Cisco Firepower Technology

History of Firepower

This is a technical book — describes various components of the Next-Generation security solutions. Each chapter walks you through a unique feature of the Firepower security technologies. Before diving into the technical detail, let's spend a little bit of time to be familiar with the background and overview of the Firepower technologies.

Sourcefire, a Part of Cisco

Cisco acquired Sourcefire in 2013. At the time of acquisition, Sourcefire was known as one of the top leaders in the Cybersecurity industry for its Intrusion Prevention System (IPS) and Next Generation Firewall (NGFW) solutions. The Sourcefire IPS was based upon Snort, an open source network intrusion detection and prevention system. In 2001, Sourcefire was founded by Martin Roesch, the creator of Snort.

Right after acquisition, Cisco has leveraged the Sourcefire technologies on various existing Cisco appliances, such as, ASA 5500-X series and Integrated Services Router (ISR). Later, Cisco has released new hardware platforms, such as Firepower 2100 Series, 4100 Series and 9300 Series, which also implement the Sourcefire technologies. Integration of the Sourcefire technologies have placed Cisco as one of the leaders in the Gartner Magic Quadrant for IPS.

Note: Gartner is a research and advisory company that performs research on a particular technology and provides the positions of the vendors on that technology

[Figure 1-1](#) illustrates Cisco's leadership position for the Intrusion Prevention System after Sourcefire acquisition.

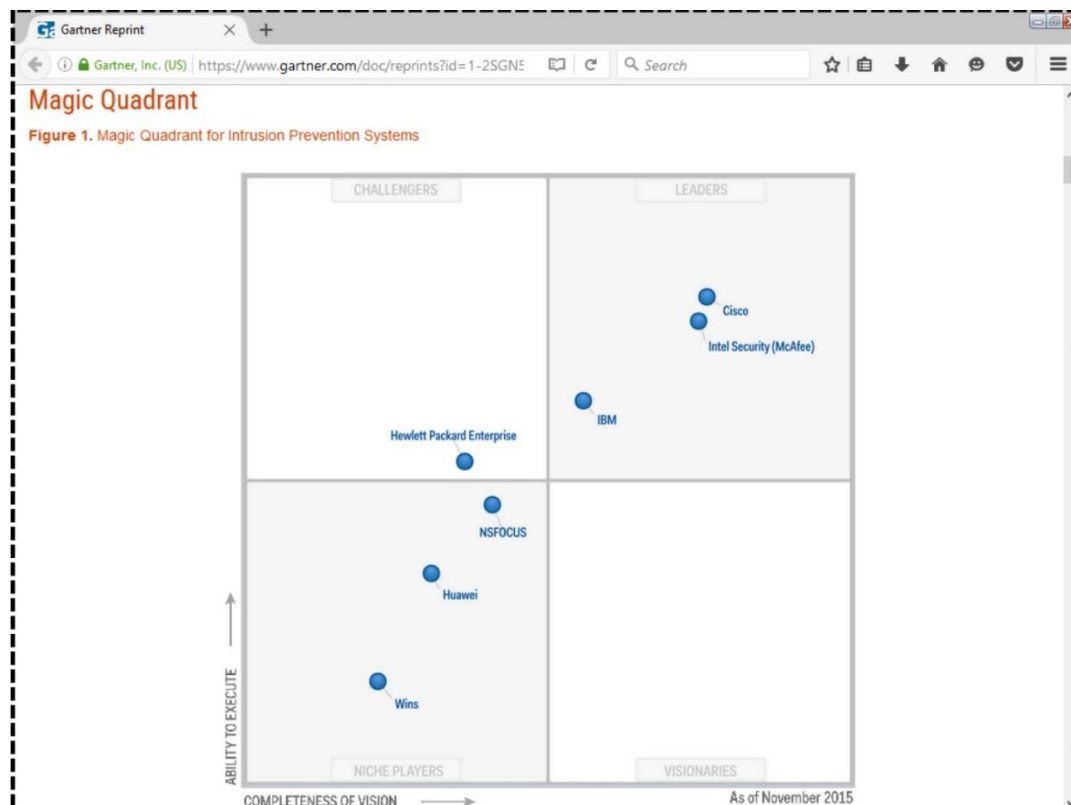


Figure: 1-1 Gartner's Magic Quadrant for IPS as of November 2015

Evolution of Firepower

Firepower refers to the military capability, which is not something we are going to discuss here! The following section provides you with a quick reference on how the word “Firepower” is now paired with Cisco, and has introduced a new technology — the Cisco Firepower technology.

A Firepower System deployment primarily consists of two types of appliances – a management appliance and a sensor. In simple word, a sensor inspects network traffic and sends any events to its management appliance. A management appliance, as the name says, also manages all kind of security policies for a sensor.

[Figure 1-2](#) shows the workflow of a Firepower System deployment.

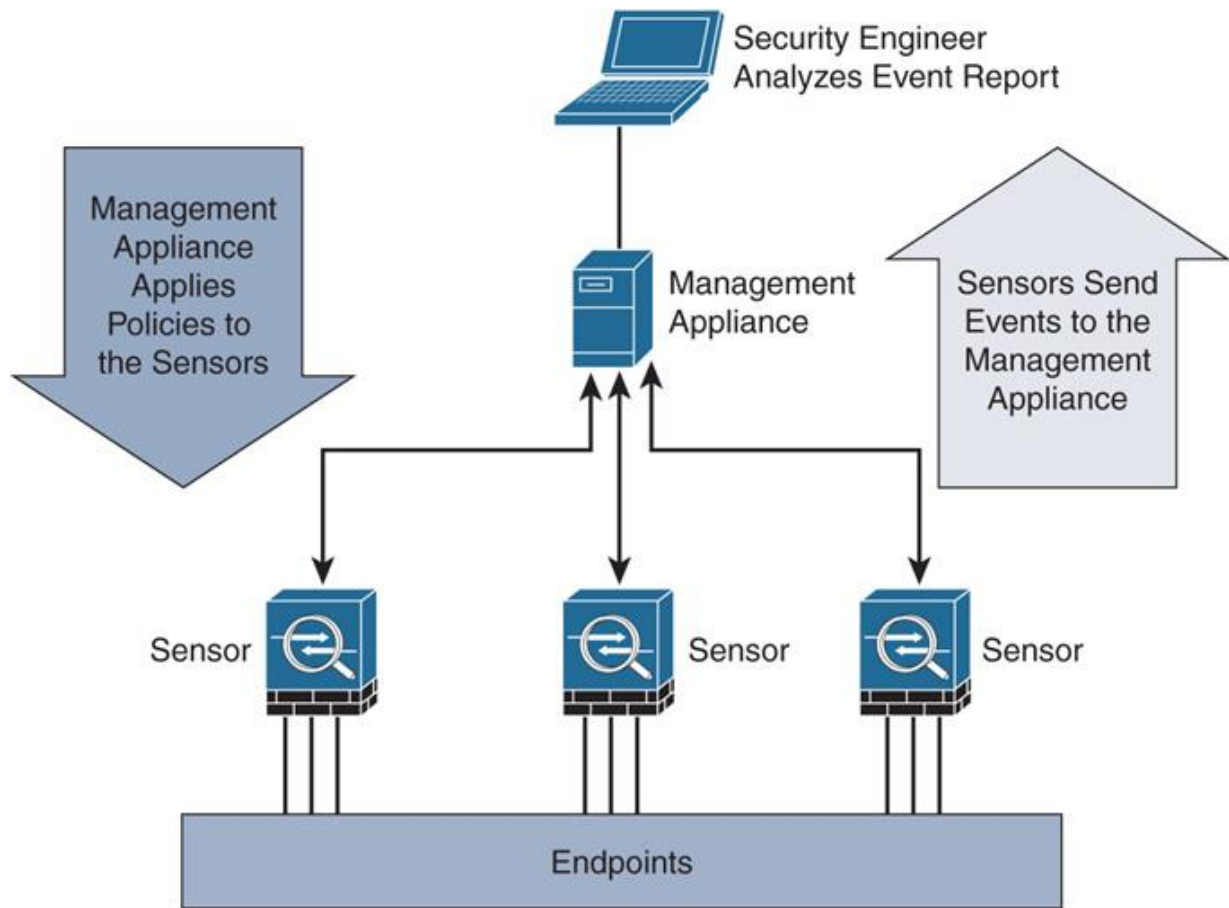


Figure 1-2. Block diagram of a Firepower System deployment

Prior to acquisition, Sourcefire released two different software trains — Version 4.x (primarily for IPS) and Version 5.x (with NGFW functionalities). Depending on the software train, the management appliance had two different names. In Version 4.x, it was known as Sourcefire Defense Center. In Version 5.x, it was known as FireSIGHT System or

FireSIGHT Management Center (FMC). Similarly, a sensor was known as 3D Sensor and FirePOWER Appliance, in Version 4.x and Version 5.x respectively.

Both statement would be correct when you say, in Version 4.x, a Sourcefire Defense Center manages the 3D Sensors, whereas, in Version 5.x, a FireSIGHT Management Center manages the FirePOWER Appliances.

FirePOWER vs Firepower

In the previous section, did you notice that different words (FireSIGHT vs FirePOWER) were used to refer to different types of appliances in different versions? Did you notice the word POWER with all uppercase letters?

To make the nomenclature simple as well as to maintain the brand reputation, Cisco, after Sourcefire acquisition in 2013, rebranded the Sourcefire technologies with one simple word — Firepower — without any uppercase in “power”.

[Figure 1-3](#) illustrates the evolution of Firepower Threat Defense (FTD) technology from pre-acquisition period to post-integration.

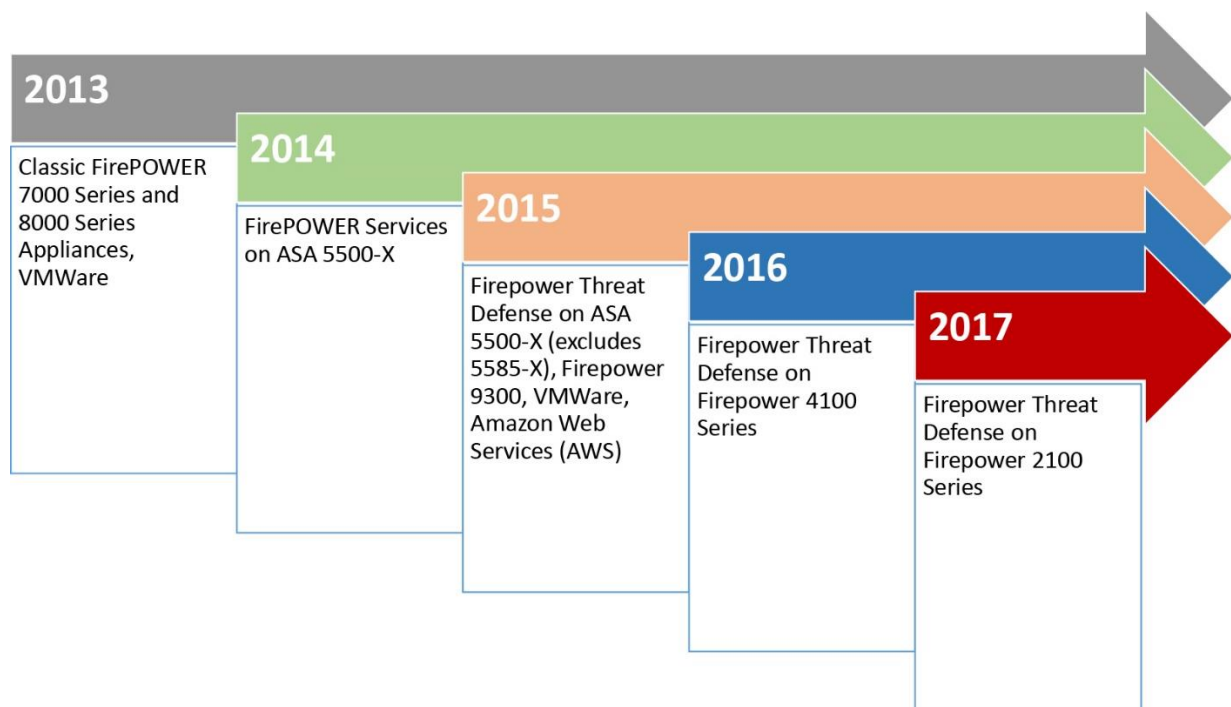


Figure 1-3. *Evolution of Firepower Threat Defense (FTD) technology*

Cisco did not retrospectively change the name of all of the legacy Sourcefire software and hardware from uppercase FirePOWER to lowercase Firepower, only the newly released hardware and software use this nomenclature. Some examples of new Firepower products are Cisco Firepower 9300 Appliance hardware, Cisco Firepower Threat Defense software. Similarly, the Cisco FirePOWER 8000 Series Appliance indicate that the series of this model has been available since pre-acquisition period.

[Table 1-1](#) shows various names of management appliance in different software version.

Software Version	Management Appliance
Version 4.x	Defense Center (DC)
Version 5.x	FireSIGHT System or FireSIGHT Management Center (FMC)
Version 6.x	Firepower System or Firepower Management Center (FMC)

Table 1-1. *Evolution of Firepower Management Center*

[Figure 1-4](#) shows the login page of a management appliance running Version 5.x. This page displays the legacy terminology “FireSIGHT” and the Sourcefire Support contact information.

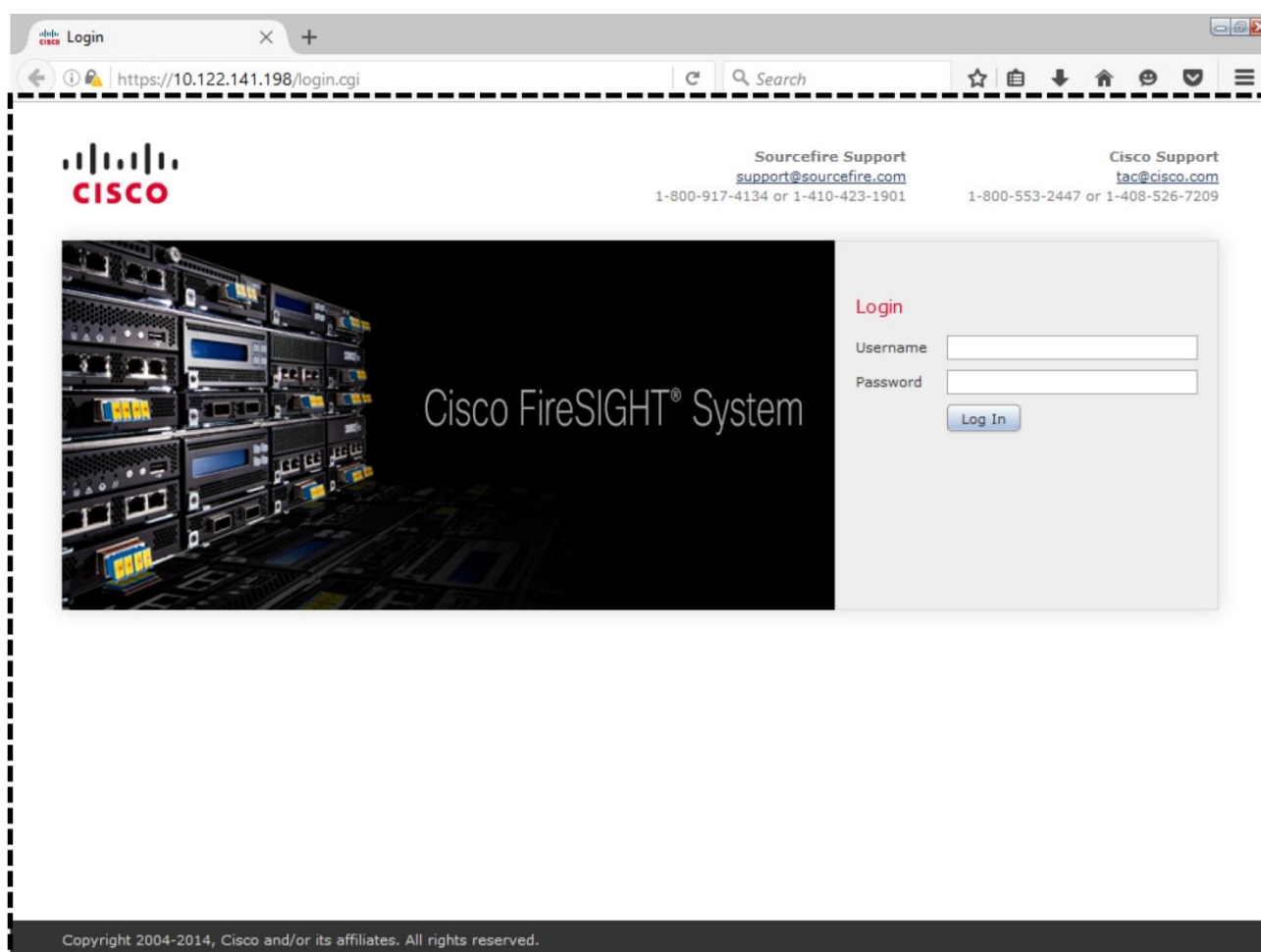


Figure 1-4. *The login page of a FireSIGHT Management Center running Version 5.x.*

[Figure 1-5](#) displays the login page of a management appliance running Version 6.x. It displays the latest brand of a management appliance — “Firepower”. Also, the legacy Sourcefire Support contact information is removed.

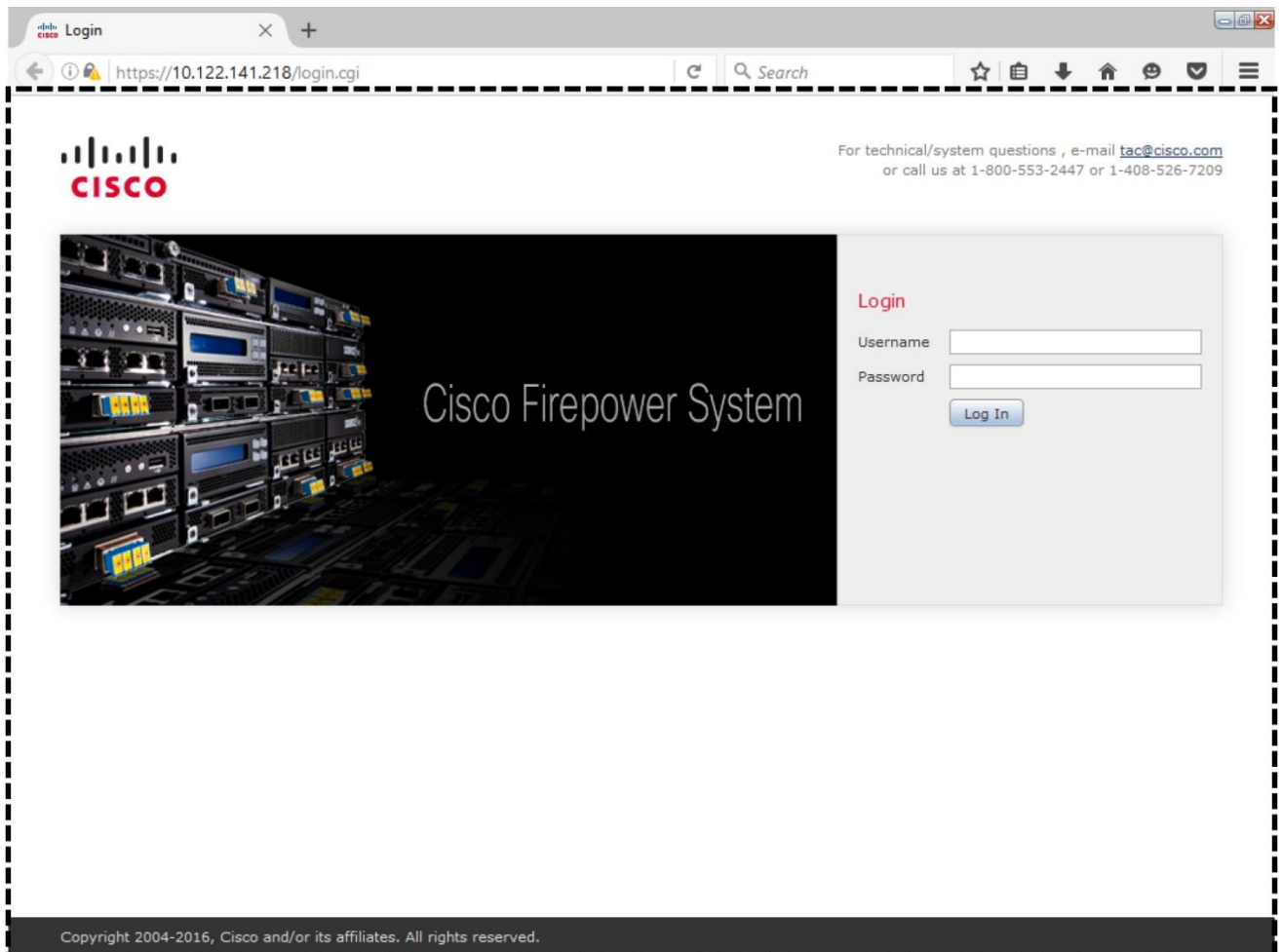


Figure 1-5. *The login page of a Firepower Management Center running Version 6.x.*

Did you notice that the login page template looks almost identical except the word FireSIGHT vs. Firepower, and the support contact information? The homepage of Version 4.x, however, is totally different than the pages on Version 5.x or 6.x.

[Figure 1-6](#) exhibits the home page of a management appliance running Version 4.x. It was called as a “Defense Center”.

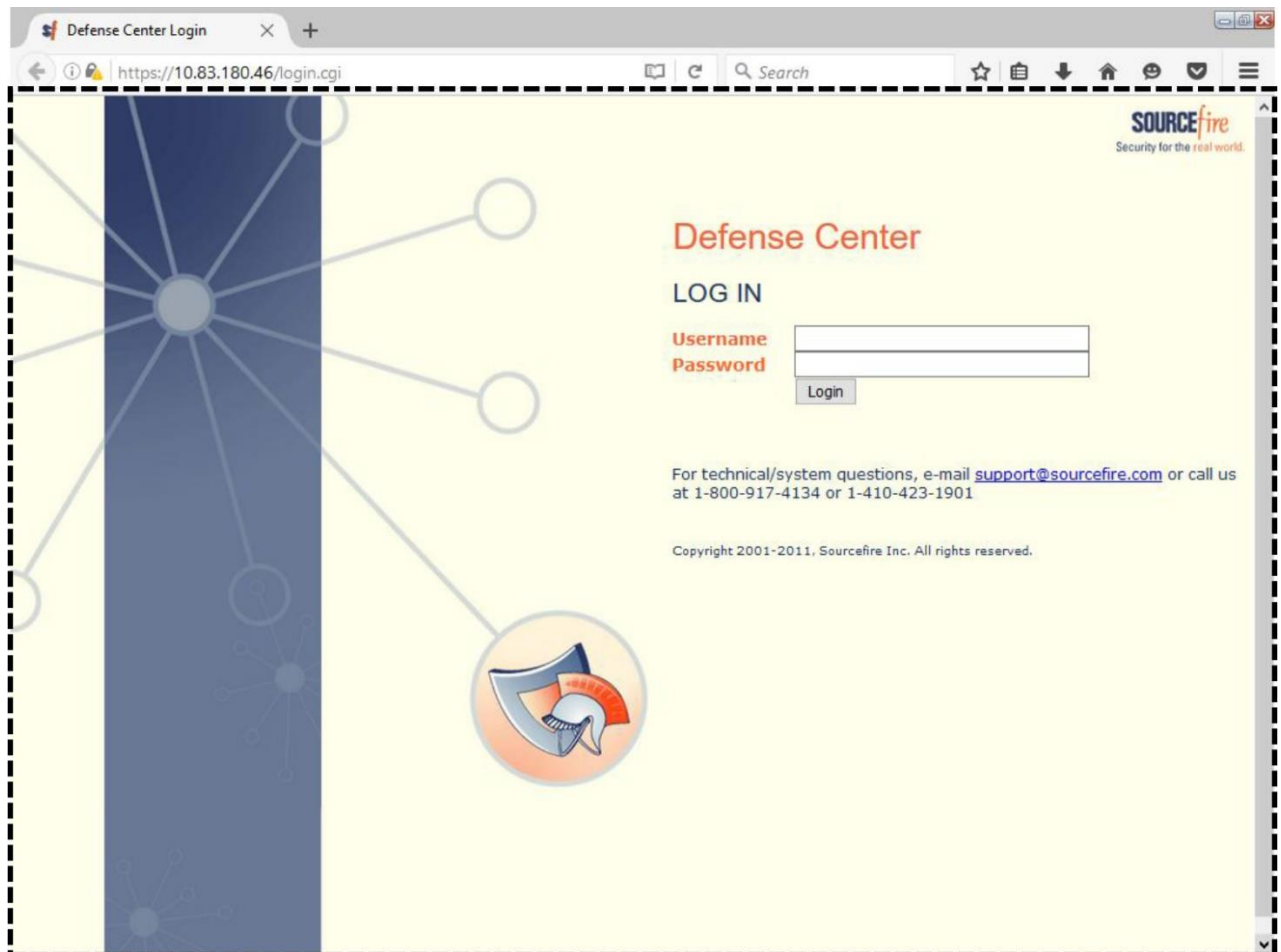


Figure 1-6. *The login page of a Defense Center running Version 4.x.*

Firepower Threat Defense (FTD)

Firepower Threat Defense (FTD) vs. FirePOWER Service

If you have just read the previous section, guess what is the difference between FirePOWER Services and Firepower Threat Defense (FTD)? Your assumption is right. The FirePOWER services refers to the features that are similar to the pre-acquisition period software releases, such as, Next Generation Intrusion Prevention System Virtual (NGIPSv). However, in the Firepower Threat Defense (FTD), Cisco converges all of the Sourcefire FirePOWER features, ASA Firewall features, as well as some additional new features into one single unified image.

[Figure 1-7](#) illustrates the convergence of Cisco ASA software with Sourcefire FirePOWER software into the Firepower Threat Defense code.

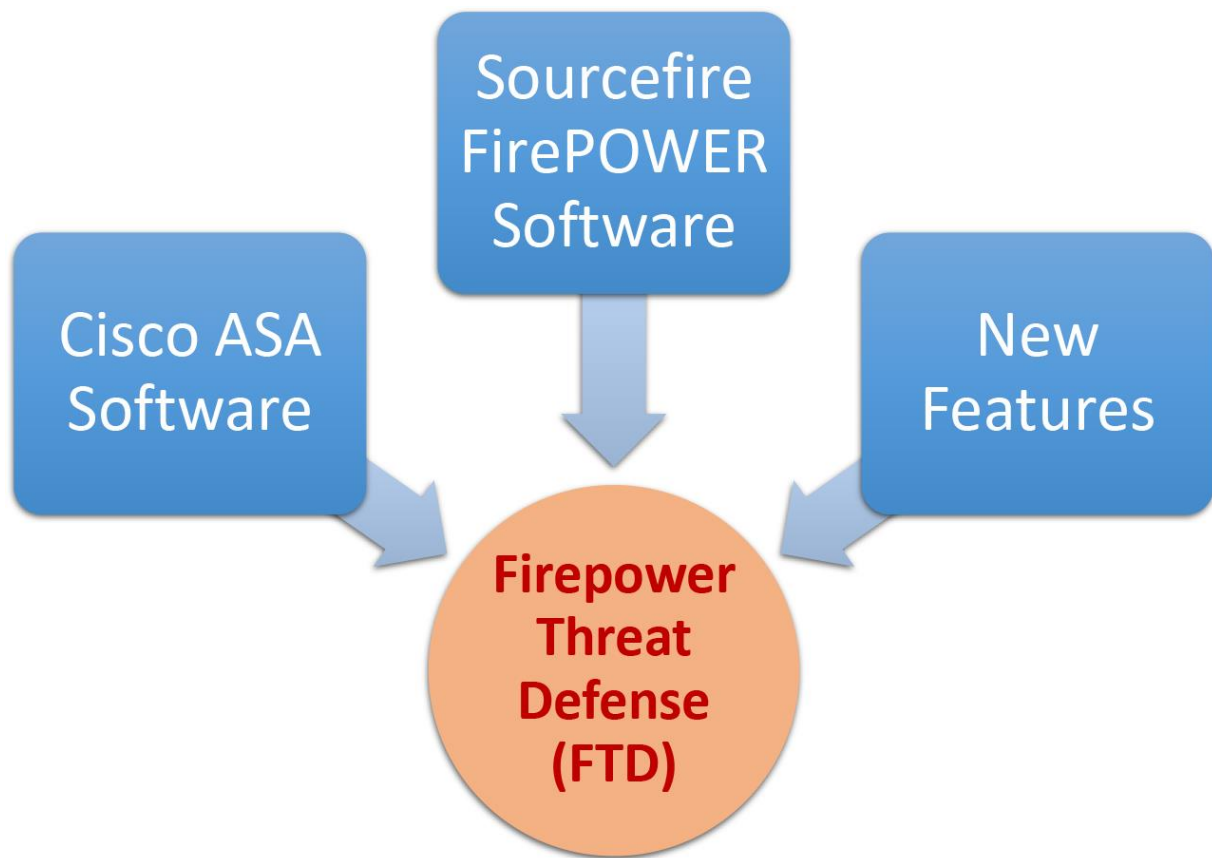


Figure 1-7. Logical representation of the Firepower Threat Defense (FTD) software

Due to this convergence, you no longer run the FirePOWER service as a separate service module. Therefore, it reduces overhead and increases efficiency.

Note

This book is written based on the Version 6.1 running on the Firepower Threat Defense (FTD). Although this book uses the ASA 5500-X series hardware, managed by a Firepower Management Center (FMC), you can still apply this knowledge on other platforms running Firepower technologies.

Software Components

A Firepower System offers lot of security features. Unlike any traditional Cisco ASA Firewall software, the security features of a Firepower System come in multiple software components. They are:

- **Firepower Core Software** – The core part of the software includes the Snort engine for intrusion detection and prevention, a web server for graphical user interface (GUI), a database to store events, any firmware for the hardware, etc. Depending on the hardware platform you are using, the core software image for your Firepower System is different.

- **Software Patch and Hotfix** – Cisco releases software patches periodically to address any security vulnerabilities, or to fix any defects with the Firepower System. When an issue demands a resolution earlier than a scheduled maintenance update, Cisco may release a Hotfix for it on case-by-case basis.
- **Snort Rules or Sourcefire Rules** – A special ruleset, used by the Snort engine, to detect and prevent any intrusion attempts. Each rule comprises of certain conditions. When a packet goes through a sensor and matches a condition in a Snort rule, the Snort engine takes an action accordingly.
- **Vulnerability Database (VDB)** – A database that stores vulnerability information and fingerprints of various applications, services and operating systems (OS). A Firepower System uses the fingerprints to discover the application, service and operating system running on a network host, and then it correlates the application and network discovery data with the vulnerability information on a VDB.
- **Geolocation Database (GeoDB)** – A database that stores various geographical information along with their associated IP addresses. For example, when a Firepower System displays an intrusion event in the GUI, you will be able to view the name and flag of the country that originated that intrusion attempt. It allows you to take any decision quickly without performing a reverse lookup for an IP address.
- **URL Filtering Database** – A Firepower System is able to categorize websites based on their targeted audience or business purpose. To give you more granular control, the system also allows you to control access to any certain type of website based on its reputation or known risk level. All of this information is stored into the URL Filtering database. Unlike any Firepower software components, any updates for the URL Filtering database is provided directly through the Cisco cloud — your Firepower Management Center must be connected to the internet.
- **Security Intelligence Feed:** The Cisco Threat Intelligence Team — known as Talos — is continuously researching the internet to identify any potential malicious IP addresses, domain names, and URLs. For Firepower System users, Talos shares their intelligence data through the Security Intelligence Feed. A Firepower Management Center can download the feed directly from the cloud.
- **Local Malware Detection:** With a malware license, Firepower Threat Defense can detect viruses on your files. It allows you to block the spread of a malware across your network. Firepower Threat Defense uses the Clam Anti-Virus engine to analyze files locally. Firepower Management Center obtains the signatures of latest viruses through the Local Malware Detection updates.
- **Integration:** You can integrate your Firepower System with various products and technologies, such as, Cisco Identity Services Engine (ISE), Microsoft Windows Active Directory Server, Event Streamer (eStreamer), Syslog Server, etc. It empowers you with unlimited opportunities to monitor and secure your network. This book focuses on core Firepower technologies. Any features related to integration are out of the scope of this book. Please read the official User Guide to learn more about integration.

[Figure 1-8](#) illustrates the various software components installed on the Firepower System. All these software components are explained in later chapters of this book.

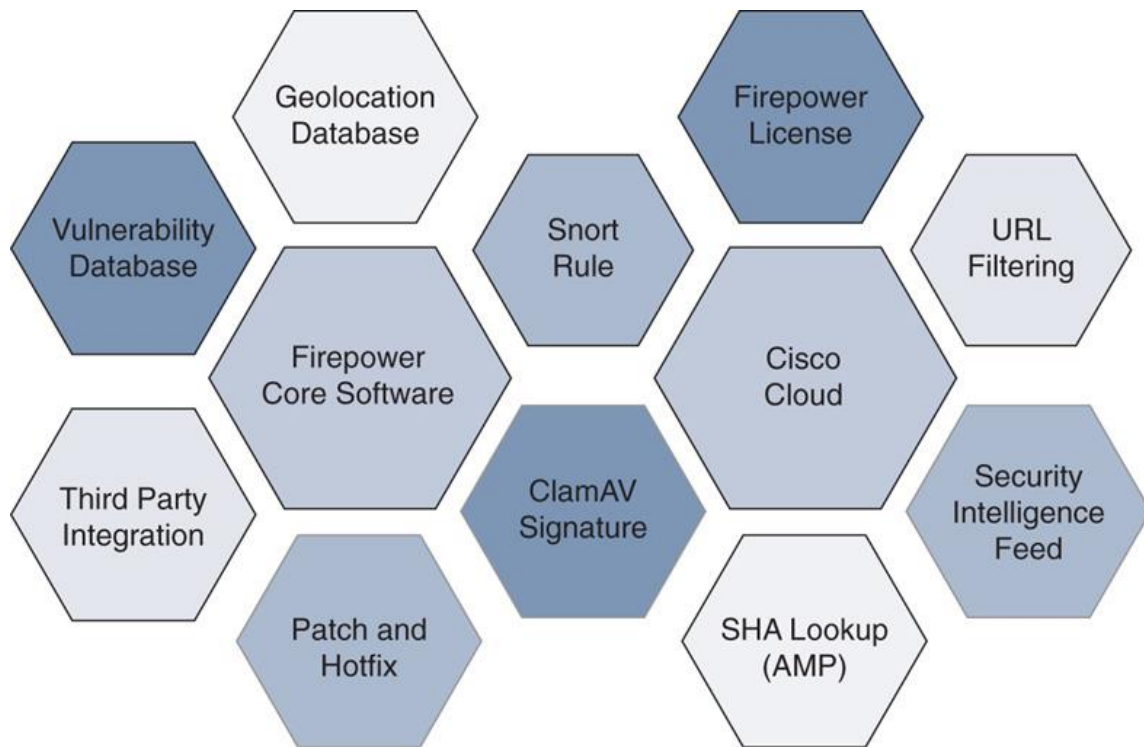


Figure 1-8. *Firepower System software components*

All of the software components are explained in the later chapters throughout this book, however, for now, just take a quick look at each of them.

Hardware Platforms

The Firepower Threat Defense Software Version 6.1 is available on wide variety of hardware platform. The internal architecture of each platform is different. There are, of course, differences in form factor, throughput and price. Later, in this book, you will learn more about the architectures and operations of a Firepower System.

[Table 1-2](#) summarizes the available hardware platforms (as of writing this book) that support the Firepower Threat Defense Software Version 6.1.

Hardware Category	Platform Name / Model Number
Cisco ASA 5500-X Series	ASA5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X, 5512-X, 5515-X, 5525-X, 5545-X, 5555-X
Firepower 2100 Series	Firepower 2110, 2120, 2130, 2140
Firepower 4100 Series	Firepower 4110, 4120, 4140, 4150
Firepower 9000 Series	Firepower 9300
Virtual	VMWare ESXi/vSphere, Kernel-Based Virtual Machine (KVM), Amazon Web Services (AWS)

Table 1-2. *Supported Hardware Platform for Firepower Threat Defense Software*

[Figure 1-9](#) illustrates the placement of various ASA and Firepower platforms in different types of networking environment. The throughput of appliances varies significantly depending on the number of enabled features, such as, Firewall (FW) only, or Firewall along with the Application Visibility and Control (AVC), the Next Generation Intrusion Prevention System (NGIPS), URL Filtering, SSL Decryption, etc.

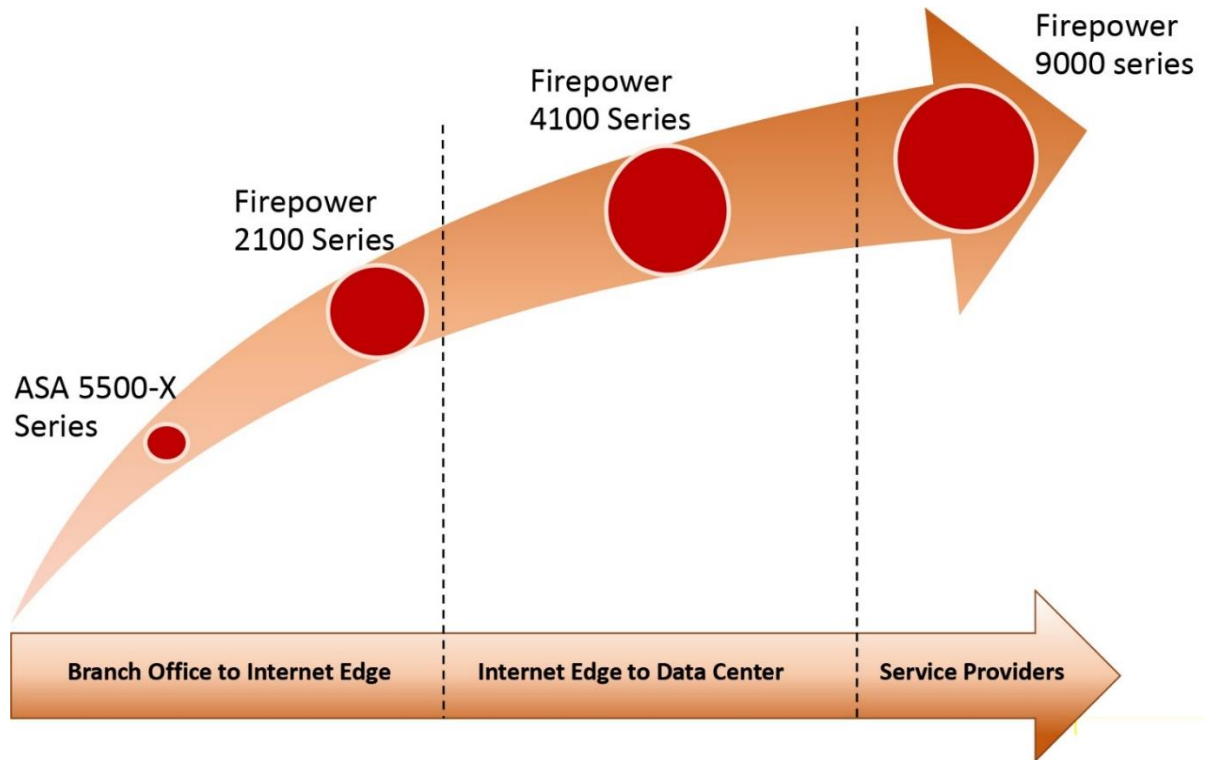


Figure 1-9. *Placement of ASA and Firepower appliances in various networking environments with different need.*

Note

To find out the latest hardware models that support FTD, and the throughput of every hardware model, please check the datasheet at cisco.com, or contact the representative of your account.

Out of the Box

After you open a brand new box of a Firepower appliance, you will find various accessories along with the actual appliance. The accessories are necessary to configure the initial setup and obtain a license.

[Figure 1-10](#) demonstrates the accessories that may come with a Cisco ASA 5506-X appliance, as example.



Figure 1-10. shows the items that you may receive when you order a Cisco ASA 5506-X appliance.

[Table 1-3](#) describes the items that are included in an ASA 5506-X package.

This table summarizes components that come with a 5506-X, doesn't match description above.

Number	Platform Name / Model Number
1	Appliance in the box (ASA 5506-X in this example)
2	Console Cable (DB-9 to RJ-45 in this example)
3	Envelope with the Product Activation Key (PAK)
4	Power Adapter
5	Power Cord, to connect with the power adapter

Table 1-3. *The ASA 5505-X Hardware and Its Accessories*

Note

The accessories in a box are subject to change, depends on various factors. In your box, you may receive more or less items than the items shown in this example.

Tip

Read the Installation Guide of your appliance model (available at cisco.com) to learn how to install it into a rack and power this up.

Summary

This chapter discusses the history and evolution of the Cisco Firepower Technology. It introduces various software components that may be installed on a Firepower System. This chapter also provides a quick overview of the supported hardware for the Cisco Firepower Threat Defense (FTD) technology.

The next few chapters of Part 1 demonstrate how to install the Firepower Threat Defense software on various hardware platforms. You will also learn how to identify any hardware related issues before beginning an advanced configuration.

Chapter 2. Firepower Threat Defense (FTD) on ASA 5500-X Series Hardware

If your ASA is currently running the FirePOWER Services as a separate module and you want to deploy the Firepower Threat Defense on your ASA, you have to reimage your ASA with the unified FTD image. This chapter discusses the steps to reimage and troubleshoot any Cisco ASA 5500-X Series Hardware.

Essential Knowledge

To reimage an ASA hardware with the Firepower Threat Defense, you need to utilize more than one type of image on the same hardware. This section describes the purpose of those images.

[Figure 2-1](#) shows the subsets of a Firepower Threat Defense software image that you install or upgrade on the Cisco ASA 5500-X Series hardware platforms during the FTD reimage process.

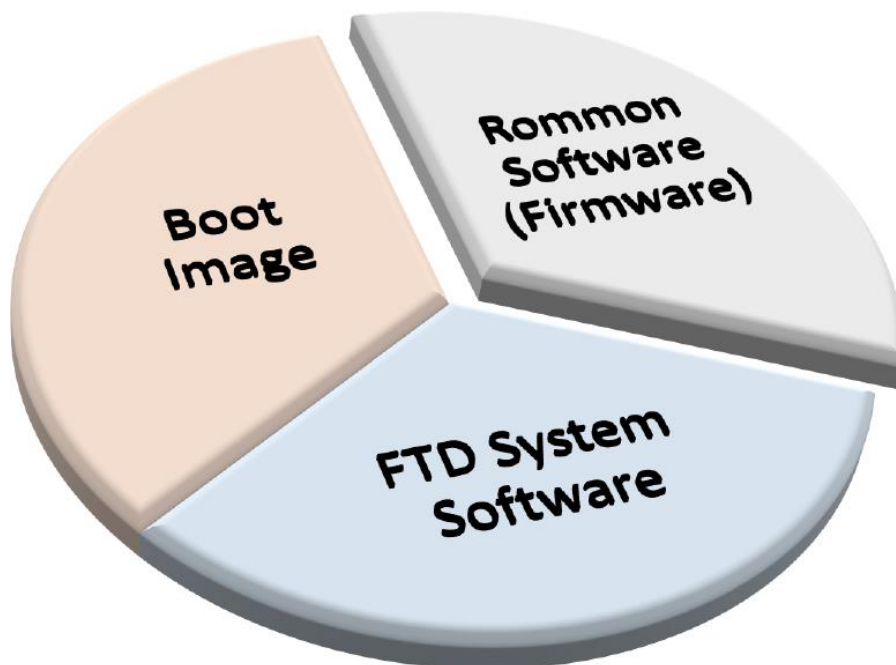


Figure 2-1. *Subsets of the Firepower Threat Defense Software*

- **Rommon Software:** The Rommon software is the firmware of an ASA. In an ASA, you enter into the Rommon mode in order to perform all of the necessary tasks to copy a boot image from an external server. If you are reimaging one of the low-end ASA hardware platforms, such as, ASA 5506-X, 5506W-X, 5506H-X, 5508-X, and 5516-X, you must update the firmware to the Release 1.1.8 or greater. If you are running one of the mid-range ASA hardware platforms, such as, 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X, and want to reimage it to the FTD software, you do not require to update the default firmware.

- **Boot Image:** The FTD boot image is a subset of the Firepower Threat Defense system software. After you load your ASA with an FTD boot image, you use the CLI of the boot image to prepare your ASA for the next level, that is, download the FTD System Software and begin the setup.

- **System Software:** All of the features of a Firepower Threat Defense are packaged in a System software image. You begin the FTD System Software installation from the CLI prompt of the boot image. This is the last step of a basic reimage process.

[Table 2-1](#) summarizes various types of software that you may have to install to complete the Firepower Threat Defense reimage process.

	Rommon Software	Boot Image	System Software
Purpose	To update the firmware of an ASA	To load an ASA with network config, and download the System software, and begin setup	To install the features of the Firepower Threat Defense System
Low-end 5506-X, 5508-X, 5516-X	Firmware release 1.1.8 or greater is required. Use the *.SPA file to upgrade firmware.	Use a *.lfbff file to load a low-end ASA with FTD Boot Image.	Use a *.pkg file to install the FTD system software package. You can use the same System Software package on any low-end and Mid-range ASA hardware models.
Mid-range 5512-X, 5515-X, 5525-X, 5545-X, 5555-X	Not necessary to update the default firmware version	Use a *.cdisk file to load a mid-range ASA with the FTD boot image.	

Table 2-1. *Software Images that are Required to Complete the FTD Reimage*

Best Practices For FTD Installation on ASA Hardware

Consider the following best practices before you reimage your ASA 5500-X Series hardware:

1. If you have just received a new ASA 5500-X, it may already have the Firepower Threat Defense software preinstalled. In such case, you just need to update the FTD to the latest release and complete the configurations. A reimage, however, is necessary when the hardware has traditional ASA software installed, or Firepower services are running as a separate module.
2. Perform the reimage during a maintenance window, because the process interrupts the network traffic.
3. Prior to your maintenance window, make sure you are able to access the cisco.com website, and entitled to download all of the FTD software. If are unable to access, register for a Cisco account. If the self-registration process does not allow you download a desired software, you may need to work with your Cisco Channel Partner or the Cisco Technical Assistance Center (TAC) for further assistance.
4. The reimage process may take about an hour, depending on the hardware model. However, you should plan for additional time to fulfill any prerequisites.
5. After you download any software from the Cisco.com, always verify the MD5 or SHA512 checksum of the files you have downloaded. It confirms that the file is not corrupt, or not modified during download.

[Figure 2-2](#) illustrates how the MD5 and SHA512 checksum values are displayed at cisco.com when you hover your mouse over a filename.

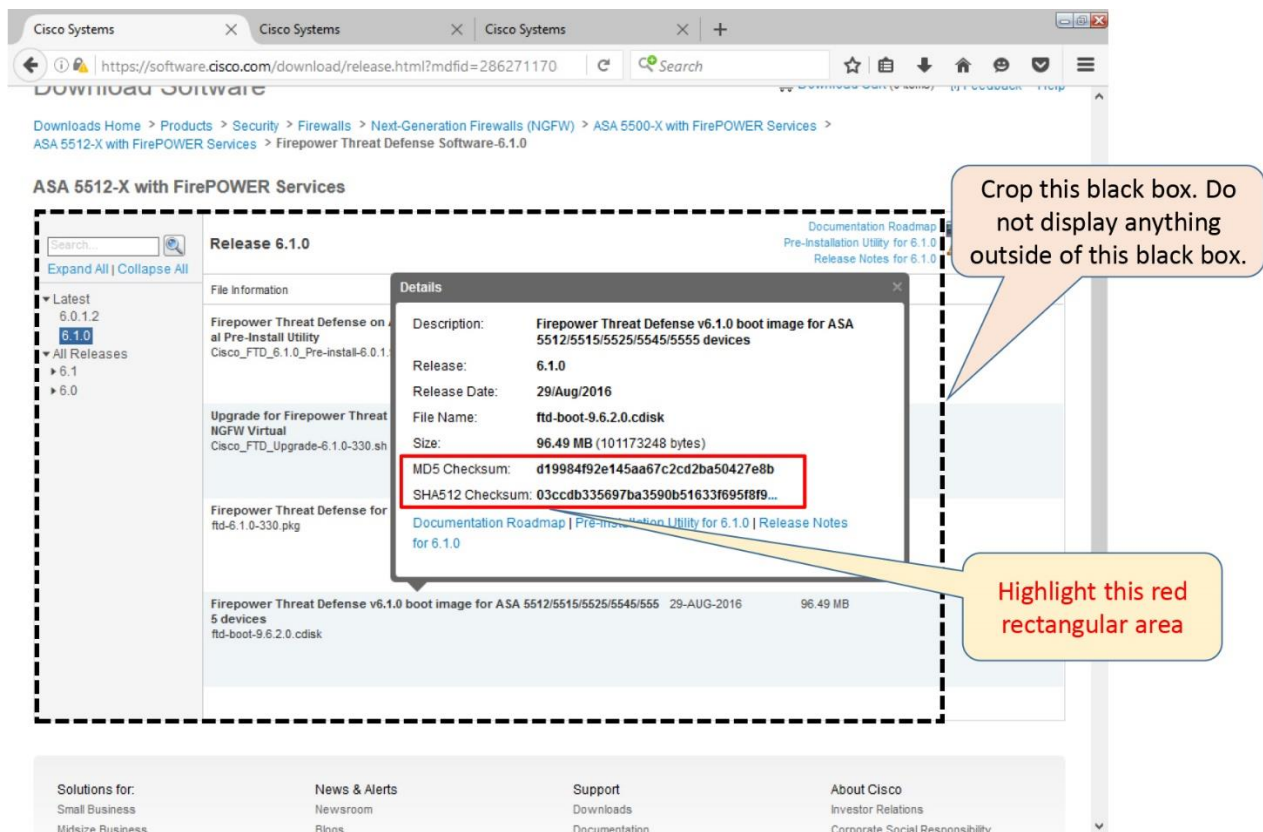


Figure 2-2. Checksum Values of a Boot Image File

6. Take a backup of the existing configurations. Reimage of an ASA with a FTD software wipes out all of the previous configurations.
7. Never power off, shutdown, or reboot an ASA hardware when the reimage is in progress. A login prompt appears after all of the reimage processes are complete.
8. Read the release notes to determine any known issues, any special requirements or instructions.

Configuration

In this section, you will learn the detail steps to install the Firepower Threat Defense system software on an ASA 5500-X Series hardware. Before you install anything on your ASA, there are some prerequisites. Once you fulfill them, you perform the remaining tasks (three steps for the low-end ASA hardware, and two steps for the mid-range hardware) of the reimage process.

[Figure 2-3](#) summarizes the steps to reimage an ASA 5500-X hardware to the Firepower Threat Defense (FTD) system software

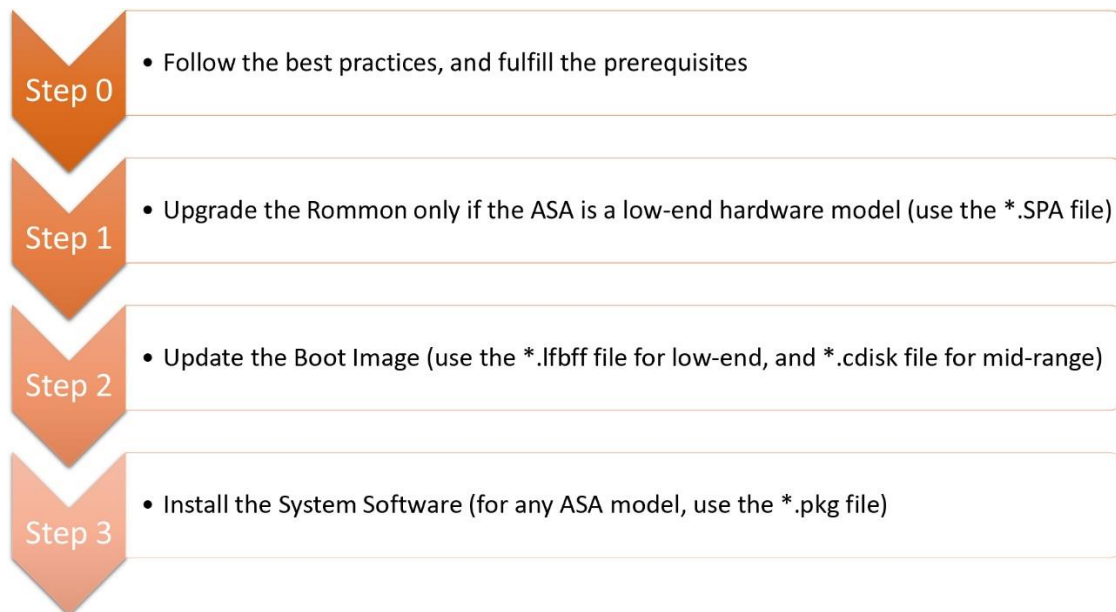


Figure 2-3. *Major Steps to Reimage an ASA 5500-X Series Hardware*

Prerequisites

You must fulfill the following requirements before you begin a reimage:

- Storage

1. To install FTD software, an ASA requires at least 3GB free space plus additional spaces to store an FTD boot image (which is usually about 100MB). Read the Verification and Troubleshooting Tools section to learn how to determine the free disk space of an ASA.
2. Make sure the ASA has an SSD installed. Read the Verification and Troubleshooting Tools section to learn how to determine if there is any SSD installed in your ASA.

Caution

If you have installed an SSD for the first time, or replaced an SSD in one of your mid-range ASA hardware, you must reload your ASA, and then you reimage or reinstall any software.

- Connectivity

1. Using a console cable, connect your computer to the console port of the ASA that you want to reimage.
2. Have an access to a TFTP and HTTP server. You use the TFTP server to copy the firmware and boot image files to the ASA during reimage process. You copy the FTD System Software from the HTTP server to the ASA. You can use an FTP server in lieu of an HTTP server, however, you may find a basic HTTP server is easier to setup.

[Figure 2-4](#) exhibits a topology where the management network is segregated from the data traffic, as a security best practice. An administrator computer is directly connected to an ASA through a console cable, while it also has access to the management network.

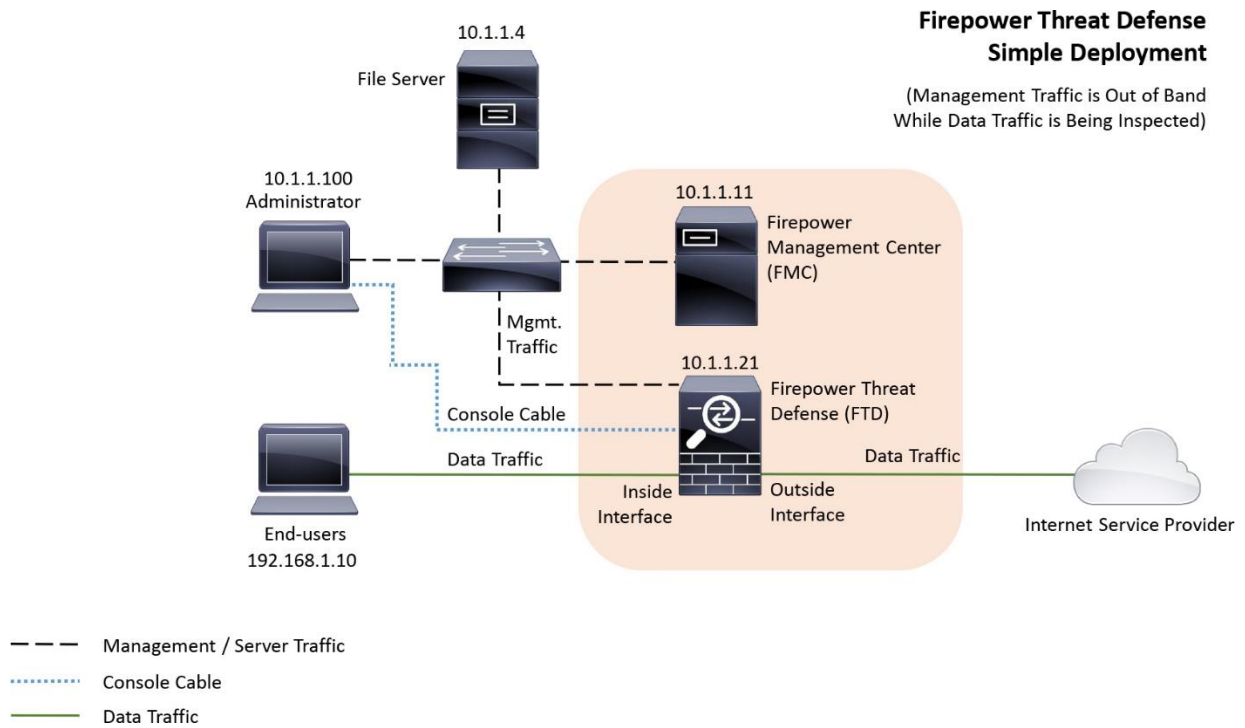


Figure 2-4. A Simple Topology Where an ASA Inspects Data Traffic and Keeps Any Management Traffic Isolated

[Figure 2-5](#) exhibits the simplest topology that provides both console and IP connectivity between an ASA and a computer, and allows an administrator to perform reimage and basic configuration.

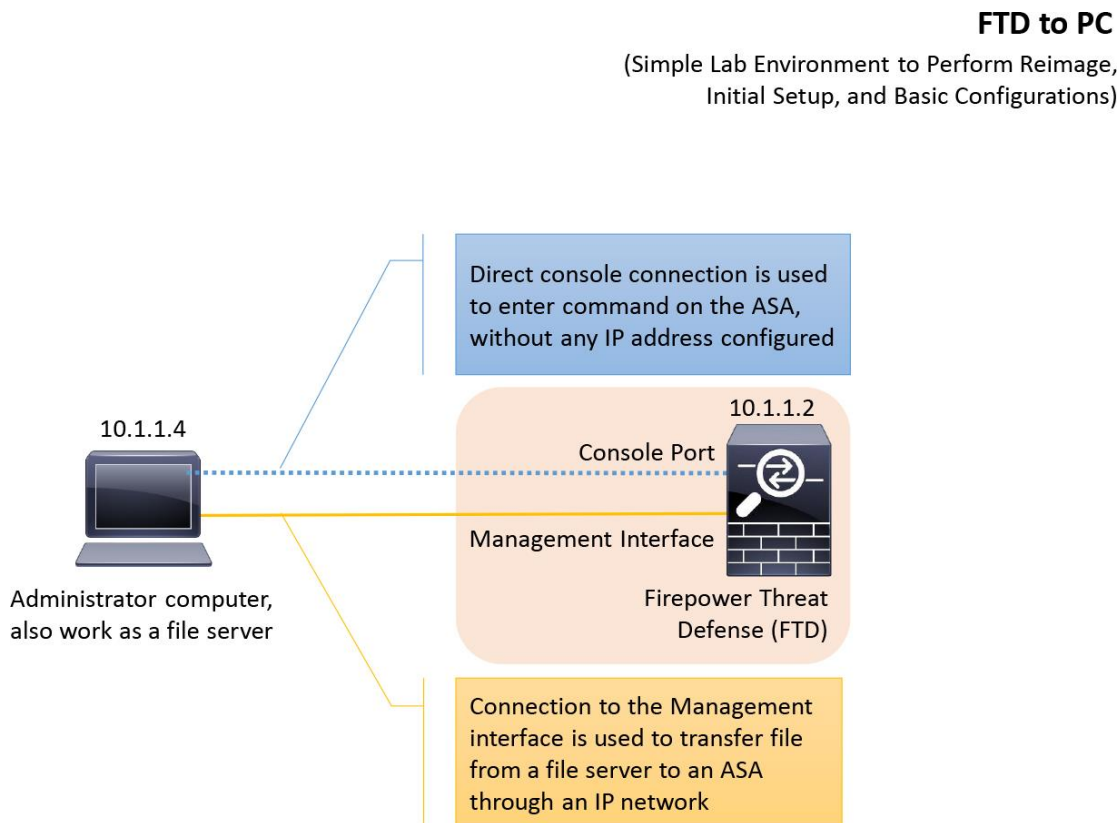


Figure 2-5. *The Most Basic Connectivity Between an ASA and a Computer (Server) That Allows You to Perform Reimage and Basic Setup*

Upgrade Firmware

If you plan to reimage one of the low-end ASA hardware models, such as, 5506-X, 5508-X, and 5516-X, to the Firepower Threat Defense software, you must make sure that the firmware version of the ASA is 1.1.8 or greater. Read the Verification and Troubleshooting Tools section to learn the ways to determine the firmware version.

Note

You do not need to upgrade the default firmware of any mid-range ASA hardware models, such as, 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X. Therefore, you can skip this section if you are running one of the mid-range ASA models.

The steps to upgrade the Firmware (Rommon software) of a low-end ASA model is described below:

1. Download the Rommon software from the cisco.com, and store it to your TFTP server.

[Figure 2-6](#) shows the Rommon software file **asa5500-firmware-1108.SPA** that you use to upgrade the firmware of a low-end ASA 5500-X Series hardware before you begin the reimage process.

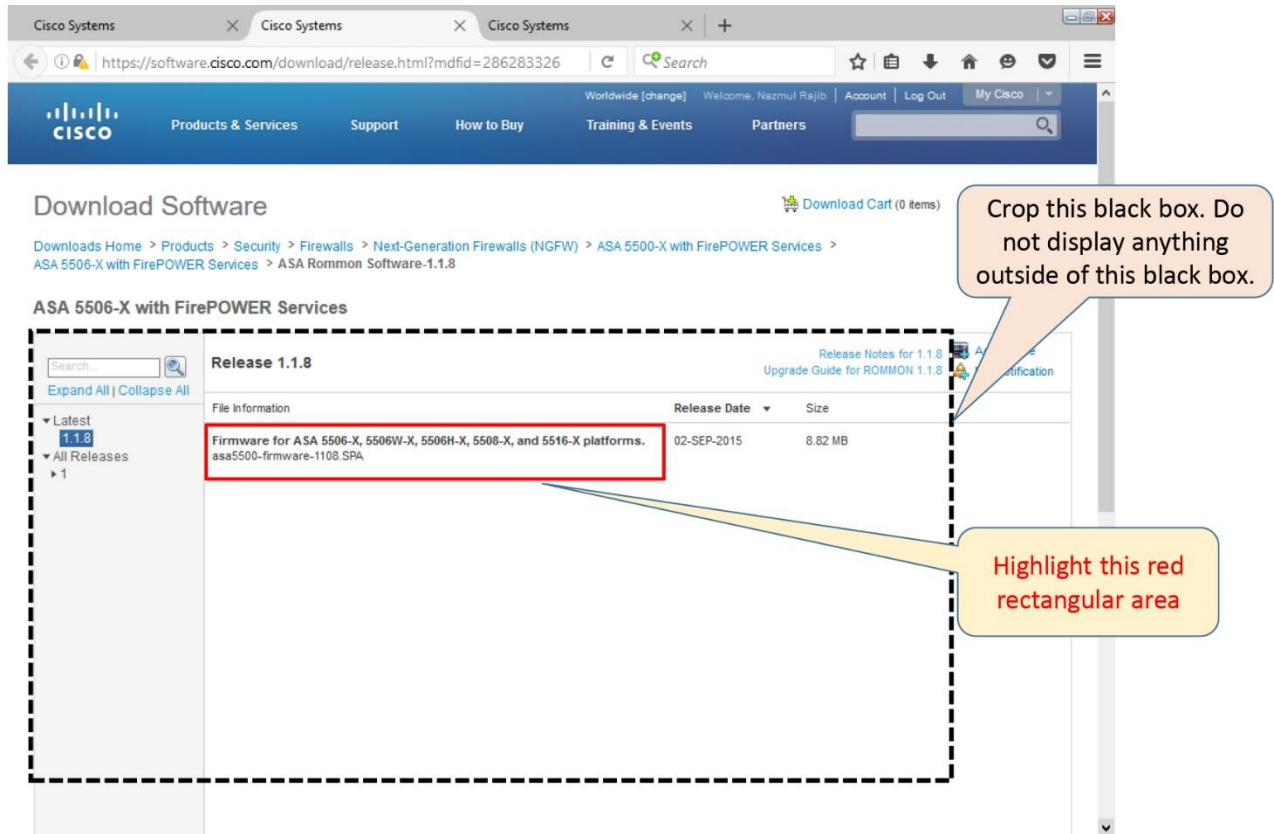


Figure 2-6. *The Rommon Software File Information*

2. Copy the file from your TFTP server to your ASA storage. To copy a file from a TFTP server to an ASA, run the following command:

```
ciscoasa# copy tftp://TFTP_server_address/filename disk0:
```

[Example 2-1](#) shows a Rommon software file **asa5500-firmware-1108.SPA** is successfully copied from a TFTP server (IP address 10.1.1.4, for example) to the storage of an ASA 5506-X hardware.

Example 2-1 *Command to Copy a File from a TFTP Server to an ASA*

```
ciscoasa# copy tftp://10.1.1.4/asa5500-firmware-1108.SPA disk0:
```

```
Address or name of remote host [10.1.1.4]?
```

```
Source filename [asa5500-firmware-1108.SPA]?
```

Destination filename [asa5500-firmware-1108.SPA]?

Accessing tftp://10.1.1.4/asa5500-firmware-1108.SPA...!!!!!!!!!!!!

Done!

Computed Hash SHA2: d824bdeecee1308fc64427367fa559e9
 eefe8f182491652ee4c05e6e751f7a4f
 5cdea28540cf60acde3ab9b65ff55a9f
 4e0cfb84b9e2317a856580576612f4af

Embedded Hash SHA2: d824bdeecee1308fc64427367fa559e9
 eefe8f182491652ee4c05e6e751f7a4f
 5cdea28540cf60acde3ab9b65ff55a9f
 4e0cfb84b9e2317a856580576612f4af

Digital signature successfully validated

Writing file disk0:/asa5500-firmware-1108.SPA...

!!!!!!!!!!!!

9241408 bytes copied in 8.230 secs (1155176 bytes/sec)

ciscoasa#

3. Once the file is copied successfully, begin the upgrade by running the following command:

ciscoasa# **upgrade rommon disk0:/asa5500-firmware-1108.SPA**

[Example 2-2](#) shows the command to upgrade the firmware of an ASA. After the Rommon software file is verified, the ASA prompts for a confirmation to reload.

Example 2-2 Command to Begin the Rommon Upgrade

ciscoasa# **upgrade rommon disk0:/asa5500-firmware-1108.SPA**

Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

Computed Hash SHA2: d824bdeecee1308fc64427367fa559e9
 eefe8f182491652ee4c05e6e751f7a4f
 5cdea28540cf60acde3ab9b65ff55a9f
 4e0cfb84b9e2317a856580576612f4af

Embedded Hash SHA2: d824bdeecee1308fc64427367fa559e9
 eefe8f182491652ee4c05e6e751f7a4f
 5cdea28540cf60acde3ab9b65ff55a9f

4e0cfb84b9e2317a856580576612f4af

```
Digital signature successfully validated
File Name           : disk0:/asa5500-firmware-1108.SPA
Image type          : Release
  Signer Information
    Common Name      : abraxas
    Organization Unit : NCS_Kenton_ASA
    Organization Name : CiscoSystems
    Certificate Serial Number : 55831CF6
    Hash Algorithm    : SHA2 512
    Signature Algorithm : 2048-bit RSA
    Key Version       : A
Verification successful.
Proceed with reload? [confirm]
```

3. Press the **Enter** key to confirm.

[Example 2-3](#) illustrates the reload of an ASA after the firmware upgrade starts.

Example 2-3 *An ASA Reloads After an Upgrade Starts*

```
***
*** --- START GRACEFUL SHUTDOWN ---
***
*** Message to all terminals:
***
***   Performing upgrade on rom-monitor.
Shutting down isakmp
Shutting down webvpn
Shutting down sw-module
Shutting down License Controller
Shutting down File system
***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   Performing upgrade on rom-monitor.
Process shutdown finished
Rebooting... (status 0x9)
..
INIT: Sending processes the TERM signal
Stopping OpenBSD Secure Shell server: sshdno /usr/sbin/sshd found; none
killed
Deconfiguring network interfaces... done.
Sending all processes the TERM signal...
Sending all processes the KILL signal...
Deactivating swap...
Unmounting local filesystems...
Rebooting...
```

4. Upon reload, the ASA begins the firmware upgrade process. During the process, the ASA reboots automatically few times.

Notes

Do not reboot an ASA manually while the Rommon or firmware upgrade is in progress.

[Example 2-4](#) shows the ASA completes the step 1 and step 2 of the Rommon upgrade process. The system reloads every time it completes a step.

Example 2-4 *Illustrates the Steps of a Rommon Upgrade*

```
Rom image verified correctly
Cisco Systems ROMMON, Version 1.1.01, RELEASE SOFTWARE
Copyright (c) 1994-2014 by Cisco Systems, Inc.
Compiled Mon 10/20/2014 15:59:12.05 by builder

Current image running: Boot ROM0
Last reset cause: PowerCycleRequest
DIMM Slot 0 : Present
INFO: Rommon upgrade state: ROMMON_UPG_START (1)
INFO: Reset code: 0x00002000
Firmware upgrade step 1...
Looking for file 'disk0:/asa5500-firmware-1108.SPA'
Located 'asa5500-firmware-1108.SPA' @ cluster 1608398.
#####
#####
###
#####
Image base 0x77014018, size 9241408
LFBFF signature verified.
Objtype: lfbff_object_rommon (0x800000 bytes @ 0x77014238)
Objtype: lfbff_object_fpga (0xd0100 bytes @ 0x77814258)
INFO: FPGA version in upgrade image: 0x0202
INFO: FPGA version currently active: 0x0202
INFO: The FPGA image is up-to-date.
INFO: Rommon version currently active: 1.1.01.
INFO: Rommon version in upgrade image: 1.1.08.
Active ROMMON: Preferred 0, selected 0, booted 0
Switching SPI access to standby rommon 1.
Please DO NOT reboot the unit, updating ROMMON.....
INFO: Duplicating machine state.....
Reloading now as step 1 of the rommon upgrade process...

Toggling power on system board...
Rom image verified correctly

Cisco Systems ROMMON, Version 1.1.01, RELEASE SOFTWARE
Copyright (c) 1994-2014 by Cisco Systems, Inc.
Compiled Mon 10/20/2014 15:59:12.05 by builder

Current image running: Boot ROM0
Last reset cause: RP-Reset
DIMM Slot 0 : Present
INFO: Rommon upgrade state: ROMMON_UPG_START (1)
INFO: Reset code: 0x00000008
Active ROMMON: Preferred 0, selected 0, booted 0
Firmware upgrade step 2...
Detected current rommon upgrade is available, continue rommon upgrade
process
Rommon upgrade reset 0 in progress
Reloading now as step 2 of the rommon upgrade process...
```

5. After step 1 and step 2 of the upgrade process, when the ASA reloads, the Rommon version shows 1.1.8. The process, however, is still in progress. Do not reboot the system until the system prompts you to do so.

[Example 2-5](#) shows the Rommon Version is updated to 1.1.8 (after the Step 2) although the upgrade is in progress. Once complete, the ASA prompts for a manual or automatic reboot. You can just wait few seconds, and let the system to reboot by itself.

Example 2-5 The Last Stage of the Rommon Upgrade Process

```
Rom image verified correctly
Cisco Systems ROMMON, Version 1.1.8, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Thu 06/18/2015 12:15:56.43 by builders

Current image running: *Upgrade in progress* Boot ROM1
Last reset cause: BootRomUpgrade
DIMM Slot 0 : Present
INFO: Rommon upgrade state: ROMMON_UPG_START (1)
INFO: Reset code: 0x00000010
PROM B: stopping boot timer
Active ROMMON: Preferred 0, selected 0, booted 1
INFO: Rommon upgrade state: ROMMON_UPG_TEST

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!! Please manually or auto boot ASAOS now to complete firmware upgrade !!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Platform ASA5506 with 4096 Mbytes of main memory
MAC Address: a4:6c:2a:e4:6b:bf
Using default Management Ethernet Port: 0

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot in 5 seconds.
```

6. At this stage, the Rommon software is fully upgraded. You are ready to begin the next step of the reimage process.

[Example 2-6](#) shows a confirmation message for the successful Rommon upgrade, after the final reboot.

Example 2-6 Demonstration of the Completion of a Successful Upgrade

```
Located '.boot_string' @ cluster 1607965.

#
Attempt autoboot: "boot disk0:/asa961-50-lfbff-k8.spa"
Located 'asa961-50-lfbff-k8.spa' @ cluster 10.

#####
#####
#####
#####
#####
LFBFF signature verified.
INIT: version 2.88 booting
Starting udev
Configuring network interfaces... done.
Populating dev cache
dosfsck 2.11, 12 Mar 2005, FAT32, LFN
There are differences between boot sector and its backup.
```

```

Differences: (offset:original/backup)
 65:01/00
  Not automatically fixing this.
Starting check/repair pass.
Starting verification pass.
/dev/sdb1: 104 files, 811482/1918808 clusters
dosfsck(/dev/sdb1) returned 0
Mounting /dev/sdb1
Setting the offload CPU count to 0
IO Memory Nodes: 1
IO Memory Per Node: 205520896 bytes

Global Reserve Memory Per Node: 314572800 bytes Nodes=1

LCMB: got 205520896 bytes on numa-id=0, phys=0x10d400000,
virt=0x2aaaab000000
LCMB: HEAP-CACHE POOL got 314572800 bytes on numa-id=0, virt=0x7fedbc200000
Processor memory: 1502270072

Compiled on Fri 04-Mar-16 10:50 PST by builders
Total NICs found: 14
i354 rev03 Gigabit Ethernet @ irq255 dev 20 index 08 MAC: a46c.2ae4.6bbf
ivshmem rev03 Backplane Data Interface @ index 09 MAC: 0000.0001.0002
en_vtun rev00 Backplane Control Interface @ index 10 MAC: 0000.0001.0001
en_vtun rev00 Backplane Int-Mgmt Interface @ index 11 MAC:
0000.0001.0003
en_vtun rev00 Backplane Ext-Mgmt Interface @ index 12 MAC:
0000.0000.0000
en_vtun rev00 Backplane Tap Interface @ index 13 MAC: 0000.0100.0001
Rom-monitor was successfully upgraded.
Verify the activation-key, it might take a while...
.
.
! Licensing and legal information are omitted for brevity
.
.
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Reading from flash...
!.
Cryptochecksum (unchanged): 868f669d 9e09ca8b e91c32de 4ee8fd7f

INFO: Power-On Self-Test in process.
.....
INFO: Power-On Self-Test complete.
INFO: Starting HW-DRBG health test...
INFO: HW-DRBG health test passed.

INFO: Starting SW-DRBG health test...
INFO: SW-DRBG health test passed.
Type help or '?' for a list of available commands.
ciscoasa>

```

When an ASA is running, you can also manually check its Rommon software version. The related command has been discussed in the Verification and Troubleshooting Tools section of this chapter.

[Example 2-7](#) shows the current firmware version is upgraded to 1.1.8.

Example 2-7 The Upgraded Firmware Version

```
ciscoasa> enable
Password: *****
ciscoasa# show module
```

Mod No.	Card Type	Model	Serial
1	ASA 5506-X with FirePOWER services, 8GE, AC,	ASA5506	
JAD191100HG	sfr Unknown	N/A	
JAD191100HG			

Mod	MAC Address Range	Hw Version	Fw Version	Sw Version
1	a46c.2ae4.6bbf to a46c.2ae4.6bc8	1.0	1.1.8	9.6(1)50
sfr	a46c.2ae4.6bbe to a46c.2ae4.6bbe	N/A	N/A	

Mod Version	SSM Application Name	Status	SSM Application

Mod	Status	Data Plane Status	Compatibility
1	Up Sys	Not Applicable	
sfr	Unresponsive	Not Applicable	

```
ciscoasa#
Install Boot Image
```

The setup of the Firepower Threat Defense software has to begin from the command line interface (CLI) of a boot image which is developed for the FTD. To access the CLI of the boot image, you need to reload the ASA with the FTD boot. This section discusses the list of tasks that are necessary to reload an ASA with an appropriate boot image on any ASA 5500-X Series hardware.

1. Download the appropriate boot image for your ASA hardware.

Note

All of the steps to reload an ASA with a boot image are same for any ASA 5500-X hardware except the boot image file you use. For a low-end and mid-range ASA hardware, use the *.lfbff file and *.cdisk file respectively.

[Figure 2-7](#) shows the Boot Image file **ftd-boot-9.6.2.0.lfbff** that you use during the reimage process of an ASA 5506-X, 5508-X and 5516-X hardware.

Download Software

Downloads Home > Products > Security > Firewalls > Next-Generation Firewalls (NGFW) > ASA 5500-X with FirePOWER Services > ASA 5506-X with FirePOWER Services > Firepower Threat Defense Software-6.1.0

ASA 5506-X with FirePOWER Services

File Information	Release Date	Size
Firepower Threat Defense on ASA with FirePOWER Services and NGFW Virtual Pre-Install Utility Cisco_FTD_6.1.0_Pre-install-6.0.1.999-1224.sh	29-AUG-2016	31.08 MB
Upgrade for Firepower Threat Defense on ASA with FirePOWER Services and NGFW Virtual Cisco_FTD_Upgrade-6.1.0-330.sh	29-AUG-2016	913.86 MB
Firepower Threat Defense for ASA 55XX series v6.1.0 ftd-6.1.0-330.pkg	29-AUG-2016	919.73 MB
Firepower Threat Defense boot image v6.1.0 for ASA 5506/5508/5516 devices ftd-boot-9.6.2.0.lfbff	29-AUG-2016	96.25 MB

Figure 2-7. The *.lfbff Boot Image File for any Low-End ASA 5500-X Series Hardware

[Figure 2-8](#) shows the Boot Image file **ftd-boot-9.6.2.0.cdisk** that you need during the reimage of an ASA 5512-X, 5515-X and 5525-X, 5545-X, and 5555-X hardware.

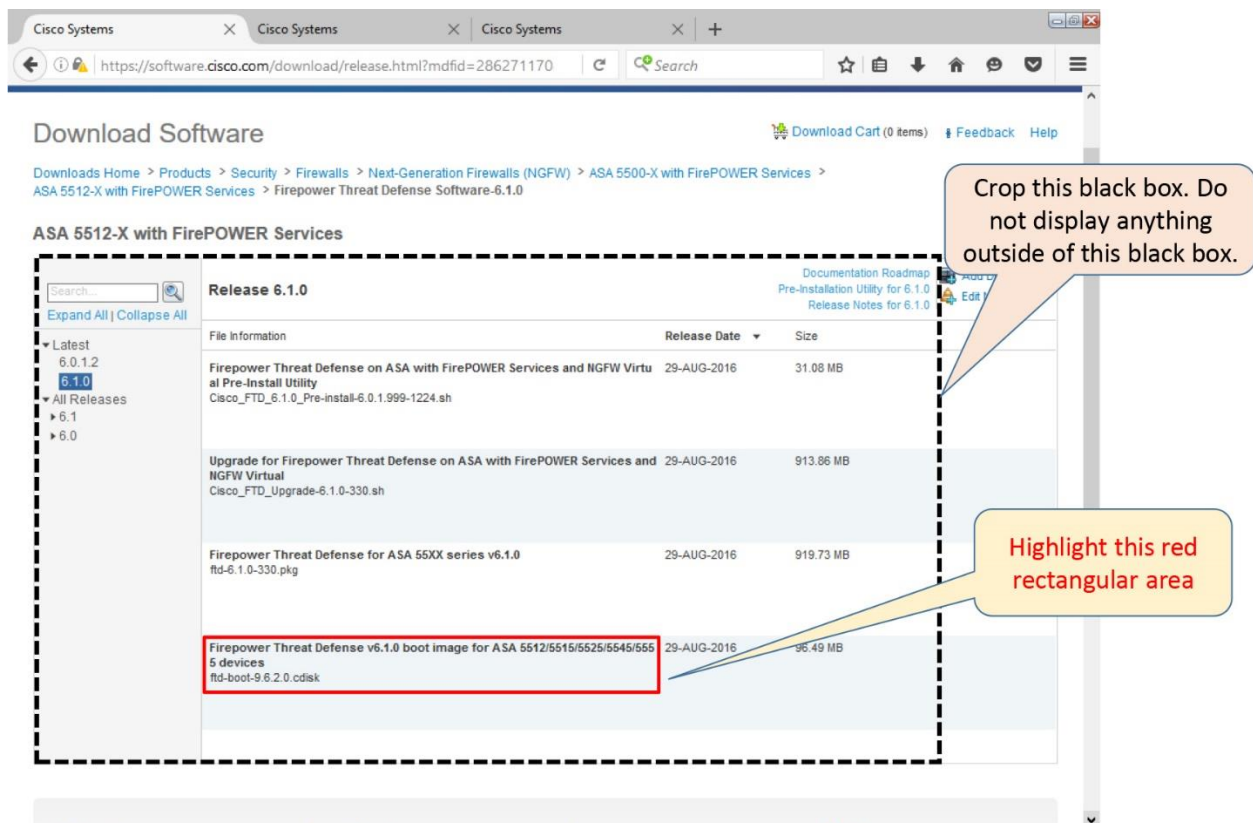


Figure 2-8. The *.cdisk Boot Image File for any Mid-Range ASA 5500-X Series Hardware

2. Reload the ASA.

[Example 2-8](#) shows the ASA is shutting down all of its processes before it gracefully reboots.

Example 2-8 The Reload of an ASA

```

ciscoasa# reload
Proceed with reload? [confirm]
ciscoasa#
***
*** --- START GRACEFUL SHUTDOWN ---
Shutting down isakmp
Shutting down webvpn
Shutting down sw-module
Shutting down License Controller
Shutting down File system
***
*** --- SHUTDOWN NOW ---
Process shutdown finished
Rebooting... (status 0x9)
..
INIT: Sending processes the TERM signal
Stopping OpenBSD Secure Shell server: sshdno /usr/sbin/sshd found; none
killed
Deconfiguring network interfaces... done.
Sending all processes the TERM signal...
Sending all processes the KILL signal...
Deactivating swap...
Unmounting local filesystems...

```

Rebooting...

3. Interrupt the boot up process by pressing the ESC key.

[Example 2-9](#) shows that the boot up process is interrupted and the ASA entered into the rommon mode.

Example 2-9 *Interruption of a Boot Up Process*

```
Rom image verified correctly

Cisco Systems ROMMON, Version 1.1.8, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Thu 06/18/2015 12:15:56.43 by builders

Current image running: Boot ROM1
Last reset cause: PowerCycleRequest
DIMM Slot 0 : Present

Platform ASA5506 with 4096 Mbytes of main memory
MAC Address: a4:6c:2a:e4:6b:bf
Using default Management Ethernet Port: 0

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot in 7 seconds.
Boot interrupted.
rommon 1 >
```

4. The rommon configuration mode has limited command options. You can run the **help** command to see the list of available options.

[Example 2-10](#) shows the available commands in the rommon configuration mode. The commands that are used to install the boot image are highlighted.

Example 2-10 *Available Commands in the Rommon Configuration Mode*

```
rommon 1 > help
? Display this help menu
address Set the local IP address
boot Boot an application program
confreg Configuration register contents display and management
console Console BAUD rate display and configuration
dev Display a list of available file system devices
dir File directory display command
erase erase the specified file system
file Set the application image file path/name to be TFTPed
gateway Set the default gateway IP address
help "help" for this menu
"help <command>" for specific command information
history Show the command line history
netmask Set the IP subnet mask value
ping Test network connectivity with ping commands
server Set the TFTP server IP address
show Display system device and status information
tftpdnld Download and run the image defined by "FILE"
reboot Reboot the system
```

reload	Reboot the system
repeat	Repeat a CLI command
reset	Reboot the system
set	Display the configured environment variables
sync	Save the environment variables to persistent storage
unset	Clear a configured environment variable

5. Configure the network.

[Example 2-11](#) shows the options that must configure to begin successful network communication between the ASA, FMC, and the other servers.

Example 2-11 *Commands to Configure the Network Settings in Rommon Mode*

```
rommon 2 > address 10.1.1.21
rommon 3 > netmask 255.255.255.0
rommon 4 > gateway 10.1.1.1
rommon 5 > server 10.1.1.4
```

Note

The IP addresses on the above configurations are based on the topology on the [Figure 2-4](#). Here, the ASA, FMC, and all other servers are in the same switching network, therefore, their IP addresses are in the same subnet. If the ASA, FMC and the servers are in different subnets, the ingress interface of the router (where the ASA is deployed) becomes the gateway for the ASA.

6. Test the connectivity from the ASA to the TFTP server where the image files are stored.

[Example 2-12](#) confirms that the ASA is able to communicate with the TFTP server.

Example 2-12 *A Successful Ping Test from the ASA to the TFTP Server*

```
rommon 6 > ping 10.1.1.4
Sending 10, 32-byte ICMP Echoes to 10.1.1.4 timeout is 4 seconds
!!!!!!!!!!!!!!
Success rate is 100 percent (10/10)
```

7. Once the connectivity is established, provide the name of the boot image file you want to download from the TFTP server, save the changes, and begin the download.

[Example 2-13](#) illustrates that the ASA 5506-X has downloaded a boot image file ftd-boot-9.6.2.0.lfbff successfully from a TFTP server.

Caution

If you are reimaging one of the mid-range ASA hardware, such as, 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X, you must use the ftd-boot-9.6.2.0.cdisk file instead of the ftd-boot-9.6.2.0.lfbff file.

Example 2-13 Commands to Select and Download a File from a TFTP server to an ASA

```
rommon 7 > file ftd-boot-9.6.2.0.lfbff
rommon 8 > sync
rommon 9 > tftpdnld
      ADDRESS: 10.1.1.21
      NETMASK: 255.255.255.0
      GATEWAY: 10.1.1.1
      SERVER: 10.1.1.4
      IMAGE: ftd-boot-9.6.2.0.lfbff
      MACADDR: a4:6c:2a:e4:6b:bf
      VERBOSITY: Progress
      RETRY: 20
      PKTTIMEOUT: 60
      BLKSIZE: 1460
      CHECKSUM: Yes
      PORT: GbE/1
      PHYMODE: Auto Detect
```

```
Receiving ftd-boot-9.6.2.0.lfbff from
10.1.1.4!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
File reception completed.
```

8. Finally, the ASA boots up automatically with the FTD boot CLI. Now you are ready to install the FTD system software package on your ASA.

[Example 2-14](#) illustrates the launch of the FTD boot CLI on an ASA.

Example 2-14 Boot Up Process of an ASA with an FTD Boot Image

```
Boot buffer bigbuf=348bd018
Boot image size = 100921600 (0x603f100) bytes
[image size]      100921600
[MD5 signaure]    0264697f6f1942b9bf80f820fb209ad5
LFBFF signature verified.
INIT: version 2.88 booting
Starting udev
Configuring network interfaces... done.
Populating dev cache
Detected PID ASA5506.
Found device serial number JAD191100HG.
Found USB flash drive /dev/sdb
Found hard drive(s): /dev/sda
fsck from util-linux 2.23.2
dosfsck 2.11, 12 Mar 2005, FAT32, LFN
There are differences between boot sector and its backup.
Differences: (offset:original/backup)
  65:01/00
  Not automatically fixing this.
/dev/sdb1: 52 files, 811482/1918808 clusters
Launching boot CLI ...
Configuring network interface using static IP
```

```

Bringing up network interface.
Depending on your network, this might take a couple of minutes when using
DHCP...
ifup: interface lo already configured
Using IPv4 address: 10.1.1.21
INIT: Starting system message bus: dbus.
Starting OpenBSD Secure Shell server: sshd
    generating ssh RSA key...
    generating ssh ECDSA key...
    generating ssh DSA key...
done.
Starting Advanced Configuration and Power Interface daemon: acpid.
acpid: starting up
acpid: 1 rule loaded
acpid: waiting for events: event logging is off
Starting ntpd: done
Starting syslog-ng:[2016-09-19T19:43:24.781411] Connection failed; fd='15',
server='AF_INET(127.128.254.1:514)', local='AF_INET(0.0.0.0:0)',
error='Network is
unreachable (101)'
[2016-09-19T19:43:24.781508] Initiating connection failed, reconnecting;
time_reopen='60'
.
Starting crond: OK

        Cisco FTD Boot 6.0.0 (9.6.2.)
        Type ? for list of commands
ciscoasa-boot>

```

9. Optionally, you can press the ? key to see the list of the available commands on the FTD Boot CLI.

[Example 2-15](#) displays a list of commands available on the FTD Boot CLI. In the next section of this chapter, the highlighted commands are used to install an FTD Software System Image.

Example 2-15 *Limited Command Options on the FTD Boot CLI*

```

ciscoasa-boot> ?
  show                => Display system information. Enter show ? for
options
  system              => Control system operation
  setup               => System Setup Wizard
  support             => Support information for TAC
  delete              => Delete files
  ping                => Ping a host to check reachability
  traceroute          => Trace the route to a remote host
  exit                => Exit the session
  help                => Get help on command syntax
ciscoasa-boot>

```

Install System Software

Installation of the FTD software is the last step of the reimage process. This section describes the steps to install the FTD system software on any ASA 5500-X series hardware.

1. Download the FTD System Software package file from the cisco.com, and copy it to an HTTP or FTP server.

Note

This book use an HTTP server in lieu of an FTP server. You can use either of them. Some users may find the setup of an HTTP server is easier than the setup of an FTP server

[Figure 2-9](#) shows the FTD System Software package **ftd-6.1.0-330.pkg** that you install on any low-end or mid-range ASA 5500-X Series hardware during a reimage process.

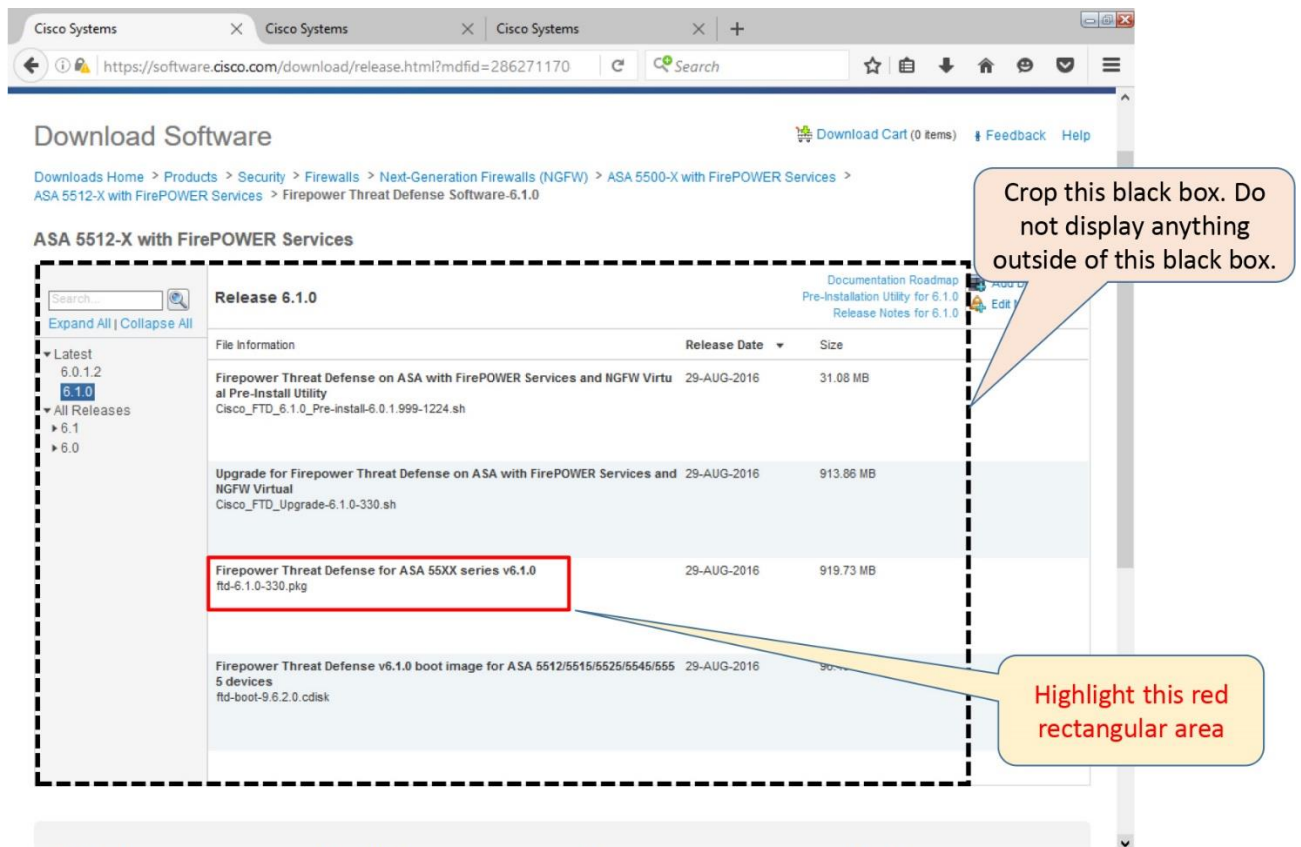


Figure 2-9. The *.pkg File is Applicable on Any Low-End and Mid-Range ASA Hardware Models

2. Run the **setup** command to configure or update the network settings, so that the ASA can download the FTD System Software package from the HTTP server. During the installation of boot image, you configured the network settings. This time, you either verify the existing configuration, or provide any missing information that was not entered before.

Tips

When a default value (mentioned in a bracket []) is acceptable, press ENTER to keep the settings unchanged.

[Example 2-16](#) shows the Cisco FTD Setup process. Upon confirmation, the networks restarts with the final configurations.

Example 2-16 A Complete Walk Through of the Network Setup Process

```

ciscoasa-boot> setup

                Welcome to Cisco FTD Setup
                [hit Ctrl-C to abort]
                Default values are inside []

Enter a hostname [ciscoasa]:
Do you want to configure IPv4 address on management interface?(y/n) [Y]:
Do you want to enable DHCP for IPv4 address assignment on management
interface?(y/n) [N]:
Enter an IPv4 address [10.1.1.21]:
Enter the netmask [255.255.255.0]:
Enter the gateway [10.1.1.1]:
Do you want to configure static IPv6 address on management interface?(y/n)
[N]:
Stateless autoconfiguration will be enabled for IPv6 addresses.
Enter the primary DNS server IP address: 10.1.1.8
Do you want to configure Secondary DNS Server? (y/n) [n]:
Do you want to configure Local Domain Name? (y/n) [n]:
Do you want to configure Search domains? (y/n) [n]:
Do you want to enable the NTP service? [Y]:
Enter the NTP servers separated by commas: 10.1.1.9

Please review the final configuration:
Hostname:                ciscoasa
Management Interface Configuration

IPv4 Configuration:      static
    IP Address:          10.1.1.21
    Netmask:             255.255.255.0
    Gateway:             10.1.1.1

IPv6 Configuration:      Stateless autoconfiguration

DNS Configuration:
    DNS Server:          10.1.1.8

NTP configuration:       10.1.1.9

CAUTION:
You have selected IPv6 stateless autoconfiguration, which assigns a global
address
based on network prefix and a device identifier. Although this address is
unlikely
to change, if it does change, the system will stop functioning correctly.
We suggest you use static addressing instead.
Apply the changes?(y,n) [Y]:
Configuration saved successfully!
Applying...
Restarting network services...
Done.
Press ENTER to continue...
ciscoasa-boot>

```

2. Test the connectivity.

[Example 2-17](#) shows the ASA is pinging successfully from the FTD Boot CLI to the HTTP server.

Example 2-17 Ping Test Between the ASA and the HTTP Server


```

ciscoasa-boot> ping 10.1.1.4
PING 10.1.1.4 (10.1.1.4) 56(84) bytes of data.
64 bytes from 10.1.1.4: icmp_seq=1 ttl=64 time=0.364 ms
64 bytes from 10.1.1.4: icmp_seq=2 ttl=64 time=0.352 ms
64 bytes from 10.1.1.4: icmp_seq=3 ttl=64 time=0.326 ms
64 bytes from 10.1.1.4: icmp_seq=4 ttl=64 time=0.313 ms
^C
--- 10.1.1.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.313/0.338/0.364/0.030 ms

ciscoasa-boot>

```

3. Download the FTD System Software package from the HTTP server.

[Example 2-18](#) illustrates the command to download file from an HTTP server to an ASA, using the FTD Boot CLI.

Example 2-18 *Download of the FTD System Software*

```

ciscoasa-boot> system install http://10.1.1.4/ftd-6.1.0-330.pkg

##### WARNING #####
# The content of disk0: will be erased during installation! #
#####

Do you want to continue? [y/N] Y
Erasing disk0 ...
Verifying
Downloading...

```

4. After a successful download, the file is extracted automatically. Upon your confirmation, the upgrade process starts.

Warning

The time to extract an FTD Software System package can take approximately 10 minutes. Similarly, the system takes additional 6 minutes to populate the system image. An ASA does not show any progress status during extracting or populating a file. Please be patient, and do not interrupt the process or reboot the ASA. Doing so might make your ASA unstable.

[Example 2-19](#) shows the extraction of the FTD System Software package **ftd-6.1.0-330.pkg**, and the beginning of the upgrade process.

Example 2-19 *Upgrade Process Starts*

```

Extracting.....
Package Detail
  Description:                Cisco ASA-FTD 6.1.0-330 System
Install
  Requires reboot:            Yes

Do you want to continue with upgrade? [y]:
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

```

Starting upgrade process ...
Populating new system image..

5. After the image is populated, the system prompts you to reboot the system. Press ENTER to reboot.

[Example 2-20](#) shows the ASA reboots after the image is populated.

Example 2-20 *A Required Reboot of an ASA to Complete an Upgrade*

Reboot is required to complete the upgrade. Press 'Enter' to reboot the system.

```
Broadcast mStopping OpenBSD Secure Shell server: sshdstopped /usr/sbin/sshd  
(pid 1723)
```

```
.  
Stopping Advanced Configuration and Power Interface daemon: stopped  
/usr/sbin/acpid (pid 1727)  
acpid: exiting
```

```
acpid.  
Stopping system message bus: dbus.  
Stopping ntpd: stopped process in pidfile '/var/run/ntp.pid' (pid 1893)  
done  
Stopping crond: OKs  
Deconfiguring network interfaces... done.  
Sending all processes the TERM signal...  
Sending all processes the KILL signal...  
Deactivating swap...  
Unmounting local filesystems...  
Rebooting...
```

Rom image verified correctly

```
Cisco Systems ROMMON, Version 1.1.8, RELEASE SOFTWARE  
Copyright (c) 1994-2015 by Cisco Systems, Inc.  
Compiled Thu 06/18/2015 12:15:56.43 by builders
```

```
Current image running: Boot ROM1  
Last reset cause: PowerCycleRequest  
DIMM Slot 0 : Present
```

```
Platform ASA5506 with 4096 Mbytes of main memory  
MAC Address: a4:6c:2a:e4:6b:bf  
Using default Management Ethernet Port: 0
```

```
Use BREAK or ESC to interrupt boot.  
Use SPACE to begin boot immediately.  
Boot in 5 seconds.
```

```
Located '.boot_string' @ cluster 260097.  
#  
Attempt autoboot: "boot disk0:os.img"  
Located 'os.img' @ cluster 235457.
```

```
#####  
#####
```

```
#####
#####
#####
#####
#####
#####
LFBFF signature verified.
INIT: version 2.88 booting
Starting udev
Configuring network interfaces... done.
Populating dev cache
Detected PID ASA5506.
Found device serial number JAD191100HG.
Found USB flash drive /dev/sdb
Found hard drive(s): /dev/sda
fsck from util-linux 2.23.2
dosfsck 2.11, 12 Mar 2005, FAT32, LFN
/dev/sdb1: 7 files, 24683/1919063 clusters
```

6. After the boot up, the initialization of the FTD software begins automatically.

Warning

Depending on the ASA hardware model, this may take about an hour to complete. At certain point, you may think the process is hung, but it is not. The system does not display any progress status in percentage. Do not interrupt the process or reboot the ASA. Doing so might make your ASA unstable. Once the FTD is completely installed, a login prompt appears.

[Example 2-21](#) shows the launch of FTD software and the execution of various scripts throughout the installation process.

Example 2-21 *The FTD Initialization Process*

```
Use ESC to interrupt boot and launch boot CLI.
Use SPACE to launch Cisco FTD immediately.
Cisco FTD launch in 21 seconds ...

Cisco FTD launch in 0 seconds ...
Running on kenton
Mounting disk partitions ...
Initializing Threat Defense ...             [ OK
]
Starting system log daemon...               [ OK
]
Stopping mysql...
Sep 19 20:29:33 ciscoasa SF-IMS[2303]: [2303] pmtool:pmtool [ERROR] Unable
to connect to UNIX socket at /ngfw/var/sf/run/PM_Control.sock: No such file
or directory
Starting mysql...
Sep 19 20:29:33 ciscoasa SF-IMS[2304]: [2304] pmtool:pmtool [ERROR] Unable
to connect to UNIX socket at /ngfw/var/sf/run/PM_Control.sock: No such file
or directory
Flushing all current IPv4 rules and user defined chains: ...success
Clearing all current IPv4 rules and user defined chains: ...success
Applying iptables firewall rules:
Flushing chain `PREROUTING'
.
! Omitted the messages related to iptables flushing for brevity
```

```

.
Flushing chain `OUTPUT'
Applying rules succeeded
Starting nscd...
mkdir: created directory '/var/run/nscd' [ OK
]
Starting , please wait...grep: /ngfw/etc/motd: No such file or directory
...complete.
Firstboot detected, executing scripts
Executing S01reset_failopen_if [ OK
]
Executing S01virtual-machine-reconfigure [ OK
]
Executing S02aws-pull-cfg [ OK
]
Executing S02configure_onbox [ OK
]
Executing S04fix-httpd.sh [ OK
]
Executing S05set-mgmnt-port [ OK
]
Executing S06addusers [ OK
]
Executing S07uuid-init [ OK
]
Executing S08configure_mysql [ OK
]
]

***** Attention *****

    Initializing the configuration database. Depending on available
    system resources (CPU, memory, and disk), this may take 30 minutes
    or more to complete.

***** Attention *****

Executing S09database-init [ OK
]
Executing S11database-populate [ OK
]
Executing S12install_infodb [ OK
]
Executing S15set-locale.sh [ OK
]
Executing S16update-sensor.pl [ OK
]
Executing S19cert-tun-init [ OK
]
Executing S20cert-init [ OK
]
Executing S21disable_estreamer [ OK
]
Executing S25create_default_des.pl [ OK
]
Executing S30init_lights_out_mgmt.pl [ OK
]
Executing S40install_default_filters.pl [ OK
]
Executing S42install_default_dashboards.pl [ OK
]
]

```

```
Executing S43install_default_report_templates.pl [ OK
]
Executing S44install_default_app_filters.pl [ OK
]
Executing S45install_default_realms.pl [ OK
]
Executing S47install_default_sandbox_EO.pl [ OK
]
Executing S50install-remediation-modules [ OK
]
Executing S51install_health_policy.pl [ OK
]
Executing S52install_system_policy.pl [ OK
]
Executing S53change_reconciliation_baseline.pl [ OK
]
Executing S70remove_casuser.pl [ OK
]
Executing S70update_sensor_objects.sh [ OK
]
Executing S85patch_history-init [ OK
]
Executing S90banner-init [ OK
]
Executing S95copy-crontab [ OK
]
Executing S96grow_var.sh [ OK
]
Executing S96install_vmware_tools.pl [ OK
]
```

***** Attention *****

Initializing the system's localization settings. Depending on available system resources (CPU, memory, and disk), this may take 10 minutes or more to complete.

***** Attention *****

```
Executing S96localize-templates [ OK
]
Executing S96ovf-data.pl [ OK
]
Executing S97compress-client-resources [ OK
]
Executing S97create_platinum_forms.pl [ OK
]
Executing S97install_cas [ OK
]
Executing S97install_cloud_support.pl [ OK
]
Executing S97install_geolocation.pl [ OK
]
Executing S97install_ssl_inspection.pl [ OK
]
Executing S97update_modprobe.pl [ OK
]
Executing S98check-db-integrity.sh [ OK
]
Executing S98htaccess-init [ OK
]
```

```

Executing S98is-sru-finished.sh [ OK
]
Executing S99correct_ipmi.pl [ OK
]
Executing S99start-system [ OK
]
Executing S99z_db_restore [ OK
]
Executing S99_z_cc-integrity.sh [ OK
]
Firstboot scripts finished.
Configuring NTP... [ OK
]
fatattr: can't open '/mnt/disk0/.private2': No such file or directory
fatattr: can't open '/mnt/disk0/.ngfw': No such file or directory
Model reconfigure detected, executing scripts
Pinging mysql
Found mysql is running
Executing 45update-sensor.pl [ OK
]
Executing 55recalculate_arc.pl [ OK
]
Starting xinetd:
Mon Sep 19 20:59:07 UTC 2016
Starting MySQL...
Pinging mysql
Pinging mysql, try 1
Pinging mysql, try 2
Found mysql is running
Running initializeObjects...
Stopping MySQL...
Killing mysqld with pid 22285
Wait for mysqld to exit\c
done
Mon Sep 19 20:59:32 UTC 2016

Starting sfifd... [ OK
]
Starting Cisco ASA5506-X Threat Defense, please wait...No PM running!
...started.
INIT: Starting system message bus: dbus.
Starting OpenBSD Secure Shell server: sshd
generating ssh RSA key...
generating ssh ECDSA key...
generating ssh DSA key...
done.
Starting Advanced Configuration and Power Interface daemon: acpid.
Starting crond: OK
Sep 19 20:59:42 ciscoasa SF-IMS[22997]: [22997] init script:system [INFO]
pmmon Setting affinity to 0-3...
pid 22993's current affinity list: 0-3
pid 22993's new affinity list: 0-3
Sep 19 20:59:42 ciscoasa SF-IMS[22999]: [22999] init script:system [INFO]
pmmon The Process Manager is not running...
Sep 19 20:59:42 ciscoasa SF-IMS[23000]: [23000] init script:system [INFO]
pmmon Starting the Process Manager...
Sep 19 20:59:42 ciscoasa SF-IMS[23001]: [23001] pm:pm [INFO] Using model
number 75J

IO Memory Nodes: 1
IO Memory Per Node: 205520896 bytes

```

Global Reserve Memory Per Node: 314572800 bytes Nodes=1

LCMB: got 205520896 bytes on numa-id=0, phys=0x2400000, virt=0x2aaaac200000
LCMB: HEAP-CACHE POOL got 314572800 bytes on numa-id=0, virt=0x7fa17d600000
Processor memory: 1583098718

Compiled on Tue 23-Aug-16 19:42 PDT by builders

Total NICs found: 14

.
! Omitted the MAC addresses, licensing and legal messages for brevity
.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Reading from flash...

!
Cryptochecksum (changed): f410387e 8aab8a4e f71eb8a9 f8b37ef9

INFO: Power-On Self-Test in process.

.....
INFO: Power-On Self-Test complete.

INFO: Starting HW-DRBG health test...

INFO: HW-DRBG health test passed.

INFO: Starting SW-DRBG health test...

INFO: SW-DRBG health test passed.

Type help o '?' for a list

Cisco ASA5506-X Threat Defense v6.1.0 (build 330)

firepower login:

7. Firepower login prompt appears. It means the installation is complete. Enter the default login credential.

[Example 2-22](#) shows the Firepower login prompt. Enter the username 'admin' and password 'Admin123'.

Example 2-22 *The Default Login Credential*

```
firepower login: admin  
Password: Admin123
```

8. Right after you enter the default login credential, an End User License Agreement (EULA) appears. Use the ENTER key to display the agreement and to accept it.

Tip

To exit from the EULA any time, press 'q'.

[Example 2-23](#) shows the system prompts for the EULA. The detail legal messages are omitted in the output for brevity.

Example 2-23 *Agree to the EULA*

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
END USER LICENSE AGREEMENT
.
.
!The EULA messages are omitted for brevity
.
.
.Please enter 'YES' or press <ENTER> to AGREE to the EULA:
```

9. System initialization process begins. After the changing the password for the admin user, you need to setup the network. You can press ENTER where you accept the default value in bracket [].

[Example 2-24](#) illustrates the configuration of password and network settings.

Example 2-24 *Configuration of the Network After the First Login to FTD*

```
System initialization in progress. Please stand by.
You must change the password for 'admin' to continue.
Enter new password:
Confirm new password:
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]:
10.1.1.21
Enter an IPv4 netmask for the management interface [255.255.255.0]:
Enter the IPv4 default gateway for the management interface [192.168.45.1]:
10.1.1.1
Enter a fully qualified hostname for this system [firepower]:
Enter a comma-separated list of DNS servers or 'none' []:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
```

10. When the question for local management appears, enter **no**. The FTD local management functionality is also known as on-box management.

Note

The option for FTD local management enables a built-in Firepower Device Manager (FDM) application, which can manage only one single FTD System – only itself. This book uses the standalone version of a manager, known as Firepower Management Center (FMC). An FMC

can manage multiple FTD Systems that might be deployed in different geographical locations.

[Example 2-25](#) exhibits the configurations that determine how you want to manage this FTD, and how you want to deploy it in your network. In this example, the system is configured to be managed by a dedicated management appliance (Firepower Management Center), and is deployed in routed mode.

Example 2-25 Responses That Determine the Deployment Type and Modes

```
Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...
Update policy deployment information
  - add device configuration
  - add network discovery
  - add system policy
```

You can register the sensor to a Firepower Management Center and use the Firepower Management Center to manage it. Note that registering the sensor to a Firepower Management Center disables on-sensor Firepower Services management capabilities.

```
When registering the sensor to a Firepower Management Center, a unique alphanumeric registration key is always required. In most cases, to register a sensor to a Firepower Management Center, you must provide the hostname or the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'
```

```
However, if the sensor and the Firepower Management Center are separated by a NAT device, you must enter a unique NAT ID, along with the unique registration key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'
```

```
Later, using the web interface on the Firepower Management Center, you must use the same registration key and, if necessary, the same NAT ID when you add this sensor to the Firepower Management Center.
>
```

The '>' prompt, at the end of [Example 2-25](#), confirms that the initial network configuration is complete.

The next step is to verify the network connectivity on the management interface and begin the registration process. Please read the [Chapter 6: Management Interface and Device Registration](#) to learn about the registration process.

Verification and Troubleshooting Tools

This section describes the commands that you can use to verify the status of an ASA hardware before and after the FTD software is installed.

Navigation to the FTD CLI

After a reboot, followed by a successful installation of FTD software, your ASA hardware should automatically display the '>' prompt, which is different than the default prompt 'ciscoasa>' on a traditional ASA software. Furthermore, when an ASA hardware runs the FTD software, you can enter various consoles or shells. For example,

- **FTD Default Shell:** You can configure most of the necessary items and view their status using this shell.
- **ASA Console:** It allows you to perform advanced commands — used for diagnostic purposes.
- **Firepower Linux Shell:** It lets you enter the backend of the operating system — used by Cisco for advanced troubleshooting.

[Figure 2-10](#) shows different types of consoles and command prompts of an ASA running the FTD software.

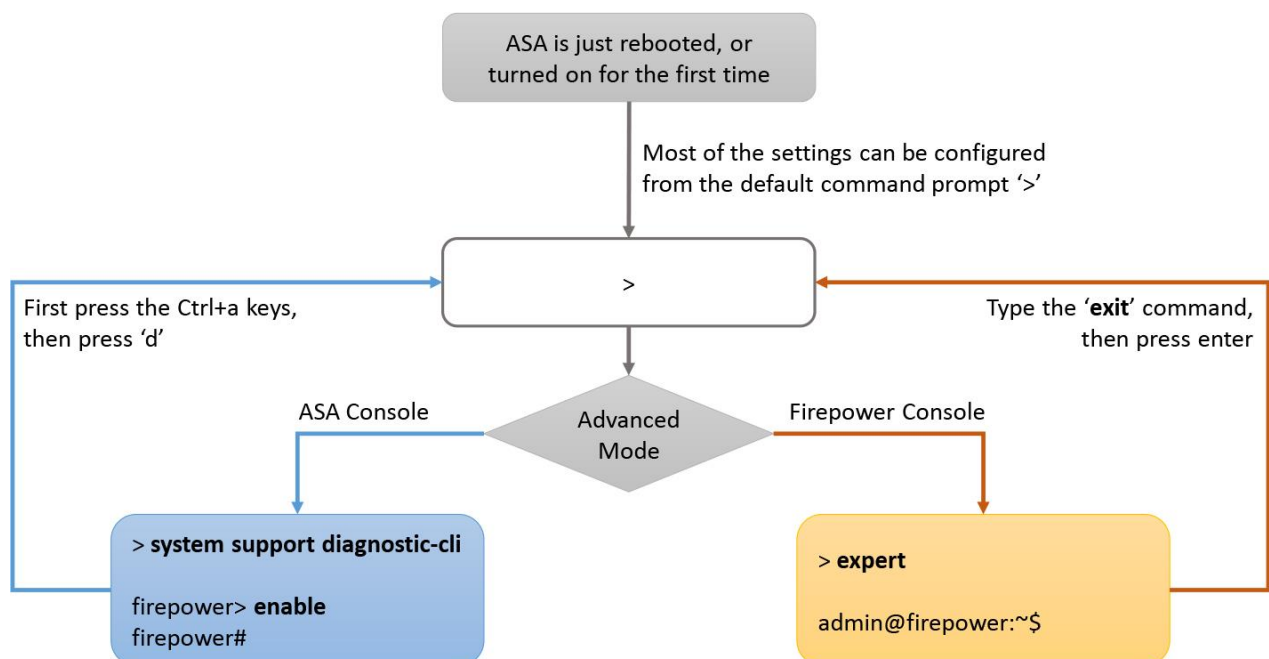


Figure 2-10. *Different Types of Command Prompts of an ASA Running FTD Software*

[Example 2-26](#) shows the commands that allow you to navigate various modes of an FTD CLI.

Example 2-26 *Commands to Connect to the Various Shells of the FTD CLI*

```
>
```

```
! The '>' prompt confirms that you are on the FTD default shell. Run the following command to connect to the ASA console:
```

```
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
firepower>
```

```
! Now you have entered the ASA console. Run the 'enable' command to enter
the
privilege exec mode.
```

```
firepower> enable
Password:
firepower# exit
```

```
Logoff
Type help or '?' for a list of available commands.
```

```
firepower>
```

```
! If you want to quit from the ASA console, the 'exit' command logs you off
from the ASA
console, but does not let you return to the FTD default shell. To
disconnect from the
ASA console, press the "Ctrl+a" keys together, then press 'd' separately.
```

```
firepower>
```

```
Console connection detached.
>
```

```
! To connect to the Firepower Linux shell, run the 'expert' command. To
return to the
FTD default shell, run the 'exit' command.
```

```
> expert
admin@firepower:~$ exit
logout
>
```

Determine the Version of Installed Software

From the default command prompt '>' on an FTD, you will be able to determine the FTD software version running on an ASA hardware.

[Example 2-27](#) shows an ASA5506-X hardware is running the Firepower Threat Defense Version 6.1.0.

Example 2-27 *The Software Version Running on an ASA after a Fresh FTD Installation*

```
> show version
```

```
-----[ firepower ]-----
Model                : Cisco ASA5506-X Threat Defense (75) Version
6.1.0 (Build 330)
UUID                 : c84ceb32-7ea7-11e6-a7ad-94bcd8f36790
Rules update version : 2016-03-28-001-vrt
VDB version          : 270
-----
```

```
>
```

Tip

The Model field on the “show version” command output must show “Cisco ASA55XX-X Threat Defense Version 6.1.0”. If the Model shows “ASA55XX Version 6.1.0” — without the “Threat Defense” keyword — it means the ASA is running the Firepower software 6.1 as a separate service, not in a unified image.

Determine the Free Disk Space of an ASA

Before you install FTD on your ASA hardware, you must check if the currently available space is sufficient. you can run one of the following commands on your ASA software in the privileged exec mode:

```
ciscoasa# dir
ciscoasa# show flash:
```

[Example 2-28](#) shows the amount of free space on the same ASA hardware from two different command outputs. The shaded portion of the example shows the ASA has free space of 4544851968 bytes which is equal to 4438332KB or 4334.3MB or 4.23GB. The first command output uses disk0: to indicate an internal flash memory. If there were an external flash memory, it would be denoted by disk1:.

Example 2-28 *Command to Know the Amount of the Free Space on an ASA*

```
ciscoasa# dir

Directory of disk0:/

88      -rwx  91290240      11:04:08 May 12 2016  asa961-50-lfbff-k8.spa
89      -rwx    63         16:25:14 Sep 19 2016  .boot_string
11      drwx   4096         12:14:22 May 12 2016  log
19      drwx   4096         12:15:12 May 12 2016  crypto_archive
20      drwx   4096         12:15:16 May 12 2016  coredumpinfo

7859437568 bytes total (4544851968 bytes free)

ciscoasa#

ciscoasa# show flash:

--#--  --length--  -----date/time-----  path
  88  91290240    May 12 2016 11:04:08  asa961-50-lfbff-k8.spa
  89    63       Sep 19 2016 16:25:14  .boot_string
  11  4096       May 12 2016 12:14:22  log
  13    0       May 12 2016 12:14:22  log/asa-appagent.log
  19  4096       May 12 2016 12:15:12  crypto_archive
  20  4096       May 12 2016 12:15:16  coredumpinfo
  21   59       May 12 2016 12:15:16  coredumpinfo/coredump.cfg

7859437568 bytes total (4544851968 bytes free)

ciscoasa#
```

```
ciscoasa# show flash:
```

```
--#--  --length--  -----date/time-----  path
  88  91290240    May 12 2016 11:04:08    asa961-50-lfbff-k8.spa
  89   63        Sep 19 2016 16:25:14    .boot_string
  11  4096        May 12 2016 12:14:22    log
  13   0        May 12 2016 12:14:22    log/asa-appagent.log
  19  4096        May 12 2016 12:15:12    crypto_archive
  20  4096        May 12 2016 12:15:16    coredumpinfo
  21   59        May 12 2016 12:15:16    coredumpinfo/coredump.cfg
```

```
7859437568 bytes total (4544851968 bytes free)
```

```
ciscoasa#
```

[Delete a File from the Storage Device](#)

When you want to delete a file to free up disk space, run the following on command on the privileged exec mode:

```
ciscoasa# delete flash:/filename
```

[Example 2-29](#) shows the command to delete a file named output.txt.

Example 2-29 *Command to Delete a File on an ASA*

```
ciscoasa# delete flash:/output.txt
```

[Determine the Availability of any Storage Device or SSD](#)

From the CLI, you can determine the type of a storage device that is installed on an ASA

[Example 2-30](#) shows the ASA 5506-X hardware has one Solid State Drive installed.

Example 2-30 *Command to View the Storage Device Information on a Low-End ASA 5500-X Series Hardware*

```
ciscoasa# show inventory
```

```
Name: "Chassis", DESCR: "ASA 5506-X with FirePOWER services, 8GE, AC, DES"
PID: ASA5506          , VID: V01          , SN: JMX1916Z07V
```

```
Name: "Storage Device 1", DESCR: "ASA 5506-X SSD"
PID: ASA5506-SSD     , VID: N/A          , SN: MSA190600NE
```

```
ciscoasa#
```

[Example 2-31](#) shows an ASA 5545-X hardware with two storage devices.

Example 2-31 *Determine the List of Storage Devices on a Mid-Range ASA 5500-X Series Hardware*

```
ciscoasa# show inventory
```

```
Name: "Chassis", DESCR: "ASA 5545-X with SW, 8 GE Data, 1 GE Mgmt"
PID: ASA5545          , VID: V02          , SN: FTX1841119Z
```

```
Name: "power supply 0", DESCR: "ASA 5545-X/5555-X AC Power Supply"
PID: ASA-PWR-AC       , VID: N/A          , SN: 47K1E0
```

```
Name: "Storage Device 1", DESCR: "Model Number: Micron_M550_MTFDDAK128MAY"
PID: N/A , VID: N/A , SN: MXA183502EG
```

```
Name: "Storage Device 2", DESCR: "Model Number: Micron_M550_MTFDDAK128MAY"
PID: N/A , VID: N/A , SN: MXA183502FW
```

```
ciscoasa#
```

[Table 2-2](#) summarizes the availability of the Solid State Drive (SSD) in various ASA 5500-X Series hardware, by default. It also shows if an SSD is hot-swappable on a particular model, in case of a failure.

ASA 5500-X Series Models	Availability of SSD	Hot-Swappable
5506-X, 5506W-X, 5506H-X	Comes with an SSD	No
5508-X, 5516-X	Comes with an SSD	Yes, requires a screwdriver.
5512-X, 5515-X, 5525-X	May not come with an SSD, if not ordered separately. You can install one Cisco SSD.	Yes, easy to hot-swap. A button is available to push and release the locking lever.
5545-X, 5555-X	May not come with an SSD, if not ordered separately. You can install up to two Cisco SSDs with RAID-1.	

Table 2-2. Availability and Replacement of SSD on ASA 5500-X Series Hardware

Determine the Version of the Rommon Software or Firmware

The version information of a Rommon software (also known as Firmware) is displayed during the boot up process of an ASA 5500-X hardware.

[Example 2-32](#) shows the initial messages that appear after an ASA 5506-X hardware is turned on. It shows the Rommon version is 1.1.01.

Example 2-32 Messages That Appear During the Boot Up Process

```
Cisco Systems ROMMON, Version 1.1.01, RELEASE SOFTWARE
Copyright (c) 1994-2014 by Cisco Systems, Inc.
Compiled Mon 10/20/2014 15:59:12.05 by builder
```

```
Current image running: Boot ROM0
Last reset cause: PowerCycleRequest
DIMM Slot 0 : Present
```

```
Platform ASA5506 with 4096 Mbytes of main memory
MAC Address: a4:6c:2a:e4:6b:bf
Using default Management Ethernet Port: 0
```

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

```
Located '.boot_string' @ cluster 1607965.
#
Attempt autoboot: "boot disk0:/asa961-50-lfbff-k8.spa"
Located 'asa961-50-lfbff-k8.spa' @ cluster 10.
```

```
#####
#####
```

```
#####
#####
#####
#####
#####
```

```
LFBBFF signature verified.
INIT: version 2.88 booting
Starting udev
Configuring network interfaces... done.
```

If your ASA is currently running in a production environment, and you do not want to reboot this at this moment, you can still determine the version of the Rommon software. Run the following command to find this information on a running system:

[Example 2-33](#) shows the Rommon version of the ASA 5506-X hardware is 1.1.01.

Example 2-33 *Command that Displays the Rommon Software Version of an ASA*

```
ciscoasa# show module

Mod  Card Type                               Model                               Serial
No.
-----
-----
1 ASA 5506-X with FirePOWER services, 8GE, AC, ASA5506
JAD191100HG
  sfr Unknown                               N/A
JAD191100HG

Mod  MAC Address Range                       Hw Version   Fw Version   Sw Version
-----
-----
1 a46c.2ae4.6bbf to a46c.2ae4.6bc8  1.0          1.1.1        9.6(1)50
  sfr a46c.2ae4.6bbe to a46c.2ae4.6bbe N/A          N/A

Mod  SSM Application Name                     Status           SSM Application
Version
-----
-----

Mod  Status           Data Plane Status   Compatibility
-----
-----
1 Up Sys           Not Applicable
  sfr Init         Not Applicable

ciscoasa#
```

Summary

This chapter describes the differences between various images that may be installed on an ASA 5500-X hardware. It demonstrates the detail process to reimage an ASA 5500-X Series hardware to the Firepower Threat Defense software. In addition, this chapter provides you the command line tools that you can use to verify the status of the hardware and software.

After installation, the next step to deploy an FTD in a network is to register it with a Firepower Management Center. The Part II of the book describes that.

Review Questions

1. What would be the correct workflow to reimage an ASA 5506-X hardware to FTD?

- i. Upgrade the rommon software
- ii. Reload an ASA with a boot image
- iii. Install the FTD system software
- iv. Copy the image files into a server

a. ii > i > iii > iv

b. iv > ii > iii

c. ii > iii

d. iv > i > ii > iii

2. What would be the correct workflow to reimage an ASA 5545-X hardware to FTD?

- i. Upgrade the rommon software
- ii. Reload an ASA with a boot image
- iii. Install the FTD system software
- iv. Copy the image files into a server

a. ii > i > iii > iv

b. iv > ii > iii

c. iii > ii

d. iv > i > ii > iii

3. A file with the following extension is not necessary to reimage an ASA 5516-X hardware to FTD?

a. *.spa

b. *.lfbff

c. *.cdisk

d. *.pkg

4. What kind of server should you use to transfer a boot image file to an ASA?

- a. TFTP Server
- b. FTP Server
- c. Web Server
- d. Secure Copy Server

5. Which protocol is used in this book to transfer the System Software image to an ASA?

- a. HTTP
- b. TFTP
- c. FTP
- d. SCP

6. Which command would you run to confirm if an SSD is installed on an ASA?

- a. **show flash**
- b. **show inventory**
- c. **show run**
- d. **show module**

7. Which command displays the firmware version of an ASA?

- a. **show firmware**
- b. **show rommon**
- c. **show module**
- d. **show inventory**

8. Which one is the default command prompt in the Firepower Threat Defense software?

- a. **ciscoasa#**
- b. **ciscoasa-boot>**
- c. **firepower>**
- d. **>**

Chapter 3. Firepower Threat Defense (FTD) on the Firepower eXtensible Operating System (FXOS)

Within the ASA 5500-X Series models, the ASA 5585-X hardware is designed for a data center network. However, an ASA 5585-X device does not support the Firepower Threat Defense (FTD) software. To meet the need of a service provider network, Cisco introduces a new career-class Firepower hardware platform that runs the Firepower Threat Defense (FTD) on top of a supervisor. The supervisor runs on an independent operating system called the Firepower eXtensible Operating System (FXOS). This chapter discusses the deployment of the FTD software on the FXOS.

Essential Knowledge

Cisco introduced the Firepower 9300 Series and the Firepower 4100 Series hardware models in 2015 and 2016, respectively. In 2017, the Firepower 2100 Series hardware models are added in the Firepower hardware family. In comparison with the traditional ASA 5500-X hardware, the new Firepower hardware platforms are designed to deliver better performance. While the architecture of every Firepower hardware series is unique, every model in this family runs FTD on the FXOS software.

Note

Since this book uses the software Version 6.1 as the baseline, the configuration examples in this chapter focus on the Firepower 9300 and 4100 Series models as they support Version 6.1. The Firepower 2100 Series hardware supports FTD software Version 6.2.1 or greater. However, the troubleshooting methodologies and configuration best practices you find in this book are useful to any Firepower deployment, regardless of the Firepower hardware model or FTD software version you use.

[Table 3-1](#) shows the hardware specifications of the Firepower 4100 series and the Firepower 9300 series platforms.

	4100	9300
CPU	Single 12-Core (4110) Dual 12-Core (4120) Dual 18-Core (4140) Dual 22-Core (4150)	Dual 12-Core (Module 24) Dual 18-Core (Module 36) Dual 22-Core (Module 44)
Memory	64 GB (4110) 128 GB (4120) 256 GB (4140, 4150)	256 GB of memory per security module
Storage	200 GB (4110, 4120) 400 GB (4140, 4150) (The SSD slot 2 is used to install an optional Malware Storage Pack)	Two 800 GB of SSDs per security module
Security Module	1 (Embedded)	3 (Online insertion and removal are supported)
Form Factor	1 Rack Unit	3 Rack Unit

Table 3-1. Specification of the Firepower 4100 and 9300 Hardware

[Figure 3-1](#) shows various modules on a Cisco Firepower 9300 Series chassis.

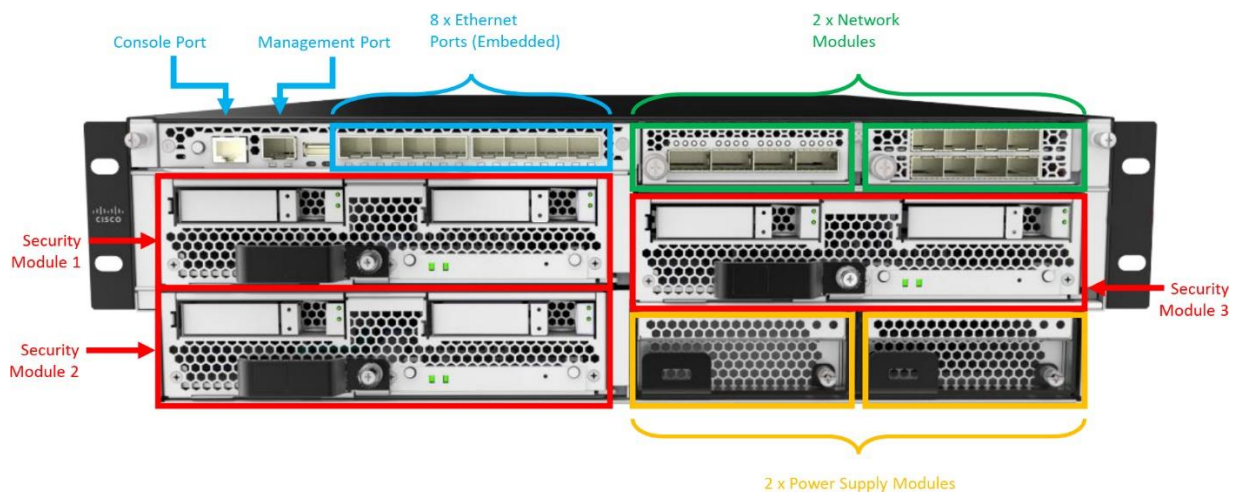


Figure 3-1. Front Panel of a Cisco Firepower 9300 Series Chassis

[Figure 3-2](#) exhibits the console, management and other network ports on a Cisco Firepower 4100 Series chassis.

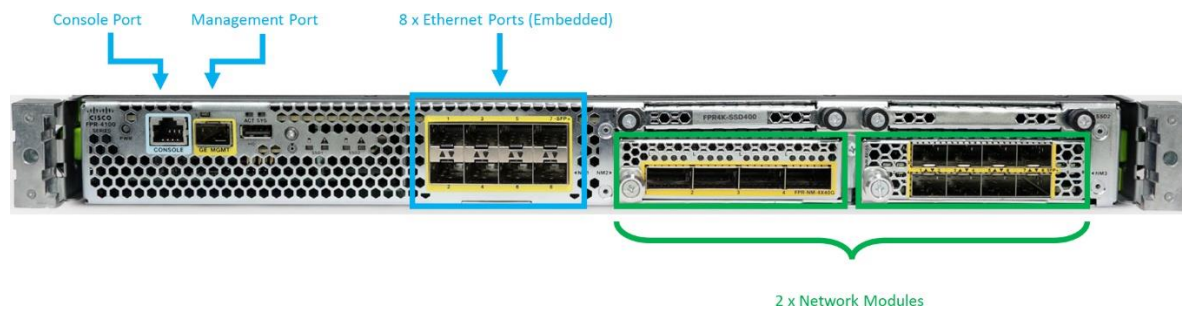


Figure 3-2. Front Panel of a Cisco Firepower 4100 Series Chassis

Architecture

The Cisco Firepower 9300 Series and 4100 Series chassis use modular hardware components. You can leverage the modular architecture to upgrade, troubleshoot, or replace any particular modules without replacing an entire Firepower chassis.

A Firepower security appliance comprised of various modules. For example, network module, security module, power supply module, fan module, etc. All of these modules interact with two major components — supervisor and security module.

- **Supervisor:** A supervisor uses the Firepower eXtensible Operating System (FXOS) to manage the configuration of network modules, security modules, and chassis. It also monitors all of the hardware components, such as, power supplies, fans, etc.

- **Security Module:** A security module runs the actual security application, such as, the Firepower Threat Defense (FTD) software. The adapters on a security module receive traffic

from the external network modules through a switch fabric, and send them to the FTD for any necessary actions.

Note

For ease of understanding, you may compare a Security Module with a blade server. The Firepower Chassis Manager of a 9300 Series and a 4100 Series platform use two different terms to refer to this blade server, which are “Security Module” and “Security Engine”, respectively.

[Figure 3-3](#) displays the architecture of a Firepower 9300 Series appliance, and demonstrates the connections between the supervisor and a security module. In a Firepower 4100 Series hardware, the number of security engine would be one.

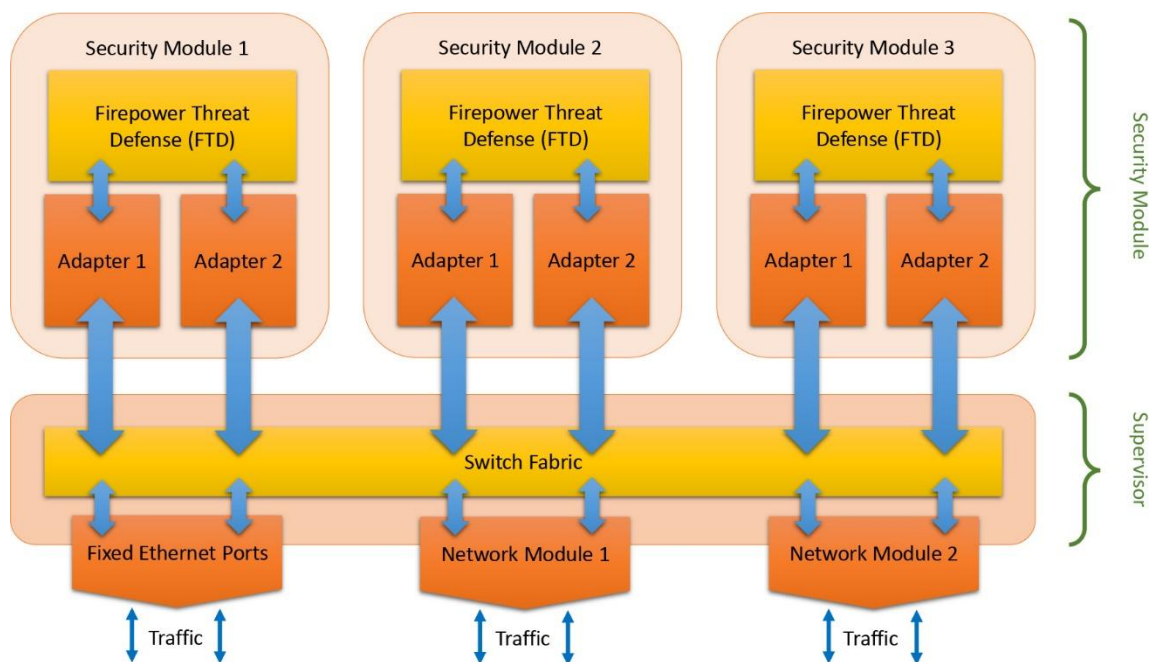


Figure 3-3. Architecture of a Cisco Firepower 9300 Security Appliance

Note

The Firepower 2100 Series hardware introduces an additional processor, called Network Processor Unit (NPU). The NPU is designed to process any traffic that is not intended for an advanced inspection. The other x86 CPU processes traffic that matches an advanced Next-Generation security policy.

Software Images

At the cisco support site, you will find various software for a Firepower security appliance. For a core FTD deployment on a Firepower appliance, you only need two types of software:

- Firepower Extensible Operating System
- Firepower Threat Defense Software

[Figure 3-4](#) highlights the software images that are necessary to install FTD on FXOS. The screenshot displays the software that you can download from the cisco support site for a Firepower 9300 series appliance. A 4100 series appliance supports all of them except the third-party software Radware Virtual Defense Pro (as of writing this book).

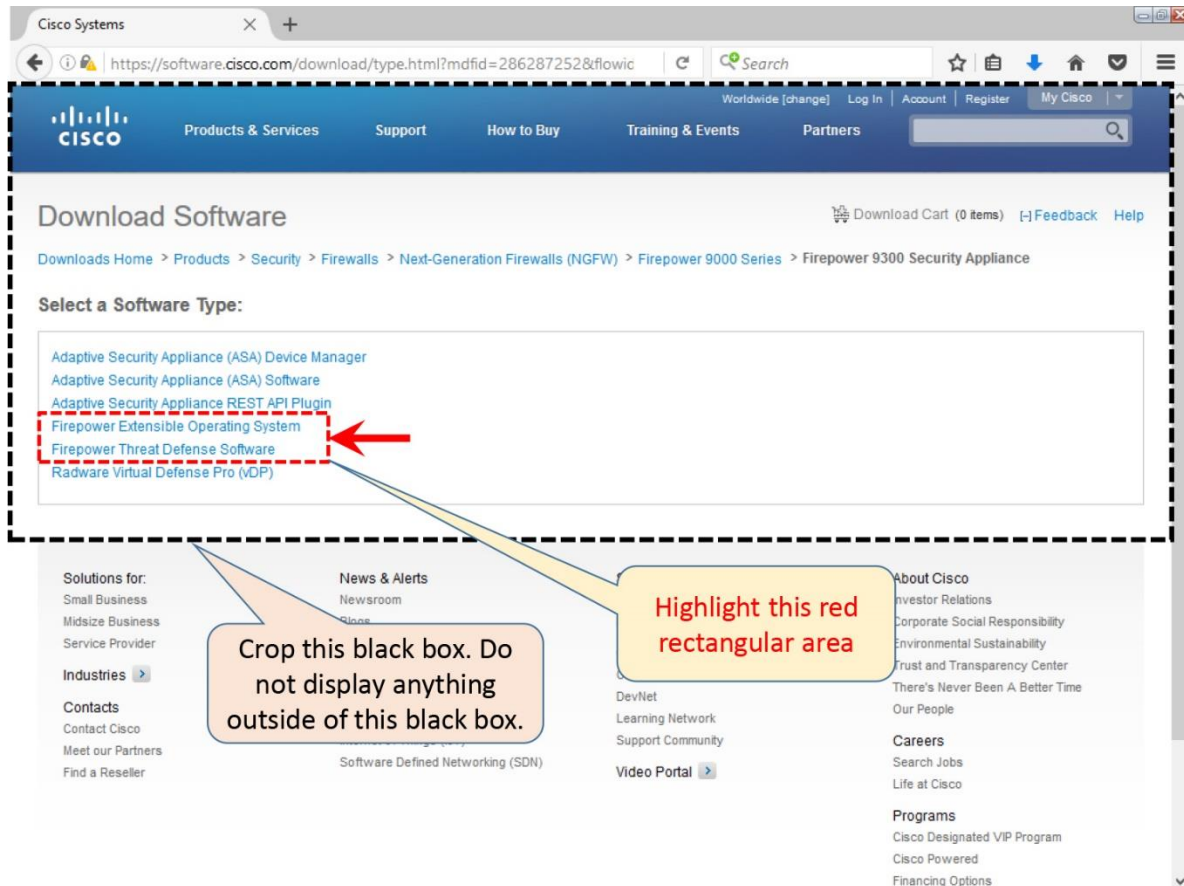


Figure 3-4. *Types of Software for a Firepower Security Appliance*

- **Firepower Extensible Operating System (FXOS):** The FXOS software, also known as *Platform Bundle*, contains software for the supervisor and the hardware components on a Firepower security appliance. The bundle includes any essential components of the FXOS except any security applications.

[Figure 3-5](#) shows the **fxos-k9.2.0.1.86.SPA** file — a platform bundle for a Firepower security appliance. It installs the FXOS Release 2.0.1.

The screenshot shows the Cisco Systems website for downloading software. The page is titled "Firepower 9300 Security Appliance" and "Release 2.0.1". A table lists several software files. A red dashed box highlights the file "FX-OS image for Firepower fxos-k9.2.0.1.86.SPA". A black dashed box encompasses the entire table area. Two callout boxes provide instructions: "Crop this black box. Do not display anything outside of this black box." and "Highlight this red rectangular area".

File Information	Release Date	Size
FX-OS image for Firepower fxos-k9.2.0.1.37.SPA	23-JUN-2016	715.15 MB
FX-OS image for Firepower fxos-k9.2.0.1.68.SPA	16-AUG-2016	715.17 MB
FX-OS image for Firepower fxos-k9.2.0.1.86.SPA	27-OCT-2016	715.23 MB
MIBS zip for Firepower FX-OS image firepower-mibs.2.0.1.37.zip	23-JUN-2016	0.73 MB
MIBS zip for Firepower FX-OS image firepower-mibs.2.0.1.68.zip	16-AUG-2016	0.73 MB
MIBS zip for Firepower FX-OS image firepower-mibs.2.0.1.86.zip	27-OCT-2016	0.73 MB

Figure 3-5. *The Platform Bundle for a Firepower Security Appliance*

• **Firepower Threat Defense (FTD) Software:** The FTD software, also called the *Application Package*, is one of the security applications that you can install on a security module of a Firepower appliance. Once the FTD software is installed and registered with a Firepower Management Center (FMC), you can manage the security policies of an FTD through an FMC.

[Figure 3-6](#) shows the **cisco-ftd.6.1.0.330.SPA.csp** file — an application package for the FTD. When you upload a .csp file to a Firepower appliance, it is stored on the supervisor, but when you install a .csp file, it is deployed on a security module.

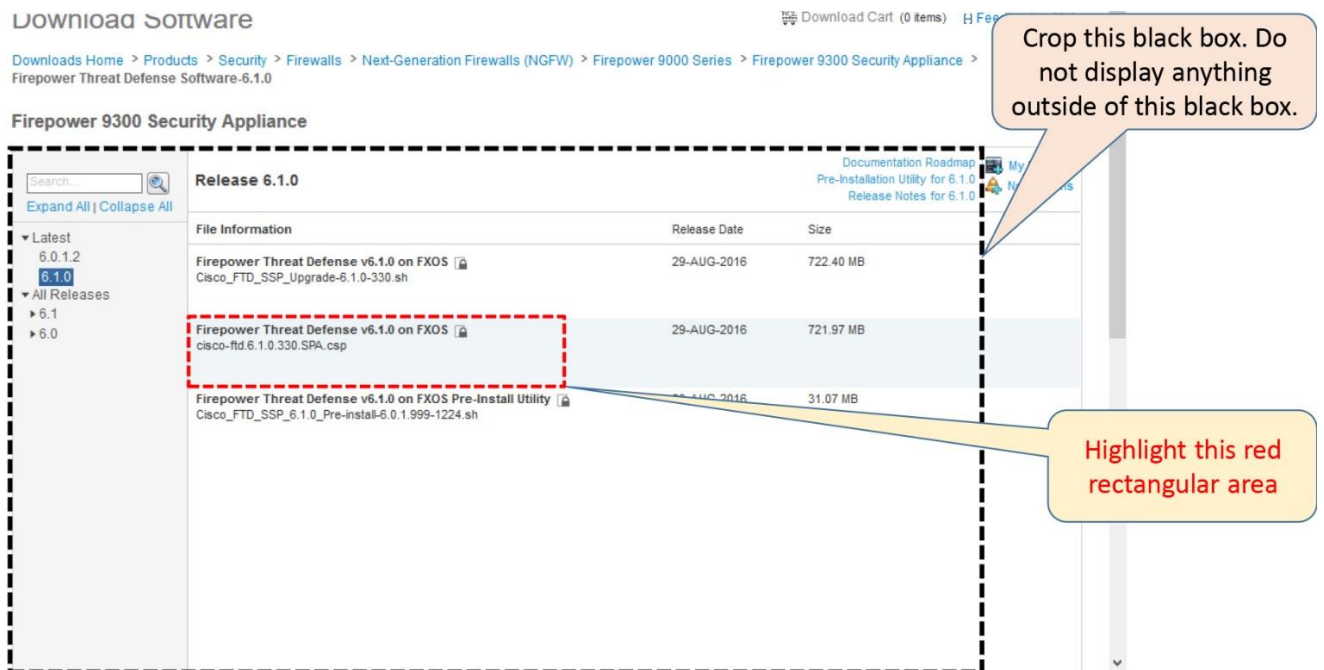


Figure 3-6. An Application Package for the FTD Software

Cisco also occasionally releases firmware image for Firepower appliance. Upgrading the firmware is not a mandatory requirement for the FTD software installation. It is rather necessary when you want to enable any enhanced or latest hardware features. For example, if your Firepower appliance is running Firepower version 1.0.09, you will need to upgrade it to version 1.0.10 or greater in order to enable the Firepower 2-port 100-G Network Module double-wide.

Read the official FXOS guides, published at cisco.com, to learn when and how to install firmware on a Firepower security appliance.

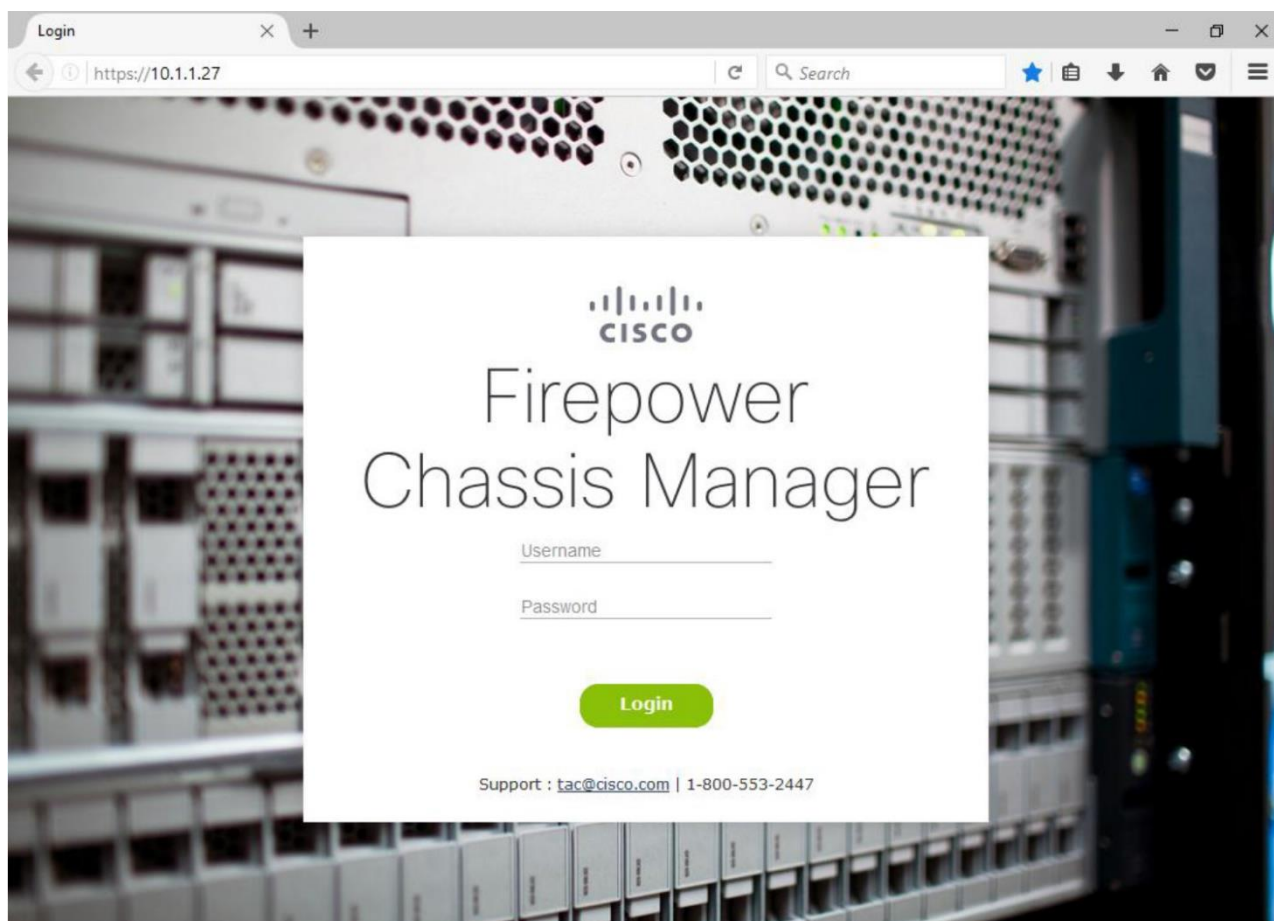
Web User Interfaces

Like a Firepower Management Center (FMC), a Firepower 9300 Series and 4100 Series security appliance has its own web interface, called *Firepower Chassis Manager*. To install, upgrade, or downgrade any security application on a Firepower appliance, login to the Firepower Chassis Manager is necessary. Alternatively, you can access the CLI of a Firepower appliance through Secure shell (SSH) or console connection.

To access the web interface, enter the management IP address of the Firepower security appliance in a supported browser, like below:

```
https://IP_Address_of_Management_Interface
```

[Figure 3-7](#) displays a login page that appears when you enter the Firepower Chassis Manager management IP address in a browser.



Copyright 2004-2015, Cisco and/or its affiliates. All rights reserved.

Figure 3-7. Login Page of the Firepower Chassis Manager

Note

If you are running a Firepower 2100 Series hardware with the software Version 6.2.1 or higher, you can choose one of the two web user interfaces to configure and manage your FTD. You can register it with a standalone Firepower Management Center (FMC) and manage it through the FMC. Alternatively, you can enable local management capability and manage the FTD directly via an on-box manager, called Firepower Device Manager (FDM).

Best Practices

Consider the following best practices when you install the FTD software on a Firepower security appliance running FXOS:

1. Perform the installation tasks during a maintenance window, so that any network interruption does not impact your business. You should also plan for an additional time to complete any post-installation setup.
2. Prior to your maintenance window, make sure you are able to access the cisco.com website, and entitled to download all of the necessary FXOS and FTD images. If you are unable to access, register for a Cisco account. If the self-registration process does not allow

you download a desired software, you may need to work with your Cisco Channel Partner or the Cisco Technical Assistance Center (TAC) for further assistance.

3. After you download any software from the Cisco.com, always verify the MD5 or SHA512 checksum of the files you have downloaded. It confirms that the file is not corrupt, or not modified during download.

Figure 3-8 illustrates how the MD5 and SHA512 checksum values are displayed at cisco.com when you hover your mouse over a filename.

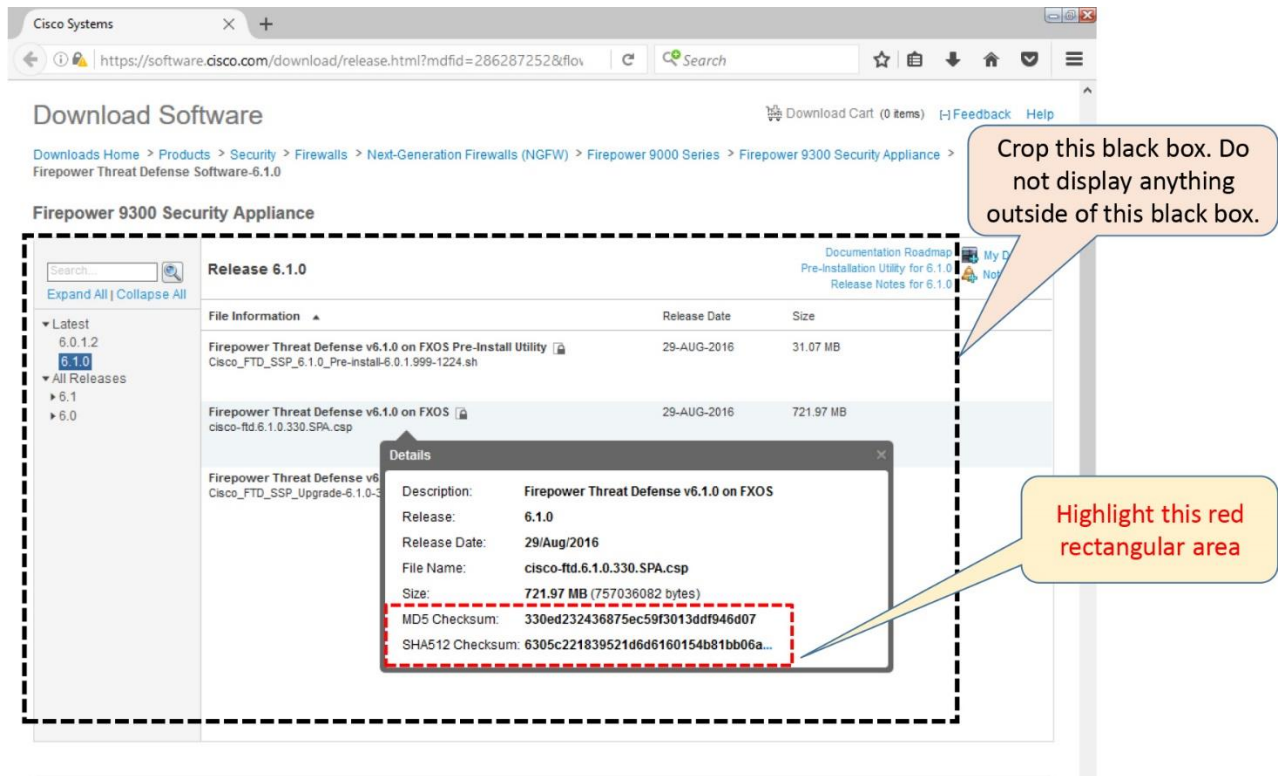


Figure 3-8. Checksum Values of an FTD Software

4. If your Firepower chassis is already running with a good configuration, take a backup of the existing configuration before you make any changes. Go to the **System > Configuration > Export** page on the Firepower Chassis Manager to export the configuration.

Warning

The export of a configuration is stored in an XML file format. Do not alter the contents of an XML file. It can fail an import attempt.

Figure 3-9 shows the options to export configurations of a Firepower security appliance.

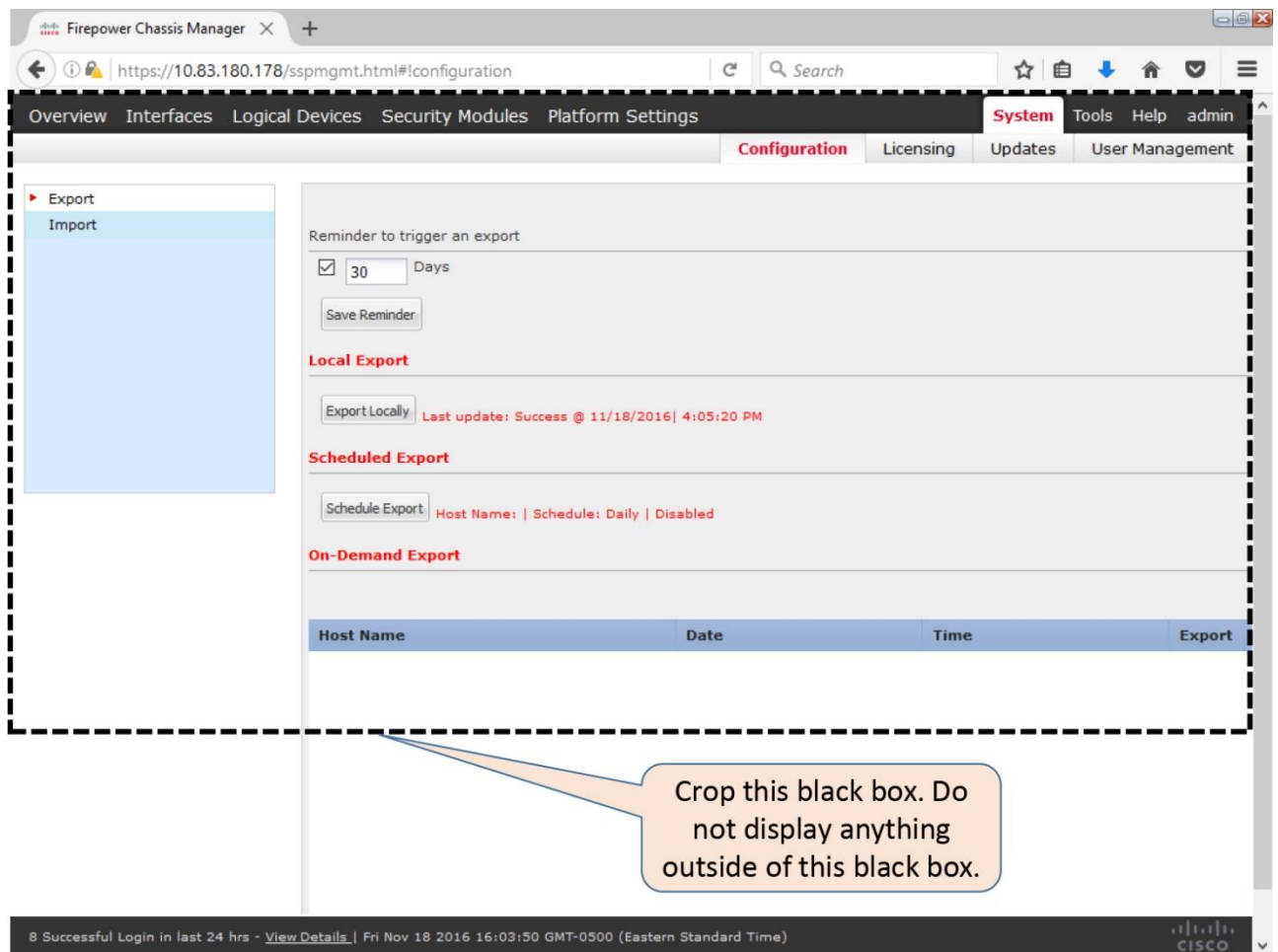


Figure 3-9. Configuration Export Page on a Firepower Chassis Manager

5. During an import, the software version of FXOS must match with the version when a configuration (XML file) was exported. Similarly, any detail of the hardware, such as, platform model, network module installed (including the slot number) must be the same during export and import.

Caution

A configuration export, using the Firepower Chassis Manager, includes the configuration settings of the FXOS. It does not include any configurations from the FTD software.

6. Do not power off, shutdown, reboot, or reinitialize a Firepower chassis or a security module when the FTD installation is in progress.

7. If you need to power down a Firepower chassis with an FTD software already installed, you must gracefully shutdown the FTD application beforehand. An ungraceful power down of a Firepower chassis can corrupt the data and file system of an FTD.

8. Some of the modules on a Firepower appliance support Online Insertion and Removal (OIR) feature. For example, the security module, power supply module, and fan module. However, to replace a network module that does not support OIR (as of writing this book), you must gracefully shutdown the FTD software and then power down the Firepower chassis.

9. Before you deploy FTD on a Firepower chassis, read the hardware installation guide to learn the latest information about any hardware features.

Configuration

In this section, you will learn the detail steps to install the Firepower Threat Defense system software on a Cisco Firepower 9300 Series hardware. The processes are identical for a Firepower 4100 Series hardware.

Prerequisites

Before you install the Firepower Threat Defense application, you must fulfill any prerequisites. For example, delete any existing logical devices from the FXOS, upgrade the FXOS software version, and enable necessary interfaces. This section elaborates these prerequisites.

Delete Any Existing Logical Devices

If your Firepower appliance is currently running any logical devices with different types of software, such as, any ASA software or earlier version of FTD software, you will need to delete them. The installation of multiple types software on a single Firepower appliance is not supported (as of writing this book). To delete a logical device, follow the steps below:

Step 1. Go to the **Logical Devices** tab on the Firepower Chassis Manager.

[Figure 3-10](#) shows the ASA security application is running as a logical device on a Firepower 9300 appliance. Note the recycle bin icon. It is used to delete a logical device.

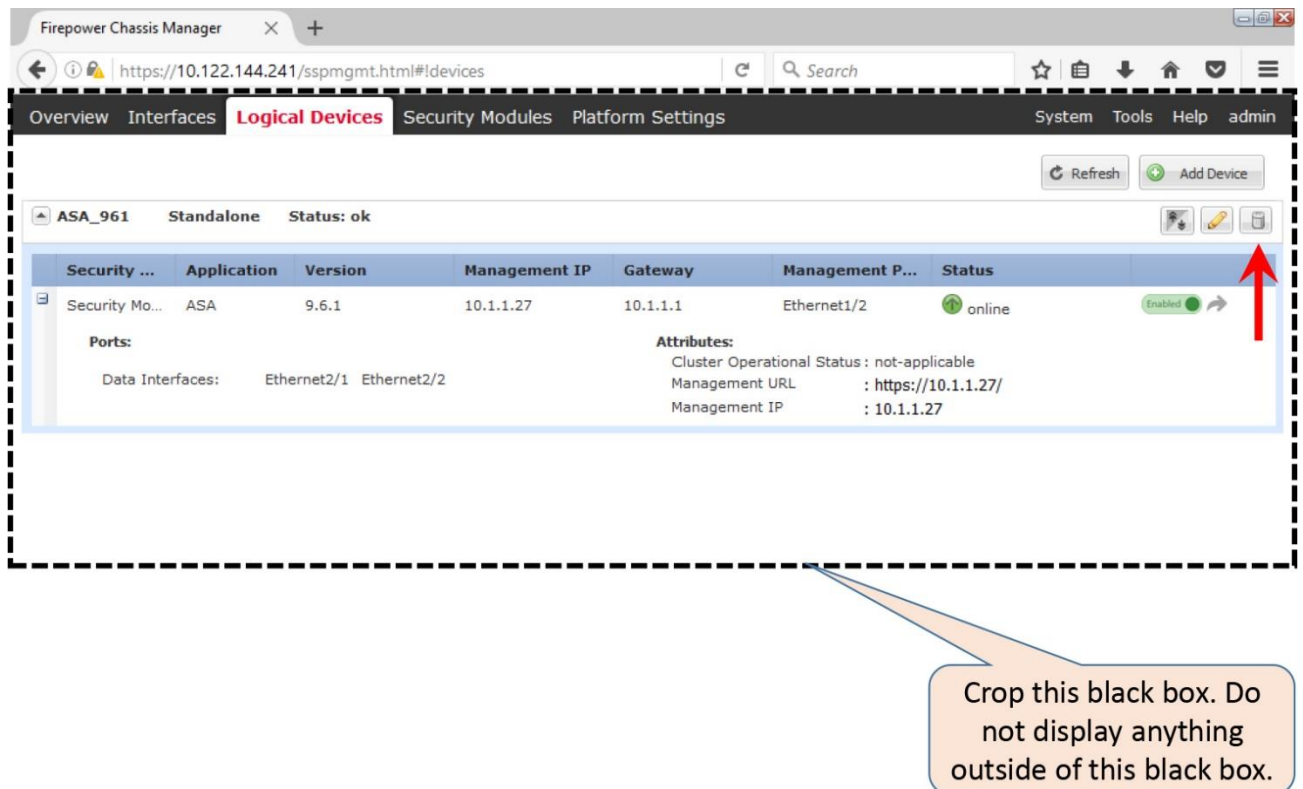


Figure 3-10. Logical Devices Page on a Firepower Appliance

Step 2. Click on the delete icon next to a logical device. A confirmation window appears. Select 'Yes' when the system asks you if you want to delete the logical device.

Step 3. Select **Yes** once again, when the system asks you if you want to delete its application configuration.

Figure 3-11 shows the second confirmation window. It asks for your confirmation to delete the application configuration.

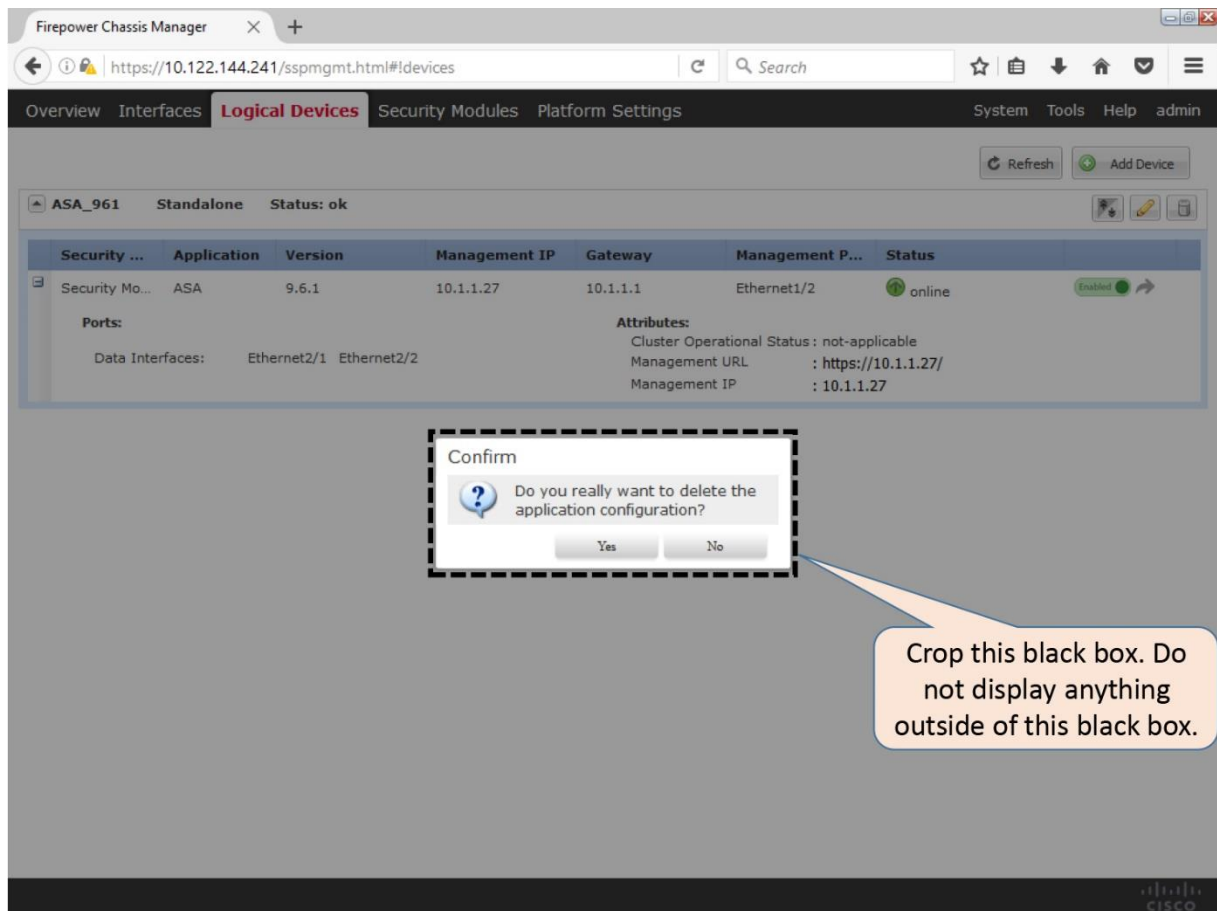
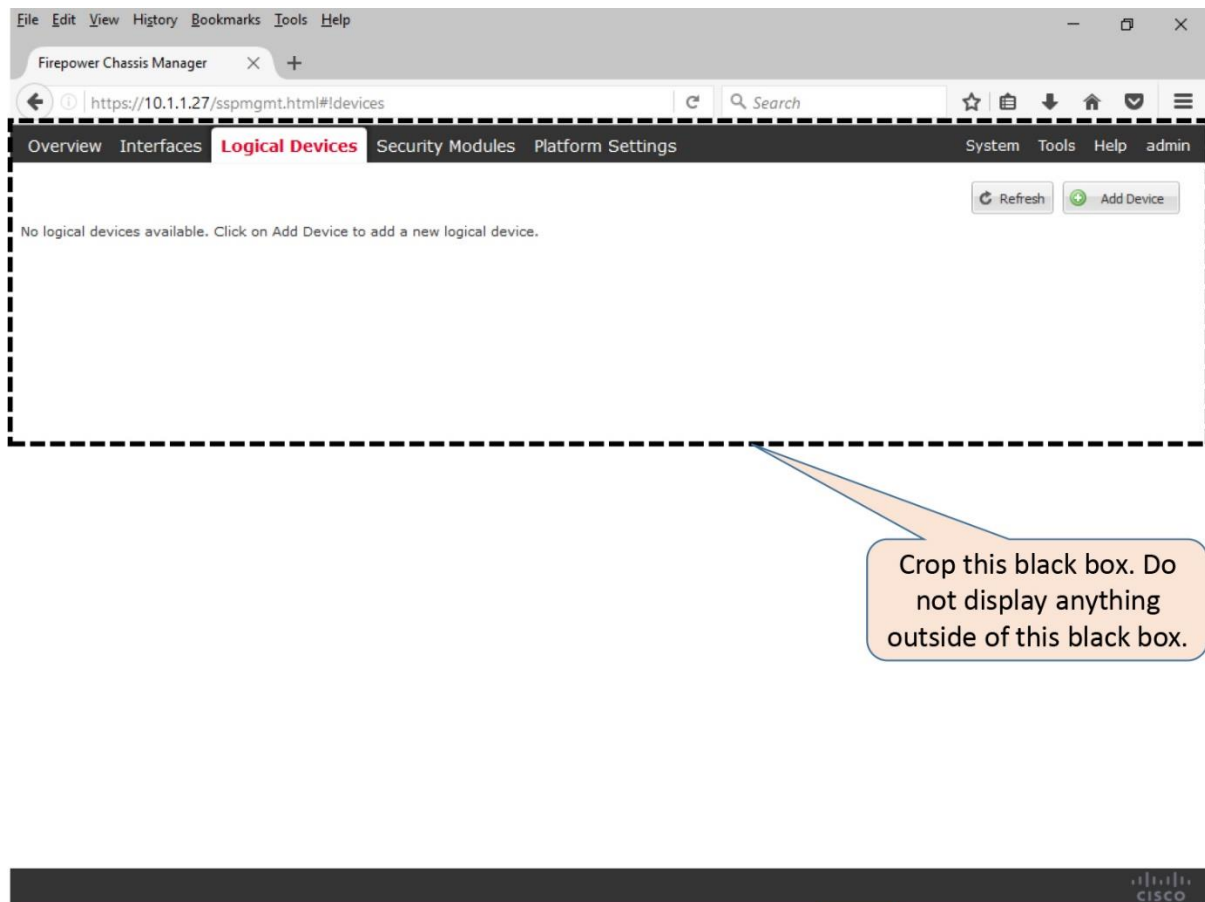


Figure 3-11. Confirmation Window During Deleting a Logical Device

When all of the logical devices are deleted, a Firepower Chassis Manager displays the message “No logical devices available. Click on Add Device to add a new logical device.”

[Figure 3-12](#) shows no logical devices on this Firepower appliance. You will see this message in a brand new system, or when you delete all of the existing logical devices.



Crop this black box. Do not display anything outside of this black box.

Figure 3-12. Confirmation of the Deletion of All of the Logical Devices

Upgrade the FXOS Software

To install the FTD software Version 6.1, a Firepower appliance must be running the FXOS Version 2.0.1 or greater. If your appliance runs any earlier release, follow the steps below to upgrade the FXOS software:

- Step 1.** Download an appropriate FXOS platform bundle from the Cisco support site.
- Step 2.** Login to the Firepower Chassis Manager, and go to the **System > Updates** page.
- Step 3.** Select the **Upload Image** button and then **Browse** the FXOS platform bundle image. Once an image is selected, click on the **Upload** button to begin the upload process.

[Figure 3-13](#) demonstrates a workflow for uploading a software image to the Firepower Chassis Manager. The Upload Image window appears on top of the **System > Updates** Page.

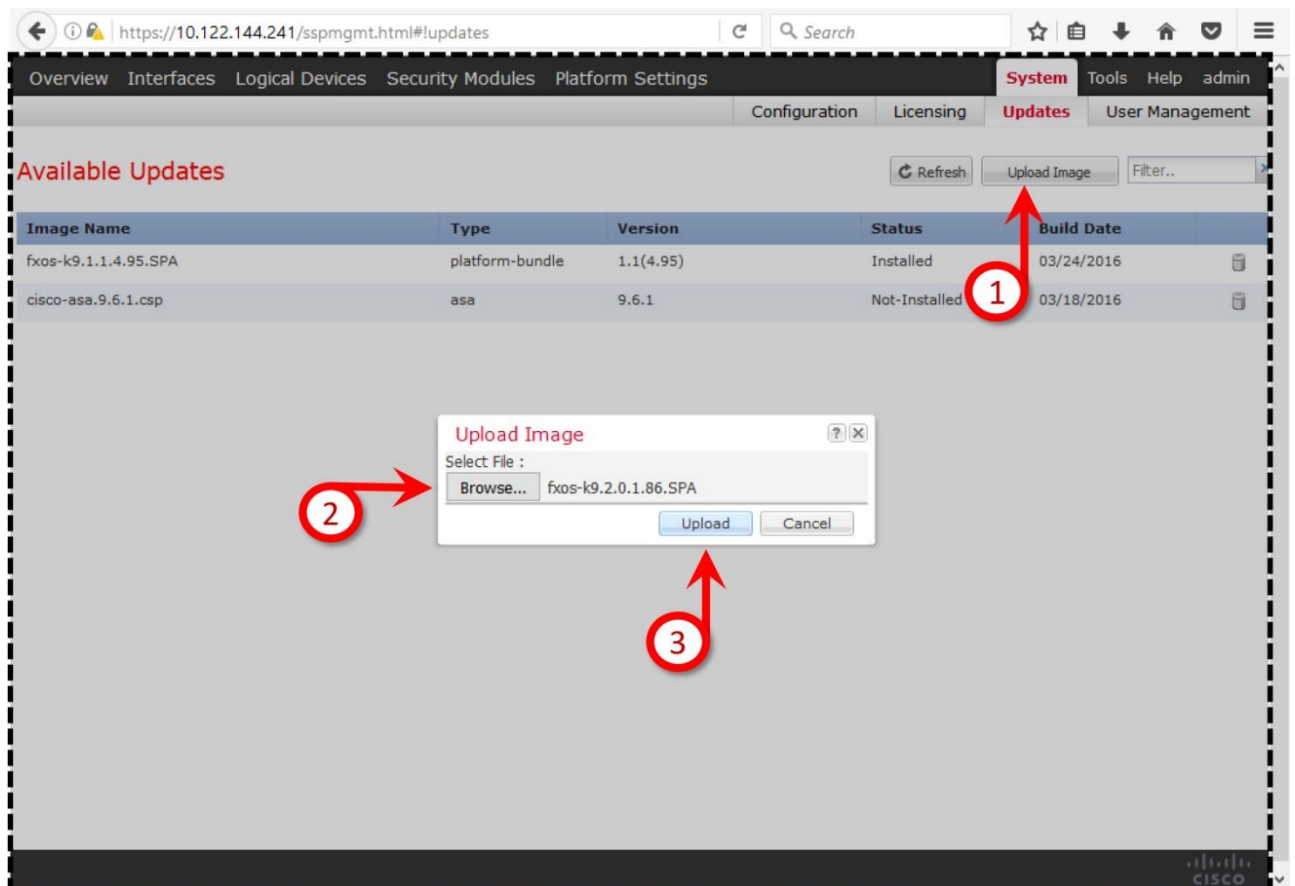


Figure 3-13. Workflow for Uploading an Image

Step 4. After a successful upload, a confirmation window appears. Press **OK** to close the window.

[Figure 3-14](#) shows a success message after an FXOS image is successfully uploaded into the Firepower Chassis Manager.

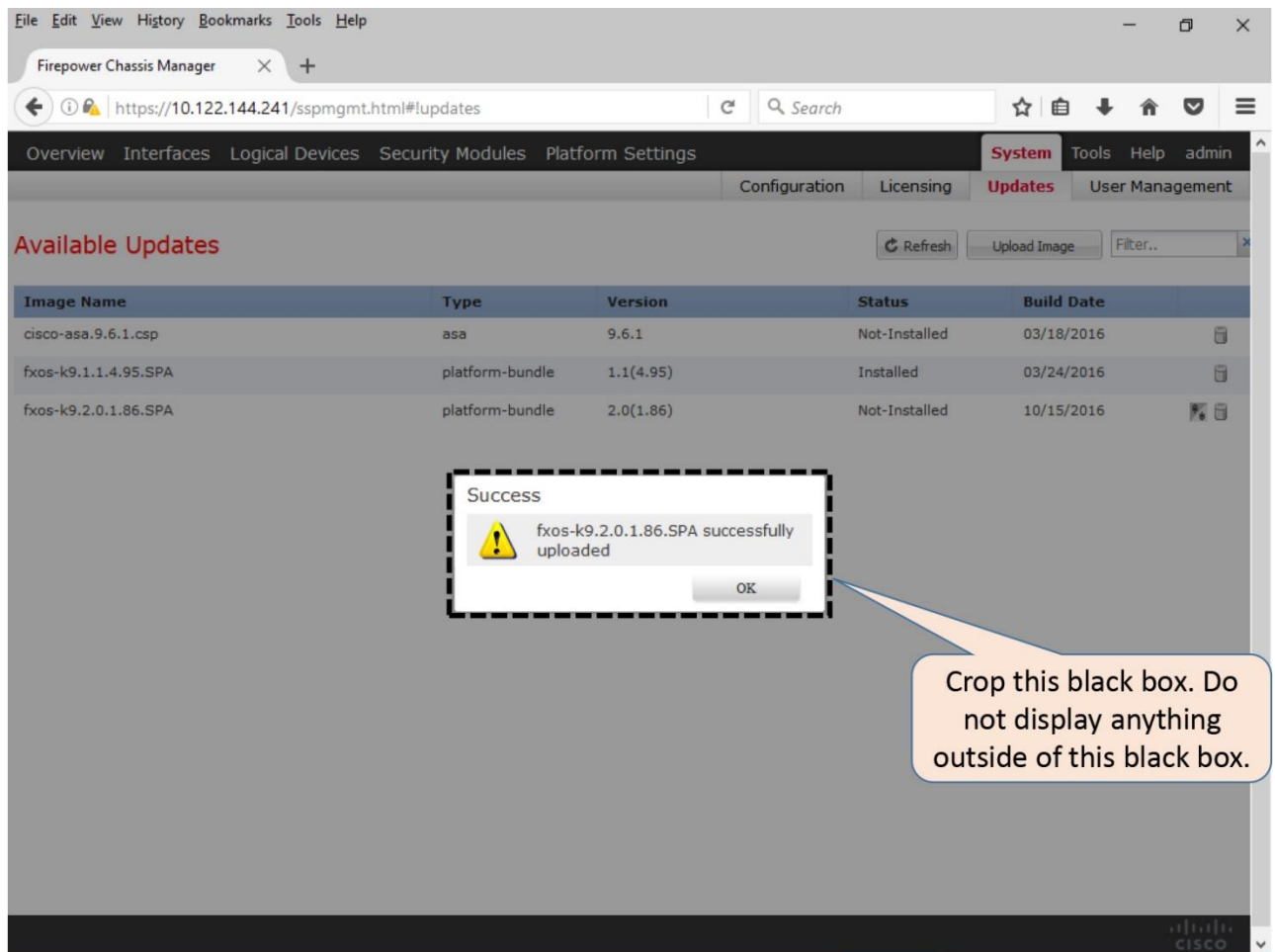


Figure 3-14. *Confirmation of a Successful Upload*

Step 5. At this point, in the **System > Updates** page, you should see an upgrade icon next to the image that you have just uploaded. Click on that icon to begin the upgrade.

Figure 3-15 displays an upgrade icon followed by a successful image upload.

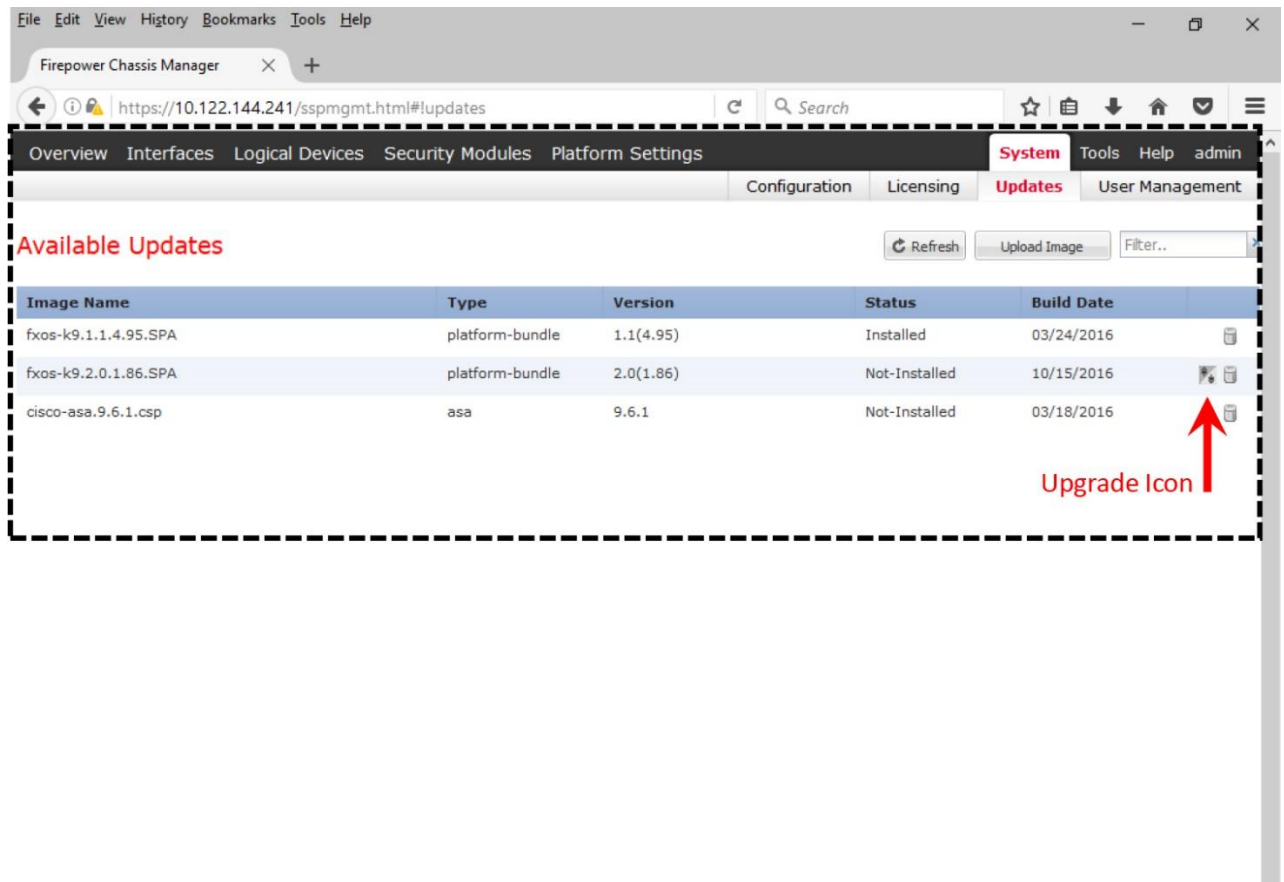


Figure 3-15. Icon for the FXOS Platform Bundle Upgrade

Step 6. Select **Yes** when a confirmation window appears, and asks if you want to proceed.

Figure 3-16 shows the final confirmation window before an upgrade begins.

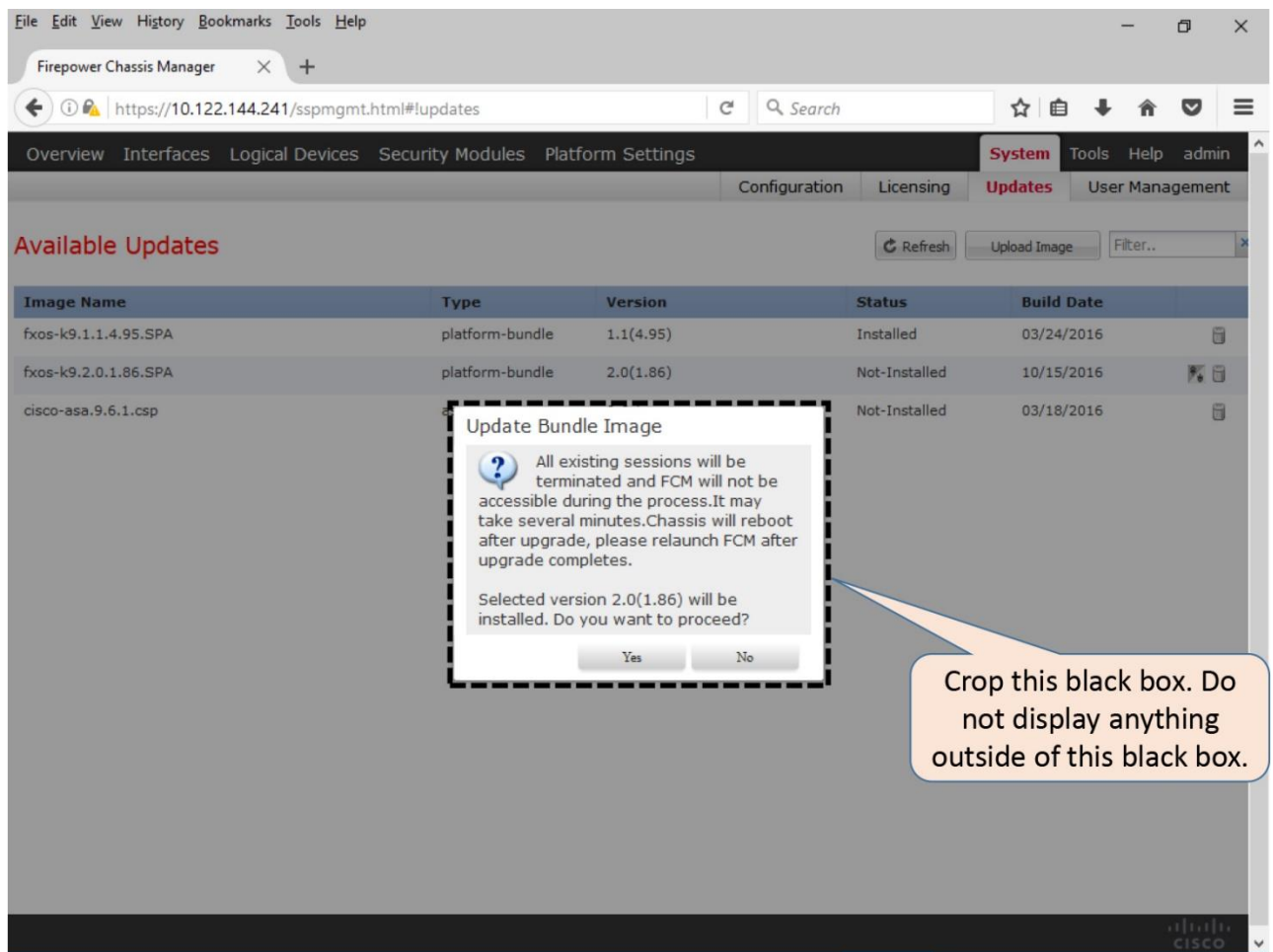


Figure 3-16. Update Bundle Image Confirmation Window

Step 7. After the upgrade begins, the web interface does not show any progress status, and the connection to the GUI is lost for some time. When it comes back, the status of the new software shows as *Installed*.

[Figure 3-17](#) shows the desired new software Version 2.0.1 is installed.

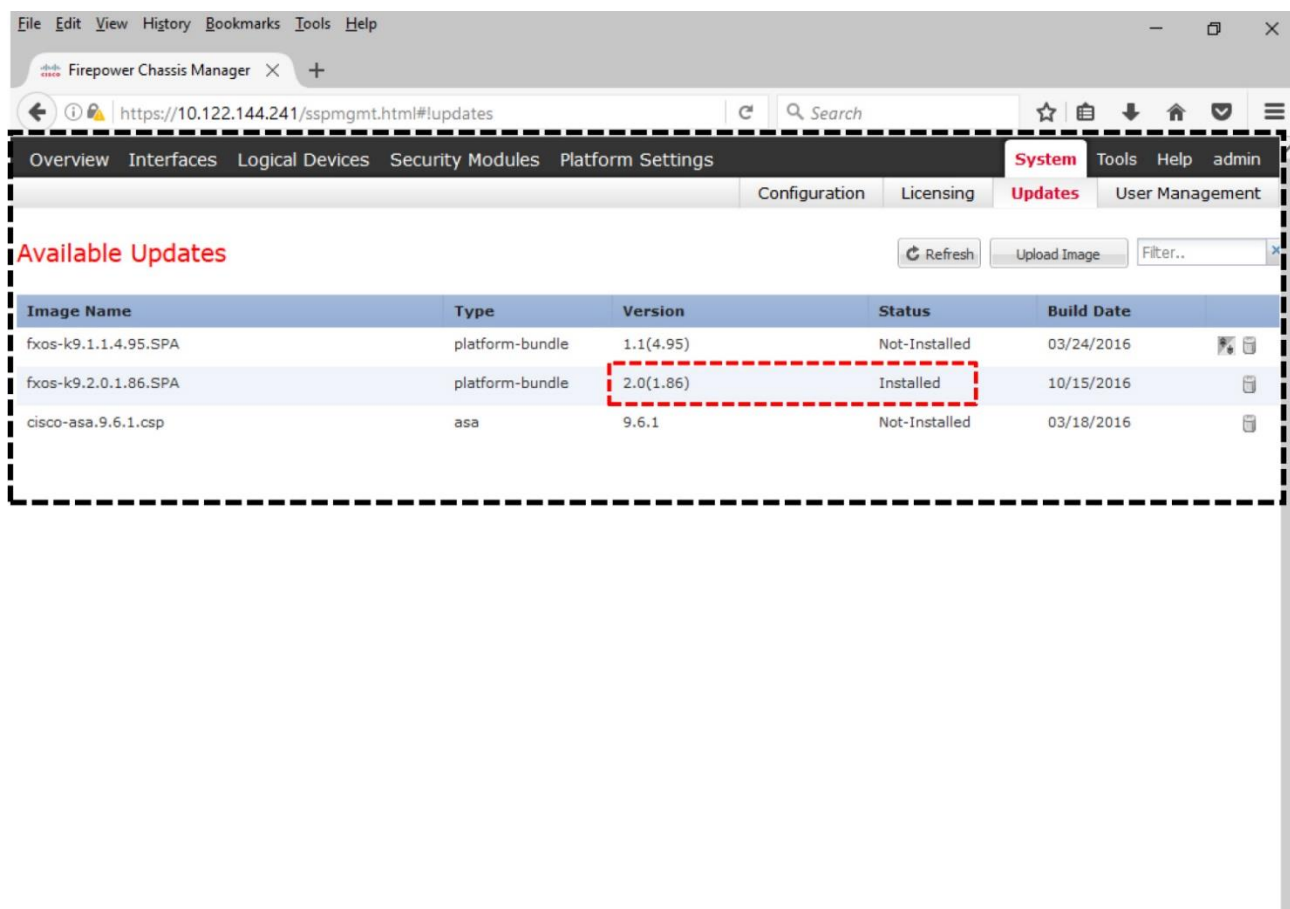


Figure 3-17. *The System Updates Page with List of Available Update Files*

Tip

During an upgrade, you can access the console terminal to determine the upgrade status. Read the Verification and Troubleshooting Tools section to learn the CLI commands for it.

Enable Interfaces

Before installing an FTD software, you need to enable the network interfaces on your Firepower appliance (physical chassis) that will be used by the FTD (a logical device) to transfer traffic. The options to configure interfaces can be categorized into two types:

- Mandatory (Defines traffic type — Management or data)
- Optional (Defines traffic aggregation or segregation)

Let's take a look at an overview of the different types of interface configurations.

- **Mandatory Configurations:** When you enable an interface, you must define if the interface will be used to transfer management traffic or data traffic. The interfaces on a Firepower appliance carry only one type of traffic at the same time. A Firepower appliance does not share the same data interface between two logical devices, however it can share a management interface between multiple logical devices.

- **Optional Configurations:** You can, optionally, utilize the built-in features to segregate or aggregate traffic. For example, you can enable an interface with the *Firepower-eventing* option. It segregates events from the management traffic, and allows you to utilize an interface exclusively to transfer events.

You can also bundle multiple physical interfaces, and aggregate their traffic into a single logical port, known as Port Channel or EtherChannel. The FXOS software uses the Link Aggregation Control Protocol (LACP) to bundle up to 16 interfaces.

Enablement of Management and Data Interface

To enable an interface with an existing configuration, go to the **Interfaces** page of the Firepower Chassis Manager. By default, you should be at the **All Interfaces** tab. Here, you can just click on the **Disabled** button, located under the **Admin State** column.

[Figure 3-18](#) displays the options that allows you to enable, disable or modify the settings of an interface.

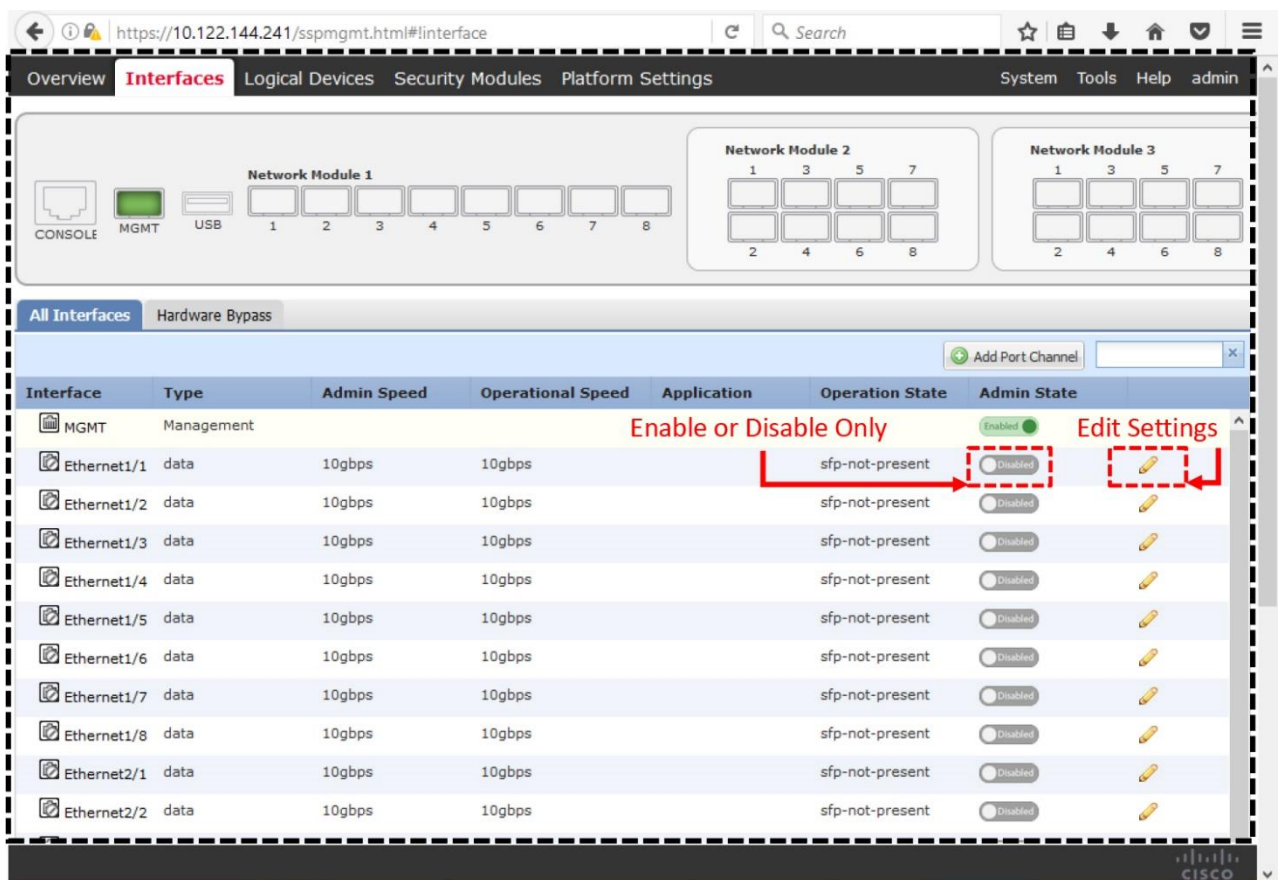


Figure 3-18. Options to Change the Status of an Interface

If you, however, want to modify any existing settings, such as, changing the type from data traffic to management traffic or vice versa, follow the steps below:

Step 1. Navigate to the **Interfaces** page of the Firepower Chassis Manager.

Step 2. Under the **All Interfaces** tab, click the *pencil* icon (at the right-hand side of a row) for the interface you want to modify. The Edit Interface popup window appears.

[Figure 3-19](#) shows the Ethernet1/1 interface is enabled, and configured with the Management (mgmt) type traffic.

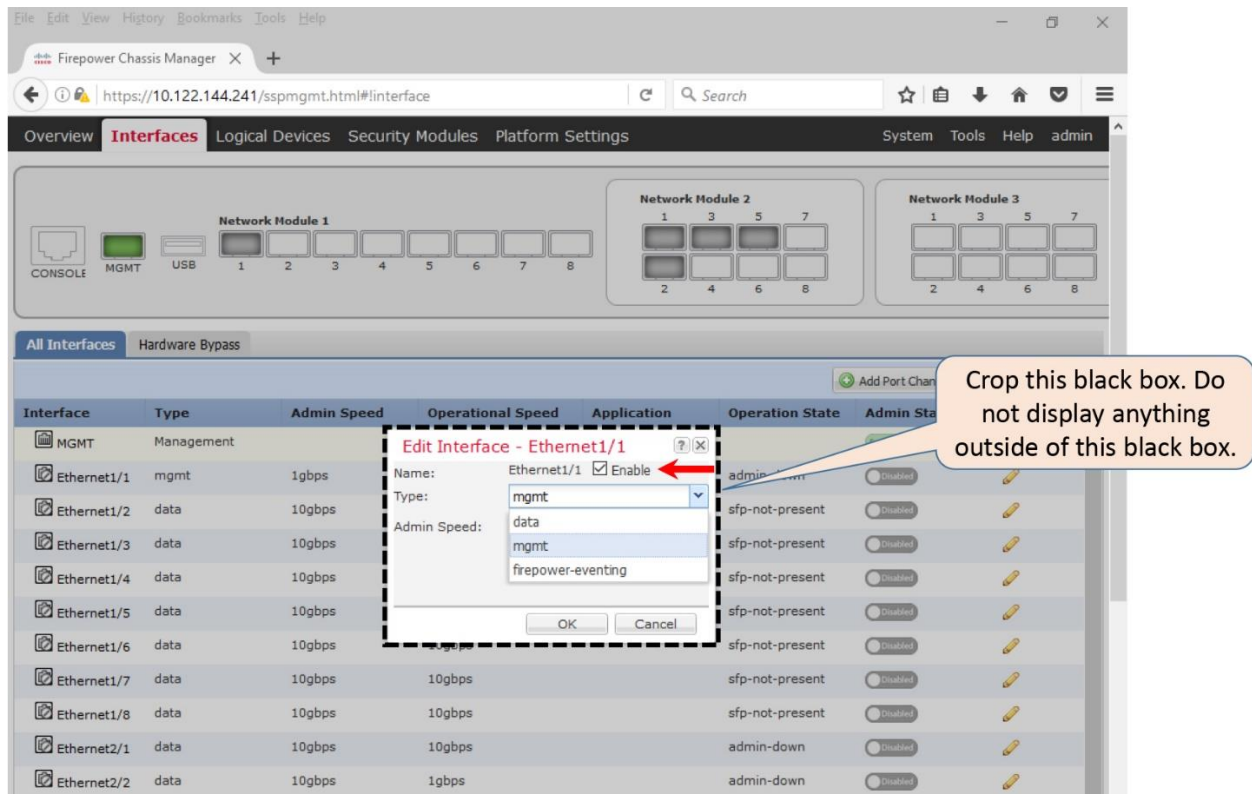


Figure 3-19. *The Configurable Options for an Interface*

Step 3. Using the **Type** drop-down, select the type of traffic that you want the interface to carry. Optionally, you can also modify the speed.

Step 4. Select the **Enable** checkbox if you want to enable this interface immediately with the updated settings.

Step 5. Click the **OK** button to save the changes. The Interfaces page returns and reflects the changes you have just made.

[Figure 3-20](#) shows the **Operation State** is **Up** and the **Admin State** is **Enabled** after the Ethernet1/1 interface is configured and enabled. The first port on the **Network Module 1** also becomes green.

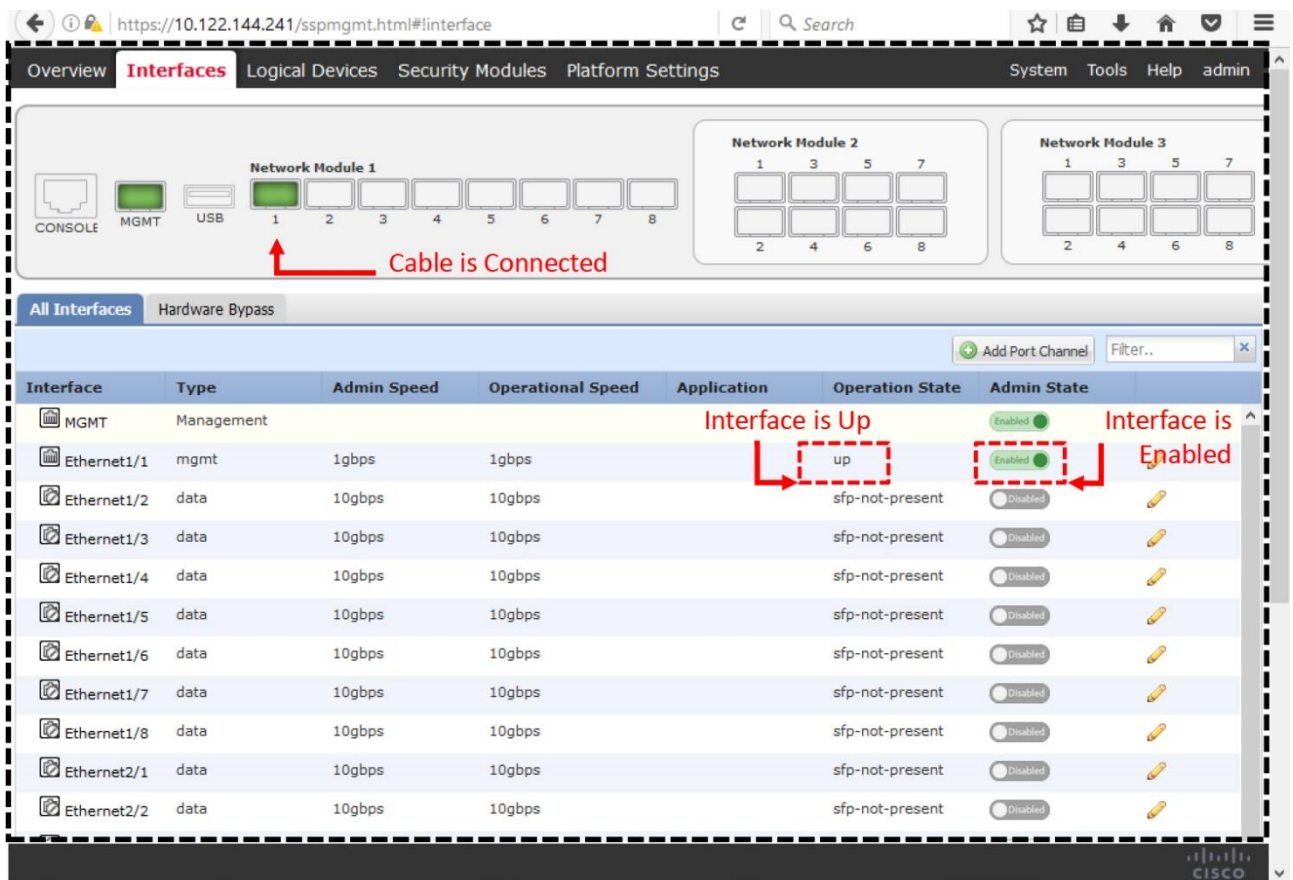


Figure 3-20. Changes on the User Interface After an Interface is Enabled

Addition of a Port Channel or EtherChannel

A Port channel or EtherChannel is a logical group of several (up to 16) physical ports. It is able to aggregate traffic from individual interfaces into a logical port, therefore, the appliance can have an aggregated higher bandwidth. It is also fault tolerant — when one of the links in a logical group fails, the remaining links on the group stays up. The Firepower security appliance natively supports port channel. You can configure it as below:

Step 1. On the Interfaces page, select the **Add Port Channel** button. The **Add Port Channel** configuration window appears.

Step 2. Assign a **Port Channel ID**. The valid values range from 1 to 47.

Step 3. Select the **Enable** checkbox if you want to activate the port channel as soon as the configuration is saved.

[Figure 3-21](#) shows the Ethernet2/1 and Ethernet2/2 are being grouped together in a port channel (ID = 20) to carry data traffic.

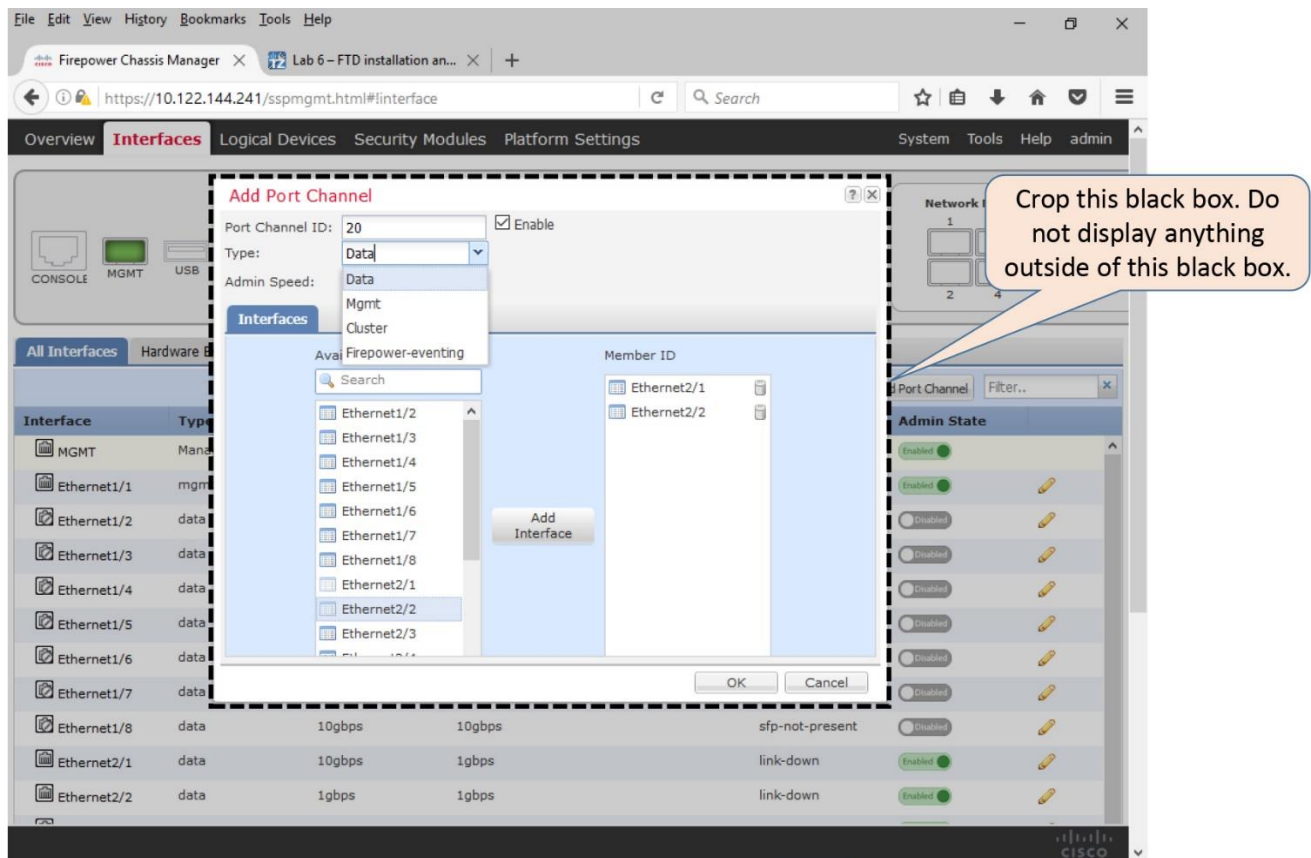


Figure 3-21. Configurations of a Port Channel

Step 4. Define the purpose of the channel by selecting an appropriate **Type** — Management, Data or Firepower-eventing.

Note

The Cluster type is used exclusively by clustered devices as a cluster control link. You can cluster multiple security modules of a Firepower 9300 appliance to gain higher throughput and redundancy.

Step 5. Select the desired interfaces that you want to bundle together in a channel, and click the **Add Interface** button. The selected interfaces move to the **Member ID** section. You can bundle up to 16 interfaces in one port channel.

Step 6. Click the **OK** button to save your configuration. The **Interfaces** page returns. You can view the status of the port-channel you have just created, along with its member interfaces.

Figure 3-22 shows the port channel 20 with two member interfaces Ethernet2/1 and Ethernet2/2.

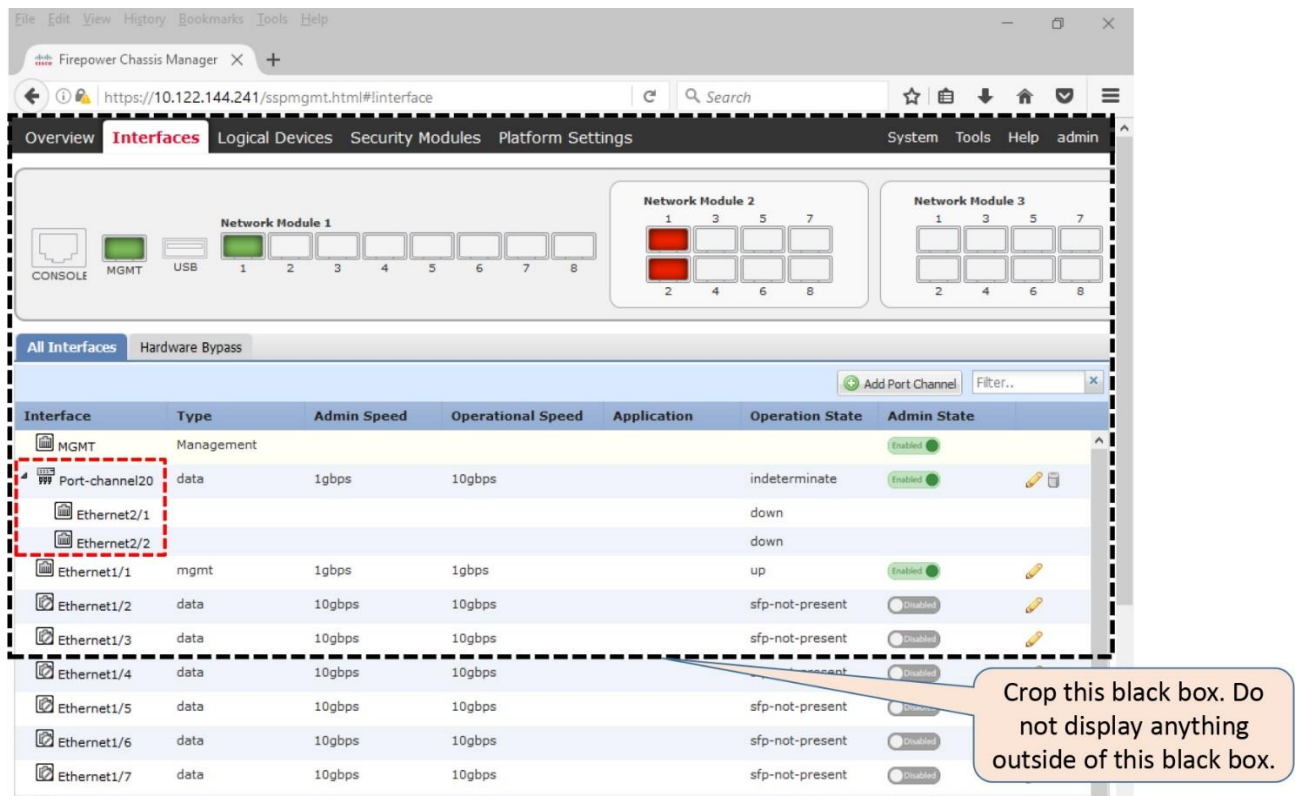


Figure 3-22. Status of a Port Channel is Available on the Interfaces Page

Note

This section has described the process to create a port channel for demonstration purpose only. The remaining sections of this chapter does not use any port channel in the configuration examples. To learn more about port channel and any additional Firepower hardware specific features, please read the Cisco official documentation on FXOS.

Installation of the FTD

Once your Firepower appliance runs FXOS version 2.0.1 or greater, and the necessary interfaces are enabled, you are ready to install the FTD software Version 6.1. The following steps describes the FTD installation process:

Upload the FTD Software

Step 1. Download the FTD software Version 6.1 from the Cisco support site.

Step 2. Login to the Firepower Chassis Manager, and go to the **System > Updates** page.

Step 3. Select the **Upload Image** button and then **Browse** the FTD software image. Once an image is selected, click on the **Upload** button to begin the upload process.

Figure 3-23 demonstrates a workflow for uploading an FTD software image to the Firepower Chassis Manager.

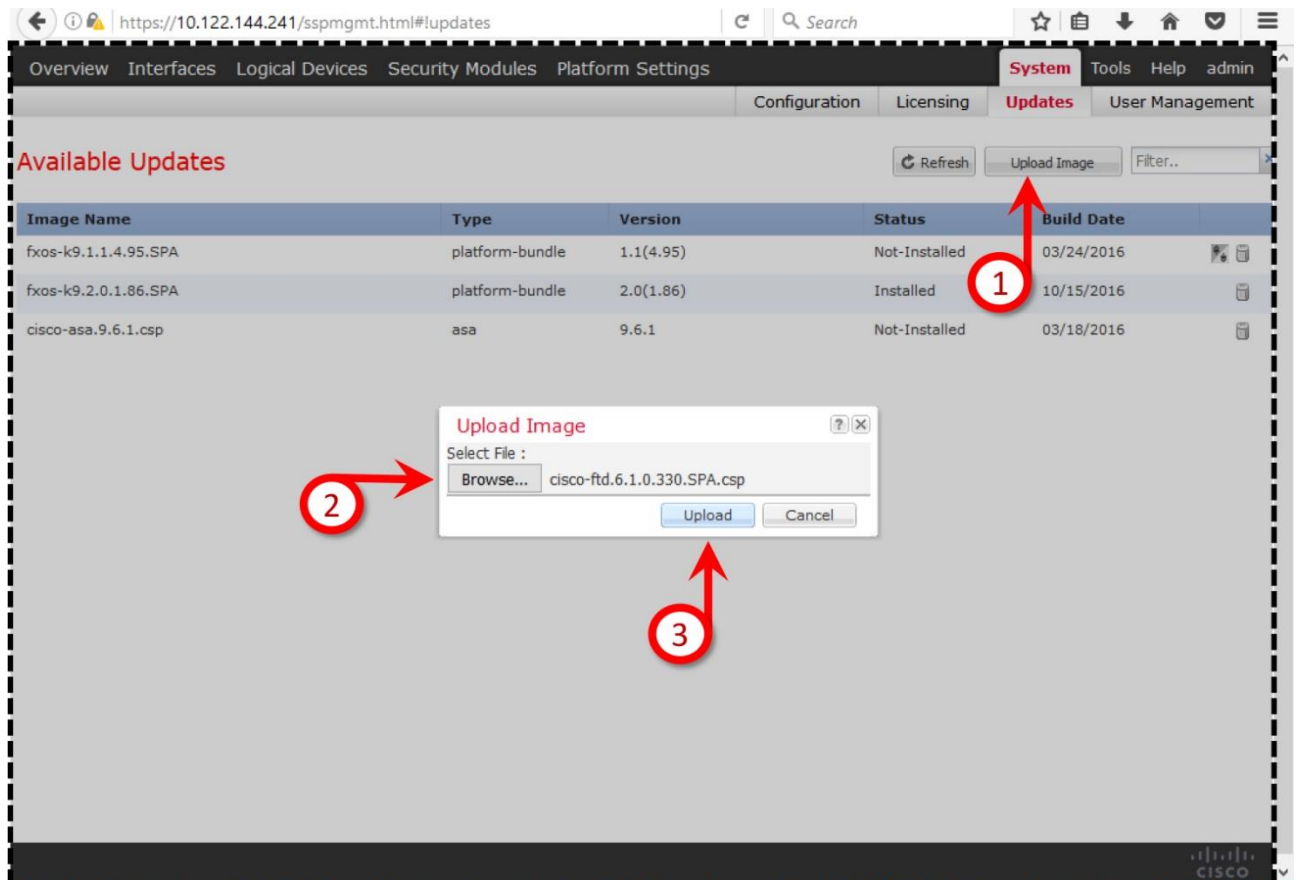


Figure 3-23. Workflow for Uploading an FTD Software Image

Step 4. After a successful upload, an End User License Agreement (EULA) window appears. Accept the EULA and press **OK**. The FTD software image now is stored on the appliance, but it is not installed yet.

[Figure 3-24](#) displays the EULA after an FTD software image is successfully uploaded into the Firepower Chassis Manager.

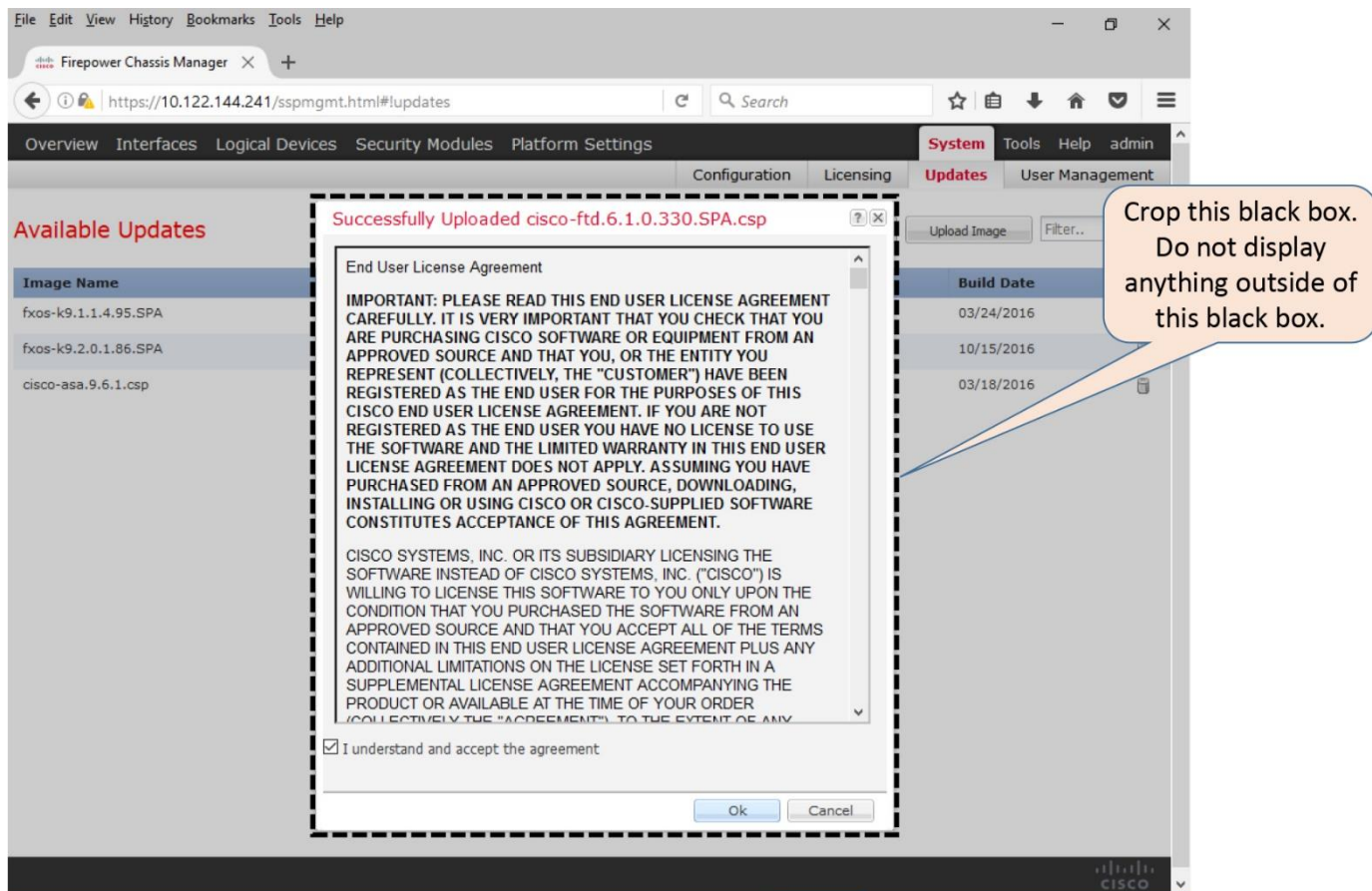


Figure 3-24. Confirmation of a Successful Upload Appears with the EULA Messages

Add a Logical Device for FTD

If you completed all of the steps described in the previous sections, you are now ready to add a logical device for FTD. During adding the logical device, the FTD software Version 6.1 is installed on the FXOS Release 2.0.1. Let's learn the processes step by step.

Step 1. On the Firepower Chassis Manager, navigate to the **Logical Devices** page, and click the **Add Device** button. The **Add Device** window appears.

Step 2. Provide a name for the logical device you are going to deploy on the FXOS, select the FTD template and the image version 6.1.x.

[Figure 3-25](#) illustrates the steps to navigate to the **Add Device** window, and to add a new FTD logical device called *FTD_610*.

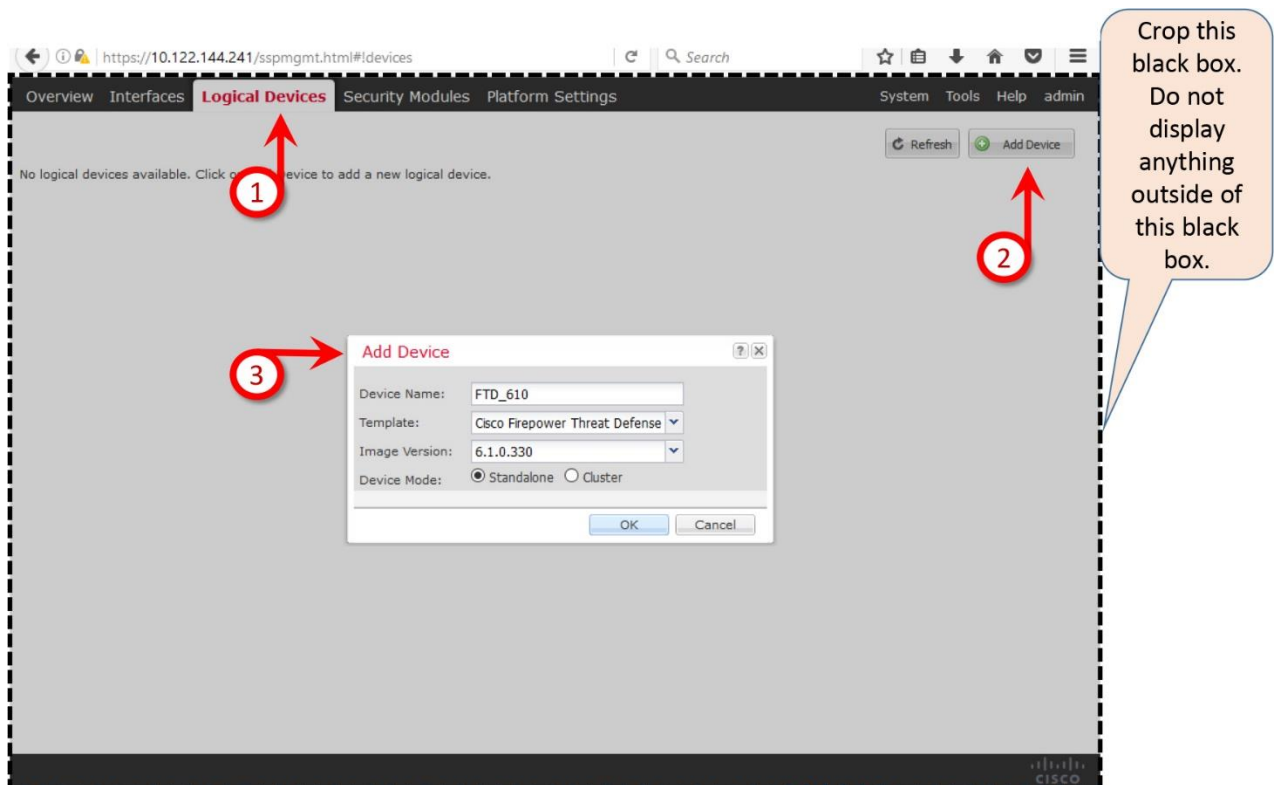


Figure 3-25. *Navigation to the Add Device Page*

Step 3. Choose the **Standalone** device mode, and click **OK**. A configuration page appears where you provision the standalone FTD logical device.

Note

A Standalone mode allows you to create unique logical device on each security module, whereas a Cluster mode allows you to bundle multiple security modules into one logical device.

Figure 3-26 demonstrates the three major steps to provision an FTD logical device.

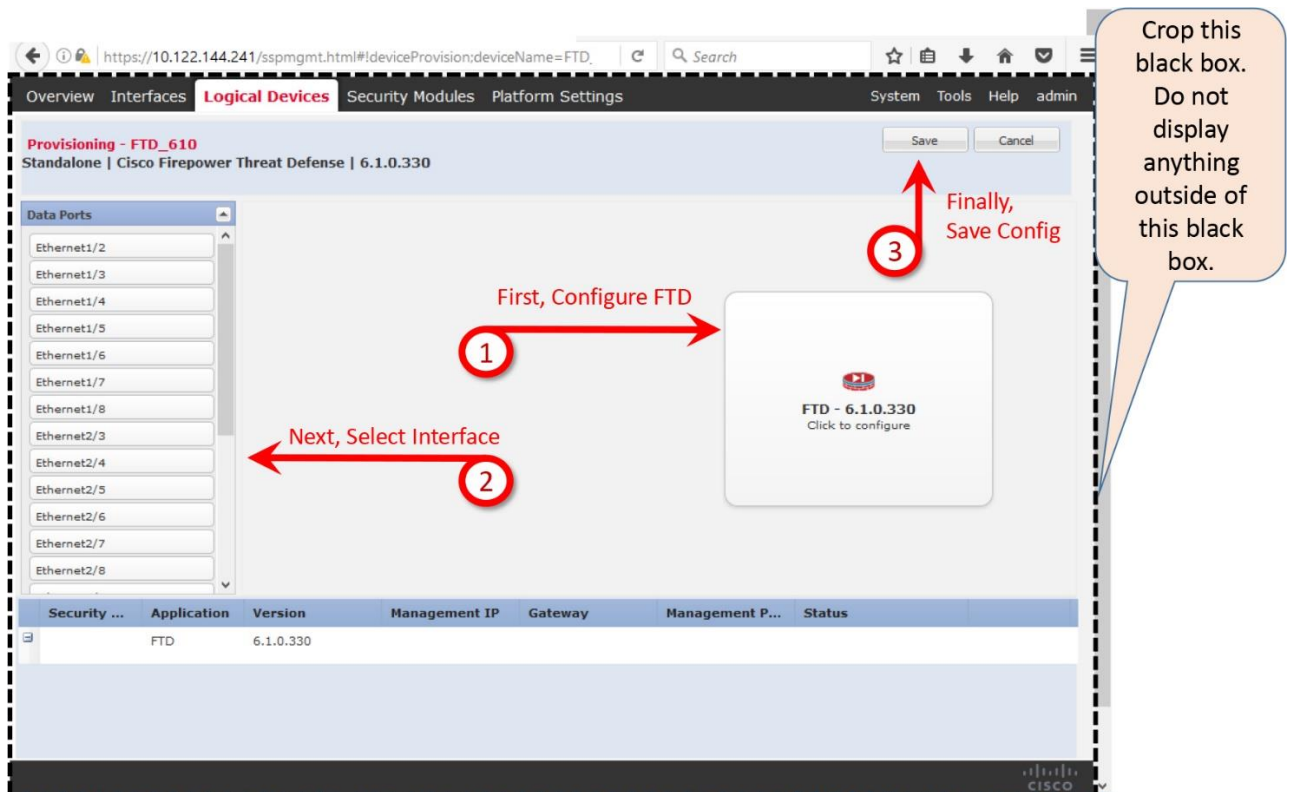


Figure 3-26. Workflow for Provisioning an FTD Logical Device

Step 4. On your right hand side, click on the FTD icon. A configuration window appears.

Step 5. In the **General Information** section of the configuration window, select a security module where you want to install the FTD software, and configure the management network. Once complete, click **OK** to return to the provisioning page.

[Figure 3-27](#) indicates that the security module 1 (SM 1) is selected for the FTD installation, where the Ethernet1/1 is configured as the management interface for the FTD.

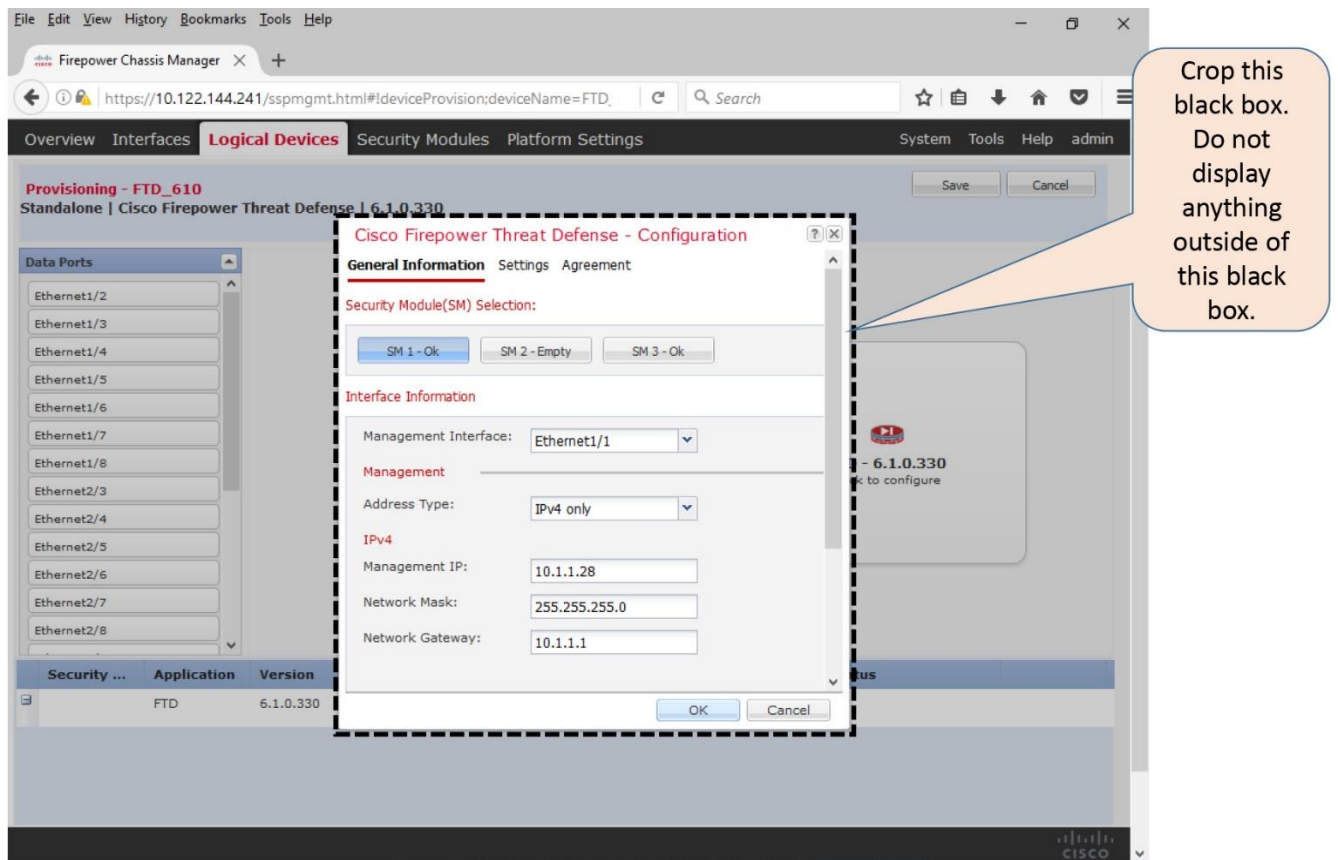


Figure 3-27. Configuration of the FTD Management Network

Tip

This example skips the configurable items under the Settings and Agreement sections for now, because they reappear on the CLI of the FTD, during the initialization process. You can configure them at that time through the CLI.

Step 6. After you return to the provisioning page, select the interfaces or port channels that will be transferring data traffic to and from FTD.

[Figure 3-28](#) confirms the interfaces of the FTD logical device. The Ethernet2/3 and Ethernet2/4 interfaces of the Firepower chassis are selected as the data interfaces, while the Ethernet1/1 interface is configured as a management interface.

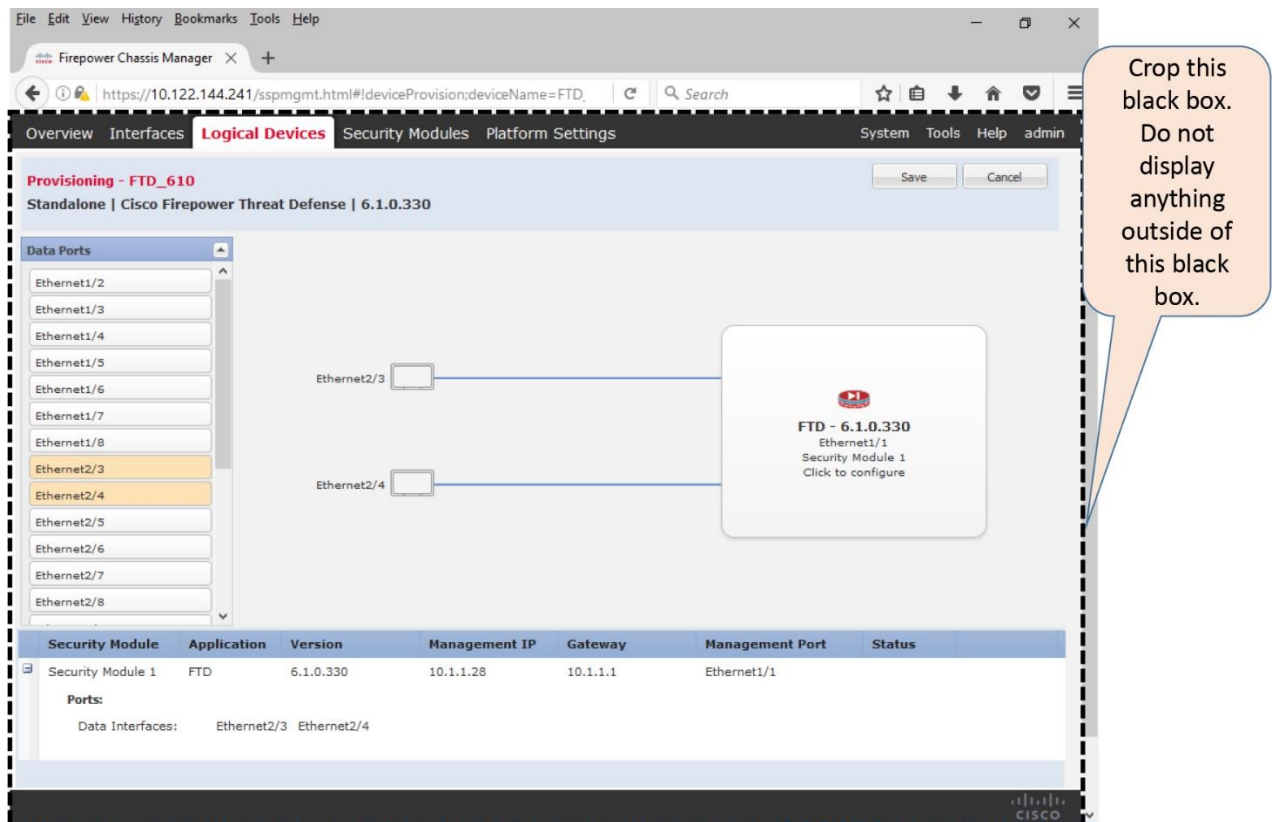


Figure 3-28. Graphical Representation of the FTD Logical Device

Step 7. Once complete, click the **Save** button. The **Logical Devices** page returns. The FTD installation process begins. It takes about 5 minutes to complete the installation.

[Figure 3-29](#) confirms the launch of the FTD software installation. The **installing** Status Indicates the FTD Installation is in Progress

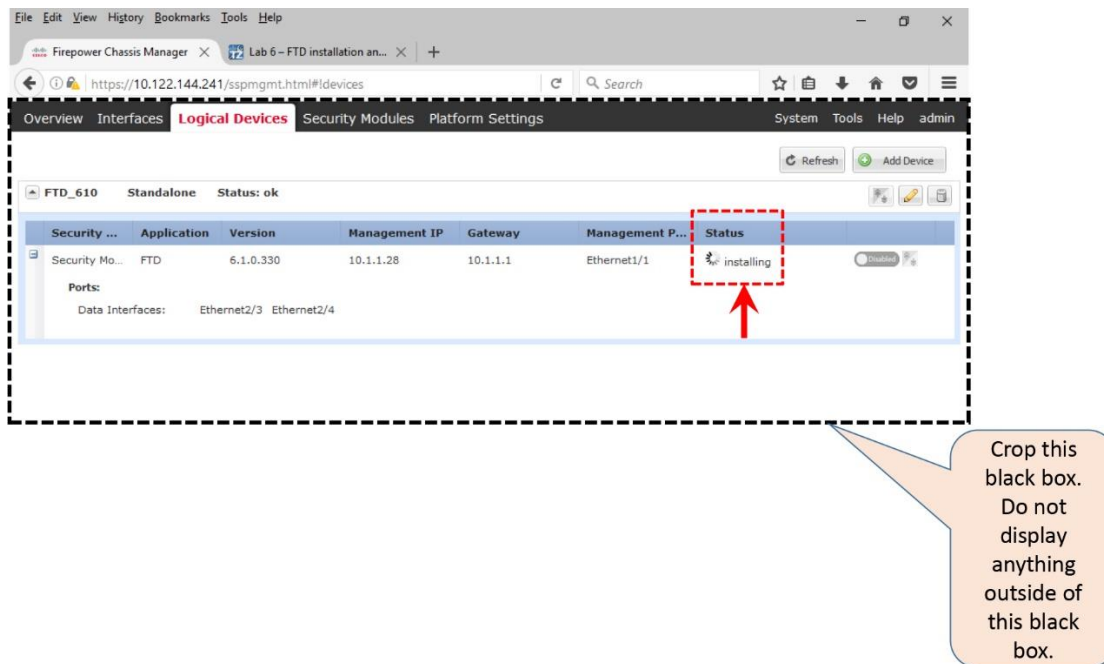


Figure 3-29. *The FTD Installation Process is in Progress*

[Figure 3-30](#) shows the FTD software installation is complete and online. From the time when the FTD installation begins, the system takes about 5-10 minutes to come to the **online** state.

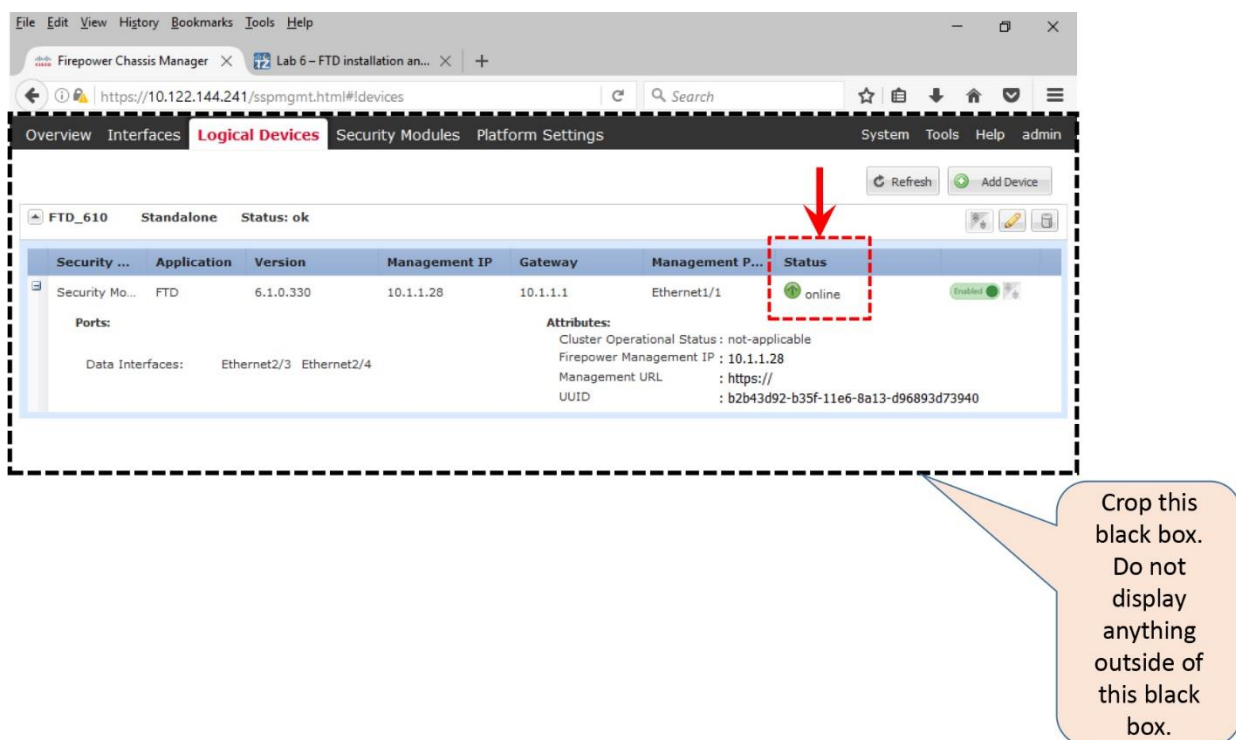


Figure 3-30. *The FTD Installation Process is Fully Complete*

Complete the Initialization of FTD

After the installation is complete, the FTD logical device begins initialization by itself and applies the settings that you configured in the FTD provisioning page. Using the CLI, you can now view the progress of initialization and configure any additional settings, such as, password for the admin user.

To access the CLI of the FTD, first you have to access the CLI of the FXOS via Secure Shell (SSH) or the console terminal. Then connect to the security module where FTD is installed, and then complete any necessary steps.

[Example 3-1](#) demonstrates the process to access the CLI of the FTD software from the CLI of the FXOS, and to complete the system initialization.

Example 3-1 Access the CLI of an FTD for the First Time

! Run the following command on the CLI of the FXOS

```
Firepower-9300# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
CISCO Serial Over LAN:
Close Network Connection to Exit
Firepower-module1>
```

! Now, run the following command to connect to the CLI of the FTD:

```
Firepower-module1> connect ftd
Connecting to ftd console... enter exit to return to bootCLI
System initialization in progress. Please stand by.
You must change the password for 'admin' to continue.
Enter new password:
Confirm new password:
```

! The following network settings should auto-populate, if you configured them in the FTD provisioning page. In such case, no action necessary. Please be patient.

```
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]: manual
Enter an IPv4 address for the management interface [10.1.1.28]: 10.1.1.28
Enter an IPv4 netmask for the management interface [255.255.255.0]:
255.255.255.0
Enter the IPv4 default gateway for the management interface [10.1.1.1]:
10.1.1.1
Enter a fully qualified hostname for this system [Firepower-module1]:
Firepower-module1
Enter a comma-separated list of DNS servers or 'none' [none]: none
Enter a comma-separated list of search domains or 'none' [none]: none
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
```



```
Configure firewall mode? (routed/transparent) [routed]: routed
Configuring firewall mode ...
```

Update policy deployment information

- add device configuration
- add network discovery
- add system policy

You can register the sensor to a Firepower Management Center and use the Firepower Management Center to manage it. Note that registering the sensor to a Firepower Management Center disables on-sensor Firepower Services management capabilities.

When registering the sensor to a Firepower Management Center, a unique alphanumeric registration key is always required. In most cases, to register

a sensor to a Firepower Management Center, you must provide the hostname or the IP address along with the registration key.

```
'configure manager add [hostname | ip address ] [registration key ]'
```

However, if the sensor and the Firepower Management Center are separated by a

NAT device, you must enter a unique NAT ID, along with the unique registration key.

```
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'
```

Later, using the web interface on the Firepower Management Center, you must use the same registration key and, if necessary, the same NAT ID when you add

this sensor to the Firepower Management Center.

>

The '>' prompt at the end of [Example 3-1](#) confirms that the installation is complete. The next step is to verify the network connectivity on the management interface, and then begin the registration process.

Verification and Troubleshooting Tools

This section describes the commands that you can run to verify the status of a Firepower hardware before and after an FTD logical device is added.

Navigation to the FTD CLI

In order to determine the status of various hardware and software components, first you need learn how to go back and forth between the FXOS CLI and FTD CLI.

[Figure 3-31](#) describes the processes to access various levels of the FTD CLI from the FXOS CLI.

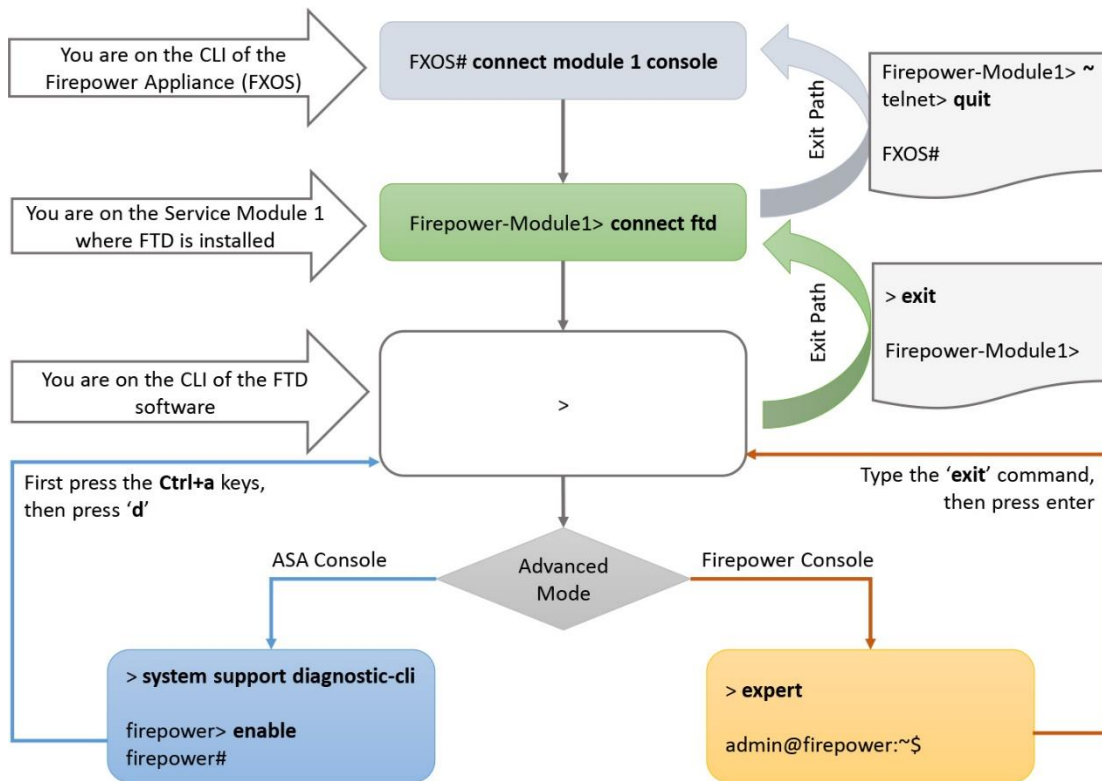


Figure 3-31. Workflow for the FTD CLI Navigation

[Example 3-2](#) demonstrates the commands to connect to the FTD software and then return to the FXOS software.

Example 3-2 Commands to Enter and Exit the CLI of FTD and FXOS

! Assuming you are on the CLI of FXOS, first run the following command to connect to the Security Module (SM 1) where FTD software is installed.

```
Firepower-9300# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
CISCO Serial Over LAN:
Close Network Connection to Exit
```

```
Firepower-module1>
```

! Now, you are on the CLI of the Security Module 1 (SM 1). Run the following command to connect to the CLI of the FTD:

```
Firepower-module1>connect ftd
Connecting to ftd console... enter exit to return to bootCLI
```

```
>
```

! Now, you are on the CLI of the FTD software where you perform most of the FTD related

tasks. If you want to ASA console, run the following command on the CLI of the FTD:

```
> system support diagnostic-cli
```

```
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
```

```
Type help or '?' for a list of available commands.
```

```
firepower>
```

! Now, you are on the CLI of the ASA software. Run the following command to access the privileged mode. Press the enter key when you are prompted for a password.

```
firepower> enable
```

```
Password:
```

```
firepower#
```

! To exit from the ASA console, press 'Ctrl+a then d' to detach.

```
firepower#
```

```
Console connection detached.
```

```
>
```

! You are now back to the CLI of FTD. To exit from the FTD CLI, run the following command:

```
> exit
```

```
Firepower-module1>
```

! You have now returned to the Service Module CLI. To exit, press the escape character

'~', run the 'quit' command.

```
Firepower-module1> ~
```

```
telnet> quit
```

```
Connection closed.
```

```
Firepower-9300#
```

! You are now back to the CLI of the FXOS software.

[Verification of the FXOS Software](#)

Using the CLI of the FXOS, you can verify the version, settings and status of various software components, for example, firmware, host operating system, guest operating system, etc. You can also enter into the modular components of the Firepower hardware independently by changing the modes on the CLI. The command to change the current mode is **scope**. To find the available modes and their descriptions, add a '?' sign after the **scope** command. A mode (scope) can also have a sub-mode — a child mode within a parent mode.

[Example 3-3](#) shows that the Firepower security appliance is running firmware version 1.0.10.

Example 3-3 *Command to Verify the Firmware Version and Its Status*

```
Firepower-9300# scope chassis 1
```

```
Firepower-9300 /chassis # show sup version detail
```

```
SUP FIRMWARE:
```

```
ROMMON:
```

```

Running-Vers: 1.0.10
Package-Vers: 1.0.10
Activate-Status: Ready
Upgrade Status: SUCCESS
FPGA:
Running-Vers: 1.05
Package-Vers: 1.0.10
Activate-Status: Ready

```

```
Firepower-9300 /chassis #
```

[Example 3-4](#) shows that the Firepower Manager is running FXOS release 2.0.1. However, the FXOS software on the security module 3 is being currently upgraded from 1.1.4 to 2.0.1.

Example 3-4 *Command to Determine the Status of the FXOS Software*

```

Firepower-9300# scope system
Firepower-9300 /system # show firmware monitor
FPRM:
Package-Vers: 2.0(1.86)
Upgrade-Status: Ready

Fabric Interconnect A:
Package-Vers: 2.0(1.86)
Upgrade-Status: Ready

Chassis 1:
Server 1:
Package-Vers: 2.0(1.86)
Upgrade-Status: Ready
Server 3:
Package-Vers: 2.0(1.86),1.1(4.95)
Upgrade-Status: Upgrading

```

```
Firepower-9300 /system #
```

Verification of the Status of a Security Application

When you add an FTD logical device on a Firepower appliance, it installs the FTD software as an application. If you suspect an issue with the FTD software operation, you need to check the status of the application, at first.

[Example 3-5](#) displays the status of the “FTD_610” logical device. The device is operational and running on the Security Module 1 (Slot ID 1) on a Firepower 9300 appliance.

Example 3-5 *Status of the Logical Device*

```

Firepower-9300 /ssa # show logical-device

Logical Device:
Name      Description Slot ID   Mode      Operational State
Template Name
-----
FTD_610           1      Standalone Ok
ftd

Firepower-9300 /ssa #

```

[Example 3-6](#) exhibits the status of an FTD application. The first output confirms that the application is being installed. The second output appears when the FTD installation is complete and the application comes online.

Example 3-6 *Status of the FTD Application Instance*

! The following output confirms that FTD application is being installed.

```
Firepower-9300# scope ssa
Firepower-9300 /ssa # show app-instance detail

Application Name: ftd
Slot ID: 1
Admin State: Disabled
Operational State: Installing
Running Version:
Startup Version: 6.1.0.330
Cluster Oper State: Not Applicable
Current Job Type: Install
Current Job Progress: 0
Current Job State: Queued
Clear Log Data: Available
Error Msg:
Hotfixes:
Externally Upgraded: No
```

```
Firepower-9300 /ssa #
```

! The following output proves that the FTD application is up and running.

```
Firepower-9300# scope ssa
Firepower-9300 /ssa # show app-instance detail

Application Name: ftd
Slot ID: 1
Admin State: Enabled
Operational State: Online
Running Version: 6.1.0.330
Startup Version: 6.1.0.330
Cluster Oper State: Not Applicable
Current Job Type: Start
Current Job Progress: 100
Current Job State: Succeeded
Clear Log Data: Available
Error Msg:
Hotfixes:
Externally Upgraded: No
```

```
Firepower-9300 /ssa #
```

Verification of the Security Modules, Adapters and Switch Fabric

An FTD software is installed on a Security Module. If you experience an issue with the FTD, you should check the status of the security module where the FTD software is installed.

Note

The terms “Security Module” and “Security Engine” are used on two different platforms — the Firepower 9300 and 4100 appliances, but refer to the same hardware component.

You can verify the status from the Firepower Chassis Manager:

- On a Firepower 9300 appliance, go to the **Security Modules** page.
- On a Firepower 4100 series appliance, go to the **Security Engine** page.

[Figure 3-32](#) exhibits three security modules on a Firepower 9300 appliance. If you run a Firepower 4100 series appliance, you would see only one Security Engine. For demonstration purpose, the icons for each Security Module are highlighted.

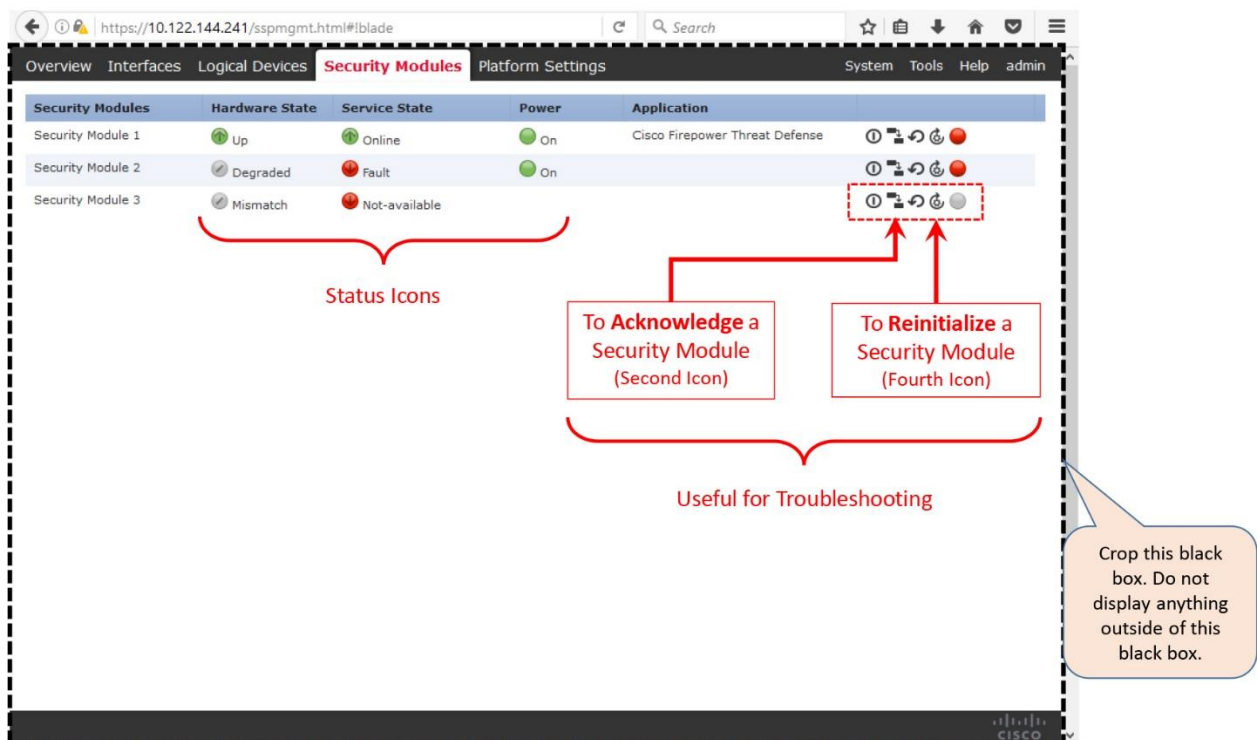


Figure 3-32. *Different Hardware and Service States of the Service Modules*

Tips

Read the Firepower Chassis Manager Configuration Guide to learn more about the possible hardware and service states.

If you want to determine the status of a service module from the CLI, you can run the **show server** command.

[Example 3-7](#) shows that the service modules 1 and 2 are equipped, but only the module 1 is up and module 2 is faulty. The module 3 is mismatched, which means this module is decommissioned, unacknowledged, or newly installed.

Example 3-7 Overall Status of the Security Modules

```
Firepower-9300# show server status
Server Slot Status Overall Status Discovery
-----
1/1 Equipped Ok Complete
1/2 Equipped Degraded Complete
1/3 Mismatch
Firepower-9300#
```

[Table 3-2](#) describes various scenarios of a security module, and the action item that you should take to bring the module in operational state.

Scenario	Action
Security module is new, and installed into a slot	Acknowledge the security module
Security module has existing data, but you want to place it in a new or different slot	Reinitialize the security module before you deploy a logical device on it
Security module is decommissioned, in order to discontinue the use temporarily	Acknowledge the security module
Error in an security module	Try restarting the security module
Security module shows "mismatch" or "token mismatch" status	Acknowledge the security module. If it is not fixed, reinitialize the security module

Table 3-2. Actions to Operate a Security Module in Various States

[Example 3-8](#) shows that security modules 1 and 3 are operable, which means they are in good health. The module 1 is running, and module 3 is booting up (config state). However, the module 2 is inoperable.

Example 3-8 Determine the Health of a Security Module

```
Firepower-9300# show server environment
Server 1/1:
  Overall Status: Ok
  Operability: Operable
  Oper Power: On

Server 1/2:
  Overall Status: Degraded
  Operability: Inoperable
  Oper Power: On

Server 1/3:
  Overall Status: Config
  Operability: Operable
  Oper Power: On
Firepower-9300#
```

In the architectural diagram ([Figure 3-3](#)) of a Firepower appliance, you have learned that each security module is connected to two adapters which are connected to a switch fabric. When you are troubleshooting, it is also important to determine if the adapter and the switch fabric are operational.

[Example 3-9](#) shows two adapters on each security module. All of the adapters are in good health.

Example 3-9 Overall Status of the Adapters

```
Firepower-9300# show server adapter
Server 1/1:
  Adapter PID                Vendor                Serial                Overall
Status
-----
-----
      1 FPR-C9300-MP          Cisco Systems Inc    XXXXXXXXXXXXX        Operable
      2 FPR-C9300-MP-MEZZ    Cisco Systems Inc    XXXXXXXXXXXXX        Operable

Server 1/3:
  Adapter PID                Vendor                Serial                Overall
Status
-----
-----
-
      1 FPR-C9300-MP          Cisco Systems Inc    XXXXXXXXXXXXX        Operable
      2 FPR-C9300-MP-MEZZ    Cisco Systems Inc    XXXXXXXXXXXXX        Operable

Firepower-9300#
```

[Example 3-10](#) shows that the Switch Fabric Interconnect A is operable.

Example 3-10 Operability of the Switch Fabric

```
Firepower-9300# show fabric-interconnect environment
Fabric Interconnect A:
  Operability: Operable

  Fabric Card 1:
    Threshold Status: N/A
    Overall Status: Operable
    Operability: Operable
    Power State: Online
    Thermal Status: N/A
    Voltage Status: N/A
.
.
<Output_Omitted>

Firepower-9300#
```

[Verification of the Hardware Chassis](#)

You can determine the FXOS software versions of your Firepower appliance from the **Help > About** page. Alternatively, the **System > Updates** page shows any software installed on a system. However, the Firepower Chassis manager web interface does not show the detail of the Firepower hardware. To find more detail information about the hardware components, run the show detail command on the Firepower chassis.

[Example 3-11](#) shows the detail hardware information of a Firepower 4110 appliance. It also shows an operable condition of the appliance.

Example 3-11 *Hardware Overview of a Firepower Security Appliance*

```
Firepower-4110# show chassis detail
```

```
Chassis:
```

```
  Chassis: 1
  User Label:
  Overall Status: Operable
  Oper qualifier: N/A
  Operability: Operable
  Conf State: Ok
  Admin State: Acknowledged
  Conn Path: A
  Conn Status: A
  Managing Instance: A
  Product Name: Cisco Firepower 4110 Security Appliance
  PID: FPR-4110-K9
  VID: V00
  Part Number: XX-XXXXXX-XX
  Vendor: Cisco Systems Inc
  Model: FPR-4110-K9
  Serial (SN): XXXXXXXXXXXX
  HW Revision: 0
  Mfg Date: 2015-12-05T00:00:00.000
  Power State: Ok
  Thermal Status: Ok
  SEEPROM operability status: Operable
  Dynamic Reallocation: Chassis
  Reserved Power Budget (W): 600
  PSU Capacity (W): 0
  PSU Line Mode: Lower Line
  PSU State: Ok
  Current Task:
```

```
Firepower-4110#
```

You can view a summary of the hardware operations on the **Overview** page of a Firepower Chassis Manager. This page displays any hardware errors with severity level, description, cause, occurrence and the time of the incidents.

[Figure 3-33](#) shows the Overview page of a Firepower 9300 appliance. While it shows an overall operational state at the top of the page, below it provides more detail information.

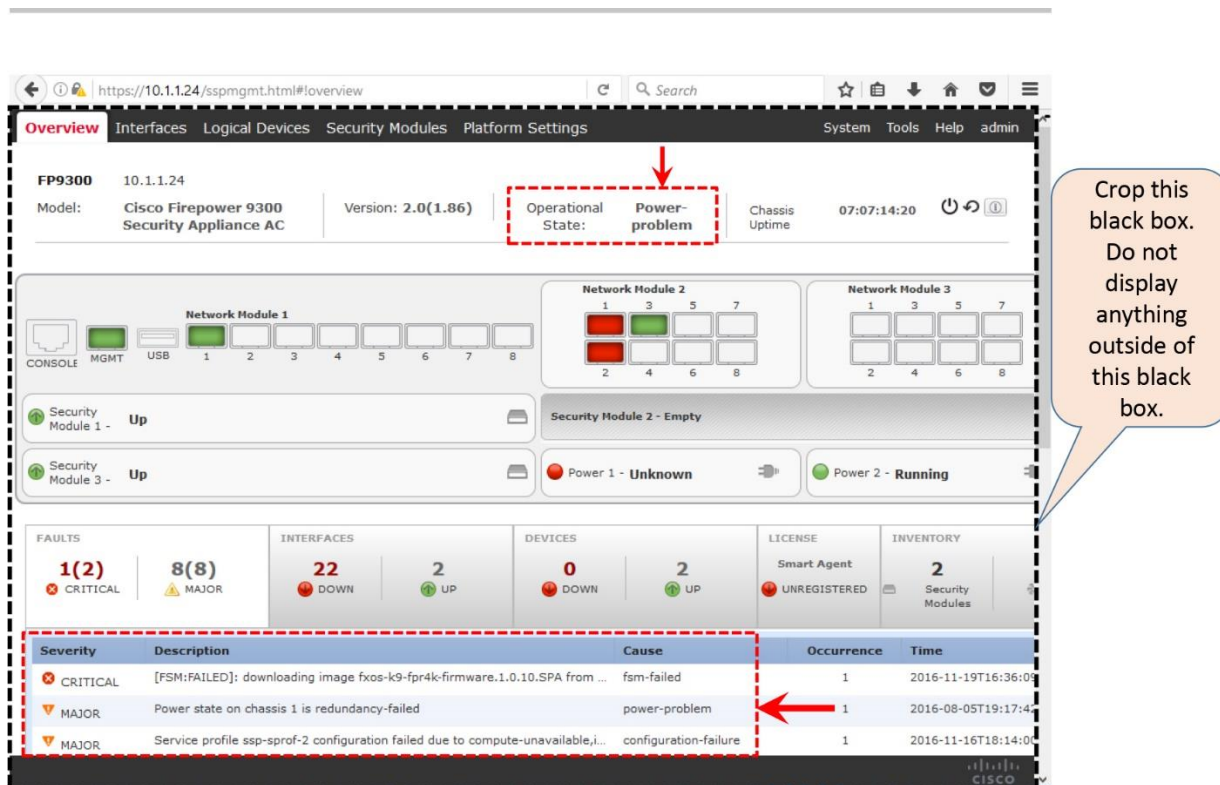


Figure 3-33. Identify Hardware Error from a Firepower Chassis Manager

Similarly, if you choose to use the CLI, there are multiple commands you can run to determine a failure of any major hardware components on a Firepower appliance.

[Example 3-12](#) shows the same errors that you have also found in the web interface, displayed in the previous figure.

Example 3-12 Identification of Hardware Errors from the CLI of FXOS

```
Firepower-9300# show fault
Severity Code Last Transition Time ID Description
-----
Critical F999690 2016-11-19T16:36:09.980 15304334 [FSM:FAILED]:
downloading image fxos-k9-fpr4k-firmware.1.0.10.SPA from
(FSM:sam:dme:FirmwareDownloaderDownload)
Major F0327 2016-11-16T18:14:00.622 15234559 Service profile ssp-
sprof-2 configuration failed due to compute-unavailable,insufficient-
resources
Warning F0528 2016-08-05T19:17:42.663 44431 Power supply 1 in
chassis 1 power: off

Firepower-9300#
```

You can also view the System Event Log (SEL) of a Firepower appliance from the CLI. The **show sel** command on FXOS provides similar output that you can see in the **ipmitool** command on a linux system.

[Example 3-13](#) shows events from the Cisco Integrated Management Controller (CIMC) and Basic Input/Output System (BIOS). The 1/1 parameter with the **show sel** command represents the chassis-1/module-1.

Example 3-13 System Event Logs (SEL) of a Firepower Security Appliance

```
Firepower-9300# show sel 1/1
1 | 12/22/2016 00:03:52 | CIMC | Drive slot(Bay) LED_BLADE_STATUS #0xa6 |
Drive Presence | Asserted
2 | 12/22/2016 00:03:55 | CIMC | Voltage P2V63_VPP_EF #0x1c | Lower
critical - going low | Asserted | Reading 2.48 <= Threshold 2.48 Volts
3 | 12/22/2016 00:03:55 | CIMC | Platform alert LED_SYS_ACT #0xa4 | LED
color is amber | Asserted
4 | 12/22/2016 00:04:29 | BIOS | System Event #0x00 | Timestamp clock synch
| SEL timestamp clock updated, event is first of pair | Asserted
5 | 12/22/2016 00:05:53 | BIOS | System Event #0x83 | OEM System Boot Event
| | Asserted
6 | 12/22/2016 00:18:26 | CIMC | Entity presence MAIN_POWER_PRS #0x55 |
Device Absent | Asserted
7 | 12/22/2016 00:37:15 | CIMC | Temperature GPU1_TEMP_SENS #0x59 | Upper
Non-critical - going high | Asserted | Reading 136 >= Threshold 136 degrees
C
8 | 12/22/2016 00:37:35 | CIMC | Temperature GPU1_TEMP_SENS #0x59 | Upper
Non-critical - going high | Deasserted | Reading 134 <= Threshold 136
degrees C
.
.
<Output_Omitted>
```

Firepower-9300#

[Verification of the Power Supply Unit \(PSU\) Modules](#)

You can find an issue with a Power Supply Unit (PSU) from the **Overview** page of the Firepower Chassis Manager. In addition, you can run several commands on the CLI to investigate any power related issues.

[Example 3-14](#) confirms that one of the power supply units is not turned on. You can identify it from the output of the **show fault** command.

Example 3-14 Overall Operational Status of a Firepower Appliance

```
Firepower-9300# show fault
Severity Code Last Transition Time ID Description
-----
Warning F0528 2016-08-05T19:17:42.663 44431 Power supply 1 in
chassis 1 power: off
Major F0408 2016-08-05T19:17:42.662 44430 Power state on chassis
1 is redundancy-failed
```

Firepower-9300#

[Example 3-15](#) indicates a power problem, and therefore the Firepower 9300 appliance has a power redundancy failure. You can determine this from the output of the **show chassis environment** command.

Example 3-15 Overall Operational Status of a Firepower Security Appliance

```
Firepower-9300# show chassis environment
Chassis 1:
  Overall Status: Power Problem
  Operability: Operable
  Power State: Redundancy Failed
  Thermal Status: Ok
```

```
Firepower-9300#
```

[Example 3-16](#) shows a filtered output of the **show sel** command. It shows events with the “power” keyword only. The events on this example were generated when the main power was disconnected and then reconnected.

Example 3-16 *System Event Log (SEL) of a Firepower Appliance*

```
Firepower-9300# show sel 1/1 | egrep ignore-case power
1 | 12/13/2016 16:37:52 | CIMC | Entity presence MAIN_POWER_PRS #0x55 |
Device Absent | Asserted
2 | 12/13/2016 16:39:23 | CIMC | Entity presence MAIN_POWER_PRS #0x55 |
Device Present | Asserted
```

```
Firepower-9300#
```

[Example 3-17](#) confirms that the Firepower appliance is equipped with two power supply units, but the PSU 1 has no power.

Example 3-17 *A Detail View of the Both Power Supply Units*

```
Firepower-9300# show chassis psu detail
```

```
PSU:
```

```
  PSU: 1
  Overall Status: N/A
  Operability: N/A
  Threshold Status: N/A
  Power State: Off
  Presence: Equipped
  Thermal Status: OK
  Voltage Status: N/A
  Product Name: Cisco Firepower 9000 Series AC Power Supply
  PID: FPR9K-PS-AC
  VID: V01
  Part Number: 341-0723-01
  Vendor: Cisco Systems Inc
  Serial (SN): ART1918F298
  HW Revision: 0
  Firmware Version: N/A
  Type: Unknown
  Wattage (W): 0
  Input Source: Unknown
```

```
  PSU: 2
  Overall Status: Operable
  Operability: Operable
  Threshold Status: OK
  Power State: On
  Presence: Equipped
  Thermal Status: OK
```

```
Voltage Status: OK
Product Name: Cisco Firepower 9000 Series AC Power Supply
PID: FPR9K-PS-AC
VID: V01
Part Number: 341-0723-01
Vendor: Cisco Systems Inc
Serial (SN): ART1918F28X
HW Revision: 0
Firmware Version: N/A
Type: Unknown
Wattage (W): 2500
Input Source: Unknown
```

Firepower-9300#

[Verification of the Fan Modules](#)

A Firepower 9300 and 4100 series appliances have 4 and 6 fan modules, respectively. There are couple of ways to determine the status of any fan modules on a Firepower security appliance:

- You can look at the LED on a fan module. If you notice the color of the LED is amber, it represents a failure.
- On a Firepower Chassis Manager, you can go to the **Overview** page to identify the status of the fans.
- If you choose to use the CLI, there are several commands you can run on the CLI to investigate any fan related issue.

[Example 3-18](#) shows a warning for a missing fan module. One of the fan modules was removed to demonstrate this alert.

Example 3-18 *Warning Message Appears When a Fan Module is Missing or Inoperable*

```
Firepower-9300 /chassis # show fault
Severity Code      Last Transition Time      ID      Description
-----
Warning  F0377    2016-12-02T18:06:24.196  15575670 Fan module 1-2 in
chassis 1 presence: missing
.
.
<Output_Omitted>
```

Firepower-9300 /chassis #

[Example 3-19](#) shows the overall status of the fan modules on a Firepower 9300 appliance. If you run the same command on a 4100 Series appliance, you would find six modules in the output.

Example 3-19 *Overall Health Status of the Fan Modules on a Firepower 9300 Appliance*

```
Firepower-9300 /chassis # show fan-module

Fan Module:
  Tray      Module      Overall Status
```

1	1	Operable
1	2	Removed
1	3	Operable
1	4	Operable

Firepower-9300 /chassis #

[Example 3-20](#) shows detail information about the fan modules on a Firepower 9300 Appliance. The first module is equipped and operational, while the second module is missing.

Example 3-20 *Detail Information About the Fan Modules*

Firepower-9300 /chassis # **show fan-module detail**

Fan Module:

```

Tray: 1
Module: 1
Overall Status: Operable
Operability: Operable
Threshold Status: OK
Power State: On
Presence: Equipped
Thermal Status: OK
Product Name: Cisco Firepower 9000 Series Fan
PID: FPR9K-FAN
VID: 01
Part Number: XX-XXXXXX-XX
Vendor: Cisco Systems Inc
Serial (SN): XXXXXXXXXXXXX
HW Revision: 0
Mfg Date: 2015-05-28T00:00:00.000

```

```

Tray: 1
Module: 2
Overall Status: Removed
Operability: N/A
Threshold Status: N/A
Power State: Off
Presence: Missing
Thermal Status: N/A
Product Name:
PID:
VID: 01
Part Number: XX-XXXXXX-XX
Vendor:
Serial (SN):
HW Revision: 0
Mfg Date: 2015-05-28T00:00:00.000

```

.
.
<Output_Omitted>

Firepower-9300 /chassis #

Summary

This chapter describes the architecture, implementation and installation of FTD on a Firepower Security Appliance running Firepower eXtensible Operating System (FXOS). It demonstrates several command line tools to determine the status of various components of the appliance.

After installation, the next step to deploy an FTD in a network is to register it with a Firepower Management Center. The Part II of the book describes that.

Quiz

1. A Firepower 4100 series security appliance is comprised of various hardware components. Where is an FTD software installed?

- a. Switch Fabric
- b. Security Engine
- c. Supervisor
- d. Adapter

2. The “Mismatch” status of a security module indicates the following:

- a. The module has been decommissioned
- b. The module is recently installed
- c. The module has prior data that does not match
- d. All of the above

3. Which command on the CLI displays any hardware errors that you could view them in the Overview page of a Firepower Chassis Manager?

- a. **show environment**
- b. **show fault**
- c. **show status**
- d. **show chassis**

4. Which command is necessary in order to access the ASA console, if you are currently on the FXOS CLI?

- a. **connect module 1 console**

b. connect ftd

c. system support diagnostic-cli

d. All of the above

5. A Firepower 9300 appliance is currently running FXOS Release 1.1.4. If you want to install FTD Version 6.1 on it, what would be the right order of action?

a. Install Firmware 1.1.10, then install FTD Version 6.1

b. Install FXOS Release 2.0.1, then install FTD Version 6.1

c. Install FTD 6.0, then upgrade to 6.1

d. Install FTD Version 6.1 only

Chapter 4. Firepower Management Center (FMC) Hardware

In the previous chapters, you have learned how to install Firepower Threat Defense (FTD) in various hardware platforms. You cannot, however, define and apply any security policies for your network without an assistance from a manager. This chapter discusses different options to deploy a manager for a Firepower Threat Defense. It illustrates the processes to reimage a manager with the Firepower software, and describes various tools related to the hardware troubleshooting.

Essential Knowledge

To manage a Firepower Threat Defense (FTD), you must require a manager. Depending on the deployment scenario and hardware model, you can choose either an on-box manager, or an off-box manager. This section provides an overview of both types of Firepower manager.

Additionally, in this section, you can learn about some key hardware components of a Firepower manager, such as, Integrated Management Controller (IMC), internal storage for system restoration, etc. This section also introduces you with different types of user interfaces used in a Firepower manager hardware.

On-Box Manager

The FTD software introduces a new user interface that you can run from a web browser, without any requirement for a third party client. This is known as the Firepower Device Manager (FDM). An FDM supports the ASA 5500-X Series low-end and mid-range platforms. As of writing this book, it does not support the Firepower 4100 Series, 9300 Series or Virtual platforms.

The FDM can manage one FTD at any time. If you have more than one FTD system, you will not be able to manage all of the FTD Systems using the same FDM. Therefore, an FDM is a good solution for Small to Medium Business (SMB) network, but not a scalable solution for a large enterprise network. The user interface of FDM targets the users who are not experts on the Firepower System, i.e. the FDM is designed to be simple and intuitive.

[Figure 4-1](#) exhibits a simple topology where an FTD could be managed by an on-box manager — the Firepower Device Manager (FDM).

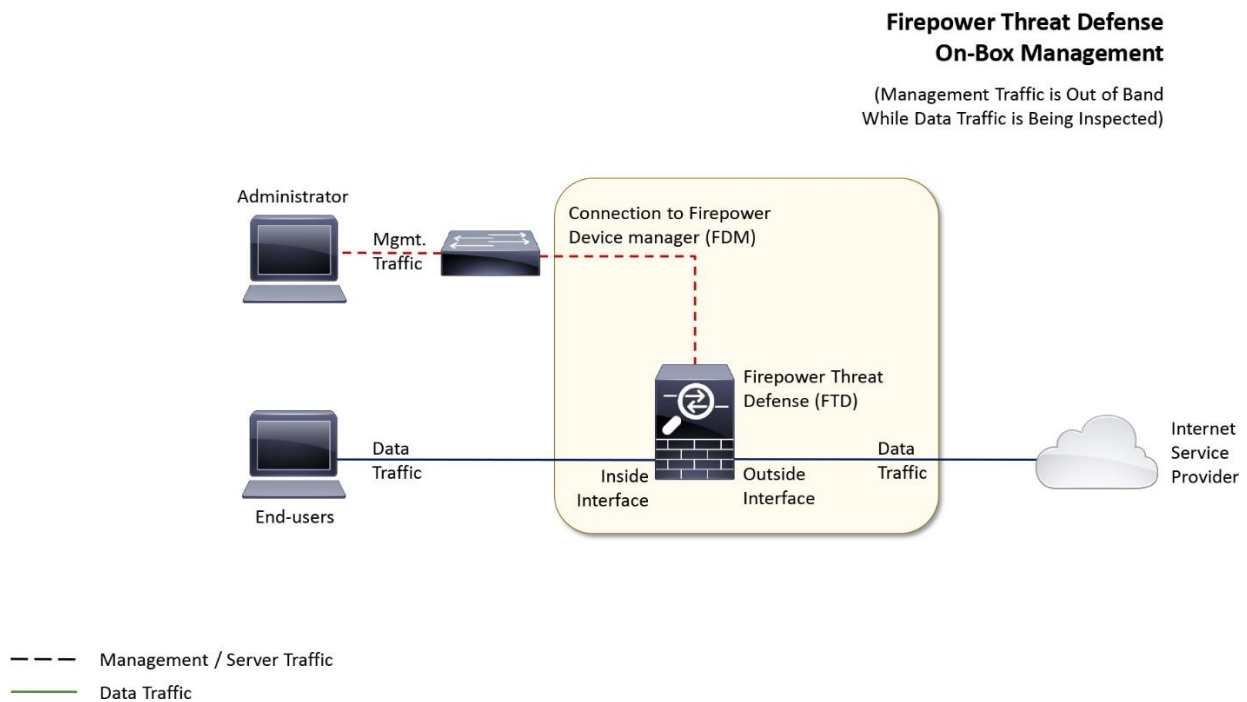


Figure 4-1. An FTD is Managed by an FDM

[Table 4-1](#) shows the key differences between two available options to manage a Firepower Threat Defense (FTD), and provides reasons for choosing an off-box manager over an on-box solution.

	On-Box	Off-Box
Name of the GUI Software	Firepower Device Manager (FDM)	Firepower Management Center (FMC)
Management Capability	1 FTD System	Depending on the model, it can manage hundreds of FTD Systems
Supported FTD Platform	Low-end and mid-range ASA 5500-X series hardware	Any platforms that support FTD software
Deployment	Small to Medium Business (SMB)	Large enterprise network
Cost	Free. No additional hardware necessary	Need to purchase an additional hardware, or a license for virtual appliance
Policy Configuration	Limited functionality	Full functionality
Number of Stored Events	Can store only few hundreds of events	Can store millions of events
API Integration	Does not support third party integration	Fully support integration with various API

Table 4-1. Major Differences Between an On-Box Manager and an Off-Box Manager

Note

This book uses the user interface of an off-box manager to demonstrate any advanced configurations. The user interface of an on-box manager, which is different than the interface of an off-box manager, is out of the scope of this book.

Off-Box Manager

An off-box manager, as the name means, is located off of an FTD appliance. This is designed to configure, monitor, and administer multiple FTD systems using just one single user interface. This off-box manager, a dedicated standalone appliance, is known as the Firepower Management Center (FMC).

An FMC is available as a physical hardware or a virtual appliance. You may find a virtual FMC is easier and cheaper to deploy, as it allows you to use your existing virtual machines infrastructure. On the other hand, although a physical FMC requires you to purchase and deploy an additional hardware in your network, it is able to manage more FTD systems, process additional hosts and users in a network, and store more events.

[Figure 4-2](#) exhibits a typical topology where multiple FTD appliances from different geographical locations are managed by one off-box manager — the Firepower Management Center (FMC).

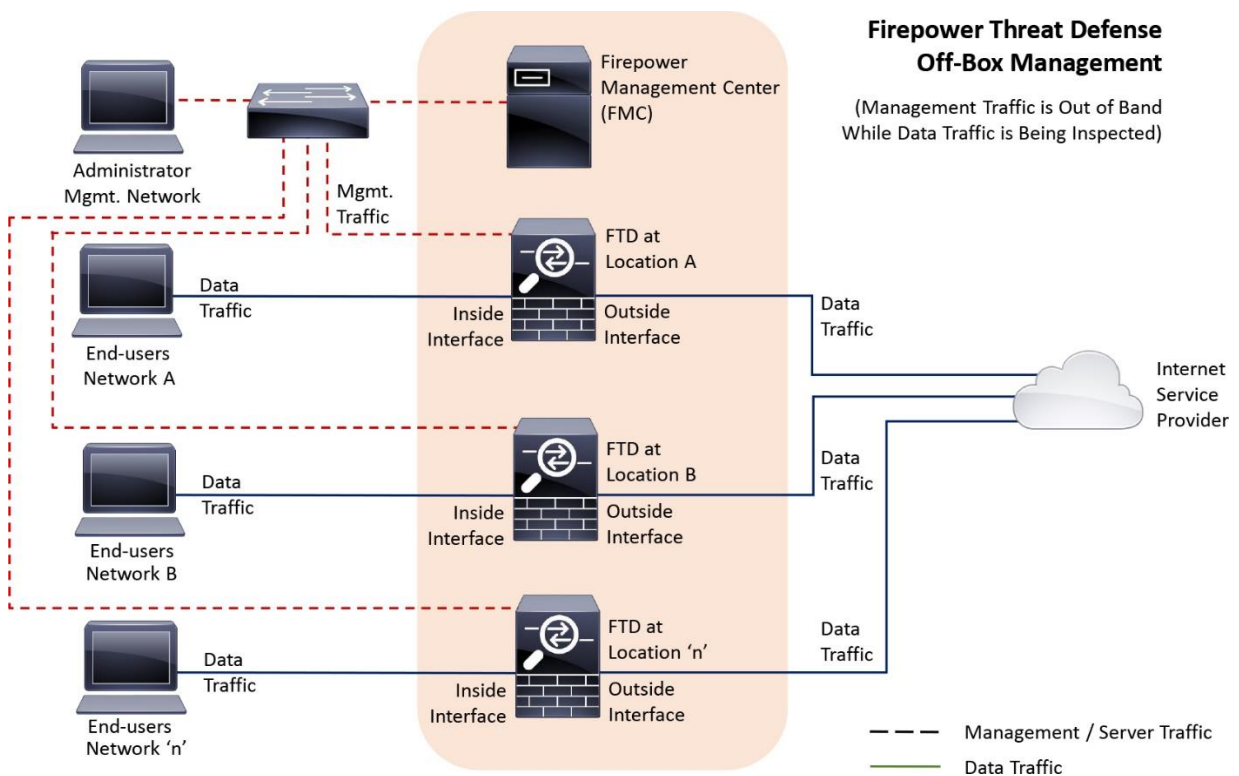


Figure 4-2. Multiple FTD Appliances Are Managed by One Single FMC

[Table 4-2](#) shows the specifications of various FMC hardware. It compares the two latest FMC models that are based on the Cisco UCS C220 M3 chassis, with an FMC Virtual appliance.

Specification	FMC 2000	FMC 4000	Virtual
Processor	Intel(R) Xeon(R) CPU E5-2630 v2 @ 2.60GHz	Intel(R) Xeon(R) CPU E5-2660 v2 @ 2.20GHz	64-bit with virtualization support
Thread/Core x Core/Socket x Socket	24 (2x6x2)	40 (2x10x2)	4 to 8 Virtual CPUs
Memory	64GB	128GB	8GB (Min)
Storage	4 x 600GB SAS	6 x 960GB SSD	250GB

Table 4-2. *Hardware Specifications of Various FMC Appliances*

[Table 4-3](#) shows the differences in performances of various FMC appliances. The differences are based on the hardware resources available in each appliance.

Maximum Number of...	FMC 2000	FMC 4000	Virtual
Managed FTD	250	300	2, 10, 25
Event Storage	1.8 TB	3.2 TB	250 GB
Hosts	150,000	600,000	50,000
Users	150,000	600,000	50,000
IPS Events	60 Million	300 Million	10 Million
Flow Rate	12,000 fps	20,000 fps	Resource Depended
Support High Availability	Yes	Yes	No

Table 4-3. *Performance of Various FMC Appliances*

Note

As of writing this book, Cisco supports additional FMC models. For example, prior to FMC 2000 and FMC 4000 models, the FMC 750, FMC 1500 and FMC 3500 models are released which support any trains of Version 6.x. After FMC 2000 and FMC 4000 models, Cisco introduces the FMC 1000, FMC 2500, and FMC 4500 models that support the Version 6.2 or greater. While new hardware models and software versions are continuously developed, you can apply the knowledge that you learn from this book on any FMC hardware models running the Firepower Software Version 6.1 or greater.

Cisco Integrated Management Controller (CIMC)

The two latest FMC models, FMC 2000 and FMC 4000, are based on the Cisco Unified Communication System (UCS) C220 M3 chassis. One of the hardware components of a UCS C220 server is the Cisco Integrated Management Controller (CIMC). CIMC uses the Intelligent Platform Management Interface (IPMI) to monitor a UCS server. One of the advantages of CIMC is it runs on a separate chip. Therefore, if a UCS server fails, you should still be able to connect to the CIMC to troubleshoot any hardware issues.

[Figure 4-3](#) displays an architectural overview of the CIMC. It shows how the hardware related information is exchanged with the IPMI and is viewed through Syslog, SNMP or XML API.

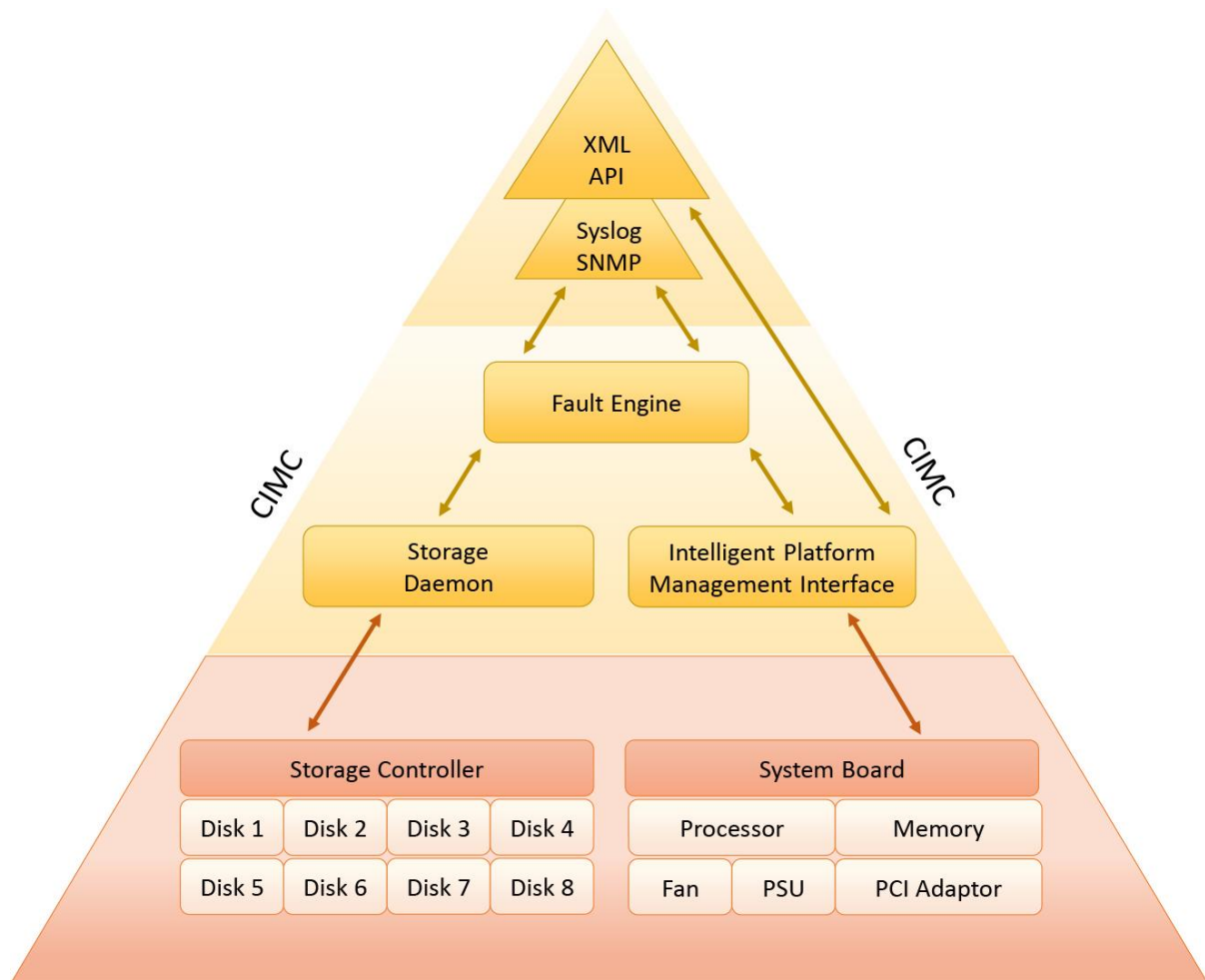


Figure 4-3. *Interaction of CIMC with Various Server Components*

You can access the CIMC Configuration Utility by pressing <F8> during the Power-On Self-Test (POST) operation. Using the configuration utility, you can assign an IP address for the CIMC interface. You can either use a web browser to access the GUI of a CIMC, or a Secure Shell (SSH) client to connect to the CLI of a CIMC.

[Figure 4-4](#) shows that an IP address 10.1.1.12 is assigned to the CIMC interface. In the Additional Settings (Press <F1>) page, you can change the default login password of the CIMC interface.

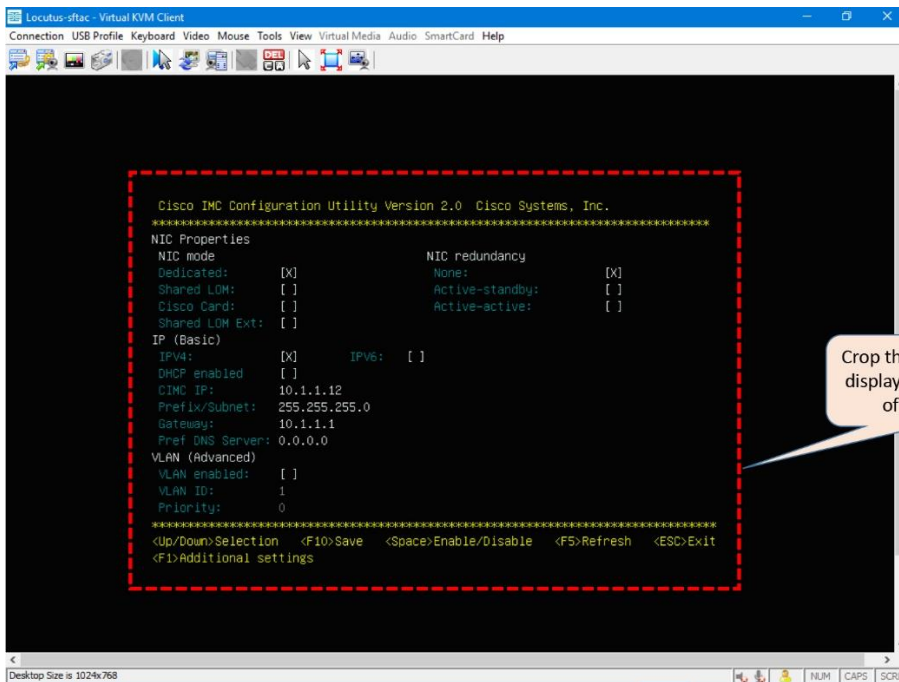


Figure 4-4. *The CIMC Configuration Utility*

One of the useful features of the CIMC is the Keyboard, Video, and Mouse (KVM) console. Using the KVM console, you can directly connect to the console of an FMC, without the need for a dedicated KVM based hardware.

[Figure 4-5](#) shows the GUI of a CIMC. To access the GUI, use the default username/password (admin/password), or reset it from the Cisco Configuration Utility.

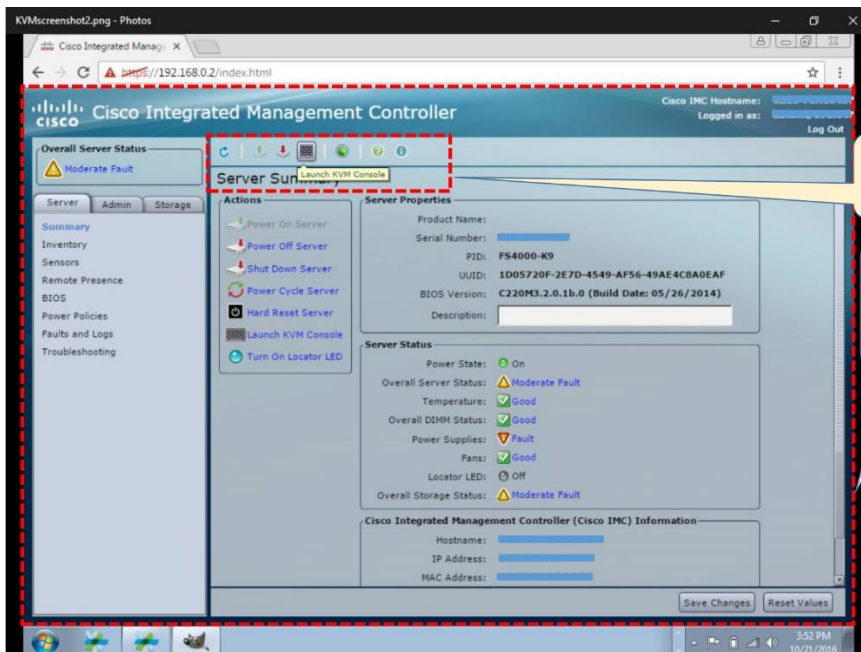


Figure 4-5. *Launch KVM Console Option in the GUI of a CIMC*

Internal USB Storage for the System_Restore Image

The UCS C-Series server has an internal USB storage which is used to store an image for the system restoration. You can select the System_Restore image from the LILO Boot Menu.

[Figure 4-6](#) shows the System_Restore image in the LILO Boot Menu.

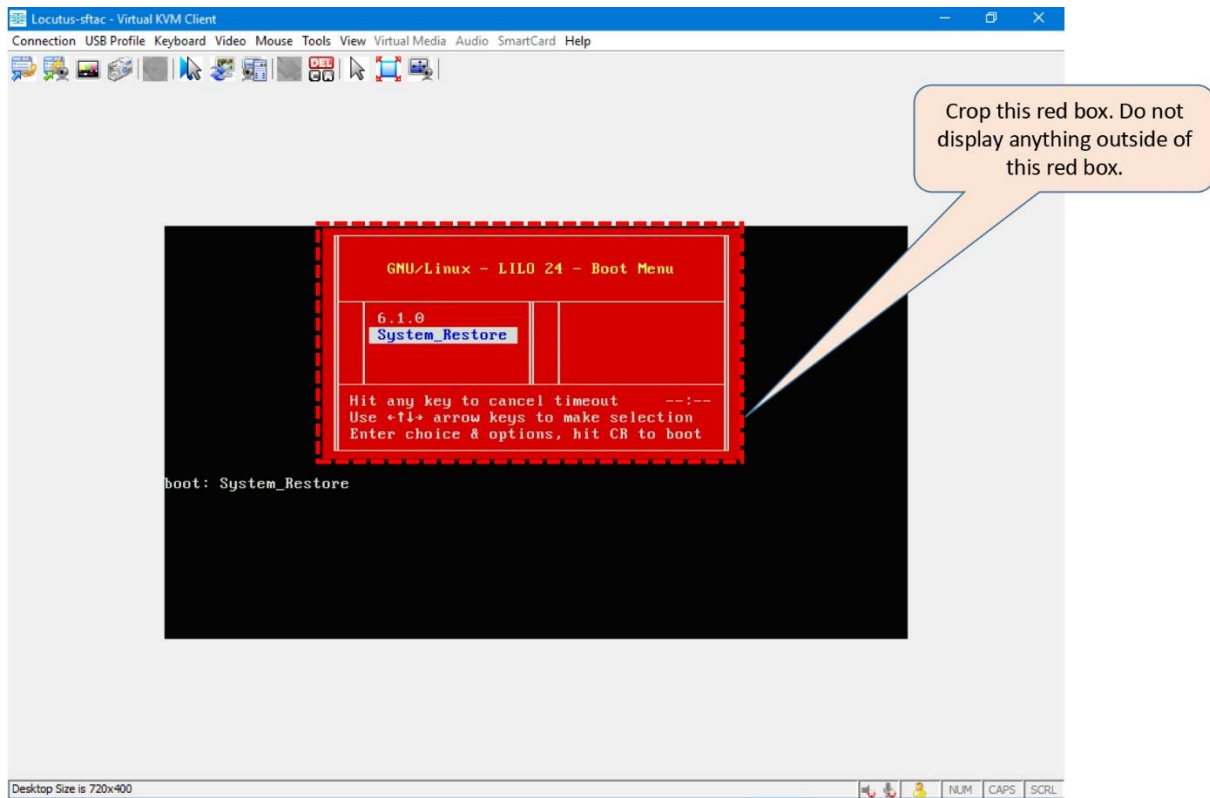


Figure 4-6. Selection of the System_Restore Image in the LILO Boot Menu

User Interfaces

After you power on any computer system, you need an interface that allows you to interact with the system. An FMC is not an exception. In fact, an FMC has many different types of user interfaces, depending on what you want to do. For example, Graphical User Interface (GUI) is used to apply security policy and monitor events, Command Line Interface (CLI) is used for advanced troubleshooting, and Text-based User Interface (TUI) is used to configure any specific components when the actual operating system is not loaded or installed.

[Figure 4-7](#) illustrates different types of user interfaces of an FMC. Each dark box represents a unique type of interface.

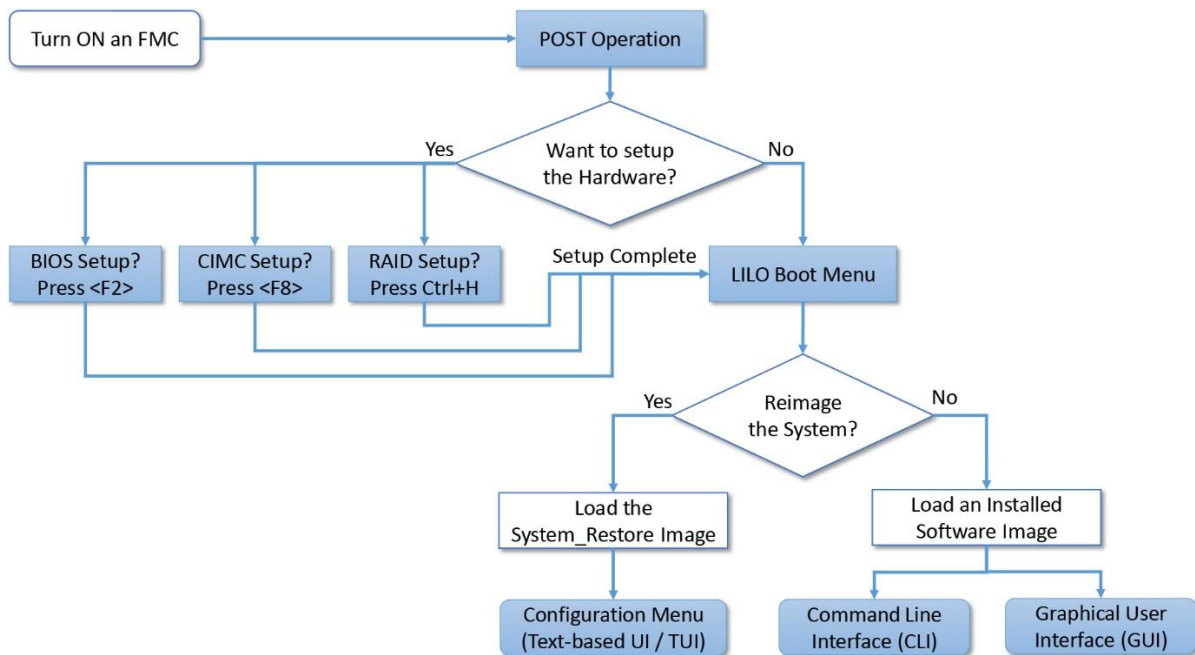


Figure 4-7. *Different Types of User Interfaces in an FMC*

Best Practices

This section discusses some of the best practices that you should follow when you reimage an FMC to 6.1. It also provides you with a list of items that you should verify on an FMC hardware after a reimage is complete.

Pre-Installation

If your Firepower Threat Defense (FTD) System in running Version 6.1, the Firepower Management Center (FMC) must be running Version 6.1 or greater. Consider the following best practices when you reimage a Firepower Management Center to 6.1:

- 1.** Prior to a maintenance window for a reimage or a fresh installation, make sure you are able to access the cisco.com website, and entitled to download any necessary software. If you are unable to access, register for a Cisco account. If the self-registration process does not allow you to download a desired software, Contact your Cisco Channel Partner or the Cisco Technical Assistance Center (TAC) for further assistance.
- 2.** Depending on the appliance model, a fresh installation or system restoration process may take about an hour. However, you should plan for additional time to fulfill any prerequisites.
- 3.** Do not rename any files after you download from the cisco.com. For FMC 2000 and FMC 4000 models, the name of the ISO file is Sourcefire_Defense_Center_S3-6.1.0-330-Restore.iso.

4. After you download any software from the Cisco.com, always verify the MD5 or SHA512 checksum of the files you have downloaded. It confirms that the file is not corrupt, or not modified during download.

Figure 4-8 illustrates how the MD5 and SHA512 checksum values are displayed at cisco.com when you hover your mouse over a filename.

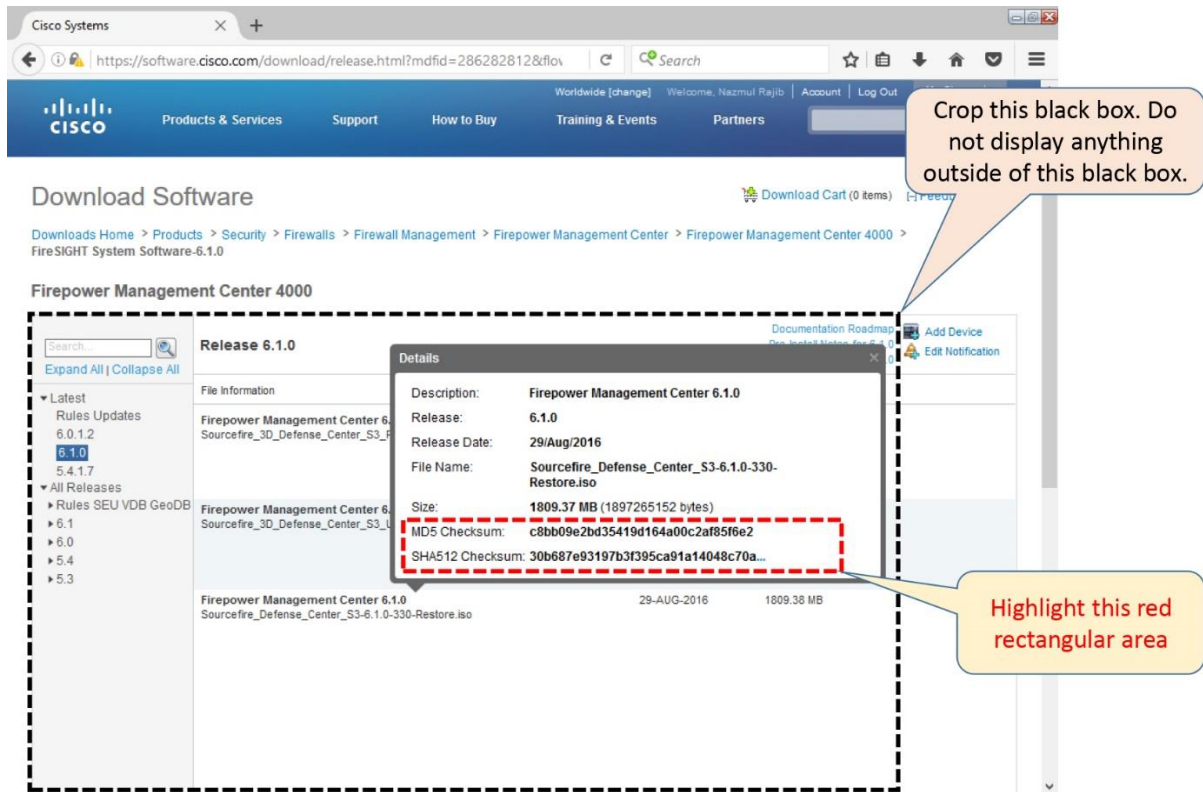


Figure 4-8. Checksum Values of an ISO Image File is Displayed in a Pop-up Box

5. Before you reimagine a currently operational FMC hardware, or redeploy a virtual machine, you should prepare a backup plan. Take a backup of the existing events and configurations. During a backup, take a note of the detail software versions and hardware models of an FMC, because they must match during restore. After a backup, make sure you copy the backup file to an external storage, because a reimagine erases backup files along with any other data on an FMC.

Figure 4-9 illustrates the backup management page of an FMC. It is located at **System > Tools > Backup/Restore**.

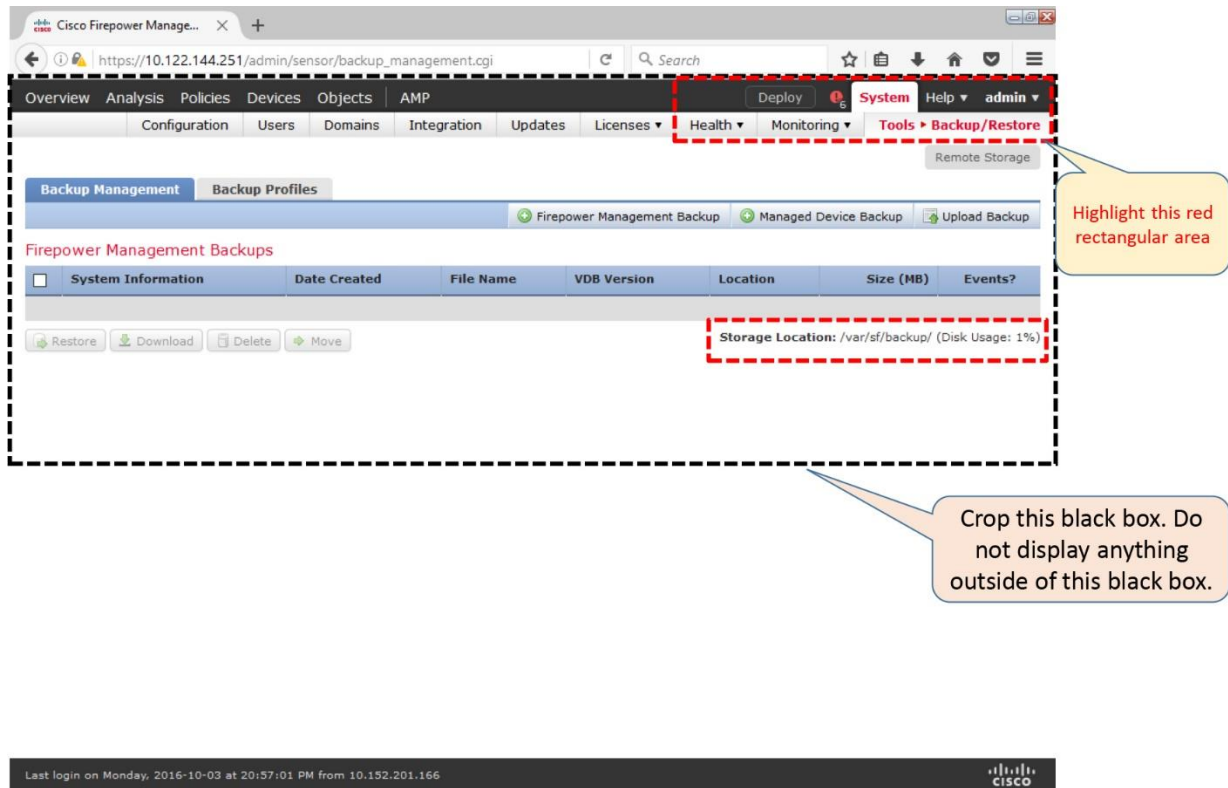


Figure 4-9. *The Backup Management Page*

6. Additionally, you can utilize the Import/Export tool to copy any policies running on your FMC. During an import, the versions of a restored system must match with the FMC from where any policies are originally exported. Therefore, when you export, you must remember the software and Rule Update version information of the original FMC.

[Figure 4-10](#) exhibits the navigations to the Import/Export page. It is located at **System > Tools > Import/Export**.

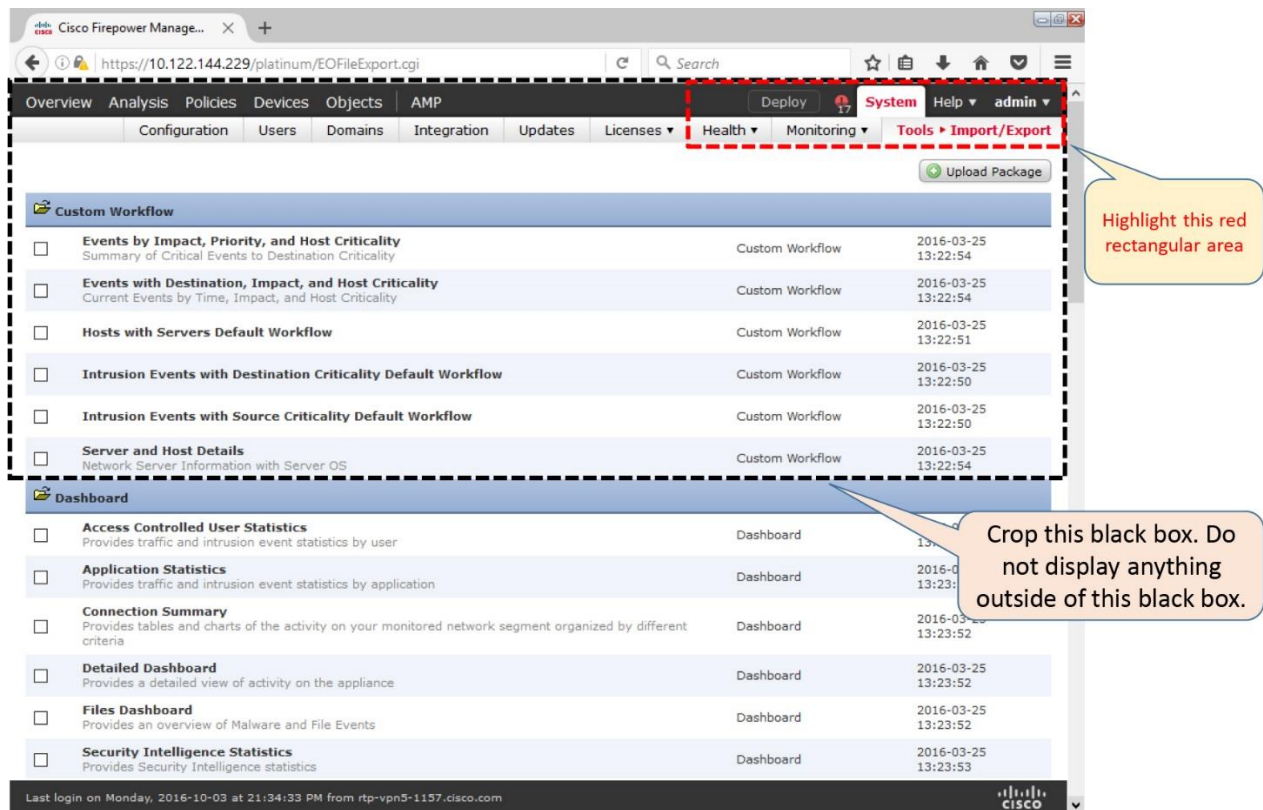


Figure 4-10. *The Import/Export Page*

7. If your FMC was previously licensed through the Cisco Smart Software Manager, deregister the FMC gracefully from the user interface of the FMC. Otherwise, upon a periodic communication attempt, the Cisco License Authority can trigger an alert for the Out-of-Compliance state.

[Figure 4-11](#) shows a red octagonal icon in the Smart License Status page which is located at **System > Licenses > Smart Licenses**. This icon deregisters an FMC from the Smart License cloud.

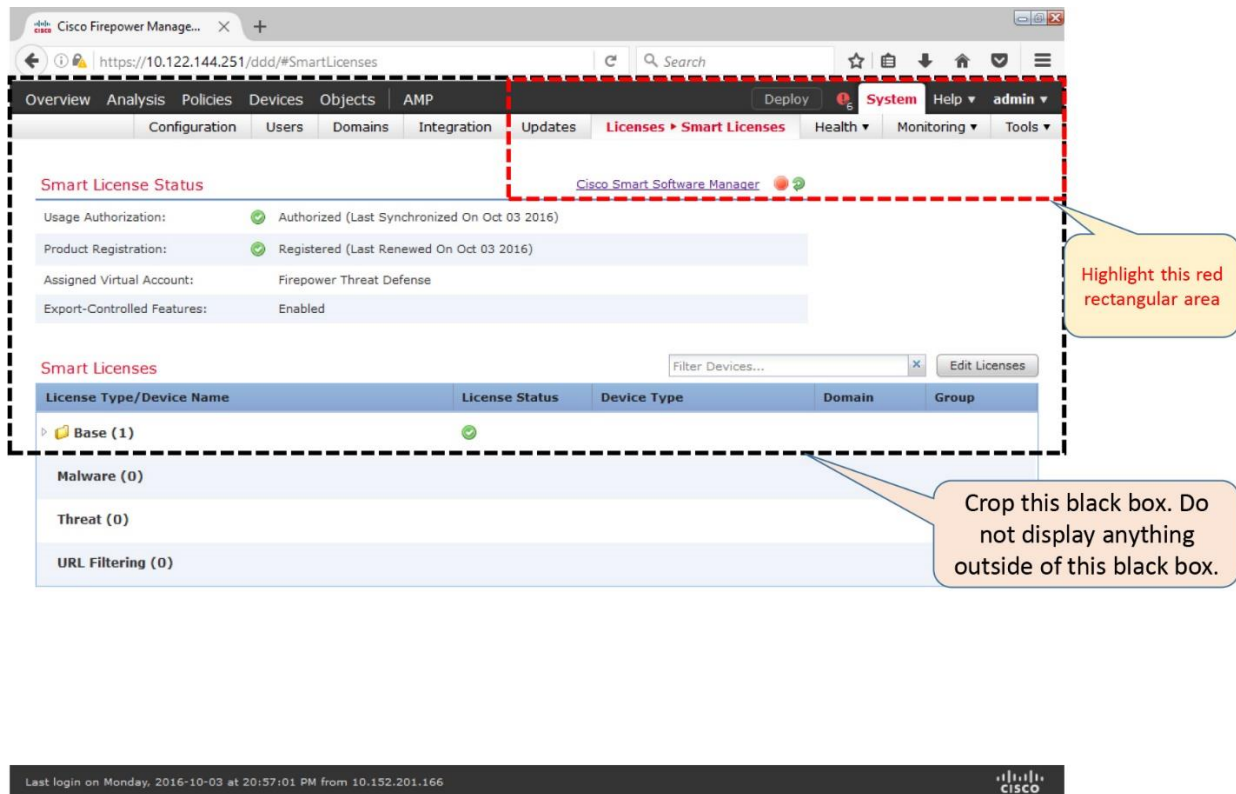


Figure 4-11. *The Smart License Management Page*

8. Never power off, shutdown, or reboot an FMC when a reimage is in progress. A login prompt appears after all of the reimage processes are complete.
9. Read the release notes to determine any known issues, any special requirements or instructions before you begin a reimage or system restoration.

Post-Installation

Once the software is installed, take some time to perform the following tests. It will help you to determine any hardware issues before you deploy an FMC in a production environment, hence avoid any potential downtime.

1. Determine the status of the RAID battery.
2. Verify the status of the Power Supply Units.
3. Identify the status of the fans.
4. Check for any errors with the Intelligent Platform Management Interface (IPMI).
5. Access the GUI. You must use a supported browser. The list of supported browsers for a particular version are available in the release notes.

Tip

To learn the commands and tools that would allow you to perform the above tests, read the Verification and Troubleshooting Tools section of this chapter.

Configuration

In this section, you will learn the detail processes of restoring or reimaging a Firepower Management Center.

Prerequisites

You must fulfill the following requirements before you begin a new installation:

- 1.** Upload the necessary software image into an HTTP server from where an FMC downloads it during a reimage. You can also use an SCP or FTP server in lieu of an HTTP server. However, you may find an HTTP server is easier to setup and to host files.
- 2.** If you choose to use an IP based KVM (Keyboard, Video, and Mouse) console to connect to the FMC you want to reimage, do not use any KVM with a USB storage, because the FMC may assume the USB storage as a boot device. Please read the official Hardware Installation Guide to find any hardware specific limitation.

Tip

Although you can, but you do not need to obtain a dedicated KVM switch for your FMC, because the CIMC of an FMC provides a built-in KVM console functionality. Read the CIMC section of this chapter to learn more.

- 3.** For reimage purpose, if you want to connect your computer directly to the management interface (eth0) of an FMC with an RJ-45 cable, make sure the computer is disconnected from the internet, and has the following network settings:

- IP address: 192.168.45.2
- Subnet/Netmask: 255.255.255.0
- Default Gateway: 192.168.45.1

Tip

This step assumes that you have downloaded any necessary software from cisco.com before you disconnect your computer from the internet.

- 4.** You need to be able to access to the System_Restore image of the FMC to perform a reimage. If the image is missing in the LILO Boot Menu, or the LILO Boot Menu itself does not appear, you will not be able to begin a reimage. In order to access the System_Restore image, follow the steps below:

Step 1. Reboot the FMC.

Step 2. During the POST operation, press the <F6> key to enter the Boot Menu.

Step 3. When the boot selection window appears, select HV. The hypervisor (HV) partition stores the System_Restore image. If you are running an older FMC model, you may see a different option, such as, USB DISK MODULE.

[Figure 4-12](#) shows hypervisor (HV) as an option in the boot menu of an FMC. You can enter this Boot Menu by pressing <F6> key during the POST operation.

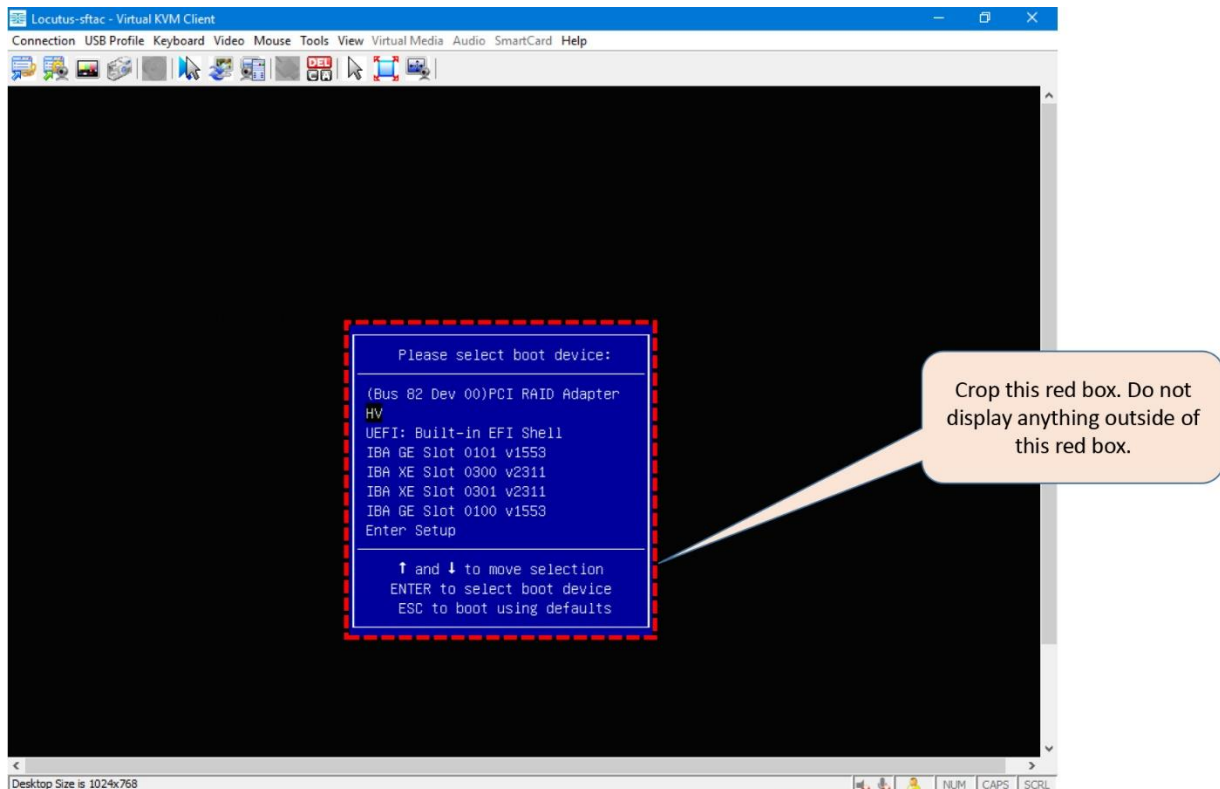


Figure 4-12. Hypervisor (HV) — The Internal Storage Option in the Boot Menu

Step 4. Press Enter key to boot the FMC with HV. The FMC should now load the System_Restore image.

Configuration Steps

In order to reimage or restore an FMC with a Firepower software image, you must complete the following key steps:

Step 1. Load the System_Restore image

Step 2. Configure the Network Settings

Step 3. Choose a Transport Protocol

Step 4. Download and Mount ISO

Step 5. Run the Install

Step 6. Reboot the System to Initialize

[Figure 4-13](#) illustrates the steps to restore or reimage an FMC with a Firepower software release. You can learn more about these steps in the next few sections of this chapter.

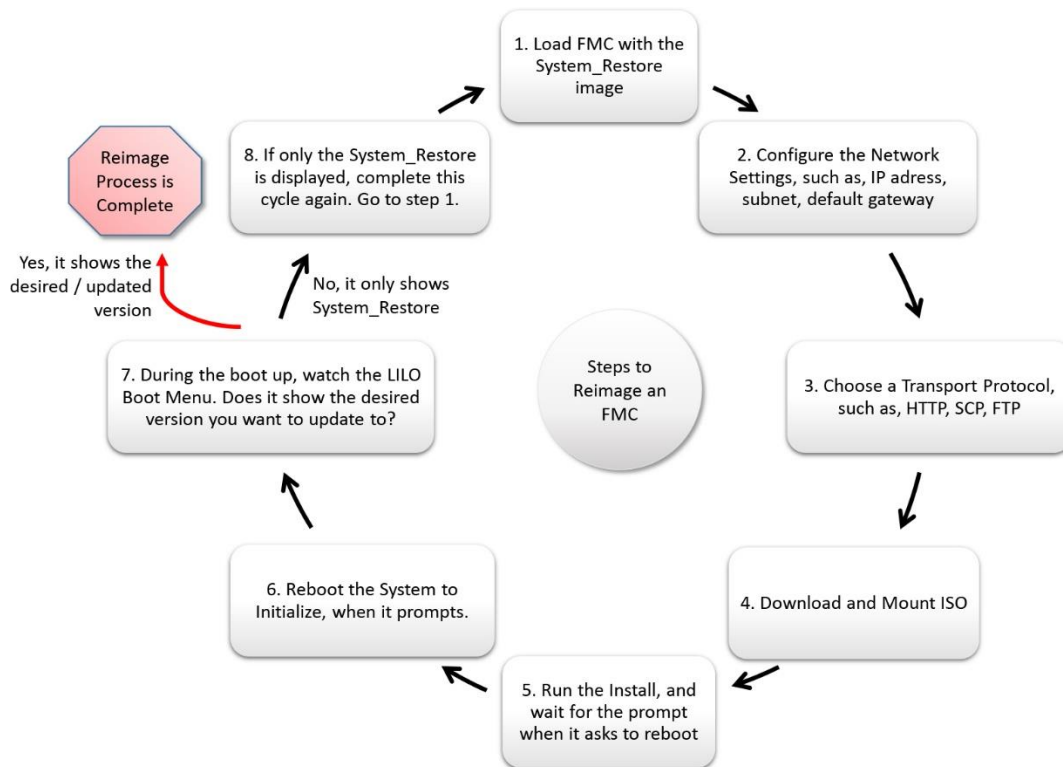


Figure 4-13. *The Process to Restore an FMC to a Factory Default Software*

Step 1. Load the System_Restore Image

1.1 Download an appropriate ISO image for your FMC hardware model and store it in a server from where the FMC will download the image. The example in this chapter uses HTTP server.

1.2 Turn on the FMC. If the FMC is already running, reboot it.

[Example 4-1](#) shows that entering a **reboot** command with **sudo** (root privilege) prompts for the root password.

Example 4-1 *Command to Reboot an FMC from the CLI*

```
admin@FMC4000:~$sudo reboot
```

We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:

- #1) Respect the privacy of others.
- #2) Think before you type.
- #3) With great power comes great responsibility.

Password:

```
The system is going down for reboot NOW!  
INIT: Switching to runlevel: 6  
INIT: Sending processes the TERM signal  
Stopping Sourcefire Defense Center 4000.....ok  
.  
.  
.  
<command output>
```

1.3 During the initial boot up, BIOS displays several options, such as, setup, boot menu, diagnostic, etc. Unless you want to configure any hardware component, do not press any key. The system will display a red color **LILO Boot Menu** momentarily.

[Figure 4-14](#) shows the System_Restore image is selected as the boot option. If you would not select the System_Restore image within three seconds, the system, by default, would load the pre-installed software image 6.1.0.

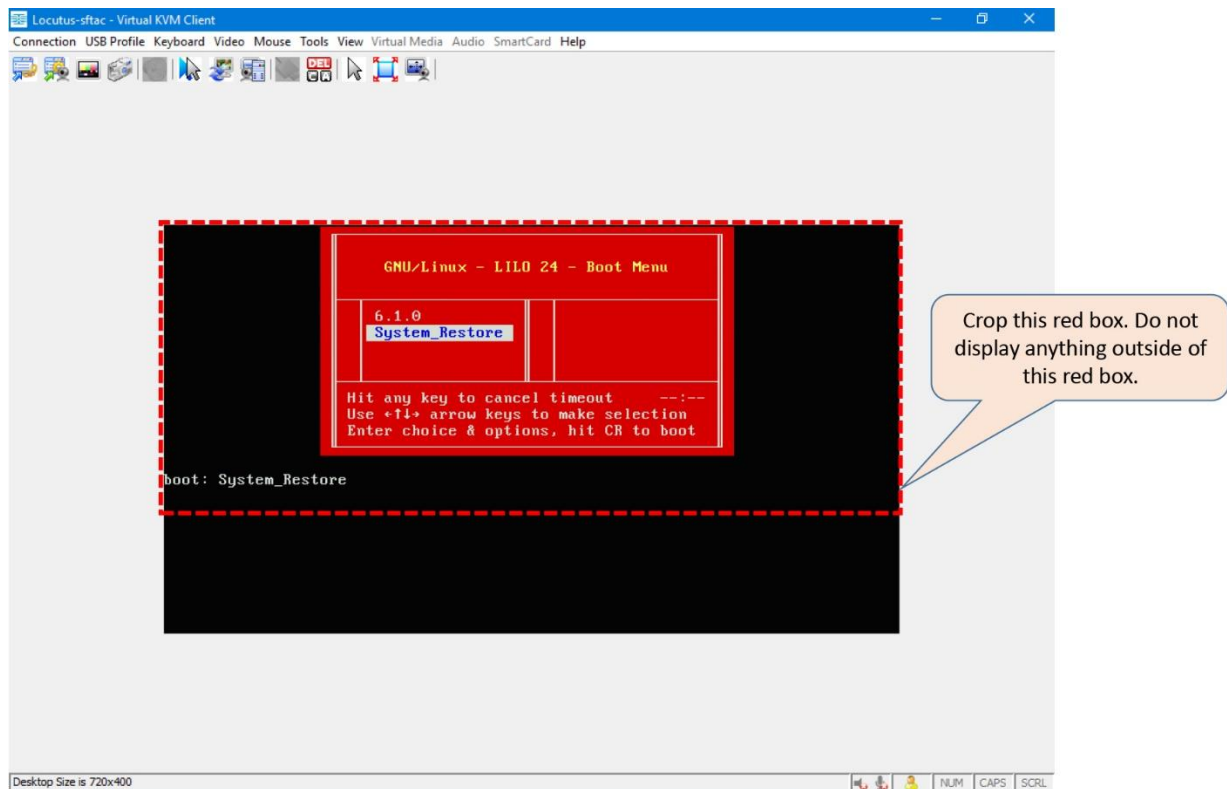


Figure 4-14. *The LILLO Boot Menu with the System_Restore Image Selection*

1.4 Once the **LILLO Boot Menu** appears, select the **System_Restore** option using an arrow key, and press the **Enter** key.

1.5 Choose an appropriate display mode to boot.

[Example 4-2](#) shows the welcome message for the Sourcefire Linux Operating system. This is what you would see after the System_Restore is loaded. The example in this chapter uses the option ‘0’ — Load with standard console — as the display mode. Select the option ‘0’ for a keyboard and monitor connection. The option ‘1’ is used for a serial, Serial over LAN (SOL), or Lights Out Management (LOM) connections.

Example 4-2 Choosing a Console Type

```
boot: System_Restore
Loading System_Restore

SYSLINUX 3.35 2007-01-28 EBIOS Copyright (C) 1994-2007 H. Peter Anvin

Welcome to the Sourcefire Linux Operating System

0. Load with standard console
1. Load with serial console

Please select a display mode to boot. If no option is selected after
a timeout of 30 seconds, the default will be display mode 0 (Load with
standard console). Press any key to cancel the timeout

boot: 0
```

1.6 A Text-based User Interface (TUI) starts, and shows a copyright notice. Select **OK** and press the **Enter** key to continue. The **Cisco Firepower Appliance Configuration Menu** appears.

[Figure 4-15](#) shows a TUI for the Cisco Firepower Appliance Configuration Menu.

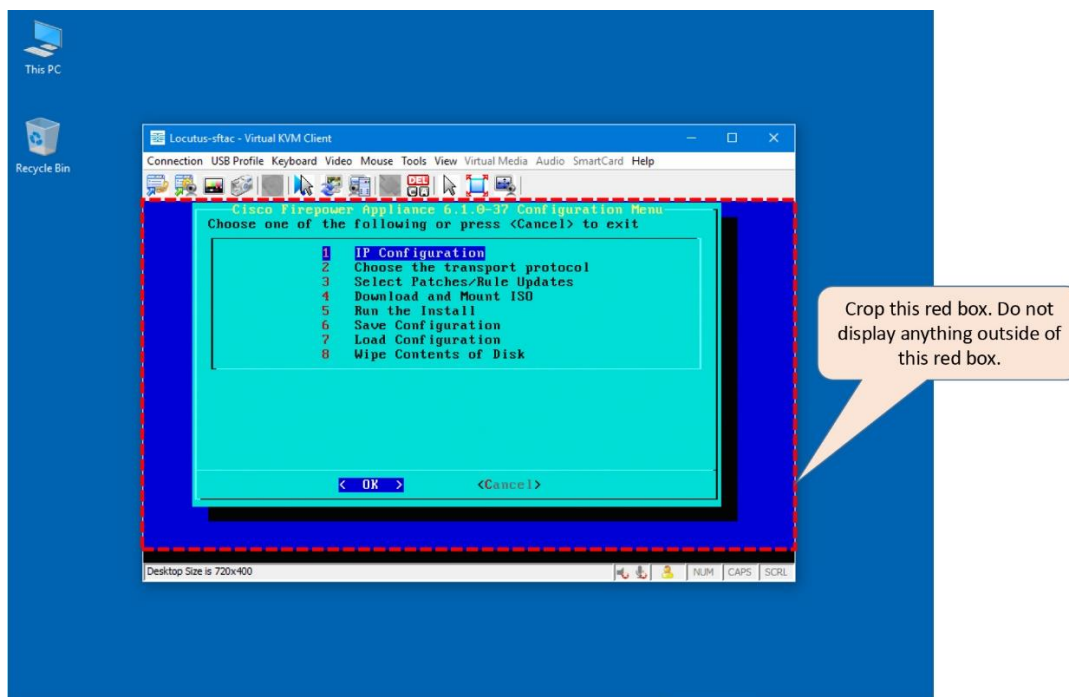


Figure 4-15. *The Cisco Firepower Appliance Configuration Menu*

Step 2. Configure the Network Settings

2.1 Select **IP Configuration**, and press the **Enter** key. The **Pick Device** window appears.

[Figure 4-16](#) shows the eth0 interface is selected as the management interface.

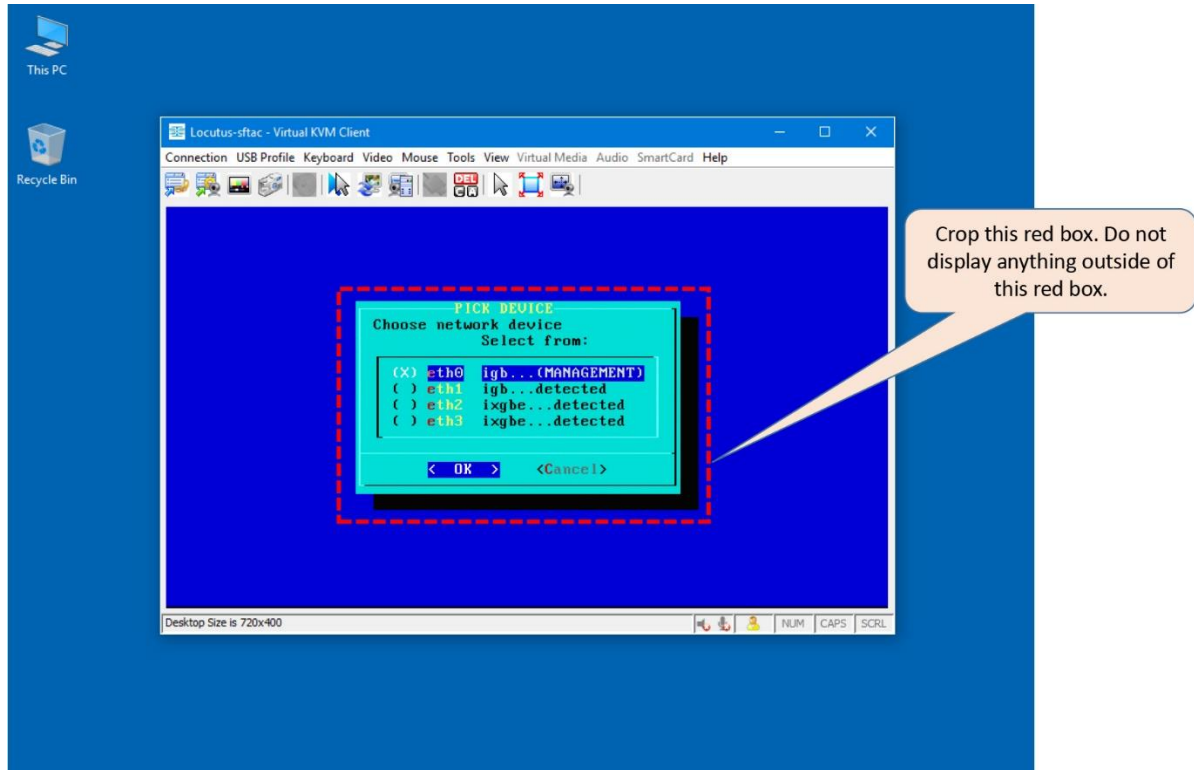


Figure 4-16. Selection of a Management Interface

2.2 Use the spacebar to select **eth0** as the management interface, and press ENTER. The **IP Configuration** window appears.

2.3 Select IP information, such as, **IPv4** vs **IPv6**, **Static** vs **DHCP**, etc. The example in this chapter uses IPv4 and Static options.

2.4 Enter an IP address, netmask, and default gateway for the FMC. At the end of the IP configurations, when a verification window appears. Press the **Enter** key to return to the main Configuration Menu.

Step 3. Choose a Transport Protocol

3.1 Enter the **Choose the Transport Protocol** option from the main Configuration Menu.

[Figure 4-17](#) shows the selection of the **Choose the Transport Protocol** option which defines a file transfer method.

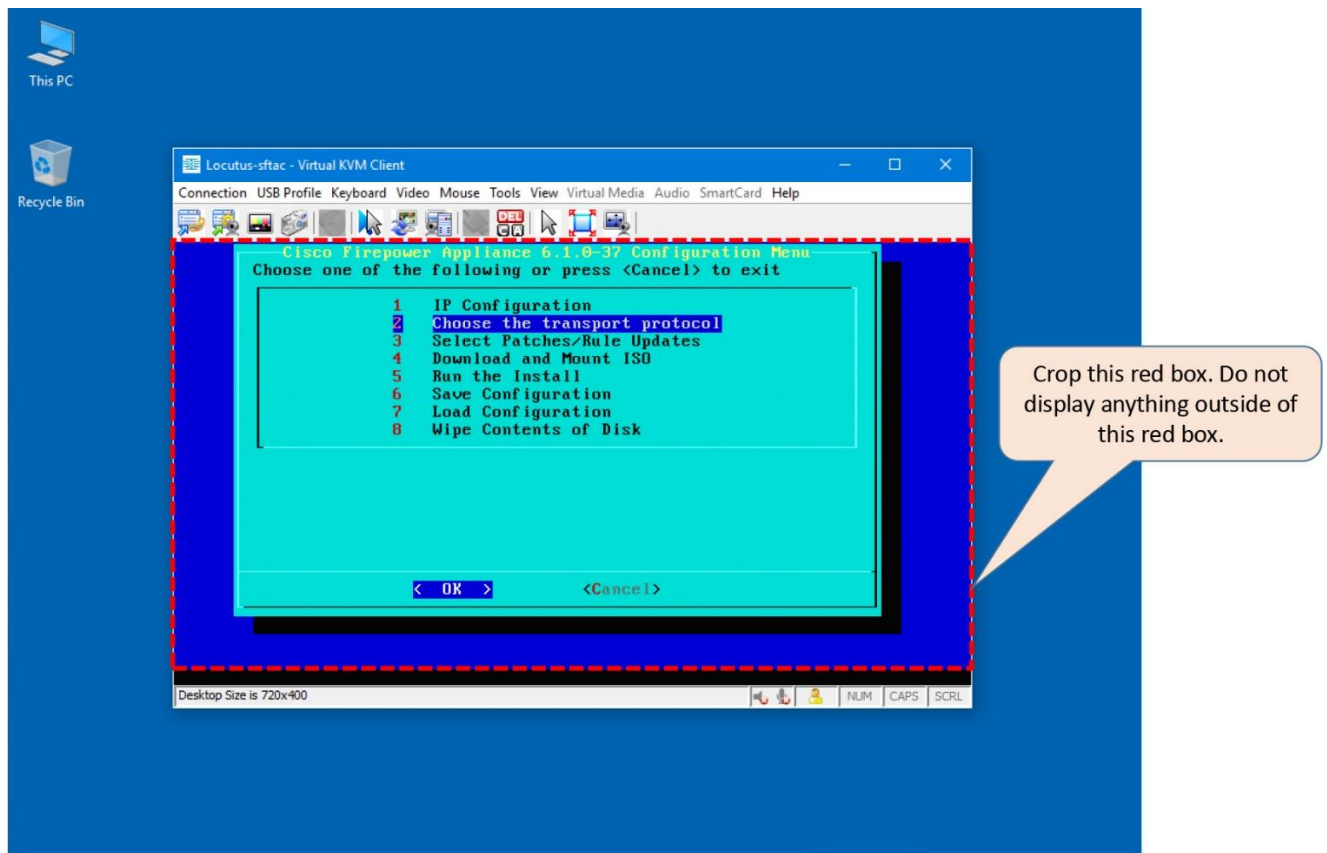


Figure 4-17. *The Choose the Transport Protocol Option is Selected*

3.2 Select **HTTP** as the transport protocol. You could select FTP or SCP as well, however, you may find an HTTP server is easier to build.

[Figure 4-18](#) shows the HTTP protocol is picked to transfer an ISO file to the FMC.

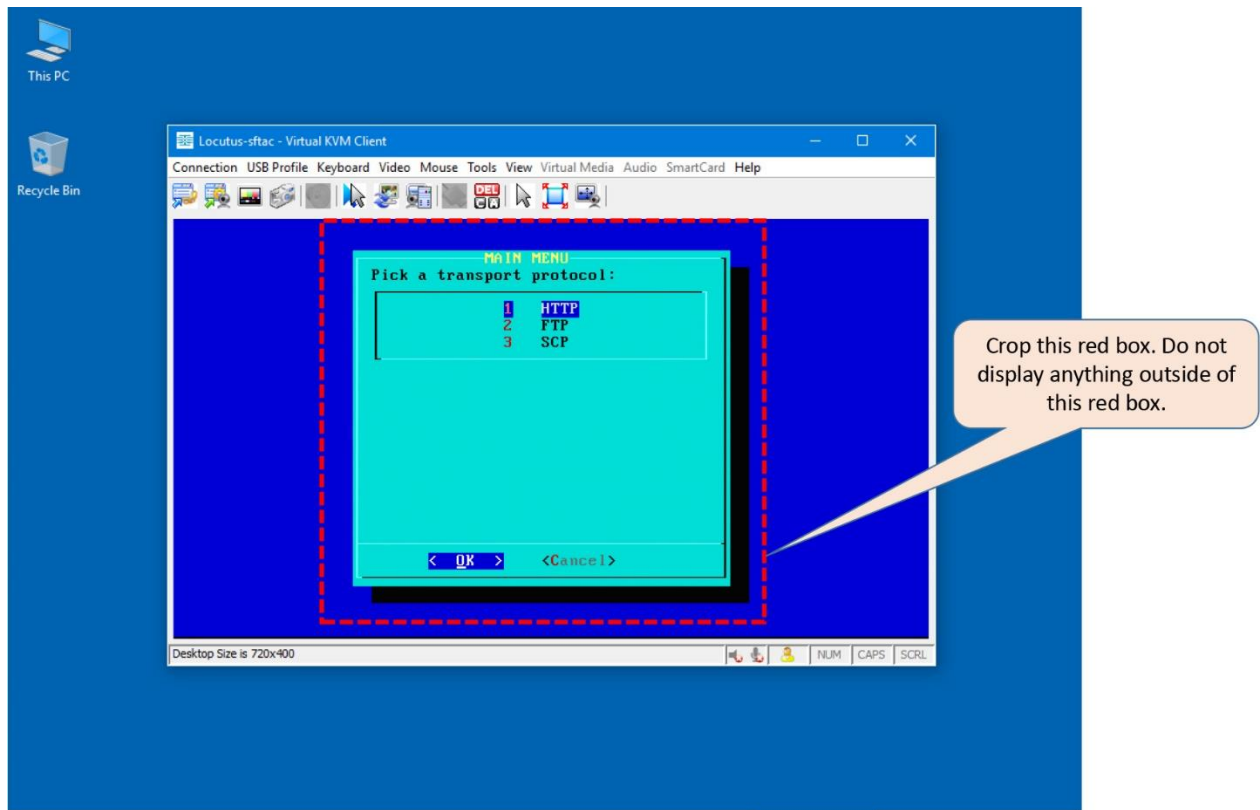


Figure 4-18. *Three Available Protocols for an ISO File Transfer*

3.3 Input the IP address of the HTTP server and press the **Enter** key.

3.4 Enter the path on the HTTP server and press the **Enter** key. Keep it blank if you stored the ISO file in the default directory of your web server.

3.5 Use the Spacebar to select an ISO that you want to download and load into your FMC.

[Figure 4-19](#) shows two ISO images. Both images are downloaded from the cisco.com to the HTTP server. Select the Sourcefire_Defense_Center_S3-6.1.0-330-Restore.iso image for an FMC hardware.

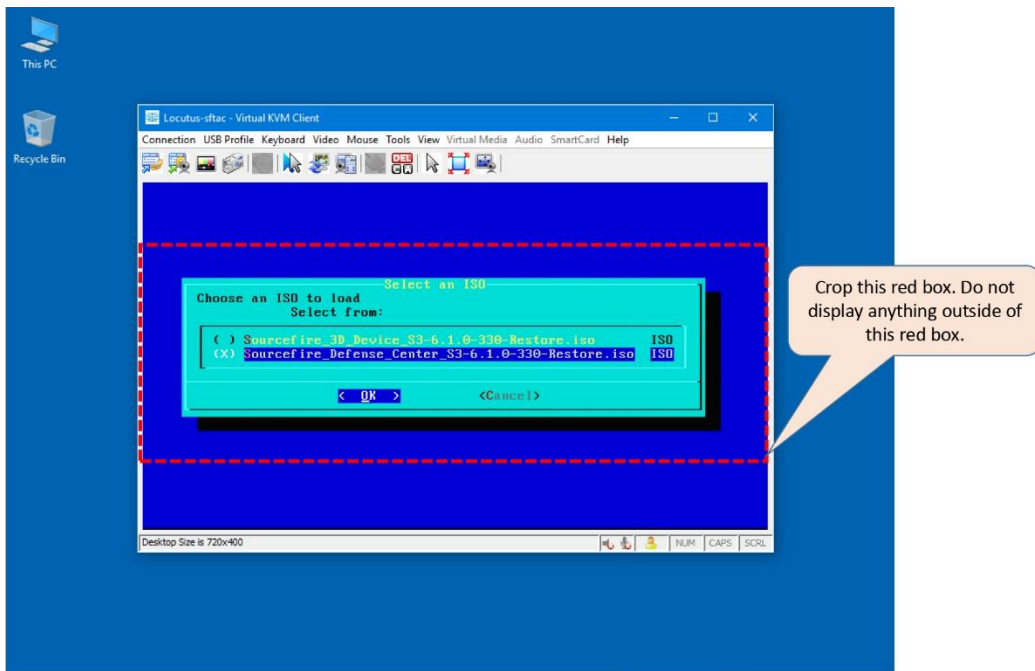


Figure 4-19. Selection of an ISO Image During a Reimage Process

3.6 Select **OK** and press the **Enter** key. A window prompts to confirm the HTTP Configuration. Select **Yes** if everything looks good. You will be returned to the main Configuration Menu.

Step 4. Download and Mount ISO

4.1 In the Main Configuration Menu, select the **Download and Mount ISO** option.

[Figure 4-20](#) shows the selection of the **Download and Mount ISO** option where a disk is repartitioned.

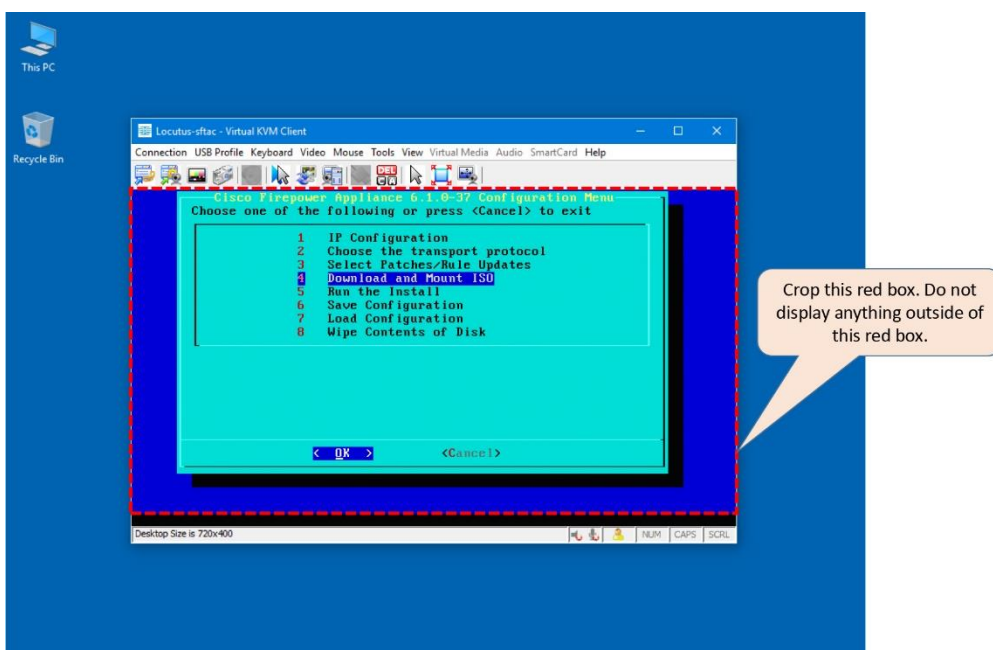


Figure 4-20. *The Download and Mount ISO Option is Selected*

4.2 A message appears to warn you about the consequence — this step destroys all existing data.

[Figure 4-21](#) shows the beginning of a repartition followed by a warning message for data loss. The message appears after you enter the **Download and Mount ISO** option.

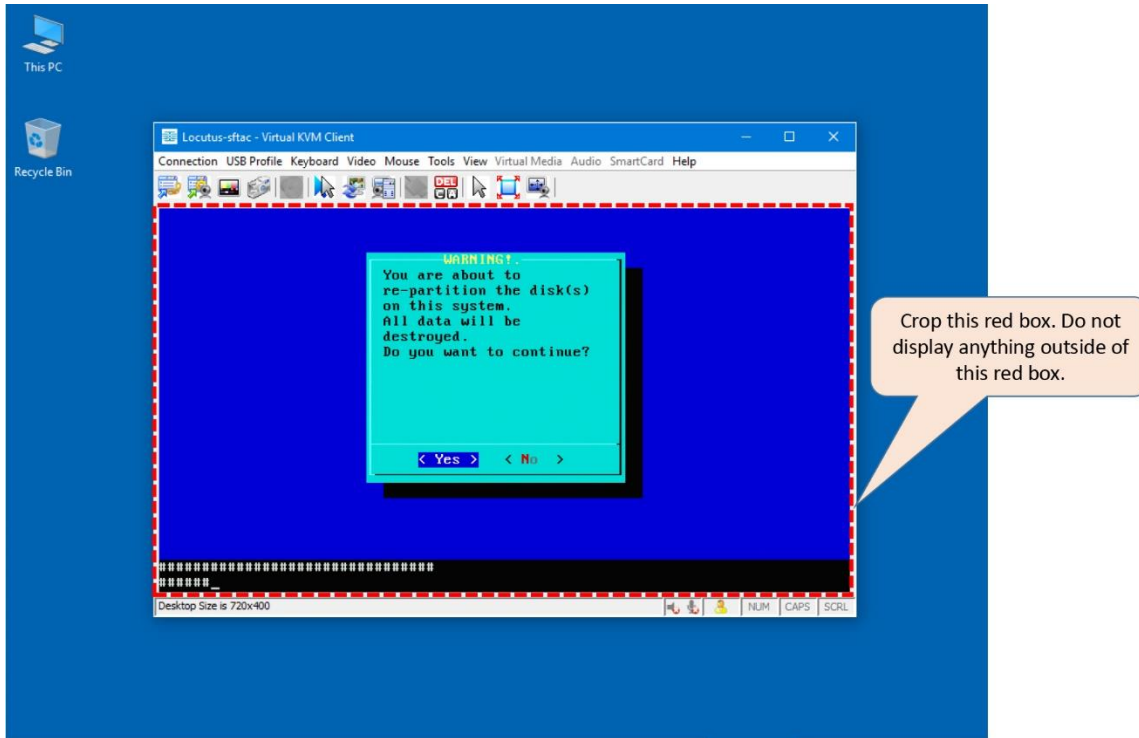


Figure 4-21. *The Repartition Process is in Progress*

4.3 Press the **Enter** key to continue. It downloads the ISO file from the HTTP server. After the download completes, the main Configuration Menu reappears.

Step 5. Run the Install

Select the **Run the Install** option on the main Configuration Menu. Depending on the state of the internal USB storage (System_restore image), an output at this stage could be one of the following:

- A prompt to press Enter to restart, or
- A prompt to confirm the restore (yes/no)

[Figure 4-22](#) shows the selection of the **Run the Install** on the Configuration Menu. After this selection, an FMC begins the installation process.

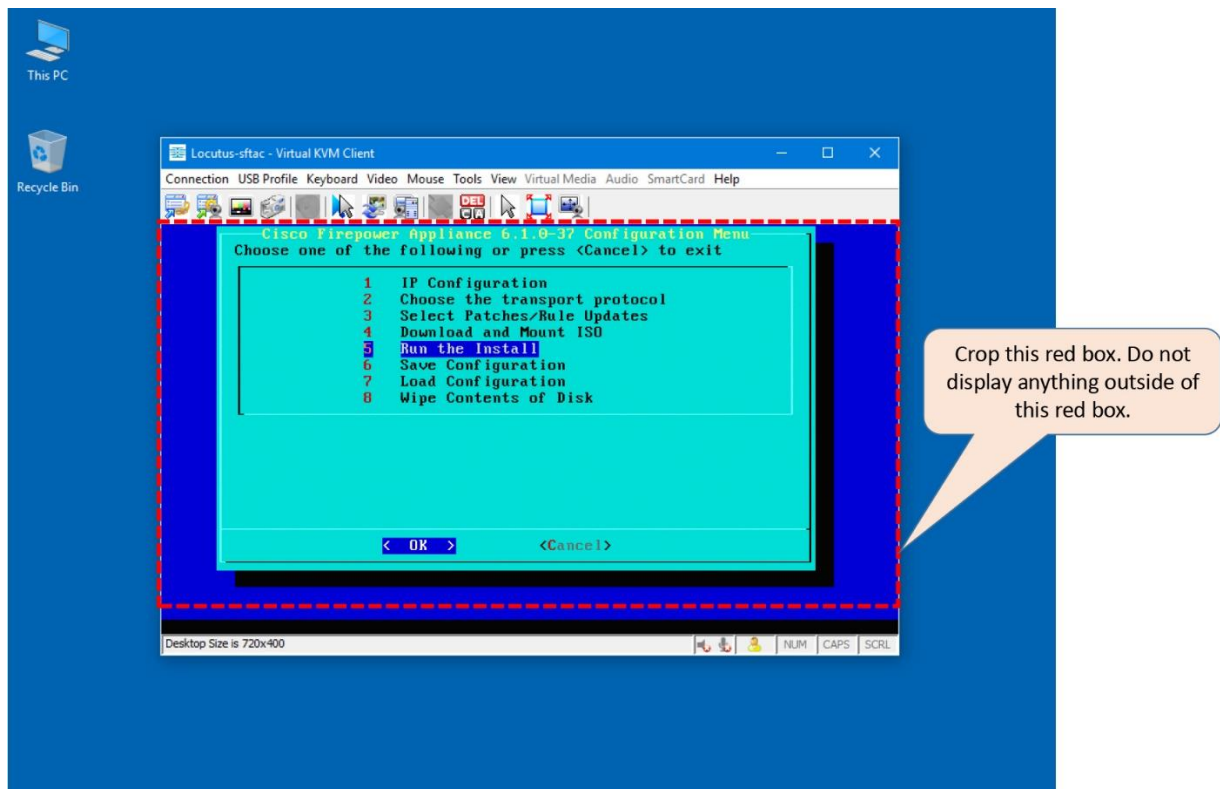


Figure 4-22. *The Run the Install Option is Selected*

Prompt to Restart

If the system does not ask for your confirmation to restore, instead it prompts you to press the **Enter** key to reboot the FMC from the internal USB, it indicates that you have just imaged the internal storage, not the hard drive, with the latest version of the System_Restore software.

[Example 4-3](#) shows a confirmation message to indicate that the USB device is imaged, not the hard drive. It also instructs to reboot the FMC from the USB device to continue installation.

Example 4-3 *Confirmation Message for a Successful Image of the Internal USB*

```
Restore CD      Sourcefire Fire Linux OS 6.1.0-37 x86_64
                Sourcefire Defense Center S3 6.1.0-330
```

```
Checking Hardware
```

```
The USB device was successfully imaged. Reboot from the USB device to
continue installation...
```

```
#####
#####
```

```
The system will restart after you press enter.
```

This happens when an FMC has been running an older version than the version you are trying to reimage to. If the internal storage of an FMC does not have a System_Restore image from the same software version you are trying to reimage to, the FMC reimages the internal storage at first. Then it reloads the FMC with the upgraded System_Restore image. Select **System_Restore**, and repeat all of the steps one more time. For example, re-download and remount ISO from your server, rerun the install on FMC, etc.

Prompt to Restore

If the system prompts for your confirmation to restore, type **'yes'** and press the **Enter** key to continue.

5.1 After you press the **Enter** key, let the system know if you want to preserve the existing license and network settings. If you want to redeploy the FMC in the exact same network, and want to reuse the previously used license and network settings, enter **'no'**. If you plan to deploy the FMC in a completely new environment, and want to wipe out the previous settings, enter **'yes'**.

5.2 Enter **'yes'** when the final confirmation message appears. It begins the software installation.

Caution

If you choose to delete the previous license and network settings, make sure you have a copy of the licenses, or you are able to regenerate the licenses from the cisco.com.

[Example 4-4](#) shows the questionnaire before the installation begins. The system warns you for the permanent data loss and provides you an option to keep the already configured license and network.

Example 4-4 Questionnaire Before an Installation Begins

```
Restore CD      Sourcefire Fire Linux OS 6.1.0-37 x86_64
                Sourcefire Defense Center S3 6.1.0-330

Checking Hardware

####
This CD will restore your Defense Center S3
to its original factory state. All data will be destroyed
on the appliance.

Restore the system? (yes/no): yes

During the restore process, the license file and basic
network settings are preserved. These files can also be
reset to factory settings

Delete license and network settings? (yes/no): no
*****
THIS IS YOUR FINAL WARNING. ANSWERING YES WILL REMOVE ALL FILES
FROM THIS DEFENSE CENTER S3.
*****
```


Are you sure? (yes/no): **yes**

[Example 4-5](#) demonstrates the beginning of an installation. Do not reboot or power off a system while the installation is in progress.

Example 4-5 *The Software Installation Has Begun*

```
Restore CD      Sourcefire Fire Linux OS 6.1.0-37 x86_64
                Sourcefire Defense Center S3 6.1.0-330
```

```
(1) Preparing Disk
```

```
#####
```

```
(2) Installing System
```

```
####
```

5.3 The system confirms you when an installation is complete, and prompts you to reboot. Press the **Enter** key to reboot the system.

Step 6. Initialize the System

6.1 After the reboot, the FMC should display the LILO Boot Menu, and load the 6.1.0 image automatically.

[Figure 4-23](#) shows the Firepower Software Version 6.1.0 which is just installed is loaded automatically after a 3-second timeout.

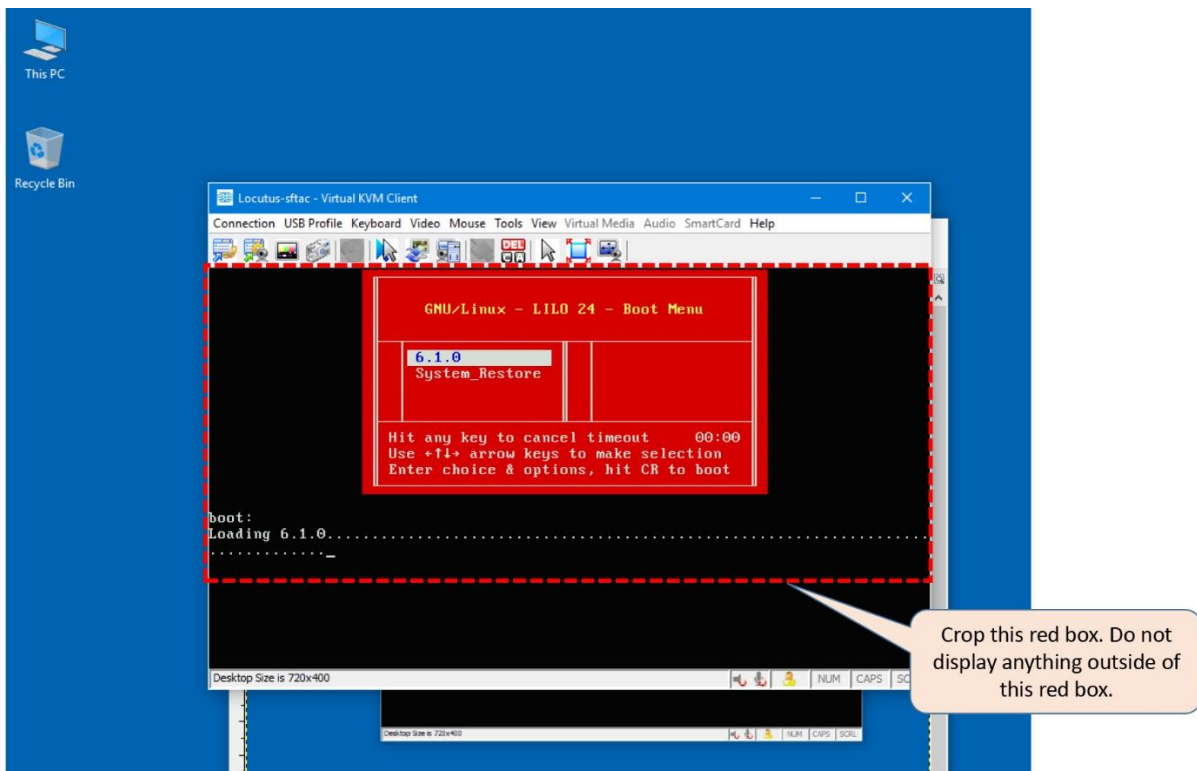


Figure 4-23. FMC Loads the Software Version 6.1.0

Tips

If the LILO does not show an option for Version 6.1.0, and only shows an entry for System_Restore, reload the FMC with the upgraded System_Restore image, and repeat all of the prior steps one more time.

6.2 The system begins initialization automatically. This process takes some time. Please be patient.

Warning

Do not reboot or power off a system while the initialization is in progress.

[Example 4-6](#) shows the executions of many scripts during the initialization process. The process may take more than 30 minutes time to complete.

Example 4-6 *Initialization of the Firepower Software*

```
<command output>
.
.
.
***** Attention *****

    Initializing the configuration database. Depending on available
    system resources (CPU, memory, and disk), this may take 30 minutes
    or more to complete.

***** Attention *****

Executing S09database-init [ OK ]
Executing S10_001_install_symmetric.pl [ OK ]
Executing S11database-populate [ OK ]
<command output>
.
.
.
<command output>
Executing S50install-remediation-modules [ OK ]
Executing S51install_health_policy.pl [ OK ]
Executing S52install_system_policy.pl [ OK ]
Executing S53change_reconciliation_baseline.pl [ OK ]
Executing S53createcsds.pl [ OK ]
Executing S85patch_history-init [ OK ]
Executing S90banner-init [ OK ]
Executing S95copy-crontab [ OK ]
Executing S96grow_var.sh [ OK ]
Executing S96install_sf_whitelist [ OK ]
Executing S96install_vmware_tools.pl [ OK ]

***** Attention *****

    Initializing the system's localization settings. Depending on
    available
    system resources (CPU, memory, and disk), this may take 10 minutes
    or more to complete.
```

```
***** Attention *****
Executing S96localize-templates           [ OK ]
Executing S96ovf-data.pl                 [ OK ]
Executing S97compress-client-resources   [ OK ]
Executing S97create_platinum_forms.pl    [ OK ]
.
.
.
<command output>
```

6.3 Once complete, the Firepower login prompt appears. Enter the default username and password to login to the Command Line Interface (CLI).

[Example 4-7](#) shows the completion of the Firepower software initialization. Once complete, you can enter the CLI using the default credentials — username **admin** and password **Admin123**.

Example 4-7 *Login to the CLI of an FMC After the Initialization is Complete*

```
Cisco Firepower Management Center 4000 v6.1.0 (build 330)
Sep 28 23:20:53 firepower SF-IMS[5124]: [5124] init script:system [INFO]
pmmon Starting
the Process Manager...
Sep 28 23:20:53 firepower SF-IMS[5125]: [5125] pm:pm [INFO] Using model
number 66F
sfpacket: module license 'Proprietary' taints kernel.
Disabling lock debugging due to kernel taint
Sourcefire Bridging Packet Driver - version 6.0.0
Copyright (c) 2004-2010 Sourcefire, Inc.

Cisco Firepower Management Center 4000 v6.1.0 (build 330)
Firepower login:admin
Password:Admin123

Copyright 2004-2016, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.1.0 (build 37)
Cisco Firepower Management Center 4000 v6.1.0 (build 330)

admin@FMC4000:~$
```

The command prompt, at the end of above example, confirms that the installation is totally complete. The next step is to verify the network connectivity on the management interface and begin the registration process.

Verification and Troubleshooting Tools

This section describes the commands and tools that you can run on an FMC. It enables you to investigate any issues with an FMC.

Identify an FMC on a Rack

If your rack is full of various hardware, and you did not label them outside, it might be challenging for you to identify an FMC. However, when necessary, you could turn on a LED on your desired FMC which would allow you locate an FMC on your rack on demand.

Follow the steps below in order to enable or disable the locator LED on your FMC:

Step 1. Login to the CIMC of your FMC through the Secure Shell (SSH) protocol.

[Example 4-8](#) shows a successful login attempt from a linux host to the CIMC of an FMC.

Example 4-8 Login to the CLI of CIMC

```
localhost:~@ ssh admin@10.1.1.10
admin@10.1.1.10's password:
CIMC#
```

Tips

If you are unable to remember the IP address or the password, you can change it from the CIMC Configuration Utility (Press <F8> during the POST operation).

Step 2. Once you are in the CIMC shell, enter the chassis command mode.

```
CIMC# scope chassis
CIMC /chassis#
```

Step 3. Run the **set locator-led** command to enable or disable the LED.

```
CIMC /chassis# set locator-led {on | off}
CIMC /chassis *#
```

Step 4. Apply the new settings.

```
CIMC /chassis *# commit
CIMC /chassis #
```

[Example 4-9](#) exhibits the steps to manage the locator LED on an FMC.

Example 4-9 Commands to Enable and Disable a Locator LED

```
! Run the following commands to enable the locator LED
.
.
CIMC# scope chassis
CIMC /chassis# set locator-led on
CIMC /chassis *# commit
.
.
! Run the following commands to disable the locator LED
.
.
CIMC# scope chassis
```

```
CIMC /chassis# set locator-led off
CIMC /chassis *# commit
```

Determine the Hardware and Software Detail of an FMC

After a successful login, an FMC displays a banner where you can find the software version and hardware model information.

[Example 4-10](#) shows a successful login to an FMC.

Example 4-10 *Login to the CLI of an FMC*

```
login as: admin
Password:
```

```
Copyright 2004-2016, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.
```

```
Cisco Fire Linux OS v6.1.0 (build 37)
Cisco Firepower Management Center 4000 v6.1.0 (build 330)
```

```
admin@FMC4000:~$
```

However, you can also run the **sfcli** command on demand that displays all types of software versions and hardware model information in the output.

[Example 4-11](#) confirms the hardware model as well as software, rule update and VDB versions of an FMC.

Example 4-11 *Output of the “sfcli.pl show version” Command*

```
admin@FMC4000:~$ sfcli.pl show version
Password:
-----[ FMC4000 ]-----
Model                : Cisco Firepower Management Center 4000 (66) Version
6.1.0 (Build 330)
UUID                 : 5bac032c-8bf5-11e6-a7c8-99be23cbc50d
Rules update version : 2016-10-05-001-vrt
VDB version          : 270
-----
```

```
admin@FMC4000:~$
```

Determine the RAID Battery Status

To determine the status of the RAID battery in an FMC, use the MegaCLI command with the necessary parameters.

[Example 4-12](#) confirms that the battery status is good, and no replacement is necessary.

Example 4-12 *The RAID Battery Status is Displayed in the MegaCLI Command Output*

```
admin@FMC4000:~$ sudo MegaCLI -AdpBbuCmd -aAll | grep -i battery
BatteryType: CVPM02
  Battery Pack Missing                : No
  Battery Replacement required        : No
  Battery backup charge time : 0 hours
Battery FRU: N/A
```

```
admin@FMC4000:~$
```

Determine the Status of a Power Supply Unit (PSU)

Before you deploy an FMC in your production network, it is one of the best practices to check the status of the PSU, and make sure they are operational. Look at the rear panel of your FMC. What is color of the power supply fault LED? If the color is amber, is it blinking or solid?

[Table 4-4](#) explains the meaning of the power supply fault LED that is located at the rear of an FMC (FMC 2000 or FMC 4000 chassis).

LED State	Condition
Solid Amber	Critical condition
Blinking Amber	Operational with warning
Off	Operational

Table 4-4. *Definitions of the Power Supply Fault LED*

You check the LED status when you have physical access to your FMC. How would you check the LED status if an FMC is in a remote location? Well, you could ask someone at that location to check the LED you, or you may send someone there (which might take several hours to several days, depending on the location).

Logs on CLI

Apart from checking the LED status, you can also investigate an issue with the PSU from the CLI or the GUI (assuming, FMC is turned on, and receives power from at least one of the PSUs).

[Example 4-13](#) demonstrates that the Power Supply 1 (PS1) has lost power while the Power Supply 2 is working.

Example 4-13 *The Status of the Power Supply Units in an FMC*

```
admin@FMC4000:~$ cat /var/sf/run/power.status

PS1: 0x08: Power Supply input lost
PS2: 0x01: Presence detected

admin@FMC4000:~$
```

You can also confirm a failure event using the Intelligent Platform Management Interface (IPMI) tool.

[Example 4-14](#) demonstrates redundancy as soon as one PSU loses power. The FMC, in this example, receives power from the second PSU.

Example 4-14 *Events are Generated When a Power Supply Unit Loses Power*

```
admin@FMC4000:~$ sudo ipmitool sel list | grep -i power

 2cf | 10/12/2016 | 18:42:33 | Power Supply #0x26 | Power Supply AC lost |
Asserted
 2d0 | 10/12/2016 | 18:42:33 | Power Supply #0x3a | Redundancy Degraded |
Asserted
 2da | 10/12/2016 | 18:43:58 | Power Supply #0x3a | Non-Redundant:
Sufficient from Redundant | Asserted

admin@FMC4000:~$
```

[Example 4-15](#) exhibits many different components (such as, voltage, temperature, etc.) related to the power supplies of an FMC, their values, and current statuses.

Example 4-15 *Status of Various Components of the Power Supply Units*

```
admin@FMC4000:~$ sudo ipmitool sdr | egrep -i "power|ps"
MAIN_POWER_PRS      | 0x00      | ok
POWER_ON_FAIL       | 0x00      | ok
PSU1_STATUS         | 0x00      | ok
PSU2_STATUS         | 0x00      | ok
PSU1_PWRGD          | 0x00      | ok
PSU1_AC_OK          | 0x00      | ok
PSU2_PWRGD          | 0x00      | ok
PSU2_AC_OK          | 0x00      | ok
LED_PSU_STATUS      | 0x00      | ok
PS_RDNDNT_MODE      | 0x00      | ok
POWER_USAGE         | 128 Watts | ok
PSU1_VOUT           | 0 Volts   | ok
PSU1_IOUT           | 0 Amps    | ok
PSU1_POUT           | 0 Watts   | ok
PSU2_VOUT           | 12 Volts  | ok
PSU2_IOUT           | 9 Amps    | ok
PSU2_POUT           | 112 Watts | ok
PSU1_PIN            | 0 Watts   | ok
PSU2_PIN            | 128 Watts | ok
PSU1_TEMP           | 30 degrees C | ok
PSU2_TEMP           | 32 degrees C | ok
admin@FMC4000:~$
```

[Alerts on GUI](#)

When one of the PSUs fails, FMC can display a health alert for it if the Power Supply health module is enabled in the current Health Policy.

[Figure 4-24](#) shows the health module setting to monitor power supplies. To find this configuration page, go to the **System > Health > Policy** page, and edit the active Health Policy.

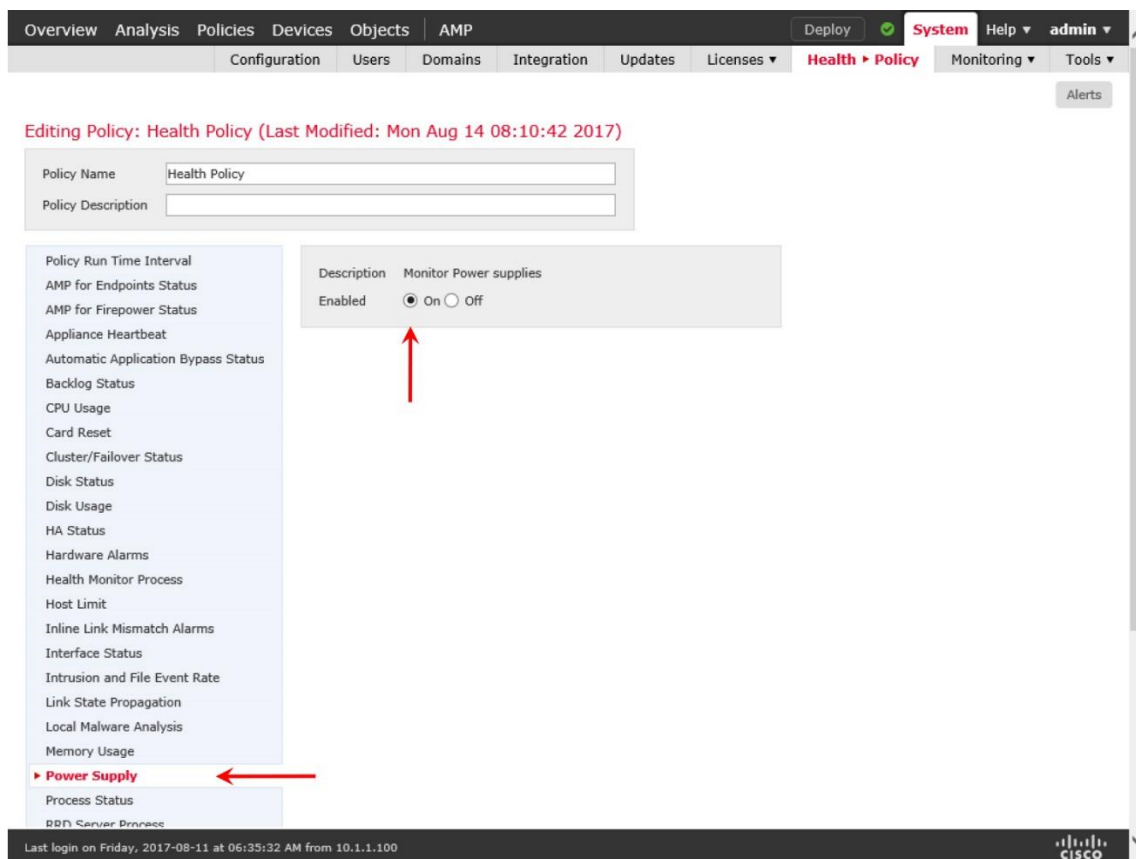


Figure 4-24. Health Module to Monitor Power Supply Units

When an alert appears, click on the health status icon — a critical alert shows a red exclamation sign, whereas a warning displays a yellow triangle.

[Figure 4-25](#) indicates a critical health status icon when an FMC detects a power supply unit failure. After you click on the icon, a small window appears on top of the regular GUI. Select the **Health** tab. You will find the cause for an alert.

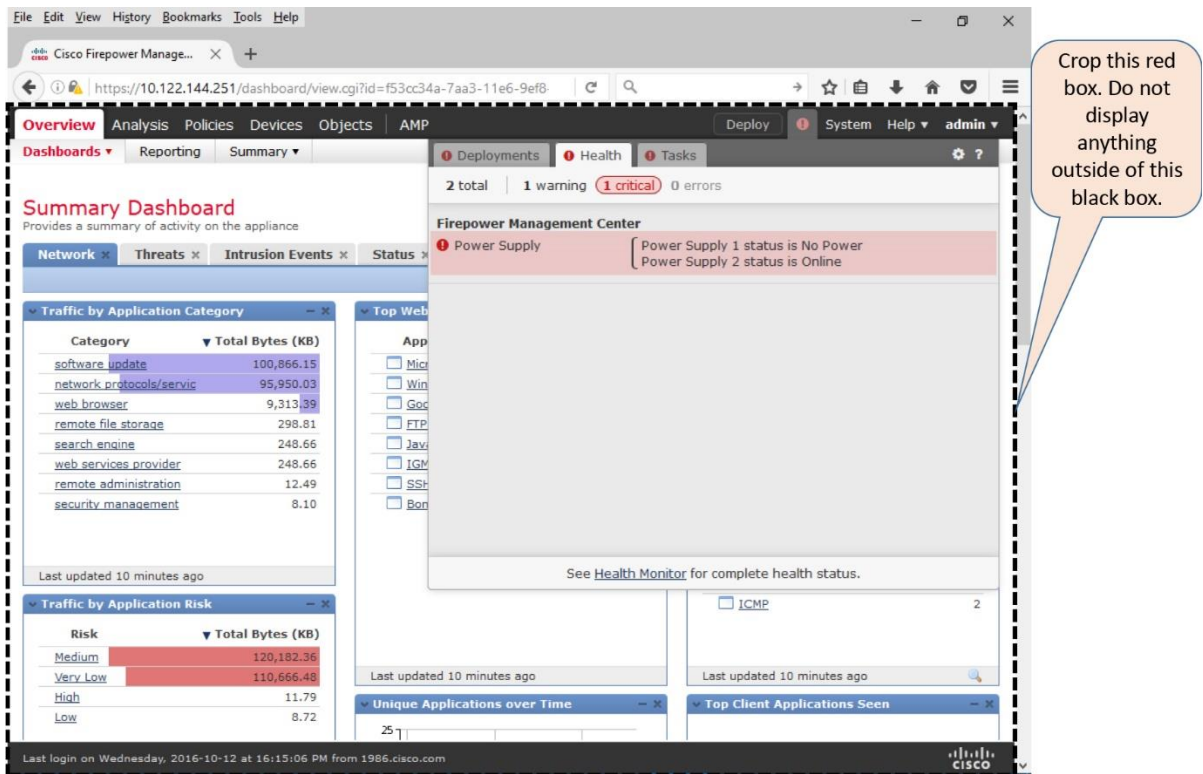


Figure 4-25. Health Alert Appears in the Top Right Corner of the GUI

[Figure 4-26](#) exhibits an alternative way to find descriptions for any health alerts — by navigating to the **Health Monitor** page at **System > Health > Monitor**.

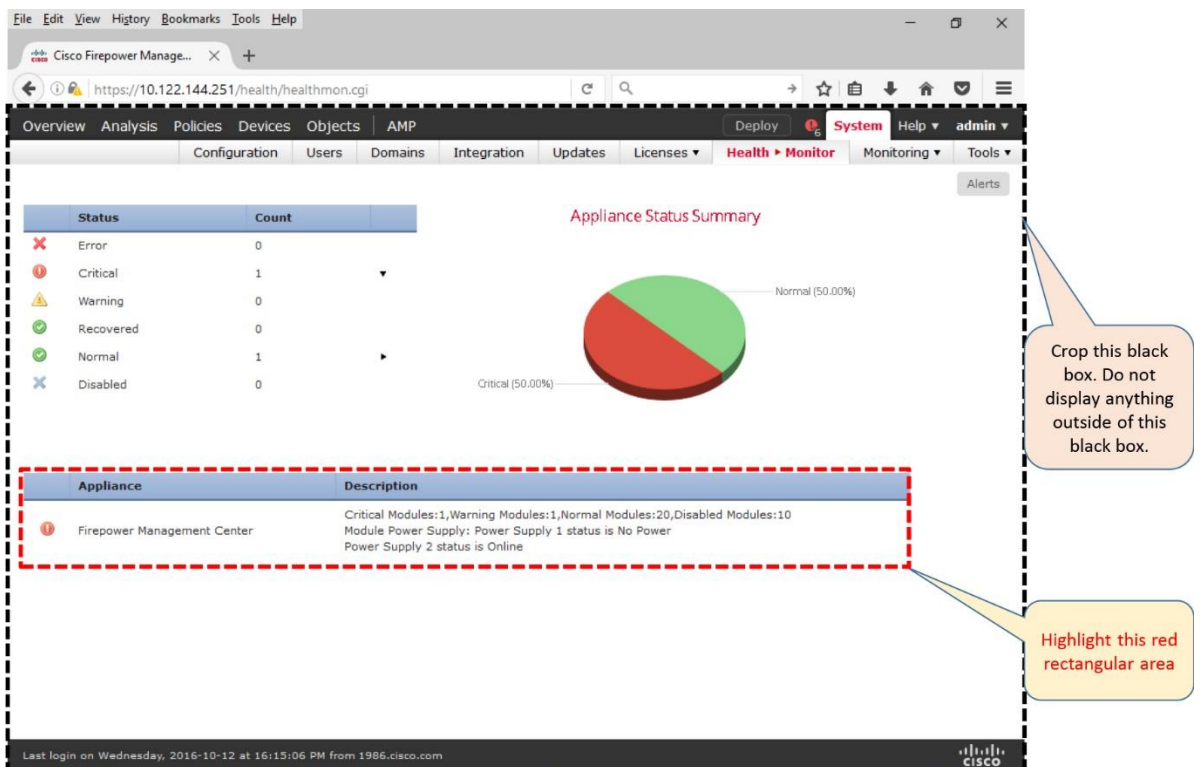


Figure 4-26. Health Monitor Page of an FMC

Complete Power Cycle

If both of the PSUs are connected, but generate health alerts, a complete power cycle might resolve the issue. To perform a complete power cycle, follow the steps below:

Step 1. Gracefully shutdown your FMC.

Step 2. Unplug all the power cords from the device.

Warning

Pulling a power cord without a graceful shutdown can corrupt the database and file system of an FMC. You may have to reimage the whole system to recover any database issues.

Step 3. Wait five minutes.

Caution

The waiting period is necessary to discharge any internal electric charges.

Step 4. Reconnect the power cords to the FMC.

Step 5. Turn on the FMC.

Checklist

You have learned various techniques to investigate an issue with a PSU. Let's create a checklist for the items that need to be verified.

- Determine if the power supply fault LED is amber.
- Check if the cords are properly connected to a power outlet.
- Verify if the power cord is faulty.
- Confirm if the power outlet is working.
- Check if the fan on the faulty power supply unit is running
- Try a complete power cycle, and see if the issue is fixed.

Verification of the Fans

The chassis of an FMC has a fan status LED. You can determine the status by looking into the front panel of the chassis.

[Table 4-5](#) explains the meaning of the fan status LED that is located at the front panel of an FMC (FMC 2000 or FMC 4000 chassis).

LED State	Condition
Green	Operating properly
Solid Amber	One of the fan modules has failed
Blinking Amber	More than one fan modules have failed

Table 4-5. *Definitions of the Fan Status LED*

If you can also confirm the status of a fan from the CLI. There are two ways to determine the status of the fans — by reading a log file, and by running a command.

[Example 4-16](#) shows the information that are logged into the `fans.status` file.

Example 4-16 *Output of a Log File That Shows the Status of Various Fans on an FMC*

```
admin@FMC2000:~$ cat /var/sf/run/fans.status
$fan_status = {
  FAN11_name => 'FAN1_TACH1',
  FAN11_alertlevel => 'Green',
  FAN11_unit => 'RPM',
  FAN11_value => '3200',
  FAN12_name => 'FAN1_TACH2',
  FAN12_alertlevel => 'Green',
  FAN12_unit => 'RPM',
  FAN12_value => '3200',
  FAN21_name => 'FAN2_TACH1',
  FAN21_alertlevel => 'Green',
  FAN21_unit => 'RPM',
  FAN21_value => '3200',
  FAN22_name => 'FAN2_TACH2',
  FAN22_alertlevel => 'Green',
  FAN22_unit => 'RPM',
  FAN22_value => '3200',
  FAN31_name => 'FAN3_TACH1',
  FAN31_alertlevel => 'Green',
  FAN31_unit => 'RPM',
  FAN31_value => '3200',
  FAN32_name => 'FAN3_TACH2',
  FAN32_alertlevel => 'Green',
  FAN32_unit => 'RPM',
  FAN32_value => '3200',
  FAN41_name => 'FAN4_TACH1',
  FAN41_alertlevel => 'Green',
  FAN41_unit => 'RPM',
  FAN41_value => '3200',
  FAN42_name => 'FAN4_TACH2',
  FAN42_alertlevel => 'Green',
  FAN42_unit => 'RPM',
  FAN42_value => '3200',
  FAN51_name => 'FAN5_TACH1',
  FAN51_alertlevel => 'Green',
  FAN51_unit => 'RPM',
  FAN51_value => '3200',
  FAN52_name => 'FAN5_TACH2',
  FAN52_alertlevel => 'Green',
```

```

        FAN52_unit => 'RPM',
        FAN52_value => '3200',
};
admin@FMC2000:~$

```

If you find the output is too long, you could use **grep** command — a regular expression tool to view a concise output with desired keywords.

[Example 4-17](#) shows the alert levels (green or amber) of the fans in an FMC. This is a concise view of the **fans.status** log file.

Example 4-17 *Determination of the Fan Status LED from the CLI*

```

admin@FMC2000:~$ grep -i alert /var/sf/run/fans.status
        FAN11_alertlevel => 'Green',
        FAN12_alertlevel => 'Green',
        FAN21_alertlevel => 'Green',
        FAN22_alertlevel => 'Green',
        FAN31_alertlevel => 'Green',
        FAN32_alertlevel => 'Green',
        FAN41_alertlevel => 'Green',
        FAN42_alertlevel => 'Green',
        FAN51_alertlevel => 'Green',
        FAN52_alertlevel => 'Green',
admin@FMC2000:~$

```

You can also see the current status of the fans by running the **ipmitool** command with specific parameters.

[Example 4-18](#) shows the alert levels (green or amber) of the fans in an FMC. This is a concise view of the **fans.status** log file.

Example 4-18 *The RPM and Status of Each Fan in an FMC*

```

admin@FMC2000:~$ sudo ipmitool sdr list | grep -i fan | grep -i tach
FAN1_TACH1      | 7490 RPM      | ok
FAN1_TACH2      | 7062 RPM      | ok
FAN2_TACH1      | 7704 RPM      | ok
FAN2_TACH2      | 7276 RPM      | ok
FAN3_TACH1      | 7704 RPM      | ok
FAN3_TACH2      | 7276 RPM      | ok
FAN4_TACH1      | 7704 RPM      | ok
FAN4_TACH2      | 7062 RPM      | ok
FAN5_TACH1      | 7704 RPM      | ok
FAN5_TACH2      | 7062 RPM      | ok
admin@FMC2000:~$

```

Summary

This chapter discusses and compares various hardware platforms for the FMC. It illustrates the complete reimage (also known as System Restore) process, and describes the best practices for a reimage. By reading this chapter, you can also learn many different commands and tools to determine any issues with an FMC hardware.

Quiz

1. Which step would be unique when reimaging an FMC from an older 5.x version to 6.1 directly?

- a. FMC supports a reimage from 5.x to 6.1 with zero downtime
- b. Go through the System_Restore reimage process twice
- c. Reimaging an FMC from 5.x to 6.1 is not supported
- d. No need to reimage, just download the single 6.1 upgrade file and install it directly

2. Which command shows the status of the RAID battery on an FMC?

- a. **sudo megacli -AdpBbuCmd -aAll | grep -i battery**
- b. **megacli -AdpBbuCmd -aAll | egrep -i battery**
- c. **MegaCLI -AdpBbuCmd -aAll | grep battery**
- d. **sudo MegaCLI -AdpBbuCmd -aAll | grep -i battery**

3. Which command would you run to determine the status of fans?

- a. **cat /var/log/run/fans.log | grep -i status**
- b. **cat /var/sf/run/fans | grep status**
- c. **cat /var/log/run/fans.status**
- d. **cat /var/sf/run/fans.status**

4. What does blinking amber LED mean for a fan status LED?

- a. Operational, but the temperature is high
- b. Operational, but one of the fan modules has failed
- c. Two or more fan modules have failed
- d. Fans are not working at all

5. Which command confirms if an FMC is running on a redundant power supply unit?

- a. **sudo ipmitool sdr | egrep -i "power|ps"**
- b. **sudo ipmitool sel list | grep -i power**
- c. **cat /var/sf/run/power.status**

d. `cat /var/sf/run/power.log .status`

6. What does blinking amber LED mean for a power supply fault LED?

a. Overheated

b. Critical Condition

c. Operational, but has warning

d. No problem, as long as it is not solid amber

7. Which command shows the Firepower software version and hardware platform detail?

a. `show version`

b. `sfcli version`

c. `show sfr version`

d. `sfcli.pl show version`

Chapter 5. Firepower System (FMC+FTD) Virtual on VMware

In the previous chapters, you have learned how to install the Firepower System software on Cisco hardware. If you choose not to purchase any additional hardware, you can still deploy the Firepower System in your existing virtual infrastructure. You can choose to virtualize both or one of the Firepower appliances — either an FMC or an FTD. This chapter discusses the implementation of Firepower Management Center (FMC) Virtual and Firepower Threat Defense (FTD) Virtual in VMware — one of the most popular virtual environments.

Essential Knowledge

An FMC virtual appliance can manage any FTD physical appliance. Similarly, an FTD virtual appliance is fully interoperable with an FMC virtual appliance as well as an FMC physical hardware. Before deploying a Firepower virtual appliance, let's take a moment to understand the key deployment options.

Supported Virtual Environment

Beginning from Version 6.1, the Firepower software supports wide variety of virtual environments, such as, VMware, Kernel-Based Virtual Machine (KVM) and Amazon Web Services (AWS). This chapter uses VMware to demonstrate the deployment of a Firepower virtual appliance.

[Table 5-1](#) provides a list of virtual environments that are compatible with the Firepower System software version 6.1.

Virtual Environments	Supported Platform
VMware	ESXi 5.5, 6.0
Amazon Web Services (AWS)	Virtual Private Cloud (VPC), Elastic Compute Cloud (EC2)
KVM	Tested on Ubuntu 14.04 LTS
Microsoft	Hyper-V is not supported.

Table 5-1. *Virtual Environments for the Firepower System Version 6.1*

In order to manage a virtual appliance on an VMware ESXi server, you can use vCloud Director, vCenter, or vSphere Client. The vSphere Client has two different variations — web and desktop. Both of them are supported by the Firepower virtual appliances.

To host a Firepower virtual appliance, you can use the VMware ESXi 5.5 and 6.0, but the following solutions are unsupported:

- VMware Workstation
- VMware Server
- VMware Player
- VMware Fusion

ESXi vs VI

The tarball (.tar.gz file) of a Firepower virtual appliance includes templates for ESXi or the Virtual Infrastructure (VI). The key difference between them is the initial setup process, such as, configuring the network, setting up a password for the admin account, etc.

In a VI template deployment, you configure the initial system settings using a deployment wizard, before a Firepower virtual software is deployed. In an ESXi template, however, you configure the initial settings from the VMware console, after an appliance is deployed.

The examples in this chapter use the ESXi OVF template to deploy a Firepower virtual appliance on VMware.

VMware Installation Package in a Tarball

The VMware installation package for Firepower virtual appliance comes in a .tar.gz file format which includes three different types of files:

- **Open Virtual Format (.ovf) file:** An XML file that stores references to many elements of a Firepower system installation package.
- **Virtual Machine Disk (.vmdk) file:** A compressed virtual disk that stores the Firepower System software.
- **Manifest (.mf) file:** A clear text file that stores the SHA1 digests of any OVF and VMDK files in a package.

[Figure 5-1](#) shows the files that are packaged in a tarball for a Firepower virtual appliance Version 6.1.

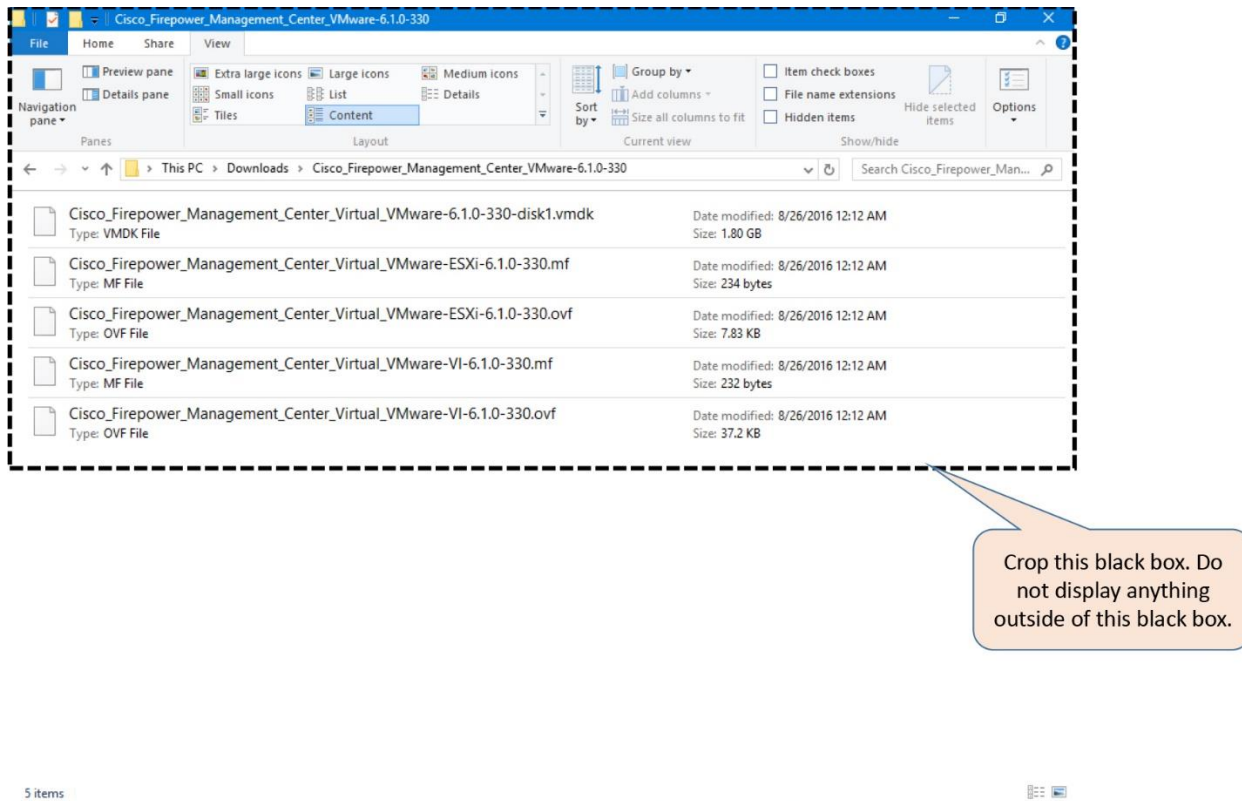


Figure 5-1. Files in a Tarball for an FMC Virtual Appliance

Disk Provisioning Options

During the deployment of a Firepower virtual appliance, you can choose one of the following provision methods for your virtual disk:

- **Thick Provision Lazy Zeroed:** Space for a virtual disk is allocated during its creation, but zeroed out later.
- **Thick Provision Eager Zeroed:** The space allocation and zero out of the data is performed at the time of a virtual disk creation. Therefore, this method might take longer time.
- **Thin Provision:** Disk space is allocated on-demand basis. The size of a virtual disk grows whenever there is a need, up to the maximum allocated limit.

[Figure 5-2](#) shows three available options for provisioning a virtual disk on ESXi host using the vSphere client software. The examples in this book uses Thick Provision Lazy Zeroed.

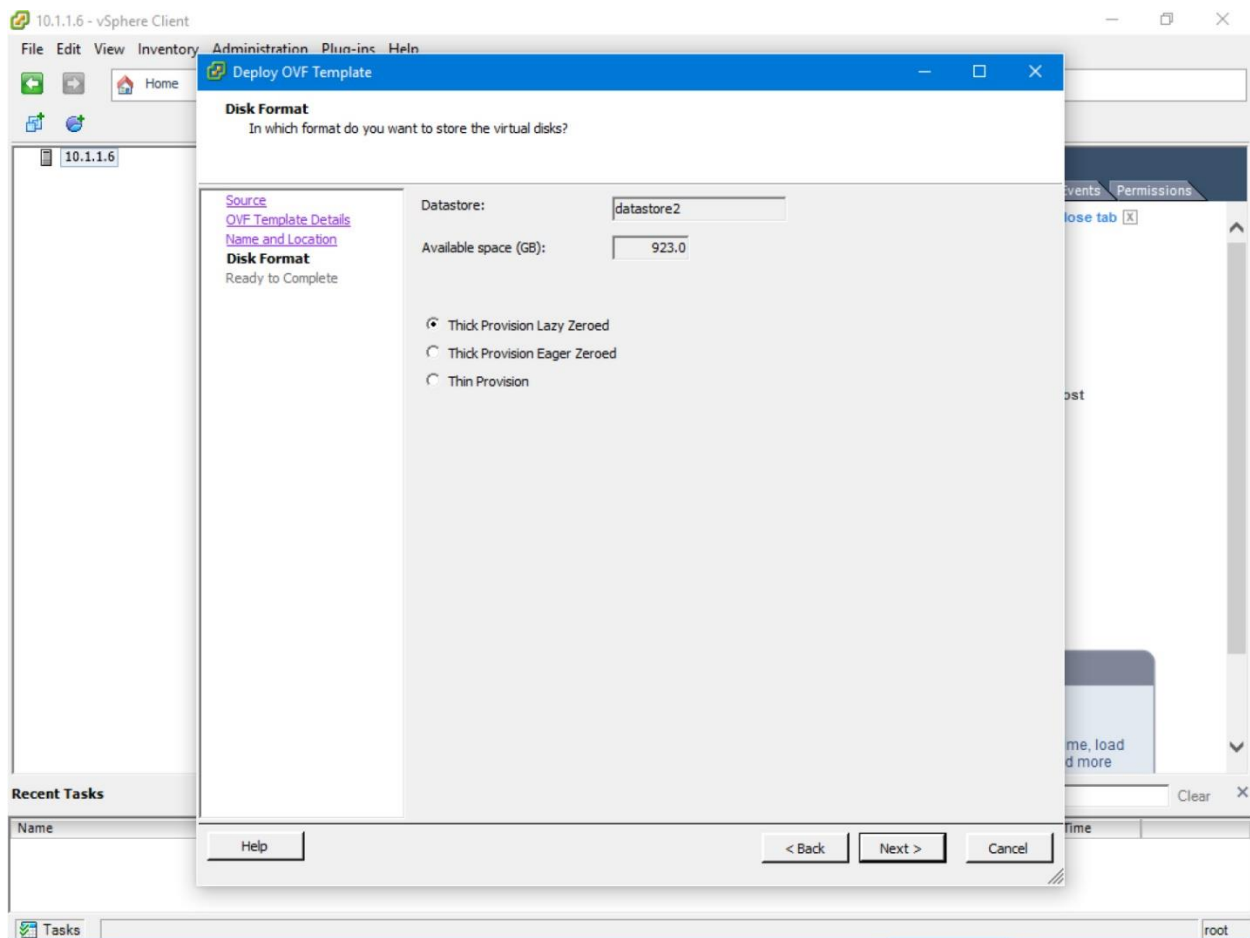


Figure 5-2. *Virtual Disk Provisioning Options*

Best Practices

If you plan to deploy a Firepower Management Center Virtual and a Firepower Threat Defense (FTD) Virtual Version 6.1, the Firepower Management Center (FMC) must be running Version 6.1 or greater. This chapter describes the process to reimage an FMC to 6.1.

Pre-Deployment

Consider the following best practices when you deploy any Firepower Virtual appliance:

1. Depending on the hardware resources of a server, a new Firepower virtual deployment process may take about an hour. You should also plan for additional time to fulfill any prerequisites and post-deployment setup.
2. Do not use an ISO file to build a Firepower appliance in your virtual environment. This is not supported. If your virtual network is based on VMware, use the Open Virtualization Format (OVF) file which is compressed in a .tar.gz file. If your infrastructure is KVM based, use the QEMU Copy On Write (QCOW2) file.

Figure 5-3 shows a .tar.gz file and a .qcow2 files that are packaged for VMware and KVM, respectively. You can download them from the Cisco Software Download page.

The screenshot shows the Cisco Software Download page for Firepower Management Center Virtual Appliance Release 6.1.0. The page displays a table of files for download. A red dashed box highlights two rows: 'Firepower Management Center Virtual64 VMWare' and 'Firepower Management Center Virtual64 KVM qcow2'. A black dashed box highlights the entire table area. Two callout boxes provide instructions: 'Highlight this red rectangular area' and 'Crop this black box. Do not display anything outside of this black box.'

File Information	Release Date	Size
Firepower Management Center Virtual64 VMWare Cisco_Firepower_Management_Center_VMware-6.1.0-330.tar.gz	29-AUG-2016	1821.82 MB
Firepower Management Center Virtual64 KVM qcow2 Cisco_Firepower_Management_Center_Virtual-6.1.0-330.qcow2	29-AUG-2016	1820.94 MB
Firepower Management Center 6.1.0 Pre-Install Utility Sourcefire_3D_Defense_Center_S3_Pre-install-6.0.1.999-1224.sh	29-AUG-2016	2.59 MB
Firepower Management Center 6.1.0 Upgrade Sourcefire_3D_Defense_Center_S3_Upgrade-6.1.0-330.sh	29-AUG-2016	1713.13 MB

Figure 5-3. FMC Virtual Appliance Installation Packages at Cisco.com

3. After you download an appropriate file for a Firepower virtual appliance from the Cisco.com, verify the MD5 or SHA512 checksum of the files you have downloaded. It confirms that the file is not corrupt, or not modified during download.

[Figure 5-4](#) exhibits the MD5 and SHA512 checksum values for the FTD Virtual installation package file at cisco.com. You can view them by hovering your mouse over a filename.

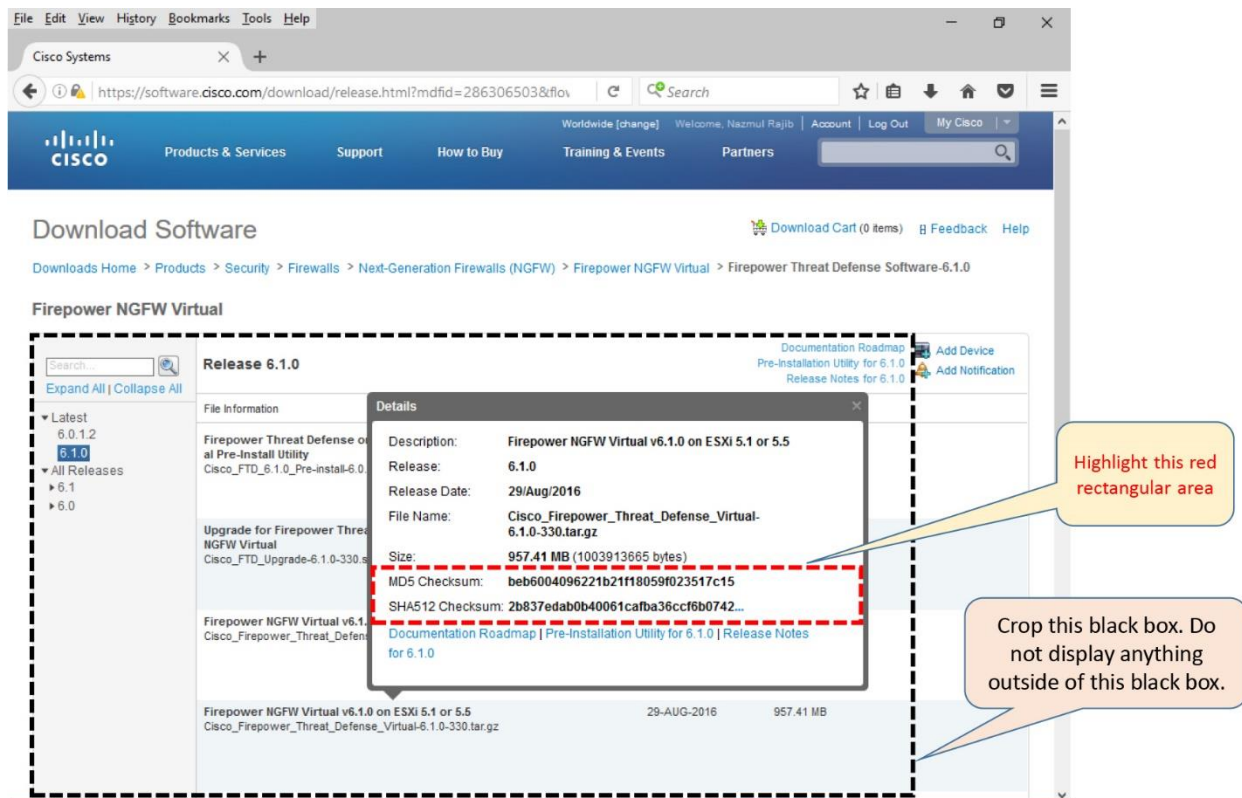


Figure 5-4. Checksum Values of the FTD Installation Package Displayed in a Pop-up Box

Tips

Inside a tarball, you will find a manifest file (*.mf) that stores the individual SHA1 checksum values of the *.vmdk and *.ovf file in a tarball.

4. Read the release notes to determine any known issues, any special requirements or instructions before you begin a reimage or system restoration.
5. Never power off a virtual appliance when the deployment or initialization is in progress. Upon a successful initialization, you will find a Firepower login prompt on the VMware console.

Post-Deployment

1. If your ESXi server has unused resources, you can allocate them to your Firepower virtual appliance. Allocating additional resource can enhance system performance. However, reducing any resources from the minimum requirement is unsupported. You can find the minimum requirements in the Prerequisites section of this chapter.
2. You can replace the E1000 network adapters with the VMXNET3 adapters for higher throughput.

Tip

The steps to upgrade a default E1000 adapter with a VMXNET3 adapter is described in the Verification and Troubleshooting Tools section of this chapter.

3. As a part of the disaster recovery plan, you should periodically take a backup of the existing events and configurations. Do not use any VMware provided built-in features to take a backup of a Firepower virtual appliance. Instead, utilize the **Backup/Restore** tool on the FMC.

[Figure 5-5](#) illustrates the backup management page of an FMC. It is located at **System > Tools > Backup/Restore**.

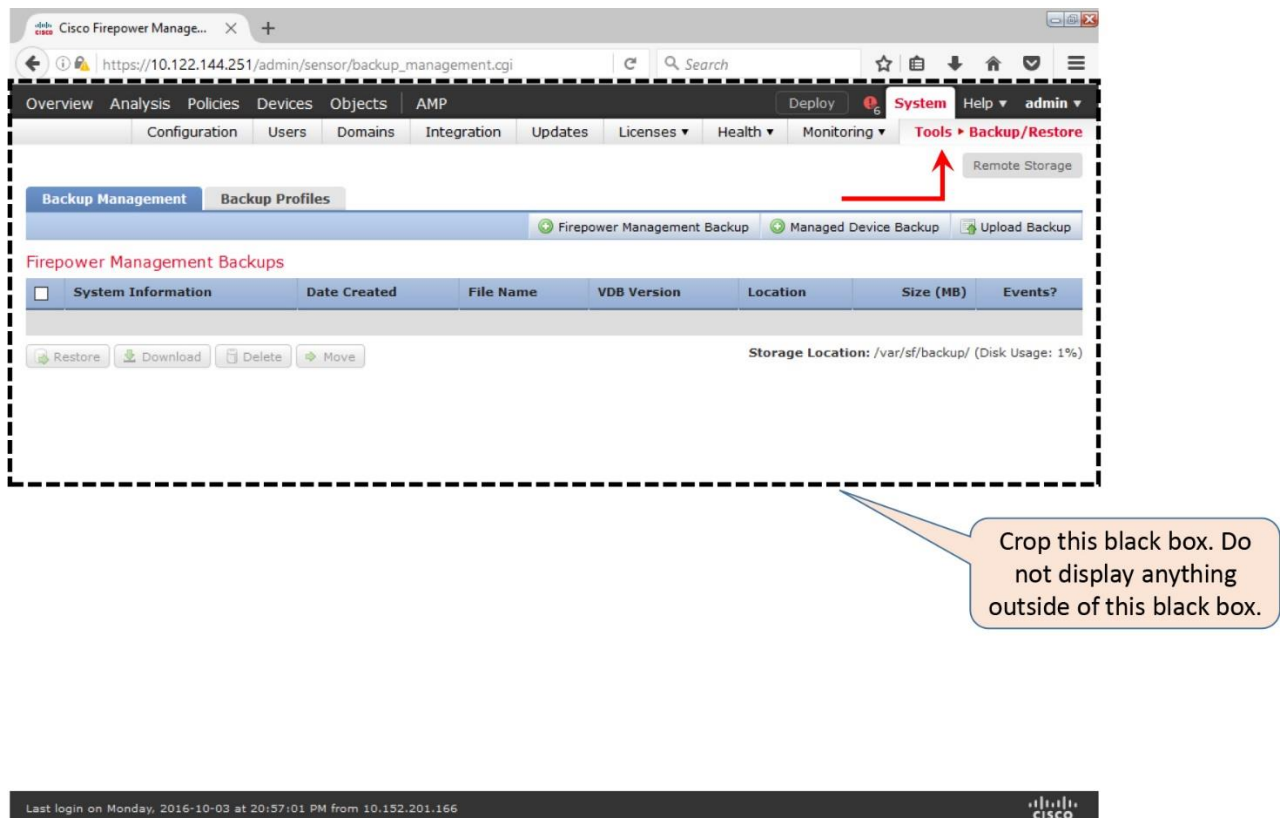


Figure 5-5. *The Backup Management Page on a Firepower Management Center*

Table 5-2 shows some of the backup tools provided by VMware. The Firepower Virtual appliances do not support these tools.

Feature	VMware Purpose	Firepower Support
Export	Export of any particular state of a virtual machine snapshot	Not supported
Clone	Duplication of a virtual machine with the same configurations and to another, without any downtime	Not supported
Motion	Migration of a running virtual machine from one physical server	Not supported

Table 5-2. Backup and Migration Tools by VMware (Unsupported by Firepower)

4. You can also utilize the Import/Export tool in an FMC to copy a policy. During an import, the versions of a restored system must match with the FMC from where any policies are originally exported. Therefore, when you export, you must remember the software and Rule Update version information of the original FMC.

Figure 5-6 exhibits the navigations to the Import/Export page. It is located at System > Tools > Import/Export.

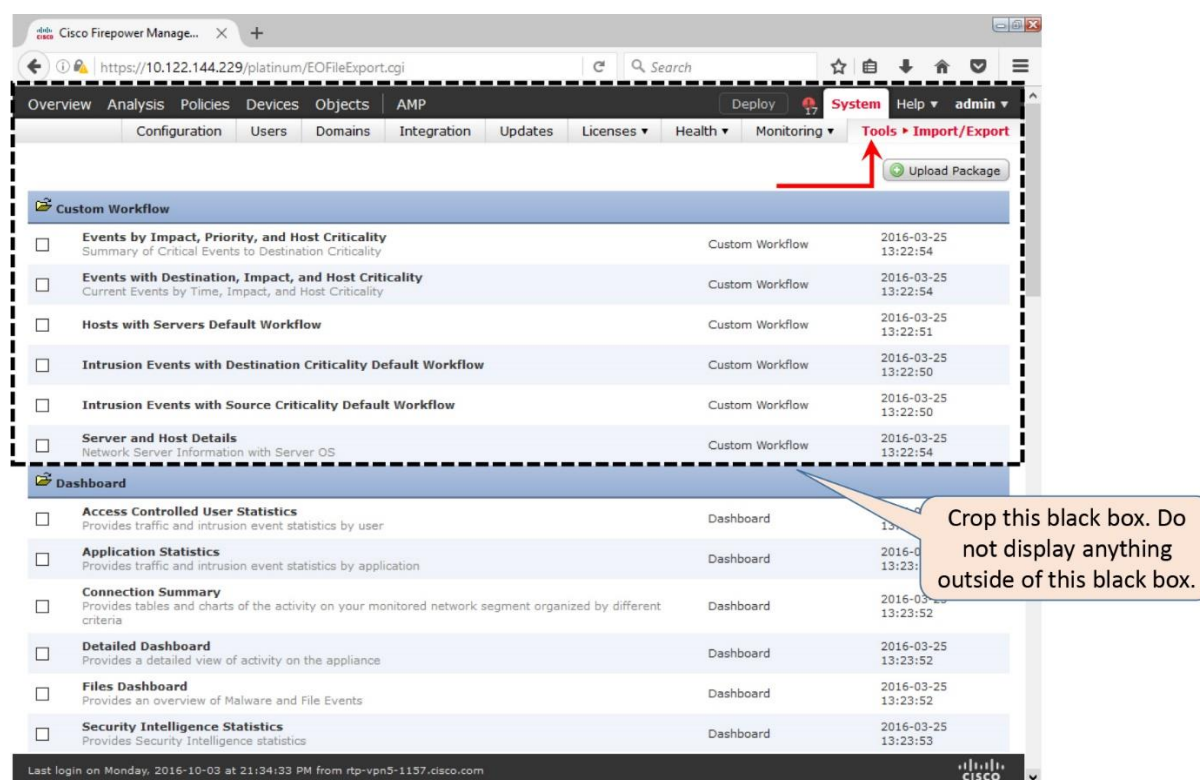


Figure 5-6. The Import/Export Page on a Firepower Management Center

Configuration

Deployment of a Firepower virtual appliance in VMware is not a one-click process. After you download a tarball for a Firepower software from the cisco.com, and extract it on your desktop, you need to complete the following steps:

1. Build an ESXi host that is compatible with Firepower.
2. Build a virtual layer 2 network on the ESXi host.
3. Deploy the OVF file for the desired Firepower appliance.
4. Verify the resource allocation and network mapping.
5. Power on the Firepower Appliance and initialize it.

[Figure 5-7](#) shows the key steps to deploy a firepower virtual appliance on a VMware ESXi host.

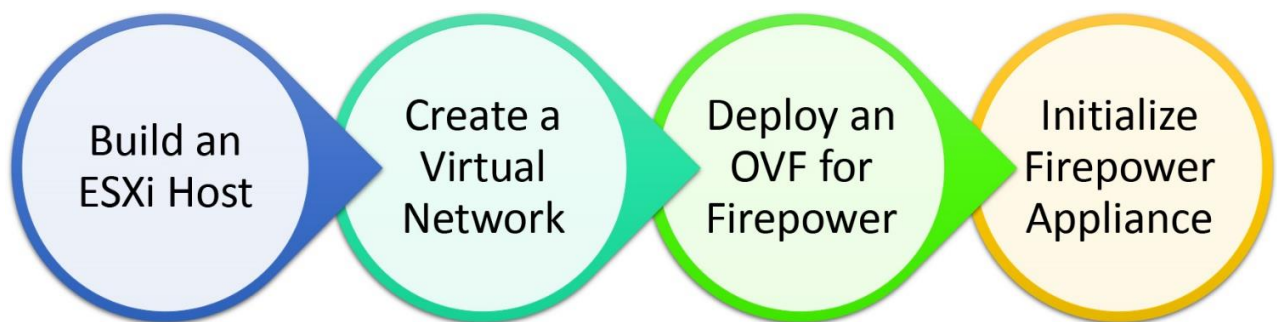


Figure 5-7. Major Steps to Deploy a Firepower Virtual Appliance

Prerequisites

1. In order to deploy any Firepower software, your server must have a 64-bit CPU that supports the virtualization technology.
2. You must enable the virtualization functionality from the BIOS Setup Utility.

Figure 5-8 shows the Intel Virtualization Technology is enabled in a BIOS Setup Utility. Depending on the hardware vendor of an ESXi server, a setup utility may look different.

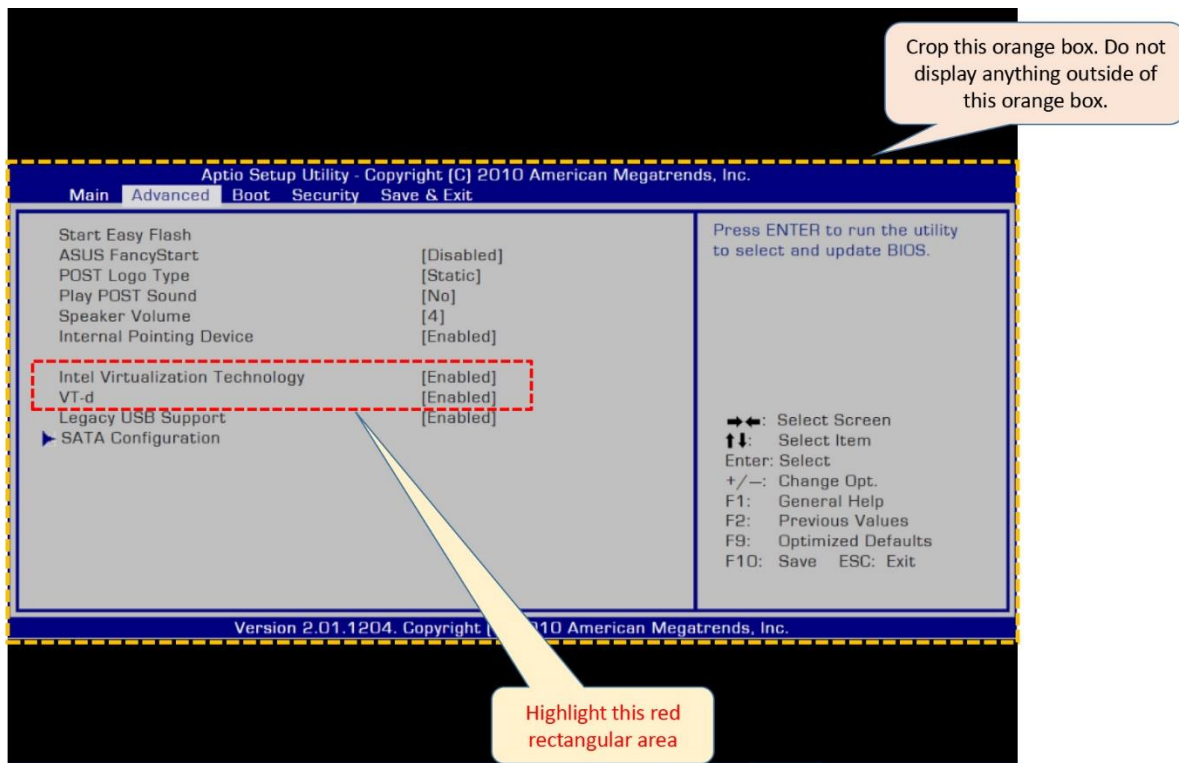


Figure 5-8. Enablement of the Virtualization Technology in the BIOS

3. After you build an ESXi host, connect to your host using a vSphere Client. You can use either a web client or a desktop client.

Figure 5-9 shows the default home page of an ESXi host. To view this page, enter the IP address of your ESXi server into a browser. This page provides you with a link to download the vSphere Client software.

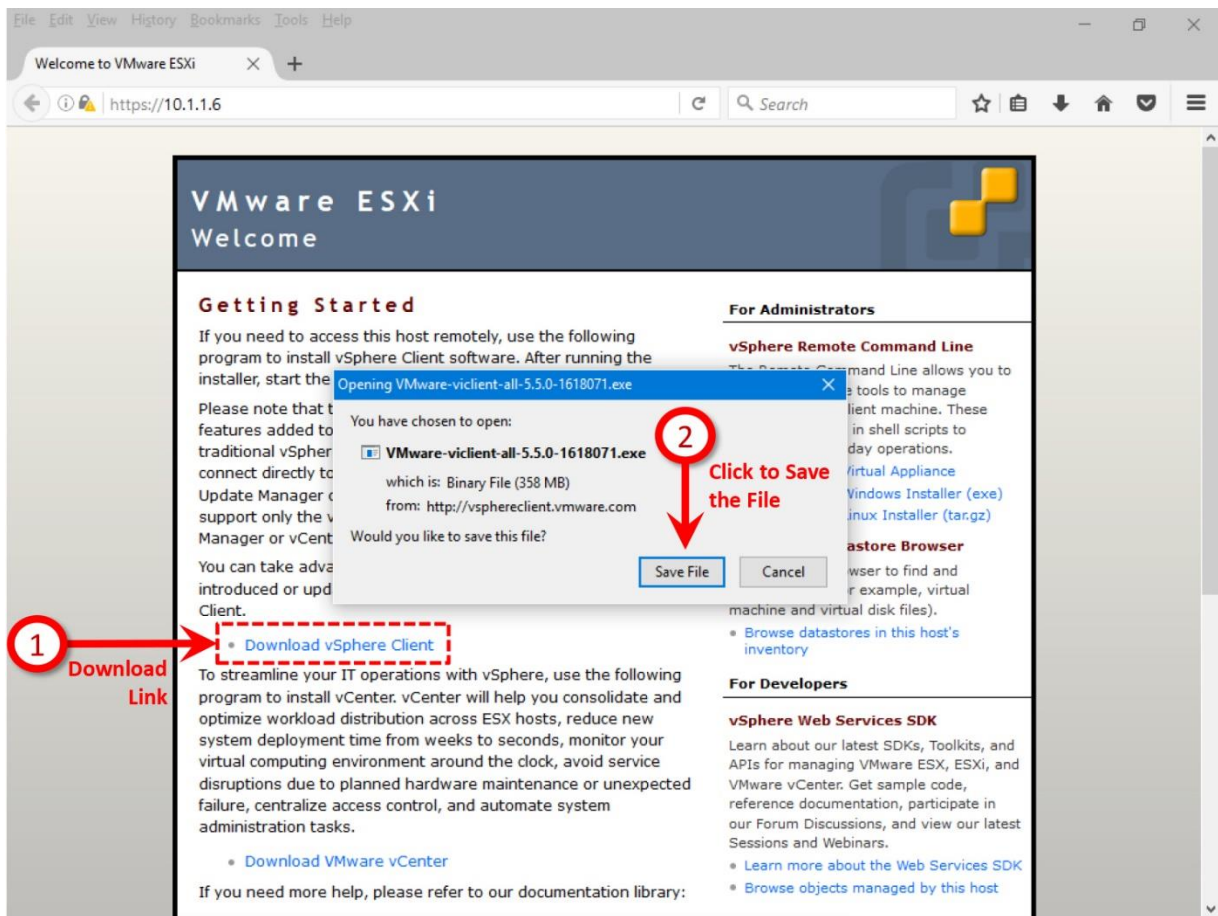


Figure 5-9. Download Link for a vSphere Client is Available on an ESXi Home Page

4. Whether your ESXi host runs version 5.5 or 6.0, ensure that your Firepower virtual appliance is allocated with the minimum amount of resources. Do not reduce the settings from the minimum requirements.

Table 5-3 shows the minimum requirements of an FMC virtual or FTD virtual appliance.

Network Interface	1	1
Disk Space	520 GB	4832 GB
Memory	8 GB	8 GB
CPU	1	1
Resource Type	FMC	FTD

Table 5-3. Minimum Resource Allocation for a Firepower Virtual Appliance

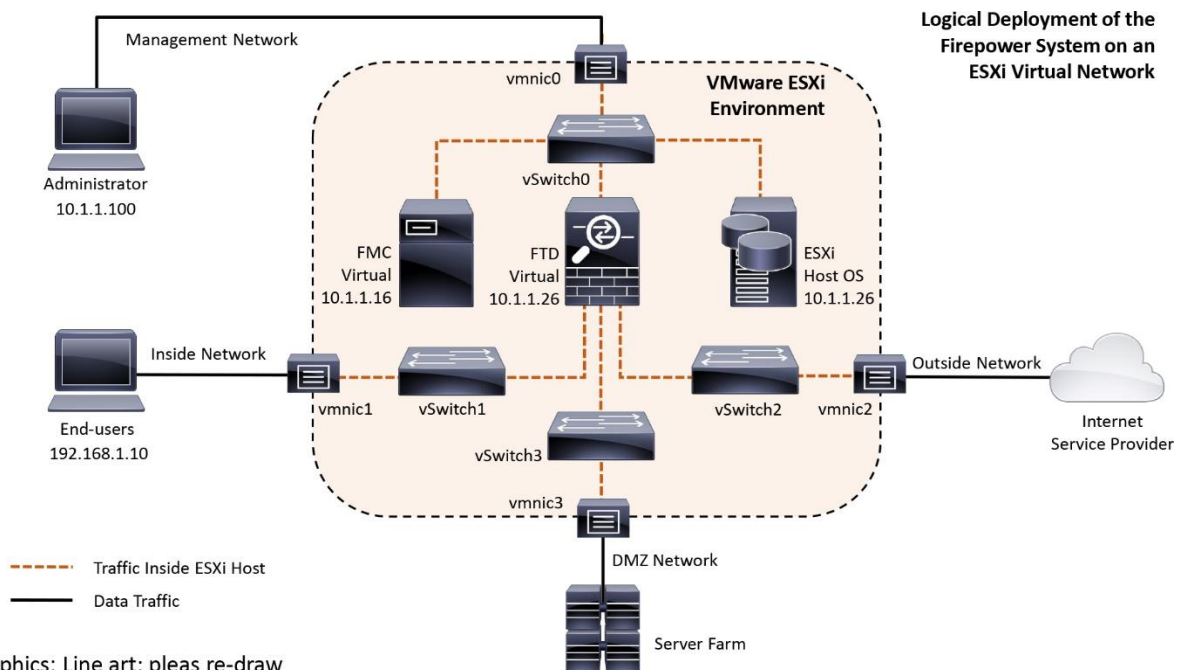
Tip

Read the *Verification and Troubleshooting Tools* section of this chapter to learn how to add an additional resource.

Creation of a Virtual Network

Let's assume, you have just built an ESXi host. Now you want to deploy both of the Firepower virtual appliances — an FMC and an FTD. The first thing you have to do is to create a layer 2 virtual topology using vSwitch and VMware network adapter.

[Figure 5-10](#) exhibits a topology that is created inside a virtual network. An ESXi Host, FMC, and FTD are connected to a management network, while data from inside network can traverse to the internet. All of the servers are placed in a DMZ network.



Graphics: Line art; pleas re-draw

Figure 5-10. A Virtual Network Topology on the VMware ESXi Host

The number of steps to create a virtual topology could be different, depending on the number of required interfaces on a particular appliance you want to deploy. For example, by default, an FMC Virtual requires only one interface for management communication, whereas an FTD Virtual requires four interfaces — one interface for management communication and three interfaces for traffic inspection.

In the next few pages, you will learn how to create a virtual network exhibited on [Figure 5-10](#) on a VMware ESXi host, using a vSphere client software.

Network for an FMC Virtual

By default, a virtual switch is created on a new ESXi installation. To view a virtual switch, go to the **Configuration > Networking** on the vSphere client.

[Figure 5-11](#) shows a default virtual switch **vSwitch0** that is created by the ESXi host. A physical adapter **vmnic0** is connected with two default virtual ports — **Management Network** and **VM Network**.

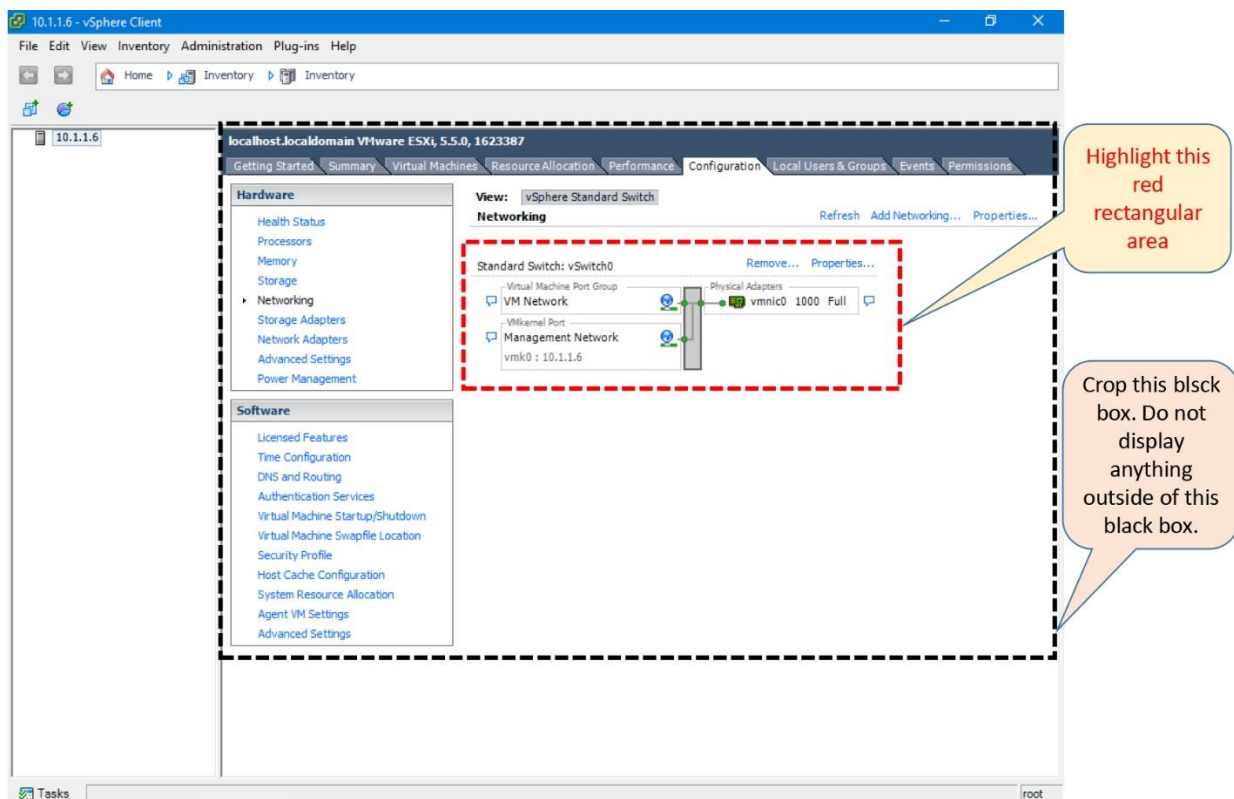


Figure 5-11. *Default Virtual Switch on an ESXi Host*

The Management Network is automatically mapped with the management interface of your ESXi host. The VM Network is available for your use. You can utilize it as the management interface for your FMC Virtual appliance. To make it clear and meaningful, you could optionally rename the default labels:

- Rename VM Network to FMC Management
- Rename Management Network to VMware Management

To rename the labels, use the following steps:

Step 1. Click on the **Properties** option next to the *Standard Switch: vSwitch0*. The **vSwitch0 Properties** window appears.

Figure 5-12 shows two virtual ports created by the ESXi host during installation.

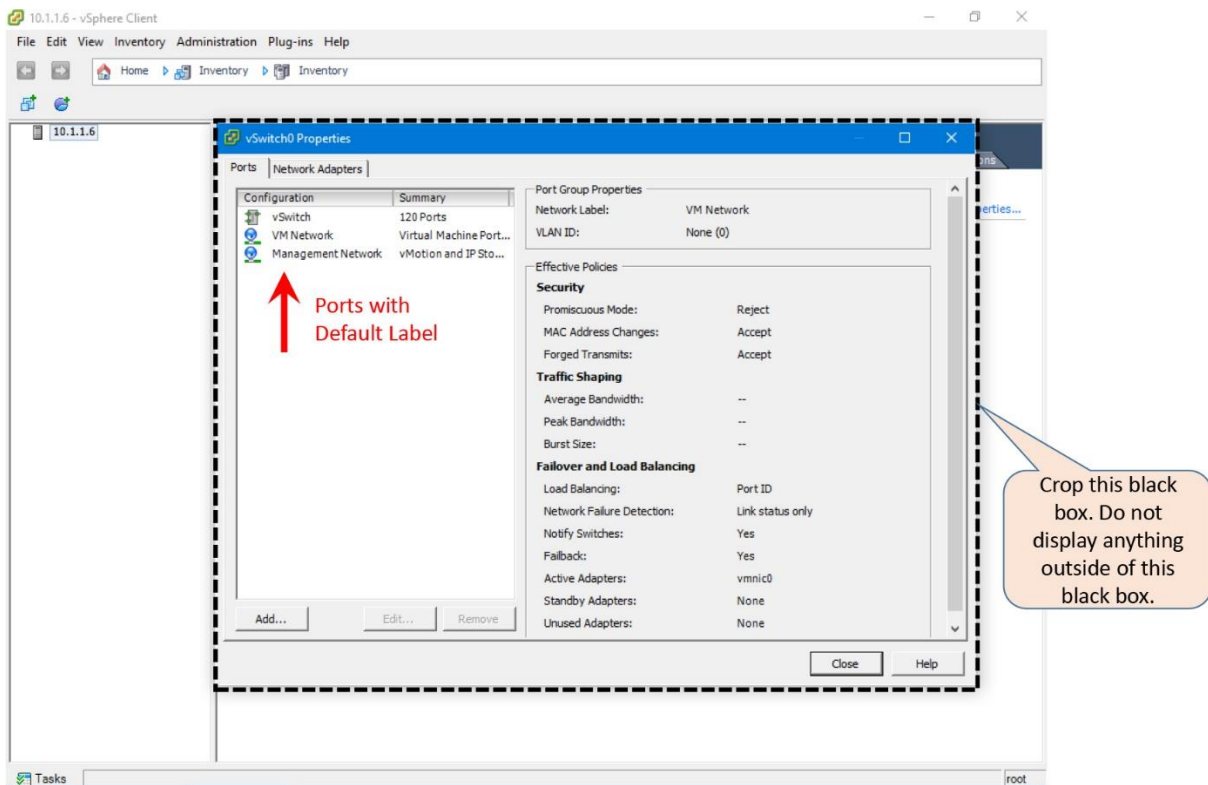


Figure 5-12. The Ports Tab in the vSwitch0 Properties Window

Step 2. Select a port, and click on the **Edit** button. The **VM Network Properties** windows appears.

[Figure 5-13](#) shows the **VM Network Properties** window that appears when you want to edit the default port **VM Network**.

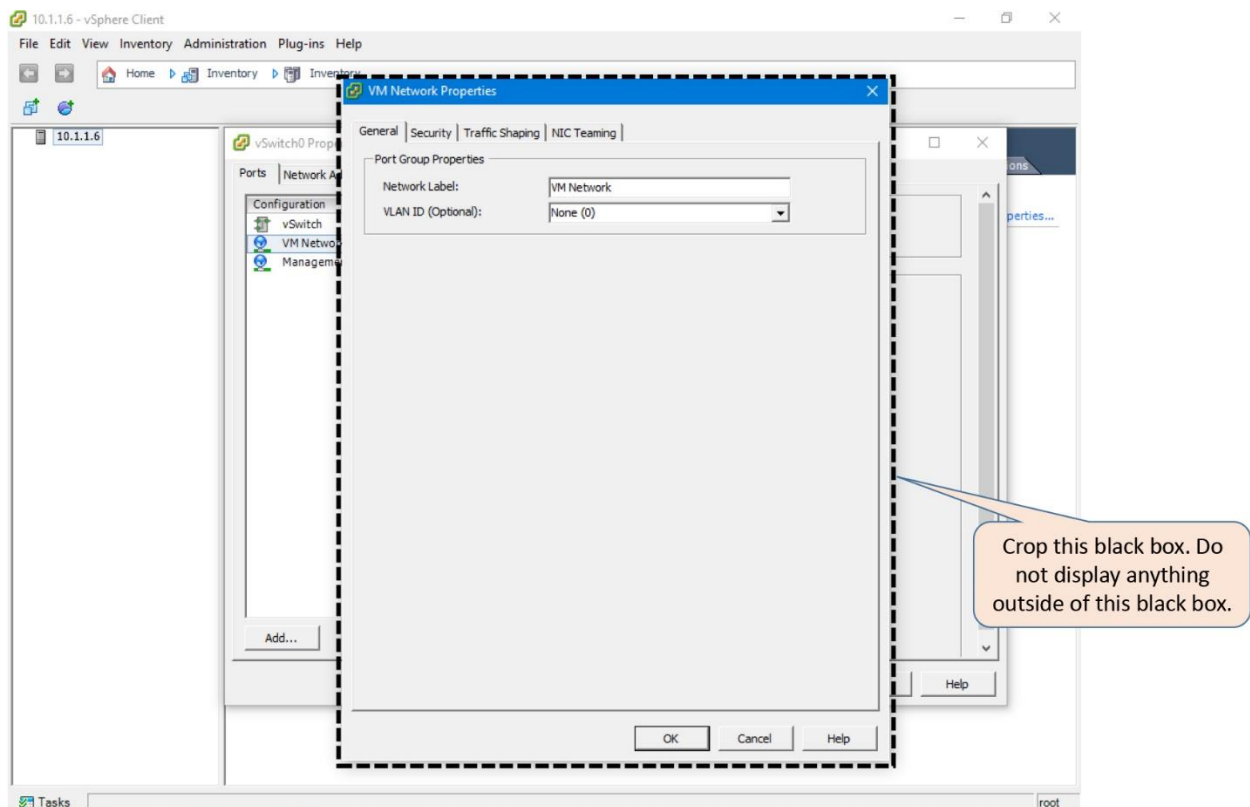


Figure 5-13. *The VM Network Properties Window*

Step 3. Replace the default label. Select **OK** when you are done.

Step 4. Optionally, repeat the steps to rename the **Management Network** to **VMware Management**.

[Figure 5-14](#) shows the **vSwitch0 Properties** window that appears when both of the ports are renamed. From the new labels, it is now clear what is the purpose of each port.

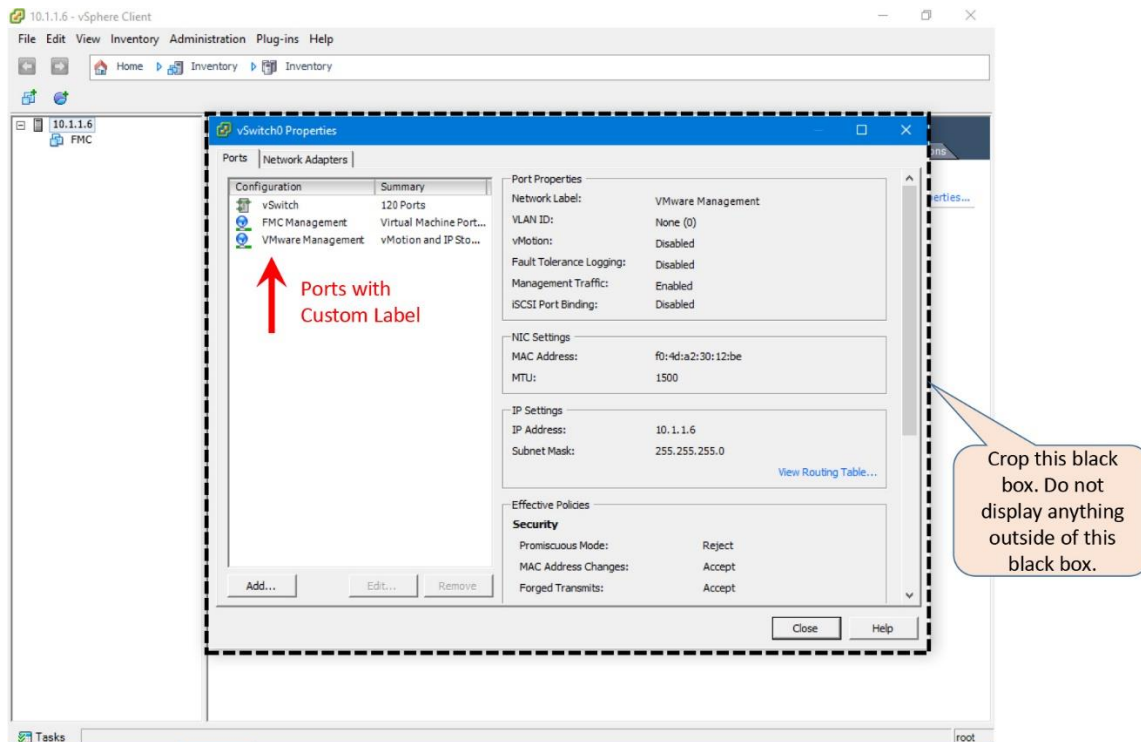


Figure 5-14. *The New Labels of Both Virtual Ports*

Step 5. Select **Close** to return to the *Networking* view where you could find the newly labeled virtual ports are connected to the same physical adapter.

If you plan to deploy an FTD Virtual, read the next section **Network for an FTD Virtual**. Otherwise, proceed to the **Deployment of an OVF Template** section.

Network for an FTD Virtual

In the pre-requisites section, you have learned that an FTD Virtual appliance requires at least four interfaces — one interface for management traffic and three interfaces for data traffic. In this section, you will learn how to add a network adapter for a virtual appliance.

Note

An FTD Virtual can support up to ten interfaces in total.

Step 1. Go to the **Configuration > Networking** page on your vSphere Client.

Step 2. Select the **Add Networking** option. The **Add Network Wizard** window appears.

[Figure 5-15](#) shows the **Add Networking** option in the networking configuration page. You can also see the new labels of the default virtual ports that you renamed in the previous section. Both of them are connected to the vmnic0 physical adapter.

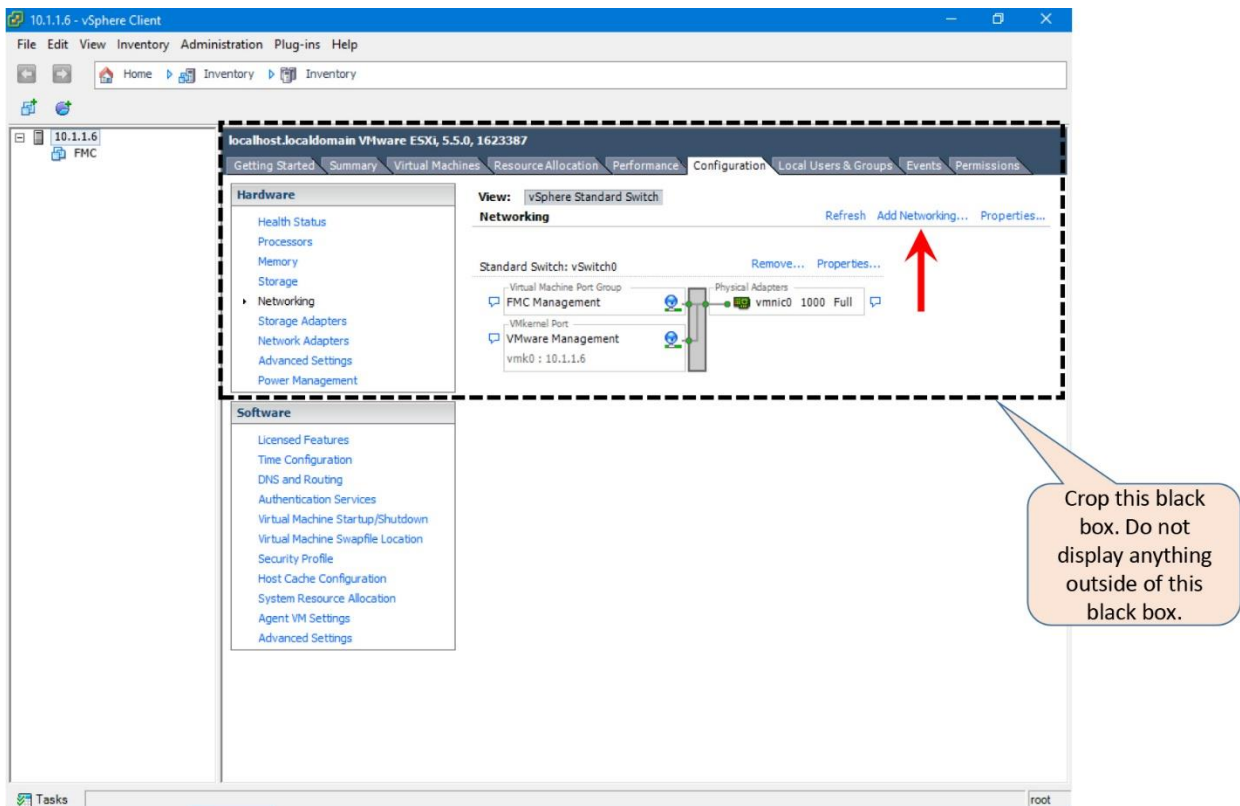


Figure 5-15. *The Default Virtual Switch vSwitch0 — After the Label Change*

Step 3. Select **Virtual Machine** as the Connection Type.

Figure 5-16 shows two connection types — Virtual Machine and VMKernel. Choose the Virtual Machine type for any Firepower Virtual Appliance.

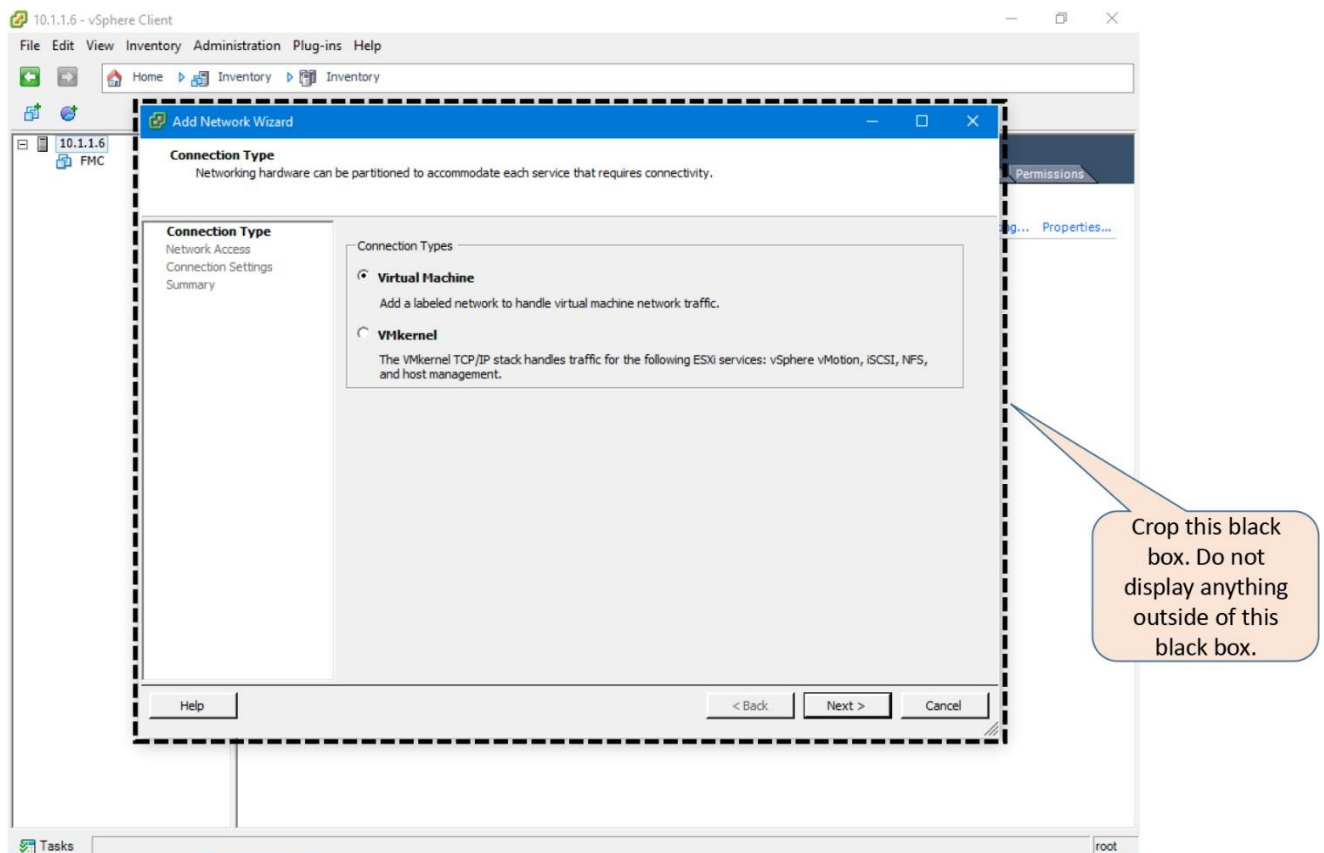


Figure 5-16. *Different Types of Connection Types in the Add Network Wizard*

Step 4. Select an existing virtual switch (vSwitch) or create a new one, which can map a physical adapter with a virtual port. You can configure each vSwitch to represent a segregated virtual network.

Figure 5-17 shows that vmnic0 is mapped with vSwitch0, which connects the FTD Virtual management port.

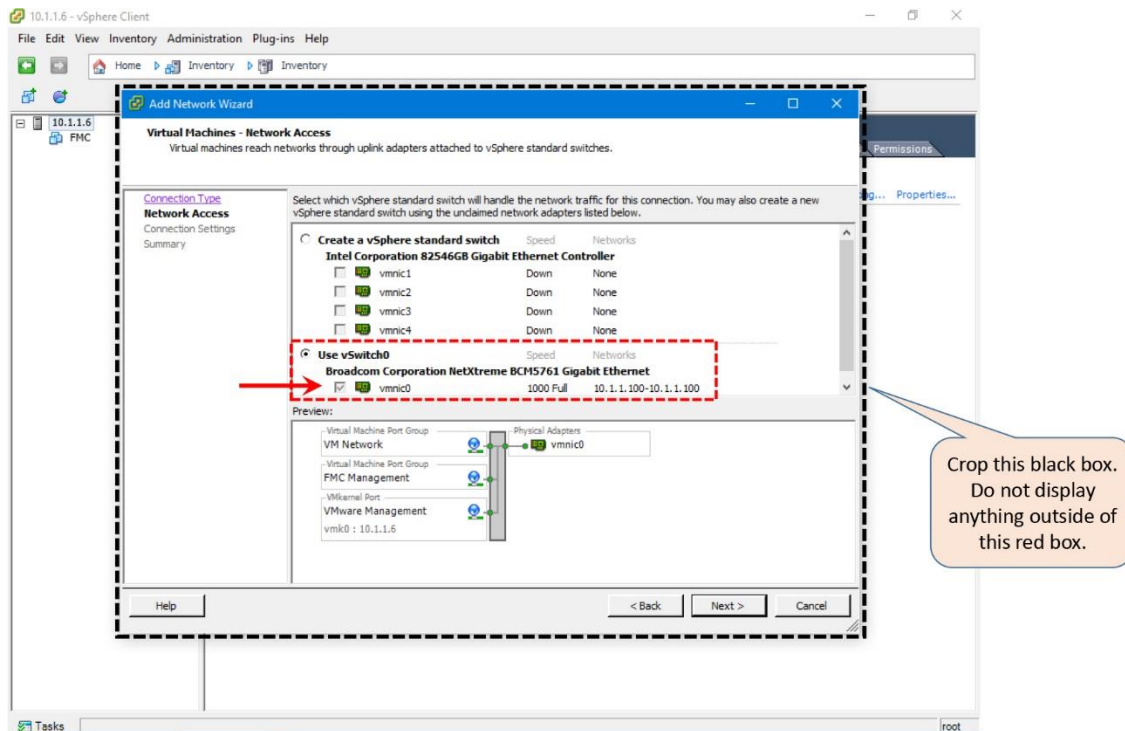


Figure 5-17. Virtual Switch Maps a Virtual Port with a Physical Adapter

Step 5. Replace the default Network Label with a meaningful name.

Figure 5-18 shows the custom Network Label. Here, you can preview the mapping of a virtual port with a physical adapter.

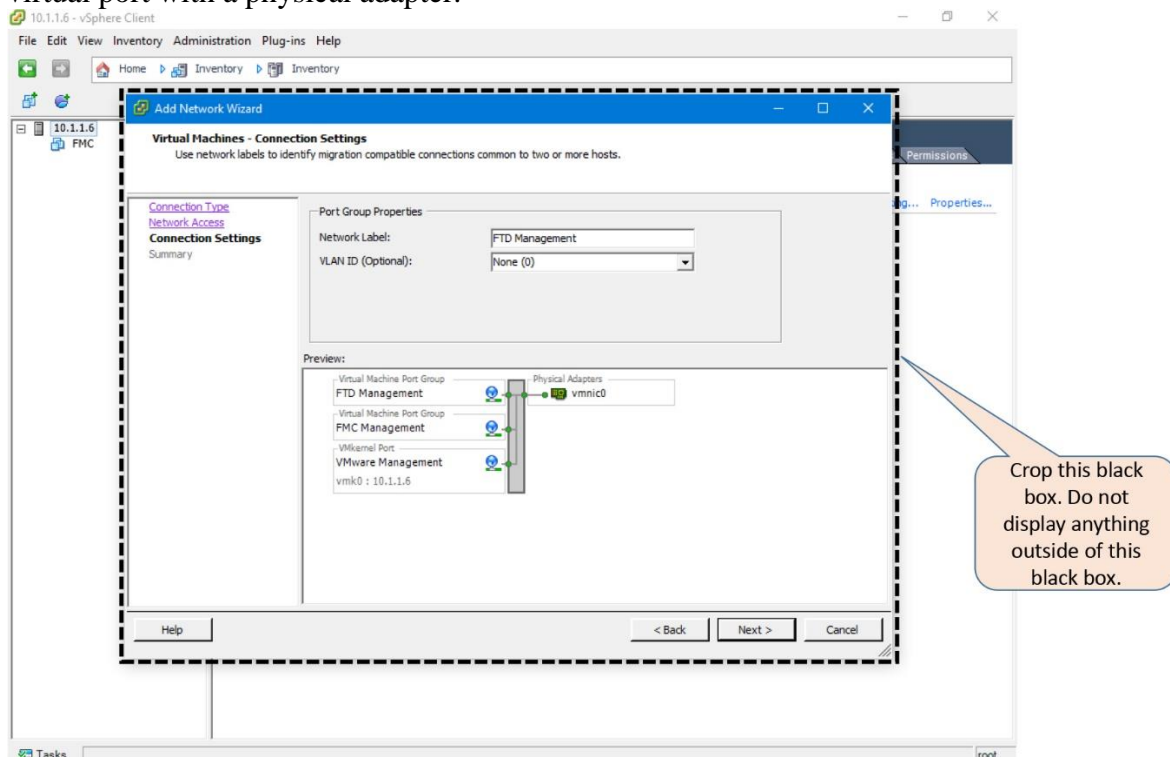


Figure 5-18. *Connections Settings and Port Group Properties of the Network Adapters*

Step 6. Select **Next** to view a summary. Click the **Finish** button to complete the configuration of the vSwitch port group for the FTD Management network.

Step 7. Repeat the previous steps at least three more times to create the remaining three vSwitches that are mandatory on an FTD Virtual appliance.

[Table 5-4](#) shows the mapping between the virtual ports and physical adapters that is used in the configuration example of this chapter.

Virtual Port	Physical Adapter	Purpose
FTD Management	vmnic0	For management traffic
Inside Network	vmnic1	For internal network
Outside Network	vmnic2	Towards the outside world
DMZ Network	vmnic3	Network for the server farm

Table 5-4. *Mapping Between the Virtual Ports and Physical Adapters*

[Figure 5-19](#) shows the final view of the networking configuration page after you create four virtual ports and map them with four individual physical adapters. Each vSwitch is configurable separately using the **Properties** option.

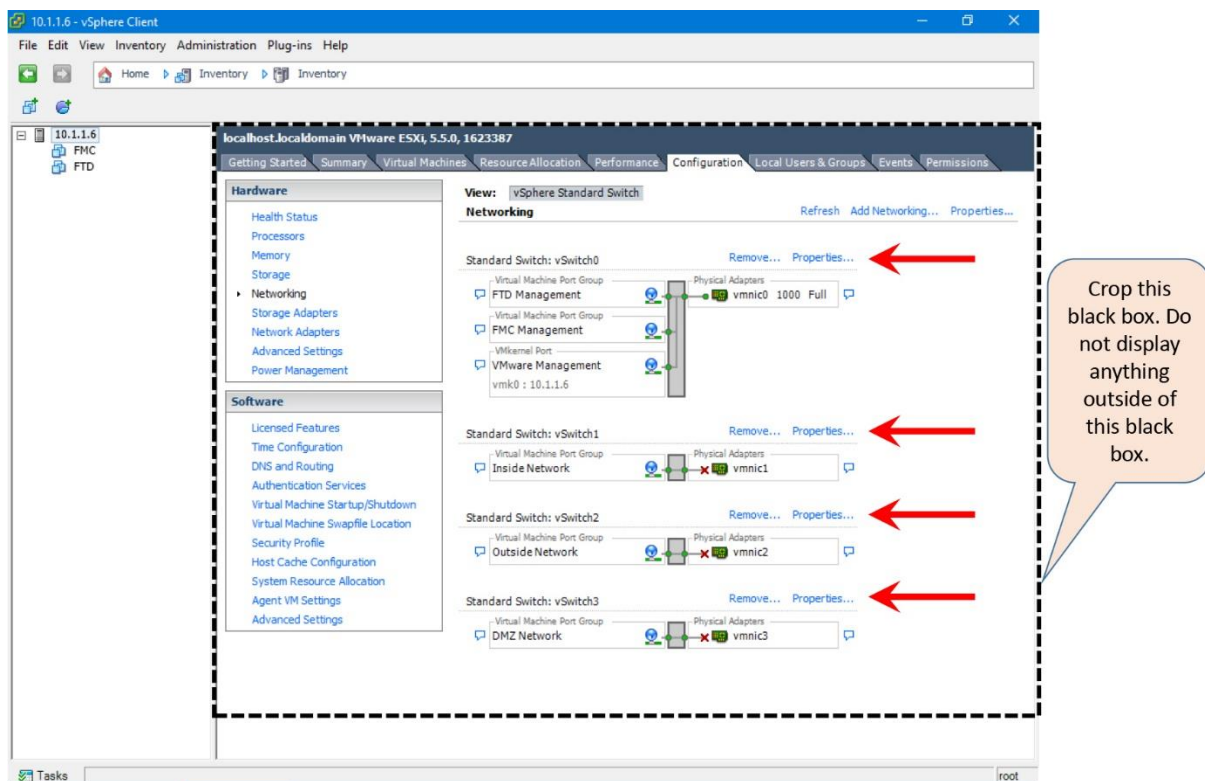


Figure 5-19. *Four Virtual Ports Are Mapped with Four Separate Physical Adapters*

Promiscuous Mode

Promiscuous mode allows a virtual switch to see any frames that traverse through it. By default, it is disabled on a virtual switch. You must enable the promiscuous mode on all of the virtual ports of a Firepower Threat Defense Virtual appliance.

The following steps describe how to enable the promiscuous mode on the management interface of an FTD virtual appliance. By following the same steps, you will be able to enable promiscuous mode on any data interfaces:

Step 1. Select the **Properties** option next to a vSwitch. The **vSwitch Properties** window appears.

[Figure 5-20](#) shows the **vSwitch0 Properties** window. Select any virtual port to find the *Promiscuous Mode* status, which is *Reject*, by default.

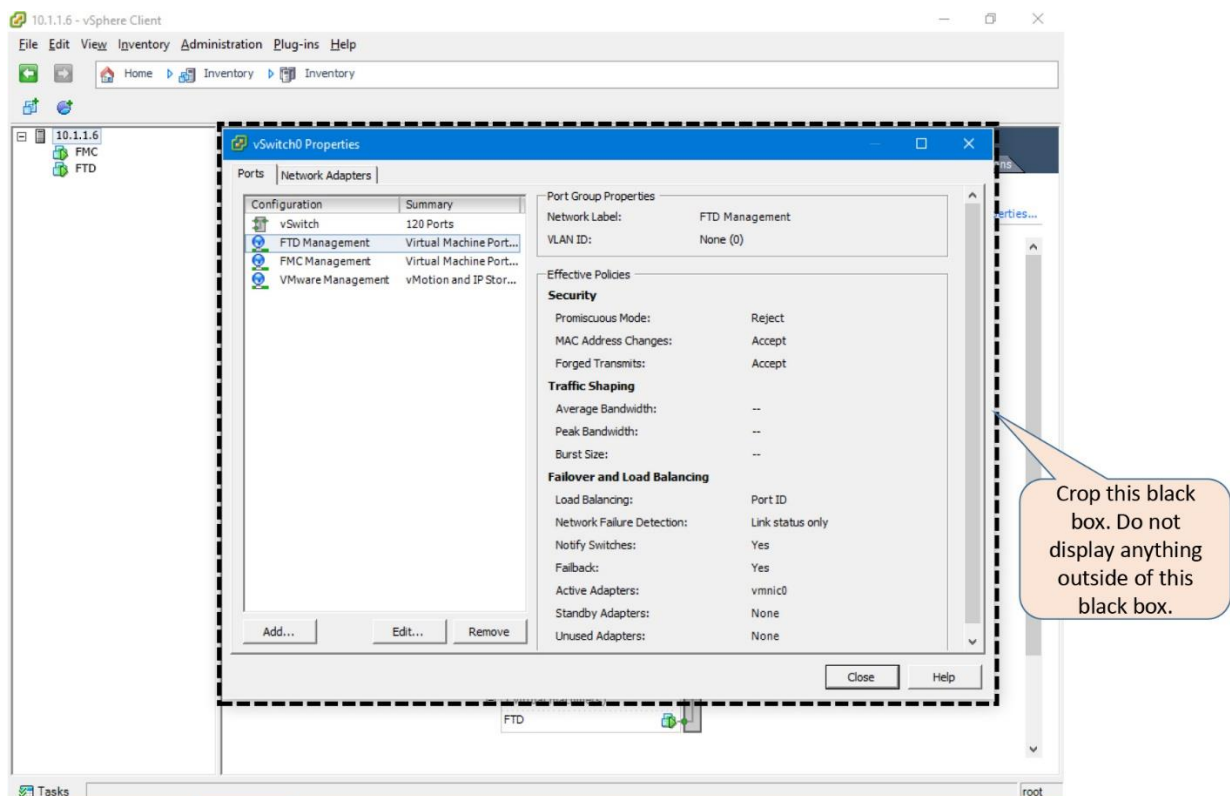


Figure 5-20. *The Properties Option That Allows You Edit a vSwitch*

Step 2. Select the port on which you want to enable the promiscuous mode. Click the **Edit** Button. The **Properties** window appears.

Step 3. Select the **Security** tab. All of the options including the Promiscuous Mode option are unchecked, by default.

Step 4. Check all of the boxes. Select **Accept** from the drop down for all of the options, such as, Promiscuous Mode, MAC Address Changes, and Forged Transmits.

[Figure 5-21](#) shows all of the **Policy Exceptions** for a vSwitch are checked. *Promiscuous Mode* is now selected as *Accept*.

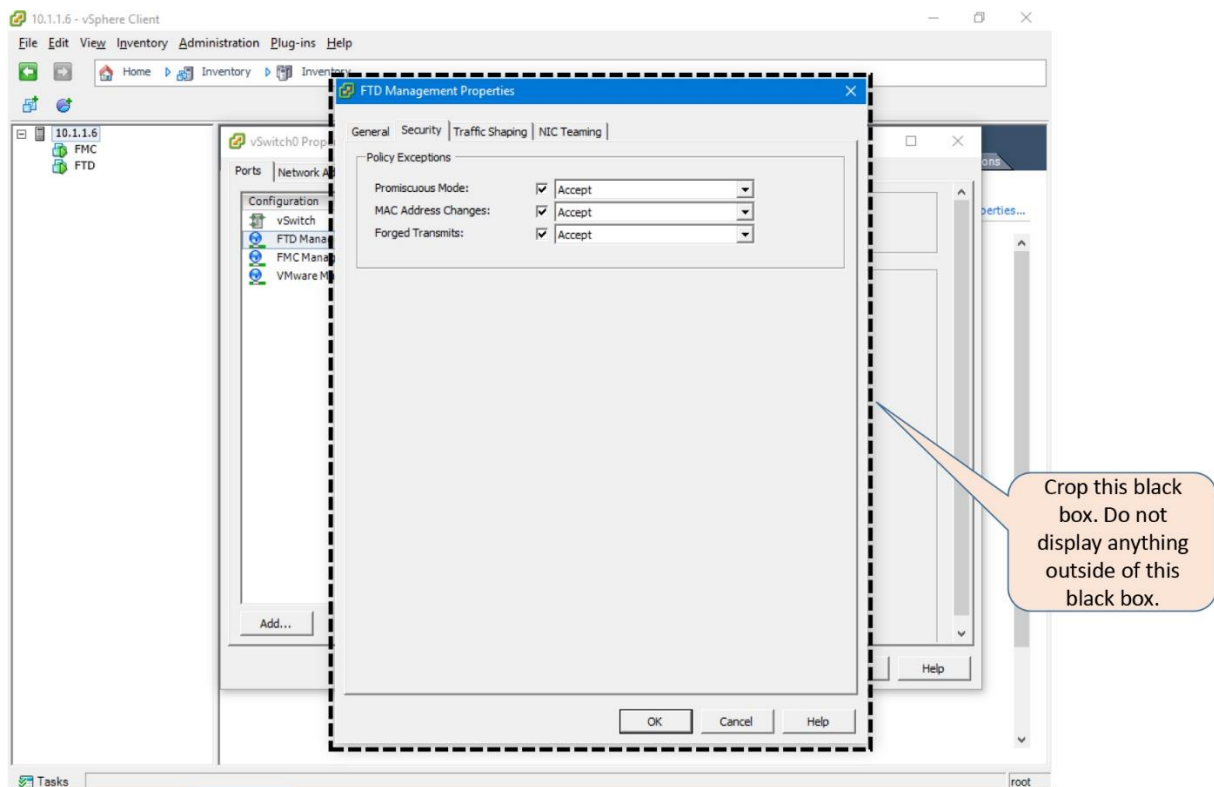


Figure 5-21. *Promiscuous Mode Along with Other Options is Enabled*

Step 5. Once you are done, select **OK** to return to the **vSwitch Properties** window. Click the **Close** button to complete the configuration.

Step 6. Repeat all of the previous steps for all of the interfaces on an FTD virtual appliance. This is a requirement.

Deployment of an OVF Template

After building a layer 2 topology in the VMware, the next step is to deploy an OVF template file into an ESXi host. Use the following steps to deploy an OVF file:

Step 1. From the **File** menu, select the **Deploy OVF Template...** option. The **Deploy OVF Template** window appears.

Figure 5-22 shows the **Deploy OVF Template** option in the File menu of a vSphere client.

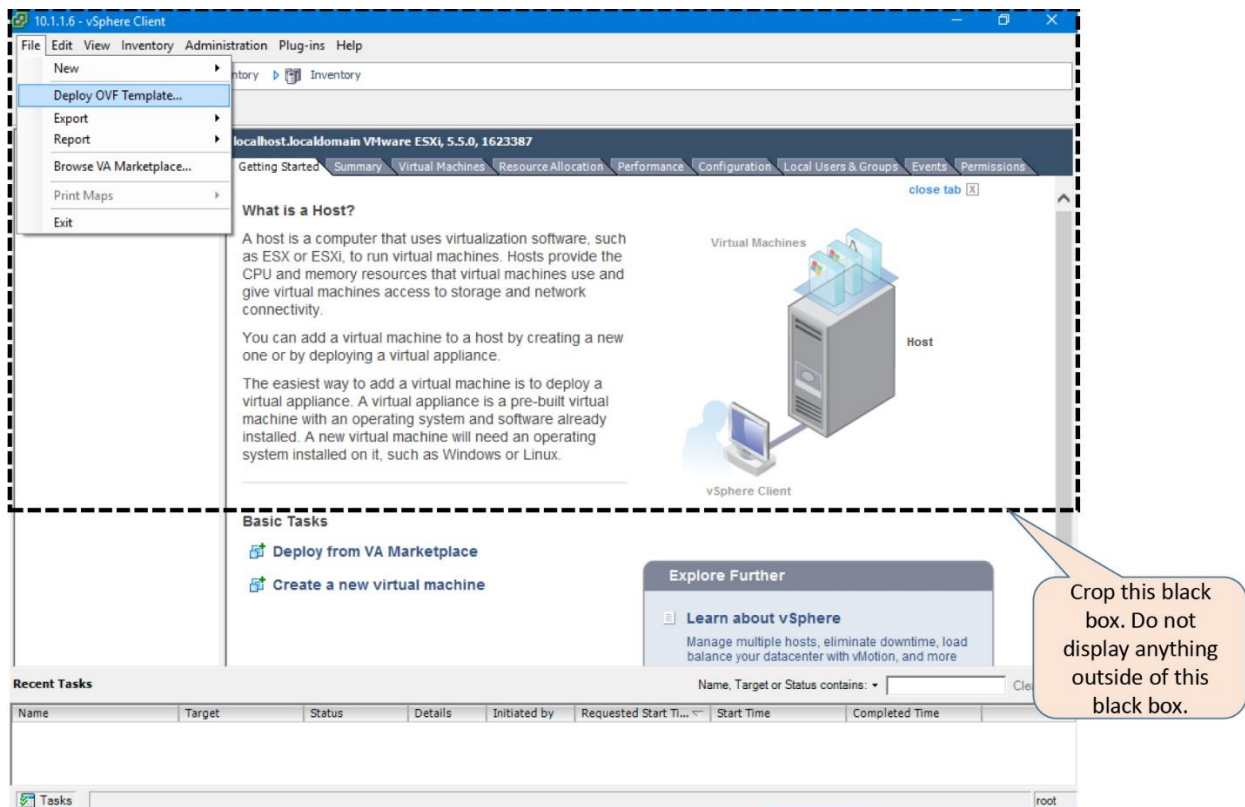


Figure 5-22. Navigation of the *Deploy OVF Template* Option in a vSphere Client

Step 2. Browse an appropriate OVF file for your virtual appliance. Select **Next** to continue.

Note

If you want to deploy an FMC Version 6.1 on an ESXi host, select the Cisco_Firepower_Management_Center_Virtual_VMware-ESXi-6.1.0-330.ovf file. Similarly, to deploy an FTD Version 6.1, select the Cisco_Firepower_Threat_Defense_Virtual-ESXi-6.1.0-330.ovf file.

[Figure 5-23](#) shows the Cisco_Firepower_Threat_Defense_Virtual-ESXi-6.1.0-330.ovf file is selected for deployment.

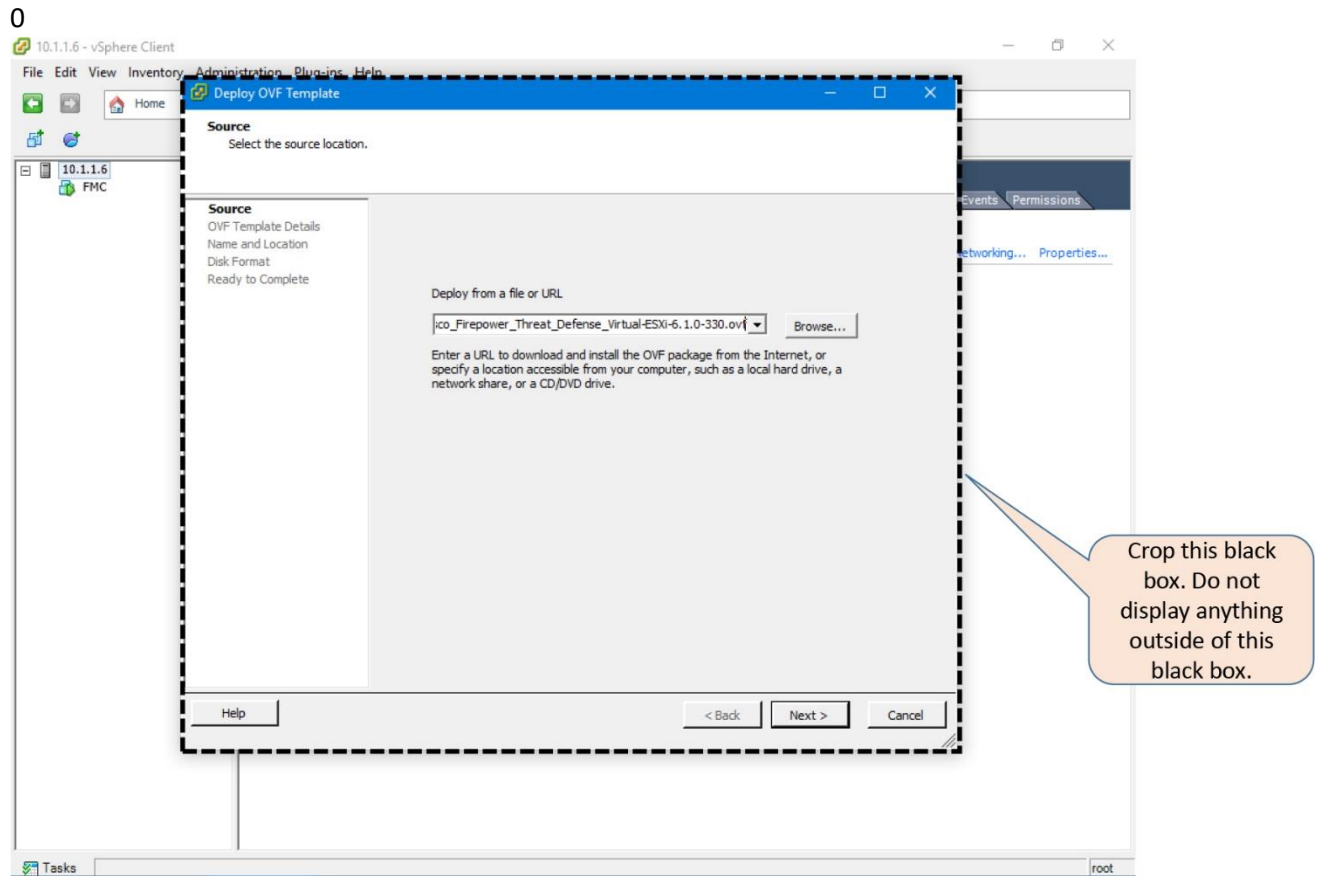


Figure 5-23. Selection of an OVF File in the Deploy OVF Template

Step 3. Verify the information on the OVF Template Detail. If everything looks good, select **Next** to continue.

[Figure 5-24](#) shows the OVF Template Details. Verify that all of the information looks good.

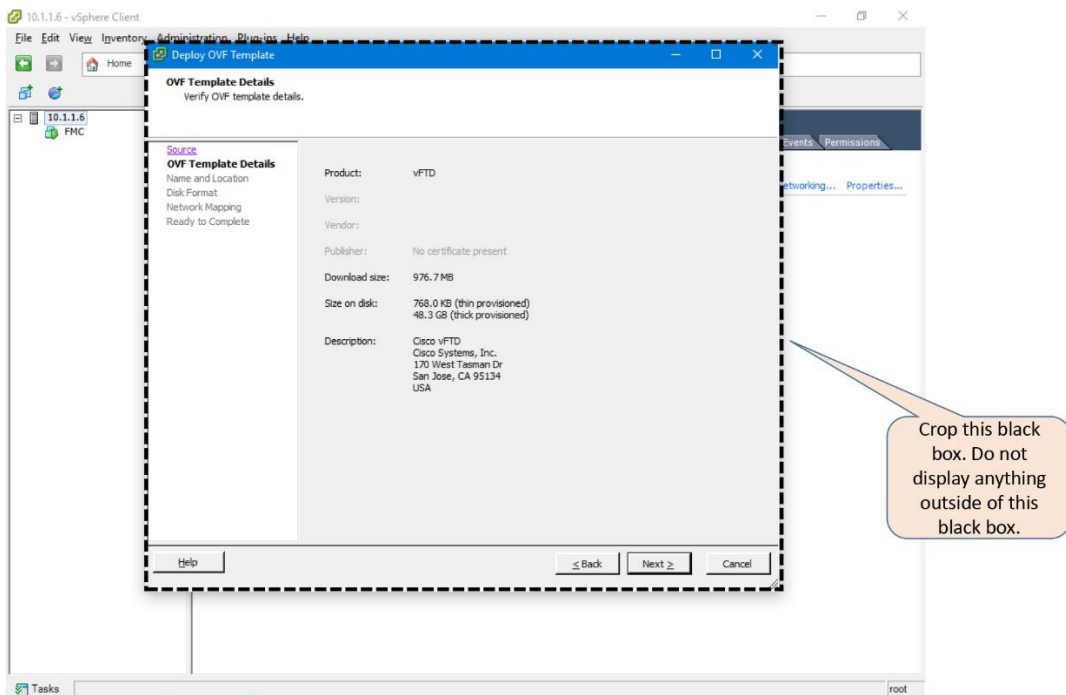


Figure 5-24. Detail Description of an OVF Template

Step 4. Specify a unique name for your virtual appliance, and click **Next**.

[Figure 5-25](#) shows a custom name "FTD" for the virtual appliance. This must be unique within an inventory.

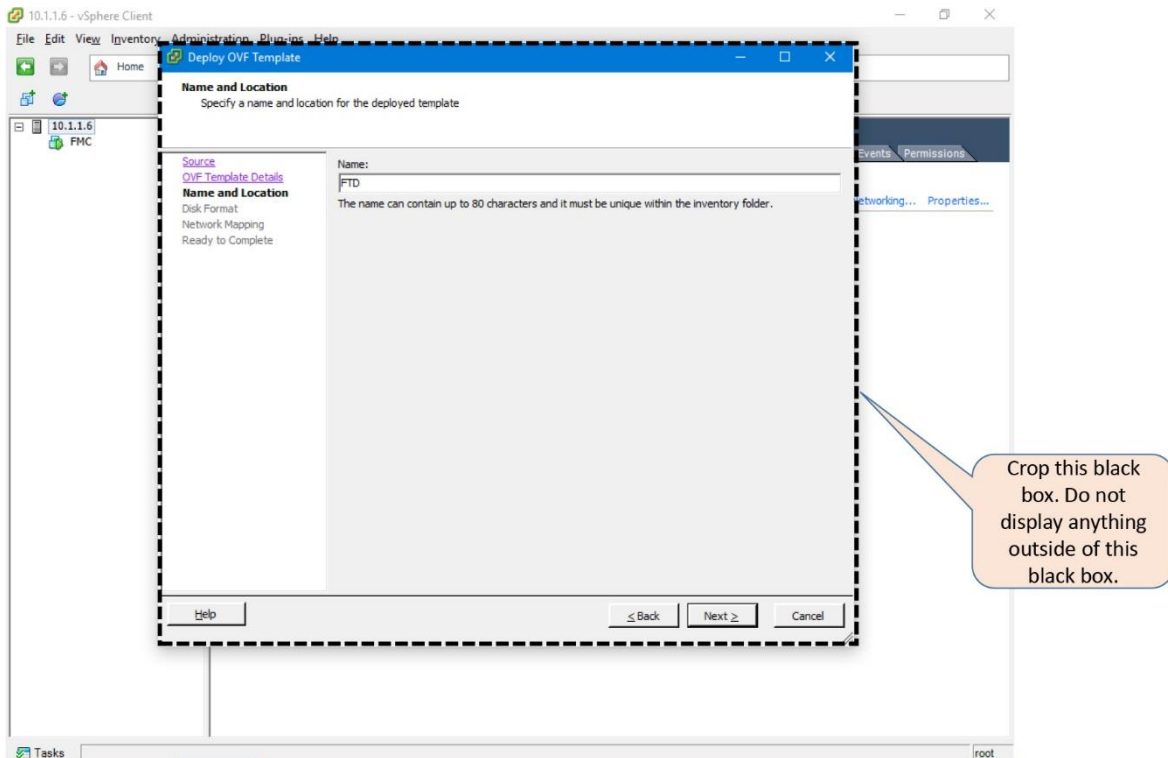


Figure 5-25. *Custom Name for a Deployed Template*

Step 5. Select a **Disk Format** type for your virtual disk, and click **Next**.

Tips

Read the Essential Knowledge section to learn about different types of disk format.

[Figure 5-26](#) shows the **Thick Provisioned Lazy Zeroed** is selected as the **Disk Format**.

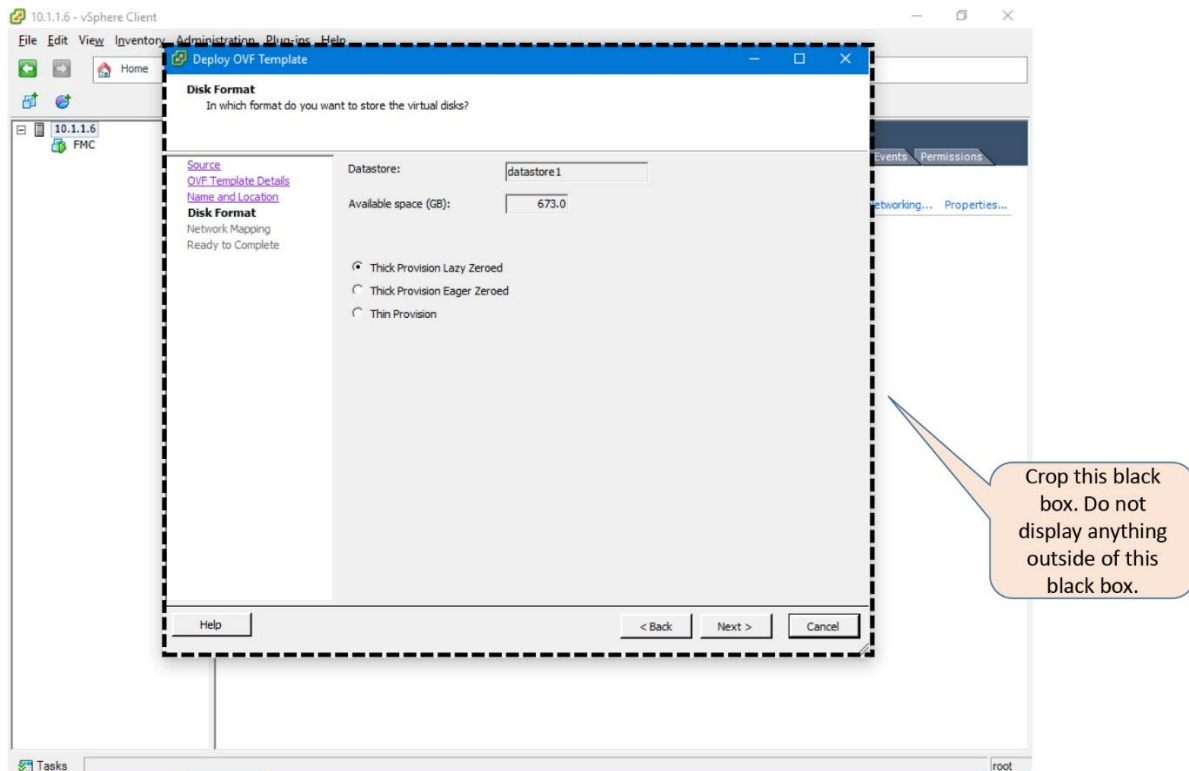


Figure 5-26. *Disk Format Options for a Virtual Appliance*

Step 6. Map the Destination Networks (virtual ports) with the Source Networks (interfaces on a virtual appliance). Use the drop down to find an appropriate interface.

Note

The number of network you need to map depends on the type of a virtual appliance. An FMC and FTD must have at least one and four interfaces respectively.

[Figure 5-27](#) shows the selection of the “FTD Management” virtual port for the management interface of an FTD virtual appliance.

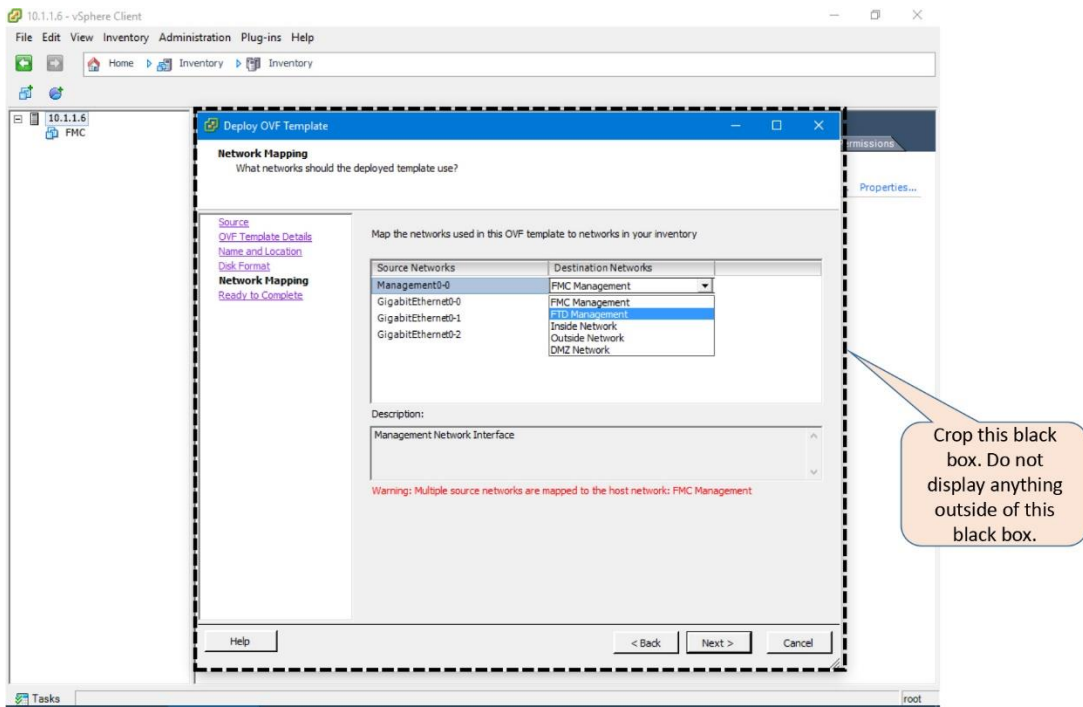


Figure 5-27. Drop Down Menu is Used to Select a Virtual Port

[Figure 5-28](#) shows all of the interfaces on an FTD virtual appliance after they are mapped with separate virtual ports.

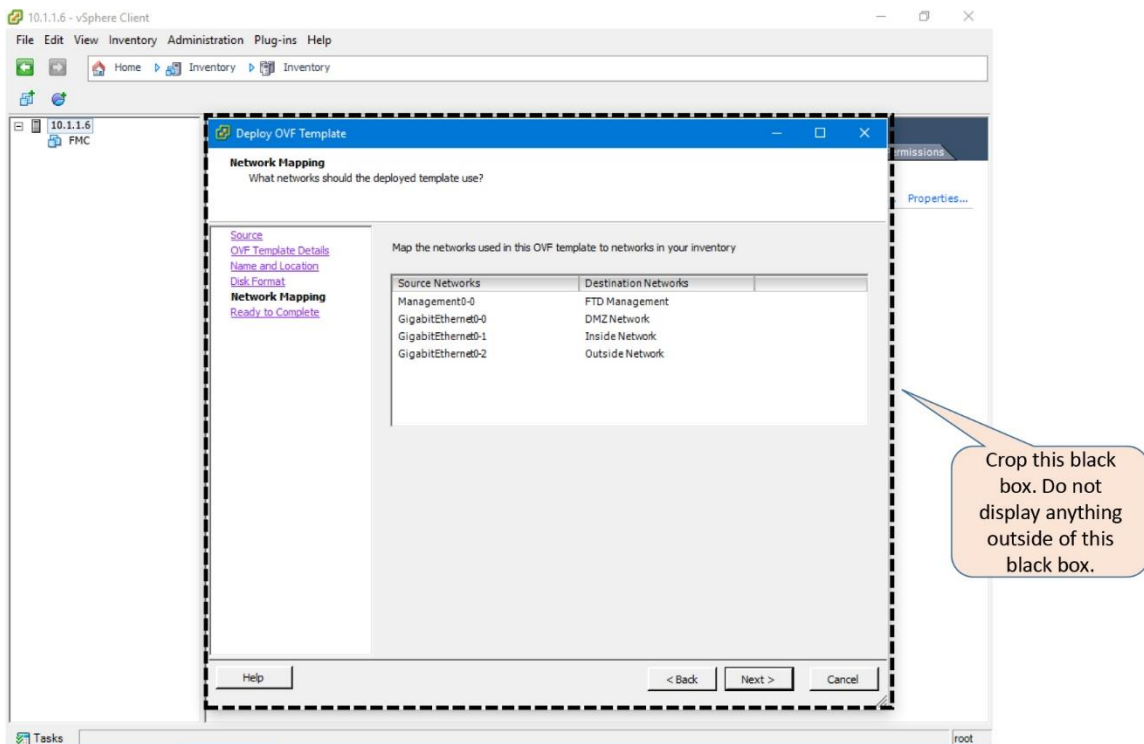


Figure 5-28. Complete Mapping of All of the Networks

Step 7. Once you finish mapping the network, select **Next**. A summary of all of the settings will be displayed. If everything looks good, click **Finish** to complete the configuration.

[Figure 5-29](#) shows a summary of all of the settings of the FTD virtual appliance that is one-click way from being deployed.

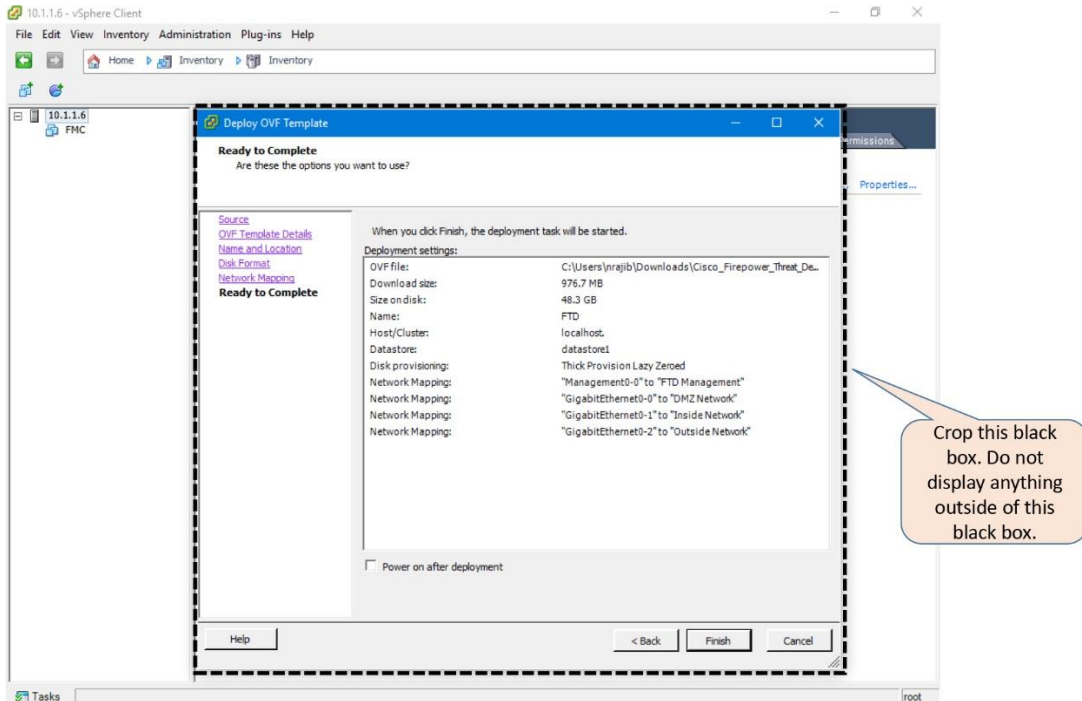


Figure 5-29. Final Prompt to Confirm the Settings of an FTD Virtual Deployment

[Figure 5-30](#) shows, just to provide you with an example, a summary of all of the pre-deployment settings of an FMC virtual appliance.

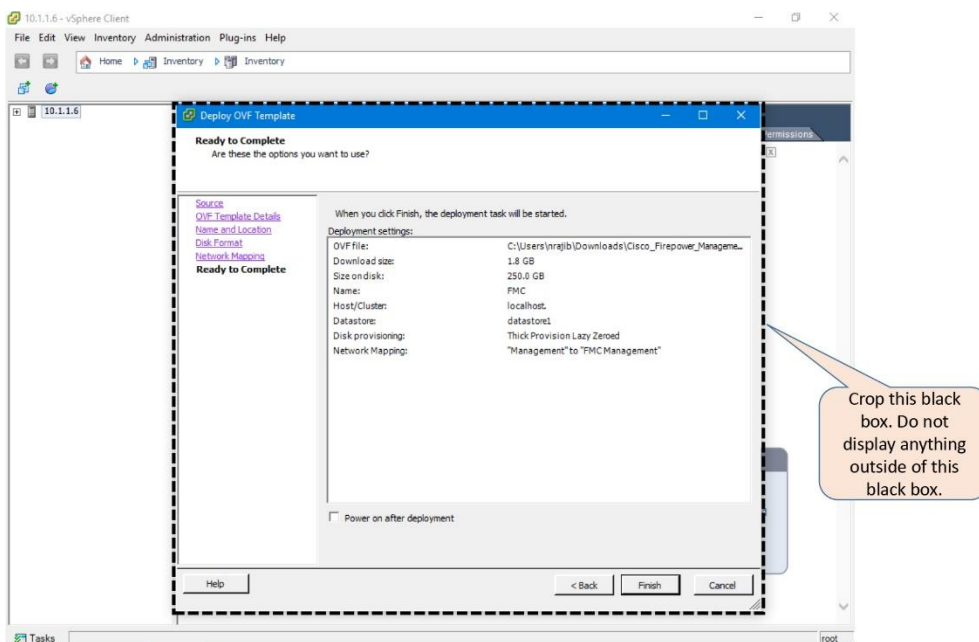


Figure 5-30. Final Prompt to Confirm the Settings of an FMC Virtual Deployment

Step 8. The deployment begins. The duration to complete a deployment depends on various factors, such as, the type of Firepower virtual appliance you are deploying, the amount of resources available in the ESXi host, and the connection speed between the ESXi server and the endpoint where the OVF file is stored. Once complete, a confirmation message appears in a **Deployment Completed Successfully** window.

[Figure 5-31](#) shows a confirmation for a successful virtual appliance deployment.

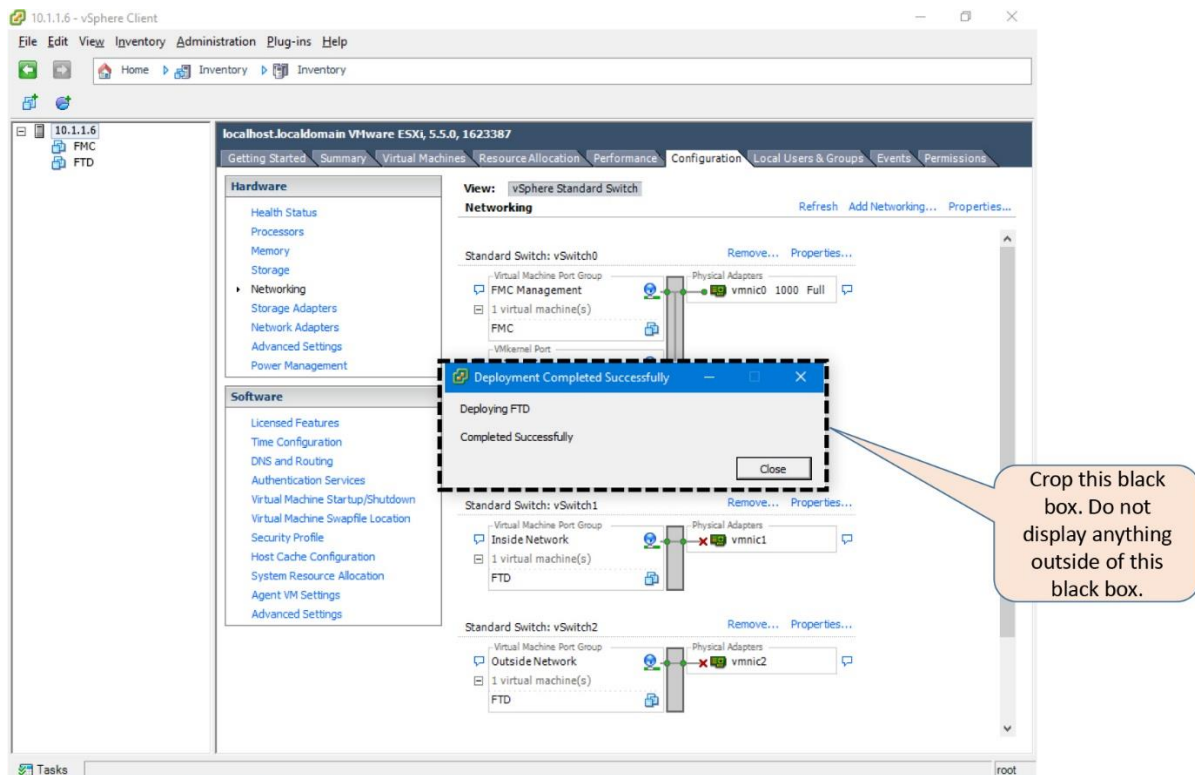


Figure 5-31. Completion of a Successful FTD Deployment

Initialization of an Appliance

Use the following process to begin the initialization of any Firepower virtual appliances (either FMC or FTD):

Step 1. Select the desired virtual appliance from the inventory.

Step 2. Go to the **Getting Started** tab.

Step 3. Click on the Power on the virtual machine option.

Step 4. The initialization begins, you can view the status in the **Console** tab.

[Figure 5-32](#) shows the **Power on the virtual machine** option in the Getting Started page.

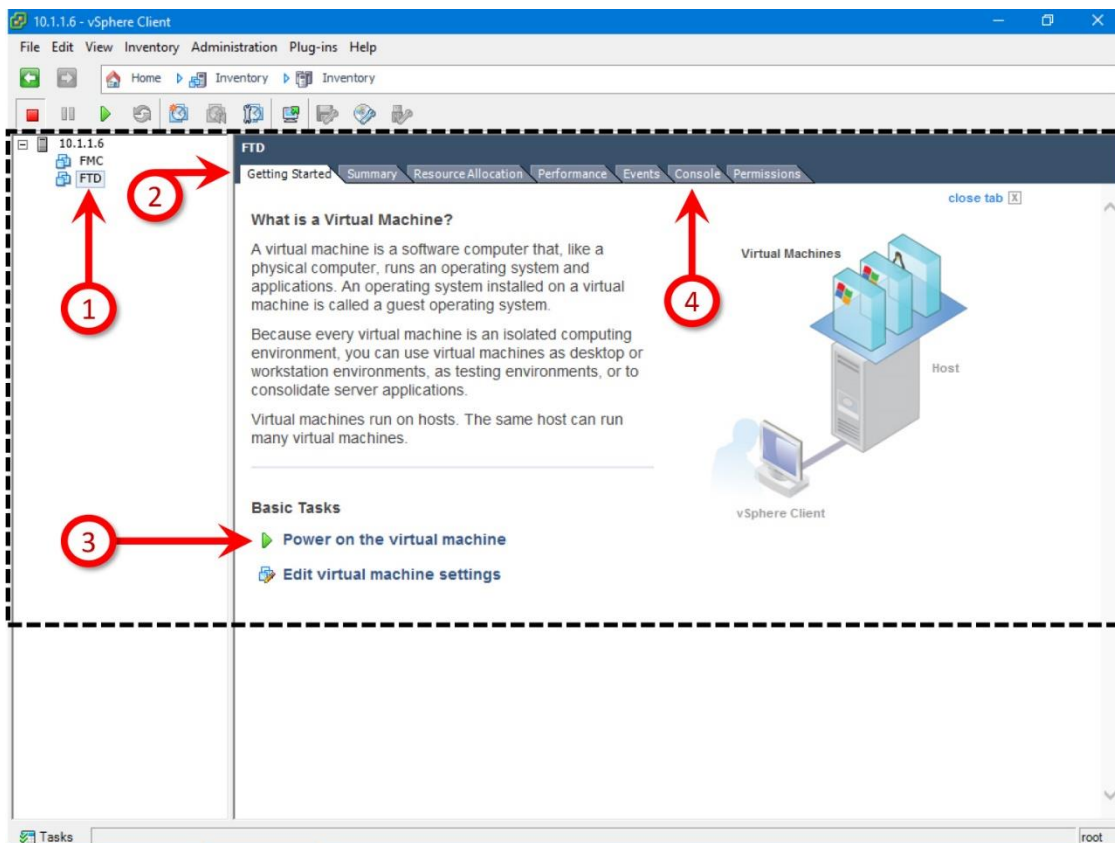


Figure 5-32. *Beginning an Initialization Process and Watching the Status on the Console Tab*

[On an FMC Virtual Appliance](#)

On an FMC Virtual appliance, the initialization process ends automatically after 40-50 minutes. You can view the status on the **Console** tab. At the end of the process, a login prompt appears.

[Example 5-1](#) shows the completion of the Firepower software initialization on VMware. Once complete, you can enter the CLI using the default credentials — username **admin** and password **Admin123**.

Example 5-1 *Login Prompt of an FMC Virtual Appliance Appears After the Initialization is Complete*

```
Cisco Firepower Management Center for VMWare v6.1.0 (build 330)
Oct 18 13:20:23 firepower SF-IMS[616]: [616] init script:system [INFO]
pmmon Starting the Process Manager...
Oct 18 13:20:23 firepower SF-IMS[617]: [617] pm:pm [INFO] Using model
number 66E
Sad7: WRITE SAME failed. Manually zeroing.
```

```
Cisco Firepower Management Center for VMWare v6.1.0 (build 330)
Firepower login:admin
Password:Admin123
```

Copyright 2004-2016, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.1.0 (build 37)
Cisco Firepower Management Center for VMWare v6.1.0 (build 330)

admin@firepower:~\$

[On an FTD Virtual Appliance](#)

On an FTD Virtual appliance, the initialization process ends in approximately 20 minutes. At the end of the process, a login prompt appears. You can enter the CLI using the default credentials — username **admin** and password **Admin123**.

[Example 5-2](#) exhibits the initialization process of a FTD virtual appliance on VMware. The process prompts for an End User License Agreement (EULA) acceptance and network configuration, before a login prompt appears.

Example 5-2 *Login Prompt of an FTD Virtual Appliance Does Not Appear Until the EULA is Accepted and the Management Network is Configured*

```
Cisco Firepower Threat Defense for VMWare v6.1.0 (build 330)
Firepower login:admin
Password:Admin123
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
.
.
.
Output Omitted
.
.
.
Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress. Please stand by.
You must change the password for 'admin' to continue.
Enter new password:
Confirm new password:
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]:
10.1.1.21
Enter an IPv4 netmask for the management interface [255.255.255.0]:
Enter the IPv4 default gateway for the management interface [192.168.45.1]:
10.1.1.1
Enter a fully qualified hostname for this system [firepower]:
Enter a comma-separated list of DNS servers or 'none' []: none
Enter a comma-separated list of search domains or 'none' []: none
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...
Update policy deployment information
```

- add device configuration
- add network discovery
- add system policy

You can register the sensor to a Firepower Management Center and use the Firepower Management Center to manage it. Note that registering the sensor to a Firepower Management Center disables on-sensor Firepower Services management capabilities.

When registering the sensor to a Firepower Management Center, a unique alphanumeric registration key is always required. In most cases, to register a sensor to a Firepower Management Center, you must provide the hostname or the IP address along with the registration key.

```
'configure manager add [hostname | ip address ] [registration key ]'
```

However, if the sensor and the Firepower Management Center are separated by a NAT device, you must enter a unique NAT ID, along with the unique registration key.

```
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'
```

Later, using the web interface on the Firepower Management Center, you must use the same registration key and, if necessary, the same NAT ID when you add this sensor to the Firepower Management Center.

```
>
```

The '>' prompt, at the end [Example 5-2](#), confirms that the installation is totally complete.

The next step is to verify the network connectivity on the management interface and begin the registration process. Please read the [Chapter 6](#), "Firepower Management Network," to learn about the registration process.

Verification and Troubleshooting Tools

In this section, you will learn how to investigate some common issues with a Firepower virtual appliance. If you experience any issues with the ESXi host operating system, you should find and read a troubleshooting guide in the VMware website.

Determine the Status of Allocated Resources

The amount of resource allocated to a Firepower virtual appliance is very critical for its system performance. You can verify the resource allocation in two different places of a vSphere Center:

- **Summary View:** The Summary page of a virtual appliance provides you an overview of the deployed OVF template and its allocated resources.

Figure 5-33 shows the allocated CPU, memory, storage, etc. of an FMC virtual appliance.

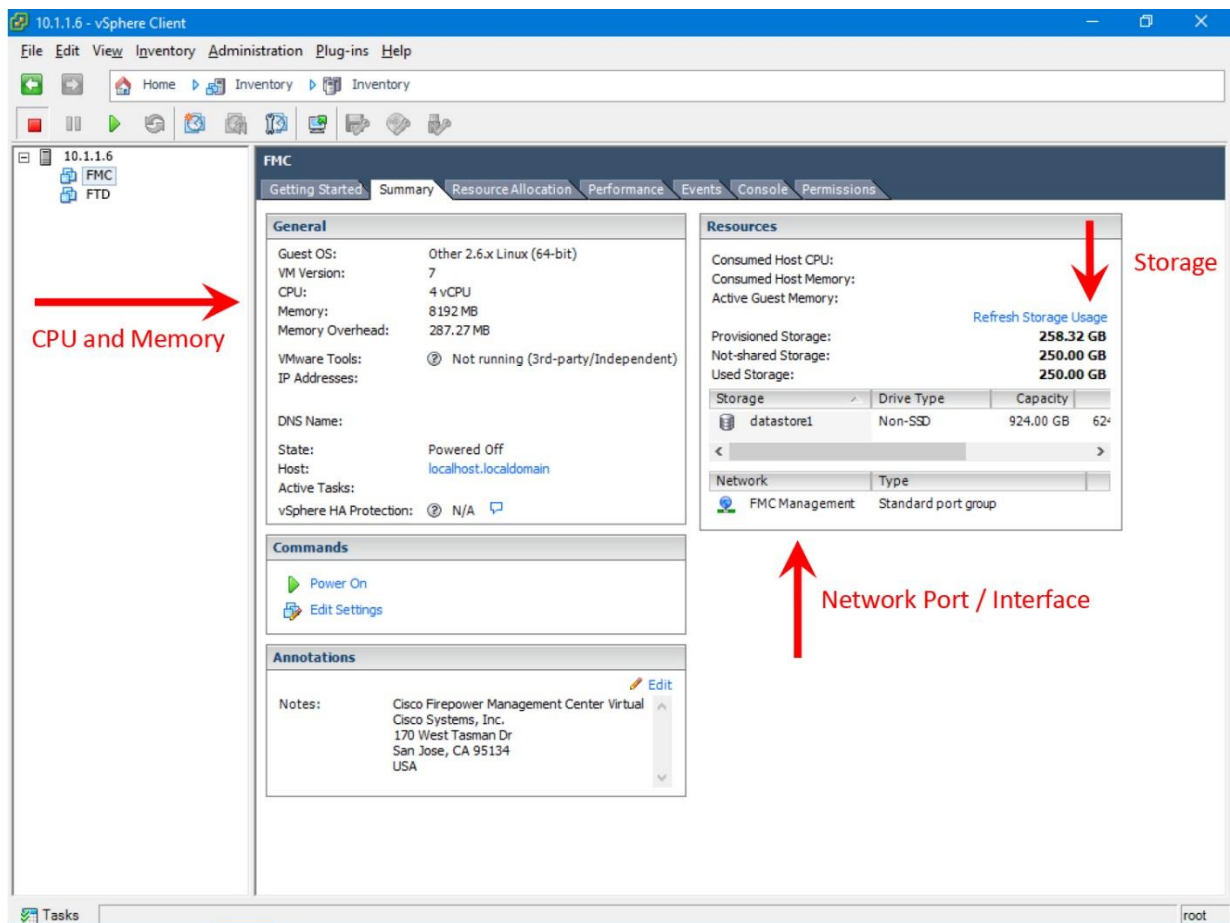


Figure 5-33. Summary of the Resource Allocations

- **Virtual machine settings editor:** The editor allows you to view, add or remove resources allocated to a virtual machine. There are two ways to navigate to the virtual machine settings editor:
 - Right-click on the name of a virtual appliance from the inventory list. Select the **Edit Settings** option. The **Virtual Machine Properties** window appears.
 - Go to the Getting Started page, and click on the virtual machine settings option under Basic Tasks. The Virtual Machine Properties window appears.

Figure 5-34 shows the options to edit the settings of a virtual appliance.

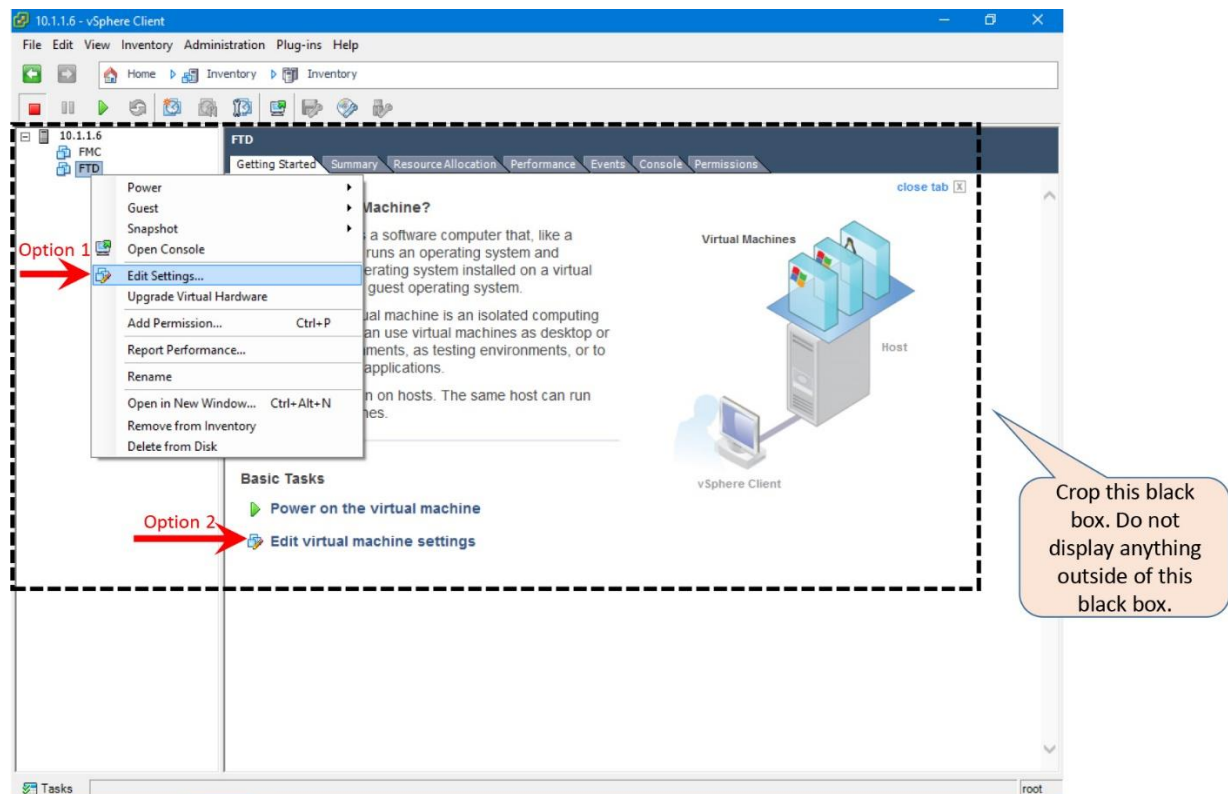


Figure 5-34. Navigation to the Virtual Machine Settings Editor

Determine the Status of a Network Adapter

If you notice any management or data interface on your Firepower virtual appliance does not show up or stays always down, you need to verify the network adapter configuration of that virtual appliance. To verify an adapter using a vSphere client use the following steps:

Step 1. From the inventory list, select the virtual appliance that does not display an interface properly.

Step 2. Edit the virtual machine settings (as it is described in the previous section). The **Virtual Machine Properties** window appears.

Step 3. From the hardware list, select the **Network Adapter** that is not functioning properly.

Step 4. Check the **Device Status** on the right side of the window, and make sure both options — **Connected** and **Connect at power on** — are checked.

[Figure 5-35](#) shows the status of the FTD management interface. It is currently connected, and configured to be connected when the FTD virtual appliance is powered on.

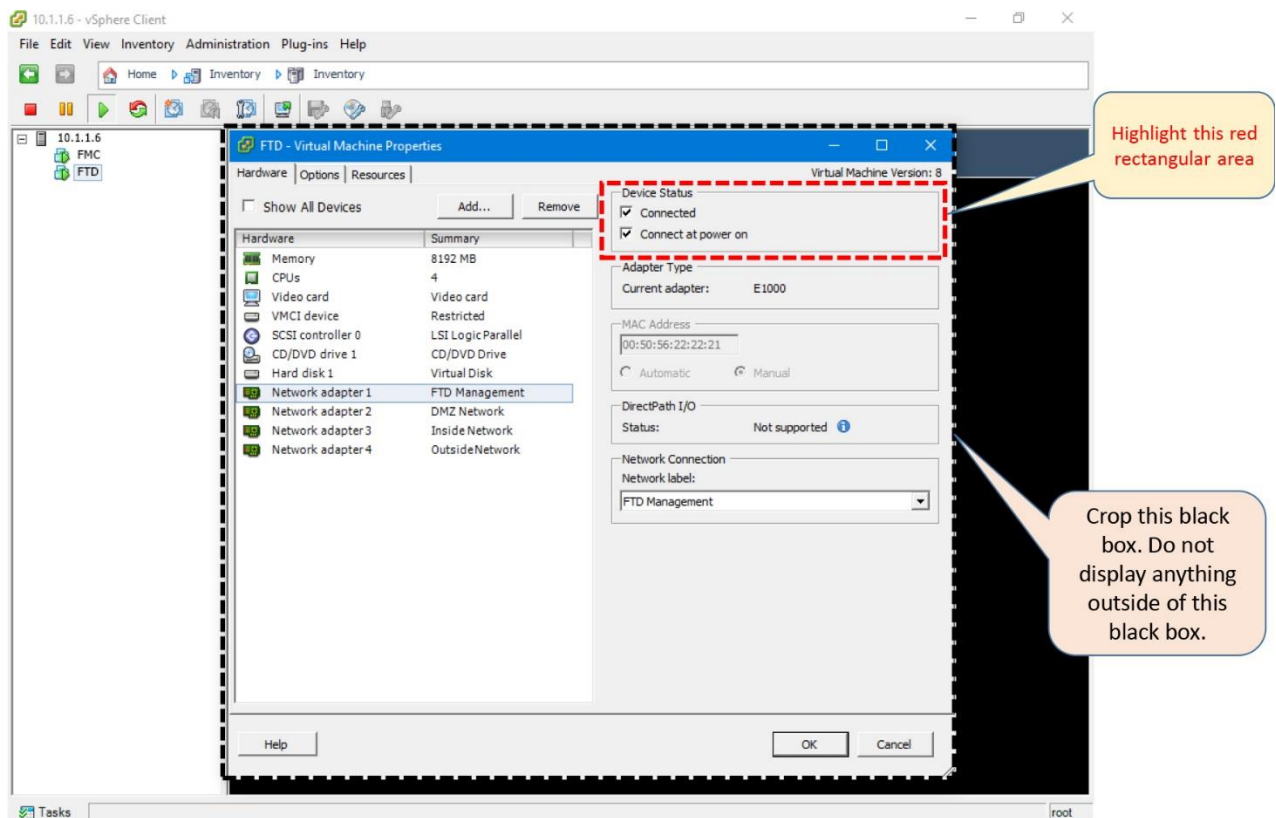


Figure 5-35. *Connected and Connect at Power On Options of a Network Adapter*

Tip

Do you still experience an issue with a network adapter? Did you complete all of the steps when you enabled promiscuous mode? Go back to [Figure 5-20](#) and [Figure 5-21](#), and verify if your vSwitch properties match the settings shown on those images.

Upgrade of a Network Adapter

When you deploy a virtual appliance, VMware uses the E1000 network adapter by default. You can also choose a VMXNET3 adapter for your Firepower virtual appliance. The difference between an E1000 and a VMXNET3 adapter is in throughput. The throughput of a VMXNET3 adapter is 10 Gbit/s whereas an E1000 adapter supports up to 1 Gbit/s.

The types of all of the adapters on any given virtual appliance have to be the same. In other words, if you want to upgrade the type of an adapter, you must upgrade it for all of the interfaces on any single virtual interface. It is, however, not a requirement to have same type of network adapters on all of the virtual appliances in any network. For example, if the management interface of an FMC virtual appliance is an E1000 adapter, it should be able to communicate with an FTD virtual appliance that has the VMXNET3 type network adapters.

To upgrade a network adapter from the default type E1000 to VMXNET3 use the following steps:

Step 1. Gracefully shutdown the virtual appliance on which a new adapter will be added. Run the **shutdown** command on the console.

```
admin@FMCv:~$ sudo shutdown -h now
```

Caution

Do not power off a virtual appliance manually. It may corrupt the Firepower System database. Instead, issue the shutdown command from the VMware console.

Step 2. Edit the virtual machine settings and open the **Virtual Machine Properties** window.

[Figure 5-36](#) shows all of the hardware resources that are allocated to an FTD virtual appliance in the **FTD – Virtual Machine Properties** window.

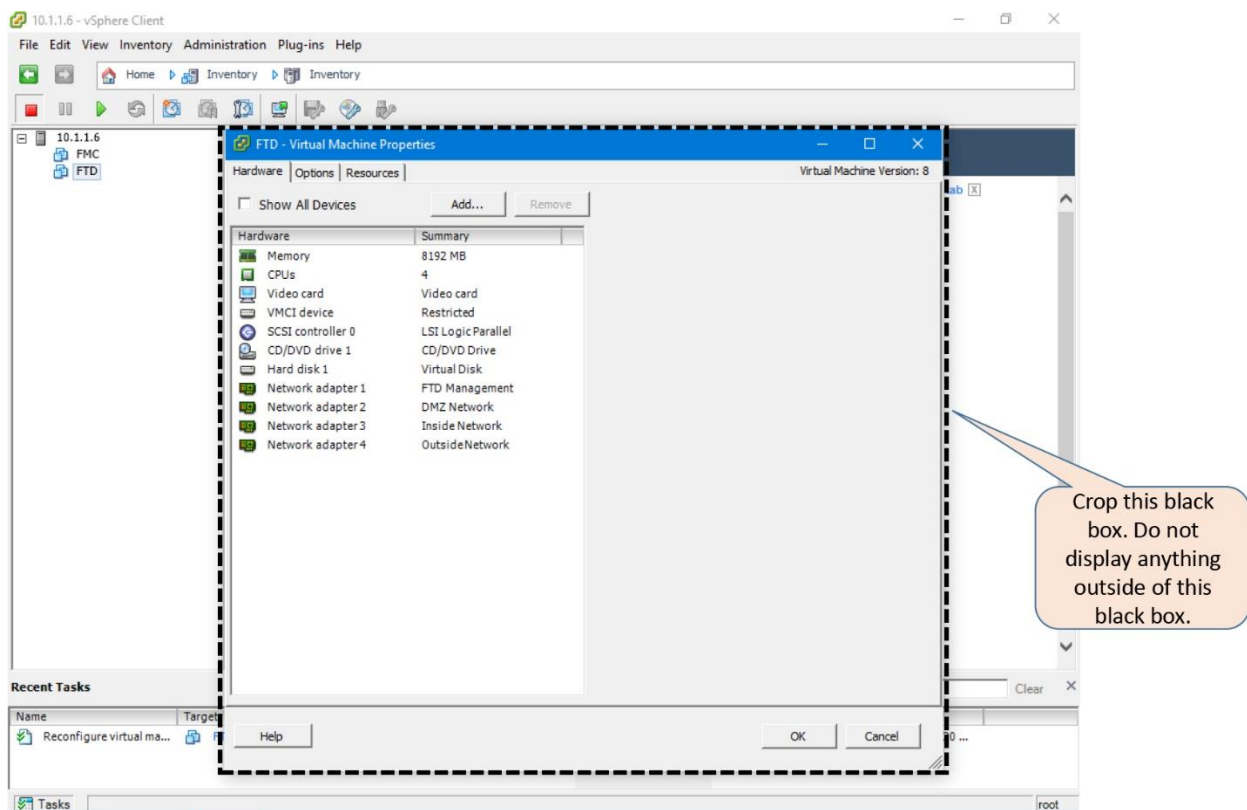


Figure 5-36. The FTD Virtual Machine Properties Window

Step 3. Using the **Remove** button, delete the Network Adapter that you want to upgrade from E1000 to VMXNET3

Step 4. Now, add a new VMXNET3 interface. To add an interface, select the **Add** button in the Virtual Machine Properties window. The **Add Hardware** window appears. Select **Ethernet Adapter** from the device list.

[Figure 5-37](#) shows a list of available virtual devices that could be added into a virtual appliance. Only an Ethernet Adapter could be added.

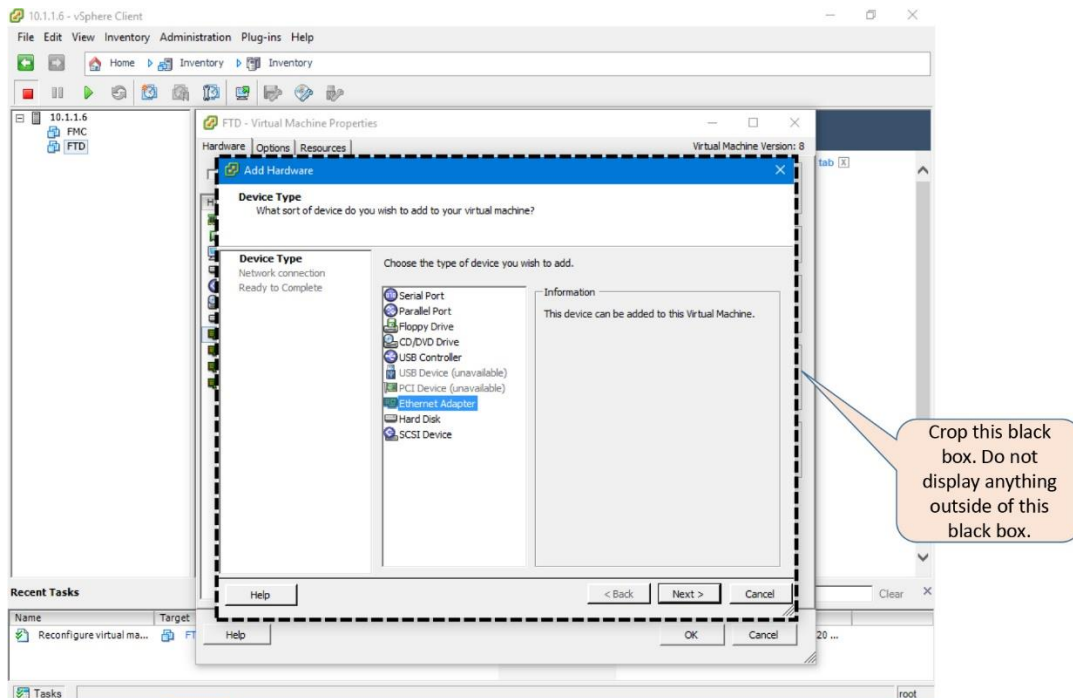


Figure 5-37. *The Add Hardware Window*

Step 5. Next, you select **VMXNET3** from the **Adapter Type** drop-down.

[Figure 5-38](#) shows three types of network adapter — E1000, VMXNET2 (Enhanced), and VMXNET3. As of writing this book, Firepower software does not support the VMXNET2 (Enhanced) adapter.

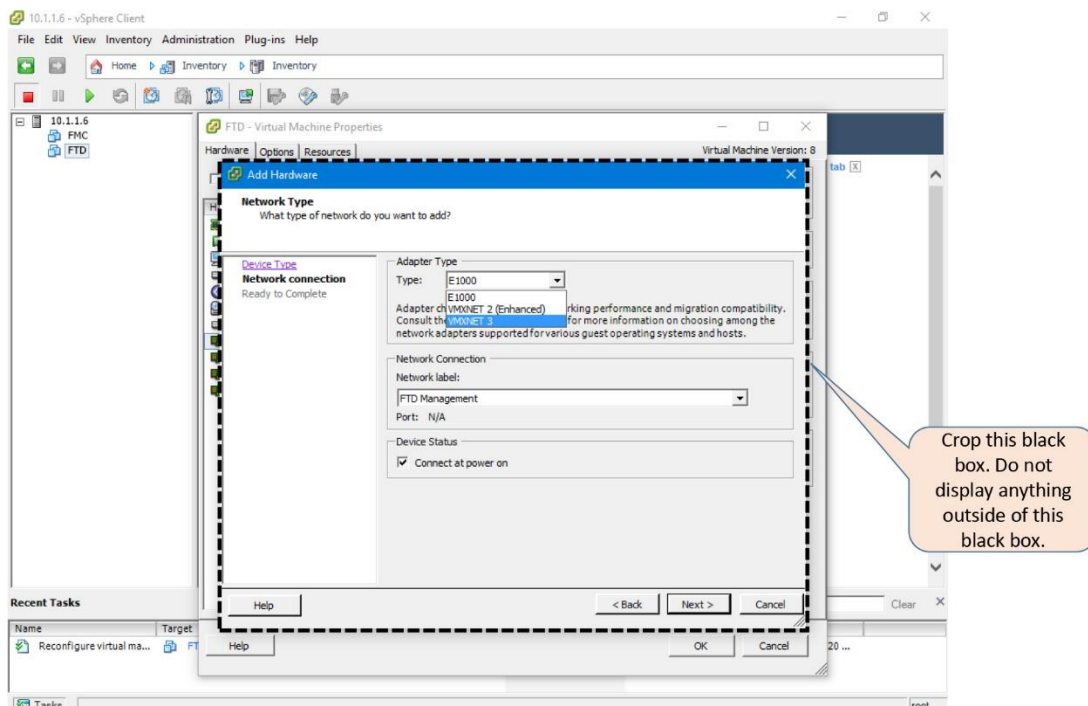


Figure 5-38. Available Adapter Types in VMware ESXi

Step 6. Make sure the **Network Label** (association of a network with an adapter) is accurate, and the **Connect at power on** is checked. Click **Next** if when you are done.

Step 7. When you are in **Ready to Complete** section, select **Finish** if everything looks good.

[Figure 5-39](#) shows all of the adapter settings, and prompts you to complete the configuration.

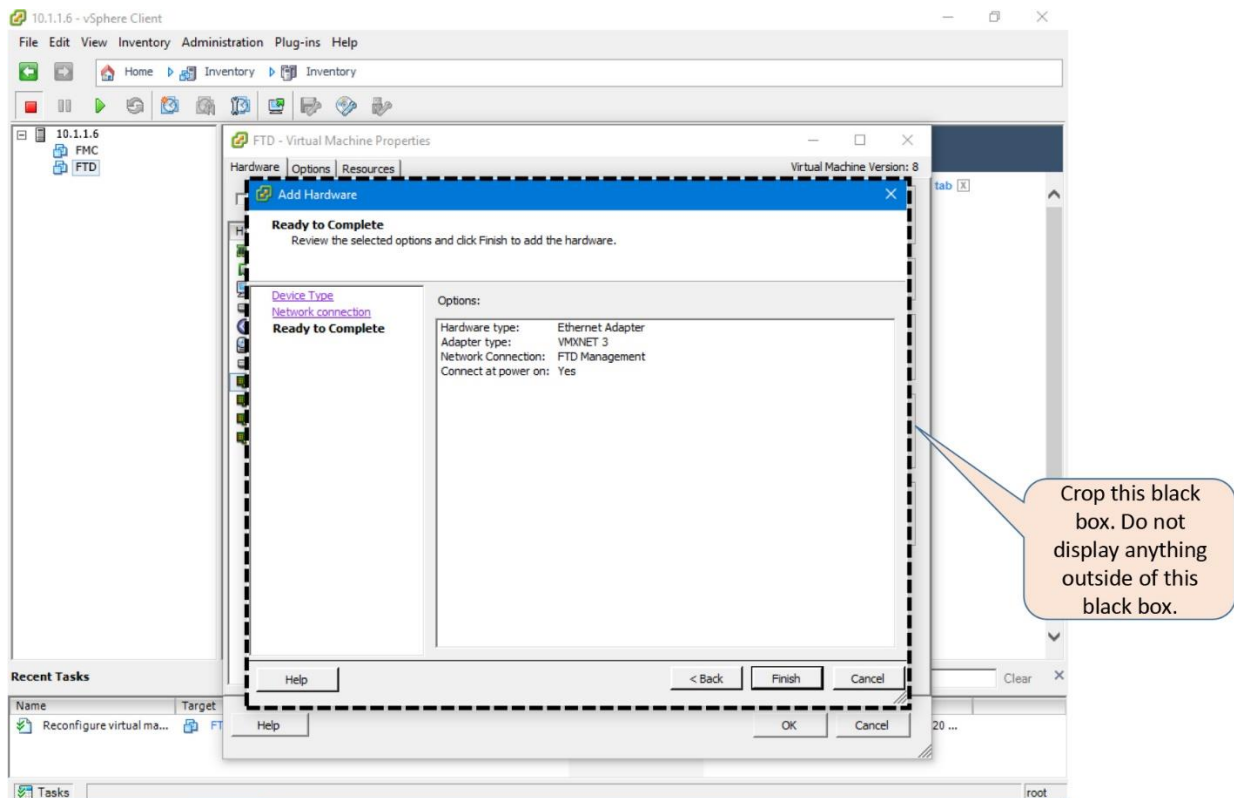


Figure 5-39. An Overview of the Ethernet Adapter Options

Step 8. If your virtual appliance has more than one network adapter (For example, an FTD Virtual appliance must have at least four interfaces), perform the previous seven steps multiple times to upgrade all of the other adapters to the same type.

Figure 5-40 shows the Virtual Machine Properties window after the management interface is replaced with a VMXNET3 adapter.

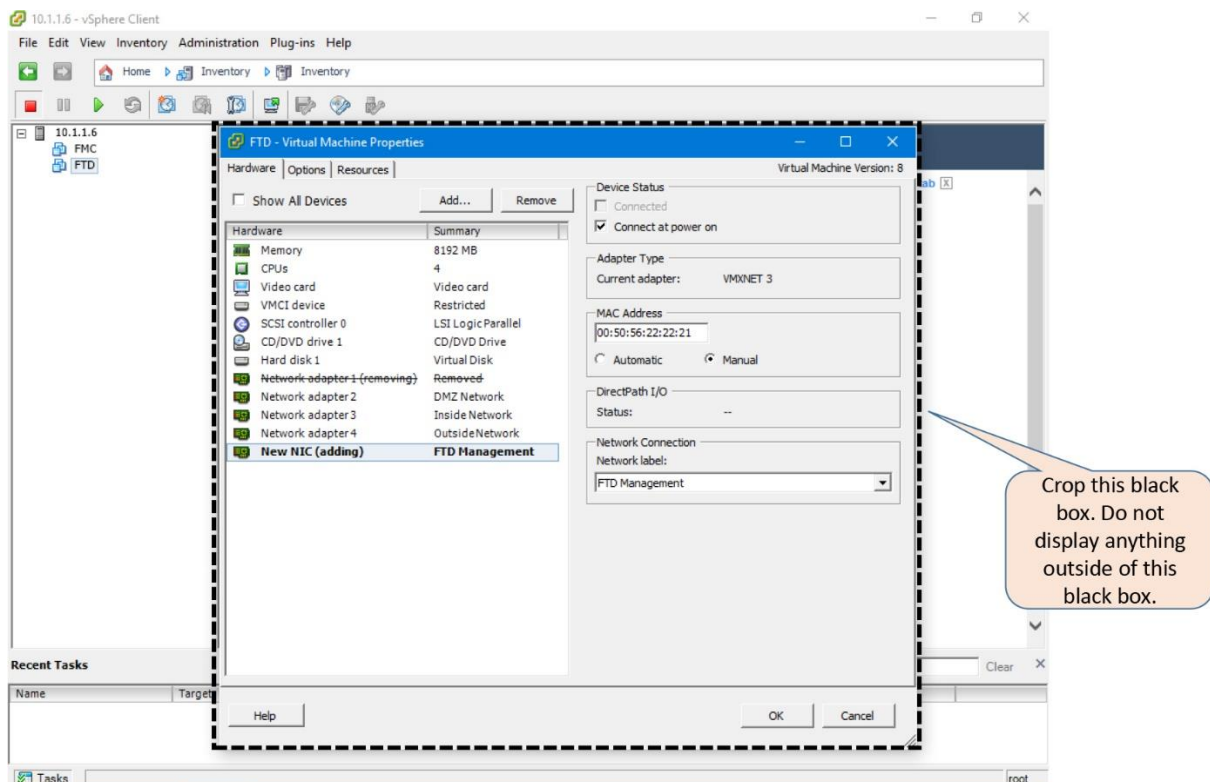


Figure 5-40. Replacement of an E1000 Adapter with VMXNET3

Step 9. Select **OK** in the **Virtual Machine Properties** Window to save the changes, and power on the virtual appliance.

Summary

This chapter describes various aspects of the Firepower virtual appliance. You have learned how to deploy a virtual appliance, how to tune the resources for optimal performance, and how to investigate issues with a new deployment.

Quiz

1. Which file can be deployed directly into an ESXi?
 - a. TAR.GZ
 - b. VMDK
 - c. OVF
 - d. MF
2. Which network adapter provides the maximum throughput?

- a. E1000
- b. VMXNET2 (Enhanced)
- c. VMXNET3
- d. VMXNET-X

3. Which of the following option should not contribute to any connectivity issues between two Firepower virtual appliances?

- a. Network adapter is configured as connected
- b. Connected at power on option is checked
- c. Promiscuous mode is enabled
- d. Network adapter type of two appliances are different

4. Which of the following resources should not be adjusted on an FMC?

- a. Network Adapter
- b. Storage
- c. Memory
- d. CPU

5. Which of the following statement is false?

- a. An OVF file for VI completes the initial setup before deployment.
- b. You cannot adjust the resource allocations on an FTD virtual appliance to improve its performance.
- c. An FTD virtual appliance must need at least four interfaces.
- d. A large deployment can be scaled by cloning an FTD using VMware.

Chapter 6. Firepower Management Network

After you install the Firepower software, the next question that might come in your mind would be how to manage a Firepower Threat Defense (FTD) system? For a smaller network, you may use the browser based on-box application — the Firepower Device Manager (FDM) — that can manage one FTD device with limited functionalities. However, for a medium to large-scale network, you must use the Firepower Management Center (FMC). Regardless of how you want to manage your FTD, it is important that you properly design and configure the management network to secure the control traffic.

Essential Knowledge

Before you begin the registration process, it is important to ensure that the FMC and FTD can communicate with each other, and they are deployed in an appropriate location in the network. In this section, you will learn an anatomy of the Firepower management interface, and various design scenarios of the Firepower management network.

FTD Management Interface

Firepower system uses the management interface to send and receive the control traffic. Depending on the hardware platform, the implementation of a management interface is different. The following section describes how a management interface works on FTD.

- **On an Adaptive Security Appliance (ASA):** On a Cisco ASA 5500-X Series hardware, the management interface is located at the rear panel of a ASA hardware, next to the console port.

[Figure 6-1](#) exhibits the location of the management interface on the ASA 5500-X Series hardware models.

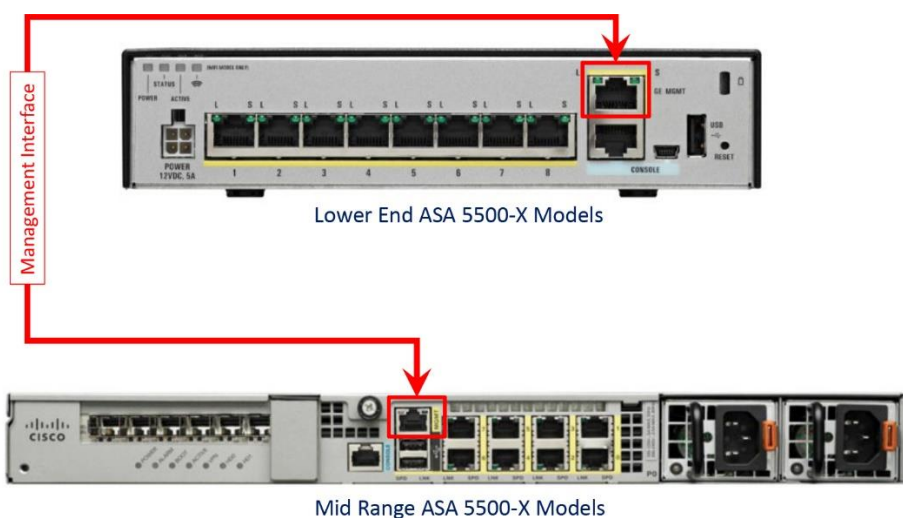


Figure 6-1. Location of the Management Interface on ASA Hardware

A physical management interface on an ASA comprises two logical interfaces — one logical management interface, and one logical diagnostic interface.

FTD uses the logical management interface to complete the registration process with an FMC, and to establish a secure tunnel with that FMC. The tunnel, thereafter, is used to setup the FTD, apply policies to FTD, and to transfer event from FTD to FMC. During the FTD installation process, when you provide an IP address for the FTD management interface, it is actually assigned to the logical management interface.

[Figure 6-2](#) illustrates the relations between different logical interfaces with different software codes, and how they are displayed on the CLI.

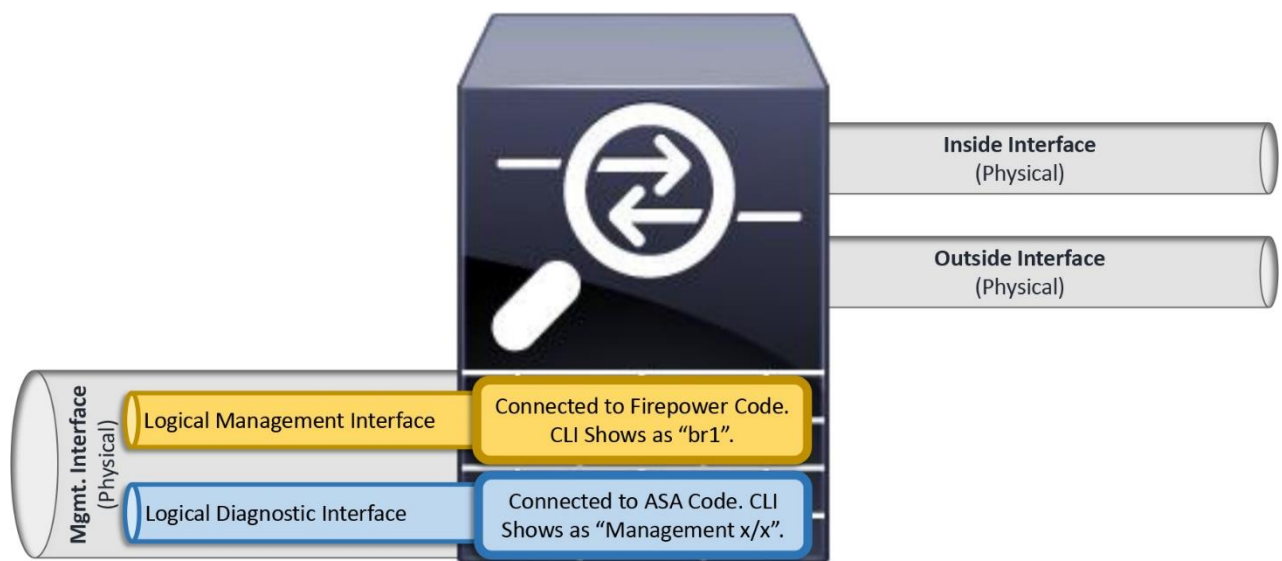


Figure 6-2. *Logical Interfaces of an ASA*

The diagnostic interface, on the other hand, is an optional logical interface. Cisco recommends you not to configure the diagnostic interface with an IP address if there is no router between the management network and inside network. It also simplifies your network design and reduces configuration overhead.

Note

Each of the data interface on an FTD is required to be on different network. When a diagnostic interface is configured with an IP address, the FTD considers it as a data interface. Therefore, the diagnostic interface (which must be on the same subnet as the logical management interface, br1) and the inside interface must be on two different subnets. To transfer traffic between two different subnetworks, a router is necessary.

- **On a Firepower Security Appliance:** Each Firepower security appliance has one fixed management interface on the front panel of the chassis. Using this interface, you can administer the Firepower eXtensible Operating System (FXOS). An FTD logical device, however, does not use this interface to communicate with an FMC. For the management communication between an FTD and FMC, select any of remaining Ethernet ports and configure it (with the `mgmt. type`) using the Firepower Chassis Manager. The configuration steps are described later in this chapter.

[Figure 6-3](#) shows the location of the management interface on the Firepower Security Appliance.

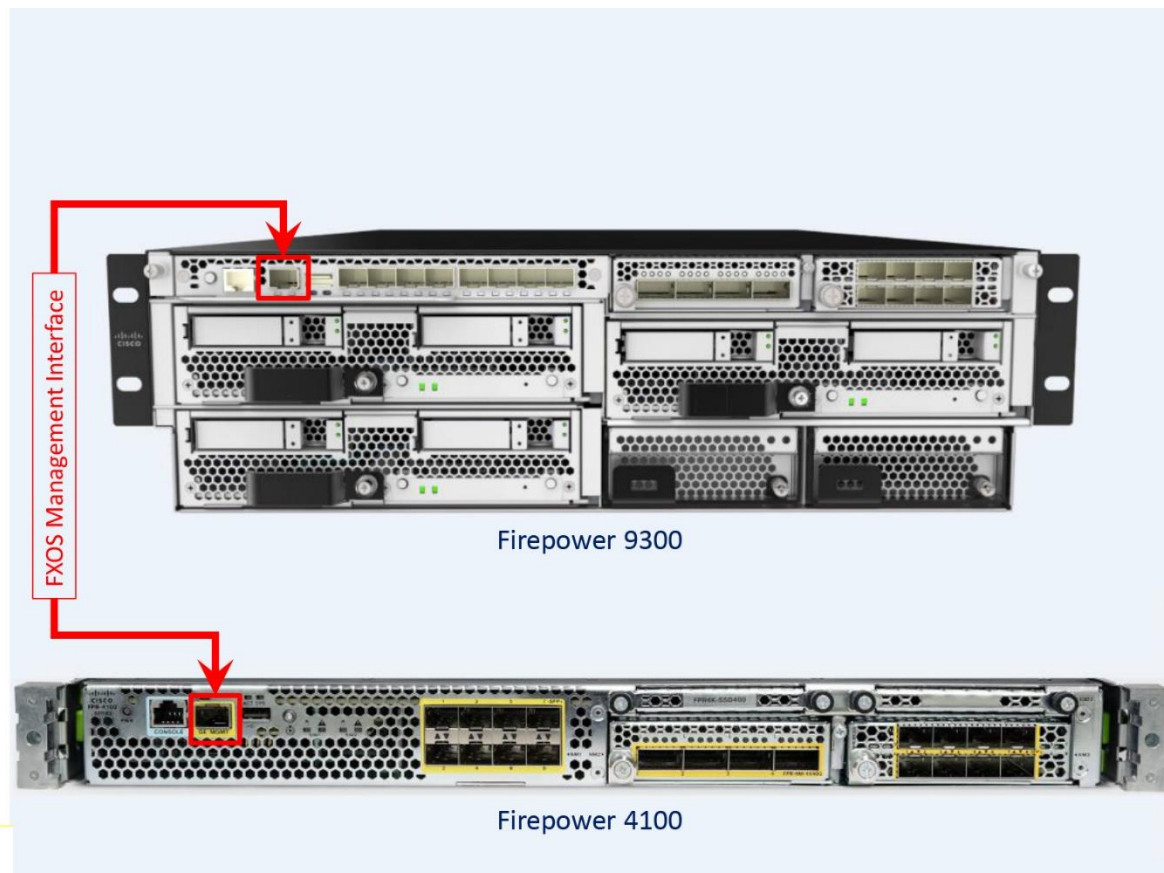


Figure 6-3. Location of the Management Interface on the Firepower Hardware

Design of a Firepower Management Network

As long as the management interfaces can communicate with each other, an FMC is able to manage an FTD from any locations — either Local Area Network (LAN) or Wide Area Network (WAN). Depending on the placement and configuration of the management interfaces, a Firepower management network can be designed various ways.

[Figure 6-4](#) categorizes the possible scenarios to deploy an FTD with an FMC.

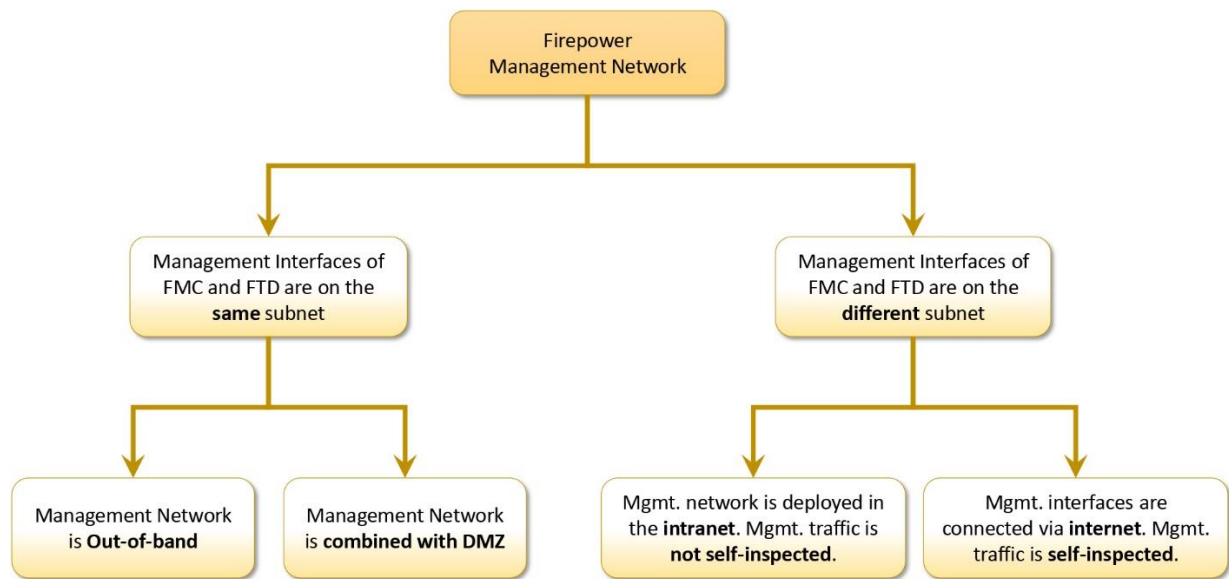


Figure 6-4. *Options to Design a Firepower Management Network*

- **Management Interfaces are on the Same Subnet:** You can configure the management interfaces of FMC and FTD on the same subnetwork and connect them through a layer 2 switch. The layer 2 switch for a management network could be completely out-of-band, or placed in a network where other servers are currently deployed.

Figure 6-5 shows a deployment where the management interfaces of FMC and FTD are configured out-of-band.

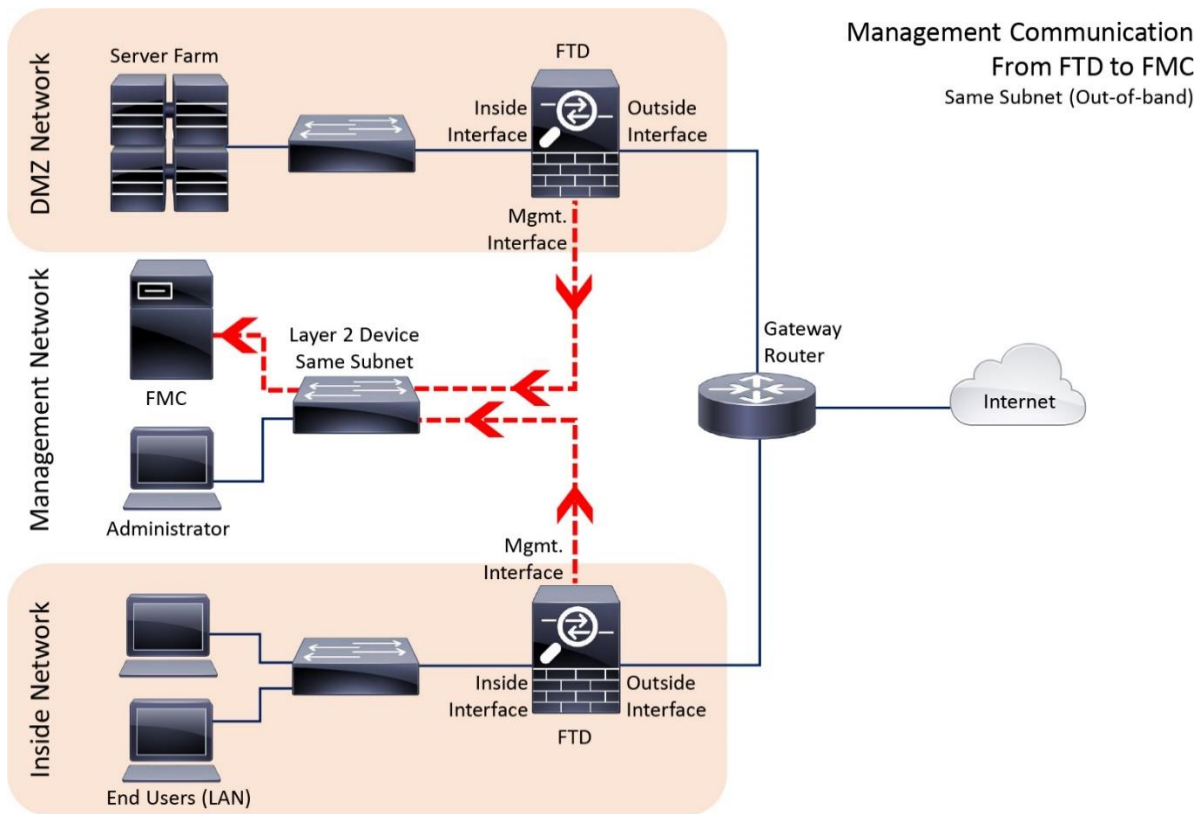


Figure 6-5. Out-of-band Firepower Management Network

- **Management Interfaces are on the Different Subnet:** FMC and FTD can be deployed in two different subnets or branch offices of your company, or even in two different countries. In such case, you need a router to route the management traffic between Firepower Systems.

[Figure 6-6](#) exemplifies a design where the management interface of an FMC is connected to two FTDs that are located at two different networks — one FTD is in the same DMZ network as the FMC, and the other FTD is in a separate inside network.

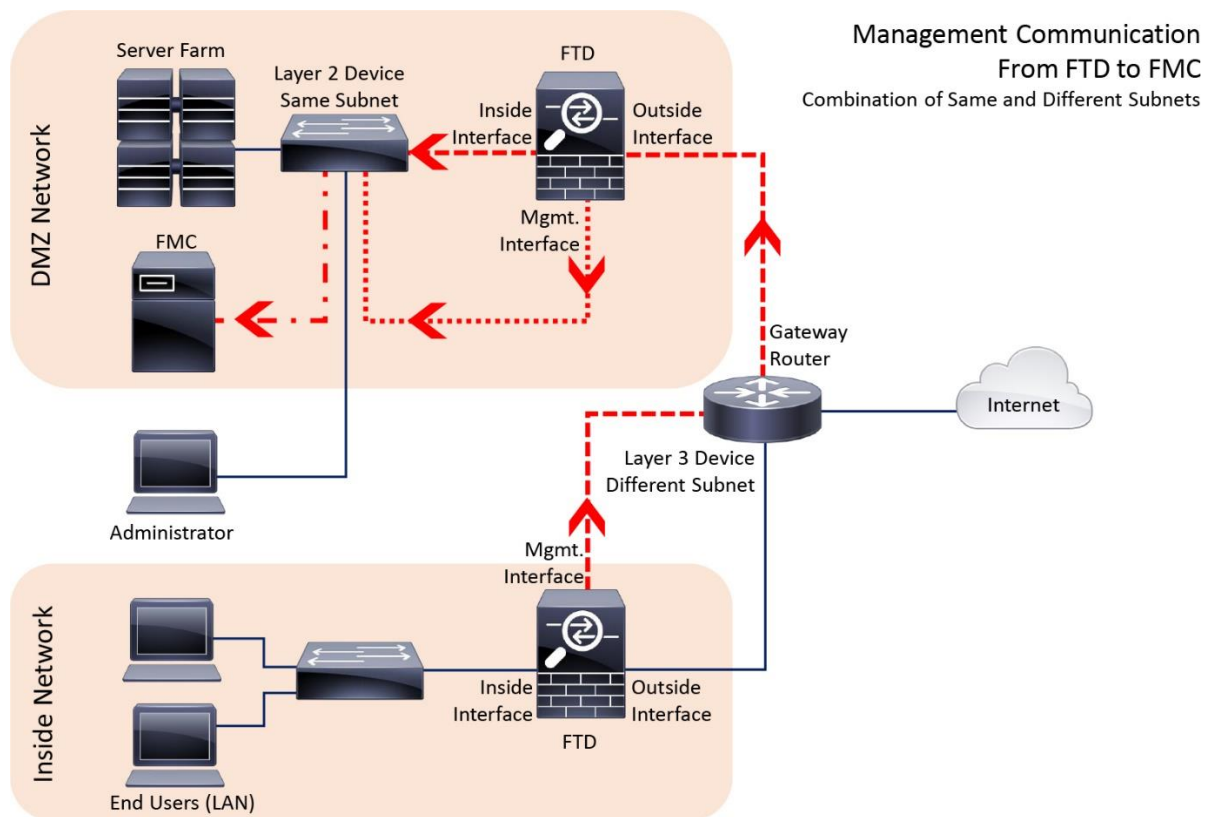


Figure 6-6. FMC is Connected with FTDs Simultaneously at Different and Same Subnets

If you do not assign an IP address to the logical diagnostic interface, you can configure the logical management interface and inside interface within the same layer 2 network, and use the inside interface as the gateway for the logical management interface. It allows the FTD to communicate with an FMC over the internet. However, if you configure the logical diagnostic interface with an IP address anyway (which is not recommended), you end up in adding a router between your management network and inside network.

Caution

Be mindful when you consider sending Firepower management traffic through the FTD inside interface. If the inside interface flaps, FTD and FMC can experience intermittent communication failure. If the inside interface goes down, FTD loses connection to the FMC completely. In this circumstance, a console connection to the FTD is critical to investigate a connectivity issue. If a console access is not provisioned, you cannot troubleshoot further until a physical access to the FTD is possible.

Note

When a Firepower appliance uses a private IP address for its management interface and needs to communicate with another Firepower appliance over the internet, the private IP address has to be translated to a publicly routable IP address. It is usually performed by a router or

firewall using the Network Address Translation (NAT) technology. When an intermediate device translates the management IP address of a Firepower appliance, the FMC and FTD must use a unique NAT ID during their registration process.

[Figure 6-7](#) positions FTDs in various locations in a company and connect them through the internet.

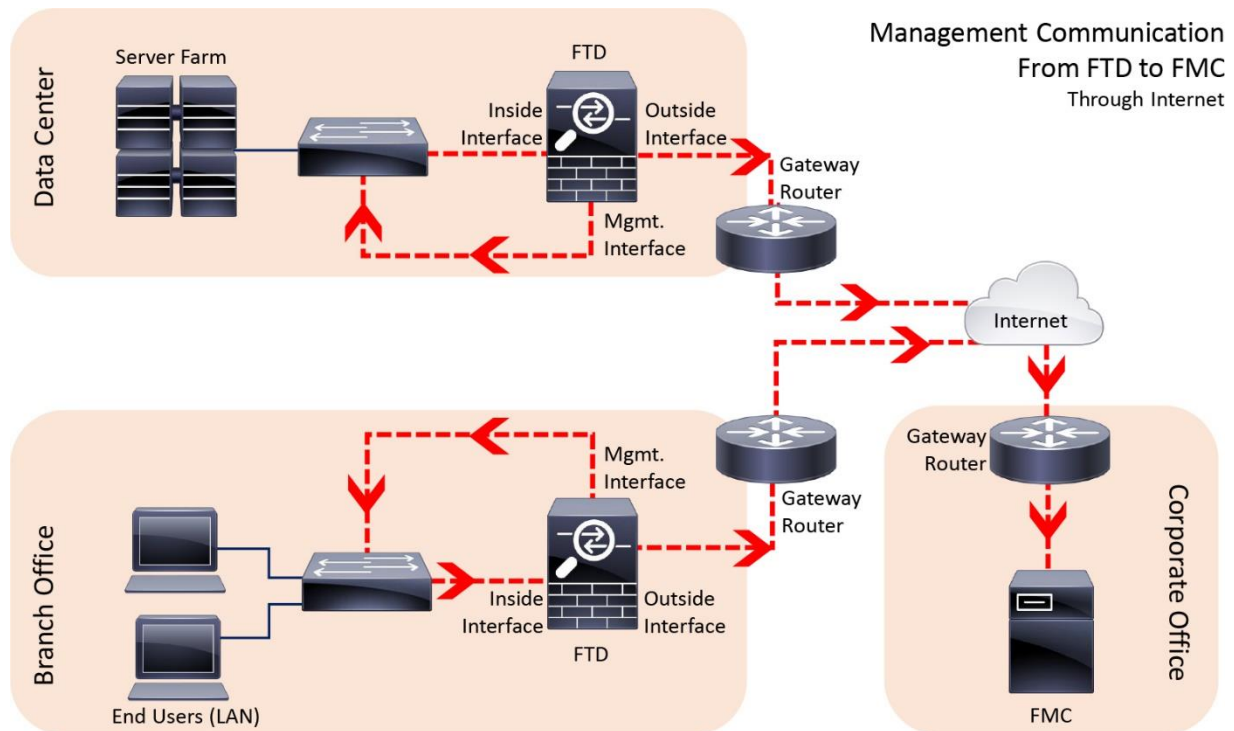


Figure 6-7. FMC and FTD Communicate over the Internet

Until an FTD is registered with an FMC, the web interface does not let you configure the inside and outside interfaces. Hence, you are unable to select the inside interface as a gateway for the management interface until the inside interface is configured and enabled. To address this challenge, follow the steps below:

Step 1. First, register your FTD with an FMC without sending the management traffic through an inside interface. At this point, you can connect the management interfaces of FTD and FMC directly through a layer 2 or layer 3 device. See the [Figure 6-5](#) as an example.

Step 2. After the registration is complete, configure the inside and outside interfaces.

Step 3. When the inside and outside network is able to communicate each other, gracefully delete the existing registration between FMC and FTD.

Step 4. Connect the management interface to inside network.

Step 5. Reregister the FTD with the FMC. This time the management traffic should go through the inside network to the FMC in the outside network.

Best Practices

Configure the management interface when a Firepower system prompts you to setup the network automatically, at the end of the software installation. If you misconfigured at that time, or want to modify the initially configured settings, you can also do that. When you design and configure the Firepower management network, there are couple of things you should consider:

1. Segregate the management traffic from the data traffic. Keeping the management network out-of-band secures the control-plane traffic if the data network is attacked.
2. Although a Firepower system allows you to change the default port for management communication, Cisco strongly recommends you use the default port TCP 8305.

On FMC Hardware

A brand new FMC, out of the box, uses 192.168.45.45 as its management IP address. To connect to an FMC through the web interface for the first time, your computer must be able to reach the FMC management network 192.168.45.0/24. Once your computer is able to communicate with the FMC management interface, enter `https://192.168.45.45` in your browser to access the GUI.

Note

When you reimage a previously configured FMC, an FMC prompts you to confirm if you want to keep the prior network settings during the reimage process. [Chapter 4](#) describes the reimage process in detail.

Configuration

You have several options to configure or modify the management IP address of an FMC. You can change the IP address during your first login to the FMC web interface. Later, you can use the GUI or CLI to modify the management IP address.

Using the GUI — During the First Login

After a reimage, when you login to the web interface of an FMC for the first time, the initialization page appears. In this page, you can change the default password, network settings, etc. You can skip the licensing configuration on this page, as you will learn more about licensing system in the next chapter.

Note

The default username and password for an FMC are admin and Admin123, respectively.

Figure 6-8 shows the initial landing page of an FMC. This page appears when you enter the management IP address on a browser, for the first time.

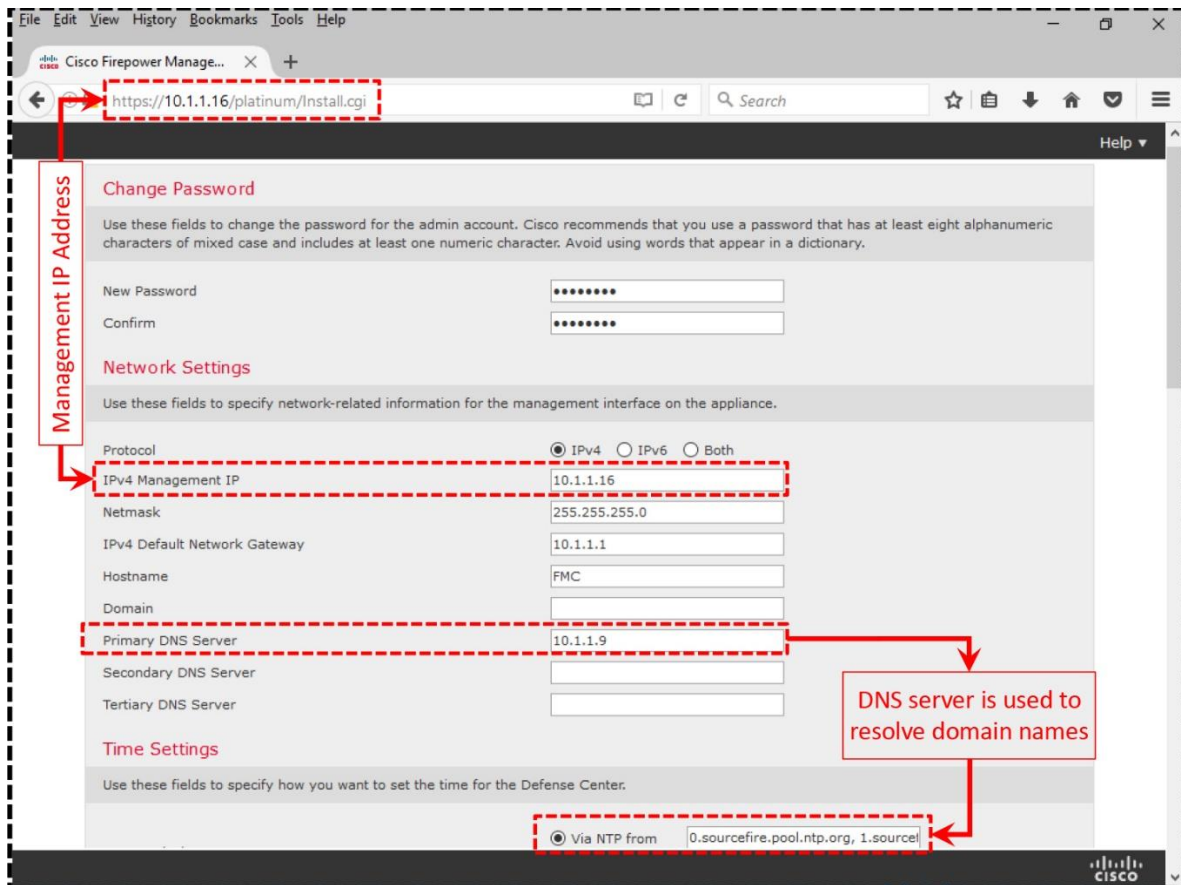


Figure 6-8. System Initialization Page of an FMC

After updating the default settings, you will need to accept the End user License Agreement (EULA), and hit the **Apply** button.

Caution

As soon as you apply a new management IP address, any SSH or HTTP session to the FMC is disconnected. You have to reconnect to the FMC using the updated IP address.

[Figure 6-9](#) shows the checkbox that you must select in order to accept the EULA and to complete the system initialization.

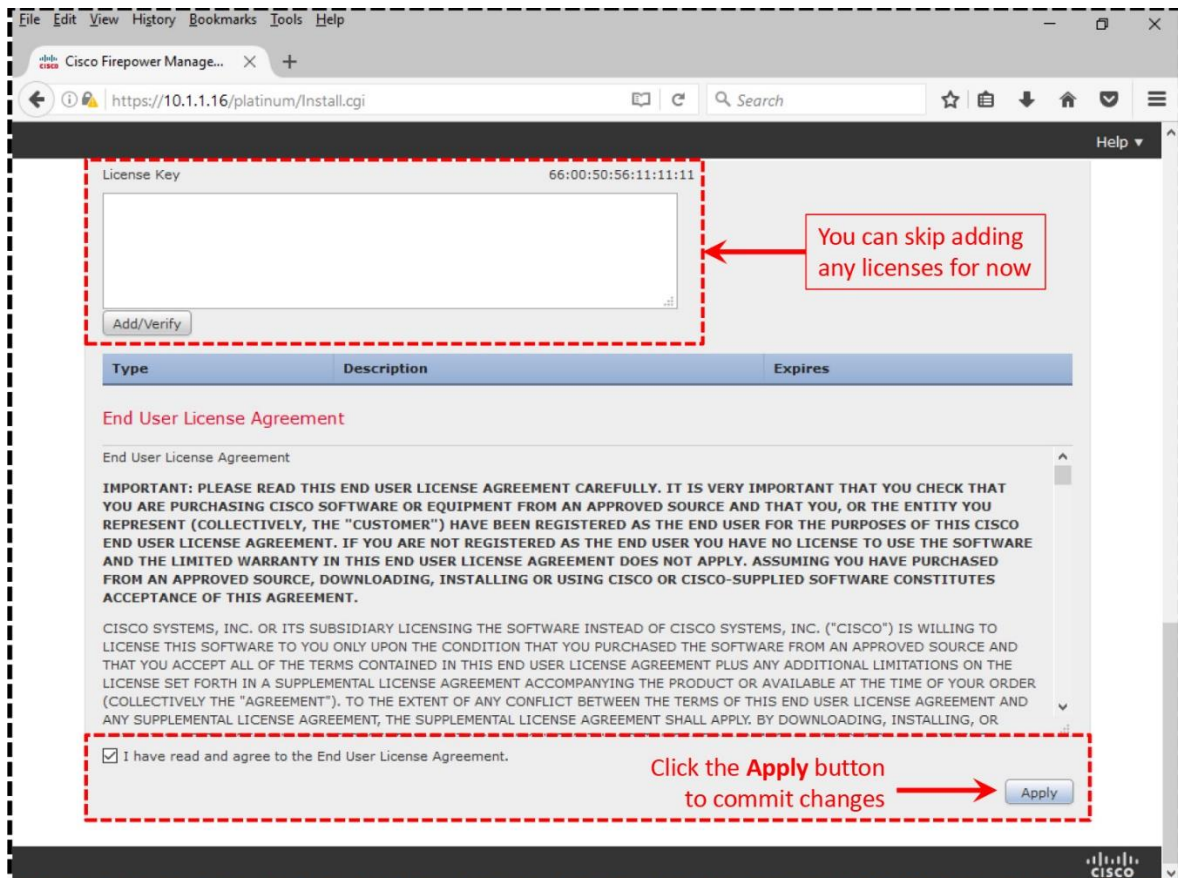


Figure 6-9. Acceptance of the End User License Agreement (EULA) of an FMC

Using the GUI — On Demand

Alternatively, you can change the management IP address of an FMC whenever you need. To change the existing network settings of an FMC via the GUI, follow the steps below:

Caution

If your FMC is currently managing any FTDs, deregister them from the FMC before you change the management IP address. After you apply the new IP address, reregister them with FMC. Follow this step to avoid any potential registration or communication issues.

Step 1. Login to the web interface of your FMC.

Step 2. Go to the System > Configuration page.

Step 3. Select the **Management Interfaces** option in the left panel.

[Figure 6-10](#) shows the configuration page of the management interface in the web interface of an FMC.

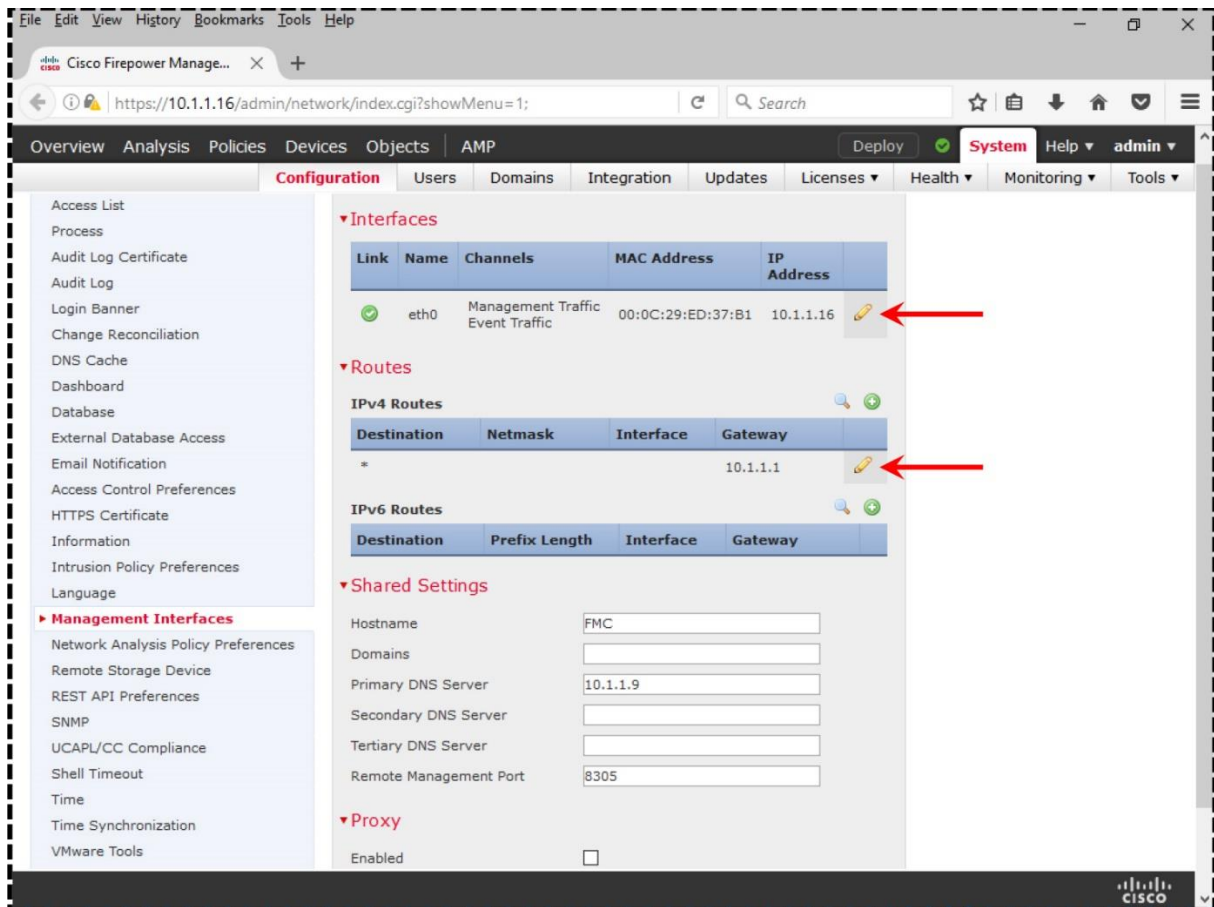


Figure 6-10. Configurable Items for the Management Interface of an FMC

Step 4. In the configuration page, use the pencil icon to modify the IP addresses. In the **Interfaces** section, you enter an IP address for the management interface. Similarly, in the **Routes** section, you provide the gateway IP address.

Step 5. Once all of the necessary network settings are entered, click the **Save** button at the bottom of the page to save your changes. You are done. Now you should be able to access to the FMC using the new IP address.

Using the Command Line Interface

To change the network settings on an FMC via CLI, access the CLI using Secure Shell (SSH) or console terminal, and then run the **configure-network** command.

[Example 6-1](#) shows the network configuration of a management interface on an FMC. It manually assigns `10.1.1.16/24` and `10.1.1.1` for its interface address and gateway, respectively.

Example 6-1 Configuration of Network Settings from the CLI of an FMC

```
admin@firepower:~$ sudo configure-network
```

We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:

- #1) Respect the privacy of others.
- #2) Think before you type.
- #3) With great power comes great responsibility.

Password:

Do you wish to configure IPv4? (y or n) **y**

Management IP address? [192.168.45.45] **10.1.1.16**

Management netmask? [255.255.255.0]

Management default gateway? **10.1.1.1**

Management IP address? 10.1.1.16

Management netmask? 255.255.255.0

Management default gateway? 10.1.1.1

Are these settings correct? (y or n) **y**

Do you wish to configure IPv6? (y or n) **n**

Updated network configuration.

Updated comms. channel configuration.

Please go to <https://10.1.1.16/> or [https://\[\]/](https://[]/) to finish installation.

admin@firepower:~\$

[Verification and Troubleshooting Tool](#)

Before the registration process, if you experience any connectivity issue between the management interfaces of an FMC and FTD, you can run couple of command line tools to verify the network connectivity between your Firepower systems.

First, run the ping test from the CLI of your FMC to the management interface of your FTD device.

[Example 6-2](#) shows a successful ping test from the FMC to 10.1.1.2 — the IP address of the management interface. The ping command on the FMC requires root privilege, therefore you need to run use **sudo** with the **ping** command.

Example 6-2 Successful Ping Test Between an FMC and an FTD

```
admin@FMC:~$ sudo ping 10.1.1.2
```

```
Password:
```

```
PING 10.1.1.2 (10.1.1.2) 56(84) bytes of data.
```

```
64 bytes from 10.1.1.2: icmp_req=1 ttl=64 time=0.615 ms
```

```
64 bytes from 10.1.1.2: icmp_req=2 ttl=64 time=0.419 ms
```

```
64 bytes from 10.1.1.2: icmp_req=3 ttl=64 time=0.536 ms
```

```
64 bytes from 10.1.1.2: icmp_req=4 ttl=64 time=0.613 ms
```

```
^C
```

```
--- 10.1.1.2 ping statistics ---
```

```
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
```

```
rtt min/avg/max/mdev = 0.419/0.545/0.615/0.084 ms
```

```
admin@FMC:~$
```

If the ping test from FMC to FTD is unsuccessful, check if your FMC is able to ping the gateway.

[Example 6-3](#) confirms the IP address of the gateway, 10.1.1.1, for eth0 — the management interface of FMC.

Example 6-3 Verification of the Routing Table

```
admin@FMC:~$ route -n
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use
Iface
0.0.0.0          10.1.1.1        0.0.0.0         UG    0      0      0
eth0
10.1.1.0         0.0.0.0         255.255.255.0  U     0      0      0
eth0
admin@FMC:~$
```

If your FMC can successfully ping the gateway, but fails to ping the FTD, it demonstrates a routing issue between the FMC and FTD. You can run the **traceroute** tool on your Firepower system to investigate this issue further, or check the configuration on any intermediate routers. The syntax to run the **traceroute** command on an FMC is below:

```
admin@FMC:~$ sudo traceroute IP_Address_of_FTD
```

If the connectivity between the FMC and gateway fails, there is no reason for the FMC to connect to the FTD successfully. You should see if the interface is up and connected with a cable. Also, make sure that the IP address and subnet mask are configured properly. Run the **ifconfig** command to verify the settings and status.

[Example 6-4](#) shows the assignment of IP address 10.1.1.16 and subnet mask 255.255.255.0. The status of management interface, eth0, is up. This output also confirms if the packets are dropped or have errors.

Example 6-4 Verification of Interface Status and IP Address Assignment

```
admin@FMC:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:ED:37:B1
          inet addr:10.1.1.16  Bcast:10.1.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feed:37b1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2190 errors:0 dropped:0 overruns:0 frame:0
          TX packets:197 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:150210 (146.6 Kb)  TX bytes:25196 (24.6 Kb)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.255.255.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:9789370 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9789370 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2482195842 (2367.2 Mb)  TX bytes:2482195842 (2367.2 Mb)
```

```
admin@FMC:~$
```

On ASA Hardware

FTD application does not offer a GUI when you want to manage it from an FMC. Therefore, to configure or reconfigure the management interface of an FTD, you need to access the CLI first.

Configuration

Once you access the CLI, run the **configure network** command to configure all kinds of basic network settings, such as, DHCP, manual, IPv4, IPv6, etc.

To obtain an IP address from the DHCP server, run the following command:

```
> configure network ipv4 dhcp
```

To assign an IP address manually, use the following syntax:

```
> configure network ipv4 manual IP_Address Subnet_Mask Gateway_Address
```

Note

This command changes the IP address of the logical management interface, br1. It does not assign or make any changes on the logical diagnostic interface.

[Example 6-5](#) shows the command to configure a static IP address 10.1.1.2/24, and a gateway IP address 10.1.1.1 for an FTD management interface, br1.

Example 6-5 Configuration of an IPv4 Address on the Management Interface of an FTD

```
> configure network ipv4 manual 10.1.1.2 255.255.255.0 10.1.1.1
Setting IPv4 network configuration.
Network settings changed.
>
```

Verification and Troubleshooting Tool

Like an FMC, an FTD provides you various tools to test network settings and connectivity, however, the command syntaxes are different on an FTD. Let's take a look at the following examples and learn some useful FTD commands.

[Example 6-6](#) shows the network settings and the status of the logical management interface, br1. The output proves the assignment of port 8305 for transferring management traffic and events. The IP address and MAC address of the logical management interface (br1) are 10.1.1.2 and A4:6C:2A:E4:6B:BE, respectively.

Example 6-6 Status of the Logical Management Interface, br1

```
> show network
===== [ System Information ] =====
Hostname                : firepower
Management port        : 8305
IPv4 Default route
  Gateway               : 10.1.1.1

===== [ br1 ] =====
State                   : Enabled
Channels                : Management & Events
Mode                    : Non-Autonegotiation
MDI/MDIX                : Auto/MDIX
MTU                     : 1500
MAC Address             : A4:6C:2A:E4:6B:BE
----- [ IPv4 ] -----
Configuration          : Manual
Address                 : 10.1.1.2
Netmask                 : 255.255.255.0
Broadcast               : 10.1.1.255
----- [ IPv6 ] -----
Configuration          : Disabled

===== [ Proxy Information ] =====
State                   : Disabled
Authentication          : Disabled

>
```

Did you notice that the previous command output did not show the status of the logical diagnostic interface, Management x/x? To determine the status of the diagnostic interface and any other interfaces, run the **show interface ip brief** command on the CLI of FTD.

[Example 6-7](#) shows an overview of all of the interfaces. The output confirms that there is no IP address assigned to the logical diagnostic interface Management1/1 (Cisco recommends you not to configure this interface).

Example 6-7 A Brief Overview of the FTD Interfaces

```
> show interface ip brief
Interface                IP-Address      OK? Method Status
Protocol
Virtual0                 127.1.0.1       YES unset  up
up
GigabitEthernet1/1      unassigned      YES unset  administratively down
down
GigabitEthernet1/2      unassigned      YES unset  administratively down
down
GigabitEthernet1/3      unassigned      YES unset  administratively down
down
GigabitEthernet1/4      unassigned      YES unset  administratively down
down
GigabitEthernet1/5      unassigned      YES unset  administratively down
down
GigabitEthernet1/6      unassigned      YES unset  administratively down
down
```

```

GigabitEthernet1/7      unassigned      YES unset      administratively down
down
GigabitEthernet1/8      unassigned      YES unset      administratively down
down
Internal-Controll1/1    127.0.1.1      YES unset      up
up
Internal-Data1/1        unassigned      YES unset      up
up
Internal-Data1/2        unassigned      YES unset      down
down
Internal-Data1/3        unassigned      YES unset      up
up
Internal-Data1/4        169.254.1.1    YES unset      up
up
Management1/1          unassigned      YES unset      up
up
>

```

In your output, if you do not see 1/1 with the management interface name, it is okay. The numbering scheme of a management interface is different based on the hardware platform you are running.

[Table 6-1](#) shows that the management interfaces are numbered differently in different hardware platforms.

Hardware Platform	Interface Name
ASA 5506, 5508, 5516	Management1/1
ASA 5512, 5515, 5525, 5545, 5555	Management0/0
Firepower 4100, 9300	Management0

Table 6-1. *Nomenclature of a Management Interface*

[Example 6-8](#) shows that an FTD is running a successful ping test to its manager using the IP address of the FMC management interface, 10.1.1.16.

Example 6-8 *Command to Run a Ping Test Appropriately*

```

> ping system 10.1.1.16
PING 10.1.1.16 (10.1.1.16) 56(84) bytes of data.
64 bytes from 10.1.1.16: icmp_seq=1 ttl=64 time=0.593 ms
64 bytes from 10.1.1.16: icmp_seq=2 ttl=64 time=0.654 ms
64 bytes from 10.1.1.16: icmp_seq=3 ttl=64 time=0.663 ms
64 bytes from 10.1.1.16: icmp_seq=4 ttl=64 time=0.699 ms
^C
--- 10.1.1.16 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.593/0.652/0.699/0.042 ms
>

```

[Example 6-9](#) shows that an FTD fails to ping the management IP address of an FMC when you send the ping request from the diagnostic CLI, instead of the default CLI. It happens because the diagnostic interface has no IP address. Use the previous example when you want to run a proper ping test from the FTD.

Example 6-9 *Ping Test Shows No Success Although the Connection is Established*

```
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower> enable
Password:
firepower# ping 10.1.1.16
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.16, timeout is 2 seconds:
No route to host 10.1.1.16

Success rate is 0 percent (0/1)
firepower#
```

[On Firepower Security Appliance](#)

To manage an FTD, you have to configure one of the interfaces from the network modules for management communication. This section describes the steps to configure and verify the status of a management interface for both software — FXOS and FTD — on a Firepower Security Appliance.

[FXOS Mgmt. Interface](#)

The embedded management interface that is located on the front panel of a Firepower security appliance is used to manage the FXOS. You can configure that interface using FXOS CLI.

[Configuration](#)

To configure the network settings for a management interface that provides administrative access to the FXOS software, run the **set out-of-band** command on the CLI. After any changes, you must apply the configuration to take an effect.

[Example 6-10](#) shows how to assign an IP address and gateway to the management interface of the FXOS.

Example 6-10 *Set Up an IP address and Gateway for the FXOS Management Interface*

```
Firepower-9300# scope fabric-interconnect a
Firepower-9300 /fabric-interconnect # set out-of-band ip 10.1.1.28 netmask
255.255.255.0 gw 10.1.1.1
Warning: When committed, this change may disconnect the current CLI session
Firepower-9300 /fabric-interconnect* #
```

! The above command does not take an effect until you run the following command and commit the changes.

```
Firepower-9300 /fabric-interconnect* # commit-buffer
```

```
Firepower-9300 /fabric-interconnect #
```

! If you misconfigured or do not want to apply a recent change, you could discard it from the buffer as well. To discard, run the following command.

```
Firepower-9300 /fabric-interconnect* # discard-buffer  
Firepower-9300 /fabric-interconnect #
```

Verification and Troubleshooting Tool

The command syntax on an FXOS is different than the syntax on an ASA or FTD software. In FXOS, when you run any particular command, you have to enter an appropriate module or scope. Below, you will find some testing tools that you previously ran on an FMC or ASA. Now you are going to perform those tests once again, but this time the command syntaxes are different — works only on an FXOS.

[Example 6-11](#) shows the command to connect to the local-mgmt module, and how to run a ping test from there.

Example 6-11 Successful Ping Test from the FXOS to an FMC Management Interface

```
Firepower-9300# connect local-mgmt  
Firepower-9300(local-mgmt)# ping 10.1.1.1  
PING 10.1.1.1 (10.1.1.1) from 10.1.1.28 eth0: 56(84) bytes of data.  
64 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=0.298 ms  
64 bytes from 10.1.1.1: icmp_seq=2 ttl=255 time=0.412 ms  
64 bytes from 10.1.1.1: icmp_seq=3 ttl=255 time=0.392 ms  
64 bytes from 10.1.1.1: icmp_seq=4 ttl=255 time=0.390 ms  
^C  
--- 10.1.1.1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3007ms  
rtt min/avg/max/mdev = 0.298/0.373/0.412/0.044 ms  
Firepower-9300(local-mgmt)#
```

[Example 6-12](#) shows the command to verify the network settings and the status of the FXOS management interface.

Example 6-12 Status of a Management Interface

```
Firepower-9300# connect local-mgmt  
Firepower-9300(local-mgmt)# show mgmt-port  
eth0      Link encap:Ethernet  HWaddr B0:AA:77:2F:84:71  
          inet addr:10.1.1.28  Bcast:10.122.144.255  Mask:255.255.255.0  
          inet6 addr: fe80::b2aa:77ff:fe2f:8471/64  Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:4980815  errors:0  dropped:0  overruns:0  frame:0  
          TX packets:2680187  errors:0  dropped:0  overruns:0  carrier:0  
          collisions:0  txqueuelen:1000  
          RX bytes:1124575588 (1.0 GiB)  TX bytes:1921268851 (1.7 GiB)  
Firepower-9300(local-mgmt)#
```


[Example 6-13](#) shows the command to determine the IP address of the gateway of the FXOS management interface.

Example 6-13 *Default Gateway for the Management Interface of the FXOS*

```
Firepower-9300# show fabric-interconnect
```

```
Fabric Interconnect:
```

ID	OOB IP Addr	OOB Gateway	OOB Netmask	OOB IPv6 Address	OOB IPv6
A	10.1.1.28	10.1.1.1	255.255.255.0	::	::

```
64 Operable  
Firepower-9300#
```

FTD Mgmt. Interface

You cannot select the embedded management interface as the FTD management interface. This section describes how to setup one for an FTD logical device.

Configuration

To configure a new physical interface for management communication, or to change the administrative state (enable/disable) of a management interface, follow the steps below:

Step 1. Go to the **Interfaces** page of the Firepower Chassis Manager. By default, you should be at the **All Interfaces** tab.

Step 2. Click the *pencil* icon (at the right-hand side of a row) for the interface you want to modify. The **Edit Interface** popup window appears.

Figure 6-11 shows the Ethernet1/1 interface is enabled, and configured for the Management (mgmt) type traffic.

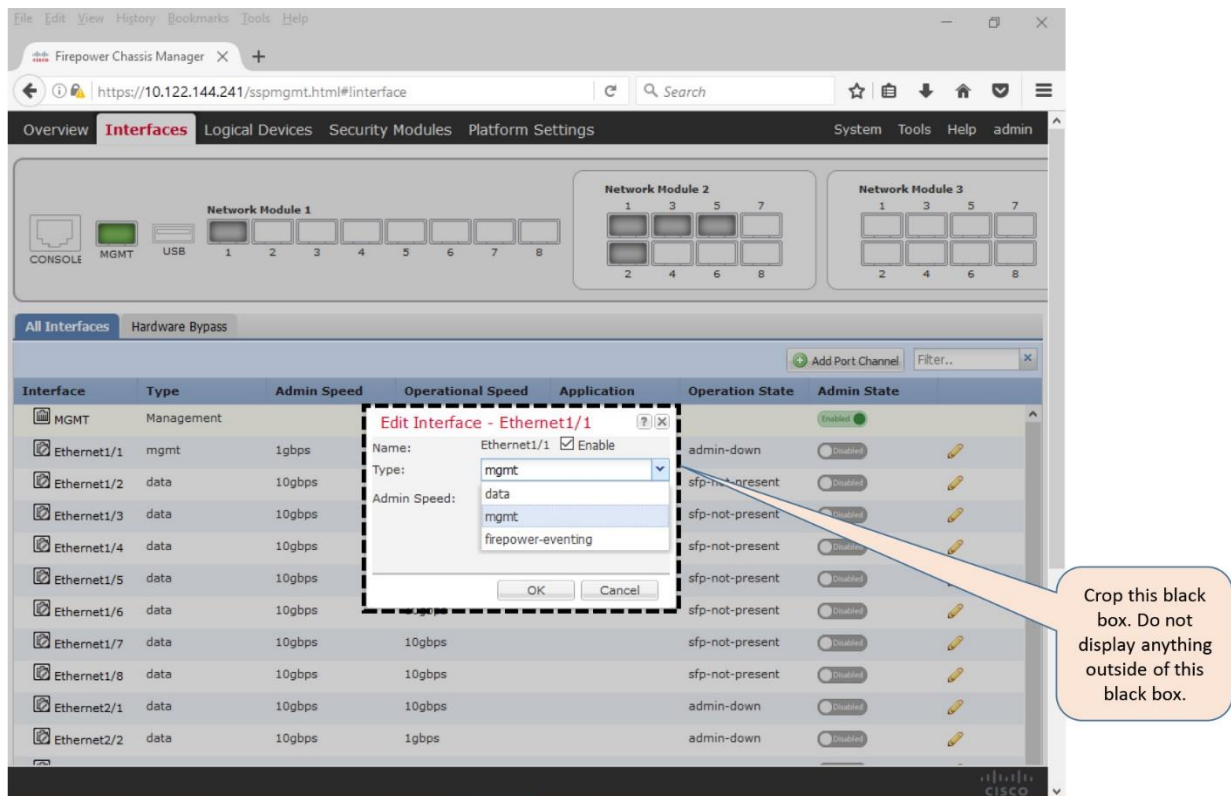


Figure 6-11. The Configurable Options for an Interface

Step 3. Using the **Type** drop-down, select the type of traffic that you want the interface to carry. For example, if you want to select an interface for management communication between an FTD and FMC, select **mgmt** from the drop down.

Step 4. Select the **Enable** checkbox if you want to enable this interface immediately with the updated settings.

Step 5. Click the **OK** button to save the changes. The **Interfaces** page returns and reflects the changes you have just made.

[Figure 6-12](#) shows the statuses of two types of management interfaces — one is for the FXOS, and the other one is for the FTD — after they are configured, administratively enabled, and physically connected.

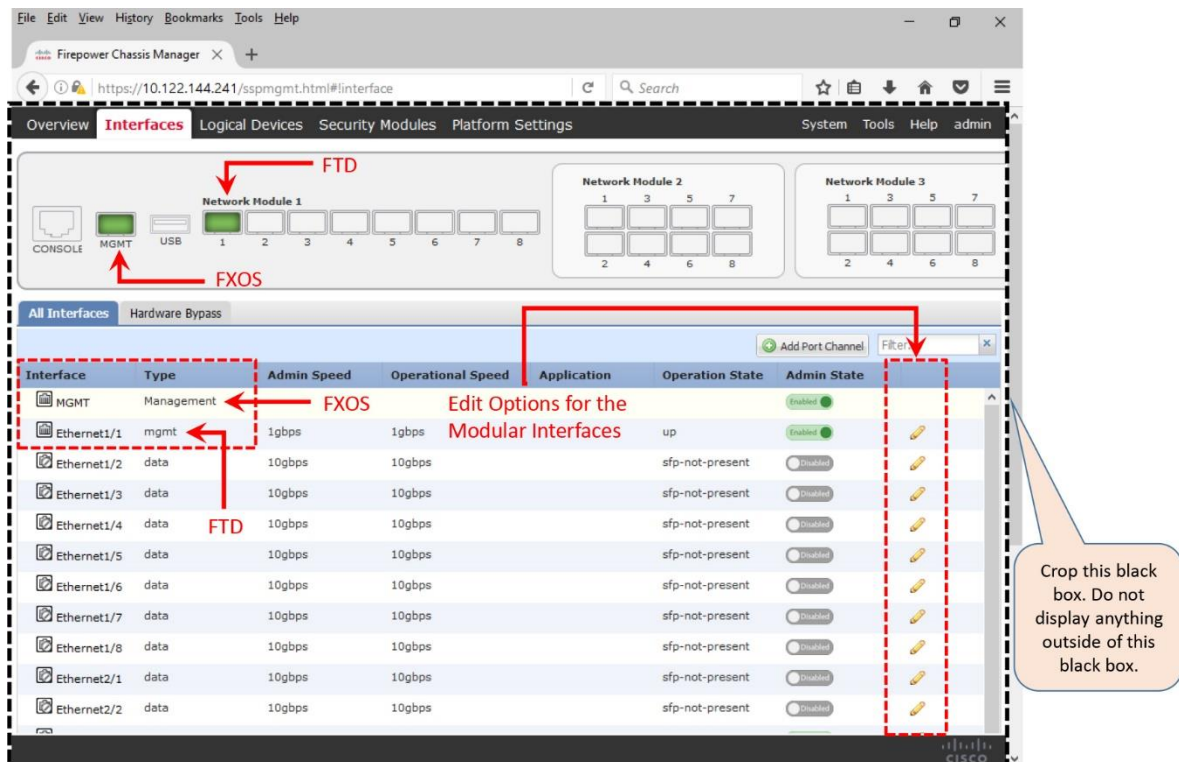


Figure 6-12. Visual Changes in the GUI, for Both Types of Management Interfaces

If you want to modify the management IP address of an already configured FTD, or intend to use a different physical management interface for an FTD, follow the steps below:

Step 1. On the Firepower Chassis Manager, go to the **Logical Devices** page. The FTD logical device, if configured, should appear.

Step 2. Click the *pencil* icon (at the right hand side of a row) for the FTD logical device you want to modify. A **Provisioning** page for the FTD appears.

Step 3. Click on the **Click to configure** rectangular box. A configuration window appears.

[Figure 6-13](#) shows the configuration window for an FTD. Here, you can modify the settings of an FTD management interface.

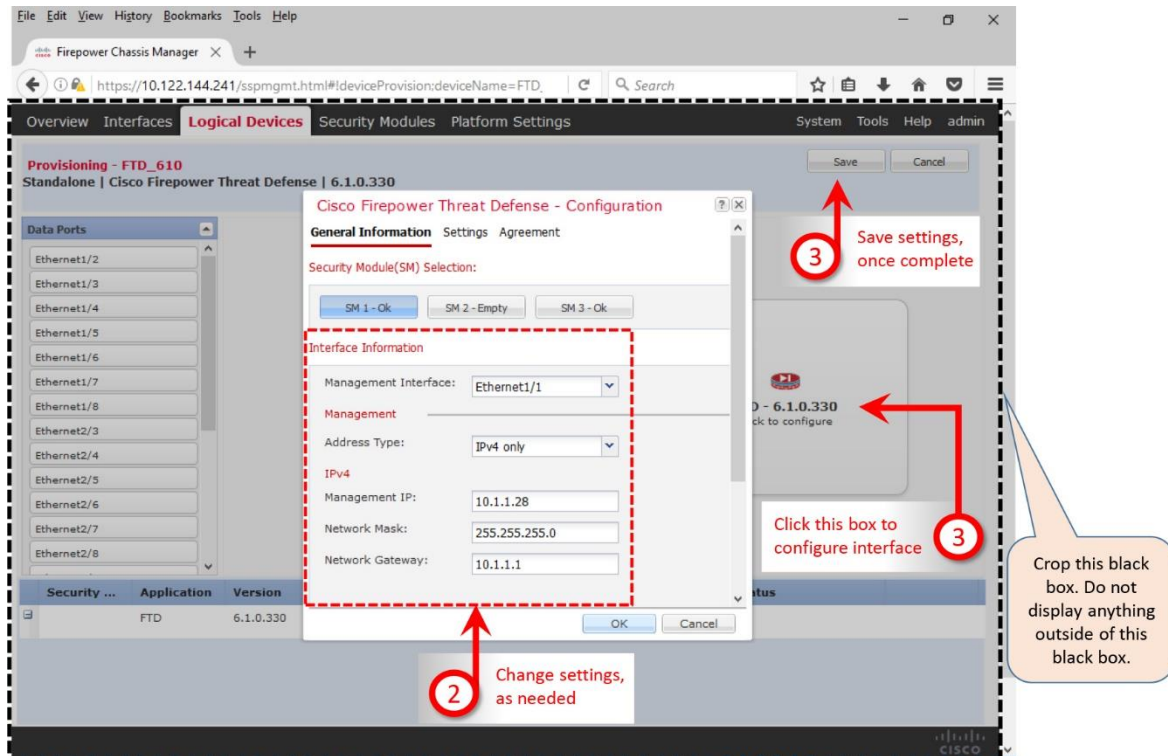


Figure 6-13. Workflow to Change the Network Settings of an FTD Logical Device

Step 4. Once you are done with any modification, click **OK** and then the **Save** button to apply the changes.

Caution

After you change the FTD management IP address and commit changes using the Firepower Chassis Manager, the FTD logical device reinitializes and resets all bootstrap settings.

Verification and Troubleshooting Tool

[Example 6-14](#) shows the interfaces for an FTD logical device. By running the **show configuration** command within the scope of **ssa**, you can verify if the selected physical interfaces are properly mapped with a logical device.

Example 6-14 Mapping of Physical Interfaces with an FTD Logical Device

```
Firepower-9300# scope ssa
Firepower-9300 /ssa # show configuration
scope ssa
  enter logical-device FTD_61 ftd 1 standalone
  enter external-port-link Ethernet11_ftd Ethernet1/1 ftd
  set decorator ""
  set description ""
  set port-name Ethernet1/1
exit
```

```

    enter external-port-link Ethernet23_ftd Ethernet2/3 ftd
        set decorator ""
        set description ""
        set port-name Ethernet2/3
    exit
    enter external-port-link Ethernet24_ftd Ethernet2/4 ftd
        set decorator ""
        set description ""
        set port-name Ethernet2/4
    exit
    enter mgmt-bootstrap ftd
        enter ipv4 1 firepower
            set gateway 10.1.1.1
            set ip 10.1.1.28 mask 255.255.255.0
        exit
    exit
    set description ""
    set res-profile-name ""
exit

```

```

.
.
.
<Output Omitted>

```

```
Firepower-9300 /ssa #
```

[Example 6-15](#) shows the administrative and operational statuses of all of the interfaces on a Firepower security appliance (except the member interfaces of a port-channel). The output shows that the FTD management interface (Ethernet1/1) and both data interfaces (Ethernet2/3 and Ethernet2/3) are enabled and up.

Example 6-15 Status of the Fixed and Modular Interfaces from the CLI of the FXOS

```

Firepower-9300# scope eth-uplink
Firepower-9300 /eth-uplink # scope fabric a
Firepower-9300 /eth-uplink/fabric # show interface

```

Interface:	Port Name	Port Type	Admin State	Oper State	State
Ethernet1/1	Mgmt		Enabled	Up	
Ethernet1/2	Data		Disabled	Sfp Not Present	Unknown
Ethernet1/3	Data		Disabled	Sfp Not Present	Unknown
Ethernet1/4	Data		Disabled	Sfp Not Present	Unknown
Ethernet1/5	Data		Disabled	Sfp Not Present	Unknown
Ethernet1/6	Data		Disabled	Sfp Not Present	Unknown
Ethernet1/7	Data		Disabled	Sfp Not Present	Unknown
Ethernet1/8	Data		Disabled	Sfp Not Present	Unknown
Ethernet2/3	Data		Enabled	Up	
Ethernet2/4	Data		Enabled	Up	
Ethernet2/5	Data		Disabled	Sfp Not Present	Unknown
Ethernet2/6	Data		Disabled	Sfp Not Present	Unknown
Ethernet2/7	Data		Disabled	Sfp Not Present	Unknown
Ethernet2/8	Data		Disabled	Sfp Not Present	Unknown
Ethernet3/1	Data		Disabled	Sfp Not Present	Unknown
Ethernet3/2	Data		Disabled	Sfp Not Present	Unknown
Ethernet3/3	Data		Disabled	Sfp Not Present	Unknown

Ethernet3/4	Data	Disabled	Sfp Not Present	Unknown
Ethernet3/5	Data	Disabled	Sfp Not Present	Unknown
Ethernet3/6	Data	Disabled	Sfp Not Present	Unknown
Ethernet3/7	Data	Disabled	Sfp Not Present	Unknown
Ethernet3/8	Data	Disabled	Sfp Not Present	Unknown

Firepower-9300 /eth-uplink/fabric #

[Example 6-16](#) demonstrates how to connect to the FTD logical device from the CLI of an FXOS, and then verify the network settings on the FTD logical device.

Example 6-16 Verification of Network Settings That Are Specific to the FTD Application

```

Firepower-9300# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1> connect ftd
Connecting to ftd console... enter exit to return to bootCLI

> show network
===== [ System Information ] =====
Hostname                : Firepower-module1
Management port         : 8305
IPv4 Default route
  Gateway                : 10.1.1.1

===== [ management0 ] =====
State                   : Enabled
Channels                : Management & Events
Mode                    : Non-Autonegotiation
MDI/MDIX                : Auto/MDIX
MTU                     : 9210
MAC Address             : B0:AA:77:2F:84:5D
----- [ IPv4 ] -----
Configuration          : Manual
Address                 : 10.1.1.28
Netmask                 : 255.255.255.0
Broadcast               : 10.1.1.255
----- [ IPv6 ] -----
Configuration          : Disabled

===== [ Proxy Information ] =====
State                   : Disabled
Authentication          : Disabled
>

```

Summary

In this chapter, you have learned the best practices for designing and configuring a management network for the Firepower system. This chapter discusses the tools that you could use to verify any communication issues between the management interfaces of an FMC and FTD. Before you begin the registration process which is described in the next chapter, you must ensure that the FMC and FTD are successfully connected through your network.

Quiz

1. In order to run a ping test from an FTD to an FMC, which command syntax would be correct?

- a.** `ping IP_Address`
- b.** `sudo ping IP_Address`
- c.** `ping system IP_Address`
- d.** `ping host IP_Address`

2. Which port is used by the Firepower Systems for management communication, by default?

- a.** 22
- b.** 443
- c.** 8080
- d.** 8305

3. During the FTD software initialization, you have to configure a network. Which interface on an ASA is assigned with an IP address, from that initial configuration?

- a.** GigabitEthernet0/0
- b.** Management0/0
- c.** Management1/1
- d.** Br1

4. Per Cisco recommendation, one of the interfaces on ASA should have no IP address configured. Which interface is this?

- a.** Management0/0
- b.** Management1/1
- c.** Br1
- d.** Both a and b

5. To investigate a communication issue between an FMC and FTD, which of the following tools could be used?

- a.** Ifconfig

b. Ping

c. Traceroute

d. All of the above

6. Which of the following statement is not true?

a. Segregation of management traffic improves security policy.

b. Default Firepower management port should not be changed.

c. Logical management interface is labeled as Management0/0 on any ASA platforms.

d. FTD does not offer any web interface when it is configured for remote management.

Chapter 7. Licensing and Registration through SFTunnel

At this point, your Firepower system is running the Firepower software and the management interface is configured. You are ready to begin the next step — installing the licenses, enabling the Firepower features, and registering the FTD with an FMC. The registration process takes place through an encrypted tunnel which is established between the management interfaces of an FMC and FTD. You cannot, however, register an FTD with an FMC unless the FMC is licensed. Let's begin the journey to learn all of these steps for an initial deployment from this chapter.

Essential Knowledge

An FMC accepts two types of licenses — classic license and smart license. To manage an FTD, you must use a smart license. A classic license is used for the prior implementations of the Sourcefire technology, such as, FirePOWER services on ASA, legacy Sourcefire products. Since this book focuses on the FTD, this section describes various components of the smart license.

Smart License Architecture

The Smart Licensing architecture offers two major benefits over the Classic licensing system. It provides you with an ability to administer all of your Firepower licenses from a single place, and oversee their usage in real time. It also allows you to enable the full functionalities of an FMC and FTD without installing any licenses for the first 90 days of an initial deployment. This grace period lets you to complete any logistic or business processes related to your new Firepower deployment.

In the Smart Licensing Architecture, the Firepower Manager uses a process — Smart Agent — to communicate and register with the Cisco License Authority. Upon a successful registration, the License Authority issues an ID certificate. The Smart Agent process uses this certificate to communicate with the Cisco License Authority from time to time, and track the status of entitlements.

Cisco offers two options to connect a Firepower Manager to the Cisco License Authority. Depending on the security and connectivity policies of your organization, you can either choose to connect to the License Authority directly over the internet, or via a satellite server.

Cisco Smart Software Manager (CSSM)

After purchase, your Firepower smart licenses are assigned to an account that is created exclusively for your organization. You can manage any smart licenses of your company using the Cisco Smart Software Manager (CSSM) — a web based application at cisco.com.

If you have an administrative access to your account, the CSSM allows you to create additional virtual accounts within the master account of your company. It helps you to organize the Firepower licenses based on departments or locations. When necessary, you can also transfer licenses and devices between the virtual accounts.

Tips

To get access to the CSSM, contact the Cisco Channel Partner, Sales Representative, or the Global Licensing Operations (GLO) team.

[Figure 7-1](#) shows that the Smart Agent process of an FMC connects to the Cisco License Authority through the internet, while an administrator is able to manage the licenses through the internet, by connecting to the Cisco Smart Software Manager (CSSM) application.

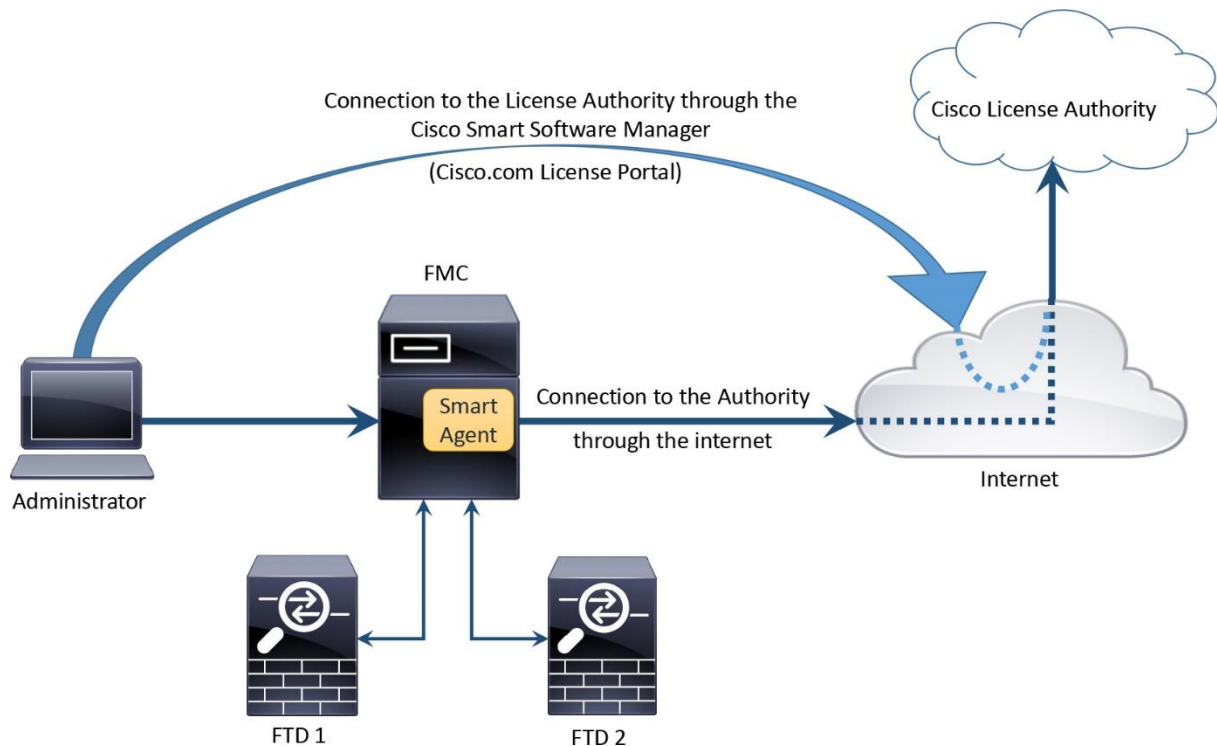


Figure 7-1. Network Connectivity between an FMC and the Cisco License Authority

CSSM Satellite

Since the Cisco License Authority is hosted at cisco.com, an FMC requires internet connectivity to obtain a smart license. For security reason, if you are unwilling to connect the management interface of your FMC to the internet, you can use the CSSM satellite — a virtual version of the CSSM deployed from an OVA image. In a CSSM satellite deployment, an FMC is connected to a CSSM satellite server. The CSSM satellite server is registered to the Cisco License Authority through the internet.

Note

The CSSM application or a satellite server is designed to integrate wide range of Cisco products. Describing the configuration of CSSM satellite is beyond the scope of this book. Cisco publishes various documents on the Smart Licensing system which you can download free from the cisco.com. Please read them to learn more.

[Figure 7-2](#) illustrates the connection of an FMC with the Cisco License Authority through the CSSM satellite server and internet.

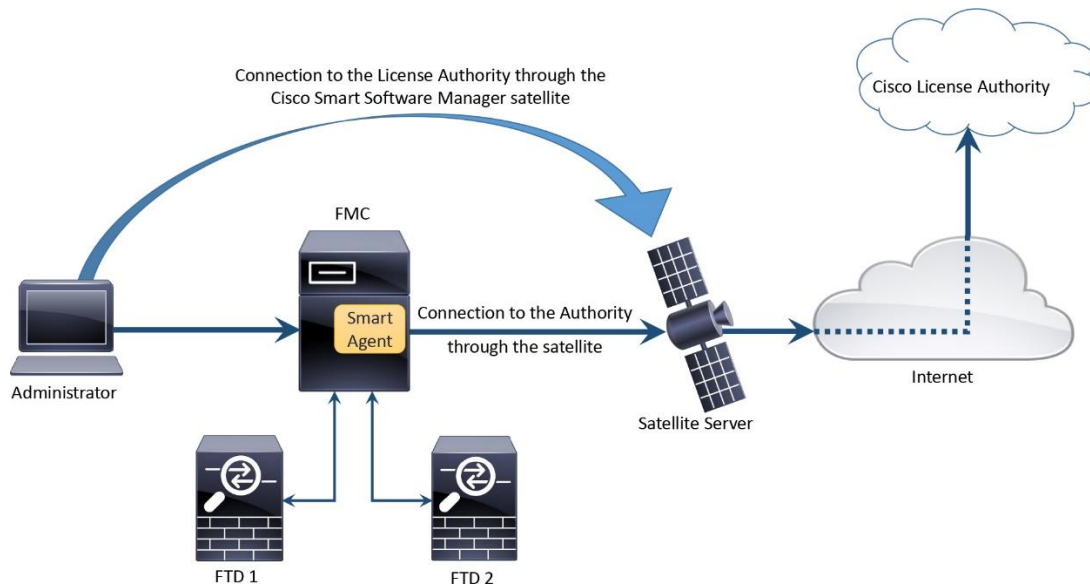


Figure 7-2. Connection of an FMC with the Cisco License Authority via CSSM Satellite

Firepower Licenses

The Cisco Firepower technology, an evolution from the Sourcefire technology, offers various features to protect your network from malicious activities. A new Firepower System, by default, comes with a base license. A base license, however, does not enable all of the security features. To enable all of the functionalities, separate feature licenses are necessary.

Tips

If you turn on the Evaluation Mode on a Firepower System, it enables all of the security features on an FMC. You can apply them on an FTD for 90-day period. Before the evaluation period expires, you must purchase a valid license, and register the FMC with the Cisco License Authority for continuous operation.

[Table 7-1](#) describes the functionalities of each Firepower license. Threat license is a prerequisite for Malware or URL Filtering license.

License	It Allows You to
URL Filtering	<ul style="list-style-type: none"> Filter URL based on reputation and category features
Malware	<ul style="list-style-type: none"> Protect network from malware, enable AMP for network and AMP Threat Grid Block transfer of certain types of files Blocklist traffic based on intelligence
Threat	<ul style="list-style-type: none"> Detect and prevent intrusion attempts
Base	<ul style="list-style-type: none"> Perform switching, routing and NAT Control applications and users Upgrade the Firepower system

Table 7-1. Capabilities of the Firepower Licenses

[Table 7-2](#) describes the subscription codes for the Firepower licenses. The Malware and URL Filtering licenses are available in two formats — as an add-on, or in a bundle with a Threat license.

License	Expiry	Which One to Purchase
Base	Permanent	No separate purchase, included automatically during a device purchase
Threat	Term based	T - Threat license only
Malware	Term based	TM - Threat and Malware licenses in a bundle AMP - Malware license only. Purchased if a Threat license is already available.
URL Filtering	Term based	TMC – Threat, Malware and URL filtering licenses in a bundle URL - URL filtering license only. Purchased if a Threat license is already available.

Table 7-2. *Firepower License Subscription Purchase Options*

Best Practices

When you register an FMC with an FTD, there are couple of things to consider:

1. If you are in the middle of procuring a Firepower smart license, you can avoid any delay by turning on the Evaluation Mode on your FMC. It enables all of the security features on an FMC for the first 90 days of enablement, and allows you to register an FTD with an FMC immediately.
2. If there is an intermediate device that translates the management IP addresses of your Firepower systems, use a unique NAT ID during their registration process.
3. Before you begin the registration process, make sure that the network settings on Firepower appliances are correct. Both FMC and FTD should be able to communicate each other using their IP addresses. If you choose to perform a registration using hostnames or domain names, verify the name resolution before you attempt to register. You can run a simple ping test between an FMC and FTD using their Fully Qualified Domain Names (FQDNs). If the ping test fails due to the name resolution failure, check if the Firepower appliances are configured with an appropriate DNS server, or if the DNS server is responding to the queries.

Licensing a Firepower System

Enabling a feature on a brand new Firepower System is not a straightforward process. First, you need to purchase the necessary subscriptions. Then, obtain the smart licenses by registering the FMC with the Smart License Server. Finally, you have to enable a feature by applying the licenses to an FTD from the web interface of an FMC.

[Figure 7-3](#) summarizes the steps to obtain and apply a smart license on a Firepower system.

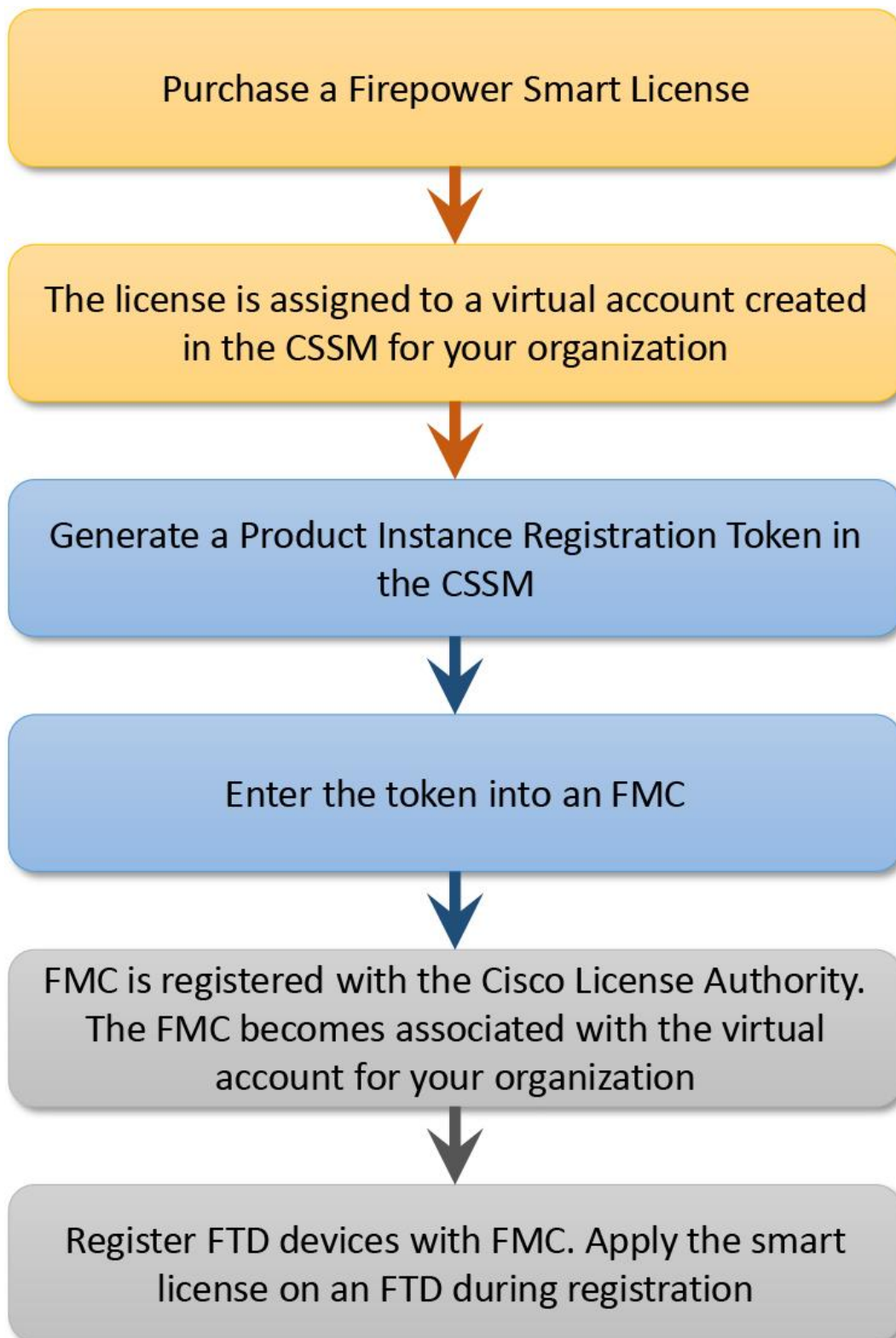


Figure 7-3. *Workflow to Purchase, Generate and Apply a Smart License*

Configuration

You cannot register an FTD with an FMC until you register the FMC with a Smart Licensing Server, or enable the evaluation mode.

[Figure 7-4](#) shows a notification in the **Add Device** window. This message appears when you attempt to register an FTD without registering the FMC with a Smart Licensing Server, or without enabling the Evaluation Mode.

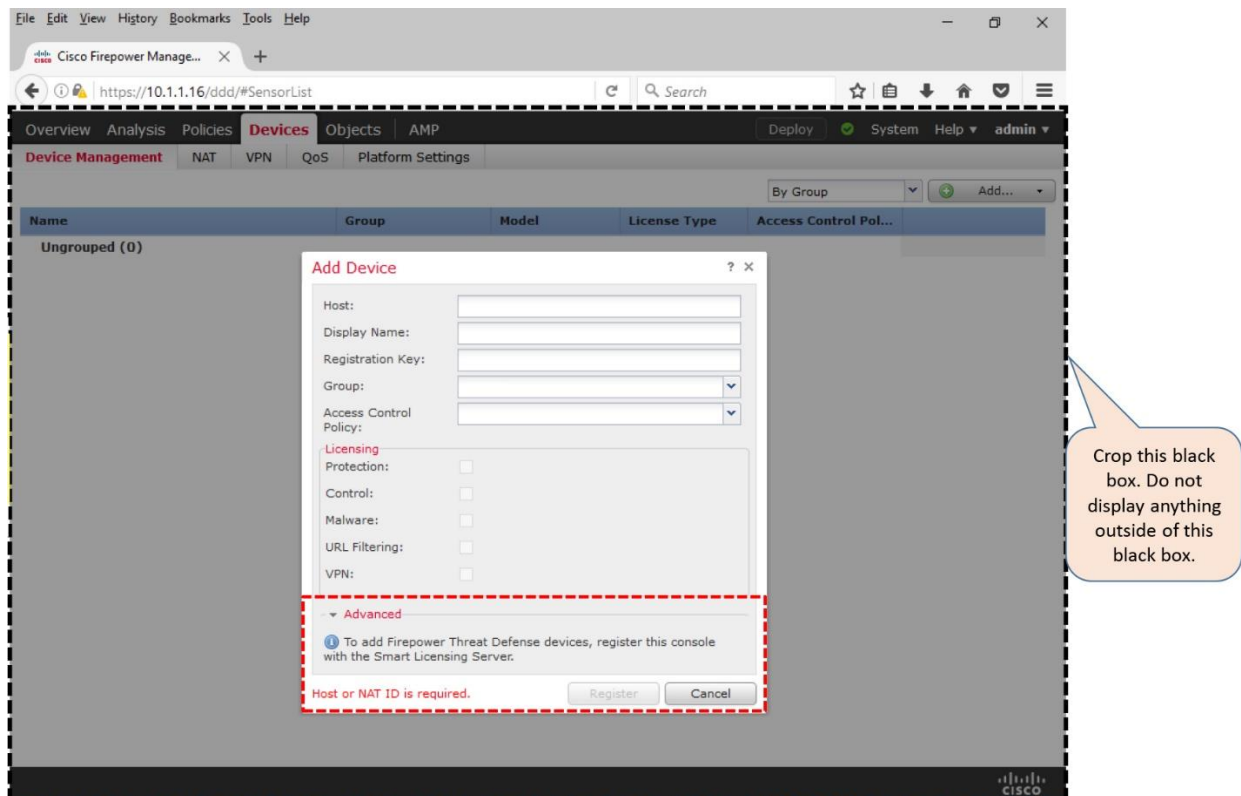


Figure 7-4. Notification for Registering an FMC with the Smart License Server

If you are in the middle of procuring a Firepower smart license, you can avoid any delay by turning on the Evaluation Mode on your FMC. It enables all of the security features on an FMC for the first 90 days of enablement, and allows you to register an FTD with an FMC immediately. The following section describes how to enable Evaluation Mode on an FMC.

Evaluation Mode

To enable the Evaluation Mode, follow the steps below:

Step 1. Go to the **System > Licenses > Smart Licenses** page. The **Evaluation Mode** button appears.

Note

The **Evaluation Mode** button does not appear once the 90-day period expires. You can retrieve the button by reimaging the FMC.

[Figure 7-5](#) shows the **Evaluation Mode** button on the Smart License page.

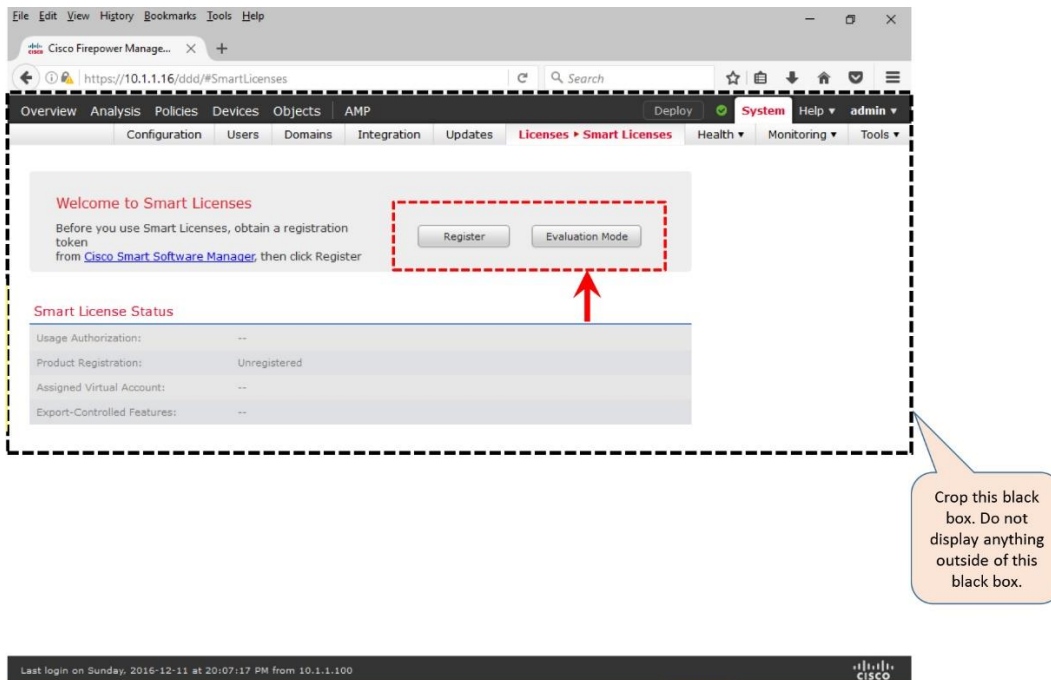


Figure 7-5. Button that Enables the Evaluation Mode

Step 2. Click the **Evaluation Mode** button. A confirmation message appears to remind you that the Evaluation Mode is a one-time option, and available for 90-day.

Step 3. Select **Yes** to begin the 90-day period.

[Figure 7-6](#) confirms that the Firepower System enables full functionality for 90-day period after you enable the Evaluation Mode.

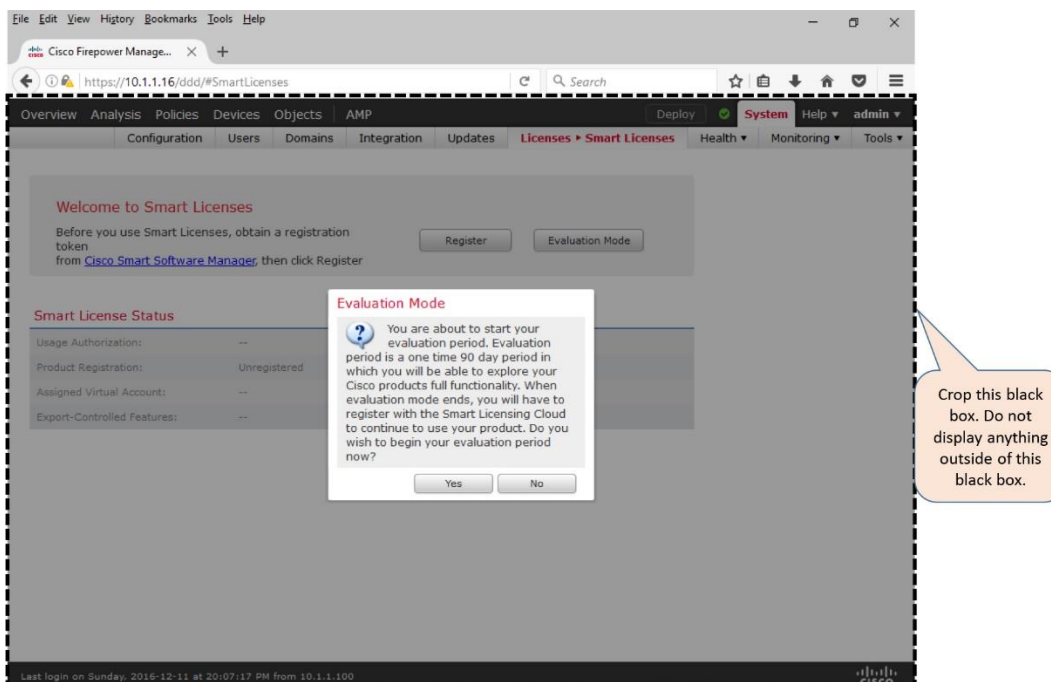


Figure 7-6. Confirmation of the Enablement of the Evaluation Mode

Registration with the Smart Software Manager

To register an FMC with the Smart Software Manager, follow the steps below:

Step 1. Login to the Cisco.com support portal, and navigate to the Cisco Smart Software Manager (CSSM).

Step 2. Access the virtual account created for your organization to generate a new token.

[Figure 7-7](#) shows the **New Token** button that randomly generates a long string. You can copy the string using the **Action** option.

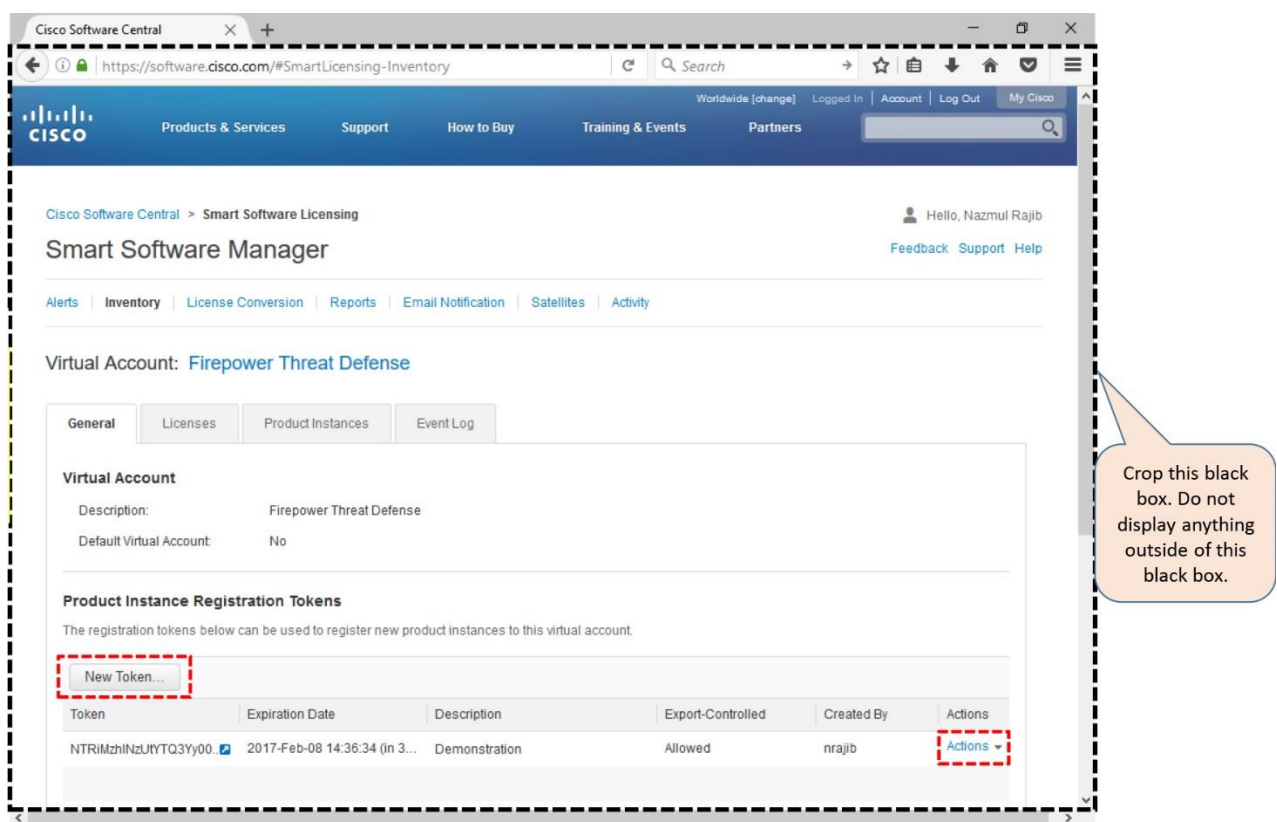


Figure 7-7. View of a Virtual Account on the CSSM Web Portal

Step 3. Copy the token from the CSSM, and paste it in the **Smart Licensing Product Registration** form on your FMC. To access the form, select the **Register** button on the **System > Licenses > Smart Licenses** page.

[Figure 7-8](#) displays a form where you paste the long string token generated by the CSSM.

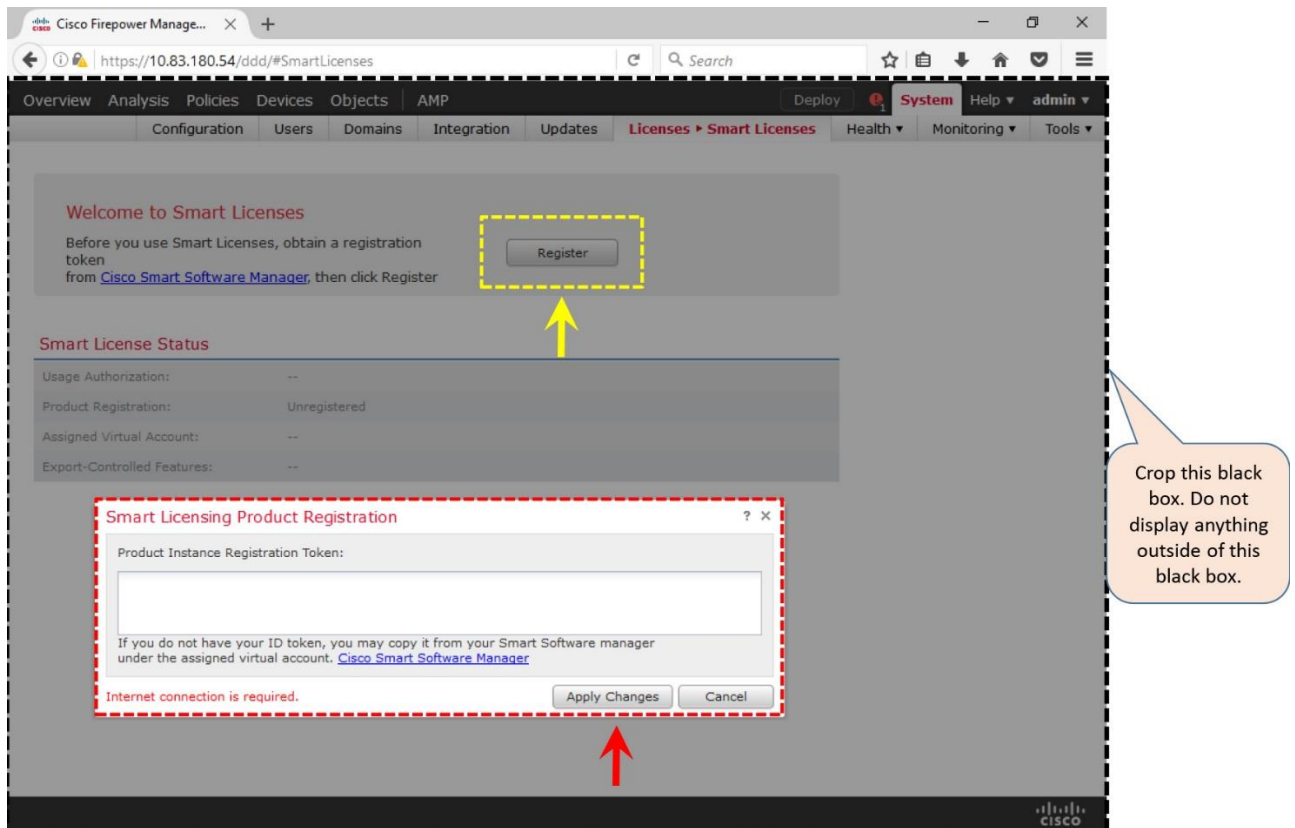


Figure 7-8. *Smart Licensing Product Registration Form*

Step 4. Select the **Apply Changes** button to begin the registration process with the Smart License Authority. A confirmation message appears upon a successful registration.

You can apply your desired license on an FTD device during the registration process. Later, you can also select the **Edit License** button to the Smart License page to manage the associations of licenses with any managed devices.

[Figure 7-9](#) confirms that the FMC is successfully registered with the Smart License authority. The Smart License Status shows healthy states (green check boxes), and the name of the virtual account of your organization.

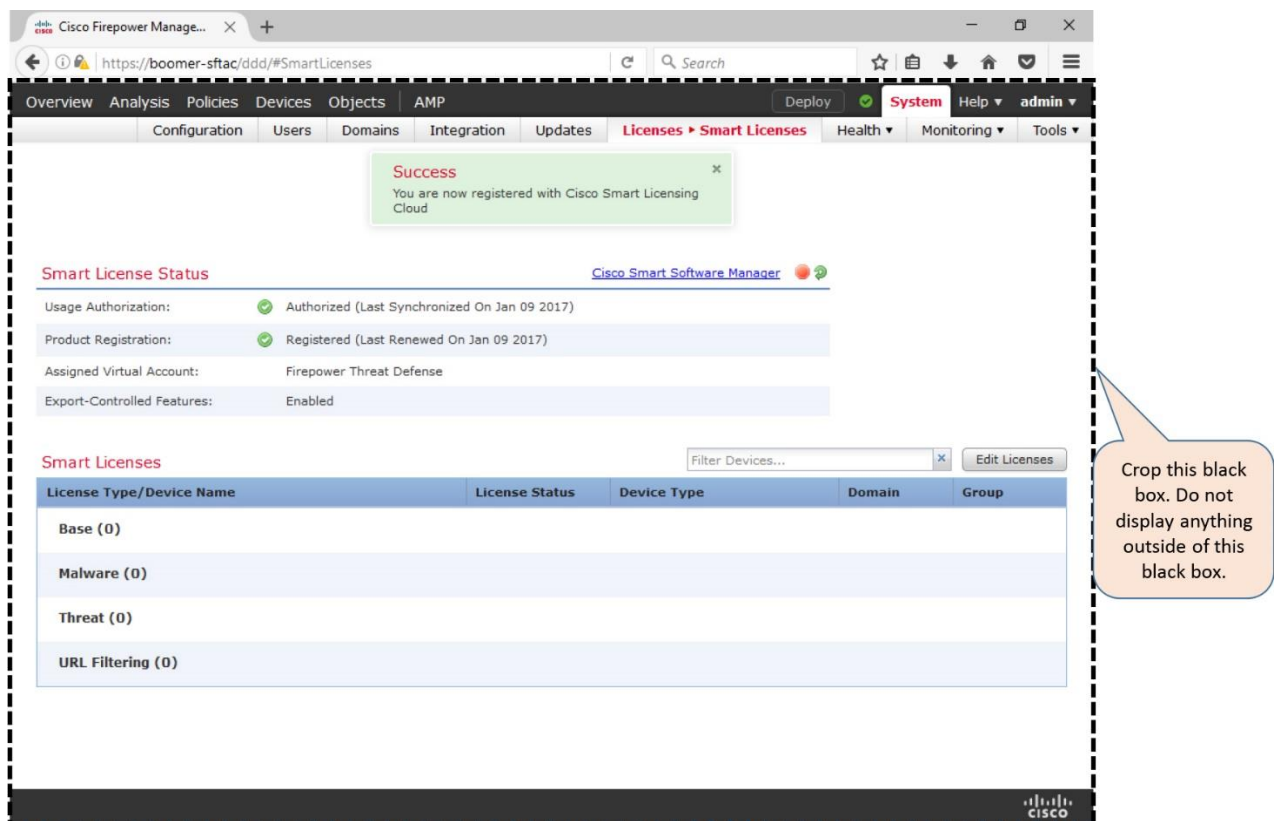


Figure 7-9. Confirmation of Registration of an FMC with the Smart License Authority

Verification of a Smart License Issue

If your FMC is unable to communicate with the License Server, make sure the FMC is configured to connect directly to the Cisco Smart Software Manager (CSSM). You can confirm the setting from the **System > Integration > Smart Software Satellite** page.

[Figure 7-10](#) shows two options to connect an FMC. By default, the **Connect directly to Cisco Smart Software Manager** is selected.

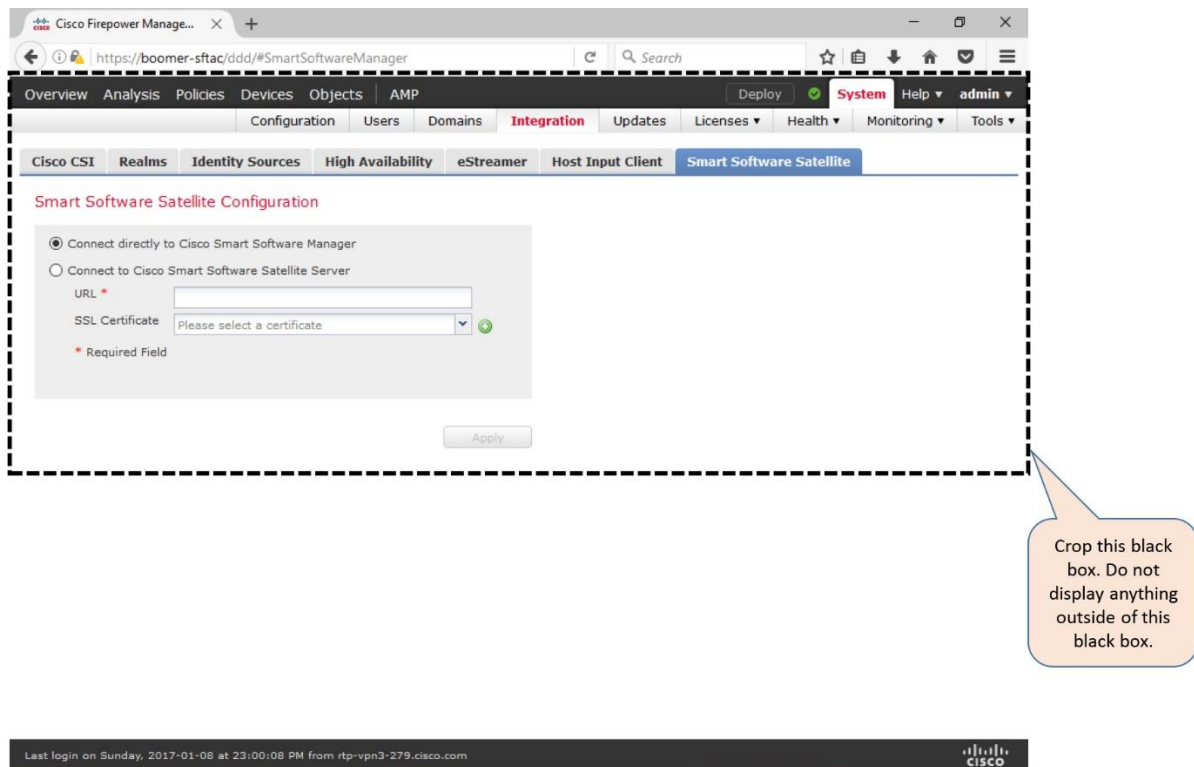


Figure 7-10. Options to Connect an FMC with Different Types of License Servers

The web interface of an FMC displays notifications when it successfully registers, or fails to register, with a License Server. To investigate any communication error, you can also debug any related processes from the CLI of an FMC.

[Example 7-1](#) shows that the FMC is able to successfully connect and register with the Cisco License Authority

Example 7-1 Debug of a Successful Connection between an FMC and a License Server

```
admin@FMC:~$ sudo tail -f /var/log/sam.log
Password:

[timestamp] PID : 12133 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
registerIdToken
start:
token (NGJmZThZjItZjVknZC00TcyLWI5MTAAatNGRhMzExZDM5MzVmLTE0ODY1NjMzZ%0AOD1MM
DN8RmZweWJ5eG
9Z0c...)
[timestamp] PID : 12133 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
[socket conn]
compose msg header: type[7], len[147], seq[1]
[timestamp] PID : 12133 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
[socket conn]
establishConnection start
[timestamp] PID : 12133 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
[socket conn]
```

```

Connected to server
[timestamp] PID : 12133 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
[socket conn]
'/var/sf/run/smart_agent.sock' Exiting the loop
[timestamp] PID : 12133 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
[socket conn]
Connection successful!
[timestamp] PID : 12133 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
[socket conn]
initSequence: 3
[timestamp] PID : 12133 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
[socket conn]
establishConnection done
[timestamp] PID : 12133 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
[socket conn]
sendMsg: successfully sent the msg!
[timestamp] PID : 12133 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
[socket conn]
recvMsg get: type[1007], len[141], seq[0], msg[error:0
authorization:AUTHORIZED,1483970615 registration:REGISTERED,1483970610
virtual_acct:Firepower Threat Defense export_control:1]

```

[Example 7-2](#) demonstrates a scenario where an FMC is able to connect a Smart License Server successfully, but fails to register with the server due to an invalid token.

Example 7-2 *Debug of a Registration Failure between an FMC and a License Server*

```

[timestamp] PID : 463 Process : mojo_server.pl [SAM-DBG-LOG]: [socket conn]
Closing
Connection
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
registerIdToken
start:
token(NGJmZThhZjItZjVkJkZCooyTcyLWI5MTAtNGRhMzExZDM5MzVmLTE0ODY1NjMz%0AODk1MD
N8RmZweWJ5eG9ZY)
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
[socket conn]
compose msg header: type[7], len[147], seq[1]
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
[socket conn]
establishConnection start
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
[socket conn]
Connected to server
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
[socket conn]
'/var/sf/run/smart_agent.sock'
Exiting the loop
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
[socket conn]
Connection successful!
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
[socket conn]
initSequence: 9
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
[socket conn]
establishConnection done
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
[socket conn]
sendMsg: successfully sent the msg!

```

```
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
[socket conn]
recvMsg get: type[1003], len [203], seq[0], msg[Response error:
{"token":["The token
'NGJmZThhZjItZjVkJkZCooyTcyLWI5MTAtNGRhMzExZDM5MzVmLTE0ODY1NjMz%0AODk1MDN8RmZ
weWJ5eG9ZY is
not valid."]]}
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
[socket conn]
Closing Connection
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
registerIdToken
return: $VAR1 = {
    'error' => 17
};
```

Registration of a Firepower System

Registration of a Firepower System is a two-step process. You must begin the registration process from your FTD. At first, you enter the FMC information on your FTD, and then you provide the FTD information on your FMC.

Configuration

In order to register an FTD with an FMC, you need to have access to the CLI of an FTD, and to the web interface of an FMC. The following section describes the entire process to complete a registration.

Setup an FTD

After you install FTD software successfully, you should be able to connect to the CLI of an FTD through Secure Shell (SSH) or console terminal. Upon a successful access to the FTD software, you will see the default CLI prompt ‘>’.

[Example 7-3](#) confirms that a freshly installed FTD has no connection with a management appliance.

Example 7-3 Output of the “show managers” Command

```
> show managers
No managers configured.
>
```

Let’s add an FMC on your FTD — run the **configure manager add** command along with the management IP address of the FMC. You also have to provide a one-time registration key which is used only during the registration process. A unique NAT ID is necessary only if there is an intermediate networking device that translates the IP addresses of your Firepower system. The command syntax is below:

```
> configure manager add IP_Address_of_FMC Registration_Key NAT_ID
```

[Example 7-4](#) demonstrates a successful addition of an FMC with the management IP address 10.1.1.16. The configuration uses *RegKey* as the one-time temporary registration key, and *NatId* as a NAT ID. The usage of a NAT ID is optional when the management IP addresses are not translated by any intermediate devices.

Example 7-4 *Addition of an FMC on the FTD*

```
> configure manager add 10.1.1.16 RegKey NatId
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in
FMC.
>
```

The configuration on your FTD is complete. The next step is to add this FTD on your FMC. Before you go to the next step, you can optionally check the current status of the registration.

[Example 7-5](#) shows the “pending” registration status after you add an FMC on an FTD. The registration status changes to “completed” after you perform the next step successfully.

Example 7-5 *Registration Status Appears as Pending After an FMC is Added on an FTD*

```
> show managers
Host                : 10.1.1.16
Registration Key    : ****
Registration        : pending
RPC Status          :
>
```

[Setup an FMC](#)

The second step of the registration process is to enter the detail of your FTD on the web interface of an FMC. When you add an FTD, you must use the same registration key (and the same NAT ID, if used) that you configured on the FTD, previously. Here are the steps you have to follow:

Step 1. Login to the web interface of your FMC. Go to the **Devices > Device Management > Add Device** page. The **Add Device** window appears.

[Figure 7-11](#) shows the navigation to the **Add Device** option. You must add an FMC on your FTD before you attempt to add the FTD detail on this window.

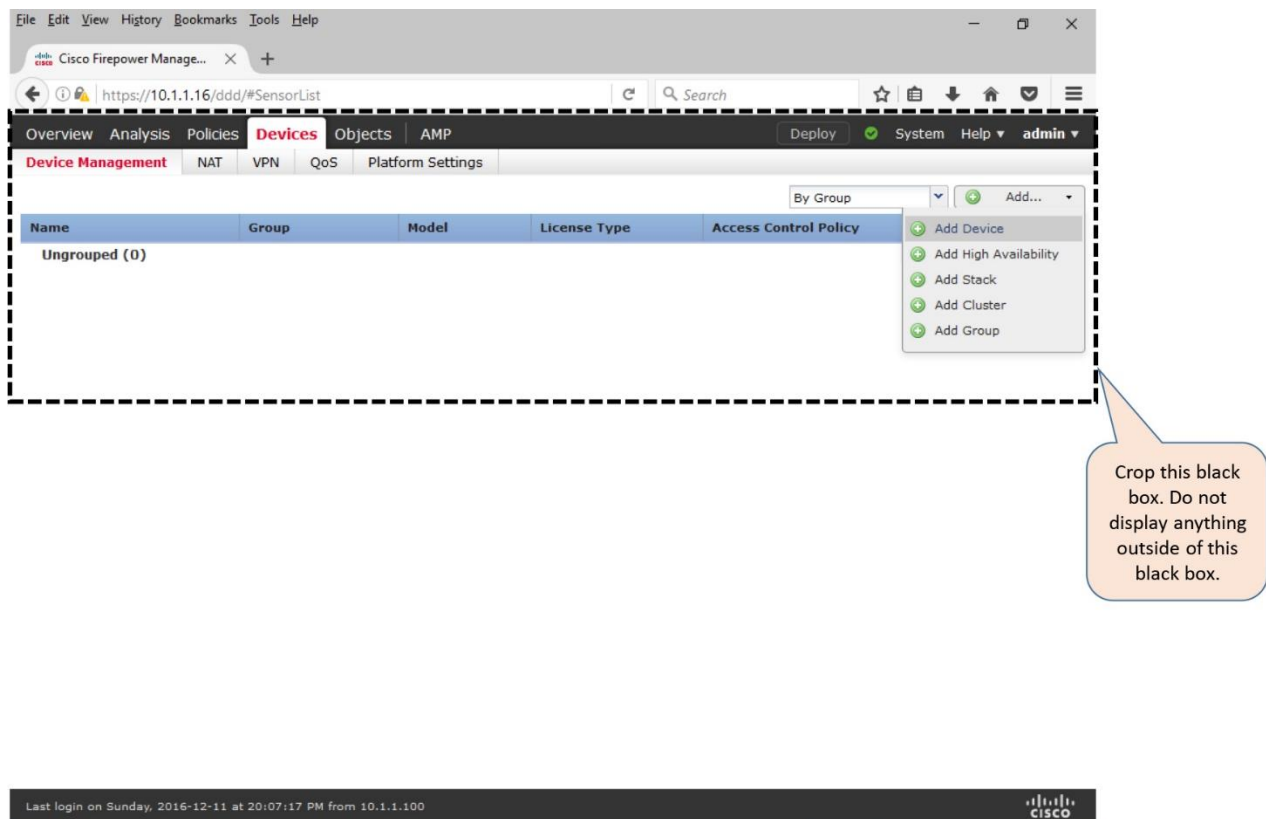


Figure 7-11. Navigation to the Add Device Window

Step 2. On the **Host** field, enter the IP address of the FTD management interface.

Step 3. On the **Display Name** field, provide a name that will be displayed on the FMC web interface to indicate this FTD.

Step 4. In the **Registration Key** field, enter *RegKey* — the same key you used when you added the FMC on your FTD earlier.

Step 5. Select an **Access Control Policy** that you want to apply to your FTD initially. If this is a new deployment, the FMC may not have any preconfigured Access Control policy. You can, however, create a policy on the fly by choosing the **Create new policy** option from the drop-down.

Caution

A registration process can fail if you select an Access Control policy that was created for a different device model, or configured with a component that is unsupported on your FTD. Therefore, if you not sure about the configurations an old Access Control policy, create a new policy on the fly, and select it. It ensures that the registration will not fail due to an incompatible Access Control policy.

[Figure 7-12](#) shows the creation of a new Access Control Policy called *AC Policy*. The **New Policy** window appears when you select the **Create new policy** option from the drop down. The image shows a very basic configuration that is good for a successful registration. You can edit and enhance this policy later.

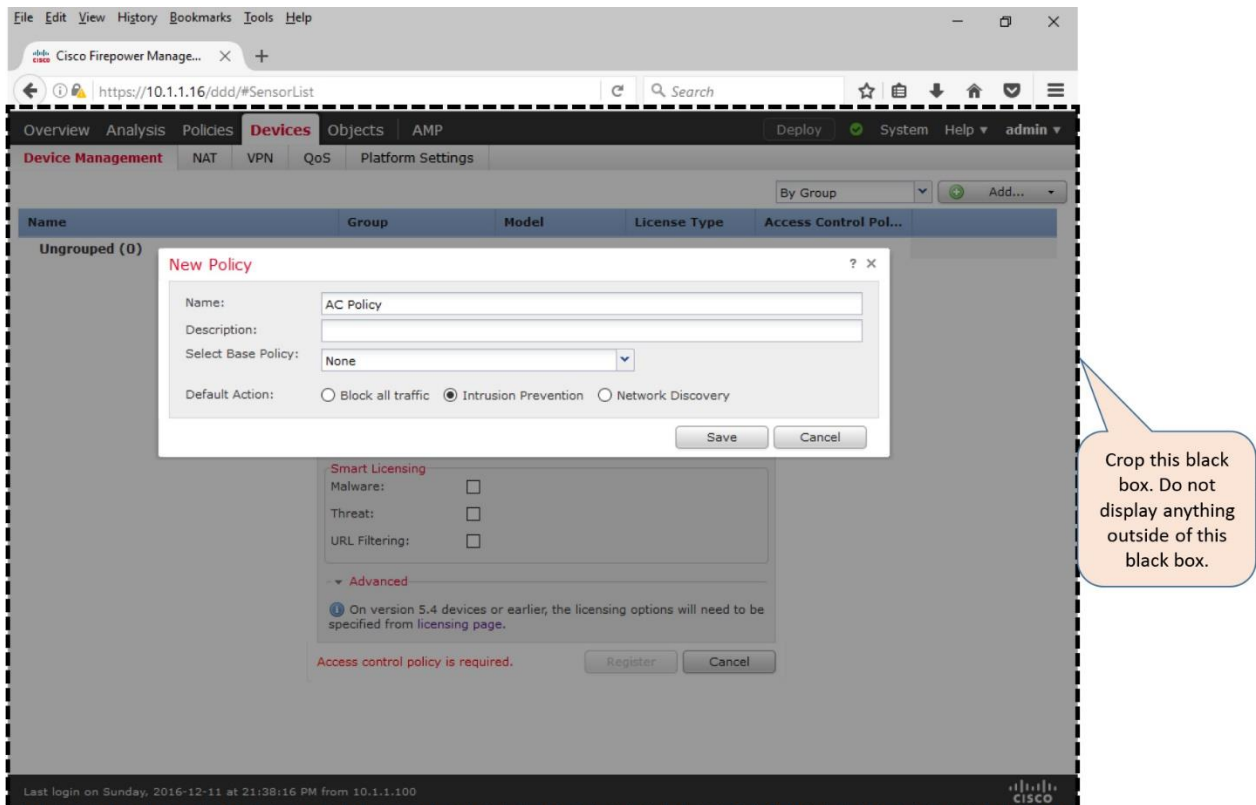


Figure 7-12. A Simple Access Control Policy — Created on the Fly during Registration

Step 6. Under **Smart Licensing** section, select the features that you want to apply, such as, Malware, Threat, URL Filtering.

Step 7. In the **Advanced** section, provide a unique NAT ID if there is an intermediate device that translates the management IP addresses of your Firepower systems. This is an optional step if there is no NAT device between your FMC and FTD.

[Figure 7-13](#) shows that the **Add Device** window is populated with the detail of the FTD. Note that the same registration key (*RegKey*) and NAT ID (*NatId*) are used on FMC and FTD.

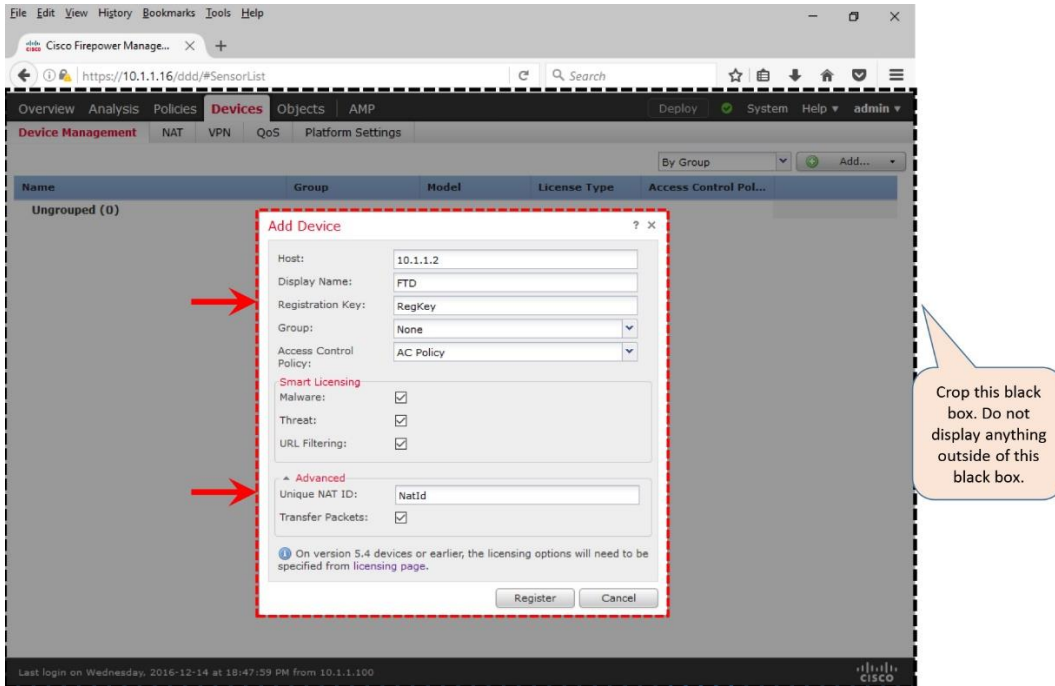


Figure 7-13. Filling Up the Fields on the Add Device Window

Step 8. The **Transfer Packets** option allows an FTD to send the associated packets to FMC when any security events are generated. By default, this option is enabled.

Step 9. Last of all, click the **Register** button. The registration process begins through an encrypted tunnel.

[Figure 7-14](#) demonstrates the ongoing registration process on the web interface.

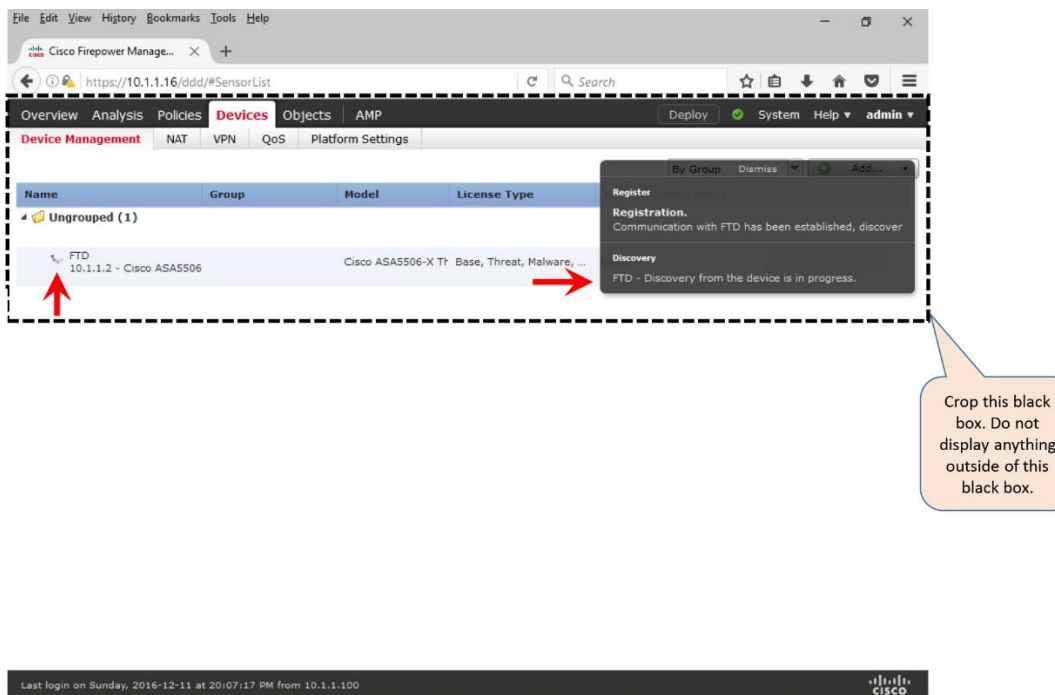


Figure 7-14. Registration Process is in Progress (Spinning Icon)

[Figure 7-15](#) confirms a successful registration. The FTD device model, software version, and the applied feature licenses are displayed upon a successful registration.

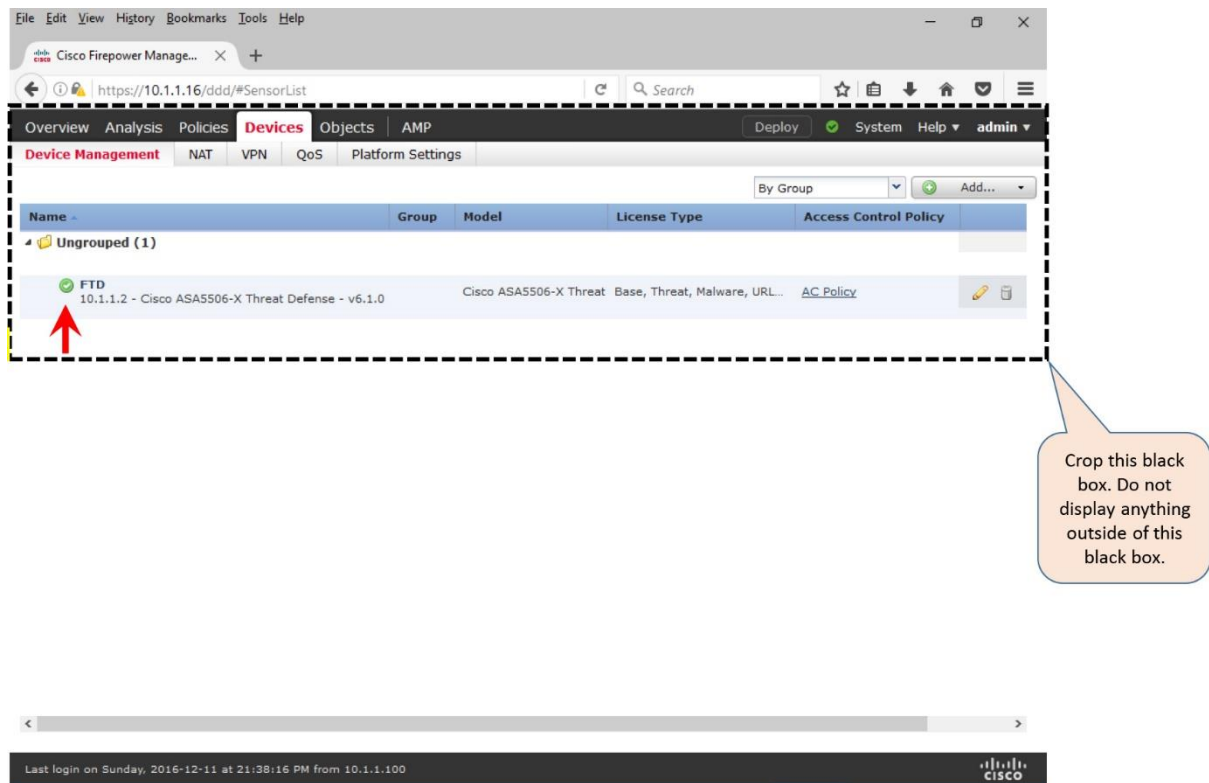


Figure 7-15. Registration Process is Complete (Spinning Icon Turns into a Solid Icon)

Verification of the Registration and Connection

If the registration process between an FTD and FMC is unsuccessful, FMC displays an error message for it. Additionally, you can run various commands to verify the communication status between an FTD and FMC.

[Figure 7-16](#) shows an error message that can appear when a registration attempt fails due to communication issue, incompatible software version, or mismatched registration key.

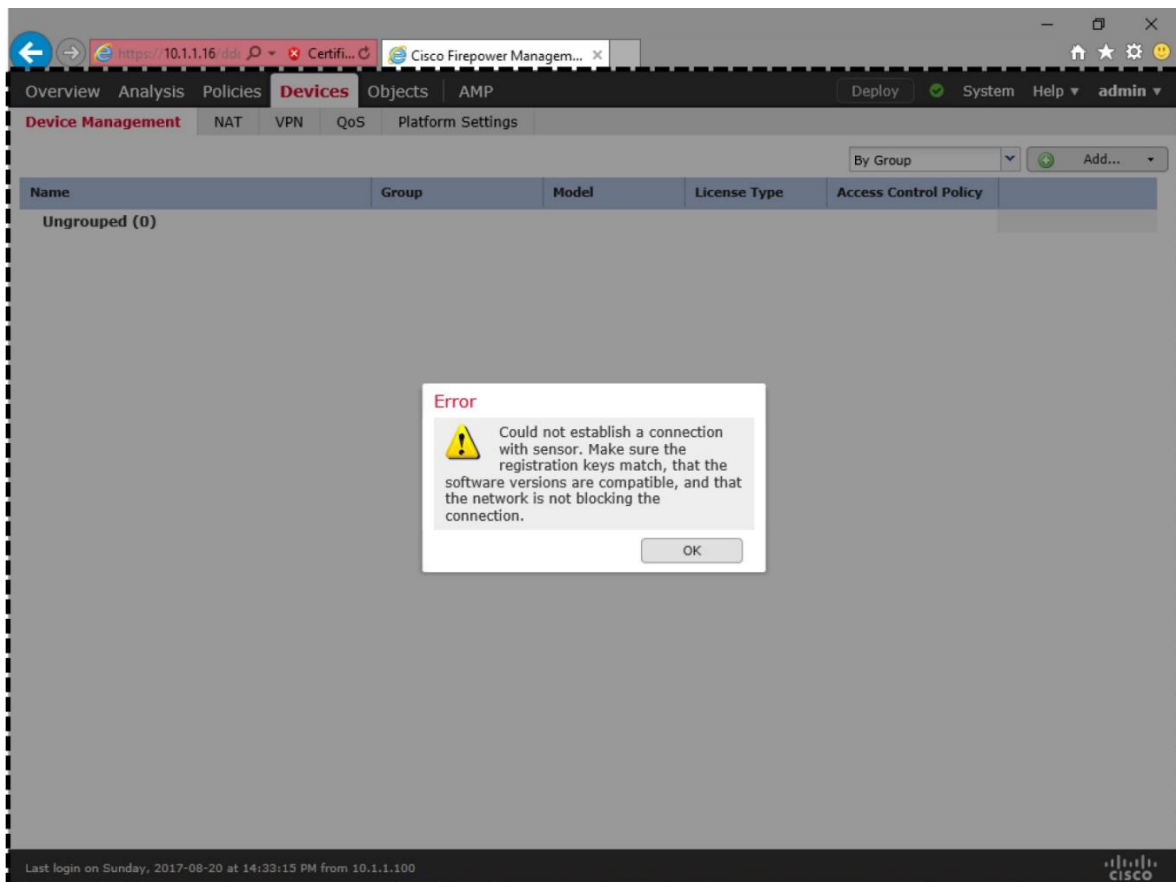


Figure 7-16. *Error Message Appears on the GUI due to a Registration Failure*

[Example 7-6](#) shows two different registration statuses — pending and completed — that appear on the CLI of the FTD. The “pending” status appears after you add an FMC on the FTD CLI. The registration status changes to “completed” after you are able to add the FTD on the FMC web interface.

Example 7-6 *Display of the Registration Status from the CLI of an FTD*

! Registration status: After you complete the first step (Add an FMC on FTD CLI)

```
> show managers
Host                : 10.1.1.16
Registration Key    : ****
Registration        : pending
RPC Status         :
>
```

! Registration status: After you complete the second and final step (Add an FTD on FMC GUI)

```
> show managers
Type                : Manager
Host                : 10.1.1.16
```

```
Registration                : Completed
>
```

As soon as you enter the FMC information on your FTD, the TCP port 8305 on FTD starts listening for incoming connections — expects packets from an FMC. Similarly, as soon as you enter the FTD information on an FMC, the FMC begins listening on TCP port 8305.

[Example 7-7](#) shows the transition of TCP port 8305 on an FTD and FMC during the registration process.

Example 7-7 *Verification of the Management Port Status*

! First, on the CLI of an FTD, when you enter the FMC detail, it opens the TCP port 8305 on FTD.

```
admin@FTD:~$ sudo netstat -antp | grep -i 8305
tcp        0      0 10.1.1.2:8305          0.0.0.0:*              LISTEN
933/sftunnel
admin@FTD:~$
```

! Then, on the GUI of an FMC, when you enter the FTD detail, the FMC begins listening on TCP port 8305. FMC responses the FTD's registration request from a random port 49707.

```
admin@FMC:~$ sudo netstat -antp | grep -i 8305
tcp        0      0 10.1.1.16:8305        0.0.0.0:*              LISTEN
10095/sftunnel
tcp        0      0 10.1.1.16:49707      10.1.1.2:8305         ESTABLISHED
10095/sftunnel
root@FMC:~#
```

! Upon a successful registration, the connections appear fully established on the FMC.

```
admin@FMC:~$ sudo netstat -antp | grep -i 8305
tcp        0      0 10.1.1.16:49707      10.1.1.2:8305         ESTABLISHED
10095/sftunnel
tcp        0      0 10.1.1.16:8305        10.1.1.2:54998        ESTABLISHED
10095/sftunnel
admin@FMC:~$
```

If the port status does not change from the listening state to the established state, the FMC may have not received any registration requests from FTD, or the FTD may have not received any acknowledgements from the FMC. Let's take a look what happens at the packet level during the registration process.

Caution

The following two examples utilize the built-in packet capture tools on FTD and FMC to display the transactions of packets. Capturing packets in a product system can impact the system performance. Therefore, if necessary, you should run this tool only during a maintenance window, or in a lab environment.

[Example 7-8](#) shows the exchange of packets right after you begin the registration process, which is, after adding an FMC on the CLI of an FTD. Since, at this stage, you have not yet entered the detail of FTD on the FMC, the FMC (IP: 10.1.1.6) keeps sending the RESET packets in response to the SYN packets from the FTD (IP: 10.1.1.2).

Example 7-8 *Transaction of Packets — After Adding an FMC on the CLI of an FTD*

```
! Capturing Packets on the FTD Management Interface

> capture-traffic

Please choose domain to capture traffic from:
 0 - br1

Selection? 0

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: host 10.1.1.16

HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on br1, link-type EN10MB (Ethernet), capture size 96 bytes

[timestamp] IP FTD.46373 > 10.1.1.16.8305: Flags [S], seq 1709676008, win
14600, options
[mss 1460,sackOK,TS val 87180 ecr 0,nop,wscale 7], length 0
[timestamp] IP 10.1.1.16.8305 > FTD.46373: Flags [R.], seq 0, ack
1709676009, win 0, length 0
[timestamp] IP FTD.58441 > 10.1.1.16.8305: Flags [S], seq 3021847438, win
14600, options
[mss 1460,sackOK,TS val 87380 ecr 0,nop,wscale 7], length 0
[timestamp] IP 10.1.1.16.8305 > FTD.58441: Flags [R.], seq 0, ack
3021847439, win 0, length 0
[timestamp] IP FTD.46814 > 10.1.1.16.8305: Flags [S], seq 1334198689, win
14600, options
[mss 1460,sackOK,TS val 88317 ecr 0,nop,wscale 7], length 0
[timestamp] IP 10.1.1.16.8305 > FTD.46814: Flags [R.], seq 0, ack
1334198690, win 0, length 0
[timestamp] IP FTD.45854 > 10.1.1.16.8305: Flags [S], seq 1274367969, win
14600, options
[mss 1460,sackOK,TS val 88517 ecr 0,nop,wscale 7], length 0
[timestamp] IP 10.1.1.16.8305 > FTD.45854: Flags [R.], seq 0, ack
1274367970, win 0, length 0
.
.
<Output Omitted>

! Capturing Packets on the FMC Management Interface

admin@FMC:~$ sudo tcpdump -i eth0 host 10.1.1.2
Password:

HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
```

```

[timestamp] IP 10.1.1.2.46373 > FMC.8305: Flags [S], seq 1709676008, win
14600, options
[mss 1460,sackOK,TS val 87180 ecr 0,nop,wscale 7], length 0
[timestamp] IP FMC.8305 > 10.1.1.2.46373: Flags [R.], seq 0, ack
1709676009, win 0, length 0
[timestamp] IP 10.1.1.2.58441 > FMC.8305: Flags [S], seq 3021847438, win
14600, options
[mss 1460,sackOK,TS val 87380 ecr 0,nop,wscale 7], length 0
[timestamp] IP FMC.8305 > 10.1.1.2.58441: Flags [R.], seq 0, ack
3021847439, win 0, length 0
[timestamp] IP 10.1.1.2.46814 > FMC.8305: Flags [S], seq 1334198689, win
14600, options
[mss 1460,sackOK,TS val 88317 ecr 0,nop,wscale 7], length 0
[timestamp] IP FMC.8305 > 10.1.1.2.46814: Flags [R.], seq 0, ack
1334198690, win 0, length 0
[timestamp] IP 10.1.1.2.45854 > FMC.8305: Flags [S], seq 1274367969, win
14600, options
[mss 1460,sackOK,TS val 88517 ecr 0,nop,wscale 7], length 0
[timestamp] IP FMC.8305 > 10.1.1.2.45854: Flags [R.], seq 0, ack
1274367970, win 0, length 0
.
.
<Output Omitted>

```

[Example 7-9](#) exhibits the next phase of the registration process. As soon as you enter the FTD detail on the web interface of the FMC, FMC stops sending RESET packets.

Example 7-9 *Transaction of Packets — After Adding the FTD on the GUI of the FMC*

! On the FMC Interface

```

.
<Output Omitted>
.
[timestamp] IP FMC.51509 > 10.1.1.2.8305: Flags [S], seq 1804119299, win
14600, options
[mss 1460,sackOK,TS val 258976 ecr 0,nop,wscale 7], length 0
[timestamp] IP 10.1.1.2.8305 > FMC.51509: Flags [S.], seq 4103916511, ack
1804119300,
win 14480, options [mss 1460,sackOK,TS val 93418 ecr 258976,nop,wscale 7],
length 0
[timestamp] IP FMC.51509 > 10.1.1.2.8305: Flags [.], ack 1, win 115,
options
[nop,nop,TS val 258976 ecr 93418], length 0
[timestamp] IP FMC.51509 > 10.1.1.2.8305: Flags [P.], ack 1, win 115,
options
[nop,nop,TS val 258985 ecr 93418], length 247
[timestamp] IP 10.1.1.2.8305 > FMC.51509: Flags [.], ack 248, win 122,
options
[nop,nop,TS val 93422 ecr 258985], length 0
[timestamp] IP 10.1.1.2.8305 > FMC.51509: Flags [.], ack 248, win 122,
options
[nop,nop,TS val 93423 ecr 258985], length 1448
[timestamp] IP 10.1.1.2.8305 > FMC.51509: Flags [P.], ack 248, win 122,
options
[nop,nop,TS val 93423 ecr 258985], length 774
.
<Output Omitted>
.

```

! Press the Control+C keys to exit and stop capturing.

! On the FTD Interface

```
.
<Output Omitted>
.
[timestamp] IP 10.1.1.16.51509 > FTD.8305: Flags [S], seq 1804119299, win
14600, options
[mss 1460,sackOK,TS val 258976 ecr 0,nop,wscale 7], length 0
[timestamp] IP FTD.8305 > 10.1.1.16.51509: Flags [S.], seq 4103916511, ack
1804119300,
win 14480, options [mss 1460,sackOK,TS val 93418 ecr 258976,nop,wscale 7],
length 0
[timestamp] IP 10.1.1.16.51509 > FTD.8305: Flags [.] , ack 1, win 115,
options
[nop,nop,TS val 258976 ecr 93418], length 0
[timestamp] IP 10.1.1.16.51509 > FTD.8305: Flags [P.] , ack 1, win 115,
options
[nop,nop,TS val 258985 ecr 93418], length 247
[timestamp] IP FTD.8305 > 10.1.1.16.51509: Flags [.] , ack 248, win 122,
options
[nop,nop,TS val 93422 ecr 258985], length 0
[timestamp] IP FTD.8305 > 10.1.1.16.51509: Flags [.] , ack 248, win 122,
options
[nop,nop,TS val 93423 ecr 258985], length 1448
[timestamp] IP FTD.8305 > 10.1.1.16.51509: Flags [P.] , ack 248, win 122,
options
[nop,nop,TS val 93423 ecr 258985], length 774
```

<Output Omitted>

! Press the Control+C keys to exit and stop capturing.

If you do not notice any activities on the management interfaces, check if the TCP port 8305 is bi-directionally allowed on any intermediate network devices between the FMC and FTD. You can test this by connecting to the TCP port 8305 of your FTD from the FMC directly.

[Example 7-10](#) shows a successful telnet connection from an FMC to the port 8305 of an FTD. It confirms that the port 8305 on the FTD (IP address 10.1.1.2) is allowed by any intermediate router or firewall.

Example 7-10 *Successful Telnet Connection from an FMC to the Port 8305 of an FTD*

```
admin@FMC:~$ telnet 10.1.1.2 8305
Trying 10.1.1.2...
Connected to 10.1.1.2.
Escape character is '^]'.
^]                               ! Press the Ctrl and ] keys together
telnet> quit
Connection closed.
admin@fmc:~$
```

The FMC and FTD complete their registration process through the SFTunnel — an encrypted communication channel between the management interfaces of an FMC and FTD. Using the TCP port 8305, an FTD and FMC establish this channel to complete any administrative tasks between them, such as, to register an FTD with an FMC, to exchange keep alive heartbeats, to receive new security policies and configurations from an FMC, to send security events to an FMC, to synchronize time with an FMC, etc.

The **netstat** or **tcpdump** command that you ran earlier confirms the establishment of a tunnel between an FMC and FTD. However, it does not display what happens inside of an encrypted tunnel at the application level. Firepower system provides a command line tool, **sftunnel-status**, that shows the statistics of all of the services running through an encrypted security tunnel.

[Example 7-11](#) exhibits an output of the **sftunnel-status** command on an FTD. From the output, you can conclude that the logical management interface of FTD (name: br1, IP: 10.1.1.2) is connected to the management interface of FMC (name: eth0, IP: 10.1.1.16). Two channels, A and B, are connected for control packets and event traffic respectively. The tunnel is encrypted using the AES256-GCM-SHA384 cipher.

Example 7-11 *Output of the sftunnel-status Command on an FTD*

```
> sftunnel-status
```

```
SFTUNNEL Start Time: Sun Dec 11 23:51:56 2016

    Both IPv4 and IPv6 connectivity is supported
    Broadcast count = 2
    Reserved SSL connections: 0
    Management Interfaces: 1
    br1 (control events) 10.1.1.2,

*****

**RUN STATUS**10.1.1.16*****
    Cipher used = AES256-GCM-SHA384 (strength:256 bits)
    ChannelA Connected: Yes, Interface br1
    Cipher used = AES256-GCM-SHA384 (strength:256 bits)
    ChannelB Connected: Yes, Interface br1
    Registration: Completed.
    IPv4 Connection to peer '10.1.1.16' Start Time: Mon Dec 12 00:13:44
2016

PEER INFO:
    sw_version 6.1.0
    sw_build 330
    Management Interfaces: 1
    eth0 (control events) 10.1.1.16,
    Peer channel Channel-A is valid type (CONTROL), using 'br1',
connected
to '10.1.1.16' via '10.1.1.2'
    Peer channel Channel-B is valid type (EVENT), using 'br1',
connected to
'10.1.1.16' via '10.1.1.2'
```


TOTAL TRANSMITTED MESSAGES <24> for Health Events service
RECEIVED MESSAGES <12> for Health Events service
SEND MESSAGES <12> for Health Events service
HALT REQUEST SEND COUNTER <0> for Health Events service
STORED MESSAGES for Health service (service 0/peer 0)
STATE <Process messages> for Health Events service
REQUESTED FOR REMOTE <Process messages> for Health Events service
REQUESTED FROM REMOTE <Process messages> for Health Events service

TOTAL TRANSMITTED MESSAGES <3> for Identity service
RECEIVED MESSAGES <2> for Identity service
SEND MESSAGES <1> for Identity service
HALT REQUEST SEND COUNTER <0> for Identity service
STORED MESSAGES for Identity service (service 0/peer 0)
STATE <Process messages> for Identity service
REQUESTED FOR REMOTE <Process messages> for Identity service
REQUESTED FROM REMOTE <Process messages> for Identity service

TOTAL TRANSMITTED MESSAGES <76> for RPC service
RECEIVED MESSAGES <38> for RPC service
SEND MESSAGES <38> for RPC service
HALT REQUEST SEND COUNTER <0> for RPC service
STORED MESSAGES for RPC service (service 0/peer 0)
STATE <Process messages> for RPC service
REQUESTED FOR REMOTE <Process messages> for RPC service
REQUESTED FROM REMOTE <Process messages> for RPC service

TOTAL TRANSMITTED MESSAGES <41> for IP(NTP) service
RECEIVED MESSAGES <27> for IP(NTP) service
SEND MESSAGES <14> for IP(NTP) service
HALT REQUEST SEND COUNTER <0> for IP(NTP) service
STORED MESSAGES for IP(NTP) service (service 0/peer 0)
STATE <Process messages> for IP(NTP) service
REQUESTED FOR REMOTE <Process messages> for IP(NTP) service
REQUESTED FROM REMOTE <Process messages> for IP(NTP) service

TOTAL TRANSMITTED MESSAGES <5> for IDS Events service
RECEIVED MESSAGES <0> for service IDS Events service
SEND MESSAGES <5> for IDS Events service
HALT REQUEST SEND COUNTER <0> for IDS Events service
STORED MESSAGES for IDS Events service (service 0/peer 0)
STATE <Process messages> for IDS Events service
REQUESTED FOR REMOTE <Process messages> for IDS Events service
REQUESTED FROM REMOTE <Process messages> for IDS Events service

.
.
<Output omitted for brevity>

.
.
Heartbeat Send Time: Mon Dec 12 00:28:17 2016
Heartbeat Received Time: Mon Dec 12 00:29:35 2016

RPC STATUS10.1.1.16*****
'ip' => '10.1.1.16',

```
'uuid' => '7d3aa42c-95c7-11e6-a825-2c6c588f5f38',
'ipv6' => 'IPv6 is not configured for management',
'name' => '10.1.1.16',
'active' => '1',
'uuid_gw' => '',
'last_changed' => 'Wed Oct 19 17:56:43 2016'
```

Check routes:

>

You can view a similar statistics on an FMC by running the **sftunnel_status.pl** tool. By comparing the data on both devices, FMC and FTD, you can determine any potential issues with the SFTunnel. The command syntax on an FMC is:

```
admin@FMC:~$ sudo sftunnel_status.pl <Management_IP_Address_of_the_FTD>
```

[Example 7-12](#) shows an output of the **sftunnel_status.pl** tool on an FMC. It confirms that the FMC (10.1.1.16) is registered with an FTD (10.1.1.2), and is communicating actively.

Example 7-12 Output of the *sftunnel_status.pl* Tool on an FMC

```
admin@FMC:~$ sudo sftunnel_status.pl 10.1.1.2
Password:
```

```
Check peer 10.1.1.2 at /usr/local/sf/bin/sftunnel_status.pl line 19
SFTUNNEL Start Time: Mon Dec 12 01:17:21 2016
```

```
Key File    = /etc/sf/keys/sftunnel-key.pem
Cert File   = /etc/sf/keys/sftunnel-cert.pem
CA Cert     = /etc/sf/ca_root/cacert.pem
FIPS,STIG,CC = 0,0,0
Both IPv4 and IPv6 connectivity is supported
Broadcast count = 1
Reserved SSL connections: 0
Management Interfaces: 1
eth0 (control events) 10.1.1.16,
```

```
*****
```

```
**RUN STATUS**10.1.1.2*****
Cipher used = AES256-GCM-SHA384 (strength:256 bits)
ChannelA Connected: Yes, Interface eth0
Cipher used = AES256-GCM-SHA384 (strength:256 bits)
ChannelB Connected: Yes, Interface eth0
Registration: Completed.
IPv4 Connection to peer '10.1.1.2' Start Time: Mon Dec 12 02:58:54
2016
```

```
PEER INFO:
  sw_version 6.1.0
  sw_build 330
  Management Interfaces: 1
  br1 (control events) 10.1.1.2,
  Peer channel Channel-A is valid type (CONTROL), using 'eth0',
connected to
'10.1.1.2' via '10.1.1.16'
  Peer channel Channel-B is valid type (EVENT), using 'eth0',
connected to
```

'10.1.1.2' via '10.1.1.16'

```
TOTAL TRANSMITTED MESSAGES <20> for Health Events service
RECEIVED MESSAGES <10> for Health Events service
SEND MESSAGES <10> for Health Events service
HALT REQUEST SEND COUNTER <0> for Health Events service
STORED MESSAGES for Health service (service 0/peer 0)
STATE <Process messages> for Health Events service
REQUESTED FOR REMOTE <Process messages> for Health Events service
REQUESTED FROM REMOTE <Process messages> for Health Events service
```

```
TOTAL TRANSMITTED MESSAGES <3> for Identity service
RECEIVED MESSAGES <1> for Identity service
SEND MESSAGES <2> for Identity service
HALT REQUEST SEND COUNTER <0> for Identity service
STORED MESSAGES for Identity service (service 0/peer 0)
STATE <Process messages> for Identity service
REQUESTED FOR REMOTE <Process messages> for Identity service
REQUESTED FROM REMOTE <Process messages> for Identity service
```

.
.
<Output omitted>

After comparing the SFTunnel statistics on both FMC and FTD, if you notice any anomaly, you can utilize the **manage_procs.pl** tool on the FTD to restart the channels between an FMC and FTD.

Caution

If you run the **manage_procs.pl** tool on an FMC, and the FMC is currently managing many FTD devices, it restarts the communication channel between the FMC and all of the FTD devices at the same time. If you need to restart the channel between the FMC and one particular FTD device only, then run the **manage_procs.pl** tool on the expert mode of the desired FTD.

[Example 7-13](#) shows the operation of the **manage_procs.pl** tool on the expert mode of an FTD. Select the option 3 to restart the communication channel.

Example 7-13 Menu of The *manage_procs.pl* Tool

```
> expert
admin@FTD:~$ sudo manage_procs.pl
Password:
***** Configuration Utility *****

 1 Reconfigure Correlator
 2 Reconfigure and flush Correlator
 3 Restart Comm. channel
 4 Update routes
 5 Reset all routes
 6 Validate Network
 0 Exit

*****
Enter choice: 3

***** Configuration Utility *****
```

- 1 Reconfigure Correlator
- 2 Reconfigure and flush Correlator
- 3 Restart Comm. channel
- 4 Update routes
- 5 Reset all routes
- 6 Validate Network
- 0 Exit

```
*****
Enter choice: 0
Thank you
admin@FTD:~$
```

While the channel restarts, the system generates debug logs for stopping and starting various services. These logs provide you a detail insight of the Firepower system communication at the application level, and allow you to determine any complex communication issues.

[Example 7-14](#) shows the debug of a restart process from the CLI of an FMC. As soon as you begin the process on the FTD, the FMC fails to connect to the FTD. After the connection to the FTD (IP: 10.1.1.2) is closed, the FMC (IP: 10.1.1.16) automatically begins the connection reestablishment process with the FTD.

Example 7-14 *Debug Logs are Generated during the Communication Channel Restart*

```
admin@FMC:~$ sudo tail -f /var/log/messages | grep 10.1.1.2
Password:
```

! The following message appears on an FMC as soon as you begin the process on the FTD. It confirms that the FMC is unable to connect to the FTD.

```
[timestamp] sftunneld:sf_connections [INFO] Unable to receive message from peer
10.1.1.2:Closed
[timestamp] sftunneld:sf_channel [INFO] >> ChannelState dropChannel peer
10.1.1.2 /
channelA / CONTROL [ msgSock & ssl_context ] <<
[timestamp] sftunneld:sf_connections [INFO] Exiting channel (recv). Peer
10.1.1.2 closed
connection on interface eth0.
[timestamp] sftunneld:sf_connections [INFO] Failed to send in control
channel for peer
10.1.1.2 (eth0)
[timestamp] sftunneld:sf_channel [INFO] >> ChannelState dropChannel peer
10.1.1.2 /
channelA / DROPPED [ msgSock & ssl_context ] <<
[timestamp] sftunneld:sf_channel [INFO] >> ChannelState freeChannel peer
10.1.1.2 /
channelA / DROPPED [ msgSock & ssl_context ] <<
[timestamp] sftunneld:sf_connections [INFO] Need to send SW version and
Published
Services to 10.1.1.2
[timestamp] sftunneld:sf_channel [INFO] >> ChannelState
do_dataio_for_heartbeat peer
10.1.1.2 / channelB / EVENT [ msgSock2 & ssl_context2 ] <<
[timestamp] sftunneld:control_services [INFO] Successfully Send Interfaces
info to peer
```



```

[timestamp] sftunneld:sf_peers [INFO] Peer 10.1.1.2 needs the first
connection
[timestamp] sftunneld:sf_ssl [INFO] Verify accepted: Need a new connection
for peer 10.1.1.2 (1)
[timestamp] sftunneld:sf_ssl [INFO] Peer 10.1.1.2 supports multiple ports
[timestamp] sftunneld:sf_ssl [INFO] Peer 10.1.1.2 supports separate events
connection
[timestamp] sftunneld:sf_ssl [INFO] Peer 10.1.1.2 registration is complete
remotely
[timestamp] sftunneld:sf_peers [INFO] Peer 10.1.1.2 needs the first
connection
[timestamp] sftunneld:sf_ssl [INFO] Accept: Will start a child thread for
peer '10.1.1.2'
[timestamp] sftunneld:sf_ssl [INFO] Accept: Start child thread for peer
'10.1.1.2'
[timestamp] sftunneld:sf_channel [INFO] >>>>>> initChannels peer: 10.1.1.2
<<<<<<
[timestamp] sftunneld:stream_file [INFO] Stream CTX initialized for
10.1.1.2
[timestamp] sftunneld:sf_connections [INFO] Peer 10.1.1.2 main thread
started
[timestamp] sftunneld:control_services [INFO] Successfully Send Interfaces
info to peer 10.1.1.2 over eth0
[timestamp] sftunneld:sf_heartbeat [INFO] Saved SW VERSION from peer
10.1.1.2 (6.1.0)

[timestamp] sftunneld:sf_connections [INFO] Need to send SW version and
Published Services to 10.1.1.2
[timestamp] sftunneld:sf_channel [INFO] >> ChannelState
do_dataio_for_heartbeat peer 10.1.1.2 /
channelA / CONTROL [ msgSock & ssl_context ] <<
[timestamp] sftunneld:control_services [INFO] Interface br1 from 10.1.1.2
supports 'control events'
[timestamp] sftunneld:control_services [INFO] Interface br1 from 10.1.1.2
supports events
[timestamp] sftunneld:control_services [INFO] Interface br1 (10.1.1.2) from
10.1.1.2 is up
[timestamp] sftunneld:control_services [INFO] Peer 10.1.1.2 Notified that
it is NOT configured for dedicated events interface
[timestamp] sftunneld:sf_connections [INFO] Need to send SW version and
Published Services to 10.1.1.2
[timestamp] sftunneld:sf_channel [INFO] >> ChannelState
do_dataio_for_heartbeat peer 10.1.1.2 /
channelA / CONTROL [ msgSock & ssl_context ] <<
[timestamp] sftunneld:sf_heartbeat [INFO] Saved SW VERSION from peer
10.1.1.2 (6.1.0)
[timestamp] sfmgr:sfmanager [INFO] Established connection to sftunnel for
peer 10.1.1.2 (fd 8)
.
.
<Output omitted for brevity>
.
.
[timestamp] sftunneld:sf_heartbeat [INFO] Identity Service is published for
peer 10.1.1.2
[timestamp] sftunneld:sf_peers [INFO] Using a 20 entry queue for 10.1.1.2 -
7770
[timestamp] sfmbservice:sfmb_service [INFO] Start getting MB messages for
10.1.1.2
[timestamp] sfmbservice:sfmb_service [INFO] Established connection to peer
10.1.1.2

```

```
[timestamp] sftunneld:sf_heartbeat [INFO] Message Broker Service is published for peer 10.1.1.2
```

Summary

This chapter describes licensing and registration — two important initial tasks of a Firepower system deployment. In this chapter, you have learned the capabilities of different Firepower licenses and the steps to register an FMC with a Smart License Server. It also discusses the registration process, and the tools to investigate any communication issues.

Quiz

1. Which tool is used on FTD to view the statistics of events inside of the encrypted tunnel between an FTD and FMC?

- a. > sftunnel
- b. > sftunnel-status
- c. > sftunnel_status
- d. > sftunnel status

2. Which command confirms if an FTD is registered with an FMC?

- a. > show fmc
- b. > show console
- c. > show managers
- d. > show registration

3. Which statement is incorrect about registration?

- a. Always begin the registration process from an FTD.
- b. NAT ID is necessary only when there is an intermediate NAT device between an FMC and FTD.
- c. Before registering an FTD, the FMC must be connected to a license server.
- d. FTD and FMC use port 8305 for registration and management communication purpose.

4. Which command shows the logs between an FMC and a License Server?

- a. **sudo tail -f /var/log/messages**
- b. **sudo tail -f /var/log/messages.log**
- c. **sudo tail -f /var/log/cssm.log**

d. `sudo tail -f /var/log/sam.log`

5. Which tool allows you to restart the communication channel between an FMC and FTD?

a. `sftunnel_status.pl`

b. `sftunnel_restart.pl`

c. `manage_procs.pl`

d. `manage_channel.pl`

6. Which statement is correct about the smart license architecture?

a. Evaluation Mode allows you to test certain features, not all.

b. FTD connects to the Smart License Server to obtain licenses.

c. The Cisco Satellite server is an on premise virtual machine.

d. To register an FMC with the Smart License Server, run the command **`configure manager add <IP_Address_of_the_CSSM>`**

Chapter 8. Firepower Deployment in Routed Mode

You can deploy a Firepower Threat Defense (FTD) device as a default gateway for your network, so that the hosts can communicate with the FTD device in order to connect to any different subnet or internet. You can also deploy an FTD transparently, so that it becomes invisible to the hosts in your network. In short, you can deploy an FTD in two ways — Routed mode and Transparent mode. This chapter describes the processes to deploy an FTD in routed mode. You can learn about the transparent mode in the next chapter.

Essential Knowledge

In routed mode, FTD performs like a layer 3 hop. Each interface on an FTD connects to a different subnet. Upon configuration, an FTD can act as a default gateway for any particular subnet and is able to route traffic between different subnets.

[Figure 8-1](#) shows how a host interacts with an FTD device as its next layer 3 hop. In routed mode, each FTD interface connects to a unique subnet.

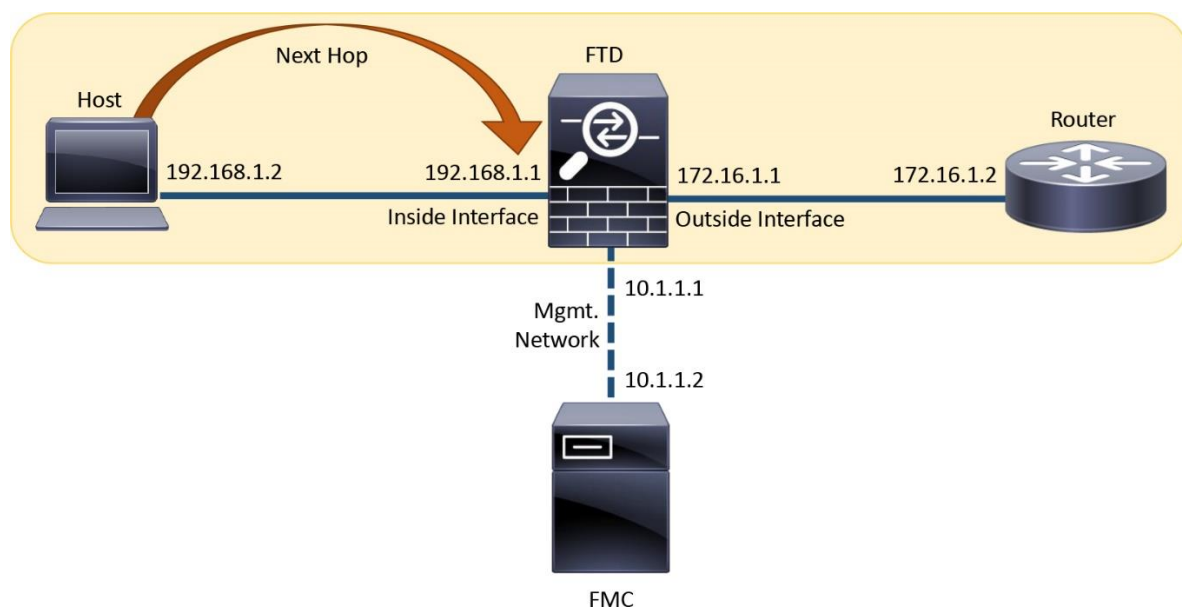


Figure 8-1. *Communication of a Host with an FTD in Routed Mode*

[Figure 8-2](#) exhibits the default gateways on each segment when an FTD is deployed in a typical real world network. The end users on a LAN uses the FTD physical interface as their gateway. An FTD can also use its inside interface as the default gateway for its management communication.

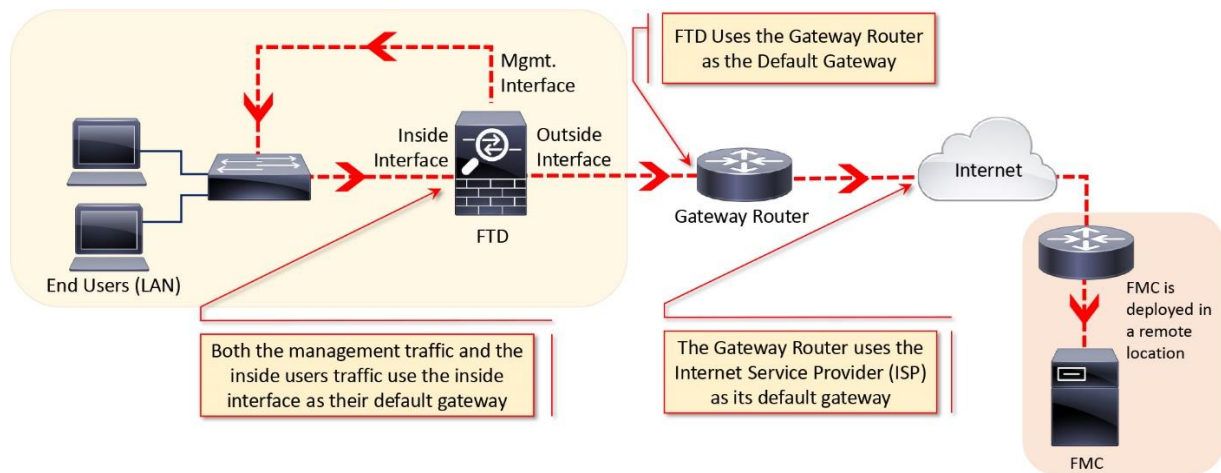


Figure 8-2. Deployment of an FTD in Routed Mode

Best Practices

If you want to deploy an FTD in routed mode, you can consider the following suggestions:

- Cisco recommends you not to configure the diagnostic interface with an IP address. It simplifies the network design and reduces configuration overhead.

When a diagnostic interface is configured with an IP address, the FTD considers it as a data interface. Each data interface on an FTD is required to be on different network. Therefore, the diagnostic interface (which must be on the same subnet as the logical management interface, br1) and the inside interface must be on two different subnets. To transfer traffic between two different subnetworks, a router is required.

- Changing of firewall mode wipes out any existing configurations on an FTD. Therefore, before you change the firewall mode from transparent to routed, or vice versa, take a note of your FTD configuration settings for future reference, in case you want to revert the FTD to the initial state. To view the current FTD configuration, run the **show running-config** on the CLI.

If you just want to change the firewall mode on your FTD, performing a backup of your security policy configuration is not necessary, because the Next-Generation security policies are defined and stored on the FMC. Once configured, FMC can deploy the same policies to one or more FTDs.

Configuration

Do you remember the last part of the FTD installation and initialization process? During the initialization, an FTD prompts to confirm the firewall mode where you select between the routed and transparent modes.

[Example 8-1](#) shows the prompts that appear during the last part of the system initialization. Here you can setup your FTD as routed or transparent mode.

Example 8-1 *Configuration of the Firewall Mode during the Initialization*

```
<Output Omitted>
.
.
Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...
Update policy deployment information
  - add device configuration
  - add network discovery
  - add system policy
.
.
<Output Omitted>
```

If you selected routed mode during the system initialization, you can skip the next two sections, and read the *Configure the Routed Interfaces* section.

Prerequisites

If you selected transparent mode during the system initialization, and now you want to reconfigure your FTD to the routed mode, you must unregister the FTD from the FMC. You cannot change the firewall mode when a manager is configured. To verify if an FTD is currently registered with an FMC, run the **show managers** command on the FTD.

[Example 8-2](#) shows that the FTD is currently registered with an FMC with IP address 10.1.1.16.

Example 8-2 *Verification of the Registration Status — FTD is Currently Registered*

```
> show managers
Type           : Manager
Host           : 10.1.1.16
Registration    : Completed
>
```

If you find that the FTD is currently registered with an FMC, you can unregister from the FMC web interface. To delete registration, go to the **Devices > Device Management** page, and click the delete icon next to your desired FTD.

[Figure 8-3](#) shows a trashcan icon that you select to delete the registration of an FTD from an FMC.

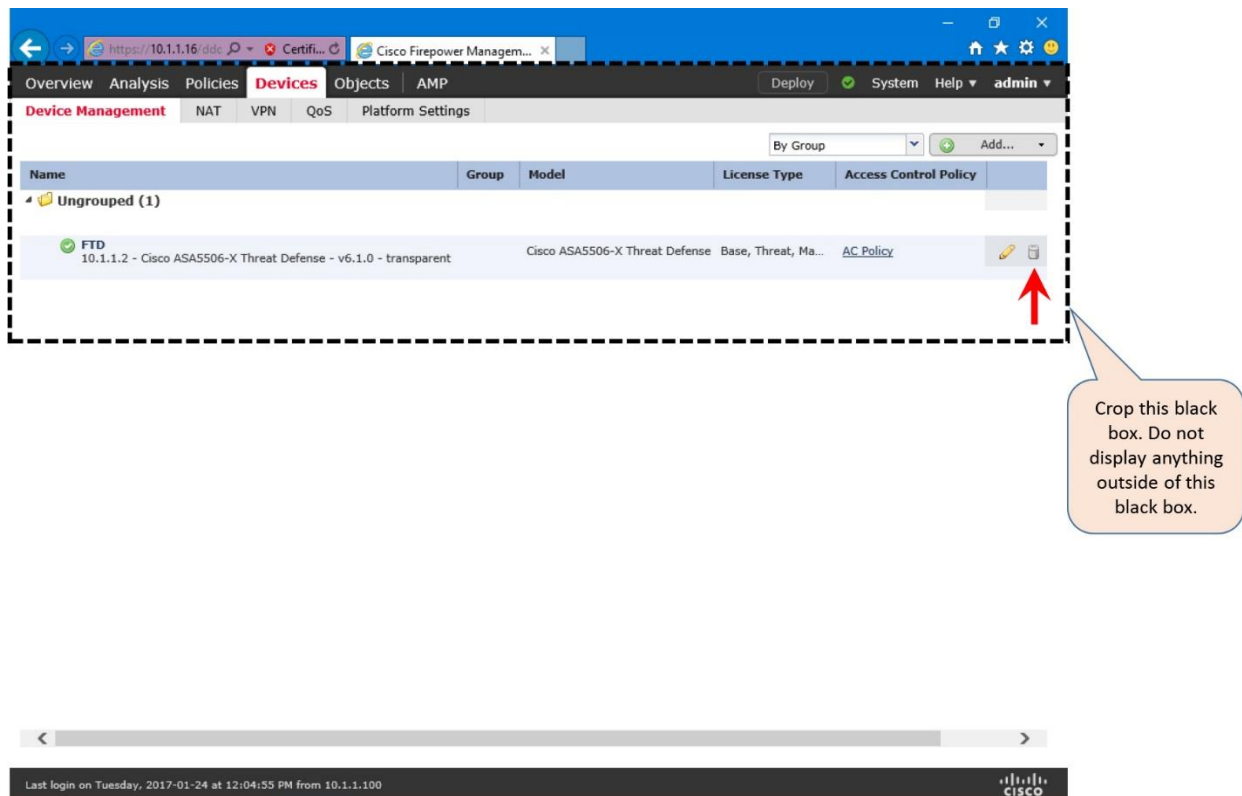


Figure 8-3. Option to Delete Firepower Registration

[Example 8-3](#) confirms that the FTD is currently not registered with any FMC.

Example 8-3 Verification of the Registration Status — FTD is not Registered

```
> show managers
No managers configured.
>
```

Firewall Mode Configuration

If your FTD is currently not registered with any FMC, you can change the firewall deployment mode. To configure an FTD with the routed mode, login to the CLI of the FTD, and run the **configure firewall routed** command.

[Example 8-4](#) illustrates the command to configure an FTD to the routed mode.

Example 8-4 Configuration of the Routed Mode

```
> configure firewall routed
```

```
This will destroy the current interface configurations, are you sure that
you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

After configuring an FTD with a desired mode, you can determine the status from the CLI.

[Example 8-5](#) confirms that the FTD is configured to the routed mode.

Example 8-5 Verification of the Firewall Deployment Mode

```
> show firewall
Firewall mode: Router
>
```

Alternatively, upon a successful registration, the web interface of an FMC also displays the current firewall deployment mode. You can view it from the **Devices > Device management** page.

[Figure 8-4](#) indicates that the FTD is configured in routed mode.

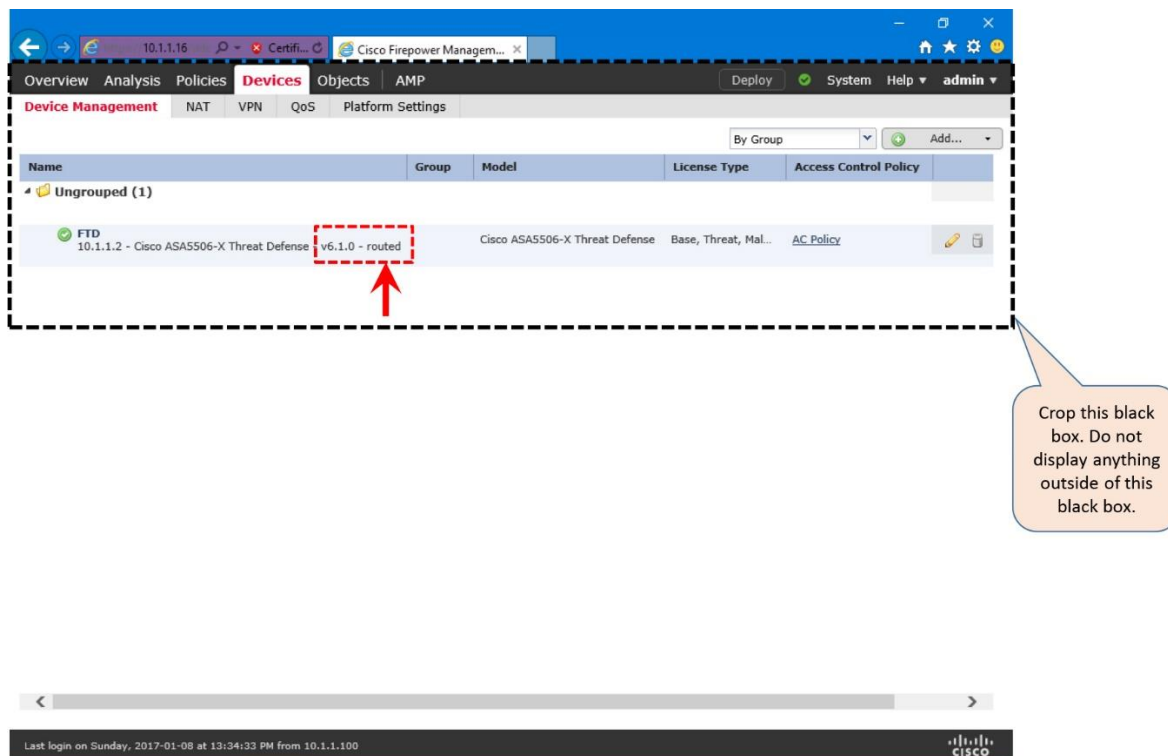


Figure 8-4. Current Deployment Mode of an FTD

Routed Interface Configuration

On an FTD, you can configure a data interface with static IP address. FTD can also work as a DHCP client, and obtain an IP address from a DHCP server. Furthermore, you can enable DHCP service on an FTD, which allows it to assign an IP address dynamically to its host.

Static IP Address

To configure a routed interface with static IP address, follow the steps below:

Step 1. Navigate to the **Devices > Device Management** page. A list of the managed devices appear.

Step 2. Click the pencil icon that is next to your desired FTD device. The device editor page appears.

[Figure 8-5](#) shows all of the physical interfaces of an FTD device in the device editor page, under the interface tab.

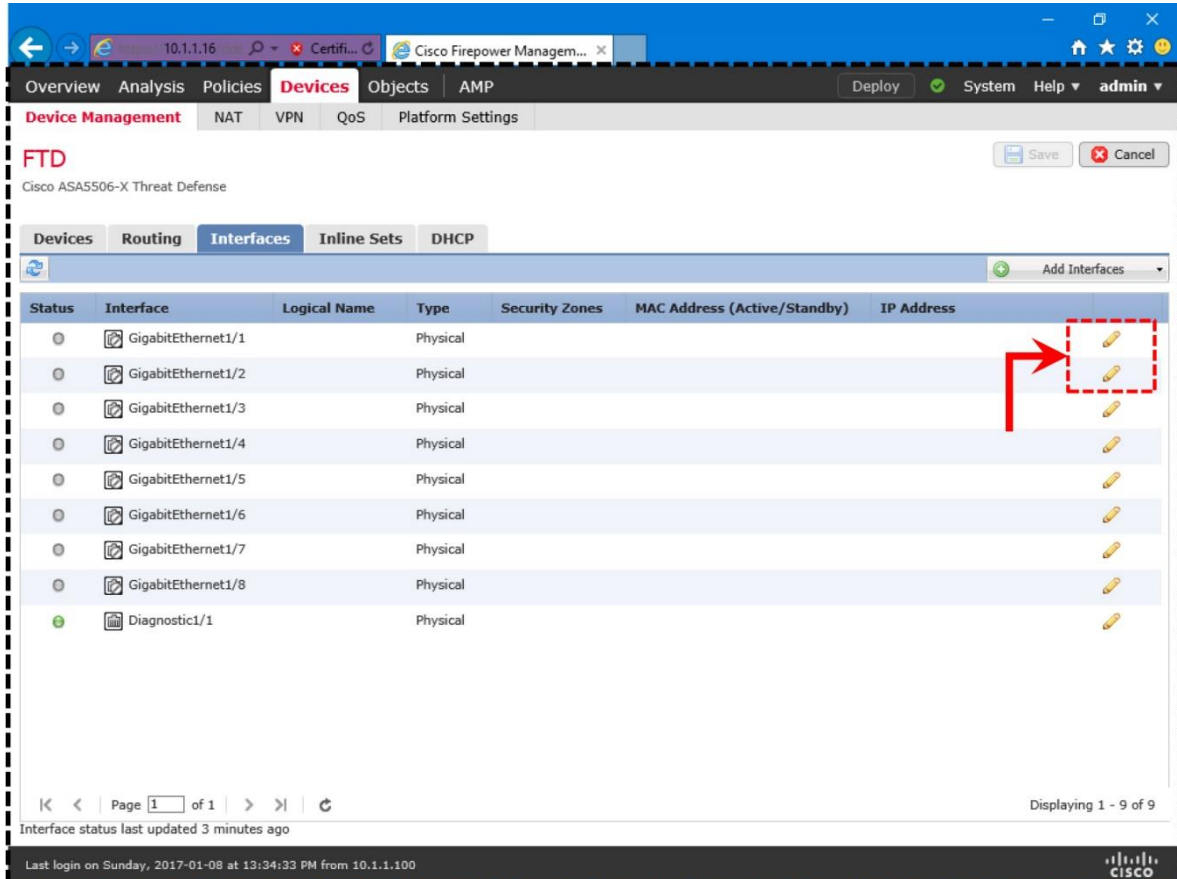


Figure 8-5. The Interface Configuration Tab is Located inside the Device Editor Page

Step 3. In the **Interfaces** tab, click the pencil icons next to the interface names to configure interfaces. Let's configure the **GigabitEthernet1/1** and **GigabitEthernet1/2** interfaces for the inside and outside networks, respectively, per the following settings.

[Figure 8-6](#) shows the interfaces of an FTD device. Note that both interfaces are connected to two different subnets.

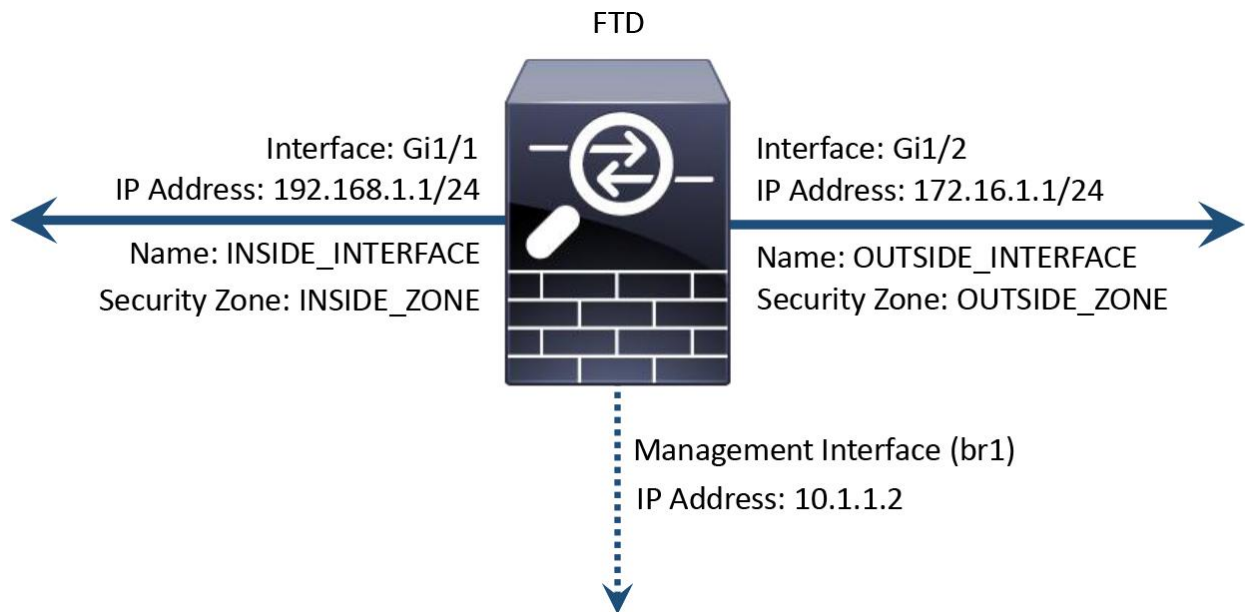


Figure 8-6. Overview of FTD Interface Configurations

[Table 8-1](#) summarizes the configuration settings for the **GigabitEthernet1/1** and **GigabitEthernet1/2** interfaces.

	GigabitEthernet1/1	GigabitEthernet1/2
Interface Name	INSIDE_INTERFACE	OUTSIDE_INTERFACE
Security Zone	INSIDE_ZONE	OUTSIDE_ZONE
IP Address	192.168.1.1/24	172.16.1.1/24

Table 8-1. Configuration Settings for GigabitEthernet1/1 and GigabitEthernet1/2

Note

To enable an interface, giving it a name is a requirement, however, configuring a security zone is an optional step.

Figure 8-7 shows the configurations on the GigabitEthernet1/1 interface that can act as the default gateway for the inside network.

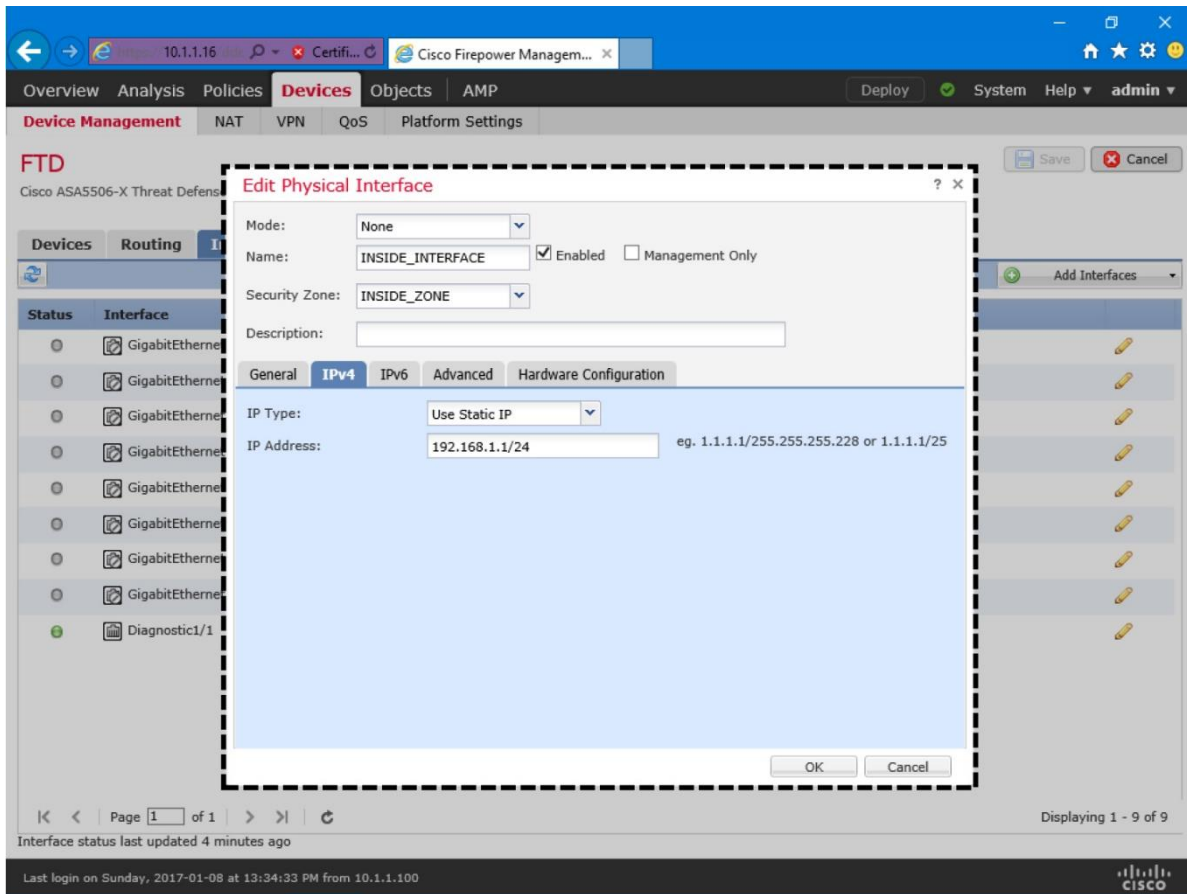


Figure 8-7. Configurations of the Inside Interface GigabitEthernet1/1

Figure 8-8 displays the configurations on the GigabitEthernet1/2 interface that is connected to the outside network.

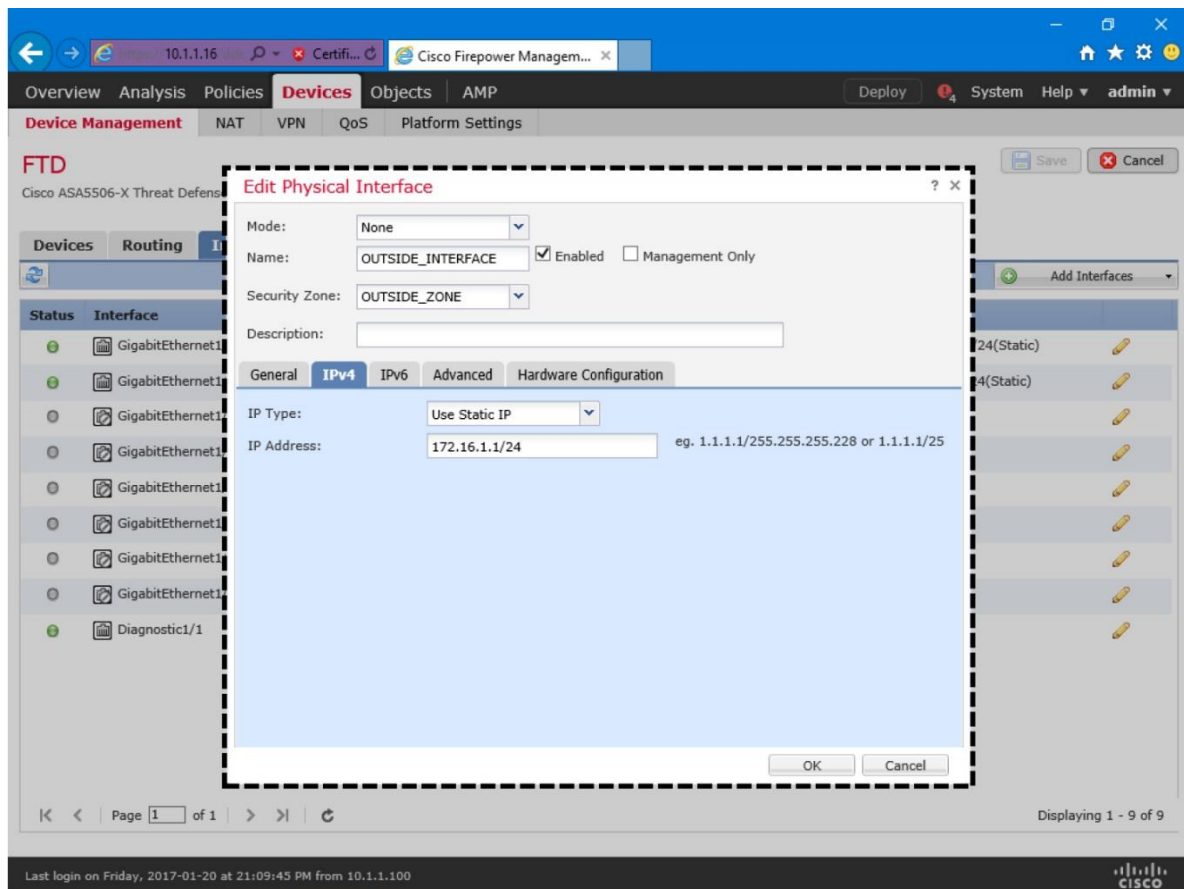


Figure 8-8. Configurations of the Outside Interface GigabitEthernet1/2

Step 4. After you configure both interfaces, click the **Save** button to save the configurations.

Step 5. Finally, you must click the **Deploy** button and apply the configurations to your FTD

Figure 8-9 shows two different buttons that you must select to save and apply any configuration changes on an FTD.

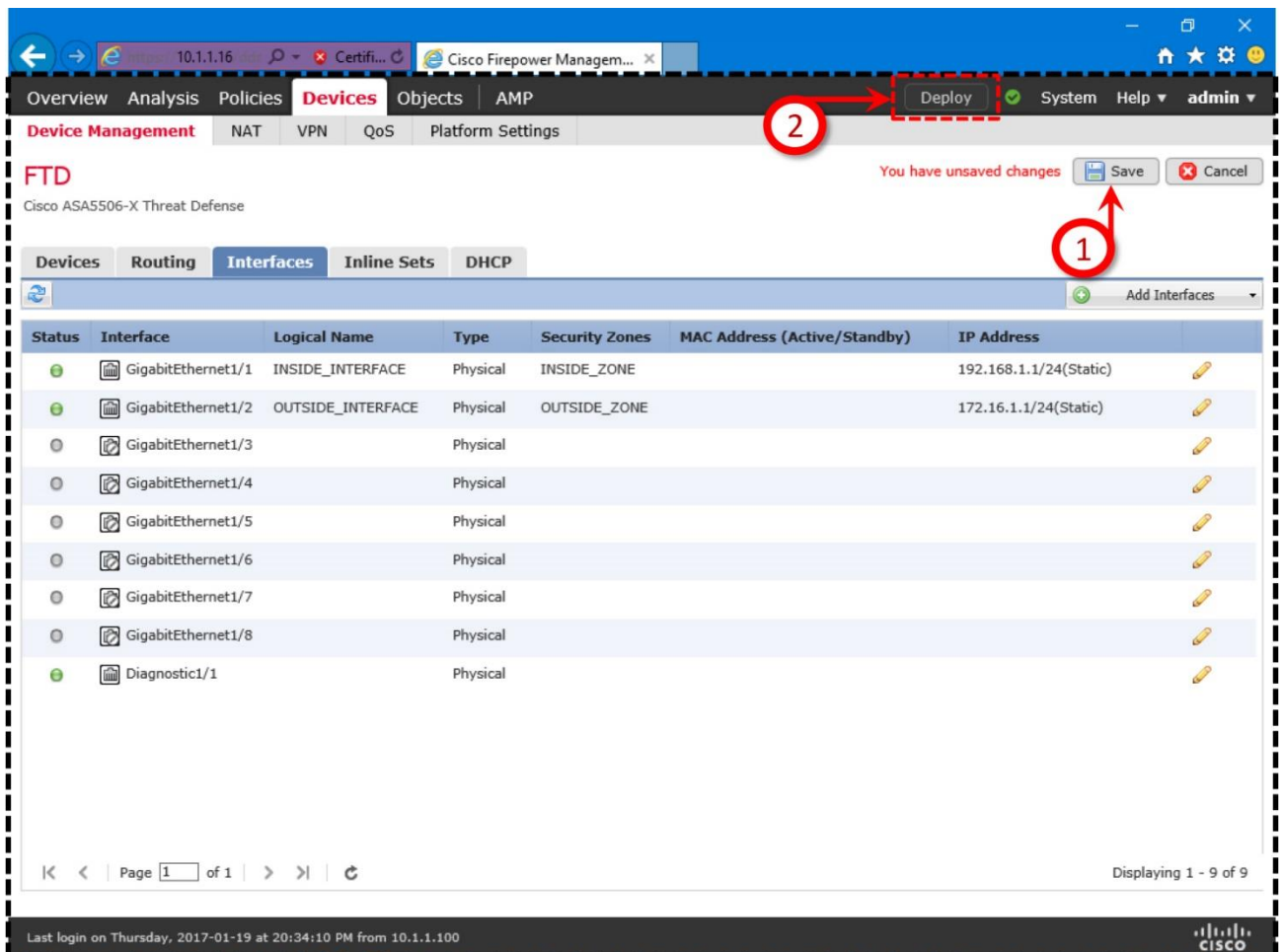


Figure 8-9. Save the Configuration First, Then Use the Deploy Button to Apply Changes

DHCP Services

FTD can function as a DHCP server as well as a DHCP client. For example, if you deploy an FTD between your inside and outside network, the FTD is able to obtain an IP address dynamically for its outside interface from an ISP router. Simultaneously, FTD can act as a DHCP server and provide IPv4 addresses dynamically to the hosts it inspects.

Note

Configuring an FTD as a DHCP server is an optional choice; it does not influence the deep packet inspection capability. The DHCP implementation on the Firepower software has its own limitation. It depends on various factors, such as, the Internet Protocol version (IPv4 vs IPv6), FTD firewall mode (routed vs transparent), and type of services (DHCP server vs DHCP relay). Read the official Cisco Firepower publications to find any version-specific limitations and enhancements.

[Figure 8-10](#) illustrates two scenarios — the inside network obtains IP address from the DHCP service running on FTD, while the outside interface of the FTD gets an IP address from a service provider.

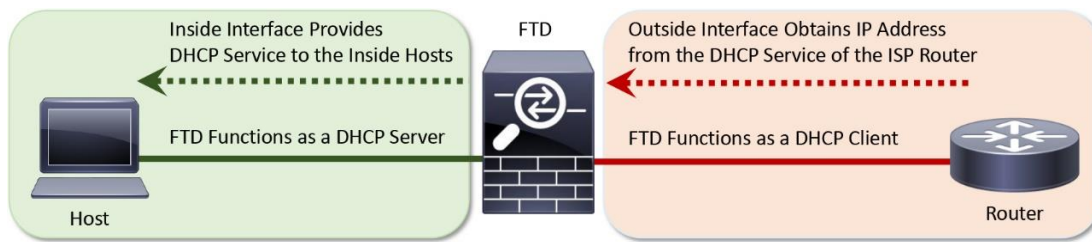


Figure 8-10. FTD can be a DHCP Server as well as a DHCP Client

FTD as a DHCP Server

The following steps describes how to enable the DHCP service on an FTD, and allow the inside interface to provide IPv4 addresses to its connected host computers:

Step 1. Go to the **Devices > Device Management** page, and click the pencil icon to edit the FTD configuration.

Step 2. Assign a Static IP address to the inside interface. Your end-users (DHCP clients) will be using this IP address as their default gateway.

[Figure 8-11](#) shows the configuration of a static IP address 192.168.1.1 on GigabitEthernet1/1 — the inside interface of FTD.

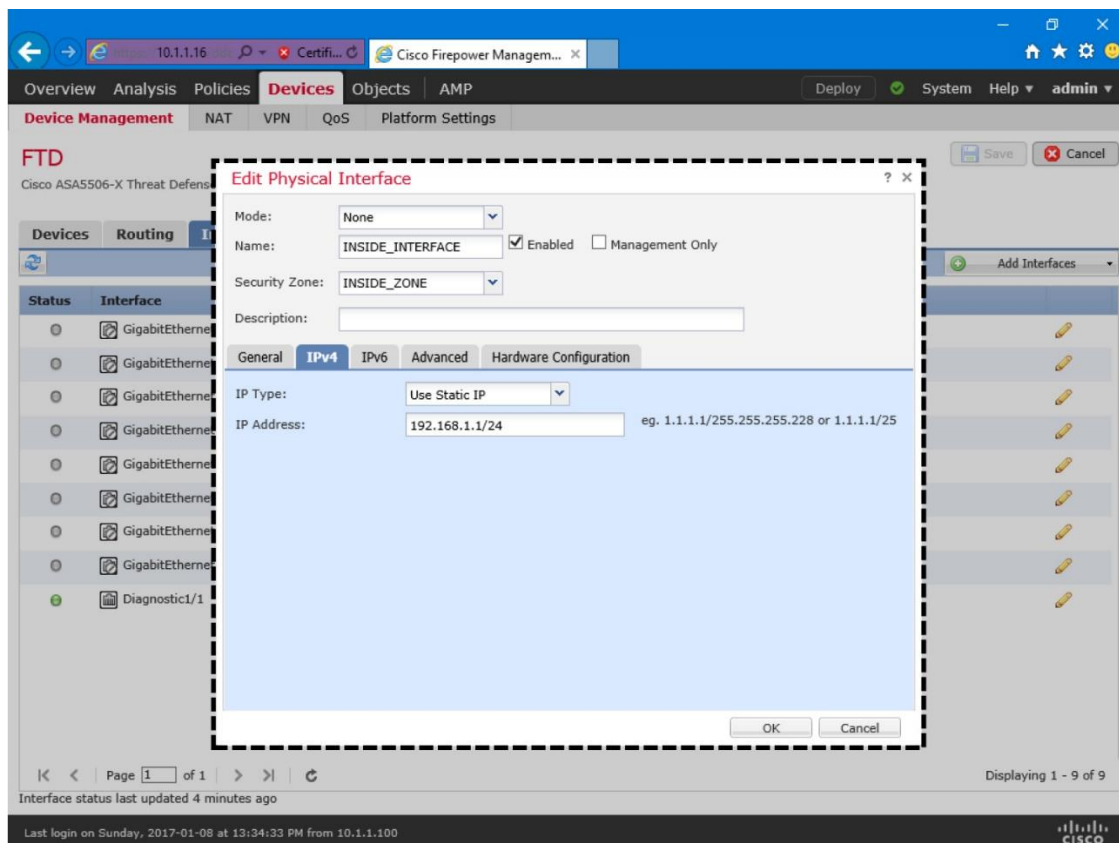


Figure 8-11. *Static IP Address Configuration on the Inside Interface*

Step 3. In the device editor, go to the **DHCP** tab. By default, the **DHCP Server** page appears.

Step 4. Click the **Add** button in the **Server** tab (located at the bottom part of the DHCP Server page). The **Add Server** window appears.

Step 5. In the **Add Server** window, select the inside interface from the drop down list as it will be offering IP addresses to the inside network.

Step 6. Create an address pool for the DHCP server. Remember, the addresses in the pool must be within the same subnet as the connected interface. For example, if you assign 192.168.1.1/24 to the inside interface, the DHCP address pool should be between 192.168.1.2 and 192.168.1.254.

[Figure 8-12](#) displays that a DHCP server is enabled on the FTD inside interface with an address pool 192.168.1.2-192.168.1.10.

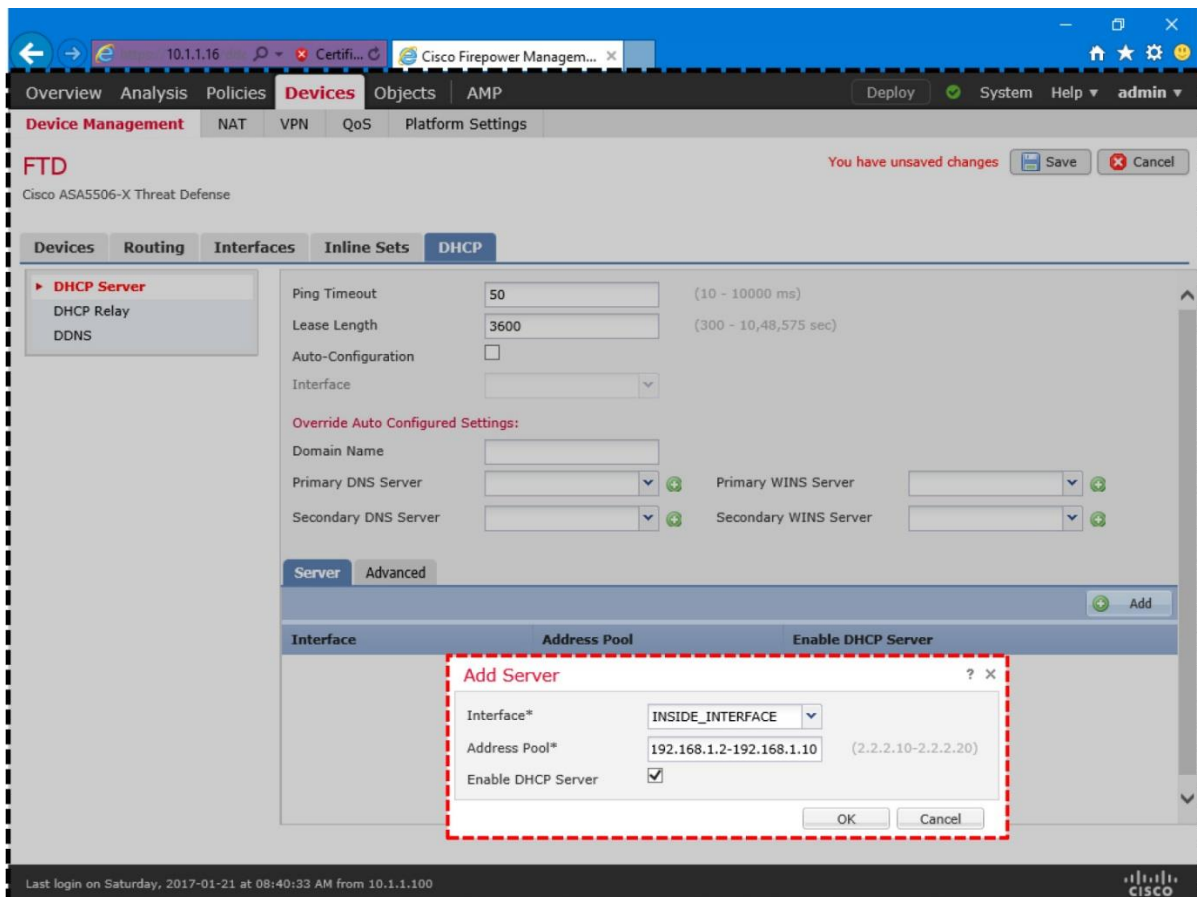


Figure 8-12. *DHCP Server Configuration on FTD*

Step 7. Select the **Enable DHCP Server** checkbox to enable the service and click **OK**. You will return to the device editor page.

Step 7. Optionally, through the DHCP service, you can transfer any DNS related information to your DHCP clients. The **DHCP Server** page allows you to enter domain name and DNS addresses manually. Alternatively, you can select the **Auto-Configuration** checkbox to let your FTD obtain any DNS information automatically from a DHCP client connected to a predefined interface.

Step 8. Finally, click the Save button to save the configuration, and apply the changes using the Deploy button.FTD as a DHCP Client

If you connect the outside interface of FTD with an Internet Service Provider (ISP), FTD is able to accept any dynamic IP address assigned by an ISP. To accept a DHCP offer from an external server, perform the following tasks on the FTD:

Step 1. Go to the **Devices > Device Management** page, and click the pencil icon to configure your desired FTD.

Step 2. Edit the interface that is connected to an external DHCP server. In this configuration example, the outside interface, GigabitEthernet1/2, is connected to a DHCP server.

Step 3. In the **Edit Physical Interface** window, select the checkbox to enable the interface. Choose a **Name** and **Security Zone** for this interface. Skip this step if you configured these items previously during the static IP address configuration.

[Figure 8-13](#) shows the configurations on the outside interface that will be able to obtain an IP address from a DHCP server.

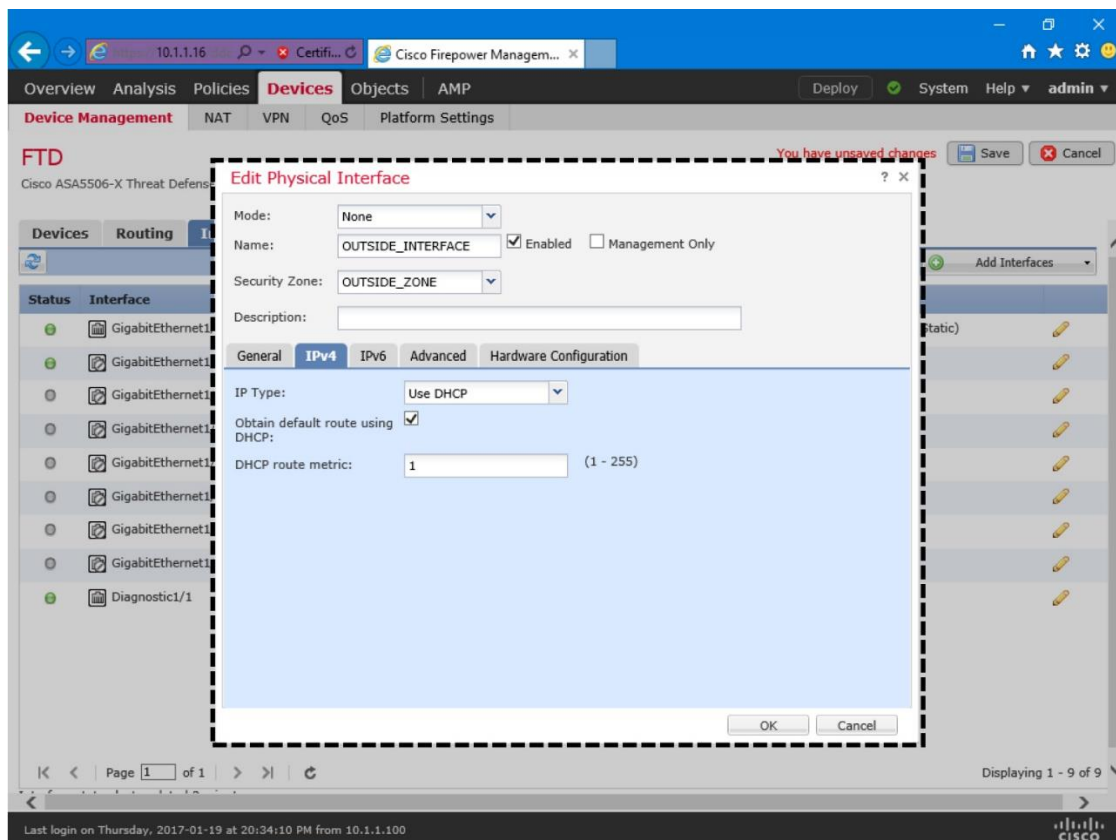


Figure 8-13. Interface Configuration to Obtain IP Address as a DHCP Client

Step 4. In the **IPv4** tab, choose **Use DHCP** from the drop down, and select the **Obtain default route using DHCP** checkbox.

Step 5. Select **OK** to exit the interface configuration window. Click the **Save** button to save the configuration, and apply the changes using the **Deploy** button.

The outside interface now should see an offer from an external DHCP server.

Verification and Troubleshooting Tools

Once the ingress and egress interfaces are successfully configured and enabled, you should be able to ping from the inside network to the outside network, or vice versa. While you run ICMP traffic, you can view the transaction of packets going through the FTD by using the **debug** command.

[Example 8-6](#) shows ICMP requests and replies exchanged between two computers located at inside and outside networks.

Example 8-6 Debug of ICMP Traffic on an FTD

```
> debug icmp trace
debug icmp trace enabled at level 1
>
ICMP echo request from INSIDE_INTERFACE:192.168.1.2 to
OUTSIDE_INTERFACE:172.16.1.100 ID=4101 seq=1 len=56
ICMP echo reply from OUTSIDE_INTERFACE:172.16.1.100 to
INSIDE_INTERFACE:192.168.1.2 ID=4101 seq=1 len=56
ICMP echo request from INSIDE_INTERFACE:192.168.1.2 to
OUTSIDE_INTERFACE:172.16.1.100 ID=4101 seq=2 len=56
ICMP echo reply from OUTSIDE_INTERFACE:172.16.1.100 to
INSIDE_INTERFACE:192.168.1.2 ID=4101 seq=2 len=56
.
.
<Output Omitted>

> undebug all
>
```

If the ping test fails, you need to determine the status of the interfaces. You can run couple of commands on the FTD to verify the configurations that you applied from the FMC to the FTD. Command outputs are slightly different — depending on the configuration method (static vs dynamic).

Verify Interface Configuration

The following commands are useful to verify the interface configuration and status. You can find some examples of their usages below.

- **show ip**
- **show interface ip brief**
- **show interface *Interface_Identifier***
- **show running-config interface**

[Example 8-7](#) shows an output of the **show ip** command. You can view the mapping between the interface, logical name and IP address from the output. You cannot, however, view the current status from the output.

Example 8-7 Output of the show ip Command

```
> show ip
System IP Addresses:
Interface          Name          IP address      Subnet mask
Method
GigabitEthernet1/1  INSIDE_INTERFACE  192.168.1.1
255.255.255.0  manual
GigabitEthernet1/2  OUTSIDE_INTERFACE  172.16.1.1
255.255.255.0  manual
Current IP Addresses:
Interface          Name          IP address      Subnet mask
Method
GigabitEthernet1/1  INSIDE_INTERFACE  192.168.1.1
255.255.255.0  manual
GigabitEthernet1/2  OUTSIDE_INTERFACE  172.16.1.1
255.255.255.0  manual
>
```

[Example 8-8](#) confirms that both GigabitEthernet1/1 and GigabitEthernet1/2 interfaces are up and configured with manual method (static IP address). The **show interface ip brief** command provides an overview, specially the current status, of all of the interfaces.

Example 8-8 Overview of the Interface Status

```
> show interface ip brief
Interface          IP-Address      OK? Method Status
Protocol
Virtual0          127.1.0.1       YES unset  up
up
GigabitEthernet1/1  192.168.1.1     YES manual up
up
GigabitEthernet1/2  172.16.1.1     YES manual up
up
GigabitEthernet1/3  unassigned      YES unset  administratively down
down
GigabitEthernet1/4  unassigned      YES unset  administratively down
down
```

```

GigabitEthernet1/5      unassigned      YES unset      administratively down
down
GigabitEthernet1/6      unassigned      YES unset      administratively down
down
GigabitEthernet1/7      unassigned      YES unset      administratively down
down
GigabitEthernet1/8      unassigned      YES unset      administratively down
down
Internal-Controll1/1    127.0.1.1      YES unset      up
up
Internal-Data1/1        unassigned      YES unset      up
up
Internal-Data1/2        unassigned      YES unset      down
down
Internal-Data1/3        unassigned      YES unset      up
up
Internal-Data1/4        169.254.1.1    YES unset      up
up
Management1/1          unassigned      YES unset      up
up
>

```

[Example 8-9](#) displays detail statistics of the GigabitEther1/1 interface. Using the **show interface interface_ID** command, you can determine any errors and drops that may occurred on an interface.

Example 8-9 *Detail Statistics of Packets in the Interface Level*

```

> show interface GigabitEthernet 1/1
Interface GigabitEthernet1/1 "INSIDE_INTERFACE", is up, line protocol is up
Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
Input flow control is unsupported, output flow control is off
MAC address a46c.2ae4.6bc0, MTU 1500
IP address 192.168.1.1, subnet mask 255.255.255.0
3541 packets input, 379530 bytes, 0 no buffer
Received 54 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
2875 packets output, 292832 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (blocks free curr/low): hardware (938/895)
output queue (blocks free curr/low): hardware (1023/1022)
Traffic Statistics for "INSIDE_INTERFACE":
3534 packets input, 315149 bytes
2875 packets output, 240884 bytes
658 packets dropped
1 minute input rate 2 pkts/sec, 168 bytes/sec
1 minute output rate 2 pkts/sec, 168 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 2 pkts/sec, 168 bytes/sec
5 minute output rate 2 pkts/sec, 168 bytes/sec
5 minute drop rate, 0 pkts/sec
>

```


[Example 8-10](#) displays the interface configurations from the CLI. You can find all of the settings you configured on the FMC, and applied to the FTD. The system, however, adds some commands automatically when you apply the final configurations.

Example 8-10 *Running Configurations of GigabitEthernet1/1 and GigabitEthernet1/2*

```
> show running-config interface
!
interface GigabitEthernet1/1
 nameif INSIDE_INTERFACE
 cts manual
 propagate sgt preserve-untag
 policy static sgt disabled trusted
 security-level 0
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet1/2
 nameif OUTSIDE_INTERFACE
 cts manual
 propagate sgt preserve-untag
 policy static sgt disabled trusted
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
.
.
<Output Omitted for Brevity>
>
```

[Verify DHCP Settings](#)

If an FTD does not offer an IP address to its DHCP clients, or if the FTD is unable to obtain an IP address from any external DHCP server, you can verify the configurations and debug any DHCP packets to and from the DHCP server. Let's take a look.

[Example 8-11](#) confirms that the GigabitEthernet1/2, connected to the outside network, is able to obtain an IP address 172.16.1.104 from a DHCP server.

Example 8-11 *Status of Outside Interface — Configured with a Dynamic IP Address*

```
> show interface ip brief
Interface                               IP-Address      OK? Method Status
Protocol
Virtual0                                127.1.0.1       YES unset  up
up
GigabitEthernet1/1                       192.168.1.1     YES manual  up
up
GigabitEthernet1/2                       172.16.1.104   YES DHCP    up
up
GigabitEthernet1/3                       unassigned      YES unset   administratively down
down
GigabitEthernet1/4                       unassigned      YES unset   administratively down
down
GigabitEthernet1/5                       unassigned      YES unset   administratively down
down
GigabitEthernet1/6                       unassigned      YES unset   administratively down
down
```

```

GigabitEthernet1/7      unassigned      YES unset      administratively down
down
GigabitEthernet1/8      unassigned      YES unset      administratively down
down
Internal-Controll1/1    127.0.1.1      YES unset      up
up
Internal-Data1/1        unassigned      YES unset      up
up
Internal-Data1/2        unassigned      YES unset      down
down
Internal-Data1/3        unassigned      YES unset      up
up
Internal-Data1/4        169.254.1.1    YES unset      up
up
Management1/1          unassigned      YES unset      up
up
>

```

[Example 8-12](#) displays the differences between the configurations of two interfaces — the inside interface GigabitEthernet1/1 is configured with a static IP address 192.168.1.1/24, whereas the outside interface GigabitEthernet1/2 is configured to obtain an address from a DHCP server.

Example 8-12 *Difference between a Static and DHCP Configuration on the CLI*

```

> show running-config interface
!
interface GigabitEthernet1/1
 nameif INSIDE_INTERFACE
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet1/2
 nameif OUTSIDE_INTERFACE
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address dhcp setroute
!
.
.
<Output Omitted for Brevity>
>

```

[Example 8-13](#) proves that FTD has dynamically assigned an IP address 192.168.1.2 to a host with MAC address C4:2C:03:3C:98:A8. This IP address is the first address from the DHCP address pool 192.168.1.2-192.168.1.10.

Example 8-13 *Verification of the IP Address Assignment from a DHCP Address Pool*

```
> show dhcpd binding
```

IP address	Client Identifier	Lease expiration	Type
192.168.1.2	c42c.033c.98a8	3580 seconds	Automatic

```
>
```

If you do not see any DHCP binding, you can debug the DHCP packets on the FTD.

[Example 8-14](#) demonstrates the process of assigning IP address by a DHCP server. In the debug output, you can analyze the four major stages of the DHCP protocol — Discovery, Offer, Request, and Acknowledgement (DORA).

Example 8-14 *Exchange of DHCP Packets between an FTD and DHCP Server*

```
> debug dhcpd packet
```

```
debug dhcpd packet enabled at level 1
```

```
>
```

```
DHCPD/RA: Server msg received, fip=ANY, fport=0 on INSIDE_INTERFACE interface
```

```
DHCPD: DHCPDISCOVER received from client c42c.033c.98a8 on interface INSIDE_INTERFACE.
```

```
DHCPD: send ping pkt to 192.168.1.2
```

```
DHCPD: ping got no response for ip: 192.168.1.2
```

```
DHCPD: Add binding 192.168.1.2 to radix tree
```

```
DHCPD/RA: Binding successfully added to hash table
```

```
DHCPD: Sending DHCPPOFFER to client c42c.033c.98a8 (192.168.1.2).
```

```
DHCPD: Total # of raw options copied to outgoing DHCP message is 0.
```

```
DHCPD/RA: creating ARP entry (192.168.1.2, c42c.033c.98a8).
```

```
DHCPD: unicasting BOOTREPLY to client c42c.033c.98a8(192.168.1.2).
```

```
DHCPD/RA: Server msg received, fip=ANY, fport=0 on INSIDE_INTERFACE interface
```

```
DHCPD: DHCPREQUEST received from client c42c.033c.98a8.
```

```
DHCPD: Extracting client address from the message
```

```
DHCPD: State = DHCP_REBOOTING
```

```
DHCPD: State = DHCP_REQUESTING
```

```
DHCPD: Client c42c.033c.98a8 specified it's address 192.168.1.2
```

```
DHCPD: Client is on the correct network
```

```
DHCPD: Client accepted our offer
```

```
DHCPD: Client and server agree on address 192.168.1.2
```

```
DHCPD: Renewing client c42c.033c.98a8 lease
```

```
DHCPD: Client lease can be renewed
```

```
DHCPD: Sending DHCPACK to client c42c.033c.98a8 (192.168.1.2).
```

```
DHCPD: Total # of raw options copied to outgoing DHCP message is 0.
```

```
DHCPD/RA: creating ARP entry (192.168.1.2, c42c.033c.98a8).
```

```
DHCPD: unicasting BOOTREPLY to client c42c.033c.98a8(192.168.1.2).
```

```
>
```

Summary

In this chapter, you have learned about the widely deployed firewall mode — the routed mode. This chapter describes the steps to configure the routed interfaces with static IP address as well as dynamic IP address. In addition, this chapter discusses various command line tools that you can use to determine any potential interface related issues.

Quiz

- 1.** Which of the following commands is used to debug and analyze ping requests?
 - a.** > `debug icmp`
 - b.** > `debug ip icmp`
 - c.** > `debug icmp trace`
 - d.** > `debug icmp reply`

- 2.** Which of the following commands is used to configure an FTD from transparent mode to the routed mode?
 - a.** `configure routed`
 - b.** `configure firewall routed`
 - c.** `configure firepower routed`
 - d.** `configure transparent disable`

- 3.** Which of the following statements is true?
 - a.** FTD in transparent mode cannot be configured by an FMC
 - b.** You can change the firewall deployment mode using an FMC.
 - c.** You cannot change the firewall mode until you unregister an FTD from an FMC.
 - d.** When you change the firewall mode, FTD saves the running configurations.

- 4.** Which of the following commands allows you to determine any interface related issues?
 - a.** `show interface ip brief`
 - b.** `show interface Interface_Identifier`
 - c.** `show running-config interface`
 - d.** All of the above

Chapter 9. Firepower Deployment in Transparent Mode

An FTD with transparent mode allows you to control your network traffic like a firewall, while the FTD stays invisible to the hosts in your network. This chapter discusses the configuration of FTD in transparent mode.

Essential Knowledge

In transparent mode, FTD bridges the inside and outside interfaces into a single layer 2 network, and remains transparent to the hosts. When an FTD is in transparent mode, an FMC does not allow you to assign an IPv4 address to a directly connected interface. As a result, the hosts are unable to communicate with any connected interfaces. Unlike routed mode, you cannot configure the connected interfaces as the default gateway for the hosts.

You can, however, assign an IP address to the Bridge Virtual Interface (BVI) that comes with each bridge group. A bridge group represents a unique layer 2 network. You can create multiple bridge groups on a single FTD, but the hosts within different bridge groups cannot communicate each other without a router. Within a bridge group, both the BVI and the hosts must have IP addresses from the same subnet. FTD uses the IP address of BVI when it communicates with its hosts.

[Figure 9-1](#) shows how a host finds a router, not an FTD, as its next hop when you configure an FTD in transparent mode.

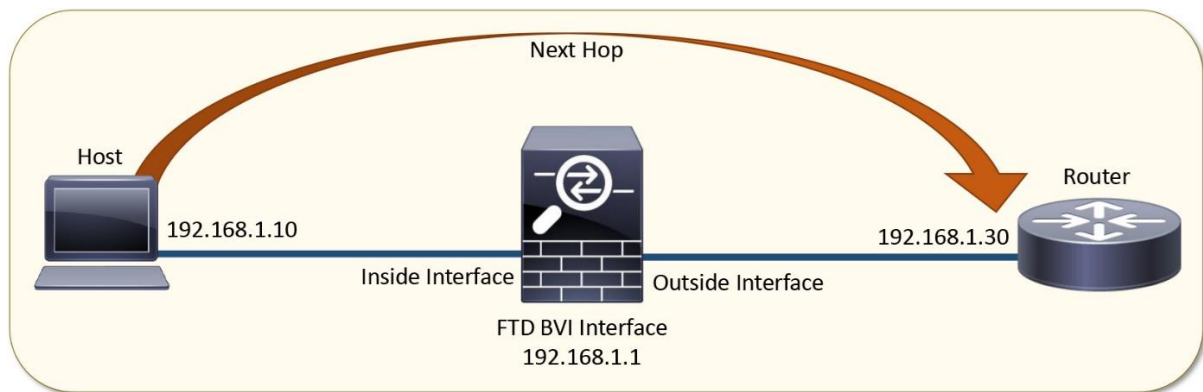


Figure 9-1. *Communication of a Host with Its Next Hop When the FTD is Transparent*

[Figure 9-2](#) shows an example of real world deployment of an FTD in transparent mode. The management interfaces of FMC and FTD are connected to the end users through 192.168.1.0/24 subnet. The default gateway for the 192.168.1.0/24 subnet is the gateway router IP address 192.168.1.30/24.

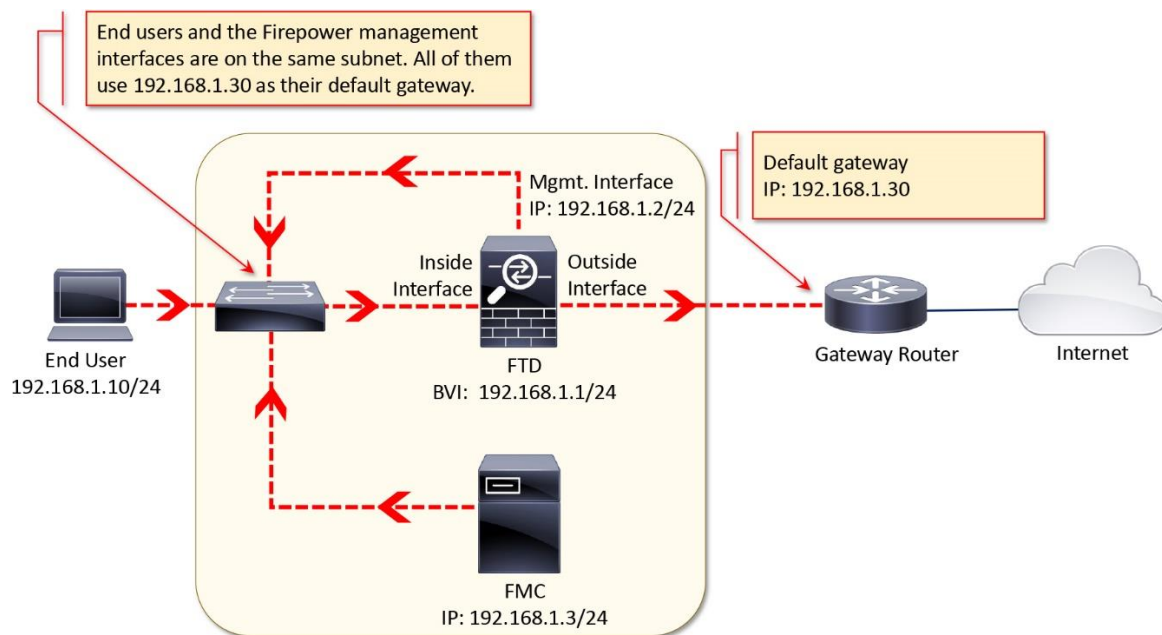


Figure 9-2. Real World Deployment Example of an FTD in Transparent Mode

Best Practices

Consider the following items when you plan to deploy an FTD in transparent mode:

- Changing of firewall mode wipes out any existing configurations on an FTD. Therefore, before you change the firewall mode from routed to transparent, or vice versa, take a note of your FTD configuration settings for future reference, in case you want to revert the FTD to the initial state. To view the current FTD configuration, run the **show running-config** on the CLI.

If you just want to change the firewall mode on your FTD, performing a backup of your security policy configuration is not necessary, because the Next-Generation security policies are defined and stored on the FMC. Once configured, FMC can deploy the same policies to one or more FTDs.

- Do not use the IP address of BVI as the default gateway for the connected hosts. Instead, use any connected router as the default gateway for the hosts in the bridged network.

- If your ultimate goal is to perform transparent inspection, you could choose inline IPS mode over the transparent firewall mode. While both modes allows you to deploy an FTD as a bump in the wire, the inline mode has less configuration overhead than the transparent mode. In addition, a dedicated IP address for each BVI is not necessary. To learn more, read the chapter *Blocking of Traffic Using Inline Interface Mode*.

- Do not forget to add access rules to allow any necessary network management traffic. By default, an FTD in Transparent firewall mode blocks the DHCP traffic, multicast traffic, dynamic routing protocol traffic, such as, RIP, OSPF, EIGRP, BGP, etc. If you select the **Access Control: Block All Traffic** as the default action, make sure you have added access rules explicitly to allow any essential traffic. If you are not sure, you can use the **Intrusion**

Prevention: Balanced Security and Connectivity as the default action. It allows any unmatched traffic as long as there is no malicious activities found.

Configuration

During the system initialization, FTD provides you an option to choose between the routed and transparent modes. To setup an FTD with the transparent firewall mode, just type **transparent** when the system prompts, and press enter.

[Example 9-1](#) shows the last part of the initialization process of an FTD where you can setup your FTD as routed or transparent mode.

Example 9-1 *Configuration of the Transparent Firewall Mode during the Initialization*

```
<Output Omitted>
.
.
Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]: transparent
Configuring firewall mode ...
.
.
<Output Omitted>
```

If you configured transparent mode during the system initialization, you can skip the following sections *Prerequisites* and *Change the Firewall Mode*.

Prerequisites

You cannot change the firewall mode if an FTD is currently registered with an FMC. If you initially configured your FTD to routed mode, and now you want to reconfigure it to the transparent mode, you must unregister the FTD from the FMC. To verify the registration status, run the **show managers** command on the FTD.

[Example 9-2](#) shows that the FTD is currently registered with an FMC with IP address 10.1.1.16.

Example 9-2 *Verification of the Registration Status — FTD is Currently Registered*

```
> show managers
Type           : Manager
Host           : 10.1.1.16
Registration   : Completed
>
```

If you find the FTD is currently registered with an FMC, unregister it using the FMC web interface. To delete registration, go to the **Devices > Device Management** page, and click the trashcan icon next to your desired FTD.

[Figure 9-3](#) shows a trashcan icon that you select to delete the registration of an FTD from an FMC.

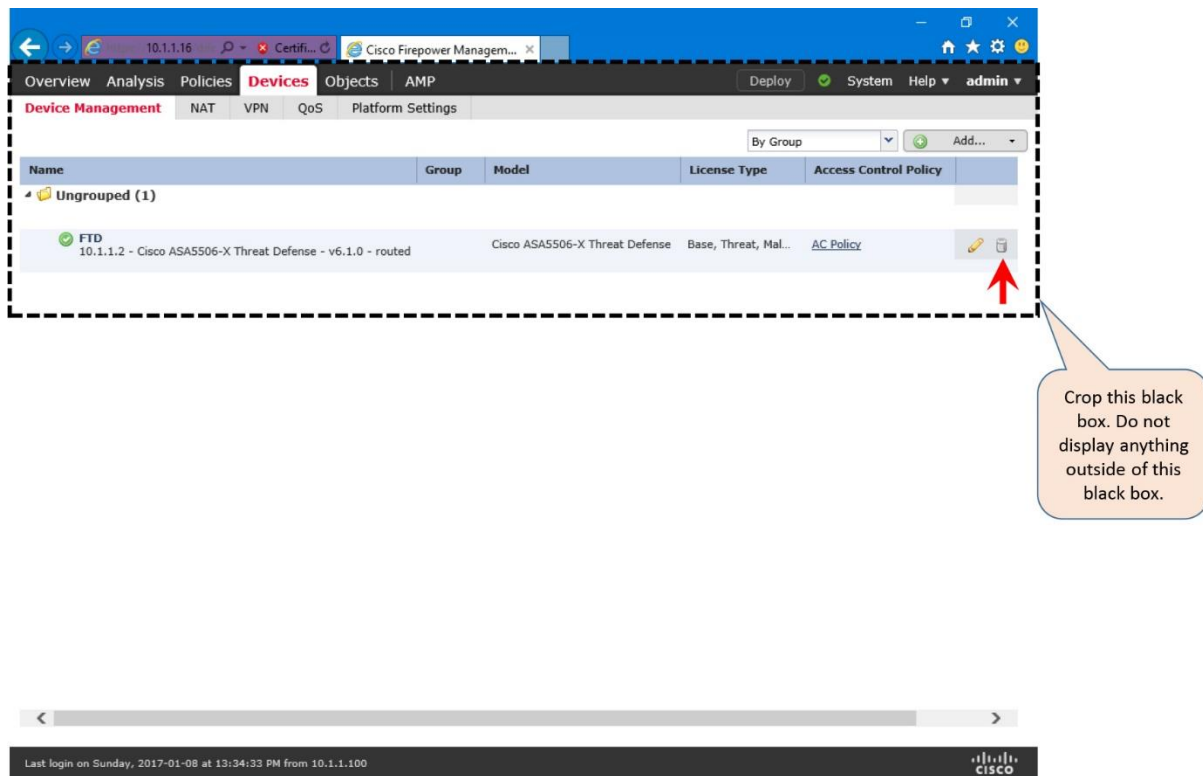


Figure 9-3. Option to Delete Firepower Registration

[Example 9-3](#) confirms that the FTD is currently not registered with any FMC.

Example 9-3 Verification of the Registration Status — FTD is not Registered

```
> show managers
No managers configured.
>
```

Change of Firewall Mode

If your FTD is currently not associated with a manager, you can change the firewall deployment mode. To configure an FTD with the transparent mode, login to the CLI of the FTD, and run the **configure firewall transparent** command.

[Example 9-4](#) illustrates the command to configure an FTD to the transparent firewall mode.

Example 9-4 Configuration of the Transparent Mode

```
> configure firewall transparent
```

```
This will destroy the current interface configurations, are you sure that
you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

After configuring an FTD with a desired mode, you can determine the status from the CLI.

[Example 9-5](#) confirms that the FTD is configured to the transparent mode.

Example 9-5 Verification of the Firewall Deployment Mode

```
> show firewall
Firewall mode: Transparent
>
```

Alternatively, upon a successful registration, the web interface of an FMC also displays the current firewall deployment mode. You can view it from the **Devices > Device management** page.

[Figure 9-4](#) shows that the FTD is configured in transparent mode.

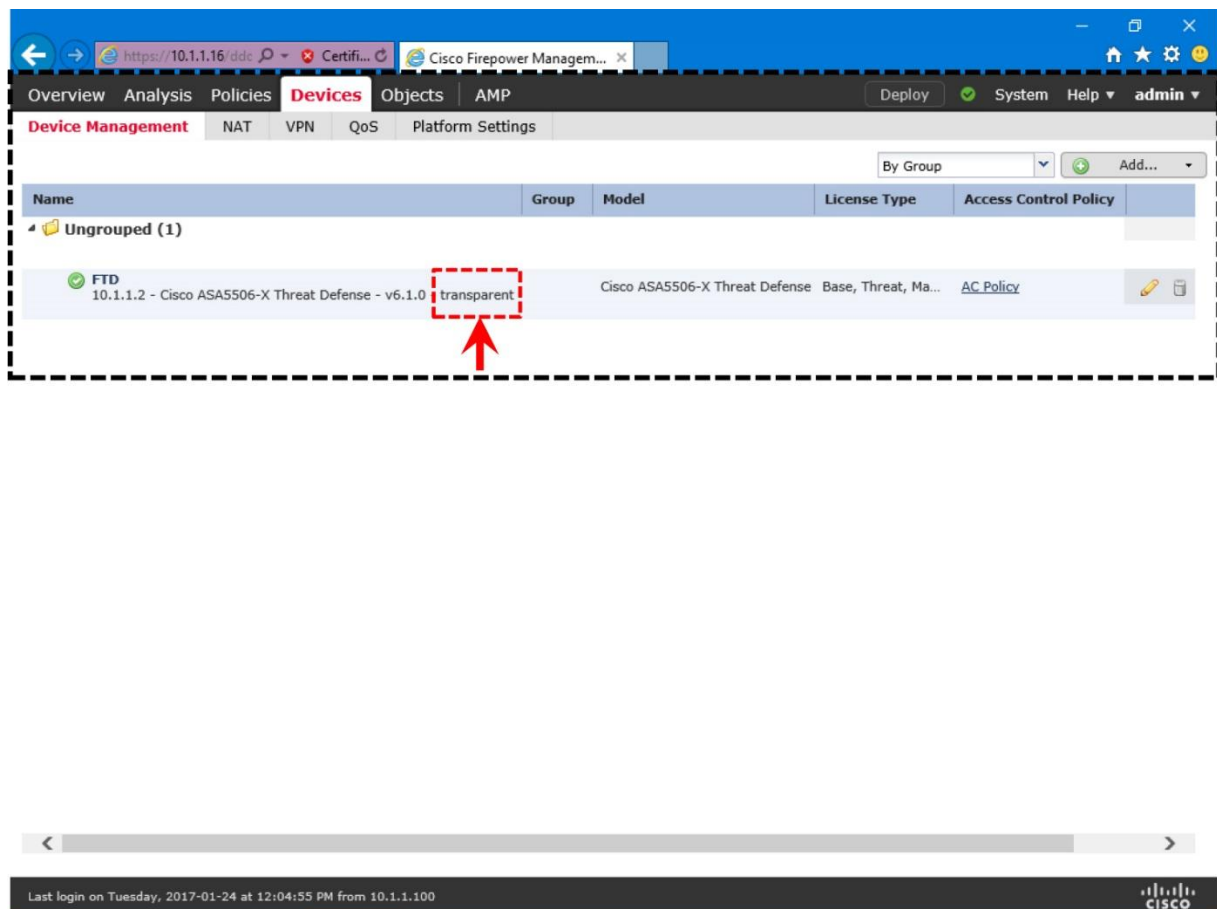


Figure 9-4. Current Deployment Mode of an FTD

Deployment in a Layer 2 Network

An FTD, in transparent mode, is able to control traffic as a firewall and inspect traffic as an intrusion prevention system while it stays transparent in the network, like a layer 2 switch. A transparent FTD supports the following deployment scenarios:

- You can deploy it in a single layer 2 network where all of the hosts reside in the same subnet, and able to communicate without a dynamic routing protocol. This type of

deployment works as soon as you configure the physical and virtual interfaces in a bridge group.

- You can also deploy an FTD between the layer 3 networks where hosts from different subnets communicate using a routing protocol. By default, when you configure an FTD in transparent mode, it blocks any underlying dynamic routing protocol traffic. Therefore, to allow them, you need to add access rules explicitly.

Physical and Virtual Interfaces Configuration

To configure the interfaces when an FTD is in transparent mode, follow the steps below:

Step 1. Navigate to the **Devices > Device Management** page. A list of the managed devices appear.

Step 2. Click the pencil icon that is next to your desired FTD device. The device editor page appears.

[Figure 9-5](#) shows all of the physical interfaces of an FTD device in the device editor page. To edit an interface, select the pencil icon next to the interface.

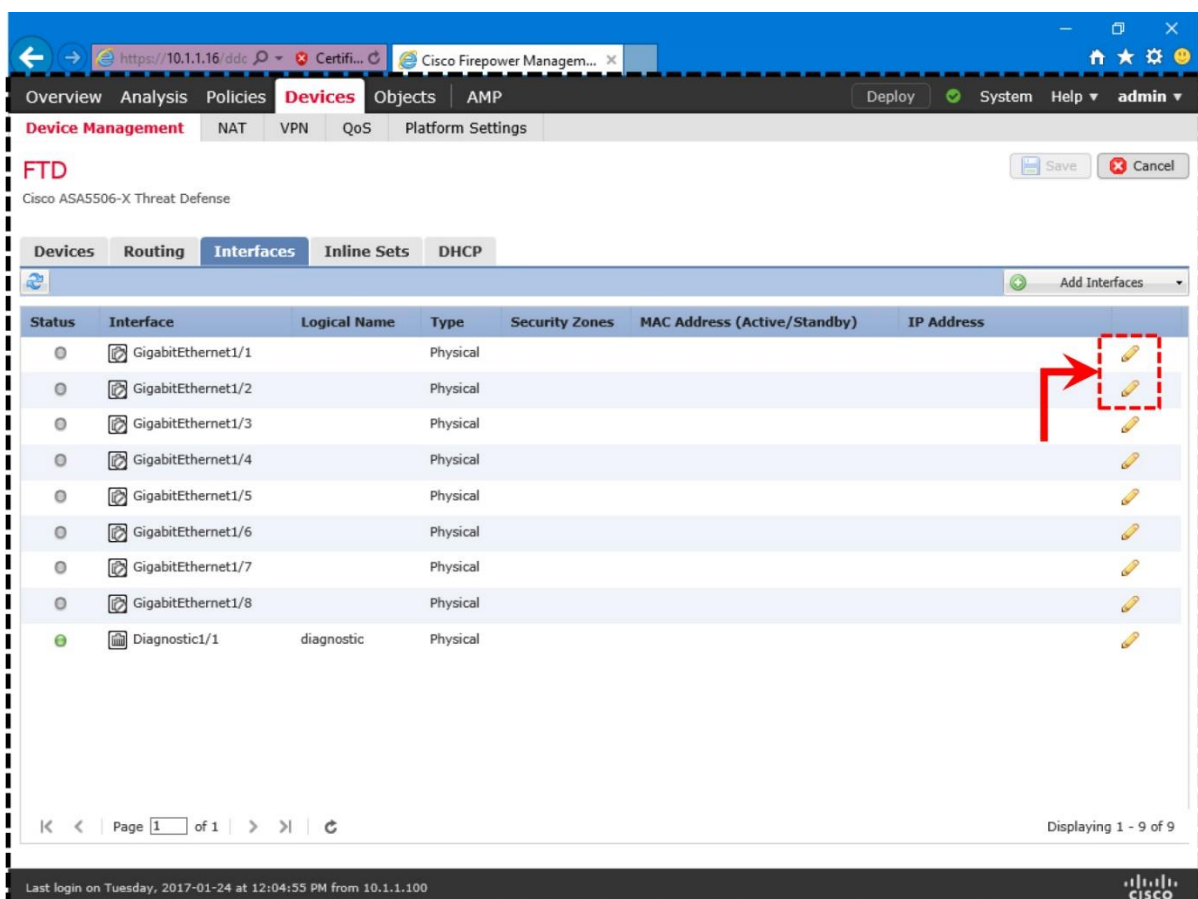


Figure 9-5. *The Device Editor Page*

Step 3. In the **Interfaces** tab, configure the **GigabitEthernet1/1** and **GigabitEthernet1/2** interfaces for the inside and outside networks, respectively, per the following settings.

[Table 9-1](#) summarizes the configuration settings for the **GigabitEthernet1/1** and **GigabitEthernet1/2** interfaces. Note that, associating a security zone to an interface is an optional configuration step in this lab.

	GigabitEthernet1/1	GigabitEthernet1/2
Interface Name	INSIDE_INTERFACE	OUTSIDE_INTERFACE
Security Zone (Optional)	INSIDE_ZONE	OUTSIDE_ZONE
IP Address	In transparent mode, IP address is not required on a data interface. Instead, assign an address to the Bridge Virtual Interface (BVI) interface.	

Table 9-1. Configuration Settings for GigabitEthernet1/1 and GigabitEthernet1/2

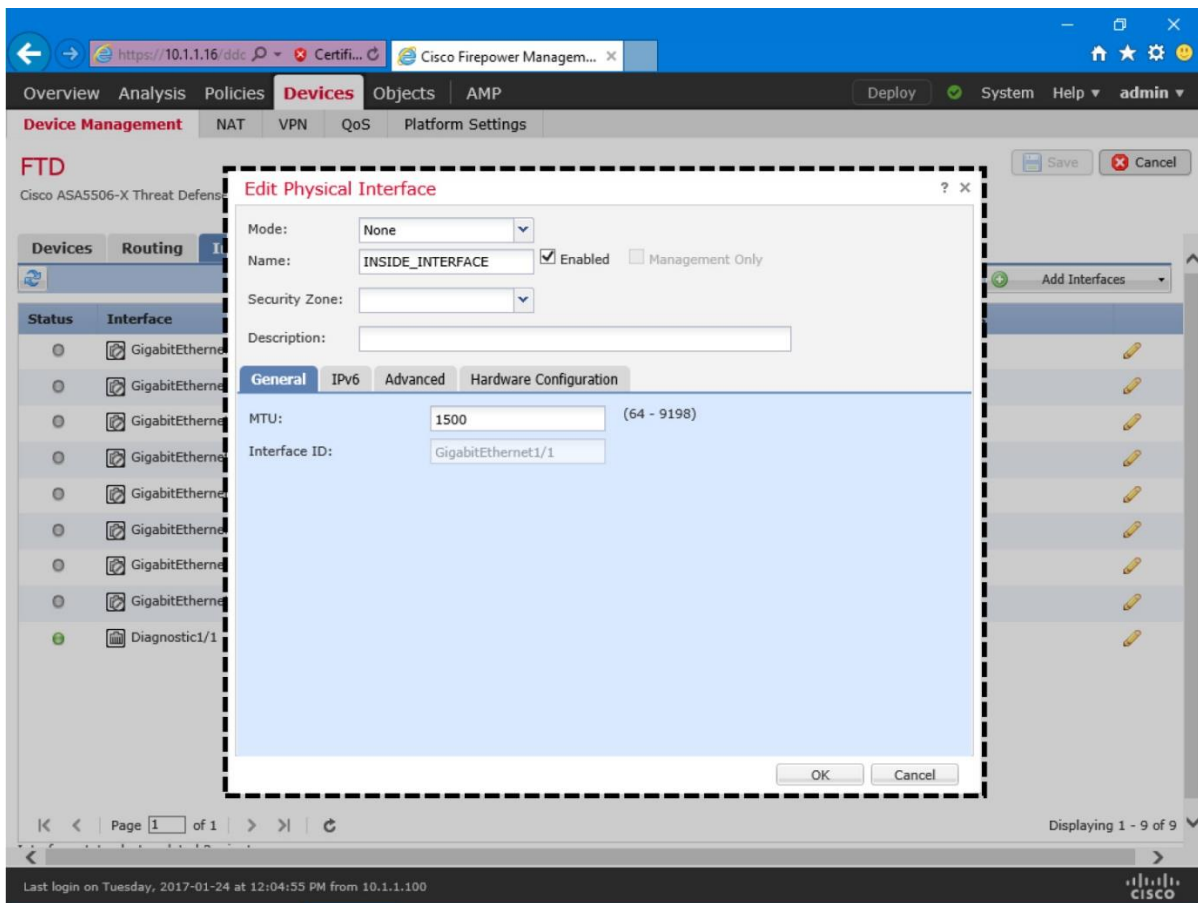


Figure 9-6. Configurations of the Inside Interface — GigabitEthernet1/1

Figure 9-7 displays the configurations on the GigabitEthernet1/2 interface that is connected to the outside network.

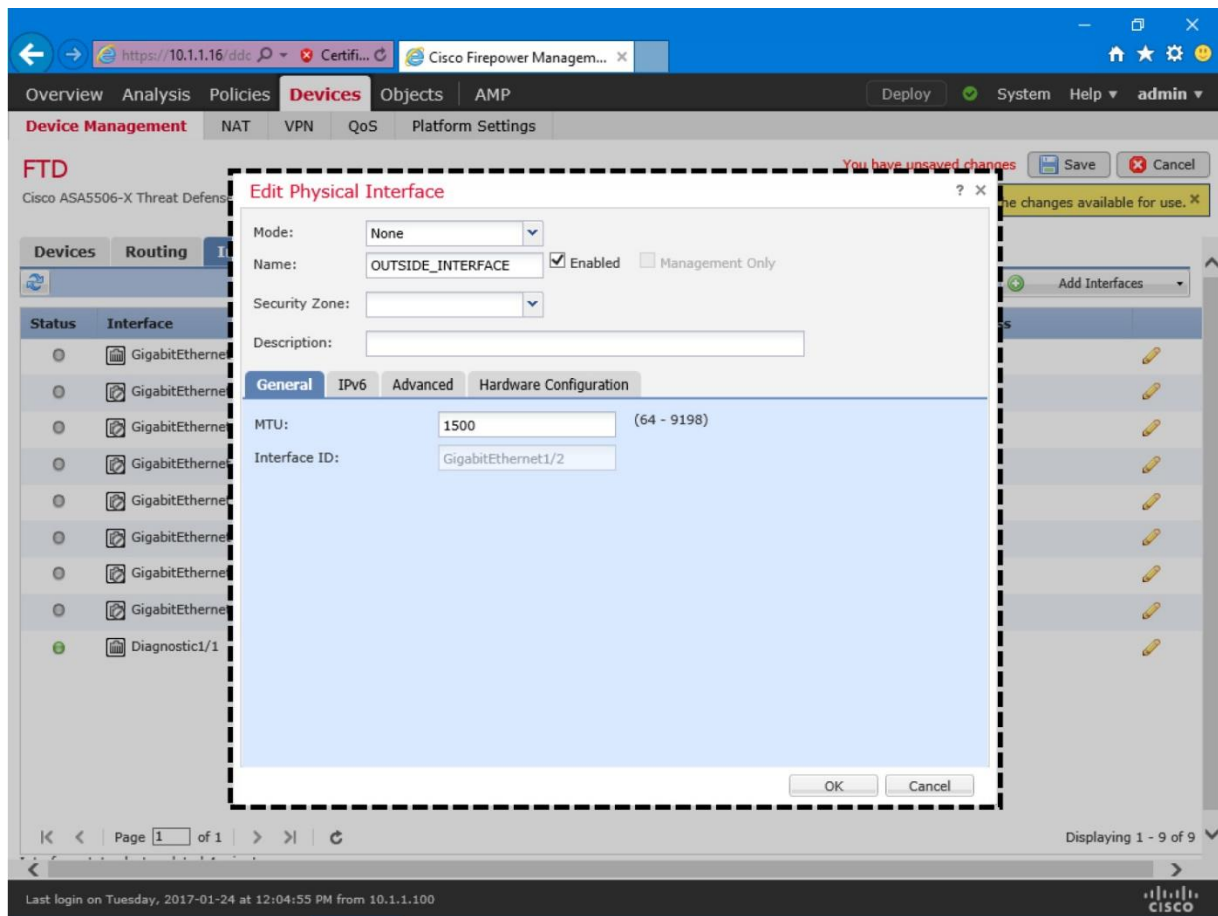


Figure 9-7. Configurations of the Outside Interface — GigabitEthernet1/2

Step 4. After you configure both interfaces, click the **Save** button to save the changes you have made so far.

Figure 9-8 shows the **Save** button and a notification for saving the configurations. When you save, it stores the configuration on the FMC for future use. FMC applies the configuration to an FTD only when you use the **Deploy** button. You will do it soon.

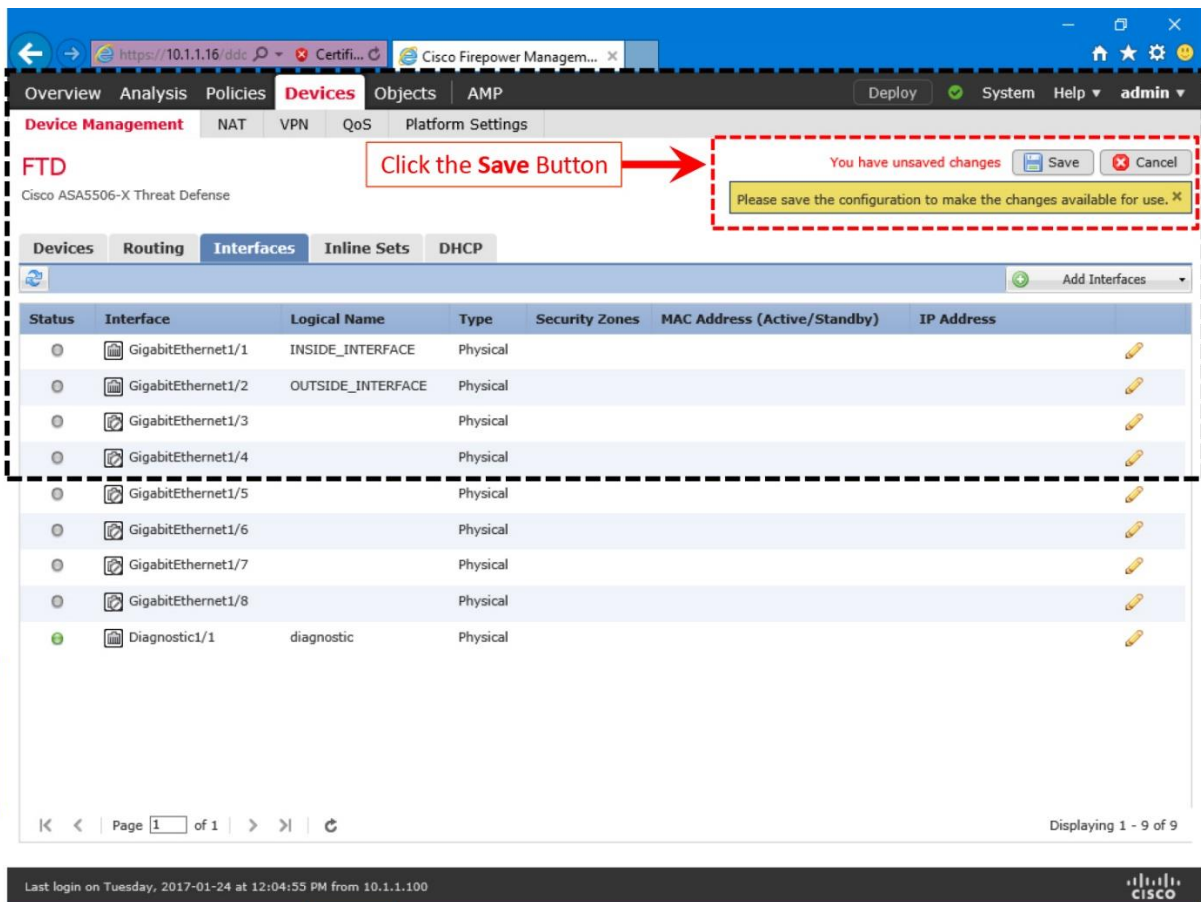


Figure 9-8. Option to Save a Configuration

Step 5. Now, let's configure a Bridge Virtual Interface (BVI) interface. On the right hand side of the **Interfaces** page, click the **Add Interfaces** button. A list of different types of interfaces appears.

Figure 9-9 shows the **Bridge Group Interface** option that you need to select to configure a BVI. It also shows where you would notice a BVI after it is configured.

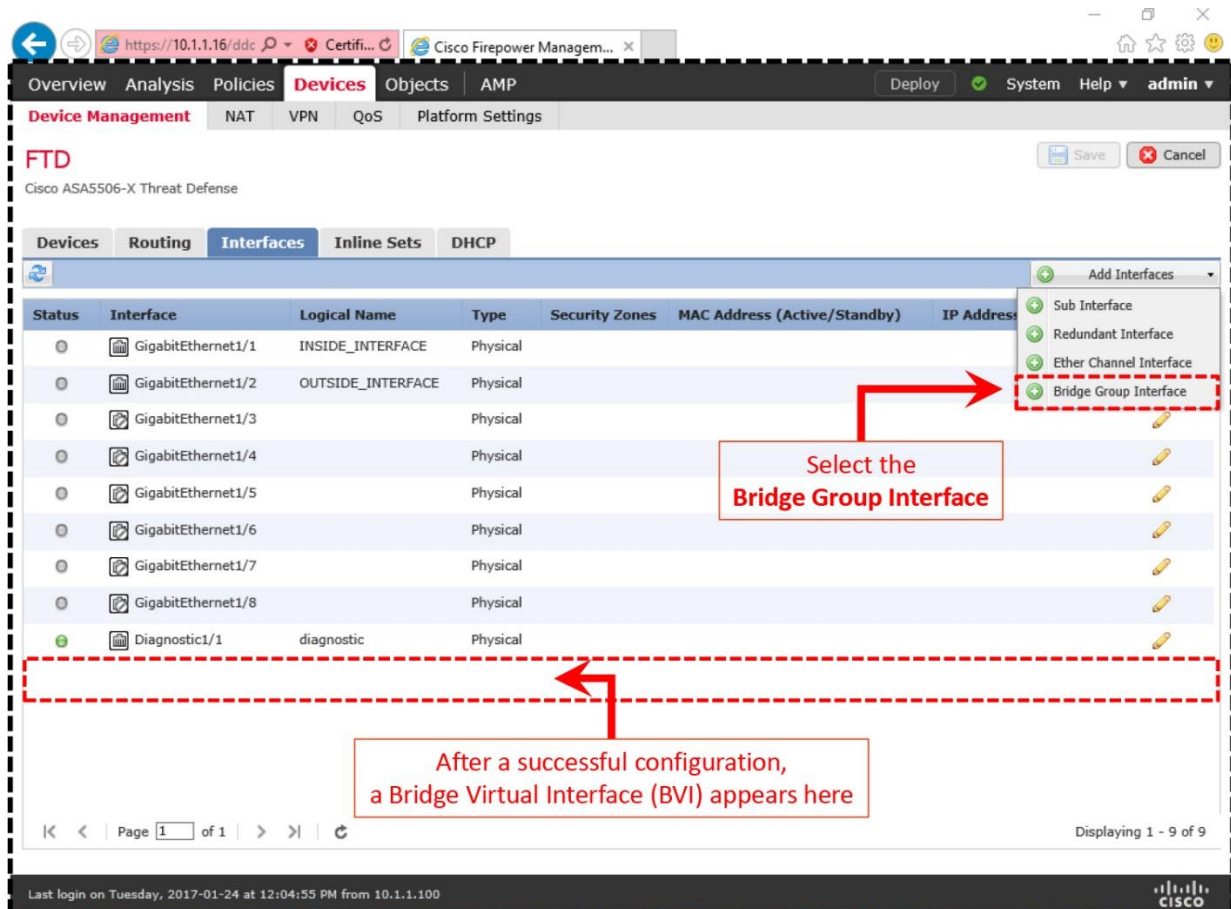


Figure 9-9. Navigation to the Bridge Group Interface Configuration

Step 6. Select the Bridge Group Interface from the list. The Add Bridge Group Interface window appears.

Step 7. In the **Interfaces** subtab, provide a **Bridge Group ID** between 1 and 250, and select the interfaces that are part of the bridged network.

Figure 9-10 shows that two interfaces GigabitEthernet1/1 and GigabitEthernet1/2 are selected for the bridge group 1 that connect the inside and outside networks, respectively,

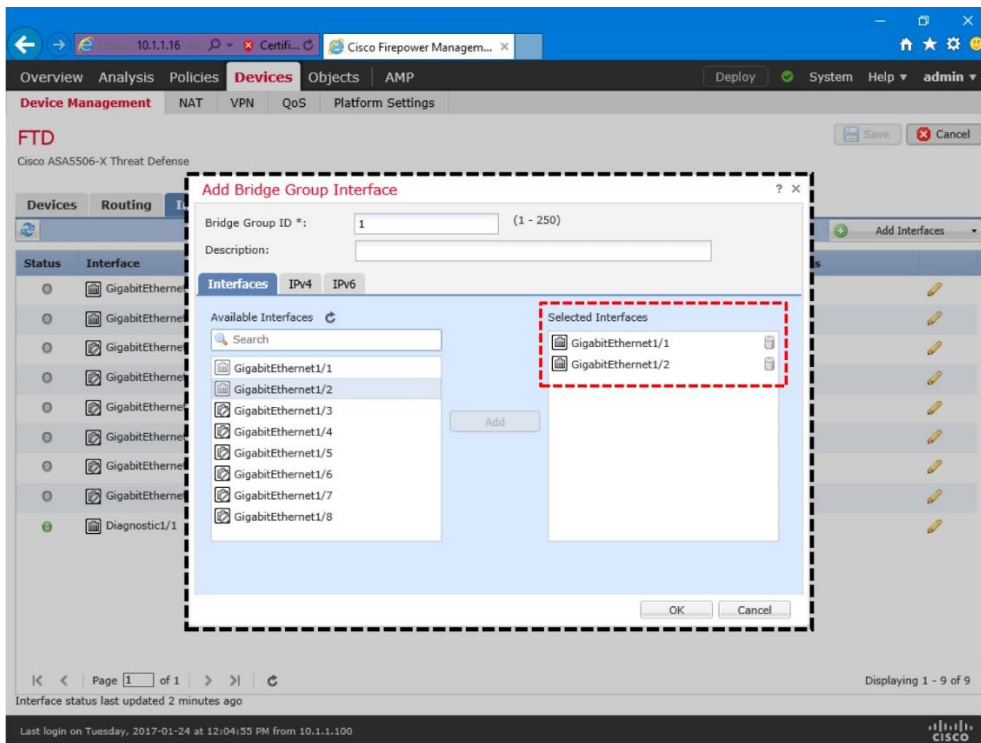


Figure 9-10. Selection of Interfaces for a Bridge group

Step 8. In the **IPv4** subtab, configure an address for the BVI. The IP address has to be on the same subnet as the hosts and default gateway router.

[Figure 9-11](#) displays where to configure an IP address for a BVI. The example uses 192.168.1.1 which is within the same /24 subnet as its hosts.

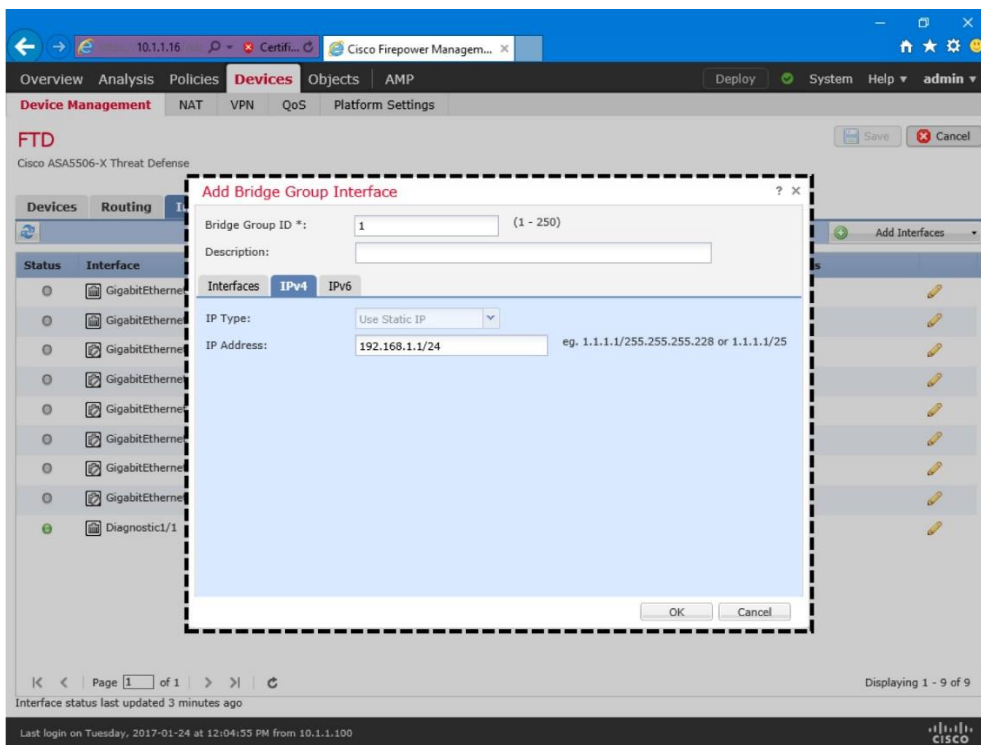


Figure 9-11. Configuration of IP Address for BVI

Step 9. Select **OK** to exit from the window. Use the **Save** button to save the changes. Finally, click the **Deploy** button to apply the configurations to your FTD.

[Figure 9-12](#) confirms the setup of a bridge group BVI1. Before you deploy the new configurations to an FTD, save the changes.

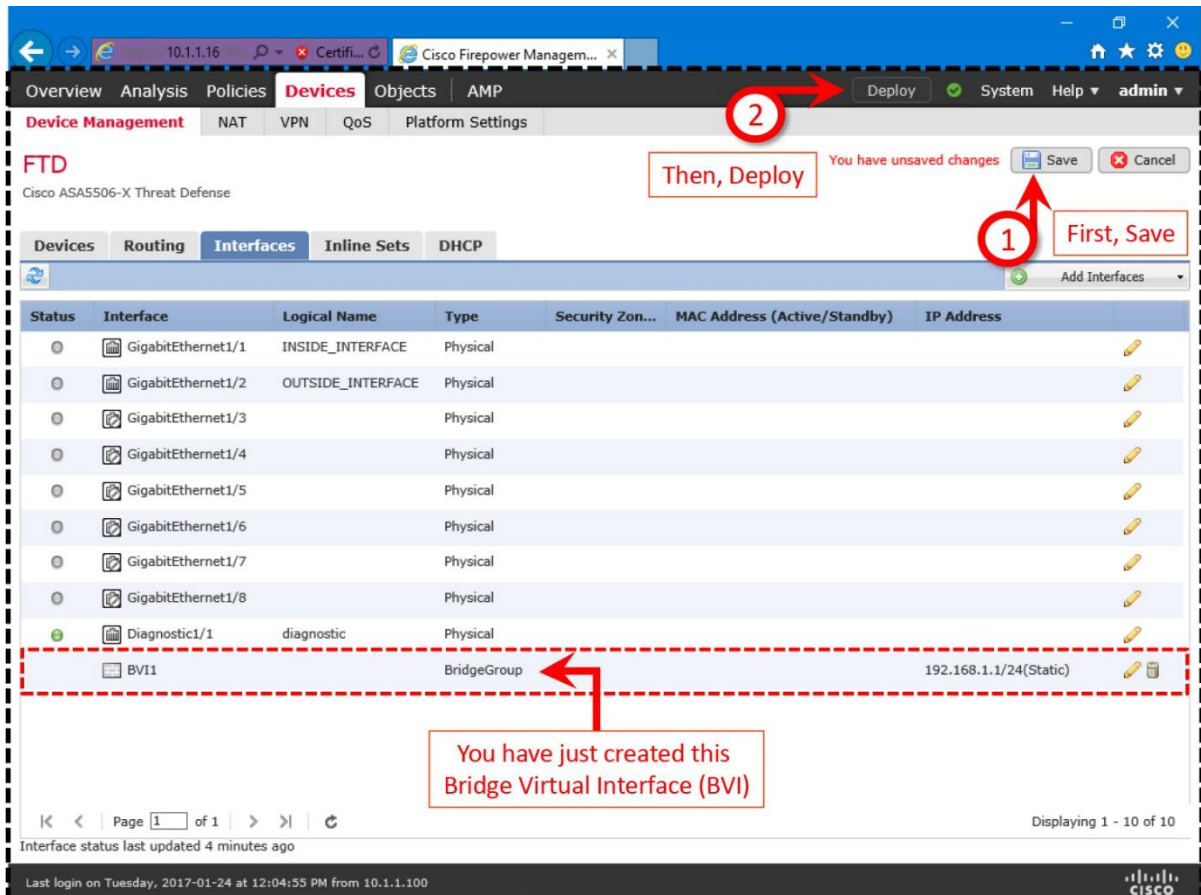


Figure 9-12. Steps to Apply Configurations to an FTD

Verification of Interface Status

After deploying an FTD using the web interface of an FMC, you can verify any configurations settings from the CLI of an FTD.

[Example 9-6](#) shows the interface configuration of an FTD in transparent mode. Both of the member interfaces are in bridge group 1, and have no IP addresses. Only the bridge Virtual Interface (BVI) 1 has an IP address 192.168.1.1/24.

Example 9-6 Interface Configurations on an FTD in Transparent Mode

```
> show running-config interface
!
interface GigabitEthernet1/1
 nameif INSIDE_INTERFACE
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 bridge-group 1
 security-level 0
!
interface GigabitEthernet1/2
 nameif OUTSIDE_INTERFACE
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 bridge-group 1
 security-level 0
.
.
<Output Omitted for Brevity>
.
.
interface Management1/1
 management-only
 nameif diagnostic
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
!
interface BVI1
 ip address 192.168.1.1 255.255.255.0
>
```

[Example 9-7](#) highlights the status of the interfaces on a transparent FTD. Although you do not configure IP addresses for the member interfaces of a bridge group, they use the same IP address as the BVI when you communicate with any connected hosts.

Example 9-7 Interface Status of an FTD in Transparent Mode

```
> show interface ip brief
Interface          IP-Address      OK? Method Status
Protocol
Virtual0           127.1.0.1       YES unset  up
up
GigabitEthernet1/1 192.168.1.1     YES unset  up
up
GigabitEthernet1/2 192.168.1.1     YES unset  up
up
GigabitEthernet1/3 unassigned      YES unset  administratively down
down
GigabitEthernet1/4 unassigned      YES unset  administratively down
down
GigabitEthernet1/5 unassigned      YES unset  administratively down
down
GigabitEthernet1/6 unassigned      YES unset  administratively down
down
```

```

GigabitEthernet1/7      unassigned      YES unset      administratively down
down
GigabitEthernet1/8      unassigned      YES unset      administratively down
down
Internal-Controll1/1    127.0.1.1      YES unset      up
up
Internal-Data1/1        unassigned      YES unset      up
up
Internal-Data1/2        unassigned      YES unset      down
down
Internal-Data1/3        unassigned      YES unset      up
up
Internal-Data1/4        169.254.1.1    YES unset      up
up
Management1/1          unassigned      YES unset      up
up
BVI1                    192.168.1.1    YES manual     up
up
>

```

[Example 9-8](#) shows the status of the logical management interface br1 which is not displayed in the previous example. FTD uses the IP address of br1 to communicate with an FMC.

Example 9-8 *Status of the Logical Management Interface, br1*

```

> show network
===== [ System Information ] =====
Hostname           : firepower
Management port    : 8305
IPv4 Default route
  Gateway          : 10.1.1.1

===== [ br1 ] =====
State              : Enabled
Channels           : Management & Events
Mode               : Non-Autonegotiation
MDI/MDIX           : Auto/MDIX
MTU                : 1500
MAC Address        : A4:6C:2A:E4:6B:BE
----- [ IPv4 ] -----
Configuration      : Manual
Address            : 10.1.1.2
Netmask            : 255.255.255.0
Broadcast          : 10.1.1.255
----- [ IPv6 ] -----
Configuration      : Disabled

===== [ Proxy Information ] =====
State              : Disabled
Authentication     : Disabled

>

```

Verification of Basic Connectivity and Operations

After configuring an FTD to transparent mode, you may want to verify if the transparent FTD is working, is it invisible in the network? You can prove this using the mechanism of the Address Resolution Protocol (ARP). When a host computer communicates through an FTD,

the host is unable to see the FTD. Instead, it can see the devices deployed on the other side of the FTD.

Before testing the functionality, let's determine the MAC and IP addresses of all of the participating interfaces.

[Figure 9-13](#) details the (layer 1, 2 and 3) addresses of the network devices in OSPF area 1 network. Instead of seeing the FTD inside interface, the inside Router sees the outside router as its next hop.

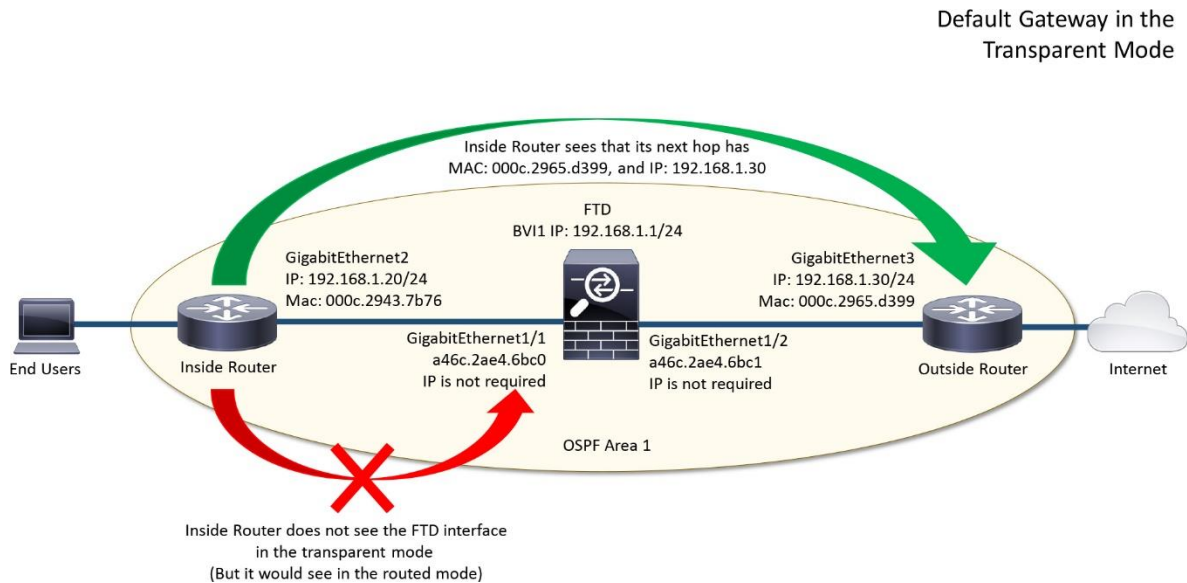


Figure 9-13. Traffic Flow between an Inside Router and Default Gateway

[Example 9-9](#) provides the commands that allows you to find the MAC and IP addresses of an interface on an FTD and a router.

Example 9-9 Commands to Determine the MAC and IP Addresses

! On FTD:

```
> show interface GigabitEthernet1/1 | include address
  MAC address a46c.2ae4.6bc0, MTU 1500
  IP address 192.168.1.1, subnet mask 255.255.255.0

> show interface GigabitEthernet1/2 | include address
  MAC address a46c.2ae4.6bc1, MTU 1500
  IP address 192.168.1.1, subnet mask 255.255.255.0
```

! On Router:

```
Inside-Router# show interfaces GigabitEthernet2 | include address
  Hardware is CSR vNIC, address is 000c.2943.7b76 (bia 000c.2943.7b76)
  Internet address is 192.168.1.20/24
```

```
Outside-Router## show interfaces GigabitEthernet3 | include address
  Hardware is CSR vNIC, address is 000c.2965.d399 (bia 000c.2965.d399)
  Internet address is 192.168.1.30/24
```

If you configured the interfaces according to the instructions on the previous section, you should be able to successfully ping from the inside router to the outside router.

[Example 9-10](#) demonstrates a successful ping test from the inside router to the outside router through the FTD. The drop of the first packet is an expected behavior. It happens because the ARP table is empty at the beginning.

Example 9-10 *Sending of a Successful Ping Request from Inside to Outside*

```
Inside-Router# ping 192.168.1.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.30, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 5/5/6 ms
Inside-Router#
```

The above ping test by the inside router does not prove if the ping replies come from the outside router, or from the BVI of the FTD. You can determine this by enabling debug on the FTD for ICMP traffic.

```
> debug icmp trace
debug icmp trace enabled at level 1
>
```

Once again, send the ping requests to the IP address of the outside router 192.168.1.30 from the inside router. The requests go through the FTD like the previous example. However, this time, the FTD shows log for the through traffic. Two lines for each ping request — one for sending a request and the other one is for receiving a reply.

```
ICMP echo request from INSIDE_INTERFACE:192.168.1.20 to
OUTSIDE_INTERFACE:192.168.1.30 ID=8 seq=1 len=72
ICMP echo reply from OUTSIDE_INTERFACE:192.168.1.30 to
INSIDE_INTERFACE:192.168.1.20 ID=8 seq=1 len=72
```

Now, check the ARP table on the inside router to view the mapping of IP addresses with the inside interface. Compare the entries on the table with the MAC addresses that you found in the previous command output ([Example 9-9](#)).

[Example 9-11](#) displays the mapping of the MAC addresses with the IP addresses. Besides the MAC address of its own interface (000c.2943.7b76), the ARP table of the inside router shows the MAC address of its next hop — the outside router (000c.2965.d399), not the FTD (a46c.2ae4.6bc0) which is transparent in the network.

Example 9-11 *Inside Router ARP Table — After Pinging from Inside to Outside Router*

```
Inside-Router# show arp
Protocol Address           Age (min)  Hardware Addr  Type   Interface
Internet 192.168.1.20          -          000c.2943.7b76 ARPA   GigabitEthernet2
Internet 192.168.1.30          2          000c.2965.d399 ARPA   GigabitEthernet2
Inside-Router#
```

If you send a ping request from the FTD itself, FTD uses the BVI interface address during reply. In that case, the ARP table on the router shows the MAC address of the FTD interface that communicates with the router.

[Example 9-12](#) demonstrates that when you ping from the FTD to the inside router, it uses the BVI address 192.168.1.1 as its IP address. Remember, in transparent mode, you do not configure any IPv4 address on the FTD physical interface.

Example 9-12 *BVI IP Address is Used When Traffic Originates from the FTD Itself*

```
> debug icmp trace
debug icmp trace enabled at level 1

> ping 192.168.1.20
ICMP echo request from 192.168.1.1 to 192.168.1.20 ID=52779 seq=30330
len=72
ICMP echo reply from 192.168.1.20 to 192.168.1.1 ID=52779 seq=30330 len=72
.
<Output Omitted for Brevity>
.

! To disable the debug of ICMP traffic:
> no debug icmp trace
debug icmp trace disabled.
>

! Alternatively, to disable all of the running debug processes:
> undebug all
>
```

[Example 9-13](#) shows a new entry in the ARP table after you sent ping requests to the inside router from the FTD itself. It now displays the MAC address of the GigabitEthernet1/1 interface (a46c.2ae4.6bc0) on FTD.

Example 9-13 *Inside Router ARP Table — After Pinging from FTD to Inside Router*

```
Inside-Router# show arp
Protocol Address          Age (min)  Hardware Addr  Type   Interface
Internet 192.168.1.1             1          a46c.2ae4.6bc0 ARPA   GigabitEthernet2
Internet 192.168.1.20           -          000c.2943.7b76 ARPA   GigabitEthernet2
Internet 192.168.1.30           5          000c.2965.d399 ARPA   GigabitEthernet2
Inside-Router#
```

Deployment between Layer 3 Networks

After configuring the physical and virtual interfaces, you are able to communicate with any hosts, through an FTD, within the same subnet. However, if you want to communicate with hosts that are in different subnets, a routing protocol is necessary.

When you configure a dynamic routing protocol across the network, FTD blocks the underlying routing traffic until you allow it in an access control policy. You can choose one of following options:

- Select a non-blocking policy as the default action
- Add a custom access rule to allow desired traffic

Figure 9-14 shows an FTD is deployed between an inside router and outside router. Both routers use loopback interfaces to simulate a host and internet. The loopback and routing interfaces are on different subnets and all of them are included in the OSPF area 1.

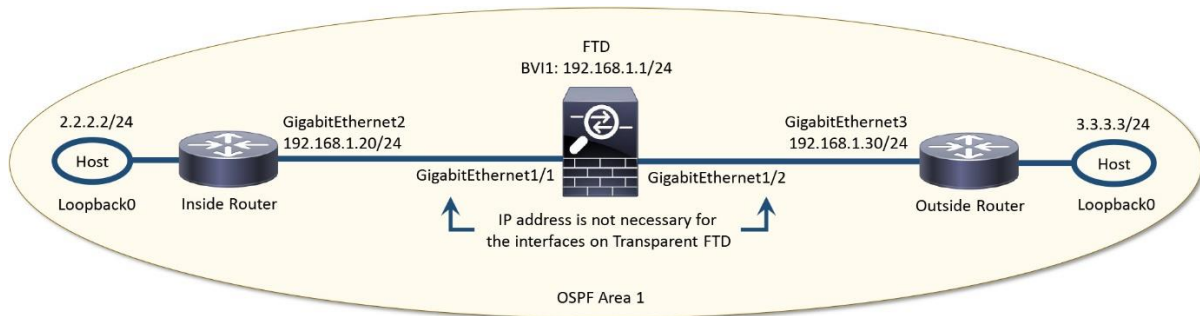


Figure 9-14. Transparent FTD Deployment in an OSPF Network

Default Action Selection

Default action in an access control policy determines how an FTD handles traffic when there is no matching access rules. To define the default action, go to the **Policies > Access Control** page to create a new policy, or you can edit an existing policy.

Figure 9-15 shows the options to create a new access control policy and to modify an existing one.

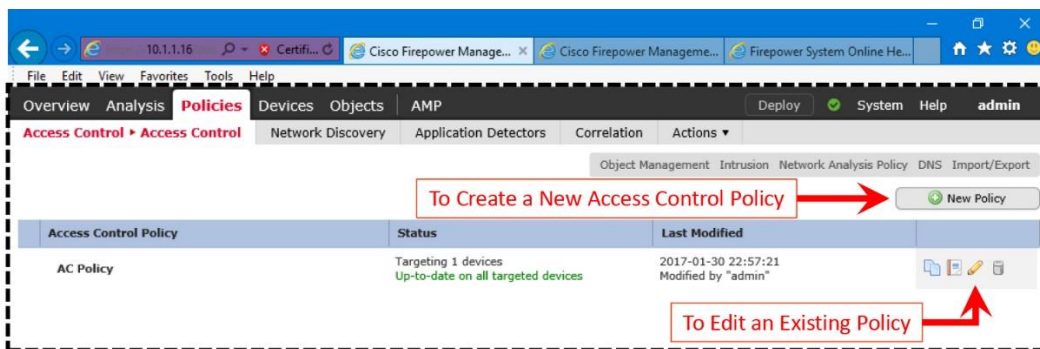


Figure 9-15. *Navigation to the Policies > Access Control Page*

When you are on the policy editor page, select the desired policy from the **Default Action** drop down. You can select one of the system provided policies that does not block traffic, or a policy that you created (if any). If you are not sure about selecting a policy, you can select the **Intrusion Prevention: Balanced Security and Connectivity** policy. It allows any unmatched traffic to go through an FTD after being inspected for malicious activities.

[Figure 9-16](#) shows a list of system provided policies that you can select for default action. Once you select a policy, save the changes and deploy it on your FTD.

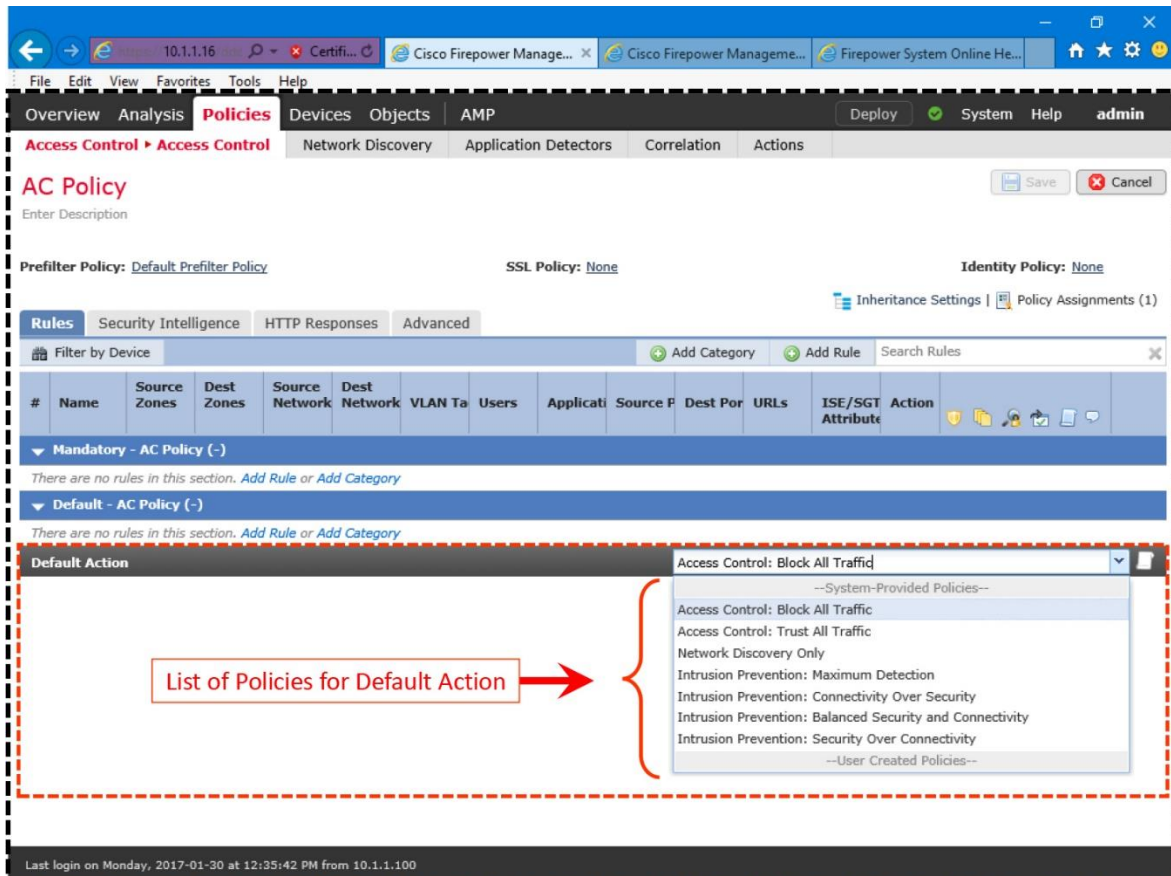


Figure 9-16. *System Provided Policies That Are Available for Default Action*

Access Rule Addition

Because of the security policy of your organization, if you select **Access Control: Block All Traffic** policy as the default action, traffic is blocked when it does not match with any custom access rules. Only the traffic that exclusively matches a rule is allowed through the FTD.

If you create an access rule to allow a particular routing protocol, such as OSPF, and select **Access Control: Block All Traffic** policy as the default action, then the FTD only allows OSPF management traffic. Any other data traffic, however, are dropped due to the default block action. In this scenario, two routers are able to build OSPF neighbor relationship through an FTD, however, you are unable to ping inside router from the outside router, or

vice versa. Similarly, you cannot use Secure Shell (SSH) to access a router from the other router although the neighbor relation is established. To allow any additional traffic, you need to add the related protocols in the access rule, and select the **Allow** action.

From the following configuration example, let's learn how to create two access rules — one for the routing traffic (OSPF), and the other one is for the data traffic (SSH).

To create an access rule for OSPF traffic:

Step 1. Go to the **Policies > Access Control** page. Click the **New Policy** button to create a new policy, or you can click on the pencil icon to edit an existing policy. The policy editor page appears.

[Figure 9-17](#) shows the **Add Rule** button that you select to create a new access rule.

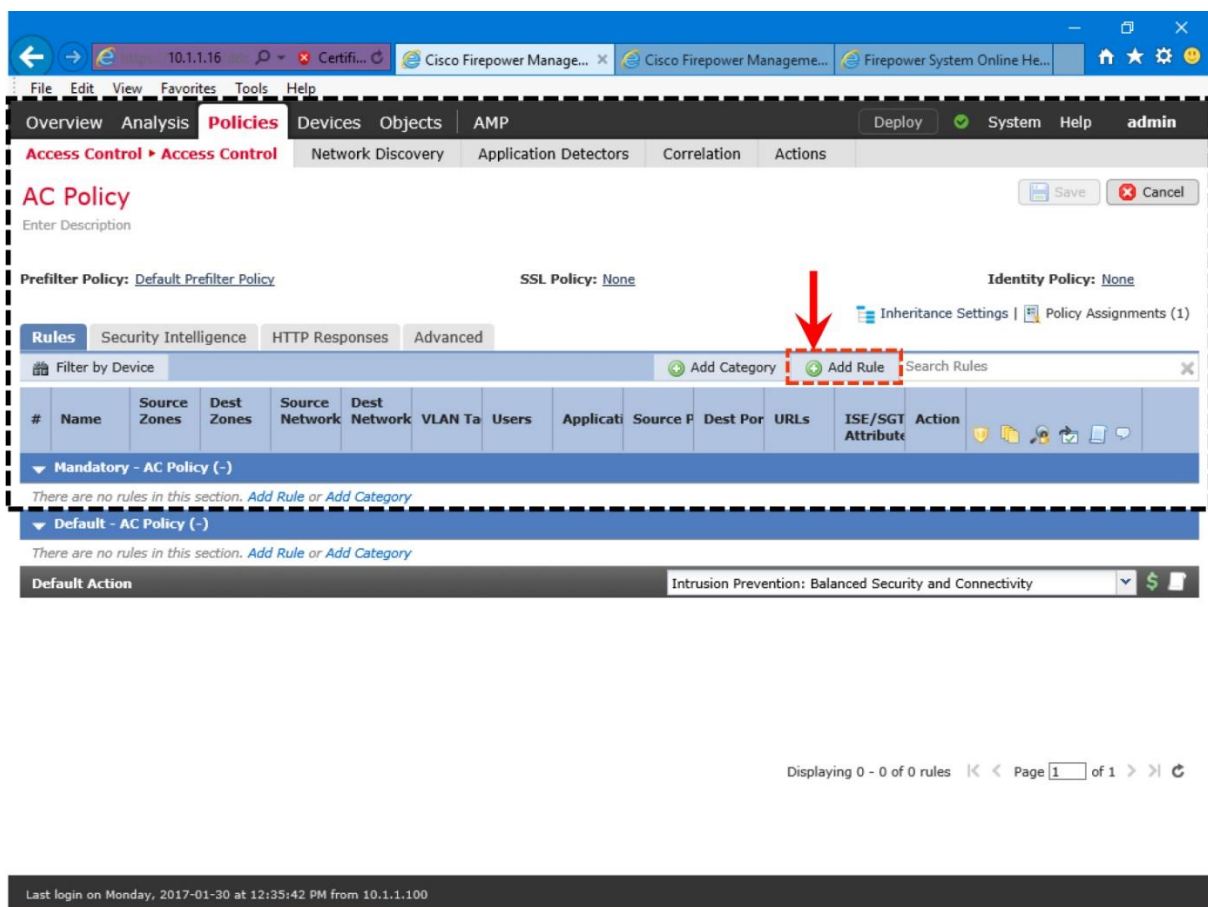


Figure 9-17. Navigation to the Add Rule Button

Step 2. On the policy editor page, click the **Add Rule** button. The **Add Rule** window appears.

Step 3. Give a name to this particular access rule, select the **Enabled** checkbox, and set the action to **Allow**.

Figure 9-18 shows the enablement of a new access rule called *Routing Access*. The rule action is set to allow.

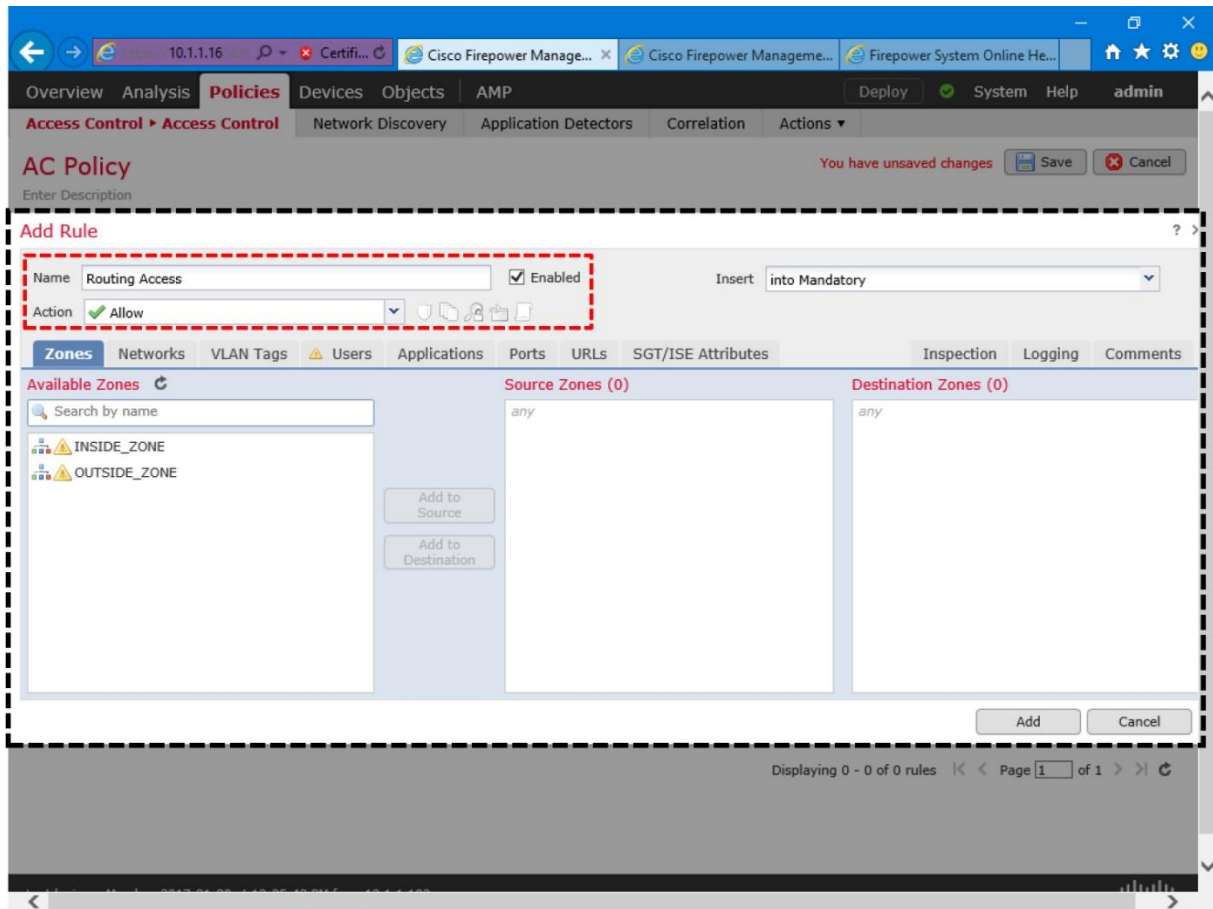


Figure 9-18. *The Add Rule Window Where You Define a Rule for Access Control*

Caution

Routers exchange keepalives to determine the state of the neighbors. If an FTD, deployed between two routers, inspects very high volume of traffic, it may delay the traverse of keepalive packets although you add an access rule to “allow” them. As a result, a router may take longer time to call its neighbor down. It worsens any reachability issues.

Tip

Firepower System offers two unique rule-actions — Trust and Fastpath — that can expedite the traverse of management traffic. In an Access Rule, you can set the action to **Trust** to let the OSPF traffic to go through the FTD without any further inspection. However, the more optimal method for bypassing an inspection is to add a Prefilter Rule for the OSPF protocol, and set the **Fastpath** action for it. To learn both options in detail, read the chapter on *Bypassing Inspection and Trusting Traffic*.

Step 4. Go to the **Ports** tab. Navigate to the **Protocol** dropdown that is under the **Selected Destination Ports** field.

Step 5. Select the OSPF/OSPFIGP protocol, and click the **Add** button next to the protocol dropdown. The selected protocol should be listed under the **Selected Destination Ports** box.

[Figure 9-19](#) shows the sequence to add an access rule called *Routing Access* to allow the OSPF protocol.

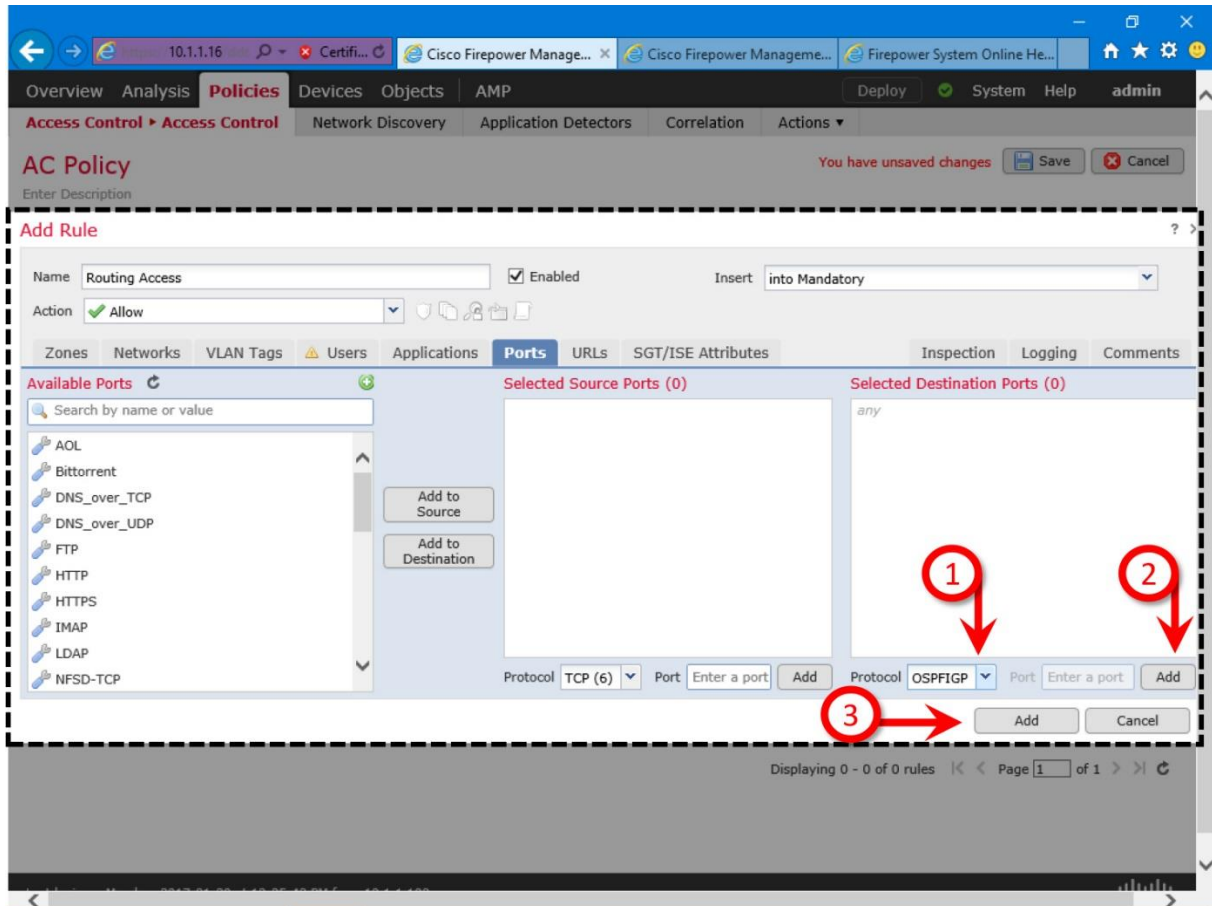


Figure 9-19. Allowing OSPF Protocol in an Access Rule

Step 6. Click the **Add** button. You will return to the policy editor page, and able to see the rule you have just created.

Access Rule for SSH

Similarly, you can create another rule to allow data traffic through SSH protocol. Below, you will learn how to allow the destination port 22 — the default port for SSH protocol.

Step 1. Click the **Add Rule** button once again. In the **Add Rule** window, repeat step 2 and 3. Such as, give a name to the rule, select the **Enabled** checkbox, and set the **Allow** action.

Step 2. Under **Available Ports** section, select **SSH** and click the **Add to Destination** button. The SSH protocol appears under the **Selected Destination Ports** box.

Figure 9-20 exhibits the steps to create an access rule, named *Shell Access*, to allow the SSH traffic via Port 22.

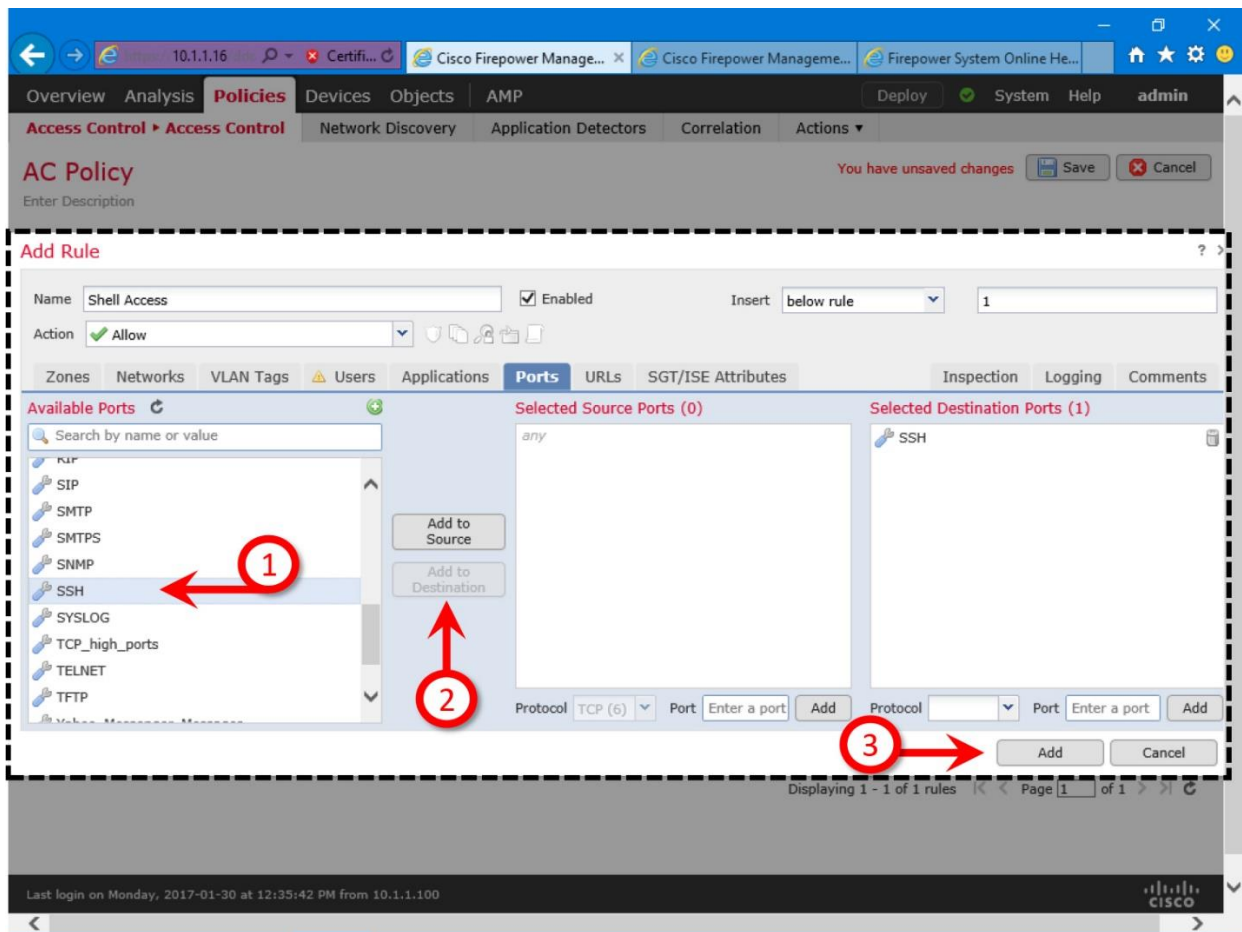


Figure 9-20. Allowing the Default SSH Port 22 in an Access Rule

Note

The above step allows SSH traffic when they are destined to the port 22, which is also the default port for SSH protocol. If you want to allow any SSH application traffic, regardless of its destination port number, you need to create a rule using **Applications** tab. To learn more about the Firepower application control, read the chapter on *Discovering Network Applications and Controlling Application Traffic*.

Step 3. Click the **Add** button to return to the policy editor page. Select **Access Control: Block All Traffic** policy as the **Default Action**.

Figure 9-21 shows two rules — *Routing Access* and *Shell Access* — are added. As the default action, **Access Control: Block All Traffic** policy is added.

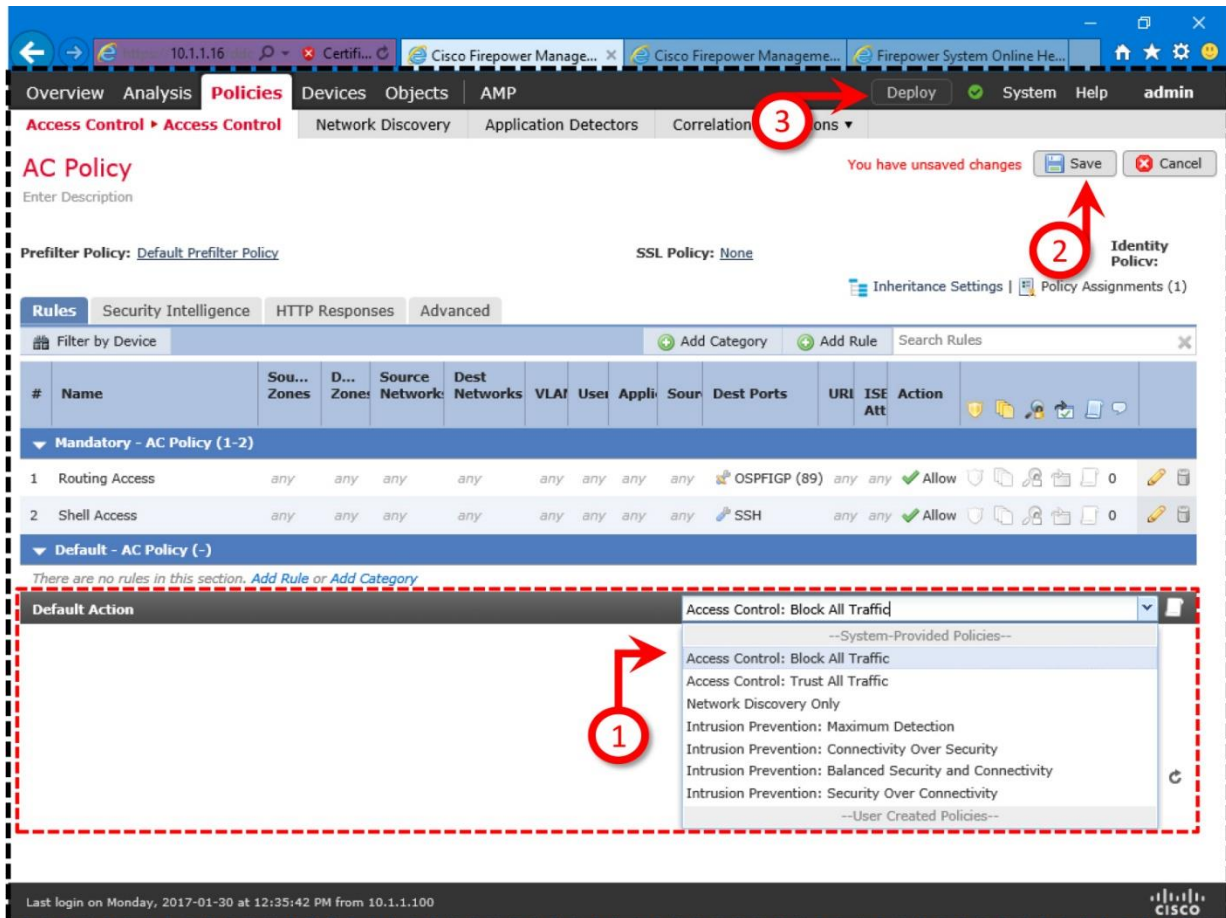


Figure 9-21. Selection of a Default Action

Step 4. You can add more access rules as necessary. For now, in this configuration example, just create the above two access rules, save the policy and deploy the new configuration on the FTD.

[Figure 9-22](#) confirms that the new access control policy is being deployed. It may take several minutes to complete the deployment.

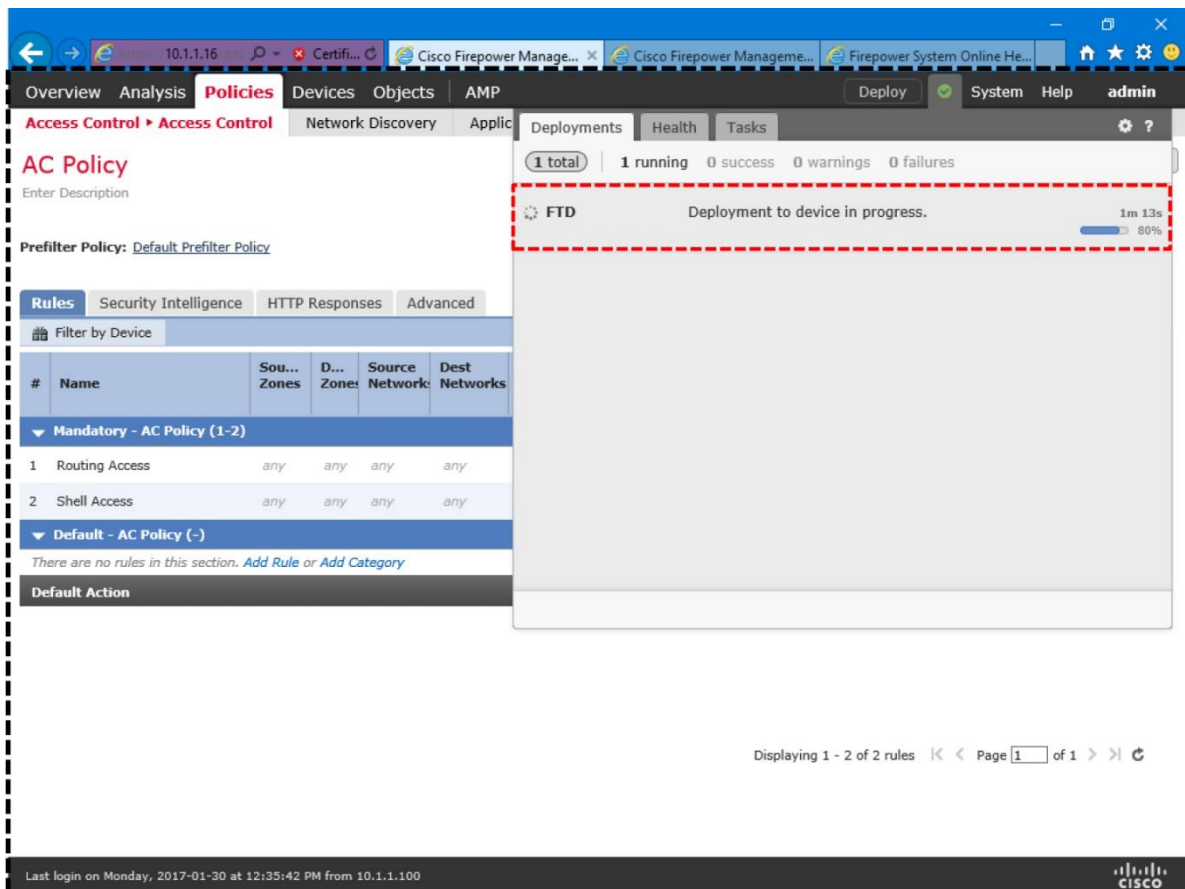


Figure 9-22. Status of a New Policy Deployment

Verification of Access Control Lists

When the traffic is not blocked or allowed according to the configurations on the FMC, you can use the CLI of the FTD to verify if the desired access rules are applied. You can run the **show access-list** command to view the custom access rules you created, as well as any implicit or system generated rules that are applied to the FTD.

[Example 9-14](#) shows the system generated access rules when an access control policy with no custom rule is applied. The last rule on line 10, **permit ip any any**, is applied implicitly when you select a non-blocking default action. The following example uses the Balanced Security and Connectivity policy as the default action.

Example 9-14 No Custom Rule with Balanced Security and Connectivity Default Policy

```
> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list CSM_FW_ACL_ ; 6 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY:
Default Tunnel and Priority Policy
```

```

access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL
ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998
(hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit 41 any any rule-id 9998
(hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 5 advanced permit gre any any rule-id 9998
(hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL_ line 6 advanced permit udp any eq 3544 any range
1025 65535 rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 7 advanced permit udp any range 1025 65535 any
eq 3544 rule-id 9998 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 8 remark rule-id 268434432: ACCESS POLICY: AC
Policy - Default/1
access-list CSM_FW_ACL_ line 9 remark rule-id 268434432: L4 RULE: DEFAULT
ACTION RULE
access-list CSM_FW_ACL_ line 10 advanced permit ip any any rule-id
268434432 (hitcnt=3281) 0xald3780e
>

```

[Example 9-15](#) shows two custom access rules on line 10 and 13, along with other system-generated rules, that are created on the FMC and applied to the FTD. These rules allow the FTD to permit OSPF and SSH traffic. The last rule on line 16, **deny ip any any**, is applied implicitly when you select **Access Control: Block All Traffic policy** as the default action.

Example 9-15 *Two Custom Rules with Block All Traffic as the Default Policy*

```

> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list CSM_FW_ACL_ ; 8 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY:
Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL
ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998
(hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit 41 any any rule-id 9998
(hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 5 advanced permit gre any any rule-id 9998
(hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL_ line 6 advanced permit udp any eq 3544 any range
1025 65535 rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 7 advanced permit udp any range 1025 65535 any
eq 3544 rule-id 9998 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 8 remark rule-id 268437504: ACCESS POLICY: AC
Policy - Mandatory/1
access-list CSM_FW_ACL_ line 9 remark rule-id 268437504: L7 RULE: Routing
Access
access-list CSM_FW_ACL_ line 10 advanced permit ospf any any rule-id
268437504 (hitcnt=4) 0x385cc1f6
access-list CSM_FW_ACL_ line 11 remark rule-id 268437505: ACCESS POLICY: AC
Policy - Mandatory/2
access-list CSM_FW_ACL_ line 12 remark rule-id 268437505: L7 RULE: Shell
Access
access-list CSM_FW_ACL_ line 13 advanced permit tcp any any object-group
SSH rule-id 268437505 (hitcnt=8) 0x030eea01
      access-list CSM_FW_ACL_ line 13 advanced permit tcp any any eq ssh rule-
id 268437505 (hitcnt=8) 0xf8ca4a86

```

```
access-list CSM_FW_ACL_ line 14 remark rule-id 268434432: ACCESS POLICY: AC
Policy - Default/1
access-list CSM_FW_ACL_ line 15 remark rule-id 268434432: L4 RULE: DEFAULT
ACTION RULE
access-list CSM_FW_ACL_ line 16 advanced deny ip any any rule-id 268434432
event-log flow-start (hitcnt=826) 0x97aa021a
>
```

If you set the default action to block all traffic, and do not permit the OSPF traffic through an access list, the neighbor relationship breaks. When a neighbor goes down, FTD triggers an alert on the CLI similar to the following:

```
Jan 31 04:00:51.434: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on
GigabitEthernet2 from FULL to DOWN, Neighbor Down: Dead timer expired
Summary
```

This chapter discusses the transparent firewall mode — how to configure the physical and virtual interfaces. Furthermore, you have learned various command line tools that enables you to investigate any potential configuration issues.

Quiz

1. Which of the following statements is true about deployment?

- a. You can replace a layer 2 switch with a transparent FTD — there is no difference between them.
- b. Switching between the transparent mode and routed mode requires a restart.
- c. You can use an FMC to configure an FTD from routed to transparent mode.
- d. Changing the firewall deployment mode erases any existing configuration.

2. Which of the following statements is true about IP address?

- a. You should use the IP address of a BVI interface as the default gateway for the hosts in a bridged network.
- b. The IP address of a BVI interface should be on a different subnet than any hosts in the bridge group.
- c. BVI IP address is used as the source IP address for packets that originate from an FTD.
- d. You can configure IPv4 address on any physical interface.

3. Which of the following statements is true when you select “Access Control: Block All Traffic” policy as the default action?

- a. It overrides any “allow” access rules deployed on an FTD.

b. It blocks the traffic when the intrusion prevention system of an FTD finds no malicious activities.

c. This policy is equivalent to the “**deny tcp any any**” access rule.

d. It blocks any traffic that do not match an existing access rule.

4. Which of the following command displays the access rule entries?

a. show access-control

b. show access-control-rule

c. show access-list

d. show access-list-config

Chapter 10. Capture of Traffic for Advance Analysis

After deploying an FTD, if your network exhibits any connectivity issue, one of the first steps is to verify the configurations. If you, however, could not determine any configuration error, you may want to capture the live traffic and analyze them. This chapter discusses the processes to capture traffic using the built-in tools of an FTD.

Essential Knowledge

As you have learned that, Cisco introduces a unified image on the Firepower Threat Defense (FTD) software. It converges the features of a traditional Cisco ASA firewall, as well the Next-Generation Firepower services. The Firepower service includes various advanced security technologies, such as, security intelligence, network discovery, application control, file control, Snort-based intrusion prevention system, and so on.

When FTD blocks the traverse of a packet from ingress to egress interface, it is actually performed by either ASA engine or Firepower engine. Therefore, if two hosts experience any connectivity issues while sending traffic through an FTD, it is essential to analyze packets from both engines to determine the root cause of a problem. For example, to investigate any registration or communications issues between an FTD and FMC, capturing traffic from the Firepower management interfaces is one of the key troubleshooting steps.

[Figure 10-1](#) provides a high-level overview of the flow of traffic through an FTD. An ASA engine receives a packet from the ingress interface and redirects to the Firepower engine.

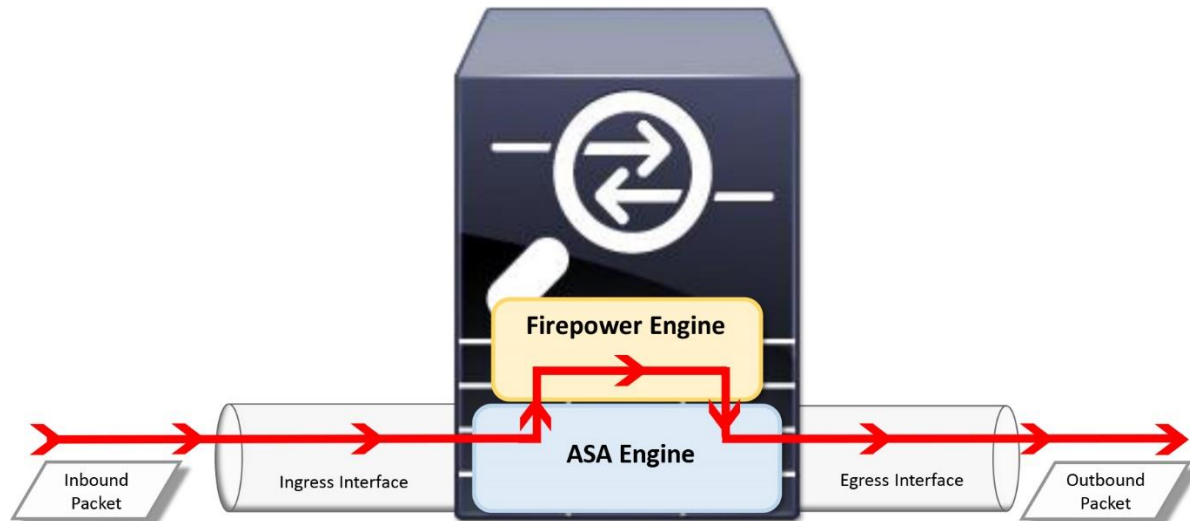


Figure 10-1. *Flow of Traffic between an Ingres and Egress Interfaces of an FTD*

You can utilize any third party packet sniffers to capture traffic from the Firepower interfaces. However, both Firepower systems — FMC and FTD — offer a native packet capturing tool within the operating system.

Best Practices

Before you consider capturing traffic, make sure you understand the following items:

- The primary objective of a Firepower system is not to capture live traffic all the time. Besides controlling and inspecting traffic, a Firepower system supports capture of live traffic only for troubleshooting purpose. If you need to capture traffic for a long period, you should find a dedicated system designed for this purpose.
- Capturing live traffic on a production system can degrade system performance. If necessary, you should capture traffic during a maintenance window.
- Instead of displaying the packets on the console, redirect them into a file, copy the file from the Firepower system to your computer, and open it using any packet analyzer. If you decide not to store the packet in a file anyway, you should limit the number of packets that you want to capture.

Configuration

The process to capture traffic varies, depends on where you want to probe. In the following sections, you will learn how to capture packets from the following hardware and software components:

- Firepower engine
- ASA engine
- Firepower Management Center (FMC)

[Figure 10-2](#) shows the lab topology that is used in this chapter to capture traffic with various options.

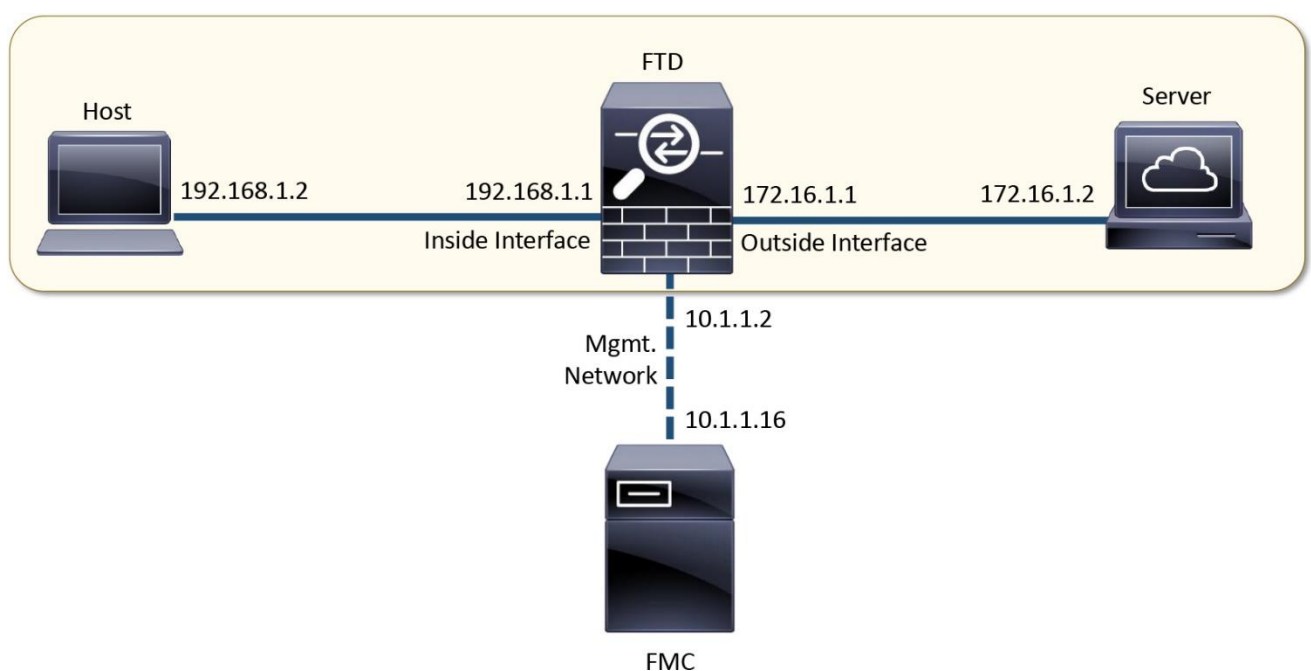


Figure 10-2. Topology for the Packet Capture Lab

On a Firepower Engine

In order to capture traffic from the Firepower engine, use the following steps:

Step 1. Login to the CLI of the FTD.

Step 2. Run the **capture-traffic** command on the shell. System prompts to choose a domain.

Step 3. Select the **Router** domain to capture traffic from the data interfaces. The **br1** domain captures traffic from the management interface. Enter your selection to continue.

[Example 10-1](#) exhibits the selection of a domain during capturing traffic. The option **1 – Router** is selected, which enables the capture from the data interfaces.

Example 10-1 Running of the capture-traffic Command for the Data Interfaces

```
> capture-traffic

Please choose domain to capture traffic from:
  0 - br1
  1 - Router

Selection? 1

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
```

Step 4. When the FTD prompts you to specify the tcpdump options, use the following tables to determine your desired options. If you do not provide any options, it captures traffic without any filter, by default.

Step 5. After you add options, press enter to begin the capture. To terminate a capture at any time, press the **Ctrl+c** keys.

Tcpdump Options

Tcpdump offers wide variety of options that you can utilize to manage captured packets. It also supports Berkley Packet Filter (BPF) that allows you to control and enhance the display of packet data.

[Table 10-1](#) provides a list of some useful options that you can use during packet capture. Some of these options allows you to collect additional information from each packet, such as, -e, -n, -v, and -X. The other options give you an ability to manage the capturing process. For instance, -c, -s, and -w.

Options	Usage
-c	Stops after certain number of packets are captured.
-e	Displays the Ethernet header in the capture.
-n	Does not resolve hostname and port name.
-s	Defines the size (snaplength) of the captured packets.
-v	Shows extra packet data. -vv shows even more data.
-w	Saves the captured packets in a file instead of displaying on the console.
-X	Shows packet contents in hex and ASCII.

Table 10-1. *Useful tcpdump Options*

[Table 10-2](#) lists some of the useful BPF Syntaxes that you can apply to filter desired traffic during capturing traffic.

Options	Usage
host, net	Filters traffic to and from a single host or the entire network, respectively.
port, portrange	Filters traffic to and from a single or range of ports, respectively.
src, dst	Select a direction for traffic flow — source or destination. Used in conjunction with host and port options.
and, or, not	Combines or isolates traffic with a precise condition.
vlan	Captures traffic related to a particular VLAN. To capture VLAN tagged traffic, you must enter the vlan option followed by the desired <i>vlan id</i> .

Table 10-2. *BPF Syntax to Filter Live Traffic during a Traffic Capture*

Tips

Whenever you capture traffic, you should view the actual IP address and port number (using -n option) in the packet. You should also either save the capture (-w option) into a file, or limit the number of packets you want to capture (-c option).

[Example 10-2](#) demonstrates the capture of traffic using various tcpdump options. The packets, in the following example, are captured by running the **capture-traffic** command separately. Use the Ctrl+c keys to exit a capture process.

Example 10-2 Usage of Different tcpdump Options

```
! To capture the 5 HTTP transactions between a web server and a host with
IP address
192.168.1.2:
```

```
Options: -n -c 5 host 192.168.1.2 and port 80
```

```
03:42:23.479970 IP 192.168.1.2.44694 > 172.16.1.2.80: Flags [S], seq
2622260089, win
29200, options [mss 1380,sackOK,TS val 2174057 ecr 0,nop,wscale 7],
```

```
length 0
03:42:23.479970 IP 172.16.1.2.80 > 192.168.1.2.44694: Flags [S.], seq
287740527, ack
2622260090, win 28960, options [mss 1380,sackOK,TS val 1270689 ecr
2174057,nop,wscale
7], length 0
03:42:23.479970 IP 192.168.1.2.44694 > 172.16.1.2.80: Flags [.] , ack 1, win
229, options
[nop,nop,TS val 2174058 ecr 1270689], length 0
03:42:23.479970 IP 192.168.1.2.44694 > 172.16.1.2.80: Flags [P.], ack 1,
win 229, options
[nop,nop,TS val 2174058 ecr 1270689], length 436
03:42:23.479970 IP 172.16.1.2.80 > 192.168.1.2.44694: Flags [.] , ack 437,
win 235, options
[nop,nop,TS val 1270689 ecr 2174058], length 0
>
```

! To capture the client side traffic – originated by a host, destined to a web server:

Options: **-n -c 5 src 192.168.1.2 and dst port 80**

```
03:47:07.529956 IP 192.168.1.2.44698 > 172.16.1.2.80: Flags [S], seq
3873637979, win
29200, options [mss 1380,sackOK,TS val 2245066 ecr 0,nop,wscale 7], length
0
03:47:07.529956 IP 192.168.1.2.44698 > 172.16.1.2.80: Flags [.] , ack
3924903157, win
229, options [nop,nop,TS val 2245066 ecr 1341696], length 0
03:47:07.529956 IP 192.168.1.2.44698 > 172.16.1.2.80: Flags [P.], ack 1,
win 229,
options [nop,nop,TS val 2245066 ecr 1341696], length 436
03:47:07.529956 IP 192.168.1.2.44698 > 172.16.1.2.80: Flags [.] , ack 1369,
win 251,
options [nop,nop,TS val 2245067 ecr 1341697], length 0
03:47:07.529956 IP 192.168.1.2.44698 > 172.16.1.2.80: Flags [.] , ack 2737,
win 274,
options [nop,nop,TS val 2245067 ecr 1341697], length 0
>
```

! To capture the server side traffic – originated by a web server, destined to host 192.168.1.2:

Options: **-n -c 5 dst 192.168.1.2 and src port 80**

```
03:49:11.779943 IP 172.16.1.2.80 > 192.168.1.2.44702: Flags [S.], seq
212338482, ack
2358717416, win 28960, options [mss 1380,sackOK,TS val 1372759 ecr
2276129,nop,wscale
7], length 0
03:49:11.789952 IP 172.16.1.2.80 > 192.168.1.2.44702: Flags [.] , ack 437,
win 235,
options [nop,nop,TS val 1372759 ecr 2276129], length 0
03:49:11.789952 IP 172.16.1.2.80 > 192.168.1.2.44702: Flags [.] , ack 437,
win 235,
options [nop,nop,TS val 1372759 ecr 2276129], length 1368
03:49:11.789952 IP 172.16.1.2.80 > 192.168.1.2.44702: Flags [.] , ack 437,
win 235,
options [nop,nop,TS val 1372759 ecr 2276129], length 1368
```

```
03:49:11.789952 IP 172.16.1.2.80 > 192.168.1.2.44702: Flags [P.], ack 437,
win 235,
options [nop,nop,TS val 1372759 ecr 2276129], length 789
>
```

[Example 10-3](#) demonstrates the options to print additional data during capturing traffic.

Example 10-3 *Displaying Additional Packet Data Using tcpdump Tool*

! First, look at the following capture with default packet data:

```
Options: -n -c 5 host 192.168.1.2
```

```
04:36:10.329969 IP 192.168.1.2.58718 > 172.16.1.2.80: Flags [S], seq
193723078, win
29200, options [mss 1380,sackOK,TS val 392486 ecr 0,nop,wscale 7], length 0
04:36:10.329969 IP 172.16.1.2.80 > 192.168.1.2.58718: Flags [S.], seq
2078424703, ack
193723079, win 28960, options [mss 1380,sackOK,TS val 2077347 ecr
392486,nop,wscale 7],
length 0
04:36:10.329969 IP 192.168.1.2.58718 > 172.16.1.2.80: Flags [.], ack 1, win
229, options
[nop,nop,TS val 392486 ecr 2077347], length 0
04:36:10.329969 IP 192.168.1.2.58718 > 172.16.1.2.80: Flags [P.], ack 1,
win 229, options
[nop,nop,TS val 392486 ecr 2077347], length 436
04:36:10.329969 IP 172.16.1.2.80 > 192.168.1.2.58718: Flags [.], ack 437,
win 235, options
[nop,nop,TS val 2077347 ecr 392486], length 0
>
```

! The `-vv` option prints additional data including the checksum of a packet.

```
Options: -n -c 5 -vv host 192.168.1.2
```

```
04:36:44.729957 IP (tos 0x0, ttl 64, id 27818, offset 0, flags [DF], proto
TCP (6), length 60)
  192.168.1.2.58720 > 172.16.1.2.80: Flags [S], cksum 0x730b (correct),
seq
2112778772, win 29200, options [mss 1380,sackOK,TS val 401086 ecr
0,nop,wscale 7], length 0
04:36:44.729957 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP
(6), length 60)
  172.16.1.2.80 > 192.168.1.2.58720: Flags [S.], cksum 0x0515 (correct),
seq
2199066473, ack 2112778773, win 28960, options [mss 1380,sackOK,TS val
2085945 ecr
401086,nop,wscale 7], length 0
04:36:44.729957 IP (tos 0x0, ttl 64, id 27819, offset 0, flags [DF], proto
TCP (6),
length 52)
  192.168.1.2.58720 > 172.16.1.2.80: Flags [.], cksum 0xa3cc (correct),
seq 1, ack 1,
win 229, options [nop,nop,TS val 401086 ecr 2085945], length 0
04:36:44.729957 IP (tos 0x0, ttl 64, id 27820, offset 0, flags [DF], proto
TCP (6),
length 488)
```

```

192.168.1.2.58720 > 172.16.1.2.80: Flags [P.], cksum 0xf6e9 (correct),
seq 1:437,
ack 1, win 229, options [nop,nop,TS val 401086 ecr 2085945], length 436
04:36:44.729957 IP (tos 0x0, ttl 64, id 65408, offset 0, flags [DF], proto
TCP (6),
length 52)
172.16.1.2.80 > 192.168.1.2.58720: Flags [.], cksum 0xa212 (correct),
seq 1, ack 437,
win 235, options [nop,nop,TS val 2085945 ecr 401086], length 0
>

```

! The -e option displays the layer 2 header in the capture.

```

Options: -n -c 5 -e host 192.168.1.2
04:37:21.909941 c4:2c:03:3c:98:a8 > a4:6c:2a:e4:6b:c0, ethertype IPv4
(0x0800), length
74: 192.168.1.2.58722 > 172.16.1.2.80: Flags [S], seq 1691712365, win
29200, options
[mss 1380,sackOK,TS val 410383 ecr 0,nop,wscale 7], length 0
04:37:21.919935 00:23:24:72:1d:3c > a4:6c:2a:e4:6b:c1, ethertype IPv4
(0x0800), length
74: 172.16.1.2.80 > 192.168.1.2.58722: Flags [S.], seq 3252338695, ack
1691712366, win
28960, options [mss 1380,sackOK,TS val 2095242 ecr 410383,nop,wscale 7],
length 0
04:37:21.919935 c4:2c:03:3c:98:a8 > a4:6c:2a:e4:6b:c0, ethertype IPv4
(0x0800), length
66: 192.168.1.2.58722 > 172.16.1.2.80: Flags [.], ack 1, win 229, options
[nop,nop,TS
val 410383 ecr 2095242], length 0
04:37:21.919935 c4:2c:03:3c:98:a8 > a4:6c:2a:e4:6b:c0, ethertype IPv4
(0x0800), length
502: 192.168.1.2.58722 > 172.16.1.2.80: Flags [P.], ack 1, win 229, options
[nop,nop,TS
val 410383 ecr 2095242], length 436
04:37:21.919935 00:23:24:72:1d:3c > a4:6c:2a:e4:6b:c1, ethertype IPv4
(0x0800), length
66: 172.16.1.2.80 > 192.168.1.2.58722: Flags [.], ack 437, win 235, options
[nop,nop,TS
val 2095242 ecr 410383], length 0
>

```

! The -X option prints the hex and ASCII values of each packet. For example, the fourth packet in the following example shows the GET request to a HTTP server.

```

Options: -n -c 5 -X host 192.168.1.2
04:40:50.069988 IP 192.168.1.2.58724 > 172.16.1.2.80: Flags [S], seq
3090457163, win
29200, options [mss 1380,sackOK,TS val 462423 ecr 0,nop,wscale 7], length 0
0x0000: 4500 003c ac1c 4000 4006 1fe3 c0a8 0102  E..<..@.@.....
0x0010: ac10 0102 e564 0050 b834 a24b 0000 0000  ....d.P.4.K....
0x0020: a002 7210 18f0 0000 0204 0564 0402 080a  ..r.....d....
0x0030: 0007 0e57 0000 0000 0103 0307          ...W.....
04:40:50.069988 IP 172.16.1.2.80 > 192.168.1.2.58724: Flags [S.], seq
1195208673, ack

```

```

3090457164, win 28960, options [mss 1380,sackOK,TS val 2147276 ecr
462423,nop,wscale 7],
length 0
    0x0000:  4500 003c 0000 4000 4006 cbff ac10 0102  E..<..@.@.....
    0x0010:  c0a8 0102 0050 e564 473d 6fe1 b834 a24c  ....P.dG=o..4.L
    0x0020:  a012 7120 9ec3 0000 0204 0564 0402 080a  ..q.....d....
    0x0030:  0020 c3cc 0007 0e57 0103 0307          .....W....
04:40:50.069988 IP 192.168.1.2.58724 > 172.16.1.2.80: Flags [.] , ack 1, win
229,
options [nop,nop,TS val 462423 ecr 2147276], length 0
    0x0000:  4500 0034 ac1d 4000 4006 1fea c0a8 0102  E..4..@.@.....
    0x0010:  ac10 0102 e564 0050 b834 a24c 473d 6fe2  ....d.P.4.LG=o.
    0x0020:  8010 00e5 3d7b 0000 0101 080a 0007 0e57  ....={.....W
    0x0030:  0020 c3cc          .....
04:40:50.069988 IP 192.168.1.2.58724 > 172.16.1.2.80: Flags [P.] , ack 1,
win 229,
options [nop,nop,TS val 462423 ecr 2147276], length 436
    0x0000:  4500 01e8 ac1e 4000 4006 1e35 c0a8 0102  E.....@.@..5....
    0x0010:  ac10 0102 e564 0050 b834 a24c 473d 6fe2  ....d.P.4.LG=o.
    0x0020:  8018 00e5 9098 0000 0101 080a 0007 0e57  .....W
    0x0030:  0020 c3cc 4745 5420 2f20 4854 5450 2f31  ....GET./..HTTP/1
    0x0040:  2e31 0d0a 486f 7374 3a20 3137 322e 3136  .1..Host::172.16
    0x0050:  2e31 2e32 0d0a 5573 6572 2d41 6765 6e74  .1.2..User-Agent
    0x0060:  3a20 4d6f 7a69 6c6c 612f 352e 3020 2858  :.Mozilla/5.0.(X
    0x0070:  3131 3b20 5562 756e 7475 3b20 4c69 6e75  11;.Ubuntu;.Linu
    0x0080:  7820 7838 365f 3634 3b20 7276 3a34 382e  x.x86_64;.rv:48.
    0x0090:  3029 2047 6563 6b6f 2f32 3031 3030 3130  0).Gecko/2010010
    0x00a0:  3120 4669 7265 666f 782f 3438 2e30 0d0a  1.Firefox/48.0..
    0x00b0:  4163 6365 7074 3a20 7465 7874 2f68 746d  Accept:.text/htm
    0x00c0:  6c2c 6170 706c 6963 6174 696f 6e2f 7868  l,application/xh
    0x00d0:  746d 6c2b 786d 6c2c 6170 706c 6963 6174  tml+xml,applicat
    0x00e0:  696f 6e2f 786d 6c3b 713d 302e 392c 2a2f  ion/xml;q=0.9,*/*
    0x00f0:  2a3b 713d 302e 380d 0a41 6363 6570 742d  *;q=0.8..Accept-
    0x0100:  4c61 6e67 7561 6765 3a20 656e 2d55 532c  Language:.en-US,
    0x0110:  656e 3b71 3d30 2e35 0d0a 4163 6365 7074  en;q=0.5..Accept
    0x0120:  2d45 6e63 6f64 696e 673a 2067 7a69 702c  -Encoding:.gzip,
    0x0130:  2064 6566 6c61 7465 0d0a 436f 6e6e 6563  .deflate..Connec
    0x0140:  7469 6f6e 3a20 6b65 6570 2d61 6c69 7665  tion:.keep-alive
    0x0150:  0d0a 5570 6772 6164 652d 496e 7365 6375  ..Upgrade-Insecu
    0x0160:  7265 2d52 6571 7565 7374 733a 2031 0d0a  re-Requests:.1..
    0x0170:  4966 2d4d 6f64 6966 6965 642d 5369 6e63  If-Modified-Sinc
    0x0180:  653a 2054 7565 2c20 3134 2046 6562 2032  e:.Tue,.14.Feb.2
    0x0190:  3031 3720 3136 3a32 343a 3339 2047 4d54  017.16:24:39.GMT
    0x01a0:  0d0a 4966 2d4e 6f6e 652d 4d61 7463 683a  ..If-None-Match:
    0x01b0:  2022 3263 3339 2d35 3438 3830 3030 3333  ."2c39-548800033
    0x01c0:  3730 6463 2d67 7a69 7022 0d0a 4361 6368  70dc-gzip"..Cach
    0x01d0:  652d 436f 6e74 726f 6c3a 206d 6178 2d61  e-Control:.max-a
    0x01e0:  6765 3d30 0d0a 0d0a          ge=0....
04:40:50.069988 IP 172.16.1.2.80 > 192.168.1.2.58724: Flags [.] , ack 437,
win 235,
options [nop,nop,TS val 2147276 ecr 462423], length 0
    0x0000:  4500 0034 1e39 4000 4006 adce ac10 0102  E..4.9@.@.....
    0x0010:  c0a8 0102 0050 e564 473d 6fe2 b834 a400  ....P.dG=o..4..
    0x0020:  8010 00eb 3bc1 0000 0101 080a 0020 c3cc  ....;.....
    0x0030:  0007 0e57          ...W
>

```

[Download a PCAP File for Offline Analysis](#)

In addition to the live view on a console, you can also redirect a capture into a .pcap file. Later, you can retrieve the file using any packet analyzer software for further analysis.

[Example 10-4](#) displays the options to capture traffic to and from the host 192.168.1.2. While the packets are being captured, the system stores them into the traffic.pcap file.

Example 10-4 *Options to Save the Packets into a PCAP File*

```
Options: -w traffic.pcap -s 1518 host 192.168.1.2
```

```
^C
```

```
Caught interrupt signal
```

```
Exiting.
```

```
>
```

```
! The following command confirms that the pcap file is created and stored  
on the disk.
```

```
> file list
```

```
Feb 15 05:03                886 /traffic.pcap
```

```
>
```

Once the traffic is captured and a PCAP file is created, you can download the file both ways — using GUI or CLI.

Using GUI

FTD does not have its own GUI. You can, however, use the GUI of the FMC to download a file, as shown in the following steps.

Step 1. Login to the GUI of the FMC, and navigate to the **System > Health > Monitor** page. The **Appliance Status Summary** chart appears.

Step 2. Find the FTD where you captured traffic. If you do not see your appliance, expand the related arrow key next to the health status.

[Figure 10-3](#) shows an arrow key next to the **Normal** status. Expansion of this arrow displays all of the appliances that have normal health status.

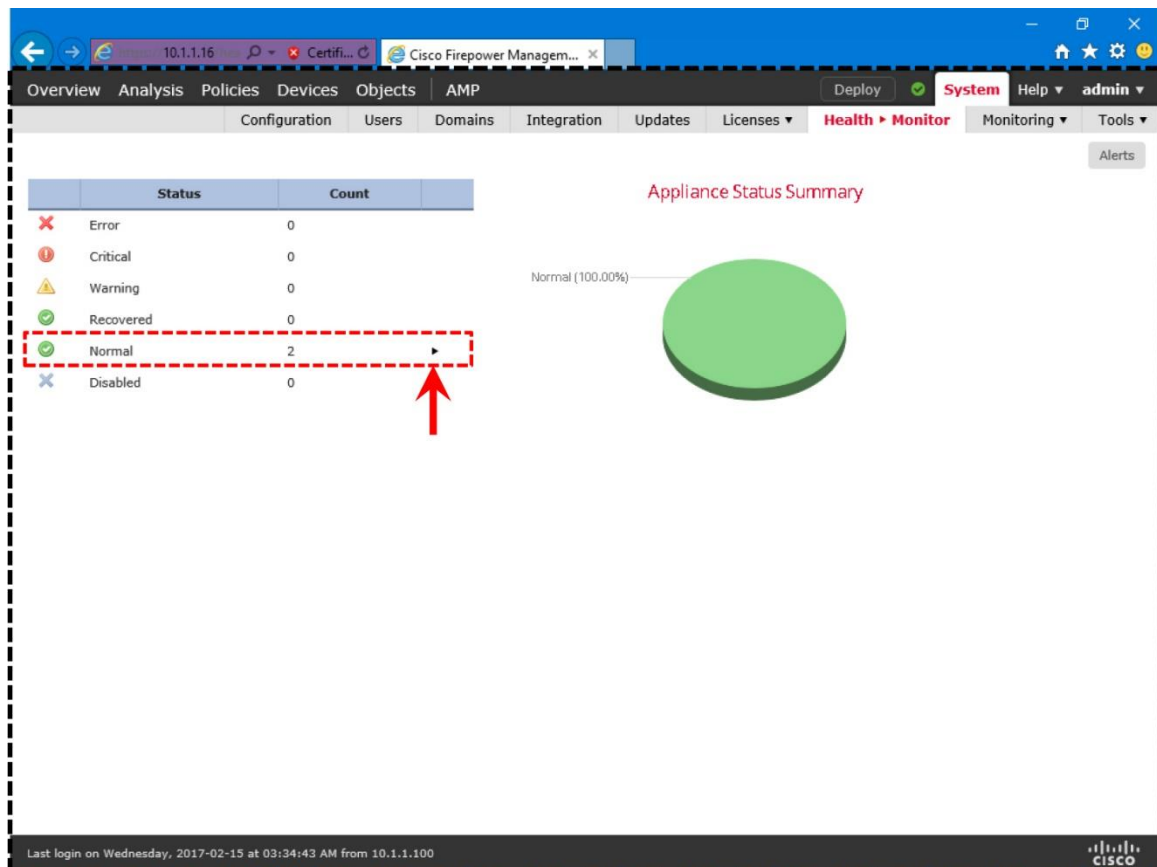


Figure 10-3. *Appliance Status Summary*

Step 3. When you find the FTD on this page, click on the appliance name. The **Health Monitor** page for the FTD appears.

Step 4. Select the **Advanced Troubleshooting** button. The **File Download** page appears.

Figure 10-4 displays the **Advanced Troubleshooting** button next to the name of the FTD appliance.

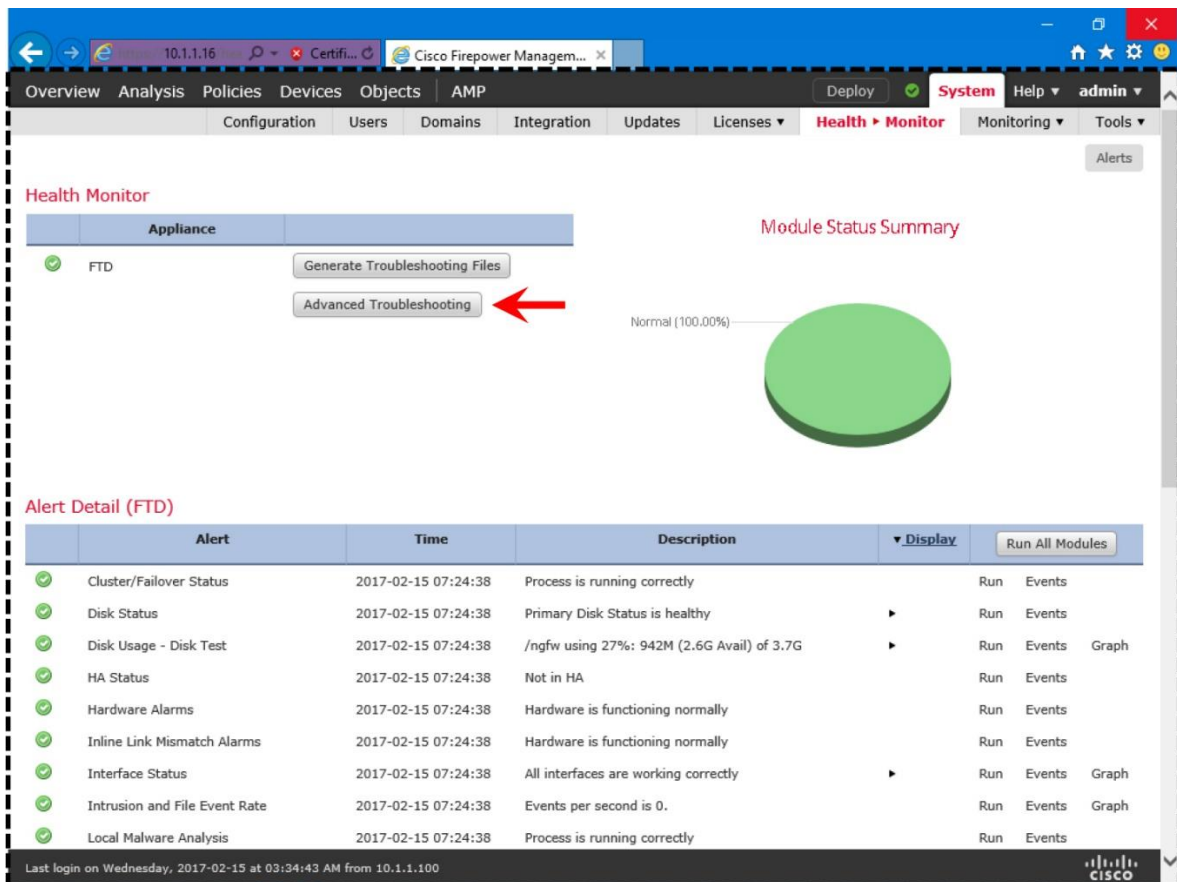


Figure 10-4. Advanced Troubleshooting Button

Step 5. On the **File Download** page, you will see a field where can enter the name of a pcap file. Use the filename with .pcap file extension.

Step 6. Click the **Download** button to begin the file download.

[Figure 10-5](#) shows the name of the pcap file, traffic.pcap, is entered on the **File Download** page.

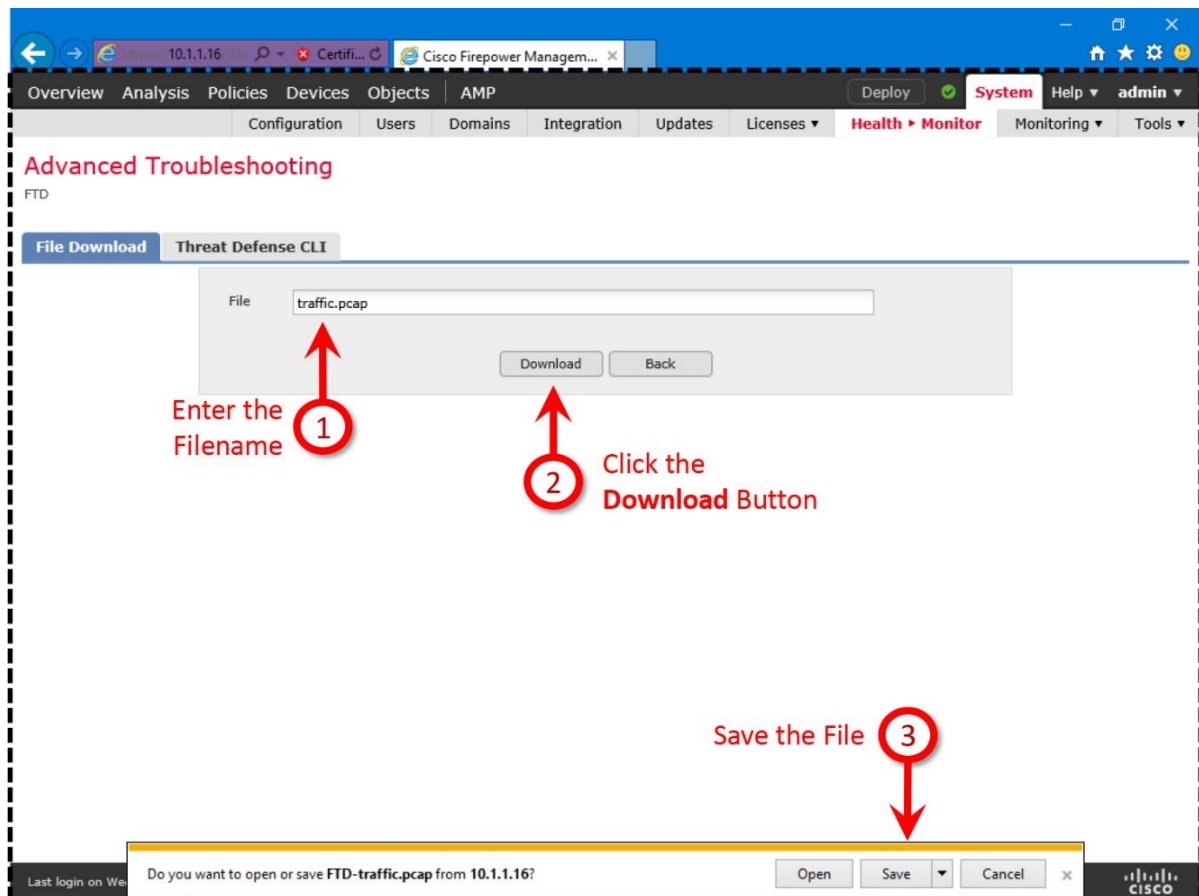


Figure 10-5. The File Download Page Appears within Advanced Troubleshooting Page

Using CLI

Alternatively, you can use the CLI to copy a file to an external system, if the system runs SSH daemon. To transfer files, FTD uses Secure Copy (SCP) protocol which is based on the Secure Shell (SSH) protocol, as shown in the following command syntax.

```
file secure-copy IP_Address Username Path Filename
```

[Example 10-5](#) demonstrates the copy of traffic.pcap file from an FTD to an external computer.

Example 10-5 Command to Copy a File Securely from an FTD to a Computer

```
> file secure-copy 10.1.1.10 admin /var/tmp traffic.pcap
The authenticity of host '10.1.1.10 (10.1.1.10)' can't be established.
ECDSA key fingerprint is 71:cf:b1:17:86:78:bf:10:41:7d:60:75:87:c3:6b:f4.
Are you sure you want to continue connecting (yes/no)? yes
Password:
copy successful.
>
```

Note

You can also run the **file copy** command to transfer files over FTP protocol.

Once the .pcap file is transferred to your desired location, you can delete the original .pcap file on FTD to maintain free disk space. Use the **file delete** command from the CLI to delete a pcap file.

```
> file delete traffic.pcap
Really remove file traffic.pcap?
Please enter 'YES' or 'NO': YES
```

```
>
```

On a ASA Engine

In the previous section, you learned how to capture traffic from a Firepower engine. However, you cannot run the same command for an ASA engine. The following section describes the process to capture traffic from an ASA engine.

Steps to Capture Traffic

The following steps are used to capture traffic from an ASA engine:

Step 1. Determine the name of the interface from where you want to capture traffic.

[Example 10-6](#) shows one of the ways to identify the name of an FTD interface. In this example, you will run capture on the GigabitEthernet1/1 that is named as `INSIDE_INTERFACE`.

Example 10-6 *The nameif Command Output Shows the Interfaces with Names*

```
> show nameif
Interface                Name                Security
GigabitEthernet1/1      INSIDE_INTERFACE    0
GigabitEthernet1/2      OUTSIDE_INTERFACE   0
Management1/1           diagnostic           0
>
```

Step 2. Run the **capture** command along with the interface name. Here is the complete command line syntax:

```
capture capture_name interface int_name match protocol_name source_detail
destination_detail
```

The following command captures ICMP traffic from a single host 192.168.1.2 to any destinations. This particular capture process, labelled as *icmp_traffic*, captures traffic only from the `INSIDE_INTERFACE` interface.

```
> capture icmp_traffic interface INSIDE_INTERFACE match icmp host
192.168.1.2 any
```

[Figure 10-6](#) clarifies the difference between **capture** and **capture-traffic** commands. To capture traffic from the ASA engine, use the **capture** command. The **capture-traffic** command captures the traffic from the Firepower engine.

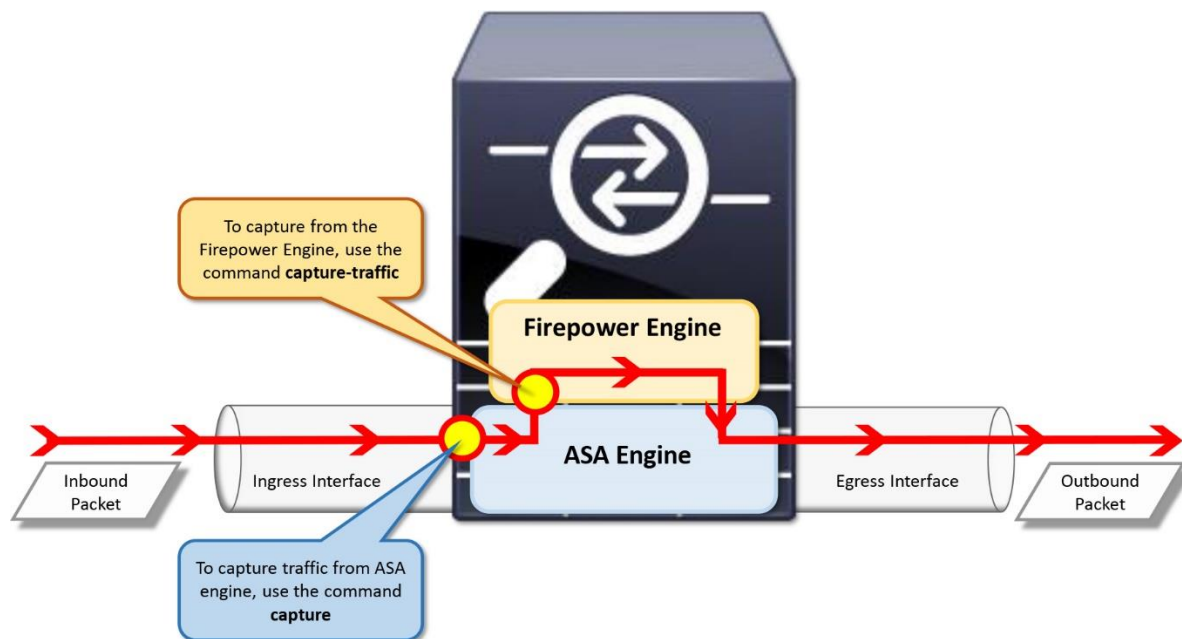


Figure 10-6. *Difference between the Application of **capture** and **capture-traffic** Tools*

Step 3. After you enter the **capture** command, run some ping tests through the FTD. Once the test traffic goes through, you can view them by running the **show capture** command on the FTD.

[Example 10-7](#) confirms that the condition within *icmp_traffic* capture process is matching and capturing traffic. You can view the captured traffic on-demand basis.

Example 10-7 *Viewing of Captured Traffic*

! Run the following command to view the condition within a capture process.

```
> show capture
capture icmp_traffic type raw-data interface INSIDE_INTERFACE [Capturing -
1140 bytes]
  match icmp host 192.168.1.2 any
>
```

! Run the following command to view the captured traffic for a particular matching condition.

```
> show capture icmp_traffic
```

6 packets captured

```
1: 05:47:38.406457      192.168.1.2 > 172.16.1.2: icmp: echo request
2: 05:47:38.407205      172.16.1.2 > 192.168.1.2: icmp: echo reply
3: 05:47:39.407617      192.168.1.2 > 172.16.1.2: icmp: echo request
4: 05:47:39.408258      172.16.1.2 > 192.168.1.2: icmp: echo reply
5: 05:47:40.408731      192.168.1.2 > 172.16.1.2: icmp: echo request
6: 05:47:40.409478      172.16.1.2 > 192.168.1.2: icmp: echo reply
```

```
6 packets shown
>
```

Step 4. The *icmp_traffic* capture process keeps growing as it matches more ICMP traffic. You can remove any previous captures and start capturing similar traffic by using the **clear** command. When you want to stop capturing completely, use the **no capture** command as the following example.

[Example 10-8](#) shows how to clear the packets from an existing capture process, as well as how to stop capturing traffic.

Example 10-8 *Deletion of a Capture*

! Run the following command to remove the previous captures.

```
> clear capture /all
>
```

! The following command confirms that all of the previously captured packets are cleared.

```
> show capture icmp_traffic
```

```
0 packet captured
0 packet shown
>
```

! To stop capturing any traffic that might match the *icmp_traffic* capturing condition, run the following command:

```
> no capture icmp_traffic interface INSIDE_INTERFACE
>
```

! To confirm that a capture instance no longer runs on an interface, run the command below. Note that an interface name is no longer associated the *icmp_traffic* capture.

```
> show capture
capture icmp_traffic type raw-data [Capturing - 1140 bytes]
  match icmp host 192.168.1.2 any
>
```

! To delete the *icmp_traffic* capture instance, run the following command:

```
> no capture icmp_traffic
>
```

! Now, if you try again, it ends with an error as the capture itself is deleted.

```
> show capture icmp_traffic
ERROR: Capture <icmp_traffic> does not exist
>
```

Download a PCAP File for Offline Analysis

You can download a capture from an ASA engine to your desktop, save it as a .pcap file, and retrieve it using a packet analyzer tool for further analysis. Instead of simple ICMP traffic, let's learn how to capture TCP traffic this time, and download the capture on your desktop. Later in this section, you can view the full TCP handshakes of an HTTP session.

Step 1. First, create a capture for the `INSIDE_INTERFACE` that will match any HTTP traffic (TCP port 80).

```
> capture http_traffic interface INSIDE_INTERFACE match tcp any any eq 80
```

Step 2. Go to a website using your browser. If the host computer is unable to access a website, check if the host is able to communicate with the `INSIDE_INTERFACE`.

Step 3. After you access a website successfully, check the status of the capture on the FTD.

[Example 10-9](#) confirms that the FTD is currently capturing HTTP traffic on the `INSIDE_INTERFACE`.

Example 10-9 Condition to Match the HTTP Traffic

```
> show capture
capture http_traffic type raw-data interface INSIDE_INTERFACE [Capturing -
5777 bytes]
  match tcp any any eq www
>
```

[Example 10-10](#) shows 15 packets that are captured by an FTD using the `http_traffic` matching condition. The capture demonstrates a complete TCP handshake process. Note the SYN, SYN-ACK, and ACK at the beginning of the session.

Example 10-10 Capture of HTTP Traffic through an FTD

```
> show capture http_traffic

15 packets captured

  1: 09:19:38.442726      192.168.1.2.58808 > 172.16.1.2.80: S
1558097726:1558097726(0) win 29200 <mss 1460,sackOK,timestamp 4644956
0,nop,wscale 7>
  2: 09:19:38.444007      172.16.1.2.80 > 192.168.1.2.58808: S
1776867665:1776867665(0) ack 1558097727 win 28960 <mss
1380,sackOK,timestamp 6329332 4644956,nop,wscale 7>
  3: 09:19:38.444129      192.168.1.2.58808 > 172.16.1.2.80: . ack
1776867666 win 229 <nop,nop,timestamp 4644956 6329332>
  4: 09:19:38.444267      192.168.1.2.58808 > 172.16.1.2.80: P
1558097727:1558098163(436) ack 1776867666 win 229 <nop,nop,timestamp
4644956 6329332>
  5: 09:19:38.444999      172.16.1.2.80 > 192.168.1.2.58808: . ack
1558098163 win 235 <nop,nop,timestamp 6329332 4644956>
  6: 09:19:38.446601      172.16.1.2.80 > 192.168.1.2.58808: .
1776867666:1776869034(1368) ack 1558098163 win 235 <nop,nop,timestamp
6329332 4644956>
```



```

7: 09:19:38.446616      172.16.1.2.80 > 192.168.1.2.58808: .
1776869034:1776870402(1368) ack 1558098163 win 235 <nop,nop,timestamp
6329332 4644956>
8: 09:19:38.446662      172.16.1.2.80 > 192.168.1.2.58808: P
1776870402:1776871191(789) ack 1558098163 win 235 <nop,nop,timestamp
6329332 4644956>
9: 09:19:38.446800      192.168.1.2.58808 > 172.16.1.2.80: . ack
1776871191 win 284 <nop,nop,timestamp 4644957 6329332>
10: 09:19:38.488011      192.168.1.2.58808 > 172.16.1.2.80: P
1558098163:1558098553(390) ack 1776871191 win 284 <nop,nop,timestamp
4644967 6329332>
11: 09:19:38.489354      172.16.1.2.80 > 192.168.1.2.58808: P
1776871191:1776871371(180) ack 1558098553 win 243 <nop,nop,timestamp
6329343 4644967>
12: 09:19:38.489476      192.168.1.2.58808 > 172.16.1.2.80: . ack
1776871371 win 305 <nop,nop,timestamp 4644968 6329343>
13: 09:19:43.397013      172.16.1.2.80 > 192.168.1.2.58808: F
1776871371:1776871371(0) ack 1558098553 win 243 <nop,nop,timestamp 6330570
4644968>
14: 09:19:43.397486      192.168.1.2.58808 > 172.16.1.2.80: F
1558098553:1558098553(0) ack 1776871372 win 305 <nop,nop,timestamp 4646195
6330570>
15: 09:19:43.397821      172.16.1.2.80 > 192.168.1.2.58808: . ack
1558098554 win 243 <nop,nop,timestamp 6330570 4646195>
15 packets shown
>

```

Step 4. Download these packets using a web browser. Use the following URL syntax in your browser to access the FTD. The browser should prompt you to save a .pcap file.

```
https://<IP_Address_of_FTD>/capture/<capture_name>/pcap/<capture_name>.pcap
```

For example, if the IP Address of the inside interface is 192.168.1.1, and the name of the capture is http_traffic, then enter the following URL on your browser:

```
https://192.168.1.1/capture/http_traffic/pcap/http_traffic.pcap
```

If the browser is unable to connect to the FTD, run the following command to check if the HTTP service is running:

```
> show running-config http
>
```

If this command shows no output, it indicates that the HTTP service is disabled. You need to enable it in order to access the FTD through a browser, and download a capture in .pcap file format.

[Enable HTTP Service on FTD](#)

Before you enable HTTP service on an FTD, you can optionally turn on debug. It generates a confirmation when the HTTP server starts, and thus help you to determine the status of the service.

```
> debug http 255
debug http enabled at level 255.
>
```

By deploying a new Platform Setting policy from the FMC, you can enable the HTTP service on an FTD. Here are the steps:

Step 1. Go to the **Devices > Platform Settings** page, and click on the **New Policy** button to find the **Threat Defense Settings** option.

[Figure 10-7](#) confirms that there is no current **Platform Settings** policy available. Select the **New Policy** button to find the **Threat Defense Settings** option.

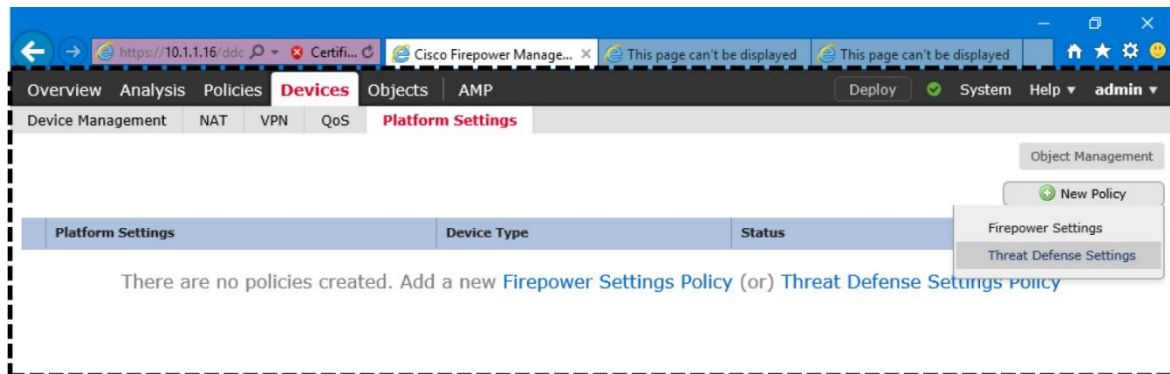


Figure 10-7. Platform Settings Page Shows the Threat Defense Settings Option

Step 2. When the **New Policy** window appears, give a name to the policy, select a device where you want to apply this new policy, and save the settings.

[Figure 10-8](#) exhibits the steps to create a new policy named *FTD Platform Settings*. FTD device is associated with the new policy.

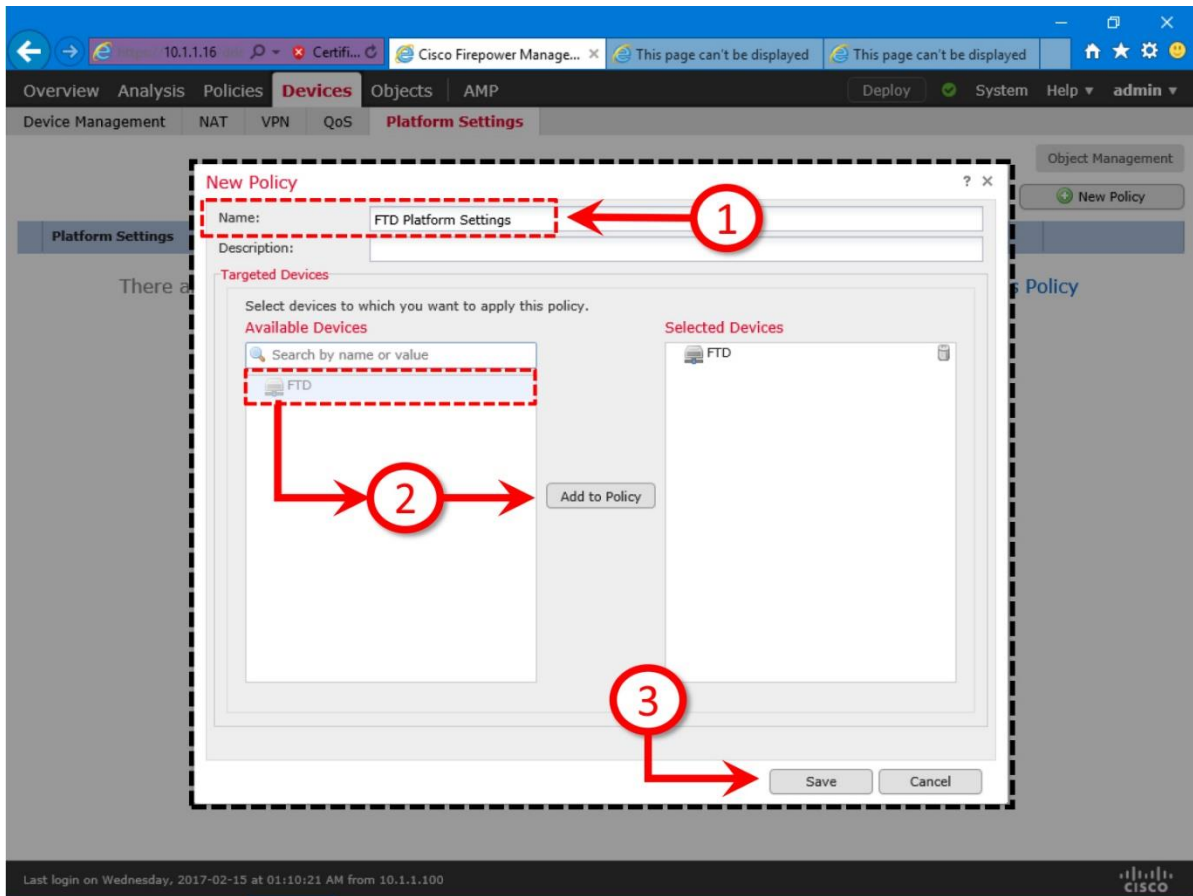


Figure 10-8. *Creating a New Platform Settings Policy*

Step 3. In the Platform Settings policy editor page, select **HTTP** from the left panel, and then select the checkbox for **Enable HTTP Server**.

Figure 10-9 shows the option that enables HTTP service through port 443.

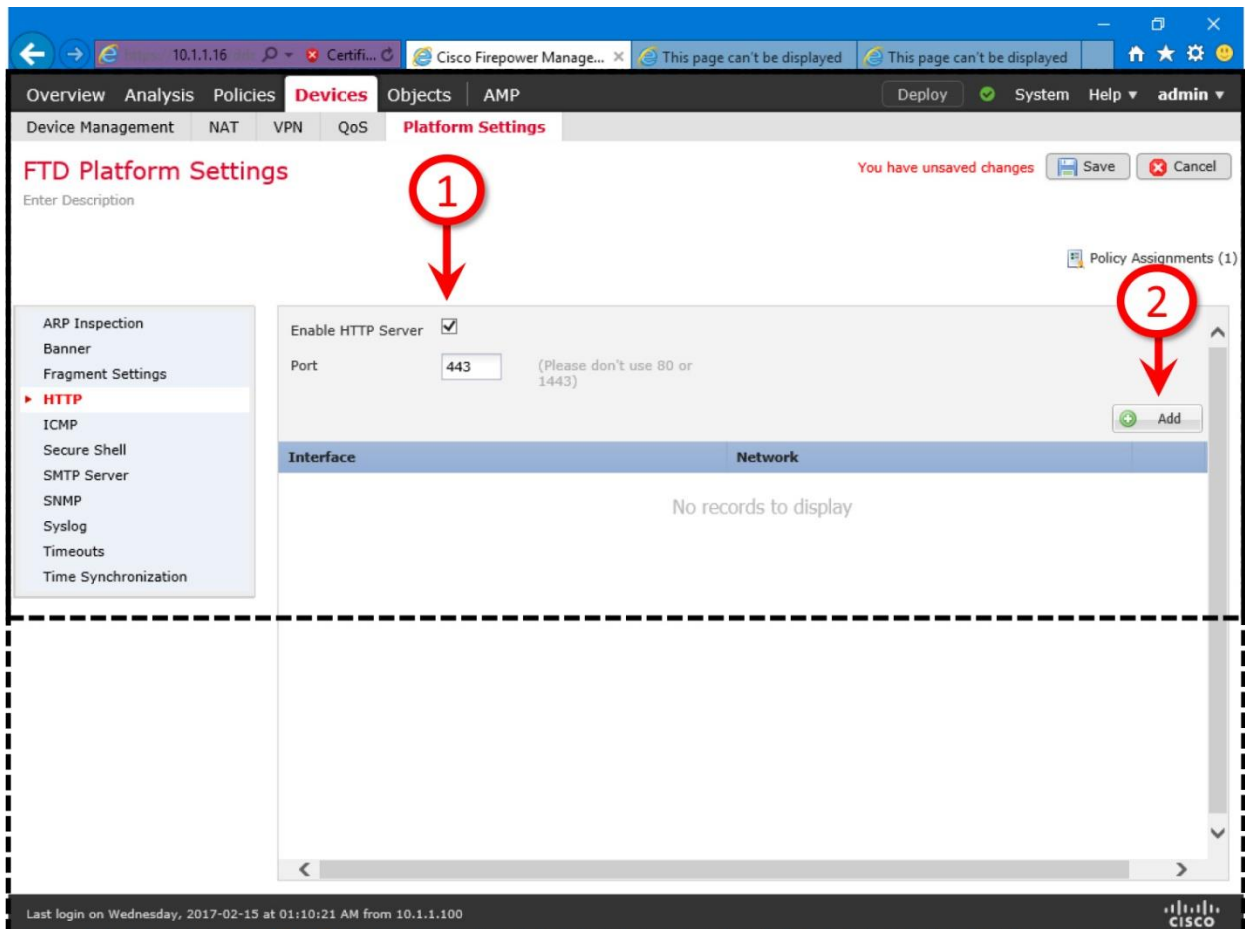


Figure 10-9. HTTP Service Enablement Page

Step 4. Click the **Add** button. The **Add HTTP Configuration** window appears. Select zones and IP addresses that are allowed to access the HTTP service on FTD.

Figure 10-10 defines that you can access the FTD web service if a host is from 192.168.0.0/16 network, and connected to INSIDE_ZONE interface.

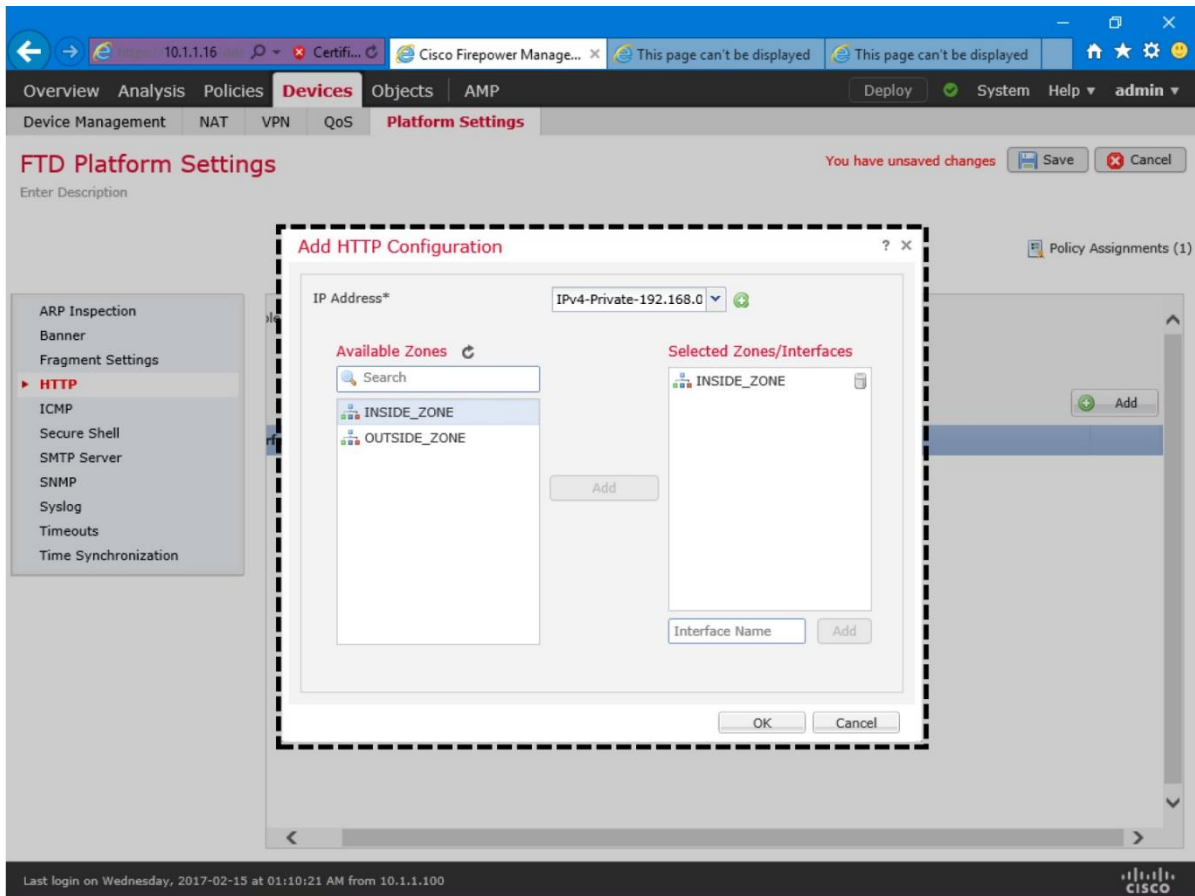


Figure 10-10. HTTP Server Configuration Page

Step 5. Press **OK** to return to the policy editor page. You should now see the zone and IP address you have just selected. Click the **Save** button to save the changes, and use the **Deploy** button to commit changes on your FTD.

[Figure 10-11](#) shows the configuration for HTTP service enablement. You must save the changes, and then deploy the configuration on FTD.

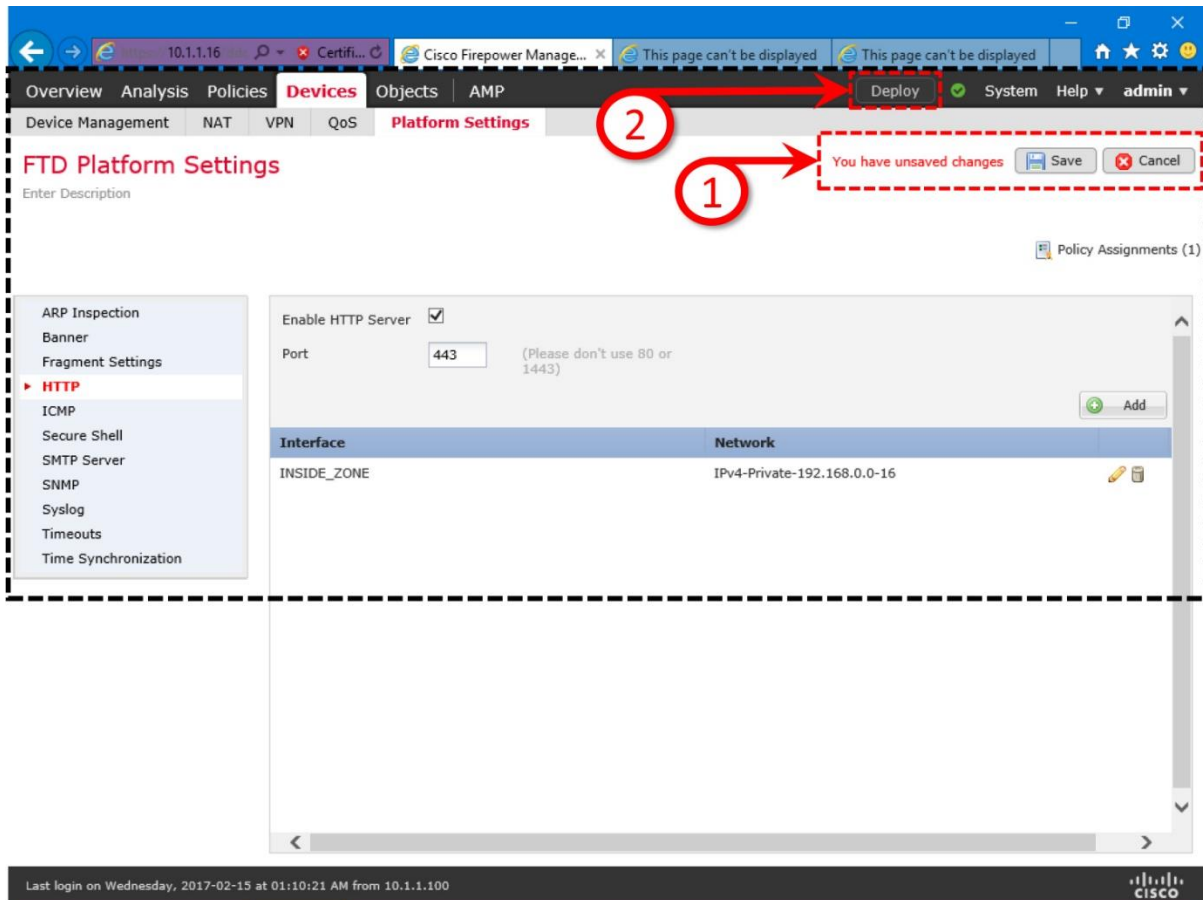


Figure 10-11. Steps to Deploy the Platform Settings with HTTP Service

You can now use the CLI to verify the deployment status. When the HTTP service starts on FTD, it generates a debug message (assuming you enabled the **debug http** already), and changes the running-configurations.

[Example 10-11](#) confirms the enablement of HTTP server. Per this configuration, users that are connected to the INSIDE_INTERFACE are able to access the FTD using a browser if the requests originate from the 192.168.0.0/16 network.

Example 10-11 Verification of HTTP Server Configuration on FTD

! As soon as the HTTP service starts, FTD generates the following debug message:

```
http_enable: Enabling HTTP server
HTTP server starting.
```

! To verify the current HTTP server configuration:

```
> show running-config http
http server enable
http 192.168.0.0 255.255.0.0 INSIDE_INTERFACE
>
```

After the deployment is verified, run the **undebbug all** command to disable debugging. Now, on a browser, enter the IP address of the inside interface as a URL with following syntax:

For example, if the IP address of the FTD inside interface is 192.168.1.1/24, enter this address on the URL field of a browser. For example, if the IP Address of the inside interface is 192.168.1.1, and the name of the capture is http_traffic, then enter the following URL on your browser:

```
https://192.168.1.1/capture/http_traffic/pcap/http_traffic.pcap
```

A browser, upon successful connection to the FTD, should prompt you to save the traffic.pcap file. After you save the file on your computer, you can use a third party packet analyzer tool to view the packets.

[Figure 10-12](#) shows the same HTTP traffic that you viewed earlier in this section. Previously, you viewed them on the console of your FTD. Now, you are viewing them on a third party packet analyzer — Wireshark.

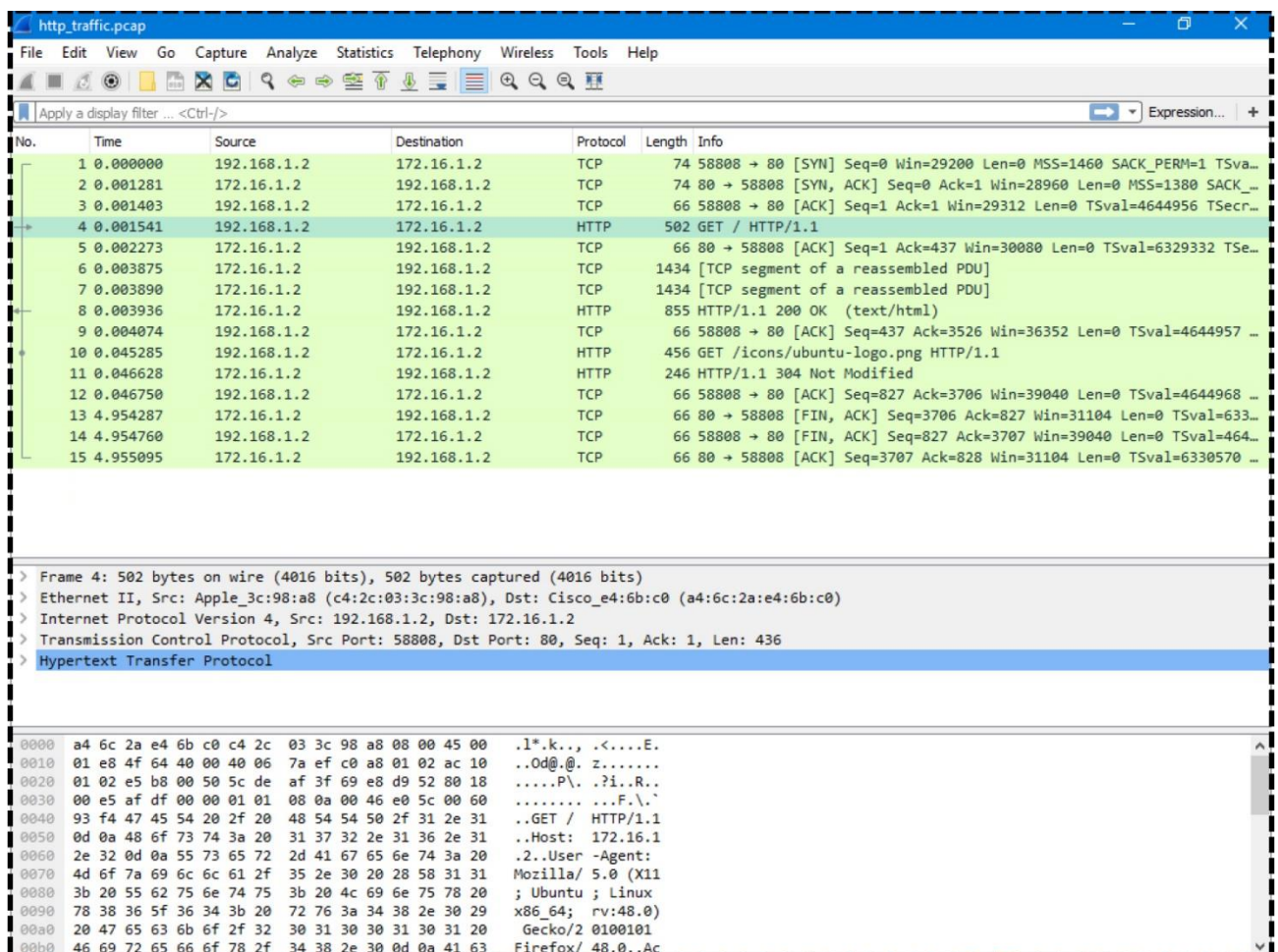


Figure 10-12. HTTP Traffic Capture on the Wireshark Packet Analyzer

Once you finish working with a packet capture, delete the rule to prevent any potential capture. It stops wasting any system resources due to a capture process.

```
> no capture http_traffic
```

On an FMC

To investigate any complicated communication issue between an FMC and FTD, analysis of the management traffic is one of the key troubleshooting tools. You cannot run the exact same commands to capture traffic on an FMC and FTD. This section describes a new different process to capture traffic from the management interface of an FMC.

Steps to Capture Traffic

First, determine the name of the FMC management interface.

[Example 10-12](#) indicates two interfaces on an FMC. The first one, eth0 with 10.1.1.16, is the management interface. The second one, lo with 127.0.0.1, is a loopback interface.

Example 10-12 Output of the ifconfig Command

```
admin@FMC:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:ED:37:B1
          inet addr:10.1.1.16  Bcast:10.1.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feed:37b1/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:99519 errors:0 dropped:0 overruns:0 frame:0
          TX packets:591461 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21356354 (20.3 Mb)  TX bytes:145518227 (138.7 Mb)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.255.255.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:79815237 errors:0 dropped:0 overruns:0 frame:0
          TX packets:79815237 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:32518661679 (31012.2 Mb)  TX bytes:32518661679 (31012.2
Mb)

admin@FMC:~$
```

Then, run the **tcpdump** command on the management interface to capture traffic. You can apply the similar BPF syntax and filtering options that you used on the Firepower engine earlier.

[Example 10-13](#) displays a capture of ICMP traffic between an FTD and FMC. The **host** options, in this example, limits the capture of traffic only from a particular host 10.1.1.2, which is an FTD. The **-i eth0** option allows the tcpdump tool to listen to only the eth0 management interface.

Example 10-13 Capture of Traffic on the eth0 Interface of an FMC

```
admin@FMC:~$ sudo tcpdump -i eth0 host 10.1.1.2
Password:
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
```



```
11:11:52.121238 IP 10.1.1.2 > FMC: ICMP echo request, id 16625, seq 1,
length 64
11:11:52.121293 IP FMC > 10.1.1.2: ICMP echo reply, id 16625, seq 1, length
64
11:11:53.121786 IP 10.1.1.2 > FMC: ICMP echo request, id 16625, seq 2,
length 64
11:11:53.121856 IP FMC > 10.1.1.2: ICMP echo reply, id 16625, seq 2, length
64
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
admin@FMC:~$
```

[Download a PCAP File for Offline Analysis](#)

To analyze a capture using a third party packet analyzer tool, you need to save the packets in a .pcap file format, and then transfer the file into your computer.

[Example 10-14](#) shows the capture of 10 packets into the traffic.pcap file. When you redirect packets into a PCAP file, it is no longer displayed into a console, thus, it reduces resource utilization.

Example 10-14 *Option to Save the Packet Capture into a PCAP File*

```
admin@FMC:~$ sudo tcpdump -i eth0 host 10.1.1.2 -w
/var/common/fmc_traffic.pcap
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96
bytes
^C
10 packets captured
10 packets received by filter
0 packets dropped by kernel
admin@FMC:~$
```

Note

To store any user generated file, use the /var/common directory on an FMC. If you save a file on this directory, FMC allows you to download it directly using the GUI.

You can use either GUI or CLI to download a packet capture. If you want to use GUI to download a .pcap file, the file should be located in the /var/common directory of an FMC.

To download a file from the FMC using its GUI, use the following the steps:

Step 1. Go to the **Health > Monitor** page, and find the FMC from the list of the appliance health status.

Step 2. Click on the FMC name. A detail view of the FMC health status appears.

Figure 10-13 shows the **Advanced Troubleshooting** button next to the name of an FMC.

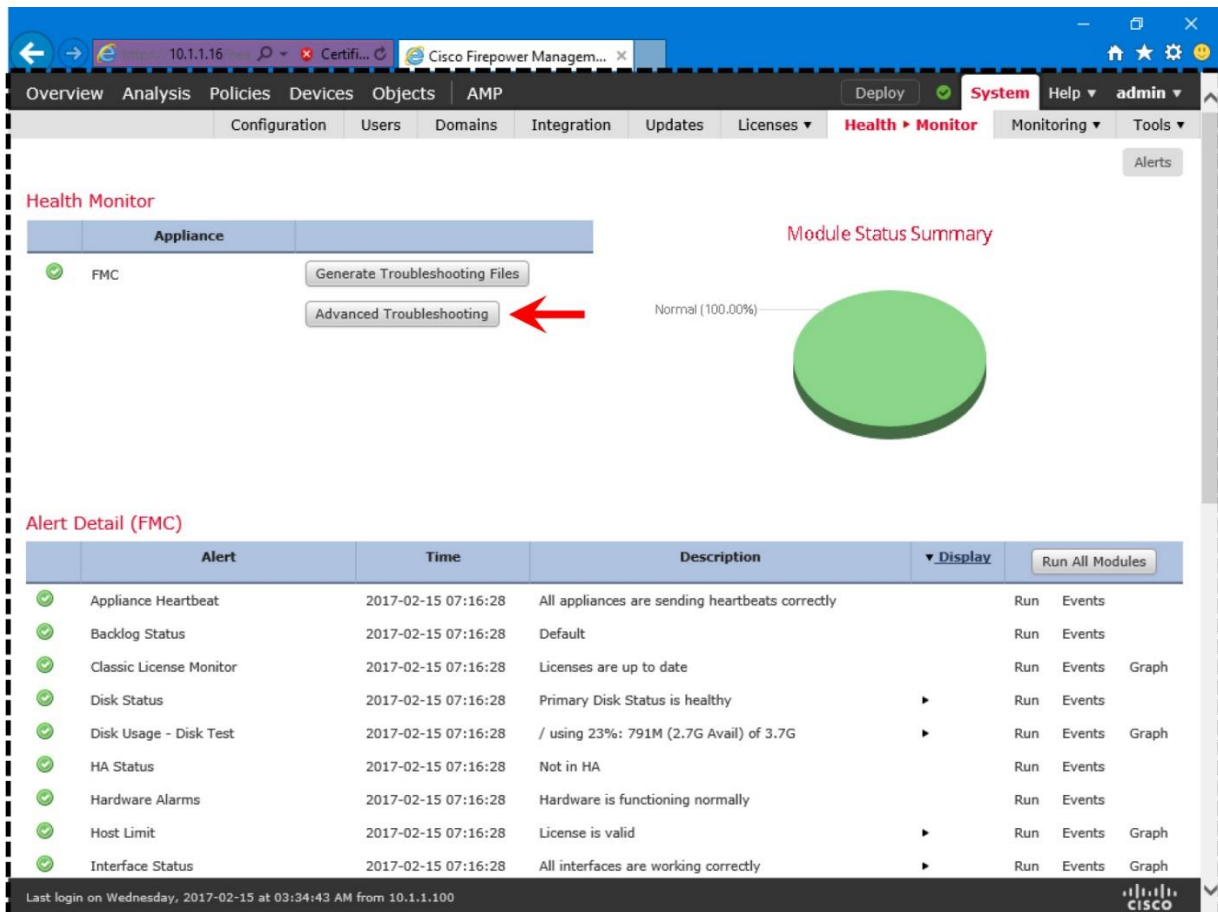


Figure 10-13. Health Module Statuses and Details of Alerts on an FMC

Step 3. Click on the **Advanced Troubleshooting** button. The **File Download** tab appears.

Step 4. Enter the name of the .pcap file (including file extension) on the **File** field.

Step 5. Select the **Download** button. The browser prompts you to save the file on your computer.

Once the .pcap file is transferred to your desired location, you can delete the original .pcap file on FMC to maintain free disk space.

Verification and Troubleshooting Tools

By deploying a simple access rule that can block ICMP traffic, you can verify how an ASA engine receives traffic from a physical interface, and then redirects it to the Firepower engine for further inspection.

Addition of an Access Rule to Block ICMP Traffic

To create a rule that can block ICMP traffic, use the following steps.

Step 1. Navigate to the **Policy > Access Control > Access Control**. A list of available Access Control policy appears.

Step 2. In the previous chapter, you created a policy called *AC Policy*. Click the pencil icon, next to the AC policy name. The policy editor page opens.

Step 3. Under the **Rules** tab, select the **Add Rule** button. The **Add Rule** window appears where you define the conditions for a rule.

Step 4. Assign a **Name** for the rule that matches with its purpose. For example, *Ping Access*. Select the **Enabled** checkbox, and **Block** from the **Action** drop-down.

Step 5. In the **Ports** tab, select **ICMP(1)** protocol as the destination port.

[Figure 10-15](#) exhibits the addition of an access rule named *Ping Access*. The rule is created to match ICMP traffic from any source.

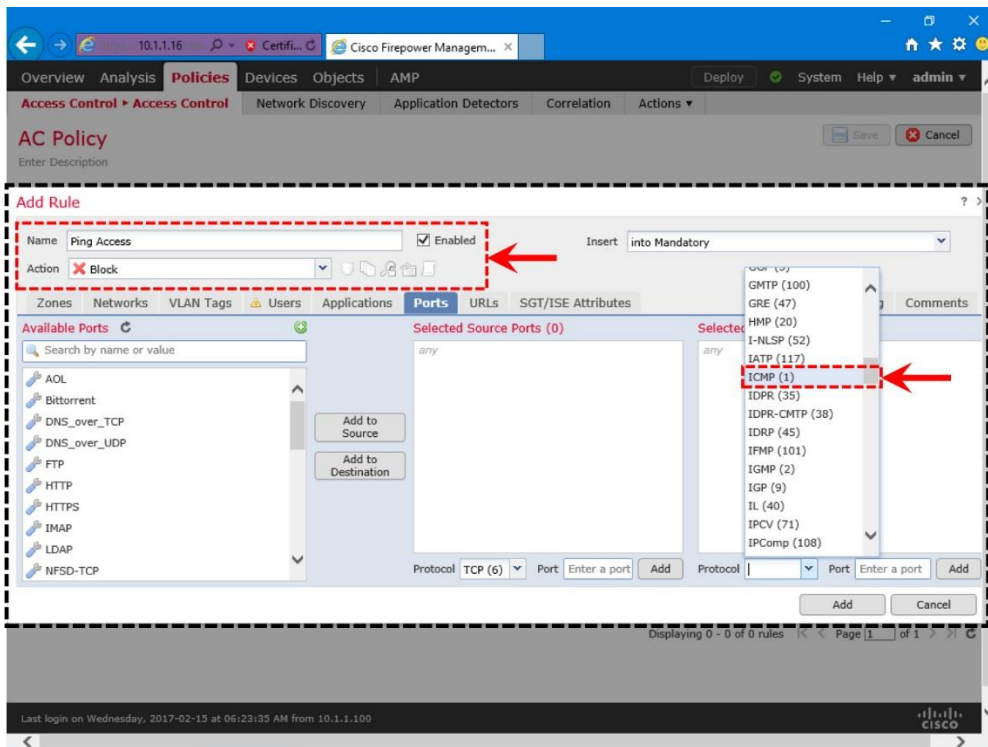


Figure 10-15. Creation of an Access Rule with Block Action

Step 6. In the **Logging** tab, select **Log at Beginning of Connection**. Send the connection events to the **Event Viewer** to view them on the GUI of the FMC.

[Figure 10-16](#) shows the options to enable logging — this optional step generates events and displays them on the FMC when this particular access rule, *Ping Access*, blocks any ICMP traffic.

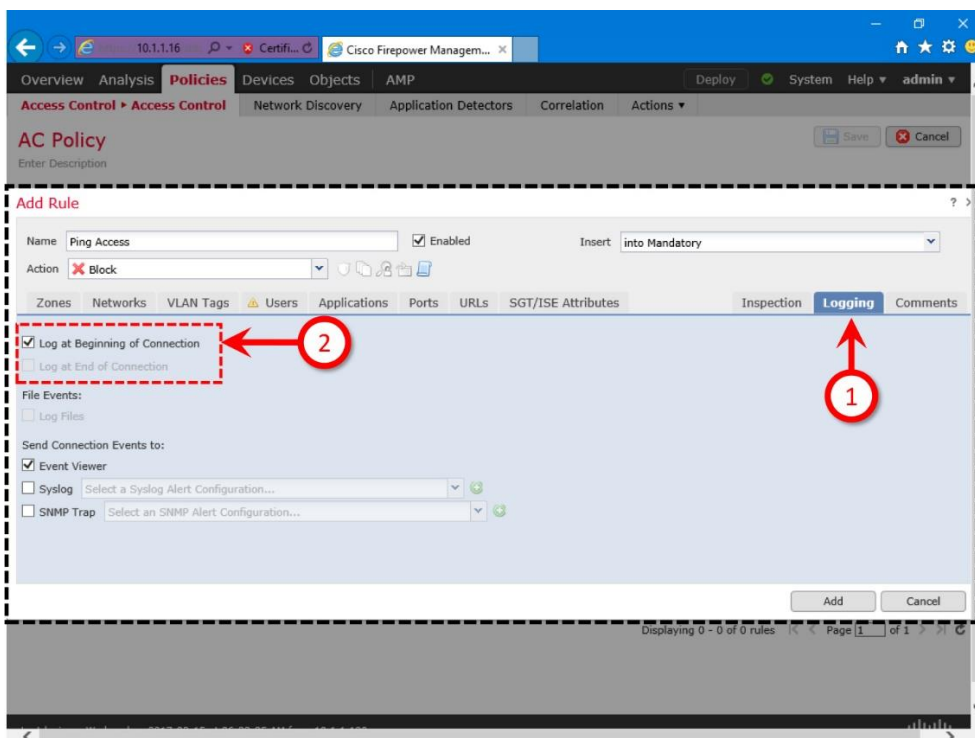


Figure 10-16. *Enablement of Logging for an Access Rule*

Step 7. That's all. Select the **Add** button to create the *Ping Access* rule. You will return to the policy editor page. Select the **Save** button to store all the changes. Finally, use the **Deploy** button to apply the new Access Control policy on the FTD.

[Figure 10-17](#) displays the final view of the access control policy editor page. Since the **Default Action** is set to **Balanced Security and Connectivity**, any non-malicious traffic except the ICMP traffic is permitted by this access control policy.

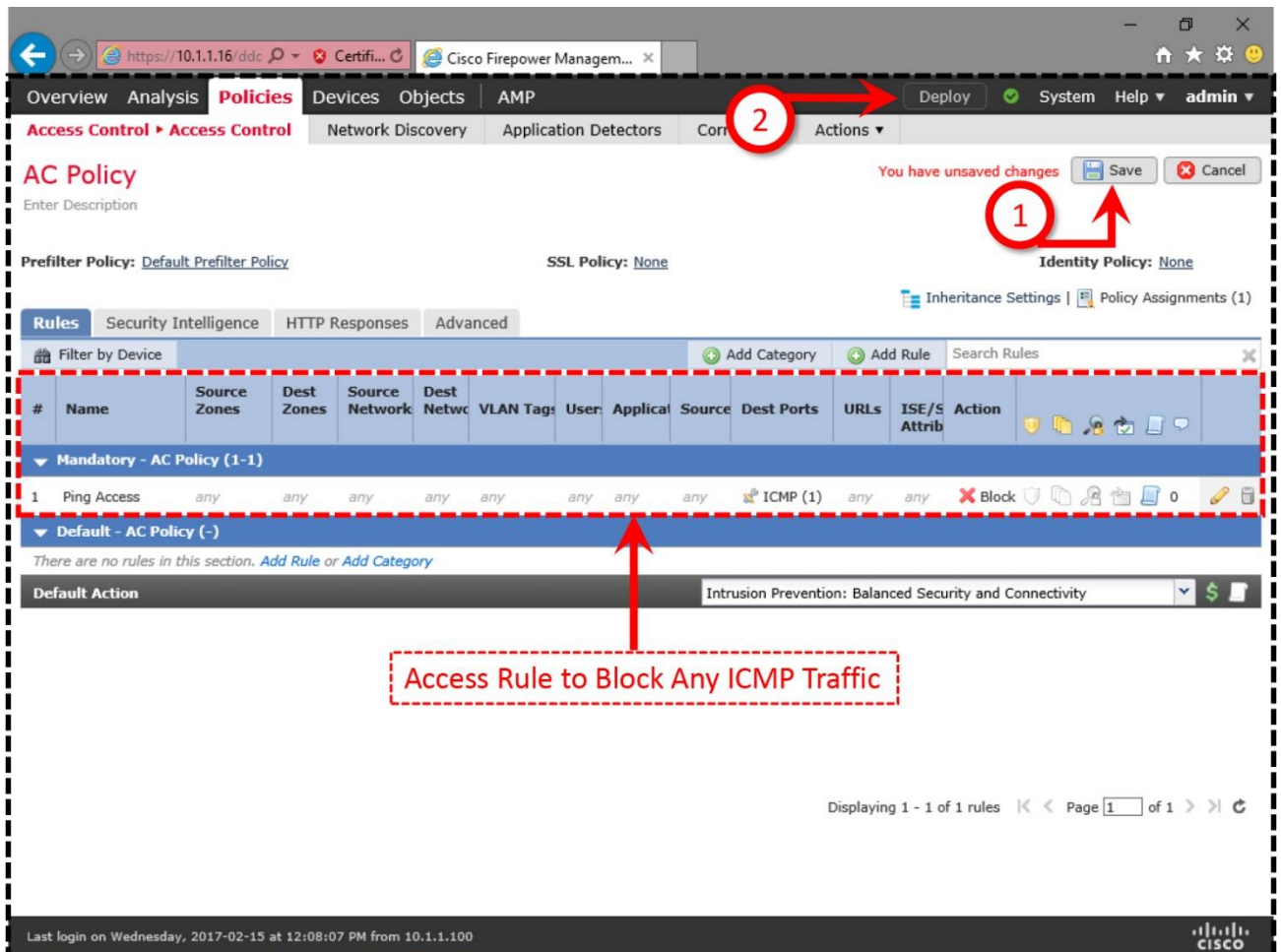


Figure 10-17. *Access Control Policy to Block Only ICMP Traffic and Permit Others*

Analysis of the Traffic Flow Using a Block Rule

Right after you hit the **Deploy** button, start sending ICMP requests from an inside host to the outside network. At the beginning, both ASA and Firepower engines are able to see the ICMP echo-requests and echo-replies. As soon as the new ICMP rule is activated on the FTD, the ASA engine begins to see the echo requests only, but no echo replies are received.

[Example 10-16](#) exhibits the behavior after a new Access Control Policy with ICMP block rule is deployed. The ASA engine stops seeing any ICMP replies because the requests could not even reach the outside network.

Example 10-16 *Capture on ASA Engine during the Deployment of an ICMP Block Rule*

```
> capture icmp_traffic interface INSIDE_INTERFACE match icmp any any

> show capture icmp_traffic

20 packets captured

  1: 16:39:55.255159      172.16.1.2 > 192.168.1.2: icmp: echo reply
  2: 16:39:56.255769      192.168.1.2 > 172.16.1.2: icmp: echo request
  3: 16:39:56.256548      172.16.1.2 > 192.168.1.2: icmp: echo reply
  4: 16:39:57.257127      192.168.1.2 > 172.16.1.2: icmp: echo request
  5: 16:39:57.257753      172.16.1.2 > 192.168.1.2: icmp: echo reply
  6: 16:39:58.258333      192.168.1.2 > 172.16.1.2: icmp: echo request
  7: 16:39:58.259019      172.16.1.2 > 192.168.1.2: icmp: echo reply
  8: 16:39:59.259630      192.168.1.2 > 172.16.1.2: icmp: echo request
  9: 16:39:59.260286      172.16.1.2 > 192.168.1.2: icmp: echo reply
 10: 16:40:00.260835      192.168.1.2 > 172.16.1.2: icmp: echo request
 11: 16:40:00.262315      172.16.1.2 > 192.168.1.2: icmp: echo reply
 12: 16:40:01.262971      192.168.1.2 > 172.16.1.2: icmp: echo request
 13: 16:40:02.273759      192.168.1.2 > 172.16.1.2: icmp: echo request
 14: 16:40:03.279663      192.168.1.2 > 172.16.1.2: icmp: echo request
 15: 16:40:04.287735      192.168.1.2 > 172.16.1.2: icmp: echo request
 16: 16:40:05.295776      192.168.1.2 > 172.16.1.2: icmp: echo request
 17: 16:40:06.303664      192.168.1.2 > 172.16.1.2: icmp: echo request
 18: 16:40:07.311919      192.168.1.2 > 172.16.1.2: icmp: echo request
 19: 16:40:08.320006      192.168.1.2 > 172.16.1.2: icmp: echo request
 20: 16:40:09.328031      192.168.1.2 > 172.16.1.2: icmp: echo request

20 packets shown
>
```

[Example 10-17](#) confirms that as soon as the new ICMP block rule is activated, the Firepower engine stops seeing any ICMP traffic.

Example 10-17 *Capture on Firepower Engine during the Deployment of an ICMP Block Rule*

```
> capture-traffic

Please choose domain to capture traffic from:
  0 - br1
  1 - Router

Selection? 1

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: icmp
16:39:57.249971 IP 192.168.1.2 > 172.16.1.2: ICMP echo request, id 12845,
seq 148, length 64
16:39:57.249971 IP 172.16.1.2 > 192.168.1.2: ICMP echo reply, id 12845, seq
148, length 64
16:39:58.249971 IP 192.168.1.2 > 172.16.1.2: ICMP echo request, id 12845,
seq 149, length 64
```

```

16:39:58.249971 IP 172.16.1.2 > 192.168.1.2: ICMP echo reply, id 12845, seq
149, length 64
16:39:59.249971 IP 192.168.1.2 > 172.16.1.2: ICMP echo request, id 12845,
seq 150, length 64
16:39:59.259965 IP 172.16.1.2 > 192.168.1.2: ICMP echo reply, id 12845, seq
150, length 64
16:40:00.259965 IP 192.168.1.2 > 172.16.1.2: ICMP echo request, id 12845,
seq 151, length 64
16:40:00.259965 IP 172.16.1.2 > 192.168.1.2: ICMP echo reply, id 12845, seq
151, length 64
.
.
^C
Caught interrupt signal
Exiting.

>

```

You have observed this behavior because of the *Ping Access* rule you deployed earlier. You can confirm this by navigating to **Analysis > Connection Events** page. You should find an event generated by the *Ping Access* rule.

[Figure 10-18](#) displays a connection event. It is generated when the ASA engine blocks the ICMP traffic using the *Ping Access* rule.

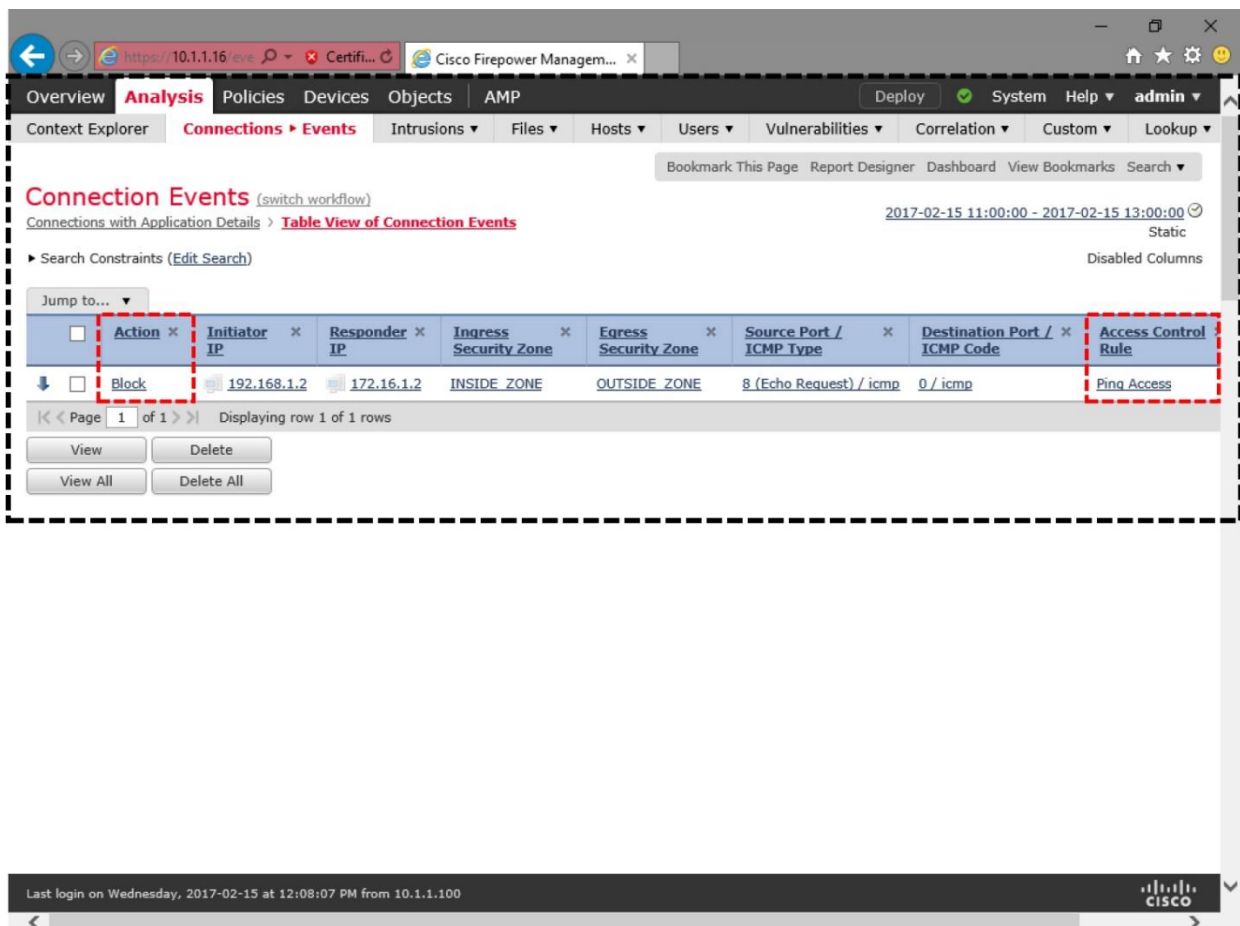


Figure 10-18. An Event with the Block Action — Triggered by the “Ping Access” Rule

[Figure 10-19](#) illustrates the behavior of the traffic flow — before and after an ICMP block rule is deployed. The Firepower engine does not see the Packet 12 in the capture, because the packet matches an access rule condition, and the ASA firewall engine blocks it.

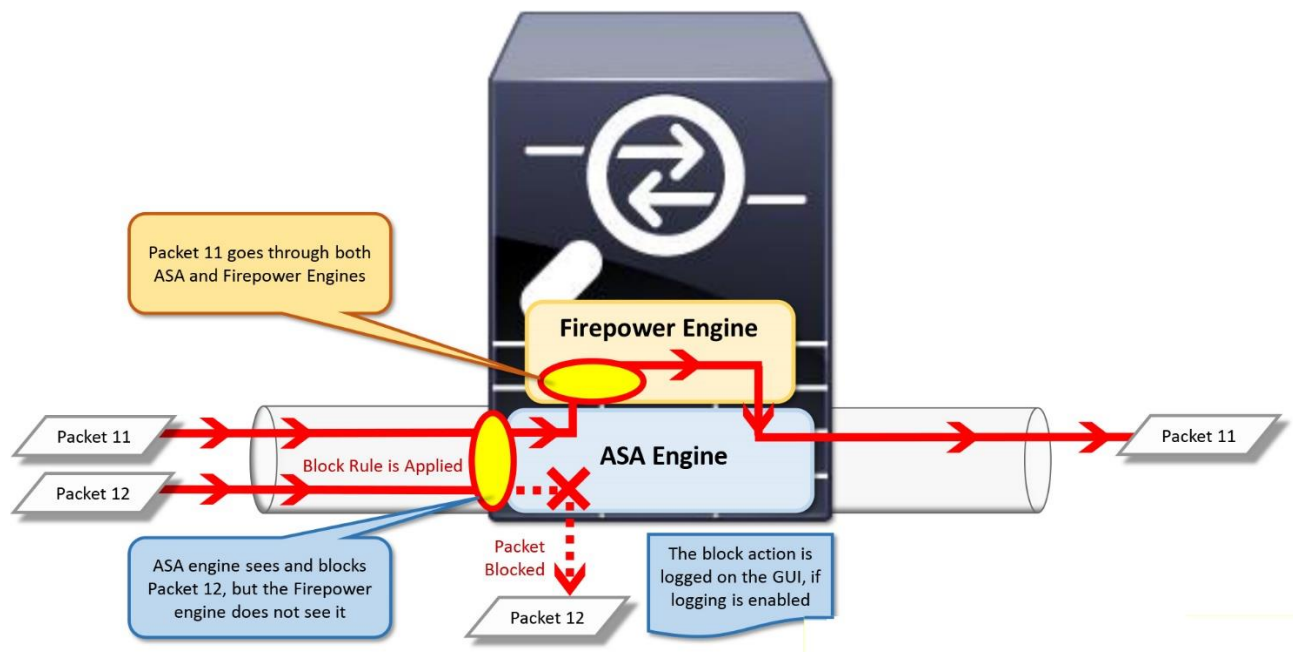


Figure 10-19. Traffic Flow — Before and After a Block Rule is Activated

Processing of Packets by an Interface

If you do not see any desired packets in the capture, make sure the filtering condition in the **capture** or **capture-traffic** command is correct. If the conditions look correct, and there is no underlying networking issues, it is important that you check the statistics of the FTD interface, and determine if any packets are dropped by the interface itself.

[Example 10-18](#) confirms that the FTD ingress interface is not dropping traffic due to the filling of the FIFO queue (**no buffer**) or the memory (**overrun**).

Example 10-18 Verification of the Packet Drops from the Interface Statistics

```
> show interface GigabitEthernet 1/1
Interface GigabitEthernet1/1 "INSIDE_INTERFACE", is down, line protocol is
down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
    Auto-Duplex, Auto-Speed
    Input flow control is unsupported, output flow control is off
    MAC address a46c.2ae4.6bc0, MTU 1500
    IP address 192.168.1.1, subnet mask 255.255.255.0
    5200 packets input, 531929 bytes, 0 no buffer
    Received 68 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 pause input, 0 resume input
    0 L2 decode drops
    2922 packets output, 2340459 bytes, 0 underruns
    0 pause output, 0 resume output
    0 output errors, 0 collisions, 0 interface resets
```

```

0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (blocks free curr/low): hardware (985/891)
output queue (blocks free curr/low): hardware (1023/997)
Traffic Statistics for "INSIDE_INTERFACE":
5153 packets input, 432852 bytes
2922 packets output, 2285241 bytes
3023 packets dropped
1 minute input rate 0 pkts/sec, 0 bytes/sec
1 minute output rate 0 pkts/sec, 0 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 0 pkts/sec, 33 bytes/sec
5 minute output rate 0 pkts/sec, 1 bytes/sec
5 minute drop rate, 0 pkts/sec

```

>

During receiving traffic, if an FTD is not fast enough in pulling the packets from its ingress interface, the interface that uses FIFO queuing algorithm becomes full. Therefore any further incoming packets get dropped. When it occurs, you can find the number of these dropped packets in the **overrun** counter.

Similarly, when an FTD has to process more traffic than a particular model is designed to handle, the FTD can run out of memory, and consequently, any incoming packets are dropped. The **no buffer** counter in an interface statistics provides the number of those dropped packets.

[Figure 10-20](#) illustrates the processing of incoming packets by an FTD. In this example, the Packet 16 is dropped due to the lack of space in the FIFO queue, and the Packet 10 is dropped due to the lack of memory or buffer.

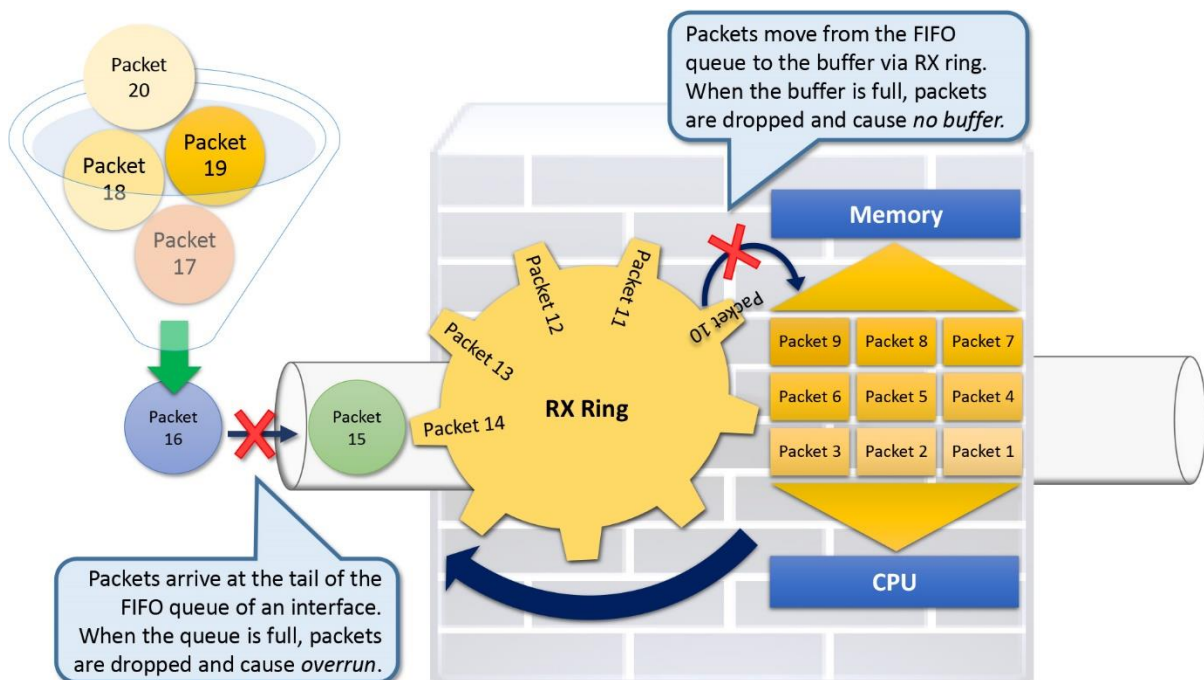


Figure 10-20. *Processing of Packets by an Ingress Interface on FTD*

Summary

This chapter describes the processes to capture live traffic on an FTD using the system-provided capturing tool. To demonstrate the benefit of the tool, this chapter utilizes various tcpdump options and BPF syntaxes to filter and manage a packet capture.

Quiz

- 1.** In terms of system performance, which of the statement about capturing traffic is true?
 - a.** When capturing traffic, always display the packets on the console to avoid system overload.
 - b.** Capturing traffic on a production system has no impact on the system performance.
 - c.** Redirecting traffic into a file can increase the utilization of resources.
 - d.** None of the above.
- 2.** Which of the filter captures HTTP client traffic only from the client host 192.168.1.2?
 - a.** src 192.168.1.2 and src port 80
 - b.** host 192.168.1.2 or src port 80
 - c.** src 192.168.1.2 and dst port 80
 - d.** host 192.168.1.2 or dst port 80
- 3.** Which option would prevent the tcpdump from oversubscribing an FTD for a long time?
 - a.** -c 10
 - b.** -e
 - c.** -vv
 - d.** -X
- 4.** In order to copy a .pcap file from an FMC to your local computer using the GUI, which of the following condition must be fulfilled?
 - a.** You must enable the HTTP service through the Platform Settings policy
 - b.** FMC must be registered with an FTD
 - c.** The .pcap file must be stored in the /var/common directory
 - d.** All of the above.

Chapter 11. Blocking of Traffic Using Inline Interface Mode

An FTD with inline interface mode is able to block unintended traffic while it remains invisible to the network hosts. However, in the [Chapter 9](#), “High Availability,” you have learned about the transparent mode that can block traffic and keeps itself transparent in the network. So, why would someone choose one over the other? Let’s explore the advantages of an inline mode over any other modes, and view a demonstration of its action followed by the detail configuration steps.

Essential Knowledge

FTD supports wide varieties of block actions, such as, simple block, block with reset, interactive block, interactive block with reset, etc. However, a block action cannot drop any suspicious packet if the interfaces are not set up properly.

[Figure 11-1](#) shows the list of actions that you can apply to an access rule. Note the different types of block action an FTD supports.

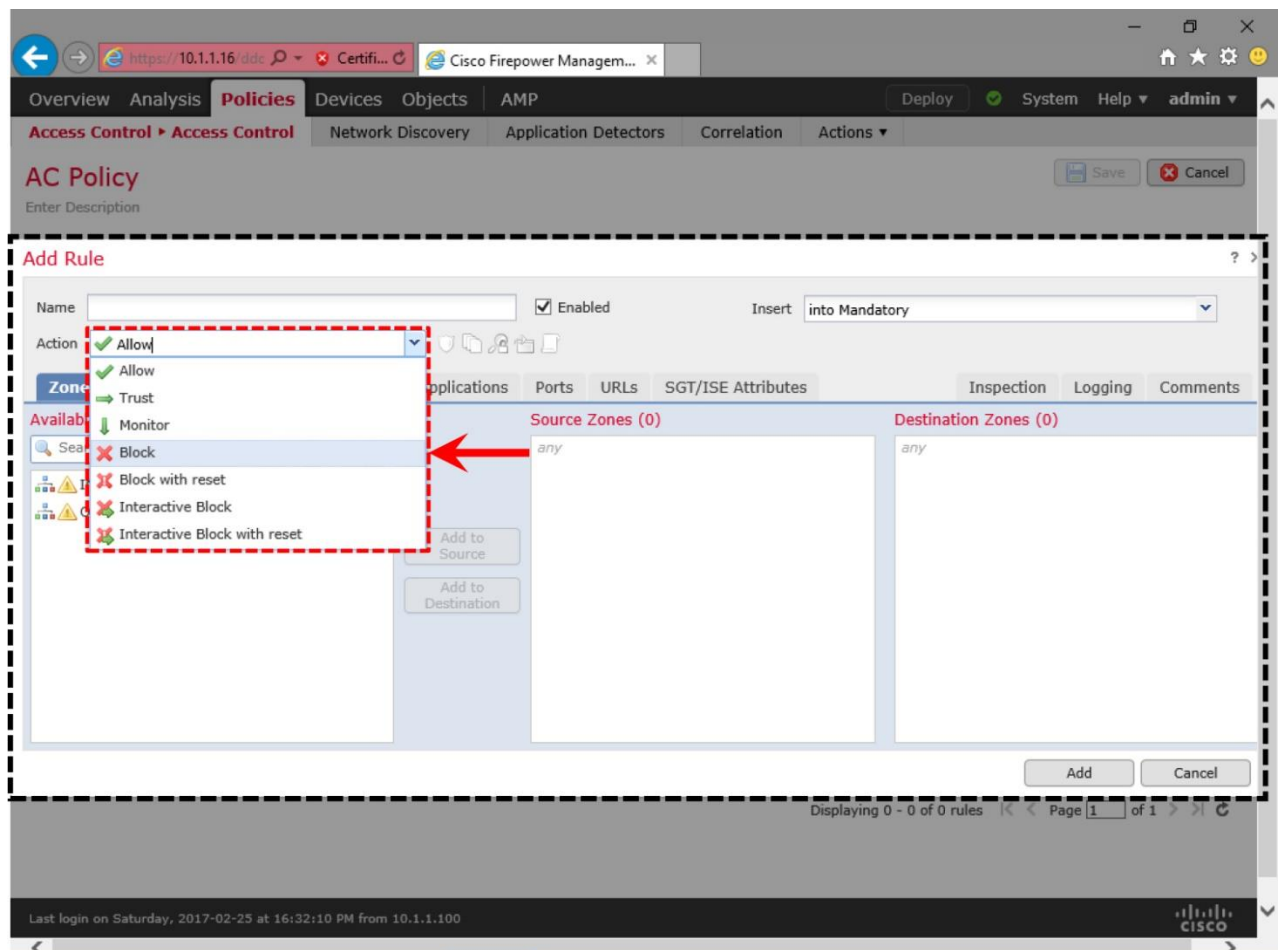


Figure 11-1. List of Available Actions

FTD allows you to choose any interface mode regardless of the underlying deployment mode — routed or transparent. However, ultimately, the capability of an interface mode defines if an FTD is going to block any suspicious traffic when it sees.

[Table 11-1](#) lists various modes of an FTD and their ability to block traffic. The deployment mode, in this table, defines how an FTD functions as a firewall. The interface mode defines how an FTD acts upon the traffic in case of any suspicious activities.

Deployment Mode	Interface Mode	Able to Block Traffic?
Routed		Yes
Transparent		Yes
	Inline	Yes
	Inline-tap	No
	Passive	No
	Passive (ERSPAN)	No

Table 11-1. Ability to Block Traffic in Various Modes

Inline vs Passive

An intrusion detection and prevention system detects suspicious activities and prevents a network from attack. You can deploy an FTD either as an intrusion detection system (IDS) or to function as an intrusion prevention system (IPS). To prevent any potential intrusion attempt in real-time, you must deploy your FTD in inline interface mode. In inline mode, the ingress and egress interfaces are bundled into an interface pair. Each pair must be associated with an inline set, which is a logical group of one or more interface pairs.

[Figure 11-2](#) illustrates how two interfaces (g1/1 with g1/2, and g1/3 with g1/4) can build the inline pairs. Note that both of the inline pairs are included in the inline set 1, in this illustration.

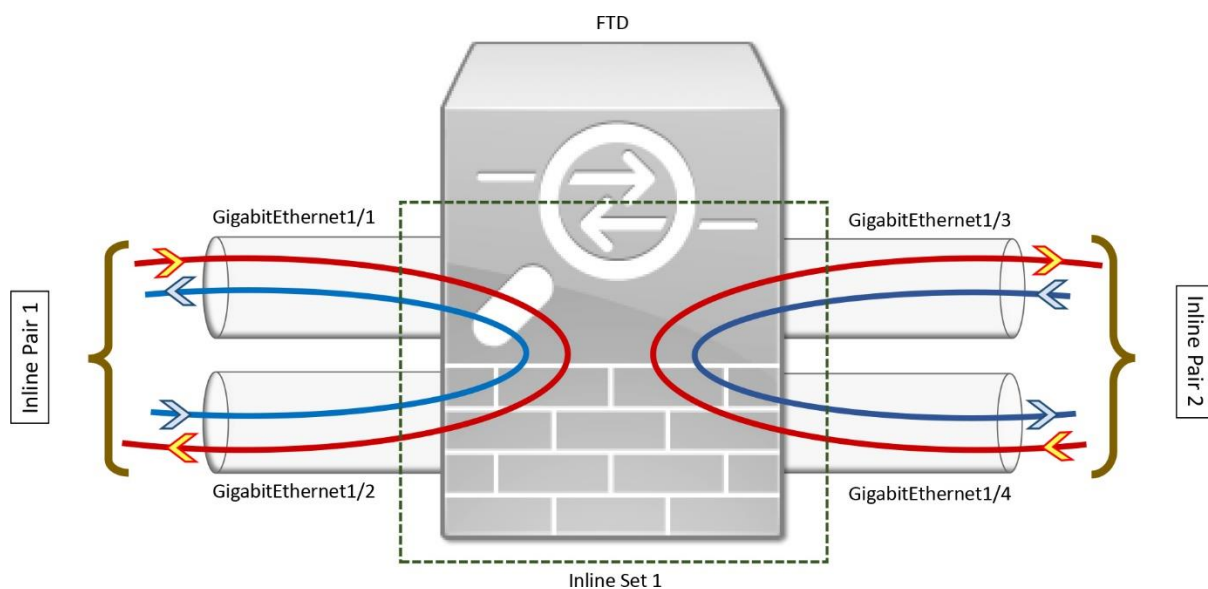


Figure 11-2. Understanding of an Inline Interface, Interface Pair, and Inline Set

An FTD in passive mode, on the contrary, can only detect intrusion attempt. A switch or tap mirrors all the packets it receives and sends a copy of the packets to the FTD using port mirroring techniques. Since the original traffic does not go through an FTD, the FTD is

unable to take any action on a packet. In other words, an FTD in passive mode cannot block any intrusion attempt; it can only detect an attempt based on the traffic it sees.

[Figure 11-3](#) provides an example of typical FTD deployment. The topology shows two FTDs devices deployed in two different modes — inline (IPS) and passive (IDS).

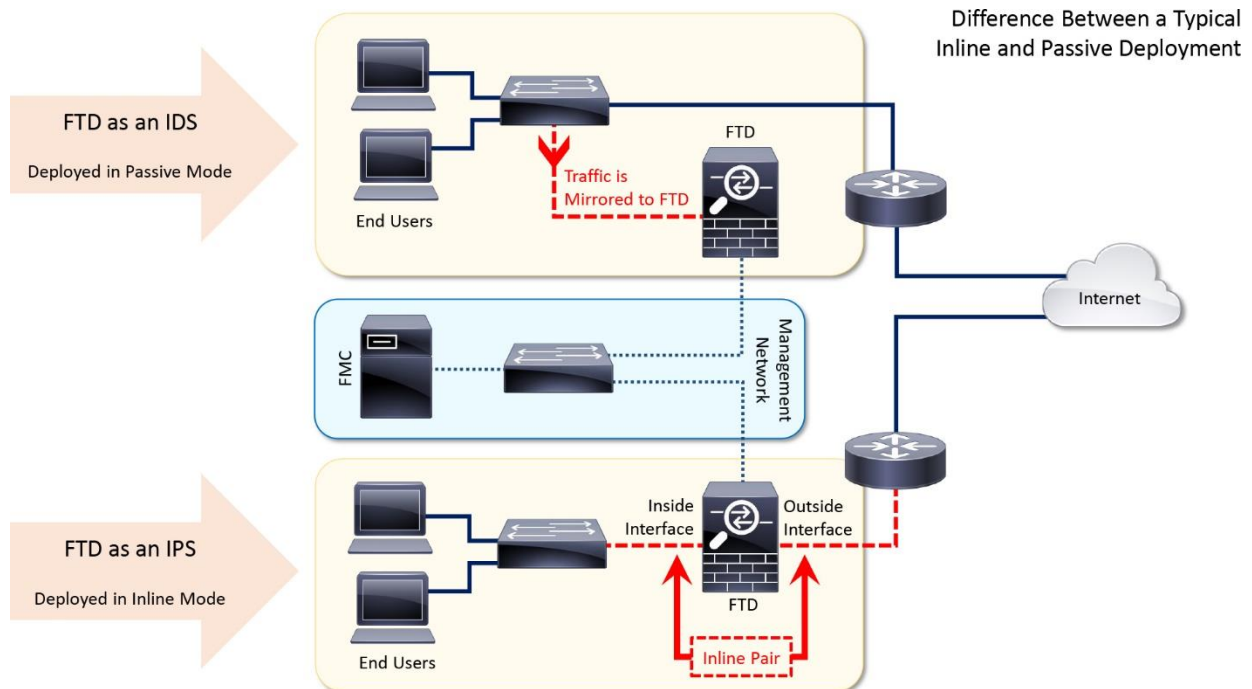


Figure 11-3. Deployment Scenarios — FTD in Inline and Passive Modes

Inline vs Transparent

Both modes — inline interface mode and transparent mode — work like a *bump in the wire*, which means they are invisible to the connected devices. However, they are two different techniques.

An FTD in transparent mode places the inside and outside networks into a virtual bridge group, and creates a layer 2 bridging network. Traffic originates from an FTD uses a Bridged Virtual Interface (BVI) as its source interface. The BVI interface, inside network, and outside network — all of them must be configured with the IP addresses from a single subnet.

In contrast, in the inline interface mode, the interfaces on an interface pair are network-agnostic. They are able to send and receive any traffic as long as the policies permit. In addition, you do not need to configure IP addresses on any of the physical interfaces or virtual interfaces.

Tracing a Packet Drop

After receiving a packet from the ingress interface, FTD processes the packets and takes an action based on the deployed access rules and intrusion rules. In the previous chapter, you have learned how to capture live traffic from an interface. In this chapter, you are going to leverage the capturing tool to trace a drop of a packet through an FTD.

[Figure 11-4](#) illustrates the potential reasons for a packet drop by an FTD. After an FTD filters traffic using its traditional firewall rules, the Firepower/Snort engine inspects traffic.

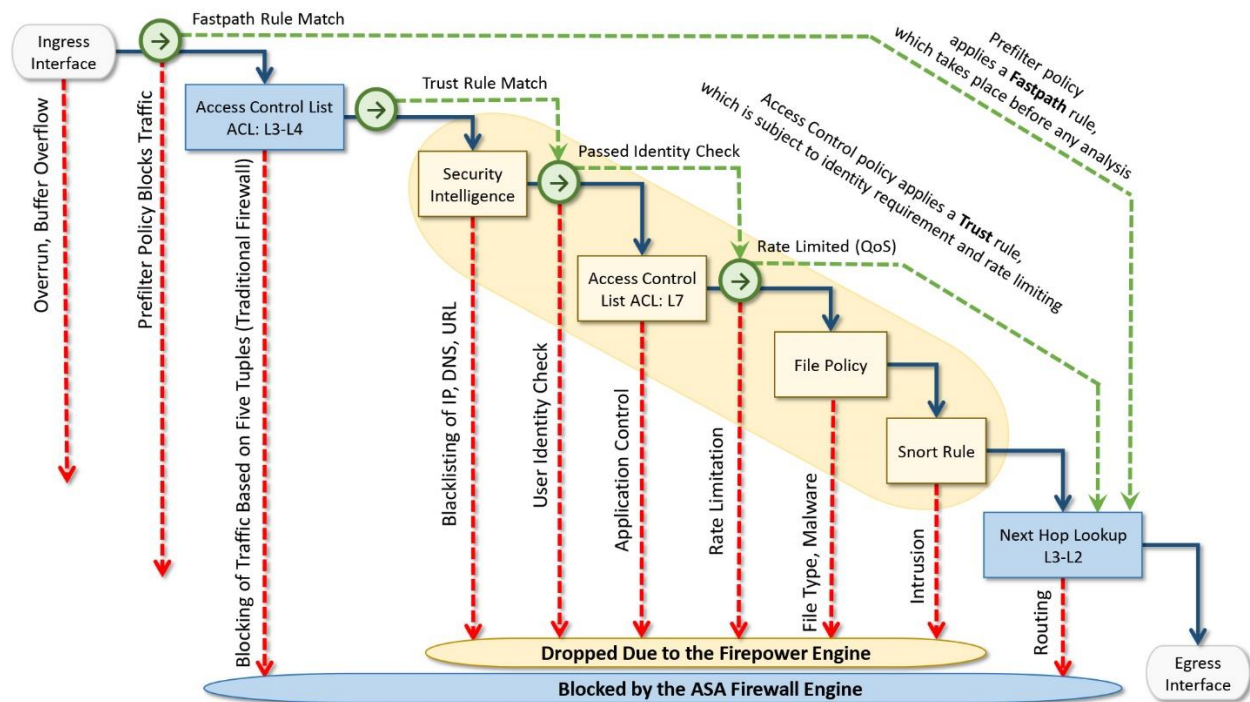


Figure 11-4. Possible Reasons for a Packet Drop

To record additional tracing data during a capture, you need to use the **trace** parameter trace with the **capture** command. For example, to capture any HTTP traffic received on an inside interface, you used the following command in [Chapter 10](#):

```
> capture http_traffic interface INSIDE_INTERFACE match tcp any any eq 80
```

Now, to capture tracing data for each packet, add the **trace** parameter as shown:

```
> capture http_traffic trace interface INSIDE_INTERFACE match tcp any any eq 80
```

To view the additional tracing data for a specific packet, add the number of that packet with trace keyword, as shown:

```
> show capture http_traffic packet-number 1 trace
```

Moreover, FTD provides a tool, called **packet-tracer**, which is able to generate simulated packets using the information of five tuples — source IP address, destination IP address, source port number, destination port number, and protocol. By considering the deployed rule conditions, this tool simulate traffic flow from ingress to egress interface, as if a client and server communicate using a network protocol through the FTD. For example,

```
> packet-tracer input INSIDE_INTERFACE tcp 192.168.1.2 10000 192.168.1.200 80
```


This command generates a virtual packet flow from the `INSIDE_INTERFACE` with the following header information:

```
Source IP Address: 192.168.1.2
Destination IP Address: 192.168.1.200
Source Port: 10000
Destination Port: 80
Protocol: TCP
```

In the *Verification* section of this chapter, you will utilize both **capture trace** and **packet-trace** tools to determine where a packet drops. For now, just keep this concept in mind.

Best Practices

When you create an inline set, consider the following items during configurations:

- If your network uses asynchronous routing, and the inbound and outbound traffic go through two different interface pairs, you should include both interface pairs into the same interface set. It ensures that FTD does not see just half of the traffic — it is able to see the flows from both directions, and recognize them when they are part of a single connection.
- Enable the failsafe feature on the inline interface set. In case of a software failure, this feature allows an FTD to continue its traffic flow through the device by bypassing the detection.
- You should allow the inline set to propagate its link state. It reduces the routing convergence time when one of the interfaces in an inline set goes down.

The configuration examples in this chapter discuss the steps to enable **failsafe** and **Propagate Link State** feature on an inline set.

Configuration

In this section, you are going to configure and verify three important elements of an inline interface:

- Creation of a simple inline set and verify traffic flow.
- Enablement of the fault tolerance features on an inline set to avoid downtime in case of a failure.
- Blocking of a particular service or port through an inline interface.

[Figure 11-5](#) provides an overview of the lab topology that is used in this chapter. The configuration examples and the command outputs are based on this topology.

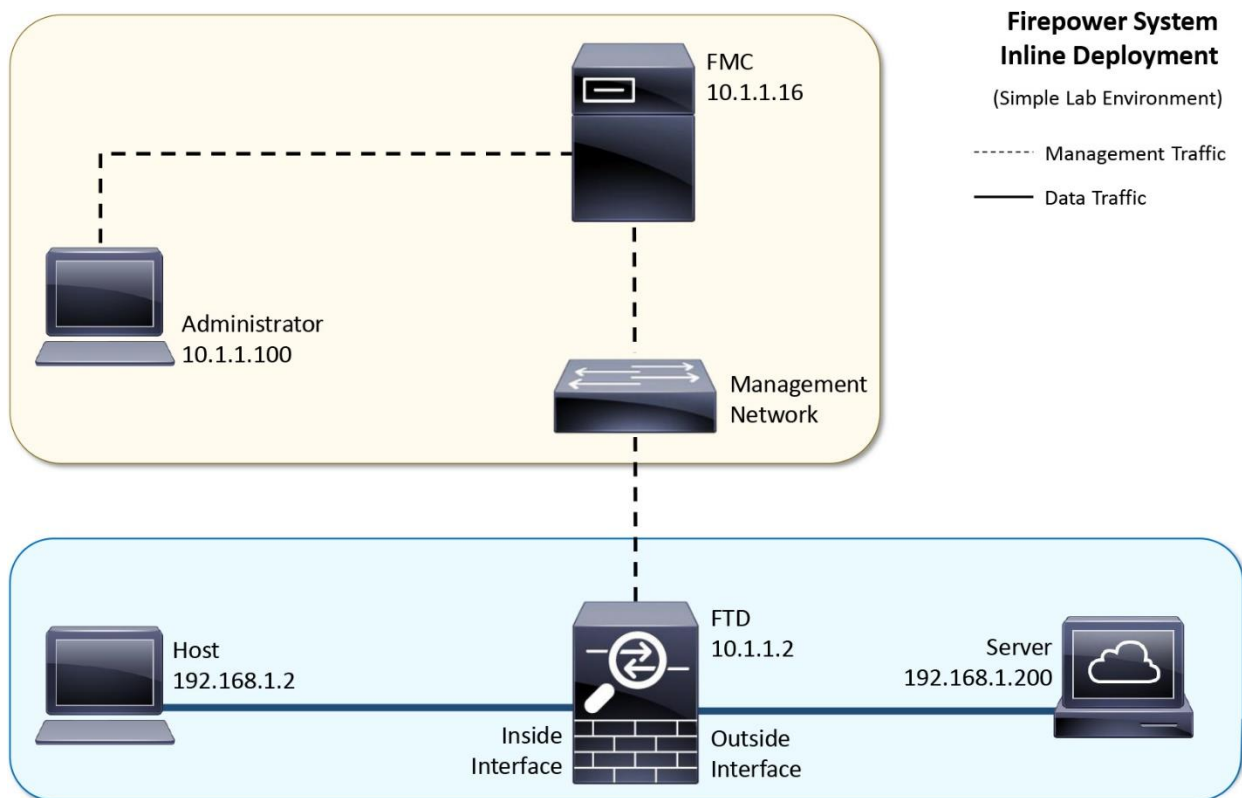


Figure 11-5. Lab Topology Used in the Configuration Examples of This Chapter

Prerequisites

If you previously configured your FTD as a firewall in routed mode, you need to remove any platform settings, IP address and DHCP server configurations from the FTD data interfaces, as they are not necessary in inline interface mode.

Creation of Inline Set

An inline set is a logical group of one or more interface pairs. Before you add an inline set, you must create an inline interface pair, and associate the pair with the inline set you want to add.

Configuration

In order to create an inline interface, use the following steps:

Step 1. Navigate to the **Devices > Device Management** page. A list of the managed devices appears.

Figure 11-6 displays the Device Management page — a page where all of the devices that are registered with an FMC are listed.

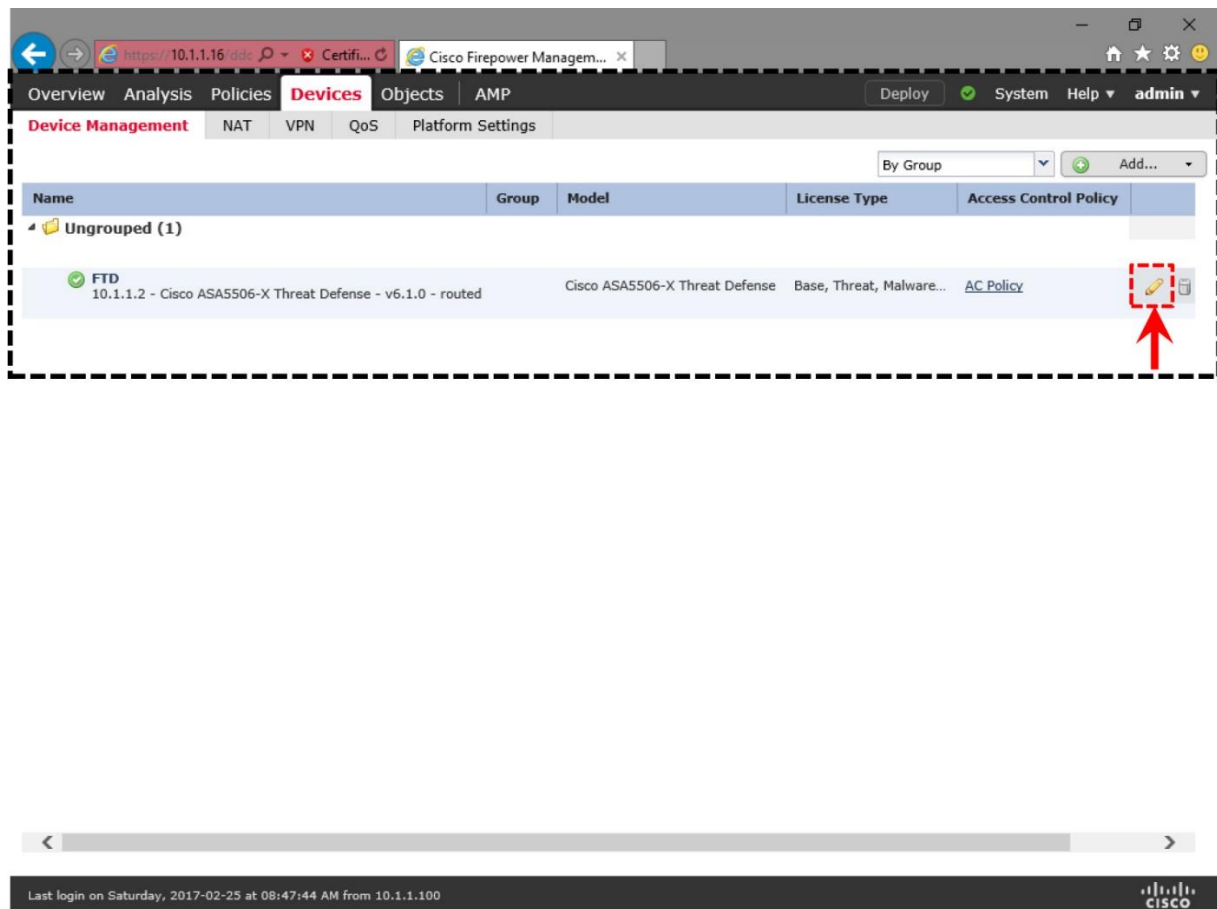


Figure 11-6. *The Device Management Page of an FMC*

Step 2. Select the **Interfaces** tab. A list of the available interfaces appears.

Step 3. Select the *pencil* icon next to the interfaces that will be part of an inline pair. In this configuration example, the GigabitEthernet1/1 and GigabitEthernet1/2 interfaces builds an inline pair.

Figure 11-7 shows the **Interfaces** tab within the device editor page. You can setup or modify interface settings using this page.

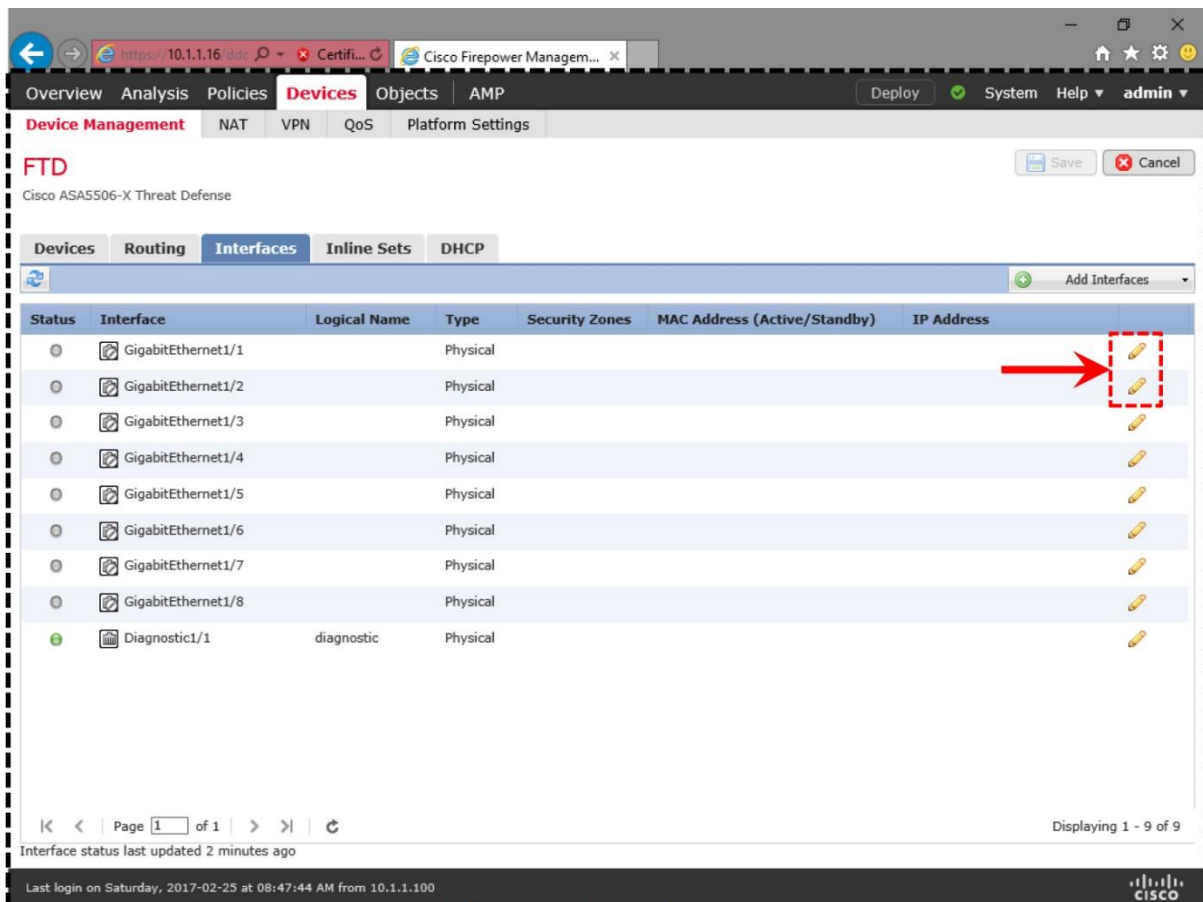


Figure 11-7. List of Available Interfaces on an FTD

Step 4. On the **Edit Physical Interface** window, the default value of the **Mode** dropdown is **None**. Keep it unchanged, as it represents the inline interface mode. Here, you just need to assign a name to the interface and enable it. An IP Address is not necessary.

Figure 11-8 shows the settings on the GigabitEthernet1/1 interface. This example uses the names INSIDE_INTERFACE and OUTSIDE_INTERFACE for the GigabitEthernet1/1 and GigabitEthernet1/2 interfaces respectively.

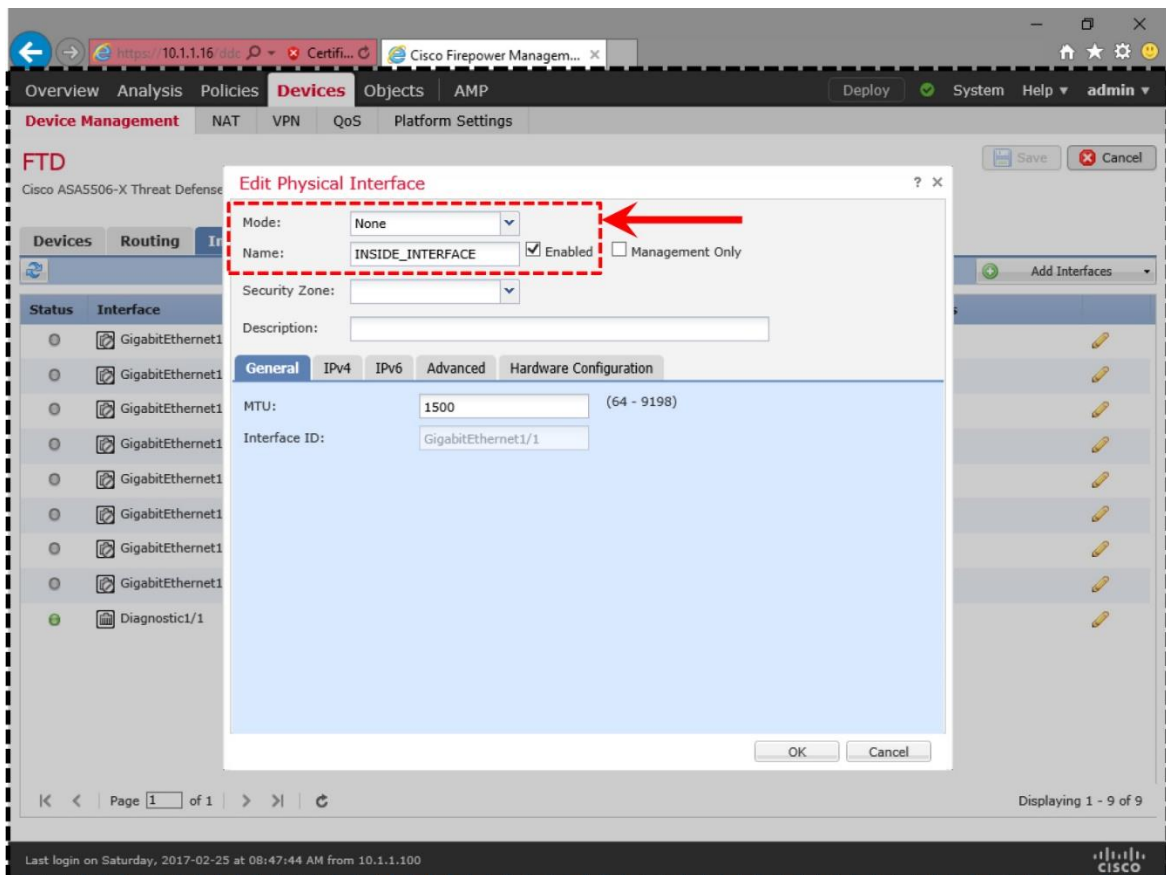


Figure 11-8. *The Edit Physical Interface Window*

Step 5. Select **OK** to return to the **Interfaces** tab. Repeat the previous step for the other interface of the pair — give a name, and enable it.

Step 6. After both interfaces are named and enabled, select the **Save** button to save the changes.

Figure 11-9 shows an overview of each interface configuration. Note that the IP address or security zone is not configured. Only the logical interface is necessary for an inline interface.

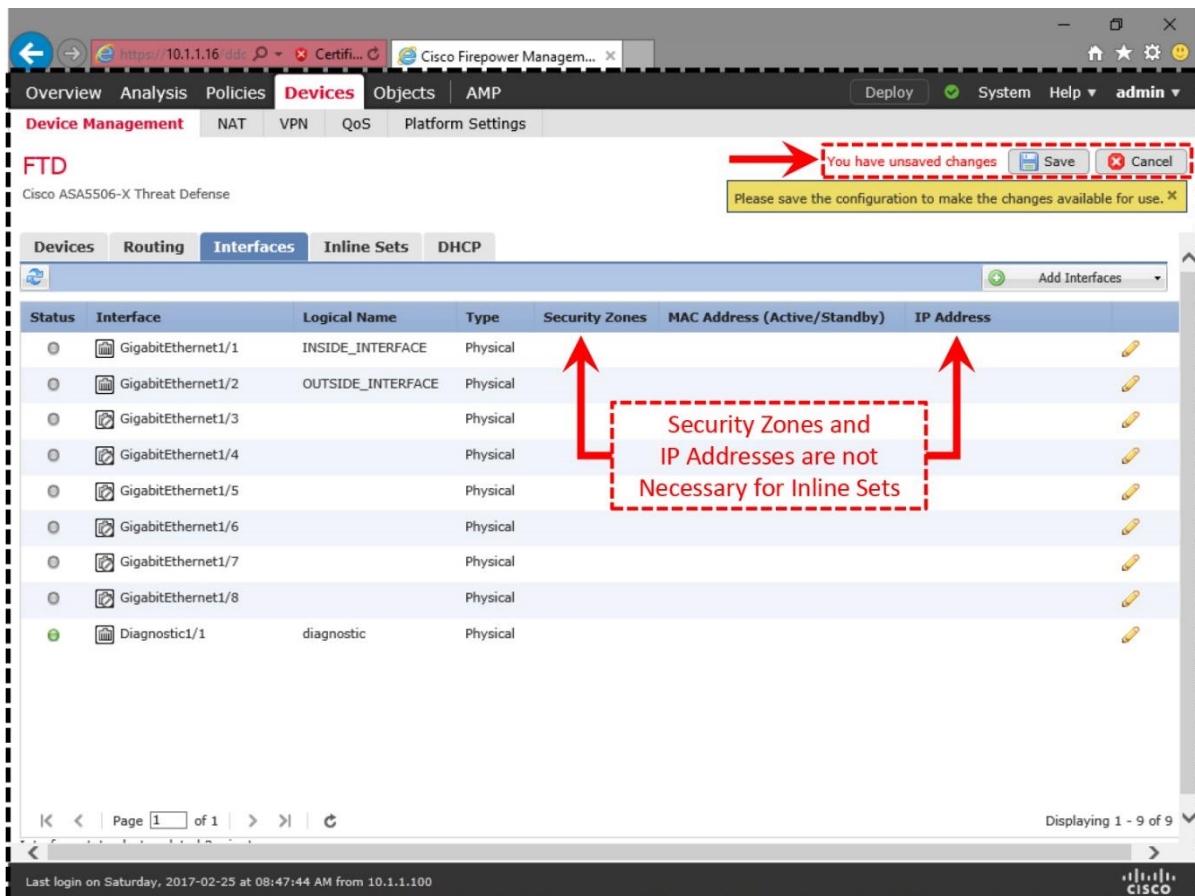


Figure 11-9. Overview of the Interface Configuration

Now, begin the second part of the configuration — adding the interface pair into an inline set by following these steps:

Step 1. On to the **Devices > Device Management** page, go to the **Inline Sets** tab and select the **Add Inline Set** button.

Step 2. On the **Add Inline Set** window, give a name to the Inline Set, select an interface pair, and add it to the Inline Set.

Note

Do not configure any additional settings at this moment. You will come back here when you will learn the fault tolerance configuration, in the next section.

[Figure 11-10](#) shows the items to configure a basic inline set —just enter a name, and select a pair.

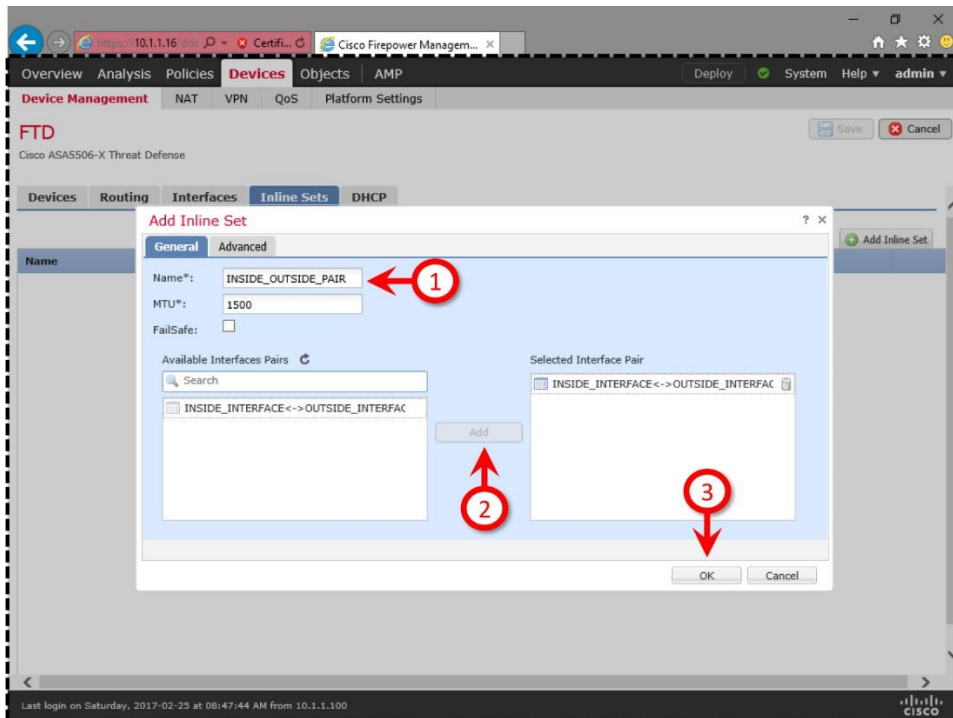


Figure 11-10. Settings of an Inline Set

Step 3. Click **OK** to return to the **Inline Sets** tab. Save the configuration, and deploy it to your FTD

[Figure 11-11](#) displays the selection of an interface pair for an inline set.

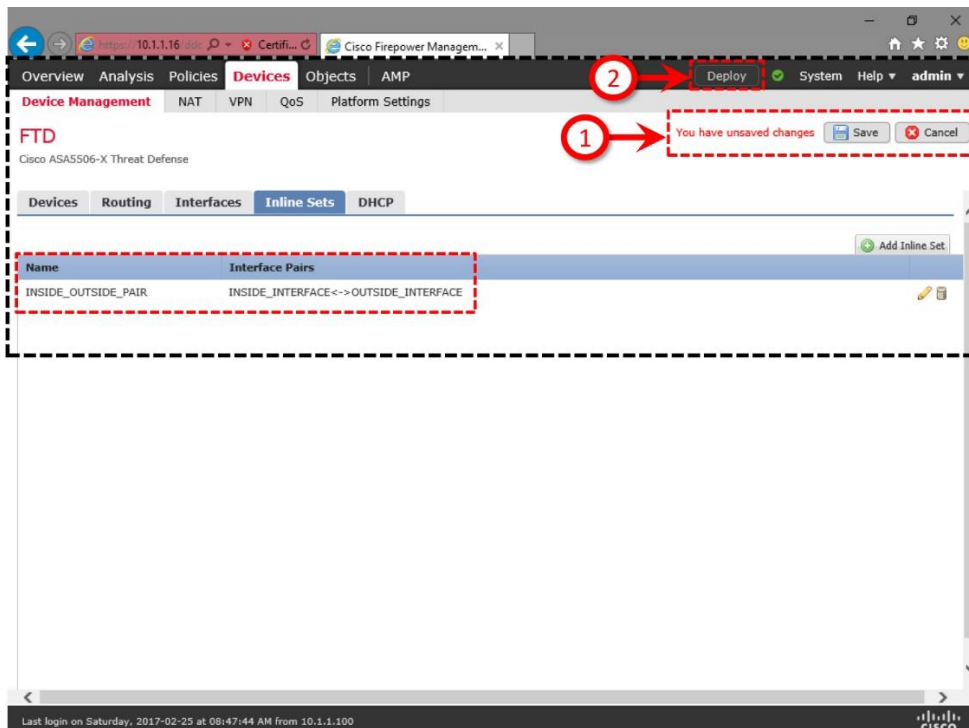
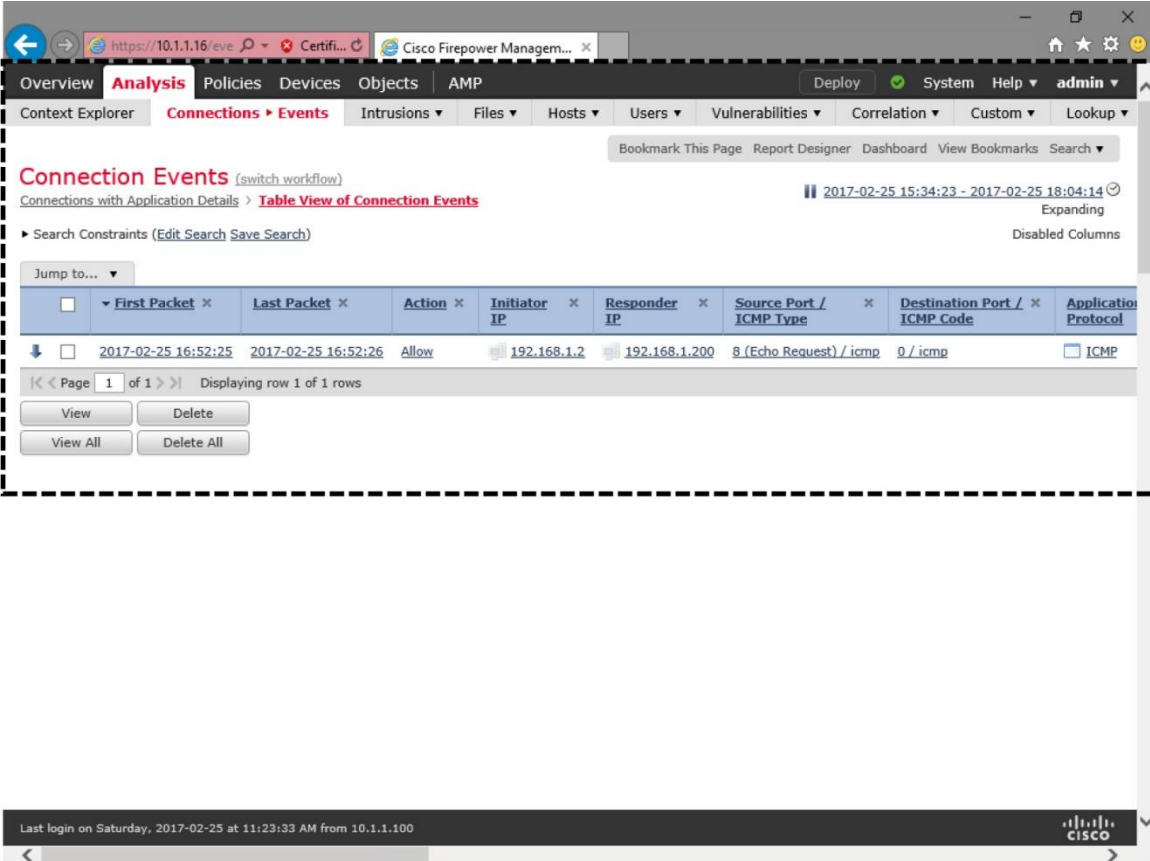


Figure 11-11. Deployment of Interface Set Configuration

Verification of the Configuration

Upon a successful deployment, you should be able to ping from your inside host 192.168.1.2 to the outside server 192.168.1.200.

[Figure 11-12](#) exhibits the table view of a connection event. The event confirms that the host 192.168.1.2 is able to send ICMP echo-requests to 192.168.1.200.



The screenshot shows the Cisco Firepower Management Center (FMC) interface. The main content area displays a table of connection events. The table has the following columns: First Packet, Last Packet, Action, Initiator IP, Responder IP, Source Port / ICMP Type, Destination Port / ICMP Code, and Application Protocol. A single row is visible, showing an event on 2017-02-25 at 16:52:25 with an 'Allow' action, initiated from 192.168.1.2 to 192.168.1.200 on port 8 (Echo Request) / icmp, with destination port 0 / icmp. The application protocol is listed as ICMP. The interface also shows navigation options like 'View', 'Delete', 'View All', and 'Delete All'.

First Packet	Last Packet	Action	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol
2017-02-25 16:52:25	2017-02-25 16:52:26	Allow	192.168.1.2	192.168.1.200	8 (Echo Request) / icmp	0 / icmp	ICMP

Figure 11-12. Connection Event for the ICMP Traffic

If a ping test fails, but the FMC does not show any reason for a failure, you begin troubleshooting by checking the interface status.

[Example 11-1](#) displays an output of the **show inline-set** command. This command provides various components of an inline set configuration, such as, member interfaces of an inline pair, their statuses and advanced settings.

Example 11-1 Status of the *INSIDE_OUTSIDE_PAIR* Inline Set

```
> show inline-set
```

```
Inline-set INSIDE_OUTSIDE_PAIR
Mtu is 1500 bytes
Failsafe mode is off
```



```

Failsecure mode is off
Tap mode is off
Propagate-link-state option is off
hardware-bypass mode is disabled
Interface-Pair[1]:
  Interface: GigabitEthernet1/1 "INSIDE_INTERFACE"
  Current-Status: UP
  Interface: GigabitEthernet1/2 "OUTSIDE_INTERFACE"
  Current-Status: UP
  Bridge Group ID: 500
>

```

[Example 11-2](#) shows an overall status of the available interfaces on an FTD. It confirms that the GigabitEthernet1/1 and GigabitEthernet1/2 interfaces are up, and configured with no IP address. However, it does not confirm if they are part of an inline pair.

Example 11-2 *Summary of the FTD Interface Status*

```

> show interface ip brief
Interface                IP-Address      OK? Method Status
Protocol
Virtual0                 127.1.0.1      YES unset  up
up
GigabitEthernet1/1      unassigned     YES unset  up
up
GigabitEthernet1/2      unassigned     YES unset  up
up
GigabitEthernet1/3      unassigned     YES unset  administratively down
down
GigabitEthernet1/4      unassigned     YES unset  administratively down
down
GigabitEthernet1/5      unassigned     YES unset  administratively down
down
GigabitEthernet1/6      unassigned     YES unset  administratively down
down
GigabitEthernet1/7      unassigned     YES unset  administratively down
down
GigabitEthernet1/8      unassigned     YES unset  administratively down
down
Internal-Controll1/1    127.0.1.1     YES unset  up
up
Internal-Data1/1        unassigned     YES unset  up
up
Internal-Data1/2        unassigned     YES unset  down
down
Internal-Data1/3        unassigned     YES unset  up
up
Internal-Data1/4        169.254.1.1   YES unset  up
up
Management1/1          unassigned     YES unset  up
up
>

```

[Example 11-3](#) confirms that the GigabitEthernet1/1 interface is in inline mode, and it is included in an inline pair called INSIDE_OUTSIDE_PAIR. It also provides detail statistic of the traffic.

Example 11-3 *Detail Statistic of the GigabitEthernet1/1 Interface*

```

> show interface GigabitEthernet1/1
Interface GigabitEthernet1/1 "INSIDE_INTERFACE", is up, line protocol is up
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
    Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
    Input flow control is unsupported, output flow control is off
    MAC address a46c.2ae4.6bc0, MTU 1500
    IPS Interface-Mode: inline, Inline-Set: INSIDE_OUTSIDE_PAIR
    IP address unassigned
    2382 packets input, 258694 bytes, 0 no buffer
    Received 142 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 pause input, 0 resume input
    0 L2 decode drops
    2079 packets output, 234133 bytes, 0 underruns
    0 pause output, 0 resume output
    0 output errors, 0 collisions, 0 interface resets
    0 late collisions, 0 deferred
    0 input reset drops, 2 output reset drops
    input queue (blocks free curr/low): hardware (946/894)
    output queue (blocks free curr/low): hardware (1023/1020)
Traffic Statistics for "INSIDE_INTERFACE":
  592 packets input, 53381 bytes
  530 packets output, 63776 bytes
  11 packets dropped
  1 minute input rate 1 pkts/sec, 85 bytes/sec
  1 minute output rate 1 pkts/sec, 88 bytes/sec
  1 minute drop rate, 0 pkts/sec
  5 minute input rate 1 pkts/sec, 79 bytes/sec
  5 minute output rate 0 pkts/sec, 103 bytes/sec
  5 minute drop rate, 0 pkts/sec
>

```

[Verification of the Packet Flow using Packet Tracer](#)

If the interface status and configuration seem correct, but the hosts in the inside and outside networks are still unable to communicate, you can use a simulated packet to determine the flow of a packet through an FTD. The **packet-tracer** command can generate a virtual packet based on the parameters you enter with it. In the next example, you will simulate the flow of an ICMP packet using the following syntax:

```
packet-tracer input source_interface protocol_name source_address ICMP_type
ICMP_code destination_address
```

Note

The packet-tracer command syntax is different for a TCP packet. You will learn the usage of it at the last part of this chapter when the blocking of a TCP service/port is simulated.

In an ICMP header, the **type** and **code** fields contain the control messages. There are many different types of ICMP control messages available. In the following exercise, however, you are going to utilize two types of messages — echo request and echo reply.

[Figure 11-13](#) shows the format of an ICMP packet. The 8-bit type and 8-bit code fields carries the ICMP control messages.

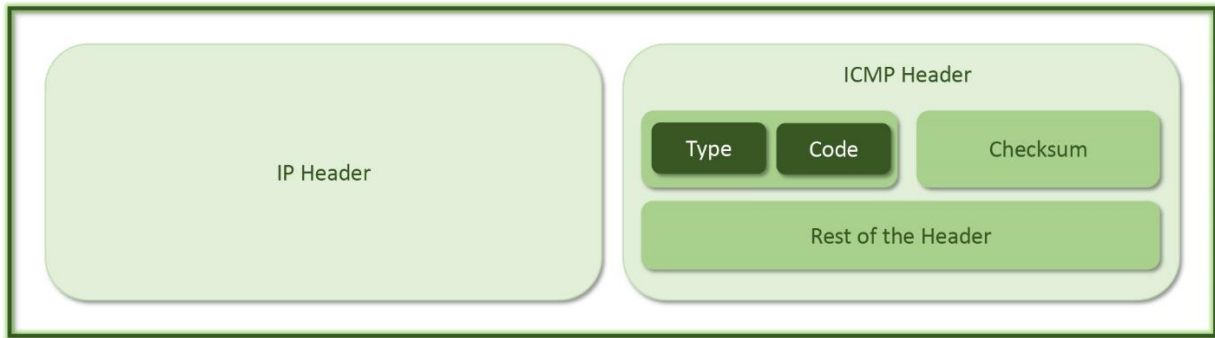


Figure 11-13. *Type and Code Fields on an ICMP Header*

[Table 11-2](#) shows the values of the type and code fields. Using these values, you can generate a particular ICMP control message.

Control Message	Type	Code
Echo Request	8	0
Echo Reply	0	0

Table 11-2. *Values for the Echo Request and Echo Reply Messages*

[Example 11-4](#) demonstrates the simulation of ICMP traffic, sent from the inside interface. The host 192.168.1.2 from the inside network sends an ICMP Echo-Request to an outside system 192.168.1.200. The ingress and egress interfaces of this simulated packet are determined by the inline-set configuration of your FTD.

Example 11-4 *Simulation of an ICMP Echo-Request*

```
> packet-tracer input INSIDE_INTERFACE icmp 192.168.1.2 8 0 192.168.1.200
```

```
Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
```

```
Phase: 2
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS
services will be applied
```

```
Phase: 3
Type: ACCESS-LIST
```

```
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434432
access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: AC Policy
- Default/1
access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION
RULE
Additional Information:
This packet will be sent to snort for additional processing where a
verdict will be reached
```

```
Phase: 4
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Ingress interface INSIDE_INTERFACE is in NGIPS inline mode.
Egress interface OUTSIDE_INTERFACE is determined by inline-set
configuration
```

```
Phase: 5
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 269, packet dispatched to next module
```

```
Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: allow
```

>

[Example 11-5](#) concludes that an ICMP Echo-Reply packet, originated by the host 192.168.1.200, should be able to reach out its destination 192.168.1.2.

Example 11-5 *Simulation of an ICMP Echo-Reply*

```
> packet-tracer input OUTSIDE_INTERFACE icmp 192.168.1.200 0 0 192.168.1.2
```

```
Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
```

```
Phase: 2
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
```

Additional Information:

The flow ingresses an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 3

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434432
```

```
access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: AC Policy  
- Default/1
```

```
access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION  
RULE
```

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 4

Type: NGIPS-EGRESS-INTERFACE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

Ingress interface OUTSIDE_INTERFACE is in NGIPS inline mode.

Egress interface INSIDE_INTERFACE is determined by inline-set configuration

Phase: 5

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 271, packet dispatched to next module

Result:

input-interface: OUTSIDE_INTERFACE

input-status: up

input-line-status: up

Action: allow

>

[Verification of the Packet Flow using Real Packet Capture](#)

In the previous section, you used a virtually generated packet to simulate the flow of a packet. In this section, you are going to use the real packets to determine the flow of a packet through an FTD by using the following steps:

Step 1. Create two capture rules with the tracing capability. To determine the flow of a packet, this example uses ping requests. To trace packets from both directions, you should capture the ICMP traffic from both of the interfaces of an inline pair.

[Example 11-6](#) demonstrates the usages of the **trace** keyword with the **capture** command. The example uses the capture command twice, to capture traffic from the ingress and egress interfaces separately. The **Capturing – 0 bytes** message on the **show capture** command confirms that the process is running, but has not seen any packet yet.

Example 11-6 Creation and Verification of Matching Conditions for Packet Captures

```
> capture inside_icmp trace interface INSIDE_INTERFACE match icmp any any
> capture outside_icmp trace interface OUTSIDE_INTERFACE match icmp any any
> show capture

capture inside_icmp type raw-data trace interface INSIDE_INTERFACE
[Capturing - 0 bytes]
  match icmp any any
capture outside_icmp type raw-data trace interface OUTSIDE_INTERFACE
[Capturing - 0 bytes]
  match icmp any any
>
```

Step 2. Send a few ping requests from your inside host to the outside system. After sending and receiving 2-4 ICMP packets, stop the ping request. You should now be able to see the capture between the inside and outside systems.

[Example 11-7](#) displays the captures of ICMP traffic from both directions on both interfaces.

Example 11-7 Captures of the ICMP Traffic

```
> show capture inside_icmp

4 packets captured

  1: 21:52:25.988428      192.168.1.2 > 192.168.1.200: icmp: echo request
  2: 21:52:25.989405      192.168.1.200 > 192.168.1.2: icmp: echo reply
  3: 21:52:26.989862      192.168.1.2 > 192.168.1.200: icmp: echo request
  4: 21:52:26.990412      192.168.1.200 > 192.168.1.2: icmp: echo reply
4 packets shown
>

> show capture outside_icmp

4 packets captured

  1: 21:52:25.989038      192.168.1.2 > 192.168.1.200: icmp: echo request
  2: 21:52:25.989252      192.168.1.200 > 192.168.1.2: icmp: echo reply
  3: 21:52:26.990106      192.168.1.2 > 192.168.1.200: icmp: echo request
  4: 21:52:26.990305      192.168.1.200 > 192.168.1.2: icmp: echo reply
4 packets shown
>
```

Step 3. From [Example 11-7](#), select a packet you want to trace using its associated number on the left.

In this lab scenario, the host 192.168.1.2 sends the echo-request packet from the inside interface. That's why you use the `inside_icmp` capture to view the tracing data. Similarly, when you want to trace the echo-reply packet from the host 192.168.1.200, you need to use the capture the `outside_icmp` capture.

[Example 11-8](#) demonstrates the flow of packet number 1. You have identified the number in the previous output example. You must use the **trace** keyword to view the tracing data.

Example 11-8 *Tracing of an Echo-Request Packet Originated by the Host 192.168.1.2*

```
> show capture inside_icmp packet-number 1 trace
```

```
4 packets captured
```

```
1: 21:52:25.988428      192.168.1.2 > 192.168.1.200: icmp: echo request
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 3
```

```
Type: NGIPS-MODE
```

```
Subtype: ngips-mode
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied
```

```
Phase: 4
```

```
Type: ACCESS-LIST
```

```
Subtype: log
```

```
Result: ALLOW
```

```
Config:
```

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434432
```

```
access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: AC Policy - Default/1
```

```
access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
```

```
Additional Information:
```

```
This packet will be sent to snort for additional processing where a verdict will be reached
```

```
Phase: 5
```

```
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
```

```
Subtype: Resolve Egress Interface
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
Ingress interface INSIDE_INTERFACE is in NGIPS inline mode.
```

```
Egress interface OUTSIDE_INTERFACE is determined by inline-set configuration
```

```
Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 279, packet dispatched to next module
```

```
Phase: 7
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'
```

```
Phase: 8
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet
```

```
Phase: 9
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list
```

```
Result:
input-interface: OUTSIDE_INTERFACE
input-status: up
input-line-status: up
Action: allow
```

```
1 packet shown
>
```

[Example 11-9](#) shows two different outputs for tracing the same packet. Only the second command shows the desired detail, because the outside interface receives the Echo-Reply packet.

Example 11-9 *Tracing of an Echo-Reply Packet Originated by the Host 192.168.1.200*

```
> show capture inside_icmp packet-number 2 trace
```

```
4 packets captured
```

```
2: 21:52:25.989405      192.168.1.200 > 192.168.1.2: icmp: echo reply
1 packet shown
>
```

```
> show capture outside_icmp packet-number 2 trace
```


4 packets captured

2: 21:52:25.989252 192.168.1.200 > 192.168.1.2: icmp: echo reply

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 279, using existing flow

Phase: 4
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 5
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet

Phase: 6
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: allow

1 packet shown

>

Tip

To learn how to inactivate a capture on an interface, or how to delete a capture process permanently, read the chapter on *Capture of Traffic for Advance Analysis*.

Enablement of Fault Tolerance Features

In Inline mode, traffic goes through an FTD. FTD can interrupt the traffic flow in case of any software or hardware failure. To avoid any network outage, Firepower system offers various fault tolerance features, such as, failsafe, link state propagation, etc.

Configuration

This section assumes that you have already configured your FTD in basic inline mode by following the steps described in the previous section. Now, you are going to edit the existing configuration to enable two fault tolerance features — failsafe, and link state propagation.

- **Failsafe:** In case of any software failure, if FTD stops processing traffic, and the buffer becomes full, it leads to the drop of traffic. The failsafe feature watches the usage of buffer. When the buffer is full, it bypasses detection, and allows the traffic to go through the FTD. Hence, users do not experience any permanent network outage.

- **Link State Propagation:** If one of links of an inline pair goes down, the second link can stay up, and able to receive traffic. However, the FTD cannot transfer traffic through an interface that has no link. The link state propagation feature automatically brings the remaining interface down if one of the interfaces in an inline pair goes down. This feature improves routing convergence time by not sending traffic through a failed link.

Use the following steps to enable these features:

Step 1. Navigate to the **Devices > Device Management** page. Edit the device where you created the inline set.

Step 2. In the device editor page, go to the **Inline Sets** tab. Select the inline set that you want to modify. Use the pencil icon. It opens the **Add Inline Set** window.

Step 3. Go to the **General** tab, and select the **Failsafe** checkbox.

[Figure 11-14](#) shows the **Failsafe** option. Select this checkbox to enable the feature.

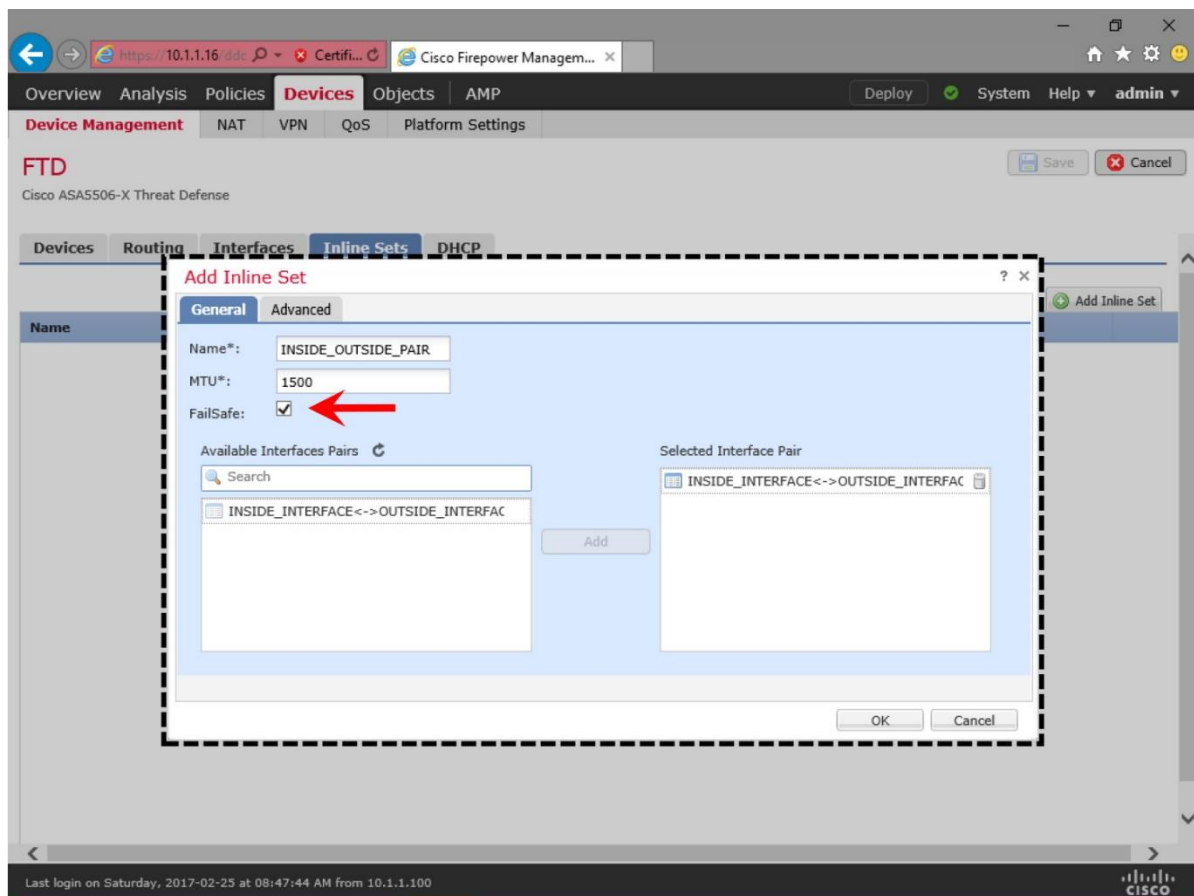


Figure 11-14. *Failsafe Feature is Available under the General Tab*

Step 4. Go to the **Advanced** tab, and select the **Propagate Link State** checkbox.

[Figure 11-15](#) shows the **Propagate Link State** option. Select this checkbox to enable the feature.

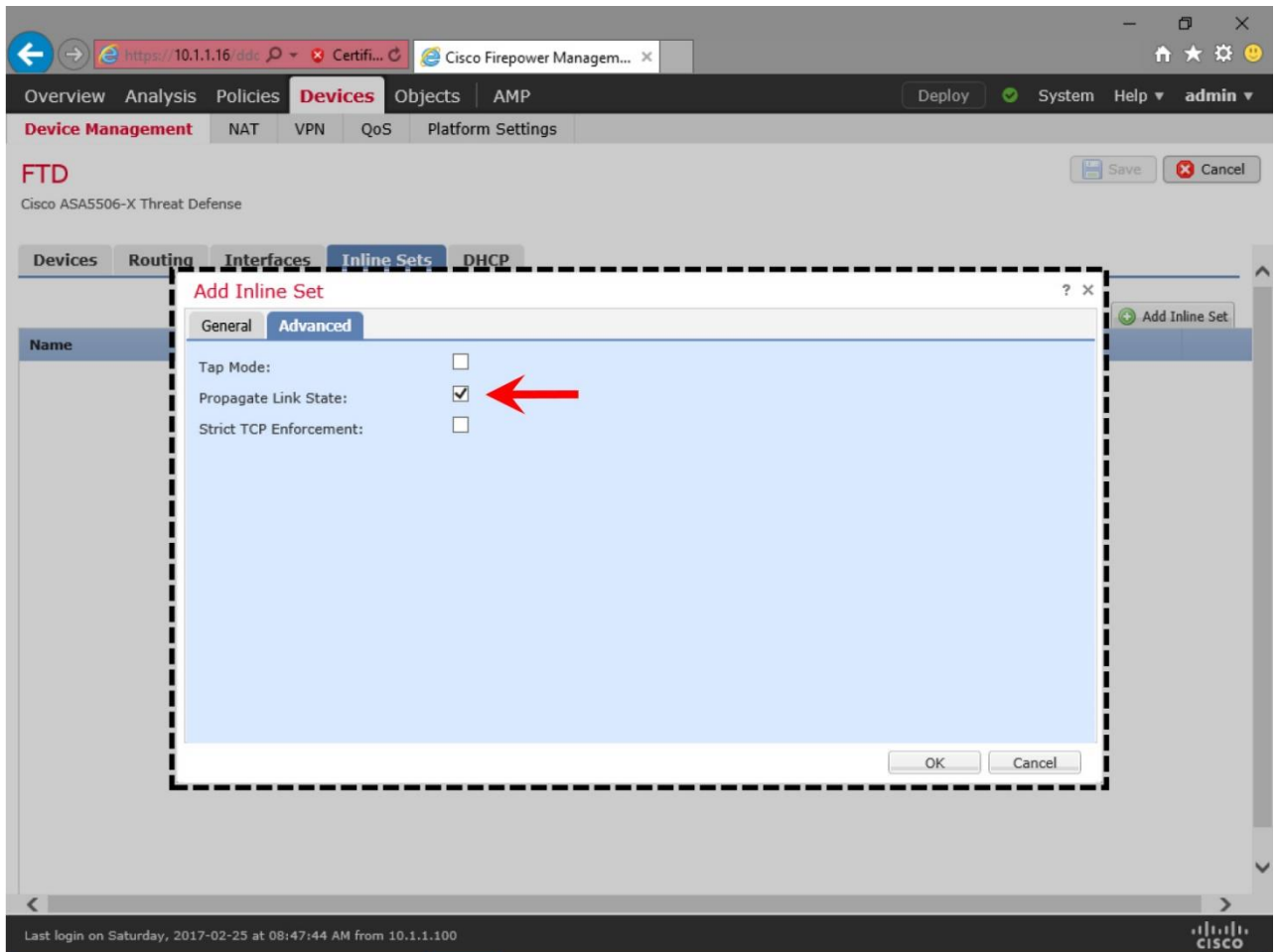


Figure 11-15. *Link State Propagate Feature is Available under the Advanced Tab*

Step 5. Click the **OK** button to return to the device editor page. Save the changes, and deploy the settings to the FTD.

Verification

After you reconfigure an inline set with the failsafe and link state propagation features, you can run the **show inline-set** command to verify the changes.

[Example 11-10](#) confirms that the failsafe and link state propagation features are enabled successfully.

Example 11-10 *Viewing the Inline Set Configuration from the CLI*

```
> show inline-set
```

```
Inline-set INLINE_OUTSIDE_PAIR
Mtu is 1500 bytes
Failsafe mode is on/activated
Failsecure mode is off
```

```

Tap mode is off
Propagate-link-state option is on
hardware-bypass mode is disabled
Interface-Pair[1]:
  Interface: GigabitEthernet1/1 "INSIDE_INTERFACE"
    Current-Status: Down(Propagate-Link-State-Activated)
  Interface: GigabitEthernet1/2 "OUTSIDE_INTERFACE"
    Current-Status: Down(Down-By-Propagate-Link-State)
  Bridge Group ID: 500
>

```

To verify if the link state propagation feature works as expected, you can unplug the cable from one of the interfaces, and run the **show interface** command to determine the status.

[Example 11-11](#) displays the output of the **show interface** commands. After unplugging the cable from the GigabitEthernet1/1 interface, the second interface GigabitEthernet1/2 has also gone down.

Example 11-11 *Status of the Link State Propagation*

```

> show interface GigabitEthernet1/1
Interface GigabitEthernet1/1 "INSIDE_INTERFACE", is down, line protocol is
down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
  Auto-Duplex, Auto-Speed
  Input flow control is unsupported, output flow control is off
  MAC address a46c.2ae4.6bc0, MTU 1500
  IPS Interface-Mode: inline, Inline-Set: INSIDE_OUTSIDE_PAIR
  Propagate-Link-State-Activated
  IP address unassigned
  14779 packets input, 1512926 bytes, 0 no buffer
  Received 147 broadcasts, 0 runts, 0 giants
.
.
<Output Omitted for Brevity>

> show interface GigabitEthernet1/2
Interface GigabitEthernet1/2 "OUTSIDE_INTERFACE", is administratively down,
line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
  Auto-Duplex, Auto-Speed
  Input flow control is unsupported, output flow control is off
  MAC address a46c.2ae4.6bc1, MTU 1500
  IPS Interface-Mode: inline, Inline-Set: INSIDE_OUTSIDE_PAIR
  Down-By-Propagate-Link-State
  IP address unassigned
  15397 packets input, 1558479 bytes, 0 no buffer
  Received 930 broadcasts, 0 runts, 0 giants
.
.
<Output Omitted for Brevity>

```

Blocking of a Specific Port

Now that you have configured the inline interface pair, let's try to block a particular port or service using an FTD. In the previous section, you used ICMP protocol to determine the

traffic flow. In this section, you will configure an FTD to block the clear text telnet traffic — a TCP protocol that uses port 23.

Configuration

The following steps describes how to add an access rule that can block any packets destined to port 23:

Step 1. Navigate to the Policies > Access Control > Access Control page.

Step 2. Select an Access Control policy that you want to deploy to an FTD. Click the pencil icon to edit.

Step 3. When the policy editor page appears, select the **Add Rule** button to create a new rule. The **Add Rule** window appears.

[Figure 11-16](#) shows the addition of an access rule that blocks traffic destined to port 23 (TELNET service).

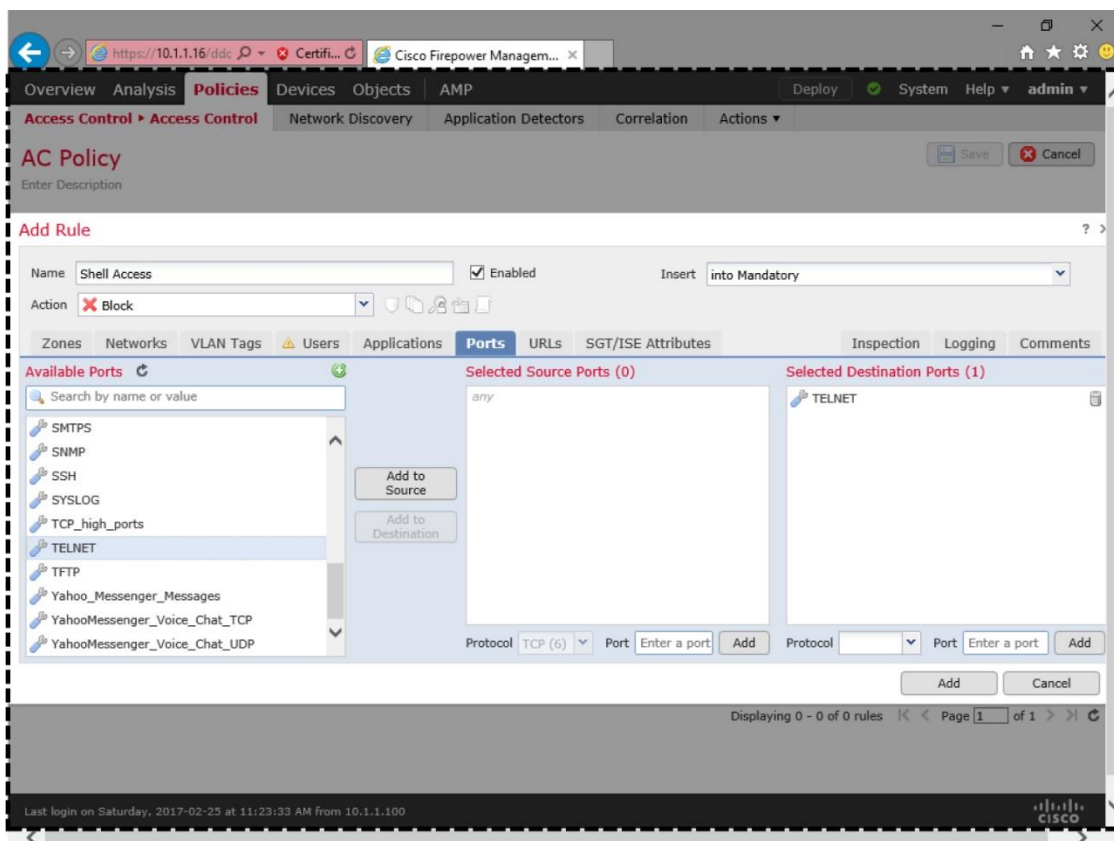


Figure 11-16. Access Rule to Block Telnet Port

Step 4. Give a name to the Access rule, enable the rule, and select the Block action.

Step 5. In the **Ports** tab, find the telnet service from the **Available Ports** selections. Add the **TELNET** port to the destination.

Step 6. Go to the **Logging** tab, and select **Log at beginning of Connection**. This step is optional — allows you to view an event when a telnet connection is blocked.

[Figure 11-17](#) displays the enablement of logging for the “Shell Access” access rule. When this access rule blocks a telnet connection, the web interface displays a “block” event for it.

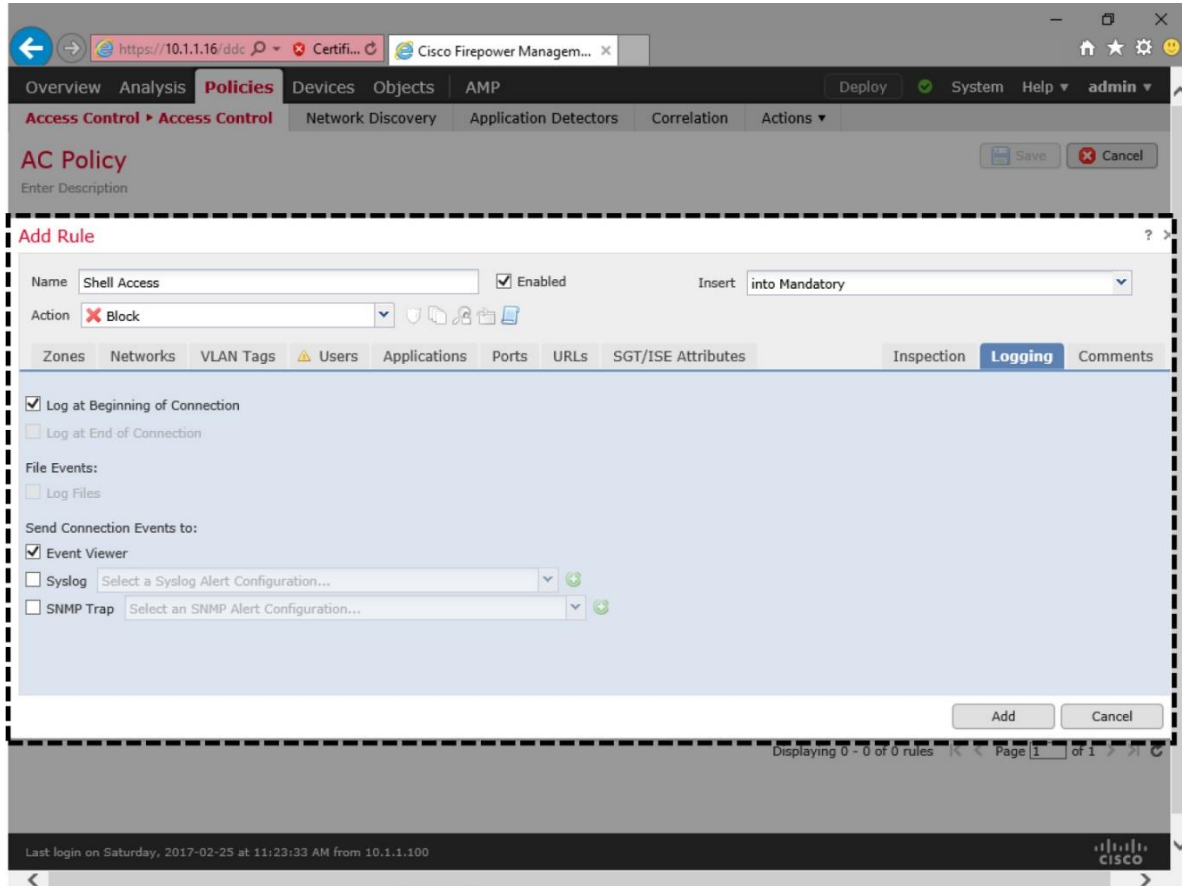


Figure 11-17. *Enablement of Logging for an Access Rule*

Step 7. Click the Add button to return to the policy editor page.

Step 8. Define a **Default Action**. Select **Balanced Security and Connectivity** from the drop-down. It allows any non-malicious traffic other than telnet application to go through.

Figure 11-18 displays the policy editor page after you add a rule to block telnet traffic. You must save the policy and deploy it to an FTD to activate the rule.

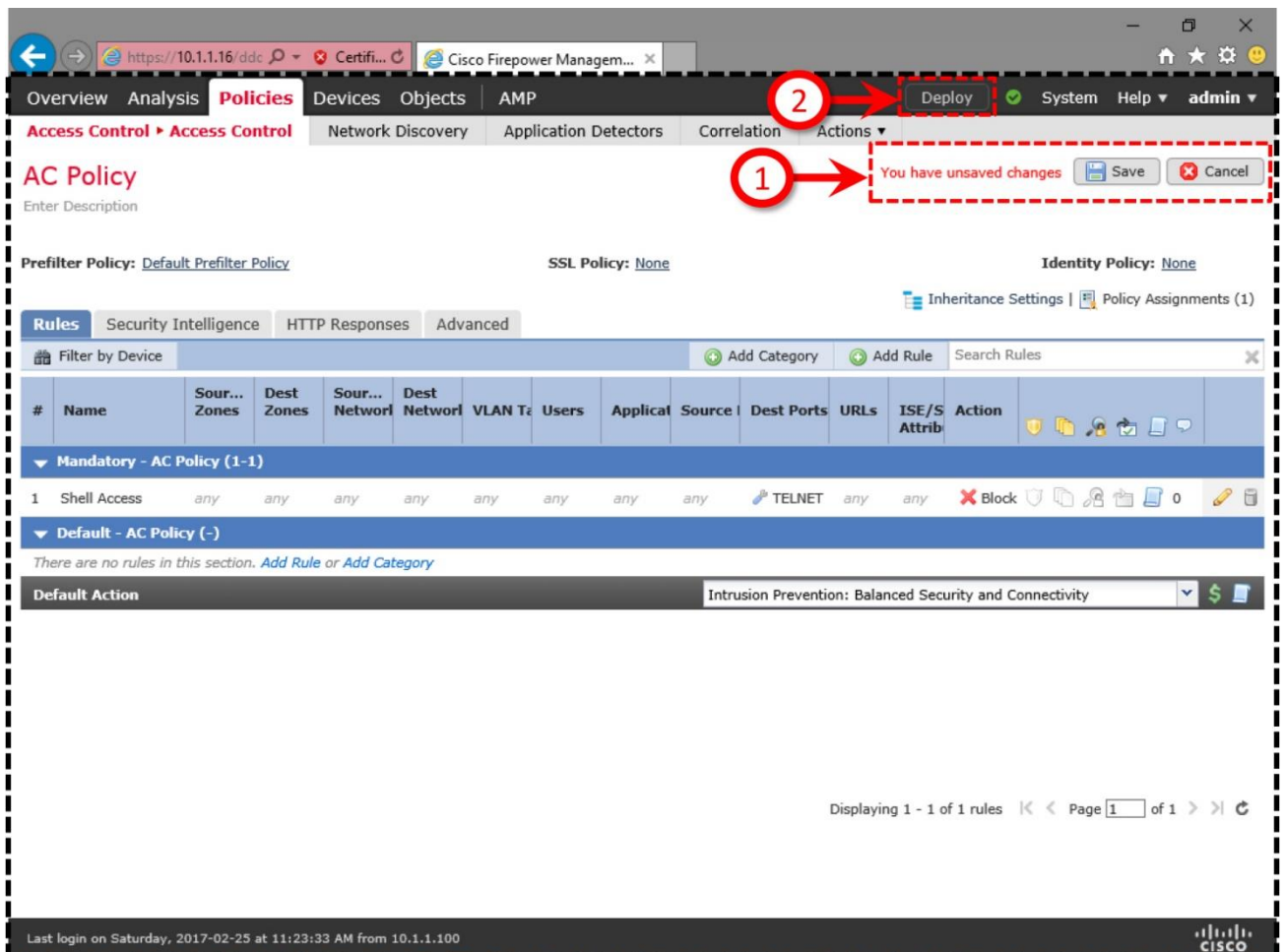


Figure 11-18. The Access Control Policy Editor Page

Step 9. Save the configuration. Deploy the Access Control Policy to the FTD.

Verification of Configuration

After a successful deployment of the updated Access Control policy, go to your inside host 192.168.1.2 to access the outside system 192.168.1.200 using telnet. Your attempt to connect through the telnet should not work, because the FTD is now blocking any traffic destined to port 23. For a blocked connection, the FMC should also log a connection event.

Figure 11-19 illustrates two types of connection events — block and allow. The telnet traffic is blocked by the *Shell Access* rule, while any other traffic (such as, ping requests) are allowed by the *Default Action*.

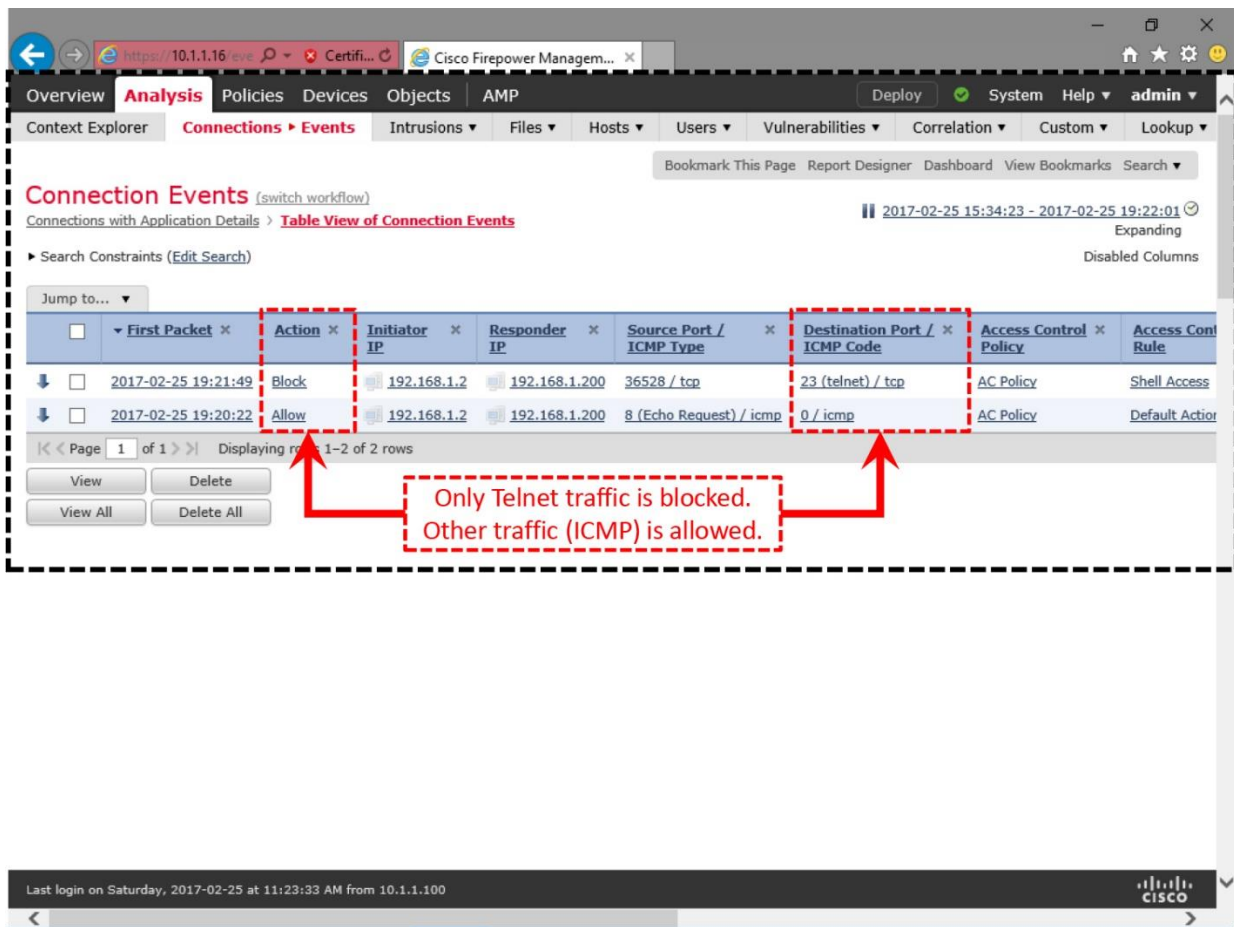


Figure 11-19. Events Logged for a Blocked Telnet Connection

Example 11-12 displays the *Shell Access* rule that you created to block telnet traffic. The line following this rule, you can find the default action to permit any other traffic. The hitcnt value increases as more telnet traffic is blocked by the FTD.

Example 11-12 Viewing the Access Control Rules from the CLI

```
> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list CSM_FW_ACL_ ; 7 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY:
Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL
ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998
(hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit 41 any any rule-id 9998
(hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 5 advanced permit gre any any rule-id 9998
(hitcnt=0) 0x52c7a066
```

```

access-list CSM_FW_ACL_ line 6 advanced permit udp any eq 3544 any range
1025 65535 rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 7 advanced permit udp any range 1025 65535 any
eq 3544 rule-id 9998 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 8 remark rule-id 268440576: ACCESS POLICY: AC
Policy - Mandatory/1
access-list CSM_FW_ACL_ line 9 remark rule-id 268440576: L4 RULE: Shell
Access
access-list CSM_FW_ACL_ line 10 advanced deny tcp any any object-group
TELNET rule-id 268440576 event-log flow-start (hitcnt=2) 0xae7f8544
  access-list CSM_FW_ACL_ line 10 advanced deny tcp any any eq telnet rule-
id 268440576 event-log flow-start (hitcnt=2) 0x2bcbaf06
access-list CSM_FW_ACL_ line 11 remark rule-id 268434432: ACCESS POLICY: AC
Policy - Default/1
access-list CSM_FW_ACL_ line 12 remark rule-id 268434432: L4 RULE: DEFAULT
ACTION RULE
access-list CSM_FW_ACL_ line 13 advanced permit ip any any rule-id
268434432 (hitcnt=134) 0xald3780e
>

```

Analysis of a Packet Drop using Simulated Packet

You can utilize the **packet-tracer** tool to generate a virtual TCP packet, and simulate the flow of the packet through an FTD. It allows you to analyze any potential packet drop due to the Access Control policy.

[Example 11-13](#) simulates the requests for telnet traffic access from both network — inside and outside — in two packet-tracer outputs. Both requests are blocked by the Shell Access rule that you created earlier. This example uses port 23 as the destination port, and assumes the port number 10000 as a randomly generated source port.

Example 11-13 Simulation of a TCP Packet Drop

! Packet originates from the inside network, Telnet server is located at the outside network

```
> packet-tracer input INSIDE_INTERFACE tcp 192.168.1.2 10000 192.168.1.200
23
```

```

Phase: 1
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS
services will be applied

```

```

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny tcp any any object-group TELNET rule-
id 268440576 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268440576: ACCESS POLICY: AC Policy
- Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268440576: L4 RULE: Shell Access

```

```
object-group service TELNET tcp
  port-object eq telnet
Additional Information:
```

```
Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

>

! Packet originates from the outside network, Telnet server is located at the inside network

```
> packet-tracer input OUTSIDE_INTERFACE tcp 192.168.1.200 10000 192.168.1.2
23
```

```
Phase: 1
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS
services will be applied
```

```
Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny tcp any any object-group TELNET rule-
id 268440576 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268440576: ACCESS POLICY: AC Policy
- Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268440576: L4 RULE: Shell Access
object-group service TELNET tcp
  port-object eq telnet
Additional Information:
```

```
Result:
input-interface: OUTSIDE_INTERFACE
input-status: up
input-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

>

[Analysis of a Packet Drop using Real Packet](#)

If your network experiences any connectivity issue, and you do not see any configuration error, you can capture the live traffic with the tracing feature enabled. It allows you to analyze a real packet — how it goes through an FTD and how is it blocked by an access rule when it matches a condition. The following steps describe the process:

Step 1. Create a rule that can capture any traffic destined to port 23. You must apply the rule on the interface that sees the incoming requests.

[Example 11-14](#) shows a command that is able to capture any traffic with destination port 23. You must use the **trace** keyword to capture additional tracing data. After you enter the command, you can view the status of a capture using the **show capture** command.

Example 11-14 *Command to Capture Telnet Traffic with Tracing Data*

```
> capture inside_telnet trace interface INSIDE_INTERFACE match tcp any any
eq 23
>
> show capture
capture inside_telnet type raw-data trace interface INSIDE_INTERFACE
[Capturing - 0 bytes]
  match tcp any any eq telnet
>
```

Step 2. Try to access telnet server. Although it is going to fail due to the *Shell Access* rule, your failure attempt generates telnet traffic that you will analyze next.

[Example 11-15](#) displays four packets with destination port 23. They are captured using the command provided in the previous example.

Example 11-15 *FTD Captures Four Telnet Packets*

```
> show capture inside_telnet

4 packets captured

  1: 01:24:06.440422      192.168.1.2.36534 > 192.168.1.200.23: S
2986077586:2986077586(0) win 29200 <mss 1460,sackOK,timestamp 3482899
0,nop,wscale 7>
  2: 01:24:07.437965      192.168.1.2.36534 > 192.168.1.200.23: S
2986077586:2986077586(0) win 29200 <mss 1460,sackOK,timestamp 3483149
0,nop,wscale 7>
  3: 01:24:09.442009      192.168.1.2.36534 > 192.168.1.200.23: S
2986077586:2986077586(0) win 29200 <mss 1460,sackOK,timestamp 3483650
0,nop,wscale 7>
  4: 01:24:13.450217      192.168.1.2.36534 > 192.168.1.200.23: S
2986077586:2986077586(0) win 29200 <mss 1460,sackOK,timestamp 3484652
0,nop,wscale 7>
4 packets shown
>
```

Step 3. Select a packet using its number. View the packet using the **show capture** command. Add the **trace** parameter with the command in order to view additional tracing data.

[Example 11-16](#) demonstrates the drop of a TCP packet through an FTD. The tracing data confirms that the packet dropped due to an access rule.

Example 11-16 *Viewing of a Captured Packet with Tracing Data*

```
> show capture inside_telnet packet-number 2 trace
```

4 packets captured

```
2: 01:24:07.437965      192.168.1.2.36534 > 192.168.1.200.23: S
2986077586:2986077586(0) win 29200 <mss 1460,sackOK,timestamp 3483149
0,nop,wscale 7>
```

```
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list
```

```
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
```

```
Phase: 3
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS
services will be applied
```

```
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny tcp any any object-group TELNET rule-
id 268440576 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268440576: ACCESS POLICY: AC Policy
- Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268440576: L4 RULE: Shell Access
object-group service TELNET tcp
port-object eq telnet
Additional Information:
```

```
Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

1 packet shown

>

Summary

In this chapter, you have learned how to configure an FTD in inline interface mode, how to enable fault tolerance features on an inline set, and how to trace a packet in order to analyze

the root cause of a drop. This chapter also describes various command line tools that you can utilize to verify the status of an interface, an inline pair, and an inline set.

Quiz

1. Which of the following statement is true?

- a.** The configuration steps of an inline interface mode and transparent mode are same.
- b.** Inline pair uses loopback IP address for communication.
- c.** Failsafe feature is enabled on an inline set, by default.
- d.** Propagate link state feature is not enabled by default on an inline set.

2. Which of the following statement is true?

- a.** You should include both interface pairs into the same inline set to ensure the recognition of asynchronous traffic.
- b.** Failsafe feature allows an FTD to continue its traffic flow through the device by bypassing the detection.
- c.** Link state propagation reduces the routing convergence time when one of the interfaces in an inline set goes down.
- d.** All of the above.

3. Which command provides an overview of the various components of an inline interface set?

- a.** show interface ip brief
- b.** show inline-set
- c.** show interface detail
- d.** show interface inline detail

4. To determine if a packet is dropped by an access rule, which of the following option is provided by FTD?

- a.** Capture traffic in .pcap file format, and open the file in an external packet analyzer.
- b.** Use the packet-tracer tool to trace a live packet directly.
- c.** Capture the traffic along with the trace functionality, and view the packets using the capture command.
- d.** None of the above.

Chapter 12. Inspecting Traffic without Blocking Them

An FTD can block packets when you deploy it in inline interface mode. However, there are some scenarios where you may not want to block a packet right away; instead, you want to watch the traffic pattern, determine the effectiveness of your access rules or intrusion rules on live traffic, and then tune the overall access control policy accordingly. Sometimes, you want to analyze any suspicious activities on your honeypot, and detect any potential attacks. Occasionally, the business continuity policy of your organization may demand for a passive detection, rather than an inline protection. In this chapter, you will learn how you can deploy an FTD to inspect your traffic and detect any suspicious activities without dropping them in real time.

Essential Knowledge

When you consider deploying an FTD for detection-only purpose, you have mainly two choices — passive mode and inline-tap mode. This section emphasizes the differences between various interface modes and monitoring technologies.

Passive Monitoring Technology

To understand the architecture of a passive deployment, you must be familiar with the underlying technologies, such as, promiscuous mode, port mirroring, etc.

- **Promiscuous Mode:** On an FTD, when you configure an interface in passive mode, it sets the interface into the promiscuous mode. Promiscuous mode allows an interface to see any packet in a network segment even if a packet is not aimed for that interface. This capability empowers an FTD to monitor the network activities without being an active part of a network.

[Figure 12-1](#) introduces the technologies — promiscuous mode and SPAN port — used in a passive FTD deployment.

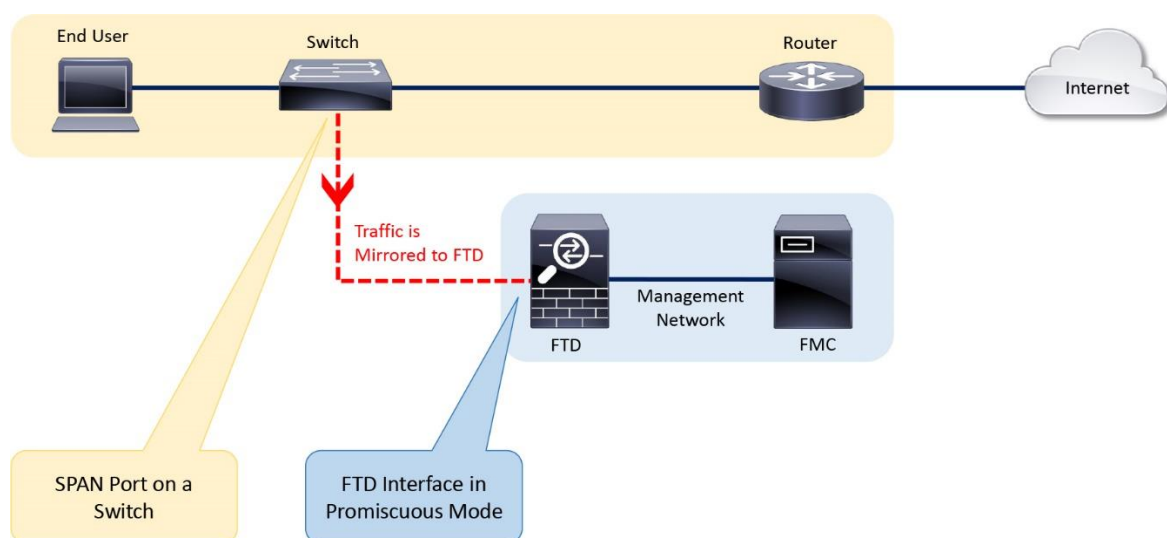


Figure 12-1. Basic Architecture of a Passive Deployment

- **Port Mirroring:** Some switch models can replicate traffic from multiple switch ports and sends the copies to a specific switch port. It allows an FTD to monitor a network without being an active part of the network flow. This feature is called port mirroring. A switch port, enabled with the port mirroring feature, is known as the Switch Port Analyzer (SPAN) port.

A SPAN port can receive mirrored traffic from the same layer 2 switch. However, if you want to send the replicated traffic to multiple switches, you can use the Encapsulated Remote Switched Port Analyzer (ERSPAN) technology. ERSPAN transports mirrored traffic over a layer 3 network by encapsulating them using the Generic Routing Encapsulation (GRE) tunneling protocol.

FTD supports inspection of both SPAN and ERSPAN traffic. However, the configuration examples in this chapter only use the SPAN port.

[Figure 12-2](#) demonstrates the differences between two types of passive deployments — using SPAN and ERSPAN ports.

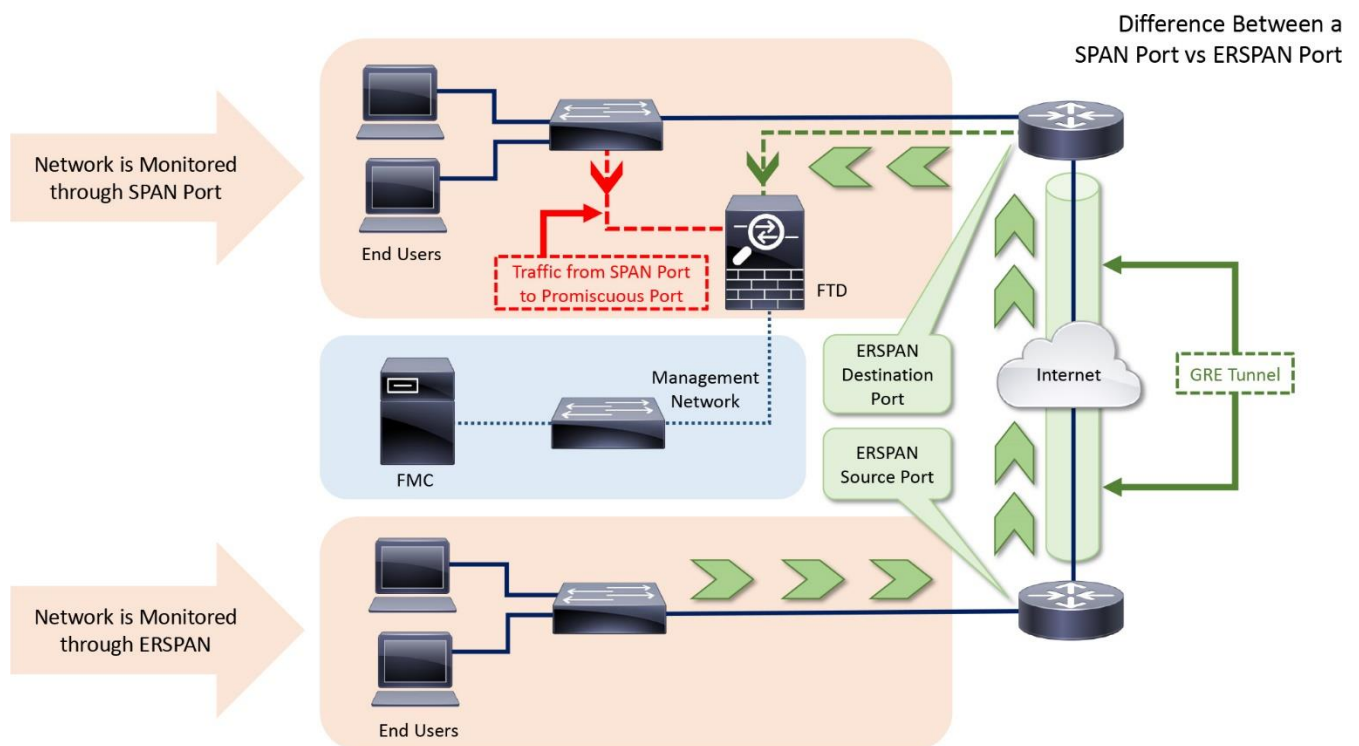


Figure 12-2. *Difference between a SPAN Port and an ERSPAN Port*

- **TAP:** TAP is a network device that copies and transfers traffic to another system. Unlike a SPAN port on a switch, which is configured in the software level, a network tap is a dedicated hardware that is designed to replicate and transfer traffic. For an additional cost, a tap offers numerous advantages over a span port. One of the most important benefits is, a tap is able to capture and copy all of the traffic (including any errors) from a highly utilized network, and transfer them to a monitoring device, like FTD, without any packet drop.

A SPAN port, on the contrary, drops packets if the utilization of a SPAN link exceeds its capacity. In a highly utilized network, if a SPAN port fails to transfer all of the traffic from

all of the switch ports, an FTD loses the complete visibility of a network, and may miss detection of any suspicious activities.

[Figure 12-3](#) shows two types of cabling that an FTD supports. Both deployments are operational in detection-only mode.

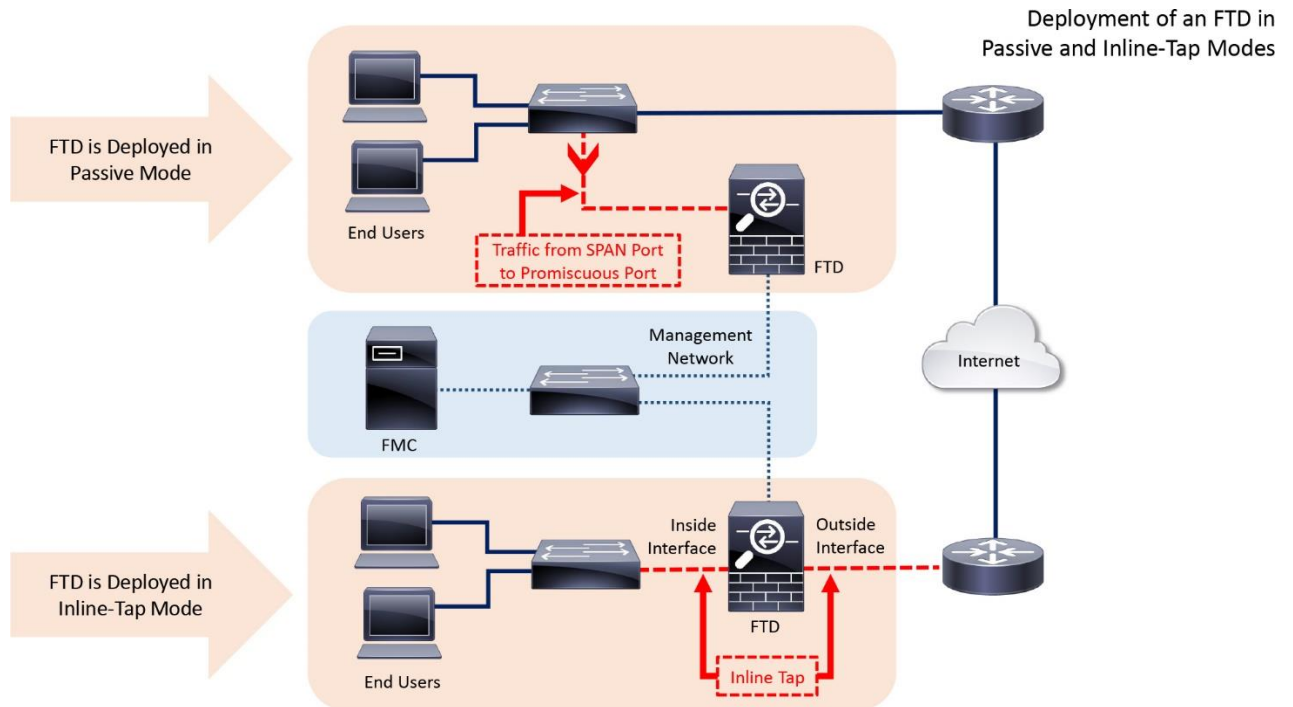


Figure 12-3. *Cabling of Interfaces in Promiscuous Mode and Inline-Tap Mode*

Inline vs. Inline-Tap vs. Passive

In the previous chapter, you learned the operation of an FTD in inline mode, which can block traffic based on the access control and intrusion rules you enable.

In contrast, if you apply a rule to block packets with certain conditions, an FTD does not actually block the original traffic when you configure it in inline-tap or passive mode. It only generates an event, and let the packet go through the FTD.

Figure 12-4 provides a flow chart of various security components of the Firepower software that can block a packet. However, the passive and inline-tap deployments do not block any traffic; they only generate an event when a packet matches a rule.

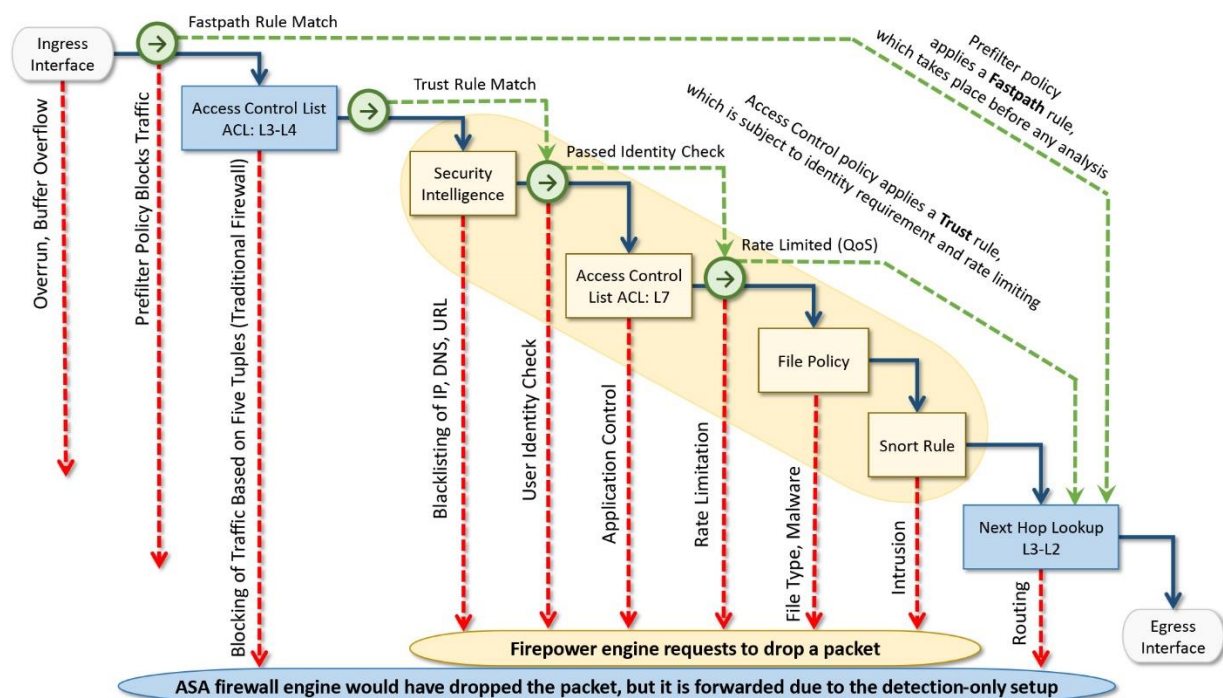


Figure 12-4. Overview of the FTD Components that Can Trigger a Block Action

From a user standpoint, a block or drop action on both modes — passive and inline-tap — exhibit the same effect. For example, if a packet matches an access rule with a *Block* action, it triggers a connection event displaying the “Block” action, while the original packet goes through. Likewise, if a packet matches an intrusion rule with the *Drop and Generate Event* rule state, FTD displays the matching packets with “Would have dropped” action, and let the traffic to go through the FTD.

Although the outcomes are same, the big advantage of an inline-tap mode over a passive mode is the ease of transition to the inline mode, when necessary. Because, the physical cabling is exactly same in inline interface mode and inline-tap mode. Besides detection, when you decide to block traffic in real time, you just need to change a setting in the GUI.

Best Practices

Consider the following best practices before you deploy an FTD in passive interface mode:

- If your plan is to deploy your FTD in detection-only mode, so that you could observe any network activities and tune the security policies accordingly, you may choose inline-tap mode over the traditional passive mode. It allows you to switch to the inline interface mode faster, without touching any physical cables.
- If your ultimate plan is to deploy an FTD in detection-only mode permanently, you can choose the passive mode over the inline-tap mode, because it eliminates any chance of traffic interruption due to an FTD.

- If the utilization of a network is medium to high, use a tap instead of a SPAN port.
- Although an FTD in passive interface mode cannot block traffic, you should still select an FTD model based on the throughput specification. It ensures that an FTD inspects all the traffic without dropping them.

Prerequisites

If you previously configured your FTD as a firewall in routed mode, you need to remove any platform settings, IP address and DHCP server configurations from the FTD data interfaces, as they are not necessary in inline, inline-tap, and passive interface modes.

Inline-Tap Mode

The inline-tap mode comes as an add-on feature to an inline set configuration. To enable the inline-tap mode, at first, you have to perform all of the steps to add an inline set in inline mode.

Configuration

The following steps are necessary to create an inline set with inline-tap mode, and to verify the operation:

- Part 1: Configuration

Step 1. Build an inline pair

Step 2. Associate an inline pair with the inline set

Step 3. Turn on the fault tolerance features

Step 4. Enable the inline-tap mode

Step 5. Save the changes, and deploy the new settings.

- Part 2: Verification

Step 1. Add an access rule with block action

Step 2. Save the changes, and deploy the new settings.

Step 3. Run traffic that matches the access rule.

Note

Except the step 4 on Part 1, which is enable the inline-tap mode, all of the above steps are described and configured in the [chapter 11](#). If you skipped that chapter, please stop here, and read the [chapter 11](#) now. This section discusses only the additional step — enablement of the inline-tap mode.

If your FTD is currently running in inline interface mode, follow the steps below to enable the inline-tap mode:

Step 1. Login to the GUI of your FMC.

Step 2. Navigate to the **Devices > Device Management** page. A list of managed devices appear.

Step 3. Click the *pencil* icon next to the FTD where you want to enable the inline-tap interface mode. The device editor page appears.

Step 4. Select the **Inline Sets** tab. If you configured an inline-set earlier, it appears here.

Step 5. Click the *pencil* icon next to the inline set to modify the existing settings. The **Edit Inline Set** window appears.

[Figure 12-5](#) shows the device editor page. The **Inline Sets** tab confirms that an inline pair is already configured.

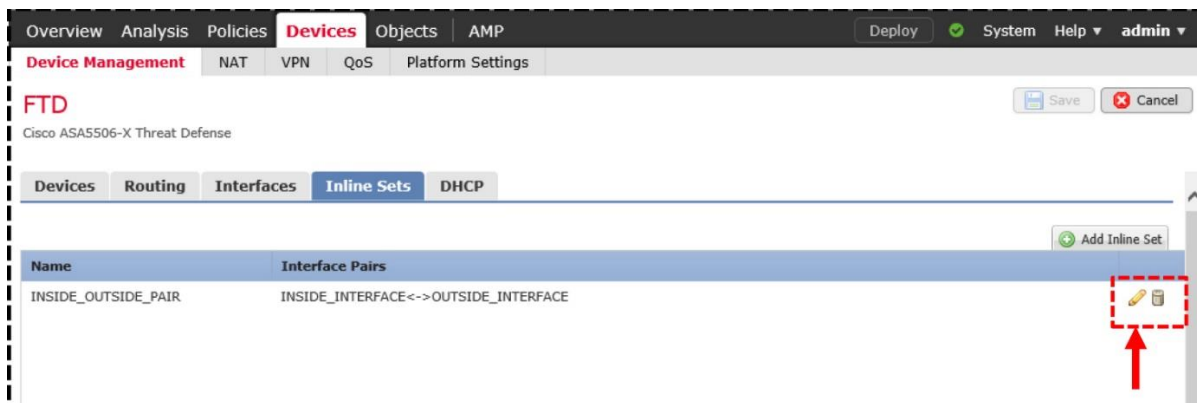


Figure 12-5. Option to Modify an Existing Inline Pair Configuration

Step 6. Select the **Advanced** tab.

Step 7. Enable the checkbox for **Tap Mode**.

[Figure 12-6](#) shows the option to enable the inline-tap mode.

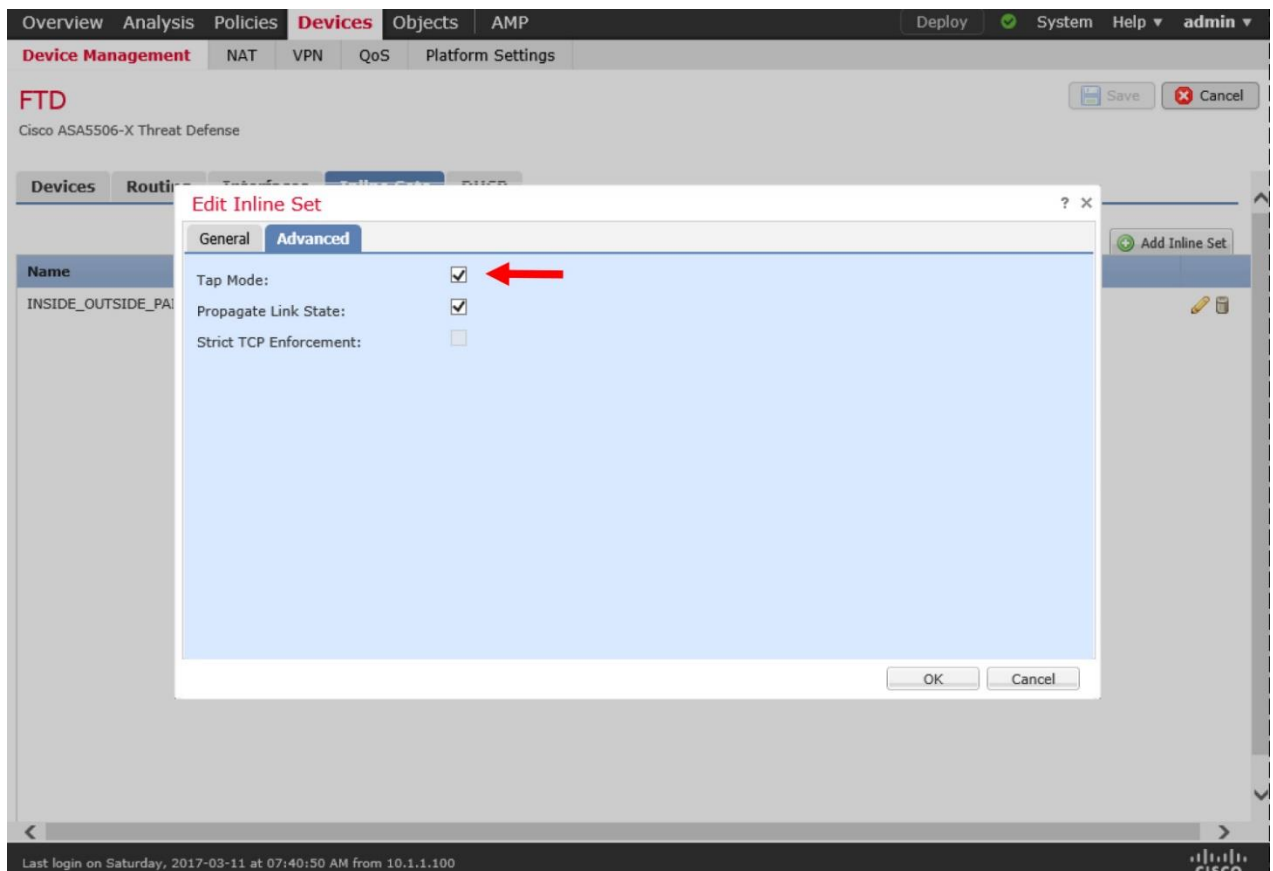


Figure 12-6. *Advanced Settings for an Inline Set Configuration*

Step 8. Select **OK** to return to the **Inline Sets** tab. Save the settings, and deploy the new changes.

Verification of a Configuration

Upon a successful deployment, you should be able to communicate from your inside host 192.168.1.2 to the outside server 192.168.1.200. The examples in this chapter use a TCP service, telnet, to test connectivity and generate a block event for it.

Note

The following steps assume that the FTD is running the same Access Control policy that you created in the previous chapter, which blocks any traffic destined to port 23 (telnet). If you revoked that policy, or skipped the previous chapter, please stop here. Read the [Chapter 11](#) to learn how to block telnet traffic in inline interface mode.

After you deploy an access control policy to block traffic with destination port 23, try to telnet into the outside system 192.168.1.200 from the inside host 192.168.1.2. You should be able to access the system successfully. You should also be able to view an event for the corresponding connections.

FTD generates only one event — for its “Block” action — when it is in inline mode. Because it logs an event at the beginning of a connection, and unable to see the rest of the connection. However, when an FTD is in detection-only mode, it generates multiple events — for “Block” and “Allow” actions — because it can see the entire connection without interrupting the flow.

Figure 12-7 shows two “Block” events that are generated in inline-tap and inline modes, at the beginning of a telnet connection.

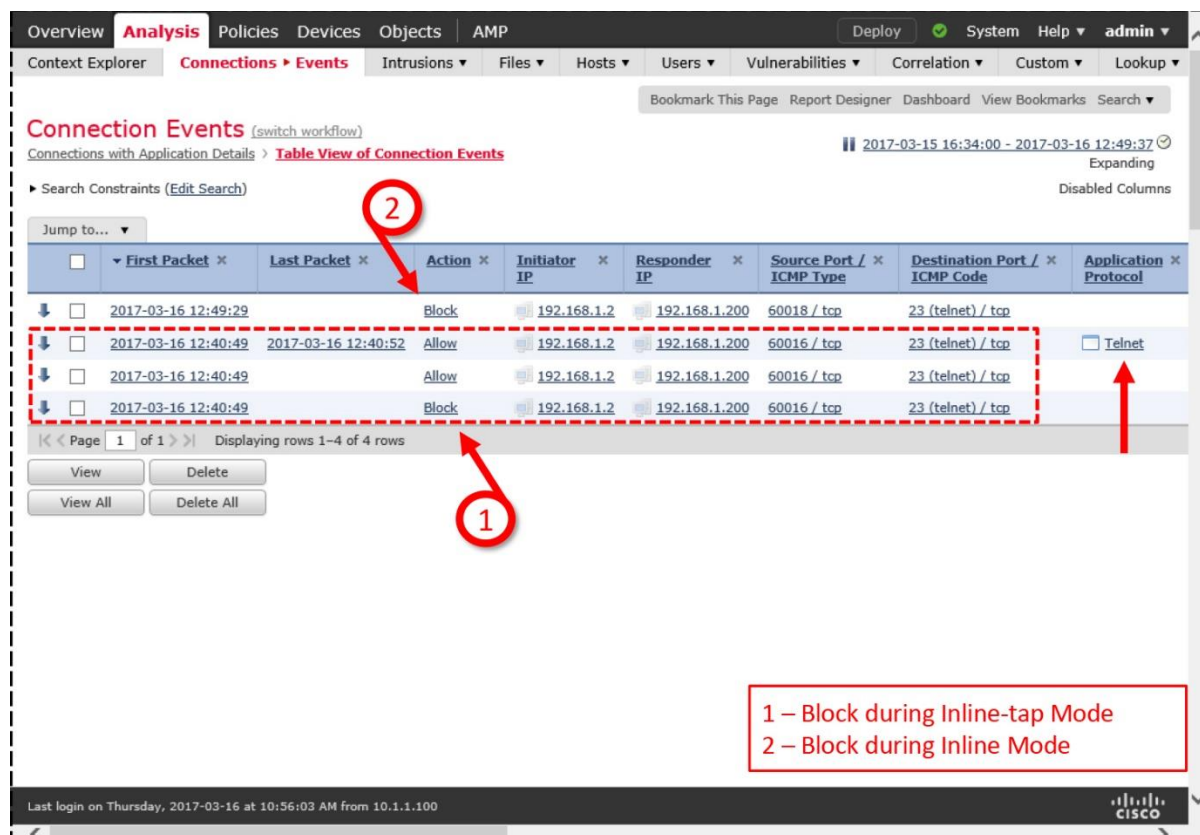


Figure 12-7. Connection Events for a Block Action in Inline-tap and Inline Modes

If a communication attempt fails, and the FMC does not indicate an error for it, you can begin troubleshooting using the CLI of the FTD.

Example 12-1 confirms that the interface set is in inline-tap mode. The command output displays various components of an inline set configuration, such as, member interfaces of an inline pair, their statuses and advanced settings.

Example 12-1 Tap Mode is Enabled on the INSIDE_OUTSIDE_PAIR Inline Set

```
> show inline-set
```

```
Inline-set INSIDE_OUTSIDE_PAIR
Mtu is 1500 bytes
Failsafe mode is on/activated
Failsecure mode is off
Tap mode is on
Propagate-link-state option is on
```

```

hardware-bypass mode is disabled
Interface-Pair[1]:
  Interface: GigabitEthernet1/1 "INSIDE_INTERFACE"
  Current-Status: UP
  Interface: GigabitEthernet1/2 "OUTSIDE_INTERFACE"
  Current-Status: UP
  Bridge Group ID: 0
>

```

[Example 12-2](#) demonstrates that the GigabitEthernet1/1 and GigabitEthernet1/2 interfaces are in the inline-tap mode. Both of them are part of an inline pair called INSIDE_OUTSIDE_PAIR. The command output also provides a detail statistic of the packets.

Example 12-2 *Status of Each Interface of an Inline Pair*

```

> show interface GigabitEthernet 1/1
Interface GigabitEthernet1/1 "INSIDE_INTERFACE", is up, line protocol is up
Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
  Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
  Input flow control is unsupported, output flow control is off
  MAC address a46c.2ae4.6bc0, MTU 1500
  IPS Interface-Mode: inline-tap, Inline-Set: INSIDE_OUTSIDE_PAIR
  IP address unassigned
  9241 packets input, 945431 bytes, 0 no buffer
  Received 89 broadcasts, 0 runts, 0 giants
.
.
> show interface GigabitEthernet 1/2
Interface GigabitEthernet1/2 "OUTSIDE_INTERFACE", is up, line protocol is
up
Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
  Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
  Input flow control is unsupported, output flow control is off
  MAC address a46c.2ae4.6bc1, MTU 1500
  IPS Interface-Mode: inline-tap, Inline-Set: INSIDE_OUTSIDE_PAIR
  IP address unassigned
  9065 packets input, 924609 bytes, 0 no buffer
  Received 30 broadcasts, 0 runts, 0 giants

```

Passive Interface Mode

A passive interface is simpler to configure than an inline set. You can employ just one interface to receive traffic from a mirror port. An egress interface is not necessary, as an FTD does not forward traffic in passive mode.

Configuration

An FTD supports both SPAN and ERSPAN ports, but they require additional configuration on a switch or router. However, you can install a plug and play tap that can mirror traffic without any additional software configuration.

The following example details the steps to connect an FTD passive interface with a SPAN port on a switch — one of the most common port mirroring options.

Passive Interface on an FTD

To configure a passive interface on FTD, the following steps are necessary:

Step 1. Login to the GUI of your FMC.

Step 2. Navigate to the **Devices > Device Management** page. A list of managed devices appear.

Step 3. Click the *pencil* icon next to the device name where you want to enable the passive interface mode. The device editor page appears.

Step 4. On the **Interfaces** tab, select an interface that will function in promiscuous mode. The interface will connect to a SPAN port on a switch. The **Edit Physical Interface** window appears.

[Figure 12-8](#) shows the configuration of GigabitEthernet1/1 interface as a passive interface.

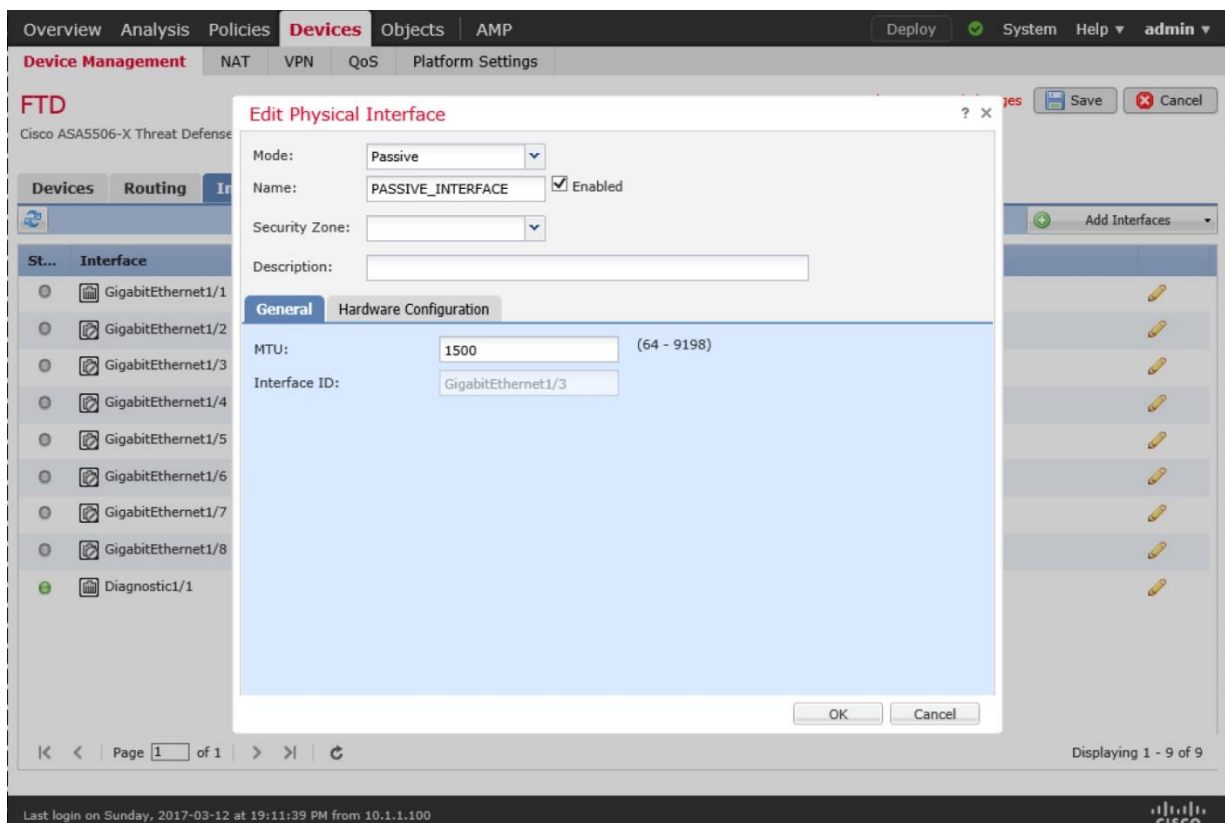


Figure 12-8. The “Edit Physical Interface” Window

Step 5. Using the **Mode** dropdown, select the **Passive** mode.

Step 6. Give a name to the interface, and select the **Enabled** checkbox.

Step 6. Click **OK** to return to the device editor page. Save the settings, and deploy the new configuration.

[Figure 12-9](#) shows an overview of the interfaces on FTD. Note that you do not need to copy an IP address and security zone for a passive interface.

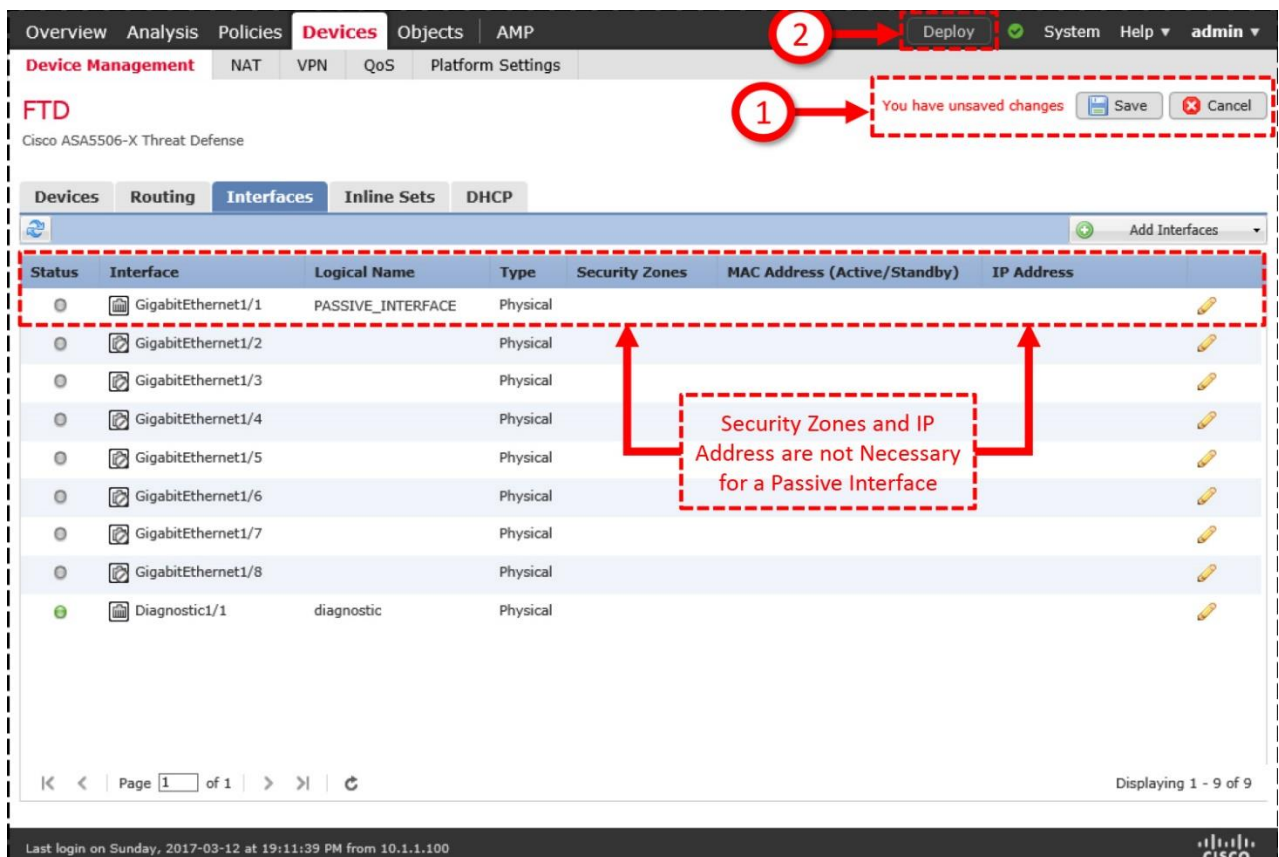


Figure 12-9. Overview of FTD Interface Configurations

SPAN Port on Switch

If you are using a Cisco switch to transmit mirrored traffic to an FTD, you have to define the source ports (the ports from where the traffic is copied) and a destination port (the port that sends duplicated traffic to an FTD).

[Example 12-3](#) shows the setup of a SPAN port on a Cisco Switch. According to the following configuration, this switch receives traffic on GigabitEthernet0/1 and GigabitEthernet0/2 interfaces, duplicates them, and retransmits the duplicated traffic through the GigabitEthernet 0/8 interface.

Example 12-3 Essential Commands to Configure a SPAN Port

```
Switch(config)# monitor session 1 source interface gigabitEthernet 0/1
Switch(config)# monitor session 1 source interface gigabitEthernet 0/2

Switch(config)# monitor session 1 destination interface g0/8
```

Verification of a Configuration

Once you complete configuration, transfer traffic between inside and outside systems. Although you applied the access control policy to block telnet traffic, FTD does not block any traffic in passive mode, it just generates events.

[Figure 12-10](#) shows three block actions that are generated in three different interface modes, during three telnet connection attempts.

The screenshot displays the Cisco FTD 'Connection Events' interface. The table below shows the events, with three specific rows highlighted by red dashed boxes and numbered 1, 2, and 3. A legend box on the right explains these numbers: 1 - Block during Inline-tap Mode, 2 - Block during Inline Mode, and 3 - Block during Passive Mode.

	First Packet	Last Packet	Action	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol
3	2017-03-16 12:57:20	2017-03-16 12:57:21	Allow	192.168.1.2	192.168.1.200	60020 / tcp	23 (telnet) / tcp	Telnet
	2017-03-16 12:57:20		Block	192.168.1.2	192.168.1.200	60020 / tcp	23 (telnet) / tcp	
2	2017-03-16 12:57:20		Allow	192.168.1.2	192.168.1.200	60020 / tcp	23 (telnet) / tcp	
	2017-03-16 12:49:29		Block	192.168.1.2	192.168.1.200	60018 / tcp	23 (telnet) / tcp	
	2017-03-16 12:40:49	2017-03-16 12:40:52	Allow	192.168.1.2	192.168.1.200	60016 / tcp	23 (telnet) / tcp	Telnet
	2017-03-16 12:40:49		Allow	192.168.1.2	192.168.1.200	60016 / tcp	23 (telnet) / tcp	
	2017-03-16 12:40:49		Block	192.168.1.2	192.168.1.200	60016 / tcp	23 (telnet) / tcp	

1 – Block during Inline-tap Mode
2 – Block during Inline Mode
3 – Block during Passive Mode

Figure 12-10. Block Actions of a Telnet Connection in Different Interface Modes

If a passive interface on an FTD does not see traffic, you need to check both devices — FTD and switch. The following examples demonstrates some commands that you run during investigation.

[Example 12-4](#) offers two useful commands that you can run on an FTD. First, enter the **show nameif** command to determine the active interfaces. Then, you can run the **show interface** command with the interface to identify the interface status, mode, traffic statistics, etc.

Example 12-4 Verification of a Passive Interface

```
> show nameif
Interface                               Name                               Security
GigabitEthernet1/1                     PASSIVE_INTERFACE                 0
Management1/1                           diagnostic                         0
>
```

```

> show interface GigabitEthernet 1/1
Interface GigabitEthernet1/1 "PASSIVE_INTERFACE", is up, line protocol is
up
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
    Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
    Input flow control is unsupported, output flow control is off
    MAC address a46c.2ae4.6bc0, MTU 1500
    IPS Interface-Mode: passive
    IP address unassigned
    289 packets input, 30173 bytes, 0 no buffer
    Received 7 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 pause input, 0 resume input
    0 L2 decode drops
    161 packets output, 17774 bytes, 0 underruns
    0 pause output, 0 resume output
    0 output errors, 0 collisions, 0 interface resets
    0 late collisions, 0 deferred
    0 input reset drops, 24 output reset drops
    input queue (blocks free curr/low): hardware (991/894)
    output queue (blocks free curr/low): hardware (1023/1018)
  Traffic Statistics for "PASSIVE_INTERFACE":
    104 packets input, 6520 bytes
    0 packets output, 0 bytes
    104 packets dropped
    1 minute input rate 0 pkts/sec, 0 bytes/sec
    1 minute output rate 0 pkts/sec, 0 bytes/sec
    1 minute drop rate, 0 pkts/sec
    5 minute input rate 0 pkts/sec, 0 bytes/sec
    5 minute output rate 0 pkts/sec, 0 bytes/sec
    5 minute drop rate, 0 pkts/sec
>

```

[Example 12-5](#) provides two useful commands that can confirm the SPAN port status on a switch.

Example 12-5 *Commands to Configure and Verify a SPAN Port*

```

Switch# show running-config | include monitor
monitor session 1 source interface Gi0/1 - 2
monitor session 1 destination interface Gi0/8
Switch#

```

```

Switch# show monitor session 1
Session 1
-----
Type                : Local Session
Source Ports        :
  Both               : Gi0/1-2
Destination Ports   : Gi0/8
Encapsulation       : Native
  Ingress            : Disabled

```

```

Switch#

```

Analysis of Operation

If a host experiences any connectivity issues in spite of deploying the FTD in detection-only mode, you can determine the root cause of an issue by analyzing the tracing information of a packet.

Connection Event with Block Action

In this section, you will analyze the packets that trigger connection events. There are two ways to analyze them — by capturing live traffic with the trace functionality, and by running the packet-tracer tool.

Analysis of Live Traffic

Follow the steps below to capture live telnet traffic, and analyze the flow a packet in inline-tap mode:

Step 1. Enter a capture rule with the **trace** keyword.

[Example 12-6](#) demonstrates the usages of the **trace** keyword with the **capture** command. It probes into the inside interface and matches any packets with destination port 23. The **Capturing – 0 bytes** message on the **show capture** command confirms that the process is running, but has not seen a packet yet.

Example 12-6 *Command to Capture Telnet Traffic with Tracing Information*

```
> capture telnet_inside trace interface INSIDE_INTERFACE match tcp any any
eq 23
>

> show capture
capture telnet_inside type raw-data trace interface INSIDE_INTERFACE
[Capturing - 0 bytes]
  match tcp any any eq telnet
>
```

Step 2. Initiate a telnet request from the inside host to the outside server. Although you enabled an access rule to block telnet traffic, the traffic is able to go through because the interface is in inline-tap mode.

[Example 12-7](#) shows the capture of 13 packets with destination port 23 (telnet). The output only displays three packets for brevity. Each packet has a sequence number on its left.

Example 12-7 *Capture of Telnet Traffic*

```
> show capture telnet_inside

13 packets captured

  1: 01:56:01.756735      192.168.1.2.59358 > 192.168.1.200.23: S
1923550801:1923550801(0) win 29200 <mss 1460,sackOK,timestamp 2340482
0,nop,wscale 7>
```

```

2: 01:56:01.757101      192.168.1.2.59358 > 192.168.1.200.23: . ack
2745314499 win 229 <nop,nop,timestamp 2340483 1541951>
3: 01:56:01.757239      192.168.1.2.59358 > 192.168.1.200.23: P
1923550802:1923550829(27) ack 2745314499 win 229 <nop,nop,timestamp 2340483
1541951>
.
.
<Output_Omitted_for_Brevity>

```

Step 3. From the above **show capture** output, select a packet you want to trace using its associated number on the left.

[Example 12-8](#) exhibits the tracing data of a telnet packet. Note the final action of the flow — *Access-list would have dropped, but packet forwarded due to inline-tap.*

Example 12-8 Detail Tracing Data of a Telnet Packet

```
> show capture telnet_inside packet-number 1 trace
```

```
13 packets captured
```

```

1: 01:56:01.756735      192.168.1.2.59358 > 192.168.1.200.23: S
1923550801:1923550801(0) win 29200 <mss 1460,sackOK,timestamp 2340482
0,nop,wscale 7>
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS
services will be applied

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: WOULD HAVE DROPPED
Config:
access-group CSM_FW_ACL_global
access-list CSM_FW_ACL_advanced deny tcp any any object-group TELNET rule-
id 268441600 event-log flow-start

```

```
access-list CSM_FW_ACL_ remark rule-id 268441600: ACCESS POLICY: AC Policy
- Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268441600: L4 RULE: Shell Access
object-group service TELNET tcp
  port-object eq telnet
Additional Information:
```

```
Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: Access-list would have dropped, but packet forwarded due to inline-
tap
```

```
1 packet shown
>
```

[Analysis of a Simulated Packet](#)

You can also use the **packet-tracer** tool to simulate the flow of a telnet packet through the FTD. The tool uses the active access control policy to simulate the packet flow.

[Example 12-9](#) simulates a telnet packet that would have dropped, but FTD forwards it due to the inline-tap interface mode setting.

Example 12-9 *Simulation of the Telnet Traffic through Inline-Tap Mode*

```
> packet-tracer input INSIDE_INTERFACE tcp 192.168.1.2 10000 192.168.1.200
23
```

```
Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
```

```
Phase: 2
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS
services will be applied
```

```
Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: WOULD HAVE DROPPED
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny tcp any any object-group TELNET rule-
id 268441600 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268441600: ACCESS POLICY: AC Policy
- Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268441600: L4 RULE: Shell Access
object-group service TELNET tcp
```

```
port-object eq telnet
Additional Information:
```

Result:

```
input-interface: INSIDE_INTERFACE
```

```
input-status: up
```

```
input-line-status: up
```

```
Action: Access-list would have dropped, but packet forwarded due to inline-tap
```

>

Intrusion Event with Inline Result

So far, you have analyzed the connection events when an FTD is deployed in passive or inline-tap mode. For an access rule with *Block* action, FMC shows a connection event with *Block* action while FTD allows the traffic to go through without an interruption. However, when a packet matches against an intrusion rule with *Drop and Generate Events* state, FMC shows a reason for logging the connection as well.

Note

Since this chapter is about inspecting traffic without blocking them, this section takes an opportunity to demonstrate the behavior of an FTD when you deploy an intrusion policy in a detection-only mode. It allows you to understand and compare different actions in different interface modes. However, to learn about the configuration and troubleshooting of an Intrusion policy, read the chapter on *Preventing Network from an Attack by Blocking an Intrusion Attempt*.

To understand various actions on connections and the reasons for their logging, this section deploys and analyzes an FTD in various interface modes with different intrusion policy settings. You will notice different behaviors on FTD when a host 192.168.1.2 attempts to connect to a telnet server 192.168.1.200 in different deployment scenarios.

[Table 12-1](#) highlights the deployment scenarios (1, 2, and 6) when the FTD “would have dropped” a packet. A gray color down-arrow under the **Inline Result** column confirms it. However, an FTD blocks a connection when it meets all three conditions together — interface mode is inline, intrusion rule state is set to **Drop and Generate Events**, and Intrusion Policy is configured with the **Drop when Inline** option enabled. In this case (scenario 5), the down-arrow turns into black.

Table 12-1. *Inline Result Behavior in Various Deployment Scenarios*

Scenario	Interface Mode	Intrusion Rule State	Drop When Inline Option	Connection Event (Action, Reason)	Intrusion Event (Inline Result)
1	Inline-tap	Drop and Generate	Enabled	Allow, Intrusion Block	Down Arrow (Gray)
2	Inline-tap	Drop and Generate	Disabled	Allow, Intrusion Block	Down Arrow (Gray)
3	Inline-tap	Generate	Enabled	Allow, Intrusion Monitor	Blank
4	Inline-tap	Generate	Disabled	Allow, Intrusion Monitor	Blank
5	Inline	Drop and Generate	Enabled	Block , Intrusion Block	Down Arrow (Black)
6	Inline	Drop and Generate	Disabled	Allow, Intrusion Block	Down Arrow (Gray)
7	Inline	Generate	Enabled	Allow, Intrusion Monitor	Blank
8	Inline	Generate	Disabled	Allow, Intrusion Monitor	Blank

Figure 12-11 exhibits different types of connection events in different deployment scenarios. Although the reasons for logging show **Intrusion Block**, FTD “allows” all of these connections (in scenario 1, 2, and 6) due to its interface modes and intrusion policies.

	First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code
↓	2017-08-30 20:53:59	2017-08-30 20:54:08	Allow	8 Intrusion Monitor	192.168.1.2	192.168.1.200	42664 / tcp	23 (telnet) / tcp
↓	2017-08-30 20:53:59		Allow		192.168.1.2	192.168.1.200	42664 / tcp	23 (telnet) / tcp
↓	2017-08-30 20:26:03	2017-08-30 20:26:17	Allow	7 Intrusion Monitor	192.168.1.2	192.168.1.200	42660 / tcp	23 (telnet) / tcp
↓	2017-08-30 20:26:03		Allow		192.168.1.2	192.168.1.200	42660 / tcp	23 (telnet) / tcp
↓	2017-08-30 20:10:23	2017-08-30 20:10:33	Allow	6 Intrusion Block	192.168.1.2	192.168.1.200	42656 / tcp	23 (telnet) / tcp
↓	2017-08-30 20:10:23		Allow		192.168.1.2	192.168.1.200	42656 / tcp	23 (telnet) / tcp
↓	2017-08-30 19:49:54	2017-08-30 19:50:21	Block	5 Intrusion Block	192.168.1.2	192.168.1.200	42654 / tcp	23 (telnet) / tcp
↓	2017-08-30 19:49:54		Allow		192.168.1.2	192.168.1.200	42654 / tcp	23 (telnet) / tcp
↓	2017-08-30 14:53:21	2017-08-30 14:53:30	Allow	4 Intrusion Monitor	192.168.1.2	192.168.1.200	40742 / tcp	23 (telnet) / tcp
↓	2017-08-30 14:53:21		Allow		192.168.1.2	192.168.1.200	40742 / tcp	23 (telnet) / tcp
↓	2017-08-30 14:35:58	2017-08-30 14:36:07	Allow	3 Intrusion Monitor	192.168.1.2	192.168.1.200	40738 / tcp	23 (telnet) / tcp
↓	2017-08-30 14:35:58		Allow		192.168.1.2	192.168.1.200	40738 / tcp	23 (telnet) / tcp
↓	2017-08-30 14:23:32	2017-08-30 14:23:40	Allow	2 Intrusion Block	192.168.1.2	192.168.1.200	40736 / tcp	23 (telnet) / tcp
↓	2017-08-30 14:23:32		Allow		192.168.1.2	192.168.1.200	40736 / tcp	23 (telnet) / tcp
↓	2017-08-30 14:04:57	2017-08-30 14:05:09	Allow	1 Intrusion Block	192.168.1.2	192.168.1.200	40734 / tcp	23 (telnet) / tcp
↓	2017-08-30 14:04:57		Allow		192.168.1.2	192.168.1.200	40734 / tcp	23 (telnet) / tcp

Figure 12-11. Connection Event — Action vs. Reason

Figure 12-12 displays three types of **Inline Result** — blank, gray arrow, and black arrow. The gray down-arrow indicates that the packet would have dropped, while the black arrow denotes a drop of original packet. All of these events in this example (and in the previous example) are created using same client host, same server host, and same application protocol.

Overview **Analysis** Policies Devices Objects AMP Deploy System Help admin

Context Explorer Connections **Intrusions Events** Files Hosts Users Vulnerabilities Correlation Custom Lookup

Bookmark This Page Report Designer Dashboard View Bookmarks Search

Events By Priority and Classification (switch workflow)

Drilldown of Event, Priority, and Classification > **Table View of Events** > Packets

2017-08-29 23:47:00 - 2017-08-30 21:39:48

Search Constraints (Edit Search)

Jump to...

	Time	Inline Result	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Generator	Application Protocol
8	2017-08-30 20:54:07		192.168.1.200	192.168.1.2	23 (telnet) / tcp	42664 / tcp	Standard Text Rule	Telnet
7	2017-08-30 20:26:11		192.168.1.200	192.168.1.2	23 (telnet) / tcp	42660 / tcp	Standard Text Rule	Telnet
6	2017-08-30 20:10:31		192.168.1.200	192.168.1.2	23 (telnet) / tcp	42656 / tcp	Standard Text Rule	Telnet
5	2017-08-30 19:50:21		192.168.1.200	192.168.1.2	23 (telnet) / tcp	42654 / tcp	Standard Text Rule	Telnet
4	2017-08-30 14:53:29		192.168.1.200	192.168.1.2	23 (telnet) / tcp	40742 / tcp	Standard Text Rule	Telnet
3	2017-08-30 14:36:06		192.168.1.200	192.168.1.2	23 (telnet) / tcp	40738 / tcp	Standard Text Rule	Telnet
2	2017-08-30 14:23:40		192.168.1.200	192.168.1.2	23 (telnet) / tcp	40736 / tcp	Standard Text Rule	Telnet
1	2017-08-30 14:05:09		192.168.1.200	192.168.1.2	23 (telnet) / tcp	40734 / tcp	Standard Text Rule	Telnet

Page 1 of 1 | Displaying rows 1-8 of 8 rows

View Copy Delete Review Download Packets

View All Copy All Delete All Review All Download All Packets

Understanding the "Inline Results"

Blank: FTD generated an event, but did not drop the original packet

Down Arrow ↓ in Gray Color: FTD would have dropped the packet

Down Arrow ↓ in Black Color: FTD dropped the packet

Modes that Trigger "Would Have Dropped" Event

- Inline-tap mode
- Passive mode
- Inline mode (Drop when Inline is disabled)

Last login on Wednesday, 2017-08-30 at 16:34:07 PM from 10.1.1.100

CISCO

Figure 12-12. Intrusion Event — Inline Result Appears as Blank, Gray Arrow, and Black Arrow

[Example 12-10](#) confirms that the Intrusion policy (Snort rule) of an FTD would have dropped a telnet packet, but FTD forwards it due to the inline-tap interface mode setting.

Example 12-10 Analysis of the Telnet Traffic through Inline-Tap Mode

```
> show capture telnet_inside packet-number 1 trace
```

```
36 packets captured
```

```
1: 19:39:24.086177      192.168.1.2.40744 > 192.168.1.200.23: S
2884265905:2884265905(0) win 29200 <mss 1460,sackOK,timestamp 6199376
0,nop,wscale 7>
```

```
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list
```

```
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
```

Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434432
access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: AC Policy - Default/1
access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Ingress interface INSIDE_INTERFACE is in NGIPS inline mode.
Egress interface OUTSIDE_INTERFACE is determined by inline-set configuration

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 257, packet dispatched to next module

Phase: 7
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 8
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Verdict: (block-packet) drop this packet

```
Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: Access-list would have dropped, but packet forwarded due to inline-
tap
```

```
1 packet shown
>
```

Summary

This chapter explains the configuration and operation of various detection-only modes of an FTD, such as, passive mode, inline-tap mode, and inline mode with Drop when Inline option disabled. It also provides various command line tools that you can utilize to determine the status of interfaces and traffic.

Quiz

1. Which of the following interface modes does not block a packet?

- a. Transparent Mode
- b. Routed Mode
- c. Inline-tap Mode
- d. All of the Above

2. Which of the following actions ensures the analysis of maximum traffic when it goes through an FTD?

- a. Use a SPAN port on a switch.
- b. Deploy a tap to replicate traffic.
- c. Configure inline-tap mode, instead of the passive mode.
- d. Any FTD model can handle all of the traffic, and ensures 100% detection.

3. Which of the following statement is true?

- a. Passive mode can work with just one interface, whereas an inline set requires at least two interfaces.
- b. Inline interface does not require an availability of port mirroring features, such as, tap or SPAN port.
- c. Transition between detection-only and prevention modes is faster and easier in inline-tap mode.

d. All of the above.

4. Which of the following commands shows if an interface mode is set to inline-tap?

a. `> show inline-tap`

b. `> show inline-set`

c. `> show interface ip brief`

d. `> show interface inline-tap`

Chapter 13. Handling of Encapsulated Traffic

FTD can analyze encapsulated traffic. It can take an action based on the outermost and innermost headers of an encapsulated packet. As of writing this book, FTD supports Generic Routing Encapsulation (GRE), IP-in-IP, IPv6-in-IP and Teredo encapsulation protocols. This chapter demonstrates how an FTD handles an encapsulated packet over a tunnel.

Essential Knowledge

An Encapsulation protocol, also known as tunneling protocol, is used to mask the original IP header of a packet, and encapsulate with a completely different IP header. Routers can leverage this protocol to transport certain type of traffic that may not be allowed via the underlying network. Some of that traffic include but not limited to multicast traffic, non-routable IP traffic, and non-IP traffic. Through this technology, a user is able to access a network or service that may be denied in the original network.

This chapter uses GRE encapsulation protocol in its configuration examples. In GRE, one tunnel endpoint encapsulates data packets with an additional header and forward them to another tunnel endpoint for de-capsulation. A router acts as a GRE tunnel endpoint.

[Figure 13-1](#) shows how a GRE header and an IP header (outer) encapsulate a TCP header and its original IP header (inner).

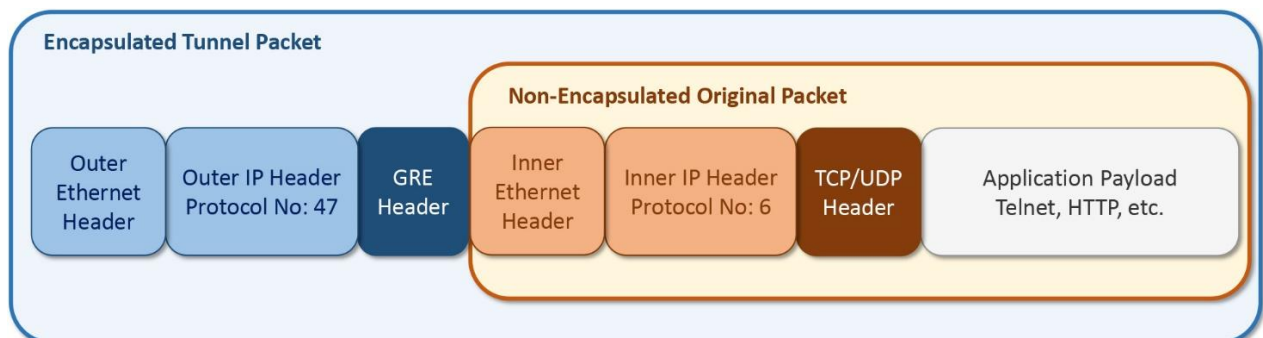


Figure 13-1. *GRE Encapsulated Packet*

You can deploy a prefilter policy on FTD to analyze the encapsulated packets based on their outermost headers. When a packet matches with a rule on a Prefilter policy, FTD takes an action accordingly before the packet hits any other security policies.

[Figure 13-2](#) illustrates how a prefilter policy can act as a gatekeeper to the rest of the security policies.

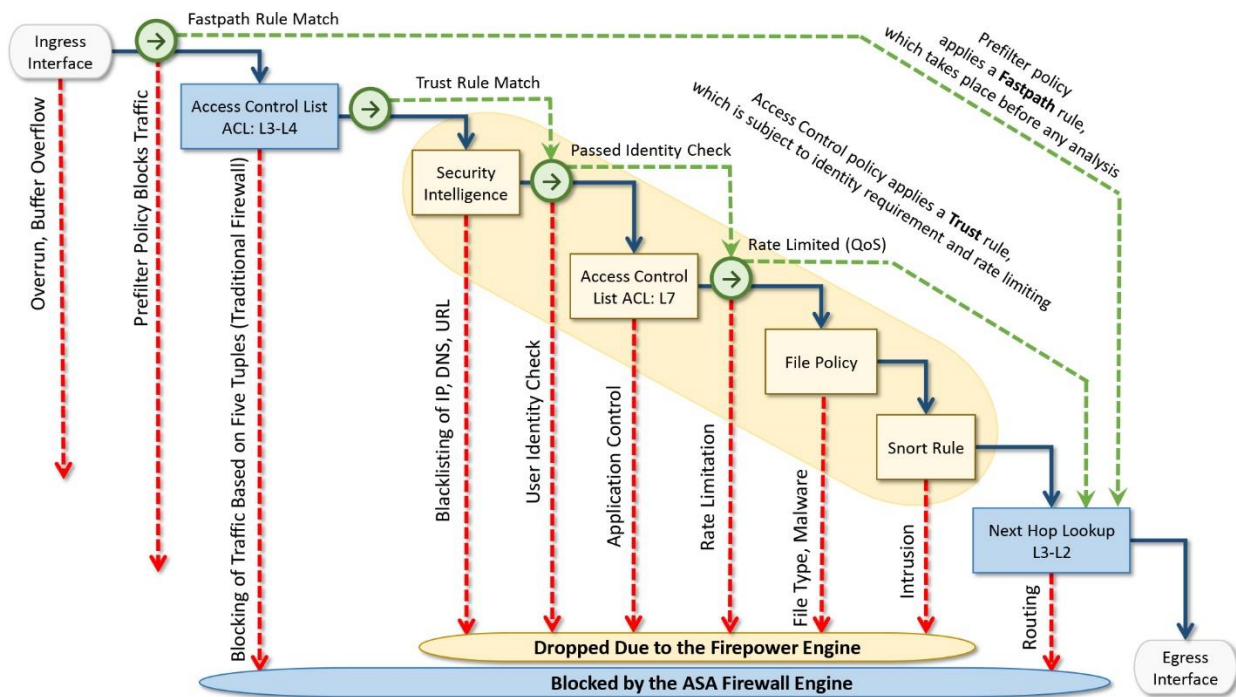


Figure 13-2. Position of a Prefilter Policy in the Workflow

FTD, by default, enables a default prefilter policy. You can change the settings of the default policy. However, you cannot delete this system-provided policy, nor add a new rule to this policy. The only configurable option is the default action. You can choose between the **Analyze all tunnel traffic** and **Block all tunnel traffic**.

A custom Prefilter policy allows you to add a **Tunnel Rule**, which can offer granular control over the tunnel traffic. Using a custom tunnel rule, you can bypass the encapsulated pass-through traffic from any further inspection.

This chapter uses both — the default policy and a custom policy — to demonstrate the flow of an encapsulated packet in various conditions.

Best Practices

Using a prefilter policy, when you define an action for the encapsulated traffic, any other remaining non-encapsulated traffic are forwarded to the next level of inspection automatically. You do not need to create a separate prefilter rule to allow the non-encapsulated traffic.

Prerequisites

This chapter assumes that you have prior experience with GRE protocol implementation. In addition, to prepare a lab for this chapter, you need to complete the following tasks:

- Deploy an FTD between two routers, and configure a simple GRE tunnel between them. FTD must be able to see all of the traffic between the routers.
- Build two pairs of subnetworks — one subnet pair transfers traffic over an encapsulated tunnel, and the other pair uses regular non-encapsulated network. You can use either physical hosts or loopback interfaces to represent the endpoints.

Figure 13-3 exhibits two subnets in each location — branch office and data center. The Network 2 (in Branch office) and the Network 200 (in Data Center) are connected over a GRE tunnel. The remaining subnets (Network 1 and Network 100) use the non-encapsulated route.

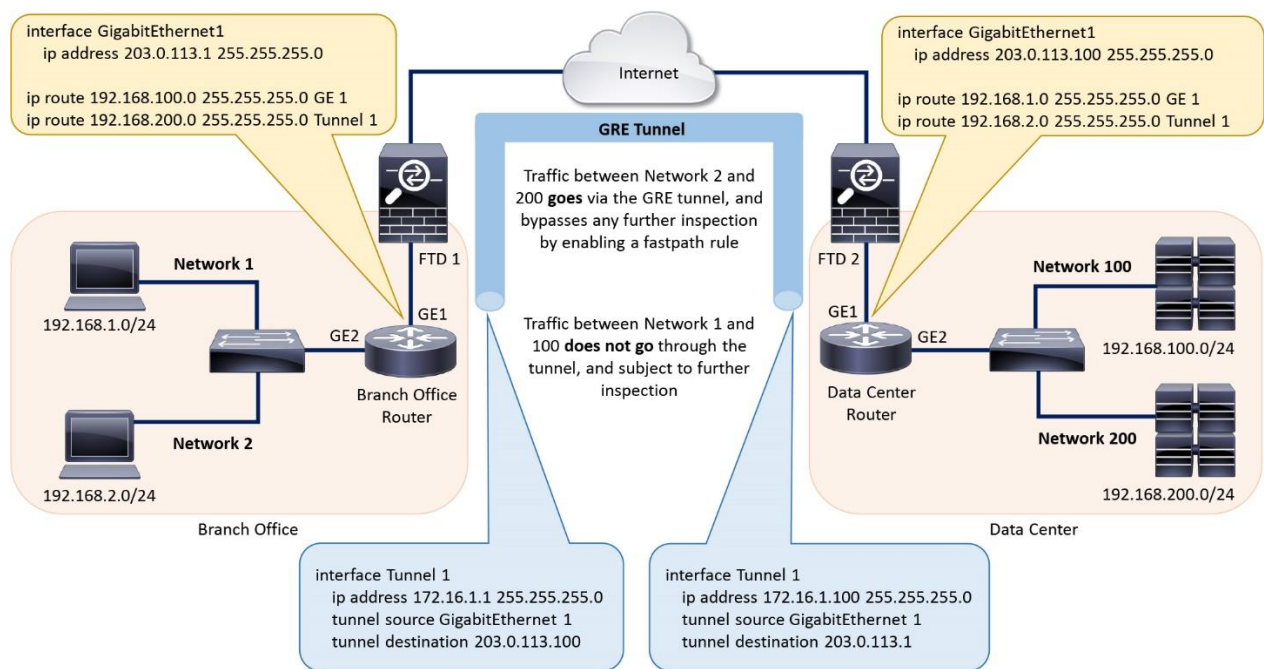


Figure 13-3. Lab Topology Used in the Configuration Examples of this Chapter

Table 13-1 shows a summary of the addressing scheme used in this chapter. The lab exercises in this chapter demonstrate that when the Network 2 and Network 200 communicate, the traffic uses the GRE tunnel, and subjects to the action in a Prefilter policy. The packet flow between Network 1 and Network 100 always remain the same, regardless of an action you define for tunnel traffic.

Table 13-1. Overview of the IP Addresses Used in this Lab

Label	Location	Subnet	Packet Header
Network 1	Branch	192.168.1.0/24	Not encapsulated
Network 2	Branch	192.168.2.0/24	Encapsulated
Network 100	Data Center	192.168.100.0/24	Not encapsulated
Network 200	Data Center	192.168.200.0/24	Encapsulated

- To demonstrate a TCP connection between the subnetworks, this chapter uses telnet service. The method to initiate a telnet connection varies — depends on the telnet client or operating system you use. This book assumes that you know how to establish a telnet connection.

Transfer and Capture of Traffic on Firewall Engine

To examine the flows of both encapsulated and non-encapsulated packets through an FTD, enable two independent capture processes — one for GRE encapsulated packet and the other one is for non-encapsulated telnet packet.

```
> capture gre_traffic trace interface INSIDE_INTERFACE match gre any any
> capture telnet_traffic trace interface INSIDE_INTERFACE match tcp any any
eq 23
>
```

Make sure that the capture is running, but not capturing any data until you manually send traffic.

[Example 13-1](#) confirms that the capture process is running. The “0 bytes” indicates that the FTD has not received any packets.

Example 13-1 *Capture is Running, But FTD has not Received Any Packets to Capture*

```
> show capture
capture gre_traffic type raw-data trace interface INSIDE_INTERFACE
[Capturing - 0 bytes]
  match gre any any
capture telnet_traffic type raw-data trace interface INSIDE_INTERFACE
[Capturing - 0 bytes]
  match tcp any any eq telnet
>
```

Step 1. First, connect to host 192.168.100.1/24 from the host 192.168.1.1/24 using telnet application. It should generate non-encapsulated telnet packets. You can verify it by viewing the capture process:

[Example 13-2](#) demonstrates that the telnet connection between the 192.168.1.1/24 and 192.168.100.1/24 triggers the *telnet_traffic* access rule, and generated 3572 bytes of traffic.

Example 13-2 *Capture is Running — FTD has Captured Telnet Packets*

```
> show capture
capture gre_traffic type raw-data trace interface INSIDE_INTERFACE
[Capturing - 0 bytes]
  match gre any any
capture telnet_traffic type raw-data trace interface INSIDE_INTERFACE
[Capturing - 3572 bytes]
  match tcp any any eq telnet
>
```


Note

The method to initiate a telnet connection varies — depends on the telnet client you use. You can use any tool, or an operating system to establish a telnet connection.

Step 2. Next, connect to host 192.168.200.1/24 from the host 192.168.2.1/24 using the telnet application. It should generate GRE encapsulated packets. Although you have used telnet application, the packets have TCP header inside, and the GRE header outside. You can verify it by viewing the GRE traffic statistics in the capture process:

[Example 13-3](#) shows that the telnet connection between the 192.168.2.1/24 and 192.168.200.1/24 triggers the *gre_traffic* access rule, instead of the *telnet_traffic* access rule. It proves that the telnet connection between these two subnets use GRE tunnel.

Example 13-3 *FTD Captures GRE Packets After Sending Traffic Over the Tunnel*

```
> show capture
capture gre_traffic type raw-data trace interface INSIDE_INTERFACE
[Capturing - 4748 bytes]
  match gre any any
capture telnet_traffic type raw-data trace interface INSIDE_INTERFACE
[Capturing - 3572 bytes]
  match tcp any any eq telnet
>
```

Note

Hosts in this lab use two different paths to transfer encapsulated and non-encapsulated traffic. The Prerequisites section of this chapter illustrates the routing on a diagram.

To clear the previously captured packets from the memory, and to begin the capture again, run the **clear capture** command:

```
> clear capture /all
```

Scenario 1: Analyzing Encapsulated Traffic

In the first scenario, you will enable the analysis of encapsulated traffic. Here are the steps you are going to perform, in summary:

Step 1. Configure the Prefilter and Access Control policies on FMC, and deploy them on FTD.

Step 2. Transfer traffic through the encapsulated tunnel and non-encapsulated path.

Step 3. Capture packets with tracing data for further analysis.

Configuration of Policies to Analyze Encapsulated Traffic

To analyze encapsulated traffic, Firepower System uses the settings from both policies — Prefilter policy and Access Control policy. A Prefilter policy allows you to select an encapsulation protocol and an action on encapsulated traffic. An Access Control policy

invokes a Prefilter policy and deploys it on your FTD. By default, a new Access Control policy invokes the settings from the system-provided **Default Prefilter Policy**.

Tip

If your goal is to simply *analyze* or *block* “all tunnel traffic”, select a default action in the **Default Prefilter Policy**. It keeps the configuration simple. However, if you need separate Tunnel Rules for different types of encapsulated traffic, create a custom Prefilter policy. A Default Prefilter Policy does not allow you to add custom rule.

Prefilter Policy Settings

To verify the settings of the **Default Prefilter Policy**, go to the **Policies > Access Control > Prefilter** page. Use the pencil icon to edit the default prefilter policy.

[Figure 13-4](#) shows the Prefilter policy page. By default, FTD provides the **Default Prefilter Policy**, and uses it in an Access Control policy.

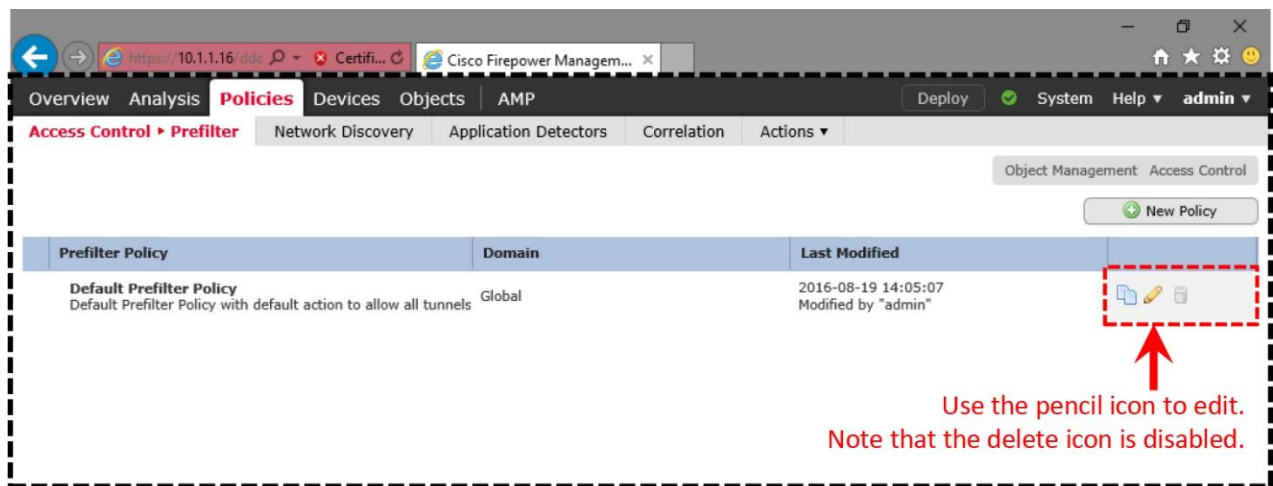


Figure 13-4. The Prefilter Policy Page Shows the System Provided Default Policy

To analyze encapsulated traffic, select **Analyze all tunnel traffic** option. It allows an FTD to forward an encapsulated packet to the next level of inspection.

Figure 13-5 shows the configurable options within the Default Prefilter Policy. You cannot add rules to the Default Prefilter Policy; you can only select a default action from the drop-down.

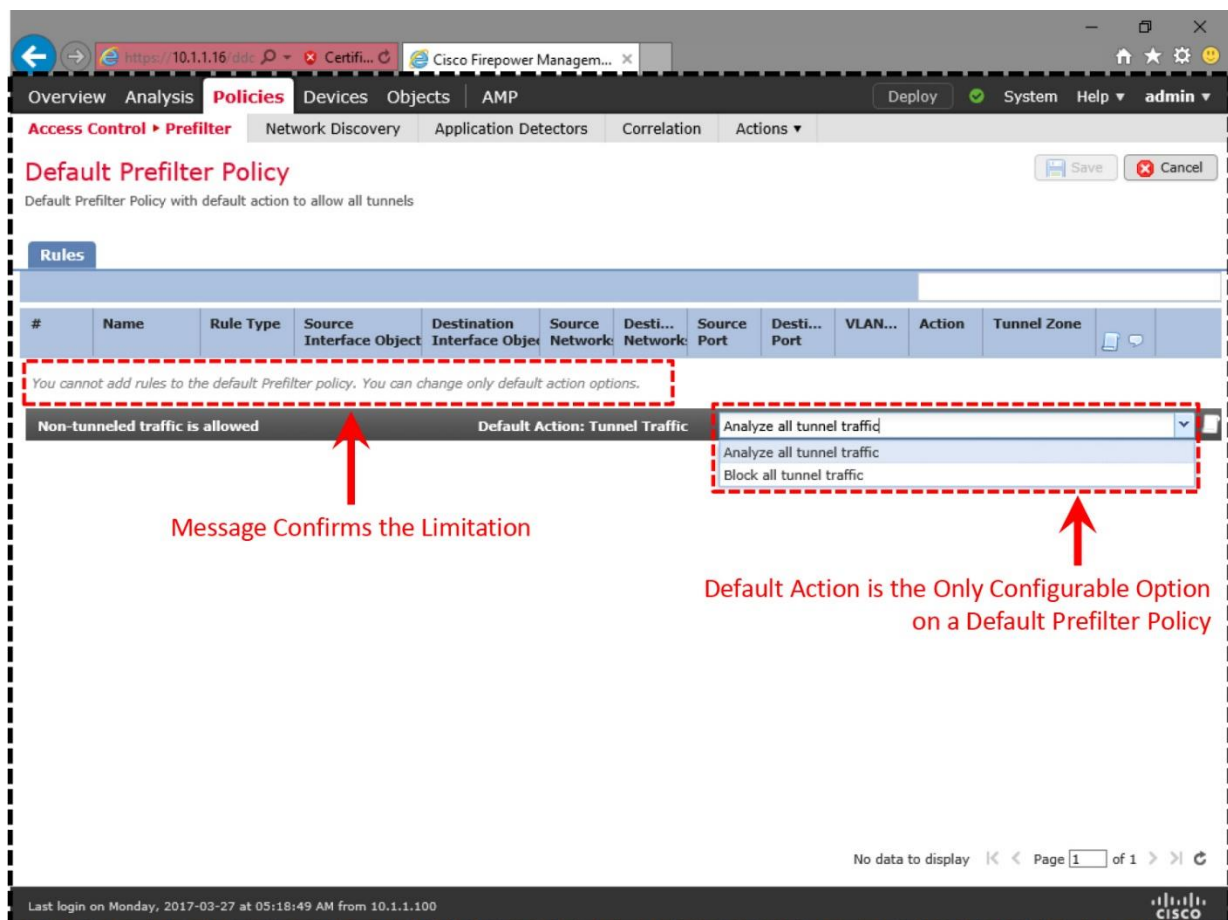


Figure 13-5. Settings for the Default Prefilter Policy

Access Control Policy Settings

By default, FTD does not generate a connection event when an access control policy has no access rule. You can change this behavior by enabling logging for the default action of an Access Control policy. Receiving connection events for a default action indicates that traffic is going through the Access Control Policy. Therefore, the lab exercises in this chapter does not use a custom access rule.

Figure 13-6 shows the selection of **Intrusion Prevention: Balanced Security and Connectivity** as the default action. Select the logging icon located next to the default action drop down. A logging configuration window appears.

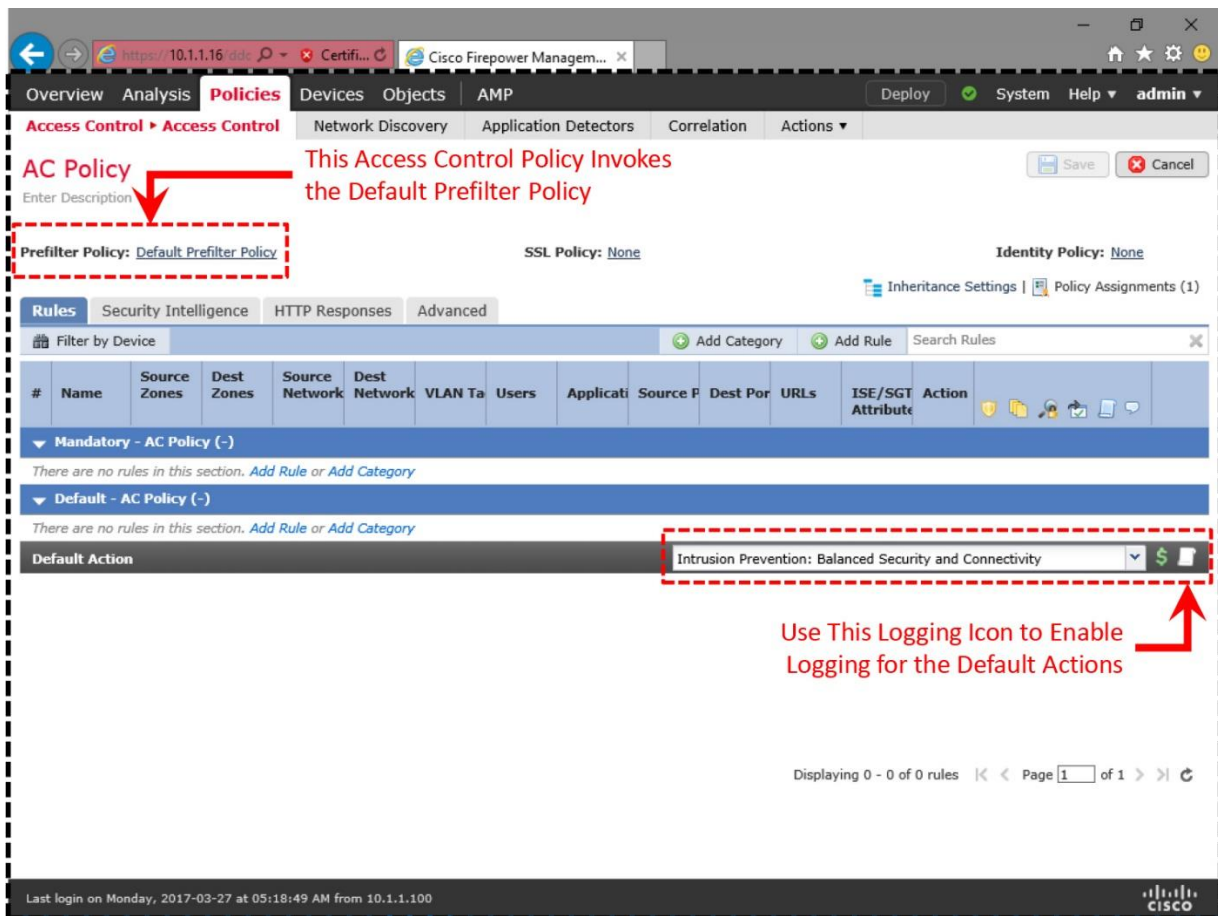


Figure 13-6. The Access Control Policy Editor Page

[Figure 13-7](#) shows the **Logging** configuration window. Enable logging either at the beginning or at the end of a connection, not for both, because it can affect the system performance.

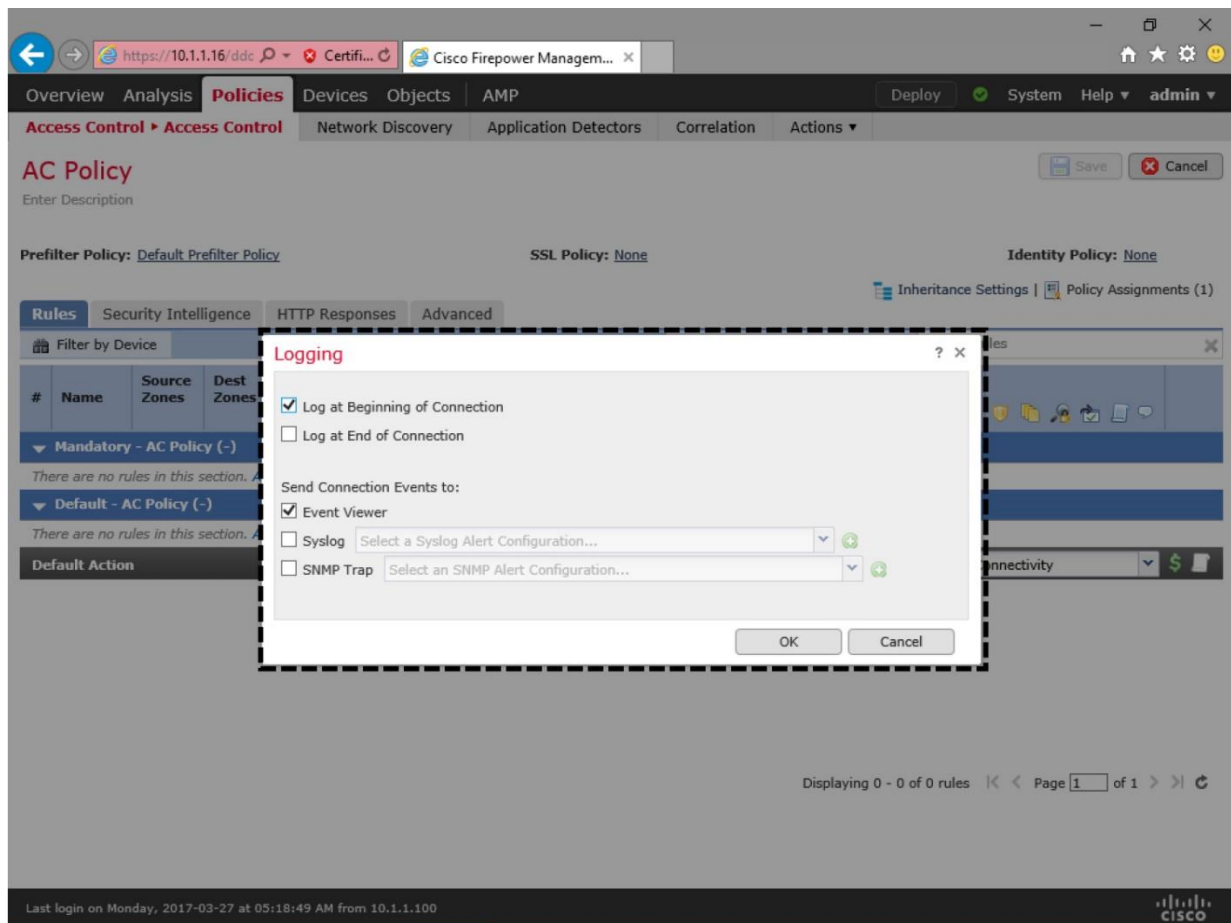


Figure 13-7. *Enablement of Logging for the Default Action*

After you make any changes on the Prefilter or Access Control policies, you must save the settings, and redeploy the Access Control policy to activate the new changes.

Verification of Configuration and Connection

You have configured the policies to generate connection events for both types of traffic — encapsulated and non-encapsulated. To verify its operations, you need to capture traffic from the ASA firewall engine. If a capture is already running, you can remove the previously captured packets by running the **clear capture** command:

```
> clear capture /all
```

Note

The steps for capturing telnet and GRE traffic is described in the *Transfer and Capture of Traffic on Firewall Engine* section of this chapter. If you want to learn more about packet capture option, read the [Chapter 10 - Capture of Traffic for Advance Analysis](#) for detail.

Once you enable the captures, use telnet to connect to the Network 100 from the Network 1. Similarly, connect to the Network 200 from the Network 2. Both connection attempts should be successful. You can view the associated connection events on the FMC.

Figure 13-8 shows two connection events for two separate telnet connections — originated from Network 1 and Network 2. Since an FTD can analyze the inner header of an encapsulated packet, FMC shows the original IP address — not the address on the outermost header — in a connection event.

Connection Events (switch workflow)

Connections with Application Details > Table View of Connection Events

2017-03-27 06:43:49 - 2017-03-27 09:01:54

Search Constraints (Edit Search)

First Packet	Action	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Access Control Rule	Tunnel/Prefilter Rule
2017-03-27 08:59:01	Allow	192.168.2.1	192.168.200.1	35575 / tcp	23 (telnet) / tcp	Default Action	Default Action
2017-03-27 08:57:33	Allow	192.168.1.1	192.168.100.1	46774 / tcp	23 (telnet) / tcp	Default Action	Default Action

Page 1 of 1 | Displaying rows 1-2 of 2 rows

View Delete View All Delete All

Last login on Monday, 2017-03-27 at 05:18:49 AM from 10.1.1.100

Figure 13-8. Connection Events due to Encapsulated and Non-encapsulated Traffic

If you do not see the events as shown in Figure 13-8, make sure you enabled logging for default action. You can verify the logging settings by running the **show access-control-config** command. If you did not enable it, read the *Configuration of Policies to Analyze Encapsulated Traffic* section to learn the process.

[Example 13-4](#) confirms that the default action of the Access Control policy is configured to generate log at the beginning of a connection.

Example 13-4 *Verification of the Setting for the Default Action*

```
> show access-control-config

===== [ AC Policy ] =====
Description           :
Default Action        : Allow
Default Policy        : Balanced Security and Connectivity
Logging Configuration
  DC                  : Enabled
  Beginning           : Enabled
  End                 : Disabled
Rule Hits             : 0
Variable Set          : Default-Set
.
.
.
! Type 'q' to quit
<Output Omitted for Brevity>
```

If you do not see an expected connection event, you can turn on the **firewall-engine-debug** tool to determine if (and why) a packet goes through the engines. As an access rule inspects a packet, the tool displays the internal ID for an active rule and its associated action in real time.

[Example 13-5](#) shows debug messages for both encapsulated and non-encapsulated telnet connections. If FTD generates debug messages during both connection attempts, it confirms that the Firepower inspection engines are able to see and inspect traffic inside and outside of a tunnel.

Example 13-5 *Debug of the Firewall Engine*

```
> system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages

! The following messages appear when you connect to 192.162.100.1/24 from
the host
192.168.1.1/24 over the non-encapsulated path. It triggers the default
action (rule
id: 268434432) on the Access Control policy:
.
192.168.1.1-43286 > 192.168.100.1-23 6 AS 5 I 1 New session
192.168.1.1-43286 > 192.168.100.1-23 6 AS 5 I 1 using HW or preset rule
order 2, id
268434432 action Allow and prefilter rule 0
192.168.1.1-43286 > 192.168.100.1-23 6 AS 5 I 1 allow action
192.168.1.1-43286 > 192.168.100.1-23 6 AS 5 I 1 Deleting session
.
```

```

.
! The following output appears when you connect to 192.162.200.1/24 from
the host
192.168.2.1/24 over the GRE tunnel. It triggers the prefilter rule id 9988:
.
192.168.2.1-23208 > 192.168.200.1-23 6 AS 5 I 0 New session
192.168.2.1-23208 > 192.168.200.1-23 6 AS 5 I 0 using prefilter rule 9998
with tunnel
zone -1
192.168.2.1-23208 > 192.168.200.1-23 6 AS 5 I 0 Starting with minimum 0, id
0 and
SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:
untagged, svc 0,
payload 0, client 0, misc 0, user 9999997, url , xff
192.168.2.1-23208 > 192.168.200.1-23 6 AS 5 I 0 match rule order 2, id
268434432
action Allow
192.168.2.1-23208 > 192.168.200.1-23 6 AS 5 I 0 allow action
.
.
<Output Omitted for Brevity>

```

If you want to know the exact rule that trigger a message on the firewall-engine-debug output, first, take a note of the rule ID from the debug output, and then, find it in the list of active access rules.

[Example 13-6](#) shows the list of active access rules on an FTD. You can find any tunnel, prefilter and access rules with their associated internal rule IDs in this list.

Example 13-6 *Verification of the Prefilter Policy Configuration Using the CLI*

```

> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list CSM_FW_ACL_ ; 6 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY:
Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL
ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998
(hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit 41 any any rule-id 9998
(hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 5 advanced permit gre any any rule-id 9998
(hitcnt=3) 0x52c7a066
access-list CSM_FW_ACL_ line 6 advanced permit udp any eq 3544 any range
1025 65535 rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 7 advanced permit udp any range 1025 65535 any
eq 3544 rule-id 9998 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 8 remark rule-id 268434432: ACCESS POLICY: AC
Policy - Default/1
access-list CSM_FW_ACL_ line 9 remark rule-id 268434432: L4 RULE: DEFAULT
ACTION RULE
access-list CSM_FW_ACL_ line 10 advanced permit ip any any rule-id
268434432 (hitcnt=2) 0xald3780e
>

```


Analysis of Packet Flows

Now that you have captured the telnet and GRE packets, you can retrieve any particular captured packets directly on the CLI of your FTD. Remember, in order to view the detail tracing data of a packet, you must add the **trace** keyword during the capture process. To learn more, read the *Transfer and Capture of Traffic on Firewall Engine* section.

[Example 13-7](#) displays the output of the **show capture** command. You can view the three-way handshake (SYN, SYN-ACK, and ACK) of a TCP connection. Each packet is assigned with a number (on the left side of each row) that you use during further analysis.

Example 13-7 Retrieval of the Non-Encapsulated Telnet Packets

```
> show capture telnet_traffic

49 packets captured

  1: 12:57:33.942105      192.168.1.1.46774 > 192.168.100.1.23: S
636710801:636710801(0) win 4128 <mss 536>
  2: 12:57:33.945706      192.168.100.1.23 > 192.168.1.1.46774: S
1516450804:1516450804(0) ack 636710802 win 4128 <mss 536>
  3: 12:57:33.947140      192.168.1.1.46774 > 192.168.100.1.23: . ack
1516450805 win 4128
  4: 12:57:33.947186      192.168.1.1.46774 > 192.168.100.1.23: P
636710802:636710814(12) ack 1516450805 win 4128
.
.
<Output Omitted for Brevity>
```

[Example 13-8](#) demonstrates the detail flow of a captured packet. The following example uses packet number 1, which is a SYN packet from 192.168.1.1 to 192.168.100.1.

Example 13-8 Analysis of a Non-Encapsulated Telnet Packet

```
> show capture telnet_traffic packet-number 1 trace

49 packets captured

  1: 12:57:33.942105      192.168.1.1.46774 > 192.168.100.1.23: S
636710801:636710801(0) win 4128 <mss 536>
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
```

Phase: 3
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434432
access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: AC Policy - Default/1
access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Ingress interface INSIDE_INTERFACE is in NGIPS inline mode.
Egress interface OUTSIDE_INTERFACE is determined by inline-set configuration

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 102, packet dispatched to next module

Phase: 7
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 8
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet

Result:
input-interface: INSIDE_INTERFACE
input-status: up

```
input-line-status: up
Action: allow
```

```
1 packet shown
>
```

[Example 13-9](#) exhibits the packets encapsulated with GRE headers (IP protocol number 47). The external IP address 203.0.113.1 represents the internal host 192.168.1.1. Each packet has a reference number (on the left side of each row) that you can use later during flow analysis.

Example 13-9 *Retrieval of the Encapsulated GRE Packets*

```
> show capture gre_traffic
```

```
49 packets captured
```

```
  1: 12:59:01.441536      203.0.113.1 > 203.0.113.100:  ip-proto-47,
length 48
  2: 12:59:01.444190      203.0.113.100 > 203.0.113.1:   ip-proto-47,
length 48
  3: 12:59:01.446525      203.0.113.1 > 203.0.113.100:  ip-proto-47,
length 44
  4: 12:59:01.446571      203.0.113.1 > 203.0.113.100:  ip-proto-47,
length 56
  5: 12:59:01.446601      203.0.113.1 > 203.0.113.100:  ip-proto-47,
length 44
  6: 12:59:01.449378      203.0.113.100 > 203.0.113.1:   ip-proto-47,
length 44
  7: 12:59:01.450156      203.0.113.100 > 203.0.113.1:   ip-proto-47,
length 56
  8: 12:59:01.450217      203.0.113.100 > 203.0.113.1:   ip-proto-47,
length 84
.
.
<Output Omitted for Brevity>
```

[Example 13-10](#) shows tracing data of a GRE encapsulated packet. Since this is a tunnel traffic, the default Prefilter policy forwards it to the inspection engines for further analysis.

Example 13-10 *Analysis of an GRE Encapsulated Packet*

```
> show capture gre_traffic packet-number 1 trace
```

```
49 packets captured
```

```
  1: 12:59:01.441536      203.0.113.1 > 203.0.113.100:  ip-proto-47,
length 48
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
```

Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Ingress interface INSIDE_INTERFACE is in NGIPS inline mode.
Egress interface OUTSIDE_INTERFACE is determined by inline-set configuration

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 103, packet dispatched to next module

Phase: 7
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 8
Type: SNORT
Subtype:
Result: ALLOW

Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet

Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: allow

1 packet shown
>

Scenario 2: Blocking Encapsulated Traffic

In the second scenario, FTD blocks tunnel traffic due to a configuration on the **Default Prefilter Policy**. The physical topology or the router configurations remain unchanged.

Configuration of Policies to Block Encapsulated Traffic

In order to block all tunnel traffic, you can use the FTD default prefilter policy. However, if you want to block tunnel traffic from a particular source and destination, you need to add a Prefilter rule for it. This exercise uses the default prefilter policy, as the goal is to analyze the flow of a blocked packet over the tunnel.

Step 1. Go to Policies > Access Control > Prefilter.

Step 2. se the *pencil* icon to edit the Default Prefilter Policy.

Step 3. In the policy editor page, use the **Default Action** drop-down to select **Block all tunnel traffic**.

[Figure 13-9](#) shows the selection of the **Block all tunnel traffic** option in the **Default Prefilter Policy**.

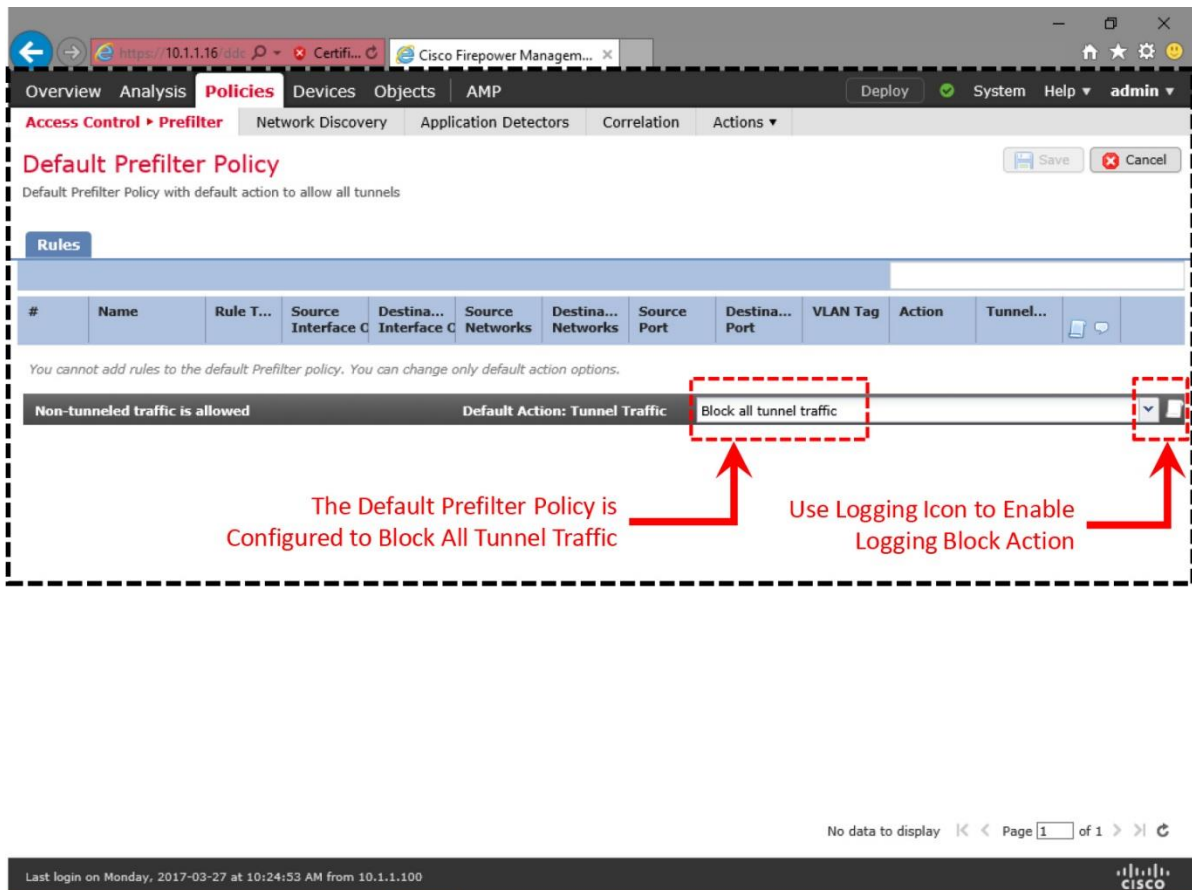


Figure 13-9. Prefilter Policy is Set to Block All Tunnel traffic

Step 4. Optionally, use the logging icon, next to the drop-down, to enable logging when the **Default Prefilter Policy** block any tunnel traffic.

Figure 13-10 shows the enablement of logging at the beginning of connection.

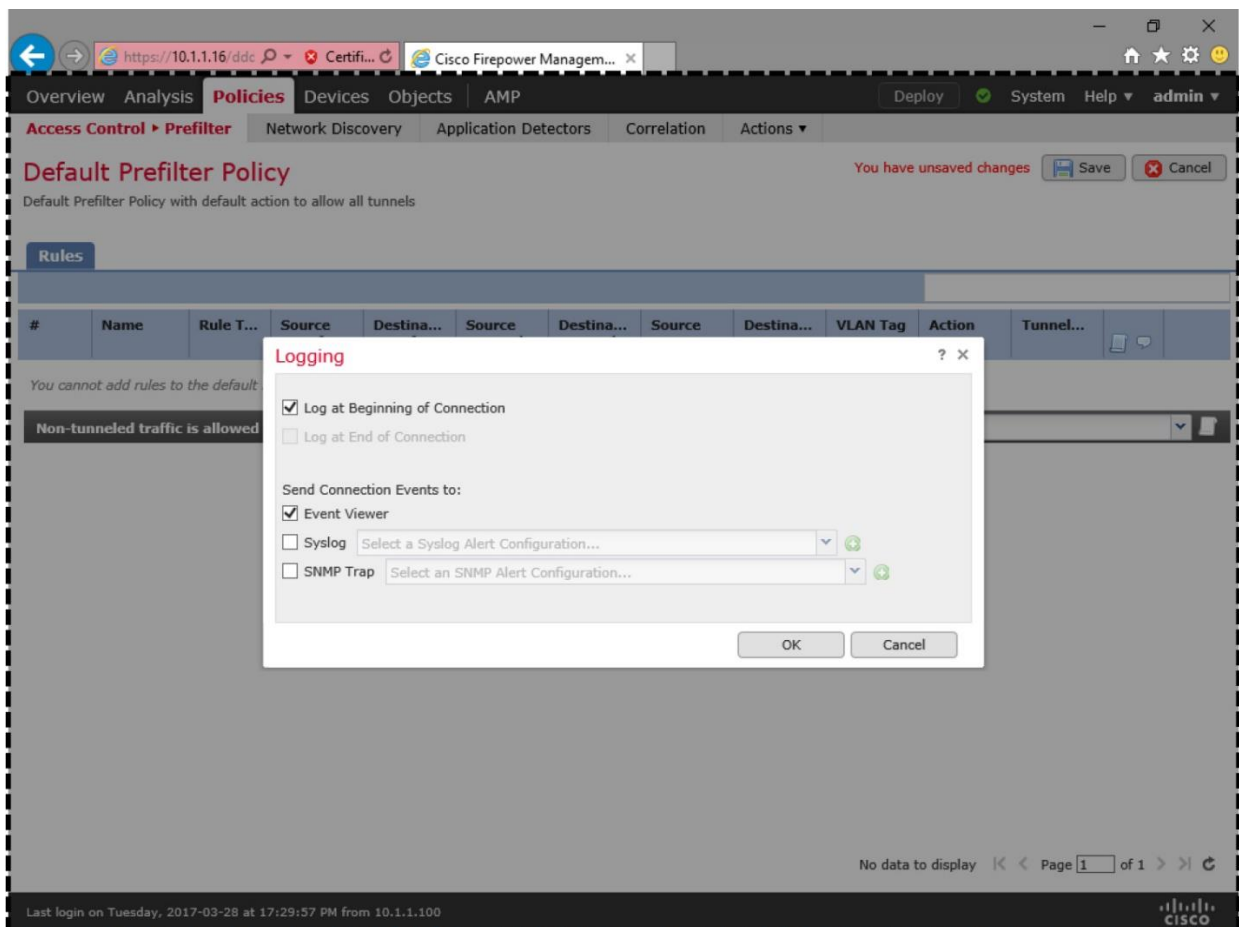


Figure 13-10. Logging for the Block Action on the Default Prefilter Policy

Step 5. Save the policy, and deploy it to your FTD.

Verification of Configuration and Connection

You have just reconfigured the prefilter policy to block all tunnel traffic. To verify its operation, enable two independent captures for telnet and GRE traffic. If the FTD has been running capture since the earlier lab exercise (Scenario 1), you can just remove any previously captured packets by running the **clear capture** command:

```
> clear capture /all
```

Note

The steps for capturing telnet and GRE traffic is described in the *Transfer and Capture of Traffic on Firewall Engine* section of this chapter. If you want to learn more about packet capture option, read the chapter on *Capture of Traffic for Advance Analysis* for detail.

In addition, run the **firewall-engine-debug** tool on the CLI of your FTD. It allows you to analyze any activities in real time as the traffic comes.

Once you enable both the **capture** and the **firewall-engine-debug** tools, you can generate live traffic through the FTD — by attempting to establish telnet connections to the Network 100 and 200, from the Network 1 and 2, respectively. In this lab exercise (Scenario 2), the Network 1 and 100 should be able establish a telnet connection, but the Network 2 should fail to connect to the Network 200 due to the block action on the prefilter policy.

[Example 13-11](#) does not show any tunnel traffic in the firewall-engine-debug output. Since the traffic is blocked before it hits an inspection engine, the firewall-engine-debug tool cannot see and log a block action.

Example 13-11 *Debug of Connections When a Prefilter Policy Blocks All Tunnel Traffic*

```
! The non-encapsulated traffic from 192.168.1.1 to 192.168.100.1 is allowed by a rule (id 268434432).
```

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
! An action on the traffic from 192.168.1.1 to 192.168.100.1 is logged below:
```

```
192.168.1.1-36257 > 192.168.100.1-23 6 AS 5 I 0 New session
192.168.1.1-36257 > 192.168.100.1-23 6 AS 5 I 0 using HW or preset rule
order 2, id 268434432 action Allow and prefilter rule 0
192.168.1.1-36257 > 192.168.100.1-23 6 AS 5 I 0 allow action
192.168.1.1-36257 > 192.168.100.1-23 6 AS 5 I 0 Deleting session
```

```
! Traffic from 192.168.2.1 to 192.168.200.1 does not appear here; because they are encapsulated and therefore, blocked by the Prefilter policy.
```

```
^C
```

```
Caught interrupt signal
Exiting.
```

```
>
```

The Firewall engine debug output shows a rule id 268434432 with allow action, but it does not display the condition that triggers this particular rule. To learn about a rule condition, you can view the list of all active access rules, and find the associated rule ID for a specific rule.

[Example 13-12](#) elaborates the default actions of both Prefilter and Access Control policies. The tunnel traffic is denied by the rule 9998, while any other traffic is permitted by the rule 268434432 and forwarded for Firepower deep packet inspection.

Example 13-12 *List of Access Rules by the Prefilter and Access Control Default Actions*

```
> show access-list
```

```
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
```



```

access-list CSM_FW_ACL_ ; 6 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY:
Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL
ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced deny ipinip any any rule-id 9998
event-log flow-start (hitcnt=0) 0x128a09cb
access-list CSM_FW_ACL_ line 4 advanced deny 41 any any rule-id 9998 event-
log flow-start (hitcnt=0) 0x6e21b1ba
access-list CSM_FW_ACL_ line 5 advanced deny gre any any rule-id 9998
event-log flow-start (hitcnt=4) 0xe9c037af
access-list CSM_FW_ACL_ line 6 advanced deny udp any eq 3544 any range 1025
65535 rule-id 9998 event-log flow-start (hitcnt=0) 0x77ac07e0
access-list CSM_FW_ACL_ line 7 advanced deny udp any range 1025 65535 any
eq 3544 rule-id 9998 event-log flow-start (hitcnt=0) 0x3054708b
access-list CSM_FW_ACL_ line 8 remark rule-id 268434432: ACCESS POLICY: AC
Policy - Default/1
access-list CSM_FW_ACL_ line 9 remark rule-id 268434432: L4 RULE: DEFAULT
ACTION RULE
access-list CSM_FW_ACL_ line 10 advanced permit ip any any rule-id
268434432 (hitcnt=12) 0xa1d3780e
>

```

For the successful and unsuccessful telnet attempts, FMC should display connection events. You can find them in the **Analysis > Connections > Events** page.

[Table 13-2](#) summarizes the actions within a lab network when FTD is configured to block all tunnel traffic.

Table 13-2. *Expected Behavior in the Lab Scenario 2 When the Tunnel Traffic is Blocked*

Network	Policy Action	Event Log
Non-encapsulated Traffic Between Network 1 and 100	Prefilter policy does not interrupt traffic because the traffic is non-encapsulated. It is allowed by the default action of the Access Control policy	An Allow event is logged by the default action of the Access Control policy
Encapsulated Traffic Between Network 2 and 200	Prefilter policy blocks all of the tunnel traffic, per configuration, before they hit any inspection engines.	A Blocked event is logged by the default action of the Prefilter policy

[Figure 13-11](#) shows that the default action of the Default Prefilter Policy blocks a GRE connection. Since the packet is blocked and not analyzed afterwards, FTD does not reveal the innermost IP header. As a result, the connection event shows the IP addresses of the router interfaces.

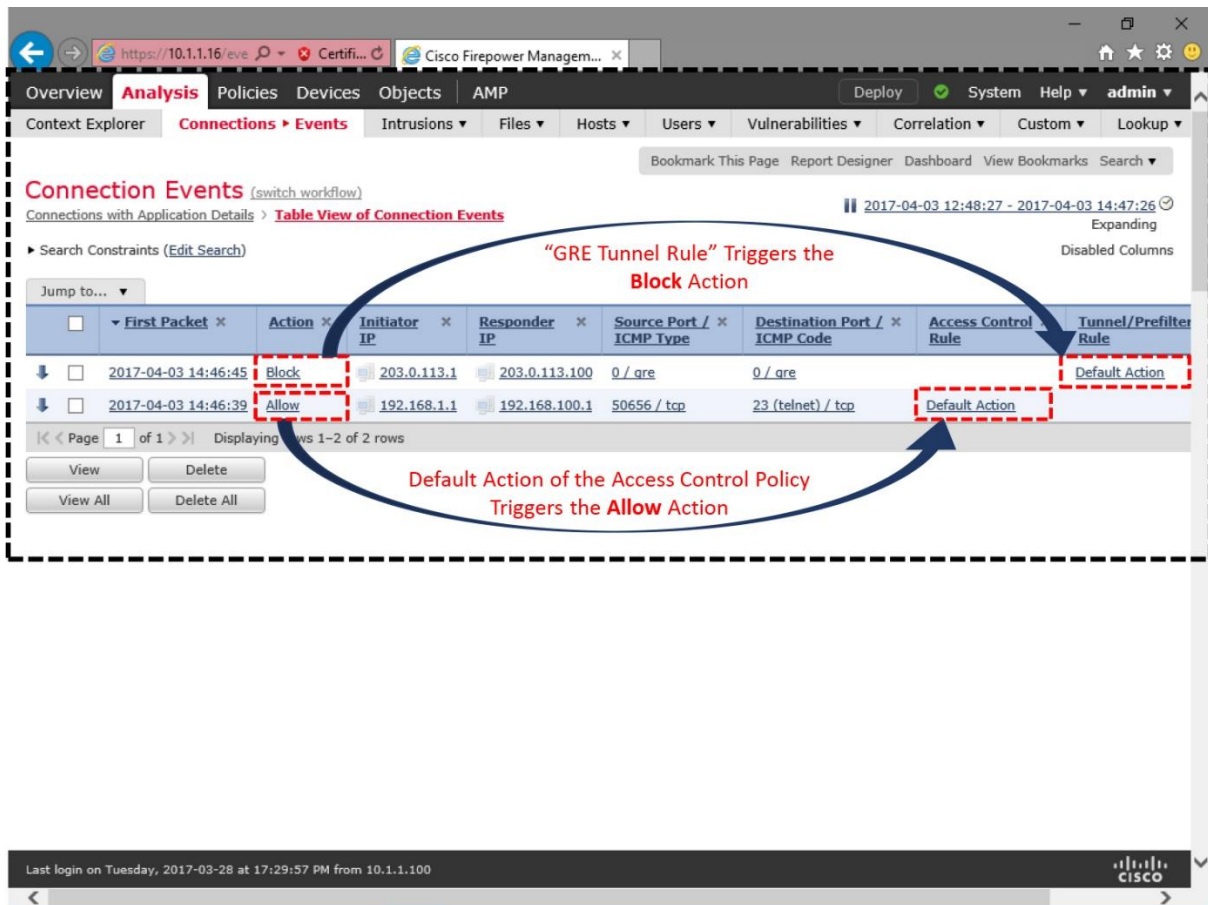


Figure 13-11. Connection Events Shows the Block of a GRE Connection

If you do not see an event as expected, make sure you enabled logging for the default actions on both Prefilter and Access Control policies. Finally yet importantly, you must check if the latest access control policy where you saved the recent changes is active. You can verify it by checking the status of the Access Control policy. To find the status, navigate to the **Policies > Access Control > Access Control**.

Analysis of Packet Flows

The packet flows between 192.168.1.1/24 and 192.168.100.1/24 are identical in Scenario 1 and 2 — regardless of the default action you choose for tunnel traffic, because these hosts transfer traffic over a non-encapsulated path. However, in this second scenario, FTD blocks traffic between the hosts 192.168.2.1/24 and 192.168.200.1/24, because they attempt to route their traffic over the tunnel.

[Example 13-13](#) displays the telnet traffic over a tunnel. First, it shows the encapsulation of packet with a GRE header (IP protocol number 47). Then, it analyzes the block of a GRE packet due to the default tunnel action rule 9998.

Example 13-13 Analysis of the GRE Encapsulated Traffic When It is Blocked by FTD

```
> show capture gre_traffic

4 packets captured

  1: 18:46:45.801670      203.0.113.1 > 203.0.113.100:  ip-proto-47,
length 48
  2: 18:46:47.802708      203.0.113.1 > 203.0.113.100:  ip-proto-47,
length 48
  3: 18:46:51.802952      203.0.113.1 > 203.0.113.100:  ip-proto-47,
length 48
  4: 18:46:59.803165      203.0.113.1 > 203.0.113.100:  ip-proto-47,
length 48
4 packets shown
>

> show capture gre_traffic packet-number 1 trace

4 packets captured

  1: 18:46:45.801670      203.0.113.1 > 203.0.113.100:  ip-proto-47,
length 48
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS
services will be applied

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny gre any any rule-id 9998 event-log
flow-start
access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY: Default
Tunnel and Priority Policy
access-list CSM_FW_ACL_ remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION
RULE
```

Additional Information:

Result:

```
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

```
1 packet shown
>
```

Scenario 3: Bypassing Inspection

In the third scenario, FTD bypasses only the tunnel traffic while any other non-encapsulated traffic can still go through the FTD like the previous two scenarios. The physical topology or the router configurations remain untouched.

Configuration of Policies to Bypass Inspection

The default prefilter policy can allow or block the tunnel traffic, but it does not offer an option to bypass inspection. To bypass, you need to create a custom prefilter policy, and invoke it in an Access Control policy that you want to deploy.

Custom Prefilter Policy

Use the following steps to create a custom prefilter policy:

Step 1. Navigate to the **Policies > Access Control > Prefilter**. The Prefilter Policy page appears. Select the **New Policy** button to create a new prefilter policy.

[Figure 13-12](#) shows the name of a new policy — **Custom Tunnel and Prefilter Policy**. In the background, you can find the **New Policy** button as well.

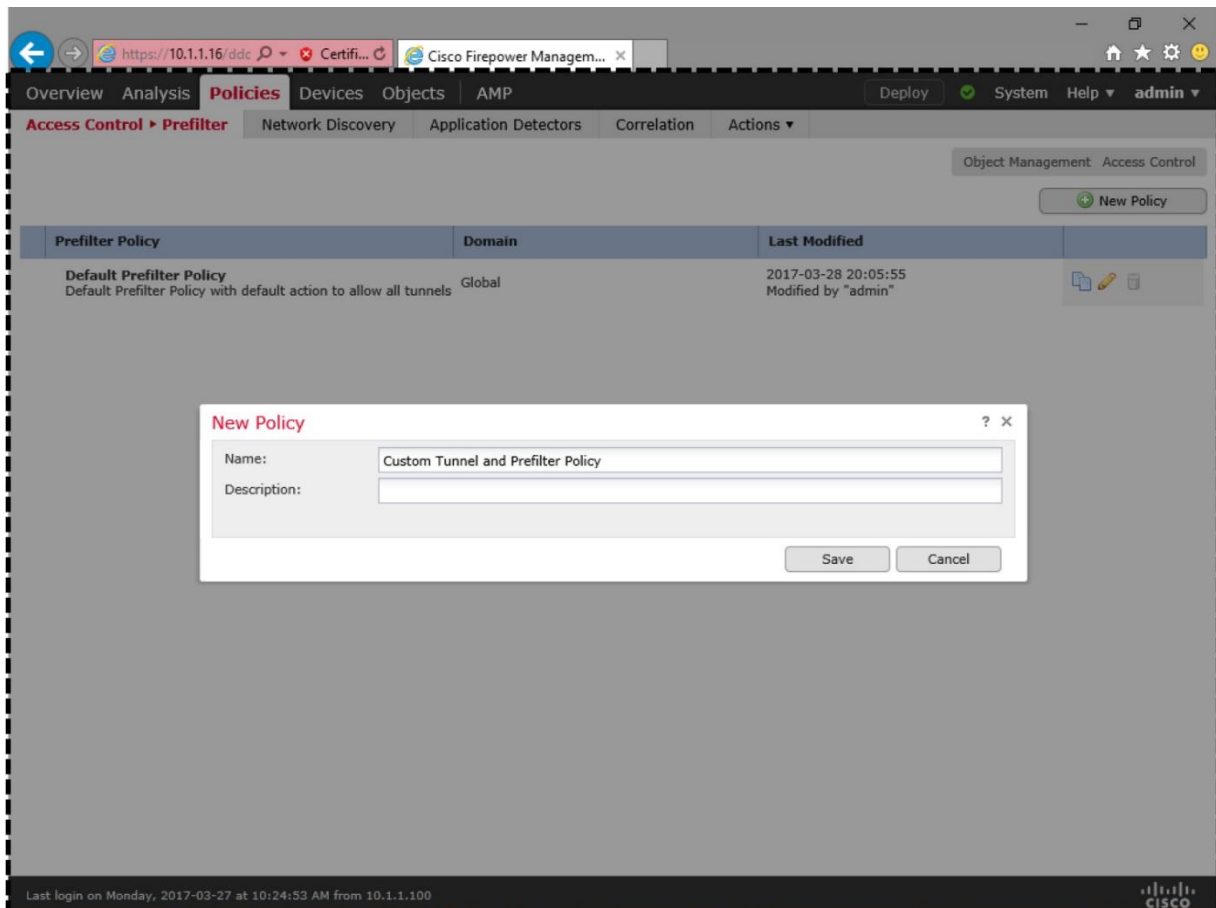


Figure 13-12. *The New Policy Window*

Step 2. When the **New Policy** window appears, give a name to the policy, and select the **Save** button to the policy. The policy editor page appears.

Step 3. On the policy editor page, select the **Add Tunnel Rule** button. The Add Tunnel Rule configuration window appears.

[Figure 13-13](#) shows the Prefilter policy editor page. A user-created policy offers two additional options — Add Tunnel Rule, and Add Prefilter Rule.

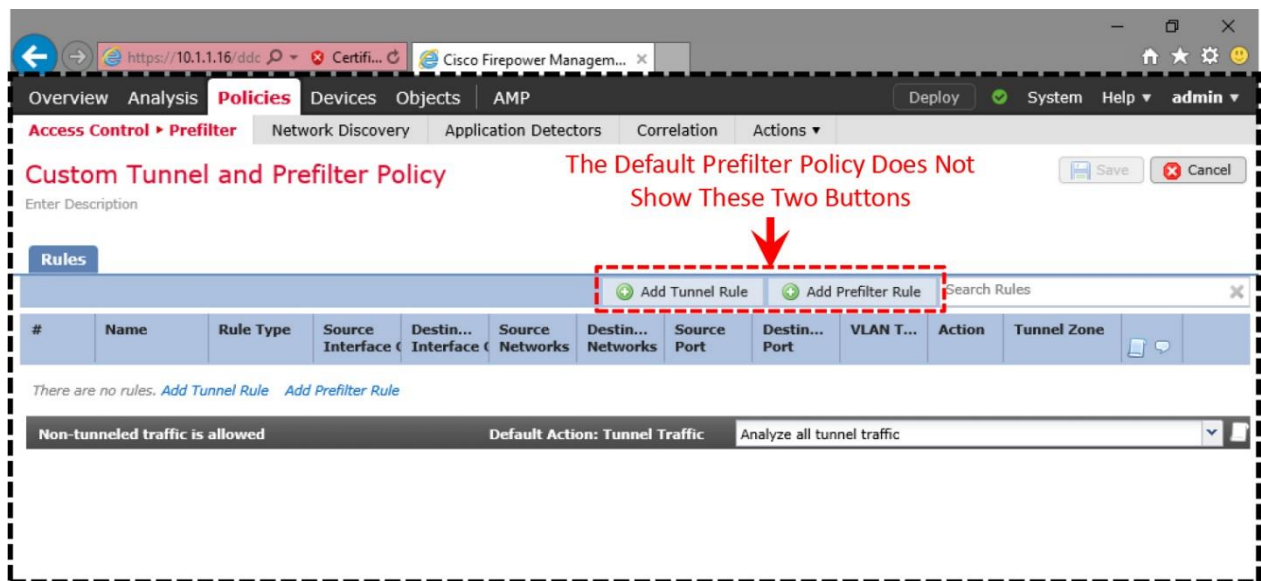


Figure 13-13. Buttons to Add Custom Tunnel and Prefilter Rules

Step 4. Assign a name to your custom tunnel rule. Select the **Fastpath** from the **Action** dropdown.

Step 5. Make sure the rule is Enabled, and configured to **Match tunnels from source and destination**.

Step 6. Click the **Encapsulation and Ports** tab. Enable **GRE** from the list of encapsulation protocols, as the lab in this chapter uses GRE protocol. Optionally, you can go to the **Tunnel Endpoints** tab, and select the source and destination tunnel endpoints. These tunnel endpoints are the IP addresses of both sides of the tunnels. You can configure them the same way you would configure a network address within an Access Rule or a Prefilter Rule.

Figure 13-14 shows the configuration of a tunnel rule, named as GRE Tunnel Rule. The rule matches GRE tunnel traffic from source and destination, and fastpath them from any further inspection.

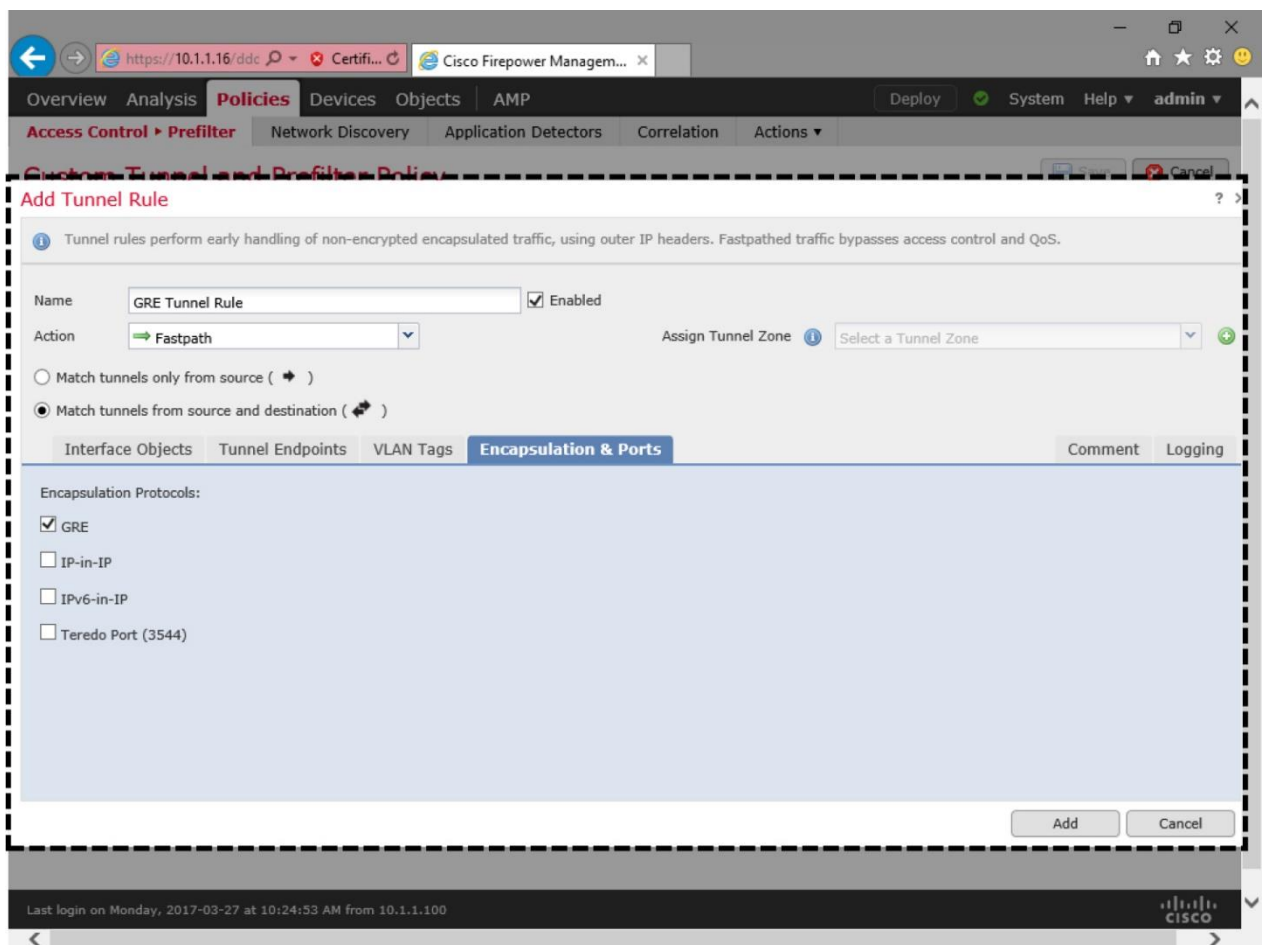


Figure 13-14. A Fastpath Rule to Bypass Only GRE Traffic

Step 7. Optionally, go to the **Logging** tab, and enable logging at the beginning of connection. It allows an FTD to generate a log when this particular rule triggers.

Figure 13-15 shows the enablement of logging at the beginning of a tunnel connection.

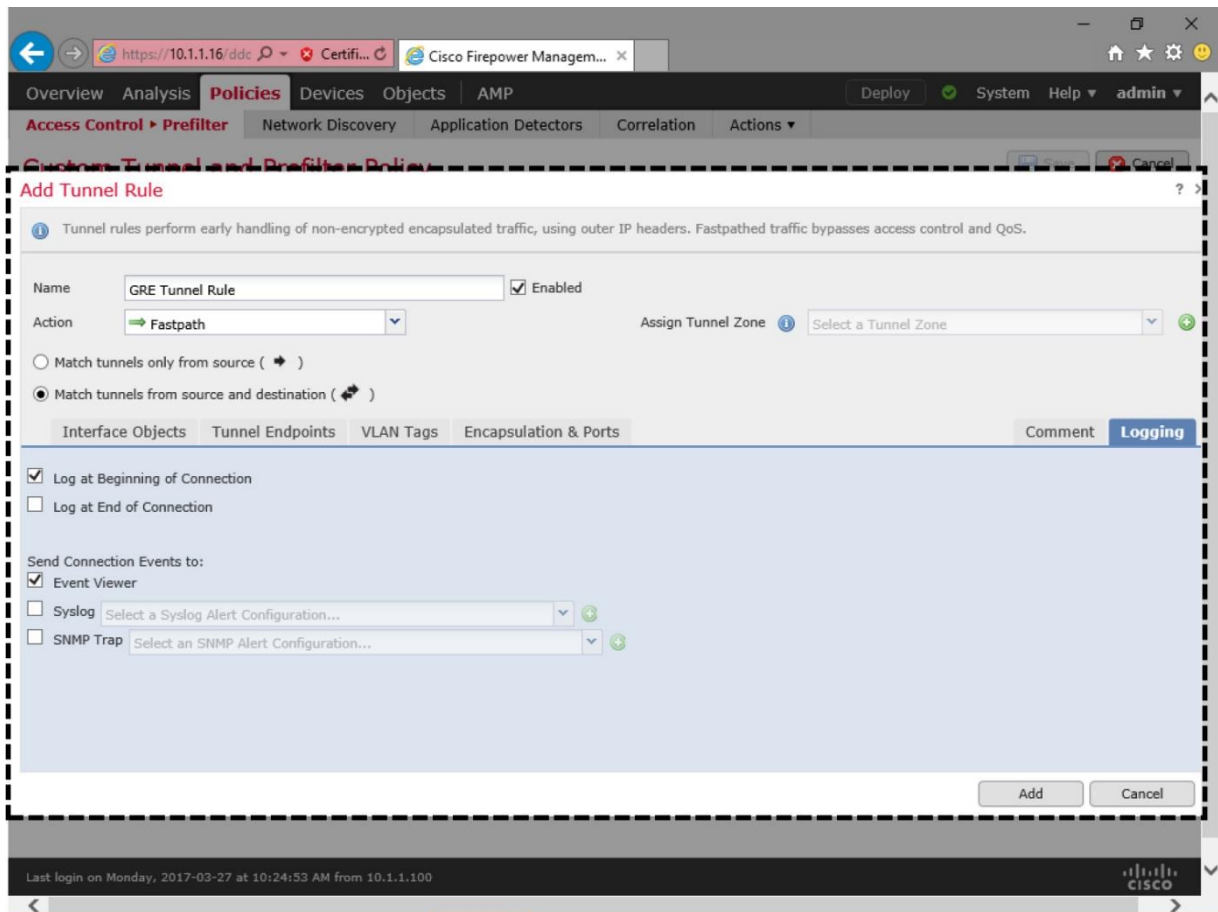


Figure 13-15. *Enablement of Logging for a Custom Tunnel Rule*

Step 8. Click the **Add** button. The GUI returns to the policy editor page. Select the **Save** button to save the policy. To activate the new custom prefilter policy, you must invoke it in the current Access Control Policy.

Figure 13-16 shows a basic, but complete configuration of a tunnel rule. It bypasses any GRE packets from further inspection.

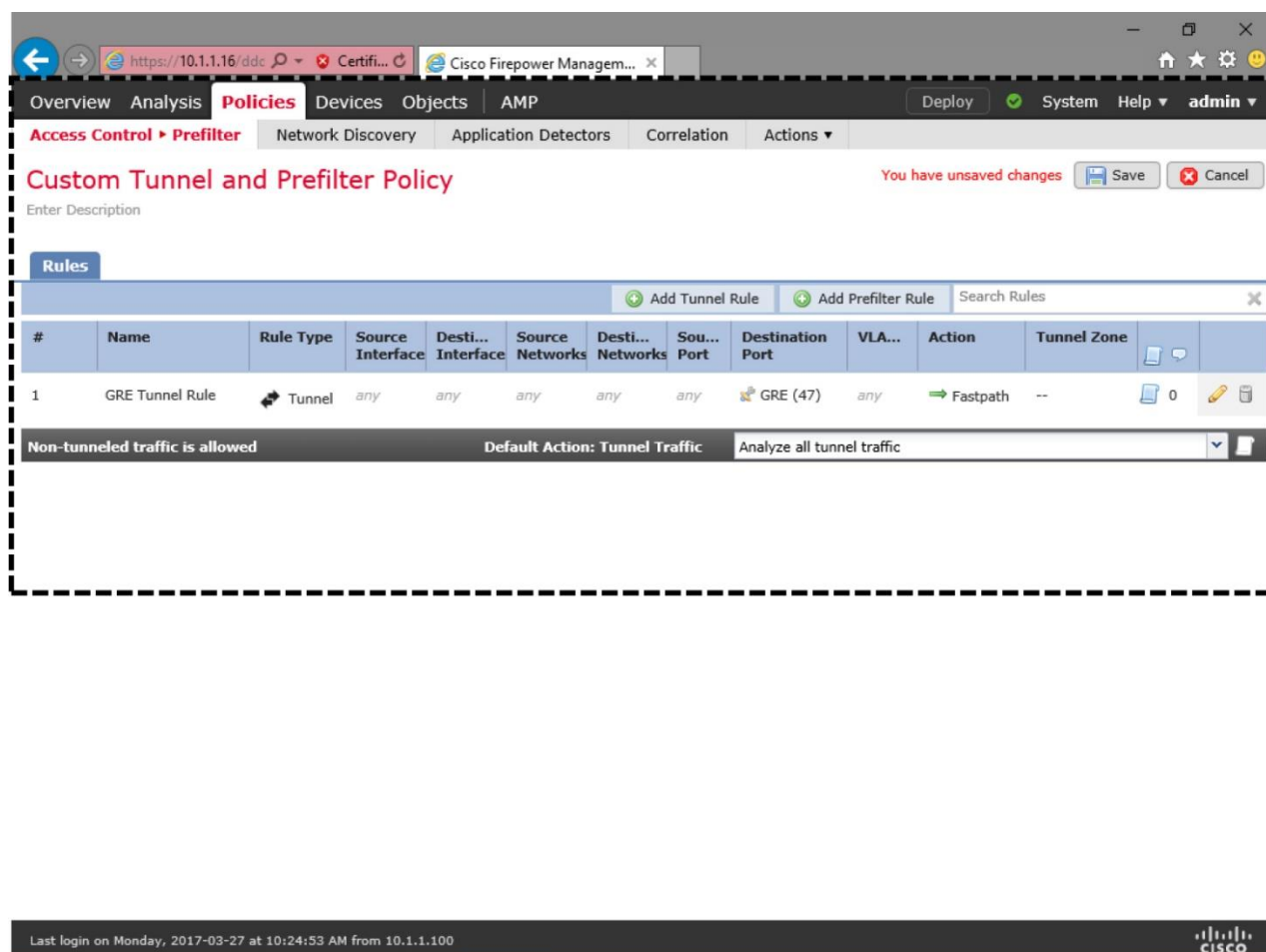


Figure 13-16. Addition of a Tunnel Rule

Access Control Policy Settings

FTD, by default, invokes the **Default Prefilter Policy**.

You can select a particular one using the Access Control policy editor page. Here are the steps to follow:

Step 1. Go to the **Policies > Access Control** page. A list of available Access control policies appears.

Step 2. Select the *pencil* icon to edit the desired policy. The Access Control policy editor page appears.

Step 3. At the top left corner, click on the link to the **Default Prefilter Policy**. The **Prefilter Policy** popup window appears. Select your desired policy using the drop-down.

Figure 13-17 shows the Access Control policy configurations for this lab scenario 3. First, you must select a custom Prefilter policy that has the fastpath rule. Then, enable logging for default action. Finally, save and deploy the policy.

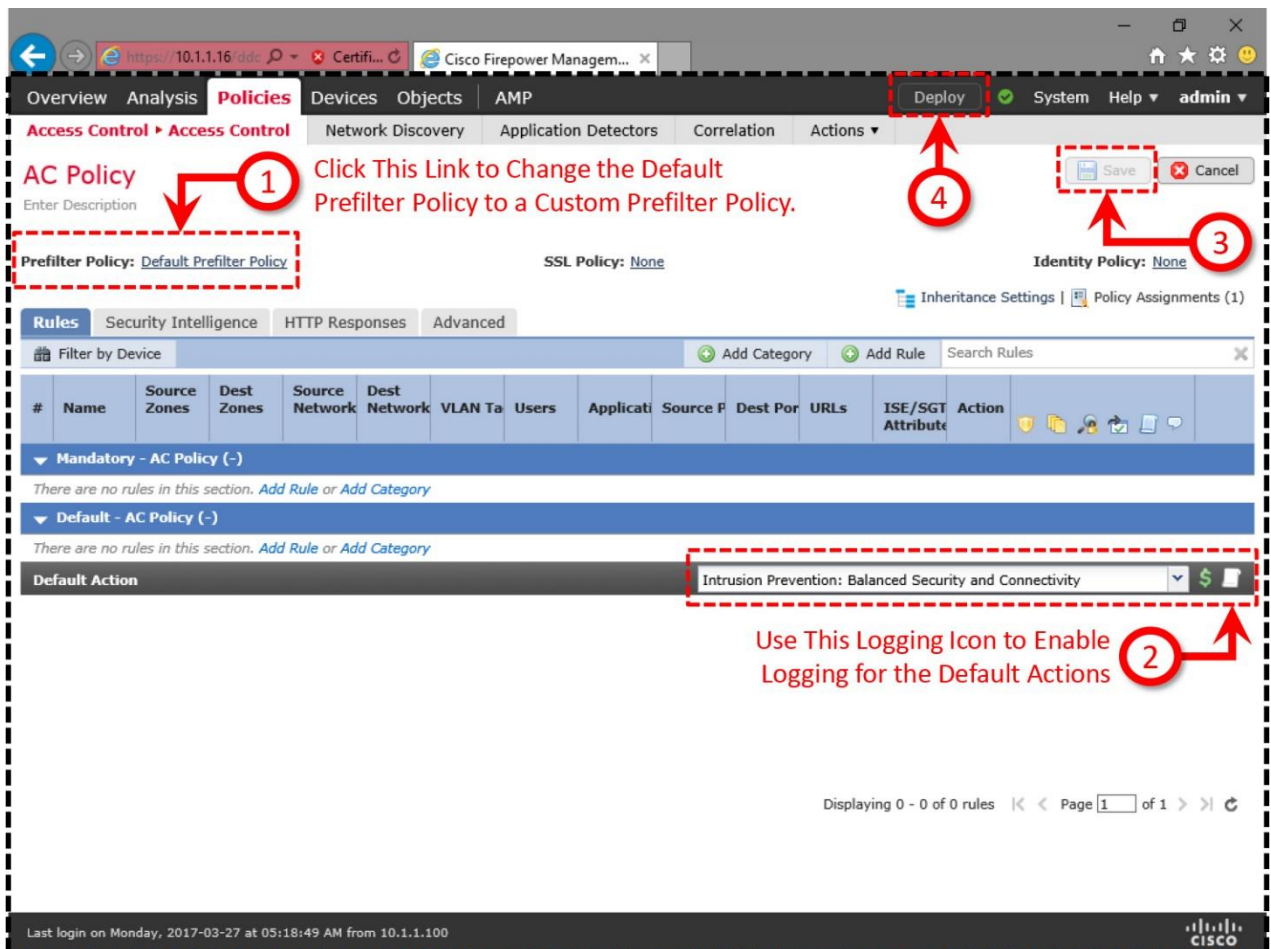


Figure 13-17. Configuration Items on an Access Control Policy for Lab Scenario 3

Step 4. Optionally, enable logging for the default action. It allows you to determine if a packet hits the default action of an Access Control policy, or bypasses the inspection before it hits the default action.

Step 5. Finally, save the changes, and deploy the revised Access Control policy to your FTD. It should activate the revised Prefilter policy as well.

Now, connect to the Network 200 from the Network 2 via telnet. Since they connect over the GRE tunnel, FTD bypasses their traffic from any additional inspection. You can verify this by viewing the associated connection events on the **Analysis > Connection > Events** page.

Figure 13-18 exhibits a Fastpath event that is triggered by the GRE tunnel Rule. In this case, since FTD does not analyze the inside of an encapsulated traffic, the connection event shows the outermost headers (IP addresses of the router interfaces), instead of the innermost headers.

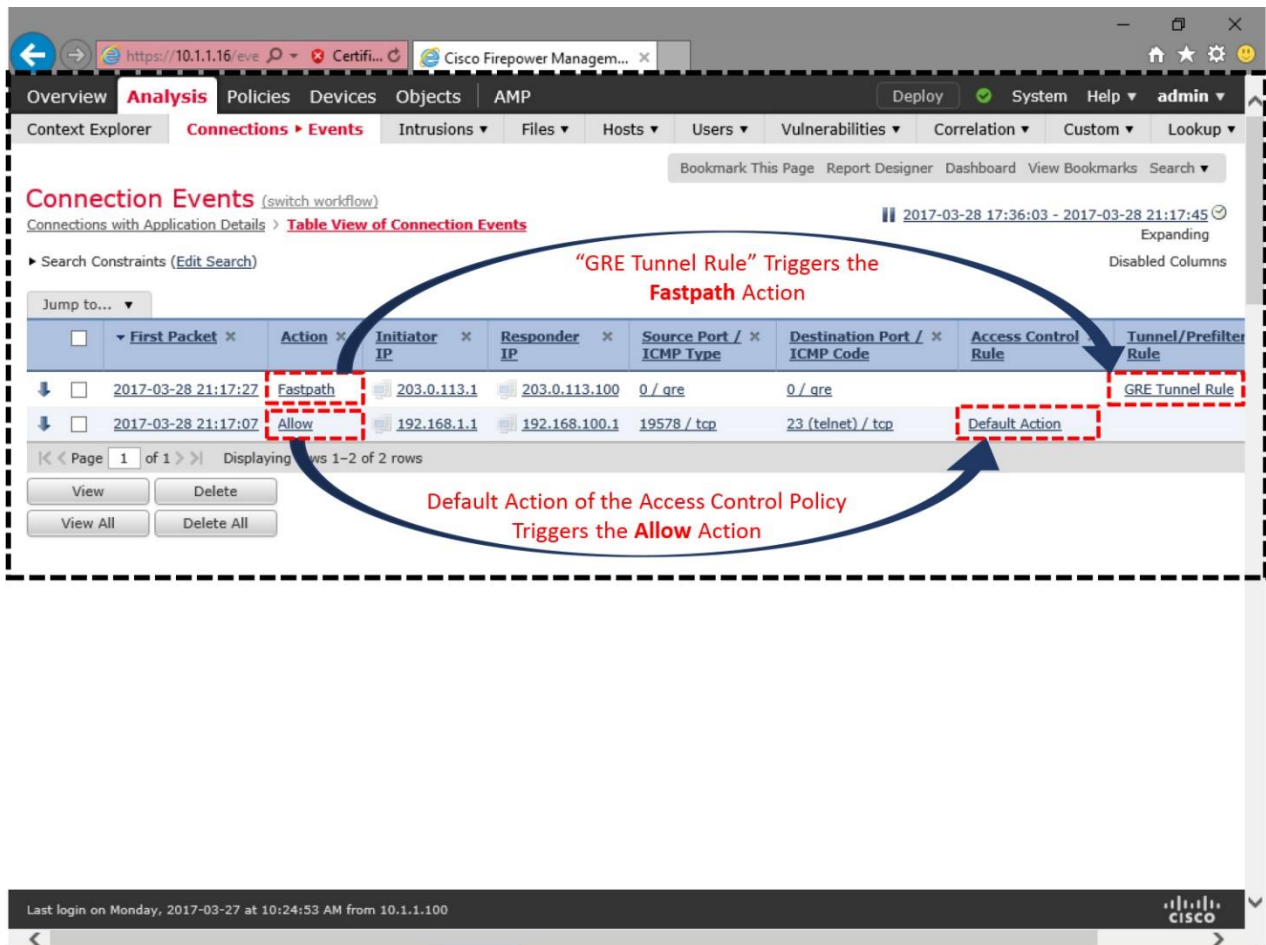


Figure 13-18. Connection Event Triggers by the Fastpath Action

If FTD still does not bypass the tunnel traffic and acts based on the previous prefilter policy, try clearing the existing connections on the FTD. It forces the hosts to establish new connections using the new policy.

To clear all of the existing connections, run the following command:

```
> clear conn all
```

To clear connections from a certain host, run the following command:

```
> clear conn address IP_Address_of_a_Host
```

Verification of Configuration and Connection

You have just enabled a custom prefilter policy to bypass all tunnel traffic. To verify its operation, enable two independent captures for telnet and GRE protocols. If the FTD has

been running capture since the earlier lab exercises (Scenario 1 and 2), you can just remove any previously captured packets by running the **clear capture** command:

```
> clear capture /all
```

Note

The steps for capturing telnet and GRE traffic is described in the *Transfer and Capture of Traffic on Firewall Engine* section of this chapter. If you want to learn more about packet capture option, read the [Chapter 10 - Capture of Traffic for Advance Analysis](#) for detail.

In addition, run the **firewall-engine-debug** tool on the CLI of your FTD. It allows you to analyze any activities in real time as the traffic comes.

Once you enable both the **capture** and the **firewall-engine-debug** tools, you can generate live traffic through the FTD — by trying to establish telnet connections between the Network 1 and 100, and between the Network 2 and 200. In the third lab scenario, both connection attempts are successful; however, the debug engine does not see traffic from the Network 2 and 200, because they are encapsulated, and bypassed from further inspection.

[Example 13-14](#) shows the debug of a connection between the Network 1 and 100. Although the telnet connection was successful, the following output does not display any related debug message, because a **Fastpath** rule in the custom prefilter policy bypasses the encapsulated traffic from any further inspection.

Example 13-14 Firewall Engine Debug Output — When FTD Bypasses Tunnel Traffic

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
! Traffic from 192.168.1.1 to 192.168.100.1 is non-encapsulated, therefore
it is
inspected by a rule (id 268434432).
```

```
192.168.1.1-40591 > 192.168.100.1-23 6 AS 5 I 1 New session
192.168.1.1-40591 > 192.168.100.1-23 6 AS 5 I 1 using HW or preset rule
order 3, id
268434432 action Allow and prefilter rule 0
192.168.1.1-40591 > 192.168.100.1-23 6 AS 5 I 1 allow action
192.168.1.1-40591 > 192.168.100.1-23 6 AS 5 I 1 Deleting session
```

```
! Traffic from 192.168.2.1 to 192.168.200.1 are transferred over a GRE
tunnel.
Therefore, they are bypassed from any further inspection, and do not appear
here in
the firewall-engine-debug output.
```

```
^C
Caught interrupt signal
Exiting.
```

```
>
```

[Example 13-15](#) confirms the deployment of a fastpath rule, named as **GRE Tunnel Rule**. An FTD trusts the traffic when the rule uses the fastpath action.

Example 13-15 *A Fastpath Rule Shows “Trust” Action in the CLI Access List*

```
> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list CSM_FW_ACL_ ; 7 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 268438530: PREFILTER POLICY:
Custom Tunnel and Prefilter Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 268438530: RULE: GRE Tunnel
Rule
access-list CSM_FW_ACL_ line 3 advanced trust gre any any rule-id 268438530
event-log both (hitcnt=3) 0xbc125eb0
access-list CSM_FW_ACL_ line 4 remark rule-id 268438529: PREFILTER POLICY:
Custom Tunnel and Prefilter Policy
access-list CSM_FW_ACL_ line 5 remark rule-id 268438529: RULE: DEFAULT
TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 6 advanced permit ipinip any any rule-id
268438529 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 7 advanced permit 41 any any rule-id 268438529
(hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 8 advanced permit gre any any rule-id
268438529 (hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL_ line 9 advanced permit udp any eq 3544 any range
1025 65535 rule-id 268438529 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 10 advanced permit udp any range 1025 65535
any eq 3544 rule-id 268438529 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 11 remark rule-id 268434432: ACCESS POLICY: AC
Policy - Default/1
access-list CSM_FW_ACL_ line 12 remark rule-id 268434432: L4 RULE: DEFAULT
ACTION RULE
access-list CSM_FW_ACL_ line 13 advanced permit ip any any rule-id
268434432 (hitcnt=16) 0xa1d3780e
>
```

Analysis of Packet Flows

The packet flows between 192.168.1.1/24 and 192.168.100.1/24 are same in all three scenarios in this chapter — regardless of any action you apply on the tunnel traffic, because these hosts transfer traffic over a non-encapsulated path. However, in this third scenario, FTD bypasses inspection for the traffic between the hosts 192.168.2.1/24 and 192.168.200.1/24, because they transfer traffic over the GRE encapsulated tunnel.

[Example 13-16](#) displays the capture of encapsulated packets with GRE headers (IP protocol number 47). Due to the fastpath rule, **trust gre any any**, FTD bypasses them without any further inspection.

Example 13-16 *Analysis of the Bypass of a GRE Encapsulated Packet*

```
> show capture gre_traffic
```

```
49 packets captured
```

```
  1: 01:17:27.046475      203.0.113.1 > 203.0.113.100:  ip-proto-47,  
length 48  
  2: 01:17:27.048871      203.0.113.100 > 203.0.113.1:  ip-proto-47,  
length 48  
  3: 01:17:27.050397      203.0.113.1 > 203.0.113.100:  ip-proto-47,  
length 44
```

```
.
```

```
.
```

```
<Output Omitted for Brevity>
```

```
> show capture gre_traffic packet-number 1 trace
```

```
49 packets captured
```

```
  1: 01:17:27.046475      203.0.113.1 > 203.0.113.100:  ip-proto-47,  
length 48  
Phase: 1  
Type: CAPTURE  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
MAC Access list
```

```
Phase: 2  
Type: ACCESS-LIST  
Subtype:  
Result: ALLOW  
Config:  
Implicit Rule  
Additional Information:  
MAC Access list
```

```
Phase: 3  
Type: NGIPS-MODE  
Subtype: ngips-mode  
Result: ALLOW  
Config:  
Additional Information:  
The flow ingressed an interface configured for NGIPS mode and NGIPS  
services will be applied
```

```
Phase: 4  
Type: ACCESS-LIST  
Subtype: log  
Result: ALLOW  
Config:  
access-group CSM_FW_ACL_ global  
access-list CSM_FW_ACL_ advanced trust gre any any rule-id 268438530 event-  
log both  
access-list CSM_FW_ACL_ remark rule-id 268438530: PREFILTER POLICY: Custom  
Tunnel and Prefilter Policy  
access-list CSM_FW_ACL_ remark rule-id 268438530: RULE: GRE Tunnel Rule  
Additional Information:
```

```
Phase: 5  
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
```

```
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Ingress interface INSIDE_INTERFACE is in NGIPS inline mode.
Egress interface OUTSIDE_INTERFACE is determined by inline-set
configuration

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 131, packet dispatched to next module

Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: allow
```

```
1 packet shown
>
```

Summary

In this chapter, you have learned how to analyze and block traffic that are encapsulated with GRE protocol. This chapter also demonstrates the steps to bypass an inspection when the traffic is transferred over a tunnel. Besides configurations, you can learn various tools to analyze an action applied by the Prefilter and Access Control policy of your FTD.

Quiz

- 1.** Which of the following statement is true?
 - a.** To analyze any tunnel traffic, you must create and apply a prefilter policy.
 - b.** Access Control policy overrides the rules in a Prefilter policy.
 - c.** The fastpath action in a prefilter policy bypasses the rules in an Access Control policy; however, traffic is still subject to Intrusion policy inspection.
 - d.** None of the above.
- 2.** Which of the following tunnel protocol is supported by FTD?
 - a.** GRE
 - b.** IP-in-IP
 - c.** Ipv6-in-IP
 - d.** All of the above

3. Which of the following command confirms if the logging is enabled for the default action in an Access Control policy?

a. show logging

b. show access-list

c. show default-action

d. show access-control-config

4. The firewall-engine-debug tool shows debug level message for the following components:

a. A tunnel rule

b. A prefilter rule

c. An access rule

d All of the above

Chapter 14. Bypassing Inspection and Trusting Traffic

If you do not want an FTD to inspect certain traffic, because, for example, they are completely trusted, you can configure the FTD to bypass inspection for that particular traffic while it continues deep packet inspections for the rest of the network. It offloads the FTD hardware resources, reduces overall processing delay, and improve network performance. This chapter describes the options to bypass the Firepower inspection for any particular traffic.

Essential Knowledge

A Firepower system offers the following tools to bypass a deep packet inspection. While their goals are identical — to bypass deep packet inspection — the architecture and implementation of each tool is different.

- **Fastpath Rule:** Enabled through a Prefilter policy.
- **Trust Rule:** Activated over an Access Control policy.

Fastpath Rule

A Prefilter policy allows you to bypass traffic before a packet even reaches the ASA and Firepower engines. This functionality is known as fastpath. A rule, enabled with **Fastpath** action, is also known as a *fastpath rule*. You can apply the fastpath action on the following rule types. They filter packets based on the outermost header data, and therefore they do not offer deep packet inspection.

- **Tunnel Rule:** Tunnel rule, as the name suggests, filters tunnel traffic that are encapsulated by additional IP header. As of writing this book, a tunnel rule supports GRE, IP-in-IP, Ipv6-in-IP and Teredo encapsulation protocols. This is elaborated in the [Chapter 13 - Handling of Encapsulated Traffic](#).
- **Prefilter Rule:** A Prefilter rule is able to filter traffic based on basic networking criteria. As of writing this book, it supports a rule condition based on an IP address, port number, VLAN tag, and interface.

Rules in a Prefilter policy support three types of actions — Fastpath, Analyze, and Block. While the **Fastpath** action bypasses traffic from further inspection, the **Analyze** action forwards the traffic to the next level of inspection. The **Block** action just drops a packet without any additional security check.

[Figure 14-1](#) shows the position of a fastpath rule in an FTD workflow. When a packet matches a fastpath rule, it bypasses the Firepower deep packet inspection completely.

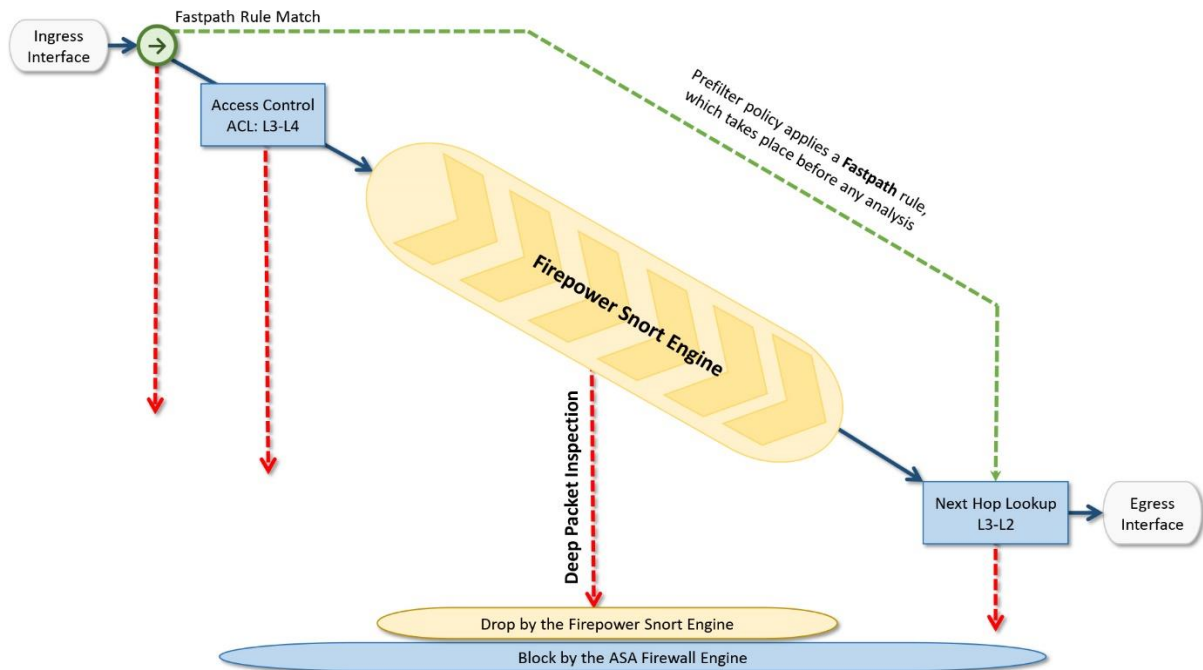


Figure 14-1. Workflow of the Fastpath Action in a Prefilter Policy

Trust Rule

An access rule is known as a *trust rule* when you assign it the Trust action. A Trust rule can bypass traffic without performing any deep packet inspection and network discovery. To ensure the entitlements, the trusted traffic, however, checks for identity and Quality of Service (QoS) requirements.

Besides the simple filtering conditions that are available in a prefilter rule, an access rule offers additional granular filters. For example, you can match and trust traffic based on network conditions, applications, URLs, users, etc. Unlike a prefilter rule, an access rule uses the innermost header of a packet to filter traffic.

Figure 14-2 shows the position of a trust rule in an FTD workflow. When a packet matches a trust rule, it bypasses various inspection components.

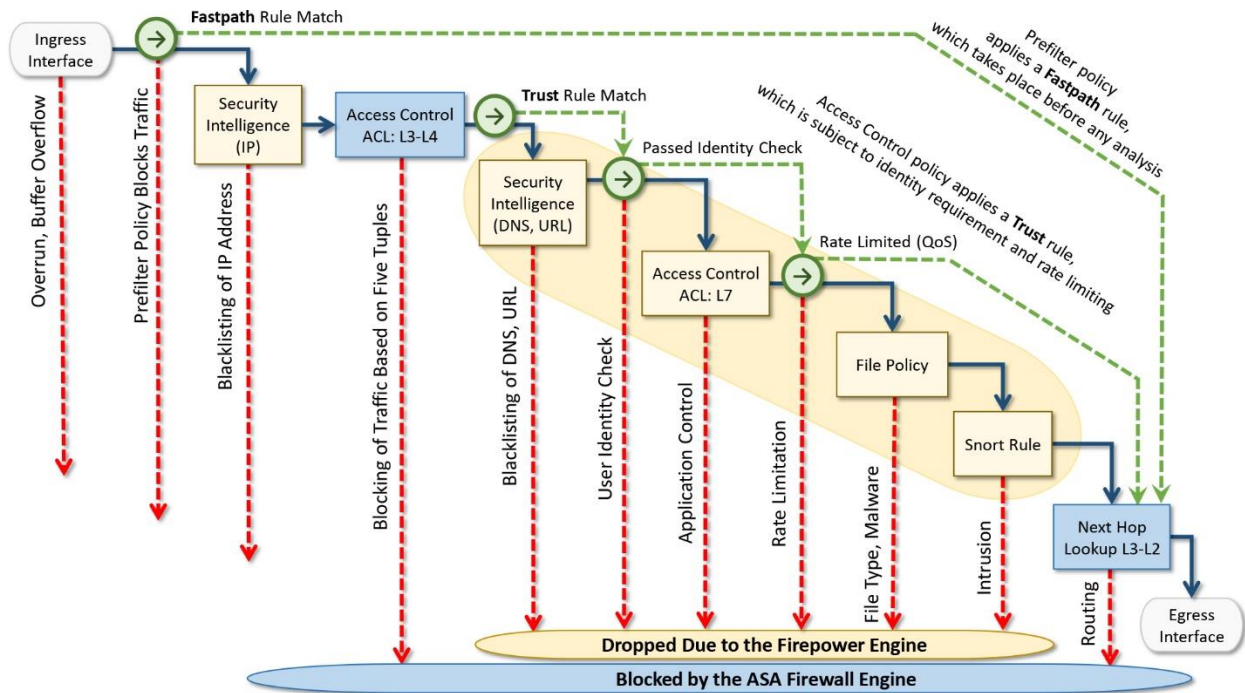


Figure 14-2. Workflow of the Trust Action in an Access Control Policy

Best Practices

For bypassing inspection, if you want to filter traffic based on simple conditions, such as, network address, port number, VLAN tags, and interface objects, then employ the capability of a Prefilter rule, instead of applying an access rule with trust action.

Prerequisites

This chapter assumes that an FTD is deployed between a client and a server. The client can access the server using Secure Shell (SSH) and Telnet services. The configuration examples on this chapter use both of these services to verify the action of the fastpath and trust rules.

Note

The method to initiate a telnet or ssh connection varies — depends on the client software or operating system you use. This book does not recommend any particular client, and therefore it does not display any telnet or ssh client commands.

[Figure 14-3](#) shows a simple topology that is used in this chapter to demonstrate the bypass of inspection.

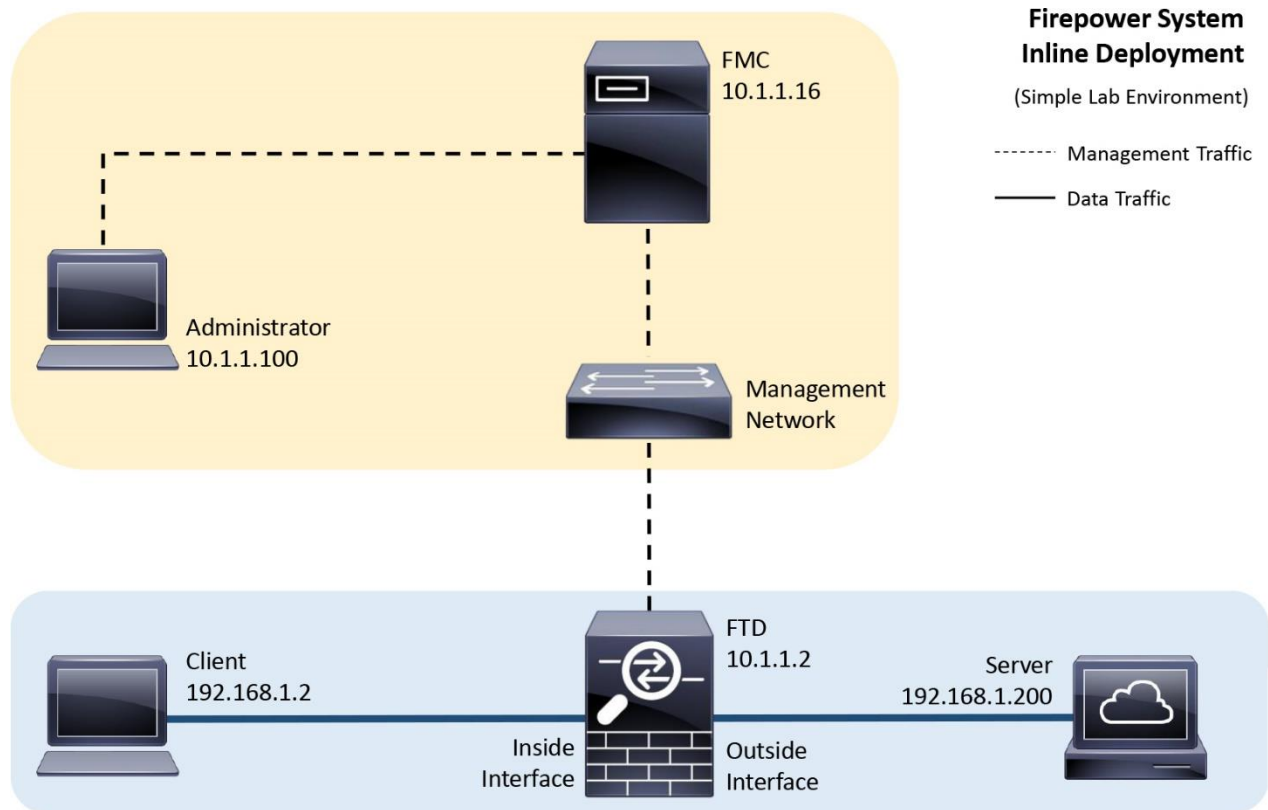


Figure 14-3. Lab Topology Used in This Chapter

Fastpath through a Prefilter Policy

The default prefilter policy that comes with an FTD out of the box provides limited configurable options. However, you can create your own prefilter policy, which supports a custom prefilter rule based on basic filtering conditions, such as, network address, port numbers, VLAN tags, and interface objects.

A custom prefilter rule supports three types of actions — analyze, block, and fastpath. This section demonstrates how to create a custom prefilter policy, add a custom prefilter rule within, and fastpath any traffic over port 22, as an example.

Configuration

The configurations for bypassing traffic can be divided into two parts:

- Configuration of Prefilter policy
- Invoking the Prefilter policy into an Access Control policy

Configuration of Prefilter policy

To configure a custom prefilter rule for traffic over port 22, follow the steps below:

Step 1. Navigate to the **Policies > Access Control > Prefilter**. The Prefilter Policy page appears.

Step 2. Use the **New Policy** button to create a new prefilter policy. If you created a **Custom Tunnel and Prefilter Policy** in the previous chapter, you can reuse the same policy for this exercise. Just use the pencil icon to edit the policy, and delete any tunnel rule you created earlier.

[Figure 14-4](#) shows the list of available policies in the Prefilter policy page. You created the top one, *Custom Tunnel and Prefilter Policy*, in the previous chapter. The bottom one, *Default Prefilter Policy*, comes with FTD by default. You can also create a brand new Prefilter policy using the **New Policy** button.

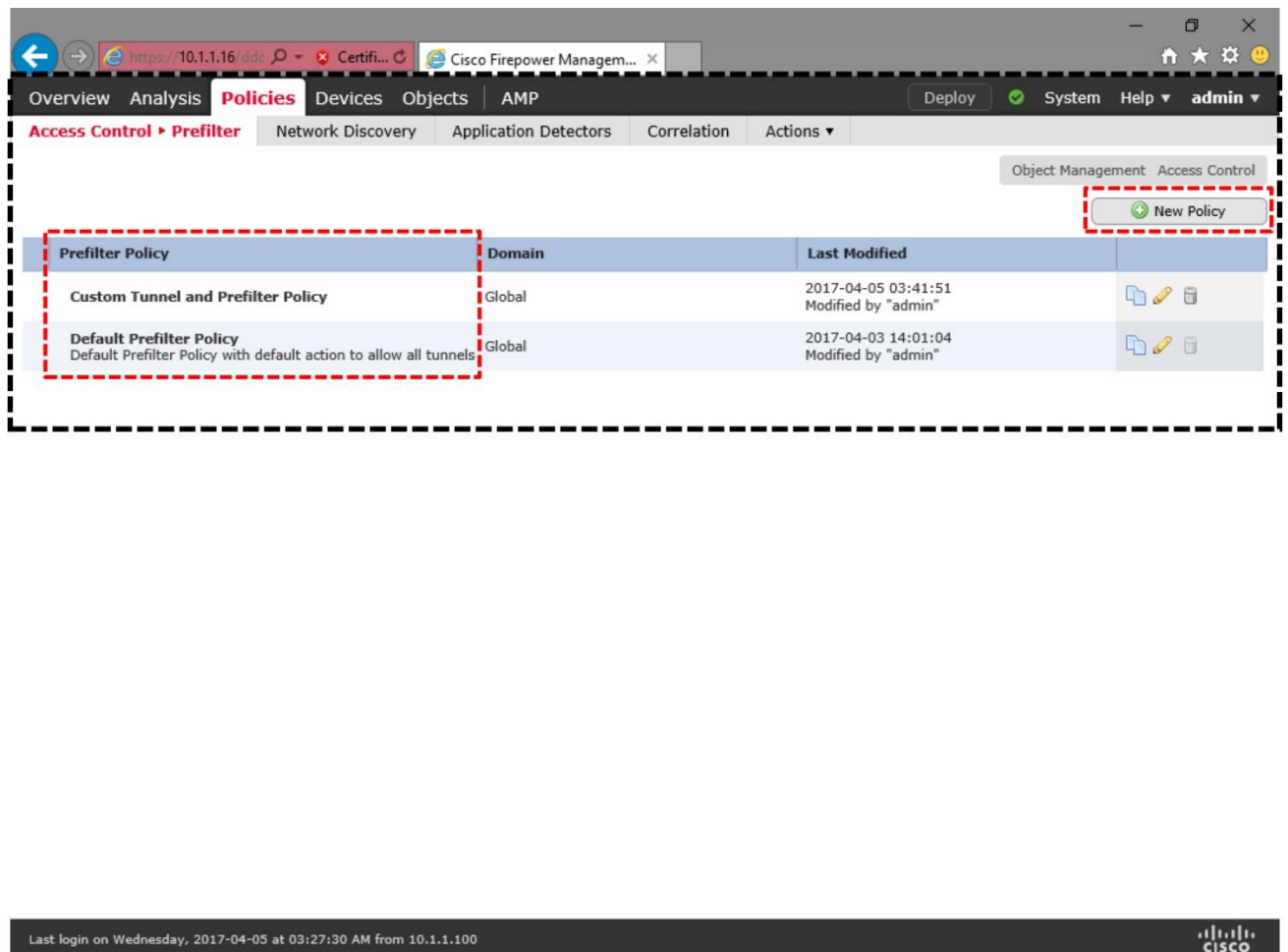


Figure 14-4. The Prefilter Policy Page Shows Available Policies and a New Policy Button

Step 3. Once you are in the Prefilter policy editor page, select the **Add Prefilter Rule** button. A configuration window appears.

Figure 14-5 highlights two key options in a Prefilter policy editor page — the **Add Prefilter Rule** button and the **Default Action** drop-down.

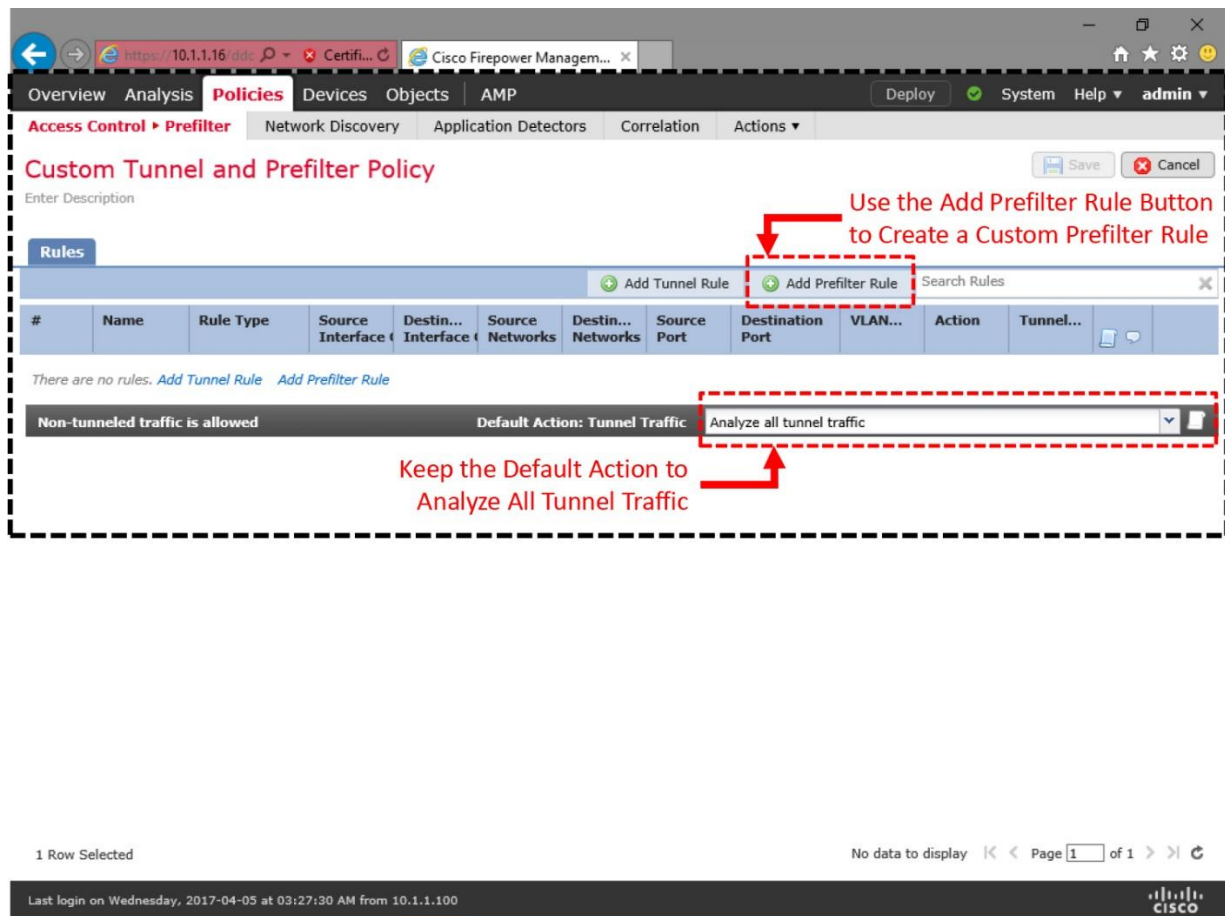


Figure 14-5. The Prefilter Policy Editor Page

Step 4. Give a name to the rule, and set the action to **Fastpath**.

Step 5. Click on the **Port** tab. Find and select SSH from the list of **Available Ports**.

Step 6. Click on the **Add to Destination** button. It selects port 22 as the destination port.

Figure 14-6 shows the creation of a custom prefilter rule, named *Shell Prefilter*. The rule uses **Fastpath** action, and selects the default port for **SSH** protocol (port 22) as the destination port.

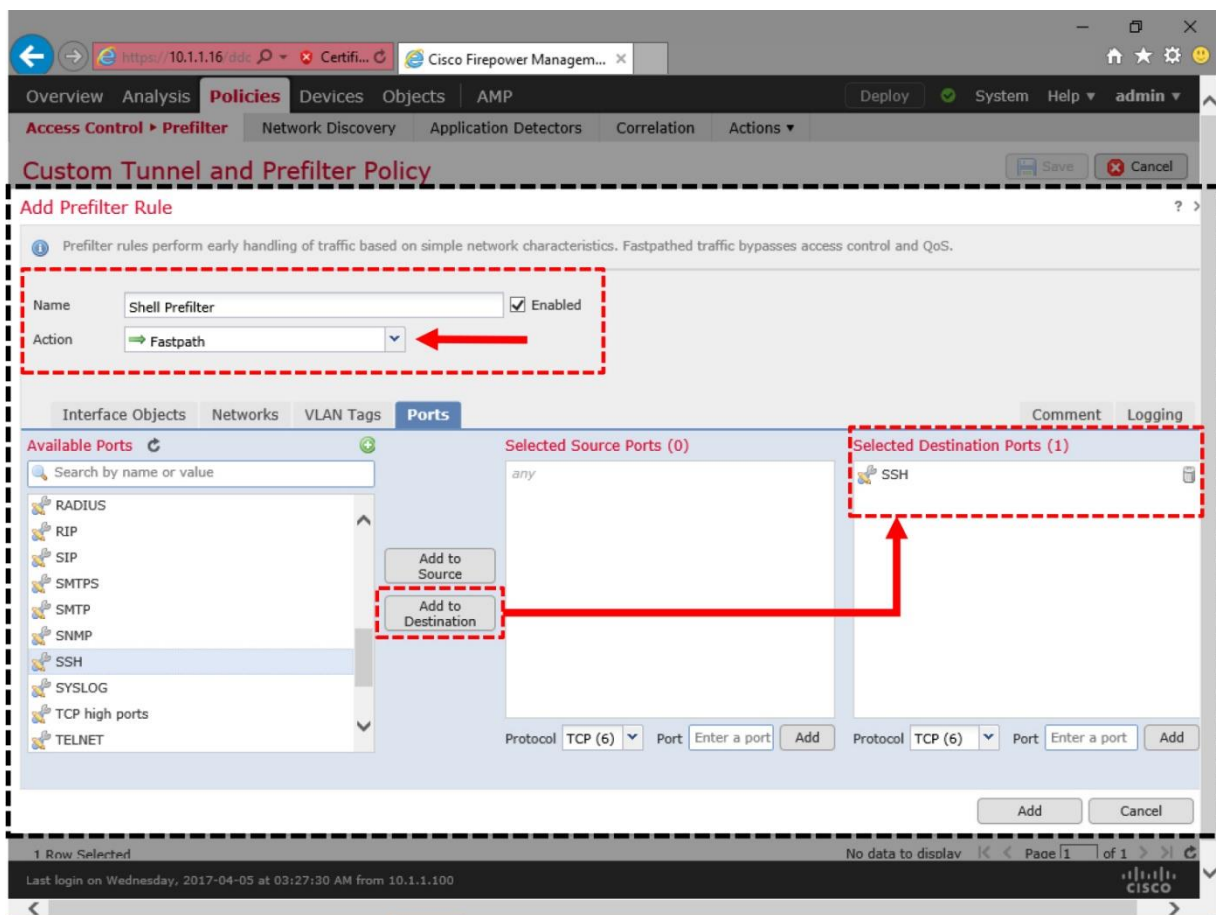


Figure 14-6. Configuration of a Prefilter Rule — Name, Action and Destination Port

Note

You could have saved the rule right here. It would bypass any traffic that is transferred over port 22 from further inspection. However, if you want to bypass traffic originated from a particular subnet only, proceed with the next steps.

Step 7. Select the **Networks** tab. By default, FTD has pre-configured objects for some common networks, such as private IP addresses, multicast addresses, etc. If they match with your network-addressing scheme, you can select from here. Alternatively, you can create a network object on the fly. Otherwise, you can just add an IP address directly as a Source or Destination.

Figure 14-7 illustrates the available options to define the source and destination for a Prefilter rule.

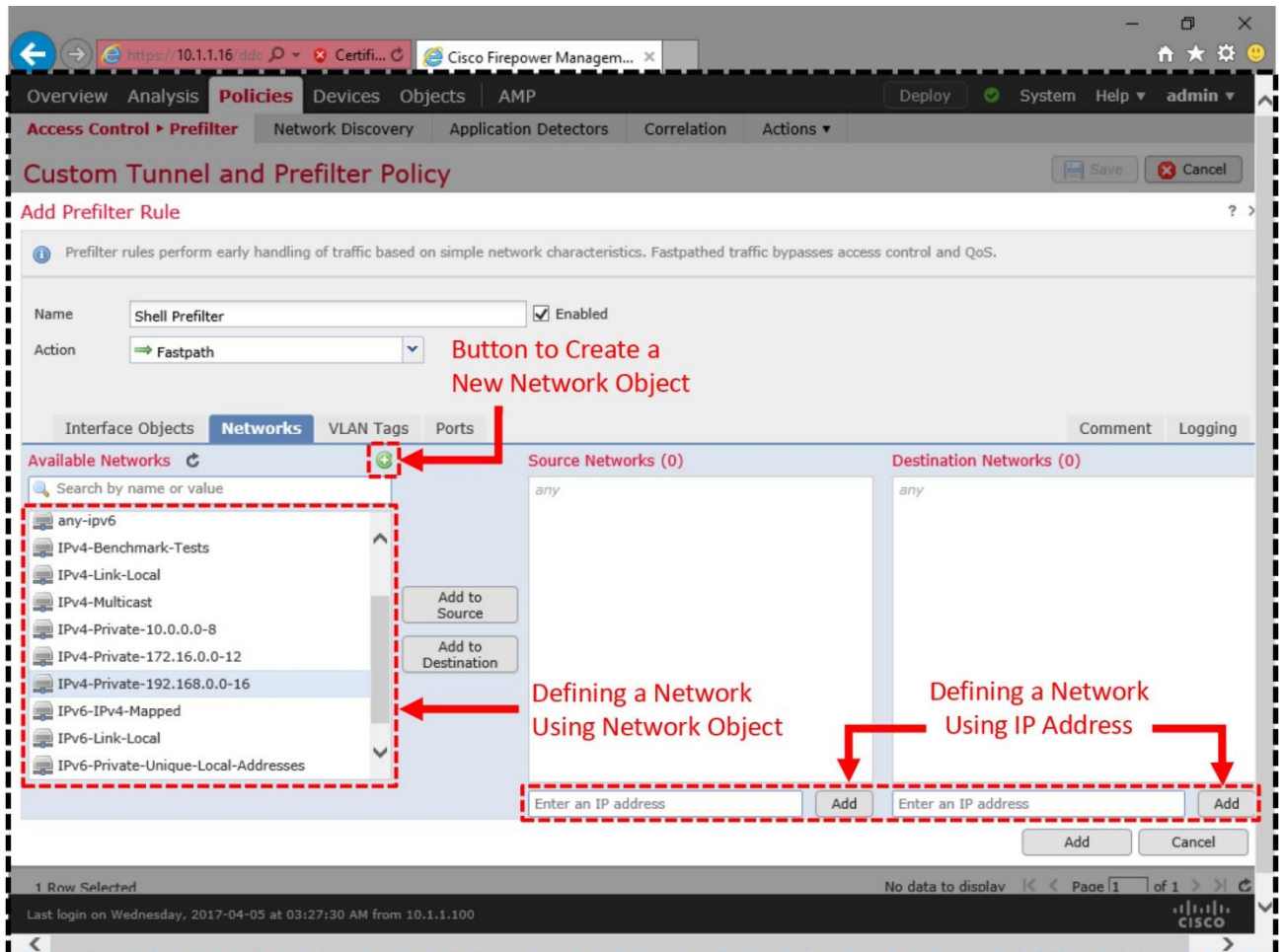


Figure 14-7. Network Tab Provides Multiple Options to Add Networks

Step 8. Click on the *green-plus* icon. A popup window for **New Network Objects** appears.

Figure 14-8 exhibits the creation of a custom network object, Corporate-Network, for 192.168.1.0/24 subnet.

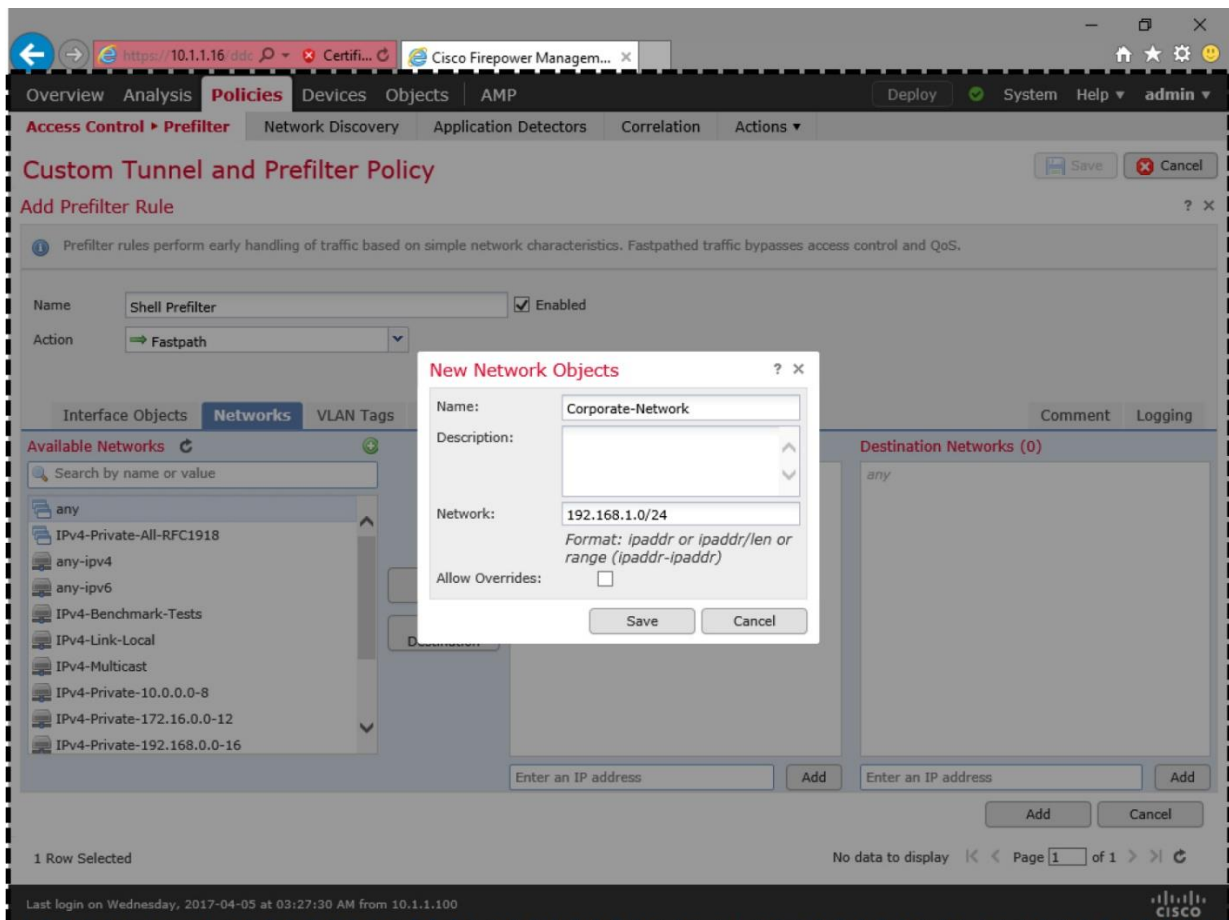


Figure 14-8. A New Network Object

Step 9. Once you save a new network object, it is available for selection. You may need to click the *refresh* icon for it to show up in the list. Use the **Add to Source** button to select your custom network object as the source network. This enables the FTD to match traffic coming from your desired subnet.

Figure 14-9 shows that a custom network object, corporate-network, is selected as the source network.

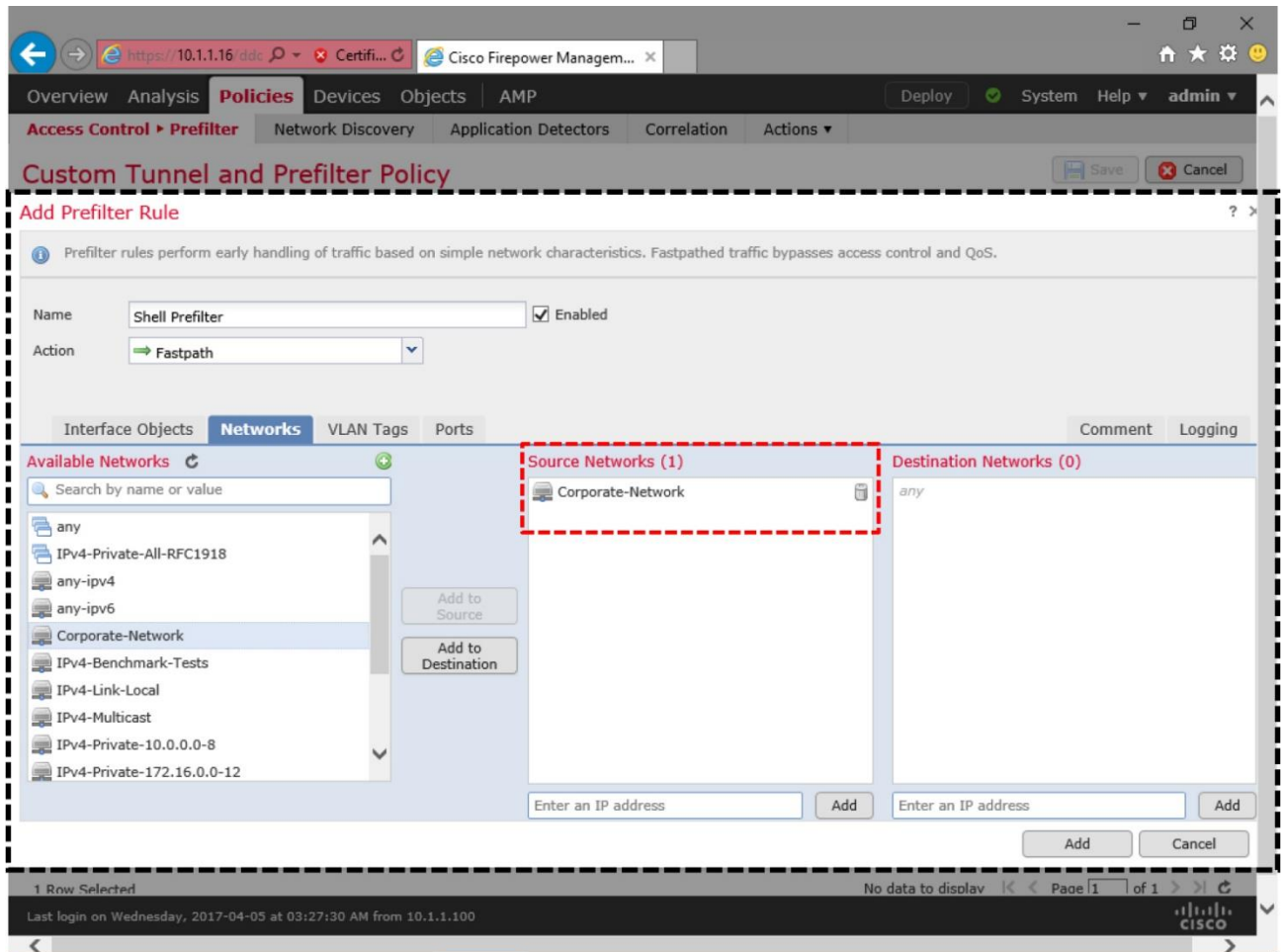


Figure 14-9. The Rule is Configured to Match 192.168.1.0/24 as the Source Network

Step 10. Optionally, you can enable logging for every time a fastpath rule triggers. It helps you to determine if a policy is operational. Go to the **Logging** tab. Select either **Log at Beginning of Connection**, or **Log at End of Connection**. However, do not select both as it can affect the system performance.

Step 11. Click the **Add** button to complete the rule configuration. You will return to the policy editor page. Use the **Save** button to save the changes.

[Figure 14-10](#) shows a complete view of the *Shell Prefilter* rule. Save the configuration, but do not use the **Deploy** button at this stage, as you have to make sure that this new prefilter policy is invoked by the required Access Control policy. The next section discusses this.

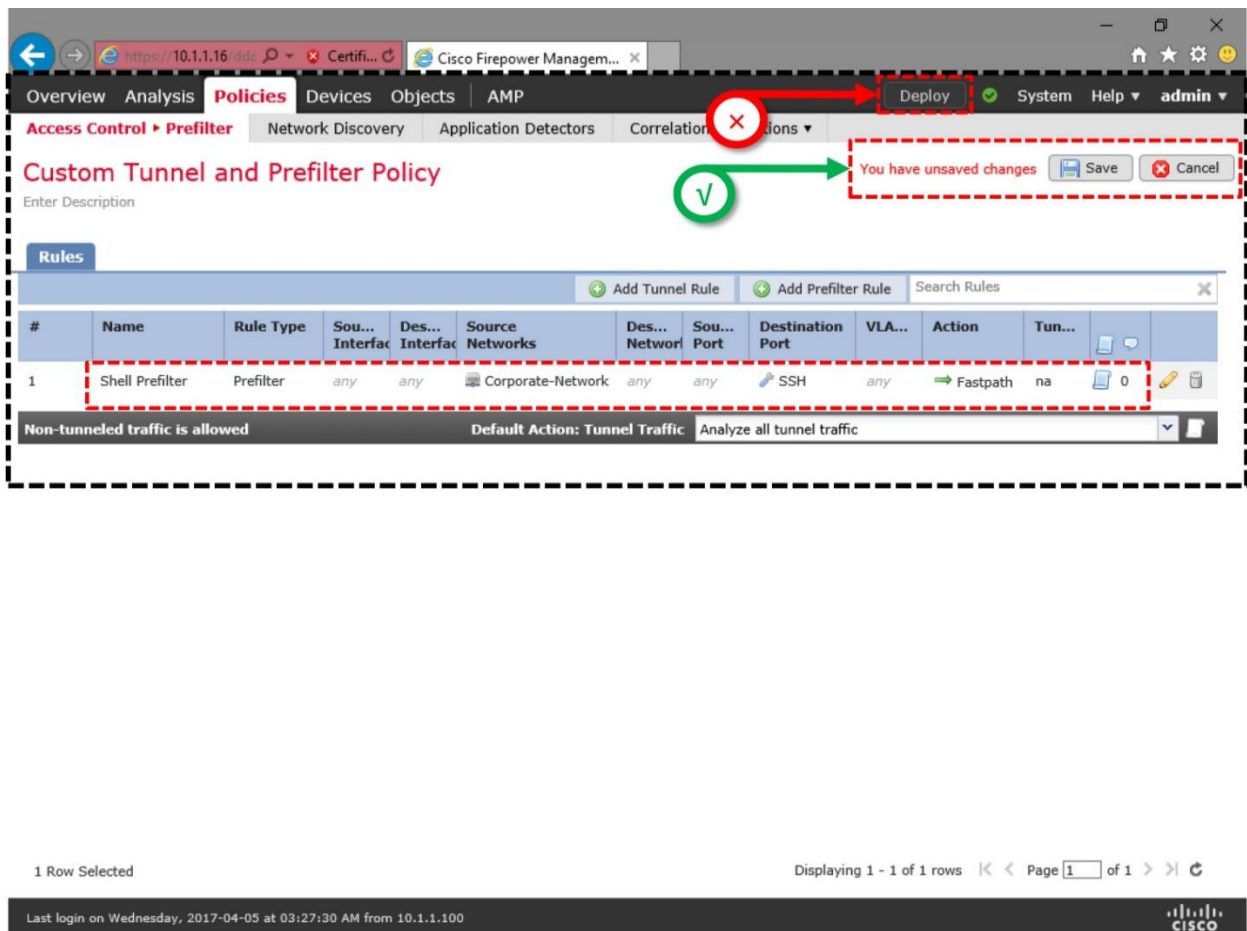


Figure 14-10. View of a Prefilter Rule that Can Bypass SSH Traffic from 192.168.1.0/24.

Invoking Prefilter Policy into an Access Control Policy

To invoke a custom prefilter policy into your desired Access Control policy, follow the steps below:

Step 1. Navigate to the **Policies > Access Control > Access Control**. The Access Control policy page appears.

Step 2. Edit the policy that you want to deploy on your FTD. Use the *pencil* icon, next to the name of a policy, to open the Access Control policy editor page.

Step 3. Look at the top-left side of the policy editor page. You should be able to find a link to the currently selected prefilter policy. Click on the link. By default, an Access Control policy uses the **Default Prefilter Policy**.

Figure 14-11 confirms that this access control policy invokes the prefilter rules from the **Default Prefilter Policy**. Click on the name of the prefilter policy to make a change.

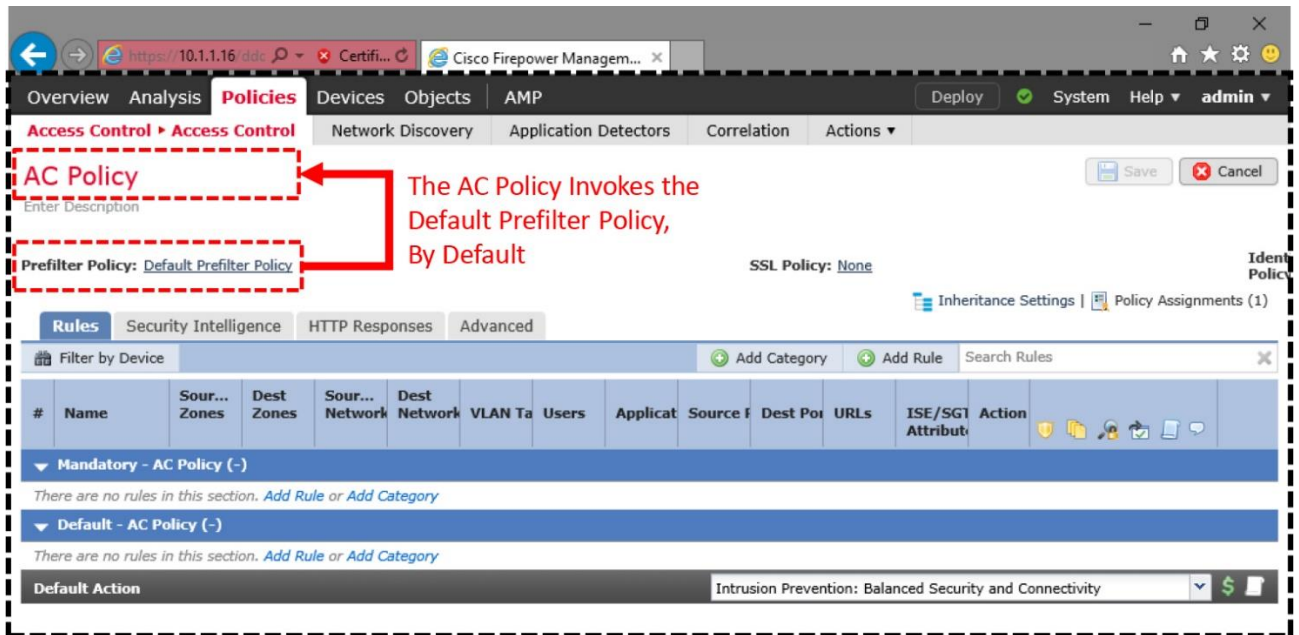


Figure 14-11. *By Default, An Access Control Policy Uses the Default Prefilter Policy*

Step 4. After you click the link, a **Prefilter Policy** popup window appears. It presents the available prefilter policies in a drop-down.

Step 5. Select the newly created **Custom Tunnel and Prefilter Policy**. Press **OK** to proceed.

Figure 14-12 shows the available options for prefilter policy. The drop-down shows the default policy along with any custom policies.

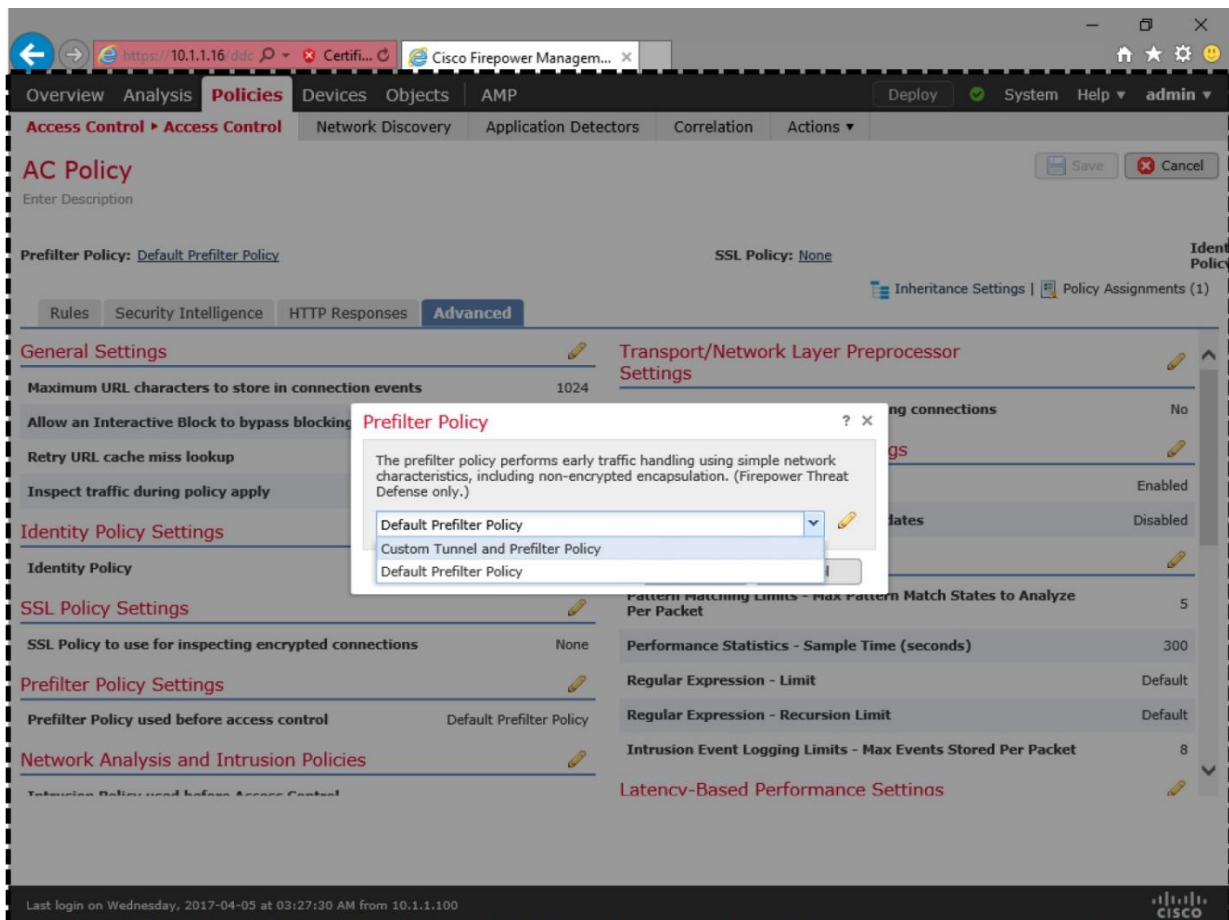


Figure 14-12. Prefilter Policy Drop-Down

You could have saved and deployed the Access Control policy at this stage. However, to determine if an Access Control policy inspects a connection, you can enable the logging for the default action. It helps to understand the lifecycle of a packet, and to troubleshoot any potential issue. Here are steps for it.

Step 1. Go to the **Rules** tab of the Access Control policy editor page.

Step 2. Select the *logging* icon that is next to the **Default Action** drop down.

Figure 14-13 shows the Logging icon that offers options to log at the beginning and end of a connection. It also confirms your selection for the custom prefilter policy.

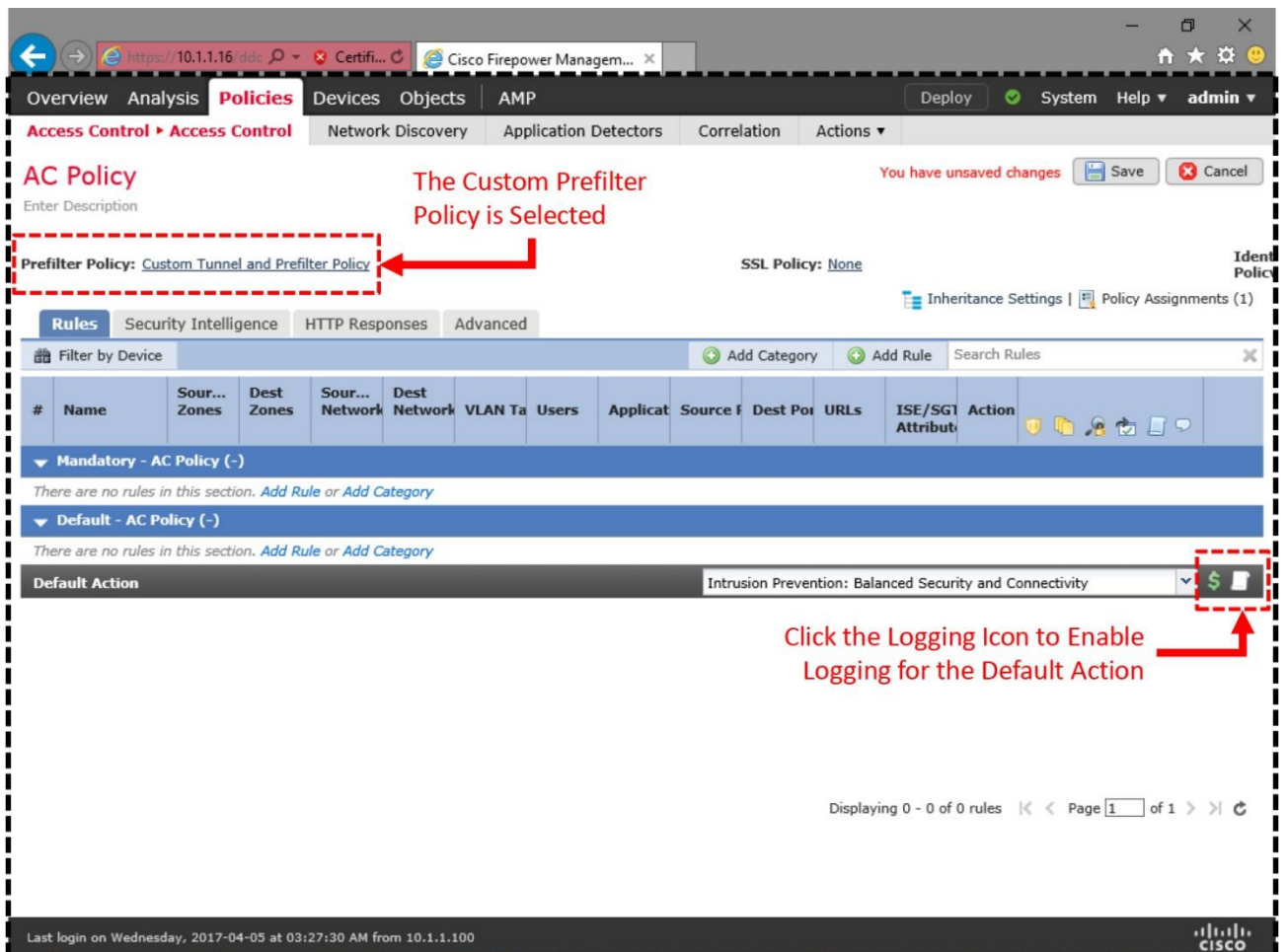


Figure 14-13. Logging Icon for the Default Action

Step 3. Select either **Log at Beginning of Connection**, or **Log at End of Connection**. However, do not select both as it can affect the system performance.

Step 4. Click the **OK** button to return to the policy editor page, and save the changes. Finally, deploy the changes to your FTD.

Verification of Configuration

Using the CLI, you can verify if a prefilter rule is active on an FTD.

[Example 14-1](#) shows the list of access rules that are active on an FTD. The custom prefilter rule, *Shell Prefilter*, is positioned on top of any other access rules, because a Prefilter policy acts on traffic before any security policies.

Example 14-1 Position of a Prefilter Rule on the Active Rule Set

```
> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list CSM_FW_ACL; 7 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL line 1 remark rule-id 268440577: PREFILTER POLICY:
Custom Tunnel and Prefilter Policy
access-list CSM_FW_ACL line 2 remark rule-id 268440577: RULE: Shell
Prefilter
access-list CSM_FW_ACL line 3 advanced trust tcp object Corporate-Network
any object-group SSH rule-id 268440577 event-log both (hitcnt=0) 0xe9257885
      access-list CSM_FW_ACL line 3 advanced trust tcp 192.168.1.0
255.255.255.0 any eq ssh rule-id 268440577 event-log both (hitcnt=0)
0xad5d48f9
access-list CSM_FW_ACL line 4 remark rule-id 268438529: PREFILTER POLICY:
Custom Tunnel and Prefilter Policy
access-list CSM_FW_ACL line 5 remark rule-id 268438529: RULE: DEFAULT
TUNNEL ACTION RULE
access-list CSM_FW_ACL line 6 advanced permit ipinip any any rule-id
268438529 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL line 7 advanced permit 41 any any rule-id 268438529
(hitcnt=0) 0x06095aba
access-list CSM_FW_ACL line 8 advanced permit gre any any rule-id
268438529 (hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL line 9 advanced permit udp any eq 3544 any range
1025 65535 rule-id 268438529 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL line 10 advanced permit udp any range 1025 65535
any eq 3544 rule-id 268438529 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL line 11 remark rule-id 268434432: ACCESS POLICY: AC
Policy - Default/1
access-list CSM_FW_ACL line 12 remark rule-id 268434432: L4 RULE: DEFAULT
ACTION RULE
access-list CSM_FW_ACL line 13 advanced permit ip any any rule-id
268434432 (hitcnt=34) 0xald3780e
>
```

Enabling Tools for Advanced Analysis

Before you run live SSH traffic, enable few debug tools. It helps you to understand the action of a rule, and flow of a packet.

Step 1. At first, capture the SSH traffic from the ASA Firewall engine:

```
> capture ssh_traffic trace interface INSIDE_INTERFACE match tcp any any eq
22
```

You can run the **show capture** command to confirm that the capture process is running. The “0 bytes” indicates that the FTD has not received any packets.

```
> show capture
capture ssh_traffic type raw-data trace interface INSIDE_INTERFACE
[Capturing - 0 bytes]
  match tcp any any eq ssh
>
```

To clear any previously captured packets from the memory, and to restart the capture from the next matched packets, run the **clear capture** command.

```
> clear capture /all
```

Step 2. Next, begin the capture of TCP traffic from the Firepower Snort engine. It helps you to determine if Snort engine see any bypassed traffic.

[Example 14-2](#) shows the command to capture TCP traffic from an inline pair.

Example 14-2 *Command to Capture Traffic from the Firepower Snort Engine*

```
> capture-traffic

Please choose domain to capture traffic from:
  0 - br1
  1 - INSIDE_OUTSIDE_PAIR inline set

Selection? 1

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: -n tcp
```

Step 3. Since the current CLI terminal has entered into the packet capture mode, access the FTD from a new separate terminal. You can connect through SSH or console connection.

On the second terminal connection to the FTD, perform the following steps:

Step 4. Reset the counters for Snort Statistics. It helps you to determine the exact number of events for your test traffic.

```
> clear snort statistics
```

Step 5. Enable debug for firewall engine. It allows you to determine the actions applied to any traffic.

[Example 14-3](#) shows the command that generates debug data when FTD inspects TCP traffic.

Example 14-3 *Command to Collect Debug Data from the Firewall Engine*

```
> system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
```


Monitoring firewall engine debug messages

Analysis of the Fastpath Action

Let's verify the action of the custom prefilter policy. Since the Prefilter policy has a rule to bypass SSH traffic, you need to generate SSH traffic between the client (192.168.1.2) and server (192.168.1.200), to verify the fastpath action.

First, connect to the server (192.168.1.200) from the host (192.168.1.2), using an SSH client. The FTD should fastpath the SSH traffic. Then, go to the **Analysis > Connection > Events** page; you should be able view a connection event for the fastpath action.

[Figure 14-14](#) exhibits a connection event triggered by the Shell Prefilter — a custom prefilter rule.

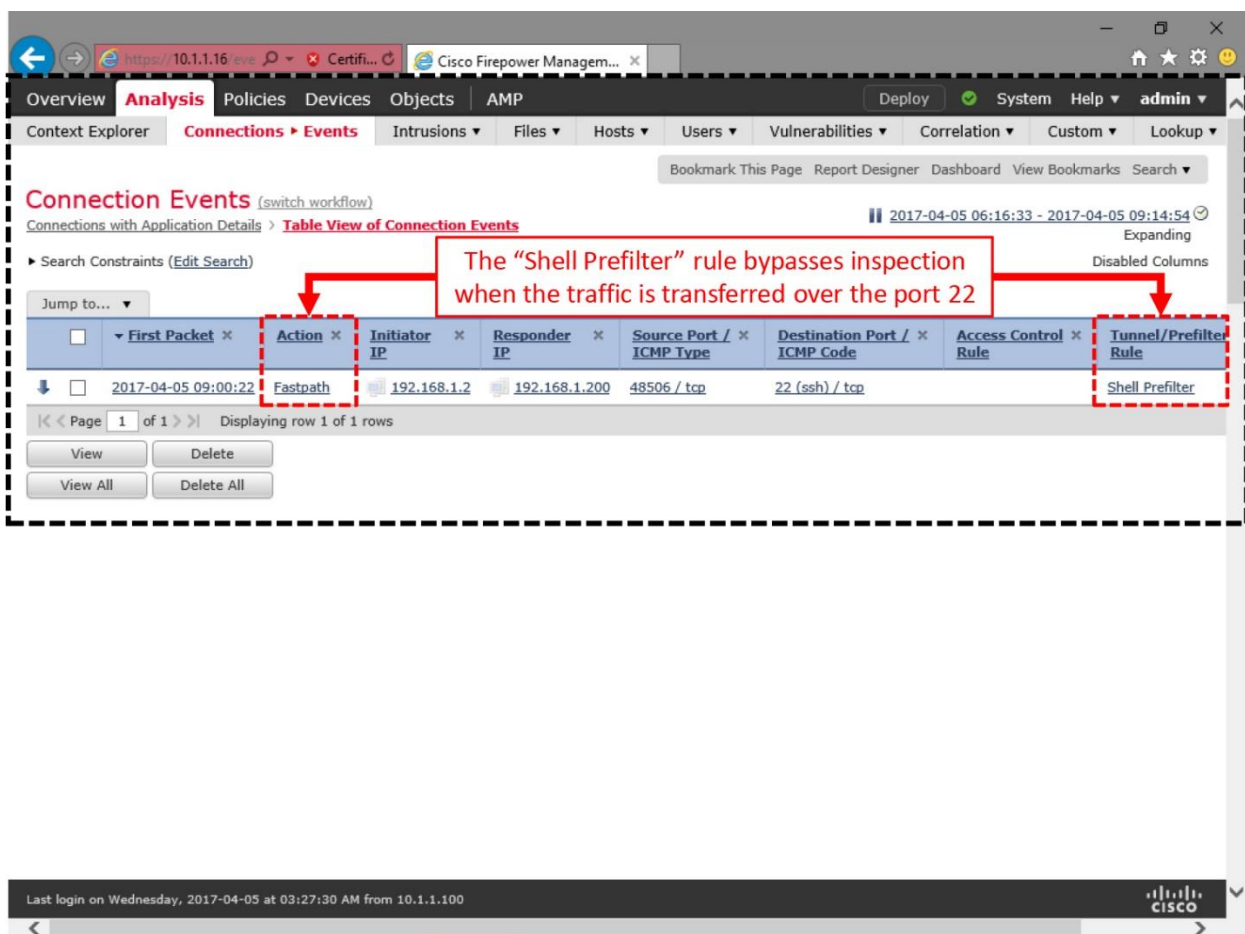


Figure 14-14. Connection Event for the Fastpath Action

Next, go to the CLI terminal where the firewall-engine-debug is running. Check the status of the tool. You should see some logs.

[Example 14-4](#) analyzes the debug data from an FTD when a prefilter rule applies fastpath action on the SSH traffic.

Example 14-4 Bypassed Connection Generates Event Logs and Increases Counters

```
! The firewall-engine-debug tool receives events from hardware in real time.
```

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages
```

```
192.168.1.2-48506 > 192.168.1.200-22 6 AS 5 I 0 Got start of flow event
from hardware with flags 84000001
192.168.1.2-48506 > 192.168.1.200-22 6 AS 5 I 0 Got end of flow event from
hardware with flags 84000001
^C
Caught interrupt signal
Exiting.
```

```
>
```

```
! The Snort statistics keeps a record of these events under the Miscellaneous Counters section.
```

```
> show snort statistics
```

```
Packet Counters:
  Passed Packets                                0
  Blocked Packets                               0
  Injected Packets                              0

Flow Counters:
  Fast-Forwarded Flows                         0
  Blacklisted Flows                            0
  Flows bypassed (Snort Down)                  0
  Flows bypassed (Snort Busy)                  0

Miscellaneous Counters:
  Start-of-Flow events                          1
  End-of-Flow events                            1
  Denied flow events                            0
  Frames forwarded to Snort before drop         0
  Inject packets dropped                        0
```

```
>
```

Next, go to the terminal where the **capture-traffic** command is running, and analyze the captured packets.

[Example 14-5](#) demonstrates that the Firepower Snort engine does not see any SSH traffic. However, the ASA Firewall engine can see and capture that traffic.

Example 14-5 Firewall and Firepower Engines Show Different Behavior during Capture

```
> capture-traffic
```

```
Please choose domain to capture traffic from:
  0 - br1
  1 - INSIDE_OUTSIDE_PAIR inline set
```

Selection? 1

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: **-n tcp**

! If the Firepower Snort engine would see traffic, it would appear here.
! Press the Control+C keys to exit from the capture-traffic tool.

^C
Caught interrupt signal
Exiting.

! Check the status of the capture on the ASA Firewall engine.

> **show capture ssh_traffic**

61 packets captured

```
1: 13:00:22.730156      192.168.1.2.48506 > 192.168.1.200.22: S
1199563799:1199563799(0) win 29200 <mss 1460,sackOK,timestamp 4732110
0,nop,wscale 7>
2: 13:00:22.730492      192.168.1.200.22 > 192.168.1.2.48506: S
2739603340:2739603340(0) ack 1199563800 win 28960 <mss
1460,sackOK,timestamp 1446067
4732110,nop,wscale 7>
3: 13:00:22.730659      192.168.1.2.48506 > 192.168.1.200.22: . ack
2739603341
win 229 <nop,nop,timestamp 4732110 1446067>
4: 13:00:22.730949      192.168.1.2.48506 > 192.168.1.200.22: P
1199563800:1199563841(41) ack 2739603341 win 229 <nop,nop,timestamp 4732110
1446067>
5: 13:00:22.731132      192.168.1.200.22 > 192.168.1.2.48506: . ack
1199563841
win 227 <nop,nop,timestamp 1446067 4732110>
.
.
```

! You can see all of the SSH packets generated by your connection. The above output shows only the first TCP three way handshake, as an example. The remaining outputs are omitted for brevity.

[Example 14-6](#) analyzes the flow of a packet that bypasses the FTD inspection due to the Fastpath action on the *Shell Prefilter* rule. Note the absence of the Snort inspection phase in this trace data.

Example 14-6 Analysis of a Packet Flow that Follows the Fastpath Action

> **show capture ssh_traffic packet-number 1 trace**

61 packets captured

1: 13:00:22.730156 192.168.1.2.48506 > 192.168.1.200.22: S
1199563799:1199563799(0) win 29200 <mss 1460,sackOK,timestamp 4732110
0,nop,wscale 7>

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS
services will be applied

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_global
access-list CSM_FW_ACL_advanced trust tcp object Corporate-Network any
object-group SSH rule-id 268440577 event-log both
access-list CSM_FW_ACL_remark rule-id 268440577: PREFILTER POLICY: Custom
Tunnel and Prefilter Policy
access-list CSM_FW_ACL_remark rule-id 268440577: RULE: Shell Prefilter
object-group service SSH tcp
port-object eq ssh
Additional Information:

Phase: 5
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Ingress interface INSIDE_INTERFACE is in NGIPS inline mode.
Egress interface OUTSIDE_INTERFACE is determined by inline-set
configuration

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 81, packet dispatched to next module

```
Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: allow
```

```
1 packet shown
>
```

Trust through an Access Policy

A Trust rule can bypass traffic without performing any deep packet inspection and network discovery. It supports granular filters based on Security Intelligence data, application fingerprint, URL filtering, user identities, etc. In this section, you will learn how to trust Telnet traffic, as an example of trusting a TCP protocol.

Caution

This chapter uses Telnet service to demonstrate the flow of a TCP packet. However, you should not trust any connection unless you have complete understanding about that particular traffic, and their source and destination.

Configuration

This section describes how to trust the default port of the Telnet protocol, port 23.

Step 1. Navigate to the **Policies > Access Control > Access Control**. The Access Control policy page appears.

Step 2. Edit the policy that you want to deploy on your FTD. Use the *pencil* icon, next to the name of a policy, to open the Access Control policy editor page.

Step 3. Select the **Add Rule** button to create a new access rule. The **Add Rule** window appears.

Figure 14-15 provides an overview of an Access Control policy editor page. It shows an **Add Rule** button that opens the access rule editor.

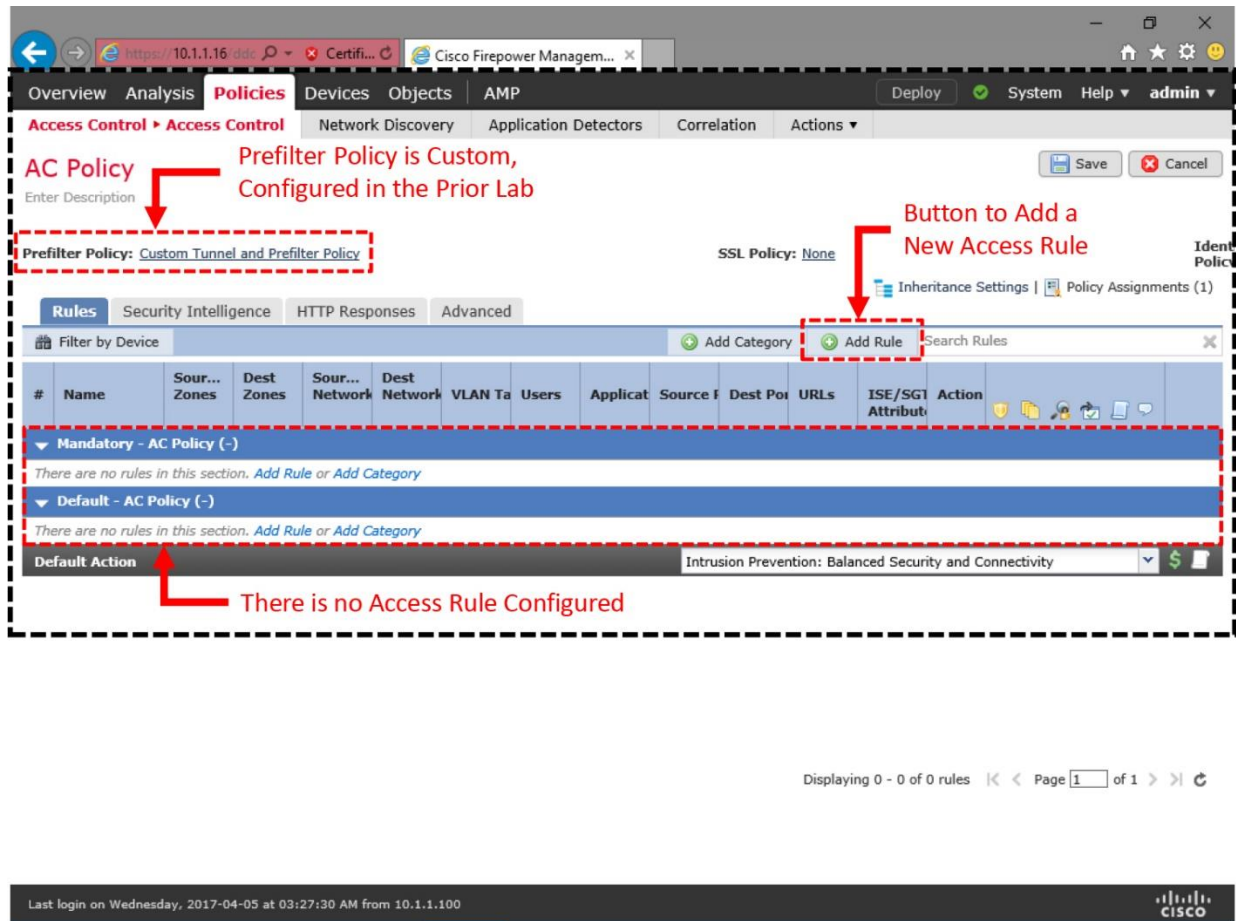


Figure 14-15. Access Control Policy Editor Shows the Status and the “Add Rule” Button

Step 4. Give a name to the access rule, and select the **Trust** action.

Step 5. Define the condition of the access rule. Go to the **Networks** tab, and select *Corporate-Network* as the Source networks.

Figure 14-16 shows the configuration of the *Telnet Access* rule. The rule trusts any Telnet traffic coming from 192.168.1.0/24, the internal corporate network.

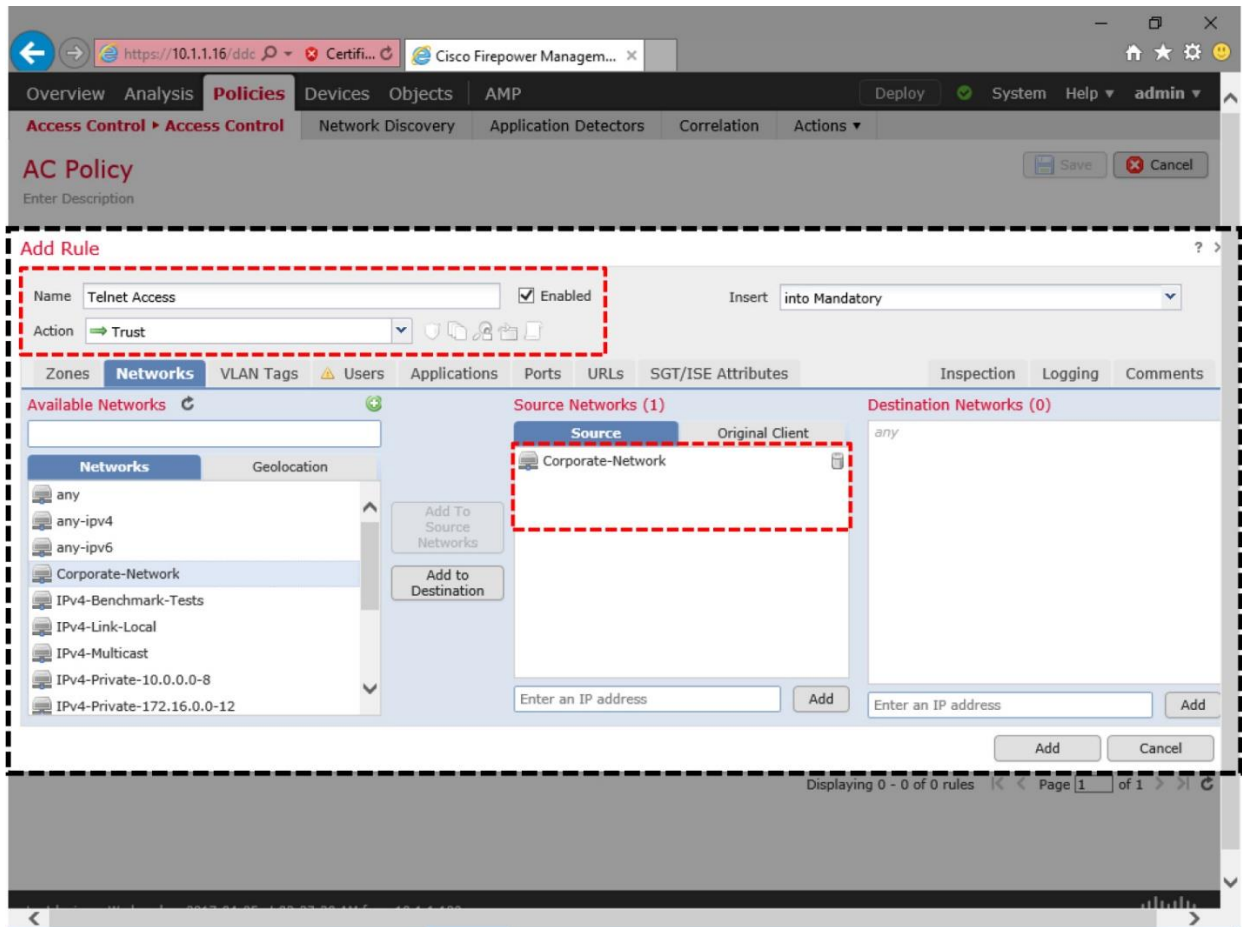


Figure 14-16. Access Rule to Trust Telnet Traffic — Configuration of Source Network

Step 6. On the **Ports** tab, select *Telnet* as the destination ports.

Figure 14-17 shows the selection of Telnet (Port 23) as the destination port.

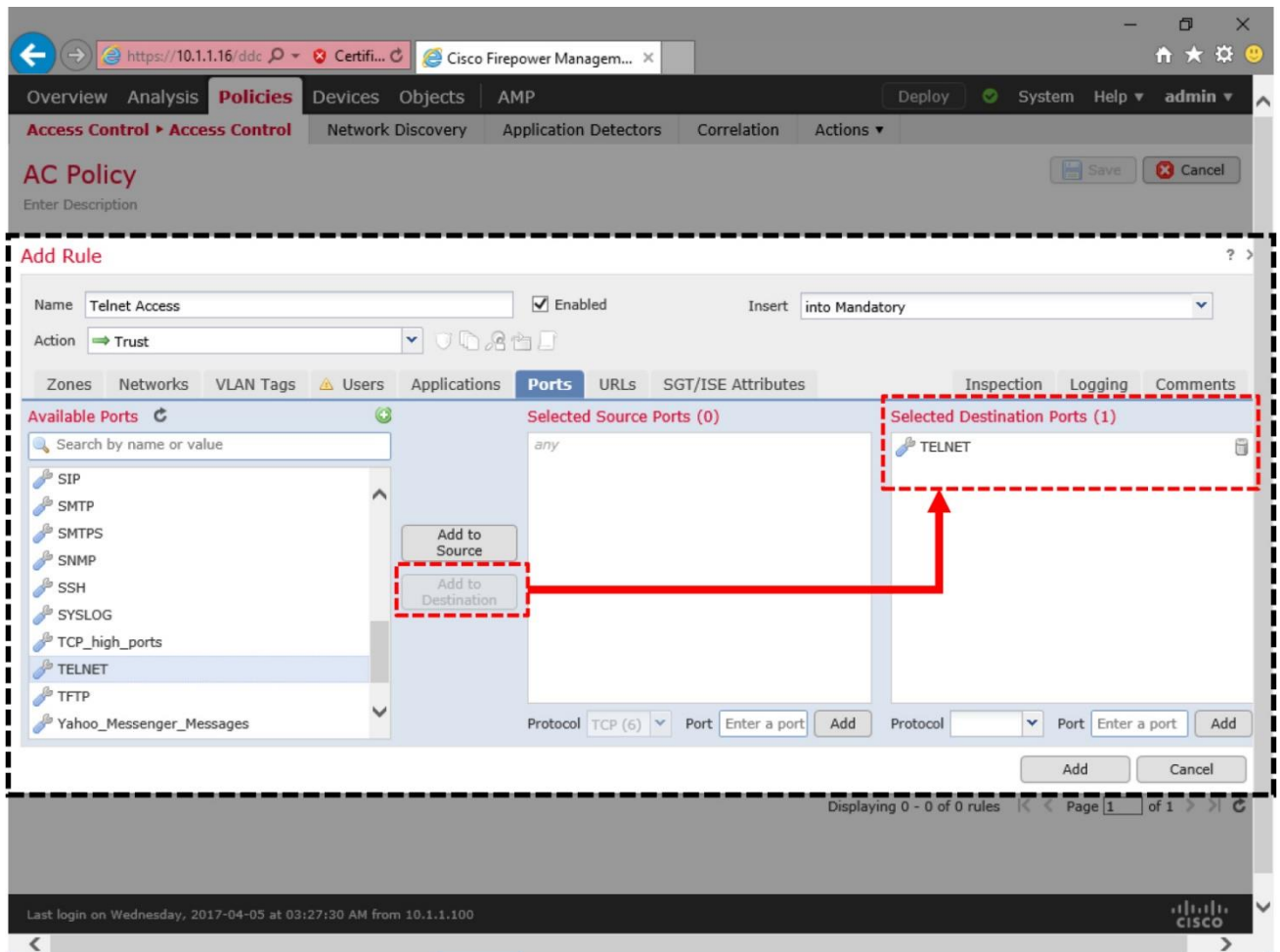


Figure 14-17. Access Rule to Trust Telnet Traffic — Configuration of Destination Port

Step 7. Optionally, go to the **Logging** tab to enable logging, so that you can determine when FTD trusts a connection. Select either **Log at Beginning of Connection**, or **Log at End of Connection**. However, do not select both as it can affect the system performance.

Step 8. Click the **Add** button to complete the trust rule configuration. You will return to the policy editor page.

Step 9. Use the **Save** button to save the changes, and then select the **Deploy** button to activate the rule.

Verification of Configuration

Using the CLI, you can verify if a trust rule is active on an FTD.

[Example 14-7](#) shows the list of access rules that are active on an FTD. The trust rule, *Telnet Access*, is placed below the prefilter rule, *Shell Prefilter*.

Example 14-7 Position of a Trust Rule on the Active Rule Set

```
> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list CSM_FW_ACL_ ; 8 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 268440577: PREFILTER POLICY:
Custom Tunnel and Prefilter Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 268440577: RULE: Shell
Prefilter
access-list CSM_FW_ACL_ line 3 advanced trust tcp object Corporate-Network
any object-group SSH rule-id 268440577 event-log both (hitcnt=4) 0xe9257885
access-list CSM_FW_ACL_ line 3 advanced trust tcp 192.168.1.0 255.255.255.0
any eq ssh rule-id 268440577 event-log both (hitcnt=4) 0xad5d48f9
access-list CSM_FW_ACL_ line 4 remark rule-id 268438529: PREFILTER POLICY:
Custom Tunnel and Prefilter Policy
access-list CSM_FW_ACL_ line 5 remark rule-id 268438529: RULE: DEFAULT
TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 6 advanced permit ipinip any any rule-id
268438529 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 7 advanced permit 41 any any rule-id 268438529
(hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 8 advanced permit gre any any rule-id
268438529 (hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL_ line 9 advanced permit udp any eq 3544 any range
1025 65535 rule-id 268438529 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 10 advanced permit udp any range 1025 65535
any eq 3544 rule-id 268438529 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 11 remark rule-id 268440580: ACCESS POLICY: AC
Policy - Mandatory/1
access-list CSM_FW_ACL_ line 12 remark rule-id 268440580: L7 RULE: Telnet
Access
access-list CSM_FW_ACL_ line 13 advanced permit tcp object Corporate-
Network any object-group TELNET rule-id 268440580 (hitcnt=3) 0x388a3b9d
access-list CSM_FW_ACL_ line 13 advanced permit tcp 192.168.1.0
255.255.255.0 any eq telnet rule-id 268440580 (hitcnt=3) 0x4a6c1f4c
access-list CSM_FW_ACL_ line 14 remark rule-id 268434432: ACCESS POLICY: AC
Policy - Default/1
access-list CSM_FW_ACL_ line 15 remark rule-id 268434432: L4 RULE: DEFAULT
ACTION RULE
access-list CSM_FW_ACL_ line 16 advanced permit ip any any rule-id
268434432 (hitcnt=144) 0xald3780e
>
```

Enabling Tools for Advanced Analysis

Before you generate live Telnet traffic, enable few debug tools. It helps you to understand the action of a rule, and flow of a packet.

Step 1. At first, capture the telnet traffic from the ASA Firewall engine:

```
> capture telnet_traffic trace interface INSIDE_INTERFACE match tcp any any
eq 23
```

You can run the **show capture** command to confirm that the capture process is running. The “0 bytes” indicates that the FTD has not received any packets.

```
> show capture
capture telnet traffic type raw-data trace interface INSIDE_INTERFACE
[Capturing - 0 bytes]
  match tcp any any eq telnet
>
```

If the FTD is running a capture for SSH traffic that you enabled in the previous lab exercise, you can remove it using the **no** keyword with the **capture** command, as it not necessary for this lab:

```
> no capture ssh_traffic
```

To clear any previously captured packets from the memory, and to restart the capture from the next matched packets, run the **clear capture** command.

```
> clear capture /all
```

Step 2. Next, begin the capture of TCP traffic from the Firepower Snort engine. It helps you to determine if Snort engine see any bypassed traffic.

[Example 14-8](#) shows the command to capture TCP traffic from an inline pair.

Example 14-8 *Command to Capture Traffic from the Firepower Snort Engine*

```
> capture-traffic

Please choose domain to capture traffic from:
  0 - br1
  1 - INSIDE_OUTSIDE_PAIR inline set

Selection? 1

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: -n tcp
```

Step 3. Since the current CLI terminal has entered into the packet capture mode, access the FTD from a new separate terminal. You can connect through SSH or console connection.

On the second terminal connection to the FTD, perform the following steps:

Step 4. Reset the counters for Snort Statistics. It helps you to determine the exact number of events for your test traffic.

```
> clear snort statistics
```

Step 5. Enable debug for firewall engine. It allows you to determine the actions applied to any traffic.

[Example 14-9](#) shows the command that generates debug data when FTD inspects TCP traffic.

Example 14-9 Command to Collect Debug Data from the Firewall Engine

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages
```

Analysis of the Trust Action

Let's verify the action of the trust rule you created. Since the Access Control policy has a rule to bypass Telnet traffic, you need to generate Telnet traffic between the client (192.168.1.2) and server (192.168.1.200), to verify the trust action.

First, connect to the server (192.168.1.200) from the host (192.168.1.2), using a Telnet client. The FTD should trust the Telnet traffic. Then, go to the **Analysis > Connection > Events** page; you should be able view a connection event for the trust action.

[Figure 14-18](#) exhibits a new connection event triggered by the *Telnet Access* rule — an access rule with trust action.

The screenshot displays the Cisco Firepower Management Center interface. The main navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP'. The 'Analysis' tab is active, and the 'Connections > Events' sub-tab is selected. The page title is 'Connection Events' with a '(switch workflow)' link. Below the title, there are search and filter options, including a 'Search Constraints (Edit Search)' field and a 'Jump to...' dropdown. The main content area shows a table of connection events. The table has columns for 'First Packet', 'Action', 'Initiator IP', 'Responder IP', 'Source Port / ICMP Type', 'Destination Port / ICMP Code', 'Access Control Rule', and 'Tunnel/Prefilter Rule'. Two rows of events are visible. The first row, dated '2017-04-05 13:19:49', shows an 'Action' of 'Trust', an 'Initiator IP' of '192.168.1.2', a 'Responder IP' of '192.168.1.200', 'Source Port / ICMP Type' of '55822 / tcp', 'Destination Port / ICMP Code' of '23 (telnet) / tcp', and an 'Access Control Rule' of 'Telnet Access'. The second row, dated '2017-04-05 09:00:22', shows an 'Action' of 'Fastpath', an 'Initiator IP' of '192.168.1.2', a 'Responder IP' of '192.168.1.200', 'Source Port / ICMP Type' of '48506 / tcp', 'Destination Port / ICMP Code' of '22 (ssh) / tcp', and a 'Tunnel/Prefilter Rule' of 'Shell Prefilter'. Red dashed boxes highlight the 'Action' and 'Access Control Rule' columns for the first row. A red arrow points from the text 'The "Telnet Access" Rule Lets the FTD to Trust Telnet Traffic' to the 'Telnet Access' rule name. Another red arrow points from the same text to the 'Trust' action. The bottom of the page shows a footer with 'Last login on Wednesday, 2017-04-05 at 07:16:29 AM from 10.1.1.100' and the Cisco logo.

First Packet	Action	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Access Control Rule	Tunnel/Prefilter Rule
2017-04-05 13:19:49	Trust	192.168.1.2	192.168.1.200	55822 / tcp	23 (telnet) / tcp	Telnet Access	
2017-04-05 09:00:22	Fastpath	192.168.1.2	192.168.1.200	48506 / tcp	22 (ssh) / tcp		Shell Prefilter

Figure 14-18. Connection Event for the Trust Action

Next, go to the CLI terminal where the firewall-engine-debug is running. Check the status of the tool. You should see some logs.

[Example 14-10](#) analyzes the debug data from an FTD when an access rule applies trust action on the Telnet traffic.

Example 14-10 *Trusted Connection Generates Event Logs*

```
! The firewall-engine-debug tool shows that the "Telnet Access" rule applies Trust action.
```

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
192.168.1.2-55822 > 192.168.1.200-23 6 AS 5 I 1 New session
192.168.1.2-55822 > 192.168.1.200-23 6 AS 5 I 1 using HW or preset rule
order 3, 'Telnet Access', action Trust and prefilter rule 0
192.168.1.2-55822 > 192.168.1.200-23 6 AS 5 I 1 Deleting session
```

```
^C
```

```
Caught interrupt signal
Exiting.
```

```
>
```

Next, go to the terminal where the **capture-traffic** command is running and analyze the captured packets.

[Example 14-11](#) demonstrates that the Firepower Snort engine starts trusting the telnet traffic after the initial TCP three-way handshake is complete. Therefore, they do not appear in the capture-traffic output. However, the ASA Firewall engine can see and capture all of the traffic.

Example 14-11 Firewall and Firepower Engines Show Different Actions during Capture

```
! The Firepower Snort engine stops seeing traffic after the initial TCP three-way handshake.
```

```
> capture-traffic
```

```
Please choose domain to capture traffic from:
```

- 0 - br1
- 1 - INSIDE_OUTSIDE_PAIR inline set

```
Selection? 1
```

```
Please specify tcpdump options desired.
```

```
(or enter '?' for a list of supported options)
```

```
Options: -n tcp
```

```
17:19:49.089991 IP 192.168.1.2.55822 > 192.168.1.200.23: Flags [S], seq 1700253547, win 29200, options [mss 1460,sackOK,TS val 7177698 ecr 0,nop,wscale 7], length 0
```

```
17:19:49.089991 IP 192.168.1.200.23 > 192.168.1.2.55822: Flags [S.], seq 495495803, ack 1700253548, win 28960, options [mss 1460,sackOK,TS val 3421593 ecr 7177698,nop,wscale 7], length 0
```

```
17:19:49.109979 IP 192.168.1.2.55822 > 192.168.1.200.23: Flags [.], ack 1, win 229, options [nop,nop,TS val 7177701 ecr 3421593], length 0
```

```
17:19:49.109979 IP 192.168.1.2.55822 > 192.168.1.200.23: Flags [P.], ack 1, win 229, options [nop,nop,TS val 7177701 ecr 3421593], length 27
```

```
! Nothing appears after the above packets, because they are trusted.
```

```
^C
```

```
Caught interrupt signal
```

```
Exiting.
```

```
>
```

```
! However, the ASA Firewall engine sees all of the traffic generated by the telnet connection.
```

```
> show capture telnet_traffic
```

```
78 packets captured
```

```
1: 17:19:49.096766 192.168.1.2.55822 > 192.168.1.200.23: S 1700253547:1700253547(0) win 29200 <mss 1460,sackOK,timestamp 7177698 0,nop,wscale 7>
2: 17:19:49.109781 192.168.1.200.23 > 192.168.1.2.55822: S 495495803:495495803(0) ack 1700253548 win 28960 <mss 1460,sackOK,timestamp 3421593 7177698,nop,wscale 7>
3: 17:19:49.110086 192.168.1.2.55822 > 192.168.1.200.23: . ack 495495804 win 229 <nop,nop,timestamp 7177701 3421593>
4: 17:19:49.110391 192.168.1.2.55822 > 192.168.1.200.23: P 1700253548:1700253575(27) ack 495495804 win 229 <nop,nop,timestamp 7177701 3421593>
5: 17:19:49.110651 192.168.1.200.23 > 192.168.1.2.55822: . ack 1700253575 win 227 <nop,nop,timestamp 3421596 7177701>
6: 17:19:49.116037 192.168.1.200.23 > 192.168.1.2.55822: P 495495804:495495816(12) ack 1700253575 win 227 <nop,nop,timestamp 3421597 7177701>
7: 17:19:49.116159 192.168.1.2.55822 > 192.168.1.200.23: . ack 495495816 win 229 <nop,nop,timestamp 7177703 3421597>
```

When a packet matches a prefilter rule with fastpath action, the packet does not go through the Snort inspection phase. You verified that in the previous section by analyzing the trace data of a captured packet.

Now, this section demonstrates that the Firepower Snort engine processes the initial TCP handshake before it begins trusting the rest of a connection. Therefore, the initial packets appear in the capture-traffic output. You can verify the cause of this behavior by looking into the tracing data. You should see two different Snort verdicts — the first telnet packet is allowed, and the subsequent flows are fast-forwarded.

[Example 14-12](#) shows an analysis of the first packet of a trusted TCP connection. The Snort verdict is to allow this packet.

Example 14-12 *Analysis of the First Packet of a Trusted Telnet Connection*

```
> show capture telnet_traffic packet-number 1 trace
```

```
78 packets captured
```

```
1: 17:19:49.096766 192.168.1.2.55822 > 192.168.1.200.23: S
1700253547:1700253547(0) win 29200 <mss 1460,sackOK,timestamp 7177698
0,nop,wscale 7>
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 3
```

```
Type: NGIPS-MODE
```

```
Subtype: ngips-mode
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
The flow ingressed an interface configured for NGIPS mode and NGIPS
services will be applied
```

```
Phase: 4
```

```
Type: ACCESS-LIST
```

```
Subtype: log
```

```
Result: ALLOW
```

```
Config:
```

```
access-group CSM_FW_ACL_global
```

```
access-list CSM_FW_ACL_advanced permit tcp object Corporate-Network any
object-group TELNET rule-id 268440580
```

```
access-list CSM_FW_ACL_remark rule-id 268440580: ACCESS POLICY: AC Policy
- Mandatory/1
```

```
access-list CSM_FW_ACL_ remark rule-id 268440580: L7 RULE: Telnet Access
object-group service TELNET tcp
port-object eq telnet
```

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: NGIPS-EGRESS-INTERFACE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

Ingress interface INSIDE_INTERFACE is in NGIPS inline mode.

Egress interface OUTSIDE_INTERFACE is determined by inline-set configuration

Phase: 6

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 282, packet dispatched to next module

Phase: 7

Type: EXTERNAL-INSPECT

Subtype:

Result: ALLOW

Config:

Additional Information:

Application: 'SNORT Inspect'

Phase: 8

Type: SNORT

Subtype:

Result: ALLOW

Config:

Additional Information:

Snort Verdict: (pass-packet) allow this packet

Result:

input-interface: INSIDE_INTERFACE

input-status: up

input-line-status: up

Action: allow

1 packet shown

>

[Example 14-13](#) shows an analysis of the third and fourth packets of a trusted TCP connection. The Snort verdicts for both packets are to fast-forward them.

Example 14-13 Analysis of the Subsequent Packets of a Trusted Telnet Connection

```
! Packet Number 3:
> show capture telnet_traffic packet-number 3 trace

78 packets captured

   3: 17:19:49.110086      192.168.1.2.55822 > 192.168.1.200.23: . ack
495495804 win 229 <nop,nop,timestamp 7177701 3421593>
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 282, using existing flow

Phase: 4
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 5
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (fast-forward) fast forward this flow

Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: allow

1 packet shown
>
```



```
! Packet Number 4:
```

```
> show capture telnet_traffic packet-number 4 trace
```

```
78 packets captured
```

```
4: 17:19:49.110391 192.168.1.2.55822 > 192.168.1.200.23: P  
1700253548:1700253575(27) ack 495495804 win 229 <nop,nop,timestamp 7177701  
3421593>
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
.
```

```
.
```

```
! Output is Omitted for Brevity
```

```
.
```

```
.
```

```
Phase: 5
```

```
Type: SNORT
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
Snort Verdict: (fast-forward) fast forward this flow
```

```
Result:
```

```
input-interface: INSIDE_INTERFACE
```

```
input-status: up
```

```
input-line-status: up
```

```
Action: allow
```

```
1 packet shown
```

```
>
```

[Example 14-14](#) shows a statistic of the passed packet and fast-forwarded flows. In this example, an FTD passes two telnet packets before it fast-forwards (trusts) the rest of the flows of a connection.

Example 14-14 Counters for a Trusted Telnet Connection

```
! The Snort statistics keep a record of these events using two types of  
counters.
```

```
> show snort statistics
```

```
Packet Counters:
```

Passed Packets	2
Blocked Packets	0
Injected Packets	0

```
Flow Counters:
```

Fast-Forwarded Flows	1
Blacklisted Flows	0
Flows bypassed (Snort Down)	0
Flows bypassed (Snort Busy)	0

```

Miscellaneous Counters:
  Start-of-Flow events          0
  End-of-Flow events           0
  Denied flow events           0
  Frames forwarded to Snort before drop 0
  Inject packets dropped        0
>

```

[Comparison with Allow Action](#)

Allow action passes a packet after it matches all of the conditions in an access rule. Unlike the trust action, the allow action does not fast-forward any packets. All of the packets in a connection is subject to inspection. To verify this behavior, deploy an access rule with allow action. This exercise redeploys the previously created Telnet Access rule by changing the action type from Trust to Allow.

[Figure 14-19](#) shows an access rule with allow action. The rule allows telnet traffic when it originates from the corporate network 192.168.1.0/24.

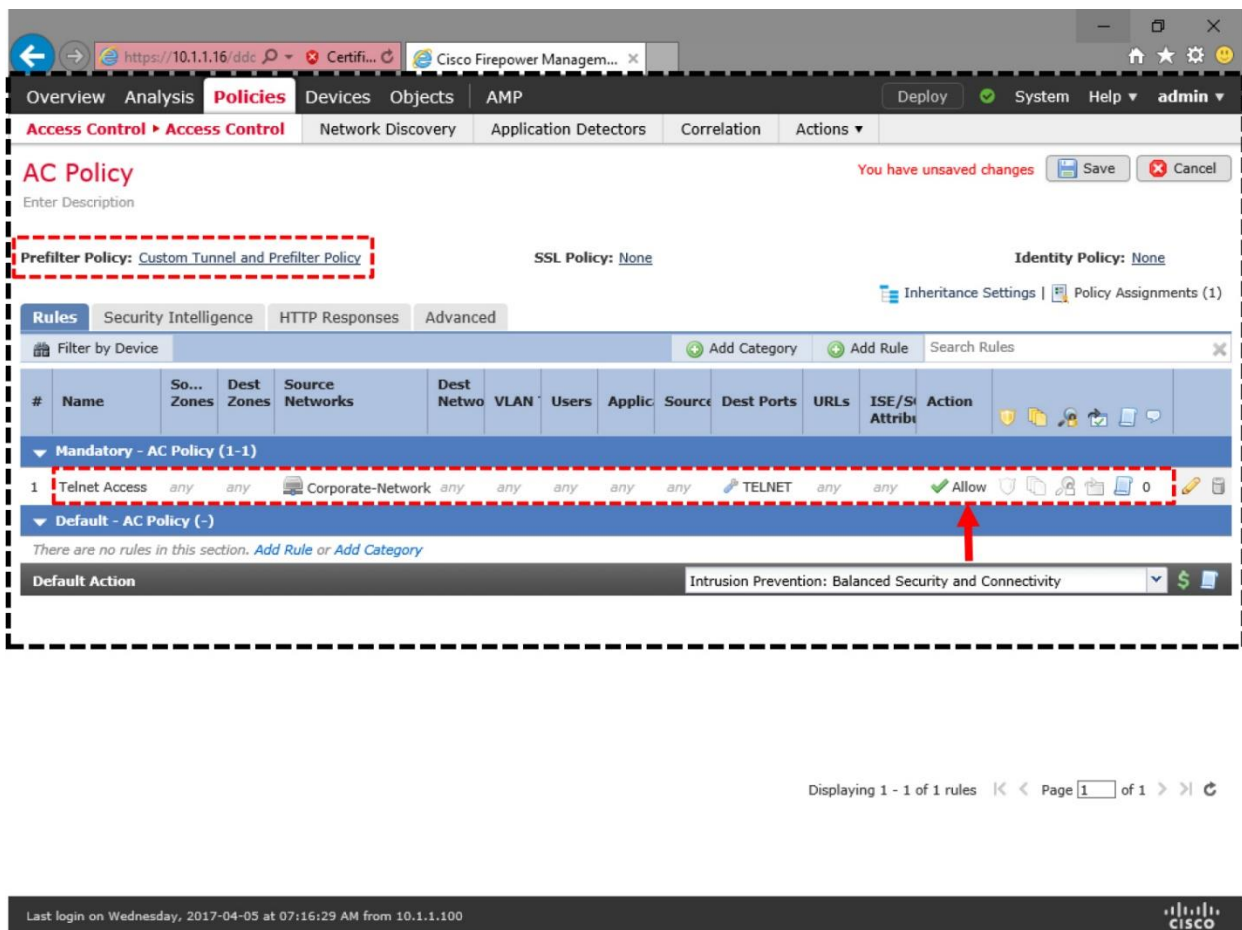


Figure 14-19. An Access Rule with Allow Action

After deploying the *Telnet Access* rule, if you connect from your host 192.168.1.2 to the server 192.168.1.200, you should be able to access. This time, the FMC shows an “Allow” action for it.

Figure 14-20 shows a connection event with allow action. FTD generates this event if you enable logging for the Telnet Access rule, and the rule matches with a telnet packet.

The Allow Action Makes the "Telnet Access" Rule to Permit Telnet Traffic Upon All Enabled Inspections

	First Packet	Action	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Access Control Rule	Tunnel/Prefilter Rule
2017-04-05 13:57:53	Allow	192.168.1.2	192.168.1.200	55828 / tcp	23 (telnet) / tcp	Telnet Access		
2017-04-05 13:19:49	Trust	192.168.1.2	192.168.1.200	55822 / tcp	23 (telnet) / tcp	Telnet Access		
2017-04-05 09:00:22	Fastpath	192.168.1.2	192.168.1.200	48506 / tcp	22 (ssh) / tcp		Shell Prefilter	

Page 1 of 1 | Displaying rows 1-3 of 3 rows

View Delete View All Delete All

Last login on Wednesday, 2017-04-05 at 07:16:29 AM from 10.1.1.100

Figure 14-20. A Connection Event for the Allowing a Telnet Connection

To verify the operation of an Allow action, you follow the same steps that you performed in the previous two exercises for Fastpath and Trust actions. However, you can just view the Snort statistics to determine if the allow action “passed” all of the packets, or “fast-forwarded” them.

[Example 14-15](#) proves that the allow action inspects and passes all of the packets. It does not fast-forward any packets the way the trust action handles the traffic.

Example 14-15 *Statistics of Packets after an “Allowed” Connection*

```
> show snort statistics
```

```
Packet Counters:
  Passed Packets                78
  Blocked Packets               0
  Injected Packets              0

Flow Counters:
  Fast-Forwarded Flows          0
  Blacklisted Flows            0
  Flows bypassed (Snort Down)   0
  Flows bypassed (Snort Busy)   0

Miscellaneous Counters:
  Start-of-Flow events         0
  End-of-Flow events           0
  Denied flow events           0
  Frames forwarded to Snort before drop 0
  Inject packets dropped       0
>
```

Summary

This chapter discusses the techniques to bypass an inspection. It provides the steps to configure different methods. The chapter also analyzes the flows of bypassed packets to demonstrate how an FTD acts during different bypassing option. You can learn the usage of various debug tools, which helps you to determine if the bypass process is working, as designed.

Quiz

- 1.** Which of the following rule can bypass one or more types of security inspection:
 - a. Prefilter rule
 - b. Tunnel rule
 - c. Access rule
 - d. All of the above

- 2.** Which of the following commands shows a statistic of the bypassed packets:
 - a. **show trust statistics**
 - b. **show snort statistics**
 - c. **show bypass statistics**
 - d. **show fastpath statistics**

- 3.** You are running the **capture-traffic** command on the FTD. When you initiate a connection between two hosts, you do not see any packet in the capture output, but they are able to connect successfully. Which of the following scenarios may be related:
 - a. Traffic between two hosts are inspected by the Snort engine, but events are suppressed.
 - b. Traffic between two hosts are trusted by the Access Control policy.
 - c. Traffic between two hosts are fastpathed by the Prefilter policy.
 - d. None of the above. If the traffic goes through an FTD and the hosts are connected, FTD must see the traffic.

- 4.** What is the difference between a prefilter rule and an access rule?
 - a. A prefilter rule matches for traffic prior to an access rule.
 - b. A prefilter rule analyzes traffic based on the outermost header of a packet, whereas an access rule analyzes the innermost header.
 - c. A prefilter rule supports limited options to create a rule condition, whereas an access rule offers many granular options.
 - d. All of the above.

Chapter 15. Rate Limiting of Traffic

You can employ your Firepower Threat Defense (FTD) to limit the rate of your network traffic after an access control rule allows or trusts the traffic. An FTD, however, does not regulate the rate of any particular traffic when a Prefilter policy applies the fastpath action on them. Limiting the rate of traffic is a way to manage the bandwidth of a network, and to ensure the Quality of Service (QoS) for business-critical applications. This chapter discusses the steps to configure QoS policy on an FTD, and to verify its operations.

Essential Knowledge

There are more than one ways to enable Quality of Service within a network. FTD implements the traffic policing mechanism to limit the rate of traffic. In this method, FTD drops excessive traffic when the traffic rate reaches a predefined limit. As of writing this book, FTD does not support traffic shaping technique, where excessive traffic is queued in a buffer — rather than dropping them — for later transmission.

[Figure 15-1](#) illustrates the crests and troughs of the traffic pattern when an FTD rate-limits traffic using the policing method.

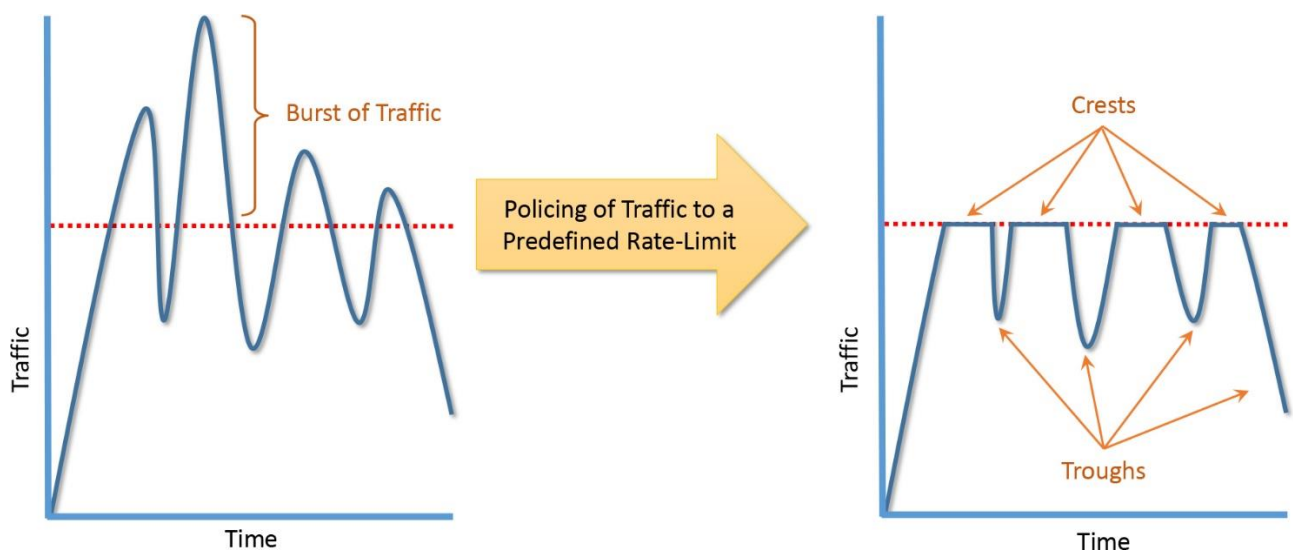


Figure 15-1. *Traffic Policing Method Drops Excessive Traffic*

[Figure 15-2](#) draws up a typical graph when traffic is rate-limited by the shaping mechanism.

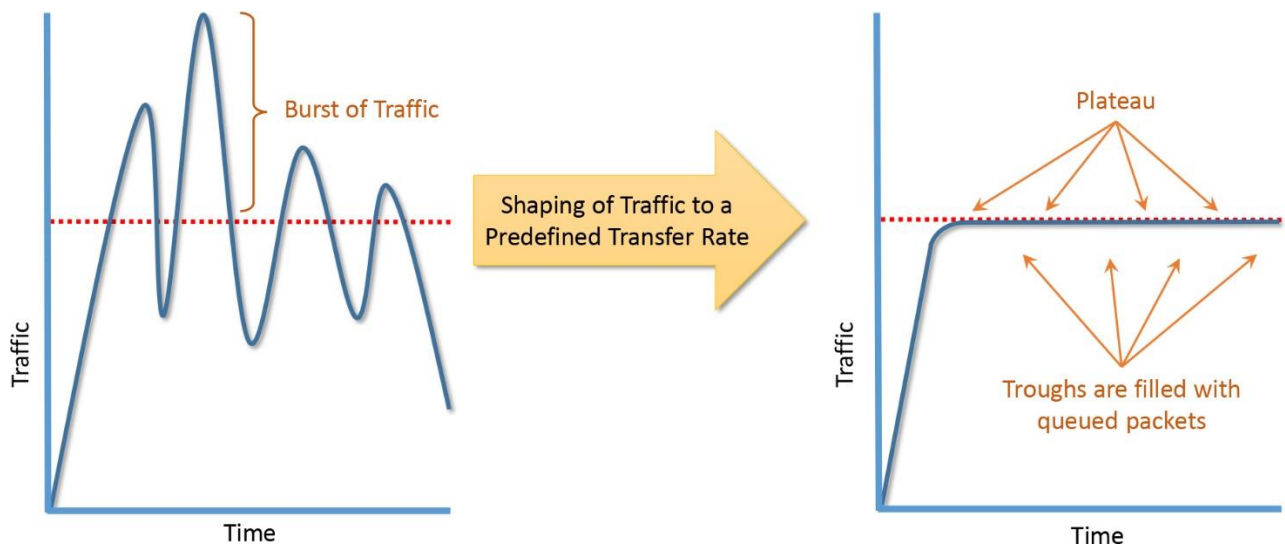


Figure 15-2. *Traffic Shaping Method Queues Excessive Traffic for Later Transmission*

At any given time, an FTD can have only one active QoS policy. However, you can add multiple QoS rules within a QoS policy. Each QoS rule must be associated with a source interface and a destination interface, where both of them have to be routed interfaces. You can set separate upload and download speed limit for the traffic that matches the conditions of a QoS rule. Furthermore, an FTD allows you to define the QoS rule conditions based on advanced networking characteristics, such as, network address, port number, application, URL, user identity, etc.

The Firepower Snort engine evaluates a QoS rule and classifies traffic. When a packet matches with a QoS rule, Snort engine sends the ID of the matching rule to the ASA Firewall engine. The Firewall engine limits the rate of individual flows based on the download and upload speed limit you defined on a QoS rule. You must enable logging at the end of a connection to view QoS related information.

[Figure 15-3](#) exhibits a workflow of the QoS feature on a Firepower system. You use an FMC to configure and apply a QoS policy, and view any QoS events. FTD ensures that the traffic conforms to the QoS rule.

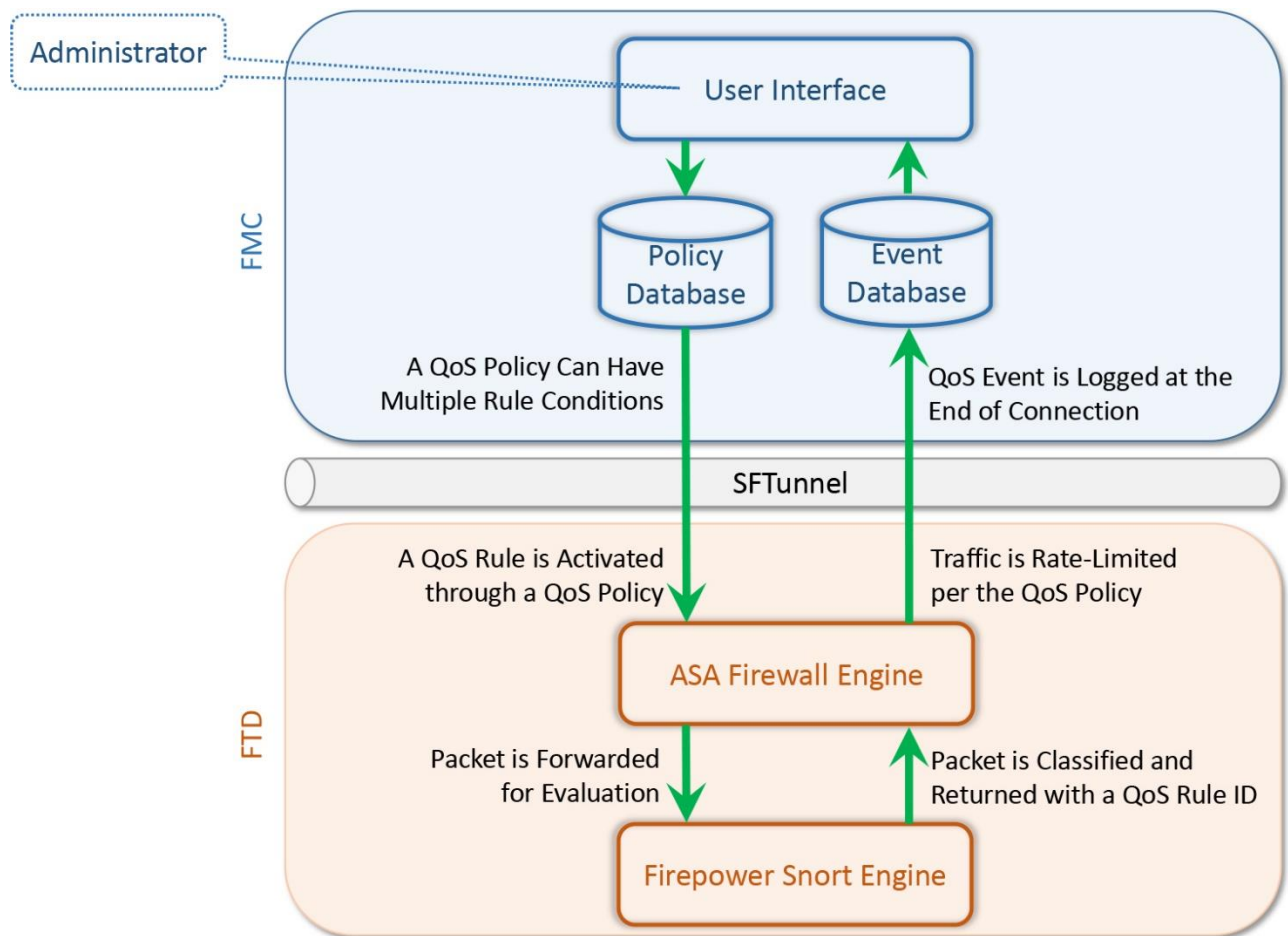


Figure 15-3. Architecture of the Quality of Service (QoS) Implementation on an FTD

Best Practices

As of writing this book, FTD supports up to 32 QoS rules within a single QoS policy. FTD allows you to add different rule conditions for different network segments that are connected to different FTD interfaces. However, you should enable a QoS rule as close to the source as possible. It ensures that the traffic does not consume the network and system resources more than it should.

[Figure 15-4](#) shows an example of a typical network where FTD enables different QoS rules through the same QoS policy. Traffic is originated from different source networks, and rate-limited by different QoS rules.

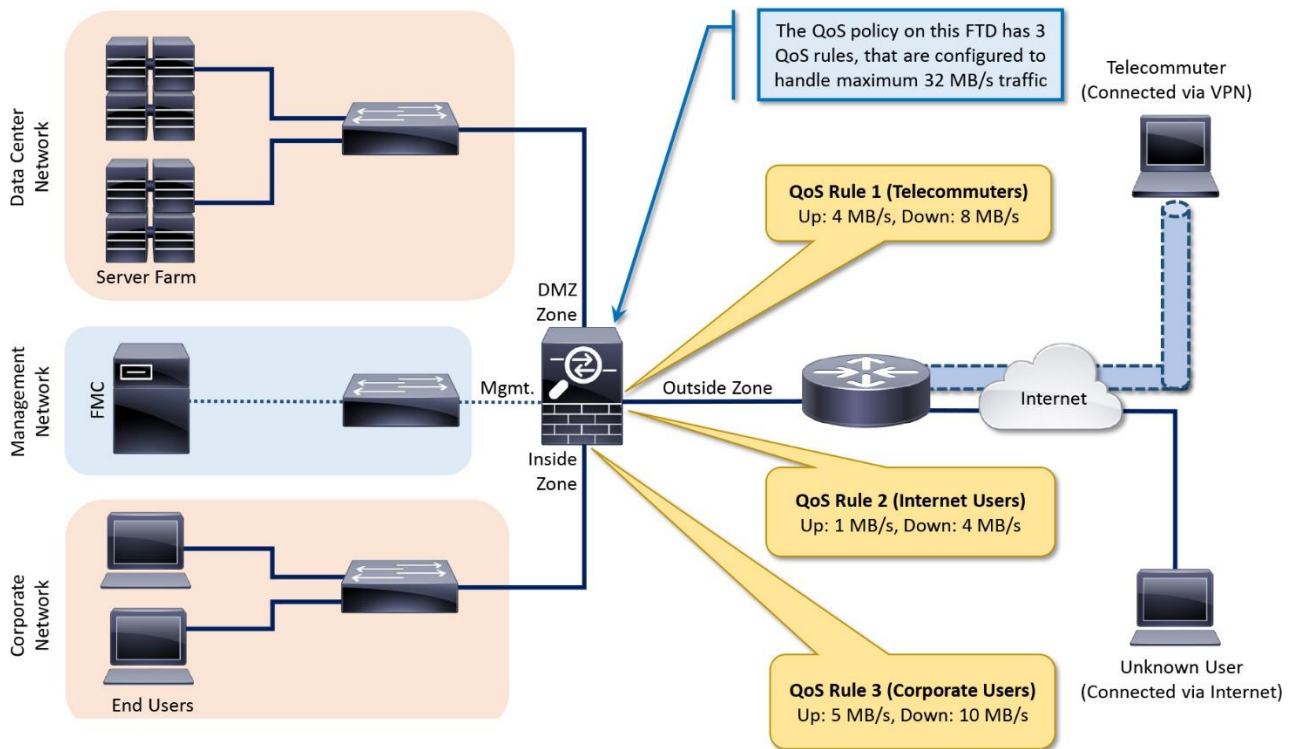


Figure 15-4. Deployment of Different QoS Rules on Different Network Segments

Prerequisites

Each interface, participating in a QoS policy, must be in routed mode and associated with an interface object. You cannot apply a QoS policy to an interface that is in inline, passive or switched mode. Read the [Chapter 8](#) to learn about the routed mode.

Figure 15-5 exhibits the configurations of FTD interface — both of the participating interfaces are in routed mode (assigned with IP addresses), and associated with security zones (interface objects).

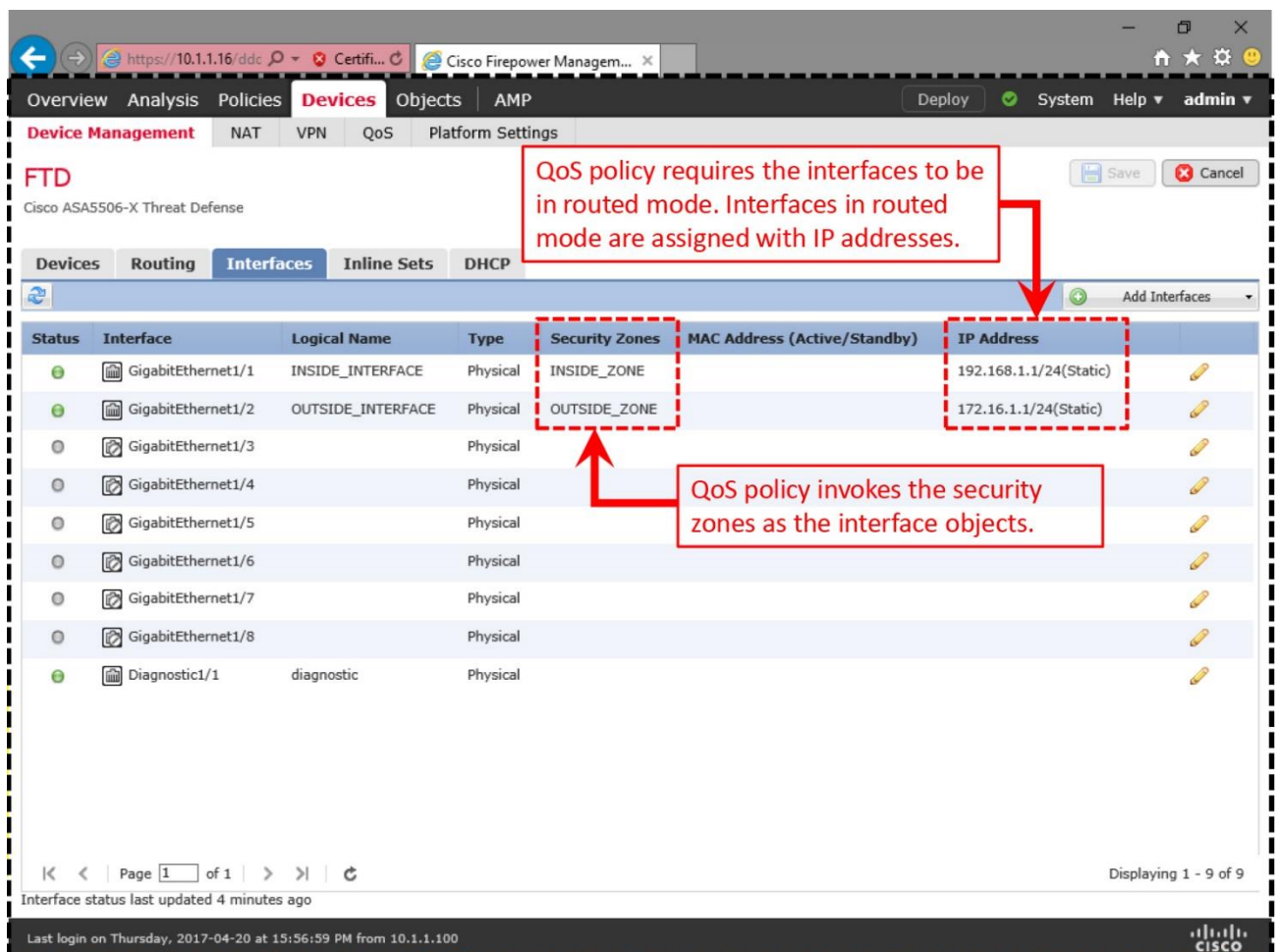


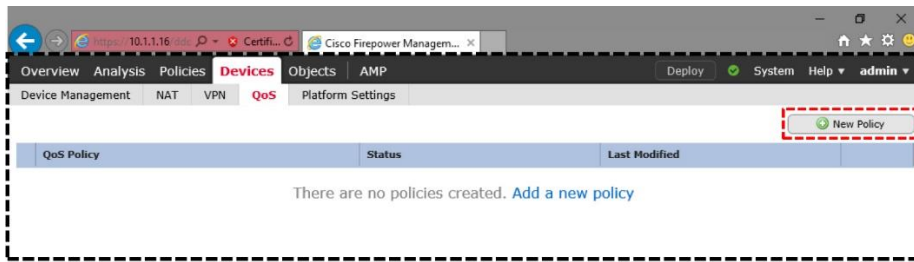
Figure 15-5. Supported Interface Settings for a QoS Policy

Configuration

Follow the steps below to create a QoS policy and add a rule within:

Step 1. Navigate to the **Devices > QoS** page. FTD does not provide a default policy. Click the **New Policy** button to create one. The **New Policy** window appears.

[Figure 15-6](#) shows the **New Policy** button on the QoS policy page. By default, there are no policies available.




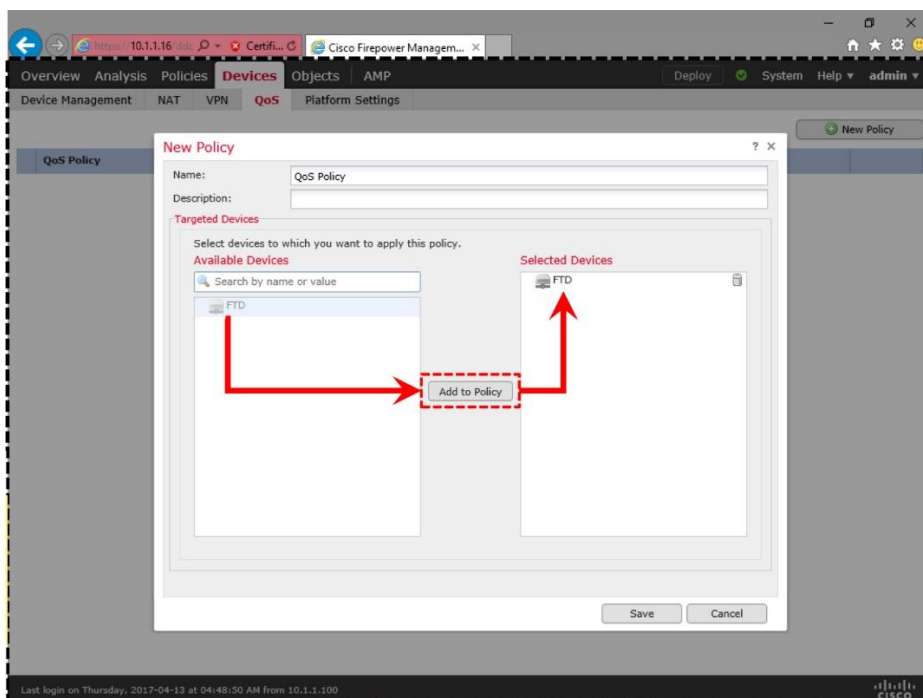
Last login on Thursday, 2017-04-13 at 04:48:50 AM from 10.1.1.100 

Figure 15-6. Homepage for the QoS Policy

Step 2. Give a name to the new policy, and add a target device to which you want to apply this policy. Save the changes. The QoS policy editor page appears.

[Figure 15-7](#) shows the selection of a device for the new the QoS policy you are about to create.




Last login on Thursday, 2017-04-13 at 04:48:50 AM from 10.1.1.100 

Figure 15-7. Assignment of a QoS Policy to an FTD

Step 2. Click the **Add Rule** button. The **Add Rule** window appears that allows you to define a rule condition.

[Figure 15-8](#) indicates the **Add Rule** button on a QoS policy editor page. The page also provides a link to the **Policy Assignments** option that you can use to associate a new managed device with this policy.

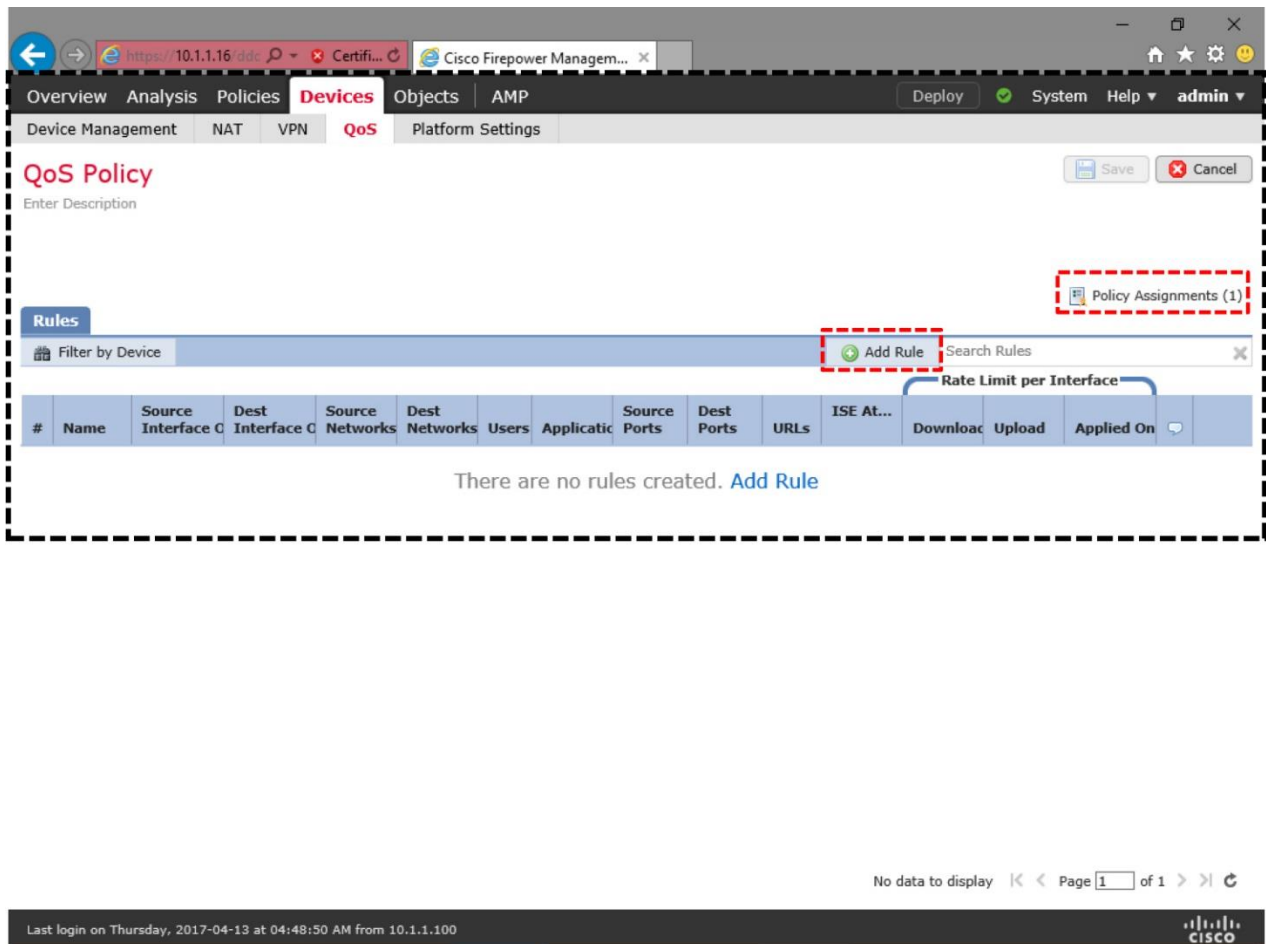


Figure 15-8. The QoS Policy Editor Page

Step 3. Give a name to the new QoS rule. Using the dropdown, select an interface where you want to apply the rule.

Tip

You should rate-limit traffic as close to the source as possible. It ensures that the traffic rate does not go beyond an entitled limit throughout the network.

Figure 15-9 shows a new QoS rule that is applied on a source interface object. Note that you have to select interface objects for two purposes — to select a location where traffic is rate limited, and to add them as a condition for a QoS rule.

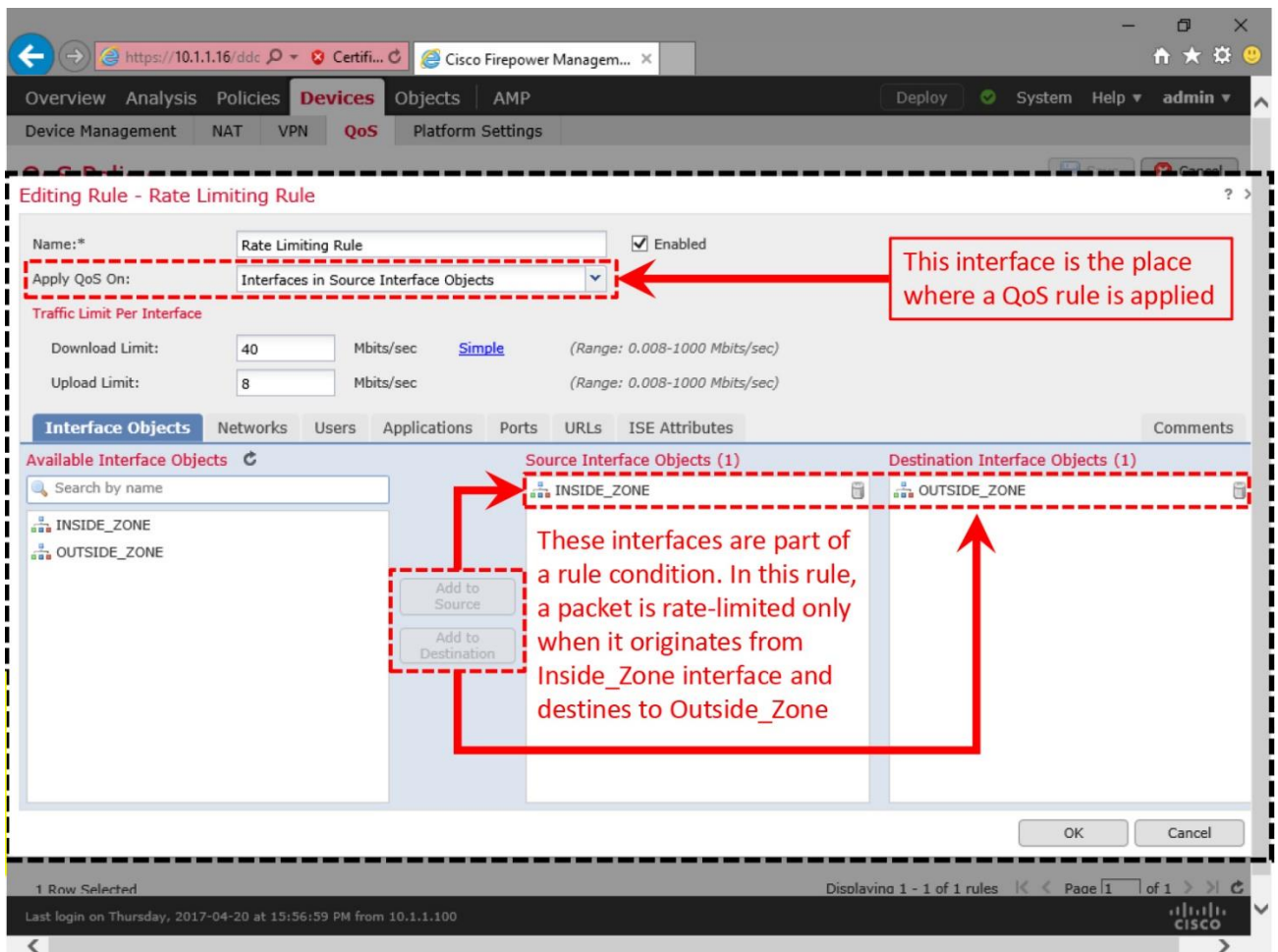


Figure 15-9. Selection of an Interface Object in a Rule

Step 4. Enter a desired traffic limit for the interface. FTD allows you to enter upload and download limits separately. If you do not enter a value, FTD supports the maximum throughput for that physical interface.

[Table 15-1](#) provides a conversation chart of commonly used traffic rates. When you enter a traffic limit, FTD considers the value as Megabit per second (Mbps), not Megabyte per second (MB/s). The highlighted rows are used in the configuration example of this chapter.

Megabit per Second	Megabyte per Second
1 Mbps	0.125 MB/s
4 Mbps	0.5 MB/s
8 Mbps	1 MB/s
10 Mbps	1.25 MB/s
16 Mbps	2 MB/s
40 Mbps	5 MB/s
80 Mbps	10 MB/s
100 Mbps	12.5 MB/s

Table 15-1. Megabit per Second to Megabyte per Second Conversion Table

Note

FTD supports the rate-limit of 0.008-1000 Mbits/sec per interface. If you want to allocate *below* 0.008 Mbits/sec to any hosts, it implies that those hosts are not important to you. You may just want to consider blocking them using an access rule or a prefilter rule.

[Figure 15-10](#) shows the traffic limits for download and upload flows, 40 Mbits/sec and 8 Mbits/sec, respectively.

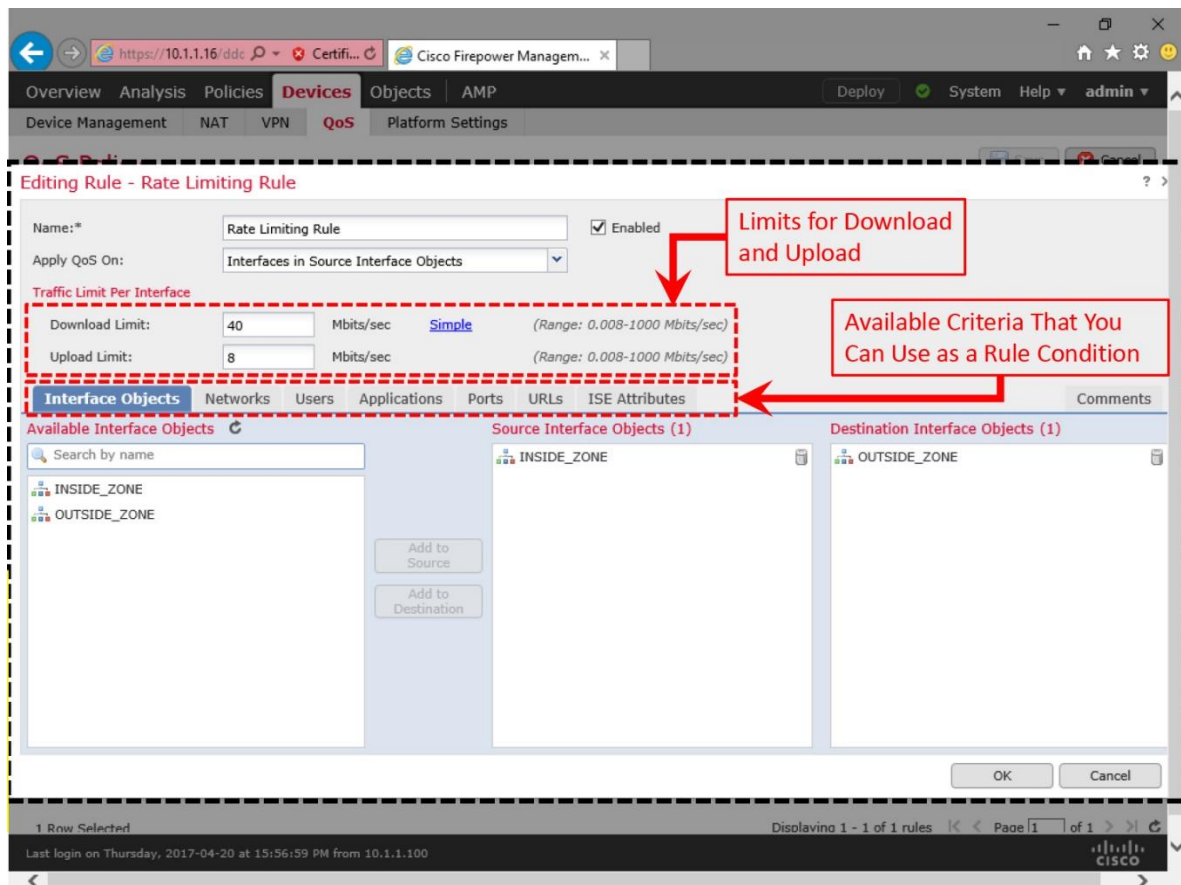


Figure 15-10. *Traffic Limit for a QoS Rule*

Step 5. Assigning interface objects with each QoS rule is a requirement. Optionally, you can add a precise rate-limiting condition based on any additional networking characteristics, such as, network address, port number, application, URL, user identity, etc.

Step 6. Once you outline a rule condition, click the **OK** button to create the QoS rule. The browser returns to the QoS policy editor page. Click the **Save** button to preserve the QoS rules you have created.

[Figure 15-11](#) shows the custom QoS rule you have just created.

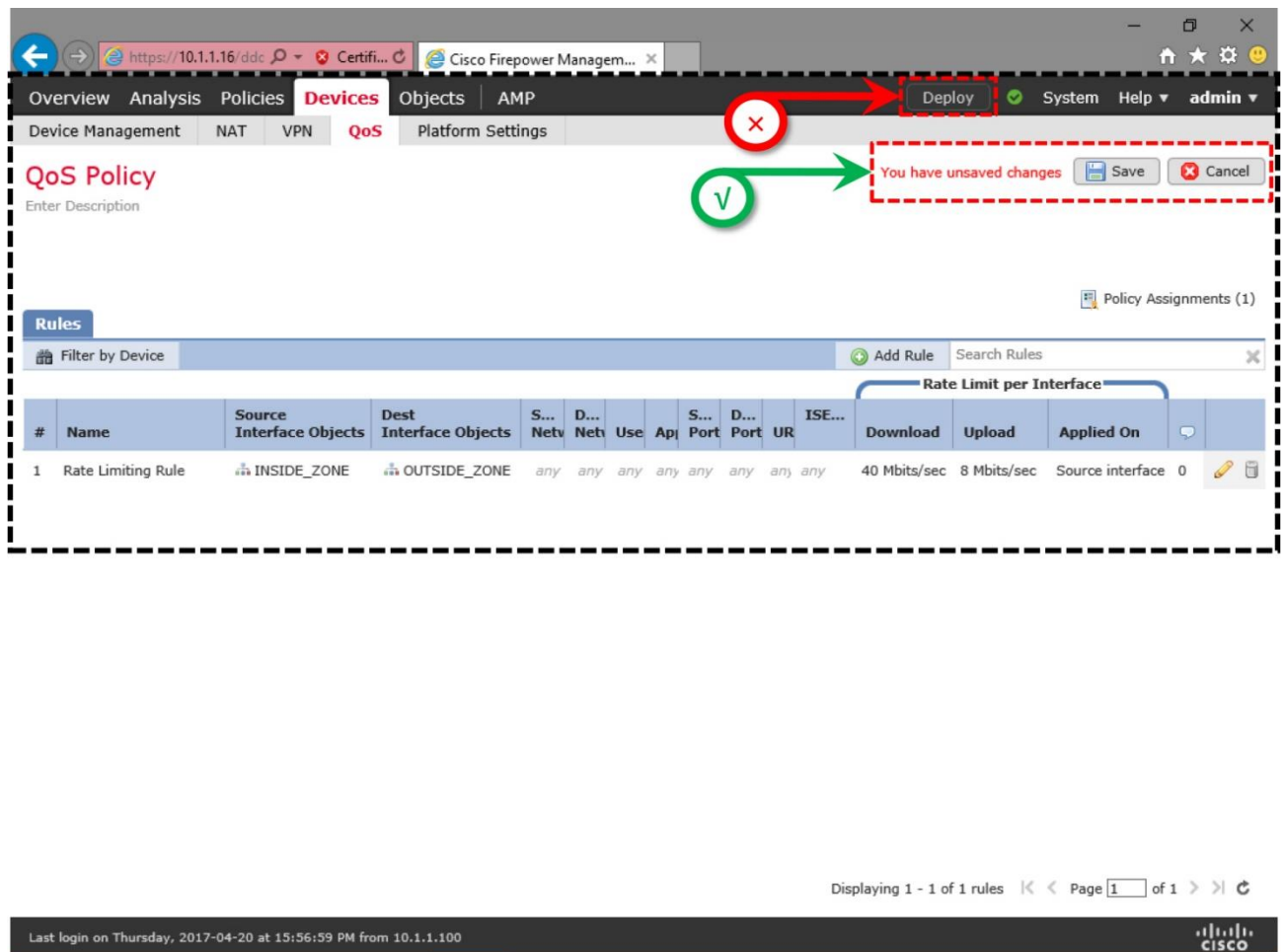


Figure 15-11. *Overview of All of the QoS Rules Appears in the QoS Policy Editor Page*

At this point, you may click the **Deploy** button to activate a QoS rule, however, by default, FTD does not generate a log when a QoS rule triggers. A QoS policy does not offer an option for logging. If you want to view any QoS related statistics for any specific connection, you must identify the associated access rule that triggers the QoS rule, and enable logging at the end of that connection. To accomplish that, you have to edit the Access Control policy and redeploy the revised policy.

Figure 15-12 shows the steps to enable logging. Since this exercise does not use any custom access rules, you can enable logging for the **Default Action**. It generates QoS data when a connection hits the default action.

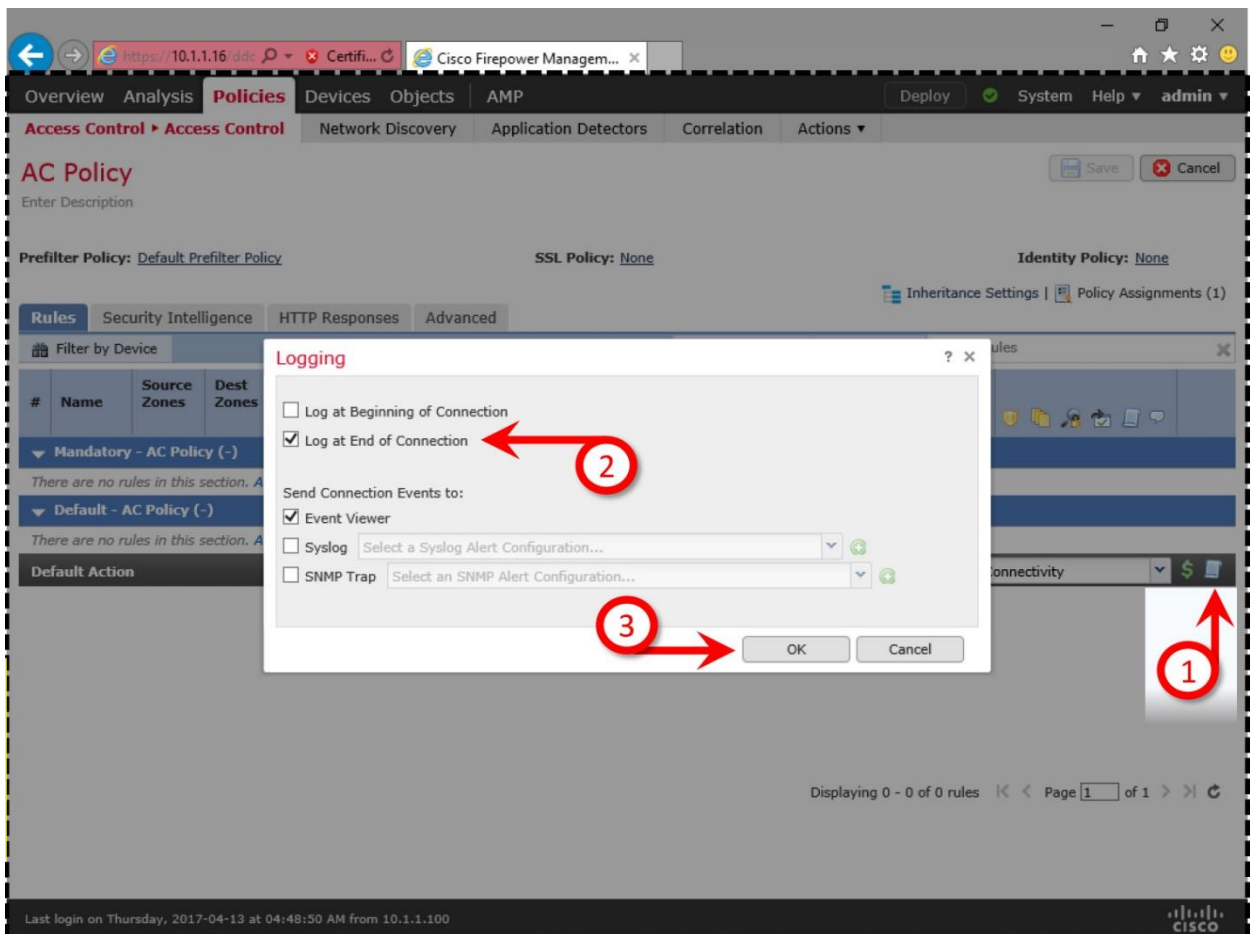


Figure 15-12. Enable Logging at the End of Connection in an Access Control Policy

Verification of Rate-Limit of a File Transfer

Once you successfully deploy a QoS policy, you can verify the deployment status from the CLI of your FTD.

[Example 15-1](#) confirms the QoS policy configurations and the interface where policy is deployed.

Example 15-1 *Policy Map Shows the Active QoS Policy on an Interface*

! To view the rate-limiting settings:

```
> show running-config policy-map
!  
policy-map type inspect dns preset_dns_map  
  parameters  
    message-length maximum client auto  
    message-length maximum 512  
    no tcp-inspection  
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP  
  parameters  
    eool action allow  
    nop action allow  
    router-alert action allow  
policy-map global_policy  
  class inspection_default  
    inspect dns preset_dns_map  
    inspect ftp  
    inspect h323 h225  
    inspect h323 ras  
    inspect rsh  
    inspect rtsp  
    inspect sqlnet  
    inspect skinny  
    inspect sunrpc  
    inspect xdmcp  
    inspect sip  
    inspect netbios  
    inspect tftp  
    inspect icmp  
    inspect icmp error  
    inspect dcerpc  
    inspect ip-options UM_STATIC_IP_OPTIONS_MAP  
  class class-default  
    set connection advanced-options UM_STATIC_TCP_MAP  
policy-map policy_map_INSIDE_INTERFACE  
  match flow-rule qos 268442624  
  police input 8000000 250000  
  police output 40000000 1250000  
!  
>
```

! To determine where a policy is applied:

```
> show running-config service-policy  
service-policy global_policy global  
service-policy policy_map_INSIDE_INTERFACE interface INSIDE_INTERFACE  
>
```

Now, let's verify the impact of the QoS policy you have deployed. First, download a file from the server to a client system. Then, upload a file from the client PC to the server. You should notice two different traffic rates.

[Figure 15-13](#) shows a topology of a simple deployment that you can use to verify the download and upload speed through an FTD.

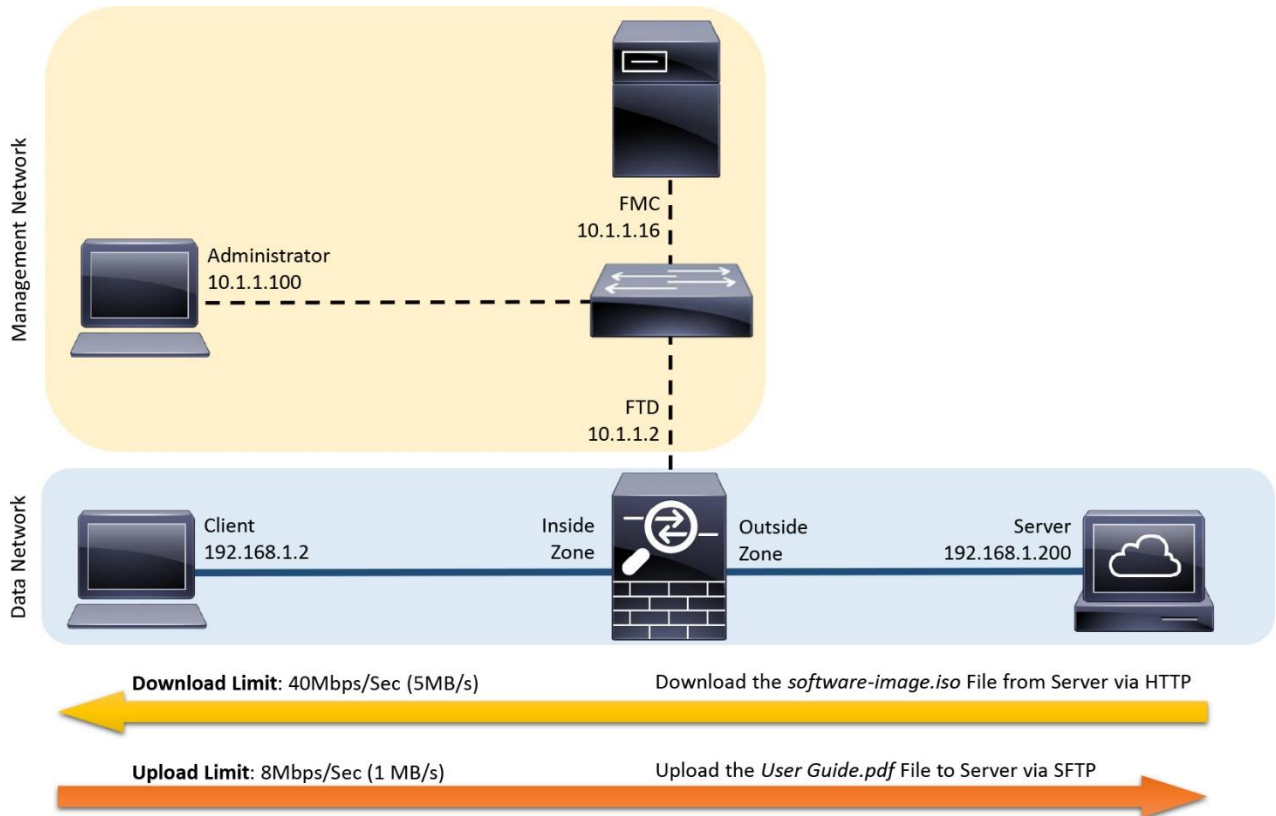


Figure 15-13. A Simple Lab Topology to Test Rate-Limiting of Traffic through an FTD

Figure 15-14 shows the download of a software image file. FTD enforces the download rate within 5 MB/Sec.

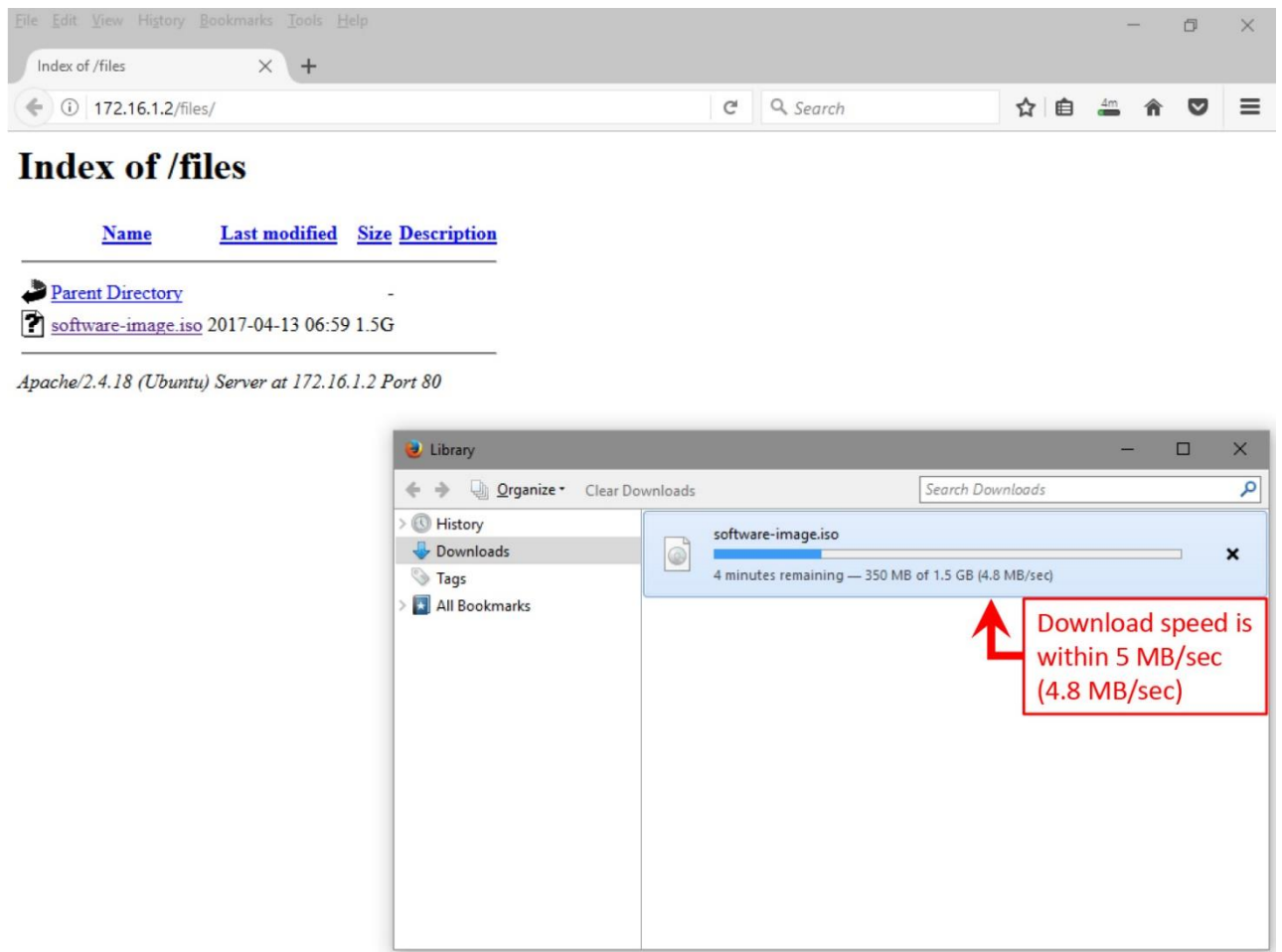


Figure 15-14. Compliance of the Download Rate with a QoS Policy

Figure 15-15 shows the upload of a PDF file. FTD regulates the upload rate below 1 MB/Sec.

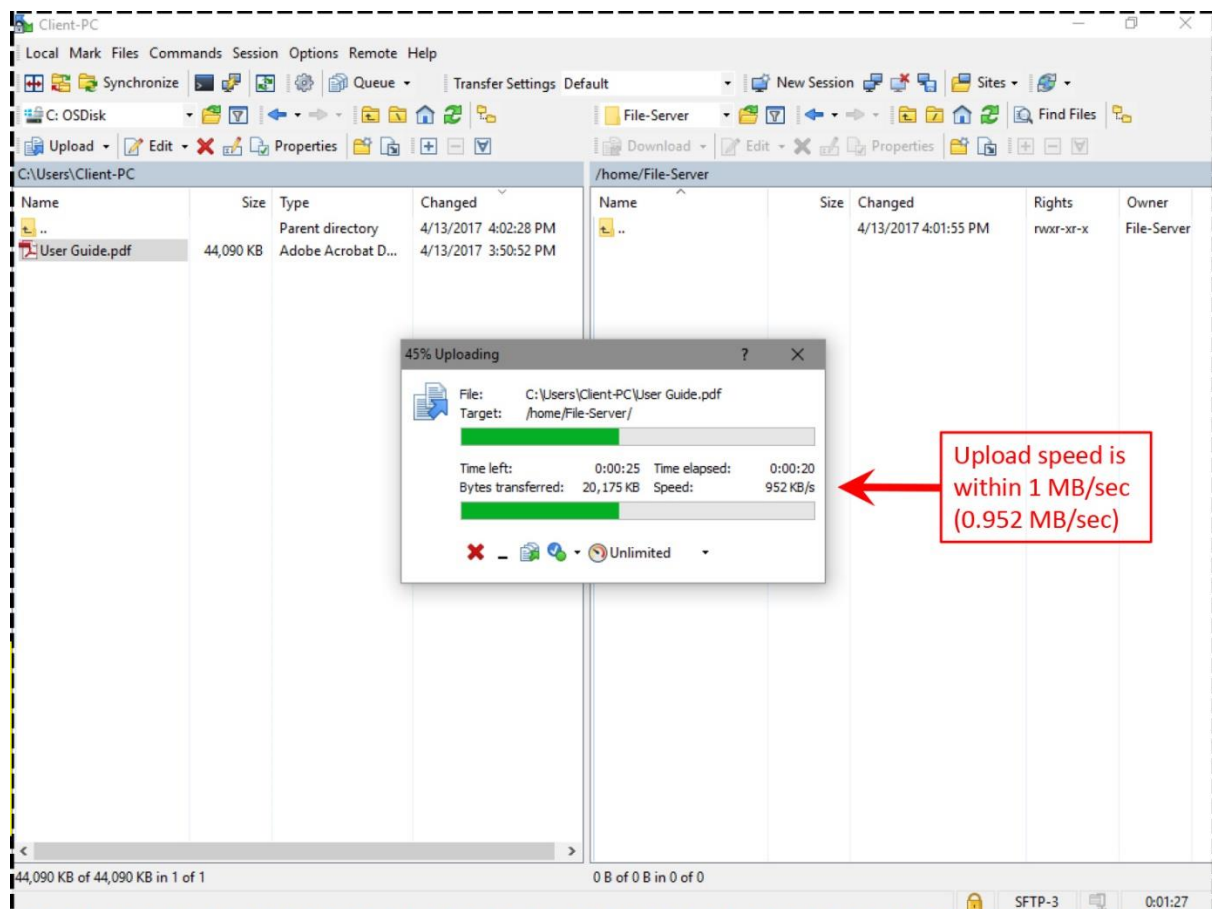


Figure 15-15. Compliance of the Upload Rate with a QoS Policy

Both of the above transfers — download of ISO and upload of PDF — are initiated by a host that is located at the inside zone. Therefore, the traffic matches the QoS rule “*Rate Limiting Rule*”; and FTD regulates the traffic rate. However, if the connection is initiated by an outside system, it does not match the QoS rule condition. Hence, the QoS policy does not limit the traffic rate — the source and destination should be able to utilize the full capacity of the FTD interface bandwidth.

Analysis of QoS Events and Statistics

If you have enabled logging for the connections that also match your QoS rule conditions, you will be able to view the QoS related statistics in the Connection Events page. Here are the steps to view them:

Step 1. Navigate to the Analysis > Connections > Events page.

Step 2. Select the Table View of Connection Events.

Step 3. Expand the **Search Constraints** arrow, on the left.

Step 4. Select the necessary QoS related data points.

Figure 15-16 shows two sets of connections events. The bottom two connections are originated by an inside client — they match the conditions in the “Rate Limiting Rule”, and rate is limited. However, the top two connections are not rate-limited, because they are initiated by an outside system.

Connection Events (switch workflow)
 Connections with Application Details > **Table View of Connection Events** 2017-04-13 12:23:53 - 2017-04-13 13:53:05

Search Constraints (Edit Search)

	First Packet	Last Packet	Action	Initiator IP	Responder IP	Application Protocol	Web Application	QoS Rule	Count
2	2017-04-13 13:49:16	2017-04-13 13:49:25	Allow	172.16.1.2	192.168.1.2	SSH			1
	2017-04-13 13:49:11	2017-04-13 13:49:14	Allow	172.16.1.2	192.168.1.2	ICMP			1
1	2017-04-13 13:13:09	2017-04-13 13:15:09	Allow	192.168.1.2	172.16.1.2	SSH	SFTP	Rate Limiting Rule	1
	2017-04-13 13:04:49	2017-04-13 13:11:46	Allow	192.168.1.2	172.16.1.2	HTTP	Web Browsing	Rate Limiting Rule	1

Page 1 of 1 | Displaying rows 1-4 of 4 rows

Last login on Thursday, 2017-04-13 at 12:43:01 PM from 10.1.1.100

Figure 15-16. Connection Events Show Associated QoS Rules

[Example 15-2](#) demonstrates the actions of a QoS policy on an FTD. This example provides two commands that you can use to determine any drop due to a rate-limiting rule during a file transfer.

Example 15-2 Statistics of Dropped Packets Due to a QoS Policy (Rule ID: 268442624)

```
! Record on the service policy statistics

> show service-policy police

Interface INSIDE_INTERFACE:
  Service-policy: policy_map INSIDE_INTERFACE
  Flow-rule QoS id: 268442624
  Input police Interface INSIDE_INTERFACE:
    cir 8000000 bps, bc 250000 bytes
    conformed 334152 packets, 21168506 bytes; actions: transmit
    exceeded 0 packets, 0 bytes; actions: drop
    conformed 473456 bps, exceed 0 bps
  Output police Interface INSIDE_INTERFACE:
    cir 40000000 bps, bc 1250000 bytes
    conformed 1129736 packets, 1618239735 bytes; actions: transmit
    exceeded 127629 packets, 182986654 bytes; actions: drop
    conformed 36194128 bps, exceed 4092744 bps

>
```

```
! Statistics of the Accelerated Security Path (ASP) counts
```

```
> show asp drop

Frame drop:
No route to host (no-route)                                79
TCP packet SEQ past window (tcp-seq-past-win)              1
Output QoS rate exceeded (rate-exceeded)                   127629
  Slowpath security checks failed (sp-security-failed)      4
  FP L2 rule drop (l2_acl)                                  18

Last clearing: 00:51:31 UTC Apr 10 2017 by enable_1

Flow drop:

Last clearing: 00:51:31 UTC Apr 10 2017 by enable_1
>
```

[Example 15-3](#) reveals the connections that are rate-limited by a QoS rule. The flags associated with a connection confirms if it is going through a Firepower deep packet inspection process.

Example 15-3 Identifying the Status of a Rate Limited Connection

```
! You can use a QoS Rule ID to view any associated active connections.

> show conn flow-rule qos 268442624
1 in use, 4 most used
```

```
TCP OUTSIDE_INTERFACE 172.16.1.2:80 INSIDE_INTERFACE 192.168.1.2:47072,
idle 0:00:00, bytes 1199375239, flags UIO N
>
```

```
! To determine the meaning of each flag, you can use the "detail" keyword.
For example, the flag 'N' confirms that the Firepower Snort engine inspects
the connection.
```

```
> show conn detail
```

```
1 in use, 4 most used
```

```
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to
SYN,
```

```
    b - TCP state-bypass or nailed,
```

```
    C - CTIQBE media, c - cluster centralized,
```

```
    D - DNS, d - dump, E - outside back connection, e - semi-distributed,
```

```
    F - initiator FIN, f - responder FIN,
```

```
    G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
```

```
    i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
```

```
    k - Skinny media, M - SMTP data, m - SIP media, N - inspected by
```

```
Snort, n - GUP
```

```
    O - responder data, P - inside back connection,
```

```
    q - SQL*Net data, R - initiator acknowledged FIN,
```

```
    R - UDP SUNRPC, r - responder acknowledged FIN,
```

```
    T - SIP, t - SIP transient, U - up,
```

```
    V - VPN orphan, v - M3UA W - WAAS,
```

```
    w - secondary domain backup,
```

```
    X - inspected by service module,
```

```
    x - per session, Y - director stub flow, y - backup stub flow,
```

```
    Z - Scansafe redirection, z - forwarding stub flow
```

```
TCP OUTSIDE_INTERFACE: 172.16.1.2/80 INSIDE_INTERFACE: 192.168.1.2/47072,
flags UIO N, qos-rule-id 268442624, idle 0s, uptime 4m42s, timeout 1h0m,
bytes 1529246551
```

```
>
```

[Example 15-4](#) exhibits the real time debug messages generated by the Firewall and Firepower Engines, due to the match of a QoS rule (ID: 268442624).

Example 15-4 *Debugging of the QoS Rule Related Events in Real Time*

```
! Debug messages in the ASA Firewall Engine:
```

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp
```

```
Please specify a client IP address:
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
192.168.1.2-47072 > 172.16.1.2-80 6 AS 1 I 0 New session
```

```
192.168.1.2-47072 > 172.16.1.2-80 6 AS 1 I 0 using HW or preset rule order
2, id
```

```

268434432 action Allow and prefilter rule 0
192.168.1.2-47072 > 172.16.1.2-80 6 AS 1 I 0 allow action
192.168.1.2-47072 > 172.16.1.2-80 6 AS 1 I 0 Starting with minimum 0, id 0
and SrcZone
first with zones 2 -> 1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 0,
payload 0,
client 0, misc 0, user 9999997, url , xff
192.168.1.2-47072 > 172.16.1.2-80 6 AS 1 I 0 match rule order 1, id
268442624 action
Rate Limit
192.168.1.2-47072 > 172.16.1.2-80 6 AS 1 I 0 QoS policy match status (match
found),
match action (Rate Limit), QoS rule id (268442624)
192.168.1.2-47072 > 172.16.1.2-80 6 AS 1 I 0 Got end of flow event from
hardware
with flags 40000001

^C
Caught interrupt signal
Exiting.

```

>

```
! Debug messages in the Firepower Snort Engine:
```

```

> debug snort event
>
Flow from 192.168.1.2/47072 to 172.16.1.2/80 matched qos_rule_id 268442624
flag Regular
flow
RL pkts = 0, RL Bytes = 0, Rv RL pkts = 153693, Rv RL Byt = 220395762,
Qos_on_Src 1

> undebug all
>

```

The statistics in the above examples were captured when a client PC was downloading a large ISO file from the server using a web browser. You could perform similar analysis on uploaded traffic. Before you begin uploading a file from the client PC to the server, you can run the following commands to reset the counters.

```

> clear service-policy interface INSIDE_INTERFACE
> clear asp drop

```

Summary

In this chapter, you have learned the steps to configure QoS policy on an FTD. It also provides an overview to the common rate-limiting mechanisms, and how an FTD implements QoS. At the end, this chapter provides the command line tools to verify the operation of QoS policy in an FTD.

Quiz

1. Which of the following statement is correct?

- a. Firepower engine not only evaluate, but also enforce a QoS rule.
- b. Snort rate-limits traffic as soon as it receives.
- c. ASA Firewall engine enforces the actual rate limit.
- d. All of the above.

2. Which step is necessary to view any QoS related events?

- a. In a QoS policy, enable logging at the beginning of a connection.
- b. In a QoS policy, enable logging at the end of a connection.
- c. In an Access Control policy, enable logging at the beginning of a connection.
- d. In an Access Control policy, enable logging at the end of a connection.

3. To limit the download rate to 50 MB/s, which value should you enter in a QoS rule?

- a. 5
- b. 50
- c. 400
- d. 500

4. Which of the following command confirms if traffic is rate-limited by an FTD?

- a. **show service-policy police**
- b. **show conn detail**
- c. **show asp drop**
- d. All of the above

Chapter 16. Blacklisting of Suspicious Addresses Using Security Intelligence

To compromise a network, an attacker uses various techniques, such as, spam, Command and Control (CNC) servers, phishing, malware, etc. The volume and source of new threats are increasing every day. As a security engineer, you may find it challenging to keep the access control list of a firewall up to date with all of the new suspicious addresses. To make this job easier, FTD offers a unique threat defense mechanism, called the Security Intelligence. This chapter describes the processes to configure the Security Intelligence technology, and verify its operations.

Essential Knowledge

Security Intelligence allows you to blacklist a suspicious address without any manual modification to the Access Control policy. It can block a packet before the packet goes through a deep packet inspection by the Firepower Snort engine. Therefore, it helps reducing the CPU utilization of an FTD, and hence, improves the performance.

[Figure 16-1](#) shows that any traffic that are not pre-filtered go through the Security Intelligence inspection.

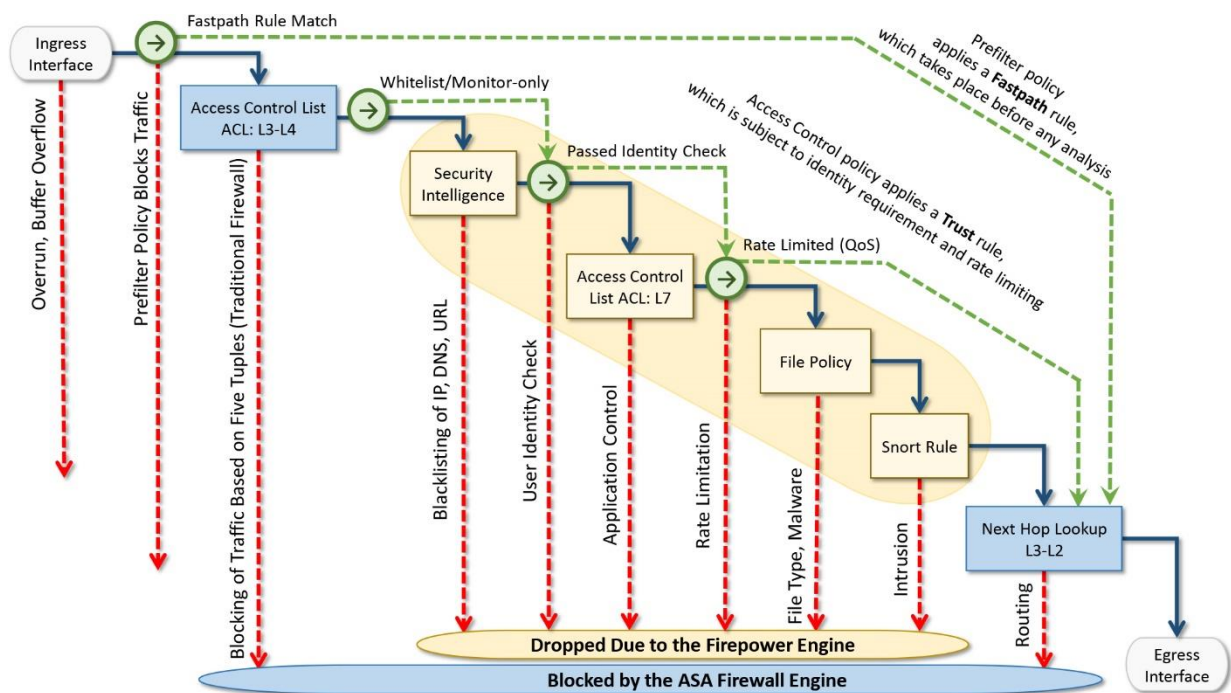


Figure 16-1. Drops of Packets by an FTD — a High Level Overview

There are several enhancements to the Security Intelligence technology since the Firepower System introduces this feature for the first time. Besides blacklisting of an IP address, which is one of the most common usages of the Security Intelligence, FTD also supports the blacklisting of URLs and domain names. To demonstrate the operations of the Security Intelligence, this chapter primarily focuses the blacklisting of IP addresses.

So far, you have been using the prior diagram to understand the flows and drops of packets through an FTD. Let's zoom in both Firewall and Firepower engines, view the low-level components of both engines, and determine the flows of packets through them.

[Figure 16-2](#) reveals the low-level architecture of an FTD. It shows that Security Intelligence is one of the earlier lines of defense within a Firepower engine.

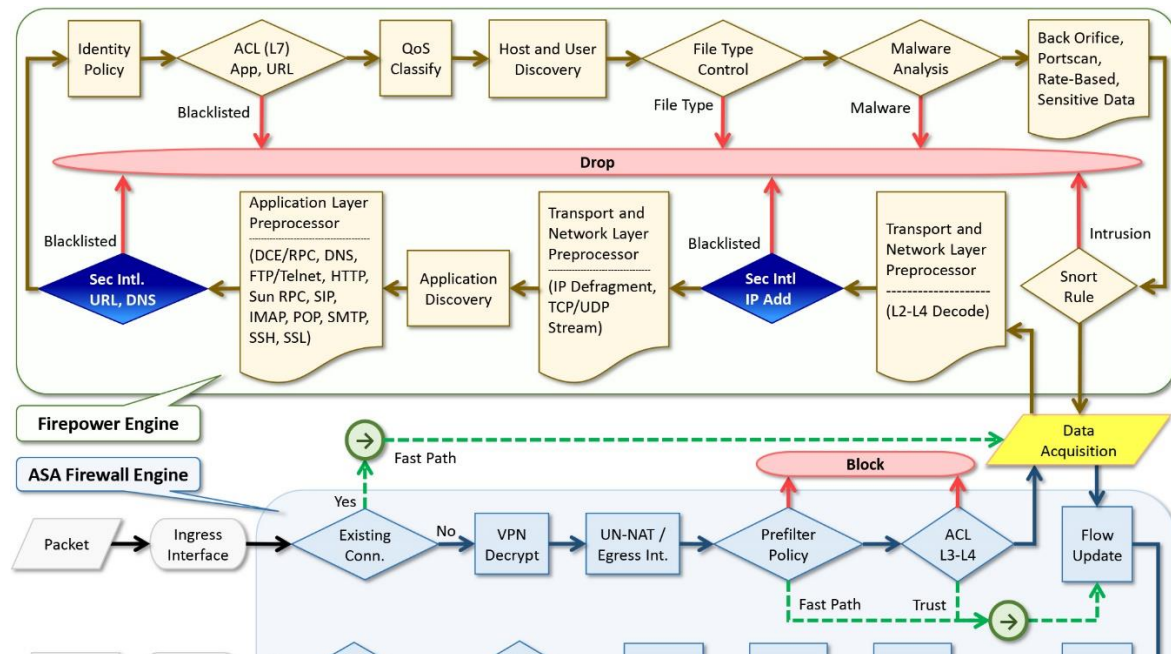


Figure 16-2. *Flows of Packets through the Firewall and Firepower Engines*

Input Methods

In order to input a potential suspicious address, the Security Intelligence supports the following three methods:

- **Feed:** Cisco has a dedicated threat intelligence and research team, known as Talos, who analyzes the behavior of the internet traffic, performs in-depth analysis on any suspicious activities, categorizes the potential addresses based on their characteristics, and list them into a file. This file is known as the Cisco Intelligence Feed. One of the processes running on an FMC, CloudAgent, periodically communicates with the Cisco Cloud to download the latest feed. Once an FMC downloads a feed, it sends the feed to its managed devices automatically. Redeployment of the Access Control policy is not necessary.
- **List:** FMC also allows you to input custom addresses for blacklisting. You can list the addresses in a text file (.txt format), and upload the file manually to an FMC through a web browser. The file requires you to enter one address per line.

[Table 16-1](#) shows the key differences between two types of Security Intelligence input — feed and list.

Table 16-1. *Security Intelligence Feed vs. Security Intelligence List*

	Feed	List
Provider	Created by the Cisco threat intelligence team	Created by you
Maintenance	Automatically update the existing list	Manually update an old list in on-demand basis
File Transfer	Update file is transferred via HTTPS or HTTP	Update file is uploaded via local browser

- **Blacklist Now:** You can blacklist a suspicious address instantly — without adding a new access rule for it. In case of an immediate need, you can avoid the process of scheduling a maintenance window for policy modification, and use the **Blacklist Now** for an instant block. Any addresses that you blacklist using the **Blacklist Now** option become part of the **Global Blacklist**.

[Figure 16-3](#) illustrates the key operational steps of the Security Intelligence feature on an FMC, FTD, and Cisco Cloud.

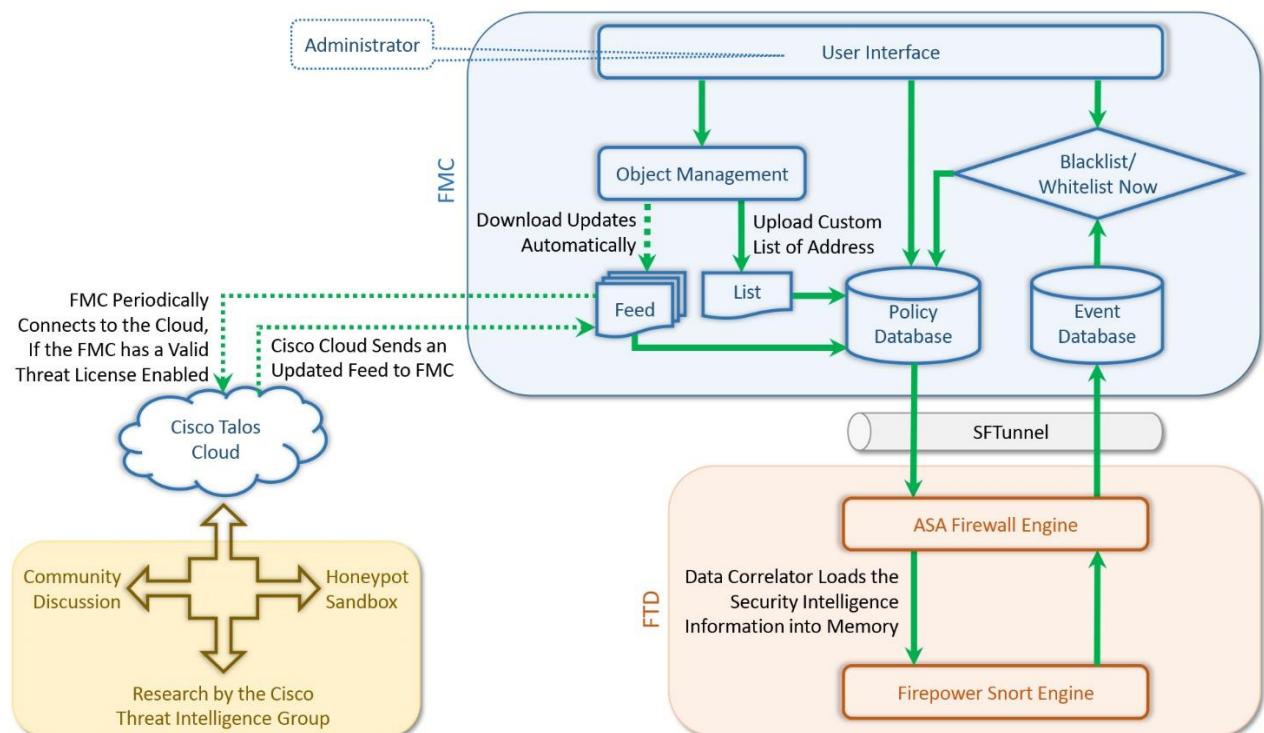


Figure 16-3. *Architecture of the Security Intelligence Technology*

Best Practices

Security Intelligence is an effective method to control suspicious traffic where traditional firewall is unable to recognize them. However, if your goal is to block or monitor traffic based on five tuples — source port, destination port, source IP, destination IP, and protocol — consider using the **Block** or **Monitor** action of an access rule. Do not use the Security

Intelligence as the primary method to monitor or block all traffic. It can affect the system performance.

Prerequisites

Security Intelligence feature requires a Threat license. If the license expires after you enable Security Intelligence feature, your FMC stops communicating with the cloud for latest intelligence feed. While you are in the process of purchasing a license, you can enable the Evaluation Mode to enable, configure and apply an Access Control policy with the Security Intelligence conditions. To learn more about the Evaluation Mode, read *the [Chapter 7 - Licensing and Registration through the SFTunnel](#)*.

Configuration

Security Intelligence is enabled through an Access Control policy. However, you do not need to add an additional access rule. There are three ways to blacklist an address, and you learn can learn all of them from this chapter.

- Automatic Blacklist using Cisco Intelligence Feed
- Manual Blacklist using Custom Intelligence List
- Immediate Blacklist using Connection Event

[Figure 16-4](#) shows a simple topology that is used in this chapter to demonstrate the configurations of Security Intelligence.

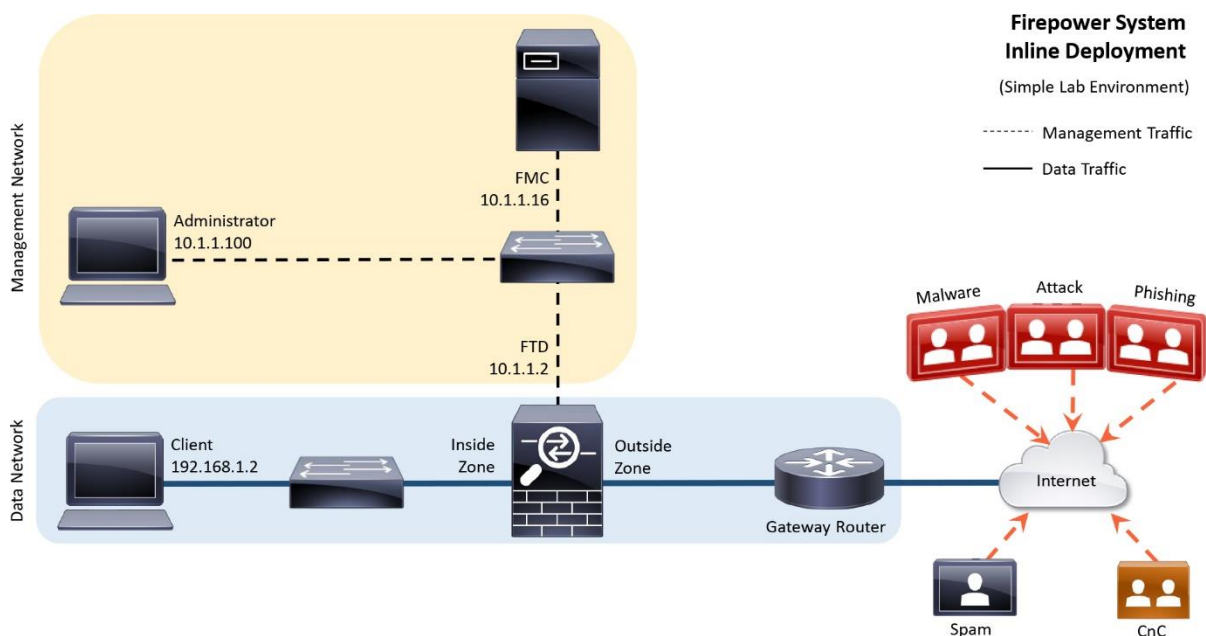


Figure 16-4. *Topology for the Security Intelligence Lab*

Automatic Blacklist using Cisco Intelligence Feed

To blacklist suspicious traffic using the Cisco Intelligence Feed, perform the following steps:

Step 1. Navigate to the Policies > Access Control > Access Control page.

Step 2. Select an Access Control policy that you want to deploy to an FTD. Click the *pencil* icon to edit.

Step 3. When the policy editor page appears, select the **Security Intelligence** tab. List of available objects and zones appear.

Note

If you are configuring a newly installed system, the list of intelligence objects may not be available for selection. To populate the Security Intelligence categories within the Available Objects field, you may need to update the Cisco Intelligence Feed from the cloud, at least once. Without populating them, you cannot use them as a rule condition.

[Figure 16-5](#) shows the page to update Security Intelligence feed and list. The list of intelligence categories may not be available for selection until you update the Cisco Intelligence Feed from the cloud.

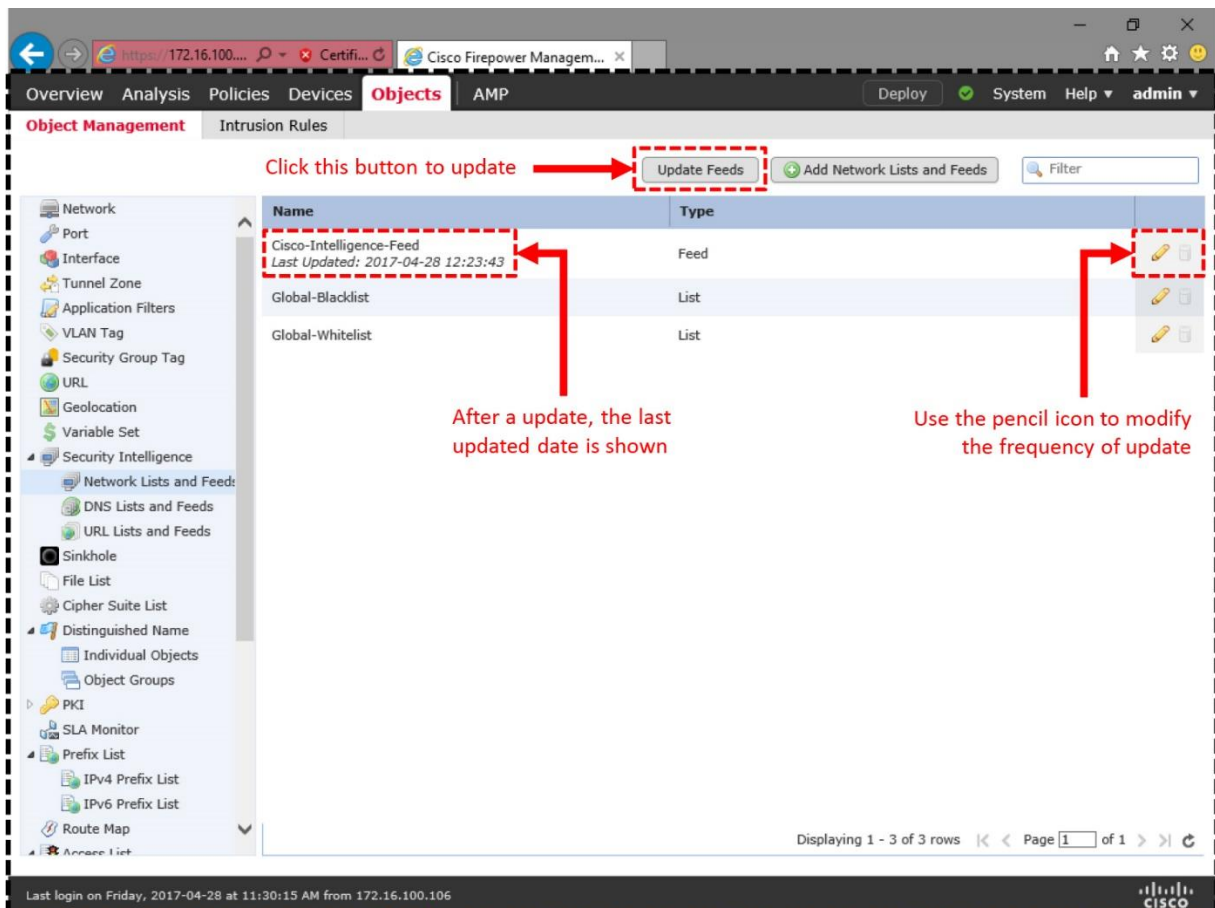


Figure 16-5. Update Page for the Security Intelligence Objects

Step 4. Under the **Network** subtab, select a category that you want to blacklist. You can also select a specific zone for inspection. By default, FTD inspects traffic from **Any** zone.

Note

This chapter enables Security Intelligence feature based on network and IP addresses. If you want to enable this feature based on URL conditions, select the URL subtab. The remaining configuration steps are identical.

Step 5. Once selected, click the **Add to Blacklist** button. The categories appear inside the **Blacklist** field.

[Figure 16-6](#) illustrates the detail steps to add the Security Intelligence categories for blacklist.

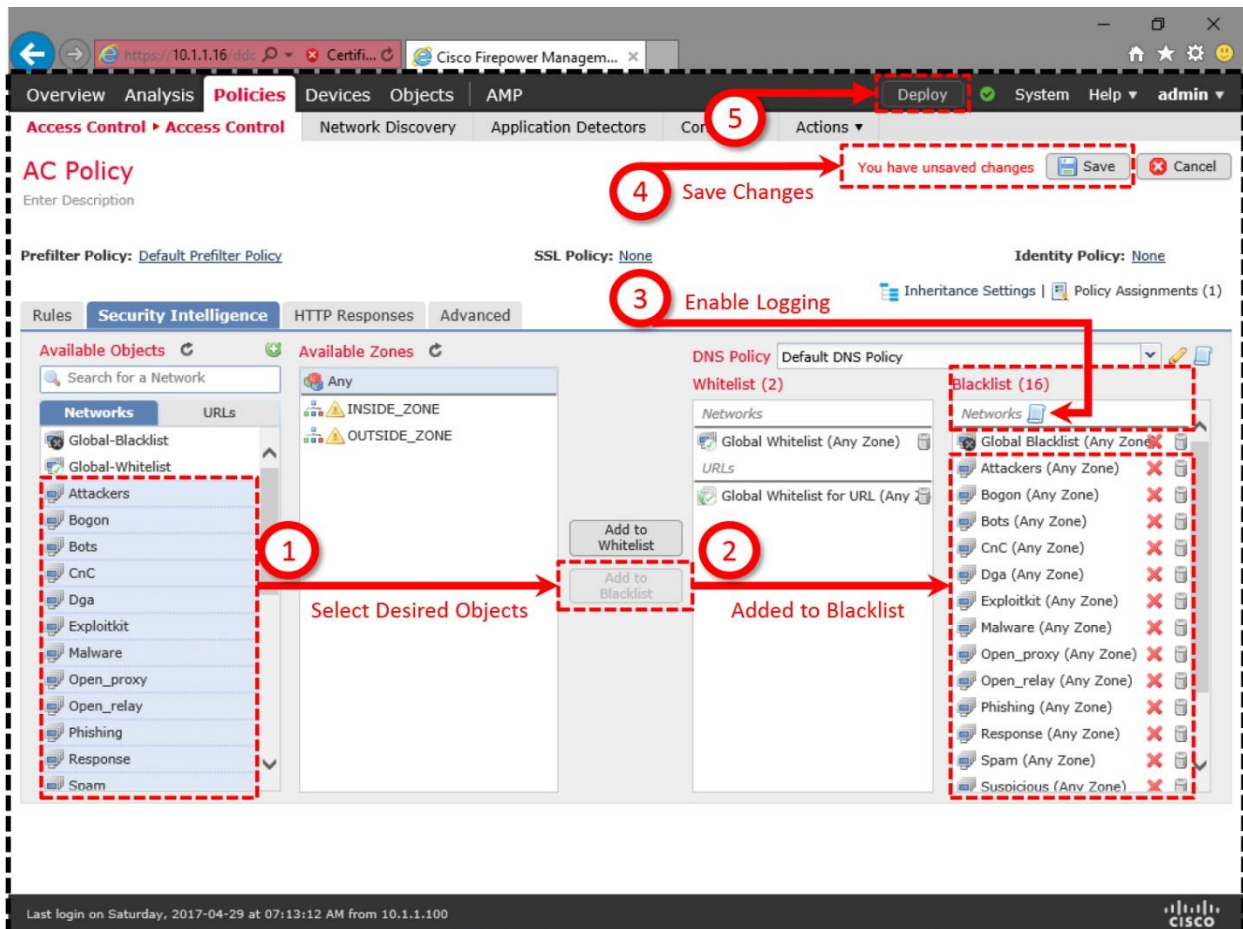


Figure 16-6. Workflow to Blacklist the Security Intelligence Categories

Step 6. The Blacklist field also has a logging icon, which you can click to verify if **Log Connections** is checked for Security Intelligence events. Click **OK** to return to the **Security Intelligence** tab.

Figure 16-7 shows the steps to verify logging for the connections that are subject to Security Intelligence blacklist.

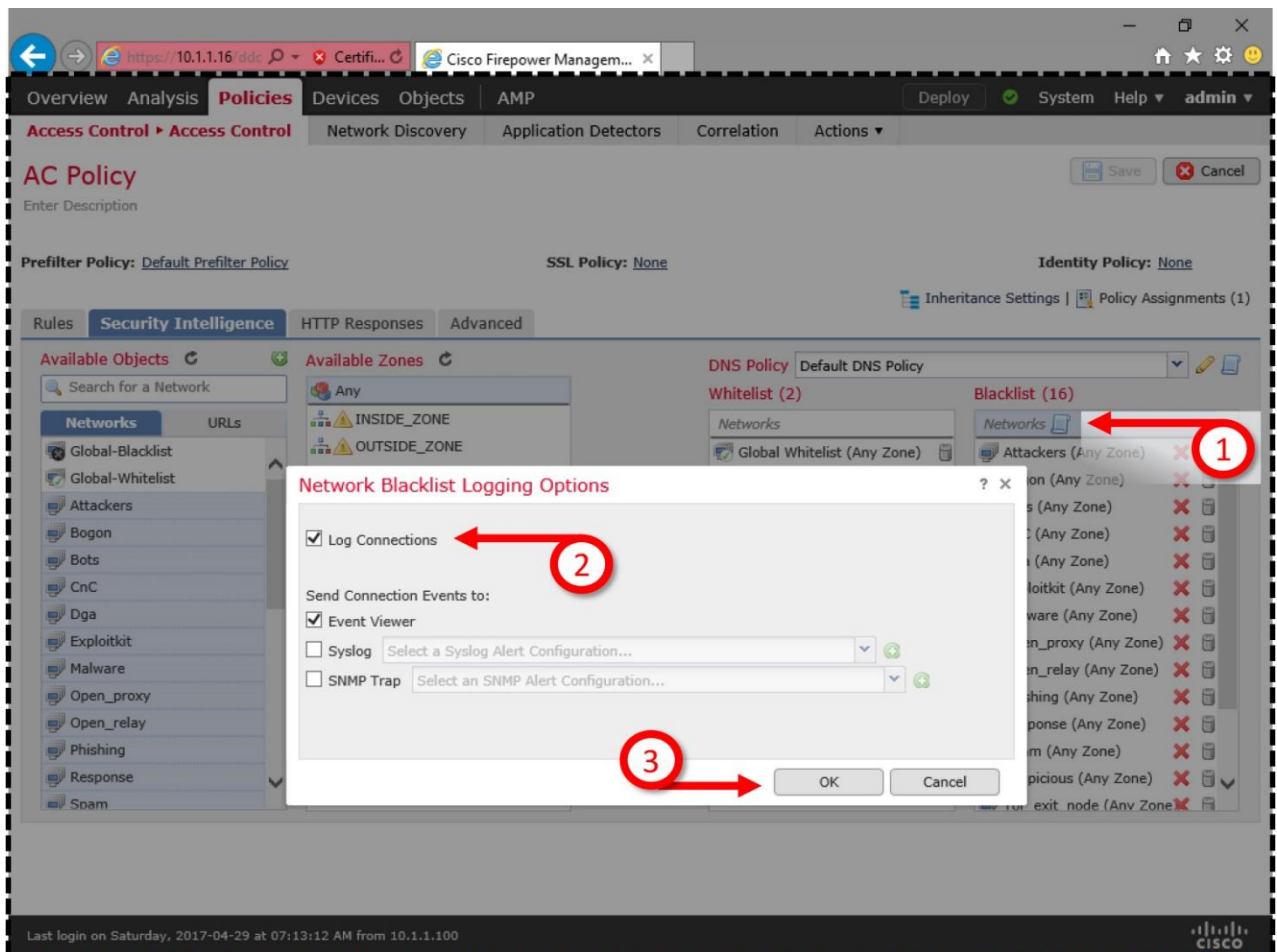


Figure 16-7. Logging for the Security Intelligence Events

Step 7. The configuration is complete. Save the changes and deploy the new Access Control policy to your FTD.

Now if you attempt to access a malicious IP address that is included in the Cisco Intelligence Feed, FTD should block the connection.

Tip

The Verification and Troubleshooting Tools section of this chapter discusses how to reverse engineer the Cisco Intelligence Feed data, and identify the addresses that are selected for blacklist.

Figure 16-8 demonstrates the action of the Security Intelligence. After it is enabled, the host is blocked from accessing certain addresses. These addresses, as of writing this book, are known for spreading malware and spam.

The screenshot shows the Cisco Firepower Management Center interface. The main content area is titled "Connection Events" and displays a table of connection events. The table has the following columns: First Packet, Last Packet, Action, Reason, Initiator IP, Responder IP, Responder Country, and Security Intelligence Category. There are four rows of data:

First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Responder Country	Security Intelligence Category
2017-04-29 14:45:57		Block	IP Block	192.168.1.2	104.97.6.228	USA	Malware
2017-04-29 14:44:05		Block	IP Block	192.168.1.2	180.124.44.98	CHN	Spam
2017-04-29 14:28:53	2017-04-29 14:28:55	Allow		192.168.1.2	104.97.6.228	USA	
2017-04-29 14:28:45	2017-04-29 14:28:49	Allow		192.168.1.2	180.124.44.98	CHN	

Annotation 1: "The connections are allowed before enabling the Security Intelligence" points to the two "Allow" rows.

Annotation 2: "The same connections are blocked after enabling the Security Intelligence" points to the two "Block" rows.

Figure 16-8. Connection Events Page Shows the Security Intelligence Events

Figure 16-9 shows an individual page that allows you to find any connections that are triggered only due to the Security Intelligence.

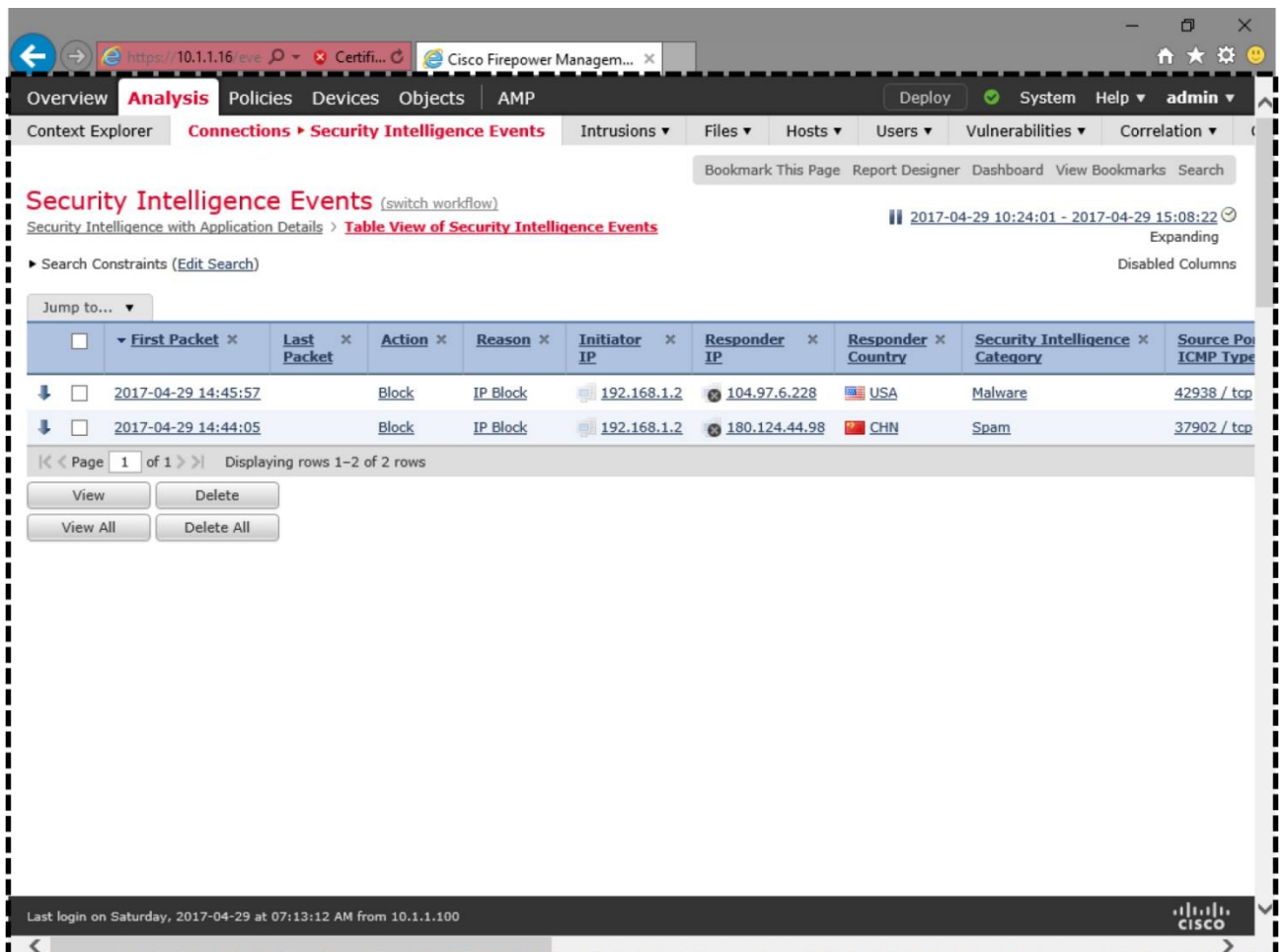


Figure 16-9. Security Intelligence Events Page Shows Only Its Own Events

Manual Blacklist using Custom Intelligence List

As a security engineer, you always track the latest threat and vulnerabilities to make sure your network is protected from the 0-day threat. Let's say, for instance, you have found a new security advisory in one of the security related websites. While Cisco is investigating the new information, you just want to blacklist them by your own.

Figure 16-10 shows a list of malicious addresses collected from the community-based security websites. You can find similar sites using a search engine; however, this book does not endorse any particular one.

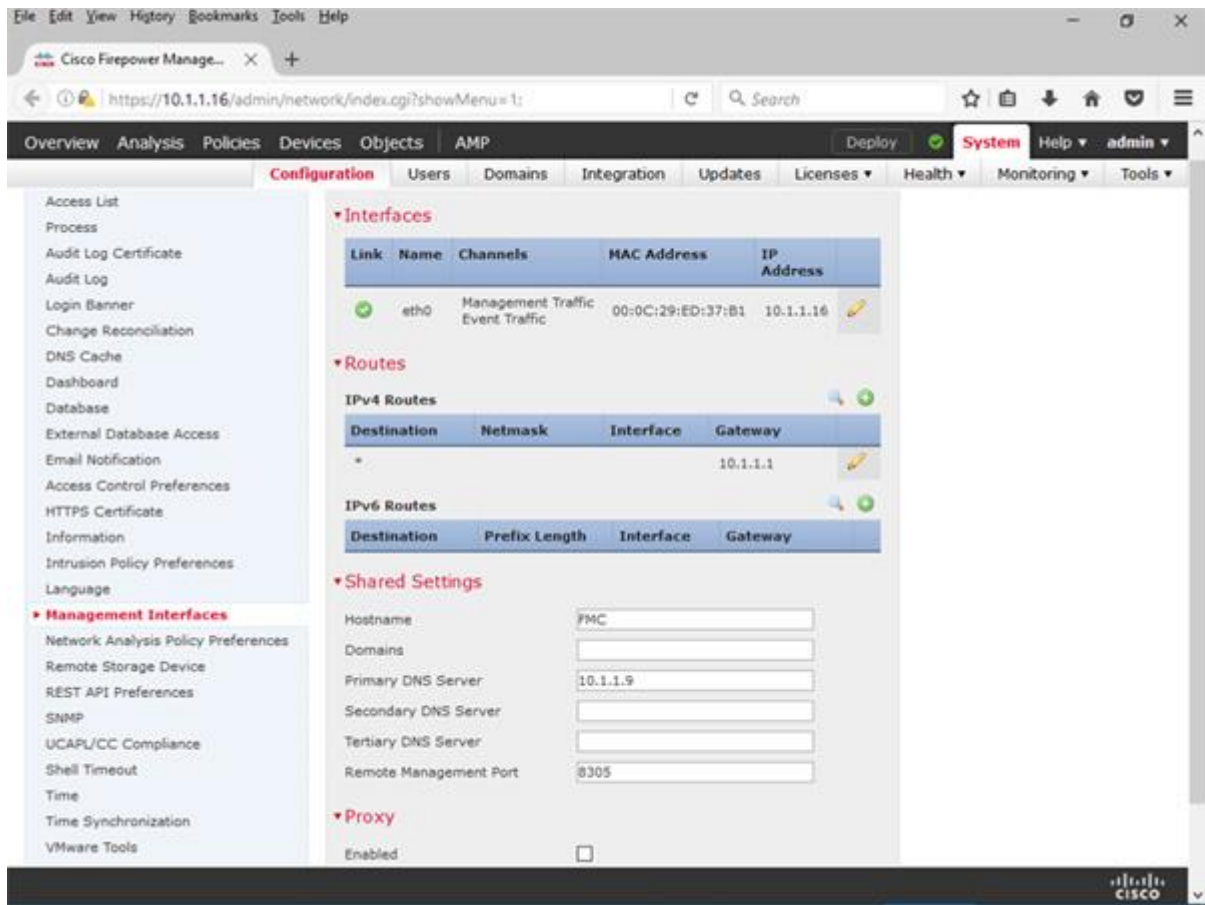


Figure 16-10. Example of Malicious Addresses from Community-Based Websites

To blacklist a custom list of IP addresses, follow the steps below:

Step 1. Write or copy the address into notepad. Enter one record per line. Save the file into .txt format.

Tip

When you create your own list of IP address for blacklist, you can add a comment on the IP address for future reference. Use the hash sign (#) at the beginning of a line to enter a comment.

Figure 16-11 shows a .txt file where a custom list of malicious IP addresses are copied.

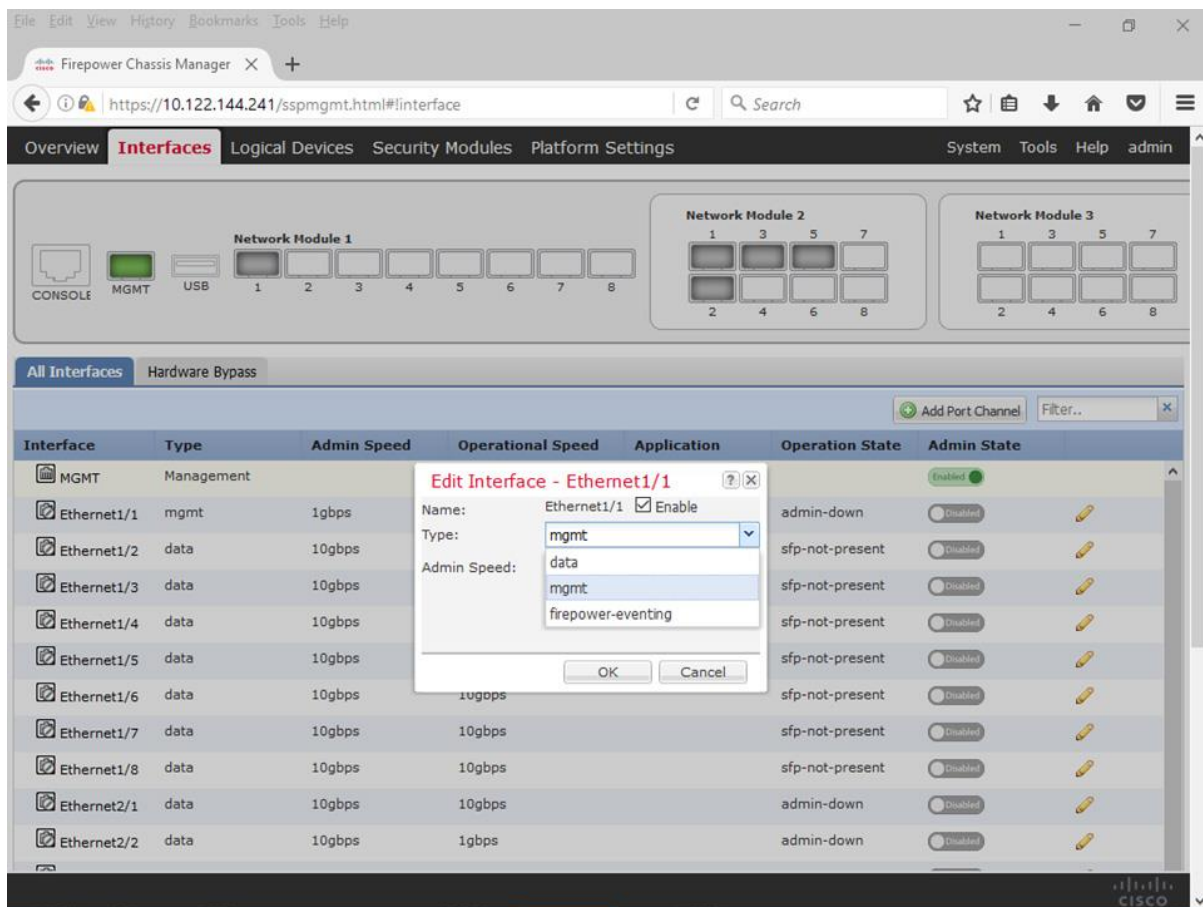


Figure 16-11. List of Malicious IP Addresses Copied from Community-Based Site

Step 2. On your FMC, navigate to the **Object > Object Management** page.

Step 3. On the left panel, select an appropriate option under the **Security Intelligence**. For example, if you want to add a custom list with IP address, select **Network Lists and Feeds** option. Then, click the **Add Network Lists and Feeds** button to upload your text file to the FMC.

[Figure 16-12](#) shows a configuration window for Security Intelligence List. After you select **List** from the **Type** drop-down, you will be able to browse your text file. Upon a successful upload, FMC can show the number addresses you uploaded.

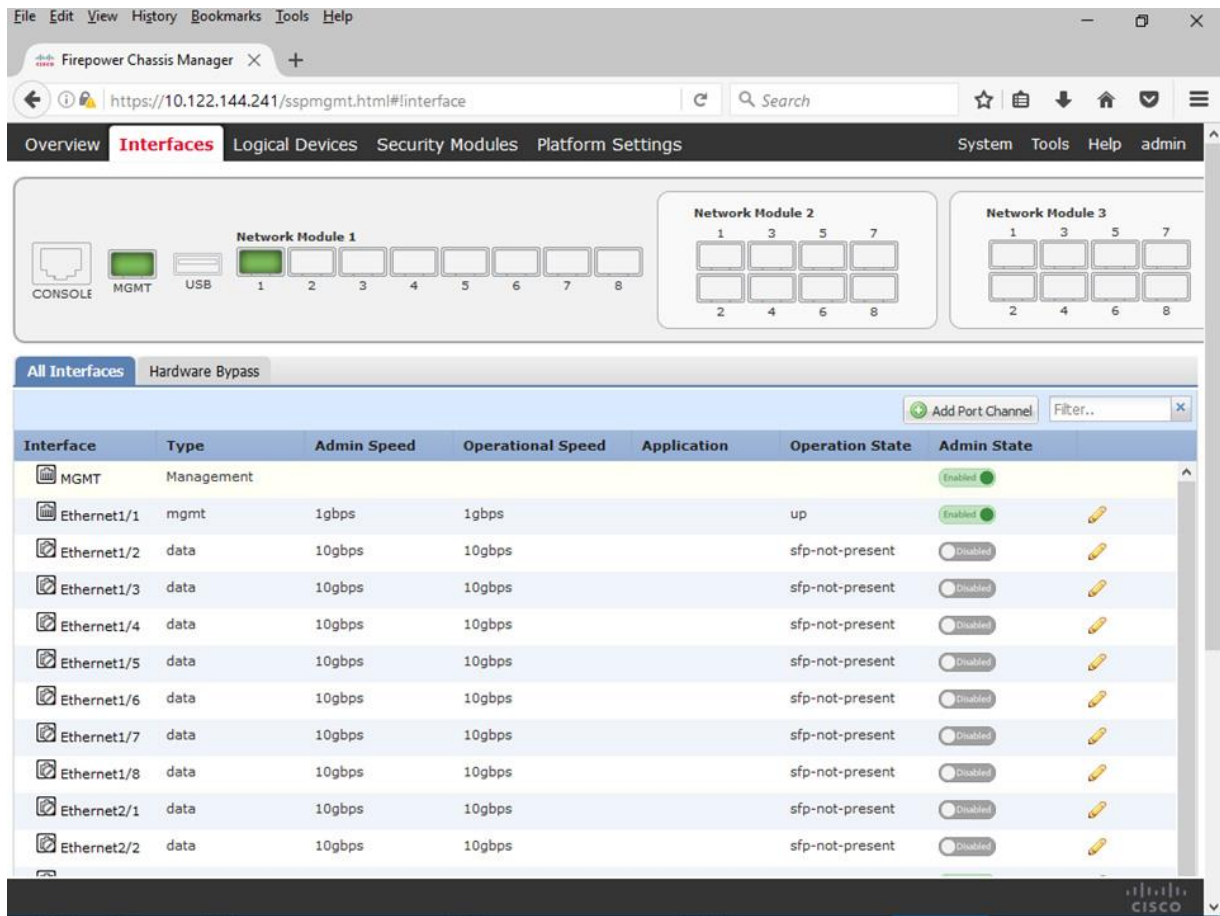


Figure 16-12. Upload of a Security Intelligence List File

Step 4. Once the file is uploaded, navigate to the **Policies > Access Control > Access Control** page, and edit the Access Control policy that you want to deploy to an FTD.

Step 5. When the policy editor page appears, select the **Security Intelligence** tab. List of available objects and zones appear.

Step 6. Under the **Network** subtab, select the custom object that you want to blacklist. You can also select a specific zone for inspection. By default, FTD inspects traffic from **Any** zone.

Note

This chapter enables Security Intelligence feature based on network and IP addresses. If you want to enable this feature based on URL conditions, select the URL subtab. The remaining configuration steps are identical.

Step 7. Once selected, click the **Add to Blacklist** button. The custom object appears inside the Blacklist field.

Figure 16-13 illustrates workflow of blacklisting a custom Security intelligence list.

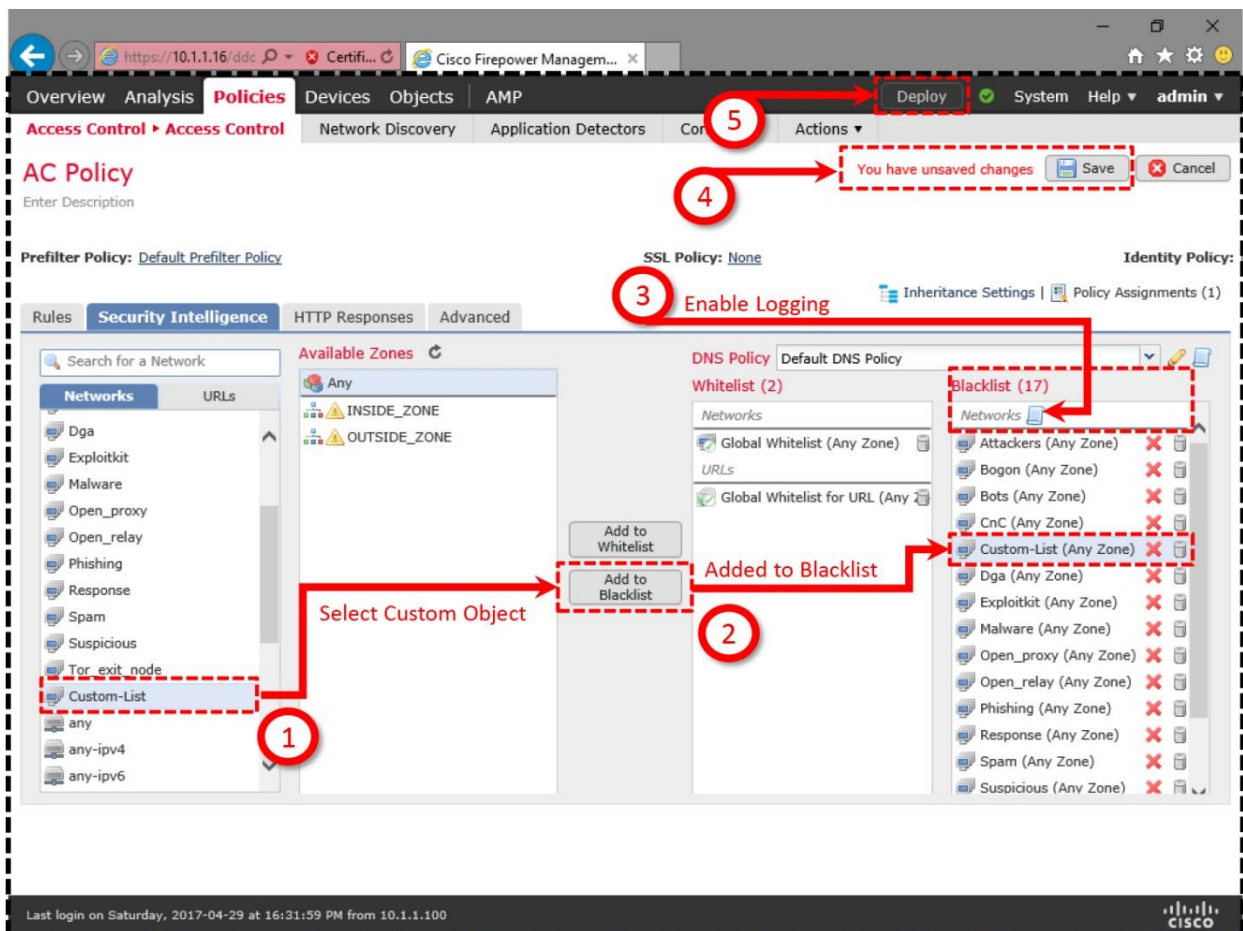


Figure 16-13. Addition of a Custom Intelligence Object for Blacklist

Step 8. Within the Blacklist field, click the logging icon to verify the settings — the **Log Connections** option should be checked. Click **OK** to return to the Security Intelligence tab.

Step 9. The configuration is complete. You can now save the changes and deploy the new Access Control policy to your FTD.

Now if you attempt to access one of the addresses that you included in the text file, FTD will block the connection.

Figure 16-14 shows the block of a connection due to a match with the Security Intelligence List.

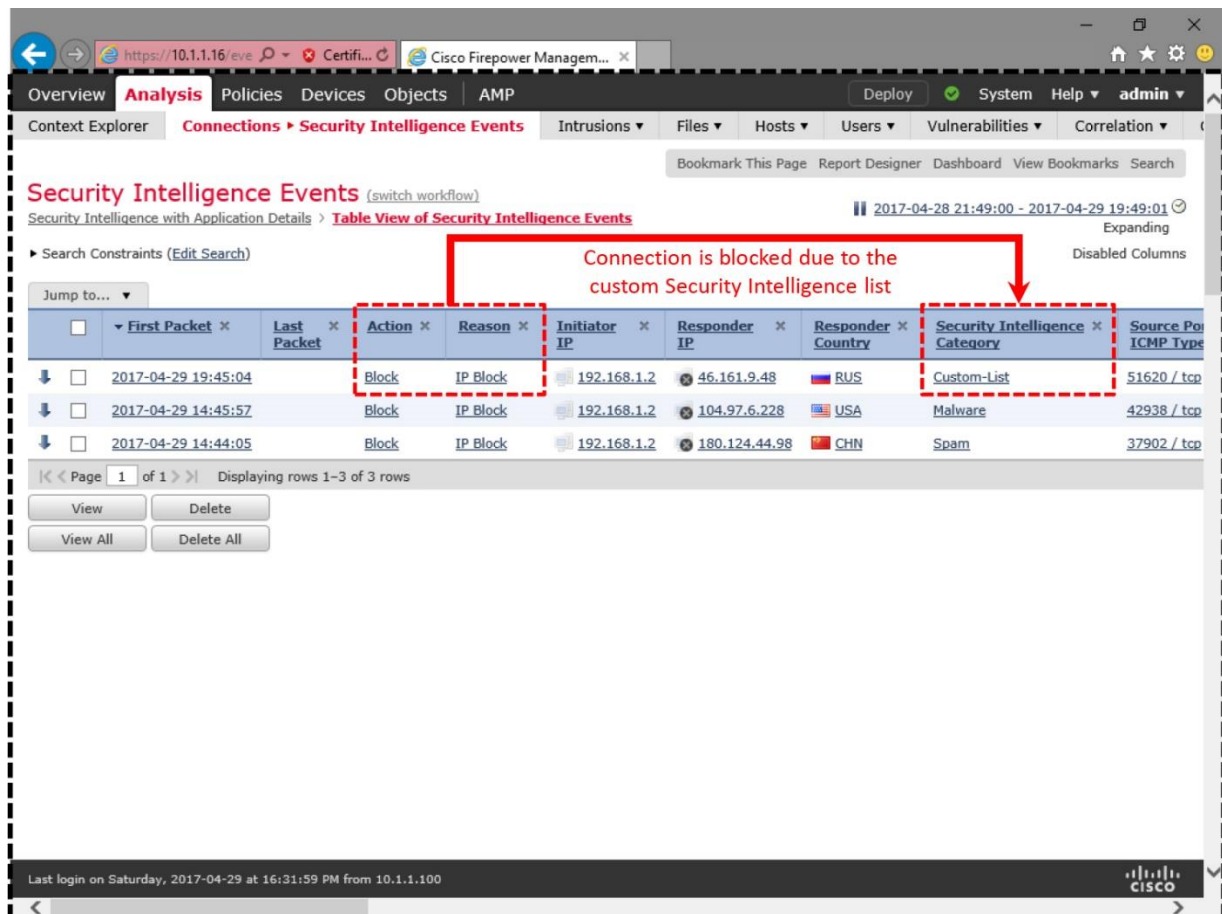


Figure 16-14. Security Intelligence Category Confirms the Matching List Name

Immediate Blacklist using Connection Event

Firepower system allows you to blacklist an address instantly — using the right-click button on your mouse. This feature is very useful when you notice a connection event for a suspicious address, but you cannot modify and reapply the Access Control policy without scheduling a maintenance window.

Adding an Address to Blacklist

Let's say, for example, you have noticed an event from an address that you cannot think of any reason for it. You believe this could be a potential for malicious activity. Here are the steps to blacklist the address immediately:

Step 1. Navigate to the Analysis > Connections > Events page.

Step 2. Right-click on the address you want to blacklist. For example, if you want blacklist an unknown suspicious address, right-click on the address under the **Responder IP** column. A context menu appears.

Figure 16-15 shows the steps to blacklist an IP address using the context menu. No additional configuration is necessary after these steps.

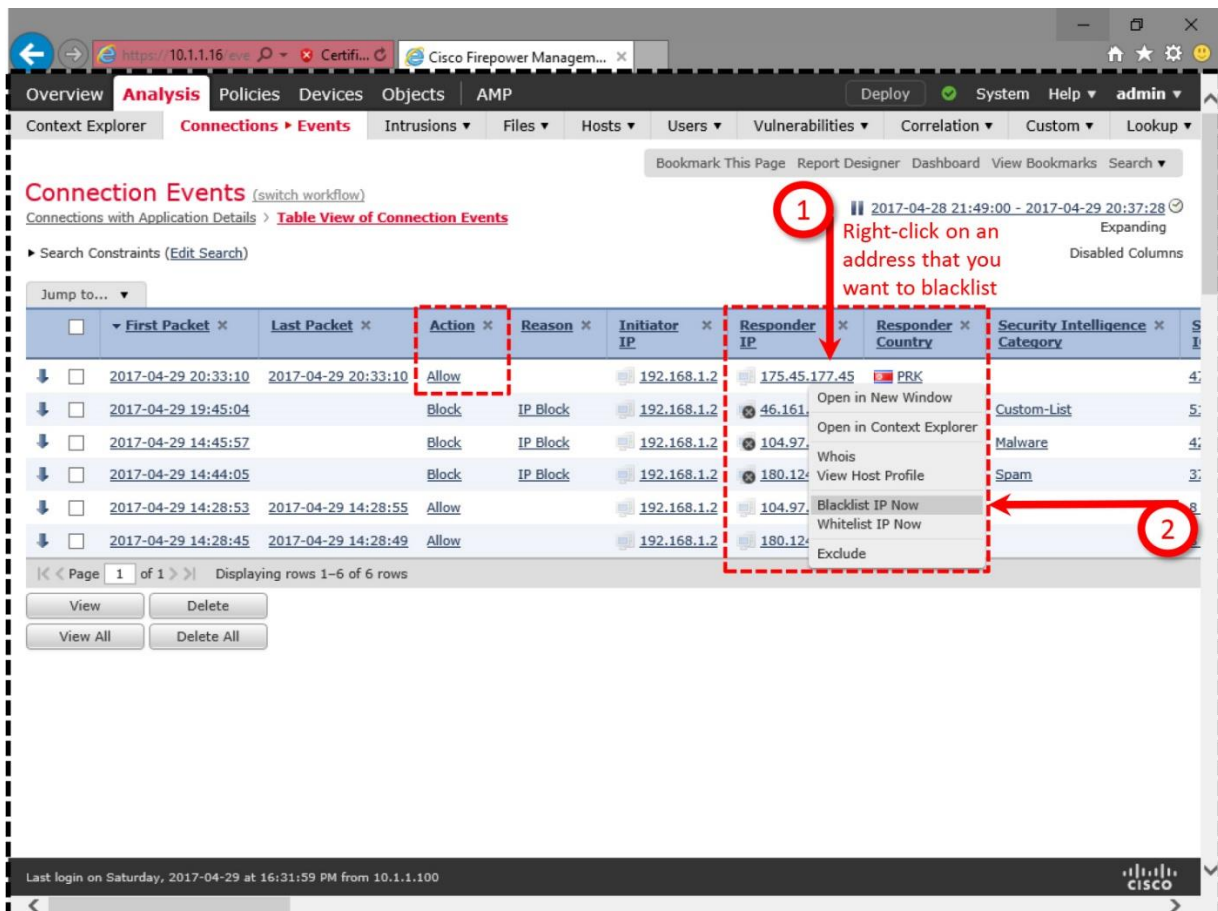


Figure 16-15. Context Menu Displays the Blacklist IP Now Option

Step 3. Select the **Blacklist IP Now** option. A confirmation window appears. Click the **Blacklist Now** button to confirm.

The configuration is complete. If you attempt to connect to the same IP address, FTD will block it this time.

Figure 16-16 shows the result of an immediate blacklist. Although the **Action** and **Reason** look identical, the Security Intelligence categorizes this event as a **Global-Blacklist** event.

The screenshot displays the Cisco Firepower Management Center (FMC) interface, specifically the **Connection Events** section. The table below shows a list of events with the following columns: **Action**, **Reason**, **Initiator IP**, **Responder IP**, **Responder Country**, and **Security Intelligence Category**. The second row is highlighted with a red dashed box, indicating a 'Block' action with the reason 'IP Block' and categorized as 'Global-Blacklist'. Red arrows point to the 'Block' action and the 'Global-Blacklist' category. Below the table, two red text annotations explain the second connection is blocked and the IP address is included in the Global-Blacklist category.

	First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Responder Country	Security Intelligence Category
4:	2017-04-29 20:43:29		Block	IP Block	192.168.1.2	175.45.177.45	PRK	Global-Blacklist
4:	2017-04-29 20:33:10	2017-04-29 20:33:10	Allow		192.168.1.2	175.45.177.45	PRK	
5:	2017-04-29 19:45:04		Block	IP Block	192.168.1.2	46.161.9.48	RUS	Custom-List
4:	2017-04-29 14:45:57		Block	IP Block	192.168.1.2	104.97.6.228	USA	Malware
3:	2017-04-29 14:44:05		Block	IP Block	192.168.1.2	180.124.44.98	CHN	Spam
8:	2017-04-29 14:28:53	2017-04-29 14:28:55	Allow		192.168.1.2	104.97.6.228	USA	
8:	2017-04-29 14:28:45	2017-04-29 14:28:49	Allow		192.168.1.2	180.124.44.98	CHN	

The second connection is blocked after selecting "Blacklist IP Now"

The blacklisted IP address is included in the Global-Blacklist category

Figure 16-16. FMC Displays a Block Event due to the Blacklist IP Now Action

Deleting an Address from Blacklist

Any addresses that you blacklist using the **Blacklist Now** option are included under the Global Blacklist category. If you want to remove the blacklisting attribute from an address, and allow the address again, go to the **Object Management** page, and edit the **Global-Blacklist** to remove the address.

Caution

If you delete the entire Global-Blacklist object using the Security Intelligence configuration page, the Access Control policy does not enforce the Blacklist Now function.

Figure 16-17 shows the IP address that you blacklisted earlier using the **Blacklist IP Now** option. To allow this IP address once again, use the delete icon, and save the changes.

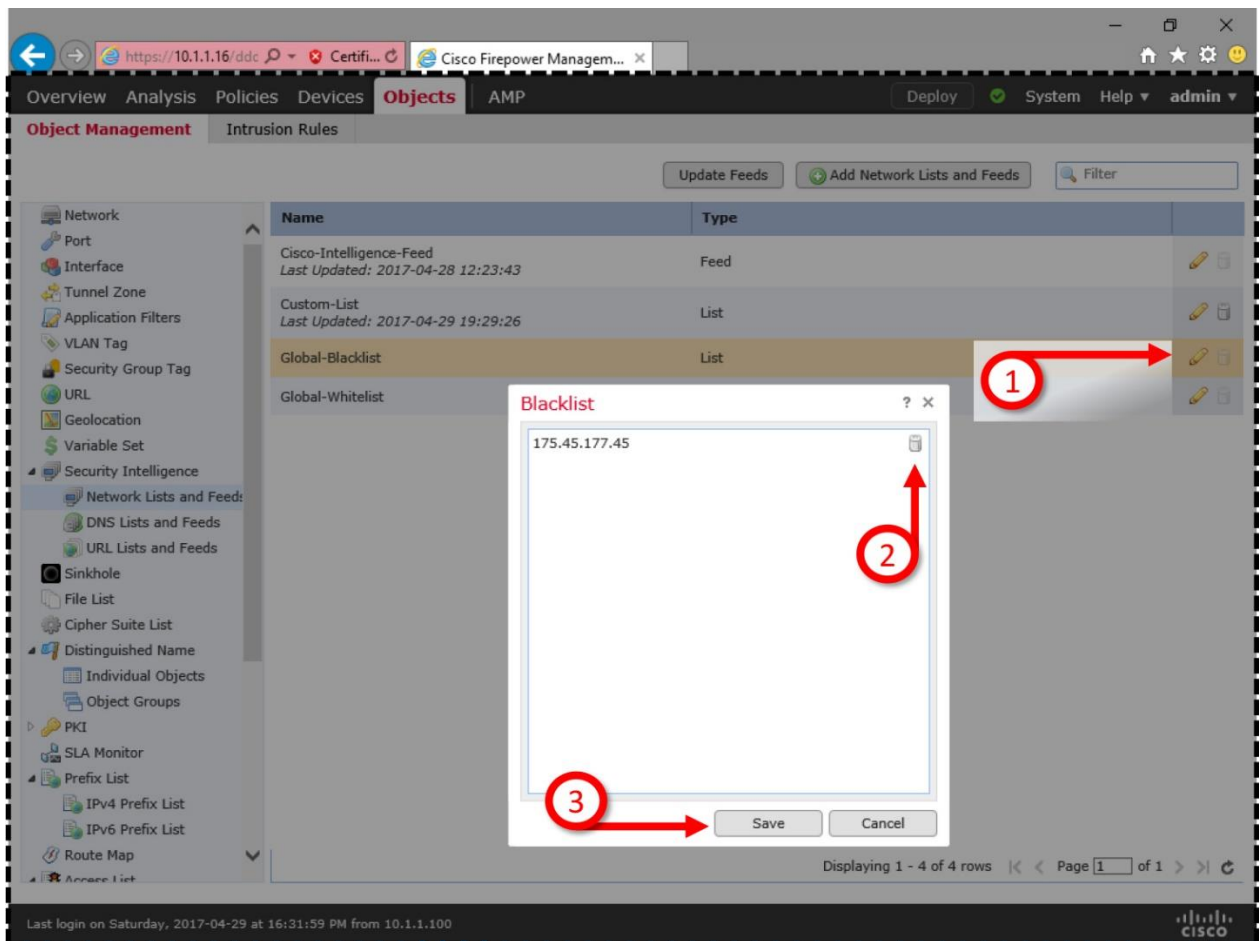


Figure 16-17. Steps to Remove Blacklisting of an Address

Monitoring a Blacklist

Occasionally, you want to monitor the activities of certain hosts in a network, instead of blocking them completely. It allows you to analyze the characteristics of suspicious traffic, and helps you to build an appropriate defense. Follow the steps below to enable monitoring functionality using the Security Intelligence:

Note

The following steps assumes that you have already blacklisted certain traffic using the instruction in the prior section. This time, you just want to change the action (monitor only, instead of block) for certain traffic.

Step 1. In the Access Control policy editor page, go to the **Security Intelligence** tab.

Step 2. Within the **Blacklist** field, select a category that you want to monitor.

Note

FTD does not support the Monitor-only mode for the Global Blacklist category.

Step 3. Once selected, click the right button. A context menu appears. Select **Monitor-only (do not block)** option. The icon changes from red 'x' to green '↓'.

[Figure 16-18](#) shows the steps to enable monitor-only mode for a certain Security Intelligence category, while all other categories remain in block mode.

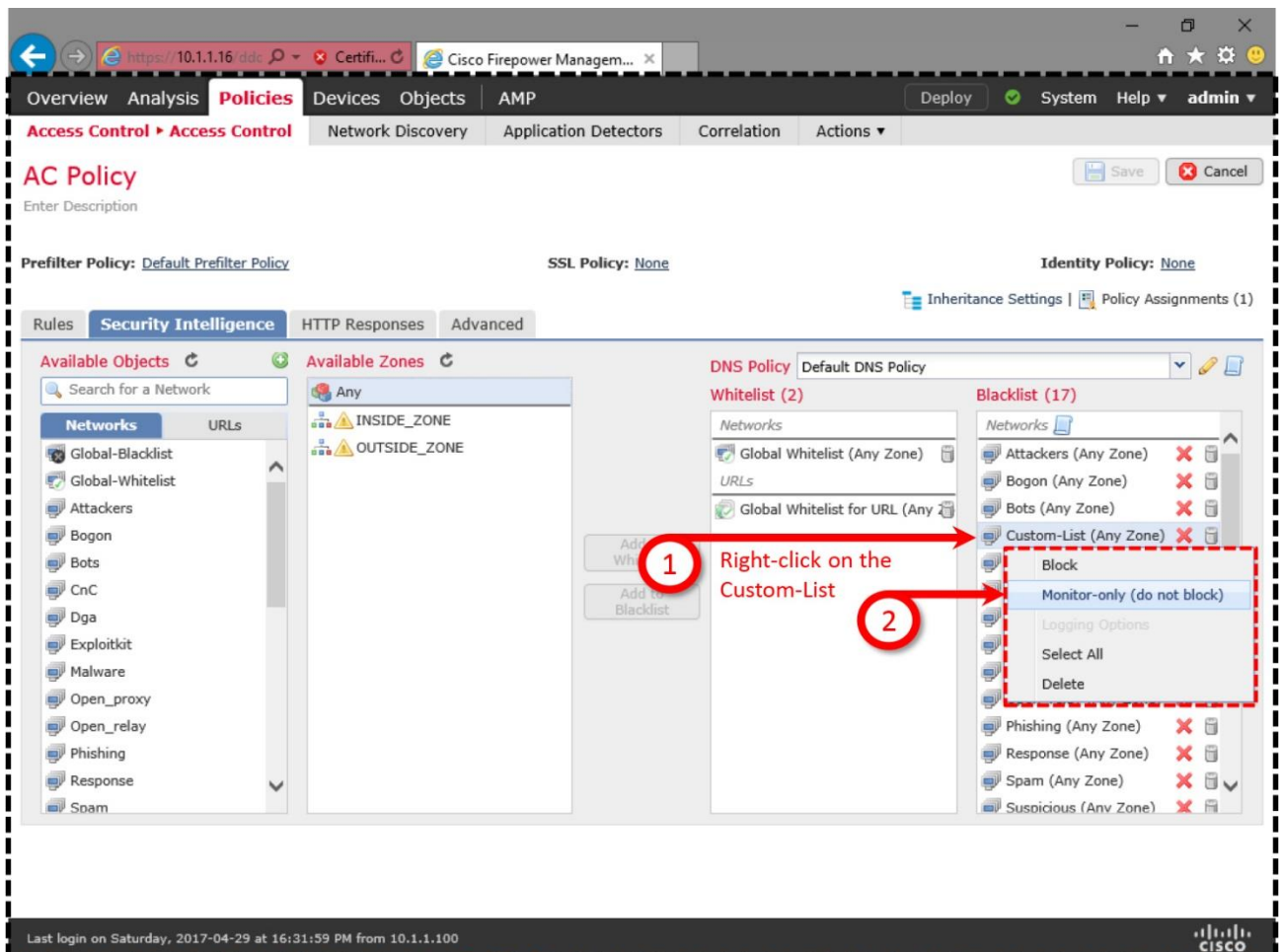


Figure 16-18. Configuration of Monitor-only Mode

Step 4. The configuration is complete. You can now save the changes and redeploy the Access Control policy.

The above configuration changes the action from Block to Monitor-only for any addresses in the custom list. To test the operation of monitor-only mode, access one of the addresses from the custom list, FTD allows that connection and generates a monitor event.

Figure 16-19 demonstrates the difference between monitor and block actions. The first connection attempt from the host 192.168.1.2 to 46.161.9.48 was blocked; however, the second attempt was allowed and the connection was monitored.

	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Security Intelligence Category
1	2017-04-29 21:32:08	2017-04-29 21:32:08	Allow	IP Monitor	192.168.1.2		46.161.9.48	RUS	Custom-List
2	2017-04-29 20:43:29		Block	IP Block	192.168.1.2		175.45.177.45	PRK	Global-Blacklist
3	2017-04-29 19:45:04		Block	IP Block	192.168.1.2		46.161.9.48	RUS	Custom-List
4	2017-04-29 14:45:57		Block	IP Block	192.168.1.2		104.97.6.228	USA	Malware
5	2017-04-29 14:44:05		Block	IP Block	192.168.1.2		180.124.44.98	CHN	Spam

Annotations in the image:

- 1: The first connection is blocked
- 2: The second connection is allowed
- The icon for monitored connection is different
- The same category experiences two different actions

Figure 16-19. Security Intelligence Events in Monitor-Only and Block Modes

Bypassing a Blacklist

If you find an address blacklisted by the Cisco Intelligence Feed, but it has been always essential for your regular business, you can report it to Cisco. If you want to access the address anyway while Cisco reinvestigates, you can whitelist that particular address. Whitelist bypasses the Security Intelligence check, but traffic is still subject to any subsequent inspection. If other components of an FTD find any anomaly, they can still block the connection, although the Security Intelligence whitelists it initially.

Adding an Address to Whitelist

The processes of whitelisting an address are identical to the process of blacklisting of address. You can add a whitelist in the Access Control policy as a Security Intelligence object. Alternatively, you can right-click on an address and use the **Whitelist Now** option from the context menu.

Figure 16-20 shows the **Whitelist IP Now** option in the context menu. After you right-click on an IP address, the connect menu appears.

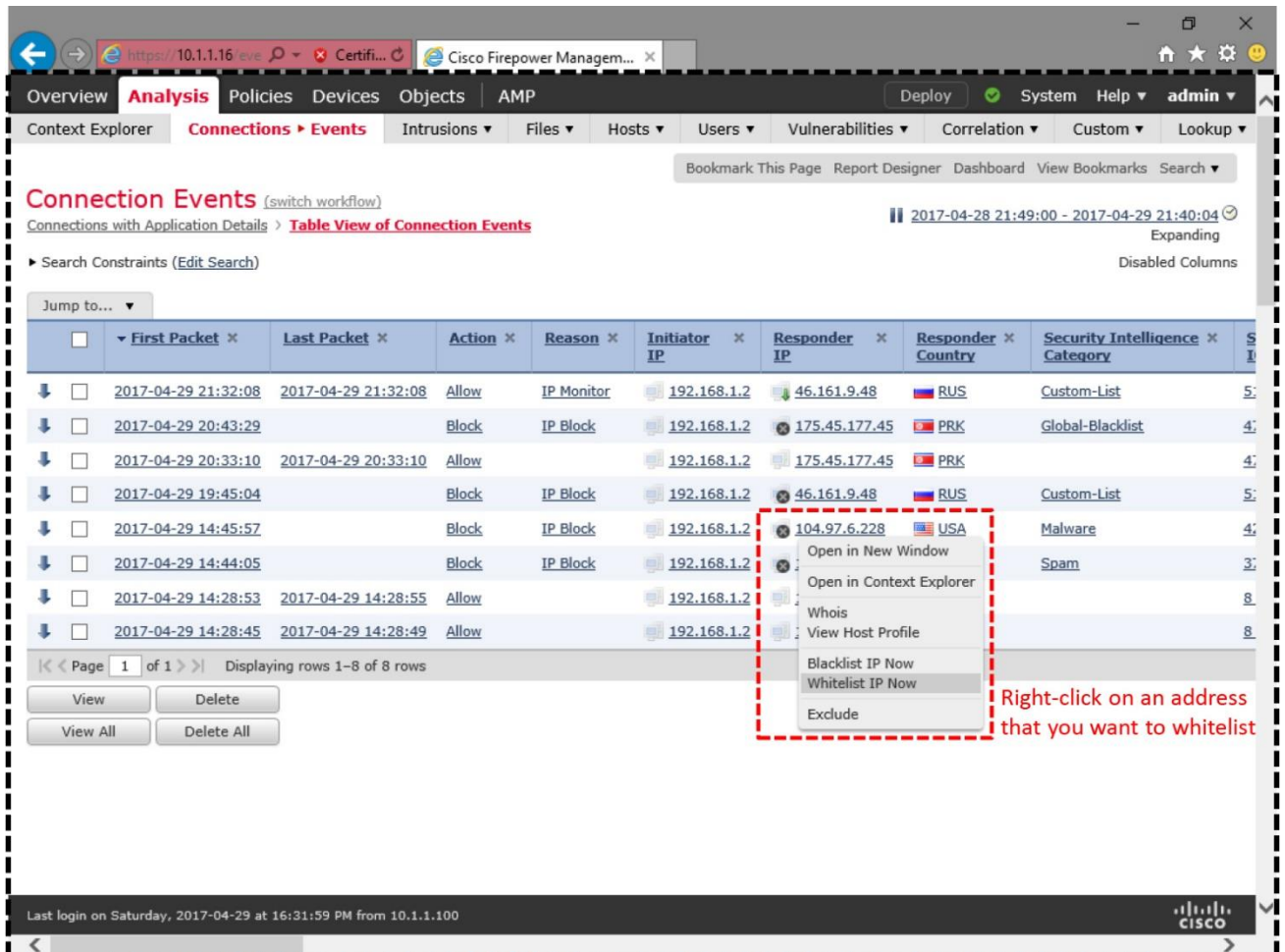


Figure 16-20. Whitelisting of an Address without Modifying an Access Control Policy

Figure 16-21 demonstrates a successful whitelisted connection. After overriding a blacklisted address with whitelist action, a connection appears like a regular allowed event.

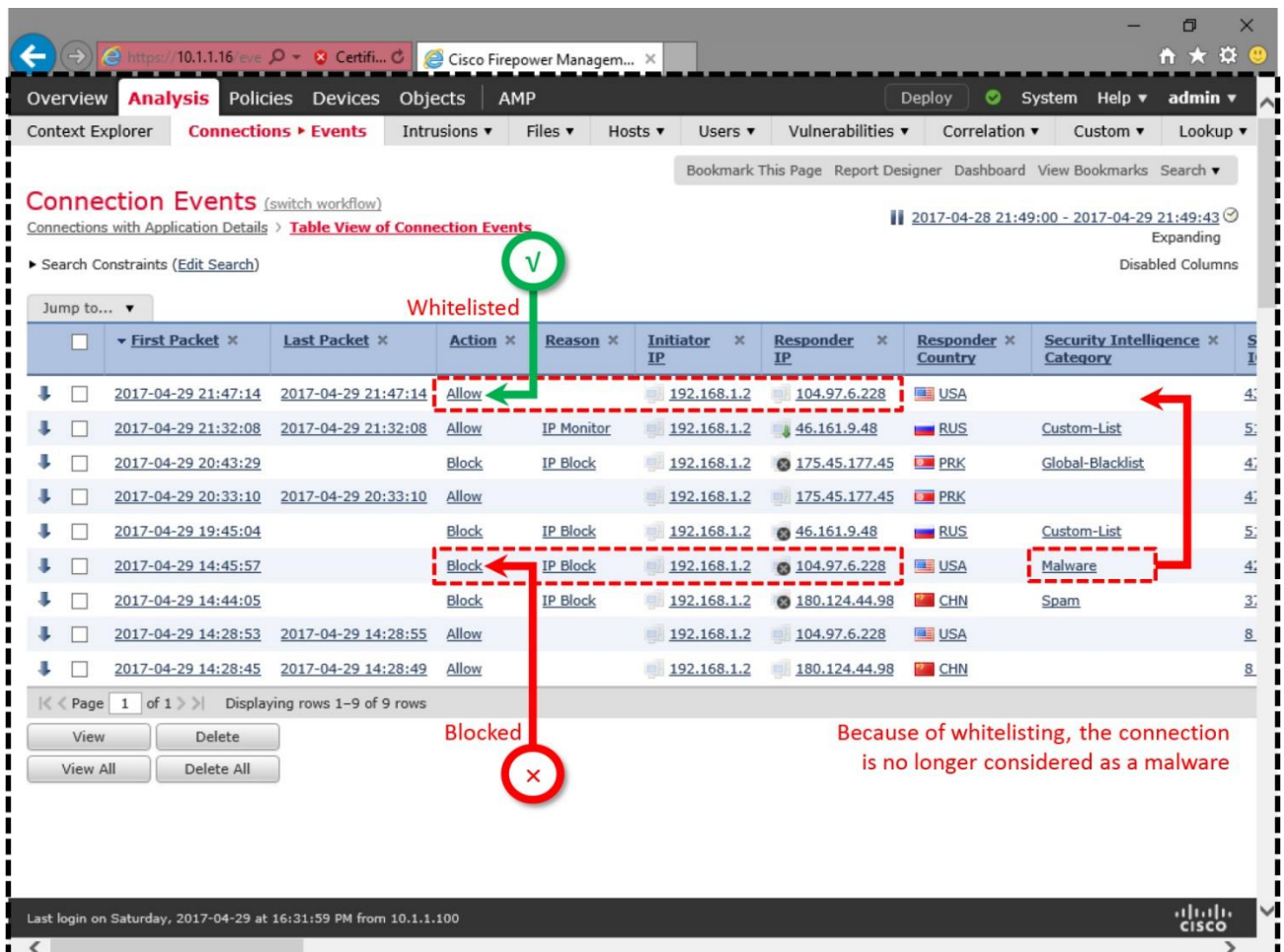


Figure 16-21. A Whitelist Action Bypasses the Security Intelligence Check

Deleting an Address from Whitelist

When you whitelist an address using the **Whitelist IP Now** option, the address is included in the Global Whitelist. If you want to stop whitelisting an address, delete the address from the **Global-Whitelist** object.

Caution

If you delete the entire Global-Whitelist object using the Security Intelligence configuration page, the Access Control policy stops enforcing the Whitelist Now function.

Figure 16-22 exhibits steps to delete an address from the Global-Whitelist Intelligence Object.

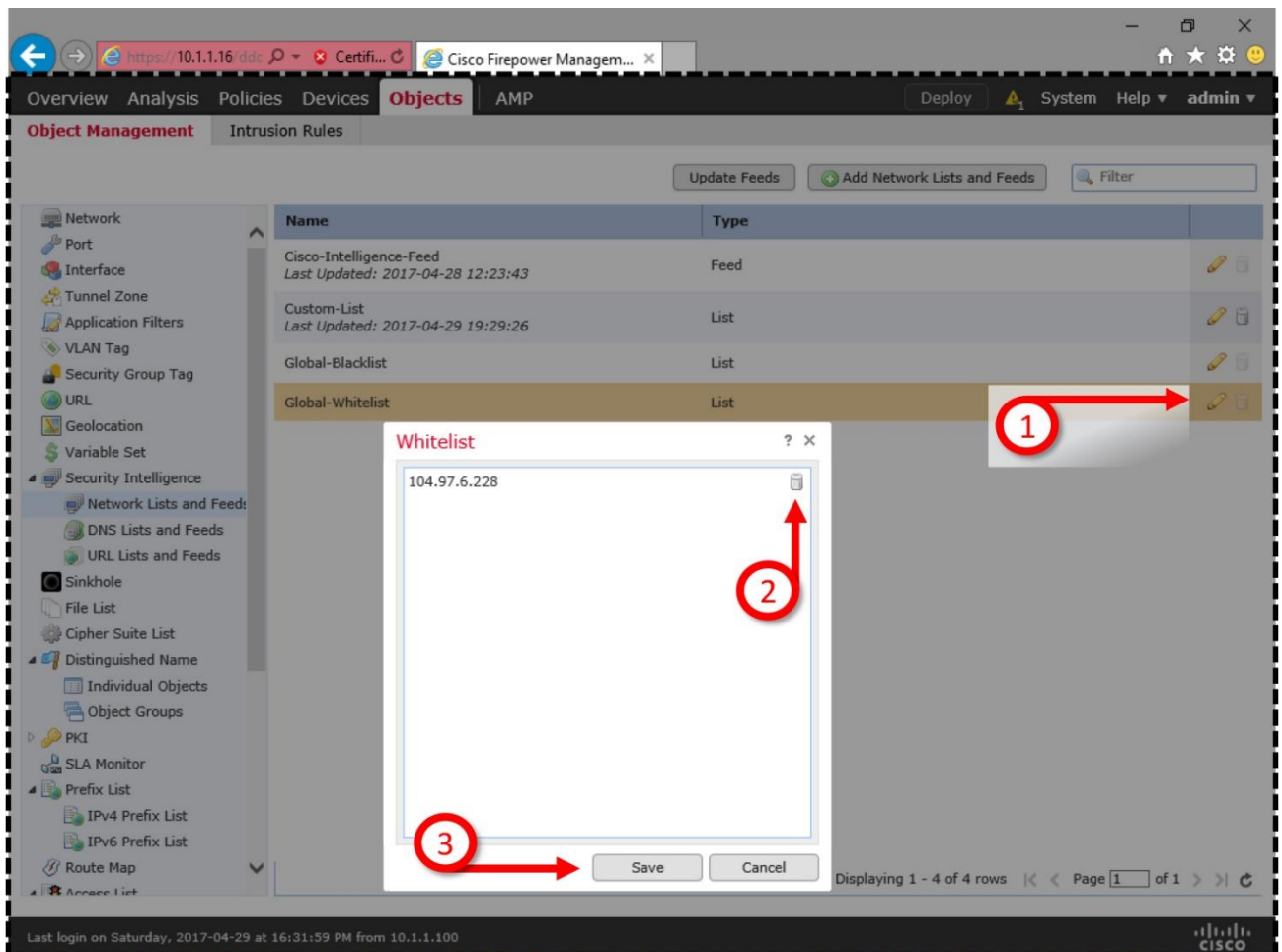


Figure 16-22. Deletion of an Address from the Global-Whitelist

Verification and Troubleshooting Tools

Before you begin investigating an issue with the Security Intelligence, check a couple of things. Such as,

- Check if the Security Intelligence health module is enabled on the health policy. It allows an FMC to generate alerts if the system fails to download the Security Intelligence data, and loads the data into memory.

[Figure 16-23](#) shows the option to enable the health module for Security Intelligence. To find this page, go to the **System > Health > Policy** page, edit a health policy, and select **Security Intelligence** from the left panel. You must redeploy a health policy if you change any settings.

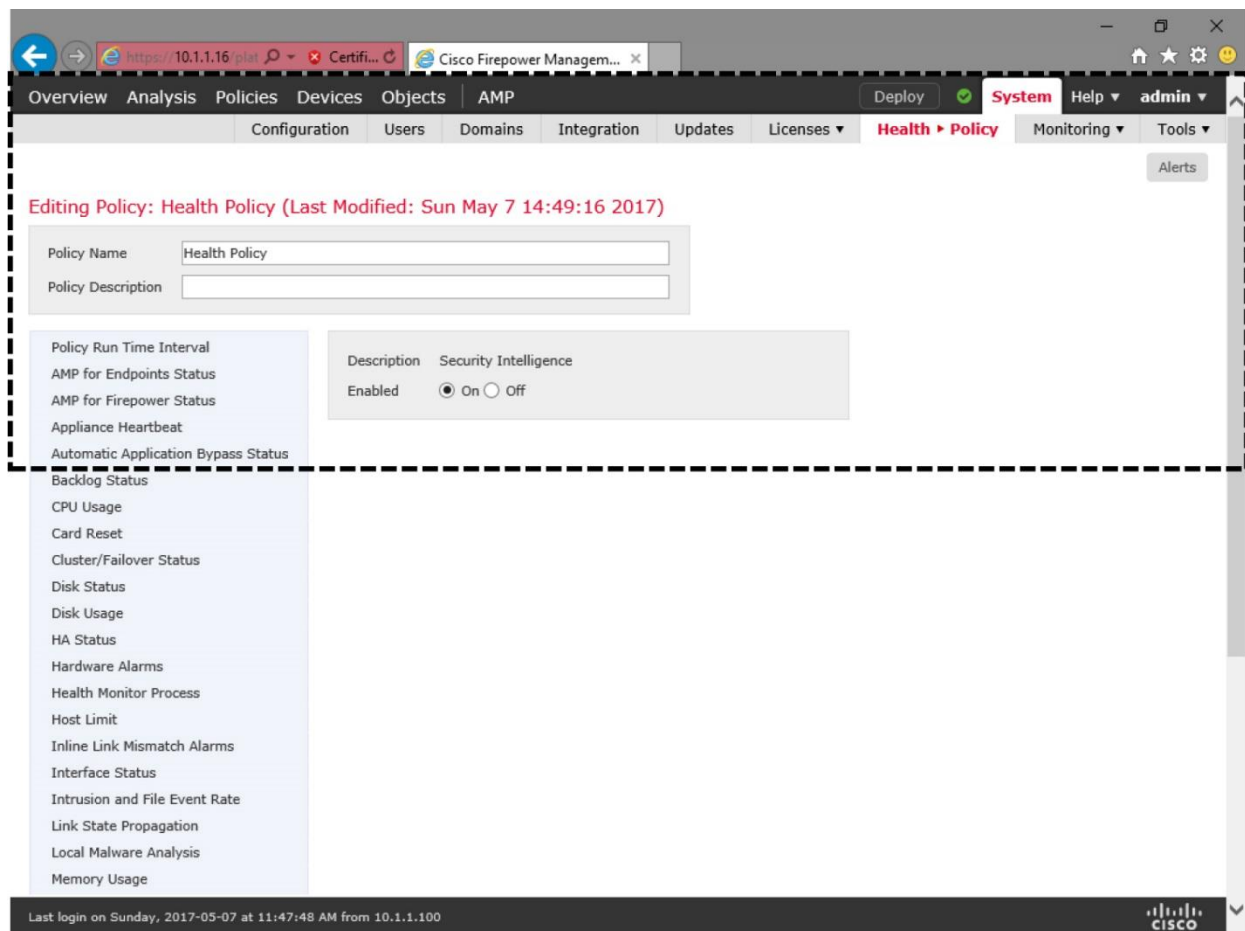


Figure 16-23. *Security Intelligence Health Module*

- Check if the FMC has a valid Threat license, and the license is applied on the desired FTD. If the Threat license is disabled or expired, an FMC stops obtaining the latest Cisco Intelligence Feed from the Cisco cloud.

Figure 16-24 shows the device management page where you can enable and disable a Threat license for a managed device.

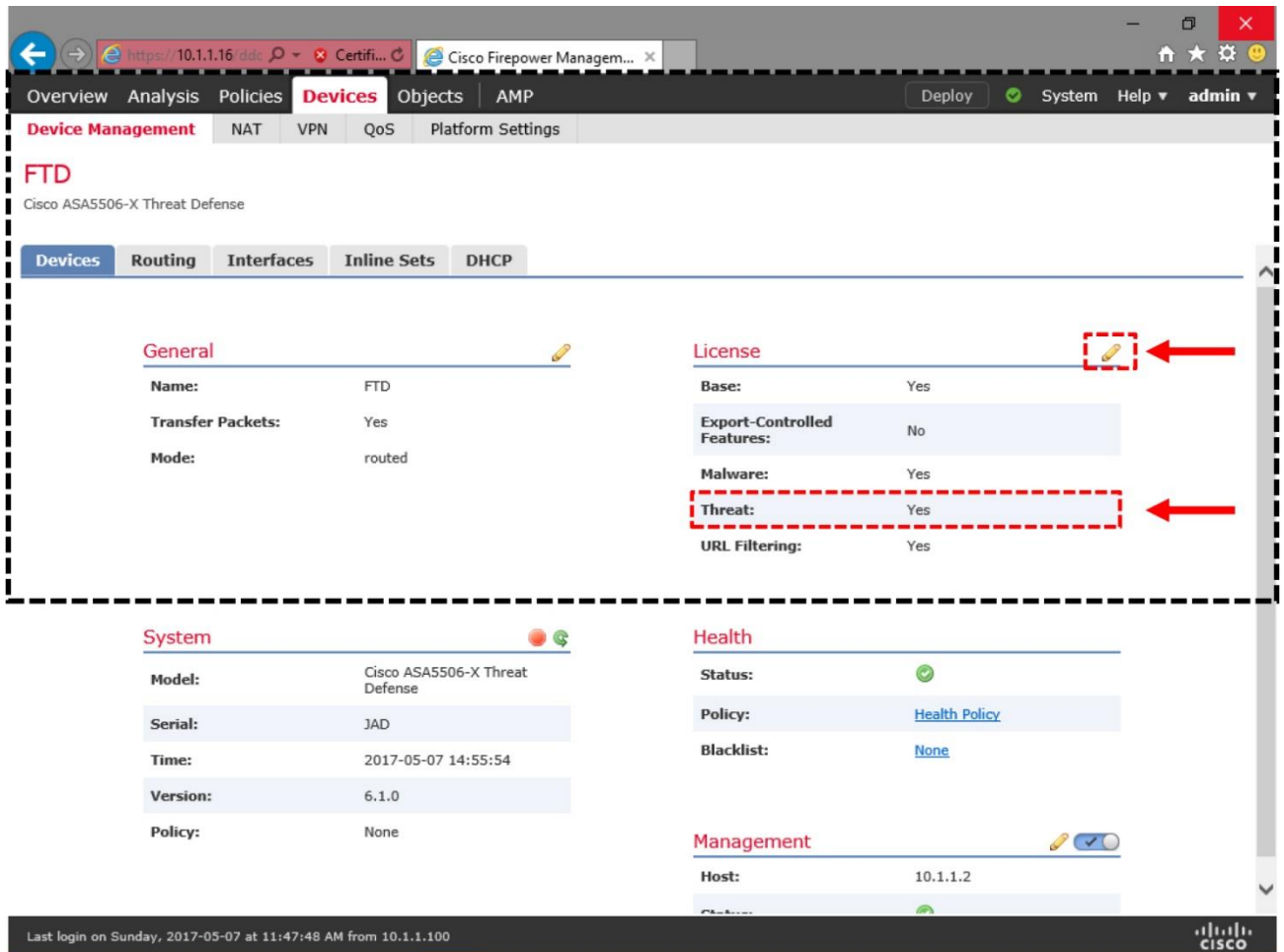


Figure 16-24. Device Management Page Provides Options for License Administration

Verifying the Download of the Latest Files

Using the CLI, you can verify if the FMC has downloaded the Intelligence Feed from the Cisco cloud. Similarly, by accessing the CLI of FTD, you can verify if an FTD has received the latest Security Intelligence files from the FMC.

[Example 16-1](#) shows the Security Intelligence files on an FMC — before and after a Cisco Intelligence Feed is downloaded.

Example 16-1 Security Intelligence (for IP Address) Files on an FMC

```
! Right after a fresh installation, an FMC does not contain any blacklist files by default:
```

```
admin@FMC:~$ ls -halp /var/sf/iprep_download/
total 20K
drwxr-xr-x  5 www  www  4.0K Apr 28 01:22 ./
drwxr-xr-x 64 root root 4.0K Apr 28 02:20 ../
-rw-r--r--  1 www  www    0 Apr 28 01:22 IPRVersion.dat
drwxr-xr-x  2 www  www  4.0K Apr 28 01:22 health/
drwxr-xr-x  2 www  www  4.0K Apr 28 01:22 peers/
drwxr-xr-x  2 www  www  4.0K Apr 28 01:22 tmp/
admin@FMC:~$
```

```
! After updating the Cisco Intelligence Feed from the cloud, FMC shows the blacklist files:
```

```
admin@FMC~$ ls -halp /var/sf/iprep_download/
total 7.3M
drwxr-xr-x  5 www  www  4.0K Apr 28 16:39 ./
drwxr-xr-x 64 root root 4.0K Apr 28 02:20 ../
-rw-r--r--  1 root root 225K Apr 28 16:23 032ba433-c295-11e4-a919-
d4ae5275a468
-rw-r--r--  1 root root   37 Apr 28 16:23 1b117672-7453-478c-be31-
b72e89calacb
-rw-r--r--  1 root root  43K Apr 28 16:23 23f2a124-8278-4c03-8c9d-
d28fe08b5e98
-rw-r--r--  1 root root  5.3K Apr 28 16:23 2CCDA18E-DDFF-4F5C-AF9A-
F009852183F4
-rw-r--r--  1 root root  9.4K Apr 28 16:23 2b15cb6f-a3fc-4e0e-a342-
ccc5e5803263
-rw-r--r--  1 root root   52 Apr 28 16:23 30f9e69c-d64c-479c-821d-
0e4edab8217a
-rw-r--r--  1 root root 682K Apr 28 16:23 3e2af68e-5fc8-4b1c-b5bc-
b4e7cab598ba
-rw-r--r--  1 root root   48 Apr 28 16:23 5a0b6d6b-e2c3-436f-b4a1-
48248b330a26
-rw-r--r--  1 root root   32 Apr 28 16:23 5f8148f1-e5e4-427a-aa3b-
ee1c2745c350
-rw-r--r--  1 root root  47K Apr 28 16:23 60f4e2ab-d96c-44a0-bd38-
830252b63f46
-rw-r--r--  1 root root   31 Apr 28 16:23 6ba968f4-7a25-4793-a2c8-
7cc77f1ff437
-rw-r--r--  1 root root  165 Apr 28 16:23 A27C6AAE-8E52-4174-A81A-
47C59FECC092
-rw-rw-r--  1 www  www   39 Apr 28 16:42 IPRVersion.dat
-rw-r--r--  1 root root  6.2M Apr 28 16:22 Sourcefire_Intelligence_Feed
-rw-r--r--  1 root root   30 Apr 28 16:23 b1df3aa8-2841-4c88-8e64-
bfaacec7fedd
-rw-r--r--  1 root root  1.7K Apr 28 16:23 d7d996a6-6b92-4a56-8f10-
e8506e431ca5
drwxr-xr-x  2 www  www  4.0K Apr 28 01:22 health/
drwxr-xr-x  2 www  www  4.0K Apr 28 01:22 peers/
-rw-r--r--  1 root root  4.6K Apr 28 16:22 rep_dd.yaml
drwxr-xr-x  2 www  www  4.0K Apr 28 16:32 tmp/
admin@FMC:~$
```

[Example 16-2](#) shows the Security Intelligence blacklist (.blf) and whitelist (.wlf) files. A new FTD installation comes with the global blacklist and whitelist files. The Cisco Intelligence Feed files appears as soon as it receives an Access Control policy from the FMC.

Example 16-2 Security Intelligence (for IP Address) Files on an FTD

!After a fresh installation, FTD shows only the empty blacklist (.blf) and whitelist (.wlf) files. At this point, FMC has not applied a Cisco Intelligence Feed yet:

```
> expert
admin@firepower:~$ ls -halp /var/sf/iprep_download/
total 40K
drwxr-xr-x  5 www  www  4.0K Apr 28 10:44 ./
drwxr-xr-x 66 root  root  4.0K Dec 12 00:19 ../
-rw-rw-r--  1 www  www  118 Apr 28 10:17 .zones
-rw-rw-r--  1 www  www   17 Apr 28 10:44 IPRVersion.dat
-rw-r--r--  1 root  root   40 Apr 28 10:17 c76556bc-6167-11e1-88e8-
479de99bdfd1.blf
-rw-r--r--  1 root  root   40 Apr 28 10:17 d8eea83e-6167-11e1-a154-
589de99bdfd1.wlf
drwxr-xr-x  2 www  www  4.0K Sep 19 2016 health/
drwxr-xr-x  2 www  www  4.0K Sep 19 2016 peers/
drwxr-xr-x  2 www  www  4.0K Apr 28 10:44 tmp/
-rw-rw-r--  1 www  www  151 Apr 28 10:44 zone.info
admin@firepower:~$
```

!Upon a successful deployment of an Access Control policy, FTD received the necessary blacklist (.blf) and whitelist (.wlf) files from an FMC. Each of these files represent a Security Intelligence category.

```
admin@firepower:~$ ls -halp /var/sf/iprep_download/
total 1.1M
drwxr-xr-x  5 www  www  4.0K May  7 16:05 ./
drwxr-xr-x 66 root  root  4.0K Dec 12 00:19 ../
-rw-rw-r--  1 www  www  1003 May  7 16:04 .zones
-rw-r--r--  1 root  root 225K May  7 16:04 032ba433-c295-11e4-a919-
d4ae5275a468.blf
-rw-r--r--  1 root  root   37 May  7 16:04 1b117672-7453-478c-be31-
b72e89calacb.blf
-rw-r--r--  1 root  root  43K May  7 16:04 23f2a124-8278-4c03-8c9d-
d28fe08b5e98.blf
-rw-r--r--  1 root  root  9.4K May  7 16:04 2b15cb6f-a3fc-4e0e-a342-
ccc5e5803263.blf
-rw-r--r--  1 root  root  5.3K May  7 16:04 2ccda18e-ddff-4f5c-af9a-
f009852183f4.blf
-rw-r--r--  1 root  root   52 May  7 16:04 30f9e69c-d64c-479c-821d-
0e4edab8217a.blf
-rw-r--r--  1 root  root 682K May  7 16:04 3e2af68e-5fc8-4b1c-b5bc-
b4e7cab598ba.blf
-rw-r--r--  1 root  root   48 May  7 16:04 5a0b6d6b-e2c3-436f-b4a1-
48248b330a26.blf
-rw-r--r--  1 root  root   32 May  7 16:04 5f8148f1-e5e4-427a-aa3b-
ee1c2745c350.blf
-rw-r--r--  1 root  root  47K May  7 16:04 60f4e2ab-d96c-44a0-bd38-
830252b63f46.blf
-rw-r--r--  1 root  root   31 May  7 16:04 6ba968f4-7a25-4793-a2c8-
7cc77f1ff437.blf
```

```

-rw-r--r-- 1 root root 373 May 7 16:04 808e55a2-2d33-11e7-ab29-
ad43fb3c690a.blf
-rw-r--r-- 1 root root 17 May 7 16:04 IPRVersion.dat
-rw-r--r-- 1 root root 165 May 7 16:04 a27c6aae-8e52-4174-a81a-
47c59fecc092.blf
-rw-r--r-- 1 root root 30 May 7 16:04 b1df3aa8-2841-4c88-8e64-
bfaacec7fedd.blf
-rw-r--r-- 1 root root 40 May 7 16:04 c76556bc-6167-11e1-88e8-
479de99bdfd1.blf
-rw-r--r-- 1 root root 1.7K May 7 16:04 d7d996a6-6b92-4a56-8f10-
e8506e431ca5.blf
-rw-r--r-- 1 root root 53 May 7 16:04 d8eea83e-6167-11e1-a154-
589de99bdfd1.wlf
drwxr-xr-x 2 www www 4.0K Sep 19 2016 health/
drwxr-xr-x 2 www www 4.0K May 7 14:26 peers/
drwxr-xr-x 2 www www 4.0K May 7 16:04 tmp/
-rw-rw-r-- 1 www www 1006 May 7 16:04 zone.info
admin@firepower:~$

```

Tip

If you have enabled Security Intelligence based on URL, you can find the list of blacklisted and whitelisted URLs in similar format. The files are located in the `/var/sf/siurl_download` directory.

Verifying the Loading of Addresses into Memory

The above example confirms that the FTD has received the Security Intelligence category files from an FMC. However, it does not prove that all the blacklisted addresses are loaded successfully into the FTD memory. You can verify it by looking at the debug messages on the CLI of the FTD while an Access Control policy is being deployed.

[Example 16-3](#) exhibits the debug messages on FTD when it loads the Security Intelligence configuration and entries into its memory. The following messages confirm that the Custom-List object has loaded all of the 25 addresses into its memory.

Example 16-3 *FTD Loads the Security Intelligence Data into Its Memory*

```

admin@firepower:~$ sudo tail -f /var/log/messages | grep -i reputation

May 7 16:05:40 ciscoasa SF-IMS[12223]: Reputation Preprocessor: Size
of shared
memory segment SFIPReputation.rt.0.0.1 is 134217728
May 7 16:05:40 ciscoasa SF-IMS[12223]: Reputation entries loaded: 1,
invalid: 0, re-defined: 0
(from file /ngfw/var/sf/iprep_download/d8eea83e-6167-11e1-a154-
589de99bdfd1.wlf)
May 7 16:05:40 ciscoasa SF-IMS[12223]: Reputation entries loaded: 0,
invalid: 0, re-defined: 0
(from file /ngfw/var/sf/iprep_download/c76556bc-6167-11e1-88e8-
479de99bdfd1.blf)
May 7 16:05:40 ciscoasa SF-IMS[12223]: Reputation entries loaded: 25,
invalid: 0,
re-defined: 0 (from file /ngfw/var/sf/iprep_download/808e55a2-2d33-11e7-
ab29-ad43fb3c690a.blf)

```

May 7 16:05:40 ciscoasa SF-IMS[12223]: Reputation entries loaded:
3310, invalid: 0,
re-defined: 7 (from file /ngfw/var/sf/iprep_download/60f4e2ab-d96c-44a0-
bd38-830252b63f46.blf)
May 7 16:05:40 ciscoasa SF-IMS[12223]: Reputation entries loaded: 0,
invalid: 0,
re-defined: 0 (from file /ngfw/var/sf/iprep_download/6ba968f4-7a25-4793-
a2c8-7cc77f1ff437.blf)
May 7 16:05:40 ciscoasa SF-IMS[12223]: Reputation entries loaded:
3050, invalid: 0,
re-defined: 1 (from file /ngfw/var/sf/iprep_download/23f2a124-8278-4c03-
8c9d-d28fe08b5e98.blf)
May 7 16:05:40 ciscoasa SF-IMS[12223]: Reputation entries loaded: 112,
invalid: 0,
re-defined: 0 (from file /ngfw/var/sf/iprep_download/d7d996a6-6b92-4a56-
8f10-e8506e431ca5.blf)
May 7 16:05:40 ciscoasa SF-IMS[12223]: Reputation entries loaded: 1,
invalid: 0,
re-defined: 0 (from file /ngfw/var/sf/iprep_download/5a0b6d6b-e2c3-436f-
b4a1-48248b330a26.blf)
May 7 16:05:40 ciscoasa SF-IMS[12223]: Reputation entries loaded: 0,
invalid: 0,
re-defined: 0 (from file /ngfw/var/sf/iprep_download/5f8148f1-e5e4-427a-
aa3b-ee1c2745c350.blf)
May 7 16:05:40 ciscoasa SF-IMS[12223]: Reputation entries loaded: 676,
invalid: 0,
re-defined: 3 (from file /ngfw/var/sf/iprep_download/2b15cb6f-a3fc-4e0e-
a342-ccc5e5803263.blf)
May 7 16:05:40 ciscoasa SF-IMS[12223]: Reputation entries loaded: 0,
invalid: 0,
re-defined: 0 (from file /ngfw/var/sf/iprep_download/1b117672-7453-478c-
be31-b72e89calacb.blf)
May 7 16:05:40 ciscoasa SF-IMS[12223]: Reputation entries loaded: 1,
invalid: 0,
re-defined: 0 (from file /ngfw/var/sf/iprep_download/30f9e69c-d64c-479c-
821d-0e4edab8217a.blf)
May 7 16:05:40 ciscoasa SF-IMS[12223]: Reputation entries loaded:
48044, invalid: 0,
re-defined: 0 (from file /ngfw/var/sf/iprep_download/3e2af68e-5fc8-4b1c-
b5bc-b4e7cab598ba.blf)
May 7 16:05:40 ciscoasa SF-IMS[12223]: Reputation entries loaded:
15962, invalid: 0,
re-defined: 112 (from file /ngfw/var/sf/iprep_download/032ba433-c295-11e4-
a919-d4ae5275a468.blf)
May 7 16:05:40 ciscoasa SF-IMS[12223]: Reputation entries loaded: 0,
invalid: 0,
re-defined: 0 (from file /ngfw/var/sf/iprep_download/b1df3aa8-2841-4c88-
8e64-bfaacec7fedd.blf)
May 7 16:05:40 ciscoasa SF-IMS[12223]: Reputation entries loaded: 9,
invalid: 0,
re-defined: 0 (from file /ngfw/var/sf/iprep_download/a27c6aae-8e52-4174-
a81a-47c59fecc092.blf)
May 7 16:05:40 ciscoasa SF-IMS[12223]: Reputation entries loaded: 377,
invalid: 0,
re-defined: 0 (from file /ngfw/var/sf/iprep_download/2ccda18e-ddff-4f5c-
af9a-f009852183f4.blf)
May 7 16:05:40 ciscoasa SF-IMS[12223]: Reputation Preprocessor shared
memory summary:
May 7 16:05:40 ciscoasa SF-IMS[12223]: Reputation total memory usage:
9442496 bytes

```
May 7 16:05:40 ciscoasa SF-IMS[12223]: Reputation total entries
loaded: 71568, invalid: 0, re-defined: 123
.
.
! <Output is Omitted for Brevity>
```

To determine if the memory is loaded with the latest set of Security Intelligence data, you can verify the timestamp of the FTD shared memory file. The timestamp should record the UTC time of the latest Access Control policy apply.

```
admin@firepower:~$ ls -halp /dev/shm/ | grep -i reputation
-rw-rw-rw- 1 root root 128M May 7 16:05 SFIPReputation.rt.0.0.1
admin@firepower:~$
```

Finding a Specific Address from the Lists

Let's say, you have just learned about a malware and its potential source address. You want to confirm if the address is included in the active Intelligence Feed, or should you consider blacklisting it manually. You can verify this from the CLI of FTD. Here are the steps:

Step 1. Run the following command to search a specific IP address within the *List* files. The following command uses the IP address 209.222.77.220 as an example. Replace this as appropriate.

```
admin@firepower:/var/sf/iprep_download$ egrep 209.222.77.220 *.blf
60f4e2ab-d96c-44a0-bd38-830252b63f46.blf:209.222.77.220
admin@firepower:/var/sf/iprep_download$
```

Step 2. The output on the prior step shows the *List* file where the IP address is listed, but it does not display the category. To determine the category type, run the following command to view the first line of the file:

```
admin@firepower:/var/sf/iprep_download$ head -n1 60f4e2ab-d96c-44a0-bd38-
830252b63f46.blf
#Cisco intelligence feed: CnC
admin@firepower:/var/sf/iprep_download$
```

Verifying the URL Based Security Intelligence Rules

You can leverage the Security Intelligence technology to blacklist, monitor and whitelist a suspicious website. The configuration of URL based Security Intelligence is similar to the configuration of the IP address based Security Intelligence. The only difference is, instead of selecting **Network** type intelligence object, you select **URL** type intelligence object. This section assumes that you have already selected URL based intelligence object by following the similar procedures for configuring the IP based Security Intelligence. Now, you want to verify if your deployment is successful.

Figure 16-25 shows the Security Intelligence configuration page. To blacklist or whitelist malicious URLs, select the **URL** subtab (instead of **Network** subtab, which you selected for IP based intelligence).

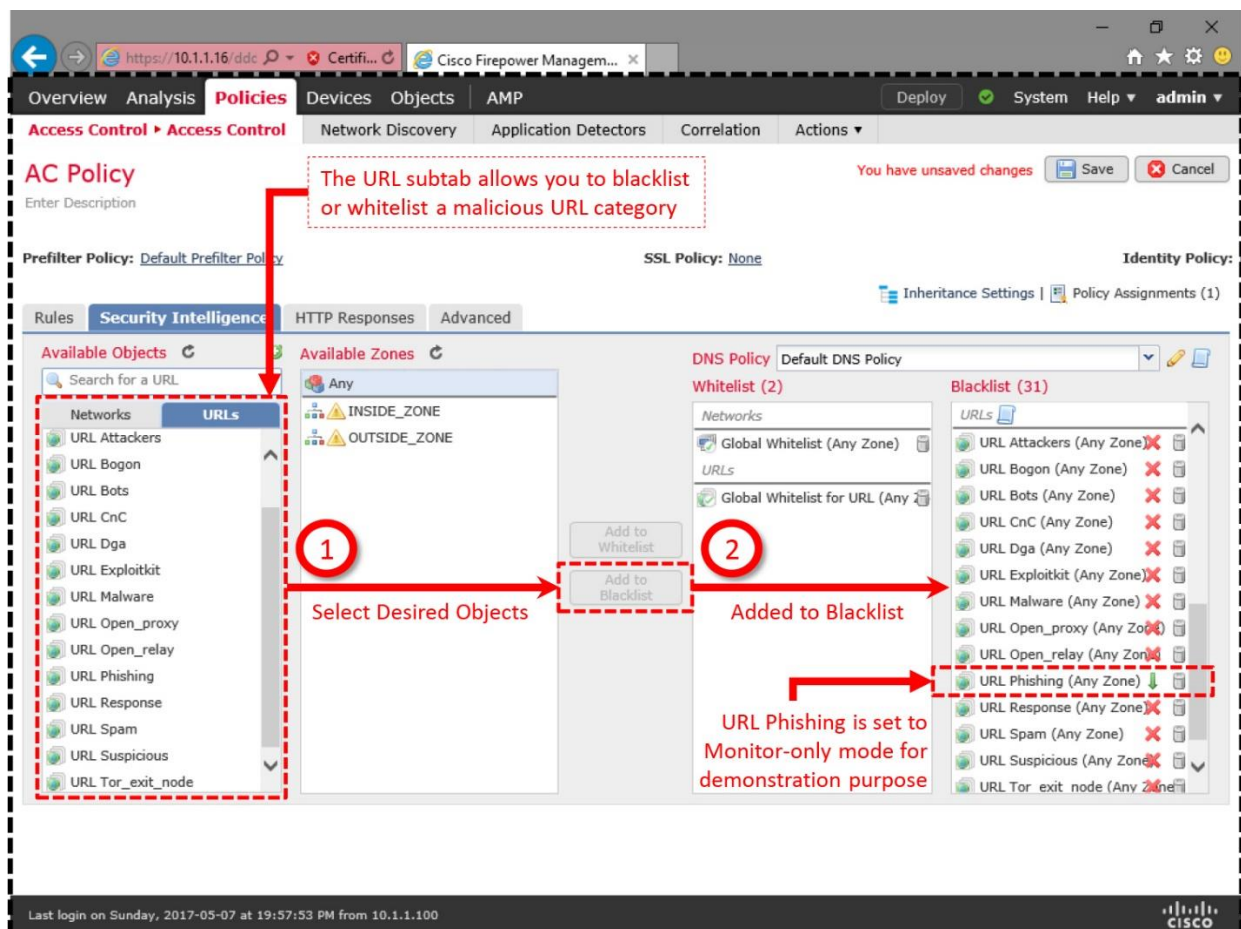


Figure 16-25. URL Subtab Shows the Categories of the Malicious Sites

Likewise, you can apply the same troubleshooting techniques to investigate an issue with the URL based Security Intelligence. You can find the blacklist and whitelist files for URL based Security Intelligence at `/var/sf/siurl_download` directory.

Example 16-4 shows the blacklist and whitelist files for the URL based Security Intelligence. Unlike IP based Security Intelligence, all of the URL based Security Intelligence files use .lf (List File) as their file extensions.

Example 16-4 Blacklist and Whitelist Files for the URL Based Security Intelligence

```
admin@firepower:~$ ls -halp /var/sf/siurl_download/
total 31M
drwxrwxr-x  5 www  detection 4.0K May  8 18:09 ./
drwxr-xr-x 66 root  root      4.0K Dec 12 00:19 ../
-rw-rw-r--  1 www  www       930 May  8 18:08 .zones
-rw-r--r--  1 root  root     422K May  8 18:08 032ba433-c295-11e4-a919-
d4ae5275d599.lf
-rw-r--r--  1 root  root      82 May  8 18:08 127dc4a2-1ea3-4423-a02d-
1f02069828ac.lf
```

```

-rw-r--r-- 1 root root          69 May  8 18:08 1b117672-7453-478c-be31-
b72e89ca4bfc.lf
-rw-r--r-- 1 root root        21M May  8 18:08 23f2a124-8278-4c03-8c9d-
d28fe08b8fc9.lf
-rw-r--r-- 1 root root          56 May  8 18:08 2b15cb6f-a3fc-4e0e-a342-
ccc5e5806394.lf
-rw-r--r-- 1 root root       147K May  8 18:08 2ccda18e-ddff-4f5c-af9a-
f0098521b525.lf
-rw-r--r-- 1 root root          53 May  8 18:08 30f9e69c-d64c-479c-821d-
0e4edab852ab.lf
-rw-r--r-- 1 root root         8.8K May  8 18:08 3e2af68e-5fc8-4b1c-b5bc-
b4e7cab5c9eb.lf
-rw-r--r-- 1 root root          65 May  8 18:08 5915d129-0d33-4e9c-969a-
eab3cde32156.lf
-rw-r--r-- 1 root root          52 May  8 18:08 5a0b6d6b-e2c3-436f-b4a1-
48248b333b57.lf
-rw-r--r-- 1 root root          48 May  8 18:08 5f8148f1-e5e4-427a-aa3b-
eelc2745f481.lf
-rw-r--r-- 1 root root       187K May  8 18:08 60f4e2ab-d96c-44a0-bd38-
830252b67077.lf
-rw-r--r-- 1 root root          47 May  8 18:08 6ba968f4-7a25-4793-a2c8-
7cc77f1f1256.lf
-rw-r--r-- 1 root root          17 May  8 18:08 IPRVersion.dat
-rw-r--r-- 1 root root        20K May  8 18:08 a27c6aae-8e52-4174-a81a-
47c59fecf1c3.lf
-rw-r--r-- 1 root root       2.2M May  8 18:08 b1df3aa8-2841-4c88-8e64-
bfaacec71300.lf
-rw-r--r-- 1 root root       2.6M May  8 18:08 d7d996a6-6b92-4a56-8f10-
e8506e434dd6.lf
-rw-rw-r-- 1 root root       5.1M May  8 18:09 dm_url10.acl
drwxr-xr-x 2 www  www       4.0K Sep 19 2016 health/
drwxr-xr-x 2 www  www       4.0K May  1 17:18 peers/
drwxr-xr-x 2 www  www       4.0K May  8 18:08 tmp/
-rw-rw-r-- 1 www  www      1015 May  8 18:08 url.rules
admin@firepower:~$

```

Since both blacklist and whitelist files use the same **.lf** extension, you cannot distinguish the purpose of a file by looking at the extension. However, you can use the **url.rules** file to determine this.

[Example 16-5](#) shows the purpose of each list file — the first file is a whitelist file, and the last file is set to monitor-only mode. All other list files are configured to block traffic.

Example 16-5 The url.rules File Shows the Action or Purpose of Each List File

```
admin@firepower:~$ cat /var/sf/siurl_download/url.rules
#security intelligence manifest file
si,5915d129-0d33-4e9c-969a-eab3cde32156.lf,1048597,white,any
si,127dc4a2-1ea3-4423-a02d-1f02069828ac.lf,1048613,block,any
si,5a0b6d6b-e2c3-436f-b4a1-48248b333b57.lf,1048599,block,any
si,5f8148f1-e5e4-427a-aa3b-ee1c2745f481.lf,1048600,block,any
si,6ba968f4-7a25-4793-a2c8-7cc77f1f1256.lf,1048601,block,any
si,30f9e69c-d64c-479c-821d-0e4edab852ab.lf,1048607,block,any
si,2b15cb6f-a3fc-4e0e-a342-ccc5e5806394.lf,1048612,block,any
si,1b117672-7453-478c-be31-b72e89ca4bfc.lf,1048606,block,any
si,3e2af68e-5fc8-4b1c-b5bc-b4e7cab5c9eb.lf,1048610,block,any
si,a27c6aae-8e52-4174-a81a-47c59fecf1c3.lf,1048604,block,any
si,2ccda18e-ddff-4f5c-af9a-f0098521b525.lf,1048611,block,any
si,60f4e2ab-d96c-44a0-bd38-830252b67077.lf,1048602,block,any
si,032ba433-c295-11e4-a919-d4ae5275d599.lf,1048609,block,any
si,b1df3aa8-2841-4c88-8e64-bfaacec71300.lf,1048603,block,any
si,23f2a124-8278-4c03-8c9d-d28fe08b8fc9.lf,1048605,block,any
si,d7d996a6-6b92-4a56-8f10-e8506e434dd6.lf,1048608,monitor,any
admin@firepower:~$
```

One last question remains — a list file uses Universally Unique Identifier (UUID) as its filename. It does not state the type of intelligence category it contains. To find that answer, you can view the first line of a list file. For example, the following example confirms that the d7d996a6-6b92-4a56-8f10-e8506e434dd6.lf stores the URL of the phishing websites.

```
admin@firepower:~$ head -n1 /var/sf/siurl_download/d7d996a6-6b92-4a56-8f10-
e8506e434dd6.lf
#Cisco DNS and URL intelligence feed: URL Phishing
admin@firepower:~$
```

Summary

In this chapter, you have learned how to detect a malicious address using the Security Intelligence feature. When there is a match, you can ask an FTD to block, monitor, or whitelist an address. This chapter also describes the backend file systems for the Security Intelligence feature. You can apply this knowledge to troubleshoot an issue with the Security Intelligence.

Quiz

1. Security Intelligence is the first level of defense mechanism implemented on a...

- a. Firewall engine
- b. Firepower Engine
- c. Firepower Management Center
- d. All of the above

2. Which of the following statement is true?

- a. FTD bypasses a whitelisted address from any further inspection.

b. FTD requires a direct connection to the internet in order to obtain the Cisco Intelligence Feed.

c. Blacklist IP Now option allows you to block an address without the redeployment of an Access Control policy.

d. Monitor-only mode of the Security Intelligence works only when FTD is deployed in passive mode.

3. Which of the following command displays the name of the Security Intelligence category from a blacklist file?

a. `tail -f filename.blf`

b. `tail filename.blf`

c. `head filename.blf`

d. `grep category_name filename.blf`

4. Which of the following command displays an exact IP address and confirms that the address is included in the current blacklist file?

a. `cat filename.blf`

b. `head ip_address filename.blf`

c. `grep ip_address *.blf`

d. `tail ip_address filename.blf`

Chapter 17. Blocking of a Domain Name Server (DNS) Query

An attacker can send phishing emails with links to malware websites. A user in your network may be deceived by the hoax content, and click on an obfuscated link by mistake. A Firepower system can intelligently prevent a user from accessing a malicious website by blocking its DNS query — one of the first things a client computer performs to access a website. This chapter describes the implementation of a DNS policy on a Firepower Threat Defense (FTD) system.

Essential Knowledge

Before diving into the DNS policy configuration, let's take a look at how a host computer learns the IP address of a website through a DNS query, and how a Firepower system can prevent a user from making a DNS query for a malicious domain.

Domain Name Server (DNS)

When you want to call one of your friends, what do you usually do with your phone? You pick up your phone, enter the phone book, find your friend in the phone book, and select his or her name. You do not need to memorize or type the phone number. The phone originates a call, on behalf of you, using the number on its phonebook. If you do not find the desired number in a phonebook, you ask someone who knows your friend for the phone number. This whole process is an analogy of how a DNS server works.

When you want to visit a website, you open a browser and enter the URL. However, before your browser learns the IP address of a website, the following tasks can happen behind the scene:

[Figure 17-1](#) shows various levels of DNS queries for a domain. Depending on the records on the intermediate server cache, the number of queries can be higher or lower. The process can happen within less than a second.

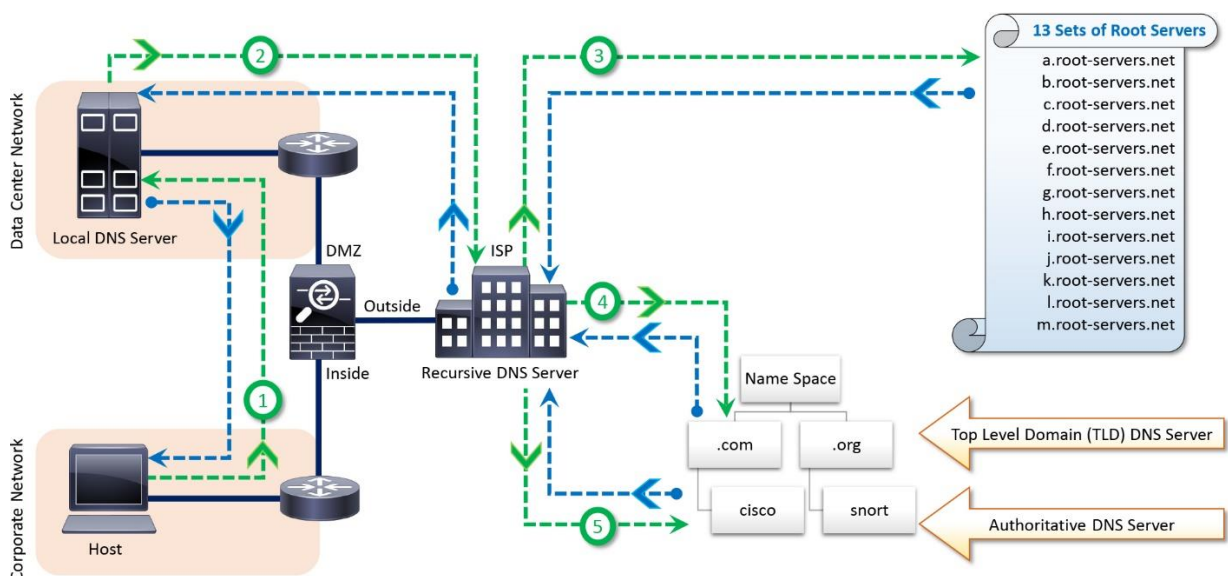


Figure 17-1. DNS Query throughout a Network

Step 1. Browser sends a query to the local DNS server in your network. If the local network has no internal DNS server or the DNS server has no information about the site you want to visit, then...

Step 2. A query is sent to the recursive DNS server of your Internet Service Provider (ISP). If the recursive server has information about the IP address on its cache, your browser receives it. No additional queries are performed. However, if the recursive server does not know the IP address, then...

Step 3. The recursive server sends the query to one of the thirteen sets of root nameservers located worldwide. A root server knows the DNS information about a Top Level Domain (TLD).

Step 4. The DNS server of a Top Level Domain sends information about the second level domain and its Authoritative nameserver. An Authoritative nameserver knows all of the addressing information for a particular domain.

Step 5. Authoritative nameserver responds to a query by returning the Address Record (A record) to your ISP. The ISP recursive server stores the record on its cache for a specific time limit, and sends the IP address to your browser.

Blocking of a DNS Query Using the Firepower System

You can add an Access Rule into your Access Control policy to block the DNS traffic; however, a traditional Access Rule is unable to identify a harmful domain based on the characteristics of its web contents.

Figure 17-2 shows an Access Rule that block DNS traffic solely based on DNS service ports. This static rule is unable to determine the risk level of a domain, and therefore, it cannot block an unsafe domain dynamically.

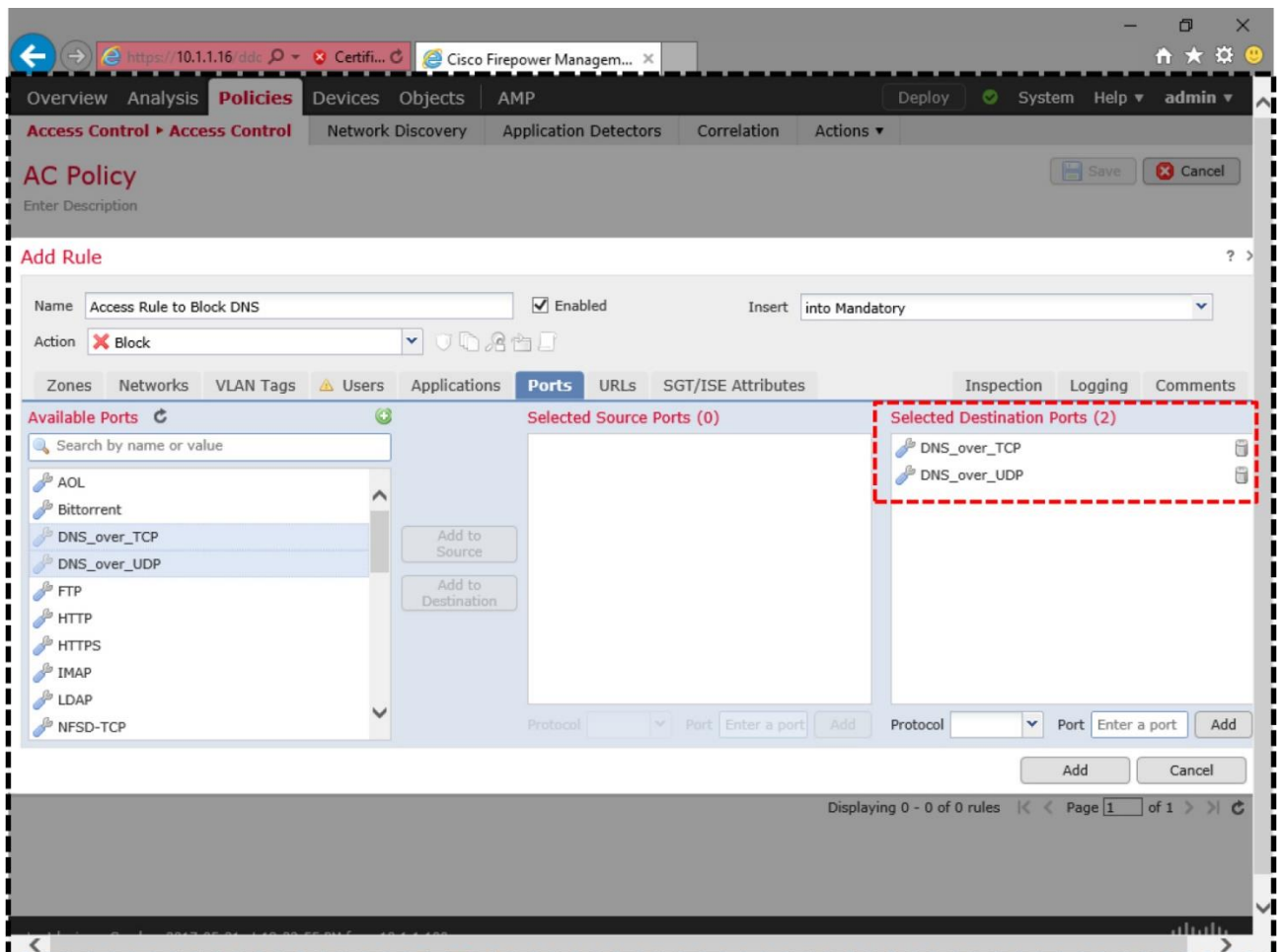


Figure 17-2. Identification and Blocking of DNS Traffic Based on Service Ports

The DNS based Security Intelligence feature of a Firepower System allows you to identify a susceptible DNS query and blacklist the resolution of an unsafe domain name, while any queries to a legitimate websites are allowed. It leads a browser not to obtain the IP address of a website. FTD blocks the request for a website before a potential HTTP connection is even established. Consequently, FTD does not require engaging its resources for further HTTP inspection.

[Figure 17-3](#) exhibits the workflow of a DNS query. It also shows where an FTD functions.

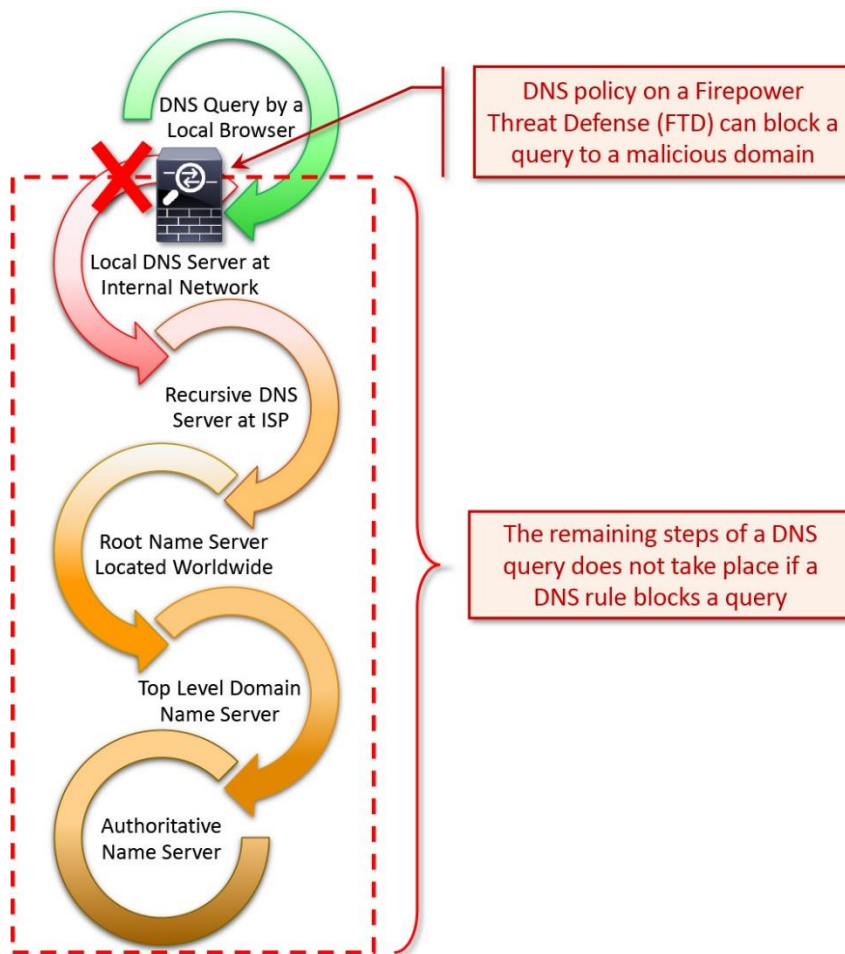


Figure 17-3. Placement of an FTD within the Workflow of a DNS Query

DNS Rule Actions

Depending on the security policy of your organization, you can add a DNS rule to blacklist, whitelist or monitor a DNS query.

Actions that can Interrupt a DNS Query

Firepower System offers various options to interrupt a DNS query. They are **Drop**, **Domain Not Found**, and **Sinkhole**.

Figure 17-4 shows the available actions that you can enable in a DNS rule.

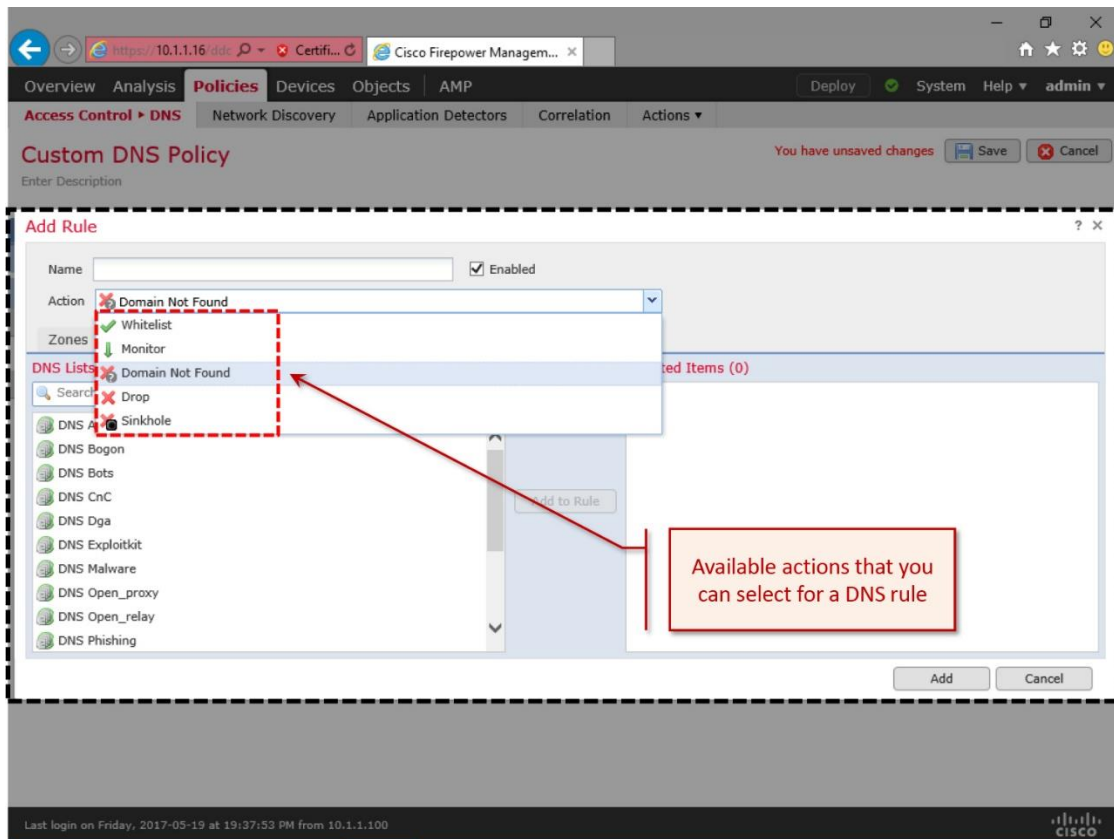


Figure 17-4. DNS Rule Actions

- **Drop:** FTD simply drops the DNS query for a particular domain.

Caution

User may still access a website if the client computer caches the DNS records and the existing records are not expired.

Figure 17-5 illustrates the drop action on an FTD. FTD simply drops the DNS query, no response is provided to the client.

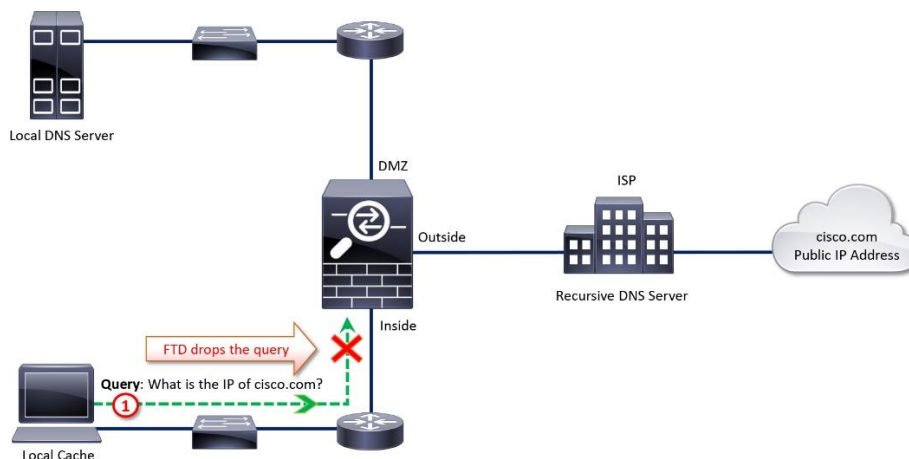


Figure 17-5. DNS Rule Action: Drop

- **Domain Not Found:** As a response to a DNS query, user receives NXDOMAIN (Non-existent Domain Name) message. The NXDOMAIN message indicates that the requested domain name does not exist. Browser cannot resolve the IP address for a domain. Consequently, the user fails to access the website.

[Figure 17-6](#) demonstrates the “Domain Not Found” action. Client computer that originates a DNS query receives a NXDOMAIN (Non-existent Domain Name) message as a response.

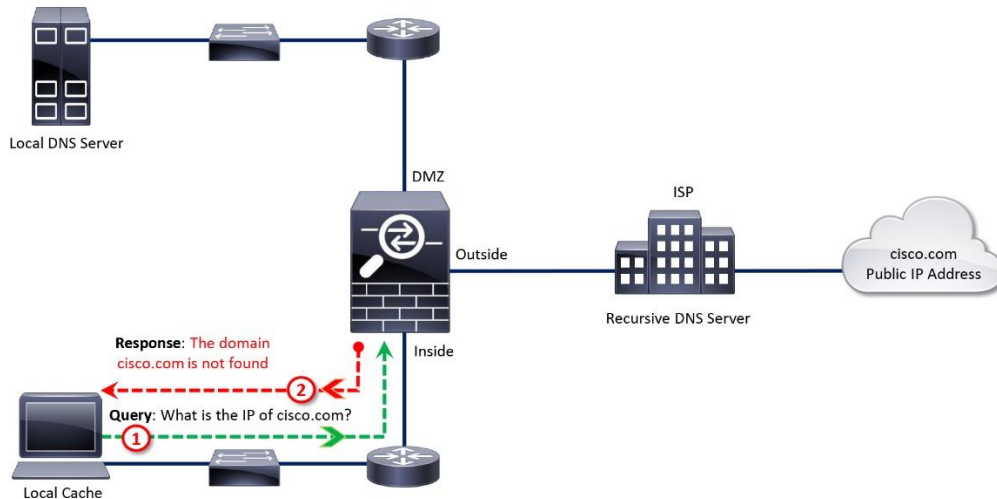


Figure 17-6. DNS Rule Action: Domain Not Found

- **Sinkhole:** FTD responds to a DNS query with a false IP address. A browser does not realize that an intermediate security device, FTD in this example, acts as a spoof DNS server, and responds to its query with a false IP address. The IP address may or may not be assigned to an existent DNS server. Using Sinkhole functionality, you can redirect malicious traffic to an alternate location for further security analysis.

[Figure 17-7](#) exhibits a spoof DNS server. FTD uses the IP address of this spoof DNS server, as a response to a DNS query, only when the domain is categorized as harmful.

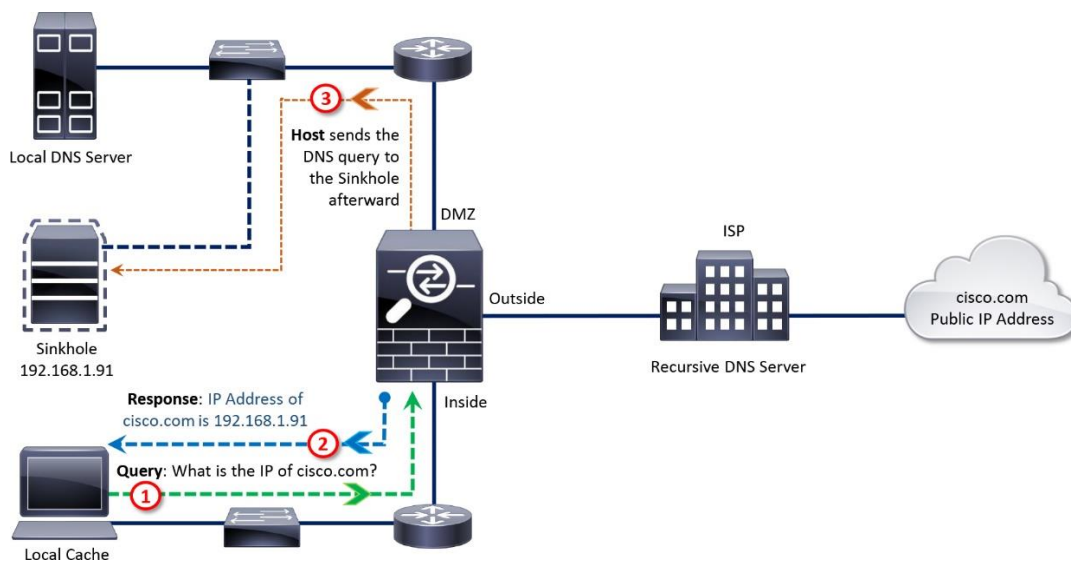


Figure 17-7. DNS Rule Action: Sinkhole (Fake Address Represents a Spoof DNS Server)

Figure 17-8 shows the implementation of sinkhole without a physical spoof server. You can assign any false IP address within a sinkhole object. FTD uses this false address to respond to any query to a harmful domain.

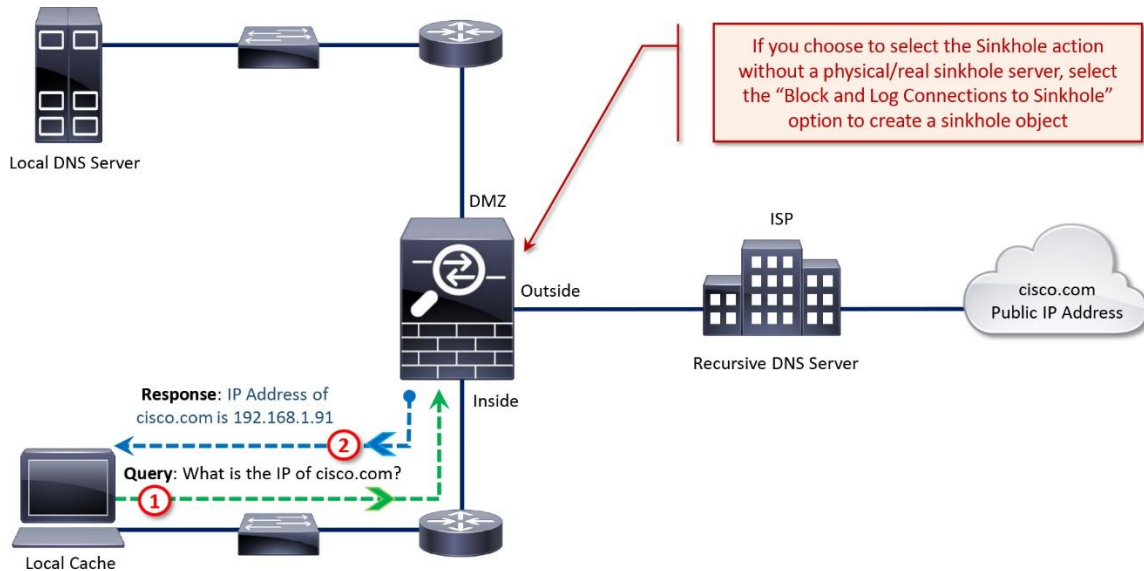


Figure 17-8. DNS Rule Action: Sinkhole (Fake Address Does Not Represent any Server)

Actions that Allow a DNS Query

Let's say, the Security Intelligence feed, provided by Cisco, blocks a query to your trusted domain. You have requested Cisco to reinvestigate the domain. While you are waiting on Cisco, you can use one of the following actions to allow a desired DNS query:

- **Whitelist:** Whitelist action allows the traffic to bypass an intelligence based check; however, they are still subject to other security inspections.
- **Monitor:** Monitor action allows an FTD to generate alerts when there is any match, however FTD does not interrupt traffic flow.

Source of Intelligence

In order to learn about the new suspicious domains, Firepower system updates its intelligence database from the following sources:

- **Feed:** Cisco has a dedicated threat intelligence and research team, known as Talos, who analyzes the behavior of the internet traffic, performs in-depth analysis on any suspicious activities, categorizes the potential domains based on their characteristics, and list them into a file.

One of the processes running on an FMC, CloudAgent, periodically communicates with the Cisco Cloud to download the latest feed. The frequency for updating the feed is configurable. Once an FMC downloads a feed, it sends the feed to its managed devices automatically. Redeployment of the Access Control policy is not necessary.

[Figure 17-9](#) shows the configuration of the update frequency for intelligence feed. To find this page, go to the **Object > Object Management** page. Under the **Security Intelligence**, select **DNS Lists and Feeds**, and edit the **Cisco-DNS-and-URL-Intelligence-Feed** using the pencil icon.

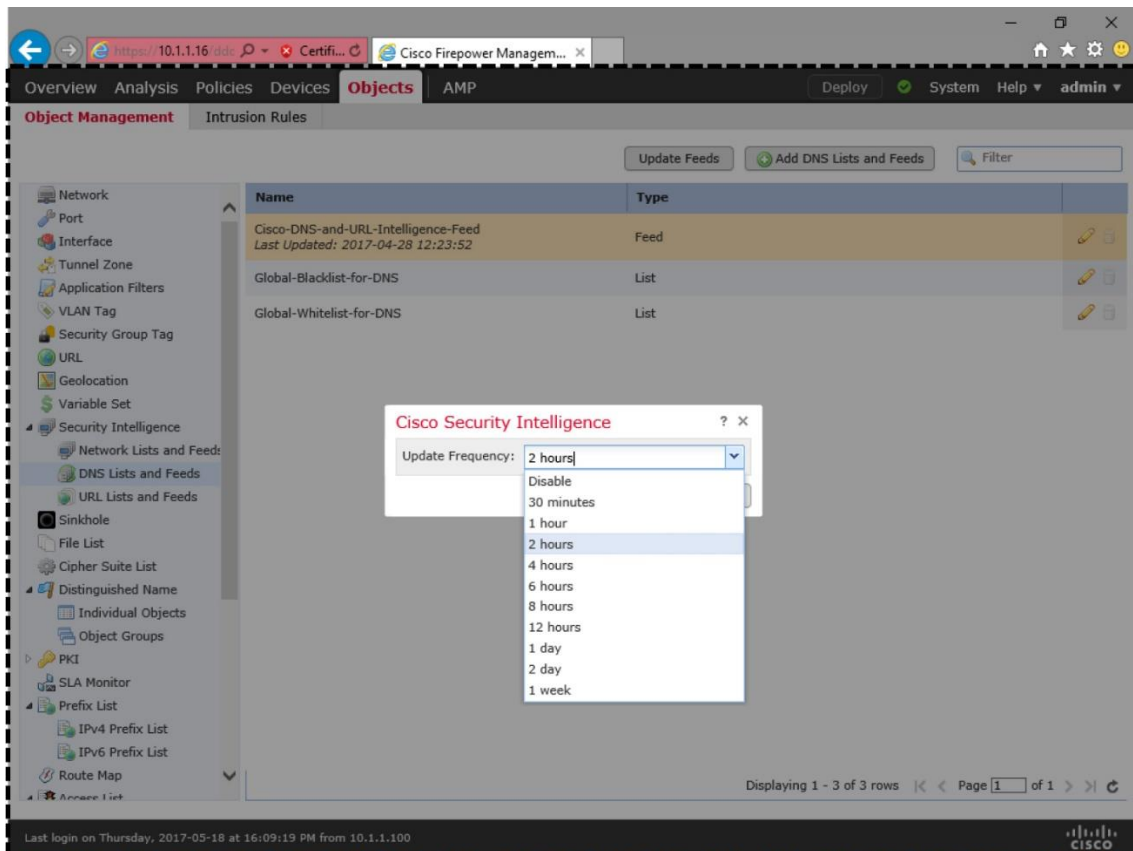


Figure 17-9. *Frequency for Cisco Intelligence Feed Update*

[Table 17-1](#) shows the key differences between feed and list.

- **List:** FMC supports the blacklisting or whitelisting of custom lists of domains. You can list the domains in a text file (.txt format), and upload the file manually to an FMC. Upon a successful upload, a custom DNS object appears along with the system-provided DNS objects. The process to add a DNS rule is described in the *Configuration* section.

Table 17-1. *Intelligence Feed vs. Intelligence List*

	Feed	List
Provider	The Cisco threat intelligence team creates and manages the Feed. FMC also supports the input of custom domains through an internal Feed URL.	Created by you, based on your own research and selection.
Maintenance	FMC can download the latest feed periodically.	You need to update an existing list file manually, as needed.

Tip

When you create your own list of domains for blacklist, enter one domain name per line. You can add a comment for future reference. Use the hash sign (#) at the beginning of a line to enter a comment.

[Figure 17-10](#) shows the DNS List/Feed configuration window. To find this window, go to the **Object Management** page, select **DNS Lists and Feeds** option under the **Security Intelligence**. Then, click the **Add DNS Lists and Feeds** button. The DNS List/Feed configuration window appears when you select **List** from the **Type** drop-down.

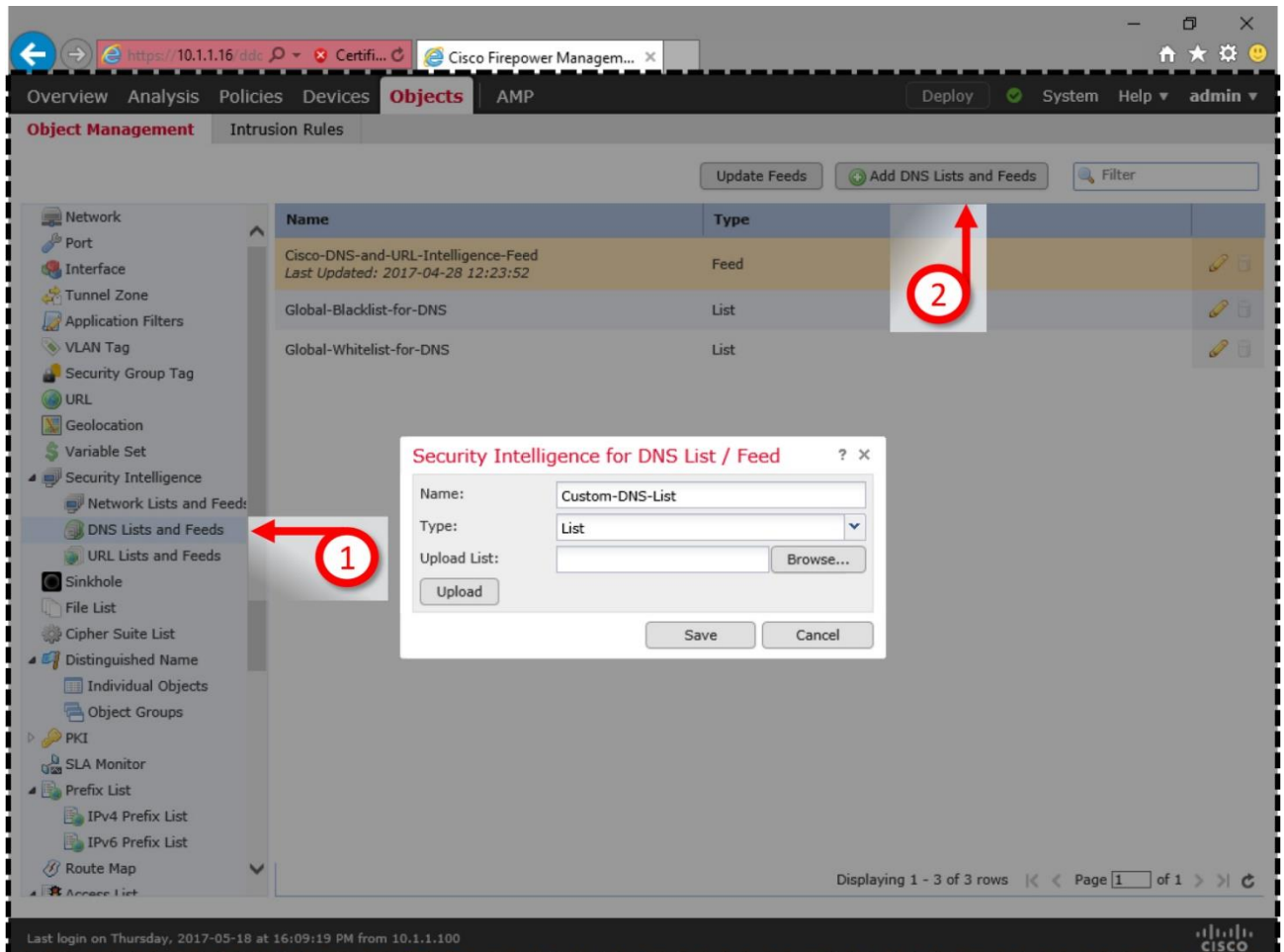


Figure 17-10. Option to Upload a DNS List File

Best Practices

Depending on the placement of an FTD in a network, you may have to wait additional time to notice an effect of a new DNS Policy. For example, if your one and only FTD is placed at the perimeter edge — between your company network and ISP network — your network hosts may continue resolving an undesired website until the local DNS cache expires. The hosts can notice the effect of a new DNS policy once the DNS cache of the client computer and local DNS server expires.

You can clear the cache of a DNS server manually. However, it may not be feasible to clear the cache of all of the network hosts manually, in real time. To expedite the enforcement of a new Firepower DNS policy, you can consider the following best practices:

- Enable IP address based Security Intelligence as well.
- Disable DNS caching on the local workstations. The System Administrator of your organization can confirm this setting.
- Position your FTD between the Local Area Network (LAN) and the DNS server, so that any egress traffic from LAN is subject to the Firepower inspection. Placing an FTD at the perimeter edge allows the hosts to resolve an address using the cache of the internal DNS server.

[Figure 17-11](#) shows different placement of an FTD. In the Network A, FTD allows queries to an internal DNS server, and block the queries to external DNS server. However, the FTD in Network B blocks queries to any — local or external — DNS servers.

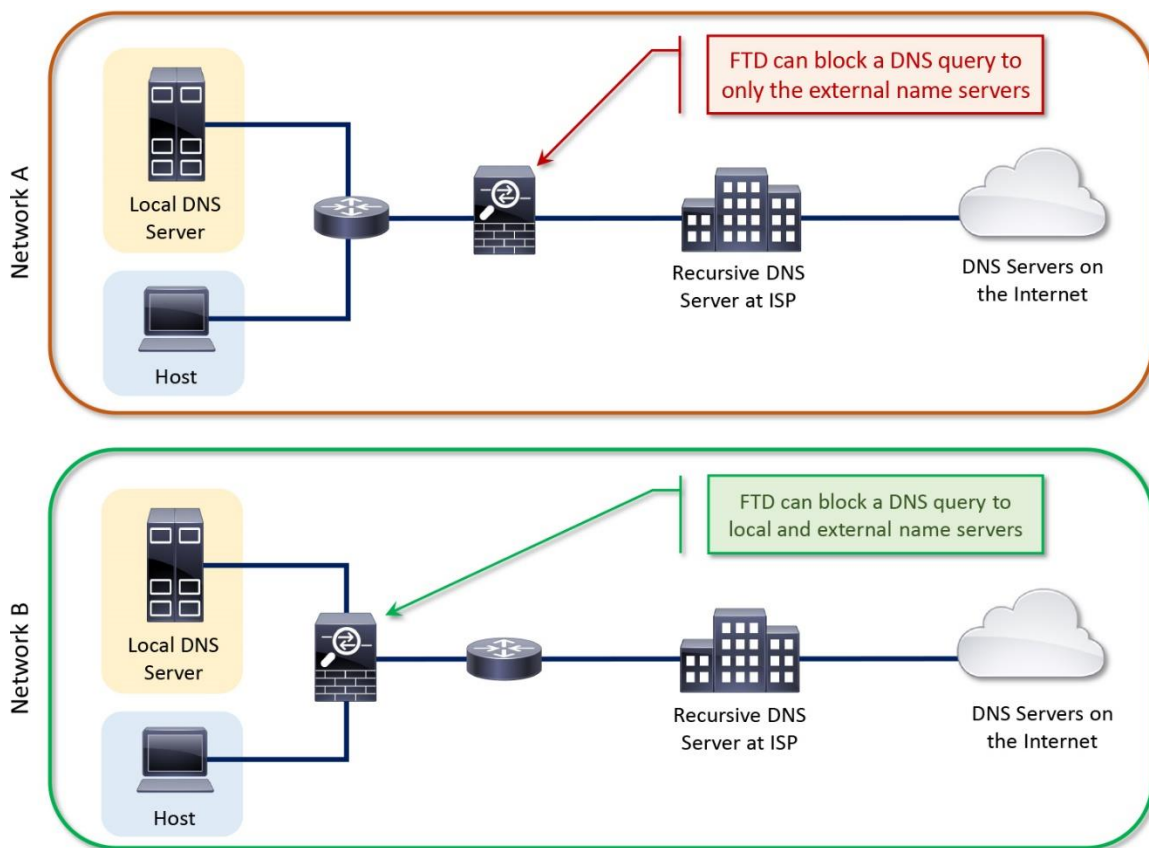


Figure 17-11. Effectiveness of a DNS Rule in Different FTD Deployment

Prerequisites

Before you configure a DNS policy, make sure that the following prerequisites are fulfilled:

- DNS Policy requires a Threat license. If you are in the process of purchasing a license, you can enable the Evaluation Mode to avoid any logistic and administrative delays. The

Evaluation Mode allows you to configure and deploy any features as if you have already installed a paid license.

- If you want to redirect a DNS query to a Sinkhole, you must configure a Sinkhole object (with a real or fake IP address) before you select the Sinkhole action for a DNS rule. You can create multiple sinkhole objects using different IP addresses, and use them for different purposes. For example, one object for malware, one object for phishing, etc.

[Figure 17-12](#) shows the configuration of a Sinkhole object. To find this configuration window, navigate to **Objects > Object Management > Sinkhole**, and click the **Add Sinkhole** button.

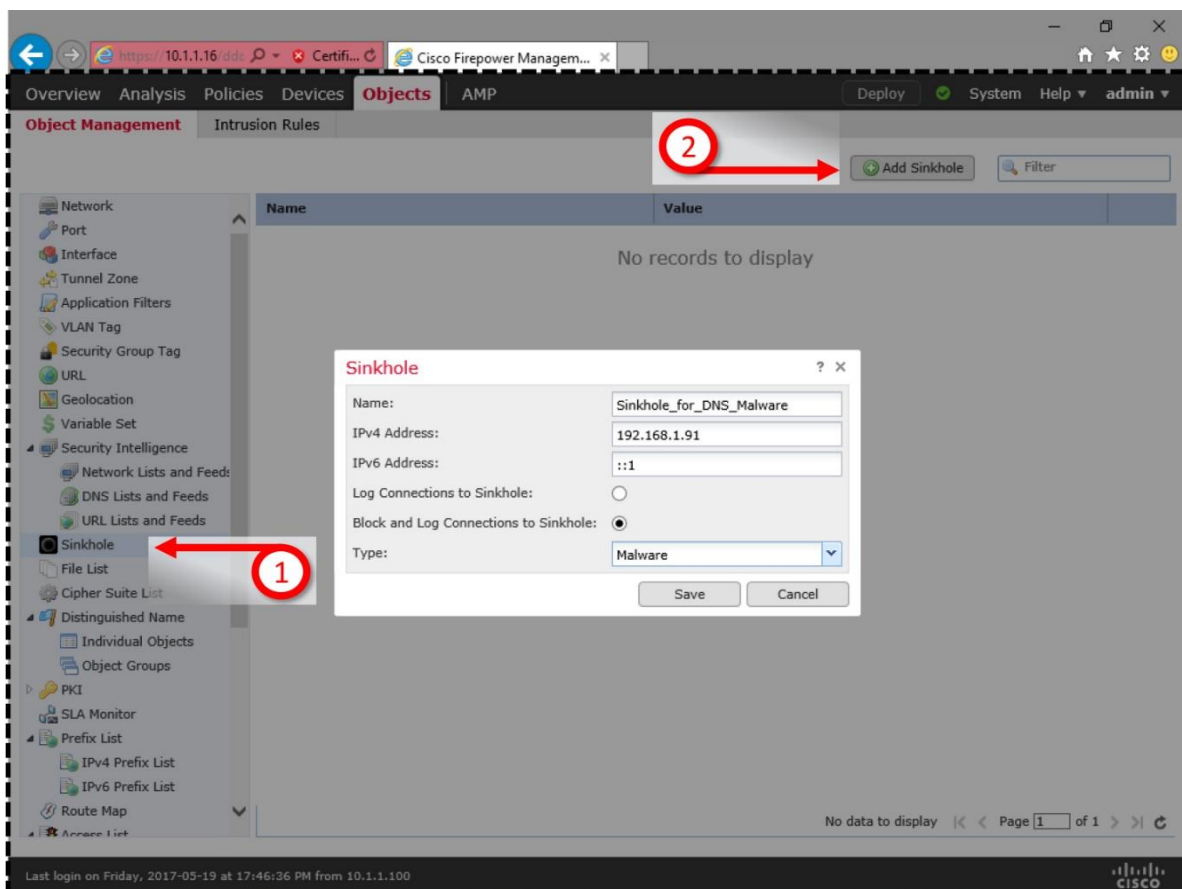


Figure 17-12. Configuration of a Sinkhole Object

Note

If you want to setup the Sinkhole functionality without a physical DNS server, select the “Block and Log Connections” option during the Sinkhole object configuration.

Configuring DNS Query Blocking

To block a DNS query using a Firepower System, you must perform the following two tasks on your FMC:

- Create a new DNS policy, or edit an existing one. Add the necessary DNS rule condition within.
- Invoke the desired DNS policy within an Access Control policy, and deploy the policies on an FTD.

The following sections describes the processes to enable DNS policies successfully on an FTD.

[Figure 17-13](#) shows the lab topology that is used in this chapter to configure DNS based Security Intelligence (DNS Policy).

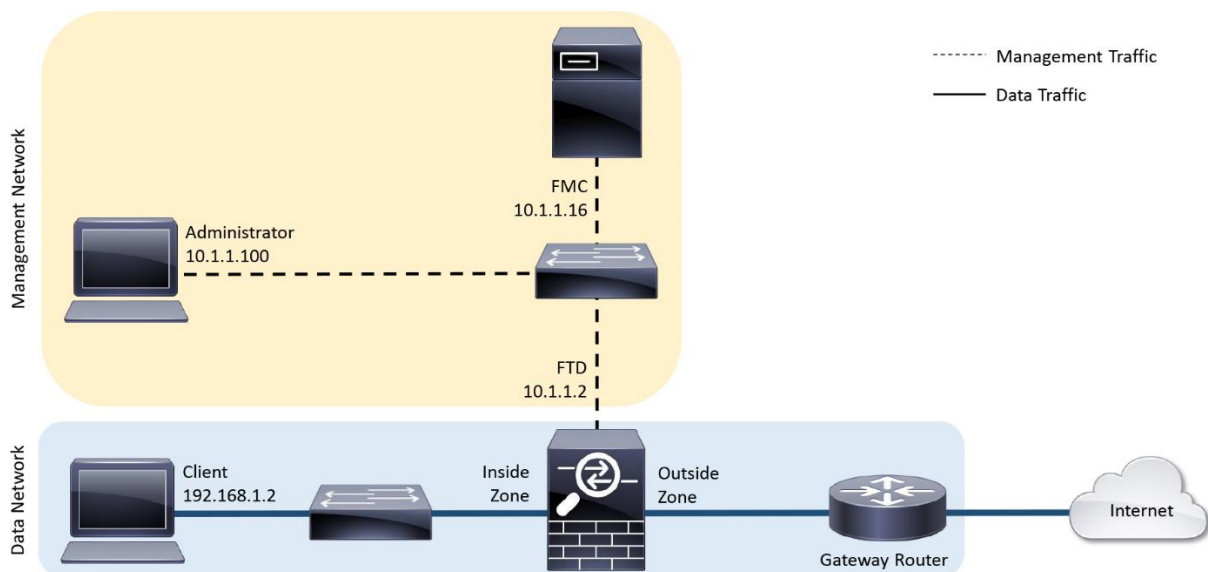


Figure 17-13. Lab Topology Used in This Chapter

Add a New DNS Rule

To add a new DNS rule, follow the steps below:

Step 1. Navigate to the **Policies > Access Control > DNS** page. Select the **Add DNS Policy** button. Alternatively, you can edit the system-provided **Default DNS Policy** and add your custom DNS rules within.

Figure 17-14 shows a DNS Policy editor page. Each DNS policy, by default, comes with two items — a Global Whitelist and Global Blacklist — that have higher precedence over a custom DNS rule.

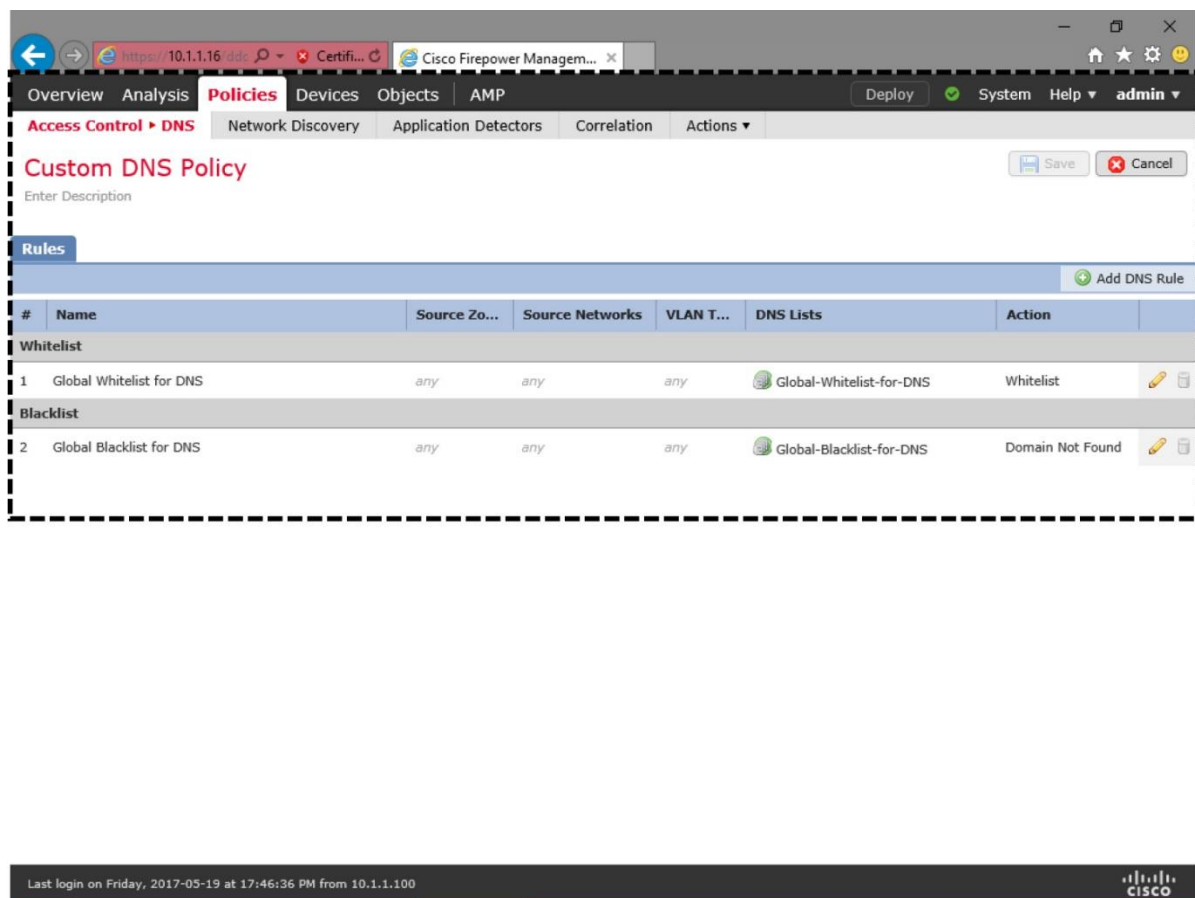


Figure 17-14. DNS Policy Editor Page

Step 2. Once the DNS Policy editor page appears, select the **Add DNS Rule** button. The **Add Rule** window appears.

Step 3. Give a name to your DNS rule, and select a desired action using the **Action** dropdown. The *Essential Knowledge* section of this chapter describes the functions of each action.

Step 4. Select **Zones**, **Networks**, and **VLAN** Tabs to define the source and destination traffic, as appropriate.

Step 5. Select the **DNS** tab. It shows the categories for unsafe DNS traffic. Add the desired categories to your rule.

[Figure 17-15](#) shows the DNS rule editor window. It allows you to select an intelligence category that you want to detect, and to define an action for any matching traffic.

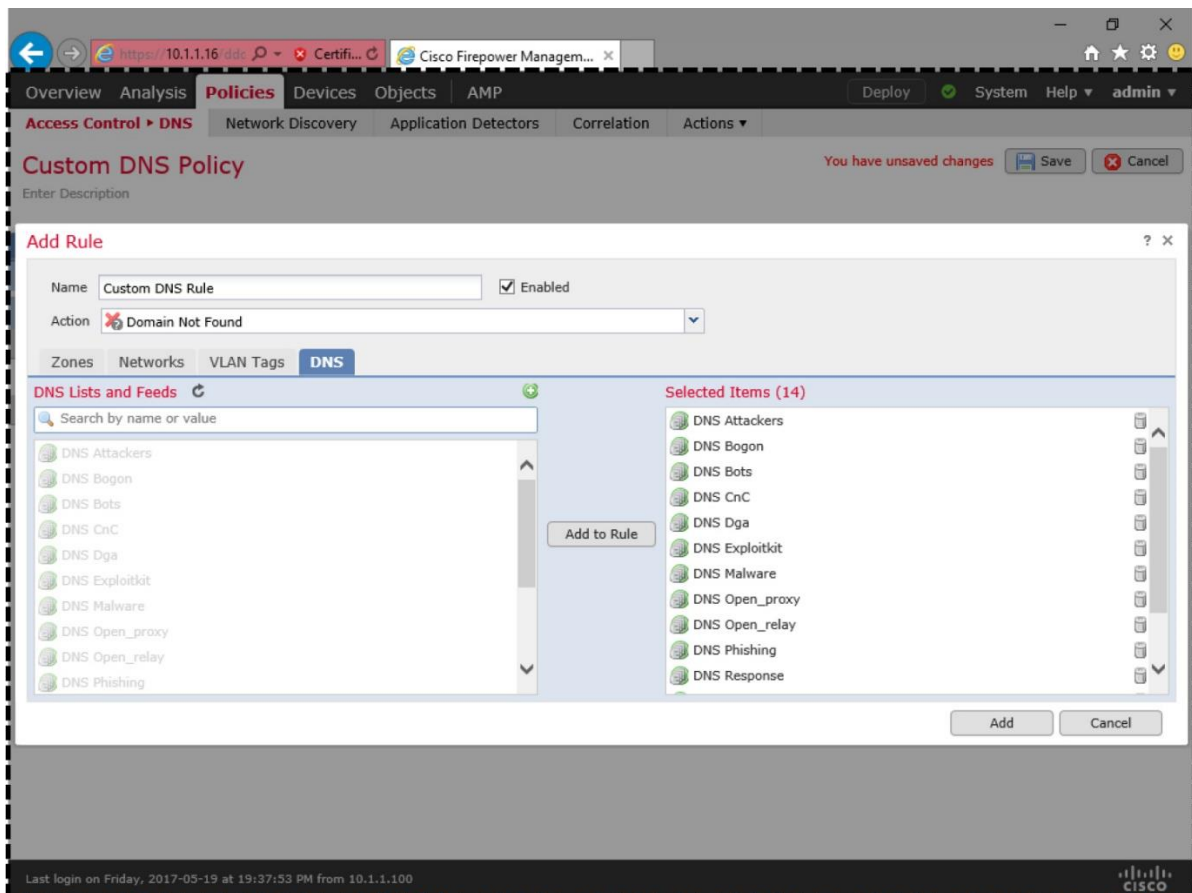


Figure 17-15. *DNS Rule Editor Window*

Step 6. The rule configuration is complete. Click the **OK** button to exit the DNS rule editor. Select the **Save** button to save the changes on your DNS policy.

[Invoke a DNS Policy](#)

You have just created a DNS policy. To deploy this policy on an FTD, you need to invoke it manually within an Access Control policy. By default, an Access Control policy invokes the system-provided default DNS policy.

To activate a desired DNS policy, follow the steps below:

Step 1. Navigate to the **Policies > Access Control > Access Control** page. Edit the Access Control policy that will be applied on an FTD.

Step 2. Once the Access Control policy editor page appears, select the **Security Intelligence** tab.

Step 3. In the Security Intelligence configuration page, you will find a **DNS Policy** dropdown. Select the desired DNS policy.

Figure 17-16 shows the Security Intelligence configuration page, which allows you to select and edit an available DNS policy on the fly.

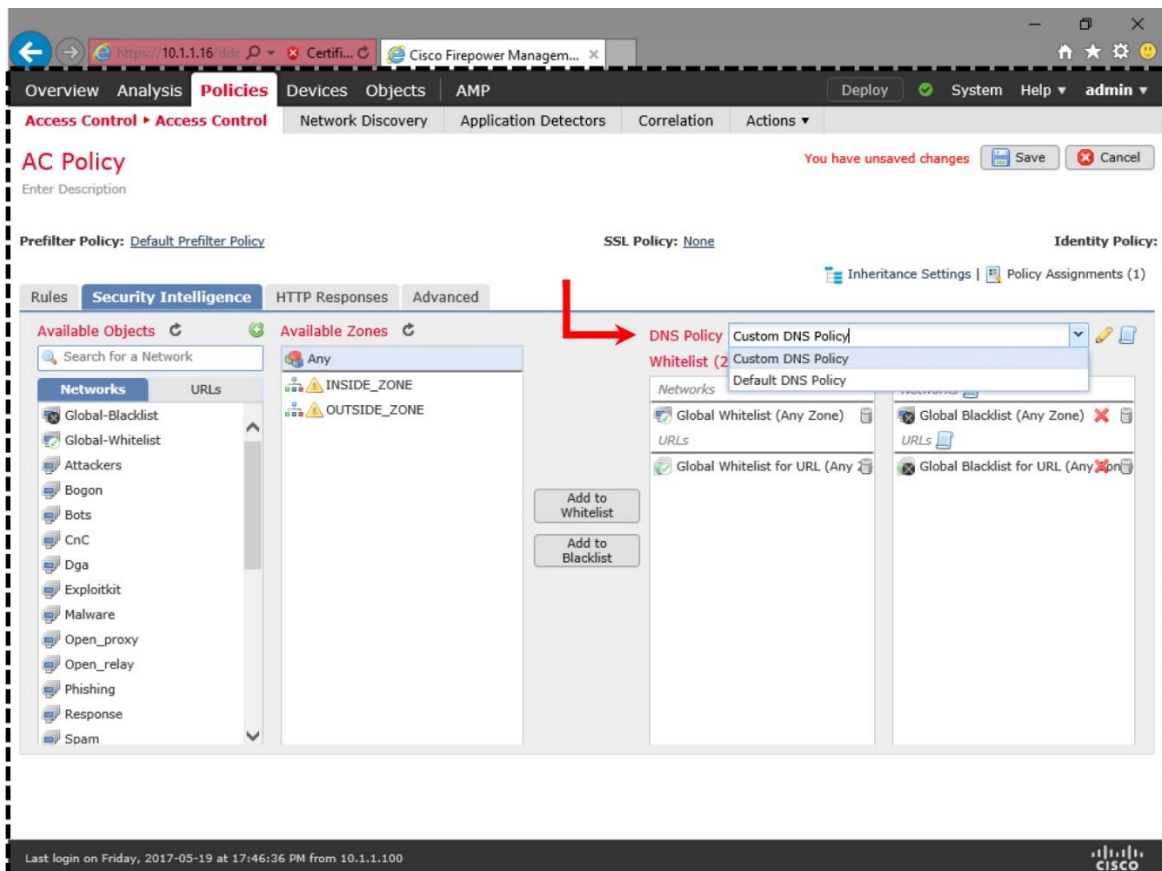


Figure 17-16. DNS Policy is Invoked within the Security Intelligence Configuration Page

Step 4. At last, save the configuration, and deploy the policy to your FTD.

Verification and Troubleshooting Tools

You can use the FTD CLI, in **expert** mode, to investigate an issue with the DNS policy configuration and inspection.

Verification of Configuration

FTD generates logs in the syslog messages file when an FMC deploys a DNS policy on it, and the FTD loads the rules into its memory. You can review any historical logs to determine any prior failure, or debug the logs in real time.

To review the old logs that are related to DNS policy, run:

```
admin@firepower:~$ sudo grep -i dns /var/log/messages
```

To debug the deployment of a DNS policy in real time, run:

```
admin@firepower:~$ sudo tail -f /var/log/messages | grep -i dns
```

[Example 17-1](#) shows confirmation that the DNS policy is allocated with a shared memory of 5 MB, and the size of the DNS blacklisting database is 4.32 MB. There are 341440 rules on this DNS policy that are loaded from 13 blacklisting categories.

Example 17-1 *Debugging Logs Related to a DNS Policy*

[Click here to view code image](#)

```
admin@firepower:~$ sudo tail -f /var/log/messages | grep -i dns
```

Password:

```
May 21 20:56:35 ciscoasa SF-IMS[4397]: [4546] SFDataCorrelator:URLUserIP_
```

```
CorrelatorThread [INFO] Writer swap dns database 2
```

```
May 21 20:56:35 ciscoasa SF-IMS[4397]: [4546] SFDataCorrelator:ShmemDB [INFO] DNS  
Blacklisting load database to segment 0 load mode 2
```

```
May 21 20:56:35 ciscoasa SF-IMS[4397]: [4546] SFDataCorrelator:ShmemDB [INFO]
```

```
loading firewall rule ID file: /var/sf/sidns_download/dns.rules
```

```
May 21 20:56:35 ciscoasa SF-IMS[4397]: [4546] SFDataCorrelator:ShmemDB [INFO]  
number
```

```
of SI category for DNS Blacklisting is 13
```

```
May 21 20:56:35 ciscoasa SF-IMS[4397]: [4546] SFDataCorrelator:ShmemDB [INFO]
```

```
reading dns/url memcap file /ngfw/etc/sf/dns_url.memcap
```

```
May 21 20:56:35 ciscoasa SF-IMS[4397]: [4546] SFDataCorrelator:ShmemDB [INFO]
```

```
Setting up shared memory memcap DNS Blacklisting 5242880
```

```
May 21 20:56:37 ciscoasa SF-IMS[4397]: [4546] SFDataCorrelator:ShmemDB [INFO]
```

```
DNS BL database size: 4532600, number of entries: 341440
```

```
May 21 20:56:37 ciscoasa SF-IMS[4397]: [4546] SFDataCorrelator:DMShmMgmt [INFO]
```

```
new database available, type:0, segment:0, path:/ngfw/var/sf/sidns_download/ dm_dns0.acl
```

```
May 21 20:56:37 ciscoasa SF-IMS[4397]: [4546] SFDataCorrelator:ShmemDB [INFO]
```

```
reading dns/url memcap file /ngfw/etc/sf/dns_url.memcap
```

```
May 21 20:56:45 ciscoasa SF-IMS[20862]: [20868] sfpreproc:DMShmMgmt [INFO]
```

successfully removed unused database /ngfw/var/sf/sidns_download/dm_dns1.acl

.
.

<Output Omitted for Brevity>

Upon a successful deployment, the DNS Security Intelligence rules are stored in the /var/sf/sidns_download directory, in list file (.lf) format. The DNS policy configuration file, dns.rules, is also located in this directory. FTD creates all these files at the time when you deploy a DNS policy. Therefore, matching the timestamp, which uses the UTC time zone, is an important indicator of whether the latest policy is deployed.

[Example 17-2](#) shows the list files that contain the blacklisted and whitelisted DNS addresses. These files are created at the same time the dns.rules file is created.

Example 17-2 *List Files (.lf) That Store the Blacklisted and Whitelisted DNS Addresses*

[Click here to view code image](#)

```
admin@firepower:~$ ls -halp /var/sf/sidns_download/
```

```
total 11M
drwxrwxr-x 5 www detection 4.0K May 21 20:58 ./
drwxr-xr-x 66 root root 4.0K Dec 12 00:19 ../
-rw-r--r-- 1 root root 400K May 21 20:56 032ba433-c295-11e4-a919-d4ae5275b77b.
lf
-rw-r--r-- 1 root root 0 May 21 20:56 17a11eb0-ff56-11e4-9081-764afb0f5dcb.
lf
-rw-r--r-- 1 root root 69 May 21 20:56 1b117672-7453-478c-be31-b72e89ca2dde.
lf
-rw-r--r-- 1 root root 0 May 21 20:56 1fca9c10-ff56-11e4-866e-ad4afb0f5dcb.
lf
-rw-r--r-- 1 root root 1.9M May 21 20:56 23f2a124-8278-4c03-8c9d-d28fe08b71ab.
lf
-rw-r--r-- 1 root root 145K May 21 20:56 2ccda18e-ddff-4f5c-af9a-f00985219707.
lf
-rw-r--r-- 1 root root 53 May 21 20:56 30f9e69c-d64c-479c-821d-0e4edab8348d.
lf
-rw-r--r-- 1 root root 8.8K May 21 20:56 3e2af68e-5fc8-4b1c-b5bc-b4e7cab5abcd.
lf
-rw-r--r-- 1 root root 52 May 21 20:56 5a0b6d6b-e2c3-436f-b4a1-48248b331d39.
lf
-rw-r--r-- 1 root root 48 May 21 20:56 5f8148f1-e5e4-427a-aa3b-ee1c2745d663.
lf
-rw-r--r-- 1 root root 187K May 21 20:56 60f4e2ab-d96c-44a0-bd38-830252b65259.
lf
-rw-r--r-- 1 root root 66 May 21 20:56 663da2e4-32f4-44d2-ad1f-8d6182720d32.
lf
-rw-r--r-- 1 root root 47 May 21 20:56 6ba968f4-7a25-4793-a2c8-7cc77f1f1074.
lf
```

```

-rw-r--r-- 1 root root    17 May 21 20:56 IPRVersion.dat
-rw-r--r-- 1 root root   20K May 21 20:56 a27c6aae-8e52-4174-a81a-47c59fecfd3a5.
If
-rw-r--r-- 1 root root  2.2M May 21 20:56 b1df3aa8-2841-4c88-8e64-bfaacec7111f.
If
-rw-r--r-- 1 root root  1.8M May 21 20:56 d7d996a6-6b92-4a56-8f10-e8506e432fb8.
If
-rw-r--r-- 1 root root    66 May 21 20:56 ded9848d-3580-4ca1-9d3c-04113549f129.If
-rw-rw-r-- 1 root root  4.4M May 21 20:57 dm_dns1.acl
-rw-r--r-- 1 root root   1.7K May 21 20:56 dns.rules
drwxr-xr-x 2 www  www    4.0K Sep 19 2016 health/
drwxr-xr-x 3 www  www    4.0K Apr 29 16:17 peers/
drwxr-xr-x 2 www  www    4.0K May 21 20:56 tmp/
admin@firepower:~$

```

After you configure a DNS policy using the GUI and deploy it on an FTD device, the FTD device writes the configurations into the dns.rules file. A dns.rules file saves the DNS rule conditions and associates the actions with the related blacklist and whitelist files. The file also records the time when the latest DNS policy is deployed.

[Example 17-3](#) explains the contents of a dns.rules file. The example elaborates the sinkhole rule as an example. The sinkhole rule (rule ID 7) matches the domain names on the 23f2a124-8278-4c03-8c9d-d28fe08b71ab.If list file (list ID 1048587). When there is a match, the rule responds to a DNS query with the sinkhole IP address 192.168.1.91.

Example 17-3 DNS Policy Configurations—View from the CLI

[Click here to view code image](#)

```
admin@firepower:~$ cat /var/sf/sidns_download/dns.rules
```

```

##### dns.rules
#####
###
#
# DNS Policy Name : Custom DNS Policy
#
# File Written   : Sun May 21 20:56:42 2017 (UTC)
#
#####
###
#
policy e5d989f8-3d01-11e7-8dc5-a7ffd42f66c2

revision e5d989f8-3d01-11e7-8dc5-a7ffd42f66c2

interface 1 e2b1d576-2cf5-11e7-8ea7-e184e4106fb3

interface 2 e295985c-2cf5-11e7-8ea7-e184e4106fb3

```

dnslist 1048594 663da2e4-32f4-44d2-ad1f-8d6182720d32.lf
dnslist 1048585 032ba433-c295-11e4-a919-d4ae5275b77b.lf
dnslist 1048599 ded9848d-3580-4ca1-9d3c-04113549f129.lf
dnslist 1048597 b1df3aa8-2841-4c88-8e64-bfaacec7111f.lf
dnslist 1048590 3e2af68e-5fc8-4b1c-b5bc-b4e7cab5abcd.lf
dnslist 1048587 23f2a124-8278-4c03-8c9d-d28fe08b71ab.lf
dnslist 1048598 d7d996a6-6b92-4a56-8f10-e8506e432fb8.lf
dnslist 1048595 6ba968f4-7a25-4793-a2c8-7cc77f1f1074.lf
dnslist 1048589 30f9e69c-d64c-479c-821d-0e4edab8348d.lf
dnslist 1048591 5a0b6d6b-e2c3-436f-b4a1-48248b331d39.lf
dnslist 1048592 5f8148f1-e5e4-427a-aa3b-ee1c2745d663.lf
dnslist 1048586 1b117672-7453-478c-be31-b72e89ca2dde.lf
dnslist 1048593 60f4e2ab-d96c-44a0-bd38-830252b65259.lf
sinkhole 1 7e550616-3e61-11e7-a338-d8a9a7208ff6 192.168.1.91 ::1

1 allow any any any 1048594

3 nxdomain any any any 1048599

5 nxdomain any any any 1048591

5 nxdomain any any any 1048592

5 nxdomain any any any 1048595

5 nxdomain any any any 1048593

6 block any any any 1048597

6 block any any any 1048586

6 block any any any 1048589

7 sinkhole any any any 1048587 (sinkhole: 1)

8 monitor any any any 1048598

8 monitor any any any 1048585

8 monitor any any any 1048590

admin@firepower:~\$

To determine the category of domains that are listed in an .lf file, view the first line of the file. For example, the following command confirms that the file 23f2a124-8278-4c03-8c9d-d28fe08b71ab.lf (DNS list ID 1048587) lists all the domains that are susceptible for malware:

[Click here to view code image](#)

admin@firepower:~\$ **head -n1 /var/sf/sidns_download/23f2a124-8278-4c03-8c9d-d28fe08b71ab.lf**

#Cisco DNS and URL intelligence feed: DNS Malware

admin@firepower:~\$

[Figure 17-17](#) shows some of the contents in a dns.rules file on the GUI—accessible from the DNS policy configuration editor. The example highlights the rule that enables the sinkhole action.

dnslist 1048587 23f2a124-8278-4c03-8c9d-d28fe08b71ab.lf

#	Name	Source Zones	Source Networks	VLAN Tags	DNS Lists	Action
Whitelist						
1	Global Whitelist for DNS	any	any	any	Global-Whitelist-for-DNS	Whitelist
Blacklist						
2	Global Blacklist for DNS	any	any	any	Global-Blacklist-for-DNS	Domain Not Found
3	Custom DNS Rule 1	any	any	any	DNS Attackers DNS Bogon DNS Bots DNS CrC	Domain Not Found
4	Custom DNS Rule 2	any	any	any	DNS Dga DNS Exploitkit DNS Open_proxy DNS Open_relay	Drop
5	Custom DNS Rule 3	any	any	any	DNS Malware	Sinkhole
6	Custom DNS Rule 4	any	any	any	DNS Phishing DNS Response DNS Spam DNS Suspicious	Monitor

7 sinkhole any any any 1048587 (sinkhole: 1)

Figure 17-17 DNS Policy Configurations—View from the GUI

Verifying the Operation of a DNS Policy

To verify the operation of a DNS policy and inspection of a DNS query, you need to access a domain that is blocked by the current DNS policy. To help you better understand this, this chapter uses three different websites that can trigger the Security Intelligence events for three different categories.

Warning

If your computer is connected to the Internet, you should not attempt to access a malicious website until an FTD device is actively protecting your network.

The status of categorization or inclusion of a domain may vary in different versions of a feed. If you want to determine the inclusion of any particular domain in the current Cisco Intelligence Feed, search that particular domain within all the list files. The following command can perform that search:

[Click here to view code image](#)

```
admin@firepower:~$ grep [domain_name] /var/sf/sidns_download/*.lf
```

[Example 17-4](#) shows the DNS intelligence category for the domains that you will be testing next.

Example 17-4 Identifying the DNS Intelligence Category for Certain Domains

[Click here to view code image](#)

```
admin@firepower:~$ egrep iolmau.com /var/sf/sidns_download/*.lf
```

```
/var/sf/sidns_download/23f2a124-8278-4c03-8c9d-d28fe08b71ab.lf:iolmau.com
```

```
admin@firepower:~$ head -n1 /var/sf/sidns_download/23f2a124-8278-4c03-8c9d-
```

```
d28fe08b71ab.lf
```

```
#Cisco DNS and URL intelligence feed: DNS Malware
```

```
admin@firepower:~$
```

```
admin@firepower:~$ egrep mrreacher.net /var/sf/sidns_download/*.lf
```

```
/var/sf/sidns_download/60f4e2ab-d96c-44a0-bd38-830252b65259.lf:mrreacher.net
```

```
admin@firepower:~$ head -n1 /var/sf/sidns_download/60f4e2ab-d96c-44a0-bd38-
```

```
830252b65259.lf
```

```
#Cisco DNS and URL intelligence feed: DNS CnC
```

```
admin@firepower:~$
```

```
admin@firepower:~$ egrep rent.sinstr.ru /var/sf/sidns_download/*.lf
```

```
/var/sf/sidns_download/d7d996a6-6b92-4a56-8f10-e8506e432fb8.lf:rent.sinstr.ru
```

```
admin@firepower:~$
```

```
admin@firepower:~$ head -n1 /var/sf/sidns_download/d7d996a6-6b92-4a56-8f10-
```

```
e8506e432fb8.lf
```

```
#Cisco DNS and URL intelligence feed: DNS Phishing
```

```
admin@firepower:~$
```

[Table 17-2](#) summarizes the domains that you will query from a client computer to test the DNS policy operation. As of writing this book, they are available in the current revision of the Cisco Intelligence Feed and added in the DNS rule.

Table 17-2 *Selection of Domains from Three Different Intelligence Categories (for Lab Test)*

Domain Name	DNS/Security Intelligence Category	DNS Rule Action
iolmau.com	Malware	Sinkhole
mrreacher.net	Command and control (CnC)	Domain not found
rent.sinstr.ru	Phishing	Monitor

Before you begin testing, enable the **firewall-engine-debug** command on the FTD CLI so that FTD device generates debug output while a client performs a DNS query. The following

pages show you how to access the selected domains one by one from a client computer in your inside network.

Tip

Depending on the placement of your FTD device, the DNS-based Security Intelligence may not begin to function if the existing cache of your DNS server is not cleared. Therefore, before you begin an investigation, wait until the existing cache expires or manually delete the cache entries from your DNS server. Read the “DNS Query Blocking Best Practices” section of this chapter for more information.

[Example 17-5](#) shows the debugging messages that are generated by the **firewall-debug-engine** tool on the FTD device. Each time a domain name is queried by the host 192.168.1.2, FTD matches the domain with the names on the list files. When there is a match, FTD triggers the action configured on the matching DNS rule.

Example 17-5 Debugging the DNS Queries Through an FTD Device

[Click here to view code image](#)

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol:
```

```
Please specify a client IP address: 192.168.1.2
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 DNS SI shared mem lookup returned 1
for iolmau.com
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 Starting SrcZone first with intfs -1
-> 0, vlan 0
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 1, id 1 action Allow
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 2, id 3 action DNS
NXDomain
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 3, id 5 action DNS
NXDomain
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 4, id 6 action Block
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 5, id 7 action DNS
Sinkhole
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 Got DNS list match. si list 1048587
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 6, id 8 action Audit
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 Firing DNS action DNS Sinkhole
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 DNS SI: Matched rule order 5, Id 7,
si list id 1048587, action 23, reason 2048, SI Categories 1048587,0
```

192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 DNS SI shared mem lookup returned 1 for **mrreacher.net**
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 Starting SrcZone first with intfs -1 -> 0, vlan 0
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 1, id 1 action Allow
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 2, id 3 action DNS NXDomain
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 3, id 5 action DNS NXDomain
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 **Got DNS list match. si list 1048593**
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 4, id 6 action Block
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 5, id 7 action DNS Sinkhole
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 6, id 8 action Audit
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 **Firing DNS action DNS NXDomain**
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 DNS SI: Matched rule order 3, Id 5, si list id 1048593, action 22, reason 2048, SI Categories 1048593,0

192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 DNS SI shared mem lookup returned 1 for **rent.sinstr.ru**
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 Starting SrcZone first with intfs -1 -> 0, vlan 0
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 1, id 1 action Allow
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 2, id 3 action DNS NXDomain
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 3, id 5 action DNS NXDomain
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 4, id 6 action Block
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 5, id 7 action DNS Sinkhole
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 6, id 8 action Audit
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 **Got DNS list match. si list 1048598**
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 **Firing DNS action Audit**
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 DNS SI: Matched rule order 6, Id 8, si list id 1048598, action 6, reason 4096, SI Categories 1048598,0

Now, for the three DNS queries in [Example 17-5](#), the FMC should log events. You can view them on the **Analysis > Connections > Security Intelligence Events** page.

Figure 17-18 shows three types of DNS-based Security Intelligence actions. FTD triggered these events when a client attempted to access three different matching websites.

First Packet	Action	Reason	Initiator IP	Security Intelligence Category	Destination Port / ICMP Code	DNS Query	DNS Response
2017-05-21 20:32:20	Allow	DNS Monitor	192.168.1.2	DNS Phishing	53 (domain) / udp	rent.sinstr.ru	NoError
2017-05-21 19:48:59	Domain Not Found	DNS Block	192.168.1.2	DNS CnC	53 (domain) / udp	mrreacher.net	NXDOMAIN
2017-05-21 19:44:16	Sinkhole	DNS Block	192.168.1.2	DNS Malware	53 (domain) / udp	iolmau.com	SINKHOLE

Actions You Enabled Within Each DNS Rule
Categories You Added to a Rule
Client and Server Communication

Figure 17-18 Security Intelligence Event Page Showing Events Triggered by DNS Rules

You can also use the **nslookup** command-line tool to resolve a domain name to its IP address. The tool is available on both Windows and Linux operating systems. It allows you to view the IP address of a domain without accessing the web contents.

Example 17-6 shows the resolutions of the same domain names used in the previous examples from a network host. The client uses the **nslookup** command-line tool and receives three different types of results.

Example 17-6 Resolving Domain Names by Using the **nslookup** Command

[Click here to view code image](#)

! The following answer demonstrates the "Sinkhole" action. It responses with IP address 192.168.1.91, which is a non-authoritative spoof DNS server.

```
Users@Linux:~$ nslookup iolmau.com
Server:      127.0.1.1
Address:    127.0.1.1#53
```

Non-authoritative answer:

```
Name: iolmau.com
Address: 192.168.1.91
Users@Linux:~$
```

! The following answer reflects the "Domain Not Found" action. The DNS query fails with NXDOMAIN message, which means the domain appears to be non-existent.

```
Users@Linux:~$ nslookup mrreacher.net
Server:      127.0.1.1
Address:     127.0.1.1#53
```

```
** server can't find mrreacher.net: NXDOMAIN
Users@Linux:~$
```

! The following answer reflects the "Monitor" action. The DNS query is able to resolve the domain name. It shows the public IP address for the domain.

```
Users@Linux:~$ nslookup rent.sinstr.ru
Server:      127.0.1.1
Address:     127.0.1.1#53
```

```
Name:  rent.sinstr.ru
Address: 81.222.82.37
Users@Linux:~$
```

Summary

This chapter describes various techniques for administering DNS queries using a Firepower DNS policy. Besides using a traditional access control rule, an FTD device can incorporate Cisco Intelligence Feed and dynamically blacklist suspicious domains. In this chapter, you have learned various ways to configure and deploy a DNS policy. This chapter also demonstrates several command-line tools you can run to verify, analyze, and troubleshoot issues with DNS policy.

Quiz

1. Which of the following actions does not interrupt traffic flow immediately?
 - a. Domain Not Found
 - b. Whitelist
 - c. Blacklist
 - d. Monitor
2. Which of the following directories stores the files related to a DNS policy?
 - a. /var/sf/sidns_intelligence
 - b. /var/sf/sidns_download
 - c. /var/log/sidns_policy
 - d. /var/log/sidns_list

3. Which of the following statements is incorrect?

- a. Sinkhole configuration requires a unique type of sinkhole object.
- b. DNS policy requires a Threat license.
- c. FTD downloads the latest Cisco Intelligence Feed directly from the cloud.
- d. The FMC supports the blacklisting of custom domain lists.

4. Which of the following actions sends an address of a spoof DNS server?

- a. Domain Not Found
- b. Sinkhole
- c. Monitor
- d. Drop

Chapter 18

Filtering URLs Based on Category, Risk, and Reputation

New websites are coming out every day. A security analyst strives to determine the relevance of a new website for business operations and its risk level for security reasons. However, it is challenging to catch up with the exponentially growing number of new websites every day. In this chapter, you will learn how Firepower can empower you with automatic classification of millions of websites using the Web Reputation technology.

URL Filtering Essentials

The URL Filtering feature of a Firepower system is able to categorize millions of URLs and domains. You can enable this feature to prevent your network hosts from accessing a specific type of URL. This feature empowers you to enforce the IT security and legal policies of your organization dynamically—without continually making manual changes to the access rule conditions.

Reputation Index

You can download the Firepower URL database from the cloud by using the FMC GUI. As of this writing, the cloud has analyzed more than 600 million domains and more than 27 billion URLs and categorized them into more than 83 different classes. The analysis engine in the cloud can categorize more than 2500 URLs per second. The URL database maintains the Web Reputation Index (WRI), which is based on many different data points, such as age and history of the site, reputation and location of the hosting IP address, subject and context of the content, and so on.

[Table 18-1](#) shows the WRI descriptions. WRI is calculated dynamically based on collective intelligence from various sources.

Table 18-1 *Web Reputation Index Used in a URL Database*

Reputation Level	Index	Description
1. High risk	01–20	Sites are at high risk. Known for exposure to malicious data.
2. Suspicious	21–40	Sites are suspicious. Threat level is higher than average.
3. Moderate risk	41–60	Benign sites but exposed to some unsafe characteristics.
4. Low risk	61–80	Benign sites but showed risks once or twice—though very rarely.
5. Trustworthy	81–100	Well-known sites with very strong security features.

Figure 18-1 shows the implementation of URL categories and reputations in the FMC web interface.

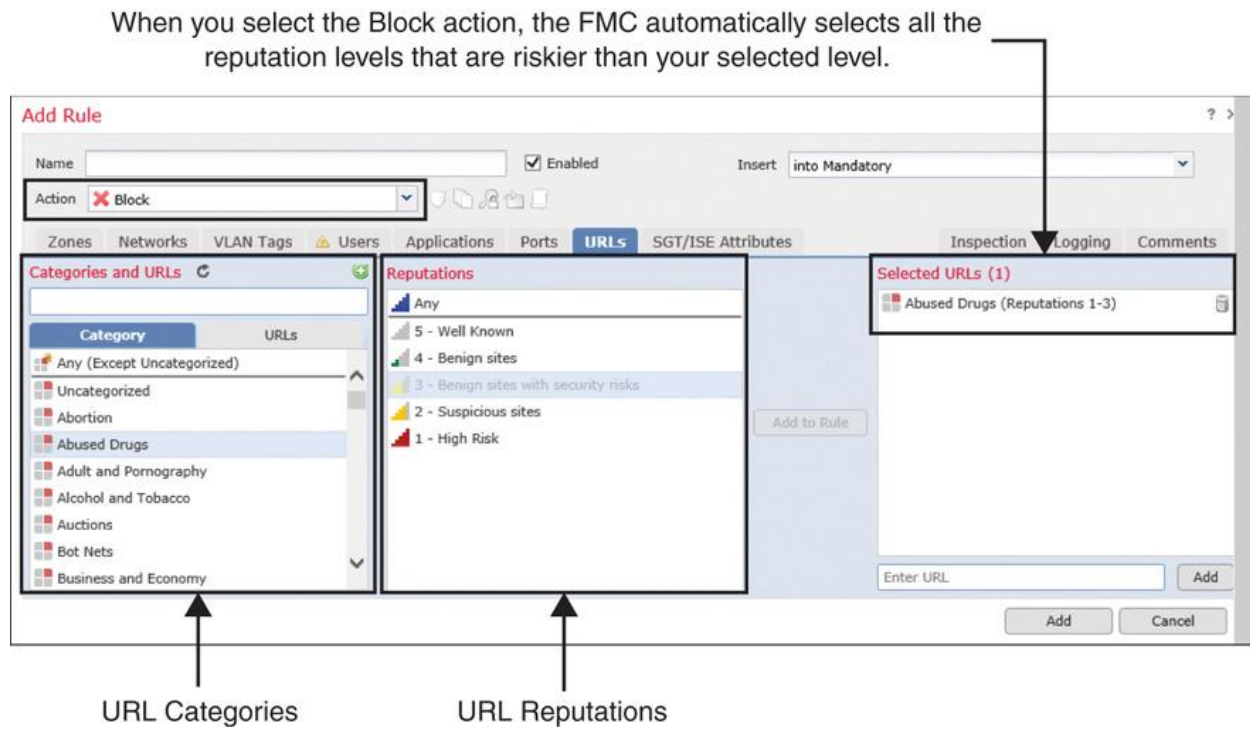


Figure 18-1 URL Categories and Reputations in the Access Rule Editor

Based on the type of action—Allow or Block—you select for an access rule, the FMC automatically adds extra URL reputation levels along with your original selection. For example, when you select the Allow action for a certain reputation level, the FMC allows all the URLs of that level as well as the URLs that are more benign than your selected level. Likewise, if you select the Block action for a particular reputation level, FMC blocks all the URLs of that level along with any URLs that are riskier than the level you selected.

[Figure 18-2](#) shows different behaviors between the Allow and Block actions. Compare this image with [Figure 18-1](#). Note that both show the same reputation level selected (3 - Benign sites with security risks), but the ultimate reputation selections are different due to the actions—Allow versus Block.

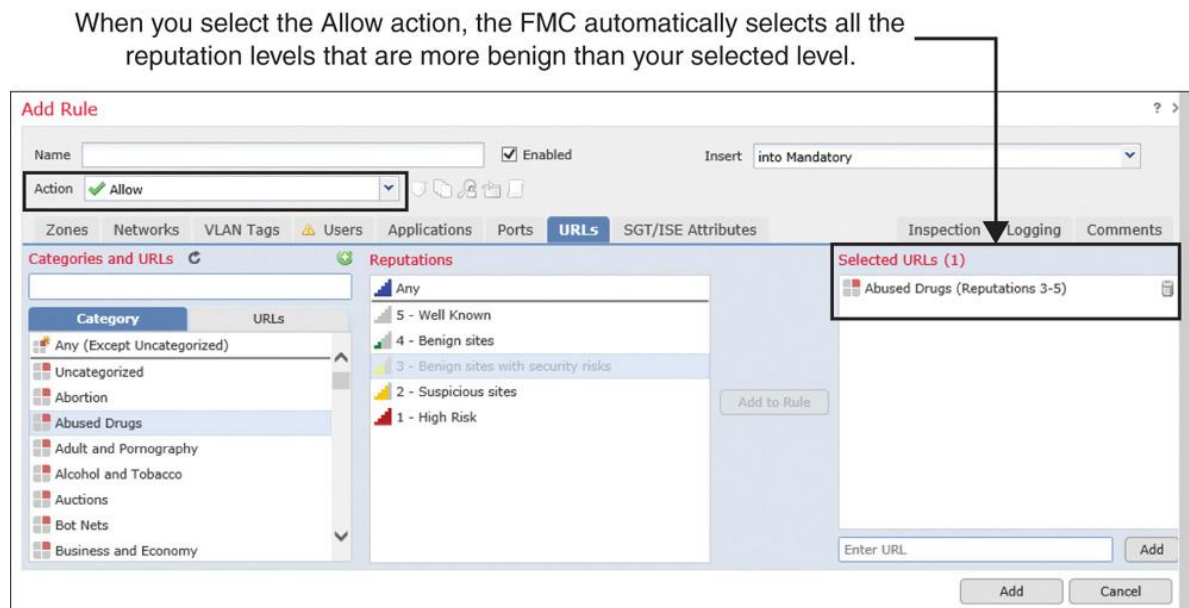


Figure 18-2 FMC Selecting Extra URL Reputations—Depending on the Selected Action

Operational Architecture

The Firepower system loads the URL dataset into its memory for a faster lookup. Depending on the size of available memory on a Firepower system, the cloud publishes two types of datasets in a URL database—20 million URLs and 1 million URLs. After the initial download of a database, the FMC receives updates from the cloud periodically, as long as the automatic update is enabled. The periodic updates are incremental and smaller. However, the total download time depends on the last URL database installed on the FMC and, of course, the download speed.

[Table 18-2](#) shows that the number of URLs included in a database depends on the available memory on a Firepower system.

Table 18-2 Available Memory Versus the Number of URLs in a Dataset

Available Memory	Number of URLs in the Dataset
More than 3.4 GB	20 million URLs
Less than or equal to 3.4 GB	1 million URLs

During traffic inspection, an FTD device can resolve most of the URLs the first time it sees them. However, depending on other factors, an FTD device might have to go through multiple steps to resolve a URL by category and reputation. Here are some steps, for example:

Step 1. The Firepower Snort engine on an FTD device performs an immediate lookup on the local URL dataset. FTD is able to determine the category in most cases. If the URL is unavailable in the FTD cache, FTD forwards the query to the FMC.

Step 2. If the FMC can retrieve the URL category from its local database, it sends the query result to the FTD device so that FTD can act on traffic according to the access control policy. [Figure 18-3](#) shows the steps to resolve an unknown new URL into its category and reputation.

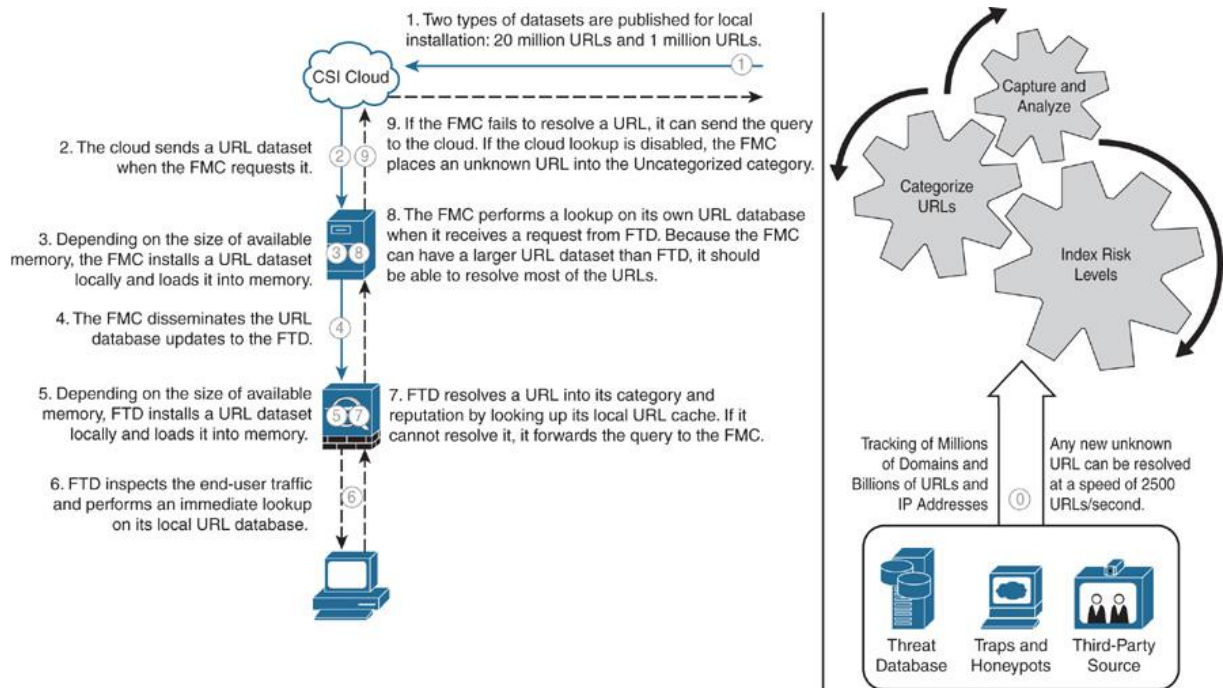


Figure 18-3 Architecture of the Firepower System URL Lookup

Step 3. If the FMC is unable to resolve the URL category from its local database, it checks the Cisco Collective Security Intelligence (CSI) configuration:

- If the query to the CSI is disabled, the FMC places the unknown URL into the Uncategorized group.
- If the query to the CSI is enabled, the FMC queries the cloud for the unknown URL.

Fulfilling Prerequisites

Before you begin configuring an access rule with URL Filtering conditions, fulfill the following requirements:

- A URL Filtering license is necessary to use the URL classification and reputation database of a Firepower system. Furthermore, as a prerequisite, the FMC requires you to enable a Threat license before you enable URL Filtering.
-

[Figure 18-4](#) shows the page where you can enable or disable any license for an FTD device. To find this page, navigate to **Devices > Device Management**. Edit the device where you want to enable URL Filtering license and then select the **Devices** tab.

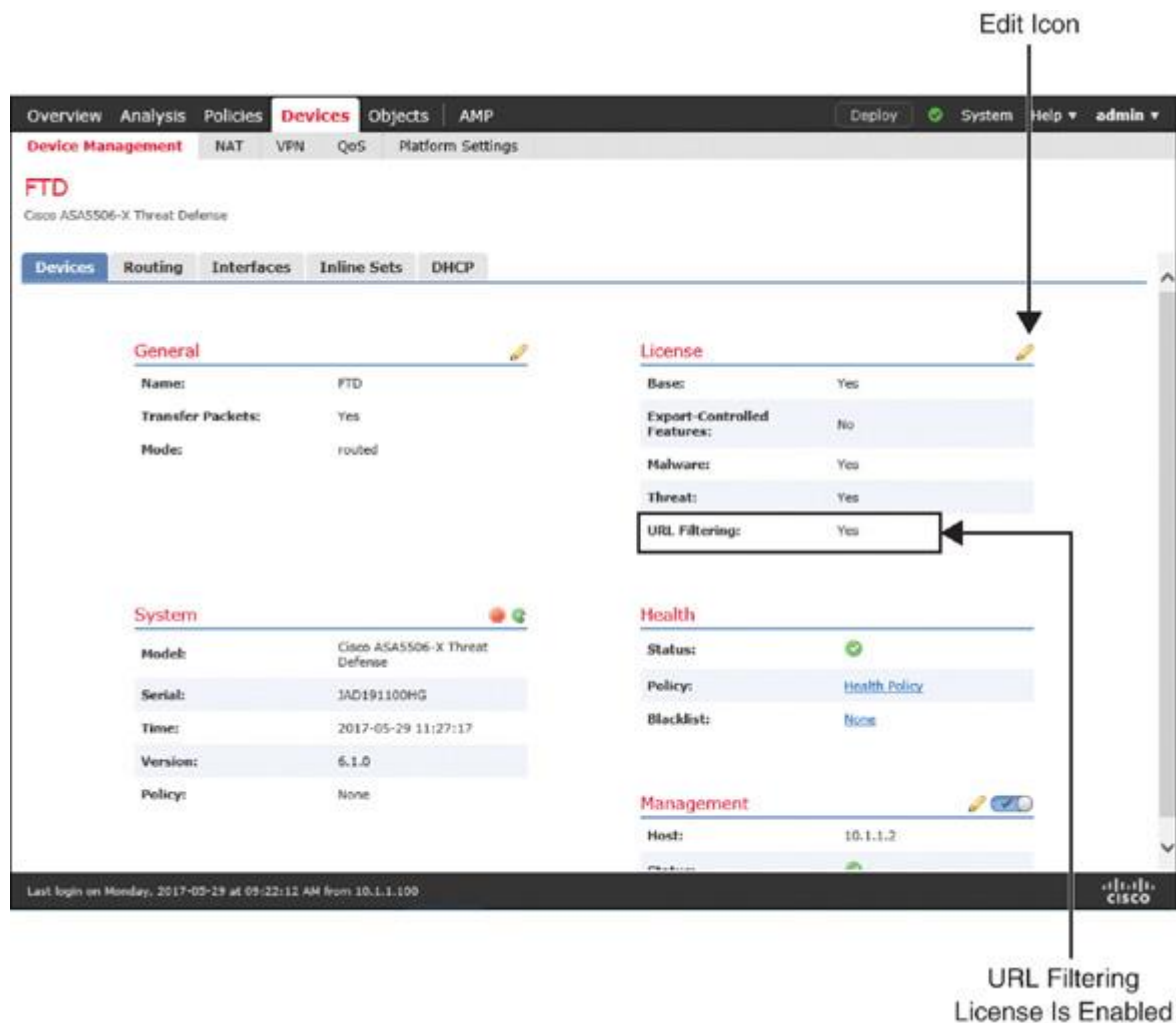


Figure 18-4 Enabling the URL Filtering License on an FTD Device

Without a URL Filtering license, you can create an access rule based on any URL conditions; however, you cannot deploy an access control policy with the URL conditions until you enable a URL Filtering license on your FTD device. Similarly, if the URL license expires after you deploy an access control policy, FTD stops matching any access rule with URL conditions, and the FMC stops updating the URL database.

Tip

If you are in the process of purchasing a license, you can enable Evaluation Mode to avoid any administrative delays. Evaluation Mode allows you to configure and deploy any features as if you have already enabled a paid license.

■ Make sure the URL Filtering and Cisco CSI communication are enabled. The FMC should enable them automatically after you add a valid URL Filtering license. [Figure 18-5](#) confirms that URL Filtering and automatic updating of the URL database have been enabled.

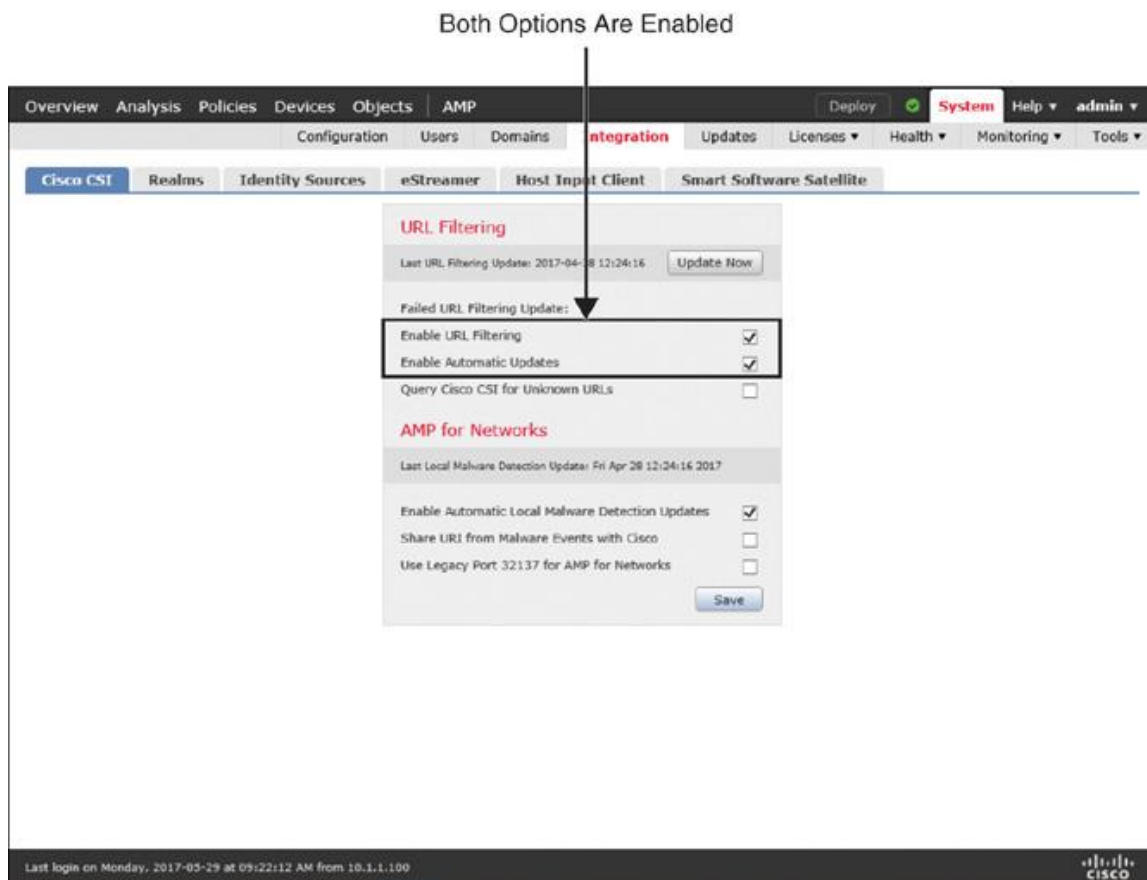


Figure 18-5 Enabling URL Filtering and Automatic Updating

Best Practices for URL Filtering Configuration

Consider the following best practices when enabling the URL Filtering feature in Firepower:

■ Check whether the URL Filtering Monitor health module is enabled in the current health policy. If this module is enabled, the FMC generates alerts if it fails to deploy a URL dataset to the managed devices or fails to download the latest URL database from the Cisco CSI.

[Figure 18-6](#) shows the option to enable the health module for URL Filtering. To find this page, go to **System > Health > Policy**, edit a health policy, and select **URL Filtering Monitor** from the left panel. You must redeploy a health policy after you change any settings.

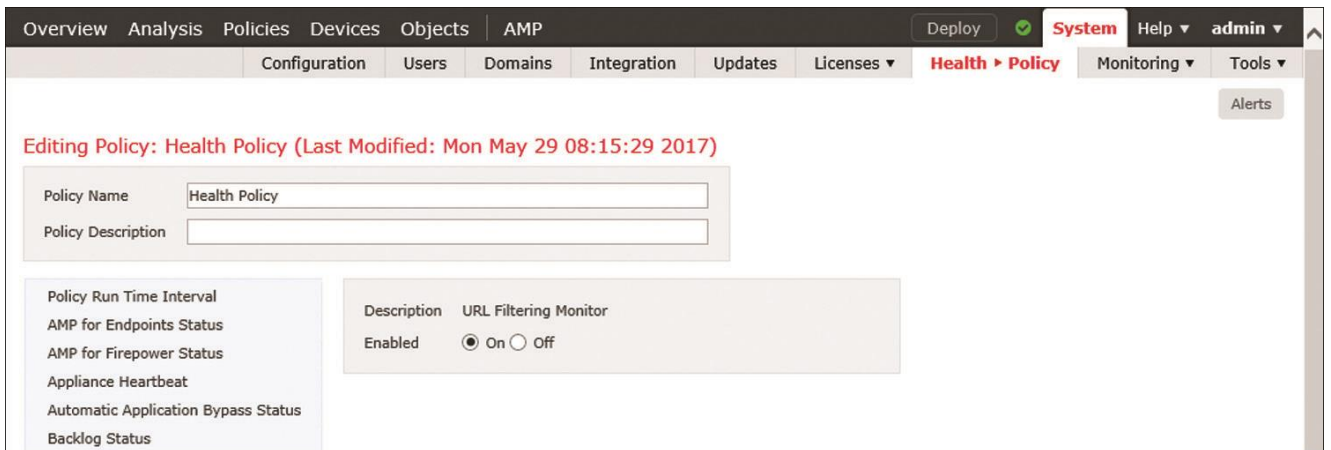


Figure 18-6 Health Module for URL Filtering Monitor

■ The FMC communicates with Cisco CSI every 30 minutes to determine if a new update for the URL Filtering database is available. Therefore, if the automatic update option is enabled, you should not create a separate scheduled task for URL database updates. However, a recurring scheduled task for URL database updates is useful if you want to manage the URL database update manually.

[Figure 18-7](#) shows the options to create a scheduled task for URL database updates. In this configuration, the FMC updates the URL Filtering database daily at 5 a.m., as opposed to the system default of every 30 minutes.

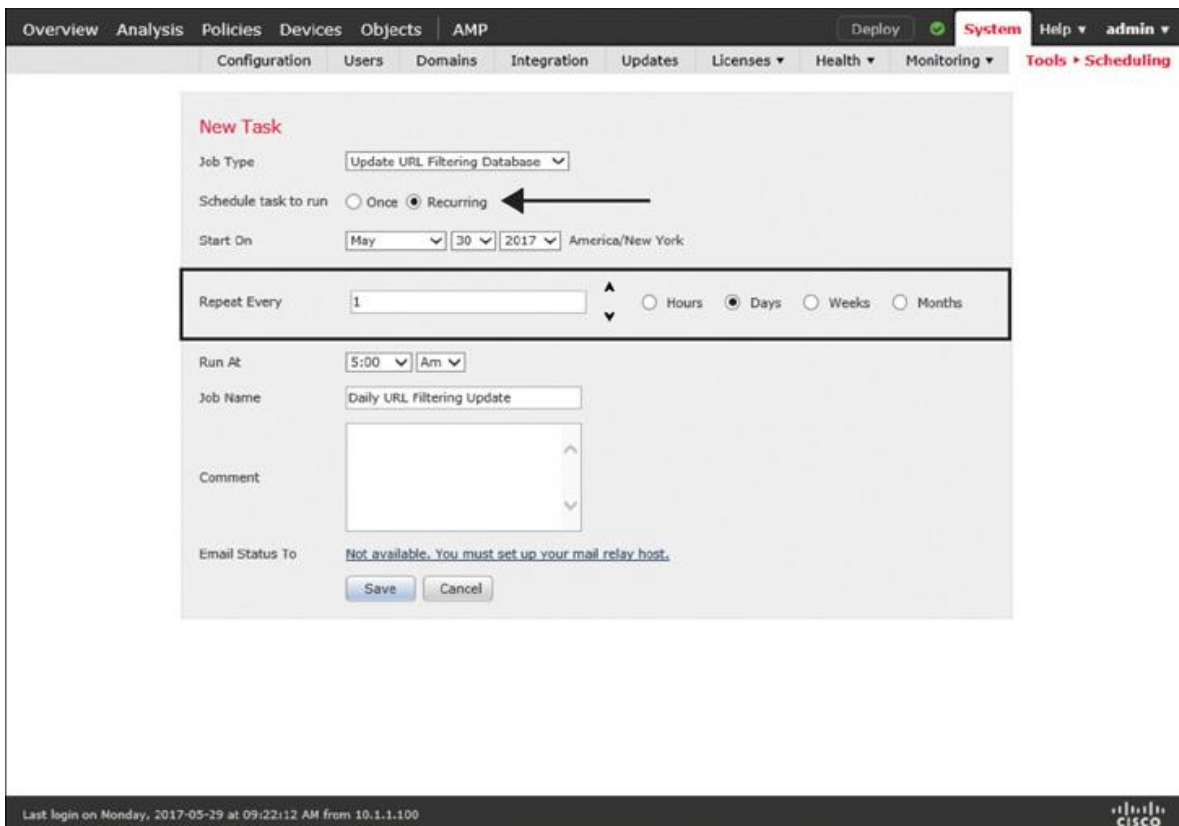


Figure 18-7 Scheduling a Recurring Task to Update the URL Filtering Database

■ To prevent access to any suspicious websites, you can consider blocking the DNS queries to those domains. If an FTD device can block a connection during DNS resolution, a URL lookup for that connection will no longer be necessary. Hence, it can improve system performance.

Figure 18-8 highlights the positions of the Firepower engine components. The URL-based Security Intelligence (DNS policy) can block a packet *before* it is categorized and blocked by a URL Filtering rule.

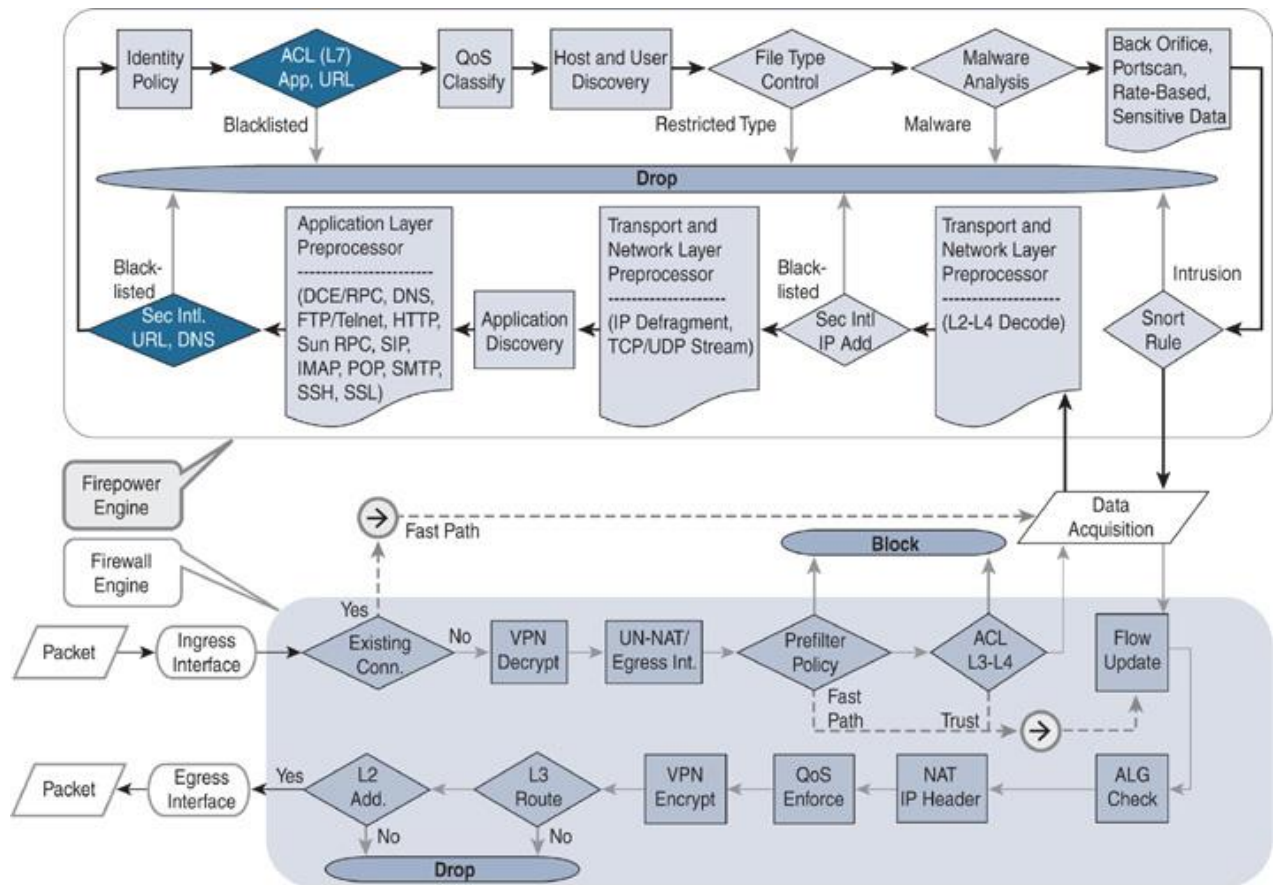


Figure 18-8 Workflow of URL Filtering Within a Firepower Engine

Blocking URLs of a Certain Category

You can block undesired URLs based on their categories and reputations. You can accomplish this by enabling an access rule with URL Filtering conditions.

Configuring an Access Rule for URL Filtering

The following steps describe how to add an access rule to block certain URL categories:

Step 1. Navigate to **Policies > Access Control > Access Control** and select an existing access control policy to edit or create a new one.

Step 2. On the access control policy editor page, click the **Add Rule** button. The Add Rule window appears.

Step 3. Give a name to the access rule and select an action for the rule.

Step 4. Click the **URLs** tab. A list of URL categories and reputations appear. Select the categories and reputations you want to block and add them to the rule.

[Figure 18-9](#) shows the creation of an access rule with a URL Filtering condition. The rule blocks all the URLs that are related to the Job Search category.

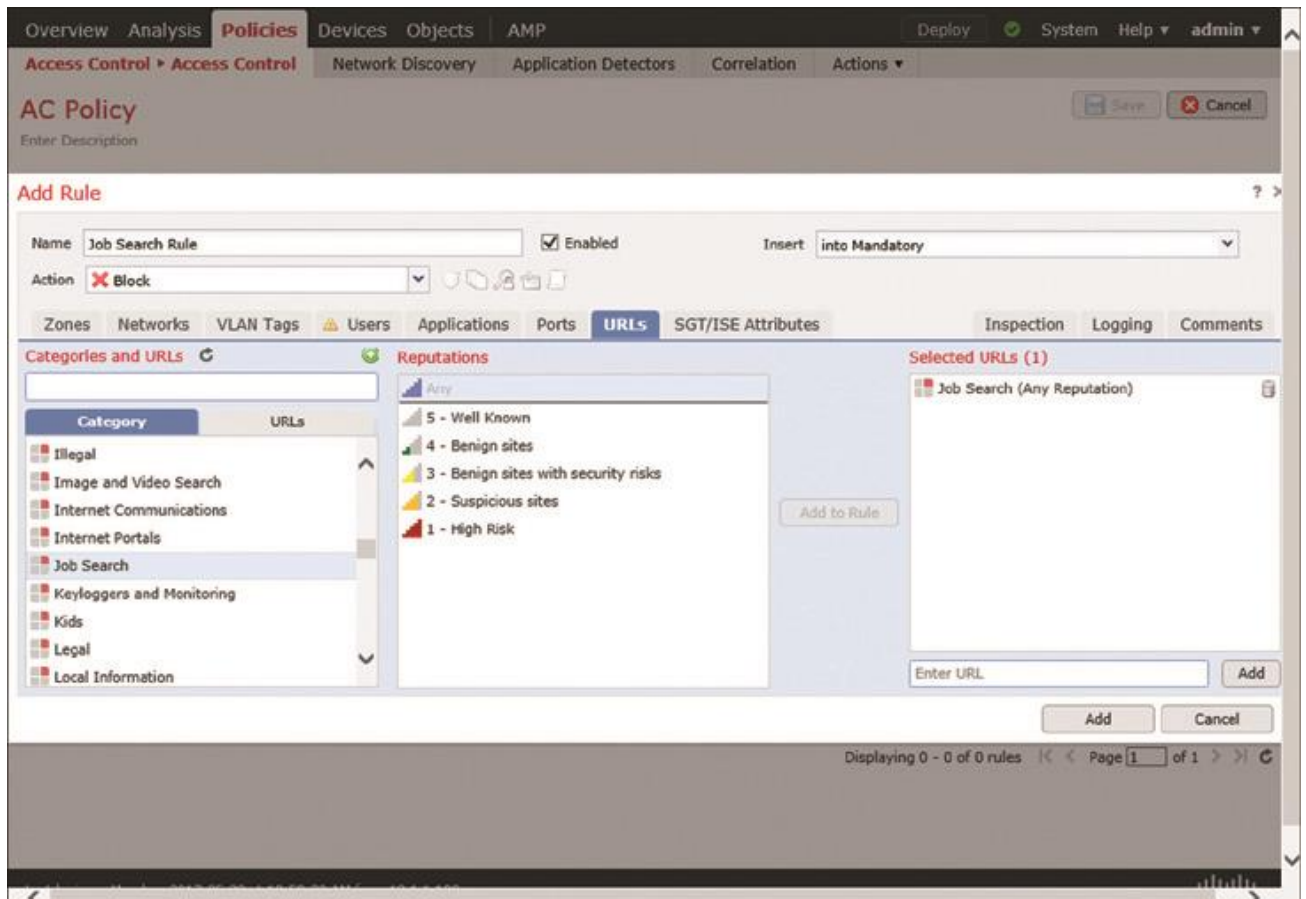


Figure 18-9 *Selecting a URL Category for Any Reputation Levels*

Step 5. On the Logging tab, enable Log at Beginning of Connection. This step is optional, but it allows you to view events when FTD blocks a connection due to a URL Filtering condition.

[Figure 18-10](#) shows how to enable logging at the beginning of a connection. Once this is enabled, FTD generates a connection event whenever it blocks a URL in the Job Search category.

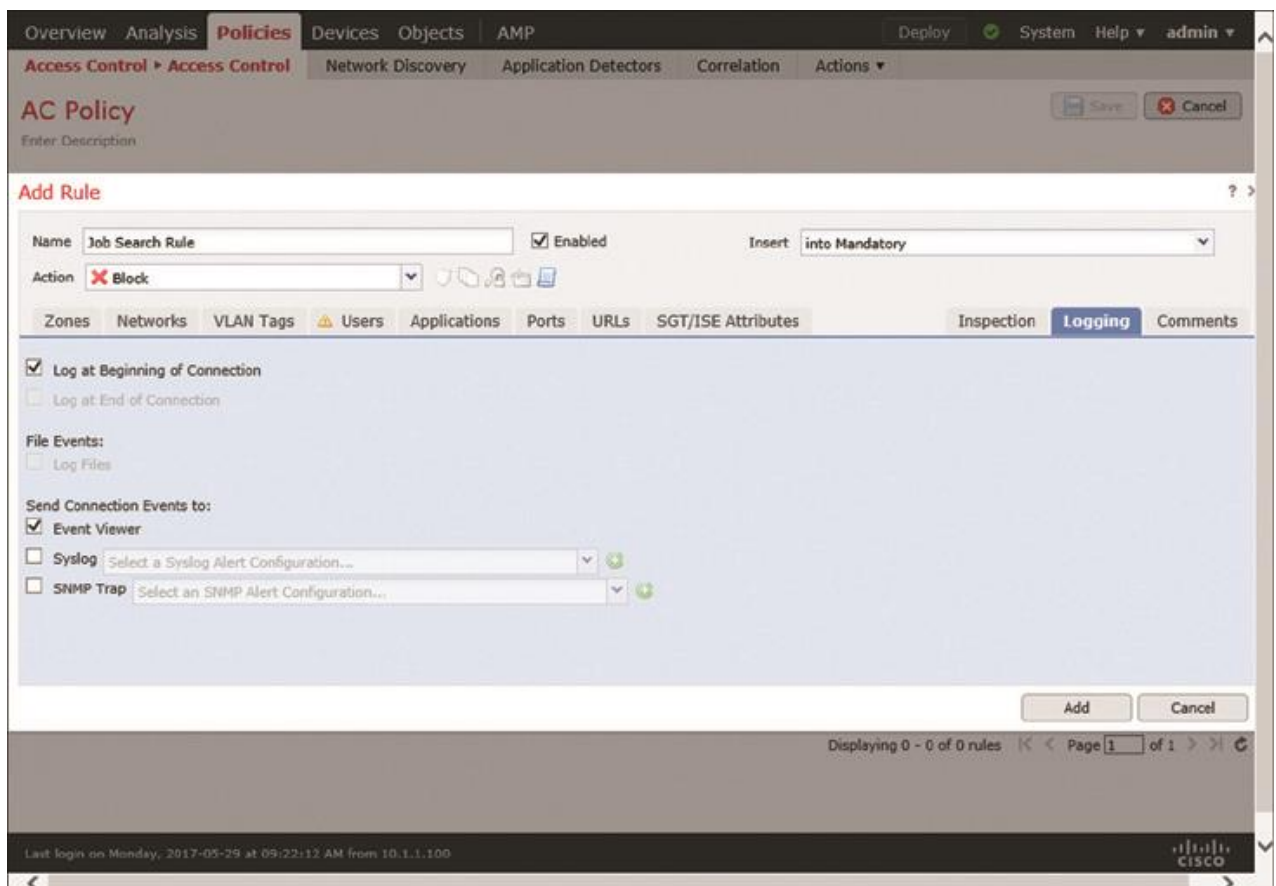


Figure 18-10 *Enabling Logging for an Access Rule with a URL Filtering Condition*

Step 6. Click the **Add** button to create the access rule.

Step 7. Click **Save** to save the changes on the access control policy. Finally, activate the policy by clicking the **Deploy** button.

[Figure 18-11](#) shows the creation of a simple access rule called Job Search Rule. This rule blocks any URLs that are within the Job Search category.

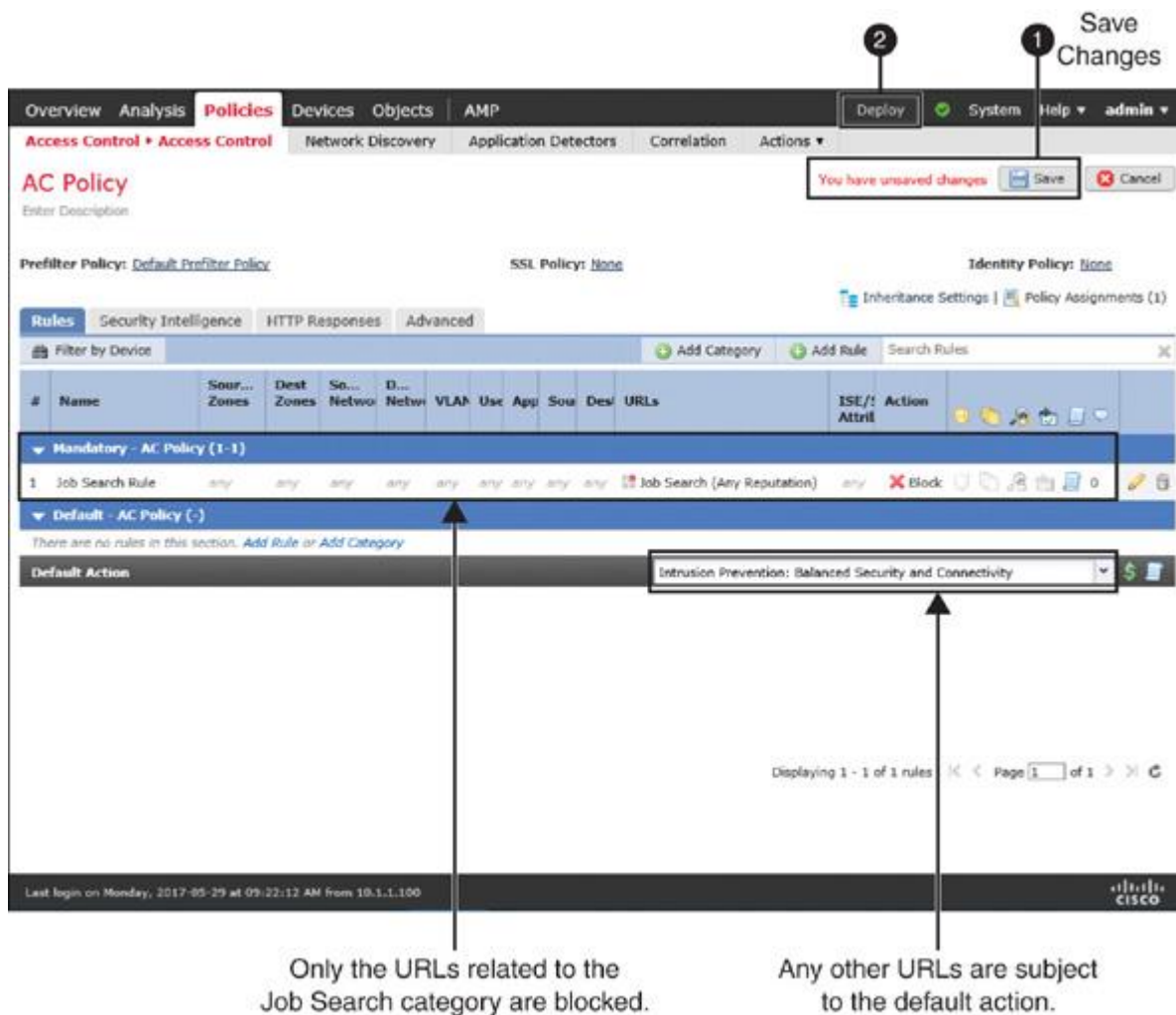


Figure 18-11 Viewing a Simple URL Filtering Rule on the Access Control Policy Editor

Verification and Troubleshooting Tools

To verify the actions of the access rule that you created in the previous section, select two URLs—one URL from the matching category, such as Job Search, and the other URL from any nonmatching category. If an access rule with a URL condition is operational, it only blocks the Job Search–related URLs, while the default action allows any other URL categories.

Attempt to visit the following websites and notice the result in each case:

- google.com (a general search engine)
- careerbuilder.com (a job search engine)
- dice.com (a job search engine)

[Figure 18-12](#) shows the blocking of both job search engines, dice.com and careerbuilder.com. However, because of the default action, FTD does not block the general search engine google.com.

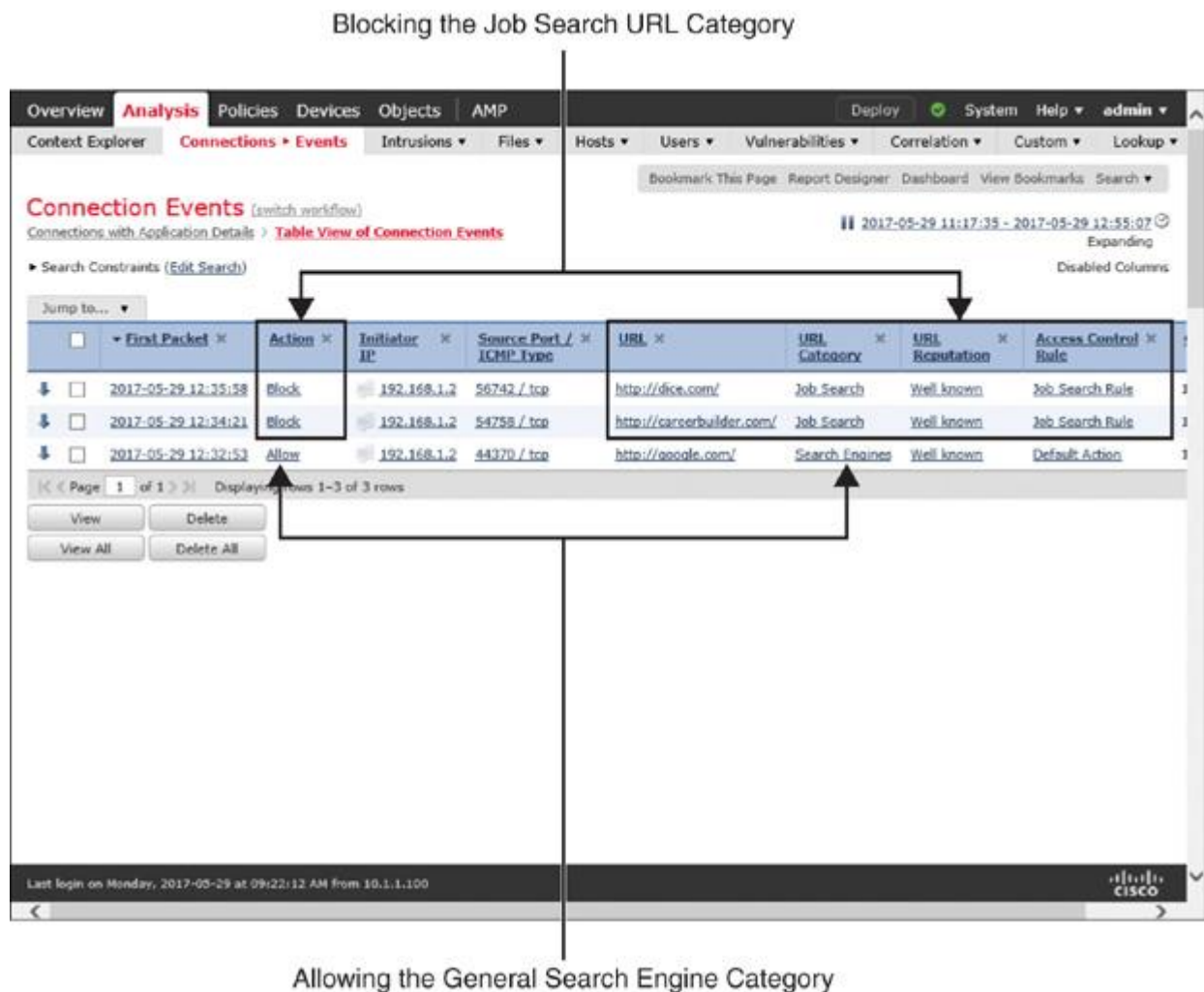


Figure 18-12 Access Rule with URL Filtering Conditions Blocking Desired Connections

You can also debug the actions in an FTD device and analyze the **firewall-engine-debug** messages for troubleshooting purposes.

[Example 18-1](#) shows the **firewall-engine-debug** messages when FTD allows you access to a general search engine, such as google.com. The debug message shows that FTD can perform a URL lookup successfully, but the URL itself does not match with a URL Filtering condition. The default action allows the URL.

Example 18-1 Debug Messages by an Access Rule with a URL Condition (Action: Allow)

[Click here to view code image](#)

> **system support firewall-engine-debug**

Please specify an IP protocol:

Please specify a client IP address: **192.168.1.2**

Please specify a client port:

Please specify a server IP address:

Please specify a server port:

Monitoring firewall engine debug messages

192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 New session

192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 Starting with minimum 2, 'Job Search

Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:

untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff

192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 pending rule order 2, 'Job Search

Rule', URL

192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 Starting with minimum 2, 'Job Search

Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:

untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff

192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 pending rule order 2, 'Job Search

Rule', URL

192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 Starting with minimum 2, 'Job Search

Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:

untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff

192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 pending rule order 2, 'Job Search

Rule', URL

192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 URL SI:

ShmDBLookupURL("http://google.com/") returned 0

192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 Starting with minimum 2, 'Job Search

Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:

untagged, svc 676, payload 184, client 638, misc 0, user 9999997, url

http://google.com/, xff

192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1: DataMessaging_GetURLData:
Returning

URL_BCTYPE for google.com

192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 rule order 2, 'Job Search Rule', URL

Lookup Success: http://google.com/ waited: 0ms

192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 no match rule order 2, 'Job Search

Rule', url=(http://google.com/) c=50 r=81

192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 match rule order 3, id 268435458

action Allow

192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 allow action

192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 Deleting session

[Example 18-2](#) shows the **firewall-engine-debug** messages when FTD denies you access to a job search engine, such as dice.com. The debug message confirms that FTD is able to perform a URL lookup successfully, but the URL itself is blocked due to a matching condition in the job search rule access rule.

Example 18-2 *Debug Messages by an Access Rule with a URL Condition (Action: Block)*

[Click here to view code image](#)

> **system support firewall-engine-debug**

Please specify an IP protocol:

Please specify a client IP address: **192.168.1.2**

Please specify a client port:

Please specify a server IP address:

Please specify a server port:

Monitoring firewall engine debug messages

192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 New session

192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search

Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:

untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff

192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 pending rule order 2, 'Job Search

Rule', URL

192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:

untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff

192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 pending rule order 2, 'Job Search Rule', URL

192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:

untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff

192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 pending rule order 2, 'Job Search Rule', URL

192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 URL SI:

ShmDBLookupURL("http://dice.com/") returned 0

192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search

Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:

untagged, svc 676, payload 0, client 638, misc 0, user 9999997, url

http://dice.com/, xff

192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0: DataMessaging_GetURLData: Returning

URL_BCTYPE for dice.com

192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 rule order 2, 'Job Search

Rule', URL

Lookup Success: http://dice.com/ waited: 0ms

192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 rule order 2, 'Job Search Rule', URL http://dice.com/ Matched Category: 26:96 waited: 0ms

192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 **match** rule order 2, **'Job Search Rule'**,
action Block

192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 **deny action**

192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 Deleting session

Allowing a Specific URL

If you do not want FTD to block a particular URL along with the other URLs that are in the same category, you can override the default reputation score of that URL. To accomplish this, you just need to add a separate access rule with the Allow action.

Configuring FTD to Allow a Specific URL

The following steps describe how to create an access rule to allow a certain URL:

Step 1. Go to **Objects > Object Management** and create an object of type URL. [Figure 18-13](#) shows the workflow to create a new URL object. In this example, the URL-Object-for-Dice.com custom object represents the dice.com site.



Figure 18-13 *Configuring a New URL Object*

Step 2. Once a URL object is created, create a new access rule to allow this URL object. [Figure 18-14](#) shows an access rule that allows the URL-Object-for-Dice.com object. Note that the job search whitelist rule is placed above the existing rule #1. The custom URL object is located under the URLs subtab.

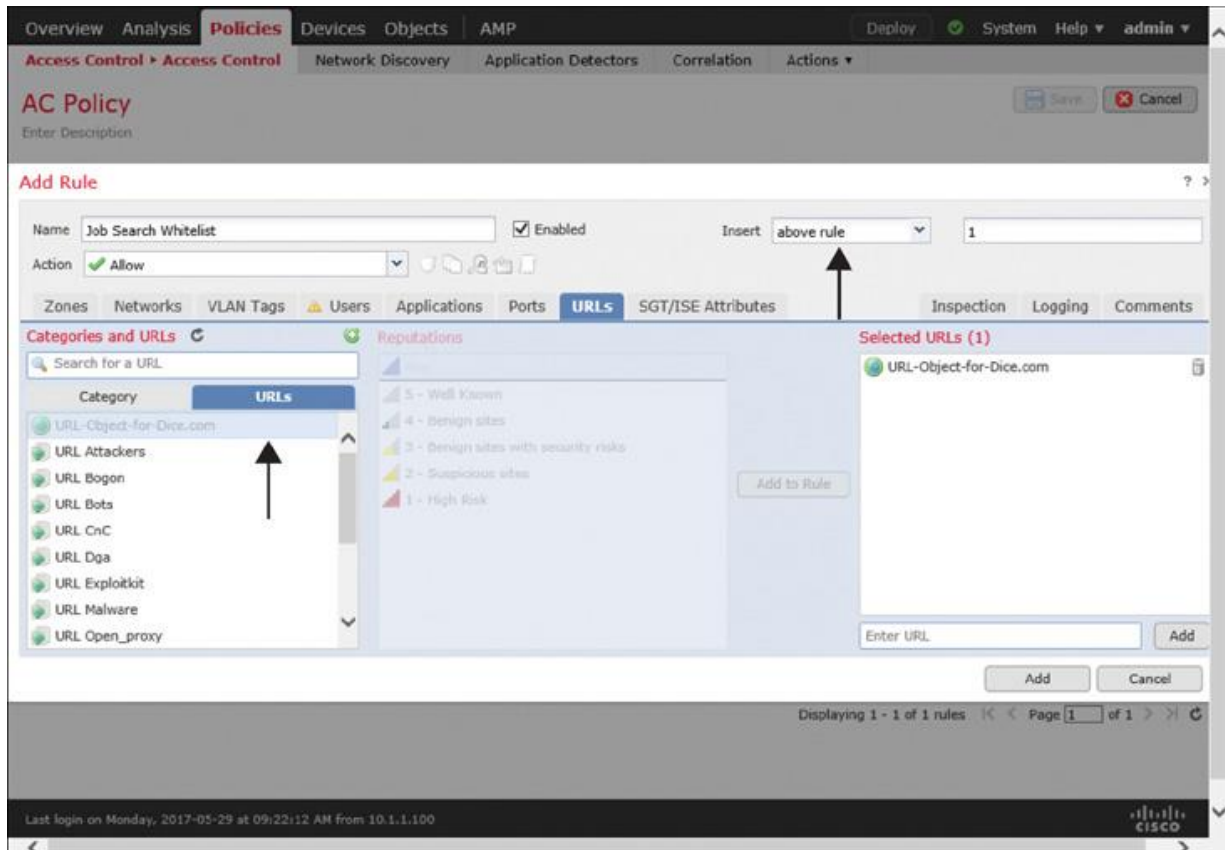


Figure 18-14 *Adding an Access Rule to Allow/Whitelist a Desired URL*

Note

Because an FTD device analyzes rules top to bottom, a whitelist rule must be positioned above a block rule. You can define the position as you add the rule. Alternatively, after adding a rule, you can go to the access control policy editor page to drag a rule to a desired position.

Step 3. Optionally, go to the Logging tab and enable Log at Beginning of Connection. This optional step allows an FTD to generate events due to any matching URL Filtering condition.

Step 4. Click the **Add** button to complete the creation of the access rule. The browser returns to the access control policy editor page.

Figure 18-15 shows all the access rules on a policy editor page. The rule that allows/whitelists your desired URL is positioned above the rule that blocks the entire Job Search category. This page allows you to drag a rule and place it in a different order.

FTD analyzes rules top to bottom, and an Allow rule must be above a Block rule for early analysis.

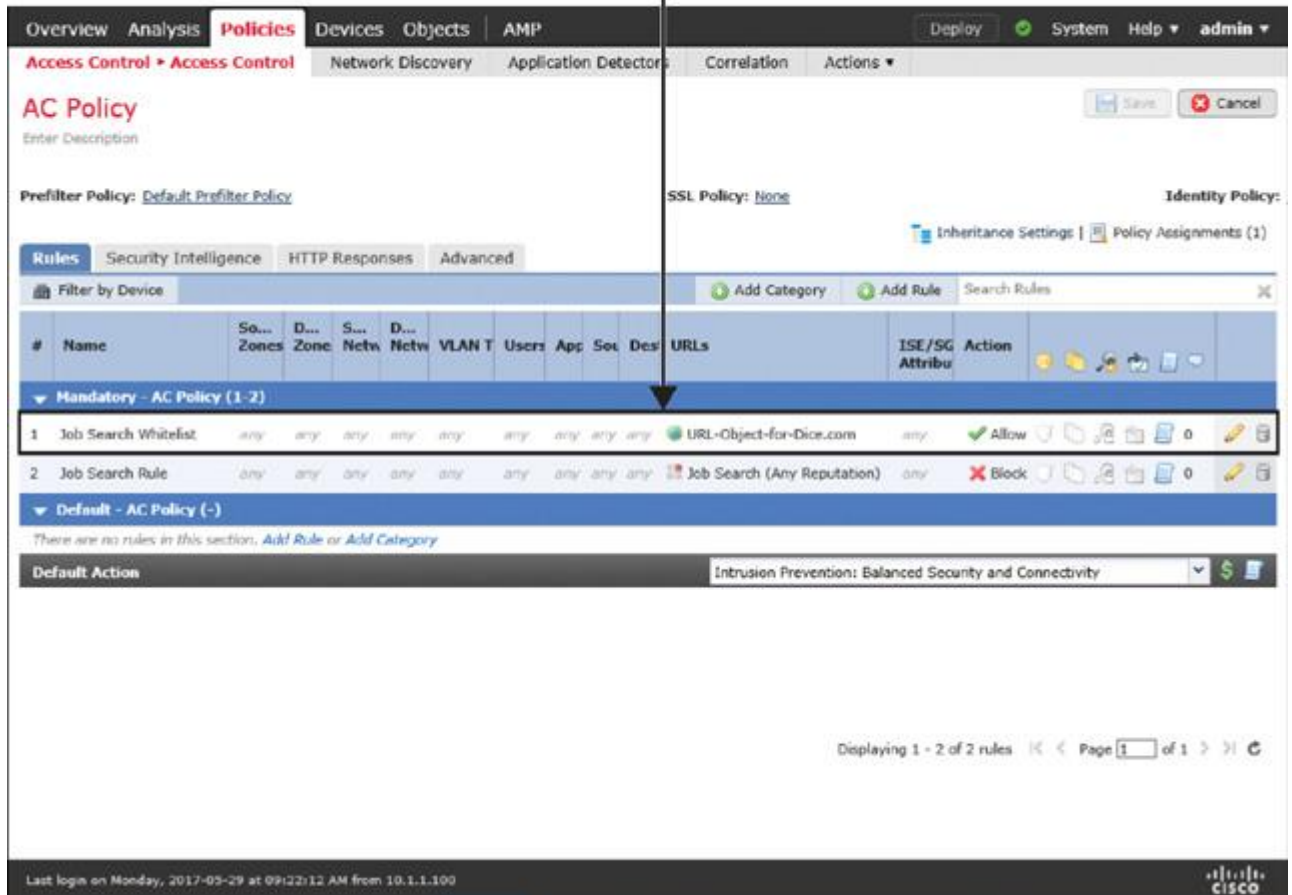


Figure 18-15 Access Control Policy Editor Page Showing a Summary of the Access Rules

Step 5. Click **Save** to save the changes in the access control policy, and click **Deploy** to deploy the policy to your FTD device.

Verification and Troubleshooting Tools

To verify the operation of the Allow action, perform the same test that you did in the previous section: Attempt to visit three search engines. This time, FTD should allow your access to dice.com, although this is a job search engine. However, FTD should continue blocking access to other job search engines, such as careerbuilder.com. Any URL categories except Job Search are allowed.

Attempt to visit the same three websites once again and notice the difference:

Figure 18-16 shows that dice.com is now allowed, while the careerbuilder.com site remains blocked. Because of the default action on the access control policy, FTD allows the general search engine google.com.

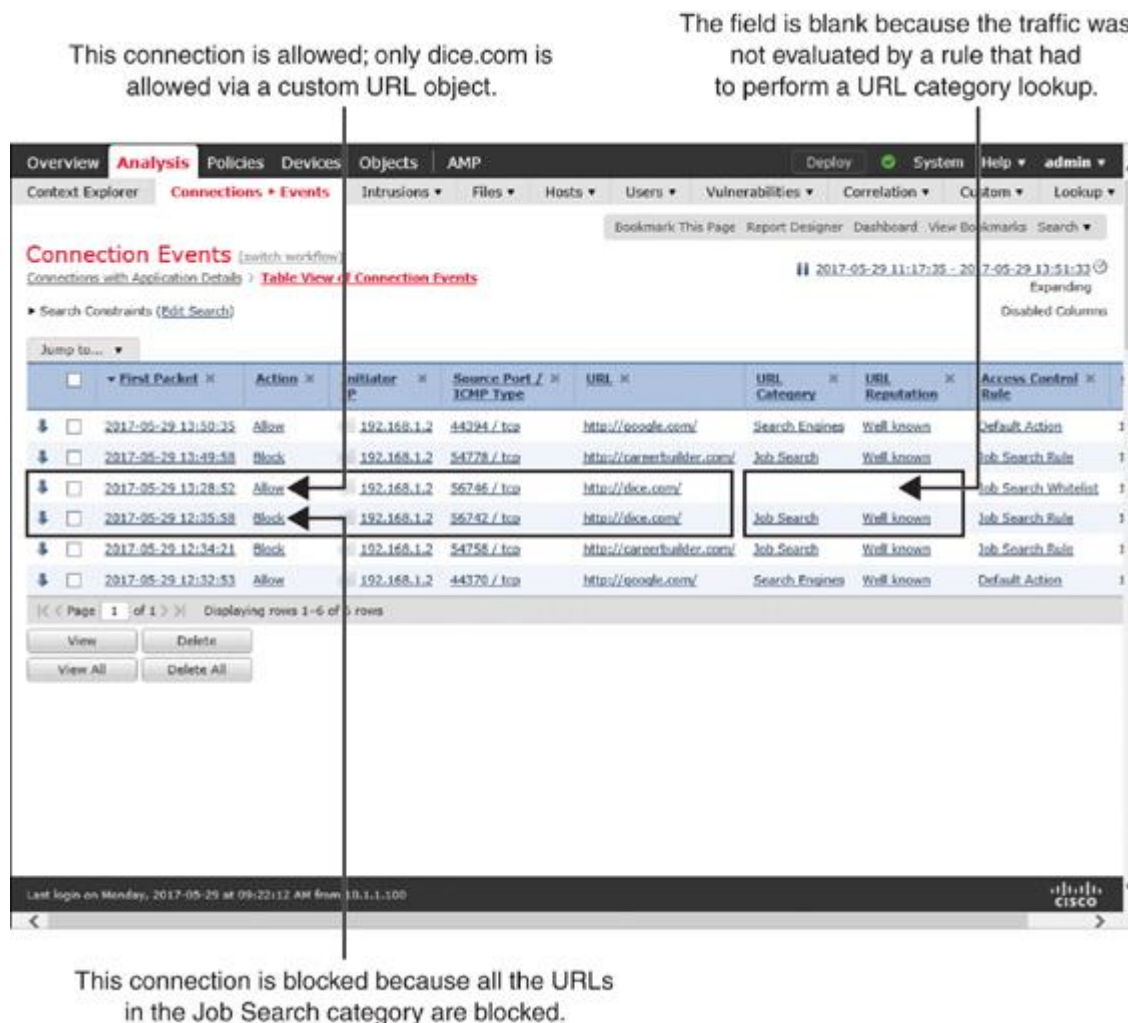


Figure 18-16 Whitelisting a URL by Using the Allow Action

You can use the **firewall-engine-debug** tool to debug the whitelisting actions. The debugging messages are helpful for troubleshooting purposes.

Example 18-3 shows the **firewall-engine-debug** messages when FTD allows you to access the whitelisted URL dice.com.

Example 18-3 Debugging Messages When Access to Dice.com Is Whitelisted/Allowed

[Click here to view code image](#)

> **system support firewall-engine-debug**

Please specify an IP protocol:
 Please specify a client IP address: 192.168.1.2
 Please specify a client port:

Please specify a server IP address:

Please specify a server port:

Monitoring firewall engine debug messages

192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 New session

192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search

Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:

untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff

192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 pending rule order 2, 'Job Search

Whitelist', URL

192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search

Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:

untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff

192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 pending rule order 2, 'Job Search

Whitelist', URL

192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search

Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:

untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff

192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 pending rule order 2, 'Job Search

Whitelist', URL

192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 URL SI:

ShmDBLookupURL("http://dice.com/") returned 0

192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search

Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:

untagged, svc 676, payload 0, client 638, misc 0, user 9999997, url

http://dice.com/, xff

```
192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 match rule order 2, 'Job Search  
Whitelist', action Allow
```

```
192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 allow action
```

```
192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 Deleting session
```

[Example 18-4](#) shows the **firewall-engine-debug** messages when FTD denies you access to a job search engine, such as careerbuilder.com. The debugging messages confirm that FTD is able to perform a URL lookup successfully, but the URL itself is blocked due to a matching condition in the job search rule access rule.

Example 18-4 *Debugging Messages When Access to careerbuilder.com Is Blocked*

[Click here to view code image](#)

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol:
```

```
Please specify a client IP address: 192.168.1.2
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 New session
```

```
192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 Starting with minimum 2, 'Job Search
```

```
Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:
```

```
untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
```

```
192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 pending rule order 2, 'Job Search
```

```
Whitelist', URL
```

```
192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 Starting with minimum 2, 'Job Search
```

```
Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag
```

```
:
```

```
untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
```

192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 pending rule order 2, 'Job Search
Whitelist', URL

192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 Starting with minimum 2, 'Job Search
Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:
untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff

192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 pending rule order 2, 'Job Search
Whitelist', URL

192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 URL SI:
ShmDBLookupURL("http://careerbuilder.com/") returned 0

192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 Starting with minimum 2, 'Job Search
Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:
untagged, svc 676, payload 1491, client 638, misc 0, user 9999997, url
http://careerbuilder.com/, xff

192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 **no match** rule order 2, **'Job Search
Whitelist'**, url=(http://careerbuilder.com/) c=0 r=0

192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1: DataMessaging_GetURLData:
Returning URL_BCTYPE for careerbuilder.com

192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 rule order 3, **'Job Search Rule', URL
Lookup Success: http://careerbuilder.com/** waited: 0ms

192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 rule order 3, 'Job Search
Rule', URL http://careerbuilder.com/ Matched Category: 26:92 waited: 0ms

192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 **match rule** order 3, **'Job Search
Rule'**, action Block

192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 **deny action**

192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 Deleting session

Querying the Cloud for Uncategorized URLs

In most cases, FTD resolves a URL into its category and reputation the first time it sees the web request. If FTD is unable to resolve a URL, it forwards the query to the FMC. The FMC performs a lookup on its own URL database. Because the FMC typically has a larger URL dataset than FTD, it should be able to resolve most of the URLs.

If you enter a new and uncommon URL, the FMC may be unable to resolve the category by looking up its local database. In such a case, it can send the query to the Cisco CSI cloud. If the cloud lookup times out, or if the query to the CSI is disabled due to privacy concerns, the FMC places the unknown URL into the Uncategorized group.

Warning

When a host attempts to connect an uncategorized URL, FTD does not match a connection against an access rule that uses the URL Filtering condition.

[Figure 18-17](#) illustrates the reason for receiving an uncategorized URL event. When the FMC is unable to query an unknown URL to the cloud, it marks that URL as Uncategorized.

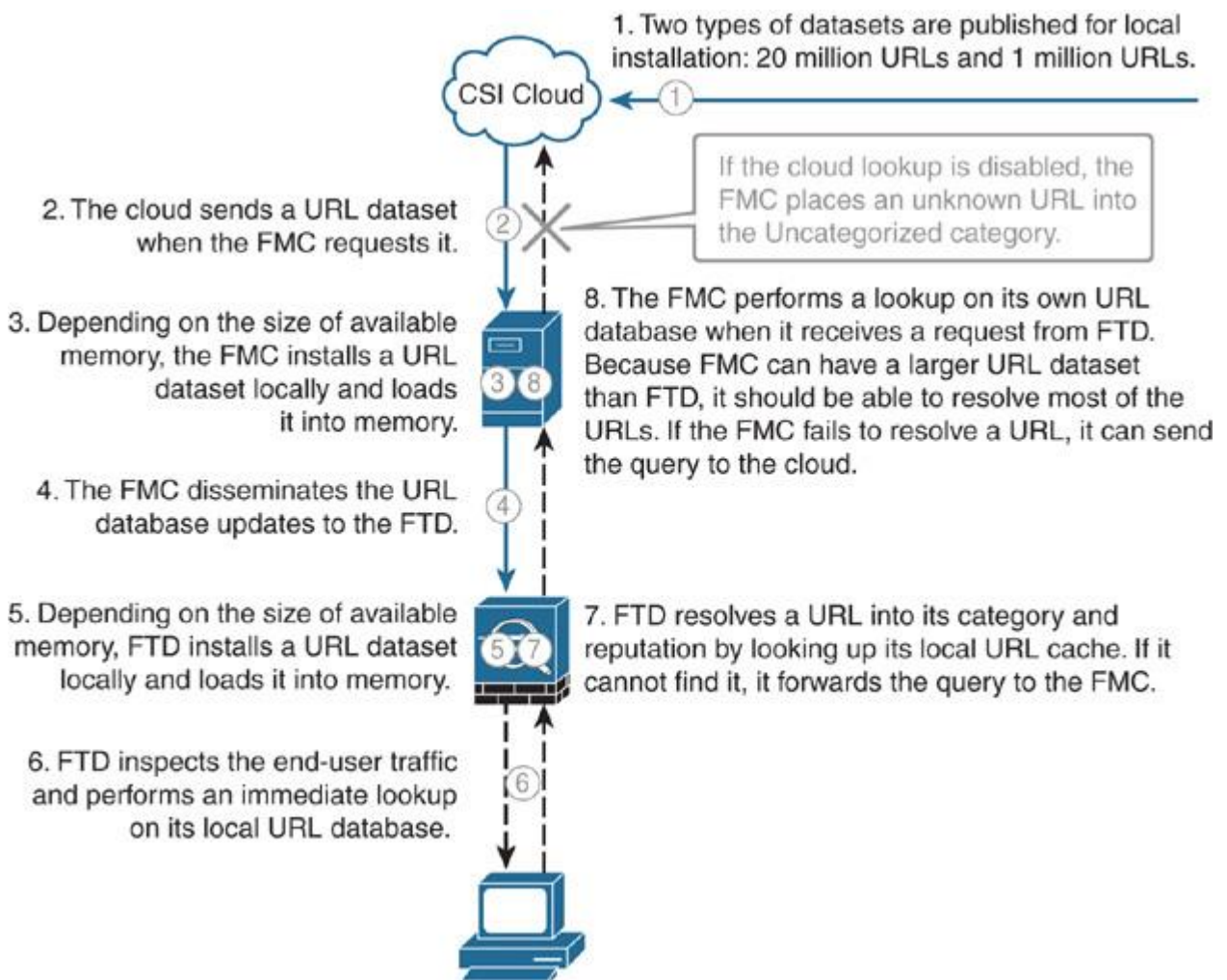


Figure 18-17 Workflow of an Uncategorized URL Event

Configuring FMC to Perform a Query

To allow the FMC to perform a cloud lookup for unknown URLs, follow these steps:

Step 1. Go to **System > Integration > Cisco CSI**.

Step 2. Enable the Query Cisco CSI for Unknown URLs option.

Step 3. Save the changes.

[Figure 18-18](#) shows the configuration page to enable cloud lookup for unknown URLs.

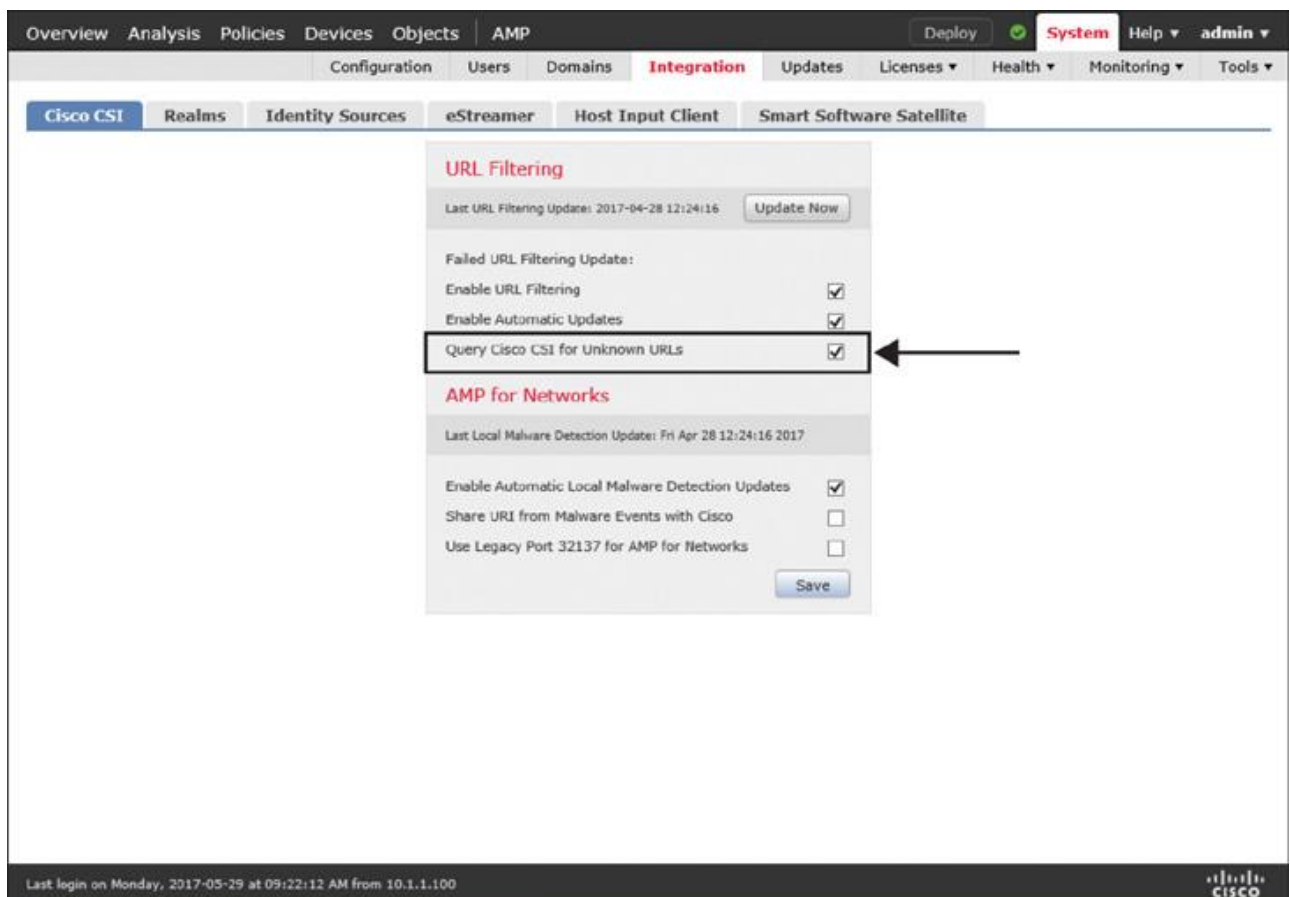


Figure 18-18 *Enabling Cloud Lookup for Unknown URLs*

While resolving a URL category, FTD does not let the uncategorized traffic pass until the URL lookup is complete or a lookup process times out, whichever comes first. If the volume of uncategorized traffic grows, FTD keeps holding the traffic in memory. FTD considers a URL uncategorized until an appropriate category is determined during a cloud lookup. FTD allows the initial flows, but for subsequent connections, it continues to look up that URL with the hope of resolving and caching it.

This behavior, however, can lead to performance degradation. To avoid this situation, you can let an FTD device pass traffic immediately whenever a URL appears uncached and the URL category cannot be determined locally. The following steps show how to disable a retry when a local cache fails the first lookup:

Step 1. Go to **Policies > Access Control > Access Control** and edit the access control policy that is deployed on your FTD device.

Step 2. In the access control policy editor page that appears, select the **Advanced** tab.

Step 3. Select the pencil icon next to General Settings. The General Settings configuration window appears.

Step 4. Disable the **Retry URL Cache Miss Lookup** option and click **OK** to return to the access control policy editor page.

Step 5. Click **Save** to save the changes and click **Deploy** to redeploy the policy to your FTD device.

[Figure 18-19](#) shows an advanced setting in an access control policy that allows an FTD device to pass uncategorized traffic immediately, without holding it for continuous cloud lookups.

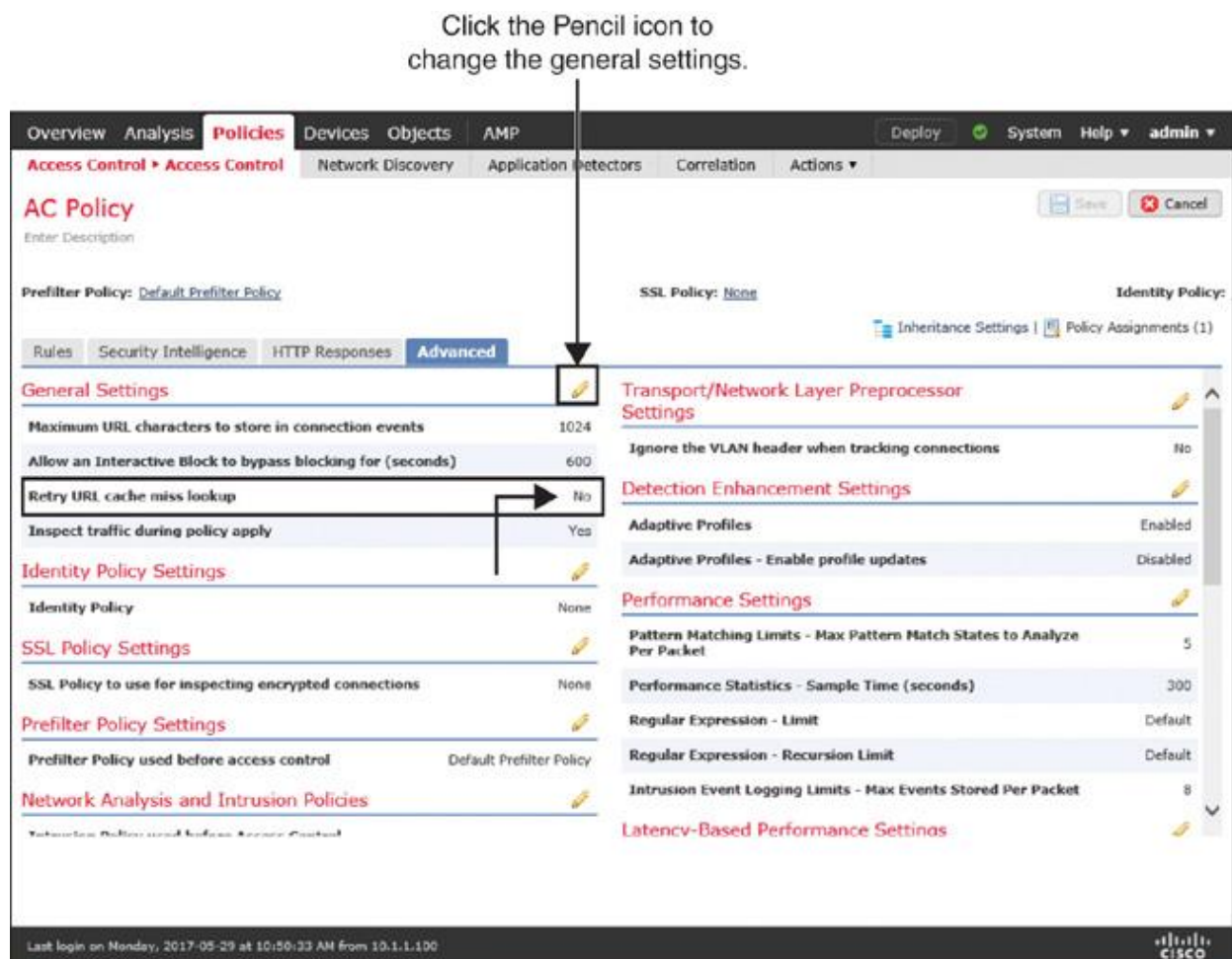


Figure 18-19 Disabling Any Retry When a Local Cache Misses URLs

Find a URL that is new or unknown and try to access it. If the URL is found uncategorized, the default action of the access control policy should allow you access to that URL.

[Figure 18-20](#) shows a connection event for accessing nazmulrajib.com. The URL category is marked as Uncategorized.

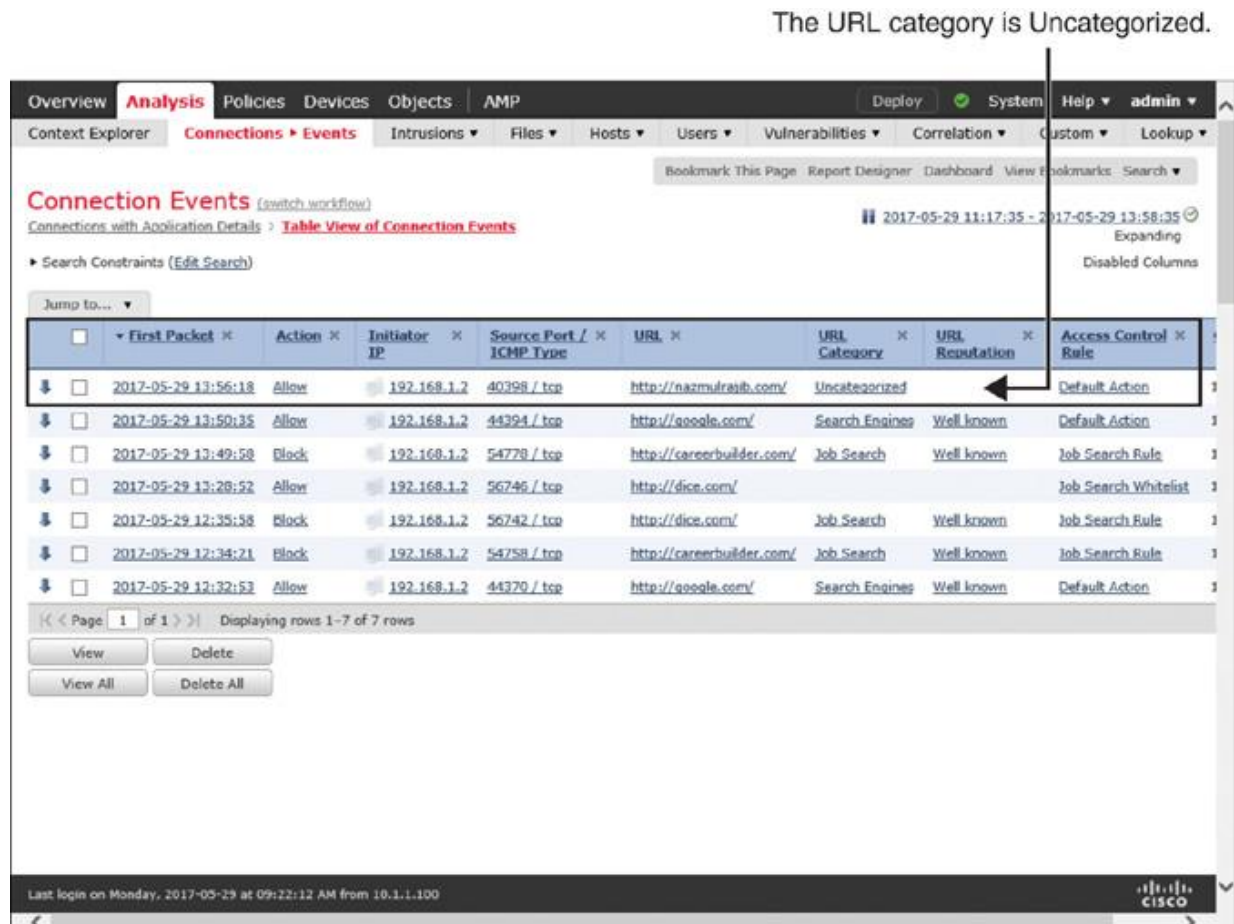


Figure 18-20 Example of an Uncategorized URL Event

[Example 18-5](#) displays the debugging messages that result from connecting to the unknown URL nazmulrajib.com. First, the FTD device performs a lookup on its local shared memory (see the keyword **ShmDBLookupURL** in the example). Then it attempts to query the cloud (see the keyword **useVendorService**). Because the cloud lookup is disabled in this example (see the keyword **feature not set**), the URL lookup eventually fails.

Example 18-5 Debugging a Connection to an Uncategorized URL

[Click here to view code image](#)

> **system support firewall-engine-debug**

Please specify an IP protocol:

Please specify a client IP address: **192.168.1.2**

Please specify a client port:

Please specify a server IP address:

Please specify a server port:

Monitoring firewall engine debug messages

192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 New session

192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search

Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:

untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff

192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 pending rule order 2, 'Job Search

Whitelist', URL

192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search

Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:

untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff

192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 pending rule order 2, 'Job Search

Whitelist', URL

192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search

Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:

untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff

192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 pending rule order 2, 'Job Search

Whitelist', URL

192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 URL SI:

ShmDBLookupURL("http://nazmulrajib.com/") returned 0

192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2,

'Job Search Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0,

vlan 0, sgt tag: untagged, svc 676, payload 0, client 638, misc 0, user 9999997,

url http://nazmulrajib.com/, xff

192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 no match rule order 2, 'Job Search
Whitelist', url=(http://nazmulrajib.com/) c=0 r=0

192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0: DataMessaging_GetURLData:
useVendorService_feature not set, returning URL_FAILEDTYPE

192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 rule order 3, 'Job Search
Rule',

URL Lookup Failed: http://nazmulrajib.com/ waited: 0ms

192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 no match rule order 3, 'Job Search
Rule', url=(http://nazmulrajib.com/) c=65534 r=0

192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 match rule order 4, id 268435458
action Allow

192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 allow action

192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 Deleting session

If the Firepower System can't categorize a URL, there are a couple items you can check on both the FMC and FTD:

Step 1. Verify whether the FMC is updated with the latest URL database.

[Example 18-6](#) shows two types of URL database files on the FMC file system. The full_bcdb_rep_1m_5.174.bin file is smaller and applied to an FTD device for an immediate URL lookup. It is 22 MB in size and has approximately 1 million URLs. The larger database file, full_bcdb_rep_5.174.bin, is used by the FMC when FTD misses a URL lookup.

Example 18-6 *Two Types of URL Datasets Available on an FMC*

[Click here to view code image](#)

```
admin@FMC:~$ ls -halp /var/sf/cloud_download/
```

```
total 450M
```

```
drwxr-xr-x 3 www www 4.0K Apr 28 23:18 ./
```

```
drwxr-xr-x 64 root root 4.0K Apr 28 02:20 ../
-rw-r--r-- 1 root root 78 Apr 28 23:18 cloudagent_dlupdate_health
-rw-r--r-- 1 root root 22M Apr 28 16:24 full_bcdb_rep_1m_5.174.bin
-rw-r--r-- 1 root root 429M Apr 28 16:24 full_bcdb_rep_5.174.bin
-rw-r--r-- 1 www www 5.4K Aug 26 2016 sfrep_catg
-rw-r--r-- 1 www www 433 Aug 26 2016 sfrep_index
drwxr-xr-x 2 www www 4.0K Apr 28 23:52 tmp/
admin@FMC:~$
```

If you do not see an up-to-date file, you should check whether the automatic update of the URL database is enabled. If it is enabled, verify whether the latest update attempt was successful. You can view the `urldb_log` file to determine the status of the URL database update. To view it, run the following command on the FMC:

```
admin@FMC:~$ cat /var/log/urldb_log
```

The `urldb_log` file can contain the following keywords:

■ **Successfully downloaded:** This message confirms that the FMC was able to download the latest database update. Along with this message, you should also find the name of the update file, as in this example:

```
$$$$$
```

```
Successfully downloaded, applied and moved, full_bcdb_rep_5.174.bin,...
Success, called perl transaction,
```

[Click here to view code image](#)

■ **Up to date:** This message confirms that there is no new update available on the cloud since the database on the FMC was updated last time.

■ **Download failed:** This message indicates that an attempt to download a URL database file failed.

Step 2. Determine whether the current URL dataset on the FTD device is derived from the latest URL database on the FMC. [Example 18-7](#) confirms that the FTD device can obtain a smaller version of the latest URL dataset from the FMC.

Example 18-7 *FTD Downloading a Subset of the URL Database from the FMC*

[Click here to view code image](#)

```
admin@FTD:~$ ls -halp /var/sf/cloud_download/
total 22M

drwxr-xr-x 3 www www 4.0K Apr 28 22:01 ./
drwxr-xr-x 66 root root 4.0K Dec 12 00:19 ../
-rw-r--r-- 1 root root 78 Sep 19 2016 cloudagent_dlupdate_health
-rw-r--r-- 1 root root 22M Apr 28 22:01 full_bcdb_rep_5.174.bin
-rw-r--r-- 1 www www 5.4K Aug 26 2016 sfrep_catg
-rw-r--r-- 1 www www 433 Aug 26 2016 sfrep_index
drwxr-xr-x 2 www www 4.0K Apr 28 22:01 tmp/

admin@FTD:~$
```

Step 3. Check whether the shared memory of FTD loaded with the latest URL dataset. [Example 18-8](#) shows the URL database files on the shared memory of an FTD device. The timestamp on the file indicates that the FTD is loaded with the latest URL dataset.

Example 18-8 *Loading the Latest URL Dataset on FTD Memory*

[Click here to view code image](#)

```
admin@FTD:~$ ls -halp /dev/shm/ | grep -i bcdb
-rwxrwxrwx 1 root root 23M Apr 28 23:17 Global.bcdb1
-rwxrwxrwx 1 root root 6.1M Apr 28 23:17 Global.bcdb1acc
-rwxrwxrwx 1 root root 256K Apr 28 23:17 Global.bcdb1cacheinx
admin@FTD:~$
```

Summary

This chapter describes techniques to filter traffic based on the category and reputation of a URL. It illustrates how Firepower performs a URL lookup and how an FTD device takes an action based on the query result. This chapter explains the connection to a URL through debugging messages, which is critical for troubleshooting.

Quiz

1. Which of the following licenses is necessary to block a URL based on its category and reputation?

- a. Threat
- b. URL
- c. Malware

d. Both A and B

2. Which of the following statements is true about the URL lookup?

- a. FTD, by itself, can resolve any URLs on the Internet within a millisecond.
- b. Only the FMC can resolve any URLs on the Internet within a millisecond.
- c. Neither the FMC nor FTD can resolve all the URLs on the Internet.
- d. Both the FMC and FTD can resolve any URLs on the Internet independently.

3. Which of the following statements about URL database updates is true?

- a. New URLs are packaged in a binary file and downloadable from the Cisco website.
- b. A recurring scheduled task for URL database updates is required to update the URL database.
- c. The FMC communicates with CSI automatically every 30 minutes to check for a new update and downloads an update if available.
- d. All of the above.

4. Which of the following are true about uncategorized URLs?

- a. FTD can hold uncategorized traffic in the buffer if the URL lookup is pending.
- b. Connections associated with an uncategorized URL are not matched against an access rule if the rule uses a URL Filtering condition.
- c. Uncategorized URLs can be categorized if the FMC is able to communicate with CSI.
- d. All of the above.

Chapter 19

Discovering Network Applications and Controlling Application Traffic

The Firepower System can dynamically discover what applications are running in a network. It can also identify the host and user who are running a particular application. FTD can discover a network application with or without the help of any active scanner. FTD allows you to block certain traffic solely based on the type of an application a user might be running. This chapter describes how to configure network discovery policy to enable Application Visibility and Control (AVC) with Firepower.

Application Discovery Essentials

When you access a website, you interact with at least three types of applications: a browser on a client computer that originates the web communication, an underlying protocol that establishes the communication channel to the web, and the web contents for which you want to access a website. When an FTD device is configured and deployed properly, it is able to discover all three of these applications in a network. Moreover, it can categorize applications based on risk level, business relevance, content category, and so on.

Application Detectors

The Firepower System uses application detectors to identify the network applications running on a monitored network. The detection capability can vary, depending on the source of the detectors. There are mainly two sources for detectors:

■ **System-provided detectors:** The Firepower software, by default, comes with a set of application detectors. However, for a precise detection of the latest applications, you must update the Vulnerability Database (VDB).

The VDB contains the fingerprints of various applications, operating systems, and client software. It also keeps a record of the known vulnerabilities. When a Firepower system discovers an application, it can correlate the application with any known vulnerabilities to determine its impact within a network.

■ **User-created detectors:** You can create your own detectors based on patterns you notice on custom applications. The FMC provides full administrative control over your custom detectors, so that you can modify or disable them as necessary. Behind the scenes, it leverages OpenAppID—an open source application detection module.

Note

When a host from a monitored network connects to a server in a nonmonitored network, the FMC infers the application protocol (on the nonmonitored network) by using the information on the client software (of the monitored network).

[Table 19-1](#) shows the type of application detectors supported by Firepower. Except for the built-in internal detectors, you can activate or deactivate any types of detector, as necessary.

Table 19-1 *Types of Application Detector*

Type of Detector	Functions
Internal detector	Detects protocol, client, and web applications. Internal detectors are always on; they are built in within the software.
Client detector	Detects client traffic. It also helps to infer an application protocol on a nonmonitored network.
Web application detector	Detects traffic based on the contents in a payload of HTTP traffic.
Port-based application protocol detector	Detects traffic based on well-known ports.
Firepower-based application protocol detector	Detects traffic based on application fingerprints.
Custom application detector	Detects traffic based on user-defined patterns.

Figure 19-1 shows the application detector page on the FMC. To find this page, go to **Policies > Application Detectors**. You can search for any desired application to determine its coverage. For example, Figure 19-1 shows retrieval of 69 detectors that are related to Facebook. The total number of detectors can vary, depending on the VDB version running on the FMC.

Search for detectors that are related to the Facebook application.

Name	Protocol	Details	Type	Port(s)	State
Facebook Facebook is a social networking service.	TCP	Facebook	Internal Detectors		<input type="checkbox"/>
Facebook Applications Other Other Application categories in Facebook.	TCP	Facebook Applic...	Web Application		<input type="checkbox"/>
Facebook Apps Any facebook add on, generally games, puzzles,	TCP	Facebook Apps	Internal Detectors		<input type="checkbox"/>
Facebook Apps Any facebook add on, generally games, puzzles,	TCP	Facebook Apps	Web Application		<input type="checkbox"/>
Facebook Apps Any facebook add on, generally games, puzzles,	TCP	Facebook Apps	Internal Detectors		<input type="checkbox"/>
Facebook Comment A comment made to another user's status updat	TCP	Facebook Com...	Web Application		<input type="checkbox"/>
Facebook event A message or page view of a social event on Fa	TCP	Facebook event	Web Application		<input type="checkbox"/>
Facebook event A message or page view of a social event on Fa	TCP	Facebook event	Internal Detectors		<input type="checkbox"/>
Facebook Games Online games section of Facebook.	TCP	Facebook Games	Web Application		<input type="checkbox"/>
Facebook Like Clicking Like on Facebook.	TCP	Facebook Like	Web Application		<input type="checkbox"/>
Facebook Message A message sent on Facebook.	TCP	Facebook Messa...	Internal Detectors		<input type="checkbox"/>

Displaying 1 - 50 of 69 Detectors matching the filter

Currently, 69 detectors are found for Facebook.

Figure 19-1 *The Application Detector Page on the FMC*

Operational Architecture

FTD can control an application when a monitored connection is established between a client and server, and the application in a session is identified. To identify an application, FTD has to analyze the first few packets in a session. Until the identification is complete, FTD cannot apply an application rule. To ensure protection during the analysis period, FTD inspects those early packets by using the default intrusion policy of an active access control policy. Upon successful identification, FTD is able to act on the rest of the session traffic based on the access rule created using an application filtering condition. If a prefilter policy or an access control policy is configured to block any particular traffic, FTD does not evaluate the traffic further against a network discovery policy.

[Figure 19-2](#) illustrates the operational workflow of the Firepower engine. It demonstrates that a connection is subject to Application Visibility and Control (AVC) only if it passes the Security Intelligence inspection.

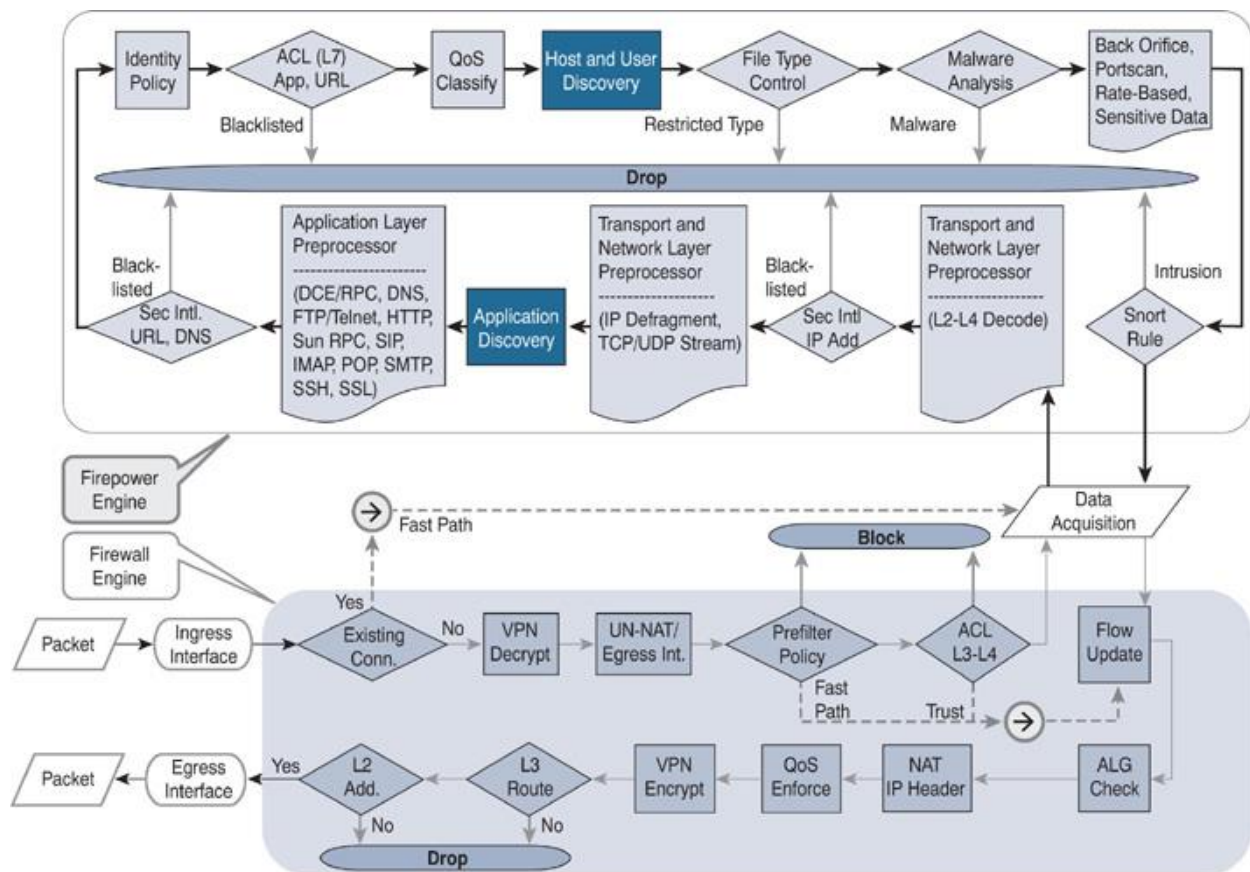


Figure 19-2 *Firepower Engine Workflow for Application Visibility and Control*

Best Practices for Network Discovery Configuration

FTD discovers a network passively; it does not directly affect the traffic flow. However, to ensure the performance of an FTD device, you should consider the following best practices when you enable network discovery:

Note

Network discovery policy on a Firepower system consists of three functionalities: application discovery, host discovery, and user discovery. This chapter primarily focuses on discovery and control of network applications. You can also learn how to perform host discovery.

- Keep the VDB version up to date. Installing the latest version ensures the detection of the latest software with more precise version information.
- By default, the FMC comes with an application discovery rule, which uses 0.0.0.0/0 and ::/0 as the network address. This address enables a Firepower system to discover applications from any observed networks. Do not remove this default rule, as Snort leverages the application discovery data for intrusion detection and prevention by detecting the service metadata of a packet.
- When you add a custom rule for host and user discovery, include only the network addresses you own. Do not add the network address 0.0.0.0/0 and ::/0 to a host and user discovery rule, because doing so can deplete the host and user licenses quickly.
- Exclude the IP addresses of any NAT and load balancing devices from the list of monitored networks. These types of IP address can represent multiple computers running in a LAN, which leads an FTD device to generate excessive discovery events whenever there are activities in the LAN. Exclusion of NAT and load balancing IP addresses can improve the performance of FTD.

[Figure 19-3](#) shows the positions of two types of intermediate devices—a router and a load balancer—that can each represent multiple network hosts.

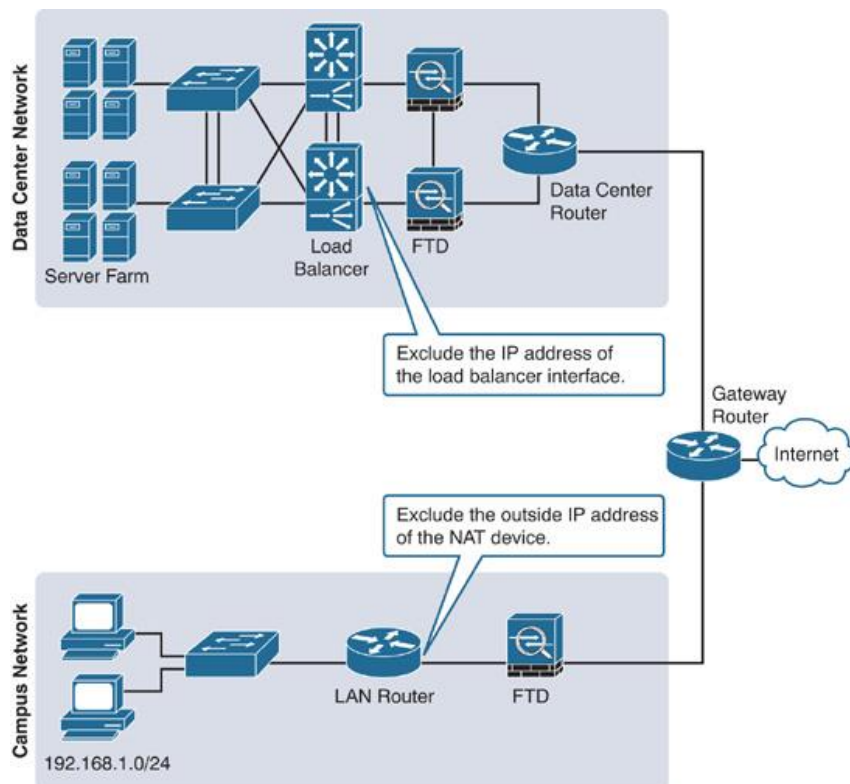


Figure 19-3 NAT Device (Router) and Load Balancer Interface Representing Multiple Hosts

■ You can also exclude any ports from monitoring if you are sure about the service a port might be running. Doing so reduces the number of discovery events for known ports and services.

■ Avoid creating overlapping rules that include the same hosts multiple times to prevent performance degradation.

■ Deploy the FTD device as close as possible to the hosts. The lower the hop count between an FTD device and a host, the faster the FTD device detects the host and with a higher confidence value.

Fulfilling Prerequisites

Before you begin configuring a network discovery rule, fulfill the following requirements:

■ The Firepower System uses the Adaptive Profiles option to perform application control. This option enhances detection capabilities of an FTD. The Adaptive Profile Updates option leverages the service metadata and helps an FTD determine whether a particular intrusion rule is pertinent to an application running on a particular host and whether the rule should be enabled.

By default, the Adaptive Profiles option is enabled (see [Figure 19-4](#)). You can verify the configuration status in the Advanced tab of an access control policy, under Detection Enhancement Settings.

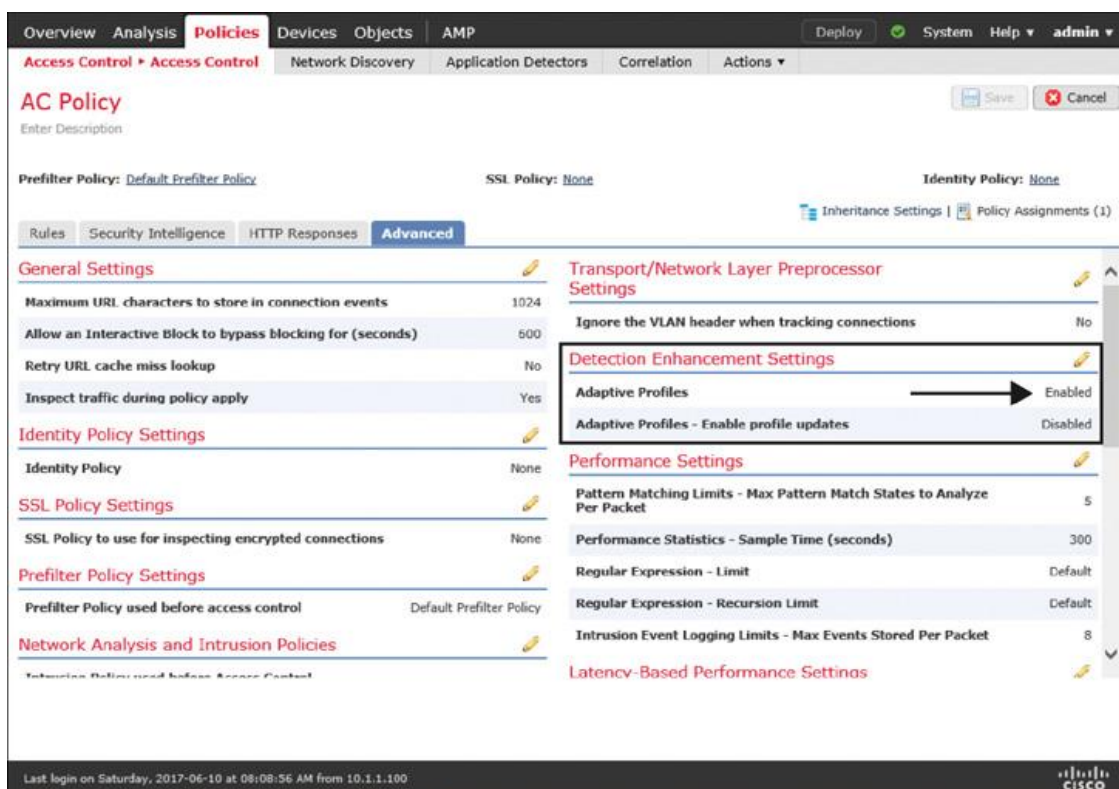


Figure 19-4 Adaptive Profiles Setting for an Access Control Policy

■ Create network objects for the network addresses that you want to add to a discovery rule. This helps you manage your configuration once you deploy a network discovery policy. To create an object, go to **Objects > Object Management** on the GUI. This page also enables you to modify the value of a custom object if necessary. However, you cannot modify a system-provided network object. To determine the type of an object, look at the rightmost column—a custom network object shows a pencil icon (see [Figure 19-5](#)), which you can select to modify the value of the object.

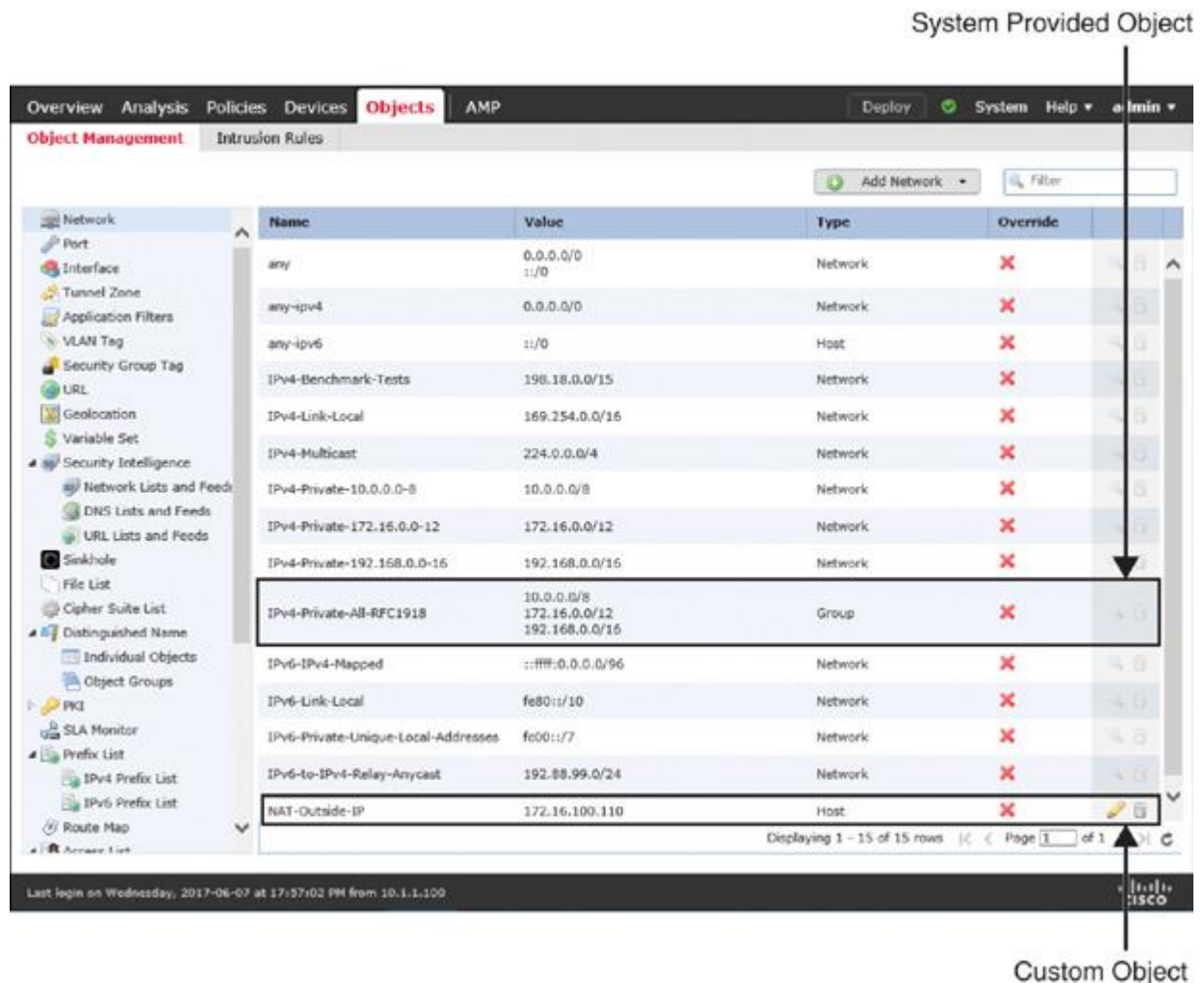


Figure 19-5 Object Management Page

Tip

The system also enables you to create an object on the fly directly from the rule editor window (see [Figure 19-8](#), later in the chapter).

Discovering Applications

In the following sections, you will learn how to configure a network discovery policy to discover network applications as well as network hosts. To demonstrate the impact of an

intermediate networking device representing multiple internal hosts, a router has been placed between the FTD device and the LAN switch in the topology.

Figure 19-6 shows the topology that is used in this chapter to demonstrate the configuration of a network discovery policy.

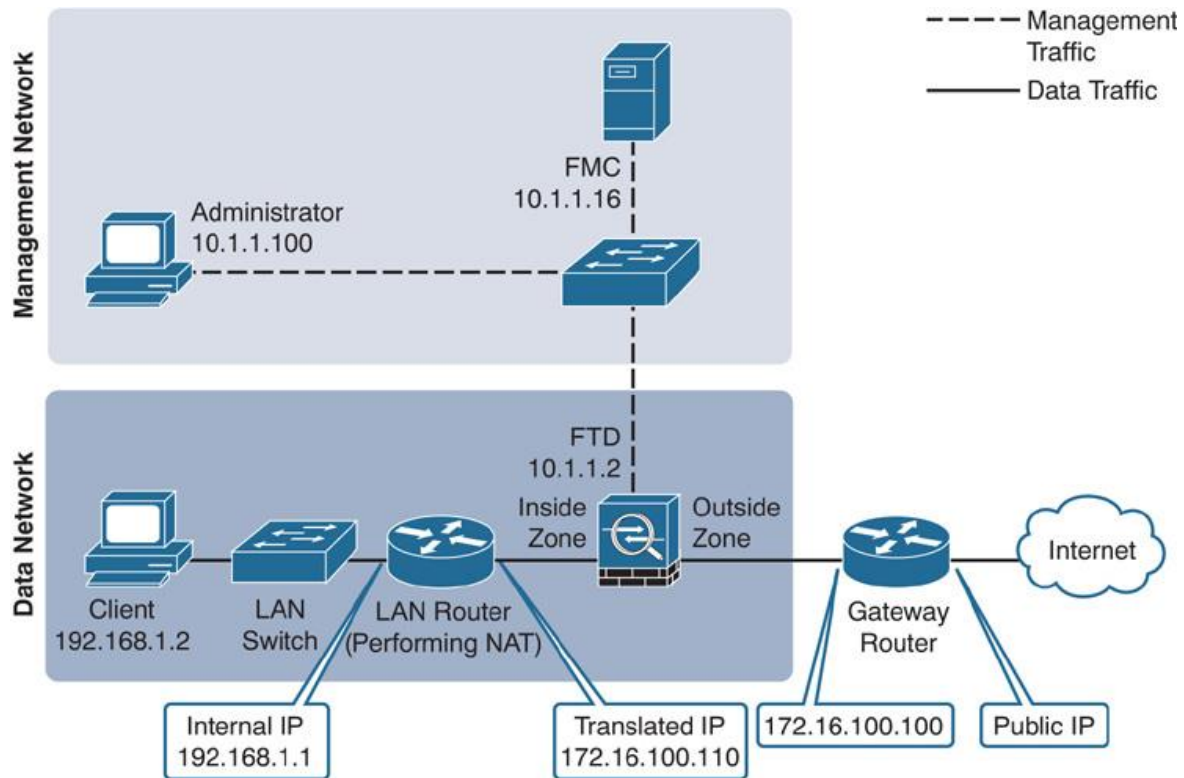


Figure 19-6 Topology to Demonstrate the Operation of a Network Discovery Policy

Configuring a Network Discovery Policy

To configure a network discovery policy, follow these steps:

Step 1. In the FMC, navigate to **Policies > Network Discovery**. The default rule for application discovery appears (see Figure 19-7). It monitors traffic from any network to discover applications.

The screenshot shows the Palo Alto Networks FMC interface. The top navigation bar includes Overview, Analysis, Policies (selected), Devices, Objects, and AMP. The main content area is titled 'Network Discovery' and shows a table with the following columns: Networks, Zones, Source Port Exclusions, Destination Port Exclusions, and Action. The table contains one row representing the default rule:

Networks	Zones	Source Port Exclusions	Destination Port Exclusions	Action
0.0.0.0/0 :::/0	any	none	none	Discover: Applications

Below the table, a text box states: "The default discovery rule monitors application traffic from any network."

Figure 19-7 *Default Rule for a Network Discovery Policy*

Step 2. Click the **Add Rule** button. The Add Rule window appears.

Step 3. First, add a rule to exclude the IP address of any intermediate NAT and load balancing devices. To do that, select **Exclude** from the Action dropdown, and then select a network object that represents your desired IP address.

Tip

If you did not create a network object previously in the Fulfilling Prerequisites section, you can do it now on the fly using the green plus icon. Alternatively, you can add an IP address directly on the rule editor window.

[Figure 19-8](#) shows a discovery rule that excludes a network object, NAT-Outside-IP. The object maps the IP address of the router's outside interface. The figure also highlights the available options to add an object or address on the fly.

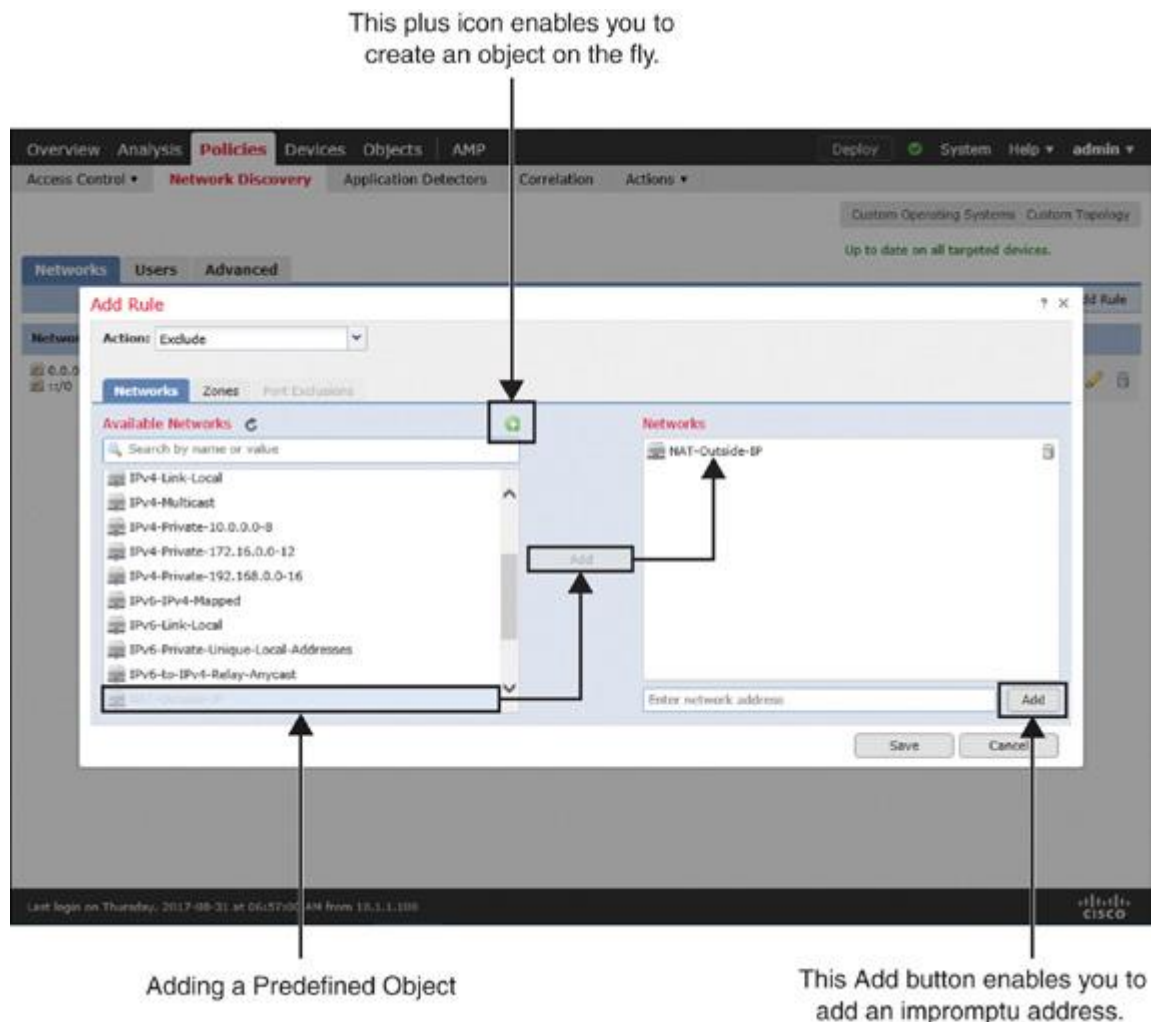


Figure 19-8 *Adding a Rule to Exclude a Network Object*

Step 4. Click the **Save** button to return to the network discovery policy page.

Step 5. Next, to include the network you want to monitor, click the **Add Rule** button again. The Add Rule window appears.

Step 6. Select **Discover** from the Action dropdown, and then select a network object that represents your desired IP network.

Tip

If you want to monitor a private network, you can select one of the system-provided network objects.

[Figure 19-9](#) shows a network discovery rule that can discover hosts and applications running on a network with private IP addresses (RFC 1918).

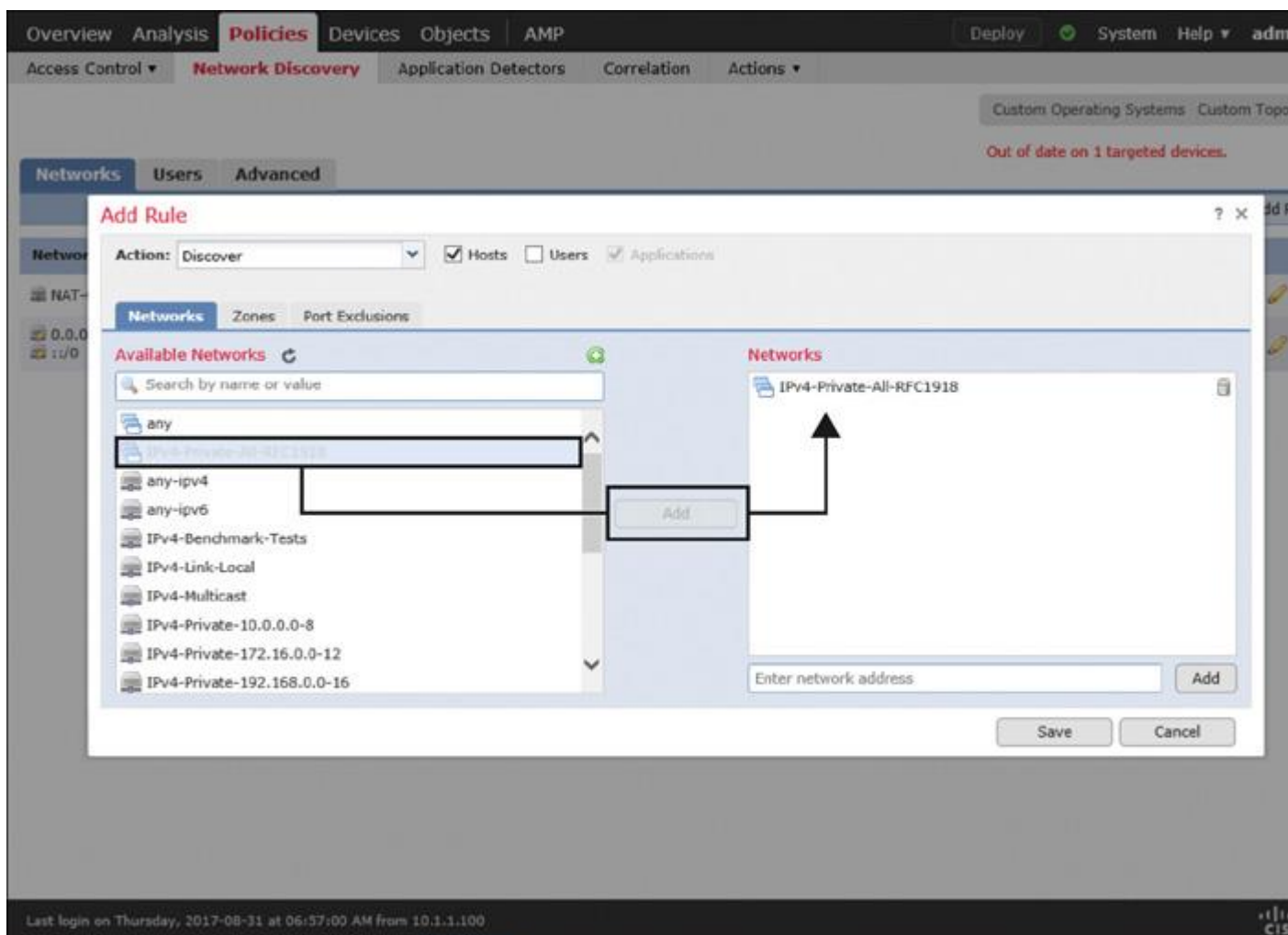


Figure 19-9 Adding a Rule to Discover Hosts and Applications

Step 7. Click the **Save** button to return to the network discovery policy page, and then click the **Deploy** button to deploy the network discovery policy on your FTD device.

Figure 19-10 shows the two network discovery rules you have just created.

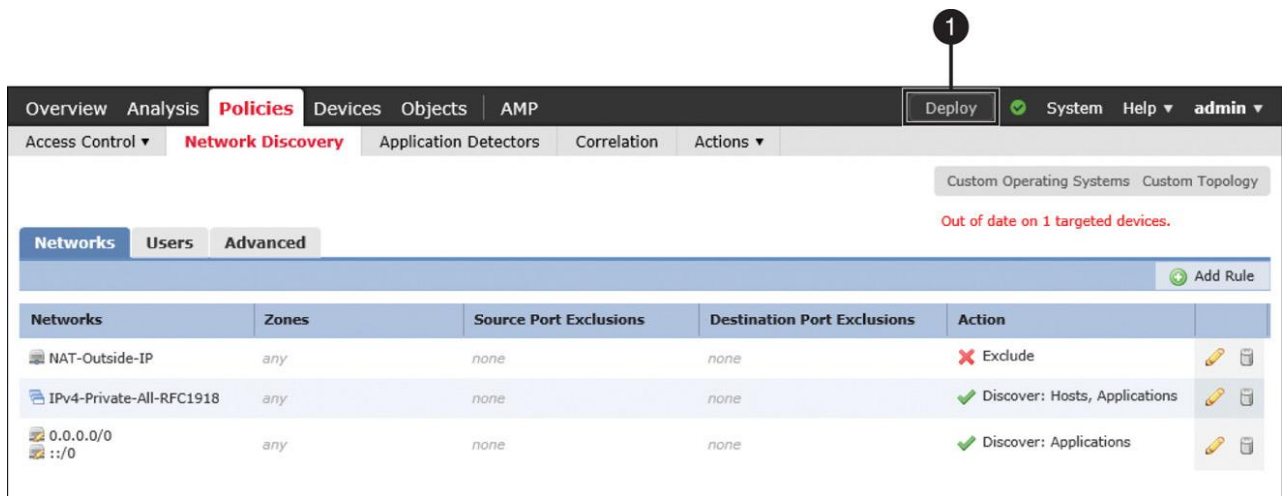


Figure 19-10 A New Exclusion Rule, a Custom Discovery Rule, and the Default Discovery Rule

Verification and Troubleshooting Tools

Now you can verify the functionality of network discovery by passing network traffic through an FTD device. First, from your client computers, go to various websites on the Internet. Doing so generates traffic through the FTD device. If the network discovery policy is properly configured and deployed, you will be able to view discovery events in the FMC GUI.

Analyzing Application Discovery

You can view a summary of the application data by using the Application Statistics dashboard, located at **Overview > Dashboards > Application Statistics**. The dashboard shows several data points in different widgets. You can add, remove, or modify any widgets, as desired.

Figure 19-11 shows six widgets in the Application Statistics dashboard. Each widget displays a unique statistic of the application running in a monitored network.

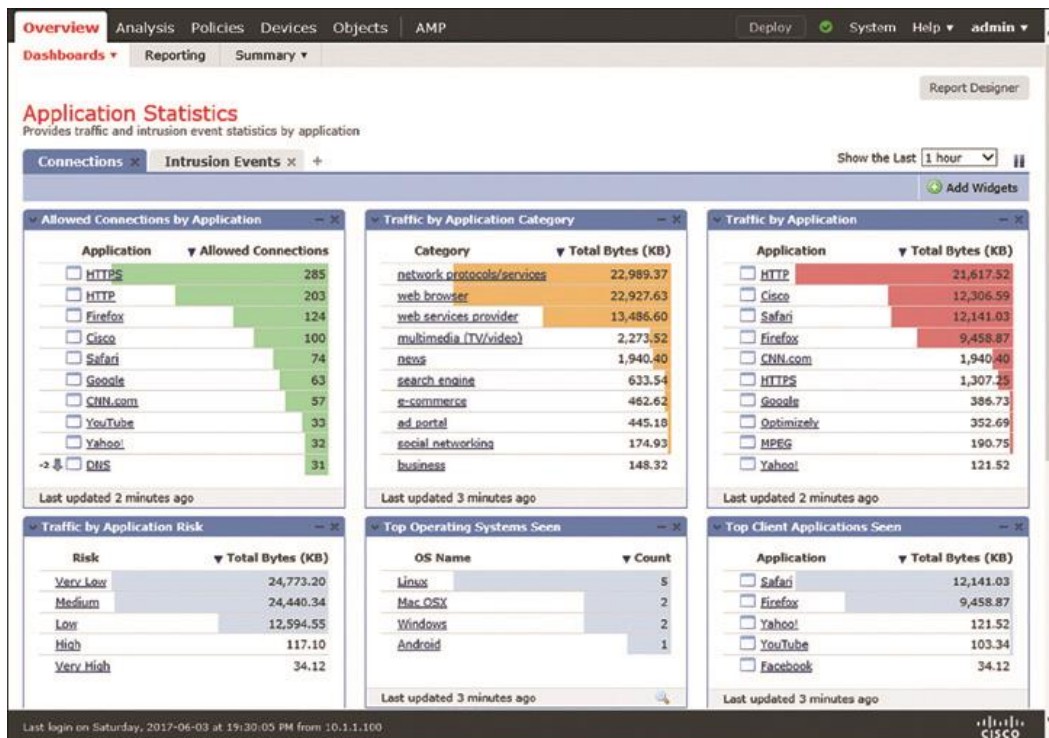
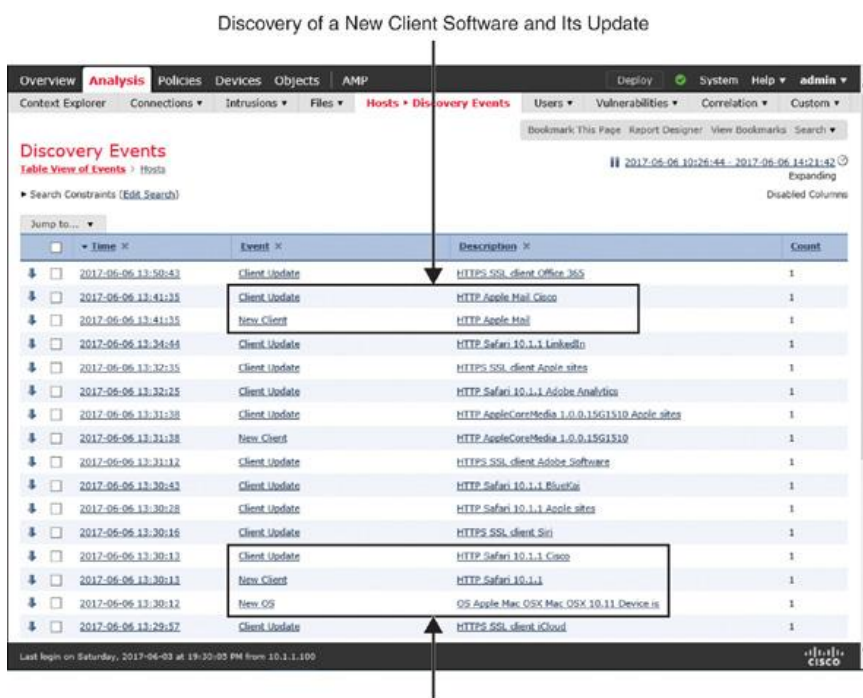


Figure 19-11 Application Statistics Dashboard

Figure 19-12 shows different types of discovery events. They are generated when a user connects an Apple Mac OS X to a network and opens a web browser, Safari. This figure also shows subsequent discoveries of various applications on the Mac.



These events appear when a user connects an Apple Mac OS X to a network and opens the Safari browser.

Figure 19-12 *Network Discovery Events*

Analyzing Host Discovery

You can view the operating systems running on a monitored network from the **Analysis > Hosts > Hosts** page. The Firepower System can identify most of the operating systems, along with their version detail. Click the Summary of the OS Versions to view the version information.

If some operating systems appear as *pending*, it is because FTD is currently analyzing the collected data or waiting on further packets to conclude. The *unknown* state indicates that the pattern of packets does not match an application detector. Updating the VDB to the latest version can reduce the number of unknown discovery events.

[Figure 19-13](#) shows the name and version of operating systems running on a monitored network. It also shows examples of *unknown* and *pending* operating system.

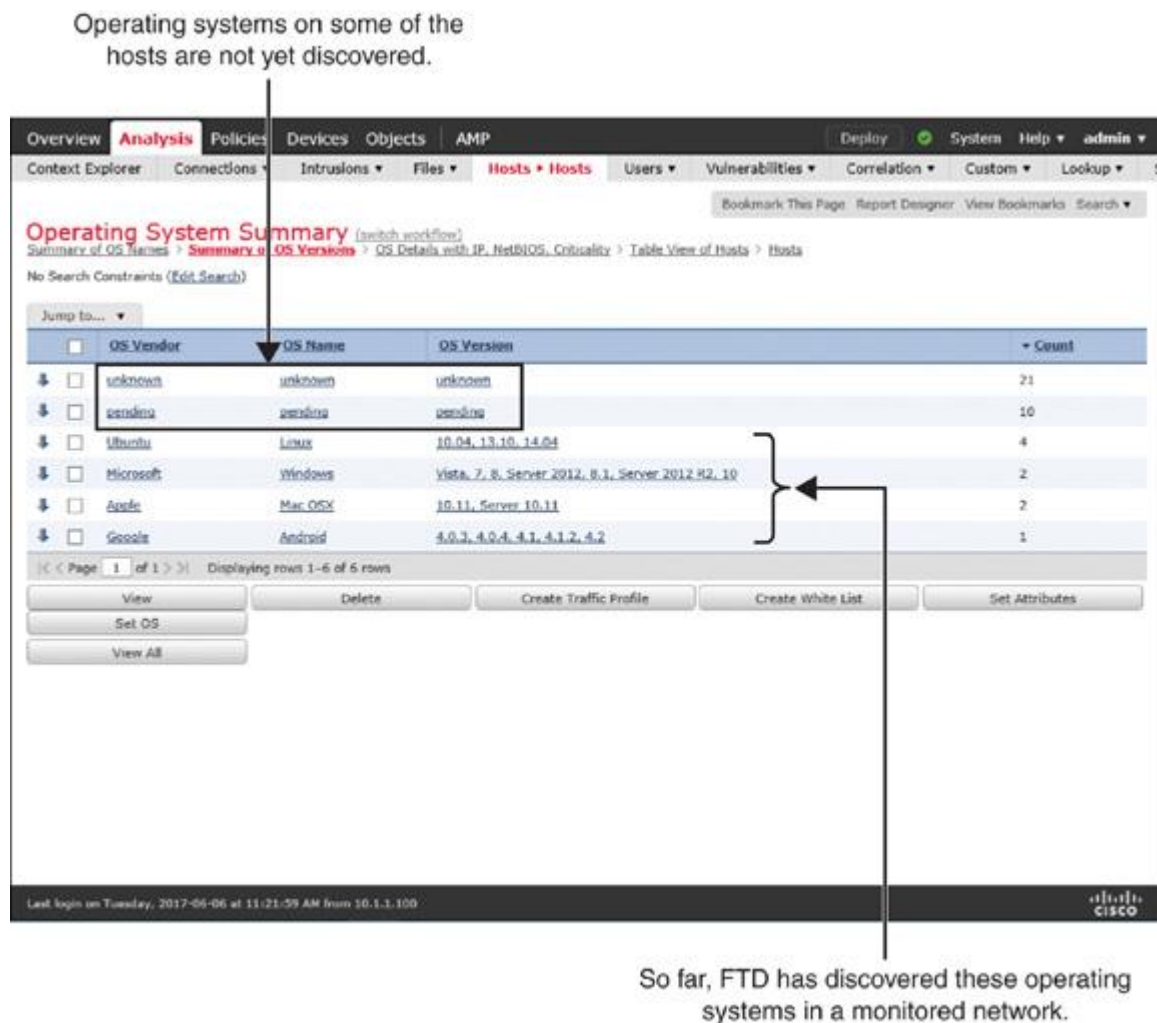


Figure 19-13 *Operating Systems on the Monitored Hosts*

Tip

Remember this best practice: The lower the hop count between an FTD device and a host, the faster the FTD device detects the host and with a higher confidence value. Moreover, additional intermediate devices between an FTD device and hosts can alter or truncate important packet data. Therefore, you should deploy an FTD device as close as possible to the monitored hosts.

Undiscovered New Hosts

If you find a new host undetected by your FTD device, you should check a couple items:

■ Check whether the FMC generates any health alerts for exceeding the host limits. To receive an alert due to the oversubscription of host discovery, the health monitor module for Host Limit must be enabled.

[Figure 19-14](#) shows the option to enable a health module that can trigger an alert when the FMC exceeds its host limit. To find this page, go to **System > Health > Policy** and edit a health policy you want to apply.

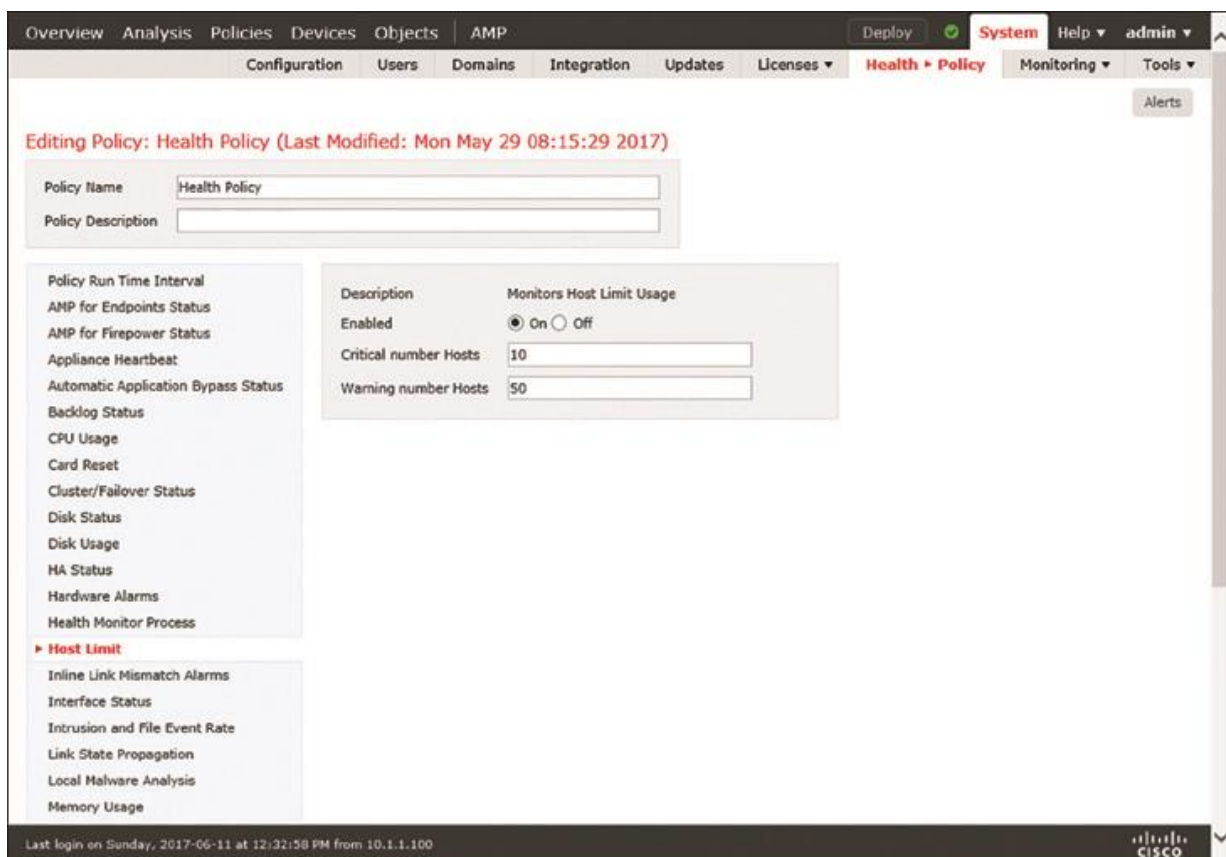


Figure 19-14 Health Module to Monitor Host Limit Usage

■ By analyzing the network map on the FMC, you can determine the number of unique hosts identified by a Firepower system and compare the number with the host limit for an FMC model. You can also recognize any hosts that might be representing multiple hosts, such as a

router with NAT feature enabled or a load balancer. It helps you to select an IP address for exclusion.

[Table 19-2](#) shows the maximum number of hosts the FMC can discover at any time.

Table 19-2 FMC Limitation for Host Discovery

FMC Model Host Limit

FS 2000	150,000
FS 4000	600,000
Virtual	50,000

Note

As of this writing, Cisco supports additional FMC models, such as FS750, FS1500, and FS3500, which were designed prior to the Sourcefire acquisition. While this book uses the latest hardware models, you can still apply this knowledge on any legacy hardware models. For any specific information on the legacy hardware models, read the official user guide.

[Figure 19-15](#) demonstrates that, although there are only 3 hosts in an internal network, FTD discovers more than 300 hosts in the external network within a few minutes. This discovery consumes additional resources and licenses from the Firepower System. To find this page, go to **Analysis > Hosts > Network Map**.

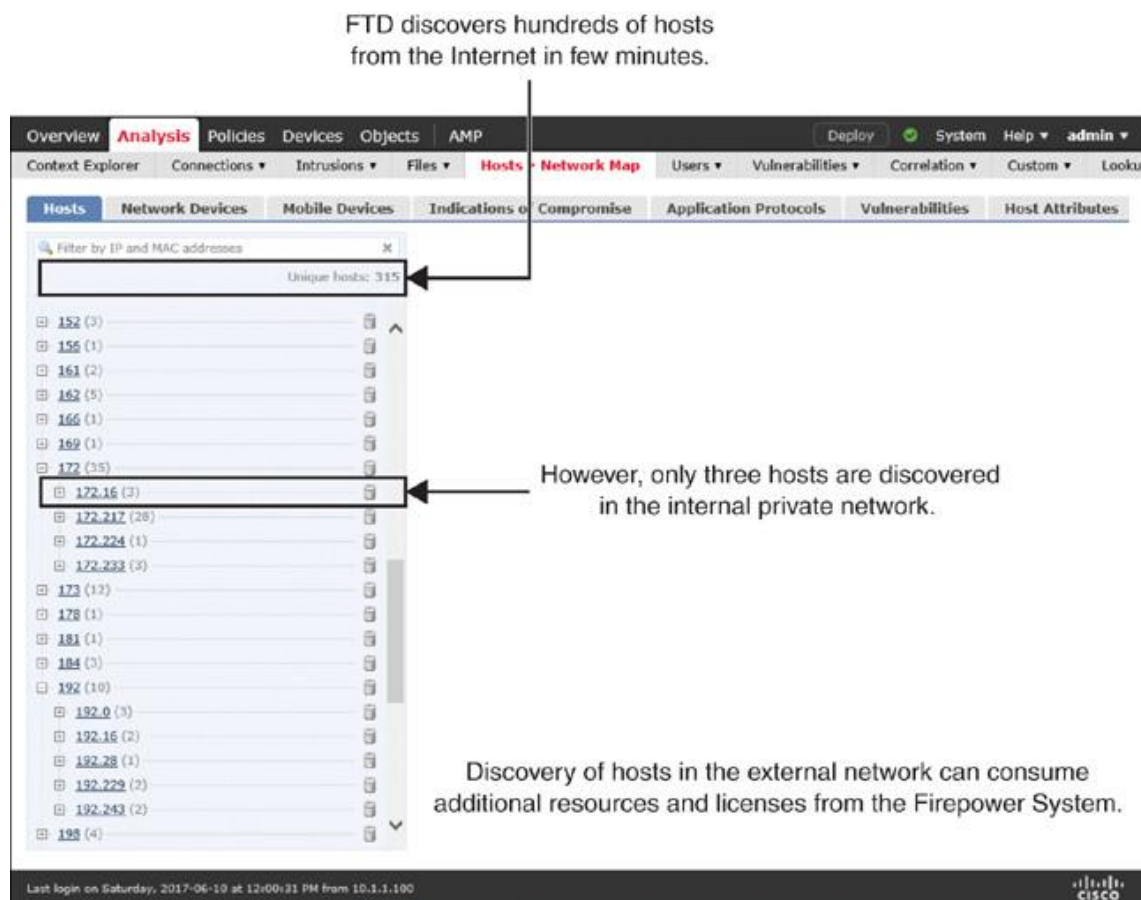


Figure 19-15 A Network Map on the FMC Shows All of the Hosts an FTD Device Discovers

■ Check how the network discovery policy is configured to handle a host when the FMC reaches the threshold for host limit. You can configure a policy to stop discovering any new hosts or to drop the earliest discoveries when the FMC reaches its limit.

[Figure 19-16](#) shows the navigation to a dropdown where you can choose between dropping an old host and locking down any new entries.

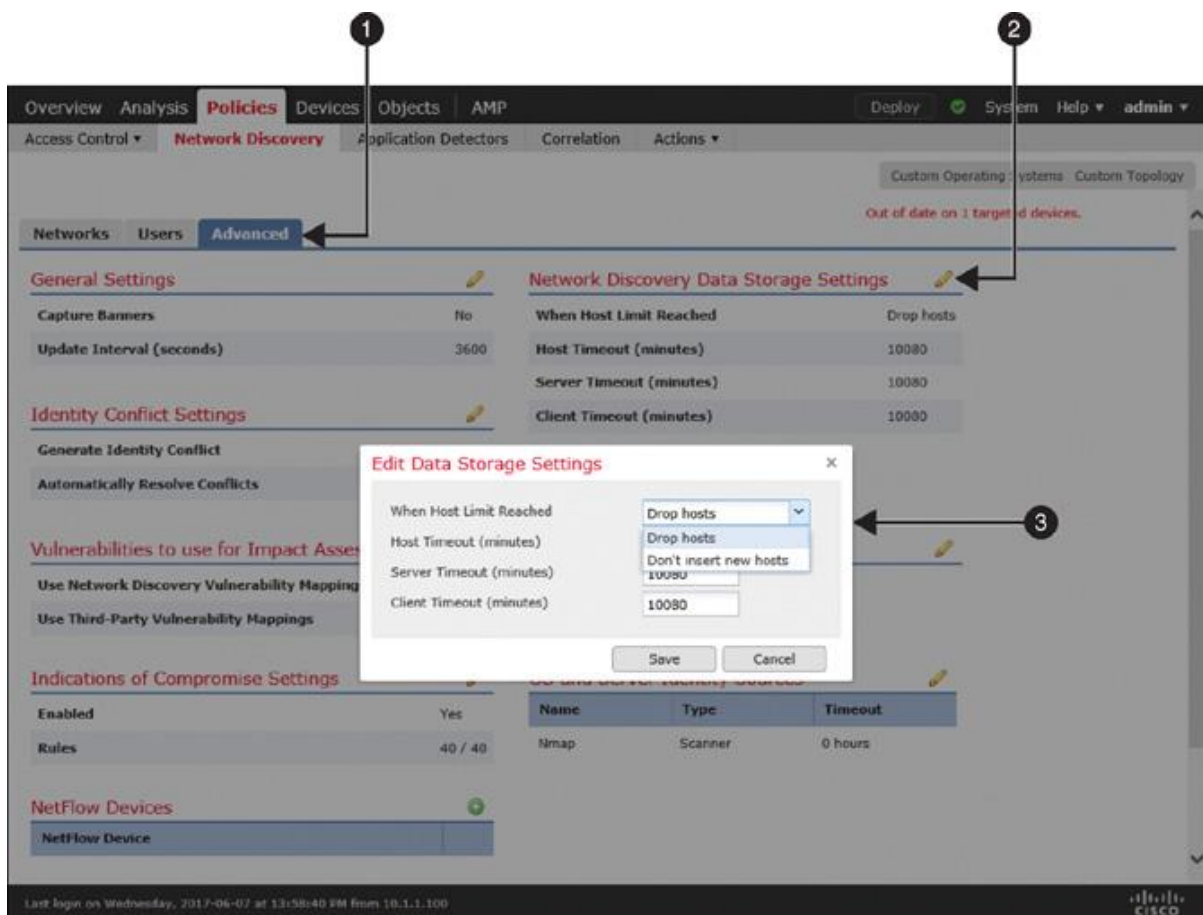


Figure 19-16 Advanced Network Discovery Settings

Blocking Applications

If an access control policy has no access rule with an application filtering condition, FTD allows any applications as long as connections to an application are permitted by the policy on the default action. You can verify this default behavior by attempting to access an application such as Facebook. However, if you want to restrict access to an application, you need to add an access rule for it.

Configuring Blocking of Applications

To block access to an application, you need to create an access rule by following these steps:

Step 1. Navigate to **Policies > Access Control > Access Control**. A list of available access control policies appears.

Step 2. Use the pencil icon to edit the access control policy that you want to deploy on an FTD device. The access control policy editor page appears.

Step 3. Click the **Add Rule** button. The rule editor window appears.

Step 4. Give a name to the rule and select a desired action for the matched traffic.

Step 5. Select the **Applications** tab. A list of available application filters appears.

[Figure 19-17](#) shows an access rule with an application filtering condition. FTD uses the rule to block a connection by sending reset packets whenever it detects an application in the Social Networking category.

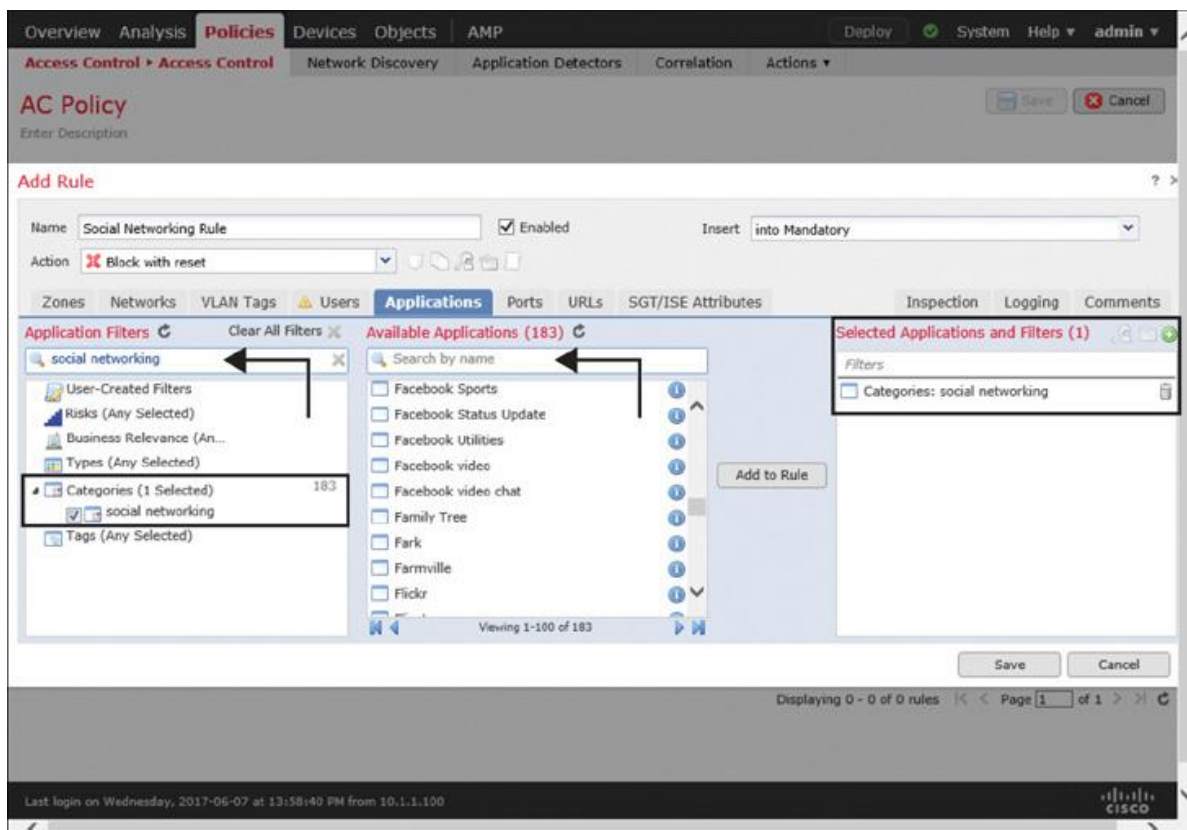


Figure 19-17 Access Rule to Block Any Applications in the Social Networking Category

Step 6. Use the search field in the Application Filter section to find a desired application category. You can select traffic based on categories, business relevance, risks, types, and so on. Alternatively, to find a specific application, you can just enter the application name in the search field in the Available Applications section.

Step 7. After you select the desired applications, add them to the rule.

Step 8. Go to the Logging tab to enable logging for any matching connections. This is an optional step, but it allows you to view an event when FTD blocks a connection.

Step 9. Click the **Save** button in the rule editor window to complete the creation of an access rule with an application filtering condition.

[Figure 19-18](#) shows this new access rule, which blocks any applications that are related to the Social Networking category only. Any other applications are subject to the default action.

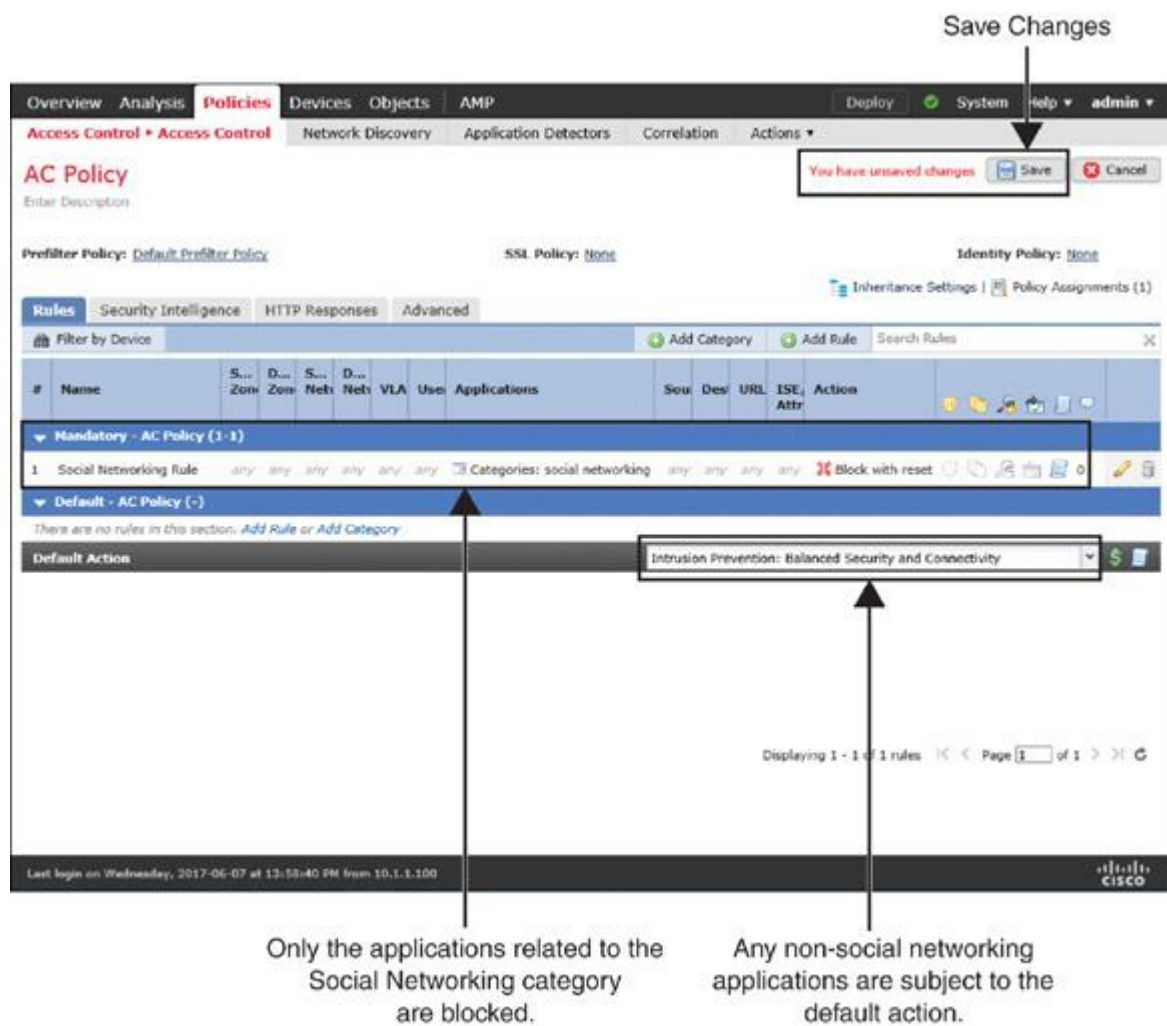


Figure 19-18 Access Control Policy Editor Page

Step 10. Finally, on the policy editor page, click **Save** to save the configurations, and click **Deploy** to deploy the policy on an FTD device.

Verification and Troubleshooting Tools

After deploying the policy that you created earlier in this chapter, in this section you'll try to access the Facebook application once again. This time the connection should be blocked.

[Figure 19-19](#) shows two types of connections to the Facebook application. When a connection is allowed, it hits the default action. However, when the social networking rule finds a match, it inspects the connection and blocks with reset packets.

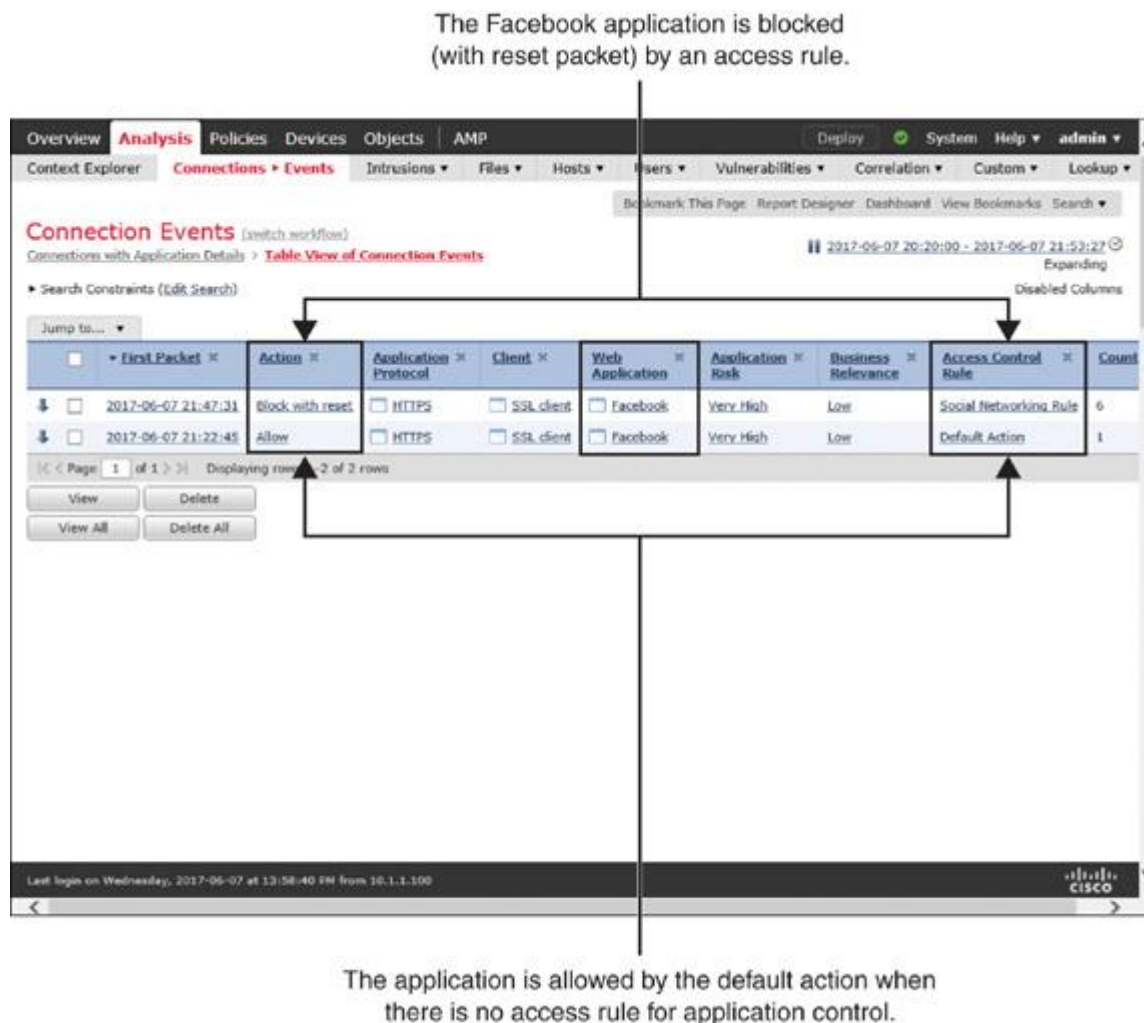


Figure 19-19 Connection Events Displaying the Actions of Application Control

[Example 19-1](#) shows the debugging data generated by the firewall engine. It confirms that FTD is able to detect facebook.com and then applies the rule action to block with reset.

Example 19-1 Debugging Messages Generated by the Firewall Engine

[Click here to view code image](#)

> **system support firewall-engine-debug**

Please specify an IP protocol: **tcp**

Please specify a client IP address:

Please specify a client port:

Please specify a server IP address:

Please specify a server port:

Monitoring firewall engine debug messages

172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 New session

172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 Starting with minimum 2, 'Social Networking Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff

172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 pending rule order 2, 'Social Networking Rule', AppId

172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 Starting with minimum 2, 'Social Networking Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff

172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 pending rule order 2, 'Social Networking Rule', AppId

172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 Starting with minimum 2, 'Social Networking Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff

172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 pending rule order 2, 'Social Networking Rule', AppId

172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 URL SI: ShmDBLookupURL ("www.facebook.com") returned 0

172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 Starting with minimum 2, 'Social Networking Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 1122, payload 629, client 1296, misc 0, user 9999997, url www.facebook.com, xff

```
172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 match rule order 2,
```

```
'Social Networking Rule', action Reset
```

```
172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 reset action
```

```
172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 Deleting session
```

[Example 19-2](#) shows the debugging of application data generated by the Firepower engine. It displays the identification number (appID) of the application that is detected by the FTD device.

Example 19-2 *Debugging Messages for Application Identification*

[Click here to view code image](#)

```
> system support application-identification-debug
```

```
Please specify an IP protocol: tcp
```

```
Please specify a client IP address:
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring application identification debug messages
```

```
.
```

```
.
```

```
172.16.100.110-4677 -> 31.13.65.36-443 6 R AS 4 I 1 port service 0
```

```
172.16.100.110-4677 -> 31.13.65.36-443 6 AS 4 I 1 3rd party returned 847
```

```
172.16.100.110-4677 -> 31.13.65.36-443 6 AS 4 I 1 SSL is service 1122,
```

```
portServiceAppId 1122
```

```
172.16.100.110-4677 -> 31.13.65.36-443 6 AS 4 I 1 ssl returned 10
```

```
172.16.100.110-4677 -> 31.13.65.36-443 6 AS 4 I 1 appId: 629
```

```
(safe)search_support_type=NOT_A_SEARCH_ENGINE
```

```
^C
```

```
Caught interrupt signal
```

```
Exiting
```

[Example 19-3](#) shows a query from the FMC database. It retrieves the mapping of the appID with an associated application name (appName). It confirms that the FTD device was able to identify the Facebook application correctly.

Example 19-3 *Mapping Application ID with an Application Name*

[Click here to view code image](#)

```
admin@FMC:~$ sudo OmniQuery.pl -db mdb -e "select appId,appName from
appIdInfo where
```

```
appId=629";
```

Password:

```
getting filenames from [/usr/local/sf/etc/db_updates/index]
```

```
getting filenames from [/usr/local/sf/etc/db_updates/base-6.1.0]
```

```
+-----+-----+
| appId | appName |
+-----+-----+
| 629   | Facebook|
+-----+-----+
```

```
-----
OmniQuery v2.1
(c) 2016 Cisco Systems, Inc.
.::~.:.
-----
```

```
mdb> exit
admin@FMC:~$
```

Summary

This chapter describes how the Firepower System can make you aware of the applications running on your network and empower you to control access to any unwanted applications. It also shows how to verify whether an FTD device can identify an application properly.

Quiz

1. Which of the following statements is true?

- A network discovery policy allows you to exclude network addresses but not any port numbers.
- You cannot determine the number of unique hosts identified by a Firepower system until it reaches the license limit.
- If a prefilter policy or an access control policy is configured to block any particular traffic, FTD does not evaluate the traffic further against a network discovery policy.
- All of the above.

[2.](#) Which of the following commands provides the ID for a discovered application?

- a. **system support app-id-debug**
- b. **system support firewall-debug**
- c. **system support firepower-engine-debug**
- d. **system support application-identification-debug**

[3.](#) Which of the following can affect the accuracy of network discovery?

- a. Snort rule database
- b. URL Filtering database
- c. Vulnerability Database
- d. Discovery event database

[4.](#) To improve the performance of network discovery, which of the following should you consider?

- a. Ensure that the network discovery policy is set to monitor the load balancer devices.
- b. Use the network address 0.0.0.0/0 and ::/0 in any discovery rules you create.
- c. Enable Firepower Recommendations in an intrusion policy.
- d. Keep the Vulnerability Database (VDB) version up to date.

Chapter 20

Controlling File Transfer and Blocking the Spread of Malware

As a security professional, you might not want your users to download and open random files from the Internet. While you allow your users to visit certain websites, you might want to block their attempts to download files from the sites they visit or to upload files to external websites. Unsafe downloads can spread viruses, malware, exploit kits, and other dangers on your network, and they can make the entire network vulnerable to various types of attacks. Likewise, to comply with the policy of your organization, you might not want your users to upload any particular types of files to the Internet from your corporate network.

The Firepower system enables you to block the download and upload of files based on file type (extension) and suspicious activity (malware).

File Policy Essentials

To govern the transfer of a file within a network, the Firepower System offers a standalone policy known as a *file policy*. A file policy allows you detect any file type, such as media files (.mp3, .mpeg), executable files (.exe, .rpm), and so on. In addition, an FTD device can analyze a file for potential malware when the file traverses a network. By design, FTD can detect and block files with a particular type before it performs lookups for malware.

[Figure 20-1](#) shows an architectural diagram of the Firepower engine. The figure highlights both components of a file policy—file type control and malware analysis—which are described in the following sections.

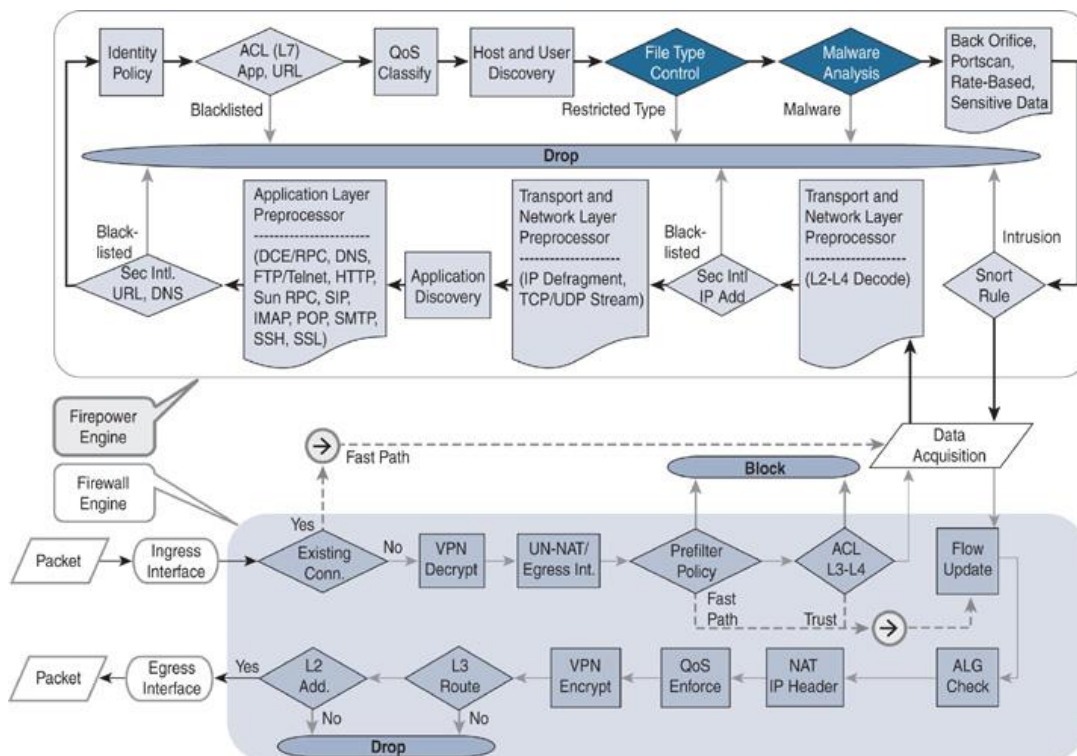


Figure 20-1 Placement of the File Policy Components in the Firepower Architecture

File Type Detection Technology

The Firepower System uses special metadata about a file, known as a magic number, to identify the file format. A magic number is a sequence of unique numbers that are encoded within files. When a file traverses a network, FTD can match the magic numbers from the stream of packets to determine the format of a file. For example, for a Microsoft executable (MSEXE) file, the magic number is 4D 5A. To find this number, Snort uses the following rule on FTD:

[Click here to view code image](#)

```
file type:MSEXE; id:21; category:Executables,Dynamic Analysis Capable,Local Malware Analysis Capable; msg:"Windows/DOS executable file "; rev:1; content:|4D 5A|; offset:0;
```

[Figure 20-2](#) demonstrates the magic number on a TCP packet. This packet is captured when a client downloads an executable file from a website. After completing the TCP three-way handshake, the server (172.16.100.100) sends this information to the client (192.168.1.200).

The screenshot shows a network packet capture tool interface. The main window displays a list of captured packets. Packet 8 is selected, showing a TCP segment of a reassembled PDU. The packet details pane shows the following information:

- Frame 8: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
- Ethernet II, Src: Vmware_fs:a9:6b (00:0c:29:f5:a9:6b), Dst: Apple_3c:98:a8 (c4:2c:03:3c:98:a8)
- Internet Protocol Version 4, Src: 172.16.100.100, Dst: 192.168.1.200
- Transmission Control Protocol, Src Port: 80, Dst Port: 47954, Seq: 1, Ack: 378, Len: 1448

The packet data pane shows the raw bytes of the packet. The magic number 4D 5A is highlighted in red and pointed to by a black arrow. The hex dump shows the following bytes:

```
0170 67 72 61 6d 0d 0a 0d 0a 4d 5a 90 00 03 00 00 00
0180 04 00 00 00 ff ff 00 00 58 00 00 00 00 00 00 00
0190 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Figure 20-2 Retrieval of the Magic Number from the Stream of Packets

Malware Analysis Technology

To empower a network with the latest threat intelligence, Cisco has integrated the Advanced Malware Protection (AMP) technology with the Firepower System. AMP enables an FTD

device to analyze a file for potential malware and viruses while the file traverses a network. To expedite the analysis process and to conserve resources, FTD can perform both types of malware analysis—local and dynamic. Let’s take a look at the technologies behind them.

[Figure 20-3](#) illustrates the purposes of any interactions between the Firepower System and the Cisco clouds.

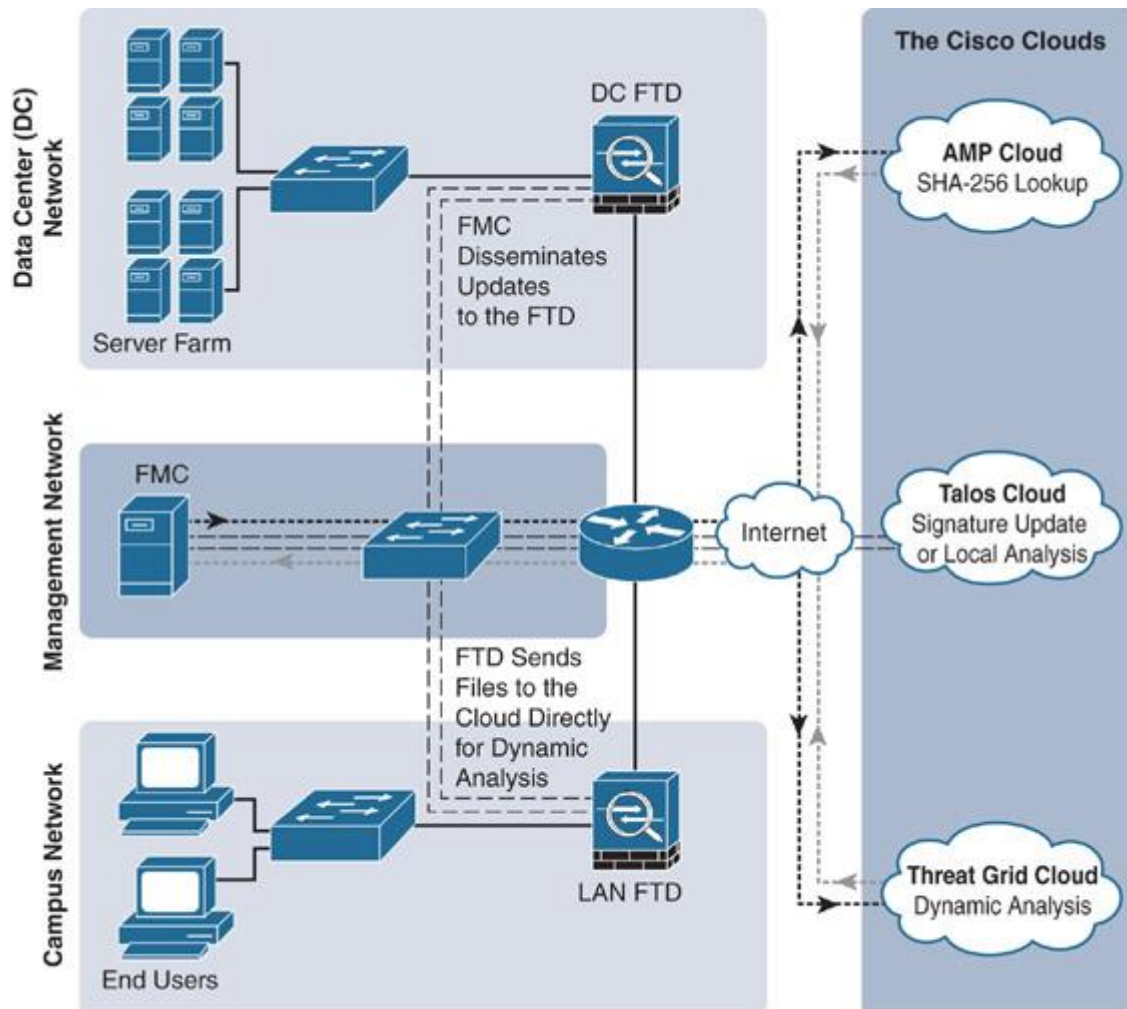


Figure 20-3 *Firepower Communications to the Cisco Clouds for Malware Analysis*

FTD calculates the SHA-256 hash value (Secure Hash Algorithm with 256 bits) of a file and uses the value to determine a disposition. The FMC performs a lookup on the cached disposition before it sends a new query to the AMP cloud. It provides a faster lookup result and improves overall performance. Depending on the action you select on a file policy, a Firepower system can perform additional advanced analysis in the following order:

- **Spero analysis:** The Spero analysis engine examines the MSEXE files only. It analyzes the structure of an MSEXE file and submits the Spero signature to the cloud.
- **Local analysis:** FTD uses two types of rulesets for local analysis: high-fidelity rules and preclassification rules. The FMC downloads high-fidelity malware signatures from Talos and

disseminates the rulesets to FTD. FTD matches the patterns and analyzes files for known malware. It also uses the file preclassification filters to optimize resource utilization.

■ **Dynamic analysis:** The dynamic analysis feature submits a captured file to the threat grid sandbox for dynamic analysis. A sandbox environment can be available in the cloud or on premises. Upon analysis, the sandbox returns a threat score—a scoring system for considering a file as potential malware. A file policy allows you to adjust the threshold level of the dynamic analysis threat score. Thus, you can define when an FTD device should treat a file as potential malware.

Dynamic analysis provides an option called capacity handling that allows a Firepower system to store a file temporarily if the system fails to submit the file to a sandbox environment. Some of the potential reasons for such a failure would be communication issues between Firepower and the sandbox (cloud or on premises), exceeding the limit for file submission, and so on.

Figure 20-4 shows an architectural workflow of the malware analysis techniques on a Firepower system.

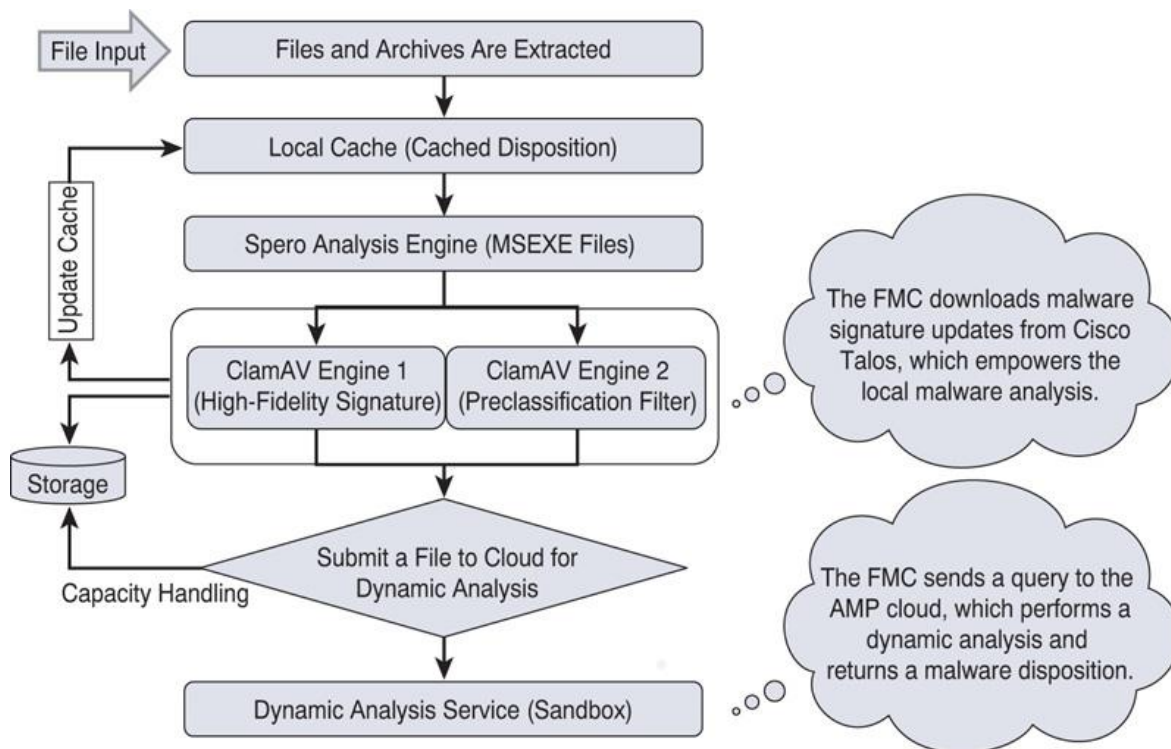


Figure 20-4 Architecture of the Advanced Malware Protection (AMP) Technology

Licensing Capability

With the installation of a Threat license, a Firepower system automatically enables the *file type control*. This means that if you are currently using the security intelligence and intrusion prevention features on an FTD device, you should be able to control the transfer of a particular file type without the need for any new license. However, to perform a malware analysis, Firepower requires an additional license, known as a Malware license.

[Figure 20-5](#) shows the actions and features you can enable by using the Threat and Malware licenses.

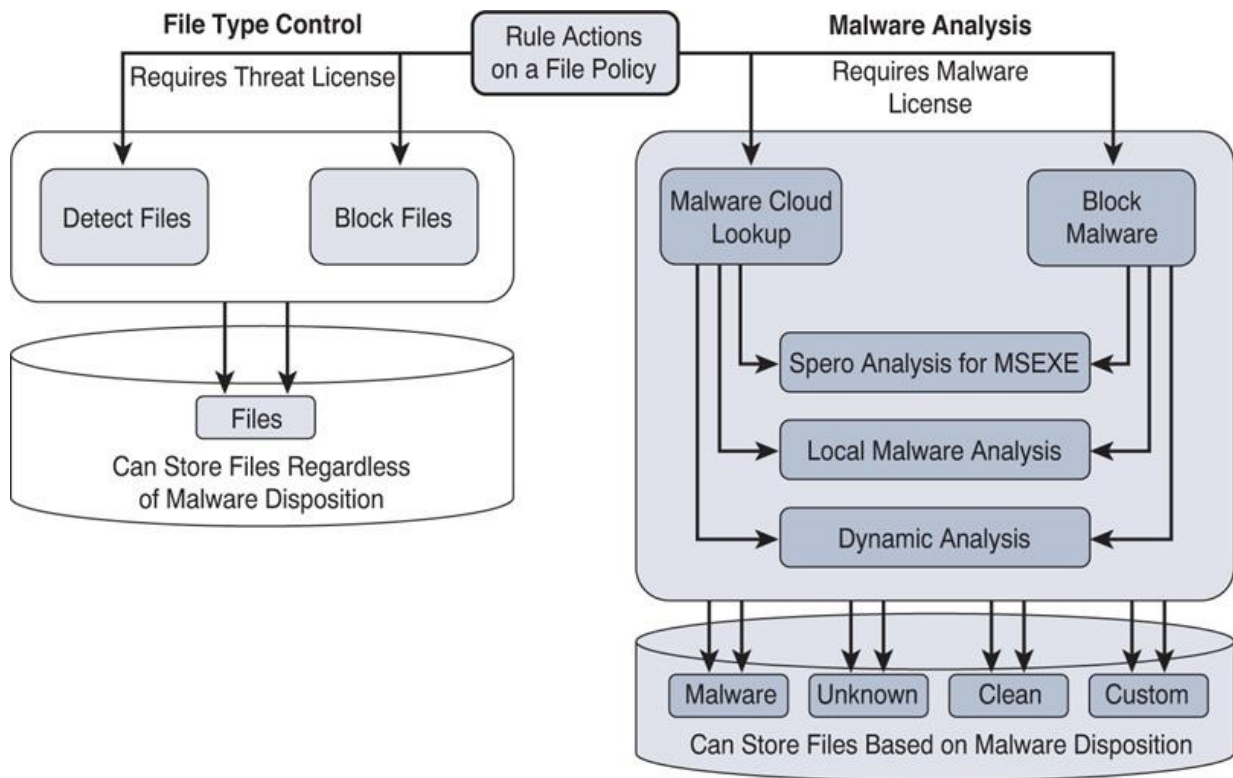


Figure 20-5 Actions on a File Rule and Their Necessary Licenses

[Table 20-1](#) summarizes the differences between the capabilities of a Threat license and a Malware license.

Table 20-1 Differences Between a Threat License and a Malware License

When Only a Threat License Is Applied...

FTD can block a file based on its file type.

FTD utilizes the file’s magic numbers to determine the file type.

FTD does not require a connection to the cloud for file type detection.

You can apply only two rule actions: Detect Files and Block Files.

When a Malware License Is Also Applied...

FTD can block a file based on its malware dispositions.

FTD matches malware signatures to perform local malware analysis.

It needs to connect to the cloud for various purposes—for example, to update signature of the latest malware, to send a file to the cloud to perform dynamic file analysis, and to perform a SHA-256 lookup.

You can apply any rule actions available, including Malware Cloud Lookup and Block Malware.

Best Practices for File Policy Deployment

You should consider the following best practices when you configure a file policy:

- When you want to block a file by using file policy, use the Reset Connection option. It allows an application session to close before the connection times out by itself.
- If you want to download a captured file to your desktop, make sure you take extra precautions on your desktop before you download. The file might be infected with malware that could be harmful to your desktop.
- Keep the file size limit low to improve performance. An access control policy allows you to limit the file size. It can impact the following activities:
 - Sending a file to the cloud for dynamic analysis
 - Storing a file locally
 - Calculating the SHA-256 hash value of a file
- In case of a communication failure between the Firepower System and the Cisco clouds, FTD can hold the transfer of a file for a short period of time when the file matches a rule with the Block Malware action. Although this holding period is configurable, Cisco recommends that you use the default value.

[Figure 20-6](#) displays the advanced settings of an access control policy in which you can define the file holding period and file size limits.

The screenshot shows the 'Advanced' settings for an AC Policy. The 'Files and Malware Settings' section is expanded, showing the following configuration:

Setting	Value
Limit the number of bytes inspected when doing file type detection	1460
Allow file if cloud lookup for Block Malware takes longer than (seconds)	2
Do not calculate SHA256 hash values for files larger than (in bytes)	10485760
Minimum file size to store (bytes)	5144
Maximum file size to store (bytes)	1048576
Minimum file size for dynamic analysis testing (bytes)	0
Maximum file size for dynamic analysis testing (bytes)	104857600

Arrows from the labels 'File Holding Period' and 'File Size Limits' point to the 'Allow file if cloud lookup for Block Malware takes longer than (seconds)' and the 'Do not calculate SHA256 hash values for files larger than (in bytes)' setting, respectively.

Figure 20-6 Configuration of the File Holding Period and File Size Limits

Fulfilling Prerequisites

The following items are necessary for a successful file policy deployment:

- Make sure to install an appropriate license. To control the transfer of a particular file type, only a Threat license is necessary. To perform malware analysis, an additional Malware license is required.
- A file policy uses the adaptive profile feature. Make sure the feature is enabled in the advanced settings of an access control policy (see [Figure 20-7](#)).

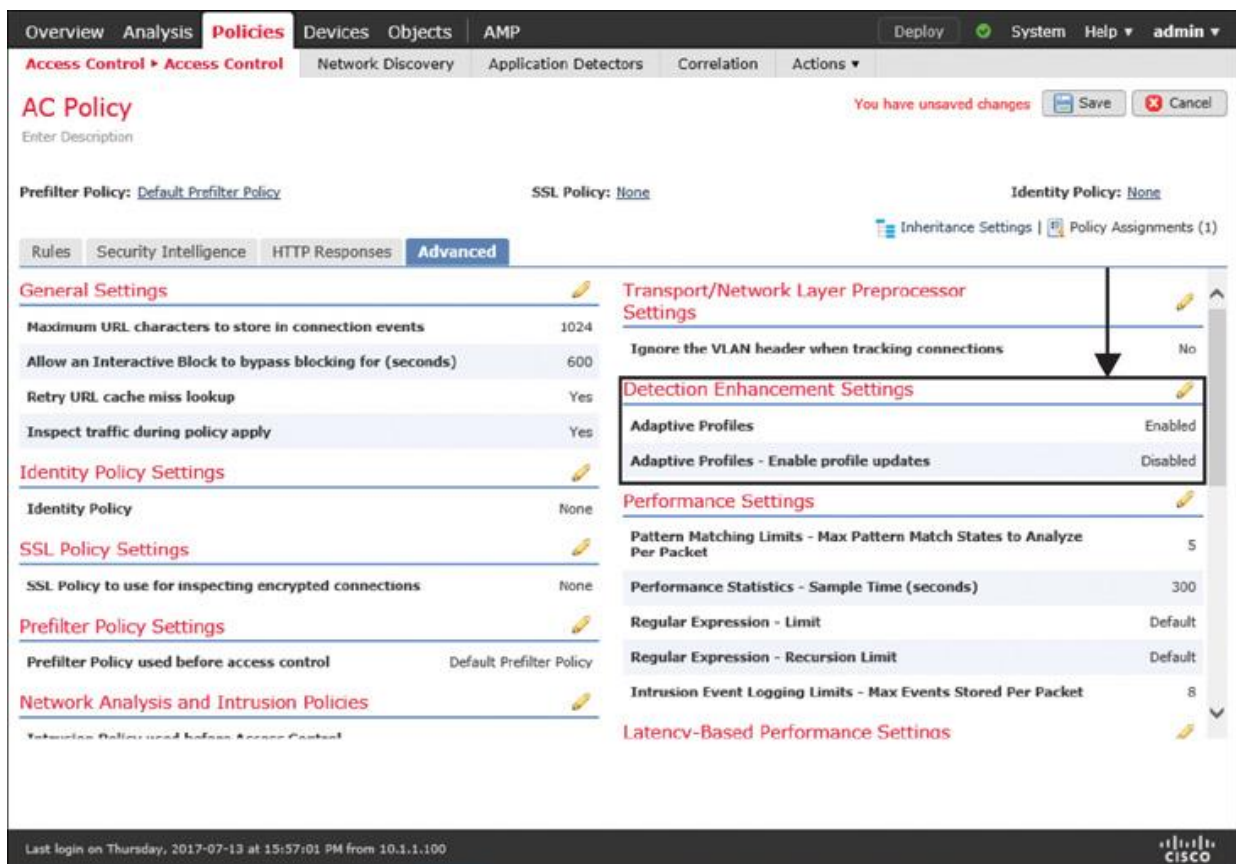


Figure 20-7 Option to Enable Adaptive Profile Updates

■ Make sure the Enable Automatic Local Malware Detection Updates option is checked (see [Figure 20-8](#)). It allows the FMC to communicate with Talos cloud every 30 minutes. When a new ruleset is available, the FMC downloads it to enrich the local malware analysis engine.

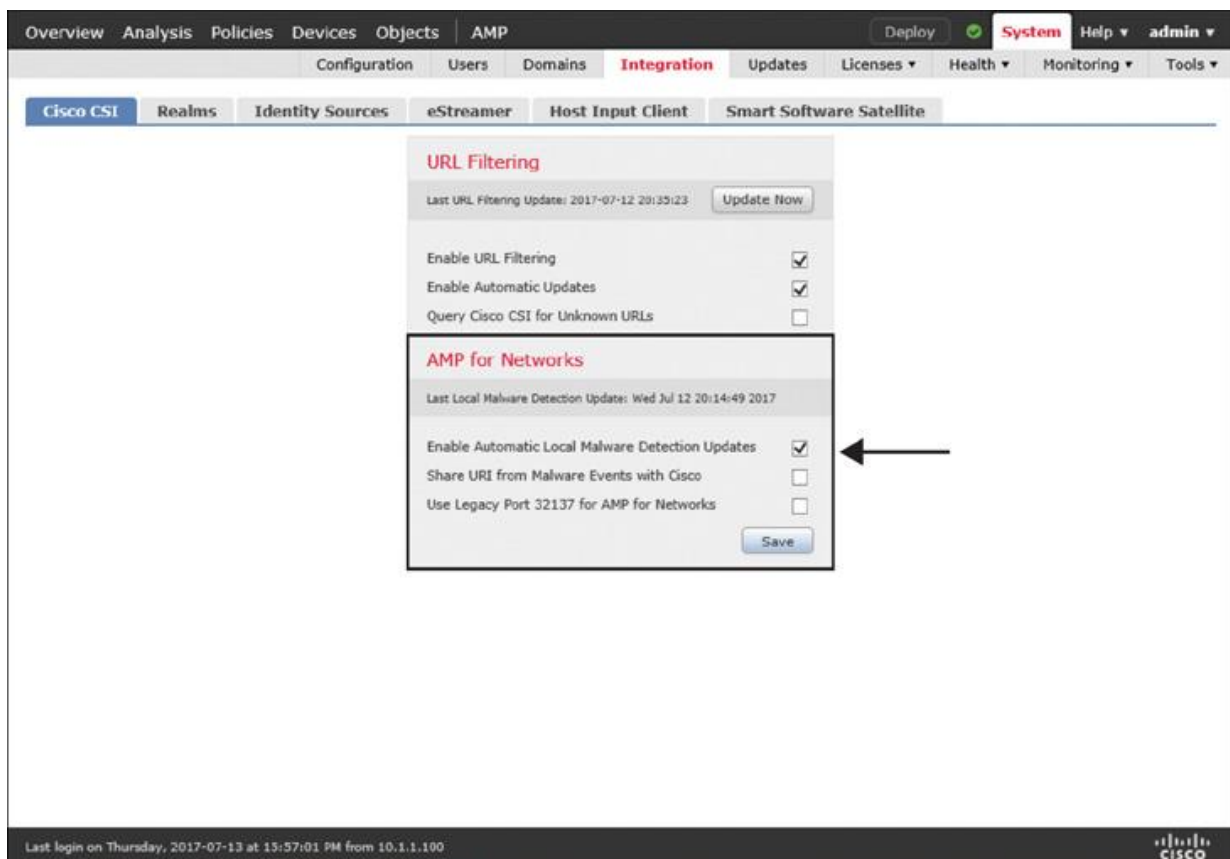


Figure 20-8 Option to Enable the Automatic Local Malware Detection Updates

■ A file policy leverages the application detection functionality to determine whether an application is capable of carrying a file. Make sure a network discovery policy is deployed to discover applications. To learn about application detection and control, read [Chapter 19](#), “[Discovering Network Applications and Controlling Application Traffic](#).”

Configuring a File Policy

Deployment of a file policy is a multistep process. First, you need to create a file policy and add any necessary file rules to it. A file rule allows you to select the file type category, application protocol, direction of transfer, and action. However, you cannot add any source or destination details on a file rule. To assign network addresses, you need to create an access rule within an access control policy and invoke the file policy within the access rule.

Creating a File Policy

To create a file policy, follow these steps:

Step 1. Navigate to **Policies > Access Control > Malware & File**. The Malware & File Policy page appears.

Step 2. Click the **New File Policy** button, and the New File Policy window appears (see [Figure 20-9](#)).

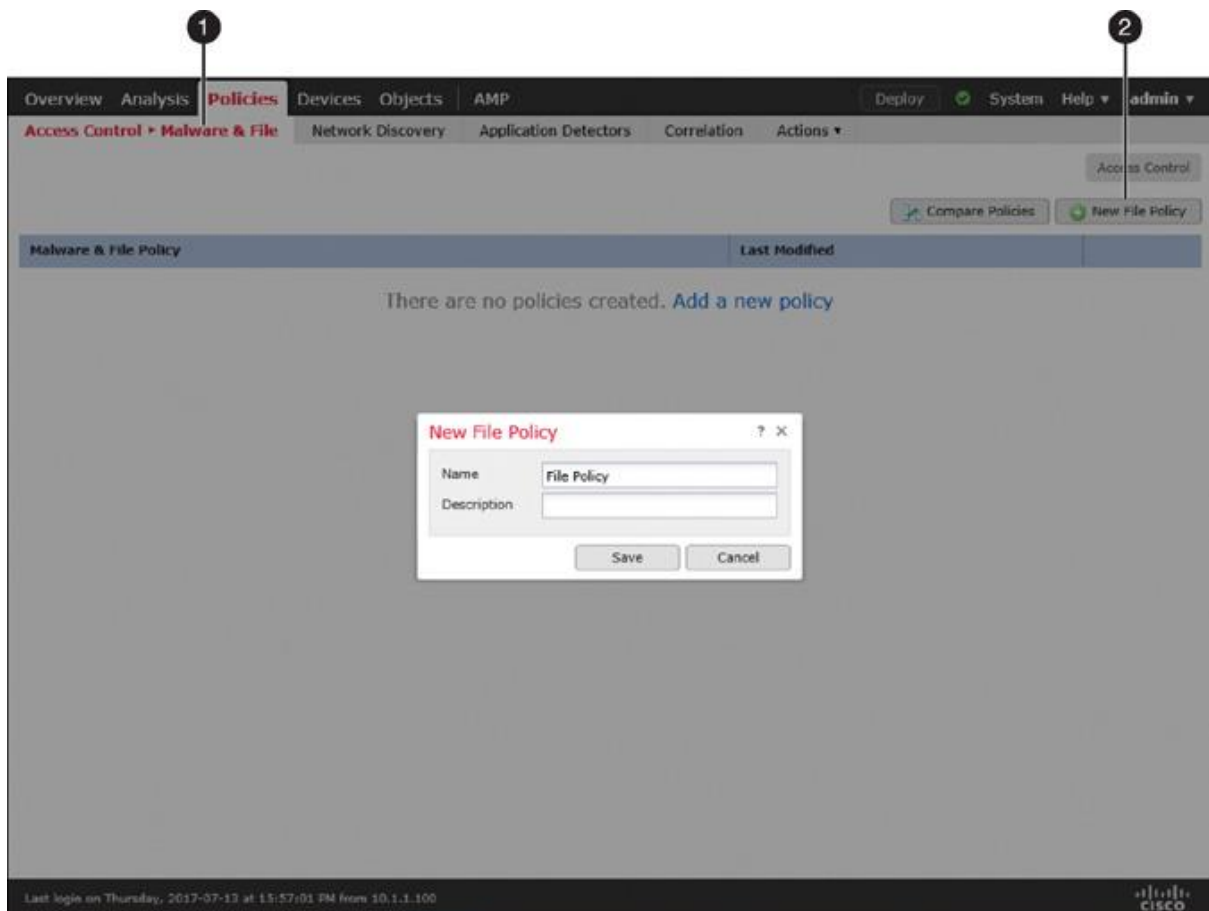


Figure 20-9 *Creating a New File Policy*

Step 3. Give a name to the policy and click the **Save** button. The file policy editor appears.

Step 4. Click the **Add Rule** button. The file rule editor appears.

Step 5. Select **Any** from the Application Protocol dropdown to detect files over multiple application protocols.

Step 6. Make a selection from the Direction of Transfer dropdown. Depending on the underlying application protocol for a file transfer, the direction can be limited. For example, the HTTP, FTP or NetBIOS-ssn (SMB) protocol allows any direction—upload or download. However, SMTP (upload only) and POP3/IMAP (download only) support unidirectional transfer.

[Figure 20-10](#) explains the reasons for unidirectional transfer with the SMTP, POP3, and IMAP protocols. While SMTP is used for outbound transfers, POP3/IMAP is used to download incoming emails and any attachments.

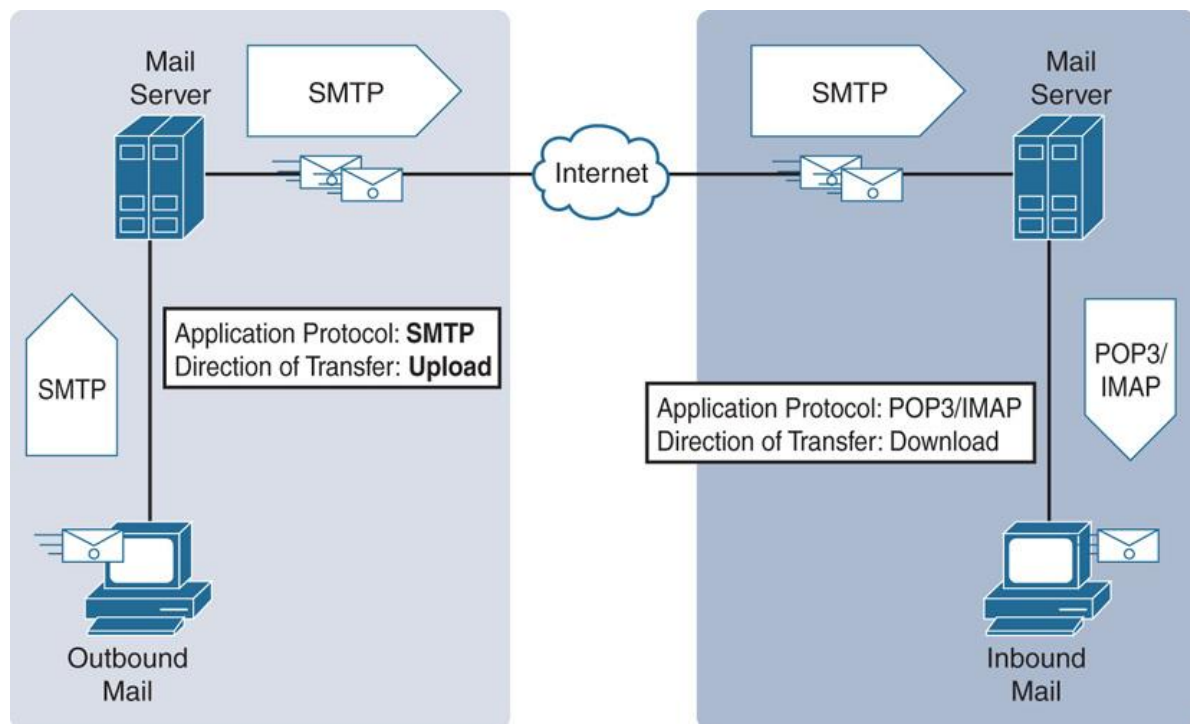


Figure 20-10 *Directions of Protocols Associated with Inbound and Outbound Emails*

Step 7. Select the file type categories you want to block, and click **Add** to add them to the rule. You can also search for a specific file type directly.

Step 8. Select an action from the Action dropdown. The following options are available:

Note

A file policy does not evaluate a file rule based on its position; rather, it uses the order of actions. The order of actions is Block Files, Block Malware, Malware Cloud Lookup, and Detect Files. When performing an advanced analysis, FTD engages Spero analysis, local malware analysis, and dynamic analysis, successively—if you have enabled all of them in a particular file rule.

■ **Detect Files:** This action detects a file transfer and logs it as a file event without interrupting the transfer.

■ **Block Files:** This action blocks certain files—depending on the file formats selected on a file rule.

Tip

If you want to block a file, select the **Reset Connection** option. It allows an application session to close before the connection times out by itself.

■ [Figure 20-11](#) displays a file rule that blocks the transfer of any system, executable, encoded, and archive files without analyzing them for malware. According to the configuration, when a file matches this rule, FTD stores the file on local storage and sends reset packets to terminate any associated connection.

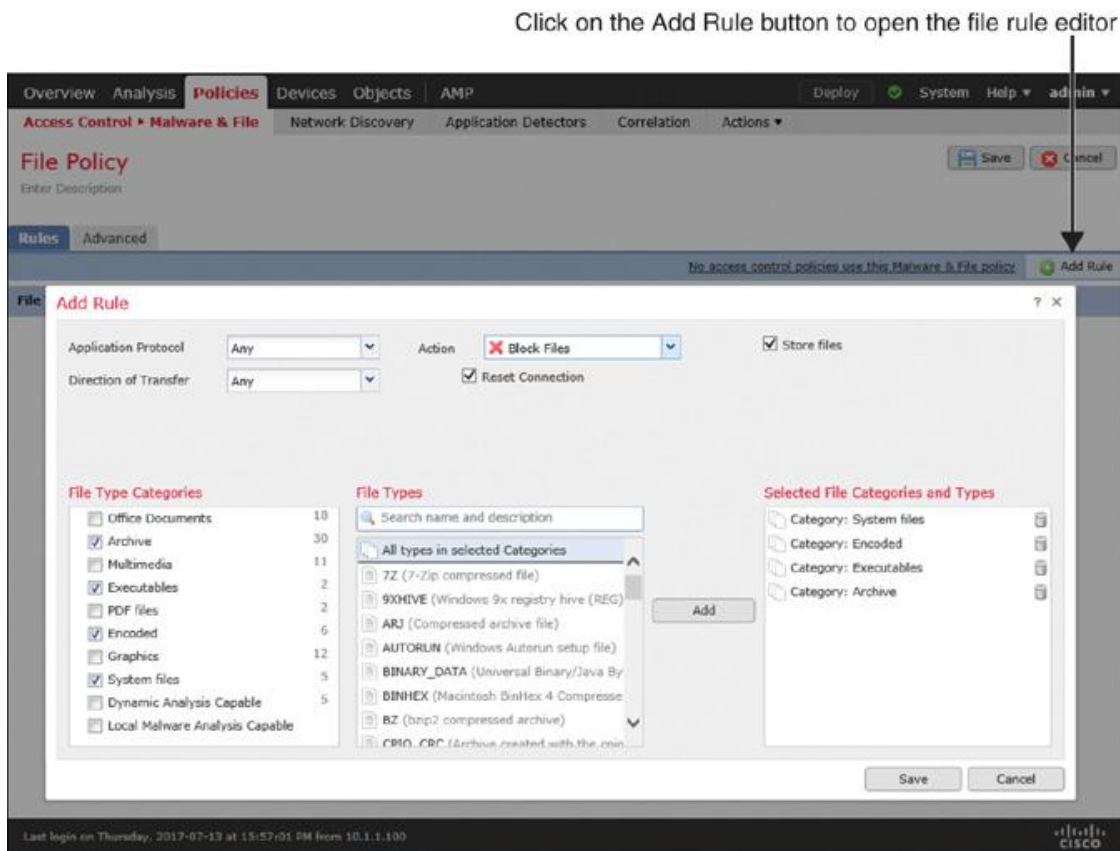


Figure 20-11 File Rule with the Block Files Action

■ [Figure 20-12](#) shows the creation of two file rules. The first rule blocks system, encoded, executable, and archive files with reset packets and stores the blocked file in local storage. The second rule detects the graphic, PDF, multimedia, and Office document files but does not block or store them as they traverse the network.

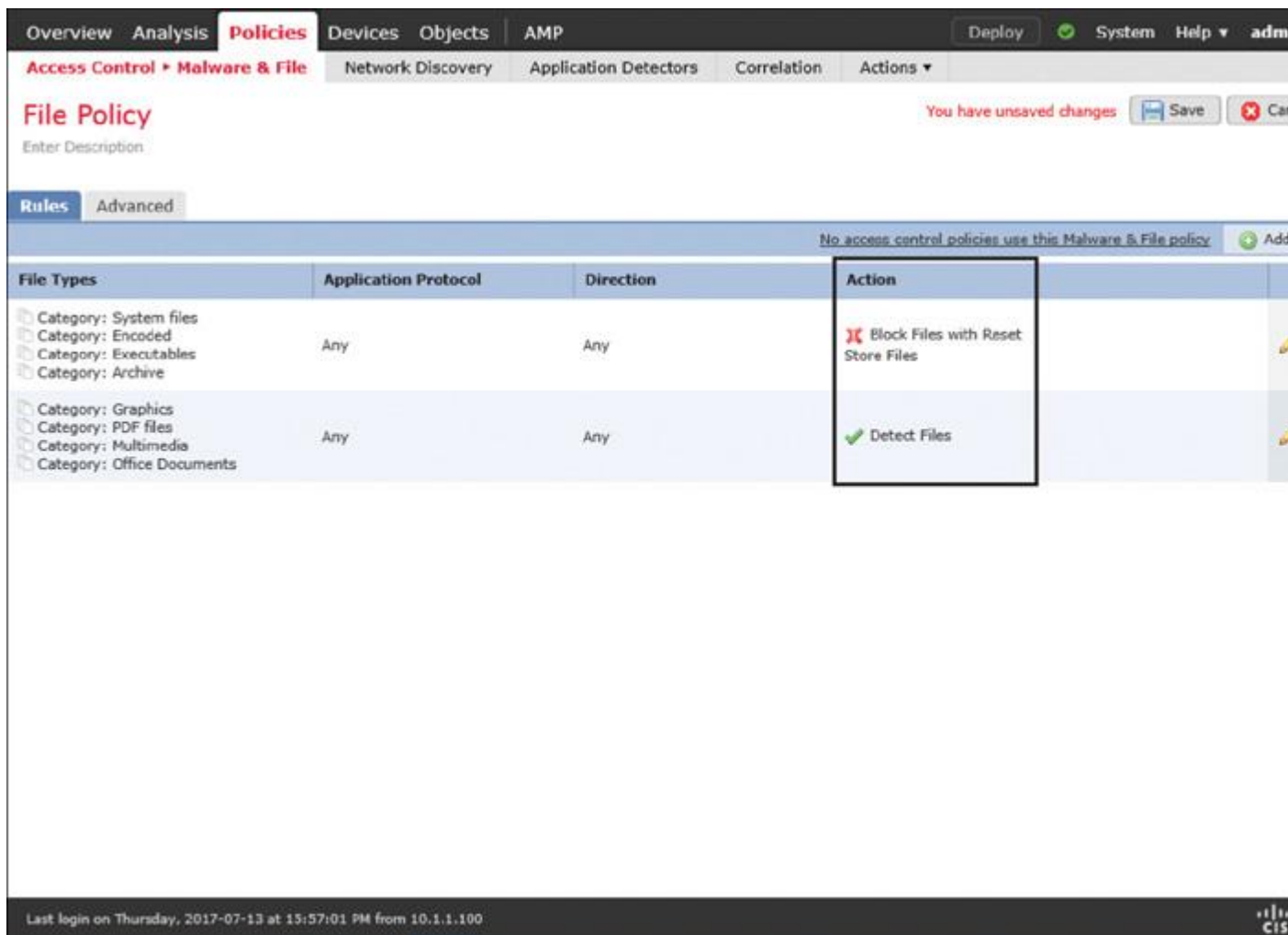


Figure 20-12 Two File Rules for Different File Types Applying Different Actions

■ **Malware Cloud Lookup:** This action enables an FTD device to perform malware analysis locally and remotely. FTD allows an uninterrupted file transfer regardless of the malware disposition.

■ **Block Malware:** This action performs the same tasks as the Malware Cloud Lookup action, with an addition of blocking the original file if the disposition is determined to be malware.

Note

When you select the Malware Cloud Analysis or Block Malware action, the Firepower System offers various analysis methods. Read the previous section for more information on malware analysis methodologies.

[Figure 20-13](#) shows another option for a file rule (which requires a Malware license). This rule enables an FTD device to block the transfer of a file and to store it locally if the file has one of three criteria: infected with malware, disposition is unknown, or matches a custom detection list. When blocking the file transfer, FTD sends reset packets to terminate any associated connection. This rule does not allow an FTD device to store a file if the file appears to be clean. It prevents storage from getting full of clean or benign files.

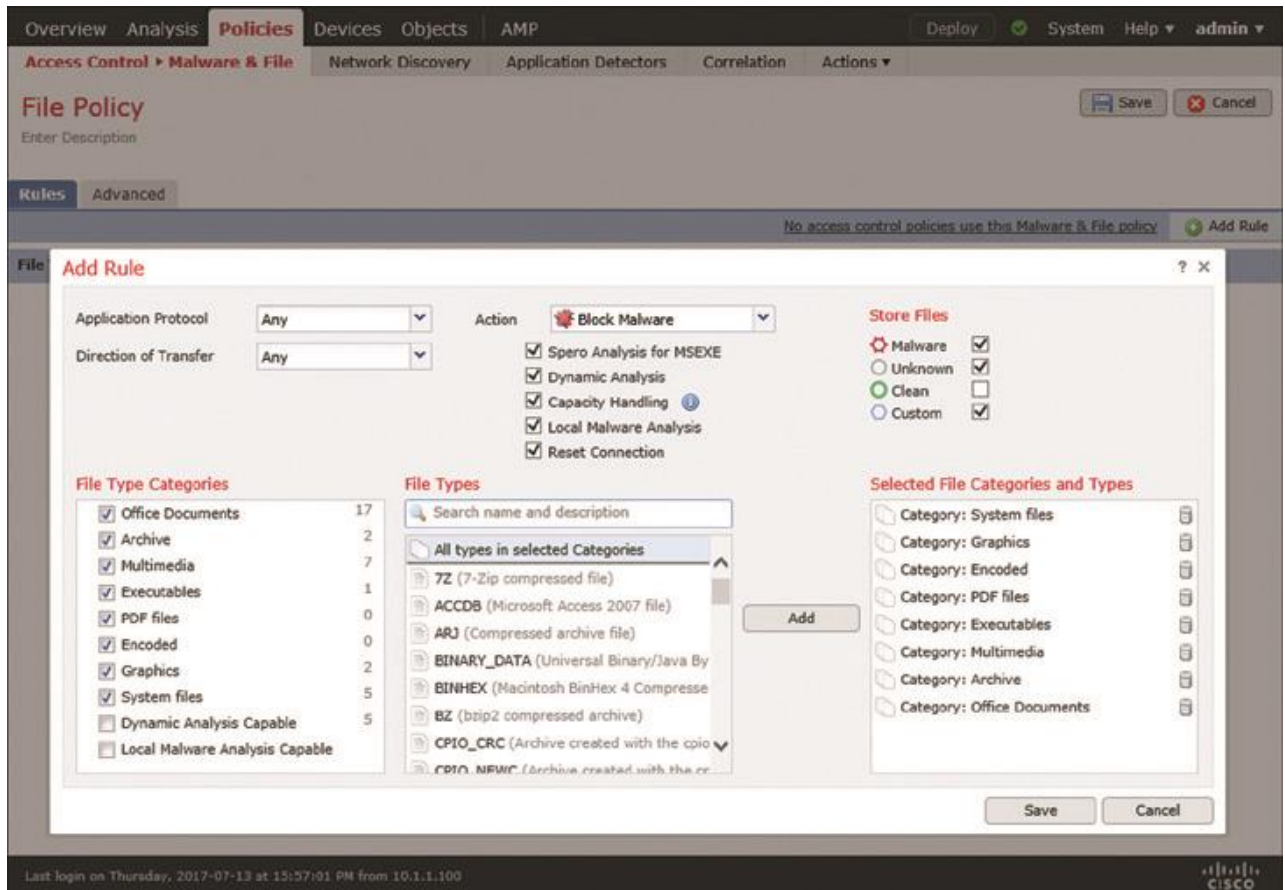


Figure 20-13 File Rule with a Block Malware Action

Step 9. Optionally, on the Advanced tab, you can enable additional features for advanced analysis and inspection. [Figure 20-14](#) shows the advanced settings of a file policy. For example, here you can adjust the threshold level of the dynamic analysis threat score, enable inspection for the archived contents, define the depth of inspection for a nested archive file, and so on.

A lower threat score increases the number of files that are going to be considered malware.

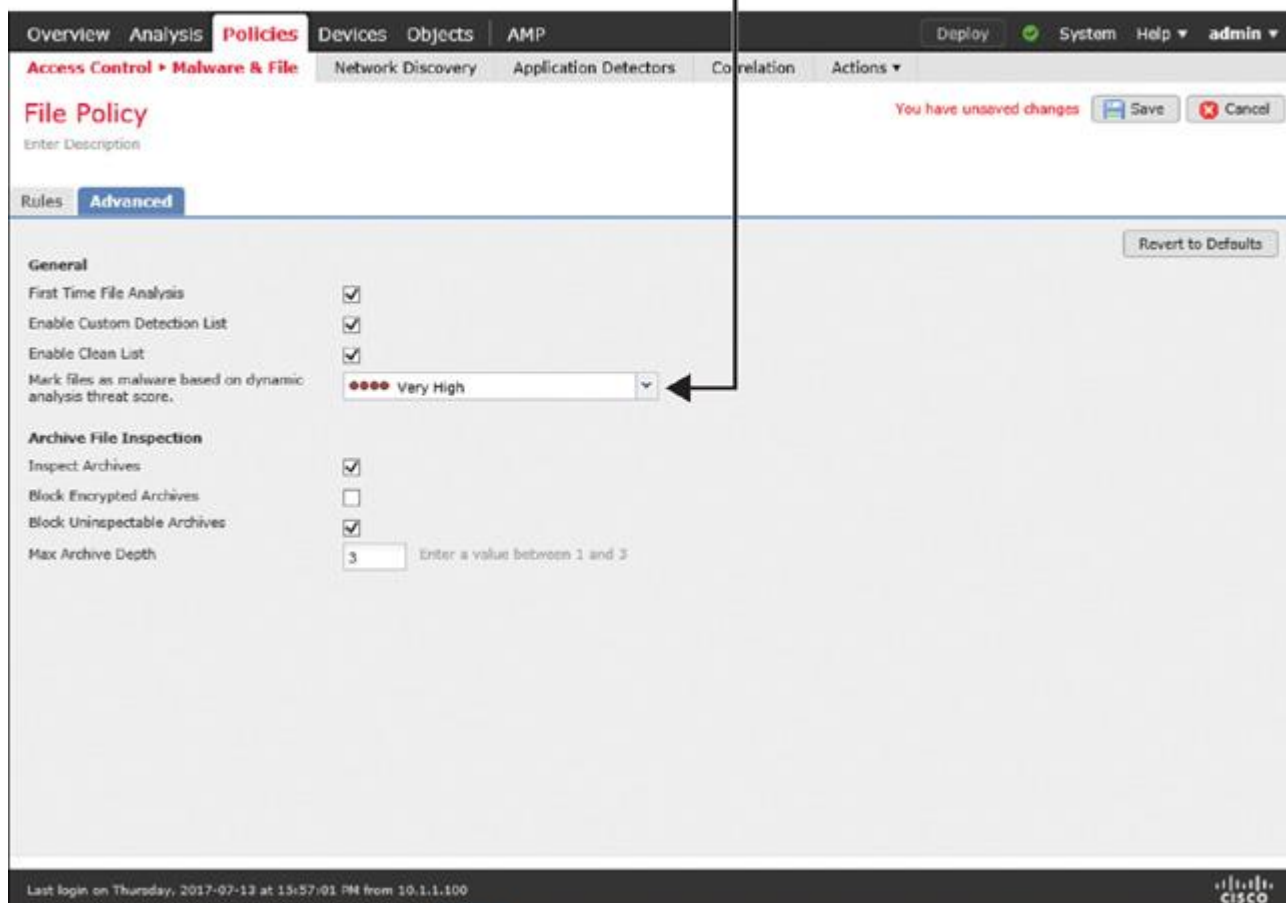


Figure 20-14 *Advanced Settings of a File Policy*

Step 10. Click the **Save** button on the policy editor to save the changes on the file policy.

Applying a File Policy

To apply a file policy on an FTD device, you need to create an access rule within an access control policy and invoke the file policy in the access rule. Here are the detailed steps:

Step 1. Navigate to **Policies > Access Control > Access Control**. The available access control policies appear. You can modify one of the existing policies or click **New Policy** to create a new one.

Step 2. On the policy editor page, use the pencil icon to modify an existing access rule to invoke a file policy. If there are no rules created, click the **Add Rule** button to create a new access rule.

Step 3. On the rule editor window, go to the Inspection tab. You will notice dropdowns for Intrusion Policy, Variable Set, and File Policy. [Figure 20-15](#) shows the dropdowns on the Inspection tab. The file policy you configured earlier should populate here, under the File Policy dropdown.

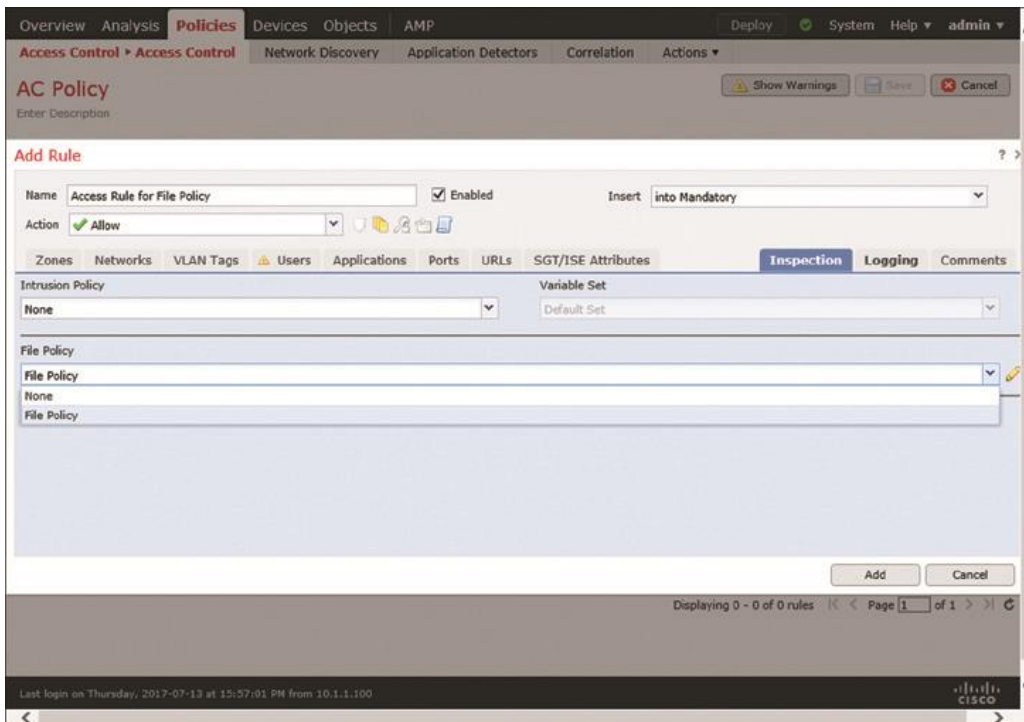


Figure 20-15 *Selecting a File Policy for an Access Rule*

Step 4. Choose a policy from the File Policy dropdown. Doing so automatically enables logging for the file event. You can verify it by viewing the settings on the Logging tab (see [Figure 20-16](#)). To view events for each connection that matches a particular access rule condition, you can manually enable Log at Beginning of Connection.

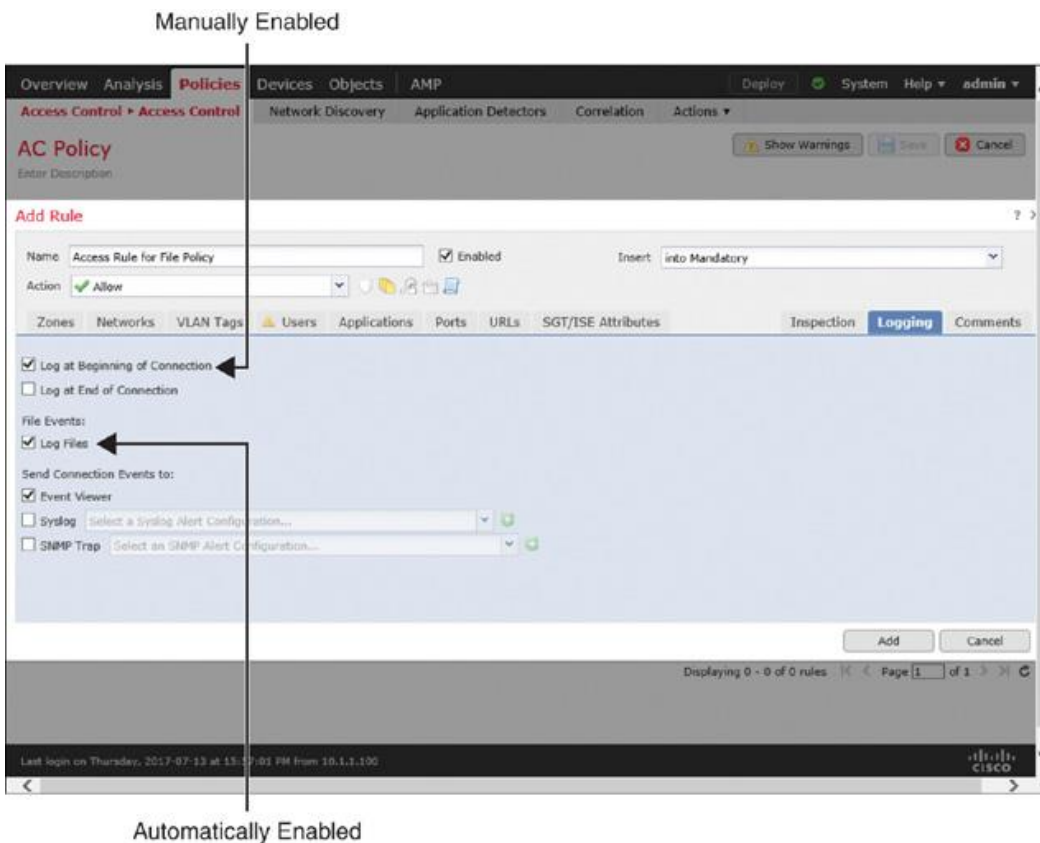


Figure 20-16 Options to Enable Logging for File Events and Connection Events

Step 5. Click the **Add** button to save the changes. You are returned to the access control policy editor page. If you are editing an existing access rule, you can click the **Save** button instead.

Step 6. On the access control policy editor page, select a default action. You cannot select a file policy as the default action of an access control policy. You can only invoke a file policy within an individual access rule.

Step 7. Finally, click **Save** to save the changes, and click **Deploy** to deploy the configuration to the FTD device.

Verification and Troubleshooting Tools

A file policy can generate two types of events: file events and malware events. FTD generates a *file event* when it detects or blocks a certain type of file without a malware lookup. FTD generates a *malware event* when it performs an analysis for malware or blocks a file due to malware disposition.

The following sections of this chapter demonstrate the operation of both policies—file type detection and malware analysis. In this scenario, a client downloads files with two different formats—Microsoft executable (MSEXE) file format and Portable Document Format (PDF). As a security engineer, you need to verify whether a file policy is operational and whether the transfer of files complies with the active file policy.

[Figure 20-17](#) shows the topology that is used in the configuration examples in this chapter. To demonstrate various scenarios, the client computer (192.168.1.200) downloads different files from a web server (172.16.100.100), and the FTD device in the LAN acts on them.

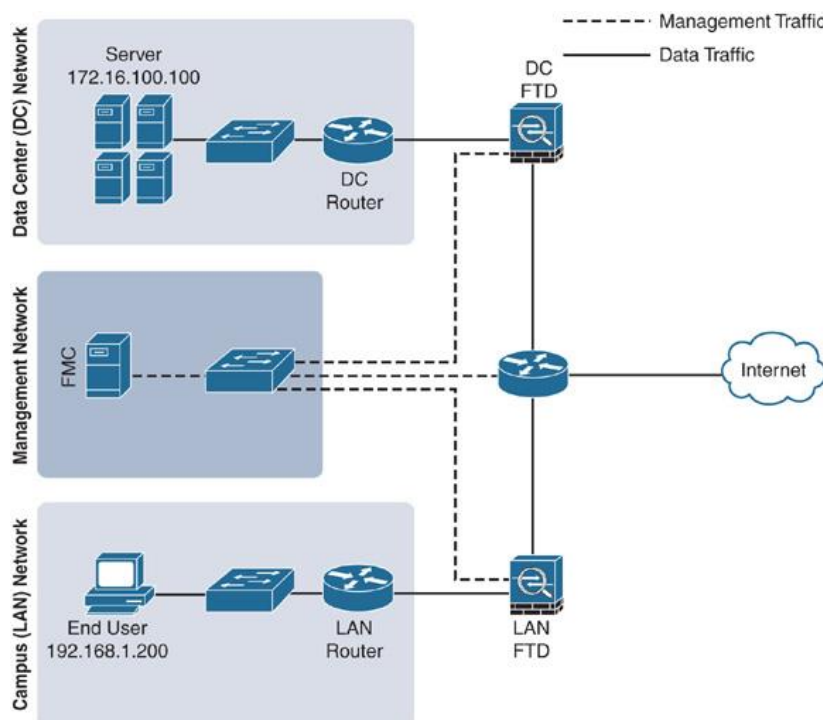


Figure 20-17 *Topology Used in This Chapter*

Analyzing File Events

Using a web browser on your client computer, you can attempt to download two files—7z1700.exe and userguide.pdf—from a web server. If the FTD device is running the following file policy, it should block the download of the 7z1700.exe file and allow and detect the download of userguide.pdf.

[Figure 20-18](#) shows the currently enabled rules on a file policy. The first rule detects and blocks files in four categories, and the second rule only detects files in four different categories.

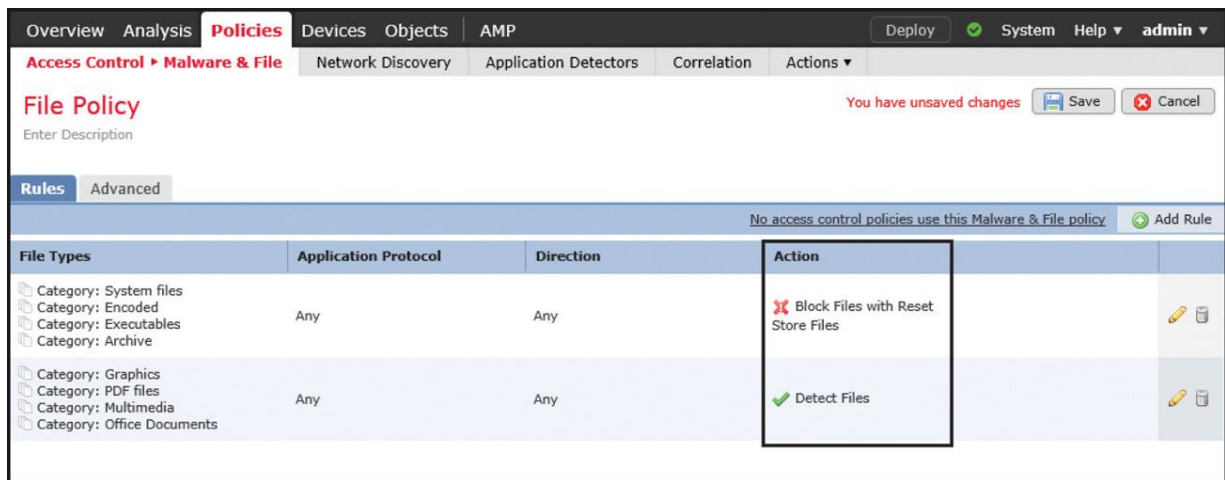


Figure 20-18 *Overview of the Active Rules Used in This Exercise*

Navigate to **Files > File Events** to view the file events. By default, the FMC shows the File Summary page. However, to find useful contextual information about file events, you should also check the Table View of File Events page.

[Figure 20-19](#) confirms the blocking and detection of an MSEXE file and a PDF file. Because the Block Files action does not perform malware analysis, the Disposition column is blank.

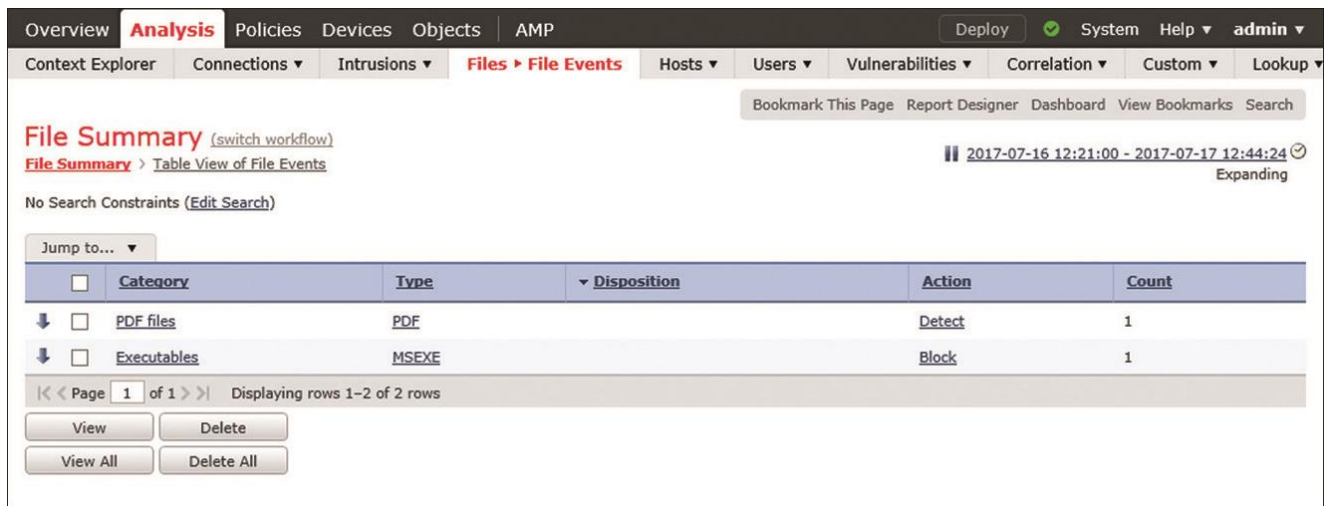


Figure 20-19 Summary View of File Events

[Figure 20-20](#) shows detailed information about the detected and blocked files and their associated source and destination hosts. The SHA256 and Threat Score columns are blank because the FTD device does not perform any kind of malware analysis but detects file type only.

	Time	Action	Sending IP	Receiving IP	File Name	SHA256	Threat Score	Type	Category	Count
↓	2017-07-17 12:37:29	Detect	172.16.100.100	192.168.1.200	userguide.pdf			PDF	PDF files	1
↓	2017-07-17 12:23:35	Block	172.16.100.100	192.168.1.200	7z1700.exe			MSEXE	Executables	1

Figure 20-20 Table View of File Events

[Figure 20-21](#) shows the data of file events visually in various widgets. To find this dashboard, go to **Overview > Dashboards > Files Dashboard**.

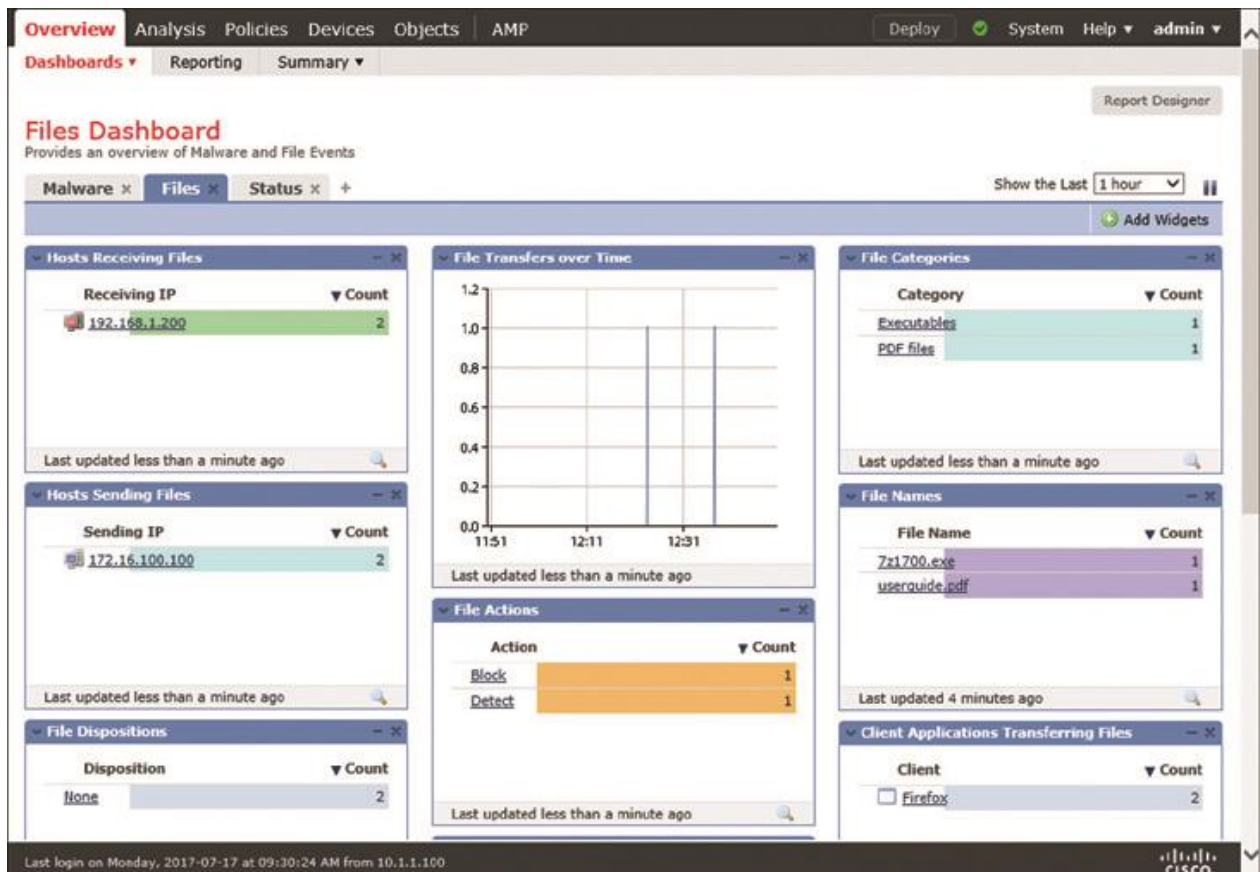


Figure 20-21 Dashboard of File Events

If you do not see a file event that you expected to see, you can use the CLI to debug the action of a file rule and verify the operation of a file policy. If you run the **system support firewall-engine-debug** command while you attempt to transfer a file, you see detailed logs associated with file inspection and analysis.

[Example 20-1](#) shows the detailed debugging messages that appear when a client computer attempts to download the executable file 7z1700.exe and the FTD device blocks it due to the actions Block Files, Reset Connection, and Store Files.

Example 20-1 Blocking a Microsoft Executable (MSEXE) File

[Click here to view code image](#)

! First, run the debug command and specify necessary parameters.

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.1.200
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages
```

! Now, begin the transfer of an executable file.

```
192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 New session
192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 using HW or preset rule order 2,
'Access Rule for File Policy', action Allow and prefilter rule 0
192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 allow action
192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 URL SI:
ShmDBLookupURL("http://172.16.100.100/files/7z1700.exe") returned 0
192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 File Policy verdict is Type,
Malware, and Capture
192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 File type verdict Unknown,
fileAction Block, flags 0x00203500, and type action Reject for type 21 of
instance 0
```

! At this stage, the file is being transferred through the FTD. The following messages appear after the file is stored on the FTD. FTD blocks the file transfer as soon as it detects the end-of-file marker on a packet.

```
192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 File type storage finished within signature using verdict Reject
```

```
192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 File signature reserved file data of partial file with flags 0x00203500 and status Exceeded Max Filesize
```

```
192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 File signature verdict Reject and flags 0x00203500 for partial file of instance 0
```

```
192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 File type event for file named 7z1700.exe with disposition Type and action Block
```

```
192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 Archive childs been processed No
```

```
192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 Deleting session
```

```
^C
```

```
Caught interrupt signal
```

```
Exiting.
```

```
>
```

[Example 20-2](#) shows the debugging messages that appears when a client computer downloads the file `userguide.pdf`. FTD generates a log, but it does not block the PDF file because the rule action is Detect Files.

Example 20-2 *Detecting a Portable Document Format (PDF) File*

[Click here to view code image](#)

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp
```

```
Please specify a client IP address: 192.168.1.200
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 New session

192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 Starting with minimum 0, id 0 and

SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged,

svc 0, payload 0, client 0, misc 0, user 9999997, url , xff

192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 match rule order 2, 'Access Rule

for File Policy', action Allow

192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 allow action

192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 URL SI:

ShmDBLookupURL("http://172.16.100.100/files/userguide.pdf") returned 0

192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 Starting with minimum 0, id 0 and

SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc

676, payload 0, client 638, misc 0, user 9999997, url <http://172.16.100.100/files/>

userguide.pdf, xff

192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 match rule order 2, 'Access Rule

for File Policy', action Allow

192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 allow action

.

<Output omitted for brevity>

.

192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 File policy verdict is Type,

Malware, and Capture

192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 File type verdict Log, fileAction

Log, flags 0x00001100, and type action Log for type 285 of instance 0

192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 File type event for file named

userguide.pdf with disposition Type and action Log

.

<Output omitted for brevity>

^C

Caught interrupt signal

Exiting.

>

Analyzing Malware Events

In this section, when you attempt to download the same MSEXEX file 7z1700.exe as before by using a web server, you will notice different behavior on the FTD device because it applies a different rule action—Block Malware instead of Block Files. You will analyze the following scenarios in this section:

- The FMC is unable to communicate with the cloud.
- The FMC performs a cloud lookup.
- FTD blocks malware.

[Figure 20-22](#) shows a file rule that blocks the transfer of any malicious files. When FTD determines that a file is a malicious file, this rule allows an FTD device to store the file in local storage and send reset packets to terminate any associated connection. To conserve disk space, files with clean disposition are not stored.

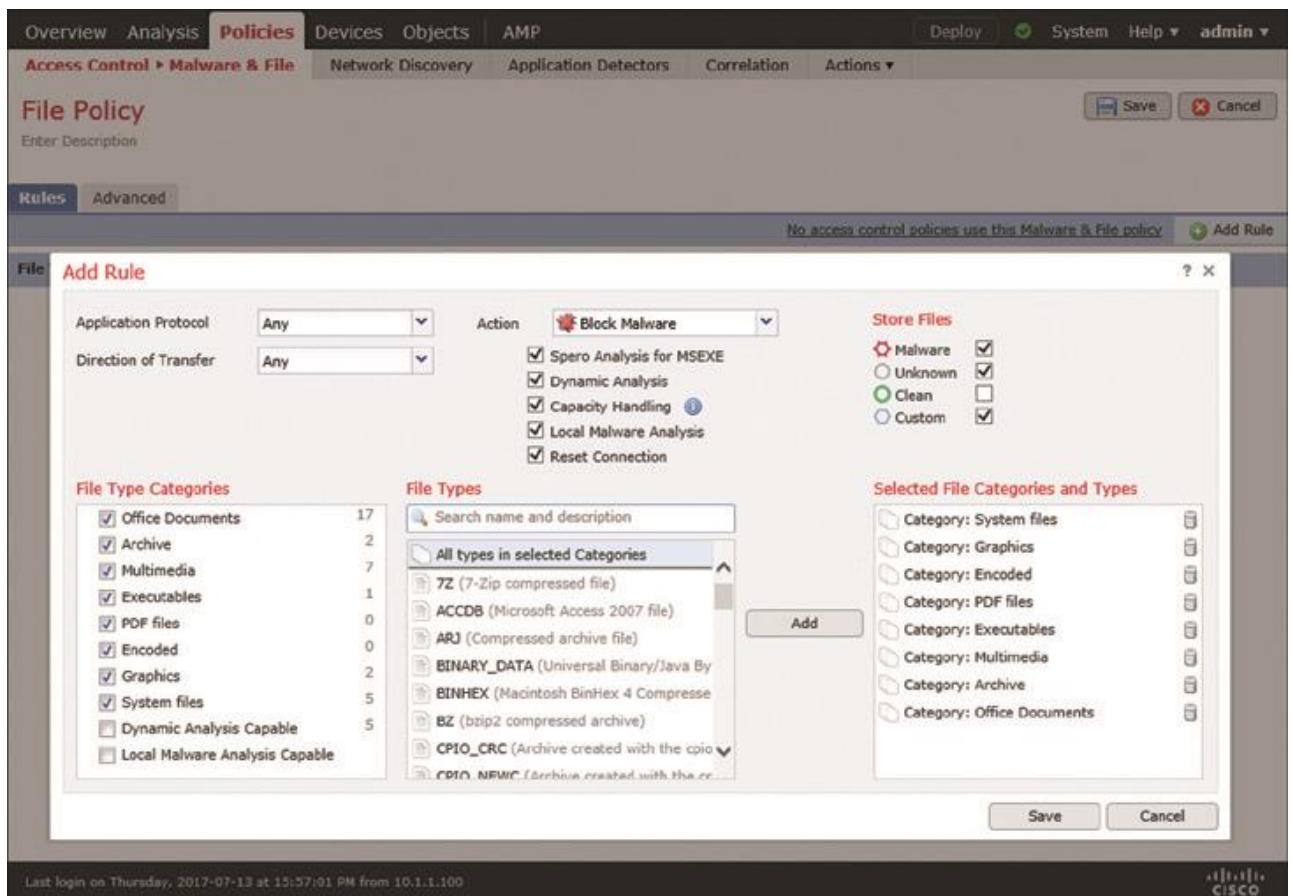


Figure 20-22 Defining the Active Rule Used in This Exercise

The FMC Is Unable to Communicate with the Cloud

After deploying a file policy with the Block Malware rule action, you can attempt to download the same MSEXE file 7z1700.exe as before but now using a web server. Unlike in the previous section, where you used file type detection, you will find the FTD to calculate the SHA-256 checksum of the file. FTD later attempts to perform a cloud lookup for the hash value.

[Figure 20-23](#) shows a file event (table view) for downloading the same 7z1700.exe file. Because the file policy enables malware analysis, FTD calculates the SHA-256 hash value. However, the cloud lookup process times out.

	Time	Action	Sending IP	Receiving IP	File Name	SHA256	Threat Score	Type	Cat
↓	2017-07-17 12:58:43	Cloud Lookup Timeout	172.16.100.100	192.168.1.200	7z1700.exe	2c8637b8...07ee982d		MSEXE	Exec
↓	2017-07-17 12:37:29	Detect	172.16.100.100	192.168.1.200	userguide.pdf			PDF	PDF
↓	2017-07-17 12:23:35	Block	172.16.100.100	192.168.1.200	7z1700.exe			MSEXE	Exec

Figure 20-23 Malware Analysis Verdict—Cloud Lookup Timeout

[Figure 20-24](#) shows the summary view of the file events. Due to the cloud lookup timeout, malware disposition is listed as Unavailable.

	Category	Type	Disposition	Action	Count
↓	Executables	MSEXE	Unavailable	Cloud Lookup Timeout	1
↓	PDF files	PDF		Detect	1
↓	Executables	MSEXE		Block	1

Figure 20-24 Malware Disposition Is Unavailable Due to Cloud Lookup Timeout

[Example 20-3](#) demonstrates that the FTD device is able to calculate the SHA-256 checksum locally. However, when it sends the calculated hash value for a lookup, the query times out (due to a communication failure to the Cisco cloud). This leads the FMC to display the disposition as Unavailable.

Example 20-3 *The FMC Calculates SHA-256 Hash Value but Is Unable to Complete a Lookup*

[Click here to view code image](#)

> **system support firewall-engine-debug**

Please specify an IP protocol: **tcp**

Please specify a client IP address: **192.168.1.200**

Please specify a client port:

Please specify a server IP address:

Please specify a server port:

Monitoring firewall engine debug messages

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 New session
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 using HW or preset rule order 2,  
'Access Rule for File Policy', action Allow and prefilter rule 0
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 allow action
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 URL SI: ShmDBLookupURL("h  
ttp://172.16.100.100/files/7z1700.exe") returned 0
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 File policy verdict is Type,  
Malware, and Capture
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 File type verdict Unknown,  
fileAction Malware Lookup, flags 0x01BDDA00, and type action Stop for type 21 of  
instance 0
```

! Next, FTD calculates the SHA-256 hash value of the file, which is

```
2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d.
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 File signature verdict Unknown  
and flags 0x01BDDA00 for partial file of instance 0
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 File signature cache query returned
```

Cache Miss for 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485dd-

b307ee982d with disposition Cache Miss, spero Cache Miss, severity 0, and transmit

Not Sent

192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I O File signature reserved file data
of 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d with flags
0x01BDDA00 and status Exceeded Max Filesize

192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I O File signature verdict Pending

and flags 0x01BDDA00 for
2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485dd-

b307ee982d of instance 0

192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I O File signature cache query

returned Cache Miss for 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485dd-

b307ee982d with disposition Cache Miss, spero Cache Miss, severity 0, and transmit
Not Sent

192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I O File signature reserved file data
of 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d with flags
0x01BDDA00 and status Exceeded Max Filesize

192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I O File signature verdict Pending

and flags 0x01BDDA00 for
2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485dd-

b307ee982d of instance 0

192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I O File malware event for

2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d named
7z1700.exe

with disposition Cache Miss and action Timeout

192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I O Archive childs been processed No

192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I O Deleting session

^C

Caught interrupt signal

Exiting.

>

To find the root cause of a lookup failure, you can analyze the syslog messages on the FMC. To view the messages, you can use any convenient Linux commands, such as **less**, **cat**, or **tail**, as needed. Note that the timestamps of messages use coordinated universal time (UTC).

Tip

Cloud Lookup Timeout in the Action column indicates that the FMC is unable to connect to the cloud. When you see this, check whether the management interface of the FMC is connected to the Internet. If the Internet connectivity is operational, then make sure the FMC can resolve a DNS query.

[Example 20-4](#) shows various states of the FMC cloud communication. The syslog messages are automatically generated by the Firepower software. To view them in real time, you can use the **tail** command with the **-f** parameter.

Example 20-4 Analyzing Syslog Messages for FMC Communications to the Cloud

[Click here to view code image](#)

```
admin@FMC:~$ sudo tail -f /var/log/messages
```

```
Password:
```

```
.
```

```
<Output is omitted for brevity>
```

```
.
```

```
! If FMC is connected to the internet, but fails to resolve a DNS query, the
```

```
following error message appears in the Syslog.
```

```
.
```

```
[timestamp] FMC stunnel: LOG3[3953:140160119551744]: Error resolving 'cloud-sa.amp.
```

```
sourcefire.com': Neither nodename nor servname known (EAI_NONAME)
```

```
.
```

```
! After you fix any communication issues, FMC should be able to connect to the
```

```
cloud. The following Syslog messages confirm a successful connection.
```

```
.
```

```
[timestamp] FMC SF-IMS[25954]: [26657] SFDataCorrelator:FireAMPCloudLookup  
[INFO]
```

```
cloud server is cloud-sa.amp.sourcefire.com
```

[timestamp] FMC SF-IMS[25954]: [26657] SFDataCorrelator:imcloudpool [INFO] connect
to cloud using stunnel

! Once the FMC is connected to the cloud, it begins the registration process. The
following messages confirm successful registrations to the Cisco Clouds.

[timestamp] FMC SF-IMS[25954]: [26657] SFDataCorrelator:FireAMPCloudLookup
[INFO]
Successfully registered with fireamp cloud

[timestamp] FMC SF-IMS[25954]: [25954] SFDataCorrelator:FileExtract [INFO]
Successfully registered with sandbox cloud

! Upon successful registration, FMC is able to perform cloud lookup and obtains
updates. The following messages confirm a successful check for malware database
update.

[timestamp] FMC SF-IMS[25275]: [25275] CloudAgent:CloudAgent [INFO] ClamUpd, time
to
check for updates

[timestamp] FMC SF-IMS[25275]: [25298] CloudAgent:CloudAgent [INFO] Nothing to do,
database is up to date

[Figure 20-25](#) shows the DNS setting on an FMC management interface. To find this page, go to **System > Configuration** and select **Management Interfaces**. Make sure the FMC can communicate with the configured DNS server and resolve a domain name using this DNS server.

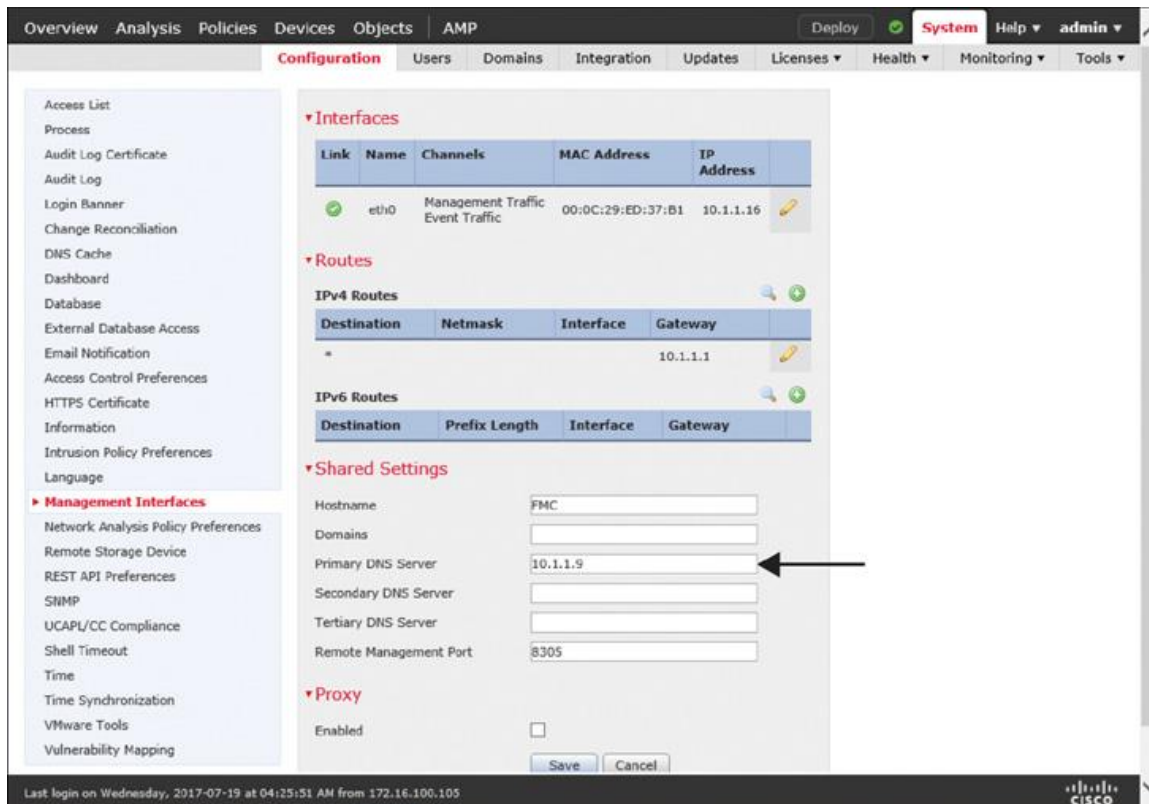


Figure 20-25 DNS Settings on the FMC

The FMC Performs a Cloud Lookup

If the FMC is able to resolve a DNS query, it should be able to connect and register with the Cisco clouds as well. Registration with clouds allows the FMC to perform cloud lookups for malware disposition. As of this writing, Cisco uses cloud-sa.amp.sourcefire.com for Advanced Malware Protection (AMP) services.

This section assumes that you have fixed any connectivity or DNS issues you experienced in the last section. Here you will download the MSEXE file 7z1700.exe once again. You should notice a different type of event this time.

Figure 20-26 shows two different actions on file events for downloading the same file. Because the FMC can communicate with the Cisco clouds, FTD returns Malware Cloud Lookup instead of Cloud Lookup Timeout.

Different Actions		Same File						
Time	Action	Sending IP	Receiving IP	File Name	SHA256	Threat Score	Type	Cat
2017-07-17 12:51:06	Malware Cloud Lookup	172.16.100.100	192.168.1.200	7z1700.exe	2c8637b8...07ec982d		MSEXE	Exec
2017-07-17 12:58:43	Cloud Lookup Timeout	172.16.100.100	192.168.1.200	7z1700.exe	2c8637b8...07ec982d		MSEXE	Exec
2017-07-17 12:37:29	Detect	172.16.100.100	192.168.1.200	userguide.pdf			PDF	PDF
2017-07-17 12:23:35	Block	172.16.100.100	192.168.1.200	7z1700.exe			MSEXE	Exec

Figure 20-26 Successful Malware Cloud Lookup

You can go to the File Summary view to find the malware dispositions. The Cisco clouds can return one of the following dispositions for a query:

- **Malware:** If Cisco determines that a file is malware
- **Clean:** If Cisco finds no malicious pattern on a file
- **Unknown:** If Cisco has not assigned a disposition (malware or clean) to a file

[Figure 20-27](#) compares two types of dispositions—unknown and unavailable—for the 7z1700.exe file. Unknown confirms a successful cloud communication with no cloud-assigned category, whereas Unavailable indicates an issue with cloud communication.

Unknown means the FMC connects to the cloud successfully,
but the cloud has not assigned a disposition to a file.

Category	Type	Disposition	Action	Count
Executables	MSEXE	Unknown	Malware Cloud Lookup	1
Executables	MSEXE	Unavailable	Cloud Lookup Timeout	1
PDF files	PDF		Detect	1
Executables	MSEXE		Block	1

Unavailable means the FMC is unable to
connect to the cloud or perform a lookup for a file.

Figure 20-27 *Malware Disposition—Unknown Versus Unavailable*

[Example 20-5](#) proves that the Firepower System checks its local cached disposition first before it sends the query to the Cisco clouds.

Example 20-5 *Firepower Queries Cached Disposition Before Performing a Cloud Lookup*

[Click here to view code image](#)

> **system support firewall-engine-debug**

- Please specify an IP protocol: **tcp**
- Please specify a client IP address: **192.168.1.200**
- Please specify a client port:
- Please specify a server IP address:
- Please specify a server port:

Monitoring firewall engine debug messages

! Now, begin the transfer of an executable file.

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 New session

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 using HW or preset rule order 2,

'Access Rule for File Policy', action Allow and prefilter rule 0

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 allow action

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 URL SI:

ShmDBLookupURL("http://172.16.100.100/files/7z1700.exe") returned 0

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File policy verdict is Type,

Malware, and Capture

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File type verdict Unknown,

fileAction Malware Lookup, flags 0x01BDDA00, and type action Stop for type 21 of

instance 0

! First, Firepower System checks the cached disposition.

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File signature verdict Unknown

and flags 0x01BDDA00 for partial file of instance 0

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File signature cache query returned

Cache Miss for 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d
With

disposition Cache Miss, spero Cache Miss, severity 0, and transmit Not Sent

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File signature reserved file data

of 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d with flags

0x01BDDA00 and status Exceeded Max Filesize

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File signature verdict Pending

and flags 0x01BDDA00 for

2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485dd-

b307ee982d of instance 0

! Here, Firepower System performs a query to the cloud for disposition.

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File signature cache query returned

Neutral for 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d
With

disposition Neutral, spero Cache Miss, severity 0, and transmit Not Sent

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File signature reserved file data

of 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d for spero
with

flags 0x01BDDA00 and status Exceeded Max Filesize

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File signature reserved file data

of 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d with flags
0x01BDDA00 and status Exceeded Max Filesize

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File signature reserved file data

of 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d with flags
0x01BDDA00 and status Exceeded Max Filesize

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File signature verdict Log and

flags 0x01BDDA00 for 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485dd-
b307ee982d of instance 0

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File malware event for

2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d named
7z1700.exe

with disposition Neutral and action Malware Lookup

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 Archive childs been processed No

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 Deleting session

^C

Caught interrupt signal

Exiting.

>

FTD Blocks Malware

This section shows how to analyze Firepower actions on malware. To emulate a malicious file, this chapter leverages an anti-malware test file available in the European Institute for Computer Antivirus Research (EICAR) website. Cisco does not develop or maintain this test file; however, you can download the latest copy from eicar.org. Alternatively, you can create a test file by your own using a text editor. It consists of the following characters:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

[Figure 20-28](#) shows the creation of `suspicious.exe`, an anti-malware test file. The example uses notepad—a text editor for Microsoft Windows—to create the file. The file simply contains the test string. After you copy the string, save the file in the Windows executable (.exe) format.

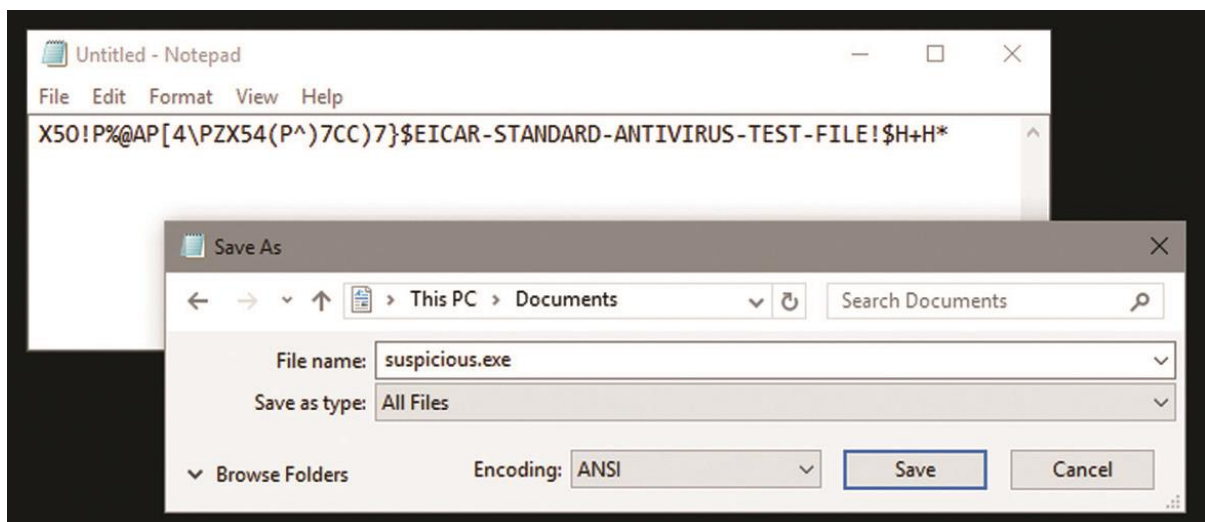


Figure 20-28 *Creation of an Anti-Malware Test File, suspicious.exe, Using a Text Editor*

To perform an experiment, at first, store the anti-malware test file (`suspicious.exe`) on a web server in your lab network. Then attempt to download the test file to a client computer by using a web browser. FTD should block the attempt.

[Figure 20-29](#) demonstrates that FTD blocks a client's attempt to download the suspicious.exe file. The cloud lookup returns a very high threat score for this anti-malware test file, because the cloud detects the test string within the file and considers it malware.

The screenshot shows the Cisco FTD Analysis interface. The main content is a table titled 'File Summary' with the following data:

Time	Action	Sending IP	Receiving IP	File Name	SHA256	Threat Score	Type
2017-07-17 14:05:20	Malware Block	172.16.100.100	192.168.1.200	suspicious.exe	275a021b...f651fd0f	Very High	EICAR
2017-07-17 13:51:06	Malware Cloud Lookup	172.16.100.100	192.168.1.200	Zz1700.exe	2c8637b8...07ee982d		MSEXE
2017-07-17 12:58:43	Cloud Lookup Timeout	172.16.100.100	192.168.1.200	Zz1700.exe	2c8637b8...07ee982d		MSEXE
2017-07-17 12:37:29	Detect	172.16.100.100	192.168.1.200	userguide.pdf			PDF
2017-07-17 12:23:35	Block	172.16.100.100	192.168.1.200	Zz1700.exe			MSEXE

Figure 20-29 FTD Blocking a File with a Malware Signature

[Example 20-6](#) details the operations of an FTD device when it analyzes a file, performs a cloud lookup, and blocks the file based on its malware disposition.

Example 20-6 Blocking a File Due to Its Malware Disposition

[Click here to view code image](#)

> **system support firewall-engine-debug**

- Please specify an IP protocol: **tcp**
- Please specify a client IP address: **192.168.1.200**
- Please specify a client port:
- Please specify a server IP address:
- Please specify a server port:

Monitoring firewall engine debug messages

! First, client attempts to download the suspicious.exe file using a web browser.

192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 New session

192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 using HW or preset rule order 2,
'Access Rule for File Policy', action Allow and prefilter rule 0

192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 allow action

192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 URL SI: ShmDBLookupURL
("http://172.16.100.100/files/suspicious.exe") returned 0

192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 File policy verdict is Type,
Malware, and Capture

192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 File type verdict Unknown,
fileAction Malware Lookup, flags 0x0025DA00, and type action Stop for type 273 of
instance 0

**! Firepower System performs a lookup on cached disposition before sending a query to
the cloud.**

192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 File signature cache
query returned Cache Miss for 275a021bbfb6489e54d471899f7db9d1663f-

c695ec2fe2a2c4538aabf651fd0f with **disposition Cache Miss**, spero Cache Miss,
severity 0, and transmit Sent

192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 File signature reserved file data
of 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f with flags
0x0025DA00 and status Smaller than Min Filesize

192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 File signature verdict
Pending and flags 0x0025DA00 for 275a021bbfb6489e54d471899f7db9d1663f-
c695ec2fe2a2c4538aabf651fd0f of instance 0

192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 File signature cache
query returned Cache Miss for 275a021bbfb6489e54d471899f7db9d1663f-
c695ec2fe2a2c4538aabf651fd0f with disposition Cache Miss, spero Cache Miss,

severity 0, and transmit Sent

192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I O File signature reserved file data of 275a021bbfb6489e54d471899f7db9d1663f-

c695ec2fe2a2c4538aabf651fd0f with flags 0x0025DA00 and status Smaller than Min Filesize

192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I O File signature verdict

Pending and flags 0x0025DA00 for 275a021bbfb6489e54d471899f7db9d1663f-

c695ec2fe2a2c4538aabf651fd0f of instance 0

! At this stage, FMC receives a malware disposition from the cloud. FTD acts on the file based on the File Policy.

192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I O File signature cache

query returned Malware for 275a021bbfb6489e54d471899f7db9d1663f-c695ec2fe2a2c4538aabf651fd0f with **disposition Malware**, spero Cache Miss, severity

76, and transmit Sent

192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I O File signature reserved file data

of 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f with flags 0x0025DA00 and status Smaller than Min Filesize

192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I O File signature verdict

Reject and flags 0x0025DA00 for 275a021bbfb6489e54d471899f7db9d1663f-

c695ec2fe2a2c4538aabf651fd0f of instance 0

192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I O File malware event for

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f named suspicious.

exe with **disposition Malware** and **action Block Malware**

192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I O Archive childs been processed No

192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I O Deleting session

.
<Output Omitted for Brevity>

·
^C

Caught interrupt signal

Exiting.

>

Overriding a Malware Disposition

If you disagree with a file disposition—whether it is analyzed locally by the FTD device or dynamically by the cloud—the FMC allows you to override an outcome by using a file list. There are two types of file list:

■ **Clean list:** If FTD blocks a file due to its malware disposition, you could manually allow the file by adding it to the clean list. This lets the file go through FTD moving forward.

■ **Custom detection list:** If the local or dynamic analysis engine identifies a file as clean or unknown and, therefore, FTD allows the file to transfer, you could change this behavior by adding the file to the custom detection list. In the future, if a client attempts to transfer the same file, FTD will block it, regardless of the disposition by the local or dynamic analysis engine.

In short, the clean list allows you to *whitelist* a file, whereas you can *blacklist* a file by adding it to the custom detection list.

To deploy a new file list, the FTD device must be running a file policy with the following rule conditions:

■ The rule matches the same file type as your selected file format for a file list. For example, if you want to add an executable file to the clean or custom detection list, the rule on a file policy needs to match the executable file types as well.

■ The action of the rule is set to one of the malware analysis rules, such as malware cloud lookup or block malware.

Once these conditions are fulfilled, you can add a file to a file list in two ways: by using the right-click context menu or by using a file list object. The context menu allows you to add a file on the fly.

Figure 20-30 shows the addition of the 7z1700.exe file to the custom detection list through the context menu.

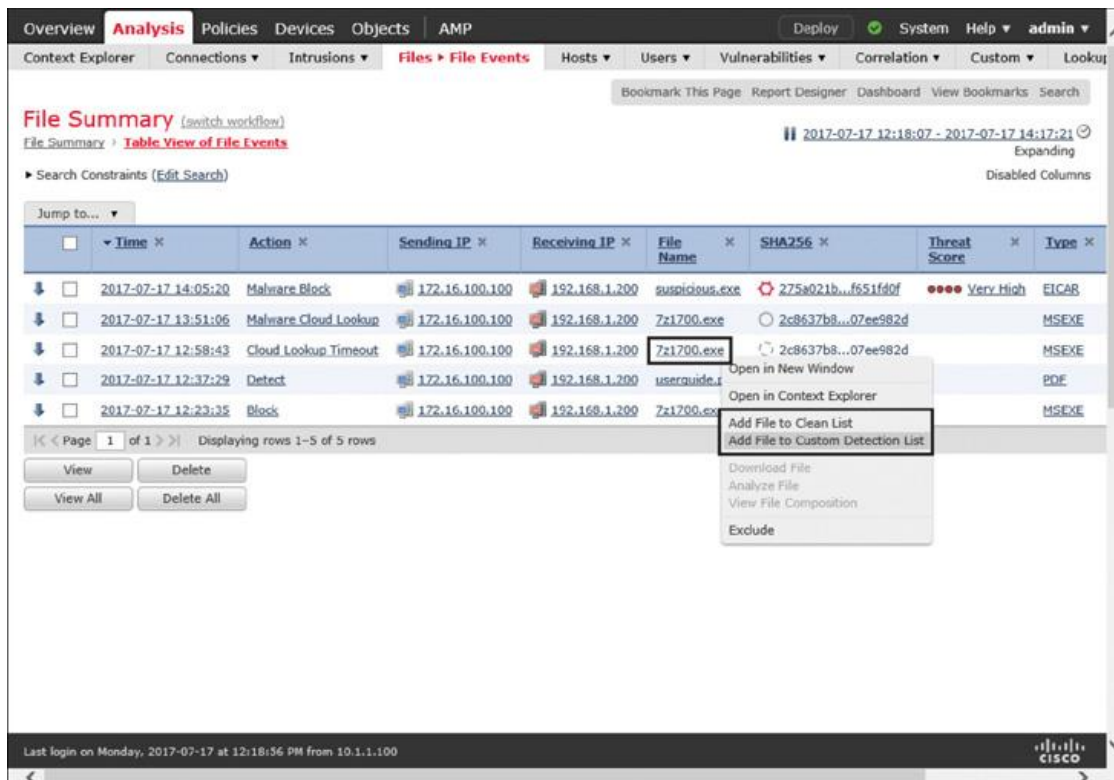


Figure 20-30 Adding a File to the Custom Detection List by Using the Context Menu

Figure 20-31 shows the navigation to the file list object configuration page. Besides adding the files and their SHA hash values, this page allows you to manage any previously added files.

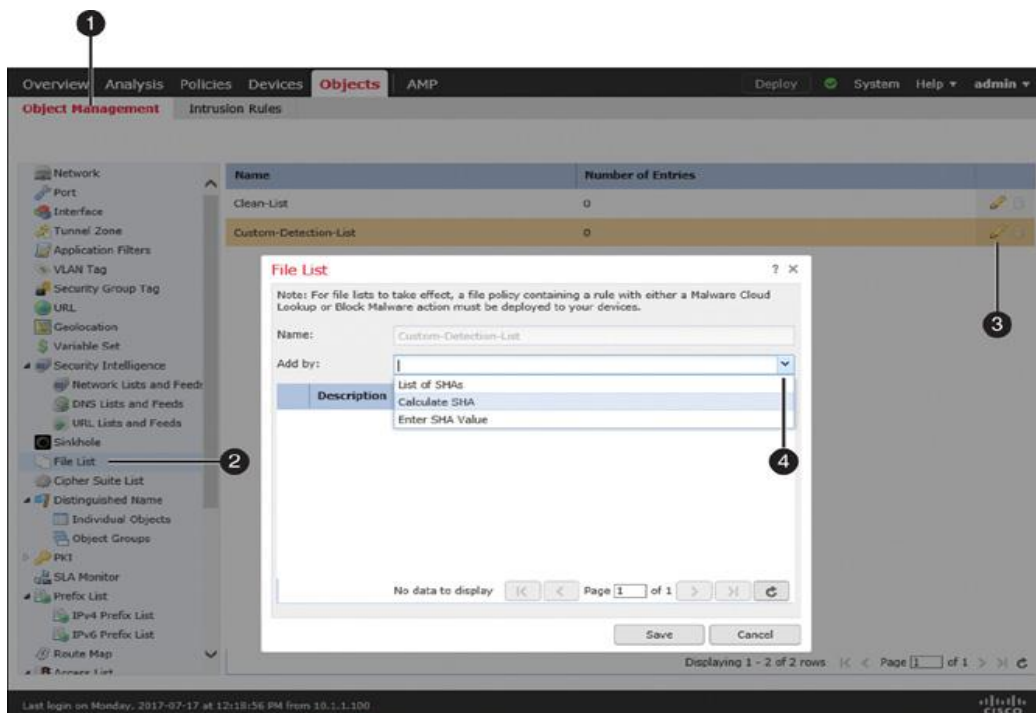


Figure 20-31 Adding a File to the Custom Detection List by Using the File List Object

Once you add your desired file to a file list, you can redeploy the file policy to FTD. Then you can attempt to redownload the file you have just added. If you added the file to the custom detection list, the client should no longer be able to download the file.

[Figure 20-32](#) confirms the block of the latest download attempt due to custom detection. This time, FTD blocks the same 7z1700.exe file that was allowed earlier due to unavailable and unknown dispositions.

The File Is Blocked Due to Custom Detection

Time	Action	Sending IP	Receiving IP	File Name	SHA256	Threat Score	Type
2017-07-17 14:33:20	Custom Detection Block	172.16.100.100	192.168.1.200	7z1700.exe	2c8637b8...07ee987d		MSEXE
2017-07-17 14:05:20	Malware Block	172.16.100.100	192.168.1.200	7z1700.exe	275a021b...f651fd0f	Very High	EICAR
2017-07-17 13:51:06	Malware Cloud Lookup	172.16.100.100	192.168.1.200	7z1700.exe	2c8637b8...07ee987d		MSEXE
2017-07-17 12:59:43	Cloud Lookup Timeout	172.16.100.100	192.168.1.200	7z1700.exe	2c8637b8...07ee987d		MSEXE
2017-07-17 12:37:29	Detect	172.16.100.100	192.168.1.200	useraide.pdf			PDF
2017-07-17 12:23:35	Block	172.16.100.100	192.168.1.200	7z1700.exe			MSEXE

The File Is Allowed Both Times Due to Disposition

Click an icon to view the network file trajectory.

Figure 20-32 File Event for the Custom Detection Block

[Example 20-7](#) displays the debugging messages for a Custom Detection Block event. Here, FTD blacklists the 7z1700.exe file due to its addition to the custom detection list.

Example 20-7 *Adding a File to the Custom Detection List Blacklists the File*

[Click here to view code image](#)

> **system support firewall-engine-debug**

Please specify an IP protocol: **tcp**

Please specify a client IP address: **192.168.1.200**

Please specify a client port:

Please specify a server IP address:

Please specify a server port:

Monitoring firewall engine debug messages

192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 New session

192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 using HW or preset rule order 2,

'Access Rule for File Policy', action Allow and prefilter rule 0

192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 allow action

192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 URL SI:

ShmDBLookupURL("http://172.16.100.100/files/7z1700.exe") returned 0

192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 File policy verdict is Type,

Malware, and Capture

192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 File type verdict Unknown,

fileAction Malware Lookup, flags 0x01BDDA00, and type action Stop for type 21 of instance 0

192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 File signature verdict Unknown

and flags 0x01BDDA00 for partial file of instance 0

192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 File signature **blacklist**

2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d

192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 File signature reserved file data

of 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d with flags 0x00A5DA00 and status Exceeded Max Filesize

192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 File signature verdict Reject

and flags 0x00A5DA00 for

2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485dd-

b307ee982d of instance 0

192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 File malware event for

2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d named

7z1700.exe

with disposition Custom and action Custom Block

192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 Archive childs been processed No

192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 Deleting session

^C

Caught interrupt signal

Exiting.

>

The FMC allows you to track and visualize the path of a file by using the network file trajectory feature. This feature can save you analysis time when you want to determine the spread of a suspicious file. You can look up a particular file by entering its SHA-256 hash value on the **Files > Network Trajectory** page. Alternatively, on the file event page, you can click a disposition icon in the SHA256 column to open the file trajectory page (as shown in the [Figure 20-32](#)).

[Figure 20-33](#) shows the network file trajectory for the 7z1700.exe file. Throughout the exercises on this chapter, the file has gone through various disposition states that you can see on this page.

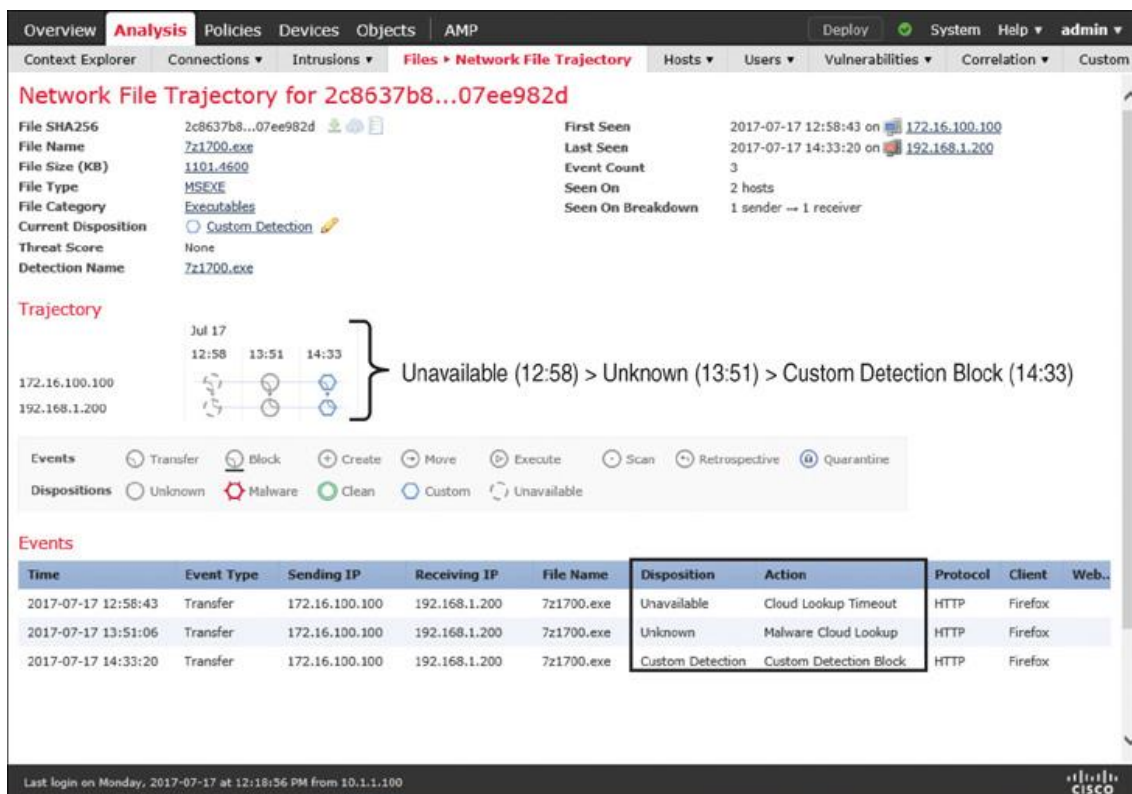


Figure 20-33 Network File Trajectory Page

Summary

Cisco integrates the Advanced Malware Protection (AMP) technology with the Firepower technology. This chapter explains how these technologies work together to help you detect and block the spread of infected files across your network. This chapter also shows the configurations and operations of a file policy on a Firepower system, and it demonstrates various logs and debugging messages that are useful for determining any issues with cloud lookup and file disposition.

Quiz

- Which of the following does not require a Malware license?
 - Sending a file to the cloud for dynamic analysis
 - Enabling a local analysis engine
 - Performing a cloud lookup without blocking a file
 - Blocking a file transfer based on its file format

2. Which type of analysis requires a connection to the cloud?

- a. Spero
- b. Sandbox
- c. High-fidelity
- d. Prefilter

3. Which of the following is recommended?

- a. Use the Reset Connection option on a file rule.
- b. Avoid storing all the files that FTD detects.
- c. Limit the file size for analysis.
- d. All of the above.

4. Which of the following is not true?

- a. FTD can interrupt traffic in case of a cloud lookup failure.
- b. A file policy uses the adaptive profile feature.
- c. The FMC sends a query to the cloud to detect a file type.
- d. The FMC connects to the cloud to obtain new signatures for malware.

Chapter 21

Preventing Cyber Attacks by Blocking Intrusion Attempts

One of the most popular features of Firepower Threat Defense (FTD) is that it can function as an intrusion detection system (IDS) as well as an intrusion prevention system (IPS). FTD uses Snort, an open-source IDS/IPS, to perform deep packet inspection. Snort can detect intrusion attempts and prevent cyber attacks in real time. When an FTD device runs Snort along with many other next-generation security technologies (described in recent chapters), the device turns into a next-generation intrusion prevention system (NGIPS). In this chapter, you will learn how to configure and deploy an intrusion policy on an FTD device.

[Figure 21-1](#) shows a packet analyzed against a Snort ruleset as the last phase of the Firepower engine inspection. However, any bypassed or trusted traffic is not subject to Snort rule inspection.

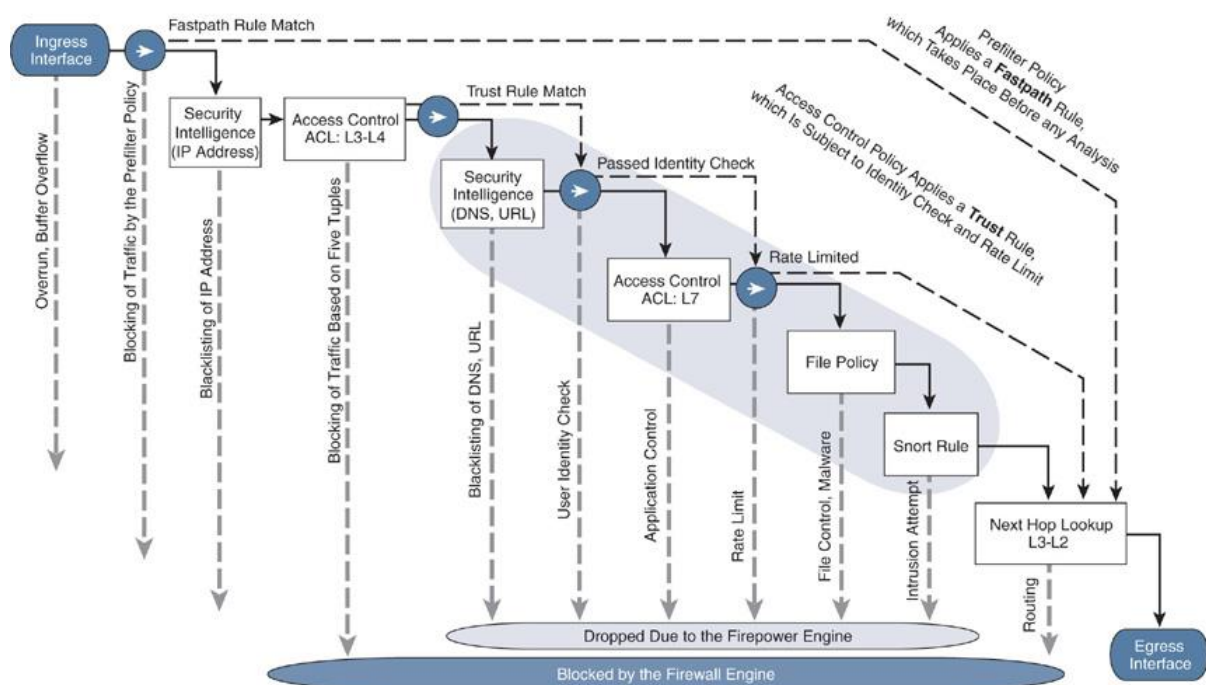


Figure 21-1 Snort Rule Drops a Packet at the Later Phase of Firepower Inspection

Firepower NGIPS Essentials

To deploy an FTD as an NGIPS, you need to work with three different policies in the FMC:

- **Network analysis policy:** This policy works in conjunction with preprocessor rules to normalize traffic.
- **Intrusion policy:** This policy employs the Snort rules to perform deep packet inspection.
- **Access control policy:** This policy invokes the network analysis policy and intrusion policy for matching and nonmatching traffic.

The following sections describe all the essential components that are part of an intrusion policy deployment.

Network Analysis Policy and Preprocessor

Before performing deep packet inspection, Snort decodes a packet and streamlines its header and payload into a format that a Snort rule can analyze easily. The component that performs this normalization is called a *preprocessor*. Snort has various protocol-specific preprocessors. They can identify anomalies within the stream of packets, detect evasion techniques, and drop them when there is an inconsistency, such as an invalid checksum or unusual ports.

The implementation of preprocessors on open source Snort and FTD are not exactly the same. The Firepower engine normalizes traffic in various phases as a packet goes through additional advanced security checks.

[Figure 21-2](#) shows the position of preprocessor in the open source Snort architecture. All the preprocessor plugins operate at the same level—after decoding a packet and before the Snort rule inspection.

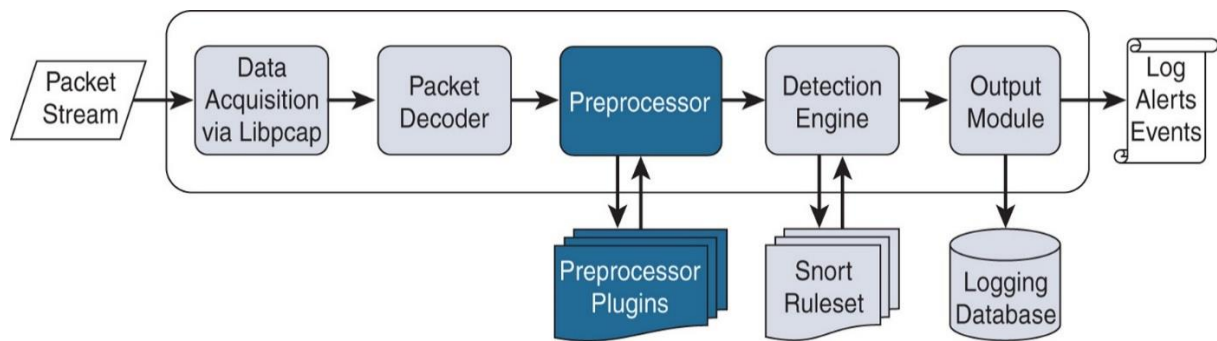


Figure 21-2 *Implementing Preprocessor Plugins on Open Source Snort*

Figure 21-3 illustrates the multiphase implementation of preprocessors on an FTD device. You can enable any of these preprocessors from one place: the network analysis policy.

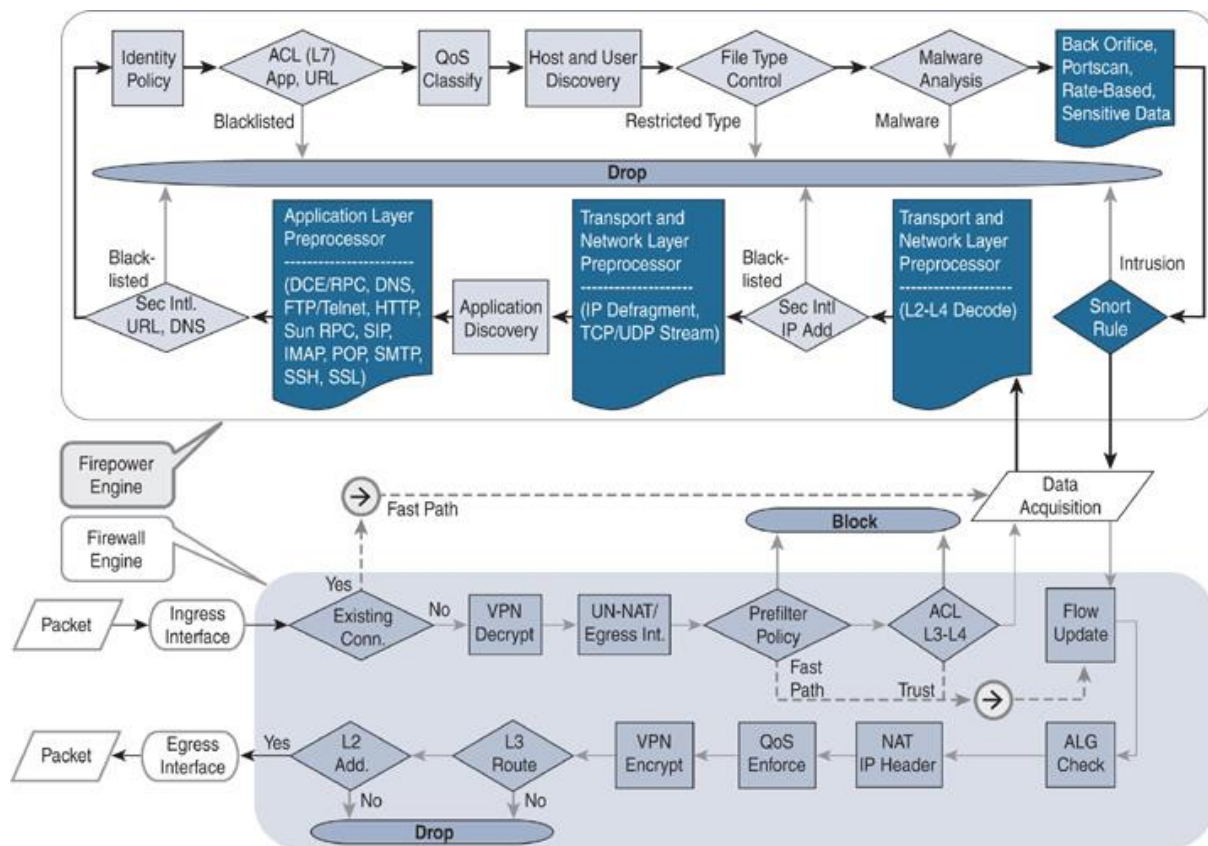


Figure 21-3 Network Analysis Policy Acting in Multiple Phases Throughout an Engine

A network analysis policy on a Firepower system allows you to enable a certain preprocessor and fine-tune any granular settings within. A preprocessor allows Snort to preprocess, decode, and normalize traffic for advance inspection. If you disable a preprocessor manually but Snort deems the preprocessor necessary, FTD can still engage that particular preprocessor in the backend to protect your network from a potential threat. However, a network analysis policy configuration does not indicate when FTD enables an essential preprocessor automatically. Visually, the preprocessor setting remains disabled on the FMC GUI.

Figure 21-4 shows the network analysis policy editor page, where you can enable and disable a desired preprocessor. Later in this chapter, you will learn how to create and deploy a network analysis policy from scratch.

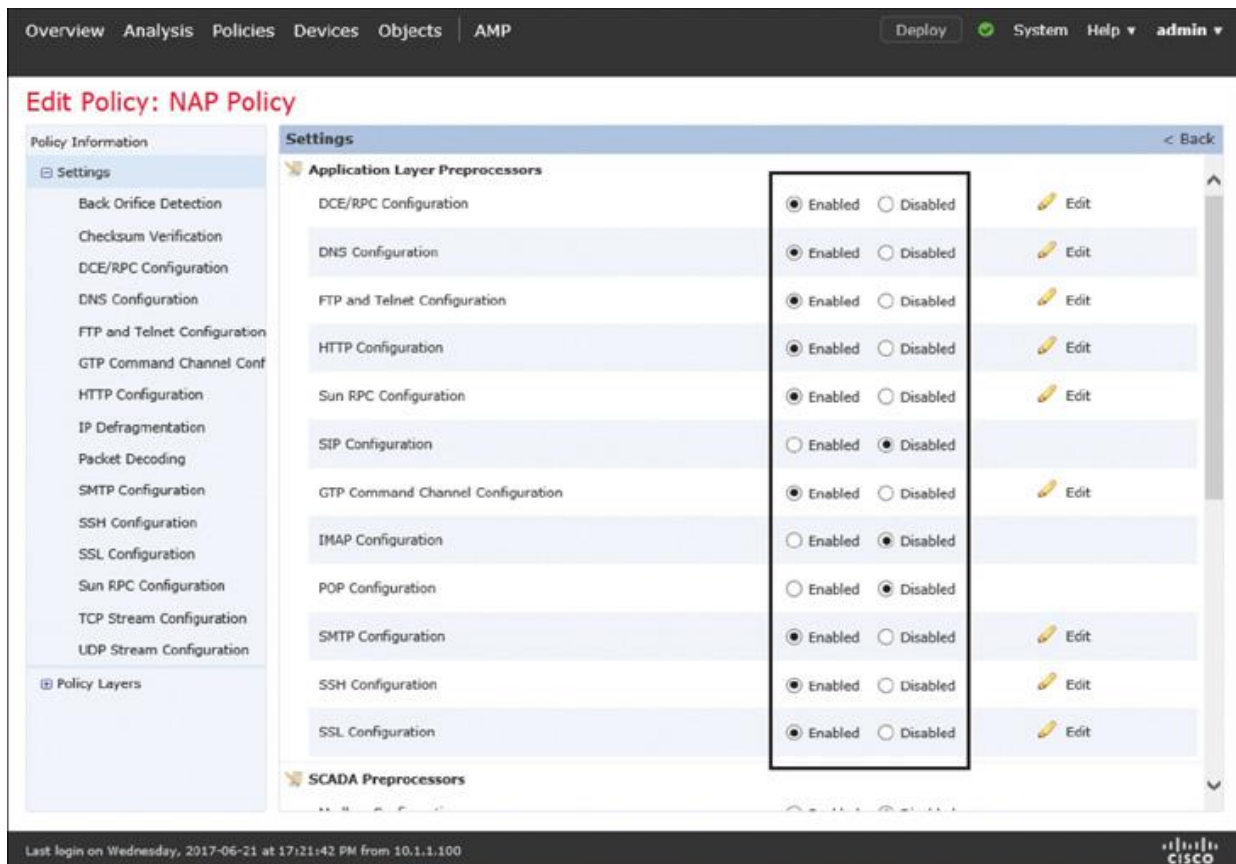


Figure 21-4 *Enabling and Disabling Preprocessor Settings in the Network Analysis Policy Editor*

The Application Layer Preprocessors section of a network analysis policy editor allows you to configure the advanced settings of various protocols traffic, such as DCE/RPC, DNS, FTP and Telnet, HTTP, Sun RPC, SIP, GTP Command Channel, IMAP, POP, SMTP, SSH, and SSL.

The Transport and Network Layer Preprocessors section of a network analysis policy editor offers granular configurable options for checksum verification, inline normalization, IP defragmentation, packet decoding, TCP stream configuration, UDP stream configuration, and so on.

The FMC also provides preprocessors for very specific environments and detection. For example, DNP3 and Modbus preprocessors have been developed for the Supervisory Control and Data Acquisition (SCADA) network environment. Similarly, three additional preprocessors are designed to detect very specific traffic patterns and threats, including Back Orifice, Portscan, and Rate-Based.

After decoding and normalizing a packet, FTD uses the intrusion ruleset to perform deep packet inspection. An intrusion rule is written based on Snort rule syntax and contains the signature of a specific vulnerability. The Firepower System supports Snort rules from various sources, including the following:

■ **Standard text rules:** The Cisco Talos security intelligence and research group writes these rules in clear-text format. The Snort detection engine uses them to analyze packets.

■ **Shared object (SO) rules:** Talos writes SO rules in the C programming language and compiles them for Snort use. The content of an SO rule is made irretrievable for various reasons, such as proprietary agreements between Cisco and third-party vendors.

■ **Preprocessor rules:** The Snort development team creates these rules, which the Firepower engine uses to decode packets with various protocols.

■ **Local rules:** The FMC enables you to create a custom Snort rule by using its GUI. You can also write your own rule in a text editor, save the file in .txt format, and upload it to the FMC. When you create your own Snort rule and import it into the FMC, the Firepower System labels it as a *local rule*. Similarly, if you obtain a Snort rule from a community-based Internet forum, the system considers it a local rule as well. The Firepower System supports text-based local rules only; it does not support the creation and compilation of your own SO rules.

Warning

Although the FMC enables you to import the community-provided rules or to write your own local rules, you should always consider enabling a Cisco-provided rule over a local rule. Cisco-provided rules are developed by Talos—a group of world-class researchers who are primarily responsible for writing and improving Snort rules. An ill-structured rule created by a new Snort user can affect the performance of an FTD device.

Snort uses a unique generator ID (GID) and Snort rule ID (SID) to identify a rule. Depending on who creates a rule, the numbering schemes of GIDs and SIDs are different. [Table 21-1](#) provides the identification numbers that you can use to distinguish one type of Snort rule from another.

Table 21-1 *Types of Snort Rules and Their Identification Numbers*

Type of Rule	Identification Number
Standard text rule	GID is 1. SID is lower than 1,000,000.
Shared object rule	GID is 3.
Preprocessor rule	GID can be anything other than 1 or 3.
Local rule	SID is 1,000,000 or higher.

Once you create an intrusion policy, you can enter the intrusion policy editor page to find and enable a specific Snort rule or all of the rules within a category.

Figure 21-5 shows a search query for all the Snort rules with Telnet metadata. You can perform a similar search to find rules with many other criteria. For now, just take a look how the intrusion policy editor displays rules in a search query. Later in this chapter, you will learn how to create, edit, and deploy an intrusion policy from scratch.

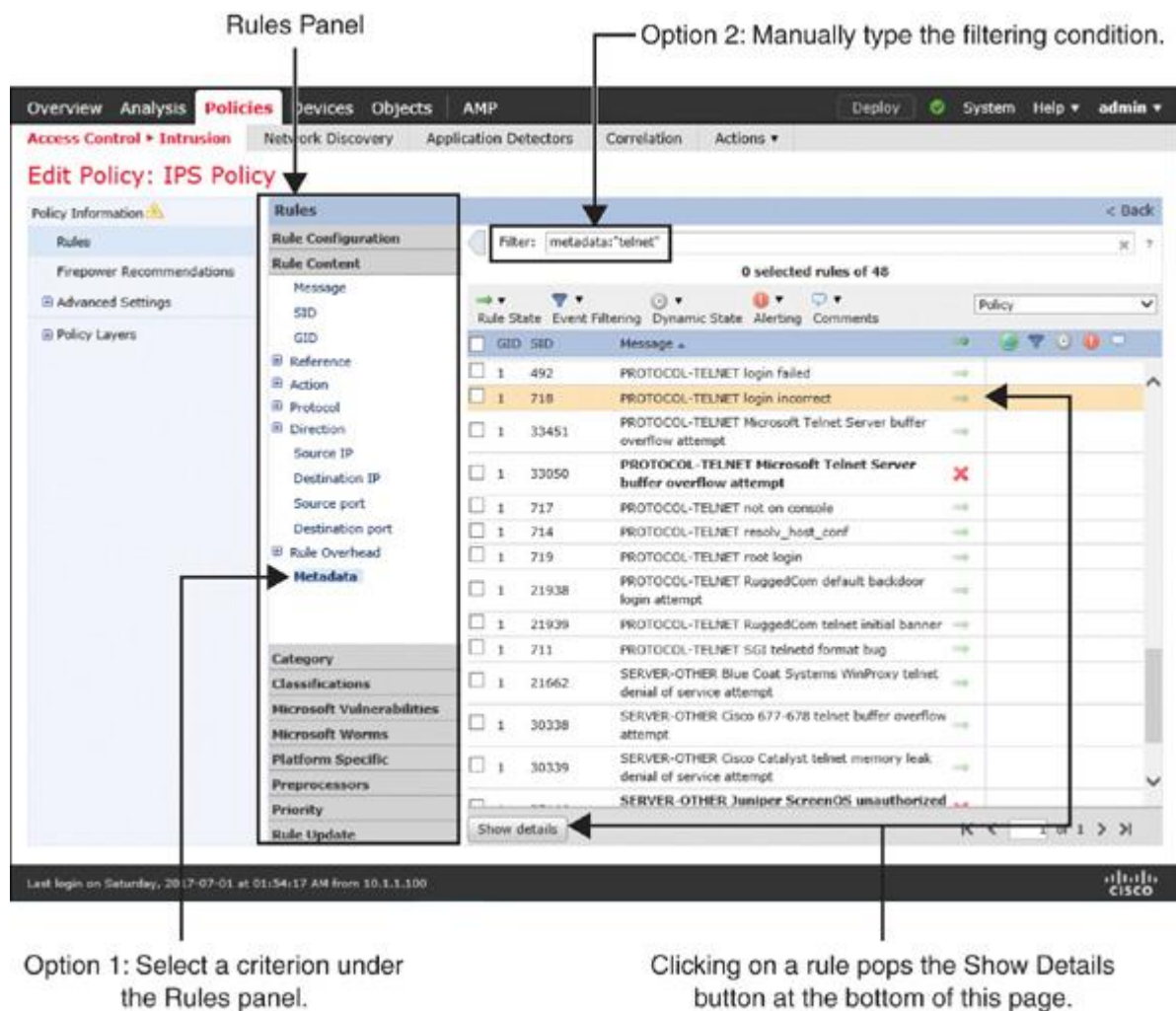


Figure 21-5 Granular Options to Search for a Specific Snort Rule in the Intrusion Policy Editor

Tip

If you want to search for rule 718 directly, enter **SID:718** in the filter—rather than just 718. If you want to perform a new search, you should clear the existing search result by clicking the X icon in the Filter bar.

Once you find a rule, you can select the rule and click the **Show Details** button to view detailed information about it.

[Figure 21-6](#) shows the syntax of Snort rule 1:718. It also provides detailed rule documentation. Later in this chapter, you will learn how to create an intrusion policy from scratch and enable a desired rule within it.

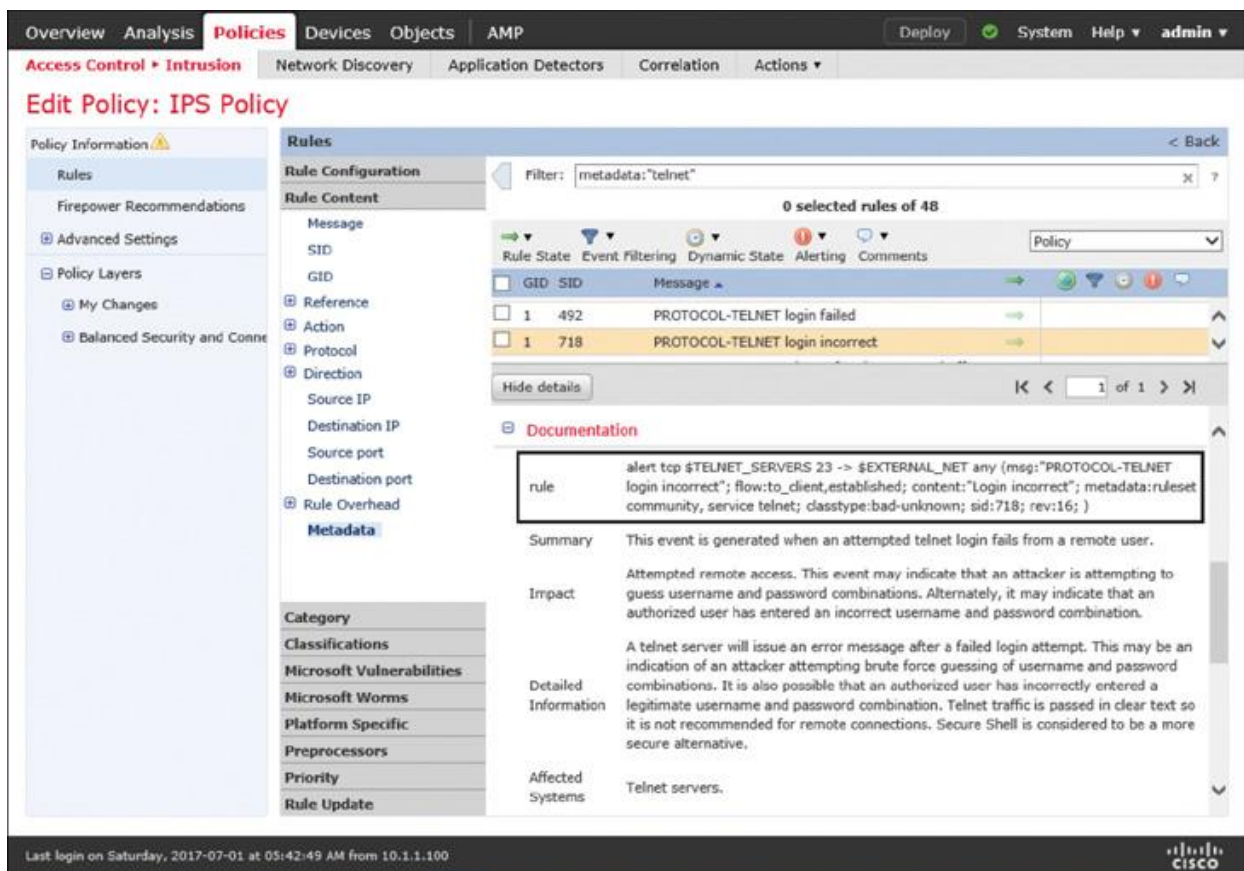


Figure 21-6 Viewing Additional Information About a Rule

Note

Throughout this chapter, Snort rule 1:718 is used as an example to demonstrate various configurations. You can replace SID:718 with any desired rule.

System-Provided Variables

Besides using a static IP address or port number, a Snort rule can use variables to represent the source and destination information. This empowers you to enable a rule in any network environment without modifying the original Snort rule.

[Figure 21-7](#) illustrates Snort rule 1:718, which analyzes traffic from the \$TELNET_SERVERS variable to detect a potential brute-force attack. If you do not change the default value of the \$TELNET_SERVERS variable, Snort analyzes packets from additional IP addresses—along with your real Telnet server—for the “Login incorrect” content with the payloads.

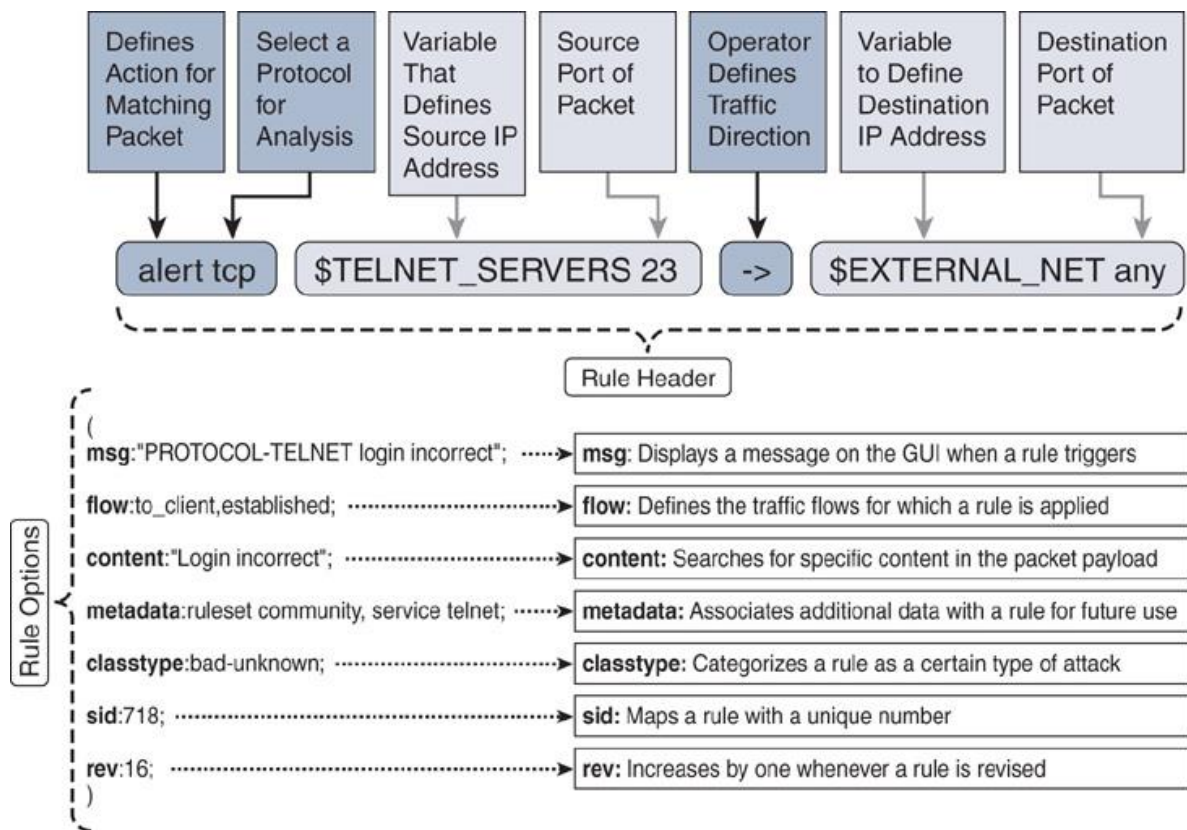


Figure 21-7 Anatomy of Snort Rule 1:718 (GID:1, SID:718)

You must define the `$HOME_NET` variable based on the network address used in your LAN. If the default value of a variable that represents a specific server is set to `any` or `$HOME_NET`, you must change it to a more specific value. It makes a Snort rule more effective and reduces the probability of false positive alerts. Thus, a proper variable setting can improve performance.

The purpose of a variable is explained by the variable's name. The names ending with `*_NET`, `*_SERVERS` and `*_PORTS` define network addresses, IP addresses, and port numbers, respectively. Consider these examples:

■ **`$HOME_NET`, `$EXTERNAL_NET`:** Defines the internal network and external network addresses, respectively.

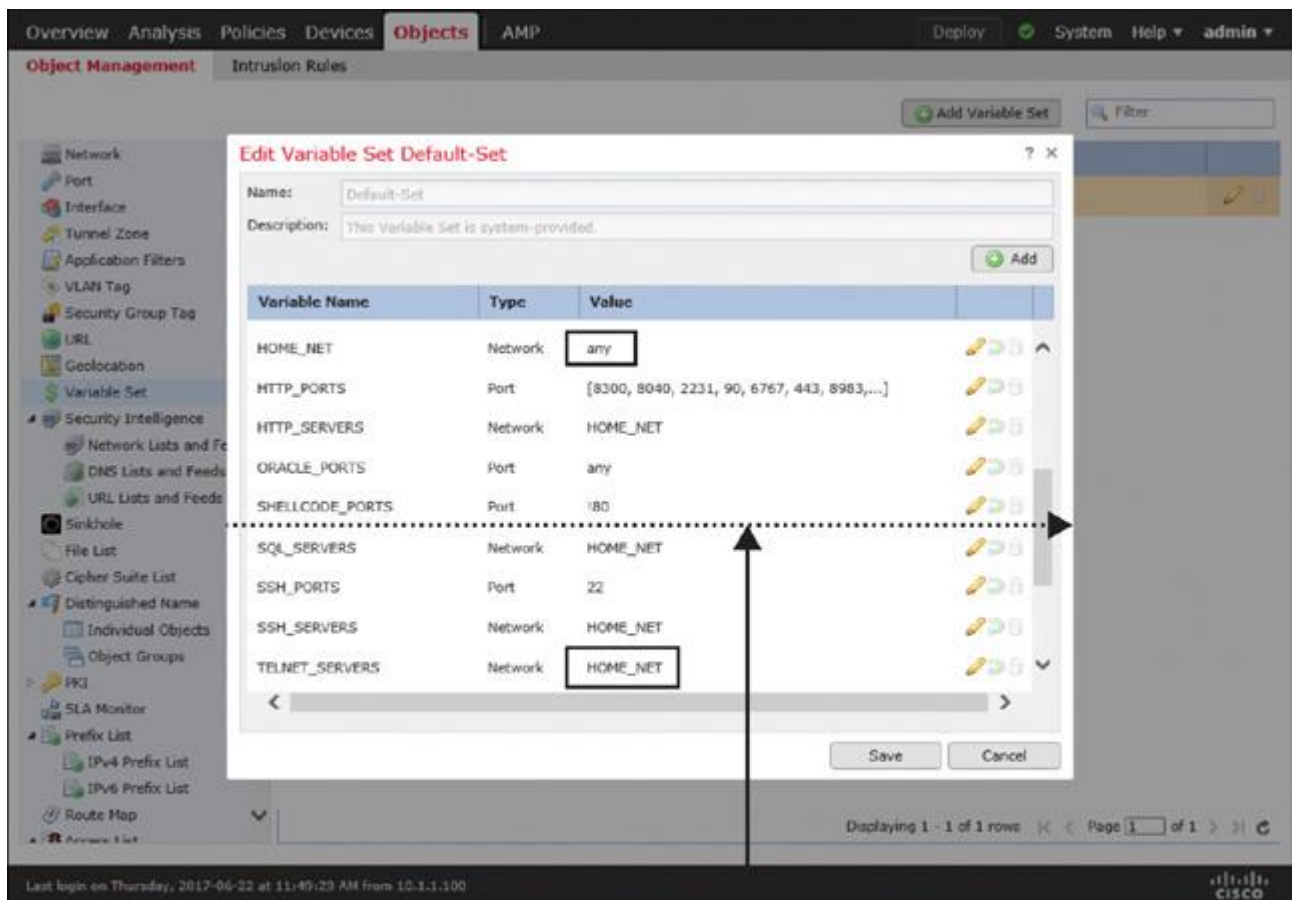
■ **`$HTTP_SERVERS`, `$DNS_SERVERS`:** Defines the IP addresses of the web servers and domain name servers, respectively.

■ **`$FTP_PORTS`, `$HTTP_PORTS`:** Defines the port numbers of the FTP servers and web servers, respectively.

Note

In this chapter, the configuration examples use the Cisco-provided Snort rules. If you want to write your own local rules, you need to know the usage of Snort variables and rule options, which are beyond the scope of this chapter. To learn more about custom rule writing, read the documentation on open-source Snort at www.snort.org.

Figure 21-8 shows a list of variables in the default variable set. You must redefine both variables—\$HOME_NET and \$TELNET_SERVERS—to trigger SID:718 efficiently in the appropriate condition. The list in this figure has been shortened to accommodate both the \$HOME_NET and \$TELNET_SERVERS in one screenshot.



The list has been shortened to accommodate the essential variables in one page.

Figure 21-8 *Redefining the Default Values of Variables with Specific Values*

System-Provided Policies

To help you expedite a deployment, Firepower software comes with several preconfigured network analysis policies and intrusion policies. You can use one of the following system-provided policies as the default security policy for your network or as a baseline for a custom security policy:

■ **Balanced Security and Connectivity:** Cisco Talos recommends this policy for the best system performance without compromising the detection of the latest critical vulnerabilities.

■ **Connectivity over Security:** This policy prioritizes connection speed while maintaining detection of a few critical vulnerabilities.

■ **Security over Connectivity:** Security has higher priority than connection speed and reachability.

■ **Maximum Detection:** Security has supreme priority over business continuity. Due to the deeper inspection of packets, end users may experience latency, and FTD may drop some legitimate traffic.

[Figure 21-9](#) shows four system-provided policies that you can use as a base policy for a network analysis policy (NAP).

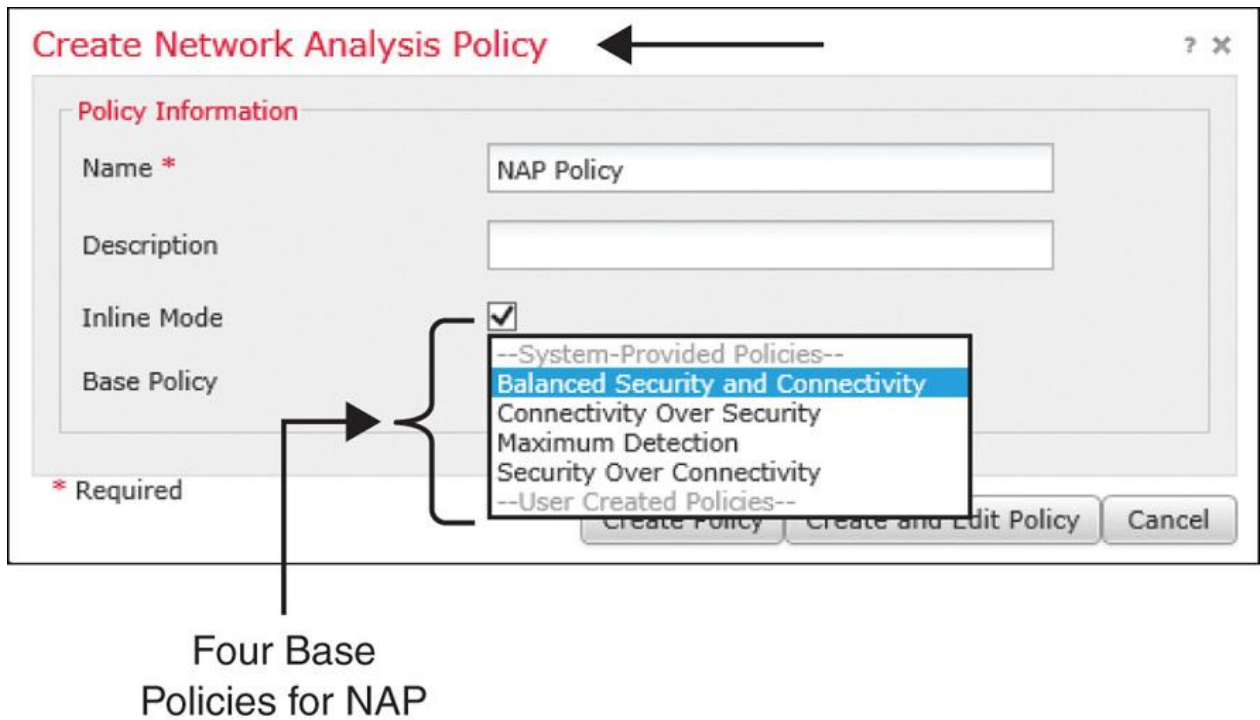
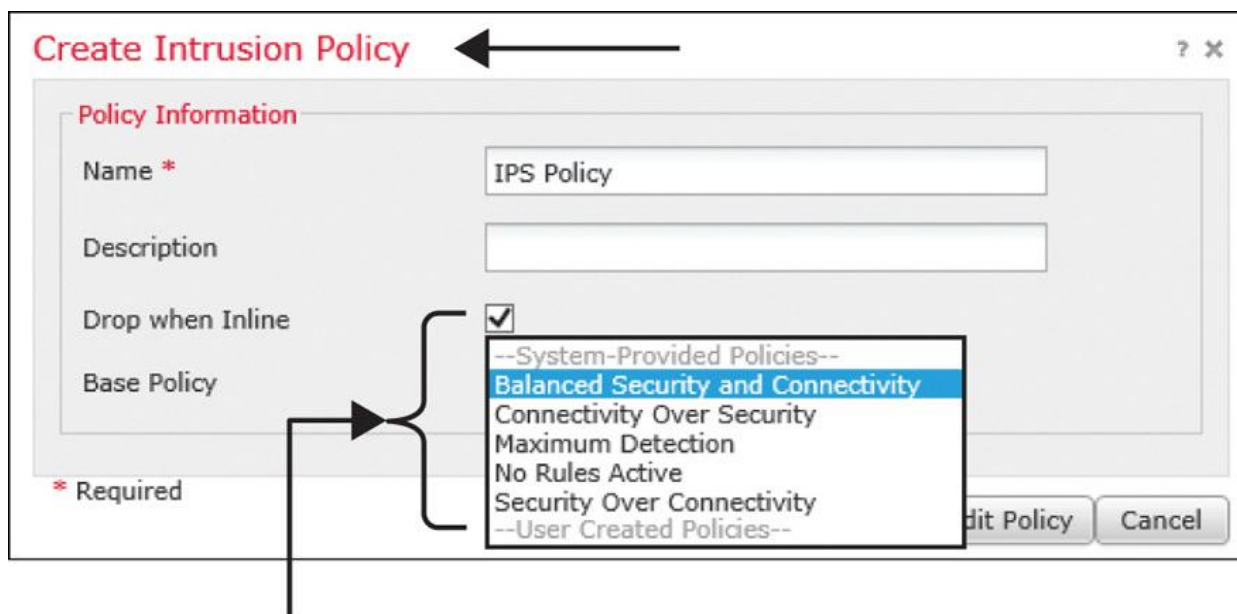


Figure 21-9 System-Provided Base Policies for Network Analysis

[Figure 21-10](#) shows five system-provided policies in the dropdown that you can use as a base policy for an intrusion policy. The base policy No Rules Active allows you to create an empty intrusion policy with all the rules disabled. You can use it for two purposes: to create an intrusion policy from scratch or to investigate any technical issues with the Snort engine.



Five Base Policies for IPS

Figure 21-10 System-Provided Base Policies for Intrusion Detection and Prevention

The number of rules enabled by default in a system-provided policy varies. Cisco uses a Common Vulnerability Scoring System (CVSS) score that is associated with a vulnerability to determine whether a rule should be part of any system-provided policy.

[Table 21-2](#) shows the criteria to determine the inclusion of an intrusion rule in a system-provided policy.

Table 21-2 System-Provided Policies and Their Associations with CVSS Scores

Intrusion Policy	CVSS Score	Age of Vulnerability
Connectivity over Security	10	Current year plus two prior years
Balanced Security and Connectivity	9 or higher	Current year plus two prior years
Security over Connectivity	8 or higher	Current year plus three prior years
Maximum Detection	7.5 or higher	All the years since 2005

[Figure 21-11](#) shows the correlation among the system-provided intrusion policies, their detection coverages, and processing overheads. The higher the threat coverage, the higher the utilization of the FTD resources.

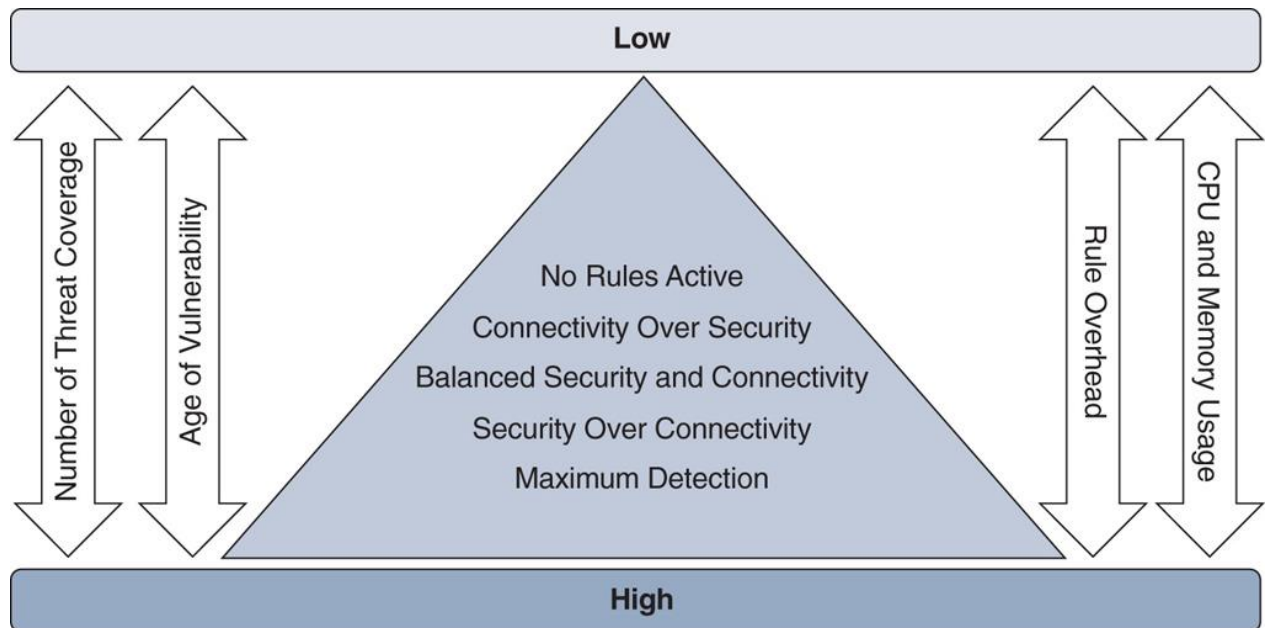


Figure 21-11 *System-Provided Policies, Coverages, and Processing Overheads*

Cisco releases rule updates periodically. The FMC can update the ruleset automatically from the cloud through a scheduled task. You can also manually download a rule update file and upload it to the FMC for installation. Each rule update comes with a unique ruleset. While the exact number of available rules on a specific rule update is unpredictable, the ratio of enabled rules among the system-provided policies is similar. For example, the Security over Connectivity policy enables the highest number of intrusion rules, whereas the Connectivity over Security policy enables the lowest number of rules. (However, the No Rules Active policy has no rules enabled.)

[Figure 21-12](#) shows the Policy Information page in an intrusion policy editor. Here you can determine the number of enabled rules and the rule update version of a base policy.

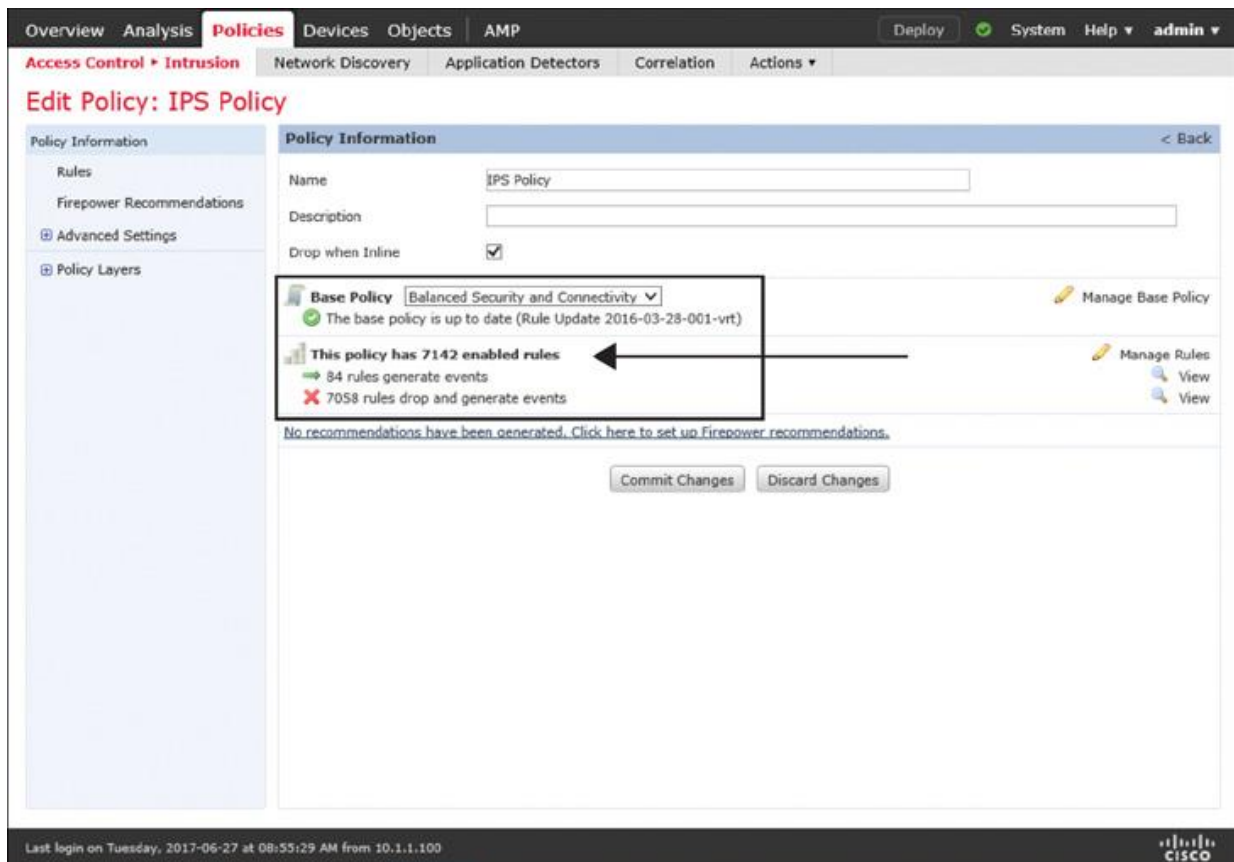


Figure 21-12 *Determining the Number of Enabled Rules on a Base Policy*

[Table 21-3](#) shows the number of rules enabled by default by Rule Update 2016-03-28-001-vrt. Firepower Version 6.1 comes with rule update 2016-03-28-001-vrt preinstalled.

Table 21-3 *Enabled Rules in the Default Ruleset of Rule Update 2016-03-28-001-vrt*

Intrusion Policy	Total Number of Enabled Rules	Rules to Generate Events	Rules to Drop and Generate Events
No Rules Active	0	0	0
Connectivity over Security	459	9	450
Balanced Security and Connectivity	7142	84	7058
Security over Connectivity	10,069	235	9834
Maximum Detection	5533	39	5494

[Table 21-4](#) shows the number of rules enabled by default by Rule Update 2017-06-15-001-vrt. You can compare the statistics shown here with the number of rules enabled on 2016-03-28-001-vrt, as shown in [Table 21-3](#). These rule updates were released one year apart, but the ratio of the enabled rules is similar.

Table 21-4 *Enabled Rules in the Default Ruleset of Rule Update 2017-06-15-001-vrt*

Intrusion Policy	Total Number of Rules Enabled	Rules to Generate Events	Rules to Drop and Generate Events
No Rules Active	0	0	0
Connectivity over Security	474	9	465
Balanced Security and Connectivity	8779	71	8708
Security over Connectivity	12,716	245	12,471
Maximum Detection	6732	40	6692

As the name suggests, the Maximum Detection policy is meant to enable the maximum number of intrusion rules. However, the numbers in Tables 21-3 and 21-4 do not support this assumption. Actually, the Security over Connectivity policy enables the maximum number of rules. So, how does the Maximum Detection policy ensure the maximum threat detection? It actually performs a much deeper analysis of packets to detect any protocol anomalies.

[Table 21-5](#) shows the number of preprocessors enabled on different system-provided network analysis policies. The Maximum Detection policy has the highest number of preprocessors enabled, by default.

Table 21-5 *Number of Preprocessors Enabled on Rule Update 2017-06-15-001-vrt*

Intrusion Policy	Number of Enabled Preprocessors
Connectivity over Security	15
Balanced Security and Connectivity	15
Security over Connectivity	17
Maximum Detection	18

Figure 21-13 illustrates the default configuration settings of the HTTP preprocessor on the Maximum Detection policy. As you can see, much deeper inspections are enabled.

The screenshot shows the 'Edit Policy: NAP Policy' configuration page for the 'Maximum Detection' policy. The 'HTTP Configuration' section is expanded, showing various settings. Annotations include:

- Deeper HTTP Inspection:** A bracket groups the following settings: Maximum Header Length (750 bytes), Maximum Number of Headers (100), Maximum Number of Spaces (0), and HTTP Client Body Extraction Depth (65495).
- More HTTP inspection options are enabled:** A bracket groups the following checked options: Inspect HTTP Cookies, Inspect HTTP Responses, Normalize UTF Encodings to UTF-8, Inspect Compressed Data, and Unlimited Decompression.
- More preprocessors are enabled on the Maximum Detection policy:** A note at the bottom points to the 'Maximum Detection' policy name.

Figure 21-13 Analysis of HTTP Preprocessor Settings on the Maximum Detection Policy

Figure 21-14 shows the default configuration settings of the HTTP preprocessor on the Balanced Security and Connectivity policy. If you compare this figure with the previous one, you will find a milder HTTP inspection setting on the Balanced Security and Connectivity policy.

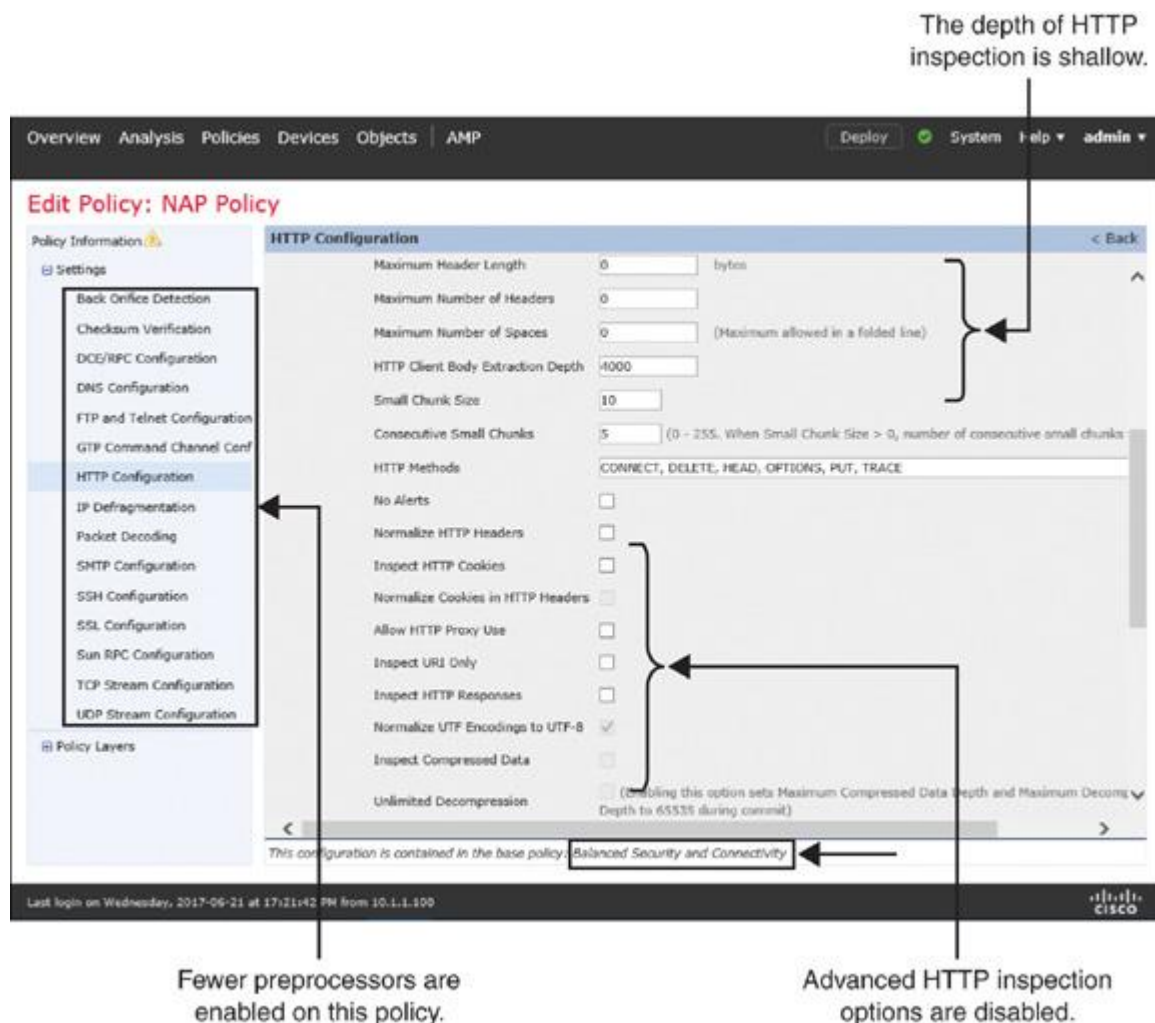


Figure 21-14 HTTP Preprocessor Settings on the Balanced Security and Connectivity Policy

Best Practices for Intrusion Policy Deployment

Note

This section discusses various tips for optimal deployment and displays GUI navigations to the related configuration pages. Later in this chapter, you will find detailed configuration steps for each of these items.

Before you deploy an intrusion policy, you should consider the following best practices, in general:

- To match a packet using five tuples—source port, destination port, source address, destination address, and protocol—you should consider using an access rule, not an intrusion

rule. The purpose of a Snort-based intrusion rule is to perform advanced deep packet inspection.

■ Select the **Balanced Security and Connectivity** policy as the default policy when you create the network analysis policy and intrusion policy.

[Figure 21-15](#) shows the selection of Balanced Security and Connectivity as the base policy for both the network analysis policy (top) and intrusion policy (bottom). Also, notice the check boxes for Inline Mode and Drop When Inline; you must select both of them if you want FTD to block an intrusion attempt.

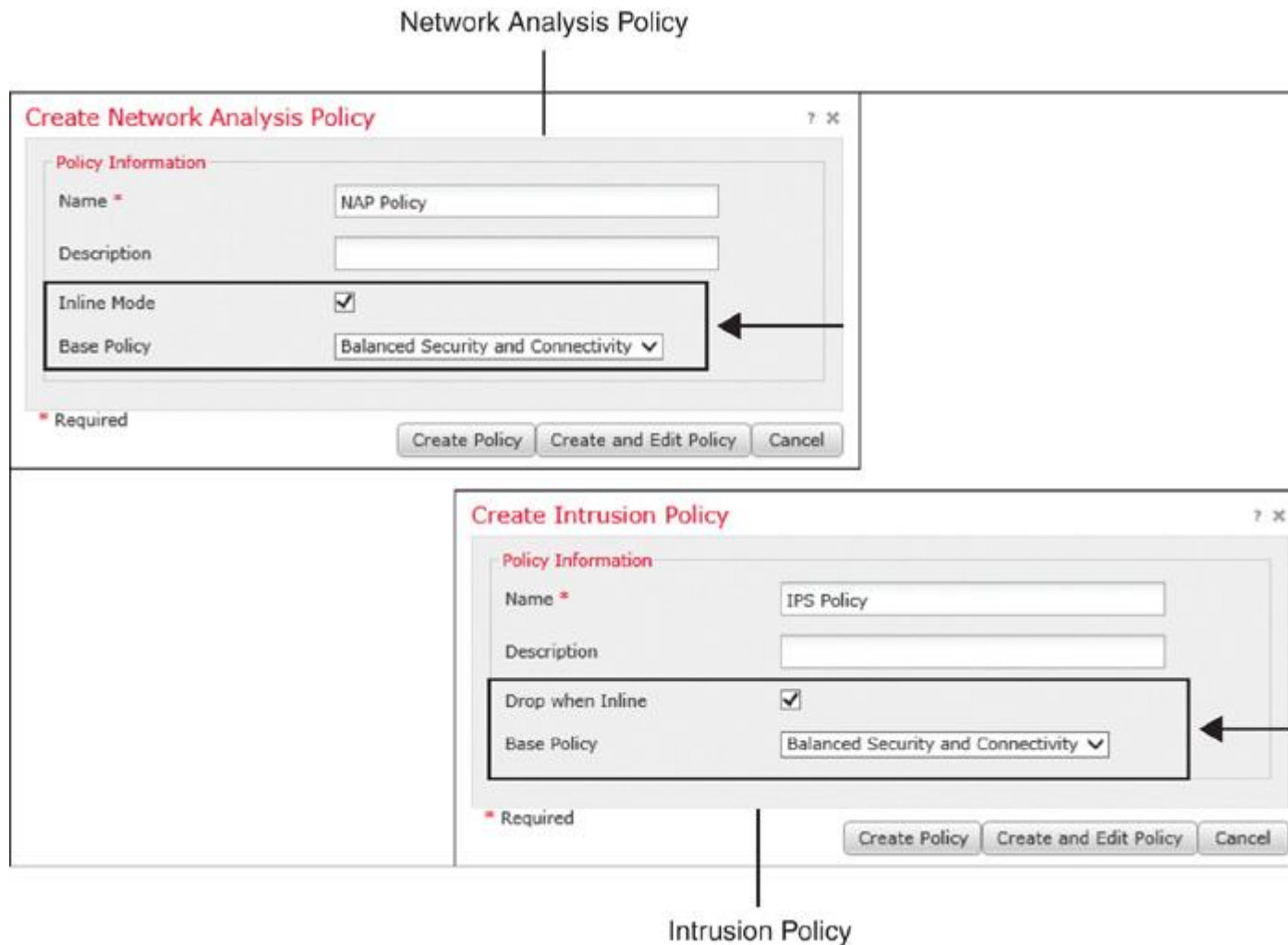


Figure 21-15 Policy Creation Windows for the Network Analysis Policy and Intrusion Policy

■ Use the Firepower Recommendations feature within the intrusion policy. This feature can incorporate the network discovery data to determine the intrusion rules that are related to the operating systems, services, and applications running in a network.

■ When you generate Firepower recommendations, define the networks to examine and set Recommendation Threshold (by Rule Overhead) to Medium or Low for optimal system performance.

[Figure 21-16](#) shows the Firepower Recommendations configuration page within the intrusion policy editor. The number of recommended rules can vary based on your settings.

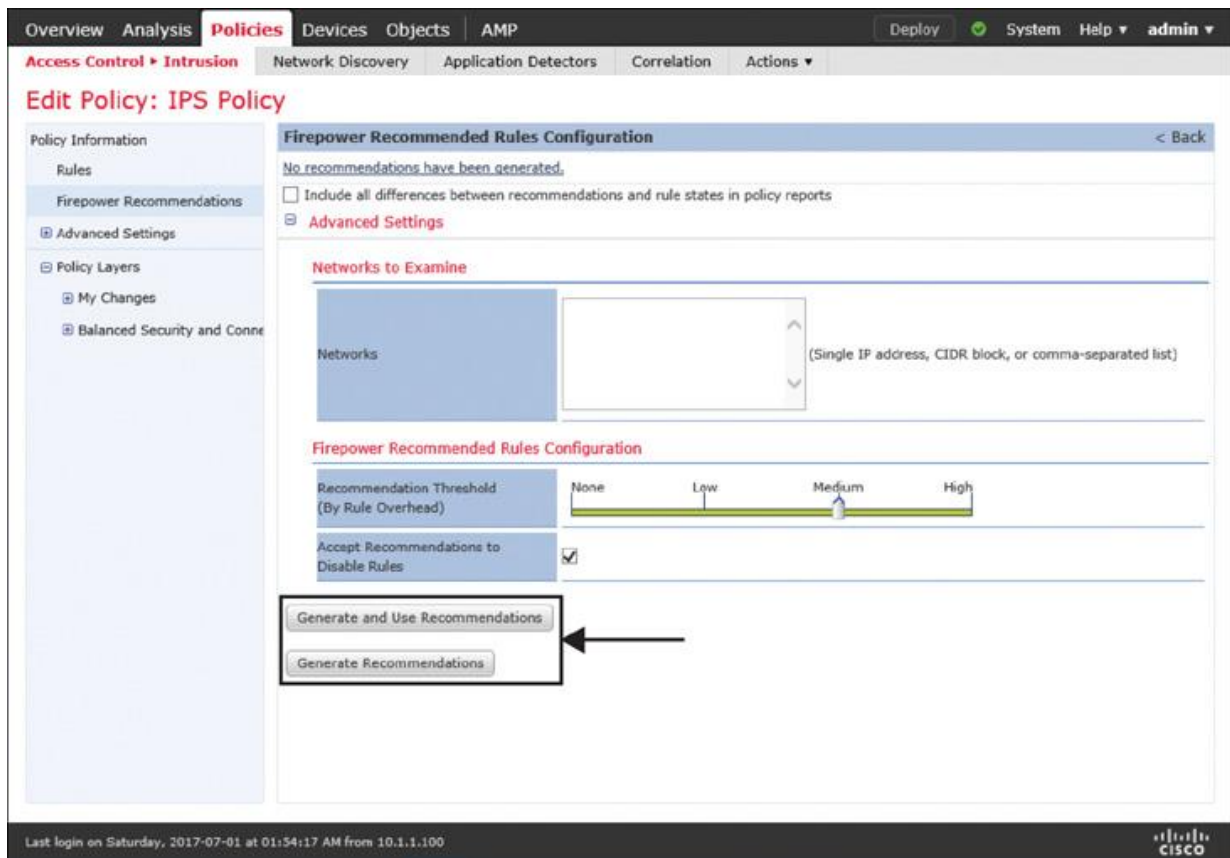


Figure 21-16 Configuration Page to Generate Firepower Recommended Rules

■ Enable the Adaptive Profiles and Enable Profile Update features to leverage the service metadata and allow FTD to apply the enabled intrusion rules to the relevant traffic intelligently.

[Figure 21-17](#) shows the advanced settings for an access control policy where you can configure the Adaptive Profiles and Enable Profile Update settings.

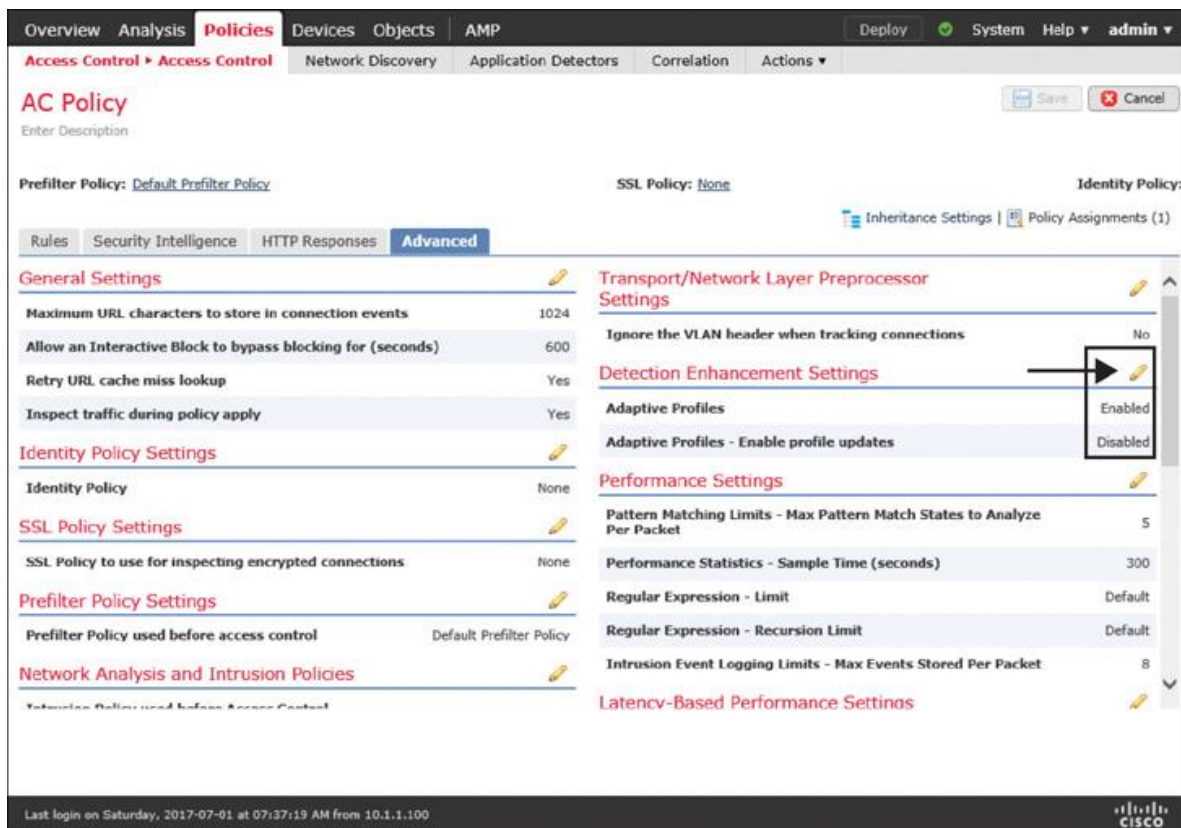


Figure 21-17 Configuration Page for an Adaptive Profile

[Table 21-6](#) shows the differences between the Firepower Recommendations and Enable Profile Update features. Although both features work together to enable traffic-specific intrusion rules, there are some differences between them.

Table 21-6 Firepower Recommendations Versus Enable Profile Update

Firepower Recommendation

Recommends enabling and disabling intrusion rules, based on the discovered applications and hosts.

Can enable a disabled rule if the rule relates to a host and application in the network.

Configured within an intrusion policy.

Enable Profile Update

Compares rule metadata with the applications and operating systems of a host and determines whether the FTD device should apply a certain rule to certain traffic from that host.

Does not change the state of a disabled rule. Only works on the enabled rules in an intrusion policy.

Configured within an access control policy.

Tip

Enable both features—Enable Profile Update and Firepower Recommendations—at the same time. Doing so enables an FTD device to enable or disable the intrusion rules that are related to the hosts, applications, and services running on a network and then apply the enabled rules to relevant traffic from those hosts.

■ In the network analysis policy, configure the Inline Normalization preprocessor with the Normalize TCP Payload option enabled to ensure consistent retransmission of data (see [Figure 21-18](#)).

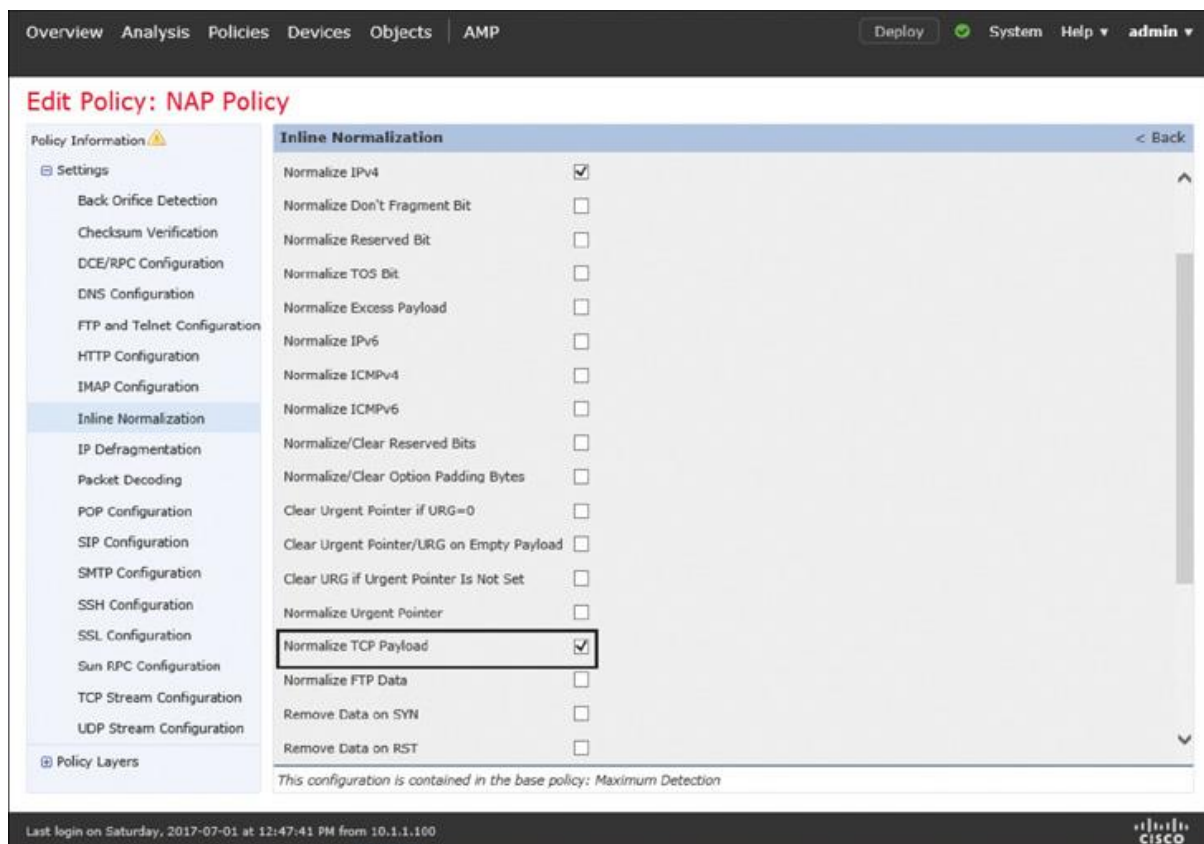


Figure 21-18 Option to Normalize TCP Payload

Some of the best practices are applicable to a particular deployment mode, and depend on your traffic handling policy. For example:

■ If you want to prevent cyber attacks by blocking intrusion attempts, you need to deploy FTD device bump in the wire (BITW). The BITW deployment requires an inline interface pair—you include the ingress and egress interfaces to an inline interface pair and then assign the interface pair to an inline set. To learn more about Inline Mode, see [Chapter 11](#), “[Blocking Traffic Using Inline Interface Mode](#).”

■ If your goal is to deploy FTD for detection-only purposes—that is, you do not want to block an intrusion attempt in real time—consider deploying an FTD device in Inline Tap Mode instead of in Passive Mode. Doing so enables you to switch to Inline Mode faster, without the need for a cabling change. This is critical in case of an emergency. To learn more, read [Chapter 12](#), “[Inspecting Traffic Without Blocking It](#).”

■ If you choose to deploy an FTD device in Passive Mode anyway, make sure the Adaptive Profiles option is enabled on the advanced settings access control policy. This option enables an FTD device to adapt intrusion rules dynamically based on the metadata of the service, client application, and host traffic.

■ When FTD prompts you to select a firewall mode (during initialization after a reimage), choose Routed Mode. While Transparent Mode can block an intrusion attempt, you could accomplish the same goal—transparency or a bump in the wire—by using Inline Mode, which has less configuration overhead. Using the FTD CLI, you can switch between Routed Mode and Transparent Mode. To learn more about Routed Mode, read [Chapter 8, “Firepower Deployment in Routed Mode.”](#)

NGIPS Configuration

Configuring an FTD device as a next-generation intrusion prevention system (NGIPS) can involve three different security policies: network analysis policy, intrusion policy, and access control policy. In the following sections, you will learn how to configure all of these policies in order to deploy an FTD device with NGIPS functionality.

Configuring a Network Analysis Policy

To create a network analysis policy (NAP), you need to navigate to the network analysis policy configuration page. However, the FMC does not provide a direct menu to go there. You can navigate to that page in two ways: through the access control policy configuration page or through the intrusion policy configuration page.

[Figure 21-19](#) shows the navigation to the network analysis policy through the intrusion policy page. You will find a similar link on the access control policy page.

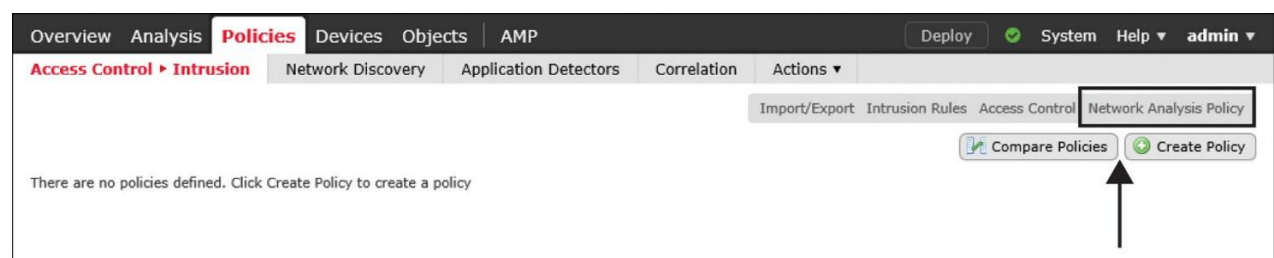


Figure 21-19 *Link to Access the Network Analysis Policy Configuration Page*

Creating a New NAP with Default Settings

Once you are on the network analysis policy configuration page, follow these steps:

Step 1. Click the **Create Policy** button. The Create Network Analysis Policy window appears (see [Figure 21-20](#)).

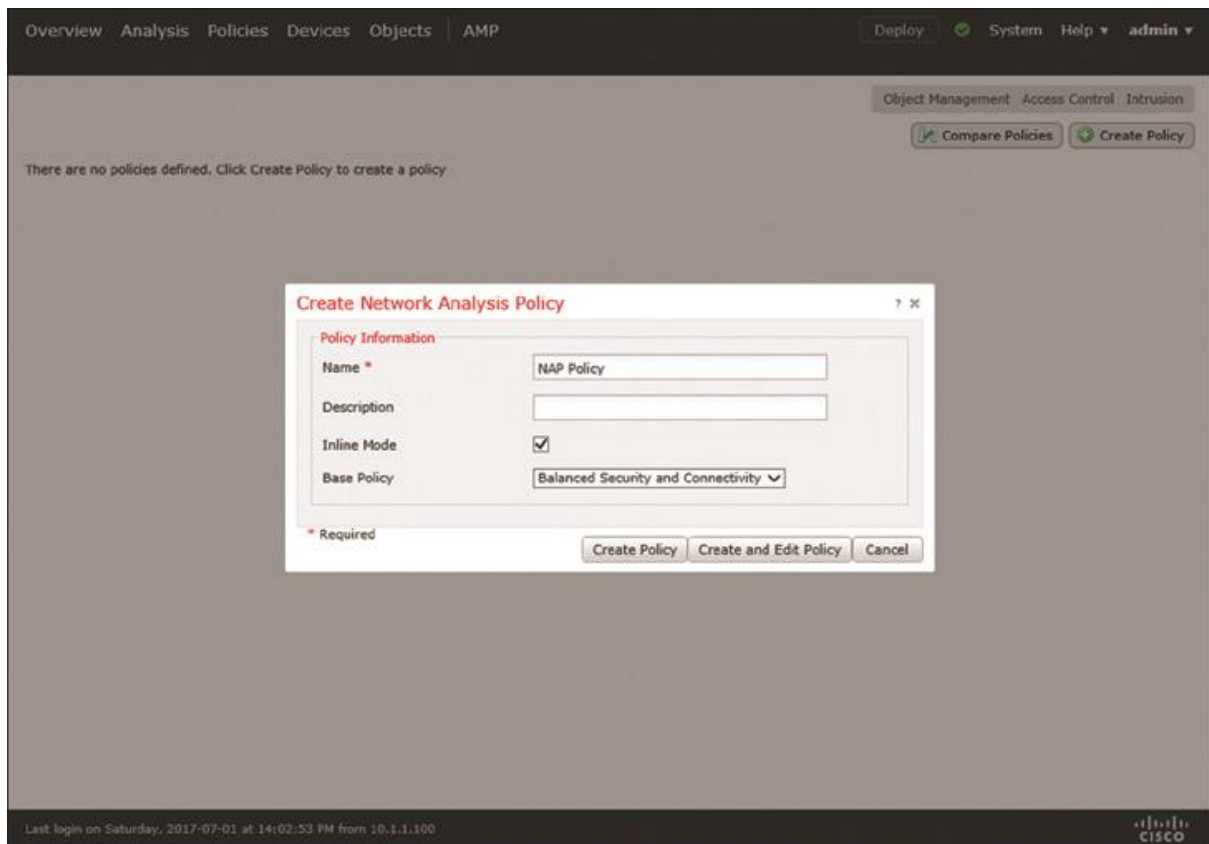


Figure 21-20 Configuration Window to Create a Network Analysis Policy

Step 2. Give a name to the policy.

Note

By default, the Inline Mode option is enabled. It allows the preprocessors to normalize traffic flows and drop any packets that contain anomalies.

Step 3. As the base policy, select **Balanced Security and Connectivity**. This policy provides the best system performance without compromising the detection of the latest and critical vulnerabilities.

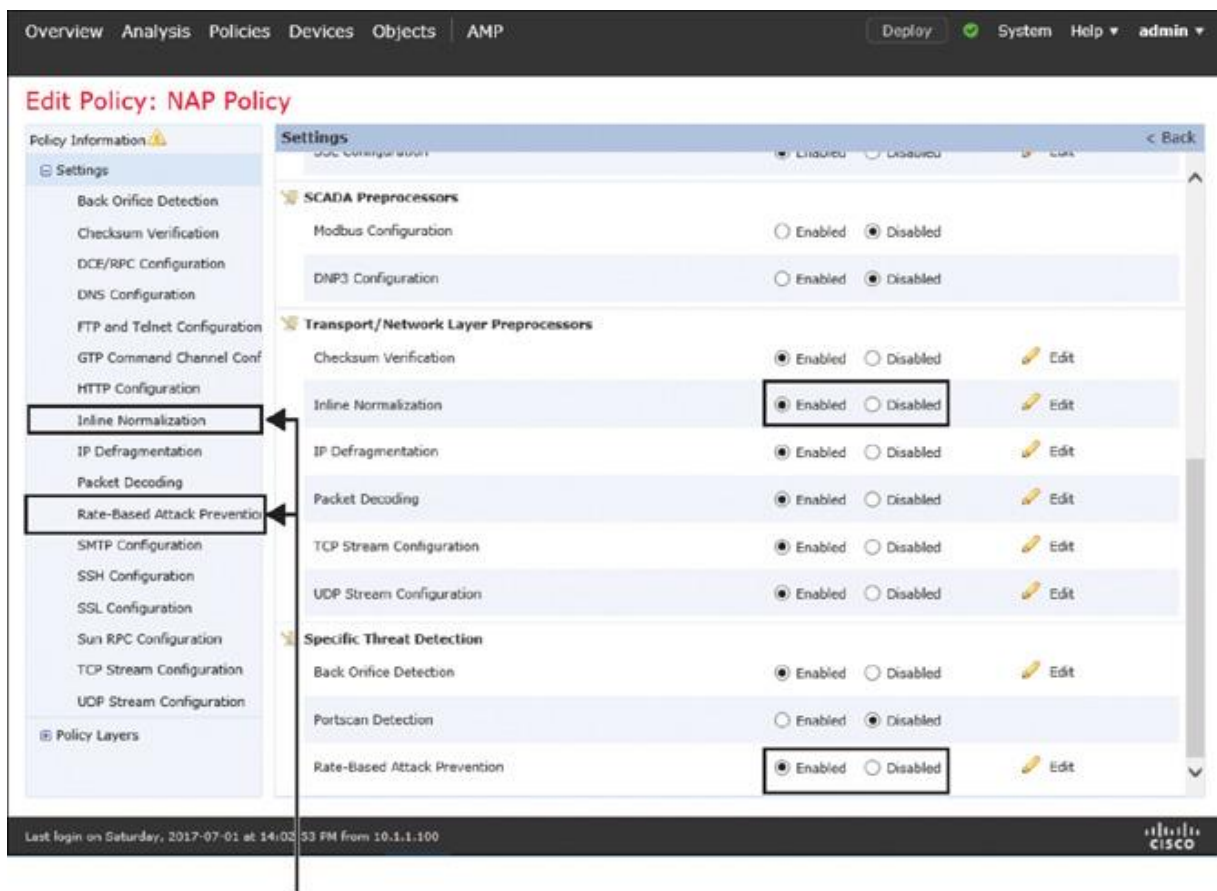
Step 4. Click the **Create Policy** button to create a network analysis policy using the default settings. You will return to the network analysis policy configuration page. The network analysis policy you have just created should appear in the list on this page.

Optionally, if you want to modify the default settings of the network analysis policy, read on; otherwise, skip to the next section, “Configuring an Intrusion Policy”.

Modifying the Default Settings of a NAP

FMC enables you to enable or disable the default settings of a network analysis policy. There are two ways to enter the policy editor page. During the network analysis policy creation, you could select the Create and Edit Policy button instead of clicking the Create Policy button. Alternatively, if you already created a network analysis policy, you could find the policy on the network analysis policy configuration page and select the pencil icon next to it. Both methods can take you to the policy editor page right way.

Step 1. On the network analysis policy editor page, select **Settings** in the panel on the left. A list of preprocessors appears. [Figure 21-21](#) shows the network analysis policy editor page, where you can enable, disable, and modify preprocessor configurations.



The extra preprocessors appear in this list after you enable them on demand.

Figure 21-21 Enabling Extra Preprocessors on Top of a Base Policy

Step 2. Enable (or disable) any desired preprocessors in addition to the preprocessors enabled (or disabled) by default on the base policy.

Tip

Enable the Inline Normalization preprocessor with the Normalize TCP Payload option to ensure consistent retransmission of data (refer to [Figure 21-18](#)).

[Figure 21-22](#) shows the impact of your changes to the network analysis policy. Although Inline Normalization and Rate-Based Attack Prevention preprocessors are disabled on the base policy, your custom configuration overrides the default behavior of the base policy.

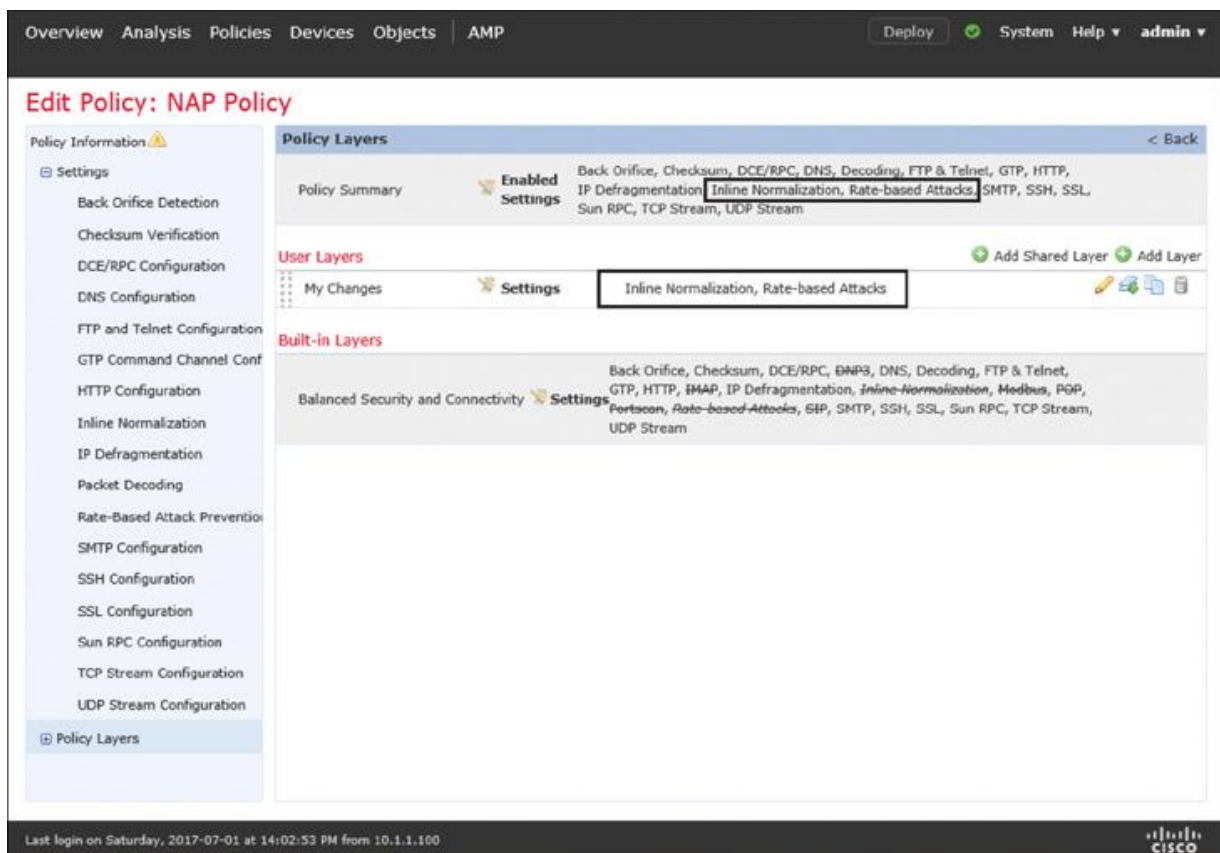


Figure 21-22 Layered View of the Preprocessor Configurations

Step 3. When you are finished with modifications, make sure you save the changes. On the left panel, select the **Policy Information** section, and click the **Commit Changes** button (see [Figure 21-23](#)). This button is comparable to a Save button, in that any modification is saved but not deployed on a managed device.

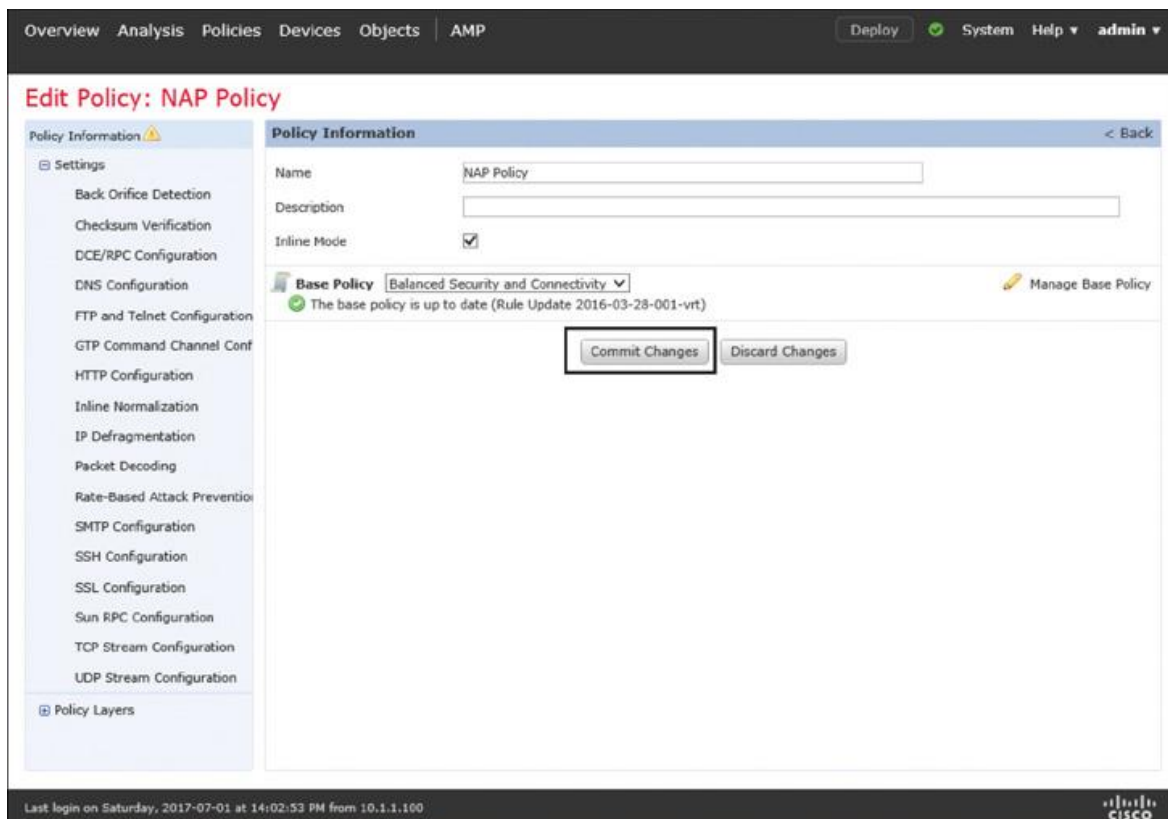


Figure 21-23 Saving Configuration Changes

[Configuring an Intrusion Policy](#)

Intrusion policy configuration is the key part of an NGIPS deployment. This is where you select a system-provided ruleset and enable any additional intrusion rules.

[Creating a Policy with a Default Ruleset](#)

To create an intrusion policy, follow these steps:

Step 1. Navigate to **Policies > Access Control > Intrusion**. The intrusion policy configuration page appears.

Step 2. Click the **Create Policy** button. The Create Intrusion Policy window appears (see [Figure 21-24](#)).

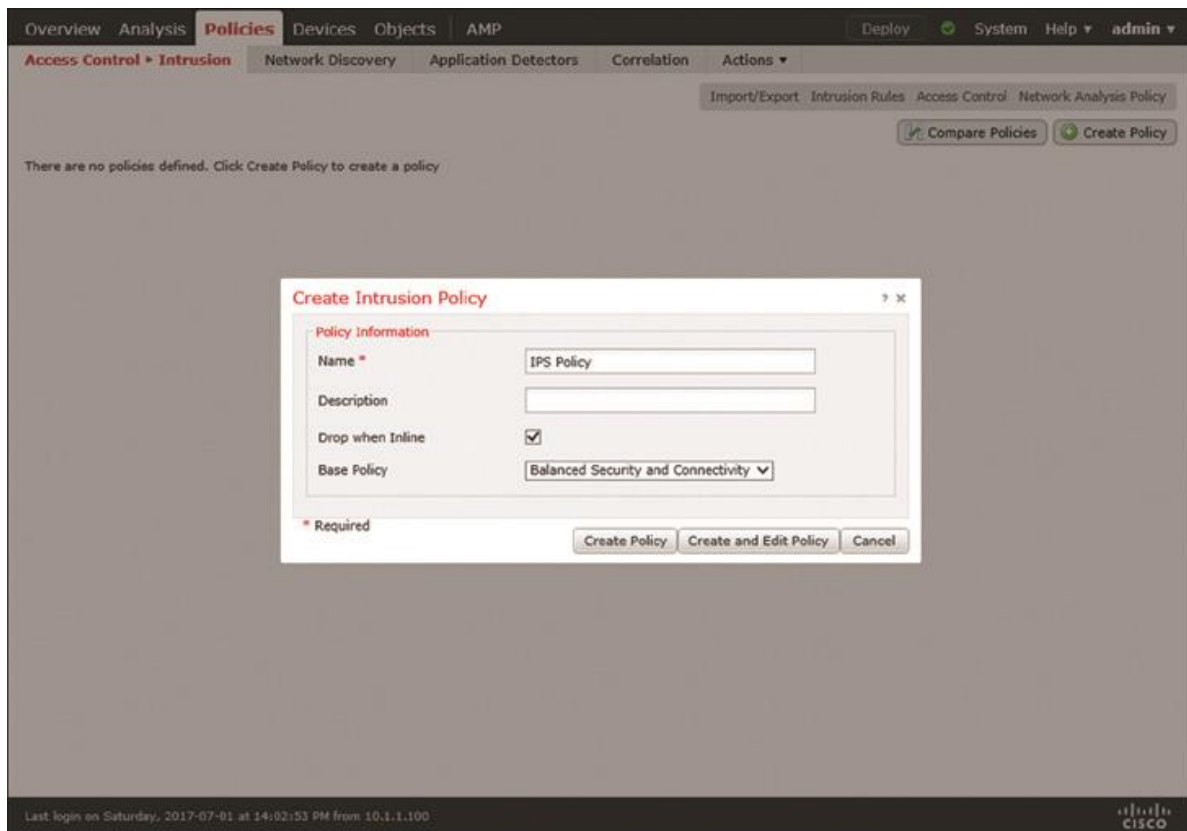


Figure 21-24 Configuration Window to Create an Intrusion Policy

Step 3. Give a name to the policy.

Note

By default, the Drop When Inline option is enabled, which means an FTD device can drop packets when you deploy it in Inline, Routed, or Transparent Mode. This option, however, does not affect the traffic flow if you deploy the FTD device in Inline Tap or Passive Mode.

Step 4. Select **Balanced Security and Connectivity** as the base policy. This policy provides the best system performance without compromising the detection of the latest and critical vulnerabilities.

Step 5. Click the **Create Policy** button to create an intrusion policy using the default settings.

[Incorporating Firepower Recommendations](#)

By default, the Firepower Recommendations feature is disabled, as it can consume additional resources to analyze the network discovery data and associated vulnerabilities and generate recommendations accordingly. You should leverage the Firepower Recommendations feature, though, because it can suggest enabling or disabling intrusion rules based on the operating systems, services, and applications running in your network.

Tip

Generate and use Firepower Recommendations *after* the majority of your network hosts generate traffic and your FTD discovers them. If you apply recommendations without waiting some time to perform the network discovery, FTD may recommend disabling many intrusion rules, which may not be desired.

To generate and use Firepower Recommendations, follow these steps:

Step 1. Edit the intrusion policy where you want to enable Firepower Recommendations. If you are currently in the process of creating an intrusion policy, click the **Create and Edit Policy** button to enter the policy editor page right away. If a policy is already created, you can enter the editor page by using the pencil icon, which is next to the name of the intrusion policy (see [Figure 21-25](#)).

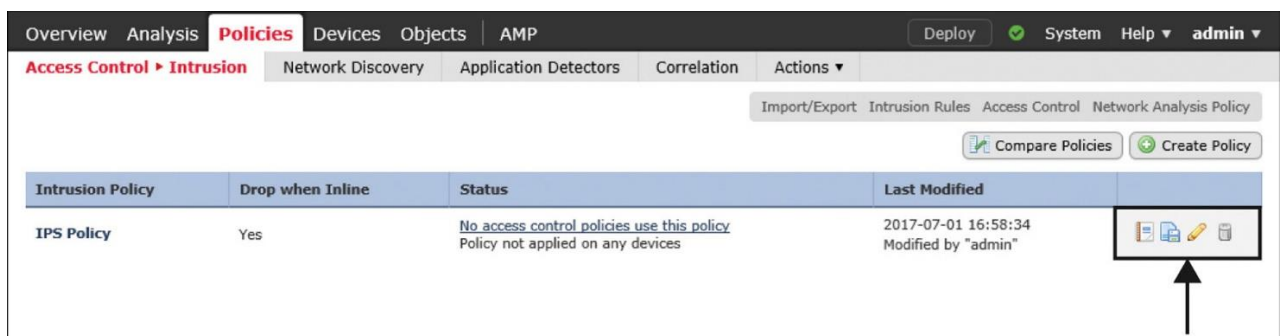


Figure 21-25 Option to Edit an Intrusion Policy

Step 2. On the intrusion policy editor page, select **Firepower Recommendations** from the blue panel on the left. The Firepower Recommended Rule Configuration page appears.

Step 3. Define the networks to examine and set Recommendation Threshold (by Rule Overhead) to low or medium so that the intrusion rules with higher processing overhead are not considered in the recommended ruleset.

[Figure 21-26](#) shows the configuration of Firepower Recommendations. The configuration in this example analyzes traffic from the 192.168.1.0/24 network and suggests intrusion rules based on the application, services, and operating systems running on the network hosts.

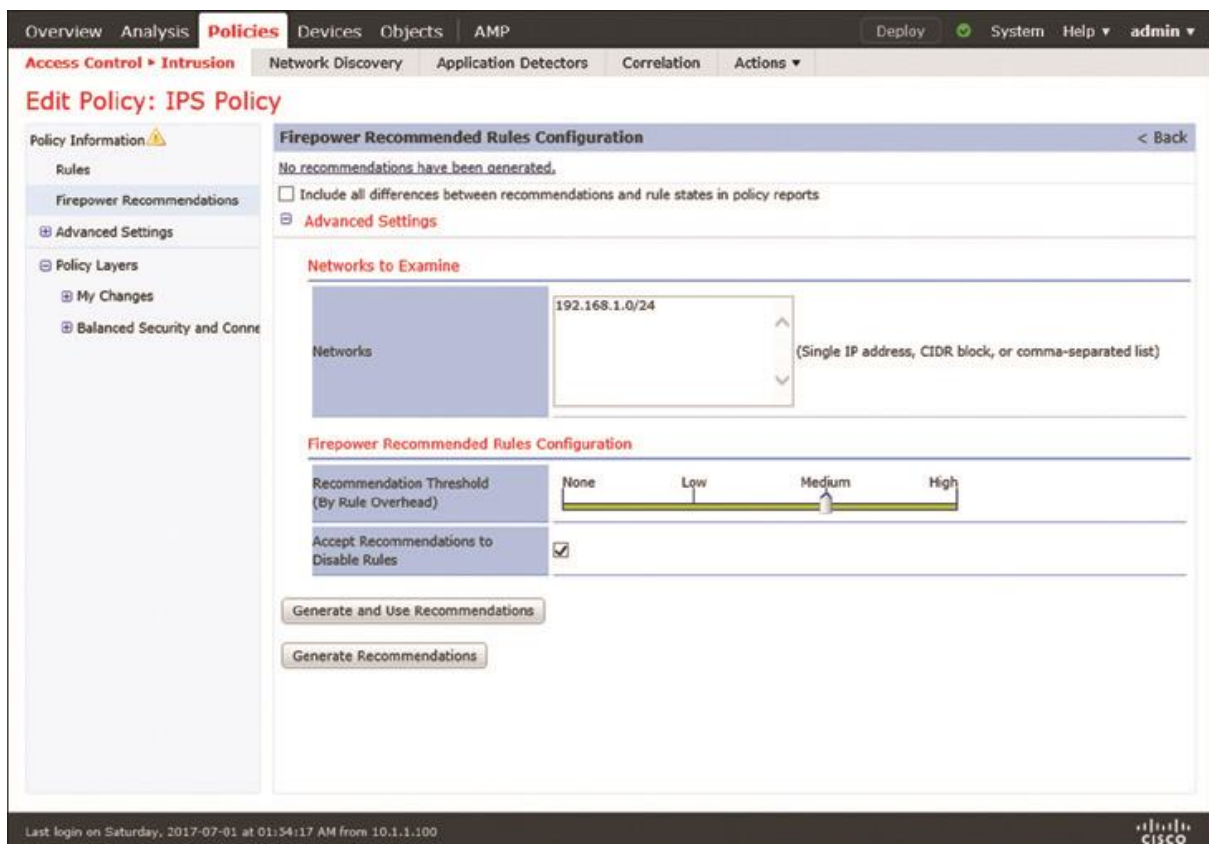


Figure 21-26 *Firepower Recommended Rules Configuration*

Step 4. Click the **Generate and Use Recommendations** button. This button appears if the FMC did not generate any recommendation before. If a recommendation has already been generated, you will see different buttons, whose labels are self-explanatory, such as Update Recommendations, Do Not Use Recommendations, and so on.

[Figure 21-27](#) shows the recommendations for 963 rules (20 rules to generate events, 943 rules to drop and generate events). These rules are suggested based on the information on two hosts.

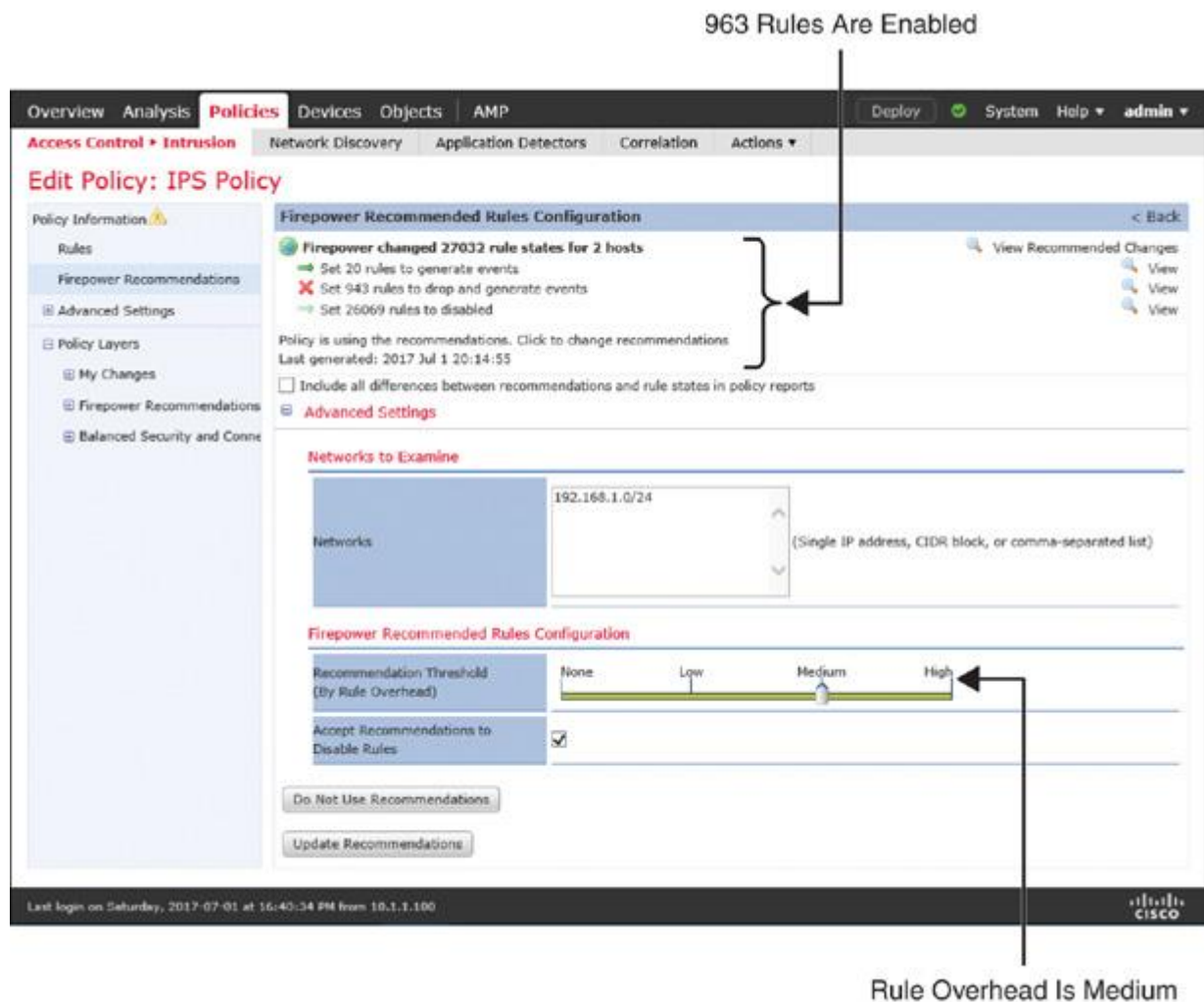


Figure 21-27 Firepower Recommended Rules—Rule Overhead Is Medium

For testing purposes, you can try regenerating recommendations with low rule overhead threshold. You will notice that, for the same network hosts, the number of recommended rules is now significantly lower. [Figure 21-28](#) shows the recommendations for only three rules (two rules to generate events and one rule to drop and generate events). The number of recommended rules for the same two network hosts are significantly lower because the rule processing overhead is set to low.

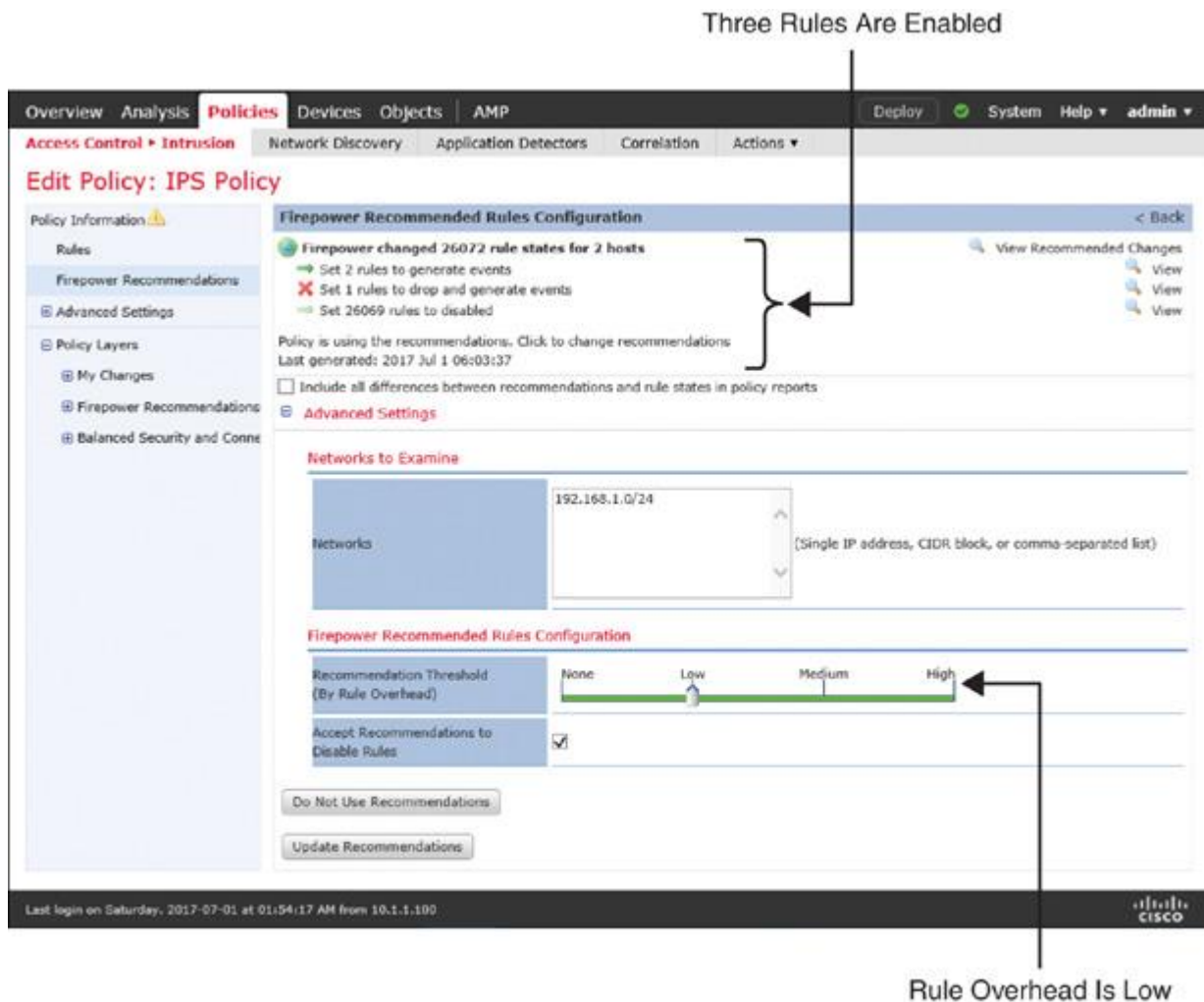


Figure 21-28 *Firepower Recommendations (for Testing Purposes)—Rule Overhead Is Low*

Step 5. Make sure to save any changes by clicking the **Commit Changes** button on the Policy Information page.

Enabling or Disabling an Intrusion Rule

Optionally, if you want to enable or disable any intrusion rule from the default ruleset, follow these steps:

Step 1. Edit the intrusion policy where you want to enable or disable an intrusion rule. If you are currently in the process of creating an intrusion policy, click the **Create and Edit Policy** button to enter the policy editor page right away. If a policy has already been created, you can enter the editor page by using the pencil icon, which is next to the name of the intrusion policy.

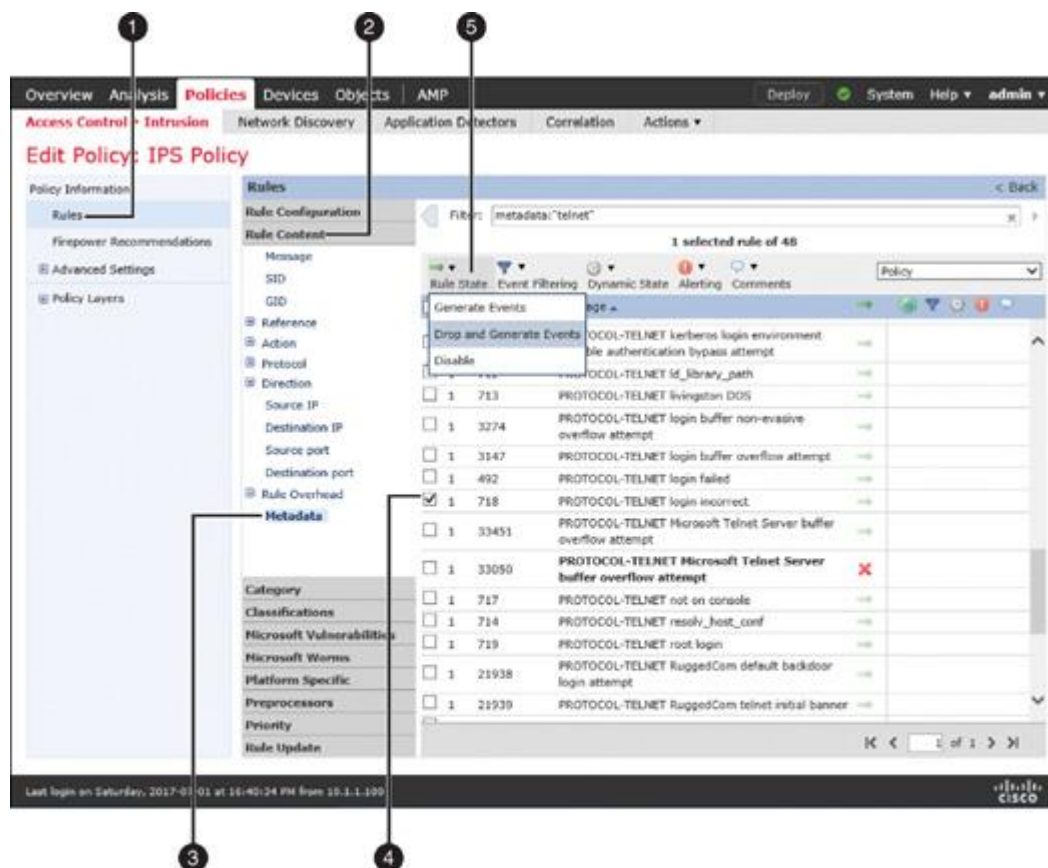
Step 2. On the intrusion policy editor page, select **Rules** in the panel on the left. A list of rules appears.

Step 3. When you find a desired rule, select its check box and define the Rule State to enable the rule.

Tip

If you manually enable additional intrusion rules (on top of a base policy), and you want FTD to block any matching packets, the state of those rules should be set to Drop and Generate Events.

[Figure 21-29](#) illustrates the steps to find and enable a desired rule using the intrusion policy editor.



Steps to enable a rule

1. Select **Rules** on the left panel.
- 2-3. Select the criteria to find the desired rules.
4. Select the desired rules using the check box.
5. Define an action by selecting a rule state.

Figure 21-29 Enabling an Intrusion Rule

Step 4. Make sure you save any changes by clicking the **Commit Changes** button on the Policy Information page.

Setting Up a Variable Set

One of the important steps in configuring an intrusion policy is to define the values of a variable set. Because a Firepower system does not make this configuration step mandatory, users may overlook this step.

You must define the \$HOME_NET variable based on the network address used in your LAN. If the default value of a variable that represents a specific server is set to any or \$HOME_NET, you must change it to a more specific value. Doing so makes a Snort rule more effective and reduces the probability of false positive alerts. Thus, a proper variable setting can improve performance.

To modify the system-provided default set or to add a new variable set, follow these steps:

Step 1. Navigate to **Objects > Object Management**.

Step 2. Select **Variable Set** from the menu on the left. The list of available variable sets appears.

Step 3. You can edit an existing variable set or create a new one. To create a new one, click the **Add Variable Set** button, and the New Variable Set configuration window appears.

Step 4. Find the variables that need updates. Click a variable's pencil icon to edit the value of the variable. To define a value, you can add a network address directly or select a predefined network object. The system also allows you to create a new network object on the fly.

[Figure 21-30](#) shows how to navigate to the New Variable Set configuration window, where you can customize the default variables. For example, when you click the pencil icon next to the HOME_NET variable, the Edit Variable HOME_NET window, which is a *variable editor*, appears. [Figure 21-30](#) shows the customized values for the HOME_NET, EXTERNAL_NET, and TELNET_SERVERS variables. (You can see the variable editor in the background in [Figure 21-31](#).)

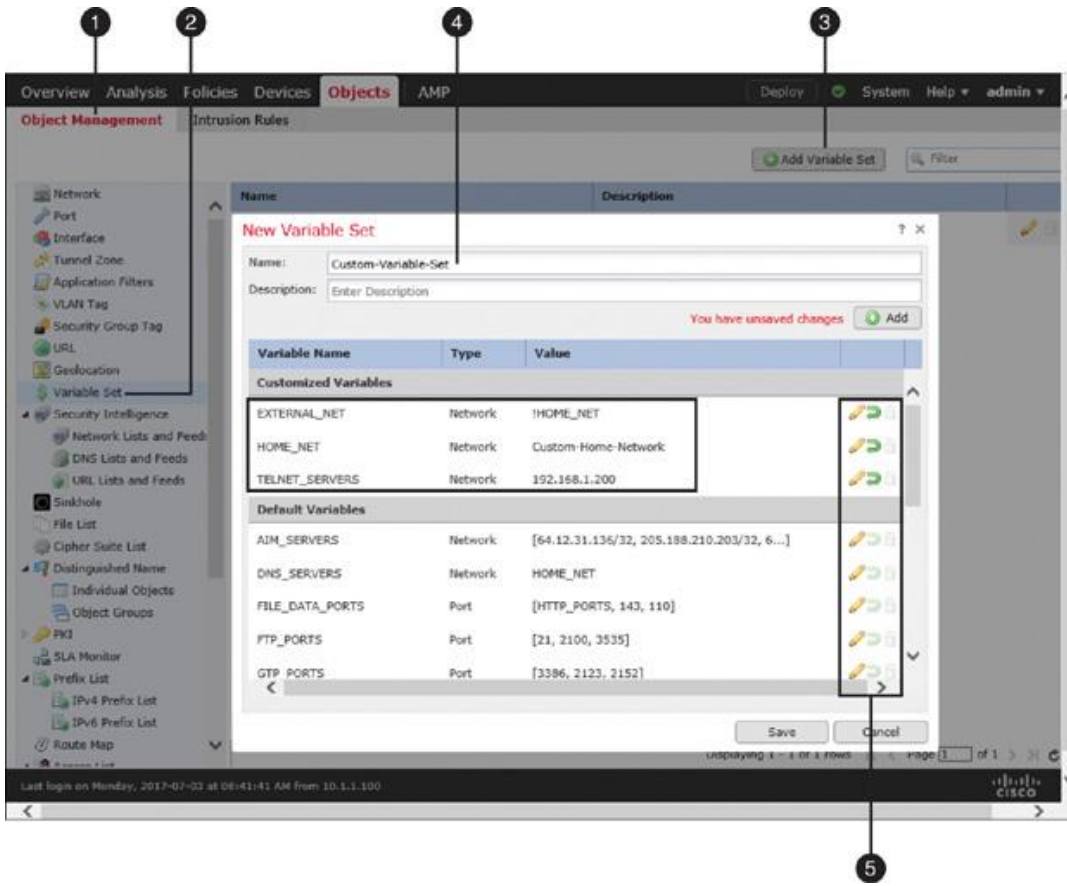


Figure 21-30 Creating a Custom Variable Set

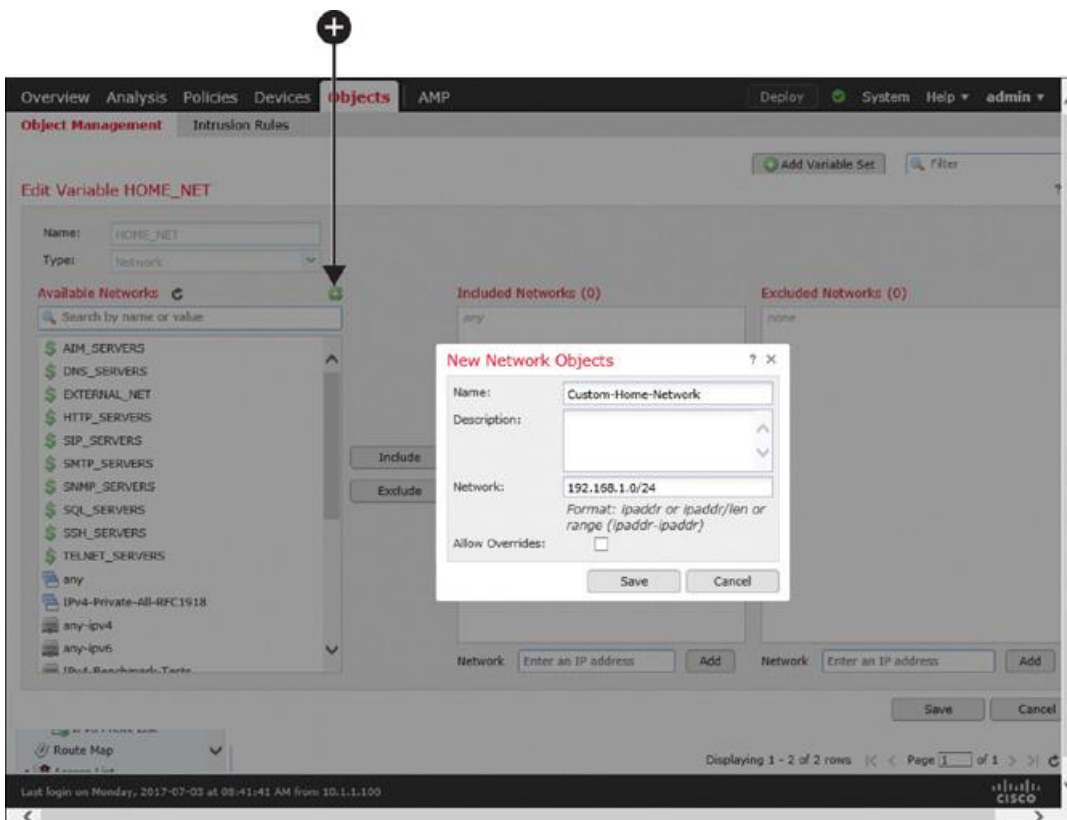


Figure 21-31 *Creating a Custom Network Object*

[Figure 21-31](#) shows the definition of a new network object, Custom-Home-Network, which will replace the default value of the HOME_NET variable. In the background, you can see the green plus icon on the variable editor that opens the New Network Objects configuration window also shown here.

Step 5. When the values of the necessary variables are updated with the new network addresses or ports, save the configuration.

Configuring an Access Control Policy

In the previous sections of this chapter, you have configured various components to detect anomalies and intrusion attempts. However, they do not begin acting upon traffic until and unless you deploy the necessary policies on an FTD device. On an access control policy, you should configure the following items for the best detection:

■ **Adaptive Profiles:** An access control policy allows you to enable Adaptive Profiles and Enable Profile Updates features, which empower an FTD device to apply the enabled intrusion rules intelligently to the relevant traffic.

[Figure 21-32](#) shows the configuration window for the Adaptive Profiles and Enable Profile Updates features. To find this window, go to the Advanced tab of the access control policy and use the pencil icon next to Detection Enhancement Settings.

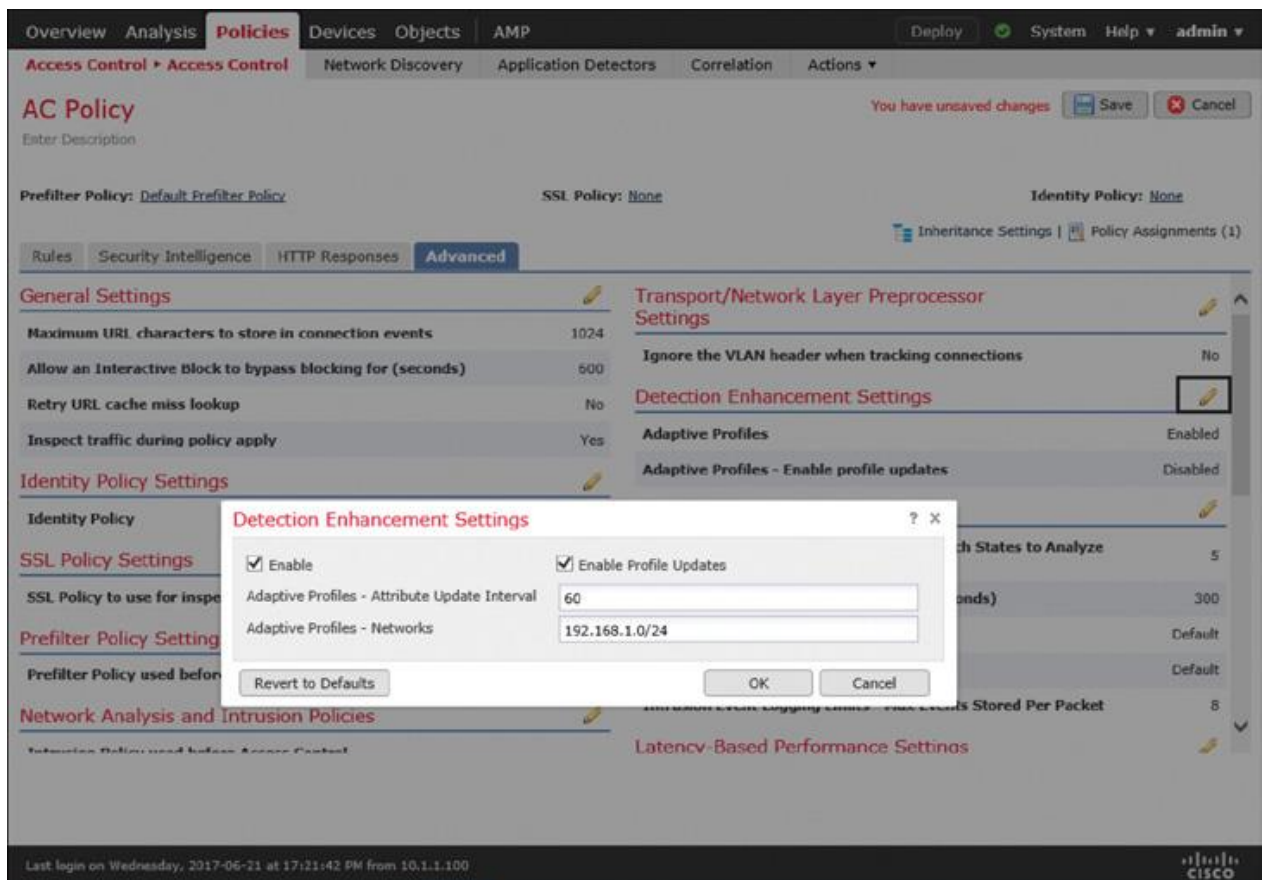


Figure 21-32 *Configuring the Adaptive Profile and Profile Update*

■ **Invoking the policies:** An access control policy invokes various Firepower policies that you configure all over the GUI (for example, network analysis policy, intrusion policy).

First, on the Advanced tab, select an intrusion policy that is applied before an access rule is determined for the traffic. Here, you can also select a variable set that is used by the intrusion policy and a network analysis policy that the system uses by default.

[Figure 21-33](#) shows the selection of an intrusion policy, a variable set, and a network analysis policy with an access control policy.

Then, when you add an access rule, you can invoke an intrusion policy and a variable set for the matching traffic. You can define this on the Inspection tab of the access rule editor.

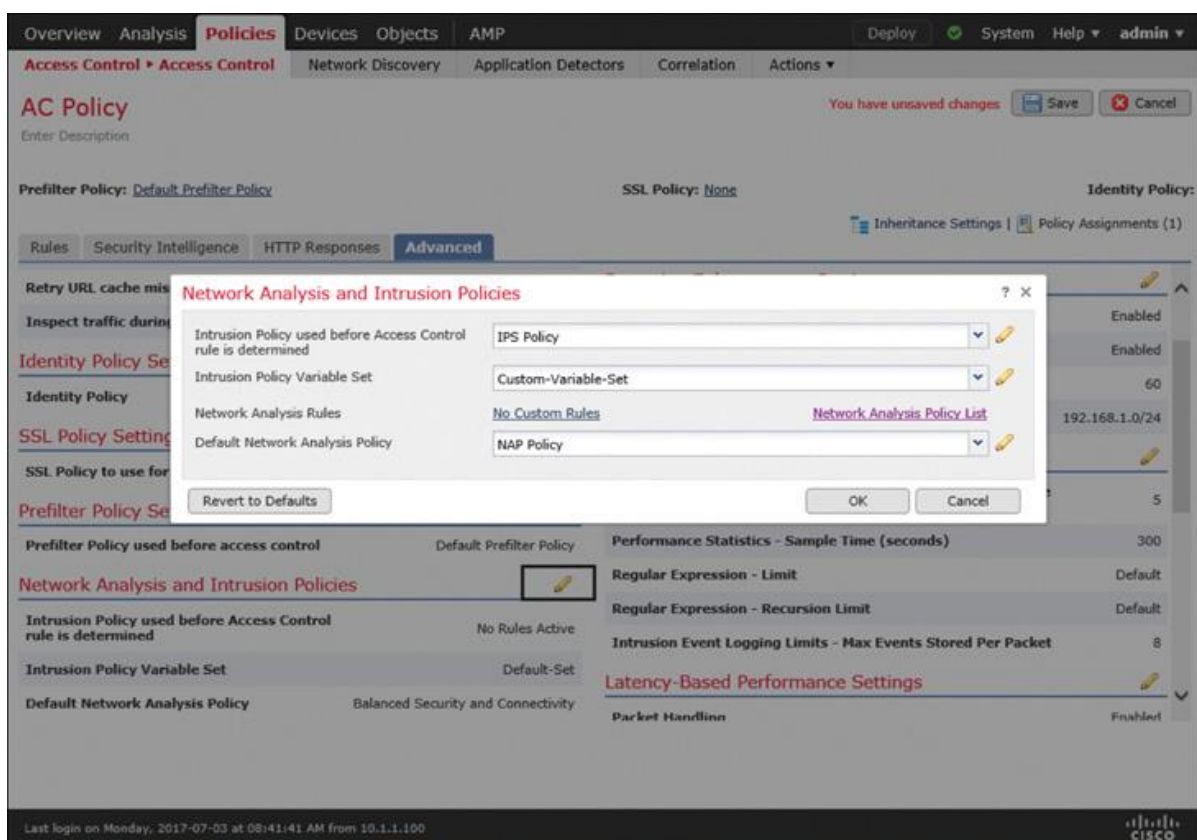


Figure 21-33 *Invoking an Intrusion Policy Before an Access Rule Is Determined*

[Figure 21-34](#) shows the selection of an intrusion policy and a variable set within an access rule. When a packet matches the condition of this access rule, it is subject to the inspection of this intrusion policy and variable set.

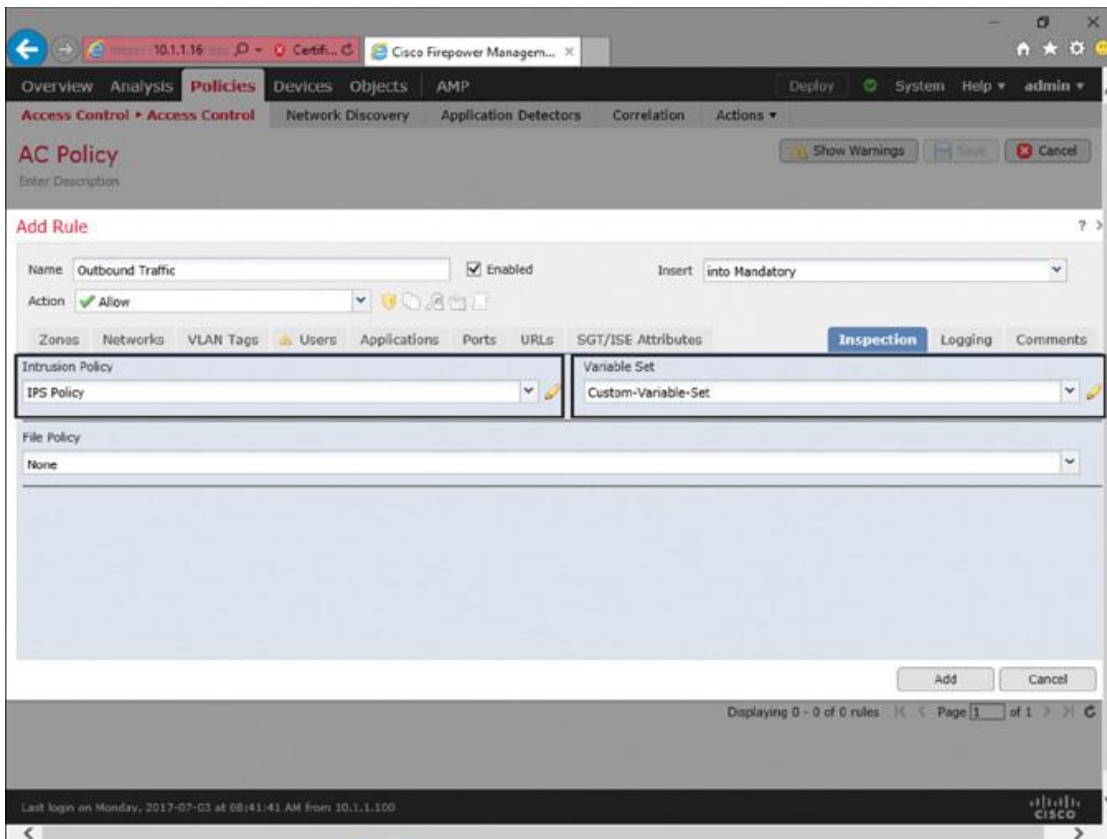


Figure 21-34 *Invoking an Intrusion Policy When It Matches a Rule Condition*

Finally, for any traffic that does not match an access rule condition, you can select an intrusion policy as the default action.

[Figure 21-35](#) shows the selection of a custom intrusion policy as the default action for the traffic that does not match any of the access rule conditions.

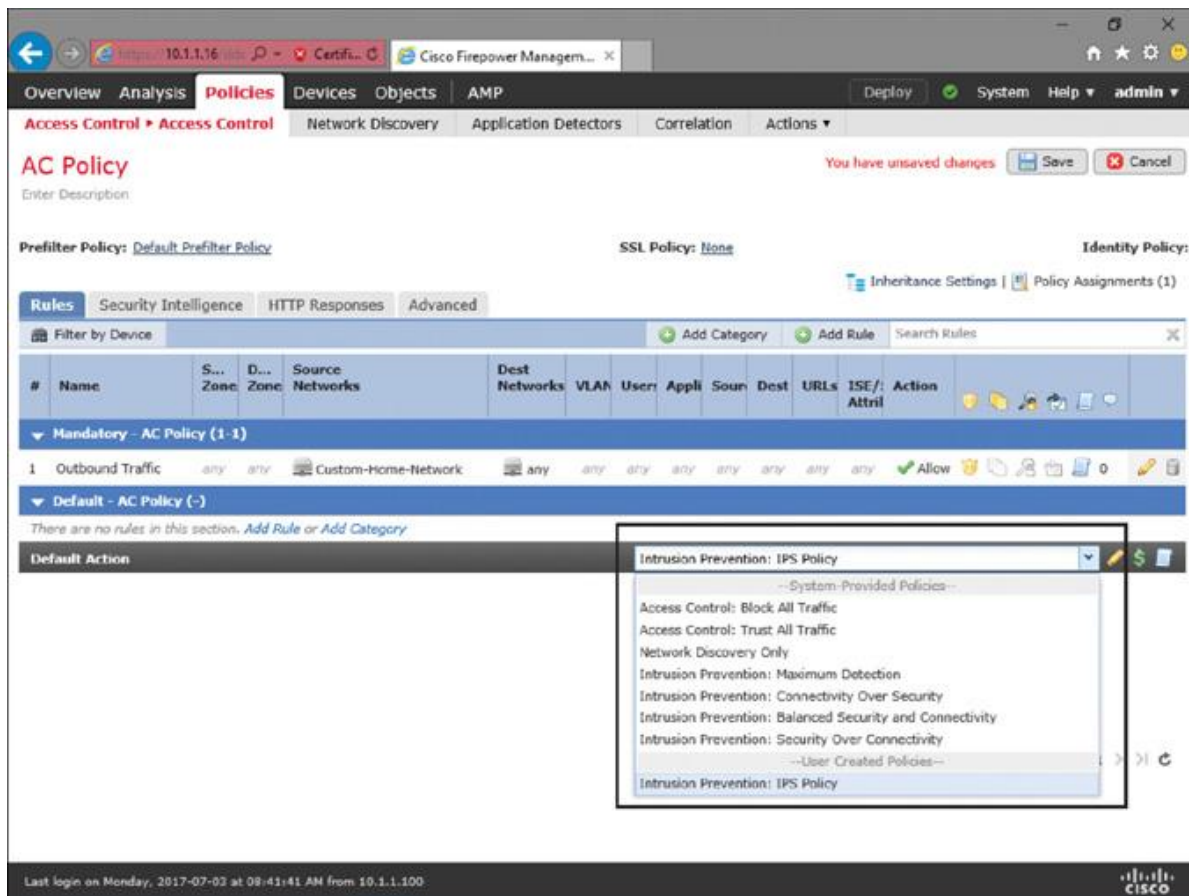


Figure 21-35 *Invoking an Intrusion Policy When Packets Do Not Match Any Access Rules*

Once you have invoked all the necessary policies and configurations in your access control policy, you must click the **Save** button to store the configurations locally. Finally, to activate the new policies, click the **Deploy** button.

[Figure 21-36](#) shows three places where you can connect an intrusion policy with an access control policy. It also clarifies their relationships with traffic flow.

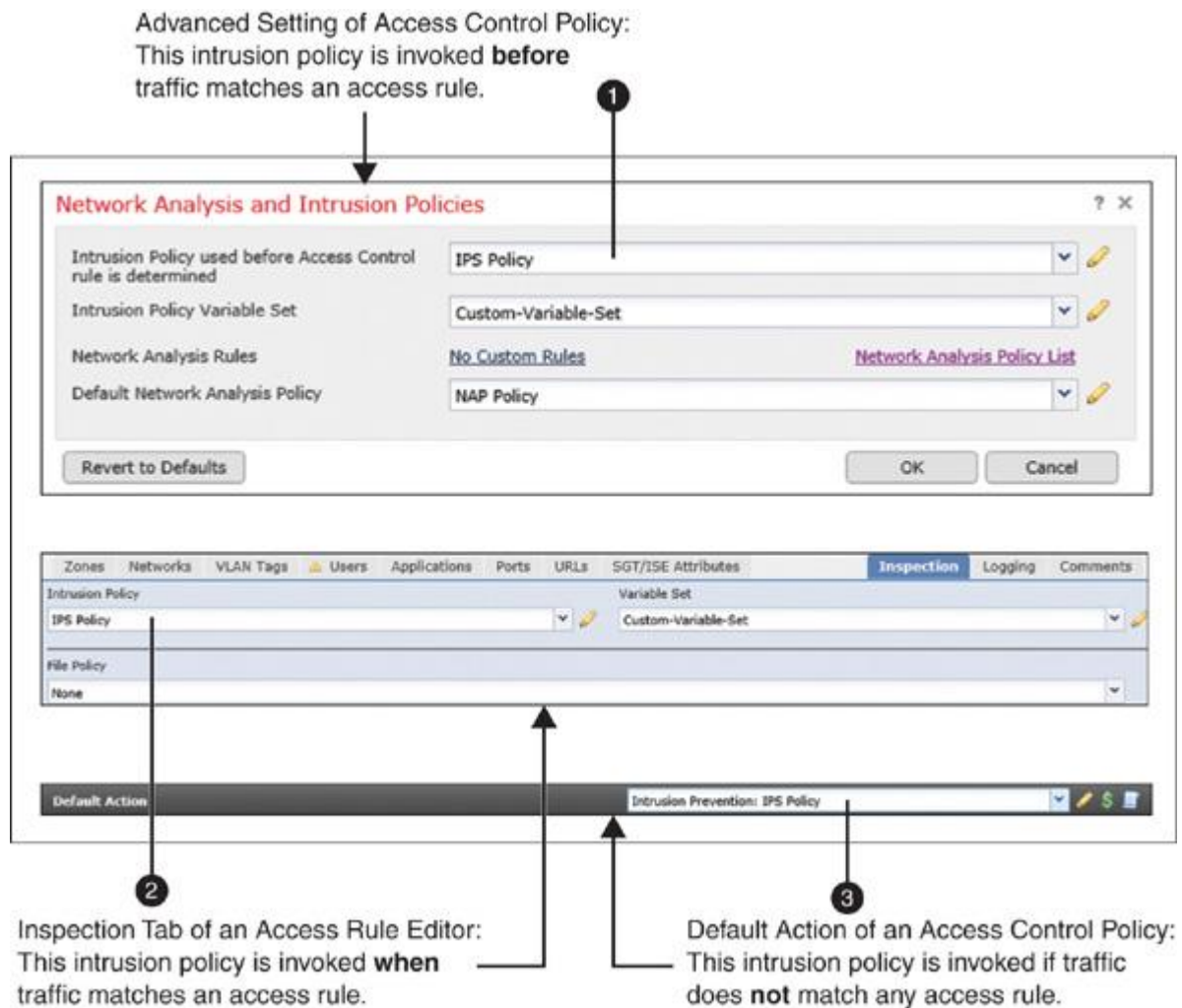


Figure 21-36 Various Places to Invoke an Intrusion Policy

Verification and Troubleshooting Tools

To verify whether an intrusion policy is active, you can run traffic to and from your network host. However, if the traffic does not carry a signature of any vulnerability, FTD does not trigger an intrusion alert for it.

To verify the action of an intrusion policy, this chapter uses a simple Snort rule 1:718. Here is the rule syntax:

[Click here to view code image](#)

```

alert tcp $TELNET_SERVERS 23 -> $EXTERNAL_NET
any (msg:"PROTOCOL-TELNET login incorrect"; flow:to_client, established;
content:"Login incorrect";

metadata: ruleset community, service telnet; classtype: bad-unknown; sid:718;
rev:16; )

```

According to the syntax of this rule, when a Telnet server does not authenticate a client and responds to the client with a “Login incorrect” message on its payload (due to an incorrect login credential), an FTD device triggers this rule to prevent any potential brute-force attack. Furthermore, if you define a variable set precisely, this rule is applicable on the Telnet traffic to \$EXTERNAL_NET. It should not apply on the Telnet traffic to \$HOME_NET.

Figure 21-37 shows the payload of a packet on a packet analyzer. A Telnet server sends this packet when you enter an incorrect credential. Snort rule 1:718 can detect this payload.

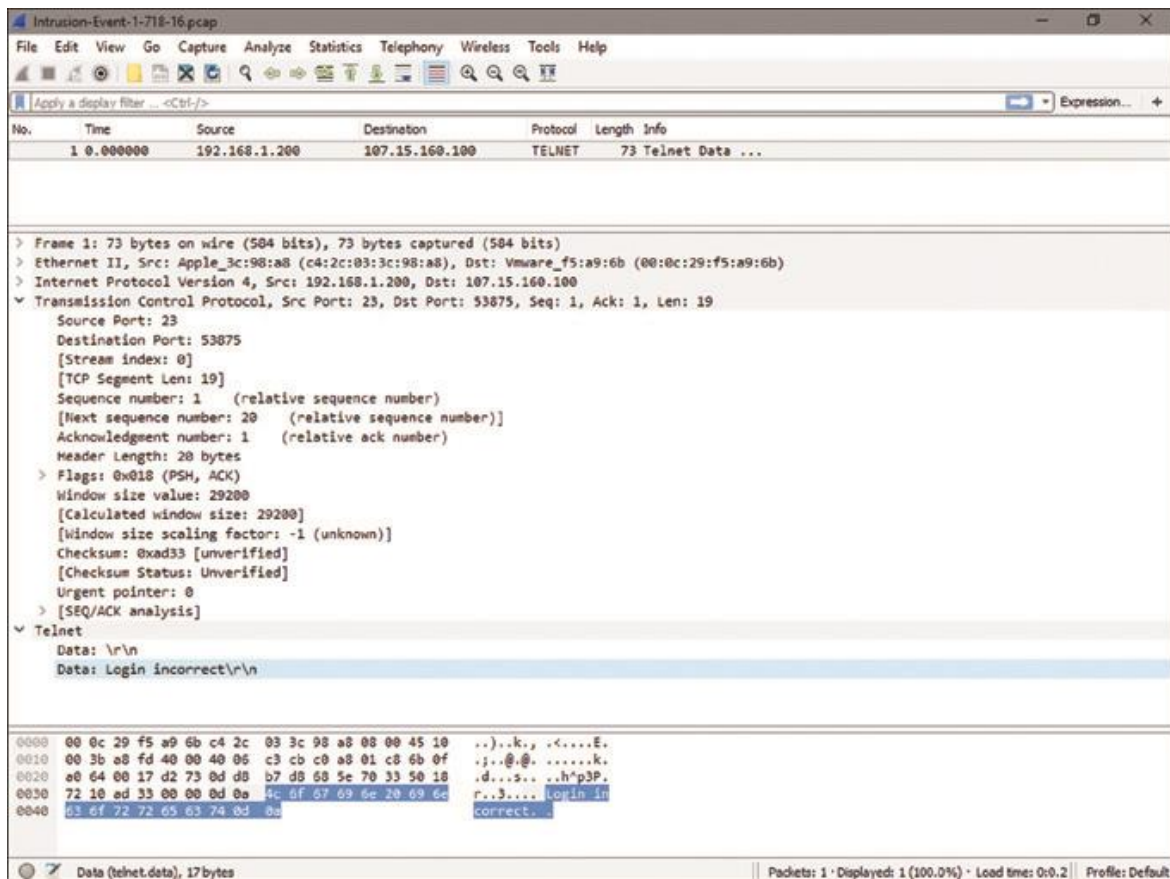


Figure 21-37 Packet Containing “Login incorrect” on the Payload

[Figure 21-38](#) shows the lab topology that is used in the configuration examples in this chapter.

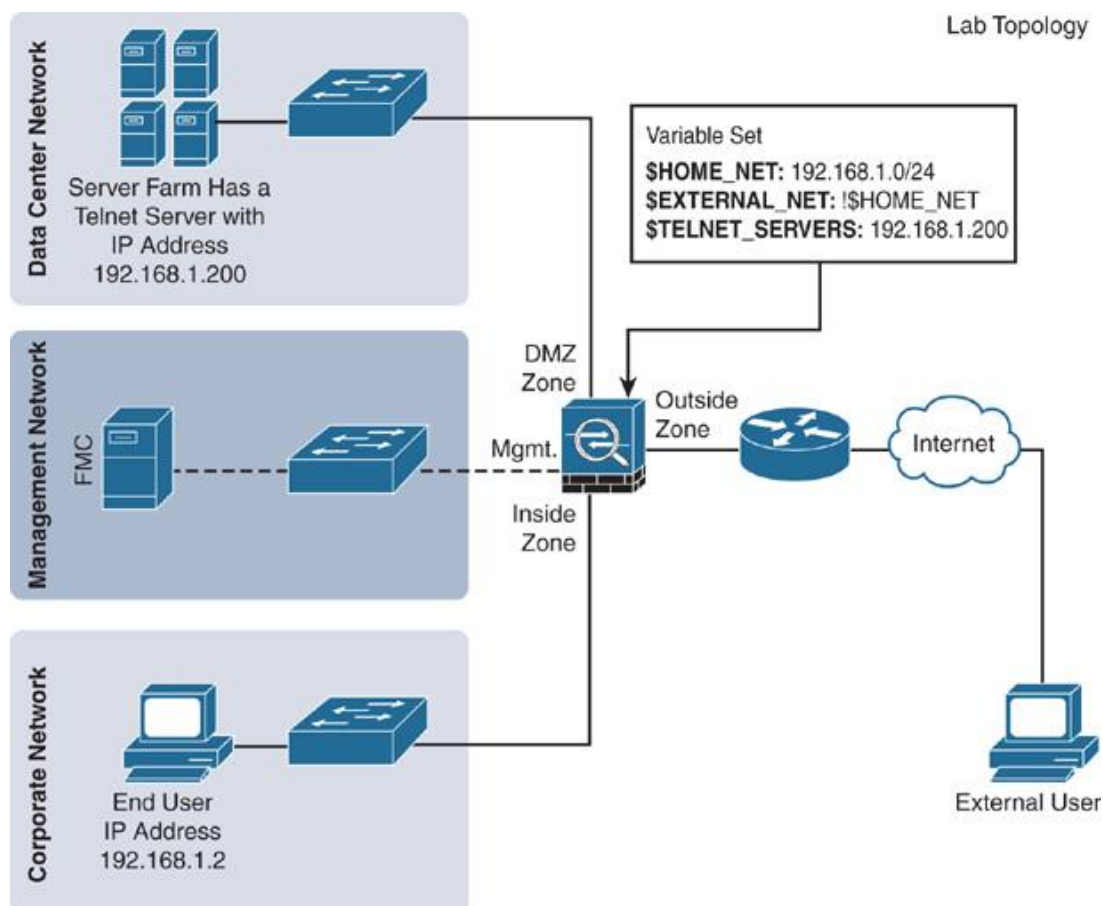


Figure 21-38 *Lab Topology Used in This Chapter*

If you attempt to connect to your Telnet server from an external network host and enter a valid login credential, you will be able to access the server as usual. However, if you enter an incorrect credential, the server sends the client a “Login incorrect” message in a packet.

[Example 21-1](#) shows the messages on the CLI when you attempt to connect to a Telnet server running on a Linux-based system. Note the “Login incorrect” message when the login attempt is unsuccessful.

Example 21-1 *Telnet Server Connection Attempts*

[Click here to view code image](#)

! When a login attempt is successful

```
external-user@Fedora:~$ telnet 192.168.1.200
```

```
Trying 192.168.1.200... Open
```

Connected to 192.168.1.200.

Ubuntu login: internal-user

Password: *****

Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-81-generic x86_64)

internal-user@Ubuntu:~\$

! When a login attempt is unsuccessful

external-user@Fedora:~\$ **telnet 192.168.1.200**

Trying 192.168.1.200... Open

Connected to 192.168.1.200.

Ubuntu login: internal-user

Password: <incorrect_password>

Login incorrect

Ubuntu login:

Tip

Some Telnet servers may return a different failure message, such as “Login Failed.” To detect this string, a different Snort rule, 1:492, is available.

Depending on the rule state, policy setting, and interface mode, a Firepower system can act differently on the same Telnet traffic, and you may find different types of intrusion events for the same Snort rule. For example, if the interface mode is set to Inline Mode, the intrusion policy is set to Drop When Inline, and the rule state is Drop and Generate Events, then an FTD device can block a matching packet. The FMC displays a “dropped” event (indicated by a dark gray down arrow).

However, if the Drop When Inline option is unchecked in the intrusion policy, or if the interface mode is Inline Tap Mode or Passive Mode, the FMC shows a “would have dropped” event (indicated by a light gray down arrow). To find more scenarios for “would have dropped” events, see [Chapter 12](#).

Figure 21-39 shows three different types of intrusion events triggered by the same Snort rule.

Rule State: Drop and Generate Events
Interface Mode: Inline Tap, Passive, or Inline Mode when the Drop When Inline option is disabled.

Time	Inflow Result	Source IP	Destination IP	Source Port / ICMP Type	Message	Classification
2017-07-03 17:44:29		192.168.1.200	107.15.160.100	23 (telnet) / tcp	PROTOCOL-TELNET login incorrect (1:718:16)	Potentially Bad T
2017-07-03 17:07:37		192.168.1.200	107.15.160.100	23 (telnet) / tcp	PROTOCOL-TELNET login incorrect (1:718:16)	Potentially Bad T
2017-07-03 16:23:31		192.168.1.200	107.15.160.100	23 (telnet) / tcp	PROTOCOL-TELNET login incorrect (1:718:16)	Potentially Bad T

Rule State: Drop and Generate Events
Interface Mode: Inline

Rule State: Generate Events
Interface Mode: Inline, Inline Tap, or Passive

Figure 21-39 Snort Rule 1:718 Generating Intrusion Events

To analyze an intrusion event further, you can click on the down arrow at the beginning of each row. It allows you to drill down into an intrusion event and the associated packet data to determine whether an event is false positive.

Figure 21-40 shows various contextual information about an intrusion event (for example, timestamp, priority, and classification of the event). You can also find the ingress and egress interfaces, source and destination details, and any associated rule and policy references.

Events By Priority and Classification [\[switch workflow\]](#)

Drilldown of Event, Priority, and Classification > [Table View of Events](#) > [Packets](#) 2017-07-03 11:39:00 - 2017-07-03 16:40:16 Expanding

Search Constraints [\(Edit Search\)](#)

Event Information

Event	PROTOCOL-TELNET login incorrect (1:718:16)
Timestamp	2017-07-03 16:23:31
Classification	Potentially Bad Traffic
Priority	medium
Device	FTD
Ingress Interface	INSIDE_INTERFACE
Egress Interface	OUTSIDE_INTERFACE
Source IP	192.168.1.200
Source Port / ICMP Type	23 (telnet) / tcp
Destination IP	107.15.160.100
Destination Port / ICMP Code	53875 / tcp
Destination Country	USA
Intrusion Policy	IPS Policy
Access Control Policy	AC Policy
Access Control Rule	Default Action
Rule	alert tcp \$TELNET_SERVERS 23 -> \$EXTERNAL_NET any (msg:"PROTOCOL-TELNET login incorrect"; flow:to_client,established; content:"Login incorrect"; metadata:ruleset community, service telnet; classtype:bad-unknown; sid:718; rev:16;)
Summary	This event is generated when an attempted telnet login fails from a remote user.

Actions

Packet Information

FRAME 1 (Expand All)

- Frame 1: 73 bytes on wire (73 bytes captured (584 bits))
- Ethernet II (Src: C4:2C:03:3C:98:A8, Dst: 00:0C:29:FS:A9:6B)

Last login on Monday, 2017-07-03 at 08:41:41 AM from 10.1.1.100

Figure 21-40 Drill-down into an Intrusion Event—Displaying Event Information

Figure 21-41 shows the packet information associated with an intrusion event. It allows you to compare the rule content with the packet payload on the same page without the need for any additional tool. This page also offers you an option to download any packet for offline analysis on third-party software.

Access Control Rule: Default Action

Rule: alert tcp \$TELNET_SERVERS 23 -> \$EXTERNAL_NET any (msg:"PROTOCOL-TELNET login incorrect"; flow:to_client,established; content:"Login incorrect"; metadata:ruleset community, service telnet; classtype:bad-unknown; sid:718; rev:16;)

Summary: This event is generated when an attempted telnet login fails from a remote user.

Packet Information

FRAME 1 (Expand All)

- Frame 1: 73 bytes on wire (73 bytes captured (584 bits))
- Ethernet II (Src: C4:2C:03:3C:98:A8, Dst: 00:0C:29:FS:A9:6B)
- Internet Protocol Version 4 (Src: 192.168.1.200, Dst: 107.15.160.100)
- Transmission Control Protocol (Src Port: 23 (23), Dst Port: 53875 (53875), Seq: 1, Ack: 1, Len: 19)
- Telnet
 - Data: Login incorrect
- Packet Text


```

      ..k.,<...E...@.....k.d...#
      ..h"p3P.r..3..
      Login incorrect
      
```
- Packet Bytes


```

      0000 00 0c 29 e5 a9 6b e4 2c 03 3c 98 a8 00 00 45 10 ..k.,<...E.
      0010 00 3b a8 fd 40 00 40 06 c3 cb c0 a8 01 c8 6b 0f ..h"p3P.r..#...k.
      0020 a0 64 00 17 d2 79 0d d8 b7 68 5e 70 33 50 18 .d...h"p3P.
      0030 72 10 ad 33 00 00 0d 0a 4c 6f 67 69 6e 20 69 6e r..3...Login in
      0040 63 6f 72 72 65 63 74 0d 0a                correct...
      
```

Displaying row 1 of 1 rows << Page 1 of 1 >>

Copy Delete Review Download Packet
Copy All Delete All Review All Download All Packets

Last login on Monday, 2017-07-03 at 08:41:41 AM from 10.1.1.100

Figure 21-41 Drill-down into an Intrusion Event—Displaying Packet Information

[Figure 21-42](#) shows the option in the Device Management page that enables an FTD device to capture a packet as it matches a Snort rule. You can disable this option if you do not want to store a complete packet due to any privacy or security policy.

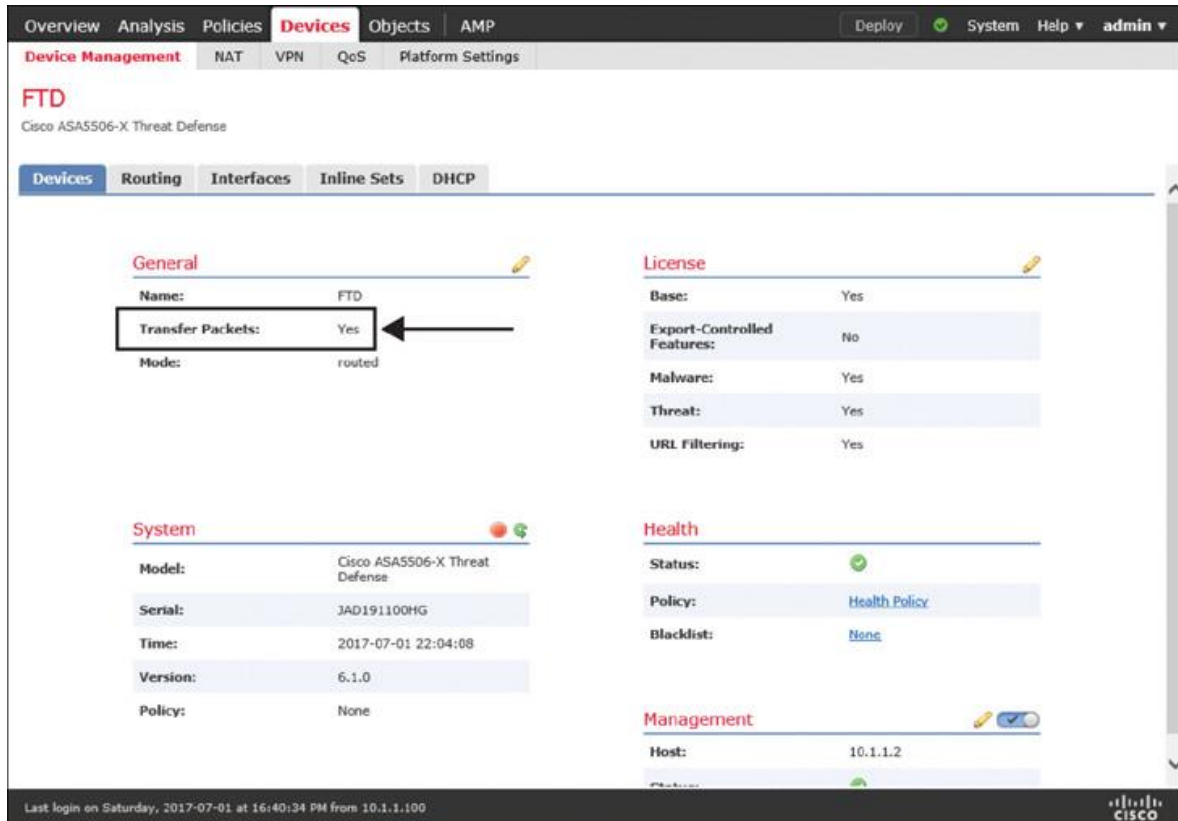


Figure 21-42 Capturing a Packet That Triggers an Intrusion Event

By analyzing the tracing data of a packet, you can determine whether a packet is blocked by Snort or any other component of the Firepower System. The process is described in detail in [Chapter 10, “Capturing Traffic for Advanced Analysis.”](#)

First, run the **capture** tool to begin capturing Telnet packets, making sure to add the **trace** keyword to collect the tracing data:

[Click here to view code image](#)

```
> capture telnet_inside trace interface INSIDE_INTERFACE match tcp any any eq 23  
>
```

You can run the **show capture** command any time to see the status of the capture or to view the captured packets:

[Click here to view code image](#)

```
> show capture  
capture telnet_inside type raw-data trace interface INSIDE_INTERFACE
```

```
[Capturing - 0 bytes]
match tcp any any eq telnet
>
```

Now, you can attempt to access the Telnet server once again. To reproduce an intrusion event, enter an incorrect credential. The **capture** tool captures all the packets on a Telnet session—including the first three-way handshake, which is completely allowed by the FTD device, per the current intrusion policy.

[Example 21-2](#) shows the first few packets of a Telnet session. Later, it analyzes the tracing data of the first packet. It reveals how an FTD device makes a decision and sends a packet to Snort for deep packet inspection.

Example 21-2 *Capturing Telnet Traffic with Tracing Information*

[Click here to view code image](#)

```
> show capture telnet_inside

119 packets captured

 1: 20:23:21.086802    107.15.160.100.53875 > 192.168.1.200.23: S
1751019501:1751019501(0) win 4128 <mss 1460>

 2: 20:23:21.087229    107.15.160.100.53875 > 192.168.1.200.23: S
1751019501:1751019501(0) win 4128 <mss 1460>

 3: 20:23:21.087565    192.168.1.200.23 > 107.15.160.100.53875: S
232306554:232306554(0) ack 1751019502 win 29200 <mss 1460>

 4: 20:23:21.087702    192.168.1.200.23 > 107.15.160.100.53875: S
232306554:232306554(0) ack 1751019502 win 29200 <mss 1460>

 5: 20:23:21.089717    107.15.160.100.53875 > 192.168.1.200.23: . ack 232306555
win 4128

 6: 20:23:21.089762    107.15.160.100.53875 > 192.168.1.200.23: P
1751019502:1751019514(12) ack 232306555 win 4128
.
.
<Output Omitted for Brevity>
```

! Now view the tracing data of the first captured packet.

```
> show capture telnet_inside packet-number 1 trace
```

119 packets captured

1: 20:23:21.086802 107.15.160.100.53875 > 192.168.1.200.23: S
1751019501:1751019501(0) win 4128 <mss 1460>

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:

The flow ingresses an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268435458
access-list CSM_FW_ACL_ remark rule-id 268435458: ACCESS POLICY: AC Policy -
Default/1
access-list CSM_FW_ACL_ remark rule-id 268435458: L4 RULE: DEFAULT ACTION
RULE
Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:

Ingress interface OUTSIDE_INTERFACE is in NGIPS inline mode.

Egress interface INSIDE_INTERFACE is determined by inline-set configuration

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 848, packet dispatched to next module

Phase: 7
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 8
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet

Phase: 9
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: allow

1 packet shown

>

[Example 21-3](#) shows the Snort verdict “drop this packet,” which appears in tracing output when a packet matches a Snort rule syntax and the rule state is set to drop and generate the event.

Example 21-3 *Snippet of the Tracing Information When a Packet Is Blocked by Snort*

[Click here to view code image](#)

<Output Omitted for Brevity>

.
.

Phase: 7

Type: EXTERNAL-INSPECT

Subtype:

Result: ALLOW

Config:

Additional Information:

Application: 'SNORT Inspect'

Phase: 8

Type: SNORT

Subtype:

Result: DROP

Config:

Additional Information:

Snort Verdict: (block-packet) drop this packet

.
.

<Output Omitted for Brevity>

[Example 21-4](#) shows the statistics of a Snort drop. According to this output, Snort requests to drop five frames after an incorrect credential was entered to authenticate a Telnet server.

Example 21-4 *Statistics of a Snort Drop*

[Click here to view code image](#)

> show asp drop

Frame drop:

Snort requested to drop the frame (snort-drop)	5
--	---

FP L2 rule drop (l2_acl)	1
--------------------------	---

Last clearing: 20:23:14 UTC Jul 3 2017 by enable_1

Flow drop:

Last clearing: 20:23:14 UTC Jul 3 2017 by enable_1

>

Summary

This chapter describes one of the most important and widely used features of a Firepower system: the Snort-based next-generation intrusion prevention system (NGIPS). In this chapter, you have learned how to configure an NGIPS, how to apply deploy associated policies, and how to drill down into intrusion events for advanced analysis. Most importantly, this chapter discusses the best practices for generating Firepower recommendations and demonstrates how the recommended ruleset can reduce system overhead by incorporating discovery data.

Quiz

1. Which of the following policy configurations can influence the behavior of the intrusion prevention functionality of an FTD?

- a. Network analysis policy
- b. Intrusion policy
- c. Access control policy
- d. All of the above

2. Which of the following numbering schemes is correct for a Snort rule?

- a. Standard text rule uses GID 1. SID is lower than 1,000,000.
- b. Preprocessor rule can use any GID other than 1 or 3.
- c. Local rule uses SID 1,000,000 or higher.
- d. All of the above.

3. Which of the following base policies enables the largest number of standard text Snort rules by default?

- a. Connectivity over Security
- b. Balanced Security and Connectivity
- c. Security over Connectivity
- d. Maximum Detection

4. Which of the following options is mandatory if you want to drop an intrusion attempt or block a packet that may constitute a potential cyber attack?

- a. The interface set has to be in Inline, Routed, or Transparent Mode.
- b. The intrusion policy must be enabled with the Drop When Inline option.
- c. The rule state must be set to Drop and Generate Events.
- d. All of the above.

Chapter 22

Masquerading the Original IP Address of an Internal Network Host

Any external user, whether an attacker or a legitimate Internet user, should have no visibility into your internal network. You can hide the internal addresses of your network by masquerading them into public addresses. However, assigning a dedicated public address to each of the internal hosts is not a feasible option. You can meet this challenge by enabling the Network Address Translation (NAT) functionality on an FTD device. This chapter demonstrates how to configure NAT and how NAT can masquerade an internal IP address as a public IP address.

Note

In this chapter, the terms *translation* and *masquerading* refer to the same operation and are interchangeable. In other words, *translation* of an address and *masquerading* of an address refer to the same technology: NAT.

NAT Essentials

NAT allows FTD to translate an internal IP address into an address from a different subnet. The NAT process is transparent to both internal and external hosts. When NAT is in action, an internal host is unaware that its original IP address is being translated or masqueraded to a public address, while the external host assumes that the public address is the actual address of the internal host.

[Figure 22-1](#) shows that the NAT operations of an FTD device take place on the Firewall engine.

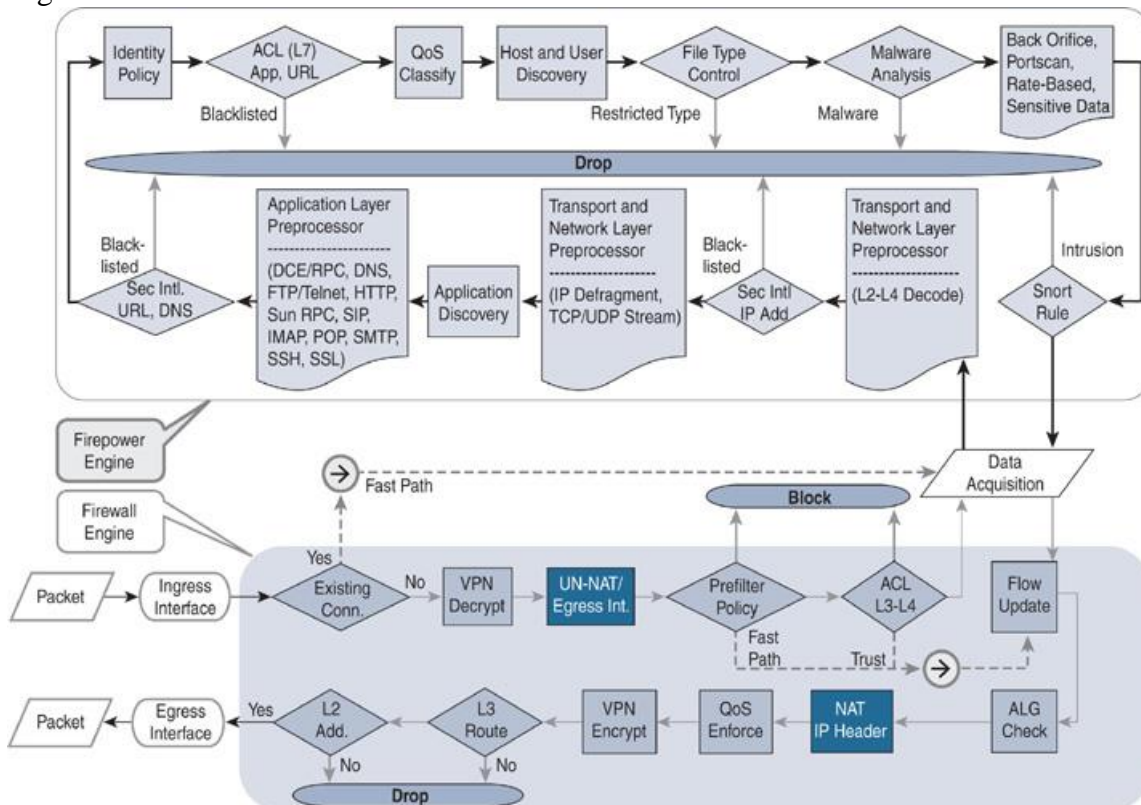


Figure 22-1 Architectural Overview of an FTD Device, Highlighting the NAT Components

Another advantage of NAT is the ability to route private traffic to the Internet. Internal hosts of an organization use private IP addresses, as defined in RFC 1918. However, these addresses are not routable to the Internet unless you map or translate them into public addresses. This “limitation” of private address space actually allows different organizations to reuse the same addresses within their internal networks and to maintain them regardless of any changes of their public IP address. Thus, it conserves the use of public IP addresses.

[Table 22-1](#) shows the range of private IP addresses and the number of available hosts in Classes A, B, and C.

Table 22-1 Private IP Addressing, as Defined in RFC 1918

Class	Range of Private IP Addresses	Number of Host
Class A	10.0.0.0–10.255.255.255	$2^{24} - 2 = 16,777,214$
Class B	172.16.0.0–172.31.255.255	$2^{20} - 2 = 1,048,574$
Class C	192.168.0.0–192.168.255.255	$2^{16} - 2 = 65,534$

NAT Techniques

NAT allows you to masquerade IP addresses in various scenarios, such as one-to-one, one-to-many, many-to-one, many-to-many, few-to-many, and many-to-few. However, before you enable NAT, you need to answer the following questions:

- How does an FTD device select a masqueraded or translated address? Is it predefined statically or allocated dynamically?
- How many external or public addresses are available for selection? One or more?

Your answers to these questions can help you determine the type of translations to enable. You can categorize NAT mainly into three types:

■ **Static NAT:** FTD permanently maps the original IP address with a translated IP address. Because the mapping is permanent, either the internal or an external host is able to initiate a connection.

■ **Dynamic NAT:** Instead of a permanent mapping, FTD selects an IP address from a predefined address pool and translates an original internal address into the selected IP address. The selection of an address is on a first-come, first-served basis.

■ **Port Address Translation (PAT):** If a dynamic address pool has fewer external addresses than there are internal hosts, it is impossible for all the internal hosts to connect to external networks at the same time. To address this issue, FTD can translate both the IP address and port number of a connection (as opposed to just the IP address) and can multiplex over 65,000 connections over a single IP address.

RFC documents describe this feature as Network Address and Port Translation (NAPT), but due to the nature of its operation, this feature is also known as *Port Address Translation (PAT)*, *NAT overload*, and *IP masquerading*. The Firepower System calls it PAT.

Figure 22-2 shows the major differences between NAT and PAT.

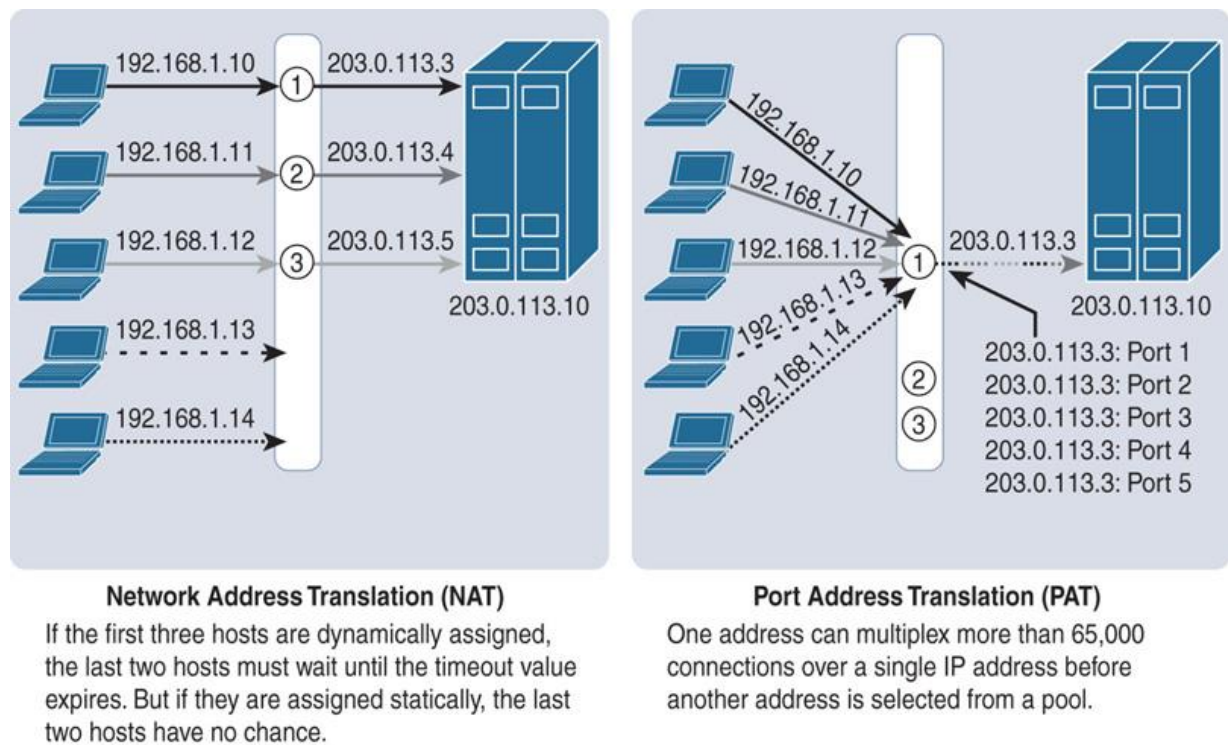


Figure 22-2 NAT Versus PAT

FTD can use the IP address of the egress interface for PAT operation. This means that when any internal host connects to a resource over the Internet, the source IP address of the connection appears as the egress interface of the FTD device instead of as the original internal host address. However, if the number of concurrent connections exceeds its limit, any additional hosts are unable to connect to the external network. To address this issue, you can combine the PAT functionality with a dynamic address pool. This allows an FTD device to select a new IP address from the pool when the first selection from the pool is no longer available for multiplexing a new connection.

NAT Rule Types

FTD offers two options to configure a NAT rule condition:

■ **Auto NAT:** An Auto NAT rule can translate one address—either a source or destination address—in a single rule. This means that to translate both source and destination addresses, two separate Auto NAT rules are necessary.

■ **Manual NAT:** A Manual NAT rule allows the translation of both source and destination addresses within the same rule. A Manual NAT rule may be necessary when you want to make an exception for translation.

[Figure 22-3](#) compares the available translation options in the NAT rule editor. An Auto NAT Rule supports the translation of one address per rule, while a Manual NAT Rule allows you to translate both source and destination addresses in a single rule.

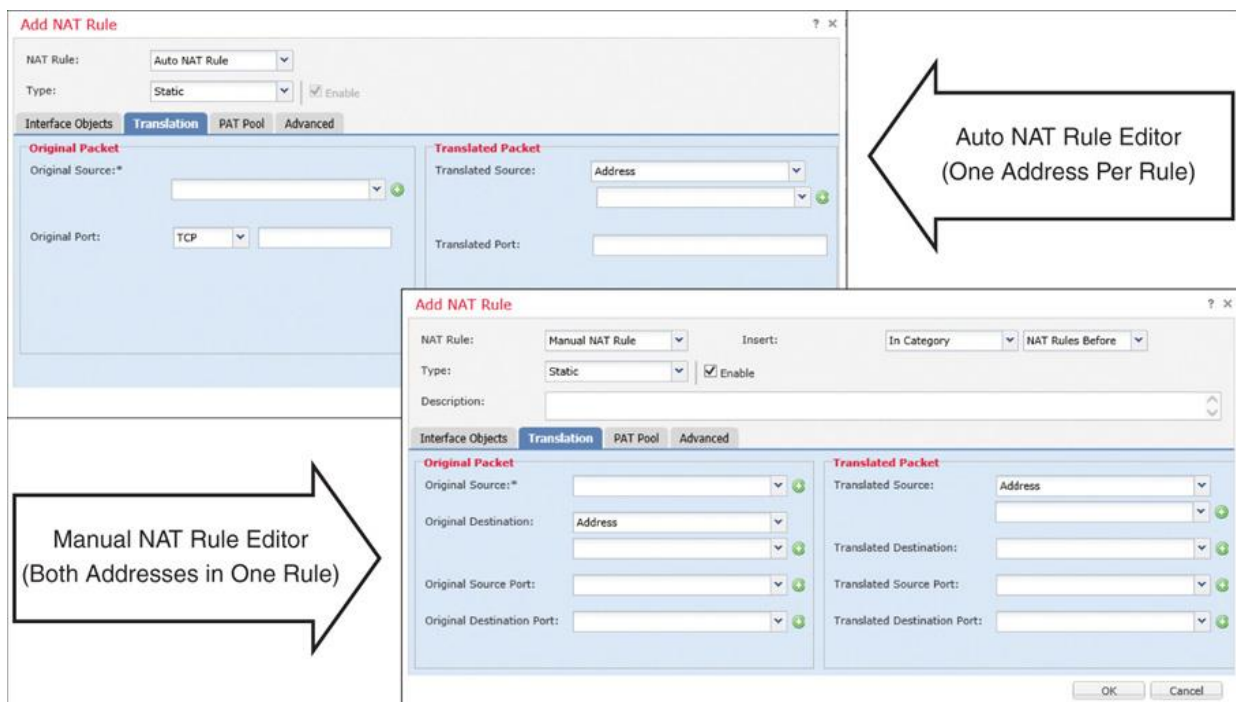


Figure 22-3 *Auto NAT Versus Manual NAT: Comparison of Rule Editor Windows*

A NAT policy editor categorizes NAT rules into three groups: NAT Rules Before, Auto NAT Rules, and NAT Rules After. In the CLI, you can find the rules under Section 1, Section 2, and Section 3, respectively. During evaluation, FTD begins with the rules under Section 1. Until there is a match, FTD continues evaluating the rules in the next sections.

Any rules under the NAT Rules Before and NAT Rules After sections are part of manual NAT policies. Their names and priorities are relative to the Auto NAT Rules, which allow you to translate one type of address at a time. To translate destination addresses, a separate Auto NAT rule is necessary.

Figure 22-4 describes the priority of each section in a NAT policy.

The screenshot shows the Cisco FTD GUI for configuring a NAT policy. The 'Rules' section is expanded to show three categories: 'NAT Rules Before', 'Auto NAT Rules', and 'NAT Rules After'. A diagram on the right explains the priority order: 1. NAT Rules Before (Manual NAT policies, top priority), 2. Auto NAT Rules (Static type has higher priority than Dynamic type, longer prefix length has higher priority within type), and 3. NAT Rules After (Manual NAT policies, lower priority than Auto NAT). A box at the top right says 'To View This NAT Policy on the CLI: > show nat detail'.

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destination	Translated Services	Options
▼ NAT Rules Before											
▼ Auto NAT Rules											
▼ NAT Rules After											

Top to Bottom Priority

GUI: NAT Rules Before CLI: Section 1	Manual NAT policies. Top priority, when available.
GUI: Auto NAT Rules CLI: Section 2	Static type has higher priority than Dynamic type. Longer prefix length has higher priority within type.
GUI: NAT Rules After CLI: Section 3	Manual NAT policies. Lower priority than Auto NAT.

Figure 22-4 Priorities of Rules on a NAT Policy

In this chapter, you will learn how to configure Auto NAT rules with both static and dynamic types.

Best Practices for NAT Deployment

Consider the following best practices when you plan to enable NAT on an FTD device:

- Configuring an Auto NAT rule is simpler than configuring a Manual NAT rule. Cisco recommends that you choose an Auto NAT rule, as you can easily implement most of the common NAT scenarios with it. A Manual NAT rule may be necessary when you want to make an exception for translation.
- If you modify an existing NAT rule or redeploy a new NAT policy, you may find that the new policy is not in action until the timer for any existing connections expires. To have FTD act on the latest NAT policy immediately, you can clear the current translations by running the command **clear xlate**.
- The larger the translation table, the higher the processing overhead. If the number of translated connections grows excessively, it can affect the CPU and memory utilization of an FTD device.

- To improve performance, prefer static NAT to dynamic NAT or PAT.
- Review the addresses on dynamic and static NAT rules carefully before you apply them. Avoid creating rules with overlapping IP addresses.
- Ensure that any applications running on a network terminate connections gracefully to prevent an FTD device from handling stale connections.
- Make sure the idle timeout values for Translation Slot (xlate) and Connection (Conn) are set for optimal performance. You can adjust the timeout values on the Platform Settings page of FTD.

Figure 22-5 shows the timeout values for an FTD. To find this configuration page, go to **Devices > Platform Settings**. You can update an existing policy or create a new one.

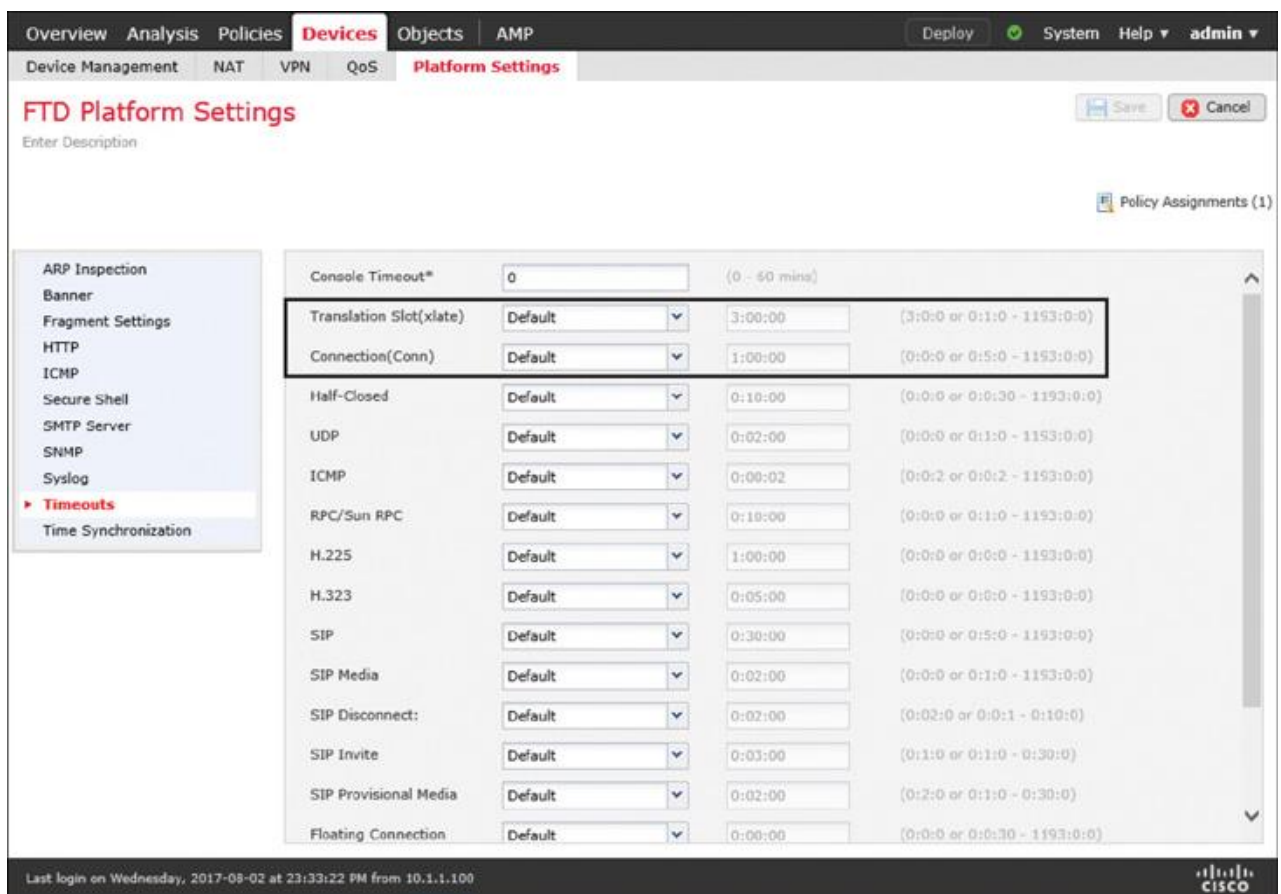


Figure 22-5 Configuring FTD Timeout Values on the Platform Settings Page

Fulfilling Prerequisites

Before you add a NAT rule, ensure that you have understood and fulfilled the following items:

■ Any associated interfaces that participate in a NAT configuration have to be in a regular firewall mode. FTD does not support NAT on IPS-only interface types, such as inline, inline-tap, and passive. [Figure 22-6](#) shows the available configuration modes for an FTD physical interface. Select **None** to enable the regular router interface mode, which supports NAT.

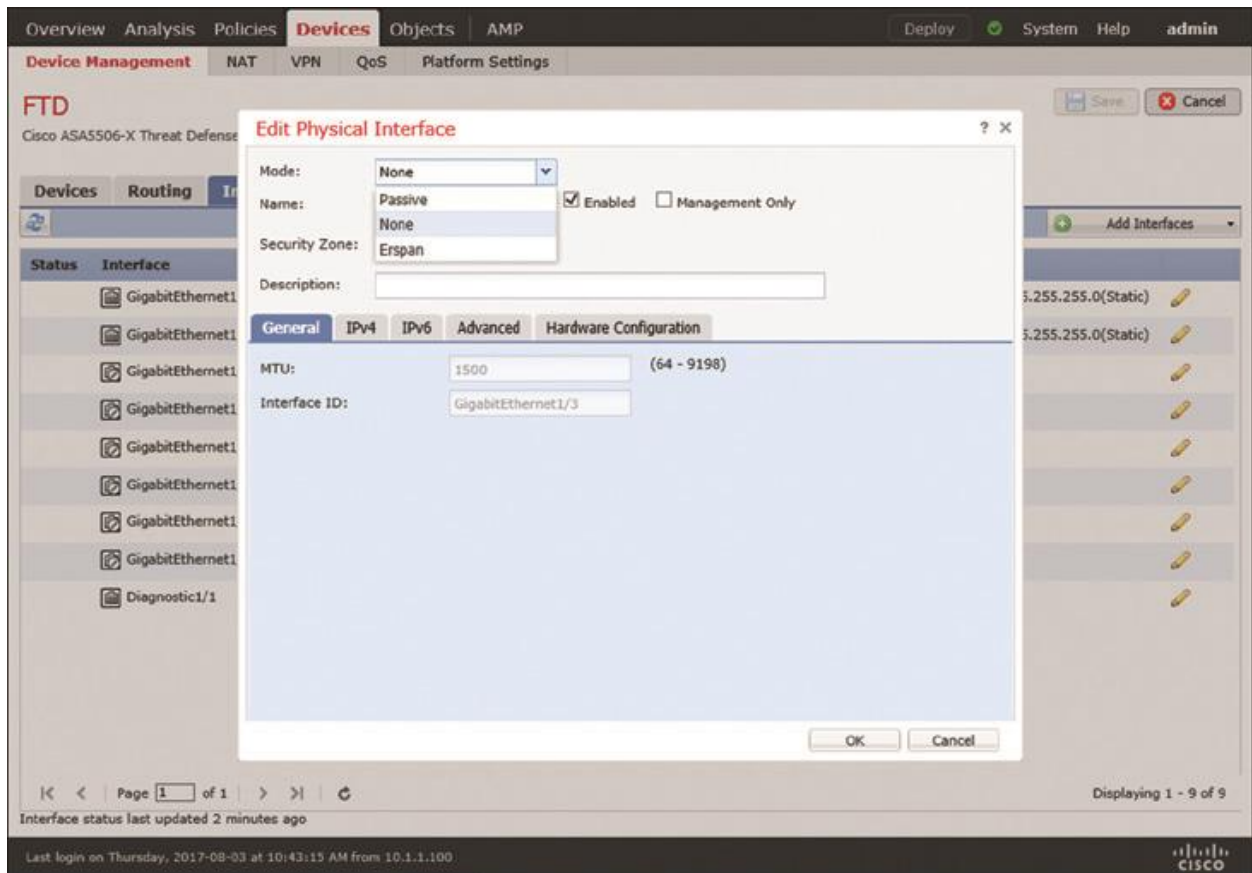


Figure 22-6 Using the None Option to Turn an Interface into a Regular Firewall Interface

■ If you use an FTD device in an IPS-only mode, make sure all the associated interfaces where you want to enable NAT are now configured with IP address and security zones.

[Figure 22-7](#) shows the allocation of IP addresses and security zones in FTD. The lab topology in this chapter uses three routed interfaces on FTD—GigabitEthernet1/1, GigabitEthernet1/2, and GigabitEthernet1/3.

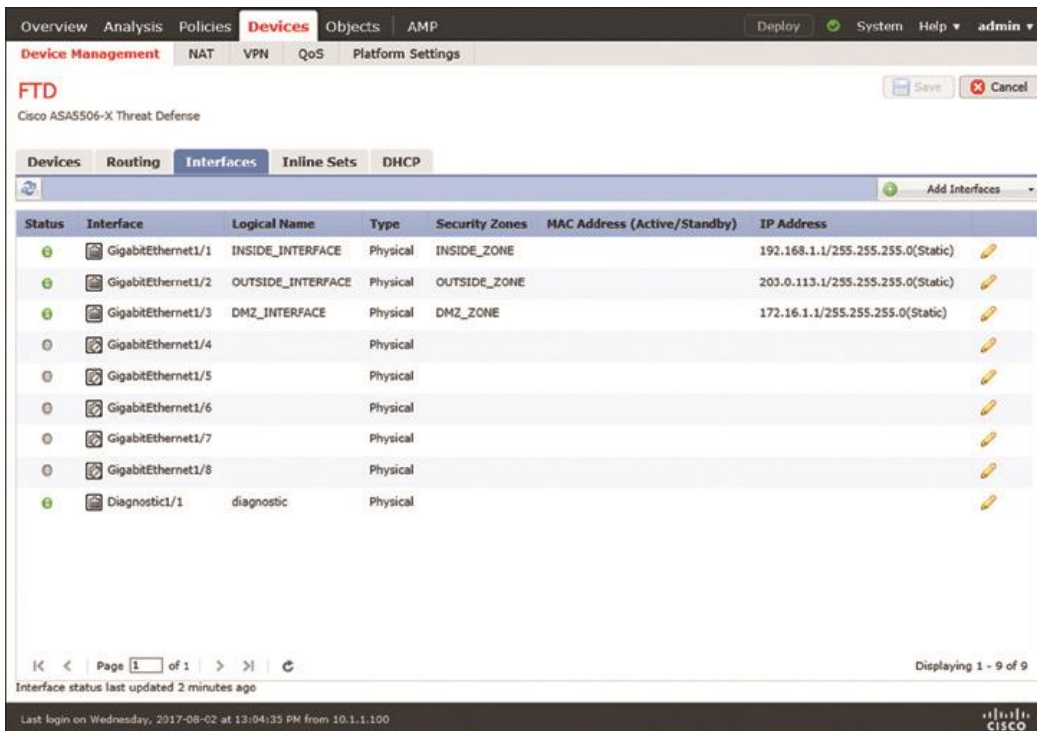


Figure 22-7 Allocating IP Addresses and Security Zones on FTD Routed Interfaces

Before you begin the process of adding a NAT rule, define any network objects that may be invoked within a NAT rule. To add a network object, go to the **Objects > Object Management** page and select the **Add Network** menu.

Figure 22-8 shows the network objects that are used in the configuration examples in this chapter. You can add any additional objects needed for your own deployment.

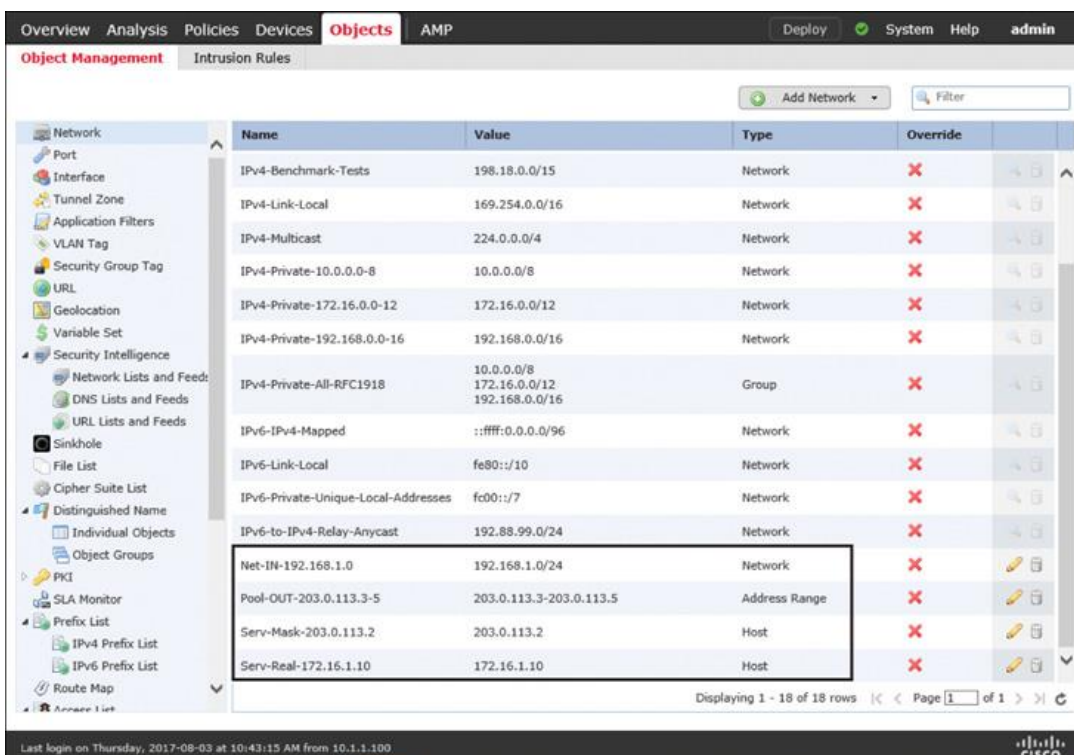


Figure 22-8 Network Object Configuration Page

Configuring NAT

FTD enables you to accomplish translation in various ways. You can select any type (static versus dynamic) with any combination of NAT rule (Auto versus Manual). However, Cisco recommends that you use Auto NAT rule, as it is easier to configure and simpler to troubleshoot. In the following sections, you will learn how to configure Auto NAT to masquerade IP addresses in the following real-world deployment scenarios:

- *Masquerading a source address* when an internal host initiates a connection to an external server

- Allowing an external host to connect to an internal host when an external host uses a *masqueraded destination address*

Masquerading a Source Address (Source NAT for Outbound Connection)

When an internal host initiates a connection to the Internet, FTD can translate the internal IP address to a public IP address. In other words, FTD can masquerade the source addresses of outbound connections. This section describes various methods to select a public IP address for an outbound connection.

Note

This section assumes that you have already configured any necessary objects described earlier in this chapter, in the “Fulfilling Prerequisites” section.

[Figure 22-9](#) shows a scenario where an internal host connects to an external host through an FTD device. When an end user initiates a connection using the original source IP address, FTD translates (masquerades) the original source IP address into an address that is predefined in an address pool.

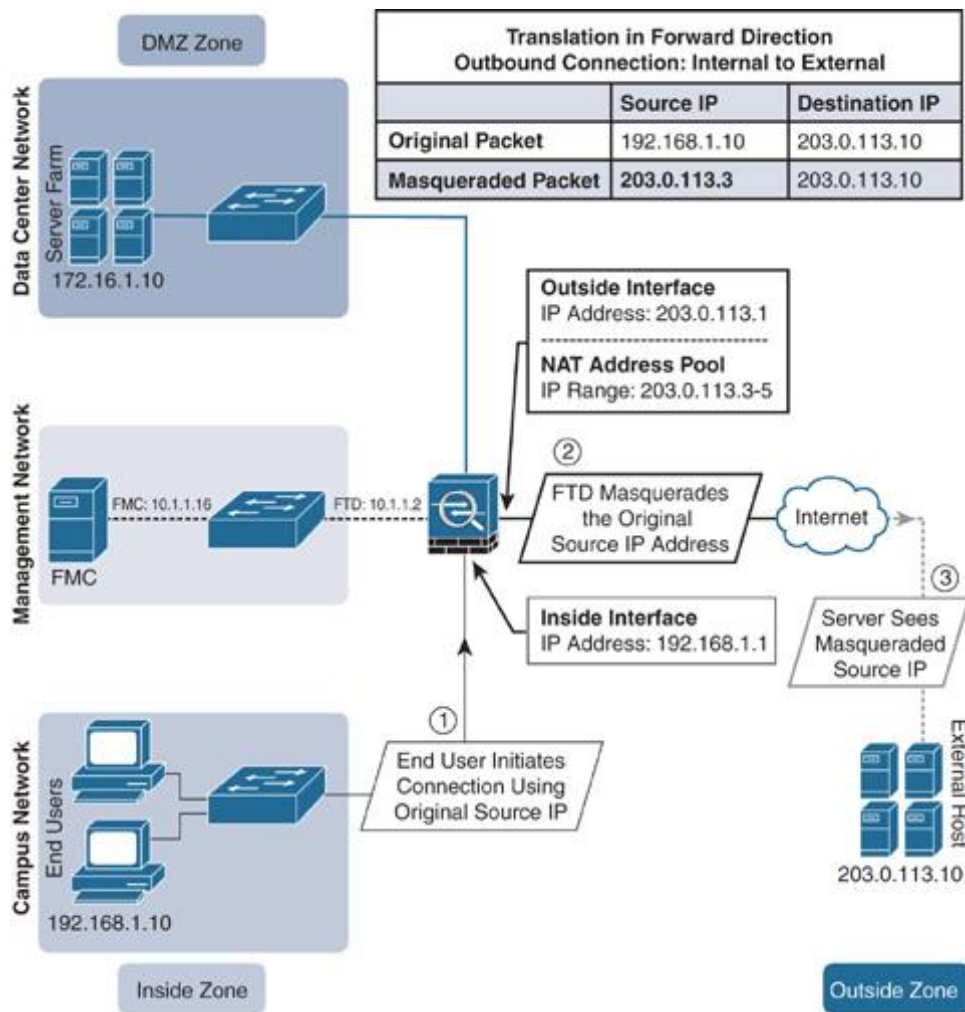


Figure 22-9 Lab Topology Demonstrating Dynamic NAT for Outbound Traffic

Configuring a Dynamic NAT Rule

The FMC offers two types of NAT policies—Firepower NAT Policy and Threat Defense NAT Policy. The former is used to enable NAT on classic Firepower hardware, such as 7000 and 8000 Series models. To enable NAT on FTD, you need to deploy Threat Defense NAT Policy on it. To do so, follow these steps:

Step 1. Navigate to **Devices > NAT**. The NAT Policy window appears.

Step 2. To create a new NAT policy for an FTD device, select **Threat Defense NAT Policy** (see [Figure 22-10](#)).

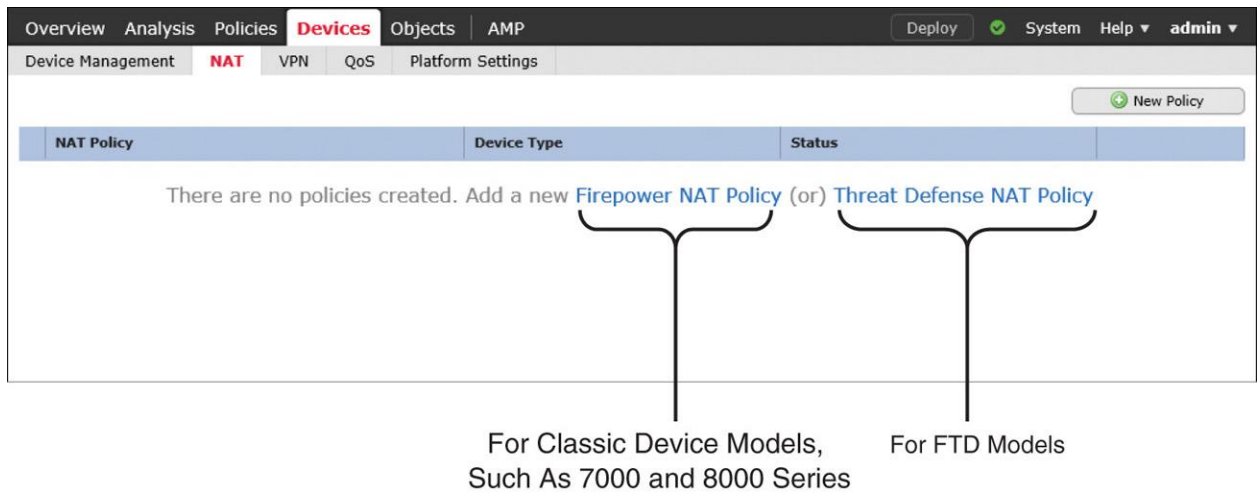


Figure 22-10 NAT Policy Configuration Options for Different Hardware Models

Step 3. When the New Policy window appears, give a name to your policy and add your FTD device from the list of available devices to the policy (see [Figure 22-11](#)). Click the **Save** button. The NAT policy editor page appears.

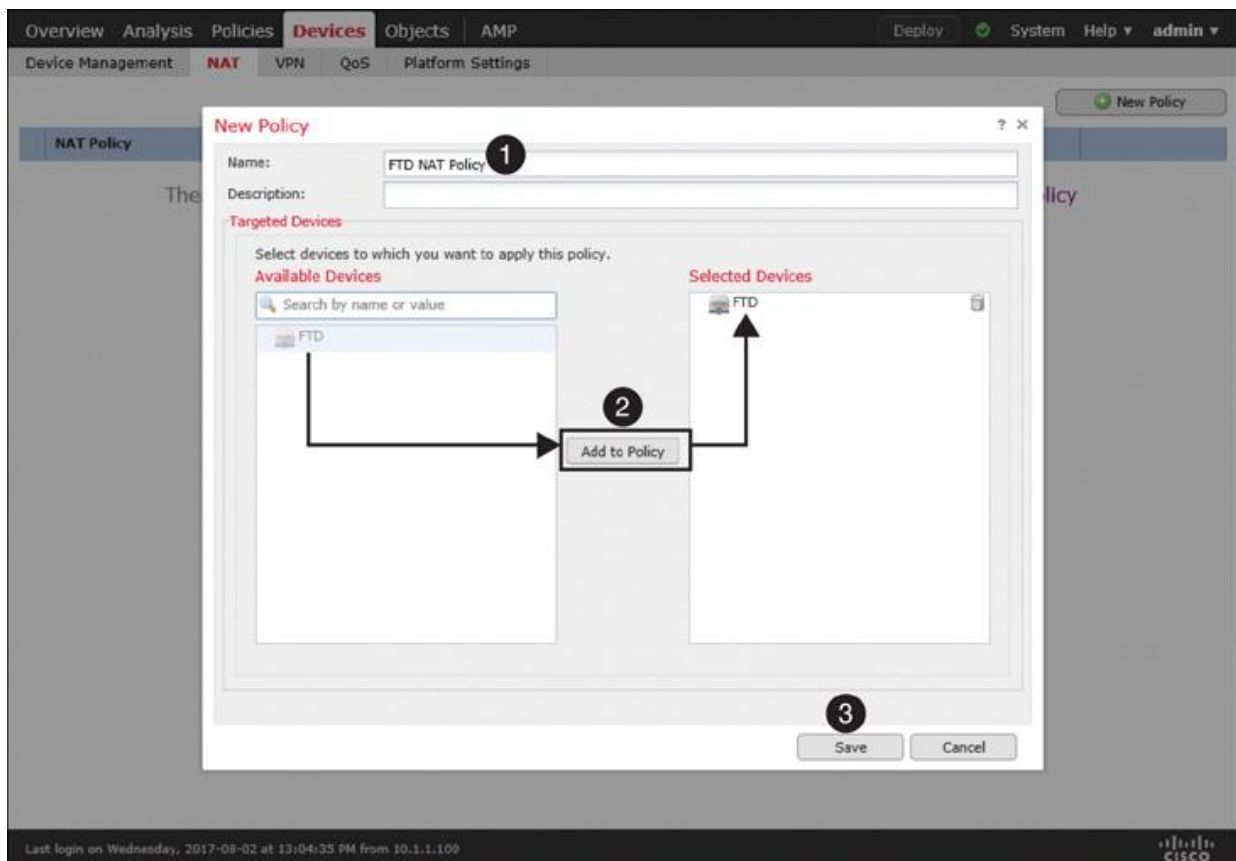


Figure 22-11 Assigning a NAT Policy to an FTD Device

Step 4. On the policy editor page, click the **Add Rule** button to create a NAT rule. The Add NAT Rule window appears.

Step 5. From the NAT Rule dropdown select **Auto NAT Rule**, and from the Type dropdown select **Dynamic**. Depending on your selections in both of these dropdowns, you will find different configurable options in the Translation tab. For instance, for an Auto NAT Rule with Dynamic type, you need to configure the Original Source and Translated Source.

Step 6. Use the Original Source dropdown to define the source IP addresses of the packets that you want to masquerade. You can select a network object that you defined in the section “Fulfilling Prerequisites,” earlier in this chapter. If you did not create an object earlier, you can create one on the fly by clicking the green plus icon next to a dropdown.

Step 7. Define a translated address—the address that appears as the source address of a translated packet. You need to select one of the following translation methods on the Translation or PAT Pool tab, depending on the type of NAT (static or dynamic) you want to configure.

■ **Destination Interface IP:** This allows an FTD device to use the same IP address as the egress interface of an FTD.

■ **Address:** This enables an FTD device to select an address from a predefined address pool.

[Table 22-2](#) shows a matrix of various Auto NAT rule selections. In this section, you will implement dynamic NAT with an address pool (highlighted row).

Table 22-2 *Auto NAT Rule—Major Configurable Options*

Type	Translation Tab (Translated Source)	Translation Tab (Port Translation)	PAT Pool Tab
Static	Destination Interface IP	Configurable	Not Configurable
Static	Address	Configurable	Not Configurable
Dynamic	Destination Interface IP	Not Configurable	Not Configurable
Dynamic	Address	Not Configurable	Unselected
Dynamic	Address	Not Configurable	Enabled with Address
Dynamic	Address	Not Configurable	Enabled with Destination Interface IP

[Figure 22-12](#) shows the configuration of original and translated addresses in a dynamic Auto NAT rule.

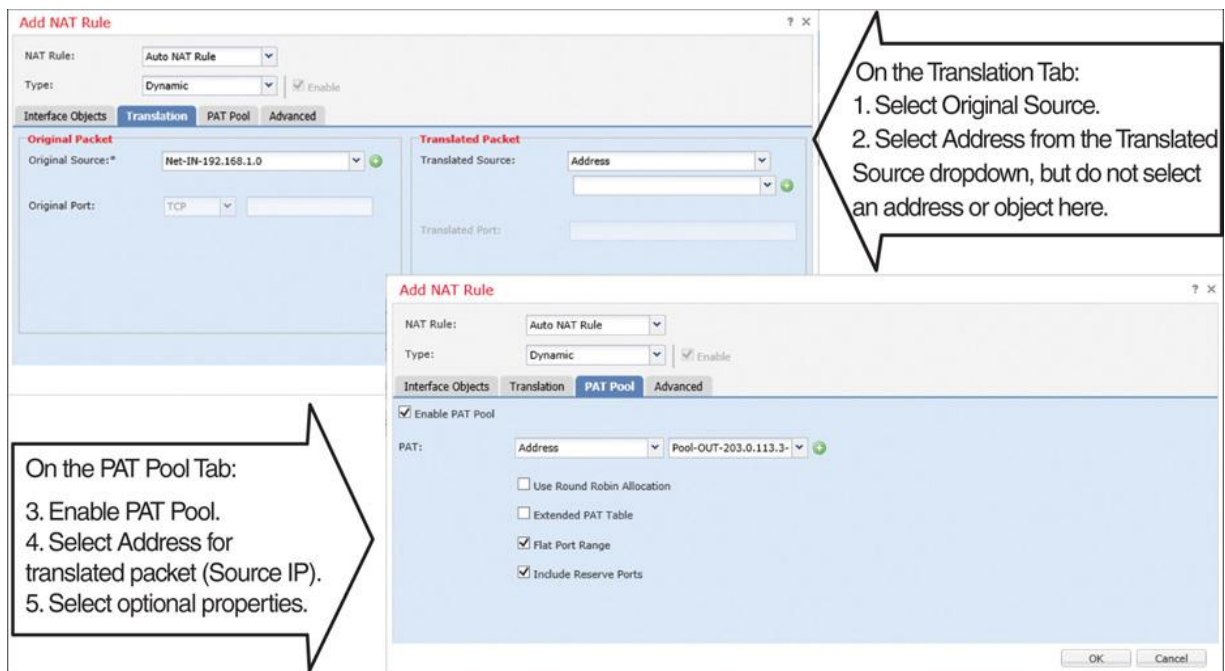


Figure 22-12 Defining a Dynamic Auto NAT Rule

At this point, you could save the configuration and deploy the policy on the FTD device. However, you may want to consider the following optional configurations.

Step 8. On the PAT Pool tab, select **Flat Port Range** and **Include Reserve Ports** to enable an FTD device to use the complete range of port numbers, 1 to 65535, even though the same source port number is unavailable for mapping.

Step 9. On the Interface Objects tab, select the ingress and egress interfaces for the traffic you want to translate. The Available Interface Objects field shows the associated security zones that you assigned in the Devices > Devices Management page.

When you complete all the steps, click the **OK** button on the NAT rule editor window to create the NAT rule. The browser returns to the NAT policy editor, where you can see the NAT rule you have just created. To activate the policy, first click **Save** to save the policy, and then click **Deploy** to deploy it on your FTD device.

[Figure 22-13](#) shows a dynamic Auto NAT rule that translates the source IP addresses of any hosts from the INSIDE_ZONE to the OUTSIDE_ZONE. The translated packet uses an address from the address pool, Pool-OUT-203.0.113.3-5, as its source IP address.

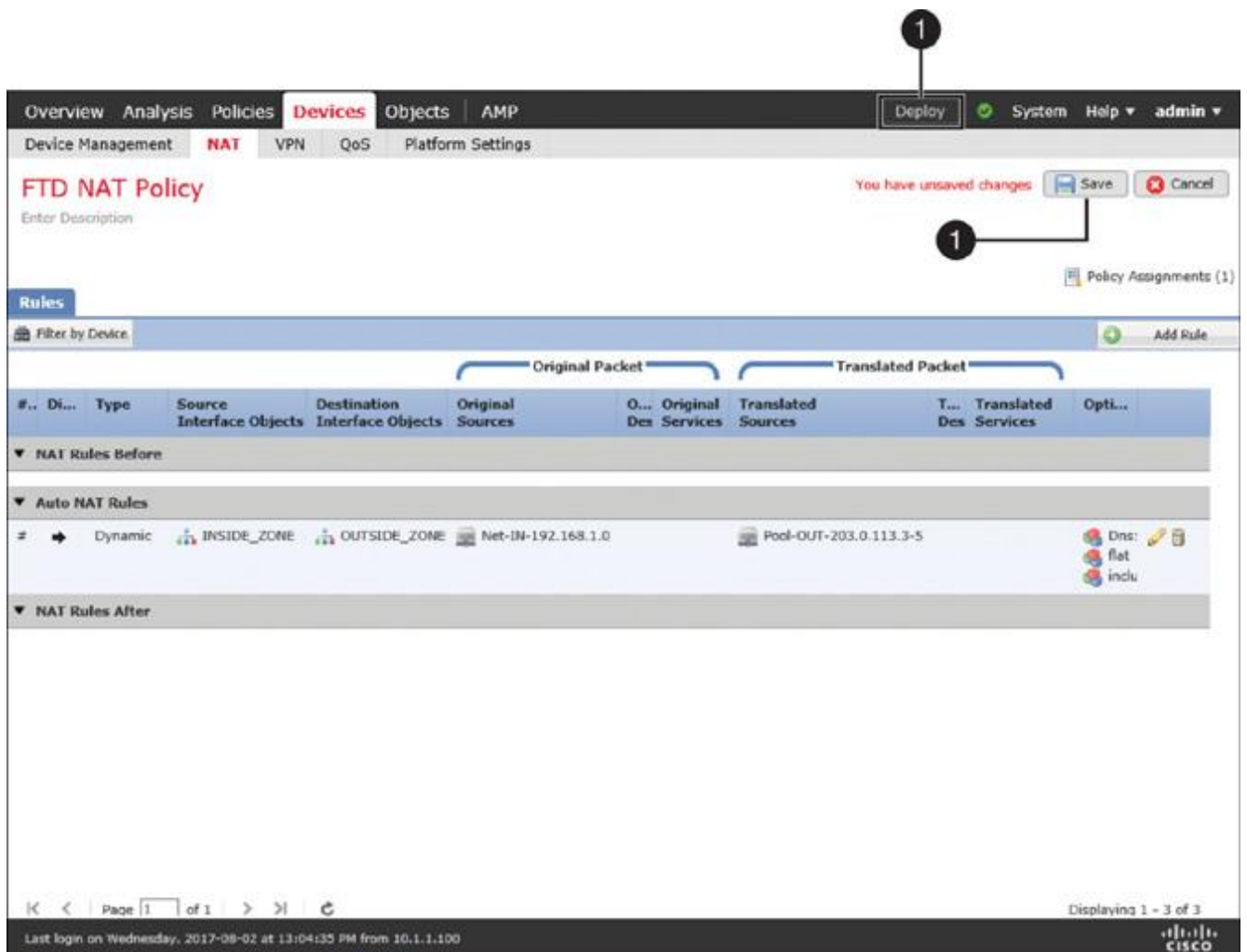


Figure 22-13 *Defining a Dynamic NAT Rule to Translate Outbound Connections*

In the following sections, you will learn how to verify the configuration on the CLI and how to determine whether an FTD device is translating addresses as expected.

Verifying the Configuration

After you deploy a NAT policy, you can run the **show running-config nat** command in the CLI to view the latest NAT configurations and to confirm whether the desired policy is active.

[Example 22-1](#) exhibits the running configurations of NAT and the definitions of any associated objects that are invoked in a NAT rule.

Example 22-1 Defining a NAT Rule and Any Associated Objects

[Click here to view code image](#)

! To view the NAT configurations:

```
> show running-config nat
!  
object network Net-IN-192.168.1.0  
  
  nat (INSIDE_INTERFACE,OUTSIDE_INTERFACE) dynamic pat-pool Pool-OUT-  
  203.0.113.3-5  
  
  flat include-reserve  
  
>
```

! To determine the scope of an object:

```
> show running-config object  
  
object network Net-IN-192.168.1.0  
  
  subnet 192.168.1.0 255.255.255.0  
  
object network Pool-OUT-203.0.113.3-5  
  
  range 203.0.113.3 203.0.113.5  
  
>
```

You can also run the **show nat detail** command to display more detailed information about a NAT policy, such as the priority of a rule (Auto NAT versus Manual NAT) or the type of a rule (static versus dynamic). The output of this command also displays the number of matching connections in both forward and reverse directions, through the `translate_hits` and `untranslate_hits` counters, respectively.

[Example 22-2](#) shows an Auto NAT rule (dynamic PAT) for translating traffic from the 192.168.1.0/24 network to the address pool 203.0.113.3 to 203.0.113.5. The zero hit count indicates that the rule has not matched any connections.

Example 22-2 Output of the **show nat detail** Command

[Click here to view code image](#)

> **show nat detail**

Auto NAT Policies (Section 2)

1 (INSIDE_INTERFACE) to (OUTSIDE_INTERFACE) source dynami Net-IN-92.168.1.0

pat-pool Pool-OUT-203.0.113.3-5 flat include-reserve

translate_hits = 0, untranslate_hits = 0

Source - Origin: 192.168.1.0/24, Translated (PAT): 203.0.113.3-203.0.113.5

>

Examples 22-1 and 22-2 display the source (INSIDE_INTERFACE) and destination (OUTSIDE_INTERFACE) defined in a NAT rule. However, the output in these examples does not show the status, IP address, or name of an interface. You can find them by running other commands, such as **show nameif** and **show interfaces ip brief**.

[Example 22-3](#) shows how to map the physical interfaces with their logical names. It also shows how to verify the IP address and status of an interface.

Example 22-3 Viewing Various Parameters of FTD Interfaces

[Click here to view code image](#)

! To view the mapping of physical interfaces with their logical names:

> **show nameif**

Interface	Name	Security
GigabitEthernet1/1	INSIDE_INTERFACE	0
GigabitEthernet1/2	OUTSIDE_INTERFACE	0
GigabitEthernet1/3	DMZ_INTERFACE	0
Management1/1	diagnostic	0

>

! To view the status and IP addresses of the FTD interfaces:

> **show interface ip brief**

Interface	IP-Address	OK?	Method Status	Protocol
Virtual0	127.1.0.1	YES	unset up	up
GigabitEthernet1/1	192.168.1.1	YES	CONFIG up	up
GigabitEthernet1/2	203.0.113.1	YES	CONFIG up	up
GigabitEthernet1/3	172.16.1.1	YES	CONFIG up	up
GigabitEthernet1/4	unassigned	YES	unset administratively down	down

```
GigabitEthernet1/5    unassigned    YES unset    administratively down down
```

```
.
```

```
<Output omitted for brevity>
```

[Verifying the Operation: Inside to Outside](#)

This section describes how to verify the NAT operation on an FTD device. To demonstrate the translation process, this example uses SSH traffic.

Let's initiate a connection from an internal host 192.168.1.10 to an external SSH server 203.0.113.10. If NAT is operational on FTD, the external SSH server sees 203.0.113.3 as the source IP address of the internal host instead of its original source IP address, 192.168.1.10.

[Example 22-4](#) shows an SSH connection between the internal client and the external server. The connection table shows the original IP address (192.168.1.10) of the internal server with a translation (**xlate**) ID. However, you can determine the masqueraded or translated address (203.0.113.3) from the translation table.

Example 22-4 *Connection and Translation Table*

[Click here to view code image](#)

```
> show conn detail
```

```
1 in use, 4 most used
```

```
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,
```

```
    b - TCP state-bypass or nailed,
```

```
    C - CTIQBE media, c - cluster centralized,
```

```
    D - DNS, d - dump, E - outside back connection, e - semi-distributed,
```

```
    F - initiator FIN, f - responder FIN,
```

```
    G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
```

```
    i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
```

```
    k - Skinny media, M - SMTP data, m - SIP media, N - inspected by Snort,
```

```
    n - GUP
```

```
    O - responder data, P - inside back connection,
```

```
    q - SQL*Net data, R - initiator acknowledged FIN,
```

```
    R - UDP SUNRPC, r - responder acknowledged FIN,
```

```
    T - SIP, t - SIP transient, U - up,
```

```
    V - VPN orphan, v - M3UA W - WAAS,
```

```
    w - secondary domain backup,
```

```
    X - inspected by service module,
```

```
    x - per session, Y - director stub flow, y - backup stub flow,
```

```
    Z - Scansafe redirection, z - forwarding stub flow
```

```
TCP OUTSIDE_INTERFACE: 203.0.113.10/22 INSIDE_INTERFACE:
```

```
192.168.1.10/41934,
```

```
    flags UxIO N, idle 6s, uptime 18s, timeout 1h0m, bytes 6718, xlate id
```

```
0x7f516987ee00
```

```
>
```



```
> show xlate detail
```

```
1 in use, 2 most used
```

```
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,  
s - static, T - twice, N - net-to-net
```

```
TCP PAT from INSIDE_INTERFACE:192.168.1.10/41934 to OUTSIDE_INTER-  
FACE:203.0.113.3/41934 flags ri idle 0:00:28 timeout 0:00:30 refcnt 1 xlate id  
0x7f516987ee00
```

```
>
```

By looking at the output of the **show nat detail** command, you can determine whether the traffic matches a particular NAT rule and how many times a rule finds a match.

[Example 22-5](#) confirms that the Auto NAT rule found one matching connection when a host sent traffic from INSIDE_INTERFACE to OUTSIDE_INTERFACE.

Example 22-5 *Matching One Connection in the Forward Direction*

[Click here to view code image](#)

```
> show nat detail
```

```
Auto NAT Policies (Section 2)
```

```
1 (INSIDE_INTERFACE) to (OUTSIDE_INTERFACE) source dynamic Net-IN-  
192.168.1.0 pat-pool Pool-OUT-203.0.113.3-5 flat include-reserve
```

```
translate_hits = 1, untranslate_hits = 0
```

```
Source - Origin: 192.168.1.0/24, Translated (PAT): 203.0.113.3-203.0.113.5
```

```
>
```

By capturing the traffic in real time when an address is translated, you can analyze the FTD operation during address translation.

[Example 22-6](#) demonstrates the capture of any SSH traffic on the inside interface. Later, you will analyze the translation of these packets.

Example 22-6 *Capturing SSH Traffic on the FTD Inside Interface*

[Click here to view code image](#)

```
! Begin the capture of SSH traffic on inside interface.
```

```
> capture ssh_traffic_inside trace interface INSIDE_INTERFACE match tcp any any  
eq 22
```

! Verify if the FTD is running a capture for SSH traffic.

> **show capture**

```
capture ssh_traffic_inside type raw-data trace interface INSIDE_INTERFACE
```

```
[Capturing - 0 bytes]
```

```
match tcp any any eq ssh
```

>

At this stage, you can initiate an SSH connection from the internal host to the external SSH server. FTD should capture the traffic on the inside interface. You can view the packets in the CLI.

[Example 22-7](#) shows the first few captured packets for an SSH connection. Later, it analyzes the first packet to demonstrate the detailed operation of an address translation.

Example 22-7 *Analyzing Captured Packets*

[Click here to view code image](#)

! To view all of the captured packets (press Ctrl+C to exit from a long show):

> **show capture ssh_traffic_inside**

```
81 packets captured
```

```
1: 02:59:47.220310    192.168.1.10.41934 > 203.0.113.10.22: S
```

```
1482617093:1482617093(0) win 29200 <mss 1460,sackOK,timestamp 15243390
```

```
0,nop,wscale 7>
```

```
2: 02:59:47.221149    203.0.113.10.22 > 192.168.1.10.41934: S
```

```
1409789153:1409789153(0) ack 1482617094 win 28960 <mss 1380,sackOK,timestamp
```

```
17762742 15243390,nop,wscale 7>
```

```
3: 02:59:47.221256    192.168.1.10.41934 > 203.0.113.10.22: . ack 1409789154
```

```
win 229 <nop,nop,timestamp 15243390 17762742>
```

```
4: 02:59:47.221729    192.168.1.10.41934 > 203.0.113.10.22: P
```

```
1482617094:1482617135(41) ack 1409789154 win 229 <nop,nop,timestamp 15243391
```

17762742>

5: 02:59:47.222186 203.0.113.10.22 > 192.168.1.10.41934: . ack 1482617135

win 227 <nop,nop,timestamp 17762742 15243391>

.
.

<Output is omitted for brevity>

! To analyze the first captured packet:

> show capture ssh_traffic_inside packet-number 1 trace

81 packets captured

1: 02:59:47.220310 192.168.1.10.41934 > 203.0.113.10.22: S

1482617093:1482617093(0) win 29200 <mss 1460,sackOK,timestamp 15243390

0,nop,wscale 7>

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

MAC Access list

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 3

Type: ROUTE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

found next-hop 203.0.113.10 using egress ifc OUTSIDE_INTERFACE

Phase: 4

Type: ACCESS-LIST

Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_global
access-list CSM_FW_ACL_advanced permit ip any any rule-id 268435457
access-list CSM_FW_ACL_remark rule-id 268435457: ACCESS POLICY: AC Policy -
Mandatory/1
access-list CSM_FW_ACL_remark rule-id 268435457: L7 RULE: Traffic Selection
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be
reached

Phase: 5
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Config:
class-map class-default
match any
policy-map global_policy
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
service-policy global_policy global
Additional Information:

Phase: 6
Type: NAT
Subtype:
Result: ALLOW
Config:
object network Net-IN-192.168.1.0
nat (INSIDE_INTERFACE,OUTSIDE_INTERFACE) dynamic pat-pool Pool-OUT-
203.0.113.3-5
flat include-reserve
Additional Information:
Dynamic translate 192.168.1.10/41934 to 203.0.113.3/41934

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 10
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 442, packet dispatched to next module

Phase: 12
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 13
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet

Phase: 14
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 203.0.113.10 using egress ifc OUTSIDE_INTERFACE

Phase: 15
Type: ADJACENCY-LOOKUP
Subtype: next-hop and adjacency

Result: ALLOW
Config:
Additional Information:
adjacency Active
next-hop mac address 0023.2472.1d3c hits 139985869104448

Phase: 16
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Result:
input-interface: OUTSIDE_INTERFACE
input-status: up
input-line-status: up
output-interface: OUTSIDE_INTERFACE
output-status: up
output-line-status: up
Action: allow

1 packet shown
>

[Verifying the Operation: Outside to Inside](#)

The NAT rule you created earlier evaluates the forward traffic—the traffic that originates from `INSIDE_INTERFACE` and is destined for `OUTSIDE_INTERFACE`. However, any traffic in the reverse direction does not match this rule. You can verify this by capturing SSH traffic on `OUTSIDE_INTERFACE` and by analyzing the trace data.

[Example 22-8](#) shows how to enable the **capture** tool on the outside interface.

Example 22-8 *Capturing SSH Traffic on the FTD `OUTSIDE_INTERFACE`*

[Click here to view code image](#)

! Enable capture on the outside interface:

```
> capture ssh_traffic_outside trace interface OUTSIDE_INTERFACE match tcp any  
any  
eq 22
```

! FTD begins capturing SSH traffic on the outside interface:

```
> show capture  
capture ssh_traffic_inside type raw-data trace interface INSIDE_INTERFACE
```

```
[Capturing - 0 bytes]
match tcp any any eq ssh
capture ssh_traffic_outside type raw-data trace interface OUTSIDE_INTERFACE
[Capturing - 0 bytes]
match tcp any any eq ssh
>
```

Now if you attempt to connect from an external host to an internal host, regardless of the destination IP address you choose—either original or masqueraded—the connection attempt fails.

[Example 22-9](#) shows the failed connection attempts from the external host 203.0.113.10 to the same internal host—through the masqueraded IP address 203.0.113.3 and the original IP address 192.168.1.10.22.

Example 22-9 *Captured Traffic on the FTD OUTSIDE_INTERFACE Shows Only SYN (S) Packets*

[Click here to view code image](#)

```
> show capture ssh_traffic_outside
```

```
8 packets captured
```

```
1: 03:56:51.100290    203.0.113.10.48400 > 203.0.113.3.22: S
```

```
3636330443:3636330443(0) win 29200 <mss 1460,sackOK,timestamp 18618684
```

```
0,nop,wscale 7>
```

```
2: 03:56:52.097269    203.0.113.10.48400 > 203.0.113.3.22: S
```

```
3636330443:3636330443(0) win 29200 <mss 1460,sackOK,timestamp 18618934
```

```
0,nop,wscale 7>
```

```
3: 03:56:54.101343    203.0.113.10.48400 > 203.0.113.3.22: S
```

```
3636330443:3636330443(0) win 29200 <mss 1460,sackOK,timestamp 18619435
```

```
0,nop,wscale 7>
```

```
4: 03:56:58.105478    203.0.113.10.48400 > 203.0.113.3.22: S
```

```
3636330443:3636330443(0) win 29200 <mss 1460,sackOK,timestamp 18620436
```

```
0,nop,wscale 7>
```

```
5: 03:57:22.069759    203.0.113.10.53048 > 192.168.1.10.22: S
```

```
1744936567:1744936567(0) win 29200 <mss 1460,sackOK,timestamp 18626426
0,nop,wscale 7>
```

```
6: 03:57:23.066250    203.0.113.10.53048 > 192.168.1.10.22: S
```

```
1744936567:1744936567(0) win 29200 <mss 1460,sackOK,timestamp 18626676
0,nop,wscale 7>
```

```
7: 03:57:25.070369    203.0.113.10.53048 > 192.168.1.10.22: S
```

```
1744936567:1744936567(0) win 29200 <mss 1460,sackOK,timestamp 18627177
0,nop,wscale 7>
```

```
8: 03:57:29.082469    203.0.113.10.53048 > 192.168.1.10.22: S
```

```
1744936567:1744936567(0) win 29200 <mss 1460,sackOK,timestamp 18628180
0,nop,wscale 7>
```

8 packets shown

>

[Example 22-10](#) analyzes the trace data of the first captured packet, where the external host tries to connect to the internal host using its masqueraded IP address, 203.0.113.3.

Example 22-10 *Trying to Connect to the Masqueraded IP Address of an Internal Host*

[Click here to view code image](#)

```
> show capture ssh_traffic_outside packet-number 1 trace
```

8 packets captured

```
1: 03:56:51.100290    203.0.113.10.48400 > 203.0.113.3.22: S
```

```
3636330443:3636330443(0) win 29200 <mss 1460,sackOK,timestamp 18618684
0,nop,wscale 7>
```

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

MAC Access list

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 3

Type: ROUTE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

found next-hop 203.0.113.3 using egress ifc OUTSIDE_INTERFACE

Result:

input-interface: OUTSIDE_INTERFACE

input-status: up

input-line-status: up

output-interface: OUTSIDE_INTERFACE

output-status: up

output-line-status: up

Action: drop

Drop-reason: (nat-no-xlate-to-pat-pool) Connection to PAT address without pre-existing xlate

1 packet shown

>

[Example 22-11](#) analyzes the trace data of the fifth captured packet where the external host tries to connect to the internal host by using its original IP address, 192.168.1.10.

Example 22-11 *Trying to Connect to the Original IP Address of an Internal Host*

[Click here to view code image](#)

> **show capture ssh_traffic_outside packet-number 5 trace**

8 packets captured

5: 03:57:22.069759 203.0.113.10.53048 > 192.168.1.10.22: S 1744936567:

1744936567(0) win 29200 <mss 1460,sackOK,timestamp 18626426 0,nop,wscale 7>

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.1.10 using egress ifc INSIDE_INTERFACE

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_global
access-list CSM_FW_ACL_advanced permit ip any any rule-id 268435457
access-list CSM_FW_ACL_remark rule-id 268435457: ACCESS POLICY: AC Policy -
Mandatory/1
access-list CSM_FW_ACL_remark rule-id 268435457: L7 RULE: Traffic Selection
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be
reached

Phase: 5
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Config:
class-map class-default
match any
policy-map global_policy
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
service-policy global_policy global

Additional Information:

Phase: 6

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 7

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 8

Type: NAT

Subtype: rpf-check

Result: DROP

Config:

object network Net-IN-192.168.1.0

nat (INSIDE_INTERFACE,OUTSIDE_INTERFACE) dynamic pat-pool Pool-OUT-203.0.113.3-5

flat include-reserve

Additional Information:

Result:

input-interface: OUTSIDE_INTERFACE

input-status: up

input-line-status: up

output-interface: INSIDE_INTERFACE

output-status: up

output-line-status: up

Action: drop

Drop-reason: (acl-drop) Flow is denied by configured rule

1 packet shown

>

[Connecting to a Masqueraded Destination \(Destination NAT for Inbound Connection\)](#)

When external hosts access any services of your company, they should access through the public IP address of your organization. Any internal addressing scheme must be invisible to the external users. In this section, you will learn how to connect to an internal host by using a masqueraded public IP address.

Figure 22-14 illustrates a scenario where an external host connects to an internal DMZ server of a company. When an external host initiates a connection to a masqueraded public address, FTD translates the address into an internal original address.

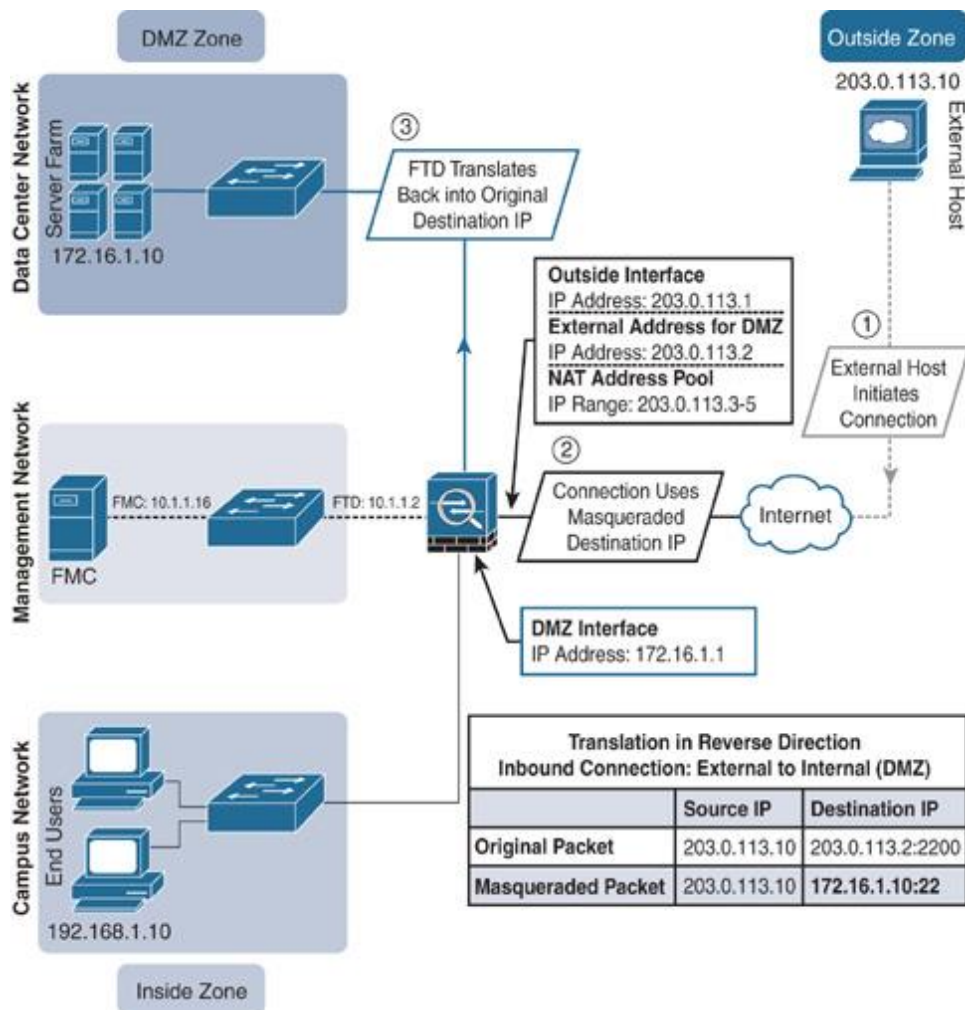


Figure 22-14 Lab Topology to Demonstrate Static NAT for Inbound Traffic

Configuring a Static NAT Rule

Because in the previous section you created an Auto NAT rule with dynamic type and analyzed its detailed operation, this section does not duplicate the same procedures for creating a NAT policy from scratch. You can just add a new NAT rule as illustrated in Figure 22-15 and then redeploy the NAT policy. If the policy deployment is successful, FTD should let an external host connect to an internal DMZ server using a masqueraded public IP address. Because the FTD in this case translates a public destination address to an internal address, this translation is known as destination NAT.

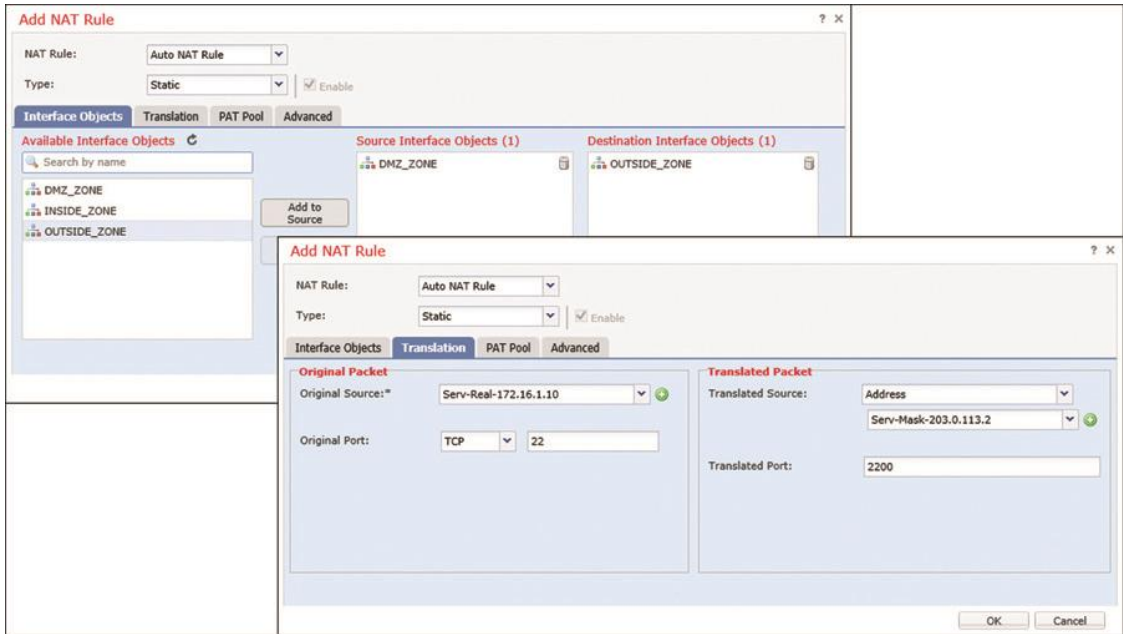


Figure 22-15 Defining a Static Auto NAT Rule for Inbound Connections

Figure 22-15 illustrates a static NAT rule that enables an outside host to connect to a DMZ server (internal IP address 172.16.1.10) via SSH service (internal port 22) without knowing the internal addressing scheme. The outside host can access the DMZ server only if the outside host uses the masqueraded IP address 203.0.113.2 and port 2200 as its destination.

Figure 22-16 shows two rules in a NAT policy—the static Auto NAT rule (bottom) has just been created to translate inbound connections. The dynamic NAT rule (top) was added earlier to translate outbound connections.

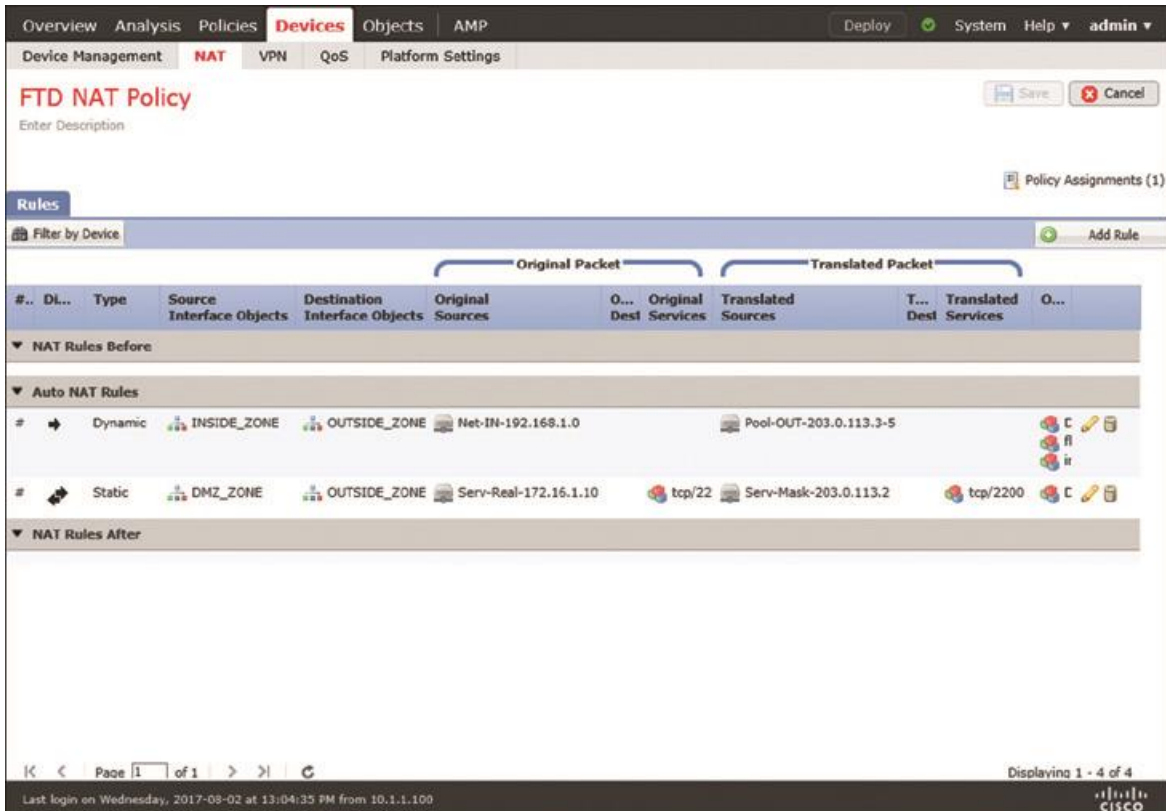


Figure 22-16 *Dynamic NAT and Static NAT Rules for Outbound and Inbound Traffic*

After you add a new NAT rule, you must click the **Save** and **Deploy** buttons to enable the new NAT policy on your FTD device.

[Verifying the Operation: Outside to DMZ](#)

This section demonstrates the operation of a static Auto NAT rule on an FTD device. As in the previous exercise, this one also uses SSH service to generate traffic. However, unlike in the previous exercise, the SSH connection is initiated by an external host.

Before you begin, you should clear the NAT counters and any existing translations so that you will be able to notice any new changes quickly:

```
> clear nat counters
> clear xlate
```

Now you can try to access the internal DMZ server from an external host. Using an SSH client, connect to port 2200 of the translated (masqueraded) IP address 203.0.113.2. You will be connected to the internal DMZ server, although the original IP address of the server is 172.16.1.10, and the server listens to port 22 for SSH connections. This happens due to the static NAT on the FTD device.

[Example 22-12](#) shows confirmation that the inbound SSH traffic matches the first rule on the Auto NAT policy. The `untranslate_hits` counter confirms the matching of one connection in the reverse direction.

Example 22-12 *Matching a Connection in the Reverse Direction*

[Click here to view code image](#)

```
> show nat detail
```

```
Auto NAT Policies (Section 2)
```

```
1 (DMZ_INTERFACE) to (OUTSIDE_INTERFACE) source static Serv-Real-172.16.1.10
```

```
Serv-Mask-203.0.113.2 service tcp ssh 2200
```

```
translate_hits = 0, untranslate_hits = 1
```

```
Source - Origin: 172.16.1.10/32, Translated: 203.0.113.2/32
```

```
Service - Protocol: tcp Real: ssh Mapped: 2200
```

```
2 (INSIDE_INTERFACE) to (OUTSIDE_INTERFACE) source dynamic Net-IN-192.168.1.0
```

```
pat-pool Pool-OUT-203.0.113.3-5 flat include-reserve
```

```
translate_hits = 0, untranslate_hits = 0
```

```
Source - Origin: 192.168.1.0/24, Translated (PAT): 203.0.113.3-203.0.113.5
```

```
>
```

[Example 22-13](#) shows the status of the current translations. The flag confirms a static port translation between an external host and an internal DMZ server.

Example 22-13 *Real-time Translation Status*

[Click here to view code image](#)

```
> show xlate detail
```

```
1 in use, 2 most used
```

```
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
```

```
s - static, T - twice, N - net-to-net
```

```
TCP PAT from DMZ_INTERFACE:172.16.1.10 22-22 to
```

```
OUTSIDE_INTERFACE:203.0.113.2
```

```
2200-2200
```

```
flags sr idle 0:00:54 timeout 0:00:00 refcnt 1 xlate id 0x7f516987ee00
```

```
>
```

To better understand the NAT operation, you can capture SSH traffic on an outside interface (on the translated port) and analyze it (see [Example 22-14](#)).

Example 22-14 *Capturing SSH Traffic on an Outside Interface (on a Translated Port)*

[Click here to view code image](#)

```
! Enable capture on outside interface:
```

```
> capture ssh_traffic_outside_masked trace interface OUTSIDE_INTERFACE match  
tcp any
```

```
any eq 2200
```

! Verify that the capture is running:

> **show capture**

```
capture ssh_traffic_inside type raw-data trace interface INSIDE_INTERFACE
```

```
[Capturing - 0 bytes]
```

```
match tcp any any eq ssh
```

```
capture ssh_traffic_outside type raw-data trace interface OUTSIDE_INTERFACE
```

```
[Capturing - 0 bytes]
```

```
match tcp any any eq ssh
```

```
capture ssh_traffic_outside_masked type raw-data trace interface OUTSIDE_INTERFACE
```

```
[Capturing - 0 bytes]
```

```
match tcp any any eq 2200
```

>

! Now, initiate an SSH connection from the external host to the internal DMZ

server. Use the masqueraded IP address and port number. It generates the following traffic.

> **show capture ssh_traffic_outside_masked**

59 packets captured

```
1: 05:21:23.785436    203.0.113.10.41760 > 203.0.113.2.2200: S
```

```
2089153959:2089153959(0) win 29200 <mss 1460,sackOK,timestamp 19887065
```

```
0,nop,wscale 7>
```

```
2: 05:21:23.786168    203.0.113.2.2200 > 203.0.113.10.41760: S
```

```
29917599:29917599(0) ack 2089153960 win 28960 <mss 1380,sackOK,timestamp
```

```
19892875
```

```
19887065,nop,wscale 7>
```



```
3: 05:21:23.786336    203.0.113.10.41760 > 203.0.113.2.2200: . ack 29917600
win 229 <nop,nop,timestamp 19887065 19892875>

4: 05:21:23.786855    203.0.113.10.41760 > 203.0.113.2.2200: P
2089153960:2089154001(41) ack 29917600 win 229 <nop,nop,timestamp
19887066 19892875>

5: 05:21:23.787312    203.0.113.2.2200 > 203.0.113.10.41760: . ack 2089154001
win 227 <nop,nop,timestamp 19892876 19887066>
.
.
<Output is omitted for brevity>
```

[Example 22-15](#) shows how to analyze the tracing data of a captured packet. FTD translates and allows the packet as you are connecting through IP address 203.0.113.2 and port 2200.

Example 22-15 *Analyzing a Translated Packet (Where the Packet Matches a Rule)*

[Click here to view code image](#)

```
> show capture ssh_traffic_outside_masked packet-number 1 trace
```

```
59 packets captured
```

```
1: 05:21:23.785436    203.0.113.10.41760 > 203.0.113.2.2200: S
2089153959:2089153959(0) win 29200 <mss 1460,sackOK,timestamp 19887065
0,nop,wscale 7>
```

```
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list
```

```
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
```

MAC Access list

Phase: 3

Type: UN-NAT

Subtype: static

Result: ALLOW

Config:

```
object network Serv-Real-172.16.1.10
```

```
nat (DMZ_INTERFACE,OUTSIDE_INTERFACE) static Serv-Mask-203.0.113.2 service  
tcp ssh 2200
```

Additional Information:

NAT divert to egress interface DMZ_INTERFACE

Untranslate 203.0.113.2/2200 to 172.16.1.10/22

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268435457
```

```
access-list CSM_FW_ACL_ remark rule-id 268435457: ACCESS POLICY: AC
```

```
Policy - Mandatory/1
```

```
access-list CSM_FW_ACL_ remark rule-id 268435457: L7 RULE: Traffic Selection
```

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

```
class-map class-default
```

```
match any
```

```
policy-map global_policy
```

```
class class-default
```

```
set connection advanced-options UM_STATIC_TCP_MAP
```

```
service-policy global_policy global
```

Additional Information:

Phase: 6

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 7

Type: IP-OPTIONS

Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network Serv-Real-172.16.1.10
nat (DMZ_INTERFACE,OUTSIDE_INTERFACE) static Serv-Mask-203.0.113.2 service tcp
ssh 2200
Additional Information:

Phase: 9
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 10
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 505, packet dispatched to next module

Phase: 12
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 13
Type: SNORT
Subtype:
Result: ALLOW
Config:

Additional Information:
Snort Verdict: (pass-packet) allow this packet

Phase: 14
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 172.16.1.10 using egress ifc DMZ_INTERFACE

Phase: 15
Type: ADJACENCY-LOOKUP
Subtype: next-hop and adjacency
Result: ALLOW
Config:
Additional Information:
adjacency Active
next-hop mac address a4ba.db9f.9460 hits 5205

Result:
input-interface: OUTSIDE_INTERFACE
input-status: up
input-line-status: up
output-interface: DMZ_INTERFACE
output-status: up
output-line-status: up
Action: allow

1 packet shown
>

Instead of using the translated address, if you attempt to connect using the original IP address, the connection attempt should fail. To verify it, you can use the command shown in [Example 22-16](#), which analyzes the tracing data of a captured packet. FTD captures the packet when an external host attempts to connect to the internal DMZ server using its original IP address, but the attempt fails.

Example 22-16 *Analyzing a Packet (Where the Packet Does Not Match a Rule)*

[Click here to view code image](#)

```
> show capture ssh_traffic_outside packet-number 1 trace
```

6 packets captured

```
1: 05:19:16.438255 203.0.113.10.48556 > 172.16.1.10.22:
```

S 1315278899:1315278899(0) win 29200 <mss 1460,sackOK,timestamp 19855229

0, nop,wscale 7>

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

MAC Access list

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 3

Type: ROUTE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

found next-hop 172.16.1.10 using egress ifc DMZ_INTERFACE

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268435457

access-list CSM_FW_ACL_ remark rule-id 268435457: ACCESS POLICY: AC

Policy - Mandatory/1

access-list CSM_FW_ACL_ remark rule-id 268435457: L7 RULE: Traffic Selection

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

class-map class-default

```
match any
policy-map global_policy
class class-default
  set connection advanced-options UM_STATIC_TCP_MAP
service-policy global_policy global
Additional Information:
```

```
Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 8
Type: NAT
Subtype: rpf-check
Result: DROP
Config:
object network Serv-Real-172.16.1.10
  nat (DMZ_INTERFACE,OUTSIDE_INTERFACE) static Serv-Mask-203.0.113.2 service
  tcp
  ssh 2200
Additional Information:
```

```
Result:
input-interface: OUTSIDE_INTERFACE
input-status: up
input-line-status: up
output-interface: DMZ_INTERFACE
output-status: up
output-line-status: up
Action: drop
```

Drop-reason: (acl-drop) Flow is denied by configured rule

1 packet shown

>

Summary

This chapter describes various types of NAT on an FTD device. It shows the steps to configure a NAT rule and demonstrates how FTD can leverage NAT technology to masquerade internal IP addresses in a real-world scenario.

Quiz

1. Which NAT technique allows you to translate one external destination IP address to multiple internal hosts?

- a. Static NAT
- b. Dynamic NAT
- c. PAT
- d. All of the above

2. Which NAT section has highest priority during rule evaluation?

- a. NAT Rules Before
- b. Auto NAT Rules
- c. NAT Rules After
- d. All of them have the same priority

3. Which command enables you to determine whether a connection matches a NAT rule and how many times it has matched?

- a. **show nat**
- b. **show nat detail**
- c. **show xlate detail**
- d. **show conn detail**

4. After you deploy a new NAT policy, if a connection still uses a rule from the prior version of the NAT policy, how could you ensure that FTD will use the new policy?

- a. Deploy the NAT policy one more time.
- b. Make the NAT rule more specific.
- c. Clear the current translation table.
- d. All of the above.

Appendixes

Appendix A

Answers to the Review Questions

Chapter 2

1. d

2. b

3. c

4. a

5. a

6. b

7. c

8. d

Chapter 3

1. b

2. d

3. b

4. d

5. b

Chapter 4

1. b

2. d

3. d

4. c

5. b

6. c

7. d

Chapter 5

1. c

2. c

3. d

4. b

5. d

Chapter 6

1. c

2. d

3. d

4. d

5. d

6. c

Chapter 7

1. b

2. c

3. c

4. d

5. c

6. c

Chapter 8

1. c

2. b

3. c

4. d

Chapter 9

1. d

2. c

3. d

4. c

Chapter 10

1. d

2. c

3. a

4. c

Chapter 11

1. d

2. d

3. b

4. c

Chapter 12

1. c

2. b

3. d

4. b

Chapter 13

1. d

2. d

3. d

4. c

Chapter 14

1. d

2. b

3. c

4. d

Chapter 15

1. c

2. d

3. c

4. d

Chapter 16

1. b

2. c

3. c

4. c

Chapter 17

1. d

2. b

3. c

4. b

Chapter 18

1. d

2. c

3. c

4. d

Chapter 19

1. c

2. d

3. c

4. d

Chapter 20

1. d

2. b

3. d

4. c

Chapter 21

1. d

2. d

3. c

4. d

Chapter 22

1. a

2. a

3. b

4. c

Appendix B

Generating and Collecting Troubleshooting Files Using the GUI

The Firepower System allows you to collect copies of various logs and configuration files so that you can investigate any technical issues offline or send them to Cisco for advanced analysis. In this appendix, you will learn the procedures to generate and collect troubleshooting files from the Firepower Management Center (FMC) and Firepower Threat Defense (FTD).

Generating Troubleshooting Files with the GUI

You can use the GUI to generate troubleshooting files from both the FMC and any managed FTD device. Here are the steps to follow:

Step 1. Navigate to **System > Health > Monitor**. The Appliance Status Summary appears, in which you can view the overall health status of all the managed devices as well as the FMC (see Figure B-1).

Step 2. Click on the name of an appliance from which you want to collect troubleshooting files. The Module Status Summary appears.

Tip

If you do not see your device in the Appliance Status Summary, expand an arrow key next to the status counts (refer to Figure B-1). This page does not display an appliance if the health status is normal.

Step 3. When you see the buttons **Generate Troubleshooting Files** and **Advanced Troubleshooting** next to the appliance name, click the **Generate Troubleshooting Files** button. The Troubleshooting Options window appears (see Figure B-2).

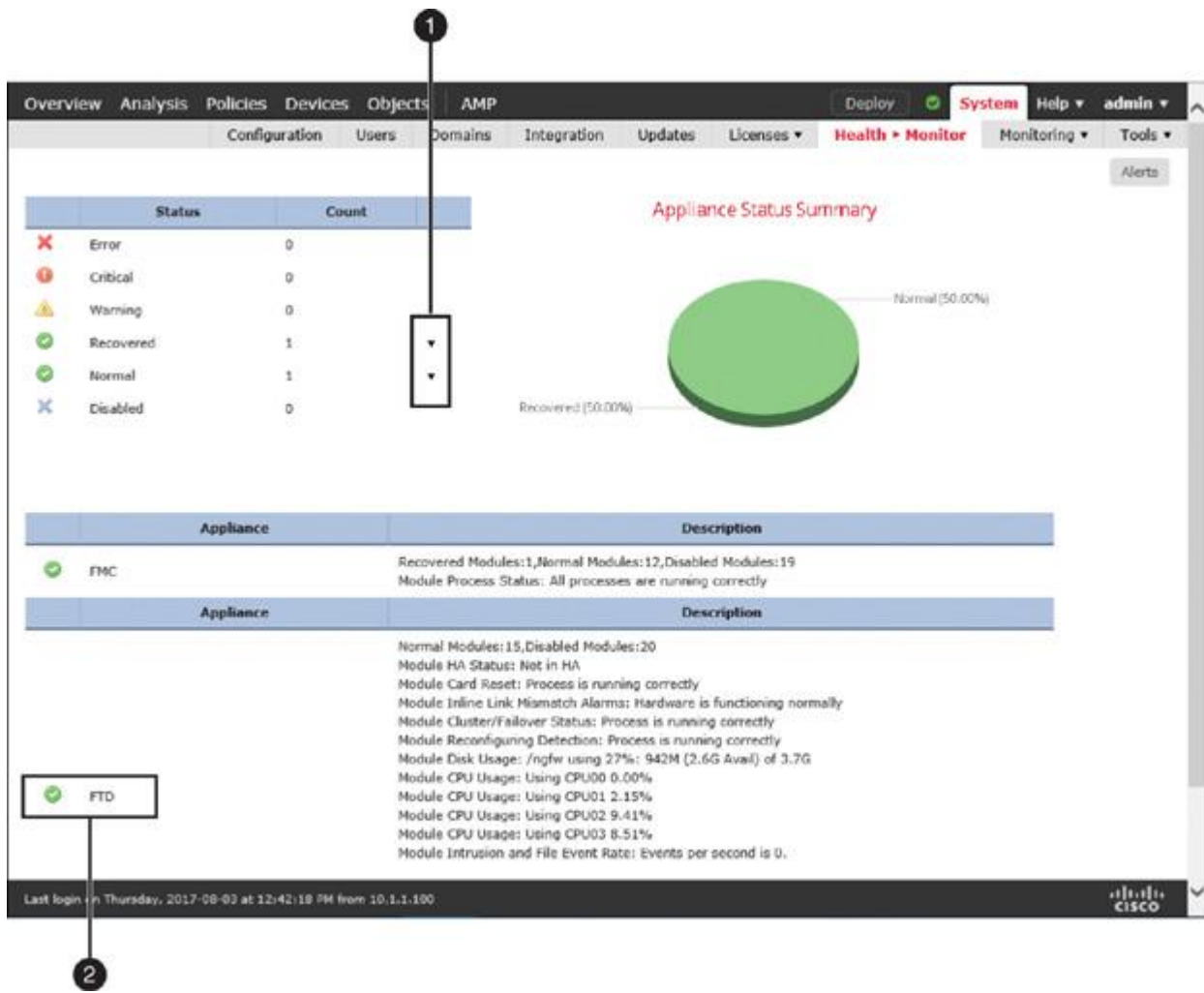


Figure B-1 Health Monitor Page Showing a Summary of the Appliance Health Status

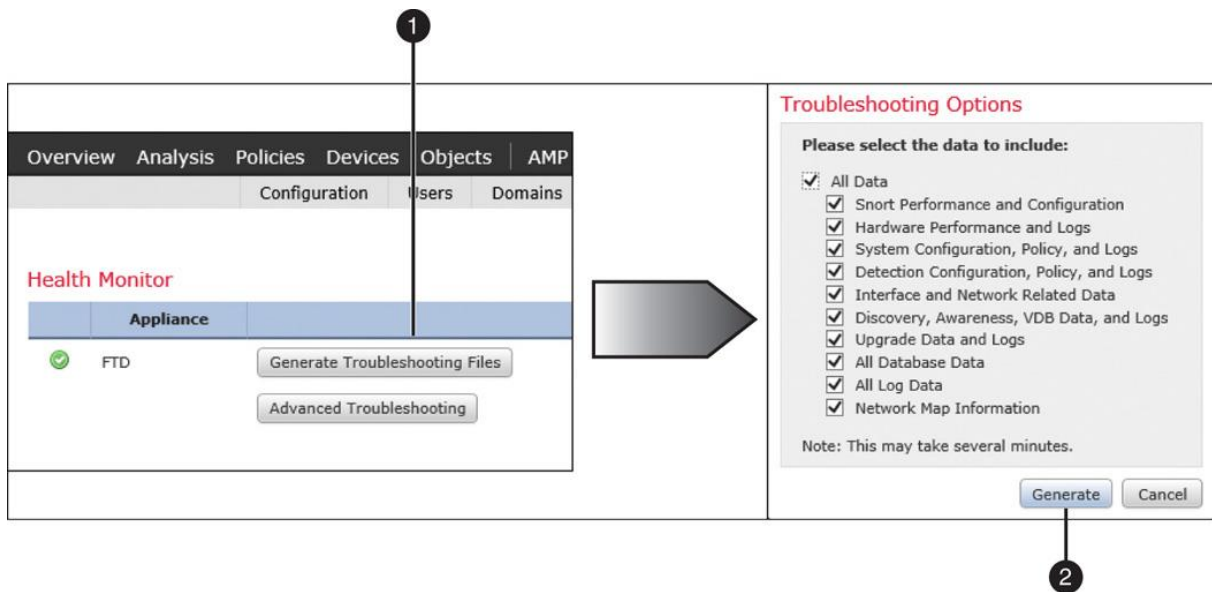


Figure B-2 Clicking the Generate Troubleshooting Files Button to Get Data Choices

Step 4. In the Troubleshooting Options window, select the data you want to include in the troubleshooting files. Click the **Generate** button to begin the process. Depending on the volume of events in the database and the sizes of various files, a Firepower system can take several minutes to complete the task.

Tip

Selecting the All Data check box allows a Firepower system to include a copy of all of the important configurations and log files in a compressed file (in .tar.gz format). It ensures that any necessary troubleshooting data is not left unidentified during the initial analysis.

Step 5. To view the status in real time, click the health status icon (in the right-top corner), and go to the Tasks tab.

Step 6. When the troubleshooting files are generated, click the **Click to retrieve generated files** download link to begin the download (see Figure B-3).

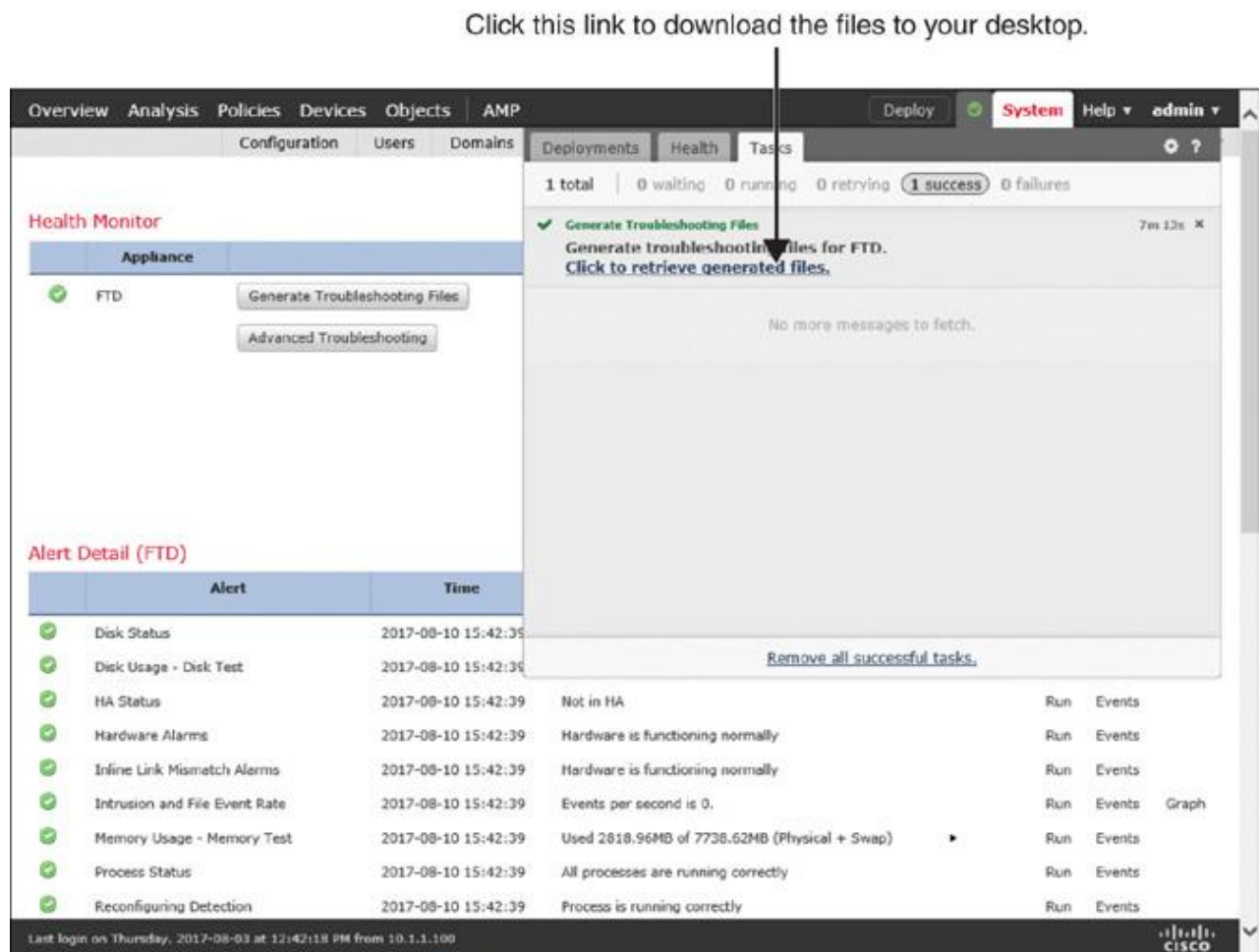


Figure B-3 Tasks Status Window Showing the Status of the File Generation Process

Appendix C

Generating and Collecting Troubleshooting Files Using the CLI

Although using the GUI is the preferred method of generating troubleshooting files, in some circumstances, generating the files using the CLI may be the only choice (for example, when the FMC is inaccessible via the GUI or when the registration between the FMC and FTD fails).

The commands to generate troubleshooting files are different at the FMC CLI and at the FTD CLI, as their shells are different. In addition, once the troubleshooting files are generated, there are multiple ways to transfer them from a Firepower system to your desktop. In the following sections, you will learn the available options and see examples.

Generating Troubleshooting Files at the FTD CLI

To generate troubleshooting files on an FTD device using the CLI, run the **system generate-troubleshoot** command at the shell. Use the **all** parameter with the command to include all the data in the .tar.gz file.

[Example C-1](#) demonstrates the use of the **system generate-troubleshoot all** command that creates troubleshooting files at the FTD CLI.

Example C-1 Generating Troubleshooting Files at the FTD CLI

[Click here to view code image](#)

```
> system generate-troubleshoot all
Starting /usr/local/sf/bin/sf_troubleshoot.pl...
Please, be patient. This may take several minutes.
The troubleshoot option code specified is ALL.
getting filenames from [/ngfw/usr/local/sf/etc/db_updates/index]
getting filenames from [/ngfw/usr/local/sf/etc/db_updates/base-6.1.0]
Troubleshooting information successfully created at /ngfw/var/common/
results-08-10-2017--201713.tar.gz
>
```

Once a .tar.gz file is created, you can view the file status by using the **file list** command.

[Click here to view code image](#)

```
> file list
Aug 10 20:23      73603794 /results-08-10-2017--201713.tar.gz
>
```

Any files you see in the **file list** command output can be copied into your desktop using either of two methods:

- Using the File Download functionality in the FMC GUI.

■ Using the **file secure-copy** command at the FTD CLI.

Downloading a File by Using the GUI

You can use the FMC GUI to copy a file from FTD. Here are the steps to accomplish that:

Step 1. Go to **System > Health > Monitor** and select the appliance from which you want to copy the file.

Step 2. Click the **Advanced Troubleshooting** button. The File Download page appears.

Step 3. Enter the name of the file you want to download (you do not need to include the full path; just enter the filename). Click the **Download** button.

Step 4. When the system prompts you to download the file to your desktop, click **Save**.

Figure C-1 shows the steps to download the FTD troubleshooting files in the FMC GUI. Note that only the filename is entered in the form.

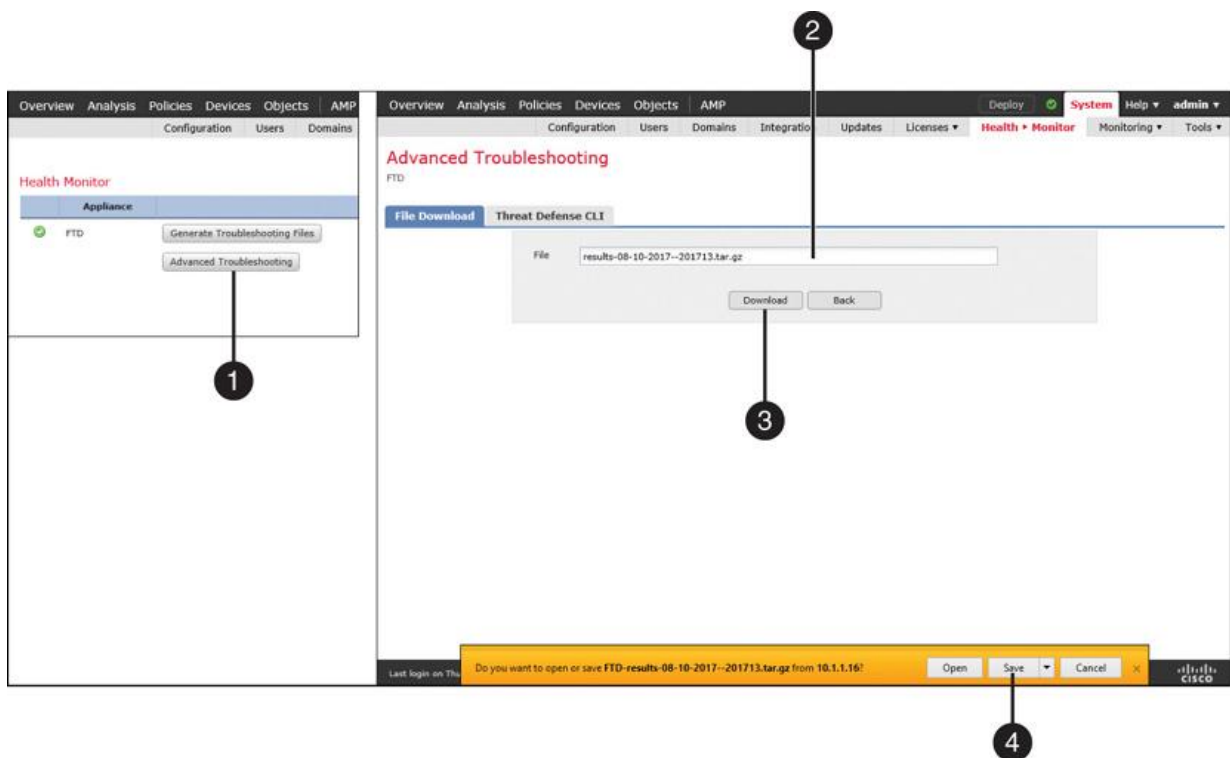


Figure C-1 Downloading a File from an FTD via FMC

Copying a File by Using the CLI

You can run the **file secure-copy** command at the FTD CLI to copy the troubleshooting files directly to your desktop. Here is the command syntax:

[Click here to view code image](#)

```
> file secure-copy <remote_IP> <remote_username> <remote_folder>  
<local_filename_on_FTD>
```

And here is an example of using the command:

[Click here to view code image](#)

```
> file secure-copy 10.1.1.100 admin /home/folder results-08-10-2017--201713.tar.gz
```

After you copy a file, you can delete it to free up the disk space. Run the **file delete** command as below:

[Click here to view code image](#)

```
> file delete results-08-10-2017--201713.tar.gz  
Really remove file results-08-10-2017--201713.tar.gz?  
Please enter 'YES' or 'NO': YES  
>
```

Generating Troubleshooting Files at the FMC CLI

To generate troubleshooting files at the FMC CLI, run the **sf_troubleshoot.pl** command with administrative privilege.

[Example C-2](#) shows the use of the **sf_troubleshoot.pl** command, which creates troubleshooting files at the FMC CLI.

Example C-2 Generating Troubleshooting Files at the FMC CLI

[Click here to view code image](#)

```
admin@FMC:~$ sudo sf_troubleshoot.pl  
Starting /usr/local/sf/bin/sf_troubleshoot.pl...  
Please, be patient. This may take several minutes.  
getting filenames from [/usr/local/sf/etc/db_updates/index]  
getting filenames from [/usr/local/sf/etc/db_updates/base-6.1.0]  
Troubleshooting information successfully created at /var/common/  
results-08-10-2017--184001.tar.gz  
admin@FMC:~$
```

Once a .tar.gz file is created, it is stored in the /var/common/ directory. You can view the file status by using the **ls** command.

[Example C-3](#) shows confirmation that the troubleshooting file is generated and stored in the /var/common folder in .tar.gz format.

Example C-3 Location of the FMC Troubleshooting File

[Click here to view code image](#)

```
admin@FMC:~$ ls -halp /var/common/
total 115M
drwxrwxr-x  2 admin detection 4.0K Aug 10 18:42 ./
drwxr-xr-x 17 root      4.0K Mar 28  2016 ../
-rw-r--r--  1 root root   115M Aug 10 18:42 results-08-10-2017--184001.tar.gz
admin@FMC:~$
```

To copy the file from the FMC CLI to your desktop, you can use the File Download feature on the GUI of the FMC. The processes are identical to the steps you followed for the FTD file transfer in the previous section. Alternatively, you can use the **scp** (Secure Copy over SSH protocol) command at the FMC CLI, which has the following syntax:

[Click here to view code image](#)

```
admin@FMC:~$ sudo scp
<local_filename_on_FMC><remote_username>@<remote_IP>: <remote_folder>
```

Here is an example of using this command:

[Click here to view code image](#)

```
admin@FMC:~$ sudo scp /var/common/results-08-10-2017--184001.tar.gz
admin@10.1.1.100:/home/folder
```

After you copy a file, you can delete it to free up disk space. To do so, run the **rm** command with administrative privilege:

[Click here to view code image](#)

```
admin@FMC:~$ sudo rm /var/common/results-08-10-2017--184001.tar.gz
Password:
admin@FMC:~$
```

Code Snippets

```
ciscoasa# copy tftp://TFTP_server_address/filename disk0:
```

```
ciscoasa# copy tftp://10.1.1.4/asa5500-firmware-1108.SPA disk0:

Address or name of remote host [10.1.1.4]?
Source filename [asa5500-firmware-1108.SPA]?
Destination filename [asa5500-firmware-1108.SPA]?

Accessing tftp://10.1.1.4/asa5500-firmware-1108.SPA...!!!!!!!
Done!
Computed Hash   SHA2: d824bdeecce1308fc64427367fa559e9
                eefe8f182491652ee4c05e6e751f7a4f
                5cdea28540cf60acde3ab9b65ff55a9f
                4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecce1308fc64427367fa559e9
                eefe8f182491652ee4c05e6e751f7a4f

Digital signature successfully validated
Writing file disk0:/asa5500-firmware-1108.SPA...
!!!!!!!
9241408 bytes copied in 8.230 secs (1155176 bytes/sec)
ciscoasa#
```

```
ciscoasa# upgrade rommon disk0:/asa5500-firmware-1108.SPA
```

```
ciscoasa# upgrade rommon disk0:/asa5500-firmware-1108.SPA

Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

Computed Hash   SHA2: d824bdeecce1308fc64427367fa559e9
                eefe8f182491652ee4c05e6e751f7a4f
                5cdea28540cf60acde3ab9b65ff55a9f
                4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecce1308fc64427367fa559e9
                eefe8f182491652ee4c05e6e751f7a4f
                5cdea28540cf60acde3ab9b65ff55a9f
                4e0cfb84b9e2317a856580576612f4af

Digital signature successfully validated
File Name       : disk0:/asa5500-firmware-1108.SPA
Image type      : Release
  Signer Information
    Common Name       : abraxas
    Organization Unit : NCS_Kenton_ASA
    Organization Name : CiscoSystems
Certificate Serial Number : 55831CF6
Hash Algorithm     : SHA2 512
Signature Algorithm : 2048-bit RSA
Key Version        : A
Verification successful.
Proceed with reload? [confirm]
```

```
***
*** --- START GRACEFUL SHUTDOWN ---
***
*** Message to all terminals:
***
***   Performing upgrade on rom-monitor.
Shutting down isakmp
Shutting down webvpn
Shutting down sw-module
Shutting down License Controller
Shutting down File system
***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
```

```
***   Performing upgrade on rom-monitor.
Process shutdown finished
Rebooting... (status 0x9)
..
INIT: Sending processes the TERM signal
Stopping OpenBSD Secure Shell server: sshdno /usr/sbin/sshd found; none killed
Deconfiguring network interfaces... done.
Sending all processes the TERM signal...
Sending all processes the KILL signal...
Deactivating swap...
Unmounting local filesystems...
Rebooting...
```

```
Rom image verified correctly
Cisco Systems ROMMON, Version 1.1.01, RELEASE SOFTWARE
Copyright (c) 1994-2014 by Cisco Systems, Inc.
Compiled Mon 10/20/2014 15:59:12.05 by builder

Current image running: Boot ROM0
Last reset cause: PowerCycleRequest
DIMM Slot 0 : Present
INFO: Rommon upgrade state: ROMMON_UPG_START (1)
INFO: Reset code: 0x00002000
Firmware upgrade step 1...
Looking for file 'disk0:/asa5500-firmware-1108.SPA'
Located 'asa5500-firmware-1108.SPA' @ cluster 1608398.
#####
###
#####
Image base 0x77014018, size 9241408
LFBFF signature verified.
Objtype: lfbff_object_rommon (0x800000 bytes @ 0x77014238)
Objtype: lfbff_object_fpga (0xd0100 bytes @ 0x77814258)
INFO: FPGA version in upgrade image: 0x0202
INFO: FPGA version currently active: 0x0202
INFO: The FPGA image is up-to-date.
INFO: Rommon version currently active: 1.1.01.
INFO: Rommon version in upgrade image: 1.1.08.
Active ROMMON: Preferred 0, selected 0, booted 0
Switching SPI access to standby rommon 1.
Please DO NOT reboot the unit, updating ROMMON.....
INFO: Duplicating machine state.....
Reloading now as step 1 of the rommon upgrade process...
```

```
Toggling power on system board...
Rom image verified correctly

Cisco Systems ROMMON, Version 1.1.01, RELEASE SOFTWARE
Copyright (c) 1994-2014 by Cisco Systems, Inc.
Compiled Mon 10/20/2014 15:59:12.05 by builder
Current image running: Boot ROM0
Last reset cause: RP-Reset
DIMM Slot 0 : Present
INFO: Rommon upgrade state: ROMMON_UPG_START (1)

INFO: Reset code: 0x00000008
Active ROMMON: Preferred 0, selected 0, booted 0
Firmware upgrade step 2...
Detected current rommon upgrade is available, continue rommon upgrade process
Rommon upgrade reset 0 in progress
Reloading now as step 2 of the rommon upgrade process...
```

Rom image verified correctly
Cisco Systems ROMMON, Version 1.1.8, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Thu 06/18/2015 12:15:56.43 by builders

Current image running: *Upgrade in progress* Boot ROM1
Last reset cause: BootRomUpgrade
DIMM Slot 0 : Present
INFO: Rommon upgrade state: ROMMON_UPG_START (1)
INFO: Reset code: 0x00000010
PROM B: stopping boot timer
Active ROMMON: Preferred 0, selected 0, booted 1
INFO: Rommon upgrade state: ROMMON_UPG_TEST

!!
!! Please manually or auto boot ASAOS now to complete firmware upgrade !!
!!

Platform ASA5506 with 4096 Mbytes of main memory
MAC Address: a4:6c:2a:e4:6b:bf
Using default Management Ethernet Port: 0

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot in 5 seconds.

```
Located '.boot_string' @ cluster 1607965.

#
Attempt autoboot: "boot disk0:/asa961-50-lfbff-k8.spa"
Located 'asa961-50-lfbff-k8.spa' @ cluster 10.

#####
#####
#####
#####
LFBFF signature verified.
INIT: version 2.88 booting
Starting udev
Configuring network interfaces... done.
Populating dev cache
dosfsck 2.11, 12 Mar 2005, FAT32, LPN
There are differences between boot sector and its backup.
Differences: (offset:original/backup)
    65:01/00
    Not automatically fixing this.
Starting check/repair pass.
Starting verification pass.
/dev/sdb1: 104 files, 811482/1918808 clusters
dosfsck(/dev/sdb1) returned 0
Mounting /dev/sdb1
Setting the offload CPU count to 0
IO Memory Nodes: 1
IO Memory Per Node: 205520896 bytes
```


Global Reserve Memory Per Node: 314572800 bytes Nodes=1

LCMB: got 205520896 bytes on numa-id=0, phys=0x10d400000, virt=0x2aaaab000000

LCMB: HEAP-CACHE POOL got 314572800 bytes on numa-id=0, virt=0x7fedbc200000

Processor memory: 1502270072

Compiled on Fri 04-Mar-16 10:50 PST by builders

Total NICs found: 14

i354 rev03 Gigabit Ethernet @ irq255 dev 20 index 08 MAC: a46c.2ae4.6bbf

ivshmem rev03 Backplane Data Interface @ index 09 MAC: 0000.0001.0002

en_vtun rev00 Backplane Control Interface @ index 10 MAC: 0000.0001.0001

en_vtun rev00 Backplane Int-Mgmt Interface @ index 11 MAC: 0000.0001.0003

en_vtun rev00 Backplane Ext-Mgmt Interface @ index 12 MAC: 0000.0000.0000

en_vtun rev00 Backplane Tap Interface @ index 13 MAC: 0000.0100.0001

Rom-monitor was successfully upgraded.

Verify the activation-key, it might take a while...

.
.

! Licensing and legal information are omitted for brevity

.
.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Reading from flash...

!.

Cryptochecksum (unchanged): 868f669d 9e09ca8b e91c32de 4ee8fd7f

INFO: Power-On Self-Test in process.

.....

INFO: Power-On Self-Test complete.

INFO: Starting HW-DRBG health test...

INFO: HW-DRBG health test passed.

INFO: Starting SW-DRBG health test...

INFO: SW-DRBG health test passed.

Type help or '?' for a list of available commands.

ciscoasa>

```

ciscoasa> enable
Password: *****
ciscoasa# show module

Mod  Card Type                               Model                               Serial No.
-----
  1  ASA 5506-X with FirePOWER services, 8GE, AC, ASA5506          JAD191100HG
sfr Unknown                               N/A                                 JAD191100HG

Mod  MAC Address Range                     Hw Version  Fw Version  Sw Version
-----
  1  a46c.2ae4.6bbf to a46c.2ae4.6bc8  1.0         1.1.8       9.6(1)50
sfr a46c.2ae4.6bbe to a46c.2ae4.6bbe  N/A         N/A

Mod  SSM Application Name                   Status           SSM Application Version
-----

Mod  Status           Data Plane Status  Compatibility
-----
  1  Up Sys           Not Applicable
sfr Unresponsive   Not Applicable

ciscoasa#

```

```

ciscoasa# reload
Proceed with reload? [confirm]
ciscoasa#
***
*** --- START GRACEFUL SHUTDOWN ---
Shutting down isakmp
Shutting down webvpn
Shutting down sw-module
Shutting down License Controller
Shutting down File system
***
*** --- SHUTDOWN NOW ---
Process shutdown finished
Rebooting... (status 0x9)
..
INIT: Sending processes the TERM signal
Stopping OpenBSD Secure Shell server: sshdno /usr/sbin/sshd found; none killed
Deconfiguring network interfaces... done.
Sending all processes the TERM signal...
Sending all processes the KILL signal...
Deactivating swap...
Unmounting local filesystems...
Rebooting...

```

Rom image verified correctly

Cisco Systems ROMMON, Version 1.1.8, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Thu 06/18/2015 12:15:56.43 by builders

Current image running: Boot ROM1
Last reset cause: PowerCycleRequest
DIMM Slot 0 : Present

Platform ASA5506 with 4096 Mbytes of main memory
MAC Address: a4:6c:2a:e4:6b:bf
Using default Management Ethernet Port: 0

Use BREAK or ESC to interrupt boot.

Use SPACE to begin boot immediately.

Boot in 7 seconds.

Boot interrupted.

rommon 1 >

rommon 1 > **help**

?	Display this help menu
address	Set the local IP address
boot	Boot an application program
confreg	Configuration register contents display and management
console	Console BAUD rate display and configuration
dev	Display a list of available file system devices
dir	File directory display command
erase	erase the specified file system
file	Set the application image file path/name to be TFTPed
gateway	Set the default gateway IP address
help	"help" for this menu "help <command>" for specific command information
history	Show the command line history
netmask	Set the IP subnet mask value
ping	Test network connectivity with ping commands
server	Set the TFTP server IP address
show	Display system device and status information
tftpdnld	Download and run the image defined by "FILE"
reboot	Reboot the system
reload	Reboot the system
repeat	Repeat a CLI command
reset	Reboot the system
set	Display the configured environment variables
sync	Save the environment variables to persistent storage
unset	Clear a configured environment variable


```
Boot buffer bigbuf=348bd018
Boot image size = 100921600 (0x603f100) bytes
[image size]      100921600
[MD5 signature]   0264697f6f1942b9bf80f820fb209ad5
LFBFF signature verified.
INIT: version 2.88 booting
Starting udev
Configuring network interfaces... done.
Populating dev cache
Detected PID ASA5506.
Found device serial number JAD191100HG.
Found USB flash drive /dev/sdb
Found hard drive(s): /dev/sda
fsck from util-linux 2.23.2
dosfsck 2.11, 12 Mar 2005, FAT32, LFN
There are differences between boot sector and its backup.
Differences: (offset:original/backup)
  65:01/00
  Not automatically fixing this.
/dev/sdb1: 52 files, 811482/1918808 clusters
Launching boot CLI ...
Configuring network interface using static IP
Bringing up network interface.
```

```
Depending on your network, this might take a couple of minutes when using DHCP...
ifup: interface lo already configured
Using IPv4 address: 10.1.1.21
INIT: Starting system message bus: dbus.
Starting OpenBSD Secure Shell server: sshd
  generating ssh RSA key...
  generating ssh ECDSA key...
  generating ssh DSA key...
done.
Starting Advanced Configuration and Power Interface daemon: acpid.
acpid: starting up
acpid: 1 rule loaded
acpid: waiting for events: event logging is off
Starting ntpd: done
Starting syslog-ng: [2016-09-19T19:43:24.781411] Connection failed; fd='15',
  server='AF_INET(127.128.254.1:514)', local='AF_INET(0.0.0.0:0)', error='Network is
  unreachable (101)'
[2016-09-19T19:43:24.781508] Initiating connection failed, reconnecting;
  time_reopen='60'
.
Starting crond: OK

Cisco FTD Boot 6.0.0 (9.6.2.)
Type ? for list of commands
ciscoasa-boot>
```

```
ciscoasa-boot> ?
  show           => Display system information. Enter show ? for options
  system        => Control system operation
  setup         => System Setup Wizard
  support       => Support information for TAC
  delete        => Delete files
  ping          => Ping a host to check reachability
  traceroute    => Trace the route to a remote host
  exit          => Exit the session
  help         => Get help on command syntax
ciscoasa-boot>
```

```
ciscoasa-boot> setup

                Welcome to Cisco FTD Setup
                [hit Ctrl-C to abort]
                Default values are inside []

Enter a hostname [ciscoasa]:
Do you want to configure IPv4 address on management interface?(y/n) [Y]:
Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n)
[N]:

Enter an IPv4 address [10.1.1.21]:
Enter the netmask [255.255.255.0]:
Enter the gateway [10.1.1.1]:
Do you want to configure static IPv6 address on management interface?(y/n) [N]:
Stateless autoconfiguration will be enabled for IPv6 addresses.
Enter the primary DNS server IP address: 10.1.1.8
Do you want to configure Secondary DNS Server? (y/n) [n]:
Do you want to configure Local Domain Name? (y/n) [n]:
Do you want to configure Search domains? (y/n) [n]:
Do you want to enable the NTP service? [Y]:
Enter the NTP servers separated by commas: 10.1.1.9

Please review the final configuration:
Hostname:                ciscoasa
Management Interface Configuration
```

```
IPv4 Configuration:      static
    IP Address:          10.1.1.21
    Netmask:             255.255.255.0
    Gateway:             10.1.1.1

IPv6 Configuration:      Stateless autoconfiguration

DNS Configuration:
    DNS Server:          10.1.1.8

NTP configuration:       10.1.1.9
```

CAUTION:

You have selected IPv6 stateless autoconfiguration, which assigns a global address based on network prefix and a device identifier. Although this address is unlikely to change, if it does change, the system will stop functioning correctly.

We suggest you use static addressing instead.

Apply the changes?(y,n) [Y]:

Configuration saved successfully!

Applying...

Restarting network services...

Done.

Press ENTER to continue...

ciscoasa-boot>

```
ciscoasa-boot> ping 10.1.1.4
PING 10.1.1.4 (10.1.1.4) 56(84) bytes of data.
64 bytes from 10.1.1.4: icmp_seq=1 ttl=64 time=0.364 ms
64 bytes from 10.1.1.4: icmp_seq=2 ttl=64 time=0.352 ms
64 bytes from 10.1.1.4: icmp_seq=3 ttl=64 time=0.326 ms
64 bytes from 10.1.1.4: icmp_seq=4 ttl=64 time=0.313 ms
^C
--- 10.1.1.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.313/0.338/0.364/0.030 ms

ciscoasa-boot>
```

```
ciscoasa-boot> system install http://10.1.1.4/ftd-6.1.0-330.pkg
```

```
##### WARNING #####  
# The content of disk0: will be erased during installation! #  
#####
```

```
Do you want to continue? [y/N] Y
```

```
Erasing disk0 ...
```

```
Verifying
```

```
Downloading...
```

```
Extracting....
```

```
Package Detail
```

```
    Description:                Cisco ASA-FTD 6.1.0-330 System Install
```

```
    Requires reboot:            Yes
```

```
Do you want to continue with upgrade? [y]:
```

```
Warning: Please do not interrupt the process or turn off the system.
```

```
Doing so might leave system in unusable state.
```

```
Starting upgrade process ...
```

```
Populating new system image..
```

```
Reboot is required to complete the upgrade. Press 'Enter' to reboot the system.
```

```
Broadcast mStopping OpenBSD Secure Shell server: sshdstopped /usr/sbin/sshd (pid 1723)
```

```
.
```

```
Stopping Advanced Configuration and Power Interface daemon: stopped /usr/sbin/acpid  
(pid 1727)
```

```
acpid: exiting
```

```
acpid.
```

```
Stopping system message bus: dbus.
```

```
Stopping ntpd: stopped process in pidfile '/var/run/ntp.pid' (pid 1893)
```

```
done
```

```
Stopping crond: OKs
```

```
Deconfiguring network interfaces... done.
```

```
Sending all processes the TERM signal...
```

```
Sending all processes the KILL signal...
```

```
Deactivating swap...
```

```
Unmounting local filesystems...
```

```
Rebooting...
```

```
Rom image verified correctly
```


Cisco Systems ROMMON, Version 1.1.8, RELEASE SOFTWARE

Copyright (c) 1994-2015 by Cisco Systems, Inc.

Compiled Thu 06/18/2015 12:15:56.43 by builders

Current image running: Boot ROM1

Last reset cause: PowerCycleRequest

DIMM Slot 0 : Present

Platform ASA5506 with 4096 Mbytes of main memory

MAC Address: a4:6c:2a:e4:6b:bf

Using default Management Ethernet Port: 0

Use BREAK or ESC to interrupt boot.

Use SPACE to begin boot immediately.

Boot in 5 seconds.

Located '.boot_string' @ cluster 260097.

#

Attempt autoboot: "boot disk0:os.img"

Located 'os.img' @ cluster 235457.

```
#####
#####
#####
#####
#####
#####
#####
```

LFBFF signature verified.

INIT: version 2.88 booting

Starting udev

Configuring network interfaces... done.

Populating dev cache

Detected PID ASA5506.

Found device serial number JAD191100HG.

Found USB flash drive /dev/sdb

Found hard drive(s): /dev/sda

fsck from util-linux 2.23.2

dosfsck 2.11, 12 Mar 2005, FAT32, LFN

/dev/sdb1: 7 files, 24683/1919063 clusters

Use ESC to interrupt boot and launch boot CLI.

Use SPACE to launch Cisco FTD immediately.

Cisco FTD launch in 21 seconds ...

Cisco FTD launch in 0 seconds ...

Running on kenton

Mounting disk partitions ...

Initializing Threat Defense ... [OK]

Starting system log daemon... [OK]

Stopping mysql...

Sep 19 20:29:33 ciscoasa SF-IMS[2303]: [2303] pmtool:pmtool [ERROR] Unable to connect to UNIX socket at /ngfw/var/sf/run/PM_Control.sock: No such file or directory

Starting mysql...

Sep 19 20:29:33 ciscoasa SF-IMS[2304]: [2304] pmtool:pmtool [ERROR] Unable to connect to UNIX socket at /ngfw/var/sf/run/PM_Control.sock: No such file or directory

Flushing all current IPv4 rules and user defined chains: ...success

Clearing all current IPv4 rules and user defined chains: ...success

Applying iptables firewall rules:

Flushing chain 'PREROUTING'

.

! Omitted the messages related to iptables flushing for brevity

.

Flushing chain 'OUTPUT'

Applying rules succeeded

Starting nscd...

mkdir: created directory '/var/run/nscd' [OK]

Starting , please wait...grep: /ngfw/etc/motd: No such file or directory

...complete.

Firstboot detected, executing scripts

Executing S01reset_failopen_if [OK]

Executing S01virtual-machine-reconfigure [OK]

Executing S02aws-pull-cfg [OK]

Executing S02configure_onbox [OK]

Executing S04fix-httpd.sh [OK]

Executing S05set-mgmt-port [OK]

Executing S06addusers [OK]

Executing S07uuid-init [OK]

Executing S08configure_mysql [OK]

***** Attention *****

Initializing the configuration database. Depending on available system resources (CPU, memory, and disk), this may take 30 minutes or more to complete.

***** Attention *****

Executing S09database-init	[OK]
Executing S11database-populate	[OK]
Executing S12install_infodb	[OK]
Executing S15set-locale.sh	[OK]
Executing S16update-sensor.pl	[OK]
Executing S19cert-tun-init	[OK]
Executing S20cert-init	[OK]
Executing S21disable_estreamer	[OK]
Executing S25create_default_des.pl	[OK]
Executing S30init_lights_out_mgmt.pl	[OK]
Executing S40install_default_filters.pl	[OK]
Executing S42install_default_dashboards.pl	[OK]
Executing S43install_default_report_templates.pl	[OK]
Executing S44install_default_app_filters.pl	[OK]
Executing S45install_default_realms.pl	[OK]
Executing S47install_default_sandbox_EO.pl	[OK]
Executing S50install-remediation-modules	[OK]
Executing S51install_health_policy.pl	[OK]
Executing S52install_system_policy.pl	[OK]
Executing S53change_reconciliation_baseline.pl	[OK]
Executing S70remove_casuser.pl	[OK]
Executing S70update_sensor_objects.sh	[OK]
Executing S85patch_history-init	[OK]
Executing S90banner-init	[OK]
Executing S95copy-crontab	[OK]
Executing S96grow_var.sh	[OK]
Executing S96install_vmware_tools.pl	[OK]

***** Attention *****

Initializing the system's localization settings. Depending on available system resources (CPU, memory, and disk), this may take 10 minutes or more to complete.

***** Attention *****

```
Executing S96localize-templates [ OK ]
Executing S96ovf-data.pl [ OK ]
Executing S97compress-client-resources [ OK ]
Executing S97create_platinum_forms.pl [ OK ]
Executing S97install_cas [ OK ]
Executing S97install_cloud_support.pl [ OK ]
Executing S97install_geolocation.pl [ OK ]
Executing S97install_ssl_inspection.pl [ OK ]
Executing S97update_modprobe.pl [ OK ]
Executing S98check-db-integrity.sh [ OK ]
Executing S98htaccess-init [ OK ]
Executing S98is-sru-finished.sh [ OK ]
Executing S99correct_ipmi.pl [ OK ]
Executing S99start-system [ OK ]
Executing S99z_db_restore [ OK ]
Executing S99_z_cc-integrity.sh [ OK ]
Firstboot scripts finished.
Configuring NTP... [ OK ]
fatattr: can't open '/mnt/disk0/.private2': No such file or directory
fatattr: can't open '/mnt/disk0/.ngfw': No such file or directory
Model reconfigure detected, executing scripts
Pinging mysql
```

```
Found mysql is running
Executing 45update-sensor.pl [ OK ]
Executing 55recalculate_arc.pl [ OK ]
Starting xinetd:
Mon Sep 19 20:59:07 UTC 2016
Starting MySQL...
Pinging mysql
Pinging mysql, try 1
Pinging mysql, try 2
Found mysql is running
Running initializeObjects...
Stopping MySQL...
Killing mysqld with pid 22285
Wait for mysqld to exit\c
done
Mon Sep 19 20:59:32 UTC 2016

Starting sfid... [ OK ]
Starting Cisco ASA5506-X Threat Defense, please wait...No PM running!
...started.
INIT: Starting system message bus: dbus.
Starting OpenBSD Secure Shell server: sshd

generating ssh RSA key...
generating ssh ECDSA key...
generating ssh DSA key...
```

```
done.
Starting Advanced Configuration and Power Interface daemon: acpid.
Starting crond: OK
Sep 19 20:59:42 ciscoasa SF-IMS[22997]: [22997] init script:system [INFO] pmmon
  Setting affinity to 0-3...
pid 22993's current affinity list: 0-3
pid 22993's new affinity list: 0-3
Sep 19 20:59:42 ciscoasa SF-IMS[22999]: [22999] init script:system [INFO] pmmon The
  Process Manager is not running...
Sep 19 20:59:42 ciscoasa SF-IMS[23000]: [23000] init script:system [INFO] pmmon
  Starting the Process Manager...
Sep 19 20:59:42 ciscoasa SF-IMS[23001]: [23001] pm:pm [INFO] Using model number 75J

IO Memory Nodes: 1
IO Memory Per Node: 205520896 bytes

Global Reserve Memory Per Node: 314572800 bytes Nodes=1

LCMB: got 205520896 bytes on numa-id=0, phys=0x2400000, virt=0x2aaaac200000
LCMB: HEAP-CACHE POOL got 314572800 bytes on numa-id=0, virt=0x7fa17d600000
Processor memory: 1583098718

Compiled on Tue 23-Aug-16 19:42 PDT by builders

Total NICs found: 14
.
! Omitted the MAC addresses, licensing and legal messages for brevity
.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
```

Reading from flash...

!

Cryptochecksum (changed): f410387e 8aab8a4e f71eb8a9 f8b37ef9

INFO: Power-On Self-Test in process.

.....

INFO: Power-On Self-Test complete.

INFO: Starting HW-DRBG health test...

INFO: HW-DRBG health test passed.

INFO: Starting SW-DRBG health test...

INFO: SW-DRBG health test passed.

Type help o '?' for a list

Cisco ASA5506-X Threat Defense v6.1.0 (build 330)

firepower login:

firepower login: **admin**

Password: **Admin123**

You must accept the EULA to continue.

Press <ENTER> to display the EULA:

END USER LICENSE AGREEMENT

.

.

!The EULA messages are omitted for brevity

.

.

.Please enter 'YES' or press <ENTER> to AGREE to the EULA:

```
System initialization in progress. Please stand by.
You must change the password for 'admin' to continue.
Enter new password:
Confirm new password:
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.1.1.21
Enter an IPv4 netmask for the management interface [255.255.255.0]:
Enter the IPv4 default gateway for the management interface [192.168.45.1]: 10.1.1.1
Enter a fully qualified hostname for this system [firepower]:
Enter a comma-separated list of DNS servers or 'none' []:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
```

```
Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...
Update policy deployment information
  - add device configuration
  - add network discovery
  - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required. In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'
```


However, if the sensor and the Firepower Management Center are separated by a NAT device, you must enter a unique NAT ID, along with the unique registration key.

```
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'
```

Later, using the web interface on the Firepower Management Center, you must use the same registration key and, if necessary, the same NAT ID when you add this sensor to the Firepower Management Center.

>

>

! The > prompt confirms that you are on the FTD default shell. Run the following command to connect to the ASA console:

```
> system support diagnostic-cli
```

Attaching to ASA console ... Press 'Ctrl+a then d' to detach.

Type help or '?' for a list of available commands.

```
firepower>
```

! Now you have entered the ASA console. Run the enable command to enter the privilege exec mode.

```
firepower> enable
```

```
Password:
```

```
firepower# exit
```

Logoff

Type help or '?' for a list of available commands.

firepower>

! If you want to quit from the ASA console, the exit command logs you off from the ASA console, but does not let you return to the FTD default shell. To disconnect from the ASA console, press the Ctrl+a keys together, then press d separately.

firepower>

Console connection detached.

>

! To connect to the Firepower Linux shell, run the expert command. To return to the FTD default shell, run the exit command.

> expert

admin@firepower:~\$ exit

logout

>

> show version

```
-----[ firepower ]-----  
Model                : Cisco ASA5506-X Threat Defense (75) Version 6.1.0  
  (Build 330)  
UUID                 : c84ceb32-7ea7-11e6-a7ad-94bcd8f36790  
Rules update version : 2016-03-28-001-vrt  
VDB version          : 270  
-----
```

>

```
ciscoasa# dir

Directory of disk0:/

88      -rwx  91290240      11:04:08 May 12 2016  asa961-50-lfbff-k8.spa
89      -rwx   63          16:25:14 Sep 19 2016  .boot_string
11      drwx  4096         12:14:22 May 12 2016  log
19      drwx  4096         12:15:12 May 12 2016  crypto_archive
20      drwx  4096         12:15:16 May 12 2016  coredumpinfo

7859437568 bytes total (4544851968 bytes free)

ciscoasa#
```

```
ciscoasa# show flash:

--#--  --length--  -----date/time-----  path
  88  91290240      May 12 2016 11:04:08  asa961-50-lfbff-k8.spa
  89   63          Sep 19 2016 16:25:14  .boot_string
  11  4096          May 12 2016 12:14:22  log
  13   0           May 12 2016 12:14:22  log/asa-appagent.log
  19  4096          May 12 2016 12:15:12  crypto_archive
  20  4096          May 12 2016 12:15:16  coredumpinfo
  21  59           May 12 2016 12:15:16  coredumpinfo/coredump.cfg

7859437568 bytes total (4544851968 bytes free)

ciscoasa#
```

```
ciscoasa# delete flash:/output.txt
```

```
ciscoasa# show inventory

Name: "Chassis", DESCR: "ASA 5506-X with FirePOWER services, 8GE, AC, DES"
PID: ASA5506          , VID: V01          , SN: JMX1916Z07V

Name: "Storage Device 1", DESCR: "ASA 5506-X SSD"
PID: ASA5506-SSD     , VID: N/A          , SN: MSA190600NE

ciscoasa#
```

```
ciscoasa# show inventory
Name: "Chassis", DESCR: "ASA 5545-X with SW, 8 GE Data, 1 GE Mgmt"
PID: ASA5545          , VID: V02          , SN: FTX1841119Z

Name: "power supply 0", DESCR: "ASA 5545-X/5555-X AC Power Supply"
PID: ASA-PWR-AC      , VID: N/A          , SN: 47K1E0

Name: "Storage Device 1", DESCR: "Model Number: Micron_M550_MTFDDAK128MAY"
PID: N/A             , VID: N/A          , SN: MXA183502EG

Name: "Storage Device 2", DESCR: "Model Number: Micron_M550_MTFDDAK128MAY"
PID: N/A             , VID: N/A          , SN: MXA183502FW

ciscoasa#
```

```
Cisco Systems ROMMON, Version 1.1.01, RELEASE SOFTWARE
Copyright (c) 1994-2014 by Cisco Systems, Inc.
Compiled Mon 10/20/2014 15:59:12.05 by builder
```

```
Current image running: Boot ROM0
Last reset cause: PowerCycleRequest
DIMM Slot 0 : Present

Platform ASA5506 with 4096 Mbytes of main memory
MAC Address: a4:6c:2a:e4:6b:bf
Using default Management Ethernet Port: 0
```

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

```
Located '.boot_string' @ cluster 1607965.
#
Attempt autoboot: "boot disk0:/asa961-50-lfbff-k8.spa"
Located 'asa961-50-lfbff-k8.spa' @ cluster 10.

#####
#####
#####
#####

LFBFF signature verified.
INIT: version 2.88 booting
Starting udev
Configuring network interfaces... done.
```

```
ciscoasa# show module
```

Mod	Card Type	Model	Serial No.
1	ASA 5506-X with FirePOWER services, 8GE, AC,	ASA5506	JAD191100HG
sfr	Unknown	N/A	JAD191100HG

Mod	MAC Address Range	Hw Version	Fw Version	Sw Version
1	a46c.2ae4.6bbf to a46c.2ae4.6bc8	1.0	1.1.1	9.6(1)50
sfr	a46c.2ae4.6bbe to a46c.2ae4.6bbe	N/A	N/A	

Mod	SSM Application Name	Status	SSM Application Version
-----	----------------------	--------	-------------------------

Mod	Status	Data Plane Status	Compatibility
1	Up Sys	Not Applicable	
sfr	Init	Not Applicable	

```
ciscoasa#
```

https://IP Address of Management Interface

! Run the following command on the CLI of the FXOS

```
Firepower-9300# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
CISCO Serial Over LAN:
Close Network Connection to Exit
Firepower-module1>
```

! Now, run the following command to connect to the CLI of the FTD:

```
Firepower-module1> connect ftd
Connecting to ftd console... enter exit to return to bootCLI
```

! The following network settings should auto-populate, if you configured them in the FTD provisioning page. In such case, no action necessary. Please be patient.

```
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]: manual
Enter an IPv4 address for the management interface [10.1.1.28]: 10.1.1.28
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.0
Enter the IPv4 default gateway for the management interface [10.1.1.1]: 10.1.1.1
Enter a fully qualified hostname for this system [Firepower-module1]: Firepower-module1
Enter a comma-separated list of DNS servers or 'none' [none]: none
Enter a comma-separated list of search domains or 'none' [none]: none
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Configure firewall mode? (routed/transparent) [routed]: routed
Configuring firewall mode ...
```

Update policy deployment information

- add device configuration
- add network discovery
- add system policy

You can register the sensor to a Firepower Management Center and use the Firepower Management Center to manage it. Note that registering the sensor to a Firepower Management Center disables on-sensor Firepower Services management capabilities.

When registering the sensor to a Firepower Management Center, a unique alphanumeric registration key is always required. In most cases, to register a sensor to a Firepower Management Center, you must provide the hostname or the IP address along with the registration key.

```
'configure manager add [hostname | ip address ] [registration key ]'
```

However, if the sensor and the Firepower Management Center are separated by a NAT device, you must enter a unique NAT ID, along with the unique registration key.

```
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'
```

Later, using the web interface on the Firepower Management Center, you must use the same registration key and, if necessary, the same NAT ID when you add this sensor to the Firepower Management Center.

>

! Assuming you are on the CLI of FXOS, first run the following command to connect to the Security Module (SM 1) where FTD software is installed.

```
Firepower-9300# connect module 1 console
```

```
Telnet escape character is '~'.
```

```
Trying 127.5.1.1...
```

```
Connected to 127.5.1.1.
```

```
Escape character is '~'.
```

```
CISCO Serial Over LAN:
```

```
Close Network Connection to Exit
```

```
Firepower-module1>
```

! Now, you are on the CLI of the Security Module 1 (SM 1). Run the following command to connect to the CLI of the FTD:

```
Firepower-module1> connect ftd
```

```
Connecting to ftd console... enter exit to return to bootCLI
```

```
>
```

! Now, you are on the CLI of the FTD software where you perform most of the FTD related tasks. If you want to ASA console, run the following command on the CLI of the FTD:

```
> system support diagnostic-cli
```

```
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
```

```
Type help or '?' for a list of available commands.
```

```
firepower>
```


! Now, you are on the CLI of the ASA software. Run the following command to access the privileged mode. Press the enter key when you are prompted for a password.

```
firepower> enable
```

```
Password:
```

```
firepower#
```

! To exit from the ASA console, press 'Ctrl+a then d' to detach.

```
firepower#
```

```
Console connection detached.
```

```
>
```

! You are now back to the CLI of FTD. To exit from the FTD CLI, run the following command:

```
> exit
```

```
Firepower-module1>
```

! You have now returned to the Service Module CLI. To exit, press the escape character '~', run the 'quit' command.

```
Firepower-module1> ~
```

```
telnet> quit
```

```
Connection closed.
```

```
Firepower-9300#
```

! You are now back to the CLI of the FXOS software.

```
Firepower-9300# scope chassis 1
```

```
Firepower-9300 /chassis # show sup version detail
```

```
SUP FIRMWARE:
```

```
  ROMMON:
```

```
    Running-Vers: 1.0.10
```

```
    Package-Vers: 1.0.10
```

```
    Activate-Status: Ready
```

```
    Upgrade Status: SUCCESS
```

```
  FPGA:
```

```
    Running-Vers: 1.05
```

```
    Package-Vers: 1.0.10
```

```
    Activate-Status: Ready
```

```
Firepower-9300 /chassis #
```

```
Firepower-9300# scope system
Firepower-9300 /system # show firmware monitor
FPRM:
  Package-Vers: 2.0(1.86)
  Upgrade-Status: Ready

Fabric Interconnect A:
  Package-Vers: 2.0(1.86)
  Upgrade-Status: Ready

Chassis 1:
  Server 1:
    Package-Vers: 2.0(1.86)
    Upgrade-Status: Ready
  Server 3:
    Package-Vers: 2.0(1.86),1.1(4.95)
    Upgrade-Status: Upgrading

Firepower-9300 /system #
```

```
Firepower-9300 /ssa # show logical-device

Logical Device:
  Name      Description Slot ID   Mode      Operational State  Template Name
  -----  -
  FTD_610           1      Standalone Ok      ftd

Firepower-9300 /ssa #
```

! The following output confirms that FTD application is being installed.

```
Firepower-9300# scope ssa
Firepower-9300 /ssa # show app-instance detail
```

```
Application Name: ftd
Slot ID: 1
Admin State: Disabled
Operational State: Installing
Running Version:
Startup Version: 6.1.0.330
Cluster Oper State: Not Applicable
Current Job Type: Install
Current Job Progress: 0
Current Job State: Queued
Clear Log Data: Available
Error Msg:
Hotfixes:
Externally Upgraded: No
```

```
Firepower-9300 /ssa #
```

! The following output proves that the FTD application is up and running.

```
Firepower-9300# scope ssa
Firepower-9300 /ssa # show app-instance detail
```

```
Application Name: ftd
Slot ID: 1
Admin State: Enabled
Operational State: Online
Running Version: 6.1.0.330
Startup Version: 6.1.0.330
Cluster Oper State: Not Applicable
Current Job Type: Start
Current Job Progress: 100
Current Job State: Succeeded
Clear Log Data: Available
Error Msg:
Hotfixes:
Externally Upgraded: No
```

```
Firepower-9300 /ssa #
```

```
Firepower-9300# show server status
```

Server	Slot	Status	Overall Status	Discovery
1/1	Equipped		Ok	Complete
1/2	Equipped		Degraded	Complete
1/3	Mismatch			

```
Firepower-9300#
```

```
Firepower-9300# show server environment
```

```
Server 1/1:
```

```
Overall Status: Ok  
Operability: Operable  
Oper Power: On
```

```
Server 1/2:
```

```
Overall Status: Degraded  
Operability: Inoperable  
Oper Power: On
```

```
Server 1/3:
```

```
Overall Status: Config  
Operability: Operable  
Oper Power: On
```

```
Firepower-9300#
```

```
Firepower-9300# show server adapter
```

```
Server 1/1:
```

Adapter	PID	Vendor	Serial	Overall Status
1	FPR-C9300-MP	Cisco Systems Inc	XXXXXXXXXXXX	Operable
2	FPR-C9300-MP-MEZZ	Cisco Systems Inc	XXXXXXXXXXXX	Operable

```
Server 1/3:
```

Adapter	PID	Vendor	Serial	Overall Status
1	FPR-C9300-MP	Cisco Systems Inc	XXXXXXXXXXXX	Operable
2	FPR-C9300-MP-MEZZ	Cisco Systems Inc	XXXXXXXXXXXX	Operable

```
Firepower-9300#
```

```
Firepower-9300# show fabric-interconnect environment
```

```
Fabric Interconnect A:
```

```
Operability: Operable
```

```
Fabric Card 1:
```

```
Threshold Status: N/A
```

```
Overall Status: Operable
```

```
Operability: Operable
```

```
Power State: Online
```

```
Thermal Status: N/A
```

```
Voltage Status: N/A
```

```
.  
.
```

```
<Output_Omitted>
```

```
Firepower-9300#
```

```
Firepower-4110# show chassis detail
```

```
Chassis:
```

```
Chassis: 1
```

```
User Label:
```

```
Overall Status: Operable
```

```
Oper qualifier: N/A
```

```
Operability: Operable
```

```
Conf State: Ok
```

```
Admin State: Acknowledged
```

```
Conn Path: A
```

```
Conn Status: A
```

```
Managing Instance: A
```

```
Product Name: Cisco Firepower 4110 Security Appliance
```

```
PID: FPR-4110-K9
```

```
VID: V00
```

```
Part Number: XX-XXXXXX-XX
```

```
Vendor: Cisco Systems Inc
```

```
Model: FPR-4110-K9
```

```
Serial (SN): XXXXXXXXXXXX
```

```
HW Revision: 0
```

```
Mfg Date: 2015-12-05T00:00:00.000
```

```
Power State: Ok
```

```
Thermal Status: Ok
```

```
EEPROM operability status: Operable
```

```
Dynamic Reallocation: Chassis
```

```
Reserved Power Budget (W): 600
```

```
PSU Capacity (W): 0
```

```
PSU Line Mode: Lower Line
```

```
PSU State: Ok
```

```
Current Task:
```

```
Firepower-4110#
```

```
Firepower-9300# show fault
```

Severity	Code	Last Transition Time	ID	Description
Critical	F999690	2016-11-19T16:36:09.980	15304334	[FSM:FAILED]: downloading image fxos-k9-fpr4k-firmware.1.0.10.SPA from (FSM:sam:dme:FirmwareDownloaderDownload)
Major	F0327	2016-11-16T18:14:00.622	15234559	Service profile ssp-sprof-2 configuration failed due to compute-unavailable,insufficient-resources
Warning	F0528	2016-08-05T19:17:42.663	44431	Power supply 1 in chassis 1 power: off

```
Firepower-9300#
```

```
Firepower-9300# show sel 1/1
```

```
1 | 12/22/2016 00:03:52 | CIMC | Drive slot(Bay) LED_BLADE_STATUS #0xa6 | Drive Presence | Asserted
2 | 12/22/2016 00:03:55 | CIMC | Voltage P2V63_VPP_EF #0x1c | Lower critical - going low | Asserted | Reading 2.48 <= Threshold 2.48 Volts
3 | 12/22/2016 00:03:55 | CIMC | Platform alert LED_SYS_ACT #0xa4 | LED color is amber | Asserted
4 | 12/22/2016 00:04:29 | BIOS | System Event #0x00 | Timestamp clock synch | SEL timestamp clock updated, event is first of pair | Asserted
5 | 12/22/2016 00:05:53 | BIOS | System Event #0x83 | OEM System Boot Event | | Asserted
6 | 12/22/2016 00:18:26 | CIMC | Entity presence MAIN_POWER_PRS #0x55 | Device Absent | Asserted
7 | 12/22/2016 00:37:15 | CIMC | Temperature GPU1_TEMP_SENS #0x59 | Upper Non-critical - going high | Asserted | Reading 136 >= Threshold 136 degrees C
8 | 12/22/2016 00:37:35 | CIMC | Temperature GPU1_TEMP_SENS #0x59 | Upper Non-critical - going high | Deasserted | Reading 134 <= Threshold 136 degrees C
.
.
<Output_Omitted>
```

```
Firepower-9300#
```

```
Firepower-9300# show fault
```

Severity	Code	Last Transition Time	ID	Description
Warning	F0528	2016-08-05T19:17:42.663	44431	Power supply 1 in chassis 1 power: off
Major	F0408	2016-08-05T19:17:42.662	44430	Power state on chassis 1 is redundancy-failed

```
Firepower-9300#
```

```
Firepower-9300# show chassis environment
```

```
Chassis 1:
```

```
Overall Status: Power Problem
```

```
Operability: Operable
```

```
Power State: Redundancy Failed
```

```
Thermal Status: Ok
```

```
Firepower-9300#
```

```
Firepower-9300# show sel 1/1 | egrep ignore-case power
```

```
1 | 12/13/2016 16:37:52 | CIMC | Entity presence MAIN_POWER_PRS #0x55 | Device  
Absent | Asserted
```

```
2 | 12/13/2016 16:39:23 | CIMC | Entity presence MAIN_POWER_PRS #0x55 | Device  
Present | Asserted
```

```
Firepower-9300#
```

```
Firepower-9300# show chassis psu detail
```

```
PSU:
```

```
PSU: 1
```

```
Overall Status: N/A
```

```
Operability: N/A
```

```
Threshold Status: N/A
```

```
Power State: Off
```

```
Presence: Equipped
```

```
Thermal Status: OK
```

```
Voltage Status: N/A
```

```
Product Name: Cisco Firepower 9000 Series AC Power Supply
```

```
PID: FPR9K-PS-AC
```

```
VID: V01
```

```
Part Number: 341-0723-01
```

```
Vendor: Cisco Systems Inc
```

```
Serial (SN): ART1918F298
```

```
HW Revision: 0
```

```
Firmware Version: N/A
```

```
Type: Unknown
```

```
Wattage (W): 0
```

```
Input Source: Unknown
```

```
PSU: 2
Overall Status: Operable
Operability: Operable
Threshold Status: OK
Power State: On
Presence: Equipped
Thermal Status: OK
Voltage Status: OK
Product Name: Cisco Firepower 9000 Series AC Power Supply
PID: FPR9K-PS-AC
VID: V01
Part Number: 341-0723-01
Vendor: Cisco Systems Inc
Serial (SN): ART1918F28X
HW Revision: 0
Firmware Version: N/A
Type: Unknown
Wattage (W): 2500
Input Source: Unknown
```

Firepower-9300#

```
Firepower-9300 /chassis # show fault
```

Severity	Code	Last Transition Time	ID	Description
Warning	F0377	2016-12-02T18:06:24.196	15575670	Fan module 1-2 in chassis 1 presence: missing
.				
.				

<Output_Omitted>

Firepower-9300 /chassis #

```
Firepower-9300 /chassis # show fan-module
```

Fan Module:

Tray	Module	Overall Status
1	1	Operable
1	2	Removed
1	3	Operable
1	4	Operable

Firepower-9300 /chassis #


```
Firepower-9300 /chassis # show fan-module detail
```

```
Fan Module:
```

```
Tray: 1
```

```
Module: 1
```

```
Overall Status: Operable
```

```
Operability: Operable
```

```
Threshold Status: OK
```

```
Power State: On
```

```
Presence: Equipped
```

```
Thermal Status: OK
```

```
Product Name: Cisco Firepower 9000 Series Fan
```

```
PID: FPR9K-FAN
```

```
VID: 01
```

```
Part Number: XX-XXXXX-XX
```

```
Vendor: Cisco Systems Inc
```

```
Serial (SN): XXXXXXXXXXXX
```

```
HW Revision: 0
```

```
Mfg Date: 2015-05-28T00:00:00.000
```

```
Tray: 1
```

```
Module: 2
```

```
Overall Status: Removed
```

```
Operability: N/A
```

```
Threshold Status: N/A
```

```
Power State: Off
```

```
Presence: Missing
```

```
Thermal Status: N/A
```

```
Product Name:
```

```
PID:
```

```
VID: 01
```

```
Part Number: XX-XXXXX-XX
```

```
Vendor:
```

```
Serial (SN):
```

```
HW Revision: 0
```

```
Mfg Date: 2015-05-28T00:00:00.000
```

```
.
```

```
.
```

```
<Output_Omitted>
```

```
Firepower-9300 /chassis #
```

```
admin@FMC4000:~$ sudo reboot
```

```
We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:
```

- #1) Respect the privacy of others.
- #2) Think before you type.
- #3) With great power comes great responsibility.

```
Password:
```

```
The system is going down for reboot NOW!
```

```
INIT: Switching to runlevel: 6
```

```
INIT: Sending processes the TERM signal
```

```
Stopping Sourcefire Defense Center 4000.....ok
```

```
.  
. .  
. .
```

```
<command output>
```

```
boot: System_Restore
```

```
Loading System_Restore
```

```
SYSLINUX 3.35 2007-01-28 EBIOS Copyright (C) 1994-2007 H. Peter Anvin
```

```
Welcome to the Sourcefire Linux Operating System
```

```
0. Load with standard console
```

```
1. Load with serial console
```

```
Please select a display mode to boot. If no option is selected after a timeout of 30 seconds, the default will be display mode 0 (Load with standard console). Press any key to cancel the timeout
```

```
boot: 0
```

```
Restore CD Sourcefire Fire Linux OS 6.1.0-37 x86_64
```

```
Sourcefire Defense Center S3 6.1.0-330
```

```
Checking Hardware
```

```
The USB device was successfully imaged. Reboot from the USB device to continue installation...
```

```
#####
```

```
#####
```

```
The system will restart after you press enter.
```

Restore CD Sourcefire Fire Linux OS 6.1.0-37 x86_64
Sourcefire Defense Center S3 6.1.0-330

Checking Hardware

####

This CD will restore your Defense Center S3
to its original factory state. All data will be destroyed
on the appliance.

Restore the system? (yes/no): **yes**

During the restore process, the license file and basic
network settings are preserved. These files can also be
reset to factory settings

Delete license and network settings? (yes/no): **no**

THIS IS YOUR FINAL WARNING. ANSWERING YES WILL REMOVE ALL FILES
FROM THIS DEFENSE CENTER S3.

Are you sure? (yes/no): **yes**

Restore CD Sourcefire Fire Linux OS 6.1.0-37 x86_64
Sourcefire Defense Center S3 6.1.0-330

(1) Preparing Disk

#####

(2) Installing System

####

```

<command output>
.
.
.
***** Attention *****

    Initializing the configuration database. Depending on available
    system resources (CPU, memory, and disk), this may take 30 minutes
    or more to complete.

***** Attention *****

Executing S09database-init                [ OK ]
Executing S10_001_install_symmetric.pl    [ OK ]
Executing S11database-populate            [ OK ]
<command output>
.
.
.
<command output>
Executing S50install-remediation-modules  [ OK ]
Executing S51install_health_policy.pl     [ OK ]
Executing S52install_system_policy.pl     [ OK ]
Executing S53change_reconciliation_baseline.pl [ OK ]
Executing S53createcsds.pl                [ OK ]
Executing S85patch_history-init            [ OK ]
Executing S90banner-init                  [ OK ]
Executing S95copy-crontab                 [ OK ]
Executing S96grow_var.sh                  [ OK ]
Executing S96install_sf_whitelist         [ OK ]
Executing S96install_vmware_tools.pl      [ OK ]

***** Attention *****

    Initializing the system's localization settings. Depending on available
    system resources (CPU, memory, and disk), this may take 10 minutes
    or more to complete.

***** Attention *****
Executing S96localize-templates            [ OK ]
Executing S96ovf-data.pl                  [ OK ]
Executing S97compress-client-resources    [ OK ]
Executing S97create_platinum_forms.pl     [ OK ]
.
.
.
<command output>

```

```
Cisco Firepower Management Center 4000 v6.1.0 (build 330)
Sep 28 23:20:53 firepower SF-IMS[5124]: [5124] init script:system [INFO] pmmon
  Starting the Process Manager...
Sep 28 23:20:53 firepower SF-IMS[5125]: [5125] pm:pm [INFO] Using model number 66F
sfpacket: module license 'Proprietary' taints kernel.
Disabling lock debugging due to kernel taint
Sourcefire Bridging Packet Driver - version 6.0.0
Copyright (c) 2004-2010 Sourcefire, Inc.
```

```
Cisco Firepower Management Center 4000 v6.1.0 (build 330)
Firepower login:admin
Password:Admin123
```

```
Copyright 2004-2016, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.
```

```
Cisco Fire Linux OS v6.1.0 (build 37)
Cisco Firepower Management Center 4000 v6.1.0 (build 330)
```

```
admin@FMC4000:~$
```

```
localhost:~@ ssh admin@10.1.1.10
admin@10.1.1.10's password:
CIMC#
```

```
CIMC# scope chassis
```

```
CIMC /chassis#
CIMC /chassis# set locator-led {on | off}
```

```
CIMC /chassis *#
CIMC /chassis *# commit
```

```
CIMC /chassis #
```

```
! Run the following commands to enable the locator LED
```

```
.
.
```

```
CIMC# scope chassis
CIMC /chassis# set locator-led on
CIMC /chassis *# commit
```

```
.
.
```

```
! Run the following commands to disable the locator LED
```

```
.
.
```

```
CIMC# scope chassis
CIMC /chassis# set locator-led off
CIMC /chassis *# commit
```

```
login as: admin
```

```
Password:
```

```
Copyright 2004-2016, Cisco and/or its affiliates. All rights reserved.
```

```
Cisco is a registered trademark of Cisco Systems, Inc.
```

```
All other trademarks are property of their respective owners.
```

```
Cisco Fire Linux OS v6.1.0 (build 37)
```

```
Cisco Firepower Management Center 4000 v6.1.0 (build 330)
```

```
admin@FMC4000:~$
```

```
admin@FMC4000:~$ sfcli.pl show version
```

```
Password:
```

```
-----[ FMC4000 ]-----
```

```
Model : Cisco Firepower Management Center 4000 (66) Version 6.1.0  
(Build 330)
```

```
UUID : 5bac032c-8bf5-11e6-a7c8-99be23cbc50d
```

```
Rules update version : 2016-10-05-001-vrt
```

```
VDB version : 270
```

```
-----
```

```
admin@FMC4000:~$
```

```
admin@FMC4000:~$ sudo MegaCLI -AdpBbuCmd -aAll | grep -i battery
```

```
BatteryType: CVPM02
```

```
Battery Pack Missing : No
```

```
Battery Replacement required : No
```

```
Battery backup charge time : 0 hours
```

```
Battery FRU: N/A
```

```
admin@FMC4000:~$
```

```
admin@FMC4000:~$ cat /var/sf/run/power.status
```

```
PS1: 0x08: Power Supply input lost
```

```
PS2: 0x01: Presence detected
```

```
admin@FMC4000:~$
```

```
admin@FMC4000:~$ sudo ipmitool sel list | grep -i power
```

```
2cf | 10/12/2016 | 18:42:33 | Power Supply #0x26 | Power Supply AC lost | Asserted
2d0 | 10/12/2016 | 18:42:33 | Power Supply #0x3a | Redundancy Degraded | Asserted
2da | 10/12/2016 | 18:43:58 | Power Supply #0x3a | Non-Redundant: Sufficient from
Redundant | Asserted
```

```
admin@FMC4000:~$
```

```
admin@FMC4000:~$ sudo ipmitool sdr | egrep -i "power|ps"
```

```
MAIN_POWER_PRS | 0x00 | ok
POWER_ON_FAIL | 0x00 | ok
PSU1_STATUS | 0x00 | ok
PSU2_STATUS | 0x00 | ok
PSU1_PWRGD | 0x00 | ok
PSU1_AC_OK | 0x00 | ok
PSU2_PWRGD | 0x00 | ok
PSU2_AC_OK | 0x00 | ok
LED_PSU_STATUS | 0x00 | ok
PS_RDNDNT_MODE | 0x00 | ok
POWER_USAGE | 128 Watts | ok
PSU1_VOUT | 0 Volts | ok
PSU1_IOUT | 0 Amps | ok
PSU1_POUT | 0 Watts | ok
PSU2_VOUT | 12 Volts | ok
PSU2_IOUT | 9 Amps | ok
PSU2_POUT | 112 Watts | ok
PSU1_PIN | 0 Watts | ok
PSU2_PIN | 128 Watts | ok
PSU1_TEMP | 30 degrees C | ok
PSU2_TEMP | 32 degrees C | ok
```

```
admin@FMC4000:~$
```

```
admin@FMC2000:~$ cat /var/sf/run/fans.status
```

```
$fan_status = {  
    FAN11_name => 'FAN1_TACH1',  
    FAN11_alertlevel => 'Green',  
    FAN11_unit => 'RPM',  
    FAN11_value => '3200',  
    FAN12_name => 'FAN1_TACH2',  
    FAN12_alertlevel => 'Green',  
    FAN12_unit => 'RPM',  
    FAN12_value => '3200',  
    FAN21_name => 'FAN2_TACH1',  
    FAN21_alertlevel => 'Green',  
    FAN21_unit => 'RPM',  
    FAN21_value => '3200',  
    FAN22_name => 'FAN2_TACH2',  
    FAN22_alertlevel => 'Green',  
    FAN22_unit => 'RPM',  
    FAN22_value => '3200',  
    FAN31_name => 'FAN3_TACH1',  
    FAN31_alertlevel => 'Green',  
    FAN31_unit => 'RPM',  
    FAN31_value => '3200',  
    FAN32_name => 'FAN3_TACH2',  
    FAN32_alertlevel => 'Green',  
    FAN32_unit => 'RPM',  
    FAN32_value => '3200',  
    FAN41_name => 'FAN4_TACH1',  
    FAN41_alertlevel => 'Green',  
    FAN41_unit => 'RPM',  
    FAN41_value => '3200',  
  
    FAN42_name => 'FAN4_TACH2',  
    FAN42_alertlevel => 'Green',  
    FAN42_unit => 'RPM',  
    FAN42_value => '3200',  
    FAN51_name => 'FAN5_TACH1',  
    FAN51_alertlevel => 'Green',  
    FAN51_unit => 'RPM',  
    FAN51_value => '3200',  
    FAN52_name => 'FAN5_TACH2',  
    FAN52_alertlevel => 'Green',  
    FAN52_unit => 'RPM',  
    FAN52_value => '3200',  
};  
admin@FMC2000:~$
```



```
admin@FMC2000:~$ grep -i alert /var/sf/run/fans.status
```

```
FAN11_alertlevel => 'Green',  
FAN12_alertlevel => 'Green',  
FAN21_alertlevel => 'Green',  
FAN22_alertlevel => 'Green',  
FAN31_alertlevel => 'Green',  
FAN32_alertlevel => 'Green',  
FAN41_alertlevel => 'Green',  
FAN42_alertlevel => 'Green',  
FAN51_alertlevel => 'Green',  
FAN52_alertlevel => 'Green',
```

```
admin@FMC2000:~$
```

```
admin@FMC2000:~$ sudo ipmitool sdr list | grep -i fan | grep -i tach
```

FAN1_TACH1	7490 RPM	ok
FAN1_TACH2	7062 RPM	ok
FAN2_TACH1	7704 RPM	ok
FAN2_TACH2	7276 RPM	ok
FAN3_TACH1	7704 RPM	ok
FAN3_TACH2	7276 RPM	ok
FAN4_TACH1	7704 RPM	ok
FAN4_TACH2	7062 RPM	ok
FAN5_TACH1	7704 RPM	ok
FAN5_TACH2	7062 RPM	ok

```
admin@FMC2000:~$
```

Cisco Firepower Management Center for VMWare v6.1.0 (build 330)

Oct 18 13:20:23 firepower SF-IMS[616]: [616] init script:system [INFO] pmmon
Starting the Process Manager...

Oct 18 13:20:23 firepower SF-IMS[617]: [617] pm:pm [INFO] Using model number
66ESad7: WRITE SAME failed. Manually zeroing.

Cisco Firepower Management Center for VMWare v6.1.0 (build 330)

Firepower login:**admin**

Password:**Admin123**

Copyright 2004-2016, Cisco and/or its affiliates. All rights reserved.

Cisco is a registered trademark of Cisco Systems, Inc.

All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.1.0 (build 37)

Cisco Firepower Management Center for VMWare v6.1.0 (build 330)

admin@firepower:~\$

Cisco Firepower Threat Defense for VMWare v6.1.0 (build 330)

Firepower login:admin

Password:Admin123

You must accept the EULA to continue.

Press <ENTER> to display the EULA:

.
.

Output Omitted

.
.

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress. Please stand by.

You must change the password for 'admin' to continue.

Enter new password:

Confirm new password:

You must configure the network to continue.

You must configure at least one of IPv4 or IPv6.

Do you want to configure IPv4? (y/n) [y]:

Do you want to configure IPv6? (y/n) [n]:

Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:

Enter an IPv4 address for the management interface [192.168.45.45]: 10.1.1.21

Enter an IPv4 netmask for the management interface [255.255.255.0]:

Enter the IPv4 default gateway for the management interface [192.168.45.1]: 10.1.1.1

Enter a fully qualified hostname for this system [firepower]:

Enter a comma-separated list of DNS servers or 'none' []: none

Enter a comma-separated list of search domains or 'none' []: none

If your networking information has changed, you will need to reconnect.

For HTTP Proxy configuration, run 'configure network http-proxy'

Configure firewall mode? (routed/transparent) [routed]:

Configuring firewall mode ...

Update policy deployment information

- add device configuration
- add network discovery
- add system policy

You can register the sensor to a Firepower Management Center and use the Firepower Management Center to manage it. Note that registering the sensor to a Firepower Management Center disables on-sensor Firepower Services management capabilities.

When registering the sensor to a Firepower Management Center, a unique alphanumeric registration key is always required. In most cases, to register a sensor to a Firepower Management Center, you must provide the hostname or the IP address along with the registration key.

```
'configure manager add [hostname | ip address ] [registration key ]'
```

However, if the sensor and the Firepower Management Center are separated by a NAT device, you must enter a unique NAT ID, along with the unique registration key.

```
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'
```

Later, using the web interface on the Firepower Management Center, you must use the same registration key and, if necessary, the same NAT ID when you add this sensor to the Firepower Management Center.

>

```
admin@firepower:~$ sudo configure-network
```

```
We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:
```

- #1) Respect the privacy of others.
- #2) Think before you type.
- #3) With great power comes great responsibility.

```
Password:
```

```
Do you wish to configure IPv4? (y or n) y
```

```
Management IP address? [192.168.45.45] 10.1.1.16
```

```
Management netmask? [255.255.255.0]
```

```
Management default gateway? 10.1.1.1
```

```
Management IP address?          10.1.1.16
```

```
Management netmask?             255.255.255.0
```

```
Management default gateway?     10.1.1.1
```

```
Are these settings correct? (y or n) y
```

```
Do you wish to configure IPv6? (y or n) n
```

```
Updated network configuration.
```

```
Updated comms. channel configuration.
```

```
Please go to https://10.1.1.16/ or https://\[\]/ to finish installation.
```

```
admin@firepower:~$
```

```
admin@FMC:~$ sudo ping 10.1.1.2
```

```
Password:
```

```
PING 10.1.1.2 (10.1.1.2) 56(84) bytes of data.
```

```
64 bytes from 10.1.1.2: icmp_req=1 ttl=64 time=0.615 ms
```

```
64 bytes from 10.1.1.2: icmp_req=2 ttl=64 time=0.419 ms
```

```
64 bytes from 10.1.1.2: icmp_req=3 ttl=64 time=0.536 ms
```

```
64 bytes from 10.1.1.2: icmp_req=4 ttl=64 time=0.613 ms
```

```
^C
```

```
--- 10.1.1.2 ping statistics ---
```

```
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
```

```
rtt min/avg/max/mdev = 0.419/0.545/0.615/0.084 ms
```

```
admin@FMC:~$
```

```
admin@FMC:~$ route -n
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use Iface
0.0.0.0          10.1.1.1        0.0.0.0         UG    0      0      0 eth0
10.1.1.0         0.0.0.0         255.255.255.0   U      0      0      0 eth0
admin@FMC:~$
```

admin@FMC:~\$ **sudo traceroute IP Address of FTD**

```
admin@FMC:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:ED:37:B1
          inet addr:10.1.1.16 Bcast:10.1.1.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feed:37b1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2190 errors:0 dropped:0 overruns:0 frame:0
          TX packets:197 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:150210 (146.6 Kb)  TX bytes:25196 (24.6 Kb)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.255.255.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:9789370 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9789370 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2482195842 (2367.2 Mb)  TX bytes:2482195842 (2367.2 Mb)

admin@FMC:~$
```

> **configure network ipv4 manual IP Address Subnet Mask Gateway Address**

```
> configure network ipv4 manual 10.1.1.2 255.255.255.0 10.1.1.1
Setting IPv4 network configuration.
Network settings changed.
>
```

```
> show network
===== [ System Information ] =====
Hostname                : firepower
Management port        : 8305
IPv4 Default route
  Gateway               : 10.1.1.1

===== [ br1 ] =====
State                   : Enabled
Channels                : Management & Events
Mode                   : Non-Autonegotiation
MDI/MDIX               : Auto/MDIX
MTU                    : 1500
MAC Address            : A4:6C:2A:E4:6B:BE
----- [ IPv4 ] -----
Configuration          : Manual
Address                : 10.1.1.2
Netmask                : 255.255.255.0
Broadcast              : 10.1.1.255
----- [ IPv6 ] -----
Configuration          : Disabled

===== [ Proxy Information ] =====
State                  : Disabled
Authentication         : Disabled

>
```

```
> show interface ip brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Virtual0	127.1.0.1	YES	unset	up	up
GigabitEthernet1/1	unassigned	YES	unset	administratively down	down
GigabitEthernet1/2	unassigned	YES	unset	administratively down	down
GigabitEthernet1/3	unassigned	YES	unset	administratively down	down
GigabitEthernet1/4	unassigned	YES	unset	administratively down	down
GigabitEthernet1/5	unassigned	YES	unset	administratively down	down
GigabitEthernet1/6	unassigned	YES	unset	administratively down	down
GigabitEthernet1/7	unassigned	YES	unset	administratively down	down
GigabitEthernet1/8	unassigned	YES	unset	administratively down	down
Internal-Controll1/1	127.0.1.1	YES	unset	up	up
Internal-Data1/1	unassigned	YES	unset	up	up
Internal-Data1/2	unassigned	YES	unset	down	down
Internal-Data1/3	unassigned	YES	unset	up	up
Internal-Data1/4	169.254.1.1	YES	unset	up	up
Management1/1	unassigned	YES	unset	up	up

```
>
```

```
> ping system 10.1.1.16
```

```
PING 10.1.1.16 (10.1.1.16) 56(84) bytes of data.  
64 bytes from 10.1.1.16: icmp_seq=1 ttl=64 time=0.593 ms  
64 bytes from 10.1.1.16: icmp_seq=2 ttl=64 time=0.654 ms  
64 bytes from 10.1.1.16: icmp_seq=3 ttl=64 time=0.663 ms  
64 bytes from 10.1.1.16: icmp_seq=4 ttl=64 time=0.699 ms  
^C  
--- 10.1.1.16 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 2999ms  
rtt min/avg/max/mdev = 0.593/0.652/0.699/0.042 ms  
>
```

```
> system support diagnostic-cli
```

```
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
```

```
Type help or '?' for a list of available commands.
```

```
firepower> enable
```

```
Password:
```

```
firepower# ping 10.1.1.16
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.1.1.16, timeout is 2 seconds:
```

```
No route to host 10.1.1.16
```

```
Success rate is 0 percent (0/1)
```

```
firepower#
```



```
Firepower-9300# scope fabric-interconnect a
Firepower-9300 /fabric-interconnect # set out-of-band ip 10.1.1.28 netmask
255.255.255.0 gw 10.1.1.1
Warning: When committed, this change may disconnect the current CLI session
Firepower-9300 /fabric-interconnect* #
```

! The above command does not take an effect until you run the following command and commit the changes.

```
Firepower-9300 /fabric-interconnect* # commit-buffer
Firepower-9300 /fabric-interconnect #
```

! If you misconfigured or do not want to apply a recent change, you could discard it from the buffer as well. To discard, run the following command.

```
Firepower-9300 /fabric-interconnect* # discard-buffer
Firepower-9300 /fabric-interconnect #
```

```
Firepower-9300# connect local-mgmt
Firepower-9300(local-mgmt)# ping 10.1.1.1
PING 10.1.1.1 (10.1.1.1) from 10.1.1.28 eth0: 56(84) bytes of data.
64 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=0.298 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=255 time=0.412 ms
64 bytes from 10.1.1.1: icmp_seq=3 ttl=255 time=0.392 ms
64 bytes from 10.1.1.1: icmp_seq=4 ttl=255 time=0.390 ms
^C
--- 10.1.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 0.298/0.373/0.412/0.044 ms
Firepower-9300(local-mgmt)#
```

```
Firepower-9300# connect local-mgmt
Firepower-9300(local-mgmt)# show mgmt-port
eth0      Link encap:Ethernet  HWaddr B0:AA:77:2F:84:71
          inet addr:10.1.1.28  Bcast:10.122.144.255  Mask:255.255.255.0
          inet6 addr: fe80::b2aa:77ff:fe2f:8471/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4980815 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2680187 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1124575588 (1.0 GiB)  TX bytes:1921268851 (1.7 GiB)
Firepower-9300(local-mgmt)#
```

```
Firepower-9300# show fabric-interconnect
```

```
Fabric Interconnect:
```

```
ID  OOB IP Addr  OOB Gateway  OOB Netmask  OOB IPv6 Address  OOB IPv6 Gateway  
Prefix Operability  
--  -----  
A  10.1.1.28    10.1.1.1     255.255.255.0  ::              ::              64  
Operable  
Firepower-9300#
```

```
Firepower-9300# scope ssa
```

```
Firepower-9300 /ssa # show configuration
```

```
scope ssa  
  enter logical-device FTD_61 ftd 1 standalone  
    enter external-port-link Ethernet11_ftd Ethernet1/1 ftd  
      set decorator ""  
      set description ""  
      set port-name Ethernet1/1  
    exit  
    enter external-port-link Ethernet23_ftd Ethernet2/3 ftd  
      set decorator ""  
      set description ""  
      set port-name Ethernet2/3  
    exit  
    enter external-port-link Ethernet24_ftd Ethernet2/4 ftd  
      set decorator ""  
      set description ""  
      set port-name Ethernet2/4  
    exit  
    enter mgmt-bootstrap ftd  
      enter ipv4 1 firepower  
        set gateway 10.1.1.1  
        set ip 10.1.1.28 mask 255.255.255.0  
      exit  
    exit  
    set description ""  
    set res-profile-name ""  
  exit
```

```
.  
. .  
. .
```

```
<Output Omitted>
```

```
Firepower-9300 /ssa #
```

```

Firepower-9300# scope eth-uplink
Firepower-9300 /eth-uplink # scope fabric a
Firepower-9300 /eth-uplink/fabric # show interface

```

Interface:

Port Name	Port Type	Admin State	Oper State	State Reason
Ethernet1/1	Mgmt	Enabled	Up	
Ethernet1/2	Data	Disabled	Sfp Not Present	Unknown
Ethernet1/3	Data	Disabled	Sfp Not Present	Unknown
Ethernet1/4	Data	Disabled	Sfp Not Present	Unknown
Ethernet1/5	Data	Disabled	Sfp Not Present	Unknown
Ethernet1/6	Data	Disabled	Sfp Not Present	Unknown
Ethernet1/7	Data	Disabled	Sfp Not Present	Unknown
Ethernet1/8	Data	Disabled	Sfp Not Present	Unknown
Ethernet2/3	Data	Enabled	Up	
Ethernet2/4	Data	Enabled	Up	
Ethernet2/5	Data	Disabled	Sfp Not Present	Unknown
Ethernet2/6	Data	Disabled	Sfp Not Present	Unknown
Ethernet2/7	Data	Disabled	Sfp Not Present	Unknown
Ethernet2/8	Data	Disabled	Sfp Not Present	Unknown
Ethernet3/1	Data	Disabled	Sfp Not Present	Unknown
Ethernet3/2	Data	Disabled	Sfp Not Present	Unknown
Ethernet3/3	Data	Disabled	Sfp Not Present	Unknown
Ethernet3/4	Data	Disabled	Sfp Not Present	Unknown
Ethernet3/5	Data	Disabled	Sfp Not Present	Unknown
Ethernet3/6	Data	Disabled	Sfp Not Present	Unknown
Ethernet3/7	Data	Disabled	Sfp Not Present	Unknown
Ethernet3/8	Data	Disabled	Sfp Not Present	Unknown

```

Firepower-9300 /eth-uplink/fabric #

```

```

Firepower-9300# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1> connect ftd
Connecting to ftd console... enter exit to return to bootCLI

> show network
===== [ System Information ] =====
Hostname                : Firepower-module1
Management port         : 8305

IPv4 Default route
  Gateway                : 10.1.1.1

===== [ management0 ] =====
State                   : Enabled
Channels                : Management & Events
Mode                   : Non-Autonegotiation
MDI/MDIX               : Auto/MDIX
MTU                    : 9210
MAC Address             : B0:AA:77:2F:84:5D

----- [ IPv4 ] -----
Configuration          : Manual
Address                : 10.1.1.28
Netmask                : 255.255.255.0
Broadcast              : 10.1.1.255

----- [ IPv6 ] -----
Configuration          : Disabled

===== [ Proxy Information ] =====
State                   : Disabled
Authentication         : Disabled

>

```

```
admin@FMC:~$ sudo tail -f /var/log/sam.log
```

```
Password:
```

```
[timestamp] PID : 12133 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:  
registerIdToken start: token(NGJmZThZjItZjVknZC00TcyLWI5MTAAAtNGRhMzExZDM5MzVmLTE0O  
DY1NjMZZ%0AOD1MMDN8RmZweWJ5eG9Z0c...)  
[timestamp] PID : 12133 Process : ActionQueueScrape.pl [SAM-DBG-LOG]: [socket conn]  
compose msg header: type[7], len[147], seq[1]  
[timestamp] PID : 12133 Process : ActionQueueScrape.pl [SAM-DBG-LOG]: [socket conn]  
establishConnection start  
[timestamp] PID : 12133 Process : ActionQueueScrape.pl [SAM-DBG-LOG]: [socket conn]  
Connected to server  
[timestamp] PID : 12133 Process : ActionQueueScrape.pl [SAM-DBG-LOG]: [socket conn]  
'/var/sf/run/smart_agent.sock' Exiting the loop  
[timestamp] PID : 12133 Process : ActionQueueScrape.pl [SAM-DBG-LOG]: [socket conn]  
Connection successful!  
[timestamp] PID : 12133 Process : ActionQueueScrape.pl [SAM-DBG-LOG]: [socket conn]  
initSequence: 3  
[timestamp] PID : 12133 Process : ActionQueueScrape.pl [SAM-DBG-LOG]: [socket conn]  
establishConnection done  
[timestamp] PID : 12133 Process : ActionQueueScrape.pl [SAM-DBG-LOG]: [socket conn]  
sendMsg: successfully sent the msg!  
[timestamp] PID : 12133 Process : ActionQueueScrape.pl [SAM-DBG-LOG]: [socket conn]  
recvMsg get: type[1007], len[141], seq[0], msg[error:0 authorization:AUTHORIZED,  
1483970615 registration:REGISTERED,1483970610 virtual_acct:Firepower Threat  
Defense export_control:1]
```

```

[timestamp] PID : 463 Process : mojo_server.pl [SAM-DBG-LOG]: [socket conn] Closing
Connection
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
registerIdToken start: token(NGJmZThhZjItZjVkZCooyTcyLWI5MTAtNGRhMzExZDM5MzVmLTE0O
DY1NjMz%0AODk1MDN8RmZweWJ5eG9ZY)
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]: [socket conn]
compose msg header: type[7], len[147], seq[1]
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]: [socket conn]
establishConnection start
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]: [socket conn]
Connected to server
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]: [socket conn]
'/var/sf/run/smart_agent.sock' Exiting the loop
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]: [socket conn]
Connection successful!
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]: [socket conn]
initSequence: 9
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]: [socket conn]
establishConnection done
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]: [socket conn]
sendMsg: successfully sent the msg!
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]: [socket conn]
recvMsg get: type[1003], len [203], seq[0], msg[Response error: {"token":
["The token 'NGJmZThhZjItZjVkZCooyTcyLWI5MTAtNGRhMzExZDM5MzVmLTE0ODY1NjMz%0AODk-
1MDN8RmZweWJ5eG9ZY is not valid."]}]
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]: [socket conn]
Closing Connection
[timestamp] PID : 13540 Process : ActionQueueScrape.pl [SAM-DBG-LOG]:
registerIdToken return: $VAR1 = {
    'error' => 17
};

```

```
> show managers
```

```
No managers configured.
```

```
>
```

```
> configure manager add IP Address of FMC Registration Key NAT ID
```

```
> configure manager add 10.1.1.16 RegKey NatId
```

```
Manager successfully configured.
```

```
Please make note of reg_key as this will be required while adding Device in FMC.
```

```
>
```

```
> show managers
```

```
Host : 10.1.1.16
```

```
Registration Key : ****
```

```
Registration : pending
```

```
RPC Status :
```

```
>
```

! Registration status: After you complete the **first step** (Add an FMC on FTD CLI)

```
> show managers
```

```
Host                : 10.1.1.16
Registration Key     : ****
Registration         : pending
RPC Status          :
```

```
>
```

! Registration status: After you complete the **second and final step** (Add an FTD on FMC GUI)

```
> show managers
```

```
Type                : Manager
Host                : 10.1.1.16
Registration         : Completed
```

```
>
```

! First, on the CLI of an FTD, when you enter the FMC detail, it opens the TCP port 8305 on FTD.

```
admin@FTD:~$ sudo netstat -antp | grep -i 8305
```

```
tcp        0      0 10.1.1.2:8305          0.0.0.0:*          LISTEN
    933/sftunnel
```

```
admin@FTD:~$
```

! Then, on the GUI of an FMC, when you enter the FTD detail, the FMC begins listening on TCP port 8305. FMC responses the FTD's registration request from a random port 49707.

```
admin@FMC:~$ sudo netstat -antp | grep -i 8305
```

```
tcp        0      0 10.1.1.16:8305        0.0.0.0:*          LISTEN
    10095/sftunnel
tcp        0      0 10.1.1.16:49707      10.1.1.2:8305     ESTABLISHED
    10095/sftunnel
```

```
root@FMC:~#
```

! Upon a successful registration, the connections appear fully established on the FMC.

```
admin@FMC:~$ sudo netstat -antp | grep -i 8305
```

```
tcp        0      0 10.1.1.16:49707      10.1.1.2:8305     ESTABLISHED
    10095/sftunnel
tcp        0      0 10.1.1.16:8305       10.1.1.2:54998    ESTABLISHED
    10095/sftunnel
```

```
admin@FMC:~$
```

! Capturing Packets on the FTD Management Interface

> capture-traffic

Please choose domain to capture traffic from:

0 - br1

Selection? 0

Please specify tcpdump options desired.

(or enter '?' for a list of supported options)

Options: host 10.1.1.16

HS_PACKET_BUFFER_SIZE is set to 4.

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on br1, link-type EN10MB (Ethernet), capture size 96 bytes

[timestamp] IP FTD.46373 > 10.1.1.16.8305: Flags [S], seq 1709676008, win 14600, options [mss 1460,sackOK,TS val 87180 ecr 0,nop,wscale 7], length 0

[timestamp] IP 10.1.1.16.8305 > FTD.46373: Flags [R.], seq 0, ack 1709676009, win 0, length 0

[timestamp] IP FTD.58441 > 10.1.1.16.8305: Flags [S], seq 3021847438, win 14600, options [mss 1460,sackOK,TS val 87380 ecr 0,nop,wscale 7], length 0

[timestamp] IP 10.1.1.16.8305 > FTD.58441: Flags [R.], seq 0, ack 3021847439, win 0, length 0

[timestamp] IP FTD.46814 > 10.1.1.16.8305: Flags [S], seq 1334198689, win 14600, options [mss 1460,sackOK,TS val 88317 ecr 0,nop,wscale 7], length 0

[timestamp] IP 10.1.1.16.8305 > FTD.46814: Flags [R.], seq 0, ack 1334198690, win 0, length 0

[timestamp] IP FTD.45854 > 10.1.1.16.8305: Flags [S], seq 1274367969, win 14600, options [mss 1460,sackOK,TS val 88517 ecr 0,nop,wscale 7], length 0

[timestamp] IP 10.1.1.16.8305 > FTD.45854: Flags [R.], seq 0, ack 1274367970, win 0, length 0


```
.  
<Output Omitted>
```

! Capturing Packets on the FMC Management Interface

```
admin@FMC:~$ sudo tcpdump -i eth0 host 10.1.1.2
```

```
Password:
```

```
HS_PACKET_BUFFER_SIZE is set to 4.
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
```

```
[timestamp] IP 10.1.1.2.46373 > FMC.8305: Flags [S], seq 1709676008, win 14600,  
options [mss 1460,sackOK,TS val 87180 ecr 0,nop,wscale 7], length 0  
[timestamp] IP FMC.8305 > 10.1.1.2.46373: Flags [R.], seq 0, ack 1709676009, win 0,  
length 0  
[timestamp] IP 10.1.1.2.58441 > FMC.8305: Flags [S], seq 3021847438, win 14600,  
options [mss 1460,sackOK,TS val 87380 ecr 0,nop,wscale 7], length 0  
[timestamp] IP FMC.8305 > 10.1.1.2.58441: Flags [R.], seq 0, ack 3021847439, win 0,  
length 0  
[timestamp] IP 10.1.1.2.46814 > FMC.8305: Flags [S], seq 1334198689, win 14600,  
options [mss 1460,sackOK,TS val 88317 ecr 0,nop,wscale 7], length 0  
[timestamp] IP FMC.8305 > 10.1.1.2.46814: Flags [R.], seq 0, ack 1334198690, win 0,  
length 0  
[timestamp] IP 10.1.1.2.45854 > FMC.8305: Flags [S], seq 1274367969, win 14600,  
options [mss 1460,sackOK,TS val 88517 ecr 0,nop,wscale 7], length 0  
[timestamp] IP FMC.8305 > 10.1.1.2.45854: Flags [R.], seq 0, ack 1274367970, win 0,  
length 0
```

```
.
```

```
.
```

```
<Output Omitted>
```

! On the FMC Interface

.

<Output Omitted>

.

[timestamp] IP FMC.51509 > 10.1.1.2.8305: Flags [S], seq 1804119299, win 14600, options [mss 1460,sackOK,TS val 258976 ecr 0,nop,wscale 7], length 0

[timestamp] IP 10.1.1.2.8305 > FMC.51509: Flags [S.], seq 4103916511, ack 1804119300, win 14480, options [mss 1460,sackOK,TS val 93418 ecr 258976,nop,wscale 7], length 0

[timestamp] IP FMC.51509 > 10.1.1.2.8305: Flags [.] , ack 1, win 115, options [nop,nop,TS val 258976 ecr 93418], length 0

[timestamp] IP FMC.51509 > 10.1.1.2.8305: Flags [P.] , ack 1, win 115, options [nop,nop,TS val 258985 ecr 93418], length 247

[timestamp] IP 10.1.1.2.8305 > FMC.51509: Flags [.] , ack 248, win 122, options [nop,nop,TS val 93422 ecr 258985], length 0

[timestamp] IP 10.1.1.2.8305 > FMC.51509: Flags [.] , ack 248, win 122, options [nop,nop,TS val 93423 ecr 258985], length 1448

[timestamp] IP 10.1.1.2.8305 > FMC.51509: Flags [P.] , ack 248, win 122, options [nop,nop,TS val 93423 ecr 258985], length 774

.

<Output Omitted>

.

! Press the Control+C keys to exit and stop capturing.

```
! On the FTD Interface
```

```
.
```

```
<Output Omitted>
```

```
.
```

```
[timestamp] IP 10.1.1.16.51509 > FTD.8305: Flags [S], seq 1804119299, win 14600, options [mss 1460,sackOK,TS val 258976 ecr 0,nop,wscale 7], length 0
```

```
[timestamp] IP FTD.8305 > 10.1.1.16.51509: Flags [S.], seq 4103916511, ack 1804119300, win 14480, options [mss 1460,sackOK,TS val 93418 ecr 258976,nop,wscale 7], length 0
```

```
[timestamp] IP 10.1.1.16.51509 > FTD.8305: Flags [.] , ack 1, win 115, options [nop,nop,TS val 258976 ecr 93418], length 0
```

```
[timestamp] IP 10.1.1.16.51509 > FTD.8305: Flags [P.] , ack 1, win 115, options [nop,nop,TS val 258985 ecr 93418], length 247
```

```
[timestamp] IP FTD.8305 > 10.1.1.16.51509: Flags [.] , ack 248, win 122, options [nop,nop,TS val 93422 ecr 258985], length 0
```

```
[timestamp] IP FTD.8305 > 10.1.1.16.51509: Flags [.] , ack 248, win 122, options [nop,nop,TS val 93423 ecr 258985], length 1448
```

```
[timestamp] IP FTD.8305 > 10.1.1.16.51509: Flags [P.] , ack 248, win 122, options [nop,nop,TS val 93423 ecr 258985], length 774
```

```
.
```

```
<Output Omitted>
```

```
.
```

```
! Press the Control+C keys to exit and stop capturing.
```

```
admin@FMC:~$ telnet 10.1.1.2 8305
```

```
Trying 10.1.1.2...
```

```
Connected to 10.1.1.2.
```

```
Escape character is '^]'.
```

```
^] ! Press the Ctrl and ] keys together
```

```
telnet> quit
```

```
Connection closed.
```

```
admin@fmc:~$
```

```
> sftunnel-status
```

```
SFTUNNEL Start Time: Sun Dec 11 23:51:56 2016
```

```
Both IPv4 and IPv6 connectivity is supported
```

```
Broadcast count = 2
```

```
Reserved SSL connections: 0
```

```
Management Interfaces: 1
```

```
br1 (control events) 10.1.1.2,
```

```
*****
```

```
**RUN STATUS**10.1.1.16*****
```

```
Cipher used = AES256-GCM-SHA384 (strength:256 bits)
```

```
ChannelA Connected: Yes, Interface br1
```

```
Cipher used = AES256-GCM-SHA384 (strength:256 bits)
```

```
ChannelB Connected: Yes, Interface br1
```

```
Registration: Completed.
```

```
IPv4 Connection to peer '10.1.1.16' Start Time: Mon Dec 12 00:13:44 2016
```

```
PEER INFO:
```

```
sw_version 6.1.0
```

```
sw_build 330
```

```
Management Interfaces: 1
```

```
eth0 (control events) 10.1.1.16,
```

```
Peer channel Channel-A is valid type (CONTROL), using 'br1', connected  
to '10.1.1.16' via '10.1.1.2'
```

```
Peer channel Channel-B is valid type (EVENT), using 'br1', connected to  
'10.1.1.16' via '10.1.1.2'
```

TOTAL TRANSMITTED MESSAGES <24> for Health Events service
RECEIVED MESSAGES <12> for Health Events service
SEND MESSAGES <12> for Health Events service
HALT REQUEST SEND COUNTER <0> for Health Events service
STORED MESSAGES for Health service (service 0/peer 0)
STATE <Process messages> for Health Events service
REQUESTED FOR REMOTE <Process messages> for Health Events service
REQUESTED FROM REMOTE <Process messages> for Health Events service

TOTAL TRANSMITTED MESSAGES <3> for Identity service
RECEIVED MESSAGES <2> for Identity service
SEND MESSAGES <1> for Identity service
HALT REQUEST SEND COUNTER <0> for Identity service
STORED MESSAGES for Identity service (service 0/peer 0)
STATE <Process messages> for Identity service
REQUESTED FOR REMOTE <Process messages> for Identity service
REQUESTED FROM REMOTE <Process messages> for Identity service

TOTAL TRANSMITTED MESSAGES <76> for RPC service
RECEIVED MESSAGES <38> for RPC service
SEND MESSAGES <38> for RPC service
HALT REQUEST SEND COUNTER <0> for RPC service
STORED MESSAGES for RPC service (service 0/peer 0)
STATE <Process messages> for RPC service
REQUESTED FOR REMOTE <Process messages> for RPC service
REQUESTED FROM REMOTE <Process messages> for RPC service

```
TOTAL TRANSMITTED MESSAGES <41> for IP(NTP) service
RECEIVED MESSAGES <27> for IP(NTP) service
SEND MESSAGES <14> for IP(NTP) service
HALT REQUEST SEND COUNTER <0> for IP(NTP) service
STORED MESSAGES for IP(NTP) service (service 0/peer 0)
STATE <Process messages> for IP(NTP) service
REQUESTED FOR REMOTE <Process messages> for IP(NTP) service
REQUESTED FROM REMOTE <Process messages> for IP(NTP) service
```

```
TOTAL TRANSMITTED MESSAGES <5> for IDS Events service
RECEIVED MESSAGES <0> for service IDS Events service
SEND MESSAGES <5> for IDS Events service
HALT REQUEST SEND COUNTER <0> for IDS Events service
STORED MESSAGES for IDS Events service (service 0/peer 0)
STATE <Process messages> for IDS Events service
REQUESTED FOR REMOTE <Process messages> for IDS Events service
REQUESTED FROM REMOTE <Process messages> for IDS Events service
```

```
.
.
```

<Output omitted for brevity>

```
.
.
```

```
Heartbeat Send Time:      Mon Dec 12 00:28:17 2016
Heartbeat Received Time:  Mon Dec 12 00:29:35 2016
```

```
*****
```

```
**RPC STATUS**10.1.1.16*****
```

```
'ip' => '10.1.1.16',
'uuid' => '7d3aa42c-95c7-11e6-a825-2c6c588f5f38',
'ipv6' => 'IPv6 is not configured for management',
'name' => '10.1.1.16',
'active' => '1',
'uuid_gw' => '',
'last_changed' => 'Wed Oct 19 17:56:43 2016'
```

Check routes:

```
>
```

```
admin@FMC:~$ sudo sftunnel_status.pl <Management_IP_Address_of_the_FTD>
```

```
admin@FMC:~$ sudo sftunnel_status.pl 10.1.1.2
```

```
Password:
```

```
Check peer 10.1.1.2 at /usr/local/sf/bin/sftunnel_status.pl line 19
```

```
SFTUNNEL Start Time: Mon Dec 12 01:17:21 2016
```

```
Key File   = /etc/sf/keys/sftunnel-key.pem
Cert File  = /etc/sf/keys/sftunnel-cert.pem
CA Cert    = /etc/sf/ca_root/cacert.pem
FIPS,STIG,CC = 0,0,0
Both IPv4 and IPv6 connectivity is supported
Broadcast count = 1
Reserved SSL connections: 0
Management Interfaces: 1
eth0 (control events) 10.1.1.16,
```

```
*****
```

```
**RUN STATUS**10.1.1.2*****
```

```
Cipher used = AES256-GCM-SHA384 (strength:256 bits)
```

```
ChannelA Connected: Yes, Interface eth0
```

```
Cipher used = AES256-GCM-SHA384 (strength:256 bits)
```

```
ChannelB Connected: Yes, Interface eth0
```

```
Registration: Completed.
```

```
IPv4 Connection to peer '10.1.1.2' Start Time: Mon Dec 12 02:58:54 2016
```

```
PEER INFO:
```

```
sw_version 6.1.0
sw_build 330
Management Interfaces: 1
br1 (control events) 10.1.1.2,
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to
'10.1.1.2' via '10.1.1.16'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to
'10.1.1.2' via '10.1.1.16'

TOTAL TRANSMITTED MESSAGES <20> for Health Events service
RECEIVED MESSAGES <10> for Health Events service
SEND MESSAGES <10> for Health Events service
HALT REQUEST SEND COUNTER <0> for Health Events service
STORED MESSAGES for Health service (service 0/peer 0)
STATE <Process messages> for Health Events service
REQUESTED FOR REMOTE <Process messages> for Health Events service
REQUESTED FROM REMOTE <Process messages> for Health Events service

TOTAL TRANSMITTED MESSAGES <3> for Identity service
RECEIVED MESSAGES <1> for Identity service
SEND MESSAGES <2> for Identity service
HALT REQUEST SEND COUNTER <0> for Identity service
STORED MESSAGES for Identity service (service 0/peer 0)
STATE <Process messages> for Identity service
REQUESTED FOR REMOTE <Process messages> for Identity service
REQUESTED FROM REMOTE <Process messages> for Identity service
.
.
<Output omitted>
```



```
> expert
admin@FTD:~$ sudo manage_procs.pl
Password:
***** Configuration Utility *****

1 Reconfigure Correlator
2 Reconfigure and flush Correlator
3 Restart Comm. channel
4 Update routes
5 Reset all routes
6 Validate Network
0 Exit

*****
Enter choice: 3

***** Configuration Utility *****

1 Reconfigure Correlator
2 Reconfigure and flush Correlator
3 Restart Comm. channel
4 Update routes
5 Reset all routes
6 Validate Network
0 Exit

*****
Enter choice: 0
Thank you
admin@FTD:~$
```

```
admin@FMC:~$ sudo tail -f /var/log/messages | grep 10.1.1.2
```

```
Password:
```

! The following message appears on an FMC as soon as you begin the process on the FTD. It confirms that the FMC is unable to connect to the FTD.

```
[timestamp] sftunneld:sf_connections [INFO] Unable to receive message from peer
10.1.1.2:Closed
[timestamp] sftunneld:sf_channel [INFO] >> ChannelState dropChannel peer 10.1.1.2 /
channelA / CONTROL [ msgSock & ssl_context ] <<
[timestamp] sftunneld:sf_connections [INFO] Exiting channel (recv). Peer 10.1.1.2
closed connection on interface eth0.
[timestamp] sftunneld:sf_connections [INFO] Failed to send in control channel for
peer 10.1.1.2 (eth0)
[timestamp] sftunneld:sf_channel [INFO] >> ChannelState dropChannel peer 10.1.1.2 /
channelA / DROPPED [ msgSock & ssl_context ] <<
[timestamp] sftunneld:sf_channel [INFO] >> ChannelState freeChannel peer 10.1.1.2 /
channelA / DROPPED [ msgSock & ssl_context ] <<
[timestamp] sftunneld:sf_connections [INFO] Need to send SW version and Published
Services to 10.1.1.2
[timestamp] sftunneld:sf_channel [INFO] >> ChannelState do_dataio_for_heartbeat peer
10.1.1.2 / channelB / EVENT [ msgSock2 & ssl_context2 ] <<
[timestamp] sftunneld:control_services [INFO] Successfully Send Interfaces info to
peer 10.1.1.2 over eth0
[timestamp] sftunneld:sf_connections [INFO] Unable to receive message from peer
10.1.1.2:Closed
[timestamp] sftunneld:sf_channel [INFO] >> ChannelState dropChannel peer 10.1.1.2 /
channelB / EVENT [ msgSock2 & ssl_context2 ] <<
[timestamp] sftunneld:sf_connections [INFO] Exiting channel (recv). Peer 10.1.1.2
closed connection on interface eth0.
[timestamp] sftunneld:sf_connections [INFO] Failed to send in control channel for
peer 10.1.1.2 (eth0)
[timestamp] sftunneld:sf_channel [INFO] >> ChannelState dropChannel peer 10.1.1.2 /
channelB / DROPPED [ msgSock2 & ssl_context2 ] <<
[timestamp] sftunneld:sf_channel [INFO] >> ChannelState freeChannel peer 10.1.1.2 /
channelB / DROPPED [ msgSock2 & ssl_context2 ] <<
```



```
[timestamp] sftunneld:sf_ssl [INFO] Accept: Start child thread for peer '10.1.1.2'
[timestamp] sftunneld:sf_channel [INFO] >>>>>> initChannels peer: 10.1.1.2 <<<<<<
[timestamp] sftunneld:stream_file [INFO] Stream CTX initialized for 10.1.1.2
[timestamp] sftunneld:sf_connections [INFO] Peer 10.1.1.2 main thread started
[timestamp] sftunneld:control_services [INFO] Successfully Send Interfaces info to
peer 10.1.1.2 over eth0
[timestamp] sftunneld:sf_heartbeat [INFO] Saved SW VERSION from peer 10.1.1.2
(6.1.0)

[timestamp] sftunneld:sf_connections [INFO] Need to send SW version and Published
Services to 10.1.1.2
[timestamp] sftunneld:sf_channel [INFO] >> ChannelState do_dataio_for_heartbeat peer
10.1.1.2 / channelA / CONTROL [ msgSock & ssl_context ] <<
[timestamp] sftunneld:control_services [INFO] Interface br1 from 10.1.1.2 supports
'control events'
[timestamp] sftunneld:control_services [INFO] Interface br1 from 10.1.1.2 supports
events
[timestamp] sftunneld:control_services [INFO] Interface br1 (10.1.1.2) from 10.1.1.2
is up
[timestamp] sftunneld:control_services [INFO] Peer 10.1.1.2 Notified that it is NOT
configured for dedicated events interface
[timestamp] sftunneld:sf_connections [INFO] Need to send SW version and Published
Services to 10.1.1.2
[timestamp] sftunneld:sf_channel [INFO] >> ChannelState do_dataio_for_heartbeat peer
10.1.1.2 / channelA / CONTROL [ msgSock & ssl_context ] <<
[timestamp] sftunneld:sf_heartbeat [INFO] Saved SW VERSION from peer 10.1.1.2
(6.1.0)
[timestamp] sfmgr:sfmanager [INFO] Established connection to sftunnel for peer
10.1.1.2 (fd 8)
.
.
<Output omitted for brevity>
.
.
[timestamp] sftunneld:sf_heartbeat [INFO] Identity Service is published for peer
10.1.1.2
[timestamp] sftunneld:sf_peers [INFO] Using a 20 entry queue for 10.1.1.2 - 7770
[timestamp] sfmbservice:sfmb_service [INFO] Start getting MB messages for 10.1.1.2
[timestamp] sfmbservice:sfmb_service [INFO] Established connection to peer 10.1.1.2
[timestamp] sftunneld:sf_heartbeat [INFO] Message Broker Service is published for
peer 10.1.1.2
```

<Output Omitted>

.
.

Manage the device locally? (yes/no) [yes]: no

Configure firewall mode? (routed/transparent) [routed]:

Configuring firewall mode ...

Update policy deployment information

- add device configuration
- add network discovery
- add system policy

.
.

<Output Omitted>

> show managers

Type	: Manager
Host	: 10.1.1.16
Registration	: Completed

>

> show managers

No managers configured.

>

> configure firewall routed

This will destroy the current interface configurations, are you sure that you want to proceed? [y/N] y

The firewall mode was changed successfully.

> show firewall

Firewall mode: Router

>

```

> debug icmp trace
debug icmp trace enabled at level 1
>
ICMP echo request from INSIDE_INTERFACE:192.168.1.2 to OUTSIDE_INTERFACE:172.16.1.100
  ID=4101 seq=1 len=56
ICMP echo reply from OUTSIDE_INTERFACE:172.16.1.100 to INSIDE_INTERFACE:192.168.1.2
  ID=4101 seq=1 len=56
ICMP echo request from INSIDE_INTERFACE:192.168.1.2 to OUTSIDE_INTERFACE:172.16.1.100
  ID=4101 seq=2 len=56
ICMP echo reply from OUTSIDE_INTERFACE:172.16.1.100 to INSIDE_INTERFACE:192.168.1.2
  ID=4101 seq=2 len=56
.
.
<Output Omitted>

> undebug all
>

```

```

> show ip
System IP Addresses:
Interface          Name                IP address      Subnet mask    Method
GigabitEthernet1/1  INSIDE_INTERFACE    192.168.1.1    255.255.255.0 manual
GigabitEthernet1/2  OUTSIDE_INTERFACE   172.16.1.1     255.255.255.0 manual
Current IP Addresses:
Interface          Name                IP address      Subnet mask    Method
GigabitEthernet1/1  INSIDE_INTERFACE    192.168.1.1    255.255.255.0 manual
GigabitEthernet1/2  OUTSIDE_INTERFACE   172.16.1.1     255.255.255.0 manual
>

```

```

> show interface ip brief
Interface          IP-Address      OK? Method Status      Protocol
Virtual0          127.1.0.1       YES unset  up          up
GigabitEthernet1/1 192.168.1.1     YES manual up          up
GigabitEthernet1/2 172.16.1.1     YES manual up          up
GigabitEthernet1/3 unassigned       YES unset  administratively down down
GigabitEthernet1/4 unassigned       YES unset  administratively down down
GigabitEthernet1/5 unassigned       YES unset  administratively down down
GigabitEthernet1/6 unassigned       YES unset  administratively down down
GigabitEthernet1/7 unassigned       YES unset  administratively down down
GigabitEthernet1/8 unassigned       YES unset  administratively down down
Internal-Controll1/1 127.0.1.1       YES unset  up          up
Internal-Data1/1    unassigned       YES unset  up          up
Internal-Data1/2    unassigned       YES unset  down        down
Internal-Data1/3    unassigned       YES unset  up          up
Internal-Data1/4    169.254.1.1     YES unset  up          up
Management1/1      unassigned       YES unset  up          up
>

```

```
> show interface GigabitEthernet 1/1
Interface GigabitEthernet1/1 "INSIDE_INTERFACE", is up, line protocol is up
Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
  Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
  Input flow control is unsupported, output flow control is off
  MAC address a46c.2ae4.6bc0, MTU 1500
  IP address 192.168.1.1, subnet mask 255.255.255.0
  3541 packets input, 379530 bytes, 0 no buffer
  Received 54 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 pause input, 0 resume input
  0 L2 decode drops
  2875 packets output, 292832 bytes, 0 underruns
  0 pause output, 0 resume output
  0 output errors, 0 collisions, 0 interface resets
  0 late collisions, 0 deferred
  0 input reset drops, 0 output reset drops
  input queue (blocks free curr/low): hardware (938/895)
  output queue (blocks free curr/low): hardware (1023/1022)
Traffic Statistics for "INSIDE_INTERFACE":
  3534 packets input, 315149 bytes
  2875 packets output, 240884 bytes
  658 packets dropped
  1 minute input rate 2 pkts/sec, 168 bytes/sec
  1 minute output rate 2 pkts/sec, 168 bytes/sec
  1 minute drop rate, 0 pkts/sec
  5 minute input rate 2 pkts/sec, 168 bytes/sec
  5 minute output rate 2 pkts/sec, 168 bytes/sec
  5 minute drop rate, 0 pkts/sec
>
```

```

> show running-config interface
!
interface GigabitEthernet1/1
 nameif INSIDE_INTERFACE
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet1/2
 nameif OUTSIDE_INTERFACE
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
.
.
<Output Omitted for Brevity>
>

```

```

> show interface ip brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
Virtual0	127.1.0.1	YES	unset	up	up
GigabitEthernet1/1	192.168.1.1	YES	manual	up	up
GigabitEthernet1/2	172.16.1.104	YES	DHCP	up	up
GigabitEthernet1/3	unassigned	YES	unset	administratively down	down
GigabitEthernet1/4	unassigned	YES	unset	administratively down	down
GigabitEthernet1/5	unassigned	YES	unset	administratively down	down
GigabitEthernet1/6	unassigned	YES	unset	administratively down	down
GigabitEthernet1/7	unassigned	YES	unset	administratively down	down
GigabitEthernet1/8	unassigned	YES	unset	administratively down	down
Internal-Controll1/1	127.0.1.1	YES	unset	up	up
Internal-Data1/1	unassigned	YES	unset	up	up
Internal-Data1/2	unassigned	YES	unset	down	down
Internal-Data1/3	unassigned	YES	unset	up	up
Internal-Data1/4	169.254.1.1	YES	unset	up	up
Management1/1	unassigned	YES	unset	up	up

```

>

```



```
> show running-config interface
!  
interface GigabitEthernet1/1  
  nameif INSIDE_INTERFACE  
  cts manual  
  propagate sgt preserve-untag  
  policy static sgt disabled trusted  
  security-level 0  
  ip address 192.168.1.1 255.255.255.0  
!  
interface GigabitEthernet1/2  
  nameif OUTSIDE_INTERFACE  
  cts manual  
  propagate sgt preserve-untag  
  policy static sgt disabled trusted  
  security-level 0  
  ip address dhcp setroute  
!  
.  
.  
<Output Omitted for Brevity>  
>
```

```
> show dhcpd binding
```

IP address	Client Identifier	Lease expiration	Type
192.168.1.2	c42c.033c.98a8	3580 seconds	Automatic

```
>
```

```
> debug dhcpd packet
debug dhcpd packet enabled at level 1
>

DHCPD/RA: Server msg received, fip=ANY, fport=0 on INSIDE_INTERFACE interface
DHCPD: DHCPDISCOVER received from client c42c.033c.98a8 on interface INSIDE_INTERFACE.
DHCPD: send ping pkt to 192.168.1.2
DHCPD: ping got no response for ip: 192.168.1.2
DHCPD: Add binding 192.168.1.2 to radix tree
DHCPD/RA: Binding successfully added to hash table
DHCPD: Sending DHCPPOFFER to client c42c.033c.98a8 (192.168.1.2).

DHCPD: Total # of raw options copied to outgoing DHCP message is 0.
DHCPD/RA: creating ARP entry (192.168.1.2, c42c.033c.98a8).
DHCPD: unicasting BOOTREPLY to client c42c.033c.98a8(192.168.1.2).
DHCPD/RA: Server msg received, fip=ANY, fport=0 on INSIDE_INTERFACE interface
DHCPD: DHCPREQUEST received from client c42c.033c.98a8.
DHCPD: Extracting client address from the message
DHCPD: State = DHCPS_REBOOTING
DHCPD: State = DHCPS_REQUESTING
DHCPD: Client c42c.033c.98a8 specified it's address 192.168.1.2
DHCPD: Client is on the correct network
DHCPD: Client accepted our offer
DHCPD: Client and server agree on address 192.168.1.2
DHCPD: Renewing client c42c.033c.98a8 lease
DHCPD: Client lease can be renewed
DHCPD: Sending DHCPACK to client c42c.033c.98a8 (192.168.1.2).

DHCPD: Total # of raw options copied to outgoing DHCP message is 0.
DHCPD/RA: creating ARP entry (192.168.1.2, c42c.033c.98a8).
DHCPD: unicasting BOOTREPLY to client c42c.033c.98a8(192.168.1.2).

>
```

```
<Output Omitted>
```

```
.  
.
```

```
Manage the device locally? (yes/no) [yes]: no
```

```
Configure firewall mode? (routed/transparent) [routed]: transparent
```

```
Configuring firewall mode ...
```

```
.  
.
```

```
<Output Omitted>
```

```
> show managers
```

```
Type           : Manager  
Host           : 10.1.1.16  
Registration    : Completed
```

```
>
```

```
> show managers
```

```
No managers configured.
```

```
>
```

```
> configure firewall transparent
```

```
This will destroy the current interface configurations, are you sure that you want  
to proceed? [y/N] y
```

```
The firewall mode was changed successfully.
```

```
> show firewall
```

```
Firewall mode: Transparent
```

```
>
```

```
> show running-config interface
!
interface GigabitEthernet1/1
 nameif INSIDE_INTERFACE
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 bridge-group 1
 security-level 0
!
interface GigabitEthernet1/2
 nameif OUTSIDE_INTERFACE
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 bridge-group 1
 security-level 0
.
.
<Output Omitted for Brevity>
.
.
interface Management1/1
 management-only
 nameif diagnostic
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
!
interface BVI1
 ip address 192.168.1.1 255.255.255.0
>
```

```
> show interface ip brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Virtual0	127.1.0.1	YES	unset	up	up
GigabitEthernet1/1	192.168.1.1	YES	unset	up	up
GigabitEthernet1/2	192.168.1.1	YES	unset	up	up
GigabitEthernet1/3	unassigned	YES	unset	administratively down	down
GigabitEthernet1/4	unassigned	YES	unset	administratively down	down
GigabitEthernet1/5	unassigned	YES	unset	administratively down	down
GigabitEthernet1/6	unassigned	YES	unset	administratively down	down
GigabitEthernet1/7	unassigned	YES	unset	administratively down	down
GigabitEthernet1/8	unassigned	YES	unset	administratively down	down
Internal-Controll1/1	127.0.1.1	YES	unset	up	up
Internal-Data1/1	unassigned	YES	unset	up	up
Internal-Data1/2	unassigned	YES	unset	down	down
Internal-Data1/3	unassigned	YES	unset	up	up
Internal-Data1/4	169.254.1.1	YES	unset	up	up
Management1/1	unassigned	YES	unset	up	up
BVI1	192.168.1.1	YES	manual	up	up

```
>
```

```
> show network
```

```
=====[ System Information ]=====
Hostname           : firepower
Management port   : 8305
IPv4 Default route
  Gateway          : 10.1.1.1

=====[ br1 ]=====
State              : Enabled
Channels          : Management & Events
Mode              : Non-Autonegotiation
MDI/MDIX         : Auto/MDIX
MTU               : 1500
MAC Address       : A4:6C:2A:E4:6B:BE

-----[ IPv4 ]-----
Configuration     : Manual
Address           : 10.1.1.2
Netmask           : 255.255.255.0
Broadcast         : 10.1.1.255

-----[ IPv6 ]-----
Configuration     : Disabled

=====[ Proxy Information ]=====
State             : Disabled
Authentication    : Disabled

>
```

! On FTD:

```
> show interface GigabitEthernet1/1 | include address
    MAC address a46c.2ae4.6bc0, MTU 1500
    IP address 192.168.1.1, subnet mask 255.255.255.0

> show interface GigabitEthernet1/2 | include address
    MAC address a46c.2ae4.6bc1, MTU 1500
    IP address 192.168.1.1, subnet mask 255.255.255.0
```

! On Router:

```
Inside-Router# show interfaces GigabitEthernet2 | include address
    Hardware is CSR vNIC, address is 000c.2943.7b76 (bia 000c.2943.7b76)
    Internet address is 192.168.1.20/24

Outside-Router## show interfaces GigabitEthernet3 | include address
    Hardware is CSR vNIC, address is 000c.2965.d399 (bia 000c.2965.d399)
    Internet address is 192.168.1.30/24
```

```
Inside-Router# ping 192.168.1.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.30, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 5/5/6 ms
Inside-Router#
```

> debug icmp trace

debug icmp trace enabled at level 1

```
>
ICMP echo request from INSIDE_INTERFACE:192.168.1.20 to OUTSIDE_
INTERFACE:192.168.1.30 ID=8 seq=1 len=72
ICMP echo reply from OUTSIDE_INTERFACE:192.168.1.30 to INSIDE_
INTERFACE:192.168.1.20 ID=8 seq=1 len=72
```

```
Inside-Router# show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.1.20 - 000c.2943.7b76 ARPA GigabitEthernet2
Internet 192.168.1.30 2 000c.2965.d399 ARPA GigabitEthernet2
Inside-Router#
```

```

> debug icmp trace
debug icmp trace enabled at level 1

> ping 192.168.1.20
ICMP echo request from 192.168.1.1 to 192.168.1.20 ID=52779 seq=30330 len=72
ICMP echo reply from 192.168.1.20 to 192.168.1.1 ID=52779 seq=30330 len=72
.
<Output Omitted for Brevity>
.

! To disable the debug of ICMP traffic:
> no debug icmp trace
debug icmp trace disabled.
>

! Alternatively, to disable all of the running debug processes:
> undebug all
>

```

```

Inside-Router# show arp

```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.1.1	1	a46c.2ae4.6bc0	ARPA	GigabitEthernet2
Internet	192.168.1.20	-	000c.2943.7b76	ARPA	GigabitEthernet2
Internet	192.168.1.30	5	000c.2965.d399	ARPA	GigabitEthernet2

```

Inside-Router#

```

```

> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list CSM_FW_ACL_ ; 6 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel
and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998
(hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit 41 any any rule-id 9998 (hitcnt=0)
0x06095aba
access-list CSM_FW_ACL_ line 5 advanced permit gre any any rule-id 9998 (hitcnt=0)
0x52c7a066
access-list CSM_FW_ACL_ line 6 advanced permit udp any eq 3544 any range 1025 65535
rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 7 advanced permit udp any range 1025 65535 any eq 3544
rule-id 9998 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 8 remark rule-id 268434432: ACCESS POLICY: AC Policy -
Default/1
access-list CSM_FW_ACL_ line 9 remark rule-id 268434432: L4 RULE: DEFAULT ACTION
RULE
access-list CSM_FW_ACL_ line 10 advanced permit ip any any rule-id 268434432
(hitcnt=3281) 0xald3780e
>

```

```

> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list CSM_FW_ACL_ ; 8 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel
  and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998
  (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit 41 any any rule-id 9998 (hitcnt=0)
  0x06095aba
access-list CSM_FW_ACL_ line 5 advanced permit gre any any rule-id 9998 (hitcnt=0)
  0x52c7a066
access-list CSM_FW_ACL_ line 6 advanced permit udp any eq 3544 any range 1025 65535
  rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 7 advanced permit udp any range 1025 65535 any eq 3544
  rule-id 9998 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 8 remark rule-id 268437504: ACCESS POLICY: AC Policy -
  Mandatory/1
access-list CSM_FW_ACL_ line 9 remark rule-id 268437504: L7 RULE: Routing Access
access-list CSM_FW_ACL_ line 10 advanced permit ospf any any rule-id 268437504
  (hitcnt=4) 0x385cc1f6
access-list CSM_FW_ACL_ line 11 remark rule-id 268437505: ACCESS POLICY: AC Policy -
  Mandatory/2
access-list CSM_FW_ACL_ line 12 remark rule-id 268437505: L7 RULE: Shell Access
access-list CSM_FW_ACL_ line 13 advanced permit tcp any any object-group SSH rule-id
  268437505 (hitcnt=8) 0x030eea01
  access-list CSM_FW_ACL_ line 13 advanced permit tcp any any eq ssh rule-id
    268437505 (hitcnt=8) 0xf8ca4a86
access-list CSM_FW_ACL_ line 14 remark rule-id 268434432: ACCESS POLICY: AC Policy -
  Default/1
access-list CSM_FW_ACL_ line 15 remark rule-id 268434432: L4 RULE: DEFAULT ACTION
  RULE
access-list CSM_FW_ACL_ line 16 advanced deny ip any any rule-id 268434432 event-log
  flow-start (hitcnt=826) 0x97aa021a
>

```

Jan 31 04:00:51.434: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on GigabitEthernet2 from FULL to DOWN, Neighbor Down: Dead timer expired


```
> capture-traffic
```

```
Please choose domain to capture traffic from:
```

- 0 - br1
- 1 - Router

```
Selection? 1
```

```
Please specify tcpdump options desired.
```

```
(or enter '?' for a list of supported options)
```

```
Options:
```

```
! To capture the 5 HTTP transactions between a web server and a host with IP address 192.168.1.2:
```

```
Options: -n -c 5 host 192.168.1.2 and port 80
```

```
03:42:23.479970 IP 192.168.1.2.44694 > 172.16.1.2.80: Flags [S], seq 2622260089, win 29200, options [mss 1380,sackOK,TS val 2174057 ecr 0,nop,wscale 7], length 0
```

```
03:42:23.479970 IP 172.16.1.2.80 > 192.168.1.2.44694: Flags [S.], seq 2877405527, ack 2622260090, win 28960, options [mss 1380,sackOK,TS val 1270689 ecr 2174057,nop,wscale 7], length 0
```

```
03:42:23.479970 IP 192.168.1.2.44694 > 172.16.1.2.80: Flags [.], ack 1, win 229, options [nop,nop,TS val 2174058 ecr 1270689], length 0
```

```
03:42:23.479970 IP 192.168.1.2.44694 > 172.16.1.2.80: Flags [P.], ack 1, win 229, options [nop,nop,TS val 2174058 ecr 1270689], length 436
```

```
03:42:23.479970 IP 172.16.1.2.80 > 192.168.1.2.44694: Flags [.], ack 437, win 235, options [nop,nop,TS val 1270689 ecr 2174058], length 0
```

```
>
```

```
! To capture the client side traffic-originated by a host, destined to a web server:
```

```
Options: -n -c 5 src 192.168.1.2 and dst port 80
```

```
03:47:07.529956 IP 192.168.1.2.44698 > 172.16.1.2.80: Flags [S], seq 3873637979, win
 29200, options [mss 1380,sackOK,TS val 2245066 ecr 0,nop,wscale 7], length 0
03:47:07.529956 IP 192.168.1.2.44698 > 172.16.1.2.80: Flags [.], ack 3924903157, win
 229, options [nop,nop,TS val 2245066 ecr 1341696], length 0
03:47:07.529956 IP 192.168.1.2.44698 > 172.16.1.2.80: Flags [P.], ack 1, win 229,
 options [nop,nop,TS val 2245066 ecr 1341696], length 436
03:47:07.529956 IP 192.168.1.2.44698 > 172.16.1.2.80: Flags [.], ack 1369, win 251,
 options [nop,nop,TS val 2245067 ecr 1341697], length 0
03:47:07.529956 IP 192.168.1.2.44698 > 172.16.1.2.80: Flags [.], ack 2737, win 274,
 options [nop,nop,TS val 2245067 ecr 1341697], length 0
>
```

```
! To capture the server side traffic—originated by a web server, destined to host
192.168.1.2:
```

```
Options: -n -c 5 dst 192.168.1.2 and src port 80
```

```
03:49:11.779943 IP 172.16.1.2.80 > 192.168.1.2.44702: Flags [S.], seq 212338482,
 ack 2358717416, win 28960, options [mss 1380,sackOK,TS val 1372759 ecr
 2276129,nop,wscale 7], length 0
03:49:11.789952 IP 172.16.1.2.80 > 192.168.1.2.44702: Flags [.], ack 437, win 235,
 options [nop,nop,TS val 1372759 ecr 2276129], length 0
03:49:11.789952 IP 172.16.1.2.80 > 192.168.1.2.44702: Flags [.], ack 437, win 235,
 options [nop,nop,TS val 1372759 ecr 2276129], length 1368
03:49:11.789952 IP 172.16.1.2.80 > 192.168.1.2.44702: Flags [.], ack 437, win 235,
 options [nop,nop,TS val 1372759 ecr 2276129], length 1368
03:49:11.789952 IP 172.16.1.2.80 > 192.168.1.2.44702: Flags [P.], ack 437, win 235,
 options [nop,nop,TS val 1372759 ecr 2276129], length 789
>
```

! First, look at the following capture with default packet data:

Options: -n -c 5 host 192.168.1.2

```
04:36:10.329969 IP 192.168.1.2.58718 > 172.16.1.2.80: Flags [S], seq 193723078, win
 29200, options [mss 1380,sackOK,TS val 392486 ecr 0,nop,wscale 7], length 0
04:36:10.329969 IP 172.16.1.2.80 > 192.168.1.2.58718: Flags [S.], seq 2078424703,
 ack 193723079, win 28960, options [mss 1380,sackOK,TS val 2077347 ecr
 392486,nop,wscale 7], length 0
04:36:10.329969 IP 192.168.1.2.58718 > 172.16.1.2.80: Flags [.), ack 1, win 229,
 options [nop,nop,TS val 392486 ecr 2077347], length 0
04:36:10.329969 IP 192.168.1.2.58718 > 172.16.1.2.80: Flags [P.), ack 1, win 229,
 options [nop,nop,TS val 392486 ecr 2077347], length 436
04:36:10.329969 IP 172.16.1.2.80 > 192.168.1.2.58718: Flags [.), ack 437, win 235,
 options [nop,nop,TS val 2077347 ecr 392486], length 0
>
```

! The -vv option prints additional data including the checksum of a packet.

Options: -n -c 5 -vv host 192.168.1.2

```
04:36:44.729957 IP (tos 0x0, ttl 64, id 27818, offset 0, flags [DF], proto TCP (6),
 length 60)
 192.168.1.2.58720 > 172.16.1.2.80: Flags [S], cksum 0x730b (correct), seq
 2112778772, win 29200, options [mss 1380,sackOK,TS val 401086 ecr 0,nop,
 wscale 7], length 0
04:36:44.729957 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6),
 length 60)
```

```

172.16.1.2.80 > 192.168.1.2.58720: Flags [S.], cksum 0x0515 (correct), seq
  2199066473, ack 2112778773, win 28960, options [mss 1380,sackOK,TS val 2085945
  ecr 401086,nop,wscale 7], length 0
04:36:44.729957 IP (tos 0x0, ttl 64, id 27819, offset 0, flags [DF], proto TCP (6),
  length 52)
  192.168.1.2.58720 > 172.16.1.2.80: Flags [.], cksum 0xa3cc (correct), seq 1,
  ack 1, win 229, options [nop,nop,TS val 401086 ecr 2085945], length 0
04:36:44.729957 IP (tos 0x0, ttl 64, id 27820, offset 0, flags [DF], proto TCP (6),
  length 488)
  192.168.1.2.58720 > 172.16.1.2.80: Flags [P.], cksum 0xf6e9 (correct), seq
  1:437, ack 1, win 229, options [nop,nop,TS val 401086 ecr 2085945], length 436
04:36:44.729957 IP (tos 0x0, ttl 64, id 65408, offset 0, flags [DF], proto TCP (6),
  length 52)
  172.16.1.2.80 > 192.168.1.2.58720: Flags [.], cksum 0xa212 (correct), seq 1,
  ack 437, win 235, options [nop,nop,TS val 2085945 ecr 401086], length 0
>

```

! The -e option displays the layer 2 header in the capture.

Options: -n -c 5 -e host 192.168.1.2

```

04:37:21.909941 c4:2c:03:3c:98:a8 > a4:6c:2a:e4:6b:c0, ethertype IPv4 (0x0800),
  length 74: 192.168.1.2.58722 > 172.16.1.2.80: Flags [S], seq 1691712365, win
  29200, options [mss 1380,sackOK,TS val 410383 ecr 0,nop,wscale 7], length 0
04:37:21.919935 00:23:24:72:1d:3c > a4:6c:2a:e4:6b:c1, ethertype IPv4 (0x0800),
  length 74: 172.16.1.2.80 > 192.168.1.2.58722: Flags [S.], seq 3252338695,
  ack 1691712366, win 28960, options [mss 1380,sackOK,TS val 2095242 ecr
  410383,nop,wscale 7], length 0
04:37:21.919935 c4:2c:03:3c:98:a8 > a4:6c:2a:e4:6b:c0, ethertype IPv4 (0x0800),
  length 66: 192.168.1.2.58722 > 172.16.1.2.80: Flags [.], ack 1, win 229, options
  [nop,nop,TS val 410383 ecr 2095242], length 0
04:37:21.919935 c4:2c:03:3c:98:a8 > a4:6c:2a:e4:6b:c0, ethertype IPv4 (0x0800),
  length 502: 192.168.1.2.58722 > 172.16.1.2.80: Flags [P.], ack 1, win 229, options
  [nop,nop,TS val 410383 ecr 2095242], length 436
04:37:21.919935 00:23:24:72:1d:3c > a4:6c:2a:e4:6b:c1, ethertype IPv4 (0x0800),
  length 66: 172.16.1.2.80 > 192.168.1.2.58722: Flags [.], ack 437, win 235, options
  [nop,nop,TS val 2095242 ecr 410383], length 0
>

```

! The -X option prints the hex and ASCII values of each packet. For example, the fourth packet in the following example shows the GET request to a HTTP server.

Options: -n -c 5 -X host 192.168.1.2

04:40:50.069988 IP 192.168.1.2.58724 > 172.16.1.2.80: Flags [S], seq 3090457163, win 29200, options [mss 1380,sackOK,TS val 462423 ecr 0,nop,wscale 7], length 0

```
0x0000: 4500 003c ac1c 4000 4006 1fe3 c0a8 0102 E..<...@.@.....
0x0010: ac10 0102 e564 0050 b834 a24b 0000 0000 .....d.P.4.K....
0x0020: a002 7210 18f0 0000 0204 0564 0402 080a ..r.....d....
0x0030: 0007 0e57 0000 0000 0103 0307          ...W.....
```

04:40:50.069988 IP 172.16.1.2.80 > 192.168.1.2.58724: Flags [S.], seq 1195208673, ack 3090457164, win 28960, options [mss 1380,sackOK,TS val 2147276 ecr 462423,nop,wscale 7], length 0

```
0x0000: 4500 003c 0000 4000 4006 cbff ac10 0102 E..<...@.@.....
0x0010: c0a8 0102 0050 e564 473d 6fe1 b834 a24c .....P.dG=o..4.L
0x0020: a012 7120 9ec3 0000 0204 0564 0402 080a ..q.....d....
0x0030: 0020 c3cc 0007 0e57 0103 0307          .....W....
```

04:40:50.069988 IP 192.168.1.2.58724 > 172.16.1.2.80: Flags [.], ack 1, win 229, options [nop,nop,TS val 462423 ecr 2147276], length 0

```
0x0000: 4500 0034 ac1d 4000 4006 1fea c0a8 0102 E..4...@.@.....
0x0010: ac10 0102 e564 0050 b834 a24c 473d 6fe2 .....d.P.4.LG=o.
0x0020: 8010 00e5 3d7b 0000 0101 080a 0007 0e57 ....={.....W
0x0030: 0020 c3cc          ....
```

04:40:50.069988 IP 192.168.1.2.58724 > 172.16.1.2.80: Flags [P.], ack 1, win 229, options [nop,nop,TS val 462423 ecr 2147276], length 436

```
0x0000: 4500 01e8 ac1e 4000 4006 1e35 c0a8 0102 E.....@.@..5....
0x0010: ac10 0102 e564 0050 b834 a24c 473d 6fe2 .....d.P.4.LG=o.
0x0020: 8018 00e5 9098 0000 0101 080a 0007 0e57 .....W
0x0030: 0020 c3cc 4745 5420 2f20 4854 5450 2f31 ...GET./.HTTP/1
0x0040: 2e31 0d0a 486f 7374 3a20 3137 322e 3136 .1..Host:.172.16
0x0050: 2e31 2e32 0d0a 5573 6572 2d41 6765 6e74 .1.2..User-Agent
0x0060: 3a20 4d6f 7a69 6c6c 612f 352e 3020 2858 :.Mozilla/5.0.(X
0x0070: 3131 3b20 5562 756e 7475 3b20 4c69 6e75 11;.Ubuntu;.Linu
0x0080: 7820 7838 365f 3634 3b20 7276 3a34 382e x.x86_64;.rv:48.
0x0090: 3029 2047 6563 6b6f 2f32 3031 3030 3130 0).Gecko/2010010
0x00a0: 3120 4669 7265 666f 782f 3438 2e30 0d0a 1.Firefox/48.0..
0x00b0: 4163 6365 7074 3a20 7465 7874 2f68 746d Accept:.text/htm
```

```

0x00c0: 6c2c 6170 706c 6963 6174 696f 6e2f 7868  l,application/xh
0x00d0: 746d 6c2b 786d 6c2c 6170 706c 6963 6174  tml+xml,applicat
0x00e0: 696f 6e2f 786d 6c3b 713d 302e 392c 2a2f  ion/xml;q=0.9,*/*
0x00f0: 2a3b 713d 302e 380d 0a41 6363 6570 742d  *;q=0.8..Accept-
0x0100: 4c61 6e67 7561 6765 3a20 656e 2d55 532c  Language:.en-US,
0x0110: 656e 3b71 3d30 2e35 0d0a 4163 6365 7074  en;q=0.5..Accept
0x0120: 2d45 6e63 6f64 696e 673a 2067 7a69 702c  -Encoding:.gzip,
0x0130: 2064 6566 6c61 7465 0d0a 436f 6e6e 6563  .deflate..Connec
0x0140: 7469 6f6e 3a20 6b65 6570 2d61 6c69 7665  tion:.keep-alive
0x0150: 0d0a 5570 6772 6164 652d 496e 7365 6375  ..Upgrade-Insecu
0x0160: 7265 2d52 6571 7565 7374 733a 2031 0d0a  re-Requests:.1..
0x0170: 4966 2d4d 6f64 6966 6965 642d 5369 6e63  If-Modified-Sinc
0x0180: 653a 2054 7565 2c20 3134 2046 6562 2032  e:.Tue,.14.Feb.2
0x0190: 3031 3720 3136 3a32 343a 3339 2047 4d54  017.16:24:39.GMT
0x01a0: 0d0a 4966 2d4e 6f6e 652d 4d61 7463 683a  ..If-None-Match:
0x01b0: 2022 3263 3339 2d35 3438 3830 3030 3333  ."2c39-548800033
0x01c0: 3730 6463 2d67 7a69 7022 0d0a 4361 6368  70dc-gzip"..Cach
0x01d0: 652d 436f 6e74 726f 6c3a 206d 6178 2d61  e-Control:.max-a
0x01e0: 6765 3d30 0d0a 0d0a                                ge=0....
04:40:50.069988 IP 172.16.1.2.80 > 192.168.1.2.58724: Flags [.] , ack 437, win 235,
options [nop,nop,TS val 2147276 ecr 462423], length 0
0x0000: 4500 0034 1e39 4000 4006 adce ac10 0102  E..4.9@.@.....
0x0010: c0a8 0102 0050 e564 473d 6fe2 b834 a400  ....P.dG=o..4..
0x0020: 8010 00eb 3bc1 0000 0101 080a 0020 c3cc  ....;.....
0x0030: 0007 0e57                                ...W
>

```

```
Options: -w traffic.pcap -s 1518 host 192.168.1.2
```

```
^C
```

```
Caught interrupt signal
```

```
Exiting.
```

```
>
```

```
! The following command confirms that the pcap file is created and stored on the disk.
```

```
> file list
```

```
Feb 15 05:03                886 /traffic.pcap
```

```
>
```

```
file secure-copy IP_Address Username Path Filename
```

```
> file secure-copy 10.1.1.10 admin /var/tmp traffic.pcap
The authenticity of host '10.1.1.10 (10.1.1.10)' can't be established.
ECDSA key fingerprint is 71:cf:b1:17:86:78:bf:10:41:7d:60:75:87:c3:6b:f4.
Are you sure you want to continue connecting (yes/no)? yes
Password:
copy successful.
>
```

```
> file delete traffic.pcap
Really remove file traffic.pcap?
Please enter 'YES' or 'NO': YES
```

```
> show nameif
Interface          Name                Security
GigabitEthernet1/1  INSIDE_INTERFACE    0
GigabitEthernet1/2  OUTSIDE_INTERFACE   0
Management1/1      diagnostic           0
>
```

```
capture capture_name interface int_name match protocol_name source_
detail destination detail
> capture icmp_traffic interface INSIDE_INTERFACE match icmp host
192.168.1.2 any
```

```
! Run the following command to view the condition within a capture process.
```

```
> show capture
capture icmp_traffic type raw-data interface INSIDE_INTERFACE [Capturing - 1140
bytes]
match icmp host 192.168.1.2 any
>
```

```
! Run the following command to view the captured traffic for a particular matching
condition.
```

```
> show capture icmp_traffic
```

```
6 packets captured
```

```
1: 05:47:38.406457      192.168.1.2 > 172.16.1.2: icmp: echo request
2: 05:47:38.407205      172.16.1.2 > 192.168.1.2: icmp: echo reply
3: 05:47:39.407617      192.168.1.2 > 172.16.1.2: icmp: echo request
4: 05:47:39.408258      172.16.1.2 > 192.168.1.2: icmp: echo reply
5: 05:47:40.408731      192.168.1.2 > 172.16.1.2: icmp: echo request
6: 05:47:40.409478      172.16.1.2 > 192.168.1.2: icmp: echo reply
```

```
6 packets shown
```

```
>
```

! Run the following command to remove the previous captures.

```
> clear capture /all
```

```
>
```

! The following command confirms that all of the previously captured packets are cleared.

```
> show capture icmp_traffic
```

```
0 packet captured
```

```
0 packet shown
```

```
>
```

! To stop capturing any traffic that might match the icmp_traffic capturing condition, run the following command:

```
> no capture icmp_traffic interface INSIDE_INTERFACE
```

```
>
```

! To confirm that a capture instance no longer runs on an interface, run the command below. Note that an interface name is no longer associated the icmp_traffic capture.

```
> show capture
```

```
capture icmp_traffic type raw-data [Capturing - 1140 bytes]
  match icmp host 192.168.1.2 any
```

```
>
```

! To delete the icmp_traffic capture instance, run the following command:

```
> no capture icmp_traffic
```

```
>
```

! Now, if you try again, it ends with an error as the capture itself is deleted.

```
> show capture icmp_traffic
```

```
ERROR: Capture <icmp_traffic> does not exist
```

```
>
```

```
> capture http_traffic interface INSIDE_INTERFACE match tcp any any eq 80
```



```
> show capture
capture http_traffic type raw-data interface INSIDE_INTERFACE [Capturing - 5777
bytes]
match tcp any any eq www
>
```

```
> show capture http_traffic
```

```
15 packets captured
```

```
1: 09:19:38.442726      192.168.1.2.58808 > 172.16.1.2.80: S 1558097726:
1558097726(0) win 29200 <mss 1460,sackOK,timestamp 4644956 0,nop,wscale 7>
2: 09:19:38.444007      172.16.1.2.80 > 192.168.1.2.58808: S 1776867665:
1776867665(0) ack 1558097727 win 28960 <mss 1380,sackOK,timestamp 6329332
4644956,nop,wscale 7>
3: 09:19:38.444129      192.168.1.2.58808 > 172.16.1.2.80: . ack 1776867666 win
229 <nop,nop,timestamp 4644956 6329332>
4: 09:19:38.444267      192.168.1.2.58808 > 172.16.1.2.80: P 1558097727:
1558098163(436) ack 1776867666 win 229 <nop,nop,timestamp 4644956 6329332>
5: 09:19:38.444999      172.16.1.2.80 > 192.168.1.2.58808: . ack 1558098163 win
235 <nop,nop,timestamp 6329332 4644956>
6: 09:19:38.446601      172.16.1.2.80 > 192.168.1.2.58808: . 1776867666:
1776869034(1368) ack 1558098163 win 235 <nop,nop,timestamp 6329332 4644956>
7: 09:19:38.446616      172.16.1.2.80 > 192.168.1.2.58808: . 1776869034:
1776870402(1368) ack 1558098163 win 235 <nop,nop,timestamp 6329332 4644956>
8: 09:19:38.446662      172.16.1.2.80 > 192.168.1.2.58808: P 1776870402:
1776871191(789) ack 1558098163 win 235 <nop,nop,timestamp 6329332 4644956>
9: 09:19:38.446800      192.168.1.2.58808 > 172.16.1.2.80: . ack 1776871191 win
284 <nop,nop,timestamp 4644957 6329332>
10: 09:19:38.488011      192.168.1.2.58808 > 172.16.1.2.80: P 1558098163:
1558098553(390) ack 1776871191 win 284 <nop,nop,timestamp 4644967 6329332>
11: 09:19:38.489354      172.16.1.2.80 > 192.168.1.2.58808: P 1776871191:
1776871371(180) ack 1558098553 win 243 <nop,nop,timestamp 6329343 4644967>
12: 09:19:38.489476      192.168.1.2.58808 > 172.16.1.2.80: . ack 1776871371 win
305 <nop,nop,timestamp 4644968 6329343>
13: 09:19:43.397013      172.16.1.2.80 > 192.168.1.2.58808: F 1776871371:
1776871371(0) ack 1558098553 win 243 <nop,nop,timestamp 6330570 4644968>
14: 09:19:43.397486      192.168.1.2.58808 > 172.16.1.2.80: F 1558098553:
1558098553(0) ack 1776871372 win 305 <nop,nop,timestamp 4646195 6330570>
15: 09:19:43.397821      172.16.1.2.80 > 192.168.1.2.58808: . ack 1558098554 win
243 <nop,nop,timestamp 6330570 4646195>
```

```
15 packets shown
```

```
>
```

```
https://<IP_Address_of_FTD>/capture/<capture_name>/pcap/<capture_name>.
pcap
https://192.168.1.1/capture/http_traffic/pcap/http_traffic.pcap
```

```
> debug http 255
```

```
debug http enabled at level 255.
```

```
>
```

```
! As soon as the HTTP service starts, FTD generates the following debug message:
```

```
http_enable: Enabling HTTP server  
HTTP server starting.
```

```
! To verify the current HTTP server configuration:
```

```
> show running-config http  
http server enable  
http 192.168.0.0 255.255.0.0 INSIDE_INTERFACE  
>
```

```
https://<IP_Address_of_FTD>/capture/<capture_name>/pcap/<capture_name>.pcap  
https://192.168.1.1/capture/http_traffic/pcap/http_traffic.pcap
```

```
admin@FMC:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 00:0      C:29:ED:37:B1  
          inet addr:10.1.1.16  Bcast:10.1.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:feed:37b1/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:99519 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:591461 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:21356354 (20.3 Mb)  TX bytes:145518227 (138.7 Mb)  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.255.255.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:65536  Metric:1  
          RX packets:79815237 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:79815237 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:32518661679 (31012.2 Mb)  TX bytes:32518661679 (31012.2 Mb)  
  
admin@FMC:~$
```



```
> capture icmp_traffic interface INSIDE_INTERFACE match icmp any any

> show capture icmp_traffic

20 packets captured

  1: 16:39:55.255159      172.16.1.2 > 192.168.1.2: icmp: echo reply
  2: 16:39:56.255769      192.168.1.2 > 172.16.1.2: icmp: echo request
  3: 16:39:56.256548      172.16.1.2 > 192.168.1.2: icmp: echo reply
  4: 16:39:57.257127      192.168.1.2 > 172.16.1.2: icmp: echo request
  5: 16:39:57.257753      172.16.1.2 > 192.168.1.2: icmp: echo reply
  6: 16:39:58.258333      192.168.1.2 > 172.16.1.2: icmp: echo request
  7: 16:39:58.259019      172.16.1.2 > 192.168.1.2: icmp: echo reply
  8: 16:39:59.259630      192.168.1.2 > 172.16.1.2: icmp: echo request
  9: 16:39:59.260286      172.16.1.2 > 192.168.1.2: icmp: echo reply
 10: 16:40:00.260835      192.168.1.2 > 172.16.1.2: icmp: echo request
 11: 16:40:00.262315      172.16.1.2 > 192.168.1.2: icmp: echo reply
 12: 16:40:01.262971      192.168.1.2 > 172.16.1.2: icmp: echo request
 13: 16:40:02.273759      192.168.1.2 > 172.16.1.2: icmp: echo request
 14: 16:40:03.279663      192.168.1.2 > 172.16.1.2: icmp: echo request
 15: 16:40:04.287735      192.168.1.2 > 172.16.1.2: icmp: echo request
 16: 16:40:05.295776      192.168.1.2 > 172.16.1.2: icmp: echo request
 17: 16:40:06.303664      192.168.1.2 > 172.16.1.2: icmp: echo request
 18: 16:40:07.311919      192.168.1.2 > 172.16.1.2: icmp: echo request
 19: 16:40:08.320006      192.168.1.2 > 172.16.1.2: icmp: echo request
 20: 16:40:09.328031      192.168.1.2 > 172.16.1.2: icmp: echo request

20 packets shown

>
```

```
> capture-traffic
```

```
Please choose domain to capture traffic from:
```

- 0 - br1
- 1 - Router

```
Selection? 1
```

```
Please specify tcpdump options desired.
```

```
(or enter '?' for a list of supported options)
```

```
Options: icmp
```

```
16:39:57.249971 IP 192.168.1.2 > 172.16.1.2: ICMP echo request, id 12845, seq 148, length 64
```

```
16:39:57.249971 IP 172.16.1.2 > 192.168.1.2: ICMP echo reply, id 12845, seq 148, length 64
```

```
16:39:58.249971 IP 192.168.1.2 > 172.16.1.2: ICMP echo request, id 12845, seq 149, length 64
```

```
16:39:58.249971 IP 172.16.1.2 > 192.168.1.2: ICMP echo reply, id 12845, seq 149, length 64
```

```
16:39:59.249971 IP 192.168.1.2 > 172.16.1.2: ICMP echo request, id 12845, seq 150, length 64
```

```
16:39:59.259965 IP 172.16.1.2 > 192.168.1.2: ICMP echo reply, id 12845, seq 150, length 64
```

```
16:40:00.259965 IP 192.168.1.2 > 172.16.1.2: ICMP echo request, id 12845, seq 151, length 64
```

```
16:40:00.259965 IP 172.16.1.2 > 192.168.1.2: ICMP echo reply, id 12845, seq 151, length 64
```

```
.
```

```
.
```

```
^C
```

```
Caught interrupt signal
```

```
Exiting.
```

```
>
```

```
> show interface GigabitEthernet 1/1
Interface GigabitEthernet1/1 "INSIDE_INTERFACE", is down, line protocol is down
Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
  Auto-Duplex, Auto-Speed
  Input flow control is unsupported, output flow control is off
  MAC address a46c.2ae4.6bc0, MTU 1500
  IP address 192.168.1.1, subnet mask 255.255.255.0
  5200 packets input, 531929 bytes, 0 no buffer
  Received 68 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 pause input, 0 resume input
  0 L2 decode drops
  2922 packets output, 2340459 bytes, 0 underruns
  0 pause output, 0 resume output
  0 output errors, 0 collisions, 0 interface resets
  0 late collisions, 0 deferred
  0 input reset drops, 0 output reset drops
  input queue (blocks free curr/low): hardware (985/891)
  output queue (blocks free curr/low): hardware (1023/997)

Traffic Statistics for "INSIDE_INTERFACE":
  5153 packets input, 432852 bytes
  2922 packets output, 2285241 bytes
  3023 packets dropped
  1 minute input rate 0 pkts/sec,  0 bytes/sec
  1 minute output rate 0 pkts/sec,  0 bytes/sec
  1 minute drop rate, 0 pkts/sec
  5 minute input rate 0 pkts/sec,  33 bytes/sec
  5 minute output rate 0 pkts/sec,  1 bytes/sec
  5 minute drop rate, 0 pkts/sec

>
```

```
> capture http_traffic interface INSIDE_INTERFACE match tcp any any eq 80
> capture http_traffic trace interface INSIDE_INTERFACE match tcp any any eq 80
> show capture http_traffic packet-number 1 trace
> packet-tracer input INSIDE_INTERFACE tcp 192.168.1.2 10000 192.168.1.200 80
Source IP Address: 192.168.1.2
```

Destination IP Address: 192.168.1.200

Source Port: 10000

Destination Port: 80

Protocol: TCP

```
> show inline-set
```

```
Inline-set INSIDE_OUTSIDE_PAIR
```

Mtu is 1500 bytes

Failsafe mode is off

Failsecure mode is off

Tap mode is off

Propagate-link-state option is off

hardware-bypass mode is disabled

Interface-Pair[1]:

```
Interface: GigabitEthernet1/1 "INSIDE_INTERFACE"
```

Current-Status: UP

```
Interface: GigabitEthernet1/2 "OUTSIDE_INTERFACE"
```

Current-Status: UP

Bridge Group ID: 500

```
>
```

```
> show interface ip brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Virtual0	127.1.0.1	YES	unset	up	up
GigabitEthernet1/1	unassigned	YES	unset	up	up
GigabitEthernet1/2	unassigned	YES	unset	up	up
GigabitEthernet1/3	unassigned	YES	unset	administratively down	down
GigabitEthernet1/4	unassigned	YES	unset	administratively down	down
GigabitEthernet1/5	unassigned	YES	unset	administratively down	down
GigabitEthernet1/6	unassigned	YES	unset	administratively down	down
GigabitEthernet1/7	unassigned	YES	unset	administratively down	down
GigabitEthernet1/8	unassigned	YES	unset	administratively down	down
Internal-Controll1/1	127.0.1.1	YES	unset	up	up
Internal-Data1/1	unassigned	YES	unset	up	up
Internal-Data1/2	unassigned	YES	unset	down	down
Internal-Data1/3	unassigned	YES	unset	up	up
Internal-Data1/4	169.254.1.1	YES	unset	up	up
Management1/1	unassigned	YES	unset	up	up

```
>
```

```

> show interface GigabitEthernet1/1
Interface GigabitEthernet1/1 "INSIDE_INTERFACE", is up, line protocol is up
Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
  Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
  Input flow control is unsupported, output flow control is off
  MAC address a46c.2ae4.6bc0, MTU 1500
  IPS Interface-Mode: inline, Inline-Set: INSIDE_OUTSIDE_PAIR
  IP address unassigned
  2382 packets input, 258694 bytes, 0 no buffer
  Received 142 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 pause input, 0 resume input
  0 L2 decode drops
  2079 packets output, 234133 bytes, 0 underruns
  0 pause output, 0 resume output
  0 output errors, 0 collisions, 0 interface resets
  0 late collisions, 0 deferred
  0 input reset drops, 2 output reset drops

  input queue (blocks free curr/low): hardware (946/894)
  output queue (blocks free curr/low): hardware (1023/1020)
Traffic Statistics for "INSIDE_INTERFACE":
  592 packets input, 53381 bytes
  530 packets output, 63776 bytes
  11 packets dropped
  1 minute input rate 1 pkts/sec, 85 bytes/sec
  1 minute output rate 1 pkts/sec, 88 bytes/sec
  1 minute drop rate, 0 pkts/sec
  5 minute input rate 1 pkts/sec, 79 bytes/sec
  5 minute output rate 0 pkts/sec, 103 bytes/sec
  5 minute drop rate, 0 pkts/sec
>

```

```

packet-tracer input source_interface protocol_name source_address ICMP_type ICMP_
code destination_address

```



```
> packet-tracer input INSIDE_INTERFACE icmp 192.168.1.2 8 0 192.168.1.200
```

Phase: 1

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 2

Type: NGIPS-MODE

Subtype: ngips-mode

Result: ALLOW

Config:

Additional Information:

The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 3

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434432

access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: AC Policy - Default/1

access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 4

Type: NGIPS-EGRESS-INTERFACE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

Ingress interface INSIDE_INTERFACE is in NGIPS inline mode.

Egress interface OUTSIDE_INTERFACE is determined by inline-set configuration

Phase: 5

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

```
> packet-tracer input OUTSIDE_INTERFACE icmp 192.168.1.200 0 0 192.168.1.2
```

```
Phase: 1
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: NGIPS-MODE
```

```
Subtype: ngips-mode
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
The flow ingresses an interface configured for NGIPS mode and NGIPS services will be applied
```

```
Phase: 3
```

```
Type: ACCESS-LIST
```

```
Subtype: log
```

```
Result: ALLOW
```

```
Config:
```

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434432
```

```
access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: AC Policy - Default/1
```

```
access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
```

```
Additional Information:
```

```
This packet will be sent to snort for additional processing where a verdict will be reached
```

Phase: 4

Type: NGIPS-EGRESS-INTERFACE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

Ingress interface OUTSIDE_INTERFACE is in NGIPS inline mode.

Egress interface INSIDE_INTERFACE is determined by inline-set configuration

Phase: 5

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 271, packet dispatched to next module

Result:

input-interface: OUTSIDE_INTERFACE

input-status: up

input-line-status: up

Action: allow

>

> capture inside_icmp trace interface INSIDE_INTERFACE match icmp any any

> capture outside_icmp trace interface OUTSIDE_INTERFACE match icmp any any

> show capture

capture inside_icmp type raw-data trace interface INSIDE_INTERFACE [Capturing - 0 bytes]

match icmp any any

capture outside_icmp type raw-data trace interface OUTSIDE_INTERFACE [Capturing - 0 bytes]

match icmp any any

>

```
> show capture inside_icmp
```

```
4 packets captured
```

```
1: 21:52:25.988428      192.168.1.2 > 192.168.1.200: icmp: echo request
2: 21:52:25.989405      192.168.1.200 > 192.168.1.2: icmp: echo reply
3: 21:52:26.989862      192.168.1.2 > 192.168.1.200: icmp: echo request
4: 21:52:26.990412      192.168.1.200 > 192.168.1.2: icmp: echo reply
```

```
4 packets shown
```

```
>
```

```
> show capture outside_icmp
```

```
4 packets captured
```

```
1: 21:52:25.989038      192.168.1.2 > 192.168.1.200: icmp: echo request
2: 21:52:25.989252      192.168.1.200 > 192.168.1.2: icmp: echo reply
3: 21:52:26.990106      192.168.1.2 > 192.168.1.200: icmp: echo request
4: 21:52:26.990305      192.168.1.200 > 192.168.1.2: icmp: echo reply
```

```
4 packets shown
```

```
>
```

```
> show capture inside_icmp packet-number 1 trace
```

```
4 packets captured
```

```
1: 21:52:25.988428 192.168.1.2 > 192.168.1.200: icmp: echo request
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 3
```

```
Type: NGIPS-MODE
```

```
Subtype: ngips-mode
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied
```

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434432

access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: AC Policy - Default/1

access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: NGIPS-EGRESS-INTERFACE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

Ingress interface INSIDE_INTERFACE is in NGIPS inline mode.

Egress interface OUTSIDE_INTERFACE is determined by inline-set configuration

Phase: 6

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 279, packet dispatched to next module

Phase: 7
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 8
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet

Phase: 9
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Result:
input-interface: OUTSIDE_INTERFACE
input-status: up
input-line-status: up
Action: allow

1 packet shown

>

```
> show capture inside_icmp packet-number 2 trace

4 packets captured

  2: 21:52:25.989405      192.168.1.200 > 192.168.1.2: icmp: echo reply
1 packet shown
>

> show capture outside_icmp packet-number 2 trace

4 packets captured

  2: 21:52:25.989252      192.168.1.200 > 192.168.1.2: icmp: echo reply
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 279, using existing flow
```


Phase: 4
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 5
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet

Phase: 6
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: allow

1 packet shown

>

```
> show inline-set
```

```
Inline-set INLINE_OUTSIDE_PAIR
```

```
Mtu is 1500 bytes
```

```
Fail-safe mode is on/activated
```

```
Fail-secure mode is off
```

```
Tap mode is off
```

```
Propagate-link-state option is on
```

```
hardware-bypass mode is disabled
```

```
Interface-Pair[1]:
```

```
Interface: GigabitEthernet1/1 "INSIDE_INTERFACE"
```

```
Current-Status: Down(Propagate-Link-State-Activated)
```

```
Interface: GigabitEthernet1/2 "OUTSIDE_INTERFACE"
```

```
Current-Status: Down(Down-By-Propagate-Link-State)
```

```
Bridge Group ID: 500
```

```
>
```

```
> show interface GigabitEthernet1/1
```

```
Interface GigabitEthernet1/1 "INSIDE_INTERFACE", is down, line protocol is down
```

```
Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
```

```
Auto-Duplex, Auto-Speed
```

```
Input flow control is unsupported, output flow control is off
```

```
MAC address a46c.2ae4.6bc0, MTU 1500
```

```
IPS Interface-Mode: inline, Inline-Set: INSIDE_OUTSIDE_PAIR
```

```
Propagate-Link-State-Activated
```

```
IP address unassigned
```

```
14779 packets input, 1512926 bytes, 0 no buffer
```

```
Received 147 broadcasts, 0 runts, 0 giants
```

```
.
```

```
.
```

```
<Output Omitted for Brevity>
```

```
> show interface GigabitEthernet1/2
```

```
Interface GigabitEthernet1/2 "OUTSIDE_INTERFACE", is administratively down, line protocol is down
```

```
Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
```

```
Auto-Duplex, Auto-Speed
```

```
Input flow control is unsupported, output flow control is off
```

```
MAC address a46c.2ae4.6bc1, MTU 1500
```

```
IPS Interface-Mode: inline, Inline-Set: INSIDE_OUTSIDE_PAIR
```

```
Down-By-Propagate-Link-State
```

```
IP address unassigned
```

```
15397 packets input, 1558479 bytes, 0 no buffer
```

```
Received 930 broadcasts, 0 runts, 0 giants
```

```
.
```

```
.
```

```
<Output Omitted for Brevity>
```

```
> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
    alert-interval 300
access-list CSM_FW_ACL_ ; 7 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel
    and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0)
    0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit 41 any any rule-id 9998 (hitcnt=0)
    0x06095aba
access-list CSM_FW_ACL_ line 5 advanced permit gre any any rule-id 9998 (hitcnt=0)
    0x52c7a066

access-list CSM_FW_ACL_ line 6 advanced permit udp any eq 3544 any range 1025 65535
    rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 7 advanced permit udp any range 1025 65535 any eq 3544
    rule-id 9998 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 8 remark rule-id 268440576: ACCESS POLICY: AC Policy -
    Mandatory/1
access-list CSM_FW_ACL_ line 9 remark rule-id 268440576: L4 RULE: Shell Access
access-list CSM_FW_ACL_ line 10 advanced deny tcp any any object-group TELNET
    rule-id 268440576 event-log flow-start (hitcnt=2) 0xae7f8544
    access-list CSM_FW_ACL_ line 10 advanced deny tcp any any eq telnet rule-id
        268440576 event-log flow-start (hitcnt=2) 0x2bcbaf06
access-list CSM_FW_ACL_ line 11 remark rule-id 268434432: ACCESS POLICY: AC Policy -
    Default/1
access-list CSM_FW_ACL_ line 12 remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ line 13 advanced permit ip any any rule-id 268434432
    (hitcnt=134) 0xald3780e
>
```

```
! Packet originates from the inside network, Telnet server is located at the outside network
```

```
> packet-tracer input INSIDE_INTERFACE tcp 192.168.1.2 10000 192.168.1.200 23
```

```
Phase: 1
```

```
Type: NGIPS-MODE
```

```
Subtype: ngips-mode
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype: log
```

```
Result: DROP
```

```
Config:
```

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced deny tcp any any object-group TELNET rule-id 268440576 event-log flow-start
```

```
access-list CSM_FW_ACL_ remark rule-id 268440576: ACCESS POLICY: AC Policy - Mandatory/1
```

```
access-list CSM_FW_ACL_ remark rule-id 268440576: L4 RULE: Shell Access
```

```
object-group service TELNET tcp
```

```
port-object eq telnet
```

```
Additional Information:
```

```
Result:
```

```
input-interface: INSIDE_INTERFACE
```

```
input-status: up
```

```
input-line-status: up
```

```
Action: drop
```

```
Drop-reason: (acl-drop) Flow is denied by configured rule
```

```
>
```

```
! Packet originates from the outside network, Telnet server is located at the inside network
```

```
> packet-tracer input OUTSIDE_INTERFACE tcp 192.168.1.200 10000 192.168.1.2 23
```

```
Phase: 1
```

```
Type: NGIPS-MODE
```

```
Subtype: ngips-mode
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
The flow ingresses an interface configured for NGIPS mode and NGIPS services will be applied
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype: log
```

```
Result: DROP
```

```
Config:
```

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced deny tcp any any object-group TELNET rule-id 268440576 event-log flow-start
```

```
access-list CSM_FW_ACL_ remark rule-id 268440576: ACCESS POLICY: AC Policy - Mandatory/1
```

```
access-list CSM_FW_ACL_ remark rule-id 268440576: L4 RULE: Shell Access
```

```
object-group service TELNET tcp
```

```
port-object eq telnet
```

```
Additional Information:
```

```
Result:
```

```
input-interface: OUTSIDE_INTERFACE
```

```
input-status: up
```

```
input-line-status: up
```

```
Action: drop
```

```
> capture inside_telnet trace interface INSIDE_INTERFACE match tcp any any eq
```

```
>
```

```
> show capture
```

```
capture inside_telnet type raw-data trace interface INSIDE_INTERFACE [Captured bytes]
```

```
match tcp any any eq telnet
```

```
>
```

```
> show capture inside_telnet
```

```
4 packets captured
```

```
1: 01:24:06.440422      192.168.1.2.36534 > 192.168.1.200.23: S 2986077586:
   2986077586(0) win 29200 <mss 1460,sackOK,timestamp 3482899 0,nop,wscale 7>
2: 01:24:07.437965      192.168.1.2.36534 > 192.168.1.200.23: S 2986077586:
   2986077586(0) win 29200 <mss 1460,sackOK,timestamp 3483149 0,nop,wscale 7>
3: 01:24:09.442009      192.168.1.2.36534 > 192.168.1.200.23: S 2986077586:
   2986077586(0) win 29200 <mss 1460,sackOK,timestamp 3483650 0,nop,wscale 7>
4: 01:24:13.450217      192.168.1.2.36534 > 192.168.1.200.23: S 2986077586:
   2986077586(0) win 29200 <mss 1460,sackOK,timestamp 3484652 0,nop,wscale 7>
```

```
4 packets shown
```

```
>
```

```
> show capture inside_telnet packet-number 2 trace
```

```
4 packets captured
```

```
2: 01:24:07.437965      192.168.1.2.36534 > 192.168.1.200.23: S 2986077586:
   2986077586(0) win 29200 <mss 1460,sackOK,timestamp 3483149 0,nop,wscale 7>
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 3
```

```
Type: NGIPS-MODE
```

```
Subtype: ngips-mode
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: DROP

Config:

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced deny tcp any any object-group TELNET rule-id  
268440576 event-log flow-start
```

```
access-list CSM_FW_ACL_ remark rule-id 268440576: ACCESS POLICY: AC Policy -  
Mandatory/1
```

```
access-list CSM_FW_ACL_ remark rule-id 268440576: L4 RULE: Shell Access
```

```
object-group service TELNET tcp
```

```
port-object eq telnet
```

Additional Information:

Result:

```
input-interface: INSIDE_INTERFACE
```

```
input-status: up
```

```
input-line-status: up
```

```
Action: drop
```

```
Drop-reason: (acl-drop) Flow is denied by configured rule
```

1 packet shown

>

```
> show inline-set
```

```
Inline-set INSIDE_OUTSIDE_PAIR
```

```
Mtu is 1500 bytes
```

```
Failsafe mode is on/activated
```

```
Failsecure mode is off
```

```
Tap mode is on
```

```
Propagate-link-state option is on
```

```
hardware-bypass mode is disabled
```

```
Interface-Pair[1]:
```

```
Interface: GigabitEthernet1/1 "INSIDE_INTERFACE"
```

```
Current-Status: UP
```

```
Interface: GigabitEthernet1/2 "OUTSIDE_INTERFACE"
```

```
Current-Status: UP
```

```
Bridge Group ID: 0
```

```
>
```

```
> show interface GigabitEthernet 1/1
```

```
Interface GigabitEthernet1/1 "INSIDE_INTERFACE", is up, line protocol is up
```

```
Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
```

```
Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
```

```
Input flow control is unsupported, output flow control is off
```

```
MAC address a46c.2ae4.6bc0, MTU 1500
```

```
IPS Interface-Mode: inline-tap, Inline-Set: INSIDE_OUTSIDE_PAIR
```

```
IP address unassigned
```

```
9241 packets input, 945431 bytes, 0 no buffer
```

```
Received 89 broadcasts, 0 runts, 0 giants
```

```
.
```

```
.
```

```
> show interface GigabitEthernet 1/2
```

```
Interface GigabitEthernet1/2 "OUTSIDE_INTERFACE", is up, line protocol is up
```

```
Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
```

```
Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
```

```
Input flow control is unsupported, output flow control is off
```

```
MAC address a46c.2ae4.6bc1, MTU 1500
```

```
IPS Interface-Mode: inline-tap, Inline-Set: INSIDE_OUTSIDE_PAIR
```

```
IP address unassigned
```

```
9065 packets input, 924609 bytes, 0 no buffer
```

```
Received 30 broadcasts, 0 runts, 0 giants
```



```
Switch(config)# monitor session 1 source interface gigabitEthernet 0/1
Switch(config)# monitor session 1 source interface gigabitEthernet 0/2
```

```
Switch(config)# monitor session 1 destination interface g0/8
```

```
> show nameif
```

Interface	Name	Security
GigabitEthernet1/1	PASSIVE_INTERFACE	0
Management1/1	diagnostic	0

```
>
```

```
> show interface GigabitEthernet 1/1
```

```
Interface GigabitEthernet1/1 "PASSIVE_INTERFACE", is up, line protocol is up
```

```
Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
```

```
Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
```

```
Input flow control is unsupported, output flow control is off
```

```
MAC address a46c.2ae4.6bc0, MTU 1500
```

```
IPS Interface-Mode: passive
```

```
IP address unassigned
```

```
289 packets input, 30173 bytes, 0 no buffer
```

```
Received 7 broadcasts, 0 runts, 0 giants
```

```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
0 pause input, 0 resume input
```

```
0 L2 decode drops
```

```
161 packets output, 17774 bytes, 0 underruns
```

```
0 pause output, 0 resume output
```

```
0 output errors, 0 collisions, 0 interface resets
```

```
0 late collisions, 0 deferred
```

```
0 input reset drops, 24 output reset drops
```

```
input queue (blocks free curr/low): hardware (991/894)
```

```
output queue (blocks free curr/low): hardware (1023/1018)
```

```
Traffic Statistics for "PASSIVE_INTERFACE":
```

```
104 packets input, 6520 bytes
```

```
0 packets output, 0 bytes
```

```
104 packets dropped
```

```
1 minute input rate 0 pkts/sec, 0 bytes/sec
```

```
1 minute output rate 0 pkts/sec, 0 bytes/sec
```

```
1 minute drop rate, 0 pkts/sec
```

```
5 minute input rate 0 pkts/sec, 0 bytes/sec
```

```
5 minute output rate 0 pkts/sec, 0 bytes/sec
```

```
5 minute drop rate, 0 pkts/sec
```

```
>
```

```
Switch# show running-config | include monitor
monitor session 1 source interface Gi0/1 - 2
monitor session 1 destination interface Gi0/8
Switch#
```

```
Switch# show monitor session 1
Session 1
-----
Type                : Local Session
Source Ports        :
    Both             : Gi0/1-2
Destination Ports   : Gi0/8
Encapsulation       : Native
    Ingress          : Disabled
```

```
Switch#
```

```
> capture telnet_inside trace interface INSIDE_INTERFACE match tcp any any eq 23
>
> show capture
capture telnet_inside type raw-data trace interface INSIDE_INTERFACE [Capturing - 0
bytes]
match tcp any any eq telnet
>
```

```
> show capture telnet_inside

13 packets captured

1: 01:56:01.756735      192.168.1.2.59358 > 192.168.1.200.23: S 1923550801:
   1923550801(0) win 29200 <mss 1460,sackOK,timestamp 2340482 0,nop,wscale 7>
2: 01:56:01.757101      192.168.1.2.59358 > 192.168.1.200.23: . ack 2745314499
   win 229 <nop,nop,timestamp 2340483 1541951>
3: 01:56:01.757239      192.168.1.2.59358 > 192.168.1.200.23: P 1923550802:
   1923550829(27) ack 2745314499 win 229 <nop,nop,timestamp 2340483 1541951>
.
.
<Output_Omitted_for_Brevity>
```

```
> show capture telnet_inside packet-number 1 trace
```

```
13 packets captured
```

```
1: 01:56:01.756735      192.168.1.2.59358 > 192.168.1.200.23: S 1923550801:  
1923550801(0) win 29200 <mss 1460,sackOK,timestamp 2340482 0,nop,wscale 7>
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 3
```

```
Type: NGIPS-MODE
```

```
Subtype: ngips-mode
```

```
Result: ALLOW
```

```
Config:
```

Additional Information:

The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: WOULD HAVE DROPPED

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced deny tcp any any object-group TELNET rule-id 268441600 event-log flow-start

access-list CSM_FW_ACL_ remark rule-id 268441600: ACCESS POLICY: AC Policy - Mandatory/1

access-list CSM_FW_ACL_ remark rule-id 268441600: L4 RULE: Shell Access

object-group service TELNET tcp

port-object eq telnet

Additional Information:

Result:

input-interface: INSIDE_INTERFACE

input-status: up

input-line-status: up

Action: Access-list would have dropped, but packet forwarded due to inline-tap

1 packet shown

>

```
> packet-tracer input INSIDE_INTERFACE tcp 192.168.1.2 10000 192.168.1.200 23
```

```
Phase: 1
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: NGIPS-MODE
```

```
Subtype: ngips-mode
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
The flow ingresses an interface configured for NGIPS mode and NGIPS services will be applied
```

```
Phase: 3
```

```
Type: ACCESS-LIST
```

```
Subtype: log
```

```
Result: WOULD HAVE DROPPED
```

```
Config:
```

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced deny tcp any any object-group TELNET rule-id 268441600 event-log flow-start
```

```
access-list CSM_FW_ACL_ remark rule-id 268441600: ACCESS POLICY: AC Policy - Mandatory/1
```

```
access-list CSM_FW_ACL_ remark rule-id 268441600: L4 RULE: Shell Access
```

```
object-group service TELNET tcp
```

```
port-object eq telnet
```

```
Additional Information:
```

```
Result:
```

```
input-interface: INSIDE_INTERFACE
```

```
input-status: up
```

```
input-line-status: up
```

```
Action: Access-list would have dropped, but packet forwarded due to inline-tap
```

```
>
```

```
> show capture telnet_inside packet-number 1 trace
```

```
36 packets captured
```

```
1: 19:39:24.086177      192.168.1.2.40744 > 192.168.1.200.23: S 2884265905:  
2884265905(0) win 29200 <mss 1460,sackOK,timestamp 6199376 0,nop,wscale 7>
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 3
```

```
Type: NGIPS-MODE
```

```
Subtype: ngips-mode
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be  
applied
```

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434432

access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: AC Policy -
Default/1

access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: NGIPS-EGRESS-INTERFACE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

Ingress interface INSIDE_INTERFACE is in NGIPS inline mode.

Egress interface OUTSIDE_INTERFACE is determined by inline-set configuration

Phase: 6

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 257, packet dispatched to next module

```
Phase: 7
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'
```

```
Phase: 8
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Verdict: (block-packet) drop this packet
```

```
Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: Access-list would have dropped, but packet forwarded due to inline-tap
```

```
1 packet shown
>
```



```
> capture gre_traffic trace interface INSIDE_INTERFACE match gre any any
> capture telnet_traffic trace interface INSIDE_INTERFACE match tcp any any eq 23
```

```
> show capture
capture gre_traffic type raw-data trace interface INSIDE_INTERFACE [Capturing - 0
bytes]
match gre any any
capture telnet_traffic type raw-data trace interface INSIDE_INTERFACE [Capturing - 0
bytes]
match tcp any any eq telnet
>
```

```
> show capture
capture gre_traffic type raw-data trace interface INSIDE_INTERFACE [Capturing - 0
bytes]
match gre any any
capture telnet_traffic type raw-data trace interface INSIDE_INTERFACE
[Capturing - 3572 bytes]
match tcp any any eq telnet
>
```

```
> show capture
capture gre_traffic type raw-data trace interface INSIDE_INTERFACE [Capturing - 4748
bytes]
match gre any any
capture telnet_traffic type raw-data trace interface INSIDE_INTERFACE
[Capturing - 3572 bytes]
match tcp any any eq telnet
>
```

```
> show access-control-config

===== [ AC Policy ] =====
Description          :
Default Action       : Allow
Default Policy       : Balanced Security and Connectivity
Logging Configuration
  DC                  : Enabled
  Beginning           : Enabled
  End                 : Disabled
Rule Hits            : 0
Variable Set         : Default-Set
.
.
.
! Type 'q' to quit
<Output Omitted for Brevity>
```

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp
```

```
Please specify a client IP address:
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
! The following messages appear when you connect to 192.162.100.1/24 from the host 192.168.1.1/24 over the non-encapsulated path. It triggers the default action (rule id: 268434432) on the Access Control policy:
```

```
.  
192.168.1.1-43286 > 192.168.100.1-23 6 AS 5 I 1 New session  
192.168.1.1-43286 > 192.168.100.1-23 6 AS 5 I 1 using HW or preset rule order 2, id 268434432 action Allow and prefilter rule 0  
192.168.1.1-43286 > 192.168.100.1-23 6 AS 5 I 1 allow action  
192.168.1.1-43286 > 192.168.100.1-23 6 AS 5 I 1 Deleting session  
.  
.
```

```
! The following output appears when you connect to 192.162.200.1/24 from the host 192.168.2.1/24 over the GRE tunnel. It triggers the prefilter rule id 9998:
```

```
.  
192.168.2.1-23208 > 192.168.200.1-23 6 AS 5 I 0 New session  
192.168.2.1-23208 > 192.168.200.1-23 6 AS 5 I 0 using prefilter rule 9998 with tunnel zone -1  
192.168.2.1-23208 > 192.168.200.1-23 6 AS 5 I 0 Starting with minimum 0, id 0 and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff  
192.168.2.1-23208 > 192.168.200.1-23 6 AS 5 I 0 match rule order 2, id 268434432 action Allow  
192.168.2.1-23208 > 192.168.200.1-23 6 AS 5 I 0 allow action  
.  
.
```

```
<Output Omitted for Brevity>
```

```
> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list CSM_FW_ACL_; 6 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel
  and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998
  (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit 41 any any rule-id 9998 (hitcnt=0)
  0x06095aba
access-list CSM_FW_ACL_ line 5 advanced permit gre any any rule-id 9998 (hitcnt=3)
  0x52c7a066
access-list CSM_FW_ACL_ line 6 advanced permit udp any eq 3544 any range 1025 65535
  rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 7 advanced permit udp any range 1025 65535 any eq 3544
  rule-id 9998 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 8 remark rule-id 268434432: ACCESS POLICY: AC Policy -
  Default/1
access-list CSM_FW_ACL_ line 9 remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ line 10 advanced permit ip any any rule-id 268434432
  (hitcnt=2) 0xald3780e
>
```

```
> show capture telnet_traffic
```

```
49 packets captured
```

```
1: 12:57:33.942105      192.168.1.1.46774 > 192.168.100.1.23: S 636710801:
  636710801(0) win 4128 <mss 536>
2: 12:57:33.945706      192.168.100.1.23 > 192.168.1.1.46774: S 1516450804:
  1516450804(0) ack 636710802 win 4128 <mss 536>
3: 12:57:33.947140      192.168.1.1.46774 > 192.168.100.1.23: . ack 1516450805
  win 4128
4: 12:57:33.947186      192.168.1.1.46774 > 192.168.100.1.23: P 636710802:
  636710814(12) ack 1516450805 win 4128
```

```
.
.
```

```
<Output Omitted for Brevity>
```

```
> show capture telnet_traffic packet-number 1 trace
```

```
49 packets captured
```

```
1: 12:57:33.942105 192.168.1.1.46774 > 192.168.100.1.23: S 636710801:  
636710801(0) win 4128 <mss 536>
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 3
```

```
Type: NGIPS-MODE
```

```
Subtype: ngips-mode
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be  
applied
```

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434432

access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: AC Policy -
Default/1

access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: NGIPS-EGRESS-INTERFACE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

Ingress interface INSIDE_INTERFACE is in NGIPS inline mode.

Egress interface OUTSIDE_INTERFACE is determined by inline-set configuration

Phase: 6

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 102, packet dispatched to next module

```
Phase: 7
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'
```

```
Phase: 8
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet
```

```
Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: allow
```

```
1 packet shown
>
```

```
> show capture gre_traffic
```

```
49 packets captured
```

```
1: 12:59:01.441536      203.0.113.1 > 203.0.113.100: ip-proto-47, length 48
2: 12:59:01.444190      203.0.113.100 > 203.0.113.1: ip-proto-47, length 48
3: 12:59:01.446525      203.0.113.1 > 203.0.113.100: ip-proto-47, length 44
4: 12:59:01.446571      203.0.113.1 > 203.0.113.100: ip-proto-47, length 56
5: 12:59:01.446601      203.0.113.1 > 203.0.113.100: ip-proto-47, length 44
6: 12:59:01.449378      203.0.113.100 > 203.0.113.1: ip-proto-47, length 44
7: 12:59:01.450156      203.0.113.100 > 203.0.113.1: ip-proto-47, length 56
8: 12:59:01.450217      203.0.113.100 > 203.0.113.1: ip-proto-47, length 84
```

```
.
.
<Output Omitted for Brevity>
```

```
> show capture gre_traffic packet-number 1 trace
```

```
49 packets captured
```

```
1: 12:59:01.441536 203.0.113.1 > 203.0.113.100: ip-proto-47, length 48
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 3
```

```
Type: NGIPS-MODE
```

```
Subtype: ngips-mode
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied
```

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998

access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy

access-list CSM_FW_ACL_ remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: NGIPS-EGRESS-INTERFACE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

Ingress interface INSIDE_INTERFACE is in NGIPS inline mode.

Egress interface OUTSIDE_INTERFACE is determined by inline-set configuration

Phase: 6

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 103, packet dispatched to next module

Phase: 7
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 8
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet

Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: allow

1 packet shown

>

```
! The non-encapsulated traffic from 192.168.1.1 to 192.168.100.1 is allowed by a rule (id 268434432).
```

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp
```

```
Please specify a client IP address:
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
! An action on the traffic from 192.168.1.1 to 192.168.100.1 is logged below:
```

```
192.168.1.1-36257 > 192.168.100.1-23 6 AS 5 I 0 New session
```

```
192.168.1.1-36257 > 192.168.100.1-23 6 AS 5 I 0 using HW or preset rule order 2, id 268434432 action Allow and prefilter rule 0
```

```
192.168.1.1-36257 > 192.168.100.1-23 6 AS 5 I 0 allow action
```

```
192.168.1.1-36257 > 192.168.100.1-23 6 AS 5 I 0 Deleting session
```

```
! Traffic from 192.168.2.1 to 192.168.200.1 does not appear here; because they are encapsulated and therefore, blocked by the Prefilter policy.
```

```
^c
```

```
Caught interrupt signal
```

```
Exiting.
```

```
>
```

```
> show access-list
```

```
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
```

```
    alert-interval 300
```

```
access-list CSM_FW_ACL_ ; 6 elements; name hash: 0x4a69e3f3
```

```
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
```

```
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
```

```
access-list CSM_FW_ACL_ line 3 advanced deny ipinip any any rule-id 9998 event-log flow-start (hitcnt=0) 0x128a09cb
```

```
access-list CSM_FW_ACL_ line 4 advanced deny 41 any any rule-id 9998 event-log flow-start (hitcnt=0) 0x6e21b1ba
```

```
access-list CSM_FW_ACL_ line 5 advanced deny gre any any rule-id 9998 event-log flow-start (hitcnt=4) 0xe9c037af
```

```
access-list CSM_FW_ACL_ line 6 advanced deny udp any eq 3544 any range 1025 65535 rule-id 9998 event-log flow-start (hitcnt=0) 0x77ac07e0
```

```
access-list CSM_FW_ACL_ line 7 advanced deny udp any range 1025 65535 any eq 3544 rule-id 9998 event-log flow-start (hitcnt=0) 0x3054708b
```

```
access-list CSM_FW_ACL_ line 8 remark rule-id 268434432: ACCESS POLICY: AC Policy - Default/1
```

```
access-list CSM_FW_ACL_ line 9 remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
```

```
access-list CSM_FW_ACL_ line 10 advanced permit ip any any rule-id 268434432 (hitcnt=12) 0xa1d3780e
```

```
>
```

```
> show capture gre_traffic
```

```
4 packets captured
```

```
  1: 18:46:45.801670      203.0.113.1 > 203.0.113.100: ip-proto-47, length 48  
  2: 18:46:47.802708      203.0.113.1 > 203.0.113.100: ip-proto-47, length 48  
  3: 18:46:51.802952      203.0.113.1 > 203.0.113.100: ip-proto-47, length 48  
  4: 18:46:59.803165      203.0.113.1 > 203.0.113.100: ip-proto-47, length 48
```

```
4 packets shown
```

```
>
```

```
> show capture gre_traffic packet-number 1 trace
```

```
4 packets captured
```

```
  1: 18:46:45.801670      203.0.113.1 > 203.0.113.100: ip-proto-47, length 48
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 3
```

```
Type: NGIPS-MODE
```

```
Subtype: ngips-mode
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
The flow ingresses an interface configured for NGIPS mode and NGIPS services will be applied
```

```
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny gre any any rule-id 9998 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY: Default Tunnel and
Priority Policy
access-list CSM_FW_ACL_ remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
Additional Information:

Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule

1 packet shown
>
```

```
> clear conn address IP_Address_of_a_Host
```

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp
```

```
Please specify a client IP address:
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
! Traffic from 192.168.1.1 to 192.168.100.1 is non-encapsulated, therefore it is inspected by a rule (id 268434432).
```

```
192.168.1.1-40591 > 192.168.100.1-23 6 AS 5 I 1 New session
```

```
192.168.1.1-40591 > 192.168.100.1-23 6 AS 5 I 1 using HW or preset rule order 3, id 268434432 action Allow and prefilter rule 0
```

```
192.168.1.1-40591 > 192.168.100.1-23 6 AS 5 I 1 allow action
```

```
192.168.1.1-40591 > 192.168.100.1-23 6 AS 5 I 1 Deleting session
```

```
! Traffic from 192.168.2.1 to 192.168.200.1 are transferred over a GRE tunnel. Therefore, they are bypassed from any further inspection, and do not appear here in the firewall-engine-debug output.
```

```
^C
```

```
Caught interrupt signal
```

```
Exiting.
```

```
>
```

```
> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list CSM_FW_ACL_ ; 7 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 268438530: PREFILTER POLICY: Custom
      Tunnel and Prefilter Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 268438530: RULE: GRE Tunnel Rule
access-list CSM_FW_ACL_ line 3 advanced trust gre any any rule-id 268438530
      event-log both (hitcnt=3) 0xbc125eb0
access-list CSM_FW_ACL_ line 4 remark rule-id 268438529: PREFILTER POLICY: Custom
      Tunnel and Prefilter Policy
access-list CSM_FW_ACL_ line 5 remark rule-id 268438529: RULE: DEFAULT TUNNEL ACTION
      RULE
access-list CSM_FW_ACL_ line 6 advanced permit ipinip any any rule-id 268438529
      (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 7 advanced permit 41 any any rule-id 268438529
      (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 8 advanced permit gre any any rule-id 268438529
      (hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL_ line 9 advanced permit udp any eq 3544 any range 1025 65535
      rule-id 268438529 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 10 advanced permit udp any range 1025 65535 any eq 3544
      rule-id 268438529 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 11 remark rule-id 268434432: ACCESS POLICY: AC Policy -
      Default/1
access-list CSM_FW_ACL_ line 12 remark rule-id 268434432: L4 RULE: DEFAULT ACTION
      RULE
access-list CSM_FW_ACL_ line 13 advanced permit ip any any rule-id 268434432
      (hitcnt=16) 0xald3780e
>
```

```
> show capture gre_traffic
```

```
49 packets captured
```

```
  1: 01:17:27.046475      203.0.113.1 > 203.0.113.100: ip-proto-47, length 48  
  2: 01:17:27.048871      203.0.113.100 > 203.0.113.1: ip-proto-47, length 48  
  3: 01:17:27.050397      203.0.113.1 > 203.0.113.100: ip-proto-47, length 44
```

```
.
```

```
.
```

```
<Output Omitted for Brevity>
```

```
> show capture gre_traffic packet-number 1 trace
```

```
49 packets captured
```

```
  1: 01:17:27.046475      203.0.113.1 > 203.0.113.100: ip-proto-47, length 48
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 3

Type: NGIPS-MODE

Subtype: ngips-mode

Result: ALLOW

Config:

Additional Information:

The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced trust gre any any rule-id 268438530 event-log both

access-list CSM_FW_ACL_ remark rule-id 268438530: PREFILTER POLICY: Custom Tunnel
and Prefilter Policy

access-list CSM_FW_ACL_ remark rule-id 268438530: RULE: GRE Tunnel Rule

Additional Information:

Phase: 5
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Ingress interface INSIDE_INTERFACE is in NGIPS inline mode.
Egress interface OUTSIDE_INTERFACE is determined by inline-set configuration

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 131, packet dispatched to next module

Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: allow

1 packet shown

>

```
> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list CSM_FW_ACL_ ; 7 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 268440577: PREFILTER POLICY: Custom
      Tunnel and Prefilter Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 268440577: RULE: Shell Prefilter
access-list CSM_FW_ACL_ line 3 advanced trust tcp object Corporate-Network any
      object-group SSH rule-id 268440577 event-log both (hitcnt=0) 0xe9257885

access-list CSM_FW_ACL_ line 3 advanced trust tcp 192.168.1.0 255.255.255.0 any eq
      ssh rule-id 268440577 event-log both (hitcnt=0) 0xad5d48f9
access-list CSM_FW_ACL_ line 4 remark rule-id 268438529: PREFILTER POLICY: Custom
      Tunnel and Prefilter Policy
access-list CSM_FW_ACL_ line 5 remark rule-id 268438529: RULE: DEFAULT TUNNEL ACTION
      RULE
access-list CSM_FW_ACL_ line 6 advanced permit ipinip any any rule-id 268438529
      (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 7 advanced permit 41 any any rule-id 268438529
      (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 8 advanced permit gre any any rule-id 268438529
      (hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL_ line 9 advanced permit udp any eq 3544 any range 1025 65535
      rule-id 268438529 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 10 advanced permit udp any range 1025 65535 any eq 3544
      rule-id 268438529 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 11 remark rule-id 268434432: ACCESS POLICY: AC Policy -
      Default/1
access-list CSM_FW_ACL_ line 12 remark rule-id 268434432: L4 RULE: DEFAULT ACTION
      RULE
access-list CSM_FW_ACL_ line 13 advanced permit ip any any rule-id 268434432
      (hitcnt=34) 0xald3780e
>
```

```
> capture ssh_traffic trace interface INSIDE_INTERFACE match tcp any
any eq 22
```

```
> show capture
```

```
capture ssh_traffic type raw-data trace interface INSIDE_INTERFACE
      [Capturing - 0 bytes]
      match tcp any any eq ssh
```

```
>
```

```
> capture-traffic
```

```
Please choose domain to capture traffic from:
```

- 0 - br1
- 1 - INSIDE_OUTSIDE_PAIR inline set

```
Selection? 1
```

```
Please specify tcpdump options desired.  
(or enter '?' for a list of supported options)
```

```
Options: -n tcp
```

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp  
Please specify a client IP address:  
Please specify a client port:  
Please specify a server IP address:  
Please specify a server port:  
Monitoring firewall engine debug messages
```

```
! The firewall-engine-debug tool receives events from hardware in real time.
```

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp  
Please specify a client IP address:  
Please specify a client port:  
Please specify a server IP address:  
Please specify a server port:  
Monitoring firewall engine debug messages
```

```
192.168.1.2-48506 > 192.168.1.200-22 6 AS 5 I 0 Got start of flow event from  
hardware with flags 84000001
```

```
192.168.1.2-48506 > 192.168.1.200-22 6 AS 5 I 0 Got end of flow event from hardware  
with flags 84000001
```

```
^C
```

```
Caught interrupt signal  
Exiting.
```

```
>
```

```
! The Snort statistics keeps a record of these events under the Miscellaneous  
Counters section.
```

```
> show snort statistics
```

```
Packet Counters:
```

```
  Passed Packets                                0
  Blocked Packets                              0
  Injected Packets                             0
```

```
Flow Counters:
```

```
  Fast-Forwarded Flows                        0
  Blacklisted Flows                           0
  Flows bypassed (Snort Down)                 0
  Flows bypassed (Snort Busy)                 0
```

```
Miscellaneous Counters:
```

```
  Start-of-Flow events                        1
  End-of-Flow events                          1
  Denied flow events                          0
  Frames forwarded to Snort before drop       0
  Inject packets dropped                       0
```

```
>
```

```
> capture-traffic
```

```
Please choose domain to capture traffic from:
```

- 0 - br1
- 1 - INSIDE_OUTSIDE_PAIR inline set

```
Selection? 1
```

```
Please specify tcpdump options desired.
```

```
(or enter '?' for a list of supported options)
```

```
Options: -n tcp
```

```
! If the Firepower Snort engine would see traffic, it would appear here.
```

```
! Press the Control+C keys to exit from the capture-traffic tool.
```

```
^C
```

```
Caught interrupt signal
```

```
Exiting.
```

! Check the status of the capture on the ASA Firewall engine.

```
> show capture ssh_traffic
```

61 packets captured

```
1: 13:00:22.730156      192.168.1.2.48506 > 192.168.1.200.22: S 1199563799:
  1199563799(0) win 29200 <mss 1460,sackOK,timestamp 4732110 0,nop,wscale 7>
2: 13:00:22.730492      192.168.1.200.22 > 192.168.1.2.48506: S 2739603340:
  2739603340(0) ack 1199563800 win 28960 <mss 1460,sackOK,timestamp 1446067
  4732110,nop,wscale 7>
3: 13:00:22.730659      192.168.1.2.48506 > 192.168.1.200.22: . ack 2739603341
  win 229 <nop,nop,timestamp 4732110 1446067>
4: 13:00:22.730949      192.168.1.2.48506 > 192.168.1.200.22: P 1199563800:
  1199563841(41) ack 2739603341 win 229 <nop,nop,timestamp 4732110 1446067>
5: 13:00:22.731132      192.168.1.200.22 > 192.168.1.2.48506: . ack 1199563841
  win 227 <nop,nop,timestamp 1446067 4732110>
```

.
.

! You can see all of the SSH packets generated by your connection. The above output shows only the first TCP three way handshake, as an example. The remaining outputs are omitted for brevity.

```
> show capture ssh_traffic packet-number 1 trace
```

61 packets captured

```
1: 13:00:22.730156      192.168.1.2.48506 > 192.168.1.200.22: S 1199563799:
  1199563799(0) win 29200 <mss 1460,sackOK,timestamp 4732110 0,nop,wscale 7>
```

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

MAC Access list

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

```
Phase: 3
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be
  applied

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced trust tcp object Corporate-Network any object-group
  SSH rule-id 268440577 event-log both
access-list CSM_FW_ACL_ remark rule-id 268440577: PREFILTER POLICY: Custom Tunnel
  and Prefilter Policy
access-list CSM_FW_ACL_ remark rule-id 268440577: RULE: Shell Prefilter
object-group service SSH tcp
  port-object eq ssh
Additional Information:

Phase: 5
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Ingress interface INSIDE_INTERFACE is in NGIPS inline mode.
Egress interface OUTSIDE_INTERFACE is determined by inline-set configuration

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 81, packet dispatched to next module

Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: allow

1 packet shown
>
```

```

> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
    alert-interval 300
access-list CSM_FW_ACL_ ; 8 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 268440577: PREFILTER POLICY: Custom
    Tunnel and Prefilter Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 268440577: RULE: Shell Prefilter
access-list CSM_FW_ACL_ line 3 advanced trust tcp object Corporate-Network any
    object-group SSH rule-id 268440577 event-log both (hitcnt=4) 0xe9257885
    access-list CSM_FW_ACL_ line 3 advanced trust tcp 192.168.1.0 255.255.255.0 any eq
        ssh rule-id 268440577 event-log both (hitcnt=4) 0xad5d48f9
access-list CSM_FW_ACL_ line 4 remark rule-id 268438529: PREFILTER POLICY: Custom
    Tunnel and Prefilter Policy
access-list CSM_FW_ACL_ line 5 remark rule-id 268438529: RULE: DEFAULT TUNNEL ACTION
    RULE
access-list CSM_FW_ACL_ line 6 advanced permit ipinip any any rule-id 268438529
    (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 7 advanced permit 41 any any rule-id 268438529
    (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 8 advanced permit gre any any rule-id 268438529
    (hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL_ line 9 advanced permit udp any eq 3544 any range 1025 65535
    rule-id 268438529 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 10 advanced permit udp any range 1025 65535 any eq 3544
    rule-id 268438529 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 11 remark rule-id 268440580: ACCESS POLICY: AC Policy -
    Mandatory/1
access-list CSM_FW_ACL_ line 12 remark rule-id 268440580: L7 RULE: Telnet Access
access-list CSM_FW_ACL_ line 13 advanced permit tcp object Corporate-Network any
    object-group TELNET rule-id 268440580 (hitcnt=3) 0x388a3b9d
access-list CSM_FW_ACL_ line 13 advanced permit tcp 192.168.1.0 255.255.255.0 any eq
    telnet rule-id 268440580 (hitcnt=3) 0x4a6c1f4c
access-list CSM_FW_ACL_ line 14 remark rule-id 268434432: ACCESS POLICY: AC Policy -
    Default/1
access-list CSM_FW_ACL_ line 15 remark rule-id 268434432: L4 RULE: DEFAULT ACTION
    RULE
access-list CSM_FW_ACL_ line 16 advanced permit ip any any rule-id 268434432
    (hitcnt=144) 0xald3780e
>
> capture telnet_traffic trace interface INSIDE_INTERFACE match tcp any
any eq 23
> show capture
capture telnet_traffic type raw-data trace interface INSIDE_INTERFACE
    [Capturing - 0 bytes]
    match tcp any any eq telnet
>

```

```
> capture-traffic
```

```
Please choose domain to capture traffic from:
```

- 0 - br1
- 1 - INSIDE_OUTSIDE_PAIR inline set

```
Selection? 1
```

```
Please specify tcpdump options desired.  
(or enter '?' for a list of supported options)
```

```
Options: -n tcp
```

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp  
Please specify a client IP address:  
Please specify a client port:  
Please specify a server IP address:  
Please specify a server port:  
Monitoring firewall engine debug messages
```

```
! The firewall-engine-debug tool shows that the "Telnet Access" rule applies Trust action.
```

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp  
Please specify a client IP address:  
Please specify a client port:  
Please specify a server IP address:  
Please specify a server port:  
  
Monitoring firewall engine debug messages
```

```
192.168.1.2-55822 > 192.168.1.200-23 6 AS 5 I 1 New session  
192.168.1.2-55822 > 192.168.1.200-23 6 AS 5 I 1 using HW or preset rule order 3,  
'Telnet Access', action Trust and prefilter rule 0  
192.168.1.2-55822 > 192.168.1.200-23 6 AS 5 I 1 Deleting session
```

```
^c
```

```
Caught interrupt signal  
Exiting.
```

```
>
```



```
! The Firepower Snort engine stops seeing traffic after the initial TCP three-way handshake.
```

```
> capture-traffic
```

```
Please choose domain to capture traffic from:
```

- 0 - br1
- 1 - INSIDE_OUTSIDE_PAIR inline set

```
Selection? 1
```

```
Please specify tcpdump options desired.
```

```
(or enter '?' for a list of supported options)
```

```
Options: -n tcp
```

```
17:19:49.089991 IP 192.168.1.2.55822 > 192.168.1.200.23: Flags [S], seq 1700253547, win 29200, options [mss 1460,sackOK,TS val 7177698 ecr 0,nop,wscale 7], length 0
```

```
17:19:49.089991 IP 192.168.1.200.23 > 192.168.1.2.55822: Flags [S.], seq 495495803, ack 1700253548, win 28960, options [mss 1460,sackOK,TS val 3421593 ecr 7177698, nop,wscale 7], length 0
```

```
17:19:49.109979 IP 192.168.1.2.55822 > 192.168.1.200.23: Flags [.), ack 1, win 229, options [nop,nop,TS val 7177701 ecr 3421593], length 0
```

```
17:19:49.109979 IP 192.168.1.2.55822 > 192.168.1.200.23: Flags [P.), ack 1, win 229, options [nop,nop,TS val 7177701 ecr 3421593], length 27
```

```
! Nothing appears after the above packets, because they are trusted.
```

```
^C
```

```
Caught interrupt signal
```

```
Exiting.
```

>

! However, the ASA Firewall engine sees all of the traffic generated by the telnet connection.

> show capture telnet_traffic

78 packets captured

```
1: 17:19:49.096766      192.168.1.2.55822 > 192.168.1.200.23: S 1700253547:
   1700253547(0) win 29200 <mss 1460,sackOK,timestamp 7177698 0,nop,wscale 7>
2: 17:19:49.109781      192.168.1.200.23 > 192.168.1.2.55822: S 495495803:
   495495803(0) ack 1700253548 win 28960 <mss 1460,sackOK,timestamp 3421593
   7177698,nop,wscale 7>
3: 17:19:49.110086      192.168.1.2.55822 > 192.168.1.200.23: . ack 495495804
   win 229 <nop,nop,timestamp 7177701 3421593>
4: 17:19:49.110391      192.168.1.2.55822 > 192.168.1.200.23: P 1700253548:
   1700253575(27) ack 495495804 win 229 <nop,nop,timestamp 7177701 3421593>
5: 17:19:49.110651      192.168.1.200.23 > 192.168.1.2.55822: . ack 1700253575
   win 227 <nop,nop,timestamp 3421596 7177701>
6: 17:19:49.116037      192.168.1.200.23 > 192.168.1.2.55822: P 495495804:
   495495816(12) ack 1700253575 win 227 <nop,nop,timestamp 3421597 7177701>
7: 17:19:49.116159      192.168.1.2.55822 > 192.168.1.200.23: . ack 495495816
   win 229 <nop,nop,timestamp 7177703 3421597>
```

.

.

! Output is Omitted for Brevity

```
> show capture telnet_traffic packet-number 1 trace
```

```
78 packets captured
```

```
1: 17:19:49.096766      192.168.1.2.55822 > 192.168.1.200.23: S 1700253547:  
1700253547(0) win 29200 <mss 1460,sackOK,timestamp 7177698 0,nop,wscale 7>
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

Phase: 3

Type: NGIPS-MODE

Subtype: ngips-mode

Result: ALLOW

Config:

Additional Information:

The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced permit tcp object Corporate-Network any
object-group TELNET rule-id 268440580

access-list CSM_FW_ACL_ remark rule-id 268440580: ACCESS POLICY: AC Policy -
Mandatory/1

access-list CSM_FW_ACL_ remark rule-id 268440580: L7 RULE: Telnet Access

object-group service TELNET tcp

port-object eq telnet

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: NGIPS-EGRESS-INTERFACE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

Ingress interface INSIDE_INTERFACE is in NGIPS inline mode.

Egress interface OUTSIDE_INTERFACE is determined by inline-set configuration

Phase: 6

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 282, packet dispatched to next module

Phase: 7
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 8
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet

Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: allow

1 packet shown
>

```
! Packet Number 3:
```

```
> show capture telnet_traffic packet-number 3 trace
```

```
78 packets captured
```

```
3: 17:19:49.110086      192.168.1.2.55822 > 192.168.1.200.23: . ack 495495804  
win 229 <nop,nop,timestamp 7177701 3421593>
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

Phase: 3

Type: FLOW-LOOKUP

Subtype:

Result: ALLOW

Config:

Additional Information:

Found flow with id 282, using existing flow

Phase: 4

Type: EXTERNAL-INSPECT

Subtype:

Result: ALLOW

Config:

Additional Information:

Application: 'SNORT Inspect'

Phase: 5

Type: SNORT

Subtype:

Result: ALLOW

Config:

Additional Information:

Snort Verdict: (fast-forward) fast forward this flow

```
Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: allow

1 packet shown
>

! Packet Number 4:

> show capture telnet_traffic packet-number 4 trace

78 packets captured

  4: 17:19:49.110391      192.168.1.2.55822 > 192.168.1.200.23: P 1700253548:
    1700253575(27) ack 495495804 win 229 <nop,nop,timestamp 7177701 3421593>
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list
.
.
! Output is Omitted for Brevity
.
.
Phase: 5
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (fast-forward) fast forward this flow

Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: allow

1 packet shown
>
```


! The Snort statistics keep a record of these events using two types of counters.

> show snort statistics

Packet Counters:

Passed Packets	2
Blocked Packets	0
Injected Packets	0

Flow Counters:

Fast-Forwarded Flows	1
Blacklisted Flows	0
Flows bypassed (Snort Down)	0
Flows bypassed (Snort Busy)	0

Miscellaneous Counters:

Start-of-Flow events	0
End-of-Flow events	0
Denied flow events	0
Frames forwarded to Snort before drop	0
Inject packets dropped	0

>

> show snort statistics

Packet Counters:

Passed Packets	78
Blocked Packets	0
Injected Packets	0

Flow Counters:

Fast-Forwarded Flows	0
Blacklisted Flows	0
Flows bypassed (Snort Down)	0
Flows bypassed (Snort Busy)	0

Miscellaneous Counters:

Start-of-Flow events	0
End-of-Flow events	0
Denied flow events	0
Frames forwarded to Snort before drop	0
Inject packets dropped	0

>

! To view the rate-limiting settings:

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
    no tcp-inspection
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
  parameters
    eool action allow
    nop action allow
    router-alert action allow
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect rsh
    inspect rtsp
    inspect sqlnet
    inspect skinny
```

```
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect icmp
inspect icmp error
inspect dcerpc
inspect ip-options UM_STATIC_IP_OPTIONS_MAP
class class-default
  set connection advanced-options UM_STATIC_TCP_MAP
policy-map policy_map_INSIDE_INTERFACE
  match flow-rule qos 268442624
  police input 8000000 250000
  police output 40000000 1250000
!
```

! To determine where a policy is applied:

```
> show running-config service-policy
service-policy global_policy global
service-policy policy_map_INSIDE_INTERFACE interface INSIDE_INTERFACE
>
```

```
! Record on the service policy statistics
```

```
> show service-policy police
```

```
Interface INSIDE_INTERFACE:
```

```
Service-policy: policy_map_INSIDE_INTERFACE
```

```
Flow-rule QoS id: 268442624
```

```
Input police Interface INSIDE_INTERFACE:
```

```
  cir 8000000 bps, bc 250000 bytes
```

```
  conformed 334152 packets, 21168506 bytes; actions: transmit
```

```
  exceeded 0 packets, 0 bytes; actions: drop
```

```
  conformed 473456 bps, exceed 0 bps
```

```
Output police Interface INSIDE_INTERFACE:
```

```
  cir 40000000 bps, bc 1250000 bytes
```

```
  conformed 1129736 packets, 1618239735 bytes; actions: transmit
```

```
  exceeded 127629 packets, 182986654 bytes; actions: drop
```

```
  conformed 36194128 bps, exceed 4092744 bps
```

```
>
```

```
! Statistics of the Accelerated Security Path (ASP) counts
```

```
> show asp drop
```

```
Frame drop:
```

No route to host (no-route)	79
TCP packet SEQ past window (tcp-seq-past-win)	1
Output QoS rate exceeded (rate-exceeded)	127629
Slowpath security checks failed (sp-security-failed)	4
FP L2 rule drop (l2_acl)	18

```
Last clearing: 00:51:31 UTC Apr 10 2017 by enable_1
```

```
Flow drop:
```

```
Last clearing: 00:51:31 UTC Apr 10 2017 by enable_1
```

```
>
```

! You can use a QoS Rule ID to view any associated active connections.

```
> show conn flow-rule qos 268442624
```

```
1 in use, 4 most used
```

```
TCP OUTSIDE_INTERFACE 172.16.1.2:80 INSIDE_INTERFACE 192.168.1.2:47072, idle  
0:00:00, bytes 1199375239, flags UIO N
```

```
>
```

! To determine the meaning of each flag, you can use the "detail" keyword. For example, the flag 'N' confirms that the Firepower Snort engine inspects the connection.

```
> show conn detail
```

```
1 in use, 4 most used
```

```
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,
```

```
    b - TCP state-bypass or nailed,
```

```
    C - CTIQBE media, c - cluster centralized,
```

```
    D - DNS, d - dump, E - outside back connection, e - semi-distributed,
```

```
    F - initiator FIN, f - responder FIN,
```

```
    G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
```

```
    i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
```

```
    k - Skinny media, M - SMTP data, m - SIP media, N - inspected by Snort, n - GUP
```

```
    O - responder data, P - inside back connection,
```

```
    q - SQL*Net data, R - initiator acknowledged FIN,
```

```
    R - UDP SUNRPC, r - responder acknowledged FIN,
```

```
    T - SIP, t - SIP transient, U - up,
```

```
    V - VPN orphan, v - M3UA W - WAAS,
```

```
    w - secondary domain backup,
```

```
    X - inspected by service module,
```

```
    x - per session, Y - director stub flow, y - backup stub flow,
```

```
    Z - Scansafe redirection, z - forwarding stub flow
```

```
TCP OUTSIDE_INTERFACE: 172.16.1.2/80 INSIDE_INTERFACE: 192.168.1.2/47072,
```

```
    flags UIO N, qos-rule-id 268442624, idle 0s, uptime 4m42s, timeout 1h0m, bytes  
1529246551
```

```
>
```

```
! Debug messages in the ASA Firewall Engine:
```

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp
```

```
Please specify a client IP address:
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
192.168.1.2-47072 > 172.16.1.2-80 6 AS 1 I 0 New session
```

```
192.168.1.2-47072 > 172.16.1.2-80 6 AS 1 I 0 using HW or preset rule order 2, id  
268434432 action Allow and prefilter rule 0
```

```
192.168.1.2-47072 > 172.16.1.2-80 6 AS 1 I 0 allow action
```

```
192.168.1.2-47072 > 172.16.1.2-80 6 AS 1 I 0 Starting with minimum 0, id 0 and  
SrcZone first with zones 2 -> 1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 0,  
payload 0, client 0, misc 0, user 9999997, url , xff
```

```
192.168.1.2-47072 > 172.16.1.2-80 6 AS 1 I 0 match rule order 1, id 268442624 action  
Rate Limit
```

```
192.168.1.2-47072 > 172.16.1.2-80 6 AS 1 I 0 QoS policy match status (match found),  
match action (Rate Limit), QoS rule id (268442624)
```

```
192.168.1.2-47072 > 172.16.1.2-80 6 AS 1 I 0 Got end of flow event from hardware  
with flags 40000001
```

```
^c
```

```
Caught interrupt signal
```

```
Exiting.
```

```
>
```

```
! Debug messages in the Firepower Snort Engine:
```

```
> debug snort event
```

```
>
```

```
Flow from 192.168.1.2/47072 to 172.16.1.2/80 matched qos_rule_id 268442624 flag  
Regular flow
```

```
RL pkts = 0, RL Bytes = 0, Rv RL pkts = 153693, Rv RL Byt = 220395762, Qos_on_Src 1
```

```
> undebg all
```

```
>
```

```
> clear service-policy interface INSIDE_INTERFACE
```

```
> clear asp drop
```

! Right after a fresh installation, an FMC does not contain any blacklist files by default:

```
admin@FMC:~$ ls -halp /var/sf/iprep_download/
total 20K
drwxr-xr-x  5 www  www  4.0K Apr 28 01:22 ./
drwxr-xr-x 64 root root 4.0K Apr 28 02:20 ../
-rw-r--r--  1 www  www    0 Apr 28 01:22 IPRVersion.dat
drwxr-xr-x  2 www  www  4.0K Apr 28 01:22 health/
drwxr-xr-x  2 www  www  4.0K Apr 28 01:22 peers/
drwxr-xr-x  2 www  www  4.0K Apr 28 01:22 tmp/
admin@FMC:~$
```

! After updating the Cisco Intelligence Feed from the cloud, FMC shows the blacklist files:

```
admin@FMC:~$ ls -halp /var/sf/iprep_download/
total 7.3M
drwxr-xr-x  5 www  www  4.0K Apr 28 16:39 ./
drwxr-xr-x 64 root root 4.0K Apr 28 02:20 ../
-rw-r--r--  1 root root 225K Apr 28 16:23 032ba433-c295-11e4-a919-d4ae5275a468
-rw-r--r--  1 root root   37 Apr 28 16:23 1b117672-7453-478c-be31-b72e89calacb
-rw-r--r--  1 root root  43K Apr 28 16:23 23f2a124-8278-4c03-8c9d-d28fe08b5e98
-rw-r--r--  1 root root  5.3K Apr 28 16:23 2CCDA18E-DDFF-4F5C-AF9A-F009852183F4
-rw-r--r--  1 root root  9.4K Apr 28 16:23 2b15cb6f-a3fc-4e0e-a342-ccc5e5803263
-rw-r--r--  1 root root   52 Apr 28 16:23 30f9e69c-d64c-479c-821d-0e4edab8217a
-rw-r--r--  1 root root 682K Apr 28 16:23 3e2af68e-5fc8-4b1c-b5bc-b4e7cab598ba
-rw-r--r--  1 root root   48 Apr 28 16:23 5a0b6d6b-e2c3-436f-b4a1-48248b330a26
-rw-r--r--  1 root root   32 Apr 28 16:23 5f8148f1-e5e4-427a-aa3b-ee1c2745c350
-rw-r--r--  1 root root  47K Apr 28 16:23 60f4e2ab-d96c-44a0-bd38-830252b63f46
-rw-r--r--  1 root root   31 Apr 28 16:23 6ba968f4-7a25-4793-a2c8-7cc77f1ff437
-rw-r--r--  1 root root  165 Apr 28 16:23 A27C6AAE-8E52-4174-A81A-47C59FECC092
-rw-rw-r--  1 www  www   39 Apr 28 16:42 IPRVersion.dat
-rw-r--r--  1 root root  6.2M Apr 28 16:22 Sourcefire_Intelligence_Feed
-rw-r--r--  1 root root   30 Apr 28 16:23 b1df3aa8-2841-4c88-8e64-bfaacec7fedd
-rw-r--r--  1 root root  1.7K Apr 28 16:23 d7d996a6-6b92-4a56-8f10-e8506e431ca5
drwxr-xr-x  2 www  www  4.0K Apr 28 01:22 health/
drwxr-xr-x  2 www  www  4.0K Apr 28 01:22 peers/
-rw-r--r--  1 root root  4.6K Apr 28 16:22 rep_dd.yaml
drwxr-xr-x  2 www  www  4.0K Apr 28 16:32 tmp/
admin@FMC:~$
```

! After a fresh installation, FTD shows only the empty blacklist (.blf) and whitelist (.wlf) files. At this point, FMC has not applied a Cisco Intelligence Feed yet:

> expert

```
admin@firepower:~$ ls -halp /var/sf/iprep_download/
```

```
total 40K
```

```
drwxr-xr-x  5 www  www  4.0K Apr 28 10:44 ./
```

```
drwxr-xr-x 66 root  root  4.0K Dec 12 00:19 ../
```

```
-rw-rw-r--  1 www  www   118 Apr 28 10:17 .zones
```

```
-rw-rw-r--  1 www  www    17 Apr 28 10:44 IPRVersion.dat
```

```
-rw-r--r--  1 root  root   40 Apr 28 10:17 c76556bc-6167-11e1-88e8-479de99bdfd1.blf
```

```
-rw-r--r--  1 root  root   40 Apr 28 10:17 d8eea83e-6167-11e1-a154-589de99bdfd1.wlf
```

```
drwxr-xr-x  2 www  www  4.0K Sep 19 2016 health/
```

```
drwxr-xr-x  2 www  www  4.0K Sep 19 2016 peers/
```

```
drwxr-xr-x  2 www  www  4.0K Apr 28 10:44 tmp/
```

```
-rw-rw-r--  1 www  www   151 Apr 28 10:44 zone.info
```

```
admin@firepower:~$
```

! Upon a successful deployment of an Access Control policy, FTD received the necessary blacklist (.blf) and whitelist (.wlf) files from an FMC. Each of these files represent a Security Intelligence category.


```
admin@firepower:~$ ls -halp /var/sf/iprep_download/
total 1.1M
drwxr-xr-x  5 www  www  4.0K May  7 16:05 ./
drwxr-xr-x 66 root  root  4.0K Dec 12 00:19 ../
-rw-rw-r--  1 www  www  1003 May  7 16:04 .zones
-rw-r--r--  1 root  root  225K May  7 16:04 032ba433-c295-11e4-a919-d4ae5275a468.blf
-rw-r--r--  1 root  root   37 May  7 16:04 1b117672-7453-478c-be31-b72e89calacb.blf
-rw-r--r--  1 root  root  43K May  7 16:04 23f2a124-8278-4c03-8c9d-d28fe08b5e98.blf
-rw-r--r--  1 root  root  9.4K May  7 16:04 2b15cb6f-a3fc-4e0e-a342-ccc5e5803263.blf
-rw-r--r--  1 root  root  5.3K May  7 16:04 2ccda18e-ddff-4f5c-af9a-f009852183f4.blf
-rw-r--r--  1 root  root   52 May  7 16:04 30f9e69c-d64c-479c-821d-0e4edab8217a.blf
-rw-r--r--  1 root  root  682K May  7 16:04 3e2af68e-5fc8-4b1c-b5bc-b4e7cab598ba.blf
-rw-r--r--  1 root  root   48 May  7 16:04 5a0b6d6b-e2c3-436f-b4a1-48248b330a26.blf
-rw-r--r--  1 root  root   32 May  7 16:04 5f8148f1-e5e4-427a-aa3b-ee1c2745c350.blf
-rw-r--r--  1 root  root  47K May  7 16:04 60f4e2ab-d96c-44a0-bd38-830252b63f46.blf
-rw-r--r--  1 root  root   31 May  7 16:04 6ba968f4-7a25-4793-a2c8-7cc77f1ff437.blf
-rw-r--r--  1 root  root  373 May  7 16:04 808e55a2-2d33-11e7-ab29-ad43fb3c690a.blf
-rw-r--r--  1 root  root   17 May  7 16:04 IPRVersion.dat
-rw-r--r--  1 root  root  165 May  7 16:04 a27c6aae-8e52-4174-a81a-47c59fecc092.blf
-rw-r--r--  1 root  root   30 May  7 16:04 b1df3aa8-2841-4c88-8e64-bfaacec7fedd.blf
-rw-r--r--  1 root  root   40 May  7 16:04 c76556bc-6167-11e1-88e8-479de99bdfd1.blf
-rw-r--r--  1 root  root  1.7K May  7 16:04 d7d996a6-6b92-4a56-8f10-e8506e431ca5.blf
-rw-r--r--  1 root  root   53 May  7 16:04 d8eea83e-6167-11e1-a154-589de99bdfd1.wlf
drwxr-xr-x  2 www  www  4.0K Sep 19 2016 health/
drwxr-xr-x  2 www  www  4.0K May  7 14:26 peers/
drwxr-xr-x  2 www  www  4.0K May  7 16:04 tmp/
-rw-rw-r--  1 www  www  1006 May  7 16:04 zone.info
admin@firepower:~$
```

```
admin@firepower:~$ sudo tail -f /var/log/messages | grep -i reputation

May  7 16:05:40 ciscoasa SF-IMS[12223]:      Reputation Preprocessor: Size of shared
memory segment SFIPReputation.rt.0.0.1 is 134217728
May  7 16:05:40 ciscoasa SF-IMS[12223]:      Reputation entries loaded: 1, invalid:
0, re-defined: 0 (from file /ngfw/var/sf/iprep_download/d8eea83e-6167-11e1-a154-
589de99bdf1.wlf)
May  7 16:05:40 ciscoasa SF-IMS[12223]:      Reputation entries loaded: 0, invalid:
0, re-defined: 0 (from file /ngfw/var/sf/iprep_download/c76556bc-6167-11e1-88e8-
479de99bdf1.blf)
May  7 16:05:40 ciscoasa SF-IMS[12223]:      Reputation entries loaded: 25, invalid:
0, re-defined: 0 (from file /ngfw/var/sf/iprep_download/808e55a2-2d33-11e7-ab29-
ad43fb3c690a.blf)
May  7 16:05:40 ciscoasa SF-IMS[12223]:      Reputation entries loaded: 3310,
invalid: 0, re-defined: 7 (from file /ngfw/var/sf/iprep_download/60f4e2ab-d96c-
44a0-bd38-830252b63f46.blf)
May  7 16:05:40 ciscoasa SF-IMS[12223]:      Reputation entries loaded: 0, invalid:
0, re-defined: 0 (from file /ngfw/var/sf/iprep_download/6ba968f4-7a25-4793-a2c8-
7cc77f1ff437.blf)
May  7 16:05:40 ciscoasa SF-IMS[12223]:      Reputation entries loaded: 3050,
invalid: 0, re-defined: 1 (from file /ngfw/var/sf/iprep_download/23f2a124-8278-
4c03-8c9d-d28fe08b5e98.blf)
May  7 16:05:40 ciscoasa SF-IMS[12223]:      Reputation entries loaded: 112, invalid:
0, re-defined: 0 (from file /ngfw/var/sf/iprep_download/d7d996a6-6b92-4a56-8f10-
e8506e431ca5.blf)
May  7 16:05:40 ciscoasa SF-IMS[12223]:      Reputation entries loaded: 1, invalid:
0, re-defined: 0 (from file /ngfw/var/sf/iprep_download/5a0b6d6b-e2c3-436f-b4a1-
48248b330a26.blf)
May  7 16:05:40 ciscoasa SF-IMS[12223]:      Reputation entries loaded: 0, invalid:
0, re-defined: 0 (from file /ngfw/var/sf/iprep_download/5f8148f1-e5e4-427a-aa3b-
eelc2745c350.blf)
```

```

May  7 16:05:40 ciscoasa SF-IMS[12223]:      Reputation entries loaded: 676, invalid:
0, re-defined: 3 (from file /ngfw/var/sf/iprep_download/2b15cb6f-a3fc-4e0e-a342-
ccc5e5803263.blf)
May  7 16:05:40 ciscoasa SF-IMS[12223]:      Reputation entries loaded: 0, invalid:
0, re-defined: 0 (from file /ngfw/var/sf/iprep_download/1b117672-7453-478c-be31-
b72e89calacb.blf)
May  7 16:05:40 ciscoasa SF-IMS[12223]:      Reputation entries loaded: 1, invalid:
0, re-defined: 0 (from file /ngfw/var/sf/iprep_download/30f9e69c-d64c-479c-821d-
0e4edab8217a.blf)
May  7 16:05:40 ciscoasa SF-IMS[12223]:      Reputation entries loaded: 48044,
invalid: 0, re-defined: 0 (from file /ngfw/var/sf/iprep_download/3e2af68e-5fc8-
4b1c-b5bc-b4e7cab598ba.blf)
May  7 16:05:40 ciscoasa SF-IMS[12223]:      Reputation entries loaded: 15962,
invalid: 0, re-defined: 112 (from file /ngfw/var/sf/iprep_download/032ba433-c295-
11e4-a919-d4ae5275a468.blf)
May  7 16:05:40 ciscoasa SF-IMS[12223]:      Reputation entries loaded: 0, invalid:
0, re-defined: 0 (from file /ngfw/var/sf/iprep_download/b1df3aa8-2841-4c88-8e64-
bfaacec7fedd.blf)
May  7 16:05:40 ciscoasa SF-IMS[12223]:      Reputation entries loaded: 9, invalid:
0, re-defined: 0 (from file /ngfw/var/sf/iprep_download/a27c6aae-8e52-4174-a81a-
47c59fecc092.blf)
May  7 16:05:40 ciscoasa SF-IMS[12223]:      Reputation entries loaded: 377, invalid:
0, re-defined: 0 (from file /ngfw/var/sf/iprep_download/2ccda18e-ddff-4f5c-af9a-
f009852183f4.blf)
May  7 16:05:40 ciscoasa SF-IMS[12223]: Reputation Preprocessor shared memory
summary:
May  7 16:05:40 ciscoasa SF-IMS[12223]:      Reputation total memory usage: 9442496
bytes
May  7 16:05:40 ciscoasa SF-IMS[12223]:      Reputation total entries loaded: 71568,
invalid: 0, re-defined: 123
.
.
! <Output is Omitted for Brevity>

```

```
admin@firepower:~$ ls -halp /dev/shm/ | grep -i reputation
```

```
-rw-rw-rw-  1 root root 128M May  7 16:05 SFIPReputation.rt.0.0.1
```

```
admin@firepower:~$
```

```
admin@firepower:/var/sf/iprep_download$ egrep 209.222.77.220 *.blf
```

```
60f4e2ab-d96c-44a0-bd38-830252b63f46.blf:209.222.77.220
```

```
admin@firepower:/var/sf/iprep_download$
```

```
admin@firepower:/var/sf/iprep_download$ head -n1 60f4e2ab-d96c-44a0-
bd38-830252b63f46.blf
```

```
#Cisco intelligence feed: CnC
```

```
admin@firepower:/var/sf/iprep_download$
```

```

admin@firepower:~$ ls -halp /var/sf/siurl_download/
total 31M
drwxrwxr-x  5 www  detection 4.0K May  8 18:09 ./
drwxr-xr-x 66 root  root      4.0K Dec 12 00:19 ../
-rw-rw-r--  1 www  www      930 May  8 18:08 .zones
-rw-r--r--  1 root root      422K May  8 18:08 032ba433-c295-11e4-a919-
d4ae5275d599.lf
-rw-r--r--  1 root root        82 May  8 18:08 127dc4a2-1ea3-4423-a02d-
1f02069828ac.lf
-rw-r--r--  1 root root        69 May  8 18:08 1b117672-7453-478c-be31-
b72e89ca4bfc.lf
-rw-r--r--  1 root root      21M May  8 18:08 23f2a124-8278-4c03-8c9d-
d28fe08b8fc9.lf
-rw-r--r--  1 root root        56 May  8 18:08 2b15cb6f-a3fc-4e0e-a342-
ccc5e5806394.lf
-rw-r--r--  1 root root      147K May  8 18:08 2ccda18e-ddff-4f5c-af9a-
f0098521b525.lf
-rw-r--r--  1 root root        53 May  8 18:08 30f9e69c-d64c-479c-821d-
0e4edab852ab.lf
-rw-r--r--  1 root root      8.8K May  8 18:08 3e2af68e-5fc8-4b1c-b5bc-
b4e7cab5c9eb.lf
-rw-r--r--  1 root root        65 May  8 18:08 5915d129-0d33-4e9c-969a-
eab3cde32156.lf
-rw-r--r--  1 root root        52 May  8 18:08 5a0b6d6b-e2c3-436f-b4a1-
48248b333b57.lf
-rw-r--r--  1 root root        48 May  8 18:08 5f8148f1-e5e4-427a-aa3b-
eelc2745f481.lf
-rw-r--r--  1 root root      187K May  8 18:08 60f4e2ab-d96c-44a0-bd38-
830252b67077.lf
-rw-r--r--  1 root root        47 May  8 18:08 6ba968f4-7a25-4793-a2c8-
7cc77f1f1256.lf
-rw-r--r--  1 root root        17 May  8 18:08 IPRVersion.dat
-rw-r--r--  1 root root       20K May  8 18:08 a27c6aae-8e52-4174-a81a-
47c59fecf1c3.lf
-rw-r--r--  1 root root      2.2M May  8 18:08 b1df3aa8-2841-4c88-8e64-
bfaacec71300.lf
-rw-r--r--  1 root root      2.6M May  8 18:08 d7d996a6-6b92-4a56-8f10-
e8506e434dd6.lf
-rw-rw-r--  1 root root      5.1M May  8 18:09 dm_url0.acl
drwxr-xr-x  2 www  www      4.0K Sep 19 2016 health/
drwxr-xr-x  2 www  www      4.0K May  1 17:18 peers/
drwxr-xr-x  2 www  www      4.0K May  8 18:08 tmp/
-rw-rw-r--  1 www  www     1015 May  8 18:08 url.rules
admin@firepower:~$

```

```
admin@firepower:~$ cat /var/sf/siurl_download/url.rules
#security intelligence manifest file
si,5915d129-0d33-4e9c-969a-eab3cde32156.lf,1048597,white,any
si,127dc4a2-1ea3-4423-a02d-1f02069828ac.lf,1048613,block,any
si,5a0b6d6b-e2c3-436f-b4a1-48248b333b57.lf,1048599,block,any
si,5f8148f1-e5e4-427a-aa3b-ee1c2745f481.lf,1048600,block,any
si,6ba968f4-7a25-4793-a2c8-7cc77f1f1256.lf,1048601,block,any
si,30f9e69c-d64c-479c-821d-0e4edab852ab.lf,1048607,block,any
si,2b15cb6f-a3fc-4e0e-a342-ccc5e5806394.lf,1048612,block,any
si,1b117672-7453-478c-be31-b72e89ca4bfc.lf,1048606,block,any
si,3e2af68e-5fc8-4b1c-b5bc-b4e7cab5c9eb.lf,1048610,block,any
si,a27c6aae-8e52-4174-a81a-47c59fecf1c3.lf,1048604,block,any
si,2ccda18e-ddff-4f5c-af9a-f0098521b525.lf,1048611,block,any
si,60f4e2ab-d96c-44a0-bd38-830252b67077.lf,1048602,block,any
si,032ba433-c295-11e4-a919-d4ae5275d599.lf,1048609,block,any
si,b1df3aa8-2841-4c88-8e64-bfaacec71300.lf,1048603,block,any
si,23f2a124-8278-4c03-8c9d-d28fe08b8fc9.lf,1048605,block,any
si,d7d996a6-6b92-4a56-8f10-e8506e434dd6.lf,1048608,monitor,any
admin@firepower:~$
```

```
admin@firepower:~$ head -n1 /var/sf/siurl_download/d7d996a6-6b92-4a56-8f10-
e8506e434dd6.lf
```

```
#Cisco DNS and URL intelligence feed: URL Phishing
```

```
admin@firepower:~$
```

```
admin@firepower:~$ sudo grep -i dns /var/log/messages
admin@firepower:~$ sudo tail -f /var/log/messages | grep -i dns
```

```
admin@firepower:~$ sudo tail -f /var/log/messages | grep -i dns
Password:

May 21 20:56:35 ciscoasa SF-IMS[4397]: [4546] SFDataCorrelator:URLUserIP_
CorrelatorThread [INFO] Writer swap dns database 2
May 21 20:56:35 ciscoasa SF-IMS[4397]: [4546] SFDataCorrelator:ShmemDB [INFO] DNS
Blacklisting load database to segment 0 load mode 2
May 21 20:56:35 ciscoasa SF-IMS[4397]: [4546] SFDataCorrelator:ShmemDB [INFO]
loading firewall rule ID file: /var/sf/sidns_download/dns.rules
May 21 20:56:35 ciscoasa SF-IMS[4397]: [4546] SFDataCorrelator:ShmemDB [INFO] number
of SI category for DNS Blacklisting is 13
May 21 20:56:35 ciscoasa SF-IMS[4397]: [4546] SFDataCorrelator:ShmemDB [INFO]
reading dns/url memcap file /ngfw/etc/sf/dns_url.memcap
May 21 20:56:35 ciscoasa SF-IMS[4397]: [4546] SFDataCorrelator:ShmemDB [INFO]
Setting up shared memory memcap DNS Blacklisting 5242880
May 21 20:56:37 ciscoasa SF-IMS[4397]: [4546] SFDataCorrelator:ShmemDB [INFO]
DNS BL database size: 4532600, number of entries: 341440
May 21 20:56:37 ciscoasa SF-IMS[4397]: [4546] SFDataCorrelator:DMShmMgmt [INFO]
new database available, type:0, segment:0, path:/ngfw/var/sf/sidns_download/
dm_dns0.acl
May 21 20:56:37 ciscoasa SF-IMS[4397]: [4546] SFDataCorrelator:ShmemDB [INFO]
reading dns/url memcap file /ngfw/etc/sf/dns_url.memcap
May 21 20:56:45 ciscoasa SF-IMS[20862]: [20868] sfpreproc:DMShmMgmt [INFO]
successfully removed unused database /ngfw/var/sf/sidns_download/dm_dns1.acl
.
.
<Output Omitted for Brevity>
```

```
admin@firepower:~$ ls -halp /var/sf/sidns_download/
total 11M
drwxrwxr-x 5 www detection 4.0K May 21 20:58 ./
drwxr-xr-x 66 root root 4.0K Dec 12 00:19 ../
-rw-r--r-- 1 root root 400K May 21 20:56 032ba433-c295-11e4-a919-d4ae5275b77b.
lf
-rw-r--r-- 1 root root 0 May 21 20:56 17a11eb0-ff56-11e4-9081-764afb0f5dcb.
lf
-rw-r--r-- 1 root root 69 May 21 20:56 1b117672-7453-478c-be31-b72e89ca2dde.
lf
-rw-r--r-- 1 root root 0 May 21 20:56 1fca9c10-ff56-11e4-866e-ad4afb0f5dcb.
lf
-rw-r--r-- 1 root root 1.9M May 21 20:56 23f2a124-8278-4c03-8c9d-d28fe08b71ab.
lf
-rw-r--r-- 1 root root 145K May 21 20:56 2ccda18e-ddff-4f5c-af9a-f00985219707.
lf
-rw-r--r-- 1 root root 53 May 21 20:56 30f9e69c-d64c-479c-821d-0e4edab8348d.
lf
-rw-r--r-- 1 root root 8.8K May 21 20:56 3e2af68e-5fc8-4b1c-b5bc-b4e7cab5abcd.
lf
-rw-r--r-- 1 root root 52 May 21 20:56 5a0b6d6b-e2c3-436f-b4a1-48248b331d39.
lf
-rw-r--r-- 1 root root 48 May 21 20:56 5f8148f1-e5e4-427a-aa3b-ee1c2745d663.
lf
```

```

-rw-r--r-- 1 root root      187K May 21 20:56 60f4e2ab-d96c-44a0-bd38-830252b65259.
  lf
-rw-r--r-- 1 root root       66 May 21 20:56 663da2e4-32f4-44d2-ad1f-8d6182720d32.
  lf
-rw-r--r-- 1 root root       47 May 21 20:56 6ba968f4-7a25-4793-a2c8-7cc77f1f1074.
  lf
-rw-r--r-- 1 root root       17 May 21 20:56 IPRVersion.dat
-rw-r--r-- 1 root root      20K May 21 20:56 a27c6aae-8e52-4174-a81a-47c59fec3a5.
  lf
-rw-r--r-- 1 root root      2.2M May 21 20:56 b1df3aa8-2841-4c88-8e64-bfaacec7111f.
  lf
-rw-r--r-- 1 root root      1.8M May 21 20:56 d7d996a6-6b92-4a56-8f10-e8506e432fb8.
  lf
-rw-r--r-- 1 root root       66 May 21 20:56 ded9848d-3580-4ca1-9d3c-04113549f129.
  lf
-rw-rw-r-- 1 root root      4.4M May 21 20:57 dm_dns1.acl
-rw-r--r-- 1 root root      1.7K May 21 20:56 dns.rules
drwxr-xr-x 2 www  www      4.0K Sep 19 2016 health/
drwxr-xr-x 3 www  www      4.0K Apr 29 16:17 peers/
drwxr-xr-x 2 www  www      4.0K May 21 20:56 tmp/
admin@firepower:~$

```

```

admin@firepower:~$ cat /var/sf/sidns_download/dns.rules
#### dns.rules
#####
#
# DNS Policy Name : Custom DNS Policy
#
# File Written      : Sun May 21 20:56:42 2017 (UTC)
#
#####
#
policy e5d989f8-3d01-11e7-8dc5-a7ffd42f66c2
revision e5d989f8-3d01-11e7-8dc5-a7ffd42f66c2

interface 1 e2b1d576-2cf5-11e7-8ea7-e184e4106fb3
interface 2 e295985c-2cf5-11e7-8ea7-e184e4106fb3

```

```
dnslist 1048594 663da2e4-32f4-44d2-ad1f-8d6182720d32.lf
dnslist 1048585 032ba433-c295-11e4-a919-d4ae5275b77b.lf
dnslist 1048599 ded9848d-3580-4ca1-9d3c-04113549f129.lf
dnslist 1048597 b1df3aa8-2841-4c88-8e64-bfaacec7111f.lf
dnslist 1048590 3e2af68e-5fc8-4b1c-b5bc-b4e7cab5abcd.lf
dnslist 1048587 23f2a124-8278-4c03-8c9d-d28fe08b71ab.lf
dnslist 1048598 d7d996a6-6b92-4a56-8f10-e8506e432fb8.lf
dnslist 1048595 6ba968f4-7a25-4793-a2c8-7cc77f1f1074.lf
dnslist 1048589 30f9e69c-d64c-479c-821d-0e4edab8348d.lf
dnslist 1048591 5a0b6d6b-e2c3-436f-b4a1-48248b331d39.lf
dnslist 1048592 5f8148f1-e5e4-427a-aa3b-ee1c2745d663.lf
dnslist 1048586 1b117672-7453-478c-be31-b72e89ca2dde.lf
dnslist 1048593 60f4e2ab-d96c-44a0-bd38-830252b65259.lf
sinkhole 1 7e550616-3e61-11e7-a338-d8a9a7208ff6 192.168.1.91 ::1
```

```
1 allow any any any 1048594
3 nxdomain any any any 1048599
5 nxdomain any any any 1048591
5 nxdomain any any any 1048592
5 nxdomain any any any 1048595
5 nxdomain any any any 1048593
6 block any any any 1048597
6 block any any any 1048586
6 block any any any 1048589
7 sinkhole any any any 1048587 (sinkhole: 1)
8 monitor any any any 1048598
8 monitor any any any 1048585
8 monitor any any any 1048590
admin@firepower:~$
```

```
admin@firepower:~$ head -nl /var/sf/sidns_download/23f2a124-8278-4c03-8c9d-
d28fe08b71ab.lf
```

```
#Cisco DNS and URL intelligence feed: DNS Malware
```

```
admin@firepower:~$
```

```
admin@firepower:~$ grep [domain_name] /var/sf/sidns_download/*.lf
```



```
admin@firepower:~$ egrep iolmau.com /var/sf/sidns_download/*.lf
/var/sf/sidns_download/23f2a124-8278-4c03-8c9d-d28fe08b71ab.1f:iolmau.com
admin@firepower:~$ head -n1 /var/sf/sidns_download/23f2a124-8278-4c03-8c9d-
d28fe08b71ab.1f
#Cisco DNS and URL intelligence feed: DNS Malware
admin@firepower:~$

admin@firepower:~$ egrep mrreacher.net /var/sf/sidns_download/*.lf
/var/sf/sidns_download/60f4e2ab-d96c-44a0-bd38-830252b65259.1f:mrreacher.net
admin@firepower:~$ head -n1 /var/sf/sidns_download/60f4e2ab-d96c-44a0-bd38-
830252b65259.1f
#Cisco DNS and URL intelligence feed: DNS CnC
admin@firepower:~$

admin@firepower:~$ egrep rent.sinstr.ru /var/sf/sidns_download/*.lf
/var/sf/sidns_download/d7d996a6-6b92-4a56-8f10-e8506e432fb8.1f:rent.sinstr.ru
admin@firepower:~$
admin@firepower:~$ head -n1 /var/sf/sidns_download/d7d996a6-6b92-4a56-8f10-
e8506e432fb8.1f
#Cisco DNS and URL intelligence feed: DNS Phishing
admin@firepower:~$
```

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol:
```

```
Please specify a client IP address: 192.168.1.2
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 DNS SI shared mem lookup returned 1
  for iolmau.com
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 Starting SrcZone first with intfs -1
  -> 0, vlan 0
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 1, id 1 action Allow
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 2, id 3 action DNS
  NXDomain
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 3, id 5 action DNS
  NXDomain
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 4, id 6 action Block
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 5, id 7 action DNS
  Sinkhole
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 Got DNS list match. si list 1048587
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 6, id 8 action Audit
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 Firing DNS action DNS Sinkhole
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 DNS SI: Matched rule order 5, Id 7,
  si list id 1048587, action 23, reason 2048, SI Categories 1048587,0
```

```
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 DNS SI shared mem lookup returned 1
for mrreacher.net
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 Starting SrcZone first with intfs -1
-> 0, vlan 0
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 1, id 1 action Allow
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 2, id 3 action DNS
NXDomain
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 3, id 5 action DNS
NXDomain
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 Got DNS list match. si list 1048593
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 4, id 6 action Block
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 5, id 7 action DNS
Sinkhole
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 6, id 8 action Audit
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 Firing DNS action DNS NXDomain
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 DNS SI: Matched rule order 3, Id 5,
si list id 1048593, action 22, reason 2048, SI Categories 1048593,0

192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 DNS SI shared mem lookup returned 1
for rent.sinstr.ru
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 Starting SrcZone first with intfs -1
-> 0, vlan 0
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 1, id 1 action Allow
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 2, id 3 action DNS
NXDomain
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 3, id 5 action DNS
NXDomain
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 4, id 6 action Block
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 5, id 7 action DNS
Sinkhole
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 match rule order 6, id 8 action Audit
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 Got DNS list match. si list 1048598
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 Firing DNS action Audit
192.168.1.2-37868 > 192.168.1.1-53 17 AS 4 I 1 DNS SI: Matched rule order 6, Id 8,
si list id 1048598, action 6, reason 4096, SI Categories 1048598,0
```

! The following answer demonstrates the "Sinkhole" action. It responses with IP address 192.168.1.91, which is a non-authoritative spoof DNS server.

```
Users@Linux:~$ nslookup iolmau.com
```

```
Server:          127.0.1.1
Address:         127.0.1.1#53
```

Non-authoritative answer:

```
Name:   iolmau.com
Address: 192.168.1.91
```

```
Users@Linux:~$
```

! The following answer reflects the "Domain Not Found" action. The DNS query fails with NXDOMAIN message, which means the domain appears to be non-existent.

```
Users@Linux:~$ nslookup mrreacher.net
```

```
Server:          127.0.1.1
Address:         127.0.1.1#53
```

```
** server can't find mrreacher.net: NXDOMAIN
```

```
Users@Linux:~$
```

! The following answer reflects the "Monitor" action. The DNS query is able to resolve the domain name. It shows the public IP address for the domain.

```
Users@Linux:~$ nslookup rent.sinstr.ru
```

```
Server:          127.0.1.1
Address:         127.0.1.1#53
```

```
Name:   rent.sinstr.ru
Address: 81.222.82.37
```

```
Users@Linux:~$
```

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol:
```

```
Please specify a client IP address: 192.168.1.2
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 New session
```

```
192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 Starting with minimum 2, 'Job Search Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
```

```
192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 pending rule order 2, 'Job Search Rule', URL
```

```
192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 Starting with minimum 2, 'Job Search Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
```

```
192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 pending rule order 2, 'Job Search Rule', URL
```

```
192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 Starting with minimum 2, 'Job Search Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
```

```
192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 pending rule order 2, 'Job Search Rule', URL
```

```
192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 URL SI:  
ShmDBLookupURL("http://google.com/") returned 0
```

```
192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 Starting with minimum 2, 'Job Search Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 676, payload 184, client 638, misc 0, user 9999997, url http://google.com/, xff
```

```
192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1: DataMessaging_GetURLData: Returning URL_BCTYPE for google.com
```

```
192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 rule order 2, 'Job Search Rule', URL  
Lookup Success: http://google.com/ waited: 0ms
```

```
192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 no match rule order 2, 'Job Search Rule', url=(http://google.com/) c=50 r=81
```

```
192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 match rule order 3, id 268435458  
action Allow
```

```
192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 allow action
```

```
192.168.1.2-44374 > XX.XX.XX.XX-80 6 AS 4 I 1 Deleting session
```

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol:
```

```
Please specify a client IP address: 192.168.1.2
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 New session
```

```
192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
```

```
192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 pending rule order 2, 'Job Search Rule', URL
```

```
192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
```

```
192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 pending rule order 2, 'Job Search Rule', URL
```

```
192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
```

```
192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 pending rule order 2, 'Job Search Rule', URL
```

```
192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 URL SI: ShmDBLookupURL("http://dice.com/") returned 0
```

```
192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 676, payload 0, client 638, misc 0, user 9999997, url http://dice.com/, xff
```

```
192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0: DataMessaging_GetURLData: Returning URL_BCTYPE for dice.com
```

```
192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 rule order 2, 'Job Search Rule', URL Lookup Success: http://dice.com/ waited: 0ms
```

```
192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 rule order 2, 'Job Search Rule', URL http://dice.com/ Matched Category: 26:96 waited: 0ms
```

```
192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 match rule order 2, 'Job Search Rule', action Block
```

```
192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 deny action
```

```
192.168.1.2-56742 > XX.XX.XX.XX-80 6 AS 4 I 0 Deleting session
```

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol:
```

```
Please specify a client IP address: 192.168.1.2
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 New session
```

```
192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search  
Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:  
untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
```

```
192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 pending rule order 2, 'Job Search  
Whitelist', URL
```

```
192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search  
Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:  
untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
```

```
192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 pending rule order 2, 'Job Search  
Whitelist', URL
```

```
192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search  
Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:  
untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
```

```
192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 pending rule order 2, 'Job Search  
Whitelist', URL
```

```
192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 URL SI:  
ShmDBLookupURL("http://dice.com/") returned 0
```

```
192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search  
Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag:  
untagged, svc 676, payload 0, client 638, misc 0, user 9999997, url  
http://dice.com/, xff
```

```
192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 match rule order 2, 'Job Search  
Whitelist', action Allow
```

```
192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 allow action
```

```
192.168.1.2-56746 > XX.XX.XX.XX-80 6 AS 4 I 0 Deleting session
```

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol:
```

```
Please specify a client IP address: 192.168.1.2
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 New session
```

```
192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 Starting with minimum 2, 'Job Search Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
```

```
192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 pending rule order 2, 'Job Search Whitelist', URL
```

```
192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 Starting with minimum 2, 'Job Search Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
```

```
192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 pending rule order 2, 'Job Search Whitelist', URL
```

```
192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 Starting with minimum 2, 'Job Search Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
```

```
192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 pending rule order 2, 'Job Search Whitelist', URL
```

```
192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 URL SI: ShmDBLookupURL("http://careerbuilder.com/") returned 0
```

```
192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 Starting with minimum 2, 'Job Search Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 676, payload 1491, client 638, misc 0, user 9999997, url http://careerbuilder.com/, xff
```

```
192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 no match rule order 2, 'Job Search Whitelist', url=(http://careerbuilder.com/) c=0 r=0
```

```
192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1: DataMessaging_GetURLData: Returning URL_BCTYPE for careerbuilder.com
```

```
192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 rule order 3, 'Job Search Rule', URL Lookup Success: http://careerbuilder.com/ waited: 0ms
```

```
192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 rule order 3, 'Job Search Rule', URL http://careerbuilder.com/ Matched Category: 26:92 waited: 0ms
```

```
192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 match rule order 3, 'Job Search Rule', action Block
```

```
192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 deny action
```

```
192.168.1.2-54772 > XX.XX.XX.XX-80 6 AS 4 I 1 Deleting session
```



```
> system support firewall-engine-debug
```

```
Please specify an IP protocol:
```

```
Please specify a client IP address: 192.168.1.2
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 New session
```

```
192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
```

```
192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 pending rule order 2, 'Job Search Whitelist', URL
```

```
192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
```

```
192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 pending rule order 2, 'Job Search Whitelist', URL
```

```
192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
```

```
192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 pending rule order 2, 'Job Search Whitelist', URL
```

```
192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 URL SI:  
ShmDBLookupURL("http://nazmulrajib.com/") returned 0
```

```
192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 Starting with minimum 2, 'Job Search Whitelist', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc 676, payload 0, client 638, misc 0, user 9999997, url http://nazmulrajib.com/, xff
```

```
192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 no match rule order 2, 'Job Search Whitelist', url=(http://nazmulrajib.com/) c=0 r=0
```

```
192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0: DataMessaging_GetURLData:  
useVendorService_feature not set, returning URL_FAILEDTYPE
```

```
192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 rule order 3, 'Job Search Rule',  
URL Lookup Failed: http://nazmulrajib.com/ waited: 0ms
```

```
192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 no match rule order 3, 'Job Search Rule', url=(http://nazmulrajib.com/) c=65534 r=0
```

```
192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 match rule order 4, id 268435458  
action Allow
```

```
192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 allow action
```

```
192.168.1.2-40398 > XX.XX.XX.XX-80 6 AS 4 I 0 Deleting session
```

```
admin@FMC:~$ ls -halp /var/sf/cloud_download/
total 450M
drwxr-xr-x  3 www  www  4.0K Apr 28 23:18 ./
drwxr-xr-x 64 root root 4.0K Apr 28 02:20 ../
-rw-r--r--  1 root root   78 Apr 28 23:18 cloudagent_dlupdate_health
-rw-r--r--  1 root root  22M Apr 28 16:24 full_bcdb_rep_1m_5.174.bin
-rw-r--r--  1 root root 429M Apr 28 16:24 full_bcdb_rep_5.174.bin
-rw-r--r--  1 www  www  5.4K Aug 26 2016 sfrep_catg
-rw-r--r--  1 www  www  433 Aug 26 2016 sfrep_index
drwxr-xr-x  2 www  www  4.0K Apr 28 23:52 tmp/
admin@FMC:~$
```

Successfully downloaded, applied and moved, full_bcdb_rep_5.174.bin,...

Success, called perl transaction,

```
admin@FTD:~$ ls -halp /var/sf/cloud_download/
total 22M
drwxr-xr-x  3 www  www  4.0K Apr 28 22:01 ./
drwxr-xr-x 66 root root 4.0K Dec 12 00:19 ../
-rw-r--r--  1 root root   78 Sep 19 2016 cloudagent_dlupdate_health
-rw-r--r--  1 root root  22M Apr 28 22:01 full_bcdb_rep_5.174.bin
-rw-r--r--  1 www  www  5.4K Aug 26 2016 sfrep_catg
-rw-r--r--  1 www  www  433 Aug 26 2016 sfrep_index
drwxr-xr-x  2 www  www  4.0K Apr 28 22:01 tmp/
admin@FTD:~$
```

```
admin@FTD:~$ ls -halp /dev/shm/ | grep -i bcdb
-rwxrwxrwx  1 root root  23M Apr 28 23:17 Global.bcdb1
-rwxrwxrwx  1 root root  6.1M Apr 28 23:17 Global.bcdb1acc
-rwxrwxrwx  1 root root 256K Apr 28 23:17 Global.bcdb1cacheinx
admin@FTD:~$
```

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp
```

```
Please specify a client IP address:
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 New session
```

```
172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 Starting with minimum 2, 'Social  
Networking Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0,  
sgt tag: untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
```

```
172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 pending rule order 2,  
'Social Networking Rule', AppId
```

```
172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 Starting with minimum 2, 'Social  
Networking Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0,  
sgt tag: untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
```

```
172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 pending rule order 2,  
'Social Networking Rule', AppId
```

```
172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 Starting with minimum 2, 'Social  
Networking Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0,  
sgt tag: untagged, svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
```

```
172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 pending rule order 2,  
'Social Networking Rule', AppId
```

```
172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 URL SI: ShmDBLookupURL  
("www.facebook.com") returned 0
```

```
172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 Starting with minimum 2, 'Social  
Networking Rule', and SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0,  
sgt tag: untagged, svc 1122, payload 629, client 1296, misc 0, user 9999997, url  
www.facebook.com, xff
```

```
172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 match rule order 2,  
'Social Networking Rule', action Reset
```

```
172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 reset action
```

```
172.16.100.110-4677 > 31.13.65.36-443 6 AS 4 I 1 Deleting session
```

```
> system support application-identification-debug
```

```
Please specify an IP protocol: tcp
```

```
Please specify a client IP address:
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring application identification debug messages
```

```
.  
.  
172.16.100.110-4677 -> 31.13.65.36-443 6 R AS 4 I 1 port service 0  
172.16.100.110-4677 -> 31.13.65.36-443 6 AS 4 I 1 3rd party returned 847  
172.16.100.110-4677 -> 31.13.65.36-443 6 AS 4 I 1 SSL is service 1122,  
portServiceAppId 1122  
172.16.100.110-4677 -> 31.13.65.36-443 6 AS 4 I 1 ssl returned 10  
172.16.100.110-4677 -> 31.13.65.36-443 6 AS 4 I 1 appId: 629  
(safe)search_support_type=NOT_A_SEARCH_ENGINE
```

```
^C
```

```
Caught interrupt signal
```

```
Exiting
```

```
admin@FMC:~$ sudo OmniQuery.pl -db mdb -e "select appId,appName from appIdInfo where  
appId=629";
```

```
Password:
```

```
getting filenames from [/usr/local/sf/etc/db_updates/index]
```

```
getting filenames from [/usr/local/sf/etc/db_updates/base-6.1.0]
```

```
+-----+-----+  
| appId | appName |  
+-----+-----+  
| 629   | Facebook |  
+-----+-----+
```

```
-----  
OmniQuery v2.1
```

```
(c) 2016 Cisco Systems, Inc.
```

```
.:|:.:|:.
```

```
-----  
mdb> exit
```

```
admin@FMC:~$
```

! First, run the debug command and specify necessary parameters.

> system support firewall-engine-debug

Please specify an IP protocol: tcp

Please specify a client IP address: 192.168.1.200

Please specify a client port:

Please specify a server IP address:

Please specify a server port:

Monitoring firewall engine debug messages

! Now, begin the transfer of an executable file.

192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 New session

192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 using HW or preset rule order 2, 'Access Rule for File Policy', action Allow and prefilter rule 0

192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 allow action

192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 URL SI:

ShmDBLookupURL("http://172.16.100.100/files/7z1700.exe") returned 0

192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 File Policy verdict is Type, Malware, and Capture

192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 File type verdict Unknown, fileAction Block, flags 0x00203500, and type action Reject for type 21 of instance 0

! At this stage, the file is being transferred through the FTD. The following messages appear after the file is stored on the FTD. FTD blocks the file transfer as soon as it detects the end-of-file marker on a packet.

192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 File type storage finished within signature using verdict Reject

192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 File signature reserved file data of partial file with flags 0x00203500 and status Exceeded Max Filesize

192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 File signature verdict Reject and flags 0x00203500 for partial file of instance 0

192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 File type event for file named 7z1700.exe with disposition Type and action Block

192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 Archive childs been processed No

192.168.1.200-47954 > 172.16.100.100-80 6 AS 4 I 0 Deleting session

^C

Caught interrupt signal

Exiting.

>

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp
```

```
Please specify a client IP address: 192.168.1.200
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 New session
```

```
192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 Starting with minimum 0, id 0 and  
SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged,  
svc 0, payload 0, client 0, misc 0, user 9999997, url , xff
```

```
192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 match rule order 2, 'Access Rule  
for File Policy', action Allow
```

```
192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 allow action
```

```
192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 URL SI:  
ShmDBLookupURL("http://172.16.100.100/files/userguide.pdf") returned 0
```

```
192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 Starting with minimum 0, id 0 and  
SrcZone first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, sgt tag: untagged, svc  
676, payload 0, client 638, misc 0, user 9999997, url http://172.16.100.100/files/  
userguide.pdf, xff
```

```
192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 match rule order 2, 'Access Rule  
for File Policy', action Allow
```

```
192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 allow action
```

```
.
```

```
<Output omitted for brevity>
```

```
.
```

```
192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 File policy verdict is Type,  
Malware, and Capture
```

```
192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 File type verdict Log, fileAction  
Log, flags 0x00001100, and type action Log for type 285 of instance 0
```

```
192.168.1.200-58374 > 172.16.100.100-80 6 AS 4 I 0 File type event for file named  
userguide.pdf with disposition Type and action Log
```

```
.
```

```
<Output omitted for brevity>
```

```
^C
```

```
Caught interrupt signal
```

```
Exiting.
```

```
>
```

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp
```

```
Please specify a client IP address: 192.168.1.200
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 New session
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 using HW or preset rule order 2, 'Access Rule for File Policy', action Allow and prefilter rule 0
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 allow action
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 URL SI: ShmDBLookupURL("http://172.16.100.100/files/7z1700.exe") returned 0
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 File policy verdict is Type, Malware, and Capture
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 File type verdict Unknown, fileAction Malware Lookup, flags 0x01BDDA00, and type action Stop for type 21 of instance 0
```

```
! Next, FTD calculates the SHA-256 hash value of the file, which is 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d.
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 File signature verdict Unknown and flags 0x01BDDA00 for partial file of instance 0
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 File signature cache query returned Cache Miss for 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d with disposition Cache Miss, spero Cache Miss, severity 0, and transmit Not Sent
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 File signature reserved file data of 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d with flags 0x01BDDA00 and status Exceeded Max Filesize
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 File signature verdict Pending and flags 0x01BDDA00 for 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d of instance 0
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 File signature cache query returned Cache Miss for 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d with disposition Cache Miss, spero Cache Miss, severity 0, and transmit Not Sent
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 File signature reserved file data of 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d with flags 0x01BDDA00 and status Exceeded Max Filesize
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 File signature verdict Pending and flags 0x01BDDA00 for 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d of instance 0
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 File malware event for 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d named 7z1700.exe with disposition Cache Miss and action Timeout
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 Archive childs been processed No
```

```
192.168.1.200-58466 > 172.16.100.100-80 6 AS 4 I 0 Deleting session
```

```
admin@FMC:~$ sudo tail -f /var/log/messages
```

```
Password:
```

```
.  
<Output is omitted for brevity>
```

```
.
```

```
! If FMC is connected to the internet, but fails to resolve a DNS query, the following error message appears in the Syslog.
```

```
.
```

```
[timestamp] FMC stunnel: LOG3[3953:140160119551744]: Error resolving 'cloud-sa.amp.sourcefire.com': Neither nodename nor servname known (EAI_NONAME)
```

```
.
```

```
! After you fix any communication issues, FMC should be able to connect to the cloud. The following Syslog messages confirm a successful connection.
```

```
.
```

```
[timestamp] FMC SF-IMS[25954]: [26657] SFDataCorrelator:FireAMPCloudLookup [INFO] cloud server is cloud-sa.amp.sourcefire.com  
[timestamp] FMC SF-IMS[25954]: [26657] SFDataCorrelator:imcloudpool [INFO] connect to cloud using stunnel
```

```
.
```

```
! Once the FMC is connected to the cloud, it begins the registration process. The following messages confirm successful registrations to the Cisco Clouds.
```

```
.
```

```
[timestamp] FMC SF-IMS[25954]: [26657] SFDataCorrelator:FireAMPCloudLookup [INFO] Successfully registered with fireamp cloud  
[timestamp] FMC SF-IMS[25954]: [25954] SFDataCorrelator:FileExtract [INFO] Successfully registered with sandbox cloud
```

```
.
```

```
! Upon successful registration, FMC is able to perform cloud lookup and obtains updates. The following messages confirm a successful check for malware database update.
```

```
.
```

```
[timestamp] FMC SF-IMS[25275]: [25275] CloudAgent:CloudAgent [INFO] ClamUpd, time to check for updates
```

```
.
```

```
[timestamp] FMC SF-IMS[25275]: [25298] CloudAgent:CloudAgent [INFO] Nothing to do, database is up to date
```

```
.
```

```
file type:MSEXE; id:21; category:Executables,Dynamic Analysis Capable,Local Malware Analysis Capable; msg:"Windows/DOS executable file "; rev:1; content: | 4D 5A|; offset:0;
```



```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp
```

```
Please specify a client IP address: 192.168.1.200
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
! Now, begin the transfer of an executable file.
```

```
192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 New session
```

```
192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 using HW or preset rule order 2,  
'Access Rule for File Policy', action Allow and prefilter rule 0
```

```
192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 allow action
```

```
192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 URL SI:  
ShmDBLookupURL("http://172.16.100.100/files/7z1700.exe") returned 0
```

```
192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File policy verdict is Type,  
Malware, and Capture
```

```
192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File type verdict Unknown,  
fileAction Malware Lookup, flags 0x01BDDA00, and type action Stop for type 21 of  
instance 0
```

```
! First, Firepower System checks the cached disposition.
```

```
192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File signature verdict Unknown  
and flags 0x01BDDA00 for partial file of instance 0
```

```
192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File signature cache query returned  
Cache Miss for 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d with  
disposition Cache Miss, spero Cache Miss, severity 0, and transmit Not Sent
```

```
192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File signature reserved file data  
of 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d with flags  
0x01BDDA00 and status Exceeded Max Filesize
```

```
192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File signature verdict Pending  
and flags 0x01BDDA00 for 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485dd-  
b307ee982d of instance 0
```

! Here, Firepower System performs a query to the cloud for disposition.

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File signature cache query returned Neutral for 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d with disposition Neutral, spero Cache Miss, severity 0, and transmit Not Sent

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File signature reserved file data of 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d for spero with flags 0x01BDDA00 and status Exceeded Max Filesize

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File signature reserved file data of 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d with flags 0x01BDDA00 and status Exceeded Max Filesize

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File signature reserved file data of 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d with flags 0x01BDDA00 and status Exceeded Max Filesize

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File signature verdict Log and flags 0x01BDDA00 for 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d of instance 0

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 File malware event for 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d named 7z1700.exe with disposition Neutral and action Malware Lookup

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 Archive child's been processed No

192.168.1.200-58552 > 172.16.100.100-80 6 AS 4 I 0 Deleting session

^C

Caught interrupt signal

Exiting.

>

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp
```

```
Please specify a client IP address: 192.168.1.200
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
! First, client attempts to download the suspicious.exe file using a web browser.
```

```
192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 New session
```

```
192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 using HW or preset rule order 2, 'Access Rule for File Policy', action Allow and prefilter rule 0
```

```
192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 allow action
```

```
192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 URL SI: ShmDBLookupURL ("http://172.16.100.100/files/suspicious.exe") returned 0
```

```
192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 File policy verdict is Type, Malware, and Capture
```

```
192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 File type verdict Unknown, fileAction Malware Lookup, flags 0x0025DA00, and type action Stop for type 273 of instance 0
```

```
! Firepower System performs a lookup on cached disposition before sending a query to the cloud.
```

```
192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 File signature cache query returned Cache Miss for 275a021bbfb6489e54d471899f7db9d1663f-c695ec2fe2a2c4538aabf651fd0f with disposition Cache Miss, spero Cache Miss, severity 0, and transmit Sent
```

```
192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 File signature reserved file data of 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f with flags 0x0025DA00 and status Smaller than Min Filesize
```

```
192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 File signature verdict Pending and flags 0x0025DA00 for 275a021bbfb6489e54d471899f7db9d1663f-c695ec2fe2a2c4538aabf651fd0f of instance 0
```

```
192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 File signature cache query returned Cache Miss for 275a021bbfb6489e54d471899f7db9d1663f-c695ec2fe2a2c4538aabf651fd0f with disposition Cache Miss, spero Cache Miss, severity 0, and transmit Sent
```

```
192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 File signature reserved file data of 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f with flags 0x0025DA00 and status Smaller than Min Filesize
```

```
192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 File signature verdict Pending and flags 0x0025DA00 for 275a021bbfb6489e54d471899f7db9d1663f-c695ec2fe2a2c4538aabf651fd0f of instance 0
```

```
! At this stage, FMC receives a malware disposition from the cloud. FTD acts on the file based on the File Policy.
```

```
192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 File signature cache
query returned Malware for 275a021bbfb6489e54d471899f7db9d1663f-
c695ec2fe2a2c4538aabf651fd0f with disposition Malware, spero Cache Miss, severity
76, and transmit Sent
192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 File signature reserved file data
of 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f with flags
0x0025DA00 and status Smaller than Min Filesize
192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 File signature verdict
Reject and flags 0x0025DA00 for 275a021bbfb6489e54d471899f7db9d1663f-
c695ec2fe2a2c4538aabf651fd0f of instance 0
192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 File malware event for
275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f named suspicious.
exe with disposition Malware and action Block Malware
192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 Archive childs been processed No
192.168.1.200-58566 > 172.16.100.100-80 6 AS 4 I 0 Deleting session
.
<Output Omitted for Brevity>
.
^C
Caught interrupt signal
Exiting.
>
```

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: tcp
```

```
Please specify a client IP address: 192.168.1.200
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Monitoring firewall engine debug messages
```

```
192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 New session
```

```
192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 using HW or preset rule order 2,  
'Access Rule for File Policy', action Allow and prefilter rule 0
```

```
192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 allow action
```

```
192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 URL SI:  
ShmDBLookupURL("http://172.16.100.100/files/7z1700.exe") returned 0
```

```
192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 File policy verdict is Type,  
Malware, and Capture
```

```
192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 File type verdict Unknown,  
fileAction Malware Lookup, flags 0x01BDDA00, and type action Stop for type 21 of  
instance 0
```

```
192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 File signature verdict Unknown  
and flags 0x01BDDA00 for partial file of instance 0
```

```
192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 File signature blacklist  
2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d
```

```
192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 File signature reserved file data  
of 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d with flags  
0x00A5DA00 and status Exceeded Max Filesize
```

```
192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 File signature verdict Reject  
and flags 0x00A5DA00 for 2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485dd-  
b307ee982d of instance 0
```

```
192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 File malware event for  
2c8637b812f7a47802f4f91f8bfaccb978df9b62de558d038485ddb307ee982d named 7z1700.exe  
with disposition Custom and action Custom Block
```

```
192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 Archive childs been processed No
```

```
192.168.1.200-58588 > 172.16.100.100-80 6 AS 4 I 0 Deleting session
```

```
^C
```

```
Caught interrupt signal
```

```
Exiting.
```

```
>
```

```
alert tcp $TELNET_SERVERS 23 -> $EXTERNAL_NET any (msg:"PROTOCOL-TELNET
login incorrect"; flow:to_client,established; content:"Login incorrect";
metadata:ruleset community, service telnet; classtype:bad-unknown; sid:718;
rev:16; )
```

```
! When a login attempt is successful
```

```
external-user@Fedora:~$ telnet 192.168.1.200
```

```
Trying 192.168.1.200... Open
```

```
Connected to 192.168.1.200.
```

```
Ubuntu login: internal-user
```

```
Password: *****
```

```
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-81-generic x86_64)
```

```
internal-user@Ubuntu:~$
```

```
! When a login attempt is unsuccessful
```

```
external-user@Fedora:~$ telnet 192.168.1.200
```

```
Trying 192.168.1.200... Open
```

```
Connected to 192.168.1.200.
```

```
Ubuntu login: internal-user
```

```
Password: <incorrect_password>
```

```
Login incorrect
```

```
Ubuntu login:
```

```
> capture telnet_inside trace interface INSIDE_INTERFACE match tcp any any eq 23
```

```
> show capture
```

```
capture telnet_inside type raw-data trace interface INSIDE_INTERFACE
```

```
[Capturing - 0 bytes]
```

```
match tcp any any eq telnet
```

```
>
```

```
> show capture telnet_inside
```

```
119 packets captured
```

```
 1: 20:23:21.086802      107.15.160.100.53875 > 192.168.1.200.23: S  
1751019501:1751019501(0) win 4128 <mss 1460>  
 2: 20:23:21.087229      107.15.160.100.53875 > 192.168.1.200.23: S  
1751019501:1751019501(0) win 4128 <mss 1460>  
 3: 20:23:21.087565      192.168.1.200.23 > 107.15.160.100.53875: S  
232306554:232306554(0) ack 1751019502 win 29200 <mss 1460>  
 4: 20:23:21.087702      192.168.1.200.23 > 107.15.160.100.53875: S  
232306554:232306554(0) ack 1751019502 win 29200 <mss 1460>  
 5: 20:23:21.089717      107.15.160.100.53875 > 192.168.1.200.23: . ack 232306555  
win 4128  
 6: 20:23:21.089762      107.15.160.100.53875 > 192.168.1.200.23: P  
1751019502:1751019514(12) ack 232306555 win 4128  
.  
.
```

```
<Output Omitted for Brevity>
```

```
! Now view the tracing data of the first captured packet.
```

```
> show capture telnet_inside packet-number 1 trace
```

```
119 packets captured
```

```
 1: 20:23:21.086802      107.15.160.100.53875 > 192.168.1.200.23: S  
1751019501:1751019501(0) win 4128 <mss 1460>  
Phase: 1  
Type: CAPTURE  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
MAC Access list
```

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 3

Type: NGIPS-MODE

Subtype: ngips-mode

Result: ALLOW

Config:

Additional Information:

The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268435458

access-list CSM_FW_ACL_ remark rule-id 268435458: ACCESS POLICY: AC Policy - Default/1

access-list CSM_FW_ACL_ remark rule-id 268435458: L4 RULE: DEFAULT ACTION RULE

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: NGIPS-EGRESS-INTERFACE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

Ingress interface OUTSIDE_INTERFACE is in NGIPS inline mode.

Egress interface INSIDE_INTERFACE is determined by inline-set configuration

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 848, packet dispatched to next module

Phase: 7
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 8
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet

Phase: 9
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Result:
input-interface: INSIDE_INTERFACE
input-status: up
input-line-status: up
Action: allow

1 packet shown

>

```
<Output Omitted for Brevity>
```

```
.
```

```
.
```

```
Phase: 7
```

```
Type: EXTERNAL-INSPECT
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
Application: 'SNORT Inspect'
```

```
Phase: 8
```

```
Type: SNORT
```

```
Subtype:
```

```
Result: DROP
```

```
Config:
```

```
Additional Information:
```

```
Snort Verdict: (block-packet) drop this packet
```

```
.
```

```
.
```

```
<Output Omitted for Brevity>
```

```
> show asp drop
```

```
Frame drop:
```

Snort requested to drop the frame (snort-drop)	5
FP L2 rule drop (l2_acl)	1

```
Last clearing: 20:23:14 UTC Jul 3 2017 by enable_1
```

```
Flow drop:
```

```
Last clearing: 20:23:14 UTC Jul 3 2017 by enable_1
```

```
>
```

```
! To view the NAT configurations:
```

```
> show running-config nat
```

```
!
```

```
object network Net-IN-192.168.1.0
```

```
  nat (INSIDE_INTERFACE,OUTSIDE_INTERFACE) dynamic pat-pool Pool-OUT-203.0.113.3-5  
  flat include-reserve
```

```
>
```

```
! To determine the scope of an object:
```

```
> show running-config object
```

```
object network Net-IN-192.168.1.0
```

```
  subnet 192.168.1.0 255.255.255.0
```

```
object network Pool-OUT-203.0.113.3-5
```

```
  range 203.0.113.3 203.0.113.5
```

```
>
```

```
> show nat detail
```

```
Auto NAT Policies (Section 2)
```

```
1 (INSIDE_INTERFACE) to (OUTSIDE_INTERFACE) source dynamic Net-IN-192.168.1.0  
  pat-pool Pool-OUT-203.0.113.3-5 flat include-reserve
```

```
  translate_hits = 0, untranslate_hits = 0
```

```
  Source - Origin: 192.168.1.0/24, Translated (PAT): 203.0.113.3-203.0.113.5
```

```
>
```

! To view the mapping of physical interfaces with their logical names:

> show nameif

Interface	Name	Security
GigabitEthernet1/1	INSIDE_INTERFACE	0
GigabitEthernet1/2	OUTSIDE_INTERFACE	0
GigabitEthernet1/3	DMZ_INTERFACE	0
Management1/1	diagnostic	0

>

! To view the status and IP addresses of the FTD interfaces:

> show interface ip brief

Interface	IP-Address	OK?	Method	Status	Protocol
Virtual0	127.1.0.1	YES	unset	up	up
GigabitEthernet1/1	192.168.1.1	YES	CONFIG	up	up
GigabitEthernet1/2	203.0.113.1	YES	CONFIG	up	up
GigabitEthernet1/3	172.16.1.1	YES	CONFIG	up	up
GigabitEthernet1/4	unassigned	YES	unset	administratively down	down
GigabitEthernet1/5	unassigned	YES	unset	administratively down	down

.

.

<Output omitted for brevity>

```
> show conn detail
```

```
1 in use, 4 most used
```

```
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,  
b - TCP state-bypass or nailed,  
C - CTIQBE media, c - cluster centralized,  
D - DNS, d - dump, E - outside back connection, e - semi-distributed,  
F - initiator FIN, f - responder FIN,  
G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,  
i - incomplete, J - GTP, j - GTP data, K - GTP t3-response  
k - Skinny media, M - SMTP data, m - SIP media, N - inspected by Snort,  
n - GUP  
O - responder data, P - inside back connection,  
q - SQL*Net data, R - initiator acknowledged FIN,  
R - UDP SUNRPC, r - responder acknowledged FIN,  
T - SIP, t - SIP transient, U - up,  
V - VPN orphan, v - M3UA W - WAAS,  
w - secondary domain backup,  
X - inspected by service module,  
x - per session, Y - director stub flow, y - backup stub flow,  
Z - Scansafe redirection, z - forwarding stub flow
```

```
TCP OUTSIDE_INTERFACE: 203.0.113.10/22 INSIDE_INTERFACE: 192.168.1.10/41934,  
flags UxIO N, idle 6s, uptime 18s, timeout 1h0m, bytes 6718, xlate id  
0x7f516987ee00
```

```
>
```

```
> show xlate detail
```

```
1 in use, 2 most used
```

```
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,  
s - static, T - twice, N - net-to-net
```

```
TCP PAT from INSIDE_INTERFACE:192.168.1.10/41934 to OUTSIDE_INTER-  
FACE:203.0.113.3/41934 flags ri idle 0:00:28 timeout 0:00:30 refcnt 1 xlate id  
0x7f516987ee00
```

```
>
```

```
> show nat detail
```

```
Auto NAT Policies (Section 2)
```

```
1 (INSIDE_INTERFACE) to (OUTSIDE_INTERFACE) source dynamic Net-IN-192.168.1.0  
  pat-pool Pool-OUT-203.0.113.3-5 flat include-reserve  
    translate_hits = 1, untranslate_hits = 0  
    Source - Origin: 192.168.1.0/24, Translated (PAT): 203.0.113.3-203.0.113.5  
>
```

```
! Begin the capture of SSH traffic on inside interface.
```

```
> capture ssh_traffic_inside trace interface INSIDE_INTERFACE match tcp any any  
  eq 22
```

```
! Verify if the FTD is running a capture for SSH traffic.
```

```
> show capture
```

```
capture ssh_traffic_inside type raw-data trace interface INSIDE_INTERFACE  
  [Capturing - 0 bytes]  
  match tcp any any eq ssh  
>
```

```
! To view all of the captured packets (press Ctrl+C to exit from a long show):
```

```
> show capture ssh_traffic_inside
```

```
81 packets captured
```

```
  1: 02:59:47.220310      192.168.1.10.41934 > 203.0.113.10.22: S
1482617093:1482617093(0) win 29200 <mss 1460,sackOK,timestamp 15243390
0,nop,wscale 7>
  2: 02:59:47.221149      203.0.113.10.22 > 192.168.1.10.41934: S
1409789153:1409789153(0) ack 1482617094 win 28960 <mss 1380,sackOK,timestamp
17762742 15243390,nop,wscale 7>
  3: 02:59:47.221256      192.168.1.10.41934 > 203.0.113.10.22: . ack 1409789154
win 229 <nop,nop,timestamp 15243390 17762742>
  4: 02:59:47.221729      192.168.1.10.41934 > 203.0.113.10.22: P
1482617094:1482617135(41) ack 1409789154 win 229 <nop,nop,timestamp 15243391
17762742>
  5: 02:59:47.222186      203.0.113.10.22 > 192.168.1.10.41934: . ack 1482617135
win 227 <nop,nop,timestamp 17762742 15243391>
```

```
.
```

```
.
```

```
<Output is omitted for brevity>
```

```
! To analyze the first captured packet:
```

```
> show capture ssh_traffic_inside packet-number 1 trace
```

```
81 packets captured
```

```
1: 02:59:47.220310      192.168.1.10.41934 > 203.0.113.10.22: S
1482617093:1482617093(0) win 29200 <mss 1460,sackOK,timestamp 15243390
0,nop,wscale 7>
```

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

MAC Access list

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 3

Type: ROUTE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

found next-hop 203.0.113.10 using egress ifc OUTSIDE_INTERFACE

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268435457
```

```
access-list CSM_FW_ACL_ remark rule-id 268435457: ACCESS POLICY: AC Policy -
Mandatory/1
```

```
access-list CSM_FW_ACL_ remark rule-id 268435457: L7 RULE: Traffic Selection
```

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

```
class-map class-default
```

```
  match any
```

```
policy-map global_policy
```

```
  class class-default
```

```
    set connection advanced-options UM_STATIC_TCP_MAP
```

```
service-policy global_policy global
```

Additional Information:

Phase: 6

Type: NAT

Subtype:

Result: ALLOW

Config:

```
object network Net-IN-192.168.1.0
```

```
  nat (INSIDE_INTERFACE,OUTSIDE_INTERFACE) dynamic pat-pool Pool-OUT-203.0.113.3-5
```

```
  flat include-reserve
```

Additional Information:

Dynamic translate 192.168.1.10/41934 to 203.0.113.3/41934

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 10
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:

New flow created with id 442, packet dispatched to next module

Phase: 12
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 13
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet

Phase: 14
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 203.0.113.10 using egress ifc OUTSIDE_INTERFACE

```
Phase: 15
Type: ADJACENCY-LOOKUP
Subtype: next-hop and adjacency
Result: ALLOW
Config:
Additional Information:
adjacency Active
next-hop mac address 0023.2472.1d3c hits 139985869104448
```

```
Phase: 16
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Result:
input-interface: OUTSIDE_INTERFACE
input-status: up
input-line-status: up
output-interface: OUTSIDE_INTERFACE
output-status: up
output-line-status: up
Action: allow
```

```
1 packet shown
>
```

```
! Enable capture on the outside interface:
```

```
> capture ssh_traffic_outside trace interface OUTSIDE_INTERFACE match tcp any any eq 22
```

```
! FTD begins capturing SSH traffic on the outside interface:
```

```
> show capture
```

```
capture ssh_traffic_inside type raw-data trace interface INSIDE_INTERFACE
  [Capturing - 0 bytes]
  match tcp any any eq ssh
capture ssh_traffic_outside type raw-data trace interface OUTSIDE_INTERFACE
  [Capturing - 0 bytes]
  match tcp any any eq ssh
```

```
>
```

```
> show capture ssh_traffic_outside
```

```
8 packets captured
```

```
 1: 03:56:51.100290      203.0.113.10.48400 > 203.0.113.3.22: S  
3636330443:3636330443(0) win 29200 <mss 1460,sackOK,timestamp 18618684  
0,nop,wscale 7>
```

```
 2: 03:56:52.097269      203.0.113.10.48400 > 203.0.113.3.22: S  
3636330443:3636330443(0) win 29200 <mss 1460,sackOK,timestamp 18618934  
0,nop,wscale 7>
```

```
 3: 03:56:54.101343      203.0.113.10.48400 > 203.0.113.3.22: S  
3636330443:3636330443(0) win 29200 <mss 1460,sackOK,timestamp 18619435  
0,nop,wscale 7>
```

```
 4: 03:56:58.105478      203.0.113.10.48400 > 203.0.113.3.22: S  
3636330443:3636330443(0) win 29200 <mss 1460,sackOK,timestamp 18620436  
0,nop,wscale 7>
```

```
 5: 03:57:22.069759      203.0.113.10.53048 > 192.168.1.10.22: S  
1744936567:1744936567(0) win 29200 <mss 1460,sackOK,timestamp 18626426  
0,nop,wscale 7>
```

```
 6: 03:57:23.066250      203.0.113.10.53048 > 192.168.1.10.22: S  
1744936567:1744936567(0) win 29200 <mss 1460,sackOK,timestamp 18626676  
0,nop,wscale 7>
```

```
 7: 03:57:25.070369      203.0.113.10.53048 > 192.168.1.10.22: S  
1744936567:1744936567(0) win 29200 <mss 1460,sackOK,timestamp 18627177  
0,nop,wscale 7>
```

```
 8: 03:57:29.082469      203.0.113.10.53048 > 192.168.1.10.22: S  
1744936567:1744936567(0) win 29200 <mss 1460,sackOK,timestamp 18628180  
0,nop,wscale 7>
```

```
8 packets shown
```

```
>
```

```
> show capture ssh_traffic_outside packet-number 1 trace
```

```
8 packets captured
```

```
1: 03:56:51.100290      203.0.113.10.48400 > 203.0.113.3.22: S  
3636330443:3636330443(0) win 29200 <mss 1460,sackOK,timestamp 18618684  
0,nop,wscale 7>
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 3
```

```
Type: ROUTE-LOOKUP
```

```
Subtype: Resolve Egress Interface
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
found next-hop 203.0.113.3 using egress ifc OUTSIDE_INTERFACE
```

```
Result:
```

```
input-interface: OUTSIDE_INTERFACE
```

```
input-status: up
```

```
input-line-status: up
```

```
output-interface: OUTSIDE_INTERFACE
```

```
output-status: up
```

```
output-line-status: up
```

```
Action: drop
```

```
Drop-reason: (nat-no-xlate-to-pat-pool) Connection to PAT address without pre-exist-  
ing xlate
```

```
1 packet shown
```

```
>
```

```
> show capture ssh_traffic_outside packet-number 5 trace
```

```
8 packets captured
```

```
5: 03:57:22.069759      203.0.113.10.53048 > 192.168.1.10.22: S 1744936567:  
1744936567(0) win 29200 <mss 1460,sackOK,timestamp 18626426 0,nop,wscale 7>
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 3
```

```
Type: ROUTE-LOOKUP
```

```
Subtype: Resolve Egress Interface
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
found next-hop 192.168.1.10 using egress ifc  INSIDE_INTERFACE
```

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268435457
```

```
access-list CSM_FW_ACL_ remark rule-id 268435457: ACCESS POLICY: AC Policy -  
Mandatory/1
```

```
access-list CSM_FW_ACL_ remark rule-id 268435457: L7 RULE: Traffic Selection
```

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

```
class-map class-default
```

```
match any
```

```
policy-map global_policy
```

```
class class-default
```

```
set connection advanced-options UM_STATIC_TCP_MAP
```

```
service-policy global_policy global
```

Additional Information:

Phase: 6

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 7

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 8

Type: NAT

Subtype: rpf-check

Result: DROP

Config:

object network Net-IN-192.168.1.0

nat (INSIDE_INTERFACE,OUTSIDE_INTERFACE) dynamic pat-pool Pool-OUT-203.0.113.3-5
flat include-reserve

Additional Information:

Result:

input-interface: OUTSIDE_INTERFACE

input-status: up

input-line-status: up

output-interface: INSIDE_INTERFACE

output-status: up

output-line-status: up

Action: drop

Drop-reason: (acl-drop) Flow is denied by configured rule

1 packet shown

>

```
> show nat detail
```

```
Auto NAT Policies (Section 2)
```

```
1 (DMZ_INTERFACE) to (OUTSIDE_INTERFACE) source static Serv-Real-172.16.1.10
  Serv-Mask-203.0.113.2 service tcp ssh 2200
  translate_hits = 0, untranslate_hits = 1
  Source - Origin: 172.16.1.10/32, Translated: 203.0.113.2/32
  Service - Protocol: tcp Real: ssh Mapped: 2200
2 (INSIDE_INTERFACE) to (OUTSIDE_INTERFACE) source dynamic Net-IN-192.168.1.0
  pat-pool Pool-OUT-203.0.113.3-5 flat include-reserve
  translate_hits = 0, untranslate_hits = 0
  Source - Origin: 192.168.1.0/24, Translated (PAT): 203.0.113.3-203.0.113.5
>
```

```
> show xlate detail
```

```
1 in use, 2 most used
```

```
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
```

```
TCP PAT from DMZ_INTERFACE:172.16.1.10 22-22 to OUTSIDE_INTERFACE:203.0.113.2
2200-2200
```

```
flags sr idle 0:00:54 timeout 0:00:00 refcnt 1 xlate id 0x7f516987ee00
```

```
>
```

```
! Enable capture on outside interface:
```

```
> capture ssh_traffic_outside_masked trace interface OUTSIDE_INTERFACE match tcp any any eq 2200
```

```
! Verify that the capture is running:
```

```
> show capture
```

```
capture ssh_traffic_inside type raw-data trace interface INSIDE_INTERFACE  
[Capturing - 0 bytes]
```

```
match tcp any any eq ssh
```

```
capture ssh_traffic_outside type raw-data trace interface OUTSIDE_INTERFACE  
[Capturing - 0 bytes]
```

```
match tcp any any eq ssh
```

```
capture ssh_traffic_outside_masked type raw-data trace interface OUTSIDE_INTERFACE  
[Capturing - 0 bytes]
```

```
match tcp any any eq 2200
```

```
>
```

```
! Now, initiate an SSH connection from the external host to the internal DMZ server. Use the masqueraded IP address and port number. It generates the following traffic.
```

```
> show capture ssh_traffic_outside_masked
```

```
59 packets captured
```

```
1: 05:21:23.785436      203.0.113.10.41760 > 203.0.113.2.2200: S  
2089153959:2089153959(0) win 29200 <mss 1460,sackOK,timestamp 19887065  
0,nop,wscale 7>
```

```
2: 05:21:23.786168      203.0.113.2.2200 > 203.0.113.10.41760: S  
29917599:29917599(0) ack 2089153960 win 28960 <mss 1380,sackOK,timestamp 19892875  
19887065,nop,wscale 7>
```

```
3: 05:21:23.786336      203.0.113.10.41760 > 203.0.113.2.2200: . ack 29917600  
win 229 <nop,nop,timestamp 19887065 19892875>
```

```
4: 05:21:23.786855      203.0.113.10.41760 > 203.0.113.2.2200: P  
2089153960:2089154001(41) ack 29917600 win 229 <nop,nop,timestamp 19887066  
19892875>
```

```
5: 05:21:23.787312      203.0.113.2.2200 > 203.0.113.10.41760: . ack 2089154001  
win 227 <nop,nop,timestamp 19892876 19887066>
```

```
.  
.
```

```
<Output is omitted for brevity>
```

```
> show capture ssh_traffic_outside_masked packet-number 1 trace
```

```
59 packets captured
```

```
1: 05:21:23.785436      203.0.113.10.41760 > 203.0.113.2.2200: S  
2089153959:2089153959(0) win 29200 <mss 1460,sackOK,timestamp 19887065  
0,nop,wscale 7>
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

Phase: 3

Type: UN-NAT

Subtype: static

Result: ALLOW

Config:

```
object network Serv-Real-172.16.1.10
```

```
  nat (DMZ_INTERFACE,OUTSIDE_INTERFACE) static Serv-Mask-203.0.113.2 service  
  tcp ssh 2200
```

Additional Information:

NAT divert to egress interface DMZ_INTERFACE

Untranslate 203.0.113.2/2200 to 172.16.1.10/22

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268435457
```

```
access-list CSM_FW_ACL_ remark rule-id 268435457: ACCESS POLICY: AC  
  Policy - Mandatory/1
```

```
access-list CSM_FW_ACL_ remark rule-id 268435457: L7 RULE: Traffic Selection
```

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Config:
class-map class-default
 match any
policy-map global_policy
 class class-default
 set connection advanced-options UM_STATIC_TCP_MAP
service-policy global_policy global
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network Serv-Real-172.16.1.10
 nat (DMZ_INTERFACE,OUTSIDE_INTERFACE) static Serv-Mask-203.0.113.2 service tcp
 ssh 2200
Additional Information:

Phase: 9
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 10
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 505, packet dispatched to next module

Phase: 12
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 13
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet

Phase: 14
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 172.16.1.10 using egress ifc DMZ_INTERFACE

Phase: 15
Type: ADJACENCY-LOOKUP
Subtype: next-hop and adjacency
Result: ALLOW
Config:
Additional Information:
adjacency Active
next-hop mac address a4ba.db9f.9460 hits 5205

Result:
input-interface: OUTSIDE_INTERFACE
input-status: up
input-line-status: up
output-interface: DMZ_INTERFACE
output-status: up
output-line-status: up
Action: allow

1 packet shown

>


```
> show capture ssh_traffic_outside packet-number 1 trace
```

```
6 packets captured
```

```
1: 05:19:16.438255      203.0.113.10.48556 > 172.16.1.10.22:  
S 1315278899:1315278899(0) win 29200 <mss 1460,sackOK,timestamp 19855229 0,  
nop,wscale 7>
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 3
```

```
Type: ROUTE-LOOKUP
```

```
Subtype: Resolve Egress Interface
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
found next-hop 172.16.1.10 using egress ifc DMZ_INTERFACE
```

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268435457
```

```
access-list CSM_FW_ACL_ remark rule-id 268435457: ACCESS POLICY: AC  
Policy - Mandatory/1
```

```
access-list CSM_FW_ACL_ remark rule-id 268435457: L7 RULE: Traffic Selection
```

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

```
class-map class-default
```

```
match any
```

```
policy-map global_policy
```

```
class class-default
```

```
set connection advanced-options UM_STATIC_TCP_MAP
```

```
service-policy global_policy global
```

Additional Information:

Phase: 6

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 7

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 8

Type: NAT

Subtype: rpf-check

Result: DROP

Config:

object network Serv-Real-172.16.1.10

```
nat (DMZ_INTERFACE,OUTSIDE_INTERFACE) static Serv-Mask-203.0.113.2 service tcp
ssh 2200
```

Additional Information:

Result:

input-interface: OUTSIDE_INTERFACE

input-status: up

input-line-status: up

output-interface: DMZ_INTERFACE

output-status: up

output-line-status: up

Action: drop

Drop-reason: (acl-drop) Flow is denied by configured rule

1 packet shown

>

```
> system generate-troubleshoot all
Starting /usr/local/sf/bin/sf_troubleshoot.pl...
Please, be patient. This may take several minutes.
The troubleshoot option code specified is ALL.
getting filenames from [/ngfw/usr/local/sf/etc/db_updates/index]
getting filenames from [/ngfw/usr/local/sf/etc/db_updates/base-6.1.0]
Troubleshooting information successfully created at /ngfw/var/common/
results-08-10-2017--201713.tar.gz
>
```

```
> file list
```

```
Aug 10 20:23          73603794 /results-08-10-2017--201713.tar.gz
```

```
> file secure-copy <remote_IP> <remote_username> <remote_folder> <local_filename_
on_FTD>
> file secure-copy 10.1.1.100 admin /home/folder results-08-10-2017--201713.tar.gz
> file delete results-08-10-2017--201713.tar.gz
```

```
Really remove file results-08-10-2017--201713.tar.gz?
```

```
Please enter 'YES' or 'NO': YES
```

```
>
```

```
admin@FMC:~$ sudo sf_troubleshoot.pl
Starting /usr/local/sf/bin/sf_troubleshoot.pl...
Please, be patient. This may take several minutes.
getting filenames from [/usr/local/sf/etc/db_updates/index]
getting filenames from [/usr/local/sf/etc/db_updates/base-6.1.0]
Troubleshooting information successfully created at /var/common/
results-08-10-2017--184001.tar.gz
admin@FMC:~$
```

```
admin@FMC:~$ ls -halp /var/common/
total 115M
drwxrwxr-x  2 admin detection 4.0K Aug 10 18:42 ./
drwxr-xr-x 17 root          4.0K Mar 28  2016 ../
-rw-r--r--  1 root   root    115M Aug 10 18:42 results-08-10-2017--184001.tar.gz
admin@FMC:~$
```

```
admin@FMC:~$ sudo scp <local_filename_on_FMC><remote_username>@<remote_IP>:
<remote_folder>
```

```
admin@FMC:~$ sudo scp /var/common/results-08-10-2017--184001.tar.gz
```

```
admin@10.1.1.100:/home/folder
```

```
admin@FMC:~$ sudo rm /var/common/results-08-10-2017--184001.tar.gz
```

```
Password:
```

```
admin@FMC:~$
```