



CCIE Security v4.0 Practice Labs

Natalie Timms

Cisco Press

About This eBook

ePUB is an open, industry-standard format for eBooks. However, support of ePUB and its many features varies across reading devices and applications. Use your device or app settings to customize the presentation to your liking. Settings that you can customize often include font, font size, single or double column, landscape or portrait mode, and figures that you can click or tap to enlarge. For additional information about the settings and features on your reading device or app, visit the device manufacturer's Web site.

Many titles include programming code or configuration examples. To optimize the presentation of these elements, view the eBook in single-column, landscape mode and adjust the font size to the smallest setting. In addition to presenting code and configurations in the reflowable text format, we have included images of the code that mimic the presentation found in the print book; therefore, where the reflowable format may compromise the presentation of the code listing, you will see a "Click here to view code image" link. Click the link to view the print-fidelity code image. To return to the previous page viewed, click the Back button on your device or app.

CCIE Security v4.0 Practice Labs

Natalie Timms, CCIE No. 37959

Cisco Press

800 East 96th Street
Indianapolis, IN 46240

CCIE Security v4.0 Practice Labs

Natalie Timms, CCIE No. 37959

Copyright © 2014 Pearson Education, Inc.

Published by:

Pearson Education, Inc.
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.

ISBN-13: 978-1-58714-414-1

ISBN-10: 1-58714-414-X

Warning and Disclaimer

This book is designed to provide information about exam topics for the Cisco Certified Internetwork Expert (CCIE) Security Lab 4.0 Exam. 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 author, 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 e-mail at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger
Business Operation Manager, Cisco Press: Jan Cornelssen

Associate Publisher: Dave Dusthimer
Senior Development Editor: Christopher Cleveland

Acquisition Editor: Denise Lincoln
Managing Editor: Sandra Schroeder

Senior Project Editor: Tonya Simpson
Technical Editors: Tim Rowley, Tyson Scott

Proofreader: Paula Lowell
Editorial Assistant: Vanessa Evans

Cover Designer: Mark Shirar
Composition: Mary Sudul



Americas Headquarters

Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters

Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters

Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.



CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Stadium Vision, Cisco Telepresence, Cisco WebEx, DCE, and Welcome to the Human Network are

trademarks; Changing the Way We Work. Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS. Bringing the Meeting To You. Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, Phone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy. Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert. StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

About the Author

Natalie Timms, CCIE No. 37959, is a former program manager with the CCIE certification team at Cisco, managing exam curricula and content for the CCIE Security track before becoming an independent consultant.

Natalie has been involved with computer networking for more than 20 years, much of which was spent with Cisco. Natalie has contributed at the IETF standards level and has written many technical papers, and is also a Cisco Press author and U.S. patent holder.

Natalie has also been a technical instructor in the Asia-Pacific region for Wellfleet Communications/Bay Networks, and is the winner of multiple Cisco Live Distinguished Speaker awards.

Natalie has a CCIE Security certification and a bachelor's degree in computer science and statistics from Macquarie University in Sydney, Australia.

About the Technical Reviewers

Tim Rowley, CCIE No. 25960 (Security/Wireless), CWNE No. 124, CCSI No. 33858, CISSP, is a consultant within the Cisco Global Security Services. He is responsible for design, implementation, and support of customer networks with a focus on network security and wireless. Tim regularly contributes to the development of certification exams and the related training material, including CCNA, CCNP, and CCIE security and wireless. He has a passion for technical development and enjoys helping others achieve their certification goals.

Tyson Scott, Triple CCIE No. 13513, is a consulting systems engineer for Cisco Systems with more than 14 years in the IT industry. He has traveled the globe delivering learning solutions to the Cisco certification community, specializing in CCIE Security and CCIE Routing and Switching. Today, he helps to deliver leading security solutions in the state, local government, and education verticals.

Dedication

I have been so very fortunate to be surrounded by people who have always encouraged me to march to the beat of my own drum. To my husband, Randy, I give my love and gratitude for letting me be me; never being in my face yet always being there. To my parents, Helen and Denis, thank you for putting up with my craziness and patiently waiting for me to find my niche in life. I am Russian passion tempered with an Aussie sense of humor. And to my brother, Mick, you have always been the “little” brother I looked up to both in stature and knowing who you wanted to be.

Finally, this book is also dedicated to all those who strive to be the best they can be.

Acknowledgments

I would like to thank the folks at Cisco Press, Denise Lincoln and Brett Bartow, for inviting me to contribute, and Chris Cleveland, for wading through pages of edits and not imploding.

To my technical editors, Tyson Scott and Tim Rowley, I appreciate all you have done to help me complete this book. You guys are network rock stars and I bow at your feet.

I need to acknowledge Scott Fanning, who for so many years was my partner in crime at Cisco. Scott, you helped foster my love for security technologies, all-night coding sessions, Tim Hortons Coffee, and ice hockey. I'm so proud of all you have achieved.

So many others have helped and supported me over the years, and kicked my ass when required; it is impossible to list everyone who has made an impact in my life. I hope I can pay it forward.

Sometimes, inspiration comes in the most unexpected way, even a Cake Pop.

Contents at a Glance

[Introduction](#)

[**Part I Lab Topology Components, Cabling, and Routing and Switching Configuration**](#)

[**Part II Practice Lab 1**](#)

[Practice Lab 1](#)

[Practice Lab 1 Solutions](#)

[**Part III Practice Lab 2**](#)

[Practice Lab 2](#)

[Practice Lab 2 Solutions](#)

[**Part IV Appendices**](#)

[Manual Configuration Guide](#)

[Preparing for the CCIE Exam](#)

[Sample Written Exam Questions and Answers](#)

Contents

[Introduction](#)

[Part I Lab Topology Components, Cabling, and Routing and Switching Configuration](#)

[Equipment List](#)

[General Guidelines](#)

[Prelab Setup Instructions](#)

[Catalyst Switchport Cabling Diagram](#)

[Lab Topology Diagram](#)

[Lab Guide Addressing Scheme](#)

[Lab Guide IP Routing Details](#)

[VPN Solutions Diagrams](#)

[Initial Device Configurations](#)

[Final Configuration Files](#)

[CCIE Security Exam Study and Preparation Tips](#)

[CCIE Security Written Exam](#)

[Part II Practice Lab 1](#)

[Section 1 Perimeter Security and Services](#)

[Exercise 1.1: Initialize the Cisco ASA in Multi-Context Routed Mode](#)

[Notes](#)

[Exercise 1.2: Configure Routing and Basic Access on ASA2](#)

[Notes](#)

[Exercise 1.3: Configure IP Services on ASA1](#)

[Task 1: Configure Network Object NAT](#)

[Task 2: Configure Twice NAT](#)

[Task 3: Configure and Troubleshoot NTP Services Using Authentication](#)

[Task 4: Configure Support for IPv6 in IPv4 Tunneling Through ASA1](#)

[Exercise 1.4: Configure IP Routing Security on ASA2](#)

[Task 1: BGP Connectivity Through the ASA2](#)

[Task 2: OSPF Authentication for Routing Update Security](#)

[Section 2 Intrusion Prevention and Content Security](#)

[Exercise 2.1: Initialize and Deploy the Cisco IPS Sensor Appliance](#)

[Task 1: Initialize the Cisco IPS Sensor](#)

[Task 2: Deploy the Cisco IPS Sensor in Inline VLAN Pair Mode](#)

[Task 3: Deploy the Cisco IPS Sensor in Inline Interface Pair Mode](#)

[Task 4: Deploy the Cisco IPS Sensor in Promiscuous Mode](#)

[Exercise 2.2: Initialize the Cisco WSA](#)

[Exercise 2.3: Enable Web Content Features on the Cisco WSA](#)

[Task 1: Configure WCCPv2 Proxy Support on the WSA \(Client\) and ASA1 \(Server\)](#)

[Task 2: Configure Proxy Bypass on the WSA](#)

[Task 3: Create a Custom URL Access Policy on the WSA](#)

Section 3 Secure Access

[Exercise 3.1: Configure and Troubleshoot IPsec EZVPN](#)

[Exercise 3.2: Troubleshoot DMVPN Phase 3: DMVPNv3](#)

[Exercise 3.3: Configure Security Features on the Cisco WLC](#)

[Task 1: Initialize the WLC and Establish Control over the Cisco Access Points \(AP\)](#)

[Task 2: Enable IP Services on the WLC to Enhance Security](#)

[Task 3: Creating and Assigning Security Policy to WLANs and Users](#)

[Exercise 3.4: Configure the Cisco IOS Certificate Server](#)

Section 4 System Hardening and Availability

[Exercise 4.1: Configure SPAN on the Cisco Catalyst Switch](#)

[Exercise 4.2: Troubleshoot Secure Routing Using OSPFv3 in Cisco IOS](#)

[Exercise 4.3: Configure Control Plane Policing \(CoPP\)](#)

[Exercise 4.4: Troubleshoot Management Plane Protection](#)

[Exercise 4.5: Device Hardening on the Cisco WLC](#)

[Task 1: Disable SSID Broadcasting](#)

[Task 2: Protect the WLC Against Associating with a Rogue AP](#)

[Task 3: Enable Infrastructure Management Frame Protection on the WLC](#)

[Task 4: Enable Encryption for CAPWAP Packets](#)

[Task 5: Create a Rate Limiting Policy for Guest Users on the Guest WLAN](#)

Section 5 Threat Identification and Mitigation

[Exercise 5.1: Troubleshoot IPv6 in IPv4 Tunnel](#)

[Exercise 5.2: Mitigating DHCP Attacks on a Cisco Catalyst Switch](#)

[Exercise 5.3: Identifying Attacks with NetFlow and Mitigating Attacks Using Flexible Packet Matching](#)

[Exercise 5.4: Application Protocol Protection](#)

Section 6: Identity Management

[Exercise 6.1: Configure Router Command Authorization and Access Control](#)

[Exercise 6.2: Configure Cut-Through Proxy on ASA2 Using TACACS+](#)

[Exercise 6.3: Configure Support for MAB/802.1X for Voice and Data VLANs](#)

[Exercise 6.3a: Authentication and Authorization Using MAB](#)

[Exercise 6.3b: Authentication and Authorization Using 802.1X](#)

Part II Practice Lab 1 Solutions

Section 1 Perimeter Security and Services

[Solution and Verification for Exercise 1.1: Initialize the Cisco ASA in Multi-Context Routed Mode](#)

[Skills Tested](#)

[Solution and Verification](#)

[Basic Parameters](#)

[Admin Context Parameters](#)

[Context c1 Parameters](#)

[Context c2 Parameters](#)

[ASA1 Configuration](#)

[Tech Notes](#)

[Solution and Verification for Exercise 1.2: Configure Routing and Basic Access on ASA2](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Tech Notes](#)

[Solution and Verification for Exercise 1.3: Configure IP Services on ASA1](#)

[Skills Tested](#)

[Solution and Verification](#)

[Task 1: Network Object NAT](#)

[Task 2: Twice NAT](#)

[Task 3: NTP with Authentication](#)

[Task 4: Tunneling ipv6ip](#)

[Configuration](#)

[Tech Notes](#)

[Solution and Verification for Exercise 1.4: Configure IP Routing Security on ASA2](#)

[Skills Tested](#)

[Solution and Verification](#)

[Task 1: BGP Connectivity Through ASA2](#)

[Task 2: OSPF Authentication for Routing Update Security](#)

[Configuration](#)

[Tech Notes](#)

Section 2 Intrusion Prevention and Content Security

[Solution and Verification for Exercise 2.1: Initialize and Deploy the Cisco IPS Sensor Appliance](#)

[Skills Tested](#)

[Solution and Verification](#)

[Task 1: Initialize the Cisco IPS](#)

[Task 2: Deploy the Cisco IPS Sensor in Inline VLAN Pair Mode](#)

[Task 3: Deploy the Cisco IPS Sensor in Inline Interface Pair Mode](#)

[Task 4: Deploy the Cisco IPS Sensor in Promiscuous Mode](#)

[Configuration](#)

[Tech Notes](#)

[Solution and Verification for Exercise 2.2: Initialize the Cisco WSA](#)

[Skills Tested](#)

[Solution and Verification](#)

[Tech Notes](#)

[Solution and Verification for Exercise 2.3: Enable Web Content Features on the Cisco WSA](#)

[Skills Tested](#)

[Solution and Verification](#)

[Task 1: Configure WCCPv2 Proxy Support on the Cisco WSA \(Client\) and the Cisco ASA \(Server\)](#)

[Task 2: Configure Proxy Bypass on the Cisco WSA](#)

[Task 3: Create a Custom URL Access Policy on the Cisco WSA](#)

[Configuration](#)

[Tech Notes](#)

[WCCP Support Across Cisco Products](#)

[Transparent Proxy Versus Explicit Proxy](#)

[Connection Assignment and Redirection](#)

[Service Groups](#)

Section 3 Secure Access

[Solution and Verification for Exercise 3.1: Configure and Troubleshoot IPsec EZVPN](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Tech Notes](#)

[*Initiating the EZVPN Tunnel*](#)

[*Split Tunnel Options*](#)

[*EZVPN Client Modes of Operation in Cisco IOS*](#)

[*Client U-Turn Versus IPsec Hairpinning*](#)

[*External Versus Internal Policy*](#)

[Solution and Verification for Exercise 3.2: Troubleshoot DMVPN Phase 3: DMVPNv3](#)

[Skills Tested](#)

[Solution and Verification](#)

[*NHRP Spoke Registration*](#)

[*Spoke-to-Spoke Connection from R4 to R3*](#)

[*Verification*](#)

[Configuration](#)

[Tech Notes](#)

[*DMVPNv1*](#)

[*DMVPNv2*](#)

[*DMVPNv3*](#)

[Solution and Verification for Exercise 3.3: Configure Security Features on the Cisco WLC](#)

[Task 1: Initialize the Cisco WLC and Establish Control over the Cisco Access Points](#)

[Task 2: Enable IP Services on the Cisco WLC to Enhance Security](#)

[Task 3: Creating and Assigning Security Policy to WLANs and Users](#)

[Configuration](#)

[Solution and Verification for Exercise 3.4: Configure the Cisco IOS Certificate Server](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Tech Notes](#)

Section 4 System Hardening and Availability

[Solution and Verification for Exercise 4.1: Configure SPAN on the Cisco Catalyst Switch](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Tech Notes](#)

[*SPAN Versus RSPAN*](#)

[*SPAN and RSPAN Terminology and Guidelines*](#)

[*VLAN-Based SPAN*](#)

[Solution and Verification for Exercise 4.2: Troubleshoot Secure Routing Using OSPFv3 in](#)

Cisco IOS

Skills Tested

Solution and Verification

Configuration

Tech Notes

Solution and Verification for Exercise 4.3: Configure Control Plane Policing (CoPP)

Skills Tested

Solution and Verification

Verification

Configuration

Tech Notes

Router Planes

CoPP Versus CPPr

Solution and Verification for Exercise 4.4: Troubleshoot Management Plane Protection

Skills Tested

Solution and Verification

Configuration

Solution and Verification for Exercise 4.5: Device Hardening on the Cisco WLC

Skills Tested

Solution and Verification

Task 1: Disable SSID Broadcasting

Task 2: Protect the WLC Against Associating with a Rogue AP

Task 3: Enable Infrastructure Management Frame Protection on the Cisco WLC

Task 4: Enable Encryption for CAPWAP Packets

Task 5: Create a Rate Limiting Policy for Guest Users on the Guest WLAN

Configuration

Tech Notes

Summary of Wireless Attacks

Management Frame Protection via 802.11w

Section 5 Threat Identification and Mitigation

Solution and Verification for Exercise 5.1: Troubleshoot IPv6 in IPv4 Tunnel

Skills Tested

Solution and Verification

Configuration

Solution and Verification for Exercise 5.2: Mitigating DHCP Attacks on a Cisco Catalyst Switch

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Tech Notes](#)

[DHCP Implementation Notes](#)

[*DHCP Option 82*](#)

[*DHCP Snooping and the DHCP Server on Cisco IOS Routers*](#)

[Solution and Verification for Exercise 5.3: Identifying Attacks with NetFlow and Mitigating Attacks Using Flexible Packet Matching](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Solution and Verification for Exercise 5.4: Application Protocol Protection](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

Section 6 Identity Management

[Solution and Verification for Exercise 6.1: Configure Router Command Authorization and Access Control](#)

[Skills Tested](#)

[Solution and Verification](#)

[*ACS Solution*](#)

[Configuration](#)

[Tech Notes](#)

[*Tracing the Command Authorization Process*](#)

[*Understanding AAA and Login on the Router Lines*](#)

[*Test AAA Commands*](#)

[*AAA Accounting*](#)

[Solution and Verification for Exercise 6.2: Configure Cut-Through Proxy on ASA2 Using TACACS+](#)

[Skills Tested](#)

[Solution and Verification](#)

[*CiscoSecure ACS Configuration*](#)

[Configuration](#)

[Tech Notes](#)

[Solution and Verification for Exercise 6.3: Configure Support for MAB/802.1X for Voice and Data VLANs](#)

[Skills Tested](#)

[Verification: Part A](#)

[Verification: Part B](#)

[Configuration](#)

[Cisco ISE Configuration](#)

[Tech Notes](#)

Part III Practice Lab 2

Section 1 Perimeter Security

[Exercise 1.1: Configure a Redundant Interface on ASA2](#)

[Exercise 1.2: SSH Management Authentication and Local Command Authorization on ASA1](#)

[Exercise 1.3: Configuring Advanced Network Protection on the ASA](#)

[Task 1: Botnet Traffic Filtering on ASA1](#)

[Task 2: Threat Detection on ASA2](#)

[Task 3: IP Audit on ASA1](#)

[Exercise 1.4: Configure IPv6 on ASA2](#)

[Exercise 1.5: Cisco IOS Zone-Based Firewall with Support for Secure Group Tagging](#)

Section 2 Intrusion Prevention and Content Security

[Exercise 2.1: Configuring Custom Signatures on the Cisco IPS Sensor](#)

[Custom Signature to Track OSPF TTL](#)

[Custom Signature to Identify and Deny Large ICMP Packets](#)

[Custom Signature to Identify and Deny an ICMP Flood Attack](#)

[Exercise 2.2: Enable Support for HTTPS on the Cisco WSA](#)

[Exercise 2.3: Enable User Authentication for Transparent Proxy Using LDAP](#)

[Exercise 2.4: Guest User Support on the Cisco WSA](#)

Section 3 Secure Access

[Exercise 3.1: Configure and Troubleshoot IPsec Static VTI with IPv6](#)

[Exercise 3.2: Troubleshoot and Configure GETVPN](#)

[Exercise 3.3: SSL Client and Clientless VPNs](#)

[Exercise 3.4: Configure and Troubleshoot FlexVPN Site-to-Site Using RADIUS Tunnel Attributes](#)

[Exercise 3.5: Configure and Troubleshoot FlexVPN Remote Access \(Client to Server\)](#)

Section 4 System Hardening and Availability

[Exercise 4.1: BGP TTL-Security Through the Cisco ASA](#)

[Exercise 4.2: Configure and Troubleshoot Control Plane Protection](#)

[Exercise 4.3: Control Plane Protection for IPv6 Cisco IOS](#)

[Section 5 Threat Identification and Mitigation](#)

[Exercise 5.1: Preventing IP Address Spoofing on the Cisco ASA](#)

[Exercise 5.2: Monitor and Protect Against Wireless Intrusion Attacks](#)

[Exercise 5.3: Identifying and Protecting Against SYN Attacks](#)

[Exercise 5.4: Using NBAR for Inspection of HTTP Traffic with PAM and Flexible NetFlow](#)

[Section 6 Identity Management](#)

[Exercise 6.1: Cisco TrustSec—Dynamically Assigning Secure Group Tagging and SGACLs: 802.1X and MAB](#)

[Part A: Configuring SGTs on the Cisco ISE](#)

[Part B: Dynamically Assigning SGTs via 802.1X and MAB](#)

[Task 1: Cisco Access Point as an 802.1X Supplicant with SGTs](#)

[Task 2: Cisco IP Phone Using MAB and SGTs](#)

[Part C: Create the SGA Egress Policy](#)

[Exercise 6.2: Cisco TrustSec—NDAC and MACsec](#)

[Exercise 6.3: Cisco TrustSec—SGT Exchange Protocol over TCP](#)

[Part III Practice Lab 2 Solutions](#)

[Section 1 Perimeter Security](#)

[Solution and Verification for Exercise 1.1: Configure a Redundant Interface on ASA2](#)

[Skills Tested:](#)

[Solution and Verification](#)

[Configuration](#)

[Solution and Verification for Exercise 1.2: SSH Management Authentication and Local Command Authorization on ASA1](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Tech Notes](#)

[Solution and Verification for Exercise 1.3: Configuring Advanced Network Protection on the ASA](#)

[Skills Tested](#)

[Solution and Verification](#)

[Task 1: Botnet Traffic Filtering on ASA1](#)

[Task 2: Threat Detection on ASA2](#)

[Task 3: IP Audit](#)

[Configuration](#)

[Tech Notes](#)

[Solution and Verification for Exercise 1.4: Configure IPv6 on ASA2](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Tech Notes](#)

[*IPv6 Addressing Review*](#)

[*IPv6 Addressing Notation*](#)

[*IPv6 Address Types*](#)

[*IPv6 Address Allocation*](#)

[*IPv6 Addressing Standards*](#)

[Solution and Verification for Exercise 1.5: Cisco IOS Zone-Based Firewall with Support for Secure Group Tagging](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Tech Notes](#)

Section 2 Intrusion Prevention and Content Security

[Solution and Verification for Exercise 2.1: Configuring Custom Signatures on the Cisco IPS Sensor](#)

[Skills Tested](#)

[Solution and Verification](#)

[*Custom Signature to Track OSPF TTL*](#)

[*Custom Signature to Identify and Deny Large ICMP Packets*](#)

[*Custom Signature to Identify and Deny an ICMP Flood Attack*](#)

[Configuration](#)

[Tech Notes](#)

[*Risk Ratings*](#)

[*Understanding Threat Rating*](#)

[Solution and Verification for Exercise 2.2: Enable Support for HTTPS on the Cisco WSA](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Solution and Verification for Exercise 2.3: Enable User Authentication for Transparent Proxy Using LDAP](#)

[Skills Tested](#)

[Solution and Verification](#)

[Solution and Verification for Exercise 2.4: Guest User Support on the Cisco WSA](#)

[Skills Tested](#)

[Solution and Verification](#)

[WSA Configuration](#)

Section 3 Secure Access

[Solution and Verification for Exercise 3.1: Configure and Troubleshoot IPsec Static VTI with IPv6](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Tech Notes](#)

[Tip and Tricks](#)

[Static VTIs for IPv6 Using Preshared Keys](#)

[Solution and Verification for Exercise 3.2: Troubleshoot and Configure GETVPN](#)

[Skills Tested](#)

[Solution and Verification](#)

[Verify Network Connectivity](#)

[Configure and Verify the COOP Key Servers](#)

[Configure and Verify the Group Members](#)

[Configure and Verify DPD and Authorization](#)

[Configuration](#)

[Tech Notes](#)

[Key Server Design Considerations for IKE](#)

[Key Server Design Considerations for IPsec](#)

[Key Server Design Considerations for Traffic Encryption Key Lifetime](#)

[Key Server Design Considerations for ACLs in a Traffic Encryption Policy](#)

[Key Server Design Considerations for Key Encryption Key Lifetime](#)

[Rekey Retransmit Interval](#)

[Time-Based Antireplay](#)

[Key Server Design Considerations for Authentication Policies for GM Registration](#)

[Implementing Rekeying Mechanisms](#)

[Unicast Rekeying](#)

[Implementing Multicast Rekeying with No ASA Considerations](#)

[Implementing Multicast Rekeying Through the ASA in Routed Mode](#)

[Solution and Verification for Exercise 3.3: SSL Client and Clientless VPNs](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Tech Notes](#)

[*Importing Third-Party Trusted CA Certificates*](#)

[*Default Group Policy and Attribute Inheritance*](#)

[Solution and Verification for Exercise 3.4: Configure and Troubleshoot FlexVPN Site-to-Site Using RADIUS Tunnel Attributes](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Tech Notes](#)

[*IKEv2 Smart Defaults*](#)

[*IKEv2 Anti-Clogging Cookie*](#)

[*RADIUS Tunnel Attributes and IKEv2*](#)

[Solution and Verification for Exercise 3.5: Configure and Troubleshoot FlexVPN Remote Access \(Client to Server\)](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Tech Notes](#)

[*Debugging FlexVPN*](#)

[*Understanding IKEv2 Routing Options*](#)

Section 4 System Hardening and Availability

[Solution and Verification for Exercise 4.1: BGP TTL-Security through the Cisco ASA](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Tech Notes](#)

[Solution and Verification for Exercise 4.2: Configure and Troubleshoot Control Plane Protection](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Tech Notes](#)

[Solution and Verification for Exercise 4.3: Control Plane Protection for IPv6 Cisco IOS](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

Section 5 Threat Identification and Mitigation

[Solution and Verification for Exercise 5.1: Preventing IP Address Spoofing on the Cisco ASA](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Tech Notes](#)

[*Understanding Unicast Reverse Path Forwarding in Cisco IOS: Technology Overview*](#)

[*Understanding Unicast Reverse Path Forwarding: Deployment Guidelines*](#)

[*Understanding Unicast Reverse Path Forwarding: Other Guidelines*](#)

[Solution and Verification for Exercise 5.2: Monitor and Protect Against Wireless Intrusion Attacks](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Solution and Verification for Exercise 5.3: Identifying and Protecting Against SYN Attacks](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Tech Notes](#)

[*Configuring Maximum Connections*](#)

[*TCP Intercept and Limiting Embryonic Connections*](#)

[Solution and Verification for Exercise 5.4: Using NBAR for Inspection of HTTP Traffic with PAM and Flexible NetFlow](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Tech Notes](#)

[*Configuring a NetFlow Exporter*](#)

[*Comparing NetFlow Types*](#)

[*Migrating from Traditional Netflow to Flexible Netflow*](#)

Section 6 Identity Management

[Solution and Verification for Exercise 6.1: Cisco TrustSec—Dynamically Assigning Secure Group Tagging and SGACLs: 802.1X and MAB](#)

[Skills Tested](#)

[Solution and Verification](#)

[Part A: Configuring SGTs on the Cisco ISE](#)

[Part B: Dynamically Assigning SGT's via 802.1X and MAB](#)

[Part C: Create the SGA Egress Policy](#)

[Configuration](#)

[Tech Notes](#)

[IP Device Tracking](#)

[Solution and Verification for Exercise 6.2: Cisco TrustSec—NDAC and MACsec](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Tech Notes](#)

[Protected Access Credential](#)

[MACsec Overview](#)

[Solution and Verification for Exercise 6.3: Cisco TrustSec—SGT Exchange Protocol over TCP](#)

[Skills Tested](#)

[Solution and Verification](#)

[Configuration](#)

[Tech Notes](#)

[SXP on the Cisco WLC](#)

[Summary of Secure Group Access Features](#)

Part IV Appendixes

Appendix A Manual Configuration Guide

[Cisco Catalyst Switches: SW1, SW2](#)

[Cisco Routers R1, R2, R3, R4, R5, R6, R7](#)

[Cisco Router R6: Also Used as the CME Server](#)

[Cisco ASA Appliances ASA1, ASA2](#)

[Cisco WLC](#)

[Cisco IPS Sensor](#)

[Cisco WSA](#)

Appendix B Preparing for the CCIE Exam

[CCIE Certification Process](#)

[CCIE Security Written Exam](#)

[CCIE Security Lab Exam](#)

[Planning Resources](#)

[Assessing Strengths and Weaknesses](#)

[Training, Practice Labs, and Boot Camps](#)

[Books and Online Materials](#)

[Lab Preparation](#)

[Lab Exam Tips](#)

[A Word on Cheating...](#)

[**Appendix C Sample Written Exam Questions and Answers**](#)

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

For more than ten years, the CCIE program has identified networking professionals with the highest level of expertise. Fewer than 3 percent of all Cisco certified professionals actually achieve CCIE status. The majority of candidates who take the exam fail at the first attempt because they are not fully prepared; they generally find that their study plan did not match what was expected of them in the exam. These practice exercises are indicative of the types of questions you can expect in an actual exam. Completion of these exercises with a solid understanding of the solutions will be an indication of whether you are ready to schedule your lab or you need to reevaluate your study plan.

Exam Overview

The CCIE qualification consists of two separate exams, a two-hour written exam and an eight-hour hands-on lab exam that includes troubleshooting questions. Written exams are computer-based multiple-choice exams lasting two hours and available at hundreds of authorized testing centers worldwide. The written exam is designed to test your theoretical knowledge to ensure you are ready to take the lab exam; as such, you are eligible to schedule the lab exam only after you have passed the written exam. Having purchased this publication, it is assumed that you have passed the written exam and are ready to practice for the lab exam. The lab exam is an eight-hour hands-on exam in which you are required to configure a series of complex scenarios in strict accordance to the questions—it's tough but achievable. Current exam blueprint content information can be found at the following URL: https://learningnetwork.cisco.com/community/certifications/ccie_security

Study Roadmap

Taking the lab exam is all about experience: You can't expect to take it and pass after just completing your written exam, relying on your theoretical knowledge. You must spend countless hours of rack time configuring features and learning how protocols interact with one another. To be confident enough to schedule your lab exam, review the following outlined points.

Assessing Your Strengths

Using the content blueprint, determine your experience and knowledge in the major topic areas. For areas of strength, practicing for speed should be your focus. For weak areas, you might need training or book study in addition to practice.

Study Materials

Choose lab materials that provide configuration examples and take a hands-on approach. Look for materials approved or provided by Cisco and its Learning Partners.

Hands-On Practice

Build and practice your lab scenarios on a per-topic basis. Go beyond the basics and practice additional features. Learn the **show** and **debug** commands along with each topic. If a protocol has multiple ways of configuring a feature, practice all of them.

Cisco Documentation

Make sure you can navigate Cisco documentation with confidence because you will have limited access to cisco.com when you take the lab exam.

Further Study Information and Exam-Taking Tips

[Appendix B](#) of this guide outlines additional study information and reviews exam preparation and exam-taking tips and guidelines.

Part I: Lab Topology Components, Cabling, and Routing and Switching Configuration

The exercises in this lab guide are based on topics outlined in the CCIE Security Lab Exam Topics v4.0 and CCIE Security Lab Exam Checklist v4.0. The latest version of these documents can be found at https://learningnetwork.cisco.com/community/certifications/ccie_security.

The CCIE Security v4.0 Lab Exam was built using inputs from security subject matter experts and is based on real-world deployments and industry-relevant requirements.

The information in this guide serves not only as a practice tool for prospective CCIE Security exam candidates, but through the use of a real-world lab topology and in-depth solutions and technical notes, also serves as a useful reference for any security professional involved with practical customer deployments that use Cisco products and solutions.

This guide consists of two practice lab sessions. Both labs are based on the same topology and may be run as independent exercises or combined to form a complete complex security solution that is representative of many typical customer deployments and provides exam candidates with a challenging practice environment.

- Lab 1 focuses on more basic exercises and includes several device initialization tasks.
- Lab 2 is a more advanced set of exercises that builds upon the concepts presented in Lab 1.

Exercise solutions are presented as a series of highlighted outputs derived from the actual working configuration as well as important **show** and **debug** commands. Each solution also highlights key concepts, caveats, and potential issues to avoid.

Tech Notes are included to further explain the solution to an exercise and provide practical implementation tips. Tech Notes also are the catalyst for further reading and research. Many discussion points in the Tech Notes cover subjects that are listed in the “CCIE Security Written Exam Topics v4.0” document.

The material covered in this guide is designed to help a candidate prepare for the CCIE Security exam by providing a complex topology that forces problem solving, troubleshooting, and policy design using topics and equipment that are detailed in the official exam documents.

Each lab groups exercises within the top-level domains defined in the CCIE Security Lab Exam Topics v4.0:

1. Perimeter Security and Services
2. Intrusion Prevention and Content Security
3. Confidentiality and Secure Access
4. System Hardening and Availability
5. Threat Identification and Mitigation
6. Identity Management

Disclaimer

The purpose of this guide is not to be the sole study resource for preparing for the CCIE Security Exam. Exercises presented in this guide are not a complete reproduction of any official exam.

Equipment List

The equipment list in [Table 1](#) was used as the basis for this lab. The type of equipment, the number of devices, and the cabling scheme are not representations of the actual CCIE Security Lab Exam. The “CCIE Security Lab Equipment and Software v4.0” document is available at https://learningnetwork.cisco.com/community/certifications/ccie_security.

Device	Model*	Software**	Interfaces***
R1	ISR	15.1(3)T3 or above k9 image	1 GE
R2	ISR G2 (required for IKEv2)	15.2(2)T1 or above Security license	1 GE
R3	ISR	15.1(3)T3 or above k9 image	1 GE
R4	ISR G2 (required for IKEv2)	15.2(2)T1 or above Security license	1 GE
R5	ISR	15.1(3)T3 or above k9 image	1 GE
R6	ISR G2 (required for IKEv2 and TrustSec SGT)	15.2(2)T1 or above Security and UC license	2 GEs
R7	ISR G2 (required for IKEv2)	15.2(2)T1 or above Security license	1 GE
SW1	3750-X (any device that supports SXP, SGTs)	15.0(2)SE4 or above ipservices license	24 ports
SW2	3750-X (any device that supports SXP, SGTs)	15.0(2)SE4 or above ipservices license	24 ports
ASA1	5520 (5510 or above)	8.4(5) security plus license	4 GEs
ASA2	5520 (5510 or above)	8.4(5) security plus license	4 GEs
IPS	4240 (4220 or above)	7.0(8)E4	4 GEs, 1 mgmt
ISE	VM (ESX 5.0)	V1.1	
WSA	VM (ESX 5.0) or S170 or above	V7.7.5	
ACS	VM (ESX 5.0)	V5.3	
Win2k	VM (ESX 5.0)	Win2k R8 server	1 GE
Test-PC****	VM (ESX 5.0)	Win7	2 GEs (min 1 GE)
WLC	5508	7.2.111.3	2 GEs
AP1	CAP3502	12.4(25e)JA2	1 GE
AP2	LAP1262	12.4(25e)JA2	1 GE
IP Phone	7971	7971 SW on R6	2 ports

* Minimum hardware, can use Cisco IOS on Unix (IOU)

** Software versions can change during the life cycle of the Lab Exam version; only the topics advertised in the exam topic documents can be tested.

*** Minimum interfaces actually used in this lab. This lab was developed using some IOU-based routers that have the designation EthernetX.

**** This Test-PC uses one interface to connect to the IP Phone. The other may be used to connect to the 192.168.2.0 subnet.

Table 1 *Lab Hardware and Software List*

Note that software versions used in the guide might differ from those used in the official lab exam; however, only features covered by the CCIE Security Lab Exam Topics v4.0 list are presented.

General Guidelines

1. Several routers used in the development of this guide were IOU virtual devices, which is why many outputs display interfaces as Ethernet rather than GigabitEthernet. This does not impact the features covered in the labs.
2. Lab exercises may be configured as individual solutions if you do not have access to enough equipment to create the complete topology shown in [Diagram 2](#).
3. The Cisco ISE, Cisco WSA, CiscoSecure ACS, Microsoft Windows 2000 Server, and Microsoft Windows 7 Professional Test-PC are running on a VMware ESX 5.0 server. These devices may be run as standalone hardware if VMware is not available.
4. The Test-PC may be single homed and connected to the IP Phone only. Any tasks that require connectivity from a workstation in the 192.168.2.0 subnet can be done using the Windows 2000 server as has been done in the development of this guide.
5. The base routing, wireless, and Cisco Call Manager Express functionality is provided in the initial configuration files. Preconfiguration steps are included in [Appendix A](#), “[Manual Configuration Guide](#),” and initial device configurations are included in an online file. Do not alter any base configuration information because this can impact the solutions to the exercises.
6. The Cisco Wireless LAN Controller (WLC) is configured to manage and push configuration policy to the two Access Points (AP). The Cisco APs will not need to be configured individually.
7. There is no requirement in this lab to test wireless connectivity from the Test-PC. You are encouraged to do additional configuration of wireless clients for practice.
8. The Cisco IP Phone is not required to make calls. The only requirement in this guide is to bootstrap the phone and have it register with the CME.
9. Each question will outline tasks to be performed and includes notes and warnings. Read each exercise completely before beginning any configuration.
10. Unless explicitly defined in the question, you may name configuration constructs, such as access lists, policy maps, class maps, and so on.
11. Read through each lab in its entirety before beginning configuration to identify any exercise dependencies.
12. If any additional interfaces are to be configured, refer to the IP addressing summary in [Table 2](#) for address information.

Device	Interface	IP Address (v4 and v6)/ Mask	VLAN	
R1	Ethernet0/0	10.50.100.1/24 2001:128:BAD:64::1/64	100	
	Loopback1	3001:0:1:3::/64		
	Tunnel0	Created by PIM-SM		
	Tunnel1	Created by PIM-SM		
	Tunnel2	Created by PIM-SM		
	Tunnel6	10.50.101.1/24		
	Tunnel7	10.50.102.1/24		
	R2	Ethernet0/0.1		10.50.100.2/24 2001:128:BAD:64::2/64
Ethernet0/0.2		10.10.110.1/24	110	
Ethernet0/0.3		10.10.120.1/24	120	
Ethernet0/0.4		10.10.130.1/24	130	
Loopback0		172.17.100.2/24		
Loopback1		3001:0:2:3::/64		
Tunnel0		Created by PIM-SM		
Tunnel1		Created by PIM-SM		
Tunnel2		Created by PIM-SM		
Tunnel8		10.50.201.1/24		
Tunnel9		10.50.202.1/24		
R3	Ethernet0/1	10.50.30.3/24	30	
	Loopback0	172.16.33.3/24		
	Loopback1	10.3.3.3/24		
	Loopback10	10.50.50.4/24 (TEST only)		
	Tunnel1	172.17.70.3/24		

R4	Ethernet0/1	10.50.30.4/24 2001:DB9:30::4/64	30
	Loopback0	172.16.34.4/24	
	Loopback1	10.4.4.4/24 2011::/64	
	Loopback2	172.18.34.4/24	
	Tunnel0	IP negotiated	
	Tunnel1	172.17.70.4/24	
	Tunnel2	2001:DBA::1:2/64	
	<hr/>		
R5	Ethernet0/0	10.50.90.5/24	90
	Loopback0	172.16.35.5/24	
	Loopback1	1010::/64	
	Tunnel0	2001:DB8::1:5/64	
	Tunnel1	172.17.70.5/24	
<hr/>			
R7	Ethernet0/1	10.50.40.7/24 2001:DB8:40::7/64	40
	Loopback0	172.18.107.7/24	
	Loopback1	10.7.7.7/24 1011::/64	
	Loopback2	172.17.70.7/24	
	Tunnel0	Created by PIM-SM	
	Tunnel1	172.16.70.7/24	
	Tunnel2	2001:DBA::1:1/64	
	Tunnel3	Created by PIM-SM	
	Tunnel7	10.50.102.7/24	
	Tunnel9	10.50.202.7/24	
<hr/>			

R6	GigabitEthernet0/0	10.50.80.6/24	60	
	GigabitEthernet0/1	10.50.70.6/24	70	
	Loopback0	172.18.106.6/24		
	Loopback1	2010::/64		
		10.7.6.6/24		
	Loopback2 (CME)	10.50.170.6/24		
	Loopback3	172.16.70.6/24		
	Loopback4	172.17.60.6/24		
	Loopback6	10.50.60.6/24		
	Tunnel0	2001:DB8::1:6/64		
	Tunnel1	Created by PIM-SM		
	Tunnel2	Created by PIM-SM		
	Tunnel6	10.50.101.6/24		
	Tunnel8	10.50.201.6/24		
	Virtual-Template1	172.17.70.6/24		
	ASA1 c1	GigabitEthernet0/0	10.50.80.20/24	80
		GigabitEthernet0/2.1	192.168.2.20/24	101
	GigabitEthernet0/2.2	192.168.1.20/24	102	
ASA1 c2	GigabitEthernet0/0	10.50.80.30/24	80	
	GigabitEthernet0/1	10.50.90.20/24	90	
	GigabitEthernet0/3	10.50.100.20/24	100	
ASA2	GigabitEthernet0/0	10.50.50.20/24	50	
	GigabitEthernet0/1			
	GigabitEthernet0/2	10.50.40.20/24	40	
		2001:db8:40::20/64		
	GigabitEthernet0/3	10.50.30.20/24	30	
		2001:db9:30::20/64		

WLC	GigabitEthernet0/0/1	10.50.100.10/24	100
AP1	DHCP	10.50.100.x/24	100
AP2	DHCP	10.50.77.x/24	77
IPS	Management0/0	192.168.2.100/24	101
SW1	Vlan101	192.168.2.5/24	101
	Vlan102	192.168.1.5/24	102
	Vlan192	192.168.100.1/24	192
	Vlan70	10.50.70.4/25	70
SW2	Vlan77	10.50.77.5/24	77
	Vlan9	10.50.9.5/24	9
	Vlan99	10.50.99.5/24	99
	Vlan50	10.50.50.5/24	50
	Vlan70	10.50.70.5/24	70
IP Phone	DHCP	10.50.9.x/24	9
Win7k	Nic1: DHCP (Phone)	10.50.99.x/24	99
WSA	M1	192.168.2.50/24	101
ACS		192.168.2.18/24	101
ISE		192.168.2.15/24	101
Test-PC		192.168.2.30/24	101
Win2k Server		192.168.2.25/24	101

Table 2 *Lab Guide Addressing Scheme Summary*

13. Many exercises specify usernames and passwords. Specific usernames are often used in solution outputs, and it is recommended that these names not be changed. You may set passwords. They are included in the guide for your information.
14. Do not configure Authentication, Authorization, Accounting (AAA) services on the console or AUX ports of devices to avoid being inadvertently locked out of a device.
15. Each solution will include the specific configuration required for that exercise for all devices. Final device configuration files are included in an online file. This file does not include complete configurations for the VMware-based machines, Cisco WLC, and Cisco access points.
16. Verification color codes are used to highlight solution outputs. Command/output syntax in **red** must match; other parameters can vary. **Required tasks** indicates that this step must be performed to generate the appropriate output for verification.

For all “Solution and Verification” sections for each lab solution, you will see the following legend (denoted as applicable):

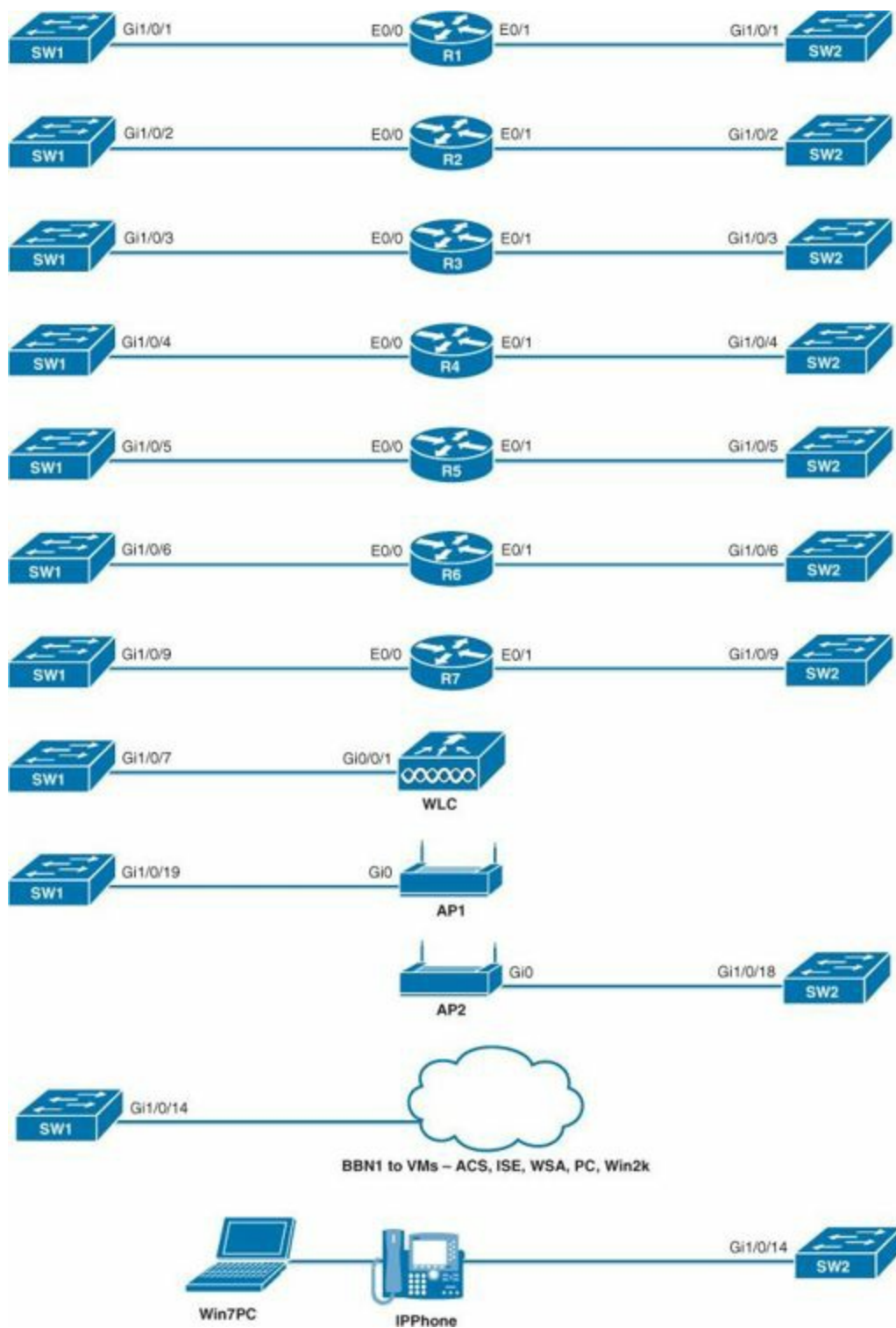
For all verification syntax that follows:

- Required output appears in **red**.
- Required tasks appear in **indigo**.
- Nonzero/non-null syntax appears in **violet**.
- Variable syntax appears in **green**.

- Troubleshooting syntax appears in cyan.

Prelab Setup Instructions

There is some flexibility in the type of routers and switches that may be used to build the complete lab topology as shown in [Diagram 2](#); however, as indicated in the equipment list in [Table 1](#), there are some minimum requirements for the exercises. [Diagram 1](#) outlines the cabling plan needed to build the complete lab topology defined in [Diagram 2](#).



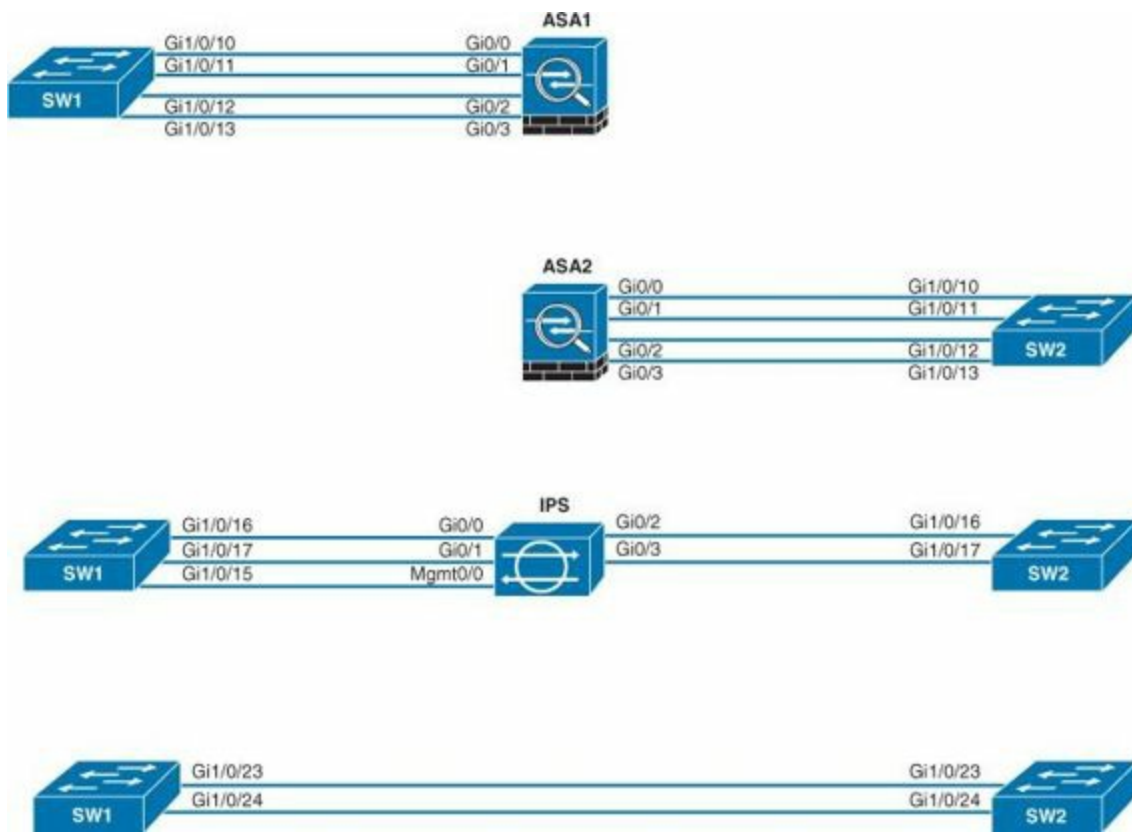


Diagram 1 *Lab Switch Cabling Guide*

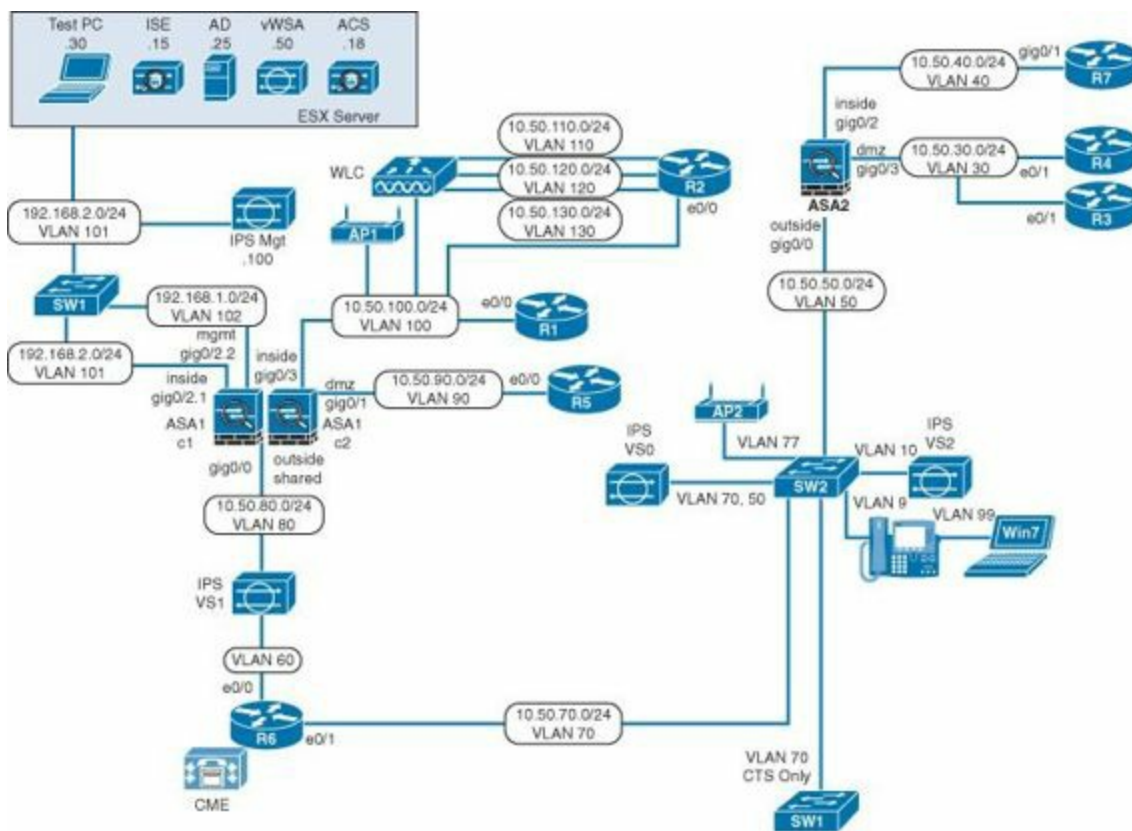


Diagram 2 *Lab Logical Topology Diagram*

The same cabling and topology are used for Lab 1 and Lab 2, and devices do not need to be reinitialized when beginning Lab 2. For reference, a manual initialization guide is included in [Appendix A](#). Initial configuration files are provided from the Downloads link at www.ciscopress.com/title/9781587144141 and may be cut and pasted via the device command-line

interface (CLI). Note that some changes to these configuration files might be required to accommodate any differences in hardware.

Catalyst Switchport Cabling Diagram

[Diagram 1](#) illustrates the physical cabling details for the Catalyst switches. There is some flexibility in the interface types used (FastEthernet versus GigabitEthernet, for example); however, the initial configuration files for the switches might need to be edited to accommodate any differences.

Lab Topology Diagram

[Diagram 2](#) illustrates the logical lab topology diagram that is used by both Lab 1 and Lab 2. It is important to be very familiar with this topology because it is the blueprint for every exercise in this guide. The major VLAN and subnet designators are included in the diagram. Complete addressing information is presented in [Table 2](#).

Lab Guide Addressing Scheme

[Table 2](#) outlines all IP addressing information, as well as VLAN identifiers. Both IPv4 and IPv6 addressing are used in this guide. Many of the addresses and VLANs are preconfigured by the initial configuration files. You will add some devices, such as the Cisco ASAs. Do not change any preconfigured addressing details.

Lab Guide IP Routing Details

The underlying lab guide routing protocols and some static routes are preconfigured as illustrated in [Diagram 3](#) (IPv4) and [Diagram 4](#) (IPv6) and summarized in [Table 3](#) through [Table 7](#). You will be required to enhance some routing features and add static routes as part of lab exercise requirements. Do not change any preconfigured routing details.

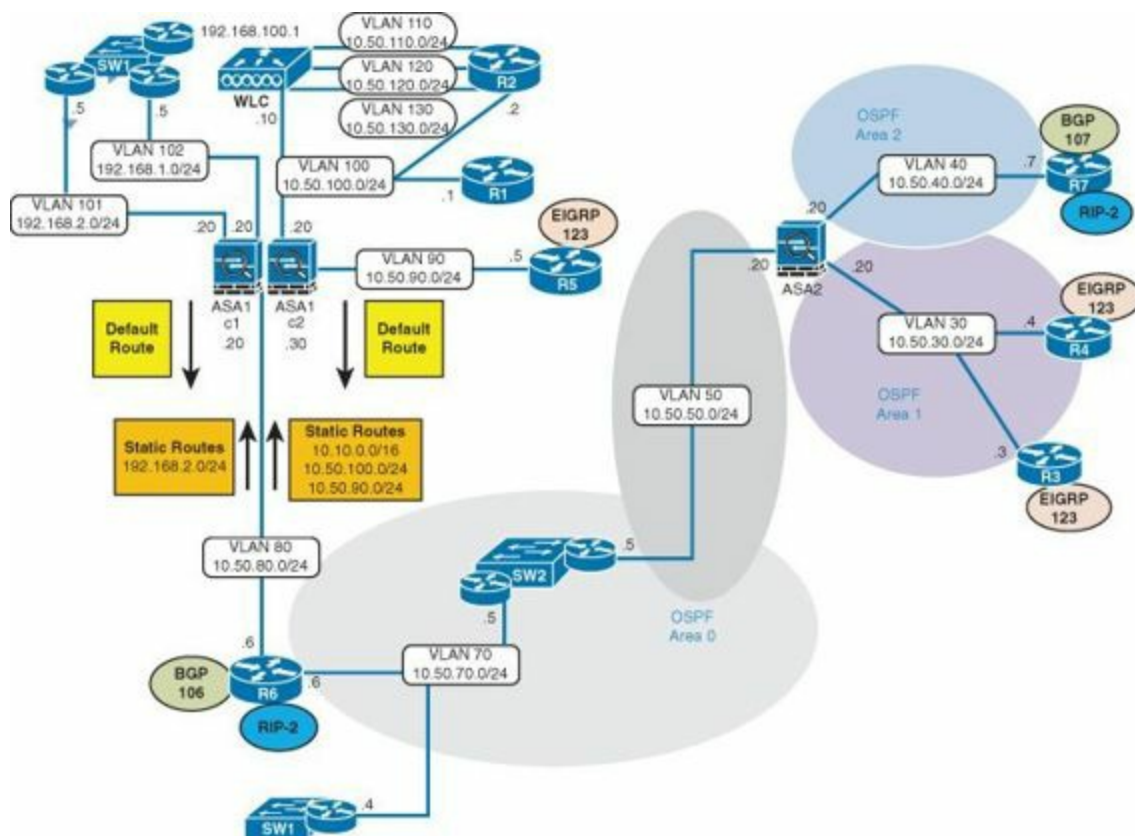


Diagram 3 IPv4 Addressing and Routing Details

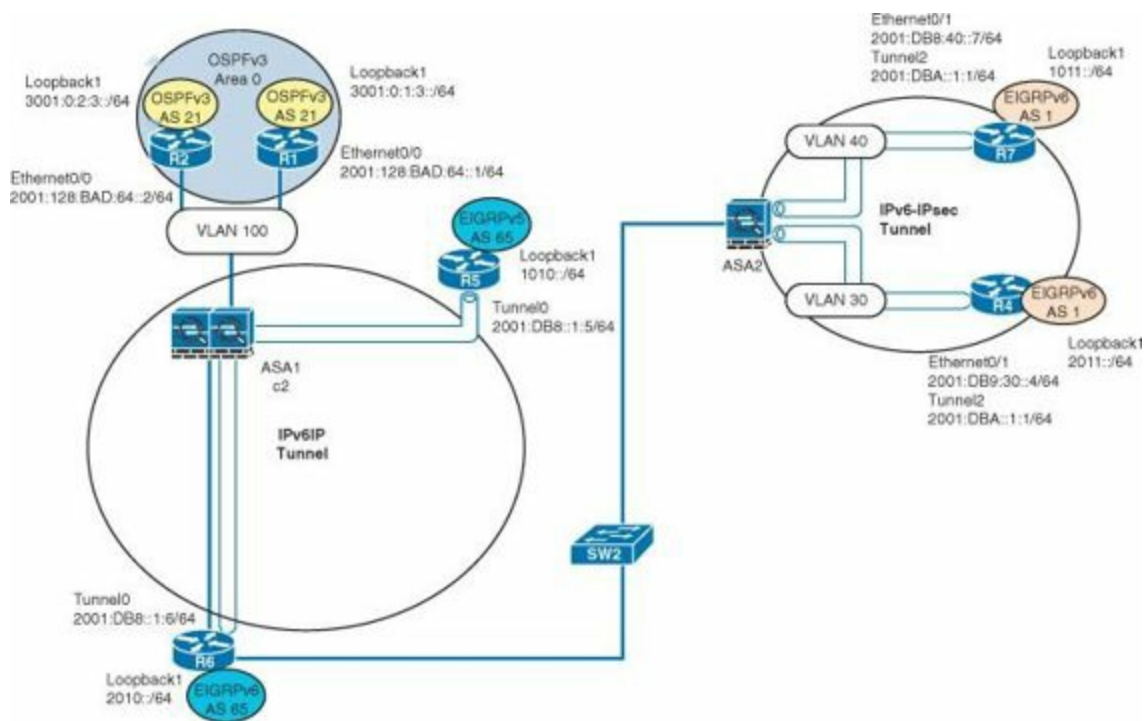


Diagram 4 IPv6 Addressing and Routing Details

Router	AS	Networks
R3	1	10.50.30.0 0.0.0.255 area 1
R4	1	10.50.30.0 0.0.0.255 area 1
R6	1	10.50.70.0 0.0.0.255 area 0
R7	1	10.50.40.0 0.0.0.255 area 2 10.7.7.0/24 area 2
SW2	1	10.50.9.0 0.0.0.255 area 0 10.50.50.0 0.0.0.255 area 0 10.50.70.0 0.0.0.255 area 0 10.50.77.0 0.0.0.255 area 0 10.50.99.0 0.0.0.255 area 0
ASA2	1	10.50.30.0 255.255.255.0 area 1 10.50.40.0 255.255.255.0 area 2 10.50.50.0 255.255.255.0 area 0

Table 3 *OSPF Routing Details*

Router	AS	Networks
R3	123	172.16.33.0 0.0.0.255 172.17.70.0 0.0.0.255
R4	123	172.16.34.0 0.0.0.255 172.17.70.0 0.0.0.255
	1	2011::/64
R5	123	172.16.35.0 0.0.0.255 172.17.70.0 0.0.0.255
	65	1010::/64
R6	65	2010::/64
R7	1	1011::/64

Table 4 *EIGRP Routing Details*

Router	AS/Neighbor	Networks
R6	106/10.50.40.7	172.18.106.0/24
R7	107/10.50.70.6	172.18.107.0/24

Table 5 *BGP Routing Details*

Router	Networks
R6	172.16.0.0 172.17.0.0
R7	172.16.0.0 172.17.0.0

Table 6 *RIPv2 Routing Details*

Router	Route	Next Hop
R1	0.0.0.0 0.0.0.0	10.50.100.20
R2	0.0.0.0 0.0.0.0	10.50.100.20
R3	10.4.4.0 255.255.255.0	10.50.30.20
R4	10.3.3.0 255.255.255.0	10.50.30.20
	::/0	2001:DB9:30::20
R5	0.0.0.0 0.0.0.0	10.50.90.20
R6	10.10.0.0 255.255.0.0	10.50.80.30
	10.50.60.0 255.255.255.0	10.50.80.30
	10.50.90.0 255.255.255.0	10.50.80.30
	10.50.100.0 255.255.255.0	10.50.80.30
	192.168.2.0 255.255.255.0	10.50.80.20
	192.168.100.0 255.255.255.0	10.50.80.20
R7	::/0	2001:DB8:40::20
SW1	0.0.0.0 0.0.0.0	192.168.2.20
ASA1/c1 (outside)	0.0.0.0 0.0.0.0	10.50.80.6
ASA1/c1 (inside)	192.168.100.0 255.255.255.0	192.168.2.5
ASA1/c2 (outside)	0.0.0.0 0.0.0.0	10.50.80.6
ASA1/c2 (inside)	10.10.0.0 255.255.0.0	10.50.100.2
ASA2 (dmz)	10.3.3.0 255.255.255.0	10.50.30.3
ASA2 (dmz)	10.4.4.0 255.255.255.0	10.50.30.4

Table 7 Static Routing Details

VPN Solutions Diagrams

[Diagram 5](#) through [Diagram 10](#) are additional diagrams that highlight several of the VPN exercises and are referred to within each exercise as required.

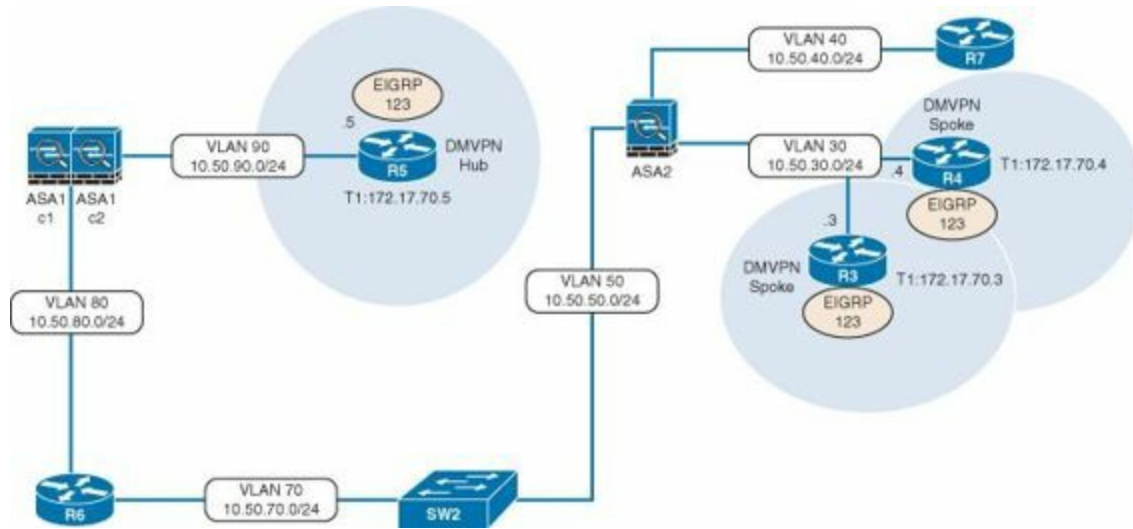


Diagram 5 *Secure Access DMVPN Lab*

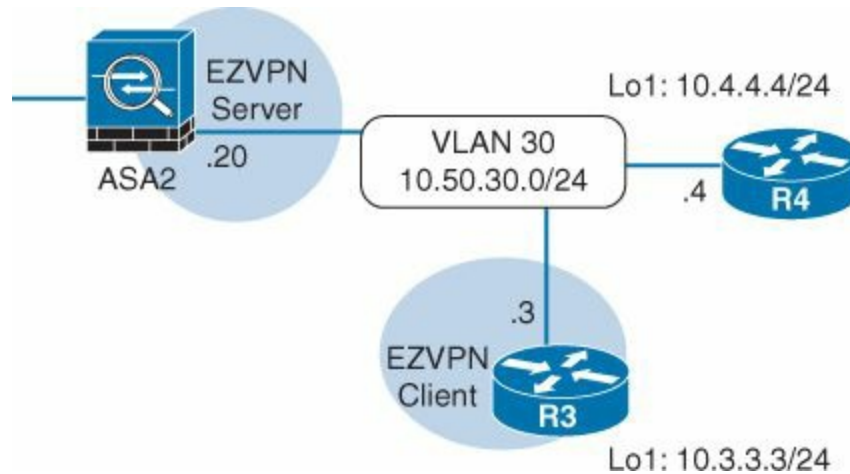


Diagram 6 *Secure Access EZVPN Lab*

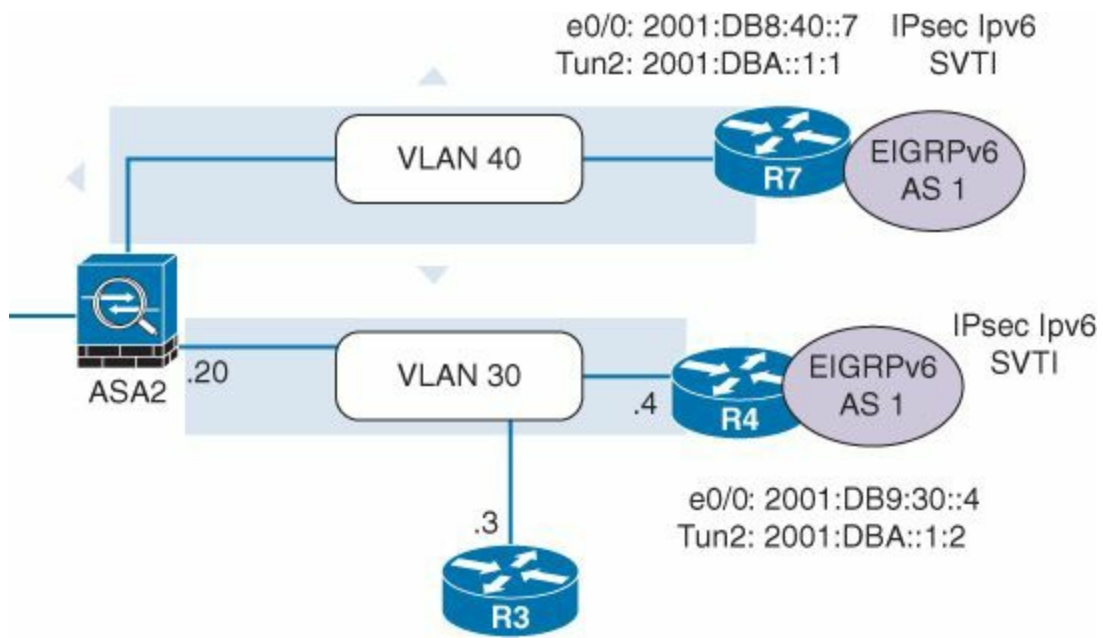


Diagram 7 *Secure Access IPsec IPv6 SVTI Lab*

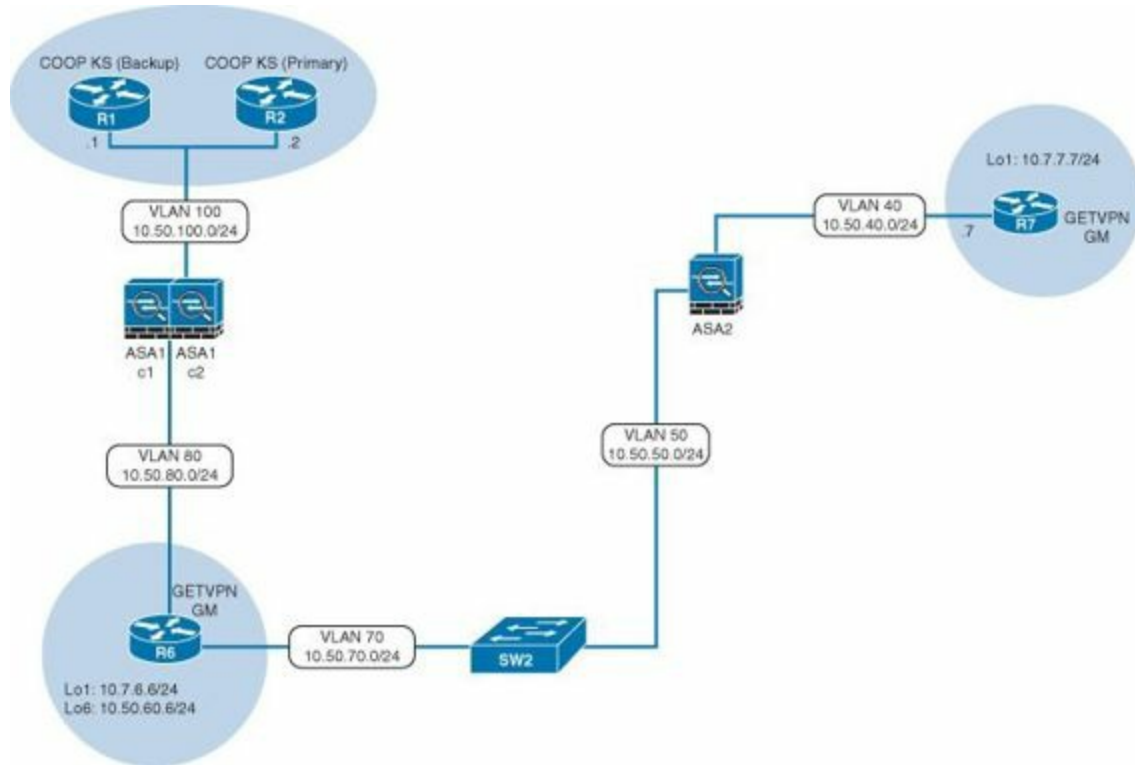


Diagram 8 *Secure Access GETVPN Lab*

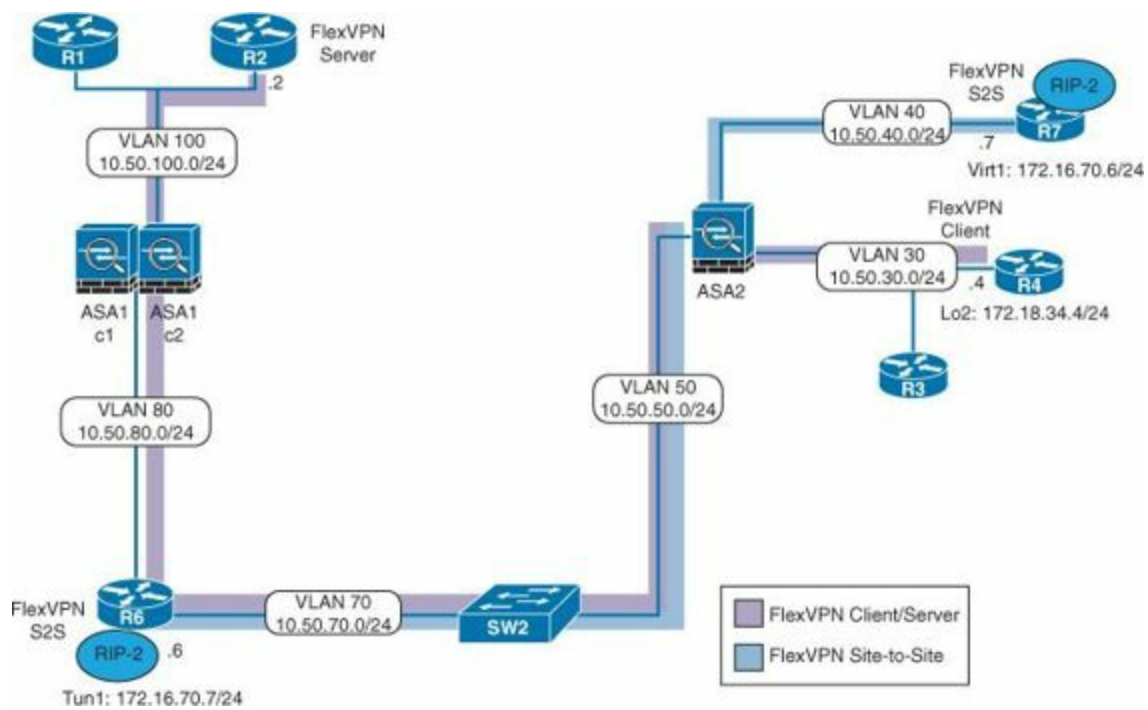


Diagram 9 *Secure Access FLEXVPN Lab*

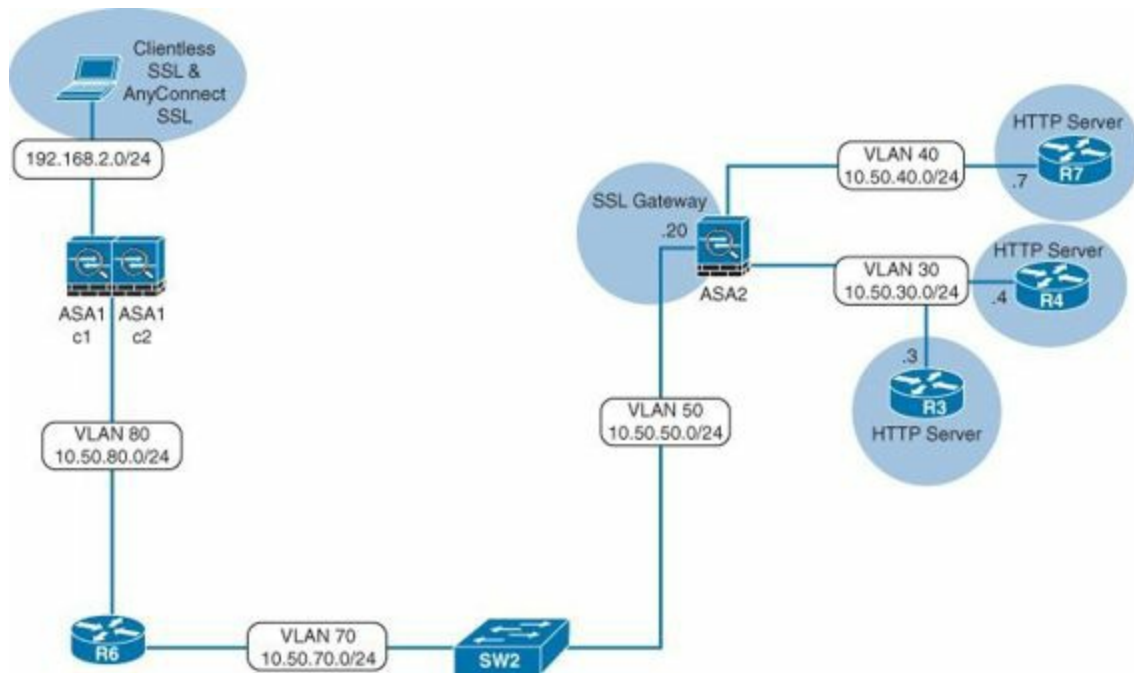


Diagram 10 *Secure Access SSLVPN Lab*

Initial Device Configurations

Initial configuration files may be cut and pasted from the online resource file.

Final Configuration Files

Final configuration files that incorporate solutions to both Lab 1 and Lab 2 are presented in the online resource file.

CCIE Security Exam Study and Preparation Tips

Information to help study and prepare for the CCIE Security Exam is presented in [Appendix B](#), “[Preparing for the CCIE Security Exam](#).”

CCIE Security Written Exam

[Appendix C](#), “[Sample Written Exam Questions and Answers](#),” includes some sample written exam questions and answers designed to give candidates an idea of what to expect. Topics are taken from the CCIE Security Written Exam Topics v4.0.

Part II: Practice Lab 1

Practice Lab 1

Section 1: Perimeter Security and Services

Securing the perimeter around important networks and devices is a fundamental part of network protection. In this section, you are asked to implement firewall services that include not only traditional features, such as Network Address Translation (NAT) and traffic inspection, but also secured routing features. This section focuses on initializing and configuring the Cisco Adaptive Security Appliance (ASA) in both single- and multi-context modes. Connectivity through perimeter devices must be verified before moving on to other exercises in this guide.

Exercise 1.1: Initialize the Cisco ASA in Multi-Context Routed Mode

ASA1 must be configured as a multi-context firewall using a shared outside interface. In addition, context c1 and the admin context will be using VLANs for logical segregation on a physical interface. The logical placement of ASA1 is shown in the network topology presented in [Diagram 2](#) in [Part I](#). [Table 1-1](#) through [Table 1-6](#) outline the initialization requirements.

Hostname	ASA1
Enable Password	cisco

Table 1-1 Administration

Physical Interface	Logical Name	VLAN	config-url
GigabitEthernet0/2.2	mgmt (management traffic only)	102	disk0:/admin.cfg

Table 1-2 Context Admin

Physical Interface	Logical Name	VLAN	config-url
GigabitEthernet0/0	outside	80	disk0:/c1.cfg
GigabitEthernet0/2.1	inside	101	

Table 1-3 Context c1

Physical Interface	Logical Name	VLAN	config-url
GigabitEthernet0/0	outside	80	disk0:/c2.cfg
GigabitEthernet0/1	dmz	90	
GigabitEthernet0/3	inside	100	

Table 1-4 Context c2

Context	Interface	IP Address/Mask	Nameif	Security Level
admin	GigabitEthernet0/2.2	192.168.1.20/24	mgmt	100
c1	GigabitEthernet0/0	10.50.80.20/24	outside	0
	GigabitEthernet0/2.1	192.168.2.20/24	inside	100
c2	GigabitEthernet0/0	10.50.80.30/24	outside	0
	GigabitEthernet0/1	10.50.90.20/24	dmz	50
	GigabitEthernet0/3	10.50.100.20/24	inside	100

Table 1-5 *Context Initialization Details*

Context	Type	Network Prefix	Next Hop
c1	Default	0.0.0.0/0	10.50.80.6
c2	Default	0.0.0.0/0	10.50.80.6
admin	Default	0.0.0.0/0	192.168.1.5
c2	Static	10.10.0.0/16	10.50.100.2

Table 1-6 *Routing Details*

Use names and addresses exactly as outlined. Remember that names are case sensitive.

Notes

- To validate your configuration, ensure that all interfaces in all contexts are up. You should ensure that Internet Control Message Protocol (ICMP) is permitted through each context to test connectivity and routing to the major subnets in the topology. You may use **permit icmp any any** for this purpose. Refer to [Part I](#) of this guide for information on the network addressing used in the topology.
- You might need to add or modify the configuration of switches and routers to ensure you have full connectivity.
- Some subnets might not be accessible until the configuration of ASA2 (see [Exercise 1.2](#)) and the Cisco IPS sensor ([Exercise 2.1](#)) is complete.
- The subinterface used for management traffic (admin context) must connect to inside secure hosts for management purposes only.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 1.1: Initialize the Cisco ASA in Multi-Context Routed Mode.](#)”

Exercise 1.2: Configure Routing and Basic Access on ASA2

In this exercise, ASA2 should be configured in single-context routed mode with support for Open Shortest Path First (OSPF). [Table 1-7](#) through [Table 1-10](#) provide the necessary configuration details. Use names exactly as they are shown; remember that they are case sensitive. You will not need to change any of the OSPF parameters on neighboring routers. Refer to [Diagram 2](#) and [Diagram 3](#) in [Part I](#) for device placement, addressing, and routing details.

Hostname	ASA2
Enable Password	cisco

Table 1-7 Administration

Interface	IP Address/Mask	Nameif	Security Level
GigabitEthernet0/0	10.50.50.20/24	outside	0
GigabitEthernet0/2	10.50.40.20/24	inside	100
GigabitEthernet0/3	10.50.30.20/24	dmz	50

Table 1-8 Interface Initialization Details

Interface	Type	Network Prefix	Next Hop
dmz	Static	10.3.3.0/24	10.50.30.3
dmz	Static	10.4.4.0/24	10.50.30.4

Table 1-9 Static Routing Details

Interface	Area	Network Prefix	Network Mask
outside	0	10.50.50.0	255.255.255.0
dmz	1	10.50.30.0	255.255.255.0
inside	2	10.50.40.0	255.255.255.0

Table 1-10 OSPF Routing Details

Notes

- To validate your configuration, ensure that all interfaces are up. You should ensure that ICMP is permitted through the firewall to test connectivity and routing to the major subnets in the topology. Refer to [Part I](#) of this guide for information on the network addressing used in the topology.
- You might need to add or modify the configuration of switches and routers to ensure you have full connectivity.
- Some subnets might not be accessible until the configuration of ASA1 (in [Exercise 1.1](#)) and the Cisco IPS sensor (in [Exercise 2.1](#)) is completed.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 1.2: Configure Routing and Basic Access on ASA2.](#)”

Exercise 1.3: Configure IP Services on ASA1

This exercise has four tasks that build on the initial configuration of ASA1 [Exercise 1.1](#). You may use any names for configuration elements such as access lists or objects, unless otherwise specified. Note that because the version of software currently running on ASA1 is post 8.3, the NAT configuration tasks will require the use of objects. Refer to [Diagram 2](#) and [Diagram 3](#) in [Part I](#) for device placement and addressing details.

Task 1: Configure Network Object NAT

Task 2: Configure Twice NAT

Task 3: Configure and Troubleshoot NTP Services Using Authentication

Task 4: Configure Support for IPv6 in IPv4 Tunneling Through ASA1

Task 1: Configure Network Object NAT

Use network object NAT to translate 10.50.90.5/32 on R5 to 10.50.80.50/32 in the appropriate context. This translation must allow bidirectional communication.

Task 2: Configure Twice NAT

Using Twice NAT, create a policy that will translate network 10.50.100.0/24 to the range 10.50.80.100–10.50.80.150 if the destination is 10.50.50.0/24. Translation for this task is unidirectional.

Task 3: Configure and Troubleshoot NTP Services Using Authentication

Network Time Protocol (NTP) on ASA1 using authentication is required with the NTP master service, which is partially configured on SW1 as follows:

[Click here to view code image](#)

```
SW1# show run | begin ntp
ntp authentication-key 1 md5 cisco
ntp source Vlan102
ntp access-group peer 1
ntp master 2
```

Complete the configuration and troubleshoot any issues using the following outputs to verify your solution:

[Click here to view code image](#)

```
ASA1# show ntp associations detail
192.168.1.5 configured, authenticated, our_master, sane, valid, stratum 2
```

```
ASA1# show ntp status
Clock is synchronized, stratum 3, reference is 192.168.1.5
```

Task 4: Configure Support for IPv6 in IPv4 Tunneling Through ASA1

Enable support for the ipv6ip tunnel configured between the tunnel endpoints 10.50.80.6 (R6) and 10.50.90.5 (R5). This configuration will be important for the completion of [Exercise 5.1](#).

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 1.3: Configure IP Services on ASA1](#).”

Exercise 1.4: Configure IP Routing Security on ASA2

There are two tasks in this exercise that will focus on configuring the ASA2 to support dynamic routing protocols. Refer to [Diagram 3](#) for routing protocol and addressing details.

Task 1: BGP Connectivity Through the ASA2

External Border Gateway Protocol (eBGP) has been preconfigured on R7 and R6 in Autonomous Systems 107 and 106, respectively. The BGP peering function cannot establish a session between these two routers through ASA2. Configure a solution that will enable the BGP peers to establish a connection. The following outputs can be used to verify your solution:

[Click here to view code image](#)

```
R6# show ip bgp
```

```
BGP table version is 3, local router ID is 172.18.106.6
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,  
r RIB-failure, S
```

```
Stale, m multipath, b backup-path, x best-external, f RT-Filter, a additional-path
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 172.18.106.0/24	0.0.0.0	0		32768	?
*> 172.18.107.0/24	10.50.40.7	0		0	107 ?

```
R7# show ip bgp
```

```
BGP table version is 5, local router ID is 172.18.107.7
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,  
r RIB-failure, S
```

```
Stale, m multipath, b backup-path, x best-external, f RT-Filter, a additional-path
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 172.18.106.0/24	10.50.70.6	0		0	106 ?
*> 172.18.107.0/24	0.0.0.0	0		32768	?

Task 2: OSPF Authentication for Routing Update Security

MD5 authentication is required in OSPF area 2. Configure a solution for this area only, and ensure that OSPF routing information is still correctly exchanged between neighbors.

Use the key cisco123.

The following outputs will verify your solution:

[Click here to view code image](#)

```
R7# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.50.50.20	1	FULL/BDR	00:00:32	10.50.40.20	GigabitEthernet0/1

```
ASA2# show ospf neighbor inside
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.18.107.7	1	FULL/DR	0:00:38	10.50.40.7	inside

```
ASA2# show ospf
Area 2
  Number of interfaces in this area is 1
  Area has message digest authentication
```

```
R7# show ip ospf
Area 2
  Number of interfaces in this area is 2 (1 loopback)
  Area has message digest authentication
```

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 1.4: Configure IP Routing Security on ASA2.](#)”

Section 2: Intrusion Prevention and Content Security

This section covers tasks applicable to some specialized Cisco appliances, the Intrusion Prevention Sensor (IPS) and the Web Services Appliance (WSA). Both devices will be initialized and deployed into the network topology as shown in [Diagram 1](#) and [Diagram 2](#) in [Part I](#). The single IPS appliance will be logically partitioned using various deployment modes of operation to service distinct traffic flows in the network. The WSA will handle redirected traffic of interest via Web Cache Communication Protocol (WCCP) from the Cisco ASA. It is important to verify whether traffic is correctly flowing through the appliances before moving on to other exercises in the lab.

Exercise 2.1: Initialize and Deploy the Cisco IPS Sensor Appliance

The exercise has four tasks.

You will be required to initialize the Cisco Intrusion Prevention Sensor (IPS) appliance and make it accessible from its management interface, and then deploy the sensor in three different interface modes: Inline VLAN pair, Inline Interface pair, and Promiscuous.

The Lab Topology diagram ([Diagram 2](#) in [Part I](#)) depicts three IPS devices; however, only one physical IPS sensor exists in the network. This requires you to pay special attention to the switches in the topology to ensure switch ports are correctly configured (switchport modes, VLANs, and so on) to support each of the three logical/virtual sensors (refer to [Diagram 1](#) in [Part I](#)).

Use names and details exactly as they appear in the tables.

Task 1: Initialize the Cisco IPS Sensor

Use the parameters in [Table 1-11](#) to complete the task of initializing the sensor.

Parameter	Settings
Hostname	IPS
Management	Configure the command and control Management0/0 interface in VLAN 101
Sensor IP address	192.168.2.100/24
Default gateway	192.168.2.20
Sensor ACL	192.168.2.0
Telnet	Enable Telnet management

Table 1-11 Initialization Parameters

Verify the Cisco IPS sensor configuration using the following:

- The username and password for the Cisco IPS console are ciscoips and 123cisco123. Do *not* change them. Use the console to initialize the Cisco IPS sensor appliance using the details in this table.
- Ensure that the Management0/0 interface is up and functioning (refer to the Lab Topology diagram). You can modify the Cisco Catalyst switch configuration if required.
- Ensure that the Cisco IPS sensor can ping the default gateway:

```
IPS# ping 192.168.2.5
```

- Ensure that the following ping and Telnet connection is successful from SW1:

```
SW1# telnet 192.168.2.100
```

Task 2: Deploy the Cisco IPS Sensor in Inline VLAN Pair Mode

Configure the Cisco IPS sensor appliance for the Inline VLAN pair as shown in [Table 1-12](#).

Parameter	Settings	Virtual Sensor Name
Physical interface	GigabitEthernet0/2	vs0
Inline VLAN pair	Vlan1 70 (VLAN70) Vlan2 50 (VLAN50)	

Table 1-12 Inline VLAN Pair Parameters

Task 3: Deploy the Cisco IPS Sensor in Inline Interface Pair Mode

Configure the Cisco IPS sensor appliance for the Inline Interface pair as shown in [Table 1-13](#).

Parameter	Name	Settings	Switch VLANS	Virtual Sensor Name
Interface Pair	ipair	GigabitEthernet0/0, GigabitEthernet0/1	60 80	vs1

Table 1-13 Inline Interface Pair Parameters

Task 4: Deploy the Cisco IPS Sensor in Promiscuous Mode

Configure the Cisco IPS sensor appliance for promiscuous mode on GigabitEthernet 0/3 and assign it to virtual sensor vs2.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 2.1: Initialize and Deploy the Cisco IPS Sensor Appliance.](#)”

Exercise 2.2: Initialize the Cisco WSA

The Cisco WSA should be pre-initialized via the CLI with an IP address of 192.168.2.50:8080 and connected via SW1 in VLAN101 as shown in [Diagram 2](#) in [Part I](#).

Using a browser, connect to the WSA and complete the initialization of the Cisco WSA using the system setup wizard as shown in [Figure 1-1](#). The information to be used for system setup is outlined in [Table 1-14](#). Aside from the username and password values, other information in the System Information parameters can be anything.

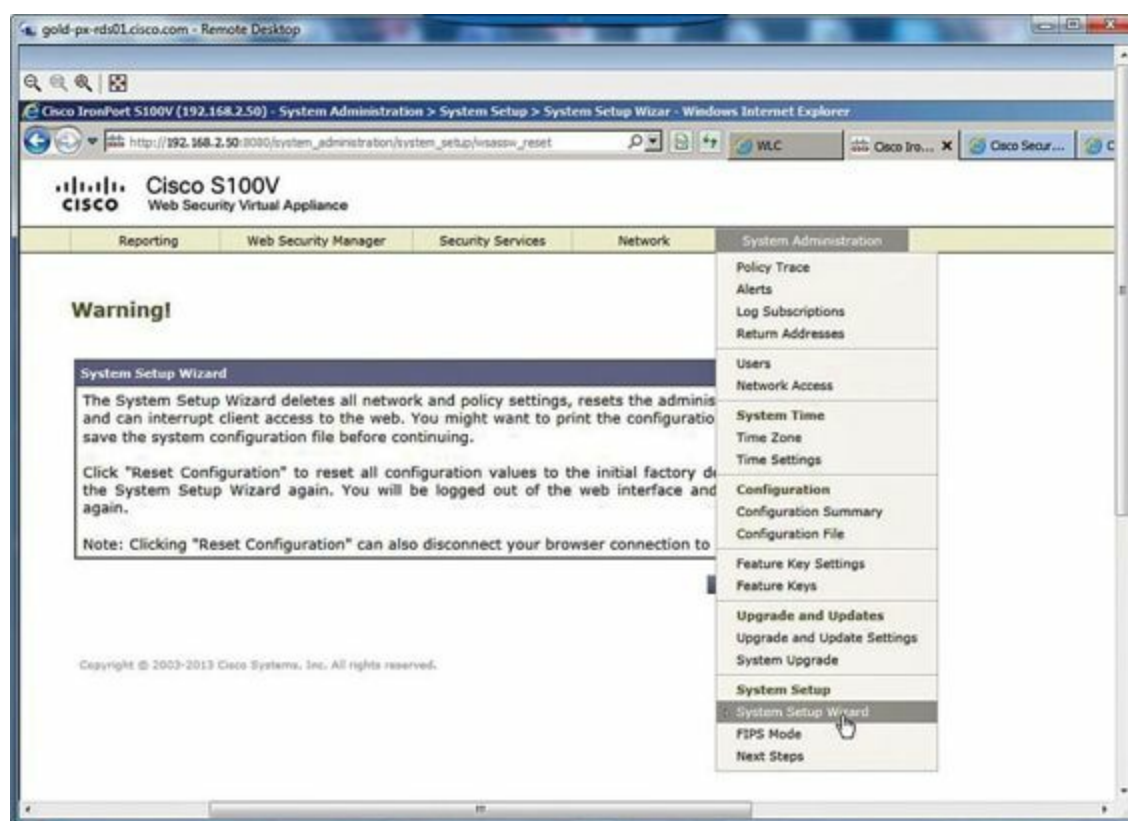


Figure 1-1 WSA System Setup Wizard

Parameter	Settings
Hostname	wsa.cisco.com
Interfaces	Management (M1) to be used for data and management
IP address	192.168.2.50/24
Default gateway	192.168.2.20
System Information	username: admin; password: ironport; email: fred@foobar.com; timezone: America/United States/Los Angeles (this will vary)
NTP server	192.168.2.5
DNS	192.168.2.25
L4 Traffic Monitoring	Duplex TAP:T1 (In/Out)

Table 1-14 *WSA Initialization Parameters*

Connection information: `http://192.168.2.50:8080`; **username:** admin; **password:** ironport

Accept all other defaults.

From ASA1/c1, verify whether you can ping the M1 interface of the Cisco WSA:

```
ASA1/c1# ping 192.168.2.50
```

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 2.2: Initialize the Cisco WSA.](#)”

Exercise 2.3: Enable Web Content Features on the Cisco WSA

This exercise consists of three tasks that build upon the basic configuration of the WSA from [Exercise 2.2](#). Each task enables features and functionality associated with transparent proxy using WCCPv2.

To verify your solutions, you should use the web browser on your client PC to connect to the appropriate HTTP servers as outlined next.

Refer to [Diagram 2](#) in [Part I](#) to help you complete these tasks.

Task 1: Configure WCCPv2 Proxy Support on the WSA (Client) and ASA1 (Server)

Configure WCCP redirect from the inside interface of ASA1/c1 to the WSA using the following parameters:

- **redirect-list** for all HTTP and HTTPS traffic destined to 10.50.0.0/16
- **group-list** to limit redirections to the WSA only
- **service-group** must be in the appropriate range; do not use the basic web-cache service group

Note

- You can use any names for your redirect-list and group-list. Be sure to use a service-group; do not use the default web-cache.
- You might have to reboot the WSA after configuring WCCP if the ASA reports the following:

[Click here to view code image](#)

```
WCCP-EVNT:D90: Here_I_Am packet from 192.168.2.50 ignored; bad web-cache id.
```

To verify your solution, connect to R7 via `http://10.50.40.7`, and then check the HTTP requests on R7 for the address of the WSA as the remote-ipaddress:

[Click here to view code image](#)

```
R7# show ip http server history
```

```
HTTP server history:
```

```
local-ipaddress:port remote-ipaddress:port in-bytes out-bytes
10.50.40.7:80          192.168.2.50:20207 314 192
```

Task 2: Configure Proxy Bypass on the WSA

Continuing from the previous task, HTTP and HTTPS traffic destined to 10.50.80.0/24 must not use the address of the WSA as a source. Create an exception for this traffic.

To verify your solution, connect to R6 via `http://10.50.80.6`, and then check the HTTP requests on R6 for the address of your client PC as the remote-ipaddress:

[Click here to view code image](#)

```
R1# show ip http server history
```

```
HTTP server history:
```

```
local-ipaddress:port remote-ipaddress:port in-bytes out-bytes
10.50.80.6:80          192.168.2.30:58785 369 1986
```

Task 3: Create a Custom URL Access Policy on the WSA

The HTTP server on R3 at 10.50.30.3 has been deemed a restricted site, and access to this server should be prevented by creating a custom URL category on the WSA that intercepts and drops any connection attempt to the R3 HTTP server.

To verify your solution, connect to R3 via `http://10.50.30.3`, and you should receive a blocked website page containing the BLOCK-DEST notification code.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 2.3: Enable Web Content Features on the Cisco WSA.](#)”

Section 3: Secure Access

This section covers fundamental ways to secure network access via wired and wireless methods. Legacy remote access virtual private networks (VPN) via EZVPN using IKEv1 can be built between various client and server platforms—in this case, the Cisco ASA will be the server and the Cisco IOS router takes on the role of client. Dynamic Multipoint Virtual Private Network (DMVPN) has evolved over phase 1, 2, and now to phase 3, which is covered here. The Cisco IOS-based Certificate Authority (CA) server exercise must be completed and will be used in other exercises in this guide. Wireless security is an increasingly important topic, and we start with some basic security access methods that will be expanded upon in other lab exercises.

Exercise 3.1: Configure and Troubleshoot IPsec EZVPN

Complete the EZVPN client/server configuration between the server ASA2 (via the dmz interface) and client R3 (via Ethernet0/1). Use the following information to complete this question, and refer to [Diagram 6](#) in [Part I](#):

- The EZVPN server configuration is partially completed on ASA2.
- Ensure that the VPN tunnel is initiated only from R3 by interesting traffic from access list ezvpn-acl, which is predefined.
- Tunnel only traffic specified by the split tunnel list, which is predefined on the EZVPN server.
- XAUTH must be fully automated with no user intervention required, both from the initial connection and across rekeys. XAUTH credentials are
 - **Username:** cisco
 - **Password:** cisco
- Do not change the names of any predefined IKE, IPsec, or crypto policies on ASA2.
- The group preshared key is cisco.
- Do not alter any of the static routes for networks 10.3.3.0/24 or 10.4.4.0/24 on the routers or ASA2 (added in [Exercise 1.2](#)).

The outputs that follow can be used to complete and verify your solution:

[Click here to view code image](#)

```
R3# show crypto session
```

```
Crypto session current status
```

```
Interface: Ethernet0/1
```

```
Session status: UP-ACTIVE
```

```
Peer: 10.50.30.20 port 500 fvrfr: (none) ivrfr: (none)
```

```
Phase1_id: 10.50.30.20
```

```
Desc: (none)
```

```
IKEv1 SA: local 10.50.30.3/500 remote 10.50.30.20/500 Active
```

```
Capabilities: CX connid:1053 lifetime:23:54:51
```

```
IPSEC FLOW: permit ip 10.3.3.0/255.255.255.0 10.4.4.0/255.255.255.0
```

```
Active SAs: 2, origin: crypto map
```

```
IPSEC FLOW: permit ip host 172.16.1.100 10.4.4.0/255.255.255.0
```

Active SAs: 2, origin: crypto map

```
R3# show crypto ipsec client ezvpn  
Easy VPN Remote Phase: 8
```

Tunnel name: ez

Inside interface list: Loopback1

Outside interface: Ethernet0/1

Connect: ACL based with access-list ezvpn-acl

Current State: IPSEC_ACTIVE

Last Event: SOCKET_UP

Address: 172.16.1.100 (applied on Loopback10000)

Mask: 255.255.255.255

DNS Primary: 192.168.2.25

Default Domain: cisco.com

Save Password: Allowed

Current EzVPN Peer: 10.50.30.20

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 3.1: Configure and Troubleshoot IPsec EZVPN.](#)”

Exercise 3.2: Troubleshoot DMVPN Phase 3: DMVPNv3

In this exercise, R5 is the DMVPN hub with R3 and R4 as the spokes. Complete the configuration and troubleshoot this DMVPNv3 solution using the following information, and refer to [Diagram 5](#) in [Part I](#):

- R5 (172.17.70.5) is the tunnel interface IP address of the hub.
- R3 (172.17.70.3) and R4 (172.17.70.4) are the tunnel interface IP addresses of the spokes.
- Each spoke must register with the hub, and *direct* spoke-to-spoke communication should use *NHRP shortcut* capabilities.
- EIGRP routing in AS 123 is preconfigured and must be advertising the loopback0 networks of R3, R4, and R5 via the Tunnel1 interface.
- The IKE and IPsec protection suites to use are predefined on R5.

Use the following outputs to verify your solution:

[Click here to view code image](#)

```
R5# show crypto session  
Crypto session current status
```

Interface: Tunnel1

Session status: UP-ACTIVE

Peer: 10.50.30.3 port 4500

IKEv1 SA: local 10.50.90.5/4500 remote 10.50.30.3/4500 Active

IPSEC FLOW: permit 47 host 10.50.90.5 host 10.50.30.3

Active SAs: 2, origin: crypto map

Interface: Tunnel1

Session status: UP-ACTIVE

Peer: 10.50.30.4 port 4500

IKEv1 SA: local 10.50.90.5/4500 remote 10.50.30.4/4500 Active

IPSEC FLOW: permit 47 host 10.50.90.5 host 10.50.30.4

Active SAs: 2, origin: crypto map

R5# show ip route

D 172.16.33.0/24 [90/25984000] via 172.17.70.3, 2d07h, Tunnel1

D 172.16.34.0/24 [90/25984000] via 172.17.70.4, 2d07h, Tunnel1

C 172.16.35.0/24 is directly connected, Loopback0

L 172.16.35.5/32 is directly connected, Loopback0

172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks

C 172.17.70.0/24 is directly connected, Tunnel1

L 172.17.70.5/32 is directly connected, Tunnel1

Note

There is a dependency on the [Exercise 1.3](#) Network Object NAT task. You might need to modify the configuration of other elements of the topology, but you should not alter any of the base dynamic routing configurations on the routers and switches.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 3.2: Troubleshoot DMVPN Phase 3: DMVPNv3.](#)”

Exercise 3.3: Configure Security Features on the Cisco WLC

This exercise has three tasks that each focus on wireless access services offered by the Cisco Wireless LAN Controller (WLC) and methods for securing them. Refer to [Diagram 2](#) in [Part I](#) to see the placement of the Cisco WLC and Cisco Access Points (AP) in the network topology.

Task 1: Initialize the WLC and Establish Control over the Cisco Access Points (AP)

Cisco APs can operate in standalone mode or, as in this task, they can be controlled and managed by the Cisco WLC. To perform this task, bootstrap your Cisco WLC with the following initial settings, and ensure the APs associate with the WLC:

[Click here to view code image](#)

```
config interface address management 10.50.100.10 255.255.255.0 10.50.100.20
config interface vlan management 100
config ap mgmtuser add username cisco password CCie123 enablesecret CCie123 all
config sysname WLC
config prompt WLC
config network webmode enable
```

Using these settings, the WLC manages the configuration and control of Cisco APs (there is no need to change any settings on the AP itself). Pay close attention to the locations of the APs in [Diagram 2](#) in

[Part I](#), and ensure that any devices attached to, or in the path of, the WLC and APs are configured correctly.

Verify your associations using the following command (AP information will be unique to your devices):

[Click here to view code image](#)

```
(WLC) >show ap summary
```

```
Number of APs..... 2
```

```
Global AP User Name..... cisco
```

```
Global AP Dot1x User Name..... Not Configured
```

```
AP Name      Slots AP Model      Ethernet MAC      Location      Port
-----
AP1cdf.0f94.8063 2  AIR-CAP3502I-A-K9 1c:df:0f:94:80:63 default location 1
AP588d.0959.4921 2  AIR-LAP1262N-A-K9 58:8d:09:59:49:21 default location 1
```

Note

- To complete the remainder of this question, you can use the CLI on the WLC or the web GUI via <http://10.50.100.10> (username cisco, password C1sc0123) as illustrated in [Figure 1-2](#).

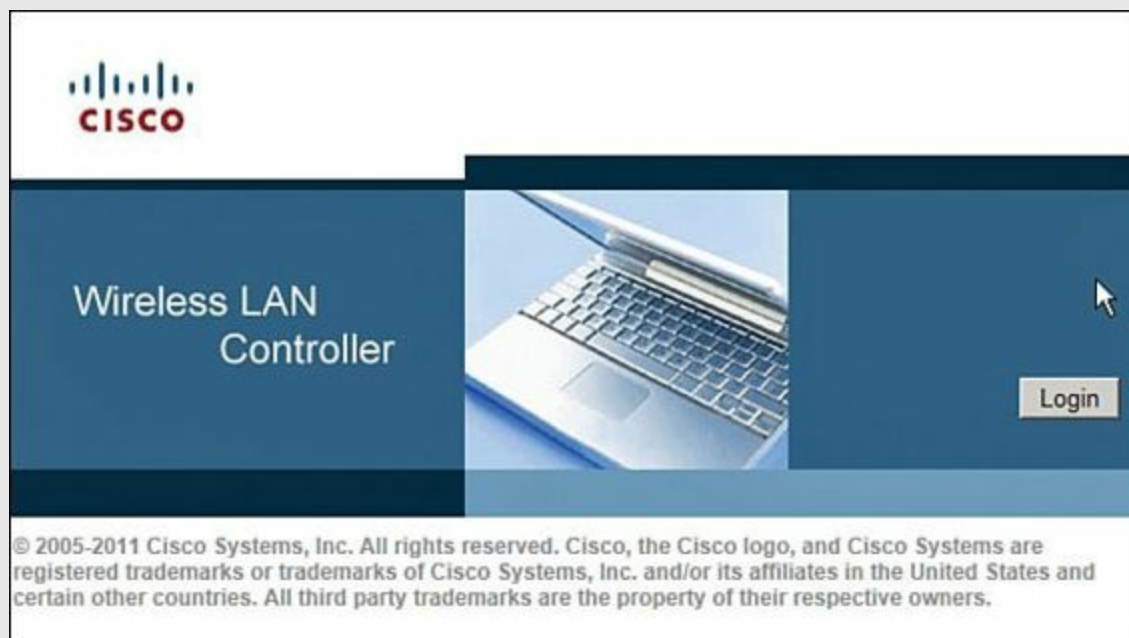


Figure 1-2 *WLC GUI Configuration Application*

- In this exercise, the Cisco AP located on the 10.50.77.0/24 network will be used in later exercises as a rogue AP.
- The Cisco APs receive their IP addresses and the IP address of the WLC via DHCP on R2 and SW2. The option 43 command in the DHCP pool definition is used to identify the WLC. The following example used option 43 with the IP address of the WLC:

[Click here to view code image](#)

```
ip dhcp pool pool100
network 10.50.100.0 255.255.255.0
default-router 10.50.100.2
option 43 ip 10.50.100.10
lease infinite
```

It is recommended that the hex format be used to identify WLCs available for Cisco APs. Further information on configuring option 43 is available at

http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008

Task 2: Enable IP Services on the WLC to Enhance Security

- Configure NTP on the WLC using 192.168.2.5 as the NTP server. Ensure that the service is enabled.
- Configure RADIUS authentication to the Identity Services Engine (ISE) authentication server at 192.168.2.15. Ensure that this connection to the RADIUS server is established.

Note

You may modify the configuration of other devices in the network to ensure you have connectivity between the WLC and the servers.

Task 3: Creating and Assigning Security Policy to WLANs and Users

Complete a wireless configuration using dynamic interfaces and WLANs requiring different levels of security for two groups of users: employee and guest, using the information in [Table 1-15](#).

Parameter	Employee Values	Guest Values
WLAN Name	employee	guest
WLAN ID	3	2
SSID	employee	guest
Security Method	WP2(aes)/Auth(802.1X)	Web Authentication
Dynamic-Interface Name	employee-wlan	guest-wlan
Dynamic-Interface Address	10.10.110.2/24	10.10.120.2/24
Dynamic-Interface GW	10.10.110.1	10.10.120.1
VLAN	110	120
Web-Auth Method		local
Netuser Account		guest/cisco
Lifetime		No Lifetime
UserType		guest

Table 1-15 *Wireless Access Configuration Parameters*

Note

- The IP addresses for wireless client will be issued from the Dynamic-Interface Gateway (GW), which for this question is R2. R2 has DHCP for the relevant scopes defined.

[Click here to view code image](#)

```
ip dhcp pool pool110
network 10.10.110.0 255.255.255.0
default-router 10.10.110.1
!
ip dhcp pool pool120
network 10.10.120.0 255.255.255.0
default-router 10.10.120.1
```

- Without wireless clients connecting to the APs, full service cannot be verified; however, the **show wlan** commands can be used to verify your configuration from the CLI. You may also ping the dynamic interface IP addresses from the Cisco AP located on the 10.50.100.0/24 network.
- You will not be able to access R2 from the AP on the 10.50.77.0/24 network.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 3.3: Configure Security Features on the Cisco WLC.](#)”

Exercise 3.4: Configure the Cisco IOS Certificate Server

A Cisco IOS certificate server is to be configured on R1 as shown in [Diagram 2](#) in [Part I](#). Ensure that R1 has access to the NTP server at 10.50.70.5 before the CA server is created. Also, make sure end entities will have HTTP access to this CA server from anywhere in the topology.

The following information should be used to configure R1 as a CA server:

- 3DES is used to encrypt the private key, and cisco123 is the pass-phrase to protect the private key
- CA root certificate with lifetime of 1 year
- Identity certificate with lifetime of 200 days
- CRL lifetime 24 hours
- Overwrite any existing keys if prompted

The following outputs should also be used to complete this task:

[Click here to view code image](#)

```
R1# sho cry key mypubkey rsa
```

Key name: ciscoca

Key type: RSA KEYS

Storage Device: private-config

Usage: General Purpose Key

Key is exportable.

```
R1# sho cry pki server
```

Certificate Server ciscoca:

Status: enabled

State: enabled

Server's configuration is locked (enter "shut" to unlock it)

Issuer name: CN=ciscoca.cisco.com L=cisco C=US

CA cert fingerprint: 1F5A02E4 C2C8230A 56FC15BB CBDFBEF6

Granting mode is: auto

Last certificate issued serial number (hex): 1

CA certificate expiration timer: 13:19:37 PST Aug 17 2014

CRL NextUpdate timer: 13:19:37 PST Aug 18 2013

Current primary storage dir: nvram:

Database Level: Minimum - no cert data written to storage

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 3.4: Configure the Cisco IOS Certificate Server.](#)”

Section 4: System Hardening and Availability

System or device hardening involves implementing techniques that protect against compromise resulting in either specific device/system failure or disruption to other network services. The goal of enabling protection and monitoring features on a system is performance predictability and network availability. This section requires implementing and troubleshooting specific hardening features, such as control and management plane policing. Features that focus on network availability, such as routing protocol security, monitoring traffic, transiting a switch, and securing wireless infrastructure, are also covered.

Exercise 4.1: Configure SPAN on the Cisco Catalyst Switch

Traffic on VLAN 77 and VLAN 9 must be mirrored to the Cisco IPS sensor using Switched Port Analyzer (SPAN) on SW2, as shown in [Diagram 1](#) and [Diagram 2](#) in [Part I](#).

The Cisco IPS sensor appliance must already be configured in promiscuous mode using interface G0/3 (see [Exercise 2.1](#)). When this interface is verified as enabled, use the information in [Table 1-16](#) to complete the configuration.

Parameter	Settings
IPS interface	Gig0/3
SW2 Dest Port	Gig1/0/17
SW2 Traffic to Monitor (Transmit and Receive)	VLANs 77 and 9

Table 1-16 *SPAN Configuration Parameters*

You may use any monitor session number.

To verify whether traffic is being mirrored to the IPS sensor, use the following command:

[Click here to view code image](#)

```
IPS# packet display gigabitEthernet0/3
```

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 4.1: Configure SPAN on the Cisco Catalyst Switch](#).”

Exercise 4.2: Troubleshoot Secure Routing Using OSPFv3 in Cisco IOS

OSPFv3 has been partially preconfigured between R1 and R2 using the command

```
ipv6 router ospf 21
```

Complete the configuration, and troubleshoot as necessary to meet the following requirements:

- Configure Encapsulating Security Payload (ESP) 3DES encryption with Secure Hash Algorithm (SHA) authentication for area 0 to protect routing information. You can define your own keys.
- Ensure that the IPv6 addresses from interface Loopback1 on R1 and R2 are being advertised through OSPFv3 on R1 and R2. The Loopback interfaces are not OSPFv3 interfaces in themselves.

■ Refer to [Diagram 2](#) and [Diagram 4](#) in [Part I](#) for additional topology information.

The following outputs can be used to verify your solution:

[Click here to view code image](#)

```
R1# show ipv6 route
OE2 3001:0:2:3::/64 [110/20]
  via FE80::21E:4AFF:FE2F:CA70, Ethernet0/0
```

```
R2# show ipv6 route
OE2 3001:0:1:3::/64 [110/20]
  via FE80::21E:4AFF:FE36:5210, Ethernet0/0.1
```

```
R1# show crypto session
Interface: Ethernet0/0
Session status: UP-NO-IKE
Peer: FF02::5 port 500
IPSEC FLOW: permit 89 FE80::/10 ::/0
  Active SAs: 2, origin: manual-keyed crypto map
```

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 4.2: Troubleshoot Secure Routing Using OSPFv3 in Cisco IOS.](#)”

Exercise 4.3: Configure Control Plane Policing (CoPP)

In this exercise, you are given a list of traffic bandwidth requirements and the actions to be taken to guarantee a predictable level of service by the route processor by protecting it against excessive CPU utilization, which could result from a successful DoS attack.

Implement CoPP using the information in [Table 1-17](#) on the control plane of R7. You may use any names for configuration constructs as long as you correctly identify the traffic types, rates, and actions as specified in the table. Try to be as specific as possible when defining your traffic classes; for example, use host IP addresses for BGP traffic, not **any any**.

Traffic Class	Rate (PPS)	Conform Action	Exceed Action
BGP	Unlimited	Transmit	Transmit
OSPF	Unlimited	Transmit	Transmit
IKE: IPv4, IPv6	250	Transmit	Transmit
Layer-2	20	Transmit	Transmit
Management (HTTP, HTTPS, NTP, DNS, Telnet)	125	Transmit	Transmit
Undesirable (ICMP, TCP fragments)	10	Drop	Drop
Default	25	Transmit	Drop

Table 1-17 Control Plane Policing Policy Requirements

Refer to [Diagram 2](#) and [Diagram 3](#) in [Part I](#) for address information and device locations.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 4.3: Configure Control Plane Policing \(CoPP\).](#)”

Exercise 4.4: Troubleshoot Management Plane Protection

The following debug output is being displayed on R7:

[Click here to view code image](#)

```
MI:DROPPED TCP dport 23 fport 18433 faddr 10.50.40.7
```

Troubleshoot R7 to prevent this output.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 4.4: Troubleshoot Management Plane Protection](#).”

Exercise 4.5: Device Hardening on the Cisco WLC

The exercise has five tasks that enable features designed to protect the WLC against various wireless attacks, and to also provide additional security to the interactions between the WLC and Cisco access points.

Task 1: Disable SSID Broadcasting

To prevent active probing of the wireless network for SSIDs, disable SSID broadcasting for the employee WLAN configured in Q3.3.

Task 2: Protect the WLC Against Associating with a Rogue AP

To prevent a man-in-the-middle (MITM) attack resulting from the insertion of a rogue AP in the network, create a rogue rule using the following information:

[Click here to view code image](#)

```
Rule Name..... RogueAP
State..... Enabled
Type..... Malicious
Match Operation..... Any
Hit Count..... 0
Total Conditions..... 2
Condition 1
  type..... Client-count
  value..... 1
Condition 2
  type..... No-encryption
  value..... Enabled
```

In addition, classify the AP on the 10.50.100.0/24 subnet as friendly.

Task 3: Enable Infrastructure Management Frame Protection on the WLC

To protect against attacks such as association flood DoS attacks, enable infrastructure management frame protection (MFP) for all APs.

Task 4: Enable Encryption for CAPWAP Packets

The friendly AP in your network supports Datagram Transport Layer Security (DTLS) encryption. Enable this service on the WLC to provide protection for CAPWAP control and data packets.

Task 5: Create a Rate Limiting Policy for Guest Users on the Guest WLAN

Guest users accessing the wireless network via the guest WLAN defined in [Exercise 3.3](#) will have their access rate limited as follows:

[Click here to view code image](#)

```
Role Name..... Guest
Average Data Rate..... 10
Burst Data Rate..... 10
Average Realtime Rate..... 100
Burst Realtime Rate..... 100
```

Configure this policy on the WLC and apply it to the guest user created in [Exercise 3.3](#).

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 4.5: Device Hardening on the Cisco WLC.](#)”

Section 5: Threat Identification and Mitigation

This section requires the implementation of threat identification and mitigation techniques on different Cisco platforms. On a Cisco IOS router, NetFlow is used to identify possible attack patterns, and this information is then used to build a flexible packet matching (FPM) policy. DHCP activities may be manipulated to launch attacks that are mitigated by methods configured on Cisco Catalyst switches. This section also covers application-specific attack mitigation features on the Cisco ASA.

Exercise 5.1: Troubleshoot IPv6 in IPv4 Tunnel

Troubleshoot the ipv6ip (IPv6 in IPv4) tunnel configured between R6 and R5. This exercise has dependencies on your results from [Exercise 1.3](#). Your solution can be verified from the following outputs, and you should refer to [Diagram 2](#) and [Diagram 4](#) in [Part I](#) to help you complete this exercise:

[Click here to view code image](#)

```
R5# show ipv6 route
EX 2010::/64 [170/27008000]
   via FE80::A32:5006, Tunnel0
```

```
R6# show ipv6 route
EX 1010::/64 [170/27008000]
   via FE80::A32:5A05, Tunnel0
```

After you have verified your solution, create a classification ACL on R5 that will log any Teredo tunnel activity as well as any ipv6ip traffic transiting the tunnel. Take care when enabling the log option on access list entries.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 5.1: Troubleshoot IPv6 in IPv4 Tunnel.](#)”

Exercise 5.2: Mitigating DHCP Attacks on a Cisco Catalyst Switch

Refer to [Diagram 2](#) in [Part I](#) for this exercise. Cisco AP1 receives an IP address from R2, which is considered a trusted DHCP server. Configure SW1 to ensure that a rogue DHCP server will not respond to DHCP requests from AP1. In addition, configure a solution that will bind the IP address issued to AP1 with the Media Access Control (MAC) of AP1 to provide protection against IP address spoofing. All traffic, apart from DHCP packets, should be dropped on GigabitEthernet1/0/19 until AP1 receives its address via DHCP and begins to transmit traffic.

Verify your solution by performing a shut/no shut on SW1 GigabitEthernet1/0/19 and checking for an address binding on SW1 for AP1:

[Click here to view code image](#)

```
SW1# show ip dhcp snooping binding
MacAddress      IpAddress      Lease(sec) Type          VLAN Interface
-----
1C:DF:0F:94:80:63 10.50.100.53  infinite  dhcp-snooping 100 Gig1/0/19
```

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 5.2: Mitigating DHCP Attacks on a Cisco Catalyst Switch.](#)”

Exercise 5.3: Identifying Attacks with NetFlow and Mitigating Attacks Using Flexible Packet Matching

NetFlow has been enabled on R7 (see [Diagram 2](#) in [Part I](#)), and the highlighted statistics indicate there could be an issue with a large ICMP packet attack:

[Click here to view code image](#)

```
R7# show ip cache flow
```

```
IP packet size distribution (52 total packets):
```

```
1-32 64 96 128 160 192 224 256 288 320 352 384 416 448 480
.000 .269 .211 .000 .000 .000 .000 .019 .000 .000 .000 .000 .000 .000 .000
```

```
512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
.000 .000 .000 .019 .480 .015 .030 .000 .000 .000 .000
```

Protocol	Total	Flows	Packets	Bytes	Packets	Active(Sec)	Idle(Sec)
-----	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/Flow
ICMP	17	0.0	8 1213	0.0	6.5	15.4	
Total:	17	0.0	8 1213	0.0	6.5	15.4	

Sending “oversized” ICMP packets could potentially crash or reboot the target host or place a performance-impacting load on the device CPU due to fragment reassembly.

Configure FPM on R7 to identify and drop ICMP packets greater than 1000 bytes in size. You may use any names for your policy constructs.

Note

The choice of packet size will vary depending on security policy. It is only 1000 bytes here because it is easy to verify.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 5.3: Identifying Attacks with NetFlow and Mitigating Attacks Using Flexible Packet Matching](#).”

Exercise 5.4: Application Protocol Protection

Monitor and protect the DNS server (192.168.2.25) behind ASA1 from attacks that are trying to exploit protocol resources and vulnerabilities. Use the following information to complete this exercise:

- Configure ASA1 context c1 to perform DNS inspection and drop any DNS requests not coming from resolvers in the cisco.com domain. In addition, log any DNS packets with the Authoritative Answer (AA) and Query/Response (QR) header bits set.
- Do not use any class-map constructs to complete this task.
- Your solution must be applied within the default global_policy and the inspection_default class.
- You may use any names for policy constructs.
- Refer to [Diagram 2](#) in [Part I](#) for topology information.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 5.4: Application Protocol Protection](#).”

Section 6: Identity Management

In this section, you configure the Cisco ISE and Cisco Secure Access Control Server (ACS) to support identity-based network access and device management using RADIUS and TACACS+. Device command authorization on a Cisco IOS router is an important method for restricting device access and limiting the potential for attack or inadvertent misconfiguration. Identity-based network access is implemented using cut-through proxy on the Cisco ASA triggered by HTTP traffic. Cisco TrustSec is applied on the Cisco Catalyst switch along with the Cisco ISE through the use of MAC Authentication Bypass (MAB) and 802.1X authentication methods enforced on a switch port.

Exercise 6.1: Configure Router Command Authorization and Access Control

This exercise has two components:

- Router R2 must be configured for command authorization and access control via TACACS+.
- Cisco Secure ACS must also be configured for user authentication and command authorization policies.

Caution

This section contains command authorization. To prevent being locked out of the router, do *not* enable command authorization until *after* you have verified that authentication is working properly to CiscoSecure ACS.

Refer to [Diagram 2](#) in [Part I](#) to verify the addressing and location of R2 and the ACS server.

Requirements for R2:

- Configure R2 for AAA server (IP address: 192.168.2.18) using the TACACS+ protocol with the CiscoSecure ACS server and a shared secret key of cisco123.
- The console port connection must not require authentication or authorization (with the exception of the enable password to get into enable mode).
- Telnet connections 1 and 3 through 5 should prompt only for a password (exec and enable) and no username. Additionally, no command authorization must be configured on these connections.
- Telnet connection 2 must be configured for authentication and command authorization for specific command levels.
- You may *not* use any “default” methods. Configure only named method lists.

Requirements for Cisco Secure ACS:

- Configure two groups with the following properties:
 - **admin:** Users in this group have full access to the router.
 - **netops:** Users in this group have access to showcrypto commands and clear crypto session.
- Configure two users, one in each group with which you can test.
 - **admin:** (with a password of cisco) should be placed in the admin group.
 - **netops:** (with a password of cisco) should be placed in the netops group.
- The command authorization configuration must be done using device administration command sets.

You may follow this checklist to troubleshoot and verify your solution:

- From R4, establish a Telnet connection to R2 and verify that you are prompted for the password and the enable password, and that command authorization is not configured. You should not be prompted for a username.
- Establish a second Telnet session to R2 and verify that this session is prompted for username and password, and that command authorization is enabled.
- Verify that admin has access to all configuration commands.
- Verify that netops has only the capability to use show crypto commands and clear crypto session.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 6.1: Configure Router Command Authorization and Access Control.](#)”

Exercise 6.2: Configure Cut-Through Proxy on ASA2 Using TACACS+

Cut-through proxy authentication is required on ASA2 and will be triggered for users initiating HTTP connections to the web servers on R4 and R7 (Refer to [Diagram 2](#) in [Part I](#)).

- Configure ASA2 to use the ACS server 192.168.2.18 for authentication and authorization, using TACACS+ as the protocol.
- Configure the ACS server using the following information:
 - TACACS+ should be used as the Authentication and Authorization protocol, with the key cisco123.
 - Configure a username userap1 and a username userap2, both with password Cisco on the ACS server
- Configure ASA2 to authenticate and authorize any hosts trying to access destination 10.50.0.0/16 (HTTP) against the ACS server.
- userap1 should be authorized to connect to the HTTP server on 10.50.40.7 (R7) only.
- userap2 should be authorized to connect to the HTTP servers on 10.50.30.4 (R4) only.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 6.2: Configure Cut-Through Proxy on ASA2 Using TACACS+.](#)”

Exercise 6.3: Configure Support for MAB/802.1X for Voice and Data VLANs

This exercise contains two parts:

- [Exercise 6.3a: Authentication and Authorization Using MAB](#)
- [Exercise 6.3b: Authentication and Authorization Using 802.1X](#)

To review the network topology, refer to [Diagram 1](#) and [Diagram 2](#) in [Part I](#).

Exercise 6.3a: Authentication and Authorization Using MAB

The Cisco IP Phone is connected to interface gig1/0/14 on SW2. It receives an IP address via DHCP for the 10.50.9.0/24 subnet and registers with Cisco Call Manager Express running on R6 (via 10.50.170.6). The requirement is to add security to this connection through authentication and authorization on SW2 using MAC Authentication Bypass (MAB) to assign the RADIUS attributes required to move the phone into the voice VLAN.

Use the following information to complete this task:

- Create an endpoint identity for the IP Phone in your rack on ISE1 (192.168.2.15).
- Verify whether you have an authentication rule for MAB on the Cisco ISE.
- Verify whether the standard authorization policy for Cisco IP Phones exists and is allowing a permit on all traffic on ISE1.
- Configure gig1/0/1 on SW6 to support a voice VLAN (9) and data VLAN (99).
- The voice VLAN will support MAB for authentication.
- The data VLAN will provide support for the Test-PC that must connect through the Cisco IP

phone using 802.1X.

- SW2 must attempt a MAB authentication first after learning the MAC address of an endpoint. 802.1X should be the first priority authentication method.

The following output should be used to verify your solution:

[Click here to view code image](#)

```
SW2# show authentication session int g1/0/14
```

```
Interface: GigabitEthernet1/0/14
MAC Address: 0023.eb54.1109
IP Address: Unknown
User-Name: 00-23-EB-54-11-09
Status: Authz Success
Domain: VOICE
Security Policy: Should Secure
Security Status: Unsecure
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: 9
ACS ACL: xACSACLx-IP-PERMIT_ALL_TRAFFIC-4fe7f797
Session timeout: 3600s (local), Remaining: 3509s
Timeout action: Reauthenticate
Idle timeout: N/A
Common Session ID: C0A842420000002E003D9546
Acct Session ID: 0x00000030
Handle: 0x3C00002F
```

Runnable methods list:

```
Method State
mab Authc Success
dot1x Not run
```

```
R6# show ephone summary
```

hairpin_block:

```
ephone-1[0] Mac:0023.EB54.1109 TCP socket:[1] activeLine:0 whisperLine:0
```

```
REGISTERED
```

```
mediaActive:0 whisper_mediaActive:0 startMedia:0 offhook:0 ringing:0 reset:0
```

```
reset_sent:0 debug:0
```

```
IP:7.7.9.6 * 7965 keepalive 10609 music 0
```

```
Max 10, Registered 1, Unregistered 0, Deceased 0 High Water Mark 11, Sockets 1
ephone_send_packet process switched 0
```

Exercise 6.3b: Authentication and Authorization Using 802.1X

The Test-PC must be allowed to connect through the authenticated Cisco IP Phone.

- SW2 Gig1/0/14 should have been configured to support a voice and data VLAN in Part A of this question.
- Configure an authorization profile and authorization policy rule for the Test-PC on the ISE using the information in [Table 1-18](#).

Attribute	Value
Group Name	Test-PC-Group
Username/Password	Test-PC/Cisco123
Access Type	ACCESS_ACCEPT
Common Tasks	
DACL Name	DATA_VLAN_DACL
DACL Policy	permit ip any any
VLAN	99

Table 1-18 *Attributes/Values for Configuring the Authorization Profile and Authorization Policy Rule*

The following output should be used for verification:

[Click here to view code image](#)

```
SW2# sho auth sess int g1/0/14
Interface: GigabitEthernet1/0/14
  MAC Address: 000c.290d.0c22
  IP Address: Unknown
  User-Name: Test-PC
  Status: Authz Success
  Domain: DATA
  Security Policy: Should Secure

  Security Status: Unsecure
  Oper host mode: multi-auth
  Oper control dir: both
  Authorized By: Authentication Server
  Vlan Policy: 99
  ACS ACL: xACSACLx-IP-DATA_VLAN_DACL-503d6911
  Session timeout: 3600s (local), Remaining: 3585s
  Timeout action: Reauthenticate
  Idle timeout: N/A
Common Session ID: C0A842420000008B37CC94A2
Acct Session ID: 0x000000B4
  Handle: 0x0F00008C
```

Runnable methods list:

Method State

mab Failed over

dot1x Authc Success

The Test-PC can be used to connect through the IP Phone to SW6. Be sure you add the username/password credentials Test-PC/Cisco123 by navigating through the sequence that follows:

Step 1. Open the IP Phone network connection > Properties, and dynamic addressing is enabled as shown in [Figure 1-3](#).

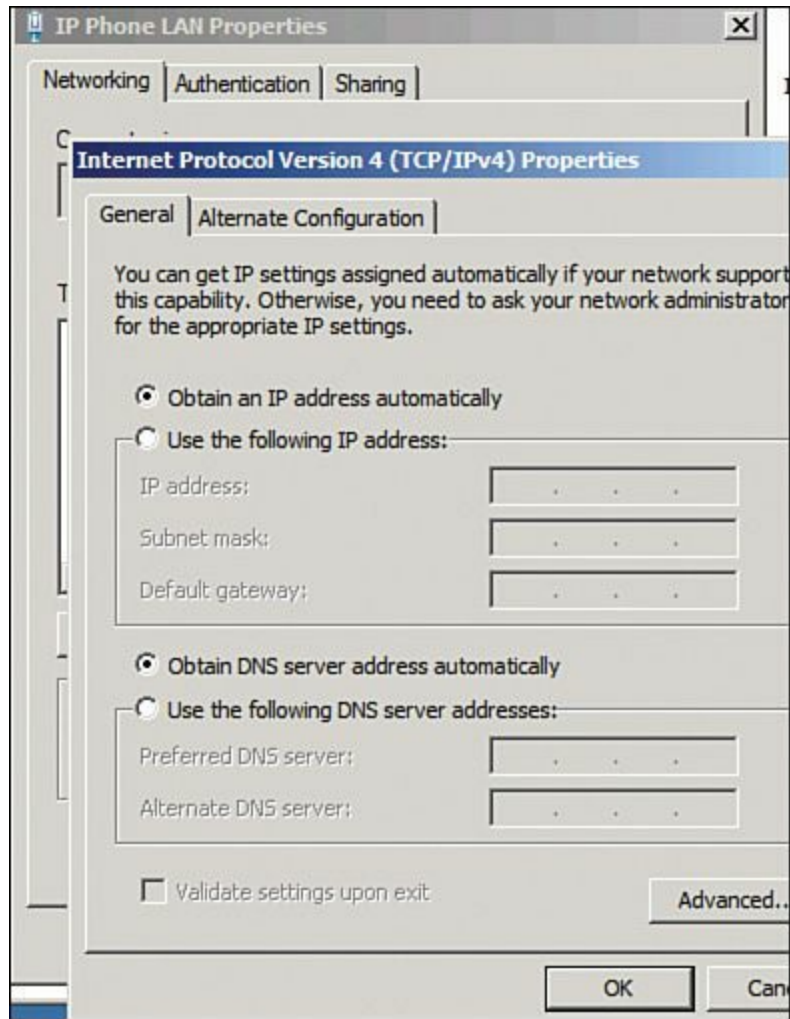


Figure 1-3 *IP Properties*

Step 2. Choose the Authentication tab and configure as shown in [Figure 1-4](#), and then select the Settings button next to Microsoft PEAP.

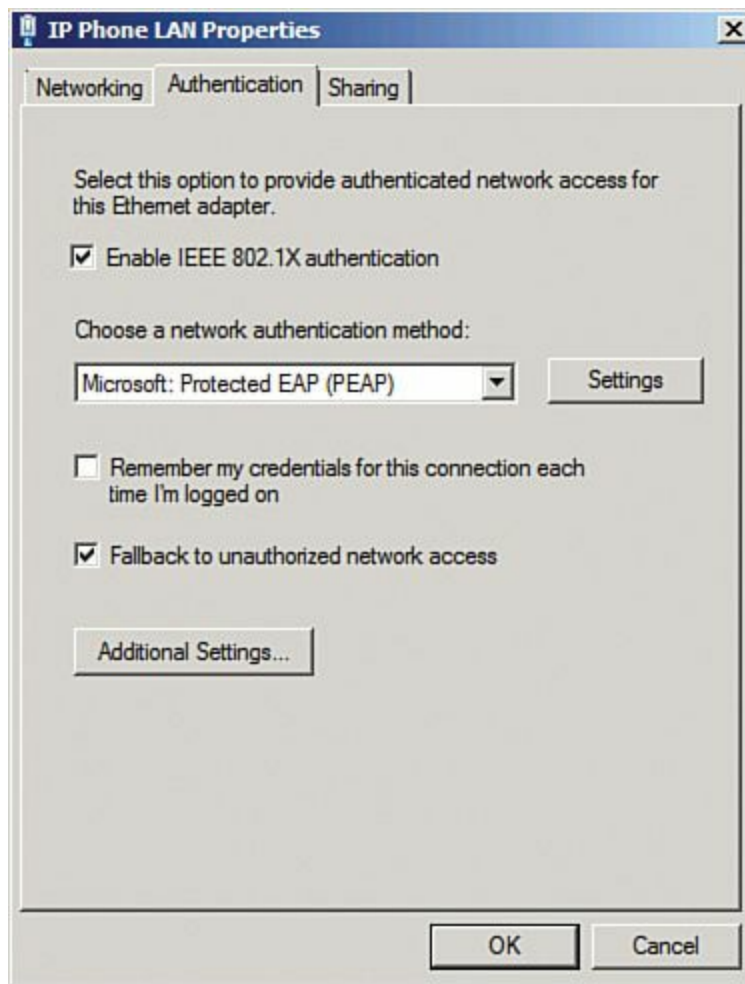


Figure 1-4 *Authentication Methods*

Step 3. Ensure PEAP is configured as shown in [Figure 1-5](#), including unselecting Windows login credentials for Configuring Secure Password.

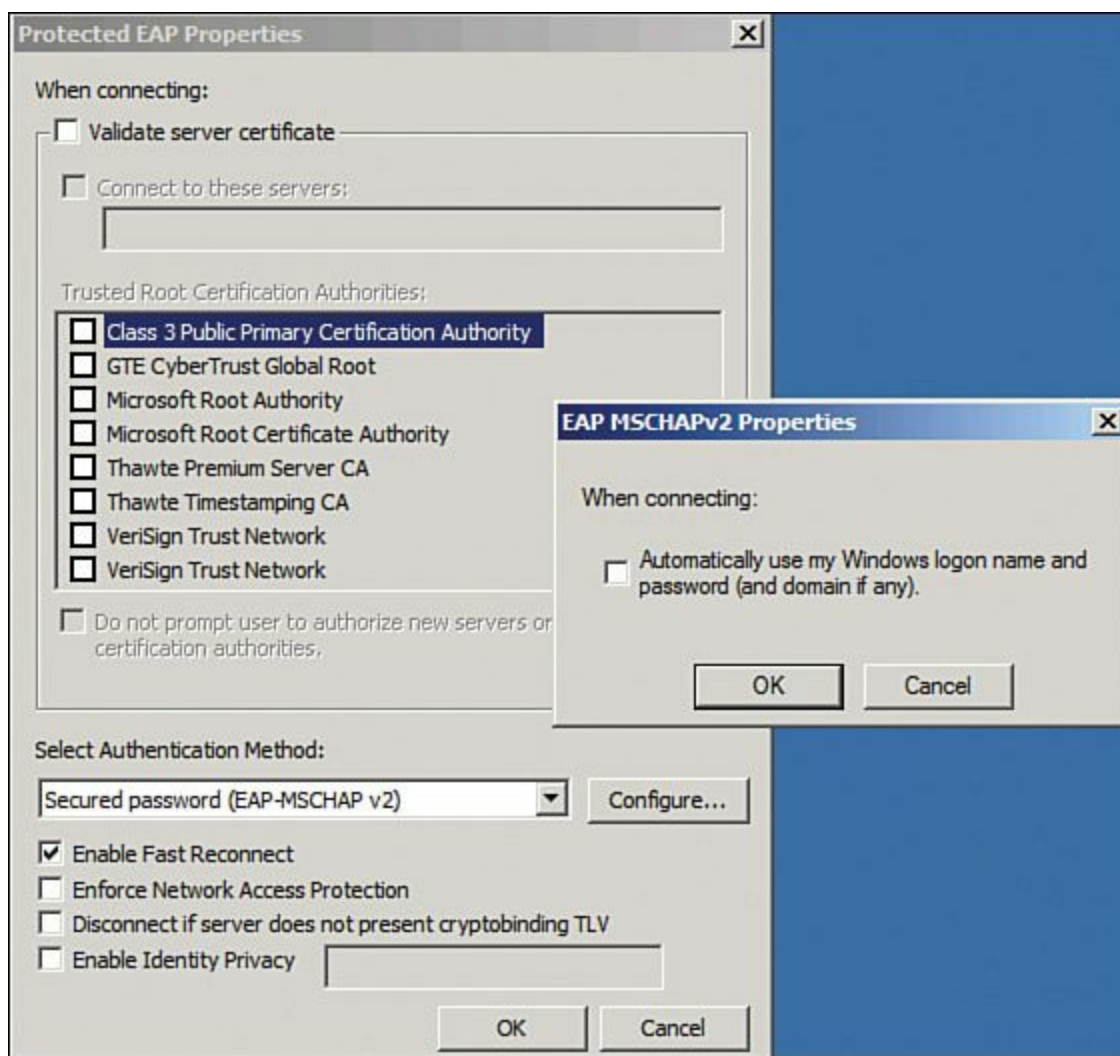


Figure 1-5 *EAP Properties*

Step 4. Return to the step 2 screen and select Additional Settings as shown in [Figure 1-6](#). Enter the Test-PC/Cisco123 credentials here.

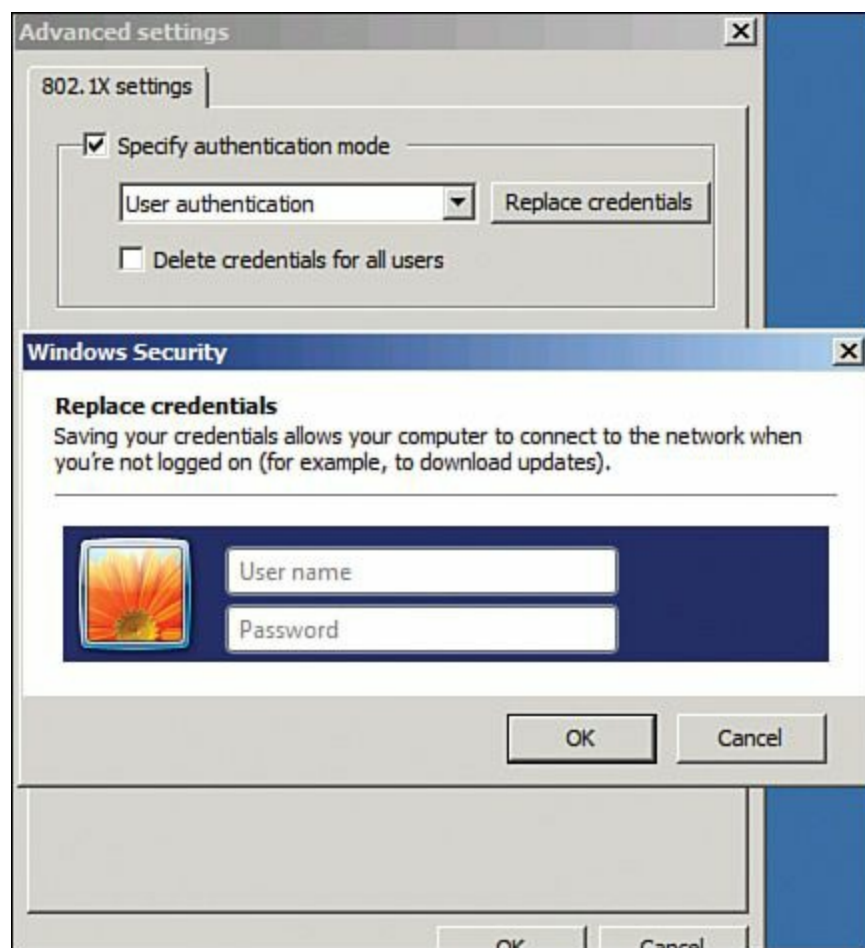


Figure 1-6 *User Credentials*

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 6.3: Configure Support for MAB/802.1X for Voice and Data VLANs.](#)”

Practice Lab 1 Solutions

Section 1: Perimeter Security and Services

Securing the perimeter around important networks and devices is a fundamental part of network protection. In this section, you are asked to implement firewall services that include not only traditional features such as Network Address Translation (NAT) and traffic inspection, but also secured routing features. The exercises in this section focus on initializing and configuring the Cisco Adaptive Security Appliance (ASA) in both single- and multi-context modes. Connectivity through perimeter devices must be verified before moving on to other exercises in this guide.

Solution and Verification for Exercise 1.1: Initialize the Cisco ASA in Multi-Context Routed Mode

Skills Tested

- Initialize and configure the Cisco ASA as a multi-context firewall. It is important to understand the functions and services available when the Cisco ASA is configured in this mode, knowing they will vary depending on the version of the OS software installed.
- The ability to integrate the security appliance into a complex network topology, understanding that the surrounding infrastructure (for example, switches and routers) also must be configured correctly.
- A good understanding of basic IP networking including IP addressing, IP routing, and Cisco Catalyst switch port and VLAN configuration.

Solution and Verification

This exercise is fairly simple, but the correct configuration of the Cisco ASA is fundamental to ensuring that the traffic flows, which will be identified in later exercises, can pass through ASA1 securely and as expected.

It is important to be familiar with ASA **show** commands and their output to be able to validate the solution.

Connectivity and configuration is verified using pings from ASA1 to various major subnets in the topology. Without all devices operational, not all subnets, as shown in [Diagram 2](#) in [Part I](#), are accessible. The **packet-tracer** command on the ASA can be used to verify that at least ASA1 is properly configured to reach any subnet in the topology.

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**

Basic Parameters

```
ASA1# changeto system
```

Check that the hostname is ASA1:

```
ASA1# show hostname
```

```
ASA1
```

Verify whether the firewall mode is Router, not Transparent:

```
ASA1# show firewall
```

```
Firewall mode: Router
```

Verify whether the mode is multi-context:

[Click here to view code image](#)

```
ASA1# show mode
```

```
Security context mode: multiple
```

Verify whether three contexts are defined and interfaces are correctly applied in the system execution space:

[Click here to view code image](#)

```
ASA1# show context
```

Context Name	Class	Interfaces	URL
*admin	default	GigabitEthernet0/2.2	disk0:/admin.cfg
c2	default	GigabitEthernet0/0, GigabitEthernet0/1, GigabitEthernet0/3	disk0:/c2.cfg
c1	default	GigabitEthernet0/0, GigabitEthernet0/2.1	disk0:/c1.cfg

```
Total active Security Contexts: 3
```

Verify that the VLAN IDs have been assigned correctly. If the subinterfaces are not up, check your switch port configuration and make sure it is set to trunking and allowing VLANs 101 and 102:

[Click here to view code image](#)

```
ASA1# show int gigabitEthernet 0/2.1
```

```
Interface GigabitEthernet0/2.1 "", is up, line protocol is up
```

```
Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
```

```
VLAN identifier 101
```

```
Available for allocation to a context
```

```
ASA1# show int gigabitEthernet 0/2.2
```

```
Interface GigabitEthernet0/2.2 "", is up, line protocol is up
```

```
Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
```

```
VLAN identifier 102
```

```
Available for allocation to a context
```

Admin Context Parameters

[Click here to view code image](#)

```
ASA1# changeto context admin
```

Verify whether the correct format for the nameif name is used (case sensitive) and the security level is set to 100:

[Click here to view code image](#)

```
ASA1/admin# show nameif
Interface      Name      Security
Management0/0 mgmt      100
```

Verify the interface assignment, status, and IP addressing:

[Click here to view code image](#)

```
ASA1/admin# show interface ip brief
Interface      IP-Address  OK? Method Status  Protocol
GigabitEthernet0/2.2  192.168.1.20  YES manual up
```

Verify the default route for the admin context:

[Click here to view code image](#)

```
ASA1/admin# show route
```

Gateway of last resort is 192.168.1.5 to network 0.0.0.0

```
C 192.168.1.0 255.255.255.0 is directly connected, mgmt
S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.1.5, mgmt.
```

Verify the IP address/interface/name assignment. Because no failover is being deployed, the system IP addresses will always match the current IP addresses. If this ASA was the secondary unit in a failover pair, the current IP addresses would point to the primary device addresses.

[Click here to view code image](#)

```
ASA1/admin# show ip address
```

System IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/2.2	mgmt	192.168.1.20	255.255.255.0	manual

Current IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/2.2	mgmt	192.168.1.20	255.255.255.0	manual

Verify whether the management interface is set to management-only:

[Click here to view code image](#)

```
ASA1/admin# show interface
```

```
Interface GigabitEthernet0/2.2 "mgmt", is up, line protocol is up
```

```
MAC address 1200.0202.0100, MTU 1500
```

```
IP address 192.168.1.20, subnet mask 255.255.255.0
```

```
Traffic Statistics for "mgmt":
```

```
138 packets input, 10938 bytes
```

```
715 packets output, 27076 bytes
```

0 packets dropped

Management-only interface. Blocked 0 through-the-device packets

Verify admin context connectivity, which is limited to the part of the network where key servers such as a syslog server and DNS are located:

[Click here to view code image](#)

```
ASA1/admin# ping 192.168.1.5
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.1.5, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
ASA1/admin# ping 192.168.2.5
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.2.5, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms
```

Context c1 Parameters

```
ASA1# changeto context c1
```

Verify whether the correct format for the nameif names are used (case sensitive) and the security levels are set correctly:

[Click here to view code image](#)

```
ASA1/c1# show nameif
```

Interface	Name	Security
GigabitEthernet0/0	outside	0
GigabitEthernet0/2.1	inside	100

Verify the interface assignment, status, and IP addressing:

[Click here to view code image](#)

```
ASA1/c1# show interface ip brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	10.50.80.20	YES	manual	up	up
GigabitEthernet0/2.1	192.168.2.20	YES	manual	up	up

Verify the default route for the user context c1:

[Click here to view code image](#)

```
ASA1/c1# show route
```

```
Gateway of last resort is 10.50.80.6 to network 0.0.0.0
```

```
C 10.50.80.0 255.255.255.0 is directly connected, outside
```

C 192.168.2.0 255.255.255.0 is directly connected, inside

S* 0.0.0.0 0.0.0.0 [1/0] via 10.50.80.6, outside

Verify the IP address/interface/name assignment. Because no failover is being deployed, the system IP addresses will always match the current IP addresses. If this ASA was the secondary unit in a failover pair, the current IP addresses would point to the primary device addresses.

[Click here to view code image](#)

```
ASA1/c1# show ip address
```

System IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0	outside	10.50.80.20	255.255.255.0	manual
GigabitEthernet0/2.1	inside	192.168.2.20	255.255.255.0	manual

Current IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0	outside	10.50.80.20	255.255.255.0	manual
GigabitEthernet0/2.1	inside	192.168.2.20	255.255.255.0	manual

Verify context c1 connectivity:

[Click here to view code image](#)

```
ASA1/c1# ping 192.168.2.25
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.2.25, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

```
ASA1/c1# ping 10.50.70.5
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.50.70.5, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

```
ASA1/c1# ping 10.50.90.5
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.50.90.5, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

Context c2 Parameters

```
ASA1# changeto context c2
```

Verify whether the correct format for the nameif names are used (case sensitive) and the security levels are set correctly:

[Click here to view code image](#)

```
ASA1/c2# show nameif
```

Interface	Name	Security
-----------	------	----------

```
GigabitEthernet0/0    outside    0
GigabitEthernet0/1    dmz        50
GigabitEthernet0/3    inside     100
```

Verify the interface assignment, status, and IP addressing:

[Click here to view code image](#)

```
ASA1/c2# show interface ip brief
Interface            IP-Address    OK? Method Status    Protocol
GigabitEthernet0/0  10.50.80.30   YES manual up        up
GigabitEthernet0/1  10.50.90.20   YES manual up        up
GigabitEthernet0/3  10.50.100.20 YES manual up        up
```

Verify the default route for the user context c2:

[Click here to view code image](#)

```
ASA1/c2# show route
```

Gateway of last resort is 10.50.80.6 to network 0.0.0.0

```
S 10.10.0.0 255.255.0.0 [1/0] via 10.50.100.2, inside
C 10.50.100.0 255.255.255.0 is directly connected, inside
C 10.50.90.0 255.255.255.0 is directly connected, dmz
C 10.50.80.0 255.255.255.0 is directly connected, outside
S* 0.0.0.0 0.0.0.0 [1/0] via 10.50.80.6, outside
```

Verify the IP address/interface/name assignment. Because no failover is being deployed, the system IP addresses will always match the current IP addresses. If this ASA was the secondary unit in a failover pair, the current IP addresses would point to the primary device addresses.

[Click here to view code image](#)

```
ASA1/c2# show ip address
```

System IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0	outside	10.50.80.30	255.255.255.0	manual
GigabitEthernet0/1	dmz	10.50.90.20	255.255.255.0	manual
GigabitEthernet0/3	inside	10.50.100.20	255.255.255.0	manual

Current IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0	outside	10.50.80.30	255.255.255.0	manual
GigabitEthernet0/1	dmz	10.50.90.20	255.255.255.0	manual
GigabitEthernet0/3	inside	10.50.100.20	255.255.255.0	manual

Verify context c2 connectivity:

[Click here to view code image](#)

```
ASA1/c2# ping 10.50.90.5
Type escape sequence to abort.
```

Sending 5, 100-byte ICMP Echos to 10.50.90.5, timeout is 2 seconds:
!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA1/c2# ping 10.50.70.5

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.50.70.5, timeout is 2 seconds:
!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA1/c2# ping 192.168.2.5

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.2.5, timeout is 2 seconds:
!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA1/c2# ping 192.168.2.50

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.2.50, timeout is 2 seconds:
!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ASA1 Configuration

[Click here to view code image](#)

```
! System Execution Space
hostname ASA1
enable password 8Ry2YjIyt7RRXU24 encrypted
mac-address auto
!
interface GigabitEthernet0/0
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface GigabitEthernet0/2.1
vlan 101
!
interface GigabitEthernet0/2.2
vlan 102
!
interface GigabitEthernet0/3
!
interface Management0/0
shutdown
```

```
!  
class default  
  limit-resource All 0  
  limit-resource ASDM 5  
  limit-resource SSH 5  
  limit-resource Telnet 5  
!  
  
ftp mode passive  
pager lines 24  
no failover  
no asdm history enable  
arp timeout 14400  
no arp permit-nonconnected  
console timeout 0  
  
admin-context admin  
context admin  
  allocate-interface GigabitEthernet0/2.2  
  config-url disk0:/admin.cfg  
!  
  
context c2  
  allocate-interface GigabitEthernet0/0  
  allocate-interface GigabitEthernet0/1  
  allocate-interface GigabitEthernet0/3  
  config-url disk0:/c2.cfg  
!  
  
context c1  
  allocate-interface GigabitEthernet0/0  
  allocate-interface GigabitEthernet0/2.1  
  config-url disk0:/c1.cfg  
!  


---

  
! Context Admin  
hostname admin  
names  
!  
interface GigabitEthernet0/2.2  
  nameif mgmt  
  security-level 100  
  ip address 192.168.1.20 255.255.255.0  
  management-only  
!  
route mgmt 0.0.0.0 0.0.0.0 192.168.1.5 1  


---


```



```
! Context c1
hostname c1
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.50.80.20 255.255.255.0
!
interface GigabitEthernet0/2.1
 nameif inside
 security-level 100
 ip address 192.168.2.20 255.255.255.0
!
access-list 101 extended permit icmp any any
pager lines 24
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
access-group 101 in interface outside
route outside 0.0.0.0 0.0.0.0 10.50.80.6 1
```

```
! Context c2
hostname c2
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.50.80.30 255.255.255.0
!
interface GigabitEthernet0/1
 nameif dmz
 security-level 50
 ip address 10.50.90.20 255.255.255.0
!
interface GigabitEthernet0/3
 nameif inside
 security-level 100
 ip address 10.50.100.20 255.255.255.0
```

```
!
access-list 101 extended permit icmp any any
pager lines 24
mtu outside 1500
mtu dmz 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
access-group 101 in interface outside
access-group 101 in interface dmz
route outside 0.0.0.0 0.0.0.0 10.50.80.6
```

Tech Notes

- In this exercise, static routes were defined in such a way as to direct context-to-context traffic through the Cisco Intrusion Prevention Sensor (IPS). Traffic that must be forwarded between contexts c1 and c2 will do so via R6, which means it will pass through the sensor twice.

In some situations, it might be allowable to pass traffic directly between contexts on the Cisco ASA. This can be accomplished by adding the following static routes:

- c1 to c2:

[Click here to view code image](#)

```
route outside 10.50.100.0 255.255.255.0 10.50.80.30
```

- c2 to c1:

[Click here to view code image](#)

```
route outside 192.168.2.0 255.255.255.0 10.50.80.20
```

Note

In later versions of Cisco ASA software (starting with v9.X), dynamic routing is supported in multicontext firewall mode, which can be used in lieu of defining static routes.

Note

The Cisco ASA is capable of hosting an IPS module that can be used as a replacement for the Cisco IPS sensor. The network administrator should be aware of any differences in the capabilities of each sensor implementation (standalone versus integrated) to find the most appropriate solution for a customer environment.

- This configuration is using the concept of a shared outside interface. By default, the two contexts c1 and c2 would share the same MAC address. This will lead to packet forwarding issues for upstream devices that will not see a unique MAC address mapped to each context IP address in the ARP cache. Using the **mac-address auto** command is the quickest way to assign

a unique MAC address to each context. To verify whether this command has been correctly configured, check the output of the ARP cache on R6 and note distinct MAC addresses for each ASA1 context IP address:

[Click here to view code image](#)

```
R6# show arp
Protocol Address      Age (min) Hardware Addr  Type  Interface
Internet 10.50.80.20      13  1200.0000.0400 ARPA  Ethernet0/0
Internet 10.50.80.30      98  1200.0000.0300 ARPA  Ethernet0/0
```

The Cisco ASA will classify a packet using the following criteria to determine the correct destination context:

- Unique interface
- Unique MAC address
- Address translation policies

In this exercise, the outside interface of ASA1 is shared, and as yet no NAT rules are defined, so the use of unique MAC addresses is critical for correct packet classification.

- On ASA1, interface GigabitEthernet0/2 is also shared using subinterfaces/VLANs. Note that the VLAN identifier is defined in the system execution space with the remainder of the logical parameters applied at the context level (admin and user). The switch port supporting multiple VLANs should be configured as a trunk port.
- In this design, the Management0/0 interface is assigned to the admin context for management-only purposes. This means the interface will accept only traffic destined to and sourced from the appliance. To enable this interface to forward traffic through the appliance, management-only mode must be disabled on the interface.

Solution and Verification for Exercise 1.2: Configure Routing and Basic Access on ASA2

Skills Tested

- Configuration of a Cisco ASA in single-context routed mode
- An understanding of the configuration of dynamic routing protocols; specifically, Open Shortest Path First (OSPF) on the Cisco ASA

Solution and Verification

This exercise focuses on initializing ASA2 as a single-mode routed firewall that can support dynamic routing protocols. It is important to carefully verify the configuration of ASA2 because it is a critical security element in the topology and assumes the role of an OSPF Area Border Router (ABR).

For all verification syntax that follows:

- Required output appears in **red**

Check that the hostname is ASA2:

```
ASA2# show hostname
```

ASA2

Verify whether the firewall mode is Router, not Transparent:

```
ASA2# show firewall
```

```
Firewall mode: Router
```

Verify whether the mode is single-context:

[Click here to view code image](#)

```
ASA2# show mode
```

```
Security context mode: single
```

Verify the interface assignment, status and IP addressing:

[Click here to view code image](#)

```
ASA2# show interface ip brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	10.50.50.20	YES	manual	up	up
GigabitEthernet0/1	unassigned	YES	unset	administratively down	up
GigabitEthernet0/2	10.50.40.20	YES	manual	up	up
GigabitEthernet0/3	10.50.30.20	YES	manual	up	up

Verify the IP address/interface/name assignment. Because no failover is being deployed, the system IP addresses will always match the current IP addresses. If this ASA was the secondary unit in a failover pair, the current IP addresses would point to the primary device addresses.

[Click here to view code image](#)

```
ASA2# show ip address
```

```
System IP Addresses:
```

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/2	inside	10.50.40.20	255.255.255.0	manual
GigabitEthernet0/3	dmz	10.50.30.20	255.255.255.0	manual
GigabitEthernet0/0	outside	10.50.50.20	255.255.255.0	manual

```
Current IP Addresses:
```

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/2	inside	10.50.40.20	255.255.255.0	manual
GigabitEthernet0/3	dmz	10.50.30.20	255.255.255.0	manual
GigabitEthernet0/0	outside	10.50.50.20	255.255.255.0	manual

Verify the routing table on ASA2. The table should contain the required static routes and receive routes from neighbors in all areas. Note the inclusion of OSPF External Type 2 (O E2) routes; for example, network 10.7.7.0/24, which was redistributed into OSPF on R7 rather than being an OSPF-originated route (using network commands under the OSPF process). Redistribution occurs between autonomous systems; hence, R7 would be considered an OSPF Autonomous System Boundary Router (ASBR). If the static routes on ASA2 were redistributed into OSPF, it too would be an ASBR.

[Click here to view code image](#)

```
ASA2# show route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 10.50.50.5 to network 0.0.0.0

```
O E2 10.10.0.0 255.255.0.0 [110/20] via 10.50.50.5, 0:01:51, outside
O E2 10.7.7.0 255.255.255.0 [110/20] via 10.50.40.7, 0:00:06, inside
S 10.3.3.0 255.255.255.0 [1/0] via 10.50.30.3, dmz
S 10.4.4.0 255.255.255.0 [1/0] via 10.50.30.4, dmz
C 10.50.50.0 255.255.255.0 is directly connected, outside
C 10.50.40.0 255.255.255.0 is directly connected, inside
C 10.50.30.0 255.255.255.0 is directly connected, dmz
O 10.50.9.0 255.255.255.0 [110/11] via 10.50.50.5, 153:41:56, outside
O 10.50.99.0 255.255.255.0 [110/11] via 10.50.50.5, 153:41:56, outside
O E2 10.50.100.0 255.255.255.0 [110/20] via 10.50.50.5, 151:10:22, outside
O E2 10.50.90.0 255.255.255.0 [110/20] via 10.50.50.5, 151:10:22, outside
O 10.50.77.0 255.255.255.0 [110/11] via 10.50.50.5, 153:41:56, outside
O 10.50.70.0 255.255.255.0 [110/11] via 10.50.50.5, 153:41:56, outside
O E2 192.168.2.0 255.255.255.0 [110/20] via 10.50.50.5, 151:10:22, outside
O E2 192.168.100.0 255.255.255.0 [110/20] via 10.50.50.5, 151:10:22, outside
O*E2 0.0.0.0 0.0.0.0 [110/1] via 10.50.50.5, 151:10:34, outside
```

Checking the routing table on OSPF neighbors will verify that route propagation is occurring correctly on ASA2. The OSPF routes from areas 1 and 2 advertised by ASA2 into area 0 will appear as OSPF Intra-Area (O IA) routes:

[Click here to view code image](#)

```
SW2# show ip route
```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 10.50.70.6 to network 0.0.0.0

```
O*E2 0.0.0.0/0 [110/1] via 10.50.70.6, 1d01h, Vlan70
```

10.0.0.0/8 is variably subnetted, 15 subnets, 2 masks

```

O E2 10.10.0.0 255.255.0.0 [110/20] via 10.50.70.6, 0:01:51, Vlan70
O E2 10.7.7.0/24 [110/20] via 10.50.50.20, 00:04:20, Vlan50
O IA 10.50.30.0/24 [110/11] via 10.50.50.20, 23:02:58, Vlan50
O IA 10.50.40.0/24 [110/11] via 10.50.50.20, 1d01h, Vlan50
C 10.50.50.0/24 is directly connected, Vlan50
L 10.50.50.5/32 is directly connected, Vlan50
C 10.50.70.0/24 is directly connected, Vlan70
L 10.50.70.5/32 is directly connected, Vlan70
C 10.50.77.0/24 is directly connected, Vlan77
L 10.50.77.5/32 is directly connected, Vlan77
O E2 10.50.90.0/24 [110/20] via 10.50.70.6, 1d01h, Vlan70
C 10.50.99.0/24 is directly connected, Vlan99
L 10.50.99.5/32 is directly connected, Vlan99
O E2 10.50.100.0/24 [110/20] via 10.50.70.6, 1d01h, Vlan70
O E2 192.168.2.0/24 [110/20] via 10.50.70.6, 1d01h, Vlan70
O E2 192.168.100.0/24 [110/20] via 10.50.70.6, 1d01h, Vlan70

```

Verify that all neighbor relationships are formed and OSPF database information has been completely exchanged. This is denoted by the FULL state for any device in the role of Designated Router (DR) or Backup Designated Router (BDR). If a neighbor is listed as 2WAY/DROTHER, it is not eligible to become the DR or BDR for a network but can assume either of these roles in the event of BDR or DR device instability.

[Click here to view code image](#)

```
ASA2# show ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.18.107.7	1	FULL/DR	0:00:36	10.50.40.7	inside
172.16.33.3	1	FULL/BDR	0:00:34	10.50.30.3	dmz
172.16.34.4	1	FULL/DR	0:00:35	10.50.30.4	dmz
10.50.99.5	1	FULL/DR	0:00:36	10.50.50.5	outside

Verify whether ASA2 is configured for three OSPF areas. Note that at this point, no authentication is occurring in the areas.

[Click here to view code image](#)

```
ASA2# show ospf 1
```

Routing Process "ospf 1" with ID 10.50.50.20 and Domain ID 0.0.0.1

Supports only single TOS(TOS0) routes

Does not support opaque LSA

It is an area border router

SPF schedule delay 5 secs, Hold time between two SPFs 10 secs

Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs

Number of external LSA 20. Checksum Sum 0x 97a04

Number of opaque AS LSA 0. Checksum Sum 0x 0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 3. 3 normal 0 stub 0 nssa
External flood list length 0

Area BACKBONE(0)

Number of interfaces in this area is 1
Area has no authentication
SPF algorithm executed 78 times
Area ranges are
Number of LSA 24. Checksum Sum 0x fdce6
Number of opaque link LSA 0. Checksum Sum 0x 0
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

Area 1

Number of interfaces in this area is 1
Area has no authentication
SPF algorithm executed 72 times
Area ranges are
Area-filter ospf in
Number of LSA 17. Checksum Sum 0x 825dd
Number of opaque link LSA 0. Checksum Sum 0x 0
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

Area 2

Number of interfaces in this area is 1
Area has no authentication
SPF algorithm executed 29 times
Area ranges are
Number of LSA 15. Checksum Sum 0x 85505
Number of opaque link LSA 0. Checksum Sum 0x 0
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

Configuration

ASA2

[Click here to view code image](#)

```
hostname ASA2
```

```
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.50.50.20 255.255.255.0
 ospf priority 0
!
!
interface GigabitEthernet0/2
 nameif inside
 security-level 100
 ip address 10.50.40.20 255.255.255.0
!
interface GigabitEthernet0/3
 nameif dmz
 security-level 50
 ip address 10.50.30.20 255.255.255.0
!
!
access-list 101 extended permit icmp any any
!
access-group 101 in interface outside
access-group 101 in interface dmz
!
!
router ospf 1
 network 10.50.30.0 255.255.255.0 area 1
 network 10.50.40.0 255.255.255.0 area 2
 network 10.50.50.0 255.255.255.0 area 0
 log-adj-changes
!
route dmz 10.3.3.0 255.255.255.0 10.50.30.3 1
route dmz 10.4.4.0 255.255.255.0 10.50.30.4 1
```

Tech Notes

- When configuring OSPF on the Cisco ASA, note the difference in the syntax for the network mask or wildcard bits from Cisco IOS.
- When redistributing routes into OSPF, be aware of the default behavior, which is to advertise classful summaries. If subnets should be explicitly advertised and not summarized according to IP address class, use the subnets option. For example:

[Click here to view code image](#)

redistribute static subnets

Other routing protocols use different commands to manipulate summarization.

- As with Cisco IOS, the router-id used by the Cisco ASA is the highest IP address on the device. This is in the absence of a user-defined router-id or a loopback address. The router-id used in the advertising router field of an OSPF Link State Advertisement (LSA) must be a routable address. Six well-known LSA types are used in OSPFv2, as described in [Table 1a-1](#).

Type	LSA	Functionality
1	Router	Defines the state of a router's link into each area and is flooded only within the applicable area.
2	Network	Defines the number of routers attached to a segment of a network and flooded into the area containing that segment.
3	Summary Network	Describes OSPF destinations (networks) outside an area. The summary of one area is flooded into other areas by the ABR.
4	Summary ASBR	Generated by an Area Border Router (ABR) and describes any Autonomous System Boundary Routers (ASBR) that connect to the same area as the ABR. An ASBR will have interfaces in an OSPF area and some other autonomous system; for example, an EIGRP AS.
5	External	Defines routes to destinations external to OSPF. Originated by an ASBR where route redistribution is occurring.
7	NSSA	Enables an external destination route to be injected into an area that is defined as a Not-So-Stubby Area (NSSA). NSSA areas accept IGRP routes but act as a stub area with respect to OSPF routes.

Table 1a-1 *Well-Known OSPFv2 LSA Types*

Solution and Verification for Exercise 1.3: Configure IP Services on ASA1

Skills Tested

- The application of NAT policies on the Cisco ASA using the Network Object NAT and Twice NAT methods
- Configuring NTP service using MD5 for authentication of the NTP peers
- Understand the order of operations on the Cisco ASA as it pertains to packet handling

Solution and Verification

The tasks in this exercise build upon the initial configuration of ASA1 in [Exercise 1.1](#). In software releases version 8.3 and later, the configuration of NAT changed significantly. If you choose to use a software version pre-8.3, the solutions presented here will not apply.

NAT rules can be configured to allow either unidirectional or bidirectional communication. Bidirectional connections are static, and can be initiated from either the nontranslated/local side or the translated/global side of the ASA; they also generally involve one-to-one mappings. If a unidirectional or “dynamic” NAT rule is configured, connections cannot be initiated on the translated side of the ASA. Dynamic translations are applicable if the number of addresses to map is greater than the number of addresses available in the translation pool.

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**
- Variable syntax appears in **green**

Task 1: Network Object NAT

Verify the NAT rule. Network Object NAT rules are added to section 2 of the NAT policy rule list. The translation requirement was to support bidirectional communication, so verify whether the NAT rule is static.

[Click here to view code image](#)

```
ASA1/c2# changeto context c2
```

```
ASA1/c2# show nat detail
```

Auto NAT Policies (Section 2)

```
1 (dmz) to (outside) source static r5 10.50.80.50  
  translate_hits = 2, untranslate_hits = 4  
  Source - Origin: 10.50.90.5/32, Translated: 10.50.80.50/32
```

Verify the complete packet path through ASA2 using the **packet-tracer**. Look for the NAT phase of processing in the command output.

[Click here to view code image](#)

```
ASA1/c2# packet-tracer input dmz icmp 10.50.90.5 0 8 10.50.30.3
```

Phase: 5

Type: NAT

Subtype:

Result: ALLOW

Config:

object network r5

nat (dmz,outside) static 10.50.80.50

Additional Information:

Static translate 10.50.90.5/0 to 10.50.80.50/0

Task 2: Twice NAT

Twice NAT rules are added to section 1 of the NAT policy rule list:

[Click here to view code image](#)

```
ASA1/c2# changeto context c2
```

```
ASA1/c2# show nat detail
```

Manual NAT Policies (Section 1)

```
1 (inside) to (outside) source dynamic 100net pool50 destination static  
  remote50net remote50net  
  translate_hits = 0, untranslate_hits = 0
```

Source - Origin: 10.50.100.0/24, Translated: 10.50.80.100-10.50.80.150

Destination - Origin: 10.50.50.0/24, Translated: 10.50.50.0/24

Verify the complete packet path through ASA2 using the **packet-tracer**. Look for the NAT phase of processing in the command output.

[Click here to view code image](#)

```
ASA1/c2# packet-tracer input inside icmp 10.50.100.1 0 8  
10.50.50.5
```

Phase: 4

Type: NAT

Subtype:

Result: ALLOW

Config:

```
nat (inside,outside) source dynamic 100net pool50 destination static remote50net  
remote50net
```

Additional Information:

Dynamic translate 10.50.100.1/0 to 10.50.80.113/0

```
ASA1/c2# packet-tracer input inside icmp 10.50.100.1 0 8  
10.50.80.6
```

Phase: 4

Type: NAT

Subtype:

Result: ALLOW

Config:

```
nat (inside,outside) source static 100net 100net
```

Additional Information:

Static translate 10.50.100.1/0 to 10.50.100.1/0

Task 3: NTP with Authentication

NTP is enabled in the system execution space when the ASA is configured in multicontext mode. Verify whether ASA1 is in sync with the NTP master server that was partially configured on SW1 (192.168.1.5). Also verify whether NTP exchanges are authenticated.

[Click here to view code image](#)

```
ASA1# changeto system
```

```
ASA1# show ntp associations detail
```

```
192.168.1.5 configured, authenticated, our_master, sane, valid, stratum 2
```

```
ASA1# show ntp status
```

```
Clock is synchronized, stratum 3, reference is 192.168.1.5
```

This task also required some troubleshooting to complete and correct issues with the NTP configuration on SW1.

Add the following commands to SW1:

```
ntp authenticate
ntp trusted-key 1
```

Correct the peer address used in the NTP access-list:

[Click here to view code image](#)

```
access-list 1 permit 192.168.1.20
```

Task 4: Tunneling ipv6ip

Verify whether the correct access list policy is defined and applied to the outside interface:

[Click here to view code image](#)

```
ASA1/c2# changeto context c2
```

```
ASA1/c2# show access-list
```

```
access-list 101 line 2 extended permit 41 host 10.50.80.6 host 10.50.90.5
```

Configuration

ASA1 System

[Click here to view code image](#)

```
ntp authentication-key 1 md5 ***** (cisco is not displayed)
ntp authenticate
ntp trusted-key 1
ntp server 192.168.1.5 key 1 source mgmt
```

ASA1/c2

[Click here to view code image](#)

```
object network r5
 host 10.50.90.5
object network r5
 nat (dmz,outside) static 10.50.80.50
```

```
object network 100net
 subnet 10.50.100.0 255.255.255.0
object network remote50net
 subnet 10.50.50.0 255.255.255.0
object network pool50
 range 10.50.80.100 10.50.80.150
```

```
nat (inside,outside) source dynamic 100net pool50 destination static remote50net
 remote50net
nat (inside,outside) source static 100net 100net
```

```
access-list 101 extended permit icmp any any
access-list 101 extended permit 41 host 10.50.80.6 host 10.50.90.5
```

```
access-group 101 in interface outside
```

SW1

[Click here to view code image](#)

```
ntp authentication-key 1 md5 cisco
ntp authenticate
ntp trusted-key 1
ntp source Vlan102
ntp access-group peer 1
ntp master 2
```

```
access-list 1 permit 192.168.1.20
```

Tech Notes

Configuring NAT in Cisco ASA software releases post version 8.3 is reliant on understanding the concept of *objects* and *object-groups*. These structures can also be used in place of access lists for identifying interesting traffic in terms of networks, protocols, and services (ports).

Additionally, object types may be combined and nested to provide more flexibility. In the following example, the pool of translated addresses available includes a range of contiguous addresses defined in the network object pool50 plus the single address 10.50.80.251:

[Click here to view code image](#)

```
object network pool50
  range 10.50.80.100 10.50.80.150

object-group network dest-remotenet50
  network-object object pool50
  network-object host 10.50.80.251
```

The **packet-tracer** command has been used to verify the NAT configurations in this question. This command can also be used to verify the configuration of other ASA features, such as access lists and routing. For example, before full connectivity in a network is available, a ping can be tested using **packet-tracer** with **icmp** options:

[Click here to view code image](#)

```
ASA1/c2# packet-tracer input outside icmp 10.50.50.5 0 8
10.50.100.10
```

```
Phase: 1
Type: ACCESS-LIST
Subtype:
```

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 2

Type: UN-NAT

Subtype: static

Result: ALLOW

Config:

nat (inside,outside) source static 100net 100net

Additional Information:

NAT divert to egress interface inside

Untranslate 10.50.100.10/0 to 10.50.100.10/0

Phase: 3

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

access-group 101 in interface outside

access-list 101 extended permit icmp any any

Additional Information:

Phase: 4

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 5

Type: INSPECT

Subtype: np-inspect

Result: ALLOW

Config:

Additional Information:

Phase: 6

Type: NAT

Subtype:

Result: ALLOW

Config:

nat (inside,outside) source static 100net 100net

Additional Information:

Static translate 10.50.50.5/0 to 10.50.50.5/0

Phase: 7

Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

```
nat (inside,outside) source dynamic 100net pool50 destination static remote50net
  remote50net
```

Additional Information:

Phase: 8

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 754623, packet dispatched to next module

Result:

input-interface: outside

input-status: up

input-line-status: up

output-interface: inside

output-status: up

output-line-status: up

Action: allow

The preceding output from the **packet-tracer** command illustrates how the order of operations on the Cisco ASA is important for understanding the relationship between features such as access lists and NAT. In this exercise, the access list for the ipv6ip tunnel specified the untranslated or actual destination address of 10.50.90.5 as the tunnel endpoint on R5. The untranslated address is used to create the ASA connection.

[Click here to view code image](#)

```
ASA1/c2(config)# show conn detail
```

```
41 outside:10.50.80.6/0 dmz:10.50.90.5/0,
```

```
idle 3s, uptime 7D11h, timeout 2m0s, bytes 11154548
```

However, as you will see in [Exercise 5.1](#), the tunnel destination from the perspective of R6 will be the translated address of 10.50.80.50.

ASA NAT rule processing follows a specific order of precedence, which checks for a more explicit rule to match first. In post 8.3 software, there is an additional order of precedence, as rule types are grouped into sections. The **show nat detail** command outlines the sections created in this question:

[Click here to view code image](#)

```
ASA1/c2(config)# show nat detail
```

Manual NAT Policies (Section 1)

```
1 (inside) to (outside) source dynamic 100net pool50 destination static
remote50net remote50net
translate_hits = 1, untranslate_hits = 1
Source - Origin: 10.50.100.0/24, Translated: 10.50.80.100-10.50.80.150
Destination - Origin: 10.50.50.0/24, Translated: 10.50.50.0/24
2 (inside) to (outside) source static 100net 100net
translate_hits = 11941, untranslate_hits = 1250
Source - Origin: 10.50.100.0/24, Translated: 10.50.100.0/24
```

Auto NAT Policies (Section 2)

```
1 (dmz) to (outside) source static r5 10.50.80.50
translate_hits = 32, untranslate_hits = 1290
Source - Origin: 10.50.90.5/32, Translated: 10.50.80.50/32
```

Section 1 comprises twice NAT rules (plus dynamically added invisible virtual private network [VPN] rules), whereas section 2 is built using network object NAT rules. In both sections, static rules take precedence over dynamic rules. It is important to be aware of overlapping rules across sections, which can yield unexpected results.

There is also a section 3, which is available for twice NAT rules that need to be processed after those in sections 1 and 2.

It is important that the administrator understand how to migrate NAT rules from a software release pre 8.3 to a post 8.3 release. The following are some examples that may be used for reference.

Old Configuration

[Click here to view code image](#)

```
static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 dns
```

Migrated Configuration

[Click here to view code image](#)

```
object network obj-192.168.100.10
host 192.168.100.10
nat (inside,outside) static 172.20.1.10 dns
```

Old Configuration

[Click here to view code image](#)

```
global (outside) 1 10.76.6.111
global (outside) 1 10.76.6.109-10.76.6.110
```

New Network Objects and Groups

[Click here to view code image](#)

```
object network obj-10.76.6.111
host 10.76.6.111
```


object network obj-10.76.6.109-10.76.6.110
 range 10.76.6.109-10.76.6.110
 object-group og-global-outside_1
 network-object obj-10.76.6.111
 network-object obj-10.76.6.109-10.76.6.110

[Table 1a-2](#) summarizes the various NAT types supported on the Cisco ASA. Note there are subtle differences in implementing these pre- and post-version 8.3.

NAT Type	Static or Dynamic	Bidirectional or Unidirectional Traffic Initiation	Ratio (private: public:port)	Notes
Static NAT	Static	Bidirectional	1:1	The same private address is always mapped to the same static address. The mapping is persistent.
Dynamic NAT	Dynamic	Unidirectional	1:1	A private address is mapped to the next available public address in a pool.
Dynamic PAT (NAT over-load)	Dynamic	Unidirectional	N:1	N private addresses are mapped to a single public address using unique port numbers to uniquely identify the mapping.
Static PAT	Static	Bidirectional	N:1:1	N private addresses are mapped to a unique public address/port pair. The port value is static and persistent, and this allows for bidirectional traffic initiation.
Identity NAT (nat 0 pre 8.3)	Dynamic	Unidirectional	1:1	The same address is used inside and outside the network. Requires an xlate to be created to allow return traffic.
Static Identity NAT	Static	Bidirectional	1:1	The same inside address is used on the outside. This mapping is persistent.
NAT Exemption (nat 0 with ACL pre 8.3)	Static	Bidirectional	1:1	Like identity NAT except the persistent Access Control List (ACL) creates a static mapping of the inside address to itself for use as the outside address.
Policy NAT	Static	Bidirectional	1:1	Extends NAT to enable a private address to be mapped to a specific public address depending on the destination of the flow. The public address can be statically defined or be part of a pool of addresses.
	Dynamic	Unidirectional	1:1	

Table 1a-2 *Cisco Supported NAT Types Summary*

Solution and Verification for Exercise 1.4: Configure IP Routing Security on ASA2

Skills Tested

- Configuring support for securing dynamic routing protocol traffic
- Understanding protocol-specific requirements for BGP to transit the Cisco ASA

Solution and Verification

The tasks in this exercise focus on configuring and troubleshooting dynamic routing security using ASA2. MD5-authenticated BGP routing traffic must transit ASA2, which will require some exceptions be made to the ASA default processing of TCP packets (discussed in more detail in the “Tech Notes” section of this exercise solution). ASA2 is also an OSPF routing neighbor responsible for sourcing routing updates and maintaining peering relationships with other devices. Applying MD5 authentication to the communications between neighbors provides a layer of security by implying origin authentication and message integrity.

For all verification syntax that follows:

- Required output appears in **red**

Task 1: BGP Connectivity Through ASA2

Verification of the solution configured on ASA2 is done by ensuring whether the BGP session between R6 and R7 is up and the network information configured under the BGP section of the router configurations is installed in the neighbor’s BGP routing tables.

[Click here to view code image](#)

```
R6# show ip bgp
```

```
BGP table version is 3, local router ID is 172.18.106.6
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,  
r RIB-failure, S Stale, m multipath, b backup-path, x best-external,  
f RT-Filter, a additional-path
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 172.18.106.0/24	0.0.0.0	0		32768	?
*> 172.18.107.0/24	10.50.40.7	0		0	107 ?

```
R7# show ip bgp
```

```
BGP table version is 5, local router ID is 172.18.107.7
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,  
r RIB-failure, S Stale, m multipath, b backup-path, x best-external,  
f RT-Filter, a additional-path
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 172.18.106.0/24	10.50.70.6	0		0	106 ?
*> 172.18.107.0/24	0.0.0.0	0		32768	?

```
ASA2# show conn
```

```
15 in use, 31 most used
```

```
TCP outside 10.50.70.6:179 inside 10.50.40.7:55489, idle 0:00:43, bytes 229761,  
flags UIO
```

Allowing the TCP session for BGP communication has more complexity in this deployment as the routing neighbors are exchanging communications that use MD5 authentication. Verify whether MD5 has been successfully applied.

[Click here to view code image](#)

```
R7# show ip bgp neighbor | inc md5
```

```
Option Flags: nagle, path mtu capable, md5
```

Task 2: OSPF Authentication for Routing Update Security

The requirement was to enable OSPF authentication within the area:

[Click here to view code image](#)

```
ASA2# show ospf | inc Area 2
```

```
Area 2
```

```
Number of interfaces in this area is 1
```

```
Area has message digest authentication
```

```
R7# show ip ospf | inc Area 2
```

```
Area 2
```

```
Number of interfaces in this area is 2 (1 loopback)
```

```
Area has message digest authentication
```

Verify whether the OSPF adjacencies have been reestablished after authentication was enabled:

[Click here to view code image](#)

```
ASA2# show ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.18.107.7	1	FULL/DR	0:00:38	10.50.40.7	inside

The following command output shows verification of the MD5 key ID being used on ASA2. Note that it is possible to enable authentication on a link by link basis if it is not required or supported by all neighbors in an area. Per interface authentication will allow for a mix of MD5, plaintext password, or NULL options.

[Click here to view code image](#)

```
ASA2# show ospf interface
```

```
....
```

```
inside is up, line protocol is up
```

```
Internet Address 10.50.40.20 mask 255.255.255.0, Area 2
```

```
Process ID 1, Router ID 10.50.50.20, Network Type BROADCAST, Cost: 10
```

```
Transmit Delay is 1 sec, State BDR, Priority 1
```

```
Designated Router (ID) 172.18.107.7, Interface address 10.50.40.7
```

Backup Designated router (ID) 10.50.50.20, Interface address 10.50.40.20
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:01
Index 1/3, flood queue length 0
Next 0x00000000(0)/0x00000000(0)
Last flood scan length is 1, maximum is 8
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 172.18.107.7 (Designated Router)
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
Youngest key id is 1

Configuration

ASA2

[Click here to view code image](#)

```
tcp-map eBGP
  tcp-options range 19 19 allow
class-map eBGPclass
  match port tcp eq bgp
policy-map global_policy
  class inspection_default
class eBGPclass
  set connection random-sequence-number disable
  set connection advanced-options eBGP

access-list 101 extended permit tcp any any eq bgp
access-list 101 extended permit tcp any eq bgp any
interface GigabitEthernet0/2
  nameif inside
  security-level 100
  ip address 10.50.40.20 255.255.255.0
  ospf message-digest-key 1 md5 cisco
  ospf authentication message-digest

router ospf 1
  area 2 authentication message-digest
```

R7

[Click here to view code image](#)

```
interface GigabitEthernet0/1
  ip address 10.50.40.7 255.255.255.0
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 cisco
```

```
router ospf 1
 area 2 authentication message-digest
```

Tech Notes

Support for MD5 authentication for BGP through the Cisco ASA requires the default behavior of the appliance—that is, to randomize TCP sequence numbers—to be disabled. MD5 authentication is applied on the TCP pseudo-IP header, TCP header, and data. TCP uses this data—which includes the TCP sequence and ACK numbers—along with the BGP neighbor password to create a 128-bit hash number. The hash number is included in the packet in a TCP header option field. TCP option 19 is used for BGP MD5 authentication.

By default, the ASA offsets the sequence number by a random number, per TCP flow. On the sending BGP peer, TCP uses the original sequence number to create the 128-bit MD5 hash number and includes this hash number in the packet. When the receiving BGP peer gets the packet, TCP uses the ASA-modified sequence number to create a 128-bit MD5 hash number and compares it to the hash number that is included in the packet.

The hash number is different because the TCP sequence value was changed by the ASA, and TCP on the BGP neighbor drops the packet and logs an MD5 failed message.

Section 2: Intrusion Prevention and Content Security

This section covers tasks applicable to some specialized Cisco appliances, the Intrusion Prevention Sensor (IPS) and the Web Services Appliance (WSA). Both devices will be initialized and deployed into the network topology as shown in [Diagram 1](#) and [Diagram 2](#) in [Part I](#). The single IPS appliance will be logically partitioned using various deployment modes of operation to service distinct traffic flows in the network. The WSA will handle redirected traffic of interest via Web Cache Communication Protocol (WCCP) from the Cisco ASA. It is important to verify whether traffic is correctly flowing through the appliances before moving on to other exercises in the lab.

Solution and Verification for Exercise 2.1: Initialize and Deploy the Cisco IPS Sensor Appliance

Skills Tested

- Basic initialization of the Cisco Intrusion Prevention Sensor (IPS) appliance and verification of the management interface
- An understanding of the different deployment modes available on the sensor, and how to configure sensor interfaces and attached switch ports to provide connectivity
- The role of virtual sensors under the service analysis engine

Solution and Verification

This exercise focused on the fundamentals of initializing and deploying the Cisco IPS appliance. Although these are basic tasks, any misconfiguration on the sensor or connected switch ports could result in traffic flows being disrupted as packets are black holed.

An important tool to verify whether packets are flowing through the sensor interfaces is the **packet**

display interface command on the sensor console.

For all verification syntax that follows:

- Required output appears in **red**

Task 1: Initialize the Cisco IPS

Verify connectivity to the sensor via the Management0/0 interface from SW1. Recall that the username/password is ciscoips/123cisco123. If the access list is correctly applied, Telnet will be allowed only from VLAN101 (192.168.2.0/24) on SW1:

[Click here to view code image](#)

```
SW1# telnet 192.168.2.100  
Trying 192.168.2.100 ... Open
```

```
login: ciscoips
```

```
Password:
```

```
***NOTICE***
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/ww1/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

```
***LICENSE NOTICE***
```

```
The license key on the IPS-4240 has expired.
```

```
The system will continue to operate with the currently installed signature set. A valid license must be obtained in order to apply signature updates. Please go to http://www.cisco.com/go/license to obtain a new license or install a license.
```

```
ips#
```

Access list will not permit Telnet from any other subnet.

[Click here to view code image](#)

```
SW1# telnet 192.168.2.100 /source-interface vlan102  
Trying 192.168.2.100 ...
```

Verification of the sensor mode configurations can be done by checking modes and status in the

interface summary. Note that the management interface is not being used to sense traffic:

[Click here to view code image](#)

```
IPS# show interfaces brief
```

CC Interface	Sensing State	Link	Inline Mode	Pair Status
GigabitEthernet0/0	Enabled	Up	Paired with interface GigabitEthernet0/1	Up
* Management0/0	Disabled	Up		
GigabitEthernet0/1	Enabled	Up	Paired with interface GigabitEthernet0/0	Up
GigabitEthernet0/2	Enabled	Up	Inline-vlan-pair	N/A
GigabitEthernet0/3	Enabled	Up	Unpaired	

Task 2: Deploy the Cisco IPS Sensor in Inline VLAN Pair Mode

Verification of the Inline VLAN pair should show that Gig0/2 is up and sensing:

[Click here to view code image](#)

```
IPS# show interfaces brief
```

CC Interface	Sensing State	Link	Inline Mode	Pair Status
GigabitEthernet0/0	Enabled	Up	Paired with interface GigabitEthernet0/1	Up
* Management0/0	Disabled	Up		
GigabitEthernet0/1	Enabled	Up	Paired with interface GigabitEthernet0/0	Up
GigabitEthernet0/2	Enabled	Up	Inline-vlan-pair	N/A
GigabitEthernet0/3	Enabled	Up	Unpaired	

Drilling down into the GigabitEthernet0/2 interface will verify the VLAN assignment for the Inline VLAN Pair:

[Click here to view code image](#)

```
IPS# show interfaces gigabitEthernet0/2
```

```
MAC statistics from interface GigabitEthernet0/2
```

```
Statistics From Subinterface 1
```

Statistics From Vlan 50

```
Total Packets Received On This Vlan = 1385065
```

```
Total Bytes Received On This Vlan = 123792833
```

```
Total Packets Transmitted On This Vlan = 546093
```

```
Total Bytes Transmitted On This Vlan = 58657037
```

Statistics From Vlan 70

```
Total Packets Received On This Vlan = 546180
```

```
Total Bytes Received On This Vlan = 58663474
```

```
Total Packets Transmitted On This Vlan = 1385010
```

```
Total Bytes Transmitted On This Vlan = 123788928
```

Task 3: Deploy the Cisco IPS Sensor in Inline Interface Pair Mode

Verification of the Inline Interface pair should show Gig0/0 and Gig0/1 paired and enabled:

[Click here to view code image](#)

```
IPS# show interfaces brief
```

CC Interface	Sensing State	Link	Inline Mode	Pair Status
--------------	---------------	------	-------------	-------------

GigabitEthernet0/0	Enabled	Up	Paired with interface GigabitEthernet0/1	Up
* Management0/0	Disabled	Up		
GigabitEthernet0/1	Enabled	Up	Paired with interface GigabitEthernet0/0	Up
GigabitEthernet0/2	Enabled	Up	Inline-vlan-pair	N/A
GigabitEthernet0/3	Enabled	Up	Unpaired	

Task 4: Deploy the Cisco IPS Sensor in Promiscuous Mode

Verification of the promiscuous mode interface should show Gig0/3 in a sensing state. When an interface is configured in promiscuous mode, the virtual sensor is associated with the physical interface operating as an IDS.

[Click here to view code image](#)

```
IPS# show interfaces brief
```

CC	Interface	Sensing State	Link	Inline Mode	Pair Status
	GigabitEthernet0/0	Enabled	Up	Paired with interface GigabitEthernet0/1	Up
*	Management0/0	Disabled	Up		
	GigabitEthernet0/1	Enabled	Up	Paired with interface GigabitEthernet0/0	Up
	GigabitEthernet0/2	Enabled	Up	Inline-vlan-pair	N/A
	GigabitEthernet0/3	Enabled	Up	Unpaired	

Verification of traffic flows through the sensor's inline (IPS) modes can be performed by pinging between major subnets in the topology.

Test connectivity across the Inline Interface Pair and the Inline VLAN Pair as follows:

[Click here to view code image](#)

```
R6# ping 192.168.2.5
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.2.5, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
R6# ping 10.50.40.7
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.50.40.7, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Verification of the sensor as an IDS (using promiscuous mode) will require traffic to be mirrored to interface GigabitEthernet0/3. In Q4.1, SPAN will be configured on SW2 to validate the IDS configuration.

Configuration

IPS

[Click here to view code image](#)

```
physical-interfaces GigabitEthernet0/0
```



```
admin-state enabled
exit
physical-interfaces GigabitEthernet0/1
admin-state enabled
exit
physical-interfaces GigabitEthernet0/2
admin-state enabled
subinterface-type inline-vlan-pair
subinterface 1
vlan1 70
vlan2 50
exit
exit
exit
physical-interfaces GigabitEthernet0/3
admin-state enabled
exit
inline-interfaces ipair
interface1 GigabitEthernet0/0
interface2 GigabitEthernet0/1
exit
exit
! -----
service authentication
exit
! -----
service event-action-rules rules0
exit
! -----
service host
network-settings
host-ip 192.168.2.100/24,192.168.2.20
host-name ips
telnet-option enabled
access-list 192.168.2.0/24
dns-primary-server disabled
dns-secondary-server disabled
dns-tertiary-server disabled
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! -----
```

```
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/2 subinterface-number 1
exit
virtual-sensor vs1
logical-interface ipair
exit
virtual-sensor vs2
physical-interface GigabitEthernet0/3
exit
exit
```

SW2

[Click here to view code image](#)

```
interface GigabitEthernet1/0/16
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 50,70
switchport mode trunk
!
interface GigabitEthernet1/0/17
switchport access vlan 10
switchport mode access
```

SW1

[Click here to view code image](#)

```
interface GigabitEthernet1/0/15
switchport access vlan 101
switchport mode access
!
interface GigabitEthernet1/0/16
switchport access vlan 60
switchport mode access
!
interface GigabitEthernet1/0/17
switchport access vlan 80
switchport mode access
```

Tech Notes

The packet display command is a useful tool when you are verifying whether the sensor is seeing traffic on its interfaces as expected. In the preceding verification, pings are used to validate whether traffic can pass through the sensor. Without visual verification on the sensor, it is possible that the sensor itself, or the switch ports to which it is connected, are misconfigured such that traffic is not actually passing through the sensor at all, even though traffic is flowing in the network.

If **ping** commands are issued with packet display for each interface enabled, you should see the ping

activity displayed on the IPS console.

[Click here to view code image](#)

```
R6# ping 192.168.2.5
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.2.5, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

The following is the output of the packet display command on the IPS sensor console:

[Click here to view code image](#)

```
02:07:43.923416 IP 10.50.80.6 > 192.168.2.5: ICMP echo request, id 29, seq 0, length 80
```

```
02:07:43.925547 IP 192.168.2.5 > 10.50.80.6: ICMP echo reply, id 29, seq 0, length 80
```

```
02:07:43.925909 IP 10.50.80.6 > 192.168.2.5: ICMP echo request, id 29, seq 1, length 80
```

```
02:07:43.926734 IP 192.168.2.5 > 10.50.80.6: ICMP echo reply, id 29, seq 1, length 80
```

```
02:07:43.927107 IP 10.50.80.6 > 192.168.2.5: ICMP echo request, id 29, seq 2, length 80
```

```
02:07:43.927831 IP 192.168.2.5 > 10.50.80.6: ICMP echo reply, id 29, seq 2, length 80
```

Solution and Verification for Exercise 2.2: Initialize the Cisco WSA

Skills Tested

- Basic configuration of the Cisco WSA via the CLI and the GUI

Solution and Verification

This question emphasizes the role of the web browser–based configuration and management GUI. Some features and functions can be performed from the WSA CLI; however, full functionality is available only via the GUI.

[Figure 1a-1](#) highlights the correct configuration of the WSA.

Administrative Settings	
Network Time Protocol (NTP):	192.168.2.5
Time Zone:	America/Los_Angeles
Email Alerts To:	foo@bar.com
Internal SMTP Relay Hosts:	No internal relay host is defined
AutoSupport:	Disabled

Network Settings	
Default System Hostname:	wsa.cisco.com
DNS Servers:	Use these DNS Servers:
	Priority IP Address
	0 192.168.2.25
Transparent Redirection Device Type:	WCCP v2 Router Service IDs: 90
Upstream Proxy:	No upstream proxy

Interfaces	
Management (M1)	
IP Address:	192.168.2.50
Network Mask:	255.255.255.0
Hostname:	wsa.cisco.com
L4 Traffic Monitor:	
Wiring Type:	Duplex TAP: T1 (In/Out)
Routes	
Management (M1)	
Default Gateway:	192.168.2.20
Static Routes:	No static routes have been defined.

Figure 1a-1 *WSA Initial Setup Parameters*

The preconfiguration of the WSA via the CLI is implemented as follows:

[Click here to view code image](#)

```
wsa.cisco.com> interfaceconfig
```

Currently configured interfaces:

1. Management (192.168.2.50/24 on Management: wsa.cisco.com)

Choose the operation you want to perform:

- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.

```
[]>
```

```
wsa.cisco.com> setgateway
```

Warning: setting an incorrect default gateway may cause the current connection to be interrupted when the changes are committed.

1. Management Default Gateway
2. Data Default Gateway

```
[]>
```

The resulting **showconfig** output is contained in an extremely large configuration file that emphasizes the need to work with the GUI.

[Click here to view code image](#)

```

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
  <hostname>wsa.cisco.com</hostname>
  <interfaces>
    <interface>
      <interface_name>Management</interface_name>
      <ip>192.168.2.50</ip>
      <phys_interface>Management</phys_interface>
      <netmask>255.255.255.0</netmask>
      <interface_hostname>wsa.cisco.com</interface_hostname>
      <ftpd_port>21</ftpd_port>
      <sshd_port>22</sshd_port>
      <httpd_port>8080</httpd_port>
      <https_redirect>0</https_redirect>
      <httpsd_port>8443</httpsd_port>
    </interface>
  </interfaces>
  <dns>
    <local_dns>
      <dns_ip priority="0">192.168.2.25</dns_ip>
    </local_dns>
    <dns_ptr_timeout>10</dns_ptr_timeout>
    <dns_routing_table>0</dns_routing_table>
  </dns>

  <default_gateway>192.168.2.20</default_gateway>
  <routes>
  </routes>

  <ntp>
    <ntp_server>192.168.2.5</ntp_server>
    <ntp_routing_table>0</ntp_routing_table>
  </ntp>

  <timezone>America/Los_Angeles</timezone>
</config>

```

Tech Notes

- The Cisco WSA uses, as a default, the M1 Management port with an assigned IP address of 192.168.42.42. Instead of using the CLI to do any preconfiguration, you can connect directly to the WSA using your browser.
- The WSA supports SSH (server), so any SSH client can be used to connect to the CLI of the Cisco WSA, as in this example:

[Click here to view code image](#)

```
SW1# ssh -l admin 192.168.2.50
```

```
Password:
```

```
Last login: Fri Sep 6 03:37:18 2013 from 192.168.2.5
```

```
Copyright (c) 2001-2011, Cisco Systems, Inc.
```

```
AsyncOS 7.7.5 for Web build 190
```

```
Welcome to the Cisco IronPort S100V Web Security Virtual Appliance  
wsa.cisco.com>
```

This can be useful for bootstrapping the device or managing feature keys.

- The serial number of the WSA is critical when deriving feature keys for the device. The serial number, along with information on feature key lifetimes, can be located via the GUI: System Administration, Feature Keys, or at the beginning of the **showconfig** output via the CLI.

[Click here to view code image](#)

```
Product: Cisco IronPort S100V Web Security Virtual Appliance
```

```
Model Number: S100V
```

```
Version: 7.7.5-190
```

```
Serial Number: 422C60745C0DE7AB65E7-2179C1D5637F
```

```
Number of CPUs: 2
```

```
Memory (MB): 6144
```

```
Current Time: Fri Sep 6 04:08:00 2013
```

Solution and Verification for Exercise 2.3: Enable Web Content Features on the Cisco WSA

Skills Tested

- Enabling WCCP functionality between the Cisco WSA and ASA to provide transparent proxy support
- Configuring proxy bypass lists
- Creating and applying custom URL categories

Solution and Verification

This exercise builds upon the basic configuration of the Cisco WSA in [Exercise 2.2](#).

Configuring and customizing how the WSA will process HTTP and HTTPS requests transparently proxied by the Cisco ASA is fundamental, yet very important. It enables the administrator to control how access requests are processed both for security and efficiency purposes.

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**
- Variable syntax appears in **green**

Task 1: Configure WCCPv2 Proxy Support on the Cisco WSA (Client) and the Cisco ASA (Server)

Verify connectivity between the WSA (WCCP client) and ASA (WCCP server). The router-ID on the ASA will be the highest IP address configured on the device (within the ASA context), and it is used to form a GRE tunnel with the WSA.

[Click here to view code image](#)

```
ASA1# changeto context c1
```

```
ASA1/c1(config)# show wccp
```

Global WCCP information:

Router information:

```
Router Identifier:      192.168.2.20
Protocol Version:      2.0
```

Service Identifier: 90

```
Number of Cache Engines:      1
Number of routers:            1
Total Packets Redirected:      201578
Redirect access-list:          WCCPRedirectionList -> name must
                                match list below
```

```
Total Connections Denied Redirect: 0
Total Packets Unassigned:        0
Group access-list:               wccpservers -> name must match list
                                below
```

```
Total Messages Denied to Group: 0
Total Authentication failures:    0
Total Bypassed Packets Received: 0
```

To ensure that the GRE tunnel has been established between the WCCP client and server, debugs on the ASA can be enabled that should show the periodic liveness check. The WCCP server is responsible for redirection of interesting traffic to the client. The clients will then apply configured service policy criteria on the assigned traffic.

[Click here to view code image](#)

```
ASA1/c1# debug wccp packet
```

```
WCCP-PKT:D90: Received valid Here_I_Am packet from 192.168.2.50 w/rcv_id 00000213
```

```
WCCP-PKT:D90: Sending I_See_You packet to 192.168.2.50 w/ rcv_id 00000214
```

Verify whether the redirection criteria are correctly configured:

[Click here to view code image](#)

```
ASA1/c1# show access-list
```

access-list WCCPRedirectionList line 1 extended permit tcp any any eq www
access-list WCCPRedirectionList line 2 extended permit tcp any any eq https
access-list wccpservers line 1 extended permit ip host 192.168.2.50 any

From the web browser, connect to http://10.50.40.7 and verify the output on R7. If the configuration is correct, the HTTP connection source address will be that of the WSA.

[Click here to view code image](#)

R7# show ip http server history

! note this must be completed after attempting a connection from a browser otherwise the history may be blank.

HTTP server history:

local-ipaddress:port remote-ipaddress:port in-bytes out-bytes

10.50.40.7:80	192.168.2.50:4507	332	192	17:21:11	04/07
10.50.40.7:80	192.168.2.50:49622	375	192	17:21:23	04/07
10.50.40.7:80	192.168.2.50:24928	379	192	17:21:37	04/07
10.50.40.7:80	192.168.2.50:39850	375	2077	17:21:45	04/07

Task 2: Configure Proxy Bypass on the Cisco WSA

From the web browser, connect to http://10.50.80.6 then verify the output on R6. This will test the proxy bypass list and should show the HTTP connection coming from the actual source address of the client browser device, not the WSA.

[Click here to view code image](#)

R6# show ip http server history

! note this must be completed after attempting a connection from a browser otherwise the history may be blank.

HTTP server history:

local-ipaddress:port remote-ipaddress:port in-bytes out-bytes

10.50.80.6:80	192.168.2.25:63596	256	192	20:12:15	09/06
10.50.80.6:80	192.168.2.25:63597	295	1986	20:12:23	09/06
10.50.80.6:80	192.168.2.25:63598	248	137	20:12:23	09/06

Task 3: Create a Custom URL Access Policy on the Cisco WSA

From the web browser, connect to http://10.50.30.3. The connection should be denied and an error page generated by the WSA displayed:

This Page Cannot Be Displayed

Configuration

[Click here to view code image](#)

! ASA1/c1

wccp 90 redirect-list WCCPRedirectionList group-list wccpservers

wccp interface inside 90 redirect in

```
access-list WCCPRedirectionList extended permit tcp any any eq www
```

```
access-list WCCPRedirectionList extended permit tcp any any eq https
```

```
access-list wccpservers extended permit ip host 192.168.2.50 any
```

Tech Notes

WCCP Support Across Cisco Products

WCCP support and functionality varies between WCCP server types. At the time of this writing, the ASA has the following capabilities:

- Redirection of multiple TCP and UDP port-destined traffic
- Unicast WCCP via UDP/2048
- Authentication for cache engines in a service group
- Multiple cache engines in a service group
- GRE encapsulation for traffic redirection

The following WCCPv2 features are not supported for the ASA but are supported on Cisco Catalyst switches and ISR routers:

- Multiple routers in a service group
- Multicast WCCP
- Layer 2 for traffic redirection
- WCCP source address spoofing

Transparent Proxy Versus Explicit Proxy

Using WCCP as the proxy mechanism is known as *transparent proxy* because the client browser settings do not have to be modified for connections to be forwarded to the WSA. The WCCP server intercepts the request and forwards it to the WSA to be proxied. DNS resolution of websites is done by the client device.

Explicit proxy requires the client browser to connect to the WSA. The WSA uses DNS to resolve the website and then connects to that site.

Connection Assignment and Redirection

Two of the more advanced WCCP concepts are those of assignment and redirection.

Assignment refers to the method by which traffic is distributed to the WSA, and it is more relevant when multiple WSAs are sharing the load within a service group.

Two assignment methods exist, both of which track the source and destination IP addresses plus source and destination ports. An algorithm is used that assigns the result to a specific “bucket.” These buckets are distributed among the WSAs within a specific service group. The assignment algorithms are

- **Hash-Based Assignment:** Uses a software-based hash algorithm to determine which WCCP appliance receives traffic. In hardware-based platforms, the Netflow table is used to apply hardware assistance. It consists of a byte-level (8-bit) XOR computation divided into 256

buckets.

- **Mask-Based Assignment:** Uses the ACL Ternary Content-Addressable Memory (TCAM) to assign WCCP entities. This method is fully handled by hardware and consists of a bit-level AND divided into 128 buckets (7 bits).

The Cisco ASA uses hash-based assignment to assign a connection to a specific bucket. The following command on the ASA illustrates how hash-based assignment is done:

[Click here to view code image](#)

```
ASA1/c1# show wccp 90 hash 10.50.70.6 192.168.2.25 80 1024
```

WCCP hash information for:

Primary Hash: Dst IP: 10.50.70.6

Bucket: 120

Cache Engine: 192.168.2.50

Because there is support for only one WSA per service group, all 256 buckets are assigned to the same WSA:

[Click here to view code image](#)

```
ASA1/c1(config)# show wccp 90 buckets
```

WCCP hash bucket assignments:

Index Cache Engine:

00 192.168.2.50

FF NOT ASSIGNED

```
XX| 0 1 2 3 4 5 6 7 8 9 A B C D E F
```

```
--|-----
```

```
00| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
10| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
20| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
30| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
40| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Traffic is forwarded to a WSA using either the GRE (IP encaps) or L2 (MAC rewrite).

When determining the most efficient WSA deployment, the following performance guidelines are useful:

- MASK (HW) > HASH (SW). HW must take TCAM resources into consideration.
- L2 (HW) > GRE (SW).
- Use GRE if WSA is located in another subnet. Check whether the device can do GRE in HW.
- Use L2 if WSA and WCCP device are in the same subnet. ASA is the exception and must use GRE.

Service Groups

An assignment method and a forwarding method are defined per service group. Traffic service types and traffic-handling requirements are also configured within the service group. Types of traffic service include support for standard “well-known” (default port 80) traffic or for dynamic services (which support other non-HTTP protocols). Traffic-handling options allow for functions such as IP address spoofing, where the original source address of the client requester is used, although the return traffic from the server will be forwarded back to the WSA by the WCCP server.

[Figure 1a-2](#) illustrates WCCP configuration options on the WCCP client (WSA) for creating service groups that handle traffic of interest redirected from the WCCP server.

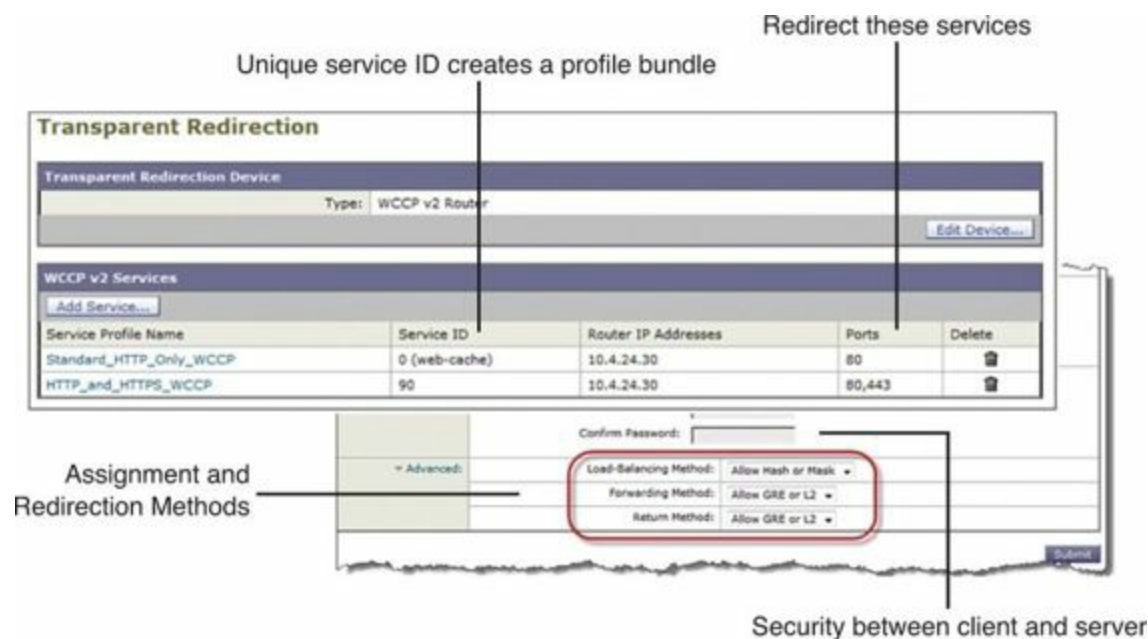


Figure 1a-2 WSA WCCP Configuration Parameters

Section 3: Secure Access

The exercises in this section cover fundamental ways to secure network access via wired and wireless methods. Legacy remote access VPNs via Easy Virtual Private Networks (EZVPN) using IKEv1 can be built between various client and server platforms—in this case, the Cisco ASA will be the server and the Cisco IOS router takes on the role of client. DMVPN has evolved over phase 1, 2, and now phase 3, which is covered here. The Cisco IOS-based Certificate Authority (CA) server exercise must be completed and will be used in other exercises in this guide. Wireless security is an increasingly important topic, and we start with some basic security access methods that will be expanded upon in other lab exercises.

Solution and Verification for Exercise 3.1: Configure and Troubleshoot IPsec EZVPN

Skills Tested

- Configuration of the EZVPN remote access IPsec VPN solution between the Cisco ASA as the server and Cisco IOS Router as the client
- Troubleshoot EZVPN, demonstrating a good understanding of more advanced deployment options

Solution and Verification

The EZVPN solution is a legacy remote access IPsec VPN that uses the client/server model. In this case, the server is the Cisco ASA and the client is a Cisco IOS router. IKEv1 is used as the key management protocol, and all IKE and IPsec policies are dictated by the server. The client does not need predefined IKE or IPsec policies because, as the initiator of the EZVPN tunnel, it will propose multiple protection suites, one of which must match the policies configured on the server.

Several requirements of this question must be configured correctly:

- Tunnel only traffic specified by the split tunnel list on the EZVPN server.
- The VPN tunnel is initiated from R3 only by interesting traffic from access-list ezvpn-acl, which is predefined.
- Traffic is flowing into the DMZ interface of ASA2 from R3 and then back out of the DMZ interface to R4. This flow requires the use of static routes to direct the encrypted traffic to ASA2; otherwise, R3 could communicate directly with R4. This type of traffic flow is known as Client U-turn.
- XAUTH must be fully automated with no user intervention required, from both the initial connection and across rekeys. To prevent the need for user intervention upon the initial XAUTH phase, a username/password must be configured on the client side. To prevent the client from being reprompted during subsequent IKE rekeys, the server must push the save-password mode config attribute to the client.
- The output of **show crypto ipsec client ezvpn** shows that an IP address has been pushed to the client via mode config. This is in addition to the IPsec selector using the IP address of R3 interface Loopback1 as a source address. This implies that the mode of operation required in this question is network extension plus.

For this exercise, the configuration for the EZVPN client on R3 must be built from scratch and use the predefined ACL ezvpn-acl. The configuration on ASA2 as the EZVPN server must be completed by troubleshooting the solution.

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**
- Nonzero/non-null syntax appears in **violet**
- Variable syntax appears in **green**

To verify the configuration, a ping is required to trigger the EZVPN tunnel establishment. The format of the ping is important because it must match the ACL that defines interesting traffic for purposes of starting EZVPN client. Note that the source of the ping is Loopback1. When the tunnel is ACTIVE, the **show** command outputs that follow will provide solution verification:

[Click here to view code image](#)

```
R3# ping 10.4.4.4 so lo1
```

```
R3# show crypto session detail  
Crypto session current status
```

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Ethernet0/1

Uptime: 00:04:20

Session status: UP-ACTIVE

Peer: 10.50.30.20 port 500 fvrf: (none) ivrf: (none)

Phase1_id: 10.50.30.20

Desc: (none)

IKEv1 SA: local 10.50.30.3/500 remote 10.50.30.20/500 Active

Capabilities: CX connid:1053 lifetime:23:54:51

IPSEC FLOW: permit ip 10.3.3.0/255.255.255.0 10.4.4.0/255.255.255.0

Active SAs: 2, origin: crypto map

Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 4233369/28780

Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4233369/28780

IPSEC FLOW: permit ip host 172.16.1.100 10.4.4.0/255.255.255.0

Active SAs: 2, origin: crypto map

Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 4294332/28780

Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4294332/28780

ASA2# show crypto isakmp sa detail

IKEv1 SAs:

Active SA: 1

Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)

Total IKE SA: 1

1 IKE Peer: 10.50.30.3

Type : user Role : responder

Rekey : no State : AM_ACTIVE

Encrypt : 3des Hash : SHA

Auth : preshared Lifetime: 86400

Lifetime Remaining: 84766

R3# show crypto ipsec client ezvpn

Easy VPN Remote Phase: 8

Tunnel name : ez

Inside interface list: Loopback1

Outside interface: Ethernet0/1

Connect : ACL based with access-list ezvpn-acl

Current State: IPSEC_ACTIVE

Last Event: SOCKET_UP

Address: 172.16.1.100 (applied on Loopback10000)

Mask: 255.255.255.255

DNS Primary: 192.168.2.25

Default Domain: cisco.com

Save Password: Allowed

Current EzVPN Peer: 10.50.30.20

ASA2# show route

S 172.16.1.100 255.255.255.255 [1/0] via 10.50.30.3, dmz

R3# show crypto ipsec sa

....

interface: Ethernet0/1

Crypto map tag: Ethernet0/1-head-0, local addr 10.50.30.3

protected vrf: (none)

local ident (addr/mask/prot/port): (10.3.3.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (10.4.4.0/255.255.255.0/0/0)

current_peer 10.50.30.20 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0

#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.50.30.3, remote crypto endpt.: 10.50.30.20

path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/1

current outbound spi: 0x866878B7(2254993591)

PFS (Y/N): Y, DH group: none

inbound esp sas:

spi: 0xE2663A09(3798350345)

transform: esp-3des esp-sha-hmac ,

in use settings = {Tunnel, }

conn id: 523, flow_id: SW:523, sibling_flags 80000040, crypto map:

Ethernet0/1-head-0

sa timing: remaining key lifetime (k/sec): (4233369/27337)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x866878B7(2254993591)

transform: esp-3des esp-sha-hmac ,

in use settings = {Tunnel, }

conn id: 524, flow_id: SW:524, sibling_flags 80000040, crypto map:
Ethernet0/1-head-0

sa timing: remaining key lifetime (k/sec): (4233369/27337)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

protected vrf: (none)

local ident (addr/mask/prot/port): (172.16.1.100/255.255.255.255/0/0)

remote ident (addr/mask/prot/port): (10.4.4.0/255.255.255.0/0/0)

current_peer 10.50.30.20 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0

#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.50.30.3, remote crypto endpt.: 10.50.30.20

path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/1

current outbound spi: 0x76CA9731(1992988465)

PFS (Y/N): Y, DH group: none

inbound esp sas:

spi: 0x28BC5612(683431442)

transform: esp-3des esp-sha-hmac ,

in use settings = {Tunnel, }

conn id: 525, flow_id: SW:525, sibling_flags 80000040, crypto map:
Ethernet0/1-head-0

sa timing: remaining key lifetime (k/sec): (4294332/27337)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x76CA9731(1992988465)

transform: esp-3des esp-sha-hmac ,

in use settings = {Tunnel, }

conn id: 526, flow_id: SW:526, sibling_flags 80000040, crypto map:
Ethernet0/1-head-0

sa timing: remaining key lifetime (k/sec): (4294332/27337)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

Configuration

Syntax highlighted in **cyan** needs to be added or modified.

R3

[Click here to view code image](#)

```
crypto ipsec client ezvpn ez
connect acl ezvpn-acl
group ezvpn key cisco
mode network-plus
peer 10.50.30.20
username cisco password cisco
xauth userid mode local
!
!
interface Loopback1
ip address 10.3.3.3 255.255.255.0
crypto ipsec client ezvpn ez inside

interface Ethernet0/1
ip address 10.50.30.3 255.255.255.0
crypto ipsec client ezvpn ez

ip route 10.4.4.0 255.255.255.0 10.50.30.20
!
```



```
ip access-list extended ezvpn-acl
 permit ip 10.3.3.0 0.0.0.255 10.4.4.0 0.0.0.255
!
```

ASA2

[Click here to view code image](#)

```
username cisco password cisco
same-security-traffic permit intra-interface
access-list split-tunnel permit 10.4.4.0 255.255.255.0
ip local pool vpnpool 172.16.1.100-172.16.1.199 mask 255.255.255.0
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set ESP-3DES-SHA
crypto map outside_map 10 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface dmz
crypto ikev1 enable dmz
crypto ikev1 policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
group-policy ezvpn1 internal
group-policy ezvpn1 attributes
 dns-server value 192.168.2.25
 vpn-tunnel-protocol ikev1
password-storage enable
default-domain value cisco.com
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split-tunnel
user-authentication disable

tunnel-group ezvpn type remote-access
tunnel-group ezvpn general-attributes
 address-pool vpnpool
 default-group-policy ezvpn1
tunnel-group ezvpn ipsec-attributes
ikev1 pre-shared-key cisco
```

Tech Notes

Initiating the EZVPN Tunnel

This exercise uses the concept of interesting traffic as defined in an access list to initiate the EZVPN connection to the server. This is known as *traffic-triggered* tunnel initiation. This allows for an automated, yet controlled, tunnel establishment. The other tunnel start modes are auto, which will initiate as soon as the **crypto ipsec client ezvpn name** is applied to the tunnel endpoint interface, and manual mode, which requires user intervention.

Split Tunnel Options

Defining a split tunnel ACL on the Cisco ASA server is not enough to implement the feature. How the split tunnel list is to be applied must also be included under the group policy:

[Click here to view code image](#)

split-tunnel-policy commands/options:

excludespecified Exclude only networks specified by
split-tunnel-network-list

tunnelall Tunnel everything

tunnelspecified Tunnel only networks specified by split-tunnel
network-list

EZVPN Client Modes of Operation in Cisco IOS

Client mode specifies that Network or Port Address Translation (NAT or PAT) be done so that the PCs and other hosts at the remote end of the VPN tunnel form a private network that does not use any IP addresses in the IP address space of the destination server. The server pushes down an IP address to the EZVPN client, and all traffic from the client will be internally translated to this address before being encrypted to the EZVPN server.

Network Extension mode specifies that the PCs and other hosts at the client end of the VPN tunnel should be using IP addresses that are fully routable and reachable by the destination network over the tunneled network so that they form one logical network.

Network Extension Plus mode is identical to Network Extension mode with the additional capability of being able to request an IP address through Mode-Config and automatically assign it to an available loopback interface. This can typically be used for management purposes.

Client U-Turn Versus IPsec Hairpinning

This question uses the concept of Client U-Turn, which requires the configuration of **same-security-traffic permit intra-interface** to enable traffic to enter and leave ASA2 via the same interface. Traffic between R3 and ASA2 is encrypted, whereas traffic between ASA and R4 is in the clear. If the traffic flows from R3 to ASA2 and ASA2 to R4 were encrypted, and R3 and R4 needed to communicate securely, this is known as *IPsec hairpinning*. This is analogous to a spoke-to-spoke VPN using a hub-and-spoke model.

External Versus Internal Policy

This exercise uses internal or local authorization and authentication. If policy storage on an external server—for example, a RADIUS server—is required, the following command syntax applies to the Cisco ASA:

[Click here to view code image](#)

```
group-policy group_policy_name type server-group server_group_name  
password server_password
```

On the ASA, *server group names* refer to usernames on the RADIUS server. If you configure external policy and use group-X as the server group name on the ASA, the RADIUS server sees the query as an authentication request for user-X. If external group attributes exist in the same RADIUS server as the users that require authentication, there must be no name duplication between them. The server group name is passed as the RADIUS username as follows:

```
RADIUS: User-Name      [1] 14 "group-X"
```

```
RADIUS: User-Password [2] 18 *
```

Solution and Verification for Exercise 3.2: Troubleshoot DMVPN Phase 3: DMVPNv3

Skills Tested

- An understanding of the DMVPN solution; specifically, Phase 3 (that is, DMVPNv3)
- Integrating DMVPN with other elements of the network topology

Solution and Verification

This exercise tests both configuration and troubleshooting skills for a VPN solution comprised of many working parts implemented on a complex topology where the path between hub and spokes transits several other network elements. The solution must also be based on DMVPN phase 3, which differs from phases 1 and 2 with its use of Next-Hop Resolution Protocol (NHRP) redirects and shortcuts.

DMVPNv3 is comprised of several components, and the verification of each is critical to troubleshooting the overall solution:

- NHRP and GRE
- Dynamic routing across the tunnel
- IKE and IPsec (this can be configured following the verification of the previous two components)

There might be other issues within the overall network topology that might need to be corrected to complete this exercise:

- The ASAs must permit IKE and IPsec to transit.
- The network object NAT configuration from [Exercise 1.3](#) on ASA1 changes the HUB's IP address from the perspective of the spokes.
- The object NAT on ASA1 also means that NAT transparency is required. The IKE negotiation

will float to UDP/4500, and UDP-encaps will be used for the secure transport of the data.

The following series of debug outputs help to outline the interactions of the protocols and features that together make up DMVPN. These narrated outputs show the administrator how to break down the task of troubleshooting by mapping configuration commands to debug events.

Useful debug commands include the following:

- **debug crypto isakmp**
- **debug crypto ipsec**
- **debug nhrp**

NHRP Spoke Registration

NHRP registration process from R4 (spoke) to R5 (hub):

[Click here to view code image](#)

! Determine NHRP server address according to static mapping on R4 tunnel interface

```
nhrp map 172.17.70.5 10.50.80.50
```

```
NHRP: Attempting to send packet via DEST 172.17.70.5
```

```
NHRP: Setting 'used' flag on cache entry with nhop: 172.17.70.5
```

```
NHRP: NHRP successfully mapped '172.17.70.5' to NBMA '10.50.80.50'
```

```
NHRP: Encapsulation succeeded. Sending NHRP Control Packet NBMA Address:  
10.50.80.50
```

! IPsec profile applied to tunnel interface will trigger IKE negotiation using
tunnel source and destination of NHRP server
interface Tunnel1

```
ip address 172.17.70.4 255.255.255.0
```

```
tunnel protection ipsec profile DMVPN
```

```
NHRP: Send Registration Request via Tunnel1 vrf 0, packet size: 105
```

```
src: 172.17.70.4, dst: 172.17.70.5
```

```
NHRP: 133 bytes out Tunnel1
```

```
IPSEC(sa_request): ,
```

```
(key eng. msg.) OUTBOUND local= 10.50.30.4:500, remote= 10.50.80.50:500,
```

```
local_proxy= 10.50.30.4/255.255.255.255/47/0,
```

```
remote_proxy= 10.50.80.50/255.255.255.255/47/0,
```

```
protocol= ESP, transform= esp-3des esp-md5-hmac (Transport),
```

```
lifedur= 3600s and 4608000kb,
```

```
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
```

! The requirement for IPsec protection triggers an IKE negotiation between R4 and
R5. Note that the translated address for R5 is used based on Q1.2 ASA NAT task

```
crypto isakmp policy 1
```

```
encr 3des
```

```
authentication pre-share
```

```
group 2
```

```
crypto isakmp key cisco address 10.50.80.5
```

```
ISAKMP: Created a peer struct for 10.50.80.50, peer port 500
```

```
ISAKMP:(0): beginning Main Mode exchange
```

ISAKMP:(0): sending packet to 10.50.80.50 my_port 500 peer_port 500 (I) MM_NO_STATE
ISAKMP:(0):Sending an IKE IPv4 Packet.
ISAKMP (0): received packet from 10.50.80.50 dport 500 sport 500 Global (I) MM_NO_STATE
ISAKMP:(0): processing SA payload. message ID = 0
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0):found peer pre-shared key matching 10.50.80.50
ISAKMP:(0): local preshared key found
ISAKMP : Scanning profiles for xauth ... ipv6
ISAKMP:(0):Checking ISAKMP transform 1 against priority 1 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP:(0): sending packet to 10.50.80.50 my_port 500 peer_port 500 (I) MM_SA_SETUP
ISAKMP:(0):Sending an IKE IPv4 Packet.
ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(0):Old State = IKE_I_MM2 New State = IKE_I_MM3

ISAKMP (0): received packet from 10.50.80.50 dport 500 sport 500 Global (I) MM_SA_SETUP
ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(0):Old State = IKE_I_MM3 New State = IKE_I_MM4

ISAKMP:(0): processing KE payload. message ID = 0
ISAKMP:(0): processing NONCE payload. message ID = 0
ISAKMP:(0):found peer pre-shared key matching 10.50.80.50
ISAKMP:(1056): processing vendor id payload
ISAKMP:(1056): vendor ID is Unity
ISAKMP:(1056): processing vendor id payload
ISAKMP:(1056): vendor ID is DPD
ISAKMP:(1056): processing vendor id payload
ISAKMP:(1056): speaking to another IOS box!
! NAT translation is occurring on the ASA in between R4 and R5. This is detected below:
ISAKMP:received payload type 20
ISAKMP (1056): His hash no match - this node outside NAT
ISAKMP:received payload type 20
ISAKMP (1056): His hash no match - this node outside NAT

ISAKMP:(1056):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1056):Old State = IKE_I_MM4 New State = IKE_I_MM4

ISAKMP:(1056):Send initial contact

ISAKMP:(1056):SA is doing pre-shared key authentication using id type ID_IPV4_ADDR

ISAKMP (1056): ID payload

next-payload : 8
type : 1
address : 10.50.30.4
protocol : 17
port : 0
length : 12

ISAKMP:(1056):Total payload length: 12

ISAKMP:(1056): sending packet to 10.50.80.50 my_port 4500 peer_port 4500 (I) MM_KEY_EXCH

ISAKMP:(1056):Sending an IKE IPv4 Packet.

ISAKMP:(1056):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE

ISAKMP:(1056):Old State = IKE_I_MM4 New State = IKE_I_MM5

! NAT-T detected, IKE floats from UDP/500 to UDP/4500. The IKE ID payload will include the real IP address of R5. If an ISAKMP profile was being referenced, the match identity statement would use the real ID value if indexed by IP address.

ISAKMP (1056): received packet from 10.50.80.50 dport 4500 sport 4500 Global (I) MM_KEY_EXCH

ISAKMP:(1056): processing ID payload. message ID = 0

ISAKMP (1056): ID payload

next-payload : 8
type : 1
address : 10.50.90.5
protocol : 17
port : 0
length : 12

ISAKMP:(0):: peer matches *none* of the profiles

ISAKMP:(1056): processing HASH payload. message ID = 0

ISAKMP:(1056):SA authentication status:

authenticated

ISAKMP:(1056):SA has been authenticated with 10.50.80.50

ISAKMP: Trying to insert a peer 10.50.30.4/10.50.80.50/4500/, and inserted successfully F20ED770.

! IPsec SA negotiation follows. Notice the use of UDP-encaps due to NAT-T. Tunnel mode GRE is configured which is reflected in IP protocol 47 as part of the traffic selector.

crypto ipsec transform-set dmvpn esp-3des esp-md5-hmac
mode transport

!

crypto ipsec profile DMVPN
set transform-set dmvpn

```
!  
interface Tunnel1  
  tunnel mode gre multipoint  
ISAKMP (1056): received packet from 10.50.80.50 dport 4500 sport 4500 Global (I)  
  QM_IDLE  
ISAKMP:(1056): processing HASH payload. message ID = 1543261932  
ISAKMP:(1056): processing SA payload. message ID = 1543261932  
ISAKMP (1056): processing NAT-OAi payload. addr = 10.50.30.4, message ID =  
  1543261932  
ISAKMP (1056): processing NAT-OAr payload. addr = 10.50.90.5, message ID =  
  1543261932  
ISAKMP:(1056):Checking IPsec proposal 1  
ISAKMP: transform 1, ESP_3DES  
ISAKMP:  attributes in transform:  
ISAKMP:  encaps is 4 (Transport-UDP)  
ISAKMP:  SA life type in seconds  
ISAKMP:  SA life duration (basic) of 3600  
ISAKMP:  SA life type in kilobytes  
ISAKMP:  SA life duration (VPI) of 0x0 0x46 0x50 0x0  
ISAKMP:  authenticator is HMAC-MD5  
ISAKMP:(1056):atts are acceptable.  
IPSEC(validate_proposal_request): proposal part #1  
IPSEC(validate_proposal_request): proposal part #1,  
  (key eng. msg.) INBOUND local= 10.50.30.4:0, remote= 10.50.80.50:0,  
  local_proxy= 10.50.30.4/255.255.255.255/47/0,  
  remote_proxy= 10.50.80.50/255.255.255.255/47/0,  
  protocol= ESP, transform= NONE (Transport-UDP),  
  lifedur= 0s and 0kb,  
  spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0  
IPSEC(key_engine): got a queue event with 1 KMI message(s)  
map_db_find_best did not find matching map  
Crypto mapdb : proxy_match  
  src addr   : 10.50.30.4  
  dst addr   : 10.50.80.50  
  protocol   : 47  
  src port   : 0  
  dst port   : 0  
IPSEC(crypto_ipsec_create_ipsec_sas): Map found Tunnel1-head-0  
IPSEC(create_sa): sa created,  
  (sa) sa_dest= 10.50.30.4, sa_proto= 50,  
  sa_spi= 0xED27ED07(3978816775),  
  sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 519  
  sa_lifetime(k/sec)= (4608000/3600)  
IPSEC(create_sa): sa created,  
  (sa) sa_dest= 10.50.80.50, sa_proto= 50,
```

```
sa_spi= 0x2CEB926C(753635948),  
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 520  
sa_lifetime(k/sec)= (4608000/3600)
```

! NHRP registration now occurs under the protection of the IPsec SA.

NHRP: Setting retrans delay to 1 for nhs dst 172.17.70.5

NHRP-ATTR: Requester Ext Len: Total ext_len with NHRP attribute VPE 53

NHRP: Attempting to send packet via DEST 172.17.70.5

NHRP: Setting 'used' flag on cache entry with nhop: 172.17.70.5

NHRP: NHRP successfully mapped '172.17.70.5' to NBMA '10.50.80.50'

NHRP: Encapsulation succeeded. Sending NHRP Control Packet NBMA Address:
10.50.80.50

NHRP: Send Registration Request via Tunnel1 vrf 0, packet size: 105
src: 172.17.70.4, dst: 172.17.70.5

NHRP: 133 bytes out Tunnel1

NHRP: Receive Registration Reply via Tunnel1 vrf 0, packet size: 125

NHRP: netid_in = 0, to_us = 1

**NHRP: NHS 172.17.70.5 Tunnel1 vrf 0 Cluster 0 Priority 0 Transitioned to 'RE'
from 'E'**

NHRP: NHS-UP: 172.17.70.5

Spoke-to-Spoke Connection from R4 to R3

[Click here to view code image](#)

! A PING is used to trigger the connection between spokes, this address is the lo0 interface on R3.

```
R4# ping 172.16.33.3
```

! R4 does not have a mapping to route "owned" by R3 so a resolution request will be sent to R5 (NHRP server) first

NHRP: Setting 'used' flag on cache entry with nhop: 172.17.70.5

NHRP: NHRP successfully mapped '172.17.70.5' to NBMA '10.50.80.50'

NHRP: Enqueued NHRP Resolution Request for destination: 172.16.33.3

NHRP: Checking for delayed event NULL/172.16.33.3 on list (Tunnel1).

NHRP: No node found.

NHRP: Enqueued NHRP Resolution Request for destination: 172.16.33.3

NHRP: Setting 'used' flag on cache entry with nhop: 172.17.70.5

NHRP: NHRP successfully mapped '172.17.70.5' to NBMA '10.50.80.50'

NHRP: Setting 'used' flag on cache entry with nhop: 172.17.70.5

NHRP: NHRP successfully mapped '172.17.70.5' to NBMA '10.50.80.50'

NHRP: Checking for delayed event NULL/172.16.33.3 on list (Tunnel1).

NHRP: No node found.

NHRP-ATTR: Requester Ext Len: Total ext_len with NHRP attribute VPE 33

NHRP: Sending NHRP Resolution Request for dest: 172.16.33.3 to nexthop:

172.17.70.5 using our src: 172.17.70.4
NHRP: Receive Resolution Request via Tunnel1 vrf 0, packet size: 105
NHRP: netid_in = 70, to_us = 1
NHRP: nhrp_rtlookup for destination on 172.17.70.4 yielded interface Tunnel1,
prefixlen 24
NHRP: nhrp_rtlookup on 172.17.70.4 yielded interface Tunnel1, prefixlen 24
NHRP: Request was to us, responding with our address
NHRP: Checking for delayed event 172.17.70.3/172.17.70.4 on list (Tunnel1).
! Target device is R3 which is using 10.50.30.3, IPsec SAs required
NHRP: >>> nhrp_need_to_delay: ENQUEUED Delaying resolution request nbma
src:10.50.30.4 nbma dst:10.50.30.3 reason:IPSEC-IFC: need to wait for IPsec SAs.
NHRP-ATTR: In nhrp_cache_pak LINE: 1391
! First negotiate IKE SA between R3 and R4
ISAKMP:(0): SA request profile is (NULL)
ISAKMP: Created a peer struct for 10.50.30.3, peer port 500
ISAKMP: New peer created peer = 0xF06A2908 peer_handle = 0x80000017
ISAKMP: Locking peer struct 0xF06A2908, refcount 1 for isakmp_initiator
ISAKMP: local port 500, remote port 500
ISAKMP: set new node 0 to QM_IDLE
ISAKMP:(0):insert sa successfully sa = F227B4C8
ISAKMP:(0): processing SA payload. message ID = 0
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0):found peer pre-shared key matching 10.50.30.3
ISAKMP:(0): local preshared key found
ISAKMP : Scanning profiles for xauth ... ipv6
ISAKMP:(0):Checking ISAKMP transform 1 against priority 1 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP:(0):atts are acceptable. Next payload is 0
ISAKMP:(0):Acceptable atts:actual life: 0
ISAKMP:(0):Acceptable atts:life: 0
ISAKMP:(0):Fill atts in sa vpi_length:4
ISAKMP:(0):Fill atts in sa life_in_seconds:86400
ISAKMP:(0):Returning Actual lifetime: 86400
ISAKMP:(0)::Started lifetime timer: 86400.

ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947

ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(0):Old State = IKE_I_MM2 New State = IKE_I_MM2

ISAKMP:(0): sending packet to 10.50.30.3 my_port 500 peer_port 500 (I) MM_SA_SETUP
ISAKMP:(0):Sending an IKE IPv4 Packet.
ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(0):Old State = IKE_I_MM2 New State = IKE_I_MM3

ISAKMP (0): received packet from 10.50.30.3 dport 500 sport 500 Global (N) NEW SA
ISAKMP: Created a peer struct for 10.50.30.3, peer port 500
ISAKMP: New peer created peer = 0xF1EBFC00 peer_handle = 0x80000012
ISAKMP: Locking peer struct 0xF1EBFC00, refcount 1 for crypto_isakmp_process_block
ISAKMP: local port 500, remote port 500
ISAKMP:(0):insert sa successfully sa = F2232F30
ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(0):Old State = IKE_READY New State = IKE_R_MM1
ISAKMP:(0): processing SA payload. message ID = 0
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
ISAKMP (0): vendor ID is NAT-T v7
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 157 mismatch
ISAKMP:(0): vendor ID is NAT-T v3
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 123 mismatch
ISAKMP:(0): vendor ID is NAT-T v2
ISAKMP:(0):found peer pre-shared key matching 10.50.30.3
ISAKMP:(0): local preshared key found
ISAKMP : Scanning profiles for xauth ... ipv6
ISAKMP:(0):Checking ISAKMP transform 1 against priority 1 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP:(0):atts are acceptable. Next payload is 0
ISAKMP:(0):Acceptable atts:actual life: 0
ISAKMP:(0):Acceptable atts:life: 0
ISAKMP:(0):Fill atts in sa vpi_length:4
ISAKMP:(0):Fill atts in sa life_in_seconds:86400
ISAKMP:(0):Returning Actual lifetime: 86400

ISAKMP:(0)::Started lifetime timer: 86400.
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
ISAKMP (0): vendor ID is NAT-T v7
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 157 mismatch
ISAKMP:(0): vendor ID is NAT-T v3
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 123 mismatch
ISAKMP:(0): vendor ID is NAT-T v2
ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(0):Old State = IKE_R_MM1 New State = IKE_R_MM1

ISAKMP:(0): constructed NAT-T vendor-rfc3947 ID
ISAKMP:(0): sending packet to 10.50.30.3 my_port 500 peer_port 500 (R) MM_SA_SETUP
ISAKMP:(0):Sending an IKE IPv4 Packet.
ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(0):Old State = IKE_R_MM1 New State = IKE_R_MM2
ISAKMP (0): received packet from 10.50.30.3 dport 500 sport 500 Global (I)
MM_SA_SETUP
ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(0):Old State = IKE_I_MM3 New State = IKE_I_MM4
ISAKMP:(0): processing KE payload. message ID = 0
ISAKMP:(0): processing NONCE payload. message ID = 0
ISAKMP:(0):found peer pre-shared key matching 10.50.30.3
ISAKMP:(1057): processing vendor id payload
ISAKMP:(1057): vendor ID is Unity
ISAKMP:(1057): processing vendor id payload
ISAKMP:(1057): vendor ID is DPD
ISAKMP:(1057): processing vendor id payload
ISAKMP:(1057): speaking to another IOS box!
ISAKMP:received payload type 20
ISAKMP (1057): His hash no match - this node outside NAT
ISAKMP:received payload type 20
ISAKMP (1057): No NAT Found for self or peer
ISAKMP:(1057):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1057):Old State = IKE_I_MM4 New State = IKE_I_MM4
ISAKMP (1057): received packet from 10.50.30.3 dport 500 sport 500 Global (I)
MM_KEY_EXCH
ISAKMP:(1057): processing ID payload. message ID = 0
ISAKMP (1057): ID payload
next-payload : 8

type : 1
address : 10.50.30.3
protocol : 17
port : 500
length : 12

ISAKMP:(0):: peer matches *none* of the profiles

ISAKMP:(1057): processing HASH payload. message ID = 0

ISAKMP:(1057):SA authentication status:

authenticated

ISAKMP:(1057):SA has been authenticated with 10.50.30.3

ISAKMP: Trying to insert a peer 10.50.30.4/10.50.30.3/500/, and inserted successfully F06A2908.

ISAKMP:(1057):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH

ISAKMP:(1057):Old State = IKE_I_MM5 New State = IKE_I_MM6

ISAKMP:(1057):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE

ISAKMP:(1057):Old State = IKE_I_MM6 New State = IKE_I_MM6

ISAKMP:(1057):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE

ISAKMP:(1057):Old State = IKE_I_MM6 New State = IKE_P1_COMPLETE

ISAKMP:(1057):beginning Quick Mode exchange, M-ID of 129959729

ISAKMP:(1057):QM Initiator gets spi

ISAKMP:(1057): sending packet to 10.50.30.3 my_port 500 peer_port 500 (I) QM_IDLE

ISAKMP:(1057):Sending an IKE IPv4 Packet.

ISAKMP:(1057):Node 129959729, Input = IKE_MESG_INTERNAL, IKE_INIT_QM

ISAKMP:(1057):Old State = IKE_QM_READY New State = IKE_QM_I_QM1

ISAKMP:(1057):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE

ISAKMP:(1057):Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

ISAKMP (1057): received packet from 10.50.30.3 dport 500 sport 500 Global (I)
QM_IDLE

ISAKMP:(1057): processing HASH payload. message ID = 129959729

ISAKMP:(1057): processing SA payload. message ID = 129959729

ISAKMP:(1057):Checking IPsec proposal 1

ISAKMP: transform 1, ESP_3DES

ISAKMP: attributes in transform:

ISAKMP: encaps is 2 (Transport)

ISAKMP: SA life type in seconds

ISAKMP: SA life duration (basic) of 3600

ISAKMP: SA life type in kilobytes

ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0

ISAKMP: authenticator is HMAC-MD5

ISAKMP:(1057):atts are acceptable.

ISAKMP:(1057): processing NONCE payload. message ID = 129959729

ISAKMP:(1057): processing ID payload. message ID = 129959729

```
ISAKMP:(1057): processing ID payload. message ID = 129959729
ISAKMP:(1057): sending packet to 10.50.30.3 my_port 500 peer_port 500 (I) QM_IDLE
ISAKMP:(1057):Sending an IKE IPv4 Packet.
ISAKMP:(1057):deleting node 129959729 error FALSE reason "No Error"
ISAKMP:(1057):Node 129959729, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
ISAKMP:(1057):Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE
! Once IPsec SAs have been created, NHRP mappings are updated on R4 to R3
NHRP: Adding Tunnel Endpoints (VPN: 172.17.70.3, NBMA: 10.50.30.3)
NHRP: Successfully attached NHRP subblock for Tunnel Endpoints (VPN: 172.17.70.3,
NBMA: 10.50.30.3)
NHRP: Attempting to send packet via DEST 172.17.70.3
NHRP: Setting 'used' flag on cache entry with nhop: 172.17.70.3
NHRP: NHRP successfully mapped '172.17.70.3' to NBMA '10.50.30.3'
NHRP: Encapsulation succeeded. Sending NHRP Control Packet NBMA Address:
10.50.30.3
NHRP: Send Resolution Reply via Tunnel1 vrf 0, packet size: 133
src: 172.17.70.4, dst: 172.17.70.3
NHRP: 161 bytes out Tunnel1
R4# ping 172.16.33.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.33.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/7/9 ms
R4#
```

Verification

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**

Verify whether the IKE and IPsec sessions have been established. The following outputs show the crypto session status for spokes to hub. Note that the IKE port is UDP/4500, not UDP/500, due to the NAT translation for the HUB IP address on ASA1.

[Click here to view code image](#)

```
R4# show crypto session
Crypto session current status
```

```
Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 10.50.80.50 port 4500
IKEv1 SA: local 10.50.30.4/4500 remote 10.50.80.50/4500 Active
IPSEC FLOW: permit 47 host 10.50.30.4 host 10.50.80.50
Active SAs: 2, origin: crypto map
```

```
R3# show crypto session
```

Crypto session current status

Interface: Tunnel1

Session status: UP-ACTIVE

Peer: 10.50.80.50 port 4500

IKEv1 SA: local 10.50.30.3/4500 remote 10.50.80.50/4500 Active

IPSEC FLOW: permit 47 host 10.50.30.3 host 10.50.80.50

Active SAs: 2, origin: crypto map

After connectivity is established directly between spokes, the crypto session status will be as follows, with IKE SA on UDP/500:

[Click here to view code image](#)

```
R4# show crypto session
```

```
Crypto session current status
```

```
Interface: Tunnel1
```

```
Session status: UP-ACTIVE
```

```
Peer: 10.50.30.3 port 500
```

```
IKEv1 SA: local 10.50.30.4/500 remote 10.50.30.3/500 Active
```

```
IKEv1 SA: local 10.50.30.4/500 remote 10.50.30.3/500 Active
```

```
IPSEC FLOW: permit 47 host 10.50.30.4 host 10.50.30.3
```

```
Active SAs: 4, origin: crypto map
```

The output of **show crypto ipsec sa** should show UDP-encaps due to the negotiation of NAT-T for spoke-to-hub. Spoke-to-spoke communication will use ESP without UDP-encaps.

[Click here to view code image](#)

```
R3# show crypto ipsec sa
```

```
interface: Tunnel1
```

```
  Crypto map tag: Tunnel1-head-0, local addr 10.50.30.3
```

```
protected vrf: (none)
```

```
local ident (addr/mask/prot/port): (10.50.30.3/255.255.255.255/47/0)
```

```
remote ident (addr/mask/prot/port): (10.50.80.50/255.255.255.255/47/0)
```

```
current_peer 10.50.80.50 port 4500
```

```
  PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 268072, #pkts encrypt: 268072, #pkts digest: 268072
```

```
#pkts decaps: 267087, #pkts decrypt: 267087, #pkts verify: 267087
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 10.50.30.3, remote crypto endpt.: 10.50.80.50
```

path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/1
current outbound spi: 0xACAB4234(2896904756)
PFS (Y/N): Y, DH group: none

inbound esp sas:

spi: 0xCDACB829(3450648617)
transform: esp-3des esp-md5-hmac ,
in use settings = {Transport UDP-Encaps, }
conn id: 727, flow_id: SW:727, sibling_flags 80000000, crypto map:
Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4246746/2900)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0xACAB4234(2896904756)
transform: esp-3des esp-md5-hmac ,
in use settings = {Transport UDP-Encaps, }
conn id: 728, flow_id: SW:728, sibling_flags 80000000, crypto map:
Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4246765/2900)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas

The routing tables on the spokes after *initial NHRP registration* will point to the HUB as the next hop for any *other* spoke routes:

[Click here to view code image](#)

R3# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 10.50.30.20 to network 0.0.0.0

```
O*E2 0.0.0.0/0 [110/1] via 10.50.30.20, 5d18h, Ethernet0/1
    10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C    10.3.3.0/24 is directly connected, Loopback1
L    10.3.3.3/32 is directly connected, Loopback1
S    10.4.4.0/24 [1/0] via 10.50.30.20
C    10.50.30.0/24 is directly connected, Ethernet0/1
L    10.50.30.3/32 is directly connected, Ethernet0/1
O E2  10.50.90.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
O E2  10.50.100.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
    172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C    172.16.33.0/24 is directly connected, Loopback0
L    172.16.33.3/32 is directly connected, Loopback0
D    172.16.34.0/24 [90/27264000] via 172.17.70.5, 00:00:37, Tunnel1
D    172.16.35.0/24 [90/27008000] via 172.17.70.5, 00:00:37, Tunnel1
    172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.17.70.0/24 is directly connected, Tunnel1
L    172.17.70.3/32 is directly connected, Tunnel1
O E2  192.168.2.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
```

To verify whether the NHRP enhancements associated with DMVPNv3 have been correctly configured, initiate a ping from R3 to R4. Note that, although the routing table on R3 still shows R5 (HUB) as the next hop to R4, there is a % besides the route, which indicates that the next hop has been overridden.

[Click here to view code image](#)

```
R3# ping 172.16.34.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.34.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/8/16 ms
R3# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override
```

Gateway of last resort is 10.50.30.20 to network 0.0.0.0

```
O*E2 0.0.0.0/0 [110/1] via 10.50.30.20, 5d18h, Ethernet0/1
```



```

10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C    10.3.3.0/24 is directly connected, Loopback1
L    10.3.3.3/32 is directly connected, Loopback1
S    10.4.4.0/24 [1/0] via 10.50.30.20
C    10.50.30.0/24 is directly connected, Ethernet0/1
L    10.50.30.3/32 is directly connected, Ethernet0/1
O E2  10.50.90.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
O E2  10.50.100.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
    172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C    172.16.33.0/24 is directly connected, Loopback0
L    172.16.33.3/32 is directly connected, Loopback0
D %   172.16.34.0/24 [90/27264000] via 172.17.70.5, 00:00:54, Tunnel1
D    172.16.35.0/24 [90/27008000] via 172.17.70.5, 00:00:54, Tunnel1
    172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.17.70.0/24 is directly connected, Tunnel1
L    172.17.70.3/32 is directly connected, Tunnel1
O E2  192.168.2.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1

```

The NHRP mapping for 172.16.34.0 is pointing to R4:

[Click here to view code image](#)

```

R3# show ip nhrp
172.16.34.0/24 via 172.17.70.4
    Tunnel1 created 00:01:20, expire 01:58:39
    Type: dynamic, Flags: router rib nho
    NBMA address: 10.50.30.4
172.17.70.3/32 via 172.17.70.3
    Tunnel1 created 00:01:20, expire 01:58:39
    Type: dynamic, Flags: router unique local
    NBMA address: 10.50.30.3
    (no-socket)
172.17.70.4/32 via 172.17.70.4
    Tunnel1 created 00:01:20, expire 01:58:39
    Type: dynamic, Flags: router implicit
    NBMA address: 10.50.30.4
172.17.70.5/32 via 172.17.70.5
    Tunnel1 created 1w6d, never expire
    Type: static, Flags: used
    NBMA address: 10.50.80.50

```

Now, verify R4 to R3. First, the routing table after initial NHRP registration:

[Click here to view code image](#)

```

R4# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

```

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, 1 - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 10.50.30.20 to network 0.0.0.0

```
O*E2 0.0.0.0/0 [110/1] via 10.50.30.20, 5d18h, Ethernet0/1
    10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
S    10.3.3.0/24 [1/0] via 10.50.30.20
C    10.4.4.0/24 is directly connected, Loopback1
L    10.4.4.4/32 is directly connected, Loopback1
C    10.50.30.0/24 is directly connected, Ethernet0/1
L    10.50.30.4/32 is directly connected, Ethernet0/1
O E2  10.50.90.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
O E2  10.50.100.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
    172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
D    172.16.33.0/24 [90/27264000] via 172.17.70.5, 00:05:38, Tunnel1
C    172.16.34.0/24 is directly connected, Loopback0
L    172.16.34.4/32 is directly connected, Loopback0
D    172.16.35.0/24 [90/27008000] via 172.17.70.5, 00:05:38, Tunnel1
    172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.17.70.0/24 is directly connected, Tunnel1
L    172.17.70.4/32 is directly connected, Tunnel1
O E2 192.168.2.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
```

Initiate a ping from R4 to R3. Note that, although the routing table on R4 still shows R5 (HUB) as the next hop to R3, there is a % besides the route, which indicates that the next hop has been overridden.

[Click here to view code image](#)

```
R4# ping 172.16.33.3
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.33.3, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/6/7 ms
```

```
R4# show ip route
```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 10.50.30.20 to network 0.0.0.0

```
O*E2 0.0.0.0/0 [110/1] via 10.50.30.20, 5d18h, Ethernet0/1
  10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
S    10.3.3.0/24 [1/0] via 10.50.30.20
C    10.4.4.0/24 is directly connected, Loopback1
L    10.4.4.4/32 is directly connected, Loopback1
C    10.50.30.0/24 is directly connected, Ethernet0/1
L    10.50.30.4/32 is directly connected, Ethernet0/1
O E2  10.50.90.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
O E2  10.50.100.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
  172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
D %   172.16.33.0/24 [90/27264000] via 172.17.70.5, 00:06:03, Tunnel1
C    172.16.34.0/24 is directly connected, Loopback0
L    172.16.34.4/32 is directly connected, Loopback0
D    172.16.35.0/24 [90/27008000] via 172.17.70.5, 00:06:03, Tunnel1
  172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.17.70.0/24 is directly connected, Tunnel1
L    172.17.70.4/32 is directly connected, Tunnel1
O E2  192.168.2.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
```

The NHRP mapping for 172.16.33.0 is pointing to R3:

[Click here to view code image](#)

```
R4# show ip nhrp
172.16.33.0/24 via 172.17.70.3
  Tunnel1 created 00:00:11, expire 01:59:48
  Type: dynamic, Flags: router rib nho
  NBMA address: 10.50.30.3
172.16.34.0/24 via 172.17.70.4
  Tunnel1 created 00:05:21, expire 01:54:38
  Type: dynamic, Flags: router unique local
  NBMA address: 10.50.30.4
  (no-socket)
172.17.70.3/32 via 172.17.70.3
  Tunnel1 created 00:05:21, expire 01:54:38
  Type: dynamic, Flags: router
  NBMA address: 10.50.30.3
172.17.70.5/32 via 172.17.70.5
  Tunnel1 created 5d20h, never expire
  Type: static, Flags: used
  NBMA address: 10.50.80.50
```

To verify the complete DMVPN solution, the **show dmvpn detail** command summarizes all component information:

[Click here to view code image](#)

R4# **show dmvpn detail**

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete

N - NATed, L - Local, X - No Socket

Ent --> Number of NHRP entries with same NBMA peer

NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting

UpDn Time --> Up or Down Time for a Tunnel

Interface Tunnel1 is up/up, Addr. is 172.17.70.4, VRF ""
Tunnel Src./Dest. addr: 10.50.30.4/MGRE, Tunnel VRF ""
Protocol/Transport: "multi-GRE/IP", Protect "DMVPN"
Interface State Control: Disabled
nhrp event-publisher : Disabled

IPv4 NHS:

172.17.70.5 RE priority = 0 cluster = 0

Type:Spoke, Total NBMA Peers (v4/v6): 3

# Ent	Peer NBMA Addr	Peer Tunnel Addr	State	UpDn Tm	Attrb	Target Network
2	10.50.30.3	172.17.70.3	UP 00:06:18	DT2		172.16.33.0/24
0	10.50.30.3	172.17.70.3	UP 00:06:18	D		172.17.70.3/32
1	10.50.30.4	172.17.70.4	UP 00:06:18	DLX		172.17.70.4/32
1	10.50.80.50	172.17.70.5	UP 02:41:45	S		172.17.70.5/32

Crypto Session Details:

Interface: Tunnel1

Session: [0xF2284140]

IKEv1 SA: local 10.50.30.4/500 remote 10.50.30.3/500 Active

Capabilities:(none) connid:1060 lifetime:23:53:41

IKEv1 SA: local 10.50.30.4/500 remote 10.50.30.3/500 Active

Capabilities:(none) connid:1059 lifetime:23:53:41

Crypto Session Status: UP-ACTIVE

fvrfr: (none), Phase1_id: 10.50.30.3

IPSEC FLOW: permit 47 host 10.50.30.4 host 10.50.30.3

Active SAs: 4, origin: crypto map
Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 4264509/3221
Outbound: #pkts enc'ed 1 drop 0 life (KB/Sec) 4264509/3221
Outbound SPI : 0xF540025B, transform : esp-3des esp-md5-hmac
Socket State: Open

Interface: Tunnel1

Session: [0xF2284238]

IKEv1 SA: local 10.50.30.4/4500 remote 10.50.80.50/4500 Active
Capabilities:N connid:1056 lifetime:21:18:13

Crypto Session Status: UP-ACTIVE

fvr: (none), Phase1_id: 10.50.90.5

IPSEC FLOW: permit 47 host 10.50.30.4 host 10.50.80.50

Active SAs: 2, origin: crypto map

Inbound: #pkts dec'ed 4144 drop 0 life (KB/Sec) 4269546/853

Outbound: #pkts enc'ed 2115 drop 0 life (KB/Sec) 4269770/853

Outbound SPI : 0x C24F6A, transform : esp-3des esp-md5-hmac

Socket State: Open

Pending DMVPN Sessions:

Configuration

Syntax highlighted in **cyan** needs to be added or modified.

R5

[Click here to view code image](#)

```
crypto isakmp policy 10
  encr 3des
  authentication pre-share
  group 2
crypto isakmp key cisco address 0.0.0.0
!
!
crypto ipsec transform-set dmvpn esp-3des esp-md5-hmac
  mode transport
!
crypto ipsec profile DMVPN
  set transform-set dmvpn
!

interface Loopback0
  ip address 172.16.35.5 255.255.255.0

interface Tunnel1
  ip address 172.17.70.5 255.255.255.0
```

```
no ip redirects
ip mtu 1360
ip nhrp authentication cisco
ip nhrp map multicast dynamic
ip nhrp network-id 70
ip nhrp holdtime 300
ip nhrp redirect
no ip split-horizon eigrp 123
delay 1000
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel key 123
tunnel protection ipsec profile DMVPN
```

```
router eigrp 123
network 172.16.35.0 0.0.0.255
network 172.17.70.0 0.0.0.255
```

R3

[Click here to view code image](#)

```
crypto isakmp policy 10
encr 3des
authentication pre-share
group 2
crypto isakmp key cisco address 0.0.0.0
!
!
crypto ipsec transform-set dmvpn esp-3des esp-md5-hmac
mode transport
!
crypto ipsec profile DMVPN
set transform-set dmvpn
!

interface Loopback0
ip address 172.16.33.3 255.255.255.0

interface Tunnel1
ip address 172.17.70.3 255.255.255.0
no ip redirects
ip nhrp authentication cisco
ip nhrp map 172.17.70.5 10.50.80.50
ip nhrp map multicast 10.50.80.50
ip nhrp network-id 70
ip nhrp nhs 172.17.70.5
```

```
ip nhrp shortcut
tunnel source Ethernet0/1
tunnel mode gre multipoint
tunnel key 123
tunnel protection ipsec profile DMVPN
```

```
router eigrp 123
network 172.16.33.0 0.0.0.255
network 172.17.70.0 0.0.0.255
```

R4

[Click here to view code image](#)

```
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key cisco address 0.0.0.0
!
!
crypto ipsec transform-set dmvpn esp-3des esp-md5-hmac
mode transport
!
crypto ipsec profile DMVPN
set transform-set dmvpn
!

interface Loopback0
ip address 172.16.34.4 255.255.255.0

interface Tunnel1
ip address 172.17.70.4 255.255.255.0
no ip redirects
ip nhrp authentication cisco
ip nhrp map 172.17.70.5 10.50.80.50
ip nhrp map multicast 10.50.80.50
ip nhrp network-id 70
ip nhrp nhs 172.17.70.5
ip nhrp shortcut
tunnel source Ethernet0/1
tunnel mode gre multipoint
tunnel key 123
tunnel protection ipsec profile DMVPN

router eigrp 123
network 172.16.34.0 0.0.0.255
```

```
network 172.17.70.0 0.0.0.255
```

ASA1/2

[Click here to view code image](#)

```
access-list 101 permit udp any any eq 4500  
access-list 101 permit esp any any  
access-group 101 in interface outside
```

Tech Notes

IKE and IPsec are unchanged across DMVPNv1, DMVPNv2, and DMVPNv3; the differences are in NHRP functionality and routing protocol configuration.

DMVPNv1

- Static hub to spoke
- Spoke-to-spoke communication is done via the hub
- The hub must be the route aggregation point and can summarize spoke routes
- No **tunnel mode gre multipoint** on spokes
- Turn off split-horizon (EIGRP, RIP); single area and no summarization (OSPF)
- Hubs must not preserve the original IP next hop
- Can use different routing protocol than on hub-spoke tunnels

[Click here to view code image](#)

```
! HUB
interface Tunnel0
ip address 10.0.0.1 255.255.255.0
no ip redirects
ip nhrp authentication cisco
ip nhrp map multicast dynamic
ip nhrp network-id 123
no ip split-horizon eigrp 123
ip summary-address eigrp 123 0.0.0.0 0.0.0.0 5
tunnel source Loopback0
tunnel mode gre multipoint
tunnel key 123
```

```
! SPOKE
interface Tunnel0
ip address 10.0.0.2 255.255.255.0
ip nhrp authentication cisco
ip nhrp map multicast 150.1.1.1
ip nhrp map 10.0.0.1 150.1.1.1
ip nhrp nhs 10.0.0.1
ip nhrp network-id 123
ip nhrp registration timeout 30
ip nhrp holdtime 60
tunnel source Loopback0
tunnel destination 150.1.1.1
tunnel key 123
```

DMVPNv2

- Static hub to spoke.
- Dynamic direct spoke to spoke.
- **Tunnel mode gre multipoint** on spokes.
- Turn off split-horizon (EIGRP, RIP); single area and no summarization (OSPF).
- Hubs must not preserve the original IP next hop.

- Hierarchical design support—spoke to spoke must use regional hubs but can bypass a central hub.
- Must use same routing protocol as on hub-spoke tunnels.
- CEF adjacency for spoke to spoke will reflect the spoke IP address as the next hop, as will FIB entry. This information is learned from the HUB. The HUB will track individual spoke routes; no summarization is possible.

[Click here to view code image](#)

```
! HUB
interface Tunnel0
ip address 10.0.0.1 255.255.255.0
no ip redirects
ip nhrp authentication cisco
ip nhrp map multicast dynamic
ip nhrp network-id 123
no ip split-horizon eigrp 123
no ip next-hop-self eigrp 123
tunnel source Loopback0
tunnel mode gre multipoint
tunnel key 123
```

```
! SPOKE
interface Tunnel0
ip address 10.0.0.2 255.255.255.0
ip nhrp authentication cisco
ip nhrp map multicast 150.1.1.1
ip nhrp map 10.0.0.1 150.1.1.1
ip nhrp nhs 10.0.0.1
ip nhrp network-id 123
ip nhrp registration timeout 30
ip nhrp holdtime 60
tunnel source Loopback0
tunnel mode gre multipoint
tunnel key 123
```

DMVPNv3

- Static hub to spoke
- Dynamic direct spoke to spoke
- **tunnel mode gre multipoint** on spokes
- Turn off split-horizon (EIGRP, RIP); single area and no summarization (OSPF)
- Hubs must preserve the original IP next hop
- Hierarchical design support—spoke to spoke can bypass regional hubs and central hub
- Can use a different routing protocol than on hub-spoke tunnels
- Routing table on spoke will contain the summary route to spokes via the next hop hub; however,

the spoke-to-spoke forwarding decision is made from the NHRP mapping table, which overrides the CEF adjacency (see [Figure 1a-3](#)).

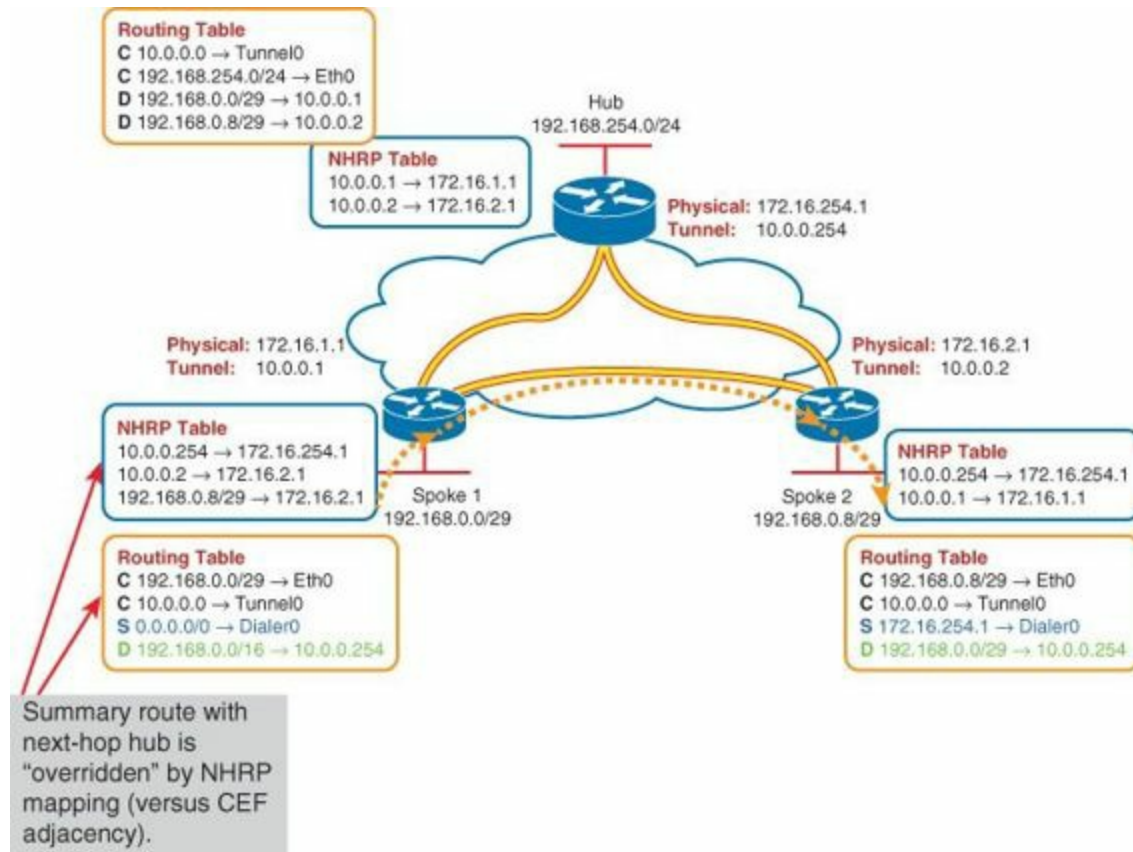


Figure 1a-3 *Illustration of Spoke-to-Spoke Forwarding*

[Click here to view code image](#)

```
! HUB
interface Tunnel0
ip address 10.0.0.1 255.255.255.0
no ip redirects
ip nhrp authentication cisco
ip nhrp map multicast dynamic
ip nhrp network-id 123
no ip split-horizon eigrp 123
ip nhrp redirect
ip summary-address eigrp 123 0.0.0.0 0.0.0.0 5
tunnel source Loopback0
tunnel mode gre multipoint
tunnel key 123
```

```
! SPOKE
interface Tunnel0
ip address 10.0.0.2 255.255.255.0
ip nhrp authentication cisco
ip nhrp map multicast 150.1.1.1
ip nhrp map 10.0.0.1 150.1.1.1
ip nhrp nhs 10.0.0.1
```

```
ip nhrp shortcut
ip nhrp network-id 123
ip nhrp registration timeout 30
ip nhrp holdtime 60
tunnel source Loopback0
tunnel mode gre multipoint
tunnel key 123
```

Solution and Verification for Exercise 3.3: Configure Security Features on the Cisco WLC

This exercise covers wireless fundamentals—specifically, configuring the Cisco WLC and Cisco access points in preparation for securely hosting wireless clients. For centralized management, the WLC can be configured to control the APs and push down configuration changes. For client access, different WLANs (the logical equivalent of VLANs) can be defined that enforce differing levels of security depending on the user. Ideally, the wireless solution is tested completely with a wireless client. If this is not available, familiarity with the various **show** commands on the WLC will help verify configurations. The verification of this exercise will be shown using the CLI on the WLC.

To verify this solution by connecting to an AP with a wireless client, the SSID and security parameters will need to be entered into the supplicant interface.

For all verification syntax that follows:

- Required output appears in **red**
- Variable syntax appears in **green**

Task 1: Initialize the Cisco WLC and Establish Control over the Cisco Access Points

The AP names and MAC addresses will be specific to the APs in the topology.

[Click here to view code image](#)

```
(WLC) >show ap summary
```

```
Number of APs..... 2
```

```
Global AP User Name..... cisco
```

```
Global AP Dot1x User Name..... Not Configured
```

AP Name	Slots	AP Model	Ethernet MAC	Location	Port
AP1cdf.0f94.8063	2	AIR-CAP3502I-A-K9	1c:df:0f:94:80:63	default location	1
AP588d.0959.4921	2	AIR-LAP1262N-A-K9	58:8d:09:59:49:21	default location	1

Task 2: Enable IP Services on the Cisco WLC to Enhance Security

Verify whether the WLC system time is using the NTP server as the clock source:

[Click here to view code image](#)

```
(WLC) >show time
```

Time..... Thu Aug 15 03:04:41 2013

Timezone delta..... 0:0

Timezone location.....

NTP Servers

NTP Polling Interval..... 6000

Index	NTP Key Index	NTP Server	NTP Msg Auth Status
1	0	192.168.2.5	AUTH DISABLED

Verify whether the connection to the RADIUS server is enabled:

[Click here to view code image](#)

(WLC) >show radius summary

```

Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..... lower
Call Station Id Type..... Mac Address
Aggressive Failover..... Enabled
Keywrap..... Disabled
Fallback Test:
  Test Mode..... Off
  Probe User Name..... cisco-probe
  Interval (in seconds)..... 300
MAC Delimiter for Authentication Messages..... hyphen
MAC Delimiter for Accounting Messages..... hyphen

```

Authentication Servers

Idx	Type	Server Address	Port	State	Tout	MgmtTout	RFC3576	IPSec
1	NM	192.168.2.15	1812	Enabled	2	2	Disabled	Disabled

Task 3: Creating and Assigning Security Policy to WLANs and Users

The solution to this task is verified using the following **show** commands:

[Click here to view code image](#)

(WLC) >show wlan summary

Number of WLANs..... 3

WLAN ID	WLAN Profile Name / SSID	Status	Interface Name
---------	--------------------------	--------	----------------

```

1    admin / admin           Enabled management
2    guest / guest          Enabled guest-wlan
3    employee / employee    Enabled employee-wlan

```

(WLC) >**show interface summary**

Interface Name	Port	Vlan Id	IP Address	Type	Ap Mgr	Guest
employee-wlan	1	110	10.10.110.2	Dynamic	No	No
guest-wlan	1	120	10.10.120.2	Dynamic	No	No
management	1	100	10.50.100.10	Static	Yes	No
service-port	N/A	N/A	0.0.0.0	DHCP	No	No
virtual	N/A	N/A	1.1.1.1	Static	No	No

(WLC) >**show wlan 2**

```

WLAN Identifier..... 2
Profile Name..... Guest
Network Name (SSID)..... Guest
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Enabled
AAA Policy Override..... Disabled
Network Admission Control
  Client Profiling Status ..... Disabled
  Radius-NAC State..... Disabled
  SNMP-NAC State..... Disabled
  Quarantine VLAN..... 0
Maximum number of Associated Clients..... 0
Maximum number of Clients per AP Radio..... 200
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... 1800 seconds
CHD per WLAN..... Enabled
Webauth DHCP exclusion..... Disabled
Interface..... guest-wlan
Radius Servers
  Authentication..... 192.168.2.15 1812
  Accounting..... Global Servers
  Interim Update..... Disabled
  Dynamic Interface..... Disabled
Local EAP Authentication..... Disabled
Security

```

802.11 Authentication:..... Open System
FT Support..... Disabled
Static WEP Keys..... Disabled
802.1X..... Disabled
Wi-Fi Protected Access (WPA/WPA2)..... Disabled
Wi-Fi Direct policy configured..... Disabled
EAP-Passthrough..... Disabled
CKIP Disabled
Web Based Authentication..... Enabled
 IPv4 ACL..... Unconfigured
 IPv6 ACL..... Unconfigured
 Web-Auth Flex ACL..... Unconfigured
Web Authentication server precedence:
 1..... local
 2..... radius
 3..... ldap

(WLC) >**show wlan 3**

WLAN Identifier..... 3
Profile Name..... employee
Network Name (SSID)..... employee
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Enabled
AAA Policy Override..... Disabled
Network Admission Control
 Client Profiling Status Disabled
 Radius-NAC State..... Disabled
 SNMP-NAC State..... Disabled
 Quarantine VLAN..... 0
Maximum number of Associated Clients..... 0
Maximum number of Clients per AP Radio..... 200
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... 1800 seconds
CHD per WLAN..... Enabled
Webauth DHCP exclusion..... Disabled
Interface..... employee-wlan

Radius Servers
 Authentication..... 192.168.2.15 1812
 Accounting..... Global Servers

Interim Update..... Disabled
Dynamic Interface..... Disabled
Local EAP Authentication..... Disabled
Security

802.11 Authentication:..... Open System

FT Support..... Disabled

Static WEP Keys..... Disabled

802.1X..... Disabled

Wi-Fi Protected Access (WPA/WPA2)..... Enabled

WPA (SSN IE)..... Disabled

WPA2 (RSN IE)..... Enabled

TKIP Cipher..... Disabled

AES Cipher..... Enabled

Auth Key Management

802.1x..... Enabled

PSK..... Disabled

CCKM..... Disabled

FT-1X(802.11r)..... Disabled

FT-PSK(802.11r)..... Disabled

The guest user account should not have an account lifetime associated with it, so it should be created as a permanent user type account or assigned a lifetime of 0 as a guest user type. If this is a user type guest account with a specified lifetime (not zero), this lifetime specifies how long the account will remain on the system before it is automatically removed. The lifetime for guest user type accounts is not an idle timer or session timer.

[Click here to view code image](#)

```
(WLC) >show netuser summary
```

User Name	WLAN Id	User Type	Lifetime	Description
guest1	Any	Permanent	N/A	
guest	WLAN 2	Guest	Infinity	

Configuration

[Click here to view code image](#)

```
config time ntp server 1 192.168.2.5
```

```
config radius auth add 1 192.168.2.15 1812 ascii cisco
```

```
interface create employee-wlan 110
```

```
interface address dynamic-interface employee-wlan 10.10.110.2 255.255.255.0  
10.10.110.1
```

```
interface dhcp dynamic-interface employee-wlan primary 10.10.110.1
```

```
interface port employee-wlan 1
```



```
interface create guest-wlan 120
interface address dynamic-interface guest-wlan 10.10.120.2 255.255.255.0
10.10.120.1
interface dhcp dynamic-interface guest-wlan primary 10.10.120.1
interface port guest-wlan 1
```

```
wlan create 3 employee employee
wlan create 2 guest guest
```

```
wlan security wpa disable 3
wlan security web-auth enable 2
```

```
wlan security wpa wpa2 ciphers aes enable 3
wlan security wpa akm 802.1x enable 3
```

```
wlan interface 3 employee-wlan
wlan interface 2 guest-wlan
wlan enable all
```

```
config netuser add guest cisco wlan 2 userType guest lifetime 0
```

ASA1/c2

```
access-list 101 extended permit udp any any eq 5246
access-list 101 extended permit udp any any eq 5247
```

Solution and Verification for Exercise 3.4: Configure the Cisco IOS Certificate Server

Skills Tested

- Configuring and enabling the Cisco IOS certificate server. This CA will issue end entity certificates to other devices in the topology using Cisco Simple Certificate Enrollment Protocol (SCEP).
- Configure other elements in the network as required to allow HTTP access to R1. HTTP is the transport for the SCEP messages.

Solution and Verification

The major criteria to verify for this exercise are the parameters on the CA server and the availability of the server from the perspective of the end entities in the network. This requires HTTP traffic to be allowed through the ASA1/c2 destined to R1. Cisco devices use SCEP for the authentication of the CA and enrollment of end entities using X.509-based certificates. In addition, other vendors, such as Microsoft, have implemented SCEP as a registration authority (RA), which acts as a translator between the Microsoft CA server and SCEP-based end entities.

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**
- Variable syntax appears in **green**

Verify whether the HTTP server is enabled on R1.

[Click here to view code image](#)

```
R1# show ip http server status
HTTP server status: Enabled
HTTP server port: 80
```

Allow HTTP through the Cisco ASA:

[Click here to view code image](#)

```
ASA1/c2# show run | include www
access-list 101 extended permit tcp any any eq www
```

Verify whether R1 is synchronized to a reliable time source. Certificates have a specified lifetime, and any issues with incorrect time can render a credential invalid.

[Click here to view code image](#)

```
R1# show ntp stat
Clock is synchronized, stratum 4, reference is 10.50.70.5
```

Before the certificate server can be configured and enabled, the CA itself must generate a public/private key pair that will be used to validate its own identity. When an end entity wishes to enroll with the CA it will request the CA's public key. The key information is verified as follows:

[Click here to view code image](#)

```
R1# show cry key mypubkey rsa
% Key pair was generated at: 22:12:36 UTC Jul 17 2012
Key name: ciscoca
Key type: RSA KEYS
Storage Device: private-config
Usage: General Purpose Key
Key is exportable.
```

The public key of the CA is distributed to the end entity in the form of a CA certificate, which is generated during the CA server configuration process. Verify whether the CA certificate has a lifetime of 1 year and the certificate itself is stored in NVRAM:

[Click here to view code image](#)

```
R1# show cry pki certificates
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
```

Issuer:

cn=ciscoca.cisco.com L=cisco C=US

Subject:

cn=ciscoca.cisco.com L=cisco C=US

Validity Date:

start date: 13:19:37 PST Aug 17 2013

end date: 13:19:37 PST Aug 17 2014

Associated Trustpoints: ciscoca

Storage: nvram:ciscocacisco#1CA.cer

To verify whether the CA server is ready to service end entities, make sure the server itself is enabled. By default, the CA server state is shut down.

When the end entity requests the CA cert, it will use **crypto ca authenticate ciscoca**, where *ciscoca* is the trustpoint name used in this question. In response, the CA will send its certificate along with a CA cert fingerprint. If the end entity trusts that the certificate is from the CA, it will accept the certificate based on accepting the fingerprint (hashed value derived from the CA cert). The fingerprint sent by the CA must match the fingerprint as it appears in the output of the **show crypto pki server** command (this value will vary). The chain of trust is now established between the end entity and CA.

The end entity will now use the **crypto ca enroll ciscoca** command to send its public key and identity information (CN, IP address, and so on) to the CA. The CA will issue a certificate based on this information and return it to the end entity signed with its private key. Using the concept of digital signatures, the end entity will verify whether the issued certificate has come from the trusted CA by decrypting the private key signed digital signature with the CA's public key. Remember that the public key was received by the end entity during the CA authentication step.

[Click here to view code image](#)

```
R1#(config)crypto pki server ciscoca  
no shutdown
```

```
R1# show crypto pki server
```

Certificate Server ciscoca:

Status: enabled

State: enabled

Server's configuration is locked (enter "shut" to unlock it)

Issuer name: CN=ciscoca.cisco.com L=cisco C=US

CA cert fingerprint: 1F5A02E4 C2C8230A 56FC15BB CBDFBEF6

Granting mode is: auto

Last certificate issued serial number (hex): 1

CA certificate expiration timer: 13:19:37 PST Aug 17 2014

CRL NextUpdate timer: 13:10:07 PST Sep 8 2013

Current primary storage dir: nvram:

Database Level: Minimum - no cert data written to storage

Configuration

R1

[Click here to view code image](#)

```
crypto key generate rsa general-keys label ciscoca exportable
!
crypto key export rsa ciscoca pem url nvram: 3des cisco123
!

crypto pki server ciscoca
 issuer-name CN=ciscoca.cisco.com L=cisco C=US
 grant auto
 lifetime crl 24
 lifetime certificate 200
 lifetime ca-certificate 365
crypto pki token default removal timeout 0
!
crypto pki trustpoint ciscoca
 revocation-check crl
 rsakeypair ciscoca
!
!
crypto pki certificate chain ciscoca
 certificate ca 01
 <cert omitted>
```

ASA1/c2

[Click here to view code image](#)

```
access-list 101 permit tcp any any eq www
access-group 101 in interface outside
```

Tech Notes

Simple Certificate Enrollment Protocol (SCEP) is the subject of an IETF informational draft that has the status of historic. It is used as a reference for those wishing to implement this protocol to handle X.509 certificates.

This document includes the definitions for the messages covered briefly in the solution review:

- **Get CA Certificate:** Sent in the clear using HTTP as a transport protocol.
- **CA Certificate Response:** Return an X.509 certificate authenticated with a fingerprint derived by calculating an MD5 or SHA hash over the entire certificate.
- **PKCSReq—Enrollment Request:** PKCS#10 cert request secured with a PKCS#7 envelop using a challenge password.
- **PKCSReq Response—Enrollment Response:** X.509 certificate secured with PKCS#7 envelop using CA private key.

The informational draft also outlines how CRLs are handled with SCEP.

Section 4: System Hardening and Availability

System or device hardening involves implementing techniques that protect against compromise resulting in either specific device/system failure or disruption to other network services. The goal of enabling protection and monitoring features on a system is performance predictability and network availability. The exercises in this section require implementing and troubleshooting specific hardening features such as control and management plane policing. Features that focus on network availability, such as routing protocol security, monitoring traffic transiting a switch, and securing wireless infrastructure, are also covered.

Solution and Verification for Exercise 4.1: Configure SPAN on the Cisco Catalyst Switch

Skills Tested

- Configuring the Cisco IPS sensor as an IDS by mirroring traffic on specific VLANs to the appliance previously configured in promiscuous mode
- Implementing SPAN on a Cisco Catalyst switch

Solution and Verification

Although the SPAN configuration is completed on SW2, the verification of this exercise will be done on the Cisco IPS sensor using the **packet display** command enabled on GigabitEthernet0/3.

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**
- Variable syntax appears in **green**

The **packet display** command should show traffic with source and/or destination IP addresses in VLAN 9 (10.50.9.0/24) and VLAN 77 (10.50.77.0/24). Some examples are highlighted.

[Click here to view code image](#)

```
IPS# packet display gigabitEthernet0/3
```

```
Warning: This command will cause significant performance degradation
```

```
tcpdump: WARNING: ge0_3: no Ipv4 address assigned
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
```

```
listening on ge0_3, link-type EN10MB (Ethernet), capture size 65535 bytes
```

```
03:29:29.669296 IP 10.50.77.5 > 224.0.0.5: OSPFv2, Hello, length: 56
```

```
03:29:29.669299 IP 10.50.77.5 > 224.0.0.5: OSPFv2, Hello, length: 56
```

```
03:29:29.669302 IP 10.50.77.5 > 224.0.0.5: OSPFv2, Hello, length: 56
```

```
03:29:31.410995 IP 10.50.100.10.5247 > 10.50.77.164.38035: UDP, length 76
```

```
03:29:31.550785 IP 10.50.9.5 > 224.0.0.5: OSPFv2, Hello, length: 56
```

```
03:29:31.550788 IP 10.50.9.5 > 224.0.0.5: OSPFv2, Hello, length: 56
```

```
03:29:31.550790 IP 10.50.9.5 > 224.0.0.5: OSPFv2, Hello, length: 56
```

```
03:29:39.472161 IP 10.50.77.5 > 224.0.0.5: OSPFv2, Hello, length: 56
```

```
03:29:39.472165 IP 10.50.77.5 > 224.0.0.5: OSPFv2, Hello, length: 56
```

```
03:29:39.472167 IP 10.50.77.5 > 224.0.0.5: OSPFv2, Hello, length: 56
```

03:29:40.621245 IP 10.50.9.5 > 224.0.0.5: OSPFv2, Hello, length: 56
03:29:40.621249 IP 10.50.9.5 > 224.0.0.5: OSPFv2, Hello, length: 56
03:29:40.621251 IP 10.50.9.5 > 224.0.0.5: OSPFv2, Hello, length: 56
03:29:41.874175 CDPv2, ttl: 180s, Device-ID "AP588d.0959.4921", length 378
14 packets captured
14 packets received by filter
0 packets dropped by kernel

Verification of the SPAN configuration on SW2 is as follows:

[Click here to view code image](#)

```
SW2# show monitor detail
```

```
Session 1
```

```
-----
```

```
Type           : Local Session  
Description     : -  
Source Ports    :  
  RX Only      : None  
  TX Only      : None  
  Both         : None  
Source VLANs    :  
  RX Only      : None  
  TX Only      : None  
  Both         : 9,77  
Source RSPAN VLAN : None  
Destination Ports : Gi1/0/17  
  Encapsulation : Native  
  Ingress       : Disabled  
Filter VLANs    : None  
Dest RSPAN VLAN : None  
IP Access-group : None  
MAC Access-group : None  
Ipv6 Access-group : None
```

Configuration

SW2

[Click here to view code image](#)

```
monitor session 1 source vlan 77  
monitor session 1 source vlan 9  
monitor session 1 destination interface Gi1/0/17
```

Tech Notes

SPAN Versus RSPAN

A local SPAN session is an association of a destination port with source ports. You can monitor incoming or outgoing traffic on a series or range of ports.

An RSPAN session is an association of source ports across your network with an RSPAN VLAN. The RSPAN VLAN must be labeled as such in the VLAN database, as shown in this command example, which defined VLAN 10 as an RSPAN VLAN:

```
vlan 10
  remote-span
```

SPAN and RSPAN Terminology and Guidelines

A *source port* (also called a monitored port) is a switched or routed port that you monitor for network traffic analysis. In a single local SPAN session or RSPAN source session, you can monitor source port traffic, such as received (Rx), transmitted (Tx), or bidirectional (both). The switch supports any number of source ports (up to the maximum number of available ports on the switch) and any number of source VLANs.

A source port has the following characteristics:

- It can be any port type (for example, EtherChannel, Fast Ethernet, Gigabit Ethernet, and so forth).
- It can be monitored in multiple SPAN sessions.
- It cannot be a destination port.
- Each source port can be configured with a direction (ingress, egress, or both) to monitor. For EtherChannel sources, the monitored direction would apply to all physical ports in the group.
- Source ports can be in the same or different VLANs.

Each local SPAN session or RSPAN destination session must have a *destination port* (also called a monitoring port) that receives a copy of traffic from the source ports and VLANs.

A destination port has these characteristics:

- A destination port must reside on the same switch as the source port (for a local SPAN session).
- A destination port can be any Ethernet physical port.
- A destination port can participate in only one SPAN session at a time. (A destination port in one SPAN session cannot be a destination port for a second SPAN session.)
- A destination port cannot be a source port.
- A destination port cannot be an EtherChannel group.
- A destination port can be a physical port that is assigned to an EtherChannel group, even if the EtherChannel group has been specified as a SPAN source. The port is removed from the group while it is configured as a SPAN destination port.
- The port does not transmit any traffic except traffic required for the SPAN session unless learning is enabled. If learning is enabled, the port also transmits traffic directed to hosts that have been learned on the destination port.

- If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.
- A destination port does not participate in spanning tree while the SPAN session is active.
- When it is a destination port, it does not participate in any of the Layer 2 protocols (STP, VTP, CDP, DTP, PagP).
- A destination port that belongs to a source VLAN of any SPAN session is excluded from the source list and is not monitored.
- A destination port receives copies of sent and received traffic for all monitored source ports. If a destination port is oversubscribed, it could become congested. This congestion could affect traffic forwarding on one or more of the source ports.

VLAN-Based SPAN

VLAN-based SPAN (VSPAN) is the monitoring of the network traffic in one or more VLANs.

Use these guidelines for VSPAN sessions:

- Traffic on RSPAN VLANs is not monitored by VLAN-based SPAN sessions.
- Only traffic on the monitored VLAN is sent to the destination port.
- If a destination port belongs to a source VLAN, it is excluded from the source list and is not monitored.
- If ports are added to or removed from the source VLANs, the traffic on the source VLAN received by those ports is added to or removed from the sources being monitored.
- VLAN pruning and the VLAN allowed list have no effect on SPAN monitoring.
- VSPAN monitors only traffic that enters the switch, not traffic that is routed between VLANs. For example, if a VLAN is being Rx-monitored, and the multilayer switch routes traffic from another VLAN to the monitored VLAN, that traffic is not monitored and is not received on the SPAN destination port.
- You cannot use filter VLANs in the same session with VLAN sources.
- You can monitor only Ethernet VLANs.

Solution and Verification for Exercise 4.2: Troubleshoot Secure Routing Using OSPFv3 in Cisco IOS

Skills Tested

- Troubleshooting IPsec support for OSPFv3, also known as OSPF for IPv6

Solution and Verification

OSPFv3 is used with IPv6 networks, which is why it is also known as OSPFv6. IPv6 introduces a series of extension headers that provide support for a number of services. The AH and ESP IPv6 extension headers are two of them.

This exercise requires the implementation of ESP to protect and authenticate the routing updates used by OSPFv3.

There is no key management mechanism like IKEv1 used with OSPFv3, so IPsec SAs are manually

keyed.

Protection can be applied to a whole area or on a link-by-link basis, because OSPFv3 does not need an explicit process to be created. This exercise states that the Loopback1 interfaces are not OSPFv3 interfaces in themselves. This means that to propagate their addresses, these interfaces are treated as “connected” and redistributed into OSPFv3. If the Loopback interfaces were labeled as OSPFv3 interfaces, it would be analogous to defining networks under OSPFv2 processes.

For all verification syntax that follows:

- Required output appears in **red**
- Nonzero/non-null syntax appears in **violet**

Verify whether the IPsec SAs are established between R1 and R2. There is no IKE SA because manual keys have been applied. The IPsecv6 policy name is automatically defined.

[Click here to view code image](#)

```
R1# show crypto session
```

```
Interface: Ethernet0/0
```

```
Session status: UP-NO-IKE
```

```
Peer: FF02::5 port 500
```

```
IPSEC FLOW: permit 89 FE80::/10 ::/0
```

```
Active SAs: 2, origin: manual-keyed crypto map
```

```
R1# show crypto ipsec sa
```

```
interface: Ethernet0/0
```

```
Crypto map tag: Ethernet0/0-OSPF-MAP, local addr FE80::A8BB:CCFF:FE00:7900
```

```
IPsecv6 policy name: OSPFv3-500
```

```
protected vrf: (none)
```

```
local ident (addr/mask/prot/port): (FE80::/10/89/0)
```

```
remote ident (addr/mask/prot/port): (::/0/89/0)
```

```
current_peer FF02::5 port 500
```

```
PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 141261, #pkts encrypt: 141261, #pkts digest: 141261
```

```
#pkts decaps: 141130, #pkts decrypt: 141130, #pkts verify: 141130
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 0, #recv errors 0
```

```
local crypto endpt.: FE80::A8BB:CCFF:FE00:7900,
```

```
remote crypto endpt.: FF02::5
```

```
path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb Ethernet0/0
```

```
current outbound spi: 0x1F4(500)
```

```
PFS (Y/N): N, DH group: none
```

inbound esp sas:
spi: 0x1F4(500)
transform: esp-3des esp-sha-hmac ,
in use settings = {Transport, }
conn id: 1, flow_id: SW:1, sibling_flags 80000001, crypto map:
Ethernet0/0-OSPF-MAP
sa timing: remaining key lifetime (sec): (0)
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: N
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x1F4(500)
transform: esp-3des esp-sha-hmac ,
in use settings = {Transport, }
conn id: 2, flow_id: SW:2, sibling_flags 80000001, crypto map:
Ethernet0/0-OSPF-MAP
sa timing: remaining key lifetime (sec): (0)
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: N
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas

To validate the IPsec SAs, check the IPv6 routing tables on R1 and R2 and make sure the Loopback1 addresses on each have been exchanged using OSPFv3.

[Click here to view code image](#)

R1# **show ipv6 route**

IPv6 Routing Table - default - 7 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP

H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea

IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO

ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect

l - LISP

O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

```
C 2001:128:BAD:64::/64 [0/0]
  via Ethernet0/0, directly connected
L 2001:128:BAD:64::1/128 [0/0]
  via Ethernet0/0, receive
C 3001:0:1:3::/64 [0/0]
  via Loopback1, directly connected
L 3001:0:1:3::/128 [0/0]
  via Loopback1, receive
L 3001:0:1:3:A8BB:CCFF:FE00:7900/128 [0/0]
  via Loopback1, receive
OE2 3001:0:2:3::/64 [110/20]
  via FE80::A8BB:CCFF:FE00:7A00, Ethernet0/0
L FF00::/8 [0/0]
  via Null0, receive
```

R2# show ipv6 route

IPv6 Routing Table - default - 6 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP

H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea

IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO

ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect

1 - LISP

O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

```
C 2001:128:BAD:64::/64 [0/0]
  via Ethernet0/0.1, directly connected
L 2001:128:BAD:64::2/128 [0/0]
  via Ethernet0/0.1, receive
OE2 3001:0:1:3::/64 [110/20]
  via FE80::A8BB:CCFF:FE00:7900, Ethernet0/0.1
C 3001:0:2:3::/64 [0/0]
  via Loopback1, directly connected
L 3001:0:2:3:A8BB:CCFF:FE00:7A00/128 [0/0]
  via Loopback1, receive
L FF00::/8 [0/0]
  via Null0, receive
```

Configuration

Syntax highlighted in cyan needed to be added or modified.

R1

[Click here to view code image](#)

ipv6 router ospf 21

```
area 0 encryption ipsec spi 500 esp 3des
1234567890123456789012345678901234567890ABCDEF12 sha1
123456789012345678901234567
8901234567890
redistribute connected
```

```
interface Loopback1
ipv6 address 3001:0:1:3::/64 eui-64
```

```
interface Ethernet0/0
ipv6 address 2001:128:BAD:64::1/64
ipv6 ospf 21 area 0
ipv6 enable
```

R2

[Click here to view code image](#)

```
interface Loopback1
ipv6 address 3001:0:2:3::/64 eui-64
```

```
interface Ethernet0/0.1
ipv6 address 2001:128:BAD:64::2/64
ipv6 ospf 21 area 0
ipv6 enable
```

```
ipv6 router ospf 21
area 0 encryption ipsec spi 500 esp 3des
1234567890123456789012345678901234567890ABCDEF12 sha1
123456789012345678901234567
8901234567890
redistribute connected
```

Tech Notes

The key differences between OSPFv2 and OSPFv3 are as follows:

- Enabling OSPF on an IPv6 interface automatically enables OSPFv3; an explicit OSPFv3 routing process does not need to be administratively created; however, other options available only under the “area” configuration might be required.
- OSPFv3 interfaces must be designated under interface configuration submode; there is no option to designate interfaces using the **network** command under router configuration.
- NBMA neighbors must be identified by link-local IPv6 address.
- Like OSPFv2, OSPFv3 will take its router ID from the highest-numbered IPv4 loopback interface; however, because this IPv4 address is likely irrelevant in your IPv6 network, it is recommended you manually specify a router ID with the **router-id** command under **ipv6 router ospf** configuration mode.

- OSPFv3 carries over the seven basic LSA types we're familiar with from OSPFv2; however, the type 1 and 2 LSAs have been repurposed. OSPFv3 also introduces two new LSA types: Link and Intra-area Prefix, as outlined in [Table 1a-3](#).

OSPFv3 LSA Types		OSPFv2 LSA Types	
0x2001	Router LSA	1	Router LSA
0x2002	Network LSA	2	Network LSA
0x2003	Inter-area Prefix LSA	3	Network Summary LSA
0x2004	Inter-area Router LSA	4	ASBR Summary LSA
0x4005	AS-External LSA	5	AS-External LSA
0x2006	Group Membership LSA	6	Group Membership LSA
0x2007	Type-7 LSA	7	NSSA External LSA
0x0008	Link LSA		
0x2009	Intra-area Prefix LSA		

Table 1a-3 *OSPFv2 and OSPFv3 LSA Types*

Solution and Verification for Exercise 4.3: Configure Control Plane Policing (CoPP)

Skills Tested

Implement CoPP to enable the route processor to service critical traffic types such as routing updates, keepalives and network management, to provide a predictable level of service by throttling back on less important traffic types in times of data congestion or device attack.

Solution and Verification

CoPP can help protect the router against DoS attacks that can occur either inadvertently or maliciously as a result of high levels of traffic being punted to the RP, causing excessive CPU utilization.

The application of CoPP is not difficult; however, it does require a good understanding of the types of traffic that need to be policed, and at what rate and granularity. For example, knowing HTTP needs to be prioritized, limit permitted HTTP traffic to flows between known sources and destinations. Configuration is done using the Modular QoS CLI (MQC) and then applied to the control plane. If a DoS attack occurs, critical traffic, such as routing protocol updates and IKE keepalives, can be guaranteed bandwidth to prevent route flaps and tunnel instability. Traffic with a recognized attack pattern or that is known to put a higher load on the router CPU can be classed as undesirable and dropped.

Verification

For all verification syntax that follows:

- Required output appears in **red**

To verify this solution on R7, the following **show** commands give a consolidated view of class maps that are used to define what traffic is of interest, and policy maps that define what actions are to be

taken on that traffic. In this case, the action taken is to be applied specifically to interesting traffic that is processed by the router control plane. Special attention must be paid to the use of **match-any** and **match-all** in class map definitions.

match-any states that any of the traffic criteria in the class map needs to be matched, whereas **match-all** requires all criteria defined in the class map to be matched.

As specified in the question, any names can be used for class maps and policy maps. It is important to correctly identify the traffic itself, and rates and actions to be applied to that traffic.

Traffic types are defined in access lists; these have been defined as specifically as possible to be relevant to R7, hence the need to understand network traffic flows.

[Click here to view code image](#)

```
R7# show access-list
Extended IP access list coppacl-VPN
  10 permit udp any any eq isakmp (1906 matches)
Extended IP access list coppacl-bgp
  10 permit tcp host 10.50.70.6 host 10.50.40.7 eq bgp (42748 matches)
  20 permit tcp host 10.50.70.6 eq bgp host 10.50.40.7 (71312 matches)
Extended IP access list coppacl-igp
  10 permit ospf any host 224.0.0.5 (158592 matches)
  20 permit ospf any host 224.0.0.6 (59 matches)
  30 permit ospf any any (123 matches)
Extended IP access list coppacl-management
  10 permit tcp 10.50.0.0 0.0.255.255 any eq telnet (72 matches)
  20 permit udp host 10.50.70.5 any eq ntp (18865 matches)
  30 permit tcp 192.168.2.0 0.0.0.255 any eq www (128 matches)
  40 permit tcp 192.168.2.0 0.0.0.255 any eq 443
  50 permit udp host 192.168.2.25 eq domain any (14 matches)
Extended IP access list coppacl-undesirable
  10 deny tcp any any fragments
  20 deny icmp any any fragments (10 matches)
IPv6 access list coppacl-VPNv6
  permit udp any any eq isakmp (60 matches) sequence 1
```

Class maps group interesting traffic into traffic classes. Note that the layer2 class uses the special **match protocol arp** and the default class, which is the catch-all for any traffic not explicitly matched, uses a **match-any** criteria.

[Click here to view code image](#)

```
R7# show class-map
Class Map match-any coppclass-VPN (id 9)
  Match access-group name coppacl-VPN
  Match access-group name coppacl-VPNv6

Class Map match-all coppclass-layer2 (id 10)
  Match protocol arp
```

Class Map match-any class-default (id 0)

Match any

Class Map match-all coppclass-igp (id 7)

Match access-group name coppacl-igp

Class Map match-all coppclass-undesirable (id 11)

Match access-group name coppacl-undesirable

Class Map match-all coppclass-bgp (id 1)

Match access-group name coppacl-bgp

Class Map match-any coppclass-management (id 8)

Match access-group name coppacl-management

For each traffic class, define the actions to be applied. There should be one policy map for each traffic class defined in [Table 1-17](#). Note that the traffic classes for BGP and OSPF have no explicit action because they were defined as having full access with no rate limiting.

```
R7# show policy-map
```

```
Policy Map copp-policy
```

```
Class coppclass-bgp
```

```
Class coppclass-igp
```

```
Class coppclass-management
```

```
police rate 125 pps
```

```
conform-action transmit
```

```
exceed-action transmit
```

```
Class coppclass-VPN
```

```
police rate 250 pps
```

```
conform-action transmit
```

```
exceed-action transmit
```

```
Class coppclass-layer2
```

```
police rate 20 pps
```

```
conform-action transmit
```

```
exceed-action transmit
```

```
Class coppclass-undesirable
```

```
police rate 10 pps
```

```
conform-action drop
```

```
exceed-action drop
```

```
Class class-default
```

```
police rate 25 pps
```

```
conform-action transmit
```

```
exceed-action drop
```

The following command is a good way to view the consolidated CoPP policies and ensure they are

correctly processing traffic on the control plane:

[Click here to view code image](#)

```
R7# show policy-map control-plane  
Control Plane
```

```
Service-policy input: copp-policy
```

```
Class-map: coppclass-bgp (match-all)  
  56964 packets, 4758874 bytes  
  5 minute offered rate 0 bps  
  Match: access-group name coppacl-bgp
```

```
Class-map: coppclass-igp (match-all)  
  158611 packets, 15826230 bytes  
  5 minute offered rate 0 bps  
  Match: access-group name coppacl-igp
```

```
Class-map: coppclass-management (match-any)  
  9537 packets, 859270 bytes  
  5 minute offered rate 0 bps, drop rate 0 bps  
  Match: access-group name coppacl-management  
  9535 packets, 859090 bytes  
  5 minute rate 0 bps
```

```
police:  
  rate 125 pps, burst 30 packets  
  conformed 9537 packets, 9537 bytes; actions:  
    transmit  
  exceeded 0 packets, 0 bytes; actions:  
    transmit  
  conformed 0 pps, exceeded 0 pps
```

```
Class-map: coppclass-VPN (match-any)  
  1007 packets, 186541 bytes  
  5 minute offered rate 0 bps, drop rate 0 bps  
  Match: access-group name coppacl-VPN  
  947 packets, 178425 bytes  
  5 minute rate 0 bps
```

```
Match: access-group name coppacl-VPNv6  
  60 packets, 8116 bytes  
  5 minute rate 0 bps  
police:  
  rate 250 pps, burst 61 packets  
  conformed 1007 packets, 1007 bytes; actions:  
    transmit
```


exceeded 0 packets, 0 bytes; actions:
transmit
conformed 0 pps, exceeded 0 pps

Class-map: coppclass-layer2 (match-all)
38523 packets, 2311380 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: protocol arp
police:
rate 20 pps, burst 4 packets
conformed 38523 packets, 38523 bytes; actions:
transmit
exceeded 0 packets, 0 bytes; actions:
transmit
conformed 0 pps, exceeded 0 pps

Class-map: coppclass-undesirable (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group name coppacl-undesirable
police:
rate 10 pps, burst 2 packets
conformed 0 packets, 0 bytes; actions:
drop
exceeded 0 packets, 0 bytes; actions:
drop
conformed 0 pps, exceeded 0 pps

Class-map: class-default (match-any)
279559 packets, 35570430 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: any
police:
rate 25 pps, burst 6 packets
conformed 279464 packets, 279464 bytes; actions:
transmit
exceeded 95 packets, 95 bytes; actions:
drop
conformed 0 pps, exceeded 0 pps

Configuration

R7

[Click here to view code image](#)

```
class-map match-all coppclass-bgp
```

```
match access-group name coppacl-bgp
class-map match-all coppclass-igp
match access-group name coppacl-igp
class-map match-any coppclass-management
match access-group name coppacl-management
class-map match-any coppclass-VPN
match access-group name coppacl-VPN
match access-group name coppacl-VPNv6
class-map match-all coppclass-layer2
match protocol arp
class-map match-all coppclass-undesirable
match access-group name coppacl-undesirable
```

```
policy-map copp-policy
class coppclass-bgp
class coppclass-igp
class coppclass-management
police rate 125 pps conform-action transmit exceed-action transmit
class coppclass-VPN
police rate 250 pps conform-action transmit exceed-action transmit
class coppclass-layer2
police rate 20 pps conform-action transmit exceed-action transmit
class coppclass-undesirable
police rate 10 pps conform-action drop exceed-action drop
class class-default
police rate 25 pps conform-action transmit exceed-action drop
```

```
ip access-list extended coppacl-VPN
 permit udp any any eq isakmp
ip access-list extended coppacl-bgp
 permit tcp host 10.50.70.6 host 10.50.40.7 eq bgp
 permit tcp host 10.50.70.6 eq bgp host 10.50.40.7
ip access-list extended coppacl-igp
 permit ospf any host 224.0.0.5
 permit ospf any host 224.0.0.6
 permit ospf any any
ip access-list extended coppacl-management
 permit tcp 10.50.0.0 0.0.255.255 any eq telnet
 permit udp host 10.50.70.5 any eq ntp
 permit tcp 192.168.2.0 0.0.0.255 any eq www
 permit tcp 192.168.2.0 0.0.0.255 any eq 443
 permit udp host 192.168.2.25 eq domain any
```

ip access-list extended coppacl-undesirable

deny tcp any any fragments

deny icmp any any fragments

control-plane

service-policy input copp-policy

Tech Notes

Router Planes

A router can be logically divided into three functional components or planes, as described in the following list, along with some protection mechanism that can be applied to each plane:

■ Data Plane:

- Drop all or selective drop IP options
- Disable redirects, source routing, directed broadcasts
- Enable ICMP packet filtering, but understand IPv4 versus IPv6 requirements
- Unicast RPF
- Enable TTL expiry

■ Management Plane:

- Out-of-band management
- Password security
- SNMP security
- Remote terminal access security
- Disable unused services
- Disable idle user sessions
- System banners
- Secure IOS file systems
- Role-based CLI access
- Management plane protection
- Authentication, Authorization, Accounting (AAA)
- AutoSecure
- Identify unused protocols—HTTP server, CDP
- Infrastructure ACLs

■ Control Plane:

- Disable unused control plane services
- ICMP techniques—no ICMP redirects, no ICMP unreachable, ICMP rate limiting
- Selective packet discard—IP options, fragments
- Control plane policing and control plane protection (port and threshold)
- MD5 authentication

- BGP techniques—max prefixes, ttl-security
- Route filtering and passive interfaces
- Infrastructure ACLs
- Selective packet discard IPv6
- OSPFv3 IPv6 ttl-security for virtual links (global addressing)

As a rule of thumb:

- Traffic to the control and management plane is always destined to the device.
- Traffic in the data plane is always destined through the device.

CoPP Versus CPPr

This exercise presented Control Plane Policing (CoPP). CoPP introduced the concept of rate-limiting protocol-specific traffic destined to the processor by applying QoS policies to the **aggregate** control-plane interface. CoPP is implemented on the router using the following command:

[Click here to view code image](#)

```
control-plane
  sevice-policy input | output policy-map-name
```

But what is Control Plane Protection (CPPr)?

Control Plane Protection extends control plane functionality by providing three additional control-plane *subinterfaces* under the top-level (aggregate) control-plane interface. Each subinterface receives and processes a specific type of control-plane traffic.

The three subinterfaces are as follows:

- **Control-plane host subinterface:** This interface receives all control-plane IP traffic that is directly destined for one of the router interfaces (for example, iBGP, EIGRP, SSH).
- **Control-plane transit subinterface:** This subinterface receives all control-plane IP traffic that is not directly destined to the router itself but rather traffic traversing the router (for example, nonterminating tunnel traffic).
- **Control-plane CEF-exception subinterface:** This control-plane subinterface receives all traffic that is either redirected as a result of a configured input feature in the CEF packet forwarding path for process switching or directly enqueued in the control plane input queue by the interface driver (for example, ARP, eBGP, or OSPF).

All protection features in the control plane are implemented as MQC policies that operate using the control plane class maps and policy maps. Additional class map and policy map types have been created for the control plane port-filter and per-protocol queue-threshold features.

CPPr is implemented on the router using the following command options:

[Click here to view code image](#)

```
control-plane host option
  cef-exception Cef-exception traffic control-plane
configuration
  host          Host traffic control-plane configuration
  transit       Transit traffic control-plane configuration
```

Solution and Verification for Exercise 4.4: Troubleshoot Management Plane Protection

Skills Tested

- Understanding management plane protection (MPP) in terms of protocols supported, monitoring, and application on the router

Solution and Verification

In this exercise, management plane protection is preconfigured to allow HTTP management to R7 via GigabitEthernet0/1. The debug output is the result of a Telnet connection that has been attempted to the same interface (10.50.40.7). The solution is to add Telnet to the list of permitted protocols on the interface. HTTP must not be removed from the list because it will impact other exercises in this guide.

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**

Initiate a Telnet session to 10.50.40.7 from another device, such as R2. The connection should succeed and MPP packets for Telnet will increment.

[Click here to view code image](#)

```
R2# telnet 10.50.40.7  
Trying 10.50.40.7 ... Open
```

User Access Verification

```
Username: cisco  
Password: cisco
```

```
R7# exit
```

```
R7# show management-interface  
Management interface GigabitEthernet0/1  
  Protocol    Packets processed  
  http        0  
  telnet     36
```

Configuration

[Click here to view code image](#)

```
! R7  
control-plane host  
management-interface GigabitEthernet0/1 allow http telnet
```

Solution and Verification for Exercise 4.5: Device Hardening on the Cisco WLC

Skills Tested

- An understanding of the types of attacks and vulnerabilities that can occur in a wireless network and how to harden the WLC and its communications with APs to defend against these attacks

Solution and Verification

The Cisco WLC can be protected from a range of different wireless attack types using features and functions in the OS. Configuration can be done either from the CLI or via the management GUI. Although using the GUI makes configuration fairly simple, it is important that the administrator be familiar with wireless attack methods and which features and protocols must be implemented to protect against them. A number of mechanisms are available, such as rate limiting, that can be used to throttle back less critical user traffic (such as guests). The features covered in this question are useful and effective ways to harden the WLC and provide protection for other wireless infrastructure like the AP under the control of the WLC. Hardening consists of enforcing security as well as ensuring availability and predictability in the wireless network.

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**
- Variable syntax appears in **green**

Task 1: Disable SSID Broadcasting

From [Exercise 3.3](#), the employee WLAN identifier is 3. To verify whether SSID broadcasting is disabled, use the following command output:

[Click here to view code image](#)

```
(WLC) >show wlan 3
```

```
WLAN Identifier..... 3  
Profile Name..... employee  
Network Name (SSID)..... employee  
Status..... Enabled  
MAC Filtering..... Disabled  
Broadcast SSID..... Disabled
```

Task 2: Protect the WLC Against Associating with a Rogue AP

Two APs exist in the network. This task involves creating a rule that will identify potential rogue APs and classify them as malicious to take further actions (alerts, containment). The match-any criteria for the rogue rule is no encryption (if the rogue access point's advertised WLAN does not have encryption enabled), and a client count of less than 1 associated with the AP.

[Click here to view code image](#)

```
(WLC) >show rogue rule summary
```

Priority	Rule Name	State	Type	Match	Hit Count
1	RogueAP	Enabled	Malicious	Any	0

```
(WLC) >show rogue rule detailed RogueAP
```

```
Priority..... 1
Rule Name..... RogueAP
State..... Enabled
Type..... Malicious
Match Operation..... Any
Hit Count..... 0
Total Conditions..... 2
Condition 1
  type..... Client-count
  value..... 1
Condition 2
  type..... No-encryption
  value..... Enabled
```

This task also required the AP receiving an IP address on the same network as the WLC—that is, 10.50.100.0/24—to be explicitly classified as friendly. The MAC address of the AP is required to create the classification policy. This AP receives an address via DHCP on R2, so the MAC address will be in the ARP cache on R2.

[Click here to view code image](#)

```
R2# show arp
Internet 10.50.100.51      0 1cdf.0f94.8063 ARPA Ethernet0/0.1
```

```
(WLC) >show rogue ap friendly summary
```

```
Number of APs..... 1

MAC Address      State      # APs # Clients Last Heard
-----
1c:df:0f:94:80:63 Internal    0    0    Not Heard
```

Task 3: Enable Infrastructure Management Frame Protection on the Cisco WLC

In 802.11, management frames, such as (de)authentication, (dis)association, beacons, and probes, are always unauthenticated and unencrypted. In other words, 802.11 management frames are always sent in an unsecured manner, unlike the data traffic, which is encrypted with protocols such as WPA and WPA2. This enables an attacker to spoof a management frame from the AP to attack a client that is associated to an AP. With the spoofed management frames, an attacker can perform actions such as the following:

- Run a Denial of Service (DoS) attack on the WLAN
- Attempt a Man-in-the-Middle attack on the client when it reconnects
- Run an offline dictionary attack

Management Frame Protection (MFP) requires the authentication of 802.11 management frames exchanged in the wireless network infrastructure.

Infrastructure MFP protects 802.11 session management functions by adding message integrity check information elements (MIC IEs) to the management frames emitted by access points (and not those emitted by clients), which are then validated by other access points in the network. Infrastructure MFP is passive. It can detect and report intrusions but has no means of stopping them.

Infrastructure MFP can be enabled locally on a per-AP basis, or globally for all associated APs as required here.

[Click here to view code image](#)

```
(WLC) >show wps mfp summary
```

```
Global Infrastructure MFP state..... Enabled
Controller Time Source Valid..... False
```

Task 4: Enable Encryption for CAPWAP Packets

By default, Control and Provisioning of Wireless Access Points protocol (CAPWAP) control packets are protected by Datagram Transport Layer Security (DTLS) encryption. If both the WLC and AP have the appropriate encryption license, DTLS can also be used to protect CAPWAP data packets. Data packets represent the actual wireless user data sent between the AP and WLC. This task requires CAPWAP control, and data packets are protected by DTLS for the “friendly” AP.

[Click here to view code image](#)

```
(WLC) >show ap link-encryption all
```

AP Name	Encryption State	Dnstream Count	Upstream Count	Last Update
AP588d.0959.4921	Dis	0	0	5:12
AP1cdf.0f94.8063	En	0	0	Never

```
(WLC) >show dtls connections
```


AP Name	Local Port	Peer IP	Peer Port	Ciphersuite
AP588d.0959.4921	Capwap_Ctrl	10.50.77.164	38035	TLS_RSA_WITH_AES_128_CBC_5
AP1cdf.0f94.8063	Capwap_Ctrl	10.50.100.54	18439	TLS_RSA_WITH_AES_128_CBC_5
AP1cdf.0f94.8063	Capwap_Data	10.50.100.54	18439	TLS_RSA_WITH_AES_128_CBC_5

Task 5: Create a Rate Limiting Policy for Guest Users on the Guest WLAN

The user guest was created in [Exercise 3.3](#). In this task, a QoS policy is created to rate limit the bandwidth used by this user. The parameters were provided in the exercise and appear in the following output as part of a guest role policy. As a rule, the burst data rate should be greater than or equal to the average data rate; otherwise, the QoS policy might block traffic to and from a wireless client. Data rates pertain to TCP traffic, Realtime rates refer to UDP traffic.

[Click here to view code image](#)

```
(WLC) >show netuser guest-roles
```

```
Role Name..... Guest
Average Data Rate..... 10
Burst Data Rate..... 10
Average Realtime Rate..... 100
Burst Realtime Rate..... 100
```

Verify whether this guest role is applied to the guest user:

[Click here to view code image](#)

```
(WLC) >show netuser detail guest
```

```
User Name..... guest
WLAN Id..... 2
User Type..... Guest
Lifetime..... Infinity
Start Time..... Tue Sep 10 05:42:22 2013
Description.....
Role Name..... Guest
Average Data Rate..... 10
Burst Data Rate..... 10
Average Realtime Rate..... 100
Burst Realtime Rate..... 100
```

Configuration

[Click here to view code image](#)

```
config wlan broadcast-ssid disable 3
config wps mfp infrastructure enable
config ap link-encryption enable AP1cdf.0f94.8063
```

```

config rogue rule add ap priority 1 classify malicious RogueAP
config rogue rule enable RogueAP
config rogue rule match any RogueAP
config rogue rule condition ap set no-encryption RogueAP
config rogue rule condition ap set client-count 1

```

```

config rogue ap friendly add 1c:df:0f:94:80:63

```

```

config netuser guest-role qos data-rate average-data-rate guest 10
config netuser guest-role qos data-rate burst-data-rate guest 10
config netuser guest-role qos data-rate average-realtime-rate guest 100
config netuser guest-role qos data-rate burst-realtime-rate guest 100

```

Tech Notes

Summary of Wireless Attacks

[Table 1a-4](#) provides a summary of well-known attacks and the features available on the Cisco WLC to prevent them. This is not an exhaustive list, and you are encouraged to do further research on attacks and the tools used to perpetrate them.

Attack Type	Attack Method	Attack Mitigation Method
Reconnaissance/Network Discovery	Passive/active probing	Don't broadcast SSID, AP cloaking
MITM	Rogue AP attacks	Rogue rules, Rogue Location Discovery Protocol (RLDP)
Surveillance	WEP cracking	TKIP/MIC, AES-CCMP
DoS	RF interference	Radio Resource Management (RRM) functions on the WLC
Flood	Associate/disassociate frames	Management Frame Protection (MFP)
Impersonation	MAC address spoofing	MAC filtering, Layer 2 switch security features

Table 1a-4 *Well-Known Attacks/Cisco Mitigation Methods*

In addition, the Cisco WLC supports Wireless IPS and includes several standard signatures that are tunable on the device, including

- Bcast deauth
- NULL probe resp
- Assoc flood
- Auth flood
- Reassoc flood
- Broadcast Probe flood
- Disassoc flood
- Deauth flood

- EAPOL flood
- NetStumbler
- Wellenreiter

Several wireless client-focused checks are enabled by default:

[Click here to view code image](#)

show wps summary

Client Exclusion Policy

Excessive 802.11-association failures..... Enabled
 Excessive 802.11-authentication failures..... Enabled
 Excessive 802.1x-authentication..... Enabled
 IP-theft..... Enabled
 Excessive Web authentication failure..... Enabled

Signature Policy

Signature Processing..... Enabled

Management Frame Protection via 802.11w

802.11w is an IEEE standard based on MFP methods that protects the integrity of connections and network-sensitive information for wireless deployments. Unlike data traffic, which can be encrypted to provide a level of confidentiality, these frames must be heard and understood by all clients and therefore must be transmitted as open or unencrypted. Although these frames cannot be encrypted, they must be protected from forgery to protect the wireless medium from attacks. For example, an attacker could spoof management frames from an AP to attack a client associated with the AP. The 802.11w protocol applies only to a set of robust management frames that are protected by the MFP service. These include disassociation, deauthentication, and robust action frames.

802.11w was introduced on Cisco WLCs in version 7.4 and above. It applies the following mechanisms:

- Client protection is added by the AP, adding cryptographic protection to deauthentication and disassociation frames, preventing them from being spoofed in a DoS attack.
- Infrastructure protection is added by adding a Security Association (SA) teardown protection mechanism consisting of an association comeback time and an SA-Query procedure, preventing spoofed association requests from disconnecting an already connected client.

Section 5: Threat Identification and Mitigation

The exercises in this section require the implementation of threat identification and mitigation techniques on different Cisco platforms. On a Cisco IOS router, NetFlow is used to identify possible attack patterns, and this information is then used to build a flexible packet matching (FPM) policy. DHCP activities may be manipulated to launch attacks that are mitigated by methods configured on Cisco Catalyst switches. This section also covers application-specific attack mitigation features on the Cisco ASA.

Solution and Verification for Exercise 5.1: Troubleshoot IPv6 in IPv4 Tunnel

Skills Tested

- Configuring and overlaying IPv6 in IPv4 tunneling in a complex network topology
- The ability to configure access lists to classify potential attack traffic such as Teredo

Solution and Verification

This exercise required an IP protocol 41–based ipv6ip tunnel to be established between R5 and R6. This tunnel is dependent on the configuration from [Exercise 1.3](#). The tunnel must be properly enabled and passing all IPv6 traffic, including EIGRPv6 routing updates.

When the tunnel state is verified, a classification ACL is required on R5 to monitor for the receipt of Teredo tunneled IPv6 traffic.

A Teredo tunnel (RFC 4380) is an IPv6-in-IPv4 tunnel that is encapsulated in UDP port 3544. It is a solution that enables ipv6ip traffic to be easily handled by NAT devices and firewalls. Teredo allows end-to-end IPv6 connectivity through IPv4 with the end hosts responsible for the tunneling process. This means potential attack traffic can slip through checks on firewalls and be propagated by the destination end systems.

The ACL should log any Teredo traffic as well as IP protocol 41 traffic, but do not log all IP traffic, especially if you are logging to the console and have no other way to connect to the router.

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**
- Nonzero/non-null syntax appears in **violet**

Two elements of the [Exercise 1.3](#) configuration will impact this solution:

- The access list applied to ASA1/c2 must allow IP protocol 41 between R6 and R5.
- The network object NAT configuration has mapped the inside IP address of 10.50.90.5 on R5 to the outside IP address 10.50.80.50. This is the IP address to which R6 must refer as the tunnel destination address.

Verify whether the ipv6ip tunnel is up and passing traffic by checking the IPv6 routing tables on R5 and R6, and look for exchanged routes:

[Click here to view code image](#)

```
R5# show ipv6 route
```

```
IPv6 Routing Table - default - 6 entries
```

```
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
```

```
  B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
```

```
  H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
```

```
  IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
```

```
  ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
```

```
  1 - LISP
```

```
  O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
```

```
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C 1010::/64 [0/0]
  via Loopback1, directly connected
L 1010::A8BB:CCFF:FE00:7D00/128 [0/0]
  via Loopback1, receive
C 2001:DB8::/64 [0/0]
  via Tunnel0, directly connected
L 2001:DB8::1:5/128 [0/0]
  via Tunnel0, receive
EX 2010::/64 [170/27008000]
  via FE80::A32:5006, Tunnel0
L FF00::/8 [0/0]
  via Null0, receive
```

```
R6# show ipv6 route
```

```
IPv6 Routing Table - default - 6 entries
```

```
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
```

```
  B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
```

```
  H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
```

```
  IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
```

```
  ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
```

```
  l - LISP
```

```
  O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
```

```
  ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
```

```
EX 1010::/64 [170/27008000]
  via FE80::A32:5A05, Tunnel0
C 2001:DB8::/64 [0/0]
  via Tunnel0, directly connected
L 2001:DB8::1:6/128 [0/0]
  via Tunnel0, receive
C 2010::/64 [0/0]
  via Loopback1, directly connected
L 2010::A8BB:CCFF:FE00:7E00/128 [0/0]
  via Loopback1, receive
L FF00::/8 [0/0]
  via Null0, receive
```

The Teredo classification ACL should contain a log entry for UDP/3544 and IP 41. You must also permit **ip any any**; otherwise, the implicit deny will block all other IP traffic. Do not use the **log** keyword with **ip any any**. Apply the list to interface ethernet0/0 on R5 outbound:

[Click here to view code image](#)

```
R5# show access-lists
```

```
Extended IP access list DetectIPv6
```

```
10 permit 41 any any log (14 matches)
```

```
20 permit udp any any eq 3544 log
```

30 **permit ip any any** (155 matches)

To verify whether the ACL is classifying traffic, check the router logs:

[Click here to view code image](#)

```
R5# show log – (logging console enabled)
*Aug 27 17:51:20.992: %SEC-6-IPACCESSLOGNP: list DetectIPv6 permitted 41
10.50.80.6 -> 10.50.90.5, 1 packet
```

Configuration

Syntax highlighted in **cyan** needs to be added or modified.

R5

[Click here to view code image](#)

```
IP access list DetectIPv6
permit 41 any any log
permit udp any any eq 3544 log
permit ip any any
```

```
int e0/0
ip access-group DetectIPv6 out
```

R6

[Click here to view code image](#)

```
interface Tunnel0
no ip address
ipv6 address 2001:DB8::1:6/64
ipv6 eigrp 65
tunnel source Ethernet0/0
tunnel mode ipv6ip
tunnel destination 10.50.80.5
```

ASA1/c2

[Click here to view code image](#)

```
access-list 101 extended permit 41 host 10.50.80.6 host
10.50.90.5
```

Solution and Verification for Exercise 5.2: Mitigating DHCP Attacks on a Cisco Catalyst Switch

Skills Tested

- Identifying and configuring protection against Layer 2 and Layer 3 attacks on a Cisco Catalyst switch, specifically those related to DHCP and IP address spoofing

Solution and Verification

This exercise requires the implementation of an attack mitigation strategy on the Cisco Catalyst switch. It is important that the administrator be familiar with attacks at both Layer 2 and Layer 3, and the features available to protect against them. This question has two requirements. The first deals with protection against DHCP-based attacks, using DHCP snooping. These include MITM attacks via rogue DHCP servers and DHCP address starvation attacks. The second requirement is the use of IP source guard (with port security) to help prevent IP and MAC spoofing attacks.

IP source guard with the port-security keyword provides an additional level of security because it will prevent a device from sending traffic on a switchport (apart from DHCP) until it receives an IP address from DHCP. The following caveats surround source guard with port security:

- The MAC address in the DHCP packet is not learned as a secure address. The MAC address of the DHCP client is learned as a secure address only when the switch receives non-DHCP data traffic.
- The DHCP server must support option 82 or the client is not assigned an IP address. Without DHCP option 82 data returned from the DHCP server, the switch cannot locate the client host port to forward the DHCP server reply.
- IP source guard with IP+MAC disables dynamic MAC learning on the port for DHCP and ARP packets.

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**
- Variable syntax appears in **green**

To verify your solution, you will first need to trigger the DHCP request from AP1.

Bounce the interface on SW1 to AP1 to generate a DHCP request to populate DHCP snooping database:

[Click here to view code image](#)

```
SW1# conf t
SW1(config)# int GigabitEthernet1/0/19
SW1(config)# shut
SW1(config)# no shut
```

When the address is assigned by R2, check that there is a binding in the DHCP snooping database:

[Click here to view code image](#)

```
SW1# show ip dhcp snooping binding
MacAddress      IpAddress      Lease(sec)  Type           VLAN  Interface
-----
1C:DF:0F:94:80:63  10.50.100.53  infinite   dhcp-snooping  100  GigabitEthernet1/0/19
Total number of bindings: 1
```

The configuration of DHCP snooping itself is verified using the following (snooping has also been enabled for all the wireless VLANs serviced by the DHCP server on R2):

[Click here to view code image](#)

```
SW1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
100,110,120
DHCP snooping is operational on following VLANs:
100,110,120
Smartlog is configured on following VLANs:
none
Smartlog is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:
```

```
Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: c464.13fb.7780 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
```

Interface	Trusted	Rate limit (pps)
GigabitEthernet1/0/2	yes	unlimited

For the IP source guard feature verification, the **show ip verify source** command will show the DHCP-issued address that has been bound to the switchport (as stored in the DHCP snooping database). The **ip-mac** filter-type indicates the IP source guard has been correctly combined with port-security to enforce the additional restriction on traffic flow until after DHCP has assigned an address to AP1.

[Click here to view code image](#)

```
SW1# show ip verify source
```

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan	Log
Gi1/0/19	ip-mac	active	10.50.100.53	1C:DF:0F:94:80:63	100	disabled

Configuration

SW1

[Click here to view code image](#)

```
ip dhcp snooping vlan 100,110,120
ip dhcp snooping
```



```

interface GigabitEthernet 1/0/2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 100,110,120
switchport mode trunk
ip dhcp snooping trust

```

```

interface GigabitEthernet1/0/19
switchport access vlan 100
switchport mode access
ip verify source port-security
switchport port-security
!

```

Tech Notes

[Table 1a-5](#) summarizes the Cisco Catalyst security features used in this exercise.

Feature Name	Functional Description	Attack Mitigation
Port Security	Identifies and limits MACs per port	CAM attacks and some DHCP starvation attacks
DHCP Snooping	Binds MAC/VLAN/IP in database based on DHCP mechanism	Rogue DHCP servers, DHCP starvation by checking CHADDR
Dynamic ARP Inspection	Incoming ARP packets to a port validated against DHCP snooping database (or manual mappings)	ARP cache poisoning, ARP spoofing
IP Source Guard	IP source binding table learned based off DHCP snooping database (or manual mappings)	IP/MAC spoofing
Spanning Tree Features	Loop Guard, Root Guard, BPDU Guard	Unpredictable STP results, improper rerouting of traffic

Table 1a-5 *Cisco Catalyst Switch Security Features*

DHCP Implementation Notes

DHCP Option 82

DHCP option 82 is on by default with DHCP snooping and ensures the VLAN ID is passed to the DHCP server on R2 to the select address pool. It allows for an address pool to be shared across VLANs. In normal DHCP address allocation, the DHCP server will look only at the giaddr (gateway IP address) field and not be able to differentiate between multiple address ranges in the same address pool.

To solve this problem, a relay agent in the switch inserts the relay information option (option 82), which carries attributes specific to the port, and the DHCP server must inspect both the giaddr field and the inserted option 82 during the address selection process. This is especially important if the

giaddr value is 0 or missing. If a deployment requirement is to share the address pool across multiple VLANs, DHCP classes are used to define ranges within the large pool.

Example:

[Click here to view code image](#)

```
ip dhcp class CLASS1
  relay agent information
  relay-information hex 01030a0b0c020500000000123
```

```
ip dhcp pool ABC
  network 10.0.20.0 255.255.255.0
  class CLASS1
  address range 10.0.20.1 10.0.20.100
  class CLASS2
  address range 10.0.20.101 10.0.20.200
```

The value hex is used to define the class generated by the relay agent based on the attributes of the requesting client. To determine how to configure a class value for specific ports, you can use the following trick:

- Configure a DHCP pool matching the remote giaddr IP address value. Create a DHCP class with a relay-information value that will never match a real-life client. For example, set the value to 00000000*. Associate this class with the pool and configure a subrange as usual.
- Enable the following debug in the server: **debug ip dhcp server class**, which tracks the class-based allocation. When an incoming packet contains a DHCP option 82 that does not match any class, the output similar to the following will appear:

[Click here to view code image](#)

```
Aug 19 21:42:52.030: DHCPD: Searching for a match to '    relay-
information 010600040064011302080006c46413fb7780' in class CLASS1
```

DHCP Snooping and the DHCP Server on Cisco IOS Routers

By default, Cisco IOS devices reject packets with zero giaddr and, by default, Cisco Catalyst switches use giaddr of zero when configured for DHCP snooping which is relaying the DHCPDISCOVER message to R2. The following debug output illustrates how DHCP snooping uses option 82, and also explains how the highlighted portion of the **show ip dhcp snooping** command is used:

[Click here to view code image](#)

```
show ip dhcp snooping.....
Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: c464.13fb.7780 (MAC)
```

```
DHCP_SNOOPING: received new DHCP packet from input interface
```

(GigabitEthernet1/0/19)

DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, input interface: Gi1/0/19,

MAC da: ffff.ffff.ffff, MAC sa: 1cdf.0f94.8063, IP da: 255.255.255.255, IP sa: 0.0.0.0, DHCP

ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr:

1cdf.0f94.8063

DHCP_SNOOPING: add relay information option.

DHCP_SNOOPING_SW: Encoding opt82 CID in vlan-mod-port format

DHCP_SNOOPING_SW: Encoding opt82 RID in MAC address format

DHCP_SNOOPING: binary dump of relay info option, length: 20 data:

0x52 0x12 0x1 0x6 0x0 0x4 0x0 0x64 0x1 0x13 0x2 0x8 0x0 0x6 0xC4 0x64 0x13 0xFB 0x77 0x80

DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (100)

In this exercise, R2 must be able to process the relay with giaddr 0 when using option 82, so the following command is needed on R2:

[Click here to view code image](#)

```
ip dhcp relay information trust-all
```

If SW1 configured for DHCP snooping had received the DHCP request with option 82 set and a giaddr of 0 from another relay through an untrusted port, it would drop the packet:

[Click here to view code image](#)

```
%DHCP_SNOOPING-5-DHCP_SNOOPING_NONZERO_GIADDR: DHCP_SNOOPING  
drop message with  
non-zero giaddr or option82 value on untrusted port
```

The following command will overcome this event:

[Click here to view code image](#)

```
ip dhcp snooping information option allow-untrusted
```

Or the **no ip dhcp snooping information option** command can be used if there are no other dependencies on option 82.

Solution and Verification for Exercise 5.3: Identifying Attacks with NetFlow and Mitigating Attacks Using Flexible Packet Matching

Skills Tested

- Understanding and interpreting Netflow data with respect to identifying potential attack patterns
- Implementing FPM as an attack mitigation strategy

Solution and Verification

Flexible packet matching is a stateless, static method of applying a granular packet matching criteria. Various attack vectors may be identified within single IP packets by examining IP protocol headers.

FPM configuration requires the following steps:

Step 1. Loading protocol headers: IP, UDP, TCP, ICMP

Step 2. Defining a protocol stack: match-all on Layer 1, Layer 2 and Layer 3 values

Step 3. Defining a traffic filter:

[Click here to view code image](#)

```
class-map type access-control: Identify IP packet of interest
policy-map type access-control: Apply actions to the matched packets
```

Step 4. Applying the policy:

[Click here to view code image](#)

```
service-policy type access-control on an interface
```

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**
- Nonzero/Non-null syntax appears in **violet**
- Variable syntax appears in **green**

To verify whether the FPM configuration is correct, initiate a **ping** to R7 with a size large enough to match the service policy. The **ping** should fail as packets are being matched by the FPM policy and dropped.

[Click here to view code image](#)

```
R6# ping 10.50.40.7 size 1200
Type escape sequence to abort.
Sending 5, 1200-byte ICMP Echos to 7.7.6.3, timeout is 2 seconds:
.....
```

After the **ping** test, verify whether the policy was matched correctly.

[Click here to view code image](#)

```
R7# show policy-map type access-control interface g0/1
GigabitEthernet0/1
```

```
Service-policy access-control input: ICMP
```

```
Class-map: ICMP (match-all)
```

```
 5 packets, 6070 bytes
```

```
 5 minute offered rate 2000 bps
```

```
Match: field IP protocol eq 1 next IP
```

Service-policy access-control : BIGIP

Class-map: **BIGIP** (match-all)

5 packets, 6070 bytes

5 minute offered rate 2000 bps

Match: field IP length gt 1000

drop

Class-map: class-default (match-any)

0 packets, 0 bytes

5 minute offered rate 0 bps, drop rate 0 bps

Match: any

Class-map: class-default (match-any)

29 packets, 2734 bytes

5 minute offered rate 0 bps, drop rate 0 bps

Match: any

Configuration

R7

[Click here to view code image](#)

```
load protocol system:/fpm/phdf/icmp.phdf
```

```
class-map type access-control match-all BIGIP  
match field IP length gt 1000
```

```
policy-map type access-control BIGIP  
class BIGIP  
drop
```

```
class-map type stack match-all ICMP  
match field IP protocol eq 1 next IP
```

```
policy-map type access-control ICMP  
class ICMP  
service-policy BIGIP
```

```
interface GigabitEthernet0/1  
service-policy type access-control input ICMP
```

Solution and Verification for Exercise 5.4: Application Protocol Protection

Skills Tested

- Understand application inspection on the Cisco ASA; specifically, DNS and the various options available for inspection of this protocol
- Configure application inspection as part of the global service policy

Solution and Verification

This exercise covers three concepts:

- Configuring a policy map for DNS application inspection that identifies the Authoritative Answer (AA) and Query/Response (QR) header flags in a DNS packet and logs these events; also, dropping any DNS packets that do not come from resolvers in the cisco.com domain.
- Matching DNS packets not coming from the cisco.com domain requires a regular expression (regex).
- Having a class map classify the packets of interest is not explicitly required because the inspection_class default is a class map in its own right.

For all verification syntax that follows:

- Required output appears in **red**
- Variable syntax appears in **green**

Change to context c1 on ASA1 because the DNS server is on the inside interface of c1. Verify that application inspection of DNS packets is applied to the global_service policy.

[Click here to view code image](#)

```
ASA1# changeto context c1
```

```
ASA1/c1# show service-policy global
```

Global policy:

Service-policy: global_policy

Class-map: inspection_default

Inspect: ftp, packet 0, drop 0, reset-drop 0

Inspect: h323 h225 _default_h323_map, packet 0, drop 0, reset-drop 0

tcp-proxy: bytes in buffer 0, bytes dropped 0

Inspect: h323 ras _default_h323_map, packet 0, drop 0, reset-drop 0

Inspect: ip-options _default_ip_options_map, packet 0, drop 0, reset-drop 0

Inspect: netbios, packet 0, drop 0, reset-drop 0

Inspect: rsh, packet 0, drop 0, reset-drop 0

Inspect: rtsp, packet 0, drop 0, reset-drop 0

tcp-proxy: bytes in buffer 0, bytes dropped 0

Inspect: skinny , packet 0, drop 0, reset-drop 0

tcp-proxy: bytes in buffer 0, bytes dropped 0

Inspect: esmtp _default_esmtp_map, packet 0, drop 0, reset-drop 0

```
Inspect: sqlnet, packet 0, drop 0, reset-drop 0
Inspect: sunrpc, packet 0, drop 0, reset-drop 0
    tcp-proxy: bytes in buffer 0, bytes dropped 0
Inspect: tftp, packet 0, drop 0, reset-drop 0
Inspect: sip , packet 0, drop 0, reset-drop 0
    tcp-proxy: bytes in buffer 0, bytes dropped 0
Inspect: xdmcp, packet 0, drop 0, reset-drop 0
Inspect: dns c1-dns, packet 580, drop 189, reset-drop 0
```

Verify whether the match criteria and actions applied to DNS inspection. Note that other policy parameters are enabled by default with DNS inspection: dns-guard, protocol-enforcement, and nat-rewrite.

[Click here to view code image](#)

```
ASA1/c1# show service-policy inspect dns
```

Global policy:

```
Service-policy: global_policy
```

```
Class-map: inspection_default
```

```
Inspect: dns c1-dns, packet 560, drop 189, reset-drop 0
```

```
dns-guard, count 13
```

```
protocol-enforcement, drop 0
```

```
nat-rewrite, count 0
```

```
id-randomization, count 547
```

```
match header-flag AA
```

```
log, packet 13
```

```
match header-flag QR
```

```
log, packet 9
```

```
match not domain-name regex domain
```

```
drop, packet 730
```

Verify whether the regular expression defined for cisco.com is “**cisco\.com**”.

The **test regex** command on the Cisco ASA is a useful tool for verifying regular expressions:

[Click here to view code image](#)

```
ASA1/c1# test regex cisco.com "cisco\.com"
```

```
INFO: Regular expression match succeeded.
```

Configuration

ASA1/c1

[Click here to view code image](#)

```
regex domain "cisco\.com"
```

```
policy-map type inspect dns c1-dns
parameters
```

```
id-randomization
match header-flag AA
log
match header-flag QR
log
match not domain-name regex domain
drop
!
policy-map global_policy
class inspection_default
inspect dns cl-dns
<.>
```

Section 6: Identity Management

In this section, you configure the Cisco Identity Services Engine (ISE) and Cisco Secure Access Control Server (ACS) to support identity-based network access and device management using RADIUS and TACACS+. Device command authorization on a Cisco IOS router is an important method for restricting device access and limiting the potential for attack or inadvertent misconfiguration. Identity-based network access is implemented using cut-through proxy on the Cisco ASA triggered by HTTP traffic. Cisco TrustSec is applied on the Cisco Catalyst switch along with the Cisco ISE through the use of MAC Authentication Bypass (MAB) and 802.1X authentication methods enforced on a switch port.

Solution and Verification for Exercise 6.1: Configure Router Command Authorization and Access Control

Skills Tested

- Understanding and configuring router access authentication and command authorization using TACACS+
- Implementing TACACS+ AAA services on a Cisco IOS Router and the CiscoSecure ACS

Solution and Verification

Device command authorization is used to manage the access that users and groups of users have to the features and functions available on a Cisco IOS Router, Cisco ASA, or Cisco Catalyst switch.

This exercise illustrates a fairly simple scenario of two groups of users that have two distinct command sets. Any command, exec, or configuration can be included in a command set. When a user logs in to a device, such as the router in this question, they are first authenticated via TACACS+. Then, as the user executes a command, it is compared to the authorized commands in the command set configured in CiscoSecure ACS, and a PASS (enable the command to be executed) or a FAIL (deny the command) is returned from the authentication server.

The authentication and authorization of the user and commands can be triggered by any or all of the following connections: console port or the aux port, or via any vty line (via telnet or SSH, for example).

Care must be taken applying authentication and authorization for router access via TACACS+ because any errors in the configuration, the use of the default method, or the unavailability of the authentication server with no specific fallback method can lock administrators out of the device. The **test aaa** commands are useful for verifying AAA access and can help identify any connectivity issues that might lock an administrator out of a device.

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**
- Variable syntax appears in **green**
- Troubleshooting syntax appears in **cyan**

Verify whether connectivity and user access have been configured correctly through the use of the **test aaa** commands:

[Click here to view code image](#)

```
R2# test aaa group tacacs+ admin cisco legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

```
R2# test aaa group tacacs+ netops cisco legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

```
R2# show tacacs
```

```
Tacacs+ Server      : 192.168.2.18/49
  Socket opens:      45
  Socket closes:     45
  Socket aborts:     0
  Socket errors:     0
  Socket Timeouts:   0
Failed Connect Attempts: 0
  Total Packets Sent: 77
  Total Packets Recv: 77
```

From R4, establish a Telnet connection to R2 and verify that you are prompted for the password and the enable password, and that command authorization is not configured. You should not be prompted for a username.

```
R4# telnet 10.50.100.2
Trying 10.50.100.2 ... Open
```

User Access Verification

Password: **cisco**

R2> **enable**

Password: **cisco**

R2#

Verify that authentication and authorization for user netops is limited to only the **show crypto** commands and **clear crypto session** command. This will need to be the second Telnet session established to R2.

[Click here to view code image](#)

R7# **telnet 10.50.100.2**

Trying 10.50.100.2 ... Open

Username: **netops**

Password: **cisco**

R2#

R2# **configure t**

Command authorization failed.

R2# **show ip route**

Command authorization failed.

R2# **show crypto ipsec sa** -> should display output, for example:

interface: Ethernet0/0.1

Crypto map tag: Ethernet0/0.1-OSPF-MAP, local addr FE80::A8BB:CCFF:FE00:7A00

IPsecv6 policy name: OSPFv3-500

protected vrf: (none)

local ident (addr/mask/prot/port): (FE80::/10/89/0)

remote ident (addr/mask/prot/port): (::/0/89/0)

Next, verify authentication and authorization for the admin user. This group has full access to all commands.

[Click here to view code image](#)

R4# **telnet 10.50.100.2**

Trying 10.50.100.2 ... Open

User Access Verification

Password: **cisco**

```

R2> enable
Password: cisco
R2#
R2#
! Second Telnet session (username/password should be prompted)
R7# telnet 10.50.100.2
Trying 10.50.100.2 ... Open

Username: admin
Password: cisco

R2#
R2# configure t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#

```

ACS Solution

Step 1. Verify users and groups as shown in [Figure 1a-4](#) and [Figure 1a-5](#):

- a. User admin assigned to the admin group.
- b. User netops assigned to the netops group.

The screenshot shows the 'Internal Users' configuration page in Cisco ACS. It features a table with columns for Status, User Name, Identity Group, and Description. The 'admin' user is assigned to the 'All Groups:admin' group, and the 'netops' user is assigned to the 'All Groups:netops' group. Other users listed include 'Guest', 'R7.cisco.com', 'userap1', and 'userap2'.

<input type="checkbox"/>	Status	User Name	Identity Group	Description
<input type="checkbox"/>	●	admin	All Groups:admin	
<input type="checkbox"/>	●	Guest	All Groups:Guest	
<input type="checkbox"/>	●	netops	All Groups:netops	
<input type="checkbox"/>	●	R7.cisco.com	All Groups	
<input type="checkbox"/>	●	userap1	All Groups:Auth-Proxy1	
<input type="checkbox"/>	●	userap2	All Groups:Auth-Proxy2	

Figure 1a-4 Cisco ACS User to Group Assignments

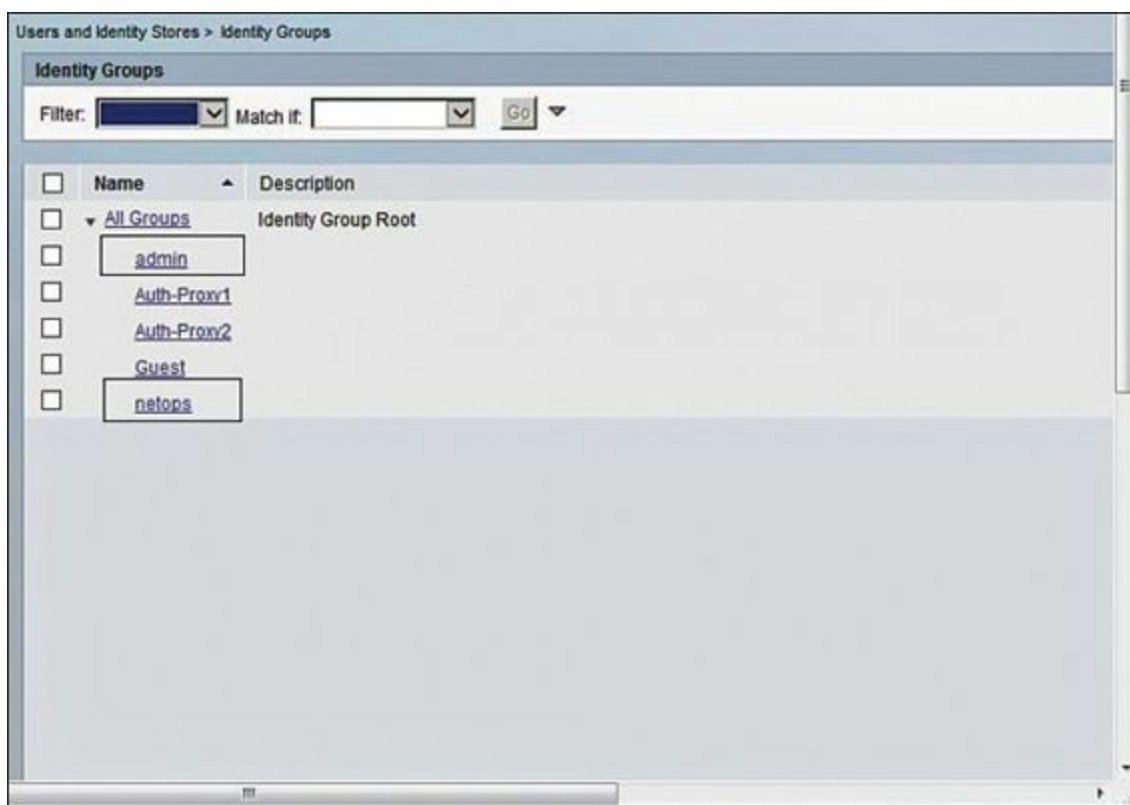


Figure 1a-5 Cisco ACS Identity Groups

Step 2. Configure the command authorization policy and shell profile for the admin group:

- a. Max privilege level assigned is 15. Defined under shell profile common tasks (see [Figure 1a-6](#)).



Figure 1a-6 Cisco ACS Admin Privilege Level

- b. This group is granted unrestricted command access by defining a blank command table and checking the box beside Permit Any Command That Is in the Table Below. This is the inverse of the logic used in versions of Cisco Secure ACS prior to 5.X (see [Figure 1a-7](#)).

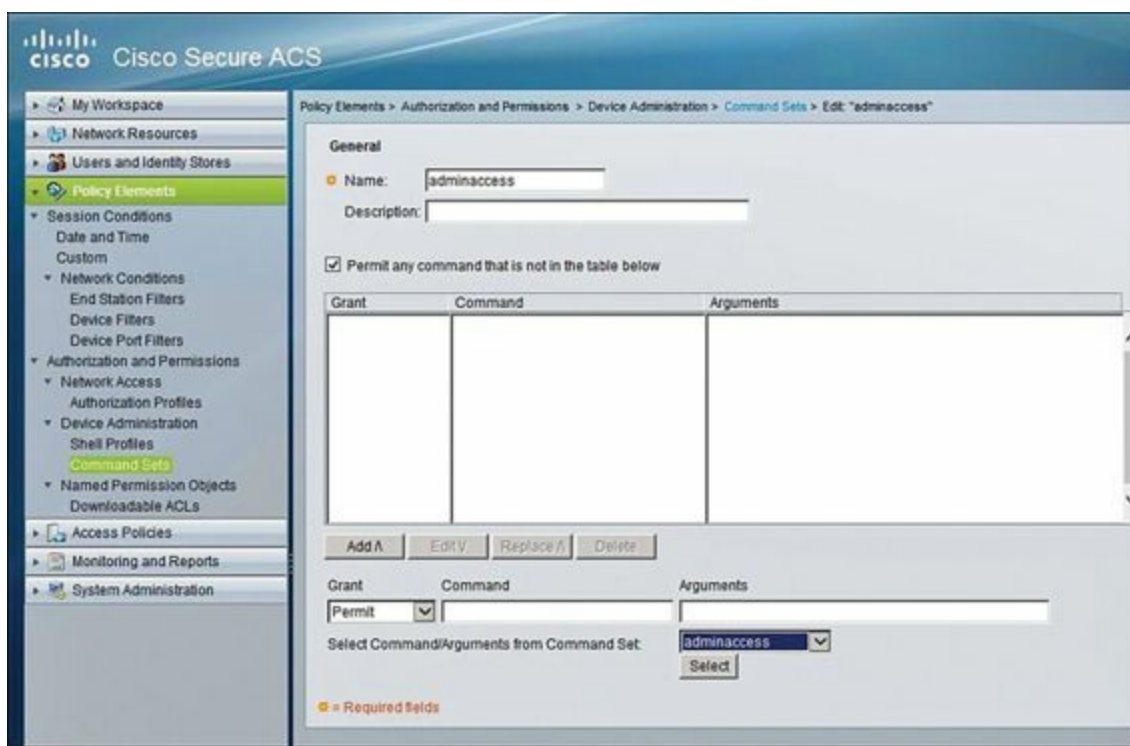


Figure 1a-7 Cisco ACS Admin User Command Permissions

Step 3. Verify that the command authorization set is applied as a Device Management Authorization Rule for the admin group.

Note

To allow the shell profile to be used as the access permission criteria for device command sets, the shell profile result must be available for assignment under Device Administration Authorization Policies. From Access Policies > Authorization, select the Customize button at the bottom-right side of the display, as shown in [Figure 1a-8](#).

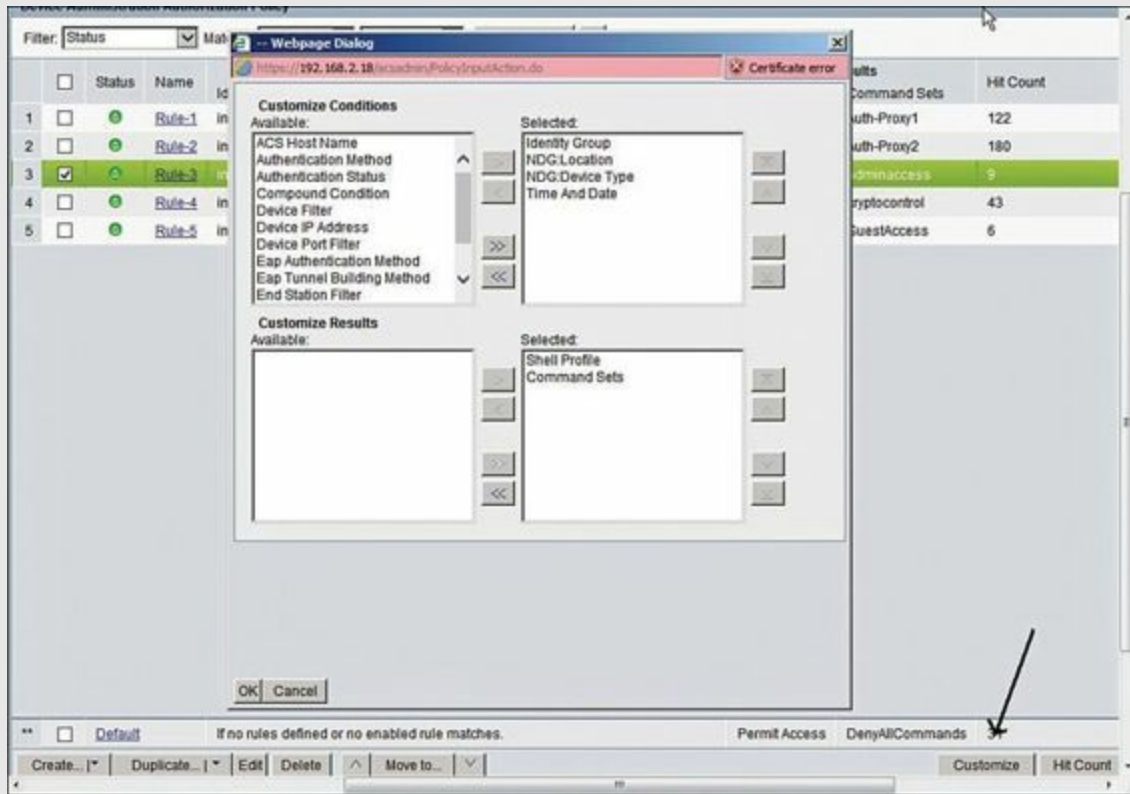


Figure 1a-8 Cisco ACS Customization of Access Policy Results

Shell Profiles can then be assigned under Results, as shown in [Figure 1a-9](#). The admin identity group is assigned privilege level 15 (via the shell profile), and this is associated with the adminaccess command set, which allows access to all router commands.

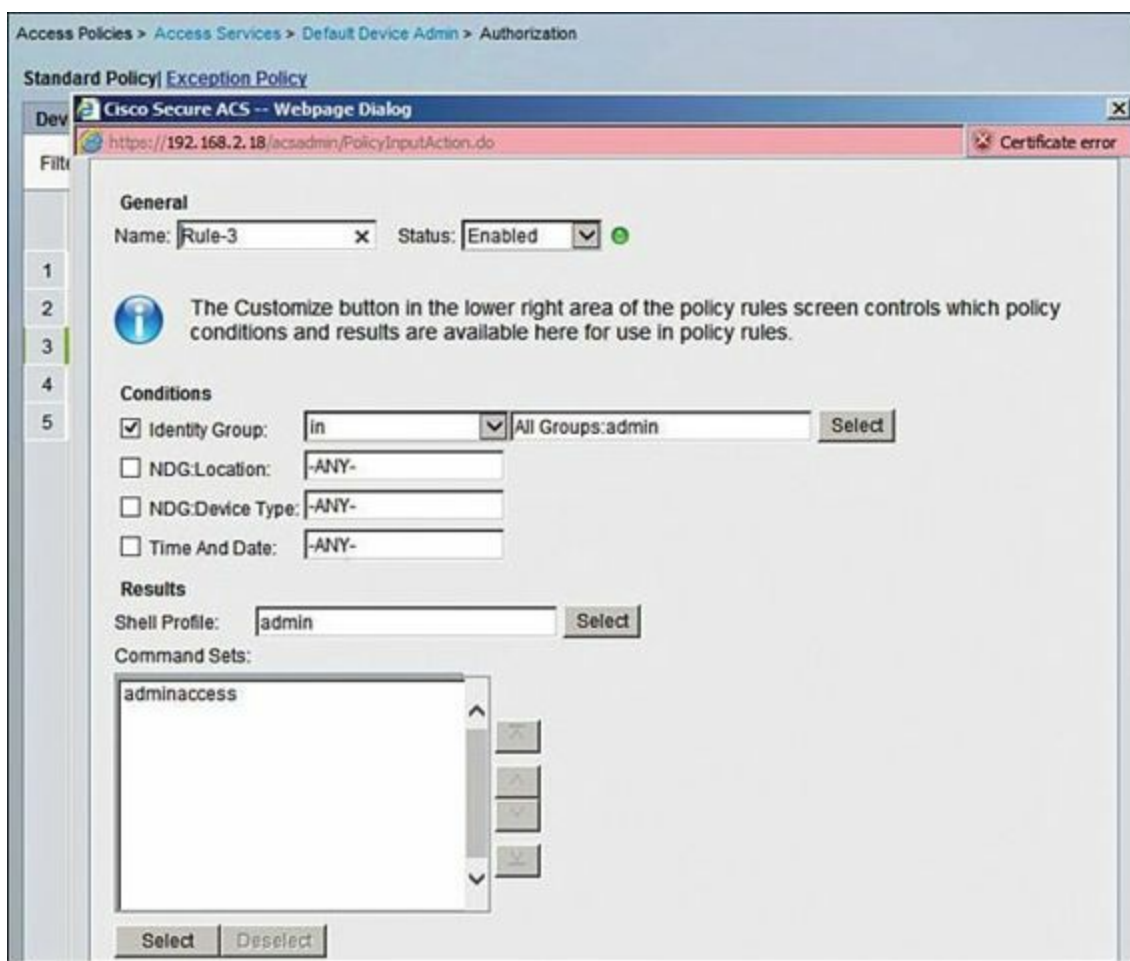


Figure 1a-9 Cisco ACS Assigning Shell Profiles and Command Sets to an Authorization Profile

Step 4. Verify the command authorization policy for the netops group:

- a. Max privilege level assigned is 1. This is defined under shell profile tasks and attributes, as shown in [Figure 1a-10](#).

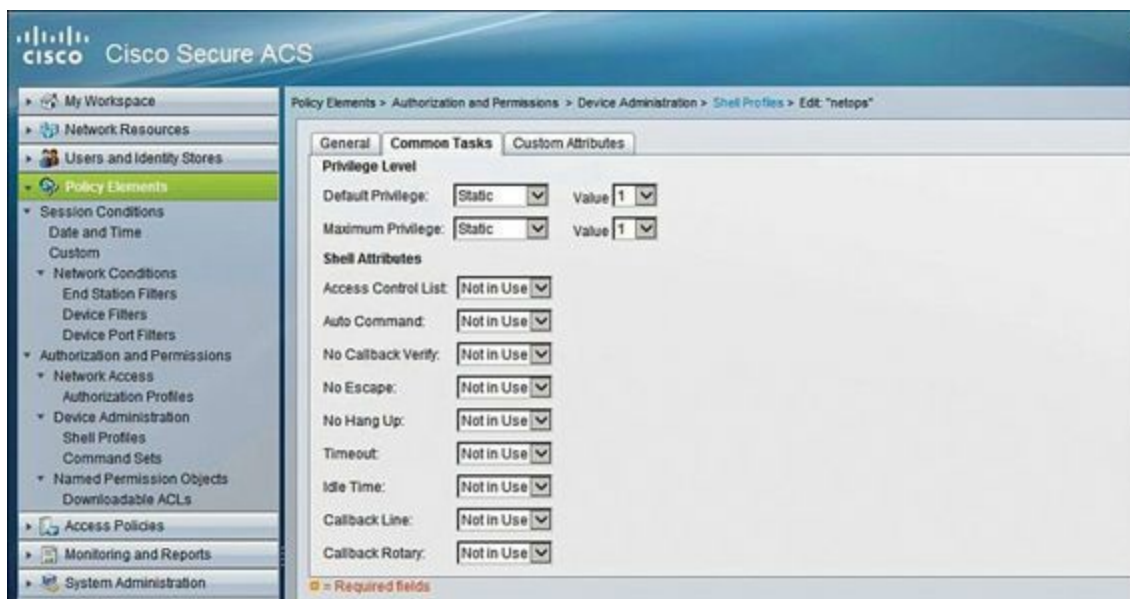


Figure 1a-10 Cisco ACS Netops Privilege Level

- b. Verify whether the command authorization allows only the following commands, and that nonspecified commands are not permitted (see [Figure 1a-11](#)):

[Click here to view code image](#)

enable

show crypto (permit any subcommands)

clear crypto session (permit any subcommands)

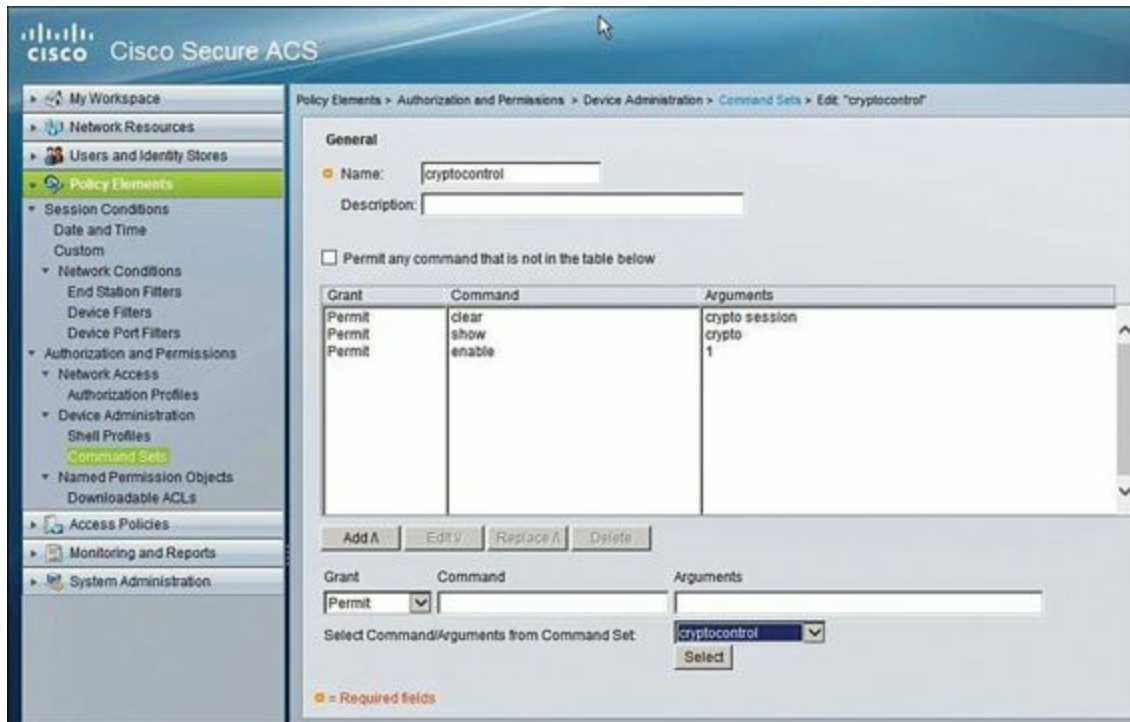


Figure 1a-11 Cisco ACS Netops Command Permissions

Step 5. Verify whether the command authorization set is applied as a device management authorization rule for the netops group, as shown in [Figure 1a-12](#). The netops identity group is assigned privilege level 1 (via the shell profile), and this is associated with the cryptocontrol command set, which enables access to specific commands only.

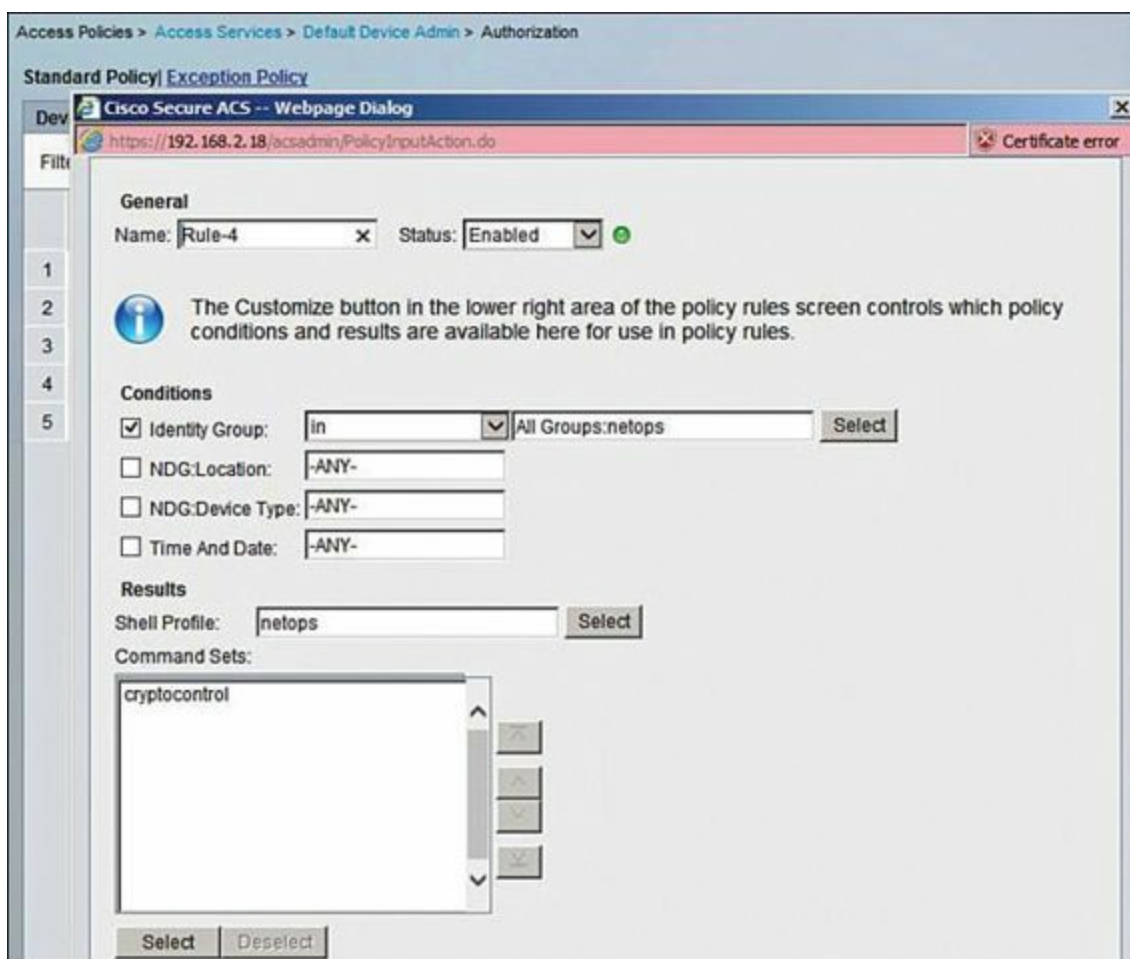


Figure 1a-12 *Cisco ACS Netops Device Authorization*

Configuration

asa1/c1

[Click here to view code image](#)

```
access-list 101 permit tcp any host 192.168.2.18 eq 49
```

R2

[Click here to view code image](#)

```
aaa new-model
!
!
aaa authentication login telnet2 group tacacs+ local
aaa authentication login no-auth none
aaa authentication login line-auth line
! Required for configuration commands
aaa authorization config-commands
aaa authorization exec no-auth none
aaa authorization exec exec-auth group tacacs+
aaa authorization commands 1 telnet2 group tacacs+ none
aaa authorization commands 15 telnet2 group tacacs+ none
```

```
username cisco password cisco
!  
<...>  
!  
tacacs-server host 192.168.2.18  
tacacs-server key cisco123  
!  
<...>  
line con 0  
 login authentication no-auth  
line aux 0  
line vty 0  
 password cisco  
 authorization exec no-auth  
 login authentication line-auth  
line vty 1  
 password cisco  
 authorization commands 1 telnet2  
 authorization commands 15 telnet2  
 authorization exec exec-auth  
 login authentication telnet2  
line vty 2 4  
 password cisco  
 authorization exec no-auth  
 login authentication line-auth  
!  
<...>
```

Tech Notes

Tracing the Command Authorization Process

The following debugs outline the process involved for router command authorization. This follows authentication of the user netops via TACACS+, which happens as an independent transaction from authorization.

- **debug aaa authorization**
- **debug tacacs**

The first debug shows an attempt to use a command for which the user is not authorized:

```
R7# telnet 10.50.100.2  
Trying 10.50.100.2 ... Open
```

```
Username: netops  
Password: cisco
```

```
R2#
```

R2# show ip route

The following command is captured at the VTY line:

[Click here to view code image](#)

```
*Aug 24 22:50:50.975: AAA/AUTHOR/CMD: tty3 (745938549) user='netops'  
*Aug 24 22:50:50.975: tty3 AAA/AUTHOR/CMD (745938549): send AV service=shell  
*Aug 24 22:50:50.975: tty3 AAA/AUTHOR/CMD (745938549): send AV cmd=show  
*Aug 24 22:50:50.975: tty3 AAA/AUTHOR/CMD (745938549): send AV cmd-arg=ip  
*Aug 24 22:50:50.975: tty3 AAA/AUTHOR/CMD (745938549): send AV cmd-arg=route  
*Aug 24 22:50:50.975: tty3 AAA/AUTHOR/CMD (745938549): send AV cmd-arg=<cr>
```

The following command is intercepted by the list telnet2, which uses TACACS+ to send the command and user credentials to the ACS server:

[Click here to view code image](#)

```
*Aug 24 22:50:50.975: tty3 AAA/AUTHOR/CMD(745938549): found list "telnet2"  
*Aug 24 22:50:50.975: tty3 AAA/AUTHOR/CMD (745938549): Method=tacacs+ (tacacs+)  
*Aug 24 22:50:50.976: AAA/AUTHOR/TAC+: (745938549): user=netops  
*Aug 24 22:50:50.976: AAA/AUTHOR/TAC+: (745938549): send AV service=shell  
*Aug 24 22:50:50.976: AAA/AUTHOR/TAC+: (745938549): send AV cmd=show  
*Aug 24 22:50:50.976: AAA/AUTHOR/TAC+: (745938549): send AV cmd-arg=ip  
*Aug 24 22:50:50.976: AAA/AUTHOR/TAC+: (745938549): send AV cmd-arg=route  
*Aug 24 22:50:50.976: AAA/AUTHOR/TAC+: (745938549): send AV cmd-arg=<cr>  
*Aug 24 22:50:50.976: TAC+: using previously set server 192.168.2.18 from group  
tacacs+  
*Aug 24 22:50:50.976: TAC+: Opening TCP/IP to 192.168.2.18/49 timeout=5  
*Aug 24 22:50:50.977: TAC+: Opened TCP/IP handle 0xF1D55260 to 192.168.2.18/49  
using source 0.0.0.0  
*Aug 24 22:50:50.977: TAC+: Opened 192.168.2.18 index=1  
*Aug 24 22:50:50.977: TAC+: 192.168.2.18 (745938549) AUTHOR/START queued
```

The following is the response FAIL from ACS:

[Click here to view code image](#)

```
*Aug 24 22:50:51.184: TAC+: (745938549) AUTHOR/START  
processed  
*Aug 24 22:50:51.184: TAC+: (745938549): received author  
response status = FAIL  
Command authorization failed.
```

This debug output reflects the use of an authorized command:

```
R7# telnet 10.50.100.2  
Trying 10.50.100.2 ... Open
```

```
Username: netops  
Password: cisco
```

R2#

```
R2# show crypto ipsec sa
```

The following command is captured at the VTY line:

[Click here to view code image](#)

```
*Aug 24 22:54:04.229: AAA/AUTHOR/CMD: tty3 (1720594819)
user='netops'
*Aug 24 22:54:04.229: tty3 AAA/AUTHOR/CMD (1720594819): send
AV service=shell
*Aug 24 22:54:04.229: tty3 AAA/AUTHOR/CMD (1720594819): send
AV cmd=show
*Aug 24 22:54:04.229: tty3 AAA/AUTHOR/CMD (1720594819): send
AV cmd-arg=crypto
*Aug 24 22:54:04.229: tty3 AAA/AUTHOR/CMD (1720594819): send
AV cmd-arg=ipsec
*Aug 24 22:54:04.229: tty3 AAA/AUTHOR/CMD (1720594819): send
AV cmd-arg=sa
*Aug 24 22:54:04.229: tty3 AAA/AUTHOR/CMD (1720594819): send
AV cmd-arg=<cr>
```

The following command is intercepted by the list telnet2, which uses TACACS+ to send the command and user credentials to the ACS server:

[Click here to view code image](#)

```
*Aug 24 22:54:04.229: tty3 AAA/AUTHOR/CMD(1720594819): found list "telnet2"
*Aug 24 22:54:04.229: tty3 AAA/AUTHOR/CMD (1720594819): Method=tacacs+ (tacacs+)
*Aug 24 22:54:04.229: AAA/AUTHOR/TAC+: (1720594819): user=netops
*Aug 24 22:54:04.229: AAA/AUTHOR/TAC+: (1720594819): send AV service=shell
*Aug 24 22:54:04.229: AAA/AUTHOR/TAC+: (1720594819): send AV cmd=show
*Aug 24 22:54:04.229: AAA/AUTHOR/TAC+: (1720594819): send AV cmd-arg=crypto
*Aug 24 22:54:04.229: AAA/AUTHOR/TAC+: (1720594819): send AV cmd-arg=ipsec
*Aug 24 22:54:04.229: AAA/AUTHOR/TAC+: (1720594819): send AV cmd-arg=sa
*Aug 24 22:54:04.229: AAA/AUTHOR/TAC+: (1720594819): send AV cmd-arg=<cr>
*Aug 24 22:54:04.229: TAC+: using previously set server 192.168.2.18 from group
tacacs+
*Aug 24 22:54:04.229: TAC+: Opening TCP/IP to 192.168.2.18/49 timeout=5
*Aug 24 22:54:04.230: TAC+: Opened TCP/IP handle 0xF2108628 to 192.168.2.18/49
using source 0.0.0.0
*Aug 24 22:54:04.230: TAC+: Opened 192.168.2.18 index=1
*Aug 24 22:54:04.231: TAC+: 192.168.2.18 (1720594819) AUTHOR/START queued
```

The response is PASS from the ACS server, and command outputs from **show crypto ipsec sa** are displayed.

[Click here to view code image](#)

*Aug 24 22:54:04.436: TAC+: (1720594819) AUTHOR/START processed

*Aug 24 22:54:04.436: TAC+: (1720594819): received author response status =
PASS_ADD

interface: Ethernet0/0.1

Crypto map tag: Ethernet0/0.1-OSPF-MAP, local addr FE80::A8BB:CCFF:FE00:7A00

Understanding AAA and Login on the Router Lines

The following is a review of how various AAA and login configuration commands impact router access. Note that the default Console and VTY configuration has no AAA or access control.

- In this example, the Console line default is applied, which is no authentication or password required. VTY lines are configured for password only.

```
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password cisco
login
```

This configuration results in the user being prompted for just a password.

Example:

```
R1> telnet 1.1.1.1
Trying 1.1.1.1 ... Open
```

User Access Verification

Password: **cisco**

- When configuring **aaa new-model** globally:

```
R1(config)#aaa new-model
```

```
R1# exit
```

This results in no authentication required at the console; however, a username and password are now required for VTY access.

Example:

R1 con0 is now available

Press RETURN to get started.

```
R1>
```

```
R1> telnet 1.1.1.1
Trying 1.1.1.1 ... Open
```

User Access Verification

Username: **admin**

Password: **pword**

- When the default method for authentication is applied to all lines, VTY and the console will all require a username and password.

[Click here to view code image](#)

```
R1(config)# aaa authentication login default local
```

```
R1(config)# end
```

Example:

```
R1# telnet 1.1.1.1
```

```
Trying 1.1.1.1 ... Open
```

User Access Verification

Username: **admin**

Password: **pword**

R1 con0 is now available

Press RETURN to get started.

User Access Verification

Username: **admin**

Password: **pword**

Test AAA Commands

As shown in the exercise, **test aaa** is recommended to ensure connectivity exists between the network access device and the authentication server. Here are examples of using this command on various Cisco platforms.

IOS Version

[Click here to view code image](#)

```
test aaa group aaa-group username password legacy
```

Output:

[Click here to view code image](#)

```
Attempting authentication test to server-group aaa group using aaa protocol  
User was successfully authenticated.
```

Note that you can specify a group of servers to check or a specific server in a group.

ASA Version

[Click here to view code image](#)

```
test aaa-server authentication aaa-server-name
Server IP Address or name: ip-addr
Username: cisc0
Password: *****
INFO: Attempting Authentication test to IP address (timeout: 12 seconds)
ERROR: Authentication Rejected: AAA failure
test aaa-server authentication aaa-server-name
Server IP Address or name: ip-addr
Username: cisco
Password: *****
INFO: Attempting Authentication test to IP address (timeout: 12 seconds)
INFO: Authentication Successful
```

AAA Accounting

Cisco IOS also supports **test aaa accounting** and requires the configuration of some or all of the following parameters:

[Click here to view code image](#)

```
test aaa accounting ?
  alloc_fid      Allocate flow id
  alloc_uid      Allocate AAA unique id
  dealloc_fid    Deallocate flow id
  dealloc_uid    Deallocate unique id
  giga           Giga-word accounting test
  init          Initialize test aaa accounting infrastructure
  reset         Reset the variables
  send_acct_start Send accounting start
  send_acct_stop Send accounting stop
  send_authen_req Send authen req
```

Solution and Verification for Exercise 6.2: Configure Cut-Through Proxy on ASA2 Using TACACS+

Skills Tested

- Configuring Auth-Proxy authentication and authorization on the Cisco ASA.
- Implementing TACACS+ AAA services on the Cisco ASA and CiscoSecure ACS

Solution and Verification

Cut-through proxy is a per-user method of providing access through the Cisco ASA (and Cisco IOS routers). Even if an access list enables specific traffic flows, cut-through proxy will intercept certain applications—for example, FTP, Telnet, and HTTP—and apply per-user authentication and authorization before permitting or denying the traffic.

Both TACACS+ and RADIUS can be used for cut-through proxy, although for this question the former is required. With TACACS+, the authentication request will happen independently of the authorization of the traffic being intercepted. Traffic to be authorized will be sent as a service authorization request to the AAA server and compared to a command set in the same way that command authorization is handled.

After a user is authenticated and authorized, this information is stored in the uauth cache on the ASA. The information in the uauth cache is how to verify the solution for this question.

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**
- Nonzero/non-null syntax appears in **violet**
- Variable syntax appears in **green**
- Troubleshooting syntax appears in **cyan**

From your client PC, initiate an HTTP connection to 10.50.40.7. If cut-through proxy is correctly implemented on ASA2, the username/password login screen will appear. Enter the credentials `userap1/cisco` and check the uauth cache to verify the configuration on CiscoSecure ACS.

[Click here to view code image](#)

```
ASA2# show uauth
           Current  Most Seen
Authenticated Users    1      1
Authen In Progress    0      1
user 'userap1' at 192.168.2.25, authorized to:
  port 10.50.40.7/http
  absolute timeout: 0:05:00
  inactivity timeout: 0:00:00
```

From your client PC, initiate an HTTP connection to 10.50.30.4. If cut-through proxy is correctly implemented on ASA2, the username/password login screen will appear. Enter the credentials `userap2/cisco` and check the uauth cache to verify the configuration on CiscoSecure ACS.

[Click here to view code image](#)

```
ASA2# show uauth
           Current  Most Seen
Authenticated Users    1      1
Authen In Progress    0      1
user 'userap2' at 192.168.2.25, authorized to:
  port 10.50.30.4/http
  absolute timeout: 0:05:00
  inactivity timeout: 0:00:00
```

CiscoSecure ACS Configuration

Step 1. Verify users and group assignments as shown in [Figure 1a-13](#).

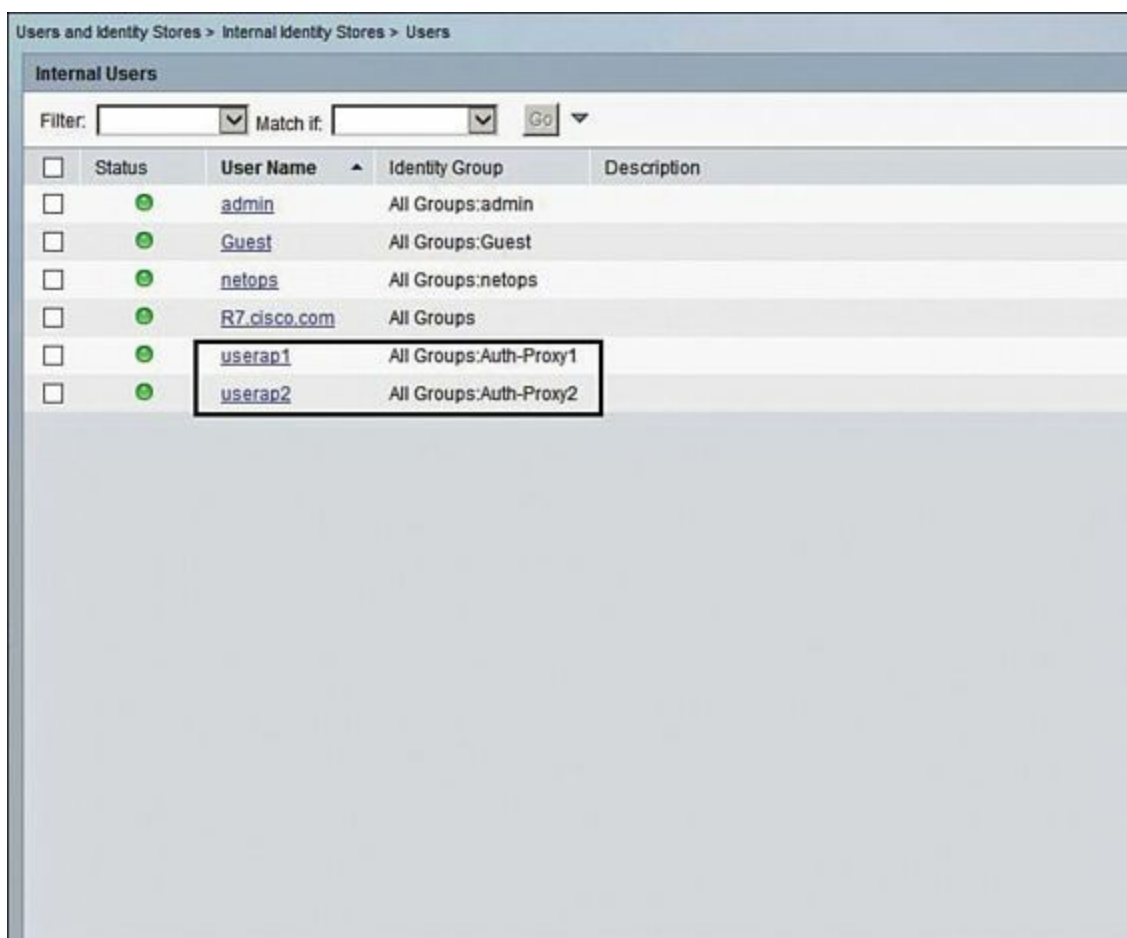


Figure 1a-13 Cisco ACS User to Group Assignments

Step 2. A command set is required for each group, allowing HTTP access to 10.50.40.7 for group Auth-Proxy1 and 10.50.30.4 for group Auth-Proxy2. The command set for group Auth-Proxy1 is shown in [Figure 1a-14](#). In the case of group Auth-Proxy2, the command set must permit HTTP to 10.50.30.4.

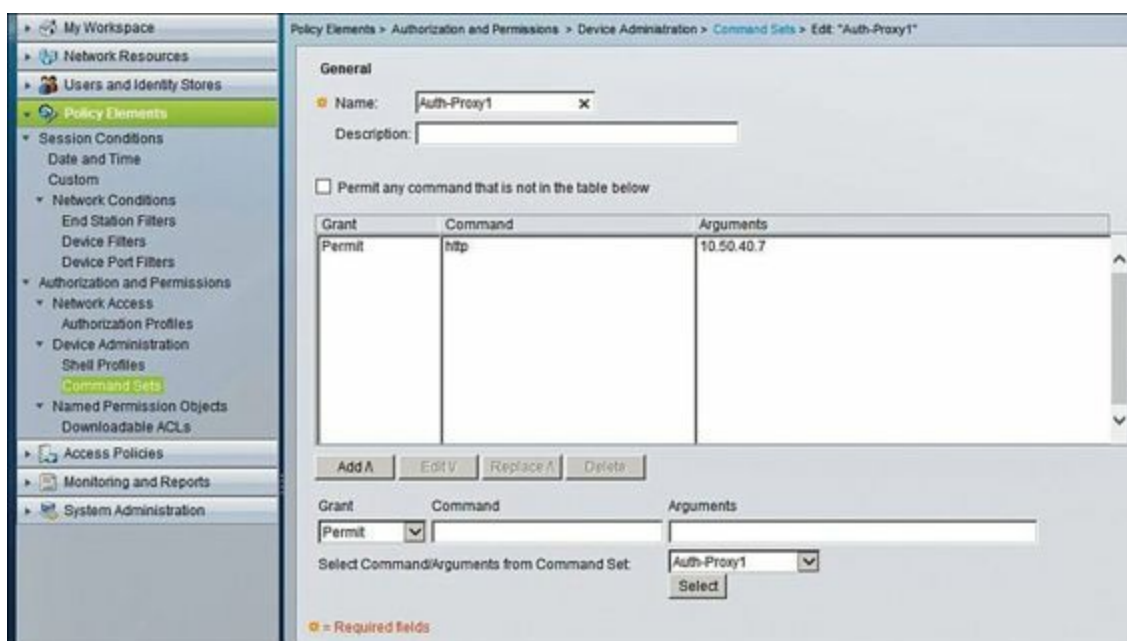


Figure 1a-14 Cisco ACS Group Auth-Proxy1 Command Sets

Step 3. Apply the command sets as device access policy authorization rules for group Auth-Proxy1 (see [Figure 1a-15](#)) and group Auth-Proxy2.

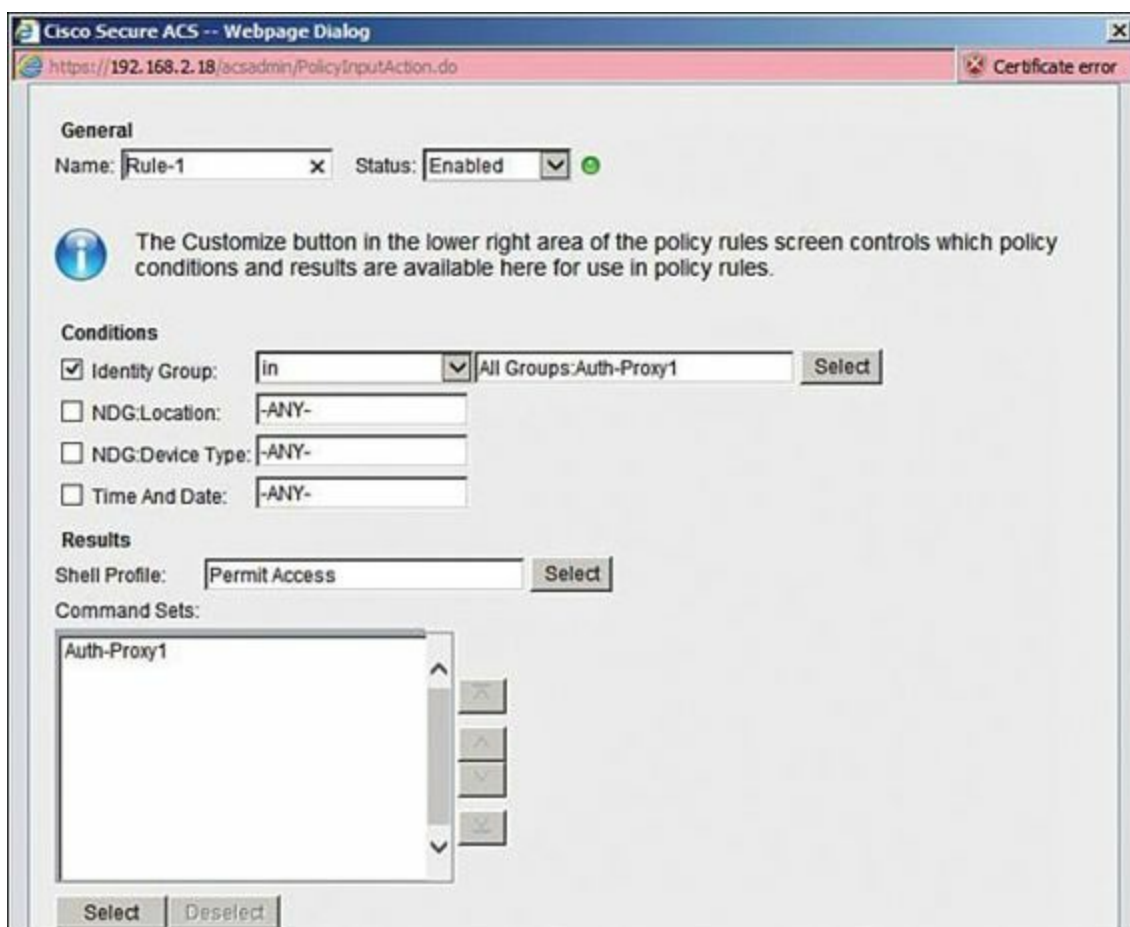


Figure 1a-15 Cisco ACS Network Authorization

Configuration

! ASA2

[Click here to view code image](#)

```

aaa-server tacacs protocol tacacs+
aaa-server tacacs (outside) host 192.168.2.18 key cisco123
access-list auth-proxy extended permit tcp any 10.50.0.0 255.255.0.0 eq www
aaa authentication match auth-proxy outside tacacs
aaa authorization match auth-proxy outside tacacs

```

Tech Notes

Using RADIUS, authentication and authorization are done in the same transaction; therefore, any authorization attributes will need to be bundled with the Access-Accept packet. For RADIUS, dynamic ACLs (DACL) are used to define the authorization permissions.

The following examples illustrate how RADIUS-based per-user authentication and authorization information is stored in the uauth cache on the Cisco ASA:

[Click here to view code image](#)

```

ASA# show uauth

```

	Current	Most Seen
Authenticated Users	1	1
Authen In Progress	0	1

user 'userap1' at 192.168.2.25, authenticated
access-list #ACSACL#-IP-CutThrough-4b208394

absolute timeout: 0:05:00
inactivity timeout: 0:00:00

ASA# **show access-list #ACSACL#-IP-CutThrough-4b208394**
permit tcp any host 10.50.40.7 eq www

Solution and Verification for Exercise 6.3: Configure Support for MAB/802.1X for Voice and Data VLANs

Skills Tested

- Understanding and configuring Identity-Based Networking Services (IBNS) on the Cisco Catalyst switch and Cisco ISE
- Configuring Flexible Authentication (FlexAuth) options for IBNS
- Implementing RADIUS AAA services on a Cisco Catalyst switch and the Cisco ISE

This exercise requires the consolidation of a number of features and products into a solution for network access based on identity.

In [part A](#), the Cisco IP Phone must be authenticated by MAC Authentication Bypass (MAB). (Note that Cisco IP Phones can also be configured for 802.1X authentication.) MAB requires no configuration on the phone itself, and the authentication process is driven by the configuration on the switchport with RADIUS as the transport for AAA between the authenticator (switch) and authentication server (Cisco ISE). The ISE must have the MAC address of the phone added to the internal endpoint list, which is then referenced during MAB authentication. An authorization profile must be defined for this device type. (ISE has a default Cisco-IP-Phone device group and default authorization policy for profiled Cisco IP Phones.) The authorization policy configured on the Cisco ISE will apply access permissions. The result is a match with the following outputs:

[Click here to view code image](#)

```
show auth sess int g1/0/14
```

```
Interface: GigabitEthernet1/0/14
```

```
MAC Address: 0023.eb54.1109
```

```
IP Address: Unknown
```

```
User-Name: 00-23-EB-54-11-09
```

```
Status: Authz Success
```

```
Domain: VOICE
```

```
Security Policy: Should Secure
```

```
Security Status: Unsecure
```

```
Oper host mode: multi-auth
```

```
Oper control dir: both
```

```
Authorized By: Authentication Server
```

```
Vlan Policy: 9
```

```
ACS ACL: xACSACLx-IP-PERMIT_ALL_TRAFFIC-4fe7f797
```

Session timeout: 3600s (local), Remaining: 3509s

Timeout action: Reauthenticate

Idle timeout: N/A

Common Session ID: C0A842420000002E003D9546

Acct Session ID: 0x00000030

Handle: 0x3C00002F

Part B builds on the AAA/RADIUS and switchport configuration on SW2 but requiring that the Cisco ISE be configured to support 802.1X authentication for the PC client. A user identity is required for the user connecting via the PC. In addition, an authorization policy containing the network access permissions must be defined and applied to a group that has the client user as a member. Verification of the permissions applied to the authenticated connection is done via the following command:

[Click here to view code image](#)

```
sho auth sess int g1/0/14
```

```
Interface: GigabitEthernet1/0/14
```

```
MAC Address: 000c.290d.0c22
```

```
IP Address: Unknown
```

```
User-Name: Test-PC
```

```
Status: Authz Success
```

```
Domain: DATA
```

```
Security Policy: Should Secure
```

```
Security Status: Unsecure
```

```
Oper host mode: multi-auth
```

```
Oper control dir: both
```

```
Authorized By: Authentication Server
```

```
Vlan Policy: 99
```

```
ACS ACL: xACSACLx-IP-DATA_VLAN_DACL-503d6911
```

```
Session timeout: 3600s (local), Remaining: 3585s
```

```
Timeout action: Reauthenticate
```

```
Idle timeout: N/A
```

```
Common Session ID: C0A842420000008B37CC94A2
```

```
Acct Session ID: 0x000000B4
```

```
Handle: 0x0F00008C
```

This exercise also requires the implementation of FlexAuth such that MAB should be the authentication method attempted first on the switchport, but 802.1X authentication takes priority in terms of access permissions. Verification of order and priority is done by checking the runnable methods list on the port; for example:

Runnable methods list:

```
Method State
```

```
mab Authc Success
```

```
dot1x Not run
```

Verification: Part A

For all verification syntax that follows:

- Required output appears in **red**
- Variable syntax appears in **green**

Verify whether the actual outputs of the verification commands match those outlined in the question. Note that dot1x has not been run because MAB was the first authentication method specified via FlexAuth authentication ordering. Even though FlexAuth authentication priority ordering is 802.1X, then MAB, the IP Phone is not configured to attempt 802.1X, so it will be authorized to use the permissions associated with MAB.

[Click here to view code image](#)

```
SW2# show authentication session int g1/0/14
  Interface: GigabitEthernet1/0/14
  MAC Address: 0023.eb54.1109
  IP Address: Unknown
  User-Name: 00-23-EB-54-11-09 -> matches IP phone MAC address above
  Status: Authz Success
  Domain: VOICE
  Security Policy: Should Secure
  Security Status: Unsecure
  Oper host mode: multi-auth
  Oper control dir: both
  Authorized By: Authentication Server
    ACS ACL: xACSACLx-IP-PERMIT_ALL_TRAFFIC-4fe7f797 -> should be the
IP_PERMIT_ALL_TRAFFIC acl matched below
  Vlan Policy: 9
  Session timeout: 3600s (local), Remaining: 3509s
  Timeout action: Reauthenticate
  Idle timeout: N/A
  Common Session ID: C0A842420000002E003D9546
  Acct Session ID: 0x00000030
  Handle: 0x3C00002F
```

Runnable methods list:

Method	State
mab	Authc Success
dot1x	Not run

The access list downloaded from the ISE as a dynamic ACL should be installed as a per-user access list on SW2. This is how you verify the permissions configured on the ISE from the switch CLI.

[Click here to view code image](#)

```
SW2# sho access-list
Extended IP access list xACSACLx-IP-PERMIT_ALL_TRAFFIC-4fe7f797 (per-user)
 10 permit ip any any
```

Finally, ensure whether the Cisco IP Phone could register with its Call Manager (the CME functionality has been preconfigured on R6):

[Click here to view code image](#)

```
R6# show ephone summary
hairpin_block:
ephone-1[0] Mac:0023.EB54.1109 TCP socket:[1] activeLine:0 whisperLine:0
REGISTERED
mediaActive:0 whisper_mediaActive:0 startMedia:0 offhook:0 ringing:0 reset:0
reset_sent:0 debug:0
IP:10.50.9.6 * 7965 keepalive 10609 music 0

Max 10, Registered 1, Unregistered 0, Deceased 0 High Water Mark 11, Sockets 1
ephone_send_packet process switched 0
```

Verification: Part B

For all verification syntax that follows:

- Required output appears in **red**
- Variable syntax appears in **green**

Verify whether the actual outputs of the verification commands match those outlined in the question. Note that the client has been authenticated and authorized using 802.1X as the authentication method.

[Click here to view code image](#)

```
SW2# show authentication session int g1/0/14
Interface: GigabitEthernet1/0/14
MAC Address: 000c.290d.0c22
IP Address: Unknown
User-Name: Test-PC
Status: Authz Success
Domain: DATA
Security Policy: Should Secure

Security Status: Unsecure
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: 99
ACS ACL: xACSACLx-IP-DATA_VLAN_DACL-503d6911 -> should be the
IP_DATA_VLAN_ACL acl
Session timeout: 3600s (local), Remaining: 3585s
Timeout action: Reauthenticate
Idle timeout: N/A
Common Session ID: C0A842420000008B37CC94A2
Acct Session ID: 0x000000B4
Handle: 0x0F00008C
```

Runnable methods list:

Method	State
mab	Failed over
dot1x	Authc Success

The access list downloaded from the ISE as a dynamic ACL should be installed as a per-user access list on SW2. This is how you verify the permissions configured on the ISE from the switch CLI.

[Click here to view code image](#)

```
SW2# show access-list
```

```
Extended IP access list xACSACLx-IP-DATA_VLAN_DACL-503d6911 (per-user)  
10 permit ip any any
```

Configuration

SW2

[Click here to view code image](#)

```
aaa new-model  
aaa authentication dot1x default group radius  
aaa authorization network default group radius  
aaa accounting dot1x default start-stop group radius
```

```
dot1x system-auth-control
```

```
interface GigabitEthernet1/0/14  
switchport access vlan 99  
switchport mode access  
switchport voice vlan 9  
ip access-group ACL_DEFAULT in  
authentication host-mode multi-auth  
authentication open  
authentication order mab dot1x  
authentication priority dot1x mab  
authentication port-control auto  
authentication periodic  
mab  
dot1x pae authenticator  
spanning-tree portfast
```

```
ip access-list extended ACL-DEFAULT  
remark DHCP  
permit udp any eq bootpc any eq bootps  
remark DNS  
permit udp any any eq domain  
remark Ping
```

```
permit icmp any any
remark PXE / TFTP
permit udp any any eq tftp
remark Drop all the rest
deny ip any any log
```

ASA1/c1

[Click here to view code image](#)

```
access-list 101 extended permit udp any any eq 1812
access-list 101 extended permit udp any any eq 1813
```

```
access-group 101 in interface outside
```

Cisco ISE Configuration

Step 1. Add the MAC address of the IP Phone to the Endpoint database, as shown in [Figure 1a-16](#).

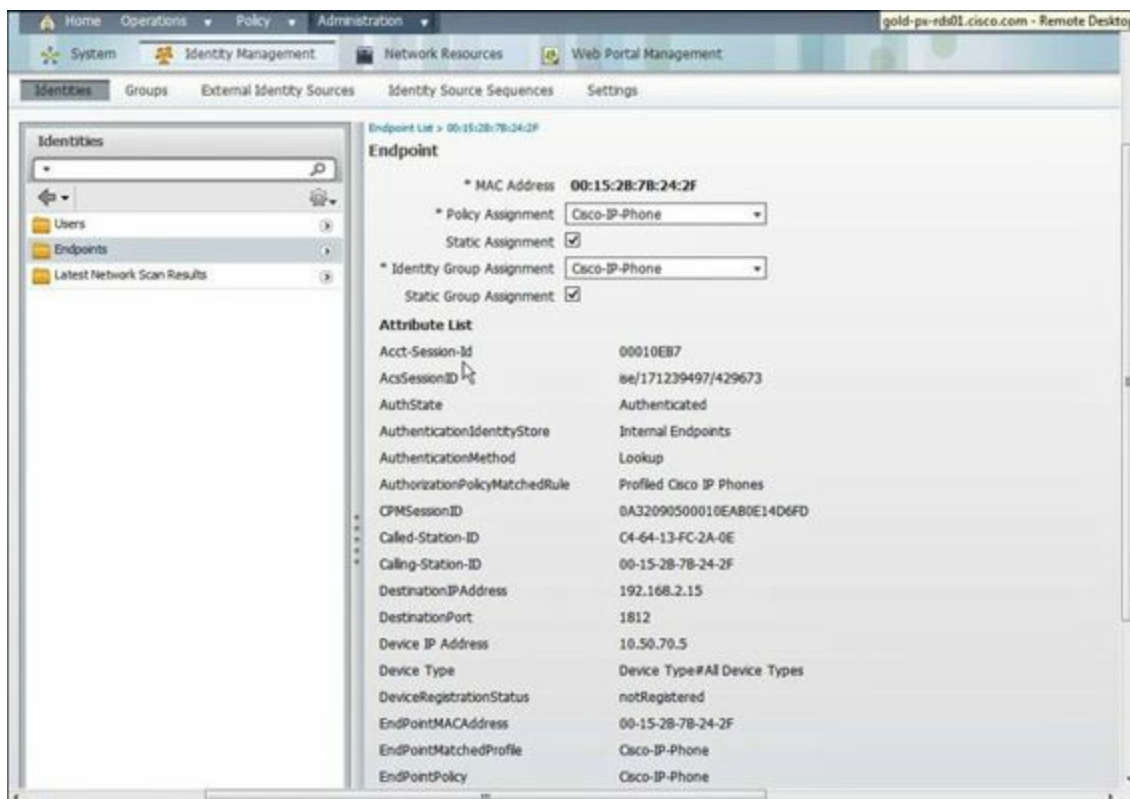


Figure 1a-16 Cisco ISE Endpoint Database

Step 2. Create a group on ISE called Test-PC-Group. The Test-PC will become a member of this group, as shown in [Figure 1a-17](#).

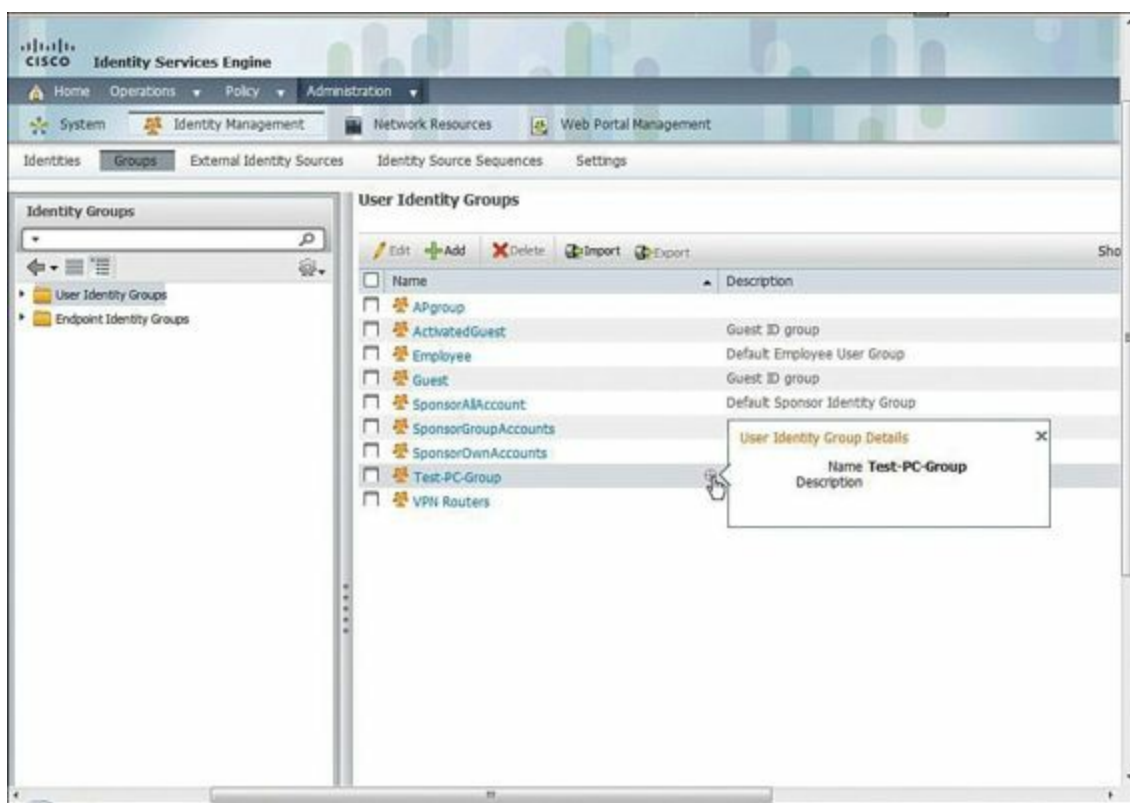


Figure 1a-17 Cisco ISE User Identity Groups

Step 3. Create the user Test-PC, as shown in [Figure 1a-18](#).

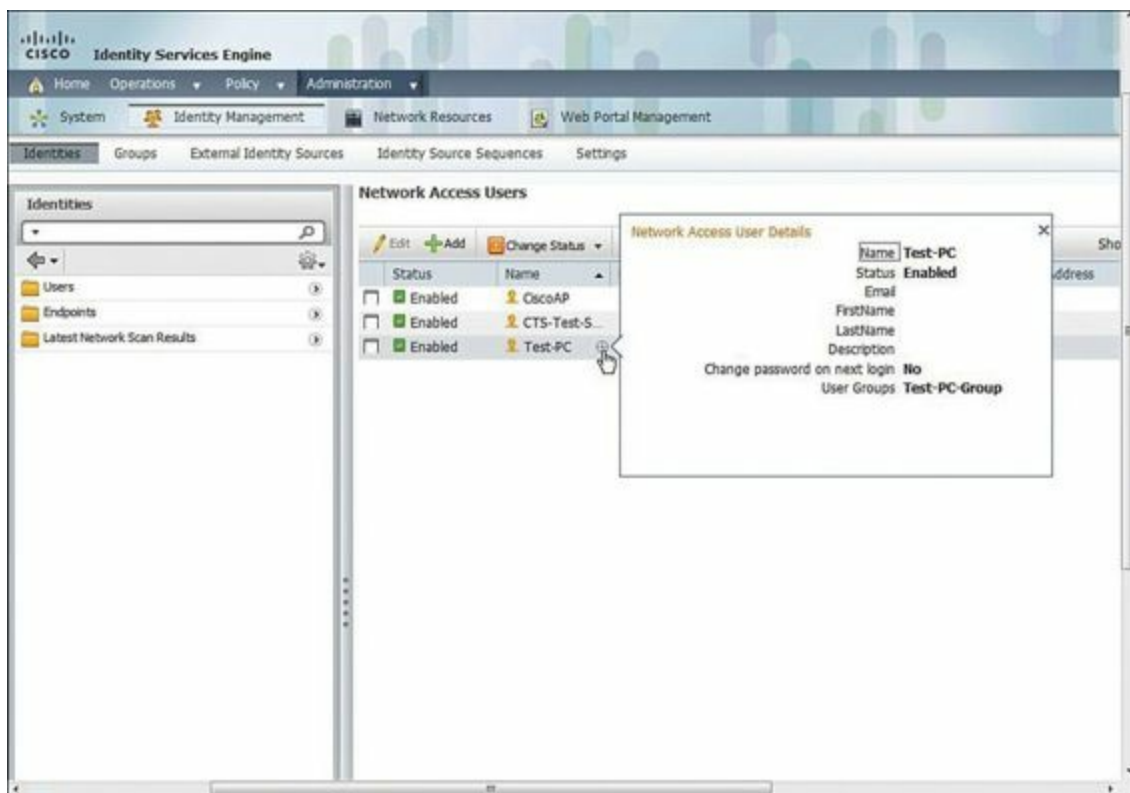


Figure 1a-18 Cisco ISE Creating Network Access Users

Step 4. Verify the authorization profile for the DATA_VLAN, as shown in [Figure 1a-19](#). This profile will be applied to the Test-PC.

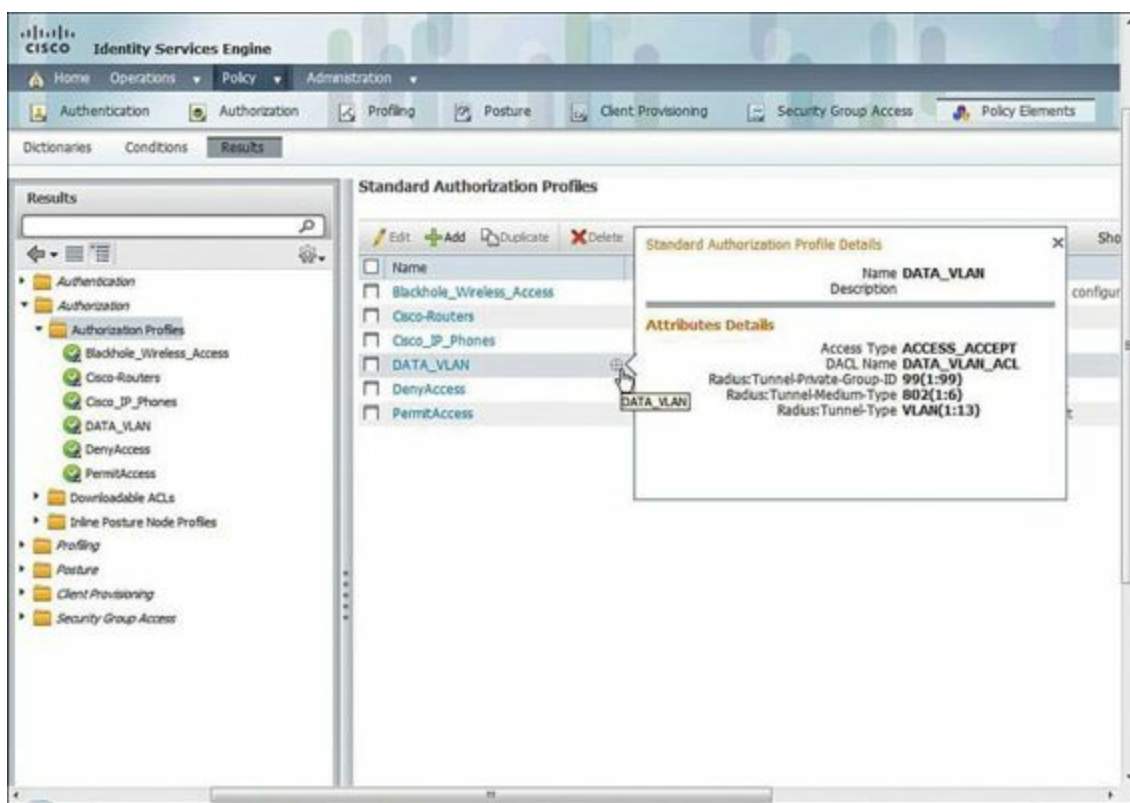


Figure 1a-19 Cisco ISE Creating a Standard Authorization Profile for the Test-PC

Step 5. Verify the authorization profile for the IP Phone, as shown in [Figure 1a-20](#).

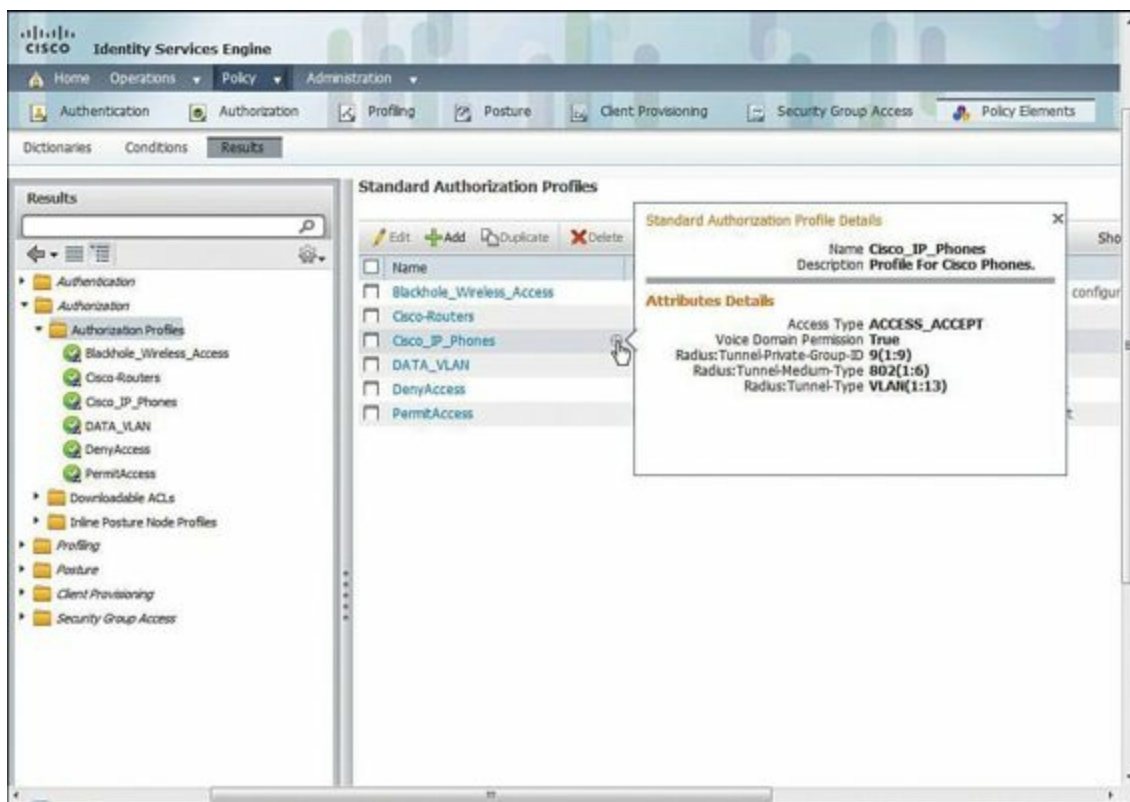


Figure 1a-20 Cisco ISE Creating a Standard Authorization Profile for the IP Phone

Step 6. Ensure that MAB is attempted for the IP Phone first; the Test-PC will be authenticated using 802.1X, as shown in [Figure 1a-21](#).

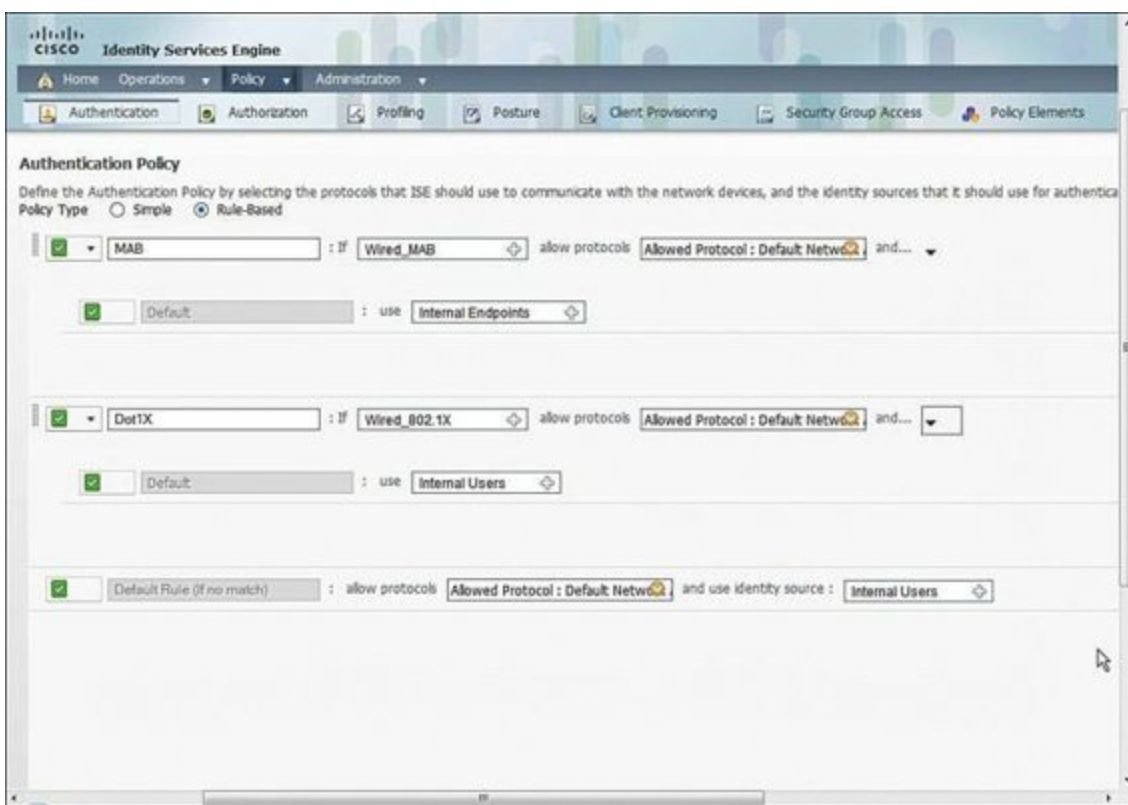


Figure 1a-21 Cisco ISE Authentication Method Policy Order

Step 7. Authorization policies link the authenticated entity with their authorization profile, as defined previously. [Figure 1a-22](#) shows the authorization policy rules for the Test-PC and the IP Phone.

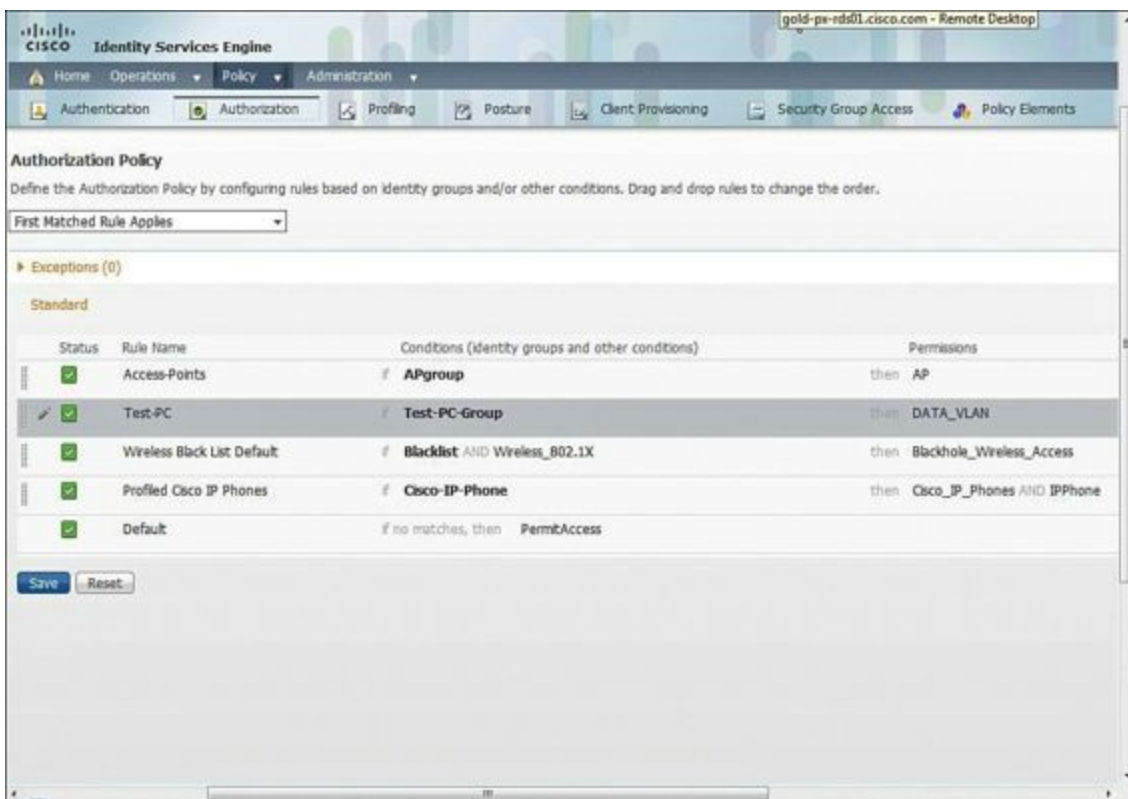


Figure 1a-22 Cisco ISE Authorization Policy Enforcement

Tech Notes

By default, the Cisco Catalyst switches configured for TrustSec authentication services will attempt 802.1X on a switchport first, even if MAB has been configured on that port. If the host attached to that switchport does not support 802.1X, it will have to wait until this authentication method fails before MAB is attempted.

Flexible authentication (FlexAuth) enables the administrator to configure an authentication method order and priority on a switchport to change the default behavior. FlexAuth authentication order dictates what authentication method to try first. Authentication priority defines the level of access the port will provide if multiple authentication method successes are possible. This exercise has the following:

[Click here to view code image](#)

```
authentication order mab dot1x
```

This forces all devices through MAB as soon as their MAC address is determined on the switchport. If MAB fails, any available supplicant should begin 802.1X.

[Click here to view code image](#)

```
authentication priority dot1x mab
```

If the device passes MAB, it is assigned the level of authorization associated with that authentication method. Because 802.1X authentication takes priority, a supplicant will initiate this method (whether MAB has been successful or not) and, if 802.1X succeeds, the level of authorization associated with 802.1X authentication will be granted to that device. If MAB has succeeded for this device, the initial level of authorization granted by this method will be overridden by 802.1X authorization access.

An issue that could occur with this priority ordering is if a client fails 802.1X. Even if MAB is successful, a supplicant may continue to retry 802.1X, which will continue to fail and the device will never be granted access on that switchport beyond some initial level.

In this exercise, we could also have specified

[Click here to view code image](#)

```
authentication priority mab dot1x
```

This would work well for both the IP Phone (MAB) and PC client (802.1X), provided the PC MAC address was not found in the MAB database. As a result, the PC might be given insufficient access to network resources as MAB authorization is applied and 802.1X will not be attempted.

This ordering has another caveat; namely, do not allow unknown MAC addresses to pass MAB authenticated via a catch-all policy. Again as discussed earlier, 802.1X failure can be an issue for clients that might continue to try this method per the configured FlexAuth options.

To help eliminate the possibility of policy loops, FlexAuth also enables local WebAuth to be specified as an acceptable authentication method or as a fallback action. Fallback actions avoid continuously looping through the list of authentication methods and can be used for scenarios where guest credentials via WebAuth are accepted, or unauthenticated clients are placed into restrictive VLANs.

Here are two examples:

- In this example, WebAuth will be used as a fallback method if MAB and 802.1X fail. Local WebAuth will ignore an 802.1X supplicant's EAPoL-Start commands and break the authentication loop.

[Click here to view code image](#)

```
authentication order mab dot1x web-auth
authentication priority dot1x mab web-auth
authentication event fail action next-method
authentication fallback web-auth
```

- Another way to break an authentication loop is to configure an event fail action that will place a device in a VLAN with restricted network access and again throttle the EAPoL-Start commands from an 802.1X supplicant.

[Click here to view code image](#)

```
authentication order mab dot1x
authentication priority dot1x mab
authentication event fail action authorize vlan 111
```

Part III: Practice Lab 2

Practice Lab 2

Section 1: Perimeter Security

In Lab 1, you initialized perimeter security services and configured some fundamental features. This section adds more advanced features on the Cisco Adaptive Security Appliance (ASA), including configuring IPv6, botnet traffic filtering and redundancy, and management services. There is also an exercise using the Cisco IOS zone-based firewall (ZFW), which has replaced context-based access control (CBAC) as the firewall solution on Cisco IOS routers. ZFW has been updated to allow support for Cisco TrustSec and security group tagging, and this will be incorporated into the exercise in this lab.

Exercise 1.1: Configure a Redundant Interface on ASA2

A redundant physical interface must be added to ASA2 to provide a high-availability solution for the *outside* interface. Combine interface GigabitEthernet0/0 and interface GigabitEthernet0/1 to create the logical interface Redundant1.

Ensure that all connectivity is in place by checking the routing tables on ASA2 and its neighbors.

Note

A user-defined shared MAC address is not required.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 1.1: Configure a Redundant Interface on ASA2.](#)”

Exercise 1.2: SSH Management Authentication and Local Command Authorization on ASA1

Secure management access via SSH is required on ASA1. This will allow **local** command authorization to be implemented on a per-user basis. Complete this exercise using the parameters in [Table 2-1](#).

Parameter	Value
Privilege Level 15 username/password	cisco/cisco
Privilege Level 5 username/password	support/cisco
Privilege Level 5 command set	show xlate, show route, changeto
SSH Key Modulus	768 bits
SSH Access ACL and session idle-timeout	permit 192.168.1.0/24 idle-timeout 5 minutes permit 192.168.2.0/24 idle-timeout 1 minute
Domain	cisco.com

Table 2-1 *SSH and Command Requirements*

You may use any names for policy constructs.

To verify your solution, connect to ASA1 from SW1 using SSH.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 1.2: SSH Management Authentication and Local Command Authorization on ASA1.](#)”

Exercise 1.3: Configuring Advanced Network Protection on the ASA

The following three tasks require the configuration of various network protection features available on the Cisco ASA.

Task 1: Botnet Traffic Filtering on ASA1

Create a botnet filter with DNS snooping enabled using the details in [Table 2-2](#).

Parameter	Value
Blacklist	server.ccie.com
Whitelist	10.10.110.0/24, 10.10.120.0/24
DNS snooping	Enabled
DNS server for ccie.com domain	R2 (10.50.100.2)

Table 2-2 Botnet Filtering Parameters

To verify your solution, use the following commands and check your outputs on ASA1, including the generated syslog messages:

```
ASA1/c2# logging console 6
```

```
R6# telnet server.ccie.com
```

```
R6# telnet 10.10.110.1
```

Note

R6 has been preconfigured with R2 as a name server. Also, you should disable console logging after you verify your solution.

Task 2: Threat Detection on ASA2

Basic threat detection is on by default on the Cisco ASA when configured in single-context routed mode. Enable advanced threat detection statistics for ports and protocols on ASA2.

Task 3: IP Audit on ASA1

Basic Intrusion Prevention Sensor (IPS) support is required on ASA/c1 to provide an additional layer of protection against common attacks and to collect audit logs on various events.

Informational events seen on the inside should be logged, and attacks coming from the outside should be dropped.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 1.3: Configuring Advanced Network Protection on the ASA.](#)”

Exercise 1.4: Configure IPv6 on ASA2

IPv6 addressing and EIGRPv6 routing has been configured on R7, R3, and R4. To exchange routing information between these three routers, IPv6 traffic must transit ASA2.

Configure IPv6 addressing using the information in [Table 2-3](#). This configuration will be required to complete [Exercise 3.1](#) in [Section 3](#).

Interface	IPv6 Address
GigabitEthernet0/2	2001:db8:40::20/64
GigabitEthernet0/3	2001:db9:30::20/64

Table 2-3 IPv6 Details

In addition, ensure that ASA2 *will not* respond to rRouter solicitation (RS) messages.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 1.4: Configure IPv6 on ASA2](#).”

Exercise 1.5: Cisco IOS Zone-Based Firewall with Support for Secure Group Tagging

R6 is an integral device in the lab topology, and a ZFW is required to inspect and monitor traffic flows through this device. An audit was performed, and the ZFW requirements outlined in [Table 2-4](#) and [2-5](#). Use this information to build a ZFW configuration on R6.

Interface	Zone Name
Ethernet0/0	inside
Ethernet0/1	outside

Table 2-4 Zone Details

Direction	Traffic Selectors	Protocol/Port	Action
out-in	—	ISAKMP, GDOI	pass
	10.50.0.0/16, 10.50.0.0/16	UDP/4500, GRE, ESP	pass
	—	ICMP, DNS, NTP, Telnet, RADIUS, TACACS, HTTP, HTTPS	inspect
	SGT4, SGT5	ICMP, UDP	inspect
in-out	any, any		inspect
	—	ISAKMP, GDOI	pass
	10.50.0.0/16, 10.50.0.0/16	UDP/4500, GRE, ESP	pass
	—	L4: HTTP	inspect
	—	L7: HTTP portmisuse (tunneling)	log, reset

Table 2-5 Traffic Analysis Summary

Note

- Ensure that all protocols currently transiting and terminating on R6 are not disrupted and are explicitly detailed in the policy match criteria.
- You may use any names for any other configuration constructs not explicitly defined in [Tables 2-4](#) and [2-5](#).
- This exercise has a dependency on the completion of [Exercise 6.2](#) and [6.3](#) in this lab.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 1.5: Cisco IOS Zone-Based Firewall with Support for Secure Group Tagging.](#)”

Section 2: Intrusion Prevention and Content Security

This section covers more advanced tasks applicable to the (IPS) and Web Services Appliance (WSA). Configuring custom signatures and defining event action overrides are important signature-tuning techniques applicable to the Cisco IPS. In Lab 1, you initialized the WSA and configured Web Cache Communication Protocol (WCCP) Transparent proxy service using the ASA as the WCCP server. In this section, you add user authentication to this scenario, and then incorporate guest services.

Exercise 2.1: Configuring Custom Signatures on the Cisco IPS

Sensor

The IPS sensor was provisioned in Lab 1. In this exercise, you must define three custom signatures and apply them to the virtual sensors specified.

Custom Signature to Track OSPF TTL

[Table 2-6](#) defines a signature required to monitor OSPF packets across area 0 to ensure that only packets with a Time to Live (TTL) of 255 are seen. This implies that only OSPF packets that have transited one (direct connection) or two hops should be seen in area 0.

Parameter	Value
Signature ID	64000
Trigger	OSPF packets with a TTL of 255
Event-Action	produce-verbose-alert
Alert-severity	Medium
Signature-definition	sig0

Table 2-6 *OSPF TTL Signature*

Note

Realistically, the signature would trigger for packets that exceed the minimum accepted TTL, and the event-action to take would be to deny the traffic.

Custom Signature to Identify and Deny Large ICMP Packets

In [Exercise 5.3](#) in Lab 1, flexible packet matching (FPM) was used to identify large Internet Control Message Protocol (ICMP) packets sourced from RFC 1918 addresses. Create a custom signature to achieve the same result using the parameters in [Table 2-7](#).

Parameter	Value
Signature ID	65,000
Trigger	ICMP packets sized 1000–5000 bytes sourced from RFC 1918 addresses
Event-Action	log-attacker-packets
Alert-severity	High
Signature-definition	sig0

Table 2-7 *Large ICMP Packet Signature*

Custom Signature to Identify and Deny an ICMP Flood Attack

A signature is required to protect critical hosts, such as the DNS/LDAP server at 192.168.2.25, from ICMP flood attacks. Use the parameters in [Table 2-8](#) to create the custom signature.

Parameter	Value
Signature ID	62,000
Trigger	ICMP ECHO packets sent at a rate of 100 pkts/sec
Event-Action	produce-alert and deny-packet-inline
Alert-severity	High
Signature-definition	sig1

Table 2-8 *ICMP Flood Signature*

Additionally, create an event-action-rules policy to be implemented on VS1 that satisfies the requirements in [Table 2-9](#).

Parameter	Value
Mission-Critical Target	192.168.2.25
Risk Rating Range	90–100
Event Action Override	produce-alert and log-attacker-packets and deny-attacker-inline

Table 2-9 *Event-Action-Rules Policy*

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 2.1: Configuring Custom Signatures on the Cisco IPS Sensor](#).”

Exercise 2.2: Enable Support for HTTPS on the Cisco WSA

The WSA has been configured to process HTTP and HTTPS packets redirected by ASA1 using WCCPv2 Transparent Proxy in Lab 1. To transparently proxy HTTPS requests, the WSA must be configured as a HTTPS proxy. Complete this task using a self-generated root certificate on the WSA with the parameters outlined in [Table 2-10](#).

Parameter	Value
Common Name	wsa
Organization	cisco.com
Organizational Unit	CCIE
Country	US
Basic Constraints	Not Critical
Lifetime	24 months

Table 2-10 WSA HTTP Proxy Parameters

To verify your solution, enable the HTTP secure server on R4 and, using the browser on the Test-PC, connect to <https://10.50.30.4>.

Note

Make sure the Invalid Certificate Handling option for an unrecognized root authority/issuer is set to monitor, or the WSA will reject R4's self-signed certificate.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 2.2: Enable Support for HTTPS on the Cisco WSA](#).”

Exercise 2.3: Enable User Authentication for Transparent Proxy Using LDAP

The WSA is processing redirected HTTP and HTTPS packets from ASA1 using transparent proxy. This exercise requires the addition of user authentication via Lightweight Directory Access Protocol (LDAP) before redirected traffic HTTP/HTTPS will be forwarded for the user.

Use the parameters in [Table 2-11](#) to complete this task.

Parameter	Value
LDAP Realm	CCIELAB
LDAP Server	192.168.2.25
User Base DN	dc=cisco, dc=com
Query Credentials Bind DN	CISCO\ccie
Group Authorization	None
Authentication Order	Above Global Policy
Surrogate Type	Session Cookies
Global Authentication Settings	Credential Encryption Enabled

Table 2-11 *User Authentication Parameters*

To verify your solution, use the Test-PC browser from the 192.168.2.0 subnet to connect to any HTTP server in the network, and you should receive a prompt from the WSA for username/password credentials as shown in [Figure 2-1](#).



Figure 2-1 *WSA User Prompt*

Note

- Ensure that users are added to the Active Directory service running on the win2k server at 192.168.2.25.
- Make sure the Test-PC browser is using the correct name-server; in this case, 192.168.2.25.
- When connecting to multiple HTTP servers that might be behind ASA2, which is configured for auth-proxy, you will have to clear the uauth cache between each connection unless you are using multiple Test-PCs.
- The use of session cookies as the surrogate type will force user authentication each time the browser is closed and reopened. If you use an IP address or persistent cookie, reauthentication will not occur until the surrogate timeout has been reached. Surrogates are important because they indicate what source state is used to distinguish between new and current sessions.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 2.3: Enable User Authentication for Transparent Proxy Using LDAP.](#)”

Exercise 2.4: Guest User Support on the Cisco WSA

Carrying on from [Exercise 2.3](#), create an identity on the WSA to support guest users who do not need to provide username/password credentials for authentication. HTTP/HTTPS traffic will still be redirected to the WSA; however, unauthenticated users will be granted guest access only by applying a guest access policy.

The guest access policy should allow access to 10.50.50.5 and block all other sites on the 10.50.0.0/16 network explicitly.

To verify your solution, close the browser on the Test-PC. Reopen the browser and connect to <http://10.50.50.5>. The WSA will prompt for the username/password; enter guest. This will fail authentication but grant guest access. You should be able to connect to the SW2 website.

[Click here to view code image](#)

HTTP server history:

local-ipaddress:port	remote-ipaddress:port	in-bytes	out-bytes	end-time
10.50.50.5:80	192.168.2.50:64008	3547	251686	19:55:45
10.50.50.5:80	192.168.2.50:9612	4118	270121	19:55:45

Next, connect to any other 10.50.0.0 HTTP server and the connection should be blocked, as shown in [Figure 2-2](#).



Figure 2-2 *Browser Blocked Connection Notification*

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 2.4: Guest User Support on the Cisco WSA](#).”

Section 3: Secure Access

This section presents some more-complex solutions for secure network access. The legacy remote access virtual private networks (VPN) using IKEv1 in Lab 1 have been replaced with FlexVPN using IKEv2. In one exercise, we look at site-to-site remote access using RADIUS tunnel attributes and Cisco Secure Access Control Server (ACS) to provide the IKEv2 preshared key. Another FlexVPN scenario involves remote access client to server, which is the new version of EZVPN that uses IKEv2 for Security Association (SA) negotiation and remote attribute distribution (config mode). This section also covers the use of IPv6 with IPsec, IKEv1 using RSA signatures and dynamic routing over VTIs, SSL VPNs using both client and clientless connections terminating on the Cisco ASA, and GETVPN deployed with multicast rekeying.

Exercise 3.1: Configure and Troubleshoot IPsec Static VTI with IPv6

An IPsec static virtual tunnel interface is required between R4 and R7, as illustrated in Figure 1-7 in [Part I](#). This interface supports IPv6 traffic, and EIGRPv6 routes (the networks from the Loopback1 interfaces) must be exchanged securely for Autonomous System 1 via the tunnel. Certificates must be used for IKE authentication and issued by the CA server running on R1 (as enabled in Lab 1).

You may use any passwords or names for configuration constructs unless otherwise predefined. Complete and troubleshoot the configuration using the following outputs to verify your solution:

[Click here to view code image](#)

```
R7# show crypto session
Interface: Tunnel2
Profile: ipv6
Session status: UP-ACTIVE
Peer: 2001:DB9:30::4 port 500
IKEv1 SA: local 2001:DB8:40::7/500
          remote 2001:DB9:30::4/500 Active
IPSEC FLOW: permit ipv6 ::/0 ::/0
Active SAs: 2, origin: crypto map
```

```
R4# show crypto session
Interface: Tunnel2
Profile: ipv6
Session status: UP-ACTIVE
Peer: 2001:DB8:40::7 port 500
IKEv1 SA: local 2001:DB9:30::4/500
          remote 2001:DB8:40::7/500 Active
IPSEC FLOW: permit ipv6 ::/0 ::/0
Active SAs: 2, origin: crypto map
```

Ensure that the interface Loopback1 subnets on either router are being advertised via EIGRPv6:

[Click here to view code image](#)

```
R7# show ipv6 route
```

IPv6 Routing Table - default - 9 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP

H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea

IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO

ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect

l - LISP

O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

EX 2011::/64 [170/27008000]

via FE80::A8BB:CCFF:FE00:7C00, Tunnel2

Note

- Do not remove any existing configuration.
- Do not modify the static or dynamic IPv6 routing configuration.
- This question has a dependency on [Exercise 1.4](#) in this lab.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 3.1: Configure and Troubleshoot IPsec Static VTI with IPv6.](#)”

Exercise 3.2: Troubleshoot and Configure GETVPN

In this exercise, R1 and R2 have been partially configured as cooperative key servers (COOP KS). R6 and R7 are the partially configured group members (GM).

Complete the configuration of this GETVPN deployment using the following information and referring to [Diagram 8](#) in [Part I](#).

- R2 (10.50.100.2) is to be the primary KS; R1 (10.50.100.1) is to be the secondary KS.
- Multicast rekeying is required.
- An IPsec antireplay mechanism is required that will support a multisender environment (default values can be used).
- Two ASAs exist in the path between GMs and KSs. ASA1 is configured in multiple context mode and will not support IP multicast. Ensure that the tunneled multicast traffic will pass through the ASAs.
- Periodic Dead Peer Detection (DPD) on the KSs is required using an interval of 60 seconds.
- R6 and R7 must be explicitly authorized to register with the GETVPN group.
- Do not remove any existing GETVPN or IKE configuration.
- Do not remove any existing IP multicast configuration on the routers.

Use the following outputs to verify your solution (the **highlighted** sections are particularly important):

[Click here to view code image](#)

```
R1# show crypto session
```


Interface: Ethernet0/0
Session status: UP-IDLE
Peer: 10.50.100.2 port 848
IKEv1 SA: local 10.50.100.1/848 remote 10.50.100.2/848 Active

Interface: Ethernet0/0
Session status: UP-IDLE
Peer: 10.50.60.6 port 848
IKEv1 SA: local 10.50.100.1/848 remote 10.50.60.6/848 Active

Interface: Ethernet0/0
Session status: UP-IDLE
Peer: 10.50.40.7 port 848
IKEv1 SA: local 10.50.100.1/848 remote 10.50.40.7/848 Active

R2# **show crypto session**
Crypto session current status

Interface: (unknown)
Session status: UP-IDLE
Peer: 239.192.1.190 port 848
IKEv1 SA: local 10.50.100.2/848 remote 239.192.1.190/848 Active

Interface: Ethernet0/0.1
Session status: UP-IDLE
Peer: 10.50.100.1 port 848
IKEv1 SA: local 10.50.100.2/848 remote 10.50.100.1/848 Active

R7# **show crypto gdoi ipsec sa**

SA created for group getvpn:
GigabitEthernet0/1:
 protocol = ip
 local ident = 10.7.0.0/16, port = 0
 remote ident = 10.7.0.0/16, port = 0
 direction: Both, replay(method/window): Time/5 sec

R7# **show crypto gdoi**

GROUP INFORMATION

Group Name : getvpn
Group Identity : 1
Rekeys received : 3
IPSec SA Direction : Both

Group Server list : 10.50.100.1

```
R6# show crypto gdoi
GROUP INFORMATION
```

```
Group Name           : getvpn
Group Identity       : 1
Rekeys received      : 4
IPSec SA Direction   : Both

Group Server list    : 10.50.100.1
                    : 10.50.100.2

Group member         : 10.50.60.6   vrf: None
Version              : 1.0.2
Registration status   : Registered
```

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 3.2: Troubleshoot and Configure GETVPN.](#)”

Exercise 3.3: SSL Client and Clientless VPNs

ASA2 is to be used as an SSL gateway for both clientless SSL and Cisco AnyConnect SSL connections as illustrated by [Diagram 10](#) in [Part I](#).

The following information should be used when completing this exercise (any naming conventions or policies not explicitly defined are user-configurable):

Create two local users:

■ user1

- Password: **cisco**
- Group/tunnel name: **SSL**
- Group homepage: <http://r3.cisco.com>
- Set an inactivity (idle) timeout of **1 minute**
- Use the following command to verify your connection:

[Click here to view code image](#)

```
ASA2# show vpn-sessiondb webvpn
```

■ user2

- Password: **cisco**
- Group/tunnel name: **anySSL**
- Permitted access: **10.50.40.0/24** from 192.168.100.0/24 only—use an identity-based firewall access rule set to be named **user2**
- Assign the client an address from pool **anyssl-clients: 192.168.100.100–192.168.100.200**
- Use the following command to verify your connection:

[Click here to view code image](#)

```
ASA2# show vpn-sessiondb anyconnect
```

Create a self-enrollment certificate for use with **crypto ca trustpoint ASA2**, being sure to match the **highlighted** attributes; other parameters can be user defined:

[Click here to view code image](#)

```
ASA2# show crypto ca cert
```

Certificate

Status: Available

Certificate Serial Number: 8b7ef551

Certificate Usage: General Purpose

Public Key Type: RSA (1024 bits)

Signature Algorithm: SHA1 with RSA Encryption

Issuer Name:

hostname=sslvpn.cisco.com

cn=sslvpn.cisco.com

Subject Name:

hostname=sslvpn.cisco.com

cn=sslvpn.cisco.com

Validity Date:

start date: 05:18:57 UTC Aug 21 2013

end date: 05:18:57 UTC Aug 19 2023

Associated Trustpoints: localtrust

To verify your solution, open a browser and connect to ASA2 using the hostname defined in the SSL certificate, as shown in [Figure 2-3](#). You should be able to select from both SSL groups.

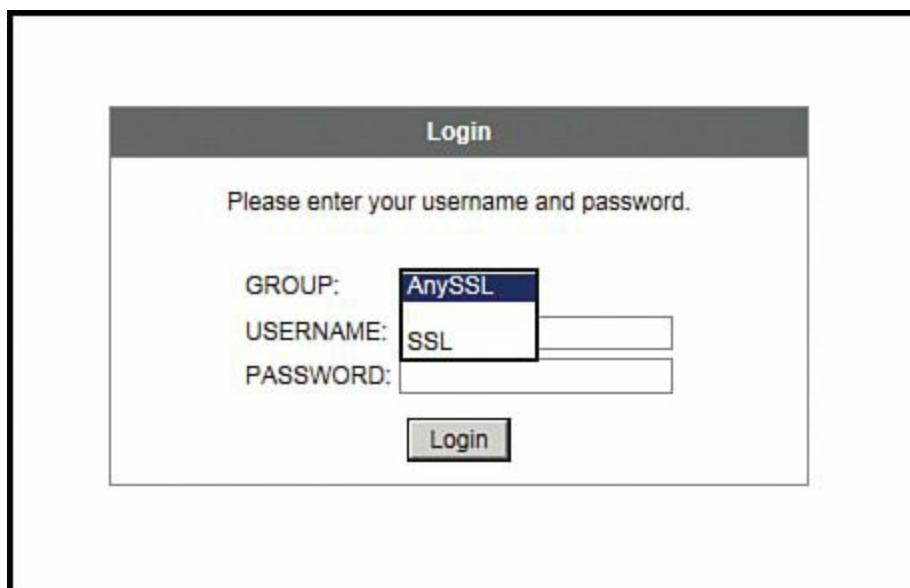


Figure 2-3 *SSL VPN Group Drop-Down Menu*

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 3.3: SSL Client and Clientless VPNs.](#)”

Exercise 3.4: Configure and Troubleshoot FlexVPN Site-to-Site Using RADIUS Tunnel Attributes

FlexVPN has been partially configured between R7 (10.50.40.7) and R6 (10.50.70.6) and is illustrated in [Diagram 9](#) in [Part I](#). Complete this configuration, and troubleshoot connectivity as necessary to meet the following requirements:

- R7 will initiate connections to R6 using RIPv2 routing updates as interesting traffic to trigger the VPN tunnel negotiation.
- The RIP-2 configuration should not be modified.
- Do not remove any preconfigured IKEv2 policy.
- The IKEv2 preshared key for R7 must be configured on the Cisco ACS server (192.168.2.18). R6 will use RADIUS-based AAA to retrieve this information.
- The IKEv2 identity type to be used for R7 is FQDN. You will need to ensure this value is used as the username passed to the ACS server.
- You may use any names for other necessary configuration constructs not explicitly predefined.

The following outputs should be used to verify the solution. Pay particular attention to the **highlighted** values.

[Click here to view code image](#)

```
R6# show crypto ikev2 session detailed
IPv4 Crypto IKEv2 Session
```

```
Session-id:18, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local          Remote          fvr/ivrf       Status
1    10.50.70.6/500    10.50.40.7/500    none/none      READY
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/1014 sec
CE id: 1008, Session-id: 18
Status Description: Negotiation done
Local spi: D60B62C207327A3D    Remote spi: 609E382CB11281D3
Local id: r6.cisco.com
Remote id: r7.cisco.com
```

```
.....
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0x88B600C5/0xDE40CB3B
AH spi in/out: 0x0/0x0
CPI in/out: 0x0/0x0
Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

```
R7# show ip route
```

R 172.17.60.0/24 [120/1] via 172.16.70.6, 00:00:07, Tunnel1

R6# show ip route

172.17.0.0/24 is subnetted, 1 subnets

R 172.17.70.0/24 [120/1] via 172.16.70.7, 00:00:21, Virtual-Access1

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 3.4: Configure and Troubleshoot FlexVPN Site-to-Site Using RADIUS Tunnel Attributes.](#)”

Exercise 3.5: Configure and Troubleshoot FlexVPN Remote Access (Client to Server)

A FlexVPN server has been partially configured on R2 (10.50.100.2). Complete the configuration of R4 (10.50.30.4) as a FlexVPN client, and troubleshoot connectivity as necessary to meet the following requirements:

- Refer to [Diagram 9](#) in [Part I](#).
- Define a crypto ikev2 client profile named **flex**.
- **Tunnel0** should be used as the logical interface for the VPN connection using a negotiated IP address.
- The trigger for the VPN connection from R4 will be the **crypto ikev2 client flexvpn connect** command.
- You may use any names for other necessary configuration constructs not explicitly predefined.
- Do not remove any preconfigured IKEv2 policy. Use it as the basis to complete the configuration required for this question.

The following outputs should be used to verify the solution. Pay particular attention to the **highlighted** values.

[Click here to view code image](#)

```
R4# show crypto ikev2 authorization policy
```

```
IKEv2 Authorization Policy : flex
```

```
route set interface
```

```
route set acl: routes
```

```
route accept any tag : 1 distance : 1
```

```
R4# show crypto ikev2 client flex
```

```
Profile : flex
```

```
Current state:ACTIVE
```

```
Peer : 10.50.100.2
```

```
Source : Ethernet0/1
```

```
ivrf : IP DEFAULT
```

```
fvrf : IP DEFAULT
```

```
Backup group: Default
```

```
Tunnel interface : Tunnel0
```

Assigned ip address: 172.17.100.55

R4# show crypto ikev2 session detail

IPv4 Crypto IKEv2 Session

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id	Local	Remote	fvr/ivrf	Status
1	10.50.30.4/500	10.50.100.2/500	none/none	READY

Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/277 sec
CE id: 1032, Session-id: 2
Status Description: Negotiation done
Local spi: 0696C6F582787B23 Remote spi: 49C2BF63CF74F456
Local id: R4.cisco.com
Remote id: 10.50.100.2
Pushed IP address: 172.17.100.55
DNS Primary: 192.168.2.25

Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0xEEF6B847/0x81642A80
AH spi in/out: 0x0/0x0
CPI in/out: 0x0/0x0
Encr: 3DES, esp_hmac: MD596
ah_hmac: None, comp: IPCOMP_NONE, mode tunnel

R2# show ip route

S 172.18.34.0 is directly connected, Virtual-Access1

For the solution and verification information of this lab exercise, see [“Solution and Verification for Exercise 3.5: Configure and Troubleshoot FlexVPN Remote Access \(Client-to-Server\).”](#)

Section 4: System Hardening and Availability

System or device hardening involves implementing techniques that protect against compromise, resulting in either specific device/system failures or disruption to other network services. The goal of enabling protection and monitoring features on a system is performance predictability and network availability. This section requires implementing and troubleshooting specific hardening features, such as control and management plane policing. Features that focus on network availability, such as routing protocol security, monitoring traffic transiting a switch, and securing wireless infrastructure, are also covered.

Exercise 4.1: BGP TTL-Security Through the Cisco ASA

BGP has been preconfigured between R7 (AS 107) and R6 (AS 106). Replace the eBGP multihop command with the TTL-security feature using the correct number of hops between R6 and R7. Additionally, configure ASA2 to appear as a hop in the path between R6 and R7.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 4.1: BGP TTL-Security Through the Cisco ASA.](#)”

Exercise 4.2: Configure and Troubleshoot Control Plane Protection

Configure a port-filter policy to drop all traffic destined to closed or “nonlistened” TCP/UDP ports on R1. Troubleshoot using the **show control-plane host open-ports** command to ensure all necessary services on R1 are not impacted.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 4.2: Configure and Troubleshoot Control Plane Protection.](#)”

Exercise 4.3: Control Plane Protection for IPv6 Cisco IOS

Implement a control plane policy to regulate the bandwidth used by essential ICMPv6 message types on R4. Allocate bandwidth on your policy using the information in [Table 2-12](#).

Traffic Class	Rate Bits per Second	Conform Action	Exceed Action
ICMPv6	8000	Transmit	Drop
Default	10,000	Transmit	Transmit

Table 2-12 *CPPr Policy Parameters*

Apply your policy to the appropriate control-plane subinterface.

Note

RFC 4890 outlines a list of ICMPv6 essential message types.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 4.3: Control Plane Protection for IPv6 Cisco IOS.](#)”

Section 5: Threat Identification and Mitigation

This section requires the implementation of threat identification and mitigation techniques on different Cisco platforms. On a Cisco IOS Router, NetFlow is used to identify possible attack patterns, and this information is then used to build a Flexible Packet Matching (FPM) policy. DHCP activities can be manipulated to launch attacks that are mitigated by methods configured on Cisco Catalyst switches. This section also covers application-specific attack mitigation features on the Cisco ASA.

Exercise 5.1: Preventing IP Address Spoofing on the Cisco ASA

R3 has an interface configured for 10.50.50.4 (to simulate an attack from a spoofed address). Configure a feature on ASA2 to prevent IP address spoofing. Do not use access lists.

You may test your solution by initiating a ping sourced from 10.50.50.3 destined to an address on the inside of ASA2.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 5.1: Preventing IP Address Spoofing on the Cisco ASA.](#)”

Exercise 5.2: Monitor and Protect Against Wireless Intrusion Attacks

The Cisco WLC should be configured to learn the IP addresses of attackers that have been shunned by the Cisco IPS appliance. The WLC can then prevent these clients from joining any wireless network.

Use the information in [Table 2-13](#) to complete this exercise.

Parameter	Value
IPS Sensor IP Address	192.168.2.100
Port	443
WLC/IPS username	wlc
WLC/IPS password	123cisco123
WLC wps index value	1

Table 2-13 *WIPS Configuration Parameters*

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 5.2: Monitor and Protect Against Wireless Intrusion Attacks.](#)”

Exercise 5.3: Identifying and Protecting Against SYN Attacks

The Cisco IOS CA server web server is configured on R1 at 10.50.100.1.

Configure TCP SYN attack protection on ASA1 for traffic destined to the web server on TCP/80 and TCP/443 from any source as follows:

- Do not allow the number of incomplete connections to exceed 100.
- Limit the number of simultaneous connections that any single client can have to this web server to 5.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 5.3: Identifying and Protecting Against SYN Attacks.](#)”

Exercise 5.4: Using NBAR for Inspection of HTTP Traffic with PAM and Flexible NetFlow

R1 is configured as the CA server for the network.

NBAR is required to inspect and police the HTTP traffic the CA server is processing. Certificate handling in Cisco IOS is done using Cisco Simple Certificate Enrollment Protocol (SCEP), which uses HTTP as a transport. Complete the following tasks, using any names for configuration constructs:

- Review the following debug output and create an NBAR policy for inspecting HTTP packets matching *all* the **highlighted** values:


```
CRYPTO_PKI: locked trustpoint ciscoca, refcount is 1
CRYPTO_PKI: http connection opened
CRYPTO_PKI: Sending HTTP message
CRYPTO_PKI: Reply HTTP header:
HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI)
Host: 10.50.100.1
```

```
CRYPTO_PKI: unlocked trustpoint ciscoca, refcount is 0
CRYPTO_PKI: locked trustpoint ciscoca, refcount is 1
CRYPTO_PKI: unlocked trustpoint ciscoca, refcount is 0
CRYPTO_PKI: Reply HTTP header:
HTTP/1.1 200 OK
Date: Sun, 18 Aug 2013 04:34:08 GMT
Server: cisco-IOS
Content-Type: application/x-x509-ca-cert
Expires: Sun, 18 Aug 2013 04:34:08 GMT
Last-Modified: Sun, 18 Aug 2013 04:34:08 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Accept-Ranges: none
```

Content-Type indicates we have received a CA certificate.

- Ensure that traffic matching the NBAR classification criteria is policed at a rate of 10,000 bits/sec with conforming traffic transmitted and traffic exceeding this rate dropped.
- Configure Port-to-Application Mapping (PAM) to allow SCEP requests only from port 8080.
- Define a Flexible NetFlow flow monitor that will track the NBAR classification using the following record fields:

```
IPV4 SOURCE ADDRESS
IPV4 DESTINATION ADDRESS
TRNS SOURCE PORT
TRNS DESTINATION PORT
IP PROTOCOL
APPLICATION NAME
interface input
interface output
counter bytes long
counter packets long
ip fragmentation flags
```

- Set the inactive flows cache timeout to 60 seconds.
- No NetFlow statistics export is required.

- Apply this flow monitor on an interface inbound only.
- To verify your solution, configure a trustpoint on R6 for the cisco server. Only the enrollment URL is required. Attempt CA authentication, and check the NBAR and NetFlow statistics on R1.

[Click here to view code image](#)

```
R6(config)# crypto pki auth cisco
```

Certificate has the following attributes:

```
Fingerprint MD5: 1F5A02E4 C2C8230A 56FC15BB CBDFBEF6
```

```
Fingerprint SHA1: 99D5D0AA 928B4DD8 7D9E6D98 B3831F1D 796C6A71
```

```
% Do you accept this certificate? [yes/no]: no
```

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 5.4: Using NBAR for Inspection of HTTP Traffic with PAM and Flexible NetFlow.](#)”

Section 6: Identity Management

In this section, you configure the Cisco Identity Services Engine (ISE) and Cisco Secure Access Control Server (ACS) to support identity-based network access and device management using RADIUS and TACACS+. Device command authorization on a Cisco IOS Router is an important method for restricting device access and limiting the potential for attack or inadvertent misconfiguration. Identity-based network access is implemented using Cut-Through Proxy on the Cisco ASA triggered by HTTP traffic. Cisco TrustSec is applied on the Cisco Catalyst switch with the Cisco ISE through the use of MAC Authentication Bypass (MAB) and 802.1X authentication methods enforced on a switch port.

This section covers the Cisco TrustSec (CTS) solution. You will be working with SW1 (10.50.70.4) and SW2 (10.50.70.5) and the Cisco ISE (192.168.2.15). SW1 and SW2 are connected via interface gig1/0/23; this is used for CTS connectivity purposes only.

Exercise 6.1: Cisco TrustSec—Dynamically Assigning Secure Group Tagging and SGACLs: 802.1X and MAB

The exercise has three parts.

Part A: Configuring SGTs on the Cisco ISE

Before secure group tags (SGT) can be assigned to authenticated end entities, they must be defined on the Cisco ISE (192.168.2.15). Configure the following security groups on the ISE using the information in [Table 2-14](#).

Secure Group Name	SGT
NADS	2
NET70	3
IPPhone	4
AP	5

Table 2-14 ISE SGT Identifiers

Part B: Dynamically Assigning SGTs via 802.1X and MAB

In this part, SGTs are dynamically assigned to devices using port-based authentication mechanisms. Devices connecting and disconnecting on switchports must be tracked to maintain accurate IP-to-SGT mappings on SW2. Complete the following two tasks.

Task 1: Cisco Access Point as an 802.1X Supplicant with SGTs

The Cisco AP connected to SW2 is to be configured as an 802.1X supplicant. Use the information that follows to complete this exercise:

- Configure 802.1X support on the WLC. This information is pushed to the AP in the rack and will facilitate 802.1X authentication of the AP. Add an 802.1X username/password (ciscoAP/CCie123) for global AP authentication via 802.1X.

Verify that the WLC has successfully pushed the 802.1X credentials to the APs and they have associated with the WLC.

[Click here to view code image](#)

```
(WLC) >show ap summary
Number of APs..... 2
```

```
Global AP User Name..... cisco
Global AP Dot1x User Name..... ciscoAP
```

```
AP Name      Slots  AP Model      Ethernet
MAC      Location      Port Country Priority
-----
AP1cdf.0f94.8063 2    AIR-CAP3502I-A-K9  1c:df:0f:94:80:63 default location 1
AP588d.0959.4921 2    AIR-LAP1262N-A-K9  58:8d:09:59:49:21 default location 1
```

- Create an identity for the AP on ISE1 using the preceding credentials. This identity will be used for authentication and mapped to an authorization policy.
- Configure an authorization profile and authorization policy rule for Cisco access points as outlined in [Table 2-15](#).

Attribute	Value
Name	Access-Points
SGT	AP (5)
SGACL Name	APSRvs
SGACL Policy	permit udp dst eq 5246 permit udp dst eq 5247 permit icmp

Table 2-15 ISE Access-Point Authorization Policy

- Configure SW2 Gig1/0/18 for 802.1X support, which will enable the Cisco AP to authenticate via RADIUS to the ISE and receive an authorization policy.

Task 2: Cisco IP Phone Using MAB and SGTs

In [Exercise 6.3](#) in Lab 1, the SW2 gig1/0/14 interface was configured to authenticate the IP Phone with MAB. In this task, MAB is still used; however, the authorization policy will change. Instead of the IP Phone being authorized for network access using DACLs, SGACLs will be used as defined in [Table 2-16](#).

Attribute	Value
Name	Profiled Cisco IP Phones
Domain	Voice
Voice VLAN	9
SGT	IPPhone (4)
SGACL Name	IPPhone
SGACL Policy	permit tcp dst eq 2000 permit tcp dst eq www permit udp dst eq bootps permit udp dst eq domain permit tcp src eq www permit icmp permit udp dst eq tftp

Table 2-16 ISE IP Phone Authorization Policy

Note

You might need to force your phone to reauthenticate. Use the **clear authentication session interface interface** command.

Part C: Create the SGA Egress Policy

Using the information from Parts [A](#) and [B](#), define an SGA egress policy on the ISE using the parameters in [Table 2-17](#). Switch VLAN values are for reference only.

Source SGT (Switch VLAN)	Destination SGT (Switch VLAN)	SGACL
5 (VLAN 77)	3 (VLAN 70)	APSRvs
4 (VLAN 9)	3 (VLAN 70)	IPPhone

Table 2-17 ISE SGACL Parameters

Only the policies defined in Part B's SGACLs must be allowed from SRC SGTs to DEST SGTs.

Traffic not explicitly defined in the egress policy is permitted by default.

Return traffic from SGT 3 to SGT 4 and SGT 5 will be covered by the default rule.

For the solution and verification information of this lab exercise, see "[Solution and Verification for Exercise 6.1: Cisco TrustSec—Dynamically Assigning Secure Group Tagging and SGACLs: 802.1X and MAB.](#)"

Exercise 6.2: Cisco TrustSec—NDAC and MACsec

This question has two tasks.

- Task 1: Configure SW2 (seed device) and SW1 (nonseed device) for NDAC using AAA RADIUS on the Cisco ISE:
 - The protected access credential (PAC) key is cisco123.
 - The AAA CTS authorization list is MLIST.
 - The SGT of NADS (2) was configured in [Exercise 6.1](#). Assign it to SW2 and SW1 via a network device authorization profile for SGA.

Because the Cat 3k does not support the downloading of the IP to SGT database from the ISE (at press time), manually configure cts enforcement on SW2 for VLANs 70, 77, and 9.

- Task 2: Enable Cisco TrustSec switch-to-switch link security in 802.1X mode between the GigabitEthernet1/0/23 switchports on SW1 and SW2 using MACsec.

The following output can be used to verify your solution:

[Click here to view code image](#)

```
SW2# show cts interface
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/23:
  CTS is enabled, mode: DOT1X
  IFC state: OPEN
  Authentication Status: SUCCEEDED
  Peer identity: "SW1"
  Peer's advertised capabilities: "sap"
  802.1X role: Authenticator
  Reauth period configured: 240 (locally configured)
  Reauth period per policy: 86400 (server configured)
  Reauth period applied to link: 86400 (server configured)
  Reauth starts in approx. 0:15:47:42 (dd:hr:mm:sec)
  Authorization Status: SUCCEEDED
  Peer SGT: 2:NADS
```

Peer SGT assignment: Trusted
SAP Status: SUCCEEDED
Version: 2
Configured pairwise ciphers:
gcm-encrypt
null
no-encap

Replay protection: enabled
Replay protection mode: STRICT

Selected cipher: gcm-encrypt

Propagate SGT: Enabled

You should also verify whether protected traffic is flowing across the switch-to-switch tunnel using the **show cts macsec counters** command.

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 6.2: Cisco TrustSec—NDAC and MACsec.](#)”

Exercise 6.3: Cisco TrustSec—SGT Exchange Protocol over TCP

This question has four tasks.

- **Task 1:** Configure SXP between SW1 (Listener) and SW2 (Speaker). A password is not required.
- **Task 2:** Configure SXP between R6 (Listener) and SW2 (Speaker). A password is not required.
- **Task 3:** Configure SXP between R6 (Listener) and the WLC (Speaker). A password of cisco is required.
- **Task 4:** Manually define the following IP-SGT mappings on SW2:

[Click here to view code image](#)

```
SW2# show cts role-based sgt all
```

```
IP Address      SGT   Source
```

```
=====
```

10.50.30.3	12	CLI
10.50.30.4	12	CLI
10.50.50.20	14	CLI
10.50.50.20	14	CLI
10.50.70.4	2	CLI
10.50.80.50	16	CLI
10.50.100.1	15	CLI
10.50.100.2	15	CLI
10.50.100.10	15	CLI
192.168.2.25	18	CLI

To verify whether the SXP connection has been established, use the following command on SW1 and R6:

```
show cts role sgt all
```

For the solution and verification information of this lab exercise, see “[Solution and Verification for Exercise 6.3: Cisco TrustSec—SGT Exchange Protocol over TCP.](#)”

Practice Lab 2 Solutions

Section 1: Perimeter Security

In Lab 1, you initialized perimeter security services and configured some fundamental features. This section adds more advanced features on the Cisco ASAs, including configuring IPv6, botnet traffic filtering and redundancy and management services. There is also an exercise using the Cisco IOS zone-based firewall (ZFW), which has replaced CBAC as the firewall solution on Cisco IOS routers. ZFW has been updated to allow support for Cisco TrustSec and security group tagging, and this will be incorporated into the exercise in this lab.

Solution and Verification for Exercise 1.1: Configure a Redundant Interface on ASA2

Skills Tested:

- Configuring high availability on the Cisco ASA using a redundant interface

Solution and Verification

There are several ways to implement high availability (HA) on the Cisco ASA. Redundant interface failover is one form of HA that provides link redundancy in a single device. The down side of this form of HA is that if there is a problem other than an interface issue on the ASA itself, or on any connected device (on the tracked interface), there will still be service disruption issues. The benefits of a redundant interface are that configuration is fairly simple, there is no need to provision a separate link to transfer state information between devices, and one MAC address is used on the redundant interface (taken from the first physical interface [the primary] added to the bundle, or user defined) that does not change as the interfaces change state. The use of one MAC address perpetually means upstream devices will not have to relearn IP-to-MAC address bindings, minimizing disruption to applications. This is also useful if, for example, a security technique such as IP source guard is configured on a switchport connecting the ASA.

The key change to the configuration of ASA2 when moving from physical interfaces to a logical interface is that the parameters associated with the physical interface in a non-HA deployment, such as nameif, IP addresses, and security level, are now configured on the redundant interface. Physical interfaces need to be defined only as member interfaces. Multiple member interfaces are associated with one redundant interface.

You must be sure to reapply all access lists, service policies, and anything else that had previously been applied to the outside interface. These policies are automatically removed when an interface nameif is deleted.

For all verification syntax that follows:

- Required output appears in **red**
- Variable syntax appears in **green**

Verify whether the physical interfaces Gig0/0 and Gig0/1 are up and are members of the logical interface Redundant1. No interface parameters, such as an IP address, will be displayed because they

are now defined on the redundant interface.

[Click here to view code image](#)

```
ASA2# show interface gig0/0
Interface GigabitEthernet0/0 "", is up, line protocol is up
Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
Input flow control is unsupported, output flow control is off
Active member of Redundant1
MAC address 0015.c695.c646, MTU not set
IP address unassigned
```

```
ASA2# show interface gig0/1
Interface GigabitEthernet0/1 "", is up, line protocol is up
Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
Input flow control is unsupported, output flow control is off
Standby member of Redundant1
MAC address 0015.c695.c647, MTU not set
IP address unassigned
```

Verify whether the redundant interface is up and has an IP address assigned. Note the MAC address used by the redundant interface. It is taken from the first physical interface member added to the grouping. This can be overridden by a user-defined MAC address via the **mac-address** *mac_address* command.

[Click here to view code image](#)

```
ASA2# show interface redundant 1
Interface Redundant1 "outside", is up, line protocol is up
Hardware is i82546GB rev03, 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 0015.c695.c646, MTU 1500
IP address 10.50.50.20, subnet mask 255.255.255.0
```

Verify whether all interface parameters have now been correctly applied to the redundant interface:

[Click here to view code image](#)

```
ASA2# show nameif
Interface      Name      Security
GigabitEthernet0/2  inside   100
GigabitEthernet0/3  dmz      50
Redundant1       outside  0
```

Checking the routing table for completeness and being able to successfully ping the next hop router will verify protocol connectivity.

[Click here to view code image](#)

ASA2# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 10.50.50.5 to network 0.0.0.0

```
C 10.50.50.0 255.255.255.0 is directly connected, outside
S 10.3.3.0 255.255.255.0 [1/0] via 10.50.30.3, dmz
S 10.4.4.0 255.255.255.0 [1/0] via 10.50.30.4, dmz
O 10.7.7.7 255.255.255.255 [110/11] via 10.50.40.7, 0:00:18, inside
C 10.50.40.0 255.255.255.0 is directly connected, inside
C 10.50.30.0 255.255.255.0 is directly connected, dmz
O 10.50.9.0 255.255.255.0 [110/11] via 10.50.50.5, 0:00:18, outside
O E2 10.50.100.0 255.255.255.0 [110/20] via 10.50.50.5, 0:00:18, outside
O E2 10.50.90.0 255.255.255.0 [110/20] via 10.50.50.5, 0:00:18, outside
O 10.50.77.0 255.255.255.0 [110/11] via 10.50.50.5, 0:00:18, outside
O 10.50.70.0 255.255.255.0 [110/11] via 10.50.50.5, 0:00:18, outside
O E2 192.168.2.0 255.255.255.0 [110/20] via 10.50.50.5, 0:00:18, outside
O*E2 0.0.0.0 0.0.0.0 [110/1] via 10.50.50.5, 0:00:18, outside
```

ASA2# ping outside 10.50.50.5

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.50.50.5, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

Configuration

ASA2

[Click here to view code image](#)

```
hostname ASA2
interface Redundant1
 member-interface GigabitEthernet0/0
 member-interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 10.50.50.20 255.255.255.0
 ospf priority 0
```

Solution and Verification for Exercise 1.2: SSH Management Authentication and Local Command Authorization on ASA1

Skills Tested

- Configuring SSH server functionality on the Cisco ASA for management purposes
- Defining local command authorization policies per privilege level
- Manipulating session parameters for SSH

Solution and Verification

The Cisco ASA can be managed using several applications: Telnet, HTTPS, and SSH. In this exercise, SSH server functionality is required on ASA1. When the ASA is configured in multi-context mode, management services and functions are enabled in the admin context. When you enable SSH and define users for access, you can configure per-user command authorization. In this exercise, the command authorization is done via the local database, but it can also be done using TACACS+ to an external authentication server. Command authorization defines an explicit set of ASA commands that is mapped to a privilege level to limit access for users granted that same privilege level upon login to the ASA.

You also can tune SSH access and session parameters. You can change parameters, such as session idle timeouts, globally or set them explicitly for certain groups of users using the Modular Policy Framework (MPF). The default idle timeout is 5 minutes, and it can be used for sessions sourced from IP addresses 192.168.1.0/24. You should use the ASA MPF configuration syntax to change the idle timeout for sessions sourced from 192.168.2.0/24.

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**
- Variable syntax appears in **green**

The first step to configuring SSH server is to define an RSA key pair for ASA1. The modulus to use is 768 bits. SSH clients will be prompted to accept this key the first time they connect to ASA1.

Verify whether the SSH server key has been generated:

[Click here to view code image](#)

```
ASA1/admin# show crypto key mypubkey rsa
```

```
Key pair was generated at: 03:37:36 UTC Aug 21 2013
```

```
Key name: <Default-RSA-Key>
```

```
Usage: General Purpose Key
```

```
Modulus Size (bits): 768
```

```
Key Data:
```

```
307c300d 06092a86 4886f70d 01010105 00036b00 30680261 00bb8204 bdf8500e  
7abf837d d9b2e0c9 a7e558c3 57e559b7 ea514afb ea1913f9 2cfd0db fb944a53  
23fd196f 38428fc2 26d2aeb9 e8060139 e0cb5f58 f089052a 8bdca9be a9357b46  
a74067ee 164efd6f 898b504c f0da88af 695af6b1 7fd34458 0b020301 0001
```

Verify the global SSH server settings. The session idle timeout is 5 minutes by default. More granular control can be applied using the MPF:

[Click here to view code image](#)

```
ASA1/admin# show ssh
Timeout: 5 minutes
Versions allowed: 1 and 2
192.168.1.0 255.255.255.0 mgmt
192.168.2.0 255.255.255.0 mgmt
```

To verify the MPF policy created to apply the 1 minute idle timeout to SSH sessions sourced from 192.168.2.0/24, show the service policy applied to the management interface. The class map will identify the traffic of interest; namely, SSH sourced from 192.168.2.0/24. The policy map enforces actions on that traffic; in this case, the 1 minute idle timeout.

[Click here to view code image](#)

```
access-list ssh-acl extended permit tcp 192.168.2.0 255.255.255.0 any eq 22
```

```
class-map mgmt-class
match access-list ssh-acl
```

```
ASA1/admin# show service-policy int mgmt
```

Interface mgmt:

Service-policy: mgmt-policy

Class-map: mgmt-class

Set connection policy: drop 0

Set connection timeout policy:

idle 0:01:00

DCD: disabled, retry-interval 0:00:15, max-retries 5

DCD: client-probe 0, server-probe 0, conn-expiration 0

To verify the SSH configuration and command authorization policy, connect from SW1:

Step 1. Log in with the privilege level 15 account:

[Click here to view code image](#)

```
SW1# ssh -l cisco 192.168.1.20
Password: cisco
Type help or '?' for a list of available commands.
ASA1/admin>en
Password: *****
```

```
ASA1/admin# show running-config
: Saved
:
ASA Version 8.4(5) <context>
```

```
!  
hostname ciscoasa
```

```
ASA1/admin# show ssh session
```

```
SID Client IP  Version Mode Encryption Hmac  State      Username  
0 192.168.1.5  2.0  IN  aes128-cbc sha1  SessionStarted  cisco  
                OUT  aes128-cbc sha1  SessionStarted  cisco
```

Step 2. Log in with the privilege level 5 account:

[Click here to view code image](#)

```
SW1# ssh -l support 192.168.1.20  
Password: cisco  
Type help or '?' for a list of available commands.  
ASA1/admin>  
ASA1/admin> en 5  
Password: *****
```

```
ASA1/admin# show running-config
```

^

```
ERROR: % Invalid input detected at '^' marker.  
ERROR: Command authorization failed
```

Verify whether the authorized commands succeed:

[Click here to view code image](#)

```
ASA1/admin# show xlate  
0 in use, 0 most used  
ASA1/admin# show route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area

* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 192.168.1.5 to network 0.0.0.0

```
C 192.168.1.0 255.255.255.0 is directly connected, mgmt  
S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.1.5, mgmt  
ASA1/admin#
```

```
ASA1/admin# show ssh session
```

```
SID Client IP  Version Mode Encryption Hma  State      Username
0 192.168.1.5  2.0 IN  aes128-cbc sha1  SessionStarted support
OUT aes128-cbc sha1  SessionStarted support
```

Configuration

[Click here to view code image](#)

```
username support password cisco privilege 5
username cisco password cisco
```

```
aaa authentication ssh console LOCAL
ssh 192.168.1.0 255.255.255.0 mgmt
ssh 192.168.2.0 255.255.255.0 mgmt
```

```
object-group service ssh tcp
port-object eq ssh
access-list ssh-acl extended permit tcp 192.168.2.0 255.255.255.0 any object-group
ssh
```

```
class-map mgmt-class
match access-list ssh-acl
```

```
policy-map mgmt-policy
class mgmt-class
set connection timeout idle 0:01:00
!
service-policy mgmt-policy interface mgmt
```

```
enable password cisco level 5
enable password cisco
```

```
privilege show level 5 mode exec command xlate
privilege show level 5 mode exec command route
```

Tech Notes

The following are some tips regarding security contexts and command authorization:

- AAA settings are discrete per context, not shared among contexts. Make sure you verify the capabilities associated with specific versions of Cisco ASA software.
- When configuring command authorization, you must configure each security context separately, allowing the enforcement of different command authorizations per security context.
- When switching between security contexts, administrators should be aware that the commands

permitted for the username specified when they log in might be different in the new context session or that command authorization might not be configured at all in the new context.

- New context sessions started with the **changeto** command always use the default enable_15 username as the administrator identity, regardless of which username was used in the previous context session. This behavior can lead to unexpected results if command authorization is not configured for the enable_15 user or if authorizations are different for the enable_15 user than for the user in the previous context session.

Solution and Verification for Exercise 1.3: Configuring Advanced Network Protection on the ASA

Skills Tested

- Configuring botnet traffic filtering using blacklists, whitelists, and DNS snooping on the ASA
- Using syslog to verify botnet traffic filtering
- Applying advanced features to the Cisco ASA's threat detection feature
- Implementing IP audit to provide basic IPS support on the Cisco ASA

Solution and Verification

All the features covered in this exercise are less traditional firewall features available on the ASA. In general, the protection and monitoring provided by threat detection and IP audit would be implemented on an IPS platform. However, in certain scenarios, these features can be useful if they are run periodically to profile the traffic seen on the ASA and devise a deployment plan for an IPS system.

Botnet traffic filtering is an important feature that can protect the hosts in the network from attaching to known malware sites and in turn infecting other devices in the network. It is most useful when combined with a dynamic database service that contains the names of thousands of questionable Internet sites. This enhanced service is easily integrated with the static blacklist used in this exercise.

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**

Task 1: Botnet Traffic Filtering on ASA1

R2 has been configured as the authoritative DNS server for the ccie.com domain. R6 is configured with R2 (10.50.100.2) as a name server. Telnet to the blacklisted server should fail, although the name should resolve to ensure the DNS query was snooped. The filters should be applied on the outside interface of ASA1/c2. Syslog output is a good way to verify whether the configuration is producing the expected results.

[Click here to view code image](#)

```
R6# telnet server.ccie.com
Translating "server.ccie.com"...domain server (10.50.100.2)

Translating "server.ccie.com"...domain server (10.50.100.2) [OK]
```

Trying server.ccie.com (10.10.130.1)...

% Connection timed out; remote host not responding

Verify whether the DNS request from R6 was snooped by ASA1:

[Click here to view code image](#)

```
ASA1/c2# show dynamic-filter dns-snoop detail
```

```
DNS Reverse Cache Summary Information:
```

```
1 addresses, 1 names
```

```
Next housekeeping scheduled at 19:23:50 UTC Sep 19 2013,
```

```
DNS reverse Cache Information:
```

```
[10.10.130.1] flags=0x2, type=2, unit=0 b:u:w=1:0:0, cookie=0x751dae80
```

```
[server.ccie.com] type=2, ttl=0
```

If logging was enabled on ASA1, you should see the following output (note the message levels):

[Click here to view code image](#)

```
%ASA-6-338301: Intercepted DNS reply for name server.ccie.com from
```

```
inside:10.50.100.2/53 to
```

```
outside:10.50.80.6/52007, matched blacklist
```

```
%ASA-6-302016: Teardown UDP connection 824265 for outside:10.50.80.6/52007 to
```

```
inside:10.50.100.2/53 duration 0:00:00 bytes 82
```

```
%ASA-4-338002: Dynamic Filter monitored blacklisted TCP traffic from
```

```
outside:10.50.80.6/16988
```

```
(10.50.80.6/16988) to inside:10.10.130.1/23 (10.10.130.1/23), destination
```

```
10.10.130.1 resolved
```

```
from local list: server.ccie.com, threat-level: very-high, category: admin-added
```

```
%ASA-4-338006: Dynamic Filter dropped blacklisted TCP traffic from
```

```
outside:10.50.80.6/16988
```

```
(10.50.80.6/16988) to inside:10.10.130.1/23 (10.10.130.1/23), destination
```

```
10.10.130.1 resolved
```

```
from local list: server.ccie.com, threat-level: very-high, category: admin-added
```

Access to the site server.ccie.com should be blocked because it has been designated a blacklisted site.

[Click here to view code image](#)

```
ASA1/c2# show dynamic-filter reports top malware-sites
```

```
Malware Sites (since last clear)
```

```
Site Connections Logged Dropped Threat-level Category
```

```
-----  
10.10.130.1 (server.ccie.com) 4 4 very-high admin-added
```

```
Last clearing of the top sites report: Never
```


You can verify the whitelisted addresses as follows:

[Click here to view code image](#)

```
R6# telnet 10.10.110.1
```

```
Trying 10.10.110.1 ... Open
```

```
ASA1/c2# show dynamic-filter statistics
```

```
Enabled on interface outside
```

```
Total conns classified 57, ingress 17, egress 40
```

```
Total whitelist classified 1, ingress 1, egress 0
```

```
Total greylist classified 0, dropped 0, ingress 0, egress 0
```

```
Total blacklist classified 56, dropped 56, ingress 16, egress 40
```

Whitelisted sites are displayed in syslog outputs. The following log messages can help verify the configuration:

[Click here to view code image](#)

```
%ASA-6-338104: Dynamic Filter monitored whitelisted TCP traffic from  
outside:10.50.80.6/52071  
(10.50.80.6/52071) to inside:10.10.110.1/23 (10.10.110.1/23), destination  
10.10.110.1 resolved  
from local list: 10.10.0.0/255.255.0.0
```

Task 2: Threat Detection on ASA2

Enabling and verifying additional statistics categories is straightforward. Protocol statistics will display any non-UDP or non-TCP IP protocols:

[Click here to view code image](#)

```
ASA2# show threat-detection statistics protocol
```

```
Average(eps) Current(eps) Trigger Total events
```

```
OSPF * 89: tot-ses:0 act-ses:0
```

```
1-hour Sent byte: 0 0 0 592
```

```
1-hour Sent pkts: 0 0 0 7
```

Port statistics will display UDP and TCP ports for a more in-depth profile of the traffic seen on ASA2:

[Click here to view code image](#)

```
ASA2# show threat-detection statistics port
```

```
Average(eps) Current(eps) Trigger Total events
```

```
Isakmp 500: tot-ses:2070 act-ses:1
```

```
1-hour Sent byte: 0 0 0 328
```

```
1-hour Sent pkts: 0 0 0 2
```

```
1-hour Recv byte: 0 0 0 344
```

```
1-hour Recv pkts: 0 0 0 2
```

Task 3: IP Audit

To verify whether attacks are dropped on the outside interface of ASA1/c1, send a large ping that will trigger the fragmented ICMP signature:

[Click here to view code image](#)

```
R6# ping 192.168.2.5 size 2000
```

```
Type escape sequence to abort.
```

```
Sending 5, 2000-byte ICMP Echos to 192.168.2.5, timeout is 2 seconds:
```

```
.....
```

```
IP AUDIT INTERFACE COUNTERS: outside
```

```
2011 I ICMP Address Mask Request 0
```

```
2012 I ICMP Address Mask Reply 0
```

```
2150 A Fragmented ICMP 10
```

```
2151 A Large ICMP 0
```

```
2154 A Ping of Death 0
```

A normal-sized ping should register as an informational event on the inside interface of ASA1/c1. Note that the ECHO reply is matched.

[Click here to view code image](#)

```
R6# ping 192.168.2.5
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.2.5, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
```

```
IP AUDIT INTERFACE COUNTERS: inside
```

```
1100 A IP Fragment Attack 0
```

```
1102 A Impossible IP Packet 0
```

```
1103 A IP Teardrop 0
```

```
2000 I ICMP Echo Reply 5
```

```
2001 I ICMP Unreachable 0
```

Configuration

ASA2

[Click here to view code image](#)

```
threat-detection basic-threat
```

```
threat-detection statistics port
```

```
threat-detection statistics protocol
```

```
threat-detection statistics access-list
```

```
no threat-detection statistics tcp-intercept
```

ASA1/c1

[Click here to view code image](#)

```
ip audit name inside info action alarm
ip audit name outside attack action reset
ip audit interface outside outside
ip audit interface inside inside
```

ASA1/c2

[Click here to view code image](#)

```
dynamic-filter enable interface outside
dynamic-filter drop blacklist interface outside
dynamic-filter blacklist
name server.ccie.com
dynamic-filter whitelist
address 10.10.110.0 255.255.255.0
address 10.10.120.0 255.255.255.0
class-map dynamic-filter-dns-snoop
match port udp eq domain

policy-map dynamic-filter-dns-snoop
class dynamic-filter-dns-snoop
inspect dns dynamic-filter-snoop

service-policy dynamic-filter-dns-snoop interface outside
```

Tech Notes

Threat detection statistics can help analyze and manage threats to the Cisco ASA. This information can be used to help the administrator understand usage patterns and devise and configure an IPS policy on a separate sensor device. The threat defense feature can also be configured for scanning; however, this is a processor-intensive feature and should be used with care.

There are two levels of threat detection statistics:

- **Basic threat detection statistics:** Includes information about attack activity for the system as a whole. Basic threat detection statistics are enabled by default and have no performance impact.
- **Advanced threat detection statistics:** Tracks activity at an object level, so the ASA can report activity for individual hosts, ports, protocols, or access lists. Advanced threat detection statistics can have a major performance impact, depending on the statistics gathered; only access list statistics are enabled by default.

A summary of IP audit attacks and informational events follows:

```
1000 I Bad IP Options List
1001 I Record Packet Route
1002 I Timestamp
1003 I Provide s,c,h,tcc
```

1004 I Loose Source Route
1005 I SATNET ID
1006 I Strict Source Route
1100 A IP Fragment Attack
1102 A Impossible IP Packet
1103 A IP Teardrop
2000 I ICMP Echo Reply
2001 I ICMP Unreachable
2002 I ICMP Source Quench
2003 I ICMP Redirect
2004 I ICMP Echo Request
2005 I ICMP Time Exceed
2006 I ICMP Parameter Problem
2007 I ICMP Time Request
2008 I ICMP Time Reply
2009 I ICMP Info Request
2010 I ICMP Info Reply
2011 I ICMP Address Mask Request
2012 I ICMP Address Mask Reply
2150 A Fragmented ICMP
2151 A Large ICMP
2154 A Ping of Death
3040 A TCP No Flags
3041 A TCP SYN & FIN Flags Only
3042 A TCP FIN Flag Only
3153 A FTP Improper Address
3154 A FTP Improper Port
4050 A Bomb
4051 A Snork
4052 A Chargen
6050 I DNS Host Info
6051 I DNS Zone Xfer
6052 I DNS Zone Xfer High Port
6053 I DNS All Records
6100 I RPC Port Registration
6101 I RPC Port Unregistration
6102 I RPC Dump
6103 A Proxied RPC
6150 I ypserv Portmap Request
6151 I ypbind Portmap Request
6152 I yppasswdd Portmap Request
6153 I ypupdated Portmap Request
6154 I ypxfrd Portmap Request
6155 I mountd Portmap Request
6175 I rexd Portmap Request

Solution and Verification for Exercise 1.4: Configure IPv6 on ASA2

Skills Tested

- Basic IPv6 configuration on the Cisco ASA
- Understanding IPv6 Neighbor Discovery Protocol

Solution and Verification

This exercise requires a basic IPv6 interface configuration. The process of neighbor discovery begins after an IPv6 address is enabled on an interface. IPv6 hosts use Neighbor Discovery Protocol (NDP) to learn their own addresses (if autoconfiguration is required), as well as the addresses of their neighbors, including any gateways. Neighbors are learned through neighbor solicitation (NS) and neighbor advertisement (NA) ICMPv6 messages. Gateways/routers are learned on a segment by sending router solicitation (RS) ICMPv6 messages to which routers will send router advertisement (RA) messages indicating their link prefixes and hop counts. Attackers can use the information in an RA message to do reconnaissance on the network, so these ICMPv6 messages are often suppressed on interfaces where a specific device should not advertise information about itself—for example, on a public-facing interface. In this question, the routers on the same segments as the ASA IPv6 interfaces will advertise themselves as the IPv6 default gateways and the source of any autoconfiguration parameters. ASA2 does not perform this function and will not send RA messages.

For all verification syntax that follows:

- Required output appears in **red**

Verify the IPv6 addresses on the inside and DMZ interfaces:

[Click here to view code image](#)

```
ASA2# show ipv6 int inside
inside is up, line protocol is up
IPv6 is enabled, link-local address is fe80::215:c6ff:fe95:c648
Global unicast address(es):
  2001:db8:40::20, subnet is 2001:db8:40::/64
Joined group address(es):
  ff02::1
  ff02::2
  ff02::1:ff00:20
  ff02::1:ff95:c648
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
Hosts use stateless autoconfig for addresses.
```

```
ASA2# show ipv6 int dmz
```

dmz is up, line protocol is up
IPv6 is enabled, link-local address is fe80::215:c6ff:fe95:c649
Global unicast address(es):
2001:db9:30::20, subnet is 2001:db9:30::/64
Joined group address(es):
ff02::1
ff02::2
ff02::1:ff00:20
ff02::1:ff95:c649
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
Hosts use stateless autoconfig for addresses.

Verify whether RA messages are being suppressed on the inside and DMZ interfaces:

[Click here to view code image](#)

```
ASA2# show run | begin interface GigabitEthernet0/2
interface GigabitEthernet0/2
 nameif inside
 security-level 100
 ip address 10.50.40.20 255.255.255.0
 ipv6 address 2001:db8:40::20/64
 ipv6 enable
 ipv6 nd suppress-ra
 ospf message-digest-key 1 md5 *****
 ospf authentication message-digest
```

```
ASA2# show run | begin interface GigabitEthernet0/3
interface GigabitEthernet0/3
 nameif dmz
 security-level 50
 ip address 10.50.30.20 255.255.255.0
 ipv6 address 2001:db9:30::20/64
 ipv6 enable
 ipv6 nd suppress-ra
```

Configuration

[Click here to view code image](#)

```
interface GigabitEthernet0/2
 ipv6 address 2001:db8:40::20/64
 ipv6 enable
 ipv6 nd suppress-ra
```

```
ASA2# show run | begin interface GigabitEthernet0/3
interface GigabitEthernet0/3
  ipv6 address 2001:db9:30::20/64
  ipv6 enable
  ipv6 nd suppress-ra
```

Tech Notes

IPv6 Addressing Review

IPv6 was created to meet the demand for more IP addresses than IPv4 could accommodate.

IPv6 provides a way to allocate address ranges in a more optimized way due to the large amount of addresses available.

IPv6 Addressing Notation

IPv6 addresses are 128 bits long, are represented in hexadecimal form, and use colon-separated fields of 16 bits as follows:

```
1234:5678:DEF0:1234:5678:9ABC:DEF0
```

A device can have more than one IPv6 address assigned to an interface, all of equal precedence. Each address consists of a network and host value referred to as the *prefix* and *interface ID*. In lieu of a subnet mask, IPv6 subnets use slash notation to identify the network portion of the address:

```
1234:5678:DEF0:1234:5678:9ABC:DEF0/64
```

Because IPv6 addresses are quite long, two abbreviation rules can be used when applicable:

- If one or more successive 16-bit groups of an IPv6 address consist of all 0s, that portion of the address can be omitted and replaced by two colons. This abbreviation can be used only once in an address.
- If any 16-bit group in an IPv6 address begins with one or more 0s, these leading 0s may be omitted. This rule can be combined with the preceding rule for any IPv6 address.

The results of applying these abbreviation rules are illustrated using the following sample address:

```
2001:0001:0000:0000:00A1:0CC0:01AB:397A
```

This address can be abbreviated as any of the following:

```
2001:1:0:0:A1:CC0:1AB:397A
```

```
2001:0001::00A1:0CC0:01AB:397A
```

```
2001:1::A1:CC0:1AB:397A
```

IPv6 Address Types

As with IPv4, IPv6 requires the use of several address types to operate as a Layer 3 protocol. The types of addresses supported by IPv6 are unicast, multicast, and anycast. There is no broadcast address in IPv6. [Table 2a-1](#) summarizes these address types and their application.

Address Type	Range	Application	Notation
Aggregate global unicast	2000::/3	Host-host	Addresses that begin with hex 2 or 3 in the first 3 bits Next 45 bits are the global routing prefix Next 16 bits are the subnet ID Last 64 bits are the interface ID
Multicast	FF00::/8	One-many, many-many	See Table 1-4
Anycast	As per unicast	Application-based	The same address shared by devices supporting specific applications or functions, such as load balancing; not used as a source address of traffic
Link-local unicast	FE80::/10	Connected-link local	Interface portion derived using EUI-64 format
Solicited-node multicast	FF02::1: FF00:0/104	Neighbor solicitation	Discussed in Section 1.3
IPv4-compatible IPv6	First 96 bits are 0	Maps a v4-to-v6 address in hex	Not a design best practice; example: 10.10.100.16 -> ::10:10:100:16
Unspecified address		No unicast address available/assigned	:: is used as the source address on an interface that has not yet been assigned an address; cannot be used as a destination

Table 2a-1 *IPv6 Address Types*

A special note must be made of IPv6 multicast addresses. Because there is no concept of a broadcast address in IPv6, multicast takes the place of all functions that would use broadcast in an IPv4 network.

As shown in [Table 2a-1](#), an IPv6 multicast address always begins with FF as the first octet. The second octet specifies lifetime (permanent—0000 or temporary—0001) and scope:

0001 = Node

0010 = Link

0101 = Site

1000 = Organization

1110 = Global

[Table 2a-2](#) shows several well-known IPv6 multicast group addresses and their functions.

Function	Multicast Group	IPv4 Equivalent
All hosts	FF02::1	Subnet broadcast address
All routers	FF02::2	224.0.0.2
OSPFv3 routers	FF02::5	224.0.0.5
OSPFv3 designated routers	FF02::6	224.0.0.6
EIGRP routers	FF02::A	224.0.0.10
PIM routers	FF02::D	224.0.0.13

Table 2a-2 IPv6 Multicast Well-known Addresses

IPv6 Address Allocation

To facilitate the administration of IPv6 addressing, a process called autoconfiguration was defined. An IPv6 host can configure its complete address or the interface ID portion of its address, depending on the method of autoconfiguration used:

- **Stateful autoconfiguration:** Assigns the entire 128-bit IPv6 address using DHCP.
- **Stateless autoconfiguration:** Dynamic assignment of a 64-bit prefix to an interface. The remaining 64 bits of the interface ID are derived from the EUI-64 address format.

With EUI-64, the interface ID is a locally configured globally unique value. Global uniqueness is ensured in Ethernet interfaces by the use of the MAC address of that interface, which is used with the IEEE EUI-64 standard. The following example illustrates how this is achieved:

Given the IPv6 prefix of 2001:128:1F:633 and a MAC address of 00:07:85:80:71:B8, the resulting EUI-64 address is

2001:128:1F:633:207:85FF:FE80:71B8/64

EUI-64 sets the seventh bit in the interface ID (universal/local scope set to global) and inserts a hex value of FFFE into the center of the MAC address to add the required 16 additional bits to the 48-bit MAC address to yield a 64-bit interface ID.

IPv6 Addressing Standards

The following standards are useful for further reading on IPv6 addressing:

- RFC 4291—IPv6 Addressing Architecture
- RFC 3587—IPv6 Global Unicast Address Format
- RFC 4862—IPv6 Stateless Address Autoconfiguration
- RFC 4007—IPv6 Scoped Address Architecture

Solution and Verification for Exercise 1.5: Cisco IOS Zone-Based Firewall with Support for Secure Group Tagging

Skills Tested

- Configuring Cisco ZFW with multi-zone application
- Defining firewall policy based on an understanding of traffic flows and network protocols in the network

- Using secure group tags and a source identifier of interesting traffic to match

Solution and Verification

When configuring ZFW, the Modular QoS CLI (MQC) style of syntax consisting of class maps, policy maps, and service policies is used with the **inspect** keyword. This command syntax is called Cisco Policy Language (CPL). Cisco IOS ZFW functionality is often referred to as **ip inspect**.

ZFW maps interface groupings to zones. Traffic passing between zones must be explicitly allowed. Zones are user-defined groups of interfaces. In addition, the addresses on the router itself form a special “self” zone. By default, traffic and protocols sourced from or destined to the self zone do not require explicit rules, although they can be applied to implement stateful firewalling or to explicitly deny flows between the self zone and the user-defined zones.

This question requires the administrator to have a clear understanding of the traffic traversing and terminating on R6. Traffic not explicitly allowed between user-defined zones is implicitly denied. ZFW will inspect at Layers 4 through 7 and track UDP and TCP connection state. IP protocols that cannot be inspected at Layer 4 or Layer 7 must be explicitly allowed between zones by using an access list; for example, Encapsulating Security Payload (ESP) traffic. DMVPN traffic is required to allow communication between hub and spokes, and ESP is encapsulated in UDP/4500 by virtue of NAT-T negotiation, which requires a firewall rule on R6.

R6 is a tunnel termination point for several virtual private network (VPN) tunnels, as well as being a Border Gateway Protocol (BGP) peer and Open Shortest Path First (OSPF) neighbor; all of these functions fall within the self zone, which in the exercise is supporting the default behavior of not requiring explicit ZFW policy to allow traffic to flow in and out of the self zone.

This exercise requires deep packet inspection (DPI) of HTTP, using the HTTP application inspection and control (AIC) engine, and the reset action must be used. A Layer 7 (DPI) policy map must be nested at the second level in a Layer 3 or Layer 4 inspect policy map; therefore, a Layer 7 policy map cannot be attached directly to a zone pair. You can specify the reset action only for TCP traffic.

ZFW also supports Security Group Tags (SGT) on specific platforms. In the case of the ISR G2 (used in this example), an SGT can be used to identify the source address of traffic within an ip inspect policy. The IP-to-SGT mappings are learned by R6 from SW2. These tags are then added to a class map to identify traffic sources of interest. SGTs will be propagated to R6 via SGT Exchange Protocol (SXP) and will be used as the source identifiers for the firewall match criteria.

To learn these mappings, R6 will take the role as an SXP local listener and peer with SW2 as the remote speaker as configured in [Exercise 6.3](#).

For all verification syntax that follows:

- Required output appears in **red**
- Variable syntax appears in **green**

This exercise required two user-defined zones. The output of the **show zone security** command will display each zone and its member interfaces. Note that the self zone, which is system-defined, will always be displayed in this output and contains no interfaces. All of the IP interfaces on the router are automatically made part of the self zone when ZFW is configured.

[Click here to view code image](#)

```
R6# show zone security
```

zone self

Description: System defined zone

zone **outside**

Member Interfaces:

Ethernet0/1

zone **inside**

Member Interfaces:

Ethernet0/0

Verification of the ZFW policy and its application on the router can be done for the most part using the **show policy-map type inspect zone-pair sessions** command. The names highlighted in green are user-defined names. The access control list (ACL) content itself is verified later in this section. Note the highlighted **match-any** and **match-all** usage. In the case of a single traffic match criteria in a class map or policy map, either **match-all** or **match-any** may be used. For multiple match criteria, **match-all** implies AND, **match-any** implies OR.

[Click here to view code image](#)

```
R6# show policy-map type inspect zone-pair sessions
```

policy exists on zp **out-in**

Zone-pair: out-in

Service-policy inspect : **firewall-policy-in**

Class-map: crypto (**match-any**)

Match: **access-group 102**

0 packets, 0 bytes

30 second rate 0 bps

Match: protocol **isakmp**

0 packets, 0 bytes

30 second rate 0 bps

Match: protocol **gdoi**

0 packets, 0 bytes

30 second rate 0 bps

Match: **access-group 103**

0 packets, 0 bytes

30 second rate 0 bps

Pass

0 packets, 0 bytes

Class-map: **sgt4policy** (**match-all**)

Match: class-map match-any sgt4

Match: security-group source tag 4

0 packets, 0 bytes

30 second rate 0 bps

Match: class-map match-any in-sgt-inspect

Match: protocol icmp

0 packets, 0 bytes

30 second rate 0 bps

Match: protocol udp

0 packets, 0 bytes

30 second rate 0 bps

Class-map: sgt5policy (match-all)

Match: class-map match-any sgt5

Match: security-group source tag 5

0 packets, 0 bytes

30 second rate 0 bps

Match: class-map match-any in-sgt-inspect

Match: protocol icmp

0 packets, 0 bytes

30 second rate 0 bps

Match: protocol udp

0 packets, 0 bytes

30 second rate 0 bps

Inspect

Class-map: in-inspect (match-any)

Match: protocol icmp

0 packets, 0 bytes

30 second rate 0 bps

Match: protocol telnet

0 packets, 0 bytes

30 second rate 0 bps

Match: protocol dns

0 packets, 0 bytes

30 second rate 0 bps

Match: protocol ntp

0 packets, 0 bytes

30 second rate 0 bps

Match: protocol radius

0 packets, 0 bytes

30 second rate 0 bps

Match: protocol tacacs

0 packets, 0 bytes

30 second rate 0 bps

Match: protocol **http**

0 packets, 0 bytes

30 second rate 0 bps

Match: protocol **https**

0 packets, 0 bytes

30 second rate 0 bps

Inspect

Class-map: class-default (match-any)

Match: any

Drop

0 packets, 0 bytes

policy exists on zp **in-out**

Zone-pair: in-out

Service-policy inspect : **firewall-policy-out**

Class-map: crypto (match-any)

Match: **access-group 102**

0 packets, 0 bytes

30 second rate 0 bps

Match: protocol **isakmp**

0 packets, 0 bytes

30 second rate 0 bps

Match: protocol **gdoi**

0 packets, 0 bytes

30 second rate 0 bps

Match: **access-group 103**

0 packets, 0 bytes

30 second rate 0 bps

Pass

0 packets, 0 bytes

Class-map: http (match-all)

Match: **protocol http**

Inspect

Class-map: out-inspect (match-any)

Match: **access-group 101**

0 packets, 0 bytes

30 second rate 0 bps

Inspect

Class-map: class-default (match-any)

Match: any

Drop

0 packets, 0 bytes

Verify ACLs are defined as follows:

[Click here to view code image](#)

```
R6# show access-list
```

```
Extended IP access list 101
```

```
10 permit ip any any
```

```
Extended IP access list 102
```

```
10 permit udp 10.50.0.0 0.0.255.255 10.50.0.0 0.0.255.255 eq non500-isakmp
```

```
20 permit esp 10.50.0.0 0.0.255.255 10.50.0.0 0.0.255.255
```

```
Extended IP access list 103
```

```
10 permit gre 10.50.0.0 0.0.255.255 10.50.0.0 0.0.255.255
```

The Layer 7 AIC engine for HTTP configuration may be verified using the following:

[Click here to view code image](#)

```
R6# show class-map type inspect http
```

```
Class Map type inspect http match-any httpDPI (id 2)
```

```
Match request port-misuse tunneling
```

```
R6# show policy-map type inspect http
```

```
Policy Map type inspect http resetportmisuse
```

```
Class httpDPI
```

```
Reset
```

```
Log
```

Support for SGTs as the source of traffic flows to be subject to ZFW inspection requires that R6 has knowledge of the mapping from an IP address to an SGT. Not all devices can natively use the tags added to packets by SGT-capable hardware. In this case, tags must be either manually defined or learned via SXP (covered in Lab 2, [Exercises 6.2](#) and [6.3](#)). If SXP is successfully configured between R6 (listener) and SW2 (speaker), the SGT tags 4 and 5 will appear in the output of **show cts role-based sgt all**. This is the preferred method for learning these dynamically created mappings because the IP addresses associated with the SGT values are DHCP issued and may not remain static.

[Click here to view code image](#)

```
R6# show cts role sgt all
```

```
Active IP-SGT Bindings Information
```

```
IP Address      SGT    Source
```

10.50.9.5	2	SXP
10.50.9.7	4	SXP
10.50.30.3	12	SXP
10.50.30.4	12	SXP
10.50.40.7	7	SXP
10.50.50.5	2	SXP
10.50.50.20	14	SXP
10.50.70.4	3	SXP
10.50.70.5	2	SXP
10.50.70.6	3	SXP
10.50.77.5	2	SXP
10.50.77.253	5	SXP
10.50.80.50	16	SXP
10.50.99.5	2	SXP
10.50.100.1	15	SXP
10.50.100.2	15	SXP
10.50.100.10	15	SXP
192.168.2.25	18	SXP

Configuration

R6

[Click here to view code image](#)

```
cts sxp enable
cts sxp connection peer 10.50.70.5 password none mode local listener
class-map type inspect match-any crypto
  match access-group 102
  match protocol isakmp
  match protocol gdoi
  match access-group 103
class-map type inspect match-any in-sgt-inspect
  match protocol icmp
  match protocol udp
class-map type inspect match-all http
  match protocol http
class-map type inspect match-any out-inspect
  match access-group 101
class-map type inspect http match-any httpDPI
  match request port-misuse tunneling
class-map type inspect match-any sgt4
  match security-group source tag 4
class-map type inspect match-all sgt4policy
  match class-map sgt4
  match class-map in-sgt-inspect
```

```
class-map type inspect match-any sgt5
  match security-group source tag 5
class-map type inspect match-all sgt5policy
  match class-map sgt5
  match class-map in-sgt-inspect
class-map type inspect match-any in-inspect
  match protocol icmp
  match protocol telnet
  match protocol dns
  match protocol ntp
  match protocol radius
  match protocol tacacs
  match protocol http
  match protocol https!
!
policy-map type inspect http resetportmisuse
  class type inspect http httpDPI
  reset
!
policy-map type inspect firewall-policy-in
  class type inspect crypto
  pass
  class type inspect sgt4policy
  inspect
  class type inspect sgt5policy
  inspect
  class type inspect in-inspect
  inspect
  class class-default
  drop
!

policy-map type inspect firewall-policy-out
  class type inspect crypto
  pass
  class type inspect http
  inspect
  service-policy http resetportmisuse
  class type inspect out-inspect
  inspect
  class class-default
  drop
!
zone security outside
zone security inside
```



```

zone-pair security out-in source outside destination inside
  service-policy type inspect firewall-policy-in
zone-pair security in-out source inside destination outside
  service-policy type inspect firewall-policy-out
!
interface Ethernet0/0
  zone-member security inside
!
interface Ethernet0/1
  zone-member security outside

```

```

access-list 101 permit ip any any
access-list 102 permit udp 10.50.0.0 0.0.255.255 10.50.0.0 0.0.255.255 eq
  non500-isakmp
access-list 102 permit esp 10.50.0.0 0.0.255.255 10.50.0.0 0.0.255.255
access-list 103 permit gre 10.50.0.0 0.0.255.255 10.50.0.0 0.0.255.255

```

Tech Notes

The Cisco IOS Zone-Based Firewall is the successor to Context-Based Access Control (CBAC) and enables multiple router interfaces to be grouped into security zones. Configuration of ZFW involves three elements:

- **Security Zone:** A security zone is a group of interfaces to which a policy can be applied. By default, traffic flows freely between interfaces in the same zone, but traffic between zones is explicitly dropped. There is no concept of levels of security that dictate implicit behavior as with the Cisco ASA. The types of policies applied per zone dictate the level of security. All flows require a rule, even if it's a simple **pass ip any any**. Flows between user-defined zones represent router transit traffic. Traffic sourced and destined to addresses on the router itself belongs to a system-defined zone known as the self zone. By default, traffic in and out of the self zone is not examined and flows freely.
- **Zone Pair:** A zone pair applies a unidirectional firewall policy between two zones. The zone pair specifies the source and destination zone and a traffic flow direction (for example, inside to outside or outside to inside). If traffic into and out of the self zone is to be processed by ZFW, the self zone must be specified as the source or destination zone in a zone pair; for example, self to outside.
- **Zone Policy:** A zone policy defines traffic match criteria and the actions to be performed on it. The command syntax for ZFW is known as Cisco Policy Language (CPL), which is a form of MQC that introduces a special class map and policy map type **inspect**. Traffic that matches the interesting criteria is subject to the following actions: **drop**, **pass**, and **inspect**.
 - **Drop:** The default action for all traffic, as applied by the class class-default that terminates every inspect-type policy map. Other class maps within a policy map can also be configured to drop unwanted traffic. Traffic that is handled by the drop action is “silently” dropped (that is, no notification of the drop is sent to the relevant end host) by the ZFW, as opposed to an ACL's behavior of sending an ICMP “host unreachable” message to the host that sent the denied traffic. The log option can be added with drop for syslog notification that traffic

was dropped by the firewall.

- **Pass:** Enables the router to forward traffic from one zone to another. The pass action does not track the state of connections or sessions within the traffic. Pass enables the traffic in only one direction. A corresponding policy must be applied to enable return traffic to pass in the opposite direction. The pass action is useful for protocols such as IPsec ESP, IPsec AH, ISAKMP, and other inherently secure protocols with predictable behavior. May be combined with the log option for syslog message generation.
- **Inspect:** The inspect action offers traffic selector (Layer 3), state-based (Layer 4), and application engine deep packet inspection (DPI) (Layer 7) traffic control. For example, if traffic from a private zone to an Internet zone is inspected, the router maintains connection or session information for TCP and UDP traffic. Therefore, the router permits return traffic sent from Internet-zone hosts in reply to private zone connection requests. Also, inspect can provide application inspection and control for certain service protocols that might carry vulnerable or sensitive application traffic. An audit trail can be applied with a parameter map to record connection/session start, stop, duration, the data volume transferred, and source and destination addresses.
- **Content Filter:** Lets you configure HTTP content inspection (URL filtering) based on a WebFilter parameter map or a WebFilter policy map. This action is generally equivalent to a Web Filter rule; however, zone-based firewall rules support additional advanced options, such as HTTP DPI.

Interesting traffic can be identified at various layers of the OSI model:

- **Layer 3:** Uses ACLs to identify specific flows. These can be used to identify IP protocols such as ESP and generic routing encapsulation (GRE), which are combined with the pass or drop actions because these encapsulated traffic flows cannot be inspected at Layer 4 or Layer 7. An ACL may also be combined with a Layer 4 protocol in a match-all class map for finer control.

Example:

[Click here to view code image](#)

```
Device(config)# class-map type inspect match-all c1
Device(config-cmap)# match access-group 101
Device(config-cmap)# match protocol http
```

Class maps can apply an ACL as one of the match criteria for policy application. If a class map's only match criterion is an ACL, and the class map is associated with a policy map applying the inspect action, the router applies basic TCP or UDP inspection for all traffic allowed by the ACL as applicable, except that for which ZFW provides application-aware inspection.

If application-specific visibility into network activity is desired, you must configure inspection for services by application name (configure **match protocol http**, **match protocol telnet**, and so on).

- **Layer 4:** Defined using **match protocol protocol** in a class map and usually combined with an inspect action. If multiple protocols are to be inspected under one class map, care must be taken with **match-all** versus **match-any** types.

Example:

If the goal is to match ICMP *or* HTTP traffic, the following will not match any traffic because a packet cannot be both an HTTP *and* ICMP packet:

[Click here to view code image](#)

```
Device(config)# class-map type inspect match-all c1
Device(config-cmap)# match protocol http
Device(config-cmap)# match protocol icmp
```

The correct configuration is

[Click here to view code image](#)

```
Device(config)# class-map type inspect match-any c1
Device(config-cmap)# match protocol http
Device(config-cmap)# match protocol icmp
```

- **Layer 7:** DPI functionality is delivered through Layer 7 class maps and policy maps for specific applications using AIC engines. The list of support applications can vary with the version of Cisco IOS in use.

[Click here to view code image](#)

```
Device(config)# class-map type inspect ?
aol      Configure Firewall class-map for IM-AOL protocol
edonkey  eDonkey
fasttrack FastTrack Traffic - KaZaA, Morpheus, Grokster...
gnutella Gnutella Version2 Traffic - BearShare, Shareaza, Morpheus ...
h323     Configure Firewall class-map for H323 protocol
http     Configure Firewall class-map for HTTP protocol
icq      Configure Firewall class-map for IM-ICQ protocol
imap     Configure Firewall class-map for IMAP protocol
kazaa2   Kazaa Version 2
match-all Logical-AND all matching statements under this classmap
match-any Logical-OR all matching statements under this classmap
msnmsgr  Configure Firewall class-map for IM-MSN protocol
pop3     Configure Firewall class-map for POP3 protocol
sip      Configure Firewall class-map for SIP protocol
smtp     Configure Firewall class-map for SMTP protocol
sunrpc   Configure Firewall class-map for RPC protocol
winmsgr  Configure Firewall class-map for IM-WINMSGR protocol
ymsgr    Configure Firewall class-map for IM-YAHOO protocol
```

Separate Layer 4 class maps are defined for HTTP, Yahoo Messenger, and eDonkey because Layer 7 application inspection policy for these protocols must be applied to their respective Layer 4 policy maps as in the exercise; for example:

Define the Layer 4 match criteria:

[Click here to view code image](#)

```
R6(config)# class-map type inspect match-all http
R6(config-cmap)# match protocol http
```

Define the DPI requirements:

[Click here to view code image](#)

```
R6(config)# class-map type inspect http match-any httpDPI
R6(config-cmap)# match request port-misuse ?
any      Any type of port misuse
im       Instant Messaging
p2p      Peer-to-peer application
tunneling Tunneling applications
```

```
R6(config-cmap)# match request port-misuse tunneling
R6(config-cmap)# exit
```

Define the actions to be performed on the DPI match criteria:

[Click here to view code image](#)

```
R6(config)# policy-map type inspect http resetportmisuse
R6(config-pmap)# class type inspect http httpDPI
R6(config-pmap-c)# reset
```

The final policy will identify HTTP traffic to be DPI inspected using the HTTP AIC engine to check for specific conditions.

[Click here to view code image](#)

```
R6(config)# policy-map type inspect firewall-policy
R6(config-pmap)# class type inspect remotes2
R6(config-pmap-c)# inspect
R6(config-pmap-c)# service-policy http resetportmisuse
```

Section 2: Intrusion Prevention and Content Security

This section covers more advanced tasks applicable to the Intrusion Prevention Sensor (IPS) and Web Services Appliance (WSA). Configuring custom signatures and defining event action overrides are important signature tuning techniques applicable to the Cisco IPS. In Lab 1, you initialized the WSA and configured Web Cache Communication Protocol (WCCP) Transparent proxy service using the ASA as the WCCP server. In this section, you add user authentication to this scenario, and then incorporate guest services.

Solution and Verification for Exercise 2.1: Configuring Custom Signatures on the Cisco IPS Sensor

Skills Tested

- IPS sensor custom signature configuration
- Understanding the components of attacks and vulnerabilities

- Defining event actions and overrides and manipulating risk ratings
- Applying signatures and event action rules to virtual sensors
- Verifying whether signatures are working correctly with real-time traffic
- Understanding the functions and benefits of IPS sensor signature engines

Solution and Verification

Implementing custom signatures requires a good understanding of the threats and vulnerabilities that impact specific network deployments. Signatures are customized based on the priorities of the network and go above and beyond the signature database that covers all types of well-known attacks. The purpose of this exercise is to illustrate the options available to the administrator in terms of signature engine selection, event actions, and alert severities and formulating signature trigger criteria. This criterion varies according to the requirements of the signature engine selected.

Signatures can also be customized in terms of how they are applied with respect to risk ratings. Although a trigger might be the same, the actions taken can differ depending on the risk to the hosts or subnets impacted. Event action rule sets are a way to override the general rules associated with a signature depending on the risk criteria. They are also an efficient way of applying a blanket policy to the groups of signatures assigned to a virtual sensor, eliminating the need to individually define actions and alerts.

Various **show** command outputs can provide custom signature configuration verification, including those that show events in real time.

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**
- Variable syntax appears in **green**

Custom Signature to Track OSPF TTL

All OSPF packets seen by vs0 should have a time to live (TTL) of 255. Vs0 is sensing traffic in OSPF Area 0 from the perspective of SW2. All neighbors are adjacent to SW2. In a real-world situation, the signature would trigger for any OSPF packet that has a TTL value less than the specific value.

The **show events alert severity-level** command displays a trigger packet in real time. In the following output, 0xFF is the TTL value 255 and 0x59 is IP protocol 89 (OSPF):

[Click here to view code image](#)

```
IPS# show events alert medium
```

```
evIdsAlert: eventId=1374345338767123448 severity=medium vendor=Cisco  
originator:  
  hostId: ips  
  appName: sensorApp  
  appInstanceId: 414  
time: 2013/08/27 21:42:25 2013/08/27 21:42:25 UTC  
signature: description=OSPF TTL id=64000 created=20000101 type=other
```

version=custom
subsigId: 0
sigDetails: My Sig Info
marsCategory: Info/Misc

interfaceGroup: vs0

vlan: 70

participants:

attacker:

addr: locality=OUT 10.50.70.5

target:

addr: locality=OUT 224.0.0.5

os: idSource=unknown relevance=relevant type=unknown

triggerPacket:

```
000000 01 00 5E 00 00 05 C4 64 13 FC 2A 44 81 00 C0 32 ..^....d..*D...2
000010 08 00 45 C0 00 50 E0 C6 00 00 FF 59 A9 91 0A 32 ..E..P....Y...2
000020 46 05 E0 00 00 05 02 01 00 30 02 02 02 02 00 00 F.....0.....
000030 00 00 3C 1B 00 00 00 00 00 00 00 00 00 00 FF FF ..<.....
000040 FF 00 00 0A 12 01 00 00 00 28 0A 32 46 06 0A 32 .....(.2F..2
000050 46 05 06 06 06 06 FF F6 00 03 00 01 00 04 00 00 F.....
000060 00 01 ..
```

riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 66

threatRatingValue: 66

interface: ge0_2

protocol: IP protocol 89

Custom Signature to Identify and Deny Large ICMP Packets

This signature is verified by sending an ICMP packet within the specified trigger range. The verbose alerts will display the packet dump. Values highlighted in green are the fragment-specific bits.

[Click here to view code image](#)

```
R6# ping 10.50.40.7 size 1500
```

```
IPS# show event alert high
```

evIdsAlert: eventId=1374345338767123402 severity=high vendor=Cisco

originator:

hostId: ips

appName: sensorApp

appInstanceId: 414

time: 2013/08/27 21:23:46 2013/08/27 21:23:46 UTC

signature: description=Large ICMP Attack id=65000 created=20000101 type=other

version=custom

subsigId: 0

sigDetails: My Sig Info

marsCategory: Info/Misc

interfaceGroup: vs0

vlan: 50

participants:

attacker:

addr: locality=OUT 10.50.70.6

target:

addr: locality=OUT 10.50.40.7

os: idSource=unknown relevance=relevant type=unknown

triggerPacket:

000000 00 15 C6 95 C6 46 C4 64 13 FC 2A 43 81 00 00 46F.d..*C...F

000010 08 00 45 00 05 DC 00 A6 00 00 FE 01 34 0A 0A 32 ..E.....4..2

000020 46 06 0A 32 28 07 08 00 C0 2E 00 0A 00 01 00 00 F..2(.....

000030 00 00 0F B9 E7 F5 AB CD AB CD AB CD AB CD AB CD

riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 85

threatRatingValue: 85

interface: ge0_2

protocol: icmp

Custom Signature to Identify and Deny an ICMP Flood Attack

To verify the flood signature and event action rules, first ping the host that has been designated as mission critical. Note that initially the ping will succeed until the configured threshold is exceeded, which triggers the signature event actions. This host was assigned a target value rating of 100, which will meet the risk rating criteria defined in the event-action rules, forcing the event-action overrides as shown under **actions** in the following output:

[Click here to view code image](#)

```
R6# ping 192.168.2.25 rep 200
```

```
Type escape sequence to abort.
```

```
Sending 2000, 100-byte ICMP Echos to 192.168.2.25, timeout is 2 seconds:
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.....
```

```
..
```

```
IPS# show events alert high
```

```
evIdsAlert: eventId=1374345338767164950 severity=high vendor=Cisco
```

```
originator:
```

```
hostId: ips
```

```
appName: sensorApp
```

```
appInstanceId: 414
```

```
time: 2013/09/21 01:34:31 2013/09/21 01:34:31 UTC
```

```
signature: description=My Sig id=62000 created=20000101 type=other
```

```
version=custom
```

```
subsigId: 0
```

```
sigDetails: My Sig Info
```

marsCategory: Info/Misc
interfaceGroup: vs1
vlan: 0
participants:
 attacker:
 addr: locality=OUT 10.50.80.6
 target:
 addr: locality=OUT 192.168.2.25
 os: idSource=learned relevance=relevant type=windows-nt-2k-xp
actions:
 logPacketsActivated: true
 deniedPacket: true
 deniedAttacker: true
 logAttackerPacketsActivated: true
ipLogIds:
 ipLogId: 1701736978
riskRatingValue: attackRelevanceRating=relevant targetValueRating=mission-critical 100
threatRatingValue: 55
interface: ge0_0
protocol: icmp

Sending a ping to a host not defined as mission critical will not meet the risk rating range of 90–100, so event-action overrides are not applied. In this case, only those actions defined under the signature definition itself are taken.

[Click here to view code image](#)

```
R3# ping 192.168.2.50 rep 100
```

```
Type escape sequence to abort.
```

```
Sending 100, 100-byte ICMP Echos to 192.168.2.50, timeout is 2 seconds:
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.
```

```
IPS# show events alert high
```

```
evIdsAlert: eventId=1374345338767164960 severity=high vendor=Cisco
```

```
originator:
```

```
  hostId: ips
```

```
  appName: sensorApp
```

```
  appInstanceId: 414
```

```
time: 2013/09/21 01:40:50 2013/09/21 01:40:50 UTC
```

```
signature: description=My Sig id=62000 created=20000101 type=other
```

```
  version=custom
```

```
  subsigId: 0
```

```
  sigDetails: My Sig Info
```

```
  marsCategory: Info/Misc
```

```
interfaceGroup: vs1
```



```
vlan: 0
participants:
  attacker:
    addr: locality=OUT 10.50.30.3
  target:
    addr: locality=OUT 192.168.2.50
    os: idSource=learned relevance=relevant type=bsd
actions:
  deniedPacket: true
riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 85
threatRatingValue: 50
interface: ge0_0
protocol: icmp
```

Viewing statistics on a virtual sensor is a good way to see a report of traffic that has been mapped to signature triggers and what actions have been taken in response to that traffic. This output is very verbose, so only the information relevant to this question is shown.

[Click here to view code image](#)

```
IPS# show stat virtual-sensor vs1
Statistics for Virtual Sensor vs1
  Name of current Signature-Defintion instance = sig1
  Name of current Event-Action-Rules instance = rules1
.....
Denied Address Information
  Number of Active Denied Attackers = 1
  Number of Denied Attackers Inserted = 1
  Number of Denied Attacker Victim Pairs Inserted = 0
  Number of Denied Attacker Service Pairs Inserted = 0
  Number of Denied Attackers Total Hits = 439
  Number of times max-denied-attackers limited creation of new entry = 0
  Number of exec Clear commands during uptime = 0
Denied Attackers and hit count for each.
  10.50.80.6 = 439
Denied Attackers with percent denied and hit count for each
Attacker Address  Victim Address  Port  Protocol  Requested Percentage
Actual Percentage Hit Count  Reputation Action
  10.50.80.6                100          100
439      false
Actions Performed
  deny-attacker-inline = 0
  deny-attacker-victim-pair-inline = 0
  deny-attacker-service-pair-inline = 0
  deny-connection-inline = 0
  deny-packet-inline = 48
  modify-packet-inline = 1588
```

```
log-attacker-packets = 20
log-pair-packets = 0
log-victim-packets = 0
produce-alert = 37
produce-verbose-alert = 2
request-block-connection = 0
request-block-host = 0
request-snmp-trap = 0
```

Configuration

[Click here to view code image](#)

```
service event-action-rules rules1
overrides deny-attacker-inline
override-item-status Enabled
risk-rating-range 90-100
exit
overrides log-attacker-packets
override-item-status Enabled
risk-rating-range 90-100
exit
overrides produce-alert
override-item-status Enabled
exit
target-value mission-critical target-address 192.168.2.25
exit
```

```
service signature-definition sig0
signatures 64000 0
alert-severity medium
sig-description
sig-name OSPF TTL
exit
engine atomic-ip
event-action produce-verbose-alert
specify-l4-protocol yes
l4-protocol other-protocol
other-ip-protocol-id 89
exit
exit
specify-ip-ttl yes
ip-ttl 255
exit
exit
status
enabled true
```

exit
exit
signatures 65000 0
alert-severity high
sig-description
sig-name Large ICMP Attack
exit
engine atomic-ip
event-action produce-verbose-alert
specify-l4-protocol yes
l4-protocol icmp

exit
exit
specify-ip-payload-length yes
ip-payload-length 1000-5000
exit
specify-ip-addr-options yes
ip-addr-options rfc-1918-address

exit
exit
status
enabled true

exit
exit
exit
! -----
service signature-definition sig1

signatures 62000 0
alert-severity high
engine flood-host
event-action produce-alert|deny-packet-inline
rate 100
protocol icmp
icmp-type 8
exit
exit
status
enabled true
exit
exit
exit

service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/2 subinterface-number 1

```
exit
virtual-sensor vs1
signature-definition sig1
event-action-rules rules1
logical-interface ipair
exit
virtual-sensor vs2
physical-interface GigabitEthernet0/3
exit
exit
```

Tech Notes

Risk Ratings

A *risk rating (RR)* is a value between 0 and 100 that represents a level of risk associated with a particular event on the network. It is configured on a per-signature basis using the attack severity rating and the signature fidelity rating, and on a per-server basis using the target value rating. The risk rating is calculated from several components, some of which are configured, some collected, and some derived. The risk rating is associated with alerts, not signatures.

Risk ratings are used to prioritize alerts. The following values are used to calculate the risk rating for a particular event:

- **Signature fidelity rating (SFR):** A weight associated with how well this signature might perform in the absence of specific knowledge of the target. The signature fidelity rating is configured per signature and indicates how accurately the signature detects the event or condition it describes.
- **Attack severity rating (ASR):** A weight associated with the severity of a successful exploit of the vulnerability.
- **Target value rating (TVR):** A weight associated with the perceived value of the target.
- **Attack relevance rating (ARR):** A weight associated with the relevancy of the targeted operating system.
- **Promiscuous delta (PD):** A weight associated with the promiscuous delta, which can be subtracted from the overall risk rating in promiscuous mode. Promiscuous delta is in the range of 0 to 30 and is configured per signature. If the trigger packet is not inline, the promiscuous delta is subtracted from the rating.
- **Watch list rating (WLR):** A weight associated with the CSA MC watch list in the range of 0 to 100. CSA MC only uses the range 0 to 35.

The risk rating formula is as follows:

$$RR = \frac{ASR * TVR * SFR}{10000} + ARR - PD + WLR$$

Understanding Threat Rating

Threat rating is risk rating that has been lowered by event actions that have been taken. Non-logging event actions have a threat rating adjustment. The largest threat rating from all the event actions taken is subtracted from the risk rating.

The event actions have the following threat ratings:

- Deny attacker inline: 45
- Deny attacker victim pair inline: 40
- Deny attacker service pair inline: 40
- Deny connection inline: 35
- Deny packet inline: 35
- Modify packet inline: 35
- Request block host: 20
- Request block connection: 20
- Reset TCP connection: 20
- Request rate limit: 20

Solution and Verification for Exercise 2.2: Enable Support for HTTPS on the Cisco WSA

Skills Tested

- WSA HTTPS proxy configuration
- Configuring HTTP Secure Server on a Cisco IOS Router

Solution and Verification

The configuration of WSA is completed using the GUI. To verify your solution, you will need to follow the steps that follow and compare your outputs.

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**

Verify whether the HTTPS server is enabled and ready to accept connections.

[Click here to view code image](#)

```
R4# show ip http server secure status  
HTTP secure server status: Enabled  
HTTP secure server port: 443  
HTTP secure server ciphersuite: 3des-edc-cbc-sha des-cbc-sha rc4-128-md5  
rc4-128-sha  
HTTP secure server client authentication: Disabled  
HTTP secure server trustpoint:  
HTTP secure server active session modules: ALL
```

Verify whether the WSA has generated its self-signed certificate under HTTP Proxy settings, as shown in [Figure 2a-1](#).



Figure 2a-1 HTTP Proxy Settings

If there is an issue with the certificate timestamp, or the Invalid Certificate Handling > Unrecognized Root Authority/Issuer option was not set from Drop to Monitor, you will encounter the error shown in [Figure 2a-2](#) when connecting to R4.

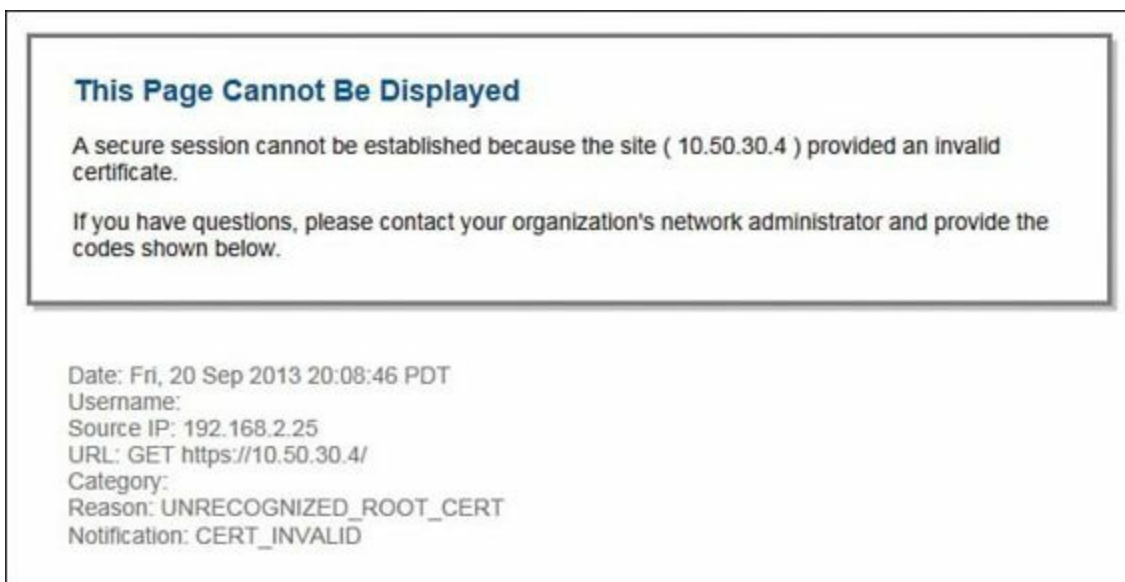


Figure 2a-2 Invalid Certificate Error

[Click here to view code image](#)

R4# **sho ip http server history** (note this must be completed after attempting a connection from a Test-PC using https://10.50.30.4 otherwise the history may be blank).

R4# **show ip http server history**

HTTP server history:

```
local-ipaddress:port remote-ipaddress:port in-bytes out-bytes end-time
10.50.30.4:443 192.168.2.50:28325 375 192 05:27:35
```

```

10.50.30.4:443    192.168.2.50:19583 371    2069    05:27:48
10.50.30.4:443    192.168.2.50:35418 324    137     05:27:48
10.50.30.4:443    192.168.2.50:50014 417    6043    05:29:08
10.50.30.4:443    192.168.2.50:55682 324    137     05:29:08

```

Configuration

R4 HTTPS Server

```
ip http secure-server
```

WSA

See [Figure 2a-1](#)

Solution and Verification for Exercise 2.3: Enable User Authentication for Transparent Proxy Using LDAP

Skills Tested

- Configuring user authentication for transparently redirected traffic on the Cisco WSA using LDAP
- Creating users on an Active Directory server
- Understanding how surrogate types impact user authentication

Solution and Verification

The configuration of the WSA is completed using the GUI. To verify your solution, you will need to follow these steps and compare your outputs:

- Step 1.** Add a user, ccie, to the Active Directory server on 192.168.2.25, as shown in [Figure 2a-3](#). These credentials will be referenced by the WSA during user authentication.

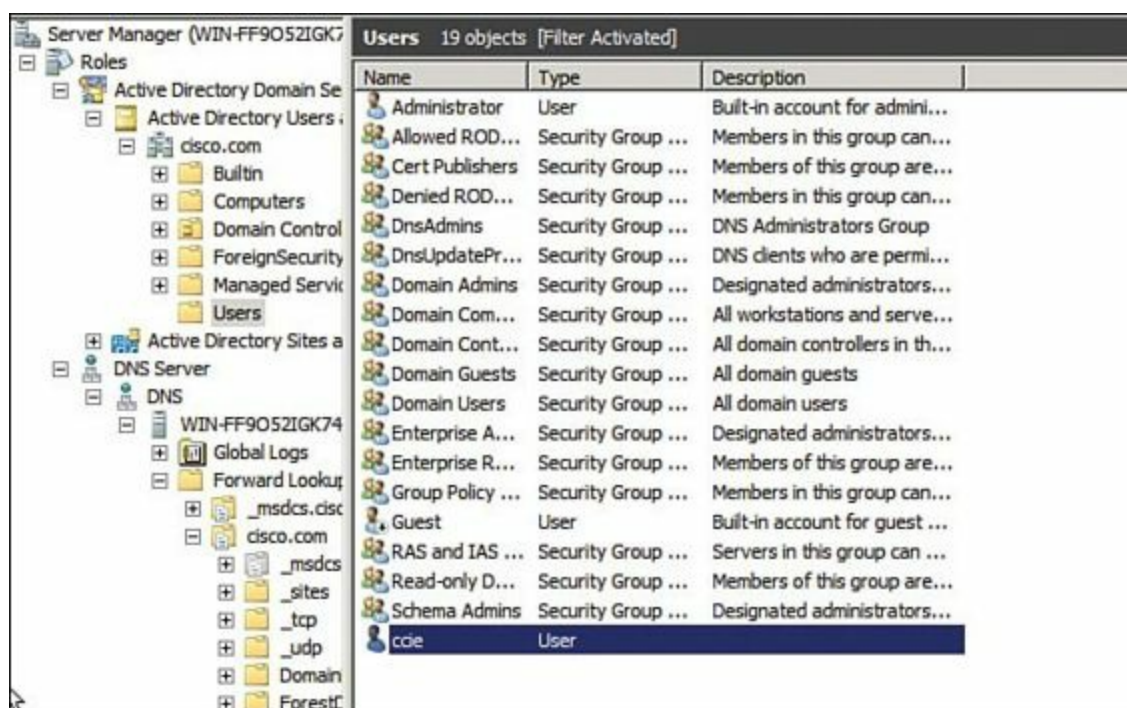


Figure 2a-3 Windows Server LDAP User Database

Step 2. Define an authentication realm using the information provided in [Table 2-11](#) in [Exercise 2-3](#) in Lab 2. After you configure the parameters, select the Start Test button at the bottom of the screen to verify whether you have connectivity with the AD server using LDAP and that your user credentials are correctly defined and accessed, as shown in [Figure 2a-4](#).

Edit Realm

LDAP Authentication Realm

Realm Name:

Authentication Protocol and Scheme(s): LDAP (Basic Authentication)

LDAP Authentication

LDAP version: Use Secure LDAP
 Enable Transparent User Identification using Novell eDirectory (?)

LDAP Server: (?) Specify up to three LDAP servers and port numbers:

:

:

:

hostname or IP address port (optional)

Advanced Optional settings for customizing the behavior of the LDAP realm

Query

User Authentication: Base DN:
(example: dc=mycompany, dc=com)

User Name Attribute:

User Filter Query:

Query Credentials: Server Accepts Anonymous Queries
 Use Bind DN
 Bind DN: (?)
 Password:
 Confirm Password:

Figure 2a-4 WSA LDAP Authentication Realm Settings

Step 3. Ensure that your global authentication settings include enabling credential encryption, as shown in [Figure 2a-5](#).

Authentication

Authentication Realms

Realm Name	Protocol	Scheme(s)	Servers	Transparent User Identification	Base DN or NetBIOS Domain	Delete
CCIELAB	LDAP	Basic	192.168.2.25	Not Enabled	dc=cisco,dc=com	<input type="button" value="Delete"/>

Global Authentication Settings

Action if Authentication Service Unavailable: Block all traffic if authentication fails

Failed Authentication Handling: Log Guest User by: IP Address

Re-authentication: Disabled

Basic Authentication Token TTL: 3600

Authentication Settings

Credential Encryption: Enabled

HTTPS Redirect Port: 443

Redirect Hostname: wsa.cisco.com

Credential Cache Options: Surrogate Timeout: 3600 seconds
 Client IP Idle Timeout: 3600 seconds
 Cache Size: 8192 entries

User Session Restrictions: Disabled

Secure Authentication Certificate: Common name: Cisco IronPort Appliance Demo Certificate
 Organization: Cisco IronPort Systems, Inc.
 Organizational Unit:
 Country: US
 Expiration Date: Mar 17 23:58:17 2022 GMT
 Basic Constraints: Not Critical

Figure 2a-5 WSA Global Authentication Settings

Step 4. Configure an authentication identity that outlines the policy to be applied to users authenticating via the CCIELAB realm defined in Step 2, as shown in [Figure 2a-6](#).

Order	Membership Definition	End-User Acknowledgement	Delete
1	Guest Policy Protocols: HTTP/HTTPS Authentication: Realm: CCIELAB (Scheme: Basic) Guest privileges for users failing authentication Surrogate Type: HTTP/HTTPS: Session Cookie	(global policy)	
2	CCIELAB Policy Protocols: HTTP/HTTPS Authentication: Realm: CCIELAB (Scheme: Basic) Surrogate Type: HTTP/HTTPS: Session Cookie	(global policy)	
	Global Identity Policy Authentication: Exempt from authentication	Not Available	

Authentication: Enabled Disabled

Figure 2a-6 WSA Identity Definitions

Step 5. To verify the solution, use the Test-PC browser to connect to any HTTP server in the network, and you should receive a prompt from the WSA for username/password credentials as shown in [Figure 2a-7](#).



Figure 2a-7 WSA User Authentication Dialog Box

Step 6. Depending on the site chosen for your initial connection, you will have to enter a username/password for cut-through proxy authentication (for sites behind ASA2). If you wish to reauthenticate, close and reopen your browser. Using session cookies as the surrogate type means that the credentials used to authenticate initially will be applicable for all HTTP/HTTPS connections launched from the browser. Closing and reopening the browser clears the session cookie.

You may also check the user logs on the WSA to verify your connection history, as shown in [Figure 2a-8](#).

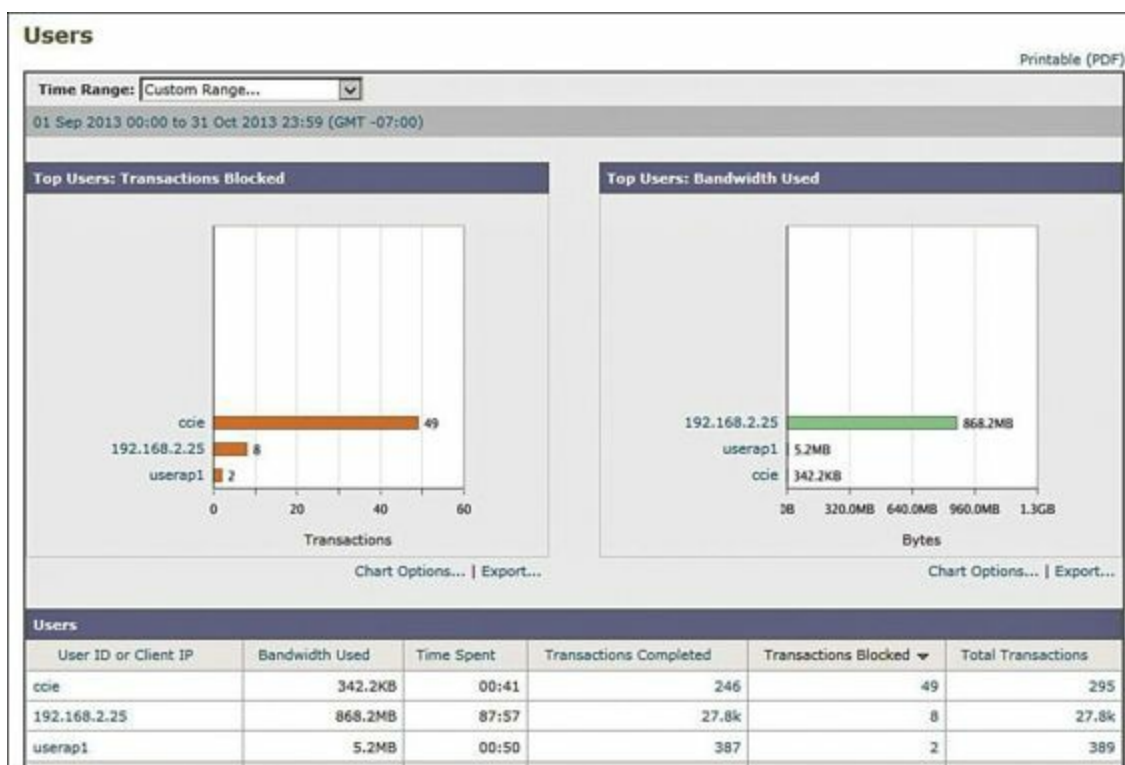


Figure 2a-8 WSA User Transaction History

Solution and Verification for Exercise 2.4: Guest User Support on the Cisco WSA

Skills Tested

- Configuring a guest user identity with no authentication
- Defining and applying guest access policies

Solution and Verification

The configuration of WSA is completed using the GUI. To verify your solution, you will need to follow the steps outlined later, and compare your outputs.

For all verification syntax that follows:

- Required tasks appear in *indigo*

To verify your solution, close the browser on the Test-PC. Reopen the browser and connect to <http://10.50.50.5>. The WSA will prompt for username/password; enter guest. This will fail authentication but grant guest access. You should be able to connect to the SW2 website.

[Click here to view code image](#)

HTTP server history:

```
local-ipaddress:port remote-ipaddress:port in-bytes out-bytes end-time
10.50.50.5:80 192.168.2.50:64008 3547 251686 19:55:45 04/23
10.50.50.5:80 192.168.2.50:9612 4118 270121 19:55:45 04/23
```

Next, connect to any other 10.50.0.0 HTTP server. The connection should be blocked and a notification displayed as shown in [Figure 2a-9](#).



Figure 2a-9 *Browser Blocked Connection Notification*

WSA Configuration

Define a guest identity and an enforceable authentication policy as shown in [Figure 2a-10](#).



Figure 2a-10 *WSA Guest Identity Definition*

Create a custom URL category that is applied to users satisfying the authentication policy criteria defined earlier; that is, 10.50.50.5/32. Also, define a URL category explicitly denying access to all other resources on 10.50.0.0/16 to guests. Ensure that your policies are applied in the correct order, as shown in [Figure 2a-11](#).

Custom URL Categories: Edit Category

Edit Custom URL Category

Category Name:

List Order:

Sites: [Sort URLs](#)
 Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

(e.g. example.com, .example.com, 10.1.1.1, 10.1.1.0/24)

Advanced Regular Expressions:

Enter one regular expression per line.

Figure 2a-11 WSA Guest URL Categories

The access policy for guests will summarize the resource privileges granted to guest users as shown in [Figure 2a-12](#). Because guests do not need to pass authentication, privileges are said to apply to those users failing authentication.

Access Policies

[Add Policy...](#)

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Web Reputation and Anti-Malware Filtering	Delete
1	Guest Users Identity: All, Guest privileges for users failing authentication Protocols: HTTP URL Categories: GuestURL, GuestNoAccess	(global policy)	Block: 1 Monitor: 1	(global policy)	(global policy)	(global policy)	
	Global Policy Identity: All	No blocked items	Block: 1 Monitor: 79	Block: 17 Monitor: 129	No blocked items	Web Reputation: Enabled Anti-Malware Scanning: Enabled	

Figure 2a-12 WSA Guest User Access Policy

Section 3: Secure Access

This section presents some more-complex solutions for secure network access. The legacy remote access VPNs using IKEv1 in Lab 1 have been replaced with FlexVPN using IKEv2. In one exercise, we look at site-to-site remote access using RADIUS tunnel attributes and Cisco Secure ACS to provide the IKEv2 preshared key. Another FlexVPN scenario involves remote access client to server, which is the new version of EZVPN that uses IKEv2 for security association (SA) negotiation and remote attribute distribution (config mode). This section also covers the use of IPv6 with IPsec, IKEv1 using RSA signatures and dynamic routing over VTIs, SSL VPNs using both client and clientless connections terminating on the Cisco ASA, and GETVPN deployed with multicast rekeying.

Solution and Verification for Exercise 3.1: Configure and Troubleshoot IPsec Static VTI with IPv6

Skills Tested

- Configuring static IPsec VTIs for IPv6 traffic
- Configuring Public Key Infrastructure (PKI) trustpoints and enrolling end entities with the Cisco Certificate Authority (CA) Server

- Deploying certificate maps with isakmp profiles
- Verifying IPv6 routing using EIGRPv6
- Troubleshooting IPsec VPNs

Solution and Verification

This exercise has several components:

- **Certificates:** Trustpoints, enrollment, cert maps
- **IPsec static VTIs:** IPv6
- **Routing:** Verifying EIGRPv6
- **Cisco ASA:** Allowing access through ASA2 for traffic sourced from the DMZ interface and destined to the inside interface

The verification of this solution will follow an ideal ordering of the necessary tasks.

As specified in the question notes, Lab 2 [Exercise 1.4](#) must be completed first. Unless the inside and DMZ interfaces of ASA2 are configured for IPv6, the IPsec VPN will not be established.

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**
- Variable syntax appears in **green**

Verify that ASA2 is configured to allow IPv6 traffic between the DMZ and inside interfaces:

[Click here to view code image](#)

```
ASA2# show ipv6 access-list
ipv6 access-list vpn line 1 permit esp 2001:DB9:30::4/64 2001:DB8:40::7/64
ipv6 access-list vpn line 3 permit udp 2001:DB9:30::4/64 2001:DB8:40::7/64 eq
isakmp
```

Ensure that R7 and R4 have a common, accurate time source; for example, add NTP server 10.50.70.6.

Define the PKI trustpoint on R4 and R7. Note that if Lab 2 [Exercise 5.4](#) has been completed, the HTTP port number will be 8080; if not, the default port 80 is used.

[Click here to view code image](#)

```
crypto pki trustpoint ciscoa
enrollment retry count 5
enrollment retry period 3
enrollment url http://10.50.100.1:8080
revocation-check none
```

Generate RSA keys on each router:

[Click here to view code image](#)

```
R7(config)# crypto key gen rsa
Specify a modulus, this lab question uses 1024 bits.
```

Verify whether the key has been created; it will be used during end entity enrollment:

[Click here to view code image](#)

```
R7# show crypto key mypubkey rsa
% Key pair was generated at: 12:17:36 PST Sep 28 2013
Key name: R7.cisco.com
Key type: RSA KEYS
Storage Device: private-config
Usage: General Purpose Key
Key is not exportable.
Key Data:
 30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00D495EA
 395B6FDF 58DEB196 A46E8AC8 1336D428 5D450B4B 53695EC1 43DAF2FA
219689D7
 5AB9245E B08D2958 B9F18189 B92A0FF1 EBD47E7B F5ED8D59 0C193191
5D25FCD2
 DC45F474 675598F4 F24EF34F 68397297 D270BC5F 6C554876 AC7A39F5 6DCD42D6
 F98D59CE CE189BFE 2C027C77 39F7ED96 784779E3 3A7EF457 F3DDB6BF
1F020301 0001
```

Obtain and authenticate the CA certificate, and then enroll the end entities (R4 and R7) with the CA cisco:

[Click here to view code image](#)

```
R4(config)# crypto pki authenticate cisco
Certificate has the following attributes:
  Fingerprint MD5: 1F5A02E4 C2C8230A 56FC15BB CBDFBEF6
  Fingerprint SHA1: 99D5D0AA 928B4DD8 7D9E6D98 B3831F1D 796C6A71
```

```
% Do you accept this certificate? [yes/no]: yes
```

```
R4(config)# crypto pki enroll cisco
```

```
%
```

```
% Start certificate enrollment ..
```

```
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
```

```
For security reasons your password will not be saved in the configuration.
```

```
Please make a note of it.
```

```
Password: cisco
```

```
Re-enter password: cisco
```

```
% The subject name in the certificate will include: R4.cisco.com
```

```
% Include the router serial number in the subject name? [yes/no]: no
```

```
% Include an IP address in the subject name? [no]: no
```

Request certificate from CA? [yes/no]: **yes**

% Certificate request sent to Certificate Authority

% The 'show crypto pki certificate verbose cisco' command will show the fingerprint.

R4(config)#

*Sep 29 01:17:00.529: CRYPTO_PKI: Certificate Request Fingerprint MD5: AC5647CD
4607D9DC 3819945F 12535ACC

*Sep 29 01:17:00.529: CRYPTO_PKI: Certificate Request Fingerprint SHA1: E01B51B5
B5F301AC 64B298FF D022E769 DA27D496

R4(config)#

*Sep 29 01:17:00.611: %PKI-6-CERTRET: Certificate received from Certificate
Authority

Verify receipt of the CA and end entity certificates. Ensure that the certificate validity dates and times are synchronized with the clock time on R4 and R7. If the certificate has not yet become valid due to a time issue, the IKE negotiation will fail; for example, **ntp server 10.50.70.6**.

[Click here to view code image](#)

R4# **show cry pki certificates**

Certificate

Status: Available

Certificate Serial Number (hex): 02

Certificate Usage: General Purpose

Issuer:

cn=cisco.cisco.com L=cisco C=US

Subject:

Name: R4.cisco.com

hostname=R4.cisco.com

Validity Date:

start date: 17:17:00 PST Sep 28 2013

end date: 17:17:00 PST Apr 16 2014

Associated Trustpoints: cisco

Storage: nvram:ciscocacisco#2.cer

CA Certificate

Status: Available

Certificate Serial Number (hex): 01

Certificate Usage: Signature

Issuer:

cn=cisco.cisco.com L=cisco C=US

Subject:

cn=cisco.cisco.com L=cisco C=US

Validity Date:

start date: 13:19:37 PST Aug 17 2013

end date: 13:19:37 PST Aug 17 2014

Associated Trustpoints: ciscoca
Storage: nvram:ciscocacisco#1CA.cer

R7# **show cry pki certificates**

Certificate

Status: Available

Certificate Serial Number (hex): 0A

Certificate Usage: General Purpose

Issuer:

cn=ciscoca.cisco.com L=cisco C=US

Subject:

Name: R7.cisco.com

hostname=R7.cisco.com

Validity Date:

start date: 18:39:45 PST Sep 28 2013

end date: 18:39:45 PST Apr 16 2014

Associated Trustpoints: ciscoca

Storage: nvram:ciscocacisco#A.cer

CA Certificate

Status: Available

Certificate Serial Number (hex): 01

Certificate Usage: Signature

Issuer:

cn=ciscoca.cisco.com L=cisco C=US

Subject:

cn=ciscoca.cisco.com L=cisco C=US

Validity Date:

start date: 13:19:37 PST Aug 17 2013

end date: 13:19:37 PST Aug 17 2014

Associated Trustpoints: ciscoca

Storage: nvram:ciscocacisco#1CA.cer

Complete the configurations on R4 and R7, and verify whether the VPN tunnel has been established. This task requires some troubleshooting. The configuration section of this exercise highlights the missing configuration commands required to successfully bring up the static VTI.

[Click here to view code image](#)

R7# **show crypto session**

Interface: Tunnel2

Profile: ipv6

Session status: UP-ACTIVE

Peer: 2001:DB9:30::4 port 500

IKEv1 SA: local 2001:DB8:40::7/500

remote 2001:DB9:30::4/500 Active

IPSEC FLOW: permit ipv6 ::/0 ::/0

Active SAs: 2, origin: crypto map

R4# **show crypto session**

Interface: Tunnel2

Profile: ipv6

Session status: UP-ACTIVE

Peer: 2001:DB8:40::7 port 500

IKEv1 SA: local 2001:DB9:30::4/500

remote 2001:DB8:40::7/500 Active

IPSEC FLOW: permit ipv6 ::/0 ::/0

Active SAs: 2, origin: crypto map

When the IPsec static VTI is up, check the IPv6 routing table and verify whether the Loopback1 interfaces have been advertised across the tunnel using EIGRPv6:

[Click here to view code image](#)

R7# **show ipv6 route**

IPv6 Routing Table - default - 9 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP

H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea

IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO

ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect

1 - LISP

O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

S ::/0 [1/0]

via 2001:DB8:40::20

C 1011::/64 [0/0]

via Loopback1, directly connected

L 1011::8A43:E1FF:FEB1:B380/128 [0/0]

via Loopback1, receive

C 2001:DB8:40::/64 [0/0]

via GigabitEthernet0/1, directly connected

L 2001:DB8:40::7/128 [0/0]

via GigabitEthernet0/1, receive

C 2001:DBA::/64 [0/0]

via Tunnel2, directly connected

L 2001:DBA::1:1/128 [0/0]

via Tunnel2, receive

EX 2011::/64 [170/27008000]

via FE80::A8BB:CCFF:FE00:7C00, Tunnel2

L FF00::/8 [0/0]

via Null0, receive

R4# **show ipv6 route**

IPv6 Routing Table - default - 9 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
I - LISP
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

```
S ::/0 [1/0]
  via 2001:DB9:30::20
EX 1011::/64 [170/27008000]
  via FE80::8A43:E1FF:FEB1:B380, Tunnel2
C 2001:DB9:30::/64 [0/0]
  via Ethernet0/1, directly connected
L 2001:DB9:30::4/128 [0/0]
  via Ethernet0/1, receive
C 2001:DBA::/64 [0/0]
  via Tunnel2, directly connected
L 2001:DBA::1:2/128 [0/0]
  via Tunnel2, receive
C 2011::/64 [0/0]
  via Loopback1, directly connected
L 2011::A8BB:CCFF:FE00:7C00/128 [0/0]
  via Loopback1, receive
L FF00::/8 [0/0]
  via Null0, receive
```

Connections for IPv6 traffic between R4 (dmz) and R7 (inside) will be installed on ASA2:

[Click here to view code image](#)

```
ASA2# show conn
UDP dmz 2001:db9:30::4:500 inside 2001:db8:40::7:500, idle 0:00:08, bytes 336,
  flags -
ESP dmz 2001:db9:30::4 inside 2001:db8:40::7, idle 0:00:03, bytes 7776
```

Configuration

Syntax highlighted in **cyan** needs to be added or modified.

R7

[Click here to view code image](#)

```
ipv6 unicast-routing
```

```
crypto pki certificate map certmap 1
  issuer-name co cisco.com
  unstructured-subject-name co r4.cisco.com
```

```
crypto pki trustpoint cisco-ca
enrollment retry count 5
enrollment retry period 3
enrollment url http://10.50.100.1:8080
revocation-check none
```

```
crypto isakmp policy 2
group 5
```

```
crypto isakmp identity dn
crypto isakmp profile ipv6
ca trust-point cisco-ca
match certificate certmap
```

```
crypto ipsec transform-set 3des esp-3des esp-md5-hmac
!
```

```
crypto ipsec profile profilev6
set transform-set 3des
set isakmp-profile ipv6
```

```
interface Loopback1
ip address 10.7.7.7 255.255.255.0
ipv6 address 1011::/64 eui-64
```

```
interface Tunnel2
no ip address
ipv6 address 2001:DBA::1:1/64
ipv6 enable
ipv6 eigrp 1
tunnel source GigabitEthernet0/1
tunnel mode ipsec ipv6
tunnel destination 2001:DB9:30::4
tunnel protection ipsec profile profilev6
```

```
interface GigabitEthernet0/1
ip address 10.50.40.7 255.255.255.0
ip flow ingress
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
duplex auto
speed auto
ipv6 address 2001:DB8:40::7/64
ipv6 enable
```

```
ipv6 route ::/0 2001:DB8:40::20
ipv6 router eigrp 1
  distribute-list prefix-list loopback out
  redistribute connected
!
!
!
ipv6 prefix-list loopback seq 5 permit 1011::/64
!
ntp server 10.50.70.6
```

R4

[Click here to view code image](#)

```
ipv6 unicast-routing

crypto pki certificate map certmap 1
  issuer-name co cisco.com
  unstructured-subject-name co r7.cisco.com

crypto isakmp policy 2
  group 5

crypto pki trustpoint ciscoca
  enrollment retry count 5
  enrollment retry period 3
  enrollment url http://10.50.100.1:8080
  revocation-check none

crypto isakmp identity dn
crypto isakmp profile ipv6
  ca trust-point ciscoca
  match certificate certmap

crypto ipsec transform-set 3des esp-3des esp-md5-hmac
!
crypto ipsec profile profilev6
  set transform-set 3des
  set isakmp-profile ipv6

interface Loopback1
  ip address 10.4.4.4 255.255.255.0
  ipv6 address 2011::/64 eui-64

interface Tunnel2
```

```
no ip address
ipv6 address 2001:DBA::1:2/64
ipv6 enable
ipv6 eigrp 1
tunnel source Ethernet0/1
tunnel mode ipsec ipv6
tunnel destination 2001:DB8:40::7
tunnel protection ipsec profile profilev6
```

```
interface Ethernet0/1
ip address 10.50.30.4 255.255.255.0
ipv6 address 2001:DB9:30::4/64
ipv6 enable
```

```
ipv6 route ::/0 2001:DB9:30::20
ipv6 router eigrp 1
  distribute-list prefix-list loopback out
  redistribute connected
!
!
!
ipv6 prefix-list loopback seq 5 permit 2011::/64
!
ntp server 10.50.70.6
```

ASA2

[Click here to view code image](#)

```
ipv6 access-list vpn permit udp 2001:DB9:30::4/64 2001:DB8:40::7/64 eq 500
ipv6 access-list vpn permit esp 2001:DB9:30::4/64 2001:DB8:40::7/64
```

```
access-group vpn in interface dmz
```

Tech Notes

Tip and Tricks

- A redistribute list is required for EIGRPv6 to prevent recursive routing if the tunnel interface address is advertised back into the tunnel. This causes an EIGRPv6 route flap, and the tunnel interface will continuously bounce.
- If you change an interface IPv6 address, be sure to explicitly remove the old IPv6 addresses because IPv6 addresses append on the interface. This can lead to invalid local address errors during IPsec VPN negotiation.
- If invalid local address errors are seen during IPsec negotiation and the addresses are correct, you might need to remove all IPv6 addresses from the interfaces and reapply them.

Static VTIs for IPv6 Using Preshared Keys

If preshared keys are to be used in lieu of certificates, the configuration of this question will change on R4 and R6 as follows:

[Click here to view code image](#)

```
crypto isakmp identity address
```

```
crypto keyring ipv6keys
```

```
pre-shared-key address ipv6 ::/0 key cisco123
```

! preceding line uses a match-all address, a specific IPv6 address per peer can also be used and is preferred when applicable.

```
crypto isakmp profile ipv6
```

```
keyring ipv6keys
```

```
match identity address ipv6 2001:DB9:30::4/64
```

Solution and Verification for Exercise 3.2: Troubleshoot and Configure GETVPN

Skills Tested

- GETVPN configuration using cooperative key servers (COOP KS)
- Key servers behind an ASA firewall
- Multicast rekeying
- Understanding antireplay mechanisms for GETVPN

Solution and Verification

GETVPN enables secure, IPsec protected connectivity between registered group members (GM). After GETVPN is enabled on a GM, it will immediately attempt to register with its configured KS. Registration involves an IKE negotiation (via UDP/848) that results in authentication of the peers (KS and GM) and the establishment of a secure control channel. The key encryption key (KEK), traffic encryption key (TEK), and IPsec policy (including access lists that define traffic which must be secured) is *pulled* from the KS to the authenticated GM. The TEK is used to protect traffic on the IPsec SAs between GMs. The KEK is used to protect rekey and other control messages *pushed* from the KS. These rekey messages can be sent unicast to each GM or multicast to all GMs that have joined the multicast group.

In this exercise, multicast rekeying is required. This involves configuring IP multicast routing using Protocol-Independent Multicast (PIM) on all interfaces that join the GM to the KS. A special consideration in the network topology is that ASA1 in multiple context mode is between the KSs and the GMs. In multiple context mode, IP multicast cannot be forwarded on the ASA. To pass multicast traffic through ASA/c2, GRE tunnels are required between the GMs and KSs.

A loopback interface (10.50.60.6) is used as the local address for the GETVPN crypto map on R6. The crypto map itself is applied on the interface facing the other GM. If the crypto map is applied on the KS facing the interface, R6 will register with the KS; however, traffic defined in the downloaded

ACL will not be encrypted and the IPsec policy is defined on the correct interface. If a local address is not set, R6 will register twice (via both physical interfaces) with the KSs and appear as two GMs. Knowledge of the following components of GETVPN is key to implementing a solution to meet the requirements of this question:

- **Multicast rekeying:** The KS will distribute refreshed keying material using unicast or multicast. In unicast mode, each GM is individually contacted and the key is provided. In multicast mode, the KS just announces the key information to a multicast address. All GMs joined to the multicast group receive the key information. If a GM does not receive the rekey, it will reregister with the KS. The current SA and key will be downloaded as part of the registration. Using multicast rekey is more scalable compared to the unicast method but it needs an IP multicast infrastructure deployed on the core.
- **Cooperative key server:** The key server is an essential component in a GETVPN deployment. If the KS becomes unavailable, the GMs will not be able to register or get new rekeys when the existing IPsec SA expires. Also, in large deployments, one KS might not be sufficient to handle the registration load of all the GMs. A cooperative key server (COOP KS) model solves these problems. Multiple key servers can be deployed to ensure redundancy, high availability, and fast recovery if one key server fails. Cooperative key servers jointly manage the Group Domain of Interpretation (GDOI) registrations for the group, sharing the registration load. The GMs can be configured to register with any one of the key servers. If more than one KS is configured on a GM, it will register with the first KS unless that KS is unreachable. Although all KSs accept registration from GMs, only one KS will be responsible for the rekey operation. This KS is called the primary KS. The primary KS is decided through an election process among all the cooperative KSs. To aid this process, a priority number should be configured on each KS. If KSs have the same priority, the one with highest IP address will be selected.
- **RSA signatures for keying message authentication:** GETVPN uses RSA signatures to authenticate GETVPN keying information, so both R1 and R2 must use the same private/public keys for signing. To accomplish this, export the keys from the first KS and import them in the second.

To generate RSA keys for a single KS, enter the following:

[Click here to view code image](#)

```
crypto key generate rsa modulus 1024 label REKEYRSA
```

To verify whether the keys exist on the router, execute the following command at the enable prompt:

[Click here to view code image](#)

```
show crypto key mypubkey rsa
```

If more than one key server must be configured in coop mode, the RSA key should be made exportable at the time of key generation:

[Click here to view code image](#)

```
crypto key generate rsa modulus 1024 label REKEYRSA  
exportable
```

These keys can then be exported from the initial KS and imported on other KSs.

For example, considering R1 was configured as the first KS, the following commands can be used to export/import RSA keys using IOS CLI from R1 to R2 (encryption method and passphrases are user defined).

To export keys at R1:

[Click here to view code image](#)

```
crypto key export rsa GETVPN_KEYS pem terminal 3des CISCO1234
```

To import keys at R2:

[Click here to view code image](#)

```
crypto key import rsa GETVPN_KEYS pem exportable terminal CISCO1234
```

Antireplay is an important feature in a data encryption protocol such as IPsec (RFC 2401). Antireplay prevents a third party from eavesdropping on an IPsec conversation, stealing packets, and injecting those packets into a session at a later time. GETVPN for groups with more than two GMs, particularly in a multisender scenario, must use the time-based Synchronous Antireplay (SAR) mechanism, not counter-based antireplay. The KS is responsible for sending the pseudotime value and window size to a GM during registration. The KS then uses the TEK payload pushed to GMs for refreshing the SAR attributes: pseudotime and window size, to ensure all members have a synchronized clock source.

When a key server serves multiple GDOI groups, key server authorization is required to prevent a GM in one group from requesting keys and policies from another group. GETVPN group member authorization can be done using preshared keys or PKI. It is a best practice to turn on GETVPN authorization and is required in this question.

For all verification syntax that follows:

- Required output appears in **red**
- Nonzero/nonnull syntax appears in **violet**
- Variable syntax appears in **green**

Verify Network Connectivity

One of the first considerations for this exercise is identifying the devices and traffic flows involved with the GETVPN solution. Examination of the topology in [Diagram 2](#) and [Diagram 8](#) in [Part I](#) shows two Cisco ASAs in the path of the GETVPN traffic flows. The necessary traffic must be permitted to pass through ASA1/c2 and ASA2.

Protocol	ASA1/c2	ASA2
UDP/848 (gdoi)	Permitted from R7, R6 to R1, R2	
ESP		Permitted between 10.7.0.0/16 as per IPsec ACL
GRE	Used to tunnel multicast traffic through the context c2 from R6, R7 to R1, R2	Used to tunnel multicast traffic through the context ASA1/c2 from R7 to R1, R2

Table 2a-3 Traffic Permitted Through ASAs

Using a redundant COOP KS model, GRE and GDOI traffic should be permitted to both KSs to ensure a seamless failover.

Support for the necessary protocols is verified as follows (only currently active connections will display):

[Click here to view code image](#)

```
ASA1/c2# show conn
```

```
16 in use, 19 most used
```

```
GRE outside 10.50.40.7:0 inside 10.50.100.2:0, idle 0:00:01, bytes 42384, flags E
GRE outside 10.50.80.6:0 inside 10.50.100.2:0, idle 0:00:03, bytes 42806, flags E
GRE outside 10.50.80.6:0 inside 10.50.100.1:0, idle 0:00:01, bytes 50952, flags E
GRE outside 10.50.40.7:0 inside 10.50.100.1:0, idle 0:00:18, bytes 56334, flags E
UDP outside 10.50.70.6:848 inside 10.50.100.1:848, idle 0:00:07, bytes 2136, flags -
UDP outside 10.50.40.7:848 inside 10.50.100.1:848, idle 0:00:07, bytes 2136, flags -
```

```
ASA2(config)# show conn
```

```
26 in use, 41 most used
```

```
GRE outside 10.50.100.2:0 inside 10.50.40.7:0, idle 0:00:12, bytes 75060, flags E
GRE outside 10.50.100.1:0 inside 10.50.40.7:0, idle 0:00:12, bytes 65186, flags E
ESP outside 10.7.6.6 inside 10.7.7.7, idle 0:00:04, bytes 700
```

Configure and Verify the COOP Key Servers

Verify whether RSA keys have been created on one of the key servers in the pair and successfully imported to the second KS. The public key values displayed must be identical between R1 and R2:

[Click here to view code image](#)

```
R1# show crypto key mypubkey rsa
```

```
% Key pair was generated at: 11:36:29 PST Jul 29 2013
```

```
Key name: getvpn
```

```
Key type: RSA KEYS
```

```
Storage Device: private-config
```

```
Usage: General Purpose Key
```

```
Key is exportable.
```

```
Key Data:
```

```
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00A57770
FFC46D29 D6D0FE28 7259CBD1 83F5B482 DBF15346 58703712 1406DA48 7D9D086D
DBAC7CEC 96CD0949 9922CE00 3B1A0A02 FB162E85 0D30EC6C 7E429954 51075365
4789E22E 53A18AE7 7A3D97DF 81DDAFB7 3C80762D 562FF7C9 A5E62918 863197C2
8782477C 32B10548 E7609536 EA37BE76 87AE3056 B10E0784 53695702 BB020301 0001
```

```
R2# show crypto key mypubkey rsa
```

```
% Key pair was generated at: 11:49:34 PST Jul 29 2013
```

```
Key name: getvpn
```

```
Key type: RSA KEYS
```

Storage Device: private-config

Usage: General Purpose Key

Key is exportable.

Key Data:

```
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00A57770
FFC46D29 D6D0FE28 7259CBD1 83F5B482 DBF15346 58703712 1406DA48 7D9D086D
DBAC7CEC 96CD0949 9922CE00 3B1A0A02 FB162E85 0D30EC6C 7E429954 51075365
4789E22E 53A18AE7 7A3D97DF 81DDAFB7 3C80762D 562FF7C9 A5E62918 863197C2
8782477C 32B10548 E7609536 EA37BE76 87AE3056 B10E0784 53695702 BB020301 0001
```

When GMs register to a KS, the COOP KS model will ensure GM information is shared between all KSs in the COOP grouping. R1 (secondary KS) and R2 (primary KS) should show two GMs.

[Click here to view code image](#)

```
R2# show crypto gdoi ks
```

```
Total group members registered to this box: 2
```

```
Key Server Information For Group getvpn:
```

```
Group Name      : getvpn
```

```
Group Identity  : 1
```

```
Group Members   : 2
```

```
IPSec SA Direction : Both
```

```
ACL Configured:
  access-list VPNA
```

```
Redundancy      : Configured
```

```
Local Address   : 10.50.100.2
```

```
Local Priority   : 175
```

```
Local KS Status : Alive
```

```
Local KS Role   : Primary
```

```
Local KS Version : 1.0.2
```

```
R1# show crypto gdoi ks
```

```
Total group members registered to this box: 2
```

```
Key Server Information For Group getvpn:
```

```
Group Name      : getvpn
```

```
Group Identity  : 1
```

```
Group Members   : 2
```

```
IPSec SA Direction : Both
```

```
ACL Configured:
  access-list VPNA
```

```
Redundancy      : Configured
```

```
Local Address   : 10.50.100.1
```

```
Local Priority   : 100
```

```
Local KS Status : Alive
```

```
Local KS Role   : Secondary
```

Local KS Version : 1.0.2

Verify that R2 is also updated with the registered GM information. Note that as the primary KS, R2 will be responsible for sending rekeying information to the registered GMs. Multicast rekeying configuration will enable R2 to send rekeys that are simultaneously received by all members of the multicast group. In the case of unicast rekeying, R2 would have to send rekey messages to all registered GMs using their unicast IP addresses. In the event of a failure of R1, R2 would need to assume responsibility for all group members, which is why it is important to ensure there is communication between all KSs in a COOP deployment.

[Click here to view code image](#)

```
R2# show cry gdoi ks members
```

Group Member Information :

Number of rekeys sent for group getvpn : **4868**

Group Member ID : 10.50.40.7 GM Version: 1.0.2

Group ID : 1

Group Name : getvpn

Key Server ID : 10.50.100.1

Group Member ID : 10.50.60.6 GM Version: 1.0.2

Group ID : 1

Group Name : getvpn

Key Server ID : 10.50.100.1

```
R1# show crypto gdoi ks members
```

Group Member Information :

Number of rekeys sent for group getvpn : **0** <- will be zero if there has been
No failovers in the COOP group.

Group Member ID : 10.50.40.7 GM Version: 1.0.2

Group ID : 1

Group Name : getvpn

Key Server ID : 10.50.100.1

Group Member ID : 10.50.60.6 GM Version: 1.0.2

Group ID : 1

Group Name : getvpn

Key Server ID : 10.50.100.1

The following outputs from **show crypto gdoi** will summarize the complete GETVPN policies

configured on the key servers R1 and R2:

[Click here to view code image](#)

```
R1# show crypto gdoi
GROUP INFORMATION
```

```
Group Name          : getvpn (Multicast)
Group Identity      : 1
Group Members       : 2
IPSec SA Direction  : Both
Redundancy          : Configured
  Local Address     : 10.50.100.1
  Local Priority     : 100
  Local KS Status   : Alive
  Local KS Role     : Secondary
  Local KS Version  : 1.0.2
Group Rekey Lifetime : 900 secs
Group Rekey
  Remaining Lifetime : 512 secs
Rekey Retransmit Period : 10 secs
Rekey Retransmit Attempts: 3
Group Retransmit
  Remaining Lifetime : 0 secs

IPSec SA Number     : 1
IPSec SA Rekey Lifetime: 600 secs
Profile Name        : profile1
Replay method       : Count Based
Replay Window Size  : 64
SA Rekey
  Remaining Lifetime : 214 secs
ACL Configured      : access-list VPNA
```

```
Group Server list   : Local
```

```
R2# show crypto gdoi
GROUP INFORMATION
```

```
Group Name          : getvpn (Multicast)
Group Identity      : 1
Group Members       : 2
IPSec SA Direction  : Both
Redundancy          : Configured
  Local Address     : 10.50.100.2
  Local Priority     : 175
  Local KS Status   : Alive
```

Local KS Role : Primary
Local KS Version : 1.0.2
Group Rekey Lifetime : 900 secs
Group Rekey
Remaining Lifetime : 438 secs
Rekey Retransmit Period : 10 secs
Rekey Retransmit Attempts: 3
Group Retransmit
Remaining Lifetime : 0 secs

IPSec SA Number : 1
IPSec SA Rekey Lifetime: 600 secs
Profile Name : profile1
Replay method : Count Based
Replay Window Size : 64
SA Rekey
Remaining Lifetime : 139 secs
ACL Configured : access-list VPNA

Group Server list : Local

When verifying crypto sessions, which will display all active IKEv1 SAs, there must be an IKEv1 SA between R1 and R2 (unless one of these KSs is down). This protected communications channel is used to exchange GETVPN control information, such as GM registration and withdrawal.

The number of IKEv1 SAs active for a given GM will vary depending on the state of the GM and the role of the KS. The ordering of KSs in the GETVPN group list on each GM will determine the KS that accepts the GM registration. The port number for IKE for GETVPN is UDP/848 (for the GDOI protocol).

[Click here to view code image](#)

```
R1# show crypto session
```

```
Interface: Ethernet0/0
```

```
Session status: UP-IDLE
```

```
Peer: 10.50.100.2 port 848
```

```
IKEv1 SA: local 10.50.100.1/848 remote 10.50.100.2/848 Active
```

```
Interface: Ethernet0/0
```

```
Session status: UP-IDLE
```

```
Peer: 10.50.60.6 port 848
```

```
IKEv1 SA: local 10.50.100.1/848 remote 10.50.60.6/848 Active
```

```
Interface: Ethernet0/0
```

```
Session status: UP-IDLE
```

```
Peer: 10.50.40.7 port 848
```

IKEv1 SA: local 10.50.100.1/848 remote 10.50.40.7/848 Active

As the primary KS, R2 is responsible for rekeying all GMs. In this case, multicast rekeying requires only one IKEv1 SA that will service all GMs that are also members of the multicast group. The PIM protocol was preconfigured to facilitate multicast routing and group joining in the network topology.

[Click here to view code image](#)

```
R2# show crypto session
```

```
Crypto session current status
```

```
Interface: (unknown)
```

```
Session status: UP-IDLE
```

```
Peer: 239.192.1.190 port 848
```

```
IKEv1 SA: local 10.50.100.2/848 remote 239.192.1.190/848 Active
```

```
Interface: Ethernet0/0.1
```

```
Session status: UP-IDLE
```

```
Peer: 10.50.100.1 port 848
```

```
IKEv1 SA: local 10.50.100.2/848 remote 10.50.100.1/848 Active
```

Configure and Verify the Group Members

When verifying the configuration of the GMs R6 and R7, one of the main policy considerations is what traffic needs to be protected between all members of the GETVPN group. The KS will push an ACL that will be installed on the GM. Note that any locally defined ACLs that overlap with any KS pushed ACLs will take precedence.

The default IPsec antireplay mechanism is window-based and works well for single sender GETVPN groups with a low number of members. This exercise required a method be implemented that allows support for a group with multiple senders. It is recommended that time-based antireplay be implemented in this type of scenario, or in fact any group with more than two GMs. Antireplay is enforced on the group IPsec SA and is defined on the KS under the IPsec SA policy. The default window size is 100, which is also the max value and should be tuned in a real-world deployment. The following syslog messages indicate that an adjustment to the window size might be required:

[Click here to view code image](#)

```
%GDOI-3-PSEUDO_TIME_LARGE
```

```
%GDOI-3-PSEUDO_TIME_TOO_OLD
```

```
R7# show crypto gdoi ipsec sa
```

```
SA created for group getvpn:
```

```
GigabitEthernet0/1:
```

```
protocol = ip
```

```
local ident = 10.7.0.0/16, port = 0
```

```
remote ident = 10.7.0.0/16, port = 0
```

```
direction: Both, replay(method/window): Time/5 sec
```

The state of the group antireplay mechanism can be checked as follows:

[Click here to view code image](#)

```
R7# show crypto gdoi group getvpn gm replay
```

```
Anti-replay Information For Group getvpn:
```

```
Timebased Replay:
```

```
Replay Value      : 1301905.18 secs
Input Packets     : 0      Output Packets      : 0
Input Error Packets : 0      Output Error Packets : 0
Time Sync Error   : 0      Max time delta    : 0.00 secs
```

The configuration and state of the GMs is displayed via **show crypto gdoi**. This command output includes both existing GETVPN policy on the GM (that is, server list) as well as configuration parameters pushed by the Ks. In this output, R7 and R6 have registered with R1 but receive rekeying messages from R2 (as the primary KS).

[Click here to view code image](#)

```
R7# show crypto gdoi
```

```
GROUP INFORMATION
```

```
Group Name      : getvpn
```

```
Group Identity  : 1
```

```
Rekeys received : 3
```

```
IPSec SA Direction : Both
```

```
Group Server list : 10.50.100.1
                  10.50.100.2
```

```
Group member    : 10.50.40.7    vrf: None
```

```
Version         : 1.0.2
```

```
Registration status : Registered
```

```
Registered with   : 10.50.100.1
```

```
Re-registers in   : 208 sec
```

```
Succeeded registration: 29
```

```
Attempted registration: 49
```

```
Last rekey from   : 10.50.100.2
```

```
Last rekey seq num : 0
```

```
Multicast rekey rcvd : 19
```

```
allowable rekey cipher: any
```

```
allowable rekey hash : any
```

```
allowable transformtag: any ESP
```

```
Rekeys cumulative
```

```
Total received   : 3
```

```
After latest register : 1
```

Rekey Rcvd(hh:mm:ss) : 00:05:35

ACL Downloaded From KS 10.50.100.2:

access-list permit ip 10.7.0.0 0.0.255.255 10.7.0.0 0.0.255.255

KEK POLICY:

Rekey Transport Type : Multicast
Lifetime (secs) : 564
Encrypt Algorithm : 3DES
Key Size : 192
Sig Hash Algorithm : HMAC_AUTH_SHA
Sig Key Length (bits) : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:

GigabitEthernet0/1:

IPsec SA:

spi: 0xDB7B4CCA(3682290890)
transform: esp-256-aes esp-sha-hmac
sa timing:remaining key lifetime (sec): (452)
Anti-Replay(Time Based) : -1 sec interval

IPsec SA:

spi: 0xA220289A(2720016538)
transform: esp-256-aes esp-sha-hmac
sa timing:remaining key lifetime (sec): (530)
Anti-Replay(Time Based) : 5 sec interval

R6# show crypto gdoi

GROUP INFORMATION

Group Name : getvpn
Group Identity : 1
Rekeys received : 4
IPSec SA Direction : Both

Group Server list : 10.50.100.1
10.50.100.2

Group member : 10.50.60.6 vrf: None
Version : 1.0.2
Registration status : Registered
Registered with : 10.50.100.1
Re-registers in : 178 sec
Succeeded registration: 18
Attempted registration: 18
Last rekey from : 10.50.100.2

Last rekey seq num : 1
Multicast rekey rcvd : 27
allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP

Rekeys cumulative

Total received : 4
After latest register : 2
Rekey Rcvd(hh:mm:ss) : 00:02:31

ACL Downloaded From KS 10.50.100.2:

access-list permit ip 10.7.0.0 0.0.255.255 10.7.0.0 0.0.255.255

KEK POLICY:

Rekey Transport Type : Multicast
Lifetime (secs) : 267
Encrypt Algorithm : 3DES
Key Size : 192
Sig Hash Algorithm : HMAC_AUTH_SHA
Sig Key Length (bits) : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:

Ethernet0/1:

IPsec SA:

spi: 0xDB7B4CCA(3682290890)
transform: esp-256-aes esp-sha-hmac
sa timing:remaining key lifetime (sec): (452)
Anti-Replay(Time Based) : -1 sec interval

IPsec SA:

spi: 0xA220289A(2720016538)
transform: esp-256-aes esp-sha-hmac
sa timing:remaining key lifetime (sec): (530)
Anti-Replay(Time Based) : 5 sec interval

Each GM will use an IKEv1 SA for registration and another IKEv1 SA for multicast rekeying. The IPsec SA will be maintained between GMs only. The IKE SA used for registration might periodically expire depending on SA lifetimes in a real-world scenario:

[Click here to view code image](#)

```
R7# show crypto session
```

```
Crypto session current status
```

```
Interface: GigabitEthernet0/1
```

```
Session status: UP-ACTIVE
```

Peer: 0.0.0.0 port 848

IKEv1 SA: local 10.50.40.7/848 remote 10.50.100.1/848 Active

IKEv1 SA: local 239.192.1.190/0 remote 10.50.100.2/848 Active

IPSEC FLOW: permit ip 10.7.0.0/255.255.0.0 10.7.0.0/255.255.0.0

Active SAs: 2, origin: crypto map

R6# **show crypto session**

Crypto session current status

Interface: Ethernet0/1

Session status: UP-ACTIVE

Peer: 0.0.0.0 port 848

IKEv1 SA: local 239.192.1.190/0 remote 10.50.100.1/848 Active

IKEv1 SA: local 10.50.60.6/848 remote 10.50.100.1/848 Active

IPSEC FLOW: permit ip 10.7.0.0/255.255.0.0 10.7.0.0/255.255.0.0

Active SAs: 2, origin: crypto map

To verify whether the IPsec connectivity between the GMs has been established, send a ping using the traffic selectors defined in the IPsec ACL pushed from the KS.

[Click here to view code image](#)

```
R6# ping 10.7.7.7 so lo1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.7.7.7, timeout is 2 seconds:
```

```
Packet sent with a source address of 10.7.6.6
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms
```

Configure and Verify DPD and Authorization

There are two additional requirements to verify. Dead Peer Detection (DPD) is implemented between R1 and R2 to help facilitate failover. Because traffic between KSs is not consistent, on-demand DPD will not be optimal for ascertaining a failure, and periodic keepalives should be configured. Negotiation of DPD between peers during IKEv1 SA establishment is indicated as follows:

[Click here to view code image](#)

```
R2# show crypto session detail
```

```
Code: C - IKE Configuration mode, D - Dead Peer Detection
```

```
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
```

```
X - IKE Extended Authentication, F - IKE Fragmentation
```

```
Crypto session current status
```

```
Interface: Ethernet0/0.1
```

```
Session status: UP-IDLE
```

```
Peer: 10.50.100.1 port 848 fvrf: (none) ivrf: (none)
```

```
Phase1_id: 10.50.100.1
```

```
Desc: (none)
```

```
IKEv1 SA: local 10.50.100.2/848 remote 10.50.100.1/848 Active
```

A GM authorization list is required on both R1 and R2 and should contain an IP address for each GM permitted into the GETVPN group:

[Click here to view code image](#)

```
R1# show run | include authorization address
authorization address ipv4 10
```

```
R1# show access-list 10
Standard IP access list 10
 10 permit 10.50.60.6
 20 permit 10.50.40.7
```

Configuration

Syntax highlighted in cyan needs to be added or modified.

R1—COOP KS

[Click here to view code image](#)

```
ip multicast-routing
```

```
crypto isakmp policy 10
 encr aes 192
 authentication pre-share
 group 5
```

```
crypto isakmp key cisco address 10.50.0.0
crypto isakmp keepalive 60 periodic
```

```
crypto ipsec profile profile1
 set security-association lifetime seconds 600
 set transform-set aes256
```

```
crypto gdoi group getvpn
 identity number 1
 server local
 rekey address ipv4 getvpn-rekey
 rekey lifetime seconds 900
 rekey retransmit 10 number 3
rekey authentication mypubkey rsa getvpn
authorization address ipv4 10
sa ipsec 1
 profile profile1
 match address ipv4 VPNA
 replay time
```

```
address ipv4 10.50.100.1
redundancy
local priority 100
peer address ipv4 10.50.100.2
```

```
interface Tunnel6
ip address 10.50.101.1 255.255.255.0
ip pim sparse-dense-mode
tunnel source Ethernet0/0
tunnel destination 10.50.60.6
```

```
!
interface Tunnel7
ip address 10.50.102.1 255.255.255.0
ip pim sparse-dense-mode
tunnel source Ethernet0/0
tunnel destination 10.50.40.7
```

```
interface Ethernet0/0
ip address 10.50.100.1 255.255.255.0
ip pim sparse-mode
```

```
ip pim accept-rp auto-rp
ip pim send-rp-announce Ethernet0/0 scope 10 group-list 1
ip pim send-rp-discovery Ethernet0/0 scope 10
```

```
ip access-list extended VPNA
permit ip 10.7.0.0 0.0.255.255 10.7.0.0 0.0.255.255
ip access-list extended getvpn-rekey
permit ip any host 239.192.1.190
```

```
!
access-list 1 permit 239.192.1.190
access-list 10 permit 10.50.60.6
access-list 10 permit 10.50.40.7
```

R2 COOP KS—Primary

[Click here to view code image](#)

```
crypto isakmp policy 10
encr aes 192
authentication pre-share
group 5
```

```
crypto isakmp key cisco address 10.50.0.0
```

```
crypto isakmp keepalive 60 periodic
```

```
crypto ipsec profile profile1
set security-association lifetime seconds 600
set transform-set aes256
!
crypto gdoi group getvpn
identity number 1
server local
rekey address ipv4 getvpn-rekey
rekey lifetime seconds 900
rekey retransmit 10 number 3
rekey authentication mypubkey rsa getvpn
authorization address ipv4 10
sa ipsec 1
profile profile1
match address ipv4 VPNA
replay time
address ipv4 10.50.100.2
redundancy
local priority 175
peer address ipv4 10.50.100.1
```

```
interface Tunnel8
ip address 10.50.201.1 255.255.255.0
ip pim sparse-dense-mode
tunnel source Ethernet0/0.1
tunnel destination 10.50.60.6
```

```
!
interface Tunnel9
ip address 10.50.202.1 255.255.255.0
ip pim sparse-dense-mode
tunnel source Ethernet0/0.1
tunnel destination 10.50.40.7
```

```
interface Ethernet0/0.1
encapsulation dot1Q 100
ip address 10.50.100.2 255.255.255.0
ip pim sparse-mode
```

```
ip pim rp-address 10.50.100.2
ip pim send-rp-announce Ethernet0/0.1 scope 10 group-list 1
ip pim send-rp-discovery Ethernet0/0.1 scope 10
ip route 0.0.0.0 0.0.0.0 10.50.100.20
!
ip access-list extended VPNA
```

```
permit ip 10.7.0.0 0.0.255.255 10.7.0.0 0.0.255.255
ip access-list extended getvpn-rekey
permit ip any host 239.192.1.190
!
access-list 1 permit 239.192.1.190
access-list 10 permit 10.50.60.6
access-list 10 permit 10.50.40.7
```

R7 GM

[Click here to view code image](#)

```
ip multicast-routing

crypto keyring getvpn
pre-shared-key address 10.50.100.1 key cisco
pre-shared-key address 10.50.100.2 key cisco
```

```
crypto gdoi group getvpn
identity number 1
server address ipv4 10.50.100.1
server address ipv4 10.50.100.2
```

```
crypto map getvpn 1 gdoi
set group getvpn
```

```
interface Loopback1
ip address 10.7.7.7 255.255.255.0
ipv6 address 1011::/64 eui-64
!
interface Tunnel7
ip address 10.50.102.7 255.255.255.0
ip pim sparse-dense-mode
tunnel source GigabitEthernet0/1
tunnel destination 10.50.100.1
!
interface Tunnel9
ip address 10.50.202.7 255.255.255.0
ip pim sparse-dense-mode
tunnel source GigabitEthernet0/1
tunnel destination 10.50.100.2
```

```
interface GigabitEthernet0/1
ip address 10.50.40.7 255.255.255.0
ip pim sparse-mode
ip flow ingress
ip ospf authentication message-digest
```

```
ip ospf message-digest-key 1 md5 cisco
duplex auto
speed auto
ipv6 address 2001:DB8:40::7/64
ipv6 enable
crypto map getvpn
```

```
ip pim rp-address 10.50.100.1
ip mroute 10.50.100.1 255.255.255.255 Tunnel7
ip mroute 10.50.100.2 255.255.255.255 Tunnel9
```

R6 GM

[Click here to view code image](#)

```
ip multicast-routing
```

```
crypto keyring getvpn
pre-shared-key address 10.50.100.1 key cisco
pre-shared-key address 10.50.100.2 key cisco
```

```
crypto gdoi group getvpn
identity number 1
server address ipv4 10.50.100.1
server address ipv4 10.50.100.2
```

```
crypto map getvpn local-address Loopback6
crypto map getvpn 1 gdoi
set group getvpn
```

```
interface Loopback1
ip address 10.7.6.6 255.255.255.0
ipv6 address 2010::/64 eui-64
!
interface Loopback6
ip address 10.50.60.6 255.255.255.0
ip pim sparse-mode
```

```
interface Tunnel6
ip address 10.50.101.6 255.255.255.0
ip pim sparse-dense-mode
tunnel source Loopback6
tunnel destination 10.50.100.1
```

```
!
interface Tunnel8
ip address 10.50.201.6 255.255.255.0
ip pim sparse-dense-mode
```

```
tunnel source Loopback6
tunnel destination 10.50.100.2
!
interface Ethernet0/0
ip address 10.50.80.6 255.255.255.0
ip pim sparse-mode
!
interface Ethernet0/1
ip address 10.50.70.6 255.255.255.0
ip pim sparse-mode
crypto map getvpn

ip pim rp-address 10.50.100.1
ip mroute 10.50.100.1 255.255.255.255 Tunnel6
ip mroute 10.50.100.2 255.255.255.255 Tunnel8
```

ASA1/c2

[Click here to view code image](#)

```
access-list 101 extended permit udp any any eq 848
access-group 101 in interface dmz
```

ASA1/c2 & ASA2

[Click here to view code image](#)

```
access-list 101 permit GRE any any
```

Tech Notes

Key Server Design Considerations for IKE

The KS should be configured for AES encryption using at least 128-bit keys to provide high security with computational efficiency.

The lifetime of IKE sessions on the KS is recommended to be the default lifetime of 24 hours.

The KSs need an active IKE session to transmit COOP messages. This is a persistent database synchronization process, so the IKE session is always required.

At press time, GETVPN supports only the use of IKEv1.

Example:

```
crypto isakmp policy 10
encryption aes
hash sha256
lifetime 86400
```

Verify:

```
show crypto isakmp policy
```


IKE periodic dead peer detection (DPD) should be configured on all KSs so the primary COOP server can keep track of the state of the secondary KSs.

Example:

[Click here to view code image](#)

```
crypto isakmp keepalive 15 periodic
```

Verify:

```
show crypto session detail
```

Key Server Design Considerations for IPsec

AES encryption is recommended for the IPsec traffic encryption.

Example:

[Click here to view code image](#)

```
crypto ipsec transform-set AES_SHA esp-aes esp-sha-hmac
!
crypto ipsec profile gdoi1
 set security-association lifetime seconds 7200
 set transform-set AES_SHA
!
crypto gdoi group dgvpn1
 identity number 61440
 server local
 rekey lifetime seconds 86400
 rekey retransmit 40 number 3
 rekey authentication mypubkey rsa getkey
 rekey transport unicast
 sa ipsec 1
 profile gdoi1
 match address ipv4 172.16.4.2
```

Verify:

```
show crypto gdoi ks policy
```

Key Server Design Considerations for Traffic Encryption Key Lifetime

It is recommended that the traffic encryption key (TEK) lifetime should be not less than the default 3600 seconds in real deployments to avoid creating a large number of key rollovers that must be synchronized among all GMs. If the KS has insufficient time to complete key distribution during a rekey cycle, before the next TEK rekey, the system operates in an unstable state. The longer lifetime improves network stability and avoids rekey overlap. A TEK lifetime of 2 hours (7200 seconds) is a recommended value.

To change the lifetime, use the following configuration:

[Click here to view code image](#)

```
crypto ipsec profile gdoi1
set security-association lifetime seconds 7200
```

Verify

```
show crypto gdoi ks policy
```

Note

The actual time at which the KS sends rekeys depends on the number of GMs, retransmission values, and a maximum of 10% or 90-second head start value. The following formula can calculate the actual rekey time:

$$\text{Lifetime} - [\max(10\% \text{ of lifetime or } 90 \text{ sec}) + (\text{required retransmission time}) + (5 \times \text{number of GMs}/50)]$$

For example, for 1000 GMs, a configured TEK lifetime of 7200 seconds and two retransmissions (60 seconds apart), the KS sends rekeys every 6260 seconds:

$$7200 - [720 (10\% \text{ lifetime}) + 120 (60 \times 2 \text{ retransmissions}) + 100 (\text{additional time to cover } 1000 \text{ GMs})]$$

The example provided leads to a TEK lifetime overlap of 940 seconds. The new TEK is prepositioned 940 seconds prior to the expiration of the previous TEK. The GMs will start encrypting with the new TEK when 30 seconds remain in the previous TEK's lifetime.

Key Server Design Considerations for ACLs in a Traffic Encryption Policy

The permit entries in the ACL for encryption policy include the subnets/protocols/applications that must be encrypted. The maximum number of lines in a traffic ACL is 100. Note that each permit statement in the KS ACL results in an SA on the GM, so the number of permit entries should be limited to minimize the SA database (SADB) on the GM. As mentioned, it is possible to add a single **permit ip any any** entry in the ACL to encrypt all traffic. Explicit deny entries should be configured in the ACL to exclude control traffic (for example, routing protocols) from encryption. The following protocols, which are commonly denied in encryption policy, are provided for reference:

- **deny tcp any eq bgp any:** When GMs use BGP for Provider Edge-Customer Edge (PE-CE) adjacency
- **deny ospf any any:** When GMs use OSPF for PE-CE adjacency
- **deny eigrp any any:** When GMs use EIGRP for PE-CE adjacency

For example:

[Click here to view code image](#)

```
deny pim any 224.0.0.0 0.0.0.255
deny udp any any eq ntp
deny udp any any eq dns
deny tcp any eq 443 any
deny udp any eq isakmp any eq isakmp
deny udp any any eq 848
permit ip any any
```

Note

A recommended best practice is to ensure that any bootstrap management and control protocols are denied encryption on the local GM during early deployment phases. A global deny policy can be constructed for all GMs and deployed from the KS to ensure that all management and control bootstrap protocols are never encrypted.

Key Server Design Considerations for Key Encryption Key Lifetime

The key encryption key lifetime should be left at the default of 86,400 seconds. Because the KEK is used to encrypt the control plane messages between the KS and GM, changing the KEK value frequently subjects the GM to possible rekey misses and subsequently requires the GM to reregister more frequently than is necessary. It is recommended that the KEK lifetime should always be at least double the TEK lifetime.

To change the value:

[Click here to view code image](#)

```
crypto gdoi group dgvpn1
identity number 61440
server local
rekey lifetime seconds 24400
```

Verify:

```
show crypto gdoi ks policy
```

Rekey Retransmit Interval

Rekey retransmits should be configured using one of the following schemes:

- Two retransmissions at 60-second intervals
- Three retransmissions at 40-second intervals

Configure:

[Click here to view code image](#)

```
crypto gdoi group dgvpn1
identity number 61440
server local
rekey retransmit 40 number 3
```

Verify:

```
show crypto gdoi ks rekey
```

Time-Based Antireplay

Time-Based Antireplay (TBAR) should be configured on all platforms for multicast rekeying. Counter-based antireplay is an option only for unicast rekeying with fewer than three GMs.

GETVPN uses a synchronous antireplay (SAR) mechanism to provide antireplay protection for

multisender traffic. SAR is independent of real-world Network Time Protocol (NTP) clock or sequential-counter mechanisms (which guarantee packets are received and processed in order). A SAR clock advances regularly. The time tracked by this clock is called *pseudotime*, and it is maintained on the key server and sent periodically to the group members within a rekey message as a timestamp field called `pseudoTimeStamp`. Group members must be resynchronized to the pseudotime of the key server periodically. The pseudotime of the key server starts ticking when the first group member registers. Initially, the key server sends the current pseudotime value of the key server and window size to group members during the registration process. New attributes, such as time-based replay-enabled information, window size, and the pseudotime of the key server, is sent under the SA payload (TEK).

By default, counter-based antireplay is configured:

```
crypto gdoi group dgvpn1
identity number 61440
server local
<..>
sa ipsec 1
<..>
replay time window-size 5
```

Verify:

```
show crypto gdoi
```

Key Server Design Considerations for Authentication Policies for GM Registration

GMs can authenticate to the KS at registration time using Pre-Shared Key (PSK) or PKI. PSKs are easy to deploy but must be managed proactively. It is recommended to deploy a peer-based PSK instead of defining a default key (the key defined with an address of 0.0.0.0) for all the devices in the network.

Note

A PSK can be updated on a KS-GM peer basis without affecting the crypto data plane or control plane because rekeys are secured using the KEK. It is important to ensure that a GM can reregister to each ordered set of KSs using the newly created key. For added security, GETVPN also supports GM authorization that is based on the ISAKMP identity sent by the GM.

Implementing Rekeying Mechanisms

The following configuration examples can be used as a reference for rekeying mechanisms not covered in this question.

Unicast Rekeying

[Click here to view code image](#)

```
crypto gdoi group getvpn
identity number 1
```

```
server local
rekey lifetime seconds 900
rekey retransmit 10 number 2
rekey authentication mypubkey rsa getvpn
rekey transport unicast
sa ipsec 1
profile profile1
match address ipv4 VPNA
replay counter window-size 64
address ipv4 10.50.100.2
redundancy
local priority 175
peer address ipv4 10.50.100.1
```

Implementing Multicast Rekeying with No ASA Considerations

The following configuration is an example of multicast rekeying for GETVPN when there is no ASA in the path between KSs and GMs. This example can be used only if multicast routing is enabled on the rest of the network and uses Source Specific Multicast (SSM) for multicast and the address 239.192.1.190. The configuration might need to be changed according to any existing multicast mechanism deployed in the network.

[Click here to view code image](#)

! Key Server Configuration

! Enable multi-cast routing

```
ip multi-cast routing
```

! Enable SSM mode

```
ip pim ssm range 1
```

!

! ACL list used in SSM range command

```
access-list 1 permit 239.192.1.190 0.0.0.0
```

!

```
interface GigabitEthernet0/1
```

! Interface connecting to the WAN network

```
ip address 10.0.0.2 255.255.255.0
```

```
ip pim sparse-mode
```

```
ip igmp version 3
```

!

```
crypto gdoi group GDOI-GROUP1
```

```
server local
```

! Default rekey method is multicast

```
no rekey transport unicast
```

! Multicast group for re-keying. This is specified as a ACL

```
rekey address ipv4 getvpn-rekey-multicast-group
```

```
rekey retransmit 10 number 3
```

```

!
! Add these ACEs in getvpn-acl
ip access-list extended getvpn-acl
deny ip any 224.0.0.0 0.255.255.255
deny pim any host 224.0.0.13
!
ip access-list extended getvpn-rekey-multicast-group
permit ip any host 239.192.1.190

```

```

! Group Member Configuration
ip multicast-routing
! Enable SSM
ip igmp ssm-map enable
ip pim ssm range 1
! ACL used in ssm range command
access-list 1 permit 239.192.1.190 0.0.0.0
interface FastEthernet4
! Interface where crypto map is applied
ip pim sparse-mode
ip igmp version 3
! Join for each KS serving the group
ip igmp join-group 239.192.1.190 source <IP-Addr-of-KS-1>
ip igmp join-group 239.192.1.190 source <IP-Addr-of-KS-2>

```

Implementing Multicast Rekeying Through the ASA in Routed Mode

Unlike the ASA in multiple-context mode, which requires GRE tunnels to pass multicast traffic through the ASA, routed mode will support IP multicast natively. However, it is not the same level of support as Cisco IOS.

[Click here to view code image](#)

```

multicast-routing
!
pim rp-address <KS-IP>
!
interface e0/1
name inside
pim
!
interface e0/0
name outside
pim

ACL_IN
none
ACL_OUT
access-list OUTSIDE_IN permit udp h <GM-IP> eq 848 h <KS-IP> eq 848

```

Solution and Verification for Exercise 3.3: SSL Client and Clientless VPNs

Skills Tested

- Configuration of client-based SSL VPN support on the Cisco ASA with basic identity firewalling using the local database
- Configuration of clientless SSL VPN support on the Cisco ASA

Solution and Verification

Configuring SSL VPN support on the Cisco ASA uses the same constructs as IPsec VPN support; group policies, tunnel group policies, and usernames. The Cisco ASA will allow a mix of simultaneous VPN connection types selected based on the tunnel group name, which maps to a group-policy definition, which in turn identifies the protocol required for the connection. All connection types can use specific tunnel group and policy attributes, whereas some attributes are specific to the connection protocol. This exercise focuses on defining the configuration required for connection establishment and applies some basic attributes. The administrator is encouraged to do further reading on the plethora of attributes and policy parameters, keeping in mind these can vary according to the version of Cisco ASA software that is being used.

For this exercise, two tunnel protocol types are required:

- **ssl-client:** Client type—AnyConnect Secure Mobility Client using SSL
- **ssl-clientless:** Client type—HTTPS/SSL from browser

The key components to verify are as follows:

- The generation and use of the self-issued certificate on ASA2
- Whether the SSL VPN Service homepage group drop-down shows two groups: SSL and anySSL
- Whether user login credentials are authenticated against the local database
- The integration of user-based identity firewalling with the AnyConnect client SSL sessions
- Whether group policies are locally defined

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**

1. Generating and installing the self-signed certificate on ASA2

Verify whether the ASA has a domain name defined and a reliable clock source/time is set to avoid issues with certificate validity:

[Click here to view code image](#)

```
domain-name cisco.com
```

```
ASA2# show ntp status
```

```
Clock is synchronized, stratum 3, reference is 192.168.2.5
```

Generate an SSL key pair using a modulus of 1024 bits. The public key value will be used by

clients to verify the authenticity of the server and will be propagated to the clients via the server-side certificate.

[Click here to view code image](#)

```
crypto key generate rsa label sslvpnkeypair modulus 1024
```

```
ASA2(config)# show cry key mypubkey rsa
Key pair was generated at: 05:15:40 UTC Aug 21 2013
Key name: sslvpnkeypair
Usage: General Purpose Key
Modulus Size (bits): 1024
Key Data:
```

```
30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 008f1541
4434bd1e f55ee0b3 91968c50 f2686d8d 3d70d8e9 1f46b0d1 fee04f35 54843579
0715f4e5 5403566e b4621a4b 632f7bc7 01883e4a b34e1b96 57152e34 3e2cfc60
f8e4435d 2985c034 3e2cc276 f5de5fe7 b0cba2e4 39cf90c9 e2c6b9ee 921e628f
bbf20662 1fe3073c 020cc34d b590115e 047ce393 2edc6e68 3d00a3f7 f9020301
0001
```

Configure your SSL trustpoint, ensuring a self-signed certificate will be generated. The FQDN used is sslvpn.cisco.com. Trustpoints enable an ASA to support different identities for different roles (SSL VPN versus IKE/IPsec, for example).

[Click here to view code image](#)

```
crypto ca trustpoint localtrust
enrollment self
fqdn sslvpn.cisco.com
subject-name CN=sslvpn.cisco.com
keypair sslvpnkeypair
```

Create the certificate and install it for use:

[Click here to view code image](#)

```
ASA2(config-ca-trustpoint)# crypto ca enroll localtrust noconfirm
```

```
ASA2# show crypto ca certificate
Certificate
Status: Available
Certificate Serial Number: 8b7ef551
Certificate Usage: General Purpose
Public Key Type: RSA (1024 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name:
  hostname=sslvpn.cisco.com
  cn=sslvpn.cisco.com
Subject Name:
```


hostname=sslvpn.cisco.com

cn=sslvpn.cisco.com

Validity Date:

start date: 05:18:57 UTC Aug 21 2013

end date: 05:18:57 UTC Aug 19 2023

Associated Trustpoints: localtrust

Apply the new certificate to the interface adjacent to the SSL clients:

[Click here to view code image](#)

```
ssl trust-point localtrust outside
```

The client's browsers should reference the FQDN defined in the certificate. Ensure that this name is added to the DNS server on 192.168.2.25 and that the certificate is added to the trusted root store to avoid being prompted each time to accept the certificate, as shown in [Figure 2a-13](#).



Figure 2a-13 *SSL Root Certificate Verification Using Microsoft Windows*

2. Verify whether the SSL VPN service home page displays both SSL groups, as shown in [Figure 2a-14](#).

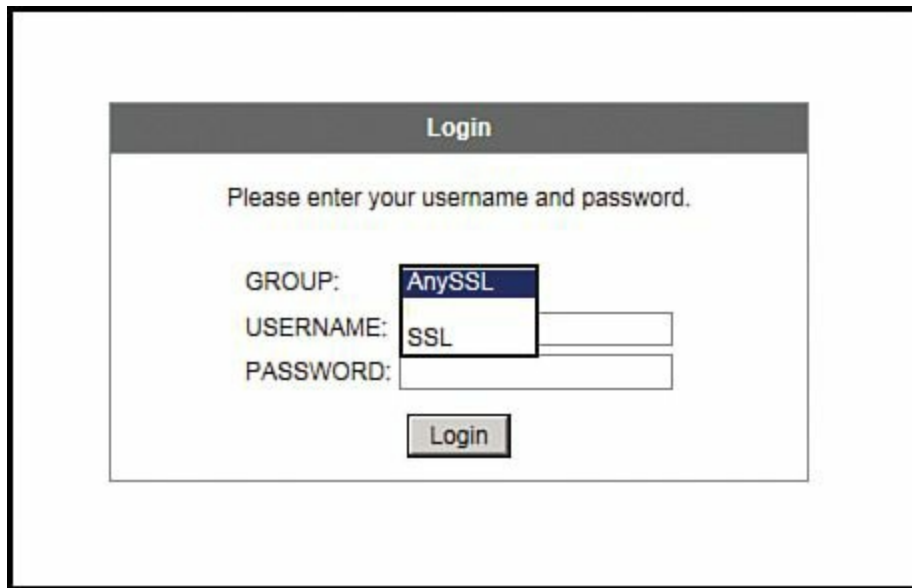


Figure 2a-14 *SSL VPN Group Drop-Down Menu*

3. Verify that group selection and entry of usernames and passwords provide the correct access for the clientless group.

Group: SSL

Username: user1

Result: Redirect to the R3 home page

The login prompt to access the HTTP server of R3 should appear, as shown in [Figure 2a-15](#).

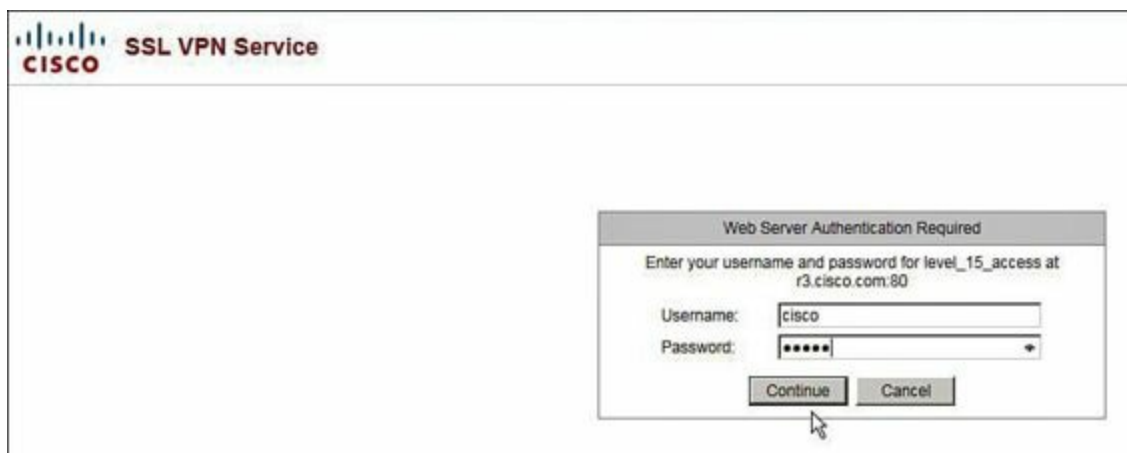


Figure 2a-15 *SSL VPN R3 Home Page Login Dialog Box*

On ASA2, this SSL session will appear as Clientless:

[Click here to view code image](#)

```
ASA2# show vpn-sessiondb
```

```
-----  
VPN Session Summary  
-----
```

```
Active : Cumulative : Peak Concur : Inactive
```

```
-----  
AnyConnect Client      : 0 : 1 : 1 : 0
```

```
SSL/TLS/DTLS      : 0 : 1 : 1 : 0
Clientless VPN    : 2 : 2 : 2
Browser           : 2 : 2 : 2
```

```
-----
Total Active and Inactive : 2      Total Cumulative : 3
Device Total VPN Capacity : 750
Device Load               : 0%
```

```
-----
Tunnels Summary
```

```
-----
Active : Cumulative : Peak Concurrent
-----
Clientless      : 2 : 3 : 2
SSL-Tunnel     : 0 : 1 : 1
DTLS-Tunnel    : 0 : 1 : 1
-----
Totals         : 2 : 5
```

To verify the correct group was selected for this connection, use the following output. Note that this session should clear after 1 minute of inactivity, although the inactivity timer in the output is not incrementing.

[Click here to view code image](#)

```
ASA2# sho vpn-sessiondb webvpn
```

```
Session Type: WebVPN
```

```
Username   : user1          Index      : 17
Public IP  : 192.168.2.25
Protocol   : Clientless
License    : AnyConnect Premium
Encryption : RC4           Hashing    : SHA1
Bytes Tx   : 2401236        Bytes Rx   : 233208
Group Policy : SSL         Tunnel Group : SSL
Login Time : 16:29:31 UTC Fri Oct 4 2013
Duration   : 0h:04m:43s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A         VLAN       : none
```

```
ASA2# show runn | begin group-policy SSL attributes
group-policy SSL attributes
vpn-idle-timeout 1
```

vpn-tunnel-protocol ssl-clientless
webvpn
homepage value http://r3.cisco.com

4. Verify that group selection and entry of usernames and passwords provide the correct access for the anyconnect group

Group: anySSL

Username: user2

Result: Use identity firewall to permit access to 10.50.40.0/24 only from 192.168.100.0/24. This subnet contains addresses assigned via IP address pool anyssl-clients.

[Click here to view code image](#)

```
ASA2# show vpn-sessiondb anyconnect
```

Session Type: AnyConnect

```
Username      : user2          Index      : 19
Assigned IP   : 192.168.100.100 Public IP   : 192.168.2.25
Protocol      : Clientless SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : RC4 RC4 AES128 Hashing      : SHA1 SHA1 SHA1
Bytes Tx      : 58736          Bytes Rx    : 38825
Group Policy  : anySSL        Tunnel Group : anySSL
Login Time    : 19:20:04 UTC Fri Oct 4 2013
Duration      : 0h:06m:34s
Inactivity    : 0h:00m:00s
NAC Result    : Unknown
VLAN Mapping  : N/A          VLAN        : none
```

When user2 has been authenticated, the identity FW access list (vpn-filter) should be enforced by associating this vpn-filter with user2 as follows:

```
username user2 attributes
vpn-filter value user2
```

Any activity sourced from an address pool assigned IP destined to 10.50.40.0/24 will pass through the SSL VPN tunnel.

The **vpn-filter** command requires that return flows be explicitly defined; otherwise, traffic will not be sent back through the SSL tunnel to the client due to implicit deny conditions. Note that the LOCAL domain will ensure that user credentials are referenced locally on the ASA:

[Click here to view code image](#)

```
ASA2# show access-list
access-list user2 line 1 extended permit ip user LOCAL\user2 192.168.100.0
255.255.255.0 10.50.40.0 255.255.255.0 (hitcnt=6) 0x91a6b0d4
access-list user2 line 2 extended permit ip any 10.50.40.0 255.255.255.0
```

(hitcnt=1) 0x4bb1a95b

Routes to the SSL client hosts are automatically created based on the assigned IP address:

[Click here to view code image](#)

```
ASA2# show route
S 192.168.100.100 255.255.255.255 [1/0] via 10.50.50.5, outside
```

Note

AnyConnect assigns the first address in a subnet mapping to an address pool to the default gateway. In this case, 192.168.100.1/24 is automatically assumed to be the default gateway for the SSL client on the Test-PC. To ensure there will be actual connectivity for this assignment, VLAN192 was created on SW1 using 192.168.100.1/24. A static route should be added to ASA/c1 and R6 to advertise this new subnet. R6 will propagate the route into the OSPF AS:

[Click here to view code image](#)

```
ASA1/c1# show route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 10.50.80.6 to network 0.0.0.0

```
C 10.50.80.0 255.255.255.0 is directly connected, outside
C 192.168.2.0 255.255.255.0 is directly connected, inside
S 192.168.100.0 255.255.255.0 [1/0] via 192.168.2.5, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 10.50.80.6, outside
```

Configuration

[Click here to view code image](#)

```
access-list user2 extended permit ip user LOCAL\user2 any 10.50.40.0 255.255.255.0
access-list user2 extended permit ip any 10.50.0.0 255.255.0.0
ip local pool anyssl-clients 192.168.100.100-192.168.100.200
user-identity default-domain LOCAL
crypto ca trustpoint localtrust
  enrollment self
  fqdn sslvpn.cisco.com
  subject-name CN=sslvpn.cisco.com
  keypair sslvpnkeypair
  crl configure
crypto ca certificate chain localtrust
  certificate 8b7ef551
    308201ef 30820158 a0030201 0202048b 7ef55130 0d06092a 864886f7 0d010105...
ssl trust-point localtrust outside
webvpn
  enable outside
  anyconnect image disk0:/anyconnect-win-3.0.11042-k9.pkg 1
  anyconnect enable
  tunnel-group-list enable

group-policy SSL internal
group-policy SSL attributes
  vpn-idle-timeout 1
  webvpn
  homepage value http://r3.cisco.com
  vpn-tunnel-protocol ssl-clientless
group-policy anySSL internal
group-policy anySSL attributes
  dns-server value 192.168.2.25
  vpn-tunnel-protocol ssl-client
  default-domain value cisco.com
  address-pools value anyssl-clients

username user1 password mbO2jYs13AXIIAGa encrypted
username user2 password mbO2jYs13AXIIAGa encrypted
username user2 attributes
  vpn-filter value user2
  service-type remote-access

tunnel-group anySSL type remote-access
tunnel-group anySSL general-attributes
  default-group-policy anySSL
```

```
tunnel-group anySSL webvpn-attributes
group-alias AnySSL enable
tunnel-group SSL type remote-access
tunnel-group SSL general-attributes
default-group-policy SSL
tunnel-group SSL webvpn-attributes
group-alias SSL enable
```

Tech Notes

Importing Third-Party Trusted CA Certificates

This exercise covered the use of a self-signed certificate, but in reality, certificates authenticated and issued by trusted certificate authority servers will be used. The following is an example of using the VeriSign certificate service with the Cisco ASA using a manual enrollment method. This procedure can be followed for other certificate services when using the ASA CLI. The Cisco ASA will support multiple CA servers and identities through the use of unique trustpoints. This example uses a manual method because not all CA services support the Cisco Simple Certificate Enrollment Protocol (SCEP). Additionally, trusted CA servers that support thousands of end entity credentials are governed by very strict security policies that often mandate these servers not be accessible by the outside world.

1. Create the key pair to be used for the specific role and trustpoint on the ASA, and generate the PKCS #10 end entity certificate request to be sent (generally via email) to the CA server administrator:

[Click here to view code image](#)

```
ciscoasa# conf t
```

```
ciscoasa(config)# crypto key generate rsa label my.verisign.key
modulus 1024
```

! Generates 1024 bit RSA key pair. "label" defines
! the name of the Key Pair.

INFO: The name for the keys will be: my.verisign.key
Keypair generation process begin. Please wait...

```
ciscoasa(config)# crypto ca trustpoint my.verisign.trustpoint
ciscoasa(config-ca-trustpoint)# subject-name
CN=webvpn.cisco.com,OU=TSWEB,
O=Cisco Systems,C=US,St=North Carolina,L=Raleigh
```

```
ciscoasa(config-ca-trustpoint)# keypair my.verisign.key
ciscoasa(config-ca-trustpoint)# fqdn webvpn.cisco.com
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)# exit
```

```
ciscoasa(config)# crypto ca enroll my.verisign.trustpoint
```

```
% Start certificate enrollment ..
```

```
% The subject name in the certificate will be: CN=webvpn.cisco.com,OU=TSWEB,  
O=Cisco Systems,C=US,St=North Carolina,L=Raleigh
```

```
% The fully-qualified domain name in the certificate will be:  
webvpn.cisco.com
```

```
% Include the device serial number in the subject name? [yes/no]: no
```

```
Display Certificate Request to terminal? [yes/no]: yes
```

```
! Displays the PKCS#10 enrollment request to the terminal.  
! You will need to copy this from the terminal to a text  
! file or web text field to submit to the 3rd party CA.
```

Certificate Request follows:

```
MIICHjCCAYcCAQAwgaAxEDAObgNVBAcTB1JhbGVpZ2gxZmFzAVBgNVBAGTDk5vcnRo  
IENhem9saW5hMQswCQYDVQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczE  
MAwGA1UECxmFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNvbTEhM  
CSqGSIb3DQEJAhYSY2lzY29hc2EuY2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUA  
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB9M4yTx5b  
Fm886s8F73WsfQPynBdfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt3oMXSNPO  
m1dZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX0luBMh7oKargwIDAQAB  
oD0wOwYJKoZIhvcNAQkOMs4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBywFIISY  
Y29hc2EuY2lzY28uY29tMA0GCSqGSIb3DQEBBAUAA4GBABrxpY0q7SeOHZf3yEJq  
po6wG+oZpsvpYI/HemKUlaRc783w4BMO5lulIEhHgRqAxrTbQn0B7JPIbkc2ykkm  
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5QIKx2Y/vrqs+Hg5SLHpvhj/Uo13yWCe  
0Bzg59cYXq/vkoqZV/tBuACr
```

```
---End - This line not part of the certificate request---
```

2. Request and verify the CA server's base 64-encoded certificate. This certificate can be cut and pasted using the ASA CLI. Note that a write memory is required to save this certificate for later use.

[Click here to view code image](#)

```
ciscoasa(config)# crypto ca authenticate my.verisign.trustpoint
```

Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----

```
MIIEwDCCBCmgAwIBAgIQY7G1zcWfeIAdoGNs+XVGezANBgekqhkig9w0BAQUFADCB
jDELMakGA1UEBhMCVVMxZjZAVBgNVBAoTDlZlcm1TaWduLCBjb250IENBMB4X
EydGb3IgVGZvdCBQdXJwb3NlcyBPbm5LiAgTm8gYXNzdXJhbmNlcy4xMjAwBgNV
BAMTKVZlcm1TaWduLFRyaWVsIFNlY3VyZSBTZXJ2ZXIgc3B290IENBMB4X
DTA1MDIwOTAwMDAwMfoXDTE1MDIwODIzNTk1OVowgcsxCzAJBgNVBAYTAiVTMRcw
FQYDVQKKEw5WZXJpU2lnbiwgSW5jLjEwMC4GA1UECxmMnRm9yIFRlc3QgUHVycG9z
ZXMgT25seS4gIE5vIGFzc3VyYW5jZXMumUIwQAYDVQQLEzluZXJtceyBvZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMpMDUxLTAr
BgNVBAMTJFZlcm1TaWduLFRyaWVsIFNlY3VyZSBTZXJ2ZXIgc3B290IENBMB4X
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAuwElv6IJ/
DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE61BBD6Zqk
d85lPl/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n451P4qoyqS
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1D/OCCmZO
5RmNqLLKSvWYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4tlqj97ydk5iDoxKfV6sb
tnp3TIY6S07bTb9gxJcK4pGbcf8DOPvOfGRu1wPpUUC8v+WKC20+sK6QMECAwEA
AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBAbgphkgB
hvhFAQcVMdIwMAYIKwYBBQUHAQEwJGh0dHBzOi8vd3d3LnZlcm1zaWduLmNvbS9j
cHMvdGVzdGNhLzAObGgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQDAgEGMB0C
A1UdDgQWBBRmlo6B4DFZ3Sp/q0bFNglGcCeHWjCBsgYDVR0jBIGqMIGnoYGSPlGP
MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4xMDAuBgNV
BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuLk9ubHkuLk9ubHkuLk9ubHkuLk9ubHku
A1UEAxMpmVyaVNpZ24gVHJpYWwU2VjdXJlIFNlcnZlciBUZXN0IFJvb3QgQ0GC
ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/SjzRvY2l
Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDDIwSRmiH3BW/SU6EEzD9oi
Ai9TXvRIcD5q0mB+nyK9fB2aBzOiaiHSiIWzAJeQjuqA+Q93jNew+peuj4AhdvGN
n/KK/+1Yv61w3+7g6ukFMARVBNg=
```

-----END CERTIFICATE-----

quit

After manually pasting the certificate into CLI, verify the certificate fingerprint display with the fingerprint, which should be supplied by the CA authority via an out-of-band mechanism.

[Click here to view code image](#)

INFO: Certificate has the following attributes:

Fingerprint: 8de989db 7fcc5e3b fdde2c42 0813ef43

Do you accept this certificate? [yes/no]: **yes**

Trustpoint 'my.verisign.trustpoint' is a subordinate CA and
holds a non self-signed certificate.

Trustpoint CA certificate accepted.

% Certificate successfully imported

ciscoasa(config)#

```
ciscoasa(config-ca-trustpoint)# exit
```

3. After the end entity certificate for the Cisco ASA has been received, it must be imported and saved. This is done from the ASA CLI as follows.

[Click here to view code image](#)

```
ciscoasa(config)# crypto ca import my.verisign.trustpoint certificate
```

```
! Initiates prompt to paste the base64 identity  
! certificate provided by the 3rd party vendor.
```

```
% The fully-qualified domain name in the certificate will be: webvpn.cisco.com
```

```
Enter the base 64 encoded certificate.  
End with the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIFZjCCBE6gAwIBAgIQMs/oXuu9K14eMGSf0mYjftANBgkqhkiG9w0BAQUFADCB  
yzELMAkGA1UEBhMCVVMxZzAVBgNVBAAoTDIzcm1TaWduLCBJbmMuMTAwLgYDVQQQL  
EydGbz3IgVGvzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xQjBAbG9u  
BAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3Bz  
L3Rlc3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwU2VjdXJlIFNl  
cnZlciBUZXN0IENBMB4XDTA3MDcyNjAwMDAwMFoXDTA3MDgwOTIzNTk1OVowgbox  
CzAJBgNVBAYTAiVTRcwFQYDVQQIEw5Ob3J0aCBDYXJvbGluYXN0aWZlcm10aW50  
UmFsZWlnaDEWMBQGA1UEChQNNjY2Z8gU3lzdGVtczEOMAwGA1UECxQVFVFNXRUIx  
OjA4BgNVBAsUMVRlcm1zIG9mIHVzZSBhdCB3d3d3cudmVyaXNpZ24uY29tL2Nwcy90  
ZXN0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXN0Y29tL2Nwcy90ZXN0Y2EgKGMp  
KoZlhvcNAQEBAQADgY0AMIGJAoGBAL56EvorHHIsIB/VRKaRlJeJKCrQ/9kER2JQ  
9UOkUP3mVPZJtYN63ZxDwACeyNb+liIdKUegJWHI0Mz3GHqcgEkKW1EcrO+6aY1R  
IaUE8/LiAZbA70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJzA1hJTxSIEgryosBMMazg  
5IcLhgSpAgMBAAGjggHXMIIB0zAJBgNVHRMEAjAAMAsGA1UdDwQEAwIFoDBDBgNV  
HR8EPDA6MDIga0hjJodHRwOi8vU1ZSU2VjdXJlLWVyaXNpZ24uY29tL2Nwcy90  
U1ZSVHJpYWwU2VjdXJlLWVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMpMDUxHDAa  
BgEFBQcCARYjaHR0cHM6Ly93d3d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMp  
VR0IBBYwFAYIKwYBBQUHAWEGCCsGAQUFBwMCMB8GA1UdIwQYMBaAFGYyjoHgMV  
Kn+rRsU2AgZwJ4daMHgGCCsGAQUFBwEBBGwwajAkBggrBgEFBQcwAYYYaHR0cDov  
L29jc3AudmVyaXNpZ24uY29tMEIGCCsGAQUFBzAChjZodHRwOi8vU1ZSU2VjdXJl  
LWFpYS52ZXJpc2lnbi5jb20vU1ZSVHJpYWwU2VjdXJlLWVyaXNpZ24uY29tL2Nwcy90  
AqWEYjBgoV6gXDBaMFgwVhYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGgQUS2u5KJYG  
DLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29tL3ZzbG9n  
bzEuZ2lmMA0GCSqGSIB3DQEBAQUAA4IBAQAAnym4GVThPIyL/9ylDBd8N7/yW3Ov3
```

```
blirHfHJyfPJ1znZQXyXdObpZkuA6Jyu03V2CYNnDomn4xRXQTUDD8q86ZiKyMij
XM2VCmcHSajmMMRyjpydxfk6CIdDMtMGotCavRHD9Tl2tvwgrBock/v/54o02lkB
SmLzVV7crlYJEuhgqu3Pz7qNRd8N0Un6c9sbwQ1BuM99QxzIzdAo89FSewy8MAIY
rtab5F+oiTc5xGy8w7NARAFNgFXihqnLgWTtA35/oWuy86bje1IWbeyqj8ePM9Td
0LdAw6kUU1PNimPttMDhcF7cuvntROksOgQPBPx5FJSqMiUZGrvju5O
-----END CERTIFICATE-----
```

quit

INFO: Certificate successfully imported
ciscoasa(config)#

ciscoasa(config)# **show crypto ca certificates**

! Display the certificates installed on the ASA.

Certificate

Status: Available

Certificate Serial Number: 32cfe85eebbd2b5e1e30649fd266237d

Certificate Usage: General Purpose

Public Key Type: RSA (1024 bits)

Issuer Name:

cn=VeriSign Trial Secure Server Test CA

ou=Terms of use at <https://www.verisign.com/cps/testca> ©)05

ou=For Test Purposes Only. No assurances.

o=VeriSign\, Inc.

c=US

Subject Name:

cn=webvpn.cisco.com

ou=Terms of use at www.verisign.com/cps/testca ©)05

ou=TSWEB

o=Cisco Systems

l=Raleigh

st=North Carolina

c=US

OCSP AIA:

URL: <http://ocsp.verisign.com>

CRL Distribution Points:

[1] <http://SVRSecure-crl.verisign.com/SVRTrial2005.crl>

Validity Date:

start date: 00:00:00 UTC Jul 19 2007

end date: 23:59:59 UTC Aug 2 2007

Associated Trustpoints: my.verisign.trustpoint

CA Certificate

Status: Available

Certificate Serial Number: 63b1a5cdc59f78801da0636cf975467b

Certificate Usage: General Purpose

Public Key Type: RSA (2048 bits)

Issuer Name:

cn=VeriSign Trial Secure Server Test Root CA

ou=For Test Purposes Only. No assurances.

o=VeriSign\, Inc.

c=US

Subject Name:

cn=VeriSign Trial Secure Server Test CA

ou=Terms of use at <https://www.verisign.com/cps/testca> ©)05

ou=For Test Purposes Only. No assurances.

o=VeriSign\, Inc.

c=US

Validity Date:

start date: 00:00:00 UTC Feb 9 2005

end date: 23:59:59 UTC Feb 8 2015

Associated Trustpoints: my.verisign.trustpoint

Default Group Policy and Attribute Inheritance

The ASA is configured with a default group policy. You can modify this default group policy, but you cannot delete it. The default group policy, named DfltGrpPolicy, always exists on the ASA but does not take effect unless the ASA is configured to use it. When you configure other named group policies, any attribute not explicitly specified takes its value from the default group policy. To view the default group policy, enter the following command:

[Click here to view code image](#)

```
hostname# show run all group-policy DfltGrpPolicy
```

Solution and Verification for Exercise 3.4: Configure and Troubleshoot FlexVPN Site-to-Site Using RADIUS Tunnel Attributes

Skills Tested

- Configuring IKEv2 on a Cisco IOS Router
- Understanding the concepts of FlexVPN in a dynamic site-to-site model using dynamic routing
- Implementing AAA integration for IKEv2 using RADIUS to the CiscoSecure ACS authentication server

Solution and Verification

FlexVPN is an umbrella term used to describe VPN solutions that use IKEv2 for tunnel negotiation and control and IPsec-protected virtual interfaces for data transport.

IKEv2 is the IETF standards-based successor to IKEv1. It was originally defined in RFC 4306, which has most recently been replaced by RFC 5996. The reader should be familiar with the implementation of both versions of IKE and the key differences from a protocol perspective. [Table 2a-4](#) summarizes the major changes.

	IKEv1	IKEv2
Auth messages	6 max with IKE main mode MM1/MM2 (policy negotiation) MM3/MM4 (DH exchange) MM5/MM6 (peer authentication)	Open ended IKE_SA_INIT (policy negotiation, DH exchange) IKE_AUTH (peer authentication and first child (IPsec/data) SA) CREATE_CHILD_SA (one for each additional IPsec SA based on selectors)
First IPsec SA	9 messages minimum required	~ 4–6 messages minimum required
Authentication	pubkey-sig, pubkey-encr, PSK	Pubkey-sig, PSK, EAP
Anti-DOS	Not integrated with the protocol	IKEv2 anti-clogging cookie
IKE rekey	Requires reauthentication (expensive)	No reauthentication
Notifies	Unreliable, vendor-specific retransmits and actions	Acknowledged

Table 2a-4 *Differences Between IKE Versions*

To complete this solution, the IKEv2 policy, profiles, and other constructs such as the name-mangler must be completed using the partial configurations defined on R7 and R6 as well as the outputs provided in the question itself. The IKEv2 implementation in Cisco IOS provides support for IKEv2 smart defaults. In this exercise, user-defined policies overrule these default parameters. The IKEv2 name-mangler is a function that takes the value of the IKE ID type passed by the remote peer to create a “username” that will index the AAA database for authorization requests. This exercise uses the FQDN value sent by R7; however, any portion of the IKE ID, based on any ID type, can be referenced when using this command. RADIUS AAA authorization for service “network” will use the IKEv2 name-mangler created username (R7.cisco.com) and the default password cisco. All Cisco IOS authorization requests use service=outbound send password cisco.

RIPv2 is being used for dynamic routing across the FlexVPN and will act as the tunnel initiation mechanism.

The configuration section that follows highlights the commands required to complete the configuration. When a virtual-template interface is used on R6, it implies that R6 will not initiate the FlexVPN.

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**

Verify whether R6 (via a virtual-access interface) and R7 (via interface Tunnel1) should be reporting ACTIVE SAs:

[Click here to view code image](#)

```
R7# show crypto session
```

```
Crypto session current status
```

```
Interface: Tunnel1
```

```
Session status: UP-ACTIVE
```

```
Peer: 10.50.70.6 port 500
```

```
IKEv2 SA: local 10.50.40.7/500 remote 10.50.70.6/500 Active
```

```
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
```

```
Active SAs: 2, origin: crypto map
```

```
R6# show crypto session
```

```
Crypto session current status
```

```
Interface: Virtual-Access1
```

```
Session status: UP-ACTIVE
```

```
Peer: 10.50.40.7 port 500
```

```
IKEv2 SA: local 10.50.70.6/500 remote 10.50.40.7/500 Active
```

```
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
```

```
Active SAs: 2, origin: crypto map
```

The **show crypto ikev2 session detailed** command displays the IKEv2 and IPsec (child) SA policies negotiated between R6 and R7. This verifies whether the user-defined policy and profile configuration was correctly completed:

[Click here to view code image](#)

```
R6# show crypto ikev2 session detailed
```

```
IPv4 Crypto IKEv2 Session
```

```
Session-id:18, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

Tunnel-id	Local	Remote	fvr/ivrf	Status
1	10.50.70.6/500	10.50.40.7/500	none/none	READY

```
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:5, Auth sign: PSK, Auth  
verify: PSK  
Life/Active Time: 86400/1014 sec  
CE id: 1008, Session-id: 18  
Status Description: Negotiation done  
Local spi: D60B62C207327A3D Remote spi: 609E382CB11281D3  
Local id: r6.cisco.com  
Remote id: r7.cisco.com  
Local req msg id: 0 Remote req msg id: 2  
Local next msg id: 0 Remote next msg id: 2  
Local req queued: 0 Remote req queued: 2  
Local window: 5 Remote window: 5
```

DPD configured for 0 seconds, retry 0

NAT-T is not detected

Cisco Trust Security SGT is disabled

Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535

remote selector 0.0.0.0/0 - 255.255.255.255/65535

ESP spi in/out: 0x88B600C5/0xDE40CB3B

AH spi in/out: 0x0/0x0

CPI in/out: 0x0/0x0

Encr: AES-CBC, keysize: 128, esp_hmac: SHA96

ah_hmac: None, comp: IPCOMP_NONE, mode tunnel

The predefined RIP-2 configuration should be correctly propagating routing information between R6 and R7:

[Click here to view code image](#)

```
R7# show ip route
```

```
R 172.17.60.0/24 [120/1] via 172.16.70.6, 00:00:07, Tunnel1
```

```
R6# show ip route
```

```
R 172.17.70.0/24 [120/1] via 172.16.70.7, 00:00:21, Virtual-Access1
```

Verify whether AAA was correctly referenced and configured with respect to the CiscoSecure ACS server by checking the RADIUS authentication logs on 192.168.2.18, as shown in [Figure 2a-16](#).

AAA Protocol > RADIUS Authentication Detail	
ACS session ID :	acs/171239151/1
Date :	October 27, 2013
Generated on October 27, 2013 10:35:54 AM PDT	
Authentication Summary	
Logged At:	October 27, 2013 10:34:45.070 AM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	r7.cisco.com
MAC/IP Address:	10.50.40.7
Network Device:	R6 : 10.50.80.6 :
Access Service:	Default Network Access
Identity Store:	Internal Users
Authorization Profiles:	IKEv2
CTS Security Group:	
Authentication Method:	PAP_ASCII
Authentication Result	
User-Name=r7.cisco.com	
Class=CACS:acs/171239151/1	
Tunnel-Type=(tag=1) ESP	
Tunnel-Medium-Type=(tag=1) IPv4	
cisco-av-pair=ipsec:tunnel-password=cisco	
cisco-av-pair=ipsec:ikev2-password-local=cisco	
cisco-av-pair=ipsec:ikev2-password-remote=cisco	

Figure 2a-16 CiscoSecure ACS RADIUS Activity

Configuration

Syntax highlighted in **cyan** needs to be added or modified.

R6

[Click here to view code image](#)

```
aaa new-model
!
!
aaa authorization network list1 group radius
!
crypto ikev2 proposal 1
  encryption aes-cbc-256
  integrity sha256
  group 5
!
crypto ikev2 policy lan2lan
  match fvrfl any
  proposal 1

crypto ikev2 name-mangler identities
  fqdn all
!
crypto ikev2 profile flexvpn
  match identity remote fqdn domain cisco.com
  identity local fqdn r6.cisco.com
  authentication local pre-share
  authentication remote pre-share
  keyring aaa list1 name-mangler identities
  virtual-template 1
!
crypto ipsec profile flexvpn
  set ikev2-profile flexvpn
!
interface Loopback3
  ip address 172.16.70.6 255.255.255.0
!
interface Ethernet0/1
  ip address 10.50.70.6 255.255.255.0

interface Virtual-Template1 type tunnel
  ip unnumbered Loopback3
  tunnel source Ethernet0/1
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile flexvpn
!
radius-server host 192.168.2.18 key cisco
!
router rip
  version 2
  passive-interface Ethernet0/0
```



```
network 172.16.0.0
network 172.17.0.0
no auto-summary
```

R7

[Click here to view code image](#)

```
crypto ikev2 proposal 1
  encryption aes-cbc-256
  integrity sha256
  group 5
!
crypto ikev2 policy lan2lan
  match fvrf any
  proposal 1
!
!
crypto ikev2 keyring flexvpn
  peer r6
  identity fqdn r6.cisco.com
  pre-shared-key cisco
!
!
!
crypto ikev2 profile flexvpn
  match identity remote fqdn r6.cisco.com
  identity local fqdn r7.cisco.com
  authentication local pre-share
  authentication remote pre-share
  keyring local flexvpn
!
crypto ipsec profile flexvpn
  set ikev2-profile flexvpn

interface Tunnel1
  ip address 172.16.70.7 255.255.255.0
  tunnel source GigabitEthernet0/1
  tunnel mode ipsec ipv4
  tunnel destination 10.50.70.6
  tunnel protection ipsec profile flexvpn

router rip
  version 2
  network 172.16.0.0
  network 172.17.0.0
  no auto-summary
```

Tech Notes

IKEv2 Smart Defaults

The Cisco IOS IKEv2 implementation includes policy and proposal smart defaults that eliminate the necessity for the user to add lines of configuration to facilitate various combinations of attributes that might be negotiated between peers. The benefit is reduced configuration and policy management overhead. One of the disadvantages of using smart defaults is that uniform policy enforcement might not occur as expected if one peer (without smart defaults) is misconfigured and negotiates a lower level of security. If both peers support smart defaults, the first policy match will be applied, which again might not be optimal. The other issue is in terms of performance and number of proposals sent by the initiator. Like an EZVPN client, which sends all combinations of proposal elements (auth method, encryption algorithm, and so on), the smart default-based initiator will send all combinations of proposals defined in the default protection suite with the expectation that the peer will accept one, even if it is the last combination!

The default IKEv2 policy and proposal suites can be displayed using the following commands:

[Click here to view code image](#)

```
show crypto ikev2 policy default
```

```
IKEv2 policy : default
```

```
Match fvrfl : any
```

```
Match address local : any
```

```
Proposal    : default
```

```
show crypto ikev2 proposal default
```

```
IKEv2 proposal: default
```

```
Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
```

```
Integrity  : SHA512 SHA384 SHA256 SHA96 MD596
```

```
PRF       : SHA512 SHA384 SHA256 SHA1 MD5
```

```
DH Group   : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
```

IKEv2 Anti-Clogging Cookie

In IKEv2, cookies serve two purposes. First, they are used as IKE SA identifiers in the headers of IKE messages. As with ESP and AH, in IKEv2 the recipient of a message chooses an IKE SA identifier that uniquely defines that SA to that recipient. The IKE SA identifier is then used as part of a security association database (SADB) index.

Cookies in IKEv2 have a second function. To reduce the potential of IKE protocol-based DoS attacks, the IKEv2 anti-clogging cookie feature is available in Cisco IOS. Receipt of a request to start an SA can consume substantial resources. A likely denial-of-service attack using the IKE protocol is to overwhelm a system with large numbers of SA requests from forged IP addresses. Upon receipt of an IKE_SA_init, a responder can either proceed with setting up the SA or can tell the initiator to send another IKE_SA_init, this time providing a supplied cookie. If the initiator was not a legitimate sender of an initiation message, it will not respond to the cookie exchange and the responder will not proceed with the original IKE request.

To prevent adding the overhead of this extra IKE exchange for each SA request, the anti-clogging cookie is a user-configurable option that enables an IKEv2 cookie challenge for incoming requests

only when the number of half-open SAs exceeds a configured number. The command syntax is as follows:

[Click here to view code image](#)

```
crypto ikev2 cookie-challenge number of half-opened SAs
```

RADIUS Tunnel Attributes and IKEv2

As with IKEv1, RADIUS may be used to retrieve a preshared key and other authorization attributes from an AAA server for IKEv2. The following debug snapshot shows AAA integration with IKEv2. R6 receives the IKE_AUTH(i) message from R7 and will use the IKE ID type and its value to build a username R7.cisco.com with default password cisco, to be used as the RADIUS user credentials to fetch the preshared key for R7.

[Click here to view code image](#)

```
IKEv2:(SA ID = 1):Stopping timer to wait for auth message
IKEv2:(SA ID = 1):Checking NAT discovery
IKEv2:(SA ID = 1):NAT not found
IKEv2:(SA ID = 1):Searching policy based on peer's identity 'r7.cisco.com' of
type 'FQDN'
IKEv2:found matching IKEv2 profile 'flexvpn'
IKEv2:Searching Policy with fvr 0, local address 10.50.70.6
IKEv2:Found Policy 'lan2lan'
IKEv2:(SA ID = 1):Verify peer's policy
IKEv2:(SA ID = 1):Peer's policy verified
IKEv2:(SA ID = 1):Get peer's authentication method
IKEv2:(SA ID = 1):Peer's authentication method is 'PSK'
IKEv2:(SA ID = 1):Get peer's preshared key for r7.cisco.com
IKEv2:(SA ID = 1):[IKEv2 -> AAA] Password request sent
RADIUS/ENCODE(00000045):Orig. component type = VPN IPSEC
RADIUS(00000045): Config NAS IP: 0.0.0.0
RADIUS(00000045): Config NAS IPv6: ::
RADIUS/ENCODE(00000045): acct_session_id: 58
RADIUS(00000045): sending
RADIUS/ENCODE: Best Local IP-Address 10.50.80.6 for Radius-Server 192.168.2.18
RADIUS(00000045): Send Access-Request to 192.168.2.18:1645 id 1645/2, len 76
RADIUS: authenticator 7E 27 B9 E8 5E 69 3C 5F - 40 16 FD 66 AF DE ED 10
RADIUS: User-Name      [1] 14 "r7.cisco.com"
RADIUS: User-Password [2] 18 *
R6#
RADIUS: Calling-Station-Id [31] 12 "10.50.40.7"
RADIUS: Service-Type      [6] 6 Outbound          [5]
RADIUS: NAS-IP-Address    [4] 6 10.50.80.6
RADIUS(00000045): Sending a IPv4 Radius Packet
RADIUS(00000045): Started 5 sec timeout
RADIUS: Received from id 1645/2 192.168.2.18:1645, Access-Accept, len 184
```

```

RADIUS: authenticator C4 1C B7 E9 52 87 19 3E - 3C 66 05 77 D7 1D 25 C3
RADIUS: User-Name      [1] 14 "r7.cisco.com"
RADIUS: Class          [25] 22
RADIUS: 43 41 43 53 3A 61 63 73 2F 31 36 34 31 35 34 37 [CACs:acs/1641547]
RADIUS: 31 35 2F 32      [ 15/2]
RADIUS: Tunnel-Type     [64] 6 01:ESP          [9]
RADIUS: Tunnel-Medium-Type [65] 6 01:IPv4      [1]
RADIUS: Vendor, Cisco   [26] 35
RADIUS: Cisco AVpair    [1] 29 "ipsec:tunnel-password=cisco"
RADIUS: Vendor, Cisco   [26] 40
RADIUS: Cisco AVpair    [1] 34 "ipsec:ikev2-password-local=cisco"
RADIUS: Vendor, Cisco   [26] 41
RADIUS: Cisco AVpair    [1] 35 "ipsec:ikev2-password-remote=cisco"
RADIUS(00000045): Received from id 1645/2
IKEv2:(SA ID = 1):[AAA -> IKEv2] Received password response
IKEv2:unsupported attr type 445
IKEv2:unsupported attr type 437
IKEv2:unsupported attr type 438
IKEv2:unsupported attr type 473
IKEv2:unsupported attr type 474
IKEv2:(SA ID = 1):Verify peer's authentication data
IKEv2:(SA ID = 1):Use preshared key for id r7.cisco.com, key len 5
IKEv2:[IKEv2 -> Crypto Engine] Generate IKEv2 authentication data
IKEv2:[Crypto Engine -> IKEv2] IKEv2 authentication data generation PASSED
IKEv2:(SA ID = 1):Verification of peer's authentication data PASSED

```

The RADIUS attributes seen in the preceding debug output are configured on the Cisco Secure ACS as shown in [Figure 2a-17](#).

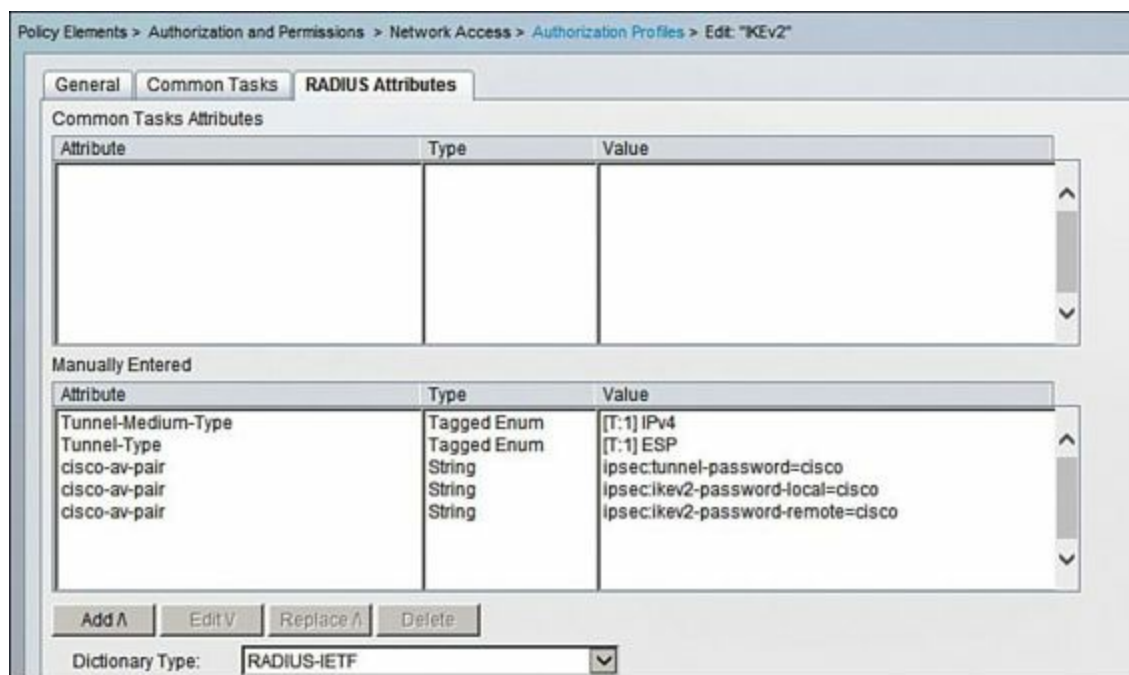


Figure 2a-17 RADIUS Tunnel Attributes Defined on Cisco Secure ACS

Solution and Verification for Exercise 3.5: Configure and Troubleshoot FlexVPN Remote Access (Client to Server)

Skills Tested

- Configuring IKEv2 with remote access client support on a Cisco IOS Router
- Understanding the concepts of FlexVPN in a client/server model
- Implementing IKEv2 integrated static route support

Solution and Verification

This solution requires the FlexVPN client configuration on R4 to be completed and a VPN tunnel be successfully established with the FlexVPN server on R2. This client/server implementation of FlexVPN using IKEv2 is the alternative to the IKEv1-based EZVPN solution. IKEv2 for remote-access clients uses mode configuration and extended authentication (XAUTH) capabilities in the form of IKEv2 protocol integrated Configuration (CFG) payloads and support for Extensible Authentication Protocol (EAP). This differs from IKEv1, which added a Phase 1.5 between IKE (Phase 1) and IPsec (Phase 2) negotiation to support remote access VPN clients. Mode configuration and XAUTH were added to IKEv1 as extensions that were not supported by all vendors. In this question, preshared keys will be used for peer authentication. If EAP was required, it would be specified as the client authentication method and the server must then use rsa-signatures.

Server-defined attributes will be sent using IKEv2 config payloads and can be configured locally on the router or remotely on a AAA server accessible via RADIUS. This solution uses locally configured attributes using the **crypto ikev2 authorization policy** syntax that can also be used to incorporate other policy attributes, as defined in an **aaa attribute list**. This replaces the IKEv1-based **crypto isakmp client configuration group** syntax.

This solution also requires the use of new IKEv2 constructs to propagate address/mask information between peers that will be used to create static routes to control the forwarding of traffic requiring protection. The functionality of reverse route injection (RRI) is replaced by the **route set** and **route accept** commands.

Finally, in EZVPN with IKEv1, configuration mode functionality was explicitly configured in an ISAKMP profile. When defining an IKEv2 profile, configuration mode functionality is on by default via the following commands that are not displayed in the configuration:

- **config-exchange set send**
- **config-exchange set accept**
- **config-exchange request**

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**
- Nonzero/nonnull syntax appears in **violet**
- Variable syntax appears in **green**

Verification of this solution requires the VPN tunnel to be established and ACTIVE. R4 must also receive all policy attributes from the server, which will be “pushed” in response to a client CONFIG-

REQUEST.

Initiate the client connection from R4:

[Click here to view code image](#)

```
R4# crypto ikev2 client flexvpn connect
```

Check that the VPN connection state is ACTIVE using Tunnel0 as the logical interface and that an address has been assigned from the address pool defined on R2. Using **ip address negotiated** on T0 will ensure the assigned address is installed.

[Click here to view code image](#)

```
R4# show crypto ikev2 client flex
```

```
Profile : flex
Current state:ACTIVE
Peer : 10.50.100.2
Source : Ethernet0/1
ivrif : IP DEFAULT
fvrf : IP DEFAULT
Backup group: Default
Tunnel interface : Tunnel0
Assigned ip address: 172.17.100.55 <- should be between .50 and .60
```

Verify whether the IKEv2 proposals and IPsec transform set were correctly defined on R4. These negotiated algorithms are displayed in the **show crypto ikev2 session detail** command.

The protection suites were explicitly defined on R2 in lieu of using IKEv2 smart defaults. If both peers were configured to use smart defaults, the most secure supported (hardware dependent) protection suite match would be applied.

[Click here to view code image](#)

```
R4# show crypto ikev2 session detail
```

```
IPv4 Crypto IKEv2 Session
```

```
Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

Tunnel-id	Local	Remote	fvrf/ivrif	Status
1	10.50.30.4/500	10.50.100.2/500	none/none	READY

```
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/277 sec
CE id: 1032, Session-id: 2
Status Description: Negotiation done
Local spi: 0696C6F582787B23 Remote spi: 49C2BF63CF74F456
Local id: R4.cisco.com
Remote id: 10.50.100.2
Local req msg id: 2 Remote req msg id: 0
```

```
Local next msg id: 2      Remote next msg id: 0
Local req queued: 2      Remote req queued: 0
Local window: 5          Remote window: 5
DPD configured for 0 seconds, retry 0
NAT-T is not detected
Cisco Trust Security SGT is disabled
Pushed IP address: 172.17.100.55
DNS Primary: 192.168.2.25
```

```
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0xEEF6B847/0x81642A80
AH spi in/out: 0x0/0x0
CPI in/out: 0x0/0x0
Encr: 3DES, esp_hmac: MD596
ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

The other key functionality to be verified is that routing information has been propagated between peers. If routes are not sent and accepted, data might not correctly be forwarded via the secure VPN.

The **crypto ikev2 profile** defined by the user must contain the following command syntax. Note that the use of **flex** as the AAA username will be a pointer to the locally configured authorization policy.

[Click here to view code image](#)

```
aaa authorization network list1 local
aaa authorization group psk list list1 flex
```

```
R4# show crypto ikev2 authorization policy
```

```
IKEv2 Authorization Policy : flex
```

```
route set interface
```

```
route set acl: routes <- this is a pointer to a pre-defined ACL that will form
the basis of a static route created on R2
```

```
route accept any tag : 1 distance : 1
```

Verify whether the route information was sent to R2 via a config-set. R2 will respond with a config-accept. Ping the Loopback0 interface of R4, and check IPsec counters to verify the VPN tunnel is being used to transport data.

[Click here to view code image](#)

```
R2# show ip route
```

```
S 172.17.100.55/32 is directly connected, Virtual-Access1
```

```
172.18.0.0/24 is subnetted, 1 subnets
```

```
S 172.18.34.0 is directly connected, Virtual-Access1
```

```
R2# ping 172.18.34.4
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.18.34.4, timeout is 2 seconds:
```

```
!!!!
```

Success rate is **100** percent (5/5), round-trip min/avg/max = 5/5/6 ms

```
R2# show crypto ipsec sa
```

```
.....  
interface: Virtual-Access1  
  Crypto map tag: Virtual-Access1-head-0, local addr 10.50.100.2  
  
protected vrf: (none)  
local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)  
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)  
current_peer 10.50.30.4 port 500  
  PERMIT, flags={origin_is_acl,}  
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5  
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5  
#pkts compressed: 0, #pkts decompressed: 0  
#pkts not compressed: 0, #pkts compr. failed: 0  
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
R4# show ip route
```

```
S    172.17.100.2/32 is directly connected, Tunnel0  
C    172.17.100.55/32 is directly connected, Tunnel0
```

Configuration

Syntax highlighted in **cyan** needs to be added or modified.

R4

[Click here to view code image](#)

```
aaa authorization network list1 local
```

```
crypto ikev2 authorization policy flex  
route set interface  
route set access-list routes
```

```
crypto ikev2 keyring key  
peer flexserver  
  address 0.0.0.0 0.0.0.0  
  pre-shared-key cisco  
!  
!  
!
```

```
crypto ikev2 profile prof  
match identity remote address 10.50.100.2 255.255.255.255  
identity local fqdn R4.cisco.com  
authentication local pre-share
```



```
authentication remote pre-share
keyring local key
aaa authorization group psk list list1 flex
config-exchange set send
config-exchange set accept
config-exchange request
!
crypto ikev2 client flexvpn flex
peer 1 10.50.100.2
connect manual
client connect Tunnel0

crypto ipsec profile ipsecprof
set transform-set 3des
set ikev2-profile prof
!
interface Loopback2
ip address 172.18.34.4 255.255.255.0

interface Tunnel0
ip address negotiated
tunnel source Ethernet0/1
tunnel mode ipsec ipv4
tunnel destination dynamic
tunnel protection ipsec profile ipsecprof

ip access-list standard routes
permit 172.18.34.0 0.0.0.255
```

R2

[Click here to view code image](#)

```
aaa authorization network local-list local
!
aaa attribute list ikev2ra
attribute type ipsec-backup-gateway "R1.cisco.com"
attribute type interface-config "ip mtu 1100"
!
!
!
crypto ikev2 name-mangler group-name
fqdn domain
!
!
crypto ikev2 authorization policy cisco.com
pool flex
```

```

dns 192.168.2.25
aaa attribute list ikev2ra
route set interface
route accept any
!
!
crypto ikev2 keyring key
peer flexclient
address 0.0.0.0 0.0.0.0
pre-shared-key cisco
!
!
crypto ikev2 profile prof
match identity remote fqdn domain cisco.com
authentication local pre-share
authentication remote pre-share
config-exchange set send
config-exchange set accept
config-exchange request
keyring local key
aaa authorization group psk list local-list name-mangler group-
name
virtual-template 1
!

crypto ipsec profile ipsecprof
set transform-set 3des
set ikev2-profile prof
!

interface Virtual-Template1 type tunnel
ip unnumbered Loopback0
tunnel source Ethernet0/0
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsecprof
!
ip local pool flex 172.17.100.50 172.17.100.60

```

Tech Notes

Debugging FlexVPN

Configuring client to server-based remote access using FlexVPN is fairly complex, and as such, the following debugging example is included as a reference.

Manually initiate the connection:

[Click here to view code image](#)

R4# crypto ikev2 client flexvpn connect

R4#

HDR, SAi1, KEi, Ni

Initiator
R4



Responder
R2

IKEv2:% Getting preshared key from profile keyring key

IKEv2:% Matched peer block 'flexserver'

IKEv2:Searching Policy with fvrfl 0, local address 10.50.30.4

IKEv2:Using the Default Policy for Proposal

IKEv2:Found Policy 'default'

IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Computing DH public key, DH Group 5

IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] DH key Computation PASSED

IKEv2:(SA ID = 1):Request queued for computation of DH key

IKEv2:IKEv2 initiator - no config data to send in IKE_SA_INIT exch

IKEv2:(SA ID = 1):Generating IKE_SA_INIT message

IKEv2:(SA ID = 1):IKE Proposal: 1, SPI size: 0 (initial negotiation),

Num. transforms: 15

AES-CBC AES-CBC AES-
CBC SHA512 SHA384 SHA256 SHA1 MD5 SHA512
SHA384 SHA256

SHA96 MD596 DH_GROUP_1536_MODP/Group

5 DH_GROUP_1024_MODP/Group 2

IKEv2:(SA ID = 1):Sending Packet [To 10.50.100.2:500/From 10.50.30.4:500/VRF
i0:f0]

Initiator SPI : 5863E01AB3750C92 - Responder SPI : 0000000000000000 Message id: 0

IKEv2 IKE_SA_INIT Exchange REQUEST

Payload contents:

SA KE N VID VID NOTIFY(NAT_DETECTION_SOURCE_IP)
NOTIFY(NAT_DETECTION_DESTINATION_
IP)

IKEv2:(SA ID = 1):Insert SA

HDR, SAR1, KEr, Nr, [CertReq]

Initiator
R4



Responder
R2

IKEv2:(SA ID = 1):Received Packet [From 10.50.100.2:500/To 10.50.30.4:500/VRF
i0:f0]

Initiator SPI : 5863E01AB3750C92 - Responder SPI : A5EAB51958821403 Message id: 0

IKEv2 IKE_SA_INIT Exchange RESPONSE

Payload contents:

SA KE N VID VID NOTIFY(NAT_DETECTION_SOURCE_IP)
NOTIFY(NAT_DETECTION_DESTINATION_
IP) CERTREQ NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED)

IKEv2:(SA ID = 1):Processing IKE_SA_INIT message
IKEv2:(SA ID = 1):Verify SA init message
IKEv2:(SA ID = 1):Processing IKE_SA_INIT message
IKEv2:(SA ID = 1):Checking NAT discovery
IKEv2:(SA ID = 1):NAT not found
IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Computing DH secret key, DH Group 5
IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] DH key Computation PASSED
IKEv2:(SA ID = 1):Request queued for computation of DH secret
IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Calculate SKEYSEED and create rekeyed
IKEv2 SA
IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] SKEYSEED calculation and creation of
rekeyed IKEv2 SA PASSED
IKEv2:(SA ID = 1):Completed SA init exchange

HDR, SK (IDi, AUTH, CP(CFG_REQUEST),
SAi2, TSi, TSr)



IKEv2:Config data to send:
Config-type: Config-request
Attrib type: ipv4-addr, length: 0
Attrib type: ipv4-netmask, length: 0
Attrib type: ipv4-dns, length: 0
Attrib type: ipv4-dns, length: 0
Attrib type: ipv4-nbns, length: 0
Attrib type: ipv4-nbns, length: 0
Attrib type: app-version, length: 259, data: Cisco IOS Software, Linux Software
(I86BI_LINUX-ADVENTERPRISEK9-M), Version 15.2(2)T2.3, DEVELOPMENT TEST
SOFTWARE

Technical Support: <http://www.cisco.com/techsupport>

Copyright (c) 1986-2012 by Cisco Systems, Inc.

Compiled Thu 08-Nov-12 06:59 by prod_rel_team

Attrib type: ipv4-subnet, length: 0
Attrib type: split-dns, length: 0
Attrib type: banner, length: 0
Attrib type: config-url, length: 0
Attrib type: config-ver, length: 0
Attrib type: backup-gateway, length: 0
Attrib type: def-domain, length: 0
IKEv2:(SA ID = 1):Have config mode data to send

IKEv2:(SA ID = 1):Generate my authentication data
IKEv2:(SA ID = 1):Use preshared key for id R4.cisco.com, key len 5
IKEv2:[IKEv2 -> Crypto Engine] Generate IKEv2 authentication data
IKEv2:[Crypto Engine -> IKEv2] IKEv2 authentication data generation PASSED
IKEv2:(SA ID = 1):Get my authentication method

IKEv2:(SA ID = 1):My authentication method is 'PSK'
IKEv2:(SA ID = 1):Generating IKE_AUTH message
IKEv2:(SA ID = 1):Constructing IDi payload: 'R4.cisco.com' of type 'FQDN'
IKEv2:(SA ID = 1):ESP Proposal: 1, SPI size: 4 (IPSec negotiation),
Num. transforms: 2

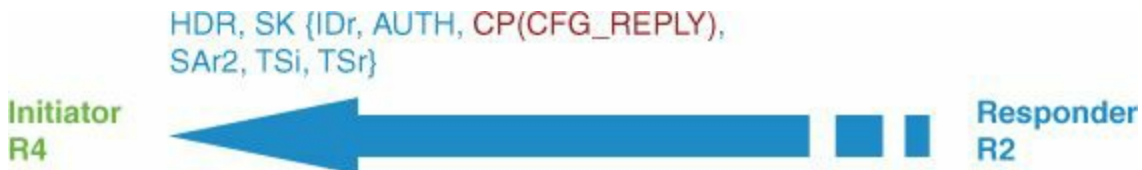
3DES Don't use ESN
IKEv2:(SA ID = 1):Building packet for encryption.

Payload contents:
VID IDi AUTH CFG SA TSi TSr NOTIFY(INITIAL_CONTACT)
NOTIFY(SET_WINDOW_SIZE) NOTIFY(ESP_TFC_NO_SUPPORT)
NOTIFY(NON_FIRST_FRAGS)

IKEv2:(SA ID = 1):Sending Packet [To 10.50.100.2:500/From 10.50.30.4:500/VRF
i0:f0]

Initiator SPI : 5863E01AB3750C92 - Responder SPI : A5EAB51958821403 Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST

Payload contents:
ENCR



IKEv2:(SA ID = 1):Received Packet [From 10.50.100.2:500/To 10.50.30.4:500/VRF
i0:f0]

Initiator SPI : 5863E01AB3750C92 - Responder SPI : A5EAB51958821403 Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE

Payload contents:
VID IDr AUTH CFG SA TSi TSr NOTIFY(SET_WINDOW_SIZE)
NOTIFY(ESP_TFC_NO_SUPPORT)
NOTIFY(NON_FIRST_FRAGS)

IKEv2:(SA ID = 1):Process auth response notify
IKEv2:(SA ID = 1):Searching policy based on peer's identity '10.50.100.2' of type
'IPv4 address'

IKEv2:Searching Policy with fvr0, local address 10.50.30.4

IKEv2:Using the Default Policy for Proposal

IKEv2:Found Policy 'default'

IKEv2:(SA ID = 1):Verify peer's policy

IKEv2:(SA ID = 1):Peer's policy verified

IKEv2:(SA ID = 1):Get peer's authentication method

IKEv2:(SA ID = 1):Peer's authentication method is 'PSK'

IKEv2:(SA ID = 1):Get peer's preshared key for 10.50.100.2

IKEv2:(SA ID = 1):Verify peer's authentication data

IKEv2:(SA ID = 1):Use preshared key for id 10.50.100.2, key len 5

IKEv2:[IKEv2 -> Crypto Engine] Generate IKEv2 authentication data

IKEv2:[Crypto Engine -> IKEv2] IKEv2 authentication data generation PASSED
IKEv2:(SA ID = 1):Verification of peer's authentication data PASSED
IKEv2:Using mlist list1 and username flex for group author request
IKEv2:(SA ID = 1):[IKEv2 -> AAA] Authorisation request sent
IKEv2:(SA ID = 1):[AAA -> IKEv2] Received AAA authorisation response

IKEv2:(SA ID = 1):Received valid config mode data
IKEv2:Config data received:
Config-type: Config-reply
Attrib type: ipv4-addr, length: 4, data: 172.17.100.55
Attrib type: ipv4-subnet, length: 8, data: 172.17.100.2 255.255.255.255
Attrib type: ipv4-dns, length: 4, data: 192.168.2.25
Attrib type: app-version, length: 259, data: Cisco IOS Software, Linux Software
(I86BI_LINUX-ADVENTERPRISEK9-M), Version 15.2(2)T2.3, DEVELOPMENT TEST
SOFTWARE
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 08-Nov-12 06:59 by prod_rel_team
Attrib type: backup-gateway, length: 12, data: R1.cisco.com
IKEv2:(SA ID = 1):Set received config mode data

IKEv2:(SA ID = 1):Processing IKE_AUTH message
IKEv2:KMI/verify policy/sending to IPsec:
prot: 3 txfm: 3 hmac 0 flags 8177 keysize 0 IDB 0x0
IKEv2:(SA ID = 1):IKEV2 SA created; inserting SA into database. SA lifetime timer
(86400 sec) started
IKEv2:IKEv2 MIB tunnel started, tunnel index 1
IKEv2:(SA ID = 1):Load IPSEC key material
IKEv2:(SA ID = 1):Checking for duplicate IKEv2 SA
IKEv2:(SA ID = 1):No duplicate IKEv2 SA found
HDR, SK {CP(CFG_SET)}



Config-type: Config-set
Attrib type: ipv4-subnet, length: 8, data: 172.17.100.55 255.255.255.255
Attrib type: ipv4-subnet, length: 8, data: 172.18.34.0 255.255.255.0
Attrib type: app-version, length: 259, data: Cisco IOS Software, Linux Software
(I86BI_LINUX-ADVENTERPRISEK9-M), Version 15.2(2)T2.3, DEVELOPMENT TEST
SOFTWARE
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 08-Nov-12 06:59 by prod_rel_team

IKEv2:(SA ID = 1):Sending info exch config
IKEv2:(SA ID = 1):Building packet for encryption.

Payload contents:

CFG

IKEv2:(SA ID = 1):Checking if request will fit in peer window

IKEv2:(SA ID = 1):Sending Packet [To 10.50.100.2:500/From 10.50.30.4:500/VRF i0:f0]

Initiator SPI : 5863E01AB3750C92 - Responder SPI : A5EAB51958821403 Message id: 2

IKEv2 INFORMATIONAL Exchange REQUEST

Payload contents:

ENCR

%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up

%FLEXVPN-6-FLEXVPN_CONNECTION_UP: FlexVPN(flex) Client_public_addr = 10.50.30.4

Server_public_addr = 10.50.100.2 Assigned_Tunnel_addr = 172.17.100.55

R4#



*Oct 28 21:15:58.500: IKEv2:(SA ID = 1):Received Packet [From 10.50.100.2:500/To 10.50.30.4:500/VRF i0:f0]

Initiator SPI : E9514C2B78FD144B - Responder SPI : FEB010A8A5E13415 Message id: 2

IKEv2 INFORMATIONAL Exchange RESPONSE

Payload contents:

CFG

IKEv2:(SA ID = 1):Processing ACK to informational exchange

IKEv2:Config data received:

Config-type: Config-ack

Attrib type: ipv4-subnet, length: 0

IKEv2:(SA ID = 1):Set received config mode data

Understanding IKEv2 Routing Options

FlexVPN supports several VPN types that use dynamic routing protocols to forward traffic that requires IPsec protection. In legacy VPN implementations that used crypto maps, or with some EZVPN deployments, RRI was used to create static routes based on IPsec source and destination proxies (addresses/masks). FlexVPN uses new IKEv2 constructs **route set** and **route accept** as described in [Table 2a-5](#).

Command	Description	Example
<code>route set {interface access-list {access-list-name access-list-number expanded-access-list-number ipv6 access-list-name}}</code>	Specifies the route set parameters to the peer via configuration mode: <i>interface</i> —Specifies the route interface. <i>access-list</i> —Specifies the route access list. <i>access-list-name</i> —Access list name. <i>access-list-number</i> —Standard access list number. <i>expanded-access-list-number</i> —Expanded access list number. <i>ipv6</i> —Specifies an IPv6 access list.	Device(config-ikev2-author-policy)# route set interface
<code>route accept any [tag value] [distance value]</code>	Filter the routes received from the peer and specify the tag and metric values to install these routes. <i>any</i> —Accepts all routes received from the peer. <i>tag value</i> —(Optional) Specifies the tag ID for the static routes added by IKEv2. The range is from 1 to 497,777. <i>distance value</i> —(Optional) Specifies the distance for the static routes added by IKEv2. The range is from 1 to 255.	Device(config-ikev2-author-policy)# route accept any tag 10

Table 2a-5 Route Support for IKEv2 Command Syntax

Section 4: System Hardening and Availability

System or device hardening involves implementing techniques that protect against compromise, resulting in either specific device/system failures or disruption to other network services. The goal of enabling protection and monitoring features on a system is performance predictability and network availability. This section requires implementing and troubleshooting specific hardening features such as control and management plane policing. Features that focus on network availability, such as routing protocol security, monitoring traffic transiting a switch, and securing wireless infrastructure, are also covered.

Solution and Verification for Exercise 4.1: BGP TTL-Security through the Cisco ASA

Skills Tested

- Configuring BGP security features; specifically, TTL-Security in Cisco IOS
- Configuring the Cisco ASA to manipulate TTL values and appear as a hop in the network
- Understanding basic BGP **show** commands to aid in troubleshooting and verification

Solution and Verification

In this exercise, the eBGP multihop command must be replaced with the newer TTL-Security command, and ASA2 must be configured to appear as an actual routed hop between R6 and R7.

TTL-Security is based on RFC 5082, “Generalized TTL Security Mechanism (GTSM).” eBGP multihop does not protect against attackers spoofing BGP packets with the TTL specifically set so that the BGP peer will see a TTL = 1 and process the packet. This can lead to DoS attacks that target the router CPU. TTL-Security inverts the TTL check so that only BGP packets with a TTL of 255 less the number of hops specified in the TTL-Security command are processed.

Configuring ASA2 to function as a routed hop in the path of IP packets means that ASA2 will decrement the TTL field of those packets. This behavior will have an impact on the hop count requirements of BGP TTL-Security. To determine how to tune this BGP command, you can use **traceroute** between the BGP neighbors as follows:

[Click here to view code image](#)

```
R7# traceroute 10.50.70.6  
Type escape sequence to abort.  
Tracing the route to r6.cisco.com (10.50.70.6)  
VRF info: (vrf in name/id, vrf out name/id)  
 1 10.50.40.20 4 msec * 0 msec  
 2 10.50.50.5 0 msec 4 msec 8 msec  
 3 r6.cisco.com (10.50.70.6) 0 msec * 0 msec
```

With TTL-Security, the BGP packet is sent with a TTL = 255. With two hops in the path between R7 and R6 (ASA2 and SW2), BGP packets will be processed only if the IP packet TTL is $255 - 2 \geq 253$. Therefore, the hop count parameter used with TTL-Security is configured as

[Click here to view code image](#)

```
neighbor ip-address ttl-security hops 2
```

For all verification syntax that follows:

- Required output appears in **red**

Verify that ASA2 has been correctly configured to decrement the TTL in IP packets:

[Click here to view code image](#)

```
R7# traceroute 10.50.70.6  
Type escape sequence to abort.  
Tracing the route to r6.cisco.com (10.50.70.6)  
VRF info: (vrf in name/id, vrf out name/id)  
 1 10.50.40.20 4 msec * 0 msec  
 2 10.50.50.5 0 msec 4 msec 8 msec  
 3 r6.cisco.com (10.50.70.6) 0 msec * 0 msec
```

The ASA2 service policy should specify the following:

[Click here to view code image](#)

```
ASA2# show service-policy  
...  
Class-map: set-ttl  
  Set connection policy:      drop 0  
  Set connection decrement-ttl
```

To verify whether the TTL-Security hop count is set correctly and BGP packets are being processed, check the state of the BGP connection and that BGP routes have been installed in the BGP route tables on R6 and R7:

[Click here to view code image](#)

```
R7# show ip bgp neighbors 10.50.70.6 | include state
  BGP state = Established, up for 1d21h
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
```

```
R7# show ip bgp
BGP table version is 15, local router ID is 172.18.107.7
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, x best-external,
               f RT-Filter, a additional-path
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 172.18.106.0/24	10.50.70.6	0	0	106	?
*> 172.18.107.0/24	0.0.0.0	0	32768		?

```
R6# show ip bgp
BGP table version is 3, local router ID is 172.18.106.6
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, x best-external,
               f RT-Filter, a additional-path
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 172.18.106.0/24	0.0.0.0	0	32768		?
*> 172.18.107.0/24	10.50.40.7	0	0	107	?

Configuration

Replace

[Click here to view code image](#)

```
neighbor 10.50.40.7 ebgp-multihop 2
neighbor 10.50.70.6 ebgp-multihop 2
```

R6

[Click here to view code image](#)

```
router bgp 106
  bgp log-neighbor-changes
  redistribute connected route-map bgp
  neighbor 10.50.40.7 remote-as 107
  neighbor 10.50.40.7 password cisco
```

```
neighbor 10.50.40.7 ttl-security hops 2
```

R7

[Click here to view code image](#)

```
router bgp 107
  bgp log-neighbor-changes
  redistribute connected route-map bgp
  neighbor 10.50.70.6 remote-as 106
  neighbor 10.50.70.6 password cisco
  neighbor 10.50.70.6 ttl-security hops 2
```

ASA2

[Click here to view code image](#)

```
class-map set-ttl
  Match any
policy-map global_policy
  class set-ttl
  set connection decrement-ttl
```

Tech Notes

By default, Cisco IOS sends BGP messages to EBGP neighbors with an IP time-to-live (TTL) of 1, implying the BGP peers are adjacent. This restriction can be adjusted with the **ebgp-multihop** command. With this command, BGP packets can be sent with the TTL at a higher number than 1. Sending BGP messages with a TTL of 1 requires the peer to be directly connected, or the packets will expire in transit. Likewise, a BGP router will only accept incoming BGP messages with a TTL of 1 (or whatever value is specified by **ebgp-multihop**), which can help mitigate spoofing attacks. However, it is still possible for a remote attacker to adjust the TTL of sent packets so that they appear to originate from a directly connected peer. Spoofing legitimate-looking packets to a BGP router at high volume can lead to a DoS attack.

The solution to this, as discussed in RFC 5082, is to invert the direction in which the TTL is counted. The maximum value of the 8-bit TTL field in an IP packet is 255. Instead of accepting only packets with a TTL set to 1, the BGP router can accept only packets with a TTL of 255 to ensure that the originator really is exactly one hop away. This is accomplished in Cisco IOS with the TTL-Security feature. Only BGP messages with an IP TTL greater than or equal to 255 minus the specified hop count will be accepted. TTL security and EBGP multihop are mutually exclusive; **ebgp-multihop** is no longer needed when TTL security is in use.

Solution and Verification for Exercise 4.2: Configure and Troubleshoot Control Plane Protection

Skills Tested

- Control Plane Protection (CPPr) options
- Understanding how to identify closed-ports on a Cisco IOS device

Solution and Verification

To prevent the unnecessary processing of packets destined to closed ports, CPPr can be tuned to track open and closed ports on the control plane. Control plane protection techniques are applied to the control plane subinterfaces (host, transit, CEF exception). In this case, because we are focusing on the ports that are open and closed on the router itself, the CPPr policy is applied to the host subinterface. It is important that only traffic destined to closed ports be dropped. This requires knowledge of the features and services running on the router. The commands **show control-plane host open-ports** and **show udp** are useful for determining the ports currently being used by the host. Note that not all ports appear in the open-ports list. As new applications are added to Cisco IOS, there could be a time lag with respect to adding them to the list of known ports. As such, this exercise requires the administrator to compare the open-ports list against the actual list of services supported by the host. When defining the CPPr policy, the MQC syntax is used with the service policy being applied to the control-plane host subinterface and the port-filter type specified on class maps and policy maps.

For all verification syntax that follows:

- Required output appears in **red**
- Variable syntax appears in **green**

Determine the ports on R1 that are open and listening:

[Click here to view code image](#)

```
R1# show control-plane host open-ports
Active internet connections (servers and established)
Prot      Local Address      Foreign Address  Service  State
tcp       *:22                *:0              SSH-Server LISTEN
tcp       *:23                *:               Telnet   LISTEN
tcp       *:8080              *:0              HTTP CORE LISTEN
tcp       *:8080              *:0              HTTP CORE LISTEN
udp       *:123               *:0              NTP      LISTEN
udp       *:4500              *:0              ISAKMP   LISTEN
udp       *:500               *:0              ISAKMP   LISTEN
```

As the preceding output displays, the **show control-plane host open-ports** command is not displaying UDP/848 for GDOI, which is running as a result of the configuration of GETVPN in [Exercise 3.2](#) in this lab.

Knowing that some ports might be missing from the **show control-plane host open-ports** output, verify the UDP-based services listening on R1. Note that UDP/848 is an open port that was not displayed by **show control-plane host open-ports**.

[Click here to view code image](#)

```
R1# show udp
Proto Remote Port Local Port In Out Stat TTY OutputIF
17 --listen-- 10.50.100.1 123 0 0 1001001 0
17(v6) --listen-- FE80::1 123 0 0 1020001 0
17 --listen-- 10.50.100.1 848 0 0 1001011 0
17(v6) --listen-- FE80::1 848 0 0 1020011 0
```

```

17    --listen--    10.50.100.1    4500  0  0  1001011  0
17(v6) --listen--    FE80::1        4500  0  0  1020011  0
17    --listen--    10.50.100.1    500   0  0  1001011  0
17(v6) --listen--    FE80::1        500   0  0  1020011  0
17    --listen--    10.50.100.1    4500  0  0  1001011  0
17(v6) --listen--    FE80::1        4500  0  0  1020011  0

```

Knowing UDP/848 is not being classified as an open port, and will in fact be deemed a closed port, the traffic of interest defined in the class map must be all closed ports except UDP/848:

[Click here to view code image](#)

```
R1# show class-map type port-filter
```

```
Class Map type port-filter match-all pf-class
```

```
Match not port udp 848
```

```
Match closed-ports
```

```
R1# show policy-map type port-filter
```

```
Policy Map type port-filter pf-policy
```

```
Class pf-class
```

```
drop
```

```
R1# show run | section control-plane host
```

```
control-plane host
```

```
service-policy type port-filter input pf-policy
```

Configuration

R1

[Click here to view code image](#)

```
class-map type port-filter match-all pf-class
```

```
match not port udp 848
```

```
match closed-ports
```

```
!
```

```
!
```

```
policy-map type port-filter pf-policy
```

```
class pf-class
```

```
drop
```

```
control-plane host
```

```
service-policy type port-filter input pf-policy
```

Tech Notes

Specific map (class, policy) types are available for enhancing CPPr.

- The port-filtering feature provides for policing/dropping of packets going to closed or nonlistening TCP/UDP ports.

- Queue thresholding limits the number of packets for a specified protocol that will be allowed in the control plane IP input queue.

The Cisco IOS CLI options are as follows:

[Click here to view code image](#)

```
class-map type
port-filter    Class map for port filter
queue-threshold Class map for queue threshold

policy-map type
port-filter    Control-plane tcp/udp port filtering
queue-threshold Control-plane protocol queue limiting
```

Solution and Verification for Exercise 4.3: Control Plane Protection for IPv6 Cisco IOS

Skills Tested

- Control Plane Protection options applied to IPv6 traffic

Solution and Verification

CPPr is applicable to all IP traffic processed by the router control plane. In this question, the policy requirements are to police ICMPv6 traffic that is seen by the CPU, and to apply policing to the default class.

As discussed in [Exercise 1.4](#) of this lab, ICMPv6 messages play an important role in the management of an IPv6 network. When a network supports IPv6 (RFC 2460), the Internet Control Message Protocol version 6 (ICMPv6) (RFC 4443) plays a fundamental role, including being an essential component in establishing and maintaining communications both at the interface level and for sessions to remote nodes. ICMPv6 is to IPv6 what ARP is to IPv4. This is a key point that can be used to identify which control-plane subinterface requires the CPPr service policy. Services such as ARP and ICMPv6 are handled by the CEF-exception subinterface.

This exercise calls for CPPr on essential ICMPv6 messages. Several messages must be allowed on the network. These are discussed in RFC 4890, “Recommendations for Filtering ICMPv6 Messages in Firewall.” Overly aggressive filtering of ICMPv6 by firewalls can have a detrimental effect on the establishment and maintenance of IPv6 communications. This document outlines the messages that should not be filtered and instead will be processed by hosts that are a part of the IPv6 network.

The interesting traffic for the class map comprises all recommended ICMPv6 messages that can be seen by the router. A match of all ICMP types can also be used; however, for purposes of this guide, the administrator should be familiar with specific ICMPv6 message types.

For all verification syntax that follows:

- Required output appears in **red**
- Variable syntax appears in **green**

Verify the contents of the ICMPv6 access list that will be referenced by the CPPr class map:

[Click here to view code image](#)

```
R4# show access-list RFC4890
```

```
IPv6 access list RFC4890
```

```
permit icmp any any echo-reply sequence 10
permit icmp any any echo-request sequence 20
permit icmp any any destination-unreachable sequence 30
permit icmp any any port-unreachable sequence 40
permit icmp any any packet-too-big sequence 50
permit icmp any any time-exceeded sequence 60
permit icmp any any parameter-problem sequence 70
permit icmp any any mld-query sequence 80
permit icmp any any mld-reduction sequence 90
permit icmp any any mld-report sequence 100
permit icmp any any nd-na (23776 matches) sequence 110
permit icmp any any nd-ns (12962 matches) sequence 120
permit icmp any any router-solicitation sequence 130
permit icmp any any router-advertisement sequence 140
```

Verify whether policing rate, conform and exceed actions, and the CEF exception subinterface have been configured correctly:

[Click here to view code image](#)

```
R4# show policy-map control-plane cef-exception
```

```
Control Plane Cef-exception
```

```
Service-policy input: COPPRv6
```

```
Class-map: ICMPv6 (match-all)
```

```
25142 packets, 2038444 bytes
```

```
5 minute offered rate 0 bps, drop rate 0 bps
```

```
Match: access-group name RFC4890
```

```
police:
```

```
  cir 8000 bps, bc 1500 bytes
```

```
  conformed 25142 packets, 2038444 bytes; actions:
```

```
    transmit
```

```
  exceeded 0 packets, 0 bytes; actions:
```

```
    drop
```

```
  conformed 0000 bps, exceeded 0000 bps
```

```
Class-map: class-default (match-any)
```

```
264174 packets, 29538421 bytes
```

```
5 minute offered rate 0 bps, drop rate 0 bps
```

```
Match: any
```

```
police:
```

```
  cir 10000 bps, bc 1500 bytes
```

```
  conformed 264163 packets, 29536519 bytes; actions:
```

```
    transmit
```

exceeded 11 packets, 1902 bytes; actions:
transmit
conformed 0000 bps, exceeded 0000 bps

Configuration

R4

[Click here to view code image](#)

```
class-map match-all ICMPv6
  match access-group name RFC4890

policy-map COPPRv6
  class ICMPv6
    police 8000 conform-action transmit exceed-action drop
  class class-default
    police 10000 conform-action transmit exceed-action transmit

ipv6 access-list RFC4890
  permit icmp any any echo-reply
  permit icmp any any echo-request
  permit icmp any any destination-unreachable
  permit icmp any any port-unreachable
  permit icmp any any packet-too-big
  permit icmp any any time-exceeded
  permit icmp any any parameter-problem
  permit icmp any any mld-query
  permit icmp any any mld-reduction
  permit icmp any any mld-report
  permit icmp any any nd-na
  permit icmp any any nd-ns
  permit icmp any any router-solicitation
  permit icmp any any router-advertisement

control-plane cef-exception
  service-policy input COPPRv6
```

Section 5: Threat Identification and Mitigation

This section requires the implementation of threat identification and mitigation techniques on different Cisco platforms. On a Cisco IOS Router, NetFlow is used to identify possible attack patterns, and this information is then used to build a Flexible Packet Matching (FPM) policy. DHCP activities can be manipulated to launch attacks that are mitigated by methods configured on Cisco Catalyst switches. This section also covers application-specific attack mitigation features on the Cisco ASA.

Solution and Verification for Exercise 5.1: Preventing IP Address Spoofing on the Cisco ASA

Skills Tested

- Understanding and configuring mitigation techniques for IP address spoofing

Solution and Verification

Several methods are available on the Cisco ASA to protect against IP address spoofing. You should apply an access list, based on recommendations in RFC 2827, “Network Ingress Filtering”; however, this exercise specifically states that access lists cannot be used to solve the problem.

The simplest solution is to implement Unicast RPF (uRPF) on those interfaces of ASA2 that are likely to be targeted by attackers; namely, the dmz and outside interfaces. uRPF prevents IP address spoofing by accepting only IP packets that arrive on an interface with a source address that is routable via the interface on which the packet was received. The IP routing table is consulted to match the source address to a route and a next-hop interface. If the actual route to the source address of an IP packet is via a different interface than the one on which the packet was received, it is dropped.

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**
- Nonzero/nonnull syntax appears in **violet**

To verify whether uRPF has been correctly configured, initiate a ping using the source address of 10.50.50.4 from R4:

[Click here to view code image](#)

```
R3# ping 10.50.40.7 so lo10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.50.40.7, timeout is 2 seconds:
Packet sent with a source address of 10.50.50.4
```

When this packet reaches ASA2 on the dmz interface, the IP routing table will be consulted. The route table shows that the route to 10.50.50.0/24 is via the outside interface, not the dmz interface.

[Click here to view code image](#)

```
C 10.50.50.0 255.255.255.0 is directly connected, outside
```

If uRPF is enabled on the dmz interface (as well as the outside as another possible attack target), RPF drop counters should be incrementing.

[Click here to view code image](#)

```
ASA2# show ip verify statistics
interface outside: 0 unicast rpf drops
interface dmz: 9 unicast rpf drops
```

Configuration

ASA2

[Click here to view code image](#)

```
ip verify reverse-path int dmz
ip verify reverse-path int outside
```

Tech Notes

Understanding Unicast Reverse Path Forwarding in Cisco IOS: Technology Overview

Unicast RPF works in one of three different modes: strict mode, loose mode, or VRF mode. Note that not all network devices support all three modes of operation.

When implementing uRPF in strict mode, the packet must be received on the interface that the router would use to forward the return packet. uRPF configured in strict mode can drop legitimate traffic that is received on an interface that was not the router's choice for sending return traffic. Dropping this legitimate traffic could occur when asymmetric routing paths are present in the network.

When implementing uRPF in loose mode, the source address must appear in the routing table. Administrators can change this behavior by using the **allow-default** option, which enables the use of the default route in the source verification process. Additionally, a packet that contains a source address for which the return route points to the Null 0 interface will be dropped. An access list can also be specified that permits or denies certain source addresses in uRPF loose mode. Care must be taken when allowing the default route to factor into permitting packets because any route not explicitly mapping the source address of the incoming packet will be covered by the default route. If the **allow-default** option must be used, it should be combined with an access list to at least block RFC 1918 and bogon addresses as described in RFC 5735 (replaces RFC 3330).

Understanding Unicast Reverse Path Forwarding: Deployment Guidelines

Administrators should use uRPF in strict mode on network interfaces for which all packets received are guaranteed to originate from the subnet assigned to the interface. A subnet composed of end stations or network resources fulfills this requirement. Such a design would be in place for an access layer network or a branch office where there is only one path into and out of the branch network. No other traffic originating from the subnet is allowed, and no other routes are available past the subnet. uRPF loose mode can be used on an uplink network interface that has a default route associated with it.

uRPF is supported on the Cisco ASA in addition to Cisco IOS; however, there are some differences in configuration and behavior:

- **Cisco IOS Support:** Unicast RPF is enabled on a per-interface basis. The **ip verify unicast source reachable-via rx** command enables uRPF in strict mode. To enable loose mode, administrators can use the **any** option to enforce the requirement that the source IP address for a packet must appear in the routing table. The **allow-default** option may be used with either the **rx** or **any** option to include IP addresses not specifically contained in the routing table. The **allow-self-ping** option should not be used because it could create a denial of service condition. An access list, such as the one that follows, can also be configured to specifically permit or deny a list of addresses through uRPF:

```
interface FastEthernet 0/0
ip verify unicast source reachable-via {rx | any} [allow-default]
[allow-self-ping] [list]
```

Addresses that should never appear on a network can be dropped by entering a route to a null interface. The following command will cause all traffic received from the 10.0.0.0/8 network to be dropped even if uRPF is enabled in loose mode with the **allow-default** option: **ip route 10.0.0.0 255.0.0.0 Null0**.

- **Cisco ASA:** uRPF can be configured on the ASA Security Appliance on a per-interface basis with the following global command: **ip verify reverse-path interface *interface_name***.

Normally, the ASA looks at the destination address only when determining where to forward the packet. uRPF instructs the ASA to also look at the source address; this is why it is called reverse path forwarding.

Unicast RPF is implemented as follows:

- ICMP packets are sessionless, so each packet is checked.
- UDP and TCP have sessions, so the initial packet requires a reverse route lookup. Subsequent packets arriving during the session are checked using an existing state maintained as part of the session. Noninitial packets are checked to ensure they arrived on the same interface used by the initial packet.

Understanding Unicast Reverse Path Forwarding: Other Guidelines

Unallocated IP addresses, IP addresses for private internets as mentioned in RFC 1918, and special-use IP addresses as mentioned in RFC 3330(5735) can be a problem when they are used to route packets on the Internet. These addresses can be used to source attacks that could make it difficult or impossible to trace back to the source. Filtering these addresses at the network boundary will provide another layer of security.

Two IETF best current practices (BCP) describe methods for limiting the risk and impact to the network and infrastructure from attacks using spoofed source addresses:

- Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing (BCP38)
- Ingress Filtering for Multihomed Networks (BCP84)

Solution and Verification for Exercise 5.2: Monitor and Protect Against Wireless Intrusion Attacks

Skills Tested

- Configuring the Cisco Wireless LAN Controller (WLC) to receive the addresses of wireless clients that should be shunned under the instruction of the Cisco IPS sensor (operating as an Intrusion Detection Sensor (IDS))
- Enabling TLS service on the Cisco IPS sensor

Solution and Verification

This exercise requires the configuration of the Cisco WLC and Cisco IPS sensor. These two devices form a secure client (WLC) to server (IPS) connection using Transport Layer Security (TLS).

The Cisco Intrusion Detection System/Intrusion Prevention System (CIDS/CIPS) instructs controllers to block certain clients from accessing the wireless network when attacks involving these clients are detected at Layer 3 through Layer 7. You can configure IDS sensors to detect various types of IP-level attacks in your network. When the sensors identify an attack, they can alert the controller to shun the offending client. When you add a new IDS sensor, you register the controller with that IDS sensor so that the controller can query the sensor to get the list of shunned clients.

When an IDS sensor detects a suspicious client, it alerts the controller to shun this client.

For all verification syntax that follows:

- Required output appears in **red**
- Variable syntax appears in **green**

After TLS is enabled on the sensor, hash values derived from the TLS certification on the sensor are calculated. The SHA-1 fingerprint must be manually added to the WLC configuration; it is used to verify the validity of the sensor:

[Click here to view code image](#)

```
IPS# show tls fingerprint  
MD5: D9:DF:83:E4:00:19:68:59:04:DA:B4:CB:6D:77:73:CA  
SHA1: 35:AB:35:7C:BA:58:21:24:1D:BC:1F:3A:8A:CB:2E:06:B0:BB:3F:EE
```

Verify whether fingerprints match and the communications connection is up. The query state should be enabled and the query result should display success. Queries are sent periodically for liveliness.

[Click here to view code image](#)

```
(WLC) >show wps cids-sensor detail 1  
  
IP Address..... 192.168.2.100  
Port..... 443  
Query Interval..... 60  
Username..... wlc  
Cert Fingerprint..... SHA1:  
35:AB:35:7C:BA:58:21:24:1D:BC:1F:3A:8A:CB:2E:06:B0:BB:3F:EE  
Query State..... Enabled  
Last Query Result..... Success  
Number of Queries Sent..... 1
```

Configuration

WLC

[Click here to view code image](#)

```
config wps cids-sensor add 1 192.168.2.100 wlc 123cisco123  
config wps cids-sensor fingerprint 1 sha1 fingerprint -> taken from IPS and will
```

```
vary
config wps cids-sensor enable 1
```

IPS

```
service web-server
enable-tls true
port 443
exit
```

ASA1/c1—Must Allow HTTPS (ACL Name Can Be Anything)

[Click here to view code image](#)

```
access-list 101 permit tcp any any eq 443
access-group 101 in interface outside
```

Solution and Verification for Exercise 5.3: Identifying and Protecting Against SYN Attacks

Skills Tested

- Configuring connection limits on the Cisco ASA to protect against TCP SYN attacks
- Understanding what methods of setting connection limits are available across ASA software versions

Solution and Verification

The solution to this exercise will vary depending on the version of Cisco ASA software being used. In post-8.3 software, maximum connections can no longer be applied on NAT statements (including identity NATs). Class maps, policy maps, and service policies must be used to configure what is also known as TCP-Intercept on the Cisco ASA.

Setting embryonic and max connection limits per client on ASA1 can protect R1 from potential TCP SYN attacks. This type of DoS attack is prevented by rate limiting TCP connections and not allowing incomplete TCP handshakes to consume resources on R1.

For all verification syntax that follows:

- Required output appears in **red**
- Variable syntax appears in **green**

Verify by checking that the **embryonic-conn-max** and **per-client-max** are set on a sample flow from ANY host to the web server 10.50.100.1 on *both* TCP 80 and 443 ports:

[Click here to view code image](#)

```
ASA1/c2# show service-policy flow tcp host 0.0.0.0 host
10.50.100.1 eq 80
```

Global policy:

```
Service-policy: global_policy
Class-map: protectCA Server
```

Match: access-list **CAServer**

Access rule: permit tcp any host 10.50.100.1 eq www

Action:

Input flow: set connection embryonic-conn-max 100 per-client-max 5

```
ASA1/c2# show service-policy flow tcp host 0.0.0.0 host
10.50.100.1 eq 443
```

Global policy:

Service-policy: global_policy

Class-map: **protectCAServer**

Match: access-list **CAServer**

Access rule: permit tcp any host 10.50.100.1 eq https

Action:

Input flow: set connection embryonic-conn-max 100 per-client-max 5

Configuration

ASA1/c2

[Click here to view code image](#)

```
access-list CAServer extended permit tcp any host 10.50.100.1 eq www
access-list CAServer extended permit tcp any host 10.50.100.1 eq https
<...>
class-map protectCAServer
 match access-list CAServer
<...>
policy-map global_policy
<...>
class protectCAServer
 set connection embryonic-conn-max 100 per-client-max 5
!
service-policy global_policy global
```

Tech Notes

Configuring Maximum Connections

In pre version-8.3, connection limits can be set on service policy flows or using a NAT translation. The following example shows how to migrate a pre-8.3–based configuration to a post-8.3 command format:

[Click here to view code image](#)

```
! Old Configuration
static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 tcp 10
 20 norandomseq nailed
! Migrated Configuration
```

```
access-list acl-conn-param-tcp-01 extended permit tcp host 192.168.100.10 any
```

```
class-map class-conn-param-tcp-01  
match access-list acl-conn-param-tcp-01
```

```
policy-map policy-conn-param-inside  
class class-conn-param-tcp-01  
set connection per-client-max 10 per-client-embryonic-max 20  
random-sequence-number disable  
set connection advanced-options tcp-state-bypass
```

```
service-policy policy-conn-param-inside interface inside
```

TCP Intercept and Limiting Embryonic Connections

Limiting the number of embryonic connections protects a device from a potential DoS attack. The ASA uses the per-client limits and the embryonic connection limit to trigger TCP Intercept, which protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. An *embryonic connection* is a connection request that has not finished the necessary three-way handshake between source and destination. TCP Intercept uses the SYN cookies algorithm to prevent TCP SYN-flooding attacks. A SYN-flooding attack consists of a series of SYN packets usually originating from spoofed IP addresses. The constant flood of SYN packets keeps the server SYN queue full, which prevents it from servicing connection requests. When the embryonic connection threshold of a connection is crossed, the ASA acts as a proxy for the server and generates a SYN-ACK response to the client SYN request. When the ASA receives an ACK back from the client, it can then authenticate the client and allow the connection to the server.

Solution and Verification for Exercise 5.4: Using NBAR for Inspection of HTTP Traffic with PAM and Flexible NetFlow

Skills Tested

- Configuring NBAR for application inspection
- Interpreting Cisco IOS debug output for the purpose of identifying NBAR policy parameters
- Configuring basic PKI trustpoints on a Cisco IOS Router
- Understanding PAM in Cisco IOS
- Configuring NetFlow v9 to track NBAR classification

Solution and Verification

Network-Based Application Recognition (NBAR) is a classification engine that recognizes many protocols and applications, allowing for the enforcement of packet-handling policies at the application level. HTTP traffic can be deep packet inspected, classifying packets by URL, host, or Multipurpose Internet Mail Extension (MIME) type or a combination of these options.

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**
- Nonzero/nonnull syntax appears in **violet**
- Variable syntax appears in **green**

From the **crypto pki** debug output, three HTTP fields were identified as the NBAR match criteria; all fields must match, requiring a **match-all** policy:

[Click here to view code image](#)

Host: 10.50.100.1

Server: cisco-IOS

Content-Type: application/x-x509-ca-cert

These must be included in the class map definition. The class map identifies interesting traffic that is to be policed to ensure bandwidth on R1 is not consumed by any potential attack on R1. The policy map will apply actions to the HTTP fields of interest; in this case, a QoS policy.

SCEP traffic uses TCP/80 as its transport; however, this port should be mapped to TCP/8080. End entities must use this port (defined in the PKI trustpoint URL) for SCEP communications. This port-to-application mapping (PAM) is only one configuration task required to facilitate TCP/8080. The Cisco IOS HTTP server must be running on the CA server and accepting requests on TCP/8080. Additionally, there must be access to R1 through ASA/c2 on TCP/8080.

The final requirement of this exercise is to enable Flexible NetFlow to provide a breakdown of the devices accessing R1. The NetFlow record must contain the following fields:

IPV4 SOURCE ADDRESS

IPV4 DESTINATION ADDRESS

TRNS SOURCE PORT

TRNS DESTINATION PORT

IP PROTOCOL

APPLICATION NAME

interface input

interface output

counter bytes long

counter packets long

ip fragmentation flags

Capitalized fields must be included in the record and are defined by “match” entries. Noncapitalized fields should be included if data is available and are defined by “collect” entries.

This record is then applied to a NetFlow flow monitor along with the requirement to set the **cache inactive timeout** to 60. The record field application name is used to reference the NBAR applications defined on the router; in this case, HTTP.

NetFlow statistics can be exported to an external NetFlow collector; however, in this case, the internal cache will be used to verify the NetFlow configuration.

Verify the configuration of the HTTP server on R1. End entities will be sending SCEP transactions to TCP/8080 and the HTTP server must be enabled and running on this port.

[Click here to view code image](#)

```
R1# show ip http server status
```

```
HTTP server status: Enabled
```

```
HTTP server port: 8080
```

The PAM mapping can be verified as follows:

[Click here to view code image](#)

```
R1# show ip port-map http detail
```

```
IP port-map entry for application 'http':
```

```
tcp 80          Hypertext Transfer Protocol  system defined
```

```
tcp 8080        user defined
```

Access to the CA server on R1 must not be blocked by the ASA. Verify whether TCP/8080 traffic is allowed through ASA1/c2:

[Click here to view code image](#)

```
ASA1/c2# show access-list
```

```
access-list 101 line 15 extended permit tcp any host 10.50.100.1 eq 8080
```

In [Exercise 5.3](#), a policy was configured on ASA1/c2 that limited connections destined to the CA server. This policy must be updated to enforce max connections on TCP/8080; otherwise, SYN attack protection will not be afforded to connections using TCP/8080:

[Click here to view code image](#)

```
ASA1/c2# show service-policy flow tcp host 0.0.0.0 host  
10.50.100.1 eq 8080
```

Global policy:

```
Service-policy: global_policy
```

```
Class-map: protectCAServer
```

```
Match: access-list CAServer
```

```
Access rule: permit tcp any host 10.50.100.1 eq 8080
```

```
Action:
```

```
Input flow: set connection embryonic-conn-max 100 per-client-max 5
```

```
Class-map: class-default
```

```
Match: any
```

```
Action:
```

```
Output flow:
```

Now that access to the CA server is verified, the **crypto pki auth cisco** command should succeed:

[Click here to view code image](#)

```
R6(config)# crypto pki auth cisco
```

```
Certificate has the following attributes:
```

```
Fingerprint MD5: 1F5A02E4 C2C8230A 56FC15BB CBDFBEF6
```

```
Fingerprint SHA1: 99D5D0AA 928B4DD8 7D9E6D98 B3831F1D 796C6A71
```

% Do you accept this certificate? [yes/no]: no

Verify the R1 NBAR configuration by checking for increasing packet counts on the required match criteria in both directions on Ethernet0/0:

[Click here to view code image](#)

```
R1# show policy-map int e0/0  
Ethernet0/0
```

Service-policy **input**: scep

Class-map: scep (match-all)

8 packets, 480 bytes

5 minute offered rate 0 bps, drop rate 0 bps

Match: protocol http mime "application/x-x509-ca-cert"

Match: protocol http server "cisco-IOS"

Match: protocol http host "10.50.100.1"

police:

cir 10000 bps, bc 1500 bytes

conformed 4 packets, 240 bytes; actions:

transmit

exceeded 0 packets, 0 bytes; actions:

drop

conformed 0000 bps, exceeded 0000 bps

Class-map: class-default (match-any)

487 packets, 106808 bytes

5 minute offered rate 0 bps, drop rate 0 bps

Match: any

Service-policy **output**: scep

Class-map: scep (match-all)

21 packets, 7960 bytes

5 minute offered rate 0 bps, drop rate 0 bps

Match: protocol http mime "application/x-x509-ca-cert"

Match: protocol http server "cisco-IOS"

Match: protocol http host "10.50.100.1"

police:

cir 10000 bps, bc 1500 bytes

conformed 6 packets, 2042 bytes; actions:

transmit

exceeded 0 packets, 0 bytes; actions:

drop

conformed 0000 bps, exceeded 0000 bps

Class-map: class-default (match-any)
520675 packets, 50074219 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: any

Verify the Flexible NetFlow configuration as follows:

[Click here to view code image](#)

```
R1# show flow monitor name SCEP cache format record
```

```
Cache type:          Normal
Cache size:          4096
Current entries:     7
High Watermark:     7

Flows added:         93
Flows aged:          86
- Active timeout    ( 1800 secs)    0
- Inactive timeout  (   60 secs)    86
- Event aged                0
- Watermark aged           0
- Emergency aged           0
```

```
IPV4 SOURCE ADDRESS: 10.50.80.6
IPV4 DESTINATION ADDRESS: 10.50.100.1
TRNS SOURCE PORT: 19689
TRNS DESTINATION PORT: 8080
IP PROTOCOL: 6
APPLICATION NAME: port http
interface input: Et0/0
interface output: Null
counter flows: 1
counter bytes long: 273
counter packets long: 3
ip fragmentation flags: 0x00
```

Configuration

R1

[Click here to view code image](#)

```
flow record SCEP
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
```

```
match application name
collect ipv4 fragmentation flags
collect interface input
collect interface output
collect counter bytes long
collect counter packets long
!
!
```

```
flow monitor SCEP
cache timeout inactive 60
record SCEP
```

```
ip port-map http port tcp 8080
```

```
ip http server
ip http port 8080
```

```
class-map match-all scep
match protocol http mime "application/x-x509-ca-cert"
match protocol http server "cisco-IOS"
match protocol http host "10.50.100.1"
```

```
policy-map scep
class scep
police 10000 conform-action transmit exceed-action drop
interface Ethernet0/0
service-policy output scep
service-policy input scep
ip flow monitor SCEP input
```

R6

[Click here to view code image](#)

```
crypto key gen rsa
crypto pki trustpoint ciscoca
enrollment url http://10.50.100.1:8080
```

ASA1/c2

[Click here to view code image](#)

```
access-list 101 extended permit tcp any host 10.50.100.1 eq 8080
access-list CAServer extended permit tcp any host 10.50.100.1 eq 8080
```

Tech Notes

Configuring a NetFlow Exporter

In this exercise, we collected NetFlow statistics and cached them making them viewable from the CLI. In practice, NetFlow information should be collected and exported to a flow collector, reducing the resources consumed by the service on the Cisco IOS device.

The following configuration outlines how to configure a flow exporter and apply it to a flow monitor:

[Click here to view code image](#)

```
flow exporter export-to-scrutinizer*  
destination 192.168.2.25  
source Ethernet0/0  
transport udp 2055  
template data timeout 60  
  
flow monitor SCEP  
record SCEP  
exporter export-to-scrutinizer*  
cache timeout active 60
```

Note

*Scrutinizer is a Cisco certified NetFlow, IPFix, and AVC engine.

Comparing NetFlow Types

NetFlow v5 is the most popular and most basic of all four formats. It displays the classic source and destination IP addresses, source and destination ports, and the bytes count of transferred data. NetFlow v5 added BGP autonomous system information and flow sequence numbers over previous versions. One limitation of NetFlow v5 is that you can only enable ingress flow export on an interface.

NetFlow v9 is an upgrade to NetFlow v5. On top of the traditional flow record of v5, it adds support for technologies such as multicast, IPsec, and Multi-Protocol Label Switching (MPLS). These enhancements are mostly due to the support for templates, which enable the content of the flows to change based on the needs of the user. For example, due to the routers' capability to perform deep packet inspection, Layer 7 application details can be exported through the use of NBAR. Also, Voice over IP and video traffic metrics, such as jitter, packet loss, and round-trip time, can also be exported. It also added IPv6 support as well as egress flow collection. v9 is supported in Cisco IOS 12.4 and above.

IPFIX is the Cisco proposed standard for IP Flow Information eXport and was designed based on NetFlow v9. It adds support for variable-length strings, which can be used for application visibility and control (AVC) exports (for example, netflix.com, youtube.com, and facebook.com).

Flexible NetFlow is the configuration interface on the router or switch that enables the user to take advantage of NetFlow v9 and IPFIX. Flexible NetFlow (FnF) enables the user to define the elements required in the flow export. Most of the latest Cisco IOS releases support FnF, which can be used to

export NetFlow v5, v9, and IPFIX.

Migrating from Traditional Netflow to Flexible Netflow

The following configurations demonstrate NetFlow v5 and Flexible NetFlow:

[Click here to view code image](#)

! Netflow Version 5

```
interface FastEthernet 0/1
  ip flow [ingress|egress]
  exit
ip flow-export destination 192.168.9.101 9996
ip flow-export source FastEthernet 0/1
ip flow-export version 5
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
```

! Flexible NetFlow

```
flow exporter FlowExporter1
  destination 192.168.9.101
  transport udp 9996
  export-protocol netflow-v5
  source FastEthernet 0/1
flow monitor FlowMonitor1
  record netflow ipv4 original-input
  exporter FlowExporter1
  cache timeout active 1
  cache timeout inactive 15
interface FastEthernet 0/1
  ip flow monitor FlowMonitor1 [input|output]
```

Section 6: Identity Management

In this section, you configure the Cisco Identity Services Engine (ISE) and Cisco Secure Access Control Server (ACS) to support identity-based network access and device management using RADIUS and TACACS+. Device command authorization on a Cisco IOS Router is an important method for restricting device access and limiting the potential for attack or inadvertent misconfiguration. Identity-based network access is implemented using Cut-Through Proxy on the Cisco ASA triggered by HTTP traffic. Cisco TrustSec is applied on the Cisco Catalyst switch with the Cisco ISE through the use of MAC Authentication Bypass (MAB) and 802.1X authentication methods enforced on a switch port.

This section covers the Cisco TrustSec (CTS) solution. You will be working with SW1 (10.50.70.4) and SW2 (10.50.70.5) and the Cisco ISE (192.168.2.15). SW1 and SW2 are connected via interface gig1/0/23; this is used for CTS connectivity purposes only.

Solution and Verification for Exercise 6.1: Cisco TrustSec—Dynamically Assigning Secure Group Tagging and SGACLs: 802.1X and MAB

Skills Tested

- Enabling 802.1X authentication on the Cisco WLC-managed Cisco AP
- Configuring 802.1X authentication support on the Cisco ISE and Cisco Catalyst switch
- Defining SGTs and SGACLs on the Cisco ISE
- Enabling dynamic SGT assignment using authorization profiles on the Cisco ISE

Solution and Verification

Much of this exercise requires configuration on the ISE in its role as the authentication server.

The Catalyst switch is the authenticator using the Dot1X RADIUS configuration already enabled on SW2 in Lab 1. The authentication mechanism for the IP Phone is still MAB; however, the content of its authorization profile is modified to push the SGT value, which the switch logic uses to identify the IP Phone. Similarly, the Cisco AP (in the role of supplicant) will be authenticated by the ISE using the 802.1X credentials (pushed to the AP from the WLC). The AP's authorization profile includes an SGT value that is dynamically allocated at successful authorization.

The switch SW2 will use the SGTs to make forwarding decisions based on the SGT values in the security group ACLs (SGACL) that it received dynamically from the ISE. The DACLs per identity used in Lab 1 have been replaced with SGTs and SGACLs.

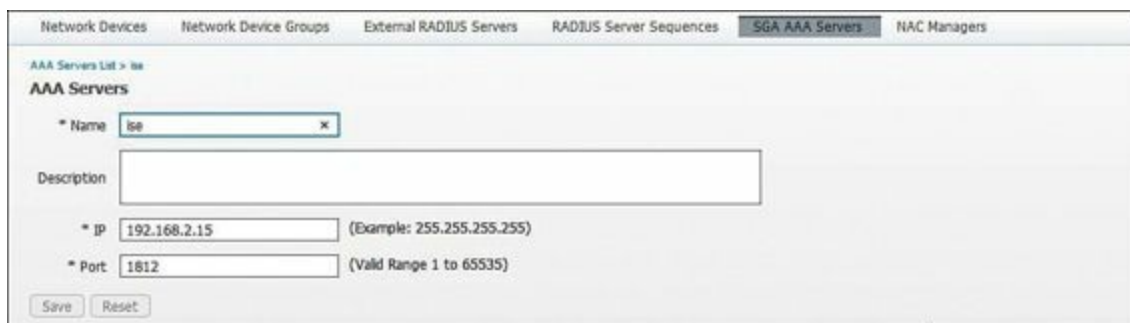
The solution to this exercise is verified by checking whether the AP and IP Phone have received their SGTs from the ISE. The SGTs and SGACLs are verified by looking at the ISE GUI. In later questions, the actual distribution and enforcement of the SGTs and SGACLs is examined.

For all verification syntax that follows:

- Required output appears in **red**
- Variable syntax appears in **green**

Part A: Configuring SGTs on the Cisco ISE

Before any Security Group Access (SGA) configuration begins on the Cisco ISE, make sure it is configured as an SGA AAA server, as shown in [Figure 2a-18](#).



The screenshot shows the Cisco ISE GUI for configuring an SGA AAA Server. The navigation tabs at the top include 'Network Devices', 'Network Device Groups', 'External RADIUS Servers', 'RADIUS Server Sequences', 'SGA AAA Servers', and 'NAC Managers'. The 'SGA AAA Servers' tab is selected. Below the navigation, there is a section titled 'AAA Servers' with a sub-section 'AAA Servers List > ise'. The configuration form includes the following fields: 'Name' (value: ise), 'Description' (empty), 'IP' (value: 192.168.2.15, with an example of 255.255.255.255), and 'Port' (value: 1812, with a valid range of 1 to 65535). There are 'Save' and 'Reset' buttons at the bottom of the form.

Figure 2a-18 ISE SGA AAA Server

Verify the security group list on the Cisco ISE. The unknown group matches all traffic that arrives

untagged and cannot be modified. The ISE will assign the actual tag values in ascending order, as shown in [Figure 2a-19](#).

Name	SGT (Dec / Hex)	Description
AP	5 / 0005	
IPPhone	4 / 0004	
NADS	2 / 0002	All NADS That Receive SGTs
Unknown	0 / 0000	Unknown Security Group
VLAN70	3 / 0003	

Figure 2a-19 ISE SGT Summary

Part B: Dynamically Assigning SGT's via 802.1X and MAB

After adding the 802.1X credentials on the WLC, verify whether the APs are still associated and the credentials are now displayed in the AP summary; the password will not be displayed.

[Click here to view code image](#)

```
(WLC) >show ap summ
```

```
Number of APs..... 2
```

```
Global AP User Name..... cisco
```

```
Global AP Dot1x User Name..... ciscoAP
```

AP Name	Slots	AP Model	Ethernet MAC	Location	Port	Country	Priority
AP1cdf.0f94.8063	2	AIR-CAP3502I-A-K9	1c:df:0f:94:80:63	default location	1		1
AP588d.0959.4921	2	AIR-LAP1262N-A-K9	58:8d:09:59:49:21	default location	1		1

The following output can be used to verify that authentication and authorization of the AP and IP Phone have been successful. The command **clear authentication session interface interface** will force reauthentication. Because traffic permissions for the phone are dictated by SGACLs, the DACLs defined in Lab 1 are not required.

[Click here to view code image](#)

```
SW2# show authentication session int g1/0/14
```

```
Interface: GigabitEthernet1/0/14
```

```
MAC Address: 0023.eb54.1109
```

```
IP Address: Unknown
```

```
User-Name: 00-23-EB-54-11-09
```

```
Status: Authz Success
```

```
Domain: VOICE
```

```
Security Policy: Should Secure
```

```
Security Status: Unsecure
```


Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: 9
SGT: 0004-0
Session timeout: 3600s (local), Remaining: 3509s
Timeout action: Reauthenticate
Idle timeout: N/A
Common Session ID: C0A842420000002E003D9546
Acct Session ID: 0x00000030
Handle: 0x3C00002F

Runnable methods list:

Method	State
mab	Authc Success
dot1x	Not run

SW2# **show auth sess int g1/0/18**

Interface: GigabitEthernet1/0/18
MAC Address: 588d.0959.4921
IP Address: Unknown
User-Name: ciscoAP
Status: Authz Success
Domain: DATA
Security Policy: Should Secure
Security Status: Unsecure
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: N/A
SGT: 0005-0
Session timeout: 3600s (local), Remaining: 3394s
Timeout action: Reauthenticate
Idle timeout: N/A
Common Session ID: 0A3209050000D66D035B9D5E
Acct Session ID: 0x0000D67F
Handle: 0xF10007B5

Runnable methods list:

Method	State
dot1x	Authc Success

The configuration of the Cisco ISE authorization outputs for the Cisco AP and Cisco IP Phone are shown in [Figure 2a-20](#).

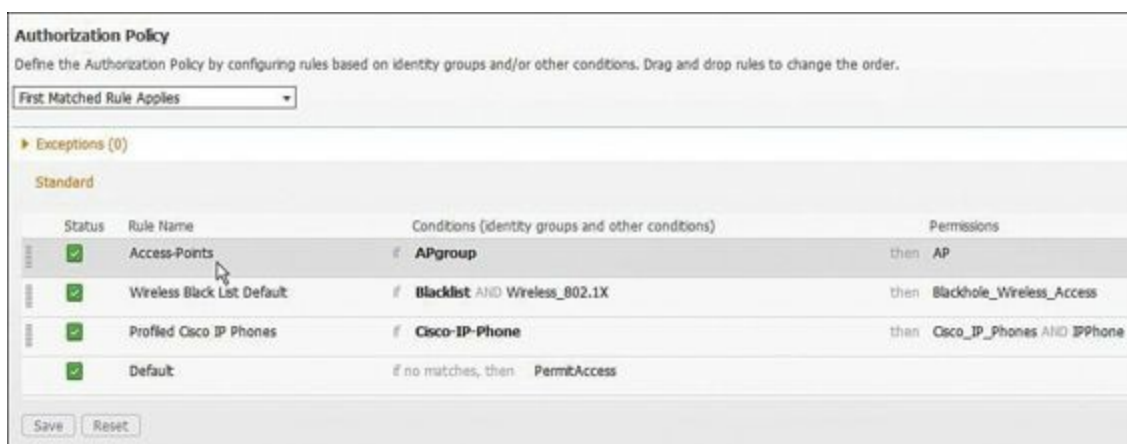


Figure 2a-20 ISE Access Point Authorization Policy

Part C: Create the SGA Egress Policy

Verify whether the SGA egress policies are correctly defined on the ISE. An egress policy will specify what traffic (based on SGACLs) can flow from the source SGT to a destination SGT.

The SGA egress policy matrix should contain two policies. Within each policy, only the protocols and services explicitly defined in the SGACLs should be permitted. All other traffic is denied. The AP and IPPhone to NET70 egress policy is shown in [Figure 2a-21](#). The content of the SGACL applied to the AP and IP Phone is shown in [Figure 2a-22](#).

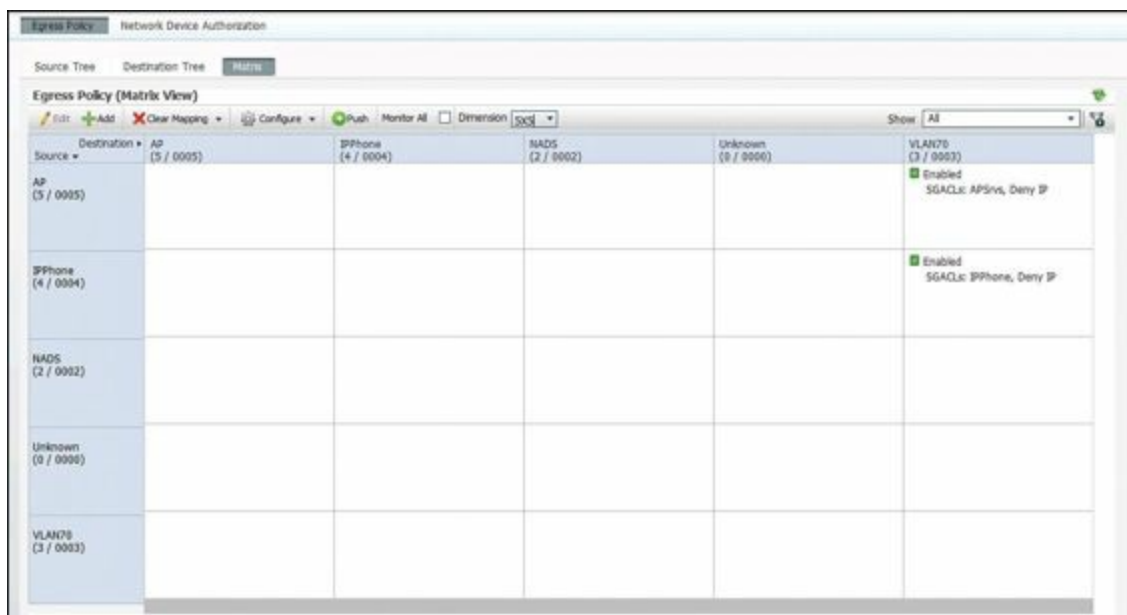


Figure 2a-21 ISE SGA Egress Policy Matrix



Figure 2a-22 ISE SGACL Rulesets for the Access Point and IP Phone

Note that we have defined access policies sourced from the IP Phone and AP switchports; policies can also be explicitly defined for traffic destined to these ports. For this particular question, return traffic will be handled by the default rule, which is permit IP any any, as shown in [Figure 2a-23](#). Changing this rule could impact all policies in the matrix. The default rule is overridden by explicitly defining inbound and outbound egress policies for each combination of source and destination SGTs.

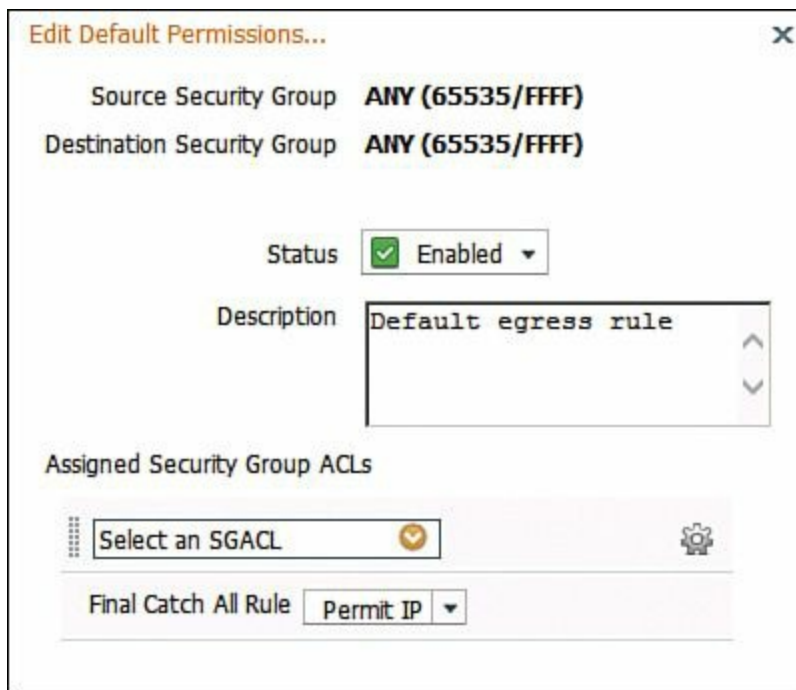


Figure 2a-23 ISE SGA Egress Policy Default Permissions

Configuration

WLC

[Click here to view code image](#)

```
config ap 802.1Xuser add username ciscoAP password CCie123 all
```

SW2

[Click here to view code image](#)

```
ip device tracking
```

```
interface GigabitEthernet1/0/14
switchport access vlan 99
switchport mode access
switchport voice vlan 9
ip device tracking maximum 2
ip access-group ACL_DEFAULT in
authentication host-mode multi-auth
authentication open
authentication order mab dot1x
authentication priority dot1x mab
authentication port-control auto
authentication periodic
mab
dot1x pae authenticator
spanning-tree portfast
```

```
interface GigabitEthernet1/0/18
switchport access vlan 77
switchport mode access
ip device tracking maximum 1
ip access-group ACL_DEFAULT in
authentication host-mode multi-auth
authentication open
authentication port-control auto
authentication periodic
dot1x pae authenticator
```

Tech Notes

IP Device Tracking

When configuring a static **cts enforcement vlan-list**, or dynamically assigning SGTs on a port, IP device tracking must be configured globally and on the port where dynamic assignment is being applied. When active hosts are detected, the switch adds the following entries to an IP device tracking table:

- IP address of host
- MAC address of host
- VLAN of the host
- The interface on which the switch detected the host
- The state of the host (Active or Inactive)

The host added to the IP device tracking table is monitored with periodic ARP probes. Hosts that fail to respond are removed from the table.

Solution and Verification for Exercise 6.2: Cisco TrustSec—NDAC and MACsec

Skills Tested

- Implementing NDAC
- Configuring seed and nonseed devices for NDAC
- Configuring MACsec between Catalyst switches using 802.1X and SAP
- Creating an NDAC authorization policy on the Cisco ISE
- Configuring the Cisco Catalyst switch for AAA/RADIUS to create a Cisco TrustSec domain

Solution and Verification

This exercise covers setting up the network to support a Cisco TrustSec (CTS) domain. In [Exercise 6.1](#), the basis for SGA was configured on the ISE, and two network devices were provisioned with SGTs. To apply and distribute TrustSec policy elements, such as SGTs and SGACLs, CTS-capable devices such as switches first must be admitted into the CTS domain. This is the purpose of Network Device Admission Control (NDAC). The first switch to be provisioned in the domain is known as the *seed device*. It must have access to the RADIUS server and will act as a relay for nonseed devices. A nonseed device does not need to have a specific configuration to locate the AAA servers to use with NDAC. Instead, the list is downloaded from the seed device. However, the nonseed device still must be added to the ISE as a TrustSec network access device. In production networks, the seed device is generally a Nexus 7k or Cat 6500; nonseed devices are access switches like the 3750-X or Cisco IOS routers like the ISR G2s and ASRs. The seed switches push SGA policy elements to the nonseed devices dynamically, eliminating the need to manually define access policies on every network device.

In this lab topology, 3750-X switches are both seed and nonseed devices. At press time, the 3k series does not support full SGA functionality; specifically, IP to SGT mappings cannot be dynamically pushed to these switches. For this reason, we are dynamically assigning SGTs at the port (see [Exercise 6.1](#)) and manually defining secure group mappings manually on the switches (see [Exercise 6.3](#)).

The other important note about this exercise is that SW1 is being configured for NDAC and, although it will receive policy from SW2, due to the layout of the lab topology, we will not be using the policy on SW1. The interface between SW1 and SW2 is solely to illustrate how to implement CTS. In a customer environment, the nonseed switches would be downstream from the seed. The connection between SW1 and SW2 for CTS is simulating a downstream relationship.

For all verification syntax that follows:

- Required output appears in **red**
- Required tasks appear in **indigo**
- Nonzero/nonnull syntax appears in **violet**

1. Configure SW1 and SW2 as network access devices on the ISE, as illustrated in [Figure 2a-24](#). Note the addresses being used on SW1 and SW2. SW2 will have a route to the ISE (192.168.2.15). SW1 does not require direct access to, or a RADIUS configuration for, the ISE because it will send requests via SW2.

Network Devices				
Edit + Add Duplicate Import Export Generate PAC Delete				
	Name	IP/Mask	Location	Type
<input type="checkbox"/>	R7	10.50.70.6/32	All Locations	All Device Types
<input type="checkbox"/>	SW1	10.50.70.4/32	All Locations	All Device Types
<input type="checkbox"/>	SW2	10.50.70.5/32	All Locations	All Device Types
<input type="checkbox"/>	WLC	10.50.100.10...	All Locations	All Device Types

Figure 2a-24 ISE Network Access Devices

2. Configure SW1 and SW2 for SGA and NDAC.

The SGA settings will enable SGT and SGACL information to be pushed to the devices. The SGA Protected Access Credential (PAC) is used to provide protected access credentials to a member of the CTS domain; without authorized credentials, devices cannot be admitted to the CTS domain. PAC file provisioning is shown in [Figure 2a-25](#). The device ID and password must match those added on the device itself using the `cts device-id` command, which is illustrated later in this solution.

Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for SGA Identification

Device Id

* Password

SGA Notifications and Updates

* Download environment data every

* Download peer authorization policy every

* Reauthentication every ⓘ

* Download SGACL lists every

Other SGA devices to trust this device

Notify this device about SGA configuration changes

Figure 2a-25 ISE SW1 CTS SGA Configuration

Note there is the ability to manually generate the PAC file on the ISE and distribute it to NDAC devices out of band. This is not required here because the PAC will automatically be distributed securely using Extensible Authentication Protocol-Flexible Authentication through Secure Tunneling (EAP-FAST).

EAP-FAST comprises three basic phases:

- a. Phase 0: The PAC is initially distributed to the client.
- b. Phase 1: Using the PAC, a secure tunnel is established.
- c. Phase 2: The client is authenticated via the secure tunnel.

[Figure 2a-26](#) shows the configuration required for provisioning the static IP-SGT mapping list from ISE to the network device. At press time, this feature was not supported on the 3750-X switch, so this figure is included for future reference.

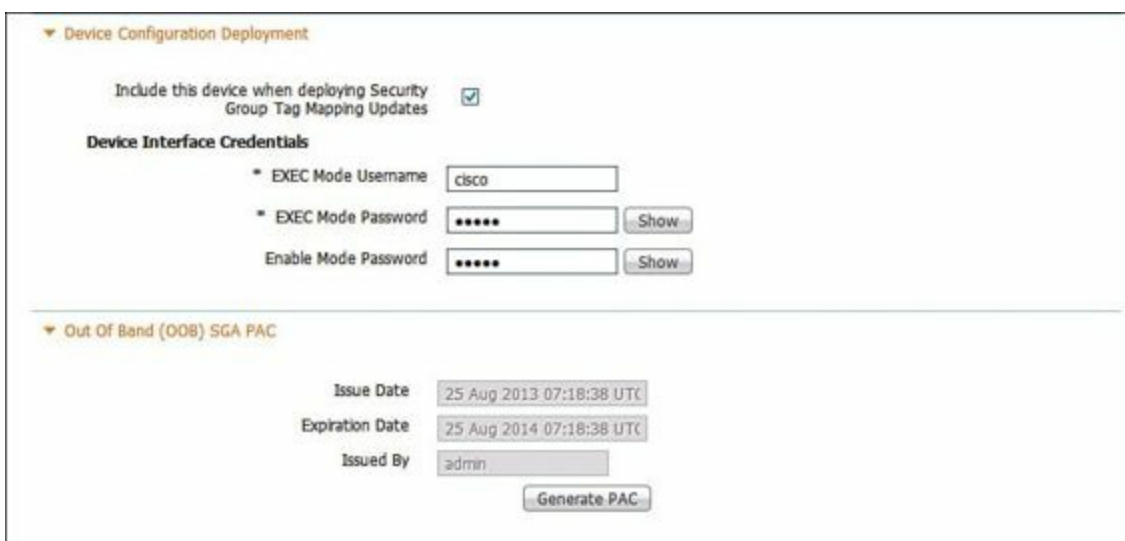


Figure 2a-26 ISE SW1 CTS IP-SGT Mapping Provisioning

3. Create a network authorization policy for the switches on the ISE, as illustrated in [Figure 2a-27](#).

SW1 and SW2 must be assigned an SGT and authorized to join the NDAC trusted domain. The switches get assigned a SGT so that packets originating from the device are tagged and can also be subject to SGACL filtering.

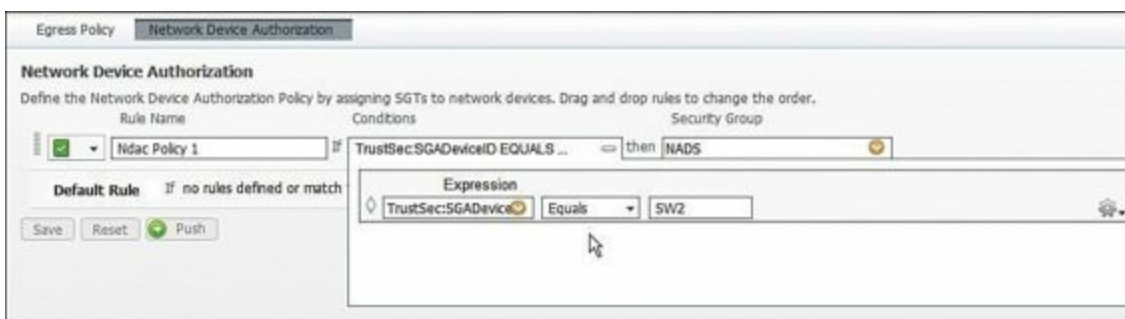


Figure 2a-27 ISE NDAC Authorization Policy

4. Prepare SW1 and SW2 to receive the PAC using AAA.

The AAA support for CTS involves using RADIUS over TLS. This “secure” RADIUS uses automatic PAC provisioning as a low overhead method to send PAC metadata and control information to clients. PAC provisioning is used with EAP-FAST to establish a TLS tunnel in which client credentials are verified.

On the seed device, ensure that RADIUS is correctly configured; both SW1 and SW2 require the AAA commands listed:

Configure AAA authentication for 802.1X using the following command:

[Click here to view code image](#)

```
aaa authentication dot1x default group radius
```

Configure AAA accounting for 802.1X using the following command:

[Click here to view code image](#)

```
aaa accounting dot1x default group radius
```

Configure AAA network authorization:

[Click here to view code image](#)

```
aaa authorization network MLIST group radius
```

SW2 as the seed also must be configured to point to the RADIUS server (ISE):

[Click here to view code image](#)

```
radius-server host 192.168.2.15 auth-port 1812 acct-port 1813 pac key  
cisco123
```

SW2 also requires

```
cts authorization list MLIST
```

On both the seed and nonseed devices, enter the **cts device id name** command and password cisco123 to immediately begin the PAC file download from the switch exec prompt (the command format can vary depending on the device platform):

[Click here to view code image](#)

```
cts device-id SW2 password cisco123  
cts device-id SW1 password cisco123
```

Verify whether SW2 has received the PAC files. SW1 has been bootstrapped to receive its credentials from the ISE; however, before this can occur, a MACsec protected and 802.1X authenticated connection must be established between SW1 and SW2 (see Step 6 that follows).

[Click here to view code image](#)

```
SW2# show cts pac  
AID: E716C410120149EFB247059C52D745D0  
PAC-Info:  
  PAC-type = Cisco Trustsec  
  AID: E716C410120149EFB247059C52D745D0  
  I-ID: SW2  
  A-ID-Info: Identity Services Engine  
  Credential Lifetime: 02:52:52 UTC Nov 24 2013  
PAC-Opaque:  
000200A80003000100040010E716C410120149EFB247059C52D745D00006008C00030100  
8EA45EE33B73000000135217589B00093A80EF958D003DD12E00CA36774CD161C3CE1  
73B45E219072916142E2332A5A84C2679B628DE62224AB8E4F6449074773E914E0B5F4  
D0D7544E74AF085E6D35F3A1BBBC2AFFD5DDC28FA0185BF67A7708F2AF0DC22B24  
Refresh timer is set for 2y34w
```

5. The supplicant SW1 receives its PAC.

When the link between the supplicant (SW1) and authenticator (SW2) comes up, the ISE will authenticate SW1 using EAP-FAST. SW1 receives a PAC from the ISE containing a shared key and an encrypted token to be used for future secure communications with the authentication server.

Verify whether SW1 has received its PAC file from the ISE:

[Click here to view code image](#)

```
SW1# show cts pac
```

```
AID: E716C410120149EFB247059C52D745D0
```

```
PAC-Info:
```

```
PAC-type = Cisco Trustsec
```

```
AID: E716C410120149EFB247059C52D745D0
```

```
I-ID: SW1
```

```
A-ID-Info: Identity Services Engine
```

```
Credential Lifetime: 22:03:34 UTC Nov 24 2013
```

```
PAC-Opaque:
```

```
000200A80003000100040010E716C410120149EFB247059C52D745D00006008C00030100
```

```
558F6023ABC6000000135217589B00093A80EF958D003DD12E00CA36774CD161C3CE4
```

```
91BFBA8759EAE57250386392FDE86B896EBEF0CB68713C84E178D962F6C77A484E58
```

```
1D528B10D7598C1428E458CD1D87530F390D46D749C05E1A2C1D95024BDC2BB35D1
```

```
Refresh timer is set for 2y34w
```

6. Verify the secured connection between SW1 and SW2.

Based on the identity of the authenticated device, in this case SW2, the ISE can provide authorization policies to each of the devices linked to SW2. The ISE provides the identity of each peer to the other, and each peer then applies the appropriate policy for the link. Verify whether each switch has been authenticated using DOT1X. Also, check whether SGTs have been assigned. When both sides of the link support encryption, Security Association Protocol (SAP) is used to negotiate policy parameters to establish a secure connection between the authenticator (SW2) and the supplicant (SW1).

[Click here to view code image](#)

```
SW2# show cts interface
```

```
Global Dot1x feature is Enabled
```

```
Interface GigabitEthernet1/0/23:
```

```
CTS is enabled, mode: DOT1X
```

```
IFC state: OPEN
```

```
Authentication Status: SUCCEEDED
```

```
Peer identity: "SW1"
```

```
Peer's advertised capabilities: "sap"
```

```
802.1X role: Authenticator
```

```
Reauth period configured: 240 (locally configured)
```

```
Reauth period per policy: 86400 (server configured)
```

```
Reauth period applied to link: 86400 (server configured)
```

```
Reauth starts in approx. 0:23:54:45 (dd:hr:mm:sec)
```

```
Authorization Status: SUCCEEDED
```

```
Peer SGT: 2:NADS
```

```
Peer SGT assignment: Trusted
```

```
SAP Status: SUCCEEDED
```

```
Version: 2
```

```
Configured pairwise ciphers:
```

gcm-encrypt
null
no-encap

Replay protection: enabled
Replay protection mode: STRICT

Selected cipher: gcm-encrypt

Propagate SGT: Enabled

Cache Info:

Cache applied to link : NONE

Statistics:

authc success:	17
authc reject:	1
authc failure:	1
authc no response:	0
authc logoff:	0
sap success:	17
sap fail:	0
authz success:	3
authz fail:	1
port auth fail:	0

L3 IPM: disabled.

Dot1x Info for GigabitEthernet1/0/23

PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30

SW1# **show cts interface**

Global Dot1x feature is Enabled

Interface GigabitEthernet1/0/23:

CTS is enabled, mode: DOT1X

IFC state: OPEN

Authentication Status: SUCCEEDED

Peer identity: "SW2"

Peer's advertised capabilities: "sap"

802.1X role: Supplicant

Reauth period applied to link: Not applicable to Supplicant role

Authorization Status: SUCCEEDED

Peer SGT: 2:NADS

Peer SGT assignment: Trusted

SAP Status: SUCCEEDED

Version: 2

Configured pairwise ciphers:

gcm-encrypt

null

no-encap

Replay protection: enabled

Replay protection mode: STRICT

Selected cipher: gcm-encrypt

Propagate SGT: Enabled

Cache Info:

Cache applied to link : NONE

Statistics:

authc success: 1

authc reject: 1

authc failure: 1

authc no response: 0

authc logoff: 0

sap success: 1

sap fail: 0

authz success: 4

authz fail: 0

port auth fail: 0

L3 IPM: disabled.

Dot1x Info for GigabitEthernet1/0/23

PAE = SUPPLICANT

StartPeriod = 30

AuthPeriod = 30

HeldPeriod = 60

MaxStart = 3

Credentials profile = CTS-ID-profile

EAP profile = CTS-EAP-profile

SGA policies are propagated over the secure link, protected by MACsec. Verify

counters are incrementing.

SW1# **show cts macsec counters int g1/0/23**

CTS Security Statistic Counters:

rxL2UntaggedPkts = 0
rxL2NotagPkts = 23
rxL2SCMissPkts = 0
rxL2CTRLPkts = 0
rxL3CTRLPkts = 0
rxL3UnknownSAPkts = 0
rxL2BadTagPkts = 0
txL2UntaggedPkts = 0
txL2CtrlPkts = 0
txL3CtrlPkts = 0
txL3UnknownSA = 0

SA Index : 0

rxL2ReplayfailPkts = 0
rxL2AuthfailPkts = 0
rxL2PktsOK = 3220
rxL3AuthCheckFail = 0
rxL3ReplayCheckFail = 0
rxL2SAMissPkts = 23
rxL3EspGcm_Pkts = 0
rxL3InverseCheckfail = 0
txL3Protected = 0

SW2# **show cts macsec counters interface g1/0/23**

CTS Security Statistic Counters:

rxL2UntaggedPkts = 0
rxL2NotagPkts = 186
rxL2SCMissPkts = 0
rxL2CTRLPkts = 0
rxL3CTRLPkts = 0
rxL3UnknownSAPkts = 0
rxL2BadTagPkts = 0
txL2UntaggedPkts = 0
txL2CtrlPkts = 0
txL3CtrlPkts = 0
txL3UnknownSA = 0

SA Index : 0

rxL2ReplayfailPkts = 0
rxL2AuthfailPkts = 0
rxL2PktsOK = 4367
rxL3AuthCheckFail = 0

```
rxL3ReplayCheckFail = 0
  rxL2SAMissPkts = 186
  rxL3EspGcm_Pkts = 0
rxL3InverseCheckfail = 0
  txL3Protected = 0
  txL2Protected = 2816
```

To verify whether both SW1 and SW2 have been authorized into the CTS domain, and also to verify the policies created on the ISE in [Exercise 6.1](#) part [A](#) and [C](#), the environment-data output should display the SGT list:

[Click here to view code image](#)

```
SW2# show cts environment-data
```

```
CTS Environment Data
```

```
=====
Current state = COMPLETE
```

```
Last status = Successful
```

```
Local Device SGT:
```

```
  SGT tag = 2-00:NADS
```

```
Server List Info:
```

```
Installed list: CTSServerList1-0001, 1 server(s):
```

```
*Server: 192.168.2.15, port 1812, A-ID E716C410120149EFB247059C52D745D0
```

```
  Status = ALIVE
```

```
    auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime
    = 20 secs
```

```
Security Group Name Table:
```

```
  0-00:Unknown
```

```
  2-00:NADS
```

```
  3-00:NET70
```

```
  4-00:IPPhone
```

```
  5-00:AP
```

```
Environment Data Lifetime = 120 secs
```

The cat3k does not support the downloading of the IP to SGT mapping table (other switches, such as the Nexus 7k and Cat 6k, can dynamically receive this table from the ISE). To provide the mapping table to the 3750-X, the IP-SGT bindings are created using a combination of manual configured mappings and mappings learned via SGT assignment during device authentication and the IP tracking mechanism. The mapping table can then be verified as follows:

[Click here to view code image](#)

```
SW2# show cts role-based sgt all
```

```
Active IP-SGT Bindings Information
```

```
IP Address      SGT   Source
=====
10.50.9.5       2     INTERNAL
```

10.50.9.6	4	LOCAL
10.50.40.7	7	VLAN
10.50.50.5	2	INTERNAL
10.50.70.4	3	VLAN
10.50.70.5	2	INTERNAL
10.50.70.6	3	VLAN
10.50.77.5	2	INTERNAL
10.50.77.8	5	LOCAL
10.50.99.5	2	INTERNAL

The SGT source values in the output list are defined as follows:

- **INTERNAL:** Any IP address on the switch receives the same SGT assigned to the switch by the NDAC authorization policy.
- **LOCAL:** SGTs assigned to devices via port authorization, such as 802.1X and MAB, are mapped to the IP addresses of those devices. If a device disconnects from the switchport, this change in state must be reflected in the IP-SGT binding table; this required IP device tracking is enabled on those ports.
- **VLAN:** These bindings are created as a result of the **cts enforcement** command with the **vlan-list** option. IP device tracking monitors information, such as IP addresses, of devices seen on each VLAN in the list. This ensures the IP-SGT bindings are dynamically maintained.
- **CLI:** Manually defined static device bindings.
- **SXP:** Bindings learned from an SXP speaker peer.

Finally, SGACL information downloaded from the ISE (as defined in [Part C](#) of [Exercise 6.1](#) in this lab) can be inspected on SW2. Note that the default permission of **permit ip** as shown in [Figure 2a-23](#) has also been downloaded.

[Click here to view code image](#)

```
SW2# show cts role-based permission
```

```
IPv4 Role-based permissions default:
```

```
Permit IP-00
```

```
IPv4 Role-based permissions from group 4:IPPhone to group 3:NET70:
```

```
IPPhone-30
```

```
Deny IP-00
```

```
IPv4 Role-based permissions from group 5:AP to group 3:NET70:
```

```
APSrvs-40
```

```
Deny IP-00
```

```
SW2# show access-list
```

```
Role-based IP access list APSrvs-40 (downloaded)
```

```
10 permit icmp
```

```
20 permit udp dst eq 5246
```

```
30 permit udp dst eq 5247
```

```
Role-based IP access list Deny IP-00 (downloaded)
```

```
10 deny ip
```

Role-based IP access list IPPhone-30 (downloaded)

```
10 permit tcp dst eq 2000
20 permit tcp dst eq www
30 permit udp dst eq bootps
40 permit udp dst eq domain
50 permit tcp src eq www
60 permit icmp
70 permit udp dst eq tftp
```

Role-based IP access list Permit IP-00 (downloaded)

```
10 permit ip
```

To verify SGACL enforcement on the switchports, check for incrementing counters:

[Click here to view code image](#)

```
SW2# show cts role-based counters
```

```
Role-based IPv4 counters
```

```
# '-' in hardware counters field indicates sharing among cells with identical policies
```

From	To	SW-Denied	HW-Denied	SW-Permitted	HW-Permitted
4	3	0	107	0	71
5	3	0	0	0	40
*	*	0	0	8595	14282

Configuration

SW1

[Click here to view code image](#)

```
aaa authentication dot1x default group radius
aaa authorization network MLIST group radius
!
!
dot1x system-auth-control
```

```
interface GigabitEthernet1/0/23
switchport trunk encapsulation dot1q
switchport mode trunk
cts dot1x
sap mode-list gcm-encrypt null no-encap
radius-server vsa send authentication
```

SW2

[Click here to view code image](#)

```
aaa authentication dot1x default group radius
```

```
aaa authorization network MLIST group radius
aaa accounting dot1x default start-stop group radius
```

```
dot1x system-auth-control
aaa server radius dynamic-author
client 192.168.2.15
server-key cisco123
```

```
cts authorization list MLIST
cts role-based enforcement
cts role-based enforcement vlan-list 9,70,77
```

```
interface GigabitEthernet1/0/23
switchport trunk encapsulation dot1q
switchport mode trunk
cts dot1x
sap mode-list gcm-encrypt null no-encap
```

```
radius-server attribute 44 include-in-access-req default-vrf
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server dead-criteria time 10 tries 5
radius-server host 192.168.2.15 auth-port 1812 acct-port 1813 pac key cisco123
radius-server vsa send accounting
radius-server vsa send authentication
```

Tech Notes

Protected Access Credential

The PAC is a unique shared credential used to mutually authenticate client and server. It is associated with a specific client username and a server A-ID. A PAC removes the need for Public Key Infrastructure (PKI) and digital certificates.

Creating a PAC consists of the following steps:

1. Server A-ID maintains a local key (master key) that is known only by the server.
2. When a client identity (I-ID) requests a PAC from the server, the server generates a randomly unique PAC key and PAC-Opaque field for this client.
3. The PAC-Opaque field contains the randomly generated PAC key along with other information, such as user identity and key lifetime.
4. PAC Key, I-ID, and Lifetime in the PAC-Opaque field are encrypted with the master key.
5. A PAC-Info field that contains the A-ID is created.
6. The PAC is distributed or imported to the client automatically or manually.

MACsec Overview

MACsec provides Layer 2 encryption on the LAN. It also encapsulates and protects the metadata field that carries the SGT.

Currently, two keying mechanisms are available: Security Association Protocol (SAP) and MAC Security Key Agreement (MKA). SAP is a proprietary Cisco keying protocol used between Cisco switches. MKA is an industry standard and is currently used between endpoints and Cisco switches. Both use 128-bit AES-GCM (Galois/Counter Mode) symmetric encryption, and provide replay attack protection of every frame.

Downlink MACsec

Downlink MACsec describes the encrypted link between an endpoint and the switch. The encryption between the endpoint and the switch is handled by the MKA keying protocol. This requires a MACsec-capable switch and a MACsec-capable supplicant on the endpoint (such as the Cisco AnyConnect Network Access Manager). The encryption on the endpoint can be handled in hardware (if the endpoint possesses the correct hardware) or in software using the main CPU for the encryption and decryption.

To configure the switch for Downlink MACsec, enter the following:

[Click here to view code image](#)

```
interface X
switchport access vlan 10
switchport mode access
switchport voice vlan 99
ip access-group ACL-ALLOW in
authentication event fail action next-method
authentication event server dead action authorize vlan 2274
authentication event server alive action reinitialize
authentication event linksec fail action next-method
authentication host-mode multi-domain
authentication open
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication violation restrict
macsec mka default-policy
mab
dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast
end
```

Uplink MACsec

Uplink MACsec is the term used to describe encrypting the link between the switches with 802.1AE. At the time this guide was written, the switch-to-switch encryption uses Cisco's proprietary SAP instead of MKA, which is used with the Downlink MACsec. The encryption is still the same AES-GCM-128 encryption used with both Uplink and Downlink MACsec.

Uplink MACsec can be achieved manually or dynamically. Dynamic MACsec requires 802.1X between the switches and is covered in this question.

Manual configuration will encrypt the interswitch links without requiring the entire domain of trust, the way that NDAC does. It also removes the dependency on ISE for the link keying, similar to how an IPsec tunnel can be built using preshared keys.

To configuring the switch for Manual Uplink MACsec, enter the following:

[Click here to view code image](#)

```
interface TenGigabitEthernet1/1/1
description Cat6K Ten1/5
no switchport
ip address 10.1.48.2 255.255.255.252
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP
load-interval 60
cts manual
policy static sgt 2 trusted
sap pmk 0000000000000000000000000000000000000000000000000000000000000000000026
mode-list
gcm-encrypt
```

MACsec Sequence in an NDAC Domain

When the link between a supplicant and an authenticator first comes up, the following sequence of events typically occurs:

- 1. Authentication:** Using NDAC, ISE authenticates a device using EAP-FAST before allowing it to join the network. During the EAP-FAST exchange, ISE creates and sends a unique PAC to the supplicant switch (the switch attempting to join the NDAC domain). That PAC contains a shared key and an encrypted token to be used for future secure communications with the authentication server.
- 2. Authorization:** Based on the identity information of the supplicant switch, ISE provides authorization policies to each of the linked peers. The authentication server provides the identity of each peer to the other, and each peer then applies the appropriate policy for the link.
- 3. Security Association Protocol (SAP) negotiation:** When both sides of a link support encryption, the supplicant and the authenticator negotiate the necessary parameters to establish a security association (SA) and encrypt the traffic.

When all three steps are complete, the authenticator changes the state of the link from the unauthorized (blocking) state to the authorized state, and the supplicant switch becomes a member of the NDAC trusted domain.

Solution and Verification for Exercise 6.3: Cisco TrustSec—SGT Exchange Protocol over TCP

Skills Tested

- Manual definition of SGTs per host and per VLAN on the Cisco Catalyst switch
- Configuring Secure Group Tag Exchange Protocol over TCP (SXP) on switches and Cisco IOS routers
- Enabling SXP on the Cisco WLC

Solution and Verification

SXP connections are required to forward SGT to IP address bindings to devices that do not use NDAC to join the CTS domain and do not support native SGT tagging. SXP is a peering protocol that uses TCP as its transport. Peers form a relationship in which one takes the role of the speaker and pushes bindings to the listener peer. The listener can then use the binding information in its own policies. For example, when an SXP connection is established between SW2 and R6, the zone-based firewall configuration in [Exercise 1.5](#) can be completed. SXP connections can be formed between adjacent (next hop) peers, or the TCP-transported information can be routed to other devices.

In [Exercise 6.2](#), the IP-SGT table on SW2 comprised different binding types: VLAN, LOCAL, and INTERNAL. This exercise requires CLI bindings to be created on SW2. These are manually defined static bindings that, along with the other binding types, can be distributed to SXP peers listening to SW2.

For all verification syntax that follows:

- Required output appears in **red**

Verify whether SW2 is the designated speaker for the SXP connections between the WLC, SW1, and R6.

Options are available for a default password and default source IP address. If a password is set, it must match the password configured on the peer device.

[Click here to view code image](#)

```
SW2# show cts sxp connection
```

```
SXP           : Enabled
```

```
Highest Version Supported: 3
```

```
Default Password : Not Set
```

```
Default Source IP: Not Set
```

```
Connection retry open period: 120 secs
```

```
Reconcile period: 120 secs
```

```
Retry open timer is not running
```

```
-----  
Peer IP       : 10.50.70.4
```

```
Source IP     : 10.50.70.5
```

```
Conn status   : On
```

```
Conn version  : 3
```

```
Local mode    : SXP Speaker
```

```
Connection inst# : 1
TCP conn fd      : 2
TCP conn password: none
Duration since last state change: 1:15:43:12 (dd:hr:mm:sec)
```

```
-----
Peer IP         : 10.50.70.6
Source IP       : 10.50.70.5
Conn status     : On
Conn version    : 2
Local mode     : SXP Speaker
Connection inst# : 1
TCP conn fd     : 1
TCP conn password: none
Duration since last state change: 911:12:20:18 (dd:hr:mm:sec)
```

Total num of SXP Connections = 2

Devices SW1 and R6 are listeners receiving IP-SGT binding from SW2. Additional bindings may be configured on SW1 and R6; however, they will not be propagated to SW2. If SW1 and R6 take the role of an SXP speaker, binding can be propagated to a listener. In addition, R6 is listening to the WLC, which can propagate bindings for wireless clients as they are authorized.

[Click here to view code image](#)

```
SW1# show cts sxp connection
```

```
SXP           : Enabled
Highest Version Supported: 3
Default Password : Not Set
Default Source IP: 10.50.70.4
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
```

```
-----
Peer IP         : 10.50.70.5
Source IP       : 10.50.70.4
Conn status     : On
Conn version    : 3
Local mode     : SXP Listener
Connection inst# : 1
TCP conn fd     : 1
TCP conn password: none
Duration since last state change: 1:15:42:01 (dd:hr:mm:sec)
```

Total num of SXP Connections = 1

```
R6# show cts sxp connection
```

```
SXP           : Enabled
```

```
Default Password : Set
```

```
Default Source IP: Not Set
```

```
Connection retry open period: 120 secs
```

```
Reconcile period: 120 secs
```

```
Retry open timer is not running
```

```
-----  
Peer IP       : 10.50.70.5
```

```
Source IP     : 10.50.70.6
```

```
Conn status   : On
```

```
Conn version  : 2
```

```
Local mode    : SXP Listener
```

```
Connection inst# : 2
```

```
TCP conn fd   : 1
```

```
TCP conn password: none
```

```
Duration since last state change: 1:22:48:33 (dd:hr:mm:sec)
```

```
-----  
Peer IP       : 10.50.100.10
```

```
Source IP     : 10.50.80.6
```

```
Conn status   : On
```

```
Conn version  : 2
```

```
Local mode    : SXP Listener
```

```
Connection inst# : 1
```

```
TCP conn fd   : 2
```

```
TCP conn password: default SXP password
```

```
Duration since last state change: 0:00:10:14 (dd:hr:mm:sec)
```

```
Total num of SXP Connections = 2
```

The WLC can only take on the role as an SXP speaker, as shown in [Figure 2a-28](#).

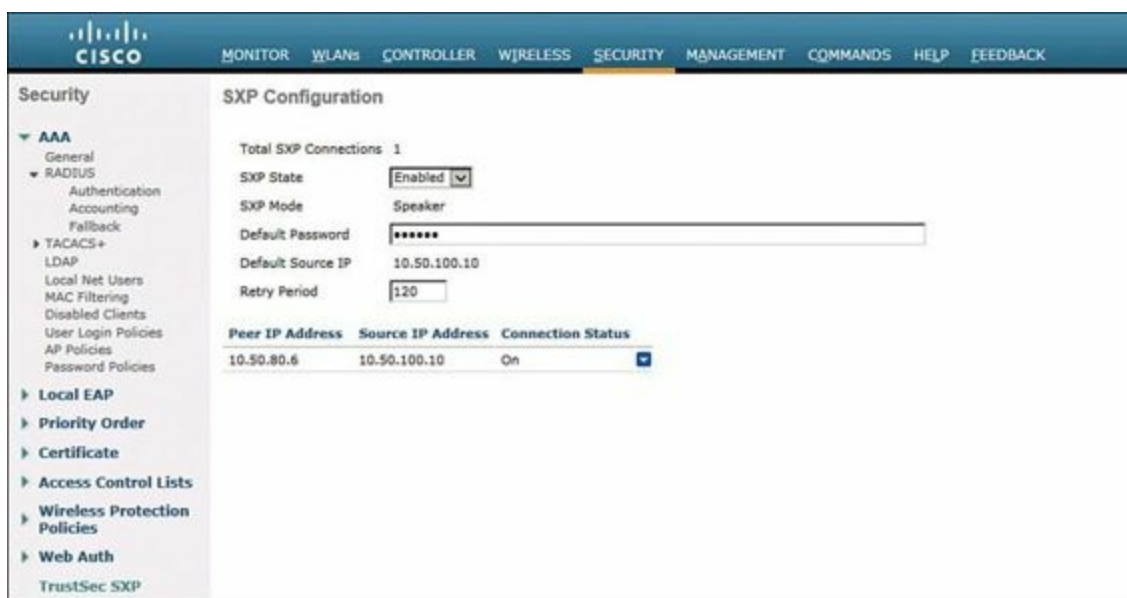


Figure 2a-28 WLC SXP Configuration

SXP status on the WLC is also displayed using the CLI.

[Click here to view code image](#)

```
(WLC) >show cts sxp connections
Total num of SXP Connections..... 1
SXP State..... Enable
Peer IP      Source IP      Connection Status
-----
10.50.80.6   10.50.100.10   On
```

The status of the SXP connections has been verified as enabled. The last task in this exercise required the definition of manual static entries on SW2. Check that all entries outlined in Task 4 have been added to the IP-SGT binding table.

[Click here to view code image](#)

```
SW2# show cts role-based sgt all
Active IP-SGT Bindings Information
```

IP Address	SGT	Source
10.50.9.5	2	INTERNAL
10.50.9.6	4	LOCAL
10.50.30.3	12	CLI
10.50.30.4	12	CLI
10.50.40.7	7	VLAN
10.50.50.5	2	INTERNAL
10.50.50.20	14	CLI
10.50.70.4	2	CLI
10.50.70.5	2	INTERNAL
10.50.70.6	3	VLAN
10.50.77.5	2	INTERNAL

10.50.77.8	5	LOCAL
10.50.80.50	16	CLI
10.50.99.5	2	INTERNAL
10.50.100.1	15	CLI
10.50.100.2	15	CLI
10.50.100.10	15	CLI
192.168.2.25	18	CLI

IP-SGT Active Bindings Summary

Total number of VLAN bindings = 2
Total number of CLI bindings = 9
Total number of LOCAL bindings = 2
Total number of INTERNAL bindings = 5
Total number of active bindings = 18

All entries learned from SW2 will be of type SXP. The manually defined entry for 10.50.70.4 will be overridden by the internal binding on SW1.

[Click here to view code image](#)

SW1# **sho cts role-based sgt all**
Active IP-SGT Bindings Information

IP Address	SGT	Source
10.50.9.5	2	SXP
10.50.9.6	4	SXP
10.50.30.3	12	SXP
10.50.30.4	12	SXP
10.50.40.7	7	SXP
10.50.50.5	2	SXP
10.50.50.20	14	SXP
10.50.70.4	2	INTERNAL
10.50.70.5	2	SXP
10.50.70.6	3	SXP
10.50.77.5	2	SXP
10.50.77.8	5	SXP
10.50.80.50	16	SXP
10.50.99.5	2	SXP
10.50.100.1	15	SXP
10.50.100.2	15	SXP
10.50.100.10	15	SXP
192.168.1.5	2	INTERNAL
192.168.2.5	2	INTERNAL
192.168.2.25	18	SXP
192.168.100.1	2	INTERNAL

IP-SGT Active Bindings Summary

Total number of SXP bindings = 17

Total number of INTERNAL bindings = 4

Total number of active bindings = 21

Ensure that R6 has all bindings from SW2. The SGTs will be used in the ZFW configuration in [Exercise 1.5](#).

[Click here to view code image](#)

```
R6# show cts role-based sgt all
```

Active IP-SGT Bindings Information

IP Address	SGT	Source
------------	-----	--------

10.50.9.5	2	SXP
10.50.9.6	4	SXP
10.50.30.3	12	SXP
10.50.30.4	12	SXP
10.50.40.7	7	SXP
10.50.50.5	2	SXP
10.50.50.20	14	SXP
10.50.70.4	2	SXP
10.50.70.5	2	SXP
10.50.70.6	3	SXP
10.50.77.5	2	SXP
10.50.77.8	5	SXP
10.50.80.50	16	SXP
10.50.99.5	2	SXP
10.50.100.1	15	SXP
10.50.100.2	15	SXP
10.50.100.10	15	SXP
192.168.2.25	18	SXP

IP-SGT Active Bindings Summary

Total number of SXP bindings = 18

Total number of active bindings = 18

Configuration

SW2

[Click here to view code image](#)

```
cts role-based sgt-map 10.50.30.3 sgt 12
```

```
cts role-based sgt-map 10.50.30.4 sgt 12
```



```
cts role-based sgt-map 10.50.50.20 sgt 14
cts role-based sgt-map 10.50.70.4 sgt 2
cts role-based sgt-map 10.50.80.50 sgt 16
cts role-based sgt-map 10.50.100.1 sgt 15
cts role-based sgt-map 10.50.100.2 sgt 15
cts role-based sgt-map 10.50.100.10 sgt 15
cts role-based sgt-map 192.168.2.25 sgt 18
cts role-based sgt-map vlan-list 70 sgt 3
cts role-based sgt-map vlan-list 40 sgt 7
cts role-based enforcement
cts role-based enforcement vlan-list 9,40,70,77
cts sxp enable
cts sxp connection peer 10.50.70.6 password none mode local
cts sxp connection peer 10.50.70.4 password none mode local
!
```

SW1

[Click here to view code image](#)

```
cts sxp enable
cts sxp default source-ip 10.50.70.4
cts sxp connection peer 10.50.70.5 password none mode local listener
```

R6

[Click here to view code image](#)

```
cts sxp enable
cts sxp connection peer 10.50.70.5 password none mode local listener
```

WLC

[Click here to view code image](#)

```
config cts sxp enable
config cts sxp default password cisco
config cts sxp connection peer 10.50.80.6
```

Tech Notes

SXP on the Cisco WLC

SXP is supported only in centrally switched networks that have central authentication.

- By default, SXP is supported for APs that work in local mode only.
- The controller always operates in the speaker mode.
- The configuration of the default password should be consistent for both controller and the switch.
- Fault tolerance is not supported because fault tolerance requires local switching on APs.
- SXP is supported for both IPv4 and IPv6 clients.

- Static IP-SGT mapping for local authentication of users is not supported.
- IP-SGT mapping requires authentication with external identity servers.
- SXP is supported on the following security policies only:
 - WPA2-dot1x
 - WPA-dot1x
 - 802.1x (Dynamic WEP)
 - MAC filtering using RADIUS servers
 - Web authentication using RADIUS servers for user authentication

Summary of Secure Group Access Features

- **802.1AE Encryption (MACsec):** Protocol for 802.1AE-based wire-rate hop-to-hop Layer 2 encryption. Between MACsec-capable devices, packets are encrypted on egress from the sending device, decrypted on ingress to the receiving device, and in the clear within the devices. This feature is available only between 802.1AE-capable devices.
- **Network Device Admission Control (NDAC):** NDAC is an authentication process by which each network device in the TrustSec domain can verify the credentials and trustworthiness of its peer device. NDAC uses an authentication framework based on IEEE 802.1x port-based authentication and uses EAP-FAST as its EAP method. Authentication and authorization by NDAC results in SAP negotiation for 802.1AE encryption.
- **Security Association Protocol (SAP):** SAP is a Cisco proprietary key exchange protocol between switches. After NDAC switch-to-switch authentication, SAP automatically negotiates keys and the cipher suite for subsequent switch-to-switch MACsec encryption between TrustSec peers. The protocol description is available under a nondisclosure agreement.
- **Security Group Tag (SGT):** An SGT is a 16-bit single label showing the security classification of a source in the TrustSec domain. It is appended to an Ethernet frame or an IP packet.
- **SGT Exchange Protocol (SXP), including SXPv2:** With SXP, devices that are not TrustSec-hardware capable can receive SGT attributes for authenticated users or devices from the Cisco Access Control System (ACS). The devices then forward the source IP-to-SGT binding to a TrustSec-hardware capable device for tagging and security group ACL (SGACL) enforcement.

Part IV: Appendices

Appendix A. Manual Configuration Guide

Cisco Catalyst Switches: SW1, SW2

Switch	Username/Password
SW1	cisco/cisco
SW2	cisco/cisco

Step 1. Erase and reload:

[Click here to view code image](#)

```
SW# wr erase  
<enter> (confirm)  
reload  
<enter> (confirm)
```

```
System configuration has been modified. Save? [yes/no]: no  
Proceed with reload? [confirm]
```

```
Would you like to enter the initial configuration dialog? [yes/no]: n
```

Step 2. Load the init file for the exam version:

[Click here to view code image](#)

```
Switch# conf t  
Enter configuration commands, one per line. End with CNTL/Z.
```

Cut and paste the init file and save the config.

Note

Copy/paste in chunks to avoid buffer overflow.

Cisco Routers R1, R2, R3, R4, R5, R6, R7

Switch	Username/Password
R1	cisco/cisco
R2	cisco/cisco
R3	cisco/cisco
R4	cisco/cisco
R5	cisco/cisco
R6	cisco/cisco
R7	cisco/cisco

Step 1. Erase any old cert info, and config and reload:

[Click here to view code image](#)

```
R# del nvram:*cer  
R# del nvram:ciscoca*
```

```
R# wr er  
<enter> (confirm)  
reload  
<enter> (confirm)
```

System configuration has been modified. Save? [yes/no]: **no**
Proceed with reload? [confirm]

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: **no**

Would you like to terminate autoinstall? [yes]: **yes**

Step 1. Load the init file for the exam version. Cut and paste the init file, and save the config.

Note

Copy/paste in chunks to avoid buffer overflow.

Cisco Router R6: Also Used as the CME Server

Cut and past the init file, and save the config:

```
R6# conf t  
telephony-service  
create cnf-files  
exit  
wri t
```

Note

Copy/paste in chunks to avoid buffer overflow.

Cisco ASA Appliances ASA1, ASA2

Two steps are required:

Step 1. For the ASA (mode specific):

[Click here to view code image](#)

```
ASAx# show mode  
If Security context mode: single  
ASAx# conf t  
ASAx(config)# clear configure all
```

```
ciscoasa(config)# hostname ASAx
ASAx(config)# enable password cisco
ASAx(config)# wri
! x = applicable number of device between 1 and 2
If Security context mode: multiple
ASAx# changeto system
ASAx# conf t
ASAx(config)# clear configure context
ASAx(config)# clear configure all
ciscoasa(config)# hostname ASAx
ASAx(config)# enable password cisco
ASAx(config)# wri
```

Step 2. For the ASA in general (either mode):

[Click here to view code image](#)

```
ASAx# del flash:c1.cfg
```

```
Delete filename [c1.cfg]? <enter>
```

```
Delete disk0:/c1.cfg? [confirm] <enter>
```

```
ASAx# del flash:c2.cfg
```

```
Delete filename [c2.cfg]? <enter>
```

```
Delete disk0:/c2.cfg? [confirm] <enter>
```

```
ASAx# del flash:admin.cfg
```

```
Delete filename [admin.cfg]? <enter>
```

```
Delete disk0:/admin.cfg? [confirm] <enter>
```

```
! x = applicable number of device between 1 and 4
```

! Note: There is a chance the files in step 2 will not exist if the device was in single mode, but the delete sequence should be run through anyway. The result may just be that the following error is displayed which is acceptable.

```
ASAx# del flash:c1.cfg
```

```
Delete filename [c1.cfg]?
```

```
Delete disk0:/c1.cfg? [confirm]
```

```
%Error deleting disk0:/c1.cfg (No such file or directory)
```

Note

The ASA will have a set of base config commands that might include call home commands, which are viewable via **wri t** or **show run**. This will not impact the labs.

Cisco WLC

Step 1. Clear the current config and reset the system:

[Click here to view code image](#)

```
User:cisco
Password:C1sc0123
(WLC) >clear config
Are you sure you want to clear the configuration? (y/n) y
Configuration Cleared!
(WLC) >reset system
```

```
The system has unsaved changes.
Would you like to save them now? (y/N) <enter>
Configuration Not Saved!
Are you sure you would like to reset the system? (y/N)y
System will now restart!
```

Step 2. Boot the system, and complete the initial configuration using the System Setup Wizard:

[Click here to view code image](#)

```
Would you like to terminate autoinstall? [yes]: yes
System Name [Cisco_ae:21:64] (31 characters max): -
Invalid response
System Name [Cisco_ae:21:64] (31 characters max): -
Invalid response
System Name [Cisco_ae:21:64] (31 characters max): -
Invalid response
System Name [Cisco_ae:21:64] (31 characters max): WLC
Enter Administrative User Name (24 characters max): cisco
Enter Administrative Password (3 to 24 characters): Cisc1123
Management Interface IP Address: 10.50.100.10
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.50.100.2
Management Interface VLAN Identifier (0 = untagged):100
Management Interface Port Num [1 to 4]:1
Management Interface DHCP Server IP Address: 10.50.100.2
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: cisco
Network Name (SSID):cisco
Configure DHCP Bridging Mode [yes][NO]:no
```

Allow Static IP Addresses [YES][no]: **yes**
Configure a RADIUS Server now? [YES][no]: **no**
Enter Country Code list (enter 'help' for a list of countries) [US]: **US**
Enable 802.11b Network [YES][no]: **no**
Enable 802.11a Network [YES][no]: **no**
Enable 802.11g Network [YES][no]: **no**
Enable Auto-RF [YES][no]: **no**
Configure a NTP server now? [**YES**][no]:
Enter the NTP server's IP address: **10.50.70.5**
Enter a polling interval between 3600 and 604800 secs: **3600**
Configuration correct? If yes, system will save it and reset. [yes][NO]: **YES**
Configuration saved!
Resetting system with new configuration...

Step 3. Add extra settings from the init file:

[Click here to view code image](#)

```
User: cisco
Password: C1sc0123
(cisco Controller) >
Cut and Paste the following:
config interface address management 10.50.100.10 255.255.255.0
 10.50.100.20
config interface vlan management 100
config ap mgmtuser add username cisco password CCie123 enablesecret
 CCie123 all
config sysname WLC
config prompt WLC
config network webmode enable
```

Are you sure you want to save? (y/n) **y**

Cisco IPS Sensor

IPS	Username/Password
IPS	ciscoips/123cisco123

[Click here to view code image](#)

```
IPS# erase current-config
```

Warning: Removing the current-config file will result in all configuration being reset to default, including system information such as IP address.

User accounts will not be erased. They must be removed manually using the "no username" command.

```
Continue? []: yes
```

```
IPS# reset
```

Warning: Executing this command will stop all applications and reboot the node.

Continue with reset? []: **yes**

sensor login: **ciscoips**

Password: **123cisco123**

System will then restart.

! Let the sensor boot to its default mode 0

GNU GRUB version 1.0(11)5 (631K lower / 2096128K upper memory)

0: Cisco IPS

1: Cisco IPS Recovery

2: Cisco IPS Clear Password (cisco)

sensor login: ciscoips

Password:

--- Basic Setup ---

--- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.

User ctrl-c to abort configuration dialog at any prompt.

Default settings are in square brackets '['].

ctrl-c

! If you get the following just select 0

[0] Go to the command prompt without saving this config.

[1] Return to setup without saving this config.

[2] Save this configuration and exit setup.

[3] Continue to Advanced setup.

Enter your selection[3]: **0**

sensor#

Cisco WSA

WSA	Username/Password
wsa	admin/ironport

Step 1. Reset the system:

[Click here to view code image](#)

```
wsa.cisco.com> resetconfig
```

```
Are you sure you want to reset all configuration values? [N]> y
```

Step 2. Cut and paste the init file:

ironport.example.com> **loadconfig**

1. Paste via CLI

2. Load from file

How would you like to load a configuration file?

[1]> **1**

Paste the configuration file now.

Press CTRL-D on a blank line when done.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
  <hostname>wsa.cisco.com</hostname>
  <interfaces>
    <interface>
      <interface_name>Management</interface_name>
      <ip>192.168.2.50</ip>
      <phys_interface>Management</phys_interface>
      <netmask>255.255.255.0</netmask>
      <interface_hostname>wsa.cisco.com</interface_hostname>
      <ftpd_port>21</ftpd_port>
      <sshd_port>22</sshd_port>
      <httpd_port>8080</httpd_port>
      <https_redirect>0</https_redirect>
      <httpsd_port>8443</httpsd_port>
    </interface>
  </interfaces>
  <dns>
    <local_dns>
      <dns_ip priority="0">192.168.2.25</dns_ip>
    </local_dns>
    <dns_ptr_timeout>10</dns_ptr_timeout>
    <dns_routing_table>0</dns_routing_table>
  </dns>

  <default_gateway>192.158.2.5</default_gateway>
  <routes>
  </routes>

  <ntp>
    <ntp_server>192.168.2.5</ntp_server>
    <ntp_routing_table>0</ntp_routing_table>
  </ntp>

  <timezone>America/Los_Angeles</timezone>
```

```
</config>
```

CNTL-D

Values have been loaded. Be sure to run "commit" to make these settings active.

```
ironport.example.com> commit
```

Please enter some comments describing your changes:

```
[]> bootstrap
```

Changes committed: Tue Oct 16 20:15:50 2012 PDT

```
wsa.cisco.com>
```

Appendix B. Preparing for the CCIE Exam

Preparing for the CCIE Security exam involves more than just identifying and reading through study materials. Successful attainment of the certification credential requires time, money, and personal commitment. Candidates often talk of the sacrifices made in terms of time away from family activities, balancing work and study, and the cost of travelling and scheduling written and lab exams. Therefore, it is extremely important that a candidate not schedule an exam until they are completely comfortable with the exam topics and, in the case of the lab exam, have spent many hours doing hands-on practice. It is also just as important that on the day of the lab exam, the candidate takes the time to read through the entire exam and formulate a plan of action to complete all questions within the 8-hour time limit. The lab exam is as much about time management and strategy as it is about actually completing the questions. Remember that getting to the lab exam requires you to achieve a passing mark in the written exam!

CCIE Security Exam topics can be found at

https://learningnetwork.cisco.com/community/certifications/ccie_security

This information outlines CCIE Security Exam preparation and test-taking tips for prospective candidates.

CCIE Certification Process

CCIEs must pass two exams, written and lab. Candidates should be familiar with exam formats, guidelines, and policies.

CCIE Security Written Exam

The goal of the Security written exam is to test concepts and theoretical knowledge of IP fundamentals, IP routing protocols, LAN switching, security protocols, and Cisco-specific technologies and solutions. The exam also tests for an awareness of industry standard best practices, standard bodies, policy frameworks, and common RFC/BCPs.

The major exam topics list is as follows:

- Infrastructure, Connectivity, Communications, Network Security
- Security Protocols
- Application and Infrastructure Security
- Threats, Vulnerability Analysis, and Mitigation
- Cisco Security Products, Features, and Management
- Cisco Security Technologies and Solutions
- Security Policies and Procedures, Best Practices, Standards

The exam format and policies are as follows:

- The written exam consists of 80 to 100 scored multiple-choice questions.
- Available worldwide at any Pearson VUE testing facility. Costs can vary due to location and exchange rates.
- Closed book; no outside reference materials allowed.

- Pass/fail results are available immediately following the exam; the passing score is set by statistical analysis and is subject to periodic change.
- There is a waiting period of five calendar days to retake the exam.
- After passing the written exam, a candidate must make a first lab exam attempt within 18 months.
- No “skip-question” functionality. A question must be completely answered before the next question will be presented.
- This is a non-proctored exam. The Pearson VUE test center staff is there to monitor the exam center, enforce center policy, and answer operational questions only. They will not clarify exam question content.

CCIE Security Lab Exam

This is a full-day (8-hour) hands-on exam that tests the candidate’s ability to configure and troubleshoot equipment and solutions.

The major exam topics list is as follows:

- System Hardening and Availability
- Threat Identification and Mitigation
- Intrusion Prevention and Content Security
- Identity Management
- Perimeter Security and Services
- Confidentiality and Secure Access

The exam format and policies are as follows:

- Available at Cisco Test Centers globally, including mobile labs.
- Roughly 20% to 30% of the lab is troubleshooting, with some question interdependencies (guideline only).
- Cisco documentation is available via the Cisco website; no personal materials of any kind are allowed in the lab.
- There is a waiting period of 30 days to retake the exam.
- Scores can be viewed online normally within 48 hours, and failing score reports indicate areas where additional study may be useful.
 - No partial credit is awarded on questions
 - Points are awarded for working solutions only
 - Some questions have multiple solutions; grading is done on verification output
- This is a proctored exam:
 - The proctor’s role is to keep the exam fair
 - Ask the proctor clarifying questions
 - Report any equipment or technical problems to the proctor immediately—do not wait until after the exam to raise a concern
- Information on scheduling a lab exam can be found at

https://learningnetwork.cisco.com/community/certifications/ccie_security/lab_exam?tab=take-your-lab-exam.

- Make sure you are familiar with the latest CCIE policy information <http://www.cisco.com/web/learning/exams/policies.html>.

Planning Resources

A good study plan is the key to success:

- Choose materials that offer configuration examples and take a hands-on approach.
- Look for materials approved or provided by Cisco and its Learning Partners.
- Customize your study plan to reflect your own personal strengths and weaknesses.
- Plan daily and weekly study activities, and keep notes on concepts that need further reading or research.

Assessing Strengths and Weaknesses

- Evaluate your experience and knowledge in the major topic areas listed on the exam topics documents.
- For areas of strength, practice for speed.
- For weaker areas, boost your knowledge with training or book study first, and then practice.

Training, Practice Labs, and Boot Camps

Although no formal training is required for the CCIE Security Certification, it is highly recommended that candidates get as much hands-on practice as possible. Many vendors offer CCIE Security boot camps and rack rentals. Candidates are encouraged to use Cisco Learning Partners or to do some research on the various offerings available. The Cisco Learning Network discussion forums are a good place to ask for reviews and recommendations on training resources.

Practice lab exercises with a high level of complexity will assist you in making improvements in your exam strategy and identifying areas requiring extra study. Practice labs can be used to gauge your readiness and help identify your strengths and weaknesses. This will help you refocus and revise your study plan and adjust it according to your progress.

Technical skill is not the only consideration for the lab exam; time management and your exam-taking strategy are also important to succeed in the CCIE Exam. Practice labs will assist you in improving your time management and test-taking approach.

Books and Online Materials

No single resource is available that can prepare a candidate for all written and lab exam topics. Here are several study options that combined will provide a well-rounded approach to your preparation:

- Many Cisco Press and other vendor books are available to assist in preparing for CCIE exams. A current list can be found on the CCIE Security website at http://www.cisco.com/web/learning/le3/ccie/security/book_list.html.
- Many candidates overlook one of the best resources for useful material and technical information: the Cisco website. Many sample scenarios are available on the Tech Support

pages for each Cisco product and technology. These articles are written to reflect current trends and demands and include sample diagrams, configurations, and invaluable **show** and **debug** command outputs.

- Discussion forums can play an essential role for a candidate during preparation; you can find qualified CCIEs and other security engineers available 24×7 to answer questions. Various online sites, such as Facebook, Twitter, and LinkedIn, have a wide variety of information available. The following are some Cisco online forums:
 - **Cisco Learning Network (CLN):** Browse technical content, and connect and share insights, opinions, and knowledge with the community.
<http://learningnetwork.cisco.com>
 - **CLN Study Groups:** Part of the Cisco Learning Network where you can ask questions and share ideas about studying for your Entry, Associate, Professional, or Expert level certification.
<http://learningnetwork.cisco.com/groups>
 - **Certification Online Support:** Questions and Answers on certification-related topics such as exam info, books, training, requirements, resources, tools, and utilities.
<http://www.cisco.com/go/certsupport>
- The Cisco documentation CD is the only resource you are allowed to access during the exam, and you must be able to look up anything you need with speed and confidence, but do NOT rely on it during the exam.

Lab Preparation

Hands-on practice is essential to passing the lab exam.

- Borrow or rent equipment for practice.
- Two or three routers will support most scenarios.
- Virtual devices can be substitutes for physical devices.
- Build and practice scenarios for each topic.
- Go beyond the basics—practice additional features and tuning options.
- If a technology has multiple configurations, practice all of them.
- Learn **show** and **debug** commands for each topic, and be familiar with command outputs.

Lab Exam Tips

- Reduce stress: arrive early.
- Read the entire exam before you begin. There might be some question interdependencies: identify them.
- Ensure that you have connectivity to all devices in your rack and that they are all in the initial state and contain base configuration information only. If there are any issues with lab equipment, tell your proctor immediately. You might be allowed more time to complete your lab if you encounter certain operational issues.
- Manage your time. Point values for each question are noted. Try not to spend too much time on

questions with lower point values if you are pushed for time.

- Redraw parts of the topology to clarify scenarios and identify devices and traffic flows.
- Don't over-think questions or look for hidden tricks. The question will tell you what is required and what NOT to do. If you are not sure of something, ask your proctor.
- Keep a list of tasks to complete for each question, and note any items you might need to go back to for revalidation.
- Work questions as a unit. Each question can be made up of several tasks or parts. Each task must be successfully completed to ensure that points for that question are awarded.
- The lab tests knowledge of solutions as well as of individual devices.
- Test your work as you go, and retest when you have completed the lab.
- Save configurations often; extra time is not given for failure to save configurations.
- Minimize last-minute changes that cannot be adequately verified.

A Word on Cheating...

Unfortunately, there are gray-market vendors and various online sites that reproduce and publish allegedly official exam content. Do not assume that materials purchased from any site are indicative of an official exam. Reproduction of any part of an official Cisco exam is a breach of copyright and confidentiality and is a legal matter. As a candidate, you sign a non-disclosure agreement (NDA), which binds you to an official agreement not to disclose the content of exams. Please take this seriously.

The CCIE credential does carry with it the possibility of career enhancement, rewards, and recognition, but it also carries a level of responsibility. Honor the program and those who achieve their CCIE based on hard work and commitment. More importantly, honor yourself by being ethical and able to show potential employers that you are a security expert and actually understand your craft. Any breaches of exam confidentiality can be forwarded to the Exam Security Enforcement Team using this email alias:

CertSec Security Tipline (security-tipline@external.cisco.com)

Appendix C. Sample Written Exam Questions and Answers

1. In what subnet does address 192.168.23.197/27 reside?
 - A. 192.168.23.0
 - B. 192.168.23.128
 - C. 192.168.23.160
 - D. 192.168.23.192
 - E. 192.168.23.196
2. Given the following IPv6 address, which is not a valid way of shortening the address?
 - A. 2001:0001:0000:0000:00A1:0CC0:01AB:397A
 - B. 2001:1:0:0:A1:CC0:1AB:397A
 - C. 2001:0001::00A1:0CC0:01AB:397A
 - D. 2001:1::A1:CC0:1AB:397A
 - E. 2001:0001::00A1:0CC:1AB:397A
3. Which Cisco ASA feature can be used to update noncompliant antivirus/antispyware definition files on an AnyConnect client?
 - A. Dynamic Access Policies
 - B. Dynamic Access Policies with Host Scan and Advanced Endpoint Assessment
 - C. Cisco Secure Desktop
 - D. Advanced Endpoint Assessment
4. When the Cisco Adaptive Security Appliance (ASA) is running in transparent mode, which two baseline items must be configured for proper operation?
 - A. NAT rules
 - B. A default route
 - C. ARP inspection
 - D. An IP address assigned to the ASA in the same network as that of directly connected devices
 - E. All traffic traversing the ASA must be inspected by a policy-map/service-policy
5. Which two of these Cisco Catalyst security features offer the best ways to prevent ARP cache poisoning?
 - A. Dynamic ARP Inspection
 - B. Port security
 - C. MAC address notification
 - D. DHCP snooping
 - E. PortFast

F. 802.1X authentication

6. You are trying to set up a site-to-site IPsec tunnel between two Cisco ASA adaptive security appliances, but you are not able to pass traffic. You try to troubleshoot the issue by enabling **debug crypto isakmp** and see the following messages:

[Click here to view code image](#)

```
CiscoASA# debug crypto isakmp
```

```
[IKEv1]: Group = 209.165.200.231, IP = 209.165.200.231, Tunnel Rejected:
```

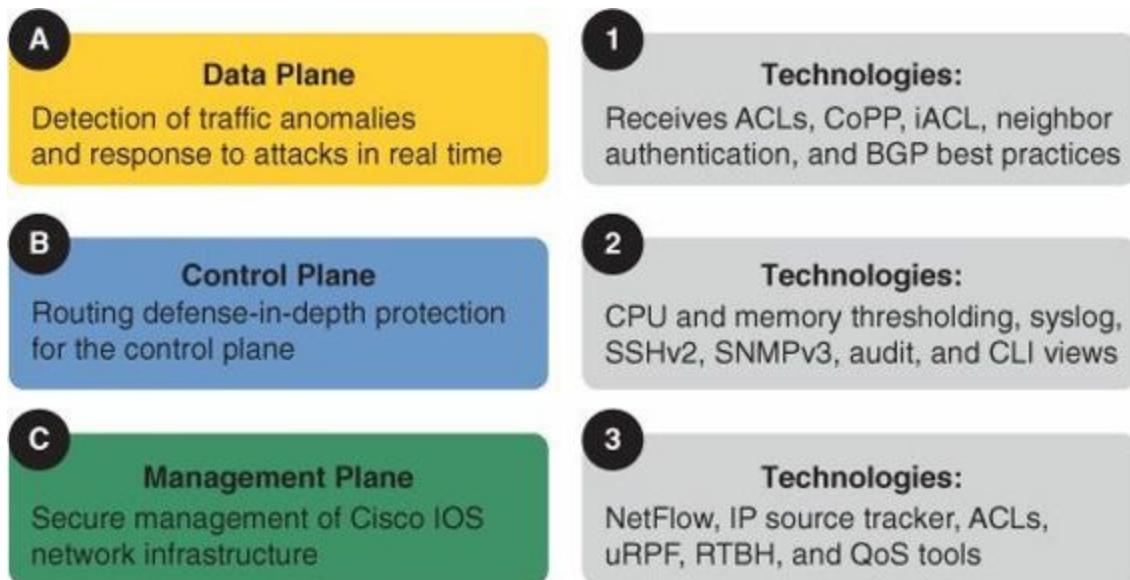
```
Conflicting protocols specified by tunnel-group and group-policy
```

```
[IKEv1]: Group = 209.165.200.231, IP = 209.165.200.231, QM FSM error (P2 struct &0xb0cf31e8, mess id 0x97d965e5)!
```

```
[IKEv1]: Group = 209.165.200.231, IP = 209.165.200.231, Removing peer from correlator table failed, no match!
```

What could the potential problem be?

- A. The policy group mapped to the site-to-site tunnel group is configured to use both IPsec and SSL VPN tunnels.
 - B. The policy group mapped to the site-to-site tunnel group is configured to use both IPsec and L2TP over IPsec tunnels.
 - C. The policy group mapped to the site-to-site tunnel group is configured to use just the SSL VPN tunnel.
 - D. The site-to-site tunnel group is configured to use both IPsec and L2TP over IPsec tunnels.
 - E. The site-to-site tunnel group is configured to use just the SSL VPN tunnel.
7. Refer to the exhibit. Match each letter to the correct number



8. Which wireless client scanning method will be unable to determine the SSID of a wireless network when the SSID cloaking is enabled?
- A. Active
 - B. Monitor
 - C. Passive

D. Enhanced

9. Which statements about SeND for IPv6 are correct? (Choose four.)

A. It protects against rogue RAs.

B. NDP exchanges are protected by IPsec SAs and provide for antireplay.

C. Defines secure extensions for Neighbor Discover Protocol.

D. Authorizes routers to advertise certain prefixes.

E. Provides a method for secure default router election on hosts.

10. As defined by Cisco TrustSec, which EAP method is used for Network Device Admission Control authentication?

A. EAP-FAST

B. EAP-TLS

C. PEAP

D. LEAP

Answers

1. D

2. E

3. B

4. B, D

5. A, D

6. C

7. A3, B1, C2

8. C

9. A, C, D, E

10. A



Cisco Learning Network

Free Test Prep and Beyond.

- ✓ Access review questions
- ✓ Watch Quick Learning Modules (QLMS)
- ✓ Search for jobs and network with others
- ✓ Take self-assessments
- ✓ Participate in study groups
- ✓ Play online learning games

Register for a free membership
and get started now.
www.cisco.com/go/learningnetwork

Cisco Learning Network
A social learning site brought to you by Learning@Cisco

```
SW1# show run | begin ntp
ntp authentication-key 1 md5 cisco
ntp source Vlan102
ntp access-group peer 1
ntp master 2
```

```
ASA1# show ntp associations detail
```

```
192.168.1.5 configured, authenticated, our_master, sane, valid, stratum 2
```

```
ASA1# show ntp status
```

```
Clock is synchronized, stratum 3, reference is 192.168.1.5
```

R6# show ip bgp

BGP table version is 3, local router ID is 172.18.106.6

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S

Stale, m multipath, b backup-path, x best-external, f RT-Filter, a additional-path

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 172.18.106.0/24	0.0.0.0	0		32768	?
*> 172.18.107.0/24	10.50.40.7	0		0	107 ?

R7# show ip bgp

BGP table version is 5, local router ID is 172.18.107.7

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S

Stale, m multipath, b backup-path, x best-external, f RT-Filter, a additional-path

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 172.18.106.0/24	10.50.70.6	0		0	106 ?
*> 172.18.107.0/24	0.0.0.0	0		32768	?

R7# show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.50.50.20	1	FULL/BDR	00:00:32	10.50.40.20	GigabitEthernet0/1

ASA2# show ospf neighbor inside

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.18.107.7	1	FULL/DR	0:00:38	10.50.40.7	inside

ASA2# show ospf

Area 2

Number of interfaces in this area is 1

Area has message digest authentication

R7# show ip ospf

Area 2

Number of interfaces in this area is 2 (1 loopback)

Area has message digest authentication

WCCP-EVNT:D90: Here_I_Am packet from 192.168.2.50 ignored; bad web-cache id.

```
R7# show ip http server history
```

```
HTTP server history:
```

```
local-ipaddress:port  remote-ipaddress:port  in-bytes  out-bytes
      10.50.40.7:80           192.168.2.50:20207  314      192
```

```
R1# show ip http server history
```

```
HTTP server history:
```

```
local-ipaddress:port  remote-ipaddress:port  in-bytes  out-bytes
      10.50.80.6:80           192.168.2.30:58785 369        1986
```

R3# show crypto session

Crypto session current status

Interface: Ethernet0/1

Session status: UP-ACTIVE

Peer: 10.50.30.20 port 500 fvrf: (none) ivrf: (none)

Phase1_id: 10.50.30.20

Desc: (none)

IKEv1 SA: local 10.50.30.3/500 remote 10.50.30.20/500 Active

Capabilities: CX connid:1053 lifetime:23:54:51

IPSEC FLOW: permit ip 10.3.3.0/255.255.255.0 10.4.4.0/255.255.255.0

Active SAs: 2, origin: crypto map

IPSEC FLOW: permit ip host 172.16.1.100 10.4.4.0/255.255.255.0

Active SAs: 2, origin: crypto map

R3# show crypto ipsec client ezvpn

Easy VPN Remote Phase: 8

Tunnel name: ez

Inside interface list: Loopback1

Outside interface: Ethernet0/1

Connect: ACL based with access-list ezvpn-acl

Current State: IPSEC_ACTIVE

Last Event: SOCKET_UP

Address: 172.16.1.100 (applied on Loopback10000)

Mask: 255.255.255.255

DNS Primary: 192.168.2.25

Default Domain: cisco.com

Save Password: Allowed

Current EzVPN Peer: 10.50.30.20

```
R5# show crypto session
Crypto session current status
```

```
Interface: Tunnell
Session status: UP-ACTIVE
Peer: 10.50.30.3 port 4500
  IKEv1 SA: local 10.50.90.5/4500 remote 10.50.30.3/4500 Active
  IPSEC FLOW: permit 47 host 10.50.90.5 host 10.50.30.3
    Active SAs: 2, origin: crypto map
```

```
Interface: Tunnell
Session status: UP-ACTIVE
Peer: 10.50.30.4 port 4500
  IKEv1 SA: local 10.50.90.5/4500 remote 10.50.30.4/4500 Active
  IPSEC FLOW: permit 47 host 10.50.90.5 host 10.50.30.4
    Active SAs: 2, origin: crypto map
```

```
R5# show ip route
D      172.16.33.0/24 [90/25984000] via 172.17.70.3, 2d07h, Tunnell
D      172.16.34.0/24 [90/25984000] via 172.17.70.4, 2d07h, Tunnell
C      172.16.35.0/24 is directly connected, Loopback0
L      172.16.35.5/32 is directly connected, Loopback0
      172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      172.17.70.0/24 is directly connected, Tunnell
L      172.17.70.5/32 is directly connected, Tunnell
```

```
config interface address management 10.50.100.10 255.255.255.0 10.50.100.20
config interface vlan management 100
config ap mgmtuser add username cisco password CCie123 enablesecret CCie123 all
config sysname WLC
config prompt WLC
config network webmode enable
```

(WLC) >show ap summary

Number of APs..... 2

Global AP User Name..... cisco

Global AP Dot1x User Name..... Not Configured

AP Name	Slots	AP Model	Ethernet MAC	Location	Port
AP1cdf.0f94.8063	2	AIR-CAP3502I-A-K9	1c:df:0f:94:80:63	default location	1
AP588d.0959.4921	2	AIR-LAP1262N-A-K9	58:8d:09:59:49:21	default location	1

```
ip dhcp pool pool100
network 10.50.100.0 255.255.255.0
default-router 10.50.100.2
option 43 ip 10.50.100.10
lease infinite
```



```
ip dhcp pool pool110
network 10.10.110.0 255.255.255.0
default-router 10.10.110.1
!
ip dhcp pool pool120
network 10.10.120.0 255.255.255.0
default-router 10.10.120.1
```

```
R1# sho cry key mypubkey rsa
```

```
Key name: ciscoca  
Key type: RSA KEYS  
Storage Device: private-config  
Usage: General Purpose Key  
Key is exportable.
```

```
R1# sho cry pki server
```

```
Certificate Server ciscoca:  
  Status: enabled  
  State: enabled  
  Server's configuration is locked (enter "shut" to unlock it)  
  Issuer name: CN=ciscoca.cisco.com L=cisco C=US  
  CA cert fingerprint: 1F5A02E4 C2C8230A 56FC15BB CBDFBEF6  
  Granting mode is: auto  
  Last certificate issued serial number (hex): 1  
  CA certificate expiration timer: 13:19:37 PST Aug 17 2014  
  CRL NextUpdate timer: 13:19:37 PST Aug 18 2013  
  Current primary storage dir: nvram:  
  Database Level: Minimum - no cert data written to storage
```

```
IPS# packet display gigabitEthernet0/3
```

R1# show ipv6 route

OE2 3001:0:2:3::/64 [110/20]

via FE80::21E:4AFF:FE2F:CA70, Ethernet0/0

R2# show ipv6 route

OE2 3001:0:1:3::/64 [110/20]

via FE80::21E:4AFF:FE36:5210, Ethernet0/0.1

R1# show crypto session

Interface: Ethernet0/0

Session status: UP-NO-IKE

Peer: FF02::5 port 500

IPSEC FLOW: permit 89 FE80::/10 ::/0

Active SAs: 2, origin: manual-keyed crypto map

MI:DROPPED TCP dport 23 fport 18433 faddr 10.50.40.7

```
Rule Name..... RogueAP
State..... Enabled
Type..... Malicious
Match Operation..... Any
Hit Count..... 0
Total Conditions..... 2
Condition 1
  type..... Client-count
  value..... 1
Condition 2
  type..... No-encryption
  value..... Enabled
```

Role Name.....	Guest
Average Data Rate.....	10
Burst Data Rate.....	10
Average Realtime Rate.....	100
Burst Realtime Rate.....	100

```
R5# show ipv6 route
EX 2010::/64 [170/27008000]
   via FE80::A32:5006, Tunnel0
```

```
R6# show ipv6 route
EX 1010::/64 [170/27008000]
   via FE80::A32:5A05, Tunnel0
```


SW1# show ip dhcp snooping binding

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
1C:DF:0F:94:80:63	10.50.100.53	infinite	dhcp-snooping	100	Gig1/0/19

R7# show ip cache flow

IP packet size distribution (52 total packets):

1-32	64	96	128	160	192	224	256	288	320	352	384	416	448	480
.000	.269	.211	.000	.000	.000	.000	.019	.000	.000	.000	.000	.000	.000	.000
512	544	576	1024	1536	2048	2560	3072	3584	4096	4608				
.000	.000	.000	.019	.480	.015	.030	.000	.000	.000	.000				

Protocol	Total	Flows	Packets	Bytes	Packets	Active (Sec)	Idle (Sec)
-----	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/Flow
ICMP	17	0.0	8	1213	0.0	6.5	15.4
Total:	17	0.0	8	1213	0.0	6.5	15.4

SW2# show authentication session int g1/0/14

Interface: GigabitEthernet1/0/14
MAC Address: 0023.eb54.1109
IP Address: Unknown
User-Name: 00-23-EB-54-11-09
Status: Authz Success
Domain: VOICE
Security Policy: Should Secure
Security Status: Unsecure
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: 9
ACS ACL: xACSACLx-IP-PERMIT_ALL_TRAFFIC-4fe7f797
Session timeout: 3600s (local), Remaining: 3509s
Timeout action: Reauthenticate
Idle timeout: N/A
Common Session ID: COA842420000002E003D9546
Acct Session ID: 0x00000030
Handle: 0x3C00002F

Runnable methods list:

Method	State
mab	Authc Success
dot1x	Not run

R6# show ephone summary

hairpin_block:

ephone-1[0] Mac:0023.EB54.1109 TCP socket:[1] activeLine:0 whisperLine:0
REGISTERED
mediaActive:0 whisper_mediaActive:0 startMedia:0 offhook:0 ringing:0 reset:0
reset_sent:0 debug:0
IP:7.7.9.6 * 7965 keepalive 10609 music 0

Max 10, Registered 1, Unregistered 0, Deceased 0 High Water Mark 11, Sockets 1
ephone_send_packet process switched 0

SW2# sho auth sess int g1/0/14

Interface: GigabitEthernet1/0/14

MAC Address: 000c.290d.0c22

IP Address: Unknown

User-Name: Test-PC

Status: Authz Success

Domain: DATA

Security Policy: Should Secure

Security Status: Unsecure

Oper host mode: multi-auth

Oper control dir: both

Authorized By: Authentication Server

Vlan Policy: 99

ACS ACL: xACSACLx-IP-DATA_VLAN_DACL-503d6911

Session timeout: 3600s (local), Remaining: 3585s

Timeout action: Reauthenticate

Idle timeout: N/A

Common Session ID: C0A842420000008B37CC94A2

Acct Session ID: 0x000000B4

Handle: 0x0F00008C

Runnable methods list:

Method	State
--------	-------

mab	Failed over
-----	-------------

dot1x	Authc Success
-------	---------------

```
ASA1# show mode
```

```
Security context mode: multiple
```

ASA1# show context

Context Name	Class	Interfaces	URL
*admin	default	GigabitEthernet0/2.2	disk0:/admin.cfg
c2	default	GigabitEthernet0/0, GigabitEthernet0/1, GigabitEthernet0/3	disk0:/c2.cfg
c1	default	GigabitEthernet0/0, GigabitEthernet0/2.1	disk0:/c1.cfg

Total active Security Contexts: 3

```
ASA1# show int gigabitEthernet 0/2.1
Interface GigabitEthernet0/2.1 "", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
    VLAN identifier 101
      Available for allocation to a context
ASA1# show int gigabitEthernet 0/2.2
Interface GigabitEthernet0/2.2 "", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
    VLAN identifier 102
      Available for allocation to a context
```

```
ASA1# changeto context admin
```



```
ASA1/admin# show nameif
```

Interface	Name	Security
Management0/0	mgmt	100

```
ASA1/admin# show interface ip brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/2.2	192.168.1.20	YES	manual	up	up

```
ASA1/admin# show route
```

```
Gateway of last resort is 192.168.1.5 to network 0.0.0.0
```

```
C    192.168.1.0 255.255.255.0 is directly connected, mgmt
```

```
S*   0.0.0.0 0.0.0.0 [1/0] via 192.168.1.5, mgmt..
```

ASA1/admin# show ip address

System IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/2.2	mgmt	192.168.1.20	255.255.255.0	manual

Current IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/2.2	mgmt	192.168.1.20	255.255.255.0	manual

```
ASA1/admin# show interface
```

```
Interface GigabitEthernet0/2.2 "mgmt", is up, line protocol is up
```

```
MAC address 1200.0202.0100, MTU 1500
```

```
IP address 192.168.1.20, subnet mask 255.255.255.0
```

```
Traffic Statistics for "mgmt":
```

```
138 packets input, 10938 bytes
```

```
715 packets output, 27076 bytes
```

```
0 packets dropped
```

```
Management-only interface. Blocked 0 through-the-device packets
```

```
ASA1/admin# ping 192.168.1.5
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.1.5, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
ASA1/admin# ping 192.168.2.5
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.2.5, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms
```

```
ASA1/c1# show nameif
```

Interface	Name	Security
GigabitEthernet0/0	outside	0
GigabitEthernet0/2.1	inside	100

```
ASA1/c1# show interface ip brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	10.50.80.20	YES	manual	up	up
GigabitEthernet0/2.1	192.168.2.20	YES	manual	up	up


```
ASA1/c1# show route
```

```
Gateway of last resort is 10.50.80.6 to network 0.0.0.0
```

```
C 10.50.80.0 255.255.255.0 is directly connected, outside
```

```
C 192.168.2.0 255.255.255.0 is directly connected, inside
```

```
S* 0.0.0.0 0.0.0.0 [1/0] via 10.50.80.6, outside
```

ASA1/c1# show ip address

System IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0	outside	10.50.80.20	255.255.255.0	manual
GigabitEthernet0/2.1	inside	192.168.2.20	255.255.255.0	manual

Current IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0	outside	10.50.80.20	255.255.255.0	manual
GigabitEthernet0/2.1	inside	192.168.2.20	255.255.255.0	manual

```
ASA1/c1# ping 192.168.2.25
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.2.25, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
ASA1/c1# ping 10.50.70.5
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.50.70.5, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

```
ASA1/c1# ping 10.50.90.5
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.50.90.5, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

```
ASA1/c2# show nameif
```

Interface	Name	Security
GigabitEthernet0/0	outside	0
GigabitEthernet0/1	dmz	50
GigabitEthernet0/3	inside	100

ASA1/c2# show interface ip brief

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	10.50.80.30	YES	manual	up	up
GigabitEthernet0/1	10.50.90.20	YES	manual	up	up
GigabitEthernet0/3	10.50.100.20	YES	manual	up	up

ASA1/c2# show route

Gateway of last resort is 10.50.80.6 to network 0.0.0.0

```
S 10.10.0.0 255.255.0.0 [1/0] via 10.50.100.2, inside
C 10.50.100.0 255.255.255.0 is directly connected, inside
C 10.50.90.0 255.255.255.0 is directly connected, dmz
C 10.50.80.0 255.255.255.0 is directly connected, outside
S* 0.0.0.0 0.0.0.0 [1/0] via 10.50.80.6, outside
```

ASA1/c2# show ip address

System IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0	outside	10.50.80.30	255.255.255.0	manual
GigabitEthernet0/1	dmz	10.50.90.20	255.255.255.0	manual
GigabitEthernet0/3	inside	10.50.100.20	255.255.255.0	manual

Current IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0	outside	10.50.80.30	255.255.255.0	manual
GigabitEthernet0/1	dmz	10.50.90.20	255.255.255.0	manual
GigabitEthernet0/3	inside	10.50.100.20	255.255.255.0	manual

ASA1/c2# ping 10.50.90.5

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.50.90.5, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA1/c2# ping 10.50.70.5

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.50.70.5, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA1/c2# ping 192.168.2.5

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.2.5, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASA1/c2# ping 192.168.2.50

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.2.50, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms


```
! System Execution Space
hostname ASA1
enable password 8Ry2YjIyt7RRXU24 encrypted
mac-address auto
!
interface GigabitEthernet0/0
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface GigabitEthernet0/2.1
vlan 101
!
interface GigabitEthernet0/2.2
vlan 102
!
interface GigabitEthernet0/3
!
interface Management0/0
shutdown
!
class default
limit-resource All 0
limit-resource ASDM 5
limit-resource SSH 5
limit-resource Telnet 5
!

ftp mode passive
pager lines 24
no failover
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
console timeout 0
```

```
admin-context admin
context admin
    allocate-interface GigabitEthernet0/2.2
    config-url disk0:/admin.cfg
!
```

```
context c2
    allocate-interface GigabitEthernet0/0
    allocate-interface GigabitEthernet0/1
    allocate-interface GigabitEthernet0/3
    config-url disk0:/c2.cfg
!
```

```
context c1
    allocate-interface GigabitEthernet0/0
    allocate-interface GigabitEthernet0/2.1
    config-url disk0:/c1.cfg
!
```

```
! Context Admin
hostname admin
names
!
interface GigabitEthernet0/2.2
    nameif mgmt
    security-level 100
    ip address 192.168.1.20 255.255.255.0
    management-only
!
route mgmt 0.0.0.0 0.0.0.0 192.168.1.5 1
```

```
! Context c1
hostname c1
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.50.80.20 255.255.255.0
!
interface GigabitEthernet0/2.1
 nameif inside
 security-level 100
 ip address 192.168.2.20 255.255.255.0
!
access-list 101 extended permit icmp any any
pager lines 24
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
access-group 101 in interface outside
route outside 0.0.0.0 0.0.0.0 10.50.80.6 1
```

```
! Context c2
hostname c2
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.50.80.30 255.255.255.0
!
interface GigabitEthernet0/1
 nameif dmz
 security-level 50
 ip address 10.50.90.20 255.255.255.0
!
interface GigabitEthernet0/3
 nameif inside
 security-level 100
 ip address 10.50.100.20 255.255.255.0
!
access-list 101 extended permit icmp any any
pager lines 24
mtu outside 1500
mtu dmz 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
access-group 101 in interface outside
access-group 101 in interface dmz
route outside 0.0.0.0 0.0.0.0 10.50.80.6
```

```
route outside 10.50.100.0 255.255.255.0 10.50.80.30
```

```
route outside 192.168.2.0 255.255.255.0 10.50.80.20
```

R6# show arp

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	10.50.80.20	13	1200.0000.0400	ARPA	Ethernet0/0
Internet	10.50.80.30	98	1200.0000.0300	ARPA	Ethernet0/0

```
ASA2# show mode
```

```
Security context mode: single
```


ASA2# show interface ip brief

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	10.50.50.20	YES	manual	up	up
GigabitEthernet0/1	unassigned	YES	unset	administratively down	up
GigabitEthernet0/2	10.50.40.20	YES	manual	up	up
GigabitEthernet0/3	10.50.30.20	YES	manual	up	up

ASA2# show ip address

System IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/2	inside	10.50.40.20	255.255.255.0	manual
GigabitEthernet0/3	dmz	10.50.30.20	255.255.255.0	manual
GigabitEthernet0/0	outside	10.50.50.20	255.255.255.0	manual

Current IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/2	inside	10.50.40.20	255.255.255.0	manual
GigabitEthernet0/3	dmz	10.50.30.20	255.255.255.0	manual
GigabitEthernet0/0	outside	10.50.50.20	255.255.255.0	manual

ASA2# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 10.50.50.5 to network 0.0.0.0

```
O E2 10.10.0.0 255.255.0.0 [110/20] via 10.50.50.5, 0:01:51, outside
O E2 10.7.7.0 255.255.255.0 [110/20] via 10.50.40.7, 0:00:06, inside
S 10.3.3.0 255.255.255.0 [1/0] via 10.50.30.3, dmz
S 10.4.4.0 255.255.255.0 [1/0] via 10.50.30.4, dmz
C 10.50.50.0 255.255.255.0 is directly connected, outside
C 10.50.40.0 255.255.255.0 is directly connected, inside
C 10.50.30.0 255.255.255.0 is directly connected, dmz
O 10.50.9.0 255.255.255.0 [110/11] via 10.50.50.5, 153:41:56, outside
O 10.50.99.0 255.255.255.0 [110/11] via 10.50.50.5, 153:41:56, outside
O E2 10.50.100.0 255.255.255.0 [110/20] via 10.50.50.5, 151:10:22, outside
O E2 10.50.90.0 255.255.255.0 [110/20] via 10.50.50.5, 151:10:22, outside
O 10.50.77.0 255.255.255.0 [110/11] via 10.50.50.5, 153:41:56, outside
O 10.50.70.0 255.255.255.0 [110/11] via 10.50.50.5, 153:41:56, outside
O E2 192.168.2.0 255.255.255.0 [110/20] via 10.50.50.5, 151:10:22, outside
O E2 192.168.100.0 255.255.255.0 [110/20] via 10.50.50.5, 151:10:22, outside
O*E2 0.0.0.0 0.0.0.0 [110/1] via 10.50.50.5, 151:10:34, outside
```

SW2# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 10.50.70.6 to network 0.0.0.0

```
O*E2 0.0.0.0/0 [110/1] via 10.50.70.6, 1d01h, Vlan70
      10.0.0.0/8 is variably subnetted, 15 subnets, 2 masks
O E2 10.10.0.0 255.255.0.0 [110/20] via 10.50.70.6, 0:01:51, Vlan70
O E2   10.7.7.0/24 [110/20] via 10.50.50.20, 00:04:20, Vlan50
O IA   10.50.30.0/24 [110/11] via 10.50.50.20, 23:02:50, Vlan50
O IA   10.50.40.0/24 [110/11] via 10.50.50.20, 1d01h, Vlan50
C     10.50.50.0/24 is directly connected, Vlan50
L     10.50.50.5/32 is directly connected, Vlan50
C     10.50.70.0/24 is directly connected, Vlan70
L     10.50.70.5/32 is directly connected, Vlan70
C     10.50.77.0/24 is directly connected, Vlan77
L     10.50.77.5/32 is directly connected, Vlan77
O E2   10.50.90.0/24 [110/20] via 10.50.70.6, 1d01h, Vlan70
C     10.50.99.0/24 is directly connected, Vlan99
L     10.50.99.5/32 is directly connected, Vlan99
O E2   10.50.100.0/24 [110/20] via 10.50.70.6, 1d01h, Vlan70
O E2 192.168.2.0/24 [110/20] via 10.50.70.6, 1d01h, Vlan70
O E2 192.168.100.0/24 [110/20] via 10.50.70.6, 1d01h, Vlan70
```

ASA2# show ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.18.107.7	1	FULL/DR	0:00:36	10.50.40.7	inside
172.16.33.3	1	FULL/BDR	0:00:34	10.50.30.3	dmz
172.16.34.4	1	FULL/DR	0:00:35	10.50.30.4	dmz
10.50.99.5	1	FULL/DR	0:00:36	10.50.50.5	outside

ASA2# show ospf 1

Routing Process "ospf 1" with ID 10.50.50.20 and Domain ID 0.0.0.1

Supports only single TOS(TOS0) routes

Does not support opaque LSA

It is an area border router

SPF schedule delay 5 secs, Hold time between two SPFs 10 secs

Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs

Number of external LSA 20. Checksum Sum 0x 97a04

Number of opaque AS LSA 0. Checksum Sum 0x 0

Number of DCbitless external and opaque AS LSA 0

Number of DoNotAge external and opaque AS LSA 0

Number of areas in this router is 3. 3 normal 0 stub 0 nssa

External flood list length 0

Area BACKBONE(0)

Number of interfaces in this area is 1

Area has no authentication

SPF algorithm executed 78 times

Area ranges are

Number of LSA 24. Checksum Sum 0x fdce6

Number of opaque link LSA 0. Checksum Sum 0x 0

Number of DCbitless LSA 0

Number of indication LSA 0

Number of DoNotAge LSA 0

Flood list length 0

Area 1

Number of interfaces in this area is 1

Area has no authentication

SPF algorithm executed 72 times

Area ranges are

Area-filter ospf in

Number of LSA 17. Checksum Sum 0x 825dd

Number of opaque link LSA 0. Checksum Sum 0x 0

Number of DCbitless LSA 0

Number of indication LSA 0

Number of DoNotAge LSA 0

Flood list length 0

Area 2

Number of interfaces in this area is 1

Area has no authentication

SPF algorithm executed 29 times

Area ranges are

Number of LSA 15. Checksum Sum 0x 85505

Number of opaque link LSA 0. Checksum Sum 0x 0

Number of DCbitless LSA 0

Number of indication LSA 0

Number of DoNotAge LSA 0

Flood list length 0

```
hostname ASA2
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.50.50.20 255.255.255.0
 ospf priority 0
!
!
interface GigabitEthernet0/2
 nameif inside
 security-level 100
 ip address 10.50.40.20 255.255.255.0
!
interface GigabitEthernet0/3
 nameif dmz
 security-level 50
 ip address 10.50.30.20 255.255.255.0
!
!
access-list 101 extended permit icmp any any
!
access-group 101 in interface outside
access-group 101 in interface dmz
!
!
router ospf 1
 network 10.50.30.0 255.255.255.0 area 1
 network 10.50.40.0 255.255.255.0 area 2
 network 10.50.50.0 255.255.255.0 area 0
log-adj-changes
!
route dmz 10.3.3.0 255.255.255.0 10.50.30.3 1
route dmz 10.4.4.0 255.255.255.0 10.50.30.4 1
```

redistribute static subnets


```
ASA1/c2# changeto context c2
```

```
ASA1/c2# show nat detail
```

```
Auto NAT Policies (Section 2)
```

```
1 (dmz) to (outside) source static r5 10.50.80.50
```

```
    translate_hits = 2, untranslate_hits = 4
```

```
    Source - Origin: 10.50.90.5/32, Translated: 10.50.80.50/32
```

```
ASA1/c2# packet-tracer input dmz icmp 10.50.90.5 0 8 10.50.30.3
Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
object network r5
  nat (dmz,outside) static 10.50.80.50
Additional Information:
Static translate 10.50.90.5/0 to 10.50.80.50/0
```

```
ASA1/c2# changeto context c2
```

```
ASA1/c2# show nat detail
```

```
Manual NAT Policies (Section 1)
```

```
1 (inside) to (outside) source dynamic 100net pool50 destination static  
remote50net remote50net
```

```
translate_hits = 0, untranslate_hits = 0
```

```
Source - Origin: 10.50.100.0/24, Translated: 10.50.80.100-10.50.80.150
```

```
Destination - Origin: 10.50.50.0/24, Translated: 10.50.50.0/24
```

```
ASA1/c2# packet-tracer input inside icmp 10.50.100.1 0 8 10.50.50.5
```

```
Phase: 4
```

```
Type: NAT
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
nat (inside,outside) source dynamic 100net pool50 destination static remote50net  
remote50net
```

```
Additional Information:
```

```
Dynamic translate 10.50.100.1/0 to 10.50.80.113/0
```

```
ASA1/c2# packet-tracer input inside icmp 10.50.100.1 0 8 10.50.80.6
```

```
Phase: 4
```

```
Type: NAT
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
nat (inside,outside) source static 100net 100net
```

```
Additional Information:
```

```
Static translate 10.50.100.1/0 to 10.50.100.1/0
```

```
ASA1# changeto system
```

```
ASA1# show ntp associations detail
```

```
192.168.1.5 configured, authenticated, our_master, sane, valid, stratum 2
```

```
ASA1# show ntp status
```

```
Clock is synchronized, stratum 3, reference is 192.168.1.5
```

```
access-list 1 permit 192.168.1.20
```

```
ASA1/c2# changeto context c2
```

```
ASA1/c2# show access-list
```

```
access-list 101 line 2 extended permit 41 host 10.50.80.6 host 10.50.90.5
```

```
ntp authentication-key 1 md5 ***** (cisco is not displayed)
ntp authenticate
ntp trusted-key 1
ntp server 192.168.1.5 key 1 source mgmt
```



```
object network r5
  host 10.50.90.5
object network r5
  nat (dmz,outside) static 10.50.80.50

object network 100net
  subnet 10.50.100.0 255.255.255.0
object network remote50net
  subnet 10.50.50.0 255.255.255.0
object network pool50
  range 10.50.80.100 10.50.80.150

nat (inside,outside) source dynamic 100net pool50 destination static remote50net
  remote50net
nat (inside,outside) source static 100net 100net

access-list 101 extended permit icmp any any
access-list 101 extended permit 41 host 10.50.80.6 host 10.50.90.5

access-group 101 in interface outside
```

```
ntp authentication-key 1 md5 cisco
ntp authenticate
ntp trusted-key 1
ntp source Vlan102
ntp access-group peer 1
ntp master 2

access-list 1 permit 192.168.1.20
```

```
object network pool50
  range 10.50.80.100 10.50.80.150

object-group network dest-remotenet50
  network-object object pool50
  network-object host 10.50.80.251
```

ASA1/c2# packet-tracer input outside icmp 10.50.50.5 0 8 10.50.100.10

Phase: 1

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 2

Type: UN-NAT

Subtype: static

Result: ALLOW

Config:

nat (inside,outside) source static 100net 100net

Additional Information:

NAT divert to egress interface inside

Untranslate 10.50.100.10/0 to 10.50.100.10/0

Phase: 3

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

access-group 101 in interface outside

access-list 101 extended permit icmp any any

Additional Information:

Phase: 4

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 5

Type: INSPECT

Subtype: np-inspect

Result: ALLOW

Config:

Additional Information:

Phase: 6

Type: NAT

Subtype:

Result: ALLOW

Config:

nat (inside,outside) source static 100net 100net

Additional Information:

Static translate 10.50.50.5/0 to 10.50.50.5/0

Phase: 7

Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

nat (inside,outside) source dynamic 100net pool50 destination static remote50net
remote50net

Additional Information:

Phase: 8

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 754623, packet dispatched to next module

Result:

input-interface: outside

input-status: up

input-line-status: up

output-interface: inside

output-status: up

output-line-status: up

Action: allow

```
ASA1/c2(config)# show conn detail
41 outside:10.50.80.6/0 dmz:10.50.90.5/0,
    idle 3s, uptime 7D11h, timeout 2m0s, bytes 11154548
```

```
ASA1/c2(config)# show nat detail
```

```
Manual NAT Policies (Section 1)
```

```
1 (inside) to (outside) source dynamic 100net pool50 destination static  
remote50net remote50net
```

```
translate_hits = 1, untranslate_hits = 1
```

```
Source - Origin: 10.50.100.0/24, Translated: 10.50.80.100-10.50.80.150
```

```
Destination - Origin: 10.50.50.0/24, Translated: 10.50.50.0/24
```

```
2 (inside) to (outside) source static 100net 100net
```

```
translate_hits = 11941, untranslate_hits = 1250
```

```
Source - Origin: 10.50.100.0/24, Translated: 10.50.100.0/24
```

```
Auto NAT Policies (Section 2)
```

```
1 (dmz) to (outside) source static r5 10.50.80.50
```

```
translate_hits = 32, untranslate_hits = 1290
```

```
Source - Origin: 10.50.90.5/32, Translated: 10.50.80.50/32
```

```
static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 dns
```



```
object network obj-192.168.100.10
host 192.168.100.10
nat (inside,outside) static 172.20.1.10 dns
```

global (outside) 1 10.76.6.111

global (outside) 1 10.76.6.109-10.76.6.110

```
object network obj-10.76.6.111
host 10.76.6.111
object network obj-10.76.6.109-10.76.6.110
range 10.76.6.109-10.76.6.110
object-group og-global-outside_1
network-object obj-10.76.6.111
network-object obj-10.76.6.109-10.76.6.110
```

R6# show ip bgp

BGP table version is 3, local router ID is 172.18.106.6

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, x best-external,
f RT-Filter, a additional-path

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 172.18.106.0/24	0.0.0.0	0		32768	?
*> 172.18.107.0/24	10.50.40.7	0		0	107 ?

R7# show ip bgp

BGP table version is 5, local router ID is 172.18.107.7

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, x best-external,
f RT-Filter, a additional-path

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 172.18.106.0/24	10.50.70.6	0		0	106 ?
*> 172.18.107.0/24	0.0.0.0	0		32768	?

ASA2# show conn

15 in use, 31 most used

TCP outside 10.50.70.6:179 inside 10.50.40.7:55489, idle 0:00:43, bytes 229761,
flags UIO

```
R7# show ip bgp neighbor | inc md5
```

```
Option Flags: nagle, path mtu capable, md5
```

```
ASA2# show ospf | inc Area 2
```

```
Area 2
```

```
Number of interfaces in this area is 1
```

```
Area has message digest authentication
```

```
R7# show ip ospf | inc Area 2
```

```
Area 2
```

```
Number of interfaces in this area is 2 (1 loopback)
```

```
Area has message digest authentication
```

```
ASA2# show ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.18.107.7	1	FULL/DR	0:00:38	10.50.40.7	inside

```
ASA2# show ospf interface
```

```
....
```

```
inside is up, line protocol is up
```

```
Internet Address 10.50.40.20 mask 255.255.255.0, Area 2
```

```
Process ID 1, Router ID 10.50.50.20, Network Type BROADCAST, Cost: 10  
Transmit Delay is 1 sec, State BDR, Priority 1
```

```
Designated Router (ID) 172.18.107.7, Interface address 10.50.40.7
```

```
Backup Designated router (ID) 10.50.50.20, Interface address 10.50.40.20
```

```
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

```
Hello due in 0:00:01
```

```
Index 1/3, flood queue length 0
```

```
Next 0x00000000(0)/0x00000000(0)
```

```
Last flood scan length is 1, maximum is 8
```

```
Last flood scan time is 0 msec, maximum is 0 msec
```

```
Neighbor Count is 1, Adjacent neighbor count is 1
```

```
Adjacent with neighbor 172.18.107.7 (Designated Router)
```

```
Suppress hello for 0 neighbor(s)
```

```
Message digest authentication enabled
```

```
Youngest key id is 1
```



```
tcp-map eBGP
  tcp-options range 19 19 allow
class-map eBGPclass
  match port tcp eq bgp
policy-map global_policy
  class inspection_default
class eBGPclass
  set connection random-sequence-number disable
  set connection advanced-options eBGP

access-list 101 extended permit tcp any any eq bgp
access-list 101 extended permit tcp any eq bgp any
interface GigabitEthernet0/2
  nameif inside
  security-level 100
  ip address 10.50.40.20 255.255.255.0
  ospf message-digest-key 1 md5 cisco
  ospf authentication message-digest

router ospf 1
  area 2 authentication message-digest
```

```
interface GigabitEthernet0/1
  ip address 10.50.40.7 255.255.255.0
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 cisco

router ospf 1
  area 2 authentication message-digest
```

SW1# telnet 192.168.2.100

Trying 192.168.2.100 ... Open

login: ciscoips

Password:

NOTICE

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wvl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

LICENSE NOTICE

The license key on the IPS-4240 has expired.

The system will continue to operate with the currently installed signature set. A valid license must be obtained in order to apply signature updates. Please go to <http://www.cisco.com/go/license> to obtain a new license or install a license.

ips#

```
SW1# telnet 192.168.2.100 /source-interface vlan102  
Trying 192.168.2.100 ...
```

IPS# show interfaces brief

CC	Interface	Sensing State	Link	Inline Mode	Pair Status
	GigabitEthernet0/0	Enabled	Up	Paired with interface GigabitEthernet0/1	Up
*	Management0/0	Disabled	Up		
	GigabitEthernet0/1	Enabled	Up	Paired with interface GigabitEthernet0/0	Up
	GigabitEthernet0/2	Enabled	Up	Inline-vlan-pair	N/A
	GigabitEthernet0/3	Enabled	Up	Unpaired	

IPS# show interfaces brief

CC	Interface	Sensing State	Link	Inline Mode	Pair Status
	GigabitEthernet0/0	Enabled	Up	Paired with interface GigabitEthernet0/1	Up
*	Management0/0	Disabled	Up		
	GigabitEthernet0/1	Enabled	Up	Paired with interface GigabitEthernet0/0	Up
	GigabitEthernet0/2	Enabled	Up	Inline-vlan-pair	N/A
	GigabitEthernet0/3	Enabled	Up	Unpaired	

IPS# show interfaces gigabitEthernet0/2

MAC statistics from interface GigabitEthernet0/2

Statistics From Subinterface 1

Statistics From Vlan 50

Total Packets Received On This Vlan = 1385065

Total Bytes Received On This Vlan = 123792833

Total Packets Transmitted On This Vlan = 546093

Total Bytes Transmitted On This Vlan = 58657037

Statistics From Vlan 70

Total Packets Received On This Vlan = 546180

Total Bytes Received On This Vlan = 58663474

Total Packets Transmitted On This Vlan = 1385010

Total Bytes Transmitted On This Vlan = 123788928

IPS# show interfaces brief

CC	Interface	Sensing State	Link	Inline Mode	Pair Status
	GigabitEthernet0/0	Enabled	Up	Paired with interface GigabitEthernet0/1	Up
*	Management0/0	Disabled	Up		
	GigabitEthernet0/1	Enabled	Up	Paired with interface GigabitEthernet0/0	Up
	GigabitEthernet0/2	Enabled	Up	Inline-vlan-pair	N/A
	GigabitEthernet0/3	Enabled	Up	Unpaired	

IPS# show interfaces brief

CC	Interface	Sensing State	Link	Inline Mode	Pair Status
	GigabitEthernet0/0	Enabled	Up	Paired with interface GigabitEthernet0/1	Up
*	Management0/0	Disabled	Up		
	GigabitEthernet0/1	Enabled	Up	Paired with interface GigabitEthernet0/0	Up
	GigabitEthernet0/2	Enabled	Up	Inline-vlan-pair	N/A
	GigabitEthernet0/3	Enabled	Up	Unpaired	

```
R6# ping 192.168.2.5
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.2.5, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
R6# ping 10.50.40.7
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.50.40.7, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
physical-interfaces GigabitEthernet0/1
admin-state enabled
exit
physical-interfaces GigabitEthernet0/2
admin-state enabled
subinterface-type inline-vlan-pair
subinterface 1
vlan1 70
vlan2 50
exit
exit
exit
physical-interfaces GigabitEthernet0/3
admin-state enabled
exit
inline-interfaces ipair
interface1 GigabitEthernet0/0
interface2 GigabitEthernet0/1
exit
exit
! -----
service authentication
exit
! -----
service event-action-rules rules0
exit
! -----
service host
network-settings
host-ip 192.168.2.100/24,192.168.2.20
host-name ips
telnet-option enabled
access-list 192.168.2.0/24
dns-primary-server disabled
dns-secondary-server disabled
dns-tertiary-server disabled
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! -----
```

```
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/2 subinterface-number 1
exit
virtual-sensor vs1
logical-interface ipair
exit
virtual-sensor vs2
physical-interface GigabitEthernet0/3
exit
exit
```

```
interface GigabitEthernet1/0/16
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 50,70
  switchport mode trunk
!
interface GigabitEthernet1/0/17
  switchport access vlan 10
  switchport mode access
```

```
interface GigabitEthernet1/0/15
  switchport access vlan 101
  switchport mode access
!
interface GigabitEthernet1/0/16
  switchport access vlan 60
  switchport mode access
!
interface GigabitEthernet1/0/17
  switchport access vlan 80
  switchport mode access
```

R6# ping 192.168.2.5

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.2.5, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

02:07:43.923416 IP 10.50.80.6 > 192.168.2.5: ICMP echo request, id 29, seq 0, length 80
02:07:43.925547 IP 192.168.2.5 > 10.50.80.6: ICMP echo reply, id 29, seq 0, length 80
02:07:43.925909 IP 10.50.80.6 > 192.168.2.5: ICMP echo request, id 29, seq 1, length 80
02:07:43.926734 IP 192.168.2.5 > 10.50.80.6: ICMP echo reply, id 29, seq 1, length 80
02:07:43.927107 IP 10.50.80.6 > 192.168.2.5: ICMP echo request, id 29, seq 2, length 80
02:07:43.927831 IP 192.168.2.5 > 10.50.80.6: ICMP echo reply, id 29, seq 2, length 80


```
wsa.cisco.com> interfaceconfig
```

Currently configured interfaces:

1. Management (192.168.2.50/24 on Management: wsa.cisco.com)

Choose the operation you want to perform:

- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.

[]>

```
wsa.cisco.com> setgateway
```

Warning: setting an incorrect default gateway may cause the current connection to be interrupted when the changes are committed.

1. Management Default Gateway
2. Data Default Gateway

[]>

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
  <hostname>wsa.cisco.com</hostname>
  <interfaces>
    <interface>
      <interface_name>Management</interface_name>
      <ip>192.168.2.50</ip>
      <phys_interface>Management</phys_interface>
      <netmask>255.255.255.0</netmask>
      <interface_hostname>wsa.cisco.com</interface_hostname>
      <ftpd_port>21</ftpd_port>
      <sshd_port>22</sshd_port>
      <httpd_port>8080</httpd_port>
      <https_redirect>0</https_redirect>
      <httpsd_port>8443</httpsd_port>
    </interface>
  </interfaces>
  <dns>
    <local_dns>
      <dns_ip priority="0">192.168.2.25</dns_ip>
    </local_dns>
    <dns_ptr_timeout>10</dns_ptr_timeout>
    <dns_routing_table>0</dns_routing_table>
  </dns>

  <default_gateway>192.168.2.20</default_gateway>
  <routes>
</routes>

  <ntp>
    <ntp_server>192.168.2.5</ntp_server>
    <ntp_routing_table>0</ntp_routing_table>
  </ntp>

  <timezone>America/Los_Angeles</timezone>
</config>
```

SW1# **ssh -l admin 192.168.2.50**

Password:

Last login: Fri Sep 6 03:37:18 2013 from 192.168.2.5

Copyright (c) 2001-2011, Cisco Systems, Inc.

AsyncOS 7.7.5 for Web build 190

Welcome to the Cisco IronPort S100V Web Security Virtual Appliance
wsa.cisco.com>

Product: Cisco IronPort S100V Web Security Virtual Appliance
Model Number: S100V
Version: 7.7.5-190
Serial Number: 422C60745CODE7AB65E7-2179C1D5637F
Number of CPUs: 2
Memory (MB): 6144
Current Time: Fri Sep 6 04:08:00 2013

```
ASA1# changeto context c1
```

```
ASA1/c1(config)# show wccp
```

```
Global WCCP information:
```

```
Router information:
```

```
Router Identifier: 192.168.2.20  
Protocol Version: 2.0
```

```
Service Identifier: 90
```

```
Number of Cache Engines: 1  
Number of routers: 1  
Total Packets Redirected: 201578  
Redirect access-list: WCCPRedirectionList -> name must  
match list below  
  
Total Connections Denied Redirect: 0  
Total Packets Unassigned: 0  
Group access-list: wccpservers -> name must match list  
below  
  
Total Messages Denied to Group: 0  
Total Authentication failures: 0  
Total Bypassed Packets Received: 0
```

ASA1/c1# debug wccp packet

WCCP-PKT:D90: Received valid Here_I_Am packet from 192.168.2.50 w/rcv_id 00000213

WCCP-PKT:D90: Sending I_See_You packet to 192.168.2.50 w/ rcv_id 00000214

```
ASA1/c1# show access-list
```

```
access-list WCCPRedirectionList line 1 extended permit tcp any any eq www  
access-list WCCPRedirectionList line 2 extended permit tcp any any eq https  
access-list wccpservers line 1 extended permit ip host 192.168.2.50 any
```

```
R7# show ip http server history
```

```
! note this must be completed after attempting a connection from a browser  
  otherwise the history may be blank.
```

```
HTTP server history:
```

local-ipaddress:port	remote-ipaddress:port	in-bytes	out-bytes	
10.50.40.7:80	192.168.2.50:4507	332	192	17:21:11 04/07
10.50.40.7:80	192.168.2.50:49622	375	192	17:21:23 04/07
10.50.40.7:80	192.168.2.50:24928	379	192	17:21:37 04/07
10.50.40.7:80	192.168.2.50:39850	375	2077	17:21:45 04/07

R6# show ip http server history

! note this must be completed after attempting a connection from a browser
otherwise the history may be blank.

HTTP server history:

local-ipaddress:port	remote-ipaddress:port	in-bytes	out-bytes	
10.50.80.6:80	192.168.2.25:63596	256	192	20:12:15 09/06
10.50.80.6:80	192.168.2.25:63597	295	1986	20:12:23 09/06
10.50.80.6:80	192.168.2.25:63598	248	137	20:12:23 09/06

! ASA1/c1

```
wccp 90 redirect-list WCCPRedirectionList group-list wccpservers  
wccp interface inside 90 redirect in
```

```
access-list WCCPRedirectionList extended permit tcp any any eq www  
access-list WCCPRedirectionList extended permit tcp any any eq https  
access-list wccpservers extended permit ip host 192.168.2.50 any
```

```
ASA1/c1# show wccp 90 hash 10.50.70.6 192.168.2.25 80 1024
```

```
WCCP hash information for:
```

```
Primary Hash: Dst IP: 10.50.70.6
```

```
Bucket: 120
```

```
Cache Engine: 192.168.2.50
```

```
ASA1/c1(config)# show wccp 90 buckets
```

```
WCCP hash bucket assignments:
```

```
Index  Cache Engine:  
00     192.168.2.50  
FF     NOT ASSIGNED
```

```
XX| 0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  
--|-----  
00| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
10| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
20| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
30| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
40| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

R3# ping 10.4.4.4 so lol

R3# show crypto session detail

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Ethernet0/1

Uptime: 00:04:20

Session status: UP-ACTIVE

Peer: 10.50.30.20 port 500 fvrf: (none) ivrf: (none)

Phase1_id: 10.50.30.20

Desc: (none)

IKEv1 SA: local 10.50.30.3/500 remote 10.50.30.20/500 Active

Capabilities: CX connid:1053 lifetime:23:54:51

IPSEC FLOW: permit ip 10.3.3.0/255.255.255.0 10.4.4.0/255.255.255.0

Active SAs: 2, origin: crypto map

Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 4233369/28780

Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4233369/28780

IPSEC FLOW: permit ip host 172.16.1.100 10.4.4.0/255.255.255.0

Active SAs: 2, origin: crypto map

Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 4294332/28780

Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4294332/28780

ASA2# show crypto isakmp sa detail

IKEv1 SAs:

Active SA: 1

Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)

Total IKE SA: 1

```
1 IKE Peer: 10.50.30.3
   Type      : user           Role      : responder
   Rekey     : no            State     : AM_ACTIVE
   Encrypt   : 3des          Hash      : SHA
   Auth      : preshared     Lifetime: 86400
   Lifetime Remaining: 84766
```

```
R3# show crypto ipsec client ezvpn
```

```
Easy VPN Remote Phase: 8
```

```
Tunnel name : ez
```

```
Inside interface list: Loopback1
```

```
Outside interface: Ethernet0/1
```

```
Connect : ACL based with access-list ezvpn-acl
```

```
Current State: IPSEC_ACTIVE
```

```
Last Event: SOCKET_UP
```

```
Address: 172.16.1.100 (applied on Loopback10000)
```

```
Mask: 255.255.255.255
```

```
DNS Primary: 192.168.2.25
```

```
Default Domain: cisco.com
```

```
Save Password: Allowed
```

```
Current EzVPN Peer: 10.50.30.20
```

```
ASA2# show route
```

```
S 172.16.1.100 255.255.255.255 [1/0] via 10.50.30.3, dmz
```

```
R3# show crypto ipsec sa
```

```
....
```

```
interface: Ethernet0/1
```

Crypto map tag: Ethernet0/1-head-0, local addr 10.50.30.3

protected vrf: (none)

local ident (addr/mask/prot/port): (10.3.3.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (10.4.4.0/255.255.255.0/0/0)

current_peer 10.50.30.20 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0

#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.50.30.3, remote crypto endpt.: 10.50.30.20

path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/1

current outbound spi: 0x866878B7(2254993591)

PFS (Y/N): Y, DH group: none

inbound esp sas:

spi: 0xE2663A09(3798350345)

transform: esp-3des esp-sha-hmac ,

in use settings = {Tunnel, }

conn id: 523, flow_id: SW:523, sibling_flags 80000040, crypto map:
Ethernet0/1-head-0

sa timing: remaining key lifetime (k/sec): (4233369/27337)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

```
outbound esp sas:
spi: 0x866878B7(2254993591)
  transform: esp-3des esp-sha-hmac ,
  in use settings =(Tunnel, )
conn id: 524, flow_id: SW:524, sibling_flags 80000040, crypto map:
  Ethernet0/1-head-0
sa timing: remaining key lifetime (k/sec): (4233369/27337)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

```
protected vrf: (none)
local ident (addr/mask/prot/port): (172.16.1.100/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.4.4.0/255.255.255.0/0/0)
current_peer 10.50.30.20 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.50.30.3, remote crypto endpt.: 10.50.30.20
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/1
current outbound spi: 0x76CA9731(1992988465)
PFS (Y/N): Y, DH group: none
```


inbound esp sas:
spi: 0x28BC5612(683431442)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 525, flow_id: SW:525, sibling_flags 80000040, crypto map:
Ethernet0/1-head-0
sa timing: remaining key lifetime (k/sec): (4294332/27337)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x76CA9731(1992988465)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 526, flow_id: SW:526, sibling_flags 80000040, crypto map:
Ethernet0/1-head-0
sa timing: remaining key lifetime (k/sec): (4294332/27337)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

```
crypto ipsec client ezvpn ez
connect acl ezvpn-acl
group ezvpn key cisco
mode network-plus
peer 10.50.30.20
username cisco password cisco
xauth userid mode local
!
!
interface Loopback1
ip address 10.3.3.3 255.255.255.0
crypto ipsec client ezvpn ez inside

interface Ethernet0/1
ip address 10.50.30.3 255.255.255.0
crypto ipsec client ezvpn ez

ip route 10.4.4.0 255.255.255.0 10.50.30.20
!
ip access-list extended ezvpn-acl
permit ip 10.3.3.0 0.0.0.255 10.4.4.0 0.0.0.255
!
```

```
username cisco password cisco
same-security-traffic permit intra-interface
access-list split-tunnel permit 10.4.4.0 255.255.255.0
ip local pool vpnpool 172.16.1.100-172.16.1.199 mask 255.255.255.0
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set ESP-3DES-SHA
crypto map outside_map 10 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface dmz
crypto ikev1 enable dmz
crypto ikev1 policy 10
  authentication pre-share
  encryption 3des
  hash sha
  group 2
  lifetime 86400
group-policy ezvpn1 internal
group-policy ezvpn1 attributes
  dns-server value 192.168.2.25
  vpn-tunnel-protocol ikev1
password-storage enable
default-domain value cisco.com
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split-tunnel
user-authentication disable

tunnel-group ezvpn type remote-access
tunnel-group ezvpn general-attributes
  address-pool vpnpool
  default-group-policy ezvpn1
tunnel-group ezvpn ipsec-attributes
ikev1 pre-shared-key cisco
```

split-tunnel-policy commands/options:

excludespecified Exclude only networks specified by
split-tunnel-network-list

tunnelall Tunnel everything

tunnelspecified Tunnel only networks specified by split-tunnel
network-list

```
group-policy group_policy_name type server-group server_group_name
password server_password
```

```
! Determine NHRP server address according to static mapping on R4 tunnel interface
nhrp map 172.17.70.5 10.50.80.50
NHRP: Attempting to send packet via DEST 172.17.70.5
NHRP: Setting 'used' flag on cache entry with nhop: 172.17.70.5
NHRP: NHRP successfully mapped '172.17.70.5' to NBMA '10.50.80.50'
NHRP: Encapsulation succeeded. Sending NHRP Control Packet NBMA Address:
    10.50.80.50
! IPsec profile applied to tunnel interface will trigger IKE negotiation using
tunnel source and destination of NHRP server
interface Tunnell
    ip address 172.17.70.4 255.255.255.0
    tunnel protection ipsec profile DMVPN
NHRP: Send Registration Request via Tunnell vrf 0, packet size: 105
    src: 172.17.70.4, dst: 172.17.70.5
NHRP: 133 bytes out Tunnell
IPSEC(sa_request): ,
    (key eng. msg.) OUTBOUND local= 10.50.30.4:500, remote= 10.50.80.50:500,
    local_proxy= 10.50.30.4/255.255.255.255/47/0,
    remote_proxy= 10.50.80.50/255.255.255.255/47/0,
    protocol= ESP, transform= esp-3des esp-md5-hmac (Transport),
    lifedur= 3600s and 4608000kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
! The requirement for IPsec protection triggers an IKE negotiation between R4 and
R5. Note that the translated address for R5 is used based on Q1.2 ASA NAT task
crypto isakmp policy 1
    encr 3des
    authentication pre-share
    group 2
crypto isakmp key cisco address 10.50.80.5
ISAKMP: Created a peer struct for 10.50.80.5, peer port 500
ISAKMP:(0): beginning Main Mode exchange
ISAKMP:(0): sending packet to 10.50.80.50 my_port 500 peer_port 500 (I) MM_NO_
STATE
```

```
ISAKMP:(0):Sending an IKE IPv4 Packet.
ISAKMP (0): received packet from 10.50.80.50 dport 500 sport 500 Global (I) MM_NO_
STATE
ISAKMP:(0): processing SA payload. message ID = 0
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0):found peer pre-shared key matching 10.50.80.50
ISAKMP:(0): local preshared key found
ISAKMP : Scanning profiles for xauth ... ipv6
ISAKMP:(0):Checking ISAKMP transform 1 against priority 1 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP:(0): sending packet to 10.50.80.50 my_port 500 peer_port 500 (I) MM_SA_
SETUP
ISAKMP:(0):Sending an IKE IPv4 Packet.
ISAKMP:(0):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(0):Old State = IKE_I_MM2  New State = IKE_I_MM3

ISAKMP (0): received packet from 10.50.80.50 dport 500 sport 500 Global (I) MM_SA_
SETUP
ISAKMP:(0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(0):Old State = IKE_I_MM3  New State = IKE_I_MM4
```

```
ISAKMP:(0): processing KE payload. message ID = 0
ISAKMP:(0): processing NONCE payload. message ID = 0
ISAKMP:(0):found peer pre-shared key matching 10.50.80.50
ISAKMP:(1056): processing vendor id payload
ISAKMP:(1056): vendor ID is Unity
ISAKMP:(1056): processing vendor id payload
ISAKMP:(1056): vendor ID is DPD
ISAKMP:(1056): processing vendor id payload
ISAKMP:(1056): speaking to another IOS box!
! NAT translation is occurring on the ASA in between R4 and R5. This is detected
  below:
ISAKMP:received payload type 20
ISAKMP (1056): His hash no match - this node outside NAT
ISAKMP:received payload type 20
ISAKMP (1056): His hash no match - this node outside NAT
ISAKMP:(1056):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1056):Old State = IKE_I_MM4 New State = IKE_I_MM4

ISAKMP:(1056):Send initial contact
ISAKMP:(1056):SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
ISAKMP (1056): ID payload
    next-payload : 8
    type          : 1
    address       : 10.50.30.4
    protocol      : 17
    port          : 0
    length        : 12
ISAKMP:(1056):Total payload length: 12
ISAKMP:(1056): sending packet to 10.50.80.50 my_port 4500 peer_port 4500 (I) MM_
  KEY_EXCH
ISAKMP:(1056):Sending an IKE IPv4 Packet.
ISAKMP:(1056):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(1056):Old State = IKE_I_MM4 New State = IKE_I_MM5
```



```
! NAT-T detected, IKE floats from UDP/500 to UDP/4500. The IKE ID payload will
include the real IP address of R5. If an ISAKMP profile was being referenced, the
match identity statement would use the real ID value if indexed by IP address.
ISAKMP (1056): received packet from 10.50.80.50 dport 4500 sport 4500 Global (I)
MM_KEY_EXCH
ISAKMP:(1056): processing ID payload. message ID = 0
ISAKMP (1056): ID payload
    next-payload : 8
    type          : 1
    address       : 10.50.90.5
    protocol      : 17
    port         : 0
    length       : 12
ISAKMP:(0):: peer matches *none* of the profiles
ISAKMP:(1056): processing HASH payload. message ID = 0
ISAKMP:(1056):SA authentication status:
    authenticated
ISAKMP:(1056):SA has been authenticated with 10.50.80.50
ISAKMP: Trying to insert a peer 10.50.30.4/10.50.80.50/4500/, and inserted
successfully F20ED770.
! IPsec SA negotiation follows. Notice the use of UDP-encaps due to NAT-T. Tunnel
mode GRE is configured which is reflected in IP protocol 47 as part of the traffic
selector.
crypto ipsec transform-set dmvpn esp-3des esp-md5-hmac
    mode transport
!
crypto ipsec profile DMVPN
    set transform-set dmvpn
!
```

```
interface Tunnell
 tunnel mode gre multipoint
ISAKMP (1056): received packet from 10.50.80.50 dport 4500 sport 4500 Global (I)
 QM_IDLE
ISAKMP:(1056): processing HASH payload. message ID = 1543261932
ISAKMP:(1056): processing SA payload. message ID = 1543261932
ISAKMP (1056): processing NAT-OAi payload. addr = 10.50.30.4, message ID =
 1543261932
ISAKMP (1056): processing NAT-OAr payload. addr = 10.50.90.5, message ID =
 1543261932
ISAKMP:(1056):Checking IPsec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP:  attributes in transform:
ISAKMP:      encaps is 4 (Transport-UDP)
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (basic) of 3600
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:(1056):atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1
IPSEC(validate_proposal_request): proposal part #1,
 (key eng. msg.) INBOUND local= 10.50.30.4:0, remote= 10.50.80.50:0,
  local_proxy= 10.50.30.4/255.255.255.255/47/0,
  remote_proxy= 10.50.80.50/255.255.255.255/47/0,
  protocol= ESP, transform= NONE (Transport-UDP),
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
IPSEC(key_engine): got a queue event with 1 KMI message(s)
map_db_find_best did not find matching map
Crypto mapdb : proxy_match
      src addr      : 10.50.30.4
      dst addr      : 10.50.80.50
```

```
protocol      : 47
src port      : 0
dst port      : 0
```

IPSEC(crypto_ipsec_create_ipsec_sas): Map found Tunnell-head-0

IPSEC(create_sa): sa created,

```
(sa) sa_dest= 10.50.30.4, sa_proto= 50,
sa_spi= 0xED27ED07(3978816775),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 519
sa_lifetime(k/sec)= (4608000/3600)
```

IPSEC(create_sa): sa created,

```
(sa) sa_dest= 10.50.80.50, sa_proto= 50,
sa_spi= 0x2CEB926C(753635948),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 520
sa_lifetime(k/sec)= (4608000/3600)
```

! NHRP registration now occurs under the protection of the IPsec SA.

NHRP: Setting retrans delay to 1 for nhs dst 172.17.70.5

NHRP-ATTR: Requester Ext Len: Total ext_len with NHRP attribute VPE 53

NHRP: Attempting to send packet via DEST 172.17.70.5

NHRP: Setting 'used' flag on cache entry with nhop: 172.17.70.5

NHRP: NHRP successfully mapped '172.17.70.5' to NBMA '10.50.80.50'

NHRP: Encapsulation succeeded. Sending NHRP Control Packet NBMA Address:
10.50.80.50

NHRP: Send Registration Request via Tunnell vrf 0, packet size: 105
src: 172.17.70.4, dst: 172.17.70.5

NHRP: 133 bytes out Tunnell

NHRP: Receive Registration Reply via Tunnell vrf 0, packet size: 125

NHRP: netid_in = 0, to_us = 1

NHRP: NHS 172.17.70.5 Tunnell vrf 0 Cluster 0 Priority 0 Transitioned to 'RE'
from 'E'

NHRP: NHS-UP: 172.17.70.5

! A PING is used to trigger the connection between spokes, this address is the lo0 interface on R3.

R4# ping 172.16.33.3

! R4 does not have a mapping to route "owned" by R3 so a resolution request will be sent to R5 (NHRP server) first

NHRP: Setting 'used' flag on cache entry with nhop: 172.17.70.5

NHRP: NHRP successfully mapped '172.17.70.5' to NBMA '10.50.80.50'

NHRP: Enqueued NHRP Resolution Request for destination: 172.16.33.3

NHRP: Checking for delayed event NULL/172.16.33.3 on list (Tunnell).

NHRP: No node found.

NHRP: Enqueued NHRP Resolution Request for destination: 172.16.33.3

NHRP: Setting 'used' flag on cache entry with nhop: 172.17.70.5

NHRP: NHRP successfully mapped '172.17.70.5' to NBMA '10.50.80.50'

NHRP: Setting 'used' flag on cache entry with nhop: 172.17.70.5

NHRP: NHRP successfully mapped '172.17.70.5' to NBMA '10.50.80.50'

NHRP: Checking for delayed event NULL/172.16.33.3 on list (Tunnell).

NHRP: No node found.

NHRP-ATTR: Requester Ext Len: Total ext_len with NHRP attribute VPE 33

NHRP: Sending NHRP Resolution Request for dest: 172.16.33.3 to nexthop:
172.17.70.5 using our src: 172.17.70.4

NHRP: Receive Resolution Request via Tunnell vrf 0, packet size: 105

NHRP: netid_in = 70, to_us = 1

NHRP: nhrp_rtlookup for destination on 172.17.70.4 yielded interface Tunnell,
prefixlen 24

NHRP: nhrp_rtlookup on 172.17.70.4 yielded interface Tunnell, prefixlen 24

NHRP: Request was to us, responding with ouraddress

NHRP: Checking for delayed event 172.17.70.3/172.17.70.4 on list (Tunnell).

! Target device is R3 which is using 10.50.30.3, IPsec SAs required

NHRP: >>> nhrp_need_to_delay: ENQUEUED Delaying resolution request nbma
src:10.50.30.4 nbma dst:10.50.30.3 reason:IPSEC-IFC: need to wait for IPsec SAs.

NHRP-ATTR: In nhrp_cache_pak LINE: 1391

```
| First negotiate IKE SA between R3 and R4
ISAKMP:(0): SA request profile is (NULL)
ISAKMP: Created a peer struct for 10.50.30.3, peer port 500
ISAKMP: New peer created peer = 0xF06A2908 peer_handle = 0x80000017
ISAKMP: Locking peer struct 0xF06A2908, refcount 1 for isakmp_initiator
ISAKMP: local port 500, remote port 500
ISAKMP: set new node 0 to QM_IDLE
ISAKMP:(0):insert sa successfully sa = F227B4C8
ISAKMP:(0): processing SA payload. message ID = 0
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0):found peer pre-shared key matching 10.50.30.3
ISAKMP:(0): local preshared key found
ISAKMP : Scanning profiles for xauth ... ipv6
ISAKMP:(0):Checking ISAKMP transform 1 against priority 1 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP:(0):atts are acceptable. Next payload is 0
ISAKMP:(0):Acceptable atts:actual life: 0
ISAKMP:(0):Acceptable atts:life: 0
ISAKMP:(0):Fill atts in sa vpi_length:4
ISAKMP:(0):Fill atts in sa life_in_seconds:86400
ISAKMP:(0):Returning Actual lifetime: 86400
ISAKMP:(0)::Started lifetime timer: 86400.
```

```
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(0):Old State = IKE_I_MM2 New State = IKE_I_MM2

ISAKMP:(0): sending packet to 10.50.30.3 my_port 500 peer_port 500 (I) MM_SA_SETUP
ISAKMP:(0):Sending an IKE IPv4 Packet.
ISAKMP:(0):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(0):Old State = IKE_I_MM2 New State = IKE_I_MM3

ISAKMP (0): received packet from 10.50.30.3 dport 500 sport 500 Global (N) NEW SA
ISAKMP: Created a peer struct for 10.50.30.3, peer port 500
ISAKMP: New peer created peer = 0xF1EBFC00 peer_handle = 0x80000012
ISAKMP: Locking peer struct 0xF1EBFC00, refcount 1 for crypto_isakmp_process_block
ISAKMP: local port 500, remote port 500
ISAKMP:(0):insert sa successfully sa = F2232F30
ISAKMP:(0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(0):Old State = IKE_READY New State = IKE_R_MM1
ISAKMP:(0): processing SA payload. message ID = 0
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
ISAKMP (0): vendor ID is NAT-T v7
ISAKMP:(0): processing vendor id payload
```

```
ISAKMP:(0): vendor ID seems Unity/DPD but major 157 mismatch
ISAKMP:(0): vendor ID is NAT-T v3
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 123 mismatch
ISAKMP:(0): vendor ID is NAT-T v2
ISAKMP:(0):found peer pre-shared key matching 10.50.30.3
ISAKMP:(0): local preshared key found
ISAKMP : Scanning profiles for xauth ... ipv6
ISAKMP:(0):Checking ISAKMP transform 1 against priority 1 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP:(0):atts are acceptable. Next payload is 0
ISAKMP:(0):Acceptable atts:actual life: 0
ISAKMP:(0):Acceptable atts:life: 0
ISAKMP:(0):Fill atts in sa vpi_length:4
ISAKMP:(0):Fill atts in sa life_in_seconds:86400
ISAKMP:(0):Returning Actual lifetime: 86400
ISAKMP:(0)::Started lifetime timer: 86400.
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
ISAKMP (0): vendor ID is NAT-T v7
```

```
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 157 mismatch
ISAKMP:(0): vendor ID is NAT-T v3
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 123 mismatch
ISAKMP:(0): vendor ID is NAT-T v2
ISAKMP:(0):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(0):Old State = IKE_R_MM1 New State = IKE_R_MM1
ISAKMP:(0): constructed NAT-T vendor-rfc3947 ID
ISAKMP:(0): sending packet to 10.50.30.3 my_port 500 peer_port 500 (R) MM_SA_SETUP
ISAKMP:(0):Sending an IKE IPv4 Packet.
ISAKMP:(0):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(0):Old State = IKE_R_MM1 New State = IKE_R_MM2
ISAKMP (0): received packet from 10.50.30.3 dport 500 sport 500 Global (I)
MM_SA_SETUP
ISAKMP:(0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(0):Old State = IKE_I_MM3 New State = IKE_I_MM4
ISAKMP:(0): processing KE payload. message ID = 0
ISAKMP:(0): processing NONCE payload. message ID = 0
ISAKMP:(0):found peer pre-shared key matching 10.50.30.3
ISAKMP:(1057): processing vendor id payload
ISAKMP:(1057): vendor ID is Unity
ISAKMP:(1057): processing vendor id payload
ISAKMP:(1057): vendor ID is DPD
ISAKMP:(1057): processing vendor id payload
ISAKMP:(1057): speaking to another IOS box!
```



```
ISAKMP:received payload type 20
ISAKMP (1057): His hash no match - this node outside NAT
ISAKMP:received payload type 20
ISAKMP (1057): No NAT Found for self or peer
ISAKMP:(1057):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1057):Old State = IKE_I_MM4 New State = IKE_I_MM4
ISAKMP (1057): received packet from 10.50.30.3 dport 500 sport 500 Global (I)
MM_KEY_EXCH
ISAKMP:(1057): processing ID payload. message ID = 0
ISAKMP (1057): ID payload
    next-payload : 8
    type          : 1
    address       : 10.50.30.3
    protocol      : 17
    port          : 500
    length        : 12
ISAKMP:(0):: peer matches *none* of the profiles
ISAKMP:(1057): processing HASH payload. message ID = 0
ISAKMP:(1057):SA authentication status:
    authenticated
ISAKMP:(1057):SA has been authenticated with 10.50.30.3
ISAKMP: Trying to insert a peer 10.50.30.4/10.50.30.3/500/, and inserted
    successfully F06A2908.
ISAKMP:(1057):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(1057):Old State = IKE_I_MM5 New State = IKE_I_MM6

ISAKMP:(1057):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1057):Old State = IKE_I_MM6 New State = IKE_I_MM6
ISAKMP:(1057):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(1057):Old State = IKE_I_MM6 New State = IKE_P1_COMPLETE
```

```
ISAKMP:(1057):beginning Quick Mode exchange, M-ID of 129959729
ISAKMP:(1057):QM Initiator gets spi
ISAKMP:(1057): sending packet to 10.50.30.3 my_port 500 peer_port 500 (I) QM_IDLE
ISAKMP:(1057):Sending an IKE IPv4 Packet.
ISAKMP:(1057):Node 129959729, Input = IKE_MSG_INTERNAL, IKE_INIT_QM
ISAKMP:(1057):Old State = IKE_QM_READY New State = IKE_QM_I_QM1
ISAKMP:(1057):Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP:(1057):Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE
ISAKMP (1057): received packet from 10.50.30.3 dport 500 sport 500 Global (I)
  QM_IDLE
ISAKMP:(1057): processing HASH payload. message ID = 129959729
ISAKMP:(1057): processing SA payload. message ID = 129959729
ISAKMP:(1057):Checking IPsec proposal 1.
ISAKMP: transform 1, ESP_3DES
ISAKMP:  attributes in transform:
ISAKMP:  encaps is 2 (Transport)
ISAKMP:  SA life type in seconds
ISAKMP:  SA life duration (basic) of 3600
ISAKMP:  SA life type in kilobytes
ISAKMP:  SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:  authenticator is HMAC-MD5
ISAKMP:(1057):atts are acceptable.
ISAKMP:(1057): processing NONCE payload. message ID = 129959729
ISAKMP:(1057): processing ID payload. message ID = 129959729
ISAKMP:(1057): processing ID payload. message ID = 129959729
ISAKMP:(1057): sending packet to 10.50.30.3 my_port 500 peer_port 500 (I) QM_IDLE
ISAKMP:(1057):Sending an IKE IPv4 Packet.
ISAKMP:(1057):deleting node 129959729 error FALSE reason "No Error"
ISAKMP:(1057):Node 129959729, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
ISAKMP:(1057):Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE
! Once IPsec SAs have been created, NHRP mappings are updated on R4 to R3
NHRP: Adding Tunnel Endpoints (VPN: 172.17.70.3, NBMA: 10.50.30.3)
NHRP: Successfully attached NHRP subblock for Tunnel Endpoints (VPN: 172.17.70.3,
  NBMA: 10.50.30.3)
NHRP: Attempting to send packet via DEST 172.17.70.3
NHRP: Setting 'used' flag on cache entry with nhop: 172.17.70.3
NHRP: NHRP successfully mapped '172.17.70.3' to NBMA '10.50.30.3'
NHRP: Encapsulation succeeded.  Sending NHRP Control Packet  NBMA Address:
  10.50.30.3
NHRP: Send Resolution Reply via Tunnell vrf 0, packet size: 133
  src: 172.17.70.4, dst: 172.17.70.3
NHRP: 161 bytes out Tunnell
R4# ping 172.16.33.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.33.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/7/9 ms
R4#
```

R4# show crypto session

Crypto session current status

Interface: Tunnel1

Session status: UP-ACTIVE

Peer: 10.50.80.50 port 4500

IKEv1 SA: local 10.50.30.4/4500 remote 10.50.80.50/4500 Active

IPSEC FLOW: permit 47 host 10.50.30.4 host 10.50.80.50

Active SAs: 2, origin: crypto map

R3# show crypto session

Crypto session current status

Interface: Tunnel1

Session status: UP-ACTIVE

Peer: 10.50.80.50 port 4500

IKEv1 SA: local 10.50.30.3/4500 remote 10.50.80.50/4500 Active

IPSEC FLOW: permit 47 host 10.50.30.3 host 10.50.80.50

Active SAs: 2, origin: crypto map

R4# show crypto session

Crypto session current status

Interface: Tunnel1

Session status: UP-ACTIVE

Peer: 10.50.30.3 port 500

IKEv1 SA: local 10.50.30.4/500 remote 10.50.30.3/500 Active

IKEv1 SA: local 10.50.30.4/500 remote 10.50.30.3/500 Active

IPSEC FLOW: permit 47 host 10.50.30.4 host 10.50.30.3

Active SAs: 4, origin: crypto map

R3# show crypto ipsec sa

interface: Tunnell

Crypto map tag: Tunnell-head-0, local addr 10.50.30.3

protected vrf: (none)

local ident (addr/mask/prot/port): (10.50.30.3/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.50.80.50/255.255.255.255/47/0)

current_peer 10.50.80.50 port 4500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 268072, #pkts encrypt: 268072, #pkts digest: 268072

#pkts decaps: 267087, #pkts decrypt: 267087, #pkts verify: 267087

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.50.30.3, remote crypto endpt.: 10.50.80.50

path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/1

current outbound spi: 0xACAB4234(2896904756)

PFS (Y/N): Y, DH group: none

inbound esp sas:

spi: 0xCDACB829(3450648617)

transform: esp-3des esp-md5-hmac ,

in use settings ={Transport UDP-Encaps, }

conn id: 727, flow_id: SW:727, sibling_flags 80000000, crypto map:
Tunnell-head-0

sa timing: remaining key lifetime (k/sec): (4246746/2900)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0xACAB4234(2896904756)

transform: esp-3des esp-md5-hmac ,

in use settings ={Transport UDP-Encaps, }

conn id: 728, flow_id: SW:728, sibling_flags 80000000, crypto map:
Tunnell-head-0

sa timing: remaining key lifetime (k/sec): (4246765/2900)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

R3# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 10.50.30.20 to network 0.0.0.0

```
O*E2 0.0.0.0/0 [110/1] via 10.50.30.20, 5d18h, Ethernet0/1
      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C      10.3.3.0/24 is directly connected, Loopback1
L      10.3.3.3/32 is directly connected, Loopback1
S      10.4.4.0/24 [1/0] via 10.50.30.20
C      10.50.30.0/24 is directly connected, Ethernet0/1
L      10.50.30.3/32 is directly connected, Ethernet0/1
O E2   10.50.90.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
O E2   10.50.100.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
       172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C      172.16.33.0/24 is directly connected, Loopback0
L      172.16.33.3/32 is directly connected, Loopback0
D      172.16.34.0/24 [90/27264000] via 172.17.70.5, 00:00:37, Tunnel1
D      172.16.35.0/24 [90/27008000] via 172.17.70.5, 00:00:37, Tunnel1
       172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      172.17.70.0/24 is directly connected, Tunnel1
L      172.17.70.3/32 is directly connected, Tunnel1
O E2   192.168.2.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
```

R3# ping 172.16.34.4

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.34.4, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 6/8/16 ms

R3# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 10.50.30.20 to network 0.0.0.0

```
O*E2 0.0.0.0/0 [110/1] via 10.50.30.20, 5d18h, Ethernet0/1
      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C      10.3.3.0/24 is directly connected, Loopback1
L      10.3.3.3/32 is directly connected, Loopback1
S      10.4.4.0/24 [1/0] via 10.50.30.20
C      10.50.30.0/24 is directly connected, Ethernet0/1
L      10.50.30.3/32 is directly connected, Ethernet0/1
O E2   10.50.90.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
O E2   10.50.100.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C      172.16.33.0/24 is directly connected, Loopback0
L      172.16.33.3/32 is directly connected, Loopback0
D %    172.16.34.0/24 [90/27264000] via 172.17.70.5, 00:00:54, Tunnel1
D      172.16.35.0/24 [90/27008000] via 172.17.70.5, 00:00:54, Tunnel1
      172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      172.17.70.0/24 is directly connected, Tunnel1
L      172.17.70.3/32 is directly connected, Tunnel1
O E2  192.168.2.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
```

R3# show ip nhrp

172.16.34.0/24 via 172.17.70.4

Tunnell created 00:01:20, expire 01:58:39

Type: dynamic, Flags: router rib nho

NBMA address: 10.50.30.4

172.17.70.3/32 via 172.17.70.3

Tunnell created 00:01:20, expire 01:58:39

Type: dynamic, Flags: router unique local

NBMA address: 10.50.30.3

(no-socket)

172.17.70.4/32 via 172.17.70.4

Tunnell created 00:01:20, expire 01:58:39

Type: dynamic, Flags: router implicit

NBMA address: 10.50.30.4

172.17.70.5/32 via 172.17.70.5

Tunnell created 1w6d, never expire

Type: static, Flags: used

NBMA address: 10.50.80.50

R4# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 10.50.30.20 to network 0.0.0.0

```
O*E2 0.0.0.0/0 [110/1] via 10.50.30.20, 5d18h, Ethernet0/1
      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
S      10.3.3.0/24 [1/0] via 10.50.30.20
C      10.4.4.0/24 is directly connected, Loopback1
L      10.4.4.4/32 is directly connected, Loopback1
C      10.50.30.0/24 is directly connected, Ethernet0/1
L      10.50.30.4/32 is directly connected, Ethernet0/1
O E2   10.50.90.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
O E2   10.50.100.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
       172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
D      172.16.33.0/24 [90/27264000] via 172.17.70.5, 00:05:38, Tunnel1
C      172.16.34.0/24 is directly connected, Loopback0
L      172.16.34.4/32 is directly connected, Loopback0
D      172.16.35.0/24 [90/27008000] via 172.17.70.5, 00:05:38, Tunnel1
       172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      172.17.70.0/24 is directly connected, Tunnel1
L      172.17.70.4/32 is directly connected, Tunnel1
O E2   192.168.2.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
```

R4# ping 172.16.33.3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.33.3, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 5/6/7 ms

R4# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 10.50.30.20 to network 0.0.0.0

```
O*E2 0.0.0.0/0 [110/1] via 10.50.30.20, 5d18h, Ethernet0/1
      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
S      10.3.3.0/24 [1/0] via 10.50.30.20
C      10.4.4.0/24 is directly connected, Loopback1
L      10.4.4.4/32 is directly connected, Loopback1
C      10.50.30.0/24 is directly connected, Ethernet0/1
L      10.50.30.4/32 is directly connected, Ethernet0/1
O E2   10.50.90.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
O E2   10.50.100.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
D %    172.16.33.0/24 [90/27264000] via 172.17.70.5, 00:06:03, Tunnel1
C      172.16.34.0/24 is directly connected, Loopback0
L      172.16.34.4/32 is directly connected, Loopback0
D      172.16.35.0/24 [90/27008000] via 172.17.70.5, 00:06:03, Tunnel1
      172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      172.17.70.0/24 is directly connected, Tunnel1
L      172.17.70.4/32 is directly connected, Tunnel1
O E2   192.168.2.0/24 [110/20] via 10.50.30.20, 5d18h, Ethernet0/1
```

R4# show ip nhrp

172.16.33.0/24 via 172.17.70.3

Tunnell created 00:00:11, expire 01:59:48

Type: dynamic, Flags: router rib nho

NBMA address: 10.50.30.3

172.16.34.0/24 via 172.17.70.4

Tunnell created 00:05:21, expire 01:54:38

Type: dynamic, Flags: router unique local

NBMA address: 10.50.30.4

(no-socket)

172.17.70.3/32 via 172.17.70.3

Tunnell created 00:05:21, expire 01:54:38

Type: dynamic, Flags: router

NBMA address: 10.50.30.3

172.17.70.5/32 via 172.17.70.5

Tunnell created 5d20h, never expire

Type: static, Flags: used

NBMA address: 10.50.80.50

R4# show dmvpn detail

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete

N - NATed, L - Local, X - No Socket

Ent --> Number of NHRP entries with same NBMA peer

NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting

UpDn Time --> Up or Down Time for a Tunnel

Interface Tunnel1 is up/up, Addr. is 172.17.70.4, VRF ""

Tunnel Src./Dest. addr: 10.50.30.4/MGRE, Tunnel VRF ""

Protocol/Transport: "multi-GRE/IP", Protect "DMVPN"

Interface State Control: Disabled

nhrp event-publisher : Disabled

IPv4 NHS:

172.17.70.5 RE priority = 0 cluster = 0

Type:Spoke, Total NBMA Peers (v4/v6): 3

# Ent	Peer NBMA Addr	Peer Tunnel Add	State	UpDn Tm	Attrb	Target Network
2	10.50.30.3	172.17.70.3	UP	00:06:18	DT2	172.16.33.0/24
0	10.50.30.3	172.17.70.3	UP	00:06:18	D	172.17.70.3/32
1	10.50.30.4	172.17.70.4	UP	00:06:18	DLX	172.17.70.4/32
1	10.50.80.50	172.17.70.5	UP	02:41:45	S	172.17.70.5/32

Crypto Session Details:

Interface: Tunnell

Session: [0xF2284140]

IKEv1 SA: local 10.50.30.4/500 remote 10.50.30.3/500 Active

Capabilities:(none) connid:1060 lifetime:23:53:41

IKEv1 SA: local 10.50.30.4/500 remote 10.50.30.3/500 Active

Capabilities:(none) connid:1059 lifetime:23:53:41

Crypto Session Status: UP-ACTIVE

fvrfr: (none), Phase1_id: 10.50.30.3

IPSEC FLOW: permit 47 host 10.50.30.4 host 10.50.30.3

Active SAs: 4, origin: crypto map

Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 4264509/3221

Outbound: #pkts enc'ed 1 drop 0 life (KB/Sec) 4264509/3221

Outbound SPI : 0xF540025B, transform : esp-3des esp-md5-hmac

Socket State: Open

Interface: Tunnell

Session: [0xF2284238]

IKEv1 SA: local 10.50.30.4/4500 remote 10.50.80.50/4500 Active

Capabilities:N connid:1056 lifetime:21:18:13

Crypto Session Status: UP-ACTIVE

fvrfr: (none), Phase1_id: 10.50.90.5

IPSEC FLOW: permit 47 host 10.50.30.4 host 10.50.80.50

Active SAs: 2, origin: crypto map

Inbound: #pkts dec'ed 4144 drop 0 life (KB/Sec) 4269546/853

Outbound: #pkts enc'ed 2115 drop 0 life (KB/Sec) 4269770/853

Outbound SPI : 0x C24F6A, transform : esp-3des esp-md5-hmac

Socket State: Open

Pending DMVPN Sessions:

```
crypto isakmp policy 10
  encr 3des
  authentication pre-share
  group 2
crypto isakmp key cisco address 0.0.0.0
!
!
crypto ipsec transform-set dmvpn esp-3des esp-md5-hmac
  mode transport
!
crypto ipsec profile DMVPN
  set transform-set dmvpn
!

interface Loopback0
  ip address 172.16.35.5 255.255.255.0

interface Tunnell
  ip address 172.17.70.5 255.255.255.0
  no ip redirects
  ip mtu 1360
  ip nhrp authentication cisco
  ip nhrp map multicast dynamic
  ip nhrp network-id 70
  ip nhrp holdtime 300
  ip nhrp redirect
  no ip split-horizon eigrp 123
  delay 1000
  tunnel source Ethernet0/0
  tunnel mode gre multipoint
  tunnel key 123
  tunnel protection ipsec profile DMVPN

router eigrp 123
  network 172.16.35.0 0.0.0.255
  network 172.17.70.0 0.0.0.255
```

```
crypto isakmp policy 10
  encr 3des
  authentication pre-share
  group 2
crypto isakmp key cisco address 0.0.0.0
!
!
crypto ipsec transform-set dmvpn esp-3des esp-md5-hmac
  mode transport
!
crypto ipsec profile DMVPN
  set transform-set dmvpn
!

interface Loopback0
  ip address 172.16.33.3 255.255.255.0

interface Tunnell
  ip address 172.17.70.3 255.255.255.0
  no ip redirects
  ip nhrp authentication cisco
  ip nhrp map 172.17.70.5 10.50.80.50
  ip nhrp map multicast 10.50.80.50
  ip nhrp network-id 70
  ip nhrp nhs 172.17.70.5
  ip nhrp shortcut
  tunnel source Ethernet0/1
  tunnel mode gre multipoint
  tunnel key 123
  tunnel protection ipsec profile DMVPN

router eigrp 123
  network 172.16.33.0 0.0.0.255
  network 172.17.70.0 0.0.0.255
```

```
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
crypto isakmp key cisco address 0.0.0.0
!
!
crypto ipsec transform-set dmvpn esp-3des esp-md5-hmac
  mode transport
!
crypto ipsec profile DMVPN
  set transform-set dmvpn
!

interface Loopback0
  ip address 172.16.34.4 255.255.255.0

interface Tunnell
  ip address 172.17.70.4 255.255.255.0
  no ip redirects
  ip nhrp authentication cisco
  ip nhrp map 172.17.70.5 10.50.80.50
  ip nhrp map multicast 10.50.80.50
  ip nhrp network-id 70
  ip nhrp nhs 172.17.70.5
  ip nhrp shortcut
  tunnel source Ethernet0/1
  tunnel mode gre multipoint
  tunnel key 123
  tunnel protection ipsec profile DMVPN

router eigrp 123
  network 172.16.34.0 0.0.0.255
  network 172.17.70.0 0.0.0.255
```



```
access-list 101 permit udp any any eq 4500
access-list 101 permit esp any any
access-group 101 in interface outside
```

```
! HUB
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp network-id 123
 no ip split-horizon eigrp 123
 ip summary-address eigrp 123 0.0.0.0 0.0.0.0 5
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel key 123
```

```
! SPOKE
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 ip nhrp authentication cisco
 ip nhrp map multicast 150.1.1.1
 ip nhrp map 10.0.0.1 150.1.1.1
 ip nhrp nhs 10.0.0.1
 ip nhrp network-id 123
 ip nhrp registration timeout 30
 ip nhrp holdtime 60
 tunnel source Loopback0
 tunnel destination 150.1.1.1
 tunnel key 123
```

```
! HUB
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp network-id 123
 no ip split-horizon eigrp 123
 no ip next-hop-self eigrp 123
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel key 123
```

```
! SPOKE
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 ip nhrp authentication cisco
 ip nhrp map multicast 150.1.1.1
 ip nhrp map 10.0.0.1 150.1.1.1
 ip nhrp nhs 10.0.0.1
 ip nhrp network-id 123
 ip nhrp registration timeout 30
 ip nhrp holdtime 60
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel key 123
```

```
! HUB
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp network-id 123
 no ip split-horizon eigrp 123
 ip nhrp redirect
 ip summary-address eigrp 123 0.0.0.0 0.0.0.0 5
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel key 123
```

```
! SPOKE
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 ip nhrp authentication cisco
 ip nhrp map multicast 150.1.1.1
 ip nhrp map 10.0.0.1 150.1.1.1
 ip nhrp nhs 10.0.0.1
 ip nhrp shortcut
 ip nhrp network-id 123
 ip nhrp registration timeout 30
 ip nhrp holdtime 60
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel key 123
```

(WLC) >show ap summary

Number of APs..... 2

Global AP User Name..... cisco

Global AP Dot1x User Name..... Not Configured

AP Name	Slots	AP Model	Ethernet MAC	Location	Port
AP1cdf.0f94.8063	2	AIR-CAP3502I-A-K9	1c:df:0f:94:80:63	default location	1
AP588d.0959.4921	2	AIR-LAP1262N-A-K9	58:8d:09:59:49:21	default location	1

(WLC) >show time

Time..... Thu Aug 15 03:04:41 2013

Timezone delta..... 0:0

Timezone location.....

NTP Servers

NTP Polling Interval..... 6000

Index	NTP Key Index	NTP Server	NTP Msg Auth Status
1	0	192.168.2.5	AUTH DISABLED

(WLC) >show radius summary

Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..... lower
Call Station Id Type..... Mac Address
Aggressive Failover..... Enabled
Keywrap..... Disabled
Fallback Test:
 Test Mode..... Off
 Probe User Name..... cisco-probe
 Interval (in seconds)..... 300
MAC Delimiter for Authentication Messages..... hyphen
MAC Delimiter for Accounting Messages..... hyphen

Authentication Servers

Idx	Type	Server Address	Port	State	Tout	MgmtTout	RFC3576	IPSec	-
1	NM	192.168.2.15	1812	Enabled	2	2	Disabled	Disabled	-

(WLC) >show wlan summary

Number of WLANs..... 3

WLAN ID	WLAN Profile Name / SSID	Status	Interface Name
1	admin / admin	Enabled	management
2	guest / guest	Enabled	guest-wlan
3	employee / employee	Enabled	employee-wlan

(WLC) >show interface summary

Interface Name	Port	Vlan Id	IP Address	Type	Ap Mgr	Guest
employee-wlan	1	110	10.10.110.2	Dynamic	No	No
guest-wlan	1	120	10.10.120.2	Dynamic	No	No
management	1	100	10.50.100.10	Static	Yes	No
service-port	N/A	N/A	0.0.0.0	DHCP	No	No
virtual	N/A	N/A	1.1.1.1	Static	No	No

(WLC) >show wlan 2

WLAN Identifier..... 2
Profile Name..... Guest
Network Name (SSID)..... Guest
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Enabled
AAA Policy Override..... Disabled
Network Admission Control


```

Client Profiling Status ..... Disabled
Radius-NAC State..... Disabled
SNMP-NAC State..... Disabled
Quarantine VLAN..... 0
Maximum number of Associated Clients..... 0
Maximum number of Clients per AP Radio..... 200
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... 1800 seconds
CHD per WLAN..... Enabled
Webauth DHCP exclusion..... Disabled
Interface..... guest-wlan
Radius Servers
  Authentication..... 192.168.2.15 1812
  Accounting..... Global Servers
    Interim Update..... Disabled
  Dynamic Interface..... Disabled
Local EAP Authentication..... Disabled
Security

802.11 Authentication:..... Open System
FT Support..... Disabled
Static WEP Keys..... Disabled
802.1X..... Disabled
Wi-Fi Protected Access (WPA/WPA2)..... Disabled
Wi-Fi Direct policy configured..... Disabled
EAP-Passthrough..... Disabled
CKIP ..... Disabled
Web Based Authentication..... Enabled

```

```

Client Profiling Status ..... Disabled
Radius-NAC State..... Disabled
SNMP-NAC State..... Disabled
Quarantine VLAN..... 0
Maximum number of Associated Clients..... 0
Maximum number of Clients per AP Radio..... 200
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... 1800 seconds
CHD per WLAN..... Enabled
Webauth DHCP exclusion..... Disabled
Interface..... guest-wlan
Radius Servers
  Authentication..... 192.168.2.15 1812
  Accounting..... Global Servers
    Interim Update..... Disabled
  Dynamic Interface..... Disabled
Local EAP Authentication..... Disabled
Security

802.11 Authentication:..... Open System
FT Support..... Disabled
Static WEP Keys..... Disabled
802.1X..... Disabled
Wi-Fi Protected Access (WPA/WPA2)..... Disabled
Wi-Fi Direct policy configured..... Disabled
EAP-Passthrough..... Disabled
CKIP ..... Disabled
Web Based Authentication..... Enabled

```

```

Client Profiling Status ..... Disabled
Radius-NAC State..... Disabled
SNMP-NAC State..... Disabled
Quarantine VLAN..... 0
Maximum number of Associated Clients..... 0
Maximum number of Clients per AP Radio..... 200
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... 1800 seconds
CHD per WLAN..... Enabled
Webauth DHCP exclusion..... Disabled
Interface..... guest-wlan
Radius Servers
  Authentication..... 192.168.2.15 1812
  Accounting..... Global Servers
    Interim Update..... Disabled
  Dynamic Interface..... Disabled
Local EAP Authentication..... Disabled
Security

802.11 Authentication:..... Open System
FT Support..... Disabled
Static WEP Keys..... Disabled
802.1X..... Disabled
Wi-Fi Protected Access (WPA/WPA2)..... Disabled
Wi-Fi Direct policy configured..... Disabled
EAP-Passthrough..... Disabled
CKIP ..... Disabled
Web Based Authentication..... Enabled

```

```

Client Profiling Status ..... Disabled
Radius-NAC State..... Disabled
SNMP-NAC State..... Disabled
Quarantine VLAN..... 0
Maximum number of Associated Clients..... 0
Maximum number of Clients per AP Radio..... 200
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... 1800 seconds
CHD per WLAN..... Enabled
Webauth DHCP exclusion..... Disabled
Interface..... guest-wlan
Radius Servers
  Authentication..... 192.168.2.15 1812
  Accounting..... Global Servers
    Interim Update..... Disabled
  Dynamic Interface..... Disabled
Local EAP Authentication..... Disabled
Security

802.11 Authentication:..... Open System
FT Support..... Disabled
Static WEP Keys..... Disabled
802.1X..... Disabled
Wi-Fi Protected Access (WPA/WPA2)..... Disabled
Wi-Fi Direct policy configured..... Disabled
EAP-Passthrough..... Disabled
CKIP ..... Disabled
Web Based Authentication..... Enabled

```

(WLC) >show netuser summary

User Name	WLAN Id	User Type	Lifetime	Description
-----	-----	-----	-----	-----
guest1	Any	Permanent	N/A	
guest	WLAN	2 Guest	Infinity	

```
config time ntp server 1 192.168.2.5
config radius auth add 1 192.168.2.15 1812 ascii cisco

interface create employee-wlan 110
interface address dynamic-interface employee-wlan 10.10.110.2 255.255.255.0
  10.10.110.1
interface dhcp dynamic-interface employee-wlan primary 10.10.110.1
interface port employee-wlan 1

interface create guest-wlan 120
interface address dynamic-interface guest-wlan 10.10.120.2 255.255.255.0
  10.10.120.1
interface dhcp dynamic-interface guest-wlan primary 10.10.120.1
interface port guest-wlan 1

wlan create 3 employee employee
wlan create 2 guest guest

wlan security wpa disable 3
wlan security web-auth enable 2

wlan security wpa wpa2 ciphers aes enable 3
wlan security wpa akm 802.1x enable 3

wlan interface 3 employee-wlan
wlan interface 2 guest-wlan
wlan enable all

config netuser add guest cisco wlan 2 userType guest lifetime 0
```

ASA1/c2

```
access-list 101 extended permit udp any any eq 5246
access-list 101 extended permit udp any any eq 5247
```

```
R1# show ip http server status
```

```
HTTP server status: Enabled
```

```
HTTP server port: 80
```

```
ASA1/c2# show run | include www
```

```
access-list 101 extended permit tcp any any eq www
```



```
R1# show ntp stat
```

```
Clock is synchronized, stratum 4, reference is 10.50.70.5
```

```
R1# show cry key mypubkey rsa
% Key pair was generated at: 22:12:36 UTC Jul 17 2012
Key name: ciscoca
Key type: RSA KEYS
Storage Device: private-config
Usage: General Purpose Key
Key is exportable.
```

R1# show cry pki certificates

CA Certificate

Status: Available

Certificate Serial Number (hex): 01

Certificate Usage: Signature

Issuer:

cn=ciscoca.cisco.com L=cisco C=US

Subject:

cn=ciscoca.cisco.com L=cisco C=US

Validity Date:

start date: 13:19:37 PST Aug 17 2013

end date: 13:19:37 PST Aug 17 2014

Associated Trustpoints: ciscoca

Storage: nvram:ciscocacisco#1CA.cer

```
R1#(config)crypto pki server ciscoca  
no shutdown
```

```
R1# show crypto pki server
```

```
Certificate Server ciscoca:
```

```
  Status: enabled
```

```
  State: enabled
```

```
  Server's configuration is locked (enter "shut" to unlock it)
```

```
  Issuer name: CN=ciscoca.cisco.com L=cisco C=US
```

```
  CA cert fingerprint: 1F5A02E4 C2C8230A 56FC15BB CBDFBEF6
```

```
  Granting mode is: auto
```

```
  Last certificate issued serial number (hex): 1
```

```
  CA certificate expiration timer: 13:19:37 PST Aug 17 2014
```

```
  CRL NextUpdate timer: 13:10:07 PST Sep 8 2013
```

```
  Current primary storage dir: nvram:
```

```
  Database Level: Minimum - no cert data written to storage
```

```
crypto key generate rsa general-keys label ciscoca exportable
!
crypto key export rsa ciscoca pem url nvram: 3des cisco123
!

crypto pki server ciscoca
  issuer-name CN=ciscoca.cisco.com L=cisco C=US
  grant auto
  lifetime crl 24
  lifetime certificate 200
  lifetime ca-certificate 365
crypto pki token default removal timeout 0
!
crypto pki trustpoint ciscoca
  revocation-check crl
  rsakeypair ciscoca
!
!
crypto pki certificate chain ciscoca
  certificate ca 01
  <cert omitted>
```

```
access-list 101 permit tcp any any eq www
access-group 101 in interface outside
```

```
IPS# packet display gigabitEthernet0/3
Warning: This command will cause significant performance degradation
tcpdump: WARNING: ge0_3: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_3, link-type EN10MB (Ethernet), capture size 65535 bytes
03:29:29.669296 IP 10.50.77.5 > 224.0.0.5: OSPFv2, Hello, length: 56
03:29:29.669299 IP 10.50.77.5 > 224.0.0.5: OSPFv2, Hello, length: 56
03:29:29.669302 IP 10.50.77.5 > 224.0.0.5: OSPFv2, Hello, length: 56
03:29:31.410995 IP 10.50.100.10.5247 > 10.50.77.164.38035: UDP, length 76
03:29:31.550785 IP 10.50.9.5 > 224.0.0.5: OSPFv2, Hello, length: 56
03:29:31.550788 IP 10.50.9.5 > 224.0.0.5: OSPFv2, Hello, length: 56
03:29:31.550790 IP 10.50.9.5 > 224.0.0.5: OSPFv2, Hello, length: 56
03:29:39.472161 IP 10.50.77.5 > 224.0.0.5: OSPFv2, Hello, length: 56
03:29:39.472165 IP 10.50.77.5 > 224.0.0.5: OSPFv2, Hello, length: 56
03:29:39.472167 IP 10.50.77.5 > 224.0.0.5: OSPFv2, Hello, length: 56
03:29:40.621245 IP 10.50.9.5 > 224.0.0.5: OSPFv2, Hello, length: 56
03:29:40.621249 IP 10.50.9.5 > 224.0.0.5: OSPFv2, Hello, length: 56
03:29:40.621251 IP 10.50.9.5 > 224.0.0.5: OSPFv2, Hello, length: 56
03:29:41.874175 CDPv2, ttl: 180s, Device-ID ''AP588d.0959.4921'', length 378
14 packets captured
14 packets received by filter
0 packets dropped by kernel
```

SW2# show monitor detail

Session 1

Type	:	Local Session
Description	:	-
Source Ports	:	
RX Only	:	None
TX Only	:	None
Both	:	None
Source VLANs	:	
RX Only	:	None
TX Only	:	None
Both	:	9,77
Source RSPAN VLAN	:	None
Destination Ports	:	Gil/0/17
Encapsulation	:	Native
Ingress	:	Disabled
Filter VLANs	:	None
Dest RSPAN VLAN	:	None
IP Access-group	:	None
MAC Access-group	:	None
Ipv6 Access-group	:	None


```
monitor session 1 source vlan 77
monitor session 1 source vlan 9
monitor session 1 destination interface Gi1/0/17
```

R1# show crypto session

Interface: Ethernet0/0

Session status: UP-NO-IKE

Peer: FF02::5 port 500

IPSEC FLOW: permit 89 FE80::/10 ::/0

Active SAs: 2, origin: manual-keyed crypto map

R1# show crypto ipsec sa

interface: Ethernet0/0

Crypto map tag: Ethernet0/0-OSPF-MAP, local addr FE80::A8BB:CCFF:FE00:7900

IPsecv6 policy name: OSPFv3-500

protected vrf: (none)

local ident (addr/mask/prot/port): (FE80::/10/89/0)

remote ident (addr/mask/prot/port): (::/0/89/0)

current_peer FF02::5 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 141261, #pkts encrypt: 141261, #pkts digest: 141261

#pkts decaps: 141130, #pkts decrypt: 141130, #pkts verify: 141130

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: FE80::A8BB:CCFF:FE00:7900,

remote crypto endpt.: FF02::5

path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb Ethernet0/0

current outbound spi: 0x1F4(500)

PFS (Y/N): N, DH group: none

```
inbound esp sas:
  spi: 0x1F4(500)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 1, flow_id: SW:1, sibling_flags 80000001, crypto map:
      Ethernet0/0-OSPF-MAP
sa timing: remaining key lifetime (sec): (0)
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: N
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x1F4(500)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Transport, }
    conn id: 2, flow_id: SW:2, sibling_flags 80000001, crypto map:
      Ethernet0/0-OSPF-MAP
sa timing: remaining key lifetime (sec): (0)
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: N
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas
```

R1# show ipv6 route

IPv6 Routing Table - default - 7 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
l - LISP
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

```
C 2001:128:BAD:64::/64 [0/0]
  via Ethernet0/0, directly connected
L 2001:128:BAD:64::1/128 [0/0]
  via Ethernet0/0, receive
C 3001:0:1:3::/64 [0/0]
  via Loopback1, directly connected
L 3001:0:1:3::/128 [0/0]
  via Loopback1, receive
L 3001:0:1:3:A8BB:CCFF:FE00:7900/128 [0/0]
  via Loopback1, receive
OE2 3001:0:2:3::/64 [110/20]
  via FE80::A8BB:CCFF:FE00:7A00, Ethernet0/0
L FF00::/8 [0/0]
  via Null0, receive
```

R2# show ipv6 route

IPv6 Routing Table - default - 6 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
l - LISP
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

```
C 2001:128:BAD:64::/64 [0/0]
  via Ethernet0/0.1, directly connected
L 2001:128:BAD:64::2/128 [0/0]
  via Ethernet0/0.1, receive
OE2 3001:0:1:3::/64 [110/20]
  via FE80::A8BB:CCFF:FE00:7900, Ethernet0/0.1
C 3001:0:2:3::/64 [0/0]
  via Loopback1, directly connected
L 3001:0:2:3:A8BB:CCFF:FE00:7A00/128 [0/0]
  via Loopback1, receive
L FF00::/8 [0/0]
  via Null0, receive
```

```
ipv6 router ospf 21
  area 0 encryption ipsec spi 500 esp 3des
1234567890123456789012345678901234567890ABCDEF12 sha1 123456789012345678901234567
8901234567890
  redistribute connected

interface Loopback1
  ipv6 address 3001:0:1:3::/64 eui-64

interface Ethernet0/0
  ipv6 address 2001:128:BAD:64::1/64
  ipv6 ospf 21 area 0
  ipv6 enable
```

```
interface Loopback1
  ipv6 address 3001:0:2:3::/64 eui-64

interface Ethernet0/0.1
  ipv6 address 2001:128:BAD:64::2/64
  ipv6 ospf 21 area 0
  ipv6 enable

ipv6 router ospf 21
  area 0 encryption ipsec spi 500 esp 3des
1234567890123456789012345678901234567890ABCDEF12 sha1 123456789012345678901234567
8901234567890
  redistribute connected
```

```
R7# show access-list
Extended IP access list coppacl-VPN
  10 permit udp any any eq isakmp (1906 matches)
Extended IP access list coppacl-bgp
  10 permit tcp host 10.50.70.6 host 10.50.40.7 eq bgp (42748 matches)
  20 permit tcp host 10.50.70.6 eq bgp host 10.50.40.7 (71312 matches)
Extended IP access list coppacl-igp
  10 permit ospf any host 224.0.0.5 (158592 matches)
  20 permit ospf any host 224.0.0.6 (59 matches)
  30 permit ospf any any (123 matches)
Extended IP access list coppacl-management
  10 permit tcp 10.50.0.0 0.0.255.255 any eq telnet (72 matches)
  20 permit udp host 10.50.70.5 any eq ntp (18865 matches)
  30 permit tcp 192.168.2.0 0.0.0.255 any eq www (128 matches)
  40 permit tcp 192.168.2.0 0.0.0.255 any eq 443
  50 permit udp host 192.168.2.25 eq domain any (14 matches)
Extended IP access list coppacl-undesirable
  10 deny tcp any any fragments
  20 deny icmp any any fragments (10 matches)
IPv6 access list coppacl-VPNv6
  permit udp any any eq isakmp (60 matches) sequence 1
```

R7# show class-map

Class Map match-any coppclass-VPN (id 9)

Match access-group name coppacl-VPN

Match access-group name coppacl-VPNv6

Class Map match-all coppclass-layer2 (id 10)

Match protocol arp

Class Map match-any class-default (id 0)

Match any

Class Map match-all coppclass-igp (id 7)

Match access-group name coppacl-igp

Class Map match-all coppclass-undesirable (id 11)

Match access-group name coppacl-undesirable

Class Map match-all coppclass-bgp (id 1)

Match access-group name coppacl-bgp

Class Map match-any coppclass-management (id 8)

Match access-group name coppacl-management

R7# show policy-map control-plane

Control Plane

Service-policy input: copp-policy

Class-map: coppclass-bgp (match-all)
56964 packets, 4758874 bytes
5 minute offered rate 0 bps
Match: access-group name coppacl-bgp

Class-map: coppclass-igp (match-all)
158611 packets, 15826230 bytes
5 minute offered rate 0 bps
Match: access-group name coppacl-igp

Class-map: coppclass-management (match-any)
9537 packets, 859270 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group name coppacl-management
9535 packets, 859090 bytes
5 minute rate 0 bps
police:
rate 125 pps, burst 30 packets
conformed 9537 packets, 9537 bytes; actions:
transmit
exceeded 0 packets, 0 bytes; actions:
transmit
conformed 0 pps, exceeded 0 pps

```
Class-map: coppclass-VPN (match-any)
  1007 packets, 186541 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group name coppacl-VPN
  947 packets, 178425 bytes
  5 minute rate 0 bps
Match: access-group name coppacl-VPNv6
  60 packets, 8116 bytes
  5 minute rate 0 bps
police:
  rate 250 pps, burst 61 packets
  conformed 1007 packets, 1007 bytes; actions:
    transmit
  exceeded 0 packets, 0 bytes; actions:
    transmit
  conformed 0 pps, exceeded 0 pps
```

```
Class-map: coppclass-layer2 (match-all)
  38523 packets, 2311380 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
Match: protocol arp
police:
  rate 20 pps, burst 4 packets
  conformed 38523 packets, 38523 bytes; actions:
    transmit
  exceeded 0 packets, 0 bytes; actions:
    transmit
  conformed 0 pps, exceeded 0 pps
```

```
Class-map: coppclass-undesirable (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: access-group name coppacl-undesirable
  police:
    rate 10 pps, burst 2 packets
    conformed 0 packets, 0 bytes; actions:
      drop
    exceeded 0 packets, 0 bytes; actions:
      drop
    conformed 0 pps, exceeded 0 pps
```

```
Class-map: class-default (match-any)
  279559 packets, 35570430 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any
  police:
    rate 25 pps, burst 6 packets
    conformed 279464 packets, 279464 bytes; actions:
      transmit
    exceeded 95 packets, 95 bytes; actions:
      drop
    conformed 0 pps, exceeded 0 pps
```

```
class-map match-all coppclass-bgp
match access-group name coppacl-bgp
class-map match-all coppclass-igp
match access-group name coppacl-igp
class-map match-any coppclass-management
match access-group name coppacl-management
class-map match-any coppclass-VPN
match access-group name coppacl-VPN
match access-group name coppacl-VPNv6
class-map match-all coppclass-layer2
match protocol arp
class-map match-all coppclass-undesirable
match access-group name coppacl-undesirable
```

```
policy-map copp-policy
class coppclass-bgp
class coppclass-igp
class coppclass-management
police rate 125 pps conform-action transmit exceed-action transmit
class coppclass-VPN
police rate 250 pps conform-action transmit exceed-action transmit
class coppclass-layer2
police rate 20 pps conform-action transmit exceed-action transmit
class coppclass-undesirable
police rate 10 pps conform-action drop exceed-action drop
class class-default
police rate 25 pps conform-action transmit exceed-action drop
```

```
ip access-list extended coppacl-VPN
 permit udp any any eq isakmp
ip access-list extended coppacl-bgp
 permit tcp host 10.50.70.6 host 10.50.40.7 eq bgp
 permit tcp host 10.50.70.6 eq bgp host 10.50.40.7
ip access-list extended coppacl-igp
 permit ospf any host 224.0.0.5
 permit ospf any host 224.0.0.6
 permit ospf any any
ip access-list extended coppacl-management
 permit tcp 10.50.0.0 0.0.255.255 any eq telnet
 permit udp host 10.50.70.5 any eq ntp
 permit tcp 192.168.2.0 0.0.0.255 any eq www
 permit tcp 192.168.2.0 0.0.0.255 any eq 443
 permit udp host 192.168.2.25 eq domain any
ip access-list extended coppacl-undesirable
 deny tcp any any fragments
 deny icmp any any fragments
```

```
control-plane
 service-policy input copp-policy
```

control-plane

service-policy input | output policy-map-name

control-plane host *option*

cef-exception Cef-exception traffic control-plane configuration

host Host traffic control-plane configuration

transit Transit traffic control-plane configuration

service-policy input | output *policy-map-name*

```
R2# telnet 10.50.40.7
Trying 10.50.40.7 ... Open
```

```
User Access Verification
```

```
Username: cisco
```

```
Password: cisco
```

```
R7# exit
```

```
R7# show management-interface
```

```
Management interface GigabitEthernet0/1
```

Protocol	Packets processed
http	0
telnet	36

```
!R7
```

```
control-plane host
```

```
management-interface GigabitEthernet0/1 allow http telnet
```


(WLC) >show wlan 3

```
WLAN Identifier..... 3
Profile Name..... employee
Network Name (SSID)..... employee
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Disabled
```

(WLC) >show rogue rule summary

Priority	Rule Name	State	Type	Match	Hit	Count
1	RogueAP	Enabled	Malicious	Any	0	

(WLC) >show rogue rule detailed RogueAP

Priority..... 1
Rule Name..... RogueAP
State..... Enabled
Type..... Malicious
Match Operation..... Any
Hit Count..... 0
Total Conditions..... 2
Condition 1
 type..... Client-count
 value..... 1
Condition 2
 type..... No-encryption
 value..... Enabled

```
R2# show arp
Internet 10.50.100.51          0 1cdf.0f94.8063 ARPA Ethernet0/0.1
```

```
(WLC) >show rogue ap friendly summary
```

```
Number of APs..... 1
```

MAC Address	State	# APs	# Clients	Last Heard
-----	-----	-----	-----	-----
1c:df:0f:94:80:63	Internal	0	0	Not Heard

```
(WLC) >show wps mfp summary
```

```
Global Infrastructure MFP state..... Enabled  
Controller Time Source Valid..... False
```

(WLC) >show ap link-encryption all

AP Name	Encryption State	Dnstream Count	Upstream Count	Last Update
AP588d.0959.4921	Dis	0	0	5:12
AP1cdf.0f94.8063	En	0	0	Never

(WLC) >show dtls connections

AP Name	Local Port	Peer IP	Peer Port	Ciphersuite
AP588d.0959.4921	Capwap_Ctrl	10.50.77.164	38035	TLS_RSA_WITH_AES_128_CBC_SHA
AP1cdf.0f94.8063	Capwap_Ctrl	10.50.100.54	18439	TLS_RSA_WITH_AES_128_CBC_SHA
AP1cdf.0f94.8063	Capwap_Data	10.50.100.54	18439	TLS_RSA_WITH_AES_128_CBC_SHA

(WLC) >show netuser guest-roles

Role Name.....	Guest
Average Data Rate.....	10
Burst Data Rate.....	10
Average Realtime Rate.....	100
Burst Realtime Rate.....	100

(WLC) >show netuser detail guest

```
User Name..... guest
WLAN Id..... 2
User Type..... Guest
Lifetime..... Infinity
Start Time..... Tue Sep 10 05:42:22 2013
Description.....
Role Name..... Guest
  Average Data Rate..... 10
  Burst Data Rate..... 10
  Average Realtime Rate..... 100
  Burst Realtime Rate..... 100
```

```
config wlan broadcast-ssid disable 3
config wps mfp infrastructure enable
config ap link-encryption enable AP1cdf.0f94.8063
```

```
config rogue rule add ap priority 1 classify malicious RogueAP
config rogue rule enable RogueAP
config rogue rule match any RogueAP
config rogue rule condition ap set no-encryption RogueAP
config rogue rule condition ap set client-count 1
```

```
config rogue ap friendly add 1c:df:0f:94:80:63
```

```
config netuser guest-role qos data-rate average-data-rate guest 10
config netuser guest-role qos data-rate burst-data-rate guest 10
config netuser guest-role qos data-rate average-realtime-rate guest 100
config netuser guest-role qos data-rate burst-realtime-rate guest 100
```


show wps summary

Client Exclusion Policy

Excessive 802.11-association failures.....	Enabled
Excessive 802.11-authentication failures.....	Enabled
Excessive 802.1x-authentication.....	Enabled
IP-theft.....	Enabled
Excessive Web authentication failure.....	Enabled

Signature Policy

Signature Processing.....	Enabled
---------------------------	---------

R5# show ipv6 route

IPv6 Routing Table - default - 6 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP

H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea

IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO

ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect

l - LISP

O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

```
C 1010::/64 [0/0]
  via Loopback1, directly connected
L 1010::A8BB:CCFF:FE00:7D00/128 [0/0]
  via Loopback1, receive
C 2001:DB8::/64 [0/0]
  via Tunnel0, directly connected
L 2001:DB8::1:5/128 [0/0]
  via Tunnel0, receive
EX 2010::/64 [170/27008000]
  via FE80::A32:5006, Tunnel0
L FF00::/8 [0/0]
  via Null0, receive
```

R6# show ipv6 route

IPv6 Routing Table - default - 6 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP

H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea

IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO

ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect

l - LISP

O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

```
EX 1010::/64 [170/27008000]
  via FE80::A32:5A05, Tunnel0
C 2001:DB8::/64 [0/0]
  via Tunnel0, directly connected
L 2001:DB8::1:6/128 [0/0]
  via Tunnel0, receive
C 2010::/64 [0/0]
  via Loopback1, directly connected
L 2010::A8BB:CCFF:FE00:7E00/128 [0/0]
  via Loopback1, receive
L FF00::/8 [0/0]
  via Null0, receive
```

```
R5# show access-lists
```

```
Extended IP access list DetectIPv6
```

```
10 permit 41 any any log (14 matches)
```

```
20 permit udp any any eq 3544 log
```

```
30 permit ip any any (155 matches)
```

R5# show log - (logging console enabled)

*Aug 27 17:51:20.992: %SEC-6-IPACCESSLOGNP: list DetectIPv6 permitted 41
10.50.80.6 -> 10.50.90.5, 1 packet

```
IP access list DetectIPv6
permit 41 any any log
permit udp any any eq 3544 log
permit ip any any
```

```
int e0/0
```

```
ip access-group DetectIPv6 out
```

```
interface Tunnel0
no ip address
ipv6 address 2001:DB8::1:6/64
ipv6 eigrp 65
tunnel source Ethernet0/0
tunnel mode ipv6ip
tunnel destination 10.50.80.5
```

```
access-list 101 extended permit 41 host 10.50.80.6 host 10.50.90.5
```

```
SW1# conf t
SW1(config)# int GigabitEthernet1/0/19
SW1(config)# shut
SW1(config)# no shut
```


SW1# show ip dhcp snooping binding

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
1C:DF:0F:94:80:63	10.50.100.53	infinite	dhcp-snooping	100	GigabitEthernet1/0/19

Total number of bindings: 1

SW1# show ip dhcp snooping

Switch DHCP snooping is enabled

DHCP snooping is configured on following VLANs:

100,110,120

DHCP snooping is operational on following VLANs:

100,110,120

Smartlog is configured on following VLANs:

none

Smartlog is operational on following VLANs:

none

DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled

 circuit-id default format: vlan-mod-port

 remote-id: c464.13fb.7780 (MAC)

Option 82 on untrusted port is not allowed

Verification of hwaddr field is enabled

Verification of giaddr field is enabled

DHCP snooping trust/rate is configured on the following Interfaces:

Interface	Trusted	Rate limit (pps)
-----	-----	-----
GigabitEthernet1/0/2	yes	unlimited

```
SW1# show ip verify source
```

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan	Log
-----	-----	-----	-----	-----	----	---
Gi1/0/19	ip-mac	active	10.50.100.53	1C:DF:0F:94:80:63	100	disabled

```
ip dhcp snooping vlan 100,110,120
ip dhcp snooping
```

```
interface GigabitEthernet 1/0/2
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 100,110,120
  switchport mode trunk
  ip dhcp snooping trust
```

```
interface GigabitEthernet1/0/19
  switchport access vlan 100
  switchport mode access
  ip verify source port-security
  switchport port-security
```

```
!
```

```
ip dhcp class CLASS1
  relay agent information
    relay-information hex 01030a0b0c02050000000123

ip dhcp pool ABC
  network 10.0.20.0 255.255.255.0
  class CLASS1
    address range 10.0.20.1 10.0.20.100
  class CLASS2
    address range 10.0.20.101 10.0.20.200
```

Aug 19 21:42:52.030: DHCPD: Searching for a match to ' relay-
information 010600040064011302080006c46413fb7780' in class CLASS1

show ip dhcp snooping.....

Insertion of option 82 is enabled

circuit-id default format: vlan-mod-port

remote-id: c464.13fb.7780 (MAC)

DHCP_SNOOPING: received new DHCP packet from input interface
(GigabitEthernet1/0/19)

DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, input
interface: Gil/0/19,

MAC da: ffff.ffff.ffff, MAC sa: 1cdf.0f94.8063, IP da: 255.255.255.255, IP sa:
0.0.0.0, DHCP

ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0,
DHCP chaddr:

1cdf.0f94.8063

DHCP_SNOOPING: add relay information option.

DHCP_SNOOPING_SW: Encoding opt82 CID in vlan-mod-port format

DHCP_SNOOPING_SW: Encoding opt82 RID in MAC address format

DHCP_SNOOPING: binary dump of relay info option, length: 20 data:

0x52 0x12 0x1 0x6 0x0 0x4 0x0 0x64 0x1 0x13 0x2 0x8 0x0 0x6 0xC4 0x64 0x13 0xFB
0x77 0x80

DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is
flooded to ingress VLAN: (100)

ip dhcp relay information trust-all

%DHCP_SNOOPING-5-DHCP_SNOOPING_NONZERO_GIADDR: DHCP_SNOOPING drop message with non-zero giaddr or option82 value on untrusted port

```
ip dhcp snooping information option allow-untrusted
```

`class-map type access-control: Identify IP packet of interest`
`policy-map type access-control: Apply actions to the matched packets`

service-policy type access-control on an interface

```
R6# ping 10.50.40.7 size 1200
```

```
Type escape sequence to abort.
```

```
Sending 5, 1200-byte ICMP Echos to 7.7.6.3, timeout is 2 seconds:
```

```
.....
```

```
R7# show policy-map type access-control interface g0/1  
GigabitEthernet0/1
```

```
Service-policy access-control input: ICMP
```

```
Class-map: ICMP (match-all)
```

```
5 packets, 6070 bytes
```

```
5 minute offered rate 2000 bps
```

```
Match: field IP protocol eq 1 next IP
```

```
Service-policy access-control : BIGIP
```

```
Class-map: BIGIP (match-all)
```

```
5 packets, 6070 bytes
```

```
5 minute offered rate 2000 bps
```

```
Match: field IP length gt 1000
```

```
drop
```

```
Class-map: class-default (match-any)
```

```
0 packets, 0 bytes
```

```
5 minute offered rate 0 bps, drop rate 0 bps
```

```
Match: any
```

```
Class-map: class-default (match-any)
```

```
29 packets, 2734 bytes
```

```
5 minute offered rate 0 bps, drop rate 0 bps
```

```
Match: any
```

```
load protocol system:/fpm/pdf/icmp.pdf
```

```
class-map type access-control match-all BIGIP  
  match field IP length gt 1000
```

```
policy-map type access-control BIGIP  
  class BIGIP  
    drop  
  class-map type stack match-all ICMP  
    match field IP protocol eq 1 next IP
```

```
policy-map type access-control ICMP  
  class ICMP  
    service-policy BIGIP
```

```
interface GigabitEthernet0/1  
  service-policy type access-control input ICMP
```

ASA1# changeto context c1

ASA1/c1# show service-policy global

Global policy:

Service-policy: global_policy

Class-map: inspection_default

Inspect: ftp, packet 0, drop 0, reset-drop 0

Inspect: h323 h225 _default_h323_map, packet 0, drop 0, reset-drop 0

tcp-proxy: bytes in buffer 0, bytes dropped 0

Inspect: h323 ras _default_h323_map, packet 0, drop 0, reset-drop 0

Inspect: ip-options _default_ip_options_map, packet 0, drop 0, reset-drop 0

Inspect: netbios, packet 0, drop 0, reset-drop 0

Inspect: rsh, packet 0, drop 0, reset-drop 0

Inspect: rtsp, packet 0, drop 0, reset-drop 0

tcp-proxy: bytes in buffer 0, bytes dropped 0

Inspect: skinny , packet 0, drop 0, reset-drop 0

tcp-proxy: bytes in buffer 0, bytes dropped 0

Inspect: esmtp _default_esmtp_map, packet 0, drop 0, reset-drop 0

Inspect: sqlnet, packet 0, drop 0, reset-drop 0

Inspect: sunrpc, packet 0, drop 0, reset-drop 0

tcp-proxy: bytes in buffer 0, bytes dropped 0

Inspect: tftp, packet 0, drop 0, reset-drop 0

Inspect: sip , packet 0, drop 0, reset-drop 0

tcp-proxy: bytes in buffer 0, bytes dropped 0

Inspect: xdmcp, packet 0, drop 0, reset-drop 0

Inspect: dns c1-dns, packet 580, drop 189, reset-drop 0


```
ASA1/c1# show service-policy inspect dns
```

```
Global policy:
```

```
Service-policy: global_policy
```

```
Class-map: inspection_default
```

```
Inspect: dns c1-dns, packet 560, drop 189, reset-drop 0
```

```
dns-guard, count 13
```

```
protocol-enforcement, drop 0
```

```
nat-rewrite, count 0
```

```
id-randomization, count 547
```

```
match header-flag AA
```

```
log, packet 13
```

```
match header-flag QR
```

```
log, packet 9
```

```
match not domain-name regex domain
```

```
drop, packet 730
```

```
ASA1/c1# test regex cisco.com "cisco\.com"  
INFO: Regular expression match succeeded.
```

```
regex domain "cisco\\.com"

policy-map type inspect dns ci-dns
  parameters
    id-randomization
  match header-flag AA
    log
  match header-flag QR
    log
  match not domain-name regex domain
    drop
!
policy-map global_policy
  class inspection_default
    inspect dns ci-dns
<...>
```

```
R2# test aaa group tacacs+ admin cisco legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

```
R2# test aaa group tacacs+ netops cisco legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

```
R2# show tacacs
```

```
Tacacs+ Server          : 192.168.2.18/49
      Socket opens:      45
      Socket closes:    45
      Socket aborts:     0
      Socket errors:    0
      Socket Timeouts:  0
Failed Connect Attempts: 0
      Total Packets Sent: 77
      Total Packets Recv: 77
```

R7# telnet 10.50.100.2

Trying 10.50.100.2 ... Open

Username: netops

Password: cisco

R2#

R2# configure t

Command authorization failed.

R2# show ip route

Command authorization failed.

R2# show crypto ipsec sa -> should display output, for example:

interface: Ethernet0/0.1

 Crypto map tag: Ethernet0/0.1-OSPF-MAP, local addr FE80::A8BB:CCFF:FE00:7A00

 IPsecv6 policy name: OSPFv3-500

 protected vrf: (none)

 local ident (addr/mask/prot/port): (FE80::/10/89/0)

 remote ident (addr/mask/prot/port): (::/0/89/0)

```
R4# telnet 10.50.100.2
Trying 10.50.100.2 ... Open
```

```
User Access Verification
```

```
Password: cisco
```

```
R2> enable
```

```
Password: cisco
```

```
R2#
```

```
R2#
```

```
! Second Telnet session (username/password should be prompted)
```

```
R7# telnet 10.50.100.2
```

```
Trying 10.50.100.2 ... Open
```

```
Username: admin
```

```
Password: cisco
```

```
R2#
```

```
R2# configure t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R2(config)#
```

enable

show crypto *(permit any subcommands)*

clear crypto session *(permit any subcommands)*

```
access-list 101 permit tcp any host 192.168.2.18 eq 49
```

```
aaa new-model
!
!
aaa authentication login telnet2 group tacacs+ local
aaa authentication login no-auth none
aaa authentication login line-auth line
! Required for configuration commands
aaa authorization config-commands
aaa authorization exec no-auth none
aaa authorization exec exec-auth group tacacs+
aaa authorization commands 1 telnet2 group tacacs+ none
aaa authorization commands 15 telnet2 group tacacs+ none
username cisco password cisco
!
<...>
!
tacacs-server host 192.168.2.18
tacacs-server key cisco123
!
<...>
line con 0
  login authentication no-auth
line aux 0
line vty 0
  password cisco
  authorization exec no-auth
  login authentication line-auth
line vty 1
  password cisco
  authorization commands 1 telnet2
  authorization commands 15 telnet2
  authorization exec exec-auth
  login authentication telnet2
line vty 2 4
  password cisco
  authorization exec no-auth
  login authentication line-auth
!
<...>
```

```
*Aug 24 22:50:50.975: AAA/AUTHOR/CMD: tty3 (745938549) user='netops'  
*Aug 24 22:50:50.975: tty3 AAA/AUTHOR/CMD (745938549): send AV service=shell  
*Aug 24 22:50:50.975: tty3 AAA/AUTHOR/CMD (745938549): send AV cmd=show  
*Aug 24 22:50:50.975: tty3 AAA/AUTHOR/CMD (745938549): send AV cmd-arg=ip  
*Aug 24 22:50:50.975: tty3 AAA/AUTHOR/CMD (745938549): send AV cmd-arg=route  
*Aug 24 22:50:50.975: tty3 AAA/AUTHOR/CMD (745938549): send AV cmd-arg=<cr>
```

```
*Aug 24 22:50:50.975: tty3 AAA/AUTHOR/CMD(745938549): found list "telnet2"
*Aug 24 22:50:50.975: tty3 AAA/AUTHOR/CMD (745938549): Method=tacacs+ (tacacs+)
*Aug 24 22:50:50.976: AAA/AUTHOR/TAC+: (745938549): user=netops
*Aug 24 22:50:50.976: AAA/AUTHOR/TAC+: (745938549): send AV service=shell
*Aug 24 22:50:50.976: AAA/AUTHOR/TAC+: (745938549): send AV cmd=show
*Aug 24 22:50:50.976: AAA/AUTHOR/TAC+: (745938549): send AV cmd-arg=ip
*Aug 24 22:50:50.976: AAA/AUTHOR/TAC+: (745938549): send AV cmd-arg=route
*Aug 24 22:50:50.976: AAA/AUTHOR/TAC+: (745938549): send AV cmd-arg=<cr>
*Aug 24 22:50:50.976: TAC+: using previously set server 192.168.2.18 from group
    tacacs+
*Aug 24 22:50:50.976: TAC+: Opening TCP/IP to 192.168.2.18/49 timeout=5
*Aug 24 22:50:50.977: TAC+: Opened TCP/IP handle 0xF1D55260 to 192.168.2.18/49
    using source 0.0.0.0
*Aug 24 22:50:50.977: TAC+: Opened 192.168.2.18 index=1
*Aug 24 22:50:50.977: TAC+: 192.168.2.18 (745938549) AUTHOR/START queued
```

*Aug 24 22:50:51.184: TAC+: (745938549) AUTHOR/START processed
*Aug 24 22:50:51.184: TAC+: (745938549): received author response status = FAIL
Command authorization failed.

```
*Aug 24 22:54:04.229: AAA/AUTHOR/CMD: tty3 (1720594819) user='netops'  
*Aug 24 22:54:04.229: tty3 AAA/AUTHOR/CMD (1720594819): send AV service=shell  
*Aug 24 22:54:04.229: tty3 AAA/AUTHOR/CMD (1720594819): send AV cmd=show  
*Aug 24 22:54:04.229: tty3 AAA/AUTHOR/CMD (1720594819): send AV cmd-arg=crypto  
*Aug 24 22:54:04.229: tty3 AAA/AUTHOR/CMD (1720594819): send AV cmd-arg=ipsec  
*Aug 24 22:54:04.229: tty3 AAA/AUTHOR/CMD (1720594819): send AV cmd-arg=sa  
*Aug 24 22:54:04.229: tty3 AAA/AUTHOR/CMD (1720594819): send AV cmd-arg=<cr>
```

```
*Aug 24 22:54:04.229: tty3 AAA/AUTHOR/CMD(1720594819): found list "telnet2"
*Aug 24 22:54:04.229: tty3 AAA/AUTHOR/CMD (1720594819): Method=tacacs+ (tacacs+)
*Aug 24 22:54:04.229: AAA/AUTHOR/TAC+: (1720594819): user=netops
*Aug 24 22:54:04.229: AAA/AUTHOR/TAC+: (1720594819): send AV service=shell
*Aug 24 22:54:04.229: AAA/AUTHOR/TAC+: (1720594819): send AV cmd=show
*Aug 24 22:54:04.229: AAA/AUTHOR/TAC+: (1720594819): send AV cmd-arg=crypto
*Aug 24 22:54:04.229: AAA/AUTHOR/TAC+: (1720594819): send AV cmd-arg=ipsec
*Aug 24 22:54:04.229: AAA/AUTHOR/TAC+: (1720594819): send AV cmd-arg=sa
*Aug 24 22:54:04.229: AAA/AUTHOR/TAC+: (1720594819): send AV cmd-arg=<cr>
*Aug 24 22:54:04.229: TAC+: using previously set server 192.168.2.18 from group
tacacs+
*Aug 24 22:54:04.229: TAC+: Opening TCP/IP to 192.168.2.18/49 timeout=5
*Aug 24 22:54:04.230: TAC+: Opened TCP/IP handle 0xF2108628 to 192.168.2.18/49
using source 0.0.0.0
*Aug 24 22:54:04.230: TAC+: Opened 192.168.2.18 index=1
*Aug 24 22:54:04.231: TAC+: 192.168.2.18 (1720594819) AUTHOR/START queued
```

*Aug 24 22:54:04.436: TAC+: (1720594819) AUTHOR/START processed

*Aug 24 22:54:04.436: TAC+: (1720594819): received author response status =
PASS_ADD

interface: Ethernet0/0.1

Crypto map tag: Ethernet0/0.1-OSPF-MAP, local addr FE80::A8BB:CCFF:FE00:7A00

```
R1(config)# aaa authentication login default local
R1(config)# end
```



```
test aaa group aaa-group username password legacy
```

Attempting authentication test to **server-group** aaa group using aaa protocol
User was successfully authenticated.

```
test aaa-server authentication aaa-server-name
Server IP Address or name: ip-addr
Username: cisc0
Password: *****
INFO: Attempting Authentication test to IP address (timeout: 12 seconds)
ERROR: Authentication Rejected: AAA failure
test aaa-server authentication aaa-server-name
Server IP Address or name: ip-addr
Username: cisco
Password: *****
INFO: Attempting Authentication test to IP address (timeout: 12 seconds)
INFO: Authentication Successful
```

test aaa accounting ?

alloc_fid	Allocate flow id
alloc_uid	Allocate AAA unique id
dealloc_fid	Deallocate flow id
dealloc_uid	Deallocate unique id
giga	Giga-word accounting test
init	Initialize test aaa accounting infrastructure
reset	Reset the variables
send_acct_start	Send accounting start
send_acct_stop	Send accounting stop
send_authen_req	Send authen req

ASA2# show uauth

	Current	Most Seen
Authenticated Users	1	1
Authen In Progress	0	1

user 'userap1' at 192.168.2.25, authorized to:
port 10.50.40.7/http
absolute timeout: 0:05:00
inactivity timeout: 0:00:00

ASA2# show uauth

	Current	Most Seen
Authenticated Users	1	1
Authen In Progress	0	1

user 'userap2' at 192.168.2.25, authorized to:

port 10.50.30.4/http

absolute timeout: 0:05:00

inactivity timeout: 0:00:00

```
aaa-server tacacs protocol tacacs+
aaa-server tacacs (outside) host 192.168.2.18 key cisco123
access-list auth-proxy extended permit tcp any 10.50.0.0 255.255.0.0 eq www
aaa authentication match auth-proxy outside tacacs
aaa authorization match auth-proxy outside tacacs
```

ASA# show uauth

	Current	Most Seen
Authenticated Users	1	1
Authen In Progress	0	1

user 'userapl' at 192.168.2.25, authenticated
access-list #ACSACL#-IP-CutThrough-4b208394

absolute timeout: 0:05:00

inactivity timeout: 0:00:00

ASA# show access-list #ACSACL#-IP-CutThrough-4b208394

permit tcp any host 10.50.40.7 eq www

show auth sess int g1/0/14

Interface: GigabitEthernet1/0/14

MAC Address: 0023.eb54.1109

IP Address: Unknown

User-Name: 00-23-EB-54-11-09

Status: Authz Success

Domain: VOICE

Security Policy: Should Secure

Security Status: Unsecure

Oper host mode: multi-auth

Oper control dir: both

Authorized By: Authentication Server

Vlan Policy: 9

ACS ACL: xACSACLx-IP-PERMIT_ALL_TRAFFIC-4fe7f797

Session timeout: 3600s (local), Remaining: 3509s

Timeout action: Reauthenticate

Idle timeout: N/A

Common Session ID: C0A842420000002E003D9546

Acct Session ID: 0x00000030

Handle: 0x3C00002F

```
sho auth sess int g1/0/14
Interface: GigabitEthernet1/0/14
      MAC Address: 000c.290d.0c22
      IP Address: Unknown
      User-Name: Test-PC
      Status: Authz Success
      Domain: DATA
Security Policy: Should Secure

Security Status: Unsecure
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: 99
      ACS ACL: xACSACLx-IP-DATA_VLAN_DACL-503d6911
Session timeout: 3600s (local), Remaining: 3585s
Timeout action: Reauthenticate
Idle timeout: N/A
Common Session ID: C0A842420000008B37CC94A2
Acct Session ID: 0x000000B4
      Handle: 0x0F00008C
```

SW2# show authentication session int g1/0/14

```
    Interface: GigabitEthernet1/0/14
    MAC Address: 0023.eb54.1109
    IP Address: Unknown
    User-Name: 00-23-EB-54-11-09 -> matches IP phone MAC address above
    Status: Authz Success
    Domain: VOICE
    Security Policy: Should Secure
    Security Status: Unsecure
    Oper host mode: multi-auth
    Oper control dir: both
    Authorized By: Authentication Server
    ACS ACL: xACSACLx-IP-PERMIT_ALL_TRAFFIC-4fe7f797 -> should be the
IP_PERMIT_ALL_TRAFFIC acl matched below
    Vlan Policy: 9
    Session timeout: 3600s (local), Remaining: 3509s
    Timeout action: Reauthenticate
    Idle timeout: N/A
    Common Session ID: C0A8424200000002E003D9546
    Acct Session ID: 0x00000030
    Handle: 0x3C00002F
```

Runnable methods list:

Method	State
mab	Authc Success
dot1x	Not run

```
SW2# sho access-list
```

```
Extended IP access list xACSACLx-IP-PERMIT_ALL_TRAFFIC-4fe7f797 (per-user)
```

```
10 permit ip any any
```

R6# show ephone summary

hairpin_block:

ephone-1[0] Mac:0023.EB54.1109 TCP socket:[1] activeLine:0 whisperLine:0
REGISTERED

mediaActive:0 whisper_mediaActive:0 startMedia:0 offhook:0 ringing:0 reset:0
reset_sent:0 debug:0

IP:10.50.9.6 * 7965 keepalive 10609 music 0

Max 10, Registered 1, Unregistered 0, Deceased 0 High Water Mark 11, Sockets 1
ephone_send_packet process switched 0

SW2# show authentication session int g1/0/14

Interface: GigabitEthernet1/0/14

MAC Address: 000c.290d.0c22

IP Address: Unknown

User-Name: Test-PC

Status: Authz Success

Domain: DATA

Security Policy: Should Secure

Security Status: Unsecure

Oper host mode: multi-auth

Oper control dir: both

Authorized By: Authentication Server

Vlan Policy: 99

ACS ACL: xACSACLx-IP-DATA_VLAN_DACL-503d6911 -> should be the
IP_DATA_VLAN_ACL acl

Session timeout: 3600s (local), Remaining: 3585s

Timeout action: Reauthenticate

Idle timeout: N/A

Common Session ID: C0A842420000008B37CC94A2

Acct Session ID: 0x000000B4

Handle: 0x0F00008C

Runnable methods list:

Method	State
--------	-------

mab	Failed over
-----	-------------

dot1x	Authc Success
-------	---------------

```
SW2# show access-list
```

```
Extended IP access list xACSACLx-IP-DATA_VLAN_DACL-503d6911 (per-user)
```

```
10 permit ip any any
```

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius

dot1x system-auth-control

interface GigabitEthernet1/0/14
 switchport access vlan 99
 switchport mode access
 switchport voice vlan 9
 ip access-group ACL_DEFAULT in
 authentication host-mode multi-auth
 authentication open
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 authentication periodic
 mab
 dot1x pae authenticator
 spanning-tree portfast

ip access-list extended ACL-DEFAULT
 remark DHCP
 permit udp any eq bootpc any eq bootps
 remark DNS
 permit udp any any eq domain
 remark Ping
 permit icmp any any
 remark PXE / TFTP
 permit udp any any eq tftp
 remark Drop all the rest
 deny ip any any log
```



```
access-list 101 extended permit udp any any eq 1812
access-list 101 extended permit udp any any eq 1813
```

```
access-group 101 in interface outside
```



```
authentication order mab dot1x web-auth
authentication priority dot1x mab web-auth
authentication event fail action next-method
authentication fallback web-auth
```

```
authentication order mab dot1x
authentication priority dot1x mab
authentication event fail action authorize vlan 111
```

HTTP server history:

local-ipaddress:port	remote-ipaddress:port	in-bytes	out-bytes	end-time
10.50.50.5:80	192.168.2.50:64008	3547	251686	19:55:45
10.50.50.5:80	192.168.2.50:9612	4118	270121	19:55:45

```
R7# show crypto session
Interface: Tunnel2
Profile: ipv6
Session status: UP-ACTIVE
Peer: 2001:DB9:30::4 port 500
  IKEv1 SA: local 2001:DB8:40::7/500
             remote 2001:DB9:30::4/500 Active
  IPSEC FLOW: permit ipv6 ::/0 ::/0
             Active SAs: 2, origin: crypto map
```

```
R4# show crypto session
Interface: Tunnel2
Profile: ipv6
Session status: UP-ACTIVE
Peer: 2001:DB8:40::7 port 500
  IKEv1 SA: local 2001:DB9:30::4/500
             remote 2001:DB8:40::7/500 Active
  IPSEC FLOW: permit ipv6 ::/0 ::/0
             Active SAs: 2, origin: crypto map
```


R7# show ipv6 route

IPv6 Routing Table - default - 9 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP

H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea

IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO

ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect

l - LISP

O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

EX 2011::/64 [170/27008000]

via FE80::A8BB:CCFF:FE00:7C00, Tunnel2

R1# show crypto session

Interface: Ethernet0/0

Session status: UP-IDLE

Peer: 10.50.100.2 port 848

IKEv1 SA: local 10.50.100.1/848 remote 10.50.100.2/848 Active

Interface: Ethernet0/0

Session status: UP-IDLE

Peer: 10.50.60.6 port 848

IKEv1 SA: local 10.50.100.1/848 remote 10.50.60.6/848 Active

Interface: Ethernet0/0

Session status: UP-IDLE

Peer: 10.50.40.7 port 848

IKEv1 SA: local 10.50.100.1/848 remote 10.50.40.7/848 Active

R2# show crypto session

Crypto session current status

Interface: (unknown)

Session status: UP-IDLE

Peer: 239.192.1.190 port 848

IKEv1 SA: local 10.50.100.2/848 remote 239.192.1.190/848 Active

Interface: Ethernet0/0.1

Session status: UP-IDLE

Peer: 10.50.100.1 port 848

IKEv1 SA: local 10.50.100.2/848 remote 10.50.100.1/848 Active

R7# show crypto gdoi ipsec sa

SA created for group getvpn:

GigabitEthernet0/1:

protocol = ip

local ident = 10.7.0.0/16, port = 0

remote ident = 10.7.0.0/16, port = 0

direction: Both, replay(method/window): Time/5 sec

R7# show crypto gdoi

GROUP INFORMATION

Group Name	:	getvpn
Group Identity	:	1
Rekeys received	:	3
IPSec SA Direction	:	Both
Group Server list	:	10.50.100.1 10.50.100.2

R6# show crypto gdoi

GROUP INFORMATION

Group Name	:	getvpn	
Group Identity	:	1	
Rekeys received	:	4	
IPSec SA Direction	:	Both	
Group Server list	:	10.50.100.1 10.50.100.2	
Group member	:	10.50.60.6	vrf: None
Version	:	1.0.2	
Registration status	:	Registered	

```
ASA2# show vpn-sessiondb webvpn
```

```
ASA2# show vpn-sessiondb anyconnect
```

ASA2# show crypto ca cert

Certificate

Status: Available

Certificate Serial Number: 8b7ef551

Certificate Usage: General Purpose

Public Key Type: RSA (1024 bits)

Signature Algorithm: SHA1 with RSA Encryption

Issuer Name:

hostname=sslvpn.cisco.com

cn=sslvpn.cisco.com

Subject Name:

hostname=sslvpn.cisco.com

cn=sslvpn.cisco.com

Validity Date:

start date: 05:18:57 UTC Aug 21 2013

end date: 05:18:57 UTC Aug 19 2023

Associated Trustpoints: localtrust

R6# show crypto ikev2 session detailed

IPv4 Crypto IKEv2 Session

Session-id:18, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id	Local	Remote	fvr/ivrf	Status
1	10.50.70.6/500	10.50.40.7/500	none/none	READY

Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:5, Auth sign: PSK, Auth verify: PSK

Life/Active Time: 86400/1014 sec

CE id: 1008, Session-id: 18

Status Description: Negotiation done

Local spi: D60B62C207327A3D Remote spi: 609E382CB11281D3

Local id: r6.cisco.com

Remote id: r7.cisco.com

.....

Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535

remote selector 0.0.0.0/0 - 255.255.255.255/65535

ESP spi in/out: 0x88B600C5/0xDE40CB3B

AH spi in/out: 0x0/0x0

CPI in/out: 0x0/0x0

Encr: AES-CBC, keysize: 128, esp_hmac: SHA96

ah_hmac: None, comp: IPCOMP_NONE, mode tunnel

R7# show ip route

R 172.17.60.0/24 [120/1] via 172.16.70.6, 00:00:07, Tunnel1

R6# show ip route

172.17.0.0/24 is subnetted, 1 subnets

R 172.17.70.0/24 [120/1] via 172.16.70.7, 00:00:21, Virtual-Access1

R4# show crypto ikev2 authorization policy

```
IKEv2 Authorization Policy : flex
  route set interface
  route set acl: routes
  route accept any tag : 1 distance : 1
```

R4# show crypto ikev2 client flex

```
Profile : flex
Current state:ACTIVE
Peer : 10.50.100.2
Source : Ethernet0/1
ivrf : IP DEFAULT
fvrf : IP DEFAULT
Backup group: Default
Tunnel interface : Tunnel0
Assigned ip address: 172.17.100.55
```

R4# show crypto ikev2 session detail

IPv4 Crypto IKEv2 Session

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id	Local	Remote	fvrf/ivrf	Status
1	10.50.30.4/500	10.50.100.2/500	none/none	READY

Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK

Life/Active Time: 86400/277 sec

CE id: 1032, Session-id: 2

Status Description: Negotiation done

Local spi: 0696C6F582787B23 Remote spi: 49C2BF63CF74F456

Local id: R4.cisco.com

Remote id: 10.50.100.2

Pushed IP address: 172.17.100.55

DNS Primary: 192.168.2.25

Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535

remote selector 0.0.0.0/0 - 255.255.255.255/65535

ESP spi in/out: 0xEEF6B847/0x81642A80

AH spi in/out: 0x0/0x0

CPI in/out: 0x0/0x0

Encr: 3DES, esp_hmac: MD596

ah_hmac: None, comp: IPCOMP_NONE, mode tunnel

R2# show ip route

S 172.18.34.0 is directly connected, Virtual-Access1

CRYPTO_PKI: locked trustpoint ciscoca, refcount is 1
CRYPTO_PKI: http connection opened
CRYPTO_PKI: Sending HTTP message
CRYPTO_PKI: Reply HTTP header:
HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI)
Host: 10.50.100.1

CRYPTO_PKI: unlocked trustpoint ciscoca, refcount is 0
CRYPTO_PKI: locked trustpoint ciscoca, refcount is 1
CRYPTO_PKI: unlocked trustpoint ciscoca, refcount is 0
CRYPTO_PKI: Reply HTTP header:
HTTP/1.1 200 OK
Date: Sun, 18 Aug 2013 04:34:08 GMT
Server: cisco-IOS
Content-Type: application/x-x509-ca-cert
Expires: Sun, 18 Aug 2013 04:34:08 GMT
Last-Modified: Sun, 18 Aug 2013 04:34:08 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Accept-Ranges: none

Content-Type indicates we have received a CA certificate.

```
R6(config)# crypto pki auth ciscoca
```

```
Certificate has the following attributes:
```

```
    Fingerprint MD5: 1F5A02E4 C2C8230A 56FC15BB CBDFBEF6
```

```
    Fingerprint SHA1: 99D5D0AA 928B4DD8 7D9E6D98 B3831F1D 796C6A71
```

```
% Do you accept this certificate? [yes/no]: no
```

(WLC) >show ap summary

Number of APs..... 2

Global AP User Name..... cisco

Global AP Dot1x User Name..... ciscoAP

AP Name Country	Slots Priority	AP Model	Ethernet MAC	Location	Port
AP1cdf.0f94.8063	2	AIR-CAP3502I-A-K9	1c:df:0f:94:80:63	default location	1
AP588d.0959.4921	2	AIR-LAP1262N-A-K9	58:8d:09:59:49:21	default location	1

SW2# show cts interface

Global Dot1x feature is Enabled

Interface GigabitEthernet1/0/23:

```
CTS is enabled, mode: DOT1X
IFC state: OPEN
Authentication Status: SUCCEEDED
  Peer identity: "SW1"
  Peer's advertised capabilities: "sap"
  802.1X role: Authenticator
  Reauth period configured: 240 (locally configured)
  Reauth period per policy: 86400 (server configured)
  Reauth period applied to link: 86400 (server configured)
  Reauth starts in approx. 0:15:47:42 (dd:hr:mm:sec)
Authorization Status: SUCCEEDED
  Peer SGT: 2:NADS
  Peer SGT assignment: Trusted
SAP Status: SUCCEEDED
  Version: 2
  Configured pairwise ciphers:
    gcm-encrypt
    null
    no-encap

  Replay protection: enabled
  Replay protection mode: STRICT

Selected cipher: gcm-encrypt
```

Propagate SGT: Enabled

SW2# show cts role-based sgt all

IP Address	SGT	Source
------------	-----	--------

=====

10.50.30.3	12	CLI
10.50.30.4	12	CLI
10.50.50.20	14	CLI
10.50.50.20	14	CLI
10.50.70.4	2	CLI
10.50.80.50	16	CLI
10.50.100.1	15	CLI
10.50.100.2	15	CLI
10.50.100.10	15	CLI
192.168.2.25	18	CLI

```
ASA2# show interface gig0/0
```

```
Interface GigabitEthernet0/0 "", is up, line protocol is up
```

```
Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
```

```
Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
```

```
Input flow control is unsupported, output flow control is off
```

```
Active member of Redundant1
```

```
MAC address 0015.c695.c646, MTU not set
```

```
IP address unassigned
```

```
ASA2# show interface gig0/1
```

```
Interface GigabitEthernet0/1 "", is up, line protocol is up
```

```
Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
```

```
Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
```

```
Input flow control is unsupported, output flow control is off
```

```
Standby member of Redundant1
```

```
MAC address 0015.c695.c647, MTU not set
```

```
IP address unassigned
```

```
ASA2# show interface redundant 1
Interface Redundant1 "outside", is up, line protocol is up
Hardware is i82546GB rev03, 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 0015.c695.c646, MTU 1500
IP address 10.50.50.20, subnet mask 255.255.255.0
```

ASA2# show nameif

Interface	Name	Security
GigabitEthernet0/2	inside	100
GigabitEthernet0/3	dmz	50
Redundant1	outside	0

ASA2# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 10.50.50.5 to network 0.0.0.0

```
C 10.50.50.0 255.255.255.0 is directly connected, outside
S 10.3.3.0 255.255.255.0 [1/0] via 10.50.30.3, dmz
S 10.4.4.0 255.255.255.0 [1/0] via 10.50.30.4, dmz
O 10.7.7.7 255.255.255.255 [110/11] via 10.50.40.7, 0:00:18, inside
C 10.50.40.0 255.255.255.0 is directly connected, inside
C 10.50.30.0 255.255.255.0 is directly connected, dmz
O 10.50.9.0 255.255.255.0 [110/11] via 10.50.50.5, 0:00:18, outside
O E2 10.50.100.0 255.255.255.0 [110/20] via 10.50.50.5, 0:00:18, outside
O E2 10.50.90.0 255.255.255.0 [110/20] via 10.50.50.5, 0:00:18, outside
O 10.50.77.0 255.255.255.0 [110/11] via 10.50.50.5, 0:00:18, outside
O 10.50.70.0 255.255.255.0 [110/11] via 10.50.50.5, 0:00:18, outside
O E2 192.168.2.0 255.255.255.0 [110/20] via 10.50.50.5, 0:00:18, outside
O*E2 0.0.0.0 0.0.0.0 [110/1] via 10.50.50.5, 0:00:18, outside
```

ASA2# ping outside 10.50.50.5

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.50.50.5, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

```
hostname ASA2
interface Redundant1
  member-interface GigabitEthernet0/0
  member-interface GigabitEthernet0/1
  nameif outside
  security-level 0
  ip address 10.50.50.20 255.255.255.0
  ospf priority 0
```

ASA1/admin# show crypto key mypubkey rsa

Key pair was generated at: 03:37:36 UTC Aug 21 2013

Key name: <Default-RSA-Key>

Usage: General Purpose Key

Modulus Size (bits): 768

Key Data:

```
307c300d 06092a86 4886f70d 01010105 00036b00 30680261 00bb8204 bdf8500e
7abf837d d9b2e0c9 a7e558c3 57e559b7 ea514afb ea1913f9 2cfdd0db fb944a53
23fd196f 38428fc2 26d2aeb9 e8060139 e0cb5f58 f089052a 8bdca9be a9357b46
a74067ee 164efd6f 898b504c f0da88af 695af6b1 7fd34458 0b020301 0001
```

```
ASA1/admin# show ssh
```

```
Timeout: 5 minutes
```

```
Versions allowed: 1 and 2
```

```
192.168.1.0 255.255.255.0 mgmt
```

```
192.168.2.0 255.255.255.0 mgmt
```

```
access-list ssh-acl extended permit tcp 192.168.2.0 255.255.255.0 any eq 22
```

```
class-map mgmt-class  
  match access-list ssh-acl
```

```
ASA1/admin# show service-policy int mgmt
```

```
Interface mgmt:
```

```
  Service-policy: mgmt-policy
```

```
    Class-map: mgmt-class
```

```
Set connection policy:          drop 0
```

```
Set connection timeout policy:
```

```
  idle 0:01:00
```

```
  DCD: disabled, retry-interval 0:00:15, max-retries 5
```

```
  DCD: client-probe 0, server-probe 0, conn-expiration 0
```

```
SW1# ssh -l cisco 192.168.1.20
```

```
Password: cisco
```

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

```
ASA1/admin>en
```

```
Password: *****
```

```
ASA1/admin# show running-config
```

```
: Saved
```

```
:
```

```
ASA Version 8.4(5) <context>
```

```
!
```

```
hostname ciscoasa
```

```
ASA1/admin# show ssh session
```

SID	Client IP	Version	Mode	Encryption	Hmac	State	Username
0	192.168.1.5	2.0	IN	aes128-cbc	sha1	SessionStarted	cisco
			OUT	aes128-cbc	sha1	SessionStarted	cisco

```
SW1# ssh -l support 192.168.1.20
Password: cisco
Type help or '?' for a list of available commands.
ASA1/admin>
ASA1/admin> en 5
Password: *****

ASA1/admin# show running-config
          ^
ERROR: % Invalid input detected at '^' marker.
ERROR: Command authorization failed
```

```
ASA1/admin# show xlate
0 in use, 0 most used
ASA1/admin# show route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

```
Gateway of last resort is 192.168.1.5 to network 0.0.0.0
```

```
C 192.168.1.0 255.255.255.0 is directly connected, mgmt
S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.1.5, mgmt
ASA1/admin#
```

```
ASA1/admin# show ssh session
```

SID	Client IP	Version	Mode	Encryption	Hma	State	Username
0	192.168.1.5	2.0	IN	aes128-cbc	shal	SessionStarted	support
			OUT	aes128-cbc	shal	SessionStarted	support


```
username support password cisco privilege 5
username cisco password cisco

aaa authentication ssh console LOCAL
ssh 192.168.1.0 255.255.255.0 mgmt
ssh 192.168.2.0 255.255.255.0 mgmt

object-group service ssh tcp
port-object eq ssh
access-list ssh-acl extended permit tcp 192.168.2.0 255.255.255.0 any object-group
ssh

class-map mgmt-class
match access-list ssh-acl

policy-map mgmt-policy
class mgmt-class
set connection timeout idle 0:01:00
!
service-policy mgmt-policy interface mgmt

enable password cisco level 5
enable password cisco

privilege show level 5 mode exec command xlate
privilege show level 5 mode exec command route
```

```
R6# telnet server.ccie.com
```

```
Translating "server.ccie.com"...domain server (10.50.100.2)
```

```
Translating "server.ccie.com"...domain server (10.50.100.2) [OK]
```

```
Trying server.ccie.com (10.10.130.1)...
```

```
% Connection timed out; remote host not responding
```

```
ASA1/c2# show dynamic-filter dns-snoop detail
```

```
DNS Reverse Cache Summary Information:
```

```
1 addresses, 1 names
```

```
Next housekeeping scheduled at 19:23:50 UTC Sep 19 2013,
```

```
DNS reverse Cache Information:
```

```
[10.10.130.1] flags=0x2, type=2, unit=0 b:u:w=1:0:0, cookie=0x751dae80
```

```
  [server.ccie.com] type=2, ttl=0
```

%ASA-6-338301: Intercepted DNS reply for name server.ccie.com from
inside:10.50.100.2/53 to
outside:10.50.80.6/52007, matched blacklist

%ASA-6-302016: Teardown UDP connection 824265 for outside:10.50.80.6/52007 to
inside:10.50.100.2/53 duration 0:00:00 bytes 82

%ASA-4-338002: Dynamic Filter monitored blacklisted TCP traffic from
outside:10.50.80.6/16988
(10.50.80.6/16988) to inside:10.10.130.1/23 (10.10.130.1/23), destination
10.10.130.1 resolved
from local list: server.ccie.com, threat-level: very-high, category: admin-added

%ASA-4-338006: Dynamic Filter dropped blacklisted TCP traffic from
outside:10.50.80.6/16988
(10.50.80.6/16988) to inside:10.10.130.1/23 (10.10.130.1/23), destination
10.10.130.1 resolved
from local list: server.ccie.com, threat-level: very-high, category: admin-added

ASA1/c2# show dynamic-filter reports top malware-sites

Malware Sites (since last clear)

Site	Connections	Logged	Dropped	Threat-level	Category

10.10.130.1 (server.ccie.com)	4		4	very-high	admin-added

Last clearing of the top sites report: Never

R6# telnet 10.10.110.1

Trying 10.10.110.1 ... Open

ASA1/c2# show dynamic-filter statistics

Enabled on interface outside

Total conns classified 57, ingress 17, egress 40

Total whitelist classified 1, ingress 1, egress 0

Total greylist classified 0, dropped 0, ingress 0, egress 0

Total blacklist classified 56, dropped 56, ingress 16, egress 40

```
%ASA-6-338104: Dynamic Filter monitored whitelisted TCP traffic from  
  outside:10.50.80.6/52071  
(10.50.80.6/52071) to inside:10.10.110.1/23 (10.10.110.1/23), destination  
  10.10.110.1 resolved  
from local list: 10.10.0.0/255.255.0.0
```

ASA2# show threat-detection statistics protocol

	Average (eps)	Current (eps)	Trigger	Total events
OSPF * 89: tot-ses:0 act-ses:0				
1-hour Sent byte:	0	0	0	592
1-hour Sent pkts:	0	0	0	7

ASA2# show threat-detection statistics port

	Average (eps)	Current (eps)	Trigger	Total events
Isakmp 500: tot-ses:2070 act-ses:1				
1-hour Sent byte:	0	0	0	328
1-hour Sent pkts:	0	0	0	2
1-hour Recv byte:	0	0	0	344
1-hour Recv pkts:	0	0	0	2

R6# ping 192.168.2.5 size 2000

Type escape sequence to abort.

Sending 5, 2000-byte ICMP Echos to 192.168.2.5, timeout is 2 seconds:

.....

IP AUDIT INTERFACE COUNTERS: outside

2011 I ICMP Address Mask Request	0
2012 I ICMP Address Mask Reply	0
2150 A Fragmented ICMP	10
2151 A Large ICMP	0
2154 A Ping of Death	0

```
R6# ping 192.168.2.5
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.2.5, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
```

```
IP AUDIT INTERFACE COUNTERS: inside
```

1100	A	IP Fragment Attack	0
1102	A	Impossible IP Packet	0
1103	A	IP Teardrop	0
2000	I	ICMP Echo Reply	5
2001	I	ICMP Unreachable	0

```
threat-detection basic-threat
threat-detection statistics port
threat-detection statistics protocol
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
```

```
ip audit name inside info action alarm
ip audit name outside attack action reset
ip audit interface outside outside
ip audit interface inside inside
```

```
dynamic-filter enable interface outside
dynamic-filter drop blacklist interface outside
dynamic-filter blacklist
  name server.ccie.com
dynamic-filter whitelist
  address 10.10.110.0 255.255.255.0
  address 10.10.120.0 255.255.255.0
class-map dynamic-filter-dns-snoop
  match port udp eq domain

policy-map dynamic-filter-dns-snoop
  class dynamic-filter-dns-snoop
    inspect dns dynamic-filter-snoop

service-policy dynamic-filter-dns-snoop interface outside
```

```
ASA2# show ipv6 int inside
```

```
inside is up, line protocol is up
```

```
IPv6 is enabled, link-local address is fe80::215:c6ff:fe95:c648
```

```
Global unicast address(es):
```

```
  2001:db8:40::20, subnet is 2001:db8:40::/64
```

```
Joined group address(es):
```

```
  ff02::1
```

```
  ff02::2
```

```
  ff02::1:ff00:20
```

```
  ff02::1:ff95:c648
```

```
ICMP error messages limited to one every 100 milliseconds
```

```
ICMP redirects are enabled
```

```
ND DAD is enabled, number of DAD attempts: 1
```

```
ND reachable time is 30000 milliseconds
```

```
Hosts use stateless autoconfig for addresses.
```

```
ASA2# show ipv6 int dmz
```

```
dmz is up, line protocol is up
```

```
IPv6 is enabled, link-local address is fe80::215:c6ff:fe95:c649
```

```
Global unicast address(es):
```

```
  2001:db9:30::20, subnet is 2001:db9:30::/64
```

```
Joined group address(es):
```

```
  ff02::1
```

```
  ff02::2
```

```
  ff02::1:ff00:20
```

```
  ff02::1:ff95:c649
```

```
ICMP error messages limited to one every 100 milliseconds
```

```
ICMP redirects are enabled
```

```
ND DAD is enabled, number of DAD attempts: 1
```

```
ND reachable time is 30000 milliseconds
```

```
Hosts use stateless autoconfig for addresses.
```

```
ASA2# show run | begin interface GigabitEthernet0/2
interface GigabitEthernet0/2
  nameif inside
  security-level 100
  ip address 10.50.40.20 255.255.255.0
  ipv6 address 2001:db8:40::20/64
  ipv6 enable
  ipv6 nd suppress-ra
  ospf message-digest-key 1 md5 *****
  ospf authentication message-digest
```

```
ASA2# show run | begin interface GigabitEthernet0/3
interface GigabitEthernet0/3
  nameif dmz
  security-level 50
  ip address 10.50.30.20 255.255.255.0
  ipv6 address 2001:db9:30::20/64
  ipv6 enable
  ipv6 nd suppress-ra
```



```
interface GigabitEthernet0/2
  ipv6 address 2001:db8:40::20/64
  ipv6 enable
  ipv6 nd suppress-ra
```

```
ASA2# show run | begin interface GigabitEthernet0/3
interface GigabitEthernet0/3
  ipv6 address 2001:db9:30::20/64
  ipv6 enable
  ipv6 nd suppress-ra
```

```
R6# show zone security
zone self
  Description: System defined zone
```

```
zone outside
Member Interfaces:
  Ethernet0/1
```

```
zone inside
Member Interfaces:
  Ethernet0/0
```

```
R6# show policy-map type inspect zone-pair sessions
```

```
policy exists on zp out-in
```

```
Zone-pair: out-in
```

```
Service-policy inspect : firewall-policy-in
```

```
Class-map: crypto (match-any)
```

```
Match: access-group 102
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Match: protocol isakmp
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Match: protocol gdoi
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Match: access-group 103
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Pass
```

```
0 packets, 0 bytes
```

```
Class-map: sgt4policy (match-all)
```

```
Match: class-map match-any sgt4
```

```
Match: security-group source tag 4
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Match: class-map match-any in-sgt-inspect
```

```
Match: protocol icmp
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Match: protocol udp
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Class-map: sgt5policy (match-all)
```

```
Match: class-map match-any sgt5
```

```
Match: security-group source tag 5
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Match: class-map match-any in-sgt-inspect
```

```
Match: protocol icmp
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Match: protocol udp
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Inspect
```

```
Class-map: in-inspect (match-any)
```

```
Match: protocol icmp
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Match: protocol telnet
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Match: protocol dns
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Match: protocol ntp
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Match: protocol radius
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Match: protocol tacacs
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Match: protocol http
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Match: protocol https
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Inspect
```

```
Class-map: class-default (match-any)
```

```
Match: any
```

```
Drop
```

```
0 packets, 0 bytes
```

```
policy exists on zp in-out
```

```
Zone-pair: in-out
```

```
Service-policy inspect : firewall-policy-out
```

```
Class-map: crypto (match-any)
```

```
Match: access-group 102
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Match: protocol isakmp
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Match: protocol gdoi
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Match: access-group 103
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Pass
```

```
0 packets, 0 bytes
```

```
Class-map: http (match-all)
```

```
Match: protocol http
```

```
Inspect
```

```
Class-map: out-inspect (match-any)
```

```
Match: access-group 101
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Inspect
```

```
Class-map: class-default (match-any)
```

```
Match: any
```

```
Drop
```

```
0 packets, 0 bytes
```

```
R6# show access-list
```

```
Extended IP access list 101
```

```
10 permit ip any any
```

```
Extended IP access list 102
```

```
10 permit udp 10.50.0.0 0.0.255.255 10.50.0.0 0.0.255.255 eq non500-isakmp
```

```
20 permit esp 10.50.0.0 0.0.255.255 10.50.0.0 0.0.255.255
```

```
Extended IP access list 103
```

```
10 permit gre 10.50.0.0 0.0.255.255 10.50.0.0 0.0.255.255
```

```
R6# show class-map type inspect http
Class Map type inspect http match-any httpDPI (id 2)
  Match request port-misuse tunneling

R6# show policy-map type inspect http
Policy Map type inspect http resetportmisuse
  Class httpDPI
    Reset
    Log
```

R6# show cts role sgt all

Active IP-SGT Bindings Information

IP Address	SGT	Source
10.50.9.5	2	SXP
10.50.9.7	4	SXP
10.50.30.3	12	SXP
10.50.30.4	12	SXP
10.50.40.7	7	SXP
10.50.50.5	2	SXP
10.50.50.20	14	SXP
10.50.70.4	3	SXP
10.50.70.5	2	SXP
10.50.70.6	3	SXP
10.50.77.5	2	SXP
10.50.77.253	5	SXP
10.50.80.50	16	SXP
10.50.99.5	2	SXP
10.50.100.1	15	SXP
10.50.100.2	15	SXP
10.50.100.10	15	SXP
192.168.2.25	18	SXP


```
cts exp enable
cts exp connection peer 10.50.70.5 password none mode local listener
class-map type inspect match-any crypto
  match access-group 102
  match protocol isakmp
  match protocol gdoi
  match access-group 103
class-map type inspect match-any in-sgt-inspect
  match protocol icmp
  match protocol udp
class-map type inspect match-all http
  match protocol http
class-map type inspect match-any out-inspect
  match access-group 101
class-map type inspect http match-any httpDPI
  match request port-misuse tunneling
class-map type inspect match-any sgt4
  match security-group source tag 4
class-map type inspect match-all sgt4policy
  match class-map sgt4
  match class-map in-sgt-inspect
class-map type inspect match-any sgt5
  match security-group source tag 5
class-map type inspect match-all sgt5policy
  match class-map sgt5
  match class-map in-sgt-inspect
class-map type inspect match-any in-inspect
  match protocol icmp
  match protocol telnet
  match protocol dns
```

```

match protocol ntp
match protocol radius
match protocol tacacs
match protocol http
match protocol https!
!
policy-map type inspect http resetportmisuse
class type inspect http httpDPI
  reset
!
policy-map type inspect firewall-policy-in
class type inspect crypto
  pass
class type inspect sgt4policy
  inspect
class type inspect sgt5policy
  inspect
class type inspect in-inspect
  inspect
class class-default
  drop
!

policy-map type inspect firewall-policy-out
class type inspect crypto
  pass
class type inspect http
  inspect
  service-policy http resetportmisuse
class type inspect out-inspect
  inspect
class class-default
  drop
!
zone security outside
zone security inside
zone-pair security out-in source outside destination inside
  service-policy type inspect firewall-policy-in
zone-pair security in-out source inside destination outside
  service-policy type inspect firewall-policy-out
!
interface Ethernet0/0
  zone-member security inside
!
interface Ethernet0/1
  zone-member security outside

access-list 101 permit ip any any
access-list 102 permit udp 10.50.0.0 0.0.255.255 10.50.0.0 0.0.255.255 eq
  non500-isakmp
access-list 102 permit esp 10.50.0.0 0.0.255.255 10.50.0.0 0.0.255.255
access-list 103 permit gre 10.50.0.0 0.0.255.255 10.50.0.0 0.0.255.255

```

```
Device(config)# class-map type inspect match-all c1
Device(config-cmap)# match access-group 101
Device(config-cmap)# match protocol http
```

```
Device(config)# class-map type inspect match-all c1
Device(config-cmap)# match protocol http
Device(config-cmap)# match protocol icmp
```

```
Device(config)# class-map type inspect match-any c1
Device(config-cmap)# match protocol http
Device(config-cmap)# match protocol icmp
```

Device(config)# class-map type inspect ?

aol	Configure Firewall class-map for IM-AOL protocol
edonkey	eDonkey
fasttrack	FastTrack Traffic - KaZaA, Morpheus, Grokster...
gnutella	Gnutella Version2 Traffic - BearShare, Shareeza, Morpheus ...
h323	Configure Firewall class-map for H323 protocol
http	Configure Firewall class-map for HTTP protocol
icq	Configure Firewall class-map for IM-ICQ protocol
imap	Configure Firewall class-map for IMAP protocol
kazaa2	Kazaa Version 2
match-all	Logical-AND all matching statements under this classmap
match-any	Logical-OR all matching statements under this classmap
msnmsgr	Configure Firewall class-map for IM-MSN protocol
pop3	Configure Firewall class-map for POP3 protocol
sip	Configure Firewall class-map for SIP protocol
smtp	Configure Firewall class-map for SMTP protocol
sunrpc	Configure Firewall class-map for RPC protocol
winmsgr	Configure Firewall class-map for IM-WINMSGR protocol
ymsgr	Configure Firewall class-map for IM-YAHOO protocol

```
R6(config)# class-map type inspect match-all http
R6(config-cmap)# match protocol http
```

```
R6(config)# class-map type inspect http match-any httpDPI
R6(config-cmap)# match request port-misuse ?
  any          Any type of port misuse
  im           Instant Messaging
  p2p         Peer-to-peer application
  tunneling   Tunneling applications

R6(config-cmap)# match request port-misuse tunneling
R6(config-cmap)# exit
```



```
R6(config)# policy-map type inspect http resetportmisuse
R6(config-pmap)# class type inspect http httpDPI
R6(config-pmap-c)# reset
```

```
R6(config)# policy-map type inspect firewall-policy
R6(config-pmap)# class type inspect remotes2
R6(config-pmap-c)# inspect
R6(config-pmap-c)# service-policy http resetportmisuse
```

IPS# show events alert medium

evIdsAlert: eventId=1374345338767123448 severity=medium vendor=Cisco

originator:

hostId: ips

appName: sensorApp

appInstanceId: 414

time: 2013/08/27 21:42:25 2013/08/27 21:42:25 UTC

signature: description=OSPF TTL id=64000 created=20000101 type=other
version=custom

subsigId: 0

sigDetails: My Sig Info

marsCategory: Info/Misc

interfaceGroup: vs0

vlan: 70

participants:

attacker:

addr: locality=OUT 10.50.70.5

target:

addr: locality=OUT 224.0.0.5

os: idSource=unknown relevance=relevant type=unknown

triggerPacket:

```
000000 01 00 5E 00 00 05 C4 64 13 FC 2A 44 81 00 C0 32 ..^....d..*D...2
000010 08 00 45 C0 00 50 E0 C6 00 00 FF 59 A9 91 0A 32 ..E..P.....Y...2
000020 46 05 E0 00 00 05 02 01 00 30 02 02 02 02 00 00 F.....0.....
000030 00 00 3C 1B 00 00 00 00 00 00 00 00 00 00 FF FF ..<.....
000040 FF 00 00 0A 12 01 00 00 00 28 0A 32 46 06 0A 32 .....(.2F..2
000050 46 05 06 06 06 06 FF F6 00 03 00 01 00 04 00 00 F.....
000060 00 01 ..
```

riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 66

threatRatingValue: 66

interface: ge0_2

protocol: IP protocol 89

R6# ping 10.50.40.7 size 1500

IPS# show event alert high

```
evIdsAlert: eventId=1374345338767123402 severity=high vendor=Cisco
  originator:
    hostId: ips
    appName: sensorApp
    appInstanceId: 414
  time: 2013/08/27 21:23:46 2013/08/27 21:23:46 UTC
  signature: description=Large ICMP Attack id=65000 created=20000101 type=other
             version=custom
    subsigId: 0
    sigDetails: My Sig Info
    marsCategory: Info/Misc
  interfaceGroup: vs0
  vlan: 50
  participants:
    attacker:
      addr: locality=OUT 10.50.70.6
    target:
      addr: locality=OUT 10.50.40.7
      os: idSource=unknown relevance=relevant type=unknown
  triggerPacket:
000000 00 15 C6 95 C6 46 C4 64 13 FC 2A 43 81 00 00 46 .....F.d..*C...F
000010 08 00 45 00 05 DC 00 A6 00 00 FE 01 34 0A 0A 32 ..E.....4..2
000020 46 06 0A 32 28 07 08 00 C0 2E 00 0A 00 01 00 00 F..2(.....
000030 00 00 0F B9 E7 F5 AB CD AB CD AB CD AB CD AB CD .....
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 85
  threatRatingValue: 85
  interface: ge0_2
  protocol: icmp
```

```
R6# ping 192.168.2.25 rep 200
Type escape sequence to abort.
Sending 2000, 100-byte ICMP Echos to 192.168.2.25, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
..
```

IPS# show events alert high

```
evIdsAlert: eventId=1374345338767164950 severity=high vendor=Cisco
originator:
  hostId: ips
  appName: sensorApp
  appInstanceId: 414
time: 2013/09/21 01:34:31 2013/09/21 01:34:31 UTC
signature: description=My Sig id=62000 created=20000101 type=other
  version=custom
  subsigId: 0
  sigDetails: My Sig Info
  marsCategory: Info/Misc
interfaceGroup: vs1
vlan: 0
participants:
  attacker:
    addr: locality=OUT 10.50.80.6
  target:
    addr: locality=OUT 192.168.2.25
    os: idSource=learned relevance=relevant type=windows-nt-2k-xp
actions:
  logPacketsActivated: true
  deniedPacket: true
  deniedAttacker: true
  logAttackerPacketsActivated: true
ipLogIds:
  ipLogId: 1701736978
riskRatingValue: attackRelevanceRating=relevant targetValueRating=mission-
  critical 100
threatRatingValue: 55
interface: ge0_0
protocol: icmp
```

R3# ping 192.168.2.50 rep 100

Type escape sequence to abort.

Sending 100, 100-byte ICMP Echos to 192.168.2.50, timeout is 2 seconds:

!!
!!.

IPS# show events alert high

evIdsAlert: eventId=1374345338767164960 severity=high vendor=Cisco

originator:

hostId: ips

appName: sensorApp

appInstanceId: 414

time: 2013/09/21 01:40:50 2013/09/21 01:40:50 UTC

signature: description=My Sig id=62000 created=20000101 type=other
version=custom

subsigId: 0

sigDetails: My Sig Info

marsCategory: Info/Misc

interfaceGroup: vs1

vlan: 0

participants:

attacker:

addr: locality=OUT 10.50.30.3

target:

addr: locality=OUT 192.168.2.50

os: idSource=learned relevance=relevant type=bsd

actions:

deniedPacket: true

riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 85

threatRatingValue: 50

interface: ge0_0

protocol: icmp

IPS# show stat virtual-sensor vs1

Statistics for Virtual Sensor vs1

Name of current Signature-Definition instance = sig1

Name of current Event-Action-Rules instance = rules1

.....

Denied Address Information

Number of Active Denied Attackers = 1

Number of Denied Attackers Inserted = 1

Number of Denied Attacker Victim Pairs Inserted = 0

Number of Denied Attacker Service Pairs Inserted = 0

Number of Denied Attackers Total Hits = 439

Number of times max-denied-attackers limited creation of new entry = 0

Number of exec Clear commands during uptime = 0

Denied Attackers and hit count for each.

10.50.80.6 = 439

Denied Attackers with percent denied and hit count for each

Attacker Address	Victim Address	Port	Protocol	Requested Percentage	Actual Percentage	Hit Count	Reputation	Action
10.50.80.6				100	100	439	false	

Actions Performed

deny-attacker-inline = 0

deny-attacker-victim-pair-inline = 0

deny-attacker-service-pair-inline = 0

deny-connection-inline = 0

deny-packet-inline = 48

modify-packet-inline = 1588

log-attacker-packets = 20

log-pair-packets = 0

log-victim-packets = 0

produce-alert = 37

produce-verbose-alert = 2

request-block-connection = 0

request-block-host = 0

request-snmp-trap = 0

```
service event-action-rules rules1
overrides deny-attacker-inline
override-item-status Enabled
risk-rating-range 90-100
exit
overrides log-attacker-packets
override-item-status Enabled
risk-rating-range 90-100
exit
overrides produce-alert
override-item-status Enabled
exit
target-value mission-critical target-address 192.168.2.25
exit
```

```
service signature-definition sig0
signatures 64000 0
alert-severity medium
sig-description
sig-name OSPF TTL
exit
engine atomic-ip
event-action produce-verbose-alert
specify-14-protocol yes
14-protocol other-protocol
other-ip-protocol-id 89
exit
exit
specify-ip-ttl yes
ip-ttl 255
exit
```



```
exit
status
enabled true
exit
exit
signatures 65000 0
alert-severity high
sig-description
sig-name Large ICMP Attack
exit
engine atomic-ip
event-action produce-verbose-alert
specify-l4-protocol yes
l4-protocol icmp
exit
exit
specify-ip-payload-length yes
ip-payload-length 1000-5000
exit
specify-ip-addr-options yes
ip-addr-options rfc-1918-address
exit
exit
status
enabled true
exit
exit
exit
! -----
service signature-definition sig1
signatures 62000 0
alert-severity high
engine flood-host
event-action produce-alert|deny-packet-inline
rate 100
protocol icmp
icmp-type 8
exit
exit
status
enabled true
exit
exit
exit
```

```
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/2 subinterface-number 1
exit
virtual-sensor vs1
signature-definition sig1
event-action-rules rules1
logical-interface ipair
exit
virtual-sensor vs2
physical-interface GigabitEthernet0/3
exit
exit
```

```
R4# show ip http server secure status
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5
    rc4-128-sha
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:
HTTP secure server active session modules: ALL
```

R4# **sho ip http server history** (note this must be completed after attempting a connection from a Test-PC using https://10.50.30.4 otherwise the history may be blank).

R4# **show ip http server history**

HTTP server history:

local-ipaddress:port	remote-ipaddress:port	in-bytes	out-bytes	end-time
10.50.30.4:443	192.168.2.50:28325	375	192	05:27:35
10.50.30.4:443	192.168.2.50:19583	371	2069	05:27:48
10.50.30.4:443	192.168.2.50:35418	324	137	05:27:48
10.50.30.4:443	192.168.2.50:50014	417	6043	05:29:08
10.50.30.4:443	192.168.2.50:55682	324	137	05:29:08

HTTP server history:

local-ipaddress:port	remote-ipaddress:port	in-bytes	out-bytes	end-time
10.50.50.5:80	192.168.2.50:64008	3547	251686	19:55:45 04/23
10.50.50.5:80	192.168.2.50:9612	4118	270121	19:55:45 04/23

```
ASA2# show ipv6 access-list
```

```
ipv6 access-list vpn line 1 permit esp 2001:DB9:30::4/64 2001:DB8:40::7/64
```

```
ipv6 access-list vpn line 3 permit udp 2001:DB9:30::4/64 2001:DB8:40::7/64 eq  
  isakmp
```

```
crypto pki trustpoint ciscoca
enrollment retry count 5
enrollment retry period 3
enrollment url http://10.50.100.1:8080
revocation-check none
```

```
R7(config)# crypto key gen rsa
```

Specify a modulus, this lab question uses 1024 bits.

R7# show crypto key mypubkey rsa

% Key pair was generated at: 12:17:36 PST Sep 28 2013

Key name: R7.cisco.com

Key type: RSA KEYS

Storage Device: private-config

Usage: General Purpose Key

Key is not exportable.

Key Data:

30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00D495EA
395B6FDF 58DEB196 A46E8AC8 1336D428 5D450B4B 53695EC1 43DAF2FA 219689D7
5AB9245E B08D2958 B9F18189 B92A0FF1 EBD47E7B F5ED8D59 0C193191 5D25FCD2
DC45F474 675598F4 F24EF34F 68397297 D270BC5F 6C554876 AC7A39F5 6DCD42D6
F98D59CE CE189BFE 2C027C77 39F7ED96 784779E3 3A7EF457 F3DDB6BF 1F020301 0001

R4(config)# crypto pki authenticate ciscoca

Certificate has the following attributes:

Fingerprint MD5: 1F5A02E4 C2C8230A 56FC15BB CBDFBEF6

Fingerprint SHA1: 99D5D0AA 928B4DD8 7D9E6D98 B3831F1D 796C6A71

% Do you accept this certificate? [yes/no]: yes

R4(config)# crypto pki enroll ciscoca

%

% Start certificate enrollment ..

% Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate.

For security reasons your password will not be saved in the configuration.

Please make a note of it.

Password: cisco

Re-enter password: cisco

% The subject name in the certificate will include: R4.cisco.com

% Include the router serial number in the subject name? [yes/no]: no

% Include an IP address in the subject name? [no]: no

Request certificate from CA? [yes/no]: yes

% Certificate request sent to Certificate Authority

% The 'show crypto pki certificate verbose ciscoca' command will show the fingerprint.

R4(config)#

*Sep 29 01:17:00.529: CRYPTO_PKI: Certificate Request Fingerprint MD5: AC5647CD
4607D9DC 3819945F 12535ACC

*Sep 29 01:17:00.529: CRYPTO_PKI: Certificate Request Fingerprint SHA1: E01B51B5
B5F301AC 64B298FF D022E769 DA27D496

R4(config)#

*Sep 29 01:17:00.611: %PKI-6-CERTRET: Certificate received from Certificate Authority

R4# show cry pki certificates

Certificate

Status: Available
Certificate Serial Number (hex): 02
Certificate Usage: General Purpose
Issuer:
 cn=ciscoca.cisco.com L=cisco C=US
Subject:
 Name: R4.cisco.com
 hostname=R4.cisco.com
Validity Date:
 start date: 17:17:00 PST Sep 28 2013
 end date: 17:17:00 PST Apr 16 2014
Associated Trustpoints: ciscoca
Storage: nvram:ciscocacisco#2.cer

CA Certificate

Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
 cn=ciscoca.cisco.com L=cisco C=US
Subject:
 cn=ciscoca.cisco.com L=cisco C=US
Validity Date:
 start date: 13:19:37 PST Aug 17 2013
 end date: 13:19:37 PST Aug 17 2014
Associated Trustpoints: ciscoca
Storage: nvram:ciscocacisco#1CA.cer

R7# show cry pki certificates

Certificate

Status: Available
Certificate Serial Number (hex): 0A
Certificate Usage: General Purpose
Issuer:
 cn=ciscoca.cisco.com L=cisco C=US
Subject:
 Name: R7.cisco.com
 hostname=R7.cisco.com
Validity Date:
 start date: 18:39:45 PST Sep 28 2013
 end date: 18:39:45 PST Apr 16 2014
Associated Trustpoints: ciscoca
Storage: nvram:ciscocacisco#A.cer

CA Certificate

Status: Available

Certificate Serial Number (hex): 01

Certificate Usage: Signature

Issuer:

cn=ciscoca.cisco.com L=cisco C=US

Subject:

cn=ciscoca.cisco.com L=cisco C=US

Validity Date:

start date: 13:19:37 PST Aug 17 2013

end date: 13:19:37 PST Aug 17 2014

Associated Trustpoints: ciscoca

Storage: nvram:ciscocacisco#1CA.cer

R7# show crypto session

Interface: Tunnel2

Profile: ipv6

Session status: UP-ACTIVE

Peer: 2001:DB9:30::4 port 500

 IKEv1 SA: local 2001:DB8:40::7/500

 remote 2001:DB9:30::4/500 Active

 IPSEC FLOW: permit ipv6 ::/0 ::/0

 Active SAs: 2, origin: crypto map

R4# show crypto session

Interface: Tunnel2

Profile: ipv6

Session status: UP-ACTIVE

Peer: 2001:DB8:40::7 port 500

 IKEv1 SA: local 2001:DB9:30::4/500

 remote 2001:DB8:40::7/500 Active

 IPSEC FLOW: permit ipv6 ::/0 ::/0

 Active SAs: 2, origin: crypto map

R7# show ipv6 route

IPv6 Routing Table - default - 9 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP

H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea

IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO

ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect

l - LISP

O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

```
S ::/0 [1/0]
  via 2001:DB8:40::20
C 1011::/64 [0/0]
  via Loopback1, directly connected
L 1011::8A43:E1FF:FEB1:B380/128 [0/0]
  via Loopback1, receive
C 2001:DB8:40::/64 [0/0]
  via GigabitEthernet0/1, directly connected
L 2001:DB8:40::7/128 [0/0]
  via GigabitEthernet0/1, receive
C 2001:DBA::/64 [0/0]
  via Tunnel2, directly connected
L 2001:DBA::1:1/128 [0/0]
  via Tunnel2, receive
EX 2011::/64 [170/27008000]
  via FE80::A8BB:CCFF:FE00:7C00, Tunnel2
L FF00::/8 [0/0]
  via Null0, receive
```

R4# show ipv6 route

IPv6 Routing Table - default - 9 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP

H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea

IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO

ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect

l - LISP

O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

```
S ::/0 [1/0]
  via 2001:DB9:30::20
EX 1011::/64 [170/27008000]
  via FE80::8A43:E1FF:FEB1:B380, Tunnel2
C 2001:DB9:30::/64 [0/0]
  via Ethernet0/1, directly connected
L 2001:DB9:30::4/128 [0/0]
```

```
    via Ethernet0/1, receive
C 2001:DBA::/64 [0/0]
    via Tunnel2, directly connected
L 2001:DBA::1:2/128 [0/0]
    via Tunnel2, receive
C 2011::/64 [0/0]
    via Loopback1, directly connected
L 2011::A8BB:CCFF:FE00:7C00/128 [0/0]
    via Loopback1, receive
L FF00::/8 [0/0]
    via Null0, receive
```

ASA2# show conn

UDP dmz 2001:db9:30::4:500 inside 2001:db8:40::7:500, idle 0:00:08, bytes 336,
flags -

ESP dmz 2001:db9:30::4 inside 2001:db8:40::7, idle 0:00:03, bytes 7776


```
ipv6 unicast-routing

crypto pki certificate map certmap 1
  issuer-name co cisco.com
  unstructured-subject-name co r4.cisco.com

crypto pki trustpoint ciscoca
  enrollment retry count 5
  enrollment retry period 3
  enrollment url http://10.50.100.1:8080
  revocation-check none

crypto isakmp policy 2
  group 5

crypto isakmp identity dn
crypto isakmp profile ipv6
  ca trust-point ciscoca
  match certificate certmap

crypto ipsec transform-set 3des esp-3des esp-md5-hmac
!
crypto ipsec profile profilev6
  set transform-set 3des
  set isakmp-profile ipv6

interface Loopback1
  ip address 10.7.7.7 255.255.255.0
  ipv6 address 1011::/64 eui-64

interface Tunnel2
  no ip address
  ipv6 address 2001:DBA::1:1/64
  ipv6 enable
  ipv6 eigrp 1
  tunnel source GigabitEthernet0/1
  tunnel mode ipsec ipv6
  tunnel destination 2001:DB9:30::4
  tunnel protection ipsec profile profilev6

interface GigabitEthernet0/1
```

```
ip address 10.50.40.7 255.255.255.0
ip flow ingress
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
duplex auto
speed auto
ipv6 address 2001:DB8:40::7/64
ipv6 enable

ipv6 route ::/0 2001:DB8:40::20
ipv6 router eigrp 1
  distribute-list prefix-list loopback out
  redistribute connected
!
!
!
ipv6 prefix-list loopback seq 5 permit 1011::/64
!
ntp server 10.50.70.6
```

```
ipv6 unicast-routing

crypto pki certificate map certmap 1
  issuer-name co cisco.com
  unstructured-subject-name co r7.cisco.com

crypto isakmp policy 2
  group 5

crypto pki trustpoint ciscoca
  enrollment retry count 5
  enrollment retry period 3
  enrollment url http://10.50.100.1:8080
  revocation-check none

crypto isakmp identity dn
crypto isakmp profile ipv6
  ca trust-point ciscoca
  match certificate certmap

crypto ipsec transform-set 3des esp-3des esp-md5-hmac
!
crypto ipsec profile profilev6
  set transform-set 3des
  set isakmp-profile ipv6

interface Loopback1
  ip address 10.4.4.4 255.255.255.0
  ipv6 address 2011::/64 eui-64

interface Tunnel2
  no ip address
  ipv6 address 2001:DBA::1:2/64
  ipv6 enable
  ipv6 eigrp 1
  tunnel source Ethernet0/1
  tunnel mode ipsec ipv6
  tunnel destination 2001:DB8:40::7
  tunnel protection ipsec profile profilev6

interface Ethernet0/1
```

```
ip address 10.50.30.4 255.255.255.0
ipv6 address 2001:DB9:30::4/64
ipv6 enable

ipv6 route ::/0 2001:DB9:30::20
ipv6 router eigrp 1
  distribute-list prefix-list loopback out
  redistribute connected
!
!
!
ipv6 prefix-list loopback seq 5 permit 2011::/64
!
ntp server 10.50.70.6
```

```
ipv6 access-list vpn permit udp 2001:DB9:30::4/64 2001:DB8:40::7/64 eq 500  
ipv6 access-list vpn permit esp 2001:DB9:30::4/64 2001:DB8:40::7/64
```

```
access-group vpn in interface dmz
```

```
crypto isakmp identity address
```

```
crypto keyring ipv6keys
```

```
pre-shared-key address ipv6 ::/0 key cisco123
```

```
! preceding line uses a match-all address, a specific IPv6 address per peer can  
also be used and is preferred when applicable.
```

```
crypto isakmp profile ipv6
```

```
keyring ipv6keys
```

```
match identity address ipv6 2001:DB9:30::4/64
```

```
crypto key generate rsa modulus 1024 label REKEYRSA
```

```
show crypto key mypubkey rsa
```



```
crypto key generate rsa modulus 1024 label REKEYRSA exportable
```

```
crypto key export rsa GETVPN_KEYS pem terminal 3des CISCO1234
```

```
crypto key import rsa GETVPN_KEYS pem exportable terminal CISCO1234
```

```
ASA1/c2# show conn
```

```
16 in use, 19 most used
```

```
GRE outside 10.50.40.7:0 inside 10.50.100.2:0, idle 0:00:01, bytes 42384, flags E  
GRE outside 10.50.80.6:0 inside 10.50.100.2:0, idle 0:00:03, bytes 42806, flags E  
GRE outside 10.50.80.6:0 inside 10.50.100.1:0, idle 0:00:01, bytes 50952, flags E  
GRE outside 10.50.40.7:0 inside 10.50.100.1:0, idle 0:00:18, bytes 56334, flags E  
UDP outside 10.50.70.6:848 inside 10.50.100.1:848, idle 0:00:07, bytes 2136, flags -  
UDP outside 10.50.40.7:848 inside 10.50.100.1:848, idle 0:00:07, bytes 2136, flags -
```

```
ASA2(config)# show conn
```

```
26 in use, 41 most used
```

```
GRE outside 10.50.100.2:0 inside 10.50.40.7:0, idle 0:00:12, bytes 75060, flags E  
GRE outside 10.50.100.1:0 inside 10.50.40.7:0, idle 0:00:12, bytes 65186, flags E  
ESP outside 10.7.6.6 inside 10.7.7.7, idle 0:00:04, bytes 700
```

R1# show crypto key mypubkey rsa

% Key pair was generated at: 11:36:29 PST Jul 29 2013

Key name: getvpn

Key type: RSA KEYS

Storage Device: private-config

Usage: General Purpose Key

Key is exportable.

Key Data:

```
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00A57770
FFC46D29 D6D0FE28 7259CBD1 83F5B482 DBF15346 58703712 1406DA48 7D9D086D
DBAC7CEC 96CD0949 9922CE00 3B1A0A02 FB162E85 0D30EC6C 7E429954 51075365
4789E22E 53A18AE7 7A3D97DF 81DDAFB7 3C80762D 562FF7C9 A5E62918 863197C2
8782477C 32B10548 E7609536 EA37BE76 87AE3056 B10E0784 53695702 BB020301 0001
```

R2# show crypto key mypubkey rsa

% Key pair was generated at: 11:49:34 PST Jul 29 2013

Key name: getvpn

Key type: RSA KEYS

Storage Device: private-config

Usage: General Purpose Key

Key is exportable.

Key Data:

```
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00A57770
FFC46D29 D6D0FE28 7259CBD1 83F5B482 DBF15346 58703712 1406DA48 7D9D086D
DBAC7CEC 96CD0949 9922CE00 3B1A0A02 FB162E85 0D30EC6C 7E429954 51075365
4789E22E 53A18AE7 7A3D97DF 81DDAFB7 3C80762D 562FF7C9 A5E62918 863197C2
8782477C 32B10548 E7609536 EA37BE76 87AE3056 B10E0784 53695702 BB020301 0001
```

R2# show crypto gdoi ks

Total group members registered to this box: 2

Key Server Information For Group getvpn:

Group Name : getvpn
Group Identity : 1
Group Members : 2
IPSec SA Direction : Both
ACL Configured:
 access-list VPNA
Redundancy : Configured
 Local Address : 10.50.100.2
 Local Priority : 175
 Local KS Status : Alive
 Local KS Role : Primary
 Local KS Version : 1.0.2

R1# show crypto gdoi ks

Total group members registered to this box: 2

Key Server Information For Group getvpn:

Group Name : getvpn
Group Identity : 1
Group Members : 2
IPSec SA Direction : Both
ACL Configured:
 access-list VPNA
Redundancy : Configured
 Local Address : 10.50.100.1
 Local Priority : 100
 Local KS Status : Alive
 Local KS Role : Secondary
 Local KS Version : 1.0.2

R2# show cry gdoi ks members

Group Member Information :

Number of rekeys sent for group getvpn : 4868

Group Member ID : 10.50.40.7 GM Version: 1.0.2
Group ID : 1
Group Name : getvpn
Key Server ID : 10.50.100.1

Group Member ID : 10.50.60.6 GM Version: 1.0.2
Group ID : 1
Group Name : getvpn
Key Server ID : 10.50.100.1

R1# show crypto gdoi ks members

Group Member Information :

Number of rekeys sent for group getvpn : 0 <- will be zero if there has been
No failovers in the COOP group.

Group Member ID : 10.50.40.7 GM Version: 1.0.2
Group ID : 1
Group Name : getvpn
Key Server ID : 10.50.100.1

Group Member ID : 10.50.60.6 GM Version: 1.0.2
Group ID : 1
Group Name : getvpn
Key Server ID : 10.50.100.1

GROUP INFORMATION

```
Group Name           : getvpn (Multicast)
Group Identity       : 1
Group Members        : 2
IPSec SA Direction   : Both
Redundancy           : Configured
  Local Address      : 10.50.100.1
  Local Priority      : 100
  Local KS Status     : Alive
  Local KS Role       : Secondary
  Local KS Version    : 1.0.2
Group Rekey Lifetime : 900 secs
Group Rekey
  Remaining Lifetime : 512 secs
Rekey Retransmit Period : 10 secs
Rekey Retransmit Attempts: 3
Group Retransmit
  Remaining Lifetime : 0 secs

IPSec SA Number      : 1
IPSec SA Rekey Lifetime: 600 secs
Profile Name          : profile1
Replay method         : Count Based
Replay Window Size   : 64
SA Rekey
  Remaining Lifetime : 214 secs
ACL Configured        : access-list VPNA

Group Server list     : Local
```

R2# show crypto gdoi

GROUP INFORMATION

```
Group Name           : getvpn (Multicast)
Group Identity       : 1
Group Members        : 2
IPSec SA Direction   : Both
Redundancy           : Configured
  Local Address      : 10.50.100.2
  Local Priority      : 175
  Local KS Status     : Alive
  Local KS Role       : Primary
  Local KS Version    : 1.0.2
Group Rekey Lifetime : 900 secs
Group Rekey
  Remaining Lifetime : 438 secs
Rekey Retransmit Period : 10 secs
```


Rekey Retransmit Attempts: 3

Group Retransmit

Remaining Lifetime : 0 secs

IPSec SA Number : 1

IPSec SA Rekey Lifetime: 600 secs

Profile Name : profile1

Replay method : Count Based

Replay Window Size : 64

SA Rekey

Remaining Lifetime : 139 secs

ACL Configured : access-list VPNA

Group Server list : Local

```
R1# show crypto session
```

```
Interface: Ethernet0/0
```

```
Session status: UP-IDLE
```

```
Peer: 10.50.100.2 port 848
```

```
IKEv1 SA: local 10.50.100.1/848 remote 10.50.100.2/848 Active
```

```
Interface: Ethernet0/0
```

```
Session status: UP-IDLE
```

```
Peer: 10.50.60.6 port 848
```

```
IKEv1 SA: local 10.50.100.1/848 remote 10.50.60.6/848 Active
```

```
Interface: Ethernet0/0
```

```
Session status: UP-IDLE
```

```
Peer: 10.50.40.7 port 848
```

```
IKEv1 SA: local 10.50.100.1/848 remote 10.50.40.7/848 Active
```

R2# show crypto session

Crypto session current status

Interface: (unknown)

Session status: UP-IDLE

Peer: 239.192.1.190 port 848

IKEv1 SA: local 10.50.100.2/848 remote 239.192.1.190/848 Active

Interface: Ethernet0/0.1

Session status: UP-IDLE

Peer: 10.50.100.1 port 848

IKEv1 SA: local 10.50.100.2/848 remote 10.50.100.1/848 Active

%GDOI-3-PSEUDO_TIME_LARGE

%GDOI-3-PSEUDO_TIME_TOO_OLD

R7# show crypto gdoi ipsec sa

SA created for group getvpn:

GigabitEthernet0/1:

protocol = ip

local ident = 10.7.0.0/16, port = 0

remote ident = 10.7.0.0/16, port = 0

direction: Both, replay(method/window): Time/5 sec

R7# show crypto gdoi group getvpn gm replay

Anti-replay Information For Group getvpn:

Timebased Replay:

Replay Value	:	1301905.18 secs			
Input Packets	:	0	Output Packets	:	0
Input Error Packets	:	0	Output Error Packets	:	0
Time Sync Error	:	0	Max time delta	:	0.00 secs

GROUP INFORMATION

```
Group Name           : getvpn
Group Identity       : 1
Rekeys received      : 3
IPSec SA Direction   : Both

Group Server list    : 10.50.100.1
                    : 10.50.100.2

Group member         : 10.50.40.7      vrf: None
Version              : 1.0.2
Registration status   : Registered
Registered with      : 10.50.100.1
Re-registers in      : 208 sec
Succeeded registration: 29
Attempted registration: 49
Last rekey from      : 10.50.100.2
Last rekey seq num   : 0
Multicast rekey rcvd : 19
allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP
```

Rekeys cumulative

```
Total received      : 3
After latest register : 1
Rekey Rcvd(hh:mm:ss) : 00:05:35
ACL Downloaded From KS 10.50.100.2:
  access-list permit ip 10.7.0.0 0.0.255.255 10.7.0.0 0.0.255.255
```

KEK POLICY:

```
Rekey Transport Type : Multicast
Lifetime (secs)       : 564
Encrypt Algorithm      : 3DES
Key Size               : 192
Sig Hash Algorithm     : HMAC_AUTH_SHA
Sig Key Length (bits) : 1024
```

TEK POLICY for the current KS-Policy ACEs Downloaded:

```
GigabitEthernet0/1:
IPsec SA:
  spi: 0xDB7B4CCA(3682290890)
  transform: esp-256-aes esp-sha-hmac
  sa timing:remaining key lifetime (sec): (452)
```

Anti-Replay(Time Based) : -1 sec interval

IPsec SA:

spi: 0xA220289A(2720016538)
transform: esp-256-aes esp-sha-hmac
sa timing:remaining key lifetime (sec): (530)
Anti-Replay(Time Based) : 5 sec interval

R6# show crypto gdoi

GROUP INFORMATION

Group Name : getvpn
Group Identity : 1
Rekeys received : 4
IPSec SA Direction : Both

Group Server list : 10.50.100.1
10.50.100.2

Group member : 10.50.60.6 vrf: None
Version : 1.0.2
Registration status : Registered
Registered with : 10.50.100.1
Re-registers in : 178 sec
Succeeded registration: 18
Attempted registration: 18
Last rekey from : 10.50.100.2
Last rekey seq num : 1
Multicast rekey rcvd : 27
allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP

Rekeys cumulative
Total received : 4
After latest register : 2
Rekey Rcvd(hh:mm:ss) : 00:02:31

ACL Downloaded From KS 10.50.100.2:
access-list permit ip 10.7.0.0 0.0.255.255 10.7.0.0 0.0.255.255

KEK POLICY:

Rekey Transport Type : Multicast

Lifetime (secs) : 267
Encrypt Algorithm : 3DES
Key Size : 192
Sig Hash Algorithm : HMAC_AUTH_SHA
Sig Key Length (bits) : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:

Ethernet0/1:

IPsec SA:

spi: 0xDB7B4CCA(3682290890)
transform: esp-256-aes esp-sha-hmac
sa timing:remaining key lifetime (sec): (452)
Anti-Replay(Time Based) : -1 sec interval

IPsec SA:

spi: 0xA220289A(2720016538)
transform: esp-256-aes esp-sha-hmac
sa timing:remaining key lifetime (sec): (530)
Anti-Replay(Time Based) : 5 sec interval

R7# show crypto session

Crypto session current status

Interface: GigabitEthernet0/1

Session status: UP-ACTIVE

Peer: 0.0.0.0 port 848

IKEv1 SA: local 10.50.40.7/848 remote 10.50.100.1/848 Active

IKEv1 SA: local 239.192.1.190/0 remote 10.50.100.2/848 Active

IPSEC FLOW: permit ip 10.7.0.0/255.255.0.0 10.7.0.0/255.255.0.0

Active SAs: 2, origin: crypto map

R6# show crypto session

Crypto session current status

Interface: Ethernet0/1

Session status: UP-ACTIVE

Peer: 0.0.0.0 port 848

IKEv1 SA: local 239.192.1.190/0 remote 10.50.100.1/848 Active

IKEv1 SA: local 10.50.60.6/848 remote 10.50.100.1/848 Active

IPSEC FLOW: permit ip 10.7.0.0/255.255.0.0 10.7.0.0/255.255.0.0

Active SAs: 2, origin: crypto map

```
R6# ping 10.7.7.7 so lol
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.7.7.7, timeout is 2 seconds:
```

```
Packet sent with a source address of 10.7.6.6
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms
```

R2# show crypto session detail

Code: C - IKE Configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal, T - cTCP encapsulation

X - IKE Extended Authentication, F - IKE Fragmentation

Crypto session current status

Interface: Ethernet0/0.1

Session status: UP-IDLE

Peer: 10.50.100.1 port 848 fvrf: (none) ivrf: (none)

Phase1_id: 10.50.100.1

Desc: (none)

IKEv1 SA: local 10.50.100.2/848 remote 10.50.100.1/848 Active

Capabilities:D connid:1072 lifetime:22:53:36

```
R1# show run | include authorization address
  authorization address ipv4 10
```

```
R1# show access-list 10
Standard IP access list 10
 10 permit 10.50.60.6
 20 permit 10.50.40.7
```

```
ip multicast-routing

crypto isakmp policy 10
  encr aes 192
  authentication pre-share
  group 5

crypto isakmp key cisco address 10.50.0.0
crypto isakmp keepalive 60 periodic

crypto ipsec profile profile1
  set security-association lifetime seconds 600
  set transform-set aes256

crypto gdoi group getvpn
  identity number 1
  server local
  rekey address ipv4 getvpn-rekey
  rekey lifetime seconds 900
  rekey retransmit 10 number 3
  rekey authentication mypubkey rsa getvpn
  authorization address ipv4 10
  sa ipsec 1
  profile profile1
  match address ipv4 VPNA
  replay time
  address ipv4 10.50.100.1
  redundancy
  local priority 100
  peer address ipv4 10.50.100.2

interface Tunnel6
  ip address 10.50.101.1 255.255.255.0
  ip pim sparse-dense-mode
  tunnel source Ethernet0/0
  tunnel destination 10.50.60.6
!
interface Tunnel7
  ip address 10.50.102.1 255.255.255.0
  ip pim sparse-dense-mode
  tunnel source Ethernet0/0
  tunnel destination 10.50.40.7
```

```
interface Ethernet0/0
  ip address 10.50.100.1 255.255.255.0
  ip pim sparse-mode

ip pim accept-rp auto-rp
ip pim send-rp-announce Ethernet0/0 scope 10 group-list 1
ip pim send-rp-discovery Ethernet0/0 scope 10

ip access-list extended VPNA
  permit ip 10.7.0.0 0.0.255.255 10.7.0.0 0.0.255.255
ip access-list extended getvpn-rekey
  permit ip any host 239.192.1.190
!
access-list 1 permit 239.192.1.190
access-list 10 permit 10.50.60.6
access-list 10 permit 10.50.40.7
```

```
crypto isakmp policy 10
  encr aes 192
  authentication pre-share
  group 5

crypto isakmp key cisco address 10.50.0.0

crypto isakmp keepalive 60 periodic

crypto ipsec profile profile1
  set security-association lifetime seconds 600
  set transform-set aes256
!
crypto gdoi group getvpn
  identity number 1
  server local
  rekey address ipv4 getvpn-rekey
  rekey lifetime seconds 900
  rekey retransmit 10 number 3
  rekey authentication mypubkey rsa getvpn
  authorization address ipv4 10
  sa ipsec 1
  profile profile1
  match address ipv4 VPNA
  replay time
  address ipv4 10.50.100.2
  redundancy
  local priority 175
  peer address ipv4 10.50.100.1

interface Tunnel8
  ip address 10.50.201.1 255.255.255.0
  ip pim sparse-dense-mode
  tunnel source Ethernet0/0.1
  tunnel destination 10.50.60.6
!
interface Tunnel9
  ip address 10.50.202.1 255.255.255.0
  ip pim sparse-dense-mode
  tunnel source Ethernet0/0.1
  tunnel destination 10.50.40.7

interface Ethernet0/0.1
  encapsulation dot1Q 100
```

```
ip address 10.50.100.2 255.255.255.0
ip pim sparse-mode

ip pim rp-address 10.50.100.2
ip pim send-rp-announce Ethernet0/0.1 scope 10 group-list 1
ip pim send-rp-discovery Ethernet0/0.1 scope 10
ip route 0.0.0.0 0.0.0.0 10.50.100.20
!
ip access-list extended VPNA
  permit ip 10.7.0.0 0.0.255.255 10.7.0.0 0.0.255.255
ip access-list extended getvpn-rekey
  permit ip any host 239.192.1.190
!
access-list 1 permit 239.192.1.190
access-list 10 permit 10.50.60.6
access-list 10 permit 10.50.40.7
```



```
ip multicast-routing

crypto keyring getvpn
  pre-shared-key address 10.50.100.1 key cisco
  pre-shared-key address 10.50.100.2 key cisco

crypto gdoi group getvpn
  identity number 1
  server address ipv4 10.50.100.1
  server address ipv4 10.50.100.2

crypto map getvpn 1 gdoi
  set group getvpn

interface Loopback1
  ip address 10.7.7.7 255.255.255.0
  ipv6 address 1011::/64 eui-64
!
interface Tunnel7
  ip address 10.50.102.7 255.255.255.0
  ip pim sparse-dense-mode
  tunnel source GigabitEthernet0/1
  tunnel destination 10.50.100.1
!
interface Tunnel9
  ip address 10.50.202.7 255.255.255.0
  ip pim sparse-dense-mode
  tunnel source GigabitEthernet0/1
  tunnel destination 10.50.100.2

interface GigabitEthernet0/1
  ip address 10.50.40.7 255.255.255.0
  ip pim sparse-mode
  ip flow ingress
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 cisco
  duplex auto
  speed auto
  ipv6 address 2001:DB8:40::7/64
  ipv6 enable
  crypto map getvpn

ip pim rp-address 10.50.100.1
ip mroute 10.50.100.1 255.255.255.255 Tunnel7
ip mroute 10.50.100.2 255.255.255.255 Tunnel9
```

```
ip multicast-routing

crypto keyring getvpn
  pre-shared-key address 10.50.100.1 key cisco
  pre-shared-key address 10.50.100.2 key cisco

crypto gdoi group getvpn
  identity number 1
  server address ipv4 10.50.100.1
  server address ipv4 10.50.100.2

crypto map getvpn local-address Loopback6
crypto map getvpn 1 gdoi
  set group getvpn

interface Loopback1
  ip address 10.7.6.6 255.255.255.0
  ipv6 address 2010::/64 eui-64
!
interface Loopback6
  ip address 10.50.60.6 255.255.255.0
  ip pim sparse-mode

interface Tunnel6
  ip address 10.50.101.6 255.255.255.0
  ip pim sparse-dense-mode
  tunnel source Loopback6
  tunnel destination 10.50.100.1
!
interface Tunnel8
  ip address 10.50.201.6 255.255.255.0
  ip pim sparse-dense-mode
  tunnel source Loopback6
  tunnel destination 10.50.100.2
!
interface Ethernet0/0
  ip address 10.50.80.6 255.255.255.0
  ip pim sparse-mode
!
interface Ethernet0/1
  ip address 10.50.70.6 255.255.255.0
  ip pim sparse-mode
  crypto map getvpn

ip pim rp-address 10.50.100.1
ip mroute 10.50.100.1 255.255.255.255 Tunnel6
ip mroute 10.50.100.2 255.255.255.255 Tunnel8
```

```
access-list 101 extended permit udp any any eq 848
access-group 101 in interface dmz
```

```
access-list 101 permit GRE any any
```

crypto isakmp keepalive 15 periodic

```
crypto ipsec transform-set AES_SHA esp-aes esp-sha-hmac
!
crypto ipsec profile gdoi1
 set security-association lifetime seconds 7200
 set transform-set AES_SHA
!
crypto gdoi group dgvpn1
 identity number 61440
 server local
  rekey lifetime seconds 86400
  rekey retransmit 40 number 3
  rekey authentication mypubkey rsa getkey
  rekey transport unicast
 sa ipsec 1
  profile gdoi1
  match address ipv4 172.16.4.2
```

```
crypto ipsec profile gdoil
```

```
  set security-association lifetime seconds 7200
```

```
deny pim any 224.0.0.0 0.0.0.255
deny udp any any eq ntp
deny udp any any eq dns
deny tcp any eq 443 any
deny udp any eq isakmp any eq isakmp
deny udp any any eq 848
permit ip any any
```



```
crypto gdoi group dgvpn1
identity number 61440
server local
rekey lifetime seconds 24400
```

crypto gdoi group dgvpn1

identity number 61440

server local

rekey retransmit 40 number 3

```
crypto gdoi group getvpn
identity number 1
server local
rekey lifetime seconds 900
rekey retransmit 10 number 2
rekey authentication mypubkey rsa getvpn
rekey transport unicast
sa ipsec 1
profile profile1
match address ipv4 VPNA
replay counter window-size 64
address ipv4 10.50.100.2
redundancy
local priority 175
peer address ipv4 10.50.100.1
```

```
! Key Server Configuration

! Enable multi-cast routing
ip multi-cast routing
! Enable SSM mode
ip pim ssm range 1
!
! ACL list used in SSM range command
access-list 1 permit 239.192.1.190 0.0.0.0
!
interface GigabitEthernet0/1
! Interface connecting to the WAN network
ip address 10.0.0.2 255.255.255.0
ip pim sparse-mode
ip igmp version 3
!
crypto gdoi group GDOI-GROUP1
server local
! Default rekey method is multicast
no rekey transport unicast
! Multicast group for re-keying. This is specified as a ACL
rekey address ipv4 getvpn-rekey-multicast-group
rekey retransmit 10 number 3
!
! Add these ACEs in getvpn-acl
ip access-list extended getvpn-acl
deny ip any 224.0.0.0 0.255.255.255
deny pim any host 224.0.0.13
!
ip access-list extended getvpn-rekey-multicast-group
permit ip any host 239.192.1.190

```

```
! Group Member Configuration
ip multicast-routing
! Enable SSM
ip igmp ssm-map enable
ip pim ssm range 1
! ACL used in ssm range command
access-list 1 permit 239.192.1.190 0.0.0.0
interface FastEthernet4
! Interface where crypto map is applied
ip pim sparse-mode
ip igmp version 3
! Join for each KS serving the group
ip igmp join-group 239.192.1.190 source <IP-Addr-of-KS-1>
ip igmp join-group 239.192.1.190 source <IP-Addr-of-KS-2>
```

```
multicast-routing
!
pim rp-address <KS-IP>
!
interface e0/1
  name inside
  pim
!
interface e0/0
  name outside
  pim

ACL_IN
none
ACL_OUT
access-list OUTSIDE_IN permit udp h <GM-IP> eq 848 h <KS-IP> eq 848
```

domain-name `cisco.com`

ASA2# `show ntp status`

Clock is `synchronized`, stratum 3, reference is 192.168.2.5

```
crypto key generate rsa label sslvpnkeypair modulus 1024
```

```
ASA2(config)# show cry key mypubkey rsa
```

```
Key pair was generated at: 05:15:40 UTC Aug 21 2013
```

```
Key name: sslvpnkeypair
```

```
Usage: General Purpose Key
```

```
Modulus Size (bits): 1024
```

```
Key Data:
```

```
30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 008f1541  
4434bd1e f55ee0b3 91968c50 f2686d8d 3d70d8e9 1f46b0d1 fee04f35 54843579  
0715f4e5 5403566e b4621a4b 632f7bc7 01883e4a b34e1b96 57152e34 3e2cfc60  
f8e4435d 2985c034 3e2cc276 f5de5fe7 b0cba2e4 39cf90c9 e2c6b9ee 921e628f  
bbf20662 1fe3073c 020cc34d b590115e 047ce393 2edc6e68 3d00a3f7 f9020301  
0001
```

```
crypto ca trustpoint localtrust
enrollment self
fqdn sslvpn.cisco.com
subject-name CN=sslvpn.cisco.com
keypair sslvpnkeypair
```



```
ASA2(config-ca-trustpoint)# crypto ca enroll localtrust noconfirm
```

```
ASA2# show crypto ca certificate
```

```
Certificate
```

```
Status: Available
```

```
Certificate Serial Number: 8b7ef551
```

```
Certificate Usage: General Purpose
```

```
Public Key Type: RSA (1024 bits)
```

```
Signature Algorithm: SHA1 with RSA Encryption
```

```
Issuer Name:
```

```
hostname=sslvpn.cisco.com
```

```
cn=sslvpn.cisco.com
```

```
Subject Name:
```

```
hostname=sslvpn.cisco.com
```

```
cn=sslvpn.cisco.com
```

```
Validity Date:
```

```
start date: 05:18:57 UTC Aug 21 2013
```

```
end date: 05:18:57 UTC Aug 19 2023
```

```
Associated Trustpoints: localtrust
```

ssl trust-point localtrust outside

ASA2# show vpn-sessiondb

VPN Session Summary

	Active	Cumulative	Peak Concur	Inactive
AnyConnect Client	: 0	: 1	: 1	: 0
SSL/TLS/DTLS	: 0	: 1	: 1	: 0
Clientless VPN	: 2	: 2	: 2	
Browser	: 2	: 2	: 2	

Total Active and Inactive	: 2		Total Cumulative	: 3
Device Total VPN Capacity	: 750			
Device Load	: 0%			

Tunnels Summary

	Active	Cumulative	Peak Concurrent
Clientless	: 2	: 3	: 2
SSL-Tunnel	: 0	: 1	: 1
DTLS-Tunnel	: 0	: 1	: 1

Totals	: 2	: 5	

```
ASA2# sho vpn-sessiondb webvpn
```

```
Session Type: WebVPN
```

```
Username      : user1                Index      : 17
Public IP     : 192.168.2.25
Protocol      : Clientless
License       : AnyConnect Premium
Encryption    : RC4                  Hashing    : SHA1
Bytes Tx      : 2401236              Bytes Rx   : 233208
Group Policy  : SSL                  Tunnel Group : SSL
Login Time    : 16:29:31 UTC Fri Oct 4 2013
Duration      : 0h:04m:43s
Inactivity    : 0h:00m:00s
NAC Result    : Unknown
VLAN Mapping  : N/A                  VLAN       : none
```

```
ASA2# show runn | begin group-policy SSL attributes
```

```
group-policy SSL attributes
```

```
  vpn-idle-timeout 1
```

```
  vpn-tunnel-protocol ssl-clientless
```

```
  webvpn
```

```
    homepage value http://r3.cisco.com
```

ASA2# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username	: user2	Index	: 19
Assigned IP	: 192.168.100.100	Public IP	: 192.168.2.25
Protocol	: Clientless SSL-Tunnel DTLS-Tunnel		
License	: AnyConnect Premium		
Encryption	: RC4 RC4 AES128	Hashing	: SHA1 SHA1 SHA1
Bytes Tx	: 58736	Bytes Rx	: 38825
Group Policy	: anySSL	Tunnel Group	: anySSL
Login Time	: 19:20:04 UTC Fri Oct 4 2013		
Duration	: 0h:06m:34s		
Inactivity	: 0h:00m:00s		
NAC Result	: Unknown		
VLAN Mapping	: N/A	VLAN	: none

ASA2# show access-list

access-list user2 line 1 extended permit ip user LOCAL\user2 192.168.100.0
255.255.255.0 10.50.40.0 255.255.255.0 (hitcnt=6) 0x91a6b0d4

access-list user2 line 2 extended permit ip any 10.50.40.0 255.255.255.0
(hitcnt=1) 0x4bb1a95b

ASA2# show route

S 192.168.100.100 255.255.255.255 [1/0] via 10.50.50.5, outside

ASA1/c1# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 10.50.80.6 to network 0.0.0.0

```
C    10.50.80.0 255.255.255.0 is directly connected, outside
C    192.168.2.0 255.255.255.0 is directly connected, inside
S    192.168.100.0 255.255.255.0 [1/0] via 192.168.2.5, inside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.50.80.6, outside
```



```
access-list user2 extended permit ip user LOCAL\user2 any 10.50.40.0 255.255.255.0
access-list user2 extended permit ip any 10.50.0.0 255.255.0.0
ip local pool anyssl-clients 192.168.100.100-192.168.100.200
user-identity default-domain LOCAL
crypto ca trustpoint localtrust
  enrollment self
  fqdn sslvpn.cisco.com
  subject-name CN=sslvpn.cisco.com
  keypair sslvpnkeypair
  crl configure
crypto ca certificate chain localtrust
  certificate 8b7ef551
    308201ef 30820158 a0030201 0202048b 7ef55130 0d06092a 864886f7 0d010105...
ssl trust-point localtrust outside
webvpn
  enable outside
  anyconnect image disk0:/anyconnect-win-3.0.11042-k9.pkg 1
  anyconnect enable
  tunnel-group-list enable

group-policy SSL internal
group-policy SSL attributes
  vpn-idle-timeout 1
  webvpn
    homepage value http://r3.cisco.com
  vpn-tunnel-protocol ssl-clientless
group-policy anySSL internal
group-policy anySSL attributes
  dns-server value 192.168.2.25
  vpn-tunnel-protocol ssl-client
  default-domain value cisco.com
  address-pools value anyssl-clients

username user1 password mb02jYs13AXlIAGa encrypted
username user2 password mb02jYs13AXlIAGa encrypted
username user2 attributes
  vpn-filter value user2
  service-type remote-access

tunnel-group anySSL type remote-access
tunnel-group anySSL general-attributes
  default-group-policy anySSL
tunnel-group anySSL webvpn-attributes
  group-alias AnySSL enable
tunnel-group SSL type remote-access
tunnel-group SSL general-attributes
  default-group-policy SSL
tunnel-group SSL webvpn-attributes
  group-alias SSL enable
```

```
ciscoasa# conf t
```

```
ciscoasa(config)# crypto key generate rsa label my.verisign.key modulus 1024
```

```
! Generates 1024 bit RSA key pair. "label" defines  
! the name of the Key Pair.
```

```
INFO: The name for the keys will be: my.verisign.key
```

```
Keypair generation process begin. Please wait...
```

```
ciscoasa(config)# crypto ca trustpoint my.verisign.trustpoint
```

```
ciscoasa(config-ca-trustpoint)# subject-name CN=webvpn.cisco.com,OU=TSWEB,  
O=Cisco Systems,C=US,St=North Carolina,L=Raleigh
```

```
ciscoasa(config-ca-trustpoint)# keypair my.verisign.key
```

```
ciscoasa(config-ca-trustpoint)# fqdn webvpn.cisco.com
```

```
ciscoasa(config-ca-trustpoint)# enrollment terminal
```

```
ciscoasa(config-ca-trustpoint)# exit
```

```
ciscoasa(config)# crypto ca enroll my.verisign.trustpoint
```

```
% Start certificate enrollment ..
```

```
% The subject name in the certificate will be: CN=webvpn.cisco.com,OU=TSWEB,  
O=Cisco Systems,C=US,St=North Carolina,L=Raleigh
```

```
% The fully-qualified domain name in the certificate will be:  
webvpn.cisco.com
```

```
% Include the device serial number in the subject name? [yes/no]: no
```

```
Display Certificate Request to terminal? [yes/no]: yes
```

```
! Displays the PKCS#10 enrollment request to the terminal.
```

```
! You will need to copy this from the terminal to a text
```

```
! file or web text field to submit to the 3rd party CA.
```

```
Certificate Request follows:
```

```
MIICHjCCAYcCAQAwgaAxEDA0BgNVBACTB1JhbGVpZ2gxZmZAVBgNVBAgTDk5vcnRo  
IENhem9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2l2Y28gU3lzdGVtczEO  
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNvbTEhMB8G  
CSqGSIB3DQEJAhYSY2l2Y29hc2EuY2l2Y28uY29tMIGfMA0GCSqGSIB3DQEBQUA  
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB9M4yTx5b  
Fm886s8F73WsfQPynBDFB8sejD0nBpFYzKsGf7TUMQB2m2RFAqfyNxYt3oMXSNPO  
mldZ0xJVnRip9cyQp/983pm5PFDD6/ho0nTktx0i+1cEX0luBMh7oKargwIDAQAB  
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBAwHQYDVR0RBBYwFIISY2l2  
Y29hc2EuY2l2Y28uY29tMA0GCSqGSqGSIB3DQEBBAUAA4GBABrxpY0q7SeOHZf3yEJq  
po6wG+oZpsvpYI/HemKulaRc783w4BMO5lulIEnHgrqAxrTbQn0B7JPIbkc2ykkm  
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5QlKx2Y/vrqs+Hg5SLHpbhj/Uo13yWce  
0Bzg59cYXq/vkoqZV/tBuACr
```

```
---End - This line not part of the certificate request---
```

```
ciscoasa(config)# crypto ca authenticate my.verisign.trustpoint
```

Enter the base 64 encoded CA certificate.

End with the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----

```
MIIEwDCCBCmgAwIBAgIQY7GlzcWfeIAdoGNs+XVGezANBgkqhkiG9w0BAQUFADCB
jDELMAkGA1UEBhMCVVMxPzAVBgNVBAoTD1ZlcmlTaWduLCBjb250aW50LWVudC50
EydGbz3IqVGVzdCBQdXJwb3NlcyBPbm50LiAgTm8gYXNzdXJhbmNlcy4xMjAwBgNV
BAMTKVZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIqVGVzdCBzSb290IENBMB4X
DTA1MDIwOTAwMDAwMFoXDTE1MDIwODIzNTk1OVowgcscCzAJBgNVBAYTAlVTMRcw
FQYDVQQKEw5WZXJpU2lnbiwgSW5jLjEwMC4GA1UECXMnRm9yIFRlc3QgUHVycG9z
ZXMGt25seS4gIE5vIGFzc3VyYW5jZXMuMUIwQAYDVQQLEz1UZXXJtcyBvZiB1c2Ug
YXQgHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMpMDUxLTAr
BgNVBAMTJFZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIqVGVzdCBQdCCASiW
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAuwElv6IJ/
DV8zgpvxuwaMv6fNQBHSP4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE61BBD6Zqk
d85lPl/6XxK0EdmrN7qVmmvBMGRsm0jje1op5f0nKpQvONK2qNUB6n451P4qoyqS
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1D/OCCmZO
5RmNqLLKSvYHhJ25EskFhgR2qCXX2EQJdnDXuTw0+4t1qj97ydk5iDoxjKfV6sb
tnp3TIY6S07bTb9gxJCK4pGbcf8DOPvOfGRu1wpfUUC8v+WKC20+sK6QMECAwEA
AaOCAVwgggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBABgpghkgB
hvhFAQcVMDIwMAYIKwYBBQUHAgEwJGh0dHBzOi8vd3d3LnZlcmlzaWduLmNvbS9j
cHMvdGVzdG9hLzA0BGNVHQ8BAf8EBAMCAQYwEQQYJYIZIAyb4QgEBBAQDAGEMBOG
A1UdDgQWBRRmIo6B4DFZ3Sp/q0bFNgIGcCeHwjCBsgYDVR0jBIGqMIGNoYGSPIGP
MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UECHMOVmVyaVNPZ24sIEluYy4xMDAuBgNV
BASzTj0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICB0byBhc3N1cmFuY2VzLjEwMDAw
A1UEAxMpVmVyaVNPZ24gVHJpYWwgU2VjdXJlIFNlcnZlcjBUZXN0IFJvb3QgQ0GC
ECCol67bggLEwTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/SjzRvY2l
Kqf234YROiL51ZS11loUZ2MANp2H4biw4itfsG5snDDlwSRmiH3BW/SU6EEzD9oi
Ai9TXvRiC5q0mB+nyK9fB2aBzOiaHSiIWzAJeQjuqA+Q93jNew+peuj4AhdvGN
n/KK/+1Yv61w3+7g6ukFMARVBNG=
```

-----END CERTIFICATE-----

quit

INFO: Certificate has the following attributes:

Fingerprint: 8de989db 7fcc5e3b fdde2c42 0813ef43

Do you accept this certificate? [yes/no]: **yes**

Trustpoint 'my.verisign.trustpoint' is a subordinate CA and
holds a non self-signed certificate.

Trustpoint CA certificate accepted.

% Certificate successfully imported

ciscoasa(config)#

ciscoasa(config-ca-trustpoint)# **exit**

```
ciscoasa(config)# crypto ca import my.verisign.trustpoint certificate
```

```
! Initiates prompt to paste the base64 identity
```

```
! certificate provided by the 3rd party vendor.
```

```
% The fully-qualified domain name in the certificate will be: webvpn.cisco.com
```

```
Enter the base 64 encoded certificate.
```

```
End with the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIFZjCCBE6gAwIBAgIQMs/oXuu9K14eMGSf0mYjftANBgkqhkiG9w0BAQUFADCB  
yzELMAkGA1UEBhMCVVMxZjZAVBgNVBAoTDlZlcm1TaWduLCEBbnMuMTAwLgYDVQQL  
EydGbz3IgvGVzdCBQdXJwb3NlcyBpbm5LiAgTm8gYXNzdXJhbnNlcy4xQjBAbG9u  
BAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3Bz  
L3Rlc3RjYSAoYykwNTEtMCSGA1UEAxMkVmVyaVNPZ24gVHJpYWwgU2VjdXJlIFN1  
cnZlciBUZXN0IENBMB4XDTA3MDcyNjAwMDAwMFoXDTA3MDgwOTIzNTk1OVowgbox  
CzAJBgNVBAYTAlVTMRcwFQYDVQQIEW5Ob3J0aCBDYXJvbGluYTEQMA4GA1UEBxQH  
UmFsZWlnaDEWMBQGA1UEChQONQ2lzY28gU3lzdGVtczEOMAwGA1UECmQVFNXRUIx  
OjA4BgNVBAsUMVRlcm1zIG9mIHVzZSBhdCB3d3cuZmVyaXNPZ24uY29tL2Nwcy90  
ZXN0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXNjby5jb20wgZ8wDQYJ  
KoZIHvcNAQEBBQADgY0AMIGJAoGBAL56EvorHHlsIB/VRKaRlJeJKCrQ/9KER2JQ  
9UOKUP3mVPZJtYN63ZxDwACeyNb+liidKUegJWHI0Mz3GHqcgEkKW1EcrO+6aY1R  
IaUE8/LiAZbA70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJzAlhJTxSlEgryosBMMazg  
5IcLhgSpAgMBAAGjggHXMIIB0zAJBgNVHRMEAjAAMAsGA1UdDwQEAwIFoDBDBGNV  
HR8EPDA6MDigNgA0hjJodHRwOi8vU1ZSU2VjdXJlLWVybC52ZXJpc2lnbi5jb20v  
U1ZSVHJpYWwgMDA1LmNybDBKBG9mVHSAEQzBBMD8GCMCGSAGG+EUBBxUwMTAvBggr  
BgEFBQcCARYjaHR0cHM6Ly93d3cuZmVyaXNPZ24uY29tL2Nwcy90ZXN0Y2EwHQYD  
VR0lBBYwFAYIKwYBBQUHAWEGCCsGAQUFBwMCMB8GA1UdIwQYMBaAFGYijohGmVnd  
Kn+rRsU2AgZwJ4daMHgGCCsGAQUFBwEBBGwwajAkBggrBgEFBQcwAyyyAHR0cDov  
L29jc3AudmVyaXNPZ24uY29tMEIGCCsGAQUFBzAChjZodHRwOi8vU1ZSU2VjdXJl  
LWVybC52ZXJpc2lnbi5jb20vU1ZSVHJpYWwgMDA1LWVybC52ZXJpc2lnbi5jb20v  
AQwEYjBgoV6gXDBAMFgwVhYJaw1hZ2UvZ2lmMCEwHzAHBgUrDgMCGGQUS2u5KJYG  
DLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNPZ24uY29tL3ZzbG9n  
bzEuZ2lmMA0GCSqSIsb3DQEBBQUAA4IBAQAAnym4GVThPIyL/9y1DBd8N7/yW3Ov3  
bIirHfHJyfpJ1znZQXyXdoBpZkuA6Jyu03V2CYNnDomn4xRXQTUDD8q86ZiKyMIj  
XM2VCmchSAjmmMryjpydxfk6CIdDMtMGotCavRHD9Tl2tvwgrBock/v/54o02lkB  
SmLzVV7crlyJEuhggu3Pz7qNRd8N0Un6c9sbwQ1BuM99QxzIzdAo89FSewy8MAIY  
rtab5F+oiTc5xGy8w7NARafNgFXihqnLgWtTA35/oWuy86bje1IWbeyqj8ePM9Td  
0LdAw6kUU1PNimPttMDhcF7cuevntROksOgQPBPx5FJSqMiUZGrvju50
```

```
-----END CERTIFICATE-----
```

```
quit
```

```
INFO: Certificate successfully imported
ciscoasa(config)#
ciscoasa(config)# show crypto ca certificates
```

! Display the certificates installed on the ASA.

Certificate

```
Status: Available
Certificate Serial Number: 32cfe85eebbd2b5e1e30649fd266237d
Certificate Usage: General Purpose
Public Key Type: RSA (1024 bits)
Issuer Name:
  cn=VeriSign Trial Secure Server Test CA
  ou=Terms of use at https://www.verisign.com/cps/testca ®)05
  ou=For Test Purposes Only. No assurances.
  o=VeriSign\, Inc.
  c=US
Subject Name:
  cn=webvpn.cisco.com
  ou=Terms of use at www.verisign.com/cps/testca ®)05
  ou=TSWEB
  o=Cisco Systems
  l=Raleigh
  st=North Carolina
  c=US
OCSP AIA:
  URL: http://ocsp.verisign.com
CRL Distribution Points:
  [1] http://SVRSecure-crl.verisign.com/SVRTrial2005.crl
Validity Date:
  start date: 00:00:00 UTC Jul 19 2007
  end   date: 23:59:59 UTC Aug 2 2007
Associated Trustpoints: my.verisign.trustpoint
```

CA Certificate

```
Status: Available
Certificate Serial Number: 63b1a5cdc59f78801da0636cf975467b
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Issuer Name:
  cn=VeriSign Trial Secure Server Test Root CA
  ou=For Test Purposes Only. No assurances.
```

o=VeriSign\, Inc.

c=US

Subject Name:

cn=VeriSign Trial Secure Server Test CA

ou=Terms of use at <https://www.verisign.com/cps/testca> ®)05

ou=For Test Purposes Only. No assurances.

o=VeriSign\, Inc.

c=US

Validity Date:

start date: 00:00:00 UTC Feb 9 2005

end date: 23:59:59 UTC Feb 8 2015

Associated Trustpoints: my.verisign.trustpoint

```
hostname# show run all group-policy DfltGrpPolicy
```


R7# show crypto session

Crypto session current status

Interface: Tunnel1

Session status: UP-ACTIVE

Peer: 10.50.70.6 port 500

IKEv2 SA: local 10.50.40.7/500 remote 10.50.70.6/500 Active

IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0

Active SAs: 2, origin: crypto map

R6# show crypto session

Crypto session current status

Interface: Virtual-Access1

Session status: UP-ACTIVE

Peer: 10.50.40.7 port 500

IKEv2 SA: local 10.50.70.6/500 remote 10.50.40.7/500 Active

IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0

Active SAs: 2, origin: crypto map

R6# show crypto ikev2 session detailed

IPv4 Crypto IKEv2 Session

Session-id:18, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id	Local	Remote	fvr/ivrf	Status
1	10.50.70.6/500	10.50.40.7/500	none/none	READY

Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:5, Auth sign: PSK, Auth verify: PSK

Life/Active Time: 86400/1014 sec

CE id: 1008, Session-id: 18

Status Description: Negotiation done

Local spi: D60B62C207327A3D Remote spi: 609E382CB11281D3

Local id: r6.cisco.com

Remote id: r7.cisco.com

Local req msg id: 0 Remote req msg id: 2

Local next msg id: 0 Remote next msg id: 2

Local req queued: 0 Remote req queued: 2

Local window: 5 Remote window: 5

DPD configured for 0 seconds, retry 0

NAT-T is not detected

Cisco Trust Security SGT is disabled

Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535

remote selector 0.0.0.0/0 - 255.255.255.255/65535

ESP spi in/out: 0x88B600C5/0xDE40CB3B

AH spi in/out: 0x0/0x0

CPI in/out: 0x0/0x0

Encr: AES-CBC, keysize: 128, esp_hmac: SHA96

ah_hmac: None, comp: IPCOMP_NONE, mode tunnel

```
R7# show ip route
```

```
R      172.17.60.0/24 [120/1] via 172.16.70.6, 00:00:07, Tunnel1
```

```
R6# show ip route
```

```
R      172.17.70.0/24 [120/1] via 172.16.70.7, 00:00:21, Virtual-Access1
```

```
aaa new-model
!
!
aaa authorization network list1 group radius
!
crypto ikev2 proposal 1
  encryption aes-cbc-256
  integrity sha256
  group 5
!
crypto ikev2 policy lan2lan
  match fvrfl any
  proposal 1

crypto ikev2 name-mangler identities
  fqdn all
!
crypto ikev2 profile flexvpn
  match identity remote fqdn domain cisco.com
  identity local fqdn r6.cisco.com
  authentication local pre-share
  authentication remote pre-share
  keyring aaa list1 name-mangler identities
  virtual-template 1
!
crypto ipsec profile flexvpn
  set ikev2-profile flexvpn
!
interface Loopback3
  ip address 172.16.70.6 255.255.255.0
!
interface Ethernet0/1
  ip address 10.50.70.6 255.255.255.0

interface Virtual-Template1 type tunnel
  ip unnumbered Loopback3
  tunnel source Ethernet0/1
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile flexvpn
!
radius-server host 192.168.2.18 key cisco
!
router rip
  version 2
  passive-interface Ethernet0/0
  network 172.16.0.0
  network 172.17.0.0
  no auto-summary
```

```
crypto ikev2 proposal 1
  encryption aes-cbc-256
  integrity sha256
  group 5
!
crypto ikev2 policy lan2lan
  match fvrf any
  proposal 1
!
!
crypto ikev2 keyring flexvpn
  peer r6
    identity fqdn r6.cisco.com
    pre-shared-key cisco
!
!
!
crypto ikev2 profile flexvpn
  match identity remote fqdn r6.cisco.com
  identity local fqdn r7.cisco.com
  authentication local pre-share
  authentication remote pre-share
  keyring local flexvpn
!
crypto ipsec profile flexvpn
  set ikev2-profile flexvpn

interface Tunnell
  ip address 172.16.70.7 255.255.255.0
  tunnel source GigabitEthernet0/1
  tunnel mode ipsec ipv4
  tunnel destination 10.50.70.6
  tunnel protection ipsec profile flexvpn

router rip
  version 2
  network 172.16.0.0
  network 172.17.0.0
  no auto-summary
```

show crypto ikev2 policy default

IKEv2 policy : default
Match fvrf : any
Match address local : any
Proposal : default

show crypto ikev2 proposal default

IKEv2 proposal: default
Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
Integrity : SHA512 SHA384 SHA256 SHA96 MD596
PRF : SHA512 SHA384 SHA256 SHA1 MD5
DH Group : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2


```
IKEv2:(SA ID = 1):Stopping timer to wait for auth message
IKEv2:(SA ID = 1):Checking NAT discovery
IKEv2:(SA ID = 1):NAT not found
IKEv2:(SA ID = 1):Searching policy based on peer's identity 'r7.cisco.com' of
  type 'PQDN'
IKEv2:found matching IKEv2 profile 'flexvpn'
IKEv2:Searching Policy with fvrf 0, local address 10.50.70.6
IKEv2:Found Policy 'lan2lan'
IKEv2:(SA ID = 1):Verify peer's policy
IKEv2:(SA ID = 1):Peer's policy verified
IKEv2:(SA ID = 1):Get peer's authentication method
IKEv2:(SA ID = 1):Peer's authentication method is 'PSK'
IKEv2:(SA ID = 1):Get peer's preshared key for r7.cisco.com
IKEv2:(SA ID = 1):[IKEv2 -> AAA] Password request sent
RADIUS/ENCODE(00000045):Orig. component type = VPN IPSEC
RADIUS(00000045): Config NAS IP: 0.0.0.0
RADIUS(00000045): Config NAS IPv6: ::
RADIUS/ENCODE(00000045): acct_session_id: 58
RADIUS(00000045): sending
RADIUS/ENCODE: Best Local IP-Address 10.50.80.6 for Radius-Server 192.168.2.18
RADIUS(00000045): Send Access-Request to 192.168.2.18:1645 id 1645/2, len 76
RADIUS:  authenticator 7E 27 B9 E8 5E 69 3C 5F - 40 16 FD 66 AF DE ED 10
RADIUS:  User-Name           [1]  14  "r7.cisco.com"
RADIUS:  User-Password      [2]  18  *
R6#
RADIUS:  Calling-Station-Id [31] 12  "10.50.40.7"
RADIUS:  Service-Type       [6]   6  Outbound           [5]
RADIUS:  NAS-IP-Address     [4]   6  10.50.80.6
RADIUS(00000045): Sending a IPv4 Radius Packet
RADIUS(00000045): Started 5 sec timeout
RADIUS: Received from id 1645/2 192.168.2.18:1645, Access-Accept, len 184
RADIUS:  authenticator C4 1C B7 E9 52 87 19 3E - 3C 66 05 77 D7 1D 25 C3
RADIUS:  User-Name           [1]  14  "r7.cisco.com"
RADIUS:  Class               [25] 22
RADIUS:  43 41 43 53 3A 61 63 73 2F 31 36 34 31 35 34 37 [CACS:acs/1641547]
RADIUS:  31 35 2F 32           [ 15/2]
RADIUS:  Tunnel-Type         [64]  6  01:ESP           [9]
RADIUS:  Tunnel-Medium-Type [65]  6  01:IPv4          [1]
RADIUS:  Vendor, Cisco      [26] 35
RADIUS:  Cisco AVpair       [1]  29  "ipsec:tunnel-password=cisco"
RADIUS:  Vendor, Cisco      [26] 40
RADIUS:  Cisco AVpair       [1]  34  "ipsec:ikev2-password-local=cisco"
RADIUS:  Vendor, Cisco      [26] 41
RADIUS:  Cisco AVpair       [1]  35  "ipsec:ikev2-password-remote=cisco"
RADIUS(00000045): Received from id 1645/2
```



```
IKEv2:(SA ID = 1):[AAA -> IKEv2] Received password response
IKEv2:unsupported attr type 445
IKEv2:unsupported attr type 437
IKEv2:unsupported attr type 438
IKEv2:unsupported attr type 473
IKEv2:unsupported attr type 474
IKEv2:(SA ID = 1):Verify peer's authentication data
IKEv2:(SA ID = 1):Use preshared key for id r7.cisco.com, key len 5
IKEv2:[IKEv2 -> Crypto Engine] Generate IKEv2 authentication data
IKEv2:[Crypto Engine -> IKEv2] IKEv2 authentication data generation PASSED
IKEv2:(SA ID = 1):Verification of peer's authentication data PASSED
```

```
R4# crypto ikev2 client flexvpn connect
```

```
R4# show crypto ikev2 client flex
```

```
Profile : flex
```

```
Current state:ACTIVE
```

```
Peer : 10.50.100.2
```

```
Source : Ethernet0/1
```

```
ivrf : IP DEFAULT
```

```
fvrfr : IP DEFAULT
```

```
Backup group: Default
```

```
Tunnel interface : Tunnel0
```

```
Assigned ip address: 172.17.100.55 <- should be between .50 and .60
```

R4# show crypto ikev2 session detail

IPv4 Crypto IKEv2 Session

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id	Local	Remote	fvr/ivrf	Status
1	10.50.30.4/500	10.50.100.2/500	none/none	READY

Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK

Life/Active Time: 86400/277 sec

CE id: 1032, Session-id: 2

Status Description: Negotiation done

Local spi: 0696C6F582787B23

Remote spi: 49C2BF63CF74F456

Local id: R4.cisco.com

Remote id: 10.50.100.2

Local req msg id: 2

Remote req msg id: 0

Local next msg id: 2

Remote next msg id: 0

Local req queued: 2

Remote req queued: 0

Local window: 5

Remote window: 5

DPD configured for 0 seconds, retry 0

NAT-T is not detected

Cisco Trust Security SGT is disabled

Pushed IP address: 172.17.100.55

DNS Primary: 192.168.2.25

Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535

remote selector 0.0.0.0/0 - 255.255.255.255/65535

ESP spi in/out: 0xEEF6B847/0x81642A80

AH spi in/out: 0x0/0x0

CPI in/out: 0x0/0x0

Encr: 3DES, esp_hmac: MD596

ah_hmac: None, comp: IPCOMP_NONE, mode tunnel

```
aaa authorization network list1 local
aaa authorization group psk list list1 flex
```

```
R4# show crypto ikev2 authorization policy
```

```
IKEv2 Authorization Policy : flex
```

```
route set interface
```

```
route set acl: routes <- this is a pointer to a pre-defined ACL that will form
the basis of a static route created on R2
```

```
route accept any tag : 1 distance : 1
```

R2# show ip route

```
S      172.17.100.55/32 is directly connected, Virtual-Access1
      172.18.0.0/24 is subnetted, 1 subnets
S      172.18.34.0 is directly connected, Virtual-Access1
```

R2# ping 172.18.34.4

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.18.34.4, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms

R2# show crypto ipsec sa

.....

interface: Virtual-Access1

 Crypto map tag: Virtual-Access1-head-0, local addr 10.50.100.2

protected vrf: (none)

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

current_peer 10.50.30.4 port 500

 PERMIT, flags={origin_is_acl,}

 #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5

 #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5

 #pkts compressed: 0, #pkts decompressed: 0

 #pkts not compressed: 0, #pkts compr. failed: 0

 #pkts not decompressed: 0, #pkts decompress failed: 0

R4# show ip route

```
S      172.17.100.2/32 is directly connected, Tunnel0
C      172.17.100.55/32 is directly connected, Tunnel0
```

```
aaa authorization network list1 local

crypto ikev2 authorization policy flex
  route set interface
  route set access-list routes

crypto ikev2 keyring key
  peer flexserver
    address 0.0.0.0 0.0.0.0
    pre-shared-key cisco
  !
  !
  !
crypto ikev2 profile prof
  match identity remote address 10.50.100.2 255.255.255.255
  identity local fqdn R4.cisco.com
  authentication local pre-share
  authentication remote pre-share
  keyring local key
  aaa authorization group psk list list1 flex
  config-exchange set send
  config-exchange set accept
  config-exchange request
  !
crypto ikev2 client flexvpn flex
  peer 1 10.50.100.2
  connect manual
  client connect Tunnel0

crypto ipsec profile ipsecprof
  set transform-set 3des
  set ikev2-profile prof
  !
interface Loopback2
  ip address 172.18.34.4 255.255.255.0

interface Tunnel0
  ip address negotiated
  tunnel source Ethernet0/1
  tunnel mode ipsec ipv4
  tunnel destination dynamic
  tunnel protection ipsec profile ipsecprof

ip access-list standard routes
  permit 172.18.34.0 0.0.0.255
```

```
aaa authorization network local-list local
!
aaa attribute list ikev2ra
  attribute type ipsec-backup-gateway "R1.cisco.com"
  attribute type interface-config "ip mtu 1100"
!
!
!
crypto ikev2 name-mangler group-name
  fqdn domain
!
!
crypto ikev2 authorization policy cisco.com
  pool flex
  dns 192.168.2.25
  aaa attribute list ikev2ra
  route set interface
  route accept any
!
!
crypto ikev2 keyring key
  peer flexclient
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco
!
!
crypto ikev2 profile prof
  match identity remote fqdn domain cisco.com
  authentication local pre-share
  authentication remote pre-share
  config-exchange set send
  config-exchange set accept
  config-exchange request
  keyring local key
  aaa authorization group psk list local-list name-mangler group-name
  virtual-template 1
!

crypto ipsec profile ipsecprof
  set transform-set 3des
  set ikev2-profile prof
!

interface Virtual-Templatel type tunnel
  ip unnumbered Loopback0
  tunnel source Ethernet0/0
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile ipsecprof
!
ip local pool flex 172.17.100.50 172.17.100.60
```



```
R4# crypto ikev2 client flexvpn connect
R4#
```



```
IKEv2: % Getting preshared key from profile keyring key
IKEv2: % Matched peer block 'flexserver'
IKEv2: Searching Policy with fvrf 0, local address 10.50.30.4
IKEv2: Using the Default Policy for Proposal
IKEv2: Found Policy 'default'
IKEv2: (SA ID = 1): [IKEv2 -> Crypto Engine] Computing DH public key, DH Group 5
IKEv2: (SA ID = 1): [Crypto Engine -> IKEv2] DH key Computation PASSED
IKEv2: (SA ID = 1): Request queued for computation of DH key
IKEv2: IKEv2 initiator - no config data to send in IKE_SA_INIT exch
IKEv2: (SA ID = 1): Generating IKE_SA_INIT message
IKEv2: (SA ID = 1): IKE Proposal: 1, SPI size: 0 (initial negotiation),
Num. transforms: 15
    AES-CBC  AES-CBC  AES-CBC  SHA512  SHA384  SHA256  SHA1  MD5  SHA512
    SHA384  SHA256
    SHA96  MD596  DH_GROUP_1536_MODP/Group 5  DH_GROUP_1024_MODP/Group 2

IKEv2: (SA ID = 1): Sending Packet [To 10.50.100.2:500/From 10.50.30.4:500/VRF
i0:f0]
Initiator SPI : 5863E01AB3750C92 - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
  SA KE N VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_
  IP)

IKEv2: (SA ID = 1): Insert SA
```



```
IKEv2:(SA ID = 1):Received Packet [From 10.50.100.2:500/To 10.50.30.4:500/VRF
10:f0]
Initiator SPI : 5863E01AB3750C92 - Responder SPI : A5EAB51958821403 Message id: 0
IKEv2 IKE_SA_INIT Exchange RESPONSE
Payload contents:
SA KE N VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_
IP) CERTREQ NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED)
```

```
IKEv2:(SA ID = 1):Processing IKE_SA_INIT message
IKEv2:(SA ID = 1):Verify SA init message
IKEv2:(SA ID = 1):Processing IKE_SA_INIT message
IKEv2:(SA ID = 1):Checking NAT discovery
IKEv2:(SA ID = 1):NAT not found
IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Computing DH secret key, DH Group 5
IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] DH key Computation PASSED
IKEv2:(SA ID = 1):Request queued for computation of DH secret
IKEv2:(SA ID = 1):[IKEv2 -> Crypto Engine] Calculate SKEYSEED and create rekeyed
IKEv2 SA
IKEv2:(SA ID = 1):[Crypto Engine -> IKEv2] SKEYSEED calculation and creation of
rekeyed IKEv2 SA PASSED
IKEv2:(SA ID = 1):Completed SA init exchange
```



```
IKEv2:Config data to send:
Config-type: Config-request
Attrib type: ipv4-addr, length: 0
Attrib type: ipv4-netmask, length: 0
Attrib type: ipv4-dns, length: 0
Attrib type: ipv4-dns, length: 0
Attrib type: ipv4-nbns, length: 0
Attrib type: ipv4-nbns, length: 0
Attrib type: app-version, length: 259, data: Cisco IOS Software, Linux Software
(I86BI_LINUX-ADVENTERPRISEK9-M), Version 15.2(2)T2.3, DEVELOPMENT TEST SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 08-Nov-12 06:59 by prod_rel_team
Attrib type: ipv4-subnet, length: 0
Attrib type: split-dns, length: 0
Attrib type: banner, length: 0
Attrib type: config-url, length: 0
Attrib type: config-ver, length: 0
Attrib type: backup-gateway, length: 0
Attrib type: def-domain, length: 0
IKEv2:(SA ID = 1):Have config mode data to send

IKEv2:(SA ID = 1):Generate my authentication data
IKEv2:(SA ID = 1):Use preshared key for id R4.cisco.com, key len 5
IKEv2:[IKEv2 -> Crypto Engine] Generate IKEv2 authentication data
IKEv2:[Crypto Engine -> IKEv2] IKEv2 authentication data generation PASSED
IKEv2:(SA ID = 1):Get my authentication method
IKEv2:(SA ID = 1):My authentication method is 'PSK'
IKEv2:(SA ID = 1):Generating IKE_AUTH message
IKEv2:(SA ID = 1):Constructing IDi payload: 'R4.cisco.com' of type 'FQDN'
```

```

IKEv2:(SA ID = 1):ESP Proposal: 1, SPI size: 4 (IPSec negotiation),
Num. transforms: 2
    3DES    Don't use ESN
IKEv2:(SA ID = 1):Building packet for encryption.
Payload contents:
    VID IDi AUTH CFG SA TSi TSr NOTIFY(INITIAL_CONTACT) NOTIFY(SET_WINDOW_SIZE)
    NOTIFY(ESP_TFC_NO_SUPPORT) NOTIFY(NON_FIRST_FRAGS)

IKEv2:(SA ID = 1):Sending Packet [To 10.50.100.2:500/From 10.50.30.4:500/VRF
    10:f0]
Initiator SPI : 5863E01AB3750C92 - Responder SPI : A5EAB51958821403 Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
Payload contents:
    ENCR

```



```

IKEv2:(SA ID = 1):Received Packet [From 10.50.100.2:500/To 10.50.30.4:500/VRF
    10:f0]
Initiator SPI : 5863E01AB3750C92 - Responder SPI : A5EAB51958821403 Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
Payload contents:
    VID IDr AUTH CFG SA TSi TSr NOTIFY(SET_WINDOW_SIZE) NOTIFY(ESP_TFC_NO_SUPPORT)
    NOTIFY(NON_FIRST_FRAGS)

IKEv2:(SA ID = 1):Process auth response notify
IKEv2:(SA ID = 1):Searching policy based on peer's identity '10.50.100.2' of type
    'IPv4 address'
IKEv2:Searching Policy with fvrf 0, local address 10.50.30.4
IKEv2:Using the Default Policy for Proposal
IKEv2:Found Policy 'default'
IKEv2:(SA ID = 1):Verify peer's policy
IKEv2:(SA ID = 1):Peer's policy verified
IKEv2:(SA ID = 1):Get peer's authentication method
IKEv2:(SA ID = 1):Peer's authentication method is 'PSK'
IKEv2:(SA ID = 1):Get peer's preshared key for 10.50.100.2
IKEv2:(SA ID = 1):Verify peer's authentication data

```

```

IKEv2:(SA ID = 1):Use preshared key for id 10.50.100.2, key len 5
IKEv2:[IKEv2 -> Crypto Engine] Generate IKEv2 authentication data
IKEv2:[Crypto Engine -> IKEv2] IKEv2 authentication data generation PASSED
IKEv2:(SA ID = 1):Verification of peer's authentication data PASSED
IKEv2:Using mlist list1 and username flex for group author request
IKEv2:(SA ID = 1):[IKEv2 -> AAA] Authorisation request sent
IKEv2:(SA ID = 1):[AAA -> IKEv2] Received AAA authorisation response

IKEv2:(SA ID = 1):Received valid config mode data
IKEv2:Config data received:
Config-type: Config-reply
Attrib type: ipv4-addr, length: 4, data: 172.17.100.55
Attrib type: ipv4-subnet, length: 8, data: 172.17.100.2 255.255.255.255
Attrib type: ipv4-dns, length: 4, data: 192.168.2.25
Attrib type: app-version, length: 259, data: Cisco IOS Software, Linux Software
(I86BI_LINUX-ADVENTERPRISEK9-M), Version 15.2(2)T2.3, DEVELOPMENT TEST SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 08-Nov-12 06:59 by prod_rel_team
Attrib type: backup-gateway, length: 12, data: R1.cisco.com
IKEv2:(SA ID = 1):Set received config mode data

```

```

IKEv2:(SA ID = 1):Processing IKE_AUTH message
IKEv2:KMI/verify policy/sending to IPSec:
    prot: 3 txfm: 3 hmac 0 flags 8177 keysize 0 IDB 0x0
IKEv2:(SA ID = 1):IKEV2 SA created; inserting SA into database. SA lifetime timer
(86400 sec) started
IKEv2:IKEv2 MIB tunnel started, tunnel index 1
IKEv2:(SA ID = 1):Load IPSEC key material
IKEv2:(SA ID = 1):Checking for duplicate IKEv2 SA
IKEv2:(SA ID = 1):No duplicate IKEv2 SA found

```



```
Config-type: Config-set
Attrib type: ipv4-subnet, length: 8, data: 172.17.100.55 255.255.255.255
Attrib type: ipv4-subnet, length: 8, data: 172.18.34.0 255.255.255.0
Attrib type: app-version, length: 259, data: Cisco IOS Software, Linux Software
(I86BI_LINUX-ADVENTERPRISEK9-M), Version 15.2(2)T2.3, DEVELOPMENT TEST SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 08-Nov-12 06:59 by prod_rel_team
```

```
IKEv2:(SA ID = 1):Sending info exch config
IKEv2:(SA ID = 1):Building packet for encryption.
Payload contents:
CFG
IKEv2:(SA ID = 1):Checking if request will fit in peer window
```

```
IKEv2:(SA ID = 1):Sending Packet [To 10.50.100.2:500/From 10.50.30.4:500/VRF
i0:f0]
Initiator SPI : 5863E01AB3750C92 - Responder SPI : A5EAB51958821403 Message id: 2
IKEv2 INFORMATIONAL Exchange REQUEST
Payload contents:
ENCR
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
%FLEXVPN-6-FLEXVPN_CONNECTION_UP: FlexVPN(flex) Client_public_addr = 10.50.30.4
Server_public_addr = 10.50.100.2 Assigned_Tunnel_addr = 172.17.100.55
R4#
```



```
*Oct 28 21:15:58.500: IKEv2:(SA ID = 1):Received Packet [From 10.50.100.2:500/To
10.50.30.4:500/VRF i0:f0]
Initiator SPI : E9514C2B78FD144B - Responder SPI : FEB010A8A5E13415 Message id: 2
IKEv2 INFORMATIONAL Exchange RESPONSE
Payload contents:
CFG
```

```
IKEv2:(SA ID = 1):Processing ACK to informational exchange
IKEv2:Config data received:
Config-type: Config-ack
Attrib type: ipv4-subnet, length: 0
IKEv2:(SA ID = 1):Set received config mode data
```

```
R7# traceroute 10.50.70.6
```

```
Type escape sequence to abort.
```

```
Tracing the route to r6.cisco.com (10.50.70.6)
```

```
VRF info: (vrf in name/id, vrf out name/id)
```

```
 1 10.50.40.20 4 msec * 0 msec
```

```
 2 10.50.50.5 0 msec 4 msec 8 msec
```

```
 3 r6.cisco.com (10.50.70.6) 0 msec * 0 msec
```

```
neighbor ip-address ttl-security hops 2
```



```
R7# traceroute 10.50.70.6
```

```
Type escape sequence to abort.
```

```
Tracing the route to r6.cisco.com (10.50.70.6)
```

```
VRF info: (vrf in name/id, vrf out name/id)
```

```
 1 10.50.40.20 4 msec * 0 msec
```

```
 2 10.50.50.5 0 msec 4 msec 8 msec
```

```
 3 r6.cisco.com (10.50.70.6) 0 msec * 0 msec
```

```
ASA2# show service-policy
```

```
. . .
```

```
Class-map: set-ttl
```

```
  Set connection policy:          drop 0
```

```
  Set connection decrement-ttl
```

```
R7# show ip bgp neighbors 10.50.70.6 | include state
  BGP state = Established, up for 1d21h
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
```

```
R7# show ip bgp
```

```
BGP table version is 15, local router ID is 172.18.107.7
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, x best-external,
               f RT-Filter, a additional-path
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 172.18.106.0/24	10.50.70.6	0		0	106 ?
*> 172.18.107.0/24	0.0.0.0	0		32768	?

```
R6# show ip bgp
```

```
BGP table version is 3, local router ID is 172.18.106.6
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, x best-external,
               f RT-Filter, a additional-path
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 172.18.106.0/24	0.0.0.0	0		32768	?
*> 172.18.107.0/24	10.50.40.7	0		0	107 ?

```
neighbor 10.50.40.7 ebgp-multihop 2  
neighbor 10.50.70.6 ebgp-multihop 2
```

```
router bgp 106
  bgp log-neighbor-changes
  redistribute connected route-map bgp
  neighbor 10.50.40.7 remote-as 107
  neighbor 10.50.40.7 password cisco
  neighbor 10.50.40.7 ttl-security hops 2
```

```
router bgp 107
  bgp log-neighbor-changes
  redistribute connected route-map bgp
  neighbor 10.50.70.6 remote-as 106
  neighbor 10.50.70.6 password cisco
  neighbor 10.50.70.6 ttl-security hops 2
```

```
class-map set-ttl
  Match any
  policy-map global_policy
    class set-ttl
      set connection decrement-ttl
```

R1# show control-plane host open-ports

Active internet connections (servers and established)

Prot	Local Address	Foreign Address	Service	State
tcp	*:22	*:0	SSH-Server	LISTEN
tcp	*:23	*:	Telnet	LISTEN
tcp	*:8080	*:0	HTTP CORE	LISTEN
tcp	*:8080	*:0	HTTP CORE	LISTEN
udp	*:123	*:0	NTP	LISTEN
udp	*:4500	*:0	ISAKMP	LISTEN
udp	*:500	*:0	ISAKMP	LISTEN

R1# show udp

Proto	Remote	Port	Local	Port	In	Out	Stat	TTY	OutputIF
17	--listen--		10.50.100.1	123	0	0	1001001		0
17(v6)	--listen--		FE80::1	123	0	0	1020001		0
17	--listen--		10.50.100.1	848	0	0	1001011		0
17(v6)	--listen--		FE80::1	848	0	0	1020011		0
17	--listen--		10.50.100.1	4500	0	0	1001011		0
17(v6)	--listen--		FE80::1	4500	0	0	1020011		0
17	--listen--		10.50.100.1	500	0	0	1001011		0
17(v6)	--listen--		FE80::1	500	0	0	1020011		0
17	--listen--		10.50.100.1	4500	0	0	1001011		0
17(v6)	--listen--		FE80::1	4500	0	0	1020011		0

```
R1# show class-map type port-filter
Class Map type port-filter match-all pf-class
Match not port udp 848
Match closed-ports

R1# show policy-map type port-filter
Policy Map type port-filter pf-policy
Class pf-class
drop

R1# show run | section control-plane host
control-plane host
service-policy type port-filter input pf-policy
```

```
class-map type port-filter match-all pf-class
  match not port udp 848
  match closed-ports
!
!
policy-map type port-filter pf-policy
  class pf-class
    drop

control-plane host
  service-policy type port-filter input pf-policy
```

class-map type

port-filter Class map for port filter

 queue-threshold Class map for queue threshold

policy-map type

port-filter Control-plane tcp/udp port filtering

 queue-threshold Control-plane protocol queue limiting

R4# show access-list RFC4890

IPv6 access list RFC4890

```
permit icmp any any echo-reply sequence 10
permit icmp any any echo-request sequence 20
permit icmp any any destination-unreachable sequence 30
permit icmp any any port-unreachable sequence 40
permit icmp any any packet-too-big sequence 50
permit icmp any any time-exceeded sequence 60
permit icmp any any parameter-problem sequence 70
permit icmp any any mld-query sequence 80
permit icmp any any mld-reduction sequence 90
permit icmp any any mld-report sequence 100
permit icmp any any nd-na (23776 matches) sequence 110
permit icmp any any nd-ns (12962 matches) sequence 120
permit icmp any any router-solicitation sequence 130
permit icmp any any router-advertisement sequence 140
```

R4# show policy-map control-plane cef-exception

Control Plane Cef-exception

Service-policy input: COPPRV6

Class-map: ICMPv6 (match-all)

25142 packets, 2038444 bytes

5 minute offered rate 0 bps, drop rate 0 bps

Match: access-group name RFC4890

police:

cir 8000 bps, bc 1500 bytes

conformed 25142 packets, 2038444 bytes; actions:

transmit

exceeded 0 packets, 0 bytes; actions:

drop

conformed 0000 bps, exceeded 0000 bps

Class-map: class-default (match-any)

264174 packets, 29538421 bytes

5 minute offered rate 0 bps, drop rate 0 bps

Match: any

police:

cir 10000 bps, bc 1500 bytes

conformed 264163 packets, 29536519 bytes; actions:

transmit

exceeded 11 packets, 1902 bytes; actions:

transmit

conformed 0000 bps, exceeded 0000 bps

```
class-map match-all ICMPv6
  match access-group name RFC4890

policy-map COPPRv6
  class ICMPv6
    police 8000 conform-action transmit exceed-action drop
  class class-default
    police 10000 conform-action transmit exceed-action transmit

ipv6 access-list RFC4890
  permit icmp any any echo-reply
  permit icmp any any echo-request
  permit icmp any any destination-unreachable
  permit icmp any any port-unreachable
  permit icmp any any packet-too-big
  permit icmp any any time-exceeded
  permit icmp any any parameter-problem
  permit icmp any any mld-query
  permit icmp any any mld-reduction
  permit icmp any any mld-report
  permit icmp any any nd-na
  permit icmp any any nd-ns
  permit icmp any any router-solicitation
  permit icmp any any router-advertisement

control-plane cef-exception
  service-policy input COPPRv6
```

```
R3# ping 10.50.40.7 so lo10
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.50.40.7, timeout is 2 seconds:
```

```
Packet sent with a source address of 10.50.50.4
```


C 10.50.50.0 255.255.255.0 is directly connected, outside

```
ASA2# show ip verify statistics
interface outside: 0 unicast rpf drops
interface dmz: 9 unicast rpf drops
```

```
ip verify reverse-path int dmz
ip verify reverse-path int outside
```

```
interface FastEthernet 0/0
ip verify unicast source reachable-via {rx | any} [allow-default]
[allow-self-ping] [list]
```

IPS# show tls fingerprint

MD5: D9:DF:83:E4:00:19:68:59:04:DA:B4:CB:6D:77:73:CA

SHA1: 35:AB:35:7C:BA:58:21:24:1D:BC:1F:3A:8A:CB:2E:06:B0:BB:3F:EE

(WLC) >show wps cids-sensor detail 1

```
IP Address..... 192.168.2.100
Port..... 443
Query Interval..... 60
Username..... wlc
Cert Fingerprint..... SHA1:
35:AB:35:7C:BA:58:21:24:1D:BC:1F:3A:8A:CB:2E:06:B0:BB:3F:EE
Query State..... Enabled
Last Query Result..... Success
Number of Queries Sent..... 1
```

```
config wps cids-sensor add 1 192.168.2.100 wlc 123cisco123
config wps cids-sensor fingerprint 1 sha1 fingerprint -> taken from IPS and will
    vary
config wps cids-sensor enable 1
```

```
access-list 101 permit tcp any any eq 443
access-group 101 in interface outside
```



```
ASA1/c2# show service-policy flow tcp host 0.0.0.0 host 10.50.100.1 eq 80
```

```
Global policy:
```

```
Service-policy: global_policy
```

```
Class-map: protectCAServer
```

```
Match: access-list CAServer
```

```
Access rule: permit tcp any host 10.50.100.1 eq www
```

```
Action:
```

```
Input flow: set connection embryonic-conn-max 100 per-client-max 5
```

```
ASA1/c2# show service-policy flow tcp host 0.0.0.0 host 10.50.100.1 eq 443
```

```
Global policy:
```

```
Service-policy: global_policy
```

```
Class-map: protectCAServer
```

```
Match: access-list CAServer
```

```
Access rule: permit tcp any host 10.50.100.1 eq https
```

```
Action:
```

```
Input flow: set connection embryonic-conn-max 100 per-client-max 5
```

```
access-list CAServer extended permit tcp any host 10.50.100.1 eq www
access-list CAServer extended permit tcp any host 10.50.100.1 eq https
<...>
class-map protectCAServer
  match access-list CAServer
<...>
policy-map global_policy
  <...>
  class protectCAServer
    set connection embryonic-conn-max 100 per-client-max 5
!
service-policy global_policy global
```

```
! Old Configuration
static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 tcp 10
    20 norandomseq nailed
! Migrated Configuration

access-list acl-conn-param-tcp-01 extended permit tcp host 192.168.100.10 any

class-map class-conn-param-tcp-01
match access-list acl-conn-param-tcp-01

policy-map policy-conn-param-inside
class class-conn-param-tcp-01
set connection per-client-max 10 per-client-embryonic-max 20
random-sequence-number disable
set connection advanced-options tcp-state-bypass

service-policy policy-conn-param-inside interface inside
```

Host: 10.50.100.1

Server: cisco-IOS

Content-Type: application/x-x509-ca-cert

```
R1# show ip http server status
```

```
HTTP server status: Enabled
```

```
HTTP server port: 8080
```

```
R1# show ip port-map http detail
```

```
IP port-map entry for application 'http':
```

tcp 80	Hypertext Transfer Protocol	system defined
tcp 8080		user defined

```
ASA1/c2# show access-list
```

```
access-list 101 line 15 extended permit tcp any host 10.50.100.1 eq 8080
```

```
ASA1/c2# show service-policy flow tcp host 0.0.0.0 host 10.50.100.1 eq 8080
```

```
Global policy:
```

```
Service-policy: global_policy
```

```
Class-map: protectCAServer
```

```
Match: access-list CAServer
```

```
Access rule: permit tcp any host 10.50.100.1 eq 8080
```

```
Action:
```

```
Input flow: set connection embryonic-conn-max 100 per-client-max 5
```

```
Class-map: class-default
```

```
Match: any
```

```
Action:
```

```
Output flow:
```



```
R6(config)# crypto pki auth ciscoca
```

```
Certificate has the following attributes:
```

```
    Fingerprint MD5: 1F5A02E4 C2C8230A 56FC15BB CBDFBEF6
```

```
    Fingerprint SHA1: 99D5D0AA 928B4DD8 7D9E6D98 B3831F1D 796C6A71
```

```
% Do you accept this certificate? [yes/no]: no
```

```
R1# show policy-map int e0/0
Ethernet0/0
```

```
Service-policy input: scep
```

```
Class-map: scep (match-all)
  8 packets, 480 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: protocol http mime "application/x-x509-ca-cert"
  Match: protocol http server "cisco-IOS"
  Match: protocol http host "10.50.100.1"
  police:
    cir 10000 bps, bc 1500 bytes
    conformed 4 packets, 240 bytes; actions:
      transmit
    exceeded 0 packets, 0 bytes; actions:
      drop
    conformed 0000 bps, exceeded 0000 bps

Class-map: class-default (match-any)
  487 packets, 106808 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any
```

```
Service-policy output: scep
```

```
Class-map: scep (match-all)
  21 packets, 7960 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: protocol http mime "application/x-x509-ca-cert"
  Match: protocol http server "cisco-IOS"
  Match: protocol http host "10.50.100.1"
  police:
    cir 10000 bps, bc 1500 bytes
    conformed 6 packets, 2042 bytes; actions:
      transmit
    exceeded 0 packets, 0 bytes; actions:
      drop
    conformed 0000 bps, exceeded 0000 bps

Class-map: class-default (match-any)
  520675 packets, 50074219 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any
```

R1# show flow monitor name SCEP cache format record

Cache type:		Normal
Cache size:		4096
Current entries:		7
High Watermark:		7
Flows added:		93
Flows aged:		86
- Active timeout	(1800 secs)	0
- Inactive timeout	(60 secs)	86
- Event aged		0
- Watermark aged		0
- Emergency aged		0

IPV4 SOURCE ADDRESS:	10.50.80.6
IPV4 DESTINATION ADDRESS:	10.50.100.1
TRNS SOURCE PORT:	19689
TRNS DESTINATION PORT:	8080
IP PROTOCOL:	6
APPLICATION NAME:	port http
interface input:	Et0/0
interface output:	Null
counter flows:	1
counter bytes long:	273
counter packets long:	3
ip fragmentation flags:	0x00

```
flow record SCEP
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  match application name
  collect ipv4 fragmentation flags
  collect interface input
  collect interface output
  collect counter bytes long
  collect counter packets long
!
!
flow monitor SCEP
  cache timeout inactive 60
  record SCEP

ip port-map http port tcp 8080

ip http server
ip http port 8080

class-map match-all scep
  match protocol http mime "application/x-x509-ca-cert"
  match protocol http server "cisco-IOS"
  match protocol http host "10.50.100.1"

policy-map scep
  class scep
    police 10000 conform-action transmit exceed-action drop
interface Ethernet0/0
  service-policy output scep
  service-policy input scep
  ip flow monitor SCEP input
```

```
crypto key gen rsa
crypto pki trustpoint ciscoca
  enrollment url http://10.50.100.1:8080
```

```
access-list 101 extended permit tcp any host 10.50.100.1 eq 8080
access-list CAServer extended permit tcp any host 10.50.100.1 eq 8080
```

```
flow exporter export-to-scrutinizer*
destination 192.168.2.25
source Ethernet0/0
transport udp 2055
template data timeout 60

flow monitor SCEP
record SCEP
exporter export-to-scrutinizer*
cache timeout active 60
```

```
! Netflow Version 5
```

```
interface FastEthernet 0/1
  ip flow [ingress|egress]
  exit
ip flow-export destination 192.168.9.101 9996
ip flow-export source FastEthernet 0/1
ip flow-export version 5
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
```

```
! Flexible NetFlow
flow exporter FlowExporter1
  destination 192.168.9.101
  transport udp 9996
  export-protocol netflow-v5
  source FastEthernet 0/1
flow monitor FlowMonitor1
  record netflow ipv4 original-input
  exporter FlowExporter1
  cache timeout active 1
  cache timeout inactive 15
interface FastEthernet 0/1
  ip flow monitor FlowMonitor1 [input|output]
```


(WLC) >show ap summ

Number of APs..... 2

Global AP User Name..... cisco

Global AP Dot1x User Name..... ciscoAP

AP Name Country	Priority	Slots	AP Model	Ethernet MAC	Location	Port
AP1cdf.0f94.8063		2	AIR-CAP3502I-A-K9	1c:df:0f:94:80:63	default location	1
AP588d.0959.4921		2	AIR-LAP1262N-A-K9	58:8d:09:59:49:21	default location	1

SW2# show authentication session int g1/0/14

Interface: GigabitEthernet1/0/14
MAC Address: 0023.eb54.1109
IP Address: Unknown
User-Name: 00-23-EB-54-11-09
Status: Authz Success
Domain: VOICE
Security Policy: Should Secure
Security Status: Unsecure
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: 9
SGT: 0004-0
Session timeout: 3600s (local), Remaining: 3509s
Timeout action: Reauthenticate
Idle timeout: N/A
Common Session ID: C0A842420000002E003D9546
Acct Session ID: 0x00000030
Handle: 0x3C00002F

Runnable methods list:

Method	State
mab	Authc Success
dot1x	Not run

SW2# show auth sess int g1/0/18

Interface: GigabitEthernet1/0/18
MAC Address: 588d.0959.4921
IP Address: Unknown
User-Name: ciscoAP
Status: Authz Success
Domain: DATA
Security Policy: Should Secure
Security Status: Unsecure
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: N/A
SGT: 0005-0
Session timeout: 3600s (local), Remaining: 3394s
Timeout action: Reauthenticate
Idle timeout: N/A
Common Session ID: 0A3209050000D66D035B9D5E
Acct Session ID: 0x0000D67F
Handle: 0xF10007B5

Runnable methods list:

Method	State
dot1x	Authc Success

```
config ap 802.1Xuser add username ciscoAP password CCie123 all
```

```
ip device tracking
```

```
interface GigabitEthernet1/0/14
  switchport access vlan 99
  switchport mode access
  switchport voice vlan 9
  ip device tracking maximum 2
  ip access-group ACL_DEFAULT in
  authentication host-mode multi-auth
  authentication open
  authentication order mab dot1x
  authentication priority dot1x mab
  authentication port-control auto
  authentication periodic
  mab
  dot1x pae authenticator
  spanning-tree portfast
```

```
interface GigabitEthernet1/0/18
  switchport access vlan 77
  switchport mode access
  ip device tracking maximum 1
  ip access-group ACL_DEFAULT in
  authentication host-mode multi-auth
  authentication open
  authentication port-control auto
  authentication periodic
  dot1x pae authenticator
```

```
aaa authentication dot1x default group radius
```

```
aaa accounting dot1x default group radius
```

```
aaa authorization network MLIST group radius
```

```
radius-server host 192.168.2.15 auth-port 1812 acct-port 1813 pac key  
cisco123
```



```
cts device-id SW2 password cisco123  
cts device-id SW1 password cisco123
```

SW2# show cts pac

AID: E716C410120149EFB247059C52D745D0

PAC-Info:

PAC-type = Cisco Trustsec

AID: E716C410120149EFB247059C52D745D0

I-ID: SW2

A-ID-Info: Identity Services Engine

Credential Lifetime: 02:52:52 UTC Nov 24 2013

PAC-Opaque: 000200A80003000100040010E716C410120149EFB247059C52D-
745D00006008C0003010097E3F0A137617E7D755A
8EA45EE33B73000000135217589B00093A80EF958D003DD12E00CA36774CD161C3CEBA98A8D-
1C71BF4ADE26FBB21
73B45E219072916142E2332A5A84C2679B628DE62224AB8E4F6449074773E914E0B-
5F4CD684557A6748A09E75045
D0D7544E74AF085E6D35F3A1BBBC2AFFD5DDC28FA0185BF67A7708F2AF0DC22B241E

Refresh timer is set for 2y34w

SW1# show cts pac

AID: E716C410120149EFB247059C52D745D0

PAC-Info:

PAC-type = Cisco Trustsec

AID: E716C410120149EFB247059C52D745D0

I-ID: SW1

A-ID-Info: Identity Services Engine

Credential Lifetime: 22:03:34 UTC Nov 24 2013

PAC-Opaque: 000200A80003000100040010E716C410120149EFB247059C52D-
745D00006008C00030100236058BADC2408055D44
558F6023ABC6000000135217589B00093A80EF958D003DD12E00CA36774CD161C3CE-
4FA82A29C82F2D1FCFA79CCA
91BFBA8759EAE57250386392FDE86B896EBEF0CB68713C84E178D962F6C77A484E580BBF4726
F4094DE7F945FB4E
1D528B10D7598C1428E458CD1D87530F390D46D749C05E1A2C1D95024BDC2BB35D1D
Refresh timer is set for 2y34w

SW2# show cts interface

Global Dot1x feature is Enabled

Interface GigabitEthernet1/0/23:

```
CTS is enabled, mode:      DOT1X
IFC state:                 OPEN
Authentication Status:    SUCCEEDED
  Peer identity:          "SW1"
  Peer's advertised capabilities: "sap"
  802.1X role:           Authenticator
  Reauth period configured:      240 (locally configured)
  Reauth period per policy:      86400 (server configured)
  Reauth period applied to link: 86400 (server configured)
  Reauth starts in approx. 0:23:54:45 (dd:hr:mm:sec)
Authorization Status:     SUCCEEDED
  Peer SGT:                2:NADS
  Peer SGT assignment: Trusted
SAP Status:               SUCCEEDED
  Version:                 2
  Configured pairwise ciphers:
    gcm-encrypt
    null
    no-encap

  Replay protection:       enabled
  Replay protection mode: STRICT

  Selected cipher:        gcm-encrypt

Propagate SGT:           Enabled
Cache Info:
  Cache applied to link : NONE
```

```
Statistics:
  authc success:          17
  authc reject:           1
  authc failure:          1
  authc no response:      0
  authc logoff:           0
  sap success:            17
  sap fail:               0
  authz success:          3
  authz fail:             1
  port auth fail:        0
```

L3 IPM: disabled.

Dot1x Info for GigabitEthernet1/0/23

```
-----
PAE                               = AUTHENTICATOR
QuietPeriod                       = 60
ServerTimeout                     = 0
SuppTimeout                       = 30
ReAuthMax                         = 2
MaxReq                             = 2
TxPeriod                          = 30

```

SW1# show cts interface

Global Dot1x feature is Enabled

Interface GigabitEthernet1/0/23:

```
  CTS is enabled, mode:   DOT1X
  IFC state:              OPEN
  Authentication Status:  SUCCEEDED
    Peer identity:       "SW2"
    Peer's advertised capabilities: "sap"
  802.1X role:           Supplicant
  Reauth period applied to link: Not applicable to Supplicant role

```

```
  Authorization Status:  SUCCEEDED
    Peer SGT:            2:NADS
    Peer SGT assignment: Trusted
  SAP Status:            SUCCEEDED
  Version:               2

```

Configured pairwise ciphers:

```
  gcm-encrypt
  null
  no-encap

```

```
  Replay protection:     enabled
  Replay protection mode: STRICT

```

```
  Selected cipher:       gcm-encrypt

```

```
  Propagate SGT:         Enabled

```

Cache Info:

```
  Cache applied to link : NONE

```

Statistics:

```
  authc success:         1
  authc reject:          1
  authc failure:         1
  authc no response:     0
  authc logoff:          0
  sap success:           1
  sap fail:              0

```

```
authz success:      4
authz fail:         0
port auth fail:    0
```

L3 IPM: disabled.

Dot1x Info for GigabitEthernet1/0/23

```
-----
PAE                = SUPPLICANT
StartPeriod        = 30
AuthPeriod         = 30
HeldPeriod         = 60
MaxStart           = 3
Credentials profile = CTS-ID-profile
EAP profile        = CTS-EAP-profile
```

SGA policies are propagated over the secure link, protected by MACsec. Verify counters are incrementing.

SW1# show cts macsec counters int g1/0/23

```
CTS Security Statistic Counters:
    rxL2UntaggedPkts = 0
    rxL2NotagPkts = 23
    rxL2SCMissPkts = 0
    rxL2CTRLPkts = 0
    rxL3CTRLPkts = 0
    rxL3UnknownSAPkts = 0
    rxL2BadTagPkts = 0
    txL2UntaggedPkts = 0
    txL2CtrlPkts = 0
    txL3CtrlPkts = 0
    txL3UnknownSA = 0

    SA Index : 0
    rxL2ReplayfailPkts = 0
    rxL2AuthfailPkts = 0
    rxL2PktsOK = 3220
    rxL3AuthCheckFail = 0
    rxL3ReplayCheckFail = 0
    rxL2SAMissPkts = 23
    rxL3EspGcm_Pkts = 0
    rxL3InverseCheckfail = 0
    txL3Protected = 0
```

SW2# show cts macsec counters interface g1/0/23

```
CTS Security Statistic Counters:
    rxL2UntaggedPkts = 0
    rxL2NotagPkts = 186
```

```
rxL2SCMissPkts = 0
rxL2CTRLPkts = 0
rxL3CTRLPkts = 0
rxL3UnknownSAPkts = 0
rxL2BadTagPkts = 0
txL2UntaggedPkts = 0
txL2CtrlPkts = 0
txL3CtrlPkts = 0
txL3UnknownSA = 0

SA Index : 0
rxL2ReplayfailPkts = 0
rxL2AuthfailPkts = 0
rxL2PktsOK = 4367
rxL3AuthCheckFail = 0
rxL3ReplayCheckFail = 0
rxL2SAMissPkts = 186
rxL3EspGcm_Pkts = 0
rxL3InverseCheckfail = 0
txL3Protected = 0
txL2Protected = 2816
```

SW2# show cts environment-data

CTS Environment Data

=====

Current state = COMPLETE

Last status = Successful

Local Device SGT:

SGT tag = 2-00:NADS

Server List Info:

Installed list: CTSServerList1-0001, 1 server(s):

*Server: 192.168.2.15, port 1812, A-ID E716C410120149EFB247059C52D745D0

Status = ALIVE

auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime
= 20 secs

Security Group Name Table:

0-00:Unknown

2-00:NADS

3-00:NET70

4-00:IPPhone

5-00:AP

Environment Data Lifetime = 120 secs

SW2# show cts role-based sgt all

Active IP-SGT Bindings Information

IP Address	SGT	Source
10.50.9.5	2	INTERNAL
10.50.9.6	4	LOCAL
10.50.40.7	7	VLAN
10.50.50.5	2	INTERNAL
10.50.70.4	3	VLAN
10.50.70.5	2	INTERNAL
10.50.70.6	3	VLAN
10.50.77.5	2	INTERNAL
10.50.77.8	5	LOCAL
10.50.99.5	2	INTERNAL

```
SW2# show cts role-based permission
```

```
IPv4 Role-based permissions default:
```

```
Permit IP-00
```

```
IPv4 Role-based permissions from group 4:IPPhone to group 3:NET70:
```

```
IPPhone-30
```

```
Deny IP-00
```

```
IPv4 Role-based permissions from group 5:AP to group 3:NET70:
```

```
APSRvs-40
```

```
Deny IP-00
```

```
SW2# show access-list
```

```
Role-based IP access list APSRvs-40 (downloaded)
```

```
10 permit icmp
```

```
20 permit udp dst eq 5246
```

```
30 permit udp dst eq 5247
```

```
Role-based IP access list Deny IP-00 (downloaded)
```

```
10 deny ip
```

```
Role-based IP access list IPPhone-30 (downloaded)
```

```
10 permit tcp dst eq 2000
```

```
20 permit tcp dst eq www
```

```
30 permit udp dst eq bootps
```

```
40 permit udp dst eq domain
```

```
50 permit tcp src eq www
```

```
60 permit icmp
```

```
70 permit udp dst eq tftp
```

```
Role-based IP access list Permit IP-00 (downloaded)
```

```
10 permit ip
```

SW2# show cts role-based counters

Role-based IPv4 counters

'-' in hardware counters field indicates sharing among cells with identical policies

From	To	SW-Denied	HW-Denied	SW-Permitted	HW-Permitted
4	3	0	107	0	71
5	3	0	0	0	40
*	*	0	0	8595	14282

```
aaa authentication dot1x default group radius
aaa authorization network MLIST group radius
!
!
dot1x system-auth-control

interface GigabitEthernet1/0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
 cts dot1x
  sap mode-list gcm-encrypt null no-encap
 radius-server vsa send authentication
```

```
aaa authentication dot1x default group radius
aaa authorization network MLIST group radius
aaa accounting dot1x default start-stop group radius

dot1x system-auth-control
aaa server radius dynamic-author
  client 192.168.2.15
  server-key cisco123

cts authorization list MLIST
cts role-based enforcement
cts role-based enforcement vlan-list 9,70,77

interface GigabitEthernet1/0/23
  switchport trunk encapsulation dot1q
  switchport mode trunk
  cts dot1x
  sap mode-list gcm-encrypt null no-encap

radius-server attribute 44 include-in-access-req default-vrf
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server dead-criteria time 10 tries 5
radius-server host 192.168.2.15 auth-port 1812 acct-port 1813 pac key cisco123
radius-server vsa send accounting
radius-server vsa send authentication
```

```
interface X
switchport access vlan 10
switchport mode access
switchport voice vlan 99
ip access-group ACL-ALLOW in
authentication event fail action next-method
authentication event server dead action authorize vlan 2274
authentication event server alive action reinitialize
authentication event linksec fail action next-method
authentication host-mode multi-domain
authentication open
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication violation restrict
macsec mka default-policy
mab
dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast
end
```


SW2# show cts sxp connection

SXP : Enabled

Highest Version Supported: 3

Default Password : Not Set

Default Source IP: Not Set

Connection retry open period: 120 secs

Reconcile period: 120 secs

Retry open timer is not running

Peer IP : 10.50.70.4

Source IP : 10.50.70.5

Conn status : On

Conn version : 3

Local mode : SXP Speaker

Connection inst# : 1

TCP conn fd : 2

TCP conn password: none

Duration since last state change: 1:15:43:12 (dd:hr:mm:sec)

Peer IP : 10.50.70.6

Source IP : 10.50.70.5

Conn status : On

Conn version : 2

Local mode : SXP Speaker

Connection inst# : 1

TCP conn fd : 1

TCP conn password: none

Duration since last state change: 911:12:20:18 (dd:hr:mm:sec)

Total num of SXP Connections = 2


```
SW1# show cts sxp connection
  SXP           : Enabled
Highest Version Supported: 3
Default Password : Not Set
Default Source IP: 10.50.70.4
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
-----
Peer IP       : 10.50.70.5
Source IP     : 10.50.70.4
Conn status   : On
Conn version  : 3
Local mode    : SXP Listener
Connection inst# : 1
TCP conn fd   : 1
TCP conn password: none
Duration since last state change: 1:15:42:01 (dd:hr:mm:sec)

Total num of SXP Connections = 1
```

```
R6# show cts sxp connection
  SXP           : Enabled
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
-----
```

Peer IP : 10.50.70.5
Source IP : 10.50.70.6
Conn status : On
Conn version : 2
Local mode : SXP Listener
Connection inst# : 2
TCP conn fd : 1
TCP conn password: none
Duration since last state change: 1:22:48:33 (dd:hr:mm:sec)

Peer IP : 10.50.100.10
Source IP : 10.50.80.6
Conn status : On
Conn version : 2
Local mode : SXP Listener
Connection inst# : 1
TCP conn fd : 2
TCP conn password: default SXP password
Duration since last state change: 0:00:10:14 (dd:hr:mm:sec)

Total num of SXP Connections = 2

```
(WLC) >show cts sxp connections
Total num of SXP Connections..... 1
SXP State..... Enable
Peer IP          Source IP          Connection Status
-----
10.50.80.6       10.50.100.10      On
```

SW2# show cts role-based sgt all

Active IP-SGT Bindings Information

IP Address	SGT	Source
10.50.9.5	2	INTERNAL
10.50.9.6	4	LOCAL
10.50.30.3	12	CLI
10.50.30.4	12	CLI
10.50.40.7	7	VLAN
10.50.50.5	2	INTERNAL
10.50.50.20	14	CLI
10.50.70.4	2	CLI
10.50.70.5	2	INTERNAL
10.50.70.6	3	VLAN
10.50.77.5	2	INTERNAL
10.50.77.8	5	LOCAL
10.50.80.50	16	CLI
10.50.99.5	2	INTERNAL
10.50.100.1	15	CLI
10.50.100.2	15	CLI
10.50.100.10	15	CLI
192.168.2.25	18	CLI

IP-SGT Active Bindings Summary

Total number of VLAN bindings = 2
Total number of CLI bindings = 9
Total number of LOCAL bindings = 2
Total number of INTERNAL bindings = 5
Total number of active bindings = 18

SW1# sho cts role-based sgt all

Active IP-SGT Bindings Information

IP Address	SGT	Source
10.50.9.5	2	SXP
10.50.9.6	4	SXP
10.50.30.3	12	SXP
10.50.30.4	12	SXP
10.50.40.7	7	SXP
10.50.50.5	2	SXP
10.50.50.20	14	SXP
10.50.70.4	2	INTERNAL
10.50.70.5	2	SXP
10.50.70.6	3	SXP
10.50.77.5	2	SXP
10.50.77.8	5	SXP
10.50.80.50	16	SXP
10.50.99.5	2	SXP
10.50.100.1	15	SXP
10.50.100.2	15	SXP
10.50.100.10	15	SXP
192.168.1.5	2	INTERNAL
192.168.2.5	2	INTERNAL
192.168.2.25	18	SXP
192.168.100.1	2	INTERNAL

IP-SGT Active Bindings Summary

Total number of SXP bindings = 17
Total number of INTERNAL bindings = 4
Total number of active bindings = 21

R6# show cts role-based sgt all
Active IP-SGT Bindings Information

IP Address	SGT	Source
10.50.9.5	2	SXP
10.50.9.6	4	SXP
10.50.30.3	12	SXP
10.50.30.4	12	SXP
10.50.40.7	7	SXP
10.50.50.5	2	SXP
10.50.50.20	14	SXP
10.50.70.4	2	SXP
10.50.70.5	2	SXP
10.50.70.6	3	SXP
10.50.77.5	2	SXP
10.50.77.8	5	SXP
10.50.80.50	16	SXP
10.50.99.5	2	SXP
10.50.100.1	15	SXP
10.50.100.2	15	SXP
10.50.100.10	15	SXP
192.168.2.25	18	SXP

IP-SGT Active Bindings Summary

Total number of SXP bindings = 18
Total number of active bindings = 18

```
cts role-based sgt-map 10.50.30.3 sgt 12
cts role-based sgt-map 10.50.30.4 sgt 12
cts role-based sgt-map 10.50.50.20 sgt 14
cts role-based sgt-map 10.50.70.4 sgt 2
cts role-based sgt-map 10.50.80.50 sgt 16
cts role-based sgt-map 10.50.100.1 sgt 15
cts role-based sgt-map 10.50.100.2 sgt 15
cts role-based sgt-map 10.50.100.10 sgt 15
cts role-based sgt-map 192.168.2.25 sgt 18
cts role-based sgt-map vlan-list 70 sgt 3
cts role-based sgt-map vlan-list 40 sgt 7
cts role-based enforcement
cts role-based enforcement vlan-list 9,40,70,77
cts sxp enable
cts sxp connection peer 10.50.70.6 password none mode local
cts sxp connection peer 10.50.70.4 password none mode local
!
```

```
cts sxp enable
```

```
cts sxp default source-ip 10.50.70.4
```

```
cts sxp connection peer 10.50.70.5 password none mode local listener
```



```
cts exp enable
```

```
cts exp connection peer 10.50.70.5 password none mode local listener
```

```
config cts sxp enable
config cts sxp default password cisco
config cts sxp connection peer 10.50.80.6
```

SW# **wr erase**

<enter> (confirm)

reload

<enter> (confirm)

System configuration has been modified. Save? [yes/no]: **no**

Proceed with reload? [confirm]

Would you like to enter the initial configuration dialog? [yes/no]: **n**

Switch# **conf t**

Enter configuration commands, one per line. End with CNTL/Z.

R# del nvram:*cer

R# del nvram:ciscoca*

R# wr er

<enter> (confirm)

reload

<enter> (confirm)

System configuration has been modified. Save? [yes/no]: no

Proceed with reload? [confirm]

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no

Would you like to terminate autoinstall? [yes]: yes

```
ASAx# show mode
If Security context mode: single
ASAx# conf t
ASAx(config)# clear configure all
ciscoasa(config)# hostname ASAx
ASAx(config)# enable password cisco
ASAx(config)# wri
! x = applicable number of device between 1 and 2
If Security context mode: multiple
ASAx# changeto system
ASAx# conf t
ASAx(config)# clear configure context
ASAx(config)# clear configure all
ciscoasa(config)# hostname ASAx
ASAx(config)# enable password cisco
ASAx(config)# wri
```

```
ASAx# del flash:c1.cfg
```

```
Delete filename [c1.cfg]? <enter>
```

```
Delete disk0:/c1.cfg? [confirm] <enter>
```

```
ASAx# del flash:c2.cfg
```

```
Delete filename [c2.cfg]? <enter>
```

```
Delete disk0:/c2.cfg? [confirm] <enter>
```

```
ASAx# del flash:admin.cfg
```

```
Delete filename [admin.cfg]? <enter>
```

```
Delete disk0:/admin.cfg? [confirm] <enter>
```

```
! x = applicable number of device between 1 and 4
```

```
! Note: There is a chance the files in step 2 will not exist if the device was in single mode, but the delete sequence should be run through anyway. The result may just be that the following error is displayed which is acceptable.
```

```
ASAx# del flash:c1.cfg
```

```
Delete filename [c1.cfg]?
```

```
Delete disk0:/c1.cfg? [confirm]
```

```
%Error deleting disk0:/c1.cfg (No such file or directory)
```

User: **cisco**

Password: **Clsc0123**

(WLC) **>clear config**

Are you sure you want to clear the configuration? (y/n) **y**

Configuration Cleared!

(WLC) **>reset system**

The system has unsaved changes.

Would you like to save them now? (y/N) **<enter>**

Configuration Not Saved!

Are you sure you would like to reset the system? (y/N) **y**

System will now restart!


```
Would you like to terminate autoinstall? [yes]: yes
System Name [Cisco_ae:21:64] (31 characters max): -
Invalid response
System Name [Cisco_ae:21:64] (31 characters max): -
Invalid response
System Name [Cisco_ae:21:64] (31 characters max): -
Invalid response
System Name [Cisco_ae:21:64] (31 characters max): WLC
Enter Administrative User Name (24 characters max): cisco
Enter Administrative Password (3 to 24 characters): Cisc1123
Management Interface IP Address: 10.50.100.10
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.50.100.2
Management Interface VLAN Identifier (0 = untagged):100
Management Interface Port Num [1 to 4]:1
Management Interface DHCP Server IP Address: 10.50.100.2
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: cisco
Network Name (SSID):cisco
Configure DHCP Bridging Mode [yes][NO]:no
Allow Static IP Addresses [YES][no]: yes
Configure a RADIUS Server now? [YES][no]: no
Enter Country Code list (enter 'help' for a list of countries) [US]: US
Enable 802.11b Network [YES][no]:no
Enable 802.11a Network [YES][no]: no
Enable 802.11g Network [YES][no]: no
Enable Auto-RF [YES][no]: no
Configure a NTP server now? [YES][no]:
Enter the NTP server's IP address: 10.50.70.5
Enter a polling interval between 3600 and 604800 secs: 3600
Configuration correct? If yes, system will save it and reset. [yes]
[NO]: YES
Configuration saved!
Resetting system with new configuration...
```

User: cisco

Password: Cisc0123

(cisco Controller) >

Cut and Paste the following:

```
config interface address management 10.50.100.10 255.255.255.0
  10.50.100.20
```

```
config interface vlan management 100
```

```
config ap mgmtuser add username cisco password CCie123 enablesecret
  CCie123 all
```

```
config sysname WLC
```

```
config prompt WLC
```

```
config network webmode enable
```

Are you sure you want to save? (y/n) **y**

IPS# **erase current-config**

Warning: Removing the current-config file will result in all configuration being reset to default, including system information such as IP address.

User accounts will not be erased. They must be removed manually using the "no username" command.

Continue? []: **yes**

IPS# **reset**

Warning: Executing this command will stop all applications and reboot the node.

Continue with reset? []: **yes**

sensor login: **ciscoips**

Password: **123cisco123**

System will then restart.

! Let the sensor boot to its default mode 0

GNU GRUB version 1.0(11)5 (631K lower / 2096128K upper memory)

0: **Cisco IPS**

1: Cisco IPS Recovery

2: Cisco IPS Clear Password (cisco)

sensor login: ciscoips

Password:

--- Basic Setup ---

--- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.

User ctrl-c to abort configuration dialog at any prompt.

Default settings are in square brackets '[]'.

ctrl-c

! If you get the following just select 0

[0] Go to the command prompt without saving this config.

[1] Return to setup without saving this config.

[2] Save this configuration and exit setup.

[3] Continue to Advanced setup.

Enter your selection[3]: **0**

sensor#

```
wsa.cisco.com> resetconfig
```

```
Are you sure you want to reset all configuration values? [N]> y
```

```
ironport.example.com> loadconfig
```

```
1. Paste via CLI
```

```
2. Load from file
```

```
How would you like to load a configuration file?
```

```
[1]> 1
```

```
Paste the configuration file now.
```

```
Press CTRL-D on a blank line when done.
```

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

```
<!DOCTYPE config SYSTEM "config.dtd">
```

```
<config>
```

```
  <hostname>wsa.cisco.com</hostname>
```

```
  <interfaces>
```

```
    <interface>
```

```
      <interface_name>Management</interface_name>
```

```
      <ip>192.168.2.50</ip>
```

```
      <phys_interface>Management</phys_interface>
```

```
      <netmask>255.255.255.0</netmask>
```

```
      <interface_hostname>wsa.cisco.com</interface_hostname>
```

```
      <ftpd_port>21</ftpd_port>
```

```
      <sshd_port>22</sshd_port>
```

```
      <httpd_port>8080</httpd_port>
```

```
      <https_redirect>0</https_redirect>
```

```
      <httpsd_port>8443</httpsd_port>
```

```
    </interface>
```

```
  </interfaces>
```

```
</config>
```

```
<local_dns>
  <dns_ip priority="0">192.168.2.25</dns_ip>
</local_dns>
<dns_ptr_timeout>10</dns_ptr_timeout>
<dns_routing_table>0</dns_routing_table>
</dns>

<default_gateway>192.158.2.5</default_gateway>
<routes>
</routes>

<ntp>
  <ntp_server>192.168.2.5</ntp_server>
  <ntp_routing_table>0</ntp_routing_table>
</ntp>

  <timezone>America/Los_Angeles</timezone>
</config>
```

CNTRL-D

Values have been loaded. Be sure to run "commit" to make these settings active.

ironport.example.com> **commit**

Please enter some comments describing your changes:

[]> **bootstrap**

Changes committed: Tue Oct 16 20:15:50 2012 PDT
wsa.cisco.com>

CiscoASA# debug crypto isakmp

[IKEv1]: Group = 209.165.200.231, IP = 209.165.200.231, Tunnel Rejected:
Conflicting protocols specified by tunnel-group and group-policy

[IKEv1]: Group = 209.165.200.231, IP = 209.165.200.231, QM FSM error (P2
struct &0xb0cf31e8, mess id 0x97d965e5)!

[IKEv1]: Group = 209.165.200.231, IP = 209.165.200.231, Removing peer from
correlator table failed, no match!