SENSS

Implementing Cisco Edge Network Security Solutions

Volume 2 **Student Guide**
Version 1.0

Part Number: 97-3330-01

https://t.me/learningnets



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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1110R)

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED "AS IS" AND AS SUCH MAY INCLUDE TYPOGRAPHICAL, GRAPHICS, OR FORMATTING ERRORS. CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

© 2014 Cisco Systems, Inc.

https://t.me/learningnets

Table of Contents

Threat Controls Deployment on Cisco ASA	***4-1***
Introducing Cisco Firewall Threat Controls	**4-3**
Overview of Firewall Threat Controls	4-4
Cisco Modular Network Architecture and Firewall Threat Controls	4-7
Firewall Filtering Layers	4-8
Firewall Filtering Approaches	4-9
Firewall Filtering Technologies	4-10
Combining Firewall Filtering Technologies	4-15
Firewall Threat Controls and Cisco Products and Features	4-17
Summary	4-19
Deploying Basic Cisco ASA Access Policies	**4-21**
Overview of Cisco ASA Access Control Features	4-23
Connection Table	4-24
Examining the Connection Table	4-27
Local Host Table	4-29
Examining the Local Host Table	4-30
Connection Table Logging	4-31
Interface ACLs	4-32
Configure Interface ACLs	4-38
Verify Interface ACLs	4-48
Global ACLs	4-50
Configure Global ACLs	4-51
Verify Global ACLs	4-56
Object Groups	4-58
Configure Object Groups	4-59
Verify Object Groups	4-67
Troubleshoot ACLs	4-69
Summary	4-75
Deploying Advanced Cisco ASA Access Policies	**4-77**
Advanced Cisco ASA Access Policies Overview	4-79
Cisco MPF Overview	4-80
OSI Layer 3–4 Policies Overview	4-81
Default OSI Layer 3–4 Stateful Tracking	4-85
Tune OSI Layer 3–4 Stateful Tracking	4-87
Verify OSI Layer 3–4 Stateful Tracking	4-93
Support for Dynamic Protocols	4-94
Configure Support for Dynamic Protocols	4-98
Verify Support for Dynamic Protocols	4-103
Application Layer (OSI Layer 5–7) Policies Overview	4-104
HTTP Inspector Overview	4-110
Configure HTTP Inspection	4-114
Verify HTTP Inspection	4-126

https://t.me/learningnets

FTP Inspector Overview 4-127
Evaluate Application Inspection of Other Protocols 4-130
Summary 4-132
Deploying Reputation-Based Cisco ASA Access Policies 4-133
Overview of the Cisco Botnet Traffic Filter 4-134
Configure the Cisco Botnet Traffic Filter 4-138
Verify the Cisco Botnet Traffic Filter 4-145
Summary 4-149
Deploying Identity-Based Cisco ASA Access Policies 4-151
Overview of the Identity Firewall 4-153
Identity Firewall Flow 4-155
Cisco CDA Overview 4-159
Integrate Cisco CDA with AD and Cisco ASA 4-162
Verify Cisco CDA Integration with AD 4-166
Integrate Cisco ASA with AD and Cisco CDA 4-167
Verify Cisco ASA Integration with AD and Cisco CDA 4-173
Configure Identity-Based Access Rules 4-177
Verify the Identity-Based Firewall 4-182
Troubleshoot Identity-Based Firewall 4-186
Summary 4-190
Module Summary 4-191
Module Self-Check 4-193
Threat Controls Deployment on Cisco IOS Software 5-1
Deploying Basic Cisco IOS Zone-Based Policy Firewall Access Policies 5-3
Overview of the Cisco IOS Zone-Based Policy Firewall 5-4
Configure Zones and Zone Pairs 5-7
Verify Zones and Zone Pairs 5-10
Configure a Basic OSI Layer 3 and 4 Interzone Access Policy 5-11
Verify a Basic OSI Layer 3 and 4 Interzone Access Policy 5-23
Configure a Basic OSI Layer 3 and 4 Intrazone Access Policy 5-26
Configure Inspection of Control Plane and Management Plane Traffic 5-29
Tune Stateful Engine and Connection Settings 5-35
Configure Support for NAT 5-42
Troubleshoot the Zone-Based Policy Firewall 5-44
Summary 5-47
Deploying Advanced Cisco IOS Zone-Based Policy Firewall Access Policies 5-49
Overview of Advanced Access Policies 5-51
Overview of Application-Layer Access Policies 5-52
HTTP Inspector Overview 5-54
Configure HTTP Inspection 5-58
Verify HTTP Inspection 5-63
Inspection of Instant Messaging 5-64
Inspection of Peer-to-Peer Protocols 5-65

 © 2014 Cisco Systems, Inc.

https://t.me/learningnets

Additional Application Inspection 5-66
URL Filtering Methods in Cisco IOS Zone-Based Policy Firewall 5-67
Configure Local List-Based URL Filtering 5-68
Summary 5-71
Module Summary 5-73
Module Self-Check 5-75
Glossary G-1

https://t.me/learningnets

https://t.me/learningnets

Module 4

Threat Controls Deployment on Cisco ASA

Introduction

The Cisco ASA adaptive security appliance helps enforce security policies within networks. In this module, you will examine the basic and advanced threat controls that are available in Cisco ASA product line.

The threat controls include access control features, application inspection features, Botnet traffic filtering, and Identity-based access.

Upon completing this module, you will be able to:

- Provide an overview of Cisco firewall threat controls
- Describe and configure basic Cisco ASA access polices
- Describe and configure advanced Cisco ASA access policies
- Describe and configure reputation-based Cisco ASA access policies
- Describe and configure identity-based Cisco ASA access policies

https://t.me/learningnets

https://t.me/learningnets

Lesson 1

Introducing Cisco Firewall Threat Controls

Overview

Firewall systems are the mainstream threat defense method based on network zoning and zone interface points filtering. Firewall systems can provide a set of effective methods to reduce risk to exposed services and business processes by using different traffic filtering approaches and technologies. This lesson describes firewall systems, and common filtering approaches and technologies that are found inside a firewall system.

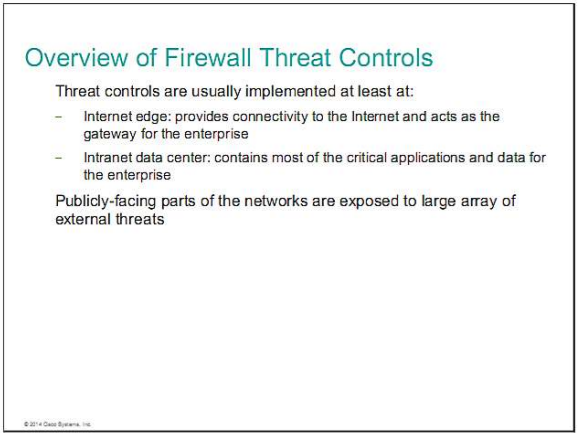
Upon completing this lesson, you will be able to:

- Describe firewall threat controls
- Place firewall threat controls into the Cisco modular network architecture design architectures
- Describe how a firewall system can filter traffic at different OSI layers
- Describe restrictive and permissive firewall filtering approach
- Describe firewall filtering technologies
- Describe how to combine firewall filtering technologies
- Describe Cisco products and features that are available to implement firewall threat controls

https://t.me/learningnets

Overview of Firewall Threat Controls

This topic describes firewall threat controls.



Controls against various threats should be implemented at least at the most exposed and critical parts of the enterprise networks:

The Internet edge is the network infrastructure that provides connectivity to the Internet and that acts as the gateway for the enterprise to the rest of the cyberspace. The Internet edge is a public-facing network infrastructure and is particularly exposed to large array of external threats. Some of the expected threats are as follows:

- DoS, DDoS
- Spyware, malware, and adware
- Network intrusion, takeover, and unauthorized network access
- E-mail spam and viruses
- Web-based phishing, viruses, and spyware
- Application-layer attacks (XML attacks, cross scripting, and so on)
- Identity theft, fraud, and data leakage

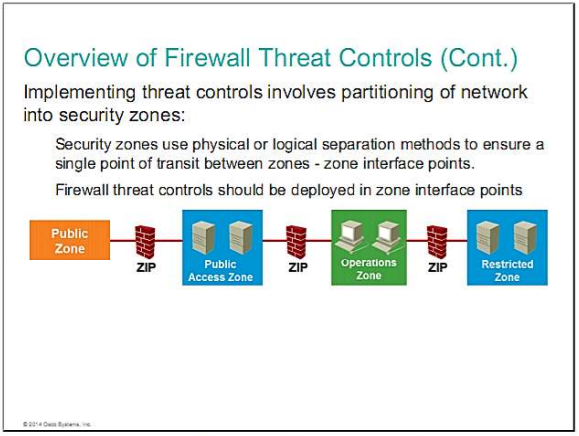
The Intranet data center houses most of the critical applications and data for the enterprise. The Intranet data center is primarily inward facing and most clients are on the internal enterprise network. The Intranet data center is still subject to external threats, but must also be guarded against threat sources inside of the network perimeter. The following are some of the threat vectors affecting the Intranet data center:

- Unauthorized access
- Interruption of service
- Data loss

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

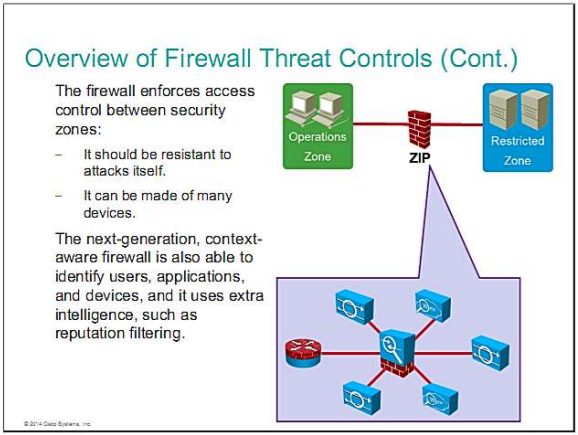
– Data modification

Unauthorized access can include unauthorized device access and unauthorized data access. Interruption of service, data loss, and data modification can be the result of targeted attacks. A single threat can target one or more of these areas. Specific threats can include the following: privilege escalation; malware; spyware; botnets; DoS; traversal attacks (including directory, URL); cross-site scripting attacks; SQL attacks; malformed packets; viruses; worms; and, man-in-the-middle.



A common approach to implementing threat controls involves separating the network into individual zones, and minimizing the interactions between these zones. This approach is commonly applied to enterprise networks, where security designers partition the network into security zones, and control network access between these zones using access controls that are implemented by firewall systems.

These zones are created by using either physical separation, where each zone uses a separate physical infrastructure, or by using logical separation, where resources are separated using logical separation techniques, such as VLANs, VRF Lite, MPLS, and similar methods. In most cases, there should be only one single point of transit between these zones (often called a zone interface points), where access control can be enforced in a scalable and manageable manner.



A firewall is a system that enforces an access control policy between two or more security zones.

All firewalls share common properties:

The firewall itself must be resistant to attack; otherwise, it would allow an attacker to disable the firewall or change its access rules.

All traffic between security domains must flow through the firewall. This restriction prevents a backdoor connection that could be used to bypass the firewall, violating the network access policy.

A firewall can be a single device or a large set of multiple devices. Each device provides a specific traffic-filtering role to achieve the desired level of protection. For example, a firewall designer may choose to include stateful filtering devices, proxies, network intrusion prevention systems, and similar components to build a firewall system.

A next-generation, context-aware firewall also performs these functions:

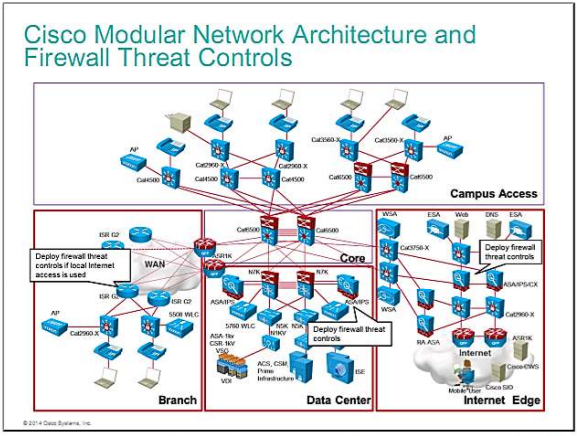
It identifies users, devices, and applications, and it applies application-specific policies. Identification of users is usually done with integration with user databases, such as LDAP or Microsoft Active Directory.

It uses additional security intelligence, such as application visibility and filtering, or reputation-based filtering.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Cisco Modular Network Architecture and Firewall Threat Controls

This topic places firewall threat controls into the Cisco modular network architecture design architectures.



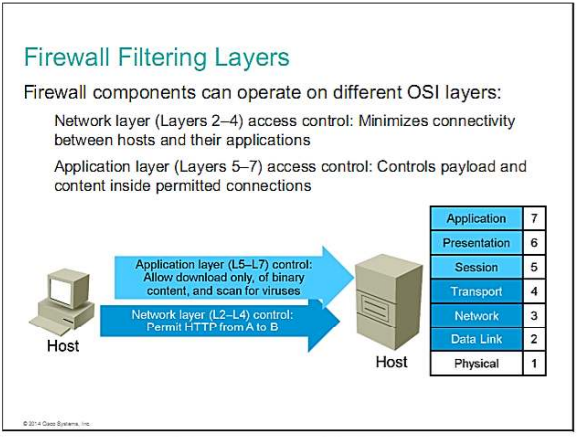
The figure illustrates where in the Cisco modular network architecture architecture firewall threat controls should be deployed. Usually, the firewall threat controls are implemented on the Internet edge, which consists at least of Service Provider edge, enterprise DMZ, remote access, and Internet edge distribution. The firewall system should control traffic when traversing all these parts of the Internet edge.

Firewall threat controls should also be deployed in the intranet data center to control access to critical enterprise applications and data. Virtualization in data centers did not only change the way how data centers are built, but also the way how security in data centers is built. Server virtualization created new challenges for security deployments. Visibility into virtual machine activity and isolation of server traffic became more difficult when virtual machine-sourced traffic could reach other virtual machines within the same server without being sent outside the physical server. Therefore, security architects should also take into considerations implementation of virtualized firewall controls, which offer visibility into traffic within a single server with many virtual machines.

Firewall threat controls should also be deployed in branch offices if the offices require local connectivity to the Internet, or zoning of the branch network is required to limit traffic between different branch compartments.

Firewall Filtering Layers

This topic describes how a firewall system can filter traffic at different OSI layers.



A network access policy defines which network connectivity is allowed according to the security policy of an organization. Firewall systems enforce network access control on two basic functional layers:

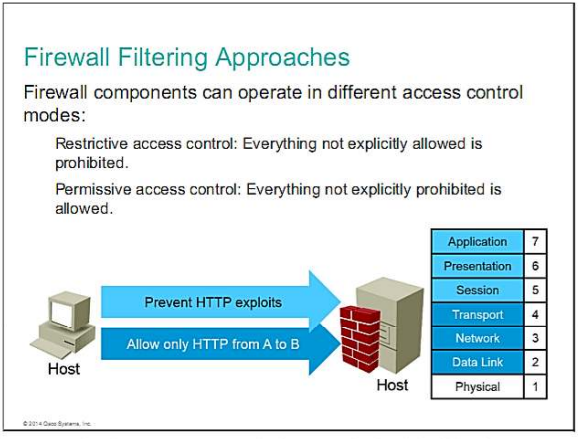
Network layer access control: This approach works at OSI Layers 2 through 4 and determines which application hosts can intercommunicate using which protocols and applications. An example of network layer access control is a firewall system that permits all inside users to open TCP port 80 (HTTP) connections to all servers on the Internet.

Application layer access control: This approach works at OSI Layers 5 through 7 and determines what a user can do within an application. Using this control option, the firewall system can verify the adherence of the session to the standard application layer protocol. It can also allow users to view web pages but prohibit them from posting data to the servers, block viruses in email messages by examining application layer content, and permit only well-formed XML messages inside a web services application.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Firewall Filtering Approaches

This topic describes restrictive and permissive firewall filtering approach.



A firewall system can implement access control using one or both of the following two approaches:

The restrictive (or proactive) approach: In this approach, the firewall by default denies all communication and allows only the aspects of communication that are explicitly permitted. Examples of this approach are stateful packet filtering devices that allow only specific hosts and applications to pass or a mail proxy that would allow only text-based file attachments.

The permissive (or reactive) approach: In this approach, the firewall by default permits all communication and blocks only the aspects of communication that it considers malicious based on its attack signature database. Examples of this approach are network IPSs and network antivirus.

Firewall Filtering Technologies

This topic describes firewall filtering technologies.

Firewall Filtering Technologies

The following are the mainstream filtering technologies:

- Stateless packet filtering
- Stateful packet filtering
- Stateful packet filtering with AIC (or AVC)
- Reputation-based filtering
- Network IPS
- Application layer gateways (proxies)

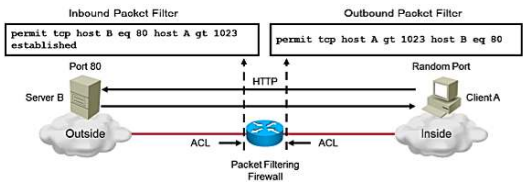
© 2014 Cisco Systems, Inc.

When you deploy firewall systems for network protection, you must understand their different components. Depending on your network needs, mandatory compliances, and access methods, you may require that specific firewall system options be set. Modern firewall systems use several mainstream traffic filtering technologies.

Firewall Filtering Technologies (Cont.)

Stateless packet filtering:

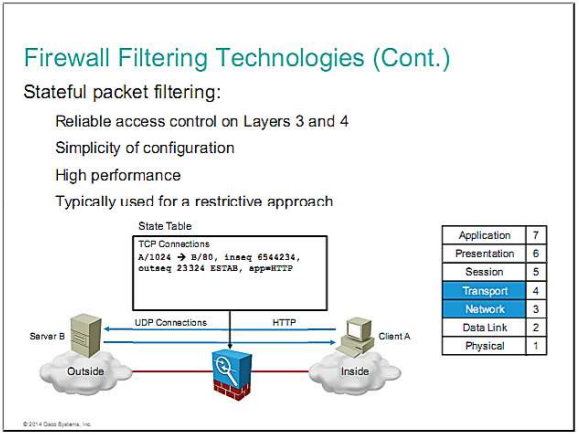
- Relies on a static rulebase of packet descriptions to permit or deny access
- Works best with static TCP applications or Layer 3-only filtering
- Transparency and high performance
- Typically used for a restrictive approach



© 2014 Cisco Systems, Inc.

https://t.me/learningnets

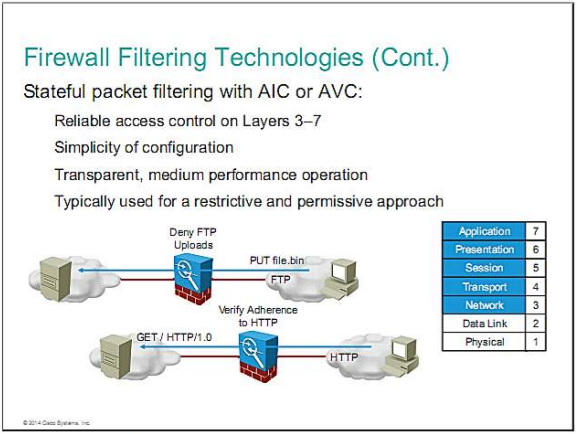
Stateless packet filtering is one of the oldest and most widely used network access control technologies. Stateless packet filtering is usually employed by an OSI Layer 3 device, such as a network router using ACLs. Stateless packet filters use a statically defined set of rules that independently (that is, statelessly—without regard to previous or future packets) examine the header or payload of each packet to permit or deny its forwarding across the device. Stateless packet filtering usually examines protocol headers of the network and transport OSI layers. However, it can be extended to the application layer by examining packet payloads and parsing packets to decode their application layer protocols for simpler access rule configuration. Cisco IOS FPM allows the decoding of OSI Layer 3 through Layer 7 protocols and matching based on the packet payload.



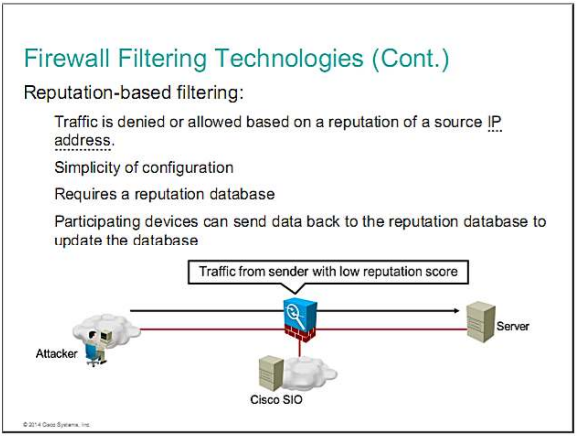
Stateful packet filtering is an application-aware method of packet filtering that works on the connection (or flow) level with occasional looks into the application layer.

Stateful packet filters maintain a state table to keep track of all active sessions that are crossing the firewall, such as a Cisco Adaptive Security Appliance or a Cisco Integrated Services Routers that is configured with a zone-based policy firewall. A state table, which is an internal data structure of a stateful packet filter, tracks all OSI Layer 4 sessions and inspects all packets that are passing through the device. Based on its memory of previous packets in a session, a stateful packet filter can anticipate what kind of traffic should arrive from communicating hosts in the near future. If the packets have the properties that are predicted by the state table, they are forwarded. The state table changes dynamically because of traffic flow.

Stateful packet filters are also application-aware while additional deeper inspection of transit traffic is being performed, which is required to manage dynamic applications. Dynamic applications typically open an initial connection on a well-known port and then negotiate additional OSI Layer 4 connections through the initial session. Stateful packet filters support these dynamic applications by analyzing the contents of the initial session and parsing the application protocol just enough to learn about the additional negotiated channels. A stateful packet filter typically assumes that if the initial connection was permitted, any additional transport layer connections of that application should also be permitted.

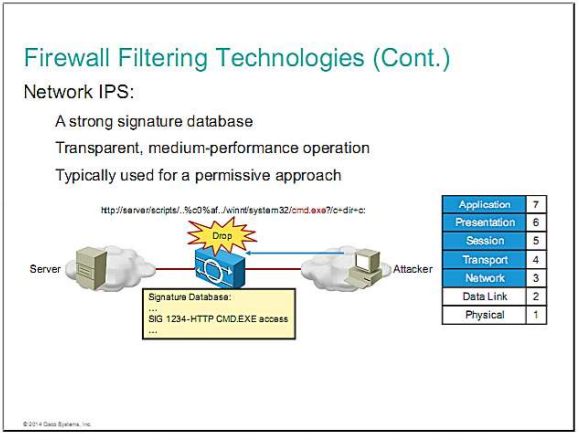


Stateful packet filtering with AIC or AVC: Many users of stateful packet filtering have increasingly demanded higher application layer awareness in their stateful packet filter-based firewalls. Most vendors have improved the application layer analysis on their pure stateful packet filtering devices by enhancing the traffic analysis engine with a service called AIC or AVC. Such devices can verify whether the application conforms to standards and is able to filter traffic based on application protocol headers and their content. Example of devices that employ stateful packet filtering with AIC and AVC include the Cisco ASA 5500-X Series Next-Generation Firewalls, which can recognize and filter over 1000 applications and more than 75,000 microapplications.

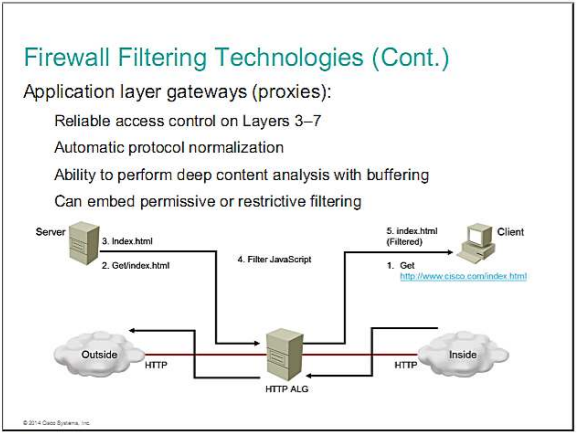


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Reputation-based filtering: This form of filtering analyzes traffic and correlates the results of analyses with the reputation of a traffic source or destination IP address. Reputation-based filtering requires an external reputation database, to which a filtering device communicates and which provides a reputation score for each traffic source or destination IP address. The participating devices send data back to the reputation database, where feedback is stored to keep the updates in the database current. Examples of devices that use reputation-based filtering include the Cisco ASA 5500-X Series Next-Generation Firewalls with botnet traffic filtering, Cisco IPS Sensors with Global Correlation, the Cisco Email Security Appliance, and the Cisco Web Security Appliance. All Cisco devices that use reputation-based filtering use threat intelligence feeds from Cisco Security Intelligence Operations, with optional URL filtering.



A **network IPS** is a network control that analyzes traffic and attempts to block known malicious traffic based on a built-in and periodically updated attack signature database. The attack signature database contains descriptions of traffic patterns—usually thousands—that indicate a known attack inside the network stream.



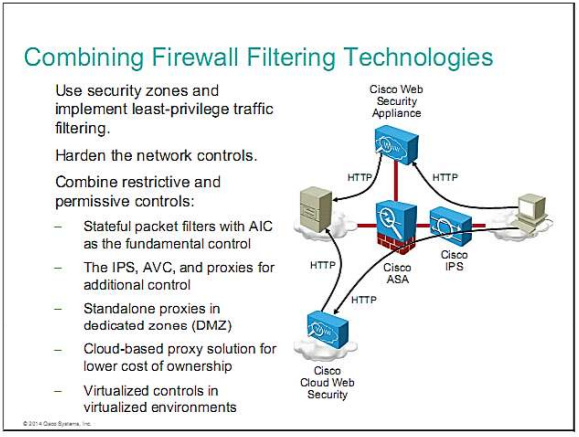
Application layer gateway, also known as proxy, acts as an intermediary and relays application layer requests and responses between clients and servers. The client connects to the proxy and submits an application layer request that indicates the true destination and the requested data. The proxy opens a session to the destination server, impersonates the client, and obtains the requested data. The proxy passes the data, which might be filtered and changed, back to the client.

In terms of access control, a proxy can limit access based on the source and destination of the request, the request itself, and the data that is returned. This access control can include allowing only specific file types to be downloaded, limiting scripting languages inside HTML content, scanning content for malware, and so on. In the example in the figure, the HTTP ALG filters out the JavaScript in the response from the web server to the client. Cisco Email Security Appliances, and the Cisco WSA are examples of proxy devices.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Combining Firewall Filtering Technologies

This topic describes how to combine firewall filtering technologies.



When you implement network controls, follow these guidelines:

Separate the network into security zones and implement least-privilege traffic filtering on the boundaries between the zones.

Harden the network controls with updated and patched software, and use AAA and secure management protocols to access the network controls.

A firewall system should use multiple technologies and devices in order to combine permissive and restrictive approaches:

- Stateful packet filters with AIC are the most flexible technology and a good starting point to base your network layer access control on. Therefore, build your basic firewall architecture with stateful packet filters as the central access control elements and then add additional features or devices to the architecture.
- You can add network IPS component to provide permissive (signature-based) access control to and from a particular security zone. Moreover, you can preferably use an integrated IPS software or hardware module (such as the IPS module inside a Cisco Adaptive Security Appliance appliance) to add IPS services to traffic selectively, based on the traffic flow specification, rather than apply it to all traffic to and from a specific zone. You can also use the AVC component of the Cisco ASA 5500-X Series Next-Generation Firewalls to provide application visibility and control for more than 1000 applications and 75,000 microapplications. You can add proxies (by using a product such as the Cisco Web Security Appliance) to provide deep packet inspection with buffering.
- Complex security devices, such as standalone proxies, should be set up in a DMZ in order to limit the damage if the proxy component is compromised.
- You can also use cloud-based proxies (such as Cisco Cloud Web Security) in order to lower the total cost of ownership and to provide a single access policy for all users, regardless of their connectivity type or location.

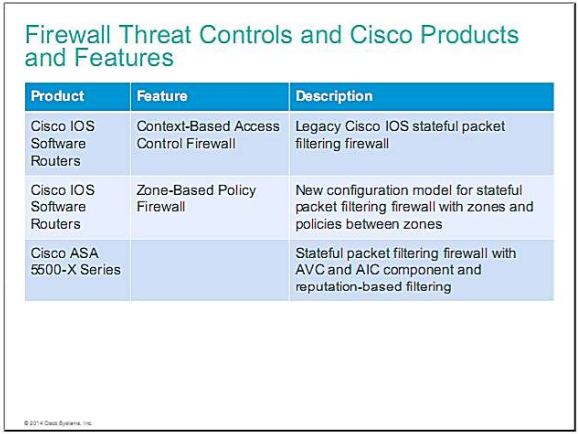
https://t.me/learningnets

- You can use virtualized controls (such as the Cisco Virtual Security Gateway and the Cisco ASA 1000V Cloud Firewall) to secure access to virtualized data centers in enterprise and cloud provider environments.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Firewall Threat Controls and Cisco Products and Features

This topic describes Cisco products and features that are available to implement firewall threat controls.



The following are some common Cisco devices and features that can be used to implement firewall threat controls:

Cisco IOS (and IOS XE) Software Routers with Context-Based Access Control Firewall: CBAC specifies what traffic needs to be let in and what traffic needs to be let out by using access lists (in the same way that Cisco IOS uses access lists). However, CBAC access lists include ip inspect statements that allow the inspection of the protocol to allow returning traffic to go to the systems behind the firewall.

Cisco IOS (and IOS XE) Software Routers with Zone-Based Policy Firewall: Cisco IOS Software Release 12.4(6)T introduced ZFW, a new configuration model for the Cisco IOS Firewall feature set. This new configuration model offers intuitive policies for multiple-interface routers, increased granularity of firewall policy application, and a default deny-all policy that prohibits traffic between firewall security zones until an explicit policy is applied to allow desirable traffic.

Cisco Adaptive Security Appliance 5500-X Series, and Cisco ASA Services Module: Cisco ASA 5500-X Series Next-Generation Firewalls are powered by Cisco ASA Software, with enterprise-class stateful packet inspection and next-generation firewall capabilities. Cisco ASA 5500-X Series Next-Generation Firewalls are available as:

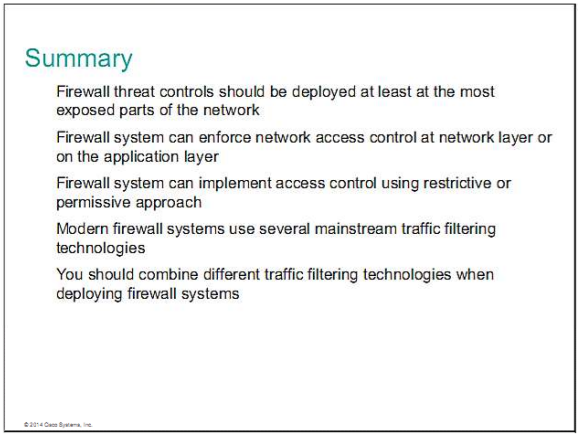
- Scalable, standalone appliances for branch offices, midsize businesses securing the Internet edge, and enterprise data centers
- High-performance blades that integrate with the Cisco Catalyst 6500 Series Switches
- Virtual instances to provide enterprise-class security for private and public clouds

Note	This course focuses on configuring Zone-Based Policy Firewall on Cisco IOS Software and on configuring Cisco ASA 5500-X Series standalone appliances.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Summary

This topic summarizes the key points that were discussed in this lesson.



https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lesson 2

Deploying Basic Cisco ASA Access Policies

The Cisco Adaptive Security Appliance5500-X Series Next-Generation Firewalls provides the administrator with a set of access control methods that can tightly control access between security zones in networks. The Cisco ASA is an application-aware, stateful packet filtering firewall, which tracks connections in a connection table. To control which session can enter the connection table, administrators use the most fundamental of Cisco ASA access controls; interface and global access control lists. This lesson describes the Cisco ASA connection table, and describes how to configure and verify interface and global ACLs. The lesson also describes how to configure object groups, which can significantly reduce ACL complexity. The lesson concludes with instructions on troubleshooting ACLs on the Cisco ASA.

Upon completing this lesson, you will be able to:

- Describe Cisco ASA basic access control features
- Describe the connection table
- Examine and administer the connection table
- Describe the local host table
- Examine and administer the local host table
- Describe connection table logging
- Describe Cisco ASA interface ACLs
- Configure interface ACLs
- Verify interface ACLs
- Describe Cisco ASA global ACLs
- Configure global ACLs
- Verify global ACLs
- Describe Cisco ASA object groups

https://t.me/learningnets

Configure object groups on the Cisco ASA

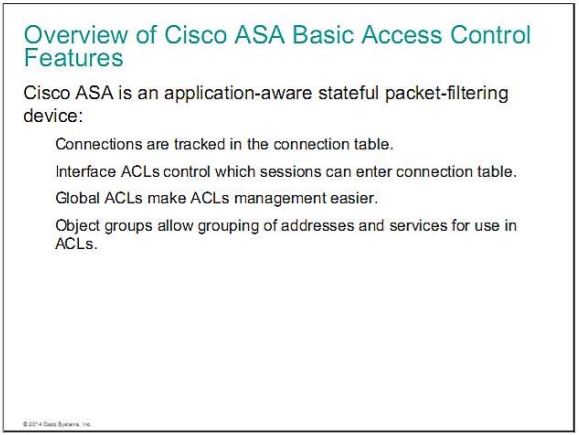
Verify object groups on the Cisco ASA

Troubleshoot ACLs on the Cisco ASA

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Overview of Cisco ASA Access Control Features

This topic describes Cisco Adaptive Security Appliance basic access control features.



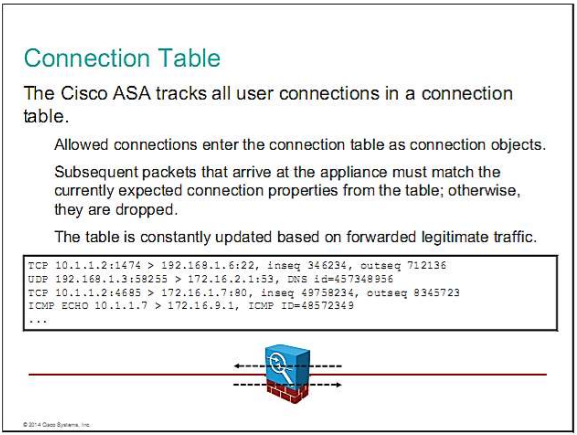
Cisco ASA access control features:

- The Cisco ASA security appliance is fundamentally an application-aware stateful packet-filtering device. The ASA tracks all connections across the ASA in the connection table.
- Cisco ASA security appliance interface ACLs are the most commonly used access control mechanism on the appliance and control which sessions can enter the connection table.
- The global ACLs of Cisco ASA make management of the access policy configuration easier.
- The object groups allow you to arbitrarily group hosts, resources, or services that share the same policy. This grouping optimizes the access rules.

https://t.me/learningnets

Connection Table

This topic describes the connection table.



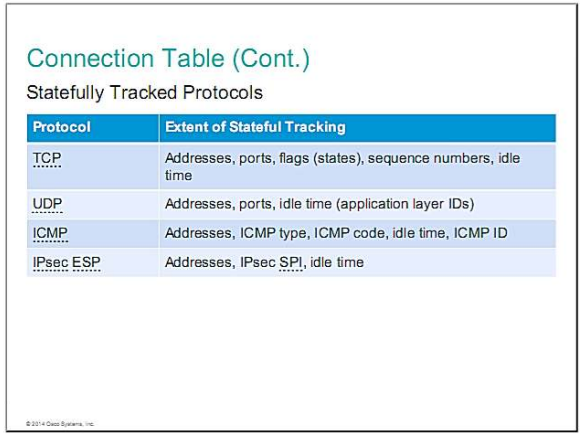
State tables on the Cisco Adaptive Security Appliance act as device short-term memory. In essence, the state tables describe the environment of the current device and the traffic it has seen in the past to predict correct future traffic.

In the connection table, the appliance tracks all connections that were permitted across the device. All packets of existing sessions that arrive at a security appliance interface must match the packet properties that are recorded in the connection table for that particular connection. If the packet belongs to an existing connection but does not match the expected properties, the Cisco ASA drops the packet.

Note	Packets that arrive at a security appliance interface and do not match any connection in the connection table are compared against the Cisco ASA access rules.

The connection table is constantly updated based on the properties of permitted packets. When a packet is permitted, the state table of the particular connection is adjusted based on the protocol that is involved.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



The Cisco ASA tracks various connection properties, depending on the transport protocol on which the connection is based. By default, the Cisco ASA security appliance statefully inspects TCP and UDP flows and automatically allows TCP and UDP return packets; however, the stateful inspection of ICMP and IPsec ESP is disabled by default.

TCP connections: The security appliance tracks a comprehensive set of connection parameters—the communicating IP addresses, the source and destination ports, the TCP state machine (so that it knows whether the connection is establishing, established, or closing), and the TCP sequence numbers in both directions. Additionally, by default for each new connection, the security appliance randomizes the sequence number of the host on the more secure interface (based on security levels). It also remembers the difference between the initial and randomized sequence numbers to adjust all subsequent packets accordingly. The security appliance also tracks the idle time of the connection to time out abandoned, dead connections. A TCP connection enters the connection table if the security policy of the appliance permits its initial synchronization SYN packet. If either connection endpoint closes the connection with a reset or if the hosts mutually close the connection using FIN packets, the connection is deleted from the connection table. A TCP flow that is idle for more than a configurable idle time is deleted from the connection table. The security appliance also supports half-closed flows. It uses a separate idle timer to delete flows that remain in the half-closed state for too long.

UDP flows: The security appliance tracks the IP addresses, the source and destination ports of the UDP flow, and the idle time since the last packet of the flow was seen by the security appliance. For select applications, the security appliance also tracks application request identifiers (such as the DNS request identifier) to further defend against packet spoofing attacks. A UDP flow enters the connection table if the appliance security policy permits it. A UDP flow that is idle for more than a configurable idle time is deleted from the connection table.

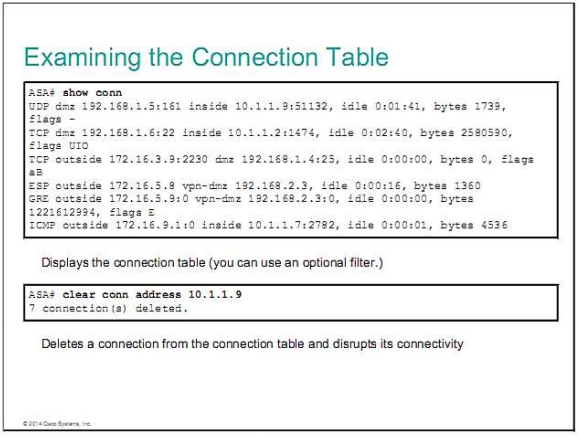
ICMP: The security appliance tracks IP addresses, ICMP type and code, the ICMP packet identifier, and the idle time of the request. A ping request enters the connection table if the appliance security policy permits it. When the ping target replies with an echo-reply, the ICMP entry is deleted from the connection table. A ping entry that is idle for more than a configurable idle time is deleted from the connection table. However, by default, the security appliance treats ICMP ping traffic statelessly. To permit echo-reply packets, you must allow the packets by using an ACL or you must enable ICMP inspection.

ESP tunnel flows through the Cisco ASA: The appliance tracks IP addresses and the security parameter index (SPI, the tunnel ID), and the idle time of the ESP tunnel session. An IPsec ESP session enters the connection table if the appliance security policy permits it. An IPsec ESP session that is idle for more than a configurable idle time is deleted from the connection table. By default, the security appliance treats ESP traffic statelessly. To enable the appliance to treat ESP statefully, you must enable IPsec inspection of pass-through traffic.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Examining the Connection Table

This topic describes how to examine and administer the connection table.

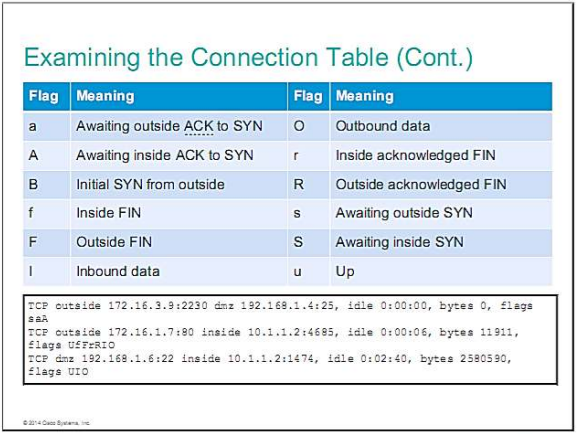


You can use the **show conn** command to examine the current contents of the connection table. The **show conn** command displays the number of active connections and information about each individual connection. In the figure, there are eight connections in the connection table, three of them based on TCP, two based on UDP, an ICMP ping entry, an IPsec ESP tunnel and a GRE.

For each entry, you can observe the involved Cisco Adaptive Security Appliance interfaces, IP addresses, ports (for TCP and UDP sessions), or session IDs (for GRE and ICMP sessions, where they are listed in the source port field), the current idle time, and the cumulative bytes that are transferred between the two endpoints. For TCP connections, you can also observe connection flags that indicate the state of the TCP state machine for that particular connection.

GRE traffic is allowed if the access rule permits it. The Cisco ASA does not statefully inspect GRE traffic.

You can use the **clear conn** command to delete a specific connection from the connection table. When you delete a TCP connection, the application using that connection will be disrupted and may not automatically recover. For other types of connections, such as UDP, applications will typically re-create their connection objects automatically. You can also use the **clear conn** command without any arguments to delete all connections from the connection table.



It is useful to analyze the flags of the entries in the TCP connection table because the flags can indicate various issues if you are troubleshooting connectivity. For example, a connection that is noted with the "saA" flags typically indicates that there is a routing problem or an unresponsive host on an interface with the lower security level. However, if most of the TCP connections have the "UIO" flags and a nonzero byte count, this typically indicates that the Cisco ASA is operating normally.

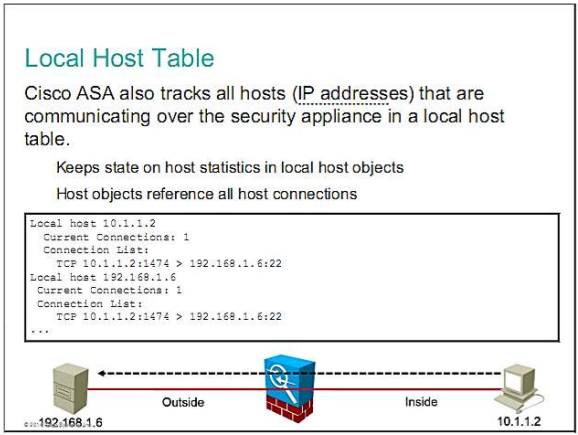
This figure shows three examples of connections with associated flags. The figure also explains flags that are associated with the TCP state engine. Other connection flags (also for other protocols) suggest application awareness and indicate that the security appliance is applying deeper inspection on these connections.

Connections that are initiated from an interface with a higher security level to an interface with a lower security level are outbound connections. Connections that are initiated from an interface with a lower security level to an interface with a higher security level are inbound connections. The "B" flag indicates that the connection is inbound.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Local Host Table

This topic describes local host table.

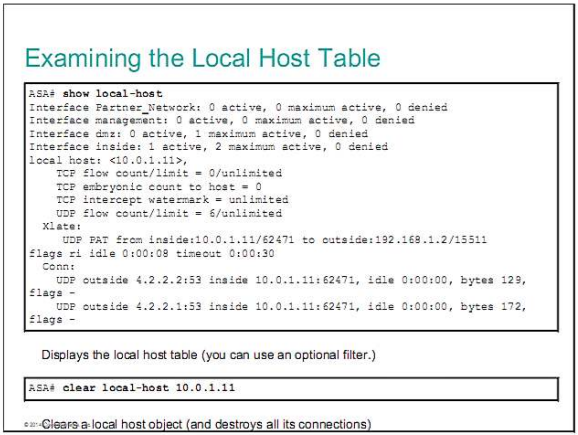


The Cisco Adaptive Security Appliance also keeps a second state table, which is referred to as the local host table. This table tracks all hosts (that is, IP addresses) that have connections that are established across the appliance. Each host is tracked in a local host object where the security appliance groups per-host statistics — xlates, connections, and AAA information. Each local host object references all connections that involve that particular host in the connection table. Therefore, by examining the local host table, you can also see the relevant portions of the connection table that are linked to the particular host (IP address).

In the figure, the inside 10.1.1.2 host initiates a SSH connection to the 192.168.1.6 outside host. These two hosts share an SSH connection. If the Cisco ASA allows this connection, it creates two local host objects (local host 10.1.1.2 and local host 192.168.1.6) and one connection object (TCP 10.1.1.2:1474 > 192.168.1.6:22) that is linked to both local host objects.

Examining the Local Host Table

This topic describes how to examine and administer the local host table.



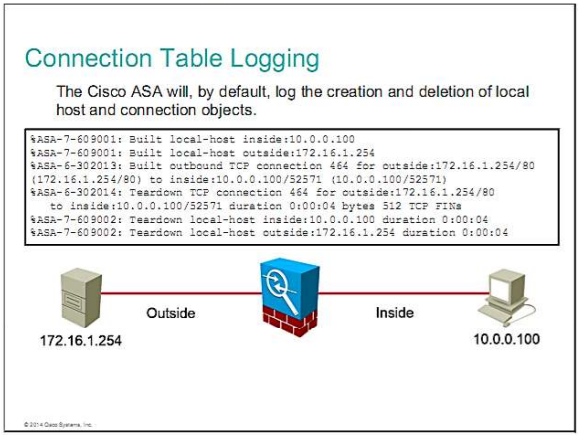
You can use the **show local-host** command to examine the local host state table. In the figure, the host 10.0.1.11 is shown with flow statistics, translations, and active connections.

You can use the command **clear local-host** to delete a specific local host object or a group of (or all) local host objects. When you delete a local host object, you also destroy all the connection objects that are associated with it, disrupting the current network applications of the host in question.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Connection Table Logging

This topic describes connection table logging.

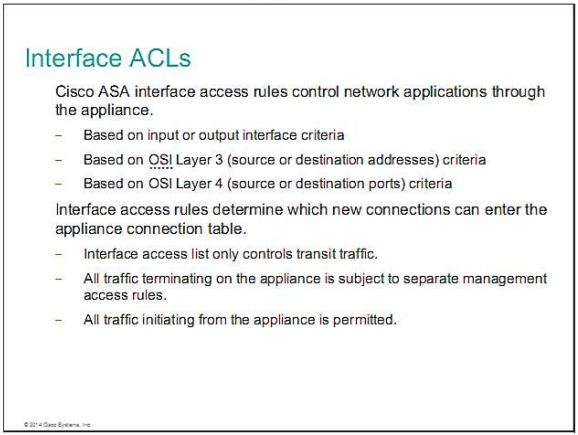


By default, when you enable system logging on the Cisco Adaptive Security Appliance, the appliance logs events that signal the creation and deletion of local host and connection objects. The security appliance logs creation and deletion events of local host objects at the debugging (7) level by default and the creation of and deletion of connection objects at the informational (6) level. The example output shows a sequence of state-change messages that the Cisco ASA generates for a short-lived connection.

In the example, a TCP (HTTP/Port 80) outbound connection is established between the 10.0.0.100 inside host and the 172.16.1.254 outside host. Before this connection could occur, two local host objects were created: one for the 10.0.0.100 host and one for the 172.16.1.254 host. The connection is torn down and the two local host objects are deleted.

Interface ACLs

This topic describes Cisco Adaptive Security Appliance interface ACLs.



Cisco ASA interface access rules are the most commonly used access control mechanism on the appliance. Interface access rules permit or do not allow (deny) network applications to establish their sessions through the security appliance based on the following information:

The input or output appliance interface of the session

OSI Layer 3 (source and destination IP address) criteria

OSI Layer 4 (source and destination port or service) criteria

Effectively, interface access rules determine which new connections can enter the Cisco ASA connection table. If a packet arrives at an appliance interface that does not belong to an existing connection, the Cisco ASA compares the packet to the interface access rules. If these rules permit the packet (that is, the network application), the connection that is initiated by this packet enters the connection table. If the packet is not permitted, the packet and its associated application session are denied.

Interface access rules control only transit traffic through the Cisco ASA—that is, traffic that terminates on a host beyond the appliance itself. Interface access rules do not control traffic that terminates on the security appliance itself, such as VPN tunnels, management protocols, or ICMP traffic to the appliance.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Interface ACLs (Cont.)

Interface access rules are per-interface ordered lists of permit and deny rules that are evaluated sequentially from the top.

- The rule that matches first is selected. The rules then stop matching further entries.
- There is an implicit deny-all rule at the end of the rules.
- The Cisco ASA interface access rules use netmasks instead of wildcards.

Action	Source Address	Destination Address	Service
Deny	10.1.1.0 255.255.255.0	192.168.1.0 255.255.255.0	Any
Permit	10.1.1.0 255.255.255.0	172.16.0.0 255.255.0.0	SSH
Permit	10.1.1.0 255.255.255.0	Any	HTTP
Deny	Any	Any	Any

© 2014 Cisco Systems, Inc.

Interface access rules are an ordered list of permit and deny rules that are applied to a particular Cisco ASA interface. Each appliance interface typically has its own separate set of interface access rules.

The ruleset is evaluated sequentially from the top and the rule that first matches the new connection is evaluated. The connection is then permitted or denied. When a rule matches a connection, all subsequent rules are ignored.

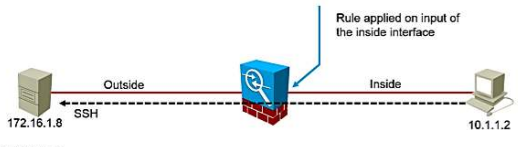
There is an implicit (invisible) deny-all rule at the end of the interface access rules list. Therefore, a new connection that does not match any of the rules is denied.

This example shows a simple set of interface access rules. The first rule denies the 10.1.1.0/24 network and does not allow it to make any connections to the 192.168.1.0/24 network. The next two rules allow the 10.1.1.0/24 network to make SSH connections to the 172.16.0.0/16 network and HTTP connections to any host. All other connections are implicitly denied. You can apply this set of interface access rules to connections that arrive to the most trusted interface of the security appliance from adjacent networks.

Interface ACLs (Cont.)

For all statefully managed protocols and applications, the Cisco ASA interface access rules only need to permit the initial packet of an application.

Action	Source Address	Destination Address	Service
PERMIT	10.1.1.0 255.255.255.0	172.16.0.0 255.255.0.0	SSH (TCP, source port = any, destination port = 22)



© 2014 Cisco Systems, Inc.

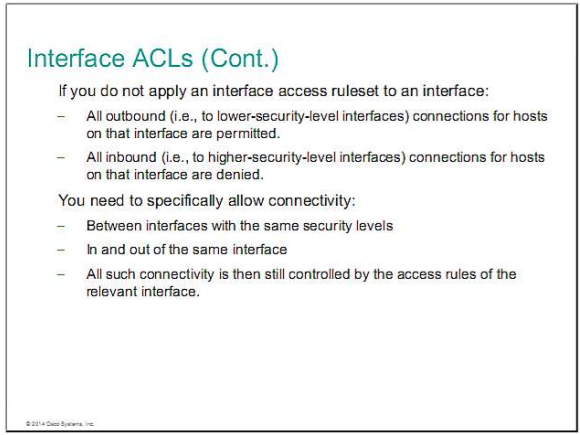
Because the Cisco ASA is a stateful packet-filtering device, its interface access rules rely on its statefulness to simplify rule creation. When you create interface access rules, you only need to permit the initial packet of a network application if the security appliance statefully inspects that application. Therefore, your interface access rules do not have to consider these conditions:

Any traffic flowing in the reverse direction of that connection: Because these packets belong to the same flow, the Cisco ASA automatically permits them if they match the properties that are expected from them by the connection table.

Any additional connections or flows that this application may establish: Because the Cisco ASA is application-aware, it automatically permits any additional connections of the same application session if you permit the initial packet of the session.

In the figure, the 10.1.1.2 host wants to establish an SSH session with the 172.16.1.8 host. As the initial SSH packet arrives at the Cisco ASA, the appliance compares this packet to its connection table and finds that it is a new connection. The packet is compared to the interface access rules that are applied to control sessions arriving on the inside interface. The rule that is shown in the example permits the connection, so the security appliance creates local host objects and a connection object. Now, the appliance permits all packets of this specific SSH session instance.

https://t.me/learningnets



However, applying interface ACLs on security appliance interfaces is optional. If you do not apply interface access rules to a specific interface, the appliance applies a default access policy:

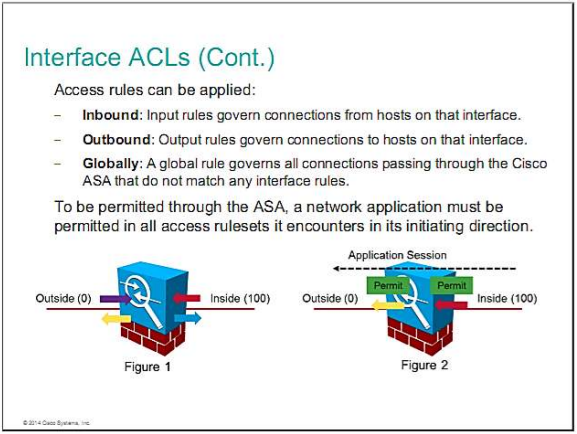
All connections arriving on the interface that are routed to interfaces with lower security levels than the incoming interface (outbound connections) are automatically permitted.

All connections arriving on the interface that are routed to interfaces with higher security levels than the incoming interface (inbound connections) are automatically denied.

Assigning the same security level to two interfaces often implies that you want to prevent any connectivity between the interfaces. By default, the Cisco ASA does not allow any application traffic to pass between interfaces with the same security level, even if interface access rules would allow the traffic. However, you can use the global configuration command **same-security-traffic permit** to globally enable communication between interfaces with the same security level. If you enable this communication, the traffic is allowed to flow between hosts on both interfaces without an access list. However, if there is already an access list on either interface, you must permit the required connections in relevant interface access rules.

Communication in and out of the same interface is often needed in certain VPN scenarios. By default, the Cisco ASA denies such communication. If needed, communication of the same security level in and out of the same interface can be enabled by using a global configuration command that is discussed in the interface configuration lesson. If you enable communication between hosts on the same interface, the traffic is allowed to flow between hosts without an access list. However, if there is already an access list present on the interface, you must permit the required connections in relevant interface access rules.

https://t.me/learningnets



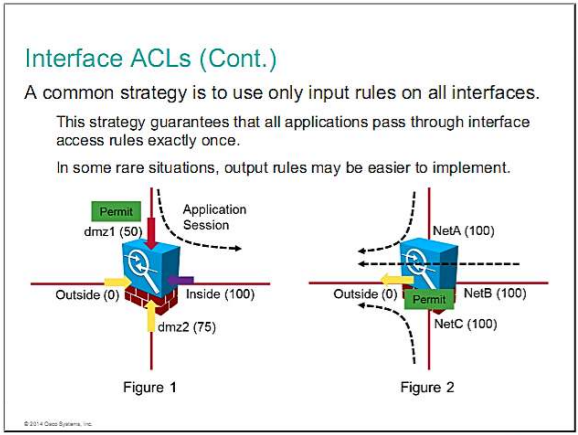
You can apply interface access rules on the input or output direction of a Cisco ASA interface. You can also optionally apply a global access rule. You can use a global access rule to control access to all interfaces on the security appliance only in the input direction.

Interface access rules that you apply on the input of the interface control the connections that the security appliance accepts from hosts on that interface. Interface access rules that are applied on the output of the interface control the connections that are about to be forwarded to hosts on that interface. The global access rule, if configured, applies to all traffic that does not match any interface access rules.

In Figure 1, an appliance is using four sets of interface access rules. The red and purple arrows (the two top arrows) represent access rules that are applied on the input of the outside and inside interfaces. The blue and yellow arrows (the two bottom arrows) represent access rules that are applied on the output of the outside and inside interfaces. This configuration is not a representative or common security appliance configuration; it is an illustration of one possibility of interface access rule deployment.

When a network application requires access through the Cisco ASA , you must permit it in all access rules that are applied in the direction of the session across the appliance. In Figure 2, an application session is initiated from a host on the inside interface to a host on the outside interface. For this session to be permitted through the security appliance, you would have to permit it in the input interface access rules on the inside interface and in the output interface access rules on the outside interface, if both of these rules are configured on the appliance.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

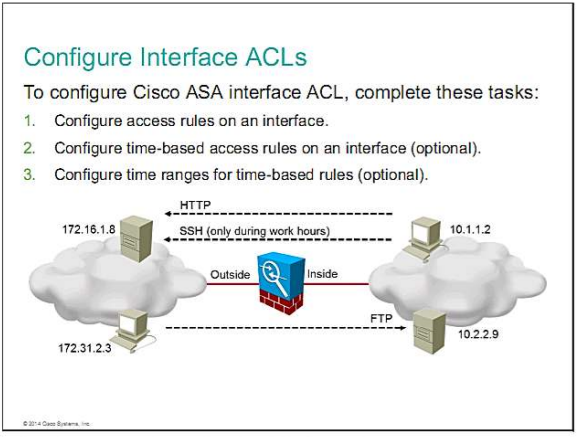


To simplify the Cisco ASA configuration, you can use only input interface access rules and apply a separate set of input interface rules to each appliance interface, covering all interfaces. This configuration philosophy guarantees that each network application that passes through the Cisco ASA does so through exactly one set of input interface rules on its incoming interface. In Figure 1, the security appliance is configured with four sets of interface access rules, each of which is applied on the input of a particular interface. When an application initiates from a host on the dmz1 interface, it must be permitted only by the input interface access rules on the dmz1 interface.

In rare situations, it may be helpful to also use output interface access rules. In Figure 2, the Cisco ASA is configured with four interfaces, three of which have a security level of 100 and are therefore isolated by default. If the requirement is to configure an access rule that permits only certain applications between hosts on these three high-security-level interfaces to communicate with hosts on the fourth low-security-level interface, it is simpler to apply a single set of interface access rules on the output of the fourth interface (the Outside interface in the example).

Configure Interface ACLs

This topic describes how to configure interface ACLs.



To configure interface access rules, perform the following tasks:

1. Configure access rules on the interface by specifying each individual rule in the ruleset.
2. Optionally, if you plan to use time-based rules, configure time ranges.
3. Optionally, if you plan to use time-based rules, configure access rules that use the configured time ranges.

This figure shows the scenario that the configuration tasks of this topic use. The Cisco Adaptive Security Appliance controls traffic between an internal enterprise network that is connected over the inside interface and an external network that is connected over the outside interface.

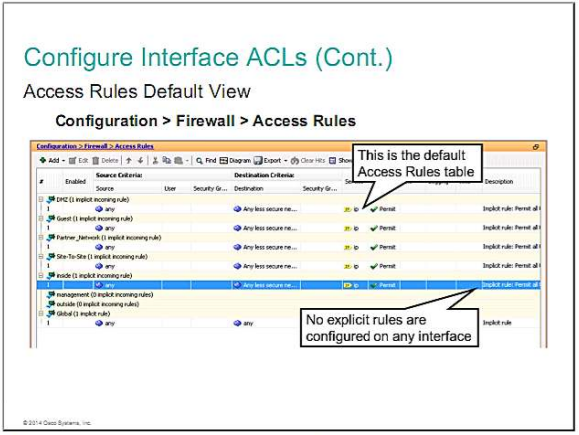
For this configuration scenario, the Cisco ASA should enforce the following access policy:

The internal client (10.1.1.2) should have permanent HTTP access to the 172.16.1.8 external server.

The internal client (10.1.1.2) should have SSH access to the 172.16.1.8 external server, but only during work hours (every weekday from 8 a.m. to 5 p.m. [8:00 to 17:00]).

The external client (172.31.2.3) should have permanent FTP access to an internal server (10.2.2.9).

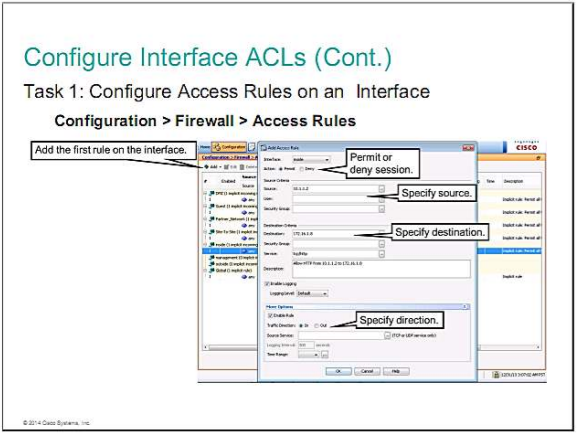
© 2014 Cisco Systems, Inc.
https://t.me/learningnets



The Cisco Adaptive Security Device Manager Access Rules table is a consolidated view of all interface access rules that are configured and applied on the security appliance interfaces. To access the Access Rules table, choose **Configuration > Firewall > Access Rules**.

This figure shows the default view of the Access Rules table on a Cisco ASA that does not have any explicit interface access rules or any explicit global access rules configured. With no explicit rules, the security appliance permits all connections that arrive to an interface, if these connections are routed to interfaces with lower security levels. This behavior is indicated by the implicit permit incoming rule on the DMZ and inside interfaces as shown in the figure. Interface-specific access rules are evaluated before the global access rules.

The figure also shows that there are no separate ACLs for IPv4 and IPv6. The ASA supports unified ACLs for IPv4 and IPv6 from Cisco ASA Software 9.0(1), where you can create IPv4 and IPv6 ACL entries in a single ACL, or you can even mix IPv4 and IPv6 addresses in a single ACL entry. Prior to the Cisco ASA Software 9.0(1), IPv4 and IPv6 ACLs were configured separately.



Task 1 implements the first interface access rule, which allows the internal client (10.1.1.2) to access the external server (172.16.1.8) using HTTP. When no explicit rules are configured on a Cisco ASA security appliance interface, you must add the initial rule to the interface.

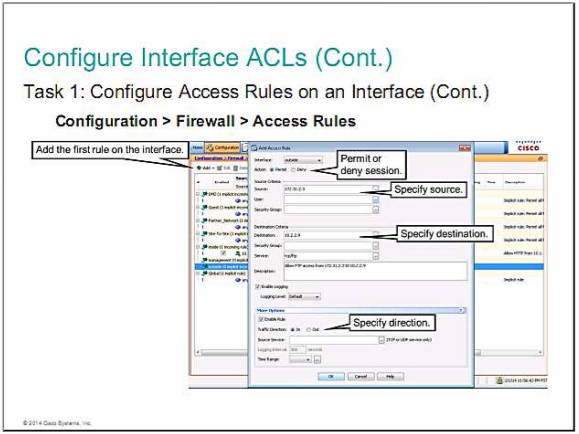
Note Cisco ASDM allows you to add or insert rules to the set of interface access rules. The Add function appends a new rule to the end of the ruleset and the Insert function inserts a rule in a particular position inside the ruleset. If no rules have been configured on an interface, you must add the first rule, and the insert option is dimmed.

Follow these steps to add this access rule:

1. From Cisco ASDM, choose **Configuration > Firewall > Access Rules**. The Access Rules panel appears.
2. Click **Add** and choose **Add Access Rule** from the menu. The Add Access Rule window appears.
3. Verify that the interface to which the rule will be added is the inside interface.
4. Choose the action that applies to the rule by clicking the **Permit** or **Deny** radio button. In the example, **Permit** is chosen.
5. In the Source field, enter the IP address from which traffic is permitted or denied. You can also click the ellipsis (**...**) button to choose an address from a predefined list. To specify a host address, you can enter /32 for the subnet mask or you can enter the IP address without a subnet mask. To specify a network address, enter the subnet mask in slash notation after the IP address. In the example, 10.1.1.2 is the source address.
6. In the Destination field, enter the IP address to which traffic is permitted or denied. You can also click the ellipsis (**...**) button to choose an address from a predefined list. To specify a host address, you can enter /32 for the subnet mask or you can enter the IP address without a subnet mask. To specify a network address, enter the subnet mask in slash notation after the IP address. In the example, 172.16.1.8 is the destination address.
7. Specify the service or protocol for the rule in the Service field. You can also click the ellipsis (**...**) button to choose a service from a predefined list. In the figure, TCP/HTTP is entered.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

8. Optionally, you can enter a description about the access rule.
9. Optionally, you can disable the logging function, which is enabled by default.
10. Expand the **More Options** section to configure additional settings for the rule.
11. Verify that the **Enable Rule** check box is checked (which is the default).
12. Verify that the Traffic Direction **In** radio button is clicked (which is the default). You can apply only one set of access rules to each direction of an interface. This rule belongs to the input set of rules on the inside interface.
13. Click **OK** to close the Add Access Rule window, and click **Apply** in the Access Rules panel.



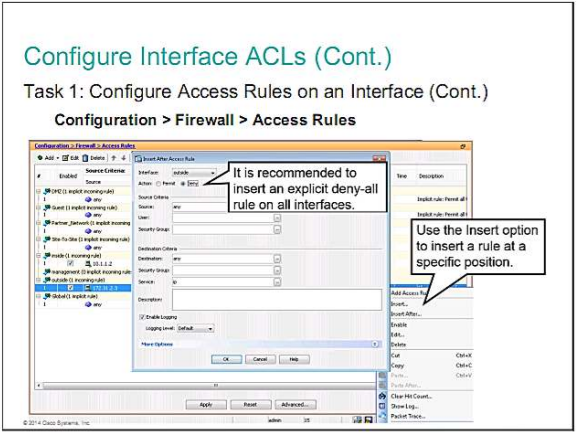
In the second part of Task 1, create an access rule on the outside interface to permit inbound FTP connectivity from the external client (172.31.2.3) to the internal FTP server (10.2.2.9). Follow these steps to configure this access rule:

Follow these steps to add this access rule:

1. From Cisco ASDM, choose **Configuration > Firewall > Access Rules**. The Access Rules panel appears.
2. Click **Add** and choose **Add Access Rule** from the menu. The Add Access Rule window appears.
3. Verify that the interface to which the rule will be added is the outside interface.
4. To choose the action that applies to the rule, click the **Permit** or **Deny** radio button. In the example, Permit is chosen.
5. In the Source field, enter the IP address of the external client. In the example, 172.31.2.3 is the source address.
6. In the Destination field, enter the IP address of the internal server. In the example, 10.2.2.9 is the destination address, and it is not being translated.
7. Specify the service or protocol for the rule in the Service field. You can also click the ellipsis (**...**) button to choose a service from a predefined list. In the figure, TCP/FTP is entered.

https://t.me/learningnets

8. Optionally, you can enter a description about the access rule and you can disable the logging function, which is enabled by default.
9. Expand the **More Options** section to configure additional settings for the rule.
10. Verify that the **Enable Rule** check box is checked (which is the default).
11. Verify that the Traffic Direction In radio button is clicked. This choice causes the rule to belong to the input set of rules on the outside interface (which is the default
12. Click **OK** to close the Add Access Rule window, and click **Apply** in the Access Rules panel.



To complete the configuration part of the first task, insert explicit deny-all rules at the end of all interface access rulesets. This configuration is optional, but recommended, because it allows you to track the number of denied packets. The explicit deny-all rule is needed to monitor hit-count statistics.

To create the explicit deny-all rule in Cisco ASDM, use the Insert function that creates a new rule in a particular location inside a ruleset. From the list of rules, choose the rule before or after which you want to insert a new rule. To insert a new rule before the selected rule, choose **Insert** from the Add drop-down list. The Insert Access Rule window appears. To insert a new rule after the selected rule, choose **Insert After** from the Add drop-down list. The Insert After Access Rule window appears.

Follow these steps to create the explicit deny-all rule on the inside interface:

1. From Cisco ASDM, choose **Configuration > Firewall > Access Rules**. The Access Rules panel appears.
2. Choose and right-click the last explicit rule on the inside interface. Choose **Insert After** from the pop-up menu. The Insert After Access Rule window appears.
3. Complete the Insert After Access Rule window using the following values:

   Verify that the interface to which the rule will be applied is the outside interface.

   Action: **Deny**.

   Source: **any** (indicates all possible addresses)

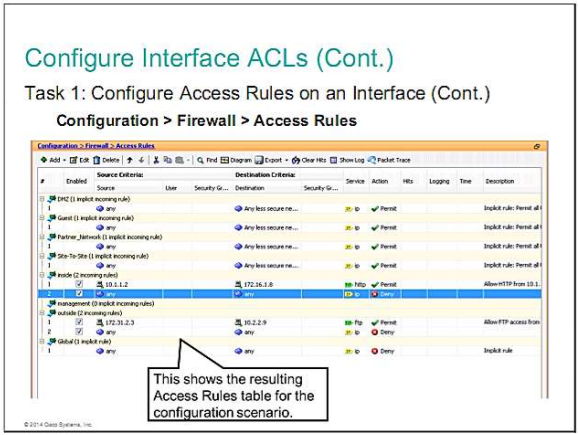
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Destination: **any** (indicates all possible addresses)

Service: **ip** (indicates all possible IP-based services)

4. Optionally, you can enter a description about the access rule and you can disable the logging function, which is enabled by default.
5. Expand the **More Options** section to configure additional settings for the rule (not shown in the figure).
6. Verify that the **Enable Rule** check box is checked, which is the default (not shown in the figure).
7. Verify that the Traffic Direction In radio button is clicked, which is the default (not shown in the figure).
8. Click **OK** to close the Add Access Rule window, and click **Apply** in the Access Rules panel.

Repeat these steps to create an explicit deny-all rule on the outside interface.

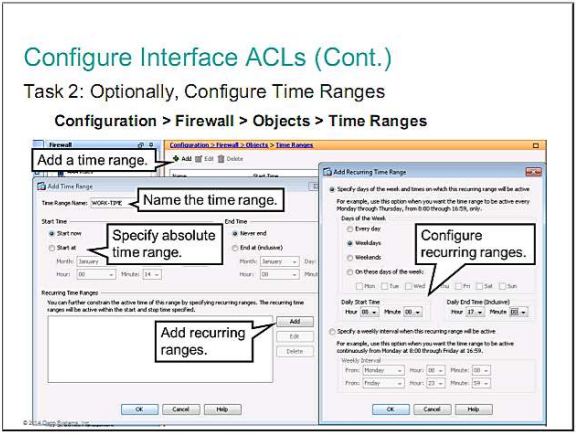


This figure shows the resulting interface access rules that appear after you complete Task 1.

A set of interface access rules on the inside interface, permitting a specific outbound HTTP session and explicitly denying all other traffic, has been added.

The implicit interface access rule that permits all inside IPv4 traffic to the lower-security-level interfaces has been removed.

A set of interface access rules on the outside interface, permitting a specific inbound FTP session and explicitly denying all other traffic has been added.

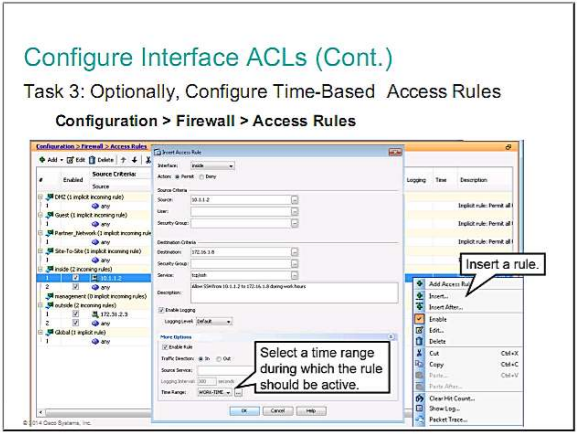


In Tasks 2 and 3, add a time-based access rule to your ruleset to implement the time-based requirement of the access policy. For Task 2, create a time range that specifies when the time-based access rule is active. For the configuration scenario of this topic, create a time range that activates the access rule on weekdays from 8 a.m. to 5 p.m. (8:00 to 17:00).

Follow these steps to create a time range:

1. From Cisco ASDM, choose **Configuration > Firewall > Objects > Time Ranges**.
2. Click **Add** to add a new time range. The Add Time Range window appears.
3. In the Add Time Range window, enter a name for the time range (WORK-TIME is used in the example), and, optionally, specify absolute time boundaries that apply to this range (for example, a starting data and an ending date). Because you are creating a recurring time range without absolute boundaries, choose the **Start Now** and **Never End** boundaries.
4. You can optionally specify one or more recurring time ranges inside the absolute time interval that was defined in the previous step. To create a recurring time range, click **Add** in the Add Time Range window. The Add Recurring Time Range window appears
5. Complete the fields in the Add Recurring Time Range window and click **OK**. The example in the figure creates a time range that is active on weekdays from 8 a.m. to 5 p.m. (08:00 to 17:00).
6. Click **OK** to close the Add Recurring Time Range window.
7. Click **OK** to close the Add Time Range window.
8. Click **Apply** to apply the configuration.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



In Task 3, apply the created time range to a newly created access rule in the ruleset. In this scenario, you must configure a time-based rule that allows the internal client (10.1.1.2) to access the external server (172.16.1.8) using SSH only during the configured time range.

Follow these steps to create a time-based rule

1. From Cisco ASDM, choose **Configuration > Firewall > Access Rules**. The Access Rules panel appears.
2. Click a rule in the existing ruleset before which or after which you want to add the time-based rule. In this configuration scenario, you need to permit outbound connectivity from the internal network; therefore, you must add an input permit rule before the explicit deny-all rule on the inside interface. Right-click the explicit deny-all rule on the inside interface, and choose **Insert** from the pop-up menu.
3. The Insert Access Rule window appears. Enter the following values in this window:

   Verify that the interface to which the rule will be applied is the inside interface.

   Action: **Permit**

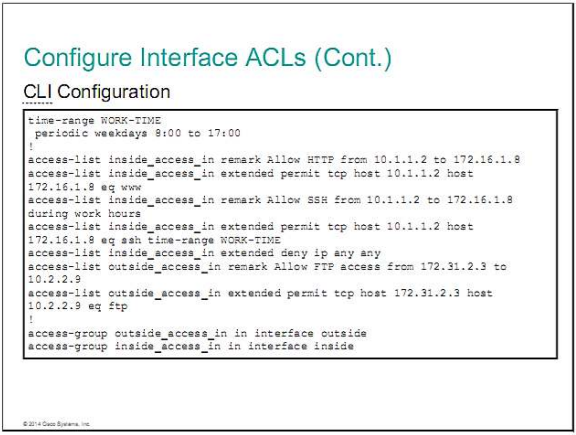
   Source: 10.1.1.2

   Destination: 172.16.1.8

   Service: TCP/SSH
4. Optionally, you can enter a description about the access rule and you can disable the logging function, which is enabled by default.
5. Expand the **More Options** section to configure additional settings for the rule (not shown in the figure).
6. Verify that the **Enable Rule** check box is checked, which is the default (not shown in the figure).
7. In the Time Range field, click the ellipsis (**…**) button and choose the time range that was defined in the previous task (WORK-TIME in the example). This rule is active only when the time range is active (that is, when the security appliance local time matches the conditions that are defined inside the time range object).

https://t.me/learningnets

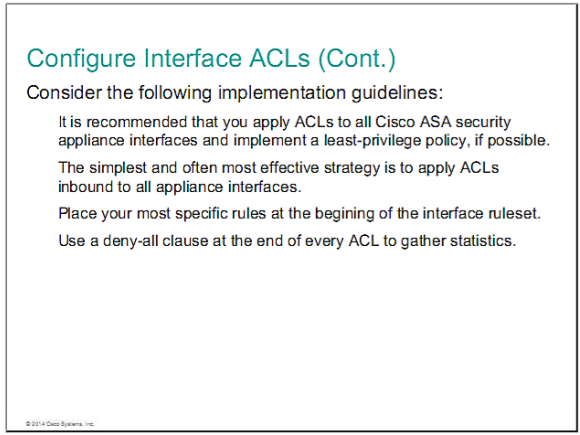
8. Click **OK** to close the Add Access Rule window, and click **Apply** in the Access Rules panel.



To configure interface ACLs on the Cisco ASA device using command line interface, use the commands that are described in the table.

Commands	Description
time-range WORK-TIME **periodic weekdays 8:00 to 17:00**	Creates a recurring time range
access-list inside_access_in remark Allow HTTP from 10.1.1.2 to 172.16.1.8 **access-list inside_access_in extended permit tcp host 10.1.1.2 host 172.16.1.8 eq www** **access-list inside_access_in remark Allow SSH from 10.1.1.2 to 172.16.1.8 during work hours** **access-list inside_access_in extended permit tcp host 10.1.1.2 host 172.16.1.8 eq ssh time-range WORK-TIME** **access-list inside_access_in extended deny ip any any**	Creates an ACL
access-list outside_access_in remark Allow FTP access from 172.31.2.3 to 10.2.2.9 **access-list outside_access_in extended permit tcp host 172.31.2.3 host 10.2.2.9 eq ftp**	Creates an ACL
access-group outside_access_in in interface outside **access-group inside_access_in in interface inside**	Applies ACLs to interfaces in inbound direction

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



When you implement access control on the Cisco ASA security appliance using interface ACLs, consider the following implementation guidelines:

Consider applying interface access rules on all interfaces and permitting only the minimal required set of services. This approach enforces a minimal access policy, which can be effective in preventing both known and yet-unknown attacks. Some organizations may configure the Cisco ASA security appliance in a more relaxed manner to increase manageability, if the number of rules would otherwise be too high. Configurations of this type generally increase the risk to which endpoints are exposed.

Generally, the simplest and most effective strategy is to use only input interface access rules that are applied to all security appliance interfaces. This approach guarantees that every connection always passes through one set of interface access rules. It also prevents rule duplication on multiple interfaces.

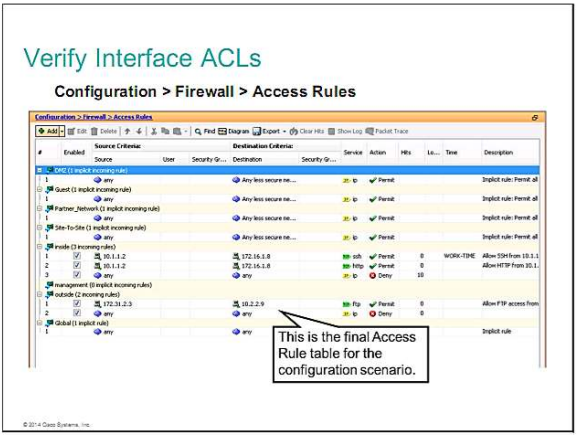
As with any sequential rulesets, it is recommended that you place your most-specific rules (that is, rules that govern specific hosts or services) toward the top of the ruleset to avoid overriding them with more-general rules.

In all interface access rules, it is recommended that you add an explicit deny-all statement at the end of the list to gather statistics on traffic that is denied and to observe which traffic is being denied by this specific catch-all rule.

The Cisco ASA security appliance has no hard-coded limit on the number of elements (ACEs) in an ACL. The limit is based on the amount of memory that is available on the security appliance. Use the **show access-list include elements** command to see how many ACEs are on the security appliance.

Verify Interface ACLs

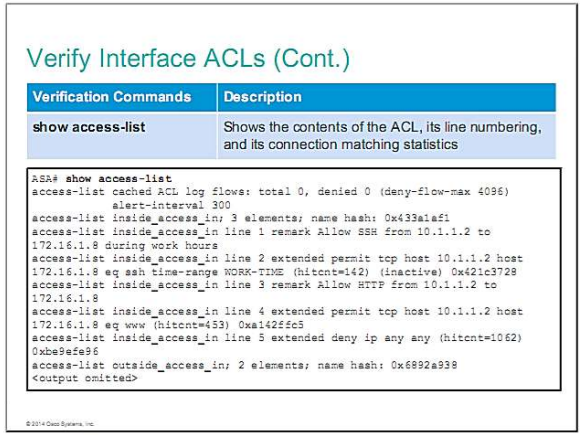
This topic describes how to verify interface ACLs.



This figure shows the final Cisco Adaptive Security Appliance Access Rules table and the corresponding interface access rules that implement the desired policy. The Hits field is automatically updated to show the number of times that traffic has matched a particular rule.

Note Traffic only matches a rule for each new connection or session; it does not match a rule on a per-packet basis.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



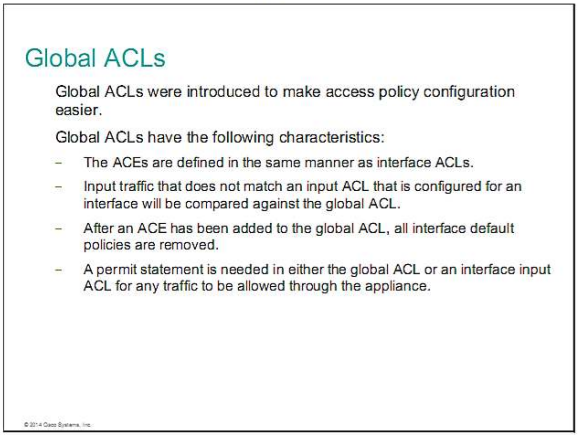
Use the **show access-list** command to view configured ACLs. The **show access-list** command lists all of the configured ACLs, the ACEs for each ACL, hit counts for each ACE, and a unique hexadecimal identifier (hash) for each ACE. You can use this number to match the ACE that appears in the syslog output.

In the figure, the **show access-list** command is used with the argument of an ACL name, so it displays only the outside_access_in ACL. There are two ACEs in this ACL; one is a remark (description) and one is a traffic-controlling permit ACE.

Notice that the **access-list** commands in the figure are listed by ACL line number. The line number that appears with **show access-list** is optional when the ACL is configured from the command line. If you do not specify the line number when you enter the **access-list** command, the line number is assigned by the operating system and placed at the end of the ACL. Each individual ACE is given a unique line number within an ACL.

Global ACLs

This topic describes Cisco Adaptive Security Appliance global ACLs.



The global ACLs of Cisco ASA make it easier to manage the access policy configuration.

After you define a global ACL policy, all the default interface implicit access policies (which permit traffic from high-security-level interfaces to low-security-level interfaces) are removed, and the global policy is used for all input traffic. If you want to define specific interface access policies that differ from the global policy, you must configure interface ACLs.

You add ACEs to the global ACL in the same way that you add ACEs to interface ACLs. The global ACL is checked only when the manually configured input interface ACLs do not find a match for the input packet. Interface ACLs are always matched before the global ACL.

The Cisco ASA uses the following order to match access rules when only interface ACLs are configured:

1. Interface access list rules
2. Implicit deny ip any any interface access list rule

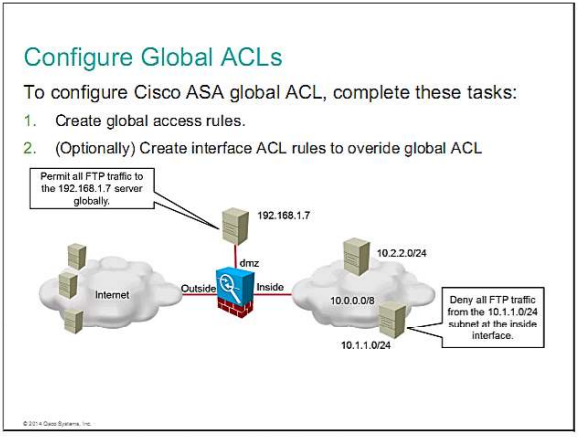
The Cisco ASA uses the following order to match access rules when both interface ACLs and the global ACL are configured:

1. Interface access list rules
2. Global access list rules
3. Implicit deny IP any any global access list rule

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Configure Global ACLs

This topic describes how to configure global ACLs.



To configure global access rules, perform the following tasks:

1. Create global access list rules.
2. Optionally create an interface ACL to override permissions in the global ACL.

In this configuration scenario, you will simplify the access policy configuration by using a global ACL with an interface ACL. You will apply a global ACL statement that allows FTP from all hosts to the FTP server at 192.168.1.7. By using a global ACL, you will not need to put specific rules on the outside or inside interfaces to permit this traffic.

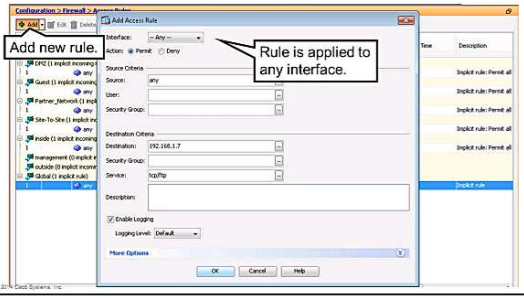
You will also apply an ACE to the input ACL on the inside interface to block all FTP traffic from the 10.1.1.0/24 subnet, which preempts the global ACL for only that specific traffic.

Allow all other traffic from the inside interface to the DMZ interface and the outside interface.

Configure Global ACLs (Cont.)

Task 1: Create Global Access Rules

Configuration > Firewall > Access Rules



The first task of this case study configuration is to implement the first global access rule. This global access rule should allow any client to access the server (192.168.1.7) using FTP. When no explicit global access rules are configured on a Cisco ASA security appliance, you must add the initial rule to the global access rule.

Follow these steps to add the first access rule:

1. From Cisco Adaptive Security Device Manager, choose **Configuration > Firewall > Access Rules**. The Access Rules panel appears.
2. Select the global implicit rule, click **Add** and choose **Add Access Rule** from the menu. The Add Access Rule window appears.
3. Enter the following values to complete the Add Access Rule window:

   Interface: **Any** (Interface = Any means that the ACE is part of the global access rule)

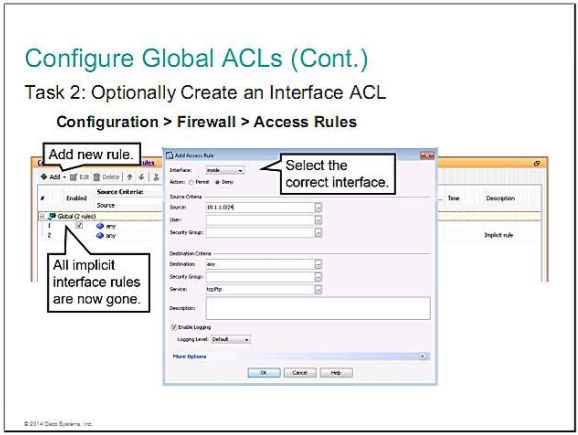
   Action: **Permit**

   Source: **any**

   Destination: **192.168.1.7**

   Service: **tcp/ftp** (You can also click the ellipsis (**...**) button to choose a service from a predefined list.)
4. Click **OK** to close the Add Access Rule window, and click **Apply** in the Access Rules panel.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



The second task is to implement the first inside access rule, which should deny any client from the network 10.1.1.0/24 from accessing FTP from the inside interface. When you configure a global access rule, all the default interface policies are removed (permit traffic from high security level to low security level) so you must create the interface access policy for the inside interface. The ASDM Access Rules pane in the figure shows the result of configuring a global access rule.

Follow these steps to add this interface access rule:

1. From the **Configuration > Firewall > Access Rules** window, click **Add Access Rule**. The Add Access Rule window appears
2. Click **Add** and choose **Add Access Rule** from the menu. The Add Access Rule window appears.
3. Enter the following values to complete the Add Access Rule window:

   Interface: **inside**

   Action: **Deny**

   Source: **10.1.1.0/24**

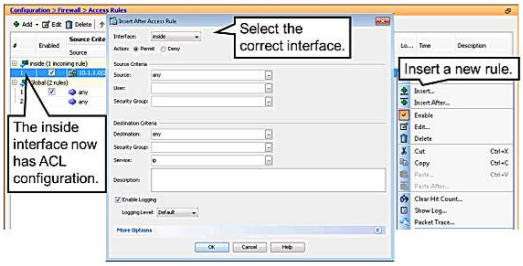
   Destination: **any**

   Service: **ftp** (You can also click the ellipsis (**...**) button to choose a service from a predefined list.)
4. Click **OK** to close the Add Access Rule window, and click **Apply** in the Access Rules panel.

Configure Global ACLs (Cont.)

Task 2: Optionally Create an Interface ACL (Cont.)

Configuration > Firewall > Access Rules



In the second part of the second task in this configuration scenario, you have to implement the second inside access rule, which should permit all other traffic from the inside interface. This task is very important; without this ACE, all other input traffic to the inside interface is denied because of the implicit deny any any global access rule.

Configure Global ACLs (Cont.)

CLI Configuration

```
access-list inside_access_in line 1 extended deny tcp 10.1.1.0 255.255.255.0
any eq ftp
access-list inside_access_in line 2 extended permit ip any any
access-list global_access line 1 extended permit tcp any host 192.168.1.7 eq
ftp
!
access-group inside_access_in in interface inside
access-group global_access global
```

To configure global interface ACLs on the Cisco ASA device using command line interface, use the commands that are described in the table.

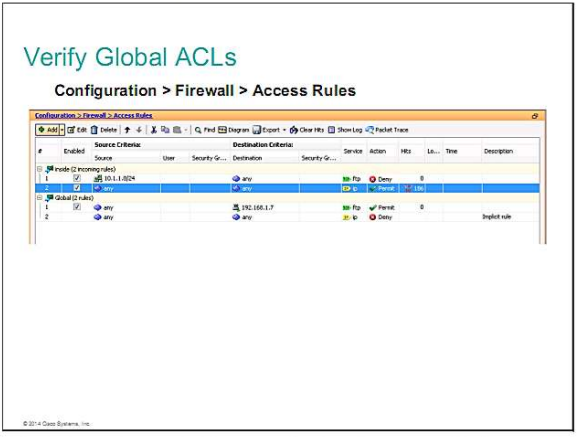
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Commands	Description
access-list inside_access_in line 1 extended deny tcp 10.1.1.0 255.255.255.0 any eq ftp **access-list inside_access_in line 2 extended permit ip any any**	Creates an ACL.
access-list global_access line 1 extended permit tcp any host 192.168.1.7 eq ftp	Creates an ACL.
access-group inside_access_in in interface inside	Applies the ACL to the inside interface.
access-group global_access global	Applies the ACL globally.

https://t.me/learningnets

Verify Global ACLs

This topic describes how to verify global ACLs.



The example in the figure shows a global access policy that allows FTP traffic from anywhere to the server at 192.168.1.7. The example also shows an interface-specific input access policy that denies FTP traffic from the 10.1.1.0/24 subnet, but allows all other traffic. Based on this configuration, the following traffic access policies are applied:

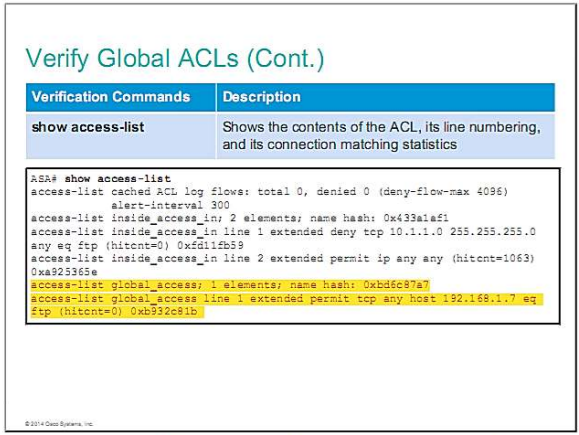
Traffic entering the Cisco Adaptive Security Appliance on the inside interface sourcing from subnet 10.1.1.0/24 with any FTP destination is denied.

All other traffic entering the Cisco ASA on the inside interface is allowed.

Any FTP traffic entering the Cisco ASA on any interface with a destination address of 192.168.1.7 is permitted.

All other traffic is dropped.

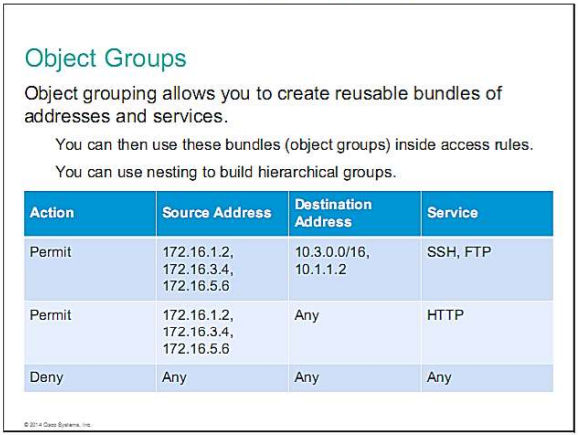
© 2014 Cisco Systems, Inc.
https://t.me/learningnets



Similarly as with the interface ACLs, you can use the **show access-list** command to display content and statistics for the global ACL.

Object Groups

This topic describes Cisco Adaptive Security Appliance object groups.



A set of interface access rules can cause the Cisco Adaptive Security Appliance to permit or deny a designated host to access another particular host with a specific network application (service). When there is only one client, one host, and one service, you need only a minimum number of lines in an interface rule set. However, as the number of clients, servers, and services increases, the number of rules that you need for each individual access type can increase and become unmanageable.

One solution for this problem is to group specific hosts into networks (subnets) and to allow entire networks to access resources. You can also allow complete TCP, UDP, or IP connectivity between hosts, instead of specifying individual services. This approach is suboptimal because it departs from the philosophy of minimal access, which increases risk while allowing unnecessary connectivity.

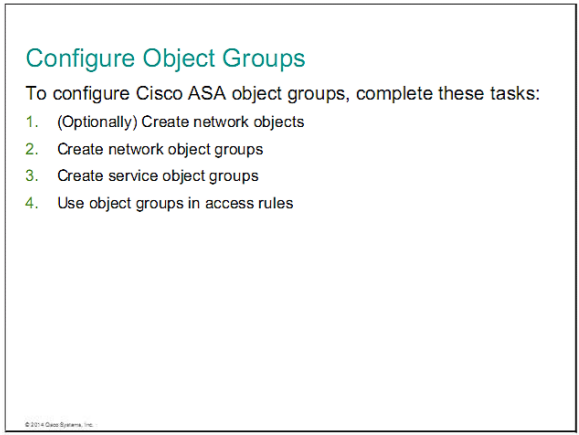
A better approach is to introduce object grouping. This solution allows you to arbitrarily group hosts, resources, or services that share the same policy, which optimizes the access rules.

In the table, hosts 172.16.1.2, 172.16.3.4, and 172.16.5.6 are granted SSH and FTP access to host 10.1.1.2 and the 10.3.0.0/16 network. Normally, 12 individual interface access rules would be required to specify this policy, listing individual hosts and policies. However, if these hosts are grouped as a source group, a destination group, and a service group, only a single access rule is required to reference the three groups.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

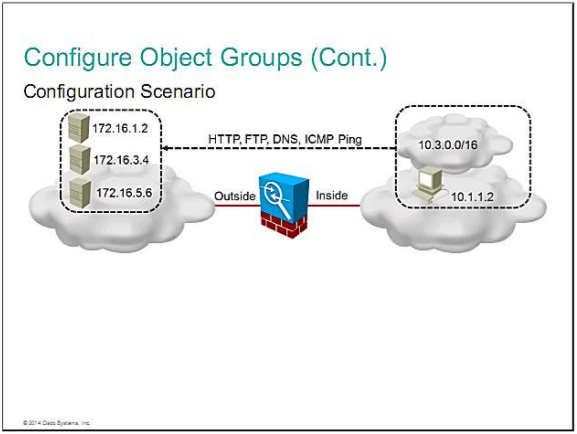
Configure Object Groups

This topic describes how to configure object groups on the Cisco Adaptive Security Appliance.



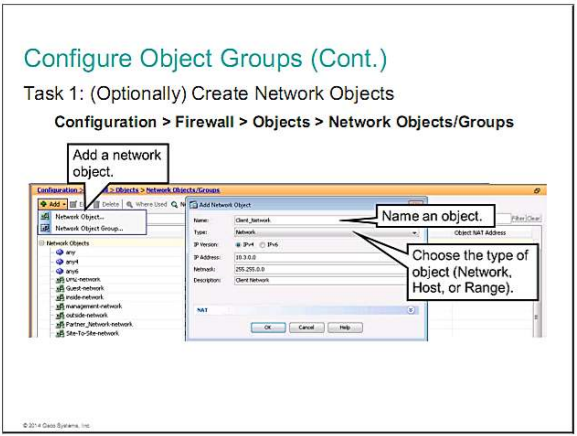
Complete these optional tasks to create objects and object groups, and to use them in your configuration:

1. Create individual network objects (host, network, or network range) and assign them a name. This task is optional and is used only to increase the readability of your configuration. If you would rather use raw IP addresses to visualize your policy, you can bypass this task. These network objects are also used in the NAT configuration to define translated hosts.
2. Create groups of hosts that will share a common access rule by defining the members of a network object group.
3. Create groups of services that will share a common access rule by defining the members of a service object group.
4. Apply the object group in specific interface access rules. You can use object groups as access rule parameters, including source, destination, and service.



This figure presents the configuration scenario that is used in upcoming configuration tasks. The security appliance controls traffic between an internal enterprise network that is connected over the inside interface and an external network that is connected over the outside interface.

The Cisco ASA should enforce the following access policy: An internal client (10.1.1.2) and an internal subnet (10.3.0.0/16) should both have permanent HTTP, FTP, DNS, and ICMP ping access to a group of external servers (172.16.1.2, 172.16.3.4, and 172.16.5.6).



In the optional Task 1, create user-friendly names and descriptions for the network object.

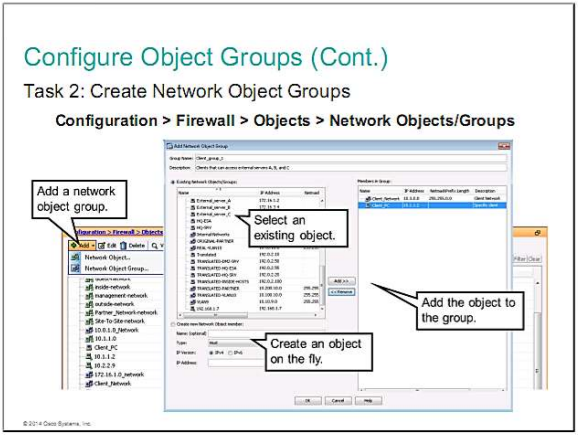
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Follow these steps to create a named network object using Cisco Adaptive Security Device Manager:

1. Navigate to **Configuration > Firewall > Objects > Network Objects/Groups** to administer network objects.
2. To add a new named network object, click the **Add** button and choose **Network Object**. The Add Network Object window appears.
3. In the Add Network Object window, enter a name for the object (the name cannot contain spaces), choose network object type from the Type drop-down list (Network in the example), and enter the IP address, IP subnet, or IP address range that the network object represents. You can also add a user-friendly description of the object.
4. Click **OK** to close the Add Network Object window.
5. Click **Apply** to apply the configuration.

In the figure, a network object named Client_Network is created that references the 10.3.0.0/16 internal network.

Repeat these steps to configure additional network objects if needed.



This figure shows five custom network objects that were added for the policy for this configuration example (Client_Network, Client_PC, External_server_A, External_server_B, and External_server_C).

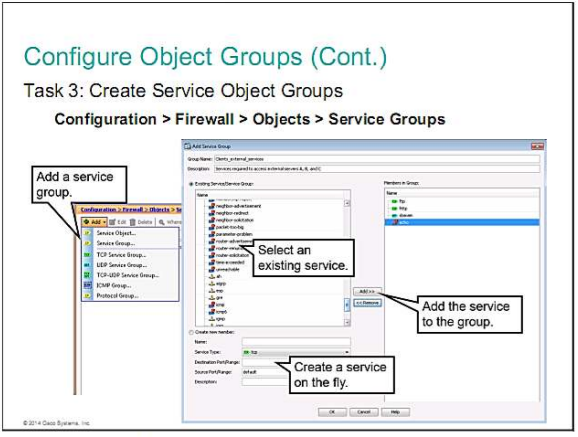
In Task 2, create network object groups to group hosts (raw IP addresses or subnets, or named network objects that were created in the previous task) that share the same access rule, either as a source or a destination condition.

Follow these steps to configure a network object group from Cisco ASDM:

1. Navigate to **Configuration > Firewall > Objects > Network Objects/Groups** to administer network objects.
2. To add a new network object group, click the **Add** button and choose **Network Object Group**. The Add Network Object Group window appears.

3. Enter a name for the group in the Group Name field. The group name can be up to 64 characters in length. The name must be unique for each object group. A network object group name cannot share a name with a service object group. In the figure, the network object group is named **Client_group_1**.
4. From the Existing Network Objects/Groups list, click the object that you want to add to the group. Click **Add**. If a named object or address that you want to add is not in the list, click the **Create New Network Object Member** radio button to create an object in real time. Click **Add** to add it to the object group. In the figure, the existing **Client_Network** and **Client_PC** objects were added to the **Client_group_1** network object group
5. When you are finished adding all the addresses, click **OK** to close the Add Network Object Group window.
6. Click **Apply** to apply the configuration.

Repeat this procedure for all other network object groups that you need to create. For this example, you must create another network object group (External_servers), listing the three network objects that represent the three external servers.



In Task 3, configure service object groups that are used to group all services that are permitted or denied by a particular interface access rule.

The Cisco ASA supports six types of service groups. However, this course discusses only the most generic and flexible one—the IP service group. You can group any service into an IP service group; therefore the IP service group obsoletes all other service groups that were useful in older versions of Cisco ASA software.

Follow these steps to configure an IP service group using Cisco ASDM:

1. Navigate to **Configuration > Firewall > Objects > Service Groups** to administer service objects and service object groups.
2. Click **Add**. The following list of service types appears:

   Service Object: Creates an IP service object.

   Service Group: Creates an IP service object group. An IP service object group groups services based on arbitrary protocols. It is the only recommended service group that you should use.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

TCP Service Group: Creates a TCP service object group, which you could use to group services that use the TCP protocol.

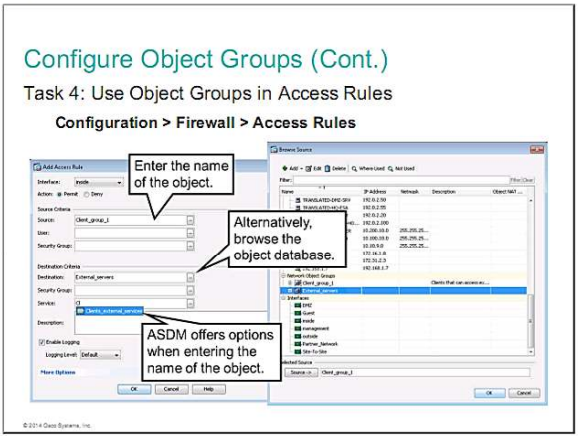
UDP Service Group: Creates a UDP service object group, which you could use to group services that use the UDP protocol

TCP-UDP Service Group: Creates a TCP and UDP service object group, which you could use to group services that use the same destination port over the TCP and UDP protocols.

ICMP Group: Creates an ICMP service object group, which you could use to group various ICMP services.

Protocol Group: Creates an IP service object group, which you could use to group IP protocols.

3. Follow these steps to configure an IP service object group:
4. Choose **Service Group** from the Add menu. The Add Service Group window appears.
5. Enter a name for the group in the Group Name field. The name can be up to 64 characters in length. The name must be unique for each object group. An IP service object group name cannot share a name with a network object group. In the figure, the IP service object group is named **Clients_external_services**.
6. From the Existing Service/Service Group pane, choose the members of the service object group. In the figure, the TCP HTTP, TCP FTP, UDP DNS, and ICMP echo services have been added to the service object group named **Clients_external_services**. You can choose individual services from a predefined list based on commonly used port, type, or protocol names. Otherwise, you can enter a new member in the Create New Member area. To create a new member, click the **Create New Member** radio button, specify the protocol and ports, types, codes, or protocol numbers, and click **Add**.
7. Click **Add** to add the group members to the Members in Group pane.
8. Click **OK** to close the Add Service Group window.
9. Click **Apply** to apply the configuration.



https://t.me/learningnets

Finally, in Task 4, you can use the created object groups to develop granular and manageable interface access rules. When creating rules in Cisco ASDM, you can click the ellipsis (...) button to the right of the Source, Destination, or Service field to select an object group. This action opens a browser window that enables you to choose configured object groups to be used as parameters for the access rule. This window is used in multiple configuration screens and is named appropriately for the current task. For example, from the Add Access Rule window, the Browse window is named "Browse Source," "Browse Destination," or "Browse Service," as shown in the figure. You can also enter the object group name directly into the Source, Destination, and Service fields, and you can add multiple object groups separated by commas.

In the figure, the previously configured object groups are used to create an access rule, as follows:

The action is Permit, and the rule is part of the inside interface input ruleset.

The source condition is the Client_group_1 network object group that you created.

The destination condition is the **External_servers** network object group that you created.

The service condition is the **Clients_external_services** IP service object group that you created.

Note You cannot delete an object group if it is part of an active rule because its removal would result in the rule becoming incomplete or invalid.

Configure Object Groups (Cont.)

CLI Configuration

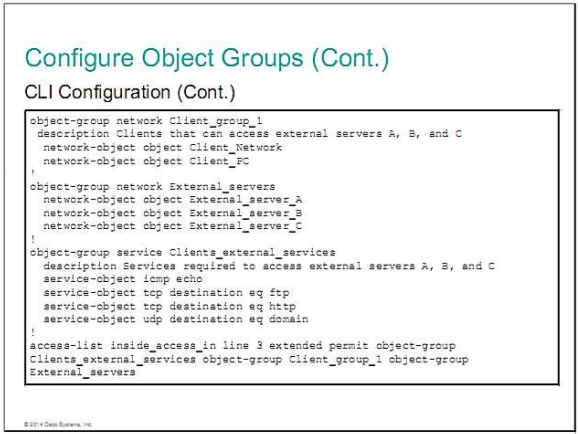
```
object network Client_Network
  subnet 10.3.0.0 255.255.0.0
  description Client Network
!
object network Client_PC
  host 10.1.1.2
  description Specific client
!
object network External_server_A
  host 172.16.1.2
!
object network External_server_B
  host 172.16.3.4
!
object network External_server_C
  host 172.16.5.6
```

© 2014 Cisco Systems, Inc.

To configure network objects on the Cisco ASA device using command line interface, use the commands that are described in the table.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Commands	Description
object network Client_Network **subnet 10.3.0.0 255.255.0.0** **description Client Network**	Creates a network object for a network.
object network Client_PC **host 10.1.1.2** **description Specific client**	Creates a network object for a host.
object network External_server_A **host 172.16.1.2**	Creates a network object for a host.



To configure object groups on the Cisco ASA device using command line interface, use the commands that are described in the table.

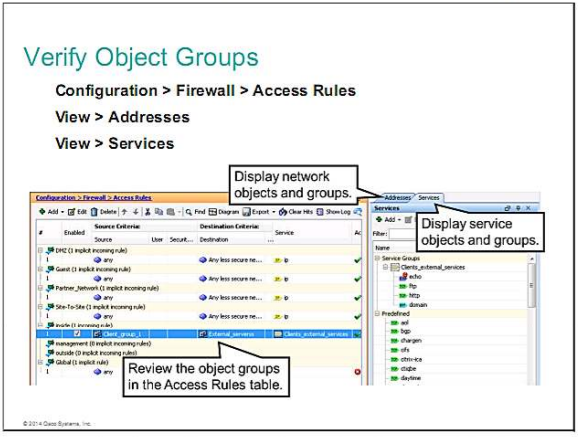
Commands	Description
object-group network Client_group_1 **description Clients that can access external servers A, B, and C** **network-object object Client_Network** **network-object object Client_PC**	Creates a network object group.
object-group network External_servers **network-object object External_server_A** **network-object object External_server_B** **network-object object External_server_C**	Creates a network object group.

Commands	Description
object-group service Clients_external_services **description Services required to access external servers A, B, and C** **service-object icmp echo** **service-object tcp destination eq ftp** **service-object tcp destination eq http** **service-object udp destination eq domain**	Creates a service object group.
access-list inside_access_in line 3 extended permit object-group Clients_external_services object-group Client_group_1 object-group External_servers	Configures an ACL that uses network and service object groups.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

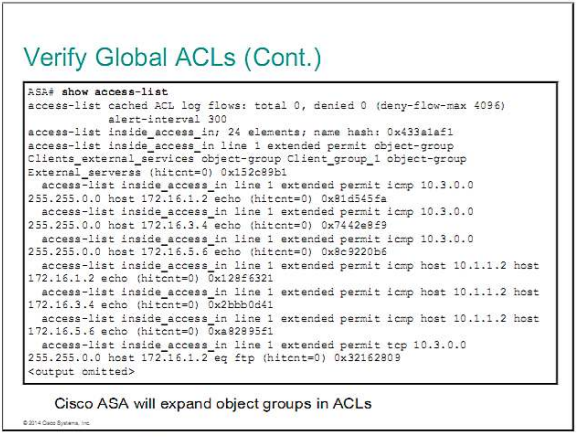
Verify Object Groups

This topic describes how to verify object groups on the Cisco Adaptive Security Appliance.



To verify the configuration of your object groups, inspect the Addresses and Services view in the Cisco Adaptive Security Device Manager and cross-reference the groups with the Access Rules table. You can expand all object groups to display all their members to easily verify rule accuracy.

Note Editing the contents of an object group automatically updates the policy of any rule that references the object group.



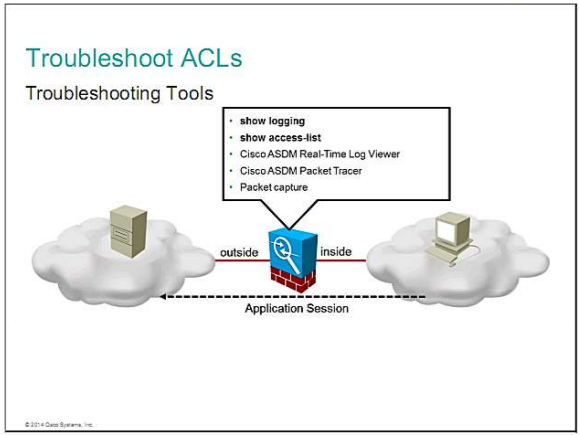
When you use the **show access-list** command on an access list that uses object groups, by default the Cisco ASA expands all object groups to create individual ACEs for each combination of object group members in a rule.

This figure illustrates the beginning of the expanded ACL that was used in the configuration scenario. In line 2 of the ACL, you can see the expansion that the security appliance created for the object-group-based ACE, which creates individual ACEs that describe members of the object group. This situation is often beneficial because you can observe rule hits for individual object group members or track rule hits by the individual ACE hexadecimal identifier.

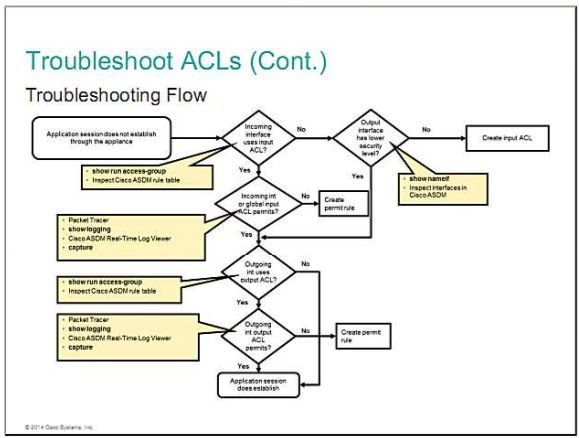
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Troubleshoot ACLs

This topic describes how to troubleshoot ACLs on the Cisco Adaptive Security Appliance.



To troubleshoot issues that are related to basic access control, you can use a set of Cisco ASA CLI and Cisco Adaptive Security Device Manager verification and debugging features. The figure lists some common commands and features that you might find useful during the troubleshooting session. Typically, you will examine why a particular session cannot be established through the security appliance.



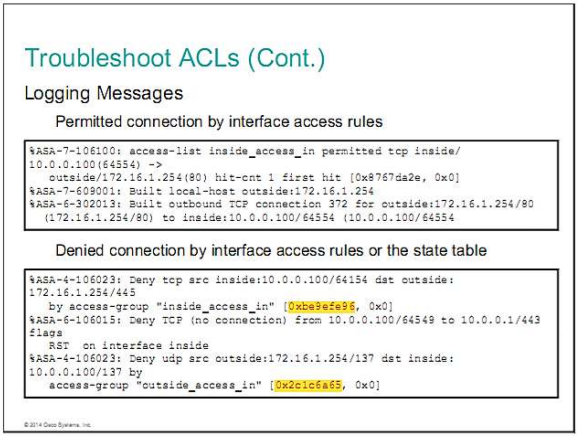
This figure shows the recommended task flow for troubleshooting basic access control through the Cisco ASA security appliance.

Follow these steps and use the provided commands to troubleshoot events where a host appears to have connectivity issues due to an implemented security policy:

First, determine whether the interface on which the connection is arriving at the security appliance uses a set of input access rules (an input ACL in the CLI). You can verify this condition by using the **show running-config access-group** command or by inspecting the Cisco ASDM Access Rules table. If it does, verify that the ACL permits this connection by using the CLI or Cisco ASDM Packet Tracer, by examining the Cisco ASA security appliance log for denied or permitted connections, or by using the packet capture facility. If no issues are revealed, you can proceed to Step 3. If the ruleset does not permit the problematic connection, create a permit rule that allows it.

If the input interface does not use a set of input access rules (an input ACL), you should determine whether the connection is routed to an output interface with a lower security level. If it is, the connection should be automatically permitted on the input interface and you can proceed to Step 3. However, remember that if you have configured any ACE in the global ACL, the implicit permit rule (permitting all traffic from high-security-level interface to lower-security-level interfaces) on the interface ACL is removed. If the connection is routed to an output interface with a higher security level, you must create an interface access ruleset (ACL) to permit such a connection.

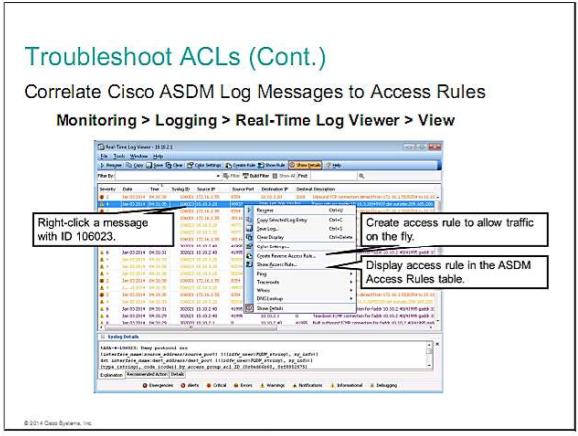
Finally, determine whether the interface to which the connection is routed inside the Cisco ASA uses a set of output access rules (an output ACL). You can verify this condition by using the **show running-config access-group** command or by inspecting the Cisco ASDM Access Rules table. If it does, verify that the ACL permits this connection by using the methods that are described in Step 1. If the ruleset does not permit the problematic connection, create a permit rule that allows it.



This figure shows typical syslog messages that can assist you in the troubleshooting process. The first output shows the expected messages that you see when a connection is permitted through the Cisco ASA security appliance. If you see these messages and still have connectivity issues, you should verify routing information in your network, especially if connection slots are inactivated with a synchronization timeout for TCP connections.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

If the security appliance denies a new connection because of an access rule, you see the 106023 syslog messages. You can use the hexadecimal identifier in a 106023 syslog message (highlighted in the figure) and the **show access-list** command to find an appropriate access list entry. You may also see the 106015 message. This message indicates that a non-initial packet has arrived to the Cisco ASA but it could not be matched to any connection object in the connection table. These packets are usually reconnaissance attempts or delayed legitimate packets that were received after legitimate sessions had already closed their transport connections.

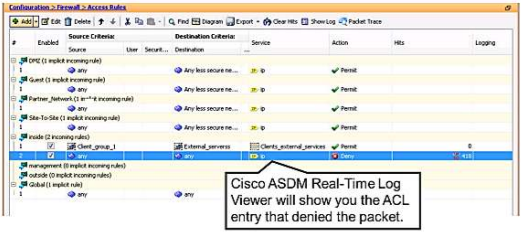


You can also use the Cisco ASDM Real-Time Log Viewer to examine the logging messages. You can right-click a message with ID 106023 and select the **Show Access Rule** option from the menu to correlate the logging message with the ACL entry that denied the packet.

You can also select the **Create Reverse Access Rule** option from the menu, which automatically creates an ACL rule that will allow previously denied packet and lets you review the rule before its application.

Troubleshoot ACLs (Cont.)

Correlate Access Rule to Log Messages - Real-Time Log Viewer

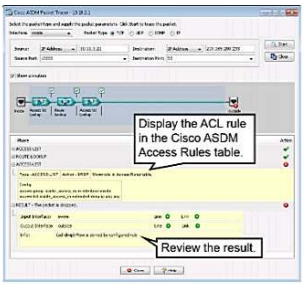


When you select the **Show Access Rule** option from the menu in the Cisco ASDM Real-Time Log Viewer, the ACL entry that denied the packet will be highlighted in the Access Rules table. Then, you can modify the ACL to allow the packets in the future.

Troubleshoot ACLs (Cont.)

Using the Cisco ASDM Packet Tracer

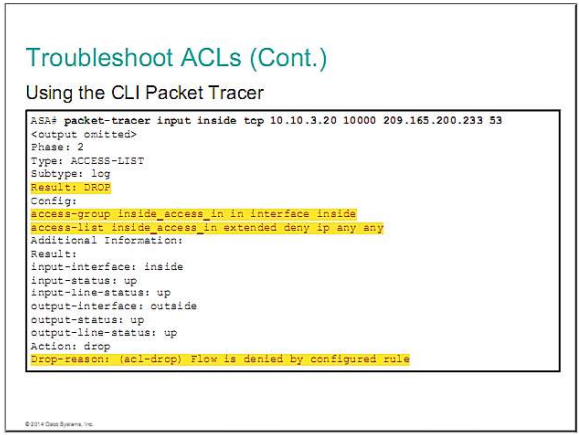
Tools > Packet Tracer



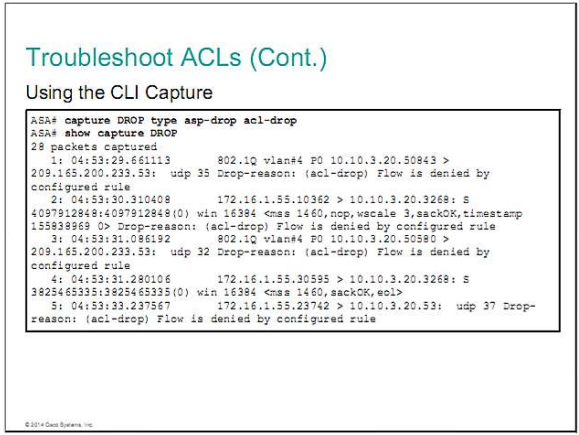
The Packet Tracer tool, discussed in an earlier module of this course, allows you to quickly pinpoint some possible reasons for connectivity issues through the Cisco ASA security appliance. You can start the Packet Tracer from the **Tools** menu. When the window appears, enter the connection parameters: the input interface, the source and destination IP addresses, and the source and destination ports. Click **Start** to diagnose the issue.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

In the example, the packet tracer has determined that the connection is blocked by a configured access rule. This is shown in the Result section of the Packet Tracer output. You can also expand the ACCESS-LIST phase of the trace to examine the ACL that denied the was matched by the packet. You can also display the ACL rule in the Cisco ASDM Access Rules table by clicking the **Show rule in the Access Rules table** option.



You can also use the packet tracer tool from the CLI, supplying it with the same information to start the tracing action. The figure shows an equivalent Packet Tracer session as was performed through Cisco ASDM in the previous figure.

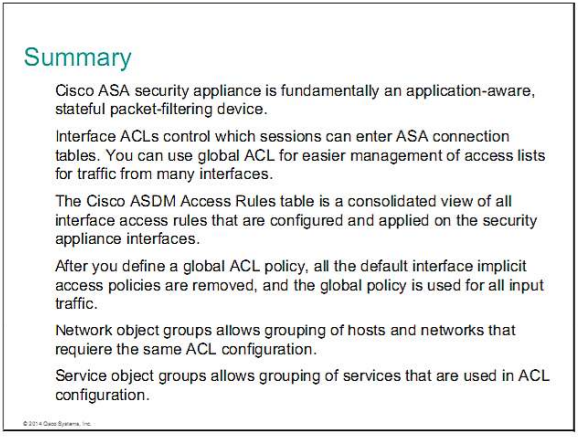


You can also use the packet capture facility on the Cisco ASA to find packets that were denied by configured access rules. Use the **capture** command and only capture packets that are dropped by configured access rules using the type **asp-drop acl-drop** filter. The figure shows an example of such a capture.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Summary

This topic summarizes the key points that were discussed in this lesson.



https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lesson 3

Deploying Advanced Cisco ASA Access Policies

Overview

Advanced Cisco Adaptive Security Appliance access policies allow security administrators to apply different policies to different types of traffic. For example, traffic coming from the Internet could be analyzed for any sign of malicious software. On the other hand, voice over IP traffic could be prioritized on all Cisco ASA interfaces to prevent delays and packet losses. The Cisco Modular Policy Framework is a configuration tools which enables security administrators to assign different network policies to different traffic flows in flexible and granular manner. The MPF enhances ASA interface Access Control Lists by allowing the administrator to specify a multitude of advanced access controls on network flows independently of interface ACLs.

This lesson first provides an overview of advanced access controls and policies. Then the lesson describes the Cisco MPF, which is used to implement advanced policies. Then the lesson discusses how to tune OSI Layer 3-4 stateful inspection and inspection of dynamic protocols. The lesson concludes with application inspection of HTTP and FTP protocols.

Upon completing this lesson, you will be able to:

- Provide an overview of advanced access policies
- Describe Cisco MPF on the Cisco ASA
- Describe Cisco MPF OSI Layer 3–4 policies
- Describe default OSI layer 3–4 stateful tracking
- Tune OSI Layer 3–4 stateful tracking
- Verify OSI Layer 3–4 stateful tracking
- Describe support for dynamic protocols
- Configure support for dynamic protocols

https://t.me/learningnets

Verify support for dynamic protocols

Describe Cisco MPF application layer (OSI layer 5-7) policies

Describe Cisco ASA HTTP inspector

Configure HTTP inspection

Verify HTTP inspection

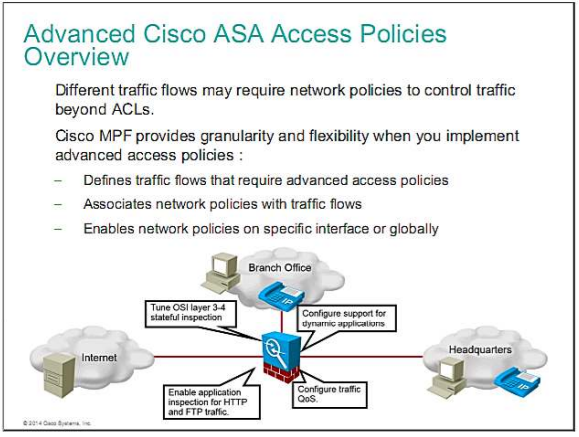
Describe Cisco ASA FTP inspector

Evaluate application inspection of other protocols

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Advanced Cisco ASA Access Policies Overview

This topic provides an overview of advanced access policies.



Different traffic flows traversing the Cisco ASA may require different network policies.

Some examples of advanced policies are listed bellow:

You could redirect traffic coming from the Internet to the Cisco Intrusion Prevention System module tool to scan the traffic for malicious traffic.

You could prioritize VoIP traffic between the branch office and headquarters to prevent delays and packet losses for voice traffic.

You could inspect HTTP traffic coming to the company web servers to allow only specific HTTP methods.

You could inspect outgoing HTTP and FTP traffic to prevent data loss.

The Cisco MPF configuration tool and philosophy enable administrators to describe network traffic and apply advanced and granular services to that traffic. Cisco MPF software provides tools for the following:

Defining traffic flows by describing their network properties

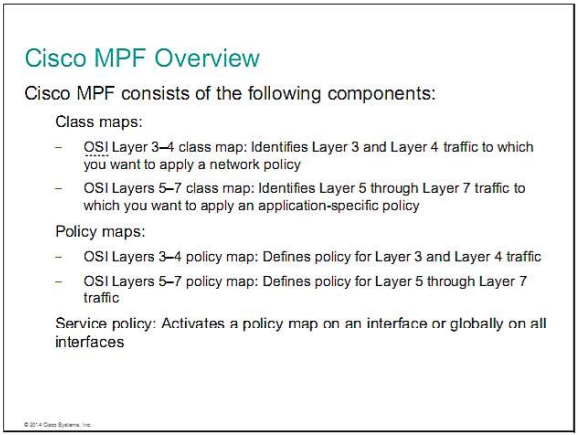
Associating network policies (actions) with traffic flows

Enabling network policies on a specific interface or globally on all interfaces of an enforcing device (Cisco ASA)

ACLs are the fundamental access control method on the Cisco ASA, and the Cisco MPF tool does not replace them. Instead, Cisco MPF provides an independent configuration tool to provide additional security policies to specific traffic flows.

Cisco MPF Overview

This topic describes Cisco Modular Policy Framework on the Cisco Adaptive Security Appliance.



The Cisco MPF consists of the following main components:

Class maps: A class map is a basic Cisco MPF object that is used to identify and group a set of particular traffic flows into a traffic class. A traffic flow is generally an OSI Layer 4 network session between endpoints that is used by a specific application. For example, a voice call can be defined as one traffic flow. For this flow, a class map can identify a traffic class as a set of voice calls between specific hosts or networks across the Cisco ASA security appliance. You can create class maps for OSI Layers 3 and 4 that classify traffic based only on the OSI Layer 3 and Layer 4 information that is found in a packet. This information would include such things as IP addresses, DSCP values, or ports. You can also create class maps for OSI Layers 5 through 7, which use application layer content to identify flows and classify them as part of the same class.

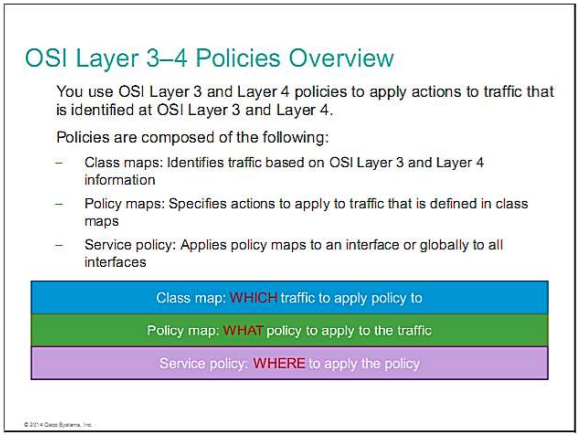
Policy map: You use a policy map to associate one or more actions with a class of traffic for one or more classes. For example, all voice traffic coming from headquarters to the branch office can be classified into a traffic class and associated with low latency queuing. To associate an action with a specific traffic class, you would create a policy map, specify a traffic class in the policy map, and associate an action with this specific class of traffic. You can create policy maps for OSI Layers 3 and 4, which define actions that are applied to traffic classes for these layers. You can also create policy maps for OSI Layers 5 through 7, which define actions that are applied to traffic classes for these layers.

Service policy: You use a service policy to activate policies by specifying where policy maps should classify and apply actions to traffic. A service policy activates a policy map either on a specific Cisco ASA security appliance interface or globally on all appliance interfaces. For example, you can apply the voice priority queuing policy to the outside interface, where it will identify packets of the voice traffic class and apply the appropriate egress queuing action.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

OSI Layer 3–4 Policies Overview

This topic describes Cisco Modular Policy Framework OSI layer 3-4 policies.

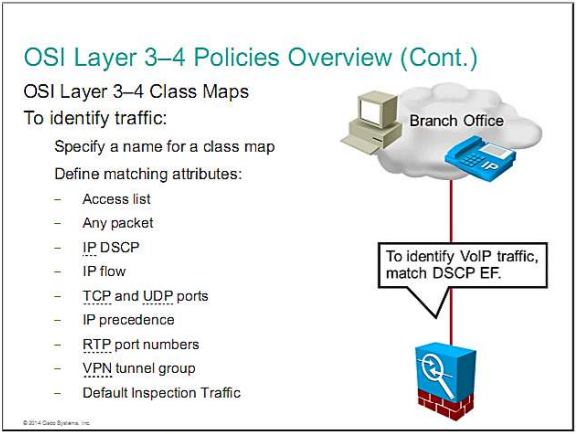


Use OSI Layers 3 and 4 policies to apply policy controls to traffic at OSI Layers 3 and 4. There are three components of the OSI Layers 3 and 4 network policies:

Class maps for Layers 3 and 4: These components identify traffic based on the packet information for these layers.

Policy maps for Layers 3 and 4: These components specify what actions to apply to traffic classes that are defined by class maps.

Service policy: This component applies a policy map to an interface or globally to all interfaces.



Class maps for OSI Layers 3 and 4 identify traffic based on protocols, ports, IP addresses, and other attributes for these layers. Configuring a class map is a two-step process:

You must assign a name to the class map that identifies a class of traffic.

You must specify matching attributes for the class of traffic.

After you configure a name for a class of traffic, you must identify the characteristics of the traffic flow. To identify traffic based on information for Layers 3 and 4, you can select the following matching criteria:

Access list: You can create an ACL, and all traffic matching this ACL will belong to the specified class.

Note You do not apply this classification ACL to an interface; it is solely used to identify traffic as belonging to a class. Traffic that this ACL permits belongs to the traffic class, and traffic that the ACL denies does not belong to the traffic class.

Any: Any packet will belong to this class.

IP DSCP: Defined by the IETF, this criterion is a DSCP value in the IP header. It allows you to define classes that are based on the DSCP values that are defined within the ToS byte in the IP header.

IP flow: This criterion represents all traffic that is going to a unique IP destination address. The policy action is applied to each flow instead of to the entire class of traffic.

TCP and UDP ports: This criterion represents traffic that is using the specified TCP or UDP destination port, or a contiguous range of ports.

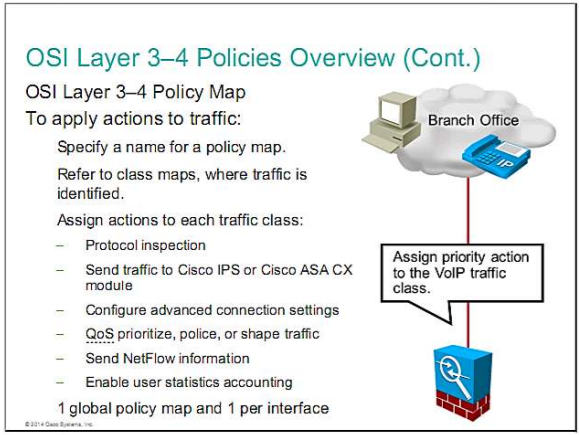
IP precedence: This criterion allows the user to define classes based on the IP precedence that is defined within the ToS byte in the IP header.

RTP port numbers: Representing a RTP destination port, this criterion allows you to match on a UDP port number within the specified range. The allowed range is targeted at capturing applications that are likely to be using RTP. The packet matches the defined class only if the UDP port falls within the specified range, inclusive, and the port number is an even number.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Tunnel group: This criterion represents VPN tunnel traffic that belongs to a specific VPN connection profile.

Default inspection traffic: This criterion will match all default TCP and UDP destination ports that the security appliance inspects by default. Mostly dynamic, navigating applications use these ports, and the stateful algorithm must additionally inspect these ports.



Configuring a policy map is a three-step process:

1. Create a policy map and assign a name to it
2. Refer to a class map inside the policy map, where traffic is identified
3. Assign actions to the traffic that is identified by the class map

You can apply the following policy actions to the traffic:

Perform a specified protocol inspection or inspections by creating an inspection policy

Send traffic to the Cisco IPS or Cisco ASA CX software module for further inspection

Configure advanced connection parameters on the traffic by creating a connection policy

Send NetFlow information about the traffic to the NetFlow collector

Prioritize, police, or shape traffic by creating a QoS policy

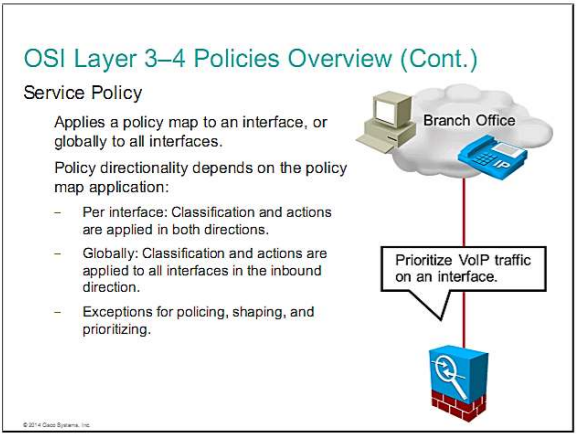
Enable user statistics accounting for identity firewall

A policy map can contain multiple policies. Each policy within a policy map can consist of a class map and its associated actions. For example, in a policy map, you can refer to the voice traffic and assign a priority action to it. In the same policy map, you can also refer to the traffic coming from the Internet and assign an action to send the traffic to the Cisco IPS module.

Note	Some of these actions are further discussed later in this lesson.

The Cisco ASA security appliance supports one global policy map and one policy map per interface.

In the example, a policy map should be configured that assigns a priority (low latency queuing) action to the traffic that was defined in the VoIP class map.

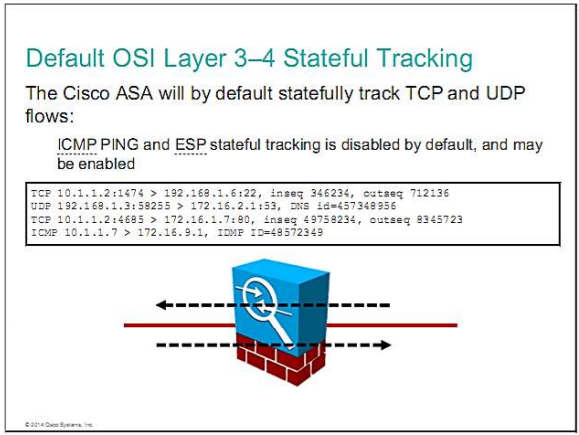


Service polices are used to apply policy maps to an interface or globally to all interfaces. Directionality of flow classification and policy actions that are specified in the policy map differ if you apply the policy map globally or to a specific interface.

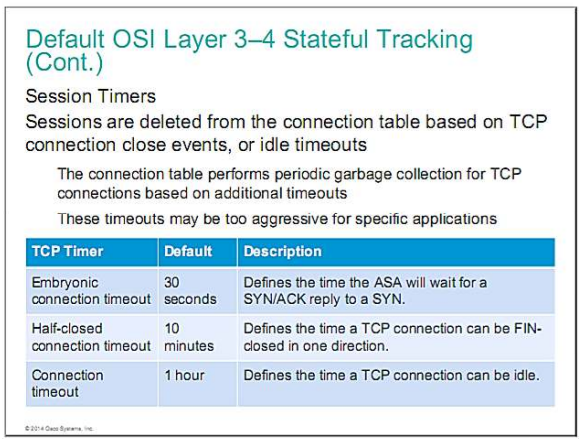
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Default OSI Layer 3–4 Stateful Tracking

This topic describes default OSI layer 3-4 stateful tracking.



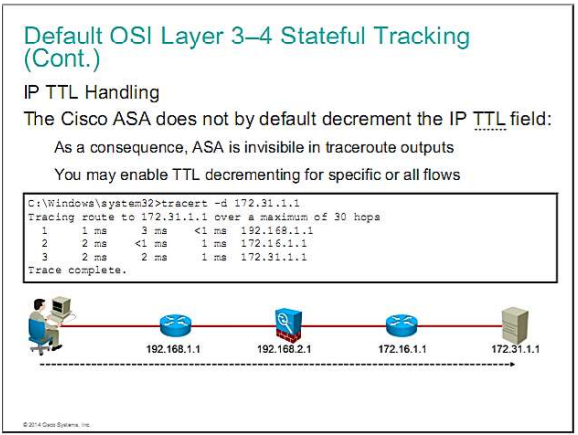
The Cisco ASA is fundamentally a stateful packet filtering device, which is application aware and is able to verify the legitimacy and correctness of network packets arriving on its interfaces by using various state tables. The Cisco ASA by default tracks all TCP and UDP flows using its connection table. You can optionally also enable tracking of ICMP requests and ESP traffic flows, which will automatically allow the ICMP echo reply and ESP packets to the originating hosts. Stateful tracking of ICMP and ESP flows is enabled using Cisco Modular Policy Framework.



The ASA will normally delete sessions from its state table based on normal connection-close events (for TCP, the FIN-based connection close sequence, or a RST-based forceful close; for UDP, and ICMP ping, based on an idle timeout, and for DNS, after it sees a DNS reply to the original request). However, the state table also anticipates extraordinary events by performing additional garbage collection and deletes connections from the table in several other scenarios: with unresponsive hosts, idle TCP connections, and more aggressively in some rare types of TCP exchanges.

The table above shows the three most important TCP connection timers and their default values. On the Cisco ASA, you can tune these timers using MPF or global timer settings to support local specifics, such as hosts using slightly non-standard TCP/IP stacks, or applications requiring specific session handling.

DCD is the Cisco ASA feature that detects a dead connection and allows it to expire, without expiring connections that can still handle traffic. You configure DCD when you want idle, but valid connections to persist. After a TCP connection times out, the security appliance sends DCD probes to the end hosts to determine the validity of the connection. If one of the end hosts fails to respond after the maximum retries are exhausted, the security appliance frees the connection. If both end hosts respond that the connection is valid, the security appliance updates the activity timeout to the current time and reschedules the idle timeout accordingly.

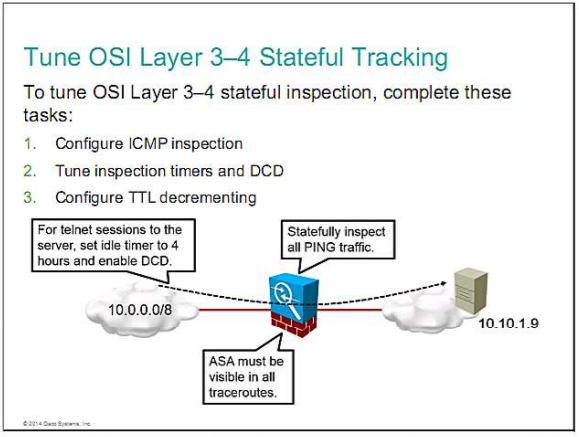


Although the ASA appears like an OSI Layer 3 router to its neighboring devices, it does not by default decrement the IP TTL field in transit packets. As a consequence, the ASA is not visible in a traceroute sequence, and relies on neighboring OSI Layer 3 devices to prevent routing loops. If you wish, you may configure the ASA to decrement the TTL for all, or only specific traffic flows through it, using MPF-based configuration.

https://t.me/learningnets

Tune OSI Layer 3–4 Stateful Tracking

This topic describes how to tune OSI Layer 3–4 stateful tracking.



To tune basic Cisco ASA OSI Layer 3–4 inspection parameters, perform one or more of the following steps, as needed in your environment:

1. Configure ICMP PING inspection if you want the ASA to track ICMP PING sessions statefully.
2. Tune the timers used by the connection table garbage collection routines, and configure the optional DCD feature to more optimally handle defunct long-lived sessions.
3. Configure the Cisco ASA to decrement the IP TTL for all or a subset of flows.

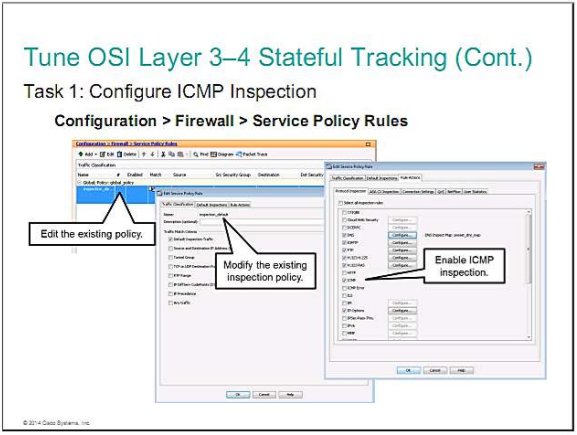
This figure shows the configuration scenario used in upcoming configuration tasks.

You will configure the Cisco ASA with the following exceptions to the default basic inspection policy:

Statefully inspect ICMP traffic crossing the appliance

For all telnet sessions to the host computer, configure a maximum idle time of 4 hours, and enable DCD for these connections to avoid expiring live sessions

Configure the Cisco ASA to be visible in all transit traceroute probes

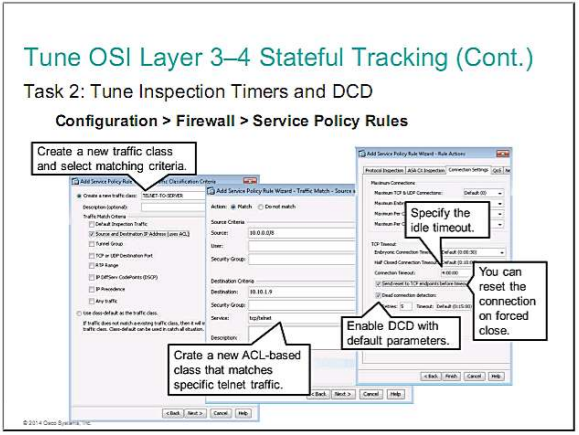


In the first task of this configuration sequence, you will configure stateful handling of ICMP across the security appliance. To configure stateful ICMP handling for all traffic across the appliance, you can modify the default inspection traffic class which by default already matches ICMP requests, but its associated default policy does not inspect it. You could also create a more specific class that matches ICMP packets instead, if needed.

Perform the following steps to enable stateful inspection of ICMP traffic

1. In the Cisco ASDM, navigate to **Configuration > Firewall > Service Policy Rules**.
2. Edit the service policy rule that applies to the inspection_default traffic class.
3. In the **Rule Actions** tab, and its **Protocol Inspection** sub-tab, check the **ICMP** inspection action.
4. Click **OK**.
5. Click **Apply** to apply your configuration.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

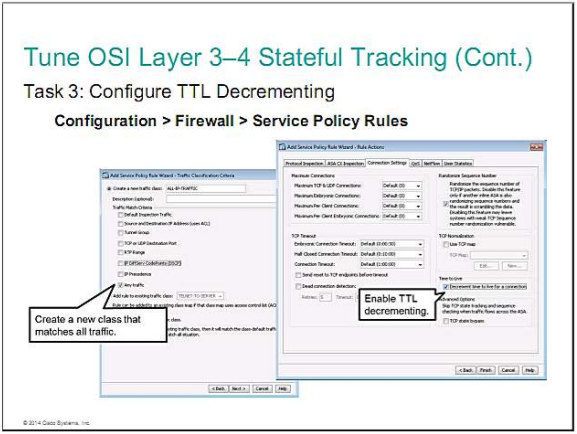


In the second task, you will tune the default TCP timers to configure a longer idle timeout, and enable DCD for a class of traffic. Using MPF configuration, you will create a new class of traffic that matches all telnet sessions to the server, and tune the TCP timeout settings for this class.

Perform the following ASDM steps:

1. From Cisco ASDM, choose **Configuration > Firewall > Service Policy Rules.**
2. Click the **Add** button to use the Add Service Policy Rule Wizard (not shown in the example).
3. Choose a global or per-interface policy rule (not shown in the example).
4. Choose to create a new class of traffic. Assign this class of traffic a unique name, and choose to define this class of traffic using an ACL.
5. In the Traffic Match step of the wizard, specify the source addresses (10.0.0.0/8 in this example) and the destination address (the host computer, 10.10.1.9 in this example) of traffic, and the tcp/telnet service.
6. In the Rule Actions step of the wizard, navigate to the **Connection Settings** tab. In the TCP Timeout section, specify the as 4:00:00 (4 hours), and enable the **Dead connection detection** checkbox to enable DCD for this class. You can optionally also check the **Send reset to TCP endpoints before timeout** option where the ASA will send connection close (TCP reset) segments to endpoints before it will delete the connection from its connection table.
7. Click **Finish** to close the Add Service Policy Rule Wizard - Rule Actions window, and click **Apply** to apply the configuration.

https://t.me/learningnets

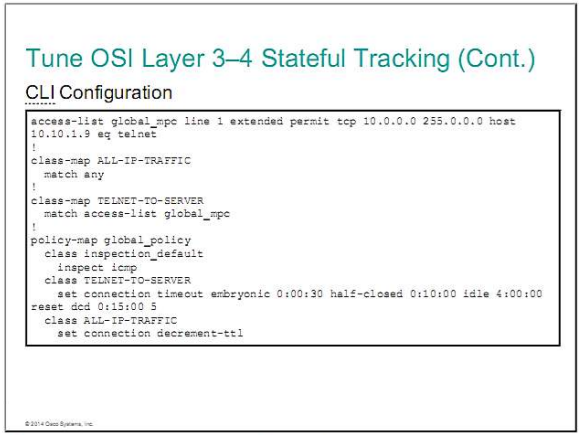


In the third task of this configuration sequence, you will tune the default TTL decrementing policy of the ASA to decrement the TTL for all IP packets across the ASA. Using MPF configuration, you will enable TTL decrementing for a "match any" class of the global policy.

Perform the following ASDM steps:

1. From Cisco ASDM, choose **Configuration > Firewall > Service Policy Rules.**
2. Click the **Add** button to use the Add Service Policy Rule Wizard (not shown in the example).
3. Choose a global policy rule.
4. Choose to create a new class of traffic. Assign this class of traffic a unique name, and choose **Any traffic** as the match criteria for this class.
5. In the Rule Actions step of the wizard, navigate to the **Connection Settings** tab. In the Time to Live section, check the **Decrement time to live for a connection** option to decrement TTL for all packets of this class.
6. Click **Finish**.
7. Click **Apply** to apply your configuration.

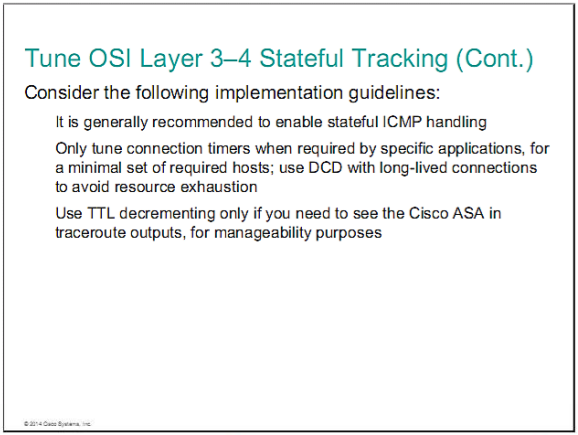
© 2014 Cisco Systems, Inc.
https://t.me/learningnets



To tune OSI Layer 3–4 stateful tracking on the Cisco ASA device using command line interface, use the commands that are described in the table.

Commands	Description
access-list global_mpc line 1 extended permit tcp 10.0.0.0 255.0.0.0 host 10.10.1.9 eq telnet	Creates an ACL
class-map ALL-IP-TRAFFIC **match any**	Creates a traffic class and matches all IP traffic
class-map TELNET-TO-SERVER **match access-list global_mpc**	Creates a traffic class and matches access list
policy-map global_policy	Enters the existing global policy configuration mode
class inspection_default **inspect icmp**	Enters inspection_default class configuration mode and enables ICMP inspection
class TELNET-TO-SERVER **set connection timeout embryonic 0:00:30 half-closed 0:10:00 idle 4:00:00 reset dcd 0:15:00 5**	Enters TELNET-TO-SERVER class configuration mode and changes session timers and enables DCD
class ALL-IP-TRAFFIC **set connection decrement-ttl**	Enters ALL-IP-TRAFFIC class configuration mode and enables TTL decrement

https://t.me/learningnets



When implementing the tuning of Cisco ASA OSI Layer 3-4 inspection, consider the following implementation guidelines:

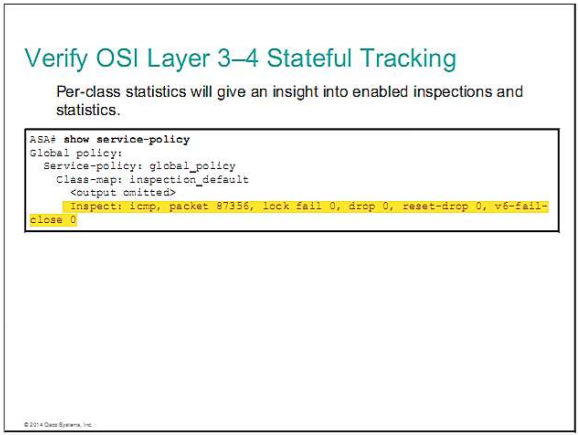
Generally, it is recommended to enable stateful ICMP handling on the ASA, as the alternative is to statelessly permit all ICMP echo replies to possible PING sources. On the other hand, enabling stateful ICMP inspection can impose additional load on the ASA if there are high rates of legitimate or malicious ICMP ping traffic in your network.

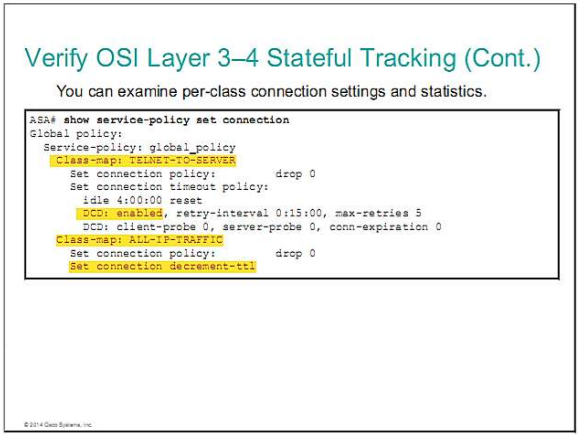
As suggested in general deployment guidelines, make minimal required changes to the stateful engine. This applies to tuning of connection timers and TTL decrementing. When tuning TCP idle timers, it is generally recommended to also enable DCD.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Verify OSI Layer 3–4 Stateful Tracking

This topic describes how to verify OSI Layer 3-4 stateful tracking.



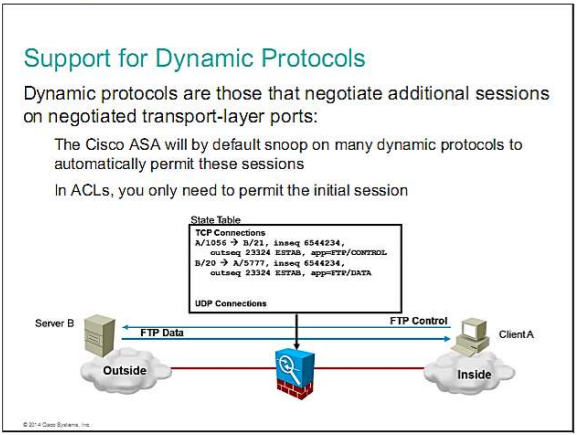


To display some global statistics and gain a general overview of the operation of protocol inspection and Layer 3-4 stateful inspection, use the **show service-policy** command. This command shows whether a protocol, such as ICMP, is inspected.

Use the **show service-policy set connection** command to display specific statistics for changed session timers, or changed TTL behaviour.

Support for Dynamic Protocols

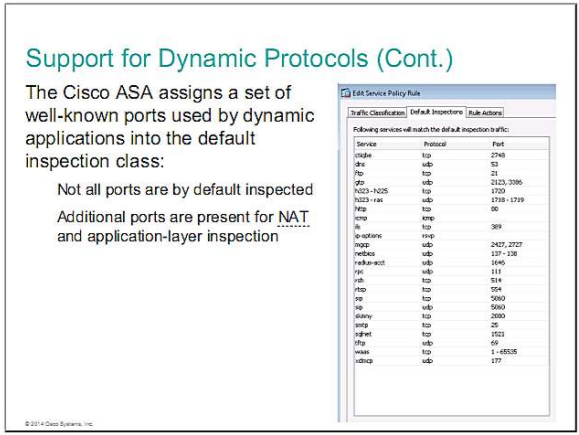
This topic describes support for dynamic protocols.



Dynamic protocols are those application protocols that establish a control session, and negotiate additional network sessions using dynamically-determined and negotiated ports between hosts. The Cisco ASA supports many dynamic protocols by snooping on the port negotiation and automatically permitting additional sessions of supported protocols.

Configuration-wise, you do not have to perform any configuration tasks to enable this behavior, if the dynamic protocol you are using is inspected by the Cisco ASA by default, inside its default inspection policy class. Inside Cisco ASA interface ACLs, you only need to permit the initial, control session, and all subsequent negotiated sessions will be permitted automatically.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



The Cisco ASA default inspection class includes protocols (services) that often require special handling. Special handling may be required because of:

Dynamic port negotiation (for example, for FTP, CTIQBE, GTP, H.323, MGCP, UNIX RPC, RSH, RTSP, SIP, SKINNY, SQL*net, TFTP, and XDCMP).

Special NAT requirements, where the CiscoASA must inspect and modify sessions to address the problem of IP addresses inside application layer payloads (FTP, CTIQBE, GTP, H.323, MGCP, RTSP, SIP, SKINNY, SQL*net).

Application-layer inspection, where the Cisco ASA may perform some default application-layer inspection for a service (DNS, ESMTP).

Note Note that not all services in the default inspection class are by default inspected. You can analyze the default enabled inspectors by examining the inspect actions assigned to the default inspection class in Cisco ASDM or the CLI.

Support for Dynamic Protocols (Cont.)

Default Inspectors in the Default Inspection Class

Inspector	Function
FTP	Allows FTP data connections
H.323 (H.225)	Allows negotiated RTP flows
H.323 (RAS)	Allows negotiated RTP flows
RSH	Allows RSH stderr connections
RTSP	Allows negotiated RTP flows
SCCP	Allows negotiated RTP flows
SIP	Allows negotiated RTP flows
Oracle SQL*Net (TNS)	Allows dynamic database connections
UNIX RPC (SUNRPC)	Allows all available UNIX RPC applications via the RPC portmapper

© 2014 Cisco Systems, Inc.

Support for Dynamic Protocols (Cont.)

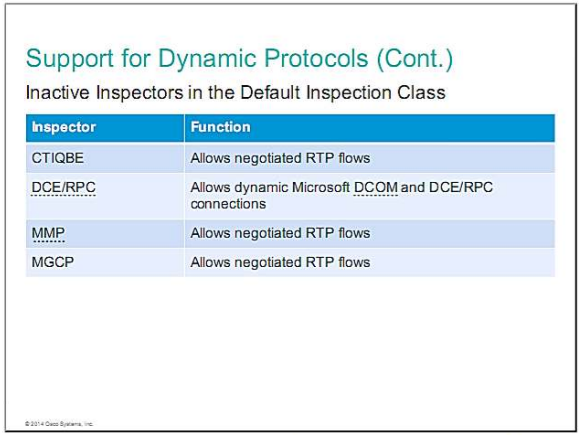
Default Inspectors in the Default Inspection Class (Cont.)

Inspector	Function
TFTP	Allows TFTP data connections
XDCMP	Allows dynamic XWindows display sessions

© 2014 Cisco Systems, Inc.

This table lists the dynamic protocol inspectors enabled by default for traffic matching the default inspection class. Default inspectors which only provide NAT or application-layer inspection are omitted from this table.

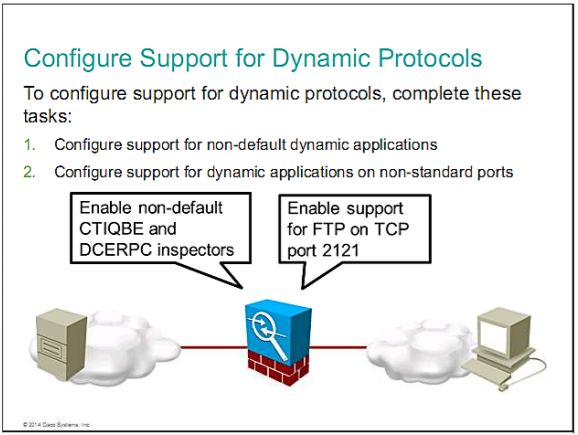
https://t.me/learningnets



This table lists the dynamic protocol inspectors disabled by default for traffic matching the default inspection class. Default inspectors which only provide NAT or application-layer inspection are omitted from this table as well. You may want to enable these inspectors by default if your firewall system should support the CTIQBE, DCERPC, MMP, and MGCP dynamic protocols.

Configure Support for Dynamic Protocols

This topic describes how to configure support for dynamic protocols.



When configuring Cisco ASA support for dynamic protocols, you will perform one or more of the following configuration tasks:

1. You will enable Cisco ASA support for non-default dynamic applications.
2. You will configure the Cisco ASA to support dynamic applications on non-default ports.

This figure shows the configuration scenario used in upcoming configuration tasks.

You will configure the Cisco ASA with the following changes to its default dynamic inspection policy:

You will enable inspection for the non-default CTIQBE and DCE/RPC protocols inside the default inspection class.

You will configure inspection support for the FTP protocol running over the non-default server port of 2121, in addition to the default port of 21.

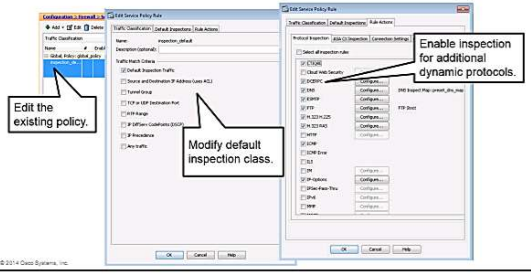
The configuration tasks assume that the Cisco ASA is already configured with all IP routing, an OSI Layer 3 – 4 security policy permitting CTIQBE, DCERPC, and FTP sessions, using a default inspection policy.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Configure Support for Dynamic Protocols (Cont.)

Task 1: Configure Support for Non-default Dynamic Applications

Configuration > Firewall > Service Policy Rules



To enable support for non-default dynamic protocol inspection inside the default inspection policy, you only need to enable additional inspectors for the Cisco ASA inspection_default class.

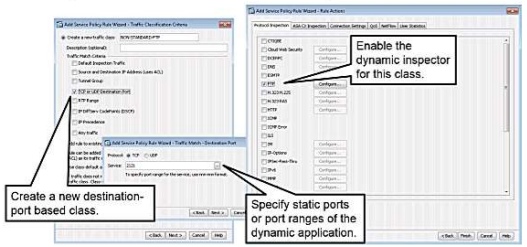
Perform the following steps to enable stateful inspection of ICMP traffic

1. In the Cisco ASDM, navigate to **Configuration > Firewall > Service Policy Rules**.
2. Edit the service policy rule that applies to the inspection_default traffic class.
3. In the Traffic Classification tab, verify that you are editing the rule that applies to the Default Inspection Traffic.
4. Switch to the **Rule Actions** tab, and additionally check the **CTIQBE** and **DCERPC** checkboxes to enable these inspectors with their default settings.
5. Click **OK**.
6. Click **Apply** to apply your configuration.

Configure Support for Dynamic Protocols (Cont.)

Task 2: Configure support for dynamic applications on non-standard ports

Configuration > Firewall > Service Policy Rules

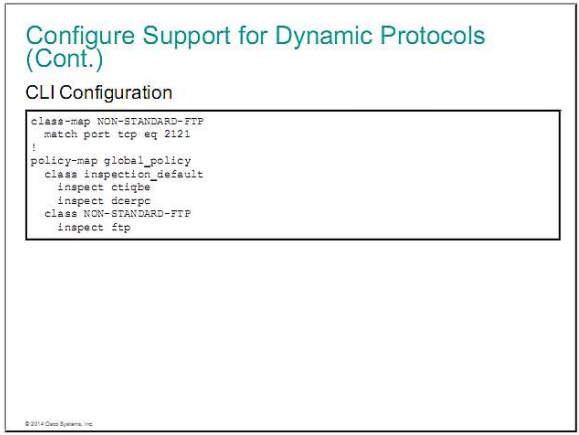


In the second task of this configuration sequence, you will create a service policy rule that will inspect FTP traffic on a non-default port. The default inspector for FTP traffic is already enabled by default in the default inspection class.

Perform the following Cisco ASDM steps:

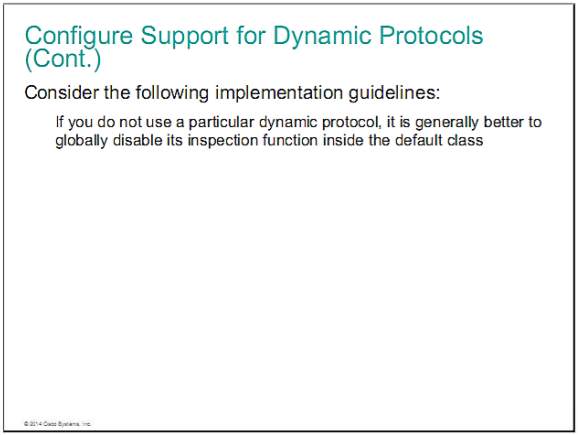
1. From Cisco ASDM, choose **Configuration > Firewall > Service Policy Rules.**
2. Click the **Add** button to use the Add Service Policy Rule Wizard (not shown in the example).
3. Choose a global policy rule (not shown in the figure).
4. Choose **Create a new class of traffic**. Assign this class of traffic a unique name, and choose **TCP or UDP destination port** as the match criteria for this class.
5. In the **Traffic Match** step of the wizard, specify TCP as the protocol, and the service port of 2121 as the additional FTP service port.
6. In the **Rule Actions** step of the wizard, navigate to the **Protocol Inspection** tab, and check the FTP protocol inspector check box to enable the inspector using its default settings.
7. Click **Finish** to close the Add Service Policy Rule Wizard - Rule Actions window, and click **Apply** to apply the configuration.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



To configure support for dynamic protocols on the Cisco ASA device using command line interface, use the commands that are described in the table.

Commands	Description
class-map NON-STANDARD-FTP **match port tcp eq 2121**	Creates a traffic class and matches TCP port 2121
policy-map global_policy	Enters the existing global policy configuration mode
class inspection_default **inspect ctiqbe** **inspect dcerpc**	Enters inspection_default class configuration mode and enables CTIQBE and DCERPC inspection
class NON-STANDARD-FTP **inspect ftp**	Enters class configuration mode and enables FTP inspection

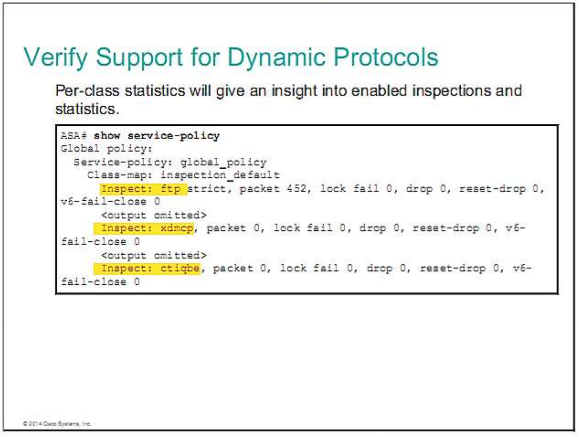


If your network does not use and support a particular dynamic protocol, it is generally recommended to disable its inspection on the Cisco ASA in order minimize Cisco ASA's unneeded functionality and therefore its attack surface.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Verify Support for Dynamic Protocols

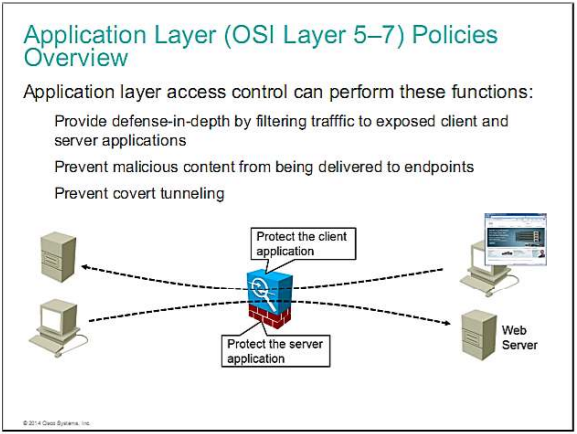
This topic describes how to verify support for dynamic protocols.



To display some global statistics and gain a general overview of the enabled inspectors, use the **show service-policy** command. This command shows whether a dynamic protocol, such as FTP, is inspected.

Application Layer (OSI Layer 5–7) Policies Overview

This topic describes Cisco Modular Policy Framework application layer (OSI layer 5-7) policies.



Firewall application inspections and controls inspect protocols on OSI Layers 5 to 7 and can filter on application layer protocol features and payloads to protect exposed server or client applications.

Application inspections and controls generally provide the following functions:

- It can prevent malicious protocol-level traffic (malformed protocol units, access to vulnerable protocol functions, and access to unwanted applications on the server) from being delivered to the target, thus protecting the target before traffic even reaches it. For example, a firewall that inspects and filters at the application layer can permit only required HTTP requests and allow access only to a specific URL pattern (that is, specific application) on a web server.
- It can prevent malicious content from being delivered to clients. For example, a firewall that inspects and filters at the application layer can permit only specific types of email or web content (HTML, text, Microsoft Office documents) to be delivered to an endpoint.
- It can restrict or prevent covert tunneling channels, where attackers or legitimate users tunnel one protocol within another. For example, the firewall can block attempts to tunnel other protocols in their raw form through port 80 (HTTP) or other protocols that are encapsulated within the HTTP fields that resemble legitimate HTTP.

Very importantly, firewall application layer inspections and controls can act as an independent, strong layer of defense to build a defense-in-depth solution. Network-based application layer inspections and controls are fully independent from the defenses of the endpoint and work well even if the endpoint is vulnerable or misconfigured.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

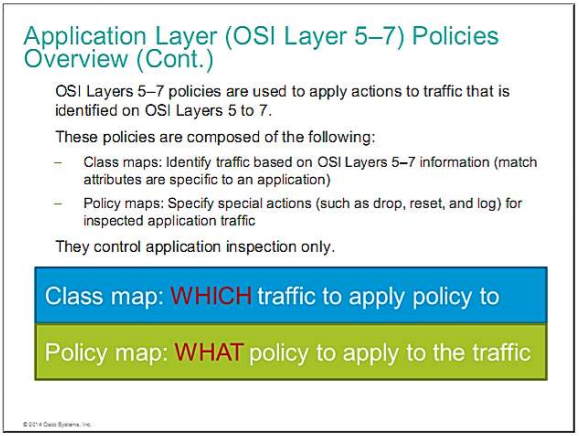
You can use four main approaches to implement application layer controls on an AIC-capable firewall, such as the Cisco ASA. These approaches are often combined to achieve the desired filtering goals:

Protocol minimization: With this approach, the AIC-capable firewall allows only a minimal required set of protocol features through to the endpoint. The purpose of this filtering is to minimize the attack surface of the endpoint and reduce the likelihood that a particular vulnerability is exposed to the untrusted network. This approach can prevent both known and unknown attacks, because it will block any traffic that is not part of its minimal specification.

Payload minimization: With this approach, the AIC-capable firewall allows only a minimal required set of application layer payloads (that is, application data) through to the endpoint. This approach can also prevent both known and unknown attacks, because it will block any data that is not part of its minimal specification.

Application layer signatures: With this approach, the AIC-capable firewall drops specific bad content (described by patterns that are known as signatures) that is inside application layer protocols and payloads. Typically, this approach prevents only known attacks that are described by signatures. You can use the native AIC functions of the Cisco ASA security appliance to implement application layer signatures, or you can use the Cisco IPS module that is integrated with the appliance.

Protocol verification: With this approach, the AIC-capable firewall drops application layer sessions that contain malformed (nonstandard) application layer protocol units. This approach can also prevent both known and unknown attacks, and can prevent tunneling of other protocols inside legitimate protocols that are allowed through the firewall.

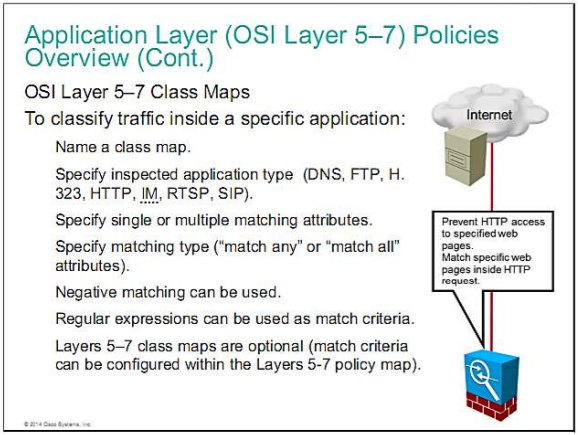


Policies for OSI Layers 5–7 are used to apply actions to traffic that is identified on OSI Layers 5 to 7. These policies are composed of the following:

Class maps for Layers 5 to 7: These components are used to identify traffic based on OSI Layers 5 to 7 inside a specific application. Application layer matching criteria that you can use are specific to each application protocol that is inspected by the Cisco ASA security appliance.

Policy maps for Layers 5 to 7: These components are used to assign actions, such as drop connection, reset connection, and log connection to the network traffic that is specified in a class map for OSI Layers 5 to 7.

Policies for OSI Layers 5 to 7 are used only for application inspection. You cannot use policies for Layers 5 to 7 to assign any other action to the traffic that is specified by the class maps for these layers.



To identify traffic inside a specific application that is based on information for OSI Layers 5 to 7, you must configure the following:

Create a class-map for OSI Layers 5–7 and assign a name to the class-map. Specify the type of application when you are creating the class-map for OSI Layers 5–7 for which you want to classify packets. Supported applications include DNS, FTP, H.323, HTTP, IM, RTSP, and SIP.

Within the class map for OSI Layers 5 to 7, specify matching attributes that are specific to each application. You can match single or multiple attributes.

If you use multiple attributes, you must specify a matching type:

- **Match any** attribute (the logical OR operator)
- **Match all** attributes (the logical AND operator)—this is the default

In addition, you can use the following:

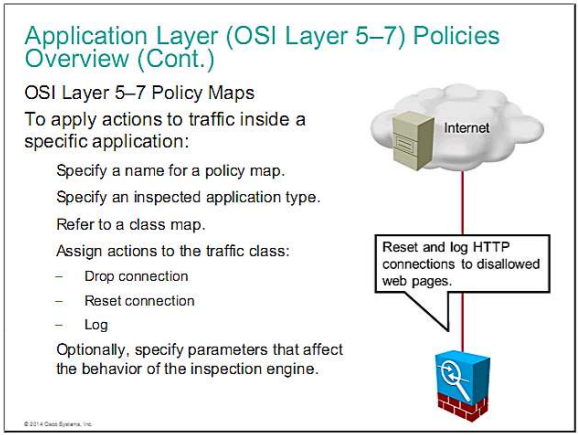
Negative matching (**match not**) allows you to specify attributes that should *not* occur in a packet (the logical NOT operator).

In some matching attributes, regular expressions enable you to search for a specific string inside an application.

Note Class maps for Layers 5–7 are an optional component. You can also specify matching statements directly in a policy map for Layers 5 to 7. However, class maps for these layers are useful when you would like to reuse the matching criteria or use very complex matching criteria that involve logical operators between multiple conditions.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

In the example, web browsing to disallowed websites should be denied. You would have to configure a class map for Layers 5 to 7 that matches specific hosts or domains inside the HTTP hostname parameter inside an HTTP request.



Policy maps for Layers 5–7 are used to apply actions to traffic inside a specific application. To configure a policy map for Layers 5–7, you must configure the following:

Create a policy-map for OSI Layers 5 to 7 and assign a name to the policy map.
Specify a type of application inspection when you create the policy map.

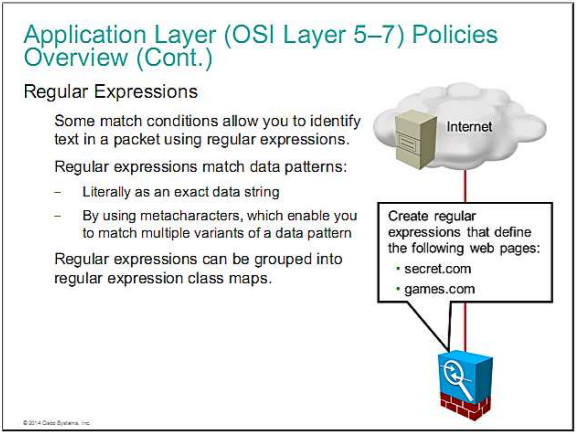
Refer to a class map for Layers 5–7.

Assign actions to the traffic class. The following actions are supported:

- Drop connection
- Reset connection
- Log connection

Optionally, specify parameters that affect the behavior of an inspection engine.

In the example, you would have to configure a policy map for OSI Layers 5–7 that resets and logs HTTP connections to disallowed websites.



In a class map for OSI Layers 5-7, some match conditions allow you to identify data patterns inside the application layer protocols using regular expressions (regex). Regular expressions are a data description language that is used to identify patterns in data. For example, you can use regular expressions to match URL strings or hostnames inside HTTP requests.

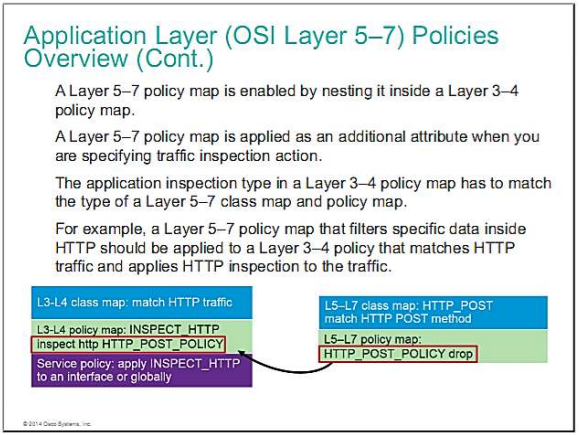
The Cisco ASA security appliance contains several built-in regular expressions; however, you can also create your own regular expressions for use in pattern matching. A regular expression matches data either literally, through exact data strings, or partially through metacharacters, which enable you to match multiple variants of data. Regular expressions that begin with "_default" are the built-in regular expressions; they cannot be modified or deleted. The maximum number of regular expressions per security appliance context is 2048.

You can use regular expressions to create custom security checks; you can permit, deny, or log any packet based on user-defined fields and regular expressions. In addition, you can combine these custom security checks for increased granular control.

You can group regular expressions into a special type of class maps called regular expressions class maps. Instead of configuring several match statements for each regular expression, you can group regular expressions into regular expression class maps and configure one match statement for an entire regular expression class map.

In the example, you would have to configure a regular expression class-map with two match regex statements that match the secret.com or games.com strings.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

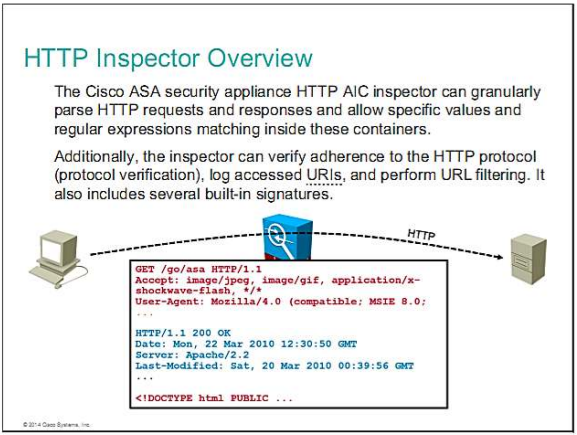


A policy map for Layers 5–7 is applied to traffic by nesting it inside a policy map for Layers 3-4. The policy map for Layers 5 to 7 is used as an additional attribute when you are enabling application inspection inside the policy map for Layers 3-4. You can only apply a Layer 5–7 policy map within another policy map that is inspecting the same application. For example, when configuring HTTP inspection, you can use policies for Layers-7 that are of HTTP application type.

In the example, a policy map for Layers 3–4 matches HTTP traffic and applies HTTP inspection action to the HTTP traffic. Additional HTTP inspections and controls are applied by nesting the policy map for Layers 5–7 in the policy map for Layers 3–4. The class map for Layers 5–7 matches the HTTP POST method and the policy map for Layers 5–7 drops HTTP packets that use the HTTP POST method.

HTTP Inspector Overview

This topic describes Cisco ASA HTTP inspector.

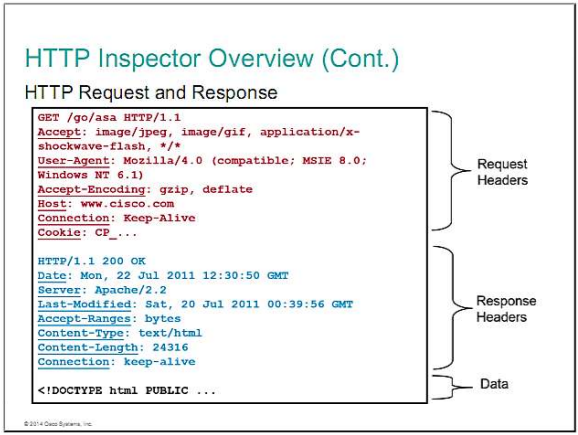


This topic focuses on the HTTP inspection routines of the Cisco ASA, because HTTP is the most widely used protocol across most firewalls. You can also deploy many of the following examples and functionalities with other protocols.

The HTTP inspection routines of the security appliance inspect the HTTP protocol and allow administrators to specify granular access rules that provide protection of both HTTP clients and servers. The HTTP inspection routines analyze the HTTP protocol and break it into granular containers, inside which the administrators can filter specific protocol values or use regular expressions to create custom pattern matching rules.

Additionally, the Cisco ASA provides built-in HTTP protocol verification routines. It can also log the accessed objects (URIs filter HTTP access category, that is, perform URL filtering), and include some built-in application layer signatures that can automatically detect tunneling of peer-to-peer, IM, and other sessions inside the HTTP protocol.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

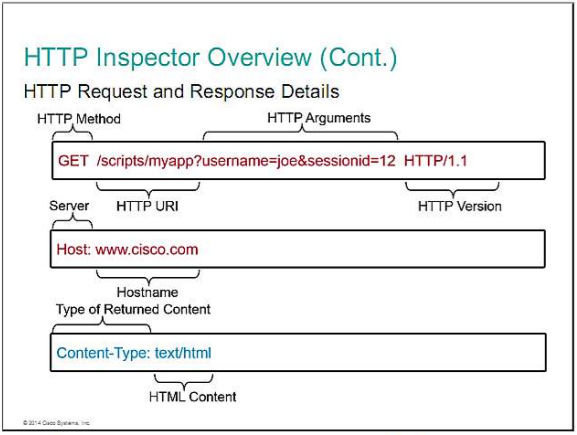


The HTTP protocol is a simple, text-oriented protocol that is used to exchange data between HTTP clients and servers. The protocol uses a request-response philosophy. This figure shows a typical HTTP exchange, where the HTTP client requests content from an HTTP server. In the example, a web browser navigated to the http://www.cisco.com/go/asa URL and requested content using the 1.1 version of the HTTP protocol.

The upper part of the transaction is the HTTP request headers, which the client submitted to the server. These headers identify the resource that the client wants to access, the HTTP virtual server (http://www.cisco.com) where content resides, and the parameters that the client supports.

In the middle part of the transaction, the server responded by first providing HTTP response headers. These headers are used to signal the status of the transaction (success, as indicated by the 200 OK code) and the parameters that identify the content that follows.

In the last part of the transaction, the server sends the actual content (HTML data) in the HTTP response body.



This output describes some of the most useful values in the parsed HTTP exchange.

The first line of the client HTTP request consists of an HTTP method (GET is the most common method), indicating that the client is requesting content. The next part after the HTTP method consists of the HTTP URI, indicating the server resource location. If the client needs to supply some application-specific data to the server inside a GET request, it can optionally use the HTTP arguments. (The arguments are separated from the URI by the question-mark character; multiple argument-value pairs are separated by the ampersand character.) The first line ends with the version of the HTTP protocol (1.1 in the example).

Later in the HTTP request headers, you can observe the host header, which indicates the HTTP virtual server that is being requested. This is the hostname from the URL in the browser address bar. You could filter on this value to restrict access to external resources based on their domain name.

In the HTTP response headers of the server, the Content-Type field identifies the type of content that follows in the HTTP response body. You could filter on this value to block specific types of content from being forwarded to clients or to allow only specific types of content to be available to clients.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

HTTP Inspector Overview (Cont.)

HTTP Request Field	Type of Match
Request Method	Specific values
Request URI	Regular expressions
Request Length	Numeric (greater than)
Request Arguments	Regular expressions
Request Header Field (names and values)	Specific values or regular expressions
Request Header Field Count	Numeric (greater than)
Request Header Field Length	Numeric (greater than)
Request Header Count	Numeric (greater than)
Request Header Length	Numeric (greater than)
Request Header Non-ASCII	Boolean (true or false)

© 2014 Cisco Systems, Inc.

The table provides a reference for the available filtering containers on the Cisco ASA AIC HTTP inspector for HTTP requests and the method of matching type that you can employ.

The type of match can be either a list of specific values that are hard-coded into Cisco ASA security appliance software (for example, specific HTTP request methods), numeric comparisons, user-defined patterns using regular expressions, or some signatures (built-in regular expressions) that are included inside Cisco ASA security appliance software.

HTTP Inspector Overview (Cont.)

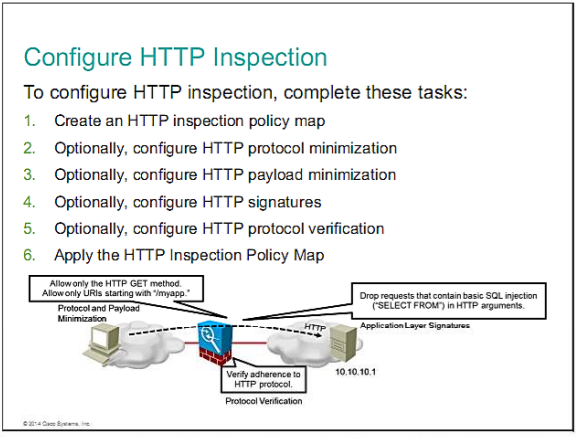
HTTP Response Field	Type of Match
Response Status Line	Regular expressions
Response Body	Java, ActiveX, regular expressions
Response Body Length	Numeric (greater than)
Response Header Field (names and values)	Specific values or regular expressions
Response Header Field Count	Numeric (greater than)
Response Header Field Length	Numeric (greater than)
Response Header Count	Numeric (greater than)
Response Header Length	Numeric (greater than)
Response Header Non-ASCII	Boolean (true or false)

© 2014 Cisco Systems, Inc.

The table provides you with a reference to the available filtering containers of the Cisco ASA AIC HTTP inspector for HTTP responses and the method of matching type that you can employ.

Configure HTTP Inspection

This topic describes how to configure HTTP inspection.



To configure an HTTP protection policy that can be used to filter application layer traffic to a web server that you want to protect, you will perform the following configuration tasks.

1. Create an HTTP inspection policy map
2. Optionally, configure HTTP protocol minimization
3. Optionally, configure HTTP payload minimization
4. Optionally, configure HTTP signatures
5. Optionally, configure HTTP protocol verification
6. Apply the HTTP Inspection Policy Map

This figure shows the configuration scenario that is used in the configuration tasks of this topic. You will create the following application layer policy between clients that are reachable over the outside interface of the Cisco ASA security appliance to a web server (10.10.10.1) that is reachable over the dmz interface:

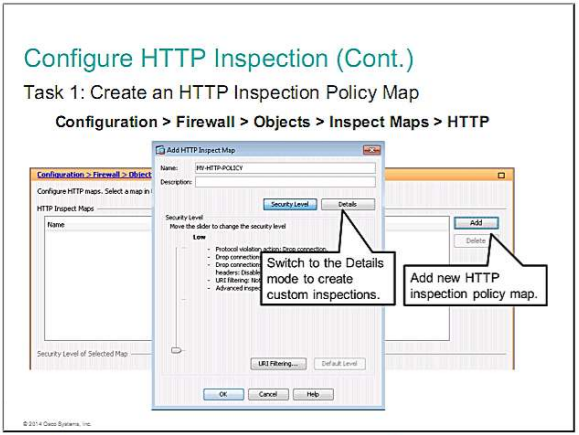
All outside clients can only use the HTTP GET method on the protected web server.

All outside clients can only access HTTP URIs starting with the "/myapp" string on the protected web server.

The ASA should drop all requests that contain basic SQL injection attempts (the string "SELECT" followed by the string "FROM") inside HTTP arguments.

The ASA should drop all requests that do not conform to the HTTP protocol.

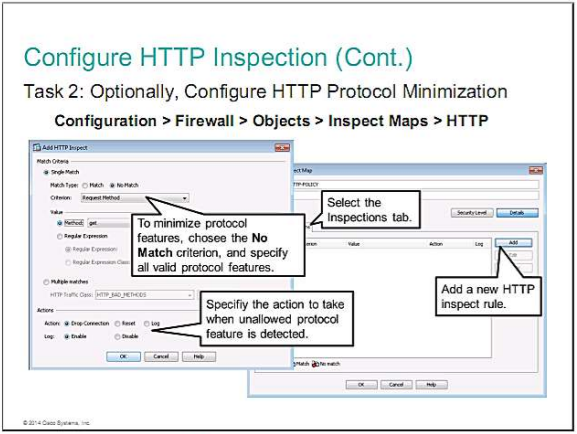
© 2014 Cisco Systems, Inc.
https://t.me/learningnets



In the first task of this configuration sequence, you create an HTTP inspection policy map on the Cisco ASA security appliance. An HTTP inspection policy map is a configuration container that encapsulates a set of inspections that will be applied to a specific set of flows (that is, a Cisco MPF traffic class) and is reusable in multiple traffic classes.

Follow these steps to create an HTTP inspection policy map using Cisco ASDM:

1. In the Cisco ASDM, navigate to **Configuration > Firewall > Objects > Inspect Maps.**
2. Choose **HTTP** from the Inspect Maps menu (not shown in the figure). The HTTP window appears.
3. Click **Add** to add a new HTTP inspection policy map. The Add HTTP Inspect Map window appears.
4. The Add HTTP Inspect Map window allows you to select a predefined security level to use in this HTTP inspection policy map or switch to the Details view to configure individual inspection. To configure the policy in this configuration sequence, you will use the Details view to configure the policy from inception. Click the **Details** button to switch to the Details mode.



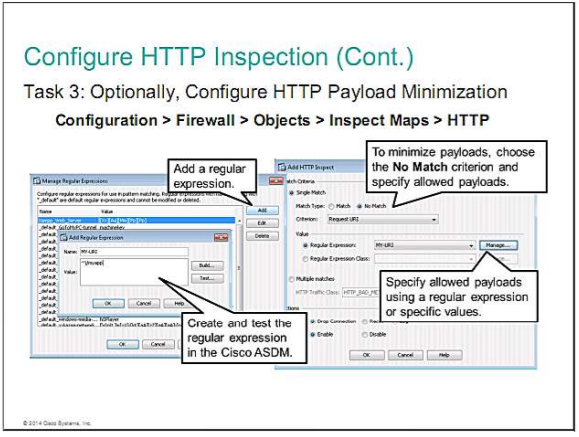
In Task 2, you optionally configure HTTP protocol minimization by allowing only specific features of the HTTP protocol to be passed to the protected web server. In the example, you will allow only the GET request method to the server. You could configure additional rules to minimize other aspects of the HTTP protocol.

Follow these steps to create an HTTP protocol minimization inspection rule in the HTTP inspection policy map using Cisco ASDM:

1. In the Inspections tab of the Details view of the HTTP inspection policy map, click **Add** to add a new inspection rule. The Add HTTP Inspect window appears.
2. Click the **Add** buttoIn the Match Criteria section, click the **Single Match** option to specify a single condition (only one match statement) that will match traffic in this inspection rule. You could also choose the **Multiple Matches** options to match the traffic using a predefined HTTP (Layers 5 to 7) class map. In the HTTP class map, you can specify multiple match statements.n to use the Add Service Policy Rule Wizard (not shown in the example).
3. In the Match Criteria section, choose **No Match** as the match type if you want to drop all traffic except traffic that matches specific criteria (that is, a minimization policy).
4. From the Criterion drop-down list, choose the HTTP protocol container in which you want to analyze traffic for specific values. In the example the Request Method container is chosen to filter traffic based on the HTTP request method.
5. In the Value area, specify the values of the criterion container that you expect for this rule. Because you want this rule to trigger on all requests that do not use the GET method, choose **Get** from the Method drop-down list. You could also specify a custom regular expression (or a set of regular expressions in a regular expression class) to describe the expected HTTP method. However, if the value you are expecting is available in a predefined list, it is strongly recommended that you use the predefined value instead of defining regular expressions.
6. In the Actions section, define the actions that the Cisco ASA security appliance should take when it is successfully matching traffic against this rule. In the example, the Drop Connection action is chosen and the logging of match events is enabled by enabling the Log option.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

7. Click **OK** when you are finished defining the inspection rule.
8. You can apply the inspection policy map and save the configuration if needed or continue defining additional inspections.

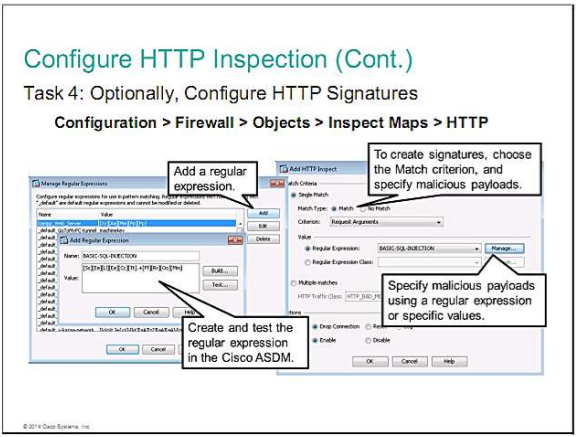


In Task 3, you optionally configure HTTP payload minimization by allowing only specific payloads that are inside the HTTP protocol to be delivered to the protected web server. In the example, you will allow only a specific URL prefix to the server. You could configure additional rules to minimize other payloads inside the HTTP protocol, such as request arguments or content types.

Follow these steps to create an HTTP payload minimization inspection rule in the HTTP inspection policy map using Cisco ASDM:

1. In the Inspections tab of the Details view of the HTTP inspection policy map, click **Add** to add a new inspection rule. The Add HTTP Inspect window appears.
2. In the Match Criteria section, choose the **Single Match** option to specify a single condition that will match traffic in this inspection rule (not shown in the example).
3. In the Match Criteria section, choose **No Match** as the match type if you want to drop all traffic except traffic that matches specific criteria (that is, a minimization policy).
4. From the Criterion drop-down list, choose the HTTP protocol container in which you want to analyze traffic for specific values. In the example, the Request URI container is chosen to filter traffic based on the HTTP URI that users are accessing on the web server.
5. In the Value subsection, specify the values of the criterion container that you expect for this rule. If you want this rule to trigger on all requests that do not start with "/myapp," specify a custom regular expression to describe the expected HTTP URI. Click **Manage** to enter the Cisco ASDM regular expression configuration tool. The Manage Regular Expressions window appears.
6. In the Manage Regular Expressions window, click **Add** to add a new regular expression. The Add Regular Expression window appears.

7. In the Add Regular Expression window, assign a name (in the example, "MY-URI") to the regular expression. In the Value field, enter the regular expression that describes the URI prefix on which you want to filter. In the example, the "/myapp" prefix is described with the "^\/myapp" regular expression. The caret (^) in the regular expression indicates the start of the URI and the slash (/) is escaped with the backslash (\).
8. Optionally, click the **Test** button and enter **/myapp** as the test input to test the regular expression. The match should succeed.
9. Click **OK** in the Add Regular Expression window.
10. Ensure that your new regular expression is selected in the Manage Regular Expressions window and click **OK**. Your new regular expression should be selected in the inspection rule. (The regular expression value from Step 5 should now show "MY-URI.")
11. In the Actions section, define the actions that the Cisco ASA security appliance should take when it is successfully matching traffic against this rule. In the example, the Drop Connection action is chosen and logging of match events is enabled by enabling the Log option (not visible in the example).
12. Click **OK** when you are finished defining the inspection rule.
13. You can apply the inspection policy map and save the configuration if needed or continue defining additional inspections.



In Task 4, you will optionally configure HTTP signatures by dropping known bad payloads that are inside HTTP sessions to the protected web server. In the example, you will drop all HTTP sessions that contain the "SELECT FROM" string inside HTTP request arguments. You could also configure additional signatures to block other known attacks.

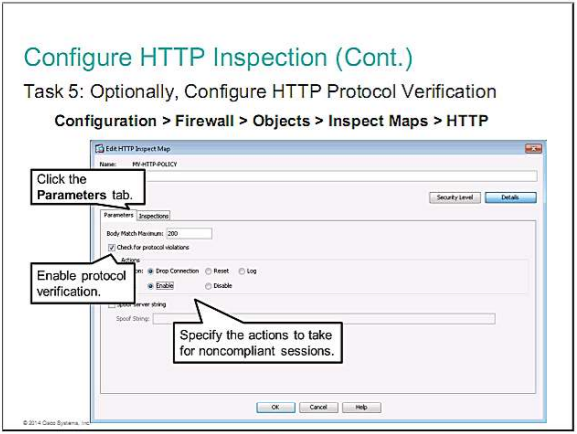
Follow these steps to create an HTTP signature rule in the HTTP inspection policy map using Cisco ASDM:

1. In the Inspections tab of the Details view of the HTTP inspection policy map, click **Add** to add a new inspection rule. The Add HTTP Inspect window appears.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

2. In the Match Criteria section, choose the **Single Match** option to specify a single condition that will match traffic in this inspection rule.
3. In the Match Criteria section, choose **Match** as the match type if you want to drop traffic that matches specific criteria (that is, a signature approach).
4. From the Criterion drop-down list, choose the HTTP protocol container in which you want to analyze traffic for specific values. In the example, the Request Arguments container is chosen to filter traffic based on the contents of the HTTP arguments field.
5. In the Value area, specify the values of the criterion container that you expect for this rule. Because you want this rule to trigger on all requests that contain the basic SQL injection "SELECT FROM" substring, specify a custom regular expression to describe the malicious pattern. Click the **Manage** button to enter the Cisco ASDM regular expression configuration tool. The Manage Regular Expressions window appears.
6. In the Manage Regular Expressions window, click **Add** to add a new regular expression. The Add Regular Expression window appears.
7. In the Add Regular Expression window, enter a name (BASIC-SQL-INJECTION in the example) for the regular expression. In the Value field, enter the regular expression that describes the malicious pattern that you want to match. In the example, the malicious pattern is described with the "[Ss][Ee][Ll][Ee][Cc][Tt].+[Ff][Rr][Oo][Mm]" regular expression. The regular expression is case insensitive to prevent evasion by changing character case and the ".+" expression matches one or more characters (including spaces and tabs) between the two words.
8. Click **OK** in the Add Regular Expression window.
9. Ensure that your new regular expression is selected in the Manage Regular Expressions window and click **OK**. Your new regular expression should be selected in the inspection rule. (The regular expression value from Step 5 should now show "BASIC-SQL-INJECTION.")
10. In the Actions section, define the actions that the Cisco ASA security appliance should take when successfully matching traffic against this rule. In the example, the Drop Connection action is chosen and logging of match events is enabled by enabling the Log option.
11. Click **OK** when you are finished defining the inspection rule.
12. You can apply the inspection policy map and save the configuration if needed or continue defining additional inspections.

https://t.me/learningnets

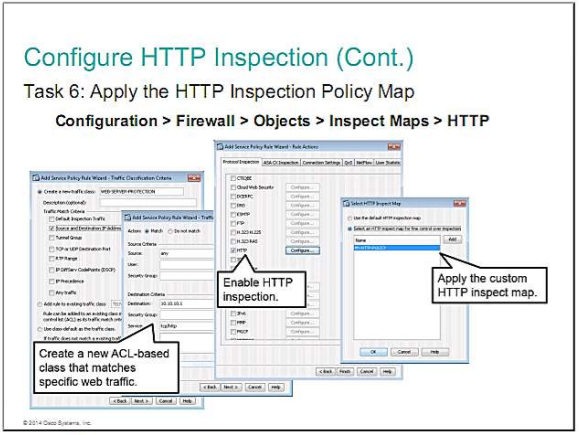


In Task 5, you configure optional HTTP protocol verification to drop all HTTP sessions that do not conform to the standard protocol specification.

Follow these steps to enable HTTP protocol verification in the current HTTP inspection policy map:

1. Click the **Parameters** tab in the Details view of the HTTP inspection policy map and check the **Check for Protocol Violations** check box to enable HTTP protocol verification.
2. In the Actions section, define the actions that the Cisco ASA security appliance should take when detecting protocol violations. In the example, the **Drop Connection** action is chosen and logging of violation events is enabled by enabling the **Log** option.
3. Click **OK** when you are done defining the inspection rule.
4. Click **Apply** to apply the inspection policy map. Click **Save** to save the configuration if needed.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

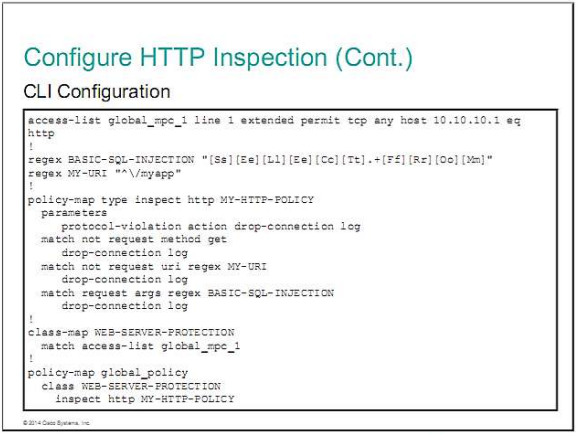


Finally, in Task 6 of this configuration sequence, you configure a service policy rule that applies the configured HTTP inspection policy map to a traffic class that describes HTTP traffic to the web server.

Follow these steps to apply the configured HTTP inspection policy map to a new traffic class. Perform the following Cisco ASDM configuration steps:

1. Choose **Configuration > Firewall > Service Policy Rules**. The Service Policy Rules window appears.
2. Choose **Add Service Policy Rule** from the Add drop-down menu to add a new service policy rule to the Cisco ASA security appliance. The Add Service Policy Rule window appears (not shown in the example).
3. Choose an interface-based or global service policy rule, depending on your configuration needs. In the example, Global is selected. Click **Next** to continue. (The example does not show this step.)
4. In the Traffic Classification Criteria window, click the **Create a New Traffic Class** radio button and assign the traffic class a name (WEB-SERVER-PROTECTION in the example). Check the **Source and Destination IP Address (Uses ACL)** check box under Traffic Match Criteria. Click **Next**.
5. In the Traffic Match window, click the **Match** radio button for the Action, choose **ANY** as the source address, choose **10.10.10.1** (the web server IP address) as the destination address, and choose **tcp/http** as the Service. Click Next.
6. In the Rule Actions window, click the **Protocol Inspection** tab. Check the **HTTP** check box and click the Configure button to launch the Select HTTP Inspect Map window. Choose the configured HTTP inspection policy map and click **OK**. In the example, MY-HTTP-POLICY inspection policy that was previously configured is chosen.
7. Click **Apply** to apply the configuration.

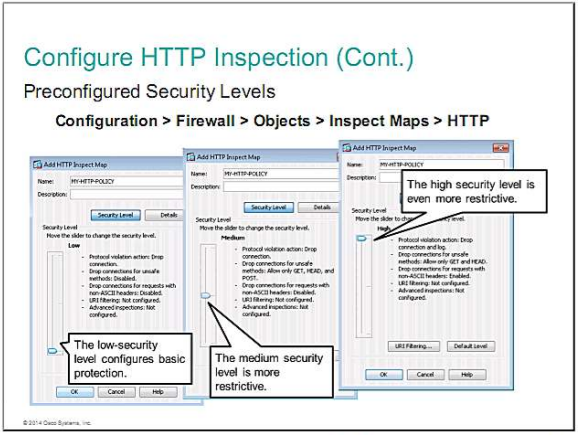
https://t.me/learningnets



To configure HTTP inspection on the Cisco ASA device using command line interface, use the commands that are described in the table.

Commands	Description
access-list global_mpc_1 line 1 extended permit tcp any host 10.10.10.1 eq http	Creates an ACL that matches HTTP traffic
regex BASIC-SQL-INJECTION "[Ss][Ee][Ll][Ee][Cc][Tt].+[Ff][Rr][Oo][Mm]" **regex MY-URI "^\/myapp"**	Creates two regular expressions
policy-map type inspect http MY-HTTP-POLICY **parameters** **protocol-violation action drop-connection log** **match not request method get** **drop-connection log** **match not request uri regex MY-URI** **drop-connection log** **match request args regex BASIC-SQL-INJECTION** **drop-connection log**	Creates an OSI layer 5-7 policy map of type HTTP and specifies matching conditions
class-map WEB-SERVER-PROTECTION **match access-list global_mpc_1**	Creates a class-map based on the ACL
policy-map global_policy **class WEB-SERVER-PROTECTION** **inspect http MY-HTTP-POLICY**	Enables HTTP inspection with the previously defined layer 5-7 policy map for the traffic class.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



In the preceding configuration scenario, you configured an HTTP inspection policy map by configuring individual inspection parameters. You can also configure an HTTP inspection policy map in a simplified fashion using the security level slider, which allows you select low, medium, or high (depending on the inspected protocol) levels of application layer protection using built-in default policies.

With the HTTP inspector, you can choose between the low, medium, and high security levels inside the initial Add/Edit HTTP Inspect Map window.

The low security level enables only protocol verification and drops all connections that violate the HTTP specification. You can quickly add simple URL filtering rules to this policy using the URI Filtering button, which will take you to an inspection rule that filters on HTTP request URIs. The following is an example of an inspection policy map with a low security level:

```
policy-map type inspect http low
  parameters
    protocol-violation action drop-connection
```

The medium security level extends the features of the low security level by also allowing only the GET, HEAD, and POST HTTP methods. The following is an example of an inspection policy map with a medium security level:

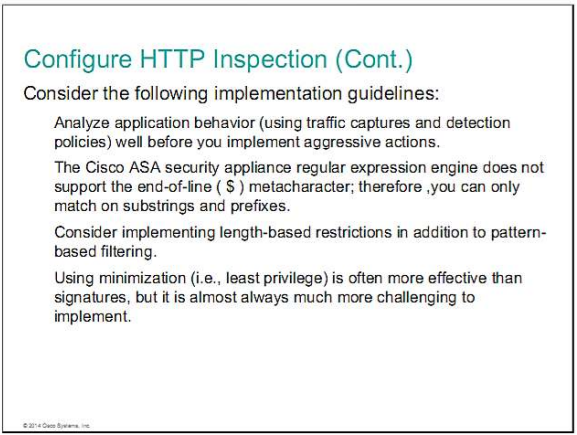
```
class-map type inspect http match-all asdm_medium_security_methods
  match not request method head
  match not request method post
  match not request method get
policy-map type inspect http med
  parameters
     protocol-violation action drop-connection
  class asdm_medium_security_methods
     drop-connection
```

The high security level extends the features of the medium security level by also allowing only the GET and HEAD HTTP methods and dropping connections that contain non-ASCII HTTP headers (which is unusual and suspicious). The following is an example of an inspection policy map with a high security level:

```
class-map type inspect http match-all asdm_high_security_methods
```

```
    match not request method head
    match not request method get
policy-map type inspect http high
    parameters
      protocol-violation action drop-connection log
    class asdm_high_security_methods
      drop-connection
    match request header non-ascii
      drop-connection
```

Note You can start configuring an HTTP inspection policy map using security levels to enable a starting set of inspection settings and then switch to the Details view to customize (add, remove, or modify) the settings that are created by the Security Level macro.



When you deploy HTTP application layer access control policies using the AIC features of the Cisco ASA, consider the following implementation guidelines:

Analyze application behavior in detail before enabling aggressive actions that will affect application layer features. Use traffic captures and deploy your policies in detection mode, using only the logging of unwanted traffic, before implementing a preventive policy.

The regular expression engine of the Cisco ASA does not support the end-of-line ($) metacharacter and therefore does not allow you to match a specific custom value that would encompass an entire container (for example, a URI). For example, you cannot match requests that *only* contain the string "/myapp" inside their request URI. Instead, you can match requests whose URIs contain a substring (for example, the substring "app") or requests whose URIs start with a particular prefix, for example "/myapp" (which would also match requests whose URIs may be "/myapps," "/myapplication," and so on).

In addition to pattern-based policies, which are configured in this topic, you should also consider deploying policies that impose length-based restrictions on application layer containers. Such policies can also effectively prevent many overflow attacks.

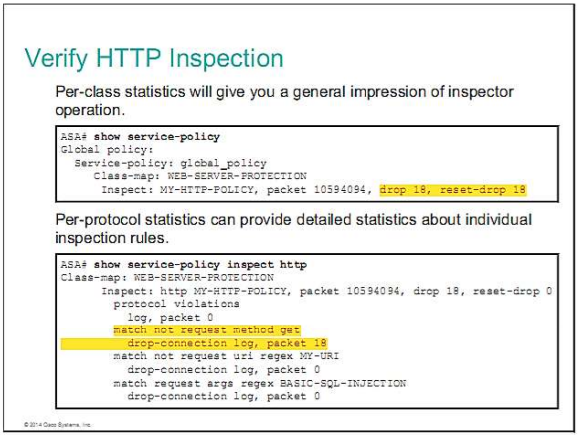
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

A policy that only permits minimal required connectivity is usually the most effective, but also the most difficult to deploy, as you need deep knowledge of all required application transactions. Often, it may be easier to deploy a signature-based approach or a combination of the two, with a more relaxed minimization approach.

https://t.me/learningnets

Verify HTTP Inspection

This topic describes how to verify HTTP inspection.



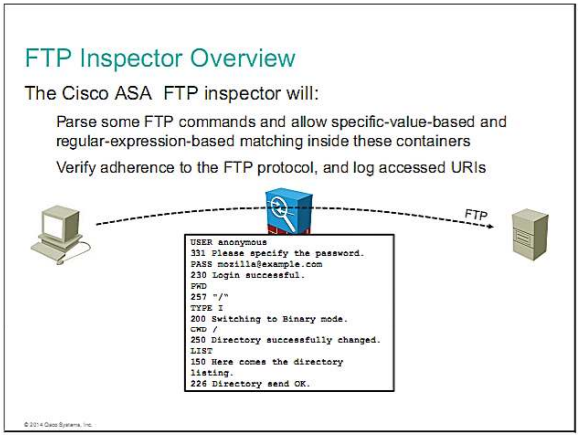
To display some global per-class statistics and gain a general overview of the operation of application layer inspection, use the **show service-policy** command. This command shows whether the inspector is actively inspecting traffic, as indicated by the packet count, and whether packets are being dropped by the inspector.

Use the **show service-policy inspect http** command to display specific statistics for HTTP inspectors and observe the operation of individual matching rules. The example shows that 18 packets have been dropped and logged because the request method is not GET.

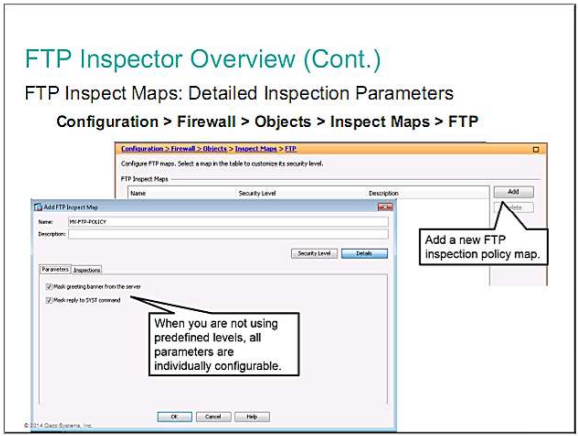
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

FTP Inspector Overview

This topic describes Cisco ASA FTP inspector.

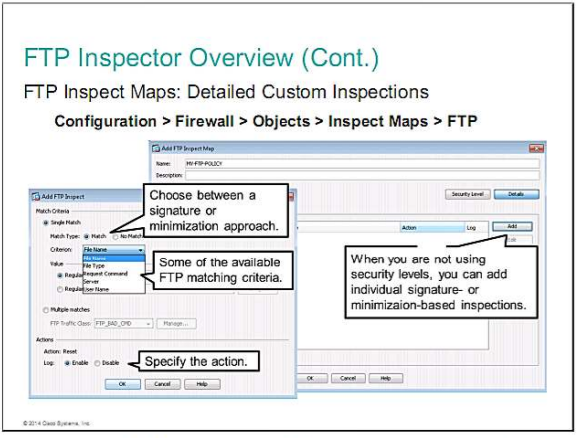


The FTP inspection routines on the Cisco ASA inspect the FTP protocol and break it into containers. Inside these containers, administrators can filter specific protocol values or use regular expressions to create custom pattern matching rules. The FTP inspector on the security appliance also verifies adherence to the FTP protocol and logs all accessed FTP URI objects (files) at the highest level of logging (debugging). Additionally, you can filter FTP access by category using an external URL filtering server in the same manner as with the HTTP and HTTPS protocols.



Just like you did with the HTTP protocol inspector, you can individually select and configure all of the parameters that are available in the FTP inspector by switching to the **Details** view of the Inspect Map window. From this view, you can tune the parameters that are set by the Security Level macros or you can configure the entire policy from inception without initially using the Security Level options.

From the **Parameters** tab, you can individually enable or disable the masking of the FTP server banner and the masking of the response to the FTP SYST command.



From the Inspections tab of the Details pane of the FTP inspector, you can add individual inspection criteria where you can granularly filter on aspects of the FTP protocol and its payloads. To create an inspection rule, click **Add**. The Add FTP Inspect window appears, allowing you to create an inspection rule that is based on the following criteria:

The filename pattern that is uploaded or downloaded through the FTP session

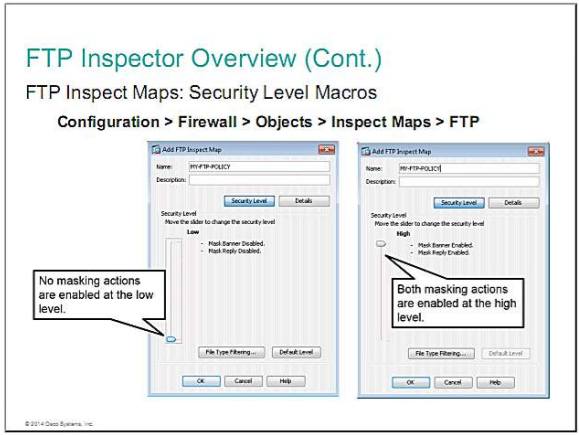
The file type that is uploaded or downloaded through the FTP session

The individual FTP commands that are passed between the client and the server

The server banner that is returned by the FTP server

The name of the user logging on to the FTP server

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



The FTP inspection policy maps for the security appliance allow you to choose between the low and high security levels inside the Add/Edit FTP Inspect Map window.

The low security level does not enable any additional actions except the default protocol verification and URI (file) logging. You can quickly add simple file type filtering rules to this policy using the File Type Filtering button, which will take you to an inspection rule that filters on FTP filenames.

The high security level extends the features of the low security level by masking (hiding) the FTP server banner (hiding the vendor and version of the FTP application from clients). It also extends them by masking the server reply to the FTP SYST command that could help an attacker fingerprint the operating system of the FTP server.

Evaluate Application Inspection of Other Protocols

This topic evaluates application inspection of other protocols.

Evaluate Application Inspection of Other Protocols

Other Available Inspectors

Inspector	Configuration Possibilities
DNS	Protocol verification, request and response filtering, DNS ID, etc.
ESMTP	Protocol verification, sender and recipient filtering, etc.
H.323	Protocol verification, call duration, caller and called party, media type, etc.
SIP	Protocol verification, address hiding, caller and called party, content type, etc.
Skinny (SCCP)	Protocol verification, message ID filtering
IM	Protocol, service, login name, file name, etc.
SNMP	Protocol version
DCE/RPC	Protocol verification

© 2014 Cisco Systems, Inc.

Evaluate Application Inspection of Other Protocols (Cont.)

Other Available Inspectors (Cont.)

Inspector	Configuration Possibilities
MGCP	Gateway and call agent role
NetBIOS	Protocol verification
RTSP	URL, URL length, request method

© 2014 Cisco Systems, Inc.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

The Cisco ASA supports application layer inspection for a handful of other application layer protocols. You can configure the following inspection functionality:

For DNS, the DNS Application Inspection and Control feature on the appliance inspects the DNS protocol and allows administrators to specify access rules that provide protection of DNS clients and servers.

For the ESMTP, the ESMTP inspection features on the appliance examine ESMTP sessions between clients and servers, or among servers, and parse them to verify adherence to the protocol. The features also allow granular filtering to protect ESMTP endpoints that use signatures or minimization rules.

For the H.323 protocol suite, the AIC H.323 inspector on the appliance can perform H.323 protocol verification and filter on various protocol-level aspects, such as call duration, caller ID, called party ID, and media type (audio, video).

For the SIP, the AIC SIP inspector can perform SIP protocol verification, provide privacy features (such as IP address and message path masking) and filter on various protocol-level aspects, such as message content type, caller ID, and called party ID.

For the SCCP protocol, the AIC SCCP inspector can perform SCCP protocol verification and filter messages based on their message IDs.

For IM protocols, the security appliance can filter their sessions based on the IM protocol, IM service (chat, file transfer, and so on), IM login name, filename of transferred files, and so on.

For the SNMP, the SNMP inspector can filter SNMP packets based on the SNMP protocol version.

For the DCE/RPC protocol, the DCE/RPC AIC inspector performs protocol verification with some tuning options.

For the MGCP, the Cisco ASA security appliance can enforce the call agent and gateway roles of all communicating parties based on your static configuration of these roles inside the inspection policy map.

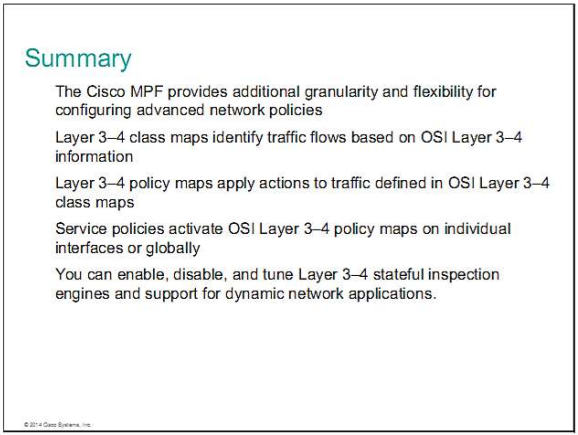
For the NetBIOS protocol, the AIC inspector performs protocol verification.

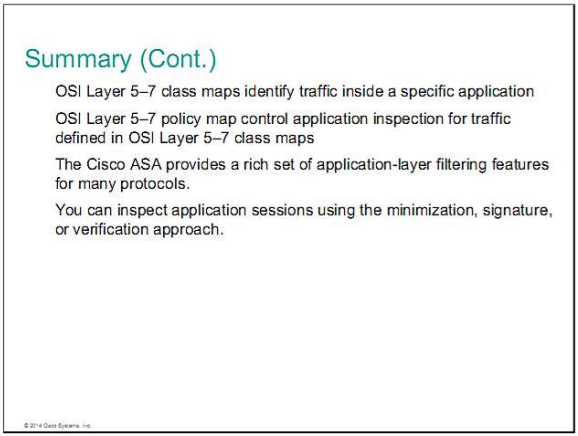
For the RTSP, the RTSP AIC inspector can filter inside RTSP sessions based on the requested URL, its length, and the RTSP request method.

https://t.me/learningnets

Summary

This topic summarizes the key points that were discussed in this lesson.





© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Lesson 4

Deploying Reputation-Based Cisco ASA Access Policies

The Cisco ASA 5500-X Series Next-Generation Firewalls use the Botnet Traffic Filter feature to detect and prevent botnet activity that is detected in transit traffic. The Botnet Traffic Filter feature detects and prevents traffic from bot-infected hosts to their control servers using a reputation-based mechanism. This lesson provides an overview of the Cisco ASA Botnet Traffic Filter, and explains how to configure and verify Cisco ASA Botnet Traffic Filter.

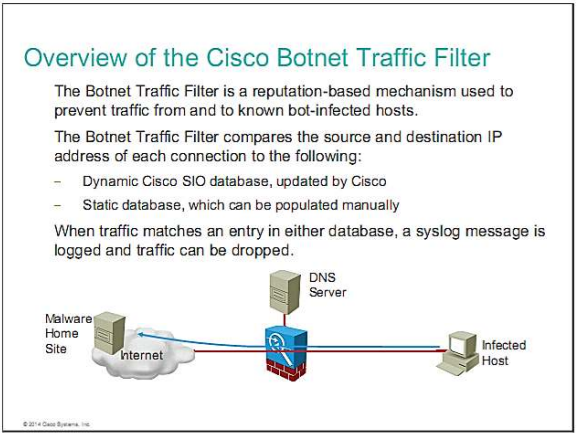
Upon completing this lesson, you will be able to:

- Describe the Cisco ASA Botnet Traffic Filter
- Configure the Cisco ASA Botnet Traffic Filter
- Verify the Cisco ASA Botnet Traffic Filter

https://t.me/learningnets

Overview of the Cisco Botnet Traffic Filter

This topic describes the Cisco ASA Botnet Traffic Filter.



The Cisco ASA uses the Cisco ASA Botnet Traffic Filter feature to detect and prevent botnet activity that is observed in transit traffic.

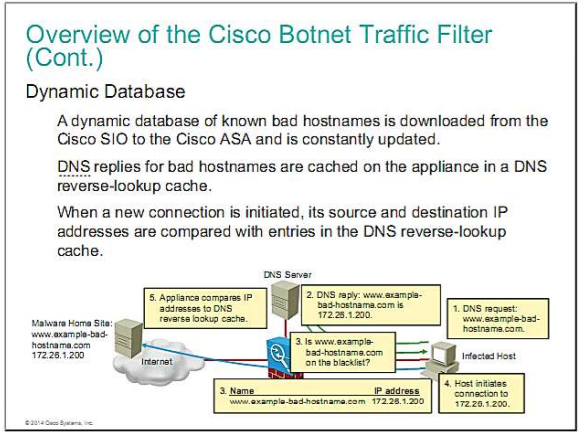
The Botnet Traffic Filter feature detects and prevents traffic from bot-infected hosts to their control servers using a reputation-based mechanism. The Botnet Traffic Filter feature compares the source and destination IP addresses of each connection across the security appliance to entries in two databases:

A dynamic database from Cisco SIO (Security Intelligence Operations), which is updated by Cisco and is dynamically downloaded to the Cisco ASA at periodic intervals

A static database, which you can manually populate by adding good and bad IP addresses and domain names according to your local policy

When traffic transiting through the appliance matches an entry in either database, the Cisco ASA will generate a syslog message and drop the offending traffic, if it is so configured.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



This figure describes how the Botnet Traffic Filter feature uses its dynamic database to detect and drop the botnet traffic. The Botnet Traffic Filter feature receives periodic updates for the dynamic database from the Cisco update server. This database lists thousands of known bad host or domain names and IP addresses that are known to host bots or botnet control channels.

The Cisco ASA uses the dynamic database as follows:

1. An infected host wants to initiate connection to www.example-bad-hostname.com, which is a host acting as a known control host for a botnet. The host issues a DNS request for www.example-bad-hostname.com.
2. The DNS server responds with a DNS reply for the www.example-bad-hostname.com host.
3. The Cisco ASA inspects the DNS reply. When the domain name in the DNS reply matches a name in the dynamic database, the Botnet Traffic Filter adds the name and IP address to a special DNS reverse-lookup cache.
4. The infected host starts a connection to the botnet control site.
5. The security appliance compares the source and destination IP addresses to entries in the DNS reverse-lookup cache. If there is a match, the Cisco ASA sends a syslog message informing you of the suspicious botnet activity, and can have the traffic dropped.

Note In some cases, the IP address is supplied in the dynamic database instead of in the domain name. In these cases, the Botnet Traffic Filter can log or drop any traffic to that IP address without having to inspect the DNS requests.

Note Before you can use the Cisco dynamic database, you must configure a domain name server on the security appliance so that it can access the Cisco dynamic database update server URL.

https://t.me/learningnets

Overview of the Cisco Botnet Traffic Filter (Cont.)

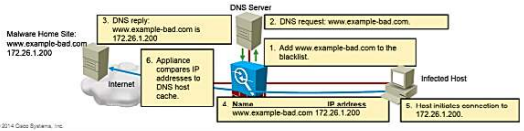
Static Database

You can manually add bad or good hostnames and IP addresses to the static database.

Bad names are added to the blacklist; good names are added to the whitelist.

The Cisco ASA performs a DNS lookup for all statically added names, and adds mappings to the DNS host cache.

When a new connection is initiated, its source and destination IP addresses are compared with entries in the DNS host cache.



In addition to using the dynamic database, you can manually enter domain names or IP addresses into a static database. In the static database, you can add known, good domain names or IP addresses to a whitelist. You can also add known, bad domain names and IP addresses to a blacklist. A whitelist entry always takes precedence over the static or dynamic blacklist entry.

The Botnet Traffic Filter uses ambiguous (graylisted) and unlisted addresses. Unlisted addresses are not in either the dynamic or the static database. The Cisco ASA does not generate syslog messages or statistics when traffic matches unlisted addresses. Ambiguous addresses are associated with multiple domain names, but not all of these domain names are on the blacklist. When you add a domain name to the whitelist or blacklist in the static database, the Cisco ASA security appliance waits 1 minute, and then sends a DNS request for that domain name and adds the domain name or IP address pairing to the DNS host cache.

Note Be sure to configure a DNS server on the appliance so that it can perform DNS resolution of statically added domain names.

If the Cisco ASA cannot access the DNS server to resolve static domain names to IP addresses, the appliance uses its Botnet Traffic Filter DNS snooping feature instead of the regular DNS lookup approach.

The Cisco ASA security appliance uses the static database as follows:

1. **www.example-bad.com** is manually added to the blacklist.
2. The security appliance issues a DNS request for **www.example-bad.com**.
3. The DNS server responds with a DNS reply for **www.example-bad.com**.
4. The Botnet Traffic Filter adds the www.example-bad.com domain and its IP address to a special DNS reverse-lookup cache.
5. The infected host starts a connection to **www.example-bad.com**.
6. The security appliance compares the source and destination IP addresses to entries in the DNS reverse-lookup cache. If there is a match, the security appliance sends a syslog message informing you of the suspicious botnet activity and can drop the suspicious botnet traffic.

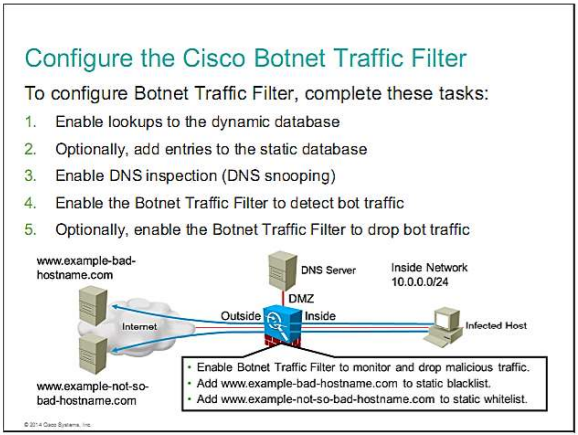
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Note	If you add IP addresses to the static database, the Botnet Traffic Filter logs or drops any traffic to that IP address without having to inspect DNS requests.

https://t.me/learningnets

Configure the Cisco Botnet Traffic Filter

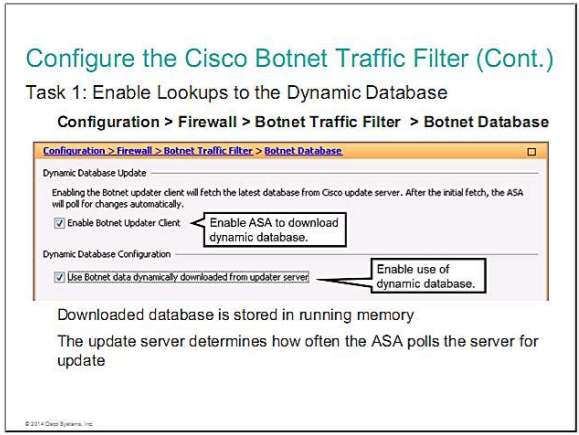
This topic describes how to configure the Cisco ASA Botnet Traffic Filter.



To configure the Botnet Traffic Filter feature on the Cisco ASA, complete the following configuration tasks:

1. Enable dynamic lookups using the dynamic botnet database. This task is recommended if the traffic crossing your security appliance is destined to or coming from the Internet and you want to automatically detect or prevent botnet threats.
2. Optionally, add blacklist entries, whitelist entries, or both to the static database.
3. Enable DNS inspection with Botnet Traffic Filter DNS snooping.
4. Enable the Botnet Traffic Filter feature to detect bot traffic.
5. Optionally, enable the Botnet Traffic Filter feature to drop the botnet traffic.

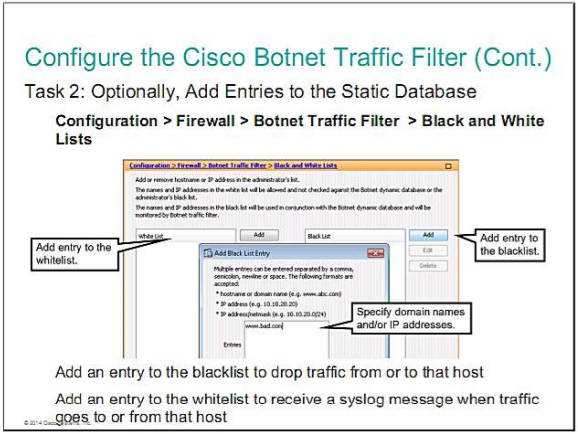
© 2014 Cisco Systems, Inc.
https://t.me/learningnets



To enable use of the dynamic Botnet Traffic Filter database using the Cisco ASDM, complete the following steps:

1. In the Cisco ASDM, navigate to **Configuration > Firewall > Botnet Traffic Filter > Botnet Database**.
2. Enable downloading of the dynamic database by checking the **Enable Botnet Updater Client** checkbox. The update server will determine how often the ASA polls the update server. Typically, this is done every hour which is the default.
3. Enable use of the dynamic database by checking the **Use Botnet data dynamically downloaded from updater server** checkbox.
4. Click **Apply** to apply your configuration.

Note	The database files are stored in running memory; they are not stored in Flash memory. If you need to delete the database, you can use the **Purge Botnet Database** database (not shown in the figure). You can also fetch the database manually for testing purposes using the **Fetch Botnet Database** button (not shown in the figure).

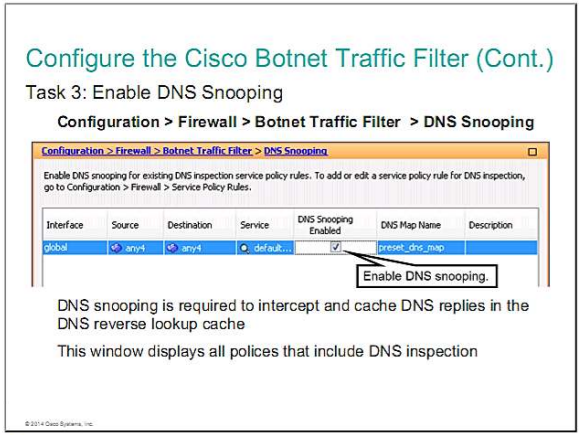


To add entries to the static database, complete the following steps:

1. In the Cisco ASDM, navigate to **Configuration > Firewall > Botnet Traffic Filter > Black and White Lists**.
2. Click the **Add** button in the **White List** area to add a domain name or IP address to the whitelist or click the **Add** button in the **Black List** area to add a domain name or IP address to the blacklist. The **Add White List Entry** or the **Add Black List Entry** is displayed. In the example, the **Add Black List Entry** is displayed. When traffic matches an entry in the static whitelist or blacklist, a syslog message is logged. When traffic matches an entry in the static blacklist, traffic is also dropped if the ASA is configured to do so.
3. Enter the domain name, individual IP address or IP address of a network into the Entries input field. In the example, the www.bad.com host is added to the blacklist.
4. Click **Apply** to apply your configuration.

Note Configure the DNS server for the ASA to resolve static domain names to IP addresses.

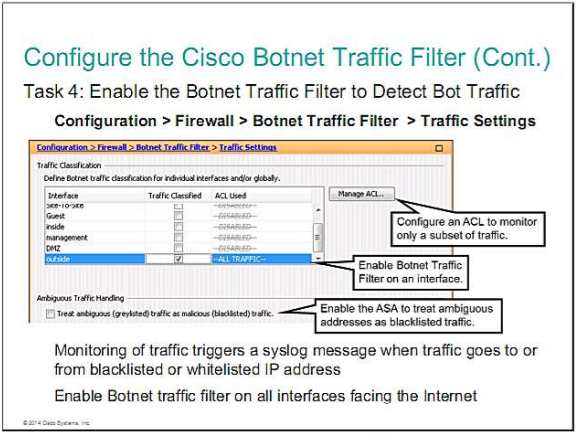
© 2014 Cisco Systems, Inc.
https://t.me/learningnets



To enable the Botnet Traffic Filter DNS snooping component to intercept and cache DNS replies, complete the following steps:

1. In the Cisco ASDM, navigate to **Configuration > Firewall > Botnet Traffic Filter > DNS Snooping**. This window displays you all configured policies that include DNS inspection.
2. Check the **DNS Snooping Enabled** checkbox.
3. Click **Apply** to apply your configuration.

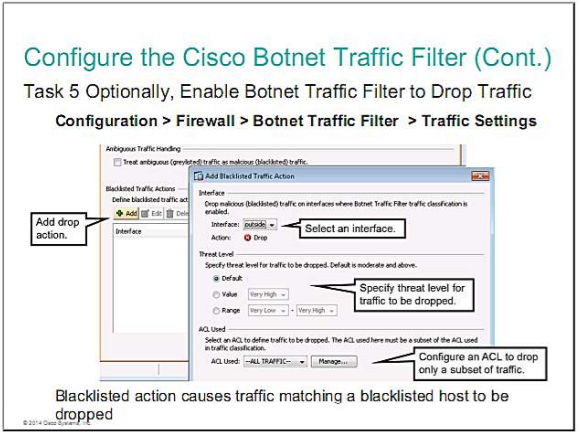
Note	You can also enable DNS inspection with Botnet Traffic Filter DNS snooping using the Service Policy Rules menu.



To enable Botnet Traffic Filter to monitor traffic, complete the following steps:

1. In the Cisco ASDM, navigate to **Configuration > Firewall > Botnet Traffic Filter > Traffic Settings**.
2. In the **Traffic Classification** area, check the **Traffic Classified** check box for each interface on which you want to enable the Botnet Traffic Filter. It is recommended to monitor traffic on all interfaces facing the Internet. In the example, Botnet Traffic Filter is enabled on the outside interface.
3. For each interface, from the ACL Used drop-down list choose either --ALL TRAFFIC-- to monitor all traffic (the default), or any access list configured on the ASA to only monitor a subset of traffic. For example, you might want to monitor all HTTP traffic on the outside interface. To add or edit access lists, click **Manage ACL** to bring up the ACL Manager where you can create or edit access lists. In the example, all traffic is monitored.
4. Click **Apply** to apply your configuration.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



To enable the Botnet Traffic Filter feature to drop malicious traffic, complete the following steps:

1. In the Cisco ASDM, navigate to **Configuration > Firewall > Botnet Traffic Filter > Traffic Settings**.
2. Click **Add** in the **Blacklisted Traffic Actions** section of the panel.
3. From the **Interface** drop-down list, choose the interface on which you want to drop traffic. Only interfaces on which you enabled Botnet Traffic Filter traffic classification are available. In the example, the outside interface is selected.
4. In the **Threat Level** area, choose one of the following options to drop traffic specific threat levels. The options are:

   Default: The default level is a range between **Moderate** and **Very High**.

   Value: Specify the threat level you want to drop:

   - Very Low
   - Low
   - Moderate
   - High
   - Very High

   Range: Specify a range of threat levels. It is recommended to initially set the Threat level to the Default value.
5. In the **ACL Used** area, from the **ACL Used** drop-down list choose either --ALL TRAFFIC—to drop malicious traffic inside all traffic (the default), or any access list configured on the ASA to drop malicious traffic inside specific traffic. If you use an access list, the access list should be a subset of the traffic you specified in the **Traffic Classification** area. To add or edit access lists, click **Manage** to bring up the ACL Manager.
6. Click **Apply** to apply your configuration.

https://t.me/learningnets

Configure Support for Dynamic Protocols (Cont.)

CLI Configuration

```
dynamic-filter updater-client enable
dynamic-filter use-database
!
dynamic-filter enable interface outside
dynamic-filter drop blacklist interface outside
!
dynamic-filter whitelist
 name www.notsobad.com
!
dynamic-filter blacklist
 name www.bad.com
!
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map dynamic-filter-snoop
```

© 2014 Cisco Systems, Inc.

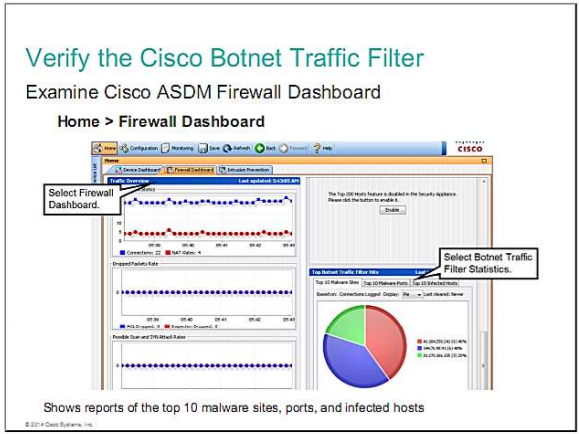
To configure Botnet Traffic Filter on the Cisco ASA device using command line interface, use the commands that are described in the table.

Commands	Description
dynamic-filter updater-client enable **dynamic-filter use-database**	Enable ASA to download dynamic database Enable use of dynamic database
dynamic-filter enable interface outside **dynamic-filter drop blacklist interface outside**	Enable Botnet Traffic Filter to monitor traffic Enable Botnet Traffic Filter to drop traffic
dynamic-filter whitelist **name www.notsobad.com**	Add entries to static whitelist
dynamic-filter blacklist **name www.bad.com**	Add entries to static blacklist
policy-map global_policy **class inspection_default** **inspect dns preset_dns_map dynamic-filter-snoop**	Enable DNS snooping

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Verify the Cisco Botnet Traffic Filter

This topic describes how to verify the Cisco ASA Botnet Traffic Filter.



The Botnet Traffic Filter Hist dashlet shows reports of the top 10 malware sites, ports, and infected hosts. This report is a snapshot of the data, and may not match the top 10 items since the statistics started to be collected. If you right-click an IP address, you can invoke the whois tool to learn more about the botnet site.

Top Malware Sites: Shows top malware sites.

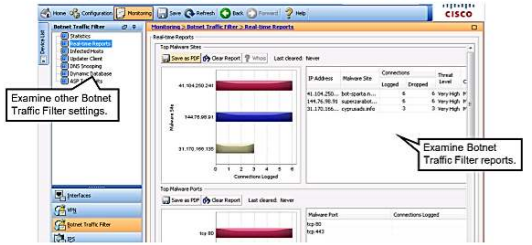
Top Malware Ports: Shows top malware ports.

Top Infected Hosts: Shows the top infected hosts.

Verify the Cisco Botnet Traffic Filter (Cont.)

Examine Cisco ASDM Botnet Traffic Filter Reports

Monitoring > Botnet Traffic Filter > Real-time Reports



Generates reports of the top 10 malware sites, ports, and infected hosts

© 2014 Cisco Systems, Inc.

In Cisco ASDM, you can also generate reports of the top 10 malware sites, ports, and infected hosts that are monitored by navigating to **Monitoring > Botnet Traffic Filter > Real-time Reports**. The top 10 malware-sites report includes the number of connections dropped, and the threat level and category of each site. This report is a snapshot of the data, and may not match the top 10 items since the statistics started to be collected.

If you right-click a site IP address, you can invoke the whois tool to learn more about the malware site. Reports can be saved as a PDF file.

Verify the Cisco Botnet Traffic Filter (Cont.)

Command	Description
show dynamic-filter data	Displays dynamic database information.
show dynamic-filter dns-snoop	Displays the DNS reverse-lookup cache.
show dynamic-filter statistics	Displays how many connections were classified with the Botnet Traffic Filter.
show dynamic-filter reports top malware-sites	Generates reports on the top 10 malware sites.

© 2014 Cisco Systems, Inc.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

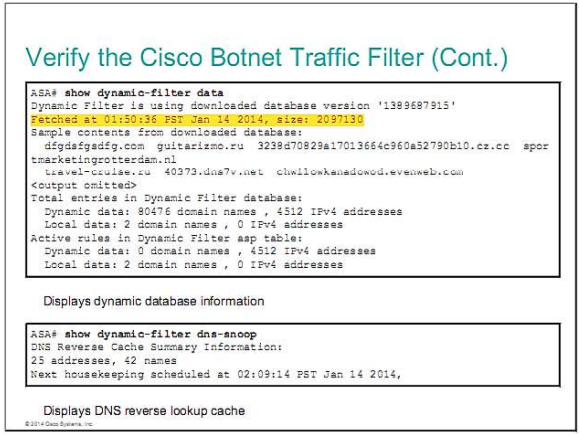
Cisco IOS Software includes the following commands used with Botnet Traffic Filter validation features.

Use the **show dynamic-filter data** command to verify the dynamic database information of the Botnet Traffic Filter.

Use the **show dynamic-filter dns-snoop** command to examine the DNS reverse-lookup cache.

Use the **show dynamic-filter statistics** command to display the statistics about connections that are monitored with the Botnet Traffic Filter, and how many of those connections matched the whitelist, the blacklist, and the graylist.

Use the **show dynamic-filter reports top malware-sites** command to generate reports of the top 10 malware sites, ports, and infected hosts that are classified by the Botnet Traffic Filter.



The **show dynamic-filter data** command displays the following information:

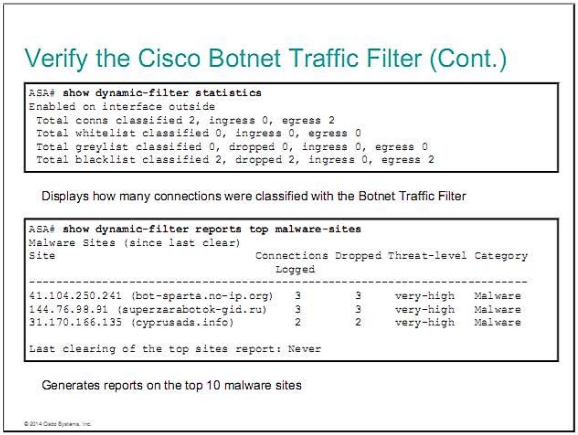
The version of the database

The time the database was last downloaded

The number of entries that the database contains

Up to 10 sample entries

The **show dynamic-filter dns-snoop** command displays only the summary of the DNS reverse-lookup cache. To display actual mappings between domain names and IP addresses, use the **show dynamic-filter dns-snoop detail** command.



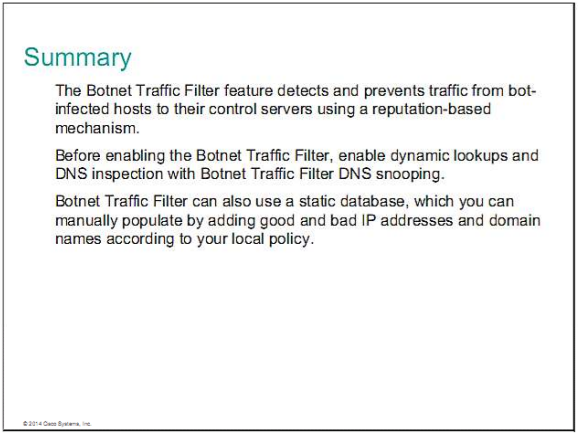
To display the statistics on connections monitored with the Botnet Traffic Filter, and how many of those connections matched the whitelist, the blacklist, and the greylist, use the **show dynamic-filter statistics** command.

To generate reports of the top 10 malware sites, ports, and infected hosts classified by the Botnet Traffic Filter, use the **show dynamic-filter reports top** command. The printout in the figure show output for top 10 malware sites.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Summary

This topic summarizes the key points that were discussed in this lesson.



https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lesson 5

Deploying Identity-Based Cisco ASA Access Policies

Users in an enterprise often need access to one or more server resources. Typically, a firewall is not aware of user identities and, therefore, cannot apply security policies based on identity. To configure per-user access policies, you must configure a user authentication proxy, which requires user interaction (a user name/password query).

The Identity Firewall in the Cisco ASA provides granular access control based on user identities. You can configure access rules and security policies based on usernames and a user group name rather than through source IP addresses. The Cisco ASA applies the security policies based on an association of IP addresses to Windows Active Directory login information and reports events based on the mapped usernames instead of on the network IP addresses.

The Identity Firewall integrates with the Microsoft Active Directory in conjunction with an external Cisco Context Directory Agent that provides the actual identity mapping. The Cisco ASA uses the Windows Active Directory as the source to retrieve current user identity information for specific IP addresses and allows transparent authentication for Active Directory users.

Identity-based firewall services enhance the existing access control and security policy mechanisms by allowing users or groups to be specified in place of source IP addresses. Identity-based security policies can be interleaved without restriction between traditional IP address-based rules.

This lesson describes how to configure, verify and troubleshoot the Cisco ASA Identity Firewall.

Upon completing this lesson, you will be able to:

- Describe the Cisco ASA Identity Firewall
- Describe the Cisco ASA Identity Firewall process flow, using a sequence of figures
- Describe Cisco CDA
- Configure the Cisco CDA to integrate with Microsoft Active Directory and with Cisco ASA
- Verify Cisco CDA integration with Microsoft Active Directory
- Configure the Cisco ASA to integrate with Microsoft Active Directory and with Cisco CDA

https://t.me/learningnets

Verify Cisco ASA integration with Microsoft Active Directory and with Cisco CDA

Configure identity-based access rules

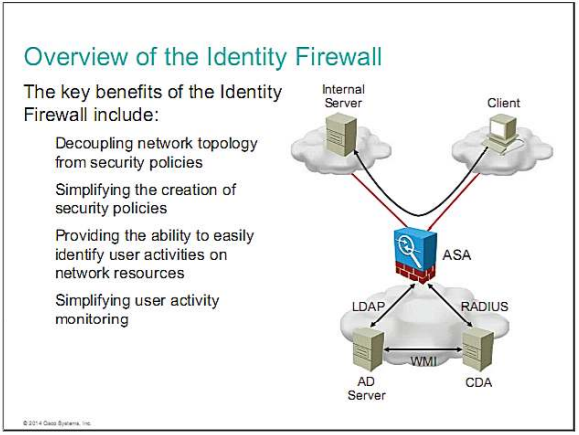
Verify the identity-based firewall

Troubleshoot identity-based firewall

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Overview of the Identity Firewall

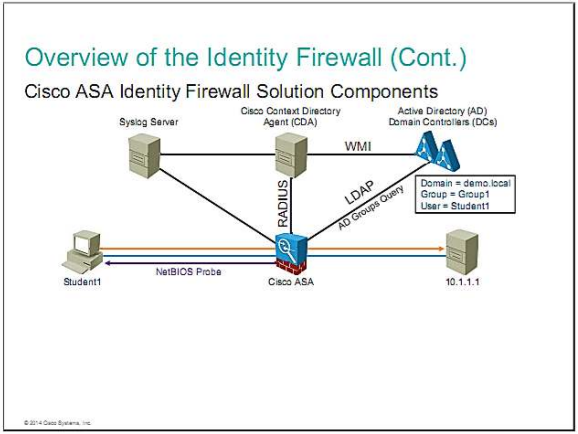
This topic describes the Cisco Adaptive Security Appliance Identity Firewall.



The Cisco ASA Identity Firewall solution provides granular access control, based on user identity. For example, the network administrator can set up a network in which only engineers can access an engineering lab and only marketing staff can access a marketing lab. Without knowing a user identity, the firewall cannot properly apply the user identity based on access control. Currently, to configure per-user policies, the network administrator can use the Cisco ASA cut-through proxy feature, which requires user interactions. Cisco ASA prompts users to enter their usernames and passwords before they can receive the required network access, whereas the identity-based firewall allows security policy definitions based on the username or user group name rather than the IP address. The Cisco ASA Identity Firewall solution works in the Active Directory environment and in tandem with the existing 5-tuple information (protocol, source or destination IP address, and source or destination port), based on access rules.

The benefits of the Cisco ASA Identity Firewall solution include the following:

- Increased flexibility and simplicity in policy creation by decoupling the policy from the network topology
- Decreased cost of creating and maintaining security policies
- Better visibility of who is doing what



The three main components of the Cisco ASA Identity Firewall solution are the Cisco ASA device, Cisco Context Directory Agent, and Microsoft Active Directory domain controllers.

The Cisco ASA device does the following:

- Downloads Active Directory user-group and group-membership information from the Active Directory domain controllers, via LDAP
- Receives IP-to-user address mapping information from Cisco CDA, via RADIUS
- Applies ACL or MPF security policies, based on the Active Directory user or user-group identity

Cisco CDA does the following:

- Monitors the Active Directory domain controller login security log events, via Microsoft WMI
- Sends the IP-to-user address mapping information to Cisco ASA, via RADIUS
- Provides user IP-to-user address mapping information to other Cisco security devices, such as the Cisco Web Security Appliance and Cisco ASA CX.
- Uses a web-based GUI for Cisco CDA system configurations and uses a CLI (similar to the Cisco IOS Software CLI) for basic network-setup configurations

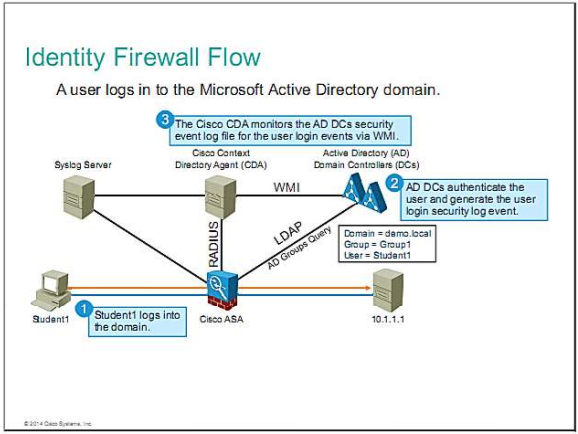
Active Directory is a directory service that Microsoft created for Windows domain networks. Active Directory provides a central location for network administration and security. Server computers that run Active Directory are called domain controllers and do the following:

- Authenticate Windows users in the domain
- Generate user login security log events
- Reply to the Cisco ASA LDAP query for Active Directory user-group information

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

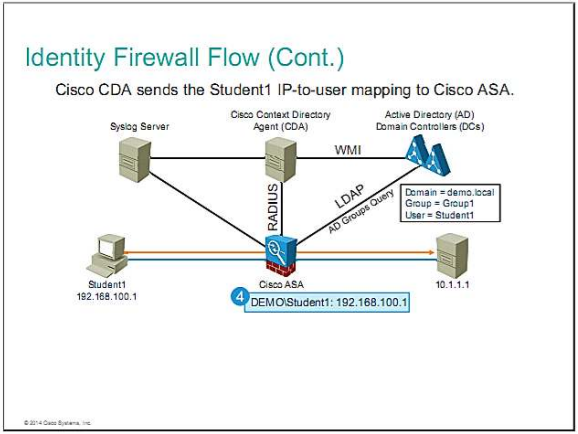
Identity Firewall Flow

This topic describes the Cisco Adaptive Security Appliance Identity Firewall process flow, using a sequence of figures.



The figures in this topic follow the process flow of the Cisco ASA Identity Firewall solution:

1. The user Student1 logs into the Active Directory demo.local domain.
2. The Active Directory domain controllers authenticate the user and generate the user login security log event.
3. Cisco Context Directory Agent monitors the Active Directory domain controller security log event file by using Microsoft WMI for user login and logout events. All security events are pushed by the Active Directory domain controller to Cisco CDA, in real time. This usually takes 1 to 2 seconds, unless the Active Directory domain controllers are under stress. Cisco CDA stores the IP-to-user mapping information for Student1.



When interacting with Cisco CDA, the Cisco ASA device can be configured in one of two modes: on-demand or full-download.

Full-download: Cisco ASA sends a bulk request to Cisco CDA, to download the entire IP-user mapping table when Cisco ASA starts and then to receive incremental IP-user mapping information when users log in or out.

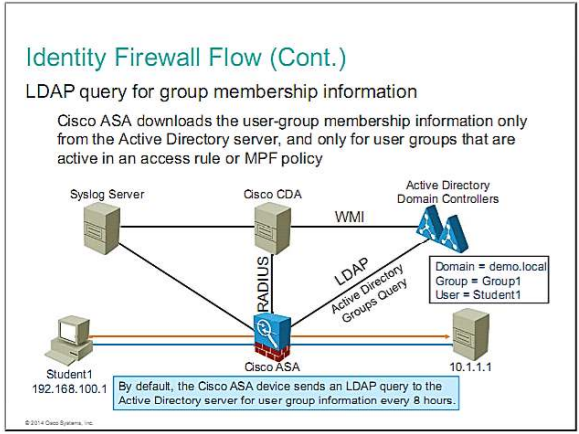
On-demand: Cisco ASA sends on-demand requests to Cisco CDA to retrieve specific IP-user mapping information, only when required. With on-demand mode and identity firewall configured (ingress ACL applied to the interface), the source IP of every incoming connection is checked against the identity database first. If there is no match in on-demand mode, the ASA will do a query to CDA in an attempt to resolve the user identity. If it does, the appropriate ACL rules are enforced. If not, only regular (non identity based) ACL rules are applied to the user traffic.

Note	For the Cisco ASA 5505 Adaptive Security Appliance, which has limited memory and CPU power and is usually deployed in a limited network environment to support only 1024 or fewer users, the default mode is the on-demand mode. The default mode on all other Cisco ASA platforms is the full-download mode.

As the figure shows, Cisco ASA is using full-download mode:

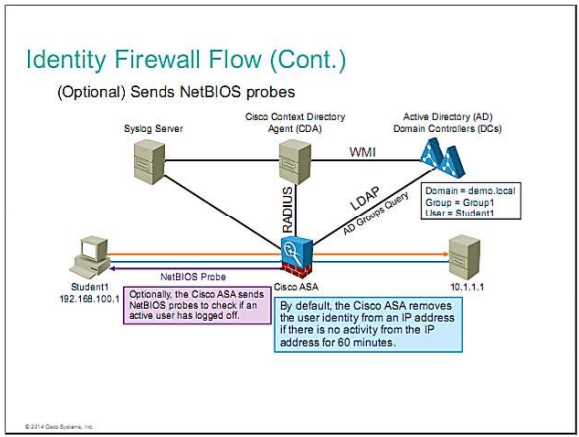
4. The Student1 user login event triggers Cisco CDA to immediately send an update to Cisco ASA to provide the user IP address-to-user mapping information.
5. In this example, Student1 in the DEMO domain has the 192.168.100.1 IP address.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



The Cisco ASA access rules or MPF-based security policies can also be Active Directory user-group-based instead of user-based. Cisco ASA uses an LDAP query to retrieve the Active Directory user-group memberships information directly from the Active Directory domain controllers. By default, Cisco ASA refreshes the Active Directory group-membership information every 8 hours. If a user is added to a group, the user is not recognized as being a member of the group until the next update. Cisco ASA downloads the user-group membership information only from the Active Directory server, and only for user groups that are active in an access rule or MPF policy.

As the figure shows, Cisco ASA learns the Group1 Active Directory group information from the Active Directory domain controllers. Group1 currently has one member: Student1 in the DEMO domain.



The Microsoft Windows Active Directory logout-detection mechanism has certain constraints. Windows might not accurately report logout events to the Active Directory domain controllers, under all conditions. For example, a user can suspend and undock a laptop and move it to another location rather than logging out. Or if a user turns off a computer without logging out, Windows does not have an opportunity to generate the logout event until the system restarts. Therefore, some logout events are logged much later than the time at which they actually occur. The Active Directory domain controllers might not detect these events, and the user IP addresses, while still valid on both Cisco CDA and Cisco ASA, might already be used by other users.

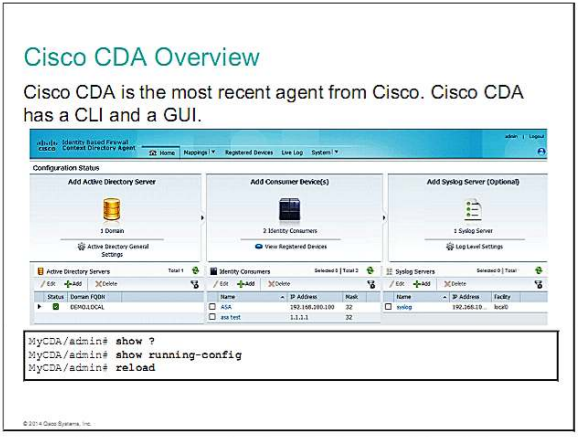
To cause the user identity of IP addresses to expire, Cisco ASA by default removes the user identity from an IP address when there is no activity from the IP address for 60 minutes. To improve the accuracy of IP-to-user mappings, the Cisco ASA can be configured to send NetBIOS probes (if NetBIOS traffic is permitted in the network) to a user machine to determine whether active users have logged out of their machines. By default, when NetBIOS probes are enabled, the Cisco ASA waits 15 minutes before probing the IP address of an active user.

The NetBIOS probes support IPv4 but not IPv6. In Microsoft Windows 7 and Windows Vista, NetBIOS traffic is blocked by the Windows firewall, by default. A user needs to enable NetBIOS traffic in the Windows firewall. For NetBIOS probes to work, the network between Cisco ASA and all the end-user stations must allow UDP-encapsulated NetBIOS traffic. This traffic consists of NetBIOS query packets with any UDP source port directed to UDP port 137 and NetBIOS query responses from UDP port 137 directed to any source port that is sent in the NetBIOS query.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Cisco CDA Overview

This topic describes Cisco Context Directory Agent.



Cisco CDA is an application that runs on Linux CentOS. Cisco CDA is installed as an ISO image, either on a physical hardware server or as a VM. Cisco CDA has both a CLI and GUI. All the system configurations are performed by using the GUI. The CLI is used mainly to initially set up Cisco CDA on the network (IP address, network mask, default gateway, DNS settings, NTP settings, etc.) and to perform maintenance tasks, such as backing up the system configurations to an FTP server.

Cisco CDA monitors, in real time, a collection of Microsoft Active Directory domain controller machines for authentication-related security events. These events indicate user logins and logouts, by using WMI. Cisco CDA caches mappings of IP addresses and user identities in its database. The agent also makes the most recent mappings available to connected consumer devices, such as Cisco Adaptive Security Appliance.

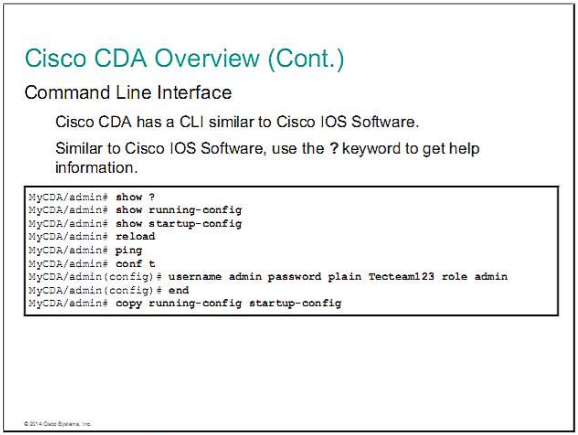
Consumer devices interact with Cisco CDA by using RADIUS, to obtain the most recent set of IP-to-user mappings in one of two modes:

On-demand: Cisco CDA responds to an on-demand query from the consumer device for a specific IP-to-user mapping.

Full-download: The consumer device downloads the complete current IP address-to-user mapping database from Cisco CDA, when the consumer device first boots. The device then receives incremental mapping information from Cisco CDA.

The older Cisco Active Directory Agent 1.0 is a Microsoft Windows-based application. Active Directory Agent has only a CLI, with no web-based GUI configuration. Cisco CDA provides the same functionalities as Active Directory Agent, with the addition of a web-based GUI that is used for system configurations. The flows and semantics between Cisco CDA, consumer devices, and Active Directory domain controllers remain the same as in Active Directory Agent.

https://t.me/learningnets



The figure shows some of the CLI commands that are available, such as **show running-config**, **reload**, and **ping**. As with Cisco IOS Software, use the **conf t** command to enter global configuration mode. From global configuration mode, you can change the various network settings.

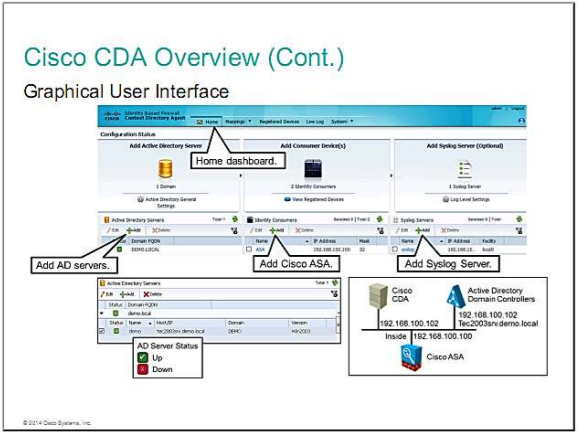
Cisco CDA also supports Cisco Discovery Protocol, which is enabled by default.

The **username** CLI global configuration mode command is used to manage the user accounts that are used for CLI access. The user accounts that are used for web-based GUI access are managed separately, by using the GUI. Both CLI and GUI users are assigned a role (privilege level) of either "admin" or "user." By default, the administrator using the setup dialog has the admin role, which is assigned both CLI and GUI access. CLI users with the admin role can access all the CLI commands. CLI users with the user role have limited CLI access. For example, CLI users with the user role cannot enter global configuration mode and cannot show the running configurations.

The CLI is used mainly during the initial setup of the Cisco CDA appliance and for performing system-maintenance functions, such as backing up and restoring the Cisco CDA application and all of its system-configuration data.

Refer to the *Installation and Configuration Guide for Context Directory Agent, Release 1.0* for more information about the available CLI commands.

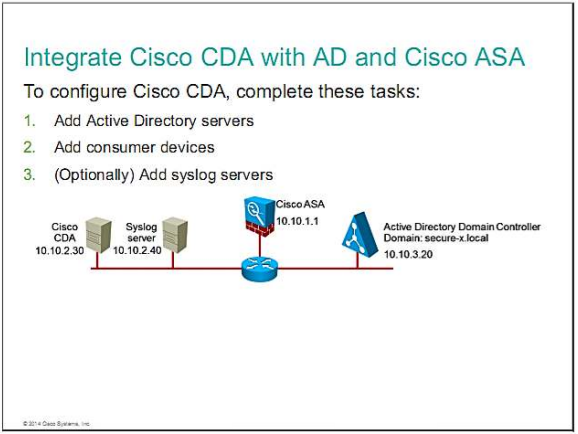
© 2014 Cisco Systems, Inc.
https://t.me/learningnets



When logging in to the GUI for the first time after installing Cisco CDA, use the "admin" user credential that was created during the setup CLI dialog. The figure shows the Cisco CDA home page dashboard, which provides "dashlets" to quickly create, edit, or delete Active Directory servers, consumer devices (such as Cisco ASA), and syslog servers. Other dashlets provide lists of existing Active Directory servers, consumer devices, and syslog servers. In addition, the dashboard provides links to Active Directory general settings, a registered devices page, and log level settings. To go back to the dashboard from any other page, click **Home**.

Integrate Cisco CDA with AD and Cisco ASA

This topic describes how to configure the Cisco Context Directory Agent to integrate with Microsoft Active Directory and with Cisco ASA.

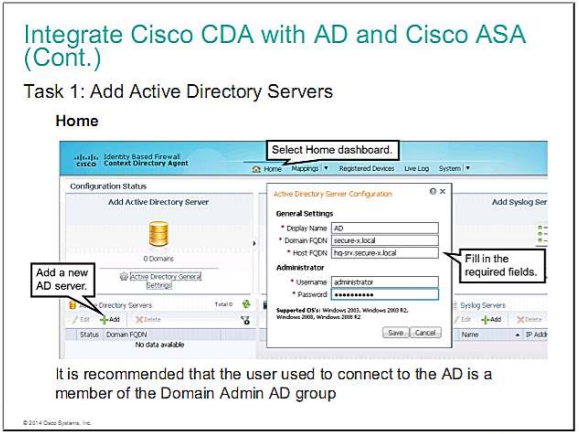


To configure Cisco CDA, complete the following configuration tasks:

1. Add Active Directory servers to configure CDA integration with Microsoft Active Directory
2. Add consumer devices, such as Cisco Adaptive Security Appliance, that are responsible for actively retrieving (and/or passively receiving) the latest IP-to-user-identity mappings from the Cisco CDA
3. Optionally add syslog servers to enable the Cisco CDA to send administrative and troubleshooting information to a syslog server.

The figure shows a configuration scenario that will be used in the upcoming configuration tasks. The scenario assumes that the Cisco CDA has been installed and configured with the basic networking settings. You will configure the Cisco CDA with the Active Directory server, then you will add the Cisco ASA as the customer device, and finally you will configure syslog server on the Cisco CDA.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



Cisco CDA communicates with the Active Directory domain controllers to obtain IP-to-user mapping information, by using WMI. Active Directory domain controllers can be added, edited, or deleted from the Cisco CDA home page Active Directory Servers section.

The figure shows an example of the Active Directory server configuration:

The Active Directory server name to be displayed on the GUI is "AD"

The FQDN for the Active Directory domain is "secure-x.local."

The Active Directory server FQDN is "hq-srv-secure-x.local."

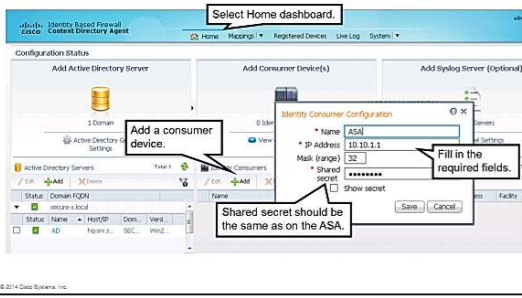
The Active Directory server administrator account login name is "administrator".

Note It is recommended, but not required, that the user that is used to connect the Cisco CDA to the Microsoft Active Directory is a member of the Domain Admin AD group. Consult the procedures in "Active Directory Requirements for Successful Connection with Cisco CDA" part of the Cisco CDA installation guide for the Windows Server setup and user account requirements.

Integrate Cisco CDA with AD and Cisco ASA (Cont.)

Task 2: Add Consumer Devices

Home



Consumer devices can be added, edited, or deleted from the Cisco CDA home page Identity Consumer section. This lesson covers using the Cisco ASA as a Cisco CDA consumer device for the purpose of implementing identity-based firewall rules in Cisco ASA. The use of Cisco ASA CX and Cisco Web Security Appliance as consumer devices is not covered in this lesson.

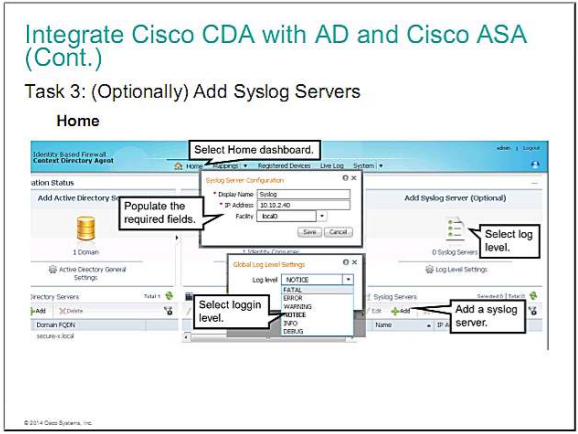
The figure shows an example of the Identity Consumer configuration:

The identity consumer name to be displayed on the GUI is set to ASA.

The IP address of the Cisco ASA is set to 10.10.1.1.

The shared secret between this Cisco ASA device and Cisco CDA is set to cisco123. This must match the shared secret that is configured on the Cisco ASA device.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



Cisco CDA can forward logs that contain administrative and troubleshooting information to one or more syslog servers. The contents of these logs are identical to that of the logs that are locally available on the Cisco CDA appliance. Syslog servers can be added, edited, or deleted from the Cisco CDA home page Syslog Servers section.

The figure shows an example of the Syslog Servers configuration:

The syslog server name to be displayed on the GUI is set to Syslog.

The IP address of the syslog server is set to 10.10.2.40, using the default Facility of local0.

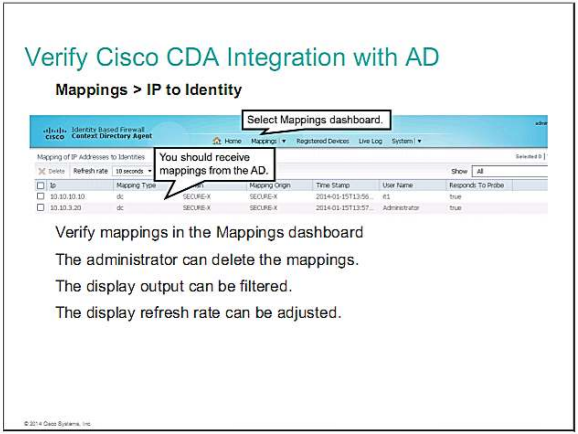
As the figure also shows, from the Cisco CDA home page Syslog Servers section, click the **Log Level Settings** link to open the Global Log Level Settings page. Use this page to globally configure log-level settings. These settings are used for the logs that are sent to syslog servers and for the logs that are stored on the Cisco CDA device, and which can be viewed in the GUI under live logs.

Cisco CDA provides these log levels: Fatal, Error, Warning, Notice, Info, and Debug. The default level is Notice, which means that only messages that are labeled as Notice or above are reported. For customer troubleshooting, the recommended level is Info; for Cisco TAC support, the recommended level is Debug.

Note	Using debug-level logging might affect system performance.

Verify Cisco CDA Integration with AD

This topic describes how to verify Cisco Context Directory Agent integration with Microsoft Active Directory.



The Cisco CDA IP to Identity page lists all the current IP-to-user mappings and allows the administrator to refresh, filter, and delete the mappings. The default screen refresh rate is 10 seconds, which can be adjusted to 20 seconds, 30 seconds, 1 minute, 2 minutes, or none. The figure shows the GUI screen for monitoring IP-to-user mappings. From the Cisco CDA home page, click **Mapping** and choose **IP to Identity**.

If there is no User to IP mappings on the Cisco CDA, one of the cause maybe the clock on the Cisco CDA and Active Directory server is not synchronized.

In the figure, Cisco CDA has two active IP-to-user mapping, in which the it1 user in the SECURE-X domain is mapped to the 10.10.10.10 IP address, and user Administrator is mapped to the 10.10.3.20 IP address.

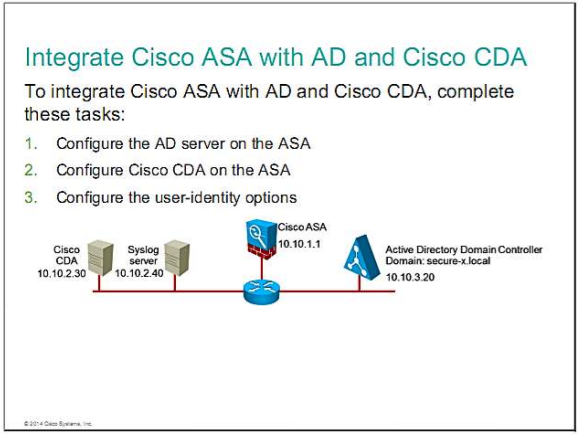
Users can have multiple IP addresses if they are logged in to multiple machines. So if an ACL rule matches the user, then the rule will match the user on either IP address.

From the IP to Identity page, click the filter icon on the top right-hand side to open the filter options. The IP to Identity display can be filtered based on IP address, Message Type, Domain, Mapping Origin, Time Stamp, User Name, and Responds to Probe. When Response to Probe is set to true for a mapping, Cisco ASA uses NetBIOS probes at the predefined interval and notifies Cisco CDA if this IP mapping is no longer valid.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Integrate Cisco ASA with AD and Cisco CDA

This topic describes how to configure the Cisco Adaptice Security Appliance to integrate with Microsoft Active Directory and with Cisco Context Directory Agent.



The figure lists the three main tasks to configure the Cisco ASA to integrate with Microsoft Active Directory and with Cisco CDA:

1. Configure the Active Directory servers in Cisco ASA.
2. Configure the Cisco CDA device in Cisco ASA as a RADIUS server.
3. Configure the identity-based firewall options in Cisco ASA.

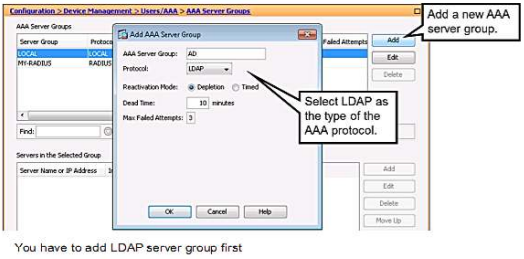
The figure also shows a configuration scenario that will be used in the upcoming configuration tasks. You will first configure the Cisco ASA with the Active Directory server, then you will add the Cisco CDA to the ASA as the RADIUS server, and finally you will enable identity options on the Cisco ASA.

https://t.me/learningnets

Integrate Cisco ASA with AD and Cisco CDA (Cont.)

Task 1: Configure the AD Server on the ASA

Configuration > Device Management > Users/AAA > AAA Server Groups

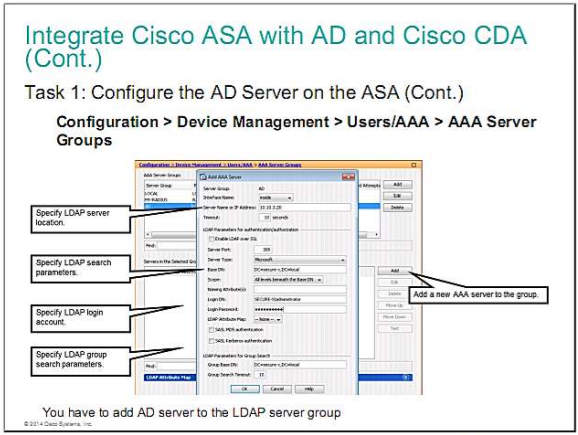


To configure the AD server on the Cisco ASA using Cisco ASDM, you have to add a AAA server group first.

Complete the following steps to add a AAA server group:

1. In the Cisco ASDM, navigate to **Configuration > Device Management > Users/AAA > AAA Server Groups**.
2. Click **Add** in the **AAA Server Groups** section of the pane.
3. Enter the name of the AAA server group into the **Server Group** input field. The example in the figure uses the name AD.
4. Select **LDAP** as the protocol that is used to communicate with the Active Directory server.
5. Click **OK**.
6. Click **Apply** to apply the configuration.

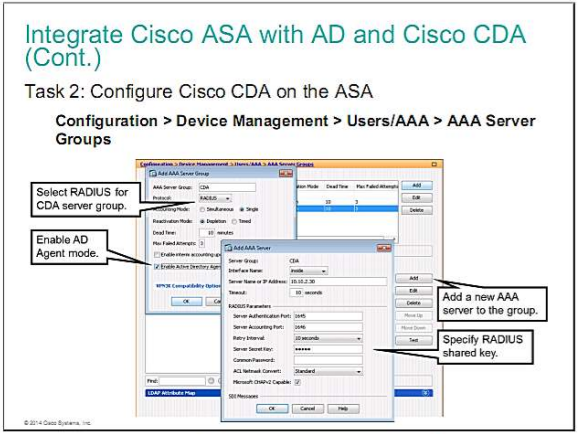
© 2014 Cisco Systems, Inc.
https://t.me/learningnets



When you are done with adding the server group, you have to add a server to the group.

To add a server to the LDAP server group using Cisco ASDM, complete the following steps.

1. In the **AAA Server Groups** pane, make sure that the LDAP server group is selected.
2. Click **Add** in the Servers in the Selected Groups section of the pane.
3. Choose the Cisco ASA interface that connects to the Active Directory server. In the example in the figure, the Active Directory server is connected to the inside interface.
4. Enter the Active Directory server FQDN or server IP address. In the example, the Active Directory server IP address is 10.10.3.20.
5. Optionally, click the **Enable LDAP over SSL** check box to enable encryption between Cisco ASA and the Active Directory server. By default, if LDAP over SSL is not enabled, then the default server port is 389. If LDAP over SSL is enabled, then the default server port is 636. Choose **Microsoft** as the Server Type.
6. Specify the location in the LDAP hierarchy where the Active Directory server should begin searching when it receives an authorization request. In the example, the Base DN is set to DC=secure-x and DC=local. Specify the extent of the search in the LDAP hierarchy that the Active Directory server should make when it receives an authorization request from Cisco ASA. The default is to search one level beneath the base DN. In the example, **Search All Levels Beneath the Base DN** is chosen (a subtree search).
7. Enter the login DN and password for Cisco ASA, to log in to the domain. In the example, SECURE-X \administrator is used as the login DN.
8. Specify group base DN where the Active Directory server should begin searching for AD groups. In the example, group base DN is set to DC=secure-x and DC=local.
9. Click **OK**.
10. Click **Apply** to apply the configuration.



When configuring Cisco CDA on the ASA, you have to first configure AAA server group and then add the CDA server to the group.

To add AAA server group using Cisco ASDM, complete the following steps:

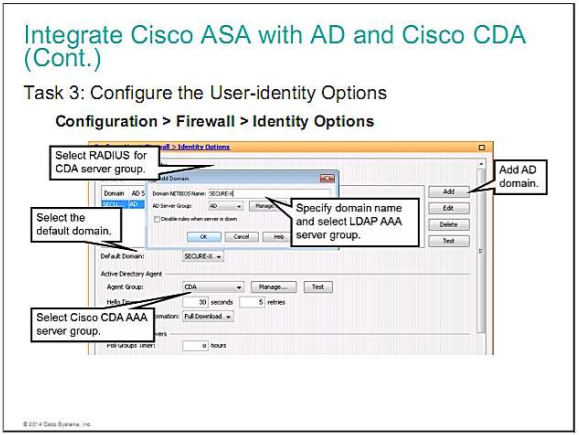
1. In the Cisco ASDM, navigate to **Configuration > Device Management > Users/AAA > AAA Server Groups**.
2. Click **Add** in the **AAA Server Groups** section of the pane.
3. Enter the name of the AAA server group. In the example, the name is CDA.
4. Select **RADIUS** as the protocol that is used to communicate with Cisco CDA.
5. Check the **Enable Active Directory Agent mode** checkbox to specify that a RADIUS server group includes AD agents that are not full-function RADIUS servers.
6. Click **OK**.
7. Click **Apply** to apply the configuration.

To add the CDA server to the RADIUS server group using Cisco ASDM, complete the following steps:

1. In the **AAA Server Groups** pane, make sure that the RADIUS server group is selected.
2. Click **Add** in the Servers in the Selected Groups section of the pane.
3. Choose the Cisco ASA interface that connects to the Cisco CDA server. In the example, the Cisco CDA is connected to the inside interface.
4. Enter the Cisco CDA FQDN or IP address. In the example, the CDA server IP address is 10.10.2.30.
5. The Cisco CDA can use either UDP port 1645 or UDP port 1812 for RADIUS authentication messages.
6. The Cisco CDA can use either UDP port 1646 or UDP port 1813 for RADIUS accounting messages.
7. Enter the Server Secret Key. This is the shared secret key between the Cisco ASA and the Cisco CDA. The key must match the configuration on the Cisco CDA.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

8. Click **OK**.
9. Click **Apply** to apply the configuration.

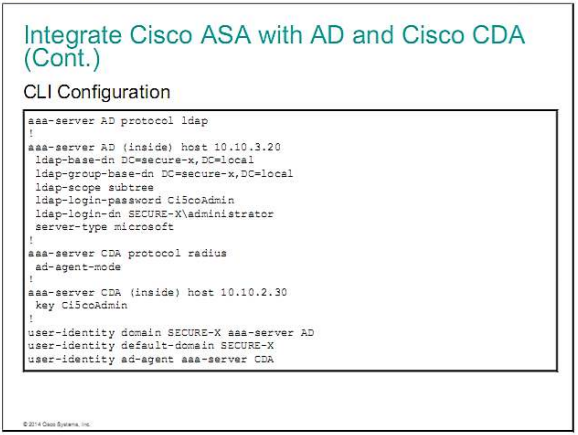


To configure user-identity options using Cisco ASDM, complete the following steps:

1. In the Cisco ASDM, navigate to **Configuration > Firewall > Identity Options**.
2. Click **Add**. Specify domain NETBIOS name and select the previously configured LDAP AAA server group. In the example, SECURE-X is used as the domain name and AD AAA server group is selected. Click **OK**.
3. Select the default domain. In the example, SECURE-X is used as the default domain.
4. Select the CDA AAA server group from the **Agent Group** drop-down menu. In the example, CDA server group is selected.
5. Optionally, specify how frequently Cisco ASA exchanges hello packets with Cisco CDA. Cisco ASA uses the hello packet to obtain the Cisco ASA user-to-IP mapping status (in-sync or out-of-sync) and the Active Directory domain status (up or down) from the Cisco CDA. If Cisco ASA does not receive a response from Cisco CDA, then Cisco ASA resends a hello packet after the specified interval. By default, the hello timer is set to 30 seconds and five retries.
6. Optionally select how Cisco ASA will retrieve the IP-to-user mappings from Cisco CDA. The two modes are on-demand and full-download. Full-download specifies that Cisco ASA sends a bulk request to Cisco CDA to download the entire IP-user mapping table when Cisco ASA starts, and then to receive incremental IP-to-user mapping information when users log in and out. On-demand mode specifies that Cisco ASA sends an on-demand request to Cisco CDA to retrieve specific IP-to-user mapping information only when required. For the Cisco ASA 5505 Adaptive Security Appliance, which has limited memory and CPU power and is usually deployed in a limited network environment to support only as many as 1024 users, the default mode is on-demand mode. The default mode on all other Cisco ASA platforms is full-download mode.

https://t.me/learningnets

7. Optionally, adjust the time for how often Cisco ASA polls the Active Directory server for Active Directory group-membership information. If a user is added to or deleted from an Active Directory group, the Cisco ASA receives the updated user group after this timer expires. By default, this timer is set to every 8 hours.
8. Click **Apply** to apply the configuration.



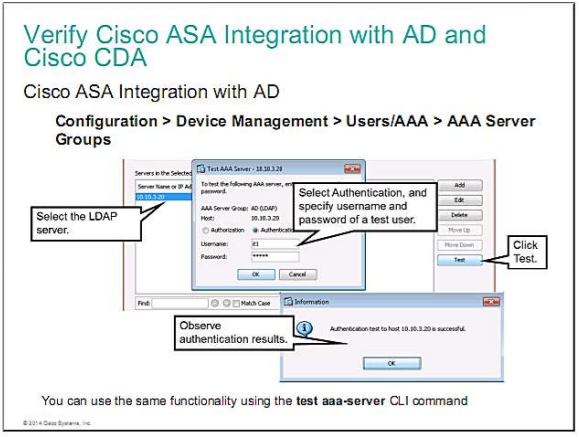
To integrate Cisco ASA with Microsoft Active Directory and Cisco CDA for identity-based firewall using command line interface, use the commands that are described in the table.

Commands	Description
aaa-server AD protocol ldap	Creates LDAP AAA server group
aaa-server AD (inside) host 10.10.3.20 **ldap-base-dn DC=secure-x,DC=local** **ldap-group-base-dn DC=secure-x,DC=local** **ldap-scope subtree** **ldap-login-password Ci5coAdmin** **ldap-login-dn SECURE-X\administrator** **server-type microsoft**	Configures LDAP server in the LDAP server group
aaa-server CDA protocol radius **ad-agent-mode**	Creates RADIUS AAA server group and enables AD agent mode
aaa-server CDA (inside) host 10.10.2.30 **key Ci5coAdmin**	Configures CDA server in the CDA server group
user-identity domain SECURE-X aaa-server AD **user-identity default-domain SECURE-X** **user-identity ad-agent aaa-server CDA**	Configures user-identity options.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Verify Cisco ASA Integration with AD and Cisco CDA

This topic describes how to verify Cisco Adaptive Security Appliance integration with Microsoft Active Directory and with Cisco Context Directory Agent.



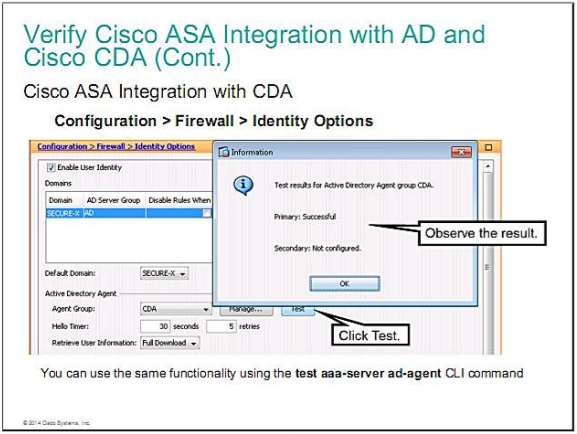
You can use the **Test** functionality in the Cisco ASDM to verify if the ASA can communicate with the AD server.

You can use the Test AAA server group functionality in the Cisco ASDM to verify if the ASA can communicate with the AD server:

1. In Cisco ASDM, navigate to **Configuration > Device Management > Users/AAA > AAA Server Groups**.
2. Select the LDAP server group and select the AD server.
3. Click the **Test** button. In the window that opens, select the **Authentication** radio button and specify username and password of a test user. In the example, **it1** is used as the test user. Click **OK**.
4. Observe the result of the test. In the example, the test was successful.

You can use the same functionality by using the **test aaa-server** CLI command. The following is an example of the command output:

```
ASA# test aaa-server authentication AD host 10.10.3.20 username it1 password cisco
INFO: Attempting Authentication test to IP address <10.10.3.20> (timeout: 12 seconds)
INFO: Authentication Successful
```



You can use the **Test** functionality in the Cisco ASDM to verify if the ASA can communicate with the CDA server.

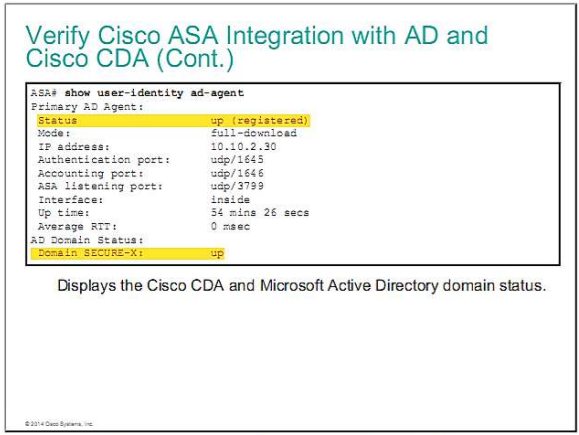
You can use the Test Active Directory Agent functionality in the Cisco ASDM to verify if the ASA can communicate with the CDA server:

1. In Cisco ASDM, navigate to **Configuration > Firewall > Identity Options**.
2. Click the **Test** button.
3. Observe the result of the test. In the example, the test was successful.

You can use the same functionality by using the **test aaa-server ad-agent** CLI command. The following is an example of the command output:

```
ASA# test aaa-server ad-agent CDA host 10.10.2.30
INFO: Attempting Ad-agent test to IP address <10.10.2.30> (timeout: 12 seconds)
INFO: Ad-agent Successful
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

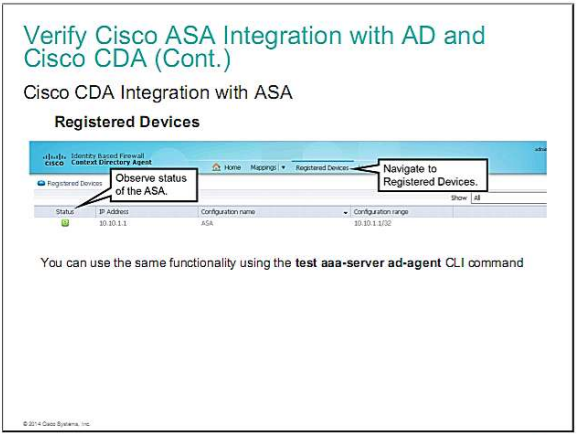


Use the **show user-identity ad-agent** command to verify the Cisco CDA status.

As the figure shows, both the Cisco CDA status and Active Directory domain status should be in the up state.

This command output also displays information about the mode of operations (on-demand or full-download) between the Cisco ASA and Cisco CDA devices. This information shows that the IP address of the Cisco CDA device and the ports that are used for RADIUS communications between Cisco ASA and Cisco CDA. The output also shows the Cisco ASA interface to which Cisco CDA connects, that the Cisco CDA device is up, and the average RTT time.

Cisco ASA is also listening on UDP port 3799. Cisco CDA uses UDP port 3799 to send notifications to Cisco ASA.



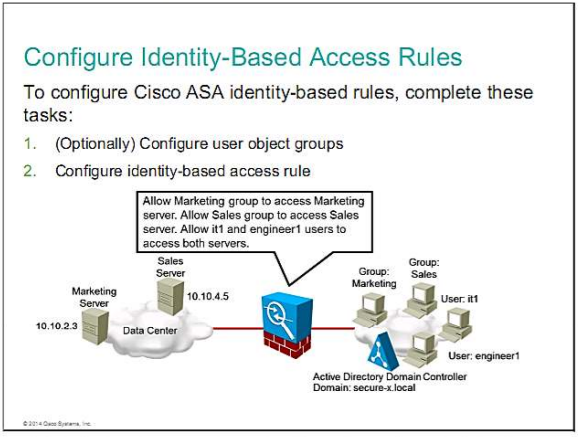
The Registered Devices page displays a list of consumer devices that are connected to Cisco CDA and that are subscribed to receive IP-to-identity mapping updates (on-demand or full-download). To view all the registered devices, click the **Registered Devices** tab in the home page. Or from the home page, click the **View Registered Devices** link in the **Add Consumer Device(s)** section to open the Registered Devices page (which is not shown in the figure).

The figure shows that the Cisco ASA device with the 10.10.1.1 IP address is the only registered device.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Configure Identity-Based Access Rules

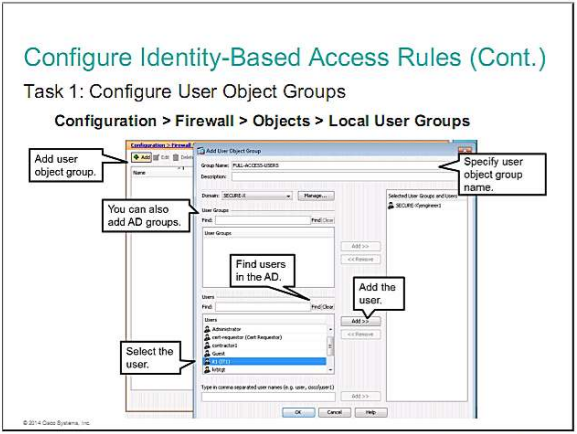
This topic describes how to configure identity-based access rules.



To configure the identity-based access rules on the Cisco ASA, perform the following tasks:

1. Optionally configure user object groups which allows you to group Active Directory users and groups
2. Configure identity-based access rules

The figure shows a configuration scenario that will be used for the upcoming configuration tasks. You will allow the Marketing AD group to access the Marketing server and Sales AD group to access the Sales server. You will also create a user object group consisting of it1 and engineer1 users and allow them access to both servers.

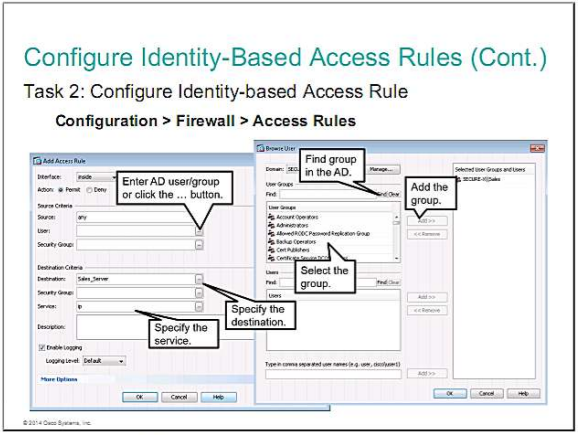


In the first task of this configuration sequence, you will configure a user object group that will include the it1 and engineer1 users.

Perform the following steps to configure a user object group:

1. In the Cisco ASDM, navigate to **Configuration > Firewall > Objects > Local User Groups**.
2. Click **Add** to add new group. The **Add User Object Group** pane will display.
3. Enter a name for the user object group into the **Group Name** input field. In the example, the name of the group is FULL-ACCESS-USERS.
4. In the **Users** section of the pane, click **Find** to list all users in the AD. You can also specify a filter to find only a subset of users in the AD.
5. Select a required user and click the **Add >>** button. Repeat this step to add all required users. In the example, engineer1 and it1 users are being added to the group
6. Similarly, by navigating to the **User Groups** section of the pane, you could also add an AD group to the user object group
7. Click **OK**.
8. Click **Apply** to apply your configuration.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



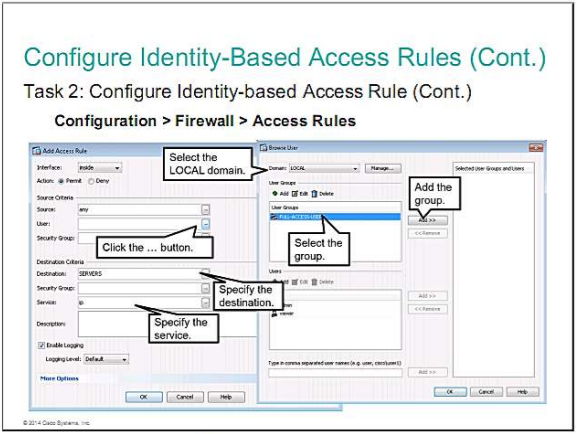
In the first part of the second task of this configuration sequence, you will configure an access rule that will allow the Sales AD group access to the Sales server.

Perform the following steps to configure a user-based access rule:

1. In the Cisco ASDM, navigate to **Configuration > Firewall > Access Rules** (not shown in the figure).
2. Select the interface you want to create the ACL rule on. Click **Add**. The Add Access Rule window will display.
3. Make sure that the correct interface is selected.
4. Select the action. In the example, **Permit** action is selected.
5. In the **Source Criteria** section of the window, enter the AD group name into the **User** input field or click the ... button to find the group in the AD. If you click the ... button, the **Browse User** window is displayed.
6. In the **User Groups** section of the pane, click **Find** to list all groups in the AD. You can also specify a filter to find only a subset of groups in the AD.
7. Select a required group and click the **Add >>** button. In the example, Sales group has been added.
8. Click **OK**.
9. Fill in the rest of the required information, such as destination IP address or object (or object group) and service. In the example, the Sales_Server object is specified as destination and all IP traffic is specified as a service.
10. Click **OK**.
11. Click **Apply** to apply your configuration.

Similarly you would create another rule to allow the Marketing group to access the Marketing server.

https://t.me/learningnets

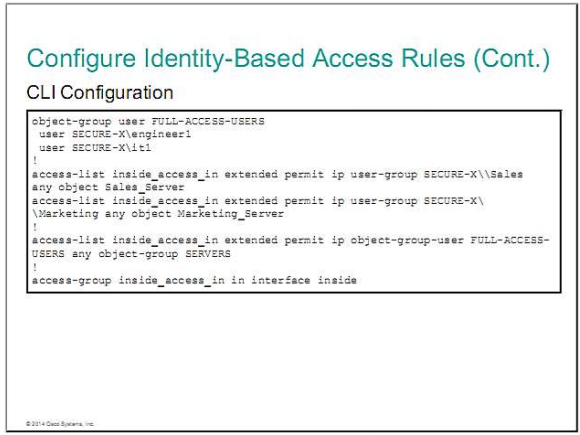


In the second part of the second task of this configuration sequence, you will configure an access rule to allow the FULL-ACCESS-USERS object group to access both servers.

Perform the following steps to configure the user-based access rule:

1. In the Cisco ASDM, navigate to **Configuration > Firewall > Access Rules** (not shown in the figure).
2. Select the interface you want to create the ACL rule on. Click **Add**. The Add Access Rule window will display.
3. Make sure that the correct interface is selected.
4. Select the action. In the example, **Permit** action is selected.
5. In the **Source Criteria** section of the window, click the ... button. The **Browse User** window is displayed.
6. Select **LOCAL** from the Domain drop-down menu.
7. Select a required local group and click the **Add >>** button. In the example, FULL-ACCESS-USERS group has been selected.
8. Click **OK**.
9. Fill in the rest of the required information, such as destination IP address or object (or object group) and service. In the example, the SERVERS object is specified as destination and all IP traffic is specified as a service.
10. Click **OK**.
11. Click **Apply** to apply your configuration.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

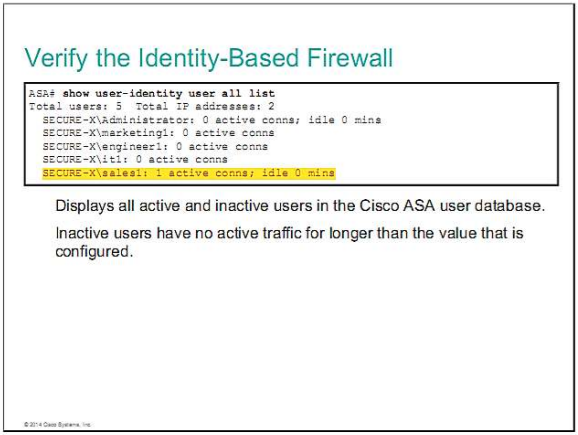


To integrate Cisco ASA with Microsoft Active Directory and Cisco CDA for identity-based firewall using command line interface, use the commands that are described in the table.

Commands	Description
object-group user FULL-ACCESS-USERS **user SECURE-X\engineer1** **user SECURE-X\it1**	Creates an user object group and references AD domain users
access-list inside_access_in extended permit ip user-group SECURE-X\\Sales any object Sales_Server **access-list inside_access_in extended permit ip user-group SECURE-X\\Marketing any object Marketing_Server**	Creates ACL entries that use AD group as the source
access-list inside_access_in extended permit ip object-group-user FULL-ACCESS-USERS any object-group SERVERS	Creates an ACL entry that uses local user object group as the source
access-group inside_access_in in interface inside	Applies the ACL to the inside interface in inbound direction

Verify the Identity-Based Firewall

This topic describes how to verify the identity-based firewall.



Use the **show user-identity user all list** command to display all the users (referenced in an active policy) in the Cisco Adaptive Security Appliance user database. This includes both active and inactive users. The output also shows which users have active connections.

Inactive users have no active traffic for longer than the value that is configured with the **user-identity inactive-user-timer** command. The IP address of an inactive user is marked as inactive and removed from the Cisco ASA IP-to-user mappings.

In the figure, the output shows all the active and inactive users in the Cisco ASA user database.

In this example, only the SECURE-X\sales1 user currently has an active connection on Cisco ASA.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Verify the Identity-Based Firewall (Cont.)

```
ASA# show user-identity user active list detail
Total active users: 2    Total IP addresses: 2
  LOCAL: 0 users, 0 IP addresses
  SECURE-X: 2 users, 2 IP addresses
  SECURE-X\Administrator: 0 active conns; idle 0 mins
    10.10.3.20: login 3 mins, idle 0 mins, 0 active conns
  SECURE-X\sales1: 1 active conns; idle 0 mins
    10.10.10.10: login 644 mins, idle 0 mins, 1 active conns
```

Displays all of the active users

```
ASA# show user-identity ip-of-user SECURE-X\sales1
SECURE-X\10.10.10.10 (Login)
```

Displays the IP address of the demo\student1 active user

© 2014 Cisco Systems, Inc.

Use the **show user-identity user active list detail** command to display information about all the active users. In the figure, Cisco ASA has two active users, SECURE-X\Administrator, who has the IP address 10.10.3.20, and SECURE-X\sales1, who has the IP address 10.10.10.10. The sales1 user has logged in for 644 minutes with one active connection.

Use the **show user-identity ip-of-user** command to display the IP address of a particular user. In the figure, the SECURE-X\sales1 user has the IP address 10.10.10.10, and the user is currently logged in to the DEMO domain.

Verify the Identity-Based Firewall (Cont.)

Monitoring > Properties > Identity > Users



Cisco ASDM Identity Firewall monitoring options:

- Monitoring the Cisco CDA
- Monitoring groups
- Monitoring memory usage for the Identity Firewall
- Monitoring users for the Identity Firewall

© 2014 Cisco Systems, Inc.

To monitor the Identity Firewall by using the Cisco Adaptive Security Device Manager (Cisco ASDM), choose **Monitoring > Properties > Identity** and monitor the following options:

Monitoring Active Directory Agents: This pane displays the following information about the primary and secondary Cisco CDA (not shown in the figure):

- Status of the Cisco CDAs
- Status of the domains
- Statistics for the Cisco CDAs

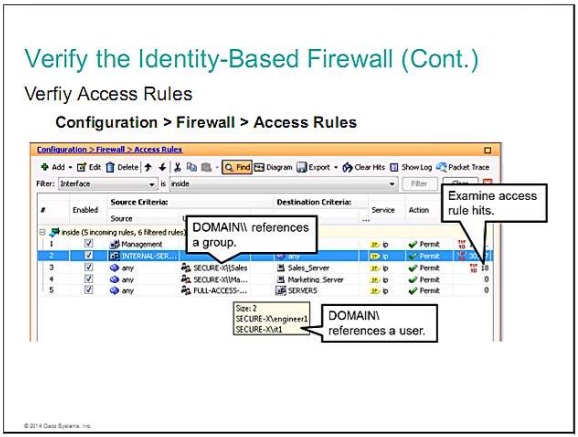
Monitoring Groups: This pane displays the list of user groups in the *domain\group_name* format (not shown in the figure).

Monitoring Memory Usage for the Identity Firewall: This pane displays the memory usage in bytes of various modules in the Identity Firewall (not shown in the figure):

- Users
- Groups
- User statistics
- LDAP

Monitoring Users for the Identity Firewall: This pane displays the following information for users (shown in the figure):

- domain\user_name
- Status (active or inactive)
- Connections
- Minutes idle



Use the **Configuration > Firewall > Access Rules** ADSM panel to verify configured user-based access rules and hit statistics.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

In the figure, the first user-based ACE in the ACL that is applied inbound to the inside interface permits all IP traffic that is sourced from the Sales Active Directory group in the SECURE-X domain to the Sales server destination. The users in the Sales group can have any IP address.

In the figure, the secnd user-based ACE in the ACL that is applied inbound to the inside interface permits all IP traffic that is sourced from the Marketing Active Directory group in the SECURE-X domain to the Marketing server destination. The users in the Marketing group can have any IP address.

In the figure, the third ACE in the ACL that is applied inbound to the inside interface permits all IP traffic that is sourced from the engineer1 or it1 user in the Active Directory in the SECURE-X domain to both marketing and slaes servers. The users can have any IP address.

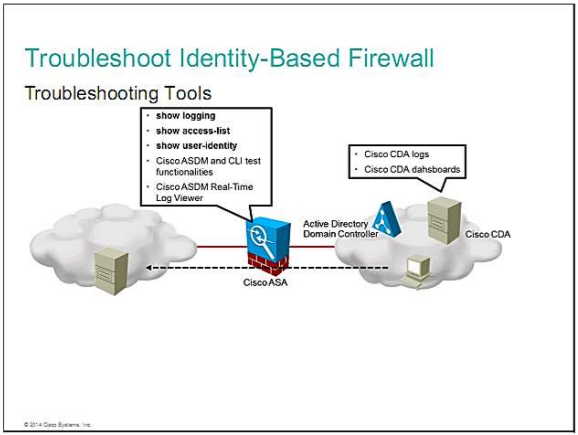
To reference an Active Directory user group in an ACE when manually entering the group, use a "\\" after the domain name; for example, SECURE-X\\group1. To reference an Active Directory user in an ACE when manually entering the user, use a "\" after the domain name; for example, SECURE-X\user1.

Users and user group names are not case-sensitive.

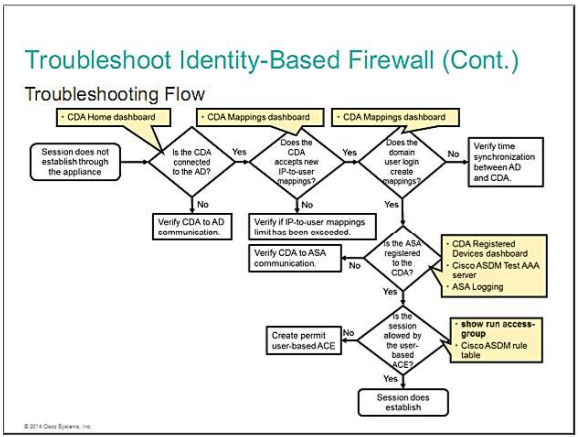
https://t.me/learningnets

Troubleshoot Identity-Based Firewall

This topic describes how to troubleshoot identity-based firewall.



To troubleshoot issues that are related to identity-based firewall, you can use a set of Cisco Adaptive Security appliance CLI, Cisco Adaptive Security Device Manager, and Cisco Context Directory Agent verification features. The figure lists some common commands and features that you might find useful during the troubleshooting session. Typically, you will examine why a particular session cannot be established through the security appliance.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

This figure shows the recommended task flow for troubleshooting identity-based firewall on the Cisco ASA.

Follow these steps and use the provided commands to troubleshoot events where a host appears to have connectivity issues due to the identity-based firewall:

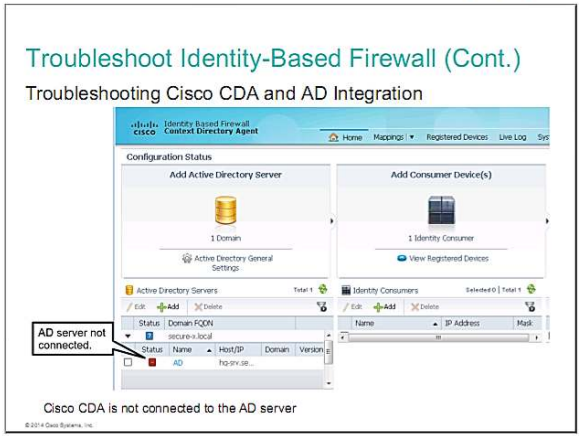
First, determine whether the Cisco CDA is connected to the AD server. You can verify this condition by examining the Cisco CDA Home dashboard. The green checkbox next to the AD domain and server indicates successful connection. If the CDA is not connected to the AD, verify CDA to AD connectivity. Verify if a firewall blocks communication on required ports. You should also verify requirements for user account that is used to connect to the AD, and the Window Server setup requirements.

Then verify if the CDA accepts new IP-to-user mappings. Determine whether the IP-to-user mapping limit of 200,000 has been exceeded. The recommended limit is 64,000. From the Cisco CDA GUI, use the counter in the IP-to-user mappings table to see the current IP-to-user mapping count.

Next, determine whether Microsoft Windows user login does trigger the IP-to-user mapping. If not, determine whether the clock of the Active Directory domain controllers is within 10 minutes of the Cisco CDA clock. Use an NTP server to synchronize the clocks.

Then verify if the Cisco ASA is registered to the Cisco CDA. You can do this by verifying the Cisco CDA Registered Devices dashboard, or by testing Cisco CDA to Cisco ASA communication from the Cisco ASDM or CLI. If the communication is not successful, verify connectivity between the CDA and ASA, and verify that the shared secret between Cisco ASA and Cisco CDA is the same.

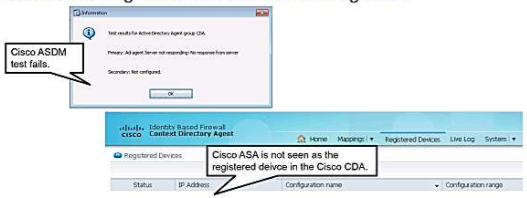
Finally, verify if the user-based ACE on the Cisco ASA allows communication for hosts to a specific destination. If a rule does not allow the communication, then you should create a permit access rule.



The figure shows an example when the Cisco CDA is not connected to the AD server, as indicated by the red flag next to the AD server. In such example, either the Active Directory domain controllers are down, or communication between the Cisco CDA and AD server is blocked by a firewall. You should also verify if the AD user account and Windows server setup met the requirements as required by the Cisco CDA installation and configuration guide.

Troubleshoot Identity-Based Firewall (Cont.)

Troubleshooting Cisco CDA and ASA Integration



Cisco ASA is not registered to the Cisco CDA

```
%ASA-3-746005: user-identity: The AD Agent 10.10.2.30 cannot be reached - No
response - Retry
```

Logging message that indicates connectivity problem between Cisco CDA and Cisco ASA

© 2014 Cisco Systems, Inc.

The figure shows two symptoms when communication between the Cisco ASA and Cisco CDA is not successful. The reason could be connectivity problem between the Cisco ASA and Cisco CDA, or misconfigured shared RADIUS key. In such case, make sure that the Cisco ASA is configured on the Cisco CDA as the consumer device, and that the RADIUS shared key is the same on both ends. The figure also shows the Cisco ASA logging message, which indicates that the ASA cannot reach the Cisco CDA.

Troubleshoot Identity-Based Firewall (Cont.)

Cisco CDA Open Ports

Port	Protocol	Service
22	TCP	SSH
80	TCP	HTTP Redirected to HTTPS
123	UDP	NTP
443	TCP	HTTPS (GUI)
1645	UDP	RADIUS (Authenticating)
1646	UDP	RADIUS (Accounting)
1812	UDP	RADIUS (Authenticating)
1813	UDP	RADIUS (Accounting)

© 2014 Cisco Systems, Inc.

The figure shows the ports that Cisco CDA uses for communication with consumer devices, such as Cisco ASA and with the Active Directory domain controllers. These ports are open by default on Cisco CDA.

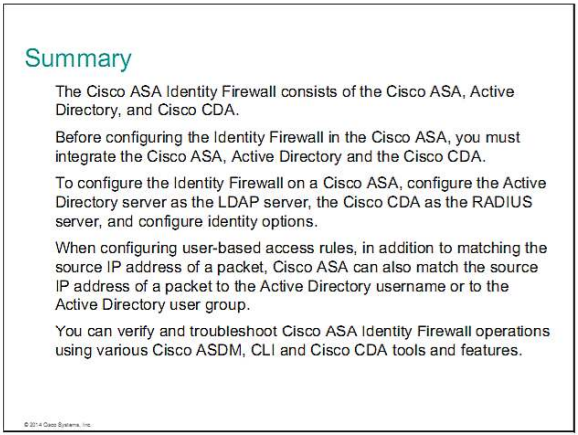
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Cisco ASA is also listening on UDP port 3799. Cisco CDA uses UDP port 3799 to send notification information to Cisco ASA.

https://t.me/learningnets

Summary

This topic summarizes the key points that were discussed in this lesson.

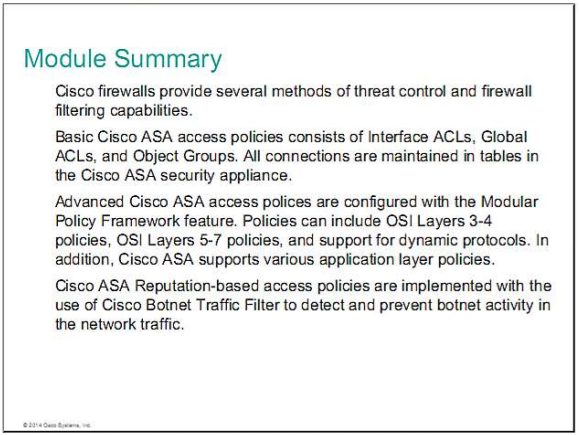


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Module Summary

Overview

This topic summarizes the key points that were discussed in this module.



https://t.me/learningnets

Module Summary (Cont.)

The Cisco ASA Identity Firewall services enhance the existing access control and security policy mechanisms, and consist of the Cisco ASA, Active Directory, and Cisco CDA.

© 2014 Cisco Systems, Inc.

https://t.me/learningnets

Module Self-Check

Questions

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

1. Minimally, where are firewall threat controls usually implemented? (Choose two.) (Source: Introducing Cisco Firewall Threat Controls)

   A. User VLANs
   B. Internet edge
   C. Intranet data center
   D. Sensitive internal subnets

2. Which two are true of stateful packet filtering technology? (Choose two,) (Source: Introducing Cisco Firewall Threat Controls)

   A. Offers reliable access control on layers 3 and 4
   B. Typically used for a permissive approach
   C. Works best for static TCP applications
   D. Requires a more complex configuration
   E. Offers high performance

3. By default, which two protocols does the the Cisco ASA security appliance statefully inspect? (Source: Deploying Basic Cisco ASA Access Policies)

   A. TCP
   B. ICMP
   C. UDP
   D. ESP
   E. GRE

https://t.me/learningnets

4. Which type of access rule is matched first when both interface and global ACLs are configured? (Source: Deploying Basic Cisco ASA Access Policies)

   A. Implicit deny ip any any interface access list rule
   B. Interface access rules
   C. Implicit deny ip any any global access list rule
   D. Global access rules

5. The Cisco Modular Policy Framework consist of which three main components? (Choose three.) (Source: Deploying Advanced Cisco ASA Access Policies)

   A. Class maps
   B. Service policy
   C. Interface ACLs
   D. Netflow collector
   E. Policy maps

6. What must be configured when implementing application layer inspection? (Source: Deploying Advanced Cisco ASA Access Policies)

   A. Regular expressions
   B. Class map for OSI layers 3-4
   C. Class map for OSI layers 5-7
   D. Application layer signatures

7. What must be configured when using the Cisco SIO dynamic database? (Source: Deploying Reputation-Based Cisco ASA Access Policies)

   A. The security appliance domain name server
   B. The security appliance DNS reverse-lookup cache
   C. Unlisted (graylisted) addresses
   D. Dynamic database update poll interval

8. Which CLI command will display the number of entries contained in the dynamic filter database? (Source: Deploying Reputation-Based Cisco ASA Access Policies)

   A. **show dynamic-filter detail**
   B. **show dynamic-filter statistics**
   C. **show dynamic-filter data**
   D. **show dynamic-filter reports**

9. Which is a benefit of the the Cisco ASA Identity Firewall solution? (Source: Deploying Identity-Based Firewall Features)

   A. Coupling network topology from security polices
   B. Increased flexibility and simplicity in policy creation
   C. Tight integration with the cut-through proxy feature
   D. Monitors the Active Directory domain controller security log event file for user login and logout events

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

10. What are two methods of verifying that the Cisco ASA can communicate with with the Cisco CDA? (Choose two.) (Source: Deploying Identity-Based Firewall Features)

A. Use the **test aaa-server ad-agent** CLI command
B. Use the **test aaa-server authentication AD** CLI command
C. Use the **TEST** button in the AAA Server Groups window in ASDM
D. Use the **TEST** button in the Identity Options window in ASDM

https://t.me/learningnets

Answer Key

1. B, C
2. A, E
3. A, C
4. B
5. A, B, E
6. C
7. A
8. C
9. B
10. A, D

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Module 5

Threat Controls Deployment on Cisco IOS Software

Introduction

Cisco IOS Software Threat Control features provide security controls that can establish flexible network access control policies between security domains (zones), into which enterprise networks are often partitioned. This module provides configuration, verification, troubleshooting, and general deployment guidelines for security controls that are available with Cisco IOS Threat Control features.

Upon completing this module, you will be able to:

- Describe and configure Cisco IOS Zone-Based Policy Firewall
- Describe and configure application inspection policies on Cisco IOS Zone-Based Policy Firewall

https://t.me/learningnets

https://t.me/learningnets

Lesson 1

Deploying Basic Cisco IOS Zone-Based Policy Firewall Access Policies

The Cisco IOS Zone-Based Policy Firewall is a Cisco IOS Software stateful packet filtering firewall function. The Zone-Based Policy Firewall changed the firewall from an interface-based model to a more easily understood zone-based model. In this lesson, you will learn to configure and verify the OSI Layer 3 and 4 access control features of the Zone-Based Policy Firewall.

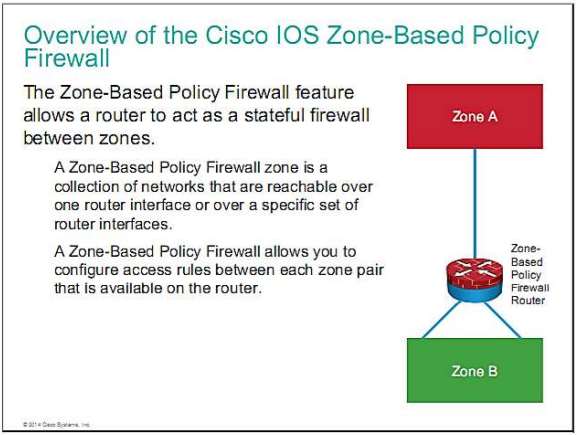
Upon completing this lesson, you will be able to:

- Describe the Cisco IOS Zone-Based Policy Firewall
- Configure Zone-Based Policy Firewall zones and zone pairs
- Verify Zone-Based Policy Firewall zones and zone pairs
- Configure a basic OSI Layer 3 and 4 interzone access policy
- Verify a basic OSI Layer 3 and 4 interzone access policy
- Configure a basic OSI Layer 3 and 4 intrazone access policy
- Configure a Zone-Based Policy Firewall inspection of control-plane and management-plane traffic
- Tune stateful engine and connection settings
- Integrate Zone-Based Policy Firewall with Cisco IOS Software NAT configuration
- Troubleshoot the operation of basic Zone-Based Policy Firewall functions

https://t.me/learningnets

Overview of the Cisco IOS Zone-Based Policy Firewall

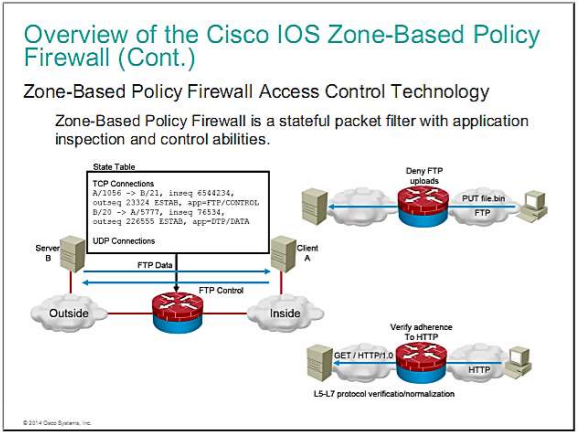
This topic describes the Cisco IOS Zone-Based Policy Firewall.



The Zone-Based Policy Firewall is a Cisco IOS Software data plane security feature that allows a router to act as a powerful and flexible stateful firewall between zones that correspond to security domains that are created through network separation. The router that is configured with Zone-Based Policy Firewall features can act either as a standalone firewall system or as an element of a more complex firewall system.

A Zone-Based Policy Firewall zone is a collection of networks that are reachable over one or more specific router interfaces that are designated to belong to the same zone. Zone-Based Policy Firewall access control policies then control access between two or more zones that are configured on the router, using a flexible configuration language that allows you to specify simple or complex access policies in a manageable manner.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



Stateful Packet Filtering

Stateful packet filtering is an application-aware method of packet filtering that works on the connection, or flow, level, with occasional peeks into the application layer of an application.

Stateful packet filters maintain a state table to keep track of all active sessions that cross the firewall. A state table, which is an internal data structure of a stateful packet filter, tracks all OSI Layer 4 sessions and inspects all packets that pass through the device. Based on its memory of previous packets in a session, a stateful packet filter can expect what kind of traffic should arrive from communicating hosts. Packets with the expected properties that are predicted by the state table are forwarded. The state table updates itself dynamically as a result of traffic flow.

Stateful packet filters are also application-aware through additional, deeper inspection of transit traffic, which is required to manage dynamic applications. Dynamic applications typically open an initial connection on a well-known port, and then negotiate additional OSI Layer 4 connections through a negotiation process inside the initial session. Stateful packet filters support these dynamic applications by analyzing the contents of the initial session, and then parsing the application protocol just enough to learn about the additional negotiated channels. A stateful packet filter typically assumes that if the initial connection was permitted, any additional transport-layer connections of that application should be permitted as well.

Application Inspection and Control

Many users of stateful packet filtering technology have increasingly demanded higher application layer awareness in their stateful packet filtering -based devices. Most vendors responded by improving application layer analysis of pure stateful packet filtering devices, by enhancing the traffic analysis engine with the following services:

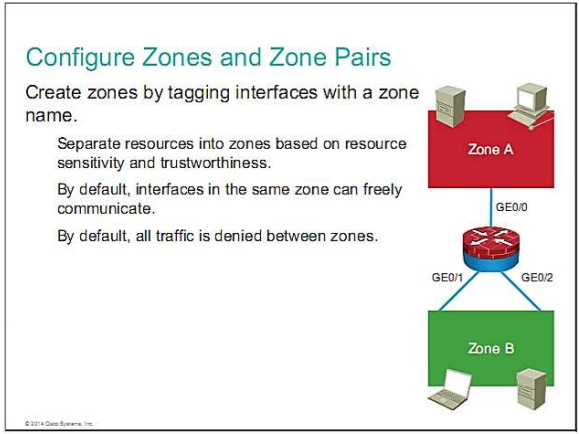
- In-memory reassembly of Layer 4 (TCP, UDP) sessions to obtain the sequential stream of bytes exchanged between hosts, over which the application-layer inspection engine can reliably parse the application layer protocol
- Application layer protocol decoding, to allow for filtering inside the protocol and its content
- Application layer protocol verification, in which the engine drops application layer protocol units that do not conform to the protocol standard

This additional functionality is often called AIC or DPI.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Configure Zones and Zone Pairs

This topic describes how to configure Zone-Based Policy Firewall zones and zone pairs.



You create zones (security domains) on a Zone-Based Policy Firewall-enabled router by tagging router network interfaces with a zone name. Create as many zones as are needed by your access control requirements. You typically create zones by grouping resources that have the same level of sensitivity or trustworthiness or that require special isolation due to their criticality or vulnerability.

When you designate router interfaces as zone members, the default policy of the Zone-Based Policy Firewall is to permit all traffic between interfaces of the same zone (that is, intrazone traffic). The Zone-Based Policy Firewall denies all traffic between different zones by default.

The figure shows a Cisco Integrated Services Router that is configured with three interfaces. Interface GigabitEthernet0/0 (and all networks that are reachable over it) belongs to Zone A. Interfaces GigabitEthernet0/1 and GigabitEthernet0/2 (and all networks that are reachable over them) belong to Zone B. By default, all traffic between interfaces GigabitEthernet0/1 and GigabitEthernet0/2 can flow freely. Traffic between interfaces GigabitEthernet0/0 and GigabitEthernet0/1, and between interfaces GigabitEthernet0/0 and GigabitEthernet0/2, is denied by default and will need to be explicitly authorized by Zone-Based Policy Firewall rules.

Configure Zones and Zone Pairs (Cont.)

Configuration Tasks

1. Create zones.
2. Assign router interfaces to zones.
3. Create zone pairs.

© 2014 Cisco Systems, Inc.

To configure Zone-Based Policy Firewall zones on a Cisco Integrated Services Routers that runs Cisco IOS Software, you will need to perform these configuration tasks:

1. Create security zones in Cisco IOS Software.
2. Assign router network interfaces to configured zones.
3. Create zone pairs for each zone pair that requires unidirectional communication.

Configure Zones and Zone Pairs (Cont.)

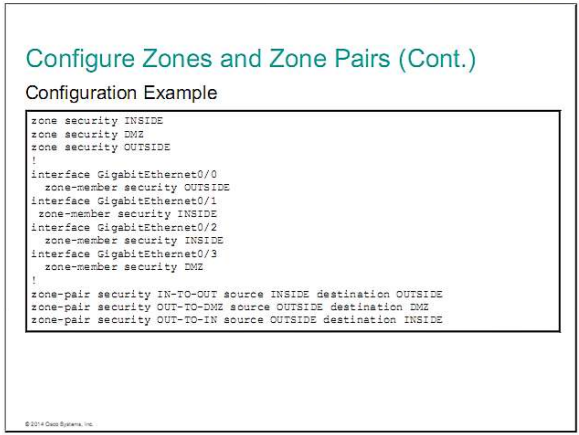
Configuration Scenario



© 2014 Cisco Systems, Inc.

https://t.me/learningnets

This figure presents the scenario that will be used in the configuration tasks. You will create three zones—OUTSIDE, DMZ, and INSIDE. The Cisco ISR uses four interfaces—interface GigabitEthernet0/0 will be assigned to the OUTSIDE zone, interface GigabitEthernet0/3 will be assigned to the DMZ zone, and interfaces GigabitEthernet0/1 and GigabitEthernet0/2 will be assigned to the INSIDE zone.



The first step of this configuration sequence is to globally create zones on the router. This example uses the INSIDE, DMZ, and OUTSIDE zones.

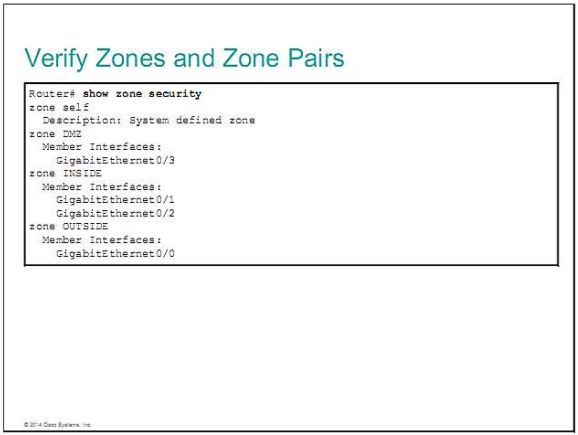
In the second configuration step, assign router network interfaces to zones. You do not have to assign all local interfaces to configured zones, but only interfaces that should participate in the Zone-Based Policy Firewall system. To assign an interface to a zone, enter interface configuration mode and use the **zone-member security** command to specify the name of the zone that the interface is assigned to. You can only assign a network interface to a single zone.

A zone pair allows you to specify that a unidirectional firewall policy (which is configured using the Cisco Common Classification Policy Language) between two security zones will exist. The direction of the traffic is indicated by a specified source and destination security zone. If you want traffic to flow in both directions between two zones, you must create two zone pairs—one for each direction.

Create zone pairs by using the **zone-pair security** command, naming the zone pair, and specifying the source and destination zones, with respect to the direction in which application sessions will be established between zones. Only create zone pairs that will interact in one direction. If you do not specify a zone pair for a possible pair of zones, all sessions between those two zones (in that direction) will be denied by default.

Verify Zones and Zone Pairs

This topic describes how to verify Zone-Based Policy Firewall zones and zone pairs.



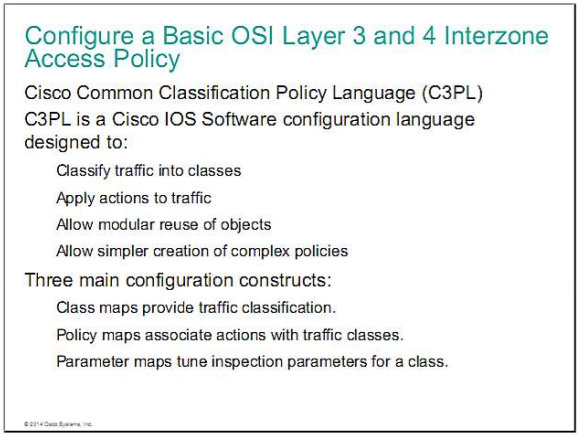
Use the **show zone security** command to display the zone description and the interfaces that are contained in the specified zone. If you do not specify the zone name, the command displays information for all of the zones that are configured.

The output shows that interface GigabitEthernet0/3 belongs to the zone named DMZ, interfaces GigabitEthernet0/1 and GigabitEthernet0/2 belong to the zone named INSIDE, and interface GigabitEthernet0/0 belongs to the zone named OUTSIDE.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Configure a Basic OSI Layer 3 and 4 Interzone Access Policy

This topic describes how to configure a basic OSI Layer 3 and 4 interzone access policy.



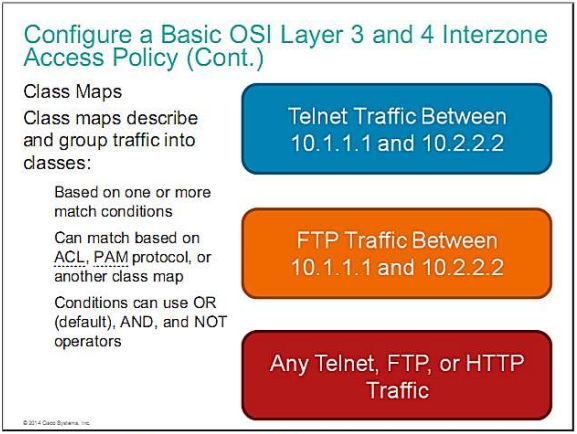
The second major change that is introduced by the Zone-Based Policy Firewall feature is a new configuration policy language that is known as C3PL. The C3PL structure is like the MQC structure in which class maps specify the traffic that is affected by the action that the policy map applies. C3PL is also highly modular in order to allow the reuse of configured objects in multiple policies, and flexible in order to allow the creation of complex policies in a manageable fashion.

C3PL uses three main configuration constructs:

Class maps: Objects that describe different classes of traffic, and therefore provide classification of traffic that is based on administrator-specified criteria.

Policy maps: Specify the actions to take when traffic matches the criteria that is defined in class maps. In order for a router to use the information in a policy map and its associated class maps, the policy map must be associated with a zone pair.

Parameter maps: Augment basic inspection with the capability to recognize and apply service-specific actions, such as tuning the stateful engine, or applying application-layer inspection.



Class maps define the traffic that a Zone-Based Policy Firewall selects for policy application. Basic class maps classify network traffic based on the following criteria:

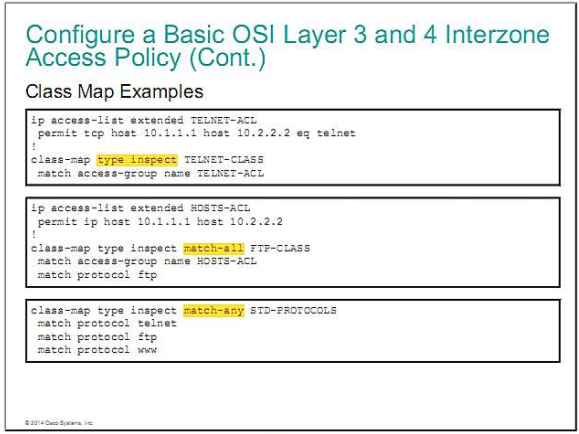
Access group: A standard, extended, or named ACL that can select traffic based on source and destination IP address, source and destination port, and other criteria available in the ACL. A *permit* action in the ACL selects traffic to belong to the class.

Protocol: Selects traffic based on OSI transport layer protocols, such as TCP, UDP, and ICMP, as well as application-layer protocols, such as HTTP, FTP, and DNS. Any well-known or user-defined service that is known to Cisco IOS Software PAM can be specified.

Class map: You can nest a subordinate class map that provides additional match criteria inside another class map, creating a hierarchy of classification.

Class maps can apply "match any" (logical OR, which is the default) or "match all" (logical AND) operators to determine how to apply the match criteria, if multiple criteria are specified. If the **match-any** command is specified, traffic must meet at least one of the match criteria in the class map. If **match-all** is specified, traffic must match all of the criteria in the class map to belong to that particular class. You can also use the negation (NOT) operator to describe traffic that is based on traffic that does not have a particular property.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



This figure shows three examples of class maps that define traffic classes.

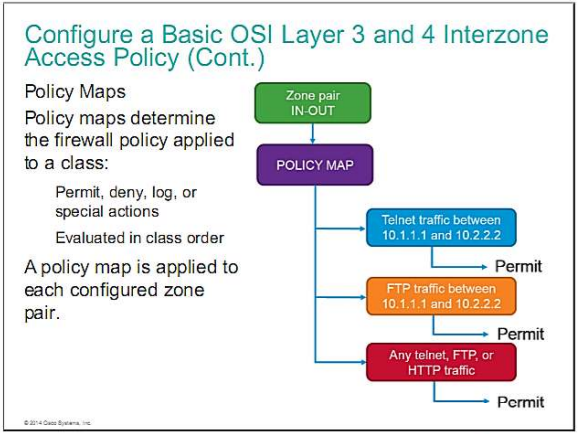
The first class must match all telnet traffic from host 10.1.1.1 and host 10.2.2.2. The class map is implemented by defining an extended ACL that matches the first packet of the telnet session from host 10.1.1.1 to host 10.2.2.2. Then, a named class map is defined using the **class-map type inspect** command, and the **match access-group name** command inside the class map specifies the condition that classifies flows into this class.

Note Because the Zone-Based Policy Firewall is stateful, you can only specify the first packet of a session to make the entire flow belong to a class.

The second class must match all FTP sessions from host 10.1.1.1 to host 10.2.2.2. The class map is implemented by first defining an extended ACL that matches all IP traffic from host 10.1.1.1 to host 10.2.2.2. Then, a named class map is defined using the **class-map type inspect match-all** command, requiring that all criteria inside the class map are met for traffic to be classified into this class. Inside the class map, the **match access-group name** command and the **match protocol ftp** command specify the two conditions that classify flows into this class. Both of these conditions must be true, that is, the session must establish from host 10.1.1.1 to host 10.2.2.2), and it should be an FTP session for traffic to belong to this class.

Note With the **match protocol** command, you can specify any protocol that is supported by Cisco IOS (PAM).

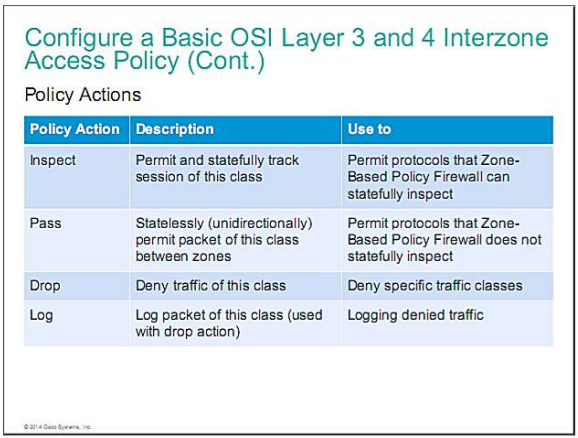
The third class must match all telnet, FTP, and HTTP sessions, regardless of source and destination addresses. A named class map is defined by using the **class-map type inspect match-any** command, and requires that any of the criteria inside the class map could be met for traffic to be classified into this class. Inside the class map, the three **match protocol** commands specify the three conditions that classify flows into this class. Any one (or more) of these conditions must be true for traffic to belong to this class.



A C3PL policy map is a configuration object that determines the actions (firewall policy) that will be applied to a particular class, for a particular zone pair to which the policy map will be applied. Generally, a policy map can permit access, deny access, and log access for a traffic class between zones.

A policy map is a sequential list of classes and the actions applied to them. When a session is being established between zones, the policy map is consulted in sequence (class order), and the action that is assigned to the first matching class is applied to the session.

Policy maps must be applied to zone pairs. While you can apply a policy map to multiple zone pairs, most configurations will use a single, unique policy map for each zone pair.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

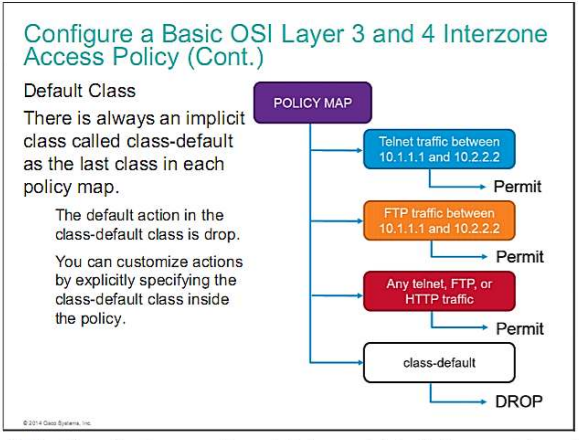
A Zone-Based Policy Firewall can take the following four possible actions for a particular class, as dictated by the policy map:

Inspect: This action permits the class, and enables stateful tracking for all sessions of the class that can be inspected. You should use this action for traffic classes that should be permitted through the firewall, and contain protocols that the Zone-Based Policy Firewall is able to inspect.

Pass: This action permits the class, and statelessly (without keeping state) allows the packet to be delivered to the destination zone. The pass action allows traffic only in one direction. A corresponding policy must be applied to allow return traffic to pass in the opposite direction. You should use this action for traffic classes that should be permitted through the firewall, and contain protocols that the Zone-Based Policy Firewall is not able to inspect statefully, for example, asynchronous ICMP messages (such as ICMP unreachables), GRE, or OSPF traffic.

Drop: This action denies the class between the zone pair

Log: This action is only used in conjunction with the drop action to log packets denied by the Zone-Based Policy Firewall configured policy.



Zone-Based Policy Firewall policy maps always include a special, implicitly present class called *class-default* as the last class in the policy map. The class-default class is a catch-all class that matches traffic that was not previously matched by other, more specific classes.

The default action of the class-default class is to drop traffic. You can, however, tune the class-default policy by explicitly listing it inside your policy map and, for example, also including the log action.

Note	You cannot assign the inspect or pass actions to the class-default class.

Configure a Basic OSI Layer 3 and 4 Interzone Access Policy (Cont.)

Default Access Policy

Source interface member of zone?	Destination interface member of zone?	Zone pair exists?	Policy map exists?	Result
No	No	—	—	Permit
Yes (zone A)	Yes (zone A)	—*	—	Permit
Yes	No	—	—	Deny
No	Yes	—	—	Deny
Yes (zone A)	Yes (zone B)	No	—	Deny
Yes (zone A)	Yes (zone B)	Yes	No	Deny
Yes (zone A)	Yes (zone B)	Yes	Yes	Apply policy map actions

* Can be optionally inspected from Cisco IOS Software Release 15.0(1)M.

© 2014 Cisco Systems, Inc

The zone memberships of the router network interfaces is subject to several rules governing interface behavior, as with the traffic moving between the router interfaces:

You must configure a zone before you can assign interfaces to it.

You can assign an interface to only one security zone.

Traffic is implicitly allowed to flow by default among interfaces that are members of the same zone. You can, however, change this behavior from Cisco IOS Software Release 15.0(1)M.

To permit traffic to and from a zone member interface, you must configure a policy that allows or inspects traffic between that zone and another zone.

Traffic cannot flow between a zone member interface and an interface that is not a zone member. You can apply pass, inspect, and drop actions only between two zones.

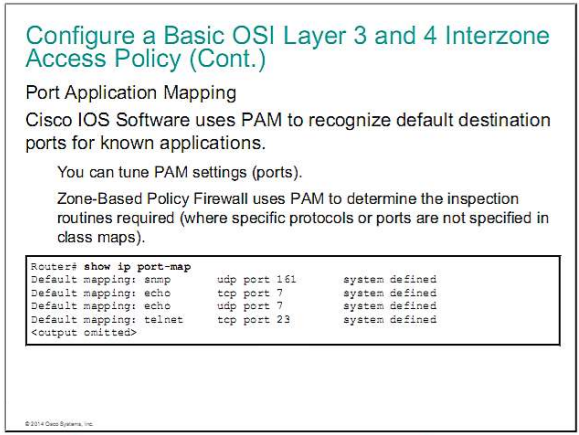
Interfaces that have not been assigned to a zone function as classical router ports and might still use CBAC configuration.

If you do not want an interface on the router to be part of the Zone-Based Policy Firewall policy, it might still be necessary to put that interface in a zone and configure a pass-all policy (a dummy policy) between that zone and any other zone to which traffic flow is desired.

From the preceding rules, it follows that, if traffic is to flow among all of the interfaces in a router, all of the interfaces must be part of the zoning model (each interface must be a member of a zone).

The figure shows a number of examples of different interface and configuration combinations.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



Cisco IOS Software PAM is a feature that allows you to customize TCP or UDP port numbers for network services or applications. PAM uses this information to support network environments that run services using ports that are different from the registered or well-known ports associated with an application. Using the port information, PAM establishes a table of default port-to-application mapping information at the firewall. The information in the PAM table enables Zone-Based Policy Firewall supported services to run on nonstandard ports.

If you specify class maps without any port-based selector, Zone-Based Policy Firewall will automatically use PAM to determine the applications matching your class, and use appropriate inspection routines. You can use the **show ip port-map** command to observe the default port mappings used by PAM, and consequently, by the Zone-Based Policy Firewall inspection routines.

Configure a Basic OSI Layer 3 and 4 Interzone Access Policy (Cont.)

Configuration Tasks

1. Configure classes.
2. (Optional) Configure object groups.
3. Configure access policies.
4. Apply policy maps to a zone pairs.

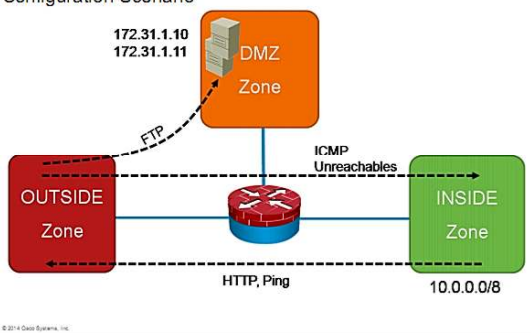
© 2014 Cisco Systems, Inc.

To configure the Zone-Based Policy Firewall with a basic (Layer 3 and 4) inter-zone access control policy, you will need to perform the following tasks:

1. Configure traffic classes using C3PL class maps.
2. (Optional) Use object groups to group similar objects together in order to simplify access rules.
3. Configure access policies using C3PL policy maps, for all configured zone pairs.
4. Apply configured policy maps to zone pairs.

Configure a Basic OSI Layer 3 and 4 Interzone Access Policy (Cont.)

Configuration Scenario



© 2014 Cisco Systems, Inc.

https://t.me/learningnets

This figure presents the configuration scenario used in upcoming configuration tasks. You will create the following basic interzone access policy:

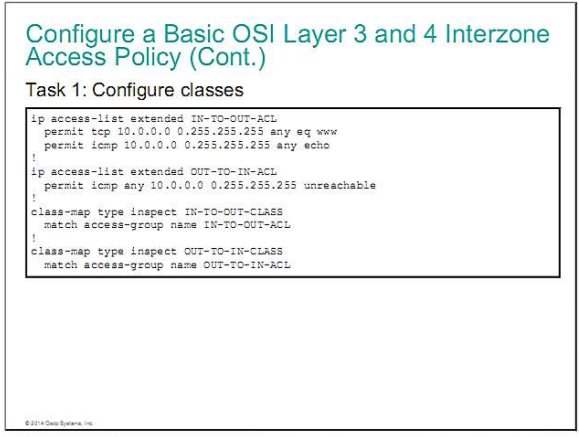
Hosts in the INSIDE zone, with addresses in the 10.0.0.0/8 network, can access any host in the OUTSIDE zone by using the HTTP and ping (ICMP echo) protocols.

Hosts in the OUTSIDE zone can access two FTP servers (172.31.1.10 and 172.31.1.11) in the DMZ zone by using the FTP protocol.

Hosts in the OUTSIDE zone can send ICMP "destination unreachable" messages to hosts in the INSIDE zone, with addresses in the 10.0.0.0/8 network. This is typically required for TCP/IP stacks to work optimally, including enabling their Path MTU Discovery functions.

All other traffic between zone pairs is prohibited and should be dropped.

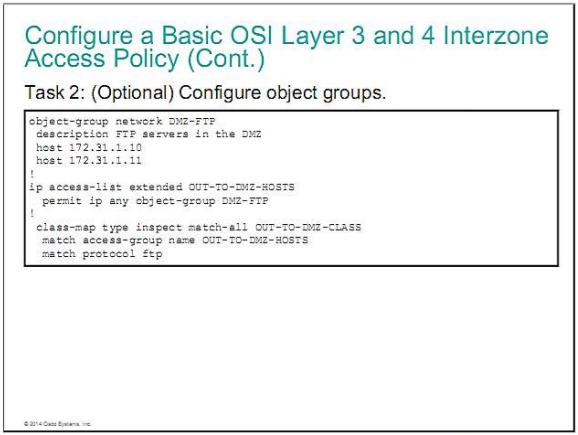
The steps in the upcoming configuration sequence assume that the Cisco ISR is already configured with all required Zone-Based Policy Firewall zones (INSIDE, OUTSIDE, DMZ), and appropriate network interfaces assigned to these zones, as specified in the previous topic.



In the first task of the configuration sequence, configure class maps that describe traffic that must be permitted across the Zone-Based Policy Firewall-enabled router.

To describe HTTP and ping traffic that will be permitted between the INSIDE and OUTSIDE zones, the IN-TO-OUT-ACL ACL describes the initial packets of HTTP and PING sessions from the 10.0.0.0/8 network. The IN-TO-OUT-CLASS matches the configured ACL to classify these two applications into the same class. Alternatively, you could configure two distinct classes for HTTP and ping.

To describe ICMP destination unreachable packets that will be permitted between the OUTSIDE and INSIDE zones, the OUT-TO-IN ACL describes the required ICMP packet type. The OUT-TO-IN-CLASS matches the configured ACL to classify these packets into a separate class.

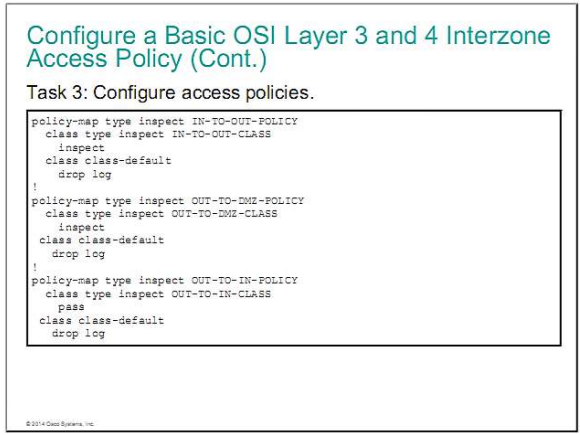


To describe FTP traffic that will be permitted between the OUTSIDE and FTP zones, the example uses an object group to create a set of two hosts that can be treated as a single entity in access policies. Use the **object-group network** command to create a named object group, and use **host** commands inside it to specify members of the object group.

The OUT-TO-DMZ-HOSTS ACL describes connections between a host and the previously configured object group describing the two hosts in the DMZ zone, using the object-group parameter as the destination in the ACL access control element..

The OUT-TO-DMZ-CLASS uses two match conditions in a match-all (AND) combination: it refers to the configured OUT-TO-DMZ-HOSTS ACL to specify the source and destination condition, and the match protocol statement to add the FTP protocol condition to the class. You could also alternatively configure this class by only matching an ACL (**match access-group** command), which would also specify the FTP destination port.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

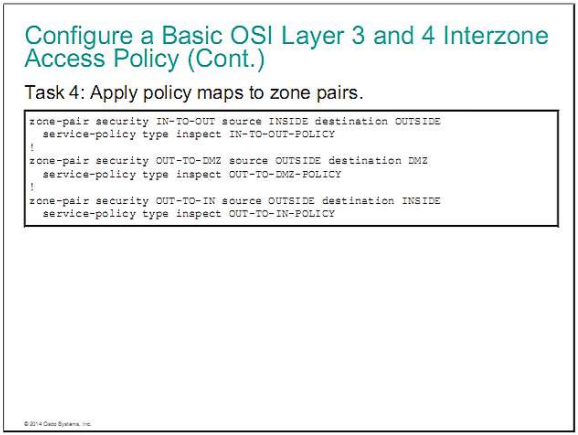


In the third task of the configuration sequence, configure policy maps to determine the access policy for each required and configured zone pair.

First, configure a policy map to control access between the INSIDE and OUTSIDE zones. Use the **policy-map type inspect** command to create a named policy map (IN-TO-OUT-POLICY). In the policy map configuration mode, use the **class type-inspect** command to refer to a previously configured IN-TO-OUT-CLASS, and in the class submode, specify the **inspect** action to permit and statefully inspect the class protocols (HTTP and ping). Exit the class submode, and create an optional reference to the class-default class, using the **class class-default** command. In the class-default class, tune the default **drop** action to also **log** denied traffic, by specifying both actions (**drop log**) in the class policy.

Next, configure a policy map to control access between the OUTSIDE and DMZ zones (OUT-TO-DMZ-POLICY). In the policy map configuration mode, use the **class type-inspect** command to refer to a previously configured OUT-TO-DMZ-CLASS, and in the class submode, specify the **inspect** action to permit and statefully inspect the class protocol (FTP). Exit the class submode, and assign the **drop log** actions to the class-default class of this policy map.

Finally, configure a policy map to control access between the OUTSIDE and INSIDE zones (OUT-TO-IN-POLICY). In the policy map configuration mode, use the **class type-inspect** command to refer to a previously configured OUT-TO-IN-CLASS, and in the class submode, specify the **pass** action to statelessly inspect the class protocol (ICMP "destination unreachable" messages), because it cannot be treated statefully. Exit the class submode, and assign the **drop log** actions to the class-default class of this policy map.



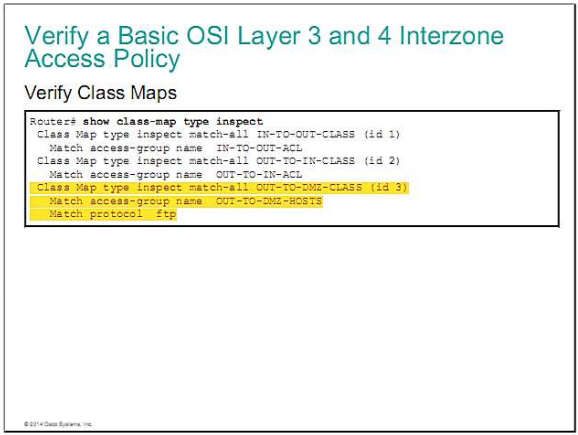
In task four of this configuration sequence, apply the configured policy maps to their respective zone pairs.

Use the **zone-pair security** global configuration command to enter the zone pair configuration mode, and then use the **service-policy type inspect** command to associate a named policy map with each configured zone pair. In this example, associate the IN-TO-OUT-POLICY policy configured in the previous task with the IN-TO-OUT zone pair, the OUT-TO-DMZ-POLICY policy configured in the previous task with the OUT-TO-DMZ zone pair, and the OUT-TO-IN-POLICY policy configured in the previous task with the OUT-TO-IN zone pair.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

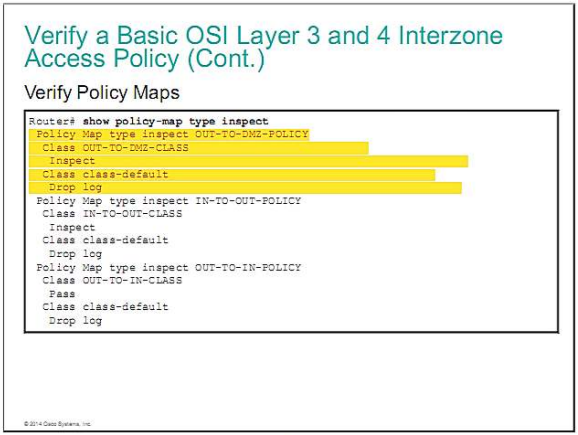
Verify a Basic OSI Layer 3 and 4 Interzone Access Policy

This topic describes how to verify a basic OSI Layer 3 and 4 interzone access policy.

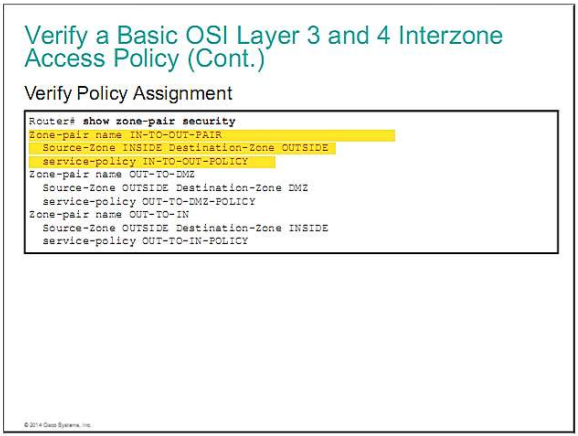


To verify your configuration, you can use Cisco IOS Software commands to verify the contents of your class maps, policy maps, and service policies.

To display a specific class map, use the **show class-map type inspect** *class-map-name* command in privileged EXEC mode. If a class map name is not specified, all class maps displays. The example in the figure shows all of the inspection class maps that were created in the preceding configuration sequence.



To display a specific policy map, use the **show policy-map type inspect** *policy-map-name* command in privileged EXEC mode. If a policy map name is not specified, all policy maps display. The example in the figure shows all of the inspection policy maps that were created in the preceding configuration sequence.



To display the source zone, destination zone, and policy that are attached to the zone pair, enter the **show zone-pair security** command, followed by a source-zone name and destination-zone name. If you do not specify a source and a destination, then every zone pair and its associated policy displays. If you specify only a source or a destination zone, then every zone-pair that contains that zone as the source or destination (depending on which one you specify) displays.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Verify a Basic OSI Layer 3 and 4 Interzone Access Policy (Cont.)

Verify Classification and Policy Enforcement

```
Router# show policy-map type inspect zone-pair
policy exists on zp IN-TO-OUT-PAIR
 Zone-pair: IN-TO-OUT-PAIR
  Service-policy inspect : IN-TO-OUT-POLICY
   Class-map: IN-TO-OUT-CLASS (match-all)
    Match: access-group name IN-TO-OUT-ACL
   Inspect
     Session creations since subsystem startup or last reset 845647433
     Current session counts (estab/half-open/terminating) [72:2:9]
     Maxever session counts (estab/half-open/terminating) [4386:15:563]
   <output omitted>
  Class-map: class-default (match-any)
   Match: any
   Drop
    46579346 packets, 9568934789 bytes
```

© 2014 Cisco Systems, Inc.

To display statistics of an applied policy and verify that it is matching traffic and enforcing a policy, you can use the **show policy-map type inspect zone-pair** command. This command will display a policy map along with its class maps, and display session statistics, including the number of dropped packets in its class-default class.

Verify a Basic OSI Layer 3 and 4 Interzone Access Policy (Cont.)

Verify Sessions

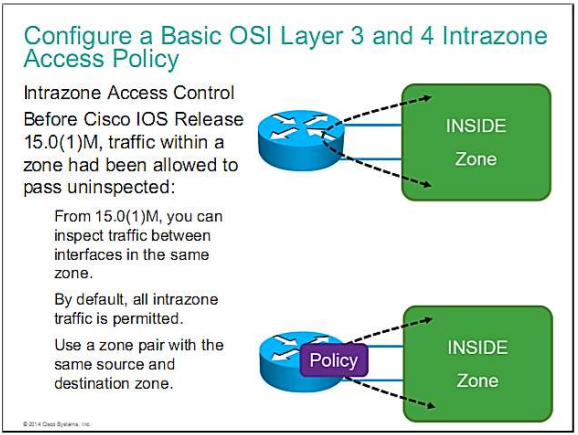
```
Router# show policy-map type inspect zone-pair sessions
policy exists on zp IN-TO-OUT-PAIR
 Zone-pair: IN-TO-OUT-PAIR
  Service-policy inspect : IN-TO-OUT-POLICY
   Class-map: IN-TO-OUT-CLASS (match-all)
    Match: access-group name IN-TO-OUT-ACL
   Inspect
    Number of Half-open Sessions = 0
    Sessions
     Session 673E1FE0 (10.1.1.10:52227)=>(192.168.1.20:80) tcp SIS_OPEN
      Created 00:00:12, Last heard
00:00:12
      Bytes sent (initiator:responder)
[534:6786]
    <output omitted>
```

© 2014 Cisco Systems, Inc.

To display all individual sessions (which can be limited to a specific zone pair), you can extend the **show policy-map type inspect zone-pair sessions** command with the sessions argument. In the output of this command, the router will display all statefully tracked sessions between a particular zone pair, allowing you to verify that a particular session is statefully handled by the router.

Configure a Basic OSI Layer 3 and 4 Intrazone Access Policy

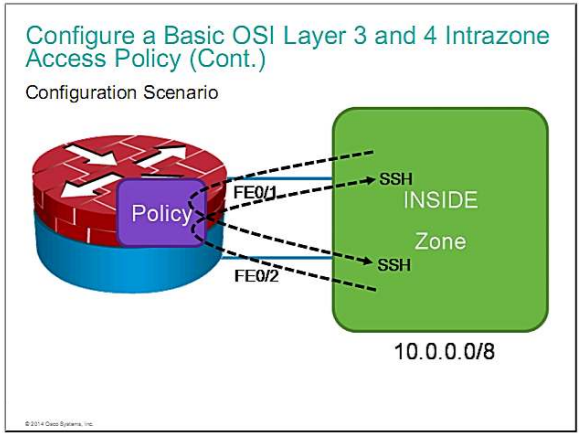
This topic describes how to configure a basic OSI Layer 3 and 4 intrazone access policy.



Cisco IOS Software Release 15.0(1)M introduced the possibility of intrazone filtering within the Zone-Based Policy Firewall framework. Before Cisco IOS Software Release 15.0(1)M, traffic between interfaces in the same zone was allowed to pass uninspected. Cisco IOS Software Release 15.0(1)M allows you to configure Zone-Based Policy Firewall rules to inspect arbitrary intrazone traffic, although the default policy is still to allow all traffic within a zone to be forwarded without restrictions.

You can configure intrazone access rules by creating a new zone pair, using the same zone name as the source and destination zone.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

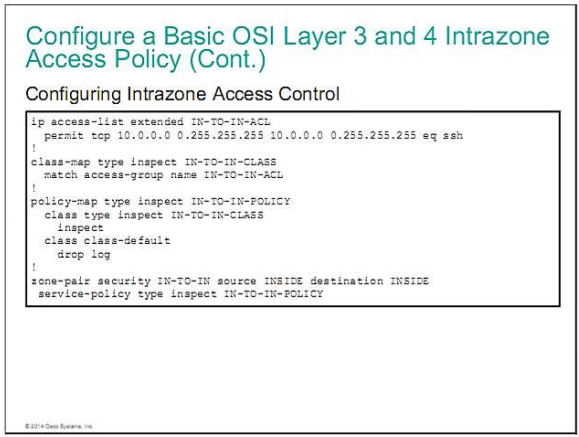


This figure presents the configuration scenario used in upcoming configuration tasks. You will create the following basic intrazone access policy:

Hosts in the INSIDE zone, with addresses in the 10.0.0.0/8 network, can access any host in the INSIDE zone using the SSH protocol.

All other traffic between interfaces in the same zone is prohibited and should be dropped.

The steps in the upcoming configuration sequence assume that the Cisco ISR is already configured with all of the required Zone-Based Policy Firewall zones (in this case, the INSIDE zone), and appropriate network interfaces assigned to these zones, as specified in previous topics.



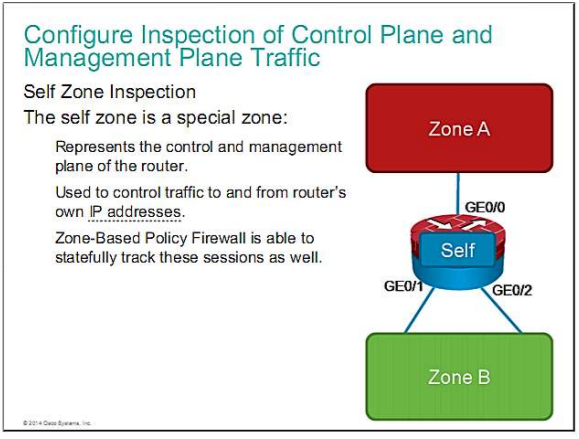
This figure shows a configuration that implements an intrazone filtering policy. The class map defines intrazone SSH traffic, and the policy map defines the **inspect** action to be applied to it. The class-default class is explicitly configured to **drop** and **log** all other intrazone traffic.

The **zone-pair security** command applies the configured policy map to traffic sourced to and destined for the same zone—the INSIDE zone—by specifying the same zone name as the source zone and destination zone.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Configure Inspection of Control Plane and Management Plane Traffic

This topic describes how to configure a Zone-Based Policy Firewall inspection of control-plane and management-plane traffic.



The rules for Zone-Based Policy Firewalls are different when the router is involved in the traffic flow, whether as the source of traffic or the destination. A Zone-Based Policy Firewall can be used to control router management and control traffic (such as routing protocols and ICMP) in which the router is the source or destination.

When you configure an interface to be a zone member, the hosts that are connected to the interface are included in the zone, but traffic that is flowing to and from the interfaces of the router is not controlled by the zone policies. Instead, all of the IP interfaces on the router are automatically made part of the self zone when you configure a Zone-Based Policy Firewall. To limit IP traffic that moves to the IP addresses of the router from the various zones on the router, you must apply policies to block, allow, or inspect traffic between one zone and the self zone of the router, and vice versa. If there are no policies between a zone and the self zone, all traffic is permitted to move to the interfaces of the router without being inspected.

If desired, you can define a policy using the self zone as either the source or destination zone. The self zone is a system-defined zone. It does not require you to configure any interfaces as members. A zone pair that includes the self zone, along with the associated policy, applies to traffic that is directed to the router or to traffic that the router generates, but does not apply to traffic traversing the router.

Configure Inspection of Control Plane and Management Plane Traffic (Cont.)

Self Zone Default Access Policy

Source interface member of zone?	Destination interface member of zone?	Zone pair exists?	Policy exists?	Result
Self	Yes	No	—	Permit
Self	Yes	Yes	No	Permit
Self	Yes	Yes	Yes	Apply policy map actions
Yes	Self	No	—	Permit
Yes	Self	Yes	No	Permit
Yes	Self	Yes	Yes	Apply policy map actions

© 2014 Cisco Systems, Inc.

The following are additional rules for Zone-Based Policy Firewalls that govern interface behavior when the router is involved in the traffic flow:

All traffic to and from a given interface is implicitly blocked when the interface is assigned to a zone. The exception to this rule is the traffic to or from other interfaces in the same zone, as well as the traffic to any interface on the same router.

All of the IP interfaces on the router are automatically made part of the self zone when you configure a Zone-Based Policy Firewall. The self zone is the only exception to the default deny-all policy. All traffic to any router interface is allowed until traffic is explicitly denied.

Configure Inspection of Control Plane and Management Plane Traffic (Cont.)

Configuration Tasks

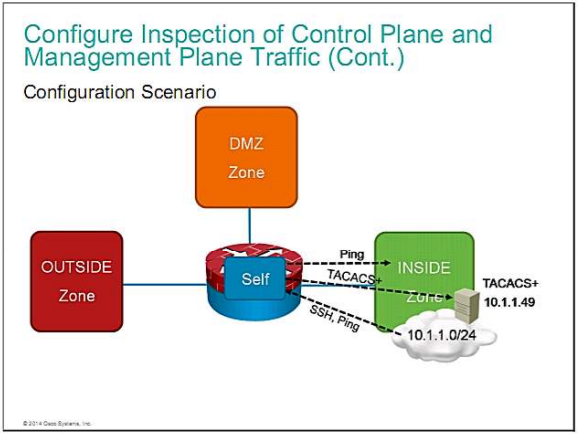
1. (Optional) Configure an inbound policy for the self zone.
2. (Optional) Configure an outbound policy for the self zone.

© 2014 Cisco Systems, Inc.

https://t.me/learningnets

To configure the Zone-Based Policy Firewall self-zone access control policy, you will need to perform the following configuration tasks:

1. Optionally, configure an inbound access policy for the self zone, which will protect the router from unwanted incoming sessions.
2. Optionally, configure an outbound access policy for the self zone, which will control outbound sessions from the router.



This figure presents the configuration scenario that will be used in upcoming configuration tasks. You will create the following basic self zone access policy:

Hosts in the 10.1.1.0/24 network, in the INSIDE zone, can make SSH and ping sessions to the router.

The router can ping all hosts in the INSIDE zone.

The router can access the TACACS+ server in the inside zone.

Deny any other inbound sessions from other zones.

Permit all other sessions to other zones.

The configuration steps in the upcoming configuration sequence assume that the Cisco ISR is already configured with all of the required Zone-Based Policy Firewall zones (INSIDE, OUTSIDE, DMZ), and appropriate network interfaces assigned to these zones, as specified in previous topics.

Configure Inspection of Control Plane and Management Plane Traffic (Cont.)

Task 1: (Optional) Configure an inbound policy for the self zone.

```
access-list IN-TO-SELF-ACL permit icmp 10.1.1.0 0.0.0.255 any eq echo
access-list IN-TO-SELF-ACL permit tcp 10.1.1.0 0.0.0.255 any eq ssh
!
class-map type inspect IN-TO-SELF-CLASS
  match access-group name IN-TO-SELF-ACL
!
policy-map type inspect IN-TO-SELF-POLICY
  class type inspect IN-TO-SELF-CLASS
    inspect
  class class-default
    drop log
!
zone-pair security IN-TO-SELF source INSIDE destination self
 service-policy type inspect IN-TO-SELF-POLICY
```

© 2014 Cisco Systems, Inc.

In the first task of the configuration sequence, configure class maps that describe traffic that must be controlled to the self zone of the router, configure policy maps that permit or deny these classes, and apply these policy maps to the zone pairs that include the self zone as the destination zone.

First, create a class that describes SSH and ping traffic from the specific subnet of the INSIDE zone. The IN-TO-SELF-ACL defines this traffic, and is the only criterion used in the definition of the IN-TO-SELF-CLASS class. The IN-TO-SELF-POLICY policy map permits this class by using the inspect keyword, and drops and logs other traffic. The configured policy map is applied to the new IN-TO-SELF zone pair that uses the self zone as the destination zone.

Configure Inspection of Control Plane and Management Plane Traffic (Cont.)

Task 1: (Optional) Configure an inbound policy for the self zone (cont.)

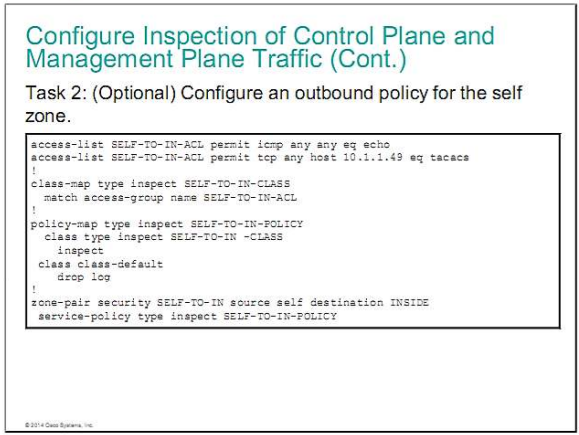
```
policy-map type inspect DENY-ALL-POLICY
  class class-default
    drop log
!
zone-pair security DMZ-TO-SELF source DMZ destination self
 service-policy type inspect DENY-ALL-POLICY
!
zone-pair security OUT-TO-SELF source OUTSIDE destination self
 service-policy type inspect DENY-ALL-POLICY
```

© 2014 Cisco Systems, Inc.

https://t.me/learningnets

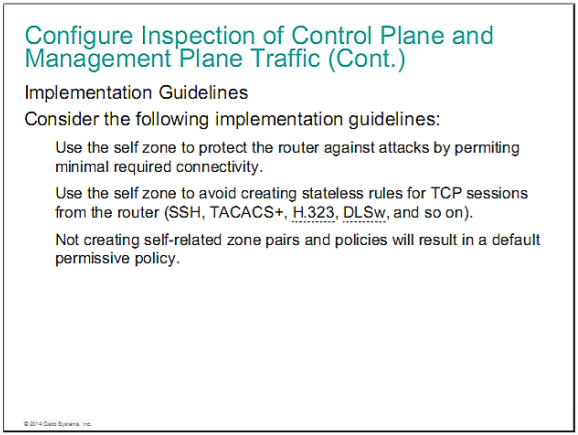
Next, you must drop all traffic from other zones to the self zone. Because such traffic would be permitted by default (if no zone pair exists), you can configure a policy map with only the class-default class inside it. This would match all traffic, and drop (and optionally log) it.

This policy map is then applied to the new DMZ-TO-SELF and OUT-TO-SELF zone pairs that use the self zone as the destination zone.



In the second task of the configuration sequence, configure a class map that describes traffic that must be controlled from the self zone of the router to the INSIDE zone, configure a policy map that permits the configured class, and apply the configured policy map to the zone pairs that specifies the self zone as the source zone and the INSIDE zone as the destination zone.

First, create a class that describes ping and TACACS+ traffic to the specific host in the INSIDE zone. The SELF-TO-IN-ACL defines this traffic, and is the only criterion used in the definition of the SELF-TO-IN-CLASS class. The SELF-TO-IN-POLICY policy map permits this class by using the inspect keyword, and drops and logs other traffic. The configured policy map is applied to the new SELF-TO-IN zone pair that uses the self zone as the source zone and the INSIDE zone as the destination zone.



When implementing self-zone access control, consider the following implementation guidelines:

To protect the router from all unwanted connectivity and permitting only the minimal required sessions to the control and management planes of the router, use self-zone policies that use the self zone as the destination zone as a router host firewall..

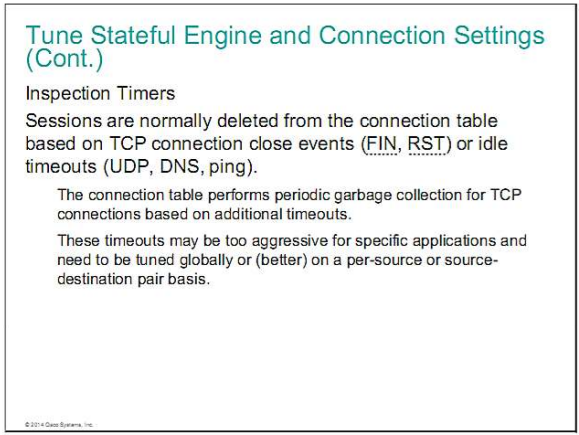
You should use self-zone policies to enable outbound connectivity from the router, which is tracked by the Zone-Based Policy Firewall stateful inspectors, and does not require any changes to inbound policies in order to permit return (reverse) traffic flows of outbound sessions. Such outbound sessions may include management sessions (for example, SSH, TACACS+, RADIUS),control sessions (for example, BGP, H.323), or tunnels (for example, DLSw, X.25 over TCP).

Remember that not creating self-zone policies will result in a permissive policy and expose the router control and management planes to network users. Consider deploying other hardening methods, such as Control Plane Protection, to mitigate this risk.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Tune Stateful Engine and Connection Settings

This topic describes how to tune stateful engine and connection settings.



The Zone-Based Policy Firewall will normally delete sessions from its state table based on normal connection-close events:

- **For TCP:** Sessions are normally deleted based on the FIN-based connection-close sequence or an RST-based forceful close.
- **For generic UDP, DNS, and ICMP ping:** Sessions are normally deleted based on an idle timeout.

However, the state table anticipates extraordinary events by performing additional garbage collection and deletes connections from the table in several other scenarios, such as unresponsive hosts, idle TCP connections, and some unexpected TCP exchanges. You can tune this behavior to support local specifics, such as hosts using slightly nonstandard TCP/IP stacks, or applications requiring specific session handling.

When tuning Zone-Based Policy Firewall stateful table behaviors and timers, it is strongly recommended that you only change these values for the specific hosts or applications that exhibit issues with default values, and not change global settings.

Tune Stateful Engine and Connection Settings (Cont.)

Inspection Timers

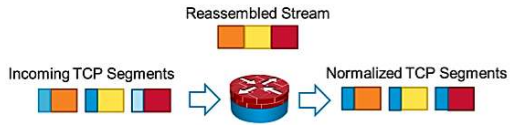
Timer	Default	Description
SYN timeout	5 seconds	Defines the time that the ZBPF will wait for the completion of the TCP three-way handshake
TCP idle timeout	1 hour	Defines the time that a TCP connection can be idle (that is, no traffic passed over it)
FIN timeout	5 seconds	Defines the time that the ZBPF waits for connection close acknowledgments
UDP idle timeout	60 seconds	Defines the time a UDP session can be idle (that is, no traffic passed over it)
DNS idle timeout	5 seconds	Defines the time that the ZBPF waits for DNS replies to DNS requests
Ping idle timeout	10 seconds	Defines the time that the ZBPF will wait for ICMP echo replies

© 2014 Cisco Systems, Inc.

This table shows the stateful engine timers and their default values. For most applications, these timers are optimal and require no change.

Tune Stateful Engine and Connection Settings (Cont.)

TCP Normalizer



The Zone-Based Policy Firewall TCP normalizer feature

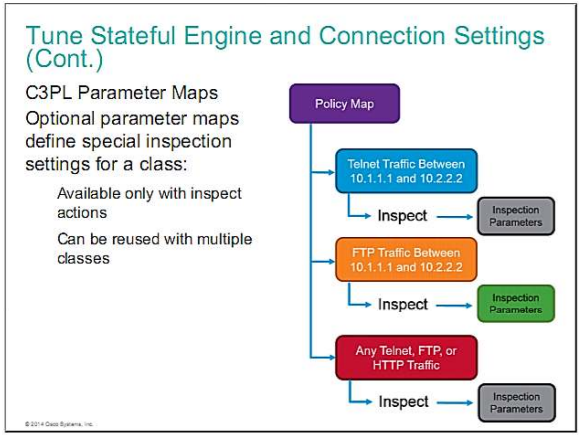
- Verifies adherence to the TCP protocol and prevents evasion attacks
- Provides the reassembled bytestream to upper-layer inspectors
- May interfere with some TCP stack quirks and out-of-order packet delivery
- TCP normalizer can only be tuned globally, for all flows

© 2014 Cisco Systems, Inc.

The Zone-Based Policy Firewall includes a TCP normalizer feature that is able to verify that a TCP session adheres to the TCP protocol specification. The purpose of the TCP normalizer is to reassemble the TCP stream, if application-layer filtering is configured on the router, to provide a proper byte stream to upper-layer inspection routines, which then parse the application-layer protocol. The TCP normalizer prevents certain ambiguities in TCP traffic, and, therefore, prevents evasion attacks that attackers may use to bypass application-layer filtering.

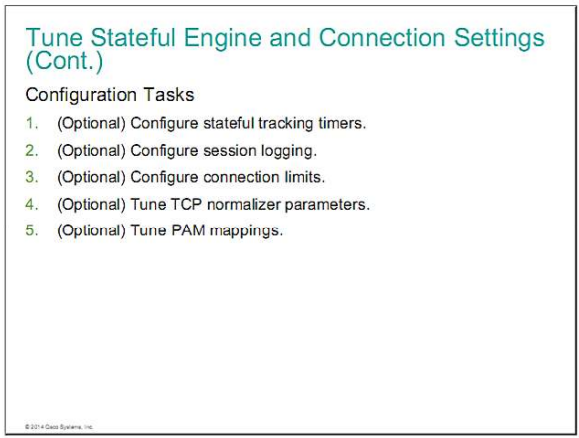
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

The TCP normalizer can sometimes impact legitimate applications, especially if they do not fully adhere to the TCP specification or if significant packet reordering occurs in the network. In this case, the Zone-Based Policy Firewall allows you to globally tune some of the TCP normalizer parameters to support such applications.



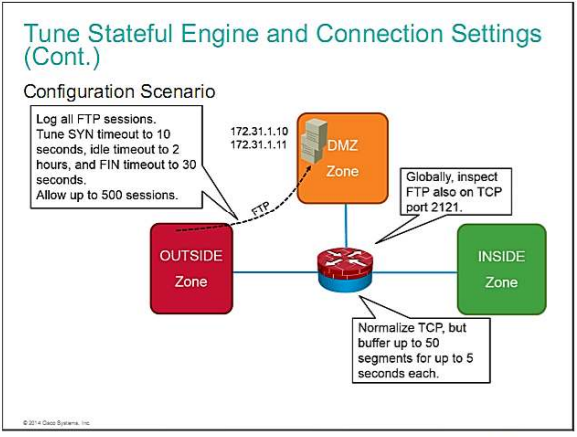
To configure special session requirements for specific classes (or globally), the Zone-Based Policy Firewall uses parameter maps to create sets of session settings that you can apply to a single class or multiple classes in a policy map.

Parameter maps are available only in classes that use the inspect action in a policy map.



If you need to configure Zone-Based Policy Firewall stateful engine tuning and special connection settings, perform the following optional configuration tasks:

1. Tune the stateful tracking timers for a class. Enable session logging to create an audit (accounting) trail for network sessions across the Zone-Based Policy Firewall-enabled router.
2. Configure connection limits to specify the maximum number of sessions available to a class.
3. Tune TCP normalizer parameters to support specific TCP-handling scenarios.
4. Tune PAM to support applications running on nonstandard ports



This figure presents the configuration scenario used in upcoming configuration tasks. You will configure the Zone-Based Policy Firewall with the following functions:

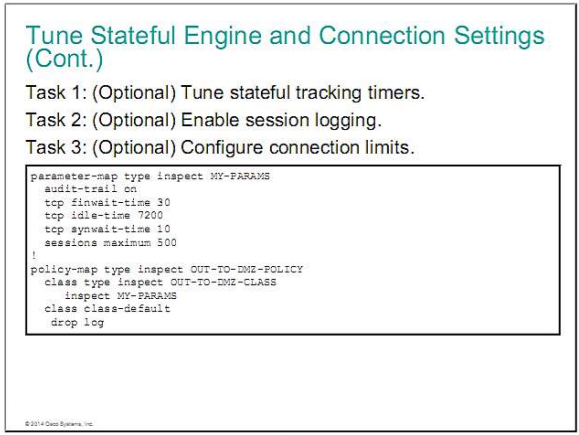
For the FTP sessions between the OUTSIDE zone and the two FTP servers in the DMZ zone, you will log all sessions (using the Cisco IOS Software syslog facility), tune the SYN timeout to 10 seconds, tune the TCP idle session timeout to 2 hours, and tune the TCP FIN timeout to 30 seconds. Additionally, you will allow only up to 500 sessions in this class.

You will configure the router to treat all TCP sessions on port 2121 as FTP sessions.

You will globally tune the TCP normalizer to buffer up to 50 out-of-order TCP segments, up to 5 seconds for each buffered segment, to support additional out-of-order traffic.

The configuration steps in the upcoming configuration sequence assume that the Cisco ISR is already configured with all required Zone-Based Policy Firewall zones (INSIDE, OUTSIDE, DMZ), appropriate network interfaces assigned to these zones, and the interzone access policy as specified in previous topics.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

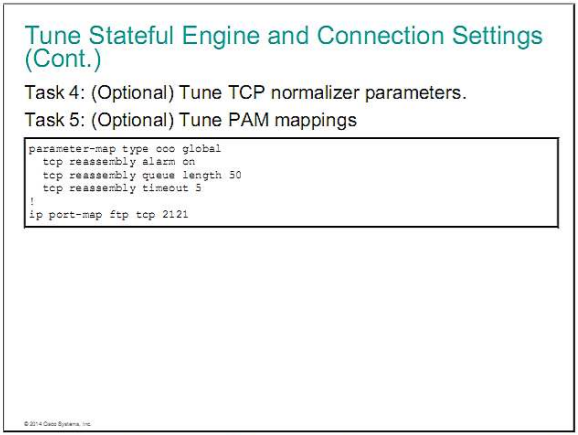


In the first configuration task, you will tune stateful tracking timers for a specific class. First, configure a new named parameter map using the **parameter-map type inspect** command. In the parameter map, specify the TCP SYN timeout using the **tcp synwait-time** command, the TCP idle session timeout using the **tcp idle-time** command, and the TCP FIN timeout using the **tcp finwait-time** command.

Next, apply this parameter map to the class that matches FTP traffic to the two DMZ servers (OUT-TO-DMZ-CLASS) in the relevant policy map (OUT-TO-DMZ-POLICY), by referencing the parameter map name next to the **inspect** command in the class.

In the second configuration task, you will request the router to create an audit trail for a specific class by creating logging messages for each created or deleted session in the stateful table. In the existing parameter map, use the **audit-trail on** command to enable session logging for this class.

In the third configuration task, you will specify a maximum connection limit for a specific class. In the existing parameter map, use the **sessions maximum** command to limit the total number of sessions for this class to 500.

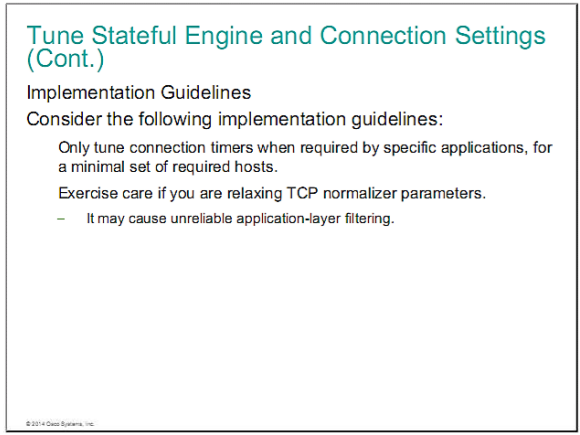


In the fourth configuration task, you will globally tune the TCP normalizer parameters on the router. First, create a new parameter map of type "ooo" (out of order) using the **parameter-map type ooo global** command. In the parameter map, use the **tcp reassembly alarm on** command to enable log messages that alert you when TCP protocol violations are detected, and lengthen the TCP normalizer buffering queue to 50 packets, with a timeout of 5 seconds for each packet.

In the final configuration task, you will tune the PAM database on the router to also inspect FTP traffic on port 2121. Use the **ip port-map ftp** command to add TCP port 2121 to the PAM database and associate it with the FTP protocol.

Note that this command now automatically permits FTP sessions on port 2121 (as well as on the standard port 21) to the two servers in the DMZ zone because the class map describing FTP flows uses the PAM-related **match protocol ftp** statement.

https://t.me/learningnets



When tuning the stateful engine and specifying special connection settings, consider the following guidelines:

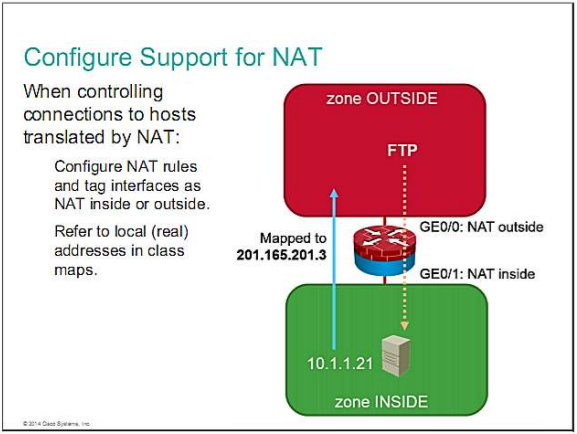
Make only minimal changes to the policy because assigning additional resources to all possible hosts communicating to the router may lead to performance or security issues.

Exercise care when tuning the TCP normalizer, especially when disabling or relaxing TCP normalizer features because this may impact the reliability of higher-layer traffic inspection functions that rely on the TCP normalizer for anti-evasion protection.

https://t.me/learningnets

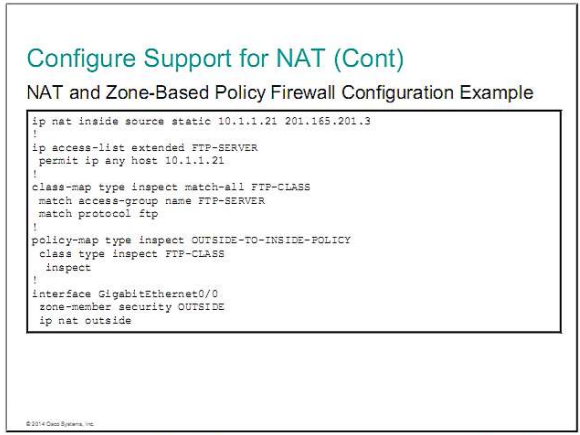
Configure Support for NAT

This topic describes how to integrate Zone-Based Policy Firewall with Cisco IOS Software NAT configuration.



You can deploy Zone-based Policy Firewall on a router that also performs NAT between its interfaces. When controlling access to or from hosts whose addresses are translated by NAT, configure Cisco IOS Software NAT rules and tag interfaces (which may be members of zones) as NAT inside or NAT outside. Then, in the Zone-based Policy Firewall class maps which match transit traffic, refer to the local (real) addresses of hosts that are communicating across the firewall router. Therefore, you do not have to take into account any NAT mappings when configuring firewall rules because the router will automatically identify the correct traffic flows even if addresses are also mapped using NAT.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

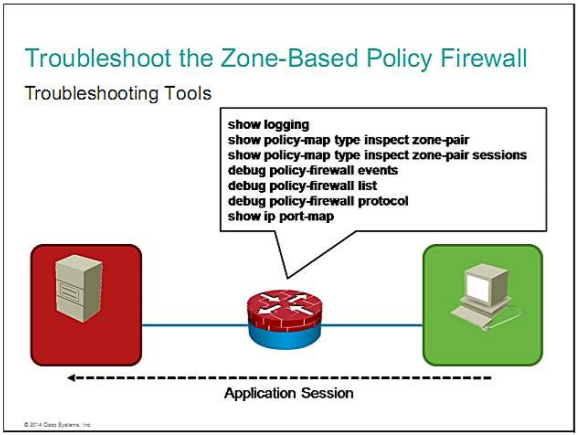


As with VRF-aware Zone-Based Policy Firewall, configuring the Zone-Based Policy Firewall feature with NAT does not require a change to the configuration philosophy. This figure shows a sample configuration of a NAT-enabled router, where NAT rules map an internal FTP server (with a real IP address of 10.1.1.21) to a global network, using a global (mapped) IP address of 209.165.201.3.

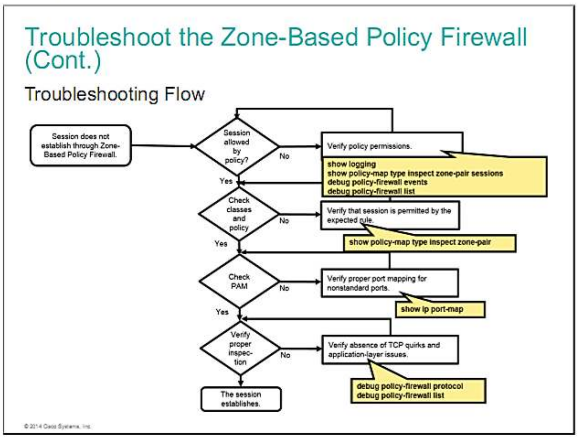
If you want to permit FTP access to this server from the OUTSIDE security zone, of which the NAT outside interface FastEthernet0/0 is a member, you would create appropriate class maps and policy maps that govern access between zones. Note that in the class map, you should simply refer to the real IP address of the FTP server, even though its IP address is translated to a mapped address on the GigabitEthernet0/0 (OUTSIDE zone, NAT outside) interface.

Troubleshoot the Zone-Based Policy Firewall

This topic describes how to troubleshoot the operation of basic Zone-Based Policy Firewall functions.



In order to troubleshoot issues related to basic access control, you can use a set of Cisco IOS Software CLI verification and debugging features. This figure lists some common commands and features that you may find useful during the troubleshooting session. Typically, you will examine why a particular session cannot establish through a Zone-Based Policy Firewall-enabled router.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

The figure shows the recommended task flow for troubleshooting basic access control through a Zone-Based Policy Firewall-enabled router. Follow these steps, and use the provided commands to troubleshoot events where a host appears to have connectivity issues due to implemented security policy:

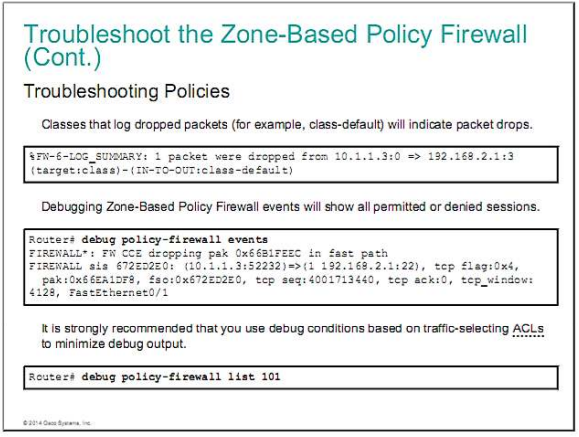
Verify that the problematic connection is allowed by an interzone or intrazone policy. If you have configured logging in the class-default class, use the **show logging** command to observe possible events that indicate a denied connection. Use the **show policy-map type inspect zone-pair sessions** command to see if your session enters the state table of the router. Additionally, consider using the **debug policy-firewall events** command to see if it is the Zone-Based Policy Firewall that handles the session, because this debug output will indicate creation of state table objects and denied packets even if logging has not been configured in the class-default class.

If the session appears to be permitted, verify that it is permitted by the correct class and policy map combination. Use the **show policy-map type inspect zone-pair** to observe matching statistics, if possible, because other sessions may also increase counters, or examine the configured class maps and policy maps manually.

If the problematic session is using a nonstandard port, and if it requires special inspection (for example, if it is a dynamic application, such as FTP or Oracle SQL*Net/TNS), use the **show ip port-map** command to verify that this port is defined by the PAM module.

Verify that the Zone-Based Policy Firewall properly inspects the session by performing a deep-dive in the inspection routines of the Zone-Based Policy Firewall. Use the **debug policy-firewall protocol** command, and debug either the application or transport protocol to observe possible issues with either protocol or router behavior.

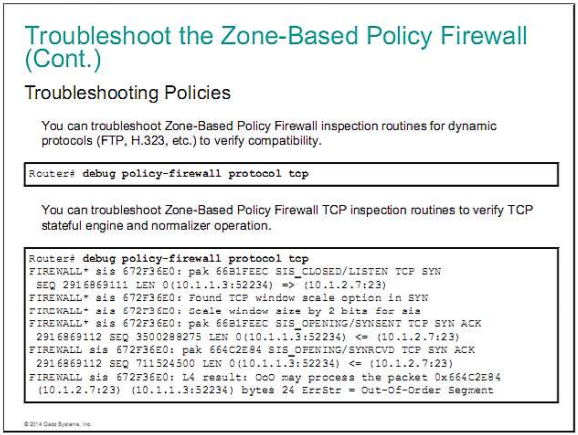
If all these steps do not resolve your issue, you may need to deploy troubleshooting tools that are beyond the scope of this course.



The first box indicates the message that a Zone-Based Policy Firewall-enabled router will generate if the class-default class is configured with a **log** action, and a packet or session is denied.

The second box shows an example output of the **debug policy-firewall events** command, showing a dropped and permitted session.

It is strongly recommended that you limit debugging to specific sessions, otherwise the amount of debug output is very likely to overwhelm you in the presence of other traffic. Use the **debug policy-firewall list** command to specify an extended ACL that will limit the flows that are subject to debugging (that is, the flows permitted by the specified ACL).

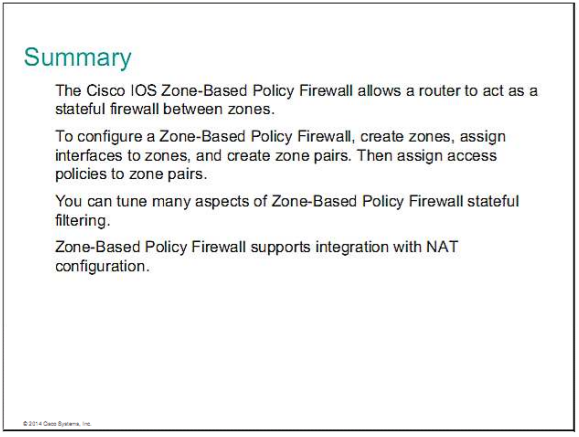


The **debug policy-firewall protocol** command allows for very extensive debugging of low-level inspection routines, and it should be used as a last resort. The figure shows the output of application-layer protocol (FTP) debugging and transport-layer (TCP) protocol debugging.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Summary

This topic summarizes the key points that were discussed in this lesson.



https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lesson 2

Deploying Advanced Cisco IOS Zone-Based Policy Firewall Access Policies

Overview

The Cisco IOS Zone-Based Policy Firewall represents the latest set of Cisco IOS Software firewall functions. Deploying access control based on OSI Layer 3 and 4 parameters establishes a minimal connectivity policy for network applications. However, such filtering alone cannot provide protection to exposed applications and control over access to specific types of content on the Internet. The Cisco IOS Zone-Based Policy Firewall provides advanced application layer (OSI Layer 5 to 7) filtering and content filtering controls to address these scenarios when risk assessment demands them. This lesson enables you to configure and verify these advanced controls of the Zone-Based Policy Firewall feature set.

Upon completing this lesson, you will be able to:

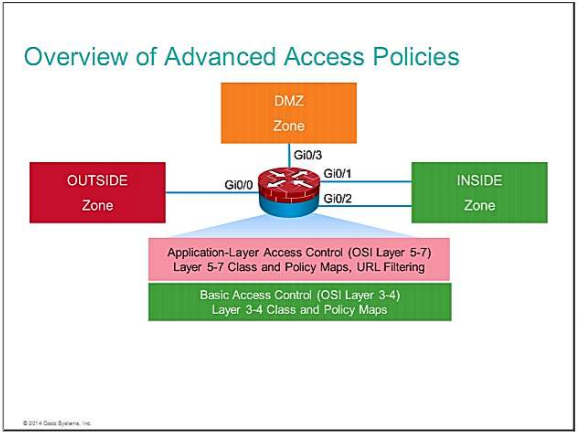
- Describe Cisco IOS Zone-Based Policy Firewall advanced access policies
- Describe the key features of Cisco IOS Zone-Based Policy Firewall application inspection
- Describe Cisco IOS Zone-Based Policy Firewall HTTP inspector
- Configure HTTP inspection on Cisco IOS Zone-Based Policy Firewall
- Verify HTTP inspection on Cisco IOS Zone-Based Policy Firewall
- Describe instant messaging inspection on Cisco IOS Zone-Based Policy Firewall.
- Describe peer-to-peer protocols inspection on Cisco IOS Zone-Based Policy Firewall
- Describe inspection of additional applications on Cisco IOS Zone-Based Policy Firewall
- Describe URL filtering methods on Cisco IOS Zone-Based Policy Firewall
- Configure local list-based URL filtering

https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Overview of Advanced Access Policies

This topic describes Cisco IOS Zone-Based Policy Firewall advanced access policies.



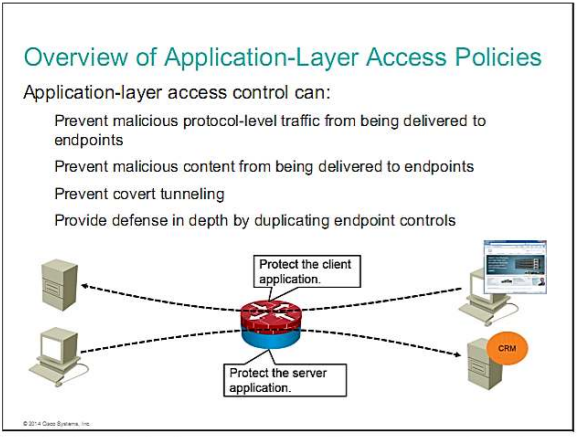
The Cisco IOS Zone-Based Policy Firewall provides multiple layers of access control to suit particular risk and application environments. Basic access control provides policies to control network access between zones based on Layer 3 and 4 criteria (IP addresses, protocols, and ports).

To provide deeper insight into network traffic, and allow you to control application traffic to protect potentially vulnerable applications, the Zone-Based Policy Firewall provides AIC functions that can parse application-layer protocols and filter inside it. As part of this functionality, you can also invoke content, or URL filtering, to restrict access to Internet content based on categories. This functionality increases productivity of company users and prevents access to possibly malicious sites.

https://t.me/learningnets

Overview of Application-Layer Access Policies

This topic describes the key features of Cisco IOS Zone-Based Policy Firewall application inspection.



Firewall application-layer filtering inspects protocols on OSI Layer 5 to 7, and can filter on application-layer protocol features and payloads to protect exposed server or client applications.

Application-layer filtering generally provides the following functions:

It can prevent malicious protocol-level traffic (malformed protocol units, access to vulnerable protocol functions, and access to unwanted applications on the server) from being delivered to the target, thus protecting the target before traffic even reaches it. For example, an application-layer-filtering firewall can only permit required HTTP protocol requests, and allow access only to a specific URL pattern (that is, specific application) on a web server.

It can prevent malicious content from being delivered to clients. For example, an application-layer-filtering firewall can permit only specific types of email or web content (HTML, text, Microsoft Office documents) to be delivered to an endpoint.

It can restrict or prevent covert tunneling channels, where attackers or legitimate users tunnel one protocol within another. For example, the firewall can block attempts to tunnel other protocols in their raw form through port 80 (HTTP), or other protocols encapsulated within HTTP fields that resemble a legitimate HTTP.

Very importantly, it can act as an independent, strong layer of defense to build a defense-in-depth solution. Network-based application-layer filtering is fully independent from the endpoint defenses, and works well even if the endpoint is vulnerable or misconfigured.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

You can implement application-layer controls on an AIC-capable firewall using the following four main approaches, which are often combined to achieve the desired filtering goals:

Protocol minimization: The AIC-capable firewall allows only a minimal required set of protocol features through to the endpoint. The purpose of such filtering is to minimize the attack surface of the endpoint, and reduce the likelihood that a particular vulnerability is exposed to the untrusted network. This approach can prevent both known and unknown attacks because it will block traffic that is not part of its minimal specification.

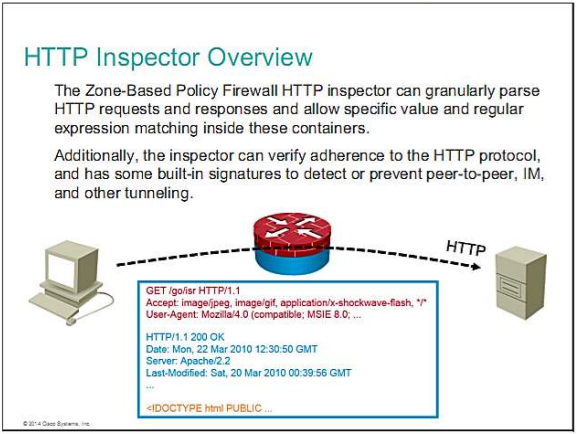
Payload minimization: The AIC-capable firewall allows only a minimal required set of application-layer payloads (application data) through to the endpoint. This approach can also prevent both known and unknown attacks because it will block data that is not part of its minimal specification.

Application-layer signatures: The AIC-capable firewall drops specific bad content (described by patterns known as signatures) inside application-layer protocols and payloads. Such an approach generally only prevents known attacks, described by signatures, and can be implemented using Zone-Based Policy Firewall AIC functions, Cisco IOS Software IPS functions, or the Cisco Integrated Services Router AIM and NME IPS modules.

Protocol verification: The AIC-capable firewall drops application-layer sessions that contain malformed (nonstandard) application-layer protocol units. This approach can also prevent both known and unknown attacks, and can prevent tunneling of other protocols inside legitimate protocols that are allowed through the firewall.

HTTP Inspector Overview

This topic describes Cisco IOS Zone-Based Policy Firewall HTTP inspector.



The rest of this lesson focuses on the Zone-Based Policy Firewall HTTP inspection routines, since HTTP is the most widely used protocol across most firewalls. Note that many of the following examples and functionalities can be deployed with other protocols as well.

The Zone-Based Policy Firewall AIC HTTP inspection routines inspect the HTTP protocol and allow administrators to specify granular access rules that provide protection of both HTTP clients and servers. The HTTP inspection routines analyze the HTTP protocol and break it up into granular containers, inside which administrators can filter specific protocol values, or use regular expressions to create custom pattern matching rules.

Additionally, the Zone-Based Policy Firewall provides built-in HTTP protocol verification routines, and includes some built-in application-layer signatures that can automatically detect tunneling of peer-to-peer, IM, and other sessions inside the HTTP protocol.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

HTTP Inspector Overview (Cont.)

Request Inspection Options

HTTP Request Field	Type of Match
Request Method	Specific values
Request URI	Regular expression(s)
Request URI Length	Numeric (greater than)
Request Arguments	Regular expression(s)
Request Arguments Length	Numeric (greater than)
Request Header Field (names and values)	Specific values or regular expression(s)
Request Header Field Count	Numeric (greater than)
Request Header Field Length	Numeric (greater than)
Request Header Count	Numeric (greater than)

© 2014 Cisco Systems, Inc.

HTTP Inspector Overview (Cont.)

Request Inspection Options (Cont.)

HTTP Request Field	Type of Match
Request Header Length	Numeric (greater than)
Request Body	Regular expression(s)
Request Body Length	Numeric (greater than, less than)
All fields	Port misuse signatures (IM, peer-to-peer, tunneling)

© 2014 Cisco Systems, Inc.

This table provides you with a reference of the available Zone-Based Policy Firewall AIC HTTP inspector's filtering containers for HTTP requests, and the method of matching that you can employ. The method can be either a list of specific values, hard-coded into Cisco IOS Software (for example, specific HTTP request methods), numeric comparisons, user-defined patterns using regular expressions, or some signatures hard-coded into Cisco IOS Software.

HTTP Inspector Overview (Cont.)

Response Inspection Options

HTTP Response Field	Type of Match
Response Status Line	Regular expression(s)
Response Body	Regular expression(s)
Response Body Length	Numeric (greater than)
Response Body Java Applets	Boolean (true or false)
Response Header Field (names and values)	Specific values or regular expression(s)
Response Header Field Count	Numeric (greater than)
Response Header Field Length	Numeric (greater than)
Response Header Count	Numeric (greater than)
Response Header Length	Numeric (greater than)

© 2014 Cisco Systems, Inc.

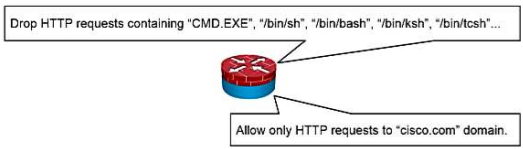
This table provides you with a reference of the available Zone-Based Policy Firewall AIC HTTP inspector's filtering containers for HTTP responses, and the method of matching that you can employ.

HTTP Inspector Overview (Cont.)

Regular Expressions

Regular expressions are a computer language used to describe patterns:

- Used to describe a set of strings without describing individual elements
- Used by Zone-Based Policy Firewall to match custom application-layer content



© 2014 Cisco Systems, Inc.

Regular expressions are a computer language that is used to describe patterns inside data, and are often used in networking when creating application-layer rules that use payload matching.

A regular expression is a string of characters that are used to describe a whole set of strings without describing individual set members. The Zone-Based Policy Firewall supports the use of regular expressions in many of its AIC inspectors, allowing administrators to write fully customized rules for their environments.

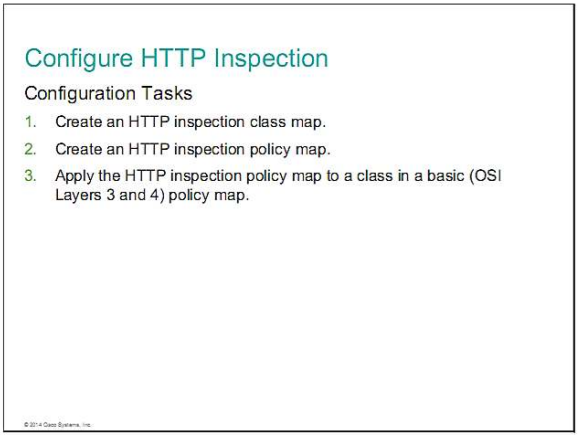
https://t.me/learningnets

The figure shows a typical example of where regular expressions could be used. In order to create a custom application-layer signature that would block HTTP requests containing the listed malicious strings in the HTTP URI, you could create a regular expression (or a set of expressions) to describe all of these strings in a manageable fashion. In the second example, you could create a regular expression that would describe allowed domains that can send content to clients, by describing these domains using a regular expression.

https://t.me/learningnets

Configure HTTP Inspection

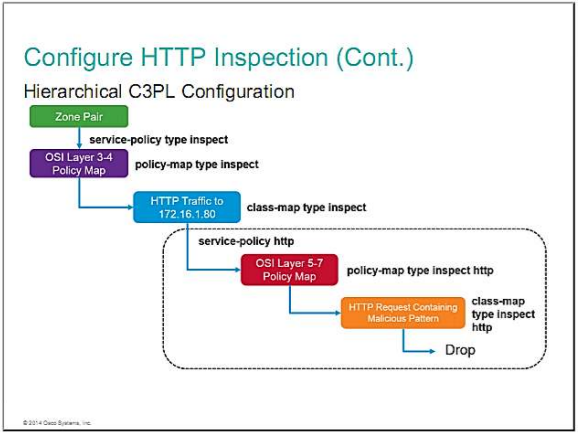
This topic describes how to configure HTTP inspection on Cisco IOS Zone-Based Policy Firewall.



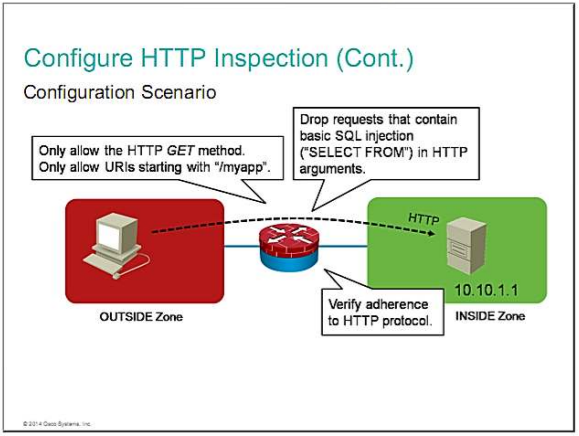
In order to configure an application-layer access policy for HTTP traffic, you will need to perform the following configuration tasks:

1. Create a special HTTP inspection class map to identify application-layer HTTP properties that will make sessions belong to this class.
2. Create an HTTP inspection policy map that will specify the policy actions that the router will take for traffic matching inspection class maps
3. Apply the HTTP inspection policy to a basic (OSI Layer 3 and 4) class map that matches generic HTTP traffic.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



This figure shows the hierarchical configuration of policy maps, class maps, AIC inspection policy maps, and AIC inspection class maps that are used for application-layer policy enforcement using C3PL.



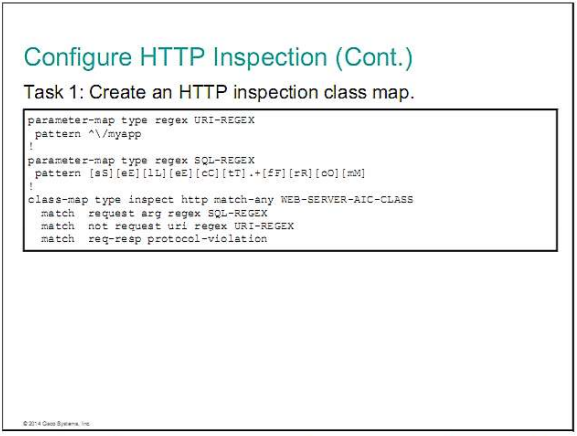
This figure shows the configuration scenario that will be used in upcoming configuration tasks. You will create the following application-layer policy between the OUTSIDE and INSIDE zones:

Only HTTP is allowed to the 10.10.1.1 server in the INSIDE zone, with the following policy:

- All hosts in the OUTSIDE zone can only use the HTTP GET method.
- All hosts in the OUTSIDE zone can only access HTTP URIs starting with the /myapp string.

- The router should drop all requests that contain basic SQL injection attempts (the string SELECT followed by the string FROM) inside HTTP arguments.
- The router should drop all requests that do not conform to the HTTP protocol.

The steps in the upcoming configuration sequence assume that the Cisco ISR is already configured with all required Zone-Based Policy Firewall zones (INSIDE, OUTSIDE), a basic Layer 3 and 4 policy that only allows HTTP to the internal server, and appropriate network interfaces assigned to these zones, as specified in the previous lesson.



In the first task of the configuration sequence, define the class (or multiple classes) that will match traffic inside HTTP application-layer sessions. In this example, you will configure a single class that will match unwanted traffic.

Start by creating regular expressions that will define legitimate URIs (URIs starting with /myapp), and define malicious HTTP arguments (data containing the SELECT string followed by the FROM string). Use the **parameter-map type regex** command to create a regular expression group, and the **pattern** command to specify the regular expression that will match data:

In the first regular expression, the value of ^\/myapp will match all data that starts with the /myapp string. The caret operator (^) defines the start of the matching container (the HTTP URI), and the \/ construct will match a literal slash.

In the second regular expression, the value of **[sS][eE][lL][eE][cC][tT].+[fF][rR][oO][mM]** will match any capitalization of the SELECT string, followed by any number of any non-newline characters (.+), followed by any capitalization of the FROM string. When defining signatures, it is important to account for all possible variations of malicious data, in order to prevent simple evasion attacks where the attacker could transform malicious data in a trivial manner (for example, by changing capitalization of the SQL statement) and still achieve the desired goal.

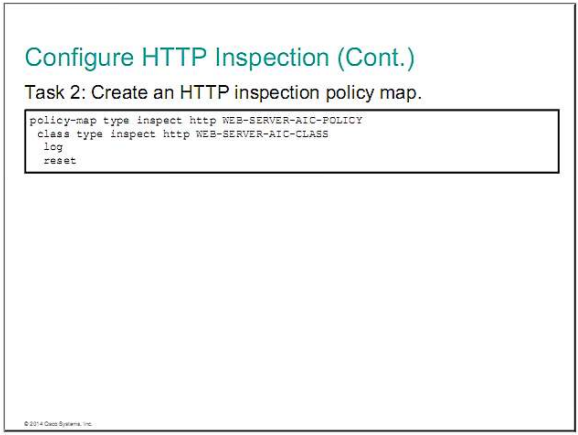
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Then, define an HTTP inspection class map using the **class-map type inspect http** command. Use the match-any variety of the class map because you will use multiple conditions, of which any can be met. Inside the HTTP inspection class map, define the conditions for malicious traffic as follows:

Use the **match request arg regex** command to define the malicious pattern that should be denied in the HTTP Arguments field.

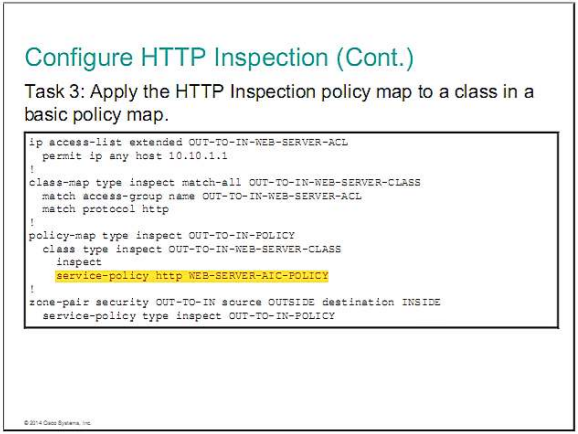
Use the **match not request uri regex** command, to define that all requests that do not match the legitimate URI pattern are malicious.

Use the **match req-resp protocol-violation** command to match all sessions violating the HTTP protocol.



In the second configuration task, you will create a policy map to specify the actions imposed on traffic that is identified by application-layer inspection class maps.

Use the **policy-map type inspect http** command to create a named HTTP inspection policy map. Inside this map, reference the previously configured HTTP inspection class map, using the **class type inspect http** command. Inside the class policy configuration mode, specify to **log** and **reset** sessions matching the HTTP inspection class.



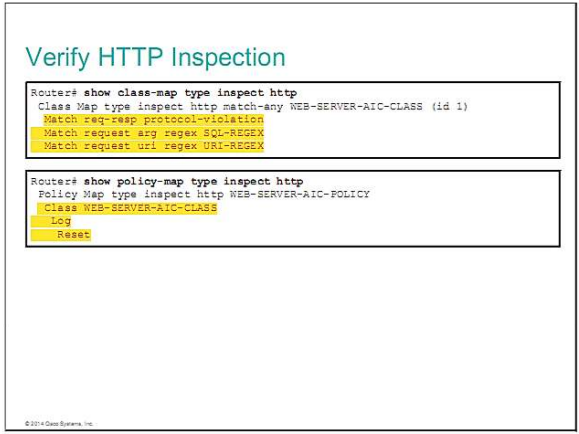
In the third configuration task, you will apply the HTTP inspection policy map to a Layer 3 and 4 class in a basic policy map. This example shows a basic policy map applied to a zone pair, and matches all HTTP traffic to the exposed web server.

In the basic (Layer 3 and 4) policy map, enter class configuration mode for the class that matches HTTP traffic. In this class, use the **service-policy http** command to apply the previously configured HTTP inspection policy map (that is, an OSI Layer 5 to 7 policy) to this class.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Verify HTTP Inspection

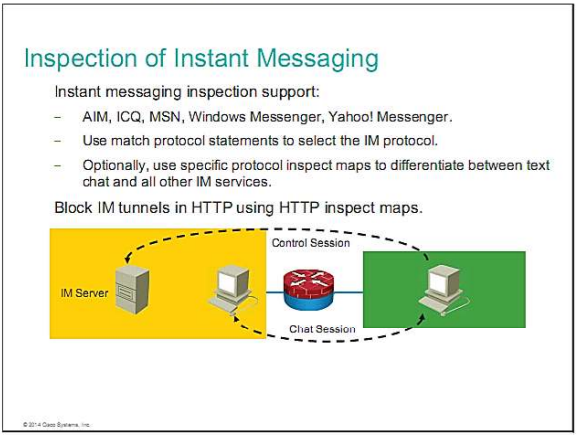
This topic describes how to verify HTTP inspection on Cisco IOS Zone-Based Policy Firewall.



You can use the usual **show class-map type inspect** command, extended with the application-layer protocol name (**http**) to display the configuration (matching criteria) of a Layer 5 to 7 inspection class map. Similarly, you can use the usual **show policy-map type inspect** command, extended with the application-layer protocol name (**http**) to display the policy actions that are configured for Layer 5 to 7 inspection class maps.

Inspection of Instant Messaging

This topic describes instant messaging inspection on Cisco IOS Zone-Based Policy Firewall.



The Zone-Based Policy Firewall supports the classification inspection of the AIM, ICQ, MSN, Windows Messenger, and Yahoo! Messenger protocols, where you can do one of the following:

Permit or deny their use, based on protocol identification.

Differentiate between text chat, and all other services inside the instant messaging protocol, and selectively permit or deny them.

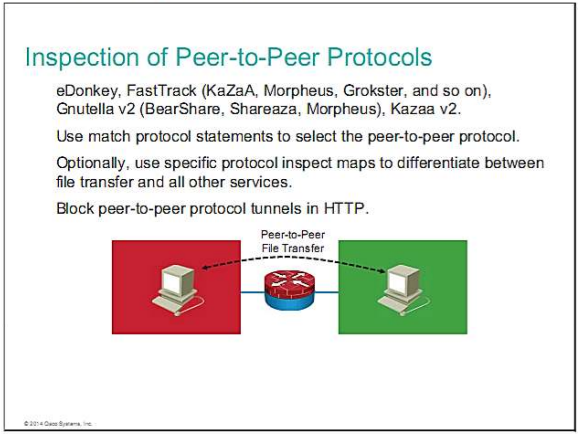
To match instant messaging protocols, use an appropriate match protocol statement inside a basic class map. Optionally, you can create AIC inspection policy maps for more granular inspection of these protocols.

The Zone-Based Policy Firewall can only identify instant messaging tunneling inside HTTP sessions, which most instant messaging will attempt if their native protocols are denied. If you are controlling instant messaging use, make sure that you also block messages inside HTTP, using an appropriate Zone-Based Policy Firewall HTTP AIC policy map configuration. The Zone-Based Policy Firewall includes predefined signatures that will help you classify such tunneled traffic.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Inspection of Peer-to-Peer Protocols

This topic describes peer-to-peer protocols inspection on Cisco IOS Zone-Based Policy Firewall.

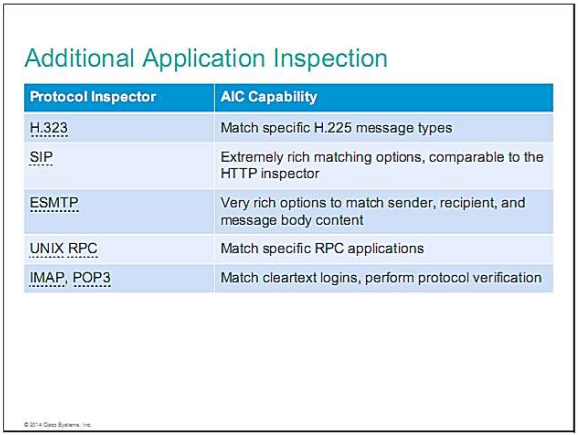


The Zone-Based Policy Firewall also supports inspection of peer-to-peer sessions, using their native protocols, and is able to identify them inside HTTP sessions. The Zone-Based Policy Firewall supports the classification of the eDonkey, FastTrack, Gnutella version 2, and Kazaa version 2 peer-to-peer protocols.

Like with instant messaging, use an appropriate match protocol statement inside a basic class map to match peer-to-peer protocols. Optionally create AIC inspection policy maps for some additional inspection options (differentiation between file transfer and other services, supported with some peer-to-peer varieties) for these protocols.

Additional Application Inspection

This topic describes inspection of additional applications on Cisco IOS Zone-Based Policy Firewall.



Zone-Based Policy Firewall supports application-layer inspection for a few other application-layer protocols. You can configure the following Zone-Based Policy Firewall inspection functionalities:

For the H.323 protocol suite: The H.323 AIC inspector is able to filter based on specific H.225 message types.

For SIP: The SIP AIC inspector offers an extremely rich set of filtering options that is comparable to those of the HTTP AIC inspector.

For ESMTP: The ESMTP AIC inspector offers a rich set of options with which you can filter based on ESMTP sender and recipient addresses, and various fields of the email message itself (for example, the type of content that is encapsulated inside MIME messages).

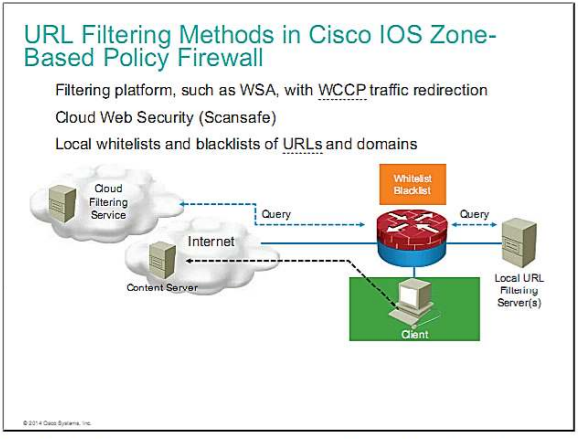
For UNIX RPCs: The UNIX RPC inspector can filter based on application identifiers inside RPC requests, and hence permit or deny access to specific RPC applications that are offered through the UNIX portmapper service.

For the IMAP and POP3 protocols: The AIC inspectors can verify the application-layer protocols, and detect and possibly prevent cleartext logins to the mail service.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

URL Filtering Methods in Cisco IOS Zone-Based Policy Firewall

This topic describes URL filtering methods on Cisco IOS Zone-Based Policy Firewall.



The Zone-Based Policy Firewall provides a mechanism to allow, block, or simply log web (HTTP URL) requests going through the router. The filtering is based on categories such as gaming, pornography, and weapons configured in Cisco IOS Software or an external filtering method. Whereas these categories are used to improve employee productivity, another set of categories is used to protect the network and resources: security categories protect users from adware, malware, spyware, and phishing sites.

To reduce the latency of future HTTP transactions and thus improve your experience, the router caches the categorization information and uses this information to verify policy, instead of sending every URL categorization request to external URL filtering servers.

When a client makes an HTTP request, the information about the accessed URL can be compared against one these methods, the first two of which are common and recommended:

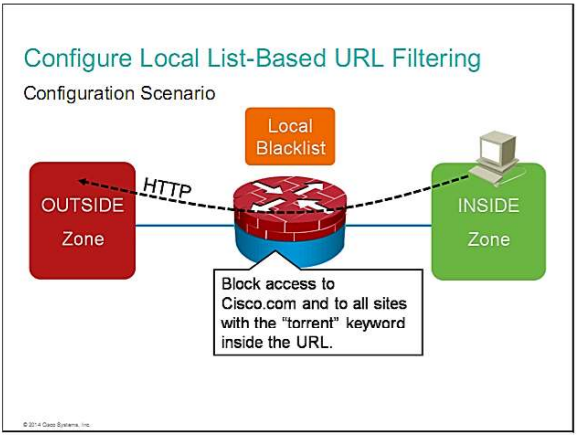
The router can consult with a specialized filtering platform, such as the Cisco Web Security Appliance, where administrators specify the web access policy for network users. The WSA is completely under local control. The traffic redirection is typically implemented using the WCCP.

Cisco Cloud Web Security, powered by Cisco Security Intelligence Operations, provides threat protection and control - delivered through the cloud.

You can configure blacklists and whitelists locally in Cisco IOS Software to permit and deny URLs and domains.

Configure Local List-Based URL Filtering

This topic describes how to configure local list-based URL filtering.



This figure shows the configuration scenario that will be used in upcoming configuration tasks. You will use a local blacklist on the router to deny access to specific sites based on server (domain) name and URL keywords. You will create the following URL filtering policy between the INSIDE and OUTSIDE zones:

- The router will inspect all outbound HTTP traffic.
- The router will block access to sites in the cisco.com domain, and to all sites containing the "torrent" keyword in the URL.

The steps in the upcoming configuration sequence assume that the Cisco Integrated Services Routers is already configured with all required Zone-Based Policy Firewall zones (INSIDE, OUTSIDE), a basic Layer 3 and 4 policy that only allows HTTP to the Internet, and appropriate network interfaces assigned to these zones, as specified in the previous lesson.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Configure Local List-Based URL Filtering (Cont.)

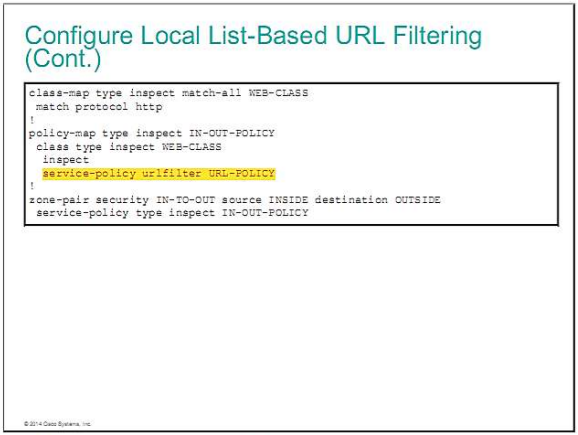
```
parameter-map type urlf-glob BAD-DOMAINS
  pattern cisco.com
parameter-map type urlf-glob BAD-KEYWORDS
  pattern torrent
!
class-map type urlfilter BAD-DOMAINS-CLASS
 match server-domain urlf-glob BAD-DOMAINS
!
class-map type urlfilter BAD-KEYWORDS-CLASS
 match url-keyword urlf-glob BAD-KEYWORDS
!
policy-map type inspect urlfilter URL-POLICY
  class type urlfilter BAD-DOMAINS-CLASS
    reset
  class type urlfilter BAD-KEYWORDS-CLASS
    reset
```

© 2014 Cisco Systems, Inc.

To configure URL filtering using local whitelists and blacklists, first define the server (domain) name and URL keyword patterns for use in local white lists and blacklists. Use the **parameter-map type urlf-glob** command to define a set of patterns that you want to include in a whitelist or blacklist. In this example, you will define the cisco.com pattern for server (domain) name matching, and torrent for URL keyword matching.

Next, define the class maps that will describe traffic that matches the desired domains or URL keywords. Use the **class-map type urlfilter** command to create a named URL filtering class map, and inside the class map, use the **match server-domain urlf-glob** or **match url-keyword urlf-glob** conditions to match on the configured server (domain) name pattern, and the URL keyword pattern, respectively.

Then, create a named URL filtering policy map using the **policy-map type inspect urlfilter** command. Inside the policy map, reference the two created URL filtering class maps, and specify the action to be used when a class is matched. In this example, the reset action drops all connections that match the two server (domain) name-based and URL keyword-based classes.

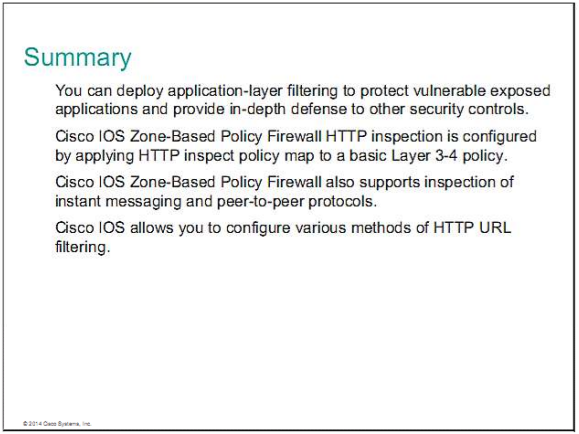


Finally, apply the configured URL filtering policy to a class in the basic policy map that governs HTTP access between zones.To enable URL filtering for a class, enter the policy map configuration mode, and specify the particular class that matches HTTP traffic. Inside the class, apply the URL filtering policy using the **service-policy urlfilter** command, referencing the custom URL filtering policy map.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Summary

This topic summarizes the key points that were discussed in this lesson.



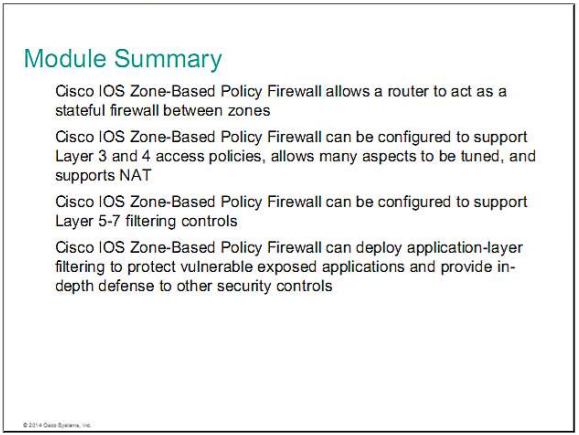
https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Module Summary

Overview

This topic summarizes the key points that were discussed in this module.



https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Module Self-Check

Questions

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

1. What two are default behaviors when tagging interfaces into Cisco IOS Zone-Based Policy Firewall zones? (Choose two) (Source: Deploying Basic Cisco IOS ZBPF Access Policies)

   A. By default, interfaces in the same zone can freely communicate.
   B. By default, interfaces in the same zone can not communicate.
   C. By default, all traffic is denied between zones.
   D. By default, all traffic is permitted between zones.

2. Match the configuration constructs on the left with their definition on the right.(Source: Deploying Basic Cisco IOS ZBPF Access Policies)

A.	Class map	‘	Augment basic inspection with the capability to recognize and apply service-specific actions
B.	Policy map	‘	Objects that describe different classes of traffic
C.	Parameter map	‘	Specify the actions to take when traffic matches defined criteria

3. Match the term on the left with the correct response on the right. (Source: Deploying Advanced Cisco IOS ZBPF Access Policies)

A.	Protocol minimization	‘	Allows only a minimal required set of protocol features through to the endpoint
B.	Protocol verification	‘	Drops specific bad content inside application-layer protocols and payloads
C.	Application-layer signatures	‘	Drops application-layer sessions that contain malformed (nonstandard) application-layer protocol units
D.	Payload minimization	‘	Allows only a minimal required set of application data through to the endpoint

https://t.me/learningnets

4. In which two class maps would you use an ACL to match interesting traffic when inspecting HTTP in Cisco IOS Zone-Based Policy Firewall? (Choose two.) (Source: Deploying Advanced Cisco IOS ZBPF Access Policies)

A. **class-map type inspect match-all**
B. **class-map type inspect match-any**
C. **class-map type inspect http match-all**
D. **class-map type inspect http match-any**
E. **class-map type inspect protocol match-all**
F. **class-map type inspect protocol match-any**

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Answer Key

1. A, C

2.

A.	Class map	Objects that describe different classes of traffic
B.	Policy map	Specify the actions to take when traffic matches defined criteria
C.	Parameter map	Augment basic inspection with the capability to recognize and apply service-specific actions

3.

A.	Protocol minimization	Allows only a minimal required set of protocol features through to the endpoint
B.	Payload minimization	Allows only a minimal required set of application data through to the endpoint
C.	Application-layer signatures	Drops specific bad content inside application-layer protocols and payloads
D.	Protocol verification	Drops application-layer sessions that contain malformed (nonstandard) application-layer protocol units

4. A, B

https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Glossary

Term	Definition
AAA	authentication, authorization, and accounting. Pronounced "triple a."
ACE	access control entry.
ACK	acknowledgment. Notification sent from one network device to another to acknowledge that some event occurred (for example, the receipt of a message).
ACL	access control list. A list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).
ACL	access control list. A list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).
AIC	Application Inspection and Control.
AIM	Advanced Integration Module
ALG	application layer gateway.
ASCII	American Standard Code for Information Interchange. 8-bit code for character representation (7 bits plus parity).
AVC	Application Visibility and Control.
BGP	Border Gateway Protocol. Interdomain routing protocol that replaces EGP. BGP exchanges reachability information with other BGP systems. It is defined by RFC 1163.
C3PL	Cisco Common Classification Policy Language
CBAC	Context-Based Access Control
CLI	command-line interface. An interface that allows the user to interact with the operating system by entering commands and optional arguments. The UNIX operating system and DOS provide CLIs.
CLI	command-line interface. An interface that allows the user to interact with the operating system by entering commands and optional arguments. The UNIX operating system and DOS provide CLIs.
CLI	command-line interface. An interface that allows the user to interact with the operating system by entering commands and optional arguments. The UNIX operating system and DOS provide CLIs.
CTIQBE	Computer Telephony Interface Quick Buffer Encoding.
DCD	dead connection detection.
DCE/RCP	Distributed Computing Environment/Remote Procedure Call.

https://t.me/learningnets

Term	Definition
DCOM	Distributed Component Object Model. Protocol that enables software components to communicate directly over a network. Developed by Microsoft and previously called Network OLE, DCOM is designed for use across multiple network transports, including such Internet protocols as HTTP.
DDoS	distributed DoS
DLSw	Data-Link Switching
DMZ	demilitarized zone.
DN	Domain Name
DNS	Domain Name System. System used on the Internet for translating names of network nodes into addresses.
DoS	denial of service. An intentional or unintentional attack on a device that makes the resource unavailable to perform its normal function.
DPI	deep packet inspection.
DSCP	differentiated services code point.
ESMTP	Extended Simple Mail Transfer Protocol. Extended version of the Simple Mail Transfer Protocol (SMTP), which includes additional functionality, such as delivery notification and session delivery. ESMTP is described in RFC 1869, *SMTP Service Extensions*.
ESP	Encapsulating Security Payload. Security protocol that provides data privacy services, optional data authentication, and antiplay services. ESP encapsulates the data to be protected.
FIN	Finish
FIN	finish
FPM	Flexible Packet Matching.
FQDN	fully qualified domain name. FQDN is the full name of a system, rather than just its host name. For example, aldebaran is a host name, and aldebaran.interop.com is an FQDN.
FTP	File Transfer Protocol. Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP is defined in RFC 959.
GET	Group Encrypted Transport.
GRE	Generic Routing Encapsulation. Tunneling protocol that was developed by Cisco and that can encapsulate a variety of protocol packet types inside IP tunnels. This process creates a virtual point-to-point link to Cisco routers at remote points over an IP network.
GTP	General Packet Radio Service (GPRS) Tunneling Protocol.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Term	Definition
GUI	graphical user interface. A user environment that uses pictorial as well as textual representations of the input and the output of applications and the hierarchical or other data structure in which information is stored. Such conventions as buttons, icons, and windows are typical, and many actions are performed using a pointing device (such as a mouse). Microsoft Windows and the Apple Macintosh are prominent examples of platforms using a GUI.
H.225.0	An ITU standard that governs H.225.0 session establishment and packetization. H.225.0 actually describes several different protocols: RAS, use of Q.931, and use of RTP.
H.323	H.323 allows dissimilar communication devices to communicate with each other by using a standardized communication protocol. H.323 defines a common set of codecs, call setup and negotiating procedures, and basic data transport methods.
HTML	Hypertext Markup Language. Simple hypertext document formatting language that uses tags to indicate how a given part of a document should be interpreted by a viewing application, such as a Web browser.
HTTP	Hypertext Transfer Protocol. The protocol used by Web browsers and Web servers to transfer files, such as text and graphic files.
ICMP	Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. Documented in RFC 792.
IETF	Internet Engineering Task Force. Task force consisting of over 80 working groups responsible for developing Internet standards. The IETF operates under the auspices of ISOC.
IM	instant messaging.
IMAP	Internet Message Access Protocol. Method of accessing email or bulletin board messages kept on a mail server that can be shared. IMAP permits client email applications to access remote message stores as if they were local without actually transferring the message.
IP	Internet Protocol. Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Defined in RFC 791.
IP address	32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address. CIDR provides a new way of representing IP addresses and subnet masks. Also called an Internet address.

https://t.me/learningnets

Term	Definition
IP address	32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address. CIDR provides a new way of representing IP addresses and subnet masks. Also called an Internet address.
IPS	intrusion prevention system.
IPsec	IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer. IPsec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.
IPv4	IP version 4. Internet Protocol version 4 is the fourth version in the development of the IP and the first version of the protocol to be widely deployed. Along with IPv6, IPv4 is at the core of standards-based internetworking methods of the Internet. IPv4 is still used to route most traffic across the Internet. IPv4 is a connectionless protocol for use on packet-switched link layer networks (for example, Ethernet). It operates on a best-effort delivery model in that it does not guarantee delivery and does not assure proper sequencing or avoidance of duplicate delivery.
IPv6	IP version 6. Replacement for the current version of IP (version 4). IPv6 includes support for flow ID in the packet header, which can be used to identify flows. Formerly called IPng (next generation).
LDAP	Lightweight Directory Access Protocol. Protocol that provides access for management and browser applications that provide read/write interactive access to the X.500 Directory.
LDAP	Lightweight Directory Access Protocol. Protocol that provides access for management and browser applications that provide read/write interactive access to the X.500 Directory.
MGCP	Media Gateway Control Protocol. A merging of the IPDC and SGCP protocols.
MIME	Multipurpose Internet Mail Extension. Standard for transmitting nontext data (or data that cannot be represented in plain ASCII code) in Internet mail, such as binary, foreign language text (such as Russian or Chinese), audio, or video data. MIME is defined in RFC 2045.
MMP	Mobile Multiplexing Protocol.
MPF	Modular Policy Framework.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Term	Definition
MPLS	Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.
MQC	modular QoS CLI. Command line structure that allows modular configuration of QoS configuration elements to provide independence between classification and policy.
Multi-VRF	Multi-VRF Customer Edge
NAT	Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. Also known as Network Address Translator.
NetBIOS	Network Basic Input/Output System. API used by applications on an IBM LAN to request services from lower-level network processes. These services might include session establishment and termination, and information transfer.
NTP	Network Time Protocol. Protocol built on top of TCP that ensures accurate local timekeeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.
OSI	Open Systems Interconnection. International standardization program created by ISO and ITU-T to develop standards for data networking that facilitate multivendor equipment interoperability.
OSPF	Open Shortest Path First. Link-state, hierarchical IGP routing algorithm proposed as a successor to RIP in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing. OSPF was derived from an early version of the IS-IS protocol.
PAM	Port-to-Application Mapping
POP	Post Office Protocol. Protocol that client email applications use to retrieve mail from a mail server.
POST	power-on self test. Set of hardware diagnostics that runs on a hardware device when this device is powered on.
QoS	quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.
RADIUS	Remote Authentication Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.
RAS	Registration, Admission, and Status.

https://t.me/learningnets

Term	Definition
RPC	remote-procedure call. Technological foundation of client/server computing. RPCs are procedure calls that are built or specified by clients and are executed on servers, with the results returned over the network to the clients.
rsh	remote shell protocol. Protocol that allows a user to execute commands on a remote system without having to log in to the system. For example, rsh can be used to remotely examine the status of a number of access servers without connecting to each communication server, executing the command, and then disconnecting from the communication server.
RST	reset. A type of message.
RTP	Real-Time Transport Protocol. Commonly used with IP networks. RTP is designed to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services. RTP provides such services as payload type identification, sequence numbering, timestamping, and delivery monitoring to real-time applications.
RTSP	Real Time Streaming Protocol. Enables the controlled delivery of real-time data, such as audio and video. Sources of data can include both live data feeds, such as live audio and video, and stored content, such as pre-recorded events. RTSP is designed to work with established protocols, such as RTP and HTTP.
RTT	round-trip time. Time required for a network communication to travel from the source to the destination and back. RTT includes the time required for the destination to process the message from the source and to generate a reply. RTT is used by some routing algorithms to aid in calculating optimal routes.
SCCP	Skinny Client Control Protocol.
SIP	Session Initiation Protocol. Protocol developed by the IETF MMUSIC Working Group as an alternative to H.323. SIP features are compliant with IETF RFC 2543, published in March 1999. SIP equips platforms to signal the setup of voice and multimedia calls over IP networks.
SNMP	Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.
SPI	security parameter index. This is a number that, together with a destination IP address and security protocol, uniquely identifies a particular security association. When using IKE to establish the security associations, the SPI for each security association is a pseudo-randomly derived number. Without IKE, the SPI is manually specified for each security association.
SQL	Structured Query Language. International standard language for defining and accessing relational databases.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Term	Definition
SSH	Secure Shell Protocol. Protocol that provides a secure remote connection to a router through a TCP application.
SSL	Secure Socket Layer. Encryption technology for the Web used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.
SunRPC	Sun Remote Procedure Call.
SYN	synchronization.
SYN	synchronization.
TAC	Cisco Technical Assistance Center.
TACACS+	Terminal Access Controller Access Control System Plus. Proprietary Cisco enhancement to TACACS. Provides additional support for authentication, authorization, and accounting.
TCP	Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.
TCP/IP	Transmission Control Protocol/Internet Protocol. Common name for the suite of protocols developed by the U.S. DoD in the 1970s to support the construction of worldwide internetworks. TCP and IP are the two best-known protocols in the suite.
TFTP	Trivial File Transfer Protocol. A simplified version of FTP that is generally used for automated transfer of configuration or boot files from one computer to another over a network, usually without the use of client authentication.
ToS	type of service.
TTL	Time to Live. A mechanism that limits the lifespan or lifetime of data in a computer or network.
TTL	Time to Live. A mechanism that limits the lifespan or lifetime of data in a computer or network.
UDP	User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.
UIO	Universal I/O serial port (Cisco router).
UNIX	Operating system developed in 1969 at Bell Laboratories. UNIX has gone through several iterations since its inception. These include UNIX 4.3 BSD (Berkeley Standard Distribution), developed at the University of California at Berkeley, and UNIX System V, Release 4.0, developed by AT&T.

https://t.me/learningnets

Term	Definition
URI	uniform resource identifier. Type of formatted identifier that encapsulates the name of an Internet object, and labels it with an identification of the name space, thus producing a member of the universal set of names in registered name spaces and of addresses referring to registered protocols or name spaces. [RFC 1630]
URL	uniform resource locator. Type of formatted identifier that describes the access method and the location of an information resource object on the Internet. [RFC 1738]
VLAN	virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.
VM	virtual machine.
VoIP	Voice over IP. The capability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. In VoIP, the DSP segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323.
VPN	virtual private network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses tunneling to encrypt all information at the IP level.
VRF	A VPN routing/forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.
WCCP	Web Cache Communication Protocol. WCCP is a protocol for communication between routers and Web caches. Two versions exist: WCCP Version 1 (WCCPv1) and WCCP Version2 (WCCPv2). The two versions are incompatible. Cisco IOS images can support either of the two versions or both.
WMI	Windows Management Instrumentation.
X.25	ITU-T standard that defines how connections between DTE and DCE are maintained for remote terminal access and computer communications in PDNs. X.25 specifies LAPB, a data link layer protocol, and PLP, a network layer protocol. Frame Relay has to some degree superseded X.25.
XDMCP	X Display Manager Control Protocol. Protocol used to communicate between X terminals and workstations running the UNIX operating system.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Term	Definition
XML	extensible markup language. A standard maintained by the World Wide Web Consortium (W3C). It defines a syntax that lets you create markup languages to specify information structures. Information structures define the type of information, for example, subscriber name or address, not how the information looks (bold, italic, and so on). External processes can manipulate these information structures and publish them in a variety of formats. Text markup language designed to enable the use of SGML on the World Wide Web. XML allows you to define your own customized markup language.
ZFW	Zone-Based Policy Firewall

https://t.me/learningnets