SITCS

Implementing Cisco Threat Control Solutions

Volume 1 **Student Guide**
Version 1.0

Part Number: 97-3337-01

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

Welcome Students

Note Students, this letter describes important course evaluation access information.

Welcome to Cisco Systems Learning. Through the Cisco Learning Partner Program, Cisco is committed to bringing you the highest-quality training in the industry. Cisco learning products are designed to advance your professional goals and give you the expertise that you need to build and maintain strategic networks.

Cisco relies on customer feedback to guide business decisions. Therefore, your valuable input will help shape future Cisco course curricula, products, and training offerings. Please complete a brief Cisco online course evaluation of your instructor and the course materials in this student kit. On the final day of class, your instructor will provide you with a URL, directing you to a short post-course evaluation. If there is no Internet access in the classroom, please complete the evaluation within the next 48 hours or as soon as you can access the web.

On behalf of Cisco, thank you for choosing Cisco Learning Partners for your Internet technology training.

Sincerely,
Cisco Systems Learning

https://t.me/learningnets

https://t.me/learningnets

Table of Contents

Course Introduction *I-1*

Overview **I-1**

Course Goal and Objectives **I-3**

Course Flow **I-4**

Your Training Curriculum **I-5**

Additional References **I-7**

Cisco ASA (CX) NGFW Services *1-1*

Describing the Cisco ASA (CX) NGFW Services **1-3**

Cisco Modular Network Architecture and Cisco (CX) NGFW Services 1-4

Cisco ASA (CX) NGFW Benefits and Components 1-8

Cisco ASA (CX) NGFW Broad and Web AVC 1-10

Cisco ASA (CX) NGFW Policy Types 1-12

Cisco ASA (CX) NGFW Compatibility with Existing Cisco ASA Features 1-13

Cisco ASA 5585-X NGFW CX-SSP Hardware Module 1-15

Cisco ASA 5500-X (CX) NGFW Software Module 1-16

Summary 1-17

Describing the Cisco ASA (CX) NGFW Management Architecture **1-19**

Cisco ASA (CX) NGFW Management Architecture 1-20

On-Box and Off-Box Cisco PRSM 1-22

Cisco PRSM GUI Basic Functions 1-25

Cisco ASA (CX) NGFW Management Interface 1-29

Cisco ASA (CX) NGFW CLI Operations 1-33

Cisco ASA (CX) NGFW Licenses 1-38

Cisco Off-Box PRSM License 1-41

Cisco ASA (CX) NGFW and Off-Box Cisco PRSM License Management 1-42

Summary 1-43

Configuring Cisco ASA (CX) NGFW Policy Objects **1-45**

Cisco ASA-to-Cisco ASA (CX) NGFW Traffic Redirection 1-47

Cisco ASA (CX) NGFW Policy Structure 1-50

Cisco ASA (CX) NGFW Policy Object Types 1-53

Cisco ASA (CX) NGFW Network Objects 1-57

Cisco ASA (CX) NGFW Service Objects and Service Groups 1-60

Cisco ASA (CX) NGFW Application Objects and Application Service Objects 1-62

Cisco ASA (CX) NGFW URL Objects 1-64

Cisco ASA (CX) NGFW User Agent Objects 1-66

Cisco ASA (CX) NGFW Identity Objects 1-67

Cisco ASA (CX) NGFW Source Object and Destination Object Groups 1-68

Cisco ASA (CX) NGFW Secure Mobility Objects 1-70

Cisco ASA (CX) NGFW Action Profile Objects 1-71

Policy Objects in Cisco ASA (CX) NGFW Policies 1-73

Tags, Ticket IDs, and Metadata 1-75

https://t.me/learningnets

Summary 1-78
Monitoring Cisco ASA (CX) NGFW Operations 1-79
Cisco PRSM Dashboards and Reports 1-80
Cisco PRSM Event Viewer 1-83
Cisco SIO Update Verifications 1-86
Summary 1-88
Configuring Cisco ASA (CX) NGFW Access Policies 1-89
Cisco ASA (CX) NGFW Access Policy Configuration 1-90
Cisco ASA (CX) NGFW Application Control Configuration 1-95
Cisco ASA (CX) NGFW URL Filtering Configuration 1-99
Cisco ASA (CX) NGFW File Filtering Profile Configuration 1-100
Cisco ASA (CX) NGFW Web Reputation Profile Configuration 1-102
Cisco ASA (CX) NGFW Access Policies Troubleshooting 1-104
Summary 1-105
Configuring Cisco ASA (CX) NGFW Identity Policies 1-107
Cisco ASA (CX) NGFW Active and Passive Authentications 1-109
Cisco ASA (CX) NGFW Authentication Realms 1-114
Cisco ASA (CX) NGFW ADI 1-115
Cisco ASA (CX) NGFW Identity-Based Policy Configuration 1-117
LDAP Authentication Realm and Server Configurations 1-118
Active Directory Authentication Realm and Server Configurations 1-120
Cisco ASA (CX) NGFW-to-Cisco CDA Integration Configurations 1-122
Cisco ASA (CX) NGFW Identity Policies with Active Authentication 1-123
Cisco ASA (CX) NGFW Identity Policies with Passive Authentication 1-125
Cisco ASA (CX) NGFW Authentication Settings Configuration 1-126
Cisco ASA (CX) NGFW Access and Decryption Policies with Identity Objects 1-127
Cisco ASA (CX) NGFW User Identity in Event Viewer 1-130
Cisco ASA CX Identity Policy Troubleshooting 1-131
Summary 1-132
Configuring Cisco ASA (CX) NGFW Decryption Policies 1-135
Cisco ASA (CX) NGFW Decryption Policies 1-136
Cisco ASA (CX) NGFW Decryption Configurations 1-145
Cisco ASA (CX) NGFW Decryption Policy Configuration 1-151
Cisco ASA CX Decryption Policy Troubleshooting 1-153
Cisco ASA (CX) NGFW Identity, Decryption, and Access Policy Interactions 1-154
Summary 1-156
Module Summary 1-157
References 1-158
Module Self-Check 1-159
Cisco Web Security Appliance 2-1
Describing the Cisco Web Security Appliance Solutions 2-3
Cisco Modular Network Architecture and Cisco WSA 2-5
Cisco WSA Overview 2-7
Cisco WSA Architecture 2-8

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

Cisco WSA Malware Detection and Protection 2-10
Cisco Web-Based Reputation Score 2-11
Cisco WSA Acceptable Use Policy Enforcement 2-13
Cisco WSA GUI Management 2-14
Cisco WSA Committing the Configuration Changes 2-15
Cisco WSA Policy Types Overview 2-16
Cisco WSA Access Policies 2-18
Cisco WSA Identity: For Whom Does This Policy Apply To? 2-19
Cisco WSA Identity Example 2-21
Cisco WSA Policy Assignment Using Identity 2-23
Cisco WSA Identity and Authentication 2-24
Cisco WSA Policy Trace Tool 2-25
Summary 2-26

Integrating the Cisco Web Security Appliance 2-27

Explicit vs. Transparent Proxy Mode 2-28
Explicit Proxy Mode 2-29
PAC Files 2-30
PAC File Deployment Options 2-32
PAC File Hosting on Cisco WSA 2-33
Traffic Redirection in Transparent Mode 2-34
Connecting the Cisco WSA to a WCCP Router 2-35
Verifying WCCP 2-39
Summary 2-40

Configuring Cisco Web Security Appliance Identities and User Authentication Controls 2-41

Configure Identities to Group Client Transactions 2-43
Configure Policy Groups 2-45
The Need for User Authentication 2-47
Authentication Protocols and Schemes 2-48
Basic Authentication in Explicit Proxy and Transparent Proxy Mode 2-50
Configure Realms and Realm Sequences 2-52
Configure NTLM Realm for Active Directory 2-53
Join Cisco WSA to Active Directory 2-55
Configure Global Authentication Settings 2-56
Configure an Identity to Require Authentication (Basic or NTLMSSP) 2-58
Configure an Identity to Require Transparent User Identification 2-59
Configure LDAP Realm for LDAP Servers 2-61
Define How User Information Is Stored in LDAP 2-62
Bind Cisco WSA to the LDAP Directory 2-63
LDAP Group Authorization 2-64
Allowing Guest Access to Users Who Fail Authentication 2-65
Testing Authentication Settings 2-68
Authenticated Users in Reports 2-70
Summary 2-71

Configuring Cisco Web Security Appliance Acceptable Use Controls 2-73

Acceptable Use Controls 2-75
URL Categorizing Process 2-77
Application Visibility and Control Overview 2-78
Streaming Media Bandwidth Control Overview 2-79
Enable Acceptable Use Controls 2-80
Using the Policies Table 2-81
Configure URL Filtering 2-83
Enable Safe Search and Site Content Ratings 2-85
Configure Custom URL Categories 2-86
URL Category Reports 2-87
Configuring AVC 2-89
Configure Media Bandwidth Limits 2-91
AVC Reports 2-92
Summary 2-93

Configuring Cisco Web Security Appliance Anti-Malware Controls 2-95

Dynamic Vectoring and Streaming Engine Overview 2-96
Contrast Webroot with Sophos or McAfee Malware Scanning 2-98
Adaptive Scanning Overview 2-100
Web Reputation Filtering Overview 2-101
Enable Web Reputation Filtering, Adaptive Scanning and Malware Scanning 2-103
Configure Inbound Web Reputation Filtering and Malware Scanning 2-104
Configure Outbound Malware Scanning 2-107
Malware Reports 2-109
Summary 2-110

Configuring Cisco Web Security Appliance Decryption 2-111

HTTPS Proxy Operations Overview 2-112
Enable HTTPS Proxy 2-114
Invalid Destination Web Server Certificate Handling 2-116
Configure Decryption Policies 2-118
Summary 2-120

Configuring Cisco Web Security Appliance Data Security Controls 2-121

Cisco WSA Data Security Overview 2-122
Data Security Policies 2-124
Control Uploaded Content 2-126
External Data Loss Prevention 2-128
Add an ICAP Server 2-129
Summary 2-130

Module Summary 2-131

References 2-131

Module Self-Check 2-133

Cisco Cloud Web Security 3-1

Describing the Cisco Cloud Web Security Solutions 3-3

Cisco Modular Network Architecture and Cisco Cloud Web Security (CWS) 3-4
Cisco Cloud Web Security Overview 3-7

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

Cisco Cloud Web Security Traffic Flow Overview 3-9
Cisco Cloud Web Security URL Filtering, AVC and Reporting Features Overview 3-10
Cisco Cloud Web Security Scanning Processes and Day Zero Outbreak Intelligence Overview 3-11
Cisco ScanCenter Overview 3-13
Summary 3-14
Configuring Cisco Cloud Web Security Connectors 3-15
Cisco Cloud Web Security Traffic Redirection Overview 3-17
Cisco Cloud Web Security Authentication Key 3-18
Authentication Key Generation from the Cisco ScanCenter 3-20
Verifying Traffic Redirection to CWS Using Special URL 3-21
Cisco ASA Cloud Web Security Overview 3-22
Cisco ASA Cloud Web Security Basic Configuration Using ASDM 3-23
Cisco ASA Cloud Web Security Basic Configuration Using the CLI 3-27
Cisco ASA Cloud Web Security Configuration with the Whitelist and Identity Options Using the CLI 3-29
Verifying Cisco ASA Cloud Web Security Operations Using the Cisco ASDM 3-31
Verifying Cisco ASA Cloud Web Security Operations Using the CLI 3-32
Cisco AnyConnect Web Security Module Overview 3-34
Cisco AnyConnect Web Security Module for Standalone Use Overview 3-35
Configure Cisco AnyConnect Web Security Module for Standalone Use 3-37
Configure Cisco ASA to Download the Web Security Module to the Client Machine 3-42
Verifying Cisco AnyConnect Web Security Module Operations 3-43
Cisco ISR G2 Cloud Web Security Overview 3-45
Cisco ISR G2 Cloud Web Security Configuration 3-47
Cisco ISR G2 Cloud Web Security Verification 3-50
Cisco WSA Cloud Web Security Overview 3-52
Summary 3-53
Describing the Web Filtering Policy in Cisco ScanCenter 3-55
ScanCenter Web Filtering Policy Overview 3-56
ScanCenter Web Filtering Policy Configuration 3-58
HTTPS Inspection Configuration Overview 3-64
ScanCenter Web Filtering Verification 3-65
ScanCenter Web Filtering Reporting 3-68
Summary 3-71
Module Summary 3-73
References 3-73
Module Self-Check 3-75
Glossary G-1

https://t.me/learningnets

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

Course Introduction

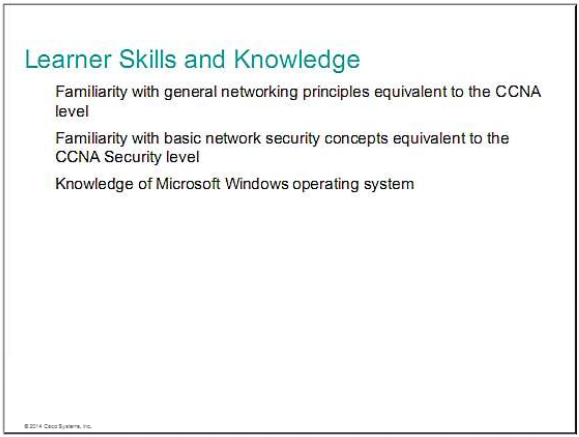
Overview

This Implementing Cisco Threat Control Solutions (SITCS) course covers the Cisco context aware security solutions offering Application Visibility and Control (AVC), Web Security (appliance and cloud based), Email Security and Intrusion Prevention (IPS) to prevent against today's new and emerging threats. The student will gain hands-on experience with configuring context-aware security functionality and assuring web security using three different solutions: on the Cisco ASA (CX) Next-Generation Firewall (NGFW), Cisco Web Security Appliance (WSA) and Cisco Cloud Web Security (CWS). This solutions deliver web security and control for organizations of all sizes, with multiple deployment options and tight integration into your existing network. Then the course describes how to use Cisco Email Security Appliance (ESA) to protects the email infrastructure and employees who use email at work by filtering unsolicited and malicious email before it reaches the user. The course ends with implementing Intrusion Prevention System (IPS) solutions, which can identify and mitigate attacks with market-leading, context-aware threat prevention that augments your firewall and VPN deployments.

https://t.me/learningnets

Learner Skills and Knowledge

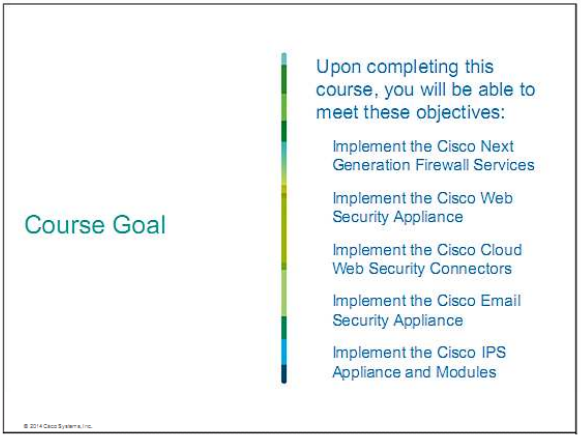
This subtopic lists the skills and knowledge that learners must possess to benefit fully from the course. The subtopic also includes recommended Cisco learning offerings that learners should first complete to benefit fully from this course.



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

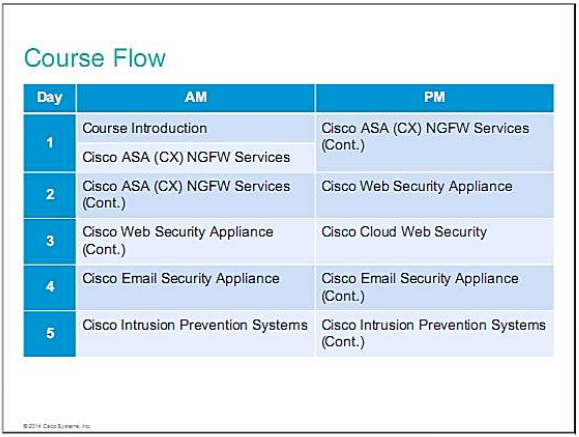
Course Goal and Objectives

This topic describes the course goal and objectives.



Course Flow

This topic presents the suggested flow of the course materials.



The schedule reflects the recommended structure for this course. This structure allows enough time for the instructor to present the course information and for you to work through the lab activities. The exact timing of the subject materials and labs depends on the pace of your specific class.

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

Your Training Curriculum

This topic presents the training curriculum for this course.



You are encouraged to join the Cisco Certification Community, a discussion forum open to anyone holding a valid Cisco Career Certification (such as Cisco CCIE®, CCNA®, CCDA®, CCNP®, CCDP®, CCIP®, CCNP® Security and CCNP® Voice, or CCSP™). It provides a gathering place for Cisco certified professionals to share questions, suggestions, and information about Cisco Career Certification programs and other certification-related topics. For more information, visit http://www.cisco.com/go/certifications.

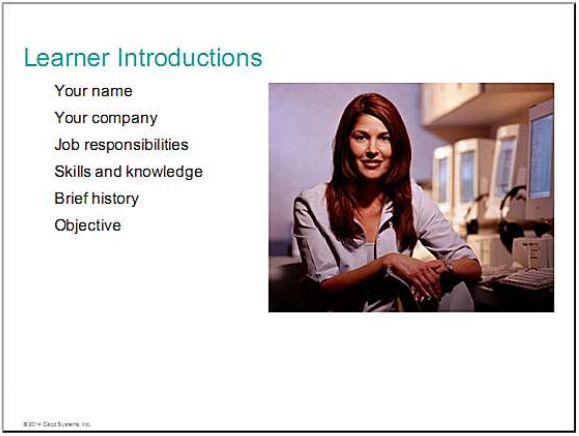
Training Curriculum

This subtopic presents the training curriculum for this course.



For more information on certifications, visit http://www.cisco.com/go/certifications.

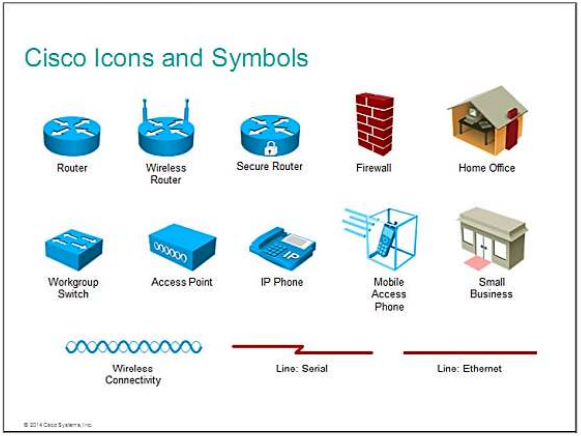
Note Cisco provides three levels of general certifications for IT professionals with several different tracks to meet individual needs. Cisco also provides focused certifications for designated areas such as cable communications and security. There are many paths to Cisco certification, but only one requirement—passing one or more exams demonstrating knowledge and skill. For details, go to www.cisco.com/go/certifications.



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

Additional References

This topic presents the Cisco icons and symbols that are used in this course, as well as information on where to find additional technical references.



Cisco Glossary of Terms

For additional information on Cisco terminology, refer to the Cisco Internetworking Terms and Acronyms glossary of terms at http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_(ITA).

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

Module 1

Cisco ASA (CX) NGFW Services

Introduction

This module describes how to implement Cisco ASA (CX) NGFW services. Cisco ASA (CX) NGFW software or hardware modules provide context-aware security functionality on the Cisco ASA adaptive security appliance platform. Context-awareness implies knowledge and control that are based on application (what), location (where), user-device type (how), and user identity (who).

Upon completing this module, you will be able to meet these objectives:

- Describe the Cisco ASA (CX) NGFW solution
- Describe the Cisco ASA (CX) NGFW management architecture and protocols
- Describe how to configure Cisco ASA (CX) NGFW policy objects
- Explain how to monitor Cisco ASA (CX) NGFW operations by using Cisco PRSM
- Describe how to configure Cisco ASA (CX) NGFW access policies to match security requirements
- Describe how to configure Cisco ASA (CX) NGFW identity policies to match security requirements
- Describe how to configure Cisco ASA (CX) NGFW decryption policies to match security requirements

https://t.me/learningnets

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

Lesson 1

Describing the Cisco ASA (CX) NGFW Services

Overview

This lesson provides an overview of Cisco Adaptive Security Appliances Context Aware Next Generation Firewall. The key Cisco ASA (CX) NGFW functions include the ability to perform user identification through active or passive authentication, broad AVC, web AVC, URL filtering, and TLS/SSL decryption.

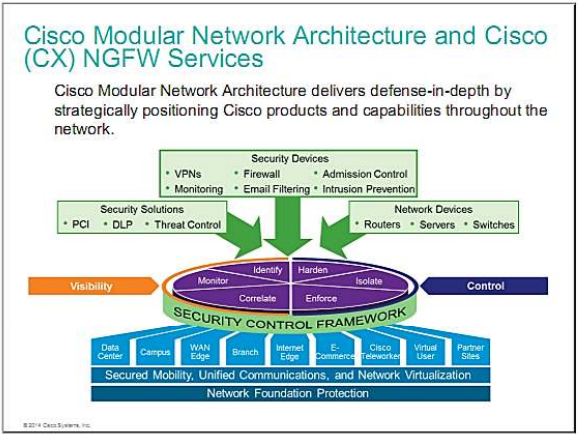
Upon completing this lesson, you will be able to meet these objectives:

- Describe where the Cisco ASA (CX) NGFW fits in the overall network topology
- List the components and explain the benefits of the Cisco ASA (CX) NGFW solution
- Describe how Cisco ASA (CX) NGFW broad and web AVC operate
- Describe the three Cisco ASA (CX) NGFW policy types
- List the Cisco ASA features that are compatible with Cisco ASA (CX) NGFW
- Identify the physical features of the Cisco ASA CX-SSP hardware module
- List the minimum Cisco ASA 5550-X image and SSD requirements to support the Cisco ASA CX software module

https://t.me/learningnets

Cisco Modular Network Architecture and Cisco (CX) NGFW Services

This topic identifies how to place Cisco Adaptive Security Appliances Context Aware Next Generation Firewall into a typical modularized network design.



Cisco Modular Network Architecture delivers defense-in-depth by strategically positioning Cisco products and capabilities throughout the network and by using the collaborative capabilities between the platforms. A wide range of security technologies are deployed in multiple layers, under a common strategy and administration. Products and capabilities are positioned where they deliver the most value, while facilitating collaboration and operations. Figure below illustrates the Cisco Modular Network Architecture.

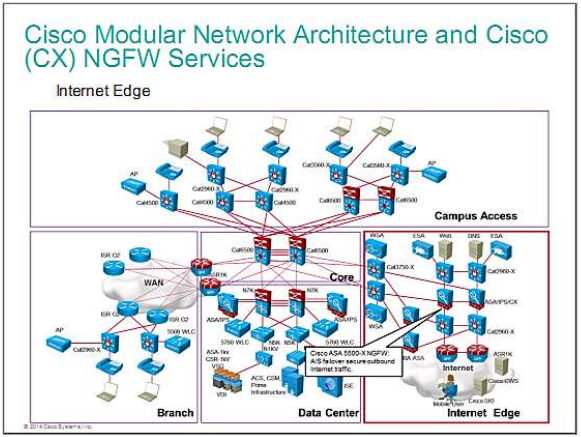
Cisco Modular Network Architecture is delivered in the form of design blueprints and security solutions:

Design blueprints—Cisco validated designs and security best practice guides. Prescriptive design guidance is provided in CVDs which cover the various places in the network (PINs) present in an enterprise network, such as campus, WAN edge, branches, and data center. Design guidance is also provided for technologies such as unified communications, network virtualization, and network foundation protection, which are present in multiple places in the network. The selection of platforms and capabilities within those designs, is driven by the application of the Cisco Security Control Framework.

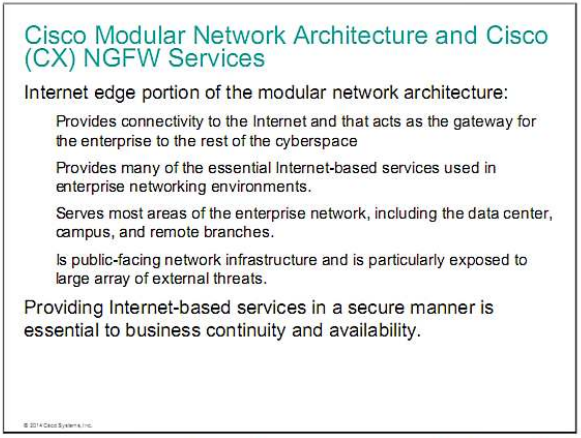
Security solutions—The Cisco SCF and the design blueprints provide the foundation for industry security solutions which address the requirements of specific industries such as retail, financial, healthcare, and manufacturing.

As illustrated in figure above, Cisco security services are embedded as an intrinsic part of the architecture. The Cisco security services support the solution lifecycle and the security products included in the designs.

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



The figure illustrates where in the Cisco modular network architecture architecture CIsco NGFW should be deployed. Ideally, the Cisco NGFW should be implemented on all Cisco ASA devices in the interned edge portion of the Cisco modular network architecture.



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 serves other building blocks that are present in a typical enterprise network. This modular building-block approach enables flexibility and customization in network design to meet the needs of customers and business models of differing sizes and requirements.

The Internet edge infrastructure serves most areas of the enterprise network, including the data center, campus, and remote branches. The proper design and implementation of the Internet edge infrastructure is crucial to ensure the availability of Internet services to all enterprise users. The Internet edge module provides many of the essential Internet-based services used in enterprise networking environments. Providing these services in a secure manner is essential to business continuity and availability.

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

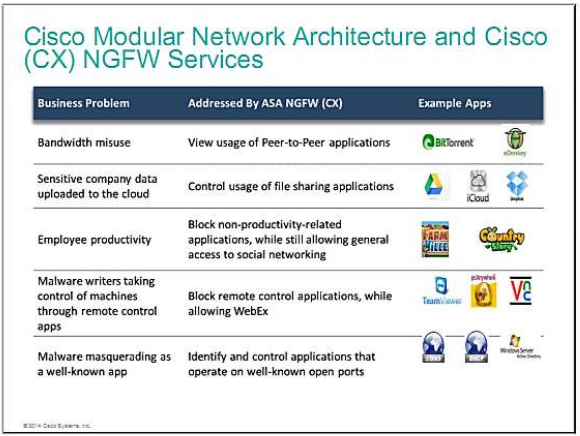
Network intrusion, takeover, and unauthorized network access

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 figure list some of the typical business challenges an enterprise may be facing today and how Cisco ASA Next-Generation Firewall Services can help address these challenges.

Cisco ASA (CX) NGFW Services empower enterprises to finally say yes to applications, devices, and the evolving global workforce. Most next-generation firewalls differ from classic firewalls in that they can identify which applications are being requested and which user has requested them. Application and user awareness can be effective, but with so much more happening in the network, these firewalls simply cannot provide the level of visibility and control that administrators need to help them effectively manage their complex network security challenges. Cisco ASA (CX) NGFW are different. Cisco ASA (CX) NGFW Services provide the application and user ID awareness that is essential for any next-generation firewall.

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

The majority of the application signatures that are currently supported by Cisco ASA (CX) NGFW Services are focused on protecting Internet activity. In addition, Cisco ASA (CX) NGFW Services bundle powerful URL filtering, NG intrusion prevention (in 9.2.1+ release), and reputation-based filtering that are most useful at the network edge. Future releases will include signatures and capabilities that will be more useful in data center deployments. For high availability support, Cisco ASA (CX) NGFW Services currently supports Active/Standby Failover.

Cisco ASA (CX) NGFW Services use threat intelligence feeds from Cisco Security Intelligence Operations, which employ the global footprint of Cisco security deployments (more than 2 million devices) to analyze 70 percent of the world's Internet traffic from email, IPS activity, and web threat vectors. The feeds are updated every three to five minutes for near-real-time protection from zero-day threat.

Cisco ASA (CX) NGFW Services enable organizations to continue to use their existing firewall rules and objects while adding richer, context-aware rules that can act intelligently on contextual information. Cisco ASA (CX) NGFW Services support Layer 3 and Layer 4 stateful firewall features, including access control, network address translation, and stateful inspection. Organizations can keep their existing stateful inspection firewall policies while adding rich Layer 7 context-aware rules.

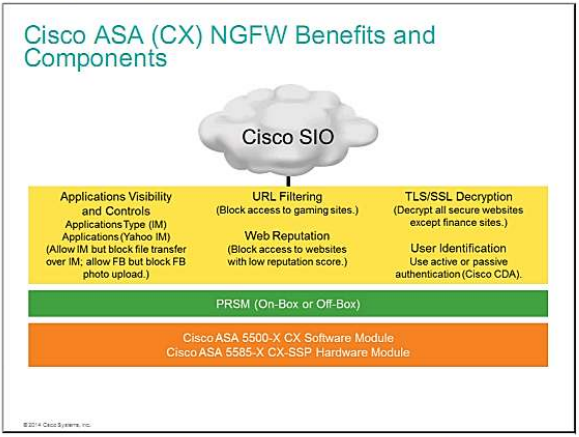
The Cisco ASA (CX) NGFW Services deliver:

- Precise application visibility and control, including behavior controls within allowed microapplications
- Reputation-based web security
- Passive and active user authentication
- TLS decryption
- User device information
- Near-real-time threat protection

https://t.me/learningnets

Cisco ASA (CX) NGFW Benefits and Components

This topic lists the components and explains the benefits of the Cisco Adaptive Security Appliances Context Aware Next Generation Firewall solution.



To mitigate current threats, Cisco ASA needs to be made context-aware. That is, Cisco ASA needs to extract the user and application identity, origin of access, and type of device that is used for access. Cisco ASA then needs to permit or deny access based on these attributes, in accordance with configured policy. In addition, Cisco ASA must have the ability to detect and protect against emerging threats. Cisco ASA (CX) NGFW provides these capabilities. Context-aware devices such as Cisco ASA (CX) NGFW enable you to enforce security according to the complete context of a situation.

A complete context includes this information:

Who: The identity of the user

What: The application or website that the user is trying to access, as well as its reputation

Where: Where the user is located at the time of the access attempt, local versus VPN access (using the Cisco AnyConnect VPN client), the source IP address, and so on

How: The device used for access (iPad, Windows, Android, and so on), if the traffic is web-based and using a browser, Cisco ASA (CX) NGFW uses the browser user agent information to determine the device type, or if the source device uses the Cisco AnyConnect VPN client to establish a VPN connection

Currently, you cannot create a time-based Cisco ASA (CX) NGFW policy.

You can extract the full context of a flow and enforce granular policies by using the Cisco ASA (CX) NGFW AVC, URL filtering, and web reputation features. For example, Cisco ASA (CX) NGFW can be configured to permit access to Yahoo IM but deny any file transfer over Yahoo IM, to allow access to Facebook but block Facebook photo uploads, to block access to all gaming obscenities, or to block access to all websites that have a low reputation score.

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

Cisco ASA (CX) NGFW can also define user- or user-group-based policies by interacting with Active Directory or LDAP directories. Cisco ASA (CX) NGFW can actively map the user IP address to the user identity or passively map the user IP address to the user identity by using Cisco Context Directory Agent.

Cisco Prime Security Manager is the management tool that you use to configure and manage Cisco ASA policies and operations. The on-box PRSM is a single, free device manager that comes with Cisco ASA (CX) NGFW. The off-box PRSM is a multidevice manager that can manage multiple Cisco ASA (CX) NGFW devices, and requires a license that is based on the number of Cisco ASA (CX) NGFW devices to be managed.

Cisco ASA (CX) NGFW is an SSP hardware module on the Cisco ASA 5585-X Adaptive Security Appliance with Cisco ASA Software Release 8.4.4 and later. Cisco ASA (CX) NGFW is also available as a software module on Cisco ASA 5500-X Series Next-Generation Firewalls with Cisco ASA Software Release 9.1.1 and later.

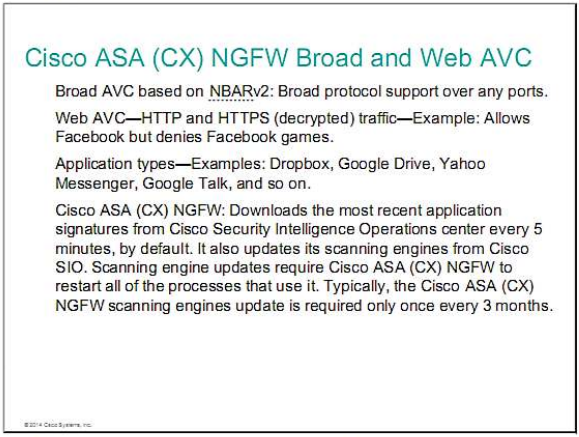
Cisco ASA (CX) NGFW and Cisco PRSM receive signatures and engine updates from Cisco Security Intelligence Operations at frequent intervals.

Note Next Generation IPS filtering, including automatic signature updates, global settings, dasbhoards, events, and reporting is now available in the Cisco ASA (CX) NGFW 9.1.3 and release. This course was written based on the Cisco ASA (CX) NGFW 9.1.2 release, for more information about the Next Generation IPS filtering feature, please refer to the latest Cisco ASA NGFW documentations on Cisco Connection Online.

https://t.me/learningnets

Cisco ASA (CX) NGFW Broad and Web AVC

This topic describes how Cisco Adaptive Security Appliances Context Aware Next Generation Firewall broad and web AVC operate.



Cisco ASA (CX) NGFW can support both web and nonweb applications.

Cisco ASA (CX) NGFW provides AVC for more than a 1000 applications and 75,000 microapplications.

For example, Facebook Chat and Facebook Games are two microapplications of the Facebook application.

Application recognition is based on signatures, heuristics, and content scanning, removing the need to tie applications to specific ports.

Cisco ASA (CX) NGFW can identify traffic even when that traffic uses nonstandard ports. For example, if HTTP is running on port 8080 or SSH is running on port 16022, Cisco ASA (CX) NGFW still identifies the traffic correctly as HTTP or SSH. Some applications, such as Skype, use port hopping and other evasive techniques. Cisco ASA (CX) NGFW can recognize such evasive applications.

The Cisco ASA (CX) NGFW AVC engines use NBARv2 application signatures for broad AVC operations. Web AVC offers fine granular HTTP (and decrypted HTTPS) inspection and control.

Cisco ASA (CX) NGFW also supports the matching of applications according to application types. For example, the File Sharing application type includes file-sharing applications such as Dropbox, Google Drive, and so on.

Cisco ASA (CX) NGFW downloads the most recent application signatures, microapplication signatures, application types, URL categories, and web reputation information from the Cisco SIO center every 5 minutes, by default.

Cisco ASA (CX) NGFW also updates its scanning engines from Cisco SIO. Scanning engine updates require Cisco ASA (CX) NGFW to restart all the processes that use it. You can set a time range to determine when the scanning update can occur; for example, check for scanning engine update only between 2 a.m. (0200) to 4 a.m. (0400). Typically, the Cisco ASA (CX) NGFW scanning engines update are required only once every three months or so.

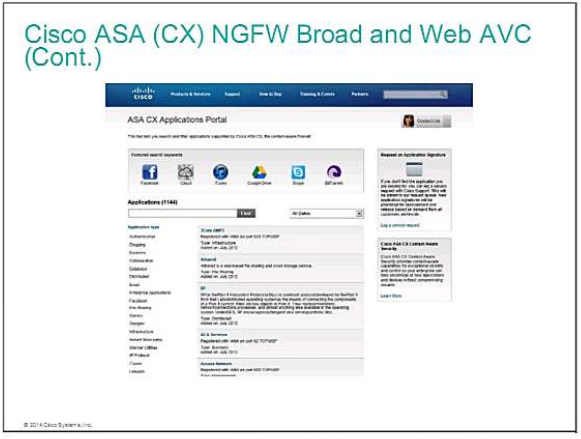
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Using the AVC engines, you can define access policies to block or allow applications by application type or by specific application. You can also apply deep controls to particular application types:

Allow access to Facebook only from the Marketing staff, and block access to all gaming microapplications.

Allow Yahoo IM traffic but disallow file sharing over Yahoo IM.

Allow SMTP over TCP port 25 and deny all other SMTP traffic over other ports.



You can view the Cisco ASA (CX) NGFW supported applications and application types by using Cisco Prime Security Manager or the Cisco ASA (CX) NGFW application portal.

From the Cisco PRSM GUI, on the **Policies > Applications** page, the administrator can see all the applications and microapplications that Cisco ASA (CX) NGFW supports. Cisco PRSM also supports quick-filtering capabilities that the administrator can use to search for a particular application.

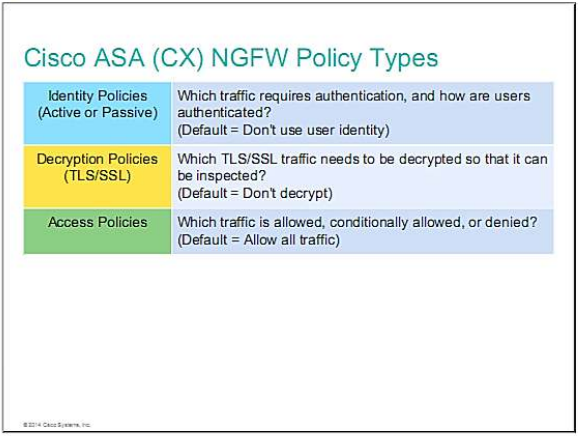
The figure shows the Cisco ASA (CX) NGFW application portal, at http://asacx-cisco.com/. This portal is a public website that lets you view the Cisco ASA (CX) NGFW supported application types and applications, as well as their details. You can view the most recent list of supported application types and applications, view application descriptions and behaviors, search and filter the applications, view the applications that were added in the past one, two, or three months, or learn about the an application by clicking the featured search keywords.

If you do not find an application that you are looking for, you can log a service request with Cisco Support. This request is added to the request queue. New application signatures are prioritized for development and release based on demand from customers worldwide.

Note The http://asacx-cisco.com/ website is now been renamed to ASA NGFW Services Applications Portal. In the Cisco ASA (CX) NGFW 9.1.3 release, the term Cisco ASA CX has been rebranded to Cisco ASA NGFW.

Cisco ASA (CX) NGFW Policy Types

This topic describes the three Cisco Adaptive Security Appliances Context Aware Next Generation Firewall policy types.



Cisco ASA (CX) NGFW uses three types of policies to provide identity and authentication, decryption, and access control:

Cisco ASA (CX) NGFW identity policies determine whether a user must be authenticated and, if so, which method is used to authenticate the user. The purpose of authentication is to determine which user is involved in a traffic flow so that identity-based access or decryption policies can be applied to those traffic flows. The default is not to require user identity (user authentication).

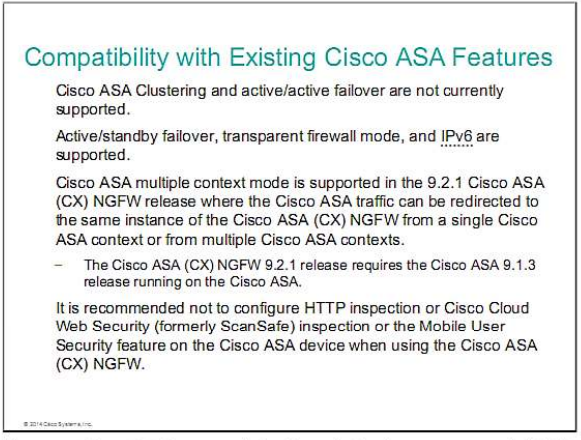
Cisco ASA (CX) NGFW decryption policies determine which TLS/SSL traffic flows need to be decrypted. Decrypting TLS/SSL traffic flows makes it possible to apply access policies that are based on the decrypted content of the HTTPS traffic flow. The default is not to decrypt any TLS/SSL traffic.

Cisco ASA (CX) NGFW access policies control access to the network. The access policies can allow traffic, deny traffic, or conditionally allow traffic. The default is to allow all traffic.

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

Cisco ASA (CX) NGFW Compatibility with Existing Cisco ASA Features

This topic lists the Cisco Adaptive Security Appliances features that are compatible with Cisco ASA Context Aware Next Generation Firewall.



The figure lists some Cisco ASA features and describes whether they are supported with Cisco ASA (CX) NGFW.

Refer to the most recent Cisco ASA configuration guide for the most recent feature-compatibility information.

To take full advantage of the Cisco ASA (CX) NGFW module features, use these guidelines:

The typical use case for Cisco ASA (CX) NGFW is to be deployed at the Internet Edge to protect the outbound traffic.

It is recommended not to configure Cisco ASA inspection on HTTP traffic. Application inspections on the Cisco ASA device take precedence over inspections in Cisco ASA (CX) NGFW. If HTTP inspection is enabled on the Cisco ASA device, then the Cisco ASA HTTP inspector inspects the traffic first. The traffic can then be directed to Cisco ASA (CX) NGFW. Customers who purchase Cisco ASA (CX) NGFW typically use HTTP inspection on Cisco ASA (CX) NGFW, so you should disable HTTP inspection on Cisco ASA if it is enabled. By default, HTTP inspection is not enabled on Cisco ASA.

Do not configure Cisco Cloud Web Security (formerly ScanSafe) inspection. If both Cisco ASA (CX) NGFW and Cloud Web Security inspection are configured for the same traffic flow, the Cisco ASA performs only the Cisco ASA (CX) NGFW action.

The Mobile User Security feature provides an "always-on" SSL VPN connection from a mobile user to the Cisco ASA device, which then directs the traffic to one or more web security appliances for content filtering. Do not enable the Mobile User Security server feature, which is incompatible with the Cisco ASA (CX) NGFW module.

Cisco ASA Clustering and active/active failover are not supported as of the Cisco ASA 9.1.2 release.

https://t.me/learningnets

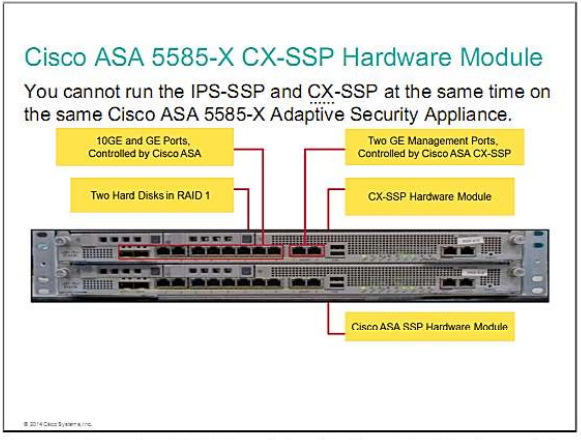
Cisco ASA multiple context mode support for Cisco ASA (CX) NGFW is available in the 9.2.1 release where the Cisco ASA traffic can be redirected to the same instance of the Cisco ASA (CX) NGFW from a single Cisco ASA context or from multiple Cisco ASA contexts. The Cisco ASA (CX) NGFW 9.2.1 release requires the Cisco ASA 9.1.3 release running on the Cisco ASA. Active/Active failover is not supported in the Cisco ASA (CX) NGFW 9.2.1 release.

Active/Standby failover is supported. When the active Cisco ASA device fails, any existing Cisco ASA (CX) NGFW flows are transferred to the new active Cisco ASA device. Traffic is allowed through the new active Cisco ASA device, without being acted on by the new active Cisco ASA (CX) NGFW module. Only new flows that the new active Cisco ASA device receives are acted on by the new active Cisco ASA (CX) NGFW module. Both the active and standby Cisco ASA (CX) NGFW need individual licenses. Licenses are not shared between the active and standby Cisco ASA (CX) NGFW. The Cisco ASA (CX) NGFW configuration is not synced from the active to the standby Cisco ASA (CX) NGFW. The configuration of the active and standby Cisco ASA (CX) NGFW should be configured to be the same.

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

Cisco ASA 5585-X NGFW CX-SSP Hardware Module

This topic identifies the various physical features of the Cisco Adaptive Security Appliances Context Aware-SSP hardware module.



The figure shows the Cisco ASA CX-SSP (top slot) and the Cisco ASA-SSP (bottom slot) on the Cisco ASA 5585-X chassis. Although the Cisco ASA 5585-X CX-SSP includes Gigabit Ethernet network interfaces, these interfaces are controlled by and logically belong to the Cisco ASA-SSP. The Cisco ASA CX-SSP does not directly process traffic that goes through these interfaces. Cisco ASA CX-SSP directly manages only the console port and the two management interfaces.

As of the 9.1.2 release, Cisco ASA (CX) NGFW is supported only on the Cisco ASA 5585-X SSP-10 and SSP-20 modules. In the 9.2.1 release, the Cisco ASA (CX) NGFW support has been extended to the Cisco ASA 5585-X SSP-40 and SSP-60 modules.

Cisco ASA 5500-X (CX) NGFW Software Module

This topic lists the minimum Cisco Adaptive Security Appliance 5500-X ASA image and SSD requirements to support the Cisco ASA Context Aware Next Generation Firewall software module.



The figure shows the Cisco ASA 5500-X Series Next-Generation Firewall platforms that support the Cisco ASA (CX) NGFW software module. The Cisco ASA (CX) NGFW software module for the Cisco ASA 5500-X Series is supported in Cisco ASA Software Release 9.1.1 and later. To support Cisco ASA (CX) NGFW on the Cisco ASA 5500-X Series, the Cisco ASA 5500-X Series appliances require the SSDs that are listed in the figure.

The Cisco ASA 5500-X appliance can run either the (CX) NGFW or the IPS software module, but not both simultaneously.

Cisco ASA (CX) NGFW is currently the only process that uses the SSD for storage.

The SSD is hot-swappable. The SSD resides in a carrier, which you install into the drive bay. You can use the SSD with an AC or DC Cisco ASA power supply.

When installing an SSD for the first time, you must reload Cisco ASA and then reimage Cisco ASA (CX) NGFW.

If the SSD fails in a single-drive model or if both SSDs fail simultaneously in a dual-drive model, you need to replace the SSDs. The Cisco ASA (CX) NGFW shuts down when this happens, so Cisco ASA (CX) NGFW features are unavailable during the SSD recovery process.

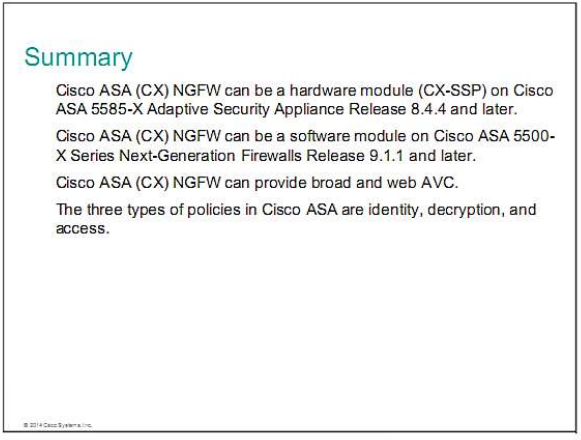
If a single SSD fails in a dual-drive model, you can hot-swap the failed SSD. Cisco ASA (CX) NGFW does not shut down and you do not need to reload Cisco ASA.

Note	Customers must use only those SSDs that are supplied by Cisco. Functionality and performance are tested only for the SSDs that Cisco supplies.

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

Summary

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



References

For additional information, refer to these resources:

Cisco Systems, Inc. *Cisco ASA Series Firewall ASDM Configuration Guide, 7.1*. http://www.cisco.com/en/US/docs/security/asa/asa91/asdm71/firewall/asdm_71_firewall_config.html.

Cisco Systems, Inc. *Cisco ASA Series Firewall CLI Configuration Guide, 9.1*. http://www.cisco.com/en/US/docs/security/asa/asa91/configuration/firewall/asa_91_firewall_config.html.

Cisco Systems, Inc. *User Guide for ASA CX and Cisco Prime Security Manager 9.1*. http://www.cisco.com/en/US/docs/security/asacx/9.1/user/guide/b_User_Guide_for_ASA_CX_and_PRSM_9_1.pdf.

https://t.me/learningnets

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

Lesson 2

Describing the Cisco ASA (CX) NGFW Management Architecture

Overview

This lesson describes the Cisco Adaptive Security Appliances Context Aware Next Generation Firewall management architecture. The Cisco Prime Security Manager is used to configure and monitor all the Cisco ASA (CX) NGFW policies and operations. This lesson describe the basic Cisco PRSM GUI functions and Cisco ASA (CX) NGFW CLI operations and explains the caveats of the Cisco (CX) NGFW management interface. The lesson also explains the Cisco (CX) NGFW and Cisco PRSM licensing requirements.

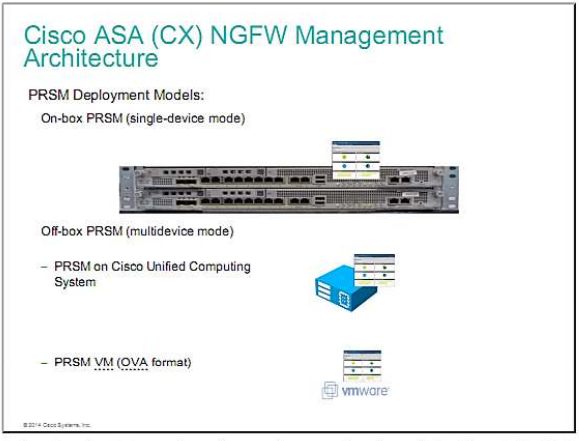
Upon completing this lesson, you will be able to meet these objectives:

- Explain the Cisco ASA (CX) NGFW management architecture and protocols
- Compare the on-box Cisco PRSM (single-device mode) and the off-box Cisco PRSM (multidevice mode)
- Explain the PRSM GUI operations
- Explain the caveats of the Cisco ASA (CX) NGFW software module management interface
- Explain the Cisco ASA (CX) NGFW CLI operations
- Explain the Cisco ASA (CX) NGFW licensing requirements
- Explain the Cisco Off-Box PRSM licensing requirements
- Explain how to install and maintain the Cisco ASA (CX) NGFW and off-box Cisco PRSM licenses

https://t.me/learningnets

Cisco ASA (CX) NGFW Management Architecture

This topic illustrates the Cisco Adaptive Security Appliances Context Aware Next Generation Firewall management architecture and protocols.



The Cisco Prime Security Manager is used to configure and monitor all the Cisco ASA (CX) NGFW policies and operations. The Cisco PRSM GUI is based on Web 2.0, using HTML5.

The on-box Cisco PRSM is a single-device manager for managing a single Cisco ASA (CX) NGFW device. Cisco ASA (CX) NGFW comes preloaded with an on-box, single-device management version of Cisco PRSM.

The off-box Cisco PRSM is a multidevice manager for managing as many as 25 Cisco ASA (CX) NGFW devices. The off-box Cisco PRSM is available either as a physical appliance or as a VMware ESXi-based virtual appliance. In either case, the off-box Cisco PRSM licensing is based on the number of Cisco ASA (CX) NGFW devices that are to be managed.

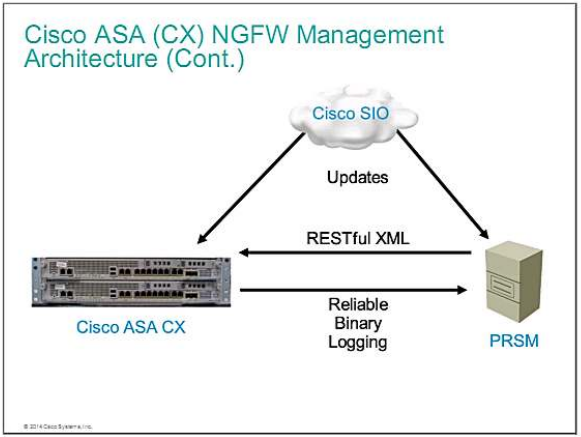
The off-box Cisco PRSM comes in two form factors:

VM: Provided as an OVA file, the VM form factor supports only VMware vSphere 4.1 and later. Refer to the PRSM Installation Guide for the VM CPU, memory, and disk requirements.

Cisco UCS: Cisco PRSM is available as a Cisco UCS C-Series M3 appliance bundle with ESXi 4.1 and a VM.

The off-box Cisco PRSM supports the ability to share policy across multiple Cisco ASA (CX) NGFW devices. This version of Cisco PRSM supports device groups, which are groups that consist of a Cisco ASA device and its installed Cisco ASA (CX) NGFW instance, which can share common Cisco ASA (CX) NGFW policies.

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



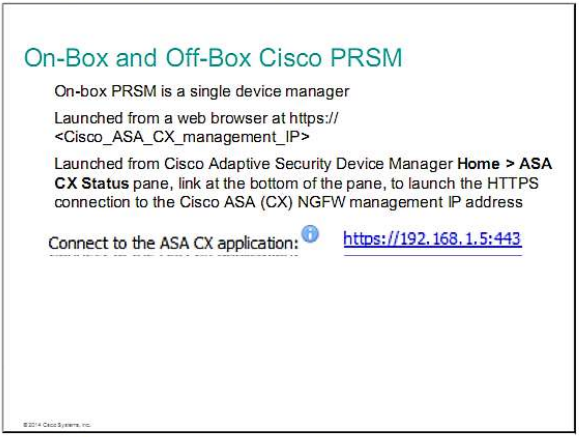
The figure shows the Cisco ASA (CX) NGFW management architecture. Cisco PRSM uses the RESTful XML API over HTTPS to communicate with Cisco ASA (CX) NGFW. The HTTP server must be enabled on the Cisco ASA device, and the IP address of the Cisco PRSM must be allowed to connect to the Cisco ASA HTTP server.

All Cisco ASA (CX) NGFW policy configurations can be performed only by using the Cisco PRSM web-based GUI interface. Currently, Cisco PRSM can also be used to configure the syslog settings of the Cisco ASA device that contains Cisco ASA (CX) NGFW. In the future, more Cisco ASA configurations may be managed by using Cisco PRSM but currently, Cisco Security Manager is the multidevice manager for multiple Cisco ASA devices.

Cisco ASA and Cisco ASA (CX) NGFW send event information to Cisco PRSM by using the Cisco proprietary Reliable Binary Logging format. The number of events that can be stored in Cisco PRSM is based on the hardware on which Cisco PRSM is deployed. Cisco PRSM does not support the forwarding of event and reporting data to an external SIEM tool as of Cisco ASA Software Release 9.1.1 or 9.1.2.

On-Box and Off-Box Cisco PRSM

This topic compares the on-box Cisco Prime Security Manager for single-device mode and the off-box PRSM for multidevice mode. This course will focus on using the on-box PRSM.

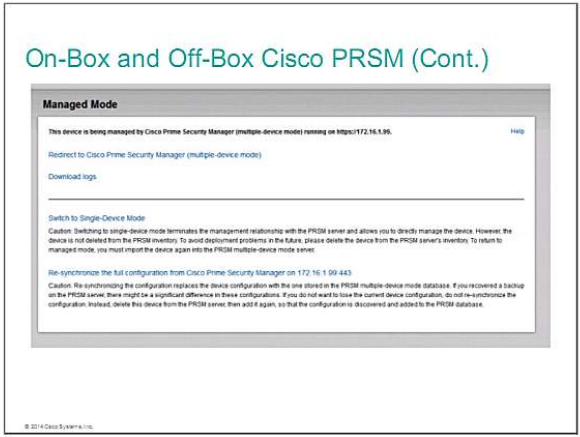


The on-box Cisco PRSM can be launched from a web browser or from within Cisco Adaptive Security Device Manager. From Cisco ASDM, go to the **Home > ASA CX Status** pane. Information and status for Cisco ASA (CX) NGFW can be seen and a link at the bottom of the pane can be used to launch the HTTPS connection to the Cisco ASA (CX) NGFW management IP address. The on-box Cisco PRSM does not require any licensing; it is free and prebundled with Cisco ASA (CX) NGFW.

The off-box Cisco PRSM (multidevice mode) and on-box Cisco PRSM (single-device mode) interfaces look similar. The differences relate to the availability of features that relate to managing multiple devices, such as the device inventory. The device inventory is the list of Cisco ASA and Cisco ASA (CX) NGFW devices that the off-box Cisco PRSM is managing.

Note Supported browsers include Google Chrome 17, Mozilla Firefox 11, and Windows Internet Explorer 8 with Google Chrome Frame.

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



Cisco ASA (CX) NGFW knows which primary management tool is used to manage it. When a customer starts using the off-box Cisco PRSM to manage Cisco ASA (CX) NGFW, direct administration access to the on-box Cisco PRSM web interface notifies the administrator that the multidevice version is the correct management tool to use.

Under emergency scenarios only, such as when the multidevice off-box Cisco PRSM is unavailable for whatever reason, the administrator can manually reset to the on-box Cisco PRSM, by choosing the **Switch to Single-Device Mode** option. The administrator can then make the necessary changes by using the on-box (single-device mode) Cisco PRSM.

Note Switching to single-device mode terminates the management relationship with the off-box Cisco PRSM server and allows you to directly manage the device. However, the device is not deleted from the off-box Cisco PRSM inventory. To avoid deployment problems in the future, you need to delete the device from the off-box Cisco PRSM server inventory. To return the device to the managed (off-box, multidevice) mode, you must reimport the device into the off-box PRSM.

To change the Cisco ASA (CX) NGFW device to the unmanaged, on-box Cisco PRSM (single-device) mode:

Preferred method: Delete the device from the device inventory in the off-box Cisco PRSM. This action returns the Cisco ASA (CX) NGFW device to unmanaged mode.

Emergency method only: If the off-box Cisco PRSM is unavailable for any reason, you can open the web interface for the Cisco ASA (CX) NGFW device in single-device mode and click the link to unmanage the Cisco ASA (CX) NGFW device (**Switch to Single-Device Mode**). This action breaks the connection with the off-box Cisco PRSM and enables the local on-box Cisco PRSM web interface. However, the device is not automatically deleted from the off-box Cisco PRSM and must be deleted manually.

To return the Cisco ASA (CX) NGFW to be managed by the off-box Cisco PRSM in multidevice mode, reimport the Cisco ASA with the Cisco ASA (CX) NGFW back into the off-box Cisco PRSM.

https://t.me/learningnets

An OOB change is any change to the configuration of a managed Cisco ASA device that happens outside the control of the off-box Cisco PRSM. Cisco PRSM considers a change to be OOB only when the change is to a Cisco ASA feature or command that Cisco PRSM can configure. Changes are not considered OOB if they are made to unmanaged Cisco ASA features. Cisco PRSM does not recognize OOB changes.

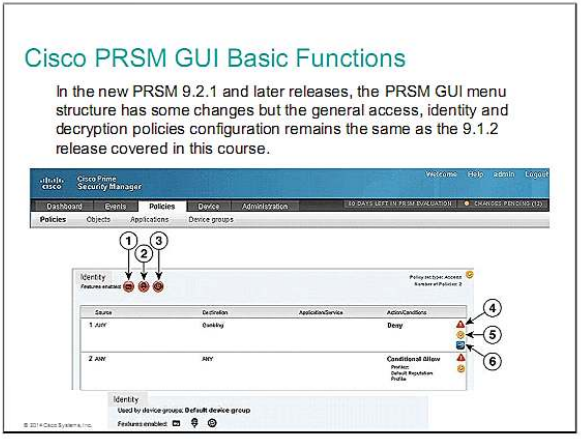
Currently, Cisco PRSM (as of the 9.1.2 release) can optionally be used to configure Cisco ASA syslog configurations.

As shown in the figure, from the 9.1.2 version of the on-box Cisco PRSM Managed Mode panel, you can click the link to redirect the user to the off-box Cisco PRSM, or download the log or resync the configurations from the off-box Cisco PRSM.

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

Cisco PRSM GUI Basic Functions

This topic describe the basic Cisco Prime Security Manager GUI functions.



The main difference between the on-box vs. the off-box PRSM GUI is the added ability in the off-box PRSM to manage multiple Cisco Adaptive Security Appliances and Cisco ASA Context Aware Next Generation Firewall devices. Traffic redirection can also be configured from the off-box Cisco PRSM or the Cisco ASA CLI or Cisco Adaptive Security Device Manager. Traffic redirection cannot be configured by using the on-box Cisco PRSM.

The figure shows the off-box Cisco PRSM main menu options (as of the 9.1.2 release) :

Dashboard: The Dashboard menu includes the primary landing page, the Network Overview, and links to each available dashboards. Use these features to monitor and evaluate the performance of your devices, policies, and so on.

Events: The Events menu includes the Event Viewer. Use the Event Viewer to view and analyze traffic and system events. These events can help you to identify and resolve problems with user access or system performance and behavior.

Policies: The Policies menu includes the core features for defining security policies. From this menu, you can create policies, policy objects, and device groups. You can also view the applications and microapplications that Cisco ASA (CX) NGFW can identify.

Device: The Device menu includes features that relate to device configuration. In Multiple Device (off-box Cisco PRSM) mode, this is also where you find the device inventory, add devices, and configure other device-specific features.

Administration: The Administration menu includes features that relate to managing the system, such as user account management, licensing, backup, and so on.

License Alerts: The space in the menu bar next to the Administration menu shows license alerts if any current or pending issues related to product licenses exist. The alerts indicate problems or potential problems. Click an alert to go to the Licenses page, where you can take action.

https://t.me/learningnets

Changes Pending/No Changes Pending: The link at the far right of the menu bar is always present and takes you to the Commit and Deploy Changes page. The text of the link indicates whether there are changes that are waiting for you to commit to the database and deploy to the device or devices. When you make changes to policies, you must commit the changes to make them take effect.

These items appear in the upper right:

Welcome: Use this link to open the Welcome page, which provides overview information and videos.

Help: Use this link to open online help.

Username: This label shows the name of the user who is logged in. This is not a link, but if you have more than one user account, it helps you to know which username you used to log in.

Logout: Use this link to log out of the web interface.

The figure also shows policy and alert icons. Icons 1, 2, and 3 show the licensed features that are available on the Cisco ASA (CX) NGFW device. Normally, the icons are black. A red background indicates a problem with the license that is required for the feature; hover over the icon to see a description of the problem. In the figure, the labeled icons represent this information:

1. AVC is enabled.
2. URL filtering is enabled.
3. Web reputation filtering is enabled.

The figure also shows these icons:

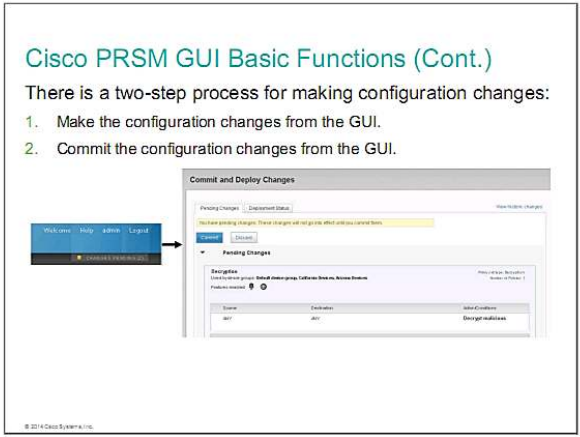
4. **Alert:** The red triangle is a general alert icon that indicates some type of problem. In policy configurations, this icon indicates a licensing problem. In the dashboards or Cisco PRSM device inventory, the icon indicates device problems, such as a device that is unreachable, and the specific alert also appears as text next to the icon. Hover over the icon to determine the reason for the alert.
5. **Pending Changes:** This icon indicates that this item has been modified. You must commit the changes before the edited version of the policy, object, or other setting becomes effective.
6. **Packet Capture:** This icon indicates that packet capture is turned on for this policy.

Built for intuitive usability, Cisco PRSM provides administrators with a consistent management interface for single-device and multidevice management. Cisco PRSM enables policies to be written and enforced, based on a rich set of contextual elements, including applications, microapplications, users, devices, and locations. The Cisco PRSM GUI is HTML5-based.

Commands that operate on the configuration items are revealed when you hover over the item in the GUI. In general, if you are not sure what to do on a page, start hovering over items to see the information that appears. As the lower part of the figure shows, hovering over the first identity policy shows several commands that relate to that policy, such as Delete Policy and Edit Policy.

Note In the new PRSM 9.2.1 and later releases, the PRSM GUI menu structure has some changes but the general access, identity and decryption policies configuration remains the same as in the 9.1.2 release covered in this course. The way the Cisco ASA and NGFW services (CX) devices are imported to the off-box PRSM and the way in which the policies are shared between devices have also been changed. Device groups are eliminated and policy sharing in the 9.2.1 release is based directly on individual devices. The importing of the Cisco ASA and NGFW services (CX) devices into the off-box PRSM will not be covered in this course. More Cisco ASA configurations like Interface, ACL and NAT can also be configured using the latest PRSM 9.2.1 or later versions.

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



The Cisco PRSM GUI uses a two-step configuration and commit process. When a policy or setting in the Cisco PRSM GUI is changed, the change is not immediately applied to the device. This two-step commit process gives you the opportunity to make a group of related changes without forcing you to run the device in a partially configured manner.

After you complete the changes that you want to make, use this procedure to commit them:

1. Click the **Changes Pending** link in the menu bar to open the Commit and Deploy Changes page. The Changes Pending link includes the number of pending changes. If there have been no changes since the last commit, this link is labeled No Pending Changes. You can still click the link to get to the Commit and Deploy Changes page; for example, if you want to check deployment status. You can also get to the page by clicking the Pending Change icon that is displayed on a changed item, such as a policy object or policy.
2. In the off-box Cisco PRSM, the Commit and Deploy Changes page is divided into two tabs: Pending Changes and Deployment Status. Click the **Pending Changes** tab to view the pending changes information. If there are no pending changes, this tab shows the message, "You have no pending changes." You can click the **Deployment Status** tab to view the configuration-deployment status. If no configurations are being deployed to the devices, this tab shows the message, "No Active Deployment Jobs found in database."
3. Evaluate the Pending Changes list to ensure that you want to apply your changes. All changes since your last commit are listed on the Pending Changes tab. The tab is not explicitly labeled in single-device (on-box Cisco PRSM) mode.
4. Click **Commit** to update the device configuration.

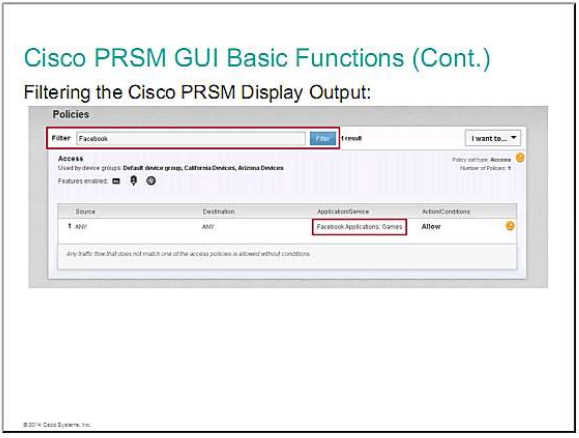
When you commit changes in on-box Cisco PRSM single-device mode, the changes are applied immediately. The Commit and Deploy Changes page is not divided into two tabs; rather, the Pending Changes tab is always active (and unnamed).

If you decide not to commit the changes, click **Discard**. All policies or settings that were configured since the last commit are erased. You cannot selectively undo or discard a single change among a group of changes.

https://t.me/learningnets

When you deploy changes to a device, the changes become part of the device configuration as soon as the device applies the changes. However, if a change involves how traffic transmitted through the device is processed, the change does not necessarily affect existing connections. Thus, if you make policy changes to deny certain types of traffic that were previously allowed, you might see some delay in the policy effectiveness. Only the connections that start after the policy changes have been committed are processed according to the new policy.

Refer to the Cisco PRSM User Guide for more information about using the off-box Cisco PRSM Deployment Manager to manage multidevice configuration deployments.



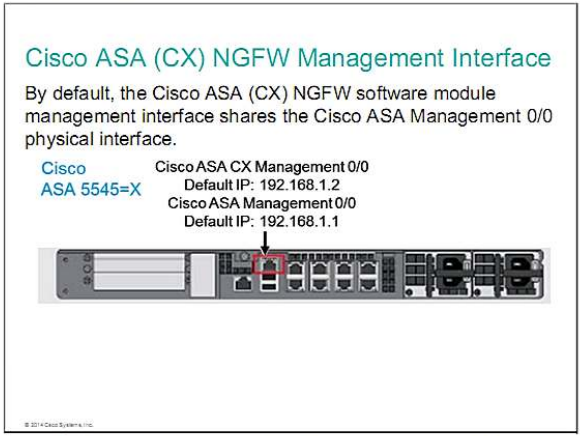
From the various pages in the Cisco PRSM GUI, the **Filter** option allows the displayed output to be filtered according to what is typed into the Filter field. The string that you enter in the Filter field is not case-sensitive.

In the example in the figure, from the Policies page, the term "Facebook" is applied as the filter. In this case, the resulting Policies page displays only the access policy that contains the term "Facebook." The remaining policies, which do not contain the term "Facebook," are not displayed.

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

Cisco ASA (CX) NGFW Management Interface

This topic explains the caveats of the Cisco Adaptive Security Appliances Context Aware Next Generation Firewall management interface.



On Cisco ASA 5500-X Series Next-Generation Firewall platforms, the default Cisco ASA (CX) NGFW management IP address shares the Management 0/0 interface of the Cisco ASA appliance. The default Management 0/0 IP address of the Cisco ASA appliance is 192.168.1.1 and the default Cisco ASA (CX) NGFW management IP address is 192.168.1.2 with a default gateway IP address of 192.168.1.1.

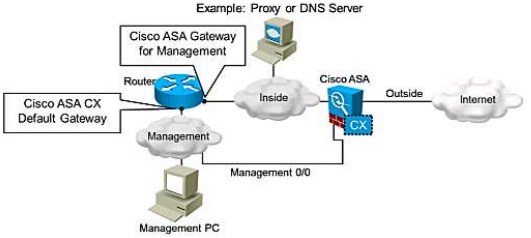
The Cisco ASA (CX) NGFW management interface shares the Management 0/0 interface with the Cisco ASA appliance. Separate MAC and IP addresses are supported for the Cisco ASA and Cisco ASA (CX) NGFW module. You must configure the Cisco ASA (CX) NGFW IP address within the Cisco ASA (CX) NGFW operating system. However, physical characteristics, such as enabling the management interface, are configured on Cisco ASA.

In addition to providing management access to the Cisco ASA (CX) NGFW module, the Cisco ASA (CX) NGFW management interface needs Internet access to receive updates from the Cisco Security Intelligence Operations center.

https://t.me/learningnets

Cisco ASA (CX) NGFW Management Interface (Cont.)

The Cisco ASA 5500-X Series management interface does not allow through-the-box traffic. An inside router is required to route traffic between the management network and the inside network for Internet access.

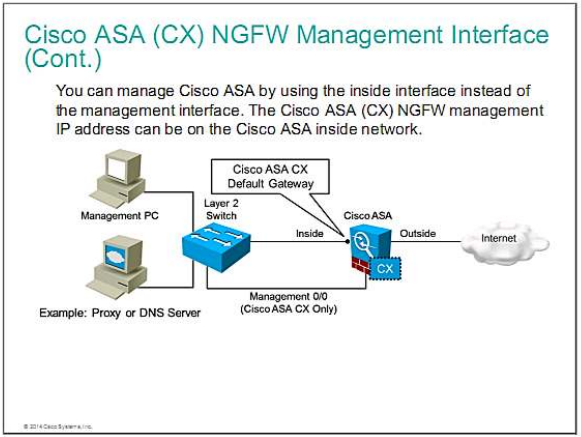


As of Cisco ASA Software Release 9.1.1 and 9.1.2, the Cisco ASA 5500-X Management 0/0 interface does not allow through-the-box traffic. For example, when Cisco ASA (CX) NGFW is using the Cisco ASA Management 0/0 interface as its default gateway, Cisco ASA (CX) NGFW outbound Internet traffic cannot be routed through the Cisco ASA Management 0/0 interface. Therefore, an inside router is required to route traffic between the management network and the inside network for Internet access, as the figure shows. Be sure to add a route on the Cisco ASA appliance, to reach the management network through the inside router.

This partial configuration example shows a Cisco ASA 5500-X appliance on which the inside router has one interface (192.168.1.254) in the inside network and another interface (192.168.2.254) in the management network. In this example, the Cisco ASA (CX) NGFW management IP is in the 192.168.2.0/24 management network (192.168.2.2) with the 192.168.2.254 default gateway:

```
interface GigabitEthernet0/1
 nameif inside
 ip address 192.168.1.1 255.255.255.0
 <output omitted>
interface Management0/0
 nameif management
 ip address 192.168.2.1 255.255.255.0
 <output omitted>
 route inside 192.168.2.0 255.255.255.0 192.168.1.254
```

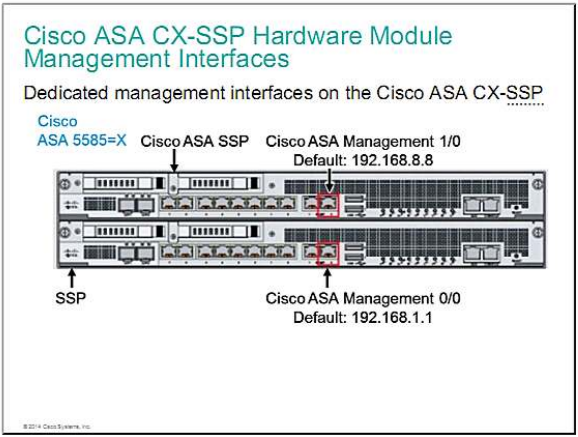

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



If there is no separate management network, as the figure shows, you can manage Cisco ASA from the inside interface instead of the Management 0/0 interface. You must remove the Cisco ASA configured name for the Cisco ASA Management 0/0 interface (using the **no nameif management** command). If the name is configured on Cisco ASA, then the Cisco ASA (CX) NGFW management IP address must be on the same Management 0/0 network as Cisco ASA, and that excludes any networks that are already configured on other Cisco ASA interfaces. If the name is not configured, then the Cisco ASA (CX) NGFW management IP address can be on any network; for example, the Cisco ASA inside network. In this case, the Cisco ASA Management 0/0 interface must connect to the inside network, and there is no internal switching between the Management 0/0 interface and any other interfaces on the Cisco ASA appliance.

This partial configuration example, on a Cisco ASA 5500-X appliance, shows the Cisco ASA (CX) NGFW management IP in the 192.168.1.0 network with the 192.168.1.1 default gateway:

```
interface GigabitEthernet0/1
 nameif inside
 ip address 192.168.1.1 255.255.255.0
 <output omitted>
interface Management0/0
 no nameif
 management-only
 <output omitted>
```

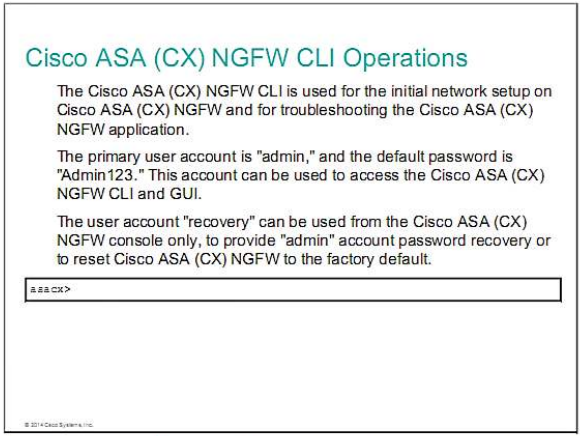


On the Cisco ASA 5585-X Adaptive Security Appliance, Cisco ASA CX-SSP has dedicated management interfaces. The default Management 0/0 IP address of the Cisco ASA is 192.168.1.1, and the default Cisco ASA CX Management 1/0 IP address is 192.168.8.8 with a default gateway IP address of 192.168.8.1.

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

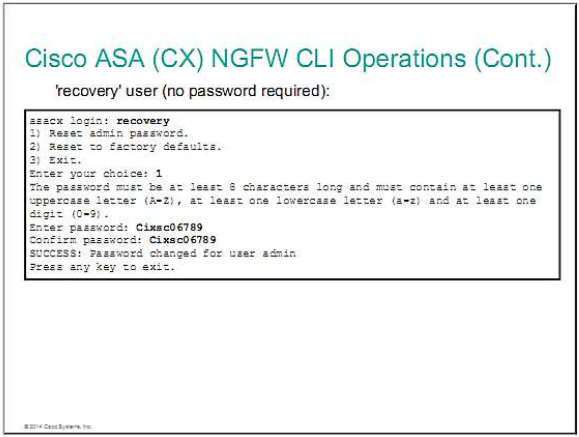
Cisco ASA (CX) NGFW CLI Operations

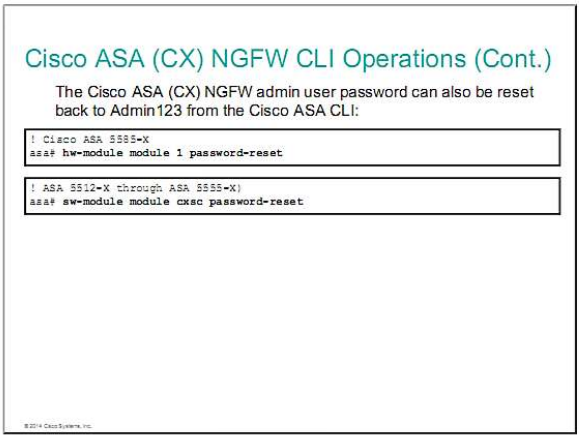
This topic explains the Cisco Adaptive Security Appliances Context Aware Next Generation Firewall CLI operations.



The Cisco ASA (CX) NGFW CLI is used for the initial network setup on Cisco ASA (CX) NGFW and for troubleshooting the Cisco ASA (CX) NGFW. The Cisco ASA (CX) NGFW CLI is not used for configuring the various Cisco ASA (CX) NGFW identity, decryption, and access policies.

Two default user accounts exist on Cisco ASA (CX) NGFW: admin and recovery. The admin user account, which has a default password of Admin123, can be used for SSH or console session access. The recovery user account has no password and is used only on a console session. The recovery user account is used to recover the admin user account password or to reset Cisco ASA (CX) NGFW to the factory defaults.





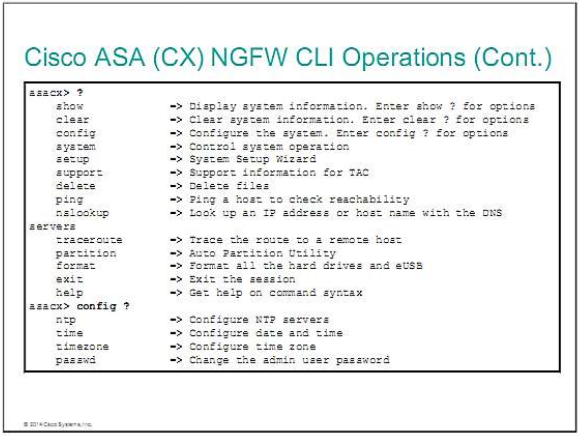
The figure shows the process of logging in to the Cisco ASA (CX) NGFW console by using the recovery user account. After you log in as the recovery user, two available options are to reset the admin user account password or to reset Cisco ASA (CX) NGFW configurations to the factory default configurations, which also resets the admin user account password to the default password Admin123.

The Cisco ASA (CX) NGFW admin user password can also be reset back to Admin123 from the Cisco ASA CLI using the following commands:

```
! Cisco ASA 5585-X
asa# hw-module module 1 password-reset
```

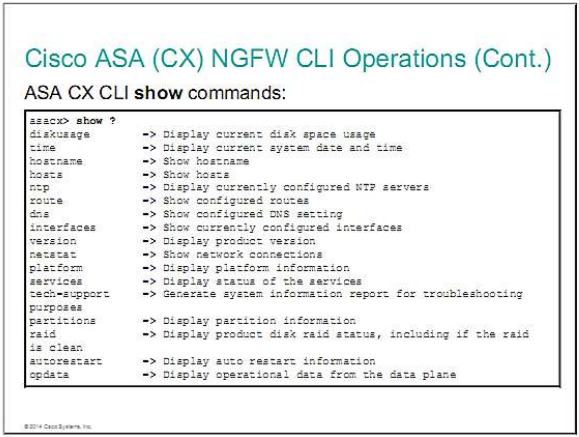

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

```
! ASA 5512-X through ASA 5555-X)
asa# sw-module module cxsc password-reset
```



Similar to the IOS CLI, from the Cisco ASA (CX) NGFW CLI, enter **?** to display the available commands or command options. The Cisco ASA (CX) NGFW CLI does not have a privileged user mode or any configuration modes; for example, to configure services such as NTP, use the **config ntp** command or use the **config passwd** command to change the admin user account password.

```
asacx> config ntp
Do you want to enable the NTP service? [N]: y
Enter the NTP servers separated by commas [192.168.1.1]: 172.16.1.1
asacx> config passwd
The password must be at least 8 characters long and must contain
at least one uppercase letter (A-Z), at least one lowercase letter
(a-z) and at least one digit (0-9).
Enter password: Admin123
Confirm password: Admin123
SUCCESS: Password changed for user admin
```



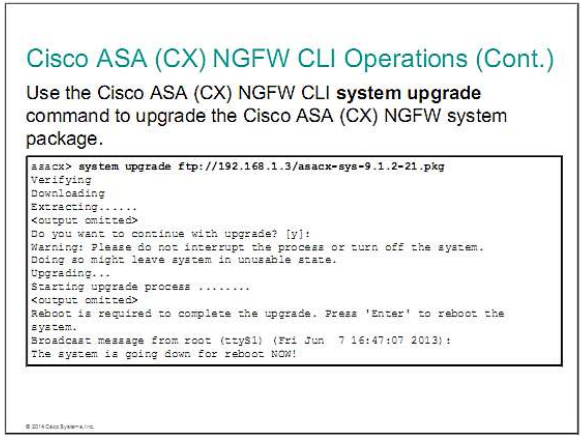
The figure lists the **show** commands that are available in the Cisco ASA (CX) NGFW CLI; for example, the **show opdata** command, which is similar in functionality to the **show asp** command on Cisco ASA.

```
asacx> show opdata ?
    summary          => Display summary data from the data plane
    interface        => Display interface data from the data plane
    connections      => Display connections data from the data plane
    policy           => Display policy data from the data plane
    framedrop        => Display frame drop from the data plane
    flowdrop         => Display flow drop from the data plane
    arptable         => Display ARP table from the data plane
    routingtable     => Display routing table from the data plane
    blocks           => Display blocks usage data from the data plane
    adisessions      => Display ADI session directory
```

Use the **show diskusage** command to verify disk usages.

```
asacx> show diskusage
FILESYSTEM                      SIZE      AVAILABLE          USE%
/                               1.2G          372.8M           67%
/boot                         288.6M          194.1M           29%
/var                            7.9G            7.3G            2%
/var/data                      74.8G           64.6G            9%
/var/packages                   7.9G            6.9G            8%
/var/config                   311.4M          285.1M            3%
/var/db                         3.9G            3.6G            4%
/var/log                        3.0G            2.6G            6%
/var/local                      3.0G            2.7G            2%
/var/data/diagnostics           5.9G            5.5G            2%
/var/data/cores                 5.9G            5.5G            2%
```


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



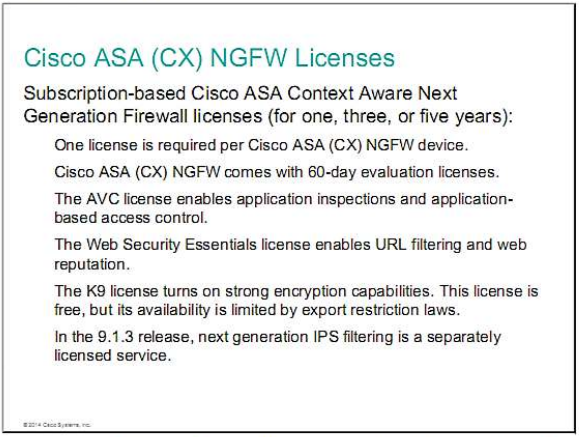
From the Cisco ASA (CX) NGFW CLI, use the **system upgrade** command to upgrade the Cisco ASA (CX) NGFW system package.

```
asacx> system upgrade ftp://192.168.1.3/asacx-sys-9.1.2-21.pkg
Verifying
Downloading
Extracting.....
Package Detail
        Description:                   Cisco ASA-CX 9.1.2-21 System Upgrade
        Requires reboot:              Yes
NOTE: If this device is being managed by a PRSM server, you must also apply the same
upgrade package to the PRSM server or you will not be able to deploy configurations
from the PRSM server to this device.
Do you want to continue with upgrade? [y]:
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.
Upgrading...
Starting upgrade process ........
Populating new system image.....
Copying over new application components
Cleaning up old application components.....
Reboot is required to complete the upgrade. Press 'Enter' to reboot the system.
Broadcast message from root (ttyS1) (Fri Jun  7 16:47:07 2013):
The system is going down for reboot NOW!
```

Refer to the Command Reference for ASA CX and Cisco Prime Security Manager for more detailed information about the CLI commands and commands options.

Cisco ASA (CX) NGFW Licenses

This topic compares the AVC, Web Security Essential, and K9 licensing requirements and lists the restrictions of the free evaluation license.



Cisco Adaptive Security Appliances (CX) NGFW features and the off-box Cisco Prime Security Manager (in multidevice mode) use separate licenses. Cisco PRSM is used to manage the feature licenses that are used on Cisco ASA (CX) NGFW devices. Cisco ASA (CX) NGFW licensing is subscription-based, so each purchased license expires at a fixed time. Currently, the available durations are one, three, or five years.

Many Cisco ASA (CX) NGFW features are available without special licensing. However, you must install these licenses to obtain the services that each license cover:

AVC license: This subscription-based license allows the use of application-based access control. Specifically, you need this license if you want to create access policies that are based on applications or application types, including application or application services policy objects.

Web Security Essentials license: This subscription-based license allows the use of URL filtering and web-reputation-based policies. Specifically, you need this license if you want to use URL objects or web reputation profiles in policies.

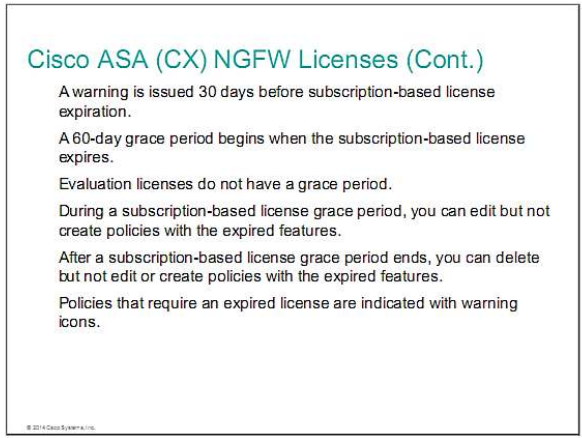
K9 license: The K9 license determines the relative strength of the encryption algorithms that are used in the product. The license is tied directly to the hardware (by serial number) and is a permanent license that does not require renewal. The license is free, but its availability is limited by export restriction laws, so it is not available for all users. Consult www.cisco.com to determine whether you can download the K9 license.

Next generation IPS filtering: In the 9.1.3 release, next generation IPS filtering is a separately licensed service.

Currently, each Cisco ASA (CX) NGFW device requires its own licenses.

Each Cisco ASA (CX) NGFW device includes evaluation licenses which are valid for 60 days. You can renew the evaluation licenses one time, to extend the period an additional 60 days and get a total 120-day evaluation period. Evaluation licenses do not have a grace period.

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



The subscription licenses that Cisco ASA (CX) NGFW uses have expiration dates. You must ensure that you have the valid, unexpired licenses for the features that you use. When a license is 30 days from its expiration date, you will be warned about the pending expiration. There is a 60-day grace period after expiration, to give you some time to upload new licenses. A link in the menu bar, next to the Pending Changes link, shows the number of expired licenses.

Evaluation licenses do not have a grace period.

These points provide more detail about subscription license expiration:

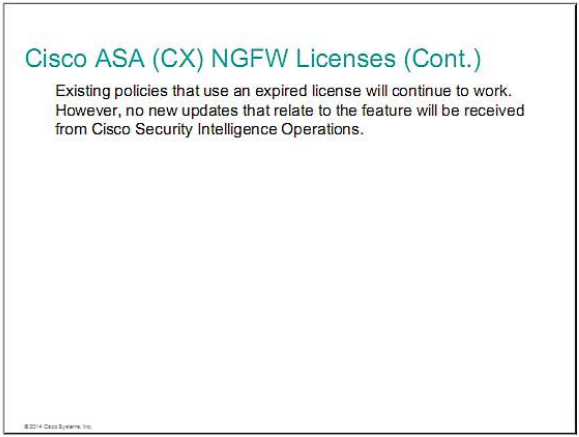
Policy sets include icons for each feature that is enabled for the set. Hover over the icons to see the feature names and the number of days left on the license or whether the license is past its expiration date.

In the off-box Cisco PRSM (multiple-device mode), the license expiration dates are derived from the devices in the device groups that use the policy set. If more than one device group uses a policy set, then the expiration date is the shortest-life license that is assigned to the devices in the various device groups. License-expiration processing is controlled by the device with the shortest-life license, not the longest-life license.

If the license has expired but is still within the grace period, then you can edit but not create policies that use the license.

If the license has expired and is beyond the grace period, you cannot edit any policy that uses a feature controlled that the license controls, and you cannot create a policy that uses that feature. For example, if the AVC license expires, you cannot edit any access policy that specifies an application, application type, application object, or application service object. However, you can delete these policies.

https://t.me/learningnets

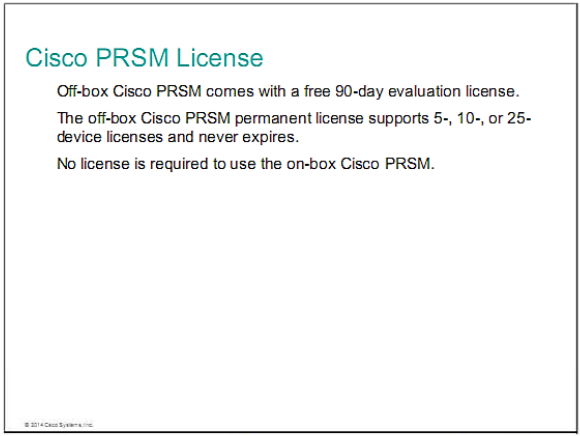


Policies that require an expired license are indicated with warning icons. Existing policies that use an expired license continue to work. However, no new updates that relate to the feature will be received from Cisco SIO. For example, if the Web Security Essentials license expires, then Cisco ASA (CX) NGFW and Cisco PRSM stop downloading URL category updates from Cisco SIO. Cisco PRSM generated reports also stop showing data that is based on the expired feature, starting at the time the grace period ends.

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

Cisco Off-Box PRSM License

This topic describes the off-box Cisco Prime Security Manager license requirements, which are based on the number of devices to be managed, and lists the restrictions of the free evaluation license.



The off-box (multidevice mode) Cisco PRSM requires a permanent license that is based on the number of Cisco Adaptive Security Appliances Context Aware devices to be managed (5, 10, or 25 devices). The off-box Cisco PRSM licenses are stackable; for example, a customer that originally purchased a 10-device license can later add a 5-device license to support management of 15 devices. If there are more Cisco ASA CX devices being managed in the off-box Cisco PRSM than the license allows, Cisco PRSM displays a warning message to recommend a new license. Cisco PRSM does not disable any feature.

The off-box Cisco PRSM includes a 90-day unlimited device-count evaluation license, which you can renew once by obtaining and uploading a new evaluation license, for a total 180-day evaluation period. The remaining period that is available in the evaluation license is shown in the menu bar, next to the Pending Changes link.

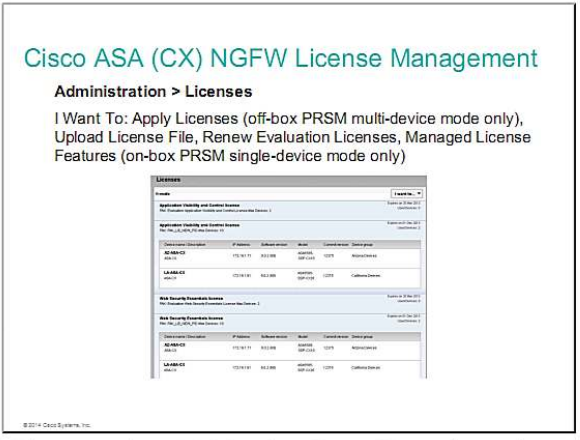
If the evaluation license expires, you can no longer deploy changes to devices.

The on-box (single-device, unmanaged mode) Cisco PRSM is included for free with the Cisco ASA CX software package and does not require a license.

https://t.me/learningnets

Cisco ASA (CX) NGFW and Off-Box Cisco PRSM License Management

This topic describes how to install and maintain the Cisco Adaptive Security Appliances Context Aware Next Generation Firewall and off-box Cisco Prime Security Manager licenses.



To open the Licenses page, choose **Administration > Licenses**. You can also open the page by clicking a license notification link in the menu bar, next to the Pending Changes link. You will see this notification if you are using an evaluation license or if a license has expired.

The figure shows the off-box PRSM Adminstration > License page.

From the **I Want To** drop-down list, choose one of these options:

Apply Licenses: For multidevice mode only, choose this option to apply unused licenses to devices that need licenses.

Upload License File: Choose this option to add a license file. You can upload multiple licenses at the same time. In single device mode, uploading a license automatically applies the license to the device if the new license has a more remote expiration date than the currently used license.

Renew Evaluation Licenses: Use this option to renew all evaluation licenses. You can renew evaluation licenses once before purchasing new licenses. This command is unavailable if you have already renewed licenses or are in single-device mode and have already uploaded the feature licenses.

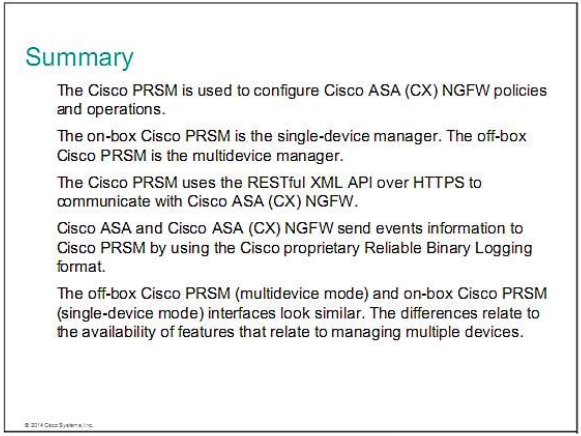
Manage Licensed Features: When in single-device mode only, use this option to selectively enable or disable licensed features. If you decide that you do not want to use a particular feature that requires a subscription license, you can disable the feature so that you cannot inadvertently define policies that require it.

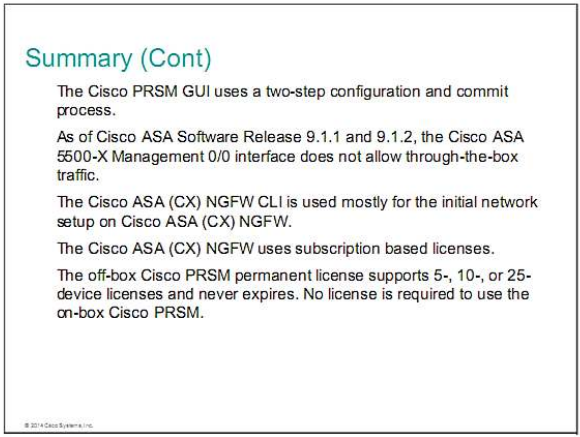
Refer to the User Guide for ASA CX and PRSM for more information about using Cisco PRSM to manage the licenses.

© 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

References

For additional information, refer to these resources:

Cisco Systems, Inc. *Cisco ASA Series Firewall CLI Configuration Guide, 9.x.* http://www.cisco.com/en/US/docs/security/asa/asa91/configuration/firewall/asa_91_firewall_config.html

Cisco Systems, Inc. *Cisco ASA Series Firewall ADSM Configuration Guide, 7.x.* http://www.cisco.com/en/US/docs/security/asa/asa91/asdm71/firewall/asdm_71_firewall_config.html

Cisco Systems, Inc. *User Guide for Cisco ASA (CX) NGFW and Cisco Prime Security Manager 9.x.* http://www.cisco.com/en/US/docs/security/asacx/9.1/user/guide/b_User_Guide_for_ASA_CX_and_PRSM_9_1.pdf

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

Lesson 3

Configuring Cisco ASA (CX) NGFW Policy Objects

Overview

This lesson describes how to configure the Cisco Adaptive Security Appliances Context Aware Next Generation Firewall policy objects. Cisco ASA (CX) NGFW policies reference policy objects. Policy objects are reusable containers that define criteria that you want to use when defining the access, identity, or decryption policies. Some policy objects are predefined in Cisco ASA (CX) NGFW, and other policy objects are user-defined.

Upon completing this lesson, you will be able to meet these objectives:

- Redirect traffic from Cisco ASA to Cisco ASA (CX) NGFW to enforce context-aware policies on the traffic
- Explain Cisco ASA (CX) NGFW policy structure
- Explain how policy objects are used within the Cisco ASA (CX) NGFW policy for traffic matching
- Describe how to configure Cisco ASA CX network groups
- Describe how to configure Cisco ASA CX service objects and service groups
- Describe how to configure Cisco ASA CX application objects and application service objects
- Describe how to configure Cisco ASA CX URL objects
- Describe how to configure Cisco ASA CX user agent objects
- Describe how to configure Cisco ASA CX identity objects
- Describe how to configure Cisco ASA CX source object groups and destination object groups
- Describe how to configure Cisco ASA CX secure mobility objects
- Describe how to configure Cisco ASA CX action profile objects
- Identify where each policy object can be used in Cisco ASA (CX) NGFW policy configurations

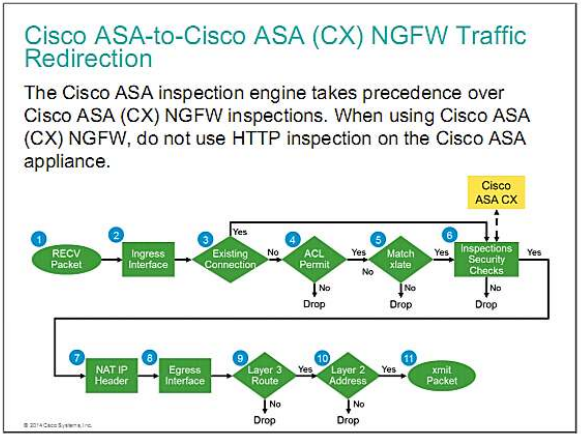
https://t.me/learningnets

Explain the use of tagging, ticket IDs, and metadata

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

Cisco ASA-to-Cisco ASA (CX) NGFW Traffic Redirection

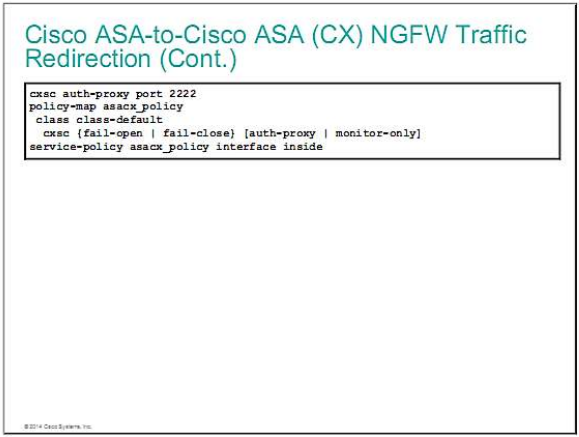
This topic describes how to redirect traffic from the Cisco Adaptive Security Appliances to the Cisco ASA Context Aware Next Generation Firewall to enforce context-aware policies on the traffic.



The figure shows the Cisco ASA packet-processing flow. Traffic is redirected from Cisco ASA to Cisco ASA (CX) NGFW during the Inspections Sec Checks step, by using the MPF configurations on the Cisco ASA.

Application inspections on Cisco ASA take precedence over inspections in Cisco ASA (CX) NGFW. If HTTP inspection is enabled on Cisco ASA, then the Cisco ASA HTTP inspector inspects traffic first. Traffic can still be directed to Cisco ASA (CX) NGFW. For such traffic, Cisco ASA (CX) NGFW skips HTTP inspection (performing no URL filtering, web reputation, or web AVC). Because customers who purchase Cisco ASA (CX) NGFW typically use HTTP inspection on Cisco ASA (CX) NGFW, you should disable HTTP inspection on Cisco ASA (if it is enabled). By default, HTTP inspection is not enabled on Cisco ASA.

https://t.me/learningnets



All traffic initially enters Cisco ASA, which applies the interface and global access rules to the traffic. Any traffic that passes these access rules can be redirected from Cisco ASA to Cisco ASA (CX) NGFW, which then applies its policies to the traffic. Cisco ASA (CX) NGFW sends allowed traffic back to Cisco ASA, which sends the traffic to its ultimate destination.

The off-box Cisco Prime Security Manager multidevice manager can also be used to redirect all traffic or traffic that is based on ports and Cisco ASA interfaces. For more granular traffic-redirection options, use the Cisco ASA MPF configurations from the Cisco ASA CLI or Cisco Adaptive Security Device Manager.

To redirect traffic from Cisco ASA to Cisco ASA (CX) NGFW by using the ASA CLI, use the **exsc {fail-open| fail-close} [auth-proxy]** command:

The **fail-open** command specifies that if Cisco ASA (CX) NGFW fails for any reason, Cisco ASA will continue to pass traffic that would otherwise be redirected to Cisco ASA (CX) NGFW.

The **fail-close** command specifies that if Cisco ASA (CX) NGFW fails, Cisco ASA will drop all traffic that would otherwise be redirected to Cisco ASA (CX) NGFW.

The **auth-proxy** command enables the authentication proxy, which is required if you want to use active authentication in the identity policies on Cisco ASA (CX) NGFW. If you do not include this keyword, you can perform passive authentication only. If you enabled the authentication proxy and want to use a nondefault port for active authentication, then configure the authentication proxy port by using the **exsc auth-proxy port** global configuration command. The default authentication proxy TCP port is 885. If users must be prompted for authentication credentials using active authentication, then they are prompted through this port.

The Cisco ASA (CX) NGFW redirection policy can be applied to the interface or globally on the Cisco ASA appliance.

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

Note

In Cisco ASA Software Release CX 9.1.2, the new **monitor-only** option allows Cisco ASA to send a copy of the packets that it would send to Cisco ASA (CX) NGFW, for monitoring purposes, while still forwarding the actual packets to endpoints. In this mode, Cisco ASA continues to remain as an inline device, forwarding packet between endpoints; Cisco ASA (CX) NGFW is not inline and only receives a copy of the packets for events and reporting purposes. Monitor-only redirection needs to be configured on both Cisco ASA and Cisco ASA (CX) NGFW for this mode to work.

If Cisco ASA is configured for **monitor-only** mode but Cisco ASA (CX) NGFW is not, then Cisco ASA (CX) NGFW drops the packets. These packet drops can be viewed by using the **show opdata framedrop** Cisco ASA (CX) NGFW CLI command. The new **monitor-mode** option in the **cxsc fail-open monitor-only** command is used to enable monitor mode on Cisco ASA.

Monitor-only mode on the Cisco ASA (CX) NGFW is configured from the **Device > Monitor-only mode** on-box PRSM screen. Monitor-only mode is supported only for the on-box PRSM and is not support in the off-box PRSM. If an ASA or CX is configured to be in monitor-only mode then device import to the off-box PRSM of such ASA and CX will fail.

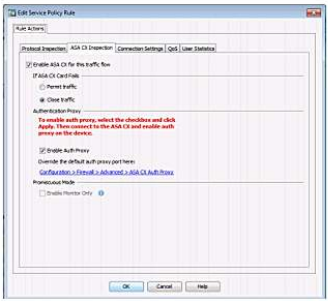
Mixing of the monitor-only and regular inline mode is not supported. Monitor-only mode is typically used for demonstration purposes.

When you configure the **monitor-only** option, you see a warning message similar to this one:

WARNING: Monitor-only mode should be used for demonstrations and evaluations only. This mode prevents CXSC from denying or altering traffic.

Cisco ASA-to-Cisco ASA (CX) NGFW Traffic Redirection (Cont.)

Cisco ASDM Add **Service Policy Rule Wizard > Rule Actions > Cisco ASA CX** Inspection tab

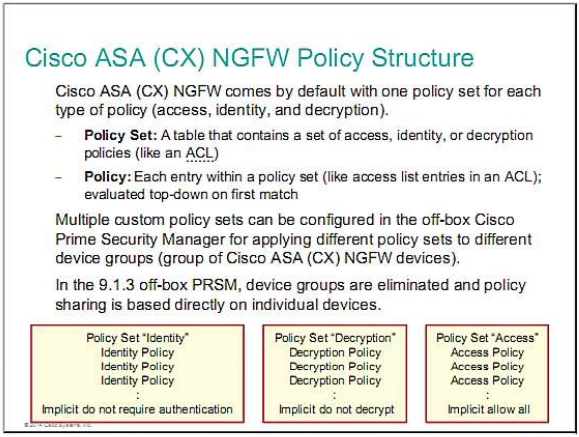


The figure shows the Cisco ASA CX Inspection tab of the Cisco ASDM Add Service Policy Rule Wizard Rule Actions page, from which you can enable traffic redirection.

Optionally, use the **Configuration > Firewall > Advanced > ASA CX Auth Proxy** page to change the default auth proxy port. The auth proxy port is used when using active authentication in the identity policies on the Cisco ASA CX.

Cisco ASA (CX) NGFW Policy Structure

This topic explains the Cisco Adaptive Security Appliances Context Aware Next Generation Firewall policy structure.



The Cisco ASA (CX) NGFW access, decryption, and identity policies are grouped into policy sets.

A policy set is an ordered list of a certain type of policy. There is a minimum of one policy set for each policy type. Policies are evaluated top-down on a first-match basis. Incoming traffic is compared to the match criteria for each policy in a policy set, from top to bottom, and the first policy whose traffic matching criteria is satisfied defines the security policy that is applied to the traffic. Thus, the policy order within a policy set is crucial. You can think of a policy set like an ACL, and the policies within a policy set like the individual access list entries within an ACL.

Cisco ASA (CX) NGFW comes by default with one policy set for each type of policy (access, decryption, and identity). Custom policy sets can be created only in the off-box Cisco PRSM multidevice mode.

When you configure a Cisco ASA (CX) NGFW device in on-box Cisco PRSM single-device mode, the policy sets are predefined. In the default policy sets, the default actions are to implicitly allow all traffic, implicitly do not decrypt any traffic, and implicitly do not require any user to be authenticated.

The Cisco ASA (CX) NGFW policy sets and policies can be configured only from the Cisco PRSM web GUI, not from the Cisco PRSM CLI.

Policies define the security characteristics and requirements of the network, such as rules for who can access the network, which applications users can use, which websites users can visit, and so on. Policies implement the network security policies for the organization. Depending on whether you need to manage multiple Cisco ASA (CX) NGFW devices or only one Cisco ASA (CX) NGFW device, policies can be shared among many devices or can be local to a device.

Note In the 9.1.3 off-box PRSM, device groups are eliminated and policy sharing is based directly on individual devices. Please refer to the latest PRSM documentations on Cisco Connection Online for more information on 9.1.3 off-box PRSM operations.

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

Cisco ASA (CX) NGFW Policy Structure (Cont.)

Policies > Policies

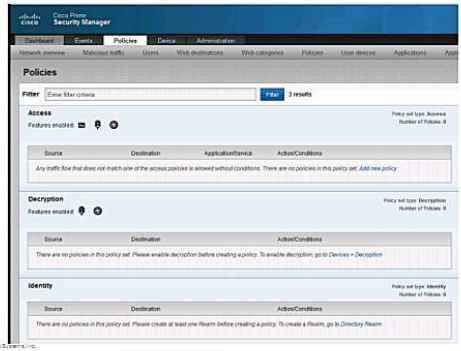
The default implicit access policy states that any traffic flow that does not match an access policy is allowed without conditions.

Recommended to always create a catch-all access policy at the bottom to set a default catch-all access policy.

By default, none of the traffic is decrypted and users are not required to be authenticated by Cisco ASA (CX) NGFW.

© 2014 Cisco Systems, Inc.

Cisco ASA (CX) NGFW Policy Structure (Cont.)



© 2014 Cisco Systems, Inc.

The three types of Cisco ASA (CX) NGFW policies are access, decryption, and identity.

Identity policies determine whether a user must be authenticated and how the user should be authenticated. The purpose of authentication is to determine the user who is involved in a traffic flow so that identity-based access or decryption policies can be applied to traffic flows.

Decryption policies determine which TLS/SSL traffic needs to be decrypted. Decrypting TLS/SSL traffic flows makes it possible to apply access policies that are based on the inspected content of the traffic flow, such as application, URL category, web reputation, and so on.

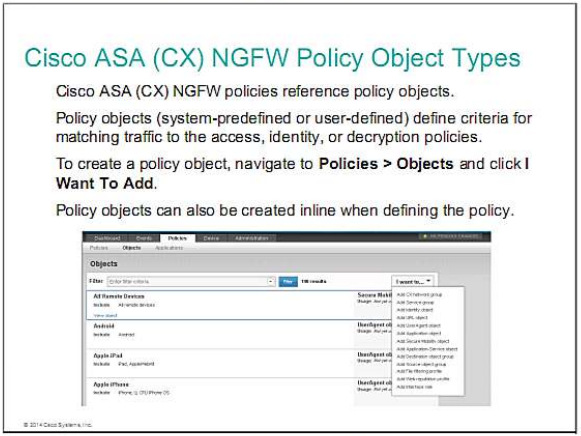
Access policies control user access to the network for implementing acceptable use policies.

It is important to note that the default implicit access policy states that any traffic flow that does not match an access policy is allowed without conditions. It is recommended to always create a catch-all access policy at the bottom of the access policy set.

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

Cisco ASA (CX) NGFW Policy Object Types

This topic describes how the policy objects are used within the Cisco Adaptive Security Appliances Context Aware Next Generation Firewall policy for traffic matching.



Cisco ASA (CX) NGFW policies reference policy objects. Policy objects define criteria for matching traffic to the access, identity, or decryption policies. Policy objects are reusable containers that define criteria that you want to use when defining access, identity, or decryption policies. Some policy objects are predefined in Cisco ASA (CX) NGFW and other policy objects are user-defined.

During the off-box The Cisco Prime Security Manager device-import process, some policy objects can also be learned from the Cisco ASA configurations. Any changes that are made to the policy objects that are imported from the Cisco ASA device are not deployed back to Cisco ASA. Rather, these changes affect the use of the objects for Cisco ASA (CX) NGFW policies only.

Cisco ASA (CX) NGFW policy objects are used in a way similar to how Cisco ASA object groups are used in Cisco ASA access list configurations.

To open the Policy Objects screen, where you can create, edit, delete, and view objects, choose **Policies > Objects** from the Cisco PRSM menu options.

This list offers a brief description of each object type:

ASA CX network group: IP addresses to identify hosts and networks; can be used only on Cisco ASA (CX) NGFW devices

Service group: Protocol and port definitions, such as TCP/80 for TCP traffic on port 80

Identity object: User identity, including usernames and user group names

URL objects: Web domains or servers (such as example.com, www.example.com), web URL resources (HTTP or HTTPS only, such as http://example.com/games), and web (URL) categories

User agent objects: Types of agents that are used to make HTTP requests, as identified in the user agent field in HTTP packet headers; for example, browser types (Internet Explorer, Firefox, and so on) or device types (iPhone, and so on)

Application objects: Applications or application types, which can be identified regardless of the port that is used during any particular connection session

Secure mobility objects: Used to identify the types of clients that are used to make remote-access VPN connections, as reported by the Cisco AnyConnect Secure Mobility application; used to tailor policies, based on the device that is used to access the network through a remote-access VPN connection

Application service: Defines an application, based on a combination of service-group objects (traditional protocol and port specifications), application names, application types, or application objects; can be used in combination with other application services in OR statements to define specific traffic patterns

Destination object group: Defines a potentially complex destination traffic-match criterion by using the objects that are allowed in the destination field of a policy; can include network group and URL objects in AND statements, so that all objects must be satisfied for traffic to match the policy; can be used in combination with other application services in OR statements to define specific traffic patterns

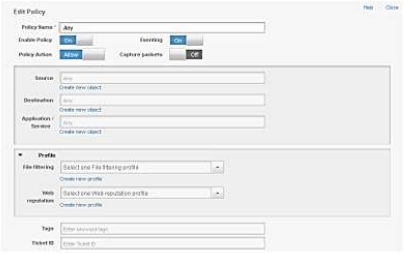
Source object group: Defines a potentially complex source traffic-match criterion by using the objects that are allowed in the source field of a policy; can include network group, identity, user agent, and Secure Mobility objects in AND statements, so that all objects must be satisfied for traffic to match the policy; can be used in combination with other application services in OR statements to define specific traffic patterns

File filtering profile: An action profile that controls the types of files that users are allowed to upload or download; applies only to HTTP traffic

Web reputation profile: An action profile that controls which parts of an otherwise allowed web page can be returned to the user, based on the reputation of the web site; applies only to HTTP traffic

Cisco ASA (CX) NGFW Policy Object Types (Cont.)

During policy editing or creation, you can use the links under the the Source, Destination, Application/Service, and Profile fields to create a new object inline.



You can create policy objects inline when configuring the access, identity, or decryption policies. When editing or creating a policy, under each configuration field is a link to Create New Object, which allows you to quickly create a new object inline from the policy screen.

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

Cisco ASA (CX) NGFW Policy Object Types (Cont.)

Hover over the policy object to see more detailed information about the object.

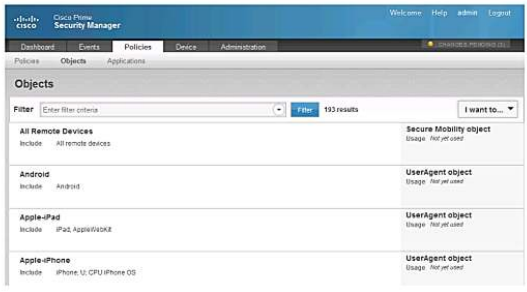


By hovering over a policy object, such as the Windows7-Workstation user agent object group that the figure shows, you can see more detailed information about the policy object.

This example shows the system predefined user agent object, Windows7-Workstation, which matches the Windows NT 6.1 User Agent. User agent objects are used to identify the type of browser, device, or operating system that is used to make HTTP requests, as identified in the user agent field in HTTP packet headers.

ASA CX Policy Object Types (Cont.)

Policies > Objects



From the **Policy > Objects screen**, you can create, edit, delete, and view the objects. The figure shows an example of the Policy Objects page, on which you can see the list of defined policy objects. The page also displays the type of policy object and how many policies use that policy object.

Hover beneath an existing policy object to bring up the links to view, delete, or edit that policy object.

The Filter option can be used to filter the output display to show only a particular policy object or objects.

System predefined objects can only be viewed, not edited or deleted.

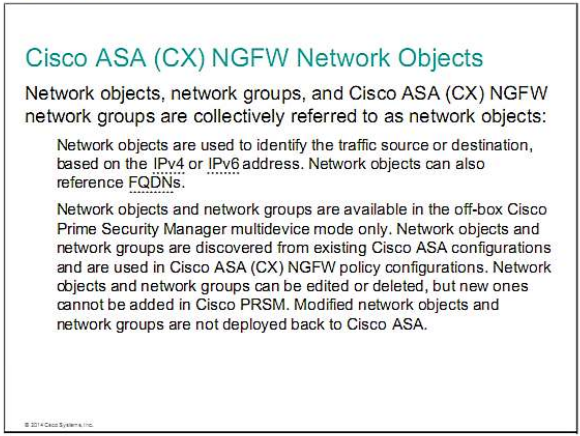
System predefined objects include many service groups and user agent objects, two identity objects, one secure mobility object, and one web reputation profile.

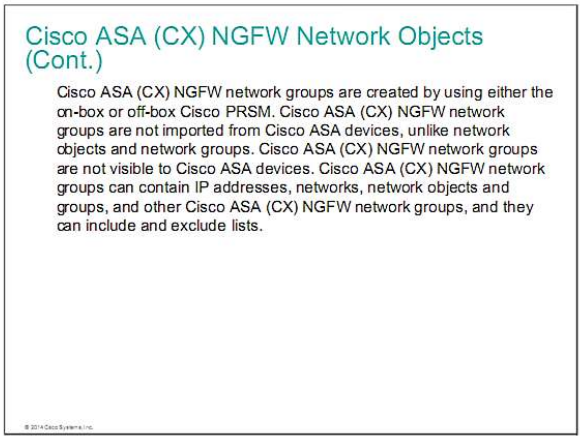
When configuring an object, you can enter multiple matching values in the object. These values are considered to be in an OR relationship, unless an explicit AND is shown; that is, traffic will match the object if the traffic matches any item specified. Typically, objects have multiple fields that allow you to enter values or nest other existing objects. For example, in a URL object, you can enter a combination of specific URLs, web categories, and other URL objects. Any fields that you leave blank are ignored.

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

Cisco ASA (CX) NGFW Network Objects

This topic describes how to configure Cisco Adaptive Security Appliances Context Aware Next Generation Firewall network objects.

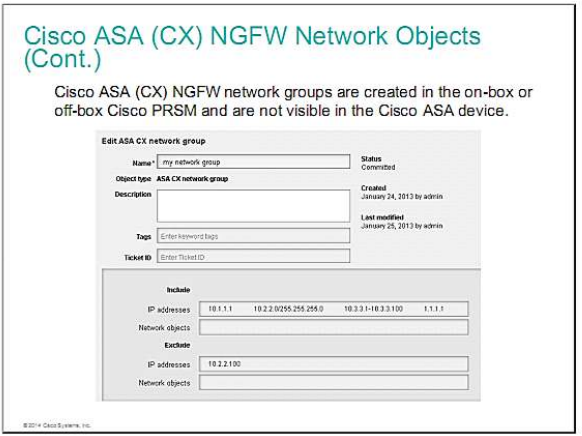




Network objects, network groups, and Cisco ASA (CX) NGFW network groups (collectively referred to as network objects) are used during Cisco ASA (CX) NGFW policy creation, to identify the traffic source or destination, based on the IP address. The IP address can be IPv4 or IPv6. Network objects can also refer to FQDNs, such as www.example.com.

During the device import process, Cisco ASA network objects and network groups can be learned from the Cisco ASA configurations. Network groups are the network object groups in Cisco ASA. Any changes that are made to network objects and network object groups are not deployed back to the Cisco ASA device; the changes affect the use of the objects for Cisco ASA (CX) NGFW policies only.

Cisco ASA (CX) NGFW can also use Cisco ASA (CX) NGFW network groups. Cisco ASA (CX) NGFW network groups are not visible or useable on the Cisco ASA device. Cisco ASA (CX) NGFW network groups are created in the on-box or off-box Cisco PRSM and can contain IP addresses, networks, network objects and network object groups, other Cisco ASA (CX) NGFW network groups as well as include and exclude lists.



The figure shows the Edit ASA CX network group screen.

In this example, the Cisco ASA (CX) NGFW network group that is being edited is named "my network group." This Cisco ASA (CX) NGFW network group includes the 10.1.1.1 IP address, the 10.2.2.0/24 subnet, the 10.3.3.1 to 10.3.3.100 range of IP addresses, or the 1.1.1.1 IP address.

For any type of object, you can enter multiple matching values, which are considered to be in an OR relationship, unless an explicit AND is shown; that is, traffic will match the object if the traffic matches any item that is specified.

When entering multiple items, press **Enter** to accept each item and choose additional items. Choosing an item from a drop-down list automatically enters it into the box. To edit an existing item, click it, make your edits, and press **Enter**. To remove an item, click it or hover over it and click the **X** to the right of the name, then press **Delete**, and click away to complete the removal. If your entry is invalid, the entry is colored yellow; click the **Errors** link next to the field for information about the problem that you must correct.

You can enter IP addresses in these formats:

IPv4 network, including subnet mask; for example, 10.100.10.0/24 or 10.100.10.0/255.255.255.0

Standard IPv4 address; for example, 10.100.10.10

IPv4 address range; for example, 192.168.1.1-192.168.1.5

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

Cisco ASA (CX) NGFW network group and network objects that support IPv4 address ranges but not IPv6 address ranges

IPv6 network, including prefix; for example, 2001:DB8:0:CD30::/60

IPv6 address in compressed format, in which you replace a series of fields of zeros with "::"; for example, 2001:DB8::0DB8:800:200C:417A

IPv6 address in uncompressed format; for example, 2001:DB8:0:0:0DB8:800:200C:417A

The Cisco ASA (CX) NGFW network groups can contain include and exclude lists. The exclude list is always related to the include list.

In this example, the exclude list includes the 10.2.2.100 IP address, so all the IP addresses that are included in the 10.2.2.0/24 subnet, except the 10.2.2.100 IP address, will be matched.

The status of the object is also shown. In this example, the status is committed, so this policy object configuration has been successfully deployed to the devices that use it. Other status example include Pending (Modified), which means that a change has been made to an existing policy object but has not been committed, and Pending (New), which means that a newly created policy object has not been committed.

https://t.me/learningnets

Cisco ASA (CX) NGFW Service Objects and Service Groups

This topic describes how to configure Cisco Adaptive Security Appliances Context Aware Next Generation Firewall service objects and service groups.

Cisco ASA (CX) NGFW Service Objects and Service Groups

Service objects and service groups provide the more traditional port-based matching and are used to identify traffic, based on protocol, port, or ICMP or ICMPv6 services.

Many system predefined service groups cover common protocols and ICMP and ICMPv6 services.

© 2014 Cisco Systems, Inc.

Cisco ASA (CX) NGFW Service Objects and Service Groups (Cont.)

Service objects are available in off-box Cisco Prime Security Manager multidevice mode only. Service objects are discovered from the Cisco ASA configurations and are used in Cisco ASA (CX) NGFW policy configurations. Service objects can be edited or deleted, but new objects cannot be added in Cisco PRSM. Modified service objects are not deployed back to Cisco ASA devices.

Service groups can contain services and other service objects. In off-box Cisco PRSM multidevice mode, service groups can be discovered from Cisco ASA configurations. Discovered service groups can be edited or deleted. Modified service groups are not deployed back to Cisco ASA devices. New service groups can also be created by using the on-box or off-box Cisco PRSM.

© 2014 Cisco Systems, Inc.

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

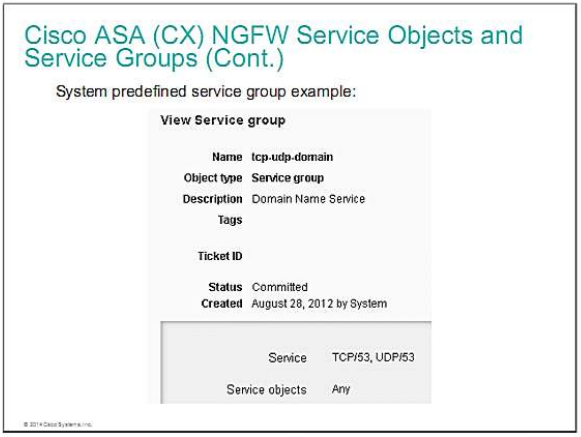
Service objects and service groups are used to identify traffic based on the protocol, port, ICMP or ICMPv6 services. Use these objects when you specifically want to target a port or range of ports, or an ICMP or ICMPv6 service. Consider using application objects if you really want to target a specific application regardless of the ports used by any given connection session. Service groups provide the more traditional port-based matching criteria.

During the device import process, you can learn Cisco ASA service objects and service groups from the Cisco ASA configurations. Any changes that are made to network objects and network object groups are not deployed back to the Cisco ASA device. These changes affect the use of the objects for the Cisco ASA (CX) NGFW policies only.

Service groups can also be created by using the Cisco PRSM. Service groups can also contain include and exclude lists. The exclude list is always related to the include list.

To specify services within a service group, use the format [tcp or udp or ip]/[source port or range]/[destination port or range].

For ICMP, use icmp/[subtype number]; for example, tcp/80, udp/313-332/5443, ip/434-450, icmp/0, icmp/16.



The figure shows an example of a system predefined service group. The service group name is tcp-udp-domain and is used to match TCP or UDP port 53.

System predefined objects can be viewed only, not edited or deleted.

https://t.me/learningnets

Cisco ASA (CX) NGFW Application Objects and Application Service Objects

This topic describes how to configure Cisco Adaptive Security Appliances Context Aware Next Generation Firewall application objects and application service objects.

Cisco ASA (CX) NGFW Application Objects and Application Service Objects

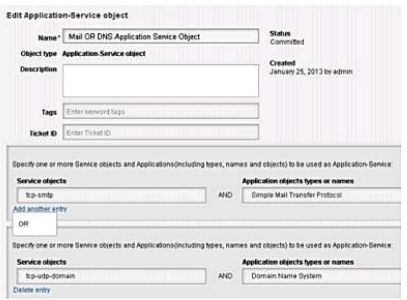
Application objects can contain applications, application types, and other application objects that are recognized by Cisco ASA (CX) NGFW.

Application service objects can contain rows of service objects and application objects. The services objects and application objects are connected with AND statements and and the rows are connected with OR statements.

Traffic inspection can identify an application regardless of the port that is used.

© 2014 Cisco Systems, Inc.

Cisco ASA (CX) NGFW Application Objects and Application Service Objects (Cont.)



© 2014 Cisco Systems, Inc.

https://t.me/learningnets

Application objects are used to identify any applications or application types that Cisco ASA (CX) NGFW can recognize, as well as other application objects. Application objects are used to identify individual applications or types of applications. Use these objects to tailor policies, based on the application or application type that is being used during a session in place of a traditional service definition that is based on protocol and port. Traffic inspection can identify an application regardless of the port that is used during any particular connection session.

Application service objects are used to identify a collection of entries. The default is only one entry. Each entry can have a service object and an application object element, connected by an AND statement. You can create a new entry by clicking the **Add Another Entry** link. To remove an entry, click the **Delete Entry** link. Different entries are connected with OR statements.

In the example that the figure shows, the application service object will match the SMTP application on TCP port 25 or the DNS application on TCP/UDP port 53:

Match (tcp-smtp service object AND the Simple Mail Transfer Protocol application)

OR

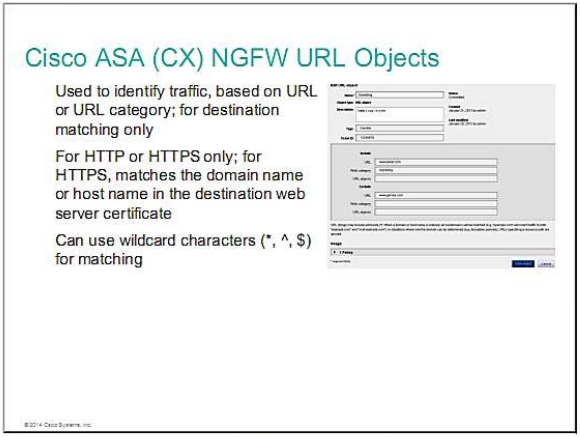
Match (tcp-udp-domain service object AND the Domain Name System application)

The **tcp-smtp** object is a predefined service object that matches TCP port 25. The **tcp-udp-domain** object is a predefined service object that matches TCP/UDP port 53.

For example, if the SMTP application uses TCP port 2525, the SMTP application will not be matched by this application service object. If the DNS application uses TCP port 5353, the DNS application will not be matched by this application service object.

Cisco ASA (CX) NGFW URL Objects

This topic describes how to configure Cisco Adaptive Security Appliances Context Aware Next Generation Firewall URL objects.



URL objects can be used to impose acceptable use policies for web browsing.

URL objects are used to identify the web domain (such as example.com) or web servers (such as www.example.com), the web URL resources (such as http://www.example.com/games or https://www.example.com/games), and web URL categories.

URL objects contain the URL field, in which you can define a list of individual web-based URLs. You can specify URLs that include only the domain name or server name, so that they apply to all the web pages that are available on all the servers on a domain or server, or you can include paths to specific web pages, to differentiate between pages that are hosted at the same site.

Do not include the protocol; for example, use www.example.com or example.com rather than http://www.example.com. HTTP and HTTPS are the only protocols that match these URLs. If you want to treat all servers in a domain equally, enter the domain name only, such as example.com. The object then applies to www.example.com, games.example.com, photos.example.com, and so on.

These wildcard characters can be used to create URL patterns that apply to multiple web pages:

Asterisk (*): Use the asterisk to match zero or more characters; for example, www.example.com/us/* matches all web pages on the www.example.com/us/ web server space.

Caret (^): Placed at the beginning of a URL, the caret indicates a URL that starts with the string that follows it; for example, ^www.example.com matches all web pages that start with www.example.com. The difference between ^www.example.com and www.example.com is that www.example.com also matches server1.www.example.com and any other sites that have modifiers prior to "www.example.com."

Dollar sign ($): Placed at the end of a URL, the dollar sign indicates a URL that ends with the preceding string; for example, /index.html$ matches all URLs that point to a page named index.html.

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

URL objects contain the Web Category field, in which you can define the desired web categories from a list of web categories.

URL objects can contain other URL objects and include and exclude lists. The exclude list is always related to the include list.

The figure shows an example of a user-defined URL object named Gambling.

This URL object will match all the web pages that are available on www.poker.com OR all sites that belong to the system-predefined Gambling web category. The object will exclude all the web pages that are available on www.games.com.

Cisco constantly evaluates the relevance of sites within a particular category to ensure the highest possible accuracy. You can use the following link to view a table that contains an alphabetical listing and descriptions of the standard categories that are used to classify websites:

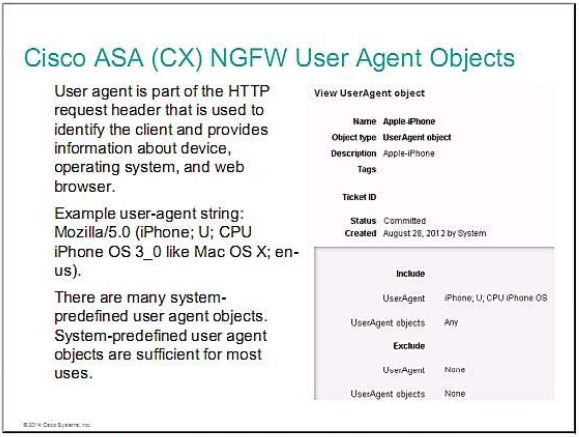
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps10142/ps10164/datasheet_C78-718442.html

Using a valid Cisco Connection Online login, the website below can be used to check the URL category of a website and to submit a request to Cisco to have the URL category of a website changed.

https://securityhub.cisco.com/web/submit_url

Cisco ASA (CX) NGFW User Agent Objects

This topic describes how to configure Cisco Adaptive Security Appliances Context Aware Next Generation Firewall user agent objects.



User agent is part of the HTTP request header that is used to identify the client and provides information about the device, operating system, and web browser.

Examples of a user-agent string:

Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us)

Mozilla/5.0 (Windows NT 6.1; WOW64; rv:18.0) Gecko/20100101 Firefox/18.0

You can use user agent information to tailor Cisco ASA (CX) NGFW policies, based on the device that is being used to access the network; for example, explicitly exclude user agents that cannot respond to active authentication prompts in an identity policy that otherwise requires authentication.

The user agent object contains the User-Agent string field. The wildcard character (*) can be used to match zero or more characters in the user agent string; for example, Mozilla/*.

The user agent object can also contain other user agent objects and include and exclude lists. The exclude list is always related to the include list.

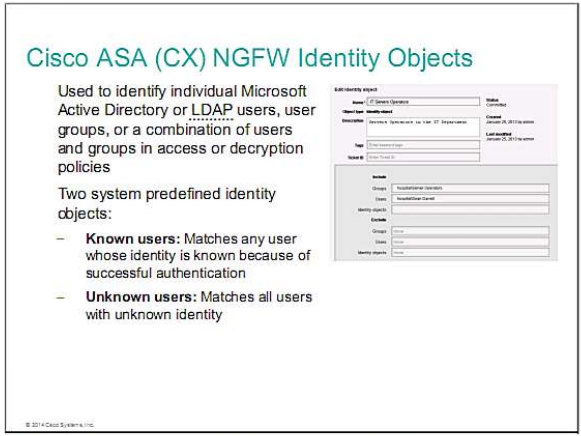
Cisco ASA (CX) NGFW comes with many system-predefined user agent objects. System-predefined user agent objects are sufficient for most use cases.

Note The User-Agent string can easily be spoofed by using browser user agent switcher add-ons.

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

Cisco ASA (CX) NGFW Identity Objects

This topic describes how to configure Cisco Adaptive Security Appliances Context Aware Next Generation Firewall identity objects.



Use identity objects to identify individual Active Directory or LDAP users, user groups, or a combination of users and groups.

Identity objects contain the Groups, Users, and Identity object fields. Identity objects can also contain the include and exclude lists. The exclude list is always related to the include list.

As you enter the user names or group names to include in the object, queries are made to help automatically complete your entry. The list of matching user or group names is retrieved from the directories that are configured for all realms that are defined on the system. Choose the desired name from the retrieved list. You must define a realm before you can create identity objects. Defining a realm is part of the configuration steps when creating identity policies.

The example in the figure shows an identity object named IT Servers Operators. This object will match the hospital\Server Operators group or the hospital\Sean Darrell user.

There are two system-predefined identity objects:

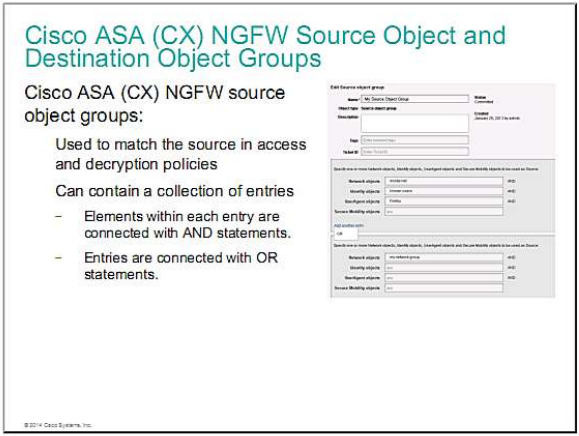
Known users: This object matches any user for whom identity is available, either because the user is actively authenticated or because a passive mapping for the user IP address was obtained from Cisco Context Directory Agent.

Unknown users: This object matches users who do not match the known users object, such as, for example, IP addresses for which a user-to-IP address mapping is unavailable, or all users with unknown identity.

https://t.me/learningnets

Cisco ASA (CX) NGFW Source Object and Destination Object Groups

This topic describes how to configure Cisco Adaptive Security Appliances Context Aware Next Generation Firewall source object and destination object groups.



Use source object groups to define a potentially complex source-traffic match criterion by using the objects that are allowed in the source field of an access or decryption policy.

Source object groups contain a collection of entries, with a default of only one entry. The elements of each entry are connected with AND statements. You can create a new entry by clicking the **Add Another Entry** link. To remove an entry, click the **Delete Entry** link. Different entries are connected with OR statements

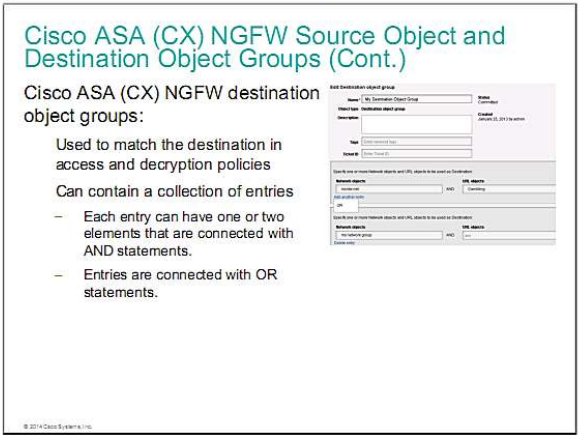
In the example in the figure, the source object group My Source Object Group uses this matching logic:

Match (the inside-net network object AND the Known users identity object AND the Firefox user agent object)

OR

Match the my network group network object

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



Destination object groups are used to define a potentially complex destination-traffic match criterion by using the objects that are allowed in the destination field of an access or decryption policy.

Destination object groups contain a collection of entries, with a default of only one entry. Each entry can have one or two elements that are connected with AND statements. You can create a new entry by clicking the **Add Another Entry** link. To remove an entry, click the **Delete Entry** link. Different entries are connected with OR statements.

In the example in the figure, the destination object group My Destination Object Group uses this matching logic:

Match (the inside-net network object AND the Gambling URL object)

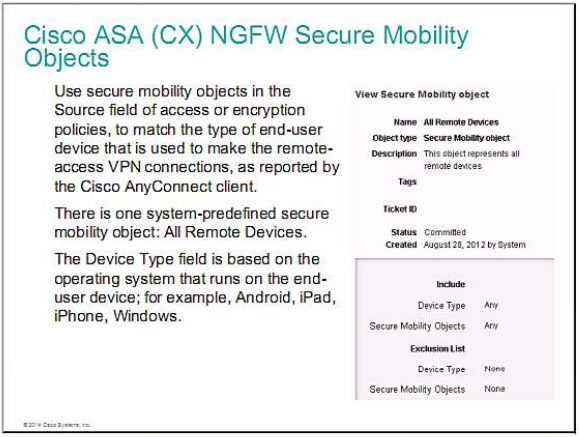
OR

Match the my network group network object to any URL destinations.

https://t.me/learningnets

Cisco ASA (CX) NGFW Secure Mobility Objects

This topic describes how to configure Cisco Adaptive Security Appliances Context Aware Next Generation Firewall secure mobility objects.



Use secure mobility objects in the Source field of access or decryption policies, to match the type of end-user device that is used to make the remote-access VPN connections, as reported by the AnyConnect client.

All Remote Devices is the one system-predefined security mobility object and will match any device that is used in a remote-access VPN connection. User-defined security mobility objects can be defined to match different user-device types.

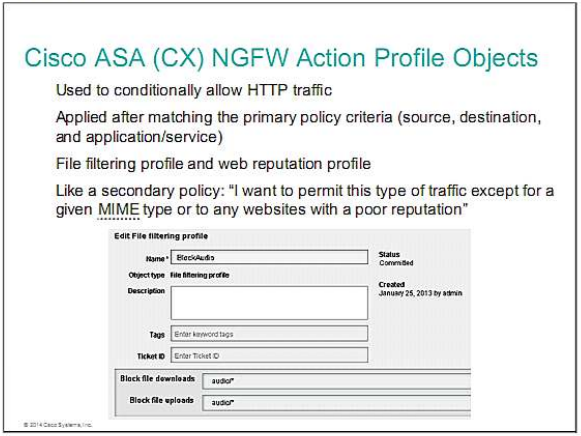
Secure mobility objects contain the Device Type field and Secure Mobility Objects field. The device type is based on the operating system that runs on the end-user device; for example, Android, iPad, iPhone, Windows, Windows Mobile. The Secure Mobility Objects field can refer to other secure mobility objects.

Secure mobility objects can also contain include and exclude lists. The exclude list is always related to the include list.

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

Cisco ASA (CX) NGFW Action Profile Objects

This topic describes how to configure Cisco Adaptive Security Appliances Context Aware Next Generation Firewall action profile objects.



Use action profile policy objects to implement acceptable use access policies. By using action profiles in the access policies, certain types of traffic that are otherwise allowed can be dropped.

There are two types of action profile:

File filtering profile: A file filtering profile object determines which types of files users cannot upload or download; for example, allow all downloads but prevent all uploads, to ensure that company files are not transferred out of network. If no file filtering profile is specified in an access rule, then all file uploads and downloads are allowed.

Web reputation profile: Web reputation is a statistical assessment that is based on context and past behavior and that combines many factors of varying significance into one correlated metric. Like a credit score, web reputation is a continuous value along a graduated scale from -10 to 10. The Cisco Threat Operations Center uses dynamic updates and actionable intelligence, obtained from Cisco ASA and Cisco Intrusion Prevention System devices, email security appliances, web security appliances, and system administrators, to calculate a web reputation score for websites. By defining a low-reputation zone, you can implement predictive, zero-day protection against low-reputation sites, which are most likely to serve malware to your users.

Web reputation profile objects can be used in access and decryption policies.

In access policies that allow traffic, you can add a web reputation profile so that the policy will generally allow matching traffic but will drop any traffic from a low-reputation site. You can apply the profile to any or all access policies that have the Allow action. Use the system-predefined object, Default Reputation Profile, to implement the recommended policy, which drops any traffic from websites with a reputation score of -6 or lower.

https://t.me/learningnets

In decryption policies whose action is Decrypt Potentially Malicious Traffic, adding a web reputation profile causes any low-reputation websites that match the policy to be decrypted, so the access policy can examine the decrypted content of the traffic. The access policy can then drop the traffic if configured to do so. Even if you do not have a matching access policy that drops traffic, decrypting the traffic to any low-reputation websites provides data that is otherwise unavailable for undecrypted TLS/SSL traffic flows.

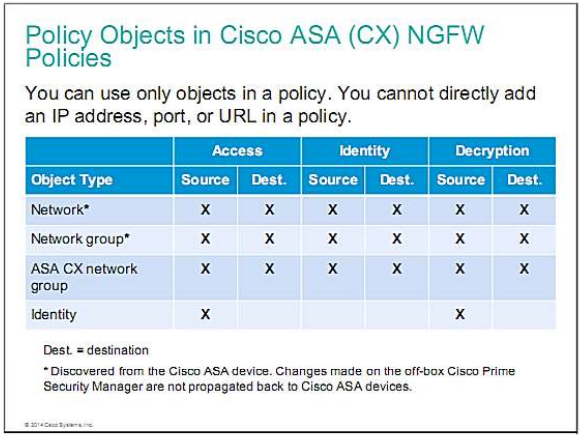
File filtering and web reputation profiles apply only to HTTP traffic.

The figure shows an example of a file filtering profile that can be used in an access policy to block any audio file downloads or uploads.

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

Policy Objects in Cisco ASA (CX) NGFW Policies

This topic identifies where each policy object can be used in Cisco Adaptive Security Appliances Context Aware Next Generation Firewall policy configurations.



Policy Objects in Cisco ASA (CX) NGFW Policies

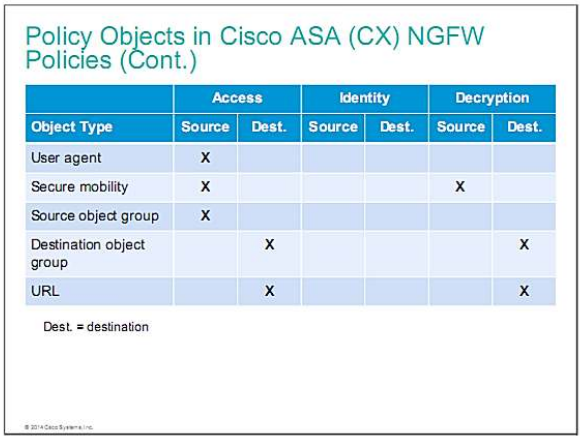
You can use only objects in a policy. You cannot directly add an IP address, port, or URL in a policy.

	Access		Identity		Decryption	
Object Type	**Source**	**Dest.**	**Source**	**Dest.**	**Source**	**Dest.**
Network*	X	X	X	X	X	X
Network group*	X	X	X	X	X	X
ASA CX network group	X	X	X	X	X	X
Identity	X				X	

Dest. = destination

* Discovered from the Cisco ASA device. Changes made on the off-box Cisco Prime Security Manager are not propagated back to Cisco ASA devices.

© 2014 Cisco Systems, Inc.



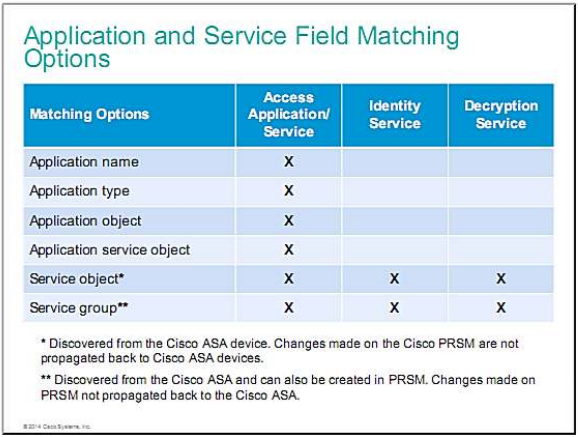
Policy Objects in Cisco ASA (CX) NGFW Policies (Cont.)

	Access		Identity		Decryption	
Object Type	**Source**	**Dest.**	**Source**	**Dest.**	**Source**	**Dest.**
User agent	X					
Secure mobility	X				X	
Source object group	X					
Destination object group		X				X
URL		X				X

Dest. = destination

© 2014 Cisco Systems, Inc.

The table in the figure shows which types of Cisco ASA (CX) NGFW policies can use which type of objects. For example, the identity object can be used only in the access or decryption policies for matching the traffic source. The URL object can be used only in the access or decryption policies for matching the traffic destination.



Application and Service Field Matching Options

Matching Options	Access Application/ Service	Identity Service	Decryption Service
Application name	X		
Application type	X		
Application object	X		
Application service object	X		
Service object*	X	X	X
Service group**	X	X	X

* Discovered from the Cisco ASA device. Changes made on the Cisco PRSM are not propagated back to Cisco ASA devices.

** Discovered from the Cisco ASA and can also be created in PRSM. Changes made on PRSM not propagated back to the Cisco ASA.

© 2014 Cisco Systems, Inc.

The table in the figure shows which application and service matching options are available in the access, identity, and decryption policies.

In an access policy, the Application/Service field can match an application name, type, or object or a service object or group.

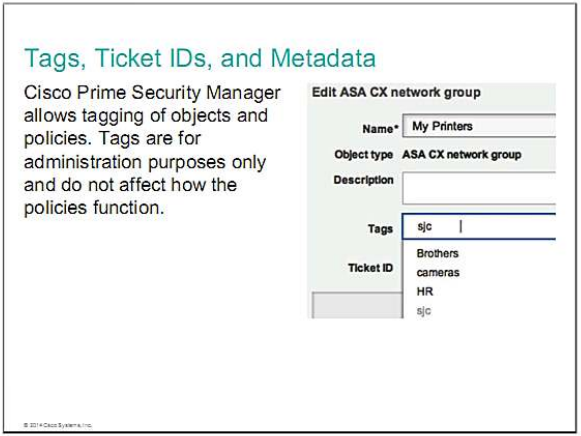
In an identity or decryption policy, the Service field can match a service object or group.

 © 2014 Cisco Systems, Inc.

https://t.me/learningnets

Tags, Ticket IDs, and Metadata

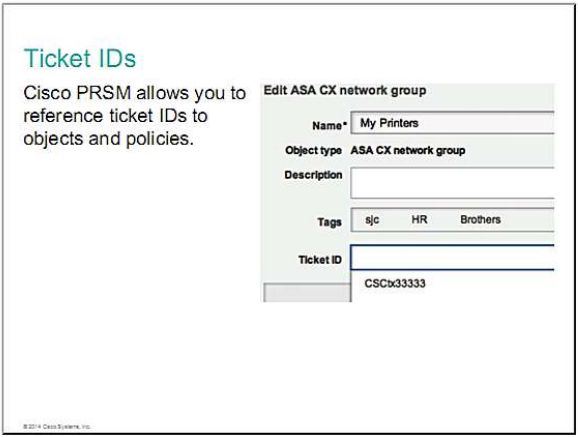
This topic identifies the purpose of tagging, ticket ID, and metadata.



Tagging allows Cisco Adaptive Security Appliances Context Aware Next Generation Firewall administrators to identify an object or a policy. The same tag can be assigned to multiple items, to make it easy to view the items through a search. Tags can be used to identify a particular use case, location, or any other characteristic. These tags are for administration purposes only and do not affect how the system or policies function. You can assign or more tags assigned to an item.

When you define a tag, previously used tags are listed. You can choose an existing tag or enter a new tag.

In the example that the figure shows, the Cisco ASA (CX) NGFW network group is being tagged with the sjc tag.

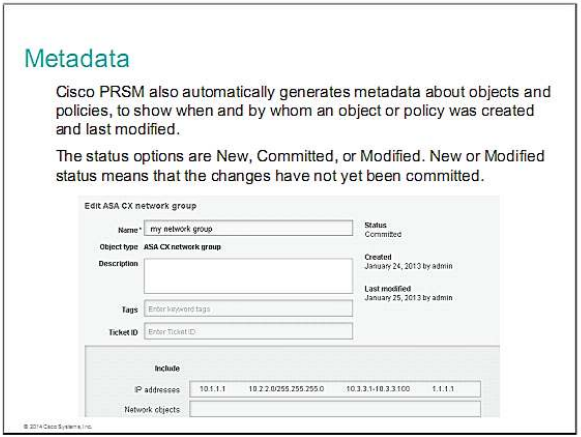


Ticket IDs allow Cisco ASA (CX) NGFW administrators to associate an object or a policy to a ticket or case ID. A ticket ID can be used as a case or ticket identifier from the support system (for example, Remedy) for tracking purposes. The same ticket ID can be assigned to multiple items, to make it easy to view the items through a search. Ticket IDs are for administration purposes only and do not affect how the system or policies function. You can assign one or more ticket IDs to an item.

You can enter new ticket IDs or choose from existing ticket IDs that are used in pending changes. Specify as many separate ticket IDs as are needed. The list from which to choose an existing ticket ID does not include ticket IDs that have been used in committed changes.

In the example that the figure shows, the Cisco ASA (CX) NGFW network group My Printers is associated with ticket ID CSCtx33333.

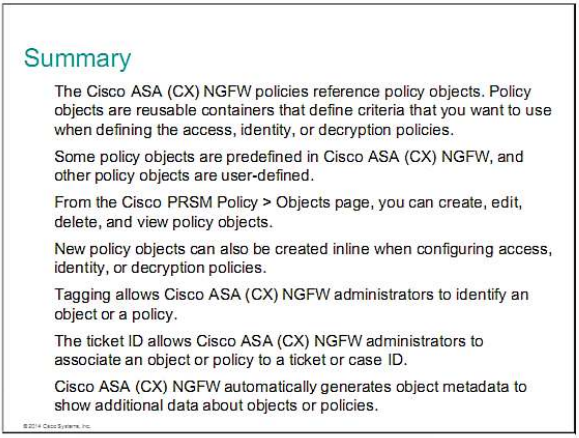
 © 2014 Cisco Systems, Inc.
https://t.me/learningnets



Cisco ASA (CX) NGFW automatically generates object metadata to show additional data about the objects or policies, such as which user created the object or policy, the creation date, the last modified date, and the item status (New, Modified, or Committed). A status of New or Modified indicates that the new or modified configuration has not yet been committed by the administrator.

Summary

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



References

For additional information, refer to these resources:

Cisco Systems, Inc. *Cisco ASA Series Firewall CLI Configuration Guide, 9.1.* http://www.cisco.com/en/US/docs/security/asa/asa91/configuration/firewall/asa_91_firewall_config.html

Cisco Systems, Inc. *Cisco ASA Series Firewall ADSM Configuration Guide, 7.1.* http://www.cisco.com/en/US/docs/security/asa/asa91/asdm71/firewall/asdm_71_firewall_config.html

Cisco Systems, Inc. *User Guide for ASA CX and Cisco Prime Security Manager 9.1* http://www.cisco.com/en/US/docs/security/asacx/9.1/user/guide/b_User_Guide_for_ASA_CX_and_PRSM_9_1.pdf

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

Lesson 4

Monitoring Cisco ASA (CX) NGFW Operations

Overview

This lesson describes how to monitor the Cisco Adaptive Security Appliances Context Aware Next Generation Firewall using the Cisco Prime Security Manager dashboards, reports and event viewer.

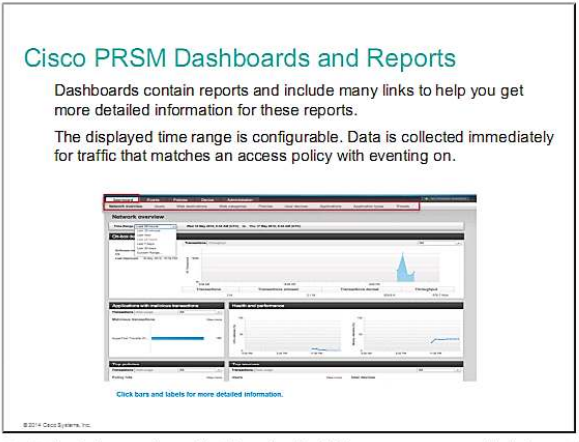
Upon completing this lesson, you will be able to meet these objectives:

- Monitor Cisco ASA (CX) by using the Cisco PRSM dashboards and reports
- Monitor and troubleshoot Cisco ASA (CX) by using the Cisco PRSM Event Viewer
- Monitor Cisco ASA (CX) and Cisco PRSM Cisco SIO updates

https://t.me/learningnets

Cisco PRSM Dashboards and Reports

This topic describes how to monitor the Cisco Adaptive Security Appliances Context Aware Next Generation Firewall by using the Cisco Prime Security Manager dashboards and reports.



The Cisco PRSM includes a variety of dashboards with different reports to provide information about Cisco ASA (CX) NGFW device health, performance, and network usage. The report data is collected only for traffic that matches an access policy in which Eventing is set to On, which is the default setting for access policies. If you turn off Eventing for an access policy, then any traffic that matches the access policy will not be represented in the dashboards and will not generate events in Event Viewer.

The figure shows an example of the Network Overview dashboard from an on-box Cisco PRSM.

Dashboards aggregate information about various aspects of your network traffic. You can view dashboards that show various periods, to analyze the traffic on your network. In most cases, you can view both general and specific information; for example, you can view a dashboard on all users, then view details about specific users. Dashboards include many links to help you find the information that you need. Hover over items to see which ones might lead you to more information.

When you view a dashboard, you can use the Time Range list to change the time range that defines the included information. The Time Range list is at the top of each dashboard and allows you to select predefined time ranges, such as the past hour or past week, or to define a custom time range with specific start and end times. The time range that you choose is carried over to any other dashboard that you view, until you change the time range. The time is based on the time zone that is defined on the device, not the zone that is configured on your workstation.

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

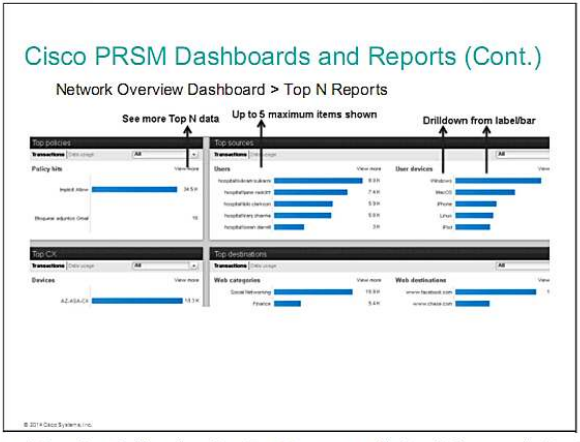
The report data is collected immediately from Cisco ASA (CX) NGFW, so there is little lag time between the data reflected in a report and network activity. Data in the reports are represented in 5-minute increments for 30-minutes and 1-hour graphs. Real-time data is added to the current 5-minutes increment. For older time ranges, these increments are further aggregated into one-hour increments (for the past day), one-day increments (for periods of more than one day to the past week), and one-week increments (for periods more than a week past). If a data point is missing, gaps will appear in the line charts; for example, because the device was unreachable for longer than 5 minutes. The reports automatically update every 10 minutes. Refresh the dashboard to display the most recently collected reports.

When you view reports in off-box Cisco PRSM multidevice mode, the report data is aggregated from all managed Cisco ASA (CX) NGFW devices. To view information that is specific to a singe device, use the Devices report.

Note In the Cisco PRSM 9.1.2 release, you can export sets of predefined reports as PDF files. Each report can have a customizable time range and an image upload widget that a user can use to add to the report. To create a report, use the link on the top-right side of all dashboard pages to launch the report-creation, pop-up window.

The Cisco PRSM 9.1.2 release also contain a new Malicious Traffic dashboard. By clicking the View More link in this dashboard, you will see a dashboard of malicious traffic and data usage in various categories: users, web categories, web destinations, and applications.

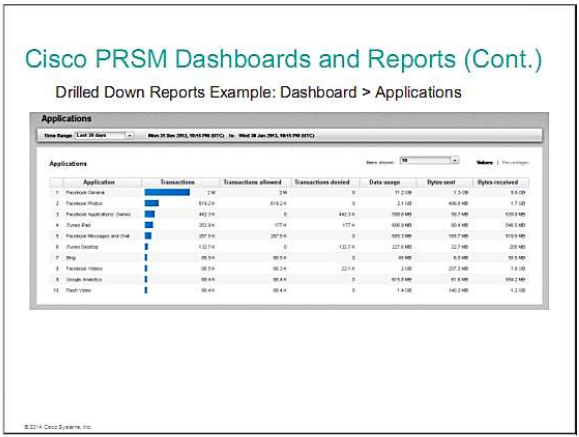
In the Cisco PRSM 9.2.1 release, there is a new ASA Traffic dashboard where you can view top sources, destinations, and services for the ASA.



In the Network Overview dashboard, various Top N reports are displayed; for example, Top Policies, Top Sources, Top CX (when using off-box Cisco PRSM multidevice mode), Top Destinations, and so on.

Within each Top N report, as many as five items can be displayed. To display all the items on a report, click the **View More** link to display the more detailed report. For example, click the **View More** link in the Top Policy report to open the **Policy Hits** detailed report. The same Policy Hits report is displayed when you choose **Dashboard > Policies**.

To get more detailed data about a particular item in a Top N report, click the label or the bar for that item. For example, click the **Windows** label in the User Devices report to open the **Dashboard > User Devices > Windows** detailed report.



To display a detailed report, choose **Dashboard > Users, Dashboard > Web Destinations**; **Dashboard > Web Categories, Dashboard > Policies**; **Dashboard > User Devices, Dashboard > Applications**; **Dashboard > Application Types**; **Dashboard > Threats**; or **Dashboard > Devices**.

The figure shows an example of the Applications detailed report, which shows application and usage information.

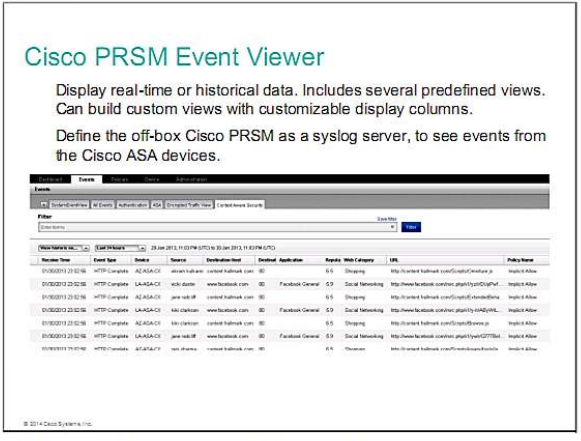
Use the **Items Shown** drop-down list to choose the number of items to show on the detailed report.

Refer to the Cisco ASA (CX) NGFW and PRSM User Guide for more information about all the other available reports and operations.

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

Cisco PRSM Event Viewer

This topic describes how to monitor Cisco Adaptive Security Appliances Context Aware Next Generation Firewall by using the Cisco Prime Security Manager Event Viewer.



Use the Event Viewer to monitor and examine events from the devices that you manage. Events are organized into views that you can filter or search to find the events that interest you. In addition to using the predefined views, you can create custom views. The off-box Cisco PRSM can show both Cisco ASA and Cisco ASA (CX) NGFW events in the Event Viewer. Cisco PRSM supports as many as 15,000 events per second.

You can create customized views and filters to fit your needs, or you can use the predefined views. To create a custom view, click the Plus (+) icon to the left of the first tab.

You can also customize the display columns in each view, by clicking the icon in the upper-right corner (not shown in the figure).

When you customized the display columns of a view, a copy of the view will be automatically created with the customized display columns.

The Event Viewer includes these predefined views:

System Event Views: Shows system events, such as signature updates

All Events: In Cisco PRSM single-device mode, shows all events for the device; in multidevice mode, shows all events from all monitored Cisco ASA and managed Cisco ASA (CX) NGFW devices

Authentication: Shows Cisco ASA (CX) NGFW authentication events

ASA: Multidevice mode only; shows events from all monitored Cisco ASA devices

Encrypted Traffic View: Shows Cisco ASA (CX) NGFW encrypted traffic events, which are related to decryption policies

Context Aware Security: Shows events from the Cisco ASA (CX) NGFW

With Event Viewer, you can either watch events as they happen or view a historical time range when analyzing events. Event Viewer shows the current date and time range for the events in the events table.

You can switch any view between real time and historical by using the drop-down box in the top left, above the events table.

Real-Time Eventing: Use this option to view events in real time as they happen. Choose the refresh rate for updating the table with new events in 5-, 10-, 20-, or 60-second intervals. Use the Play (arrow) and Pause (double hash) buttons to start and stop event-table updates. Pause the view when you want to analyze a particular event.

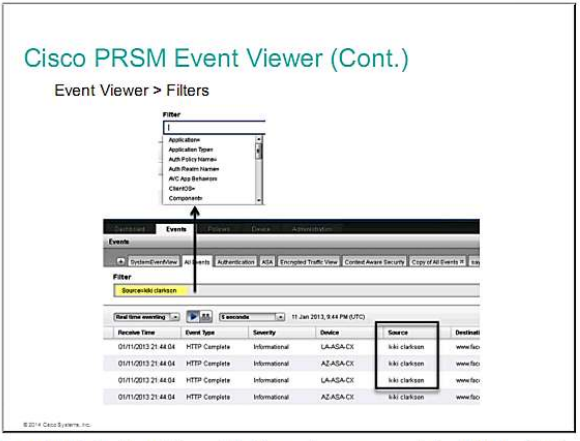
View Historic Events: Use this option to view events in a previous period. Choose the time window for the events. Most options are from the current time into the past; these views are refreshed to show new events that fit into the window. You can view events from the past 30 minutes, 1 hour, 4 hours, 12 hours, or 24 hours. The time is based on the time zone that is defined on the device, not the zone that is configured on your workstation. You can also choose Custom Date/Time and specify the exact starting and ending date and time that you want to view.

With the on-box Cisco PRSM (single-device mode), when you are logged in to an unmanaged Cisco ASA (CX) NGFW device, you can see events from that Cisco ASA (CX) NGFW only.

With the off-box PRSM (multidevice mode), events are collected from all monitored Cisco ASA devices and all managed Cisco ASA (CX) NGFW devices. You must define the off-box Cisco PRSM as a syslog server to see events from Cisco ASA devices. Managed Cisco ASA (CX) NGFW devices automatically redirect events to the off-box Cisco PRSM.

Cisco PRSM does not support the forwarding of event and report data to external stores.

The figure shows an example of the Event Viewer showing the historic Cisco ASA (CX) NGFW events of the past 24 hours. Note that the source field of the displayed events shows the username because identity policies are used to authenticate and identify users.

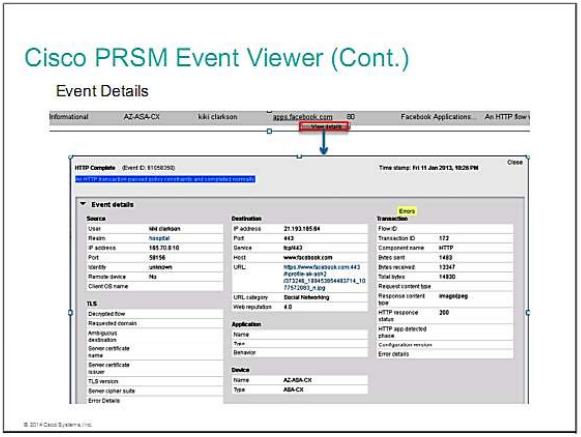


Filter can be applied in the Event Viewer. The figure shows an example in which the filter is set to Source=kiki clarkson. As a result, the Event Viewer shows only all the events that relate to the traffic that is sourced from the user kiki clarkson.

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

You can also hover over an empty Filter box to see a drop-down box with filter options. Choose a filter option. You can also click a field within an event to automatically choose that value as the filter.

To customize the columns to display in the Event Viewer, click the icon that the following figure shows. This icon is to the far right of View Historic Events or Real-Time Eventing and opens a small window, in which you can choose the columns to display.



When you need to investigate an event and need more detailed analysis, hover over the event and click the View Details button that appears. A window opens and shows the detailed event information. Click the Close link to close the window when you are finished. When open, this window can provide this information:

Complete details about the event, even if you do not include a particular column in your view. If the event contains data for an attribute, you can see that information by opening the event.

You can see the policies, including policy sets, that were involved in the event; for example, if the event was generated by a traffic flow that matched an access policy, the access policy is shown. If you want to make changes to the policy or policy set, hover over it and click Edit Policy or Edit Policy Set.

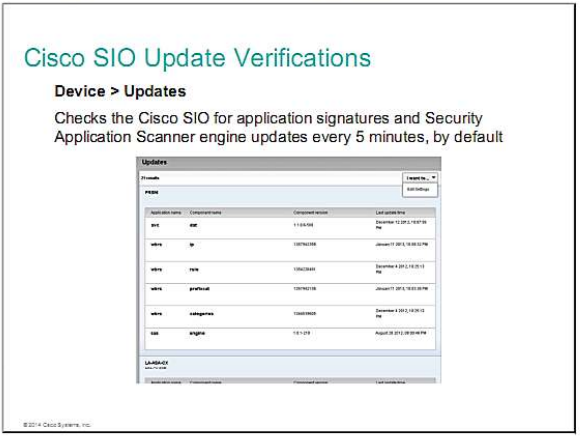
If the event includes authentication information, you can click the realm name to go to the directory realm configuration.

Refer to the Cisco ASA (CX) NGFW and PRSM User Guide for more information about all the the event views and operations and about each available event message.

https://t.me/learningnets

Cisco SIO Update Verifications

This topic describes how to monitor the Cisco Adaptive Security Appliances Context Aware Next Generation Firewall and Cisco Security Intelligence Operations updates.



There are two types of updates from Cisco SIO:

- Application signatures, URL categories, and web reputation score updates
- Security Application Scanner engine updates

Cisco SIO updates the application signatures, URL categories, and web reputation scores frequently. However Cisco SIO typically needs to update the Security Application Scanner engines only once every quarter. The Security Application Scanner engines evaluate traffic to determine the application, web category, or web reputation that is associated with the destination.

The Security Application Scanner engine updates require Cisco ASA (CX) NGFW to restart all the processes that use the Security Application Scanner engine. You can set a time range for when Security Application Scanner engine updates can occur; for example, only check for the Security Application Scanner engine update between 2 a.m. (0200) and 4 a.m. (0400).

Cisco ASA (CX) NGFW and the off-box Cisco Prime Security Manager check Cisco SIO for any new updates every 5 minutes, by default.

Go to the **Device > Updates** page to view the current signature and Security Application Scanner engine updates on the Cisco PRSM and on Cisco ASA (CX) NGFW devices.

From Device > Updates, click **I Want To > Edit Settings** to change the default update intervals:

- **Check Every 5 Minutes:** The update server is checked for signature and Security Application Scanner engines updates every 5 minutes throughout the day, seven days per week. This is the default.

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

Check Every 5 Minutes Within Window: The update server is checked every 5 minutes throughout the day for signature updates. However, Security Application Scanner engine updates are checked only within the time window that you specify. Click in the **Between** fields to choose the start and end times, which can be in 15 minute increments. For example, you can choose "Between 12:00 AM to 04:00 AM" to limit updates to a lower-traffic, early morning period. The time window is limited to a single day; for example, you cannot specify a time window that straddles midnight. The start time must be earlier than the end time when confined to a single day.

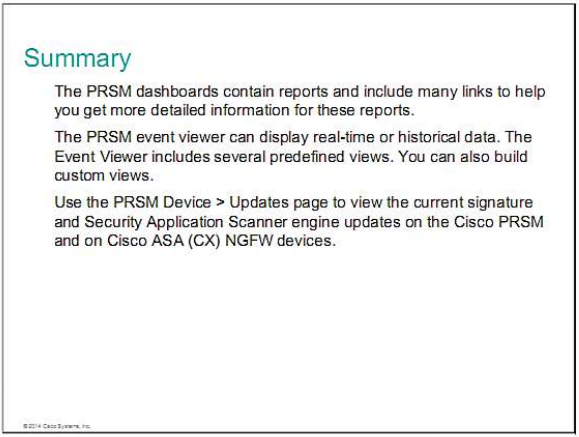
Never Check: The update server is never checked for signature or Security Application Scanner engine updates. Use this setting temporarily or if you decide not to purchase AVC or Web Security Essential licenses.

Note When using the off-box Cisco PRSM in multidevice mode, be aware that both Cisco ASA (CX) NGFW and the off-box Cisco PRSM server download the updates. If the signature levels between these systems become outdated, the off-box Cisco PRSM in multidevice mode will not deploy configurations to Cisco ASA (CX) NGFW. An out-of-date problem might be momentary, when one system receives an update slightly before the other system and you happen to try the deployment within that period. If this is the problem, simply wait and retry the deployment. If the problem persists, make sure that the earlier system has the required licenses and network connectivity to the Internet.

https://t.me/learningnets

Summary

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



References

For additional information, refer to these resources:

Cisco Systems, Inc. *Cisco ASA Series Firewall CLI Configuration Guide, 9.1.* http://www.cisco.com/en/US/docs/security/asa/asa91/configuration/firewall/asa_91_firewall_config.html

Cisco Systems, Inc. *Cisco ASA Series Firewall ADSM Configuration Guide, 7.1.* http://www.cisco.com/en/US/docs/security/asa/asa91/asdm71/firewall/asdm_71_firewall_config.html

Cisco Systems, Inc. *User Guide for ASA CX and Cisco Prime Security Manager 9.1* http://www.cisco.com/en/US/docs/security/asacx/9.1/user/guide/b_User_Guide_for_ASA_CX_and_PRSM_9_1.pdf

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

Lesson 5

Configuring Cisco ASA (CX) NGFW Access Policies

Overview

This lesson describes how to configure Cisco Adaptive Security Appliances Context Aware Next Generation Firewall access policies. Access policies are used to control access to the network. Complex traffic-matching criteria can be configured to define precise access policies.

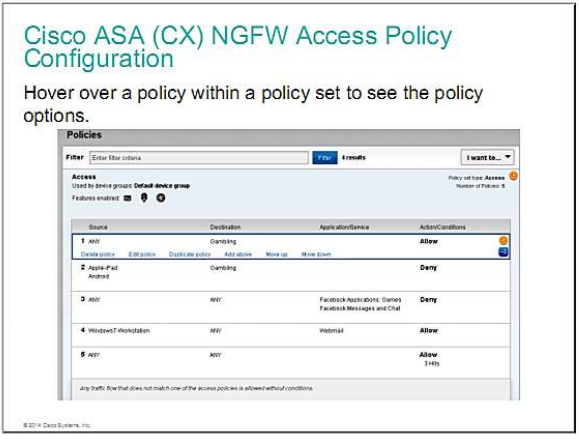
Upon completing this lesson, you will be able to meet these objectives:

- Describe how to configure Cisco ASA (CX) NGFW access policies to match security requirements
- Describe how to configure application controls within an access policy to match security requirements
- Describe how to configure URL filtering within an access policy to match security requirements
- Describe how to configure a file filtering profile and apply it to an access policy to match security requirements
- Describe how to configure a web reputation profile and apply it to an access policy to match security requirements
- Troubleshoot Cisco ASA (CX) NGFW access policies

https://t.me/learningnets

Cisco ASA (CX) NGFW Access Policy Configuration

This topic describes how to configure the Cisco Adaptive Security Appliances Context Aware Next Generation Firewall access policies to match security requirements.



An access policy is used to control access to the network. You can configure complex traffic-matching criteria to define precise access policies. Use the Source, Destination, and Application/Service fields to match the traffic to which the access policy applies. To match the access policy, there is an AND relationship between the Source, Destination,and Application/Service conditions. Within each Source, Destination, and Application/Service condition is a list of objects. If the traffic matches any of the objects within the field, then the traffic is considered to satisfy the condition. You can leave any field blank to specify the Any criteria (which is the default). Choosing the Any criteria means that the policy does not restrict traffic based on that criteria.

Hover over a policy within a policy set, then select one of the listed links:

- Delete the policy.
- Edit the policy
- Duplicate the policy.
- Add another policy above the current policy.
- Move the policy up in the policy set.
- Move the policy down in the policy set.

Policies are evaluated on a first-match basis. Incoming traffic is compared to the match criteria for each policy in a policy set, from top to bottom, and the first policy whose traffic-matching criteria is satisfied defines the security policy that is applied to the traffic. Thus, the order of the policies within a policy set is crucial.

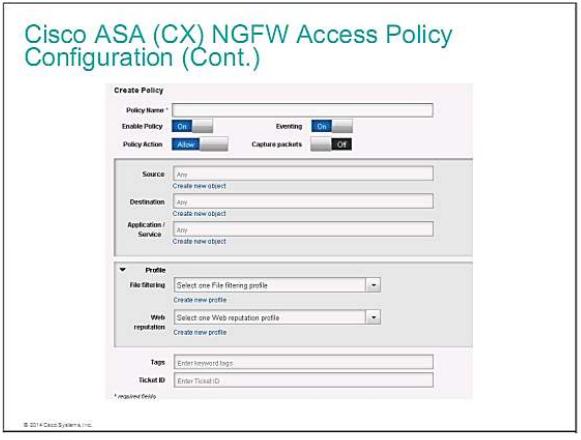
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

In the example in the figure, the first access policy in the policy set has two icons to the left of the Action/ Conditions field.

The top yellow icon indicates a pending commit; a change has been made to the policy and has not yet been committed.

The bottom blue icon indicates that Capture Packets is turned on for that policy.

Note The Capture Packets option works only for access policies that use Layer 3 or Layer 4 criteria or the default Any criteria. If you use any other match criteria, packets are not captured. Layer 3 or Layer 4 matching criteria are network objects and service objects.



Access policy configuration includes these options:

Enable Policy (On and Off): These options determine whether the policy is enabled. You can turn a policy off to temporarily disable it without deleting it. Disabled policies are never applied to any traffic flow.

Eventing (On and Off): These options determine whether the traffic flows that match the policy will generate events and dashboard data. The default is On. If you turn off eventing, traffic that matches this policy is reflected in dashboards, and you do not see events for the flows in Event Viewer.

Capture Packets (On and Off): These options determine whether to capture packets for flows that match the policy, if (and only if) the match criteria for the policy are limited to Layer 3 or Layer 4 criteria (network objects, service objects) or use the default Any criteria. The default is Off. If you turn this setting On, all packets are captured, so carefully consider the traffic volumes for matching flows before enabling Capture Packets. Packets are not captured for policies that use any criteria other than Layer 3 or Layer 4 criteria, even if you enable Capture Packets. The packet capture file is not written to disk until you turn off Capture Packets. The packet capture file is not created until you edit the policy and turn off Capture Packets. If an old capture file exists, it is overwritten. The capture file uses the policy name as the filename, with the extension .pcap. To upload packet captures to a server, use the Cisco ASA (CX) NGFW support diagnostic CLI command. Refer to the User Guide for ASA CX and Cisco Prime Security Manager for more detailed information about the support diagnostic command operations.

From the **Device > Packet Capture** window, you can configure buffer settings for the captures, such as the maximum buffer size and whether to use a circular buffer. From this screen, you can also enable all traffic that matches any Deny access policies with Layer 3 or Layer 4 match criteria only, and you can enable packets that are dropped because of any Layer 3 or Layer 4 checks to be captured globally. The packet capture file is not created until you choose **Dropped Packets > Capture > Off**. The capture filename is aspdrop.pcap. If an old capture file exists, it is overwritten.

Policy Action (Allow and Deny): These options determine whether the policy allows or denies network access. Denied traffic is dropped. If you choose **Allow** for the Policy Action, you can, optionally, choose action profile policy objects to implement acceptable use policies.

Using action profiles, you can drop certain types of traffic that is otherwise allowed.

File filtering action profile: This profile object determines the types of files that users can upload or download.

Web reputation action profile: This profile object determines which traffic is dropped, based on the web reputation of the traffic. Use the predefined system object, Default Reputation Profile, to implement the recommended policy, which drops any traffic whose web reputation score is -6 or lower.

Within each access policy in a policy set, the Source condition can contain a list of objects of these types: network group (IP addresses), identity (user or user group names), user agent (the type of client application that is making a web request), secure mobility (type of remote-access VPN client), or source object group (a collection of objects in complex AND/OR relationships that you cannot define directly in a policy). If a packet matches any selected object, then the traffic is considered to satisfy the source condition.

The destination condition can contain a list of objects of these types: network group, URL (URLs or web categories), or destination object group (a collection of objects in complex AND/OR relationships that you cannot define directly in a policy). If a packet matches any selected object, then the packet is considered to satisfy the Destination condition. If you disable the URL filtering feature or do not have a valid Web Security Essentials license, you cannot use URL objects in this field or in a destination object group.

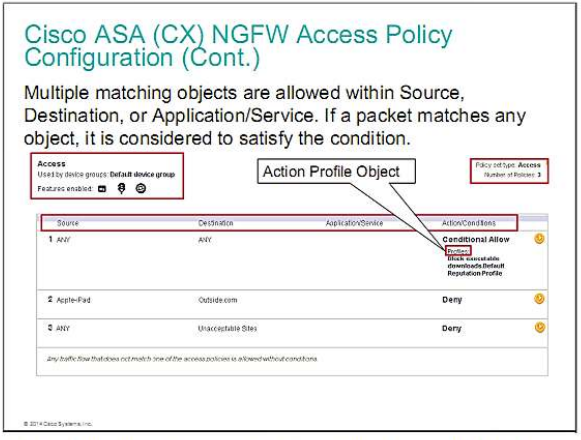
When using off-box Cisco PRSM (multiple device mode), you can also use network objects or groups that are defined on the Cisco ASA device that contains Cisco ASA (CX) NGFW as the source or destination matching criteria, or the service objects for the service matching criteria. Network group objects come in two types: those that can be used on both Cisco ASA and Cisco ASA (CX) NGFW devices, and those that can be used on Cisco ASA (CX) NGFW devices only, which is explicitly called the ASA CX network group.

The Application/Service condition can contain a list of application name, application type, application object (to identify applications or application types), service groups (protocol and port combinations), application service object (to define an application based on a combination of service and application, application type, or application object specifications), or service object.

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

Because Cisco ASA (CX) NGFW inspects the application traffic, the application for a traffic flow can be determined regardless of the port that the application uses. You can create policies that are directed to a specific application or application type by name, rather than trying to predict which ports the application will use. If a packet matches any of the selected application specifications, then the packet is considered to satisfy the application condition. If you disable the Application/Service feature or do not have a valid AVC license, you are limited to using service objects and groups.

Some applications have multiple application behaviors. For example, Facebook includes behaviors such as Post and Tag, categorized by Facebook areas or features, such as Events, General, Messages, Notes, Photos, and Places. If you specify an application type that has multiple behaviors in an access policy whose action is Allow, you gain granular control over these behaviors so that you can allow the application type in general but deny specific behaviors. For example, you can allow Facebook posting but not allow the upload of photos or message attachments. If you select an application type or an application object that specifies a type, and that type or object includes multiple behaviors, then the Set Application Behaviors control appears beneath the Application box. Each behavior is listed separately.



The example in the figure shows the access type policy set named Access, which has three defined access policies.

The Access policy set is applied to the Cisco ASA (CX) NGFW devices that belong to the Default device group.

The Features Enabled icons show which licensed features are available on Cisco ASA (CX) NGFW. Typically, the icons are black. A red background indicates a problem with the license that is required for the feature; hover over the icon to see a description of the problem. The icons represent these features: application filtering , URL filtering, and web reputation filtering.

The first access policy in the figure permits traffic from any source to any destination and uses a file filtering action profile object to block any executable file download. The policy also uses the default web reputation action profile to block websites with a web reputation score between -6 to -10.

The second access policy in the figure blocks traffic sources from devices that match the Apple-iPAD user agent object to the destinations that match the Outside.com URL object.

The third access policy in the figure blocks traffic from any source to the destinations, matching the Unacceptable Sites URL object.

The last implicit access policy in the figure allows all other traffic that has not been matched by one of the three access policies.

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

Cisco ASA (CX) NGFW Application Control Configuration

This topic describes how to configure application controls within an access policy to match the security requirements.

Cisco ASA (CX) NGFW Application Control Configuration

Cisco Adaptive Security Appliances Context Aware Next Generation Firewall can recognize supported applications on any port.

- **Application types:** Collaboration, database, email, enterprise applications, Facebook, file sharing, games, instant messaging, and so on
- **Applications:** BitTorrent, Google Calendar, Google Drive, Google Translate, iTunes, LDAP, Oracle sqlnet, Salesforce CRM, Sharepoint, Skype, WebEx, and so on
- **Application behaviors:** Some applications and application types with controllable application behaviors; for example, file sharing application types, can allow or deny Dropbox downloads, sharing, uploads, and so on.
- **Policies > Applications > I Want To > View by Application Name** or **View by Application Type**

© 2014 Cisco Systems, Inc.

Cisco ASA (CX) NGFW Application Control Configuration (Cont.)



© 2014 Cisco Systems, Inc.

The AVC engines inspect traffic to determine the application that is associated with a traffic flow. For example, the web AVC can inspect the specific application that is being carried over HTTP or HTTPS (if decryption is enabled for that traffic flow), differentiating between Facebook Games and Facebook Photos. Because there are a variety of web-based applications, the web AVC allows you to control specific web-based applications rather than forcing you to apply a blanket policy to all web traffic or to use URL filtering to control an application that is associated with a specific website. Application control gives you more granular control over web traffic than using URL filtering alone.

The broad AVC also can identity nonweb traffic, so that you can create application-based policies rather than protocol- or port-based policies. For example, you can create an application-type-based policy for email traffic that is sent over any port. The broad AVC engine allows you to create policies to control application activity on the network without needing to fully understand the underlying technology of each application.

To control traffic flows based on applications, you can create context-aware access policies that specify any combination of the following in the Application/Service field:

Application type lets you control the use of a group of related applications. For example, you might write a policy for IM applications, to treat AOL Instant Messenger, Google Talk, ICQ, and many other IM applications equally.

Application lets you control the use of a specific application; for example, Yahoo Messenger, Yahoo Mail, Flicker, and so on.

Application object lets you control a group of applications or application types that you define in an application policy object

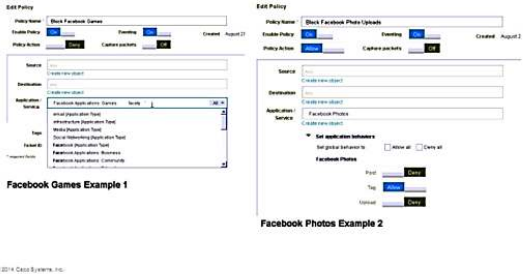
Application-Service object lets you control an application that you define based on application, application type, and traditional service group objects that specify protocol and port.

Some applications and application types have controllable application behaviors. For example, for the file sharing application type, you can allow or deny Dropbox Download, Sharing, or Upload; Google Drive Download, Editing, Sharing, or Upload; and so on.

Cisco ASA (CX) NGFW Application Control Configuration (Cont.)

The Set Application Behaviors option appears only if the overall policy action is set to Allow.

Facebook application behavior control examples:



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

The web has become the ubiquitous platform for application delivery in the enterprise, whether through browser-based application platforms such as Salesforce.com or rich media applications such as Cisco WebEx. Web protocols are a widely available transport in and out of enterprise networks. Cisco ASA (CX) NGFW includes the web AVC engine, which lets you apply deeper controls to particular applications. The web AVC engine inspects web traffic to gain a deeper understanding and control of the web traffic that is used for applications. Application control gives you more granular control over web traffic than using URL filtering alone. The web AVC engine allows you to create access policies to control application activity on the network, without needing to fully understand the underlying technology of each application. Using the web AVC engine, you can block or allow applications by application type or by a particular application. You can also apply deeper controls to particular application types. For example, you can allow IM traffic but disallow file sharing that uses IM. The web AVC engine dynamically receives updates from the Cisco Security Intelligence Operations update server, including support for new applications and application types.

If an application uses an encrypted traffic flow (SSL/TLS), you must pair an access policy for the application with a decryption policy that decrypts the traffic flow. The traffic flow must be decrypted for the application to be recognized and operated on by the access policy.

The figure shows two examples of an access policy in which the Application/Service matching criteria is used to match the Facebook application. In the Facebook Games example in the left of the figure, the Application/Service field is set to match the Facebook Gaming Applications, and the policy action is Deny.

In the Facebook Photos example in the right of the figure, the Application/Service field is set to match the Facebook Photos application. When you select an application or application type, if the applications contain any configurable behaviors, the behaviors appear beneath the Application field.

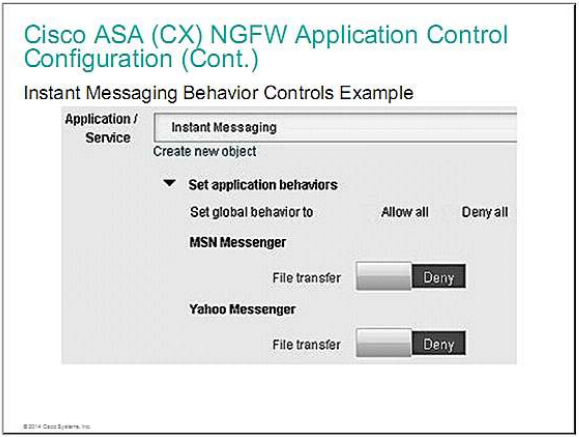
To change the settings for all behaviors at once, select **Allow All** or **Deny All** for the **Set Global Behavior To** option. For example, if your intention is to deny most behaviors but allow a few, you can select **Deny All** initially, then change the individual desired behaviors to **Allow**. The default is to **Allow All** application behaviors.

To change the setting for an individual behavior, click **Allow** or **Deny** for the desired behavior.

For example, for the Facebook Photos application, you can allow all or deny all use of Facebook photos. Or, you can specifically allow or deny posting, tagging, or uploading Facebook photos.

Note The Set Application Behaviors option appears only if the overall policy action to set to Allow.

https://t.me/learningnets



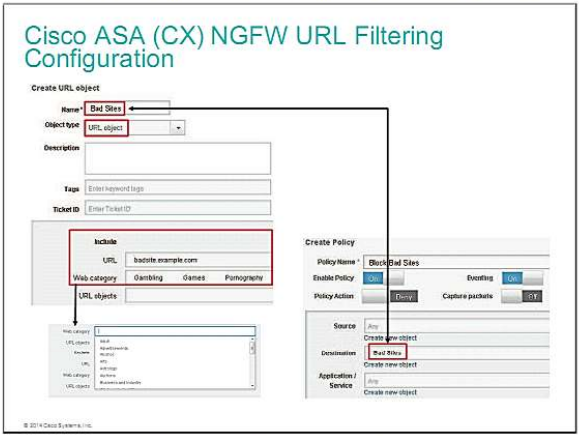
Yahoo Messenger and MSN Messenger have file transfer behaviors that can be controlled by Cisco ASA (CX) NGFW.

In the example in the figure, the Application/Service field is set to the Instant Messaging application type. Then, for more granular controls of IM usage, all file transfers over Yahoo and MSN Messenger are denied.

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

Cisco ASA (CX) NGFW URL Filtering Configuration

This topic describes how to configure URL filtering within an access policy to match security requirements.



URL filtering can be used to define an acceptable web usage policy within an access policy. You can filter on broad web categories, such as Gambling, so that you do not need to identify every individual website that should be blocked. The Cisco URL database categorizes more than 20 million websites worldwide in more than 60 languages and is automatically updated every 5 minutes. A Web Security Essentials license is required to use the web category-based URL filtering.

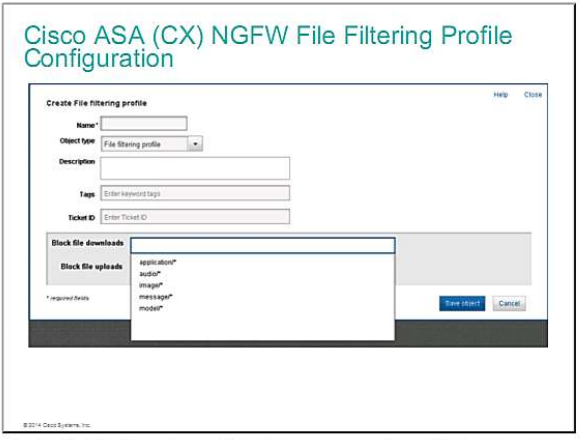
The bottom right in the figure shows an access policy that denies access from any source to any gambling, games, or pornography type websites. For example, the policy denies access to the badsite.example.com website by matching a URL object named Bad Sites in the Destination field of the access policy.

The top left in the figure shows the URL object for matching the badsite.example.com URL or the gambling, games, or pornography web category.

https://t.me/learningnets

Cisco ASA (CX) NGFW File Filtering Profile Configuration

This topic describes how to configure a file filtering profile and apply it to an access policy, to match security requirements.



When defining the file filtering action profile within an access policy, click the **Create New Profile** link to create the file filtering action profile object inline during access-policy creation.

From the Create File filtering profile screen, configure the name of the file filtering profile object. Choose the File filtering profile object type, enter a description, tags, and ticket ID for the file filtering profile object, and choose the type of files to block from download and upload.

Choose the MIME type of files that users should be prevented from downloading from destination sites. The default is to allow all file downloads.

Choose the MIME type of files that users should be prevented from uploading to destination sites. The default is to allow all file uploads.

Use the asterisk (*) as a wildcard to indicate zero or more characters. Use */* to indicate all files.

The main types of files are available in the drop-down list, but you can also specify subtypes such as audio/mp4.

When specifying a MIME type in this object, you can target an entire MIME type or a specific type or subtype:

application/*: Discrete data that does not fit into the other categories and that is typically processed by some type of application program before it is viewable or usable. The application category can include languages for computational material, which opens potential security holes if the transferred code is malware. Examples include application/pdf, application/javascript, and application/postscript. There are a large number of vendor-specific subtypes.

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

audio/*: Audio files, such as audio/mp4 and audio/mpeg. If the file includes motion pictures, the type is video/* instead of audio/*.

image/*: Image or graphic files, such as image/gif and image/jpeg.

message/*: Encapsulated email messages, such as message/http and message/sip.

multipart/*: Archives or other files that are composed of more than one object, such as multipart/mixed.

model/*: 3D model files, such as model/vrml and model/x3d+binary.

text/*: Textual files, including plain and rich text, such as text/csv, text/html, and text/rtf.

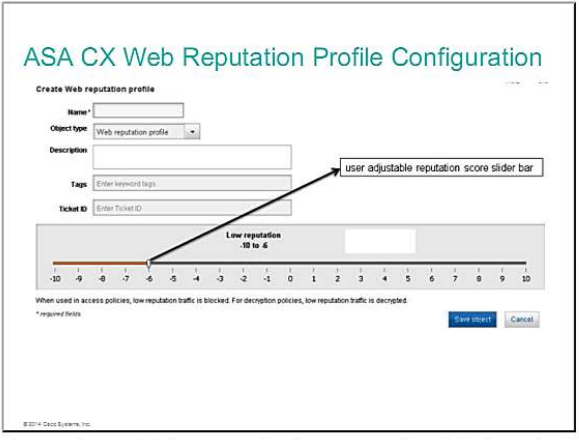
video/*: Video files, such as video/mp4 and video/mpeg. This media type can contain synchronized audio; for example, video/mpeg for a typical MPEG video file that includes motion pictures and sound.

File filtering profiles do not apply to non-HTTP traffic. Cisco Adaptive Security Appliances Context Aware Next Generation Firewall can match HTTP traffic over any port.

https://t.me/learningnets

Cisco ASA (CX) NGFW Web Reputation Profile Configuration

This topic describes how to configure a web reputation profile and apply it to an access policy to match the security requirements.



Web reputation score is a statistical assessment based on context and past behavior and combines many factors of varying significance into one correlated metric. Web reputation score can range from -10 to +10. Following is a general guideline to the scores:

-10 to -6: Sites in the lowest reputation zone are dedicated or hijacked sites that persistently distribute key loggers, rootkits, and other malware. Also included are phishing sites, bots, and drive-by installers. Sites in this reputation range are almost guaranteed to be malicious. The predefined web reputation profile, Default Reputation Profile, defines this zone as the low reputation zone.

-6 to -3: Sites in this zone tend to be aggressive ad syndication and user tracking networks. These sites are suspected of being malicious, but maliciousness has not been confirmed.

-3 to 3: Sites in this zone tend to be well managed, responsible content syndication networks and user generated content sites.

0 to 5: Sites in this zone have some history of responsible behavior or third party validation.

5 to 10: Sites in this zone have a long history of responsible behavior, have significant traffic volume, and are widely accessed.

When using the the Web reputation action profile in access policies, any traffic to the low reputation web sites will be blocked.

When using the the Web reputation action profile in decryption policies, any traffic to the low reputation web sites will be decrypted.

You can click the **Create New Profile** link to create a new web reputation action profile object inline during the access or decryption policy creation.

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

From the Create Web Reputation Action Profile screen, configure the name of the web reputation action profile object, Web reputation profile is the Object type; enter a Description, Tags, and Ticket ID for the web reputation profile object, and adjust the reputation score slider bar to determine which reputation score range is considered a low reputation.

Web reputation profiles do not apply to non-HTTP traffic. Cisco Adaptive Security Appliances Context Aware Next Generation Firewallcan match HTTP traffic over any ports.

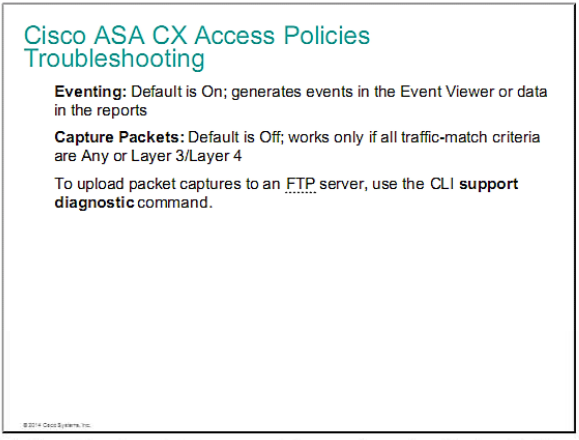
Note To look up the reputation of a site, you can use the tool at:

http://www.senderbase.org/home

https://t.me/learningnets

Cisco ASA (CX) NGFW Access Policies Troubleshooting

This topic explains how to troubleshoot Cisco Adaptive Security Appliances Context Aware access policies.



Some tools in Cisco Prime Security Manager can help to monitor and troubleshoot the Cisco ASA CX access-policy operations:

Eventing (On or Off): This setting determine whether to generate events for the policy. You must enable eventing for traffic flows that match the policy to generate events in Event Viewer or data in reports. Eventing is on by default.

Capture Packets (On or Off): This setting determines whether to capture packets that match this policy. All packets are captured, whether allowed or denied. This setting works only if all traffic match criteria are Any or are Layer 3/Layer 4 criteria only; that is, network and service type objects only. The setting is off by default.

When you turn Capture Packets on, all packets are captured, so carefully consider traffic volumes for matching flows before enabling this setting. Packets are not captured for access policies that use matching criteria other than Layer3/Layer 4 criteria, even if you enable the setting on the access policy.

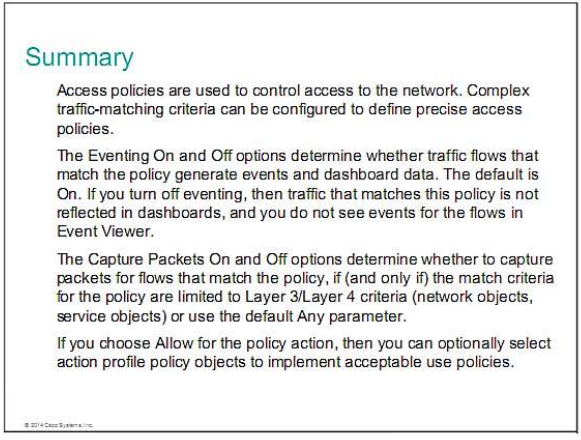
The capture file uses the policy name as the filename, with the extension .pcap. To upload packet captures to an FTP server, use the Cisco ASA CX **support diagnostic** CLI command.

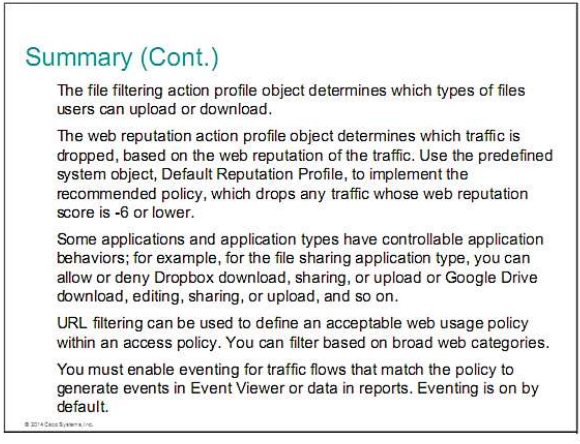
Refer to the User Guide for ASA CX and Cisco Prime Security Manager for more detailed information about **support diagnostic** command operations.

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

Summary

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





References

For additional information, refer to these resources:

Cisco Systems, Inc. *Cisco ASA Series Firewall CLI Configuration Guide, 9.1.* http://www.cisco.com/en/US/docs/security/asa/asa91/configuration/firewall/asa_91_firewall_config.html

Cisco Systems, Inc. *Cisco ASA Series Firewall ADSM Configuration Guide, 7.1.* http://www.cisco.com/en/US/docs/security/asa/asa91/asdm71/firewall/asdm_71_firewall_config.html

Cisco Systems, Inc. *User Guide for ASA CX and Cisco Prime Security Manager 9.1.* http://www.cisco.com/en/US/docs/security/asacx/9.1/user/guide/b_User_Guide_for_ASA_CX_and_PRSM_9_1.pdf

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

Lesson 6

Configuring Cisco ASA (CX) NGFW Identity Policies

Overview

This lesson describes how to configure Cisco Adaptive Security Appliances Context Aware Next Generation Firewall identity policies. Identity policies determine whether a user must be authenticated and, if so, how the user should be authenticated. The purpose of authentication is to determine which user is involved in a traffic flow so that identity-based access or decryption policies can be applied to traffic flows.

Upon completing this lesson, you will be able to meet these objectives:

- Explain the differences between Cisco ASA (CX) NGFW active and passive authentication methods
- Explain the functions of Cisco ASA (CX) NGFW authentication realms
- Explain the important features of the Cisco ASA (CX) NGFW ADI
- List the steps to configure the Cisco ASA (CX) NGFW identity policies
- Describe how to configure an LDAP authentication realm and LDAP directory servers
- Describe how to configure an Active Directory authentication realm and Active Directory directory servers
- Describe how to configure Cisco CDA to integrate with Cisco ASA (CX) NGFW
- Describe how to configure Cisco ASA (CX) NGFW identity policies that use active authentication to match security requirements
- Describe how to configure Cisco ASA (CX) NGFW identity policies using passive authentication to match security requirements
- Describe how to configure Cisco ASA (CX) NGFW authentication settings
- Describe how to configure Cisco ASA (CX) NGFW access and decryption policies that use identity objects

https://t.me/learningnets

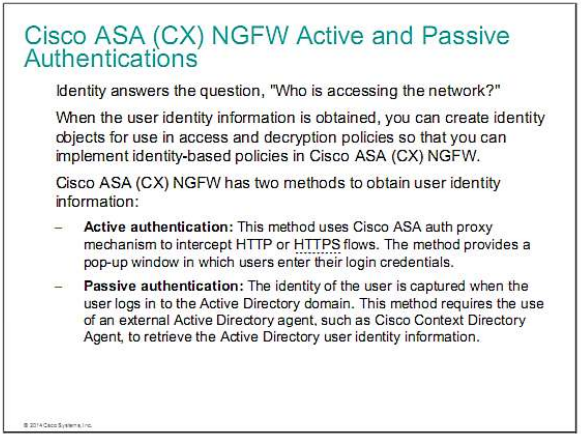
Describe how to verify the user identity by using the Cisco PRSM Event Viewer

Troubleshoot Cisco ASA (CX) NGFW identity policies

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

Cisco ASA (CX) NGFW Active and Passive Authentications

This topic explains the differences between the Cisco Adaptive Security Appliances Context Aware Next Generation Firewall active and passive authentication methods.



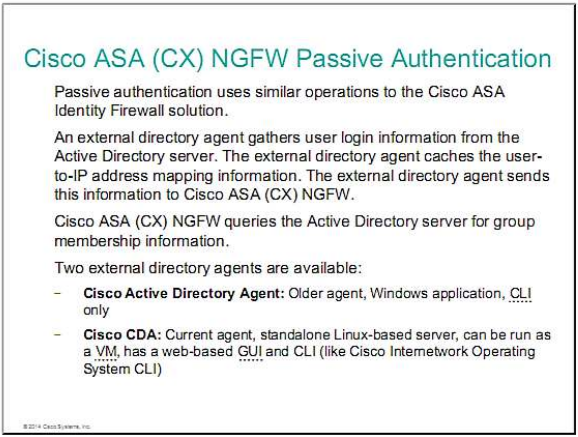
Identity policies determine whether a user must be authenticated and if so, how the user should be authenticated. The purpose of authentication is to determine which user is involved in a traffic flow, so identity-based access or decryption policies can be applied to traffic flows.

To see user-based information in the Cisco Prime Security Manager dashboards, or to implement user-based access or decryption policies, the identity of the user that is associated with a traffic flow must be known. This need requires the user to provide identification when connecting to the network. There are two options for authenticating and identifying the users.

Active authentication: Cisco ASA (CX) NGFW redirects user HTTP or HTTPS traffic to Cisco ASA, which prompts the user to enter a username and password. Active authentication occurs only when the user attempts an HTTP or HTTPS connection. Active Authentication supports Microsoft Active Directory, Open LDAP, and other LDAP servers. The active authentication prompt includes the name of the directory realm and the Cisco ASA IP address. When using Active Directory, users must also enter the domain name in front of the username, using the DOMAIN\username format. When using LDAP, users do not need to enter the domain name in the front of the username.

Passive authentication: The identity of the user is captured when the user logs in to the Active Directory domain. This method requires using an external Active Directory agent, such as Cisco CDA, to retrieve the Active Directory user-identity information. Cisco ASA can also provide VPN user-identity information to Cisco ASA (CX) NGFW. However, VPN user information is not used in Cisco ASA (CX) NGFW policies. Only Active Directory user information can be used as matching criteria in the access or decryption policies in Cisco ASA (CX) NGFW Software Release 9.1.1.

https://t.me/learningnets

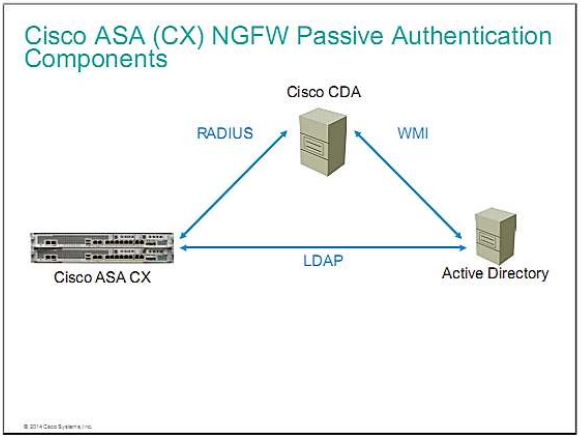


With passive authentication, a mapping between the user name and IP address of the user workstation is obtained when the user logs in to the Active Directory domain. Cisco CDA collects the mapping and then sends it to Cisco ASA (CX) NGFW. Cisco ASA (CX) NGFW obtains Active Directory user group membership information directly from the Active Directory or LDAP server.

Passive authentication functions similarly to the Cisco ASA Identity Firewall solution.

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

Cisco ASA (CX) NGFW Passive Authentication Components



The figure shows the components that are required to implement passive authentication.

Cisco ASA (CX) NGFW performs these actions:

Downloads the Active Directory user groups and group membership information from the Active Directory domain controller, by using the LDAP protocol, every 24 hours by default.

Receives the IP-to-user address mapping information from Cisco CDA, by using the RADIUS protocol. Cisco ASA (CX) NGFW supports only full-download mode, in which Cisco ASA (CX) NGFW downloads the complete IP address-to-user mapping database from Cisco CDA when Cisco ASA (CX) NGFW first boots, and then receives incremental mapping information from Cisco CDA.

The Cisco CDA performs these actions:

Monitors the Active Directory Domain Controller security log events via WMI.

Sends the IP-to-user address mappings information to Cisco ASA via RADIUS.

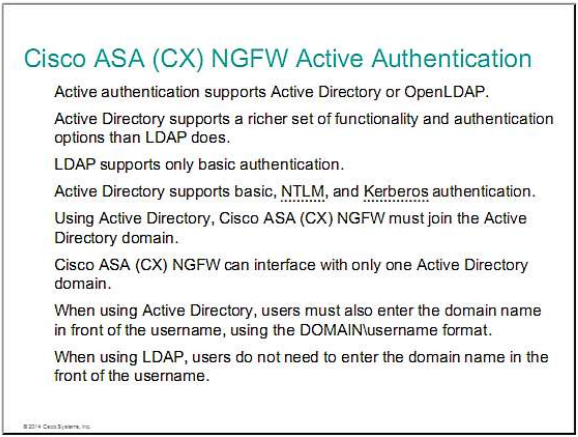
Cisco CDA is based on Linux CentOS and runs the Cisco Application Deployment Engine operating system. Cisco CDA can be installed on a hardware server or as a VM image.

Cisco CDA has a web-based GUI and a CLI. The CLI is used for the basic network setup configurations. The web-based GUI is used for Cisco CDA system configurations.

The Active Directory domain controller performs these actions:

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.

The Active Directory domain controller authenticates Windows users in the domain, generates user login security log events, and replies to the Cisco ASA (CX) NGFW LDAP query for Active Directory user group information.



Active authentication supports two types of directory server: Active Directory and OpenLDAP.

Active authentication supports only basic authentication for LDAP. With basic authentication, a Cisco ASA (CX) NGFW pop-up login window appears on the user browser and the user must enter a username and password.

Active authentication supports basic authentication, NTLM, and Kerberos authentication for Active Directory. NTLM is an older challenge-and-response-based authentication method. Kerberos is a ticket-based authentication method and is considered more secure than NTLM.

When using Active Directory, users must also enter the domain name in front of the username, using the DOMAIN\username format. When using LDAP, users do not need to enter the domain name in the front of the username.

When using Active Directory with active authentication, Cisco ASA (CX) NGFW must also join the Active Directory domain. Cisco ASA (CX) NGFW can be a member of only one Active Directory domain.

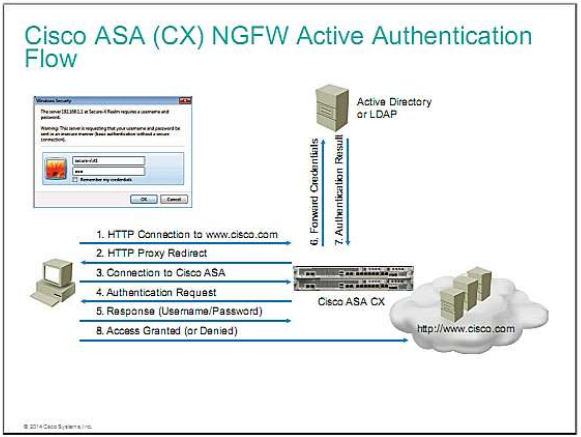
When using LDAP with active authentication, multiple LDAP realms are permitted.

The supported Active Directory versions are those in Windows Server 2008 R2 and Windows Server 2003 R2.

The supported OpenLDAP version is 2.4.21 or later.

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

Cisco ASA (CX) NGFW Active Authentication Flow



Unlike passive authentication, active authentication does not require the use of an external Active Directory agent. Active authentication requires the user to initiate an HTTP or HTTPS connection to trigger the authentication process.

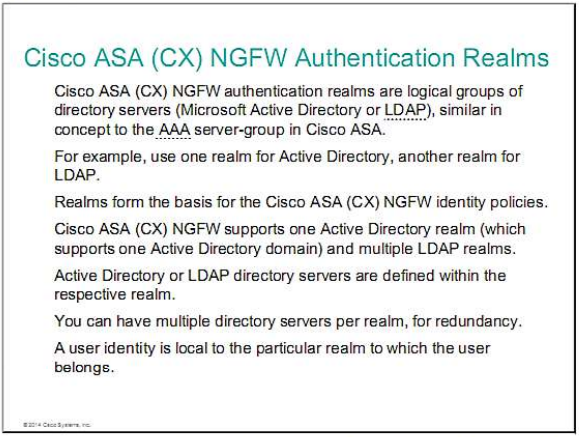
The figure illustrates the active authentication process flow when using basic authentication:

1. The user attempts to reach a remote web site by using the web browser.
2. Cisco ASA (CX) NGFW sees the HTTP or HTTPS request from the user to a remote web site and redirects the user browser to the Cisco ASA interface IP address on the auth-proxy TCP port 885 (by default). The redirect is accomplished by sending a Proxy Redirect to the user browser (HTTP return code 307 – Temporary Redirect).
3. The user browser connects to the Cisco ASA interface IP address on the auth-proxy TCP port 885.
4. Cisco ASA (CX) NGFW sends an authentication request and presents a pop-up window on the user browser (HTTP return code 401 - Unauthorized).
5. The user enters a username and password. When using Active Directory, users must also enter the domain name in front of the username, using the DOMAIN\username format (as shown in the figure). When using LDAP, users do not need to enter the domain name in the front of the username.
6. After Cisco ASA (CX) NGFW successfully authenticates the user against the directory server, Cisco ASA redirects the user browser back to the remote web site (HTTP return code 307).

When using NTLM or Kerberos with Active Directory, certain web browsers can be configured to transparently respond to the active authentication requests so that the user is unaware that any authentication challenge was made or satisfied. The web browsers take advantage of the fact that users are already logged in to the Active Directory domain. The web browser tries to use the Active Directory domain login to transparently respond to the active authentication requests. You must configure the client web browser to support integrated Windows authentication to enable transparent authentication. Refer to the Cisco ASA (CX) NGFW and PRSM User Guide for more information.

Cisco ASA (CX) NGFW Authentication Realms

This topic explains Cisco Adaptive Security Appliances Context Aware Next Generation Firewall authentication realms.



The figure describes some Cisco ASA (CX) NGFW terminologies that are used when implementing identity policies on Cisco ASA (CX) NGFW.

Within Cisco ASA (CX) NGFW, a realm is a logical group of a common type of directory servers, similar to a AAA server-group in Cisco ASA. For example, you define one realm in Cisco ASA (CX) NGFW for Active Directory servers and another realm for LDAP servers.

Cisco ASA (CX) NGFW supports only one Active Directory realm but can support multiple LDAP realms.

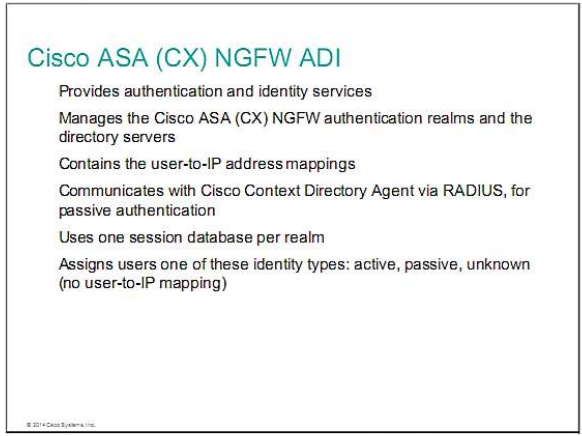
The directory servers (Active Directory servers and LDAP servers) are defined within the respective realm in Cisco ASA (CX) NGFW. Multiple directory servers can be defined per realm, for redundancy.

Cisco ASA (CX) NGFW recognizes a specific user identity local to the particular realm with which the user is associated.

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

Cisco ASA (CX) NGFW ADI

This topic explains the key features of the Cisco Adaptive Security Appliances Context Aware Next Generation Firewall ADI.



The ADI is the Cisco ASA (CX) NGFW process that provides the authentication and identity services. The ADI manages the realms and directory servers and contains the user-to-IP address mappings. ADI also communicates with Cisco CDA to support passive authentication. One ADI session per realm is configured in Cisco ASA (CX) NGFW.

From the Cisco ASA (CX) NGFW CLI, the admin user can use the **show opdata adisessions** command to display the ADI session directory.

From the Cisco ASA (CX) NGFW CLI, the admin user can use the **clear opdata adisessions** command to clear the ADI session directory. This action clears all the user-to-IP address mappings.

This output from the Cisco ASA (CX) NGFW CLI shows three examples of the **show opdata adisessions** output. The first sample shows the admin user being authenticated by using active authentication. The second sample shows the admin user being authenticated by using passive authentication. The third sample shows that the user authentication has failed; in this case, in the ADI session directory, the username is ANONYMOUS.

```
asa-cx> show opdata adisessions
Vdi Session Directory:
==========================
total_sessions: 1
contained_op_data {
  realm: "hospital"
  username: "administrator"
  ip: "10.0.70.10"
  identity_type: IDENTITY_ACTIVE
  auth_type: AUTH_TYPE_BASIC
}
Press Enter to continue, 'CTRL + C' to exit
```

```
asa-cx> show opdata adisessions
Vdi Session Directory:
============================
total_sessions: 1
contained_op_data {
  realm: "hospital"
  username: "administrator"
  ip: "172.16.1.71"
  identity_type: IDENTITY_PASSIVE
  auth_type: AUTH_TYPE_NEGOTIATE
}
Press Enter to continue, 'CTRL + C' to exit

asa-cx> show opdata adisessions
Vdi Session Directory:
============================
total_sessions: 1
contained_op_data {
  realm: "hospital"
  username: "ANONYMOUS"
  ip: "10.0.70.20"
  identity_type: IDENTITY_FAILED_AUTH
  auth_type: AUTH_TYPE_BASIC
}
Press Enter to continue, 'CTRL + C' to exit
```

Based on how the user-to-IP address mapping is obtained or not obtained, one of these user identity types is displayed in Cisco Prime Security Manager (such as in the Event Viewer):

Active: Cisco ASA (CX) NGFW directly authenticated the user. Active authentication is applied to HTTP or HTTPS traffic only. If any other type of traffic matches an identity policy that requires or allows active authentication, then active authentication is not attempted.

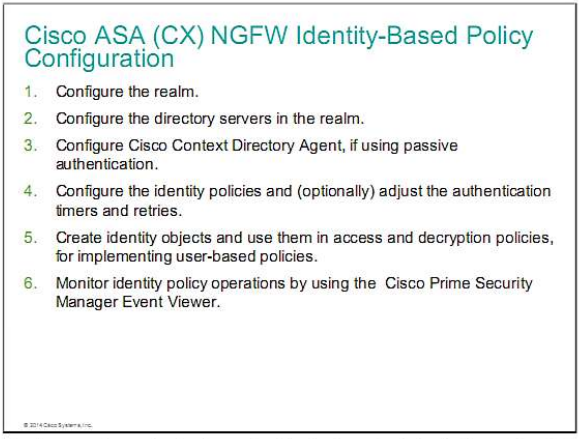
Passive: A user-to-IP address mapping was received from Cisco CDA. This type of identity can be available regardless of the types of traffic that the user sends.

Unknown: There is no user-to-IP mapping; for example, the user tried to actively authenticate to the Cisco ASA (CX) NGFW device, but authentication failed. Unknown users are also those users who simply do not have a mapping because they were not required to authenticate. Unknown users are represented by their IP address in the Cisco PRSM user dashboard and are represented as the ANONYMOUS user in the ADI session directory.

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

Cisco ASA (CX) NGFW Identity-Based Policy Configuration

This topic lists the steps to configure a Cisco Adaptive Security Appliances Context Aware Next Generation Firewall identity policy.



The figure list the general steps for implementing identity-based policies in Cisco ASA (CX) NGFW.

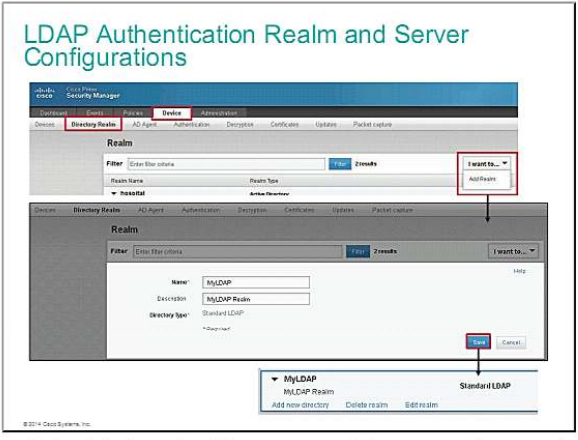
1. Configure the realm within Cisco ASA (CX) NGFW. A realm is a logical grouping of directory servers of the same type.
2. Configure the directory servers in the realm. The directory servers (Active Directory servers and LDAP servers) are defined within their respective realm in Cisco ASA (CX) NGFW. Multiple directory servers can be defined per realm, for redundancy.
3. Configure Cisco CDA as the Active Directory agent, if using passive authentication.
4. Configure the identity policies and (optionally) adjust the authentication timers and retries settings.
5. Create identity objects, to be used in the access and decryption policies for implementing user-based access and decryption policies.
6. Use the Cisco PRSM Event Viewer to monitor the identity policy operations.

Cisco ASA (CX) NGFW supports only one Active Directory realm but can support multiple LDAP realms.

There is currently not a hard-coded limit related to the number of LDAP realms.

LDAP Authentication Realm and Server Configurations

This topic describes how to configure an LDAP authentication realm and how to add an LDAP server to the realm.



A directory realm is a logical grouping of directory servers of the same type. Directory realms are similar to AAA server groups on Cisco Adaptive Security Appliances.

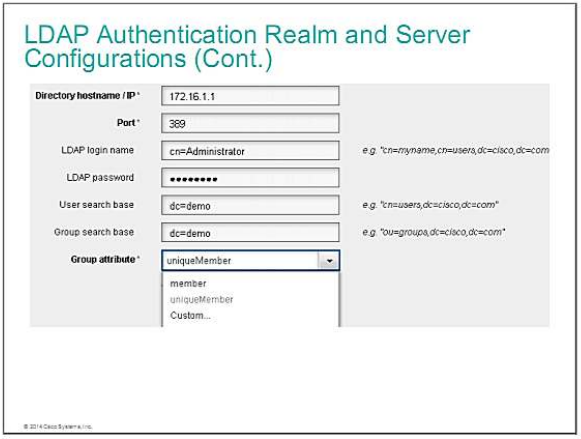
To create a new realm, follow these steps:

1. Go to the Cisco Prime Security Manager **Device > Directory Realm** screen and choose **I Want To > Add Realm**.
2. Enter the name and a description for the realm.
3. Choose the directory type: Standard LDAP or Active Directory.
   - The figure shows an example of adding a realm for the Standard LDAP directory type.
   - When adding a realm for the Active Directory directory type, more configuration information is required for Cisco Adaptive Security Appliances Context Aware Next Generation Firewall to join the Active Directory domain (not shown in the figure).

To add or edit a directory server in the realm, do one of the following:

1. To add a directory server, hover over the realm name and click **Add New Directory**.
2. To edit an existing directory server in a realm, hover over the server name under the realm and click **Edit Directory** (not shown in the figure).
3. To delete an existing directory server in a realm, hover over the server name under the realm and click **Delete Directory** (not shown in the figure).

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



The figure shows the information that is required when adding an LDAP server to a realm:

The LDAP server hostname or IP address.

The TCP port number that is used to communication with the LDAP server. Port 389 is the only supported port and uses standard LDAP (plain text) connections.

The LDAP login name and password. Administrator privileges are not required for the user. The LDAP login name represents a user record in the LDAP server that the administrator uses for binding with the LDAP server. If you do not specify a login name, the system attempts an anonymous bind to LDAP, for querying user and group information.

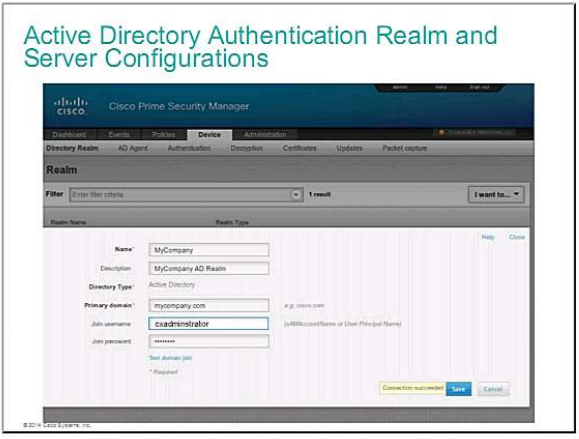
The user and group search base. The field defines the location in the LDAP hierarchy for searching or querying user or group information. If you do not specify a user search base, the system creates a generic base consisting of the entire domain components of the directory name.

The group membership attribute, which is the LDAP attribute that lists all the users that belong to a group. A member is the typical group attribute for Active Directory. A uniqueMember is the typical group attribute for OpenLDAP. The Custom option is used if you created a custom group attribute in the LDAP directory; enter the attribute value in the field that is provided.

Test Connection Link tests whether the entered LDAP server properties can successfully connect to the LDAP server.

Active Directory Authentication Realm and Server Configurations

This topic describes how to configure an Active Directory authentication realm and how to add an Active Directory server to the realm.

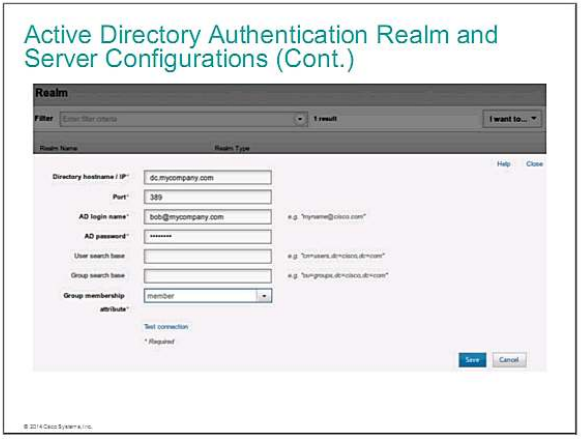


The figure shows the additional information that is required when configuring a realm that uses the Active Directory directory type:

- The FQDN for the Active Directory that Cisco Adaptive Security Appliances Context Aware Next Generation Firewall should join.
- The Active Directory sAMAccountName or User Principal Name to use when Cisco ASA (CX) NGFW joins or leaves the Active Directory domain. These credentials must have the authority within Active Directory to join devices to the domain or to leave the domain.

Use the **Test Domain Join** link to verify that the Cisco ASA (CX) NGFW can join the Active Directory domain.

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



The figure shows the information that is required to add an Active Directory server to a realm:

The Active Directory server hostname or IP address.

The TCP port number that is used to communication with the Active Directory server. Port 389 is the only supported port and uses standard plain text connections.

The Active Directory login name and password. This is the user name that is used for authenticated binding with the Active Directory server. The user privilege requirements differ based on the type of authentication that you will allow in your identity policies.

Ensure that you specify a user that has the required privileges:

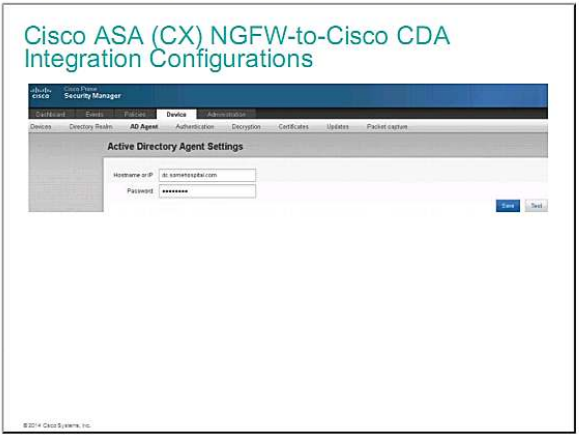
- **NTLM:** Any valid user account should work.
- **Basic:** Any valid user account should work.
- **Kerberos:** The user account must have the "Validated Write to Service Principle Name" permission.

The user and group search base field defines the location in the Active Directory hierarchy for searching or querying user or group information. If you do not specify a user search base, the system creates a generic one consisting of the entire domain components of the directory name.

The group attribute is the LDAP attribute that lists all users that belong to a group. The member is the typical group attribute for Active Directory. The uniqueMember is the typical group attribute for OpenLDAP. The Custom option is used when you create a custom group attribute in the LDAP directory; enter the attribute value in the provided field.

Cisco ASA (CX) NGFW-to-Cisco CDA Integration Configurations

This topic describes how to configure Cisco Context Directory Agent as the Active Directory agent.



Cisco CDA is used as the Active Directory agent, to support passive authentication operations.

To configure Cisco CDA, from Cisco Prime Security Manager, choose **Device > AD Agent**.

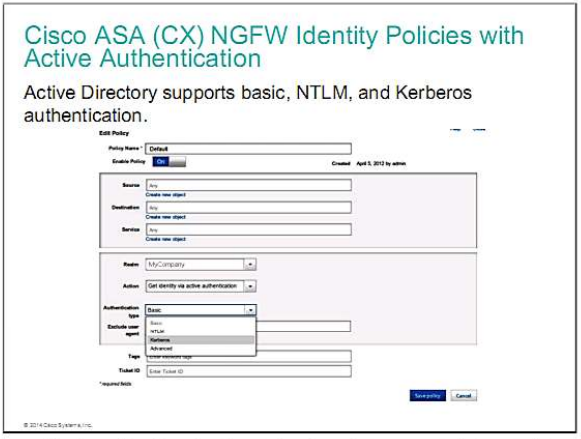
Enter the hostname or IP address of Cisco CDA and the shared secret between Cisco CDA and Cisco Adaptive Security Appliances Context Aware Next Generation Firewall.

Click the **Test** button to test the communications between the Cisco ASA (CX) NGFW and Cisco CDA.

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

Cisco ASA (CX) NGFW Identity Policies with Active Authentication

This topic describes how to configure Cisco Adaptive Security Appliances Context Aware Next Generation Firewall identity policies, by using active authentication to match security requirements.



To configure an identity policy, from the Cisco Prime Security Manager **Policies > Policies** window, under the desired identity policy set, click **Add New Policy**.

This configuration information is required within an identity policy:

Policy Name: Enter the identity policy name.

Enable Policy: Choose **On** or **Off**.

The traffic-matching criteria for matching the user traffic that will require authentication follows:

- **Source:** Choose network object, network group, ASA CX network group, or **Any**. In the figure, **Any** is chosen, to match any source.
- **Destination:** Choose network object, network group, ASA CX network group, or **Any**. In the figure, **Any** is chosen, to match any destination.
- **Service:** Choose service object, service group, or **Any**. In the figure, **Any** is chosen, to match any service

Realm: You must specify a realm within the identity policy. In the figure, the realm **MyCompany** is used.

Action: Choose an identity policy action:

- Get identity using Active Directory agent.
- If passive authentication fails, require active authentication? [Yes/No]
- Get identity via active authentication. (In the figure, this action is chosen, to enable active authentication.)

- Do Not Require Authentication.

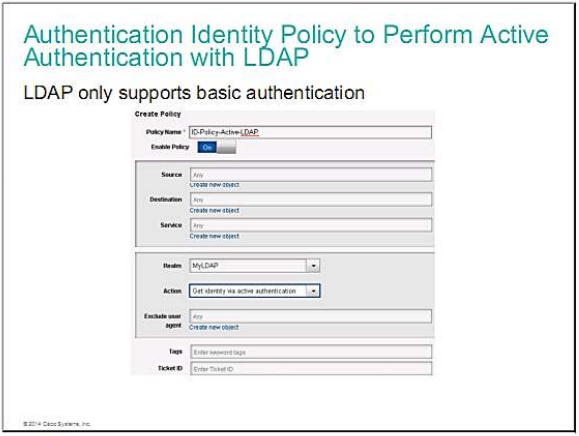
Authentication Type (Active Directory only): Choose **Basic**, **NTLM**, **Kerberos**, or **Advanced**. (In the figure, **Basic** is selected.) Choose the Advanced option to allow Cisco ASA (CX) NGFW to negotiate the method with the Active Directory server. Negotiation results in the use of the strongest commonly supported method: in order, Kerberos, NTLM, and then basic.

Exclude User Agent: If active authentication is used within an identity policy, you can exclude certain user agents that cannot respond to authentication requests. Choose the user agent policy objects that identify the user agents that you do not want to be prompted for active authentication.

Tags: Enter the tags for the identity object.

Ticket ID: Enter the ticket ID for the identity object.

Authentication Identity Policy to Perform Active Authentication with LDAP

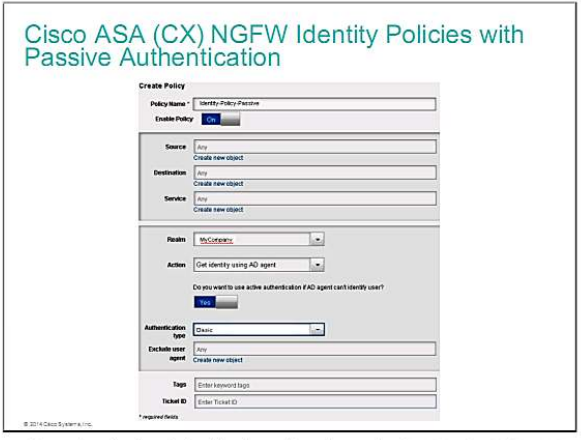


The figure shows the configuration information that is required within an identity policy when using a realm for the standard LDAP directory type. The difference between LDAP and Active Directory is that LDAP supports only basic authentication. Therefore, there is no additional drop-down selection for Authentication Type.

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

Cisco ASA (CX) NGFW Identity Policies with Passive Authentication

This topic describes how to configure Cisco Adaptive Security Appliances Context Aware Next Generation Firewall identity policies that use passive authentication to match security requirements.



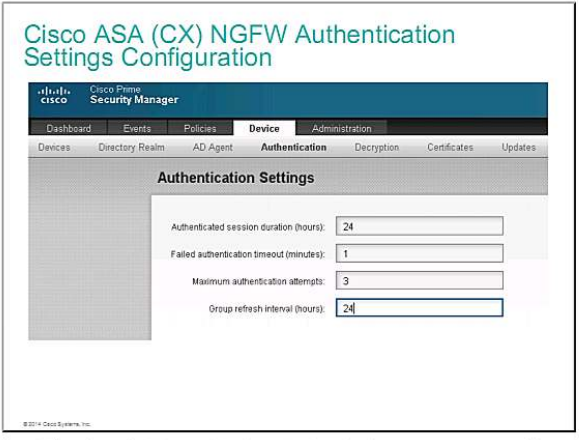
To enable passive authentication, in the identity policy, choose the **Get Identity Using AD Agent** action.

When you choose this action, then by default, active authentication is used as the fallback method if Cisco Context Directory Agent does not contain the user-to-IP address mapping for a user. If you choose No, and a passive mapping from Cisco CDA is unavailable, then the user IP address will not be associated with a username, and the user identity-based access or decryption policies will not be applied to that user traffic.

https://t.me/learningnets

Cisco ASA (CX) NGFW Authentication Settings Configuration

This topic describes how to configure the Cisco Adaptive Security Appliances Context Aware Next Generation Firewall authentication settings.



From the Cisco Prime Security Manager **Device > Authentication** page, you can configure the various authentication settings.

The figure shows all the default settings:

Authenticated Session Duration: The number of hours for which a user-to-IP address mapping is maintained. When a mapping reaches this age, it is deleted, and a new mapping is obtained, based on your identity policy settings.

Failed Authentication Timeout: If a user fails to correctly authenticate during active authentication and exceeds the maximum authentication attempts, the IP address for the user is considered to have failed authentication. This timeout value determines the length of time, in minutes, before the user at that IP address is again prompted to authenticate. During this time, all traffic from the IP address is evaluated based on the IP address alone, and no user- or user group-based policies are applied to the traffic. Thus, during this failed timeout period, a user might be prevented from accessing resources for which the user would be allowed with successful authentication.

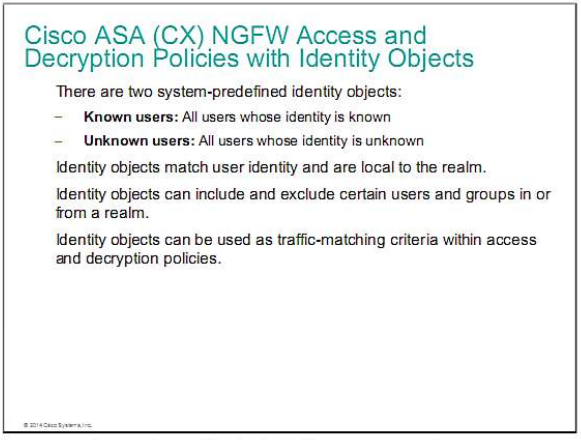
Maximum Authentication Attempts: The number of times a user can retry authentication when prompted to authenticate by Cisco ASA (CX) NGFW. The number of attempts is reset when the user successfully authenticates. If the user fails to authenticate, the user is not prompted again for authentication until the failed authentication timeout is exceeded.

Group Refresh Interval: How often user group membership is updated from the directory servers, in hours. If you add a user to a group, the user is not recognized as being a member of the group until the next update. Membership for a group is obtained only if you use the group in a policy. The default is every 24 hours.

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

Cisco ASA (CX) NGFW Access and Decryption Policies with Identity Objects

This topic describes how to configure the Cisco Adaptive Security Appliances Context Aware Next Generation Firewall access and decryption policies, using identity objects.



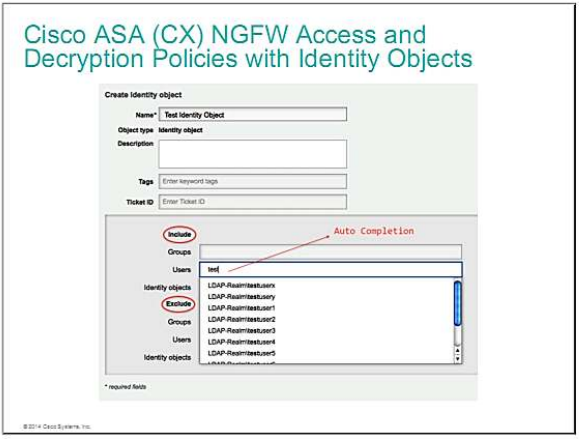
Identity objects are used to match user identity, including usernames and user group names.

There are two system-predefined identity objects: known users and unknown users. Known users match any user for whom identity is available, either because the user actively authenticated or because there is a passive mapping for the user IP address that Cisco Context Directory Agent obtained. Unknown users match users that do not match the known users object; in other words, IP addresses for which a user mapping is unavailable.

Like other object types, identity objects can have an include and exclude list. For example, an identity object can include an Active Directory group for a specific Active Directory realm but exclude a specific user within that Active Directory group.

Identity objects can be used as traffic-matching criteria in the access or decryption policies.

To add a new identity object from Cisco Prime Security Manager, choose **Policies > Objects > I Want To > Add Identity Object**.



The figure shows the Cisco PRSM Create Identity Object page, which you can use to add a new identity object:

Name: Enter the name of the identity object.

Object Type: This field displays Identity Object.

Description: Enter a description of the identity object.

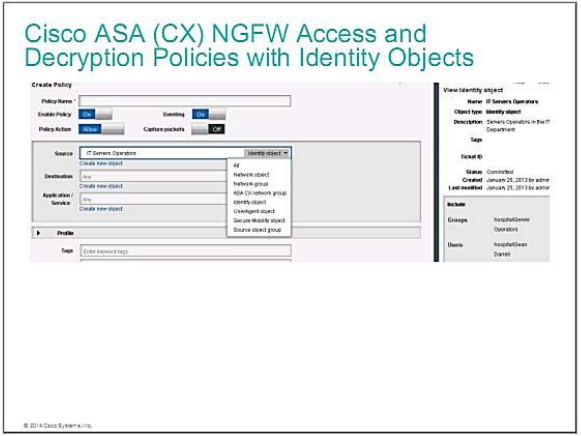
Tags: Enter the tags for the identity object.

Ticket ID: Enter the ticket ID for the identity object.

Include and Exclude: The identity object can have an include and exclude list to include or exclude groups, users, and other identity objects. As you enter a user or group name, queries are made to help automatically complete your entry. The list of matching user or group names is retrieved from the directory servers that are configured for the defined realms. Choose a name from the retrieved list. You must define a realm before you can create identity objects. User and group names are not case-sensitive but must include the realm name, in the format Realm\group_name or Realm\user_name.

In the example in the figure, the identity object is named Test Identity Object. When the user name "test" is entered in the Include > Users field, a list of usernames that start with "test" is shown in the drop-down box. In this case, all the usernames that start with "test" belong to the realm LDAP-Realm in Cisco ASA (CX) NGFW.

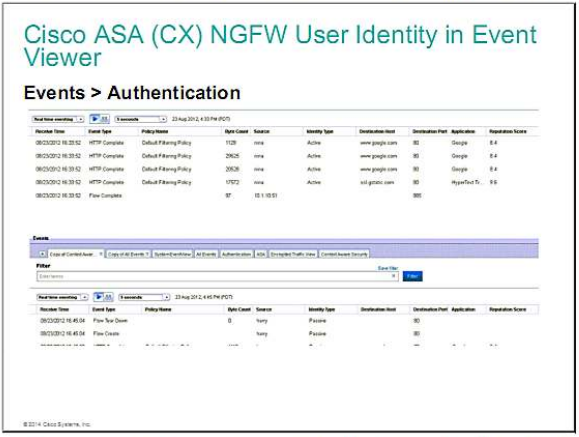
© 2014 Cisco Systems, Inc.
https://t.me/learningnets



The example in this figure shows the IT Servers Operators identity object being used as the source matching criteria in an access policy. By hovering over the IT Servers Operators object name, you can see more information about the object (shown on the right in the figure). In this example, the IT Servers Operators identity object includes the hospital\Server Operators group and the hospital\Sean Darrell user.

Cisco ASA (CX) NGFW User Identity in Event Viewer

This topic describes how to verify the user identity in the Cisco Prime Security Manager Event Viewer.



The figure shows a few sample images of the Cisco PRSM Event Viewer (**Events > Authentication**).

In the examples in the figure, after successful user authentication, the user name (instead of the IP address) is displayed as the source.

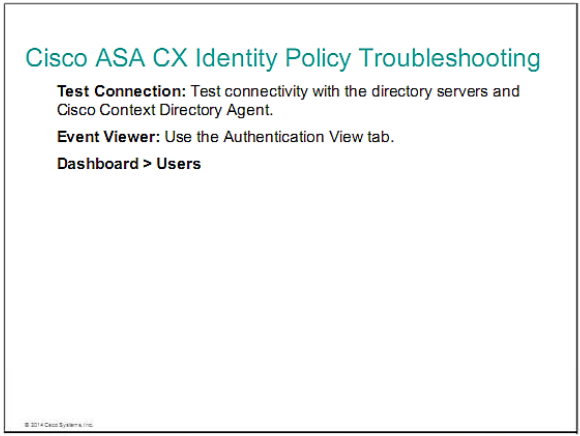
The top example shows that the user "nina" successfully authenticated by using active authentication.

The bottom example shows that the user "harry" successfully authenticated by using passive authentication.

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

Cisco ASA CX Identity Policy Troubleshooting

This topic explains how to troubleshoot Cisco Adaptive Security Appliances Context Aware identity policies.



Some of the tools that are available in Cisco Prime Security Manager to help monitor and troubleshoot the Cisco ASA CX identity policies operations include testing connections, Event Viewer, and the **Dashboard > Users screen**.

To test communications between Cisco ASA CX and the Microsoft Active Directory or LDAP servers or Cisco CDA, use the Test Connection option when configuring the Active Directory or LDAP servers or the Cisco CDA in Cisco PRSM.

On the **Event Viewer > Authentication View** tab, check for authentications-related events; for example, the Redirect Authentication events that are triggered when a traffic flow matches an identity policy that requires active authentication. You should also see the related Authentication Failure or Authentication Success events.

In Event Viewer, you can also use the Filter option to selectively filter the output to display only events that are related to a specific username, identity type, or so on.

From the **Dashboard > Users screen**, you can see the Users report, which shows information about each user; for example, the number of transactions allowed and denied, data usage information.

If passive authentication fails, things to verify include the User to IP mappings on the Cisco CDA and the Cisco ASA CX ADI Session database using the **show opdata adisessions** CLI command. If there is no User to IP mappings on the Cisco CDA, may sure the clock on the Cisco CDA and AD server is synchronized.

https://t.me/learningnets

Summary

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

Summary

Identity policies determine whether a user must be authenticated and if so, how the user should be authenticated. The purpose of authentication is to determine which user is involved in a traffic flow so that identity-based access or decryption policies can be applied to traffic flows.

There are two options for authenticating and identifying the users: active authentication and passive authentication.

With passive authentication, a mapping between the username and the IP address of the user is obtained when the user logs in to the Active Directory domain. Cisco CDA collects the mapping and then sends it to Cisco ASA (CX) NGFW.

Active authentication requires the user to initiate an HTTP or HTTPS connection to trigger the authentication process.

© 2014 Cisco Systems, Inc.

Summary (Cont.)

A realm in Cisco ASA (CX) NGFW is logical group of a common type of directory servers. The directory servers (Active Directory servers and LDAP servers) are defined within the respective realm in Cisco ASA (CX) NGFW. Multiple directory servers can be defined per realm, for redundancy.

Cisco ASA (CX) NGFW supports only one Active Directory realm but can support multiple LDAP realms.

The ADI is the Cisco ASA (CX) NGFW process that provides authentication and identity services.

From the Cisco ASA (CX) NGFW CLI, the admin user can use the **show opdata adisessions** command to display the ADI session directory. From the Cisco ASA (CX) NGFW CLI, the admin user can use the **clear opdata adisessions** command to clear the ADI session directory.

© 2014 Cisco Systems, Inc.

https://t.me/learningnets

Summary (Cont.)

From PRSM Device > Authentication, authentication settings can be configured.

Identity objects are used to match user identity, including usernames and user group names. There are two system-predefined identity objects: known users and unknown users.

To test communications between Cisco ASA CX and the Microsoft Active Directory or LDAP servers or Cisco CDA, use the Test Connection option when configuring the Active Directory or LDAP servers or the Cisco CDA in Cisco PRSM.

On the Event Viewer > Authentication View tab, check for authentications-related events; for example, the Redirect Authentication events that are triggered when a traffic flow matches an identity policy that requires active authentication. You should also see the related Authentication Failure or Authentication Success events.

© 2014 Cisco Systems, Inc.

References

For additional information, refer to these resources:

Cisco Systems, Inc. *Cisco ASA Series Firewall CLI Configuration Guide, 9.1.* http://www.cisco.com/en/US/docs/security/asa/asa91/configuration/firewall/asa_91_firewall_config.html

Cisco Systems, Inc. *Cisco ASA Series Firewall ADSM Configuration Guide, 7.1.* http://www.cisco.com/en/US/docs/security/asa/asa91/asdm71/firewall/asdm_71_firewall_config.html

Cisco Systems, Inc. *User Guide for ASA CX and Cisco Prime Security Manager 9.1* http://www.cisco.com/en/US/docs/security/asacx/9.1/user/guide/b_User_Guide_for_ASA_CX_and_PRSM_9_1.pdf

https://t.me/learningnets

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

Lesson 7

Configuring Cisco ASA (CX) NGFW Decryption Policies

Overview

This lesson describes how to configure Cisco Adaptive Security Appliances Context Aware Next Generation Firewall decryption policies. The purpose of access policies is to detect and control what users are doing on the network. When traffic is encrypted within an TLS/SSL session, Cisco ASA (CX) NGFW can inspect the traffic only if the traffic flow is first decrypted. Cisco ASA (CX) NGFW decryption policies are used to determine which traffic requires TLS/SSL decryption.

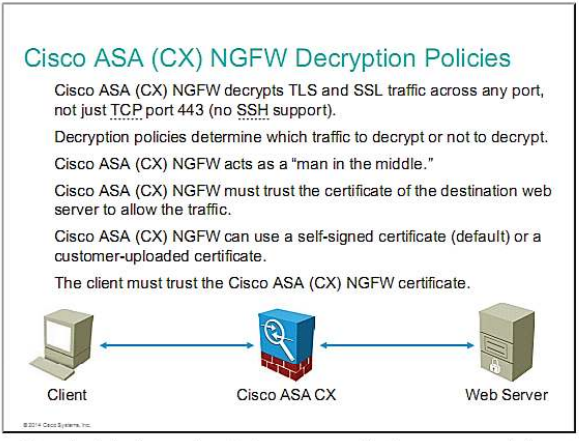
Upon completing this lesson, you will be able to meet these objectives:

- Explain Cisco ASA (CX) NGFW TLS/SSL decryption operations
- Describe how to enable Cisco ASA (CX) NGFW decryption and manage Cisco ASA (CX) NGFW certificates
- Describe how to configure Cisco ASA (CX) NGFW decryption policies to match security requirements
- Explain how the identity, decryption, and access policies interact with one another
- Troubleshoot Cisco NGFW decryption policies

https://t.me/learningnets

Cisco ASA (CX) NGFW Decryption Policies

This topic explains the Cisco Adaptive Security Appliances Context Aware Next Generation Firewall TLS/SSL decryption operations.



HTTPS uses SSL or its following version, TLS, to encrypt traffic for secure transmissions. Because encrypted traffic cannot be inspected, it must be decrypted before the content of the traffic can be inspected. The purpose of access policies is to detect and control what users are doing on the network. For traffic that is encrypted within an TLS/SSL session, Cisco ASA (CX) NGFW cannot inspect the traffic unless the traffic flow is first decrypted.

The Cisco ASA (CX) NGFW decryption policy (also known as TLS Proxy) is used to determine which traffic requires TLS/SSL decryption. Cisco ASA (CX) NGFW can decrypt TLS/SSL traffic over any port, not just TCP port 443. Other encrypted protocols, such as SSH, are not supported as of Cisco ASA (CX) NGFW Software Release 9.1.1 and 9.1.2.

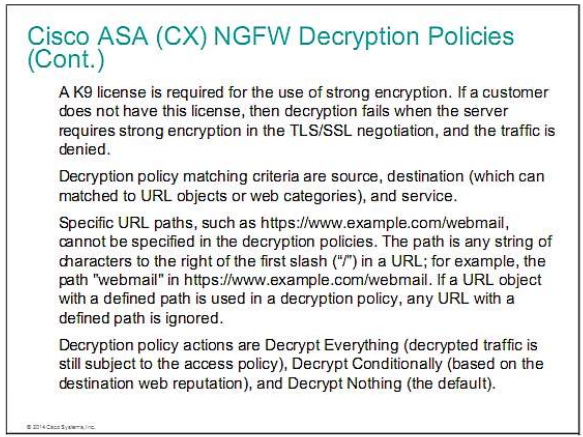
When decrypting secure web (HTTPS) traffic, you can identify the web resource or web application that is being accessed. This in turn makes it possible to apply context-aware policies to that traffic. For other protocols that are encrypted within TLS-secured sessions, you can identify the destination domain, so access policies can be applied based on that information.

Decryption policies in Cisco ASA (CX) NGFW are not used to determine how to perform the decryption, only to determine which TLS/SSL traffic should be decrypted. When Cisco ASA (CX) NGFW performs the TLS/SSL decryption, the Cisco ASA (CX) NGFW decrypts the traffic, inspects the traffic, applies any matched access-policy actions, then re-encrypts the allowed inspected traffic. Cisco ASA (CX) NGFW acts as a man in the middle between the client browser and the destination web server.

Cisco ASA (CX) NGFW must trust the certification of the destination web server, to allow the traffic from the client to the destination web server. In Cisco ASA (CX) NGFW Software Release 9.1.1 and 9.1.2, Cisco ASA (CX) NGFW does not validate whether the destination web server certificate has been revoked or expired.

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

Cisco ASA (CX) NGFW can use a self-signed certificate or a customer-uploaded certificate, which is presented to the client browser. The client browser must trust the Cisco ASA (CX) NGFW self-signed certificate or the customer-uploaded Cisco ASA (CX) NGFW certificate.



A K9 license is required for strong encryption. If you do not have a K9 license, then decryption processing with a server that requires strong encryption fails and the encrypted traffic is denied by Cisco ASA (CX) NGFW.

Decryption policies can match traffic by using the Source, Destination, and Service fields.

All these criteria can be used to determine the traffic to which a decryption policy applies:

Source: A list of policy objects of these types: network group (IP addresses), identity (user or user group names), or secure mobility (type of remote-access VPN client). If a packet matches any selected object, then the packet is considered to satisfy the source condition.

Destination: A list of policy objects of these types: network group, URL (URLs or web categories), or destination object group (a collection of network group or URL objects in complex AND/OR relationships that you cannot define directly in a policy). If a packet matches any selected object, then the packet is considered to satisfy the destination condition. If you disable the URL filtering feature or do not have a valid Web Security Essentials license, you cannot use URL objects in this field or in a destination object group.

Note When configuring URL objects for use in decryption policies, do not include path information. When evaluating whether traffic matches a URL object, the decryption policy completely ignores any URLs that include path information. If the object contains a mix of URLs with domain name only and URLs that include paths, the decryption policy treats the object as containing only those URLs that specify only a domain name.

Service: A list of service groups that define protocol and port combinations. If a packet matches any selected object, then the packet is considered to satisfy the service condition.

https://t.me/learningnets

Decryption policies can have these actions:

Decrypt Everything: Decrypt TLS/SSL traffic and inspect the decrypted traffic. Decrypted traffic is evaluated against the access policy, to determine whether the decrypted traffic is allowed, conditionally allowed, or denied. If the access policies allow the traffic flow, then the allowed traffic is re-encrypted and sent to its destination. A traffic flow can be denied if an TLS/SSL session to the destination server cannot be established; for example, because Cisco ASA (CX) NGFW does not trust the destination server certificate. Also, if the destination server requires strong encryption, you must have a K9 license or the flow is denied.

Decrypt Potentially Malicious Traffic: Conditionally decrypt the traffic, based on destination web reputation; only traffic to destinations that have a low reputation score is decrypted. If you select this option, you must also select the web reputation action profile object that defines the low reputation-score range, in the Web Reputation Action Profile field.

Do Not Decrypt (the default): Do not decrypt the traffic. These TLS/SSL encrypted traffic flows are not inspected. This is the default action for encrypted flows that do not match any decryption policy.

Tags: Words or phrases that help the administrator to identify this item. Tags are for administration purposes only and do not affect how the system or policies function. One or more tags can be entered.

Ticket ID: A case or ticket identifier from your support system (for example, Remedy). If you are making a change that is related to a network support case, you can enter the ticket ID for tracking purposes. You can enter new IDs or select from existing IDs that are used in pending changes, and you can specify as many separate IDs as needed.

Cisco ASA (CX) NGFW Decryption Policies (Cont.)

Cisco ASA (CX) NGFW also allows you to base decryption policy decisions (to decrypt or not to decrypt) on characteristics of the destination web server, such as the destination domain name or FQDN, the web category, or the web reputation.

The web category is determined according to the destination web server domain name.

The reputation is determined according to the destination server domain name and IP address.

The destination web server domain name and FQDN are determined by examining the destination server certificate. Therefore, Cisco ASA (CX) NGFW also needs to act as the man in the middle during the initial TLS/SSL negotiation, to examine the destination web server certificate, to match the domain name or FQDN against the decryption policies, and to determine whether the TLS/SSL traffic flow needs to be decrypted (even if the final decision from the decryption policy is not to decrypt the traffic).

© 2014 Cisco Systems, Inc.

Cisco ASA (CX) NGFW allows decryption policy decisions to be based on the characteristics of the destination, such as the destination domain name or the FQDN, but not on specific URL paths such as https://www.example.com/webmail, the web category, or the web reputation score.

For example, to define a decryption policy that applies to all traffic to the domain example.com, the URL object should specify example.com as the URL. This will match www.example.com, games.example.com, photos.example.com, and so on.

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

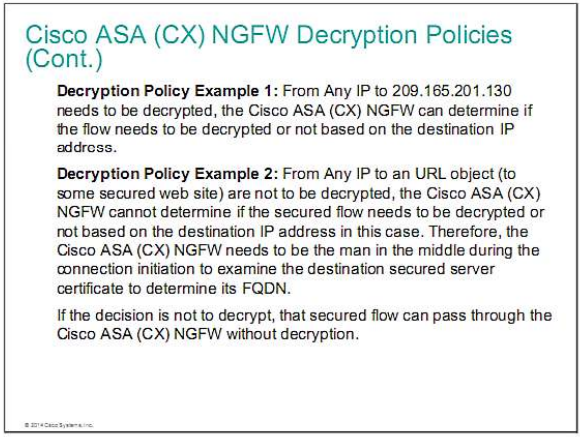
For decryption policy decisions to be based on the web category, Cisco ASA (CX) NGFW needs to determine the web category based on the destination website domain name.

For decryption policy decisions to be based on the web reputation score, Cisco ASA (CX) NGFW needs to determine the web reputation score based on the destination website domain name and IP address.

The destination web server domain name and FQDN are determined by examining the destination server certificate. Therefore, Cisco ASA (CX) NGFW also needs to act as the man in the middle during the initial TLS/SSL negotiation, to examine the destination web server certificate, to match the domain name or FQDN against the decryption policies, and to determine whether the TLS/SSL traffic flow needs to be decrypted (even if the final decision from the decryption policy is not to decrypt the traffic).

For example, a decryption policy can be defined as follows:

IF the source IP address is on the internal network AND the destination domain name is neither example.com nor example.org THEN only decrypt the potentially malicious traffic (based on the reputation score of the destination website).



When using the source IP address and destination IP address and port as the matching conditions in the decryption policies, the Cisco ASA (CX) NGFW can determine if the flow needs to be decrypted or not based on the destination IP address

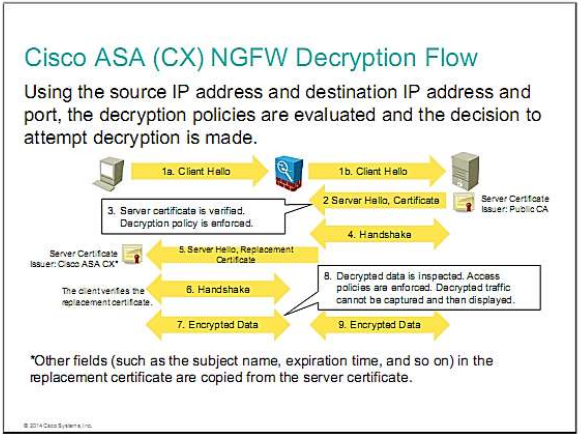
When using the domain name or FQDN, the web category, or the web reputation as the destination matching conditions in the decryption policies, the Cisco ASA (CX) NGFW can't determine if the secured flow needs to be decrypted or not based on the destination IP address in this case.

If the protocol is HTTP, then Cisco ASA (CX) NGFW can see the domain name or FQDN information in the HTTP request headers. However, in TLS/SSL, the protocol data is encrypted. Cisco ASA (CX) NGFW only knows that it might need to decrypt the traffic flow, but it needs more information that will become available by examining the destination web server certificate to make a final decision. Cisco ASA (CX) NGFW determines the destination server domain name or FQDN from the destination web server certificate, if that certificate is trusted. Using the domain name or FQDN, Cisco ASA (CX) NGFW can also find the web category and web reputation score of the destination web server.

https://t.me/learningnets

The Cisco ASA (CX) NGFW needs to be the man in the middle during the connection initiation in order to examine the destination secured server certificate to determine its FQDN. Once the Cisco ASA (CX) NGFW determines the FDQN, it can also determine its web category, or the web reputation, then determines if it needs to decrypt or not to decrypt the secured flow. Note that if the decision is not to decrypt, that secured flow can pass through the Cisco ASA (CX) NGFW without decryption.

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



The figure shows the encrypted HTTPS traffic flows that Cisco ASA (CX) NGFW decrypts.

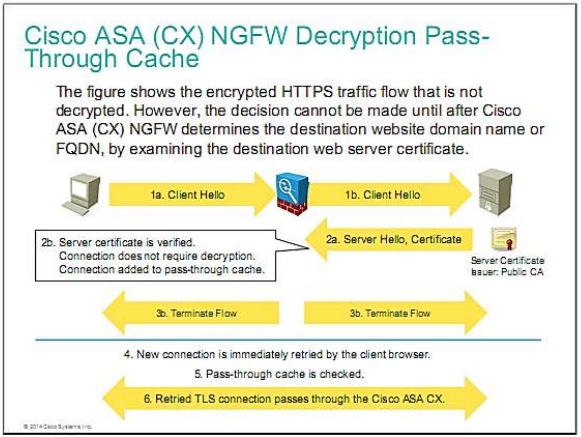
1. a. The client sends a client hello toward the destination web server. If the initial flow matches an access policy with the deny action, then Cisco ASA (CX) NGFW drops the flow.

   b. Cisco ASA (CX) NGFW sees the connection request, examines the first several bytes of the traffic flow, and identifies that the client is requesting an TLS/SSL handshake with the destination web server. Given this examined information, such as the source IP address and destination IP address and port, the decryption policies are evaluated and the decision to attempt decryption is made. If a decryption policy is matched and the decision is to decrypt (as shown in this example), then Cisco ASA (CX) NGFW initiates and sends a client hello to the destination web server, using the destination IP address and port number from the original client connection. If a decryption policy is matched and the decision is not to decrypt, then Cisco ASA (CX) NGFW passes the client hello through to the destination web server.
2. The destination web server sends a server hello and its certificate back to Cisco ASA (CX) NGFW.
3. Cisco ASA (CX) NGFW verifies whether the destination web server certificate is trusted. If the destination web server certificate is not trusted, then both the connection to the destination web server and the connection from the client are closed.
4. If the destination web server certificate is trusted, then Cisco ASA (CX) NGFW completes the TLS/SSL handshake with the destination web server.
5. Cisco ASA (CX) NGFW sends a server hello and its replacement certificate to the client. This replacement certificate basically spoofs the destination web server certificate. Within the replacement certificate, the issuer is Cisco ASA (CX) NGFW if it is using its self-signed certificate. Other fields in the replacement certificate, such as the subject name, expiration time, and so on, are copied from the real destination web server certificate.
6. The client completes the TLS/SSL handshake with Cisco ASA (CX) NGFW.
7. The client begins sending encrypted traffic toward the destination web server.

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

8. Cisco ASA (CX) NGFW decrypts the traffic and applies the matched access-policy actions to the decrypted traffic. If the decrypted traffic matches an access policy with the deny action, then Cisco ASA (CX) NGFW drops the flow.
9. Cisco ASA (CX) NGFW re-encrypts the allowed traffic and sends it to the destination web server.

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



The figure shows the encrypted HTTPS traffic flow that is not decrypted by Cisco ASA (CX) NGFW. However, the decision cannot be made until after Cisco ASA (CX) NGFW can determine the destination website domain name or FQDN, by examining the destination web server certificate.

1. a. The client sends a client hello toward the destination web server. If the initial flow matches an access policy with the deny action, then Cisco ASA (CX) NGFW drops the flow.

   b. In this example, a decryption policy cannot be matched at this point, based on information such as the source IP address and the destination IP address and port. Therefore, Cisco ASA (CX) NGFW sends the client hello to the destination web server.

2. a. The destination web server sends a server hello and its certificate back to Cisco ASA (CX) NGFW.

   b. Cisco ASA (CX) NGFW verifies the destination web server certificate and determines the destination web server domain name or FQDN from the destination web server certificate, the web category, and the web reputation for matching a decryption policy. When a decryption policy is matched and has the Do Not Decrypt action, the connection is added to a pass-through cache in Cisco ASA (CX) NGFW, which stores the triplet information of that traffic flow (source IP, destination IP, destination port).

3. a. and b. Cisco ASA (CX) NGFW resets the connections to the destination web server and to the client, with the expectation that the client browser will retry to connect to the same destination IP address and port within a short period.

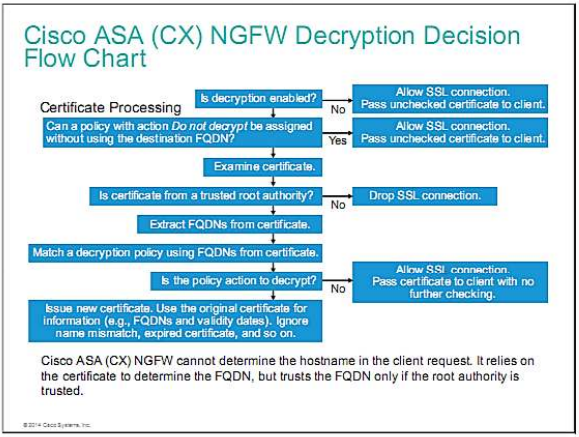
4. The client browser immediately retries the connection.

5. When this retry happens, the same triplet information is found in the Cisco ASA (CX) NGFW pass-through cache. Therefore, Cisco ASA (CX) NGFW knows to apply the Do Not Decrypt decision to this traffic flow. In other words, one of the first checks that the Cisco ASA (CX) NGFW TLS proxy engine performs when any new TLS/SSL connection is opened is whether the triplet information for that connection is already in the Cisco ASA (CX) NGFW pass-through cache.

6. The retried connection passes through Cisco ASA (CX) NGFW. Cisco ASA (CX) NGFW does not inspect the encrypted flow between the client and the destination web server.

There are some known weaknesses with this approach, the most obvious being that there is no guarantee that the client application will retry the connection after the initial failure. Ideally, Cisco ASA (CX) NGFW should close the connection that it opened to the destination server and then allow the original client packets to flow through to the destination server, without decryption. As of Cisco ASA (CX) NGFW Software Release 9.1.1 (and 9.1.2), this is not possible, although that might change in a future release.

Cisco ASA (CX) NGFW Decryption Decision Flow Chart



The figure shows a summary flow chart that illustrates how the SSL/TLS decryption decision is made.

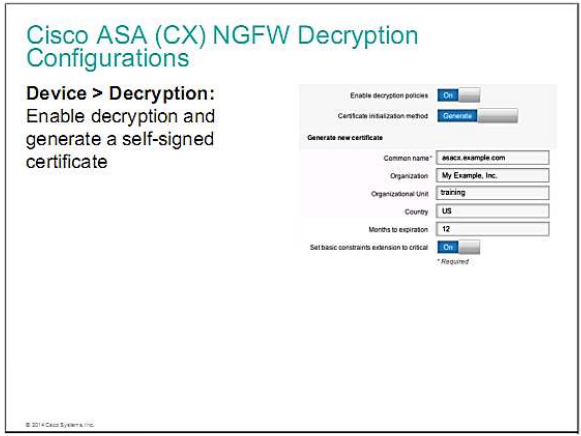
A key point to understand in the flow is that Cisco ASA (CX) NGFW cannot match a decryption policy with the Do Not Decrypt action without knowing the destination website domain name or FQDN. Therefore, Cisco ASA (CX) NGFW needs to examine the destination web server certificate to determine the destination website domain name or FQDN so that it can match a decryption policy.

Another key point is that the client must trust the Cisco ASA (CX) NGFW certificate, and Cisco ASA (CX) NGFW must trust the destination web server certificate.

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

Cisco ASA (CX) NGFW Decryption Configurations

This topic describes how to enable decryption and how to manage the Cisco Adaptive Security Appliances Context Aware Next Generation Firewall certificate.

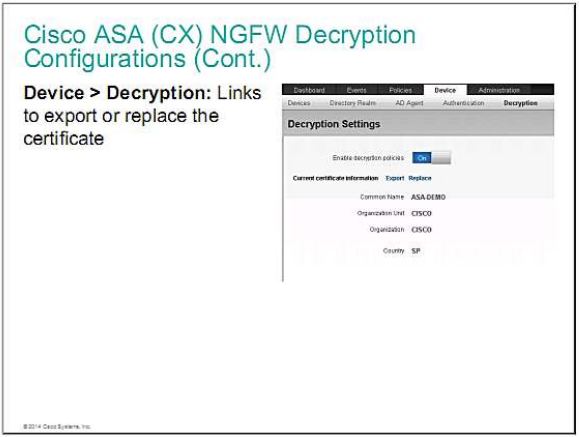


The figure shows the Cisco Prime Security Manager Device > Decryption page, which you can use to enable the decryption policies and to generate a new Cisco ASA (CX) NGFW self-signed certificate.

Choose **On** for the **Enable Decryption Policies** option, to enable TLS/SSL decryption and decryption policies.

Choose **Generate** for the **Certificate Initialization Method**.

Fill in the fields of the self-signed certificate. Only the Common Name field is required. The other fields are optional.

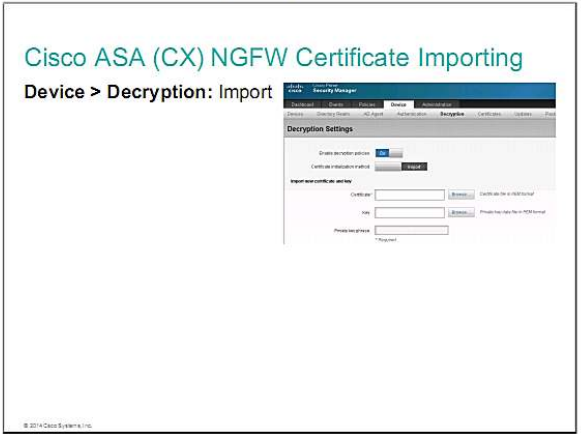


The figure shows the Cisco PRSM Device > Decryption page after decryption has been enabled and the self-signed certificated has been generated.

Summary information about the currently configured certificate appears on the screen in place of the Certificate Initialization Method field.

In addition, links to export or replace the certificate are available on this page. Click **Export** to export the certificate in a file (in PEM format) that can be uploaded to the client browser so that clients do not need to trust and save the Cisco ASA (CX) NGFW self-signed certificate when prompted during a decrypted traffic flow.

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



The figure shows the Cisco PRSM Device > Decryption page, which is used to enable the decryption policies and to import a CA signed Cisco ASA (CX) NGFW certificate and the matching private key, both in PEM format.

Choose **On** for **Enable Decryption Policies**, to enable TLS/SSL decryption and decryption policies.

Choose **Import** for the **Certificate Initialization Method**.

Click **Browse** to select the Cisco ASA (CX) NGFW certificate and matching private key to be imported. Enter the private key phrase, if required. As of Cisco ASA Software Release 9.1.1 (and 9.1.2), the only supported format for the certificate and private key file is PEM.

https://t.me/learningnets

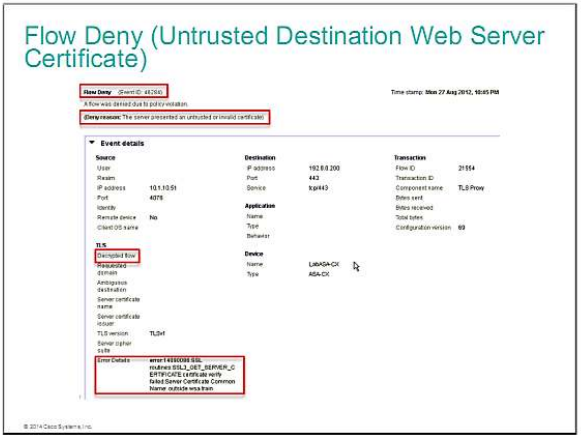


If you already enabled decryption and have the Cisco ASA (CX) NGFW certificate generated or imported, the Device > Decryption page shows summary information about the configured Cisco ASA (CX) NGFW certificate instead of showing the Certificate Initialization Method field.

The page shows links to export or replace the Cisco ASA (CX) NGFW certificate. If you click Replace, then the Certificate Initialization Method field appears and you can select how to replace the certificate.

In the figure, in the bottom-right corner, part of the replacement certificate that Cisco ASA (CX) NGFW presents to the client is shown. In this example, within this replacement certificate, the Issued By Common Name is VeriFraud. VeriFraud is the common name on the imported Cisco ASA (CX) NGFW certificate. The Issued To common name is login.yahoo.com. The other fields (such as the Issued On and Expired On fields) in the replacement certificate are copied from the original destination web server certificate. In this example, the user was browsing to the secured Yahoo Sign In web page.

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



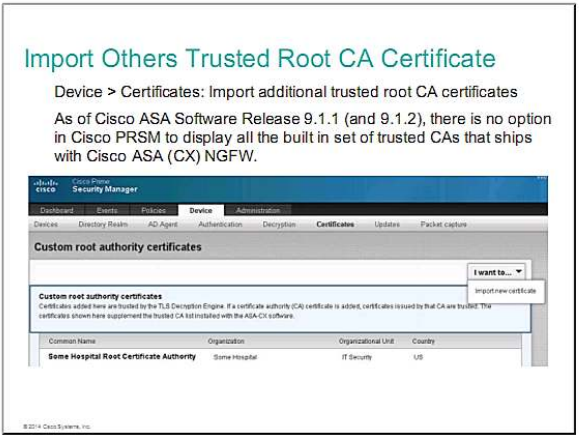
This figure shows an example of the Flow Deny event in Cisco ASA (CX) NGFW. This event can be viewed from the Cisco PRSM Event Viewer. In this example, an TLS/SSL encrypted flow was denied because Cisco ASA (CX) NGFW did not trust the destination server certificate. The failed destination server certificate has the common name outside.wsa.train.

To perform TLS/SSL decryption, Cisco ASA (CX) NGFW acts as the man in the middle and must validate the trustworthiness of the destination web server by verifying the root CA that signed the destination web server certificate. If Cisco ASA (CX) NGFW does not recognize this root CA, then it does not trust the destination web server certificate and it denies the flow. This can happen if the destination web server uses a CA that is not part of the set of trusted CAs that ships with Cisco ASA (CX) NGFW; for example, if an organization uses an internal CA to sign certificates for servers on the internal network.

To prevent Cisco ASA (CX) NGFW from potentially blocking access to servers with unrecognized root CAs, you can upload to the Cisco ASA (CX) NGFW the root CA certificates that your organization trusts. For example, you might want to upload the root CA certificate that the servers on your network use. You can upload multiple certificate files, each of which can contain multiple certificates. You can upload root CA certificates, intermediate CA certificates, or individual server certificates. However, each certificate that you upload must be in PEM format.

These imported certificates are used in conjunction with the preinstalled set of trusted CAs that ships with Cisco ASA (CX) NGFW.

As of Cisco ASA Software Release 9.1.1 (and 9.1.2), there is no option in Cisco PRSM to display all the preinstalled set of trusted CAs that ships with Cisco ASA (CX) NGFW.



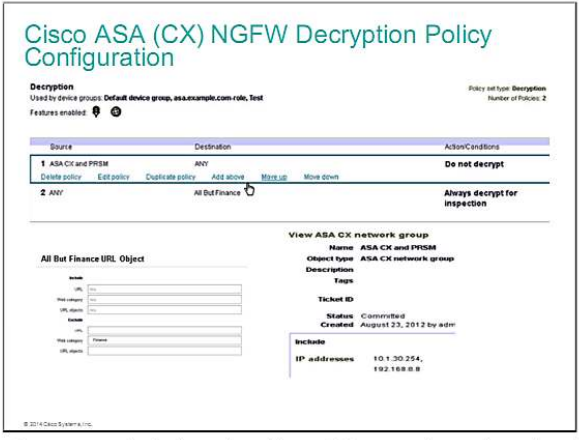
The figure shows the Cisco PRSM Device > Certificates page, which you use to import the trusted root CA certificates into Cisco ASA (CX) NGFW. The certificates list shows all certificates that have been imported, including the common name, organization, organizational unit, and country for each, if these are defined in the certificate.

In the example in the figure, one trusted root CA certificate has been imported to Cisco ASA (CX) NGFW.

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

Cisco ASA (CX) NGFW Decryption Policy Configuration

This topic describes how to configure Cisco Adaptive Security Appliances Context Aware Next Generation Firewall decryption policies to match security requirements.



This figure shows an example of a decryption policy set. This set contains two decryption policies.

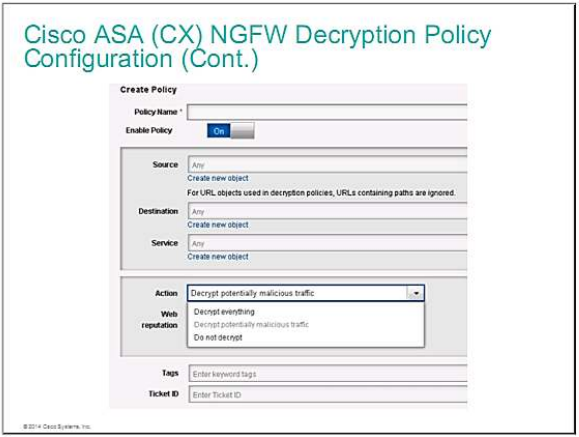
The first decryption policy will disable decryption for all the traffic that is sourced from the "ASA CX and PRSM" Cisco ASA (CX) NGFW network group object, to any destination. For example, traffic that is sourced from the Cisco ASA (CX) NGFW IP address and Cisco Prime Security Manager IP address to the Cisco Security Intelligence Operations for applications signatures, web reputation updates, and so on will not need to be decrypted, otherwise the Cisco ASA (CX) NGFW and PRSM SIO updates may fail.

Recall that the Cisco ASA 5500-X CX management interface traffic is routed through the Cisco inside interface to reach the Cisco SIO.

The second decryption policy will decrypt all traffic from any source to any destination websites, except to websites that belong to the Finance Web Category. The Source field is set to ANY, which will match traffic from any source. The Destination field is set to the All But Finance URL object. The All But Finance URL object includes all traffic except for traffic that is destined to any websites in the Finance Web Category. The Service field is set to ANY, which will match any services. The policy action is set to Decrypt Everything.

Note Do Not Decrypt is the default action for encrypted flows that do not match any decryption policy.

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



The figure shows the Create Policy screen for adding a new decryption policy.

The decryption policy traffic matching fields include the Source, Destination, and Service fields.

There are three possible actions for the decryption policy:

Decrypt Everything: Decrypt the traffic and inspect HTTPS traffic. If access policies allow the traffic flow, the the traffic is re-encrypted and sent to its destination.

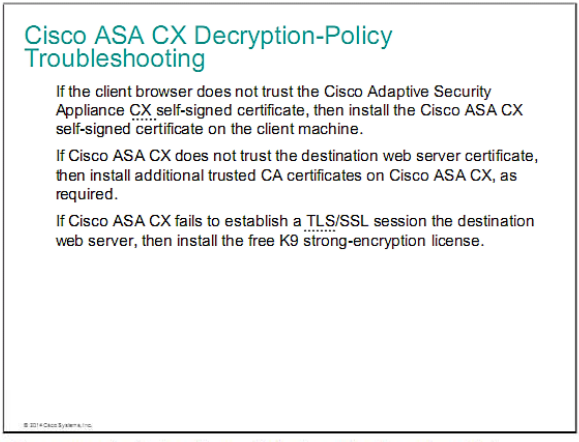
Decrypt Potentially Malicious Traffic: Conditionally decrypt traffic, based on web reputation. Matching traffic that falls into the low reputation zone is decrypted, whereas high-reputation traffic is not decrypted. If you choose this option, you must also choose the web reputation profile object that defines the low reputation zone, in the Web Reputation Action Profile field.

Do Not Decrypt (the default): Do not decrypt the traffic. These TLS/SSL encrypted traffic flows cannot be inspected.

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

Cisco ASA CX Decryption Policy Troubleshooting

This topic explains common problems and solutions with decryption policies.



This figure shows some of typical problems with implementing decryption policies.

The client browser does not trust the Cisco ASA CX replacement certificate. Cisco ASA CX can use a self-signed certificate or a customer-imported, CA signed certificate. Web browsers usually display a warning if the Cisco ASA CX replacement certificate is not trusted. Other clients (such as IM applications) might not display such a warning. Ensure the client trust the Cisco ASA CX "replacement" certificate.

Cisco ASA CX does not trust the destination web server certificate. In this case, Cisco ASA CX denies the flow. The Flow Deny event is generated. Ensure that Cisco ASA CX trusts the destination web server certificate.

Cisco ASA CX fails to establish a TLS/SSL session with the destination web server. A Flow Deny event is generated; for example, if the TLS/SSL session is trying to use a strong-encryption algorithm but the K9 strong-encryption license is not installed. In this case, Cisco ASA CX denies the flow.

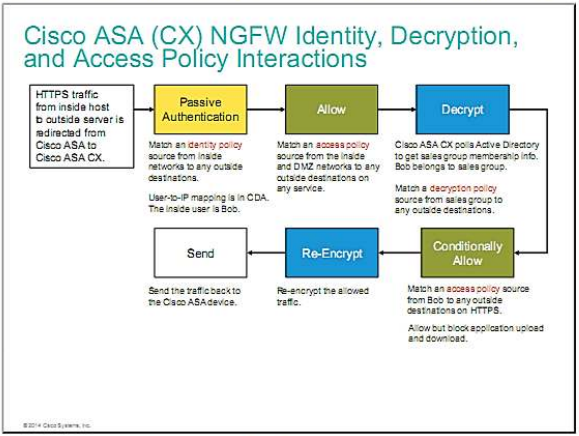
This link to the Cisco Tech Zone (which requires a valid Cisco Connection Online login) contains Cisco ASA CX -- Certificate and Decryption Problems with the CX Module Troubleshooting Guide:

https://techzone.cisco.com/t5/Context-Aware-Security/Troubleshooting-Guide-ASA-CX-Certificate-and-Decryption-Problems/ta-p/82736

Note	Traffic that is sourced from the Cisco ASA CX IP address and Cisco Prime Security Manager IP address to the Cisco Security Intelligence Operations for applications signatures, web reputation updates, and so on will not need to be decrypted, otherwise the Cisco ASA CX and PRSM SIO updates may fail.

Cisco ASA (CX) NGFW Identity, Decryption, and Access Policy Interactions

This topic explains how the identity, decryption, and access policies interact with each other.



The identity policy defines which traffic needs to be authenticated and how to perform the authentication (active or passive). The resulting user identity can be used in other access or decryption policies.

For the traffic to be matched by a decryption policy, the traffic must first be allowed by an access policy. Access policies defines which traffic is allowed, conditionally allowed, or denied. Access policies are also applied to decrypted traffic.

The decryption policy defines which traffic needs to be decrypted. Decrypted traffic is still subject to access policies.

This figure shows a traffic-flow scenario in which different policy types are matched:

1. The HTTPS traffic is redirected to the Cisco Adaptive Security Appliances Context Aware Next Generation Firewall from the Cisco ASA device.
2. The HTTPS traffic matches an identity policy, by using passive authentication. In this example, the source IP address maps to the Bob Active Directory user.
3. The HTTPS traffic matches an access policy that allows the traffic.
4. Cisco ASA (CX) NGFW determines whether the HTTPS traffic needs to be decrypted. In this case, it matches a decryption policy with the Decrypt action. The decryption policy matches the Sales Active Directory group as the source. Cisco ASA (CX) NGFW gets the Active Directory membership information from the Active Directory server every 24 hours, by default. In this example, the Bob Active Directory user belongs to the Sales Active Directory Group.
5. The decrypted HTTPS traffic is still subject to the access policy. In this example, the traffic matches an access policy with the Conditionally Allowed action blocking all application uploads and downloads.
6. Cisco ASA (CX) NGFW re-encrypts the conditionally allowed traffic.

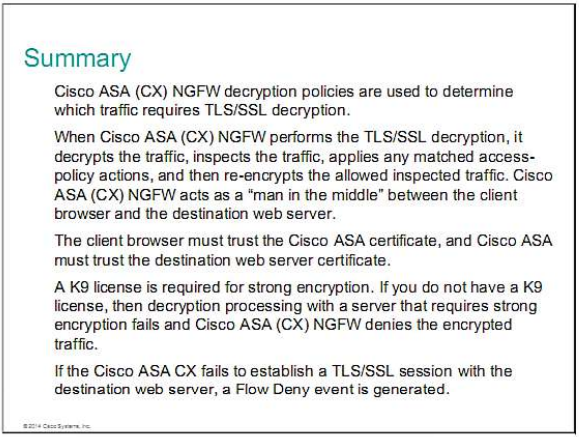
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

7. Cisco ASA (CX) NGFW sends the re-encrypted traffic back to Cisco ASA, which sends the traffic to the destination web server.

https://t.me/learningnets

Summary

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



References

For additional information, refer to these resources:

Cisco Systems, Inc. *Cisco ASA Series Firewall CLI Configuration Guide, 9.1*. http://www.cisco.com/en/US/docs/security/asa/asa91/configuration/firewall/asa_91_firewall_config.html

Cisco Systems, Inc. *Cisco ASA Series Firewall ADSM Configuration Guide, 7.1*. http://www.cisco.com/en/US/docs/security/asa/asa91/asdm71/firewall/asdm_71_firewall_config.html

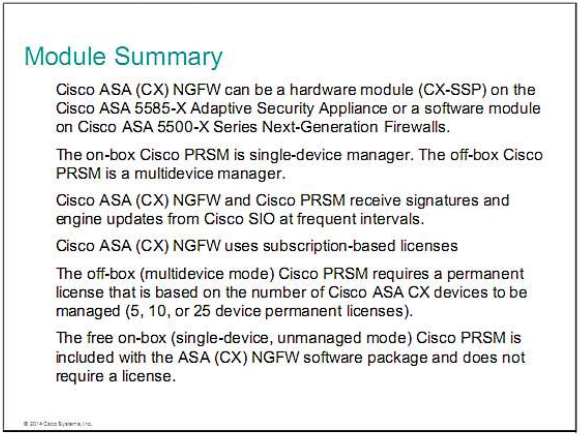
Cisco Systems, Inc. *User Guide for ASA CX and Cisco Prime Security Manager 9.1* http://www.cisco.com/en/US/docs/security/asacx/9.1/user/guide/b_User_Guide_for_ASA_CX_and_PRSM_9_1.pdf

© 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.)

There are three types of policies in Cisco ASA: identity, decryption, and access. Policy objects are used within the Cisco ASA (CX) NGFW policy for traffic matching.

Access policies are used to control access to the network. Complex traffic-matching criteria can be configured to define precise access policies.

Cisco ASA (CX) NGFW supports active or passive authentication. When the user identity information is obtained, you can create identity objects for use in access and decryption policies so that you can implement identity-based policies in Cisco ASA (CX) NGFW.

Cisco ASA (CX) NGFW can decrypt SSL/TLS traffic by acting as the man in the middle between the client web browser and the destination secured web server.

Enable eventing for traffic flows that match the policy, to generate events in Event Viewer or data in reports.

© 2014 Cisco Systems, Inc.

References

For additional information refer to this resource:

User Guide for ASA CX and Cisco Prime Security Manager 9.1

© 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. Which three options are Cisco ASA (CX) NGFW policy types? (Choose three.)

   A. encryption
   B. access
   C. identity
   D. application inspection
   E. decryption

2. Which three are the default Cisco ASA (CX) NGFW policies? (Choose three)

   A. permit all traffic
   B. deny all traffic
   C. do not decrypt any traffic
   D. decrypt HTTPS traffic to low reputation sites
   E. do not require authentication
   F. use passive authentication for all traffic

3. What can prevent events from being shown in the Cisco PRSM Event Viewer?

   A. In the access policy, Capture Packets has been disabled.
   B. In the access policy, eventing has been disabled.
   C. The Cisco ASA CX logging level is not set to the DEBUG level.
   D. The Cisco PRSM logging level is not set to the DEBUG level.

https://t.me/learningnets

4. What does the **clear opdata adisessions** Cisco ASA (CX) NGFW CLI command do?

   A. clears all the policy configurations in Cisco ASA CX
   B. clears the ADI session directory which clears all the user-to-IP address mappings in Cisco ASA CX
   C. disconnects all the passively authenticated user connections in Cisco ASA CX
   D. disconnects all the actively authenticated user connections in Cisco ASA CX

5. With ASA CX you can block web traffic based on site reputation. What is the lowest reputation configurable?

   A. –5
   B. –7
   C. –9
   D. –10

6. In the process of providing authentication and identity services, the usernames or user group names are defined in:

   A. access policies
   B. identity policies
   C. identity policy objects
   D. active directory agent

7. When managing multiple devices, which of the following is applied:

   A. policies can be shared among devices
   B. policies cannot be shared among devices
   C. configuration settings are unique per device
   D. configuration settings are not unique per device

8. When configuring ASA CX in Single Device mode, you can:

   A. add policy-sets
   B. delete policy-sets
   C. edit policy-sets
   D. none of the above

9. What is the default port number ASA CX uses for communication with the directory server?

   A. 289
   B. 389
   C. 489
   D. 589

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

10. When using the authentication type Kerberos, which of the following must be in the same domain for the authentication to succeed?

    A. ASA CX/client
    B. ASA CX/domain controller
    C. ASA CX/client/domain controller
    D. client/domain controller

11. How do you filter all the sub domains of cisco.com with URL filtering?

    A. @.cisco.com
    B. #.cisco.com
    C. ^.cisco.com
    D. *.cisco.com

12. SSL/TLS is:

    A. safe and secure
    B. safe but not secure
    C. secure but not safe
    D. none of the above

13. Before implementing the decryption policies, you must first enable them. After enabling them you must select Certificate Authority (CA) certificate that ASA CX will use. Under the Certificate Initialization Method you have the option to:

    A. export the certificate
    B. import the certificate
    C. replace the certificate
    D. generate the certificate

https://t.me/learningnets

Answer Key

1. B, C, E
2. A, C, E
3. B
4. B
5. D
6. C
7. A, C
8. D
9. B
10. C
11. D
12. C
13. B, D

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

Module 2

Cisco Web Security Appliance

Introduction

This module describes how to implement the Cisco Web Security Appliance. The Cisco WSA is a web proxy that works with other Cisco network components to monitor and control outbound requests for Web content and scrubs return traffic for unwanted or malicious content.

Upon completing this module, you will be able to:

- Describe the Cisco Web Security Appliance main features
- Describe the two Cisco Web Security Appliance integration methods (Explicit Proxy and Transparent Proxy)
- Configure identities and user authentication
- Configure URL filtering and application visibility and control
- Configure inbound and outbound anti-malware controls
- Configure decryption policies
- Configure data security controls to implement data loss prevention

https://t.me/learningnets

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

Lesson 1

Describing the Cisco Web Security Appliance Solutions

The Cisco Web Security Appliance provides exceptional web security and control for organizations of all sizes, in one appliance. Also, the appliance easily extends web security to mobile users, smart phones, and devices with the Cisco AnyConnect Secure Mobility Client.

With its Application Visibility and Control engine, the Cisco WSA gives administrators granular control of hundreds of thousands of micro-applications on Facebook and Twitter, as well as many other popular platforms and streaming media. Without blocking entire websites, administrators can allow or block specific features such as chat, messaging, video, and audio.

This lesson provides an overview of the Cisco WSA key features and describes the various supported policies.

Upon completing this lesson, you will be able to meet these objectives:

- Identify how to place Cisco WSA into a typical modularized network design
- Provide a high-level overview of the web proxy service
- Describe the Cisco WSA architecture
- Describe the Cisco WSA malware detection and protection
- Describe the Cisco Web Reputation Filters and the WBRS
- Describe how the Cisco WSA enforces acceptable use
- Describe the Cisco WSA GUI management
- Describe how to commit configuration changes on the Cisco WSA
- Describe the Cisco WSA policy types
- Describe the Cisco WSA access policies
- Describe the Cisco WSA identities
- Configure an identity in the Cisco WSA

https://t.me/learningnets

Describe the Cisco WSA access policy assignment using identity

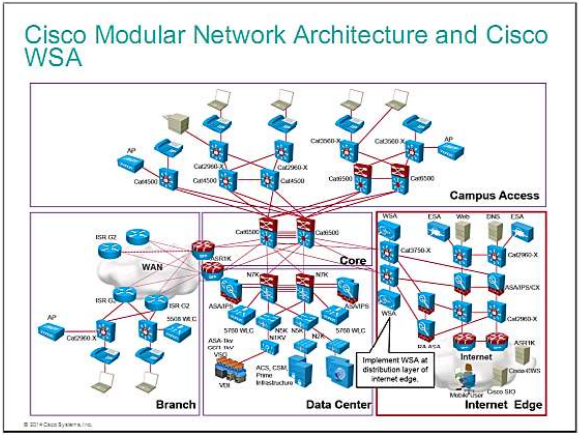
Describe identities and authentication in the Cisco WSA

Describe the Cisco WSA policy trace tool

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

Cisco Modular Network Architecture and Cisco WSA

This topic identifies how to place Cisco Web Security Appliance into a typical modularized network design.

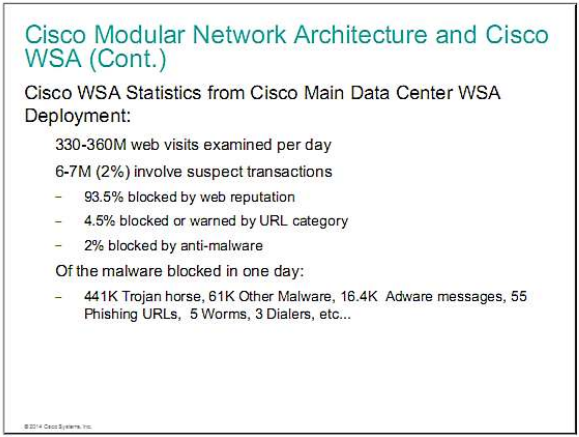


The figure illustrates where in the Cisco modular network architecture the Cisco Web Security Appliance should be deployed. Ideally, the Cisco WSA should be implemented at distribution layer of internet edge portion of Cisco modular network architecture.

The Enterprise Internet Edge module implements a layer of distribution switches that aggregate services common to the various blocks present in the module. The distribution switches reside in the inside network of the firewalls and connect to the core switches, making it accessible to other parts of the enterprise network. URL filtering, content inspection, and intrusion prevention are examples of services that may be aggregated at the distribution layer. The Cisco WSA may be deployed at this layer to enforce acceptable use policies for Web access, content inspection, and to block malware, spyware and other threats. The WSA is a web proxy and sits logically in the path between corporate users and the Internet edge firewalls. Proper placement and configuration of these appliances provides secure web access, content security and threat mitigation for web services.

The function of the WSA is to monitor and mitigate any abnormal web activity between corporate users and the outside world. The WSA is logically located in the path between corporate web users and the Internet. In effect, the WSA acts as a web proxy for the corporate users residing inside the network.

https://t.me/learningnets



The web is becoming the predominant exploit vector. Commonly used black lists and white lists fail to block a significant portion of malicious websites. According to a study, 77 percent of websites with malicious code are legitimate sites that have been compromised, and legitimate sites do not appear on black lists. The same study also found 70 percent of the 100 most popular sites either hosted malicious content or contained a masked redirect to lure unsuspecting victim to malicious sites.

A recent study of 30 sampled large multinational organizations' networks found that 100 percent generated visitor traffic to websites that host malware. Of these, 96 percent were shown to communicate with hijacked servers and 92 percent transmitted traffic to sites without content, which often host malicious activities.

Cisco is working to become a borderless enterprise, where authorized employees, partners, and customers can access any service, anywhere, from anydevice. Cisco IT's policy of allowing employees to use any device, including unregistered personal devices, requires an effective web security solution. For Cisco, this solution is the Cisco WSA, which combines signature-based malware detection with reputation filtering and inline file scanning.

Cisco IT achieved the goal of protecting against zero day threats without changing the user experience using the Cisco WSA. The Cisco WSA is a web proxy that inspects and then either forwards or drops web traffic based on reputation filters or the outcome of inline file scanning. The Cisco WSA combines many technologies in one platform. Cisco IT initially is using two capabilities: WBRS and the Webroot and McAfee anti-malware scanning engines.

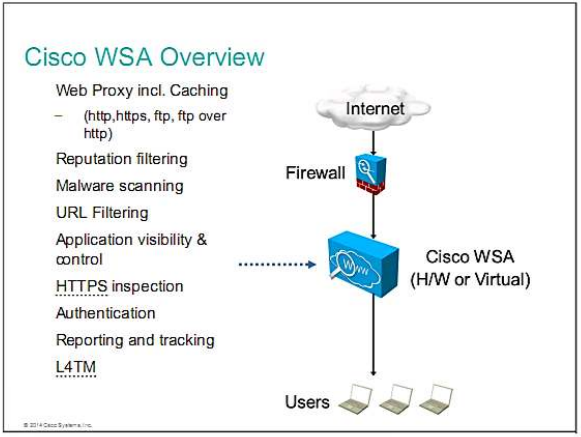
In just the first three months of production for Research Triangle Park,North Carolina and the East Coast, the Cisco WSA blocked more than 30 million malicious objects that signature-based detection alone would have missed.

The figure shows some of the statistics from the Cisco IT implementation of the Cisco WSAs.

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

Cisco WSA Overview

This topic provides an overview of the web proxy.



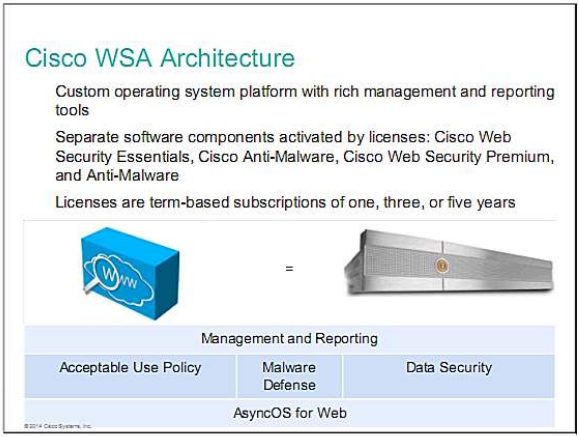
The Cisco Web Security Appliance is an enterprise-class web proxy that provides a rich set of additional security features.

The key characteristics of the Cisco Web Security Appliance include web proxy, web cache engine, reputation filtering, malware scanning, URL Filtering, application visibility & control, HTTPS inspection, authentication, rich reporting and tracking and L4TM for filtering outbound Botnet traffic.

The Cisco WSA can be deployed as a hardware appliance or as a virtual appliance.

Cisco WSA Architecture

This topic provides an overview of the Cisco Web Security Appliance architecture.



The Cisco WSA runs on the Cisco proprietary AsyncOS and provides a rich set of management and reporting features.

Using the Reporting tab on the Cisco WSA GUI, administrators can monitor the Cisco WSA by viewing dynamic data on website activity and the Cisco WSA operations.

The different WSA software components installed on every Cisco WSA product are enabled by licenses known as feature keys.

The Cisco WSA requires licenses that are term-based subscriptions of one, three, or five years. The Cisco web security portfolio uses tiered pricing based on a range of users, not devices.

Each of these WSA software components are responsible for a specific function:

Acceptable use policies using Cisco URL filter technology.

Malware defense using four technologies, including web reputation filters, malware scanning, HTTPS inspection, and L4TM.

Data security using two technologies:

- On-box Cisco WSA data security
- Off-box data loss prevention

Four web security software licenses are available: Cisco Web Security Essentials, Cisco Anti-Malware, Cisco Web Security Premium, and Sophos or McAfee Anti-Malware. The major components of each software offering are provided below:

Cisco Web Security Essentials

- Threat Intelligence via Cisco Security Intelligence Operations
- Layer 4 Traffic Monitoring

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

- AVC
- Policy management
- Actionable reporting
- URL filtering
- Third-party DLP integration via ICAP

Cisco Anti-Malware

- Real-time malware scanning

Sophos or Webroot or McAfee Anti-Malware

- Sophos or Webroot or McAfee real-time malware scanning available as a single, a la carte license

Cisco WSP

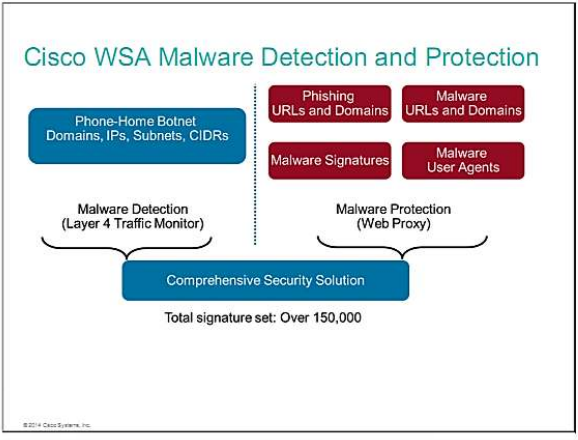
- Web Security Essentials
- Real-time malware scanning

The components interact to provide a comprehensive web security solution.

https://t.me/learningnets

Cisco WSA Malware Detection and Protection

This topic provides an overview of the Cisco Web Security Appliance malware detection and protection.



The security services provided by the Cisco WSA can be divided into two categories: malware detection, which is provided by the L4TM, and malware protection, which is provided by the web proxy.

Malware Detection Provided by the Layer 4 Traffic Monitor

The Cisco WSA L4TM deployment is independent of the Web Proxy deployment.

The Cisco WSA L4TM detects attempts by malware that is installed on client systems to phone home. Using a dynamic database of suspected Botnet command-and-control servers which is updated every 5 minutes by default from the Cisco Security Intelligence Operations, compromised client systems can be easily identified.

The default setting for the L4TM is monitor only. L4TM can also be configured to block suspicious traffic.

Malware Protection Provided by the Web Proxy

Cisco Web Based Reputation Scores are combined with the Cisco Dynamic Vectoring and Streaming engine to provide efficient malware protection.

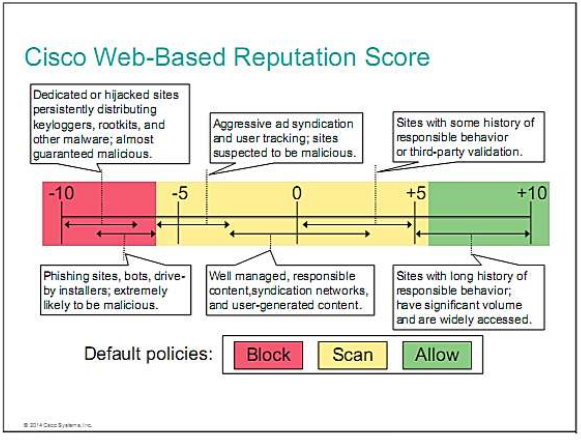
WBRS is enabled by the Cisco common security database, the SenderBase Network, one the largest Email and Web traffic monitoring network in the world. SenderBase tracks more than 50 distinct parameters that are excellent indicators of the URL reputation.

Cisco DVS provides a framework for integration of third-party scanning engines. Scanning engines from Webroot and McAfee are fully integrated into the Cisco Anti-Malware System. These two industry-leading solutions allow you to scan for web-based threats in parallel, providing superior protection and performance.

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

Cisco Web-Based Reputation Score

This topic describes the WBRS.



Malware is pervasive and persistent, and unfortunately, often finds access to the computers inside the enterprise network. Users increasingly work with customers and partners to collaborate on projects and increase productivity. This increased collaboration poses challenges for information security professionals to determine how to prevent malware infections on internal systems from accidentally infecting key partners, and therefore adversely affecting their reputation. The Cisco Web Security Appliance provides inbound malware scanning for internal system protection and outbound malware scanning to protect the reputation of the enterprise.

The Cisco Web Reputation Filters are a security feature that analyze Web server behavior and assigns a reputation score to a URL to determine the likelihood that it contains URL-based malware. It helps protect against URL-based malware that threatens end-user privacy and sensitive corporate information. The Cisco WSA uses URL reputation scores to identify suspicious activity and stop malware attacks before they occur. Web Reputation Filters use statistically significant data to assess the reliability of Internet domains and score the reputation of URLs. Data such as how long a specific domain has been registered, or where a website is hosted, or whether a Web server is using a dynamic IP address is used to judge the trustworthiness of a given URL.

The web reputation calculation associates an URL with network parameters to determine the probability that malware exists. The aggregate probability that malware exists is then mapped to a WBRS between –10 and +10, with +10 being the least likely to contain malware.

You can use Web Reputation Filters with both Web access and HTTPS decryption policies. The WBRS thresholds are a global setting, but may be disabled on a per-policy basis (though it is not recommended).

The WBRS is based on more than just the URL. The input parameters include the following:

URL categorization data

Presence of downloadable code

Presence of long, obfuscated EULAs

Global volume and changes in volume

Network owner information

History of a URL

Age of a URL

Presence on any block lists

Presence on any allow lists

URL typos of popular domains

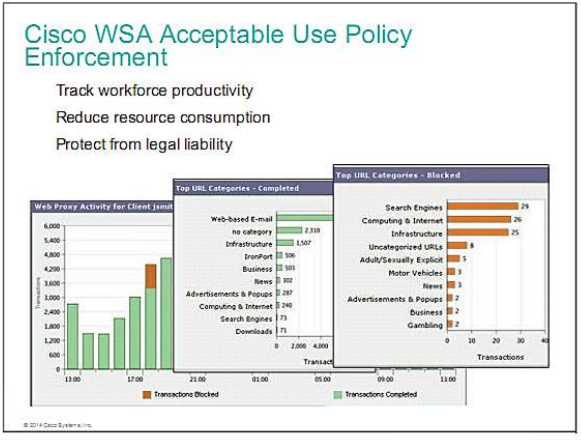
Domain registrar information

IP address information

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

Cisco WSA Acceptable Use Policy Enforcement

This topic describes how the Cisco Web Security Appliance enforces acceptable use policy.



The Cisco WSA provides greater flexibility for organizations in defining and enforcing acceptable use policies. Support for custom URL categories (based on IP addresses, subnets, CIDR ranges, URLs, domains, and regular expressions) provides additional agility to respond to violations.

Automatic, Incremental Web Database Updates

Cisco adds more than 100,000 new sites and 10 million new URLs weekly to ensure ongoing accuracy. By default, the Cisco WSA updates its internal copy of this database every 5 minutes.

Maintain Focus on Core Business Activities

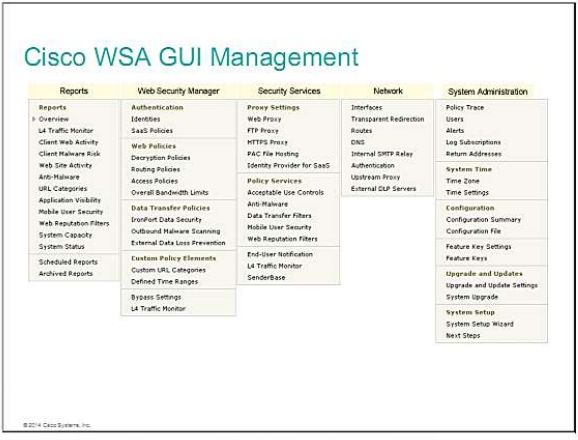
The Internet provides nearly unlimited distraction opportunities. Cisco URL filters allow organizations to implement corporate-specific policies to keep employees focused on core business activities using granular, user, and group-based policies that are applied dynamically. In addition, it allows organizations to maintain better control over resource costs, such as network bandwidth and IT staff time.

Control Legal Liabilities

By instituting appropriate web usage guidelines, corporations using Cisco URL filters can improve compliance, providing a concrete implementation of critical corporate acceptable use policies.

Cisco WSA GUI Management

This topic describes the primary management method of the Cisco Web Security Appliance.



The Cisco WSA is an easy-to-manage platform with a management GUI organized into these main menus:

Reports: This menu allows you to schedule and generate reports.

Web Security Manager: Here you configure various WSA policies.

Security Services: This menu allows global configuration of security services. An example includes the enabling or disabling of URL filters for all policies.

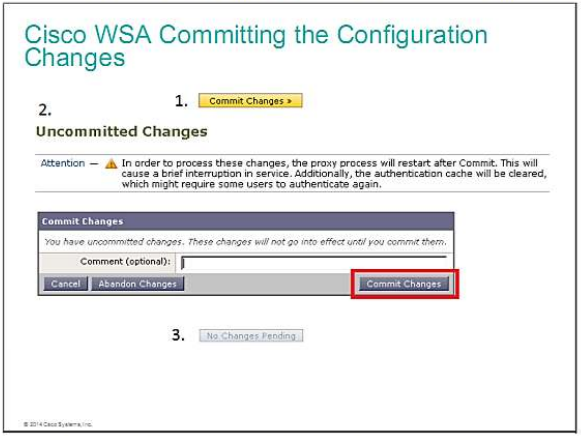
Network: In this menu, you perform network configuration, such as interface IP addresses and routing, global authentication configuration, such as the hostname or IP address of authentication servers and etc...

System Administration: It offers a wide range of WSA administration tasks. Examples include: creating users, installing licenses ("feature keys"), setting the time zone, managing configuration files and etc..

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

Cisco WSA Committing the Configuration Changes

This topic describes how to commit configuration changes on the Cisco Web Security Appliance.



When you change the configuration of the Cisco WSA, you must commit the changes before they go into effect. Or, you can choose to clear the changes you have made if you do not want to commit them.

Note	When you commit some Cisco WSA configuration changes, the Cisco WSA must restart for the changes to take effect.

Commit changes in the Web GUI using the **Commit Changes** button in the upper right corner of the Web interface. You can make multiple configuration changes before you commit all of them. When you make a change, the **Commit Changes** button color is yellow.

To commit changes made in the web interface:

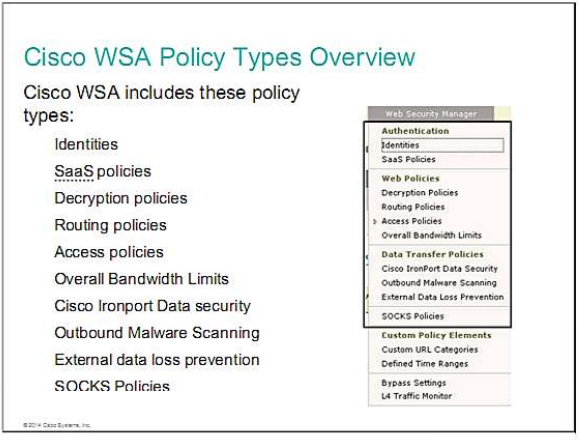
1. Click the **Commit Changes** button.
2. The **Uncommitted Changes** page appears. Enter comments in the Comment field if you choose. Click the **Commit Changes** button.
3. When there are no changes to commit, the button color is gray and the button text is **No Changes Pending**.

Commit changes in the CLI using the **commit** command. Most configuration changes you make in the CLI are not effective until you issue the **commit** command.

https://t.me/learningnets

Cisco WSA Policy Types Overview

This topic describes the policy types in Cisco Web Security Appliance.



Cisco WSA differentiates among several policy types:

Identities are used to classify the traffic/transactions into different groups so different policies can be applied based on the identity.

SaaS policies are used to control access to third-party software service providers, such as Salesforce, Google Apps, and WebEx.

Decryption policies are used to determine how to treat HTTPS traffic.

Routing policies are used to determine which traffic should be sent to which upstream (explicit forward) proxy. Two common use cases for routing policies are as follows:

- Forward a particular type of traffic to particular upstream proxies to enhance performance and optimize caching.
- Forward specific traffic to a partner reverse proxy.

Access policies determine whether to allow, block or redirect HTTP and decrypted HTTPS transactions.

The Cisco WSA controls web traffic based on the access policies that you create for groups of transaction requests:

- Allow: Permits the connection without interruption.
- Block: Does not permit the connection and instead displays an end user notification page explaining the reason for the block.
- Redirect: Does not allow the connection to the originally requested destination server and instead connects to a different specified URL.

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

- Warn: In addition to using the Cisco WSA appliance to block traffic to certain websites, you can also use it
  to warn users that a site does not meet the organization's acceptable use policies and allow them to continue if they choose.
- Monitor: All actions except Monitor are final actions. A final action is an action that causes the Cisco WSA to stop comparing the transaction to the rest of the control settings. The Monitor action is an intermediary action. The Cisco WSA continues comparing the transaction to the other control settings to determine which final action to apply.

Overall Bandwidth Limits can be used to define an overall limit for all users on the network for the supported application types. The overall bandwidth limit affects the traffic between the Cisco WSA and the Web servers. It does not limit traffic served from the Cisco WSA Web cache. You might want to define an overall bandwidth limit to restrict the amount of network traffic used for high traffic sites, such as streaming media sites.

Cisco Ironport Data security policies and External Data Loss Prevention policies are used to restrict outbound traffic.

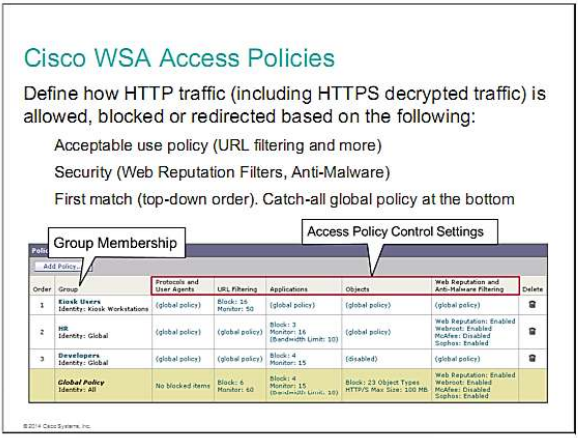
Outbound Malware Scanning policies are used to determine which outbound traffic should be scanned for malware, and which action should be taken if malware is detected.

Socket Secure (SOCKS) polices are used to process SOCKS traffic. SOCKS policies are the equivalent of access policies to control SOCKS based client/server applications, including Bloomberg Terminals. Cisco WSA SOCKS proxy only supports version 5 of the SOCKS protocol. SOCKS version 4 is not supported.

Note This course will mainly focus on Identity, Access, Decryption, Outbound Malware Scanning and Cisco Ironport Data Security/External DLP policy configurations and will not cover all the other policy configurations. Please refer to the Cisco WSA User Guide for more configurations information about the other policies.

Cisco WSA Access Policies

This topic describes the Cisco Web Security Appliance access policies.



Cisco WSA access Policies determine how to treat HTTP requests. There are five sets of access policy control settings:

Protocols and User Agents: This setting is for the port and protocol of the HTTP request (for example: block FTP over HTTP).

URL Filtering: For each custom and predefined URL category, a specific action can be specified.

Applications: You can block particular applications such as Yahoo IM or WebEx, or classes of applications such as peer-to-peer. Also, you can impose bandwidth limits on certain types of media.

Objects: The size and MIME type of the object that is contained in the HTTP response.

Web Reputation and Anti-Malware Filtering: Leverages Cisco expertise and database of web reputation and malware information.

You can apply different policy actions to specified access policy groups by using different group membership matching criteria for each access policy. Group membership criteria is matched based on identities. You can map different identities to different access policy groups. In the example shown in the figure, different policy actions can be applied to each access policy group (Kiosk Users, HR and Developers).

The access policy groups are inspected in order (top to bottom) to determine to which access policy group the transaction belongs:

First match (top-down order)

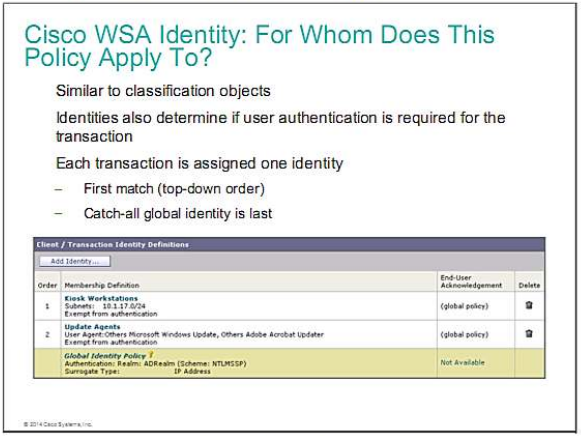
Transactions that do not match any user-defined access policy group are assigned to the catch-all global policy at the bottom.

You can also specify which ports the Cisco WSA monitors for the HTTP transactions.

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

Cisco WSA Identity: For Whom Does This Policy Apply To?

This topic describes the identities in Cisco Web Security Appliance.



Identities are objects administrators create in order for the Cisco WSA to classify the traffic/transactions.

Before a transaction is matched to an access policy group, it is first assigned an identity. A client request (transaction) always has one, and only one, identity. Identity membership is evaluated in order (as the identities appear in the GUI). Client requests (transactions) that do not match any user-defined identity are assigned the global identity.

Note You map identity to the access policy.

After an identity is assigned, the access policy groups are inspected, in order (top to bottom), to determine to which access policy group the transaction belongs to. Membership in an access policy group may be restricted to one or more identities.

Identity membership criteria are very similar to access policy criteria, but there are two key differences:

Time ranges can be used to determine access policies, but cannot be used to determine the identity of a transaction.

Authenticated users or groups can be used to determine the access policies, but cannot be used to determine the identity of a transaction. This is because the identity is assigned before the user is authenticated.

https://t.me/learningnets

Use of Identities

The key motivations for introducing identities into the Cisco WSA policy framework involves user authentication. When you create an identity, you determine whether the transaction requires user authentication.

Identities that do not require user authentication should be placed above identities that require user authentication as best practice.

The Cisco WSA assigns an identity to every transaction it processes. A global identity applies to all transactions that do not qualify for membership in a user-defined identity.

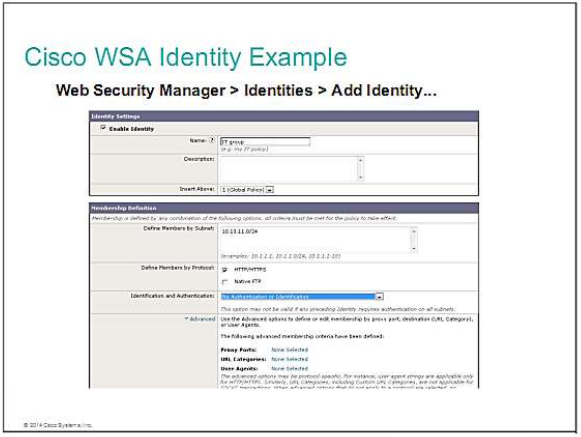
In the figure shown, both the Kiosk Workstations (defined by transaction from the 10.1.17.0/24 subnet) and the Update Agents (i.e Windows and Acrobat update transactions) identities will not require user authentication and the global identity policy will require user authentication.

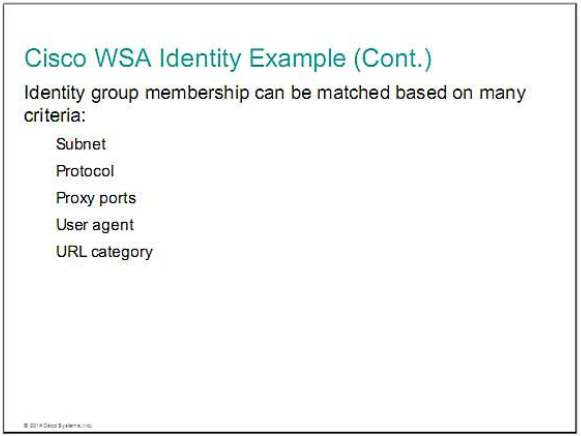
Note The yellow light bulb or key icon next to the identity indicates that the policy requires authentication.

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

Cisco WSA Identity Example

This topic describes how to configure an identity in the Cisco Web Security Appliance.





To add an identity in the Cisco WSA, go to **Web Security Manager > Identities**, and click **Add Identity**...

The following factors can be used to determine the identity that a client request (transaction) matches:

- The subnet of the client making the transaction request
- The protocol that the requested transaction will use

The proxy ports on which the client makes the request

The URL categories associated with the URL requested by the client

The user agents making the request, for example, Internet Explorer, FireFox, Windows update, Acrobat updates.

In the example shown in the figure:

The **IT group** identity is used to match any HTTP or HTTPS transactions from the 10.10.11.0/24 subnet. And this identity does not require any user authentication.

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

Cisco WSA Policy Assignment Using Identity

This topic describes the Cisco Web Security Appliance policy assignment using identity.



You can use the identities you created as a policy group membership requirement for a policy such as access policy, decryption policy and other policies. This is how the Cisco WSA can match transactions to the specific policy such as the specific access policy.

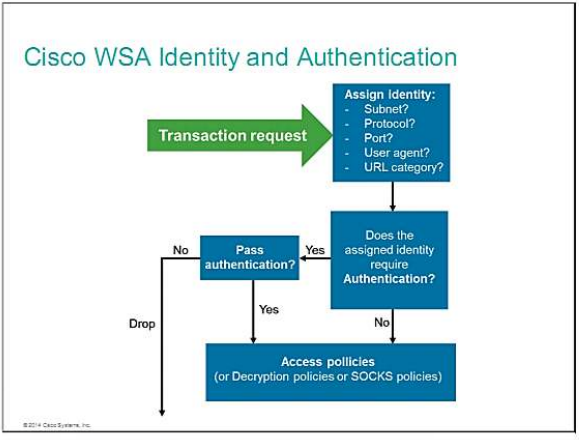
The policies are inspected in order (top to bottom) to determine to which policy group the transaction belongs to. Transactions that do not match any of the user defined policy groups are assigned the global policy.

In the example shown in the figure:

An access policy group named **IT Group Access Policy** was created by referencing the **IT group** identity as the access policy group membership matching criteria.

Cisco WSA Identity and Authentication

This topic describes identity and authentication in Cisco Web Security Appliance.



The flow chart in the figure shows how the Cisco WSA processes an incoming transaction. First, it will match the transaction to an identity. Second, based on the matched identity, determines if user authentication is required. If user authentication is required, and if the user authentication fails, drop the connection. If the user authentication is successful, match the transaction to the access policy group. If user authentication is not required, match the transaction to the access policy group.

It is the identity that determines whether user authentication is required, and against which realm the authentication should be performed. Therefore, you cannot use any information acquired during the authentication process to assign an identity to a transaction. Matching the transaction to its identity occurs before the user authentication process.

By default, if a transaction requires user authentication, and authentication fails, the client is denied access. However, you can configure the identity to support guest privileges for users failing authentication.

Identities serve these purposes:

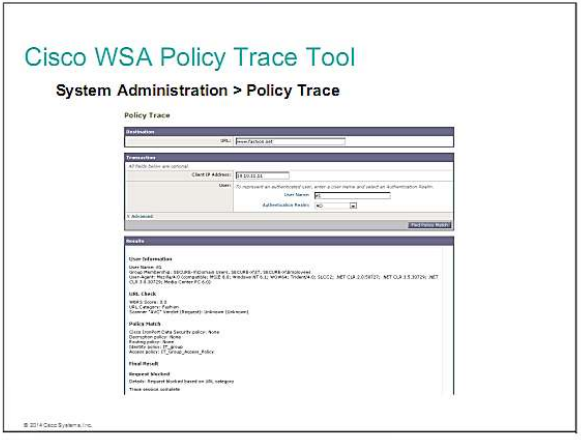
1. Group transaction requests for applying access or decryption policies.
2. Specify if user authentication is required or not for members of the identity.

For example, if you know that end users is using Internet Explorer to accesses the XYZ domain and those transaction should not require the users to be authenticated, you might create an identify for Internet Explorer (user agent). The identity for the Internet Explorer (user agent) does not require authentication. In addition, you can create an access policy that defines transactions with Internet Explorer (user agent) identity as the group member and only allows access to URLs within the XYZ domain.

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

Cisco WSA Policy Trace Tool

This topic describes the Cisco Web Security Appliance policy trace tool.



The **System Administration > Policy Trace** tool allows you to test the effect of the configured policy on a hypothetical transaction. The Cisco WSA Web interface includes policy trace tool that traces a particular client request and details how the Cisco WSA processes the request. The Cisco WSA evaluates the request against all committed Access, Decryption, Cisco IronPort Data Security, Outbound Malware Scanning, and Routing Policies and calculates other attributes, such as the Web reputation score.

The policy trace tool allows administrators to simulate client requests as if they were made by the end users and describes the Cisco WSA behavior. It can be a powerful troubleshooting or debugging tool.

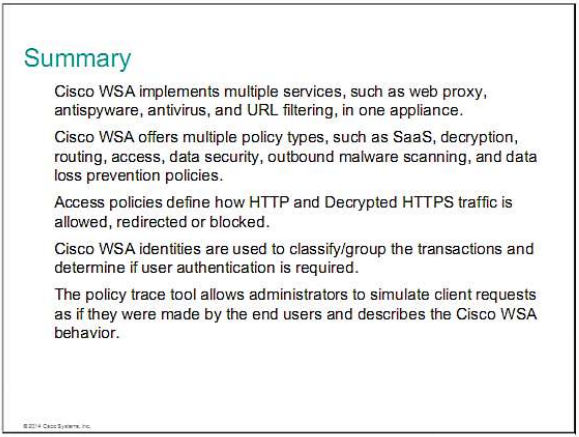
For example, assume that you configured your access policies to block downloads, during peak business hours, that are larger that 100 MB, by anyone other than IT staff. The policy trace tool allows you to "pretend" that you are a particular user, at a particular time, downloading a particular type of file.

In the example shown in the figure, the policy trace simulate the it1 AD user from the 10.10.11.11 IP address initiating a HTTP connection to www.fashion.net. The result shows that transaction matching the IT group identity and the IT Group Access Policy and the request was blocked by the IT Group Access Policy based on the URL category.

https://t.me/learningnets

Summary

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



References

For additional information, refer to these references:

Cisco Systems, Inc. Cisco IronPort AsyncOS for Web User Guide. http://www.cisco.com/en/US/docs/security/wsa/wsa7.5/user_guide/WSA_7.5.0_UserGuide.pdf

Cisco Systems, Inc. Web Security Deployment Guide. http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns982/sba_webSec_dg.pdf

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

Lesson 2

Integrating the Cisco Web Security Appliance

Overview

Determining how web traffic will be sent to the Cisco Web Security Appliance is often perceived as the most challenging portion of the Cisco WSA integration since it involves devices outside the WSA.

The Cisco WSA is not deployed in an inline manner where it would sit between the client and the website the client is trying to access. Therefore, an alternative method to divert or redirect web traffic to the Cisco WSA must be used. There are two possible methods to accomplish this redirection of traffic to the Cisco WSA: explicit proxy and transparent proxy. This lesson describes both approaches.

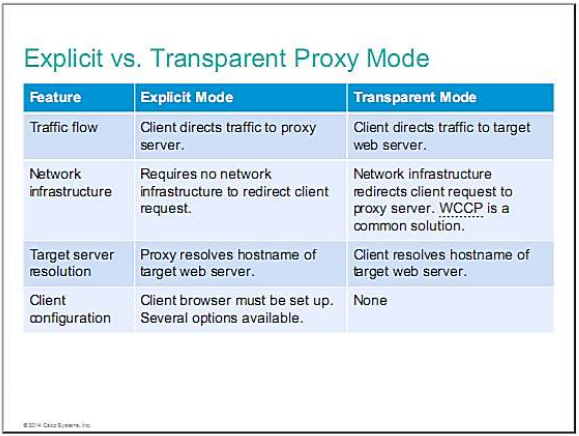
Upon completing this lesson you will able to meet these objectives:

- Contrast the Cisco WSA proxy modes
- Describe the client configuration for the explicit proxy mode
- Describe the PAC files
- Describe the PAC file deployment options
- Describe the PAC file hosting on the Cisco WSA
- Describe the traffic redirection options in the transparent proxy mode
- Describes required steps to connect the Cisco WSA to a WCCP router.
- Describe how to verify operation of WCCP.

https://t.me/learningnets

Explicit vs. Transparent Proxy Mode

This topic contrasts the Cisco Web Security Appliance explicit and transparent proxy mode.



An explicit proxy deployment is possible when a client proxy-aware application, such as a web browser, has a configuration area for proxy settings. The Cisco WSA can then be referred to as a proxy. This method is typically combined with a firewall that restricts web traffic that does not originate from the IP of the Cisco WSA to prevent users from circumventing web policy controls and accessing the Internet directly. From an operational standpoint, this method introduces the least amount of complications. However, from a deployment standpoint, it presents challenges as to how an administrator will configure every client with the Cisco WSA proxy settings in their browsers.

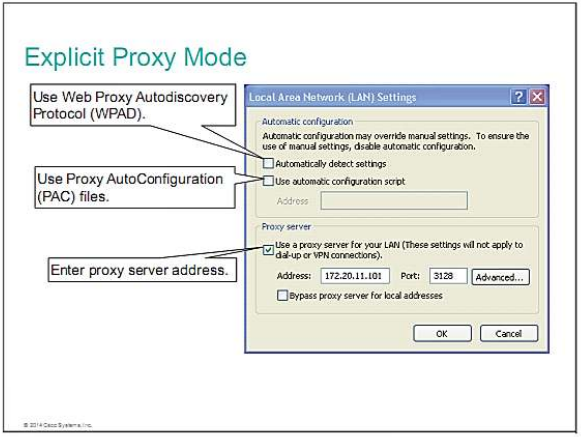
The other deployment option is a transparent proxy deployment, where all port 80 (and possibly port 443) traffic is redirected to the Cisco WSA by another network device at some network choke point. This is easily accomplished using the Cisco ASA adaptive security appliance or possibly any other network device that supports WCCP v2 redirection.

It is also possible to use both options at the same time (explicit and transparent proxy) on the same Cisco WSA.

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

Explicit Proxy Mode

This topic describes the client configuration for the explicit proxy mode.



You must configure all client applications, such as web browsers and FTP clients, used on the network to point to the Web Proxy. In general, you have three configuration choices:

Automatically Detect Settings. This method uses WPAD Protocol, which is a method used by web browsers, primarily Internet Explorer, to locate a PAC file automatically and use this to configure the browser settings.

Use Automatic Configuration Script. Input the URL for a PAC file. The PAC file is written in JavaScript and determines the location of the proxy server or servers. PAC files can determine the proxy based on the destination website and can include whitelists and blacklists.

Enter the Proxy Server Address into the Browser. This is the example shown in the slide (for Internet Explorer). The hostname or IP address of the proxy server is entered into the browser. Microsoft GPOs can be used to allow central control of this settings in an Active Directory environment.

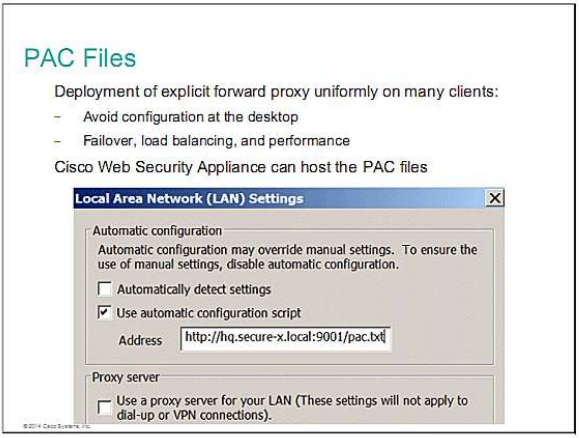
To configure the explicit forward mode in the client browser:

To configure Firefox to use an explicit forward mode, choose **Tools > Options > Advanced > Network > Connection > Settings > Manual proxy configuration**.

To configure Internet Explorer to use an explicit forward mode, choose **Tools > Internet Options > Connections > LAN Settings > Use a Proxy Server.**

PAC Files

This topic describes the PAC files.



PAC file is a text file that defines how web browsers can automatically choose the appropriate proxy server for fetching a given URL. When you use a PAC file, you only need to configure each browser once with the PAC file information.

Then, you can edit the PAC file to add, delete, or change Web Proxy connection information without editing each browser. This way you can configure the proxy information about your network in a centralized location and update it easily.

You might want to use a PAC file for the following reasons:

Centralized management: you can manage the PAC file in a single, central location.

Complex network environment: if the network of proxy servers is complicated, you can create a PAC file to accommodate different server and client needs.

Changing network environment: if your network environment is likely to change in the future, you can easily add, edit, or delete proxy servers in the PAC and have the changes automatically affect all browsers.

Failover: if you have multiple proxy servers, you can provide redundancy in case of failure. You can either program the PAC file to be redundant, or if a failure occurs, change the PAC file to use a different proxy server.

Load balancing: If you have multiple proxy servers, you can use the PAC file to specify which requests go to which proxy server. For example, you might want users on one subnet to use a particular proxy and users on a different subnet to use a different proxy.

To use a PAC file, you must publish the PAC file in a location that can be accessed by each browser that needs to access it. When you configure a browser to use a PAC file, you can use either of the following methods:

Enter the PAC file location.

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

Detect the PAC file location automatically.

You can place the PAC file in the following locations:

Local machine: you can place the PAC file on each client machine and configure the browsers to use it. You might want to use a local PAC file to test a PAC file before deploying it to the entire organization. Enter the path in the browser configuration. The path you enter depends on the browser type.

Web server: You can place the PAC file on a web server that each client machine can access. For example, you can place the PAC file on an Apache or Microsoft IIS web server. Enter the URL in the browser configuration.

Web Security appliance: you can place the PAC file on the Web Security appliance. You might want to put the PAC file on the Web Security appliance to verify every client machine can access it within the network. Enter the URL in the browser configuration.

When troubleshooting the PAC file operation, you can download the PAC file (as an ordinary HTTP text file) to the browser manually by entering the URL for the PAC file into the browser navigation toolbar:

1) Go to the connection settings and copy the PAC file URL.
2) Paste the URL into the browser navigation toolbar of a different browser. (Use a browser that is not using the PAC file.)
3) View the PAC file and identify any errors that you see.

The PAC file is written in Javascript. Whenever a PAC file is downloaded to the browser, the Javascript is parsed. When the browser is used, the Javascript is run. Therefore, Javascript errors may appear when the PAC file is first downloaded, or they may appear when the browser happens to execute a code path leading to a runtime Javascript error.

To troubleshoot Javascript:

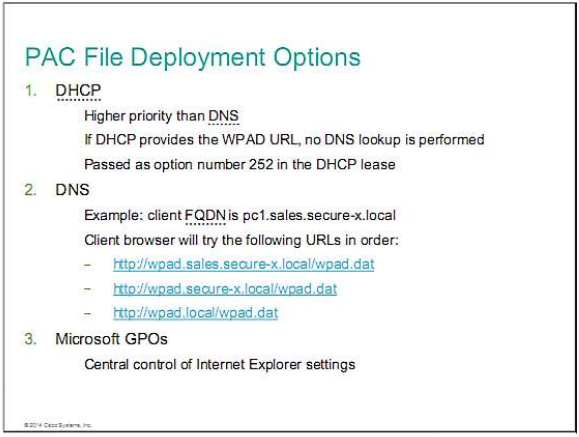
In Firefox: Go to **Tools > Error Console**

In Internet Explorer: Click the error icon that appears in the left-hand side of the status bar. A dialog box appears. Click **Show Details** in the dialog box.

https://t.me/learningnets

PAC File Deployment Options

This topic describes the PAC file deployment options.



If a browser supports the WPAD Protocol, you can configure it to automatically detect the PAC file location. WPAD is a protocol that allows the browser determine the location of the PAC file using DHCP and DNS lookups.

Before fetching its first page, a web browser configured to automatically detect the PAC file location tries to find the PAC file using DHCP or DNS. Therefore, to use WPAD, you must set up either a DHCP server or a DNS server to direct web browser requests to the PAC file on a network server. However, not all browsers support DHCP to find the PAC file using WPAD.

Most enterprises use DHCP to configure client systems. DHCP supports the provisioning of the PAC file configuration without touching the client system.

DNS search is the next option. For example, if the FQDN of the client is pc1.sales.secure-x.local, the browser will try the following URLs in order:

1) http://wpad.sales.secure-x.local/wpad.dat
2) http://wpad.secure-x.local/wpad.dat
3) http://wpad.local/wpad.dat

Microsoft GPOs can be used to provision Active Directory domain computers with settings required for Internet Explorer.

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

PAC File Hosting on Cisco WSA

This topic describes the PAC file hosting on the Cisco Web Security Appliance.



Instead of using a separate web server, the Cisco WSA can host PAC files. Multiple PAC files may be hosted on a single appliance. The PAC file to be used is configured on the browser.

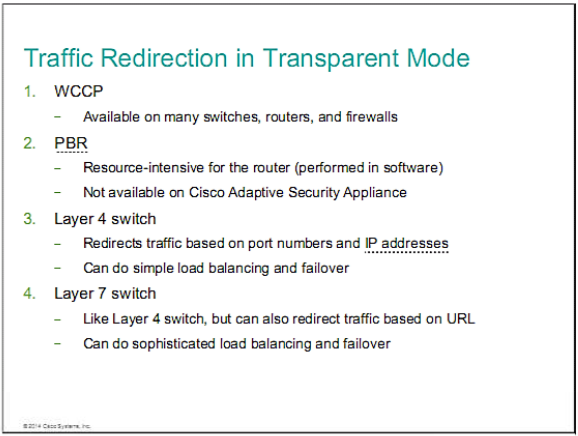
You can specify one or more PAC file server ports for the appliance to listen for PAC file requests. The client request and server response to download a PAC file is the same as any other HTTP request. The HTTP response header specifies the MIME type of the PAC file as application/x-ns-proxy-autoconfig.

To host a PAC file on Cisco WSA appliance, navigate to **Security Services > PAC File Hosting** page, and click **Enable and Edit Settings**.

Note	Although, in practice, the PAC file hosted on the Cisco WSA will point to that WSA as an explicit forward proxy, from a theoretical point of view, there is no relation between where that PAC file is hosted and what proxies are referenced in the PAC file.

Traffic Redirection In Transparent Mode

This topic describes the traffic redirection options in the transparent proxy mode.



When the appliance is configured as a transparent proxy, client applications are not aware that their traffic gets redirected to the appliance, and they do not need to be configured to point to the appliance. Transparent mode always requires some mechanism for redirecting HTTP and HTTPS traffic to the Cisco Web Security Appliance. Common approaches include the following:

WCCP: This is available on many network devices, including the Cisco ASA adaptive security appliances, Cisco IOS routers, and switches. When you specify a WCCP device, you need to configure additional settings on the appliance.

PBR: Routers can redirect HTTP and HTTPS traffic using PBR. However, PBR is implemented in software and therefore can be resource-intensive. PBR is not available on Cisco ASA appliances.

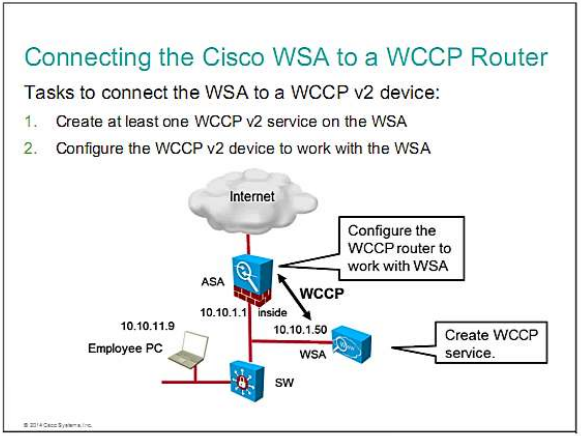
Layer 4 or 7 Switch: You can use a Layer 4 or Layer 7 switch to redirect traffic to the Cisco WSA. When you specify an Layer 4 switch, you only need to specify that the appliance is connected to an Layer 4 switch when you configure the appliance. You do not need to configure anything else on the appliance.

Typically, you configure the appliance to use an Layer 4 switch or a WCCP v2 router during initial system setup. However, you can configure it to use either an Layer 4 switch or a WCCP v2 router anytime after initial setup from the **Network > Transparent Redirection** page.

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

Connecting the Cisco WSA to a WCCP Router

This topic describes required steps to connect the Cisco Web Security Appliance to a WCCP router.



When you connect the appliance to a WCCP v2 device (Cisco Adaptive Security Appliance in the example), you must perform the following tasks:

1. You must create at least one WCCP service on the appliance. A WCCP service is an appliance configuration that defines a service group to a WCCP v2 device (Cisco ASA in this example). It includes information such as the service ID and ports used. Service groups allow a web proxy to establish connectivity with a WCCP v2 device and to handle redirected traffic from the WCCP v2 device.
2. After you create a WCCP service, you must configure the WCCP v2 device (Cisco ASA in this example) to work with the Web Security appliance.

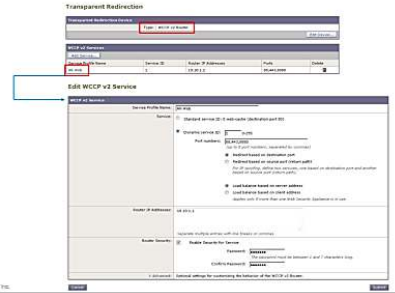
In the figure, EmloyeePC (IP address 10.10.11.9) is browsing the Internet. HTTP traffic originating from EmployeePC will be a subject of WCCP redirection on ASA.

Note	The only topology that the adaptive security appliance supports is when client and cache engine are behind the same interface of the adaptive security appliance and the cache engine can directly communicate with the client without going through the adaptive security appliance.

Connecting the Cisco WSA to a WCCP Router (Cont.)

Configuration on WSA:

Network > Transparent Redirecton



A WCCP service is an appliance configuration that defines a service group to a WCCP v2 router, which is Cisco ASA in the example. It includes information such as the service ID and ports used. Service groups allow a web proxy to establish connectivity with a WCCP router and to handle redirected traffic from the router.

Create WCCP services on the **Network > Transparent Redirection** page. The WCCP services you create determine how you configure the WCCP routers. To add a WCCP service, click **Add Service.**

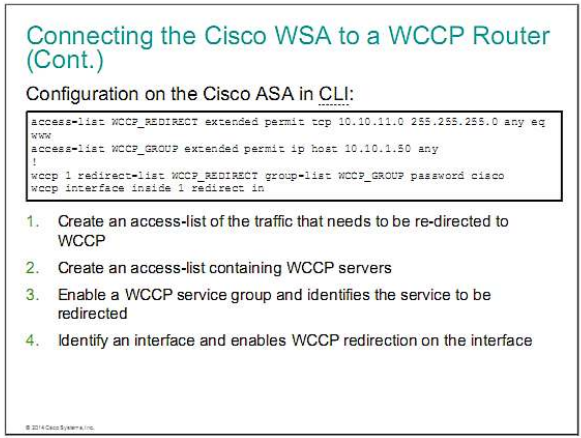
WCCP service is configured with these parameters:

Service ID is set to 1 (this needs to be matched with service group ID on Cisco ASA)

Router IP address is set to 10.10.1.1 (IP address of ASA inside interface)

Router security is enabled and password **cisco** is used (password needs to be matched on Cisco ASA)

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



This is the explanation of configuration needed on the Cisco ASA.

1. Create an access-list of the traffic that needs to be re-directed to WCCP. In the example, HTTP traffic from the subnet 10.10.11.0/24 wil be subject of WCCP predirection

```
access-list WCCP_REDIRECT extended permit tcp 10.10.11.0 255.255.255.0 any eq www
```

2. Create an access-list containing WCCP servers. In the example, access list contains WSA host.

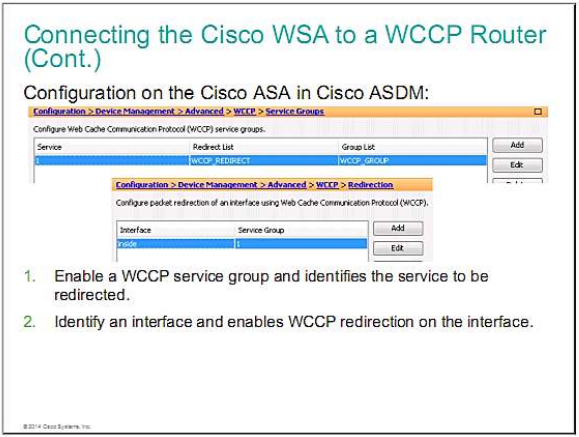
```
access-list WCCP_GROUP extended permit ip host 10.10.1.50 any
```

3. Enable a WCCP service group and identifies the service to be redirected. Also defines which cache engines can participate in the service group, and what traffic should be redirected to the cache engine. The standard service is web-cache, which intercepts TCP port 80 (HTTP) traffic and redirects that traffic to the cache engines, but you can identify a service number between 0 and 254 (1 in the example). Password for WCCP redirection on ASA should match password set for transparent redirection on WSA.

```
wccp 1 redirect-list WCCP_REDIRECT group-list WCCP_GROUP password cisco
```

4. Identifies an interface and enables WCCP redirection on the interface. In the example, HTTP traffic that enters the inside interface to a service group 1 is redirected.

```
wccp interface inside 1 redirect in
```

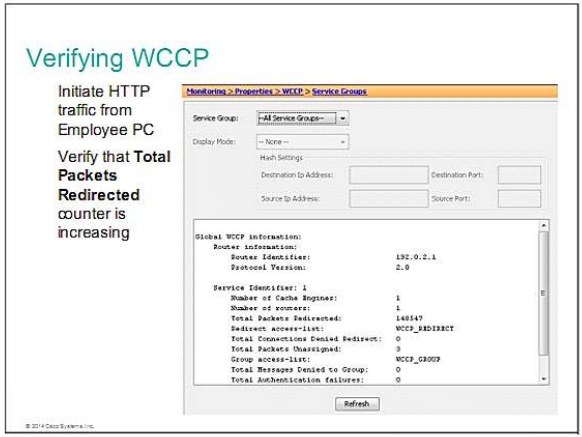


The slide shows configuration of WCCP redirection on ASA using Cisco Adaptive Security Device Manager. Slide assumes both access lists (WCCP_REDIRECT and WCCP_GROUP) are already configured. The upper figure shows how to enable a WCCP service group and identify the service to be redirected. The lower figure enables WCCP redirection on the inside interface.

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

Verifying WCCP

This topic describes how to verify operation of WCCP.



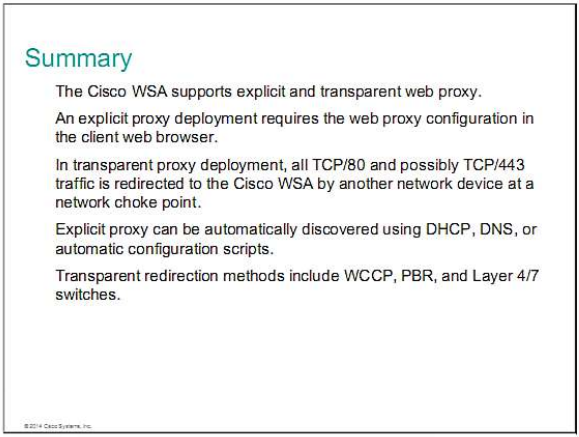
To verify WCCP operation in Cisco Adaptive Security Device Manager, navigate to **Monitoring > Properties > WCCP > Service Group**. Observe the number for **Total Packets Redirected** counter. Initiate HTTP traffic from **Employee PC** and observe the counter again, which should be increasing. The similar verification could be done in Cisco Adaptive Security Appliance CLI using **show wccp** command as shown below.

```
HQ-ASA# show wccp
Global WCCP information:
    Router information:
        Router Identifier:                  192.0.2.1
        Protocol Version:                   2.0
    Service Identifier: 1
        Number of Cache Engines:            1
        Number of routers:                  1
        Total Packets Redirected:           148983
        Redirect access-list:               WCCP_REDIRECT
        Total Connections Denied Redirect:  0
        Total Packets Unassigned:           3
        Group access-list:                  WCCP_GROUP
        Total Messages Denied to Group:     0
        Total Authentication failures:      0
        Total Bypassed Packets Received:    0
```

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

Summary

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



References

For additional information, refer to these references:

Cisco IronPort AsyncOS for Web User Guide

http://www.cisco.com/en/US/docs/security/wsa/wsa7.5/user_guide/WSA_7.5.0_UserGuide.pdf

http://www.cisco.com/en/US/docs/solutions/SBA/February2013/Cisco_SBA_BN_WebSecurityUsingCiscoWSADeploymentGuide-Feb2013.pdf

Web Security Deployment Guide

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

Lesson 3

Configuring Cisco Web Security Appliance Identities and User Authentication Controls

Overview

Identity is used to group the clients transaction requests for applying access or decryption policies. User authentication is the process of confirming the identity of a user. When you create an identity, you determine whether the transaction requires the user to be authenticated.

When you enable authentication, the Cisco Web Security Appliance verifies the identity of clients on the network before allowing them to connect to a destination server. This lesson describes the how to configure identities and user authentication on the Cisco WSA.

Upon completing this lesson, you will be able to meet these objectives:

- Describe how to configure identities to group client transactions.
- Describe how to configure policy group and assign identity to it
- Identify the need for WSA user authentication
- Describe the authentication protocols and proxy modes
- Describes basic authentication operations in explicit proxy and transparent proxy mode
- Describe the configuration of the realms and realm sequences
- Configure an NTLM realm
- Describe how to join the Cisco WSA to the Active Directory.

https://t.me/learningnets

Describe the global authentication settings

Describes how to configure an identity to require authentication

Describe how to configure transparent user identification.

Describe the creation of LDAP realms for other directories

Describe how user information is stored when using LDAP

Describe how to bind the Cisco WSA to the Directory Server

Describe LDAP group authorization

Describe how to allow guest access to users who fail authentication

Describe how to test Cisco WSA authentication settings

Describe how are authenticated users represented in the reports

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

Configure Identities to Group Client Transactions

This topic describes how to configure identities to group client transactions.



To control web traffic on the network and protect your network from web based threats, the Cisco Web Security Appliance needs to identify who is trying to access the web. Users can be identified by different criteria, such as their machine address or authenticated user name. The Cisco WSA can apply different actions to transactions based on who is submitting the request.

To identify who is accessing the web, you create Identities in the Cisco WSA. An Identity is a policy that identifies and groups users. An Identity addresses the question, "who are you?"

Identities are the only policy where you define whether or not authentication is required to access the web. However, Identities do not specify a list of users who are authorized (allowed) to access the web. You specify authorized users in the other (non-Identity) policy types, like in an access policy.

All other policy types use an Identity as the basis to determine which policy group applies to the transaction. That means you can create a single Identity and use it multiple times in the non-Identity policy groups.

When a client sends a request to a server, the Cisco WSA receives the request, evaluates it, and determines to which Identity group it belongs.

To determine the Identity group that a client request matches, the Cisco WSA follows a very specific process for matching the Identity group membership criteria. During this process, it considers the following factors for group membership:

Subnet: The client subnet must match the list of subnets in a policy group.

Protocol: The protocol used in the transaction, either HTTP/HTTPS or native FTP.

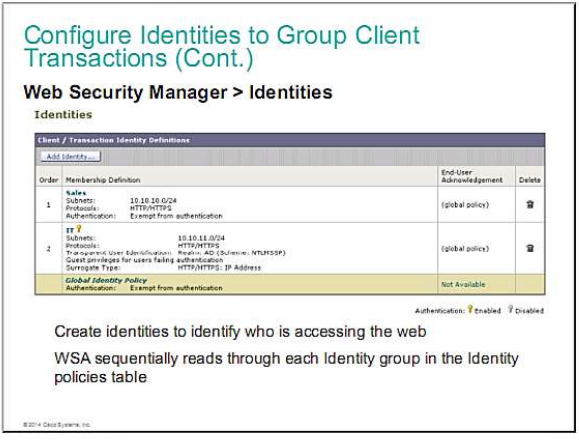
Port: The proxy port of the request must be in the Identity group's list of ports, if any are listed. For explicit forward connections, this is the port configured in the browser. For transparent connections, this is the same as the destination port.

https://t.me/learningnets

User agent: The user agent making the request must be in the Identity group's list of user agents, if any are listed. You might want to group by user agent for user agents that cannot handle authentication and you want to create an Identity that does not require authentication.

URL category: The URL category of the request URL must be in the Identity group's list of URL categories, if any are listed. You might want to group by URL destination category if you create different authentication groups based on URL categories and want to apply them to users depending on the website categorization.

Authentication requirements: If the Identity group requires authentication, the client authentication credentials must match the Identity group's authentication requirements.



The Cisco WSA sequentially reads through each Identity group in the Identity policies table. It compares the client request to the membership criteria of the first Identity group. If they match, the Cisco WSA assigns the Identity group to the transaction.

If they do not match, the Cisco WSA compares the client request to the next Identity group. It continues this process until it matches the client request to a user defined Identity group, or if it does not match a user defined Identity group, it matches the global Identity policy. When the Cisco WSA matches the client request to an Identity group or the global Identity policy, it assigns the Identity group to the transaction.

Note When authentication is required for an Identity group, a gold key icon appears next to the Identity group name in the Policies table.

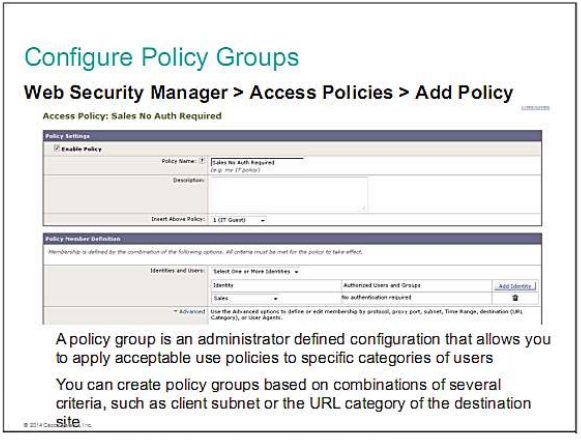
In the example, employees belonging to Sales department with IP subnet 10.10.10.0/24 will not be subject of authentication when they perform HTTP or HTTPS transactions. On the other hand, employees belonging to IT department with IP subnet 10.10.11.0/24 will be authenticated against realm named **AD.** This identity is also configured to enable guest privileges for user failing authentication.

Users that do not match either to **Sales** or **IT** identity, will be matched against global identity policy, which is configured not to authenticate users.

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

Configure Policy Groups

This topic describes how to configure policy group and assign identity to it.

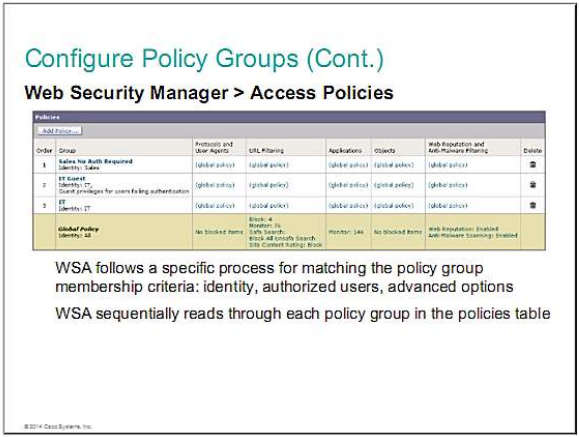


A policy group is an administrator defined configuration that allows you to apply acceptable use policies to specific categories of users. After you create policy groups, you can define the control settings for each group.

You can create as many user defined policy groups as required to enforce the proper access control. The Cisco Web Security Appliance displays policy groups together in a policies table. All policies have a default, global policy group that applies to a transaction if none of the user defined policy groups apply. A global policy group maintains default settings and rules that apply to web transactions not covered by another policy. This group appears in the last row of a policies table, and the Cisco WSA applies its rules last if no other matching occurs.

You can create policy groups based on combinations of several criteria, such as client subnet or the URL category of the destination site. You must define at least one criterion for policy group membership. When you define multiple criteria, the client request must meet all criteria to match the policy group.

https://t.me/learningnets



The policies table is an ordered list of policy groups and the settings you configure for each filtering component. It displays policy groups by row and control settings by column. The control settings you can define vary by policy type.

Any policy group that you create is added as a new row in the policies table. New policy groups inherit global policy settings for each control setting until you override them. To edit policy groups, click the links in each row.

The Cisco WSA sequentially reads through each policy group in the policies table. It compares the client request status to the membership criteria of the first policy group. If they match, the Web Proxy applies the policy settings of that policy group.

If they do not match, the Cisco WSA compares the client request to the next policy group. It continues this process until it matches the client request to a user defined policy group. If it does not match a user defined policy group, it matches the global policy group. When the Cisco WSA matches the client request to a policy group or the global policy group, it applies the policy settings of that policy group.

When the HTTPS Proxy is enabled, the Cisco WSA applies HTTP and decrypted HTTPS requests against the Access Policies.

To determine the policy group that a client request matches, the Web Proxy follows a specific process for matching the group membership criteria. During this process, it considers the following factors for group membership:

Identity: Each client request either matches an Identity, fails authentication and is granted guest access, or fails authentication and gets terminated.

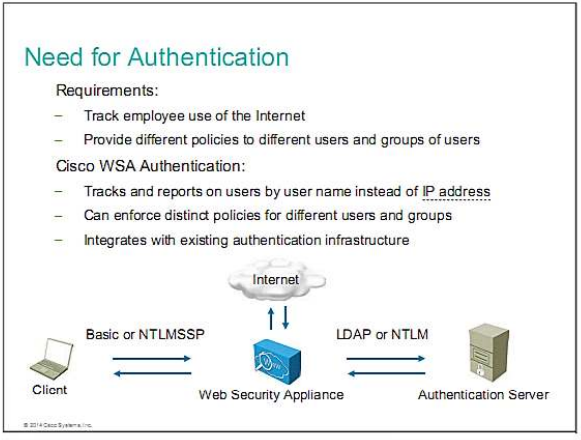
Authorized users: If the assigned Identity requires authentication, the user must be in the list of authorized users in the Access Policy group to match the policy group. The list of authorized users can be any of the specified groups or users or can be guest users if the Identity allows guest access.

Advanced options: You can configure several advanced options for Access Policy group membership. Some options (such as proxy port and URL category) can also be defined within the Identity. When an advanced option is configured in the Identity, it is not configurable in the Access Policy group level.

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

The Need for User Authentication

This topic describes the need for user authentication on the Cisco Web Security Appliance.



The key motivations for introducing identities into the Cisco WSA policy framework involves user authentication. When you create an identity, you determine whether the transaction requires the user to be authenticated.

Authentication is the act of confirming the identity of a user. By using authentication in the Cisco WSA, you can control access to the Web for each user or a group of users. This allows you to enforce the organization's policies and comply with regulations. When you enable authentication, the Cisco WSA authenticates clients on the network before allowing them to connect to a destination server.

By using authentication in the Cisco WSA, you can:

Set up different web access policies by user or group membership against a central user directory.

Enable user tracking, so that when a user violates an acceptable use policy, the Cisco WSA can match up the user with the violation instead of just using an IP address.

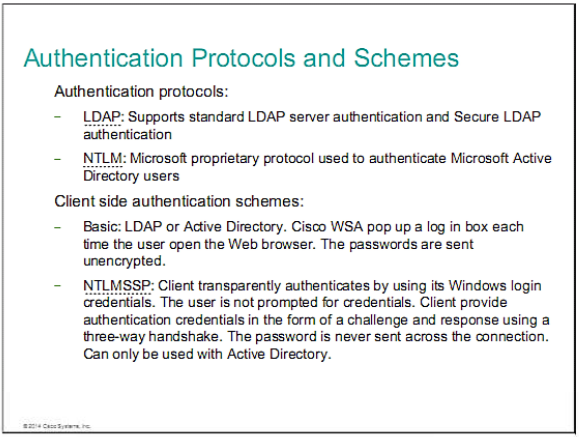
Enable compliance reporting.

To enable authentication, you must create at least one authentication realm. An authentication realm is a set of authentication servers (or a single server) supporting a single authentication protocol with a particular configuration. By creating authentication realms and sequences, you can configure the Cisco WSA to use one or more authentication servers for authenticating clients on the network.

https://t.me/learningnets

Authentication Protocols and Schemes

This topic describes the authentication protocols and schemes.



The Cisco Web Security Appliance supports two different authentication protocols: LDAP and NTLM. Since most organizations will have an Active Directory server, they will be using NTLM.

NTLM, a Microsoft proprietary protocol, is used to authenticate users who exist in Microsoft Active Directory. The NTLM protocol uses a challenge-response sequence of messages between the client and the Active Directory server. You can use either NTLMSSP or Basic authentication schemes on client side.

With LDAP authentication, the Cisco WSA uses the LDAP Bind operation to query an LDAP-compatible authentication server. The appliance supports standard LDAP server authentication and secure LDAP authentication.

In addition to the preceding protocols, the Cisco WSA supports the following client side authentication schemes:

Basic: The Cisco WSA will pop up a log in box each time the user open the Web browser. Allows a client application to provide authentication credentials in the form of a username and password when it makes a request. You can use the Basic authentication scheme with either an LDAP or Active Directory server. Credentials are sent unencrypted.

NTLMSSP: The client transparently authenticates by using its Windows login credentials. This is called "single sign-on (SSO)". The user is not prompted for credentials. Allows the client application to provide authentication credentials in the form of a challenge and response using a three-way handshake between the Cisco WSA, the user workstation and the Active Directory server. The password is never sent across the connection. It uses a binary message format to authenticate clients that use the NTLM protocol to access network resources. The NTLMSSP authentication scheme can only be used with an Active Directory server. This method is more secure than Basic and less intrusive to the end user.

- The client browser must be configured to trust the Cisco WSA to send it's credentials transparently to the Cisco WSA. Performing the needed browser configuration to enable SSO is not covered in this course.

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

Proxy mode and authentication method:

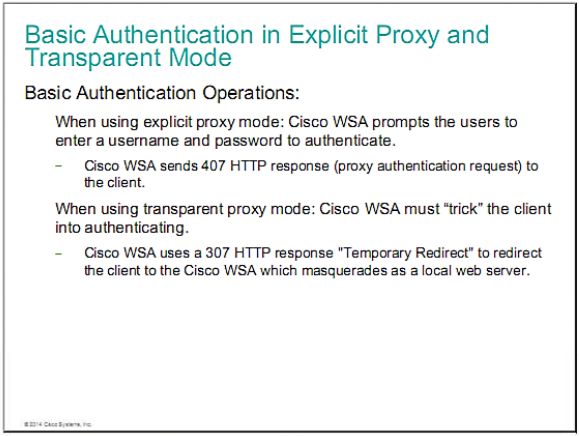
When a client explicitly sends a web page request to the Cisco WSA deployed in explicit proxy mode, the Cisco WSA prompts the users to enter a username and password to authenticate. The Cisco WSA replies to the client HTTP request with a 407 HTTP response "Proxy Authentication Required." This status informs the client that it must supply valid authentication credentials to access web resource.

Not all client applications support authentication, some client applications have no way to prompt the users to enter their usernames and passwords. Some applications might also have issues when the Cisco WSA is deployed in transparent proxy mode because the application tries to run non-HTTP traffic over port 80 and cannot handle an attempt by the Cisco WSA to authenticate the user. Using SSO or transparent authentication, the Cisco WSA can obtain the user credentials from another trusted source, assumes that the user has already been authenticated by the trusted source without prompting the user to enter a user name and password.

https://t.me/learningnets

Basic Authentication in Explicit Proxy and Transparent Proxy Mode

This topic describes basic authentication operations in explicit proxy and transparent proxy mode.



Explicit proxy mode with basic authentication example:

When a client explicitly sends a web page request to the Cisco Web Security Appliance deployed in explicit forward mode, the Cisco WSA can reply to the client with a 407 HTTP response "Proxy Authentication Required." This status informs the client that it must supply valid authentication credentials to access web resources.

Explicit forward mode proxy authentication is easy to understand and troubleshoot. The client "knows" that it is working with a proxy, so when the proxy responds to an HTTP request with a 407 (proxy authentication request), the client will accept the authentication request.

Similarly, with HTTPS, a client that is using an explicit forward proxy will send a CONNECT request to the proxy. If the client receives a 407 from the proxy, it will accept the authentication request.

Transparent proxy mode with basic authentication example:

The 407 HTTP response "Proxy Authentication Required" is allowed from the Cisco WSA when it is in explicit proxy mode. However, when the Cisco WSA is deployed in transparent proxy mode, the Cisco WSA existence is hidden from client applications on the network. Therefore, the Cisco WSA cannot return a 407 response.

To address this problem, the basic authentication in transparent proxy mode process comprises these steps:

Client sends a request to a web page and the Cisco WSA transparently intercepts it.

The Cisco WSA uses a 307 HTTP response "Temporary Redirect" to redirect the client to the Cisco WSA which masquerades as a local web server. This transaction is recorded in the Cisco WSA access logs with "TCP_DENIED/307".

Client sends the request to the redirected URL.

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

The Cisco WSA sends a 401 HTTP response "Authorization required."

User is prompted for credentials and enters them.

Client sends the request again, but this time with the credentials in an "Authorization" HTTP head.

The Cisco WSA confirms the credentials, tracks the user by IP address or with a cookie, and then redirects the client to the originally requested server. The Cisco WSA can be configured to use either IP addresses or cookies to track the authenticated users.

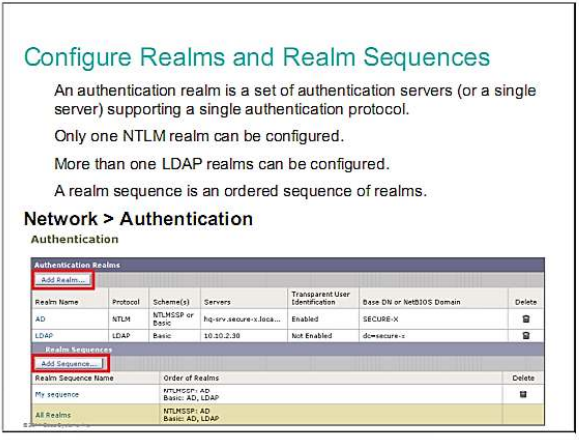
If the client requests the original web page again, the Cisco WSA transparently intercepts the request, confirms the user by IP address or cookie, and returns the requested page.

If the client tries to connect to another web page and the Cisco WSA tracked the user by IP address, the Cisco WSA confirms the user by IP address and returns the requested page.

https://t.me/learningnets

Configure Realms and Realm Sequences

This topic describes the configuration of the realms and realm sequences.



An authentication realm is a set of authentication servers (or a single server) supporting a single authentication protocol with a particular configuration. You bind the realm configured to the identity.

To enable authentication, you must create at least one authentication realm.

You create, edit, and delete authentication realms on the **Network > Authentication** page under the **Authentication Realms** section. You can perform any of the following tasks when configuring authentication:

- Include up to three authentication servers in a realm.
- More than one LDAP realms can be configured.
- Only one NTLM realm can be configured.
- Include at least one authentication server in each realm.
- Include one or more realms in a single authentication sequence.
- Include realms of different protocols in a single authentication sequence.

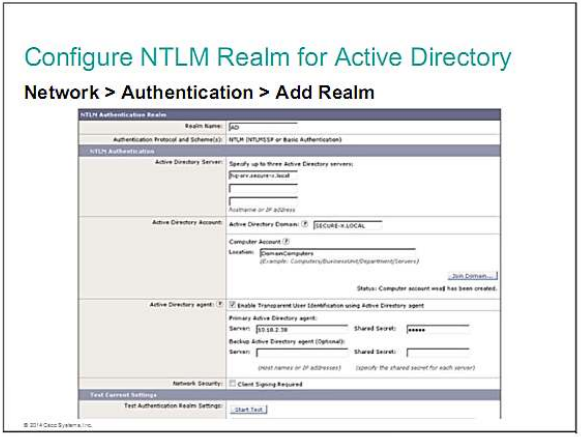
You can create multiple authentication realms, but at most one of them can be an NTLM realm. You can create more than one authentication realm within a single external LDAP database. Typically, however, you will only create one LDAP realm for each LDAP database that is used by the Cisco Web Security Appliance.

A realm sequence is an ordered sequence of realms. As soon as the user creates a second realm, the Cisco WSA creates a realm sequence called "All Realms" that contains the list of realms in the order they were created. You can create other realm sequences by clicking on **Add Sequence**, and then entering a list of existing realms.

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

Configure NTLM Realm for Active Directory

This topic describes the configuration of the NTLM Realm for Active Directory.



The NTLM authenticates users with an encrypted challenge-response sequence that occurs between the appliance and a Microsoft Windows domain controller. The NTLM challenge-response handshake occurs when a web browser attempts to connect to the appliance and before data is delivered.

When you configure an NTLM authentication realm, you do not specify the authentication scheme. Instead, you choose the scheme at the web access policy group level when you configure the policy member definition. This allows you to choose different schemes for different policy groups.

You need to fill in these authentication settings when you configure NTLM authentication under **Network > Authentication > Add Realm**:

Active Directory Server: enter the Active Directory server IP address or hostname. You can specify up to three Active Directory servers. When you configure multiple authentication servers in the realm, the appliance attempts to authorize with up to three authentication servers before failing to authorize the transaction within that realm.

Active Directory Account: enter the Active Directory server domain name and computer account location. You must click **Join Domain** to enter an Active Directory username and password.

Active Directory Agent: Choose whether or not to identify users transparently without prompting the users. When you enable transparent user identification, you will need the Cisco Context Directory Agent that can access the Active Directory server. Enter the primary server name for the machine where the primary Cisco CDA is installed and the shared secret used to access it. For redundancy, you can also enter the backup server name for the machine where the backup Cisco CDA is installed and the shared secret used to access it.

You can verify the authentication settings in the **Test Current Settings** section when you create or edit an authentication realm by clicking the **Start Test** button.

https://t.me/learningnets

When you create or edit an identity (not shown in the figure), you can choose one of the following schemes:

Use NTLMSSP

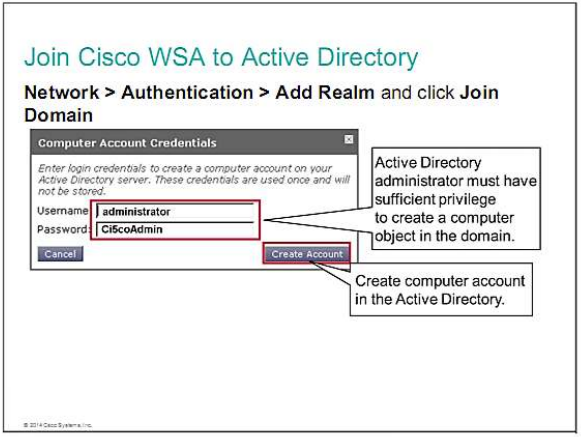
Use Basic or NTLMSSP

Use Basic

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

Join Cisco WSA to Active Directory

This topic how to join the Cisco Web Security Appliance to the Active Directory.



When you configure an NTLM realm, you must enter information to join the Active Directory domain to set up a computer account in the domain. An Active Directory computer account is an account that uniquely identifies the computer on the domain. It is also referred to as a machine trust account.

After you enter the Active Directory account information in the authentication realm, click the **Join Domain** button to set up a computer account. Use the **Location** field to define the organizational directory where AsyncOS should create the computer account in the Active Directory domain.

When you click **Join Domain**, you are prompted to enter login credentials for the Active Directory server. The login information is used only to create the Active Directory computer account and is not saved. Enter the login information and click **Create Account**.

When you click **Join Domain**, enter the name and password for the Active Directory user. If the Cisco WSA and the Active Directory server are in the same domain, any valid user that is a member of the user domain is allowed.

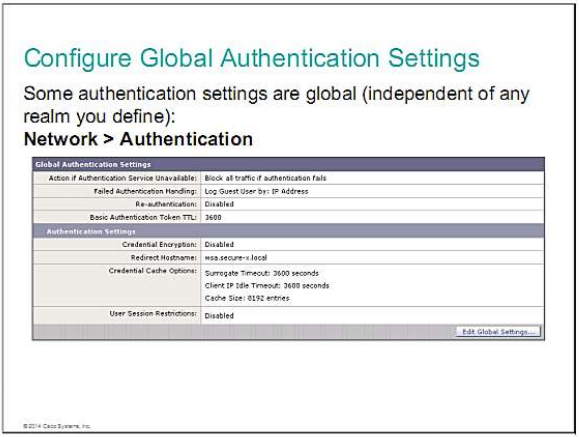
However, depending on the Active Directory server configuration, this user might need Domain Admin Group or Enterprise Admin Group credentials. For example:

If the Cisco WSA and the Active Directory server are not in the same domain, the Active Directory user must be a member of the Domain Admin Group.

If the Active Directory server configuration is a forest, the Active Directory user must be a member of the Enterprise Admin Group. Configure whether or not the Active Directory server requires signing. When you enable this check box, the appliance uses TLS when communicating with the Active Directory server.

Configure Global Authentication Settings

This topic describes the global authentication settings.



Some authentication settings are independent of any realm you define. To configure global authentication settings, navigate to the **Network > Authentication** page, click **Edit Global Settings.**

Global configuration options include:

Action if Authentication Service Unavailable: you can choose between two options

- **Permit traffic to proceed without authentication.** Processing continues as if the user was authenticated.
- **Block all traffic if user authentication fails.** Processing is discontinued and all traffic is blocked.

Failed Authentication Handling: When you grant users guest access in an Identity policy, this setting determines how the Cisco Web Security Appliance identifies and logs the user as a guest in the access logs:

- IP address
- User Name as Entered by End-User

Reauthentication: This setting allows users to authenticate again if the user is blocked from a website due to a restrictive URL filtering policy. The user sees a modified end-user notification page that includes a link that allows them to enter new authentication credentials. If the user enters credentials that allow more access permissions, the requested page appears in the browser. This setting only applies to authenticated users who are blocked due to restrictive URL filtering policies. The default setting is disabled.

Basic Authentication Token TTL: Controls the length of time that user credentials are stored in the cache before revalidating them with the authentication server. The default value of 3600 seconds is the recommended setting. When the Surrogate Timeout setting is configured and is greater than the Basic Authentication Token TTL, then the Surrogate Timeout value takes precedence and the Cisco WSA contacts the authentication server after surrogate timeout expires.

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

Credential Encryption: This setting specifies whether or not the client sends the login credentials to the Cisco WSA through an encrypted HTTPS connection. This setting applies to both Basic and NTLMSSP authentication schemes, but it is particularly useful for Basic authentication scheme because user credentials are sent as plain text.

Redirect Hostname: Enter the short hostname of the network interface on which the Web Proxy listens for incoming connections. When you configure authentication on an appliance deployed in transparent mode, the Web Proxy uses this hostname in the redirection URL sent to clients for authenticating users.

Surrogate Timeout: In transparent proxy mode, this specifies how long the surrogate (IP address or cookie) can be used by the Cisco WSA before the Cisco WSA must ask the client to reauthenticate. Generally, browsers (and other user agents) cache the end-user credentials, and can therefore reauthenticate with the Cisco WSA without prompting the end-user to re-enter credentials.

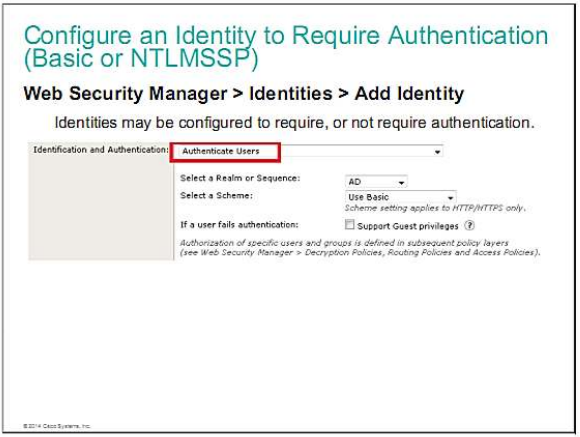
- Surrogates define how the users are tracked once the have authenticated. The Cisco WSA can track the authenticated users using IP address or cookies (persistence or session based). A surrogate is the method that the Cisco WSA uses to keep track of which user is requesting which Web site from which computer. The simplest surrogate to use is IP based. With this method, the Cisco WSA tracks User X is on Computer Y and therefore all traffic coming from Computer Y must be from User X. Unfortunately this does not work when more than one user is logged onto a system. The Cisco WSA also offers the ability to use session cookies or persistent cookies to keep track of users. With this method, the Cisco WSA will authenticate the user (using one of several possible methods) and then place a cookie on the user machine to keep track of the user. A persistent cookie will not be removed when the user closes their browser, whereas the session cookie will be deleted when the browser is closed. To use transparent user identification, you must choose IP address.

Cache Size: It is recommended that the size be set to the expected number of users.

https://t.me/learningnets

Configure an Identity to Require Authentication (Basic or NTLMSSP)

This topic describes how to configure an identity to require authentication using the Basic or NTMLSSP scheme.



Identities may be configured to require, or not require authentication. When you create an identity, you determine whether the transaction requires authentication. To configure an identity to use Basic or NTLMSSP authentication, navigate to **Web Security Manager > Identities > Add Identity**, **Identification and Authentication** section and select **Authenticate Users** from the drop-down menu.

Select the Realm, in the example, the **AD** realm is selected.

Select the Scheme: **Use NTLMSSP** or **Use Basic or NTLMSSP** or **Use Basic**. In the example, **Use Basic** is selected.

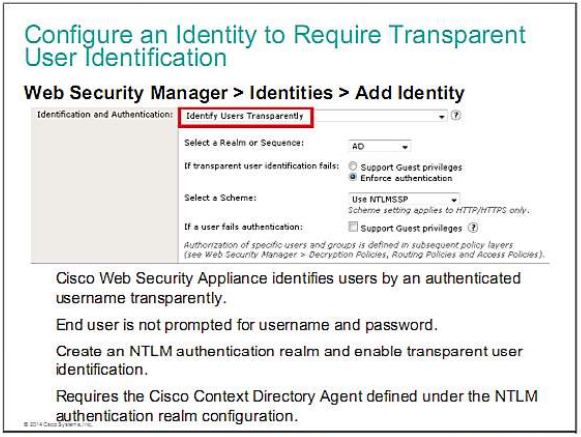
To configure an identity to not require authentication, select **No Authentication or Identification** from the drop-down menu to create authentication exemptions. For example, create an identity for the Microsoft Windows Update agent that does not require authentication. This would allow automated Windows updates to work properly.

Identities that do not require authentication should be placed above identities that require authentication. The user is allowed to break this convention, but it may create undesirable results, such as the browser asking for authentication even though it is not required for the given request.

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

Configure an Identity to Require Transparent User Identification

This topic describes how to configure an identity to require transparent user identification.



The Cisco WSA can identify users by an authenticated username transparently without prompting the end user to enter his username and password. Transparent authentication is a method of obtaining user credentials that have been obtained from another trusted source. The Cisco WSA assumes that the user has already been authenticated by another trusted source.

Using Transparent User Identification, the Cisco WSA can identify users transparently using Active Directory authentication server. Create an NTLM authentication realm and enable transparent user identification. In addition, you must deploy a separate Active Directory agent device called the Cisco Active Directory Agent.

Active Directory does not record user login event information in a method that is easily queried by other servers, such as the Cisco WSA. However, Cisco offers the Cisco CDA that queries the Active Directory security event logs to maintain an IP address to user name mapping of users authenticated with Active Directory.

The Cisco WSA to Cisco CDA interactions work similarly to how the Cisco ASA interacts with the Cisco CDA to implement identity firewall services and also similarly to how the Cisco Context-Aware Next-Generation Firewall interacts with the Cisco CDA to implement passive authentication.

The Cisco WSA communicates with the Cisco CDA to maintain a local copy of the IP address to user name mapping. When the Cisco WSA needs to associate an IP address with a user name, it first checks its local copy of the mapping. If no match is found, it queries the Cisco CDA to find a match.

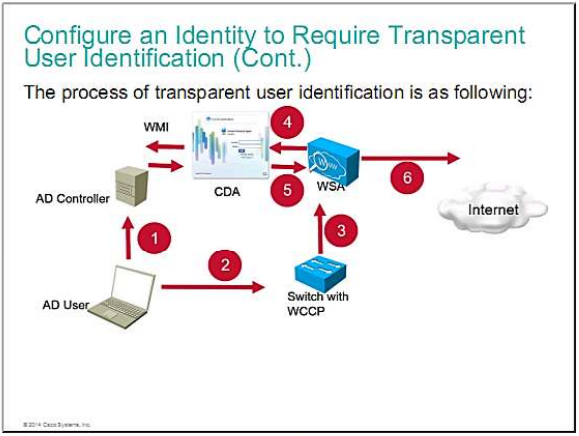
The Active Directory Agent device called the Cisco CDA is defined under the NTLM authentication realm configuration.

Transparent User Identification is supported since the AsyncOS for Web 7.5 and later releases.

To configure an identity to use transparent user identification, navigate to **Web Security Manager > Identities > Add Identity, Identification and Authentication** section and select **Identifer User Transparently** from the drop-down menu and select an NTLM Realm with the Active Directory Agent (Cisco CDA) configured.

If transparent user identification fails, guest privileges access can be enabled or either Basic or NTLMSSP authentication scheme can be enforced. In the figure, NTLMSSP is selected.

Note Transparent user identification with Active Directory works with an NTLM authentication realm only. You cannot use it with an LDAP authentication realm that corresponds to an Active Directory instance.



The process of transparent user identification is as follows:

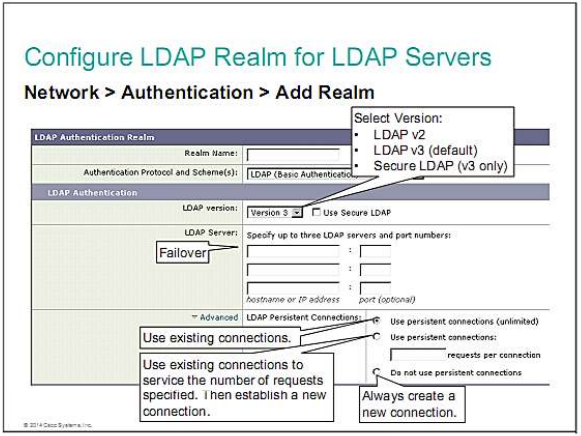
1. Client logs on to the Active Directory Domain, the Cisco CDA tracks the Active Directory server security audit logs via the WMI protocol and maps the Usename to the IP Address.
2. Client request a Web Site
3. Traffic is transparently redirected to the Cisco WSA
4. The Cisco WSA needs to authenticate the user and queries the Cisco CDA for the User to IP mapping
5. The Cisco CDA response to the Cisco WSA with the User to IP mapping
6. The client request is proxied and forwarded out by the Cisco WSA

The Cisco WSA periodically queries the Active Directory server directly to obtain the User Groups information (not shown in the figure).

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

Configure LDAP Realm for LDAP Servers

This topic describes the creation of LDAP realms for other directories.



The LDAP database is composed of objects containing attributes and values. Each object name is referred to as a DN. The location on the LDAP server where a search begins is called the base distinguished name or base DN.

The Cisco Web Security Appliance supports standard LDAP server authentication and secure LDAP authentication. Support for LDAP allows established installations to continue using their LDAP server database to authenticate users. For secure LDAP, the Cisco WSA supports LDAP connections over SSL. The SSL protocol is an industry standard for ensuring confidentiality. SSL uses key encryption algorithms along with CA signed certificates to provide the LDAP servers with a way to verify the identity of the Cisco WSA.

In the LDAP Server field, enter the LDAP server IP address or hostname and its port number. You can specify up to three LDAP servers. The hostname must be a fully qualified domain name. For example, ldap.example.com. An IP address is only required if the DNS servers that are configured on the Cisco WSA cannot resolve the LDAP server hostname. The default port number for Standard LDAP is 389. The default number for Secure LDAP is 636.

When you configure multiple authentication servers in the realm, the appliance attempts to authorize with up to three authentication servers before failing to authorize the transaction within that realm.

In the LDAP Persistent Connections area, choose one of the following values:

Use persistent connections (unlimited): Use existing connections. If no connections are available, a new connection is opened.

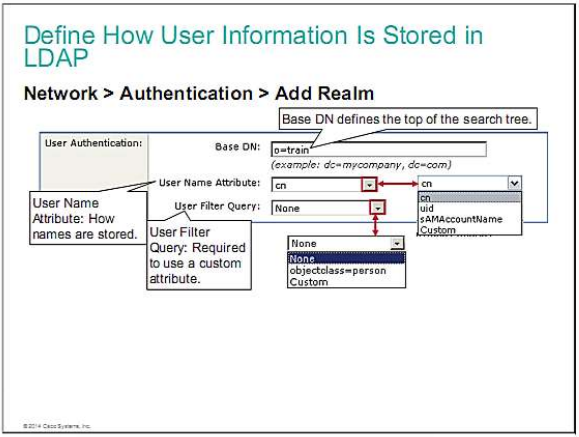
Use persistent connections: Use existing connections to service the configured number of requests per connection. When the maximum is reached, establish a new connection to the LDAP server.

Do not use persistent connections: Always create a new connection to the LDAP server.

https://t.me/learningnets

Define How User Information Is Stored in LDAP

This topic defines how user information is stored when using LDAP.



Under User Authentication, enter values for the following fields:

Base DN: The LDAP database is a tree-type directory structure and the Cisco Web Security Appliance uses the base DN to navigate to the correct location in the LDAP directory tree to begin a search. A valid base DN filter string is composed of one or more components of the form object value. For example, dc=companyname, dc=com.

User Name Attribute: Choose one of the following values:

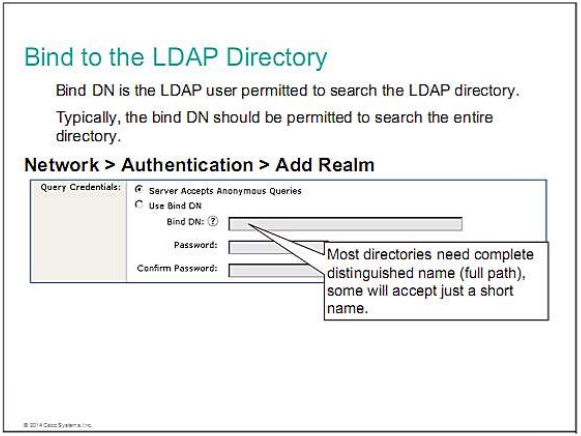
- cn
- uid
- sAMAccountName
- Custom (a custom identifier such as UserAccount)

User Filter Query: This is an LDAP search filter that locates the base DN. Custom LDAP search filters can be used to locate the base DN for a particular group of users.

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

Bind Cisco WSA to the LDAP Directory

This topic describes how to bind the Cisco Web Security Appliance to the LDAP directory.



LDAP uses a regular user-level bind to authenticate users. The Query Credentials menu, shown in the figure, allows you to choose whether the authentication server accepts anonymous queries. If the authentication server can accept anonymous queries, choose **Server Accepts Anonymous Queries**.

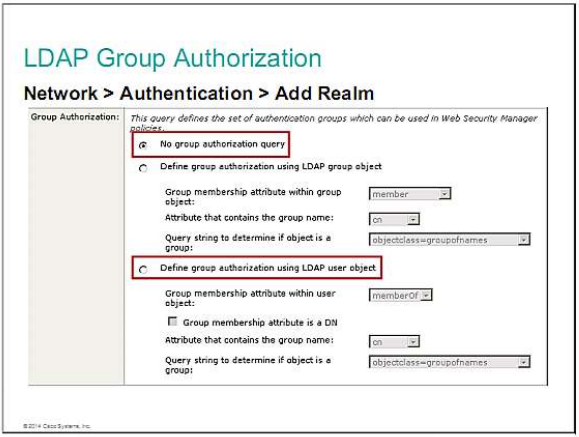
If the authentication server does not accept anonymous queries, choose **Use Bind DN** and then enter the following information:

Bind DN: The user on the external LDAP server that is permitted to search the LDAP directory. Typically, the bind DN should be permitted to search the entire directory.

Password: The password associated with the user you enter in the Bind DN field.

LDAP Group Authorization

This topic describes the LDAP group authorization.



You can use the user group membership information stored in an LDAP directory to apply a policy group to a group of users. To do this, enable group authorization in an LDAP authentication realm.

Choose whether or not to enable LDAP group authorization.

You can define group authorization using LDAP group objects or using LDAP user objects.

Sometimes, group membership information is stored in the group object, which has an attribute (such as "member") to list all users that belong to the group. Define authorized users by group object when the group object contains all users you need to define.

Sometimes, group membership information is stored in the user object, which has an attribute (such as "memberOf") that lists all groups to which a user belongs. You might want to define authorized users by user object when the authentication server does not store the member information in the group object or if it does not have a group object.

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

Allowing Guest Access to Users Who Fail Authentication

This topic describes how to allow guest access to the Internet to users who fail authentication.



You can grant limited access to users who fail authentication due to invalid credentials. By default, when a client passes invalid authentication credentials, the Cisco WSA continually requests valid credentials, essentially blocking user access to all resources. However, when you allow guest access, the first time the client passes invalid authentication credentials, the user is treated as a guest and the Cisoc WSA does not request authentication again.

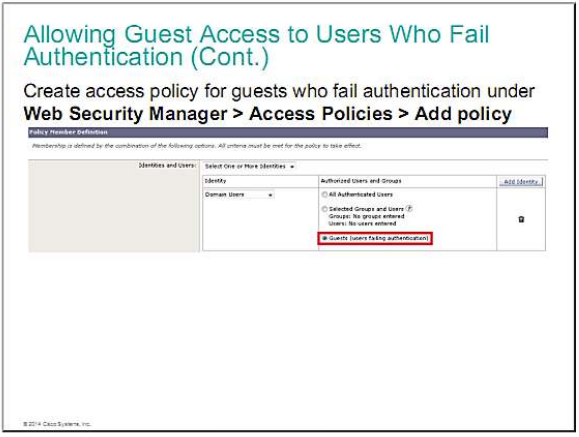
You might want to grant guest access to users in the following situations:

- A visitor comes to the office and needs to be granted restrictive Internet access, but is not in the corporate user directory.
- An employee from another branch location (or from an acquired company) comes to the corporate headquarters, and needs Internet access. The user directories of the branch location (or acquired company) and corporate headquarters are separate, so the employee's credentials do not work in the corporate headquarters.
- A new hire has been provided credentials in an email but they are not yet populated in the authentication server.
- A user logs into a Windows workstation using a local account instead of a Windows domain account and the user needs access to the Internet

The authentication server administrator in your organization can create a guest user account in the user directory. However, allowing guest access through the Cisco WSA has the benefit that the administrator does not have to communicate the guest credentials to every visitor.

https://t.me/learningnets





To grant guest access to users who fail authentication, you create an Identity that requires authentication, but also allows guest privileges as shown in the top figure.

Then you can create two access policies, one for the users who passes authentication and one for the guest users who fail authentication.

To create an access policy for the guest access, use the Identity that requires authentication, but also allows guest privileges as the policy membership definition. When users who fail authentication have guest access, they can access the resources defined in the policy group that specifies guest access for that Identity as shown in the bottom figure.

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

You can enable guest access for an Identity that uses any authentication protocol or scheme. To grant guest access to a user:

1. Define an Identity group and enable the **Support Guest privileges** option.
2. Create an Access, Decryption, Routing, Data Security, or External DLP Policy and select the Identity created in previous step .
3. In the Access, Decryption, Routing, Data Security, or External DLP Policy group membership, select "Guests (users failing authentication)" for the Identity in step 1.

A user who fails authentication has all transactions **blocked** if either of the following conditions are true:

Guest privileges are not provided in any Identity.

The user does not match any Identity that provides guest privileges.

A user who fails authentication has transactions **allowed** when all of the following conditions are true:

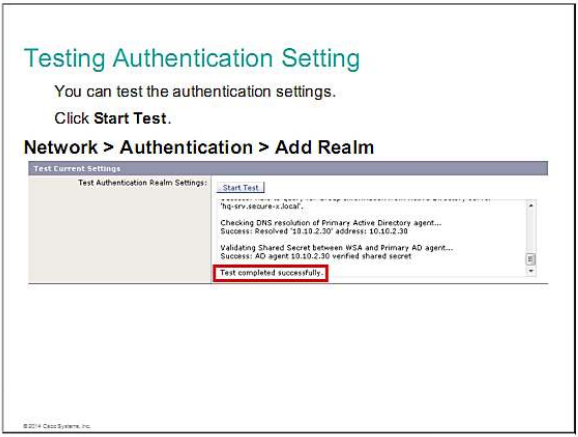
The user matches an Identity with guest privileges.

A non-Identity policy group (e.g. access policy or decryption policy) uses that Identity and applies to guest users.

https://t.me/learningnets

Testing Authentication Settings

This topic describes how to test Cisco Web Security Appliance authentication settings.



When you create or edit an authentication realm, you enter a lot of configuration settings to connect to the authentication server. You can test the settings you enter before submitting the changes to verify you entered the connection information correctly.

When you test authentication settings, the Cisco WSA first verifies that the settings you entered for the realm are in valid formats. For example, if a field requires a string and it currently contains a numeric value, the appliance informs you of that error.

If all fields contain valid values, the appliance performs different steps, depending on the authentication protocol. If the realm contains multiple authentication servers, the appliance goes through the testing process for each server in turn.

The appliance continues testing all servers in the realm and determines as many failures as possible for each server. It reports the testing outcome of each server in the realm.

You verify the authentication settings under **Network > Authentication > Add or Edit Realm** page when you create or edit an authentication realm.

You can test the authentication settings in the **Test Current Settings** section when you create or edit an authentication realm by clicking the **Start Test** button.

The appliance performs the following steps when you test NTLM authentication settings:

- It ensures that the specified Active Directory server is reachable and responds to queries.
- It ensures that a DNS lookup on the Active Directory domain is successful since the Active Directory domain must be a DNS domain name and not a WINS domain name.
- It ensures the system time of the appliance and the system time of the Active Directory server are within three minutes of each other.
- It validates the user credentials by generating a kerberos ticket.

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

It validates whether the user has the proper privileges to add the Cisco WSA to the Active Directory domain.

It validates whether you can fetch the groups within the domain.

The appliance performs the following steps when you test LDAP authentication settings:

It ensures that the LDAP server is listening on the specified LDAP port

If Secure LDAP is selected, the appliance ensures the LDAP server supports secure LDAP.

It performs an LDAP query using the supplied Base DN, User Name Attribute, and User Filter Query.

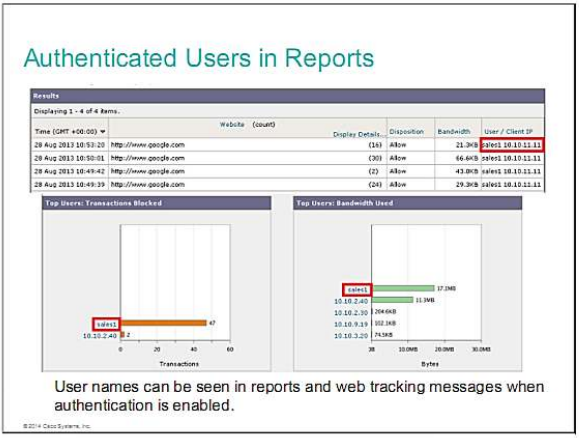
If the realm includes Bind Parameters, the Cisco WSA validates them by forming an LDAP query with the Bind Parameters.

If Group Authorization is provided, the Cisco WSA ensures that the specified group attributes are valid by fetching the groups from the LDAP server

https://t.me/learningnets

Authenticated Users in Reports

This topic describes how are authenticated users represented in the reports.



User names can be seen in reports and web tracking messages when authentication is enabled.

Reporting functionality aggregates information from individual security features and records data that can be used to monitor your web traffic patterns and security risks. You can run reports in real-time to view an interactive display of system activity over a specific period of time, or you can schedule reports and run them at regular intervals.

The Cisco Web Security Appliance not only generates high-level reports, allowing you to understand what is happening on the network, but it also allows you to drill down and see traffic details for a particular domain, user, or category.

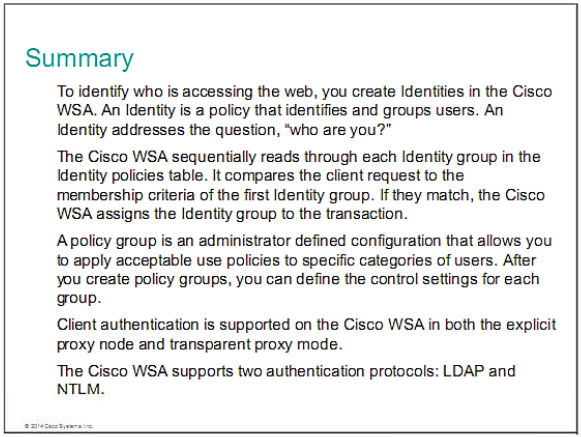
When you enable authentication, the reports can list the users by their usernames when they authenticate with the Cisco WSA. By default, usernames are written as they appear in the authentication server, such as **sales1** in the example.

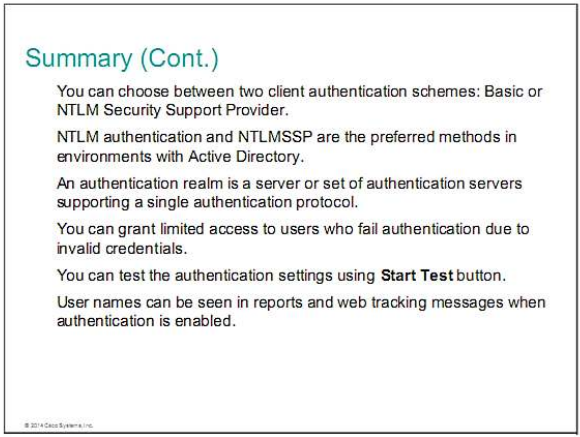
You can use the Web Tracking page to track and report on web usage for a particular user or for all users. When you enable authentication, web tracking lists transactions where you can see the information which user and from which IP address performed this web transaction.

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

Summary

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





References

For additional information, refer to these references:

Cisco IronPort AsyncOS for Web User Guide

http://www.cisco.com/en/US/docs/security/wsa/wsa7.5/user_guide/WSA_7.5.0_UserGuide.pdf

http://www.cisco.com/en/US/docs/solutions/SBA/February2013/Cisco_SBA_BN_WebSecurityUsingCiscoWSADeploymentGuide-Feb2013.pdf

Web Security Deployment Guide

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

Lesson 4

Configuring Cisco Web Security Appliance Acceptable Use Controls

Cisco Web Security Appliance enables you to control user access based on the web server category of a particular HTTP or HTTPS request. For example, you can block all HTTP requests for gambling websites or you can decrypt all HTTPS requests for secured web-based email websites. HTTPS decryption will be explained in another lesson.

Using access policy groups, you can create access policies that control access to websites containing objectionable or questionable content. The sites that are actually blocked, allowed, or decrypted depend on the categories that you select when you set up URL category filtering within each policy group.

This lesson describes the acceptable use controls provided by the Cisco WSA.

Upon completing this lesson, you will be able to meet these objectives:

- Provide an overview of the two main Cisco Web Security Appliance acceptable use controls
- Describe the process of categorizing a web site
- Describe Cisco Application Visibility Control
- Describe streaming media bandwidth control
- Describe how to enable the acceptable use controls
- Describe how to use the policies table
- Describe how to configure URL filtering
- Describe how to enable safe search and site content ratings
- Describe the custom URL categories
- Describe the URL category reports

https://t.me/learningnets

Describe how to configure AVC

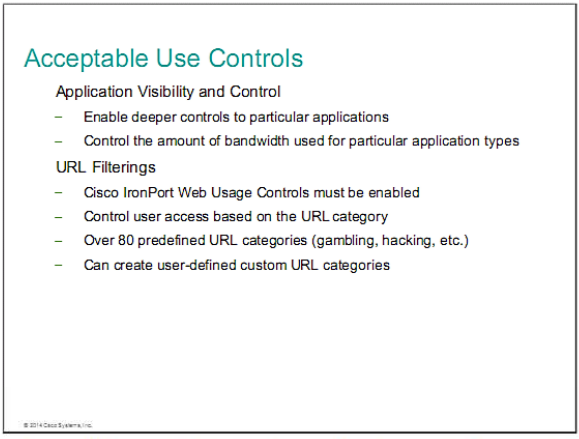
Describe how to configure media bandwidth limits

Describe the AVC reports

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

Acceptable Use Controls

This topic describes the two main Cisco Web Security Appliance acceptable use controls



The Cisco WSA acceptable use controls include a range of filtering capabilities for downloaded web content. The two main areas of web usage controls are:

Cisco Application Visibility and Control

URL filters

Cisco WSA Application Visibility and Control using the AVC engine enables deeper controls to particular applications. AVC can also be used to control the amount of bandwidth used for particular application types. Not all application types support bandwidth controls

Cisco WSA URL filterings control user access based on the Web server category of a particular HTTP or HTTPS request. For example, youcan block all HTTP requests for gambling web sites, or you can decrypt all HTTPS requests for web-based email websites.

Using policy groups, you can create access policies that control access to web sites containing objectionable or questionable content. The sites that are actually blocked, dropped, allowed, or decrypted depend on the categories you select when setting up category blocking for each policy group.

To control user access based on a URL category, you must enable Cisco IronPort Web Usage Controls. This is a multi-layered URL filtering engine that uses domain prefixes and keyword analysis to categorize URLs, and real-time response content analysis using the Dynamic Content Analysis engine if no category is determined by prefixes and keywords. It includes over 80 predefined URL categories.

The Cisco WSA ships with many predefined URL categories by default, such as web-based email, games, gambling, pornography, adult, and many other categories .

You can also create user-defined custom URL categories that specify specific hostnames and IP addresses. You can create custom URL categories for internal sites, or for a group of external sites.

https://t.me/learningnets

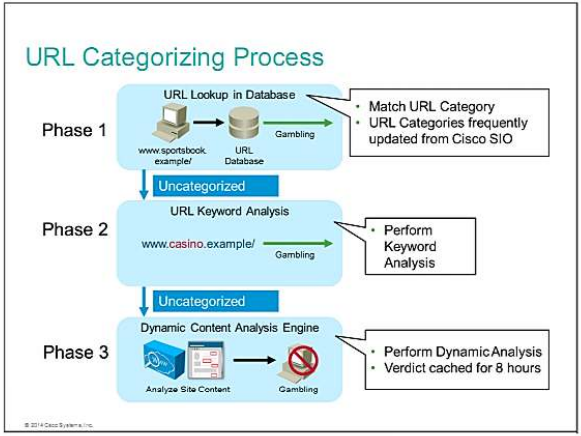
When the URL filtering engine matches a URL category to the URL in a client request, it first evaluates the URL against the custom URL categories included in the policy group.

The Dynamic Content Analysis engine is a scanning engine that can categorize a transaction that failed categorization using only the URL in the client request.

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

URL Categorizing Process

This topic describes the process of categorizing a web site.



The figure shows the order in which the Cisco Web Security Appliance can categorize a web site during a client request.

In phase 1, the requested URLs are looked up in the Cisco WSA URL category database. This database has many URL categories that are used to classify web content. This database is updated from the Cisco SIO every 5 minutes by default.

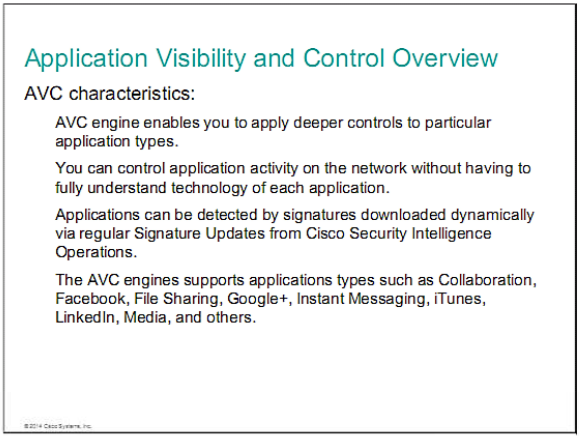
In phase 2, if the category of a web site can't be determined in the first phase using the Cisco WSA URL category database, the Cisco WSA performs the URL keyword analysis to determine the URL category. The URI is subject to analysis in this second phase.

Finally in phase 3, the Dynamic Content Analysis engine can be used to dynamically categorize an URL that failed categorization in phase 1 and 2. After the Dynamic Content Analysis engine categorizes an URL, it stores the category verdict and URL in a temporary cache. Enabling the Dynamic Content Analysis engine can impact transaction performance. However, most transactions are categorized using the Cisco WSA URL category database, so the Dynamic Content Analysis engine is usually only called for a small percentage of transactions. You might want to enable Dynamic Content Analysis when your traffic visits more of the newer, and therefore not yet categorized, sites on the Internet.

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

Application Visibility and Control Overview

This topic describes the Cisco Web Security Appliance Application Visibility and Control.



Cisco WSA web usage controls include the AVC engine, which enables you to apply deeper controls to particular application types. The AVC engine is an acceptable-use policy component that inspects web traffic to gain deeper understanding and control of web traffic used for applications. Application control gives you more granular control over web traffic than URL filtering alone.

The AVC engine allows you to create policies to control application activity on the network without having to fully understand the underlying technology of each application.

Using the AVC engine, thousands of applications can be detected and controlled by special signatures that are downloaded dynamically via regular Signature Updates from Cisco Security Intelligence Operations. Cisco SIO updates the applications signatures as necessary to adapt to the changing marketplace.

The AVC engines supports application types such as Collaboration, Facebook, File Sharing, Google+, Instant Messaging, iTunes, LinkedIn, Media, and others.

Using the AVC engine, you can block or allow applications by application type or a particular application. You can also apply deeper controls to particular application types. For example, you can perform the following tasks:

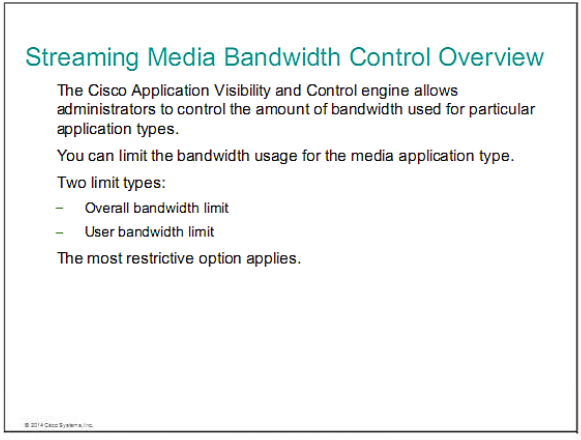
- Limit bandwidth consumed by some application types to control congestion.
- Allow instant messaging traffic, but disallow file sharing using instant messaging.
- Enforce safe search on search engines and user-generated content sites.
- Restrict access to adult content on some content-sharing sites.

The Cisco WSA HTTPS Proxy feature can decrypt HTTPS connections to web applications. This allows the AVC engine to detect and inspect web applications that use HTTPS. These web applications may use web browsers or other client applications, such as instant messaging applications. HTTPS decryption will be explained in another lesson.

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

Streaming Media Bandwidth Control Overview

This topic describes the Streaming Media Bandwidth Control.



The Cisco AVC engine allows administrators to control the amount of bandwidth used for particular application types. Not all application types support bandwidth controls.

For example, limiting the bandwidth usage for the media application type which include applications such as Hulu, Facebook Videos, Pandora, YouTube and others. Not all application types support bandwidth controls.

You can define the following bandwidth limits:

Overall bandwidth limit: Define an overall limit for all users on the network for the supported application types. The overall bandwidth limit affects the traffic between the web security appliance and web servers. It does not limit traffic served from the web cache. You might want to define an overall bandwidth limit to restrict the amount of network traffic used for high-traffic sites, such as streaming media sites.

User bandwidth limit: Define a limit for particular users on the network per application type. You can limit traffic from web servers as well as traffic served from the web cache. You might want to define user bandwidth limits to restrict the amount of traffic consumed by heavy usage users to enforce acceptable-use policies.

When both the overall limit and user limit apply to a transaction, the most restrictive option applies. You can define bandwidth limits for particular URL categories by defining an identity group for a URL category and using it in an access policy that restricts the bandwidth.

Note	Defining bandwidth limits only throttles the data going to users. It does not block data based on reaching a quota.

https://t.me/learningnets

Enable Acceptable Use Controls

This topic describes how to enable Acceptable Use Controls on the Cisco Web Security Appliance.



When setting up the Cisco WSA, choose whether or not to enable Acceptable Use Controls so you can use URL filtering. URL filtering allows you to control user access based on the category of a URL in a request.

This figure illustrates how to enable the acceptable usage controls on the Cisco Web Security Appliance. You also also separately activate the: Application Visibility and Control and Dynamic Content Analysis Engine.

You need to enable AVC to be able to use streaming media bandwidth control and many applications such as instant messaging and safe search.

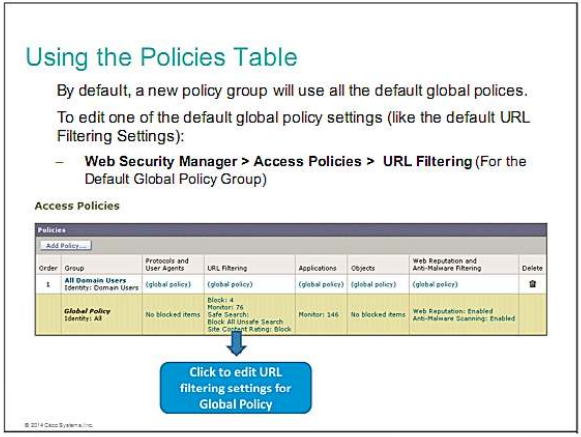
Dynamic Content Analysis engine, if enabled, is invoked only for uncategorized URLs, typically less than 5 percent of traffic.

The default action for unreachable service is monitor which can be configured to block instead.

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

Using the Policies Table

This topic describes how to use the policies table.



The policies table is an ordered list of policy groups and the settings you configure for each filtering component. It displays policy groups by row and control settings by column. The control settings you can define vary by policy type.

By default, a new policy group will use all the default global polices as shown by the All Domain Users access policy group shown in the figure. Any policy group that you create is added as a new row in the policies table. New policy groups inherit global policy settings for each control setting until you override them. To edit policy groups, click the links in each row.

To modify one of the policy setting like the URL filter setting for a new policy group, you can either edit the global policy which will affect all the other policy groups also using the global policy or you can create a custom policy for the new policy group.

To view or to edit one of the default global policy like the default URL filtering settings, from the access policies menu, for the default Global Policy, click on the link under the URL Filtering column to view or to edit the default global URL filtering settings.

In the example shown in the figure, the All Domain Users access policy group is using all the default global policies. Therefore, if the default URL filtering settings is changed, it will also effect the All Domain Users access policy group since it is also using the default URL filtering global policy.

Follow the similar procedures to edit the other default global policies like the default global policies for protocols and user agents, applications, objects and web reputation and anti-malware filtering.

Policy groups are used to match the client transactions. When a client sends a request to a server, the Cisco Web Security Appliance receives the request, evaluates it, and determines which policy group the client transaction belongs to. The Cisco WSA then applies the configured policy control settings to a client request based on the client request's policy group membership.

https://t.me/learningnets

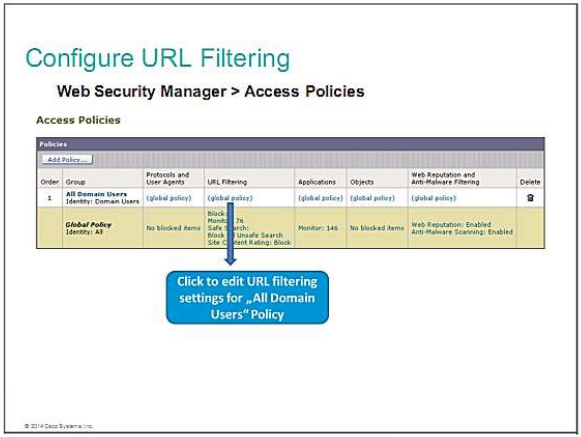
If a policy has no user defined policy groups, then each transaction belongs to the global policy group for that policy.

Note	Policy group membership for a Routing, Decryption, Access, Data Security, and External DLP Policies is based on an Identity and optional additional criteria. The Cisco WSA determines which Identity group the transaction belong to first before the evaluating the other policy types.

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

Configure URL Filtering

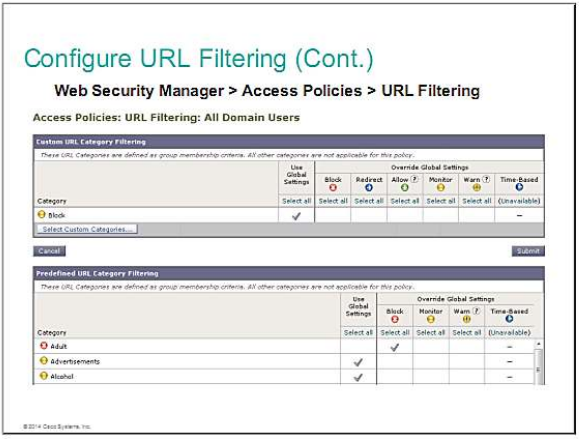
This topic describes how to configure URL filtering



When a new policy group is created, all actions are set to use the global policy as shown for the All Domain Users in the top figure.

To create a custom URL policy, click on the **(global policy)** link under URL Filtering column for the policy group to bring up the **Access Policies: URL Filtering: (Policy Group Name)** screen, which is shown in the next slide. In the figure, the policy group we are modifying the URL Filtering on is named "All Domain Users".

https://t.me/learningnets



The figure shows the **Access Policies: URL Filtering: (Policy Group Name)** screen.

The icon to the left of each of the Custom or Predefined URL category name shows the action.

The possible actions are: block, redirect, allow, monitor, warn, time-based.

Block: Denies transactions that match this setting.

Redirect: Redirects traffic originally destined for a URL in this category to a location you specify.

Allow: Always allows client requests for web sites in this category. Allowed requests bypass all further filtering and malware scanning.

Monitor: Neither allows nor blocks the request. Instead, it continues to evaluate the client request against other policy group control settings, such as web reputation filtering.

Warn: Initially blocks the request and displays a warning page, but allows the user to continue by clicking a hypertext link in the warning page.

Time-Based: Blocks or monitors the request during the time ranges you specify.

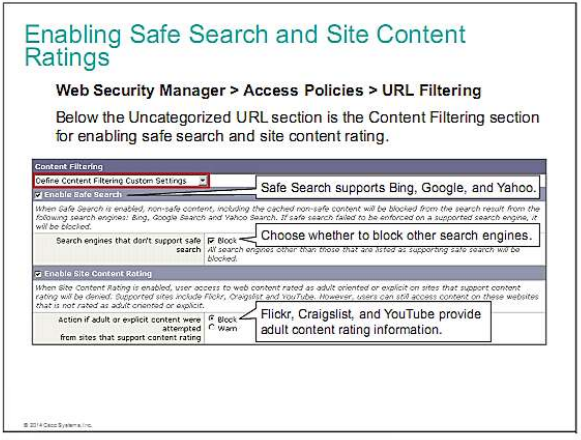
Uncategorized URLs are treated like a separate predefined category that allows you to choose from among the same actions as other predefined categories, except for the time-based action. You will find uncategorized URL configuration under the list of predefined URL categories (not shown in the figure).

Below the Uncategorized URL section is the Content Filtering section for enabling safe search and site content rating (not shown in the figure).

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

Enable Safe Search and Site Content Ratings

This topic describes how to enable safe search and site content ratings.



Many search engines support a filtering technology feature that classifies inappropriate content on the web as adult. When this filtering feature is enabled, content classified as adult is filtered from the search results before presented to the user. This feature is commonly called "safe search." For most search engines, this feature is enabled and disabled by end users. You can configure the web security appliance so that outgoing search requests appear to search engines as safe search requests. This gives the control to an administrator on the network instead of the end user. You might want to do this to prevent users from bypassing acceptable-use policies when they use search engines.

When Safe Search is enabled, non-safe content, including the cached non-safe content will be blocked from the search result from the following search engines: Yandex, Ask, Google, Yahoo, Bing, DuckDuckGo, Dailymotion and eBay. If safe search failed to be enforced on a supported search engine, it will be blocked.

Many content-sharing sites that serve user-generated photos and videos classify some of their content as adult. They allow users to restrict their own access to the adult content on these sites by either enforcing their own safe search feature or blocking access to adult content, or both. This classification feature is commonly called "content ratings."

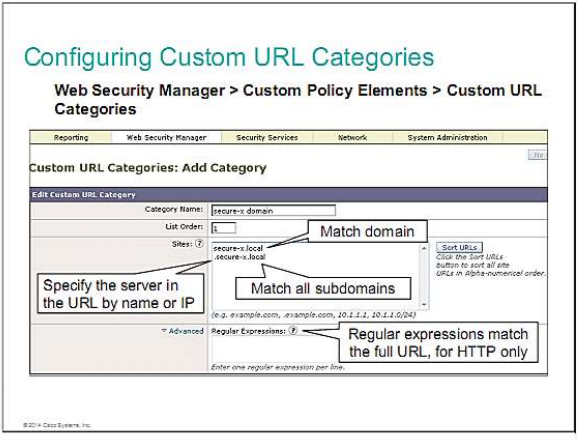
When Site Content Rating is enabled, user access to web content rated as adult oriented or explicit on sites that support content rating will be denied. Supported sites include Flickr, Craigslist and YouTube. However, users can still access content on these websites that is not rated as adult oriented or explicit.

You can enforce safe searches and site content ratings for different users by enabling the feature at the Access Policy level. Not all search engines or content-sharing websites are supported, but the Cisco Web Security Appliance can support additional search engines and websites during URL filtering engine updates from the Cisco Security Intelligence Operations.

https://t.me/learningnets

Configure Custom URL Categories

This topic describes how to configure custom URL categories.



The Web Security appliance ships with many predefined URL categories by default, such as Web-based Email and more. However, you can also create user defined custom URL categories that specify specific hostnames and IP addresses. You might want to create custom URL categories for internal sites or a group of external sites you know you can trust.

A custom URL category can be simply a list of websites. However, you must be careful to include the websites that you intend to include in the list. For example, if you enter "**secure-x.local**" in the Sites field, it will match http://secure-x.local but will not match http://www.secure-x.local or http://webmail.dev.secure-x.local. However, if you enter "**secure-x.local**" in the Sites field, it will match http://www.secure-x.local or http://webmail.dev.secure-x.local, but will not match http://secure-x.local.

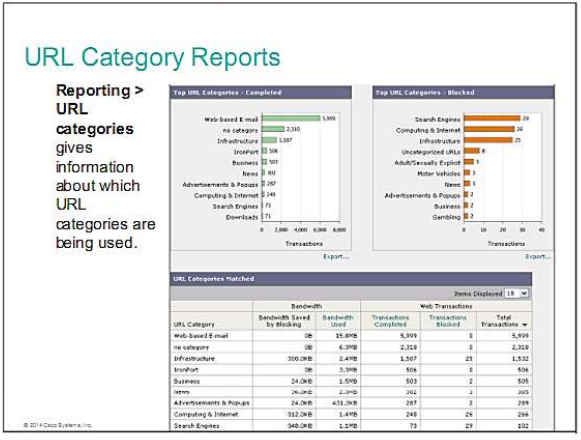
Therefore, to match any server in the secure-x.local domain, you must enter "**secure-x.local**" and ".secure-x.local" in the Site field.

There is a single advanced feature that allows the use of regular expressions in the creation of custom URL categories. Be frugal with your use of complex regular expressions. Matching large numbers of URLs to complex regular expressions can have an impact on performance.

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

URL Category Reports

This topic describes the URL category reports.



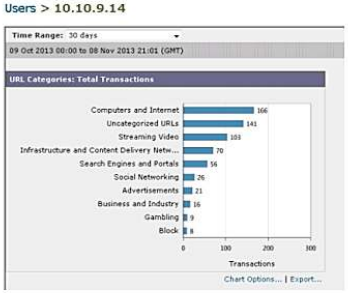
The URL category report is an example of many report types available for the web usage control functionality. These reports are printable in PDF format and can be exported in .csv format.

There are two reports of interest related to URL categories:

URL categories report: This report gives composite information about which URL categories are being used and which URL categories are being blocked as shown in the figure.

Users report: This report gives detailed information about which URL categories have been visited or blocked for a particular user (shown below).

URL Category Reports (Cont.)

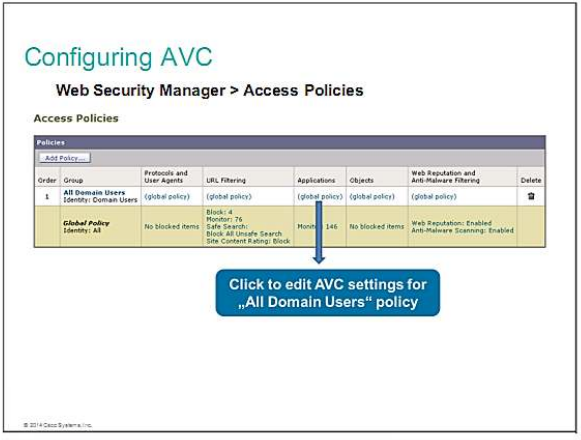


© 2014 Cisco Systems, Inc.

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

Configuring AVC

This topic describes how to configure Cisco Application Visibility and Control.



To control applications using the Cisco AVC engine, perform the following steps:

1 Enable the AVC engine

2 Define application control settings in the Access Policies

To create a custom applications visibility and control setting, from the **Access Policies** menu, click on the link under the **Applications** column for the desired access policy group to access the menu to edit the applications settings, as shown in the figure.



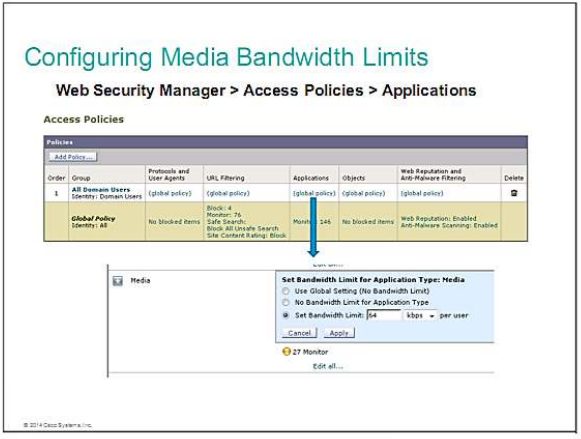
When you click the link under **Applications** column in the access policies table, **Access Policies: Application Visibility and Control: Policy name** window appears, where you configure AVC settings for applications.

The figure shows an example of blocking Facebook Games while monitoring all other Facebook Activities.

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

Configure Media Bandwidth Limits

This topic describes how to configure media bandwidth limits.

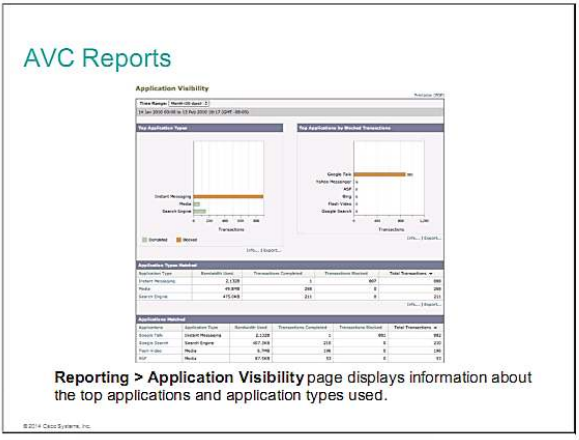


To create a custom applications visibility and control setting, from the Access Policies menu, click on the link under the Applications column for the desired access policy group to access the menu to edit the applications settings.

The figure shows an exmaple of setting a per-user media bandwidth limit to 64kbps for the All Domain Users access policy group.

AVC Reports

This topic describes the Cisco Application Visibility and Control reports.



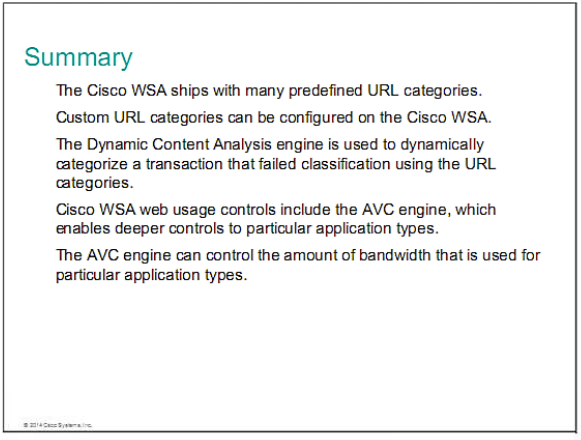
The **Reporting > Application Visibility** page displays information about the top applications and application types used. It also displays the top applications and application types blocked. You can click the individual applications and application types to view more detailed information about each.

The figure shows an example of the report page that lists various application types that were connected or blocked by the Cisco Web Security Appliance.

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

Summary

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



References

For additional information, refer to these references:

Cisco Systems, Inc. *Cisco IronPort AsyncOS for Web User Guide*, http://www.cisco.com/en/US/docs/security/security_management/sma/sma7.7/SMA_7.7_User_Guide.pdf

Cisco Systems, Inc. *Web Security Deployment Guide*, http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/February2012/SBA_Mid_BN_WebSecurityDeploymentGuide-February2012.pdf

https://t.me/learningnets

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

Lesson 5

Configuring Cisco Web Security Appliance Anti-Malware Controls

Overview

The Cisco Web Security Appliance anti-malware feature is a security component that uses the Dynamic Vectoring and Streaming engine in combination with multiple anti-malware scanning engines integrated on the appliance to identify and stop web-based malware threats, including zero-day threats. The Cisco Dynamic Vectoring and Streaming engine works with the Webroot, McAfee, and Sophos anti-malware scanning engines.

This lesson describes the anti-malware feature and its implementation on the Cisco WSA.

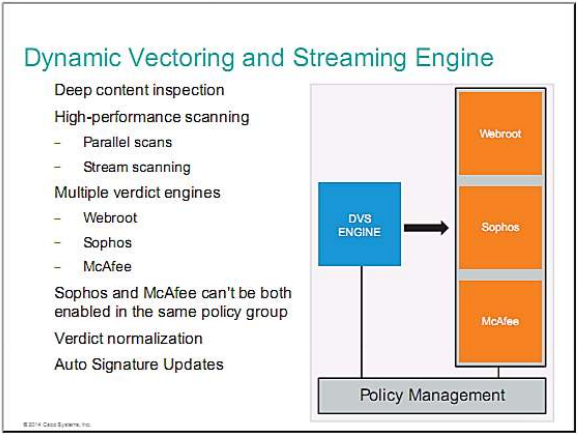
Upon completing this lesson, you will be able to meet these objectives:

- Describe the Cisco WSA DVS engine
- Describe the differences between Webroot with Sophos or McAfee
- describes the Cisco WSA adaptive scanning feature
- Describe the Cisco Web Reputation Filters
- Describe how to enable global Scanning Engines, Web Reputation Filtering and Adaptive Scanning
- Describe the inbound reputation filtering and malware scanning configuration
- Describe the outbound malware scanning configuration
- Describe the Cisco WSA malware reporting

https://t.me/learningnets

Dynamic Vectoring and Streaming Engine Overview

This topic describes the Cisco Web Security Appliance Dynamic Vectoring and Streaming engine.



The anti-malware feature uses the Cisco DVS engine in combination with multiple anti-malware scanning engines to identify and stop web-based malware threats. The Cisco DVS engine works with the Webroot, McAfee, and Sophos anti-malware scanning engines.

To use the anti-malware component of the appliance, you must first enable anti-malware scanning and configure global settings, and then apply specific settings to different policies.

The Cisco IronPort DVS engine inspects web traffic to provide protection against the widest variety of web-based malware ranging from commercially invasive adware applications, to malicious trojans, system monitors, and phishing attacks.

The scanning engines inspect transactions to determine a malware scanning verdict to pass to the DVS engine. A malware scanning verdict is a value assigned to a URL request or server response that determines the probability that it contains malware. The DVS engine determines whether to monitor or block the request based on the malware scanning verdicts.

The DVS engine performs anti-malware scanning on URL transactions that are forwarded from the Web Reputation Filters. Web Reputation Filters calculate the probability that a particular URL contains malware, and assign a URL score that is associated with an action to block, scan, or allow the transaction. When the assigned web reputation score indicates to scan the transaction, the DVS engine receives the URL request and server response content. The DVS engine, in combination with the Webroot and/or Sophos or McAfee scanning engines, returns a malware scanning verdict.

The DVS engine uses information from the malware scanning verdicts and Access Policy settings to determine whether to block or deliver the content to the client. When you enable both Webroot and Sophos or McAfee, the DVS engine determines how to scan the content to optimize performance and efficacy.

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

In some cases, the Cisco DVS engine might determine multiple malware verdicts for a single URL. Multiple verdicts can come from one or both scanning engines:

Different verdicts from different scanning engines: If you enable both Webroot and either Sophos or McAfee, each scanning engine might return different malware verdicts for the same object. When a URL causes multiple verdicts from both enabled scanning engines, the appliance performs the most restrictive action. For example, if one scanning engine returns a block verdict and the other a monitor verdict, the DVS engine always blocks the request. Only the most restrictive verdict is logged and reported.

Different verdicts from the same scanning engine: A scanning engine might return multiple verdicts for a single object when the object contains multiple infections. For example, a zip file might contain multiple files, each infected with a different kind of malware. When a URL causes multiple verdicts from the same scanning engine, the appliance takes action according to the verdict with the highest priority. Only the highest verdict is logged and reported. For example, virus has a higher priority than adware. Suppose the McAfee scanning engine detects both adware and a virus in the scanned object, and that the appliance is configured to block adware and monitor viruses. According to the priority, viruses belong in a higher priority verdict category than adware. Therefore, the appliance monitors the object and reports the verdict as virus in the reports and logs. It does not block the object even though it is configured to block adware. Refer to the latest Cisco AsyncOS for Web Security Appliance for a list of the priority order.

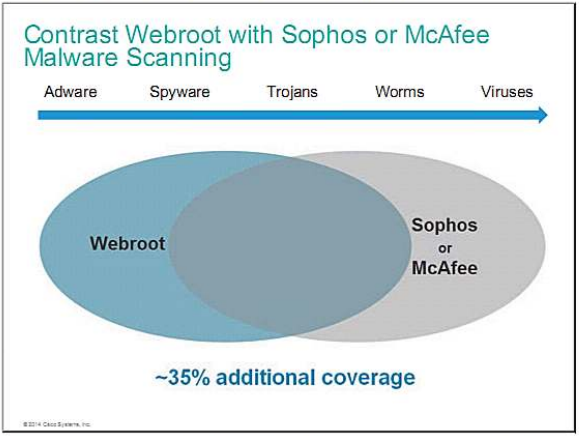
To use the anti-malware component on the Cisco WSA, you must first enable anti-malware scanning and configure global settings (under **Security Services > Web Reputation and Anti-Malware**), and then apply specific settings to different policies. Although you can enable all scanning engines globally, you can enable either the Sophos or McAfee scanning engine (but not both simultaneously) to each Access or Outbound Malware Scanning Policy. Similarly, you can also enable the Webroot scanning engine with either Sophos or McAfee to each Access or Outbound Malware Scanning Policy. You might want to enable the Sophos scanning engine instead of the McAfee scanning engine if the client machines have McAfee anti-malware software installed.

The anti-malware scanning engines also get frequent updates from the Cisco Security Intelligence Operations.

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

Contrast Webroot with Sophos or McAfee Malware Scanning

This topic describes the differences between Webroot with Sophos or McAfee.



The Cisco IronPort Dynamic Vectoring and Streaming engine can use one or more scanning engines to determine malware risk. Depending on the features purchased with the appliance, you can enable any of the following scanning engines:

Webroot: Webroot's automated spyware detection system rapidly identifies existing and new spyware threats on the Internet by intelligently scanning millions of sites on a daily basis. Webroot uses a signature database to help detect threats on the Internet.

McAfee: The McAfee scanning engine can detect existing and new malware threats by using a signature database of malware information and heuristic analysis.

Sophos: The Sophos scanning engine detects existing and new malware threats using a signature database.

Webroot Adware and Spyware detection, combined with antivirus software (Sophos or McAfee) have been tested to provide the broadest, most accurate coverage—35 percent more than individually. Each, based on its heritage, has clear strengths and the combination is very powerful.

To identify spyware and malicious code, Webroot is designed to proactively seek out the most malicious forms of spyware and malware. It includes a multitiered bot network that employs advanced research techniques, like deep packet sniffing. Webroot comprises a comprehensive set of network perimeter definitions that can be used to stop malicious threats before they reach the desktop.

The McAfee or Sophos scanning engine inspects objects downloaded from a web server in HTTP responses. After inspecting the object, it passes a malware scanning verdict to the Dynamic Vectoring and Streaming engine so the DVS engine can determine whether to monitor or block the request.

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

The McAfee scanning engine uses the following methods to determine the malware scanning verdict:

- Matching virus signature patterns
- Heuristic analysis

McAfee uses virus definitions in its database with the scanning engine to detect particular viruses, types of viruses, or other potentially unwanted software. It searches for virus signatures in files. When you enable McAfee, the McAfee scanning engine always uses this method to scan server response content.

New threats on the web appear almost daily. Using only virus signatures, the engine cannot detect a new virus or other malware because its signature is not yet known. However, by using heuristic analysis, the McAfee scanning engine can detect new classes of currently unknown viruses and malware in advance.

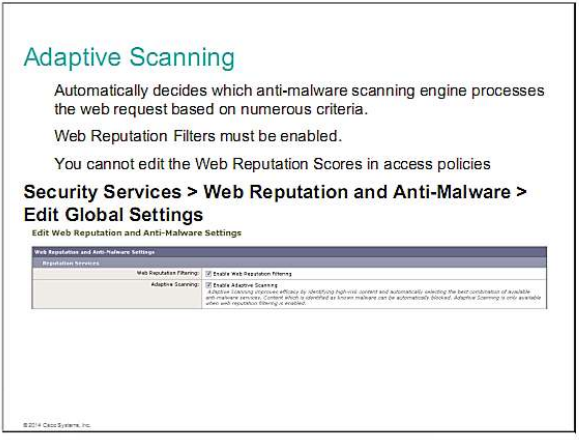
Heuristic analysis is a technique that uses general rules, rather than specific rules, to detect new viruses and malware. When the McAfee scanning engine uses heuristic analysis, it looks at the code of an object, applies generic rules, and determines how likely the object is to be virus-like. Using heuristic analysis increases the likelihood of catching viruses and malware before McAfee updates its virus signature database. However, it also increases the possibility of reporting false positives (clean content designated as a virus).

It also might impact appliance performance. When you enable McAfee, you can choose whether or not to also enable heuristic analysis when scanning objects.

Sophos offers award-winning protection against known and unknown threats using its Genotype and Behavioral Genotype Protection. The Sophos Genotype virus-detection technology proactively blocks families of viruses, and Behavioral Genotype Protection automatically guards against zero-day threats by analyzing the behavior of the code before it executes—offering protection from new and existing viruses, Trojan horses, worms, spyware, and other adware.

Adaptive Scanning Overview

This topic describes the Cisco Web Security Appliance adaptive scanning feature.



Adaptive Scanning is a logic layer that associates web reputation and the content type and decides based on the current threat profile which anti-malware scanning engine will process the web request.

Adaptive Scanning improves efficacy by identifying high-risk content and automatically selecting the best combination of available anti-malware services. Content which is identified as known malware can be automatically blocked. Adaptive Scanning applies the "Outbreak Heuristics" anti-malware category to transactions it identifies as malware prior to running any scanning engines. You can choose whether or not to block these transactions when you configure anti-malware settings on the appliance. Enabling Adaptive Scanning increases the catch rate for malware embedded in images, Javascript, text, and Flash files, but causes a slight decrease in appliance performance.

Enabling Adaptive Scanning increases efficacy for filtering out malware, but causes a slight decrease in appliance performance. To use Adaptive Scanning, you must enable Web Reputation Filters under **Security Services > Web Reputation and Anti-Malware > Edit Global Settings**, where you can also enable or disable adaptive scanning feature.

Adaptive Scanning is supported since the AsyncOS for Web 7.5 and later releases.

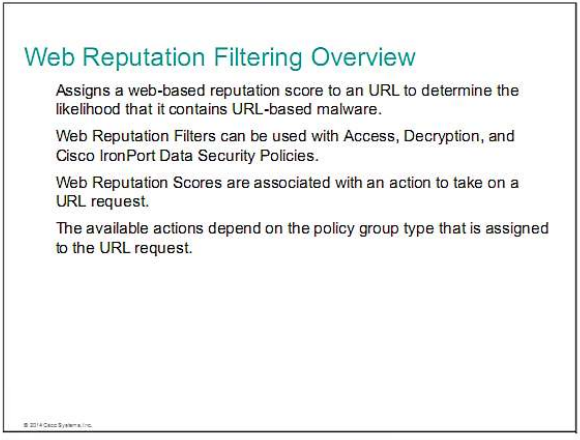
When Adaptive Scanning is enabled, the web reputation and anti-malware settings you can configure in Access Policies is slightly different:

- You can enable or disable web reputation filtering in each Access Policy, but you cannot edit the Web Reputation Scores.
- You can enable anti-malware scanning in each Access Policy, but you cannot choose which anti-malware scanning engine to enable. Adaptive Scanning chooses the most appropriate engine for each web request.

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

Web Reputation Filtering Overview

This topic describes the Cisco Web Security Appliance Web Reputation Filtering feature.



Web Reputation Filters is a security feature that analyzes web server behavior and assigns a WBRS to an URL to determine the likelihood that it contains URL-based malware. It helps protect against URL-based malware that threatens end-user privacy and sensitive corporate information. The Web Security appliance uses web reputation scores to identify suspicious activity and stop malware attacks before they occur. Web Reputation Filters are designed to combat the increasingly prevalent and dynamic nature of malware, especially to protect users from legitimate web sites that have been compromised by malware writers.

Web Reputation Filters can be used with Access, Decryption, and Cisco IronPort Data Security Policies.

Web Reputation Filters use statistically significant data to assess the reliability of Internet domains and score the reputation of URLs. Data such as how long a specific domain has been registered, or where a web site is hosted, or whether a web server is using a dynamic IP address is used to judge the trustworthiness of a given URL.

Web Reputation Scores are associated with an action to take on a URL request.

The available actions depend on the policy group type that is assigned to the URL request.

- Access Policies: block, scan, or allow
- Decryption Policies: drop, decrypt, or pass through
- Cisco IronPort Data Security Policies: block or monitor

The WBRS is based on more than just the URL. The input parameters include the following:

- URL categorization data
- Presence of downloadable code
- Presence of long, obfuscated EULAs
- Global volume and changes in volume

Network owner information

History of a URL

Age of a URL

Presence on any block lists

Presence on any allow lists

URL typos of popular domains

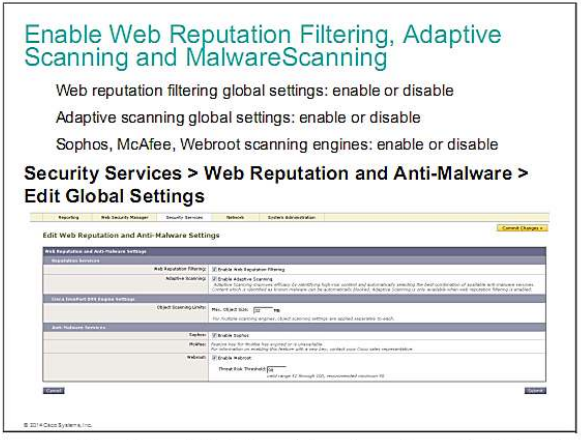
Domain registrar information

IP address information

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

Enable Web Reputation Filtering, Adaptive Scanning and Malware Scanning

This topic describes how to enable global Scanning Engines, Web Reputation Filtering and Adaptive Scanning.



The Web Reputation Filters, Dynamic Vectoring and Streaming engine, and the Webroot, McAfee, and Sophos scanning engines are enabled by default during system setup. Anytime after system setup, you can enable web reputation and anti-malware filters and configure global settings.

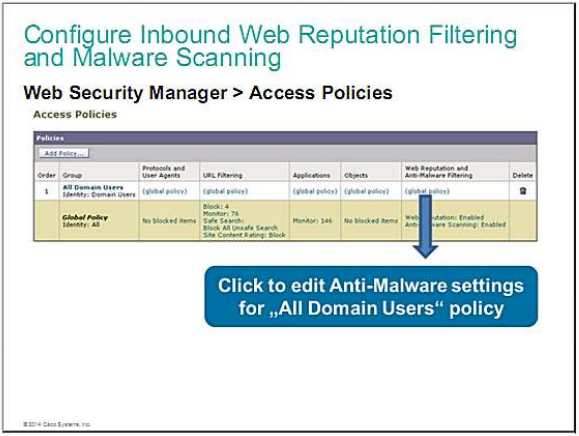
From the **Security Services > Web Reputation Filters** menu, click **Edit Global Settings** to edit the global settings to enable Web Reputation Filterings and Adaptive Scanning and Scanning Engines.

From the bottom half of the **Security Services > Web Reputation Filters** menu (not shown in the figure), you can also check the scanning engines updates and to initiate a new update.

After the Web Reputation and Anti-Malware Filters are enabled, you can configure web reputation and anti-malware settings in the policy groups.

Configure Inbound Web Reputation Filtering and Malware Scanning

This topic describes the inbound reputation filtering and malware scanning configuration.



To create a custom Web Reputation and Anti-Malware filtering setting, from the **Web Security Manager > Access Policies** menu, click on the **global policy** link under the **Web Reputation and Anti-Malware filtering** column for the desired access policy group to access the menu to enable web reputation filtering and anti-malware scanning for the desired policy group.

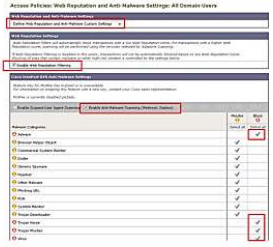
When you click on the link under the Web Reputation and Anti-Malware filtering column for the desired access policy group, **Access Policies: Web Reputation and Anti-Malware Settings: Policy Name** window appears.

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

Configure Inbound Web Reputation Filtering and Malware Scanning (Cont.)

Web Security Manager > Access Policies > Web Reputation and Anti-Malware Filtering

Example when adaptive scanning is enabled



In the example shown in the figure, the **Define Web Reputation and Anti-Malware Custom Settings** is selected from the drop down box selection to create a custom settings where Web Reputation Filtering is enabled and certain malware categories such as Adware, Trojan Horse, Trojan Phisher, Virus action is set to block instead of the default action of monitor (only Adware can be seen in the figure).

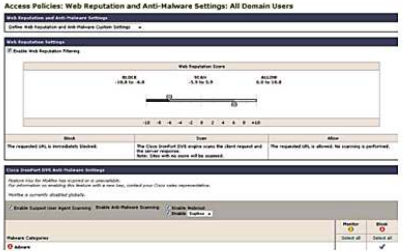
The **Enable Suspect User Agent Scanning** option is used to choose whether or not to scan traffic based on the user agent field specified in the HTTP request header. When you select this checkbox, you can choose to monitor or block suspect user agents at the bottom of the page (not shown in the figure. The Cisco Web Security Appliance examine the user-agent string in the HTTP header. The Cisco WSA maintains a list of suspect user agents and matches it to the value from the HTTP header.

When Adaptive Scanning is enabled (as shown by the example in the figure), the web reputation and anti-malware settings you can configure is slightly different than if an Adaptive Scanning is not enabled. As you can see in the figure, you can enable or disable web reputation filtering in each Access Policy, but you cannot edit the Web Reputation Score. You also cannot choose which anti-malware scanning engine to enable.

Configure Inbound Web Reputation Filtering and Malware Scanning (Cont.)

Web Security Manager > Access Policies > Web Reputation and Anti-Malware Filtering

Example when adaptive scanning is disabled



When Adaptive Scanning is disabled (as shown by the example in the figure), the web reputation and anti-malware settings you can configure is slightly different than if an Adaptive Scanning is enabled.

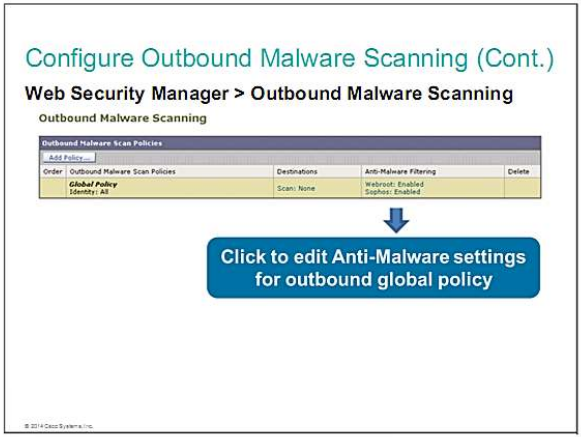
As you can see in the figure, you can edit the Web Reputation Score by using the slider bar to adjust the Web Reputation Score ranges for the block, scan and allow actions.

You can also choose which anti-malware scanning engine to enable and select the monitor or block action for each malware category.

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

Configure Outbound Malware Scanning

This topic describes the outbound malware scanning configuration.



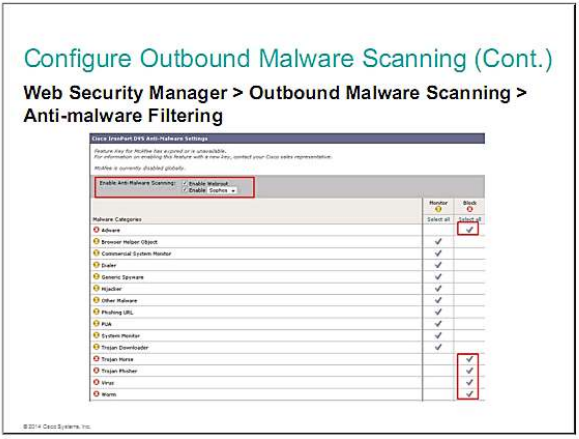
The Cisco Web Security Appliance provides the outbound malware scanning feature which allows you to stop malware that is already active on computers inside the network from escaping the network and affecting customers and partners. Outbound malware scanning policies determine whether or not to block a request to upload data that contains malicious data.

The Dynamic Vectoring and Streaming engine scans transaction requests as they leave the network in real time. By working with the DVS engine, the Cisco WSA enables you to prevent users from unintentionally uploading malicious data.

To prevent malicious data from leaving the network, the Cisco WSA provides the outbound malware scanning policy groups. You can define the uploads to be scanned for malware, the anti-malware scanning engines to use for scanning, and the malware types to block.

To create a custom outbound malware scanning setting, from the **Web Security Manager > Outbound Malware Scanning** menu, click on the **global policy** link under the **Anti-Malware Filtering** column for the desired access policy group to access the menu to set the outbound malware scanning for the desired policy group.

The example in the figure shows the **Anti-Malware Filtering** settings for the default Global Policy being selected.



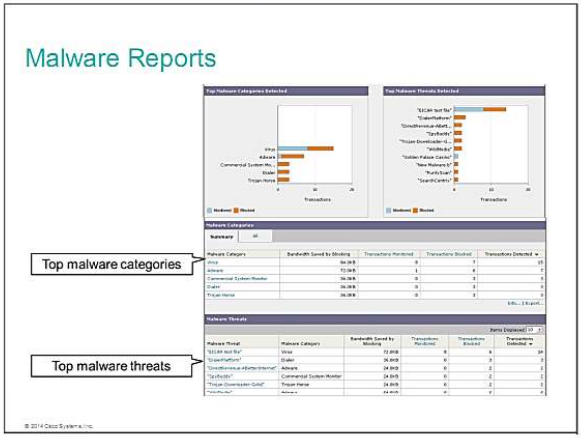
For the outbound malware scanning policy, web reputation filtering is not available.

In the example shown in the figure, shows the outbound malware scan policies for the default global policy group where both Webroot and Sophos Anti-Malware are enabled and certain malware categories such as Adware, Trojan Horse, Trojan Phisher, Virus action is set to block instead of the default action of monitor.

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

Malware Reports

This topic describes the Cisco Web Security Appliance malware reporting.



The Cisco WSA offers several malware-related reports:

The **Reporting > Anti-Malware** path, shown in the figure, allows you to monitor and identify malware detected by the Cisco Dynamic Vectoring and Streaming engine.

The Malware Category Report page, accessible through **Reporting > Anti-Malware**, allows you to view detailed information on an individual malware category and what it is doing on your network.

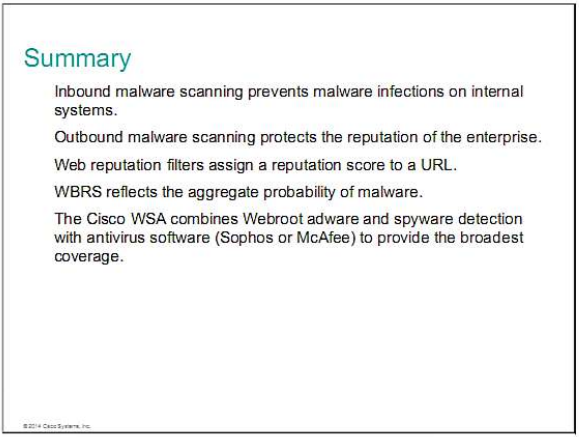
The Malware Threat Report page report, also visible in the **Reporting > Anti-Malware** menu, shows clients at risk for a particular threat, displays a list of potentially infected clients, and links to the Client Detail page. The trend graph at the top of the report shows monitored and blocked transactions for a threat during the specified time range. The table at the bottom shows the actual number of monitored and blocked transactions for a threat during the specified time range.

The Client Malware Risk page, available through the **Reporting > Client Malware Risk** menu is a security-related reporting page that can be used to monitor client malware risk activity. From the Client Malware Risk page, a system administrator can see which of their users are encountering the most blocks or warnings. Given the information gathered from this page, the administrator can click on the user link to view what this user doing on the web that makes them run into so many blocks or warnings and setting off more detections than the rest of the users on the network. Additionally, the Client Malware Risk page lists client IP addresses involved in frequent malware connections, as identified by the L4TM. A computer that connects frequently to malware sites may be infected with malware that is trying to connect to a central command and control server and should be disinfected.

https://t.me/learningnets

Summary

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



References

For additional information, refer to these references:

Cisco IronPort AsyncOS for Web User Guide

http://www.cisco.com/en/US/docs/security/wsa/wsa7.5/user_guide/WSA_7.5.0_UserGuide.pdf

http://www.cisco.com/en/US/docs/solutions/SBA/February2013/Cisco_SBA_BN_WebSecurityUsingCiscoWSADeploymentGuide-Feb2013.pdf

Web Security Deployment Guide

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

Lesson 6

Configuring Cisco Web Security Appliance Decryption

Overview

HTTPS is a web protocol that acts as a secure form of HTTP. HTTPS encrypts HTTP requests and responses before they are sent across the network. Common thinking is that any connection to a site using HTTPS is "safe." HTTPS connections are secure, not safe, and they do not discriminate against malicious or compromised servers. HTTPS is a secure way to complete legitimate transactions, but more dangerously, it is a secure way to download malware which can infect your network. This lesson describes how to configure decryption policies on Cisco Web Security Appliance. Decryption policies define how the appliance should handle HTTPS connection requests for users on the network. You can apply different actions to specified groups of users. You can also specify which ports the appliance should monitor for HTTPS transactions.

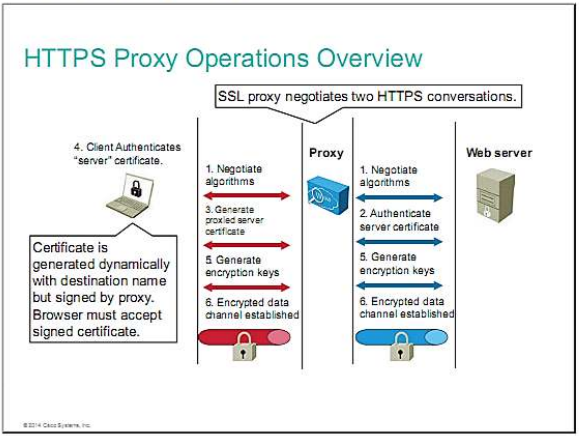
Upon completing this lesson, you will be able to meet these objectives:

- Describe the HTTPS proxy operation.
- Describe how to enable the HTTPS proxy.
- Describe the invalid certificate handling.
- Describe how to configure decryption policies

https://t.me/learningnets

HTTPS Proxy Operations Overview

This topic describes the HTTPS proxy operation.



HTTPS is a web protocol that acts as a secure form of HTTP. HTTPS encrypts HTTP requests and responses before they are sent across the network.

Not being able to inspect HTTPS traffic makes the network vulnerable to the following risks:

Secure site hosting malware. Spammers and phishers can create legitimate looking websites that are only reachable through an HTTPS connection. Some users may mistakenly trust the web server because it requires an HTTPS connection, resulting in intentional and unintentional downloaded malware.

Malware from HTTPS web applications. Some malware can infect the network from legitimateweb applications, such as secure email clients, by downloading attachments.

Secure anonymizing proxy. Some web servers offer a proxy service over an HTTPS connection that allows users to circumvent acceptable use policies. When users on the network use a secure proxy server outside the network, they can access any website, regardless of its web reputation or malware content.

The appliance uses both a URL filtering engine and Web Reputation Filters to make intelligent decisions about when to decrypt HTTPS connections. With this combination, administrators and end users are not forced to make a trade-off between privacy and security.

You can define HTTPS policies that determine if an HTTPS connection can proceed without examination or whether the appliance should act as an intermediary, decrypting the data passing each way and applying Access Policies to the data as if it were a plaintext HTTP transaction.

The Cisco Web Security Appliance can act as an SSL proxy and negotiates two HTTPS conversations. This is typically done in situations where it is required to have visibility into the encrypted traffic for access control or inspection purposes.

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

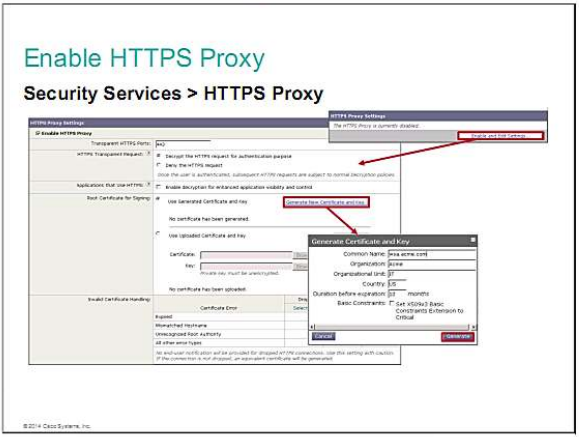
The client may be presented with a certificate that is signed by a server that is not in the default list of trusted CAs of the browser. This will then cause a dialog with the user about the certificate. You can use three methods to avoid the user dialog:

1. Use an HTTPS proxy certificate that is signed by a CA available in the trusted CA list.
2. Accept the certificate permanently.
3. Preload the certificate in the browser local certificate store.

https://t.me/learningnets

Enable HTTPS Proxy

This topic describes how to enable the HTTPS proxy.



To configure the appliance to handle HTTPS requests, you must perform the following tasks:

1. **Enable the HTTPS Proxy.** To monitor and decrypt HTTPS traffic, you must first enable the HTTPS Proxy.
2. **Create and configure Decryption Policy groups**. Once the HTTPS Proxy is enabled, you can create and configure Decryption Policy groups to determine how to handle each request from each user.
3. **Import custom root certificates (optional).** Optionally, you can import one or more custom root certificates so the Web Proxy can recognize additional trusted root certificate authorities used by HTTPS servers.

The HTTPS proxy is enabled in the **Security Services > HTTPS Proxy** menu by clicking **Enable and Edit Settings**. The HTTPS Proxy License Agreement appears. Read the terms of the HTTPS Proxy License Agreement, and click **Accept**.

In the HTTPS Ports to Proxy field, enter the ports the Cisco Web Security Appliance should check for HTTPS traffic. Port 443 is the default port.

In deployments using WCCP, the maximum number of port entries is 30 for HTTP and HTTPS ports combined. You can use port ranges to reduce the number of entries. You can use both port numbers and port ranges. Example: 443, 3128, 14001-14015.

You must provide the Cisco Web Security Appliance with a CA certificate. You have two choices, both available on this GUI page:

You may generate a self-signed Certificate Authority certificate as shown in the figure by clicking **Generate New Certificate and Key**.

You may upload an existing root certificate along with a private key.

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

X509v3 constraints dictate what a certificate can be used for, such as verifying signatures and how long a certificate chain is allowed. Setting the **Basic Constraints Extension to Critical** means that if there is an attempt to use the certificate outside of its constraints, you must notify the user and make sure the user understands what the constraint is.

The certificate file must be in PEM format. DER format is not supported.

Please add text to explain the 4 decryption options..I am not sure I understand them
And about OCSP handling.

Decryption Options:

Decrypt for Authentication: This setting determines how the Cisco WSA handles an HTTPS request that comes before any HTTP request, when authentication is enabled and uses an IP-based surrogate and credential encryption is enabled. If the user HTTPS transaction requires authentication but the user has not been authenticated yet prior to the HTTPS transaction, the client HTTPS request will be denied if decrypt for authentication is not enabled.

Decrypt for End-User Notification: You can configure the Cisco WSA to notify the user why it blocked the URL request. Web users see a web page that explains that they were blocked from accessing a website and why they were blocked. These pages are called end-user notification pages. The End-User Notification is configured **Security Services > End-User Notification page**. You can define notification pages using the on-box end-user notification pages or outside the Cisco WSA by redirecting all notification pages to a custom HTTP or HTTPS URL you specify. When using an outside HTTPS URL, enable decryption for end-user notification so the Cisco WSA can display the end-user notification to the users. If this is not enabled, the end user will see a browser error page instead of the end-user notification page from the Cisco WSA.

Decrypt for End-User Acknowledgement: You can configure the Cisco WSA to inform users that it is filtering and monitoring their web activity. The Cisco WSA does this by displaying an end-user acknowledgement page when a user first accesses a browser after a certain period of time. When the end-user acknowledgement page appears, users must click a link to access the original site requested or any other web site. If the user has not acknowledged the end-user acknowledgement, the user Web requests will be denied. The End-User Acknowledgement is configured under the **Security Services > End-User Notification page**. To keep track of when users accepted the end-user acknowledgement page, the Cisco WSA can use a surrogate (either by IP address or web browser session cookie) if no username is available for the user. When using cookies to track the users, for users who have not acknowledged the end-user acknowledgement prior to initiating a HTTPS transaction, enable decryption for end-user acknowledgement so the Cisco WSA can obtain the user information from the cookie in the HTTPS transaction and display the end-user acknowledgement to the users for acknowledgement.

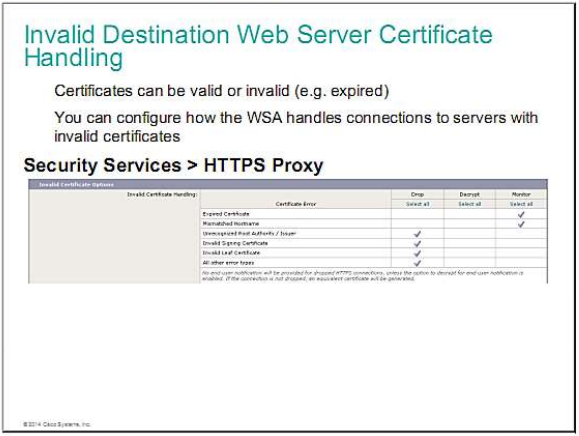
Decrypt for Application Detection: Enhances the ability of the Cisco WSA to detect HTTPS applications. The Cisco WSA can decrypt HTTPS connections to web applications. This allows the AVC engine to more accurately detect and block web applications that use HTTPS. These web applications may use web browsers or other client applications, such as instant messaging applications. The client machine must also trust the certificate from the Cisco WSA.

Also on this GUI page, you can configure what the Cisco WSA does with HTTPS traffic when the destination web server certificate is invalid under the Invalid Certificate Handling section.

https://t.me/learningnets

Invalid Destination Web Server Certificate Handling

This topic describes the invalid certificate handling.



In the **Invalid Certificate Handling** section, define the action that Cisco Web Security Appliance should take when it encounters an invalid certificate on the HTTPS server. The choices, depending on the certificate error, can range from dropping the connection, decrypting it, or monitoring it.

A certificate may be in invalid for different reasons. For example, the current time may be before or after the certificate validity period, the root authority in the certificate may not be recognized, or the Common Name of the certificate does not match the hostname specified in the HTTP "Host" header.

The Cisco WSA verifies that a server certificate is valid before it inspects and decrypts an HTTPS connection from a server. You can configure how the appliance handles connections to servers with invalid certificates.

Often, web users ignore browser warnings related to the destination web server certificate errors. One significant benefit of using the Cisco WSA is that blocking websites with certificate errors can be enforced at the proxy level.

In the **Invalid Certificate Handling** section under **Security Services > HTTPS Proxy**, you can choose how the appliance handle HTTPS traffic when it encounters invalid server certificates.

The Cisco WSA can perform one of the following actions for invalid server certificates:

Drop: Drops the connection and does not notify the client. This is the most restrictive option.

Decrypt: Allows the connection, but inspects the traffic content. It decrypts the traffic and applies Access Policies to the decrypted traffic as if it were a plain text HTTP connection.

Monitor: Does not drop the connection, and instead it continues comparing the server request with the Decryption Policy groups. When an invalid server certificate is monitored, the errors in the certificate are maintained and passed along to the end-user. This is the least restrictive option.

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

The HTTPS proxy distinguishes between the possible types of invalid certificates:

Expired: The current date falls outside of the range of validity for the certificate.

Mismatched hostname: The hostname in the certificate does not match the hostname the client was trying to access. This might happen during a "man in the middle attack," or when a server redirects a request to a different URL. For example, http://mailgoogle.com gets redirected to http://www.gmail.com.

Unrecognized Root Authority/Issuer: The root certificate authority for the certificate is not in the set of trusted root authorities on the appliance.

Invalid Signing Certificate: There was a problem with the signing certificate, for example, a failure to verify or decrypt the signature.

Invalid Leaf Certificate: There was a problem with the leaf certificate, for example, a rejection, decoding, or mismatch problem

All other error types: Most other error types are due to the appliance not being able to complete the SSL handshake with the HTTPS server.

If a certificate is both expired and has an unrecognized root authority, the action that is taken (drop, decrypt, or monitor) will be the action that is configured for a certificate with an unrecognized root authority.

In all other cases, for server certificates that are invalid for multiple reasons simultaneously, the HTTPS Proxy performs actions in order from the most restrictive action to the least restrictive action.

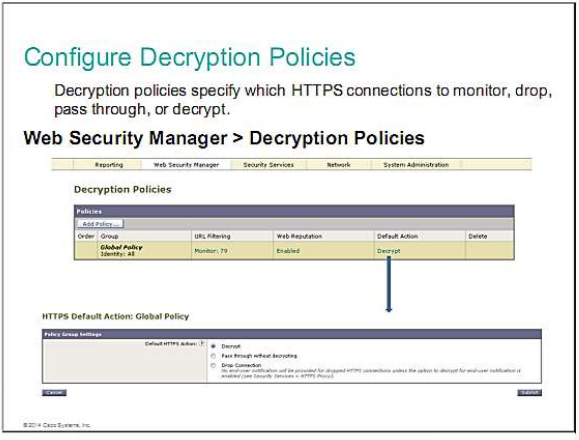
The Cisco WSA can also checks the revocation status with the issuing certificate authority in real time. If the issuing certificate authority supports OCSP, the certificate will include a URL for real-time status checking.

Cisco recommends configuring the OCSP Result Handling options to the same actions as Invalid Certificate Handling options. For example, if you set Expired Certificate to Monitor, configure Revoked Certificate to monitor also.

https://t.me/learningnets

Configure Decryption Policies

This topic describes how to configure decryption policies.



After the Cisco Web Security Appliance assigns an Identity to a client request, it evaluates the request against the other policy types to determine which policy group it belongs for each type. When the HTTPS Proxy is enabled, it applies HTTPS requests against the Decryption Policies. When the HTTPS Proxy is not enabled, it evaluates HTTP requests against the Access Policies. When an HTTPS request gets decrypted, the Cisco WSA evaluates the decrypted request against the Access Policies

Decryption Policies define how the appliance should handle HTTPS connection requests for users on the network. You can apply different actions to specified groups of users. You can also specify which ports the appliance should monitor for HTTPS transactions.

When a client makes an HTTPS request on a monitored secure port, the appliance compares the request to the Decryption Policy groups to determine in which Decryption Policy group the request belongs. Once it assigns the request to a Decryption Policy group, it can determine what to do with the connection request.

Use the **Web Security Manager > Decryption Policies** page to define the decryption polices.

You can create Decryption Policy groups based on combinations of several criteria, such as Identity or the URL category of the destination site. You must define at least one criterion for policy group membership. When you define multiple criteria, the client request must meet all criteria to match the policy group

After the Cisco Web Security Appliance assigns an HTTPS connection request to a Decryption Policy group, the connection request inherits the control settings of that policy group. The control settings of the Decryption Policy group determine whether the appliance decrypt, drop, or pass through or monitor the connection.

Monitor: An intermediary action that indicates the Cisco WSA should continue evaluating the transaction against the other control settings to determine which final action to ultimately apply.

Drop: Drops the connection and does not pass the connection request to the server. The Cisco WSA does not notify the user that it dropped the connection.

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

Pass through: Passes through the connection between the client and the server without inspecting the traffic content. You might want to pass through connections to trusted secure sites, such as well known banking and financial institutions.

Decrypt: Allows the connection, but inspects the traffic content. It decrypts the traffic and applies Access Policies to the decrypted traffic as if it were a plain text HTTP connection. By decrypting the connection and applying Access Policies, you can scan the traffic for malware.

All actions except monitor are final actions the Cisco WSA applies to a transaction. A final action is an action that causes the Cisco WSA to stop evaluating the transaction against other control settings

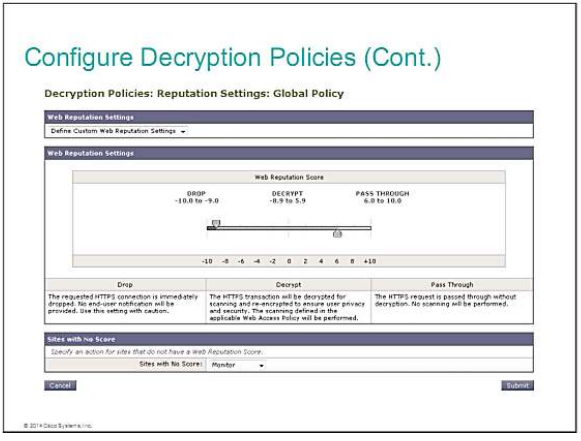
You can configure the following settings to determine what action to take on the HTTPS connection:

URL Filtering: You can configure the action (pass through, monitor, decrypt, drop, time-based) to take on HTTPS requests for each predefined and custom URL category. Click the link under the **URL Filtering** column for the policy group you want to configure.

Web reputation: You can configure the action (drop, decrypt, pass through) to take on HTTPS requests based on the web reputation score of the requested server. Click the link under the **Web Reputation** column for the policy group you want to configure.

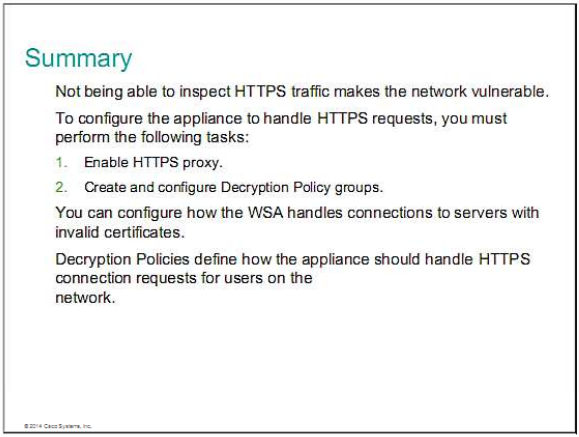
Default Action (shown in the figure): You can configure the action (decrypt, pass through without decryption, drop connection) the appliance should take when none of the other settings apply. Click the link under the **Default Action** column for the policy group you want to configure.

The configured default action only affects the transaction when no decision is made based on the URL category or Web Reputation score. If Web Reputation filtering is disabled, the default action applies to all transactions that match a Monitor action in a URL category. If Web Reputation filtering is enabled, the default action is used only if the Monitor action is selected for sites with no score (as shown in the figure below).



Summary

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



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

Lesson 7

Configuring Cisco Web Security Appliance Data Security Controls

Overview

The data of the organization is one of its most prized possessions. Organizations spend a lot of money making data available to the employees, customers, and partners. Data also travels over the web and through email. This increased access poses challenges for information security professionals to figure out how to prevent the malicious, accidental, or unintentional loss of sensitive and proprietary information.

By working with data security filters and external DLP systems, the Cisco Web Security Appliance allows you to protect information and intellectual property and enforce regulatory and organization compliance by preventing users from unintentionally uploading sensitive data. You can define what kind of data is allowed to leave the network. This lesson describes the data security controls available on the Cisco WSA.

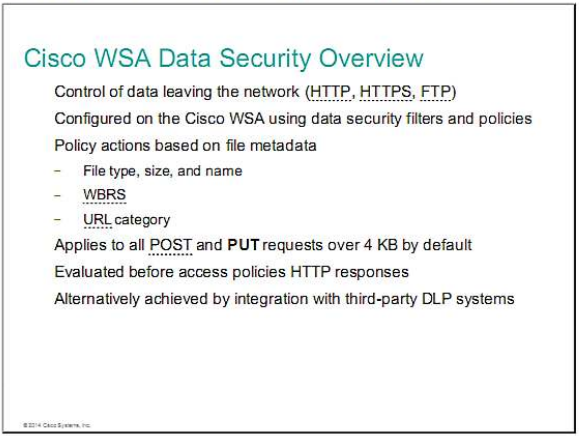
Upon completing this lesson, you will be able to meet these objectives:

- Describe data security on the Cisco WSA
- Describe data security policies
- Describe how to control uploaded content
- Describe the external DLP
- Describe how to add an ICAP server

https://t.me/learningnets

Cisco WSA Data Security Overview

This topic provides an overview of data security on the Cisco Web Security Appliance.



The Cisco WSA data security feature has been designed to prevent the malicious, accidental, or unintentional loss of sensitive and proprietary information. It allows you to protect information and intellectual property and enforce regulatory and organization compliance by preventing users from unintentionally uploading sensitive data.

The Cisco WSA secures your data by providing the following capabilities:

Data security filters: The data security filters on the Cisco WSA evaluate data leaving the network over HTTP, HTTPS, and FTP to control which data goes where and how and by whom it is sent.

Third-party DLP integration: The Cisco WSA integrates with leading third party content-aware DLP systems that identify and protect sensitive data. The Cisco WSA uses the ICAP, which is a lightweight HTTP-based protocol that allows proxy servers to offload content scanning to external systems. By offloading the content scanning to dedicated external systems, the web proxy can take advantage of the deep content scanning in other products while being free to perform other web proxy functions with minimal performance impact.

Depending on the needs of your organization, you might want to use both data security and external DLP policies. For example, you might use the data security policies to block data uploads to websites with a low reputation score. This way, the data is never sent to the external DLP system for a deep content scan, which improves overall performance.

To restrict data that is leaving the network, the Cisco WSA provides the following types of policy groups:

Data security policies. When you enable the data security filters, you can create data security policies to enforce business policies. For example, you can create a data security policy that prevents users from sending out Excel or zip files.

External DLP policies. When you configure the appliance to work with an external DLP system, you can create external DLP policies to pass data leaving the network to the external DLP system which scans the content and determines whether or not to block the request.

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

Data security policies and external DLP policies define how the Cisco WSA handles HTTP requests and decrypted HTTPS connections for transactions that upload data to a server. An upload request is an HTTP or decrypted HTTPS request that has content in the request body. When the Cisco WSA receives an upload request, it compares the request to the data security and external DLP policy groups to determine which policy group to apply. If both types of policies are configured, it compares the request to the data security policies before the external DLP policies. After it assigns the request to a policy group, it compares the request to the configured control settings of the policy group to determine what to do with the request.

To help reduce the number of upload requests scanned and recorded in the log files, you can define a minimum request body size, below which upload requests are not scanned by the data security filters or the external DLP server. The default minimum request body size is 4 KB (4096 bytes). The minimum request size is configured using the CLI. The size you specify applies to the entire size of the upload request body.

https://t.me/learningnets

Data Security Policies

This topic describes the data security policies to implement data loss prevention.

Data Security Policies

Uses URL Filtering, Web Reputation, and Content blocking configurations when evaluating the upload request.

A monitor action will not block the transaction and will proceed to the content checks.

A block action will block the transaction immediately, the transaction will not be further evaluated against the External DLP policies if configured or the access policies.

© 2014 Cisco Systems, Inc.

Data Security Policies

Web Security Manager > Cisco Ironport Data Security



© 2014 Cisco Systems, Inc.

The Cisco Web Security Appliance enables organizations to take quick, easy steps to enforce simple, common-sense data security policies. Examples include preventing engineers from sending design files by web mail, blocking uploads by finance staff of Excel spreadsheets over 100 KB, and preventing posts of content to blogs or social networking sites. These simple data security policies can be created for outbound upload requests.

https://t.me/learningnets

To scan upload requests on the appliance, you must first enable the Cisco IronPort Data Security Filters. Usually, the Cisco IronPort Data Security Filters feature is enabled during the initial setup using the System Setup Wizard. Otherwise, go to the **Security Services > Data Transfer Filters** page to enable it.

Cisco IronPort Data Security Policies use URL Filtering, Web Reputation, and Content blocking configurations when evaluating the upload request. You configure each of these security components to determine whether or not to block the upload request. The control settings of the Data Security Policy group determine whether the Cisco WSA blocks the transaction or further evaluates it against the External DLP policies if configured, otherwise, evaluate against the access polices.

From the **Web Security Manager > Cisco Ironport Data Security** page, select the **URL Filtering** control column to set the block or monitor action for the different URL category.

Select the **Web Reputation** control column to set the WBRS thresholds for the block or monitor action of the destination web servers that the users upload the data to. Web sites with no WBRS will have the monitor action. You should avoid adjusting the WBRS . If you are getting false positives for a particular site, it is better to use a custom URL category to exempt that site.

A monitor action will not block the transaction and will proceed to the content checks. If the content checks passes, the transaction will be further evaluated against the External DLP policies if configured, otherwise, evaluate against the access polices.

A block action will block the transaction immediately, the transaction will not be further evaluated against the External DLP policies if configured or the access policies.

The **Content** control settings part of the Ironport Data Security Policy to block data uploads based on the following file characteristics:

- File size: You can specify the maximum upload size allowed. All uploads with sizes equal to or greater than the specified maximum are blocked. You can specify different maximum file sizes for HTTP/ HTTPS and native FTP requests.
- File type: You can block predefined file types or custom MIME types.
- Filename: You can block files with specified names. You can use text as a literal string or a regular expression for specifying file names to block.

For outbound upload request traffic on HTTPS, the DLP policies work with HTTPS inspection as follows:

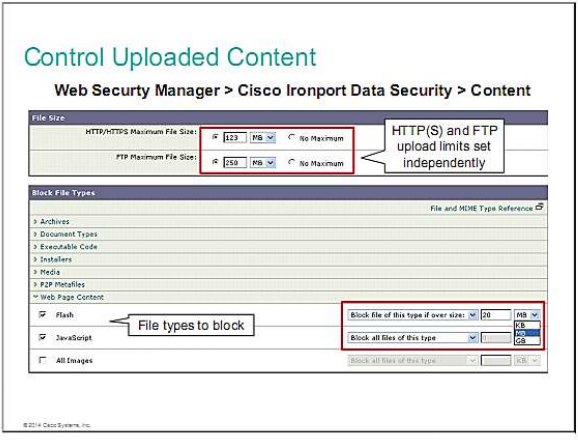
- The decryption policy is used to determine which traffic should be decrypted.
- If the decision is to decrypt the traffic, then the data security and data loss prevention policies are applied to the decrypted traffic.

In the example shown in the figure, the IT Group Data Security Policy is matched by the IT group identity and it using the global policy for URL Filtering and Web Reputation. For the Content control settings, it is using a custom setting which limits the HTTP/HTTPS maximum upload file size to 500MB and the FTP maximum upload file size to 1GB.

https://t.me/learningnets

Control Uploaded Content

This topic describes how to control uploaded content.



You can use the settings on the **Web Security Manager > Cisco IronPort Data Security Policies > Content** page to configure the Cisco Web Security Appliance to block data uploads based on the following file characteristics:

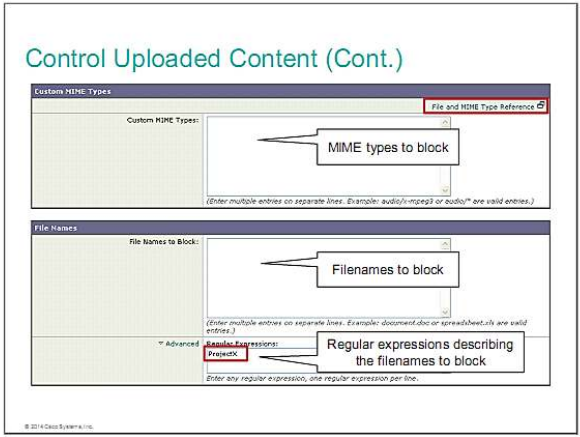
File size: Specify the maximum upload size allowed. All uploads with sizes equal to or greater than the specified maximum are blocked. You can specify different maximum file sizes for HTTP/HTTPS and native FTP requests.

File type: Block predefined file types or custom MIME types you enter. When you block a predefined file type, you can block all files of that type or files greater than a specified size.

File name: Block files with specified names. You can use text as a literal string or a regular expression for specifying file names to block.

Note Cisco IronPort Data Security Filters do not inspect the contents of archived files when blocking by file type. Archived files can be blocked by its file type or file name, not according to its content.

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



This figure illustrates the bottom part of the **Content** configuration page. To find the MIME type of an offending upload, you may want to look at the data security logs, and then add it to the **Custom MIME Types** field.

For some MIME types, blocking one type blocks all MIME types. For example, blocking **application/x-java-applet** blocks all java MIME types, such as application/java and application/javascript.

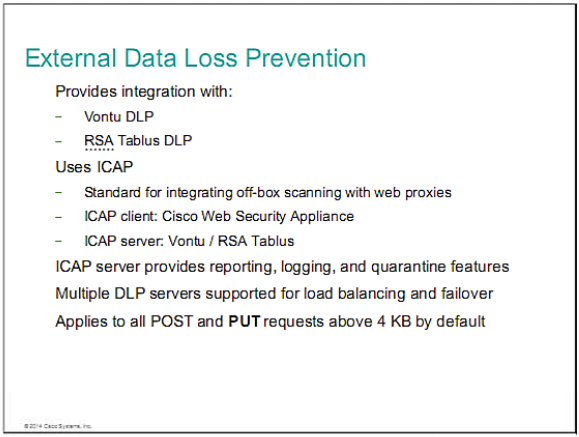
To block files with specified names, enter the file names in the **File Names to Block** field.

Note	As with custom URL categories, use regular expressions with caution. Note that you do not include the slash delimiters.

https://t.me/learningnets

External Data Loss Prevention

This topic describes the external DLP.



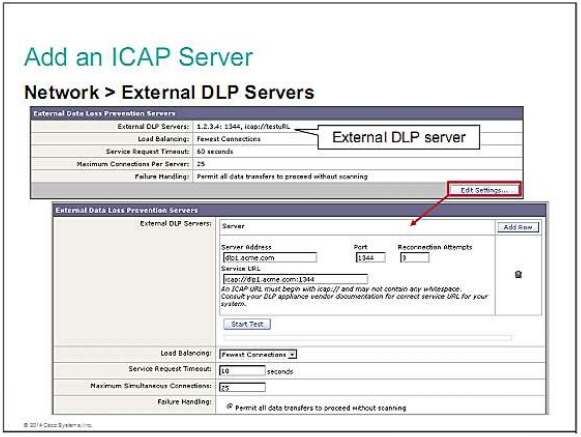
For enterprises that have already invested in special-purpose DLP systems, Cisco WSAs offer the option to interoperate with DLP vendors via ICAP.

By directing all outbound HTTP, HTTPS, and FTP traffic to the third-party DLP appliance, organizations can allow or block data based on the third-party rules and policies. This practice also enables deep content inspection for regulatory compliance and intellectual property protection, incident severity definition, case management, and performance optimization.

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

Add an ICAP Server

This topic describes how to add an ICAP server.



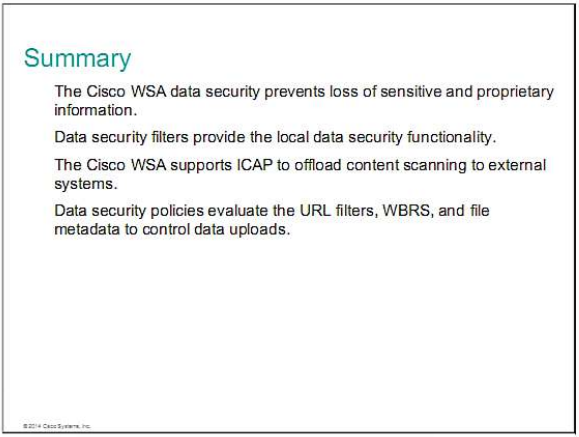
The Cisco Web Security Appliance can integrate with multiple external DLP servers from the same vendor by defining multiple DLP servers in the Cisco WSA. Define DLP systems and global settings that affect integration with all DLP systems by selecting **Network > External DLP Servers**.

You can define the load-balancing technique that the Cisco WSA uses when contacting the DLP systems. This is useful when you define multiple DLP systems. For example, the Cisco WSA can contact each DLP system using round-robin or a hash function.

https://t.me/learningnets

Summary

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



References

For additional information, refer to these references:

Cisco IronPort AsyncOS for Web User Guide

http://www.cisco.com/en/US/docs/security/wsa/wsa7.5/user_guide/WSA_7.5.0_UserGuide.pdf

http://www.cisco.com/en/US/docs/solutions/SBA/February2013/Cisco_SBA_BN_WebSecurityUsingCiscoWSADeploymentGuide-Feb2013.pdf

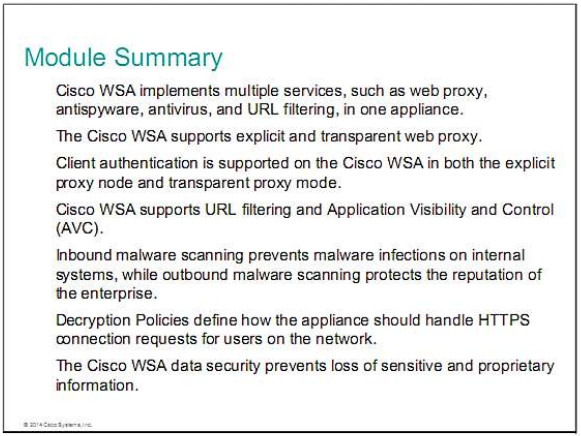
Web Security Deployment Guide

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

Module Summary

Overview

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



References

For additional information refer to this resource:

Latest Cisco IronPort AsyncOS for Web User Guide

https://t.me/learningnets

© 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. What are four major features of the Cisco WSA? (Choose four.) (Source: Cisco Web Security Appliance Overview)

   A. NGFW
   B. Web Proxy and HTTPS Decryption
   C. AVC
   D. Anti-Malware
   E. URL Filtering
   F. NGIPS

2. Which two types of Cisco WSA policies are used to control data that is uploaded to web servers? (Choose two.) (Source: Cisco Web Security Appliance Overview)

   A. Decryption policies
   B. Data security
   C. Access policies
   D. SaaS policies
   E. Data loss prevention
   F. Outbound malware scanning

3. What are the two primary purpose of Cisco WSA identities? (Choose two) (Source: Cisco Web Security Appliance Overview)

   A. Used to group user transaction requests for applying access or decryption policies
   B. Used to enable identity policy objects to be used as matching criteria in access polices
   C. Used to implement time based access policies
   D. Used to determine the authentication requirement

https://t.me/learningnets

4. What information can be provided via DHCP in an explicit proxy deployment with Cisco WSA? (Source: Deploying Cisco Web Security Appliance Integration Features)

   A. Web Cache Control Protocol (WCCP) address
   B. Network choke point address
   C. Web Proxy Auto-Discovery (WPAD) URL
   D. Web ports

5. Which method would you use on the Cisco ASA to deploy Cisco WSA transparent web proxy? (Source: Deploying Cisco Web Security Appliance Integration Features)

   A. Web Cache Control Protocol (WCCP) v2
   B. Policy Based Routing (PBR)
   C. Web Proxy Auto-Discovery (WPAD)
   D. Layer 4 or 7 redirection
   E. Transparent Proxy Control Protocol (TPCP)

6. What are two purposes of the user authentication in Cisco WSA? (Choose two) (Source: Deploying Cisco Web Security Appliance Authentication Features)

   A. Set up different web access policies by user or group membership against a central user directory.
   B. Facilitate 802.1X.
   C. Enable user tracking.
   D. Enable identity objects.

7. Which two client authentication schemes are supported on Cisco WSA? (Source: Deploying Cisco Web Security Appliance Authentication Features)

   A. LDAP
   B. Explicit proxy
   C. Transparent proxy
   D. NTLM Security Support Provider (NTLMSSP)
   E. RADIUS
   F. NT LAN Manager (NTLM)
   G. Basic

8. Which scanning engine is called to categorize a transaction that failed categorization using only the URL in the client request? (Source: Deploying Cisco Web Security Appliance Web Usage Controls)

   A. Web Usage Control engine
   B. Application Visibility and Control engine
   C. Dynamic Content Analysis
   D. WSA Scanning engine

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

9. Which string will match all subdomains of cisco.com without using the regular expressions in the URL category definition? (Source: Deploying Cisco Web Security Appliance Web Usage Controls)

A. cisco.com
B. ^cisco.com
C. *.cisco.com
D. .cisco.com

10. Which WSA engines can be combined in a policy group? (Source: Deploying Cisco Web Security Appliance Anti-Malware Controls)

A. DVS, Sophos, and McAfee
B. Webroot, Sophos, and McAfee
C. Dynamic Vectoring and Streaming (DVS), Webroot, and McAfee
D. WBRS, Webroot, and Sophos

11. Which statement describes the inbound malware scanning on Cisco WSA? (Source: Deploying Cisco Web Security Appliance Anti-Malware Controls)

A. Protects the enterprise reputation.
B. Protects internal computers from infection.
C. Protects customers and partners from infection.
D. Stops malware that is on computers inside the network from leaving the network.

12. Which parameters are evaluated in the data security policy on Cisco WSA? (Source: Deploying Cisco Web Security Appliance Data Security Controls)

A. Direction of the content transfer
B. Infection state
C. Web reputation of the source
D. Web reputation of the destination

https://t.me/learningnets

Answer Key

1. B, C, D, E
2. B, E
3. A, D
4. C
5. A
6. A, C
7. D, G
8. C
9. D
10. C
11. B
12. D

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

Module 3

Cisco Cloud Web Security

Introduction

Web security threats have become more sophisticated, targeted, and harder to avoid. Yet the use of personal devices and cloud-delivered services limit your visibility and control. Cisco Cloud Web Security (CWS), formerly known as ScanSafe, delivers web security and control for organizations of all sizes, with multiple deployment options and tight integration into your Cisco data center, network, or branch office.

This module introduces Cloud Web Security and its deployment and traffic redirection to the cloud.

Upon completing this module, you will be able to meet these objectives:

- Describe the main features of the Cisco Cloud Web Security
- Describe traffic redirection to Cloud Web Security through connectors, how to configure them on Cisco ASA, Cisco WSA and Cisco IOS, and how to configure AnyConnect web security module
- Describe how to configure web filtering policy and how to verify web filtering

https://t.me/learningnets

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

Lesson 1

Describing the Cisco Cloud Web Security Solutions

Overview

Web access is a requirement for the day-to-day functions of most organizations, but a challenge exists to maintain appropriate web access for everyone in the organization, while minimizing unacceptable or risky use. A solution is needed to control policy-based web access in order to ensure employees work effectively and ensure that personal web activity does not waste bandwidth, affect productivity, or expose the organization to undue risk.

Cisco Cloud Web Security addresses the need for a corporate web security policy by offering a combination of web usage controls with category and reputation-based control, malware filtering, and data protection. This comprehensive hosted service is also known as Cisco CWS, formerly known as Scansafe. This lesson provides overview of CWS technology and needed components in CWS solution.

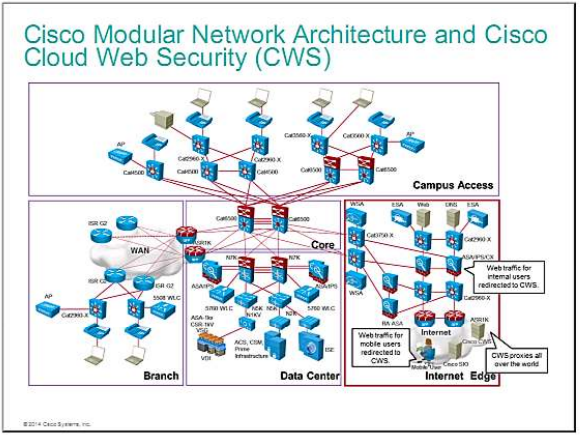
Upon completing this lesson, you will be able to meet these objectives:

- Identify how to place Cisco Cloud Web Security integration into a typical modularized network design
- Describe the Cisco Cloud Web Security solution
- Describe the Cisco Cloud Web Security traffic flow
- Describe the cloud web security URL Filtering, AVC and Reporting features
- Describe the cloud web security scanning processes
- List the features of the Cisco ScanCenter

https://t.me/learningnets

Cisco Modular Network Architecture and Cisco Cloud Web Security (CWS)

This topic identifies how to place Cisco Cloud Web Security integration into a typical modularized network design.



The figure illustrates where in the Cisco modular network architecture the Cisco CWS integration should be deployed. You should redirect HTTP and HTTPS traffic from your users, whether internal or mobile users, to the Cisco CWS Servers, which have a broad geographic distribution. The Cisco ScanCenter is the administrative portal, where you create the Web filters and rules to enforce your company Web security policies.

Cisco CWS addresses the need for a corporate web security policy by offering a combination of web usage controls with category and reputation-based control, malware filtering, and data protection. Cisco CWS is a cloud-based method of implementing web security that is similar in function to the Cisco Web Security Appliance, which uses an on-premise appliance for web security.

Browsing websites can be risky, and many websites inadvertently end up distributing compromised or malicious content as a result of inattention to update requirements or weak security configurations. The websites that serve the compromised and malicious content are constantly changing as human-operated and worm-infested computers scan the internet in search of additional web servers that they can infect in order to continue propagating. This dynamic environment introduces significant challenges to maintain up-to-date internet threat profiles.

Through the use of multiple techniques, Cisco CWS provides granular control over all web content that is accessed. These techniques include real-time dynamic web content classification, a URL-filtering database, and file-type and content filters. The policies enforced by Cisco CWS provide strong web security and control for an organization. Cisco CWS policies apply to all users regardless of their location and device type.

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

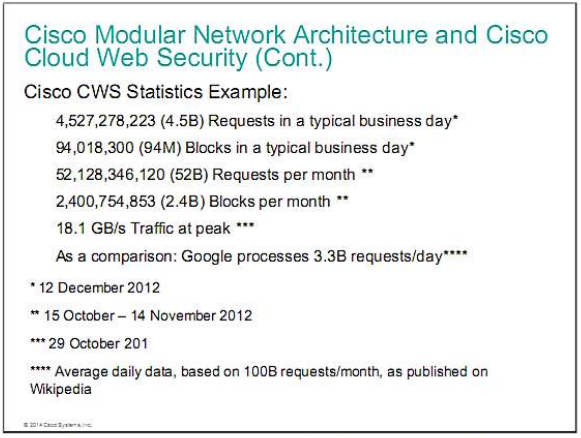
Internal users in the figure access the internet by using the internet-edge Cisco Adaptive Security Appliance, which provides stateful firewall and intrusion prevention capabilities. It is simple and straightforward to add Cisco CWS to a Cisco ASA appliance that is already configured and operational. This integration uses the Cloud Web Security Connector for Cisco ASA and requires no additional hardware.

The Cisco ASA firewall family sits between the organization's internal network and the internet and is a fundamental infrastructural component that minimizes the impact of network intrusions while maintaining worker productivity and data security. The design uses Cisco ASA to implement a service policy that matches specified traffic and redirects the traffic to the Cisco CWS cloud for inspection. This method is considered a transparent proxy, and no configuration changes are required to web browsers on the end user devices.

The Cisco CWS cloud is accessed through a network of proxy servers, which have a broad geographic distribution in order to support a globally diverse set of customers. Specific details for which proxy servers to use are provided by Cisco and based on the location and size of the deployment.

Mobile remote users connect to their organization's network by using the Cisco AnyConnect Secure Mobility Client. It is suboptimal to force all user traffic to the central site when using a remote-access VPN. This central-tunneling approach adds increased latency to internet bound user traffic and unnecessarily congests the central site's internet link. Enabling the Cisco CWS module for the Cisco AnyConnect client allows an organization to use a split-tunneling approach. Only traffic originating from within the organization is sent to the central site. All web traffic to the internet from remote-access VPN users accesses the internet through the cloud-based CWS service.

Cisco CWS is administered by using the CWS ScanCenter web portal. This includes creating filters and rules for policies, creating groups, activating keys, and viewing reports.



Cisco Security Intelligence Operations provides zero-day threat protection to all users, regardless of location. CWS relies on the strength of Cisco's data centers and offers strong, reliable security.

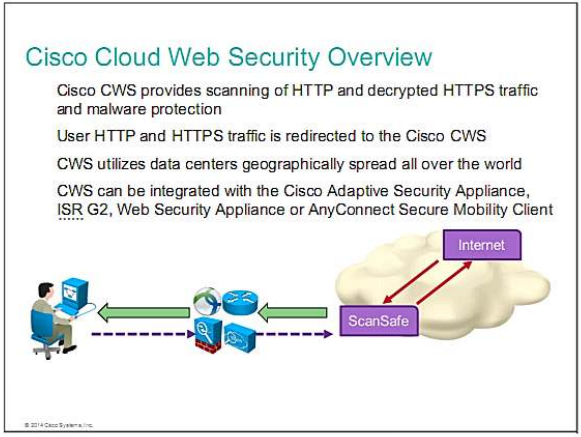
Cisco SIO receives automatic updates every three to five minutes and provides a 24x7 view into global traffic activity, enabling Cisco to analyze anomalies, uncover new threats, and monitor traffic trends. Cisco SIO generates new rules and website reputation scores as soon as new threats are detected. These near real-time updates enable CWS to deliver comprehensive threat defense hours or even days ahead of competitors

The figure shows some of the statistics obtained from the Cisco CWS ScanCenters.

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

Cisco Cloud Web Security Overview

This topic describes Cloud Web Security solution.



Web security can be ensured by using 'on premise' web security appliances or cloud web security. Cisco offers numerous appliances to ensure network security. Cisco also offers comprehensive, hosted CWS.

Cisco CWS is a SaaS product. It provides real time scanning and protection from malware, including previously unknown threats, so called Zero Day Threats. Cisco CWS is also known by its former name ScanSafe.

Cisco CWS data center is located 'in the cloud'. Cisco employs numerous data centers geographically spread all over the world to provide this service. These data centers are interconnected and redundant, so this network is characterized by the highest uptime and is very reliable. The Cisco CWS proxy servers in the world wide data centers have visibility of different and evolving network threats. This way it provides the most effective defense against all types of malware.

Cisco CWS is managed through the Cisco ScanCenter web portal. The Cisco ScanCenter web portal is the place where you can define policies, including user based policies, to prevent malicious or unwanted content to enter your network, and also prevent confidential data to leave your network. The rich reporting functions in the Cisco ScanCenter provides reportings based on many different attributes.

Besides providing security services to onsite Internet users, Cisco CWS also provides the same level of service to remote or mobile users. For these purposes, the Cisco AnyConnect Mobility Client 3.0 with the Web Security module is used.

Cisco CWS can be integrated with multiple Cisco network infrastructure elements to further enhance flexibility:

ASA connector: Cisco ASA integrates with Cisco CWS to solve the combined problems of performance and breadth of security without affecting data center and network complexity

ISR G2 connector: Save bandwidth, money, and resources by intelligently redirecting branch traffic to the cloud to enforce security and control policies away from headquarters.

Cisco AnyConnect Secure Mobility Client with the Web Security Module: Securely connects roaming users directly to the Internet through the nearest CWS proxy server. By eliminating the need to backhaul web traffic via VPN, CWS relieves web congestion at headquarters, reducing bandwidth usage while improving the end-user experience.

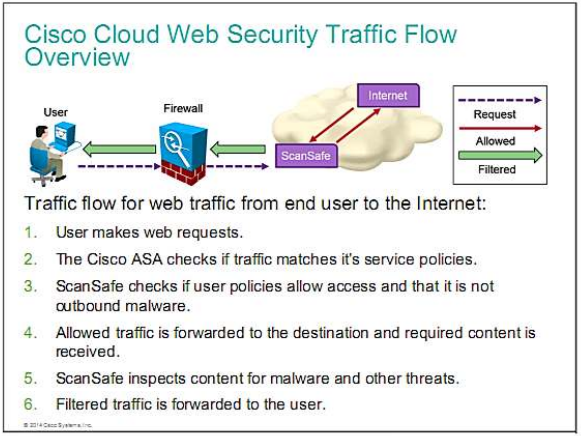
Web Security Appliance connector: Processing is moved to the cloud, lifting the computing load from the on-premises WSA and centralizing management of access policy and reporting across the cloud. WSA connector is supported on the 7.5.7 WSA special release and will be available in the 8.0 general WSA release.

Note The Cisco CWS feature was formerly called ScanSafe. The Cisco CWS licenses are term-based subscription licenses that are one, three, or five years based which uses tiered pricing based on the number of users, not devices.

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

Cisco Cloud Web Security Traffic Flow Overview

This topic describes Cloud Web Security traffic flow.



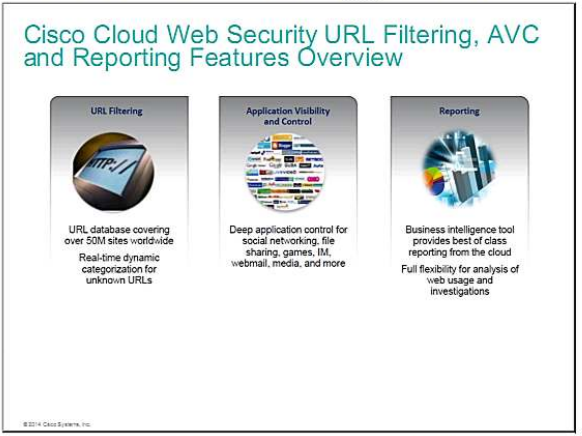
This slide describes the traffic flow for web traffic from end user to the Internet, when Cisco Adaptive Security Appliance is deployed as CWS connector:

1. User which is located behind the firewall makes his web request.
2. The Cisco ASA checks its service policies and if compliant, redirects traffic to ScanSafe.
3. ScanSafe first ensures that this is a permitted and valid web request and not an outbound malware.
4. ScanSafe then checks the validity of request against its policies.
5. Traffic which is allowed is forwarded to the desired destination in Internet and traffic from web site is returned to ScanSafe.
6. The received content is now scanned thoroughly for viruses and other malware.
7. Content which has passed the controls and deemed safe is forwarded to the user.
8. The latency added to the traffic by ScanSafe is no more than 50ms!

https://t.me/learningnets

Cisco Cloud Web Security URL Filtering, AVC and Reporting Features Overview

This topic describes the cloud web security URL Filtering, AVC and Reporting features.



URL Filtering: Cloud Web Security uses URL filtering and Dynamic Content Analysis to protect organizations from compliance, liability, and productivity risks by combining traditional URL filtering with real-time dynamic content analysis. The URL filtering database provides real-time coverage for known websites while Cisco's DCA engine accurately identifies web content that purely list-based URL filters would miss using real-time dynamic categorization for unknown URLs. The Cisco URL database covering over 50M sites worldwide. The additional outbound content control can be enabled to provide additional filtering options. The outbound content control component of CWS prevents leaks and data loss and ensures compliance. It prevents sensitive information from leaving the organization's network, helping to ensure compliance and reduce risk. Outbound content control provides the flexibility to define rules based on the HTTP protocol's POST function.

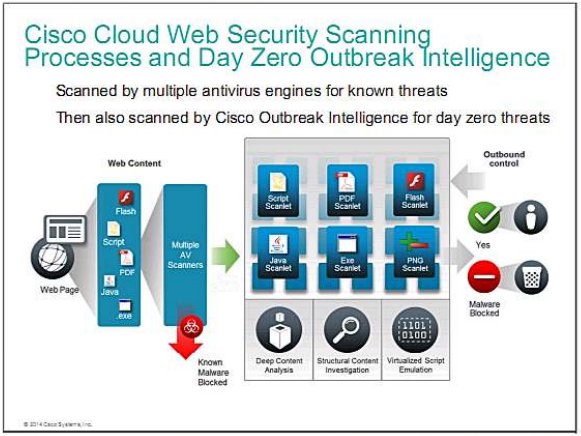
Application Visibility and Control: CWS uses AVC to ensure acceptable use and security policy enforcement with deep application control for social networking, file sharing, games, IM, webmail, media, and more. AVC enables you to easily set policy and control usage for hundreds of Web 2.0 applications and 150,000+ micro-applications. Granular policy control allows administrators to permit the use of applications such as Facebook or Dropbox while blocking users from activities such as chatting or uploading documents

Reporting: CWS includes business intelligence reporting tool to provide best of class reporting from the cloud for analysis of web usage. It provides ultimate flexibility in the reporting criteria with 100+ different attributes for each web request and provides multiple output types, detailed reports, time trending and automated scheduling.

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

Cisco Cloud Web Security Scanning Processes and Day Zero Outbreak Intelligence Overview

This topic describes the cloud web security scanning processes.



When the user traffic is processed by the Cisco Cloud Web Security, all inbound and outbound user traffic follows the same treatment.

Content which enters Cisco CWS scan center is first broken down into types, like PDF, EXE, GIF, Java, scripts etc.

These files are then scanned by more than one latest technology 3rd party antivirus signature based engines. This scan is signature based and searches for already known threats.

At this stage, all known malware is blocked.

Traffic that comes clean from this scan is delivered to Outbreak Intelligence. This is a Cisco proprietary heuristic scan engine, which looks for previously unknown threats. Outbreak Intelligence is vastly different from traditional signature based antivirus. It is a heuristics engine, based on artificial intelligence using the billions of web requests per day to train the system on good and bad, there is no waiting for signature updates in order to block malware which means the window of opportunity for zero-day threats is effectively eliminated. When an end user visits a web page, that web page is decomposed down to the components that are present on that page, html, scripts, flash, PDFs and etc and once passed through the mulitple antivirus engines, the Outbreak Intelligence "scanlets" scan each piece of content in parallel using 3 different techniques designed to accurately detect zero-day malware.

Content is again broken into types. Highly parallelized engines, "scanlets" scan for potentially harmful content. Three techniques are used for this scan:

- **Deep Content Analysis:** Content is analyzed for suspicious anomalies, like executable code in image file, animated GIF file with only one frame etc.

- **Structural Content Investigation:** Content is controlled structurally for potentially harmful, hidden behavior.
- **Virtualized Script Emulation:** Very important part of the scan, because it runs suspicious scripts in virtualized cloud infrastructure, to check for potentially hidden malicious behavior.

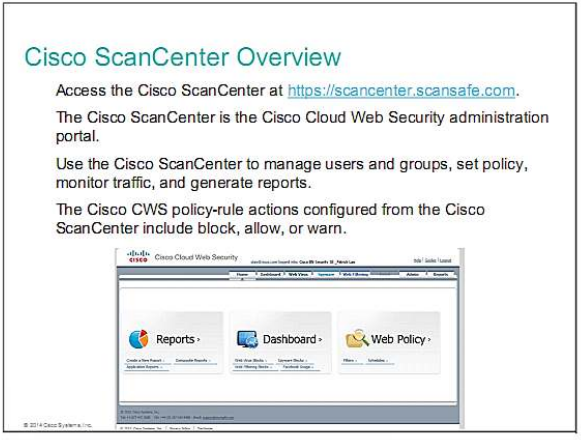
After this scan, traffic content is determined to be safe or not. If certain parts of content are found to be harmful, outbreak Intelligence will try to partially block just them on the page. If that is not possible, the whole page will be blocked.

In 2012, 25% of Web malware was blocked by Cisco Outbreak Intelligence before signature detection became available.

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

Cisco ScanCenter Overview

This topic lists the features of Cisco ScanCenter.



Cisco ScanCenter is the Cisco CWS administration portal. From this portal, the CWS administrator can manage users and groups, set policy, monitor traffic, and generate reports.

Access the Cisco ScanCenter at https://scancenter.scansafe.com.

In the Cisco ScanCenter, traffic is matched against policy rules. When a rule is matched, Cisco CWS applies the configured action for the rule.

Cisco CWS policy-rule actions includes block, allow, or send a warning about a user request:

Block: When Cisco CWS blocks a client request, the service notifies the user that access has been blocked. CWS sends an HTTP 302 "Moved Temporarily" response that redirects the client application to a web page that is hosted by the CWS proxy server and that shows the blocked error message. Cisco Adaptive Security Appliance forwards the 302 response to the client.

Allow: When Cisco CWS allows a client request, the service contacts the originally requested server and retrieves the data. CWS forwards the server response to Cisco ASA, which then forwards the response to the user.

Warn: When the Cisco CWS proxy server determines that a site might be in breach of acceptable use policy, the service displays a warning page about the site. You can choose to accept the warning and drop the request to connect, or you can click through the warning and proceed to the requested site.

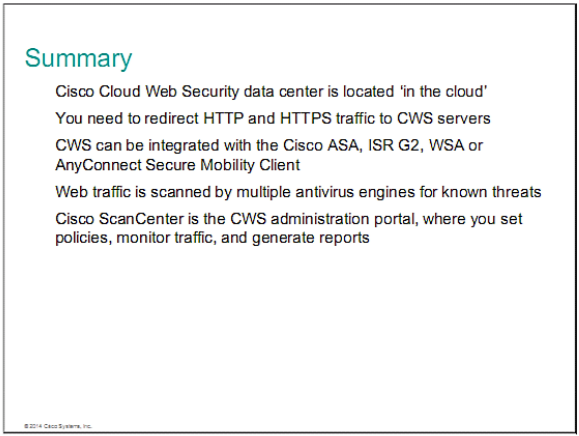
Anonymize: Users' identities will be hidden in reports.

Authenticate: This action triggers an authentication process. This is typically used for the direct to cloud users (not using the CWS connector on the Cisco devices like ASA, ISR-G2 or Web Security Appliance for traffic redirection).

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 2

Configuring Cisco Cloud Web Security Connectors

Overview

Cisco Cloud Web Security is SaaS Cisco product which provides web security and web filtering services. Companies which have Cisco Adaptive Security Appliance or Cisco IOS G2 routers in their network can use them as connectors to redirect their web traffic to the Cisco CWS, to get web security, but also to enforce their web policies and URL filtering. Cisco AnyConnect Secure Mobility client is a VPN client, which provides users with remote access to ASA appliances, using secure IPsec or SSL VPN connections. It can also be configured to access Cisco CWS. This lesson explain how to configure and verify the different CWS connectors, including the CWS connector on the Cisco ASA, ISR G2 and AnyConnect Mobility Security client. This lesson also describe the configuration requirements for the CWS connector on the Cisco Web Security Appliance.

Upon completing this lesson, you will be able to meet these objectives:

- Describe cloud web security connectors
- Describe how to obtain the correct type of Cisco Cloud Web Security authentication key
- Describe how to generate a company authentication key from Cisco ScanCenter
- Describe how to verify traffic redirection from CWS connector to the Cisco Cloud Web Security proxy servers
- Describe the Cisco ASA Cloud Web Security feature
- Describe how to configure the Cisco ASA using ASDM to integrate with the Cisco CWS
- Describe how to configure the Cisco Cloud Web Security proxy servers in Cisco ASA using the CLI
- Describe how to configure the Cisco Cloud Web Security proxy servers in Cisco ASA with the Whitelist and Identity options
- Describe how to use Cisco ASDM to verify Cisco Cloud Web Security operations
- Describe how to use the CLI to verify Cisco Cloud Web Security operations in Cisco ASA

https://t.me/learningnets

Provide Cisco AnyConnect Web Security Module overview

Describe the overview of installing the Cisco AnyConnect Web security Module procedure

Describe how to configure Cisco AnyConnect Web Security Module for Standalone Use

Describe how to configure Cisco ASA to download Cisco AnyConnect Web Security Module to the client machine

Describe how to verify Cisco AnyConnect Web Security Module operations.

Provide overview of Cloud Web Security connector on Cisco ISR G2 routers

Describe how to configure Cloud Web Security connector on Cisco ISR G2 router using the CLI

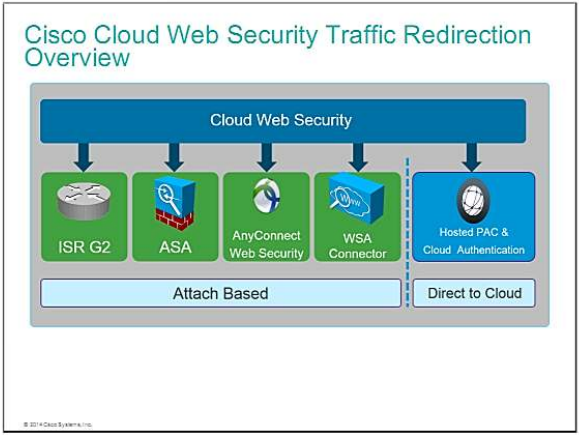
Describe how to verify Cloud Web Security connector operation on Cisco ISR G2 router

Provide Cisco WSA Cloud Web Security overview.

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

Cisco Cloud Web Security Traffic Redirection Overview

This topic describes cloud web security connectors.



There are two methods to redirect user HTTP and HTTPS traffic to Cisco Cloud Web Security, using the connector approach which leverages the existing Cisco device or using the direct to cloud approach.

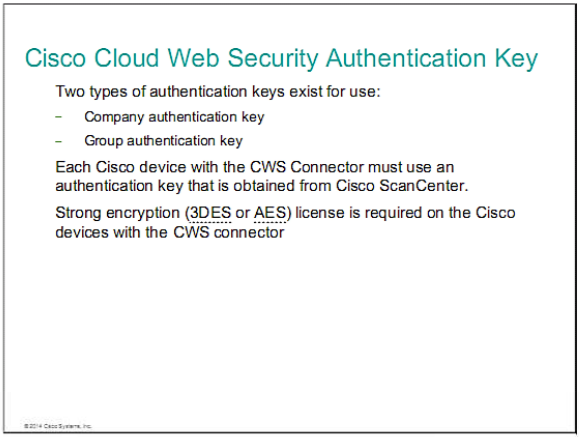
Cisco CWS is a SaaS web security service. Traditional web security services require complex configuration on end-user PCs to set up a web proxy that can provide threat protection from malicious and out-of-policy web sites. The Cisco CWS Connector eliminates that overhead for the IT organization by incorporating the connection to the Cisco CWS service directly from the existing Cisco devices such as the ISR G2, Cisco Adaptive Security Appliance, Cisco Web Security Appliance or AnyConnect mobility security client.

When no Cisco device is available, web traffic can still be redirected to the cloud through web browser proxy settings/hosted proxy auto configuration for browser redirection or by traffic forwarding on any other perimeter device that supports port forwarding of web traffic via port 8080.

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

Cisco Cloud Web Security Authentication Key

This topic describes how to obtain the correct type of Cisco Cloud Web Security authentication key



Each Cisco devices with the CWS connector must use an authentication key that is generated from the Cisco ScanCenter. When the CWS administrator generate the key from the Cisco ScanCenter, the CWS administrator will receive an email message. This email contains the key information. Save this email so the key can be retrieved later, if needed.

Note	After the key is obtained, the Cisco CWS administrator cannot look up the key in the Cisco ScanCenter. Only the last four digits are shown in the Cisco ScanCenter.

After the key has been generated from the Cisco ScanCenter, the CWS administrator can deactivate or revoke the key.

The authentication key allows CWS to identify the company that is associated with web traffic inspection requests. The key ensures that the correct Cisco device with the CWS connector is associated with the valid customer.

Two types of authentication keys can be used: a company authentication key or a group authentication key.

A company authentication key can be used on multiple Cisco devices with the CWS connector within the same company. This key simply enables the CWS service for all your Cisco devices with the CWS connector.

A group authentication key is a special key that can be unique on each Cisco devices with the CWS connector (or group of Cisco devices with the CWS connector).

For example, a unique group key can be used on each Cisco device with the CWS connector to differentiate between the traffic from each Cisco device with the CWS connector and to apply separate policy rules for each Cisco device with the CWS connector .

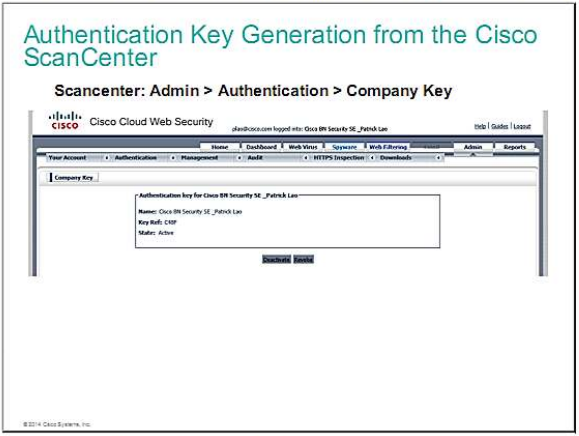
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Note	To support CWS, a strong encryption (3DES/AES) license is required on the Cisco device with the CWS connector to encrypt the traffic between Cisco device and the Cisco CWS server.

https://t.me/learningnets

Authentication Key Generation from the Cisco ScanCenter

This topic describes how to generate a company authentication key from Cisco ScanCenter.



From the Scancenter **Admin > Authentication > Company Key** page, the Cisco Cloud Web Security administrator can generate a company key, group key, or user key.

Below shows an example for generating a company key:

New authentication keys have been created

Company Name: Cisco BN Security SE _Pxxxxxx Lxx

Name: Cisco BN Security SE _Pxxxxxx Lxx Authentication Key Type: Company Authentication Key: 1111222233334444555566667777C48F

After you generate the key from ScanCenter, you will also receive the key in an email as shown in the slide.

From the Scancenter **Admin > Authentication > Company Key** page, the CWS administrator can also deactivate or revoke the key.

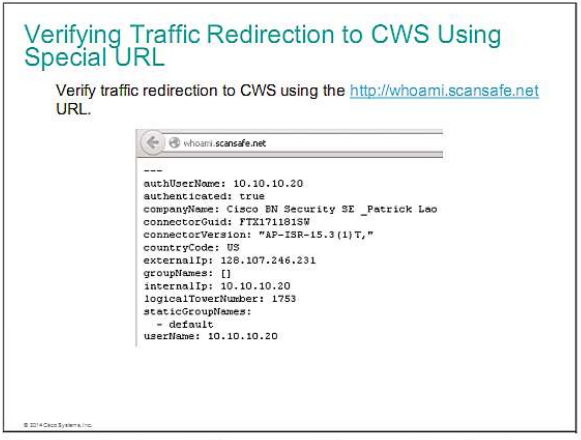
Noticed that once the key is generated, the full key can't be viewed again from the ScanCenter Web Portal, only the last four digits of the key is displayed.

Refer to the ScanCenter administration guide for information about generating group authentication keys instead of a company authentication key.

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

Verifying Traffic Redirection to CWS Using Special URL

This topic describes how to verify traffic redirection from Cisco Cloud Web Security connector to the Cisco CWS proxy servers.



You can verify traffic redirection to CWS (no matter which connector is configured) using special URL. From a web browser, access http://whoami.scansafe.net. Details such as the company name, the CWS connector version, and so on are displayed if the traffic is being redirected to the Cisco CWS proxy server.

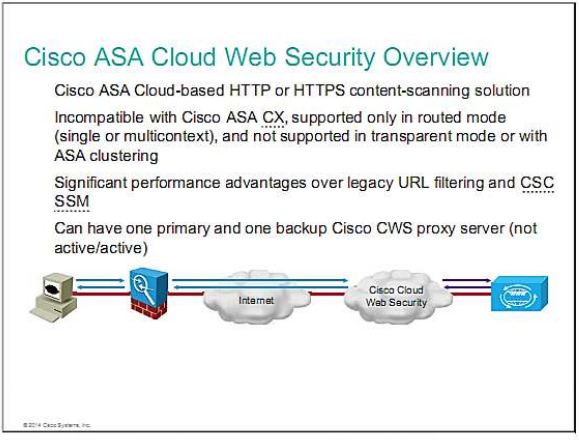
As shown in the figure, the internal 10.10.10.20 IP address is the pre-NAT IP address of the system behind the Cisco device with the CWS connector that is triggering the HTTP connection.

If a message is displayed stating "User is not currently using the service", then client web traffic is not being redirected to the Cisco CWS proxy server.

https://t.me/learningnets

Cisco ASA Cloud Web Security Overview

This topic describes the Cisco Adaptive Security Appliance Cloud Web Security feature.



Cisco CWS provides web security and filtering services through an SaaS model. An enterprise that has a Cisco ASA in its network can use Cisco CWS services without installing additional hardware.

When an end user sends an HTTP or HTTPS request, the Cisco ASA receives it and, optionally, retrieves the user or group information. If the traffic matches a Cisco ASA service policy rule for Cisco CWS, then the Cisco ASA redirects the request to the CWS proxy servers. The Cisco ASA acts as an intermediary between the end user and the Cisco CWS proxy server by redirecting the connection to the proxy server. The Cisco ASA changes the destination IP address and port in the client requests, adds specific CWS HTTP headers, and then sends the modified request to the Cisco CWS proxy server. The Cisco CWS HTTP headers include various types of information, including username and user group (if available). The Cisco CWS proxy servers then scan the content and allow it, block it, or send a warning about the traffic, based on the policy that is configured in Cisco ScanCenter, which enforces acceptable use and protects users from malware.

You can configure a primary and a backup Cisco CWS proxy server, each of which the Cisco ASA polls regularly to check for availability.

Cisco CWS is not supported with Cisco ASA CX. If you configure both Cisco ASA CX and Cisco CWS inspection for the same traffic, then the Cisco ASA performs only the Cisco ASA CX inspection.

Cisco CWS inspection is compatible with HTTP inspection for the same traffic. HTTP inspection is disabled by default as part of the default Cisco ASA global policy.

Cisco CWS currently supports only IPv4 addresses. If you use IPv6 internally, then NAT 64 must be performed on the Cisco ASA for any IPv6 flows that need to be sent to Cisco CWS.

Cisco CWS is supported in routed firewall mode only, not in transparent firewall mode.

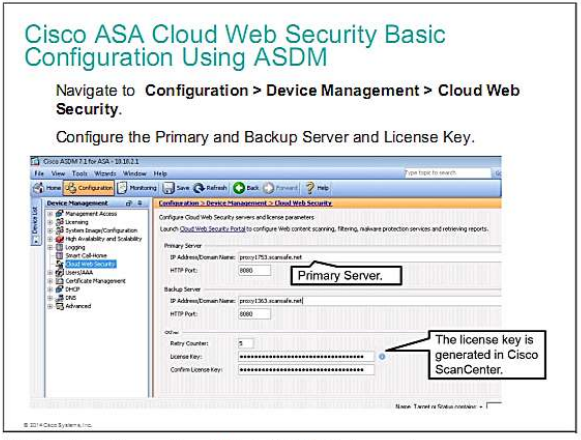
Cisco CWS is supported in multicontext mode.

Cisco CWS is not supported with Cisco ASA clustering.

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

Cisco ASA Cloud Web Security Basic Configuration Using ASDM

This topic describes how to configure the Cisco Adaptive Security Appliance using Adaptive Security Device Manager to integrate with the Cisco Cloud Web Security.



The Cisco CWS configuration on Cisco ASA is divided into two parts:

- The first part relates to the configuration of CWS proxy-server details, such as the server IP address, the port to which traffic must be redirected, license key, and so on.
- The second part of the configuration relates to identifying web traffic and enabling CWS inspection on the identified traffic. Use the Cisco ASA MPF for this part. To enable CWS, create a Layer 7 CWS policy-map and apply it to the Layer 3 and Layer 4 policy-map.

To configure the Cisco CWS proxy servers using Cisco Adaptive Security Device Manager, navigate to **Configuration > Device Management > Cloud Web Security** and enter the Primary and Backup Server FQDN or IP addresses. Primary and backup servers are assigned to the customer upon subscription to the CWS Service.

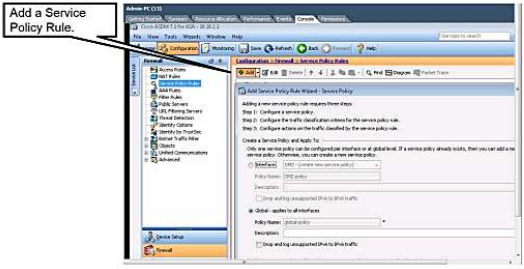
You can configure a primary and backup CWS proxy server. The Cisco ASA polls each server regularly (every 15 minutes) to check for availability. The CWS proxy server is polled through a TCP three-way handshake. If the CWS proxy server is unavailable after a configured number of retries (five, by default), then the server is declared unreachable and the backup CWS proxy server becomes active. Cisco ASA automatically falls back to the primary CWS proxy server from the backup CWS proxy server after continued polling shows that the primary proxy server is active for a configured number of consecutive retries.

Enter the license key which was generated in ScanCenter web portal. Next, you need to apply the configuration.

Cisco ASA Cloud Web Security Basic Configuration Using ASDM (Cont.)

Navigate to **Configuration > Firewall > Service Policy Rules**.

Add a Service Policy Rule.



Next, you need to define which traffic is going to pass through the Cisco ASA to be redirected to the CWS Navigate to **Configuration > Firewall > Service Policy Rules**. To add a service policy rule, click **Add**.

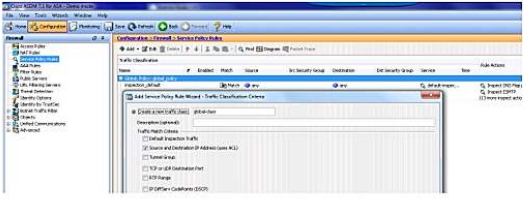
Policy rule can be defined for a particular interface or global, which will apply for all interfaces. In the figure, the global service policy is selected.

Cisco ASA Cloud Web Security Basic Configuration Using ASDM (Cont.)

Configuring Service Policy Rules:

Create a traffic classification.

Choose how do you want to define traffic matching criteria.



Traffic matching criteria can be defined using an ACL.

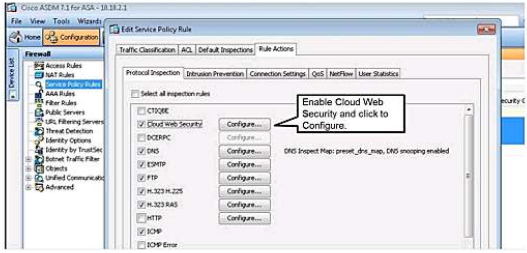
Enter the appropriate matching addresses for the source and the destination as a traffic matching criteria. The service field determines what type of service is matched in the criteria (not shown in the figure).

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

Cisco ASA Cloud Web Security Basic Configuration Using ASDM (Cont.)

Configuring Service Policy Rules (Cont.):

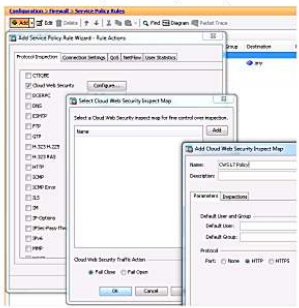
Choose **Cloud Web Security** and click **Configure**.



Now you need to choose **Cloud Web Security** for inspection. After enabling **Cloud Web Security**, click **Configure**.

Cisco ASA Cloud Web Security Basic Configuration Using ASDM (Cont.)

Configuring Service Policy Rules (Cont.):



Click **Add** to configure the inspect map (which is the layer 7 type inspect scansafe policy map) for CWS.

The **http** or **https** parameter specifies that the packets that are being forwarded to the CWS proxy servers are HTTP or HTTPS traffic. You can specify only one service type (HTTP or HTTPS) for each layer 7 CWS inspection policy map.

Other optional configurations such as sending identity and whitelist are also configurable within the layer 7 CWS inspection policy map under the **Parameters** and **Inspections** tab.

https://t.me/learningnets

The Cisco ASA can optionally be configured to send user name and user group identity information to the CWS proxy servers to enable differentiated services that are based on user identity and to provide user-based reporting (not shown in the figure).

Whitelist allows specific users and/or groups web traffic to go directly to the originally requested web server and not be scanned by CWS (not shown in the figure).

Finally, you have to determine what should the Cisco ASA do with the traffic that matches the criteria, but at that moment, the CWS proxy servers are not reachable.

There are two possibilities:

Fail Close: matching traffic will not be permitted.

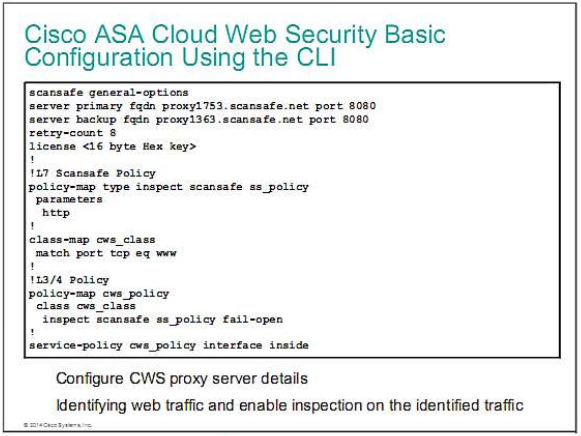
Fail Open: matching traffic will be permitted.

The last step is to apply the configuration to Cisco ASA and save it. The Cisco ASA is now ready to redirect the matching traffic to the CWS.

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

Cisco ASA Cloud Web Security Basic Configuration Using the CLI

This topic describes how to configure the Cisco Cloud Web Security proxy servers in Cisco Adaptive Security Appliance using the CLI.



The Cisco CWS configuration on Cisco ASA is divided into two parts:

The first part relates to the configuration of CWS proxy-server details, such as the server IP address, the port to which traffic must be redirected, license key, and so on. Use the **scansafe general-options** command for this part.

- Configure the CWS proxy server details by using the **scansafe general-options** global configuration command. This command is available only in the system context mode when using multicontext.
- You can configure a primary and backup CWS proxy server using the **server** command under the **scansafe general-options** configuration mode. The Cisco ASA polls each server regularly (every 15 minutes) to check for availability. The CWS proxy server is polled through a TCP three-way handshake. If the CWS proxy server is unavailable after a configured number of retries (five, by default), then the server is declared unreachable and the backup CWS proxy server becomes active. Cisco ASA automatically falls back to the primary CWS proxy server from the backup CWS proxy server after continued polling shows that the primary proxy server is active for a configured number of consecutive retries. Use the **retry-count** command to change the default retry count.
- Use the **license** command to configure the authentication key that the Cisco ASA sends to the CWS proxy servers to indicate from which organization the request comes. The authentication key is a 16-byte hexadecimal number and is obtained from the Cisco ScanCenter. This configuration is mandatory. Without the authentication key, traffic is not redirected to the CWS proxy servers.

The second part of the configuration relates to identifying web traffic and enabling inspection on the identified traffic. Use the Cisco ASA MPF for this part. Apply the Layer 7 **inspect scansafe** policy to the Layer 3 and Layer 4 policy.

- Use the **policy-map type inspect scansafe <name>** command to create an inspection policy map so that you can configure essential parameters for the ScanSafe inspection rule and (optionally) identify the whitelist.
- The **http | https** parameter specifies that the packets that are being forwarded to the CWS proxy servers are HTTP or HTTPS traffic. You can specify only one service type (HTTP or HTTPS) for an inspection policy map.
- The **inspect scansafe <scansafe_policy_name> [fail-open | fail-close]** command applies the Layer 7 **inspect scansafe** policy to the Layer 3 and Layer 4 inspection policy map.
- You can also choose how Cisco ASA processes web traffic when Cisco ASA cannot reach either the primary or backup CWS proxy server. Cisco ASA can block or allow all the web traffic by using the **fail-open** or **fail-close** options; **fail-close** is the default.
- Use the **service-policy** command to apply the ScanSafe policy on an interface or globally.

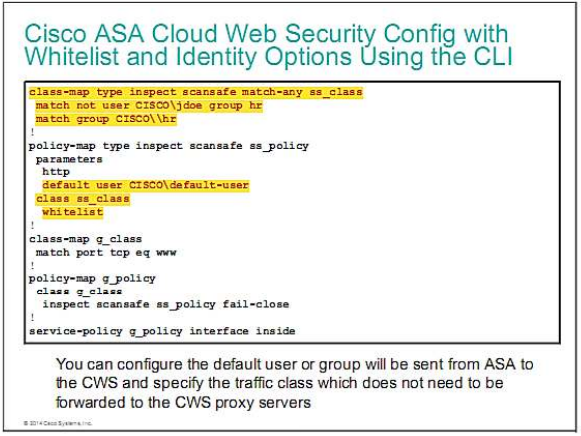
The configurations below shows another example that uses two classes: one for HTTP and one for HTTPS where all HTTP and HTTPS traffic from the inside interface is re-directed to the CWS. To customize the traffic to be sent to the CWS, when creating the service policy rules, modify the access-list that matches the traffic to the layer 3 and layer 4 policy-map.

```
access-list SCANSAFE_HTTPS extended permit tcp any4 any4 eq 443
access-list SCANSAFE_HTTP extended permit tcp any4 any4 eq 80
!
class-map cws_class1
match access-list SCANSAFE_HTTP
!
class-map cws_class2
match access-list SCANSAFE_HTTPS
!
policy-map type inspect scansafe cws_inspect_pmap1
 parameters
  http
!
policy-map type inspect scansafe cws_inspect_pmap2
 parameters
  https
!
policy-map cws_policy
 class cws_class1
  inspect scansafe cws_inspect_pmap1 fail-open
 class cws_class2
  inspect scansafe cws_inspect_pmap2 fail-open
!
service-policy cws_policy inside
```


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

Cisco ASA Cloud Web Security Configuration with the Whitelist and Identity Options Using the CLI

This topic describes how to configure the Cisco Cloud Web Security proxy servers in Cisco Adaptive Security Appliance with the Whitelist and Identity options.



The Cisco ASA can send user information, such as the user pre-NAT IP address or optionally configured to send user name and user group identity information to the CWS proxy servers to enable differentiated services that are based on user identity and to provide user-based reporting.

The Cisco ASA encrypts and includes user credentials (including username or user group name) with the traffic that it redirects to the CWS proxy server. The CWS proxy server then uses the user credentials to match the traffic to the CWS policy that is configured in Cisco ScanCenter. The proxy server also uses these credentials for user-based reporting in the Cisco ScanCenter.

The user names and group names are not mandatory for the CWS proxy server to apply the CWS policy. The Cisco ASA can optionally identify users by using the Identity Firewall or Cut-Thru Proxy feature. The Identity Firewall or Cut-Thru Proxy features are not covered in this course.

The **default** command specifies that if the Cisco ASA cannot determine the identity of the user, then the default user or group will be sent to the CWS. As shown in the figure, the Cisco ASA will send **default-user** in the **Cisco** domain as the user name to the CWS if the Cisco ASA cannot determine the identity of the user.

If you use AAA rules (cut-thru proxy) or Cisco ASA Identity Firewall on Cisco ASA, then you can also configure a whitelist. A subset of web traffic that matches the service policy rule then goes directly to the originally requested web server and is not scanned by CWS. Although you can achieve the same results (exempting traffic according to usernames or user groups) when you configure the class of traffic by using ACLs to send to CWS, you might find using a whitelist more straightforward. The whitelist feature is based only on usernames and user groups, not on IP addresses.

The **whitelist** command means that the traffic matching the traffic class does not need to be forwarded to the CWS proxy servers and can go through directly to the original destination web server.

The **class-map type inspect scansafe [match-all | match-any] <scansafe-type-classmap-name>** command is used to create a class map to match traffic, based on user names and group names. This command is used to match traffic to be whitelisted. You can specify user, group, or both under the **match** command. If you specify both user and group in the **match** command, then the AND logic will be applied on (user AND group).

The user name to be matched is in the **domain_nickname\user_name** format.

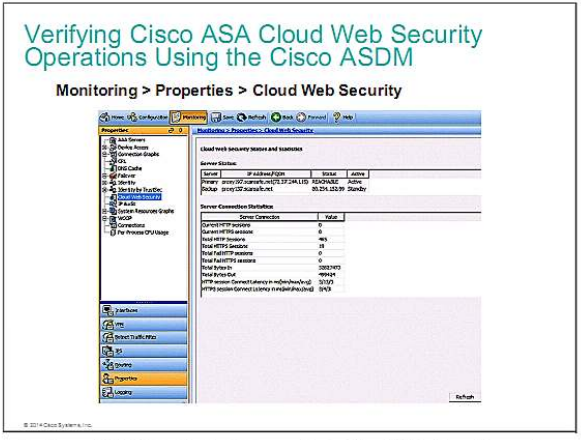
The group name to be matched is in the **domain_nickname\\group_name** format.

As shown in the figure, to whitelist the group "hr" in the Cisco domain but to scan traffic from a specific "hr" user named jdoe, specify the **match not** option for the Cisco\jdoe user.

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

Verifying Cisco ASA Cloud Web Security Operations Using the Cisco ASDM

This topic describes how to use Cisco Adaptive Security Device Manager to verify Cisco Cloud Web Security operations.



You can use the Cisco ASDM **Monitoring > Properties > Cloud Web Security** pane to monitor CWS operations.

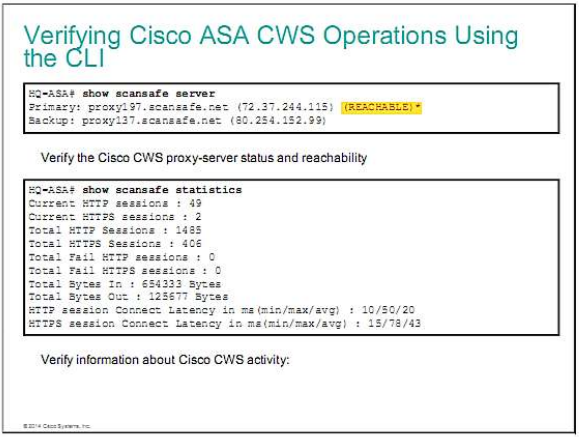
The upper part of the screen shows the Cisco CWS proxy-server status and reachability, while the lower part shows information about Cisco CWS activity: for example, the total number of HTTP or HTTPS sessions that are redirected to the proxy server, the number of current HTTP or HTTPS sessions that are redirected, and the latency.

This pane provides similar information as the **show scansafe server** and **show scansafe statistics** CLI commands.

https://t.me/learningnets

Verifying Cisco ASA Cloud Web Security Operations Using the CLI

This topic describes how to use the CLI to verify Cisco Cloud Web Security operations in Cisco Adaptive Security Appliance.



Use the **show scansafe server** command to verify the Cisco CWS proxy-server status and reachability.

Use the **show scansafe statistics** command to show information about Cisco CWS activity: for example, the total number of HTTP or HTTPS sessions that are redirected to the proxy server, the number of current HTTP or HTTPS sessions that are redirected, and the latency.

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

Verifying Cisco ASA Cloud Web Security Operations Using the CLI (Cont.)

```
HQ-ASA# show service-policy inspect scansafe
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
Interface inside:
  Service-policy: scansafe-pmap
    Class-map: scansafe-cmap
      Inspect: scansafe p-scansafe fail-open, packet 0, drop 0, reset-drop 0,
v6-fail-close 0
Number of whitelisted connections: 0
Number of connections allowed without scansafe inspection because of "fail-
open" config: 0
Number of connections dropped because of "fail-close" config: 0
Number of HTTP connections inspected: 0
Number of HTTPS connections inspected: 0
Number of HTTP connections dropped because of errors: 0
Number of HTTPS connections dropped because of errors: 0
```

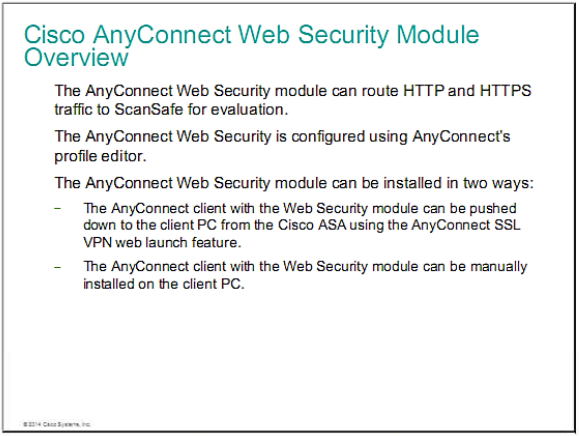
Verify the ScanSafe inspection policy

© 2014 Cisco Systems, Inc.

Use the **show service-policy inspect scansafe** command to verify the ScanSafe inspection policy. The information that is shown includes the number of HTTP or HTTPS sessions that are redirected or whitelisted by a particular policy.

Cisco AnyConnect Web Security Module Overview

This topic provides Cisco AnyConnect Web Security Module overview



The AnyConnect Web Security module is a component that can route HTTP and HTTPS traffic to a ScanSafe proxy server where ScanSafe Web Security scans and evaluates the traffic.

ScanSafe performs scanning by deconstructing elements of the web page into elements which are processed simultaneously. As we know, the web page may consist of HTTP, Flash and Java components. Once deconstructed, the web page elements are scanned by so called scanlets which perform the scanning in parallel. Based on scanning results, ScanSafe can block entire page or elements of the page which are determined to pose a threat.

AnyConnect Web Security features and functions are configured using the AnyConnect Web Security client profile which you edit by using the standalone or Cisco Adaptive Security Device Manager AnyConnect profile editor.

As mentioned before, the management portal for ScanSafe web scanning is the Cisco ScanCenter..

There are two options how to configure web security module: AnyConnect Web Security module can be configured for use through the Cisco Adaptive Security Appliance or as standalone module:

You can deploy the Web Security module as a standalone application to use with Cisco Cloud Web Security without enabling the AnyConnect VPN module and without an ASA.

There are two options how to configure web security module: AnyConnect Web Security module can be configured for use through the Cisco ASA or as standalone module:

The AnyConnect client with the Web Security module can be pushed down to the client PC from the ASA using the AnyConnect SSLVPN web launch feature.

You can deploy the Web Security module as a standalone application to use with Cisco CWS without enabling the AnyConnect VPN module and without an ASA.

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

Cisco AnyConnect Web Security Module for Standalone Use Overview

This topic describes the overview of installing the Cisco AnyConnect Web security Module procedure.



Cisco AnyConnect Web Security module can be deployed and use Cisco Cloud Web Security without having to install an Cisco Adaptive Security Appliance and without enabling the VPN capabilities of the AnyConnect Secure Mobility Client.

The slide shows the procedure of installing the Cisco AnyConnect Web Security module on Windows operating system for standalone use without VPN module being installed.



Run **Setup.exe** to install the AnyConnect Web Security Module:

1. Make sure only the **AnyConnect Web Security** check box is checked.
2. Make sure the **AnyConnect VPN** is not checked.
3. Click **Install Selected** and then **OK.**

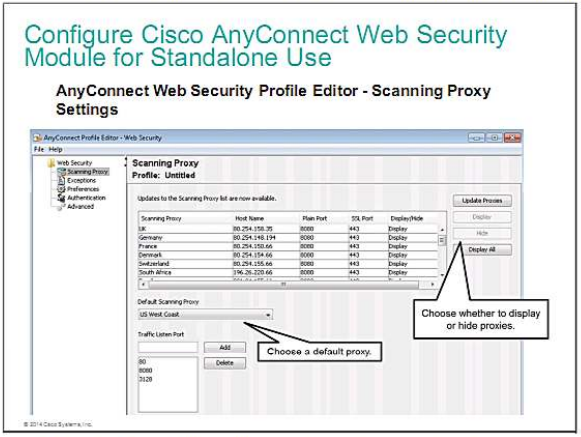
After the installation, if the AnyConnect client does not show the Web Security Module enabled, try to use the Windows Services manager to stop then restart the Cisco AnyConnect Secure Mobility Agent service to resolve the problem.

If everything is working, both the **Cisco AnyConnect Secure Mobility Agent** and the **Cisco AnyConnect Web Security Agent** Status should be Started.

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

Configure Cisco AnyConnect Web Security Module for Standalone Use

This topic describes how to configure Cisco AnyConnect Web Security Module for Standalone Use.



Configuration of the AnyConnect Web Security module, involves several steps. Cisco Cloud Web Security analyzes Web content; it allows benign content to be delivered to your browser and blocks malicious content based on a security policy. A scanning proxy is a Cisco CWS proxy server on which Cisco CWS analyzes the Web content.

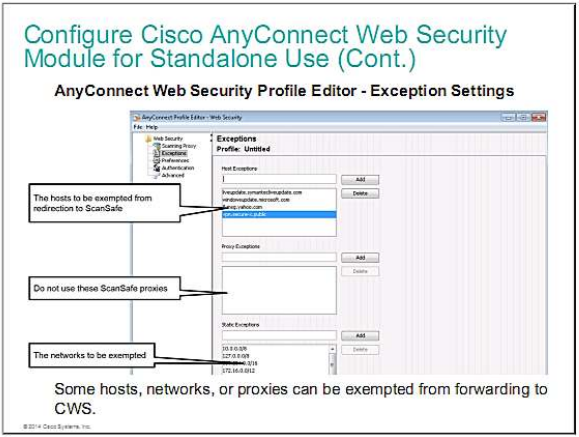
Open the **AnyConnect Web Security Profile Editor** you installed locally on your PC to create a profile. The **Scanning Proxy** panel in the **AnyConnect Web Security Profile Editor** defines to which Cisco CWS scanning proxies the AnyConnect Web Security module redirects Web traffic to.

By default, the profile you create has these Cisco CWSscanning proxy attributes:

- The scanning proxy list is populated with all the Cisco CWS scanning proxies
- A default Cisco CWS scanning proxy is pre-selected
- The list of ports on which the AnyConnect Web Security module listens for traffic is provisioned with several ports

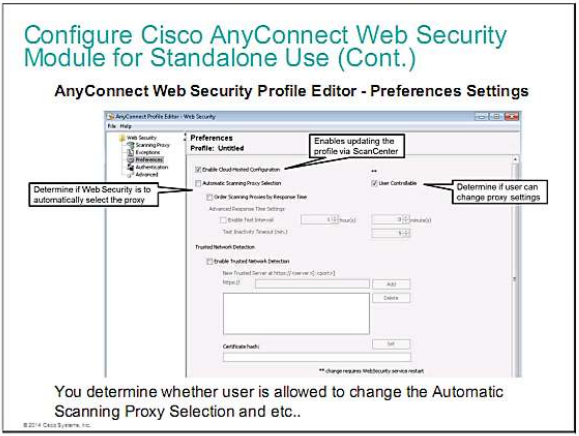
The Scanning Proxy list in the Web Security profile editor can't be edited. You can't add or remove Cisco CWS scanning proxies from the table in the **AnyConnect Web Security Profile Editor**. After you Start the **AnyConnect Web Security Profile Editor**, it updates the scanning proxy list automatically by contacting a Cisco Cloud Web Security website, which maintains the current list of scanning proxies.

https://t.me/learningnets



Specific traffic can be exempted from redirection to the CWS. As shown, you can select to exempt individual hosts or networks. These exclusions are configured in the **Exceptions** panel of the **AnyConnect Web Security Profile Editor**. You can also exempt one or more scanning proxies from redirection.

For example, when also implementing AnyConnect SSLVPN to the Adaptive Security Appliance, exempt the client traffic to the ASA for establishing the SSLVPN from being redirected to the scanning proxy.



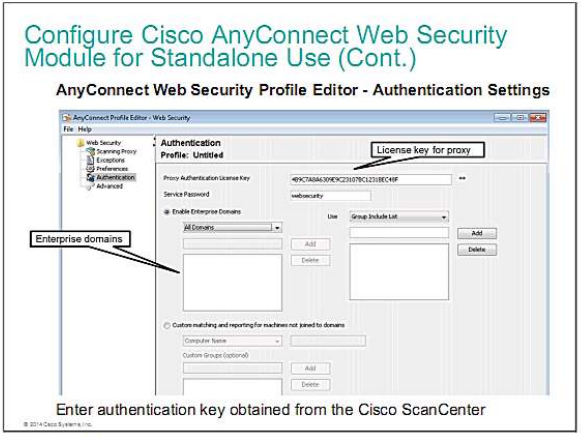
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

In the **Preferences** panel of the Web Security profile editor, select **Enable Cloud-Hosted Configuration** to enable updating the profile via Cisco ScanCenter. Select **User Controllable** (default setting) to determines if the User is allowed to change the **Automatic Scanning Proxy Selection** and **Order Scanning Proxies by Response Time** settings in the AnyConnect Web Security Client interface.

If you select **Automatic Scanning Proxy Selection**, Web Security determines which scanning proxy has the fastest response time and automatically connects the user to that scanning proxy.

If you do not select **Automatic Scanning Proxy Selection**, and you still have **Order Scanning Proxies by Response Time** selected, users will be presented with a list of scanning proxies, to which they can connect, ordered from fastest to slowest response time.

If you do not select **Automatic Scanning Proxy Selection**, the user is still free to enable this feature from the AnyConnect user interface



In **Authentication** panel, you must enter:

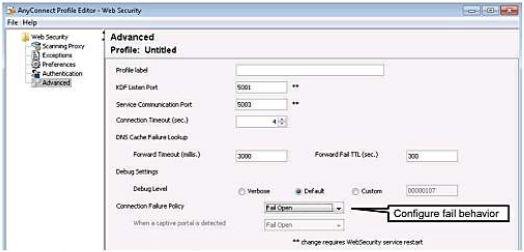
The proper authentication key obtained from the Cisco ScanCenter. If you are going to authenticate users based on their Enterprise domain, enter the company key you created. If you are going to authenticate users based on their Cisco ScanCenter or Active Directory group, enter the group key you created.

The service password. The default password is **websecurity**. This password is only required when using the `acwebsecagent -disablesvc` CLI command to disable the Web Security agent.

Optionally, you can send to the scanning proxy server the enterprise domain and active directory group information with every request. The scanning proxy will then apply the traffic filtering rules based on the enterprise domain and active directory group information.

Configure Cisco AnyConnect Web Security Module for Standalone Use (Cont.)

AnyConnect Web Security Profile Editor - Advanced Settings



Configure fail behavior if a connection to the Cisco CWS proxy server cannot be established

© 2014 Cisco Systems, Inc.

The **Advanced** panel in the **AnyConnect Web Security Profile Editor** gives you opportunity to configure fail policy. Select **Fail Close** to block traffic if a connection to the Cisco CWS proxy server cannot be established. Alternatively, select **Fail Open** to allow traffic.

If **Fail Close** is selected, in the **When a captive portal is detected** list, you can select **Fail Open** to allow traffic if the connection to the Cisco CWS proxy server cannot be established but a captive portal, such as a Wi-Fi hot spot, is detected. Alternatively, select **Fail Close** to block traffic.

Configure Cisco AnyConnect Web Security Module for Standalone Use (Cont.)

Save the XML profile using the WebSecurity_ServiceProfile filename to the Profiles\websecurity folder

- The **AnyConnect Web Security Profile Editor** will automatically create the file with the same filename with the **.wso** extension



© 2014 Cisco Systems, Inc.

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

When you finish with editing the profile settings, click **File > Save As....** in **AnyConnect Web Security Profile Editor,** and:

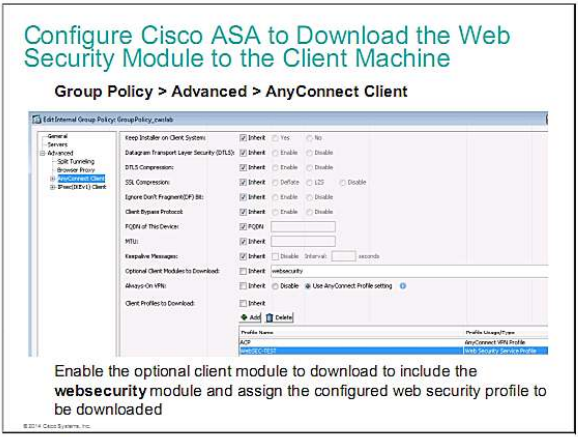
Save the profile as **WebSecurity_ServiceProfile.xml** to the Profiles\websecurity folder

The Web Security profile editor creates an additional obfuscated version of the profile called **WebSecurity_ServiceProfile.wso** and saves it to the same location as you saved the **WebSecurity_ServiceProfile.xml** file

https://t.me/learningnets

Configure Cisco ASA to Download the Web Security Module to the Client Machine

This topic describes how to configure Cisco Adaptive Security Appliance to download Cisco AnyConnect Web Security Module to the client machine.



The AnyConnect client with the Web Security module can be downloaded to the client machine from the Cisco ASA using the AnyConnect SSLVPN web launch feature. The web security profile is created in Cisco Adaptive Security Device Manager under **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Profile** the same way the web security profile can be created using the standalone web security profile editor.

The web security profile to be downloaded is tied to the group policy. This is done in Cisco Adaptive Security Device Manager under **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** screen. Edit the group policy and navigate to the **Advanced > AnyConnect Client** pane. In the **Client Profiles to Download** section, select the created web security profile and in **Optional Client Modules to Download**, select **websecurity** from the drop-down box.

Note	All the required AnyConnect SSLVPN configurations required to enable the Cisco ASA to push down the AnyConnect client with the Web Security module to the client machine is beyond the scope of this class. Refer to the SIMOS class for information on Cisco ASA SSL VPN configurations information.

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

Verifying Cisco AnyConnect Web Security Module Operations

This topic describes how to verify Cisco AnyConnect Web Security Module operations.



When users first connect to the network, they are routed to their default scanning proxy.

After that, depending on how their profile is configured, users may choose a scanning proxy or the AnyConnect Web Security module connects them to the scanning proxy with the fastest response time.

If their client profile allows user control, users will be able to select a scanning proxy from the Settings tab for the Cisco AnyConnect Secure Mobility Client Web Security tray.

If their client profile has the Automatic Scanning Proxy Selection preference enabled, AnyConnect Web Security orders the scanning proxies from fastest to slowest and connects users to the scanning proxy with the fastest response time.

If their client profile does not allow for user control but Automatic Scanning Proxy Selection is enabled, AnyConnect Web Security will switch users from their default scanning proxy to the scanning proxy with the fastest response time, provided that the response time is significantly faster than the default scanning proxy to which they originally connected.

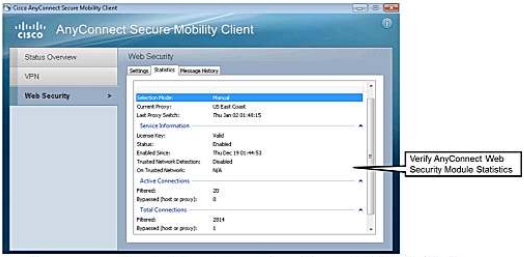
If users start to roam away from their current scanning proxy and Automatic Scanning Proxy Selection is configured in their client profile, AnyConnect Web Security could switch users to a new scanning proxy, provided that its response time is significantly faster than their current scanning proxy.

Users will know what scanning proxy they are connected to because AnyConnect Web Security displays the enabled scanning proxy name in the expanded AnyConnect tray icon on Windows, the Advanced Settings tab, and the Advanced Statistics tab of the AnyConnect GUI.

The figure shows AnyConnect opened in Windows system tray, when both VPN and Web Security modules are enabled.

Verifying Cisco AnyConnect Web Security Module Operations (Cont.)

Cisco AnyConnect Secure Mobility Client > Web Security > Statistics



Also access http://whoami.scansafe.net to verify if the traffic is redirected to the proxy

Verification of Web Security module could be performed in several ways:

From a web browser, access http://whoami.scansafe.net. Details such as the company name, the Cisco Cloud Web Security connector version, and so on are displayed if the traffic is being redirected to the Cisco CWS proxy server.

Open the AnyConnect from Windows system tray and click **Settings** button. Navigate to **Web Security > Statistics** where you can see information such as:

- Scanning proxy selection mode
- Current proxy
- License Key information
- Number of active filtered and bypassed connections
- Number of total filtered and bypassed connections

All Web Security messages are recorded in the **Windows Event Viewer** in the **Event Viewer (Local) \Cisco AnyConect Web Security Module** folder. The events Web Security records in the event viewer are intended to be analyzed by Cisco Technical Assistance Center engineers.

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

Cisco ISR G2 Cloud Web Security Overview

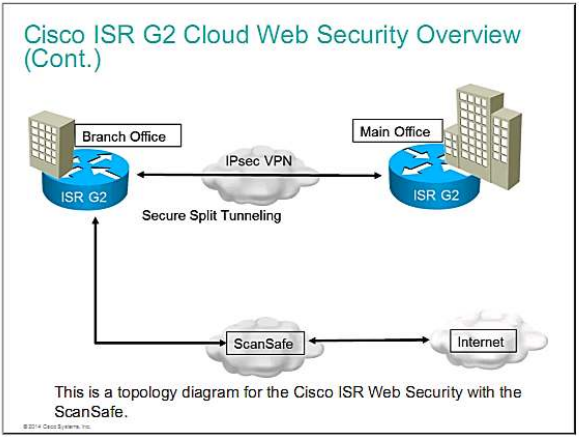
This topic provides overview of Cloud Web Security connector on Cisco Integrated Services Router G2 routers.



The Cisco ISR G2 family delivers numerous security services, including firewall, intrusion prevention, and VPN. These security capabilities have been extended with Cisco ISR Web Security with Cisco CWS for a web security and web filtering solution that requires no additional hardware or client software.

Cisco ISR G2 Web Security with Cisco ScanSafe enables branch offices to intelligently redirect web traffic to the cloud to enforce granular security and acceptable use policies over user web traffic. With this solution, you can deploy web security quickly and easily to protect branch office users from web-based threats, such as viruses, while saving bandwidth, money, and resources. Security and acceptable use policy can be configured in a granular fashion for branch offices through their ISR G2 routers without the need to backhaul the traffic to the main office.

Security features included in CWS are: URL filtering, Zero day malware protection, protection against phishing attacks, malware identification through heuristic analysis etc. Web requests are analyzed in all included elements, HTML, JavaScript, Flash etc.



Deploying security solutions in the branch offices may bring some challenges. Those challenges include connecting the branch offices to the main office without compromising the performance, the security and the availability, but also applying common policies to all users.

One of the challenges is how to consistently apply the same web usage policies to branch offices as policies defined for the main office.

The Cisco CWS Connector based on the ISR G2 Cisco routers incorporates Cisco CWS into the router. There is no need for any configuration on end user computers to provide threat protection from potentially malicious websites or sites that are not permitted by the company policy. The ISR G2 connector forwards the web traffic to the CWS where it can be filtered form threats or based on the company web usage policy.

The Cisco CWS solution on the ISR G2 can be integrated with other solutions such as Cisco Identity Services Engine to allow user Authentication and Authorization, for access control and differentiated access.

One added benefit from using Cisco ISR G2 routers in branch offices is that internet traffic originating from branch offices does not need to be sent back to the headquarters, saving the bandwidth for business and mission critical traffic.

This is provided by employing secure split tunneling. This networking concept allows a VPN user to access both internet and local LAN or WAN at the same time, by using the same network connection.

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

Cisco ISR G2 Cloud Web Security Configuration

This topic describes how to configure Cloud Web Security connector on Cisco Integrated Services Router G2 router using the CLI.



Before configuring the Cisco ISR G2 router as a connector, some preparation needs to be done on the Cisco ScanCenter administration web portal. The company must create a CWS (ScanSafe) account and will then be provided with credentials and addresses of proxies for access to the CWS proxy servers. Than a company key must be generated, which will be applied in all company routers that will access CWS proxy servers. Also, the company IT administrator has the option to create user groups, authentication key and group key.

Creating CWS policies from the Cisco ScanCenter includes creation of web filters to control the web traffic that can pass through the network. Based on filters, you can create rules and policies and apply these policies to groups of users.

Example of the email the CWS administrator will receive once the CWS account has been created:

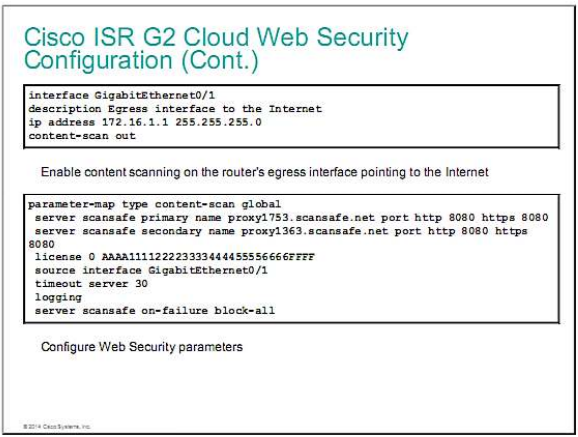
<output omitted>
Primary Web Services Proxy Name / IP Address: proxy1753.scansafe.net
Backup Web Services Proxy Name / IP Address: proxy1363.scansafe.net
Administrator Login User Name: jdoe@cisco.com
Administrator Password: z&H18%Cu
Administrator Portal ID: 1234598765
Administrator Portal Login: https://scancenter.scansafe.com/portal/admin/login.jsp
<output omitted>

These are steps for configuring a connector on Cisco IOS ISR G2 routers:

1. Requires the security k9 feature license on the ISR G2
2. **Enable Cloud Web Security:** it is necessary to choose the router's egress interface for the traffic which will be redirected to the cloud.

https://t.me/learningnets

3. **Configure the Web Security parameters on the router:** this step involves configuring several parameters for accessing the CWS such as proxy addresses, license key, and so on.
4. **Optional - Select exceptions:** it is possible to exempt certain traffic from being forwarded to the CWS proxy server using whitelist configurations.
5. **Optional - Configure authentication on the ISR G2:** to collect the user and the group identity to be passed to the CWS.
6. **Optional - Configure a default user group:** the users for which ISR G2 cannot the user's identity are assigned to this group.
7. **Optional - Configure prompting users to accept use policy agreement:** If configured, it will prompt users with a text which explains the web usage policy and forces the users to accept it if they want to continue with web access.



The content scanning process is an IOS feature that is used to redirect the user web traffic to Cisco CWS. Content scanning is enabled on an egress interface by using the **content-scan out** interface configuration command.

Next, you need to configure the Web Security parameters on the ISR G2 by using the **parameter-map type content-scan global** command. The command is followed by the parameters:

Primary and secondary servers: addresses and ports of primary and backup CWS proxy servers. These addresses are obtained from Cisco when the CWS company account is first established.

The license key: this is the company license key generated from the Cisco ScanCenter administration web portal. This key identifies the organization and should be used on all company´s routers that redirect traffic to the CWS proxy servers. When generating this key, the administrator should be careful to save the key information. When the key is generated, an email message will be sent to the administrator which contains the key information. Save this email so the key information can be retrieved later if needed. The full key can't be viewed from the Cisco ScanCenter Web Portal again, only the last four digits of the key is displayed.

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

Source interface: determines the source interface from which all traffic that is sent to the CWS proxy server originates. The interface configured here should match one that is associated with the egress interface on which **content-scan** is configured

Timeout: specifies the timeout interval of unreachability CWS proxy server after which the backup CWS proxy server is contacted.

server scansafe on-failure: specifies behavior of the traffic in case CWS proxy servers are not reachable. It can either allow or block all traffic.

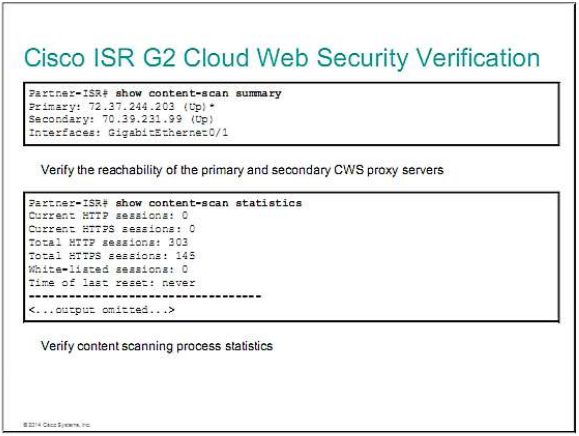
Commands	Description
content-scan out	Content scanning is enabled on an egress interface by using the **content-scan** out interface configuration command.
parameter-map type content-scan global	Enters the configuration mode for configuring parameters for the Web Security feature on the ISR G2.
server scansafe primary name proxy1753.scansafe.net port http 8080 https 8080	Configures the primary CWS proxy servers as well as ports to use for redirecting HTTP and HTTPS requests. By default, CWS uses port 8080 for both HTTP and HTTPS traffic, but you can choose to use different ports for each request type.
server scansafe secondary name proxy1363.scansafe.net port http 8080 https 8080	Configures the secondary CWS proxy servers as well as ports to use for redirecting HTTP and HTTPS requests. By default, CWS uses port 8080 for both HTTP and HTTPS traffic, but you can choose to use different ports for each request type.
license 0 AAAA1111222233334444555566666FFFF	Configures the license key that the ISR G2 sends to the CWS proxy servers to indicate from which organization the request comes. The license is a 16 byte hexadecimal key. The license key you specify here is generated from the Cisco ScanCenter. Value **0** used for prefix means indicates the license is unencrypted.
source interface GigabitEthernet0/1	Configures the interface the ISR G2 uses to originate all packets it sends to the CWS proxy servers. The interface configured here should match one that is associated with the egress interface on which **content-scan** is configured.
timeout server 30	Configures the amount of time (30 seconds in example) the ISR G2 waits before polling the CWS proxy server to check its availability. Default timeout is 300 seconds. The ISR G2 checks the primary server first and if it fails, it uses the secondary server as the active CWS proxy server. The ISR G2 automatically falls back to the primary server as long as it is successfully active for three consecutive timeout periods.
logging	Enables IOS syslogs for this feature.
server scansafe on-failure block-all |allow-all	Determines how to handle client traffic when the ISR G2 cannot reach either configured CWS proxy servers. You can block or allow all client web traffic. Default is block.

Note Some of the optional configurations such as whitelisting and authentication are not covered in this course. Please refer to the latest IOS configuration guides for more information.

https://t.me/learningnets

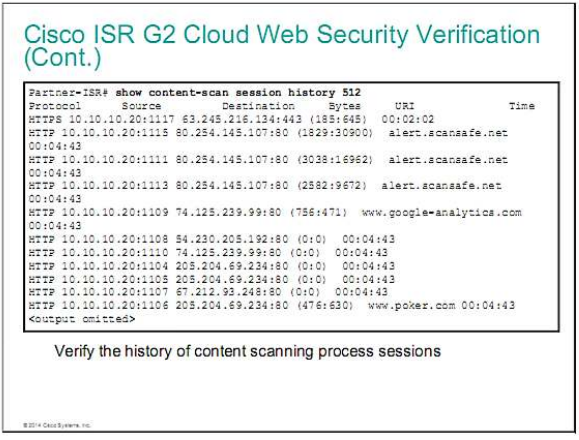
Cisco ISR G2 Cloud Web Security Verification

This topic describes how to verify Cloud Web Security connector operation on Cisco Integrated Services Router G2 router.



The **show content-scan summary** command displays generic ScanSafe related details, like active/standby ScanSafe information etc. The * signifies which is the chosen active server.

The **show content-scan statistics** displays content scanning process statistics. You can see the number of current HTTP and HTTPS sessions and number of total HTTP and HTTPS sessions.



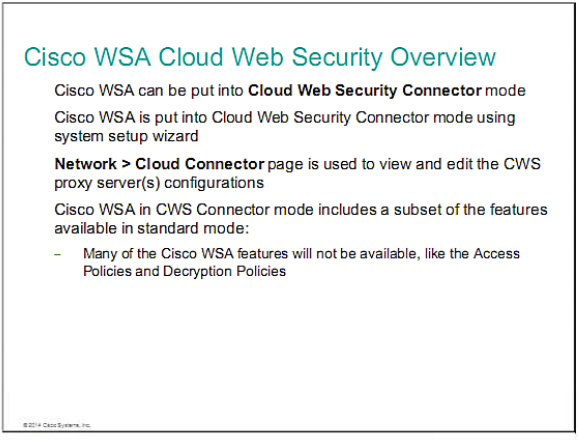
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

The **show show content-scan session history** command displays the history of content scanning process sessions, up to 512 terminated sessions.

https://t.me/learningnets

Cisco WSA Cloud Web Security Overview

This topic provides Cisco Web Security Appliance Cloud Web Security overview.



In CWS Connector mode, the Cisco WSA connects to and directs traffic to a Cisco CWS tower, where web security policies are enforced. The standard mode of the WSA includes on-site web proxy services and the Layer 4 Traffic Monitor; these services are not available in CWS Connector mode.

When setting up the Cisco WSA using the system setup wizard, select the appliance mode of operation to **Cloud Web Security Connector** then setup the Cisco WSA to communicate with the CWS proxy server(s). CWS Connector mode can be deployed in either explicit proxy mode or in transparent proxy mode.

Once the Cisco WSA has been setup in the **Cloud Web Security Connector** mode, the Cisco WSA GUI **Network > Cloud Connector** page is used to view and edit the CWS proxy server(s) configurations.

The Cisco WSA in CWS Connector mode includes a subset of the features available in standard mode. Use of the features included in the Cloud Connector subset is the same in both modes. When the Cisco WSA is in the **Cloud Web Security Connector** mode, many of the Cisco WSA features will not be available, like the Access Policies and Decryption Policies configuration will no longer be available in the Cisco WSA GUI.

Note The CWS connector is only available in the Cisco WSA 7.5.7 code. 7.5.7 is a special branch of the Cisco WSA code. The CWS connector will be available in the main streamed Cisco WSA 8.0 code. Refer to the Cisco WSA 7.5.7 User Guide for more information about the CWS Connector.

The Cloud Connector Logs provide useful information for troubleshooting problems with the Cloud Connector, for example, authenticated users and groups, the Cloud header, and the authorization key. Refer to the latest Cisco WSA User Guide for information on how to access the various logs from the Cisco WSA CLI using the `tail` command.

The Cisco WSA provides two different log types for recording Web Proxy transaction information, the access logs and the W3C access logs.

© 2014 Cisco Systems, Inc.
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 3

Describing the Web Filtering Policy in Cisco ScanCenter

The purpose of this lesson is to demonstrate through an example on how to configure Cisco Cloud Web Security policy from the Cisco ScanCenter administration web portal. We will create Web filtering policy, beginning with creation of a filter, a rule based on that filter and policy containing rules for web access. Finally, policy will be verified through reports generated by CWS.

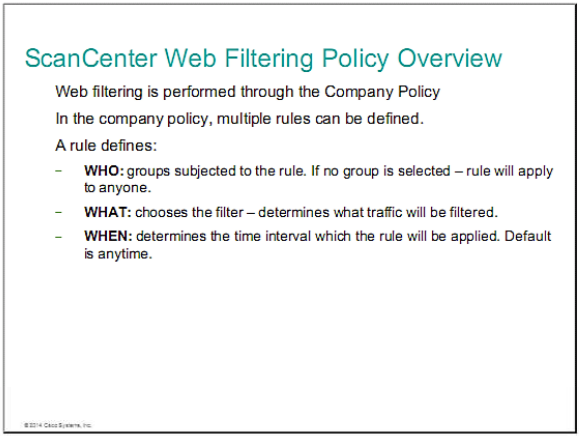
Upon completing this lesson, you will be able to meet the following objectives:

- Provide overview of the Cisco ScanCenter web filtering configuration
- Describe how to configure ScanCenter web filtering policy
- Describe how to enable HTTPS inspection in Scancenter
- Describe how to verify web filtering
- Describe how to create reports in Cisco ScanCenter

https://t.me/learningnets

ScanCenter Web Filtering Policy Overview

This topic provides overview of the Cisco ScanCenter web filtering configuration.



Web filtering is a term that means: checking web pages to determine whether their content – entirely or partially should be delivered to the user who requested it. The checking of the content is performed against a predefined set of rules. This set of rules is called the company policy.

Cisco Cloud Web Security enables companies to redirect their web traffic to Cisco CWS proxy servers where policies are enforced and traffic is scanned for unwanted and potentially harmful content.

IT administrators of enterprises define their policies through the Cisco ScanCenter adminstration Web portal.

Policy is defined by rules, and a policy can contain multiple rules. Order of rules within a policy is important.

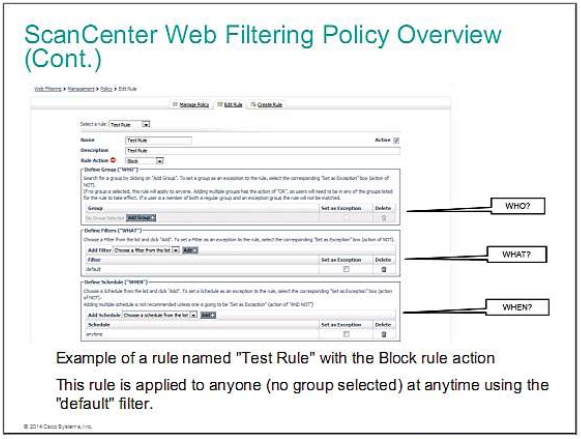
Groups, filters and schedule are applied to each rule to define:

- The groups subjected to the rule. If no group is selected – rule will apply to anyone.
- What traffic will be filtered.
- The time interval which the rule will be applied. Default is anytime.

You can create filters for the inbound or bi-directional traffic.

You can also create policies that treat separately HTTP and HTTPS traffic.

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



To access the Cisco ScanCenter administration web portal, browse to https://scancenter.scansafe.com and log in with your assigned credentials. The main page of the Cisco Scancenter administration web portal offers access to different aspects of Cisco CWS such as Web Virus, Spyware, Web Filtering, Reports, Dashboard and system administration.

Policy enables you to reference the rules for applying the filters. Each rule has one of the following actions associated with it:

Allow: Access is allowed, and data is stored for reporting purposes.

Anonymize: User, group, internal, and external IP details are replaced with "undisclosed" in reporting data.

Authenticate: The user must be authenticated. Authentication is the act of confirming the identity of a user.Cisco ScanCenter enables you to control access for each user or a group of users. Authentication enables you to enforce your organization's policies and comply with regulations. Cisco CWS can be optionally configured to authenticate the users before allowing them to connect to a destination server. This is achieved by creating an authenticate rule in Cisco ScanCenter for the user or group. Cisco ScanCenter can perform authentication using standard and secure LDAP authentication. Please refer to the latest Cisco ScanCenter Administration Guide for more information. When using the Cloud Web Security Connectors, different authentication keys for your organization, groups, and individual users can be generates to distinguish the different users or groups.

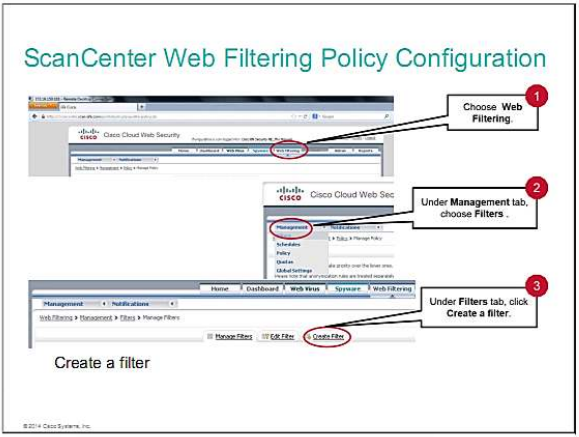
Block: Access is denied.

Warn: Access is allowed only if the user clicks through the warning page.

To create a new rule, navigate to **Web Filtering > Management > Policy > Create Rule**. The figure shows a rule named **Test Rule** which will block all types of traffic defined in the Filter named **default**. This rule is applied to anyone (no group selected) at anytime.

ScanCenter Web Filtering Policy Configuration

This topic describes how to configure ScanCenter web filtering policy.

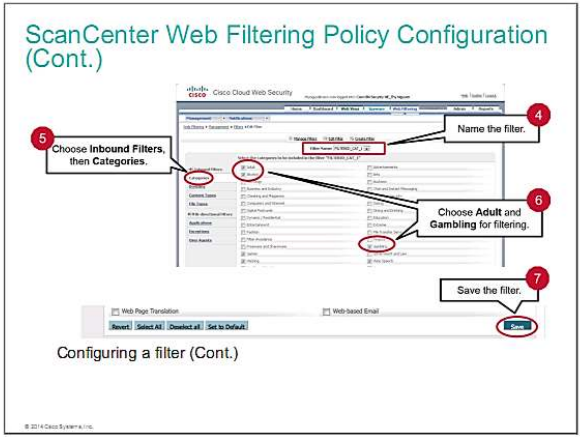


The first step in creating web filtering policy in Cisco Cloud Web Security is to create filters:

1. Select **Web Filtering** tab.
2. Select **Management** then from the drop down menu select **Filters**. A list of existing filters will be shown. From here you can create new filters or edit existing ones.
3. To create a new filter, select **Create Filter**, as shown.

   By default, there is a filter named "default" which can be edited but not deleted.

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



4. Now, enter a name for the filter, preferably a meaningful one (**FILTERED_CAT_1** is used in the example shown in the figure)
5. You can create filters for the inbound or bi-directional traffic. In this example, you will create a filter for the traffic in the inbound direction, so you will select Inbound Filters.
6. It is possible to filter traffic based on the web categories, domain-URL names or file types. In this example you will filter traffic based on the web categories. Select categories: Adult, Alcohol, Gambling, Games, Hacking, Hate Speech, etc. depending on your company security policy.
7. Once you are finished with category selection, press **Save** to save the changes.

Inbound filters are applied to incoming content only. These are possible inbound filters:

Categories: you can select the check boxes for the required web categories.

Domains: You can enter the domains or URLs to be included in the filter.

Content types: You can select the check boxes of the applications, audio, video, and image files that you want to block.

File Types: you can select the check boxes of the inbound file types to block.

Bi-directional filters are applied to incoming and outgoing content. These are possible bi-directional filters:

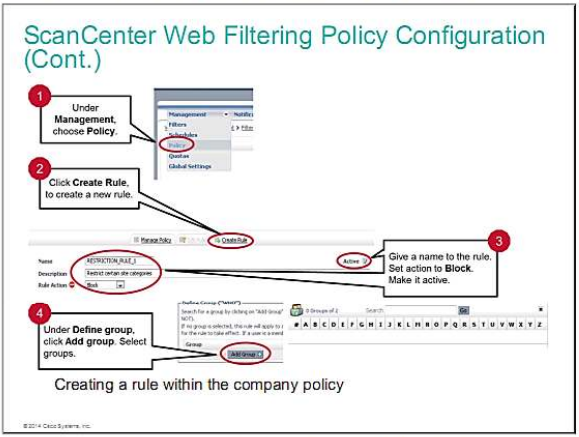
Applications: you can select the check boxes for the application types, applications, and activities to include in the filter

Exceptions: You can enter the domains or URLs to be excluded from the filter.

User Agents: You can select the required check boxes for the web browsers you want to include in the filter.

Note	Cisco CWS can also be configured to perform outbound filtering using file matching, keywords matching, regular expressions matching and pre-configured IDs that you want to prevent users from entering in web forms (such as Social Security Number). Outbound filtering is not enabled by default, most customers don't use this feature. To enable this feature, the customers can contact Cisco to have it enabled for no additional cost. Outbound filtering configurations is not covered in this course. Please refer to the latest Cisco ScanCenter Administration Guide for more information.

The next step will be to create a rule in the company policy referencing this filter.



1. To create a rule within the company policy, Select the **Web Filtering** tab then select **Management** and then select **Policy**.

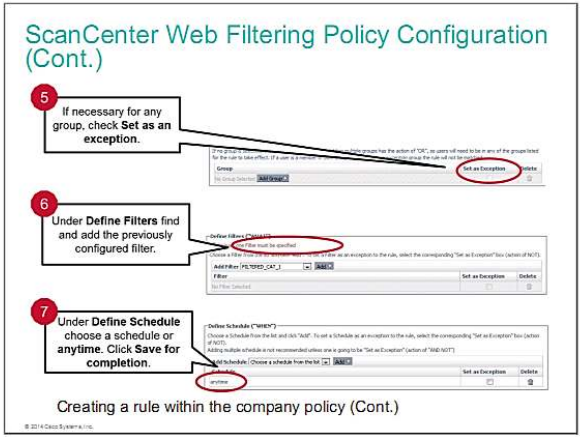
   The policy is based on rules, so you need to define rules within the policy. There is a maximum of 100 enabled rules allowed in the policy.

2. Click **Create Rule**, and the appropriate form for rule creation will be shown.

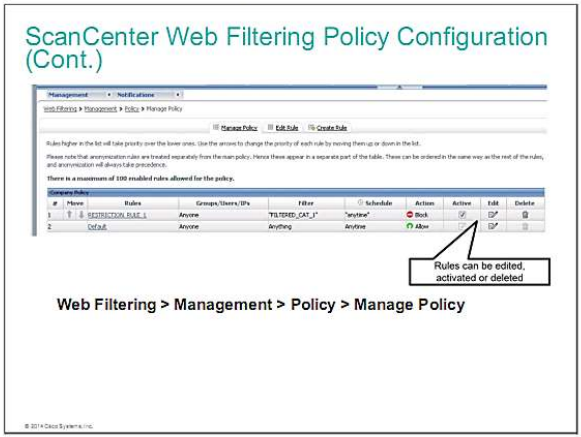
3. Give a name to the rule you are creating, preferably a meaningful one (**RESTRICTION_RULE_1** is used in the example shown in the figure), it will help you later in managing and eventual troubleshooting of the rule. It is also a good practice to give a description of the rule using the **Description** field. Choose the action to perform when rule is matched, in this case, the **Block** action is selected. Also, do not forget to make the rule active by placing the tick sign on **Active** field.

4. Next, you need to define groups which will be subjected to the rule. From the group list select groups you need to associate the policy with. If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "OR", so users will need to be in any of the groups listed for the rule to take effect.

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



5. If you need to exempt a group from the policy, you can use the **Set as Exception** field. If a user is a member of both a regular group and an exception group then the rule will not be matched.
6. Next step is to define filters which will be used by the rule. We need to select the filter which we have defined previously.
7. Part of the rule is also the scheduler – the time interval during which the rule will be applied. As said earlier, it is possible to define and apply different rules at different times. The default is **anytime**; otherwise you need to select time during which the rule will be in effect.



From the **Web Filtering > Management > Policy > Manage Policy** page, you can see the list of the rules defined within the policy. In this example, the **RESTRICTION_RULE_1** rule we created is applied before the **Default** rule which allows all traffic.

From this page, you can see the groups, filter and the schedule referenced by each rule. For the RESTRICTION_RULE_1 rule:

The rule is applied to **Anyone**.

The filter used by the rule is named **FILTERED_CAT_1**.

The rule is applied at **anytime**.

It is also possible to activate or deactivate the user defined rule, edit or delete it from this page. The **Default** rule can be edited but not deleted.

Rules higher in the list will take priority over the lower ones. Use the arrows to change the priority of each rule by moving them up or down in the list.

ScanCenter Web Filtering Policy Configuration (Cont.)

If you want to create separate rules for HTTP and HTTPS traffic:

Navigate to **Web Filtering > Management > Global Settings**.

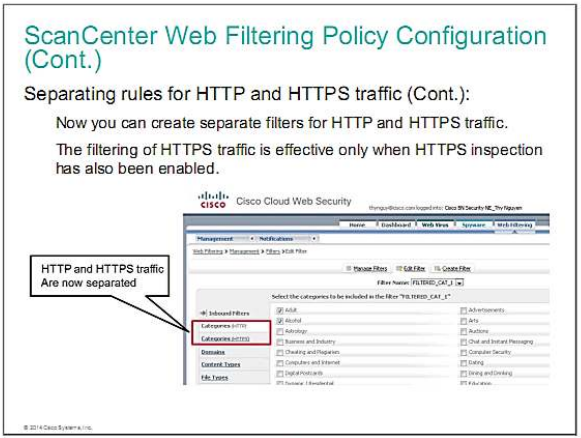
Click **Enable HTTP/HTTPS Split**.



By default, Cisco CWS gives the same treatment to HTTP and HTTPS traffic. If it is necessary, you can set different rules for HTTP and HTTPS traffic.

First, navigate to **Web filtering**, click **Management**, then choose **Global Settings** from the drop down menu. Find the item **Separate HTTPS Restrictions** and then click **Enable HTTP/HTTPS Split**. You have now enabled creating of separate filters and rules for HTTP and HTTPS traffic.

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

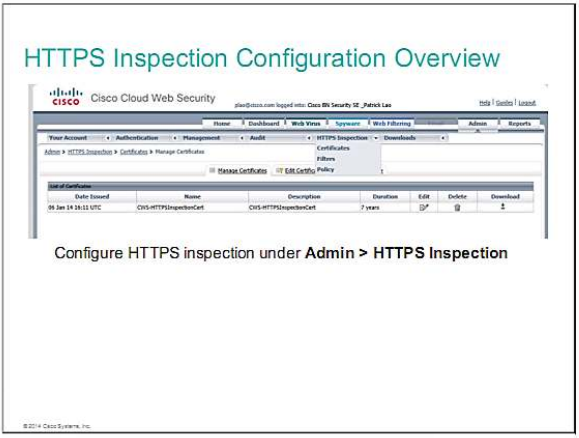


After HTTP/HTTPS Split has been enabled in Global Settings, navigate to **Web Filtering > Management > Filters**. Now you can see that separate categories for HTTP and HTTPS traffic.

The filtering of HTTPS traffic is effective only when HTTPS inspection has also been enabled.

HTTPS Inspection Configuration Overview

This topic describes how to enable HTTPS inspection in Scancenter.



When a user connects to a website via HTTPS, the session is encrypted. When HTTPS inspection is enabled, Cisco Cloud Web Security acts as the man in the middle and will block HTTPS connections to secure web servers with expired, invalid, or revoked certificates.

HTTPS inspection decrypts and scans the HTTPS traffic passing through Cisco CWS for threats and carries out actions based on your policy settings. If the traffic is deemed safe it is re-encrypted and passed back to your organization with a new certificate. All users should have the Cisco CWS certificate deployed to their browser. You can generate the CWS certificate in Cisco ScanCenter using a self signed certificate, or alternatively you can generate a CSR and use it with a tool such as Microsoft Certificate Services or OpenSSL to generate and upload your own certificate where your organization is the CA. The certificate is then associated with your HTTPS inspection policy.

To enable HTTPS inspection, navigate to the the **Admin > HTTPS Inspection > Certificates**, **Admin > HTTPS Inspection > Filters** and **Admin > HTTPS Inspection > Policy** tabs to manage the Cisco CWS certificates, the HTTPS inspection filters and the Company HTTPS policy.

The HTTPS inspection filters define what HTTPS traffic is to be decrypted for inspection and for malware scanning.

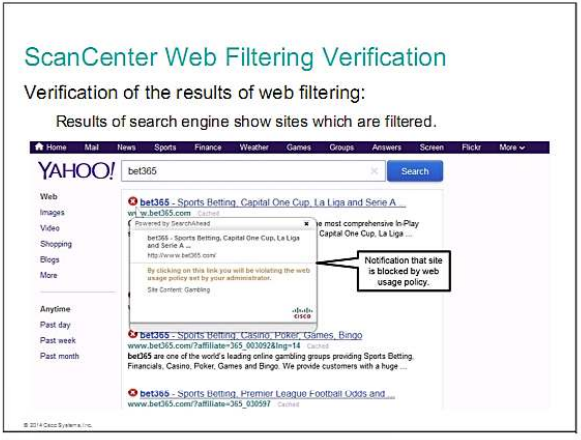
The figure shows the **Admin > HTTPS Inspection > Certificates** page where a self signed certificated named CWS-HTTPSInspectionCert is used for HTTPS inspection.

Note	Please refer to the latest Cisco ScanCenter Administration Guide for more information on enabling HTTPS inspection and other CWS features. The goal of this course is not to cover all the configuration options within the Cisco ScanCenter.

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

ScanCenter Web Filtering Verification

This topic describes how to verify web filtering.



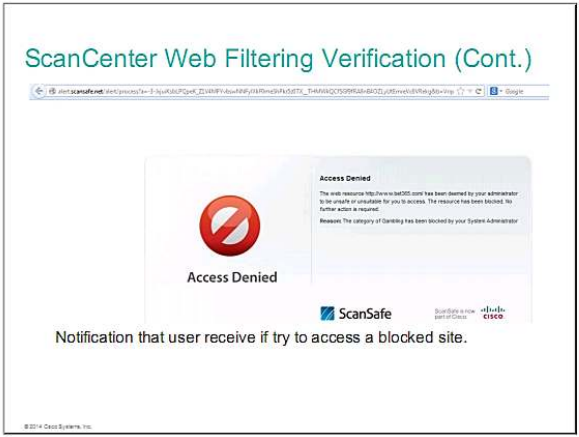
Properly configured Cisco Cloud Web Security connector redirects web traffic to one of Cisco CWS proxy server, where it is subjected to web filtering to comply with the web usage policy set up by the company.

You can see the web filtering results if you use a search engine such as Yahoo, searching for items that return results in pages that should be blocked by web usage policy will result in having a red **x** circle displayed to the left of the search result. Hover the mouse over the red x circle to see the notification message indicating that the site violates the web usage policy.

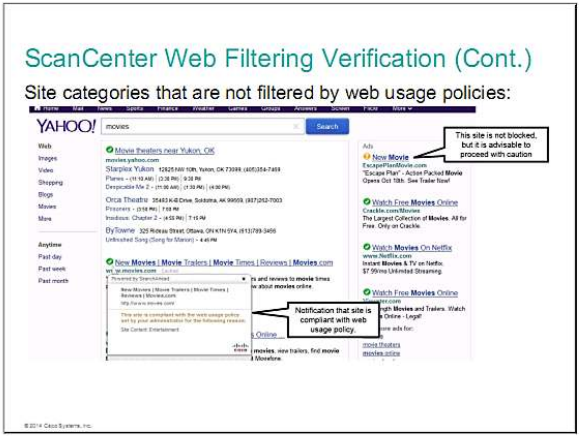
To enable this feature, Enable SearchAhead for All Users from the **Web Filtering > Management > Global Settings** page.

Note	Currently, Yahoo search uses HTTP but Google search uses HTTPS, therefore for SearchAhead to work with Google, HTTPS inspection for the Search Engines and Portals category must also be enabled using the HTTPS inspection filter.

https://t.me/learningnets

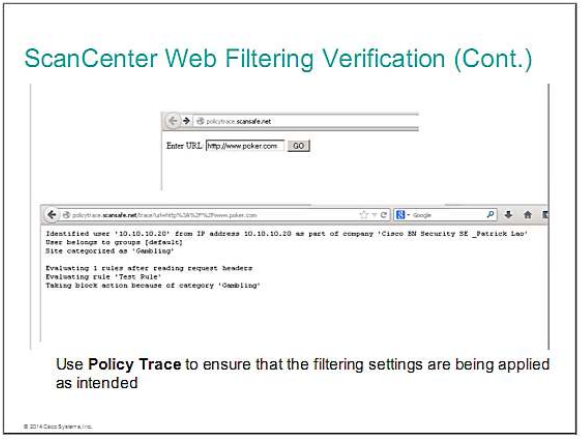


If user try to access a site that is blocked, Scansafe displays the Access Denied notification, which explains why the site cannot be accessed.



Web sites belonging to categories that are not filtered by web usage policies are displayed normally. Searching for items that return results in pages that is allowed by the web usage policy will result in having a green check mark circle displayed to the left of the search result. Hover the mouse over the green check mark circle to see the notification message indicating that the site is complaint with the web usage policy.

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



To ensure that your filtering settings are being applied as intended to users and groups, use a tool called Policy Trace.

On the end user machine which its HTTP/HTTPS traffic is being redirected to CWS, open a Web browser and enter the URL http://policytrace.scansafe.net, a page will be displayed prompting the user to enter an URL. In the Enter URL box, enter the URL for which to run a policy trace then click **Go**. The policy actions that are applied to that website are then displayed.

The figure shows the www.poker.com URL was entered in the policy trace and the result indicates "Taking block action because of category "Gambling" as matched by the "Test Rule".

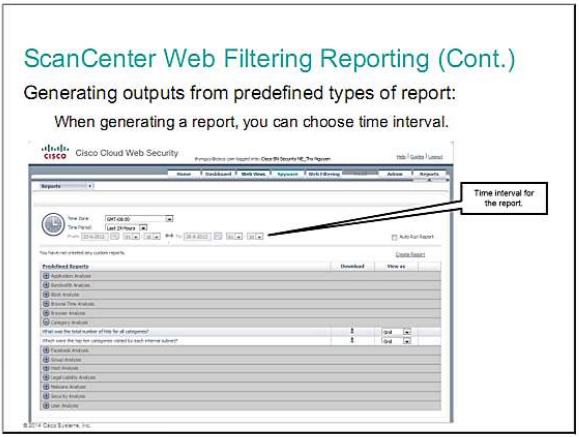
ScanCenter Web Filtering Reporting

This topic describes how to create reports in Cisco ScanCenter.



IT administrator can use Scancenter portal to generate reports on web usage and policy efficiency.

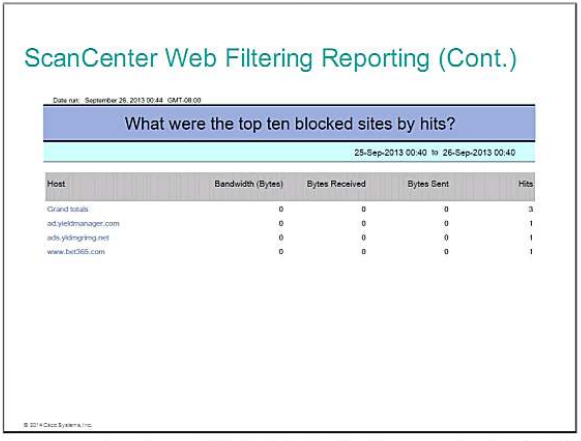
You can find the Reports menu by clicking on **Reports** from the main menu. You can choose between predefined and custom reports. There is a number of predefined reports, which Scancenter prepares automatically.



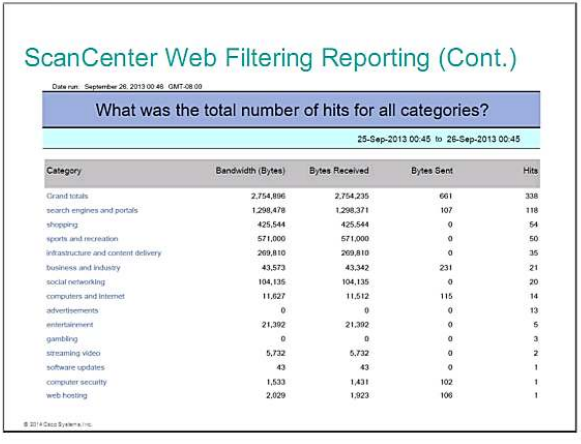
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Predefined reports include analysis of web usage by application, browser, and category as well as analysis from security perspective. It is also possible to generate report based on user behavior.

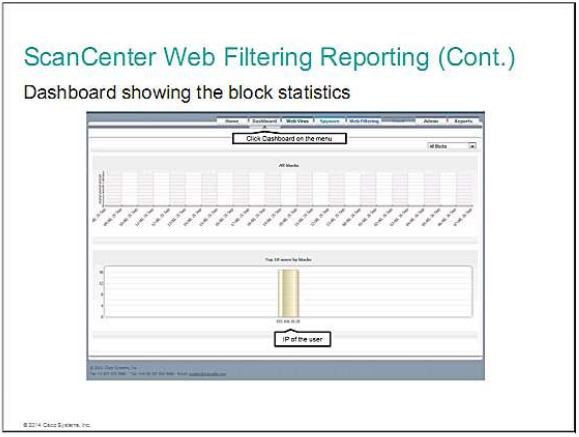
For all reports, you can set a time interval for reporting, to have a clear view on web usage and effectiveness of web usage policies.



This PDF report output shows the top 10 blocked sites by hits. You can see that there is a hit on a site that is included in a category which is blocked by the policy you have defined earlier (gambling).



This PDF report output shows the total number of hits for all categories. You can notice that the category you included in the web filtering policy, in this example, the gambling category which is being blocked had 3 hits and did not consume bandwidth at all.

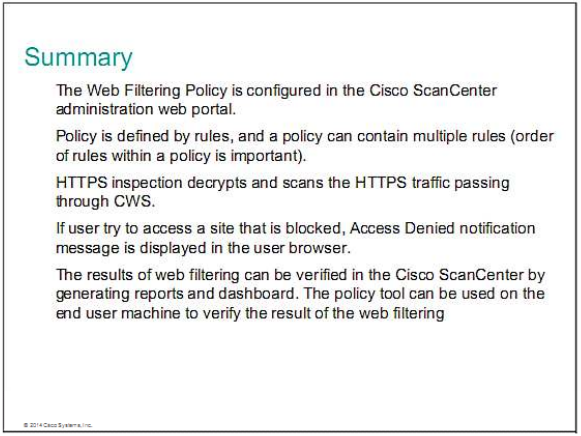


You can graphically display the block statistics by using the Dashboard tab. From the drop down box, you can select a particular type of block or select All Blocks as shown in the figure. The bottom part of the dashboard shows the top 10 users by blocks.

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

Summary

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



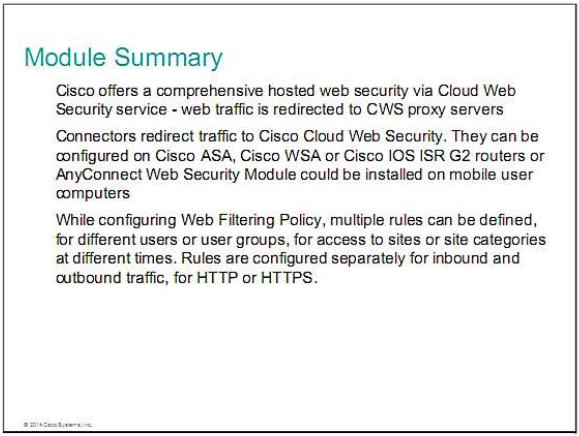
https://t.me/learningnets

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

Module Summary

Overview

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



References

For additional information refer to this resource:

- Latest Cisco ScanCenter Administrator Guide
- Latest Cisco ASA and IOS Configuration Guide

https://t.me/learningnets

© 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. Which list of common features are available in the Cisco NGFW (CX), WSA, and CWS? (Source: Cisco NGFW, WSA, CWS modules)

   A. NG-IPS, URL Filtering, Web Reputation, AVC, SSL Decryption
   B. DLP, AVC including non-Web applications, URL Filtering, Web Reputation, AVC, SSL Decryption
   C. Web Caching, DLP, AVC including non-Web applications, URL Filtering, Web Reputation, AVC, SSL Decryption
   D. URL Filtering, Web Reputation, SSL Decryption

2. Which three statements are correct about the Cisco NFGW (CX) or WSA or CWS? (Choose three) (Source: Cisco NGFW, WSA, CWS modules)

   A. The Cisco WSA is a standalone appliance
   B. The Cisco NGFW (CX version 9.2) is deployed as a hardware or software module on the ASA 5500-X or ASA 5585-X with NG-IPS capabilities
   C. Cisco CWS can be deployed as a cloud connector on the different Cisco devices such as the Cisco ASA and is managed using the Cisco ScanCenter which is the web based administration portal.
   D. The Cisco WSA and CWS uses subscription based licenses and also offer a hybrid (on-site + cloud) solution
   E. The Cisco NGFW (CX version 9.2), WSA and CWS all uses access policies, decryption policies and identity policies to implement the required company web security postures.
   F. The Cisco NGFW (CX version 9.2) is a one box web security solution which can be deployed using an implicit or explicit proxy approach.
   G. The Cisco NFGW (CX), WSA and CWS are all managed using the Cisco ScanCenter which is the web based administration portal.
   H. The Cisco NFGW (CX), WSA and CWS are all managed using the Cisco PRSM.

https://t.me/learningnets

3. What are four available CWS connectors? (Choose four.) (Source: Cisco Cloud Web Security Overview)

   A. ISR G1
   B. ISR G2
   C. AnyConnect
   D. ASA
   E. WSA
   F. IPS

4. The CWS company key is generated from where? (Choose four.) (Source: Cisco Cloud Web Security Authentication Key)

   A. ASDM
   B. CCP
   C. PRSM
   D. Cisco ScanCenter

5. When using the standalone web security profiler editor to create the Web Security XML profile, the XML profile filename (not case sensitive) must be named as what?

   A. WebSecurity_ServiceProfile
   B. WebSecurity_Profile
   C. CWS_Profile
   D. Web_Profile

6. What is the URL that can be used to verify if the user HTTP traffic is being redirected to the CWS proxy server?

   A. http://whoami.scansafe.net
   B. http://www.scansafe.net
   C. http://www.scansafe.com
   D. http://scancenter.scansafe.com

7. Which statement is correct regarding the configuration in the Cisco ScanCenter?

   A. The filter reference the filtering rule and the filter is applied to the group.
   B. The rule contains the filters and the rule is applied to the group.
   C. A time schedule can be applied within a filter.
   D. The company policy contains the rules and the rule reference the filter.
   E. Each policy can contain one rule only.

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

Answer Key

1. D
2. A, B, C
3. B, C, D, E
4. D
5. A
6. A
7. D

https://t.me/learningnets

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

Glossary

Term	Definition
AAA	authentication, authorization, and accounting. Pronounced "triple a."
AC	alternating current.
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).
AD	advertised distance.
ADI	Authentication Directory Interface.
AES	Advanced Encryption Standard.
API	application program interface. The means by which an application program talks to communications software. Standardized APIs allow application programs to be developed independently of the underlying method of communication. A set of standard software interrupts, calls, and data formats that computer application programs use to initiate contact with other devices (for example, network services, mainframe communications programs, or other program-to-program communications). Typically, APIs make it easier for software developers to create the links that an application needs to communicate with the operating system or with the network.
AVC	Application Visibility and Control.
AVC	Application Visibility and Control.
CA	certification authority. Entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.
CIDR	classless interdomain routing. Technique supported by BGP4 and based on route aggregation. CIDR allows routers to group routes together to reduce the quantity of routing information carried by the core routers. With CIDR, several IP networks appear to networks outside the group as a single, larger entity. With CIDR, IP addresses and their subnet masks are written as four octets, separated by periods, followed by a forward slash and a two-digit number that represents the subnet mask.
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.
CSC SSM	The Content Security and Control Security Services Module delivers threat protection and content control by providing comprehensive antivirus, antispyware, file blocking, antispam, antiphishing, URL blocking and filtering, and content filtering.
CSR	certificate signing request.

https://t.me/learningnets

Term	Definition
CX	context-aware. Context-aware devices such as ASA CX let you enforce security based on the complete context of a situation.
DDoS	distributed denial of service
DHCP	Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.
DLP	data loss prevention.
DLP	data loss prevention.
DN	distinguished name. Global, authoritative name of an entry in the OSI Directory (X.500).
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.
EULA	End-User License Agreement.
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.
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.
Gigabit Ethernet	Standard for a high-speed Ethernet, approved by the IEEE (Institute of Electrical and Electronics Engineers) 802.3z standards committee in 1996.
GPO	group policy object.
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.
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.

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

Term	Definition
HTTP	Hypertext Transfer Protocol. The protocol used by Web browsers and Web servers to transfer files, such as text and graphic files.
HTTPS	Hypertext Transfer Protocol Secure
ICAP	Internet Content Adaptation Protocol
ICAP	Internet Content Adaptation Protocol
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.
ICMPv6	Internet Control Message Protocol version 6 is the implementation of Internet Control Message Protocol (ICMP) for IPv6. ICMPv5 is defined in RFC 4443.
IM	instant messaging.
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).

https://t.me/learningnets

Term	Definition
ISR	integrated services router. An ISR specifies the elements to guarantee quality of service (QoS) on networks. For example, an ISR can be used to allow video and sound to reach the receiver without interruption. Every application that requires some kind of guarantee has to make an individual reservation.
Kerberos	Developing standard for authenticating network users. Kerberos offers two key benefits: it functions in a multivendor network, and it does not transmit passwords over the network.
L4TM	Layer 4 Traffic Monitor.
LAN	local-area network. High-speed, low-error data network covering a relatively small geographic area (up to a few thousand meters). LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. LAN standards specify cabling and signaling at the physical and data link layers of the OSI model. Ethernet, FDDI, and Token Ring are widely used LAN technologies.
LAPD	Link Access Procedure on the D channel. ISDN data link layer protocol for the D channel. LAPD was derived from the LAPB protocol and is designed primarily to satisfy the signaling requirements of ISDN basic access. Defined by ITU-T Recommendations Q.920 and Q.921.
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.
MAC address	Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6 bytes long and are controlled by the IEEE. Also known as a hardware address, MAC layer address, and physical address.
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.
MPEG	Motion Picture Experts Group. Standard for compressing video. MPEG1 is a bitstream standard for compressed video and audio optimized to fit into a bandwidth of 1.5 Mb/s. MPEG2 is intended for higher quality video-on-demand applications and runs at data rates between 4 and 9 Mb/s. MPEG4 is a low-bit-rate compression algorithm intended for 64-kb/s connections.
MPF	Modular Policy Framework.

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

Term	Definition
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.
NBAR	Network-Based Application Recognition. Cisco protocol discovery and classification mechanism that performs Layers 4 through 7 classification of IP packets.
NTLM	NT LAN Manager. Also known as Windows Challenge/Response, NT LAN Manager is the authentication protocol that is used on Windows systems and networks.
NTLMSSP	NTLM Security Support Provider
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.
OCSP	Online Certificate Status Protocol.
OOB	out-of-band.
OVA	Open Virtual Appliance.
PAC	Proxy Auto-Config
PBR	policy-based routing.
PEM	privacy-enhanced mail.
POST	power-on self test. Set of hardware diagnostics that runs on a hardware device when this device is powered on.
PRSM	Cisco Prime Security Manager.
RADIUS	Remote Authentication Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.
RAID	Redundant Array of Independent Disks.
RSA	Acronym stands for Rivest, Shamir, and Adleman, the inventors of the technique. Public-key cryptographic system that can be used for encryption and authentication.
SaaS	software as a service.
SIEM	Security Information and Event Management.
SMTP	Simple Mail Transfer Protocol. Internet protocol providing email services.
SSD	solid state disk.
SSH	Secure Shell Protocol. Protocol that provides a secure remote connection to a router through a TCP application.

https://t.me/learningnets

Term	Definition
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.
SSO	single sign-on.
SSP	Security Services Processor.
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.
TLS	Transport Layer Security. A future IETF protocol to replace SSL.
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.
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]
VM	virtual machine.
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.
WAN	wide-area network. Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay, SMDS, and X.25 are examples of WANs.
WBRS	Web-Based Reputation Score.
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.
WINS	Windows Internet Name Service.
WMI	Windows Management Instrumentation.
WPAD	Web Proxy Auto-Discovery

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

Term	Definition
3DES	Triple Data Encryption Standard.

https://t.me/learningnets