SENSS

Implementing Cisco Edge Network Security Solutions

Volume 1 **Student Guide**
Version 1.0

Part Number: 97-3329-01

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, I

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**

Secure Design Principles *1-1*

Network Security Zoning **1-3**

Network Security Zones Implementation Model 1-4

Zoning 1-5

Zone Interface Points 1-6

Services 1-8

Placement of Services 1-10

Summary 1-13

Cisco Modular Network Architecture **1-15**

Cisco Modular Network Architecture 1-16

Cisco Modular Network Architecture Architecture Principles 1-17

Cisco Modular Network Architecture Designs 1-19

Cisco Modular Network Architecture Example Network 1-21

Summary 1-23

Cisco SecureX Architecture **1-25**

Cisco SecureX Architecture and Components 1-26

Cisco Security Intelligence Operations Overview 1-29

Summary 1-32

Cisco TrustSec Solution **1-33**

Cisco TrustSec Solution Overview 1-34

Cisco TrustSec Architecture 1-35

Cisco TrustSec Solution Components 1-38

Summary 1-40

Module Summary **1-41**

Module Self-Check **1-43**

Network Infrastructure Protection Deployment *2-1*

Introducing Cisco Network Infrastructure Protection **2-3**

Overview of Cisco Network Infrastructure Protection 2-4

Cisco Modular Network Architecture and Network Infrastructure Protection 2-6

Identify Network Device Planes 2-7

Control Plane Security Controls 2-8

Management Plane Security Controls 2-9

Network Telemetry 2-10

Layer 2 Data Plane Security Controls 2-11

https://t.me/learningnets

Layer 3 Data Plane Security Controls 2-13
Summary 2-14
Deploying Cisco IOS Control Plane Security Controls 2-15
Overview of Control Plane Security 2-16
Infrastructure ACLs 2-19
Control Plane Policing Overview 2-21
Control Plane Protection Overview 2-22
Configure Control Plane Protection 2-24
Verify Control Plane Protection 2-27
Overview of Routing Protocol Authentication 2-28
Overview of Routing Protocol Filtering 2-30
Summary 2-33
Deploying Cisco IOS Management Plane Security Controls 2-35
Overview of Cisco IOS Management Plane Security Controls 2-36
Overview of Cisco IOS Secure Management Access 2-38
Configure Cisco IOS Secure Management Access 2-41
Verify Cisco IOS Secure Management Access 2-47
SNMPv3 Overview 2-48
Configure Cisco IOS SNMPv3 2-51
Verify Cisco IOS SNMPv3 2-55
Overview of Management Access AAA 2-56
Configure Cisco IOS Management Access AAA 2-58
Summary 2-63
Deploying Cisco ASA Management Plane Security Controls 2-65
Overview of Cisco ASA Management Plane Security Controls 2-66
Overview of Cisco ASA Secure Management Access 2-67
Configure Cisco ASA Secure Management Access 2-70
Overview of Cisco ASA Management Access AAA 2-80
Configure Cisco ASA Management Access AAA 2-82
Verify Cisco ASA Management Access AAA 2-90
Summary 2-92
Deploying Cisco Traffic Telemetry Methods 2-93
Overview of Cisco Traffic Telemetry Methods 2-95
Overview of NTP 2-96
Configure NTP on Cisco IOS Software 2-98
Verify NTP on Cisco IOS Software 2-100
Configure NTP on Cisco ASA 2-102
Verify NTP on Cisco ASA 2-106
Overview of Device and Network Events Logging 2-107
Configure Logging on Cisco IOS Software 2-110
Verify Logging on Cisco IOS Software 2-112
Configure Logging on Cisco ASA 2-113
Verify Logging on Cisco ASA 2-119
Overview of Netflow 2-120
Configure NetFlow on Cisco IOS Software 2-126

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

Verify NetFlow on Cisco IOS Software 2-129
Configure NetFlow on Cisco ASA 2-131
Verify NetFlow on Cisco ASA 2-135
Summary 2-136
Deploying Cisco IOS Layer 2 Data Plane Security Controls 2-137
Overview of Cisco Layer 2 Data Plane Security Controls 2-139
PVLAN Overview 2-142
Configure PVLANs 2-146
Verify PVLANs 2-151
DHCP Control Overview 2-154
Configure DHCP Snooping 2-157
Verify DHCP Snooping 2-160
ARP Control Overview 2-163
Configure DAI 2-165
Verify DAI 2-168
Storm Control Overview 2-170
Configure Storm Control 2-171
Verify Storm Control 2-173
MACsec Encryption Overview 2-174
Configure MACsec Encryption 2-176
Verify MACsec Encryption 2-178
Summary 2-179
Deploying Cisco Layer 3 Data Plane Security Controls 2-181
Overview of Cisco Layer 3 Data Plane Security Controls 2-182
Infrastructure Antispoofing ACLs 2-183
uRPF Overview 2-185
Configure uRPF on Cisco IOS Software 2-187
Verify uRPF on Cisco IOS Software 2-190
Configure uRPF on Cisco ASA 2-191
Verify uRPF on Cisco ASA 2-193
IP Source Guard Overview 2-194
Configure IP Source Guard 2-196
Verify IP Source Guard 2-200
Summary 2-201
Module Summary 2-203
Module Self-Check 2-205
2-205
NAT Deployment on Cisco IOS Software and Cisco ASA 3-1
Introducing Network Address Translation 3-3
Overview of Network Address Translation 3-4
Cisco Modular Network Architecture and Network Address Translation 3-5
Inside and Outside NAT 3-6
Static and Dynamic NAT 3-9
NAT and NAT with PAT 3-10

https://t.me/learningnets

Policy-based NAT 3-11
NAT and Cisco Products and Features 3-12
Summary 3-14
Deploying Cisco ASA Network Address Translation 3-15
Overview of Cisco ASA NAT 3-16
Configure Network Object NAT 3-20
Configure Static NAT Using Network Object NAT 3-23
Configure Dynamic NAT with PAT Using Network Object NAT 3-28
Verify Network Object NAT 3-30
Configure Manual NAT 3-32
Configure Dynamic NAT Using Manual NAT 3-35
Configure Twice NAT Using Manual NAT 3-37
Verify Manual NAT 3-40
Troubleshoot NAT 3-41
Summary 3-43
Deploying Cisco IOS Software Network Address Translation 3-45
Configure Static NAT and PAT 3-46
Verify Static NAT and PAT 3-50
Configure Dynamic NAT and PAT 3-52
Configure Policy-Based Dynamic NAT with PAT 3-56
Verify Dynamic NAT and PAT 3-59
Troubleshoot NAT 3-61
Summary 3-63
Module Summary 3-65
Module Self-Check 3-67
Glossary G-1

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

Course Introduction

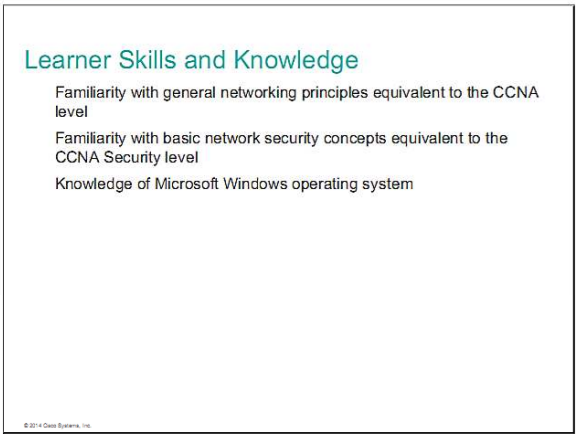
Overview

The Implementing Cisco Edge Network Security Solutions (SENSS) course is designed to prepare security engineers with the knowledge and hands-on experience to prepare them to configure Cisco perimeter edge security solutions. The student will gain hands-on experience with configuring various perimeter security solutions for mitigating inside and outside threats and securing network zones. At the end of the course, students will be able to reduce the risk to their IT infrastructures and applications using various features and provide detailed operations support for these features. The course starts with description of network security zones and Cisco modular architecture. Then the course describes how to implement network infrastructure protection using various features on Cisco IOS Software routers and switches. Then the course describes how to configure NAT on Cisco IOS Software Routers, and on Cisco ASA 5500-X Series Next-Generation Firewalls. The course ends with implementing basic and advanced threat controls on Cisco IOS Software Routers, and on Cisco ASA 5500-X Series Next-Generation Firewalls.

https://t.me/learningnets

Learner Skills and Knowledge

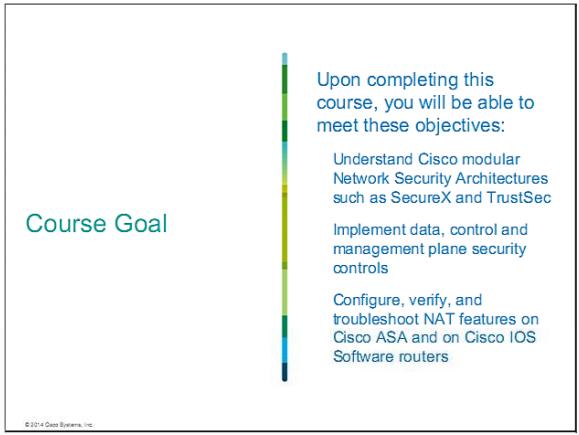
This subtopic lists the skills and knowledge that learners must possess to benefit fully from the course. The subtopic also includes recommended Cisco learning offerings that learners should first complete to benefit fully from this course.

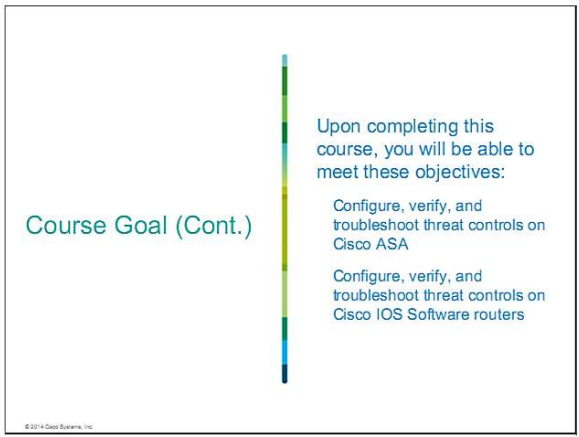


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Course Goal and Objectives

This topic describes the course goal and objectives.

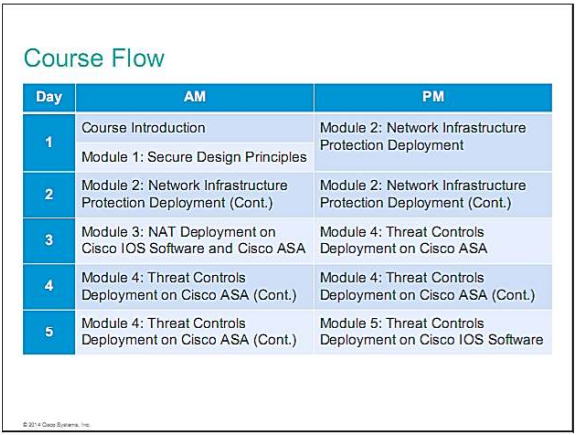




https://t.me/learningnets

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.

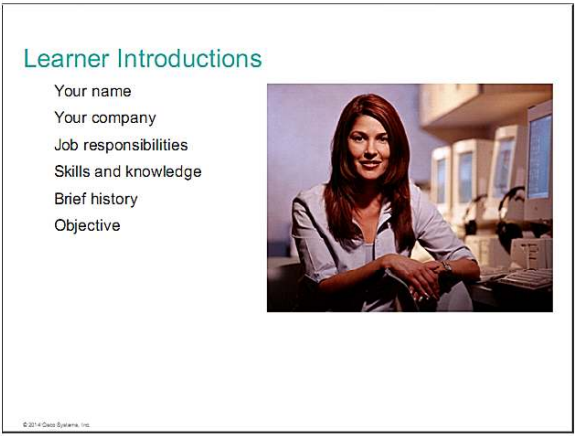
Training Curriculum

This subtopic presents the training curriculum for this course.

https://t.me/learningnets

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

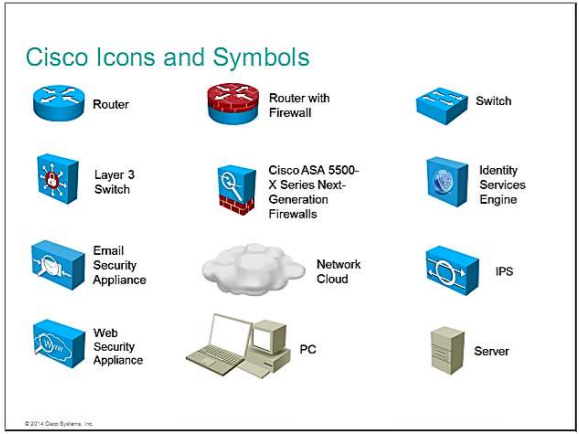
Note Cisco provides three levels of general certifications for IT professionals with several different tracks to meet individual needs. Cisco also provides focused certifications for designated areas such as cable communications and security. There are many paths to Cisco certification, but only one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



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).

https://t.me/learningnets

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

Module 1

Secure Design Principles

This module describes the basic principles of security engineering that system engineers should apply to security system design. These principles include making realistic assumptions when implementing security control and following the principles of network security zoning, defense in depth, and limiting damage. The module also describes the Cisco SecureX architecture and Cisco TrustSec, which are context-aware security solutions.

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

- Describe the concepts of Network Security Zones
- Provide an overview of the Cisco modular network architecture blueprint
- Describe the Cisco SecureX architecture as a context-aware security solution
- Describe the Cisco TrustSec solution as a part of the Cisco SecureX architecture

https://t.me/learningnets

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

Lesson 1

Network Security Zoning

This lesson is intended to assist network architects and security practitioners with the appropriate placement of services (for example, domain name service, email service, and web proxy service) into network security zones.

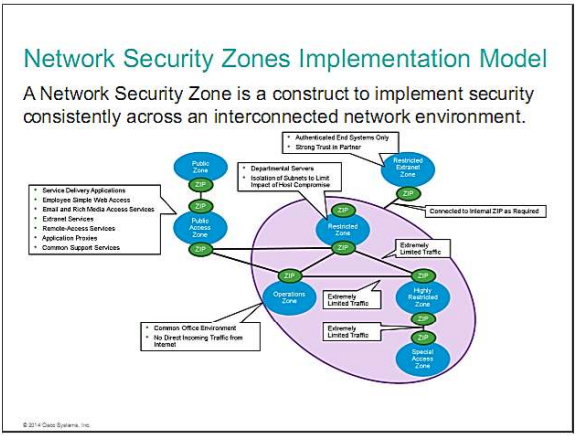
Upon completing this lesson, you will be able to meet these objectives:

- Describe the concepts of Network Security Zones
- Describe Zoning
- Describe Zone Interface Point
- Describe services in context to Network Security Zones
- Present the network zone architecture to illustrate the placement of services

https://t.me/learningnets

Network Security Zones Implementation Model

This topic describes the concepts of Network Security Zones.



A Network Security Zone is a construct to implement security consistently across an interconnected network environment. It demarcates a logical area within a networking environment with a defined level of network security. Zones define the network boundaries and their associated perimeter defence requirements. This is achieved by:

defining the entities which populate zones;

identifying discrete entry points;

monitoring and filtering network traffic at entry points;

monitoring the state of the network; and

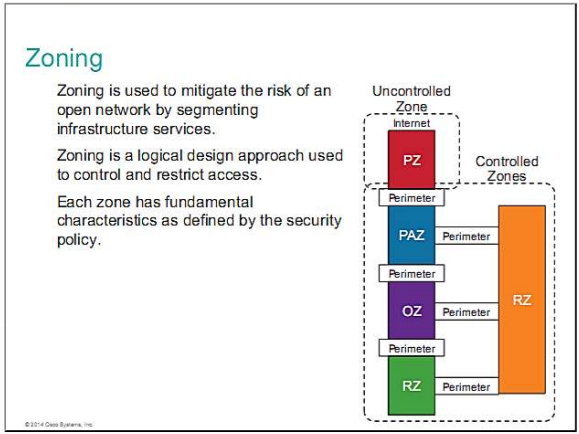
authenticating the identity of network entities.

Figure above illustrates the Network Security Zone implementation model. It shows how the seven Zones [Public Zone; PAZ; OZ; RZ; HRZ; REZ; and SAZ] relate to each other.

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

Zoning

This topic describes zoning.



Zoning is used to mitigate the risk of an open network by segmenting infrastructure services into logical groupings that have the same communication security policies and security requirements. The zones are separated by perimeters (Zone Interface Points) implemented through security and network devices.

Zoning is a logical design approach used to control and restrict access and data communication flows only to those components and users as per security policy. A new zone is defined by a logical grouping of services under the same policy constraints, driven by business requirements. When a new set of policy constraints are established, then a new zone is required.

Baseline Security Architecture Requirements for Network Security Zones identifies seven zones, however the four most common zones are shown in figure above: PZ; PAZ; OZ; and RZ

Each zone has the following fundamental characteristics:

- Every zone contains one or more separate, routable networks;
- Every separate, routable network is contained within a single zone;
- Every zone connects to another zone via a perimeter that contains zone interface points (ZIPs); and
- The only zone that may connect to the public zone is the PAZ.

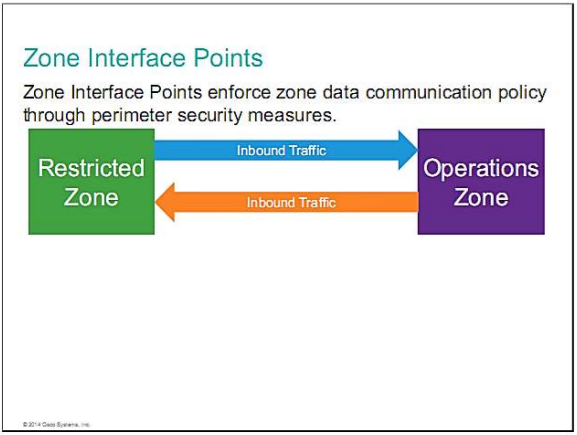
Zones where all components are entirely within or under the control of the enterprise are considered controlled zones. In the case where the enterprise does not control all zone components, the zone is considered uncontrolled.

Data communications entering and leaving a zone must conform to the data communication control requirements set by the policy for that zone.

https://t.me/learningnets

Zone Interface Points

This topic describes Zone Interface Points.



A Zone Interface Point provides a network interface between a zone and another zone. Zone Interface Points are the logical construct used to describe the controlled interfaces connecting the zones. Zone Interface Points enforce zone data communication policy through perimeter security measures.

Zone Interface Points have the following fundamental characteristics:

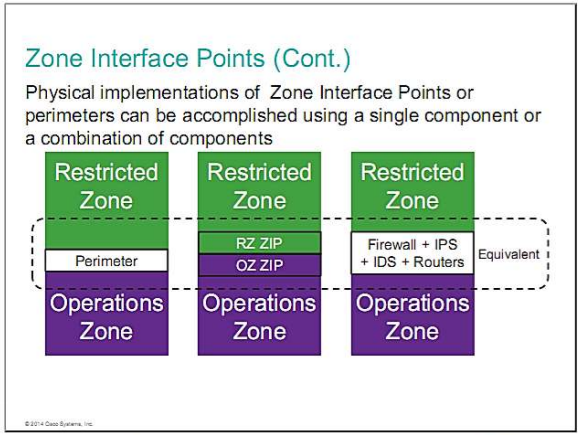
Every Zone Interface Point controls inbound data communication;

Zone Interface Points implement the security policy of their respective zones; and

All data communication must be through a Zone Interface Points.

Note	Data communication that passes through a zone without being terminated within the zone may need additional security controls

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



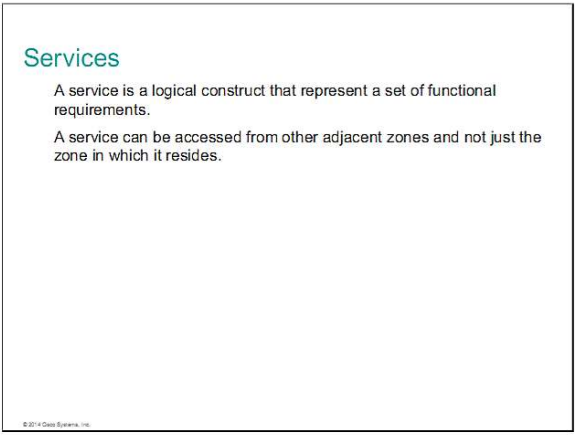
Physical implementations of Zone Interface Points or perimeters can be accomplished using a single component or a combination of components as shown in figure above. Figure also shows the perimeter is equivalent to the two Zone Interface Points [for example, RZ connecting to the OZ] and the sample physical implementation (for example, firewall, IPS, IDS, and Routers). For example, a router (a network device) may implement part of the perimeter, but it must be used in conjunction with an intrusion prevention system (a security device) and other security devices, which together provide appropriate security safeguards.

Note	Physical representations provided in figure are examples only and do not indicate a preference of design or approach.

https://t.me/learningnets

Services

The topic describes services in context to Network Security Zones.



A service is a logical construct that represent a set of functional requirements in an information technology architecture. These functional requirements can be simple such as providing resolution of domain names, or complex such as processing and transmitting email. Services can be physically implemented in many ways, for example, a single process on server, multiple processes on a virtual machine, or distributed processes among pool of servers.

A service can be accessed from other adjacent zones and not just the zone in which it resides.

The following list of services represents the most typical required for an IT infrastructure. The list is not exhaustive.

List of Services

Service Name	Description
Authentication Service	This service is the primary authentication service for all applications and end-users.
Data Service	Data service provides file storage, and database services for large repositories of non-sensitive information.
Email Service	The email service provides an internal email service and allows external email communication by communicating with the email proxy service.
Internal Domain Name Service	The internal DNS service provides domain names to the controlled zones (PAZ, OZ, and RZ). Internal DNS names are not published on the external DNS.
Remote Access Service	The remote access service provides an end-user with a secure connection to the network. Remote Access services require the use of the authentication service to authenticate the end-user.

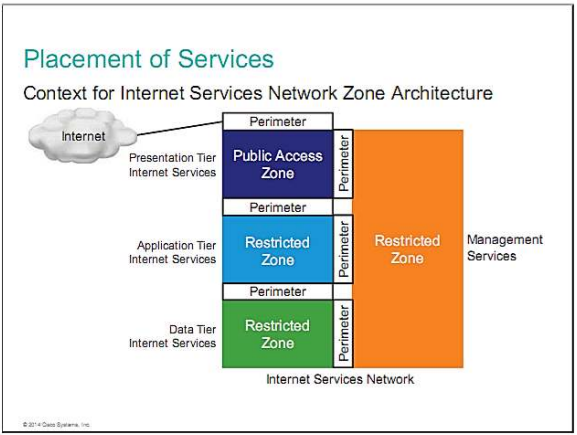
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Time Service	Time service provides accurate time and time synchronization to computer platforms within the IT infrastructure.
VoIP Service	VoIP-enabled devices are connected to an IP network for VoIP services such as telephony.

https://t.me/learningnets

Placement of Services

This topic presents some examples of the network zone architecture to illustrate the placement of services. The example architectures describe the purpose of the network, placement of services, context of the zones within the network zone architecture, and communication policies implemented in the perimeters.



The primary purpose of the internet services network is to provide business application delivery via the Internet to the public. The Internet services network, illustrated in figure below, is built with four controlled zones consisting of the following:

Data tier services RZ;

Application tier internet services RZ;

Management RZ; and

the PAZ that connects to the Public Zone (PZ; Internet).

In this architecture, business applications are hosted within enterprise departments and accessed by the public through the Internet.

For the Internet services network zone architecture, the following service are typically required:

External and Internal Domain Name Service

Email Proxy Service

Reverse Proxy Service

Authentication Service

Email Service

Application Tier Internet Service

Data Tier Internet Service

Security Administration Service

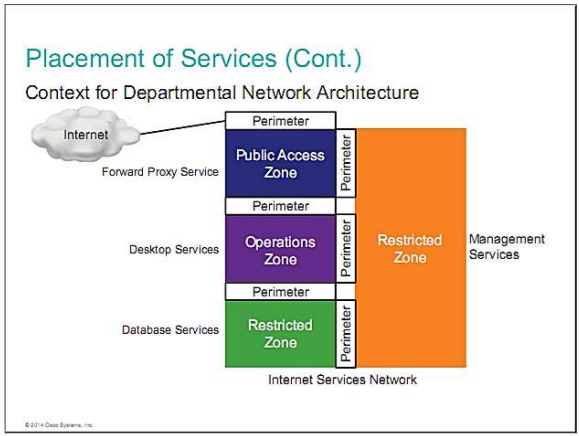
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Note	The list of services represents the most typical required for an IT infrastructure. The list is not exhaustive.

In the table below, the placements of services in the four zones of Internet services network are listed.

Services Locations in the Internet Services Network

Public Access Zone	Application Tier Internet Services Restricted Zone	Data Tier Restricted Zone	Management Restricted Zone
External Domain Name Service Email Proxy Service Reverse Proxy Service Presentation Tier Interet Service	Internal Domain Name Service Time Service Authentication Service Email Service Application Tier Intenet Service	Data Tier Internet Service	Auditing Service Backup Service IT Administration Service Security Administration Service



The enterprise network delivers business applications to employees. The enterprise network is built with the following zones:

- OZ
- RZ
- Management RZ
- The PAZ that connects to the public zone

The network zone architecture for the enterprise network is illustrated in figure above, where business applications are hosted within enterprise departmental networks and accessed by employees. The employees typically access their business applications from within their departmental network, or remote access over VPN.

https://t.me/learningnets

For the enterprise departmental network zone architecture, the following services are required:

- Application Authentication Service
- Auditing Service
- Backup Service
- Critical Data Service
- Data Service
- Desktop Service
- Email Proxy Service
- Email Service
- External Domain Name Service
- Extranet Service
- Forward (Web) Proxy Service
- Internal Intranet Service
- Reverse Proxy Service
- Security Administration Service
- Time Service
- Voice over IP Service

Note The list of services represents the most typical required for an IT infrastructure. The list is not exhaustive.

In the table below, the placements of services in the four zones of Internet services network are listed.

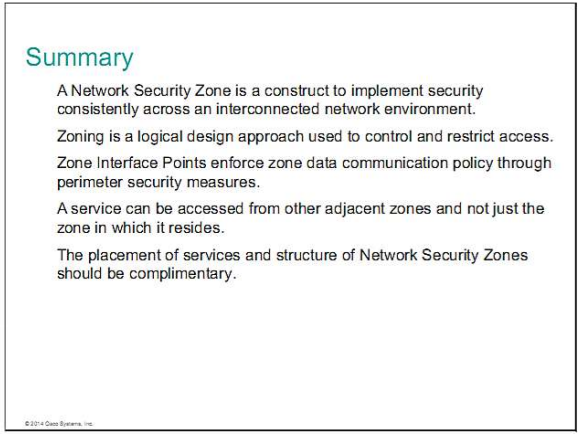
Services Locations in the Internet Services Network

Public Access Zone	Operations Zone	Restricted Zone	Management Restricted Zone
Email Proxy Service	Authentication Service	Critical Data Services	Auditing Service
External Domain Name Service	Data Services		Backup Service
Extranet Service	Desktop Service		IT Administration Service
Forward (Web) Proxy	Email Service		Security Administration Service
Presentation Tier Internet Service	Internal Domain Name Service		
Remote Access Service	Internal Intranet Service		
Reverse Proxy Service	Time Service		
	Voice Over IP Service		

© 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:

IT Security Guidance (ITSG)
http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/

https://t.me/learningnets

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

Lesson 2

Cisco Modular Network Architecture

This lesson introduces the Cisco modular network architecture best practices, designs and configurations, and provides network and security engineers with the necessary information to help them succeed in designing, implementing, and operating secure network infrastructures based on Cisco products and technologies.

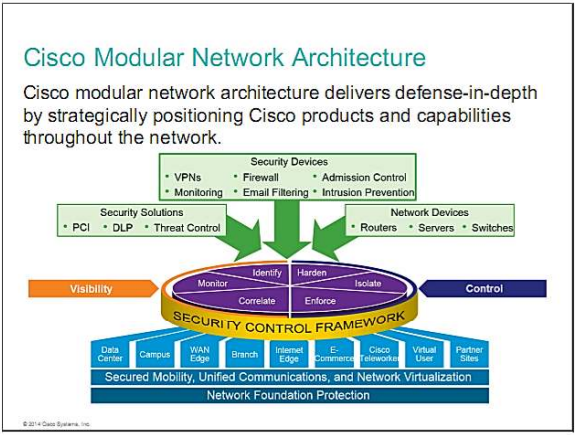
Upon completing this lesson, you will be able to:

- Describe Cisco modular network architecture
- Describe Cisco modular network architecture principles
- Provide an overview of the Cisco modular network architecture designs
- Provide an example of Cisco modular network architecture network design

https://t.me/learningnets

Cisco Modular Network Architecture

This topic describes Cisco modular network architecture solution.



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. The figure 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 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.

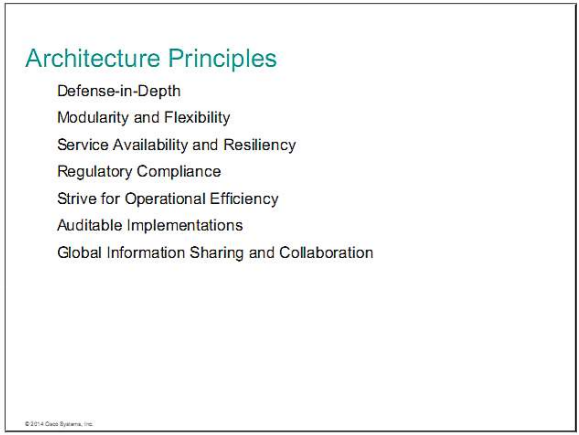
Security solutions—The Cisco SCF and the design blueprints provide the foundation for industry security solutions which address the requirements of specific industries such as retail, financial, healthcare, and manufacturing.

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

Cisco Modular Network Architecture Architecture Principles

This topic describes Cisco modular network architecture architecture principles.



The Cisco modular network architecture design blueprints follow the principles described below.

Defense-in-Depth—In the Cisco modular network architecture, security is embedded throughout the network by following a defense-in-depth approach, and to ensure the confidentiality, integrity, and availability of data, applications, endpoints, and the network itself. For enhanced visibility and control, a rich set of security technologies and capabilities are deployed in multiple layers, but under a common strategy. The selection of technologies and capabilities is driven by the application of the Cisco Security Control Framework.

Modularity and Flexibility—The Cisco modular network architecture design blueprints follow a modular design where all components are described by functional roles rather than point platforms. The overall network infrastructure is divided into functional modules, each one representing a distinctive PIN such as the campus and the data center. Functional modules are then subdivided into more manageable and granular functional layers and blocks (for example, access layer, edge distribution block), each serving a specific role in the network. The modular designs result in added flexibility when it comes to deployment, allowing a phased implementation of modules as it best fits the organization's business needs. The fact that components are described by functional roles rather than point platforms facilitate the selection of the best platforms for given roles and their eventual replacement as technology and business needs evolve. Finally, the modularity of the designs also accelerates the adoption of new services and roles, extending the useful life of existing equipment and protecting previous capital investment.

Service Availability and Resiliency—The Cisco modular network architecture design blueprints incorporate several layers of redundancy to eliminate single points of failure and to maximize the availability of the network infrastructure. This includes the use of redundant interfaces, backup modules, standby devices, and topologically redundant paths. In addition, the designs also use a wide set of features destined to make the network more resilient to attacks and network failures.

https://t.me/learningnets

Regulatory Compliance—The Cisco modular network architecture implements a security baseline built-in as intrinsic part of the network infrastructure. The security baseline incorporates a rich set of security practices and functions commonly required by regulations and standards, facilitating the achievement of regulatory compliance.

Strive for Operational Efficiency—The Cisco modular network architecture is designed to facilitate management and operations throughout the entire solution lifecycle. Products, capabilities, and topologies were carefully selected to maximize the visibility and control of the individual safeguards, while providing a unified view of the overall status of the network. Designs were conceived with simplicity to accelerate provisioning and to help troubleshoot and isolate problems quickly, effectively reducing the operative expenditures. Central points of control and management are provided with the tools and procedures necessary to verify the operation and effectiveness of the safeguards in place.

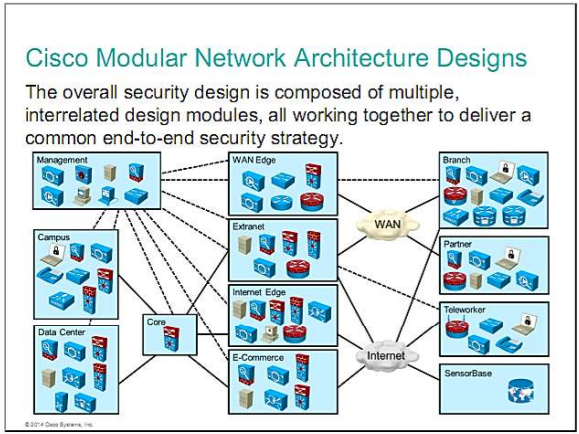
Auditable Implementations—The Cisco modular network architecture designs accommodate a set of tools to measure and verify the operation and the enforcement of safeguards across the network, providing a current view of the security posture of the network, and helping assess compliance to security policies, standards, and regulations.

Global Information Sharing and Collaboration—The Cisco modular network architecture uses the information sharing and collaborative capabilities available on Cisco's products and platforms. Logging and event information generated from the devices in the network is centrally collected, trended, and correlated for maximum visibility. Response and mitigation actions are centrally coordinated for enhanced control.

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

Cisco Modular Network Architecture Designs

This topic provides an overview of the Cisco modular network architecture designs.



The Cisco modular network architecture design blueprint follows a modular design where the overall network infrastructure is divided into functional modules, each one representing a distinctive PIN. Functional modules are then subdivided into more manageable and granular functional layers and blocks, each serving a specific role in the network.

Figure above illustrates the Cisco modular network architecture design blueprint.

Each module is carefully designed to provide service availability and resiliency, to facilitate regulatory compliance, to provide flexibility in accommodating new services and adapt with the time, and to facilitate administration.

The following is a brief description of the design modules.

Enterprise Core—The core is the piece of the infrastructure that glues all the other modules. The core is a high-speed infrastructure whose objective is to provide a reliable and scalable Layer-2/Layer-3 transport. The core is typically implemented with redundant switches that aggregate the connections to the campuses, data centers, WAN edge, and Internet edge.

Intranet Data Center—Cisco modular network architecture includes an Intranet data center design capable of hosting a large number of systems for serving applications and storing significant volumes of data. The data center design also hosts the network infrastructure that supports the applications, including routers, switches, load balancers, application acceleration devices to name some. The intranet data center is designed to serve internal users and applications, and that are not directly accessible from the Internet to the general public.

Enterprise Campus—The enterprise campus provides network access to end users and devices located at the same geographical location. It may span over several floors in a single building, or over multiple buildings covering a larger geographical area. The campus may also host local data, voice, and video services. Cisco modular network architecture includes a campus design that allows campus users to securely access any corporate or Internet resources from the campus infrastructure.

https://t.me/learningnets

Enterprise Internet Edge—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 services include public services DMZ, corporate Internet access and remote access VPN. The Cisco modular network architecture design blueprint incorporates an Internet edge design that allows users at the campuses to safely access E-mail, instant messaging, web-browsing, and other common services over the Internet. The Cisco modular network architecture Internet edge design also accommodates Internet access from the branches over a centralized Internet connection at the headquarters, in case the organization's policies mandates it.

Enterprise WAN Edge—The WAN edge is the portion of the network infrastructure that aggregates the WAN links that connect geographically distant branch offices to a central site or regional hub site. The WAN can be either owned by the same enterprise or provided by a service provider, the later being the most common option. The objective of the WAN is to provide users at the branches the same network services as campus users at the central site. The Cisco modular network architecture includes a WAN edge design that allows branches and remote offices to securely communicate over a private WAN. The design accommodates the implementation of multiple WAN clouds for redundancy or load balancing purposes. In addition, an Internet connection may also be used as a secondary backup option.

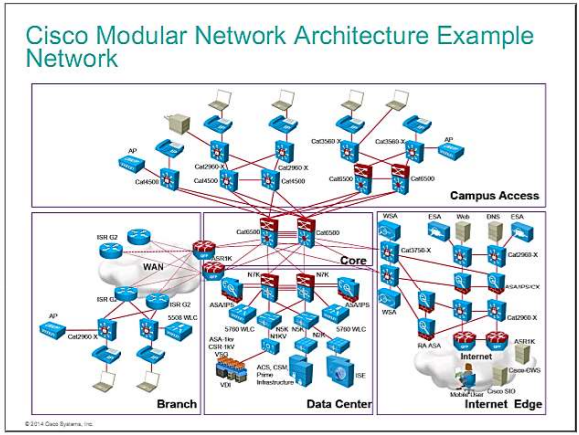
Enterprise Branch—Branches provide connectivity to users and devices at the remote location. They typically implement one or more LANs, and connect to the central sites via a private WAN or an Internet connection. Branches may also host local data, voice, and video services. The Cisco modular network architecture includes several branch designs that allow users and devices to securely access the branch resources. The Cisco modular network architecture branch designs accommodate one or two WAN clouds, as well as a backup Internet connection. Depending on the enterprise access policies, direct Internet access may be allowed while in other cases Internet access may be only permitted through a central Internet connection at the headquarters or regional office. In the later case, the Internet link at the branch would likely be used solely for WAN backup purposes.

Management—The architecture design includes a management network dedicated to carrying control and management plane traffic such as NTP, SSH, SNMP, syslog, etc. The management network combines OOB management and IB management, spanning all the building blocks. At the headquarters, an OOB management network may be implemented as a collection of dedicated switches or based on VLAN isolation.

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

Cisco Modular Network Architecture Example Network

This topic provides an example of Cisco modular network architecture network design.



The figure illustrates the range of security technologies and products in an example of a network, which is built based on the modular network architecture design principles. In the network, multiple layers of security controls are implemented throughout the network. All network devices and security controls are implemented in the high availability mode, providing confidentiality, integrity, and availability of data, applications, endpoints, and the network itself.

The security architecture shown in the figure is made up of the following security products and technologies:

Endpoint security: organizations today use a complex and diverse set of endpoints, both wired and wireless. These devices need to be secure from data loss, data theft, and privacy invasion, and must meet the local country and
state security requirements. Endpoint security within the example architecture includes the following products:

- Cisco SecureX Context-Aware Security
- Cisco Identity Services Engine
- Cisco Wireless LAN Controller
- Cisco AnyConnect Secure Mobility Client

Network security: One of the most fundamental elements of the Cisco security controls is network security, which is designed to protect the integrity of the network infrastructure itself, where entire network segments may be the target of attacks such as theft of service, service abuse, DoS, and data loss. Network security within the example architecture includes the following products:

- Cisco Adaptive Security Appliance 5500-X Series

https://t.me/learningnets

- Cisco Catalyst 6500 ASA Services Module
- Cisco ASA 1000V Cloud Firewall
- Cisco Virtual Security Gateway
- Cisco ISR G2 Integrated Security Firewall
- Cisco Cloud Services Router 1000V Series
- VPN
- Infrastructure protection on all devices

Content and application security: Organizations can be vulnerable to attacks on data and content. Spam, phishing through e-mail, and web content attacks have all been used to provide an attacker access to a target system. Content security within the example architecture includes the following products:

- Cisco Email Security Appliance
- Cisco Web Security Appliance
- Cisco Intrusion Prevention System
- Cisco ASA 5500-X Series NGFW

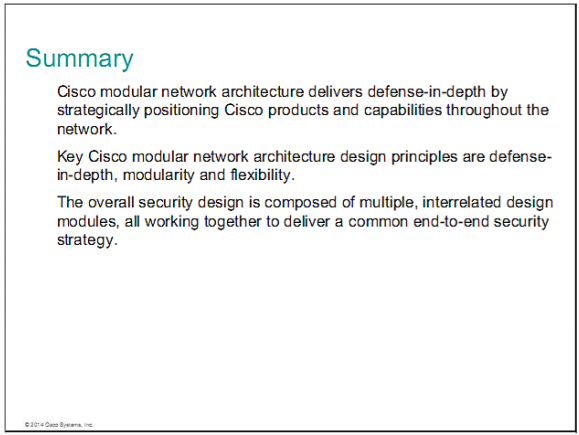
System network and event management: Network management tools help providers automate, simplify, and integrate their network to reduce operational costs. Network management within the example architecture includes the following products:

- Cisco Security Manager
- Cisco Prime Infrastructure
- Cisco Secure Access Control System

© 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 SAFE Reference Guide
http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.html

Design Zone for Security
http://www.cisco.com/en/US/partner/netsol/ns744/networking_solutions_program_home.html

https://t.me/learningnets

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

Lesson 3

Cisco SecureX Architecture

Today's organizations require security solutions that accurately detect threats, provide holistic protection, and continually adapt to a rapidly evolving, constantly changing threatscape. The Cisco SecureX Architecture, supported by Cisco Security Intelligence Operations, helps organizations achieve these goals.

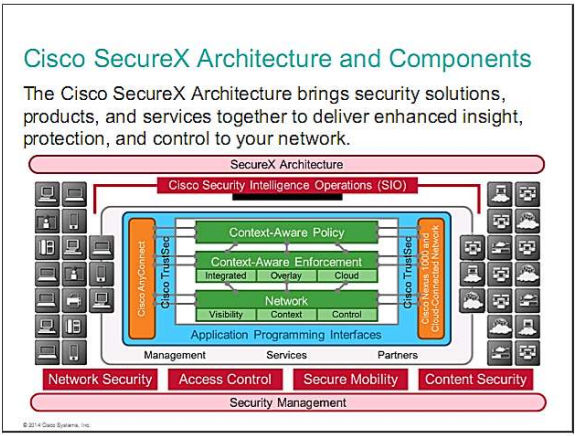
Upon completing this lesson, you will be able to:

- Describe Cisco SecureX architecture and components
- Provide an overview of Cisco Security Intelligence Operations (SIO)

https://t.me/learningnets

Cisco SecureX Architecture and Components

This topic describes Cisco SecureX architecture and components.



The Cisco SecureX architecture is a context-aware, network-centric, and integrated approach that enables consistent security enforcement throughout the organization and across security devices no matter when, where, or how the network is used.

The following security solutions are part of the Cisco SecureX architecture:

Network security—The Cisco network security infrastructure helps to prevent intruder access by detecting and blocking penetration, attacks, and exploits. With firewall and intrusion prevention in standalone and integrated deployment options, customers can prevent attacks and meet compliance requirements.

Access control—Cisco TrustSec provides secure access to your networks and network resources through policy-based access control, identity-aware networking, and data integrity and confidentiality services. Cisco TrustSec allows you to improve compliance, strengthen security, and increase operational efficiency. It is available as an appliance-based overlay solution or as an integrated IEEE 802.1X infrastructure-based service that extends access enforcement throughout the network.

Secure mobility—Cisco provides VPN, wireless security, and remote workforce security solutions that extend network access safely and easily to a wide range of users and devices. The Cisco Secure Mobility solution offers comprehensive and versatile connectivity options, endpoints, and platforms.

Content security—Cisco email and web security solutions reduce the costly downtime that is associated with email-based spam, viruses, and web threats. The solutions are available in various form factors, including on-premise appliances, cloud services, and hybrid security deployments with centralized management.

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

Security management—Cisco offers centralized operational tools to simplify and help you manage your network security deployment. These tools include Cisco Prime Security Manager, Cisco Security Manager, and Cisco Intrusion Prevention System Manager Express. In addition, Cisco has partnered with best-in-class technology vendors to deliver security information and event-management systems that have been pretested and validated with Cisco security products. This variety of management options gives you the flexibility to choose the network security management solutions that are best suited to your environment and business needs.

SecureX Architecture Components

Cisco SecureX starts with a solid foundation built on Cisco infrastructure. On top of this foundation we add context-aware security enforcement elements—like firewalls, web proxies, IPS sensors, and even the network infrastructure itself. These solutions provide critical intelligence, policy governance, and enforcement capabilities to significantly enhance the accuracy, effectiveness, and timeliness of any organization's security implementation, and can be deployed in a variety of ways–as standalone appliances, cloud services, or integrated modules into switching and routing infrastructure.

The Cisco SecureX Architecture is built upon three main components:

Context-aware policy—This policy uses a simplified descriptive business language that defines security policies that are based on five parameters: the identity of the person, the application in use, the type of device that is being used for access, the location, and the time of access. These security policies more closely align with business policies and are simpler to administer across an organization. They help businesses provide more effective security and meet compliance objectives with greater operational efficiency and control.

Context-aware security enforcement—Engineers use network and global intelligence to make enforcement decisions across the network and to deliver consistent and pervasive security anywhere in the organization. Flexible deployment options, such as integrated security services, standalone appliances, or cloud-based security services bring protection closer to the user, reducing network load and increasing protection.

Network and global intelligence—This ability provides deep insight into network activity and the global threat landscape for fast, accurate, and granular protection and policy enforcement:

- Local intelligence from the Cisco network infrastructure takes context such as identity, device, posture, location, and behavior to enforce access and data integrity policies.
- Global intelligence from Cisco Security Intelligence Operations provides full, up-to-date threat context and behavior to enable real-time, accurate protection.

https://t.me/learningnets

Examples of Components of the SecureX Architecture

The following are examples of Cisco infrastructure components of the SecureX architecture:

Cisco TrustSec and Identity Services Engine—Cisco TrustSec helps secure access to your networked resources through policy-based access control, identityaware networking, and data integrity and confidentiality services. Trustsec leverages the Cisco ISE to strengthen the deployment of policy. ISE is the industry's first policy-based service enablement platform uniquely combining identity and access control. It gathers real-time contextual information to make proactive access decisions.

Cisco AnyConnect Secure Mobility—The Cisco AnyConnect Secure Mobility Solution provides an innovative way to protect mobile employees on PC-based or smartphone platforms. This solution uses SSL or IPsec VPN to deliver a more seamless, always-on, and always-protected experience to end users, while enabling IT administrators to enforce policies and block malware with cloud-based or hybrid web security.

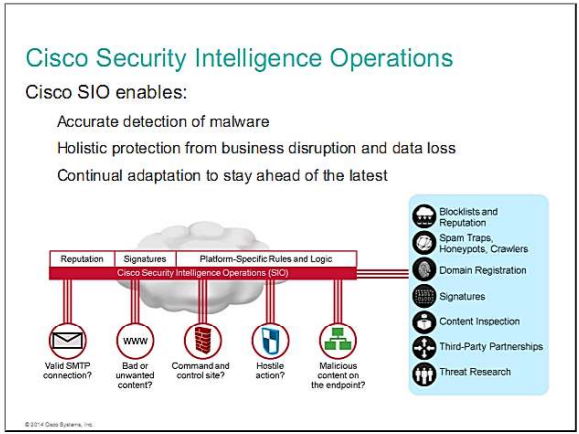
Cisco ASA 5500-X Series Adaptive Security Appliances—Cisco ASA 5500-X Series network security solutions are available in multiple form factors to provide flexible deployments: dedicated appliance or as a virtual instance or embedded module to your network infrastructure. , As a critical enforcement point, the ASA will deliver more components of multifaceted context. This will include components pertaining to users, applications, data, reputation, devices, posture, threats, destinations, sources, and locations.

Security Intelligence Organization—Core to SecureX is SIO, a cloud-based security service—a web-based global network of shared resources, software, and information provided to Cisco customers and devices on demand. SIO is used for real time-insight into the global threat environment.

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

Cisco Security Intelligence Operations Overview

This topic provides an overview of Cisco Security Intelligence Operations.



False positives and negatives are another challenge. Security should not prevent communication, which could happen should IPSs or firewalls generate a large number of false positives. In the past, whitelists were common workarounds, but this approach presents its own challenges. For example, what happens when a whitelisted domain is hit with a virus that spreads by email? Far better to have consistently accurate security, with low false negatives and low false positives.

Cisco SIO provides comprehensive threat intelligence that allows the organization's security team and network infrastructure to accurately detect malware and other threats. Analysis of content alone is no longer enough. With SIO, Cisco security products are able to make security policy enforcement decisions augmented by context, an enhancement enables more accurate and timely security protection.

Cisco SIO enables:

- Accurate detection of malware
- Holistic protection from business disruption and data loss
- Continual adaptation to stay ahead of the latest threats

https://t.me/learningnets

Three pillars of Cisco SIO:

The three pillars of Cisco SIO are:

Sensor Base—The main job of Sensor Base is to collect raw data from 700,000 sensors built into Cisco Network Security Devices deployed worldwide such as Intrusion Prevention System, firewalls and Web based security systems. Rather than collecting data from network security devices, Sensor Base also collect raw data from 600 third party news and data feeds, this collected information are like DNS registry information, global public blacklist/white list etc.

Threat Operation Center—In TOC, the collected raw data from sensor base is turned into meaningful information. There are automated algorithms which processes sensor base raw data into meaningful information and thus creating 95% of rules that Cisco's network security devices use. Rules are published to Cisco products in form of automated rules and signatures, also these rules are published to customers through alerts and bulletin. TOC is the heart of Cisco SIO with emphasis on threat research, design threat mitigation solutions and create update packages for security devices.

Dynamic Update—Cisco SIO delivers a constant stream of information and updates to Cisco customers and devices. Some security updates are available in real time, such as the reputation data used by Cisco security devices to block traffic from known malicious senders. Other systems, such as Cisco Intrusion Prevention System with Global Correlation, check for new rules roughly every three to five minutes.

Raw data is stored in Cisco SensorBase, where it is analyzed by both automated systems and human threat analysts. Reputation scores are adjusted based on observed behavior while threat technicians ensure hand-tuned filters and algorithms provide the best possible protection. Reputation updates are immediate, while filters and other updates are updated every few minutes. This interaction between devices and Cisco SIO enables advanced protection and enforcement, including protection against zero-day threats.

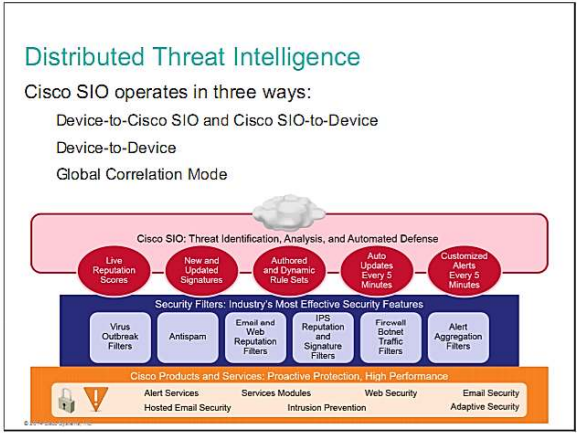
Threat mitigation data is provided through:

- Automatic rule and filter updates.
- IntelliShield vulnerability aggregation and alert services.
- Security best practice recommendations and community outreach services.

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

Distributed Threat Intelligence

Cisco SIO is the command and control center for Cisco security services and appliances around the world. However, the intelligence is distributed, with devices in the field playing an important role.



Cisco SIO operates in three ways:

Device-to-Cisco SIO and Cisco SIO-to-Device—First, Cisco devices, whether on-premise or cloud-based, act as the enforcement points in this ecosystem—they use the Cisco SIO filters and reputation data to block (or allow) traffic. They also contribute threat intelligence and data back into Cisco SIO. Just by making reputation queries, customers are contributing to the Cisco SensorBase data set.

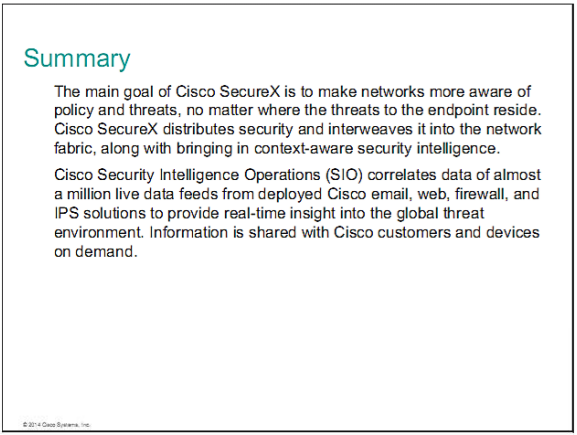
Device-to-Device—A second way that Cisco SIO works is within a corporate network. When one device in the network detects an event or a rule fires, that device informs other Cisco security deployments in that network. An IPS sending an ACL to a firewall is an example of this. Not all customers implement this level of Cisco SIO integration, but it does enable faster responses to new threats.

Global Correlation Mode—Cisco SIO works in a third, more global way. When new threats are detected, that data is shared with Cisco SIO and then with other Cisco customers around the globe.

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:

Design Zone for Security
http://www.cisco.com/en/US/partner/netsol/ns744/networking_solutions_program_home.html

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

Lesson 4

Cisco TrustSec Solution

The explosion in consumer IT devices, the need for global collaboration, and the move to cloud-based services and virtualization means that the traditional corporate network boundary is a thing of the past. Mobile workforce, collaboration, and productivity requirements have never been greater.

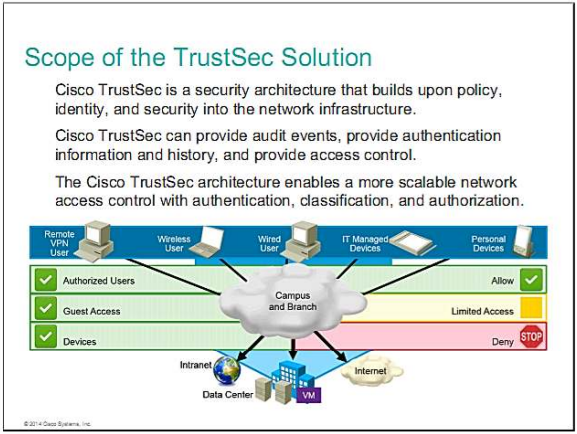
The Cisco TrustSec solution recognizes this fundamental change by telling you who and what is connecting to your wired or wireless network, and providing an innovative mechanism to control of what they can do and where they can go while they are there.

Upon completing this lesson, you will be able to:

- Provide overview of Cisco TrustSec solution
- Describe Cisco TrustSec architecture
- Describe Cisco TrustSec solution components

https://t.me/learningnets

Cisco TrustSec Solution Overview



Cisco TrustSec is a security architecture that builds upon policy, identity, and security into the network infrastructure. TrustSec security architecture creates secure networks by establishing a trusted set of network devices. Cisco TrustSec security architecture can control and identify the type of devices allowed, location, resources, and what resources are allowed access. This security architecture decouples the ACL management of defining IP addresses to ACLs on a distributed enterprise network while having employees, guests, and contractors on the network fabric.

Cisco TrustSec can provide audit events, provide authentication information and history, and provide access control to enable enterprises to adhere to regulatory and compliance guidelines. TrustSec includes dynamic VLANs, dACLs or named ACLs. The packet classification is maintained by tagging packets on ingress to the Cisco TrustSec network so that they can be properly identified for the purpose of applying security and other policy enforcement criteria along the data path. The tag, also called the SGT, enables the network to enforce the access control policy by enabling the egress device to act upon the SGT to filter traffic.

MACsec (IEEE 802.1AE) encryption provides secure data transmission combined with hop-by-hop encrypted data inspection. It builds upon existing identity-aware infrastructure while helping to ensure complete data confidentiality between network devices.

The Cisco TrustSec architecture enables a more scalable network access control with authentication, classification, and authorization. Authentication methods follows:

802.1X-based endpoint authentication

MAC Authentication Bypass

After authentication, TrustSec can classify and apply a specific policy for the authenticated endpoint. This enforcement method is Authorization. TrustSec supports the following Authorization methods:

Dynamic VLAN Assignment

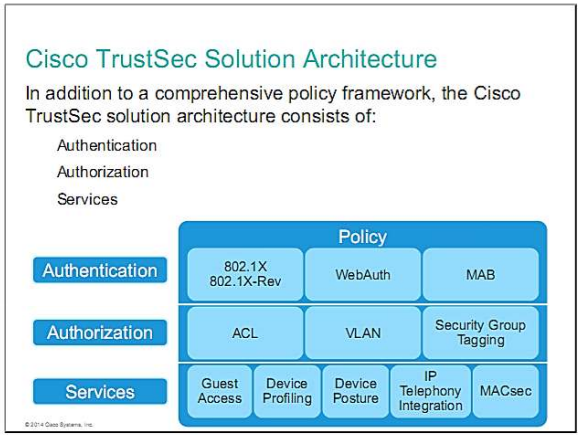
Downloadable ACL from ISE

SGTACL

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

Cisco TrustSec Architecture

The figure below shows the Cisco TrustSec solution architecture consists of authentication, authorization, and services modules. In addition, Cisco TrustSec provides a comprehensive policy framework.



Authentication

Cisco TrustSec provides a group of FlexAuth methods, including IEEE 802.1X, WebAuth, and MAB. Cisco TrustSec delivers the latest 802.1X technologies to reduce the operational overhead associated with deploying IEEE 802.1X in primarily wired environments. Some of the latest Cisco technology advances include a single switch port configuration that can accommodate all potential types of hosts, as well as managed, unmanaged, known, and unknown users. FlexAuth allows IT administrators to configure a single switch port with a consistent configuration that enables 802.1X, MAB, and WebAuth in any sequence to accommodate desired authentication requirements. Cisco Open Mode technology provides IT administrators with the flexibility to selectivity open, or pinhole, certain traffic types through the restricted 802.1X-enabled port. The most common use for this technology is to enable host management operations to function normally in an identity-based access control port implementation. Protocols such as PXE, SMS, Microsoft SUS, and others that assume network connectivity can be allowed to flow through the access-controlled port in a controlled manner. This technology also brings auditing and monitoring of 802.1X deployment readiness before 802.1X enforcement begins.

Cisco Network Edge Access Topology-powered compact switches extend 802.1X capabilities to the network edge (conference rooms, for example), providing the same level of security as the main switch in the wiring closet. Such simple and secure configuration delivers the Borderless Networks experience without sacrificing security.

Cisco TrustSec also supports the IEEE 802.1X-REV MKA standards-based key exchange protocol. 802.1X-REV builds on 802.1X to support additional capabilities such as authentication of multiple devices on a single switch port and keying material exchange for 802.1AE devices. 802.1X-REV enhances crypto key management capabilities to assist 802.1AE standard-based data encryption.

https://t.me/learningnets

Authorization

After network users and devices are authenticated and confirmed to comply with an organization's security policy, they are allowed network access. Their subsequent resource and service entitlement is accomplished by the authorization process. Cisco TrustSec supports multiple authorization methods, including ACLs, VLANs, and SGA.

These choices help organizations design their security architecture and services offerings with maximum flexibility and effectiveness. Downloadable, per-session ACLs and dynamic VLAN assignments can be implemented at the ingress point where users and devices gain their initial entry to the network. In addition, SGA allows user identity information to be captured and tagged with each data packet. SGACL can be implemented at an egress point where a network resource (such as a file server) is located. SGA-based access control allows organizations to keep the existing logical design at the access layer, and with flexible policies and services, to meet different business requirements without having to redeploy the security controls. Cisco TrustSec also delivers CoA based on RFC3576 RADIUS Disconnect Messages, which allows session-based, on-demand authorization to support advanced services such as IP telephony integration.

Services

Cisco TrustSec provides secure guest access while delivering a high-quality user experience. The guest access service supports guest access provisioning, notification, management, and reporting. Supported guest access methods include both local LAN and wireless.

Cisco TrustSec delivers endpoint profiling by automatically identifying and classifying devices by collecting endpoint data through the built-in ISE probes or network-based device sensors on the Cisco Catalyst switching and wireless infrastructure, and further refining the classification with directed, policy-based active endpoint scanning technology. This service provides visibility, intelligence, and automation to Cisco TrustSec deployments in the most efficient and scalable manner, reducing the ongoing maintenance cost.

Many organizations have strict endpoint device posture requirements such as the appropriate operating system, configurations and required system patches, as well as security software such as antivirus applications. The Cisco TrustSec solution includes endpoint agents that provide posture assessment and remediation to bring endpoint devices into compliance with security requirements. These services integrate with a wide range of endpoint security applications, and support built-in policies for more than 350 applications from leading antivirus and management software solution providers. Advanced features such as single-sign-on with Active Directory and silent remediation greatly reduce the impact on end users. Planned integration with the leading Mobile Device Management (MDM) solutions will further enhance organizations' ability to ensure mobile device compliance with their security policies.

Cisco TrustSec supports MDA that allows for the secure deployment of IP telephony, whether a Cisco or a third-party IP phone is used. Cisco Catalyst switches can be configured to secure data and voice VLANs on a single switch port. With MDA, a phone, with or without a supplicant, is authenticated and subsequently placed in the voice VLAN (or domain). Any device connecting through the phone Ethernet port will be authenticated first before access is allowed via a data VLAN.

Cisco TrustSec provides switch-port-level encryption based on IEEE 802.1AE (MACsec). Data encryption supports the AES cipher using a 128-bit key. Network traffic is encrypted to block man-in-the-middle attacks, snooping, and other forms of network attacks. Such Layer 2 encryption is implemented between an endpoint device and an access switch (for Cisco Catalyst 3560-X and 3750-X Series Switches) or between switch ports (for Cisco Nexus 7000 Series Switches). Cisco switches preserve traffic visibility within each switch to deliver the entire breadth of Cisco networking and security services.

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

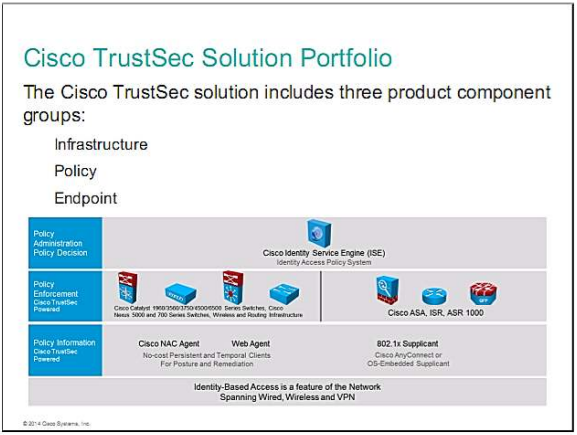
Policy

A converged policy framework is an essential factor to ensure policy consistency and efficiency to a distributed workforce. With the Cisco Identity Services Engine, Cisco TrustSec helps network and security administrators map user identity information to user groups based on their role in the organization. The policy intelligently directs network enforcement devices upon successful user authentication. The Cisco TrustSec policy framework provides a simple mechanism to provision and monitor policy based on user identity information throughout the network. This enables distributed enforcement with a central management system.

https://t.me/learningnets

Cisco TrustSec Solution Components

As figure below shows, the Cisco TrustSec solution includes three product component groups (infrastructure, policy, and endpoint), as well as Cisco and partner professional services.



Infrastructure Components

Cisco Catalyst 2960,3560,3750,4500, and 6500 Series Switches, Cisco Nexus 7000,5000, and 2000 Series Switches, Cisco Wireless LAN Controllers, Cisco Integrated Services Router Generation 2 platforms, and Cisco ASR 1000 Series Aggregation Services Routers interact with network users for authentication and authorization.

Access to the wired or wireless network is dictated by policy, user identity, and other attributes. Flexible authentication methods include 802.1X, web authentication, and MAC authentication bypass, all controlled in a single configuration for each switch port. Device sensors in the wired and wireless infrastructure automatically detect and help to classify devices attached to the network with minimal effort. Furthermore, Cisco switches that use SGA technology can tag each data packet with user identity information so that further controls can be deployed anywhere in the network. In addition, Cisco Nexus switches support MACsec (IEEE 802.1AE standard encryption) for data-in-motion confidentiality and integrity protection.

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

Policy Components

The Cisco Identity Services Engine is a next-generation identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline service operations. The Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices to make proactive governance decisions by enforcing policy across the network infrastructure. .

The Cisco ISE provides a highly powerful and flexible attribute-based access control solution that combines AAA; posture; profiling; and guest management services on a single platform. Administrators can centrally create and manage access control policies for users and endpoints in a consistent fashion, and gain end-to-end visibility into everything that is connected to the network. The Cisco ISE automatically discovers and classifies endpoints, provides the right level of access based on identity, and provides the ability to enforce endpoint compliance by checking a device's posture. The Cisco ISE also provides advanced enforcement capabilities, including SGA through the use of SGTs, SGACLs, and SG-FW.

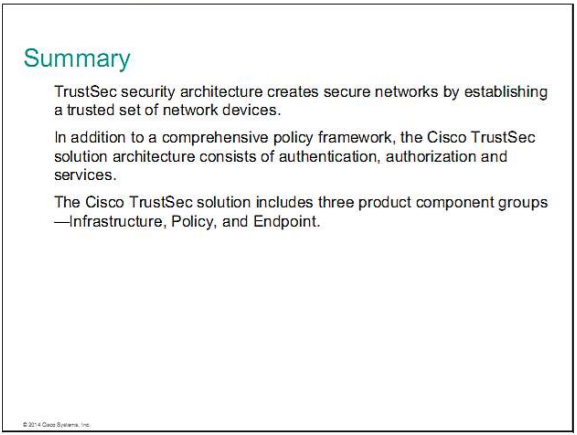
Endpoint Components

Cisco AnyConnect protects mobile employees on PC-based or smartphone platforms using an SSL or IPsec VPN to deliver a more seamless, always-on, and always-protected experience to end users, while enabling IT administrators to enforce policies and block malware with cloud-based or hybrid web security.

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:

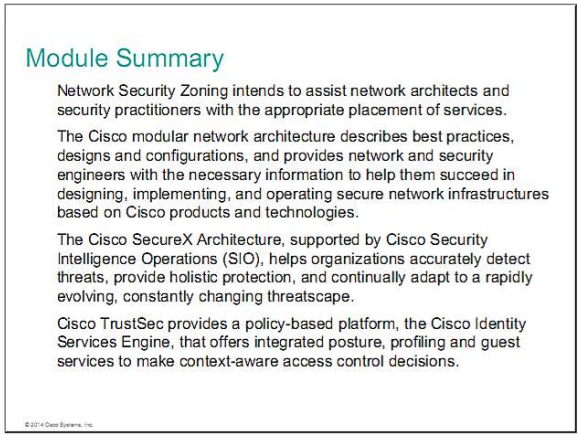
Cisco TrustSec
http://www.cisco.com/en/US/netsol/ns1051/

Cisco TrustSec: Enabling Switch Security Services
http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns147/ns774/net_implementation_white_paper0900aecd80716abd.html

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

Module Summary

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



https://t.me/learningnets

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

Module Self-Check

https://t.me/learningnets

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

Module Review Questions

1. Which option describes the Cisco SecureX architecture? (Source: Secure Network Architecture Overview)

   A. An intelligent, context-aware access control solution
   B. A context-aware, network-based solution to network security
   C. A context-aware, appliance-based solution to network security
   D. A design guide that quickly deploys security services

2. Which of the following are benefits of using Cisco modular network architecture ? (Select all that apply.)

   A. modular network architecture eases the development, implementation, and management of secure networks.
   B. modular network architecture provides for an open, modular, and expandable structure.
   C. modular network architecture is the basis for the design of highly available secure networks.
   D. modular network architecture provides for self-healing of network devices.

https://t.me/learningnets

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

Module 2

Network Infrastructure Protection Deployment

The network infrastructure is one of the foundation elements and a critical business asset of enterprise IT infrastructures. A compromise of the network infrastructure or its individual components can have far-reaching consequences that can significantly increase risk to enterprise business processes.

This module covers infrastructure protection controls that are available on Cisco IOS Software routers and switches, and Cisco ASA 5500-X Series Next-Generation Firewalls based network infrastructure. The module describes how to provide control plane, management plane, and data plane security for both switched and routed network infrastructures. Advanced features that can guarantee such protection are introduced, and configuration and verification are shown for each of these features. The module also describes how to provide network telemetry methods in the network infrastructure on Cisco IOS devices and Cisco ASA 5500-X Series Next-Generation Firewalls.

Upon completing this module, you will be able to:

- Provide an overview of network infrastructure protection controls
- Examine various defenses in Cisco IOS Software that protect the control plane
- Describe some strategies to protect the Cisco IOS management plane
- Describe some strategies to protect the Cisco ASA management plane
- Describe the baseline forms of telemetry recommended for network infrastructure devices
- Configure and verify Cisco IOS Software Layer 2 Data Plane Controls
- Configure and verify Cisco IOS Software and Cisco ASA Layer 3 Data Plane Controls

https://t.me/learningnets

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

Lesson 1

Introducing Cisco Network Infrastructure Protection

Overview

The network infrastructure is one of the foundation elements of enterprise IT infrastructures and is a critical business asset of telecommunications service providers. A compromise of the network infrastructure or its individual components can have far-reaching consequences that can significantly increase risk to enterprise and service provider business processes.

This lesson provides an overview of network infrastructure protection controls on Cisco IOS routers and switches and some of its features.

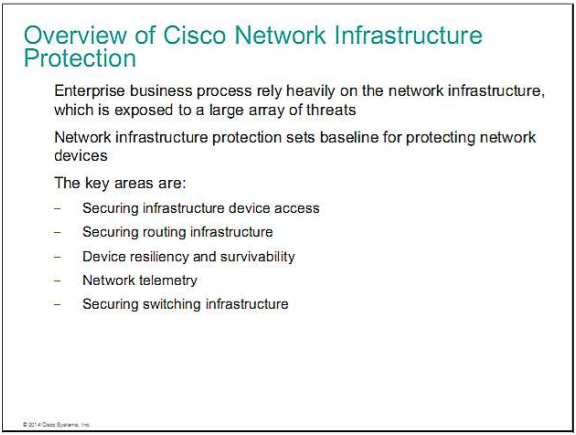
Upon completing this lesson, you will be able to:

- Provide an overview of network infrastructure protection
- Place network infrastructure protection into the Cisco modular network architecture design architectures
- Identify network device planes
- Describe control plane security controls
- Describe management plane security controls
- Describe network telemetry methods
- Describe Layer 2 data plane security controls
- Describe Layer 3 data plane security controls

https://t.me/learningnets

Overview of Cisco Network Infrastructure Protection

This topic provides an overview of network infrastructure protection.



Modern enterprise business processes rely heavily on the underlying enterprise IT infrastructure, which comprises these components:

The applications, systems (workstations, servers, laptops, smart phones and tablets, IP phones, etc.), and network infrastructure (routers, switches, security controls, telephony components, wireless APs, etc.) that provide the foundation for data processing and data transfer between various components and external parties

Data at rest (stored on systems and storage) and in motion (transferred over networks) that is processed within the foundation infrastructure

Infrastructure users who use applications that store, process, and transfer data over the foundation infrastructure

The network infrastructure, especially the public-facing part of it, is exposed to a large array of threats.

Some of the threats are:

DoS

DDoS

Unauthorized access

Session hijacking

Man-in-the-middle attack

Privilege escalation

Intrusions

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

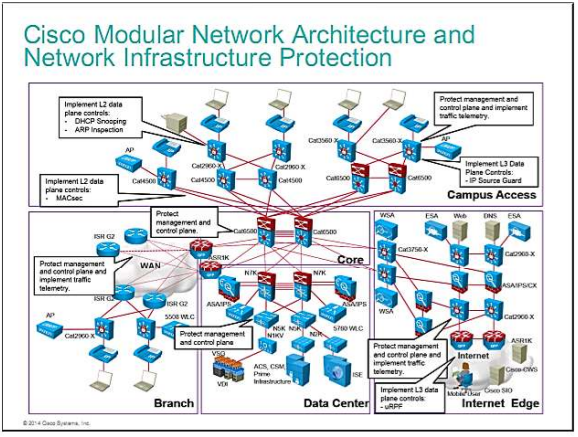
- Botnets
- Routing protocol attacks
- Spanning tree attacks
- Layer 2 attacks

Network infrastructure protection should be implemented in networks to provide a baseline to protect network devices as well to set a solid foundation on which more advanced methods and techniques can subsequently be built on.

https://t.me/learningnets

Cisco Modular Network Architecture and Network Infrastructure Protection

This topic places network infrastructure protection into the Cisco modular network architecture design architectures.

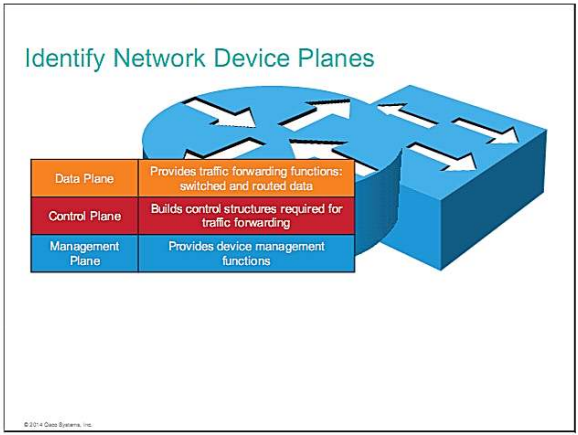


The figure illustrates where in the Cisco modular network architecture architecture network infrastructure protection controls should be deployed. Ideally, the network infrastructure protection controls should be implemented on all devices in the network. If that is not feasible, the network infrastructure protection controls should be implemented at least at the most exposed parts of the network.

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

Identify Network Device Planes

This topic identifies network device planes.



It is often beneficial to think of network devices in three separate contexts, as identified by their functionality planes. The functionality of a network device is therefore typically segmented into three planes of operation, each with a clearly identified objective:

Basic data plane functions are data switching and data routing. The data plane allows the device to forward network traffic and apply services (such as security, QoS, accounting, and optimization) to it as it is forwarded.

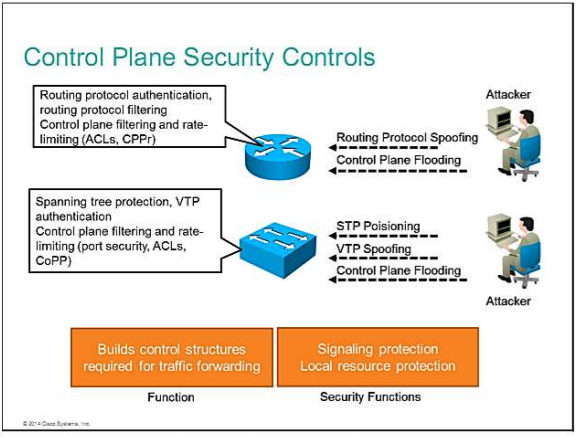
The control plane allows the device to build all of the required control structures (such as the routing table, forwarding table, and MAC address table) that will allow the data plane to operate correctly.

The management plane provides the device with all of the functions that administrators need to provision the configuration and monitor the operation of the device.

https://t.me/learningnets

Control Plane Security Controls

This topic describes control plane security controls.



The control plane of a network device can provide the following security-related features to protect the network device against compromise:

Signaling protection features, which prevent unauthorized entities from influencing traffic-forwarding control structures and, therefore, the traffic-forwarding process itself. The control plane of a device should authenticate signaling protocol (STP, VTP, or a routing protocol) information and possibly filter it before passing it on to other devices.

Methods for protecting the control plane processes of a device against access and flooding from untrusted entities. The control plane of a device should be able to filter or rate-limit packets that are destined for the control plane processes of the device. This filtering, or packet rate-limiting, is done to both minimize device exposure and to impose a strict limit on CPU and memory resources that can be consumed by control plane traffic.

The following list provides a brief description of some of the control plane controls:

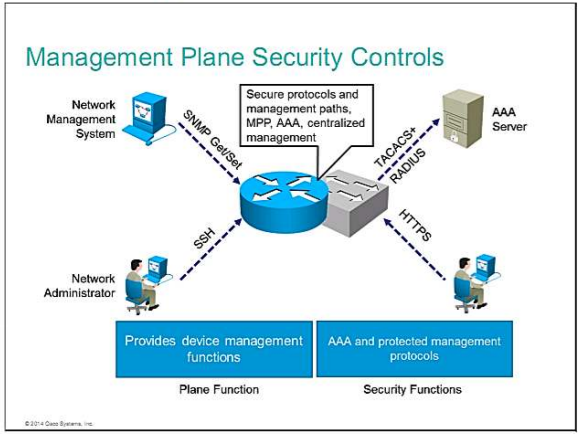
Infrastructure ACLs are used to minimize the risk and effectiveness of a direct infrastructure attack by explicitly permitting only authorized traffic to the infrastructure equipment while permitting all other transit traffic.

The Control Plane Protection feature is an extension of the policing functionality that is provided by the CoPP feature. The CoPP feature allows QoS policing of aggregate control plane traffic that is destined to the route processor. The Control Plane Protection feature extends this policing functionality by allowing finer policing granularity. The functionality that is added with Control Plane Protection includes a traffic classifier, which intercepts traffic and classifies it into three control plane categories. There are also port-filtering and queue-thresholding features. The port-filtering feature provides for policing of packets going to closed or nonlistened TCP or UDP ports, while queue-thresholding limits the number of packets for a specified protocol that will be allowed in the control plane IP input queue.

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

Management Plane Security Controls

This topic describes management plane security controls.



The management plane of a network device can provide security-related features that protect the device against compromise. These features include the following:

Protected management protocols, over which administrators access devices. If the path between administrators and devices is not trustworthy, the management plane should provide cryptographic protection to management sessions or rely on data plane features of other network devices (for example, VPN protection) to prevent interference with management sessions.

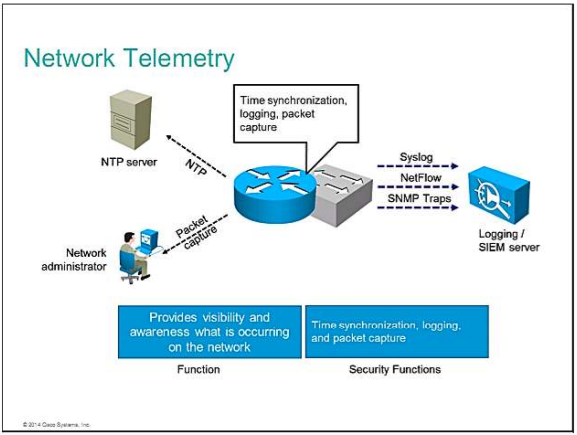
The MPP feature in Cisco IOS Software provides the capability to restrict the interfaces on which network management packets are allowed to enter a device. The MPP feature allows a network operator to designate one or more router interfaces as management interfaces. Device management traffic is permitted to enter a device only through these management interfaces. When MPP is enabled, no interfaces except designated management interfaces will accept network management traffic that is destined to the device. Restriction of management packets to designated interfaces provides greater control over the management of a device and provides more security for that device. Other benefits include improved performance for data packets on nonmanagement interfaces, support for network scalability, a need for fewer ACLs to restrict access to a device, and the prevention of management packet floods on switching and routing interfaces from reaching the CPU.

AAA feature set that validates administrator identity and suitably limits administrator access to device functions. Ideally using RBAC and minimal required privileges, the AAA feature audits all administrator actions and security-relevant device events. In most networks, centralizing AAA policy functions and audit trail collection—using a centralized AAA server function and a central logging or security information management system—is strongly recommended.

https://t.me/learningnets

Network Telemetry

This topic describes network telemetry methods.



In order to operate and ensure availability of a network, it is critical to have visibility and awareness into what is occurring on the network at any given time. Network telemetry offers extensive and useful detection capabilities that can be coupled with dedicated analysis systems to collect, trend, and correlate observed activity.

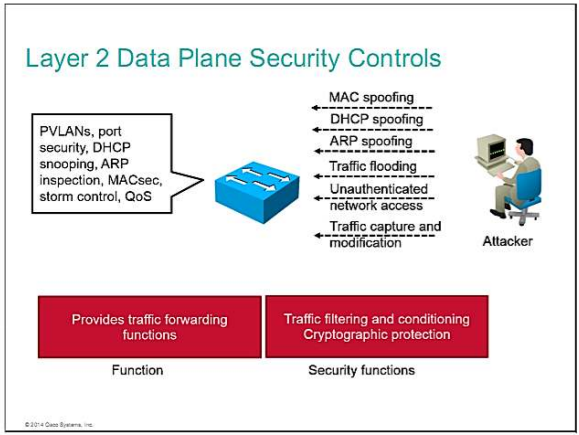
Baseline network telemetry is both inexpensive and relatively simple to implement. The following baseline forms of telemetry are recommended for network infrastructure devices:

- Time synchronization
- Local device traffic statistics
- System status information
- Syslog
- SNMP
- ACL logging
- Accounting
- Archive configuration change logger
- Packet capture

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

Layer 2 Data Plane Security Controls

This topic describes Layer 2 data plane security controls.



The data plane of a switch network device can provide the following security-related features to protect the network device and network endpoints against L2 attacks:

- Traffic filtering features, which can prevent identity theft and spoofing attack (for example, features that can address MAC, DHCP, and ARP spoofing attacks), limit flooding attacks, limit access to network devices, or prevent attacks against network-connected endpoints.
- Traffic conditioning (QoS) features, which can control and enforce proper network link use.
- Transmission protection features that cryptographically encapsulate network traffic for transport over untrusted networks (IEEE 802.1AE MACsec).

The following list provides a brief description of some of the Layer 2 data plane controls:

- DHCP snooping is a Layer 2 security feature that specifically prevents DHCP server spoofing attacks and mitigates DHCP starvation to a degree. DHCP snooping provides DHCP control by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database, which is also referred to as a DHCP snooping binding table.
- The ARP inspection feature prevents ARP spoofing attacks by intercepting and validating all ARP requests and responses. Each intercepted ARP reply is verified for valid MAC-to-IP address bindings before it is forwarded. ARP replies that have invalid MAC-to-IP address bindings are dropped.
- The traffic storm control feature monitors incoming traffic levels over a 1-second traffic storm control interval. During the interval, it compares the traffic level with the configured traffic storm control level. The traffic storm control level is a percentage of the total available bandwidth of the port. Each port has a single traffic storm control level that is used for all types of traffic—broadcast, multicast, and unicast.
- The PVLAN feature provides Layer 2 isolation between ports within the same VLAN. This isolation eliminates the need for a separate VLAN and IP subnet per customer and provides a coarse access control mechanism that is easy to manage.

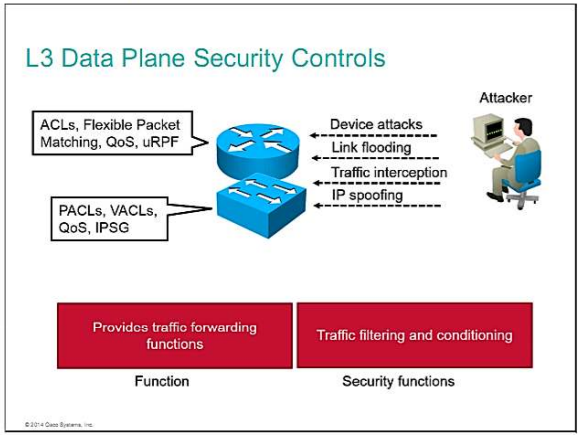
https://t.me/learningnets

MACsec encryption provides MAC-layer encryption over wired networks using OOB methods for encryption keying. With the MACsec, you can encrypt switch-to-switch links such as access to distribution, or encrypt dark-fiber links within a building or between buildings.

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

Layer 3 Data Plane Security Controls

This topic describes L3 data plane security controls.



The data plane of a Layer 3 network device can provide the following security-related features to protect the network device and network endpoints against L3 attacks:

- Traffic filtering features (ACLs, Flexible Packet Matching) and antispoofing controls (ACLs and uRPF) to prevent identity theft, limit access to network devices and endpoints, and to prevent device compromise.
- Traffic conditioning (QoS) features, which can control and enforce proper network link use.

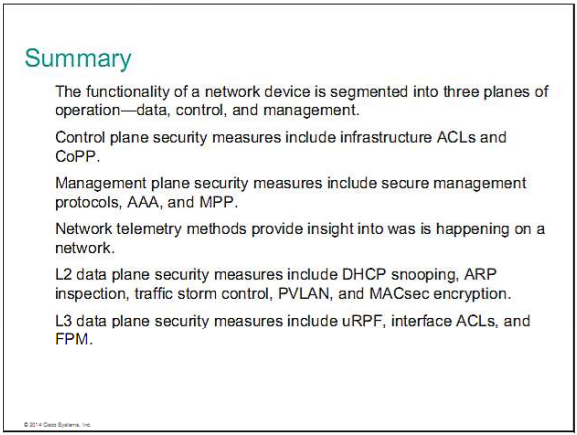
The following list provides a brief description of some of the Layer 3 data plane controls:

- As defined in RFC 3704, uRPF is an evolution of the concept that traffic from known invalid networks should not be accepted on interfaces from which they should never have originated. The original idea was to block traffic on an interface if it is sourced from private addresses. It is a reasonable assumption for many organizations to simply disallow propagation of private addresses on their networks unless they are explicitly in use. This is a benefit to the Internet backbone because blocking packets from obviously fake source addresses helps to cut down on IP address spoofing, which is commonly used in DoS, DDoS, and network scanning to obfuscate the source of the scan.
- Interface ACLs filter traffic on the interface based on the match criteria in the packet header—source and destination IP address, source and destination port, protocol, and flags.
- FPM is the ACL pattern-matching tool and provides more thorough and customized packet filters. FPM enables users to match on arbitrary bits of a packet at an arbitrary depth in the packet header and payload. FPM removes constraints to specific fields that had limited packet inspection. FPM is useful because it enables users to create their own stateless packet classification criteria and to define policies with multiple actions (such as drop, log, or send ICMP unreachable) to immediately block new viruses, worms, and attacks.

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

Deploying Cisco IOS Control Plane Security Controls

Overview

The control plane in an OSI Layer 3 device provides traffic-routing functions by building the device routing and forwarding tables, and often involves cooperation with nearby devices using dynamic routing protocols. These interactions must be controlled by authenticating the associations between devices, discarding malicious routing information, and protecting the resources of each device against excessive use.

This lesson examines various defenses in Cisco IOS Software that protect the control plane, such as infrastructure ACLs, Control Plane Policing and Control Plane Protection. This lesson also introduces strategies for protecting routing protocols using routing protocol authentication and filtering.

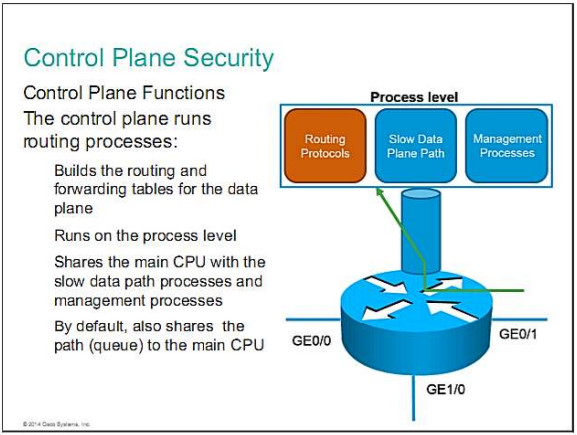
Upon completing this lesson you will be able to:

- Describe Cisco IOS Software control plane security
- Describe infrastructure ACLs
- Describe Cisco IOS Software Control Plane Policing
- Describe Cisco IOS Software Control Plane Protection
- Configure Control Plane Protection
- Verify Control Plane Protection
- Describe routing protocol authentication as a control plane countermeasure
- Describe routing protocol filtering as a control plane countermeasure

https://t.me/learningnets

Overview of Control Plane Security

This topic describes Cisco IOS Software control plane security.



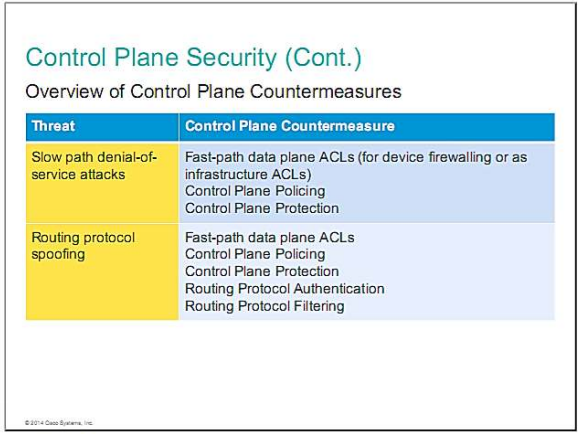
The routed control plane is a collection of processes that runs at the process level on the CPU of a network device and provides the baseline routing functions in a device. These functions primarily include building the routing and forwarding tables by using either static configuration (static routes) or with the help of dynamic routing protocols.

The routed control plane functions (shown as the routing protocols box in the figure) share the CPU of the main router with two other groups of processes:

- The management processes, which provide device management functions.
- The slow data path processes (process switching or the Cisco Express Forwarding process path), which manage traffic that cannot be managed by the fast data path. (The fast path consists of interrupt switching functions of Cisco Express Forwarding, or hardware-assisted forwarding.)

By default, these three aspects also share the path (queue) from the data plane, where packets received by the device are passed to the main CPU for detailed processing.

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



Because the CPU is shared among the three functions (control plane, management plane, slow data path), excessive traffic to one of these three functions can, by default, overwhelm the entire CPU and influence the behavior of the other two functions. This can lead to flooding attacks, in which the attacker can disable these three functions by sending a high rate of packets to the CPU. There are multiple possible countermeasures that guard against this threat:

- The use of device fast-path data plane ACLs (usually these are interface ACLs of routers and switches) to deny most traffic before it is dispatched into the slow path to the CPU of the router. Because these ACLs are very efficient and are often implemented in hardware in OSI Layer 3 switches and high-end routers, they can drop most malicious traffic without any impact to the CPU. Instead of implementing such ACLs on every device, you can deploy these ACLs at the edge of your network (that is, infrastructure ACLs) to prevent endpoints from injecting traffic that would be forwarded to device CPUs. Note however, that ACLs must be configured with appropriate destination addresses, which may not be scalable if devices use many IP addresses (interfaces). If these addresses are not contiguous, they can make ACLs difficult to manage.
- The use of specific, on-device protection methods that can filter or rate-limit traffic to the CPU, while leaving fast-path transit traffic untouched. CoPP and Control Plane Protection are two such features.

Another significant threat to routed control planes is the injection of malicious routing information. Attackers can use malicious routing information to redirect or black-hole sensitive traffic and therefore violate its confidentiality, integrity, or ability to perform a denial-of-service attack. These risks can be mitigated by the following:

- Use fast-path data plane ACLs to limit who can send routing protocol information to network devices. Again, this may not be scalable because of many interfaces and discontiguous IP addressing of network links.
- Use the CoPP and Control Plane Protection features to locally limit the authorized routing protocol peers by their IP address.
- Use routing protocol authentication, in which a cryptographic integrity and authenticity proof is embedded within each routing protocol message that prevents routing adjacency and routing update spoofing.

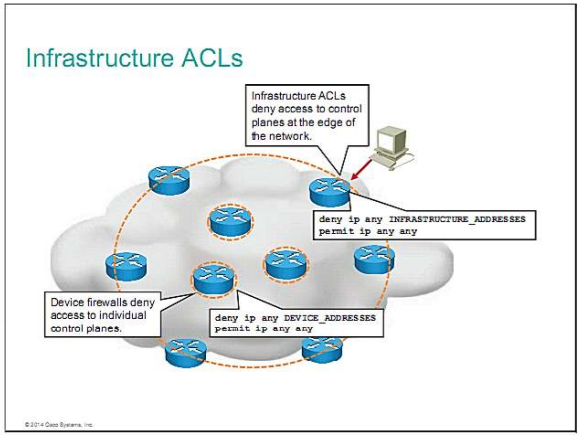
https://t.me/learningnets

Use routing protocol filtering, which prevents injection of malicious routing information from known, authenticated peers.

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

Infrastructure ACLs

This topic describes infrastructure ACLs.



Contrary to device-centric methods, infrastructure ACLs filter traffic on the network edge, on access OSI Layer 3 devices that accept IP traffic from network users or external networks.

There are various device-centric methods:

Device firewalls or "personal" firewalls are implemented on each network device to protect the device itself against unwanted connectivity.

Control plane rate limiters are implemented by on-device mechanisms (such as CoPP and Control Plane Protection).

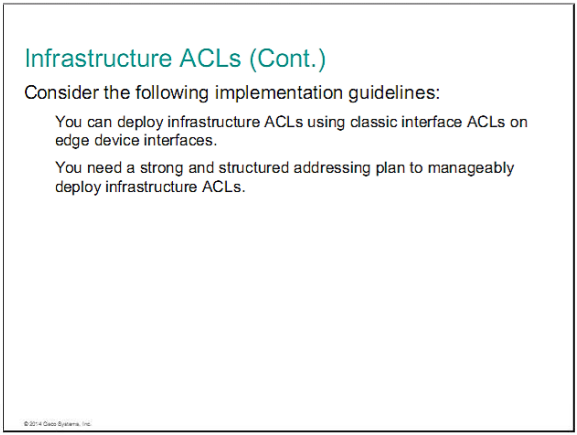
Infrastructure ACLs are typically applied in the input direction on the interface that connects to the network users or external networks with the following policies:

All traffic to the IP addresses of network infrastructure devices is dropped and logged. This rule prevents network users from sending routing protocol or management traffic to network devices. You must include destination addresses that encompass all device IP addresses as a condition. Note that this approach does not prevent users from sending malicious transit traffic that would require processing in the CPU-intensive slow data plane paths on network devices. Such transit traffic may include packets with IP options or packets that require processing that is not supported in the efficient fast data plane path.

All other traffic is permitted and allows all transit traffic over the network.

The first rule may need to be relaxed to permit some network signaling exceptions, such as BGP sessions from external networks.

https://t.me/learningnets



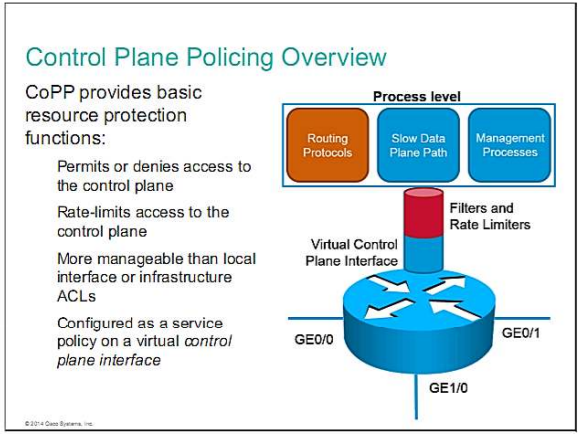
When implementing infrastructure ACLs, consider these implementation guidelines:

- You can implement these filtering rules using traditional Cisco IOS Software ACLs or FPM rules. If you need to make exceptions, you can also consider using rate-limiting functions—such as class-based policing—at the edge of the network.
- To implement infrastructure ACLs, you need a strong and structured addressing plan to minimize the size of the infrastructure ACLs. If your network lacks such a design, you may consider only on-device countermeasures instead.

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

Control Plane Policing Overview

This topic describes Cisco IOS Software Control Plane Policing.



CoPP uses early rate limiting and drops traffic that is destined for the central processor of the network device by applying QoS policies to a virtual aggregate CPU-bound queue, called the "control plane interface." This queue receives all aggregated traffic that is destined for the control plane (which includes the routing protocols), the management plane (management processes), and the slow data plane path traffic of the network device.

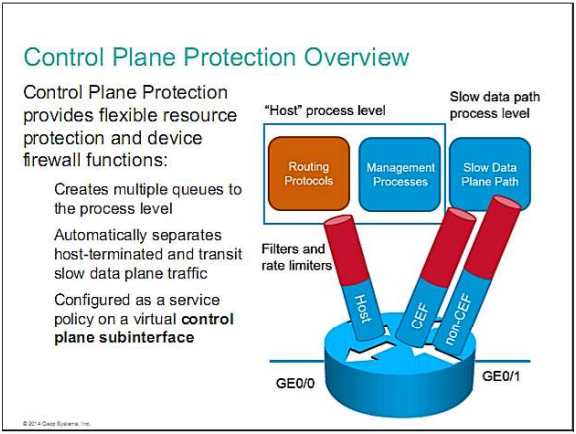
CoPP can granularly permit, drop, or rate-limit traffic to the CPU using a MQC interface. Because CoPP aggregates all traffic that is forwarded to the CPU of the network device, it is independent of interfaces. This independence allows a central configuration mechanism to protect the network device CPU resources of the process layer of a device.

Note Configuration of CoPP is not shown in this course because its functionalities have been extended by CPPr. However, CoPP is described here for the sake of better understanding of CPPr, and because some platforms do not support CPPr, but support CoPP.

https://t.me/learningnets

Control Plane Protection Overview

This topic describes Cisco IOS Software Control Plane Protection.



Control Plane Protection extends the CoPP functionality by automatically classifying all CPU-bound traffic into three queues (or subinterfaces) under the aggregate control plane interface. Each subinterface receives and processes a specific type of CPU-bound traffic, and each subinterface has a separate traffic policy that is attached to it, which makes limit configuration easier.

Thee control plane subinterfaces are automatically created by Control Plane Protection:

The control-plane host subinterface: This interface receives all control plane IP traffic that is directly destined for one of the router interfaces (physical and loopback). Examples of control plane host IP traffic include tunnel termination traffic; management traffic; and routing protocols such as SSH, SNMP, IBGP, and EIGRP. All host traffic terminates on and is processed by the router. Most control plane protection features and policies operate strictly on the control plane host subinterface. Because most critical router control plane services, such as routing protocols and management traffic, are received on the control plane host subinterface, it is critical to protect this traffic through policing and protection policies. CoPP, port filtering, and per-protocol queue thresholding protection features can be applied on the control plane host subinterface.

The control-plane Cisco Express Forwarding-exception subinterface: This control plane subinterface receives all traffic that is either redirected as a result of a configured input feature in the Cisco Express Forwarding packet forwarding path for process switching or directly enqueued in the control plane input queue by the interface driver (that is, ARP, EBGP, OSPF, LDP, Layer 2 keepalives, and all non-IP host traffic). CPPr allows specific aggregate policing of this type of control plane traffic

The control-plane transit subinterface: This subinterface receives all control plane IP traffic that is software-switched by the route processor. This means packets that are not directly destined to the router itself but rather traffic traversing through the router. A tunnel handled by the router is an example of this type of control plane traffic. CPPr allows specific aggregate policing of all traffic that is received at this subinterface.

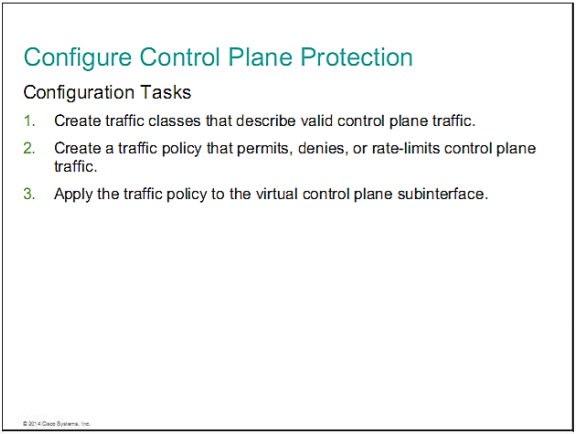
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

The transit and Cisco Express Forwarding exception subinterfaces process all slow-path data plane forwarding traffic together.

https://t.me/learningnets

Configure Control Plane Protection

This topic describes how to configure Control Plane Protection.



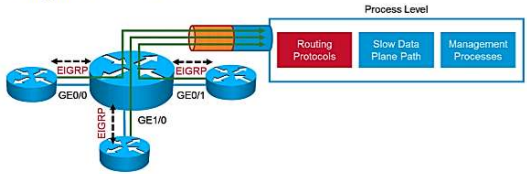
To configure Control Plane Protection, complete the following tasks:

1. Create traffic classes that describe valid control plane traffic. You can configure as many traffic classes as you need, depending on the required granularity of your policy.
2. Create a traffic policy that will permit, deny, or rate-limit the configured traffic classes and therefore conserve process layer resources, or even act as a device firewall by hiding most device resources from the network.
3. Apply the configured traffic policy to a required Control Plane Protection subinterface.

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

Configure Control Plane Protection (Cont.)

Configuration Scenario



Router peers use EIGRP:

- EIGRP peers are directly connected in the 10.0.0.0/8 network and produce no more than 200 packets per second.
- All other traffic for the control plane should not produce more then 50 packets per second.

© 2014 Cisco Systems, Inc.

This figure shows the configuration scenario for the Control Plane Protection configuration tasks. The protected device uses the EIGRP routing protocol with three EIGRP peers. All peers are connected to subnets of the 10.0.0.0/8 network and, together, produce no more than 200 EIGRP packets per second. The network in the example uses no other routing protocols. All other traffic for the control plane should not produce more then 50 packets per second.

Configure Control Plane Protection (Cont.)

Configuration Example

```
ip access-list extended CPPR-EIGRP
  permit eigrp 10.0.0.0 0.255.255.255 any
!
class-map CPPR-EIGRP-CLASS
  match access-group  name CPPR-EIGRP
!
policy-map CPPR-POLICY
  class CPPR-EIGRP-CLASS
    police rate 200 pps conform-action transmit exceed-action drop
  class class-default
    police rate 50 pps conform-action transmit exceed-action drop
!
control-plane host
  service-policy input CPPR-POLICY
```

© 2014 Cisco Systems, Inc.

In the first task of the overall configuration, you must create traffic classes to describe the valid control plane traffic. In this case, the valid control plane traffic comprises traffic from the three EIGRP adjacencies, which source EIGRP traffic (from the 10.0.0.0/8 network). In this example, the COPP-EIGRP ACL describes this traffic. The COPP-EIGRP-CLASS class refers to the COPP-EIGRP ACL.

https://t.me/learningnets

In the second task, you must create a traffic policy to describe the actions that are taken for each traffic class that is encountered in the control plane policer. In this example, the CPPR-POLICY lists the configured CPPR-EIGRP-CLASS traffic class and imposes a limit of 200 p/s for this class. Traffic conforming to this rate is permitted to the process level, and traffic exceeding it is dropped by the policer. The traffic policy also lists the class-default traffic class and imposes a limit of 50 p/s for this class, to rate limit all other traffic to the control plane subinterface.

In the last task, you have to apply the traffic policy to the control plane subinterface. In the example, the policy is applied to the host subinterface.

To configure Control Plane Protection on the Cisco IOS router, use the commands that are described in this table:

Commands	Description
ip access-list extended CPPR-EIGRP **permit eigrp 10.0.0.0 0.255.255.255 any**	Specifies the EIGRP routing protocol using the ACL.
class-map CPPR-EIGRP-CLASS **match access-group name CPPR-EIGRP**	Creates a traffic class that refers to the configured ACL.
policy-map CPPR-POLICY **class CPPR-EIGRP-CLASS** **police rate 200 pps conform-action transmit exceed-action drop** **class class-default** **police rate 50 pps conform-action transmit exceed-action drop**	Creates a traffic policy (policy map) and refers to the configured class and specifies its handling.
control-plane host **service-policy input CPPR-POLICY**	Applies the policy map to the control plane host subinterface.

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

Verify Control Plane Protection

This topic describes how to verify Control Plane Protection.

Verify Control Plane Protection

Control Plane Protection Verification Command	Description
show policy-map control-plane all	Displays the configuration and operation of Control Plane Protection.

© 2014 Cisco Systems, Inc.

Cisco IOS Software includes rich Control Plane Protection validation features.

Use the **show policy-map control-plane all** command to verify the proper configuration and operation of Control Plane Protection.

Verify Control Plane Protection (Cont.)

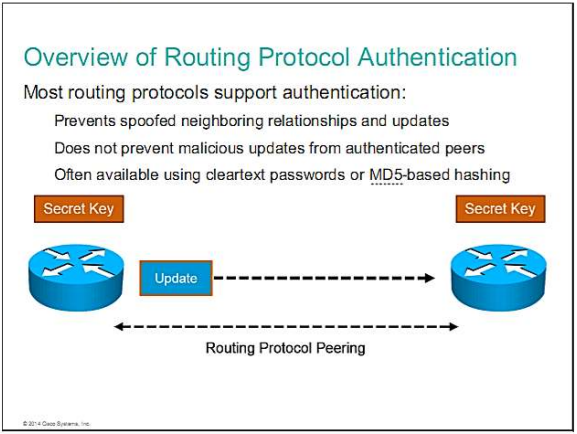
```
Router# show policy-map control-plane all
 Control Plane Host
  Service-policy input: CPPR-POLICY
    Class-map: CPPR-EIGRP-CLASS (match-all)
      13 packets, 1062 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name CPPR-EIGRP
      police:
          rate 200 pps, burst 48 packets
        conformed 13 packets, 13 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0 pps, exceeded 0 pps
    Class-map: class-default (match-any)
      16 packets, 7664 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
      police:
          rate 50 pps, burst 12 packets
        conformed 2 packets, 2 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0 pps, exceeded 0 pps
```

In the example, the **show policy-map control-plane** command verifies the proper configuration and operation of Control Plane Protection.

https://t.me/learningnets

Overview of Routing Protocol Authentication

This topic describes routing protocol authentication as a control plane countermeasure.



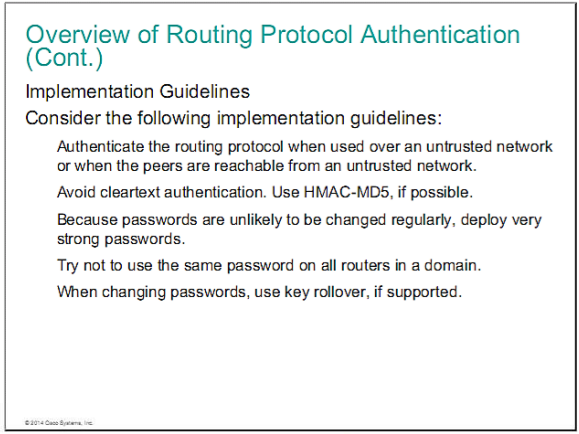
A routing protocol often needs to be protected to prevent access to unknown peers and to reject forged routing updates through routing protocol peer and update authentication. This allows only trusted routers to participate in routing, but does not prevent injection of malicious routing information in case of trusted device compromise.

Most routing protocols support both cleartext passwords (that is, the password is included in the routing update in cleartext) and the MD5 HMAC algorithm to produce the message authentication code that is sent with the update. HMAC-MD5 combines the shared secret password and the information in the packet itself, and MD5 is a "one way" function. Therefore, knowing the packet contents and the resulting hash does not enable the reverse calculation of the original secret password. However, if the shared secret is not changed for a long time, then the risk that it could still be revealed somehow increases.

This table shows the availability of routing protocol authentication features on various Cisco devices.

Feature	Platform
RIPv2 MD5 authentication	Cisco IOS routers and Layer 3 switches, Cisco ASA 5500-X
OSPF MD5 authentication	Cisco IOS routers and Layer 3 switches, Cisco ASA 5500-X
BGP MD5 authentication	Cisco IOS routers and Layer 3 switches
EIGRP MD5 authentication	Cisco IOS routers and Layer 3 switches, Cisco ASA 5500-X
HSRP MD5 authentication	Cisco IOS routers and Layer 3 switches

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



When implementing routing protocol authentication, consider following these implementation guidelines:

Authenticate the routing protocol when a broadcast segment is shared by routers and untrusted end-stations, when a public WAN can be compromised either by an attacker injecting false routing information, or by a service provider accidentally interconnecting circuits of different organizations. Generally, authenticate the routing protocol when a routing protocol runs over an untrusted network (for example, BGP over the Internet).

Always prefer HMAC-MD5 over cleartext authentication. If the attacker manages to capture a routing protocol packet, it will still be infeasible to derive the secret key (if it is strong enough).

Deploy very strong secrets initially because secret keys are unlikely to be changed regularly.

Try not to use the same secret on all routers in a domain. If possible, use multiple secrets with clearly defined groups of routers (for example, a separate secret for each OSPF area).

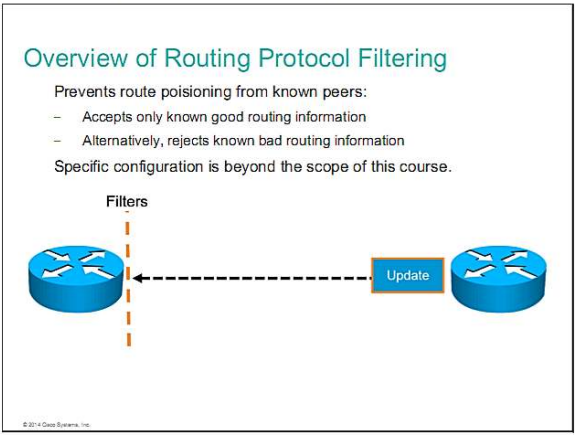
If changing keys, use key rollover, if supported.

Note Configuration of routing protocols authentication is outside of the scope of this course.

https://t.me/learningnets

Overview of Routing Protocol Filtering

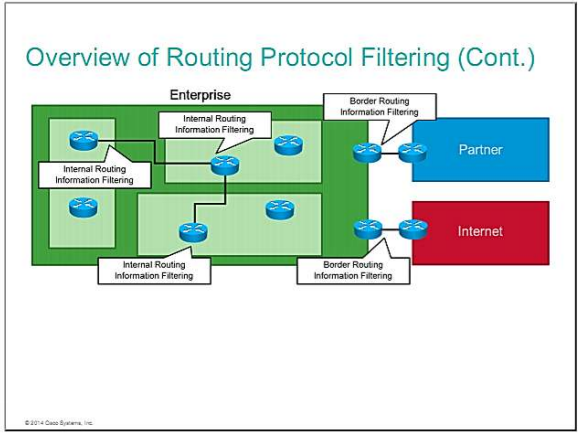
This topic describes routing protocol filtering as a control plane countermeasure.



To control the routing information that is accepted and transmitted to and from known peers, from a trusted or untrusted network, deploy routing information filtering. Such filters can allow only known good information to be accepted or transmitted from the routing cloud, or alternatively—if the first approach is not possible—drop known malicious routing information and permit all other routing information.

Note	Configuring specific routing protocols and their filtering functions is beyond the scope of this course.

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

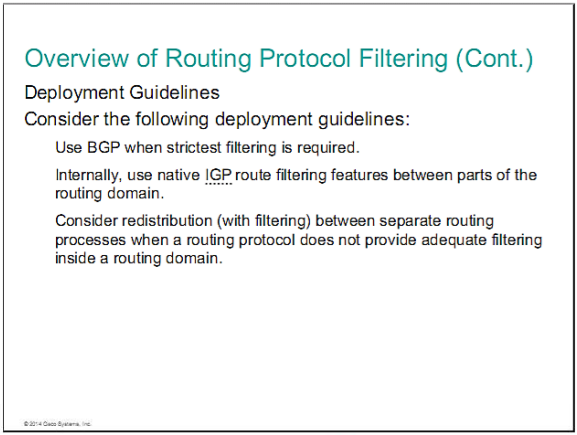


Routers on routing domain boundaries should perform routing protocol firewalling by filtering routing information (network prefixes) received or transmitted to less trusted peers. Routers should use traditional Cisco IOS Software mechanisms to perform the route filtering functions, such as distribute lists, prefix lists, community lists, and redistribution with filtering.

This table shows the availability of routing protocol filtering features on various Cisco devices.

Feature	Platform
RIPv2 distribute lists	Cisco IOS routers and Layer 3 switches, Cisco ASA 5500-X
OSPF ABR filtering	Cisco IOS routers and Layer 3 switches, Cisco ASA 5500-X
BGP filtering	Cisco IOS routers and Layer 3 switches
EIGRP distribute lists	Cisco IOS routers and Layer 3 switches, Cisco ASA 5500-X

https://t.me/learningnets



When deploying routing protocol filtering, consider the following general deployment guidelines:

- It is generally best to deploy BGP as the routing protocol when connecting to an external routing domain, where the strictest filtering is required. BGP supports the largest array of filtering mechanisms, and it is very conservative when advertising or relaying routing information.
- Internally, use the native filtering features of IGPs to filter routing information between parts of the enterprise routing domain. In large networks, you may also consider using BGP internally for the tightest control over routing information.

Redistribution between the two routing processes can be a welcome tool, when a routing protocol by itself does not provide sufficient filtering capabilities.

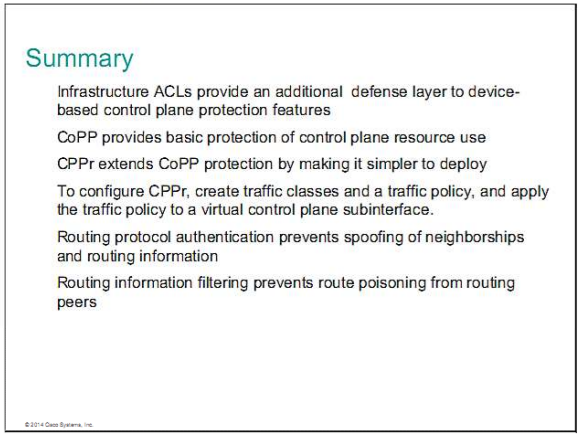
At the point where the two security zones intersect, two routing processes could exist:

- A trusted routing process that is connected into the trusted domain or segment.
- An untrusted routing process, exchanging information with less trusted peers.

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

Summary

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



https://t.me/learningnets

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

Lesson 3

Deploying Cisco IOS Management Plane Security Controls

Overview

The management plane performs all of the management functions for a device and coordinates functions between the control and data planes. These functions make the management plane a prime target for attacks.

This lesson introduces you to some strategies to protect the management plane by limiting access to it, limiting access to its individual features, configuring security features of the SNMPv3, and implementing RBAC using AAA framework.

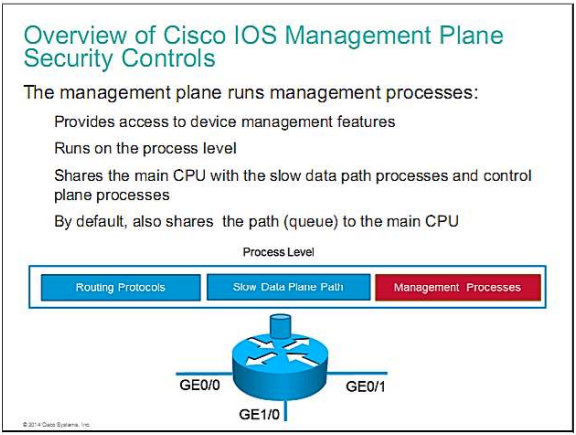
Upon completing this lesson you will be able to:

- Describe Cisco IOS management plane security controls
- Describe different ways how to secure management access to Cisco IOS devices
- Configure secure management access on the Cisco IOS devices
- Verify secure management access on the Cisco IOS devices
- Describe SNMPv3
- Configure SNMPv3 on the Cisco IOS devices
- Verify SNMPv3 on the Cisco IOS devices
- Describe management access AAA
- Configure management access AAA on the Cisco IOS Software

https://t.me/learningnets

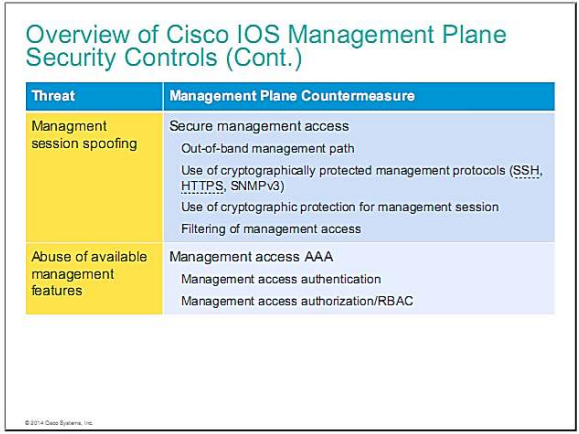
Overview of Cisco IOS Management Plane Security Controls

This topic describes Cisco IOS management plane security controls.



The management plane is a collection of processes that runs at the process level on the CPU of a network device. It provides the device with management features and management access methods that administrators can use to locally or remotely access the device. The management plane functions share the CPU of the main router with control plane processes, such as routing protocols and data plane slow-path traffic processing functions. By default, these three aspects also share the packet path (queue) to the main CPU.

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



The management plane is susceptible to two major threat classes:

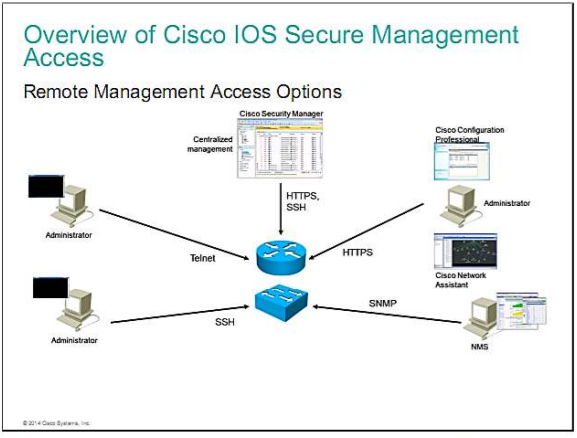
Spoofing of management sessions, in which attackers hijack existing sessions, steal administrator credentials, or spoof the legitimate IP addresses of administrators to gain management access to a device. You can reduce these risks by using out-of band management paths, or by using cryptographically protected management protocols or cryptographically protected management sessions and by tightly filtering access to devices to allow access from only specific networks, if routing in your network is trusted and IP spoofing is unlikely.

Attacker and rogue administrator abuse of management features, in which authenticated users act maliciously, or beyond their authorized profiles, to change the behavior of a network device in an undesirable manner. To reduce these risks, you can deploy strong authentication to prevent identity theft and RBAC restrictions to limit access to specific management features.

https://t.me/learningnets

Overview of Cisco IOS Secure Management Access

This topic describes different ways how to secure management access to Cisco IOS devices.



Cisco IOS Software provides four main protocols that you can use to remotely access the management functions:

Telnet: This protocol allows CLI access to Cisco routers and switches. Do not use the Telnet protocol over untrusted networks. Telnet is considered obsolete for security device management.

SSH: SSH allows secure CLI access to Cisco routers and switches.

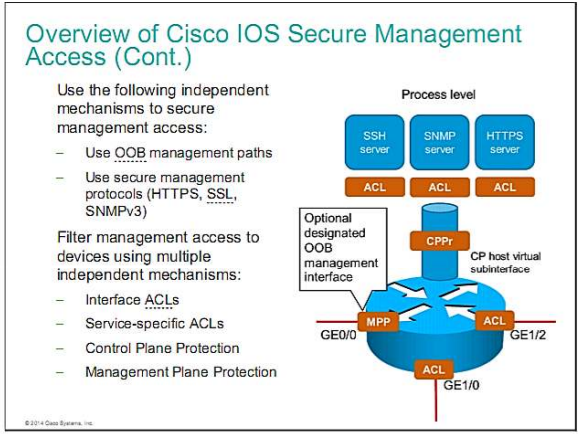
HTTPS on Cisco routers: HTTPS is a strongly encrypted and strongly authenticated protocol that allows GUI access to the Cisco router, using Cisco Configuration Professional. Cisco Configuration Professional is a GUI-based device management tool for ISRs. Cisco Configuration Professional simplifies configurations for routers, firewalls, IPS, VPN, unified communications, WAN, and basic LAN configurations, using GUI-based, easy-to-use wizards. Cisco Configuration Professional is installed on a PC.

HTTPS on Cisco switches: HTTPS is a strongly encrypted and strongly authenticated protocol that allows GUI access to Cisco switches, using Cisco Network Assistant. Cisco Network Assistant simplifies many common networking activities. Using an intuitive GUI, users can easily apply common services across Cisco switches, routers, and access points to facilitate configuration management.

SNMP: This protocol allows you to monitor Cisco router and switch parameters for performance and logging of system events.

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

Cisco IOS Software devices can be also managed centrally using Cisco Security Manager. Cisco Security Manager is a centralized policy provisioning tool that provisions configurations and security policies to many devices, including Cisco IOS Software devices and other security devices. Cisco Security Manager also supports provisioning of many platform-specific settings, for example, interfaces, routing, identity, QoS, and logging. To integrate the Cisco IOS Software devices with Cisco Security Manager, you have to enable HTTPS and SSH on the devices.



To secure management access to Cisco IOS devices you can use two general independent mechanisms:

Use the OOB management philosophy, which establishes a logically or physically separate network, over which managed devices are communicated with. Such a network is well isolated from the network forwarding user traffic, and the chance of spoofing and interception of management traffic is much lower, unless the attacker can physically compromise the OOB management network. For this reason, it may be acceptable to use unprotected (cleartext) management protocols, perhaps with weaker authentication, over such OOB management networks.

Use secure management protocols, such as SSH, HTTPS, or SNMPv3. If you use unsecure management protocol, use cryptographic traffic protection, for example IPsec VPN.

Additionally, limit access to a device management plane to reduce the risk of unauthorized management plane access. If your network is engineered to reduce the likelihood of IP spoofing, for example, by using uRPF mechanisms, or ingress and egress anti-spoofing ACLs, you can effectively deploy IP-address-based filters to only allow access to device management planes from trusted hosts and networks.

Note Cisco IOS devices support SSH version 1 and 2. SSH version 2 introduced some enhancements if compared to version 1. One of the enhancement is support for SSH clients to authenticate using RSA pair keys.

For devices using Cisco IOS Software, you can employ various independent mechanisms to limit access to device management planes:

You can deploy interface ACLs, which deny access to management IP addresses of the device on all device interfaces.

https://t.me/learningnets

You can deploy service-specific ACLs that limit access to a specific management process (using for example, vty or SNMP server ACLs).

Cisco IOS Software Control Plane Protection can simplify and enhance management access control, which is provided by interface ACLs, by centralizing access control at a virtual control plane interface.

The Cisco IOS Software Management Plane Protection feature lets you designate an interface on a device as the only interface over which management traffic is allowed to and from the device. Thus, the device can connect to a dedicated OOB management network with minimal access control configuration.

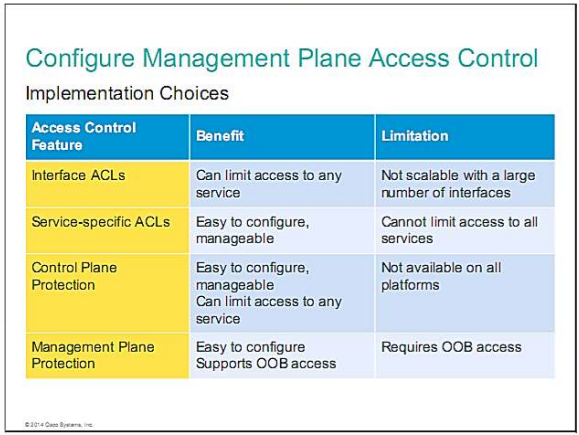
The MPP feature in Cisco IOS Software enables you to restrict the interface (or interfaces) on which network management packets are allowed to enter a device. With the MPP feature, you can designate one or more router interfaces as management interfaces. Device management traffic is permitted to enter a device only through these management interfaces. After you enable MPP, no interfaces except designated management interfaces accept network management traffic that is destined to the device.

When you configure a management interface, all incoming packets through that interface are dropped except for those from the allowed management protocols. This configuration also drops packets on all interfaces from all of the remaining management protocols (supported in the MPP feature), including the interface that you configured. The allowed management protocols are dropped by all other interfaces unless the same protocol is enabled on those interfaces.

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

Configure Cisco IOS Secure Management Access

This topic describes how to configure secure management access on the Cisco IOS devices.



Because there are multiple methods of management access control, you will typically choose one or more methods in your environment. Using more than one method provides defense in depth, which may come in handy if vulnerabilities are found in one of the configured methods, or if you accidentally misconfigure a chosen method:

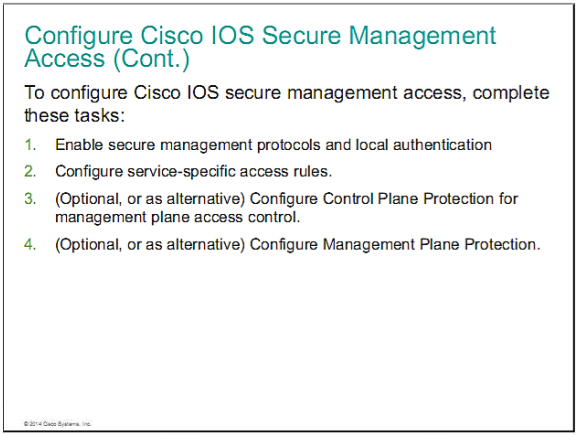
This table shows the benefits and limitations of the previously discussed management access methods. Interface ACLs are flexible, because they can limit access to any local management service. They are not manageable on devices with many interfaces, because they have to be applied on every device interface.

Service-specific ACLs are easy to configure and manage, but may not be available for all Cisco IOS Software management processes.

Control Plane Protection is easy to configure because of its centralized nature, which is flexible. It can limit access to any local management service, and it is generally recommended as a replacement for interface ACLs to limit access to the management plane. The only downside is that Control Plane Protection is not available on all Cisco hardware platforms.

MPP is very easy to configure, and it easily supports OOB management networks. Its main downside is that it requires a network that subscribes to the concept of OOB management access. MPP cannot work in in-band management environments in which management traffic is forwarded along the same paths as user traffic.

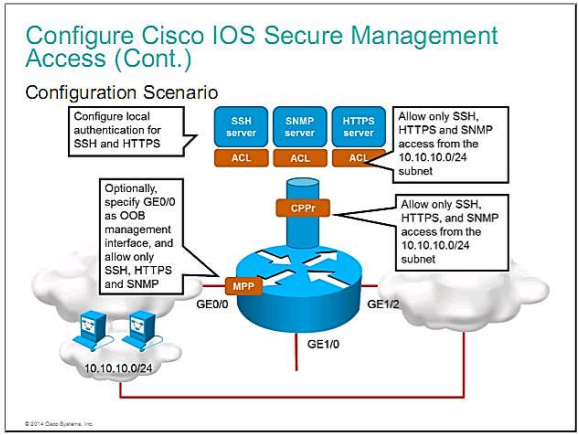
https://t.me/learningnets



When implementing management plane access control, you will typically complete one or more of the following configuration tasks, depending on the feature that you decide to use:

1. Enable use of secure management protocols (SSHv2, HTTPS) and enable local authentication
2. It is recommended that you always deploy service-specific access rules to specify the management sources that can access a specific Cisco IOS Software management process.
3. Optionally, or alternatively, you can use Control Plane Protection to limit access to management processes using a simple, centralized policy.
4. Optionally, or alternatively, you can also configure MPP, if your network design allows you to dedicate a local interface to management traffic.

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



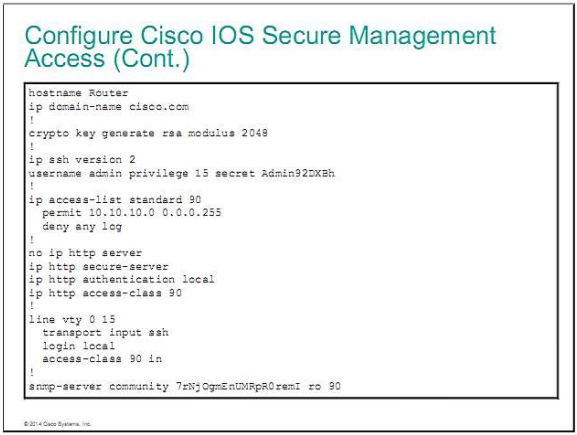
This figure shows the configuration scenario that is used in the upcoming configuration tasks. You will first enable use of SSHv2 and HTTPS protocols on a Cisco IOS router and configure it with service-specific ACLs that limit access to the SSH server, HTTPS server, and the SNMP server to hosts in the 10.10.10.0/24 subnet. You will also enable local authentication for HTTPS and SSH to enable users to log when accessing the router using HTTPS or SSH.

Then, as an additional layer of control, you will also configure Control Plane Protection to allow SSH, HTTPS, and SNMP access from hosts in the 10.10.10.0/24 subnet.

Finally, you will configure the GigabitEthernet0/0 interface as the dedicated management interface using MPP. Note that you should only configure MPP if your network uses OOB management.

The configuration steps in this topic assume that the router has already been configured with all required IP connectivity and management processes.

https://t.me/learningnets



In the first task you will enable usage of secure management protocols. First specify hostname and domain name. Both are used to create a name for an RSA key pair which is created using the **crypto key generate rsa modulus** command. Then specify that SSH version 2 will be used using the **ip ssh version 2** command. Then create a local user with privilege leve 15 using the **username privilege 15 secret** command.

The following example shows how to configure RSA-based authentication for SSHv2 clients. The key string (public key) for a specified user has to be obtained from an SSH client and copied into the router:

```
ip ssh pubkey-chain
  username user
    key-string
      30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00D09587
      <output omitted>
```

Then enable HTTPS server using the **ip http secure-server** command and disable HTTP server using the **no ip http server** command. Enable local authentication for HTTPS access using the **ip http authentication local** command.

In the second task, you will configure service-specific ACLs that limit access to specific Cisco IOS Software management processes. Every Cisco IOS Software management process uses a different syntax for such access control.

Start by configuring a Cisco IOS Software standard ACL that permits traffic from the specified network of trusted management servers (the 10.10.10.0/24 subnet). Using a deny-all rule with logging at the end of the ACL—to audit all attempts to connect to the device from unauthorized sources—is recommended.

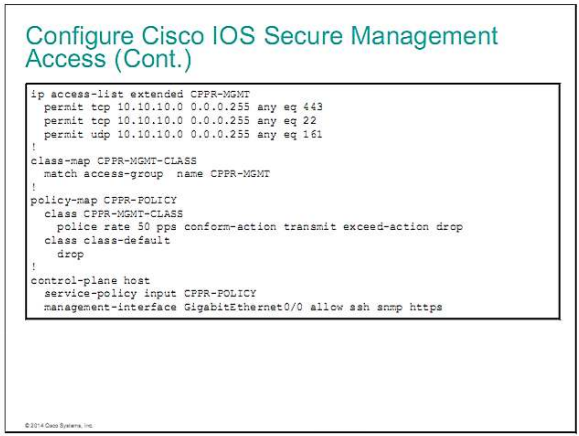
Next, use the **ip http access-class** command to allow access to the HTTPS server from only authorized sources. Then enter vty line configuration mode using the **line vty** command, enable only SSH access to vty lines using the **transport input ssh** command. Limit access to only authorized hosts using the **access-class** command. Use the **login local** command to enable local authentication for SSH access.

To limit SNMP access, specify the standard ACL as the last parameter of the **snmp-server community** command. This example limits access to the device for SNMP version 1 and 2 protocols. You will learn to limit access using the SNMPv3 protocol in a later topic of this lesson.

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

To configure secure management access a Cisco IOS device, use the commands that are described in the table.

Commands	Description
hostname Router **ip domain-name cisco.com**	Sets a hostname and domain name.
crypto key generate rsa modulus 2048	Creates an RSA key pair.
ip ssh version 2	Specifies that SSH version 2 will be used.
username admin privilege 15 secret Admin92DXBh	Creates local user account with privilege level 15.
ip access-list standard 90 **permit 10.10.10.0 0.0.0.255** **deny any log**	Creates a standard ACL.
no ip http server **ip http secure-server** **ip http authentication local** **ip http access-class 90**	Enables HTTPS server, specifies that only authorized hosts are allowed to access it, and enables local authentication.
line vty 0 15 **transport input ssh** **login local** **access-class 90 in**	Allows only SSH on VTY lines, specifies that only authorized hosts are allowed to access the SSH server, and enables local authentication.
snmp-server community 7rNjOgmEnUMRpR0reml ro 90	Limits SNMP access to the device.



In the third (optional or alternative) step, you will configure Control Plane Protection to limit access to the management plane. Because you have already learned to configure the Control Plane Protection feature to protect the control plane in an earlier lesson, you can employ the same configuration steps to protect the management plane as well.

https://t.me/learningnets

Start by defining an extended ACL and a class that describes allowed management traffic. The extended ACL in this example defines trusted management traffic as HTTPS, SNMP polling and SSH traffic from the 10.10.10.0/24 subnet.

Next, configure a policy map that references the configured class, and police the class to a rate that is not exceeded by legitimate traffic. To protect local resources, specify the exceed action as **drop** to prevent spoofed traffic from possibly overwhelming the device CPU. Also, configure the default class to drop all traffic, establishing a device firewall function on this device.

In the fourth (optional or alternative) task, you can configure a local interface as a dedicated management interface using MPP.

Enter the control plane virtual host subinterface, using the **control-plane host** command, and specify the dedicated management interface using the **management-interface** command. The command allows you to specify the individual protocols that are allowed on the interface, using the **allow** parameter. This example uses the **allow ssh snmp** parameters to only allow SSH and SNMP traffic on the dedicated management interface.

Note There may be other traffic types that you need to permit in the Control Plane Protection policy map, such as routing protocols and ICMP diagnostic traffic. Ensure that you permit all required traffic and test your configuration before production use.

Finally, apply the policy map to the control plane host virtual subinterface using the **service-policy input** command.

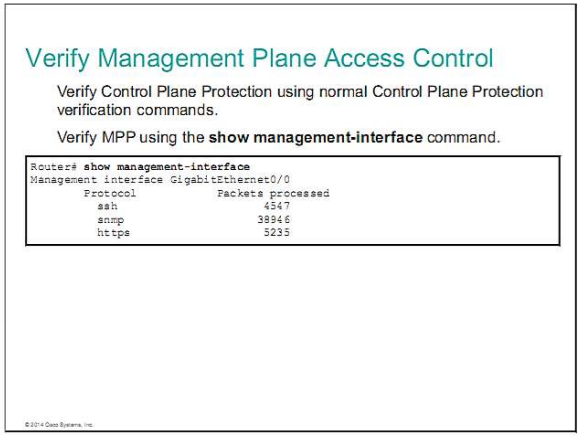
To configure secure management access a Cisco IOS device, use the commands that are described in the table.

Commands	Description
ip access-list extended CPPR-MGMT **permit tcp 10.10.10.0 0.0.0.255 any eq 443** **permit tcp 10.10.10.0 0.0.0.255 any eq 22** **permit udp 10.10.10.0 0.0.0.255 any eq 161**	Creates an extended ACL
class-map CPPR-MGMT-CLASS **match access-group name CPPR-MGMT**	Creates a class map that refers to the ACL
policy-map CPPR-POLICY **class CPPR-MGMT-CLASS** **police rate 50 pps conform-action transmit exceed-action drop** **class class-default** **drop**	Creates a policy map that refers to the class map and polices the allowed traffic and denies everything else
control-plane host **service-policy input CPPR-POLICY** **management-interface GigabitEthernet0/0 allow ssh snmp https**	Applies the policy map the host control plane subinterface. MPP also enables GigabitEthernet0/0 interface as OOB interface and allows only SSH, SNMP, and HTTPS traffic to rach the router through the interface.

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

Verify Cisco IOS Secure Management Access

This topic describes how to verify secure management access on the Cisco IOS devices.



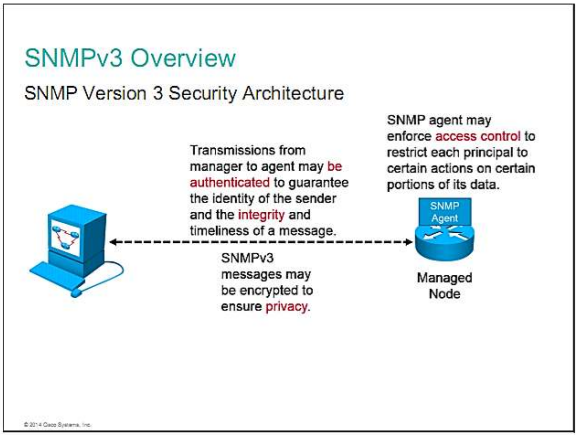
To verify MPP and view information about the configured dedicated management interfaces, including the type of interface, the protocols that are enabled on the interface, and the number of packets that are processed, use the **show management-interface** command in privileged EXEC mode. The **show management-interface** command allows you to view all of the management interface configurations and activity on a device and to filter the output by interface or protocol.

To verify Control Plane Protection functionality, use the same verification commands that you would use to verify normal Control Plane Protection configuration and operation.

https://t.me/learningnets

SNMPv3 Overview

This topic describes SNMPv3.



SNMPv3 is an interoperable, standards-based protocol for network management. SNMPv3 uses optional cryptographic methods to provide these security features:

Message integrity: Ensures that each SNMPv3 message has not been tampered with in transit.

Authentication: Determines that the SNMPv3 message is from a valid source. The SNMP agent on a managed device can use authentication information to control access to its SNMP-manageable functions.

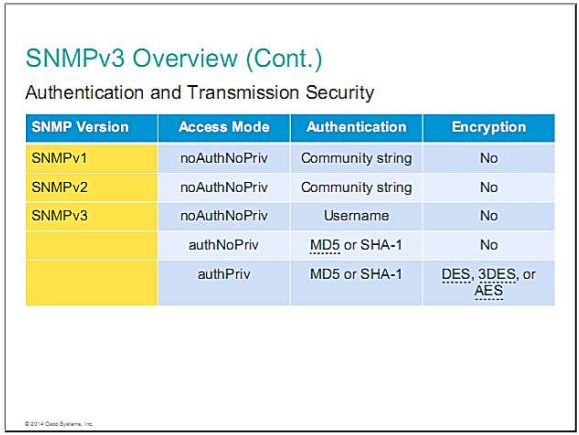
Encryption: Scrambles the content of an SNMPv3 message to prevent it from being seen by an unauthorized source.

In SNMPv3, each managed node and NMS is a single entity. There are two types of entities, each containing different applications:

Managed node SNMP entities: The managed node SNMP entity includes an SNMP agent and an SNMP MIB. The agent implements the SNMP protocol and allows a managed node to provide information to the NMS and accept instructions from it. The MIB defines the information that can be collected and used to control the managed node. Information exchanged using SNMP takes the form of objects from the MIB.

SNMP NMS entities: The SNMP entity on an NMS includes an SNMP manager and SNMP applications. The manager implements the SNMP protocol, collects information from managed nodes, and sends instructions to managed nodes. The SNMP applications are software applications that are used to manage the network.

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



Currently, Cisco IOS Software supports different security models in SNMPv1, SNMPv2, and SNMPv3. The SNMP security level defines the cryptographic security services that are applied to an SNMP session. There are three security SNMP levels:

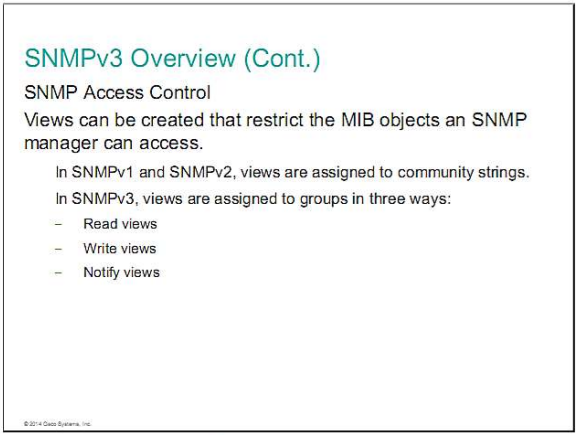
noAuth: Authenticates SNMP messages using a username or community string

Auth: Authenticates SNMP messages using either HMAC with MD5 (RFC 2104) or SHA-1

Priv: Authenticates SNMP messages by using either HMAC-MD5 or SHA. Encrypts SNMP messages using DES, 3DES, or AES.

SNMPv3 provides all three security level options. The figure identifies the combinations of security models and levels available in respective SNMP versions.

https://t.me/learningnets



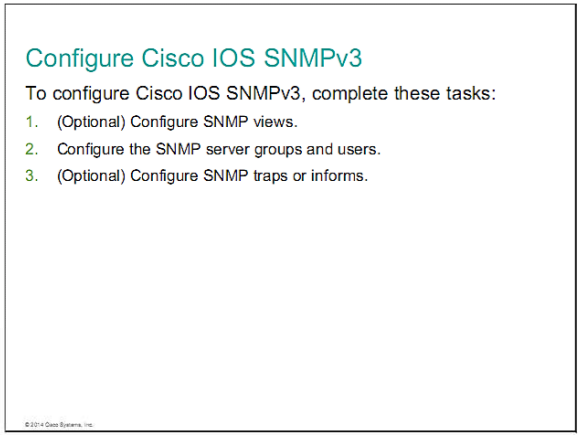
In addition to authenticating access to the MIB of a device and providing optional transmission security, SNMP agents can also limit access to their MIB based on remote SNMP client (NMS) identity. With SNMPv1 and SNMPv2, you can assign views to community strings to limit which MIB objects an SNMP manager can access. You can use a predefined view or create your own view. SNMPv3 uses views to restrict access to MIB objects in a similar manner. The views are defined as part of the group settings for read, write, or notify purposes.

Note	The configuration of views is optional in all versions of SNMP.

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

Configure Cisco IOS SNMPv3

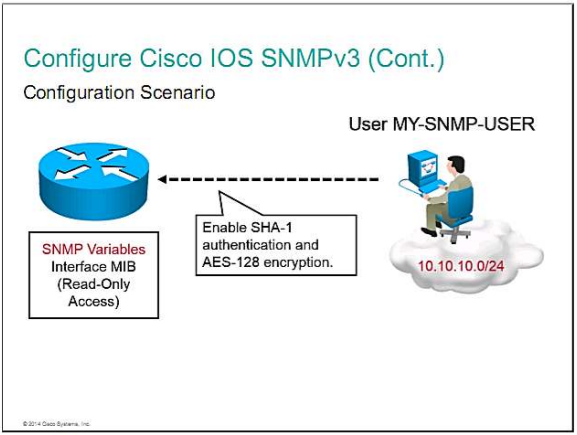
This topic describes how to configure SNMPv3 on the Cisco IOS devices.



When configuring SNMPv3 security features on Cisco IOS Software, you will typically complete the following *optional* tasks:

1. Configure SNMP views to restrict the NMS to only the required section of the MIB of the device.
2. Configure SNMP users and groups that will define transmission security, authentication, and access control parameters for individual management users (NMS systems).
3. Configure security features that are applied to SNMP traps and informs.

https://t.me/learningnets

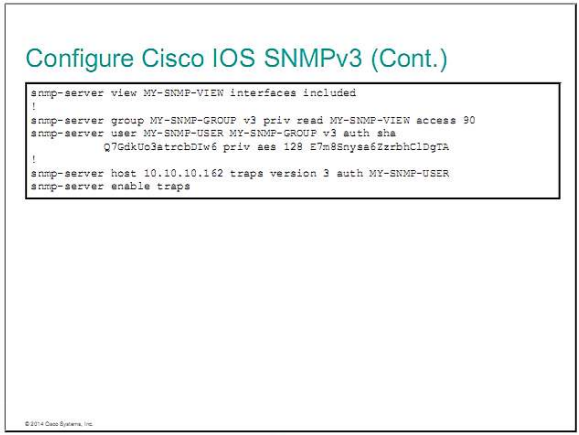


This figure shows the configuration scenario that is used in the upcoming tasks. You will configure a Cisco IOS Software router with SNMPv3 security features that will allow only the following:

- SNMP access from the 10.10.10.0/24 network
- Read-only access to the SNMP interface parameters MIB
- Authentication of all SNMPv3 messages using SHA-1 authentication
- Encryption of the messages using 128-bit AES encryption

The configuration steps in this topic assume that the router has already been configured with all required IP connectivity and nonsecurity-related SNMP functionality.

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



In the first task, you will optionally configure SNMP views to restrict access to the MIB of the local device. In this example, you will configure an SNMP view that restricts access only to the interface parameters MIB.

Use the **snmp-server view** command to create a named SNMP view, and specify the included MIB family ("**interfaces**" in this example) using the **included** parameter. Configuring a view does not yet filter access to the MIB. You will need to associate this view with an SNMP user group for it to take effect.

In the second configuration task, create SNMP groups and users to specify authentication and authorization rules for MIB access.

Start by defining a named (MY-SNMP-GROUP) SNMP group using the **snmp-server group** command. Inside the group definition, do the following:

Specify the **v3** SNMP protocol version.

Specify that this group must use the **priv** (authentication and encryption) security level.

Allow only read access to a subset of the MIB using the **read** argument, referencing the configured SNMP view.

Specify that the standard ACL 90 will limit access to specific IP addresses.

Note The standard ACL 90, used in previous topics, only permits access from the 10.10.10.0/24 subnet.

Next, configure a specific named (MY-SNMP-USER) SNMP user employing the **snmp-server user** command, and assign the user into the previously configured MY-SNMP-GROUP group. Specify that the user is limited to the **v3** SNMP protocol version. Using the **auth sha** and **priv aes** command, specify the authentication and encryption keys for the SHA-1 and 128-bit AES algorithms.

In the third, optional task, yon also apply SNMPv3 security features to SNMP traps and informs, which are notifications that are sent asynchronously from the device to the NMS. Traps and informs are authenticated and encrypted using the same methods as other SNMPv3 messages, and they are associated with a particular user to obtain the correct authentication and encryption keys.

https://t.me/learningnets

To configure SNMPv3-secured traps, extend the **snmp-server host traps** command with the **version 3 priv** parameter, specifying the configured SNMP username (MY-SNMP-USER) to determine the authentication and encryption keys that are used to protect traps. Use the **informs** parameter instead of **traps** to configure SNMPv3-secured informs. Finally, globally enable SNMP traps using the **snmp-server enable traps** command.

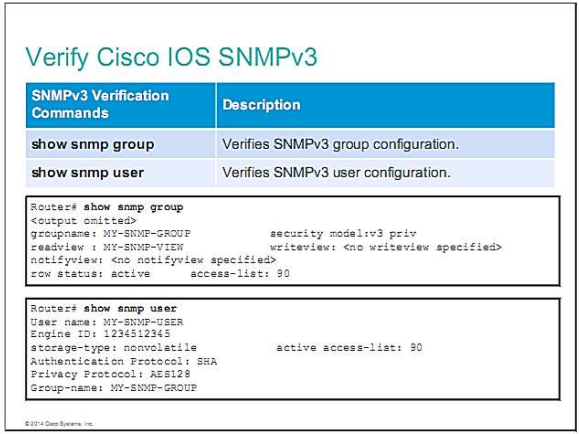
To configure SNMPv3 on a Cisco IOS device, use the commands that are described in the table.

Commands	Description
snmp-server view MY-SNMP-VIEW interfaces included	Creates a named SNMP view
snmp-server group MY-SNMP-GROUP v3 priv read MY-SNMP-VIEW access 90 **snmp-server user MY-SNMP-USER MY-SNMP-GROUP v3 auth sha Q7GdkUo3atrcbDlw6 priv aes 128 E7m8Snysa6ZzrbhClDgTA**	Creates SNMPv3 group and with authentication and encryption security level and read only access. Creates a SNMPv3 user and specifies encryption and authentication keys.
snmp-server host 10.10.10.162 traps version 3 auth MY-SNMP-USER **snmp-server enable traps**	Enables sending of protected SNMPv3 traps to a NMS.

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

Verify Cisco IOS SNMPv3

This topic describes how to verify SNMPv3 on the Cisco IOS devices.

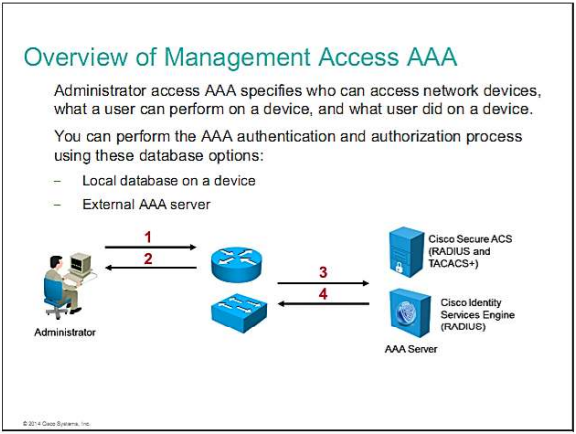


To verify your SNMPv3 group and user configuration, use the **show snmp group** and **show snmp user** commands respectively.

https://t.me/learningnets

Overview of Management Access AAA

This topic describes management access AAA.



Access control is the way you can control who is allowed to have access to a networking device and what services users are allowed to use after they have access. AAA network security services provide the primary framework that you use to set up access control on your networking devices.

AAA servers are typically used as a central repository of authentication credentials, authorization rules, and accounting logs (in other words, who can access the device, what they are authorized to do, and what they accomplished).

AAA is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing the following services:

Authentication: Provides a method to identify users before they are allowed to have access to the network and network services.

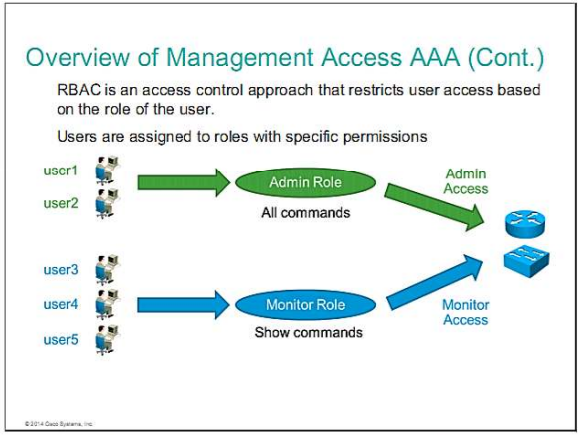
Authorization: Provides a set of attributes that describe what a given user is authorized to perform. These attributes are compared to user information in a database and returned to AAA, which determines the user's actual capabilities and restrictions. The database is located locally on the networking device or hosted remotely on a security server, such as RADIUS, TACACS+, LDAP, or Microsoft Active Directory. Remote security servers authorize users for specific rights by associating attributes that define those rights. In case of TACACS+, these attributes can be commands that are allowed for an user to be executed.

Accounting: Provides the method to collect and send security server information that is used for billing, auditing, and reporting. Accounting enables you to track the services that users access and the network resources that they consume. When AAA accounting is activated, the network access server reports user activity to the RADIUS or TACACS+ security server.

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

You perform AAA authentication and authorization using either a local database on the networking device itself or using an external AAA server. The figure illustrates the AAA process using an external AAA server, such as Cisco Identity Services Engine or Cisco Secure Access Control Server. The process consists of these steps:

1. The client establishes a connection with the networking device.
2. The networking device prompts the user for a username and password.
3. The device passes the username and password to the AAA server.
4. The AAA server authenticates the user. The user is authorized to access the networking device based on information in the AAA server authorization database.



Another way to control administrative access to networking devices is called RBAC. RBAC is an access control approach that restricts user access based on the role of the user, along with the user's individual identity. Roles are created for job or task functions and are assigned access permissions to specific assets. Users are then assigned to roles, which gives them the permissions that are defined for the role. The assignment means that users are not assigned permissions directly; users acquire permissions only through role assignment. Assigning appropriate roles to an individual user is a simple way to manage the rights of the user.

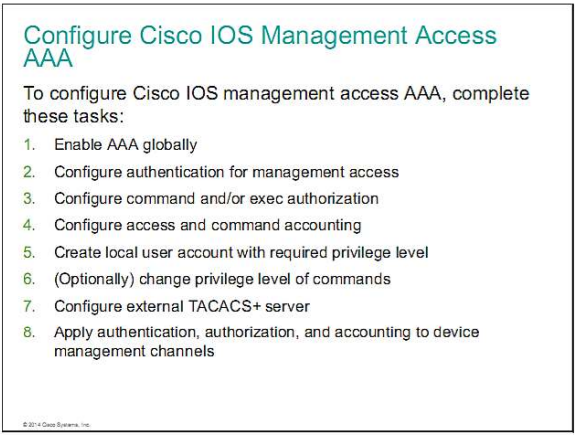
To ensure scalability, users, permissions, and roles are usually created and maintained in a central repository, which makes the access control policy available to multiple devices that are using the policy.

Note TACACS+ is usually used to perform AAA for management access because it supports command authorization and thus simplifies deployment of RBAC.

https://t.me/learningnets

Configure Cisco IOS Management Access AAA

This topic describes how to configure management access AAA on the Cisco IOS Software.

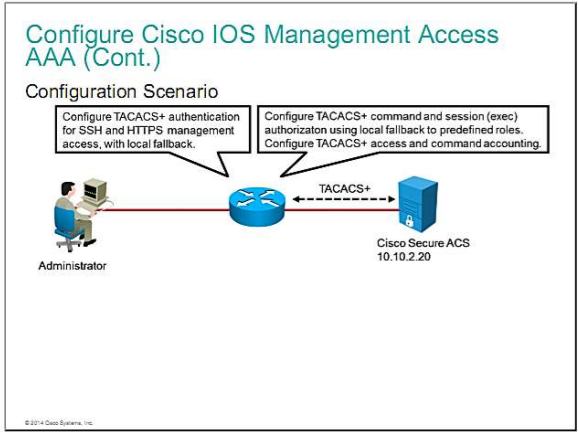


When configuring AAA for management access on Cisco IOS Software, you will typically complete the following tasks:

1. Enable AAA globally on a router or on a switch
2. Create authentication method list to configure authentication for management access
3. Create command or exec authorization method list to configure command or exec authorization for management access
4. Create access and command accounting method list to configure access or command accounting for management access
5. Create local user account with required privilege level
6. (Optionally) change privilege level of commands to enable users with predefined privilege levels to execure specific commands
7. Configure external TACACS+ server
8. Apply authentication, authorization, and accounting method lists to device management channels, such as VTY lines for Telnet or SSH access.

Note Configuration of the TACACS+ server is not shown in this course.

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

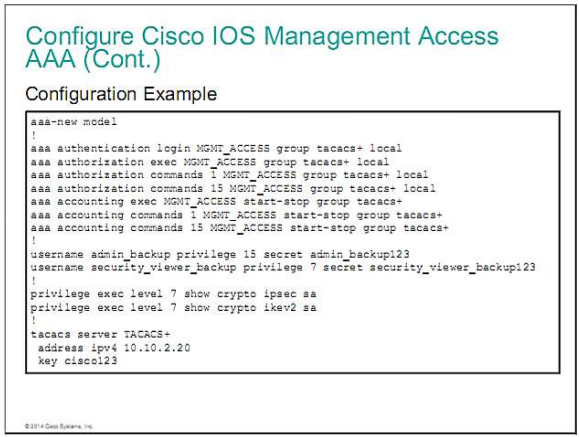


This figure shows the configuration scenario that is used in the upcoming tasks. You will configure a Cisco IOS Software router for management access AAA using TACACS+ server:

You will configure TACACS+ authentication for SSH and HTTPS management access. You will use the local user database on the router as fallback mechanism in case the TACACS+ server fails.

You will also configure TACACS+ command and exec authorization for management sessions. You will backup command authorization using local command authorization using privilege levels of commands and local users.

Finally, you will enable TACACS+ commands and exec access accounting.



https://t.me/learningnets

In the first task you have to enable the AAA functionality using the **aaa-new model** command.

In the second task you will create authentication method list for login attempts against TACACS+ external server using the **aaa authentication login MGMT_ACCESS group tacacs+ local** command. The method list is named as MGMT_ACCESS list. The command specifies that if the TACACS+ servers are not reachable, the local database will be used to authenticate users.

Then you will enable authorization for exec access and authorization of commands. Authorization of exec access governs general management access to a device, while command authorization authorizes each command a user enters on the device. Authorization of exec access is enabled using **aaa authorization exec MGMT_ACCESS group tacacs+ local** command. Authorization of commands is configured using the **aaa authorization commands 1 MGMT_ACCESS group tacacs+ local** command, and have to be enabled separately for each required privilege level. In the example, authorization is configured for level 1 and 15 privilege level.

Note The privilege levels range from 0 to 15. By default, commands are assigned either level 1 or level 15. Those commands that are executed in privileged EXEC mode are level 15 commands. With few exceptions, commands that can be executed in the user EXEC mode are level 1 command. A small number of commands are level 0 commands. These commands include **enable, disable, exit, logout**, and **help**.

In the fourth task you will enable accounting of exec access using the **aaa accounting exec MGMT_ACCESS start-stop group tacacs+** command. Accounting of commands is configured using the **aaa accounting commands 1 MGMT_ACCESS start-stop group tacacs+** command, and has to be enabled for each privilege level separately. In the example, accounting of commands is configured for level 1 and 15.

In the fifth task you will create two users in the local user database using the **username privilege secret** command. These users are created for backup, if the external TACACS+ server is not available. Two users are created, one with privilege level 15 and one with 1.

Next, you will change privilege level of two commands in order to enable the security_viewer_backup user to use these two commands. Recall that the user has a privilege level of 7 and most of the commands have the privilege level of 15 by default. Such user can only execute commands of privilege level 7 and lower. In the example, privilege level of **show crypto ipsec sa and show crypto ikev2 sa** commands is decreased to 7.

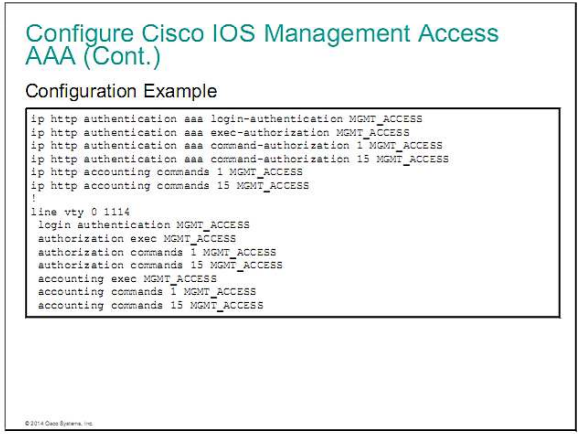
In task six, you will first enter the TACACS+ server configuration mode using the **tacacs server TACACS** + command. Then you will configure external TACACS+ server IP address using the using the **address ipv4 10.10.2.20** command, and preshared key using the **key cisco123** command.

To configure management access AAA on a Cisco router, use the commands that are described in this table:

Commands	Description
aaa-new model	Enables AAA functionality globally.
aaa authentication login MGMT_ACCESS group tacacs+ local	Creates authentication login method list that uses TACACS+ and local database as backup.
aaa authorization exec MGMT_ACCESS group tacacs + local	Creates authorization exec method list that uses TACACS+ and local database as backup.
aaa authorization commands 1 MGMT_ACCESS group tacacs+ local **aaa authorization commands 15 MGMT_ACCESS group tacacs+ local**	Creates authorization method lists that use TACACS+ and local database as backup. Authorization is configured for level 1 and 15 commands.

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

Commands	Description
aaa accounting exec MGMT_ACCESS start-stop group tacacs+	Creates accounting exec method list that uses TACACS +.
aaa accounting commands 1 MGMT_ACCESS start-stop group tacacs+ **aaa accounting commands 15 MGMT_ACCESS start-stop group tacacs+**	Creates accounting method lists that use TACACS+ . Accounting is configured for level 1 and 15 commands.
username admin_backup privilege 15 secret admin_backup123 **username security_viewer_backup privilege 7 secret security_viewer_backup123**	Creates two local users with privilege level 7 and 15.
privilege exec level 7 show crypto ipsec sa **privilege exec level 7 show crypto ikev2 sa**	Changes privilege level of two commands from 15 to 7.
tacacs server TACaCS **address ipv4 10.10.2.20** **key cisco123**	Configures TACACS+ server IP addresses and preshared key.



In the last task, you will apply configured authentication, authorization, and accounting method lists to required management channels. In the example, AAA is applied to the HTTP server and to the SSH server.

To configure management access AAA on a Cisco router, use the commands that are described in this table:

https://t.me/learningnets

Commands	Description
ip http authentication aaa login-authentication MGMT_ACCESS **ip http authentication aaa exec-authorization MGMT_ACCESS** **ip http authentication aaa command-authorization 1 MGMT_ACCESS** **ip http authentication aaa command-authorization 15 MGMT_ACCESS** **ip http accounting commands 1 MGMT_ACCESS** **ip http accounting commands 15 MGMT_ACCESS**	Applies authentication, authorization, and accounting method lists to the HTTP(S) server.
line vty 0 1114 **login authentication MGMT_ACCESS** **authorization exec MGMT_ACCESS** **authorization commands 1 MGMT_ACCESS** **authorization commands 15 MGMT_ACCESS** **accounting exec MGMT_ACCESS** **accounting commands 1 MGMT_ACCESS** **accounting commands 15 MGMT_ACCESS**	Applies authentication, authorization, and accounting method lists to the TELNET and SSH server.

Note Configuration of AAA against a RADIUS server is similar, but it does not support remote command authorization and accounting. However, you can configure the RADIUS server to send a privilege level of a user to a network device, and then implement command authorization locally, by changing privilege level of specific commands.

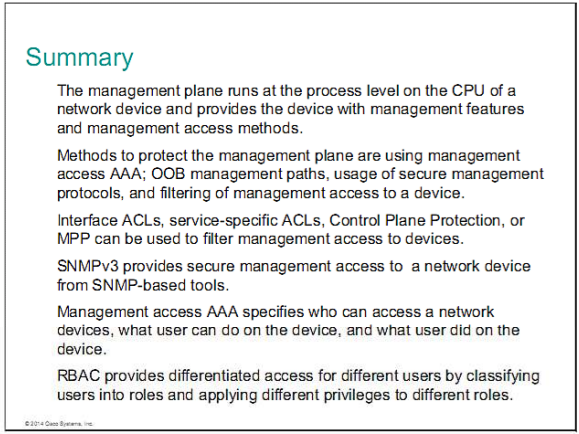
The following example shows configuration of AAA for SSH and Telnet access against a RADIUS server:

```
aaa-new model
!
aaa authentication login MGMT_ACCESS group radius local
aaa authorization exec MGMT_ACCESS group radius local
aaa accounting exec MGMT_ACCESS start-stop group radius
!
username admin_backup privilege 15 secret admin_backup123
username security_viewer_backup privilege 7 secret security_viewer_backup123
!
privilege exec level 7 show crypto ipsec sa
privilege exec level 7 show crypto ikev2 sa
!
radius server RADIUS
 address ipv4 10.10.2.20 auth-port 1645 acct-port 1646
 key cisco123
!
line vty 0 1114
 login authentication MGMT_ACCESS
 authorization exec MGMT_ACCESS
 accounting exec MGMT_ACCESS
```


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

Summary

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



https://t.me/learningnets

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

Lesson 4

Deploying Cisco ASA Management Plane Security Controls

Overview

Similarly as Cisco IOS Software devices, you can access the Cisco Adaptive Security Appliance 5500-X management interface locally, using the console connection, or you can access it remotely over an IP network. Configuring remote management access in a secure fashion is of paramount importance to ensure the integrity of the adaptive security appliance in a possibly hostile environment, such as when management paths use an untrusted network.

This lesson describes how to configure remote management access to the adaptive security appliance, and how to configure and use management access AAA features.

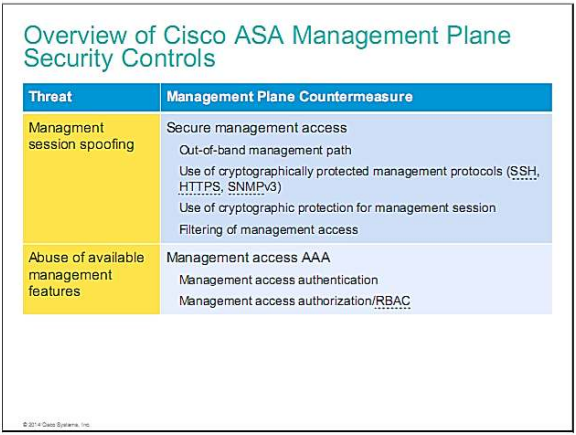
Upon completing this lesson you will be able to:

- Describe Cisco ASA management plane security controls
- Describe different ways how to secure management access to Cisco ASA devices
- Configure secure management access on the Cisco ASA devices
- Describe management access AAA on the Cisco ASA
- Configure management access AAA on the Cisco ASA
- Verify management access AAA on the Cisco ASA

https://t.me/learningnets

Overview of Cisco ASA Management Plane Security Controls

This topic describes Cisco Adaptive Security Appliance management plane security controls.



Similarly as on the Cisco IOS Software devices, the management plane of the Cisco ASA is susceptible to two major threat classes:

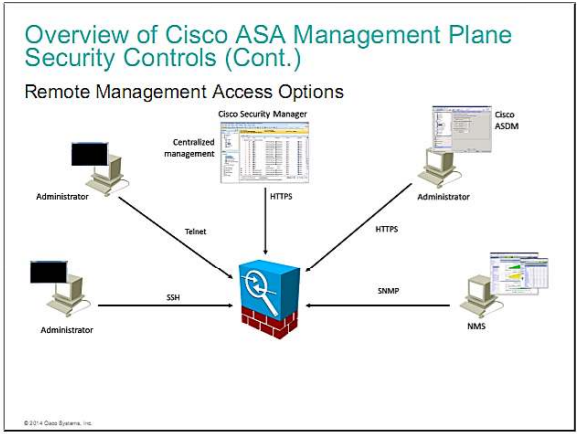
Spoofing of management sessions, in which attackers hijack existing sessions, steal administrator credentials, or spoof the legitimate IP addresses of administrators to gain management access to a device. You can reduce these risks by using out-of band management paths, or by using cryptographically protected management protocols or cryptographically protected management sessions and by tightly filtering access to devices to allow access from only specific networks, if routing in your network is trusted and IP spoofing is unlikely.

Attacker and rogue administrator abuse of management features, in which authenticated users act maliciously, or beyond their authorized profiles, to change the behavior of a network device in an undesirable manner. To reduce these risks, you can deploy strong authentication to prevent identity theft and RBAC restrictions to limit access to specific management features.

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

Overview of Cisco ASA Secure Management Access

This topic describes different ways how to secure management access to Cisco Adaptive Security Appliance devices.



The Cisco ASA 5500-X Series Next-Generation Firewalls provide four main remote access protocols to access the adaptive security appliance management functions:

Telnet: A cleartext terminal, CLI access protocol that authenticates access to the appliance based on the IP address. Its strength is determined by the resistance of the intermediate network path to IP spoofing. Telnet authenticates administrators to the adaptive security appliance based on passwords or OTPs. The Telnet protocol should not be used over untrusted networks and is generally considered obsolete for security device management.

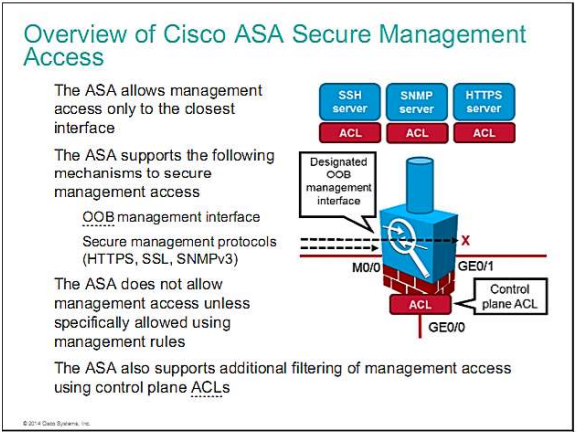
SSH: A strongly encrypted and strongly authenticated protocol that allows CLI access to the ASA. SSH protocols authenticate the ASA to the administrator using public-key-based authentication, and authenticate administrators to the adaptive security appliance using passwords or OTPs in the ASA implementation. This protocol can be used over untrusted networks, if appropriate care is taken when managing the adaptive security appliance public key (that is, not blindly accepting it over an untrusted network, but having a preprovisioned authentic copy that is already stored on the client system).

HTTPS (HTTP over SSL/TLS): A strongly encrypted and strongly authenticated protocol that allows GUI and file copy access to the adaptive security appliance, within Cisco Adaptive Security Device Manager. The HTTPS protocol authenticates the adaptive security appliance using public-key-based authentication (in the form of X.509 certificates), and administrators using passwords, OTPs, or client certificates in the ASA implementation. The HTTPS protocol can be used over untrusted networks, if appropriate care is taken when managing the adaptive security appliance public key (certificate) in the same manner as with SSH.

https://t.me/learningnets

SNMP: As opposed to Cisco IOS Software devices, this protocol only allows monitoring of Cisco ASA parameters for performance and health monitoring, and asynchronous logging of system events (via SNMP traps). The Cisco ASA SNMP server implementation supports all versions of the protocol (1, 2c, and 3). SNMP version 1 and 2c use cleartext authentication and transmission and are therefore not suitable for use over untrusted networks. SNMP version 3 uses strong cryptographic authentication and transmission protection, and therefore can be deployed over untrusted network paths.

You can also integrate the Cisco ASA with centralized management tools, such as Cisco Security Manager. The Cisco Security Manager is a centralized policy provisioning tool that provisions configurations and policy to many security devices, including ASA 5500-X Series Next-Generation Firewalls. To integrate the ASA with Cisco Security Manager, you have to enable HTTPS access on the ASA.



The Cisco ASA 5500-X Series Next-Generation Firewalls are security devices and support secure remote management features by design:

Management access to an interface other than the one from which you entered the ASA is not supported. For example, if your management host is located on the inside interface, you can only initiate a management connection directly to the inside interface. The only exception to this rule is through a VPN connection.

The ASA family supports at least one dedicated management interface which cannot be used for user traffic. However, management traffic to the management has to explicitly allowed as described in a later paragraph.

The ASA supports secure management protocols, such as SSH, HTTPS, or SNMPv3. Telnet protocol is also supported, but cannot be used on an interface with the lowest security level. Generally, use of Telnet is discouraged, and should be only used over a secure network or cryptographically protected VPN connection.

The ASA does not allow remote management access to any interface by default. Remote management access has to be explicitly enabled using management rules for each protocol on any interface, by specifying IP address of a management host, and incoming interface.

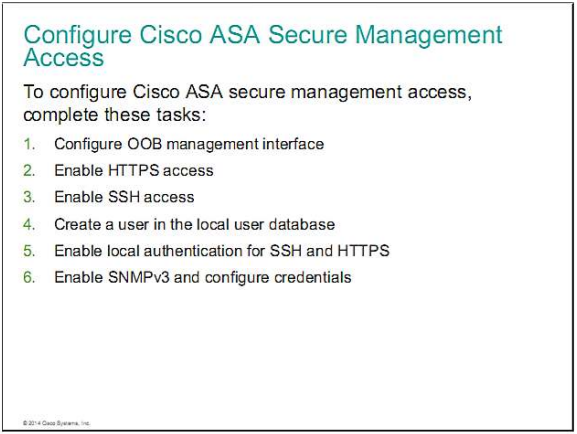
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

The ASA has no control plane protection or policing mechanisms like Cisco IOS Software. However, if you want to filter traffic that is terminated on the ASA, you can use interface ACLs with additional **control-plane** keyword in the command. The command specifies whether or not the ACL rule is for to-the-box traffic. Management rules for management traffic have higher precedence that an ACL applied to the control plane. Therefore, such permitted traffic will be allowed to come in even if explicitly denied by the control plane ACL.

https://t.me/learningnets

Configure Cisco ASA Secure Management Access

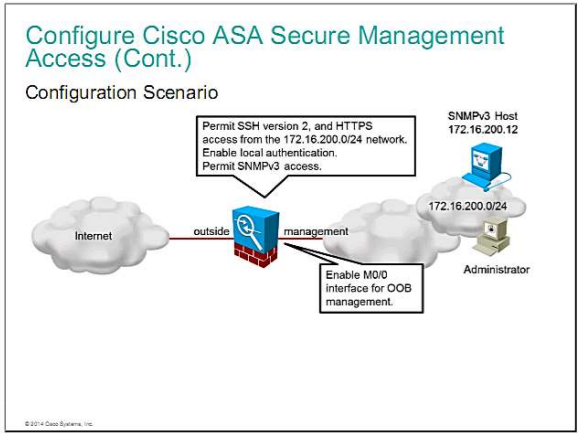
This topic describes how to configure secure management access on the Cisco Adaptive Security Appliance devices.



When implementing secure management access to the Cisco ASA, you will typically complete one or more of the following configuration tasks, depending on the feature that you decide to use:

1. You can create the built-in OOB management network interface that will be used only to accept management sessions. This step is optional and is used only when you are using an OOB management network.
2. You can choose to allow HTTPS access to the appliance to use the Cisco Adaptive Security Device Manager GUI. This step is optional and is required only if you require access to Cisco ASDM. HTTPS access to the appliance is disabled if the appliance has an empty configuration, but is enabled with a factory-default configuration or as a consequence of the initial setup dialog.
3. You can choose to allow SSH access to the appliance to use its CLI features over a secure session. This step is optional and is required only if you require SSH access. SSH access to the appliance is disabled by default.
4. Before enabling local authentication for SSH and HTTPS access, you have to create a local admin user in the local user database.
5. You can choose to enable local authentication for SSH and HTTP access.
6. You can choose to allow SNMP access to the appliance and to send SNMP traps from the appliance to a NMS. This step is optional and is required only if you require SNMP support. SNMP access to the appliance and the sending of SNMP traps are disabled by default.

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



The figure shows the configuration scenario that is used in the upcoming tasks. You will configure the Cisco ASA 5500-X with the following management access options:

You will configure the Management0/0 interface for OOB management access. You will configure this using console access, since the configuration scenario assumes that you do not have the Cisco ASDM access yet.

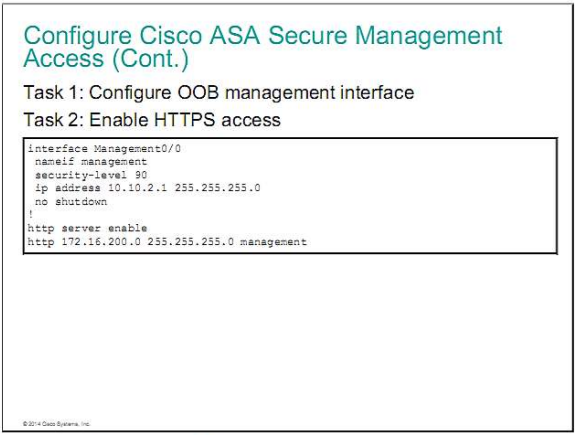
You will permit HTTPS management access from the 172.16.200.0/24 network to the management interface to allow Cisco ASDM access. You will configure this using console access, since the configuration scenario assumes that you do not have the Cisco ASDM access yet. All the subsequent steps can be configured using Cisco ASDM.

You will permit SSH management access from the 172.16.200.0/24 network to the management interface.

You will enable local authentication using local user database for SSH and HTTPS management access. HTTPS management access can work without authentication (you can log in using empty username and password if authentiacation is not enabled), but authentication for SSH access is mandatory.

You will permit SNMPv3 access with cryptographic access authentication from the 172.16.200.12 host.

https://t.me/learningnets



In the first task you will configure the Maangement0/0 interface for OOB management access. The Management0/0 interface has no support for through traffic and has no support for subinterfaces. First assign a name to the interface using the **nameif** command. Then assign a security level to the interface using the **security-level** command. Assign an IP address to the interface using the **ip address** command. Finally, enable the interface using the **no shutdown** command. The Management0/0 interface is configured for **management-only** traffic by default, and you cannot disable **management-only** for the Management interface.

In the second task, enable the HTTPS server using the **http server enable** command. Then, create a management rule using the **http 172.16.200.0 255.255.255.0 management** command to enable HTTPS command from the specified subnet through the specified interface.

To configure secure management access on the Cisco ASA device, use the commands that are described in the table.

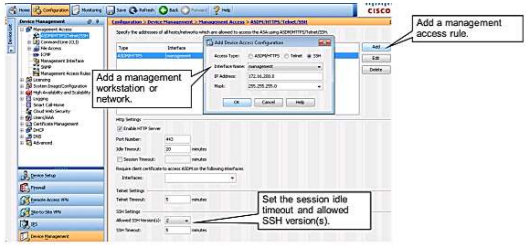
Commands	Description
interface Management0/0 **nameif management** **security-level 90** **ip address 10.10.2.1 255.255.255.0** **no shutdown**	Configures the interface with name, security level, and IP address.
http server enable **http 172.16.200.0 255.255.255.0 management**	Enables HTTPS server.

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

Configure Cisco ASA Secure Management Access (Cont.)

Task 3: Enable SSH access

Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH



SSH provides another option for remote management of the Cisco ASA. You can define specific hosts or networks that are authorized to initiate an SSH connection to the ASA, as well as how long a session can remain idle before being disconnected.

To authorize SSH access to the ASA from specific network sources, complete the following steps:

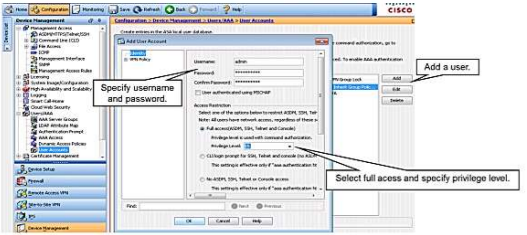
1. Click the **Configuration** button in the Cisco ASDM toolbar.
2. Choose **Device Management** from the navigation pane.
3. Expand the **Management Access** option from the Device Management menu.
4. Click the **ASDM/HTTPS/Telnet/SSH** option in the menu. The ASDM/HTTPS/Telnet/SSH panel is displayed.
5. Click **Add** to create an SSH access rule.
6. In the Add Device Access Configuration window, choose **SSH** as the access type, and specify the IP address, mask, and incoming interface for the allowed SSH management session. This example allows access from hosts in the 172.16.200.0/24 network reachable over the management interface.
7. Click **OK** when done.
8. To specify the allowed versions of the SSH Protocol, choose the versions from the Allowed SSH Version(s) drop-down box. It is strongly recommended to allow only SSH version 2.
9. To set the maximum time, in minutes, that a console SSH session can be idle before being logged off by the adaptive security appliance, enter a value from 1 to 60 in the SSH Timeout field. By default, SSH sessions left idle for five minutes are closed by the adaptive security appliance. In the example, SSH idle timeout is set to 5 minutes.
10. Click **Apply** to apply the configuration.

https://t.me/learningnets

Configure Cisco ASA Secure Management Access (Cont.)

Task 4: Create a user in the local user database

Configuration > Device Management > Users/AAA > User Accounts



©2014 Cisco Systems, Inc.

Administrative access to the ASA supports multiple authentication methods, such as simple authentication using local users, or more advanced AAA methods. In this topic, the simplest method is shown, which is authentication using usernames and passwords in the local user database. Before enabling local authentication for HTTPS and SSH access, you have to create a user in the local user database.

To create a user in the ASA local user database, complete the following steps:

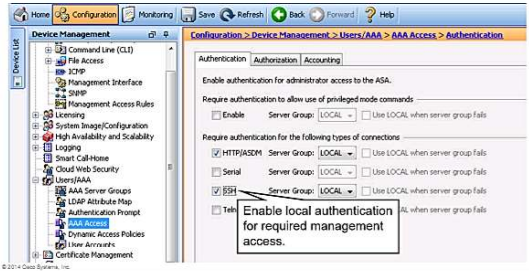
1. Click the **Configuration** button in the Cisco ASDM toolbar.
2. Choose **Device Management** from the navigation pane.
3. Expand the **Users/AAA** option from the Device Management menu.
4. Click the **User Accounts** option in the menu. The User Accounts panel is displayed.
5. Click **Add** to add a user.
6. In the Add User Account window, type the username and password into corresponding input fields. Then select **Full access (ASDM, SSH, Telnet and Console)** option to allow the user management access and specify a privilege level of the user. In the example, privilege level 15 is selected for the admin user.
7. Click **OK** when done.
8. Click **Apply** to apply the configuration.

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

Configure Cisco ASA Secure Management Access (Cont.)

Task 5: Enable local authentication for SSH and HTTPS

Configuration > Device Management > Users/AAA > AAA Access > Authentication



After you created the local admin user account, you can enable local authentication for management access.

To enable local authentication for SSH and HTTPS access, complete the following steps:

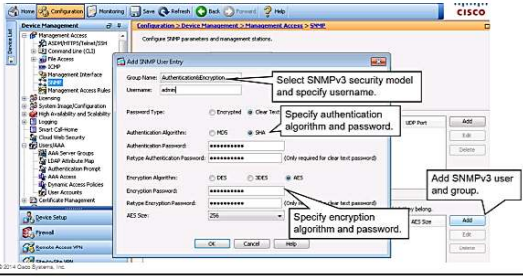
1. Click the **Configuration** button in the Cisco ASDM toolbar.
2. Choose **Device Management** from the navigation pane.
3. Expand the **Users/AAA** option from the Device Management menu.
4. Click the **AAA Access** option in the menu. The Authentication panel is displayed.
5. Enable local authentication by checking a check box next to the desired management access method and selecting LOCAL from the drop-down menu. In the example, local authentication is enabled for SSH and HTTPS access.
6. Click **Apply** to apply the configuration.

https://t.me/learningnets

Configure Cisco ASA Secure Management Access (Cont.)

Task 6: Enable SNMPv3 and configure credentials

Configuration > Device Management > Management Access > SNMP



The Cisco ASA provides support for network monitoring using SNMP Versions 1, 2c, and 3, and supports the use of all three versions simultaneously. The SNMP interface lets you monitor the ASA through network management systems. The ASA supports SNMP read-only access through issuance of a GET request. SNMP write access is not allowed, so you cannot make changes with SNMP. Therefore, the SNMP SET request is not supported.

You can configure the Cisco ASA to send traps, which are unsolicited comments from the managed device to the management station for certain events (event notifications) to an NMS, or you can use the NMS to browse the MIBs on the adaptive security appliance. MIBs are a collection of definitions, and the adaptive security appliance maintains a database of values for each definition. Browsing a MIB means issuing a series of GET-NEXT or GET-BULK requests of the MIB tree from the NMS to determine values.

SNMP requires client authentication to access the Cisco ASA. You can restrict SNMPv1 and v2c clients based on their IP address and knowledge of a password (a community string, sent in the clear), while SNMPv3 can use strong, cryptographic protection.

The fundamental difference between the previous SNMP versions and SNMP version 3 is the introduction of users and groups. Groups specify the security model that will be used to communicate between the adaptive security appliance and the NMS. By introducing users and groups, you control access to the SNMP agent and the MIB objects.

Three SNMPv3 groups are defined on the Cisco ASA:

No Authentication, No Encryption: Communication between the adaptive security appliance and the NMS will be in cleartext.

Authentication Only: Communication between the adaptive security appliance and the NMS will be authenticated.

Authentication and Encryption: Communication between the adaptive security appliance and the NMS will be authenticated and encrypted.

For authenticated and/or encrypted connections, you will need to configure the cryptographic keys, and you will need to choose algorithms to authenticate and/or encrypt SNMP packets between the appliance and the NMS for each user. These keys are symmetric and need to be defined both on the ASA and on the NMS.

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

To allow SNMPv3 clients to poll or to receive traps from the adaptive security appliance, first create a SNMPv3 user and credentials:

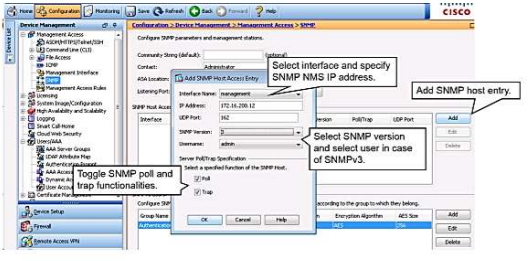
1. Click the **Configuration** button in the Cisco ASDM toolbar.
2. Choose **Device Management** from the navigation pane.
3. Expand the **Management Access** option from the menu.
4. Choose **SNMP** option from the menu.
5. In the SNMPv3 Users pane, to add a configured user or a new user to a group, click **Add**.
6. The Add SNMP User Entry dialog box appears.
7. In the Group Name drop-down list, choose the group to which the SNMP user will belong. The available groups are: Authentication&Encryption, Authentication_Only, and No_Authentication_No_Encryption.
8. In the Username field, enter the name of a configured user or a new user. The username must be unique for the SNMP server group selected.
9. To have the password encrypted, click the **Encrypt Password** radio button. If you choose this option, you must enter the password as an MD5 hash value.
10. Indicate the type of authentication that you want to use by clicking one of the two radio buttons: **MD5 or SHA**. Prefer the SHA-1 (SHA) option to MD5.
11. In the Authentication Password field, type the password to use for authentication.
12. Choose the type of encryption that you want to use by clicking one of these three radio buttons: **DES, 3DES, or AES**. Clicking 3DES or AES is recommended.
13. If you chose AES encryption, then from the AES Size drop-down list, specify which level of AES encryption to use: 128, 192, or 256.
14. In the Encryption Password field, type the password to use for encryption. The maximum number of characters allowed for this password is 64.
15. Click **OK** to create a user for that group.
16. Click **Apply** to apply your configuration.

https://t.me/learningnets

Configure Cisco ASA Secure Management Access (Cont.)

Task 6: Enable SNMPv3 and configure credentials (cont.)

Configuration > Device Management > Management Access > SNMP

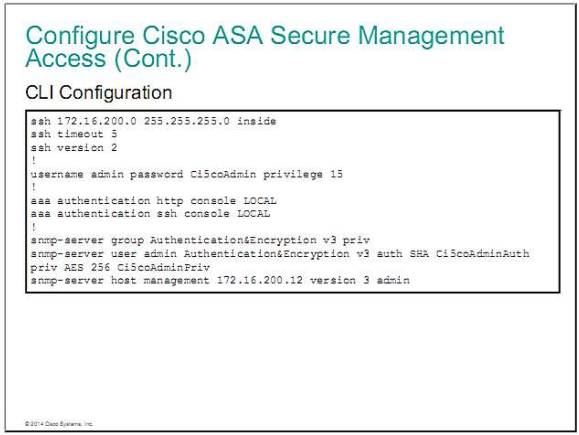


After you created SNMPv3 group and user, you can configure the ASA to allow the SNMP clients to poll or to receive traps from the ASA.

To allow SNMP clients to poll or to receive traps from the ASA, perform the following steps:

1. Click the **Configuration** button in the Cisco ASDM toolbar.
2. Choose **Device Management** from the navigation pane.
3. Expand the **Management Access** option from the menu.
4. Choose the **SNMP** option from the menu
5. Click **Add** in the SNMP Host Access List area to add new SNMP v1/v2c/3 client.
6. In the Add SNMP Host Access Entry window, enter the SNMP client's IP address and select the ASA's interface. Then select SNMP version 3 and specify SNMPv3 username from the drop-down menu. This is the username that was created in the previous steps. Then enable or disable poll or trap SNMP functionalities, as required. In the example, SNMPv3 access is allowed from the 172.16.200.12 host through the management interface, using the admin username. Polling and SNMP traps are enabled.
7. Click **OK** when done.
8. Click **Apply** to apply the configuration.

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



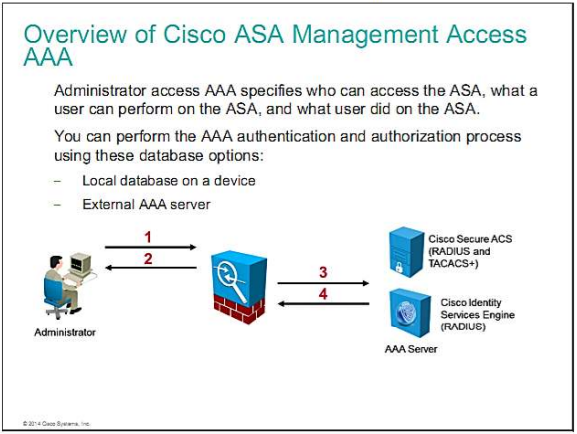
To configure secure management access on the Cisco ASA device using command line interface, use the commands that are described in the table.

Commands	Description
ssh 172.16.200.0 255.255.255.0 inside **ssh timeout 5** **ssh version 2**	Allows SSH access from the specified subnet, specifies SSH version 2 and sets SSH timeout to 5 minutes.
username admin password Ci5coAdmin privilege 15	Creates user account in the local user database with privilege level 15.
aaa authentication http console LOCAL **aaa authentication ssh console LOCAL**	Enables authentication for SSH and HTTPS access against the local user database.
snmp-server group Authentication&Encryption v3 priv **snmp-server user admin Authentication&Encryption v3 auth SHA Ci5coAdminAuth priv AES 256 Ci5coAdminPriv** **snmp-server host management 172.16.200.12 version 3 admin**	Create SNMPv3 group with Authentication and Encryption and security model. Creates SNMPv3 user, associates it with the SNMPv3 group, and specifies authentication and encryption algorithms and keys. Creates SNMPv3 access management rule.

https://t.me/learningnets

Overview of Cisco ASA Management Access AAA

This topic describes management access AAA on the Cisco Adaptive Security Appliance.

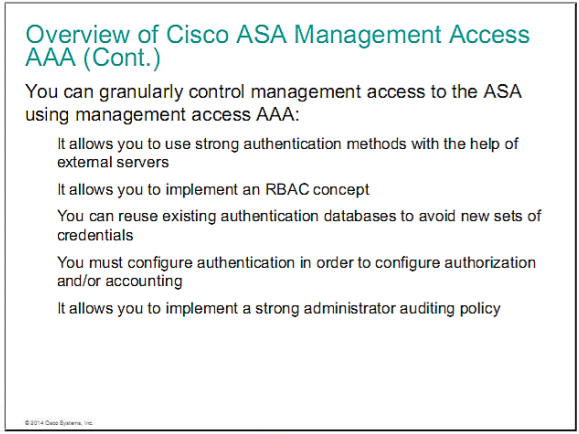


The Cisco ASA uses its AAA subsystem to provide user-based security to its administrative management interface.

The ASA can use a local database to obtain authentication/authorization information, or various external AAA servers to forward AAA requests and information to. External servers are especially useful to centralize all AAA functions in an organization for improved manageability, and to integrate with advanced and existing AAA methods. The ASA supports different types of external servers: TACACS+, RADIUS, LDAP, and SecureID are some of them, with the TACAS+ being the most common one.

This topic describes management access AAA on the Cisco ASA.

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



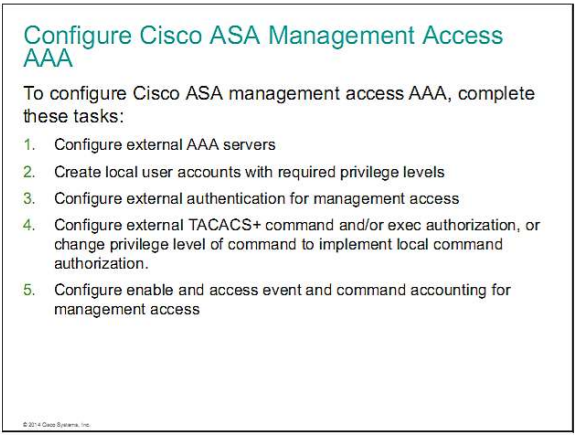
You can use simpler administrator access control features, but it is recommended that you configure the AAA subsystem to control management access. The AAA subsystem will allow you to use stronger authentication methods, implement RBAC using authorization, reuse existing authentication databases, implement strong auditing of infrastructure management, and centralize all infrastructure management AAA.

Note that AAA authorization and accounting processes require an existing authentication configuration.

https://t.me/learningnets

Configure Cisco ASA Management Access AAA

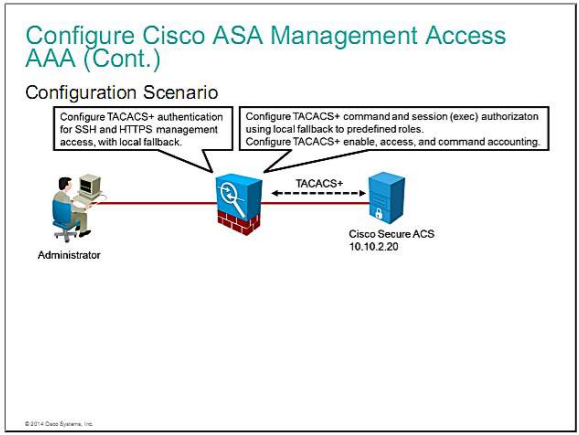
This topic describes how to configure management access AAA on the Cisco Adaptive Security Appliance.



When configuring AAA for management access on the Cisco ASA, you will typically complete the following tasks:

1. Configure external AAA servers by creating a server group and configuring a server in the server group
2. If you decide to back up authentication against an external AAA server, you have to create local user accounts with required privilege levels.
3. Enable authentication of management access for different remote management protocols separately.
4. If using TACACS+ as external server, you can enable remote command authorization and exec authorization. If using RADIUS as external server, you can enable remote exec authorization, and local command authorization by assigning privilege level to a user and to commands.
5. Configure enable and access event and command accounting for management access

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

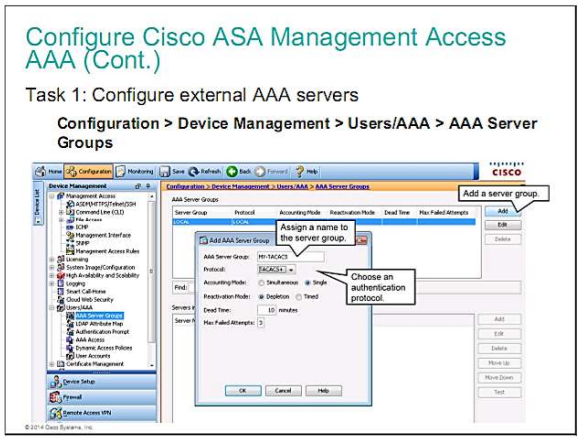


This figure shows the configuration scenario that is used in the upcoming tasks. You will configure the Cisco ASA for management access AAA using TACACS+ server:

You will configure TACACS+ authentication for SSH and HTTPS management access. You will use the local user database on the router as fallback mechanism in case the TACACS+ server fails.

You will also configure TACACS+ command and exec authorization for management sessions. You will backup command authorization using local command authorization using privilege levels of commands and local users.

Finally, you will enable TACACS+ enable and login events and commands accounting.



https://t.me/learningnets

Before configuring external AAA authentication for management access you have to configure external servers.

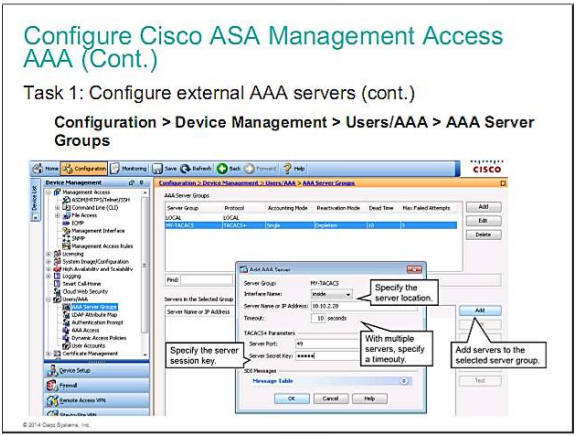
Configuration of external servers consist of of two steps:

Use the AAA Server Groups area of the AAA Server Groups panel to specify a AAA server group. Define a group name and the authentication protocol. Various authentication protocols are available.

Use the Servers in the Selected Group area of the AAA Server Groups panel to designate an authentication server. Define the location of the AAA server, and then define a symmetric session key that needs to match on the adaptive security appliance and the remote AAA server.

To specify a AAA server group, complete the following Cisco Adaptive Security Device Manager steps:

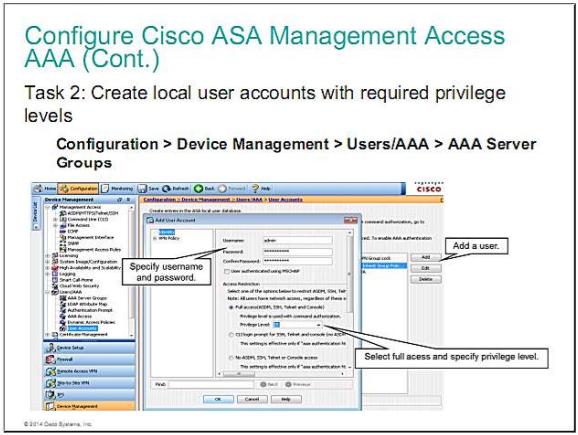
1. Click the **Configuration** button in the Cisco ASDM toolbar.
2. Choose **Device Management** from the navigation pane.
3. Expand the **Management Access** option from the menu.
4. Expand the **Users/AAA** option from the menu.
5. Click the **AAA Server Groups** option in the menu. The AAA Server Groups panel is displayed.
6. In the upper section (AAA Server Groups), click **Add** to create a new server group.
7. In the Add AAA Server Group window, provide a unique local name for the server group. This example uses the MY-TACACS name.
8. In the Protocol drop-down list, choose the authentication proxy protocol that is used by this server group. In this example, the server group is based on the TACACS+ protocol. You can leave other settings at their default values.
9. Click **OK** when done.
10. Click **Apply** to apply the configuration.



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

To add an authentication server to a AAA server group, perform the following steps:

1. Choose a configured AAA server group (MY-TACACS in this example) and click **Add** in the lower (Servers in Selected Group) pane section to add a server to the group.
2. In the Edit AAA Server window, specify the interface over which the AAA server is reachable (inside, in this example) in the Interface Name drop-down box.
3. Enter the IP address of the server (10.10.2.20 in this example) in the Server Name or IP Address field, and the secret key to protect the session with the AAA server in the Server Secret Key field.
4. Click **OK** when done.
5. Click **Apply** to apply the configuration.



To create a user in the ASA local user database, complete the following steps:

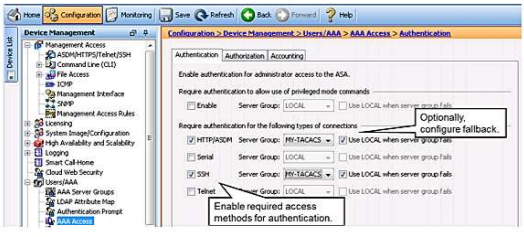
1. Click the **Configuration** button in the Cisco ASDM toolbar.
2. Choose **Device Management** from the navigation pane.
3. Expand the **Users/AAA** option from the Device Management menu.
4. Click the **User Accounts** option in the menu. The User Accounts panel is displayed.
5. Click **Add** to add a user.
6. In the Add User Account window, type the username and password into corresponding input fields. Then select **Full access (ASDM, SSH, Telnet and Console)** option to allow the user management access and specify a privilege level of the user. In the example, privilege level 15 is selected for the admin user. The privilege level of the user can be used to perform local command authorization by assigning privilege levels also commands. A user with assigned privilege level can then execute only commands with the same or lower privilege level.
7. Click **OK** when done.
8. Click **Apply** to apply the configuration.

https://t.me/learningnets

Configure Cisco ASA Management Access AAA (Cont.)

Task 3: Configure external authentication for management access

Configuration > Device Management > Users/AAA > AAA Access > Authentication



After you specify a AAA server group and designate an authentication server, enable authentication for management access by completing the following steps:

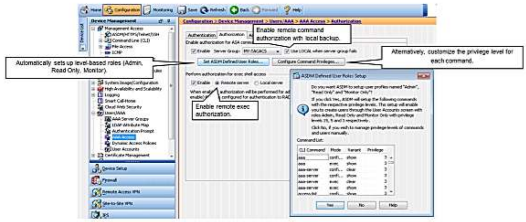
1. Click the **Configuration** button in the Cisco ASDM toolbar.
2. Choose **Device Management** from the navigation pane.
3. Expand the **Users/AAA** option from the menu.
4. Choose the **AAA Access** option in the menu. The AAA Access panel is displayed.
5. Make sure that the **Authentication** tab is selected.
6. Check the check boxes for the access methods for which you want to require remote AAA authentication. In this example, HTTPS and SSH are configured for remote authentication. From the Server Group drop-down list that corresponds to the access method, choose the predefined server group (MY-TACACS in this example).
7. If you chose a AAA server from the Server Group drop-down list, optionally choose the **Use LOCAL When Server Group Fails** check box if you want to use the local database as a fallback authentication method. This is recommended, and chosen in this example.
8. Click **Apply** to apply the configuration.

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

Configure Cisco ASA Management Access AAA (Cont.)

Task 4: Configure external TACACS+ command and/or exec authorization

Configuration > Device Management > Users/AAA > AAA Access > Authorization



There are several approaches to authorizing management access to the adaptive security appliance using a local or remote authorization database. In the configuration example, the local authorization method will be configured as a fallback method to remote authorization. Note, however, that you can also use only local authorization as a standalone method.

The simplest and most intuitive manner to configure local authorization is to assign privilege levels to administrators, and privilege levels to CLI commands (which are mapped to Cisco ASDM user interface functions). A privilege level is an integer between 0 and 15. An administrative user with a particular privilege level can execute all commands up to, and including, the administrative user privilege level. By setting these privilege levels in a desired manner, you can therefore effectively create multiple levels of administrative access to implement an RBAC-like policy.

It is strongly recommended that you first configure all authorization rules on the AAA server in order to prevent command authorization failures at the adaptive security appliance during its configuration. It is also recommended to use local fallback and authorize users using the local authorization database, if the remote server is unavailable. Note that only the TACACS+ protocol is supported for remote authorization of commands and management functions.

Complete the following steps to enable exec and command authorization (backed up with local database) with a TACACS+ server:

1. Click the **Configuration** button in the Cisco ASDM toolbar.
2. Choose **Device Management** from the navigation pane.
3. Expand the **Users/AAA** option from the menu.
4. Choose the **AAA Access** option in the menu. The AAA Access panel is displayed.
5. Click the Authorization tab that is displayed when you choose AAA Access from the Users/AAA menu.
6. From the Server Group drop-down list, choose the name of the TACACS+ server group that you created earlier. In the figure, the TACACS+ server group MY-TACACS is chosen.

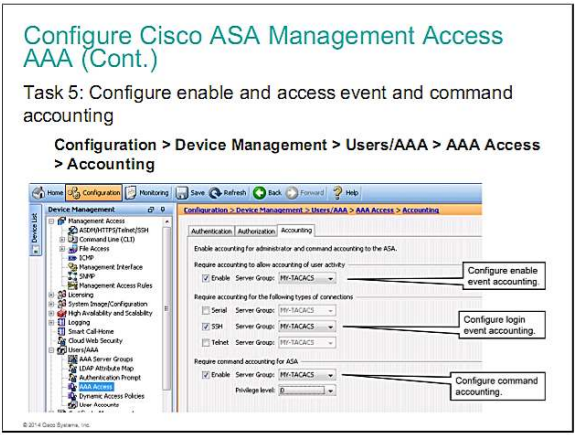
https://t.me/learningnets

7. Check the **Use LOCAL When Server Group Fails** check box to enable fallback to the local database if the TACACS+ server is unavailable.
8. To enable local command authorization, you have to change privilege levels of commands. You have two options available:

   Set ASDM Defined User Roles: Enables you to use predefined user account privileges. Clicking this button opens the ASDM Defined User Roles Setup window, which shows the commands and their levels. Click **Yes** in this window to use the predefined user account privileges. This is the option that is chosen in this configuration example, because the requirements require fallback to the three predefined roles. The predefined user account privileges are as follows:

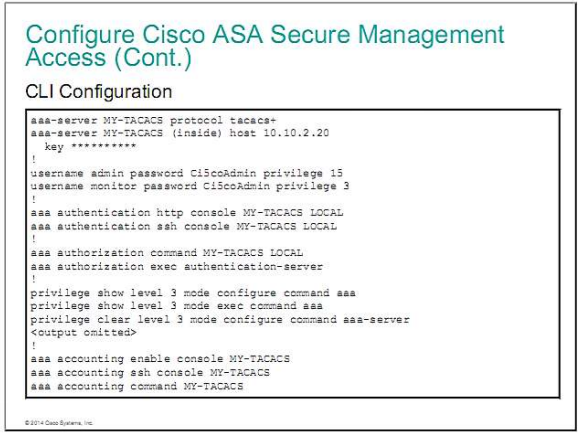
   - **Admin**: Privilege level 15 with full access to all CLI commands
   - **Read Only**: Privilege level 5 with read-only access
   - **Monitor Only**: Privilege level 3 with access to the Monitoring section only

   Configure Command Privileges (not shown in the figure): Enables you to manually assign privilege levels to individual commands or groups of commands. In the figure, this option is chosen, and the Command Privilege Setup window opens.
9. To enable remote exec authorization, check the **Enable** checkbox and select the **Remote server** radio button in the Perform authorization for exec shell access area of the pane.
10. Click **Apply** to apply the configuration.



The adaptive security appliance remote AAA accounting feature supports the auditing of specific events to a central AAA server or a group of servers. You can audit enable events (that is, events where a user enters management mode by supplying the enable password) via RADIUS or TACACS+, login events to the adaptive security appliance via RADIUS or TACACS+, or auditing of individual commands, where only TACACS+ is supported and can be enabled for each command privilege level separately. You can configure these features in the **Configuration > Device Management > Users/AAA > AAA Access > Accounting** pane by specifying the AAA server group that is used to send accounting information to.

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



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

Commands	Description
aaa-server MY-TACACS protocol tacacs+ **aaa-server MY-TACACS (inside) host 10.10.2.20** **key ************	Creates TACACS+ server group and configures a server in the group
username admin password Ci5coAdmin privilege 15 **username monitor password Ci5coAdmin privilege 3**	Creates two user accounts in the local user database with privilege level 15 and 3.
aaa authentication http console MY-TACACS LOCAL **aaa authentication ssh console MY-TACACS LOCAL**	Enables authentication for SSH and HTTPS access against the external TACACS+ server and local database as a backup.
aaa authorization command MY-TACACS LOCAL **aaa authorization exec authentication-server**	Enables authorization of commands against the external TACACS+ server and local database as a backup. Configures exec authorization against the external TACACS+ server.
privilege show level 3 mode configure command aaa **privilege show level 3 mode exec command aaa** **privilege clear level 3 mode configure command aaa-server**	Changes privilege levels of commands to 3.
aaa accounting enable console MY-TACACS **aaa accounting ssh console MY-TACACS** **aaa accounting command MY-TACACS**	Enables accounting of enable and login events and accounting of commands.

https://t.me/learningnets

Verify Cisco ASA Management Access AAA

This topic describes how to verify management access AAA on the Cisco Adaptive Security Appliance.

Verify Cisco ASA Management Access AAA

Verification Commands	Description
show aaa-server	Displays AAA server statistics for AAA servers.
test aaa-server	Verifies connectivity from the ASA to the AAA server.

© 2014 Cisco Systems, Inc.

To verify management access AAA configuration, use the **show aaa-server** and **test aaa-server** commands.

Verify Cisco ASA Management Access AAA (Cont.)

```
ASA# show aaa-server
Server Group:    MY-TACACS
Server Protocol: tacacs+
Server Address:  172.16.1.17
Server port:     49
Server status:   ACTIVE, Last transaction at 08:24:27 UTC Thu Apr 15 2010
Number of pending requests              0
Average round trip time                 36ms
Number of authentication requests       10
Number of authorization requests        0
Number of accounting requests           0
Number of retransmissions               0
Number of accepts                       5
Number of rejects                       4
Number of challenges                    0
Number of malformed responses           0
Number of bad authenticators            0
Number of timeouts                      1
Number of unrecognized responses        0
```

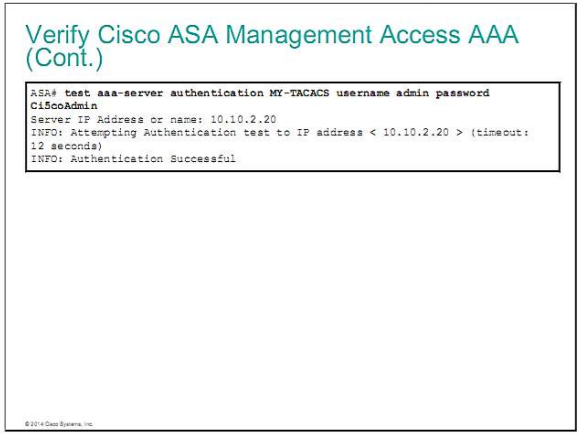
© 2014 Cisco Systems, Inc.

When using remote AAA services, you can easily verify the functionality of the AAA server by observing the AAA server status and statistics. Use the show aaa-server command to verify AAA server and statistics.

https://t.me/learningnets

The command displays the following parameters:

- The server group to which the server belongs
- The protocol that the server group uses for AAA
- The IP address of the AAA server
- The status (active or inactive) of the AAA server
- Statistics regarding authentication requests and responses



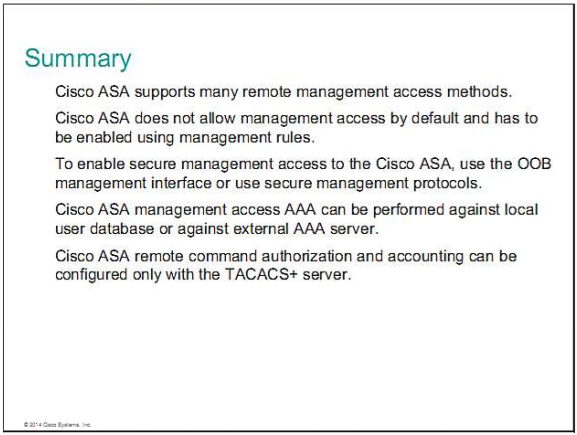
A very useful tool to verify connectivity from the adaptive security appliance to the AAA server is the **test aaa-server** command, available in the CLI. To verify connectivity to a AAA server in a specified server group, use the **test aaa-server authentication** command, followed by a AAA server group name and username and password of one user, present on a AAA server.

Note The test AAA server tool is also available in Cisco Adaptive Security Device Manager. Choose **Configuration > Device Management > Users/AAA > AAA Server Groups**, choose a AAA server, and click the **Test** button.

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 5

Deploying Cisco Traffic Telemetry Methods

Overview

In order to operate and ensure availability of a network, it is critical to have visibility and awareness into what is occurring on the network at any given time. Network telemetry offers extensive and useful detection capabilities that can be coupled with dedicated analysis systems to collect, trend, and correlate observed activity.

Baseline network telemetry is both inexpensive and relatively simple to implement. This lesson highlights the baseline forms of telemetry recommended for network infrastructure devices, including NTP, logging, and NetFlow on Cisco IOS Software and Cisco ASA 5500-X Series devices.

This ability includes being able to meet these objectives:

- Describe Cisco traffic telemetry methods
- Describe NTP
- Configure NTP on Cisco IOS Software
- Verify NTP on Cisco IOS Software
- Configure NTP on Cisco ASA
- Verify NTP on Cisco ASA
- Describe device and network events logging services on Cisco devices
- Configure logging on Cisco IOS Software
- Verify logging on Cisco IOS Software
- Configure logging on Cisco ASA
- Verify logging on Cisco ASA
- Describe NetFlow on Cisco devices

https://t.me/learningnets

Configure NetFlow on Cisco IOS Software

Verify NetFlow on Cisco IOS Software

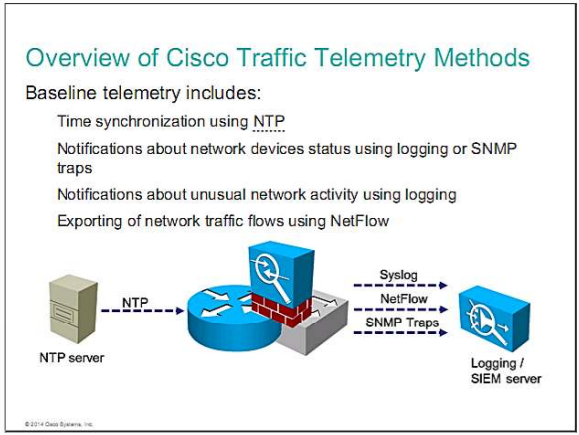
Configure NetFlow on Cisco ASA

Verify NetFlow on Cisco ASA

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

Overview of Cisco Traffic Telemetry Methods

This topic provides an overview of some traffic telemetry methods, that are available on Cisco devices.

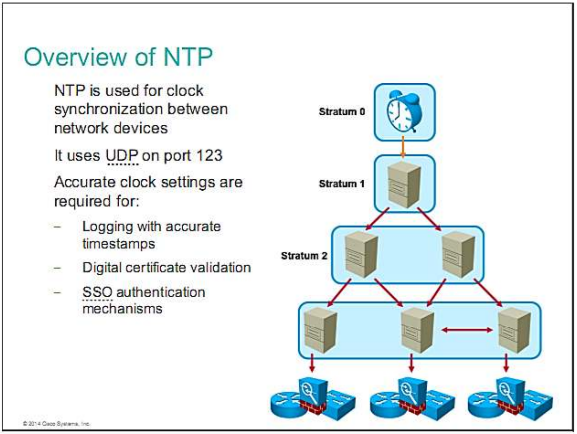


Network administrators need an insight what is happening in their network in order to detect unusual network traffic, network device failures, or just to monitor what kind of traffic most traverses the network. Traffic telemetry is implemented using various mechanism, such as syslog logging, SNMP traps, and NetFlow exports. When implementing network telemetry, it is important that dates and times on are both accurate and synchronized across all network infrastructure devices. Without time synchronization, it is very difficult to correlate different sources of telemetry.

https://t.me/learningnets

Overview of NTP

This topic provides an overview of NTP.



It is beneficial and in some cases even necessary to have accurate time (or at least synchronized time) on your network devices. These are some of the benefits of synchronized time settings:

Checking logs on different devices: Usually logs are directed to one or a few syslog servers that receive all messages, and you can view the local time stamps for all messages. If you compare logs on different devices, then synchronized time is essential to analyzing past events successfully.

Certificate validation: When using certificates, synchronized time is necessary, because a certificate is considered valid only if the current time falls within the time (and date) interval that is specified inside the certificate. A certificate that seems to be expired is not considered valid. Similarly, a certificate that shows an issue date in the future is not valid.

Single-sign on authentication mechanisms: some security devices support single-sign on authentication against Microsoft Active Directory server. Such integration requires that time both on the security device and on the Active Directory server is within specific limits.

The protocol that is used for synchronization of time is NTP, which uses UDP on port 123 for transport. There are other protocols that you can use, but NTP is widely supported. NTP makes corrections to the time using gradual adjustments, which avoids certain problems. A sudden large time change can result in logs having nonsequential time-stamp entries. To avoid such anomalies, NTP never updates a clock directly, but it causes the clock to run faster or slower until the correct time is reached.

NTP uses a hierarchical model for time data distribution, and NTP servers and clients are divided into layers that are called strata (singular: stratum). The source of the correct time is usually either an atomic clock or a GPS receiver, which receives its time signal from an atomic clock on a GPS satellite. These devices are called stratum 0 devices.

Stratum 0 devices provide time data to stratum 1 devices. The connection between stratum 0 and stratum 1 devices is typically a dedicated link, thus NTP is not used.

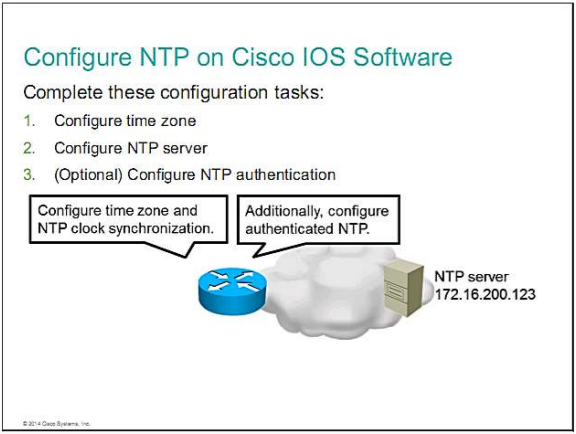
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Stratum 1 devices are servers, which do run NTP and provide time service to stratum 2 servers, which in turn provide NTP service to stratum 3 devices, and so on.

https://t.me/learningnets

Configure NTP on Cisco IOS Software

This topic explains how to configure NTP on Cisco IOS Software.

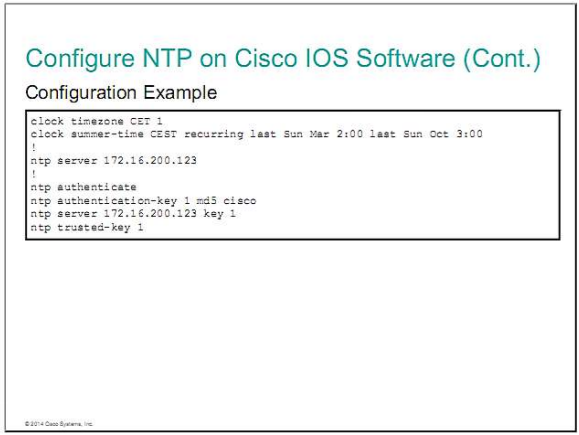


To configure NTP on a Cisco IOS Software router or switch, complete the following tasks:

1. Configure time zone
2. Configure NTP server
3. Optionally configure NTP authentication to authenticate the NTP source before synchronizing time.

The figure also shows the configuration scenario. On the Cisco IOS router, you will configure authenticated NTP association with an NTP server reachable at 172.16.200.123

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



In the first task, you will configure time zone.

The time zone is set using the **clock timezone** command, followed by the name (abbreviation) of the time zone and offset.

If your time zone uses daylight saving time, you can configure your summer time zone using the **clock summer-time** command, followed by name of the summer time zone, the keyword **recurring** (indicating that you use summer time every year), the day and hour of the start of summer time and the day and hour of the end of summer time. The last parameter (which is missing in the example in the figure) is the offset from your configured time zone (not UTC) if it is different from one hour. If summer time is winter time +1, you do not need the parameter.

In the second task, configure the NTP server using the **ntp server** command, followed by an IP address or hostname.

In the third task you will configure NTP authentication. The command **ntp authenticate** enables NTP authentication. The command **ntp authentication-key 1 md5 cisco** defines cisco string as the key. The **ntp server 172.16.200.123 key 1** command defines the key to be used for authentication. The command **ntp trusted-key 1** marks the key as trusted when the configured system is updating its own time to the server's time. If the key is not trusted, then local time cannot be modified based on remote time.

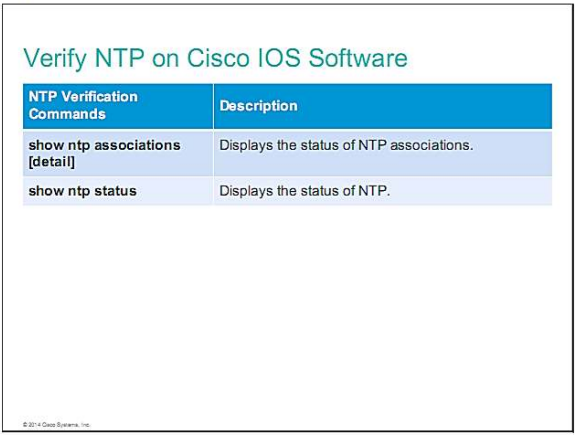
To configure NTP on the Cisco router, use the commands that are described in this table:

Commands	Description
clock timezone CET 1 **clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00**	Sets timezone and daylight savings.
ntp server 172.16.200.123	Configures NTP server.
ntp authenticate **ntp authentication-key 1 md5 cisco** **ntp server 172.16.200.123 key 1** **ntp trusted-key 1**	Configures NTP authentication.

https://t.me/learningnets

Verify NTP on Cisco IOS Software

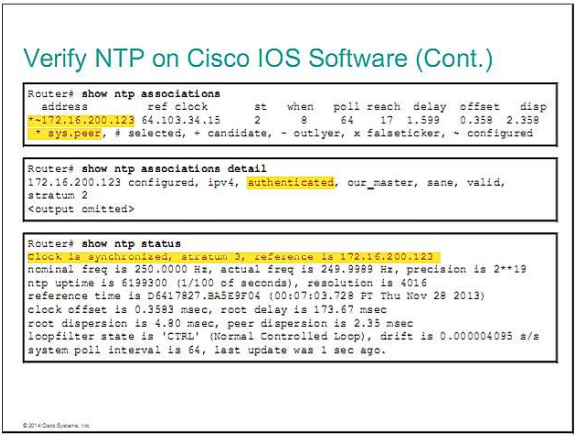
This topic explains how to verify NTP on Cisco IOS Software.



Use the following command to verify NTP on Cisco IOS routers:

Use the **show ntp associations [detail]** command to verify the status of NTP associations.

Use the **show ntp status** command to verify the status of NTP.



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

The **shown ntp associations** command shows that the clock is synchronized to the NTP server at 172.16.200.123. The stratum of the server is 2.

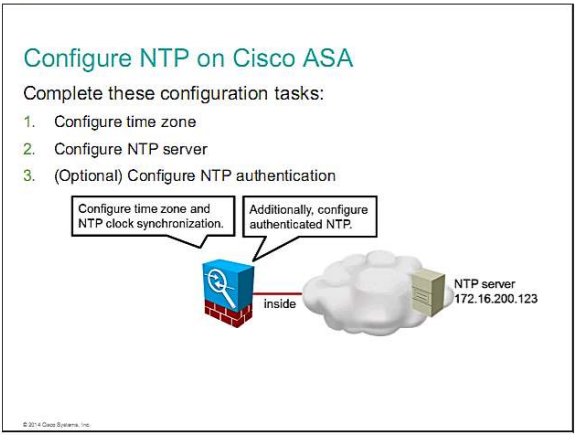
The **show ntp associations detail** command shows that NTP to the 172.16.200.123 is authenticated.

The **show ntp status** command shows that the clock is synchronized to the NTP server at 172.16.200.123. The stratum of the local router is 3.

https://t.me/learningnets

Configure NTP on Cisco ASA

This topic explains how to configure NTP on Cisco ASA.

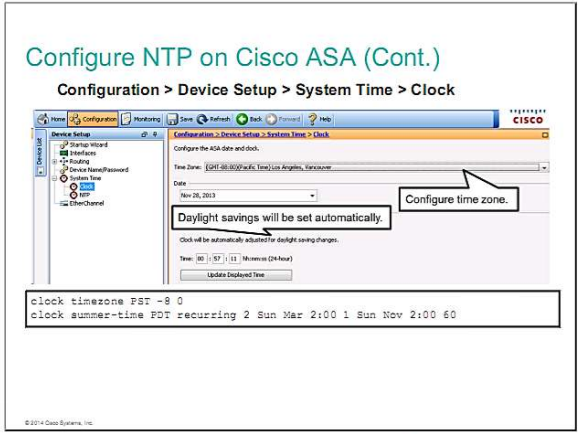


To configure NTP on the Cisco ASA, complete the following tasks:

1. Configure time zone
2. Configure NTP server
3. Optionally configure NTP authentication to authenticate the NTP source before synchronizing time.

The figure also shows the configuration scenario. You will configure authenticated NTP association with an NTP server reachable at 172.16.200.123

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



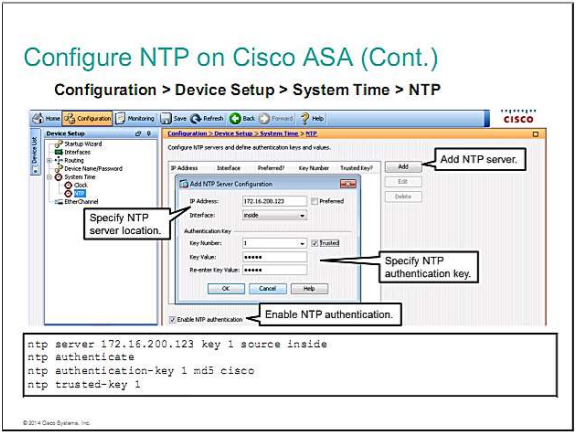
Follow these steps to configure timezone on the Cisco ASA using Cisco ASDM:

1. Choose **Configuration** from the toolbar.
2. Choose **Device Setup** from the navigation pane.
3. Expand the **System Time** menu.
4. Choose **Clock**. The Clock panel is displayed.
5. Choose the time zone from the Time Zone drop-down list. Your selection sets the time zone as GMT plus or minus the appropriate number of hours. When you choose the time zone, the time adjusts automatically for daylight savings time.
6. Click **Apply**.

In the CLI, use the following commands to configure timezone and daylight savings.

Commands	Description
clock timezone PST -8 0	Sets timezone to Pacific Time.
clock summer-time PDT recurring 2 Sun Mar 2:00 1 Sun Nov 2:00 60	Sets daylight savings.

https://t.me/learningnets



NTP is used to implement a hierarchical system of servers that provide precisely synchronized time to participating network systems. This kind of accuracy is required for time-sensitive operations that include a precise time stamp. Time derived from an NTP server overrides any time set manually.

You can configure multiple NTP servers; consider using at least 2 reliable time servers for optimal accuracy and redundancy. The security appliance chooses the server with the lowest stratum, which is a measure of how reliable the data is. You can also configure the security appliance to require authentication before synchronizing with the NTP server, if you use NTP over untrusted networks.

To dynamically set the time using an NTP server, complete the following steps:

1. Choose **Configuration** from the toolbar.
2. Choose **Device Setup** from the navigation pane.
3. Expand the **System Time** menu.
4. Choose **NTP**. The NTP panel is displayed.
5. Check the **Enable NTP authentication** checkbox to enable NTP authentication.
6. Click **Add**. The Add NTP Server Configuration window opens.
7. Enter the IP address of the NTP server in the IP Address field. The security appliance listens for NTP packets (UDP port 123) only on interfaces that have an NTP server configured. NTP packets that are not responses from a request by the security appliance are dropped. In the figure, the host at 172.16.200.123 is configured as the NTP server.
8. Specify the outgoing interface for NTP packets by selecting an interface from the Interface drop-down list. If you do not specify an interface here, the security appliance determines the interface from its routing table. In the figure, the inside interface is chosen as the outgoing interface for NTP packets to the configured NTP server.

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

9. (Optionally) Check the **Preferred** check box to designate this NTP server as a preferred server. NTP uses an algorithm to determine which server is the most accurate and synchronizes to that server. If servers are of similar accuracy, the preferred server is used. However, if a server is significantly more accurate than the preferred one, the security appliance uses the more accurate one. The security appliance uses a more accurate server over a less accurate server that is preferred. In the figure, host 172.16.200.123 will be the preferred NTP server.
10. Enter the authentication key ID number in the Key Number field. The NTP server packets must also use this key ID. The NTP server needs to include this number in its NTP packets in order for the security appliance to accept synchronization with the NTP server. If you previously configured a key ID for another server, you can select it from the drop-down list; otherwise, enter a number between 1 and 4,294,967,295. In the figure, the authentication key ID number is 1.
11. In the Key Value field, enter the authentication key as a string up to 32 characters in length. With authentication configured, the security appliance uses MD5 authentication for communicating with the NTP server. The security appliance and NTP server must be configured with the same key if authentication is used. Enter the authentication key again in the Re-enter Key Value field.
12. Check the **Trusted** check box to set this key as a trusted key. You must check this check box for authentication to work.
13. Click **Apply**.

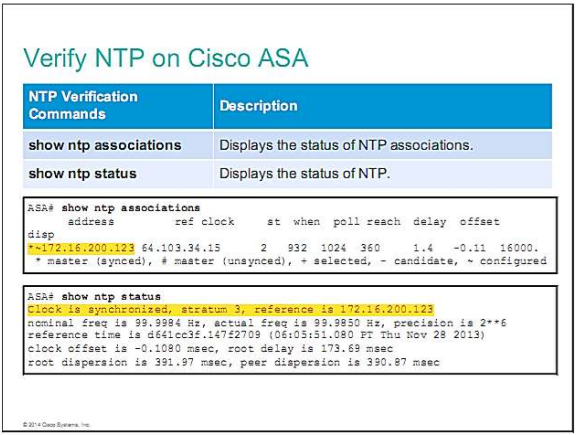
In the CLI, use the following commands to configure timezone and daylight savings.

Commands	Description
ntp server 172.16.200.123 key 1 source inside	Specifies NTP server location.
ntp authenticate	Enables NTP authentication.
ntp authentication-key 1 md5 cisco	Specifices NTP authentiaction key.
ntp trusted-key 1	Specifies the NTP authentication key as trusted.

https://t.me/learningnets

Verify NTP on Cisco ASA

Verify NTP on Cisco ASA



Use the following command to verify NTP on the Cisco ASA:

Use the **show ntp associations** command to verify the status of NTP associations.

Use the **show ntp status** command to verify the status of NTP.

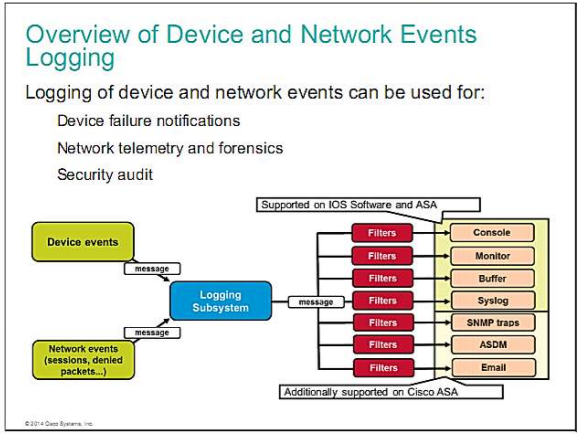
The **shown ntp associations** command shows that the clock is synchronized to the NTP server at 172.16.200.123. The stratum of the server is 2.

The **show ntp status** command shows that the clock is synchronized to the NTP server at 172.16.200.123. The stratum of the local ASA device is 3.

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

Overview of Device and Network Events Logging

This topic provides an overview of device and network events logging services on Cisco devices.



Network devices, such as routers, switches, and firewall send logging messages about network activity or abnormal device events to a logging subsystem. The logging subsystem controls the distribution of logging messages to various destinations, such as the logging buffer, terminal lines, or a UNIX syslog server, depending on your configuration. The logging subsystem ca also send messages to the console.

Before a logging subsystem distributes a logging message to a logging destination, the subsystem determines whether to filter the message or not. Filtering is generally implemented using message severity levels. The Cisco ASA devices also support advanced filtering using event classes or custom message lists.

Logging to a central syslog server helps in aggregation of logs and alerts. Cisco devices can send their log messages to a UNIX-style syslog service. A syslog service accepts messages and stores them in files, or prints them according to a simple configuration file. This form of logging provides protected long-term storage for logs. Logs are useful for device failure notifications, routine troubleshooting, security audit, and in network telemetry and forensics and incident handling.

The Cisco devices, such as Cisco IOS Software routers and switches and Cisco ASA devices support the following logging destinations:

Console: This is a low-bandwidth serial connection to which you can send system log messages inside the console CLI session. This mode

Telnet or SSH administrative sessions: Administrators can use Telnet or SSH to connect to network devices. If logging is required over such sessions, it has to be enabled explicitly.

The internal in-memory buffer: This buffer on devices is useful for storing and analyzing a snapshot of recent activity on the devices. This buffer is not persistent across device reboots.

Remote syslog servers: The Cisco devices use the standard UNIX syslog protocol to send events to a syslog server. Syslog logging uses UDP on port 514 as a transport protocol.

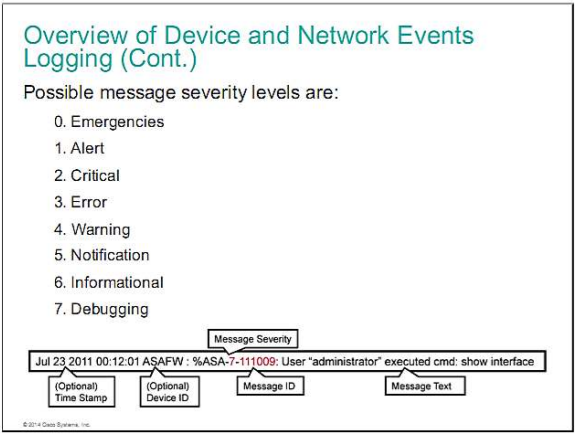
https://t.me/learningnets

The Cisco ASA devices additionally support these logging destinations:

Remote network management servers: The security appliance uses the standard SNMP trap to send events.

Cisco Adaptive Security Device Manager GUI: The Cisco ASDM provides a powerful event viewer that is useful for troubleshooting issues or monitoring network activity in real time.

Email systems: The ASA uses standard SMTP to send events to a defined set of SMTP email servers.



Most Cisco device messages that the logging subsystem generates are simple text messages that conform to a particular message format. A typical syslog message consists of these items:

A timestamp, which is disabled by default

A device ID, which is disabled by default but which can include the interface name, IP address, hostname, context name, or custom string—up to 16 characters

A message identifier, such as %ASA-7-111009 (where %ASA indicates the device type, 7 indicates severity level and 111009 event message number)

The message text, such as "User 'administrator' executed cmd: show interface"

Each system message is assigned a message severity that indicates its importance. Possible number and string values for message severity are as follows:

0 – Emergencies: Extremely critical "system unusable" messages

1 – Alerts: Messages that require the administrator to take immediate action

2 – Critical: A critical condition

3 – Errors: An error message

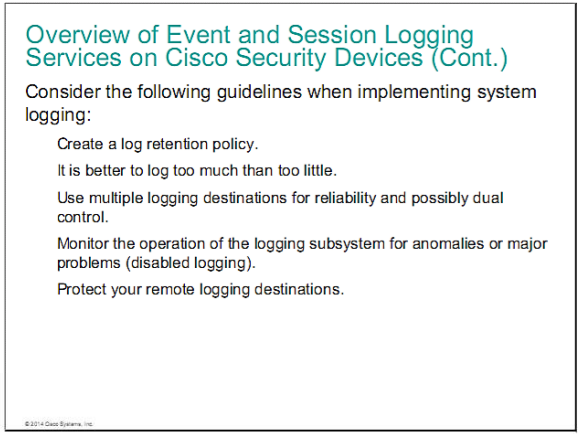
4 – Warnings: A warning message

5 – Notifications: A normal but significant condition

6 – Informational: An information message

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

7 – Debugging: A debug message or a very detailed accounting message



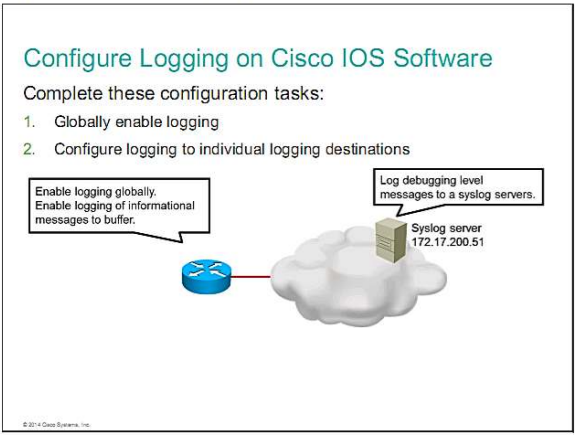
A best practice is to configure too much logging rather than too little. Gathering more information is typically harmless (unless it causes performance or capacity issues); however, gathering too little information can prevent you from effectively responding to incidents.

Access to the device logging subsystem must be limited (so that attackers or administrators cannot disable logging without detection). If fewer people have direct access to event data, it is less likely that such data will be compromised. Provide mechanisms to prevent or detect changes to stored event data. Some organizations might use a single protective layer, such as ACLs, while other organizations might use multiple layers, including cryptographic checksums and digital signatures.

https://t.me/learningnets

Configure Logging on Cisco IOS Software

This topic explains how to configure logging on Cisco IOS Software.

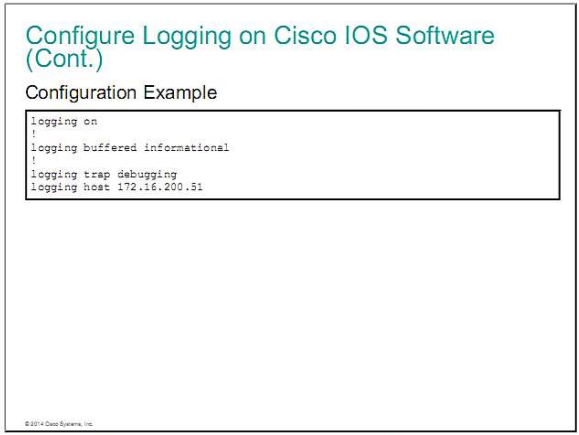


To configure logging on a Cisco IOS Software router or switch, complete the following tasks:

1. Globally enable logging.
2. Configure logging of messages with specified logging level to individual logging destinations.

The figure also shows the configuration scenario. On the Cisco IOS router, you will first make sure that the logging is enabled globally. Then, you will enable logging of informational events to internal buffer and logging of debugging events to the Syslog server at 172.17.200.51.

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



Logging is globally enabled by default on the Cisco IOS devices. However, if you have to enable it because it was disabled, use the **logging on** command. The Cisco IOS Software devices are also by default configured to send logging messages with debugging level and lower to the console and to monitor sessions.

Then enable logging to buffer using the **logging buffered** command, followed by required severity level. In the example, messages of level 6 and lower will be logged to the buffer.

Then enable logging to syslog servers using the **logging buffered** command, followed by required severity level. In the example, messages of level 7 and lower will be logged to a syslog server.

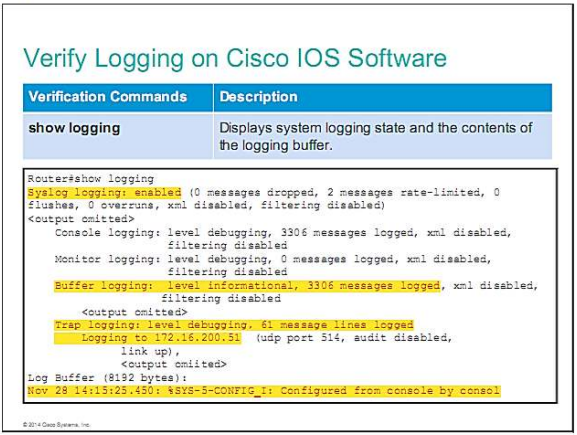
Finally, specify the location of the syslog server using the **logging host** command, followed by the IP address of the syslog server.

Commands	Description
logging on	Globally enables logging.
logging buffered informational	Enables logging of informational events to buffer
logging trap debugging **logging host 172.16.200.51**	Enables logging of debugging events to the Syslog server at 172.16.200.51.

https://t.me/learningnets

Verify Logging on Cisco IOS Software

This topic explains how to verify logging on Cisco IOS Software.



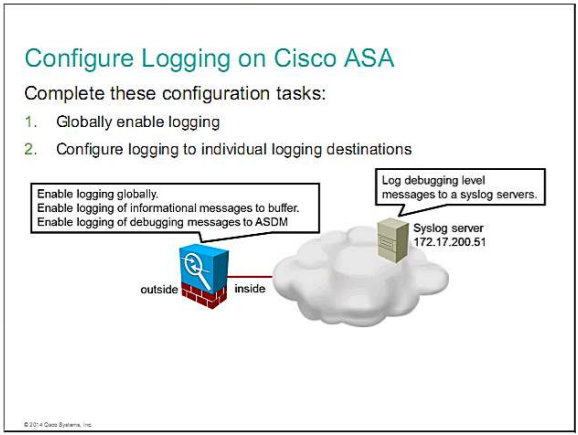
Use the **show logging** command to display system logging configuration and state and to display content od the internal logging buffer

In the example you can see that logging is globally enabled. You can also see that logging to buffer and syslog logging is enabled. Note that also logging to console and monitor sessions are enabled (the default settings). At the end of the output you can see one message that is stored in the internal logging buffer.

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

Configure Logging on Cisco ASA

This topic explains how to configure logging on the Cisco ASA.

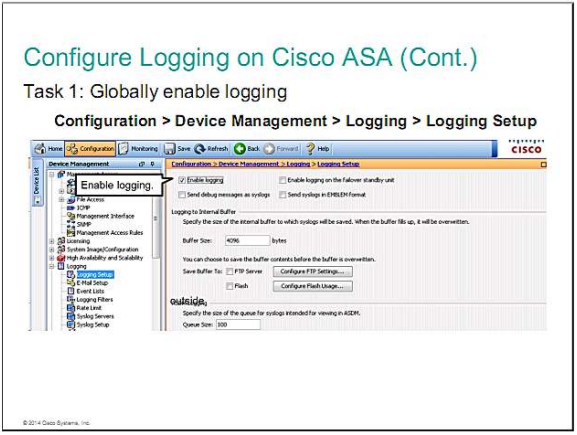


To configure logging on the Cisco ASA, complete the following tasks:

1. Globally enable logging.
2. Configure logging of messages with specified logging level to individual logging destinations.

The figure also shows the configuration scenario. You will first make sure that the logging is enabled globally on the Cisco ASA. Then, you will enable logging of informational events to internal buffer and logging of debugging events to the Syslog server at 172.17.200.51 and to the Cisco ASDM.

https://t.me/learningnets



Follow these steps to complete the first task in configuring event and session logging, enabling logging globally on the ASA:

1. Click the **Configuration** button in the Cisco ASDM toolbar.
2. Choose **Device Management** from the navigation pane.
3. Expand the **Logging** option from the Device Management menu.
4. Choose **Logging Setup**. The Logging Setup panel appears.
5. Check the **Enable Logging** check box. By default, all logging on the adaptive security appliance is disabled. From this panel, you can also optionally use the following components to configure logging parameters:

   Enable Logging on the Failover Standby Unit: Click this check box to turn on logging for the standby adaptive security appliance, if available. By default, without enabling logging on the standby unit, severity level 1 messages are still available on the standby unit. Failover configurations are discussed in a later lesson.

   Send Debug Messages as Syslogs: Click this check box to redirect all debug output to system logs. By default, the adaptive security appliance does not include debug output in system log messages. Checking this box redirects debug messages to logs as system log messages 711001 issued at severity level 7.

   Send Syslogs in EMBLEM format: Click this check box to enable Cisco EMBLEM format so that it is used for all log destinations, except syslog servers. EMBLEM syslog format is designed to be consistent with the Cisco IOS format. However, many event management solutions will not recognize messages in EMBLEM format. The EMBLEM format is used primarily for the CiscoWorks Resource Manager Essentials (RME) Syslog Analyzer.

   Buffer Size: Use this field to specify the size of the internal log buffer to which system log messages are saved if the logging buffer is enabled. When the buffer is full, messages are overwritten unless you save the logs to an FTP server or to internal flash memory. The default buffer size is 4096 bytes. You can specify a size from 4096 to 1048576 bytes.

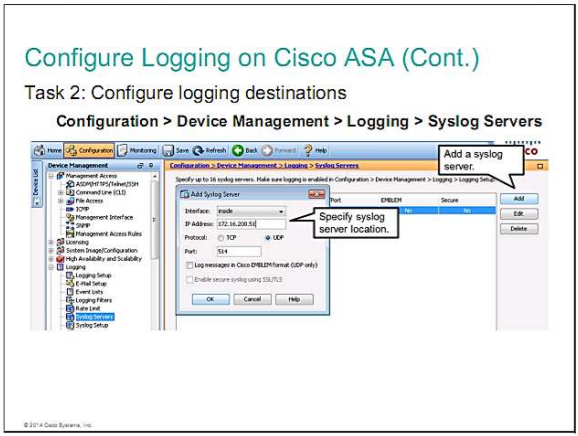
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Save Buffer To: Check one of the following check boxes to specify where logs are saved when the adaptive security appliance buffer is full:

- **FTP Server**: Choosing this option saves the logs to an FTP server. If you choose this option, click the **Configure FTP Settings** button to identify the FTP server and configure the FTP parameters that are used to save the buffer content.
- **Flash**: Choosing this option saves the buffer content to internal flash memory. If you choose this option, click **Configure Flash Usage** to specify the maximum space to be used (in KB) in internal flash memory for logging and the minimum free space to be preserved. Enabling this option creates a directory called "syslog" on the device disk on which messages are stored.

Queue Size: Use this field to specify the number of system log messages retained in the Cisco ASDM log buffer. The Cisco ASDM log buffer is a different buffer than the internal log buffer. The default Cisco ASDM syslog buffer size is 100 messages. When the Cisco ASDM log buffer is full, the adaptive security appliance deletes the oldest message to make room in the buffer for new messages.

6. Click **Apply** to apply the configuration.



Configuring the adaptive security appliance to send logs to a syslog server enables you to archive logs, limited only by the available disk space on the remote syslog server. You can specify up to 16 syslog servers. The adaptive security appliance can deliver syslog messages to remote syslog servers using UDP or TCP as a transport protocol.

The Cisco ASA also supports secure logging with an SSL/TLS transport layer between the adaptive security appliance and remote syslog servers. Certificate authentication and encrypted data transfer help mitigate security threats to the logging service when the message stream is traversing an untrusted network.

To use secure logging, you must set up an SSL connection between the syslog server and the adaptive security appliance. The syslog server that is used must have SSL/TLS capability. (This aspect of the secure logging configuration is beyond the scope of this course.

https://t.me/learningnets

When an adaptive security appliance is configured with at least one TCP-based syslog server, by default, the appliance will block all traffic through it if the TCP-based syslog server is down. This feature is used to prevent traffic through the adaptive security appliance when you cannot log it. Use this feature if your local security policy mandates such a risk control.

To define (non-SSL/TLS) syslog servers that can be used by the adaptive security appliance, complete the following steps:

1. Click the **Configuration** button in the Cisco ASDM toolbar.
2. Choose **Device Management** from the navigation pane.
3. Expand the **Logging** option from the Device Management menu.
4. Choose **Syslog Servers**. The Syslog Servers panel appears.
5. Click **Add**. The Add Syslog Server window opens. This window enables you to specify the syslog servers to which the adaptive security appliance should send system log messages.
6. Complete the following substeps to add a syslog server:

   From the Interface drop-down list, choose the interface that the adaptive security appliance will use to communicate with the syslog server. In the figure, the inside interface is chosen.

   In the IP Address field, enter the IP address of the syslog server. In the figure, the IP address of the syslog server is172.17.200.51.

   Choose one of the Protocol radio buttons (TCP or UDP) to specify the protocol used by the syslog server to communicate with the adaptive security appliance. The default protocol is UDP. You can configure the adaptive security appliance to send data to a syslog server using either UDP or TCP, but not both. If you specify TCP, the adaptive security appliance discovers when the syslog server fails and, by default, stops sending logs. If you specify UDP, the adaptive security appliance continues to send logs regardless of whether the syslog server is operational. In the figure, UDP is chosen.

   In the Port field, enter the port number that the syslog server will use to communicate with the adaptive security appliance. Valid port values are 1025 through 65535 for both TCP and UDP. The default UDP port is 514. The default TCP port is 1470.

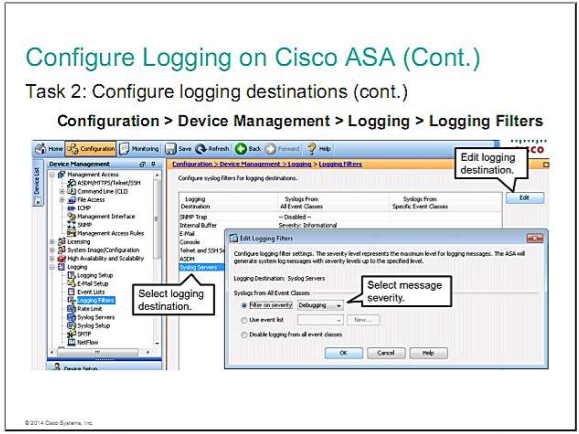
   (Optional) Check the **Log Messages in Cisco EMBLEM Format (UDP only)** check box. This option is available only if UDP is selected as the protocol.

   Click **OK**. Your configuration appears in the Syslog Servers panel.

   (Optional) Specify the number of messages that are allowed to be queued on the adaptive security appliance when a syslog server is busy. Use 0 to specify an unlimited queue size. The default is 512 messages.

   (Optional) Check the **Allow User Traffic to Pass When TCP Syslog Server Is Down** check box.
7. Click **Apply** to apply the configuration.

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



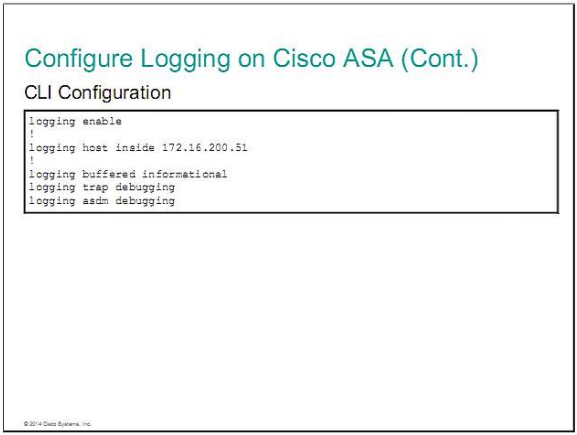
You can enable logging to the internal Cisco ASDM event viewer by specifying Cisco ASDM as a logging destination, and specifying a logging filter. The Cisco ASDM displays messages forwarded to it over the HTTPS management session at the bottom of the home pane. To use the full event viewer functionality, start the viewer by choosing the **Monitoring > Logging > Real-time Viewer** pane and clicking the **View** button.

In most cases, it is recommended to use remote syslog servers as your primary method of reporting system events to a central repository, because this is a widely supported and simple-to-deploy protocol. Because UDP transport is not reliable (that is, it does not guarantee delivery) and should only be used over reliable networks, consider using TCP transport when operating over congested and lossy transport networks. Consider using SSL/TLS protection if your logging stream uses an untrusted transport network between the adaptive security appliance and the syslog server.

Complete the following steps to enable logging to individual destination:

1. Click the **Configuration** button in the Cisco ASDM toolbar.
2. Choose **Device Management** from the navigation pane.
3. Expand the **Logging** option from the Device Management menu.
4. Choose **Logging Filters**. The Logging Filters panel appears. The Logging Filters panel enables you to apply message filters to a log destination.
5. Choose a destination from the **Logging Destinations** list in the Logging Filters panel. In the example, Syslog Servers is selected.
6. Click **Edit**. The Edit Logging Filters window opens for that particular destination.
7. Select the **Filter on Severity** radio button and select logging severity level from the drop-down menu. In the example, **Debugging** message severity is selected.
8. Click **Apply** to apply the configuration.

https://t.me/learningnets



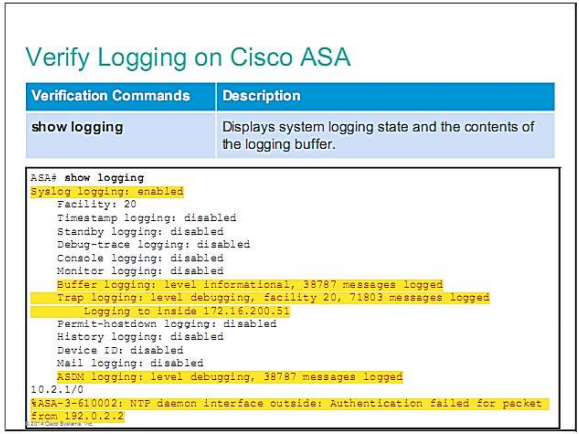
In the CLI, use the following commands to configure logging.

Commands	Description
logging enable	Globally enables logging.
logging host inside 172.16.200.51	Specifies a location on the syslog server.
logging buffered informational **logging trap debugging** **logging asdm debugging**	Configures logging to individual destinations based on message severity levels.

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

Verify Logging on Cisco ASA

This topic explains how to verify logging on the Cisco ASA.



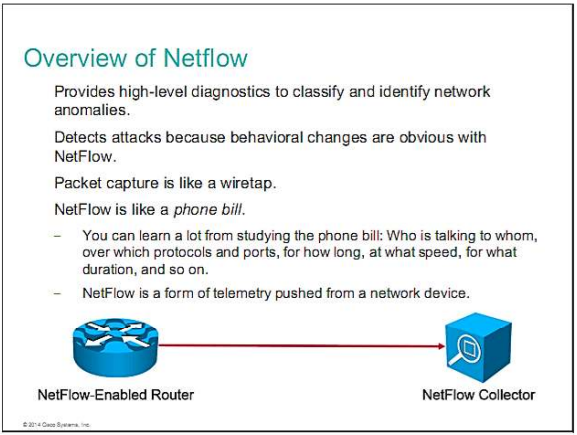
Use the **show logging** command to display system logging configuration and state and to display content od the internal logging buffer

In the example you can see that logging is globally enabled. You can also see that logging to buffer, syslog server and ASDM logging is enabled. At the end of the output you can see a message that is stored in the internal logging buffer.

https://t.me/learningnets

Overview of Netflow

This topic provides an overview of NetFlow on Cisco devices.



NetFlow is an embedded feature within Cisco IOS Software that you can use to characterize network operation by enabling the collection of network traffic telemetry. In response to new requirements and threats, network operators are finding it critical to understand how the network is behaving, including the following information:

Application and network usage

Network productivity and utilization of network resources

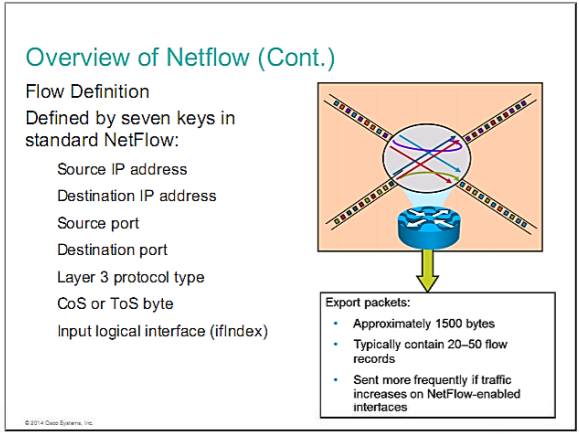
The impact of changes to the network

Network anomaly and security vulnerabilities

NetFlow technology fulfills those needs, creating an environment in which you have the tools to understand who, what, when, where, and how network traffic is flowing. When you understand the network behavior, business processes improve and an audit trail of how the network is used is available. This increased awareness reduces the vulnerability of the network to outages and allows the network to operate efficiently. Improvements in network operation lower costs and encourage higher business revenues by enabling better utilization of the network infrastructure.

NetFlow is not like a sniffer that captures all traffic that flows through it. To use an analogy from the telephone industry, NetFlow is like a phone bill, from which you can learn a lot. You can deduce who is talking to whom, how frequently, how long, and so on. With this information, you can use an analysis engine or SIEM system, to determine much of what is going on in the network.

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



Each packet that is forwarded within a router or switch is examined for a set of IP packet attributes. These attributes are the IP packet identity or fingerprint of the packet, and they determine if the packet is unique or similar to other packets. Traditionally, an IP flow is based on a set of five, and as many as seven, IP packet attributes. The following are the IP packet attributes that NetFlow can use:

- IP source address
- IP destination address
- Source port
- Destination port
- Layer 3 protocol type
- CoS
- Router or switch interface

All packets with the same source and destination IP address, source and destination ports, protocol, interface, and CoS are grouped into a flow and then packets and bytes are tallied. This methodology of fingerprinting or determining a flow is scalable because a large amount of network information is condensed into a database of NetFlow information that is called the NetFlow cache.

https://t.me/learningnets

Overview of Netflow (Cont.)

NetFlow Data Export Versions

Version	Description
1	Original
5	Standard and most common
7	Specific to Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers. Similar to version 5, but does not include AS, interface, TCP flag, and ToS information
8	Choice of 11 aggregation schemes, reduces resource usage
9	Flexible, extensible file export format to enable easier support of additional fields and technologies. Coming out now are MPLS, multicast, and BGP next-hop

© 2014 Cisco Systems, Inc.

NetFlow version 1 was the original format that was supported in Cisco IOS Software releases containing NetFlow functionality, but it is rarely used today. NetFlow version 5 is a later enhancement that adds BGP AS information and flow sequence numbers. NetFlow version 7 is an enhancement that adds NetFlow support for Cisco Catalyst switches that use hybrid or native mode. NetFlow version 8 is the NetFlow export format to use when you enable router-based NetFlow aggregation on Cisco IOS router platforms.

Note NetFlow versions 2, 4, and 6 were not released and are not supported.

NetFlow version 9 is a flexible and extensible means to carry NetFlow records from a network node to a collector. NetFlow version 9 has definable record types and is self-describing for easier NetFlow collection engine configuration. The following are characteristics of NetFlow version 9:

Templates define record formats.

The router sends the template descriptions to the NetFlow Collection Engine.

The router sends flow records to the NetFlow Collection Engine with minimal template information so that the NetFlow Collection Engine can relate the records to the appropriate template.

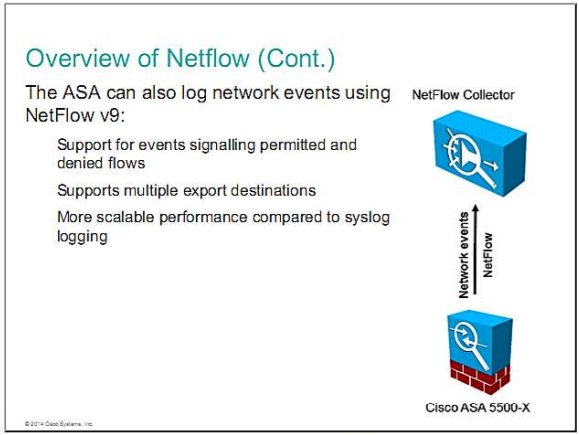
Version 9 is independent of the underlying transport protocol (UDP, TCP, SCTP, and so on).

NetFlow services provide access to information about IP flows within their data networks. You can use exported NetFlow data for various purposes, including network management and planning, enterprise accounting and departmental charge-backs, ISP billing, data warehousing, and marketing.

The main feature of the NetFlow Version 9 export format is that it is template-based. A template describes a NetFlow record format and the attributes of the fields (such as type and length) within the record. The router assigns each template an ID, which is communicated to the NetFlow Collection Engine along with the template description. The template ID is used for all further communication from the router to the NetFlow Collection Engine.

The basic output of NetFlow is a flow record. In NetFlow Version 9, a flow record follows the same sequence of fields as specified by the template definition. The template to which NetFlow records belong is determined by adding the template ID to the group of NetFlow records.

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



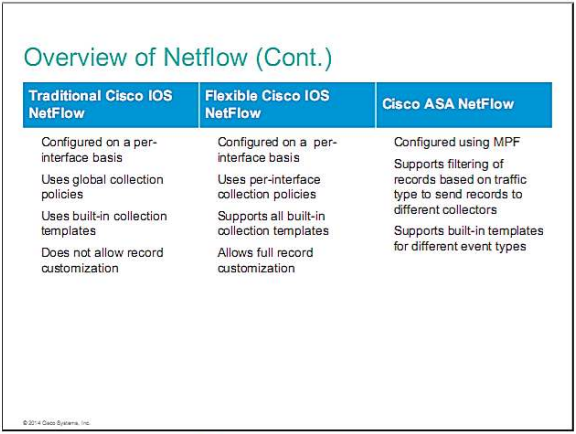
NetFlow efficiently provides an important set of services for IP applications, including network traffic accounting, usage-based network billing, network planning, security, DoS monitoring, and network monitoring. NetFlow provides valuable information about network users and applications, peak usage times, and traffic routing.

The Cisco ASA 5500-X Series support NetFlow version 9 to provide NSEL. NSEL allows specific, high-volume traffic-related events to be exported from the adaptive security appliance in a more efficient and scalable manner compared to classic syslog logging. You can use any NetFlow version 9 capable collector to receive adaptive security appliance NetFlow data.

The adaptive security appliance implementation of NSEL is a stateful, IP flow-tracking method that exports only those records that indicate significant events in a flow. In stateful flow tracking, tracked flows go through a series of state changes. NSEL events are used to export data about flow status, and are triggered by the event that caused the state change. The significant events that are tracked include flow-create, flow-teardown, and flow-denied (excluding flows that are denied by EtherType ACLs). Each NSEL record has an event ID and an extended event ID field, which describes the flow event.

The Cisco ASA adaptive security appliance supports multiple NetFlow export destinations and can therefore store its NetFlow information on multiple NetFlow collectors.

https://t.me/learningnets



Cisco IOS Software has supported NetFlow accounting and data export for a long time. Recently, Cisco has introduced the second generation of NetFlow technology named Flexible NetFlow, which provides greater flexibility and scalability when deploying NetFlow-based telemetry solutions.

"Traditional" Cisco IOS NetFlow technology is configured on OSI Layer 3 devices on a per-interface basis, and configured with global collection policies that influence how a device will collect traffic data and build NetFlow caches. You can use the built-in collection templates to choose the most suitable set of data to be collected based on a specific monitoring requirement. Additionally, besides using pre-defined collection policies, traditional NetFlow therefore does not support flow record customization by the device administrator.

Flexible Cisco IOS NetFlow lifts most of these limitations. While Flexible NetFlow is still configured on a per-interface basis, monitoring all flows over a particular interface, it can use per-interface collection policies to differentiate traffic collection based on per-interface requirements. While still supporting built-in collection profiles that define the data that is to be collected, Flexible NetFlow allows for full customization of data collection, as well as customization of data export using customizable flow records.

The Cisco ASA implementations of NetFlow (NSEL) is different that on Cisco IOS. NSEL provide a stateful, IP flow tracking method that exports records that indicate significant events in a flow. In stateful flow tracking, tracked flows go through a series of state changes. NSEL events are used to export data about flow status and are triggered by the event that caused the state change.

The significant events that are tracked include flow-create, flow-teardown, flow-denied (excluding those flows that are denied by EtherType ACLs), and flow-update. In addition, the ASA implementation of NSEL generates periodic NSEL events and flow-update events to provide periodic byte counters over the duration of the flow. These events are usually time-driven, which makes them more in line with traditional Netflow; however, these events may also be triggered by state changes in the flow.

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

The ASA implementations of NSEL provide the following major functions:

Filters NSEL events based on the traffic and event type through Modular Policy Framework, then sends records to different collectors. Traffic is matched based on the order in which classes are configured. After a match is found, no other classes are checked. The supported event types are flow-create, flow-denied, flow-teardown, flow-update, and all. Records can be sent to different collectors. For example, with two collectors, you can do the following:

Sends template information periodically to NSEL collectors. Collectors receive template definitions, normally before receiving flow records.

Tracks configured NSEL collectors and delivers templates and data records to these configured NSEL collectors through NetFlow over UDP only.

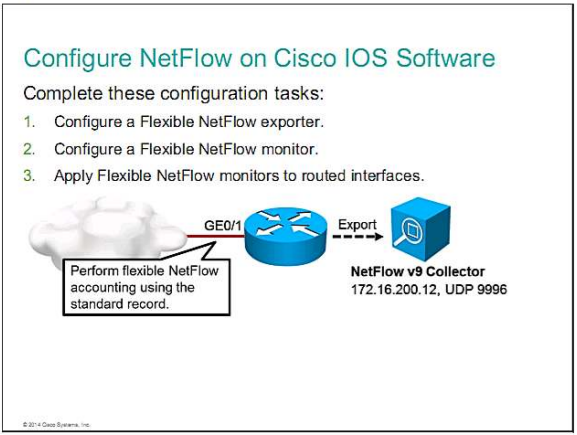
Defines and exports templates that describe the progression of a flow. Templates describe the format of the data records that are exported through NetFlow. Each event has several record formats or templates associated with it.

Tracks flow-create, flow-teardown, and flow-denied events, and generates appropriate NSEL data records.

https://t.me/learningnets

Configure NetFlow on Cisco IOS Software

This topic explains how to configure Netlow on Cisco IOS Software.

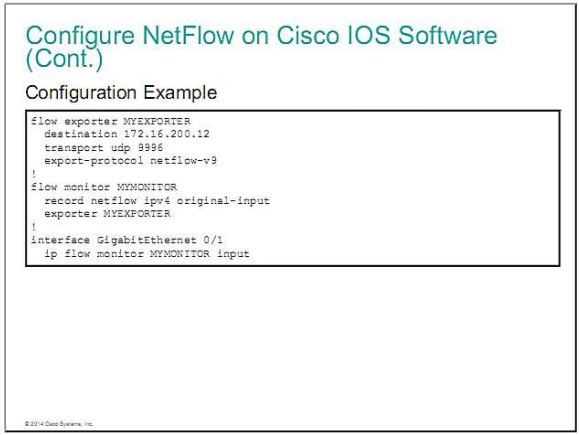


This lesson focuses only on configuring Flexible NetFlow. To configure Flexible NetFlow on a Cisco IOS Software router, perform the following tasks:

1. First, configure a Flexible NetFlow exporter, which is a Cisco IOS Software configuration entity that defines the export destinations for the local Flexible NetFlow monitoring functions of the router.
2. Then, configure a Flexible NetFlow monitor, which defines which data is collected from network flows over network interfaces.
3. Finally, apply the configured Flexible NetFlow monitor to a network interface or multiple network interfaces.

The figure also shows configuration scenario. You will configure NetFlow accounting on the GigabitEthernet 0/1 interface. You will collect network telemetry using the original NetFlow record, and export all flow data to the NetFlow collector at 172.16.200.12 using NetFlow version 9 export.

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



In the first task of Flexible NetFlow configuration, you must configure a Flexible NetFlow exporter that defines how NetFlow data will be exported from the network device to the NetFlow collector. For this purpose, you need to obtain the IP address, listening protocol and port, and the NetFlow data export format version about the remote NetFlow collector.

Follow these steps to create NetFlow exporter:

Use the **flow exporter** global configuration command to create a named Flexible NetFlow exporter. This example uses the MYEXPORTER Flexible NetFlow exporter.

Inside the flow exporter object, define the location and properties of the remote NetFlow collector using the **destination**, **transport**, and **export-protocol** commands.

In the second task, you must configure a Flexible NetFlow monitor that will define the data to be monitored on a network interface and the exporters that will be used with this monitor. The flow monitor has two major components: the flow record and the flow exporter. The flow record defines what information NetFlow will track and tells NetFlow what information to obtain from the packets being forwarded.

Follow these steps to configure a flow monitor:

Use the **flow monitor** global configuration command to create a named Flexible NetFlow monitor. This example uses the MYMONITOR Flexible NetFlow monitor.

Inside the flow monitor object, define data that will be collected by this monitor by specifying the NetFlow record type. You can use a predefined record type or create a custom record that specifies the data you want to monitor. In this example, the **record netflow ipv5 original-input** record format specifies that the default traditional NetFlow data set should be monitored and exported.

Specify the Flexible NetFlow exporter to be used with this monitor using the **exporter** command. The example uses the previously configured MYEXPORTER Flexible NetFlow exporter.

Finally, in Task 3, apply the configured flow monitor to the routed interface using the **ip flow monitor** command, and reference the configured named flow monitor names. You can apply the flow monitors to track input or output flows on an interface. This example applies the "traditional"-record-based flow monitor, MYMONITOR to the GigabitEthernet0/1 routed interfaces.

https://t.me/learningnets

To configure Flexible NetFlow on the Cisco router, use the commands that are described in this table:

Commands	Description
flow exporter MYEXPORTER **destination 172.16.200.12** **transport udp 9996** **export-protocol netflow-v9**	Configures NetFlow exporter.
flow monitor MYMONITOR **record netflow ipv4 original-input** **exporter MYEXPORTER**	Configures NetFlow monitor.
interface GigabitEthernet 0/1 **ip flow monitor MYMONITOR input**	Applies NetFlow monitor to the interface in the input direction.

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

Verify NetFlow on Cisco IOS Software

This topic explains how to verify NetFlow on Cisco IOS Software.

Verify NetFlow on Cisco IOS Software

NTP Verification Commands	Description
show flow exporter statistics	Shows NetFlow data export statistics for all exporters
show flow monitor name *name* **cache format table**	Shows the contents (flows) in a specific monitor's cache

© 2014 Cisco Systems, Inc.

Use the following command to verify NetFlow on Cisco IOS devices:

To display Flexible NetFlow flow exporter status and statistics, use the **show flow exporter** command in privileged EXEC mode.

To display the status and statistics for a Flexible NetFlow flow monitor, use the **show flow monitor** command in privileged EXEC mode.

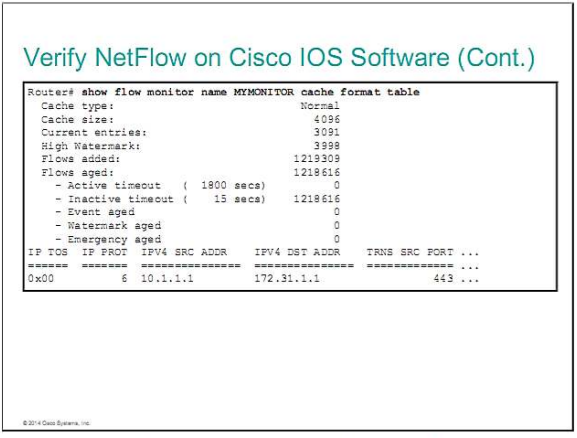
Verify NetFlow on Cisco IOS Software (Cont.)

```
Router# show flow exporter statistics
Flow Exporter MYEXPORTER:
  Packet send statistics:
    Ok 86
    No FIB 0
    Adjacency failure 0
    Enqueued to process level 0
<output omitted>
  Client send statistics:
    Client: Flow Monitor MYMONITOR
      Records added 1497
      Packets sent 86 (82024 bytes)
      Packets dropped 0 (0 bytes)
      No Packet available errors 0
```

© 2014 Cisco Systems, Inc.

https://t.me/learningnets

To verify basic Flexible NetFlow operation, it is useful to verify that data is being exported to the defined flow exporters. Use the **show flow exporter statistics** command to observe statistics for all defined Flexible NetFlow exporters. Non-zero statistics will typically indicate a working NetFlow system.

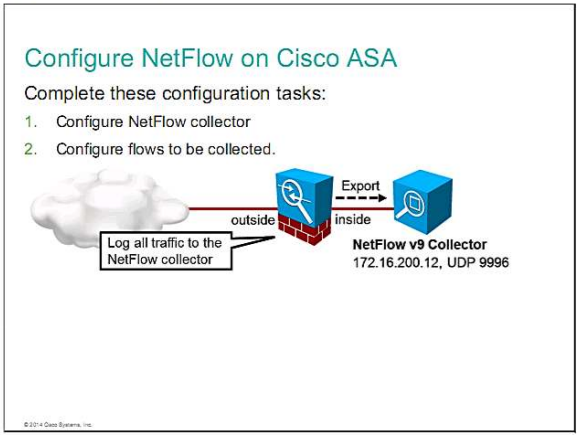


You can also examine the NetFlow caches created by Flexible NetFlow flow monitors. Non-empty caches are a good indication that NetFlow is working properly on a particular interface that uses a specific flow monitor. Use the **show flow monitor name cache** command to examine the NetFlow cache of a particular named flow monitor. Note that there are multiple formats in which the cache can be presented in the CLI: flow-record-based, table-based, or CSV-based. The example shows the table-based format.

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

Configure NetFlow on Cisco ASA

This topic explains how to configure NetFlow on the Cisco ASA.

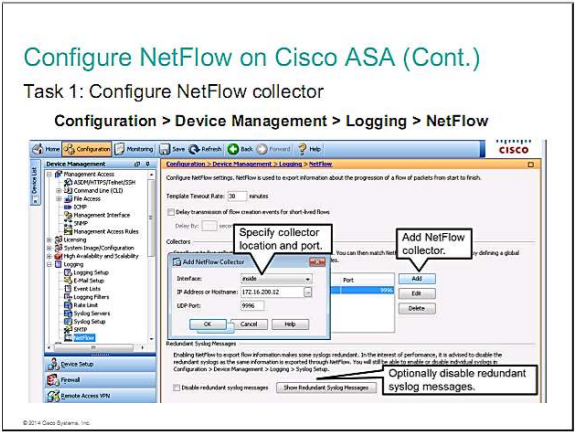


To configure NetFlow on the Cisco ASA, complete the following tasks:

1. Globally configure NetFlow collector
2. Configure flows that need to be collected using Cisco ASA MPF.

The figure also shows configuration scenario. You will configure NetFlow accounting of all traffic traversing the Cisco ASA. You will configure the ASA te export flow data to the NetFlow collector at 172.16.200.12.

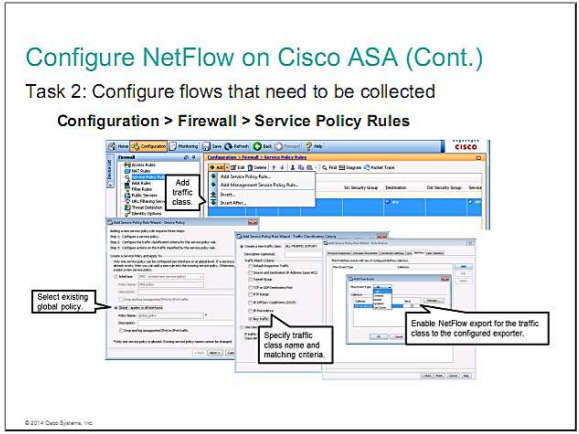
https://t.me/learningnets



To configure NetFlow export destinations by specifying the location of NetFlow collectors, perform the following steps:

1. Click the **Configuration** button in the Cisco ASDM toolbar.
2. Choose **Device Management** from the navigation pane.
3. Expand the **Logging** option from the Device Management menu.
4. Choose **NetFlow**. The NetFlow configuration panel appears.
5. Click the **Add** button to add one or more NetFlow collector addresses. Select an interface trough which the collector is accessible, specify an IP address of the collector, and specify UDP port. In the example, NetFlow collector at 172.16.200.12 is configured, with UDP port 9996.
6. Click **OK**.
7. Click **Apply** to apply the configuration.

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

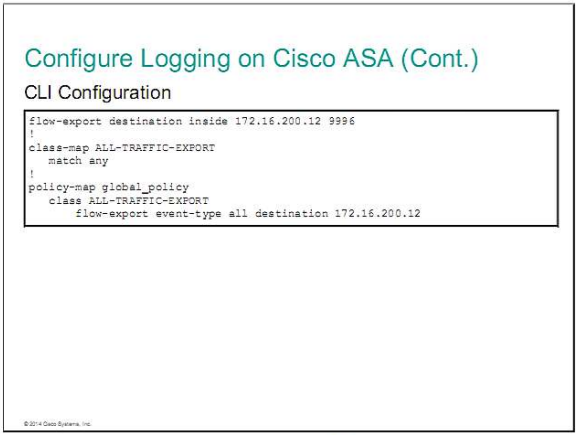


Defining the flows to be exported to NetFlow collectors is configured using Cisco ASA MPF. With Cisco ASA NetFlow, you can granularly select which flows through the adaptive security appliance are subject to NetFlow export, based on flow properties such as IP addresses, protocols, and ports.

Follow these steps to define the flows that will be exported to NetFlow collectors:

1. Click the **Configuration** button in the Cisco ASDM toolbar.
2. Choose **Service Policy Rules** from the navigation pane. In the Service Policy Rules, select the preconfigured inspection_default traffic class in the preconfigured default global policy. Click **Add**, and then select **Insert After** option from the menu. The Add Service Policy Rule Wizard is displayed.
3. Select the **Global - applies to all interfaces** radio button. Click **Next**.
4. in the next window of the wizard, first specify name of the traffic class that will describe flows that need to be exported to NetFlow exporters. In the example, ALL-TRAFFIC-EXPORT is used as the name. Then select a criteria how traffic class will be described. In the example, **Any traffic** is used to match all traffic. Click **Next**.
5. In the next window of the wizard, select the **NetFlow** tab. Click **Add** to add export of traffic to the preconfigured collector. The Add Flow Event window is displayed.
6. Check the checkbox next to the displayed configured collector in the **Send** column. Optionally select flow event type from the drop-down menu to export only flows about specific events. In the example, all events will be exported.
7. Click **OK**.
8. Click **Finish** to close the wizard and **Apply** to apply the configuration.

https://t.me/learningnets



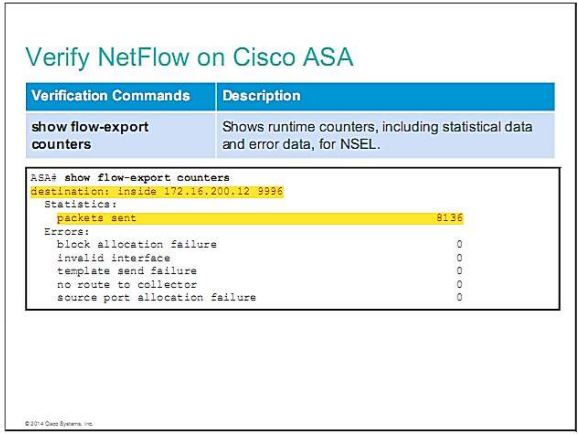
In the CLI, use the following commands to configure NetFlow.

Commands	Description
flow-export destination inside 172.16.200.12 9996	Configures NetFlow collector destination, outgoing interface and UDP port.
class-map ALL-TRAFFIC-EXPORT **match any**	Creates a traffic class and specifies matching criteria.
policy-map global_policy **class ALL-TRAFFIC-EXPORT** **flow-export event-type all destination 172.16.200.12**	Refers to the traffic class in a policy map, and configures export of flows that match the traffic class to the NetFlow exporter.

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

Verify NetFlow on Cisco ASA

This topic explains how to verify NetFlow on the Cisco ASA.

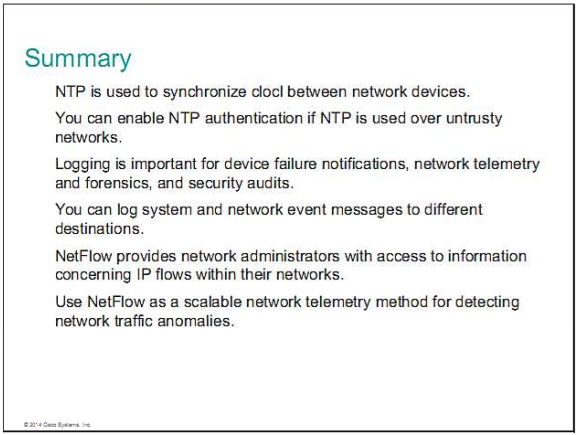


Use the **show flow-export counters** command to show runtime counters, including statistical data and error data, for NSEL. Non-zero statistics for packet sent will typically indicate a working NetFlow system.

https://t.me/learningnets

Summary

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



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

Lesson 6

Deploying Cisco IOS Layer 2 Data Plane Security Controls

Overview

Cisco IOS Software on Cisco switches provides data plane security controls that can mitigate the risks that are associated with OSI Layer 2 attacks inside a VLAN. This lesson enables you to configure and verify several of the Cisco IOS Software security features that you can use to reduce these risks in your switched network environment.

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

- Describe Cisco switched data plane security controls
- Describe a PVLAN
- Describe how to configure a PVLAN
- Describe how to verify a PVLAN
- Describe DHCP control
- Describe how to configure DHCP snooping
- Describe how to verify DHCP snooping
- Describe ARP control
- Describe how to configure DAI
- Describe how to verify DAI
- Describe storm control
- Describe how to configure storm control
- Describe how to verify storm control
- Describe MACsec encryption

https://t.me/learningnets

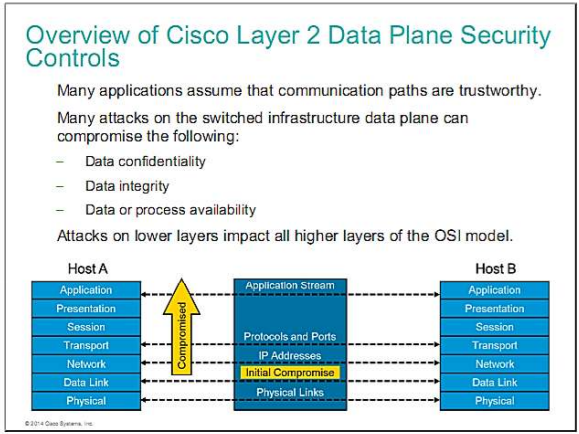
Describe how to configure MACsec encryption

Describe how to verify MACsec encryption

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

Overview of Cisco Layer 2 Data Plane Security Controls

This topic describes Cisco switched data plane security controls.



Many modern applications assume that the communication paths used between application endpoints are trustworthy. Therefore, the applications themselves do not have to provide transmission security features when they operate in a distributed fashion over a network. Additionally, it may be suboptimal to add cryptographic protection to all application traffic, because the network would be blind to application-layer features and could not provide some advanced security and performance-related services to applications.

With applications running in cleartext over many networks, attackers can use low-level attacks against the infrastructure data (forwarding) plane to compromise data confidentiality, data integrity, and data or process availability. Note that any attacks that successfully compromise data on such a low level also affect all the higher layers in the OSI stack. For example, an attacker that can intercept all cleartext IP traffic to and from a host can observe, hijack, and impersonate users of application sessions running over IP.

The threats of passive (sniffing) and active (man-in-the-middle) traffic capture, active traffic changing, and active traffic spoofing can be managed by both of the following:

Network countermeasures in the switched infrastructure (for example, ARP inspection, and DHCP snooping)

Cryptographic traffic protection (for example, IEEE 802.1AE MACsec)

https://t.me/learningnets

Overview of Cisco Layer 2 Data Plane Security Controls (Cont.)

Attack	Switched Infrastructure Countermeasure
VLAN hopping	Static access ports, disabling of DTP, avoidance of trunk native VLAN on access ports
STP spoofing	BPDU Guard/Root Guard
MAC spoofing	Port security
CAM flooding	Port security (MAC limit)
DHCP server spoofing	DHCP snooping
DHCP starvation	Port security (MAC limit) *or* DHCP snooping rate limit
ARP spoofing	ARP inspection
Traffic capture	MACsec

© 2014 Cisco Systems, Inc.

This table presents common attacks that are mounted inside switched infrastructures, and the security countermeasures that switched infrastructure devices offer. Common attacks include the following:

VLAN hopping attacks: The attacker attempts to inject frames that allow the attacker to access VLANs that should not be accessible on a particular port. Properly configuring static access ports, disabling the DTP, and avoiding trunk native VLANs on access ports mitigate this common vulnerability.

Spanning Tree Protocol spoofing: The attacker attempts to influence STP operation and divert traffic, or black-hole traffic, from the access layer. Effective countermeasures include using the BPDU guard and root guard features on network switches.

MAC address spoofing: The attacker attempts to steal the identity of endpoints, through diverting or black-holing traffic that is destined to them, by using a spoofed MAC address and poisoning switch-forwarding tables with it. Effective network defenses include the port security feature.

CAM table flooding: The attacker attempts to overflow the switch CAM table and cause sensitive traffic to flood all switch ports. A very effective countermeasure is to limit the number of allowed MAC addresses for each access port.

DHCP server spoofing: The attacker acts as a legitimate DHCP server in the network and maliciously configures clients to use it as the DNS server or default gateway, allowing the attacker to intercept client traffic. Deploying the Cisco IOS Software DHCP snooping feature effectively defends against this threat.

DHCP starvation: The attacker attempts to use all available DHCP-assigned addresses in the network to deny DHCP service to legitimate users. Limiting the maximum number of MAC addresses per port, or a DHCP rate limiting function, provide two layers of defense against these threats.

ARP spoofing: The attacker attempts to redirect traffic inside a subnet to intercept sensitive flows or spoof endpoint identities. The Cisco IOS Software ARP inspection feature provides an effective control that thwarts this threat.

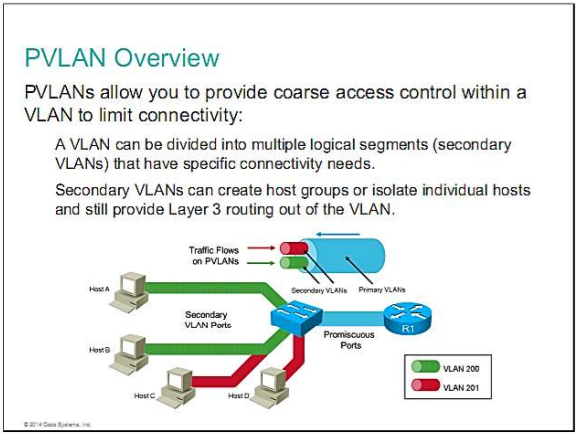
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Traffic capture/changing attacks: The attacker captures or changes and spoofs traffic using man-in-the-middle attacks. Inside the switched infrastructure, the MACsec feature provides cryptographic traffic protection against the attacks.

https://t.me/learningnets

PVLAN Overview

This topic describes PVLANs.



Many organizations often support many different network endpoints (such as clients, servers, and multimedia devices) that share the same network segment or VLAN. As security issues proliferate, it may become necessary to provide some form of coarse access control—such as traffic isolation—between devices, though they may exist on the same Layer 3 segment or VLAN. A traditional solution for addressing these requirements is to provide one VLAN per device type, with each VLAN having its own IP subnet. A Layer 3 device then provides interconnectivity between VLANs and other destinations.

Several challenges exist with this traditional solution:

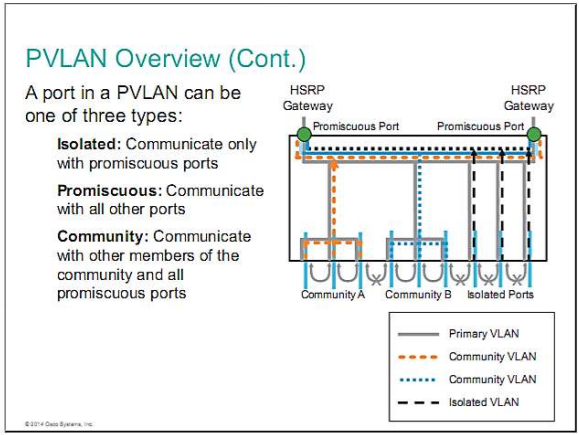
- Supporting a separate VLAN per device type can require a high number of interfaces on network devices.
- The spanning tree becomes more complicated with many VLAN iterations.
- The network address space must be divided into many subnets, which wastes space and increases management complexity.
- Multiple ACL applications are required to maintain security on multiple VLANs and results in increased management complexity.

PVLANs are a Cisco IOS Software feature that can provide Layer 2 isolation between ports within the same VLAN. This isolation eliminates the need for a separate VLAN and IP subnet per customer and provides a coarse access control mechanism that is easy to manage.

PVLANs introduce the concept of a primary VLAN, which is the VLAN to which all devices belong, and hosts a particular OSI Layer 3 subnet. Inside this VLAN, you can create secondary VLANs to create host groups (or communities) or to isolate hosts from one another, while still providing classic Layer 3 routing into and out of the primary VLAN.

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

In the example, Host A and Host B are attached to the PVLAN ports that belong to secondary VLAN 200. Host C and Host D are attached to the PVLAN ports in secondary VLAN 201. The policy that is applied to the secondary VLANs determines the type of connectivity inside a secondary VLAN and between secondary VLANs.



A port in a PVLAN can be one of three types:

Isolated port: These ports are access ports that are assigned to a secondary VLAN of an isolated type. An isolated port has complete Layer 2 separation from other ports within the same primary PVLAN, except from promiscuous ports (where you typically connect routers or other Layer 3 devices). PVLANs block all traffic to isolated ports, except the traffic from promiscuous ports. Traffic that is received from an isolated port is forwarded only to promiscuous ports. Hosts that are connected to these ports are therefore isolated from all other hosts in the primary VLAN.

Promiscuous port: These ports are access ports that are assigned only to a primary VLAN and typically connect to a router or firewall. A promiscuous port can communicate with all ports within the primary VLAN, including all community and isolated ports that are also members of their respective secondary VLANs. The default gateway for the segment would likely be hosted on a promiscuous port, given that all devices in the PVLAN need to communicate with that port.

Community port: These ports are access ports that are assigned to a secondary VLAN of a community type. Community ports can communicate with other ports in the same community secondary VLAN and with all promiscuous ports. These interfaces are isolated at Layer 2 from all other interfaces in other communities (or other community secondary VLANs) or any isolated ports within their primary VLAN. A community secondary VLAN therefore defines a group of ports that has any-to-any connectivity inside the same secondary VLAN and connectivity to the outside world via the promiscuous port.

Keep these restrictions in mind when configuring PVLANs:

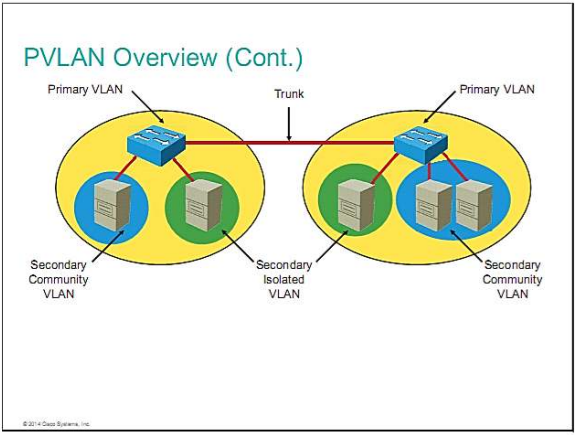
PVLAN trunk ports support only IEEE 802.1Q encapsulation.

An isolated or community VLAN can have only one primary VLAN associated with it.

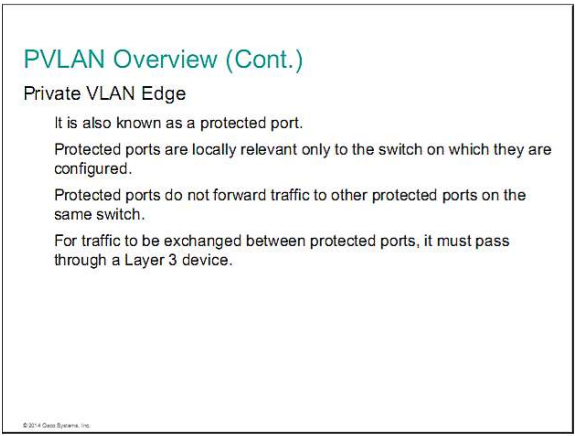
VTP does not support PVLANs. Configure PVLANs on each device on which you want PVLAN ports.

https://t.me/learningnets

For PVLANs, the VTP mode must be transparent, not client or server.



You can apply PVLAN functionality across multiple switches, with special configuration on the interswitch trunk port. The functionality that is provided by the secondary VLANs is transparently preserved, though the ports are located on different switches. For example, an isolated port on one switch cannot talk to any other ports on any other switches, except for promiscuous ports on all switches.



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

PVLANs are not supported on every Cisco switch. However, a similar Cisco IOS Software feature—Private VLAN Edge—provides functionality like isolated secondary VLANs on a standalone switch. Protected ports, also referred to as the Private VLAN Edge, have the following specific features:

The switch does not forward any data traffic (unicast, multicast, or broadcast) from one protected port to any other protected port. Only control traffic is forwarded, because control traffic packets are processed by the CPU and forwarded in software. All data traffic that needs to pass between protected ports must be forwarded through a Layer 3 device.

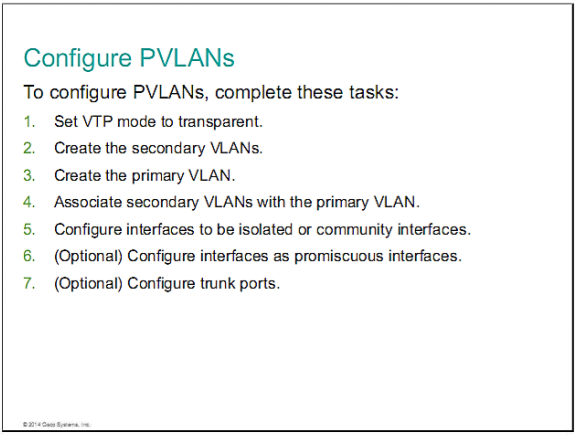
The forwarding behavior between a protected port and an unprotected port proceeds as usual. For example, on a switch that is configured with 12 protected and 12 unprotected ports, the 12 unprotected ports can normally and bidirectionally communicate with all hosts on the protected ports.

Note Isolation is not provided between two protected ports that are located on different switches. To prevent communication between protected ports on different switches, configure the protected ports for unique VLANs on each switch and configure a trunk link between the switches.

https://t.me/learningnets

Configure PVLANs

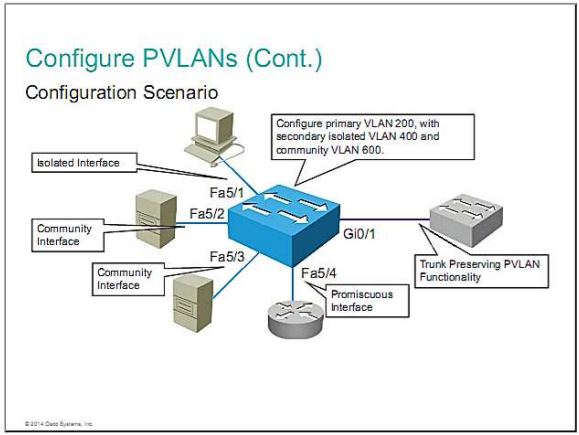
This topic describes how to configure PVLANs.



To deploy PVLAN functionality, complete the following sequence of configuration tasks:

1. Set the VTP mode on all involved switches to transparent.
2. Create the (isolated and community) secondary VLANs.
3. Create the primary VLAN.
4. Associate the secondary VLANs to the primary VLAN. You can map only one isolated VLAN to a primary VLAN, but you can map more than one community VLAN to a primary VLAN.
5. Configure an interface to be an isolated or community port by associating it with the appropriate secondary and primary VLAN.
6. (Optional) Configure an interface as a promiscuous port and associate it with all the secondary VLANs and the primary VLAN. Typically, you will configure the ports on which your router or firewall interfaces connect to the switch as promiscuous.
7. (Optional) In multiswitch PVLAN environments, configure PVLAN functionality on the interswitch trunk ports.

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



The figure shows the configuration scenario that is used for the configuration sequence. On the Cisco switch, configure VLAN 200 as the primary VLAN, with the secondary VLANs 400 (isolated VLAN) and 600 (community VLAN).

On the switch, configure the following:

Interface FastEthernet5/1 as an isolated interface to prevent the host that is attached to the interface from communicating to all other ports, except all promiscuous ports

Interface FastEthernet5/2 and FastEthernet5/3 as community interfaces to allow the host that is attached to the interface to communicate to other community ports and all promiscuous ports

Interface FastEthernet5/4 as a promiscuous interface, because it is connected to the default gateway router

Interface the GigabitEthernet0/1 trunk interface in a manner that preserves PVLAN-based separation on the neighboring switch

https://t.me/learningnets

Configure PVLANs (Cont.)

Configuration Example

```
vtp mode transparent
!
vlan 600
  private-vlan community
vlan 400
  private-vlan isolated
vlan 200
  private-vlan primary
  private-vlan association 400,600
!
interface FastEthernet 5/1
  switchport mode private-vlan host
  switchport private-vlan host-association 200,400
interface range FastEthernet 5/2 - 3
  switchport mode private-vlan host
  switchport private-vlan host-association 200,600
interface FastEthernet 5/4
  switchport mode private-vlan promiscuous
  switchport private-vlan mapping 200,400,600
interface GigabitEthernet0/1
  switchport mode trunk
  switchport trunk encapsulation dot1q
```

©2014 Cisco Systems, Inc.

In Tasks 1 to 4 of the configuration, you will configure VTP in transparent mode and create all required VLAN information on the switch.

In this example, you will first set VTP to operate in transparent mode using the **vtp mode transparent** global configuration command.

Then, create VLAN 600 using the **vlan** global configuration command. Configure it as a community VLAN using the **private-vlan community** command in VLAN configuration mode.

Next, create VLAN 400 using the **vlan** global configuration command. Configure it as an isolated VLAN using the **private-vlan isolated** command in VLAN configuration mode.

After the two secondary VLANs have been configured, you can create the primary VLAN 200 using the **vlan** global configuration mode command. Configure it as the primary VLAN using the **private-vlan primary** command in VLAN configuration mode.

While in VLAN 200 configuration mode, associate secondary VLANs 400 and 600 with this primary VLAN using the **private-vlan association** command.

Note Only one isolated VLAN can be associated with any individual primary VLAN.

In Tasks 5 and 6 of the overall configuration sequence, you will place individual interfaces (ports) to be members of appropriate secondary and primary VLANs, depending on the desired connectivity inside the primary VLAN.

The example configures three access interfaces, each interface differently. In the first instance, FastEthernet5/1 is first enabled for private VLANs using the **switchport mode private-vlan host** interface command. It is then configured as an isolated port by being assigned to VLAN 400, which was previously defined as an isolated VLAN. The interface is associated with VLAN 200 as its primary VLAN and VLAN 400 as its secondary (isolated) VLAN using the **switchport private-vlan host-association** command. This interface can therefore only exchange traffic with any defined promiscuous ports.

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

Next, interfaces FastEthernet5/1 and FastEthernet5/2 are enabled for private VLANs using the **switchport mode private-vlan host** interface command. The interfaces are configured as community ports by being assigned to VLAN 600, which was previously defined as a community VLAN. The port is associated with VLAN 200 as its primary VLAN, along with VLAN 600 as its secondary (community) VLAN using the **switchport private-vlan host-association** command. This interface can, therefore, only exchange traffic with any other interfaces that are configured in the same secondary and primary VLANs, and with any defined promiscuous ports.

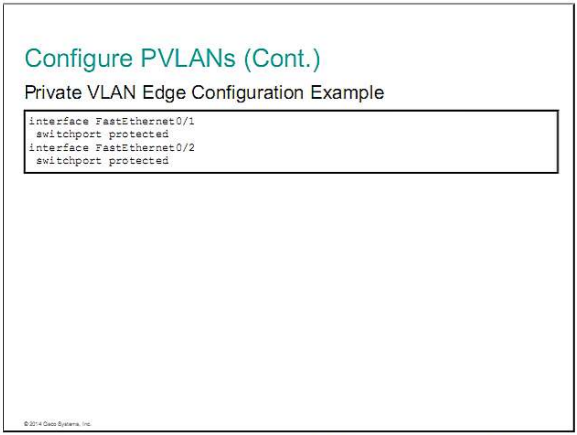
Because most PVLAN implementations require promiscuous ports for the routers or firewalls, or both, FastEthernet5/4 is enabled for private VLANs using the **switchport mode private-vlan host** interface command. This port is configured as a promiscuous port for secondary VLAN 400 and 600 using the **switchport private-vlan mapping** command. This port is used to route traffic in and out of the primary VLAN (200) using a Layer 3 device.

Finally, in the last (optional) task, you can configure a trunk port between switches to support distributed PVLAN functionality. You do not have to configure any special PVLAN-specific commands on the trunk port. Ensure that the trunk port allows the forwarding of both the primary and secondary VLANs. You can use the **switchport mode trunk**, the **switchport trunk encapsulation dot1q**, and the optional (and recommended) **switchport trunk allowed vlan** command to select specific VLANs allowed on the trunk interface.

To configure a PVLAN on a Cisco switch, use the commands that are described in the table.

Commands	Description
vtp mode transparent	Sets VTP mode to transparent.
private-vlan community	Creates a secondary community VLAN.
private-vlan isolated	Creates a secondary isolated VLAN.
private-vlan primary	Creates a primary VLAN.
private-vlan association *vlans*	Associates secondary VLANs with the primary VLAN.
interface FastEthernet 5/1 **switchport mode private-vlan host** **switchport private-vlan host-association 200,400**	Configures an isolated interface.
interface range FastEthernet 5/2 - 3 **switchport mode private-vlan host** **switchport private-vlan host-association 200,600**	Configures a community interface.
interface FastEthernet 5/4 **switchport mode private-vlan promiscuous** **switchport private-vlan mapping 200,400,600**	Configures a promiscuous interface.
interface GigabitEthernet0/1 **switchport mode trunk** **switchport trunk encapsulation dot1q**	Trunk ports do not require special PVLAN-related configuration.

https://t.me/learningnets



To define a port as a protected port, enter the command **switchport protected** in the interface configuration of the port you want to protect. Use the **show port protected** privileged EXEC command to display the port protected mode for all ports. The figure shows how to configure the FastEthernet0/1 port as a protected port and how to verify its PVLAN Edge configuration. The "Protected" status shows as *true* if the port in question is a protected port.

To configure Private VLAN Edge on a Cisco switch, use the command that is described in this table.

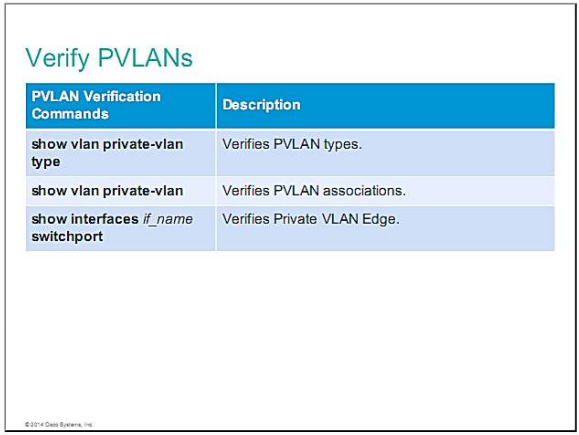
Command	Description
switchport protected	Enables Private VLAN Edge on the port.

Note Ports that are protected by Private VLAN Edge are subject to the same potential bypass problem as PVLANs where devices on unprotected ports relay traffic between protected ports. Use appropriate ACLs or firewall rules on these devices to prevent such forwarding.

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

Verify PVLANs

This topic describes how to verify PVLANs.



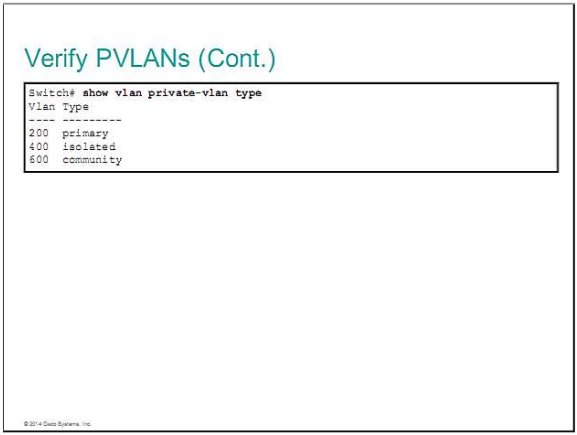
Cisco IOS Software includes rich PVLAN validation features.

Use the **show vlan private-vlan type** command to display all configured PVLANs and their individual types.

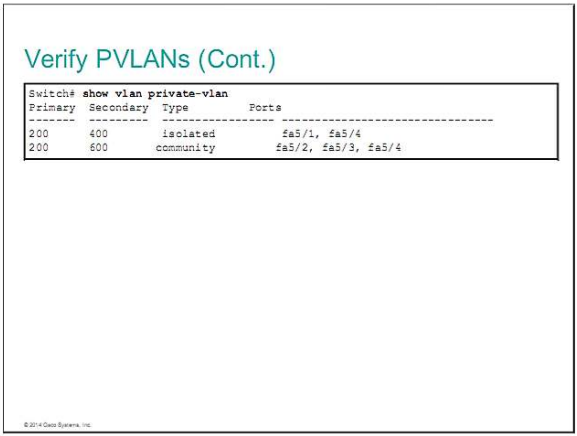
Use the **show vlan private-vlan** command to show the individual switch interfaces that are associated with PVLAN functionality.

Use the **show interfaces** *if_name* **switchport** command to display the Private VLAN Edge status of an interface.

https://t.me/learningnets

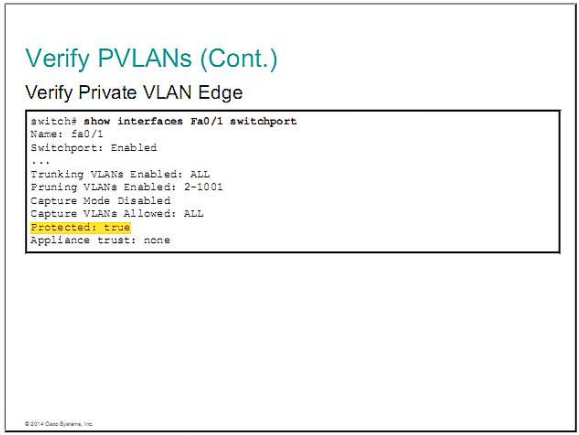


In the output of the **show vlan private-vlan type** command, you can see the configured primary VLAN 200, the isolated secondary VLAN 400, and the community secondary VLAN 600.



In the output of the **show vlan private-vlan** command, you can see the FastEthernet5/1 interface in the isolated secondary VLAN 400, and the FastEthernet5/2 and FastEthernet5/3 interfaces in the community secondary VLAN 600. The FastEthernet5/4 interface is a promiscuous interface that belongs to all secondary VLANs in a primary VLAN.

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

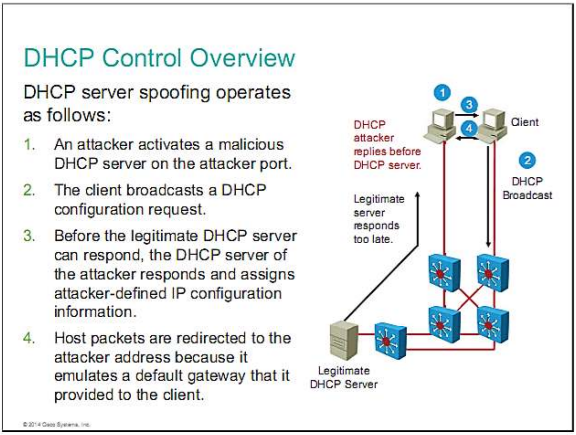


In the output of the **show interfaces Fa0/1 switchport** command, you can see the protected mode for all ports. The example shows how to verify its Private VLAN Edge configuration. The "Protected" status shows as "true" if the port in question is a protected port.

https://t.me/learningnets

DHCP Control Overview

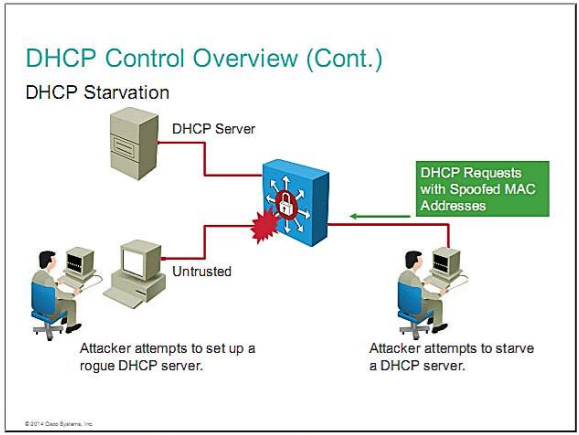
This topic describes DHCP control.



DHCP does not include authentication and is therefore vulnerable to spoofing attacks. The simplest attack is DHCP server spoofing. The attacker pretends to be the DHCP server and replies to DHCP requests from legitimate clients, causing either DoS—by providing incorrect information—or confidentiality or integrity breaches via a man-in-the-middle attack. The attackers can assign themselves as the default gateway or DNS server in all DHCP replies and later intercept all IP communication from the configured hosts to the rest of the network.

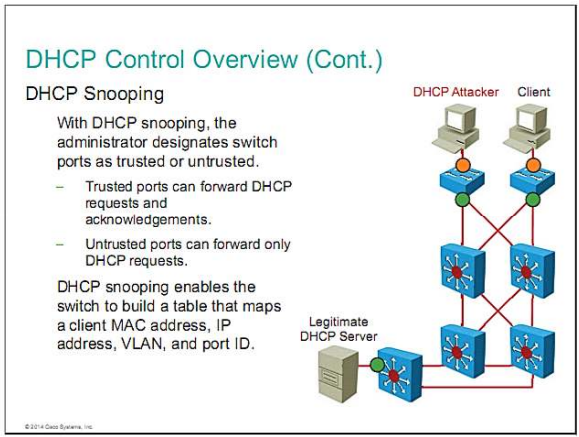
To mitigate this threat, you can use static IP addresses (which is obviously not scalable in large networks) or allow the infrastructure to use DHCP snooping to control DHCP traffic.

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



A DHCP starvation attack works by broadcasting DHCP requests with spoofed MAC addresses. If enough requests are sent, the network attacker can exhaust the address space that is available to the DHCP servers for a time. The network attacker can then set up a rogue DHCP server on the attacker system and respond to new DHCP requests from clients on the network.

To mitigate DHCP address exhaustion attacks, deploy port security address limits, which set an upper limit of MAC addresses that can be accepted into the CAM table from any single port. Because each DHCP request must be sourced from a separate MAC address, this practice effectively limits the number of IP addresses that can be requested from a switch port-connected attacker. Set this value to a number that is never legitimately exceeded in your environment.



https://t.me/learningnets

DHCP snooping is a Layer 2 security feature that specifically prevents DHCP server spoofing attacks and mitigates DHCP starvation to a degree. DHCP snooping provides DHCP control by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database, which is also referred to as a DHCP snooping binding table.

For DHCP snooping to work, each switch port must be labeled as trusted or untrusted. Trusted ports are the ports over which the DHCP server is reachable and that will accept DHCP server replies. All other ports should be labeled as untrusted ports and can only source DHCP requests. Typically, this means the following:

- All access ports should be labeled as untrusted, except the port to which the DHCP server is directly connected.
- All interswitch ports should be labeled as trusted.
- All ports that are pointing toward the DHCP server (that is, the ports over which the reply from the DHCP server is expected) should be labeled as trusted.

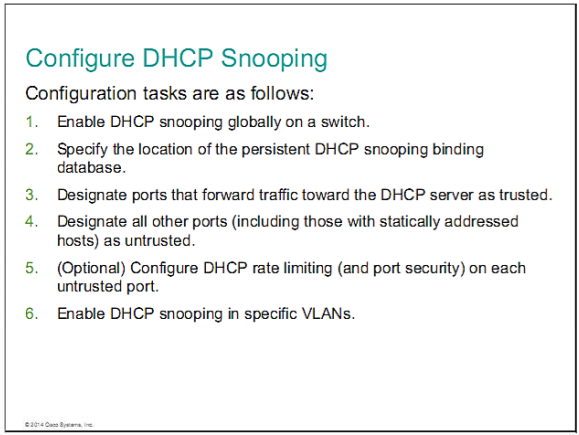
Untrusted ports are those ports that are not explicitly configured as trusted. A DHCP binding table is automatically built by analyzing normal DHCP transactions on all untrusted ports. Each entry contains the client MAC address, IP address, lease time, binding type, VLAN number, and port ID that is recorded as clients make DHCP requests. The table is then used to filter subsequent DHCP traffic. From a DHCP snooping perspective, untrusted access ports should not send any DHCP server responses, such as DHCPOFFER, DHCPACK, or DHCPNAK. The switch will drop all such DHCP packets.

The figure shows the deployment of DHCP protection mechanisms on the access layer of the network. User ports are designated as untrusted for DHCP snooping, while interswitch links are designated as trusted if the DHCP server is reachable through the network core. User ports also have limited MAC addresses to prevent DHCP address exhaustion.

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

Configure DHCP Snooping

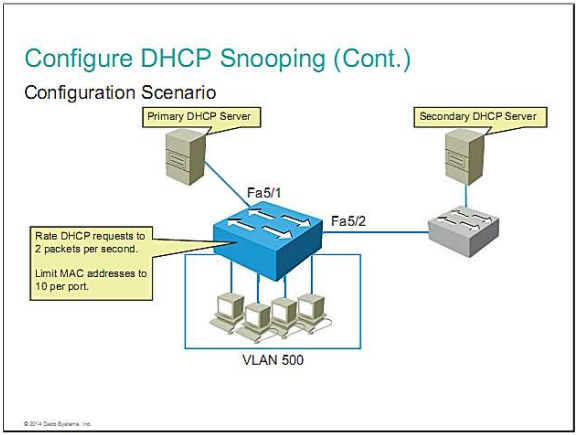
This topic describes how to configure DHCP snooping.



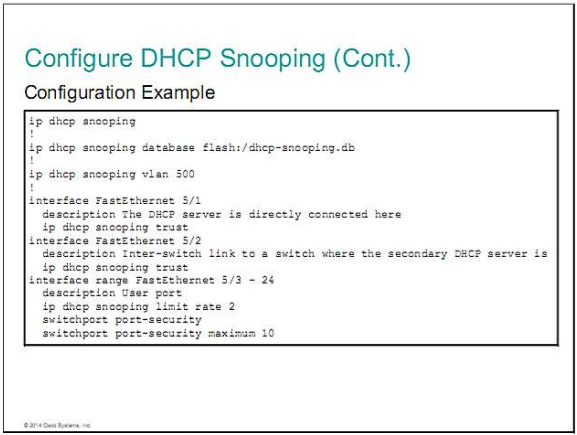
To deploy DHCP snooping, complete this sequence of configuration tasks on each switch:

1. Enable DHCP snooping globally on the switch.
2. Specify the location of the DHCP snooping binding database, which is a persistent list of learned port-MAC-IP-address mappings that is maintained by the DHCP snooping feature and stored either on the switch or on a remote file server. This database enables the switch to keep state about learned DHCP clients, even across reboots.
3. On the switch, designate all ports that forward traffic toward the legitimate DHCP servers as trusted for DHCP snooping.
4. On the switch, designate all other ports as untrusted for DHCP snooping. Note that all ports are, by default, considered untrusted.
5. Optionally, configure DHCP rate limiting on each untrusted port. It is also recommended that you enable port security to limit the maximum number of MAC addresses per port, which is a more effective countermeasure against DHCP starvation and also automatically prevents CAM flooding attacks.
6. Finally, enable DHCP snooping in all specific VLANs that require DHCP spoofing protection.

https://t.me/learningnets



This figure shows the configuration scenario for the DHCP snooping feature. The Cisco switch uses VLAN 500 to host DHCP-addressed clients. The primary DHCP server is directly connected to the FastEthernet5/1 interface, and the secondary DHCP server is reachable over the FastEthernet5/2 trunk port. The configuration sequence assumes that all ports and VLANs have been preconfigured to enable complete connectivity in VLAN 500 and that the DHCP infrastructure is already able to assign network configuration to clients in VLAN 500.



Start by enabling DHCP snooping globally on the switch using the **ip dhcp snooping** command.

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

In Task 2, specify the location of the persistent DHCP snooping binding database using the **ip dhcp snooping database** command. By default, the database is located in the local file system, but can be located off the switch on a remote server (Secure Copy Protocol [SCP], File Transfer Protocol [FTP], and so on). Ensure that the path to the remote server is trusted, or use cryptographically protected protocols (SCP).

In Tasks 3 and 4, configure an interface as *trusted* or *untrusted,* respectively, for DHCP snooping, using the **(no) ip dhcp snooping trust** interface command. The default state of an interface is untrusted.

In Task 5, (optionally) configure the number of DHCP packets per second that an interface can receive using the **ip dhcp snooping limit rate** interface command. The allowed range is 1 to 2048 DHCP packets per second. By default, no rate limit is configured. The typical recommended rate limit for an untrusted port is no more than five packets per second. If you configure rate limiting for trusted interfaces, you may need to increase the rate limit if the port is a trunk port that is assigned to more than one VLAN on which DHCP snooping is enabled.

It is generally preferred to use port security with an address limit to resolve DHCP address starvation attacks instead of, or in addition to, rate limiting.

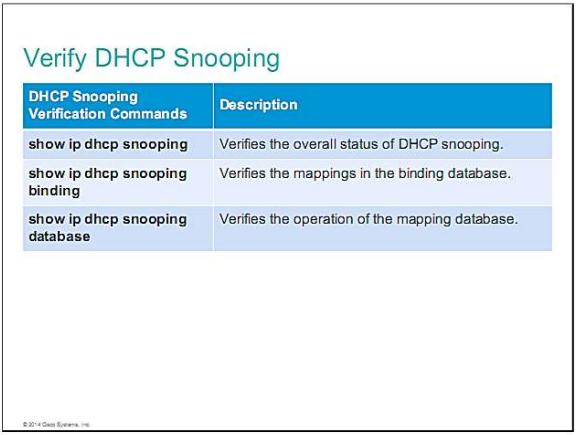
To configure DHCP snooping on a Cisco switch, use the commands that are described in this table:

Commands	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping database *location*	Configures the DHCP snooping binding database agent.
ip dhcp snooping trust	Configures the DHCP server ports as trusted and configures interswitch links as trusted if DHCP snooping is deployed on the neighboring switch or if the DHCP server is reachable over other switches.
ip dhcp snooping vlan *vlan*	Enables DHCP snooping in a specific VLAN.
ip dhcp snooping limit rate *rate*	Configures a DHCP request rate limit on untrusted ports.
switchport port-security **switchport port-security maximum** *limit*	Enables port security. It is more effective to deploy port security limits to counter DHCP starvation attacks.

https://t.me/learningnets

Verify DHCP Snooping

This topic describes how to verify DHCP snooping.



Cisco IOS Software includes rich DHCP snooping validation features.

Use the **show ip dhcp snooping** command to display the general DHCP snooping configuration for a switch.

Use the **show ip dhcp snooping binding** command to display the dynamically discovered bindings in the DHCP snooping binding database. To filter which addresses are displayed, provide either a MAC address or an IP address for the address parameter.

Use the **show ip dhcp snooping database** command to display the status of the binding database. This command is especially useful when using a remote storage server to determine its current state and historical operational statistics.

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

Verify DHCP Snooping (Cont.)

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
500
DHCP snooping is operational on following VLANs:
500
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is disabled
   circuit-id format: vlan-mod-port
   remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
Interface                Trusted    Allow option    Rate limit (pps)
-----------------------  -------    ------------    ----------------
FastEthernet5/1          yes        yes             unlimited
  Custom circuit-ids:
FastEthernet5/2          yes        yes             unlimited
  Custom circuit-ids:
FastEthernet5/3          no         no              2
  Custom circuit-ids:
```

© 2014 Cisco Systems, Inc.

In the example, the **show ip dhcp snooping** command confirms that DHCP snooping is enabled for VLAN 500. The FastEthernet5/1 and 5/2 interfaces are configured as trusted ports with no rate limit set. The FastEthernet 5/3 interface is configured as an untrusted port with a rate limit set to 2 packets per second.

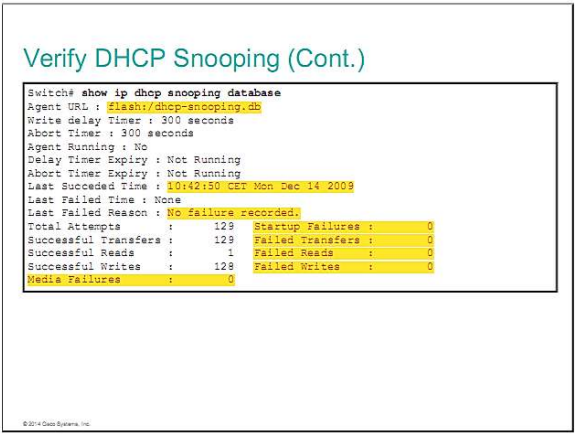
Verify DHCP Snooping (Cont.)

```
Switch# show ip dhcp snooping binding
MacAddress        IpAddress       Lease(sec)  Type           VLAN  Interface
----------------- --------------- ----------  -------------  ----  --------------------
00:1C:25:AA:73:47 192.168.1.116    19786  dhcp-snooping 500  FastEthernet5/24
00:04:27:A2:34:29 192.168.1.117    18685  dhcp-snooping 500  FastEthernet5/5
00:13:C4:49:78:F7 192.168.1.101    18686  dhcp-snooping 500  FastEthernet5/12
00:1E:37:DC:1F:24 192.168.1.133    23629  dhcp-snooping 500  FastEthernet5/4
00:1A:6B:4D:62:06 192.168.1.99     21513  dhcp-snooping 500  FastEthernet5/7
00:11:25:E2:4C:82 192.168.1.137    22748  dhcp-snooping 500  FastEthernet5/9
00:1D:72:2C:3A:FD 192.168.1.135    23836  dhcp-snooping 500  FastEthernet5/11
```

© 2014 Cisco Systems, Inc.

In the example, the **show ip dhcp snooping binding** command displays the dynamically discovered bindings in the DHCP snooping binding database.

https://t.me/learningnets

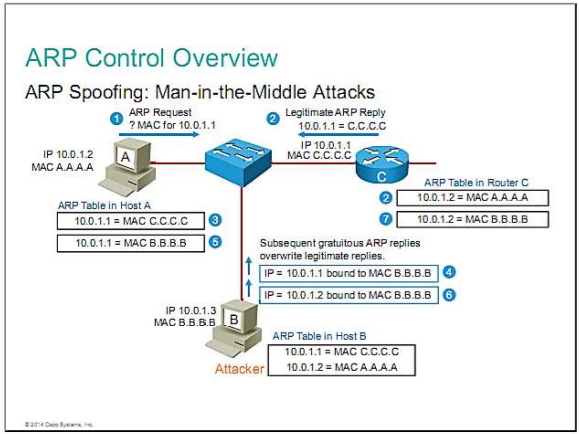


In the example, the **show ip dhcp snooping database** command shows the reachability of the database store and database statistics.

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

ARP Control Overview

This topic describes ARP control.



In normal ARP operation, a host sends a broadcast message to determine the MAC address of a destination host with a particular IP address. The device with the IP address replies with its MAC address. The originating host caches the ARP response and uses it to populate the destination Layer 2 header of packets that are sent to that IP address. By spoofing an ARP reply from a legitimate device with a GARP, an attacking device appears to be the destination host that is sought by the sender. The ARP reply from the attacker causes the sender to store the MAC address of the attacking system in its ARP cache. All packets that are destined for that IP address are forwarded to the attacker system.

An ARP spoofing attack, also known as ARP cache poisoning, can therefore target hosts, switches, and routers that are connected to your Layer 2 network. This targeting is achieved by poisoning the ARP caches of systems that are connected to the subnet and by intercepting traffic that is intended for other hosts on the subnet. The figure shows an example of ARP cache poisoning.

An ARP spoofing attack sequence works as follows:

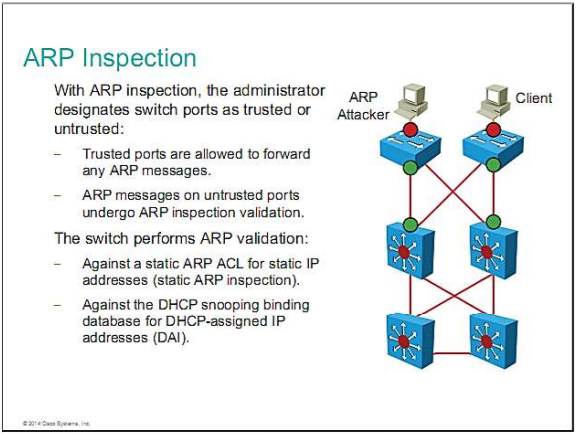
1. Host A sends an ARP request for the Router C MAC address.
2. Router C replies with its MAC and IP address. Router C also updates its ARP cache.
3. Host A binds the Router C MAC address to its IP address in the ARP cache.
4. Host B (attacker) sends a GARP to Host A, binding the MAC address of Host B to the IP address of Router C.
5. Host A updates its ARP cache with the MAC address of Host B bound to the IP address of Router C.
6. Host B (attacker) sends a GARP to Router C, binding the MAC address of Host B to the IP address of Host A.
7. Router C updates its ARP cache with the MAC address of Host B bound to the IP address of Host A.
8. Packets are now diverted through the attacker (Host B).

https://t.me/learningnets

This ARP vulnerability in the infrastructure can be addressed in several ways:

Static ARP inspection or DAI in network switches

Static ARP entries on infrastructure devices; therefore, no use of ARP at all on critical segments



To prevent ARP spoofing, or poisoning, a switch can process transit ARP traffic to ensure that only valid ARP requests and responses are relayed. The ARP inspection feature of Cisco switches prevents ARP spoofing attacks by intercepting and validating all ARP requests and responses. Each intercepted ARP reply is verified for valid MAC-to-IP address bindings before it is forwarded. ARP replies with invalid MAC-to-IP address bindings are dropped.

ARP inspection can determine the validity of an ARP reply that is based on bindings that are stored in a DHCP snooping database for DHCP-addressed hosts. For statically addressed hosts or network devices, ARP inspection can validate ARP packets against a user-configured ARP ACL that contains static MAC-to-IP address mappings.

As with DHCP snooping, ARP inspection labels all switch ports as trusted or untrusted. The switch examines all ARP packets from untrusted ports and only forwards them if they contain an expected MAC-to-IP-address mapping.

In general, follow these labeling guidelines:

Label as untrusted those ports that are connected to any host that is considered a possible source of attack. For hosts with static IP addresses, use static ARP ACL entries on the switch to permit their ARP traffic.

Label as trusted all ports to other switches that are configured with ARP inspection.

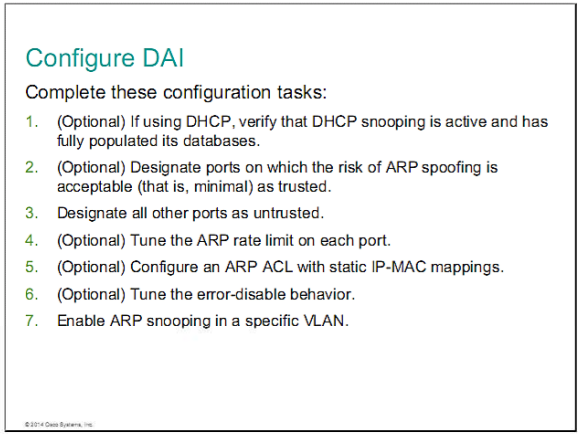
Label as untrusted all ports to other switches that do not support ARP inspection. In this case, make sure that DHCP traffic crosses the ARP inspection-enabled switch so that it can learn legitimate IP-MAC mappings and permit associated ARP traffic.

The figure shows the deployment of ARP protection mechanisms on the access (and partly distribution) layer of the network. User ports are designated as untrusted for ARP snooping, while interswitch links are designated as trusted.

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

Configure DAI

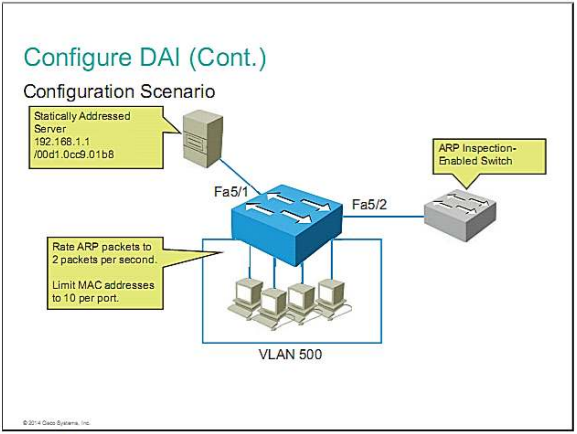
This topic describes how to configure DAI.



When you decide to implement ARP inspection on a switch, complete the following sequence of mandatory and optional configuration tasks:

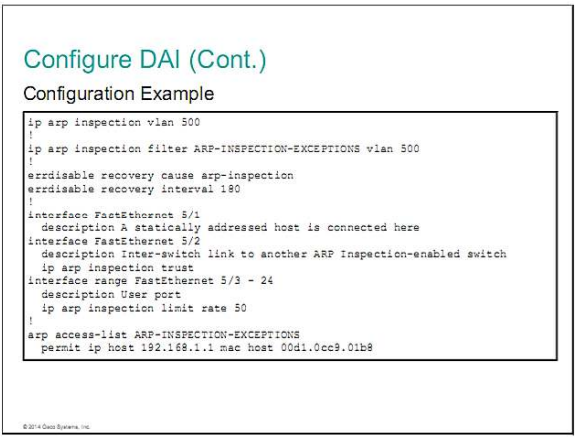
1. Verify that DHCP snooping is active, working properly, and has fully populated its database if your network and this particular switch host DHCP-enabled users. This step is optional and is not required in purely statically addressed networks.
2. Optionally, you may designate edge ports on which the risk of ARP attacks is acceptable (that is, minimal) as trusted. Ideally, do not configure any ports as trusted.
3. Designate all other ports as untrusted for ARP inspection. Note that all ports are, by default, considered untrusted.
4. Optionally, you can tune the default ARP inspection rate-limiting function on each untrusted port. You may need this step if legitimate applications are sending more ARP traffic than the default rate limit allows on a port. Some network scanning applications, including user software that searches for neighboring devices (such as printers), do exhibit such behavior.
5. Optionally, configure an ARP ACL that maps a specific IP address to a specific MAC address for all statically configured hosts whose ARP traffic will flow over this switch.
6. Optionally, you may want to tune the ARP inspection error-disable behavior. ARP inspection, by default, error-disables a port that exceeds the ARP rate limit threshold.
7. Finally, enable ARP inspection in all specific VLANs that require ARP spoofing protection.

https://t.me/learningnets



This figure shows the configuration scenario for the ARP inspection feature. The Cisco switch uses VLAN 500 to host DHCP-addressed clients. DHCP snooping is already configured. A statically addressed host (whose IP and MAC address are shown in the figure) is connected to the FastEthernet5/1 interface. Another ARP inspection-enabled switch is connected over the FastEthernet5/2 trunk port. Configure ARP inspection on the switch to prevent spoofing of ARP information from all client ports, and enforce the static IP-MAC address mapping of the statically addressed host.

The configuration sequence assumes that all ports and VLANs have been preconfigured to enable complete connectivity in VLAN 500 and that the DHCP infrastructure is able to assign network configuration to clients in VLAN 500.



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

In Task 1 of this procedure, verify the operation of DHCP snooping using the DHCP snooping commands that are provided in the previous topic of this lesson.

In Tasks 2 to 4, designate interfaces (ports) as either trusted or untrusted for ARP inspection using the **(no) ip arp inspection trust** interface command. In this example, only the interswitch port is configured as trusted. The switch will sample all ARP traffic on other ports to ensure its validity.

Optionally, configure ARP message rate limiting on a port (the default is 15 ARP packets per second) using the **ip arp inspection limit rate** interface command. It is recommended that you keep this rate limit threshold at a low enough value to protect the switch control plane, but not too low to interfere with normal endpoint operation.

In the optional Task 5, you can configure a list of authorized static IP address to MAC address mappings to support statically addressed hosts. Use an *ARP ACL*, configured using the **arp access-list** command, to provide this mapping to the switch. Attach this list to the relevant ARP-inspection-enabled VLAN using the **ip arp inspection filter** command. In this example, a mapping is configured for the statically addressed host that is attached to the FastEthernet5/1 interface.

Finally, in Tasks 6 and 7, you can optionally configure a custom error-disable behavior and mandatorily enable ARP inspection for at least one VLAN where ARP control should be exercised, using the **ip arp inspection vlan** global configuration command. ARP rate-limit violations will, by default, place the port in the "error disable" state, which can be (optionally) automatically recovered after an interval using the **errdisable recovery cause arp-inspection** command. In this example, the switch will recover the port in 10 minutes.

To configure ARP inspection on a Cisco switch, use the commands that are described in this table:

Commands	Description
ip arp inspection trust	Configures interswitch links to other ARP-inspecting switches as trusted.
ip arp inspection limit rate *rate*	Tunes the ARP rate limit.
ip arp inspection filter *ACL-name* **vlan** *vlan*	Enables static exceptions in a specific VLAN.
arp access-list *ACL-name* *ACL-statement*	Configures exceptions for all statically addressed hosts on untrusted ports. Note: A deny-all entry in this ACL disables all DAI.
ip arp inspection vlan *vlan*	Enables ARP inspection in a specific VLAN.
errdisable recovery cause arp-inspection	Specifies the type of errors that automatically reenable the ports after a specified (300 seconds by default) amount of time.
errdisable recovery interval *interval*	Specifies the time after which a port is automatically reenabled.

https://t.me/learningnets

Verify DAI

This topic describes how to verify DAI.

Verify DAI

DAI Verification Commands	Description
show ip arp inspection	Verifies the overall status of ARP inspection.
show ip arp inspection interfaces *interface*	Verifies the ARP inspection interface status.

© 2014 Cisco Systems, Inc.

Cisco IOS Software includes rich DAI validation features.

Use the **show ip arp inspection** command to display the general ARP inspection configuration for a switch.

Use the **show arp inspection interfaces** command to show the ARP inspection trust mode of all switch interfaces and the ARP rate limits that are applied to them.

Verify DAI (Cont.)

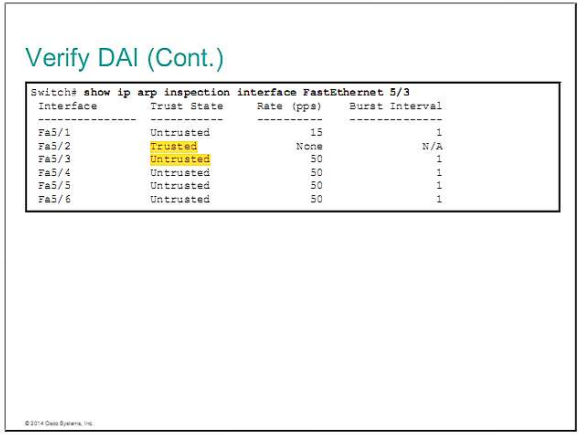
```
Switch# show ip arp inspection
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
  500     Enabled          Active      ARP-INSPECTION-E   No
```

© 2014 Cisco Systems, Inc.

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

In the example, the **show ip arp inspection** command confirms that ARP inspection is enabled for VLAN 500 and that you have configured a static ARP ACL, which also allows DAI (by not including a deny-all statement).

Note that there are several additional validation (protocol verification) checks that ARP inspection can apply to ARP traffic and these are all disabled in this example. Deploy these additional settings with care, because some clients may use nonstandard ARP messages that will be dropped by these checks.

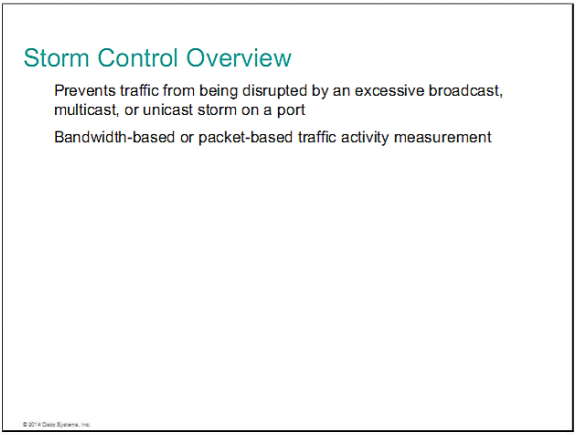


In the example, the **show ip arp inspection interface** command shows the trust mode of interfaces and their settings.

https://t.me/learningnets

Storm Control Overview

This topic describes storm control.



Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port. A LAN storm occurs when packets flood the LAN, create excessive traffic, and degrade network performance. Errors in protocol-stack implementation, mistakes in network configuration, or users issuing a DoS attack can cause a storm.

Storm control uses rising and falling thresholds to block and then restore the forwarding of broadcast, unicast, or multicast packets. You can also set the switch to shut down the port when the rising threshold is reached.

Storm control uses one of these methods to measure traffic activity:

- Bandwidth percentage
- Traffic rate at which packets are received (in packets per second)

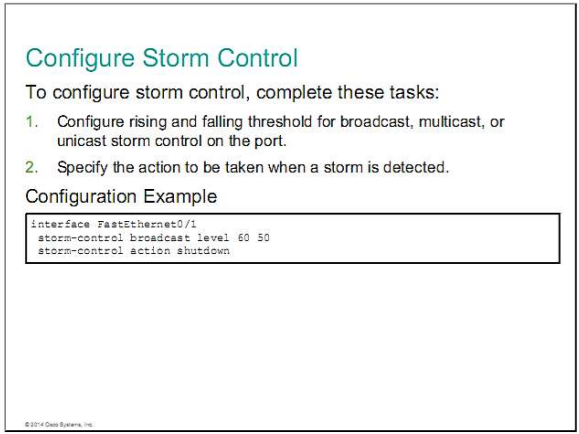
The thresholds can either be expressed as a percentage of the total available bandwidth that can be used by the broadcast, multicast, or unicast traffic, or as the rate at which the interface receives multicast, broadcast, or unicast traffic.

When a switch uses the bandwidth-based method, the rising threshold is the percentage of total available bandwidth that is associated with multicast, broadcast, or unicast traffic before forwarding is blocked. The falling threshold is the percentage of total available bandwidth below which the switch resumes normal forwarding. In general, the higher the level, the less effective the protection against broadcast storms.

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

Configure Storm Control

This topic describes how to configure storm control.



Storm control is configured for the switch as a whole, but operates on a per-port basis. By default, storm control is disabled.

You can configure storm control on a port and enter the threshold level that you want to be used for a particular type of traffic. Specify the rising threshold level for broadcast, multicast, or unicast traffic as a percentage (up to two decimal places) of the bandwidth. The port blocks traffic when the rising threshold is reached. Specify the falling threshold level as a percentage (up to two decimal places) of the bandwidth. This value must be less than or equal to the rising suppression value. The port forwards traffic when traffic drops below this level. If you do not configure a falling suppression level, it is set to the rising suppression level.

Storm control is supported on physical interfaces. You can also configure storm control on an EtherChannel, although you cannot configure storm control on the individual ports of that channel.

To implement storm control on a switch, complete this sequence of configuration tasks:

1. Specify the port, and configure rising and falling threshold for broadcast, multicast, or unicast storm control.
2. Specify the action to be taken when a storm is detected. The default is to filter out the traffic and not to send traps.
   - Use the **shutdown** keyword to error-disable the port during a storm.
   - Use the **trap** keyword to generate an SNMP trap when a storm is detected.

To configure storm control on a Cisco switch, use the commands that are described in the table.

https://t.me/learningnets

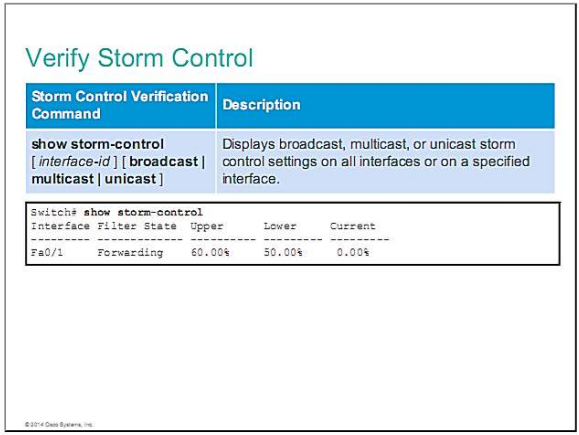
Commands	Description
interface FastEthernet0/1 **storm-control {broadcast | multicast | unicast} level** *rising_level falling_level*	Configures broadcast, multicast, or unicast storm control. The rising level specifies the rising threshold level for traffic as a percentage of the bandwidth. The storm control action occurs when traffic utilization reaches this level. The falling level specifies the falling threshold when traffic is again forwarded.
interface FastEthernet0/1 **storm-control action {shutdown | trap}**	Specifies the action to be taken when a storm is detected. The default is to filter out the traffic and not to send traps.

The example shows how to enable broadcast storm control on a port to a rising level of 60 percent and falling level of 50 percent. When the broadcast traffic exceeds the configured level of 60 percent of the available bandwidth of the port, the switch puts the port into the error-disable state. When the broadcast traffic falls bellow 50 percent of the available bandwidth of the port, the port resumes normal forwarding.

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

Verify Storm Control

This topic describes how to verify storm control.



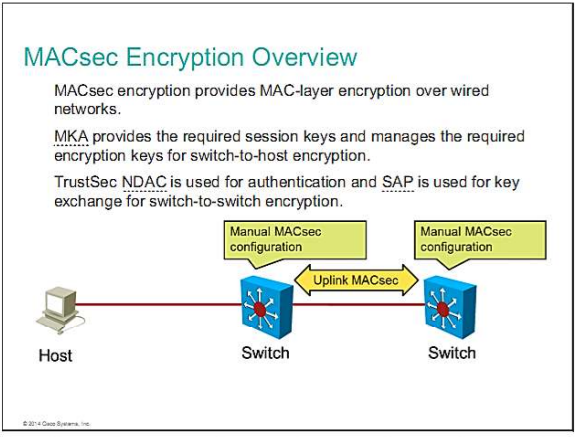
Use the **show storm-control** command to display the storm control settings on a switch.

The example displays the **show storm-control** command when no keywords are entered. Because no traffic-type keyword was entered, the broadcast storm control settings appear.

https://t.me/learningnets

MACsec Encryption Overview

This topic describes MACsec encryption.



MACsec, defined in IEEE 802.1AE, provides MAC-layer encryption over wired networks between two MACsec-capable devices by using OOB methods for encryption keying.

Some Cisco Catalyst switches support 802.1AE encryption with MKA on downlink ports for encryption between the switch and host devices. The switches also supports MACsec link layer switch-to-switch security by using Cisco TrustSec NDAC and the SAP key exchange. Link layer security can include both packet authentication between switches and MACsec encryption between switches (encryption is optional).

The MKA protocol provides the required session keys and manages the required encryption keys for switch-to-host encryption, which is also called downlink MACsec encryption. MKA and MACsec are implemented after successful authentication using the IEEE 802.1X EAP framework. Only host-facing links (links between network access devices and endpoint devices such as a PC or IP phone) can be secured using MACsec with MKA.

Note	Downlink MACsec with MKA is outside of the scope of this course and will not be discussed further.

When both switches support 802.1AE MACsec, SAP negotiation occurs. An EAPOL-key exchange occurs between the supplicant and the authenticator to negotiate a cipher suite, exchange security parameters, and manage keys. Successful completion of these tasks results in the establishment of a SA.

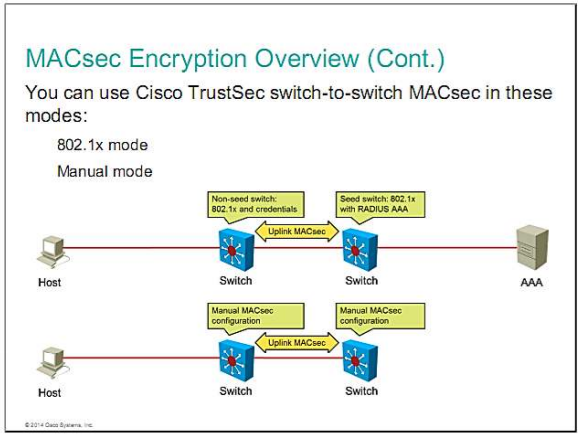
Cisco TrustSec uses AES-128 GCM and GMAC and is compliant with the 802.1AE standard. Cisco TrustSec NDAC SAP is supported on trunk ports because it is intended only for network device to network device links, that is, switch-to-switch links.

Cisco TrustSec NDAC SAP is not supported on:

- Host facing access ports (these ports support MKA MACsec)
- Switch virtual interfaces
- SPAN destination ports

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

You can configure Cisco TrustSec link layer security in 802.1x mode or manual mode. In the 802.1x mode, you must set the Cisco TrustSec credentials on a switch to create the Cisco TrustSec network.



To configure Cisco TrustSec MACsec in 802.1x mode, you have to first configure the seed switch with global 802.1x settings and RADIUS AAA settings. The seed switch is the switch that is the closest to the AAA RADIUS server. You also have to configure the SAP operation mode.

On the non-seed device you have to configure credentials that will be used to authenticate to the seed switch against the RADIUS AAA server. Then you have to configure global 802.1x settings and select SAP operation mode.

The choices for the SAP operational mode are:

gcm-encrypt: Authentication and encryption

gmac: Authentication, no encryption

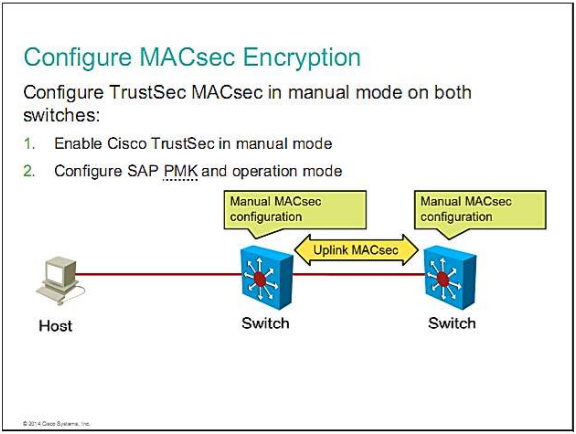
no-encap: No encapsulation

null: Encapsulation, no authentication or encryption

https://t.me/learningnets

Configure MACsec Encryption

This topic describes how to configure MACsec encryption.



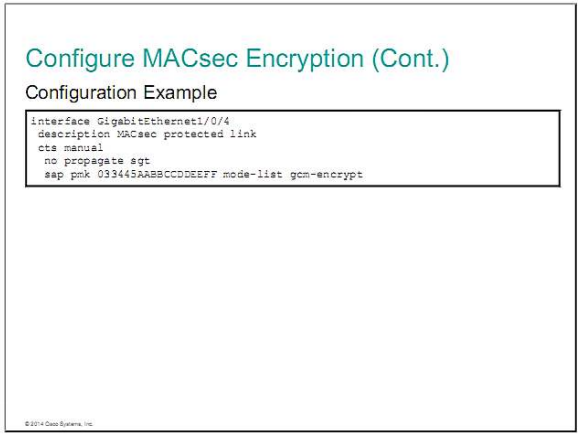
To configure the Cisco TrustSec MACsec in manual mode, complete these configuration tasks:

1. Enable Cisco TrustSec in manual mode and enter Cisco TrustSec configuration mode
2. Configure SAP PMK end select SAP operating mode

To configure the Cisco TrustSec MACsec in manual mode, complete these configuration tasks:

1. Enable Cisco TrustSec in manual mode and enter Cisco TrustSec configuration mode
2. Configures the SAP PMK and operation mode. SAP is disabled by default in Cisco TrustSec manual mode.

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



In the first task of the procedure, enter the MACsec encryption manual configuration mode using the **cts manual** command in the interface configuration mode.

In the second task configure SAP and specify operation mode using the **sap pmk** command. In the example, master key is configured and operation mode is set to **gcm-enrypt**.

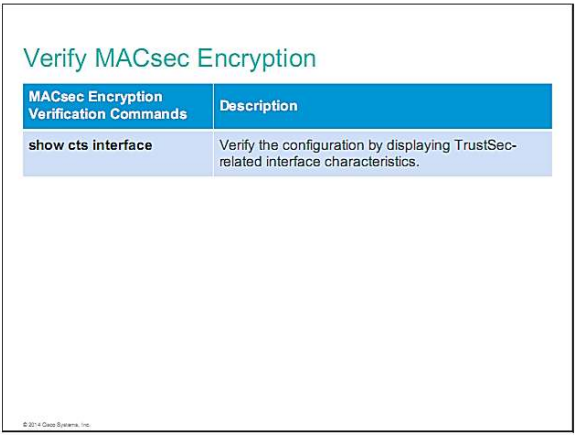
To configure Cisco Trustec MACsec encryption on a Cisco switch using manual method, use the commands that are described in the table.

Commands	Description
cts manual	Enters Cisco TrustSec manual configuration mode
no propagate sgt	Use the no form of this command when the peer is incapable of processing a security group tag. The command prevents the interface from transmitting the security group tag to the peer and is required in manual mode.
sap pmk *key* **mode-list** *sap_mode*	Configures the SAP PMK and operation mode

https://t.me/learningnets

Verify MACsec Encryption

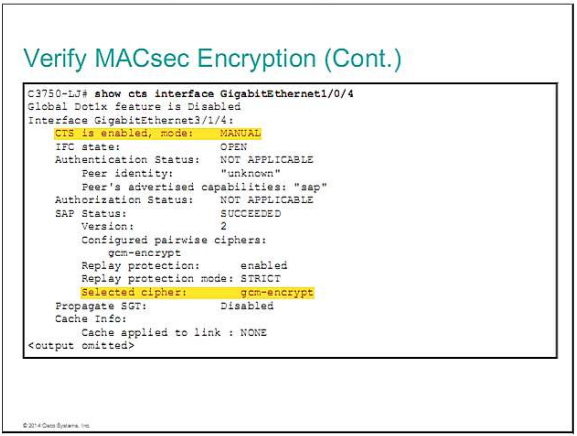
This topic describes how to verify MACsec encryption.



Cisco IOS Software includes rich MACsec encryption validation features.

Use the **show mka policy** command to display the MKA policy entries on a switch.

Use the **show authentication session** command to verify the authorized session security status.

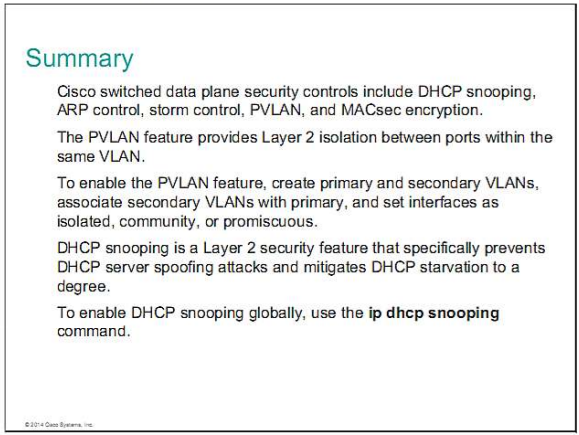


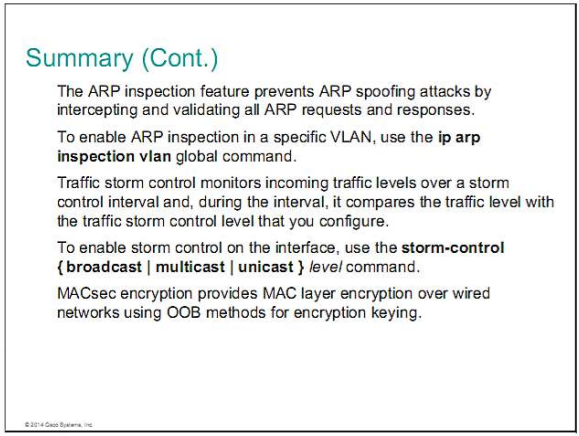
In the example, the **show authentication sessions** command verifies MACsec on an interface.

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

Summary

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





https://t.me/learningnets

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

Lesson 7

Deploying Cisco Layer 3 Data Plane Security Controls

Overview

In an OSI Layer 3 device, the data plane implements packet-forwarding functions and applies services to packets as they are forwarded through the device. The Layer 3 data plane provides various OSI Layer 3 traffic-filtering to protect both the network infrastructure and the endpoints that are connected to the network. This lesson introduces some effective tools that you can use to provide such protection.

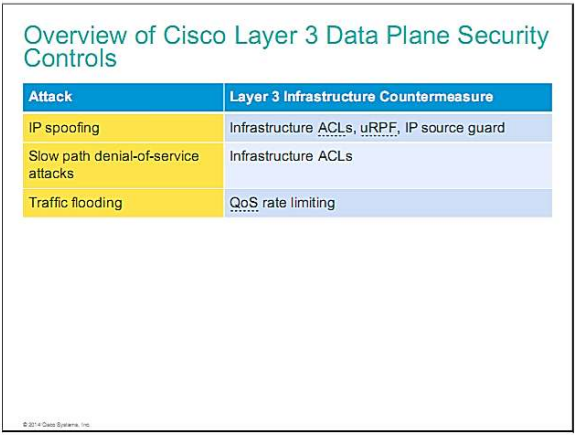
This ability includes being able to meet these objectives:

- Describe Cisco Layer 3 data plane security controls
- Describe infrastructure antispoofing ACLs
- Describe uRPF
- Configure uRPF on Cisco IOS Software
- Verify uRPF on Cisco IOS Software
- Configure uRPF on Cisco ASA
- Verify uRPF on Cisco ASA
- Describe IP Source Guard
- Configure IP Source Guard
- Verify IP source guard

https://t.me/learningnets

Overview of Cisco Layer 3 Data Plane Security Controls

This topic describes Cisco Layer 3 data plane security controls.



The Cisco Layer 3 data plane features can forward packets on OSI Layer 3 and apply per-packet services, including many security analysis and filtering functions. Common network attacks that can be mitigated through routed data plane security features are the following:

IP spoofing: Attackers use stolen or invalid IP source addresses when injecting packets into a network to steal identities or disguise their identity. These attacks can often be successfully mitigated by using antispoofing data plane ACLs, uRPF functions, or IP source guard.

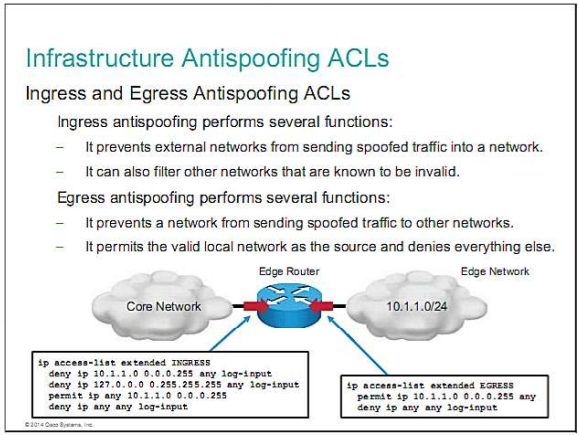
Slow path denial-of-service attacks: An attacker injects packets that network devices need to process in their slow processing path. The slow path is the CPU-intensive feature path that is used to process packets that require additional attention, such as IP packets with options or control plane packets. The two implementations of the slow path in Cisco IOS Software are the process switching path and the Cisco Express Forwarding process path. Often, these attacks are mitigated by control plane security features. However, routed fast-path (the CPU-efficient feature path using optimized features, often implemented in hardware) data plane filtering at the network edge (infrastructure ACLs) and at each device (device host firewalling), can often present a viable alternative.

Traffic flooding: The attacker uses a high rate of packets to overwhelm a network link, a network device, or an endpoint—such as a SYN flooding attack directed at a server. These attacks can sometimes be mitigated by rate limiting features that are deployed on demand to counter an attack. To detect these attacks, a scalable network traffic telemetry method is needed, and NetFlow accounting and data export provides this functionality.

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

Infrastructure Antispoofing ACLs

This topic describes infrastructure antispoofing ACLs.



If the attacker is not using IP source routing to forge source IP addresses, but simply injects packets into the network, then network devices must filter spoofed packets by examining the source IP address field of each packet. The easiest method for this examination is to use ACLs on interfaces of the Layer 3 devices. These lists should be configured to drop packets that appear to be spoofed, and only permit legitimate, nonspoofed traffic.

Two directions of filtering flow to and from each subnet:

Ingress filtering establishes rules that dictate which source addresses can enter a particular network.

Egress filtering establishes rules that dictate which source addresses can exit a particular network.

These rules can be set permissively or restrictively:

The permissive setting denies source addresses that are known to be spoofed and permits everything else. The typical implementation of an ingress filter denies inbound packets with the source addresses of the protected network because they are surely spoofed if they are coming from outside the protected network.

The restrictive setting permits source addresses that are known to be legitimate and denies everything else. The typical implementation of an egress filter permits outbound packets that are using the source addresses of the protected network and denies any other source IP address.

The figure presents an example of an antispoofing ingress packet filter (the INGRESS ACL) that is applied to an edge router that connects to an enterprise network. This filter is applied to filter packets that are coming from the core of the enterprise network. It filters out obviously spoofed IP addresses. It drops packets from several addresses:

The address space of the (protected) local network (10.1.1.0/24). You would not expect to see packets from the address space of the edge network coming in through your interface toward the network core.

The loopback address range (127.0.0.0/8).

https://t.me/learningnets

The INGRESS ACL then permits all traffic to the valid local addresses (10.1.1.0/24), and denies and logs all other IP traffic. No other traffic should be routed to this edge network.

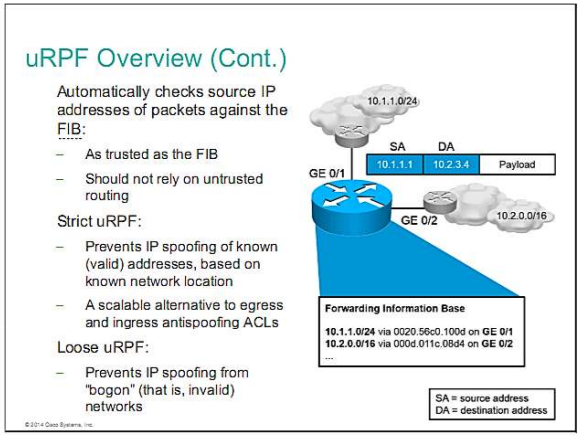
The EGRESS ACL implements a restrictive egress filter. It only allows legitimate source IP addresses from the local edge network (the 10.1.1.0/24 subnet) to be routed toward the core.

To simplify the deployment of such static ACLs, the Cisco AutoSecure feature automatically generates static antispoofing ACLs on untrusted interfaces, if so instructed.

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

uRPF Overview

This topic describes uRPF.



Ingress and egress ACLs require you to manually configure address-based filters on many chokepoints in the network. The uRPF feature attempts to automate this process, therefore making it more scalable and manageable.

It is labor-intensive to specify ACLs for each interface to protect against spoofed packets. The router knows which networks are reachable and valid through which interface. The router has a routing table and a forwarding table —RIB and FIB — that point via an interface to reach an IP network. Therefore, the routing table can also be used to validate the source addresses of the incoming packet by checking each source address against the RIB or FIB. The technique is called uRPF.

However, the uRPF mechanisms are only as reliable as the routing and forwarding tables to which they refer. That is, if routing is not appropriately secured (using routing protocol authentication and filtering), these mechanisms are not reliable.

The uRPF mechanism should be used as the first line of defense in a network and can be deploy on network devices, such as Cisco IOS routers, Cisco IOS Layer 3 switches, and Cisco Adaptive Security Appliance firewalls.

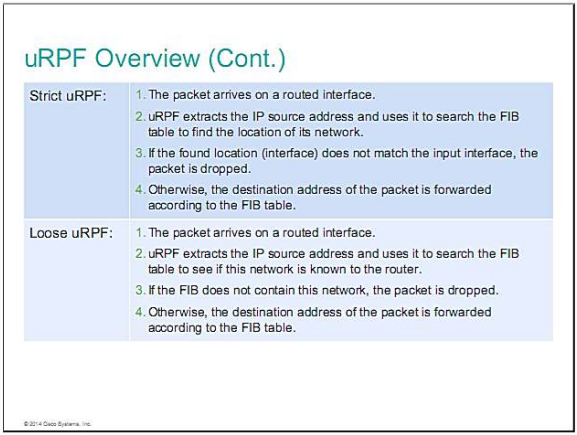
There are two types of uRPF available on the Cisco IOS routers:

Strict uRPF verifies that the packet is coming through the expected interface and therefore provides a scalable alternative to ingress and egress ACLs. Packets that are coming from unexpected interfaces (as per the RIB and FIB) are dropped.

Loose uRPF only validates the existence of the source network of the packet in the routing table and provides a method to drop packets from unknown and therefore invalid networks.

Cisco ASA adaptive security appliance supports only strict uRPF, and it allows usage of a default route to correctly identify a source interface.

https://t.me/learningnets



When a packet is received at the Cisco IOS router interface where strict uRPF has been configured, these actions occur:

1. The router accepts the packet on an input interface.
2. If it is permitted by the input ACL, uRPF extracts the source IP address from the packet. uRPF performs a lookup in the FIB to determine which outgoing interface is used to reach the network to which the source IP address belongs.
3. If the interface that is determined by the FIB lookup is not the same as the input interface, the packet is dropped.
4. Otherwise, the router extracts the destination IP address from the packet. It then performs a lookup in the FIB to determine the next hop to which the packet should be forwarded.

uRPF on the Cisco ASA is implemented differently because the Cisco ASA is a stateful packet filtering firewall. For protocols, that are treated statelessly, each packet is checked against the routing table. For protocols, that are treated statefull, the ASA verifies only the initial packet. Subsequent packets arriving during the session are checked using an existing state maintained as part of the session. Non-initial packets are checked to ensure they arrived on the same interface used by the initial packet.

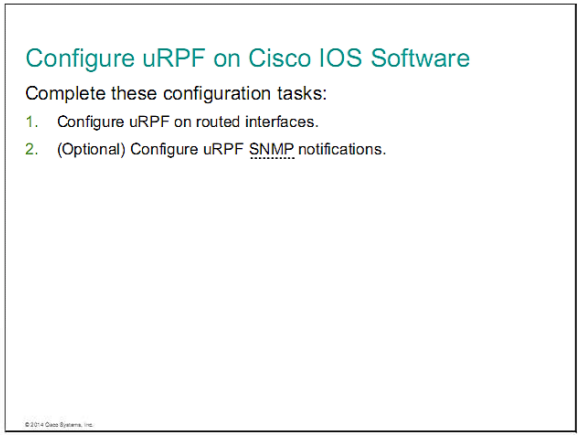
When a packet is received at the Cisco IOS router interface where loose uRPF has been configured, these actions occur:

1. The router accepts the packet on an input interface.
2. If it is permitted by the input ACL, uRPF extracts the source IP address from the packet and performs a lookup in the FIB to determine if the network to which the source IP address belongs exists in the FIB.
3. If this network does not exist (for example, there is no route matching this network in the RIB), the packet is dropped.
4. Otherwise, the router extracts the destination IP address from the packet. It then performs a lookup in the FIB to determine the next hop to which the packet should be forwarded.

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

Configure uRPF on Cisco IOS Software

This topic explains how to configure uRPF on Cisco IOS Software.

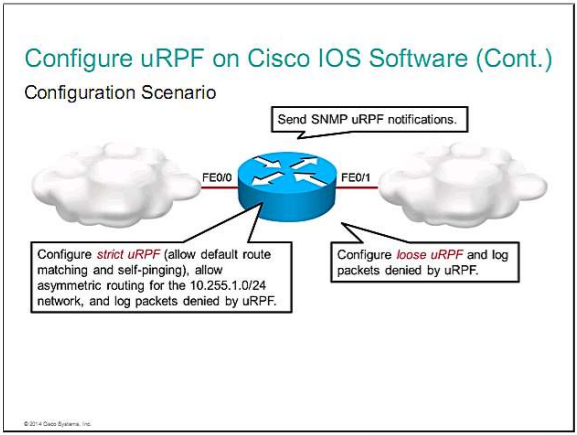


To configure uRPF on a Cisco IOS Software router or OSI Layer 3 switch, complete the following tasks:

1. Configure uRPF in strict or loose mode on routed interfaces where spoofing is likely.
2. Optionally, configure uRPF-related SNMP notifications to provide real-time auditing of uRPF violations.

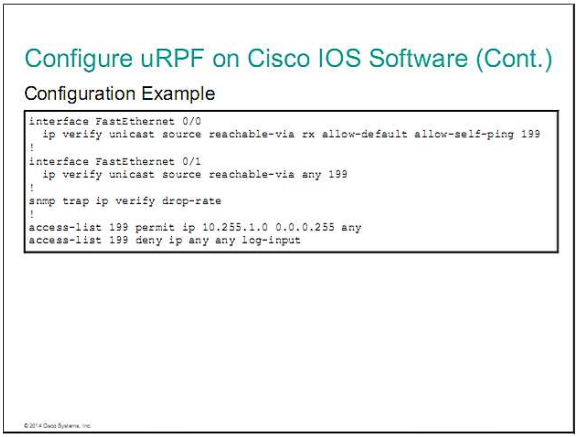
Note	Cisco Express Forwarding is required in order to configure uRPF on the Cisco IOS router.

https://t.me/learningnets



This figure shows the configuration scenario that is presented in the configuration tasks. Configure strict uRPF on the FastEthernet0/0 interface of the router to automatically drop all spoofed traffic. Strict uRPF should allow matching against the default route and allow administrators to ping the router itself. On the same interface, allow traffic from the 10.255.1.0/24 network to be asymmetrically routed and therefore bypass strict uRPF checks. Log all packets that are denied by the uRPF feature. On the FastEthernet0/1 router interface, configure loose uRPF and log all packets that are denied by it.

Additionally, configure SNMP-based notifications of uRPF violations. The example assumes that the router is appropriately preconfigured with an SNMP destination to which SNMP traps can be sent.



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

In the first task, you will configure strict and loose uRPF on router interfaces.

To configure strict uRPF on a routed interface, use the **ip verify unicast source reachable-via rx** command. You can extend this command using the **allow-default** argument to also consider the default route in source verification. This is required in environments that use a trustworthy default route. You can use the **allow-self-ping** option to allow the router to ping its own interface. Without this option, ping packets that the router generated fail the RPF verification check and, thus, self-pinging is not allowed. Additionally, you can specify an ACL as an argument. When a router decides to deny a packet based on FIB lookup, it can compare the offending packet to this ACL. You can use this ACL to make a uRPF exception and permit this packet, or simply log all denied packets via the syslog facility, as shown in the second line of the extended ACL 199 in this figure.

To configure loose uRPF on a routed interface, use the **ip verify unicast source reachable-via any** command. You should *not* extend this command using the **allow-default** argument. Doing so would make the source address of any packet valid because there would be a default network to match any source address in the FIB. Additionally, you can specify an ACL to log all denied packets, as with strict uRPF.

One problem with using strict RPF relates to asymmetrical routing. No rule in IP says that packets in either direction of a conversation must use the same path. It may be quite legitimate in a network to receive packets from a source through one interface, but send packets back to that destination through a different interface. In this case, strict uRPF would block the incoming packets because they do not correspond to the outbound route in the FIB, even though this may be a completely legitimate data stream.

uRPF accommodates asymmetrical routing in two ways. It allows a user to switch to loose RPF (therefore losing a large chunk of antispoofing functionality). Or, it configures a special uRPF ACL that specifies which unicast addresses are likely to be asymmetrically routed and which unicast addresses RPF should ignore. Such an ACL allows the deployment of both uRPF and some asymmetric routing in a controlled fashion.

In the second task, use the **snmp trap ip verify drop-rate** global configuration command to enable the sending of uRPF-related traps to all configured SNMP trap destinations.

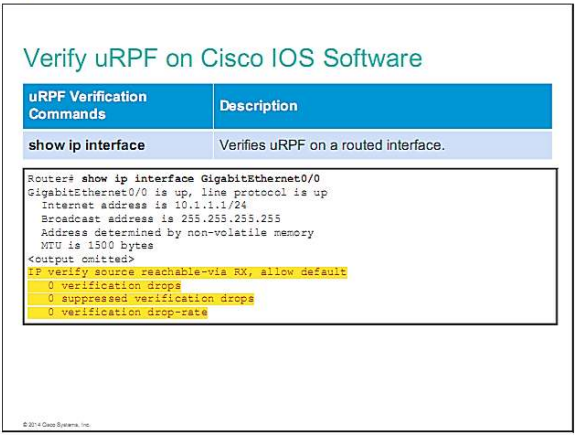
To configure uRPF on the Cisco router, use the commands that are described in this table:

Commands	Description
interface FastEthernet 0/0 **ip verify unicast source reachable-via rx allow-default allow-self-ping 199**	Enables strict uRPF on the interface. The ACL is applied for additional ACL check.
interface FastEthernet 0/1 **ip verify unicast source reachable-via any 199**	Enables loose uRPF on the interface. The ACL is applied for additional ACL check.
snmp trap ip verify drop-rate	Enables uRPF-related SNMP traps.

https://t.me/learningnets

Verify uRPF on Cisco IOS Software

This topic explains how to verify uRPF on Cisco IOS Software.



Use the following command to verify uRPF on Cisco IOS routers:

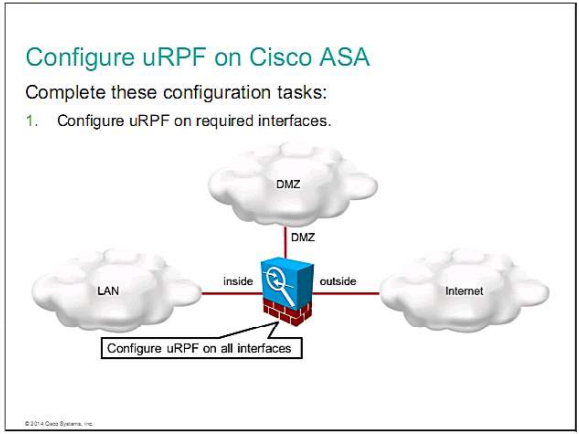
Use the **show ip interface** command to verify the configuration and operation of uRPF and uRPF-related SNMP notifications on a specific routed interface.

In the example, the **show ip interface** command shows if uRPF is enabled on a particular interface. At the end of its output, you can see the uRPF configuration parameters in addition to uRPF-related SNMP trap statistics. To troubleshoot uRPF dropping, use the ACL logging of denied packets and observe the syslog messages of the router to analyze individual drops.

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

Configure uRPF on Cisco ASA

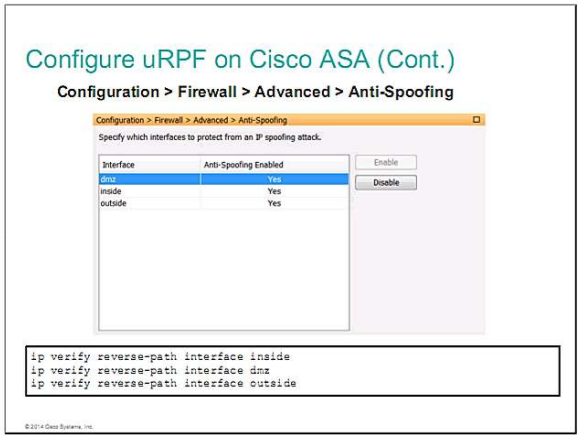
This topic explains how to configure uRPF on Cisco Adaptive Security Appliance.



To configure uRPF on a Cisco ASA, complete the following tasks:

1. Configure uRPF in strict mode on an interface where spoofing is likely.

This figure shows the configuration scenario that is presented in the configuration tasks. You will configure uRPF on the inside, outside, and DMZ interfaces.



https://t.me/learningnets

Follow these steps to configure uRPF on Cisco ASA security appliance interfaces:

1 From Cisco Adaptive Security Device Manager, choose **Configuration > Firewall > Advanced > Anti-Spoofing**. The Anti-Spoofing window appears.

2 Choose an interface on which you would like to enable uRPF and click the **Enable** button.

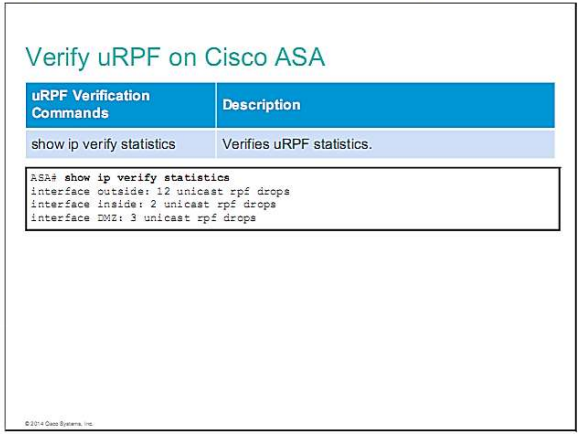
In the CLI, use the **ip verify reverse-path interface** interface-name command to enable uRPF on a specific interface.

Commands	Description
ip verify reverse-path interface *interface-name*	Enables uRPF on an interface.

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

Verify uRPF on Cisco ASA

This topic explains how to verify uRPF on Cisco Adaptive Security Appliance.



Use the following command to verify uRPF on Cisco IOS routers:

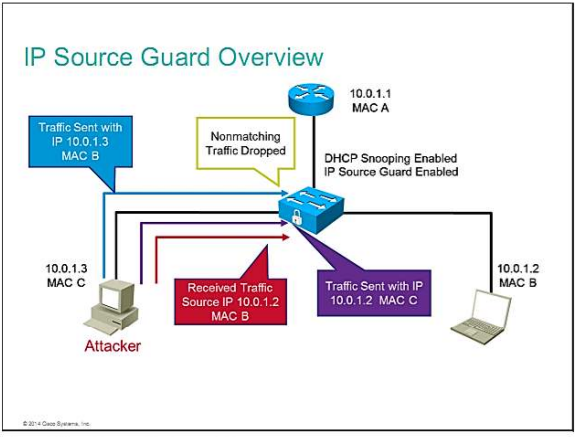
Use the **show ip verify statistics** command to verify uRPF statistics on uRPF enabled interfaces.

In the example, the **show ip verify statistics** command shows statistics for dropped packets because of uRPF checks.

https://t.me/learningnets

IP Source Guard Overview

This topic describes IP Source Guard.



IP spoofing is traditionally used in three different ways:

Spoofing an existing host by simply injecting packets with a forged source address in the network. Such spoofing is typically used to exploit IP address-based authentication between networked systems.

Spoofing an existing host using IP source routing, with the same aim as the previous technique.

Spoofing nonexistent hosts by injecting packets with a forged source address in the network. Such spoofing is used to avoid detection in an attack. A good example of this is SYN flooding, in which source addresses are "Martian" (or coming from "bogon" address space).

IP Source Guard is a Cisco IOS Software feature that is available on Cisco switches and can stop an IP spoofing attack closest to the source—on the switch port where the attacking host connects to the network. Like DHCP snooping, you can enable IP Source Guard on a DHCP snooping untrusted port.

Initially, all IP traffic on the port is blocked except for DHCP packets that are captured by the DHCP snooping process. When a client receives a valid IP address from the DHCP server, or when a static IP source binding is configured by the user, IP Source Guard installs an autogenerated PACL on the interface. The PACL allows only IP traffic from a source IP address that is in the IP source binding table and denies all other traffic. The PACL takes precedence over any router ACLs or VLAN maps that affect the same interface. This filtering limits the ability of a host to attack the network by claiming the IP address of a neighbor host.

Note	Turn on DHCP snooping at least 24 hours before enabling IP Source Guard for the switches to learn all IP addresses. Alternatively, you can force DHCP renewals using some other method to accelerate deployment.

You can also deploy IP Source Guard on ports that connect statically addressed systems to the network by specifying static mapping in the IP Source Guard configuration, or by using IP Device Tracking. Alternatively, you can use manually configured PACLs on the same port.

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

IP Source Guard for static hosts with IP Device Tracking relies on IP device tracking-table entries to install port ACLs. The switch creates static entries based on ARP requests or other IP packets to maintain the list of valid hosts for a given port. You can also specify the number of hosts allowed to send traffic to a given port. This is equivalent to port security at Layer 3.

IP Source Guard for static hosts with IP Device Tracking initially learns IP or MAC bindings dynamically through an ACL-based snooping mechanism. IP or MAC bindings are learned from static hosts by ARP and IP packets. They are stored in the device tracking database. When the number of IP addresses that have been dynamically learned or statically configured on a given port reaches a maximum, the hardware drops any packet with a new IP address. To resolve hosts that have moved or gone away for any reason, IPSG for static hosts leverages IP device tracking to age out dynamically learned IP address bindings. This feature can be used with DHCP snooping. Multiple bindings are established on a port that is connected to both DHCP and static hosts. For example, bindings are stored in both the device tracking database as well as in the DHCP snooping binding database.

The example in the figure shows the following:

The attacker attempts to spoof the IP address of the laptop (10.0.1.2). Because the switch is configured for IP Source Guard, it drops the IP address spoofing attempt.

The attacker attempts to spoof the MAC address of the laptop (MAC B). Because the switch is configured for IP Source Guard, it drops the MAC address spoofing attempt.

IP Source Guard supports only Layer 2 ports, including both access ports and trunk ports. For each untrusted Layer 2 port, there are two levels of IP traffic security filtering:

Source IP address filter: IP traffic is filtered based on its source IP address. Only IP traffic with a source IP address that matches the IP source binding entry is permitted.
An IP source address filter is changed when a new IP source entry binding is created or deleted on the port. The PACL is recalculated and reapplied in the hardware to reflect the IP source binding change. By default, if the IP filter is enabled without any IP source binding on the port, a default PACL that denies all IP traffic is applied to the port. Similarly, when the IP filter is disabled, any IP source filter PACL is removed from the interface.

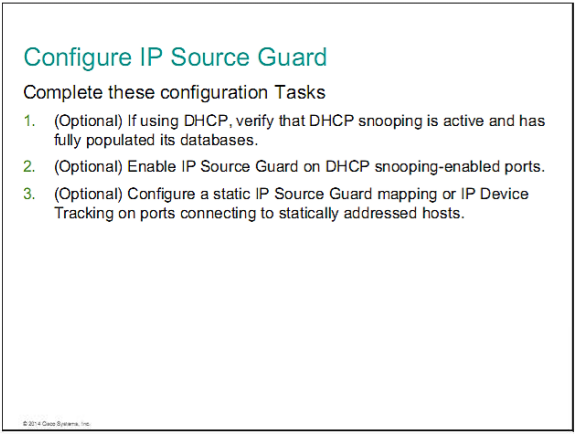
Source IP and MAC address filter: IP traffic is filtered based on its source IP address and its MAC address. Only IP traffic with source IP and MAC addresses that match the IP source binding entry are permitted.

Note If you enable IP Source Guard on a trunk port with many VLANs that have DHCP snooping enabled, you could run out of ACL hardware resources and some packets might be switched in software.

https://t.me/learningnets

Configure IP Source Guard

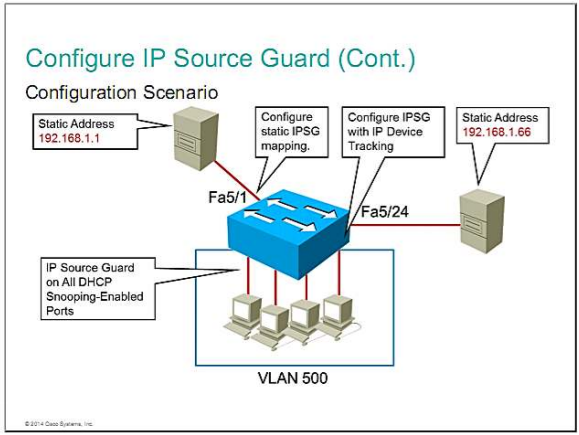
This topic explains how to configure IP Source Guard.



When you implement source address verification on a switch, complete the following sequence of optional configuration tasks:

1. Verify that DHCP snooping is active, working properly, and has fully populated its database, if your network and this particular switch host DHCP-enabled users. This step is optional and not required in purely statically addressed networks.
2. Optionally (if using DHCP), enable IP Source Guard on all ports that are designated as untrusted for DHCP snooping.
3. Optionally (if using static addressing), enable IP Source Guard and configure a static IP Source Guard mapping, or configure IP Device Tracking.

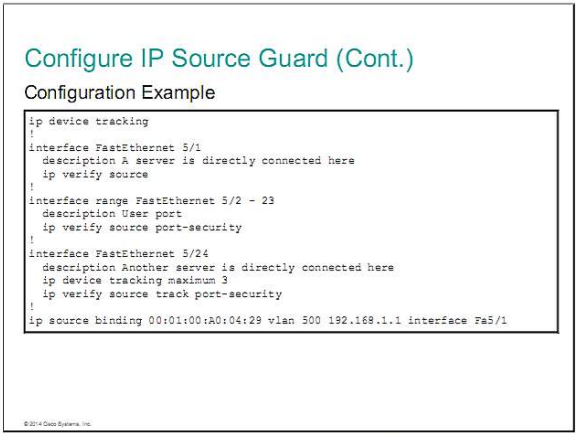
© 2014 Cisco Systems, Inc.
https://t.me/learningnets



This figure shows the configuration scenario for Cisco Catalyst IOS Software source address verification features. The Cisco Catalyst switch uses VLAN 500 to host DHCP-addressed clients. DHCP snooping is already configured according to the configuration sequence of the DHCP snooping topic. Configure IP Source Guard on all ports on which DHCP snooping is enabled (FastEthernet5/2 to FastEthernet5/23). There are two statically addressed hosts: the 192.168.1.1 server on the FastEthernet5/1 interface and the 192.168.1.66 server on the FastEthernet5/24 interface. Configure static IP Source Guard to prevent IP spoofing from the first server and IP Device Tracking to prevent IP and MAC spoofing from the second server.

The upcoming configuration sequence assumes that all ports and VLANs have been preconfigured to enable complete connectivity in VLAN 500, and that the DHCP infrastructure is able to assign network configuration to clients in VLAN 500.

https://t.me/learningnets



In Task 1 of this configuration procedure, verify the operation of DHCP snooping using the DHCP snooping commands that are provided in the DHCP snooping topic of this lesson.

Task 2 enables IP Source Guard on a DHCP snooping-enabled untrusted port using the **ip verify source** command. The additional **port-security** keyword (used in this example on all DHCP-snooping-enabled ports) enables both source IP address and source MAC address verification.

Note When you enable both IP Source Guard and port security by using the **ip verify source port-security** command, there are two caveats:

1. The DHCP server must support option 82, or the client is not assigned an IP address.
2. The MAC address in the DHCP packet is not learned as a secure address. The MAC address of the DHCP client is learned as a secure address only when the switch receives non-DHCP data traffic.

For statically addressed hosts, enable IP Source Guard on their interface using the **ip verify source** command. Create a static mapping for the MAC address, IP address, and switch port using the **ip source binding** command. This example manually binds the 192.168.1.1 IP address with the 0001.00A0.0429 MAC address on VLAN 500 to the FastEthernet5/1 interface.

Alternatively, you can globally enable IP Device Tracking using the **ip device tracking** command and configure an interface to use the Device Tracking table for verifying IP and MAC addresses using the **ip verify source track port-security** command. It is also required to set a maximum limit for the number of static IP addresses that the IP device tracking table allows on the port using the **ip device tracking maximum**. The range is 1 to 10. The maximum number is 10.

To configure IP source guard on the Cisco switch, use the commands that are described in this table:

Commands	Description
ip device tracking	Globally enables IP Device Tracking
interface FastEthernet 5/1 **description A server is directly connected here** **ip verify source**	Enables IP source guard with IP address verification on the switchport.

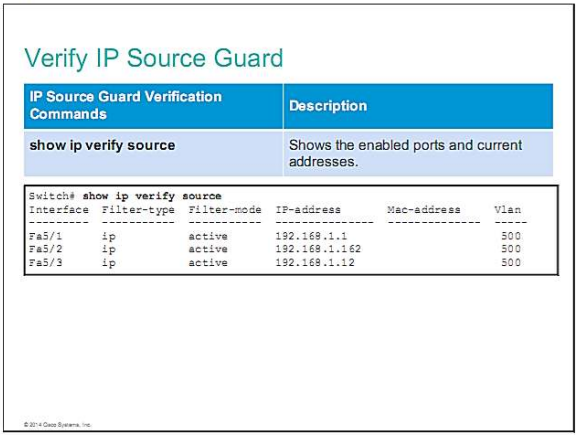
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Commands	Description
interface range FastEthernet 5/2 - 23 **description User port** **ip verify source port-security**	Enables IP source guard with IP and MAC address verification on the switchports.
interface FastEthernet 5/24 **description Another server is directly connected here** **ip device tracking maximum 3** **ip verify source track port-security**	Enables IP Source Guard with IP and MAC address verification to reference the Device Tracking table
ip source binding 00:01:00:A0:04:29 vlan 500 192.168.1.1 interface Fa5/1	Creates static binding for statically addressed hosts.

https://t.me/learningnets

Verify IP Source Guard

This topic explains how to verify IP source guard.

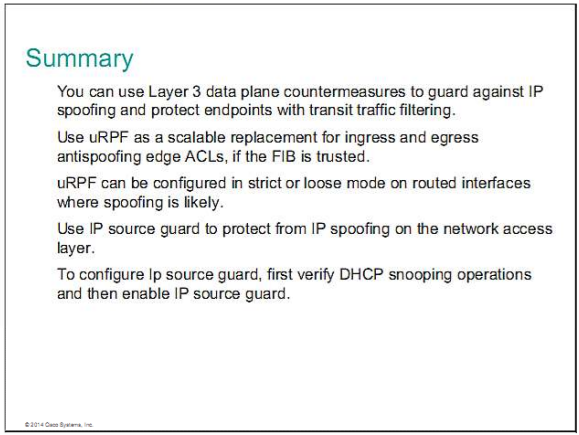


To verify the IP Source Guard configuration, use the **show ip verify source [interface** *interface-name*] command. If you do not provide an interface parameter, this command displays the IP Source Guard configuration for all ports.

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

Summary

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

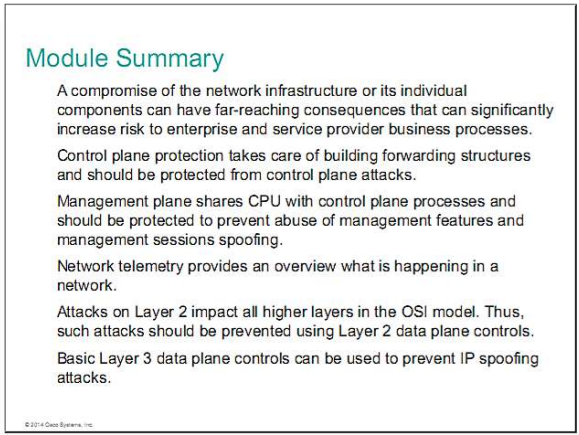


https://t.me/learningnets

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

Module Summary

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



https://t.me/learningnets

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

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 network device plane is responsible for device administration, provision configuration and monitoring the device operation? (Source: Introducing Cisco Network Infrastructure Protection)

   A. Switched data plane
   B. Switched and routed data plane
   C. Control plane
   D. Management plane

2. What security feature is able to match on arbitrary bits of a packet at an arbitrary depth in the packet header and payload? (Source: Introducing Cisco Network Infrastructure Protection)

   A. Interface ACL
   B. Flexible Packet Matching
   C. Unicast Reverse Path Forwarding
   D. ICMP

3. What are the three control plane subinterfaces that are automatically created by Control Plane Protection? (Choose three) (Source: Deploying Cisco IOS Control Plane Security Controls)

   A. The host subinterface
   B. The CEF-exception subinterface
   C. The transit subinterface
   D. The FastEthernet subinterface
   E. The Serial subinterface

4. What are the three management plane protection benefits? (Choose three) (Source: Deploying Cisco IOS Management Plane Security Controls)

   A. Increased control over the management
   B. Provides more security
   C. Degradation of performance for data packets on nonmanagement interfaces
   D. More ACLs are needed to restrict access to a device
   E. Network scalability

5. What are the two common AAA protocols that are used to configure external AAA for management access on the Cisco ASA? (Choose two) (Source: Deploying Cisco ASA Management Plane Security Controls)

   A. LDAP
   B. RADIUS
   C. TACACS
   D. SDI
   E. TACACS+
   F. NTLM

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

6. What are three types of private VLAN ports? (Choose three) (Source: Deploying Cisco IOS Layer 2 Data Plane Security Controls)

   A. Isolated
   B. Non-promiscuous
   C. Community
   D. Promiscuous

7. When implementing storm control on a switch what is the action to be taken when a storm is detected? (Source: Deploying Cisco IOS Layer 2 Data Plane Security Controls)

   A. The default is to shutdown the port.
   B. The default is to filter out the traffic and not to send traps.
   C. The default is to shutdown the port and send traps.
   D. The default is to send traps only.

8. Which solution can be used to mitigate ARP attacks in non-DHCP environments? (Choose two.) (Source: Deploying Cisco IOS Layer 2 Data Plane Security Controls)

   A. IP Device Tracking
   B. Static ARP entries on all devices
   C. Static binding between MAC and IP addresses and ARP inspection on a switch
   D. Dynamic ARP inspection
   E. DHCP Snooping

9. What does the strict uRPF do? (Source: Deploying Cisco Layer 3 Data Plane Security Controls)

   A. Prevents IP spoofing from invalid networks
   B. Prevents IP spoofing of known addresses, based on known network location
   C. Prevents MAC spoofing from invalid addresses
   D. Prevents MAC spoofing of valid addresses

10. What does IP Source Guard do? (Choose two.) (Source: Deploying Cisco Layer 3 Data Plane Security Controls)

    A. Statelessly matches IP packet header or payload (or both), based on arbitrary criteria
    B. Statefully matches IP packet header or payload (or both), based on arbitrary criteria
    C. Matches IP address of a packet against a DHCP binding table
    D. Matches IP address and MAC address of a packet against a DHCP binding table, IP Device Tracking table, or manually configured bindings.

https://t.me/learningnets

Answer Key

1. D
2. B
3. A, B, C
4. A, B, E
5. B, E
6. A, C, D
7. B
8. B, C
9. B
10. C, D

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

Module 3

NAT Deployment on Cisco IOS Software and Cisco ASA

Introduction

Network address translation features allows you to establish connectivity between different networks, when IP addresses between the networks are not routable or are overlapping. Connectivity is achieved by translating IP addresses in IP packets. This module provides you with an overview, configuration, verification, and troubleshooting of NAT features on Cisco ASA 5500-X Series Next-Generation Firewalls and on Cisco IOS Software routers.

Upon completing this module, you will be able to:

- Describe network address translation
- Configure, verify, and troubleshoot network address translation on Cisco ASA
- Configure, verify, and troubleshoot network address translation on Cisco IOS Software routers

https://t.me/learningnets

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

Lesson 1

Introducing Network Address Translation

Overview

NAT and PAT are mechanisms that you can use to conserve registered IPv4 addresses in large networks, resolve overlapping addressing scenarios, and simplify IPv4 address management tasks. NAT and PAT translate IPv4 addresses within private internal networks to legal IPv4 addresses for transport over public external networks, such as the Internet, without requiring a registered subnet address. Incoming traffic is translated back for delivery within the inside network.

This translation of IPv4 addresses eliminates the need for host renumbering and allows the same IPv4 address range to be used in multiple networks. This lesson describes the features that are offered by NAT and PAT.

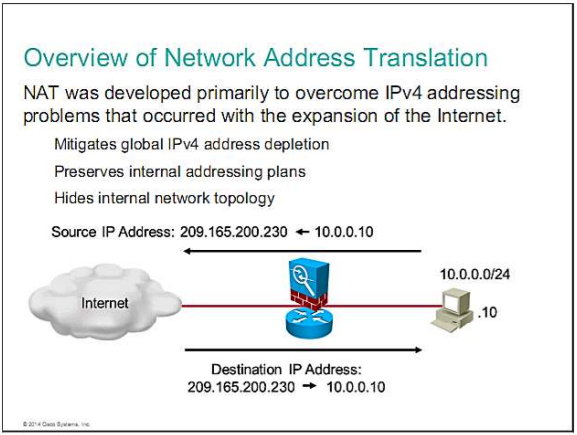
Upon completing this lesson, you will be able to:

- Provide an overview of NAT
- Place network address translation into the Cisco modular network architecture design architectures
- Describe inside and outside NAT
- Describe static and dynamic NAT
- Describe NAT with PAT
- Describe policy-based NAT
- List Cisco products and features that are available to implement NAT

https://t.me/learningnets

Overview of Network Address Translation

This topic provides an overview of NAT.



NAT technology was developed primarily to overcome IPv4 addressing problems that occurred with the expansion of the Internet and to interconnect networks with overlapping address spaces. Usually, private networks are assigned IPv4 addresses from network blocks that are defined in the RFC 1918 standard. Because these private addresses are intended only for local use, NAT is required to translate private (local) IPv4 addresses into public (global) routable IPv4 addresses. Using NAT has the following benefits:

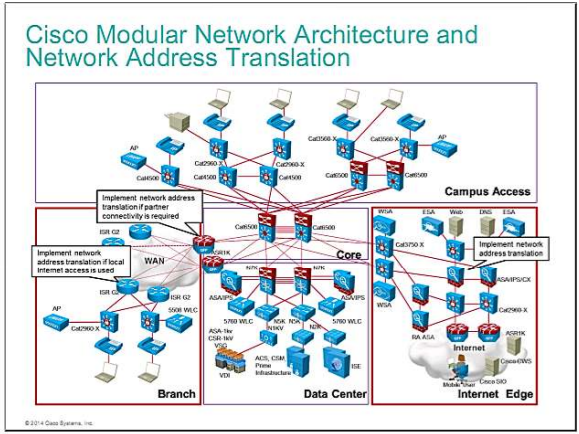
- NAT mitigates the depletion of public IPv4 addresses because many private hosts can share the same public IPv4 addresses. NAT also allows you to use private IPv4 addresses internally.
- NAT preserves the internal IP addressing plan if you change ISPs and both ISPs use a provider-dependant public (global) address space.
- NAT hides the internal IP addressing and topology of your network.

In the example in the figure, a host with the 10.0.0.10 IP address communicates with the Internet. When the NAT-enabled device (a Cisco IOS Software router or Cisco Adaptive Security Appliance) receives a packet from the internal host, it changes (translates) the source IP address of the outgoing packet. In the example, the source IP address is translated to a globally routable IP address of 209.165.200.230. When a host in the Internet receives the packet, it sends a reply to the 209.165.200.230 destination IP address. When the NAT-enabled device receives the reply, the destination IP address is translated back to the internal 10.0.0.10 address, and the packet is sent to the inside host.

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

Cisco Modular Network Architecture and Network Address Translation

This topic places network address translation into the Cisco modular network architecture design architectures.



The figure illustrates where in the Cisco modular network architecture network address translation is deployed. NAT is usually always deployed on the Internet edge, where internal IPv4 addresses are translated to the public IPv4 addresses to enable connectivity from the internal hosts to the Internet. The Internet edge should also provide static translations for services (DNS, Web servers, email servers, etc.) in the DMZ that should be publicly available.

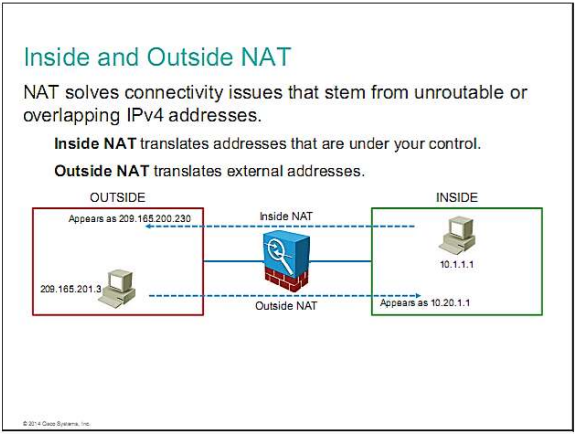
Network address translation can be also deployed in branch offices if the offices require local connectivity to the Internet. In such case, deployment of stateful packet filtering firewall device is also highly recommended in the branch offices. Since such deployment enlarges administrative domain for security administrators, enterprises often decide to implement central Internet access, where traffic from branch offices first flow to the central office, where the traffic is translated and sent to the Internet. The latter approach introduces a single point of network address translation and firewall configuration.

NAT is also required when an enterprise interconnects with partner enterprises, and both enterprises uses overlapping address space.

https://t.me/learningnets

Inside and Outside NAT

This topic describes inside and outside NAT.



NAT is a technology that solves connectivity issues for networks that use globally unroutable or overlapping address spaces. NAT gateways perform real-time translations of network addresses inside the headers of routed packets.

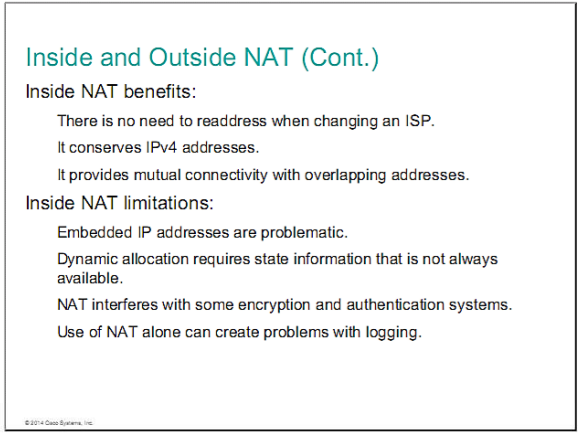
Note	Any device that is between an internal network and the public network—such as a firewall, a router, or a computer—uses NAT, which is defined in RFC 1631.

Most often, NAT enables private IPv4 internetworks that use nonregistered IPv4 addresses to connect to the Internet. The NAT gateway separates the inside NAT domain (where hosts under your addressing control are located) and the outside NAT domain (where hosts whose addressing is not under your control are located).

The NAT gateway performs the inside NAT process in which it translates the local (private) addresses of hosts in the inside NAT domain into global (public) addresses as the local hosts communicate with external hosts in the outside NAT domain. You can configure NAT to advertise only one address for the entire network. Advertising only one address effectively hides the internal network from the outside world and, therefore, provides additional security.

The NAT gateway can also perform the outside NAT process in which it translates the external addresses of hosts in the outside NAT domain to internal addresses as the external hosts communicate with internal hosts in the inside NAT domain. Outside NAT is especially useful when you have to connect networks that use overlapping IP address (for example partner companies), and only one side uses inside NAT.

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



Inside NAT offers several benefits:

There is no need to readdress if an enterprise changes ISP**:** It eliminates the need to readdress all hosts that require external access, therefore saving time and money.

It conserves IPv4 addresses: It conserves addresses through application port-level multiplexing. With NAT, internal hosts can share a single registered IPv4 address for all external communications. In this configuration, relatively few external addresses are required to support many internal hosts, and therefore conserve IPv4 addresses.

It provides mutual connectivity with overlapping addresses: It can provide mutual connectivity to networks with overlapping address spaces by using dual NAT (that is, translation of addresses from both networks).

Although NAT can provide some level of protection, its main objective is to solve addressing problems.

Inside NAT has several limitations:

Embedded IP addresses are problematic: NAT systems typically base translations on the packet header information. However, some protocols hide address information in other locations, like in the data portion of the packet. NAT systems must understand the protocol well enough to locate and modify these addresses and still preserve the validity of the packet itself.

Dynamic allocation requires state information that is not always available: Although TCP state information can be easily tracked and controlled, UDP traffic offers no mechanism at the packet header level to determine whether a packet is part of an ongoing conversation or if it is an isolated event. In such cases, when NAT systems have no additional security support, the system must guess how long a particular translation should be maintained.

NAT interferes with some encryption and authentication systems: Many data encryption systems attempt to ensure data integrity of packets to prevent tampering with the data while it is in transit. NAT systems are forms of packet tampering, and protocols must protect data so that NAT systems can perform. Protocols with combined embedded IP addresses that are used with NAT systems typically fail. One major exception is an IPsec system that protects the entire packet, including the headers.

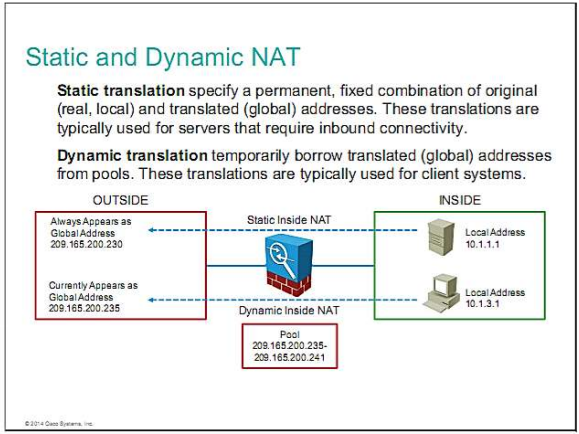
https://t.me/learningnets

Use of NAT alone can create problems with logging: In some cases, logging information might be provided after a translation. However, dynamic allocation of addresses interferes with logging. It can be complicated and tedious to correlate the logs with the NAT system to understand which internal systems were actually involved.

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

Static and Dynamic NAT

This topic describes static and dynamic NAT.



Inside NAT has many forms and varieties. One particular distinction is the difference between static and dynamic inside NAT:

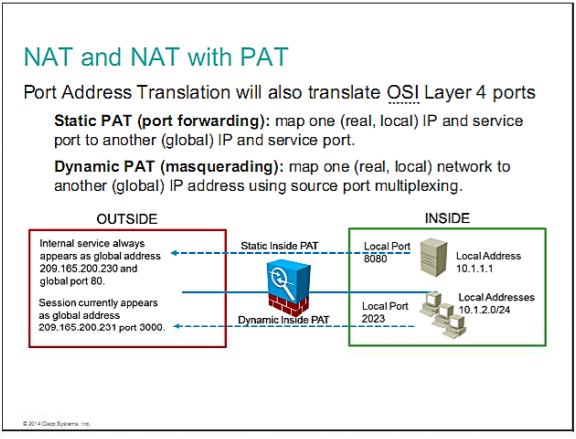
Static inside NAT maps a specific local IPv4 address in the inside NAT domain to another specific global IPv4 address (that is, one to one) with a preconfigured rule, when the local address in the inside NAT domain is communicating with the outside NAT domain. Static inside NAT is particularly useful when a device must be accessible from the outside NAT domain, using a constant global IP address. In this example, a host in the inside NAT domain with the real (local) IP address of 10.1.1.1 will appear to the outside NAT domain as a host with the (global) IP address of 209.165.200.230. Users in the outside NAT domain that connect to IP address 209.165.200.230 will be routed to host 10.1.1.1 in the inside NAT domain, based on the NAT gateway packet address rewriting.

Dynamic inside NAT maps a local IPv4 address in the inside NAT domain to a global IPv4 address that is temporarily borrowed from a pool of IPv4 addresses, when the local address in the inside NAT domain is communicating with the outside NAT domain. Dynamic NAT is typically used to support internal client access to the outside NAT domain, where the global IP address of the client as seen by the outside NAT domain does not need to be constant, and where not all clients in the inside NAT domain require translation. In this example, a host in the inside NAT domain with the local IP address of 10.1.3.1 will, when initiating a network session to the outside NAT domain, temporarily obtain a global IP address of 209.165.200.235 from the pool that is configured on the NAT gateway, and appear to the outside NAT domain as a host with that address. After some time (usually, after an idle timeout), the global address 209.165.200.235 will be returned to the pool and may be reused by another host in the inside NAT domain.

https://t.me/learningnets

NAT and NAT with PAT

This topic describes NAT with PAT.



One of the special varieties of NAT is PAT, which can also be static or dynamic. PAT translates individual connections; therefore it will alter both the address and one of the host session ports.

Static inside PAT, often called port forwarding, allows you to map a local host IP address and local service port (for example, the port that is used by a web server application) in the inside NAT domain to a global IP address and global service port that is valid in the outside NAT domain. In this example, a web server on the host with the local IP address of 10.1.1.1, running on TCP port 8080, will appear to the outside NAT domain with the IP address of 209.165.200.230, TCP port 80. Users in the outside NAT domain connecting to the IP address of 209.165.200.230, TCP port 80, will have their session translated to host 10.1.1.1, TCP port 8080, in the inside NAT domain, by the NAT gateway router.

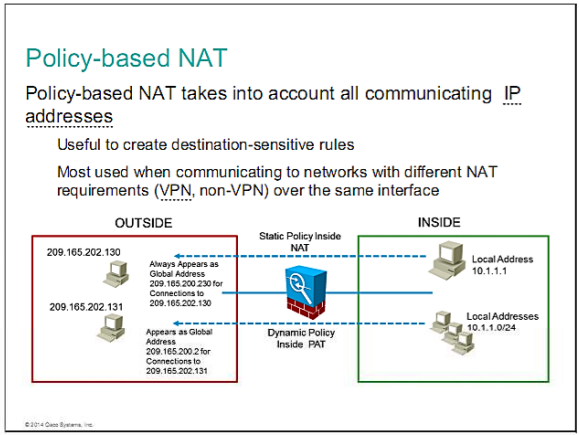
Dynamic inside PAT, sometimes also referred to as overload, enables you to translate multiple local addresses in the inside NAT domain into a single global address in the outside NAT domain. This translation essentially allows the multiple hosts in the inside NAT domain to appear as a single host in the outside NAT domain. Dynamic inside PAT translates both the local IP address and client (source) port of local hosts to distinguish between translations. Because the port number is encoded in 16 bits, the total number of addresses that PAT can translate into one global address is, theoretically, as many as 65,536, if each host would use only a single TCP or UDP connection through the NAT gateway. In this example, the subnet in the inside NAT domain using local IP addresses in the 10.1.2.0/24 prefix will appear to the outside NAT domain as 209.165.200.231 when initiating connections.

Dynamic inside PAT attempts to preserve the original source port. If the source port is already allocated, PAT attempts to find the first available port number. It starts from the beginning of the appropriate port group, 0 to 511, 512 to 1023, or 1024 to 65,535. If PAT does not find an available port from the appropriate port group, and if more than one global IPv4 address is configured, PAT moves to the next IPv4 address and tries to allocate the original source port again. PAT continues trying to allocate the original source port until it runs out of available ports and global IPv4 addresses.

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

Policy-based NAT

This topic describes policy-based NAT.



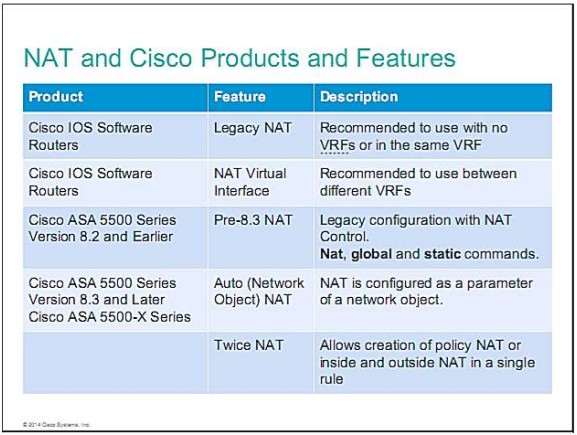
Sometimes a host might need to translate to different addresses, depending on the external host, or network, with which they are establishing a connection. NAT rules that are sensitive to all communicating endpoints are typically called policy NAT rules. A common example when policy inside NAT would be needed is when flows with a different NAT requirement are sourced by a particular network. For example, when hosts in the inside NAT domain send traffic to enterprise VPN sites in the outside NAT domain over a NAT gateway, typically they should not be translated. On the other hand, if these hosts connect to Internet destinations in the outside NAT domain, they will require translation.

In this example, a host in the inside NAT domain with the real address of 10.1.1.1 would require a static translation to the 209.165.200.230 address, but only when it is connecting to the host at the 209.165.202.130 address in the outside NAT domain. Additionally, the 10.1.1.0/24 subnet in the inside NAT domain should be translated to the global IP address 209.165.200.2, but only when connecting to the 209.165.202.131 host in the outside NAT domain.

https://t.me/learningnets

NAT and Cisco Products and Features

This topic describes Cisco products and features that are available to implement NAT.



The table lists some common Cisco devices and features that can be used to implement NAT.

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

Cisco IOS (and IOS XE) Software Routers with legacy NAT configuration: The legacy NAT configuration, where you have to designate interfaces as NAT inside or NAT outside. Cisco recommends to use legacy NAT for VRF to global NAT and between interfaces in the same VRF.

Cisco IOS (and IOS XE) Software Routers with NAT Virtual Interface: From IOS version 12.3(14)T, Cisco has introduced a new feature called NAT Virtual Interface. NVI removes the requirements to configure an interface as either NAT inside or NAT outside. NVI should be used to configure NAT between interfaces in different VRFs.

Cisco Adaptive Security Appliance 5500 Series Version 8.2 and Earlier: Cisco ASA Software Version 8.2 and earlier versions use NAT configurations that have existed since the Cisco Private Internet eXchange Firewall and can be very complex. With the capabilities that were introduced with the Cisco ASA security appliance, the earlier NAT configurations became cumbersome and difficult to organize. For example, the Cisco ASA security appliances support many virtual interfaces (VLANs) with many security levels, which make the NAT configurations of Cisco ASA Software Version 8.2 and earlier difficult to manage.

Cisco ASA 5500 Series Version 8.3 and Later and Cisco ASA 5500-X Series: Cisco ASA Software Version 8.3 and later versions use an object-oriented configuration to overcome the earlier configuration constraints. By creating an object for every host, translated address, and service that is used in translations, it is easier to understand how the NAT configuration is used. With Cisco ASA Software Version 8.3 and later, you can configure translations as network objects that are added to the configuration (auto NAT). You can also configure a policy NAT or inside and outside NAT using Twice NAT feature. You are no longer required to link nat commands into one or more global commands. As a result, the NAT configuration is easier to manage and should result in fewer configuration errors.

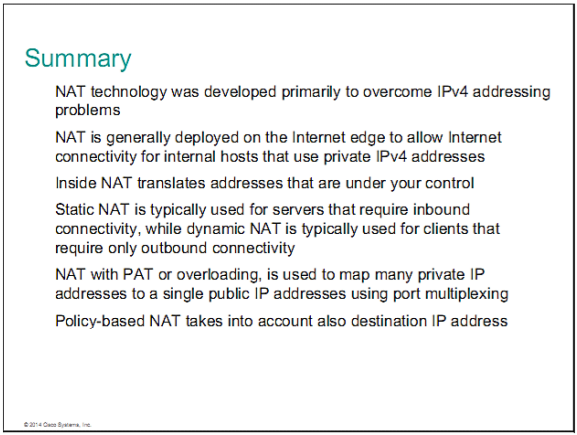
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Note	This course focuses on configuring legacy NAT on Cisco IOS Software and on configuring NAT on Cisco ASA Version 8.3 and Later.

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

Deploying Cisco ASA Network Address Translation

The Cisco Adaptive Security Appliance provides support for NAT to solve addressing issues when your internal networks interconnect with external networks. NAT translates the source and destination IP addresses of traffic that is going through the security appliance. NAT often works together with the PAT feature, which translates source ports in addition to IP addresses, and enables many internal hosts to share one public IP address. This lesson describes the configuration, verification, and troubleshooting procedures to implement NAT and PAT on the Cisco ASA.

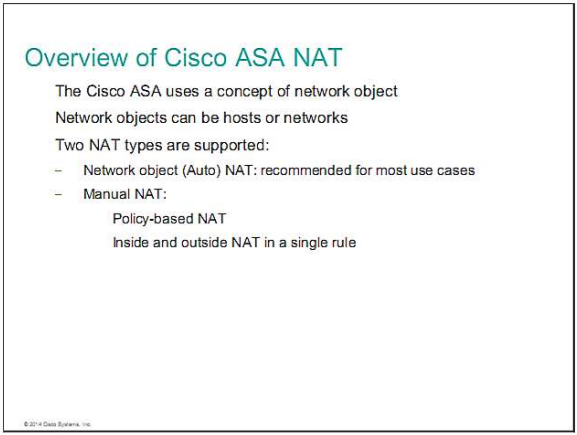
Upon completing this lesson, you will be able to:

- Describe NAT configuration on Cisco ASA
- Configure network object NAT on the Cisco ASA
- Configure static NAT using network object NAT on the Cisco ASA
- Configure dynamic NAT with PAT using network object NAT on the Cisco ASA
- Verify network object NAT on the Cisco ASA
- Configure twice NAT or manual NAT on the Cisco ASA
- Configure dynamic NAT using manual NAT on the Cisco ASA
- Configure twice NAT using manual NAT on the Cisco ASA
- Verify manual NAT on the Cisco ASA
- Troubleshoot NAT on the Cisco ASA

https://t.me/learningnets

Overview of Cisco ASA NAT

This topic provides an overview of NAT configuration on Cisco Adaptive Security Appliance.



The Cisco ASA uses a concept of network objects to configure NAT rules.

A network object defines a single host or a subnet. The host or subnet that is defined in the network object is used to identify the real (original) address in a NAT configuration. You also use network objects to define any available translation addresses, and you then refer to these objects in the NAT configurations.

While the NAT configuration usually refers to network objects, the NAT configuration might use network object groups to refer to the translated addresses.

The Cisco ASA can implement address translation in two ways: network object NAT and manual, or twice NAT. The main differences between these two NAT types are:

How you define the real address:

- Network object NAT: You define NAT as a parameter for a network object. A network object names an IP host, range, or subnet so you can then use the object in configuration instead of the actual IP addresses. The network object IP address serves as the real address. This method lets you easily add NAT to network objects that might already be used in other parts of your configuration.
- Manual NAT: You identify a network object or network object group for both the real and mapped addresses. In this case, NAT is not a parameter of the network object; the network object or group is a parameter of the NAT configuration. The ability to use a network object group for the real address means that manual NAT is more scalable.

How source and destination NAT is implemented:

- Network object NAT: Each rule can apply to either the source or destination of a packet. So two rules might be used, one for the source IP address, and one for the destination IP address. These two rules cannot be tied together to enforce a specific translation for a source/destination combination.

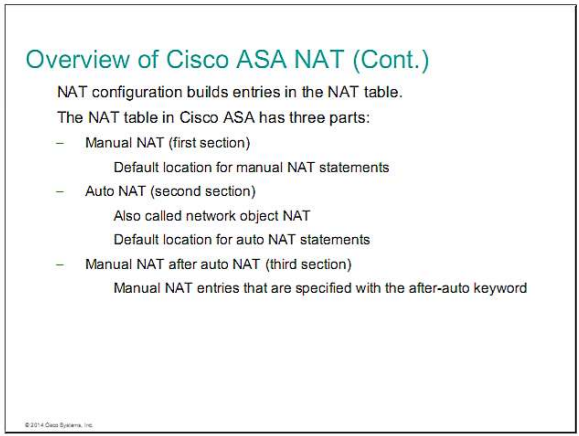
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

- Manual NAT: A single rule translates both the source and destination. A matching packet only matches the one rule, and further rules are not checked. Even if you do not configure the optional destination address for twice NAT, a matching packet still only matches one manual NAT rule. The source and destination are tied together, so you can enforce different translations depending on the source/destination combination. For example, sourceA/destinationA can have a different translation than sourceA/destinationB.

Order of NAT Rules:

- Network object NAT: Automatically ordered in the NAT table.
- Manual NAT: Manually ordered in the NAT table (before or after network object NAT rules).

It is recommended to use network object NAT unless you need the extra features that manual NAT provides, for example, when you have to implement inside and outside NAT or you have to implement policy-based NAT.



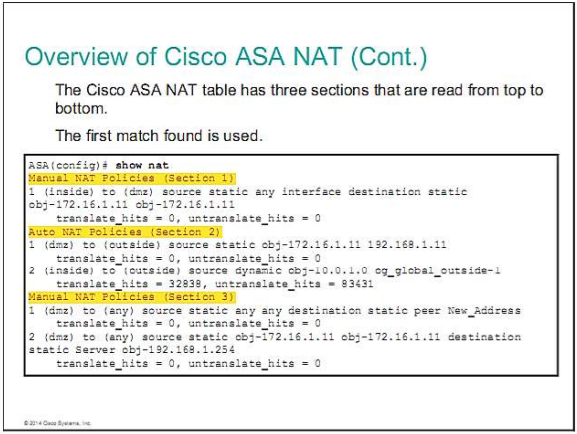
The NAT table on Cisco ASA has three sections:

Manual NAT (first section): The manual NAT section enables the administrator to define translations that the appliance compares before the other two sections. These translations are usually very precise. They can include translation on both the source and destination IP addresses, requiring the connection to be to a specific destination for the rule to match. You also add entries to this section when a host needs more than one defined translation because the translation depends on the output interface, the input interface, or the destination.

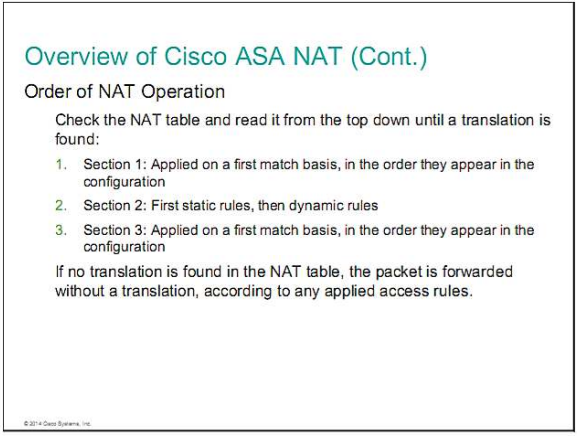
Auto NAT (second section): The auto NAT section, also referred to as network object NAT, contains translations that are defined in the object itself. This section allows each object definition to include a single translation for every object that is configured. These translations are usually static translations for servers that have clients connecting to them from the Internet or are dynamic translations for clients connecting to the Internet.

https://t.me/learningnets

Manual NAT after auto NAT (third section): The manual NAT section that comes after the auto NAT section contains manual NAT entries that could conflict with entries in the first two sections. These entries can be configured exactly like the Manual NAT section. However, these translations are not used unless the connection does not match any entries in the first two sections. This process allows you to configure less-specific translations that may conflict with one or more translations in the first two sections but that are not used unless the traffic does not match any entries in the first two sections.



The example in the figure shows the Cisco ASA NAT table.



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

The Cisco ASA use the entire NAT table to find a match. The NAT table is read from the top down, comparing all three sections, if necessary.

Network object NAT rules and twice NAT rules are stored in a single table that is divided into three sections. Section 1 rules are applied first, then section 2, and finally section 3:

Section 1: Applied on a first match basis, in the order they appear in the configuration. By default, twice NAT rules are added to section 1.

Section 2 rules are applied in the following order, as automatically determined by the ASA:

1. Static rules
2. Dynamic rules

Within each rule type, the following ordering guidelines are used:

a) Quantity of real IP addresses: From smallest to largest. For example, an object with one address will be assessed before an object with 10 addresses.

b) For quantities that are the same, then the IP address number is used, from lowest to highest. For example, 10.1.1.0 is assessed before 11.1.1.0.

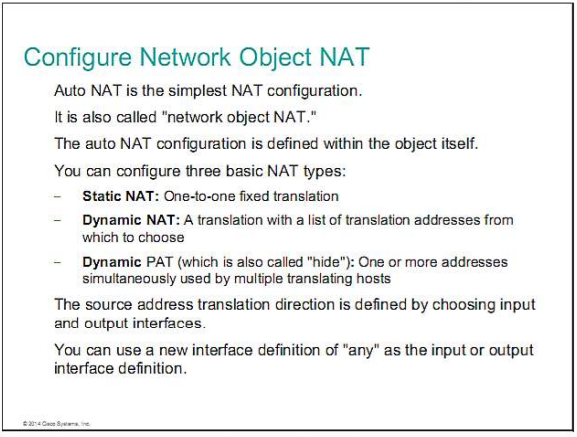
c) If the same IP address is used, then the name of the network object is used, in alphabetical order. For example, abracadabra is assessed before catwoman.

Section 3 rules are applied on a first match basis, in the order they appear in the configuration. You can specify whether to add a twice NAT rule to section 3 when you add the rule.

https://t.me/learningnets

Configure Network Object NAT

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



Auto NAT is the simplest NAT configuration on the Cisco ASA.

The configuration of auto NAT allows you to define one of three basic NAT configurations for the host:

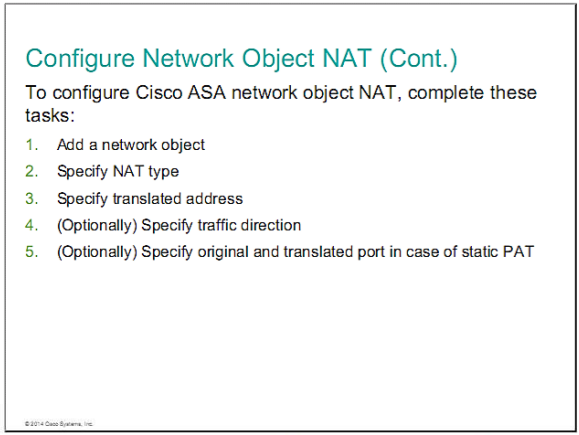
Static NAT: Static NAT is a one-to-one translation for the host that never changes. A static NAT configuration creates a permanent entry in the NAT table that can be used in both directions without the host having to initiate a connection, as long as the access policies allow the traffic.

Dynamic NAT: Dynamic NAT is a one-to-one translation that is defined after the host initiates a connection that matches the policy. This configuration allows multiple hosts to reuse translated addresses. Dynamic NAT is typically used when there are not enough translated IP addresses that are available for the number of hosts, but dynamic NAT uses fewer entries in the NAT table than PAT. (Instead of one entry per client, PAT uses a translation entry for every connection that is translated.) After a temporary translation is created by the host that is initiating the connection, that translation can be used in both directions as long as the access policies allow the traffic.

Dynamic PAT: Dynamic PAT is a many-to-one translation that allows one or more translated IP addresses to be used by multiple hosts simultaneously. A dynamic PAT translation allows connections from the host to be translated and only negotiated connections via applications that the security appliance inspects can be initiated from the server side.

The direction of the translation is defined by selecting the source host and the input and output interfaces. The use of "any" for the input or output interface adds a broader scope to the translation definition.

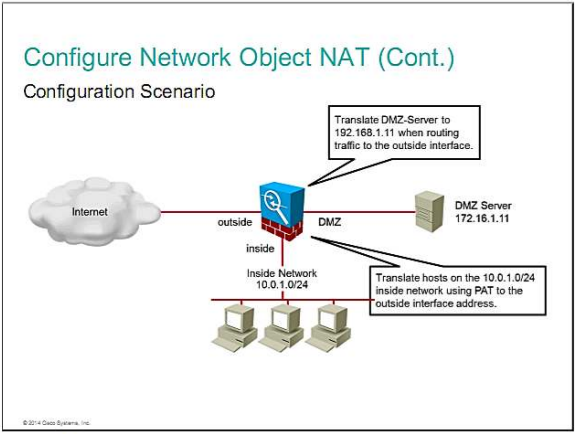
© 2014 Cisco Systems, Inc.
https://t.me/learningnets



When implementing Cisco ASA network object NAT, you will complete the following tasks:

1. First, you have to create a network object. The network object can either be a host or a network.
2. Then you have to specify a type of translation, which can be static, dynamic, or dynamic with PAT.
3. Then you have to select a translated IP address. The translated IP address can be a single IP address, a pool of addresses (both defined as network object), or the Cisco ASA interface.
4. Then you specify traffic direction by selecting incoming and outgoing interface. By default, a translation applies to traffic from any to any interface.
5. In case you are configuring static PAT, you can select original and translated port and protocol.

https://t.me/learningnets



This figure shows the configuration scenario that is used for the configuration tasks in this topic. You will configure dynamic PAT to enable internal hosts (reachable over the Cisco ASA security appliance inside interface) in the 10.0.1.0/24 subnet to connect to hosts that are reachable over the outside interface. Hosts should use the outside interface address as the translation address.

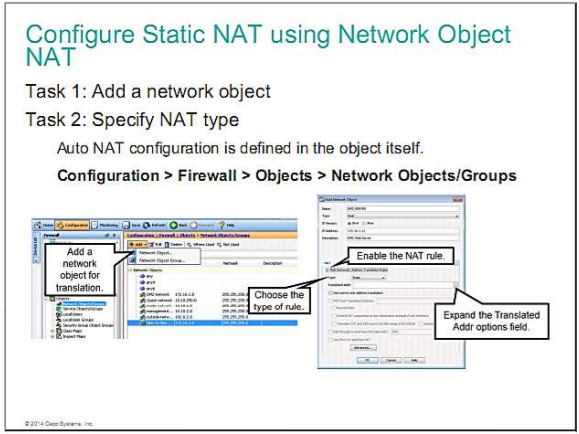
You will also configure static NAT to translate the address of the DMZ server (172.16.1.11) to 192.168.1.11 when traffic is routed to the outside interface.

This configuration scenario assumes that routing between all involved networks has been preconfigured on the Cisco ASA security appliance and that the access rules allow all the required communication between hosts.

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

Configure Static NAT Using Network Object NAT

This topic describes how to configure static NAT using network object NAT on the Cisco Adaptive Security Appliance.



Follow these steps to configure static NAT using Cisco Adaptive Security Device Manager:

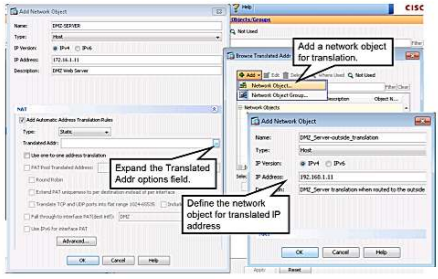
1. Choose **Configuration > Firewall > Objects > Network Objects/Groups**.
2. From the **Add** drop-down list, choose **Network Object**. The **Add Network Object** dialog box appears.
3. Enter a name for the network object. The example uses **DMZ-Server**.
4. From the **Type** drop-down list, choose the type of network object. In the example, **Host** is chosen.
5. Enter the IP address or subnet for the network object. The address **172.16.1.11** is entered in the example.
6. Check the **Add Automatic Address Translation Rules** check box.
7. From the **Type** drop-down list in the NAT section, choose the type of translation. **Static** is selected in the example.
8. To choose a translated address, expand the **Translated Addr** field.

https://t.me/learningnets

Configure Static NAT using Network Object NAT (Cont.)

Task 3: Specify translated address

Click the "…" button to choose the translated address.



Follow these steps to choose the translated address:

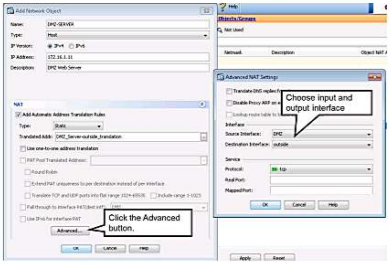
1. When you expand the **Translated Addr** field, the **Browse Translated Addr** window appears.
2. Click the **Add** button. The **Add Network Object** window appears.
3. Enter the translation object name in the **Name** field. **DMZ_Server-outside_translation** is entered in the example.
4. From the **Type** drop-down list, choose the object type. In the example, **Host** is selected.
5. Enter the object IP address. The address **192.168.1.11** is entered in the example.
6. (Optional) Enter a description for the object.
7. Click **OK** to close the **Add Network Object** window.
8. Click **OK** to close the **Browse Translated Addr** window.

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

Configure Static NAT using Network Object NAT (Cont.)

Task 4: Optionally specify traffic direction

In the **Advanced NAT Settings** window, specify in which direction to apply the source translation by selecting input and output interfaces.



Follow these steps to configure the traffic direction for the static NAT translation by choosing the source and destination interfaces:

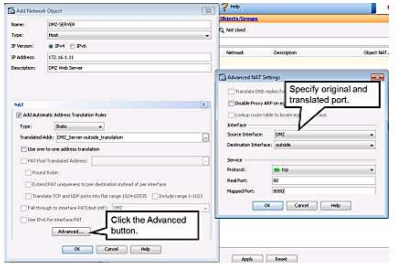
1. From the **Add Network Object** window, click the **Advanced** button. The **Advanced NAT Settings** window appears.
2. From the **Source Interface** drop-down list, choose the source (or input) interface. The default is **any**. In the example, the DMZ interface is selected.
3. From the **Destination Interface** drop-down list, choose the destination (or output) interface. The default is **any**. In the example, the outside interface is selected.
4. Click **OK** to close the **Advanced NAT Settings** window.
5. Click **OK** to close the **Add Network Object** window.
6. Click **Apply** to apply your settings.

https://t.me/learningnets

Configure Static NAT using Network Object NAT (Cont.)

Task 5: Optionally specify original and translated port

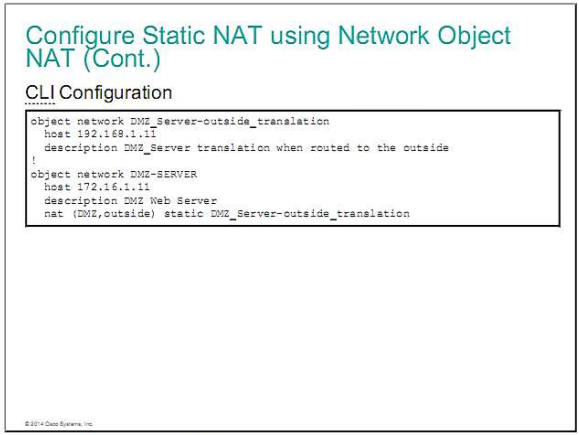
In the **Advanced NAT Settings** window, specify original and translated port.



Optionally, you can configure the real port and the mapped port to use for the static port translation (This step is not required for the configuration scenario in this topic). Follow these steps to configure this option:

1. From the Add Network Object window, click the **Advanced** button. The Advanced NAT Settings window appears.
2. From the Protocol drop-down list, choose the IP protocol for the translation. In the example, TCP is selected.
3. Enter the real port that is configured on the server. Port 80 is used in the example.
4. Enter the mapped (Translated) port. Port 8080 is used in the example.
5. Click **OK** to close the Advanced NAT Settings window.
6. Click **OK** to close the Add Network Object window.
7. Click **Apply** to apply your settings.

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



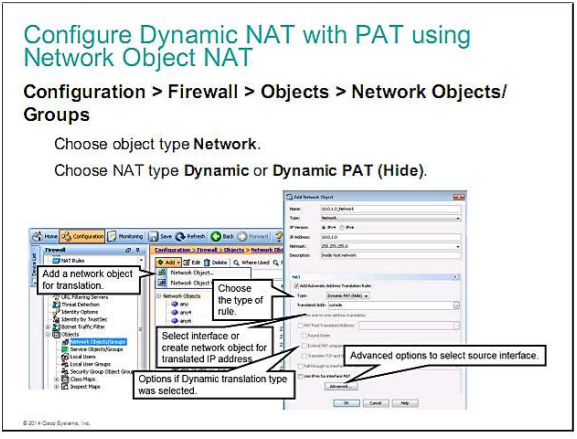
To configure static NAT using network object NAT on the Cisco ASA device using command line interface, use the commands that are described in the table.

Commands	Description
object network DMZ-SERVER	Creates the network object and enter network object group configuration mode
host 172.16.1.11	Specifies IP address of the network object
description DMZ Web Server	Specifies description for the network object
nat (DMZ,outside) static DMZ_Server-outside_translation	Configures static NAT for the network object

https://t.me/learningnets

Configure Dynamic NAT with PAT Using Network Object NAT

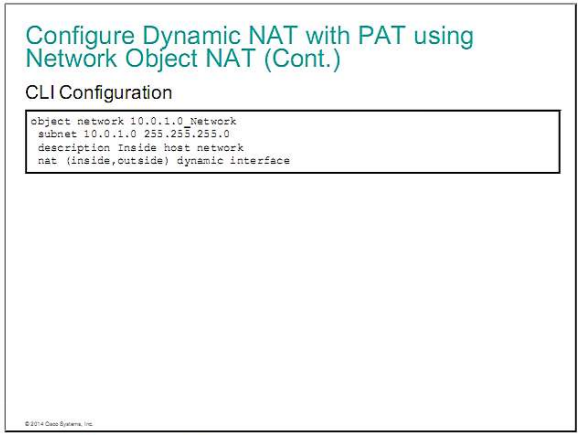
This topic describes how to configure dynamic NAT with PAT using network object NAT on the Cisco Adaptive Security Appliance.



Follow these steps to configure either dynamic NAT or dynamic PAT using Cisco Adaptive Security Device Manager:

1. Choose **Configuration > Firewall > Objects > Network Objects/Groups**.
2. From the **Add** drop-down list, choose **Network Object**. The **Add Network Object** dialog box appears.
3. Enter a name for the **Network Object**. The example uses **10.0.1.0_Network**.
4. From the **Type** drop-down list, choose the type of object. In the example, **Network** is selected.
5. Enter the **IP Address** or subnet for the network object. In the example, **10.0.1.0** is entered.
6. Enter the **Subnet Mask** for the network object. In the example, **255.255.255.0** is entered.
7. Check the **Add Automatic Address Translation Rules** check box.
8. From the **Type** drop-down list in the **NAT** section, choose the **Type** of translation. In the example, **Dynamic PAT (Hide)** is selected.
9. From the **Translated Addr** field, identify the network object or interface that should be used for the translation. In the example, the outside interface is used.
10. To configure the traffic direction for the dynamic PAT translation, from the **Add Network Object** window, click the **Advanced** button. Although not shown in this example, the **Advanced NAT Settings** window appears. From the **Source Interface** drop-down list, choose the source (input) interface and from the **Destination Interface** drop-down list, choose the destination (output) interface.
11. Click **OK** to close the **Advanced NAT Settings** window and click **OK** to close the **Add Network Object** window. Click **Apply** to apply your settings.

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



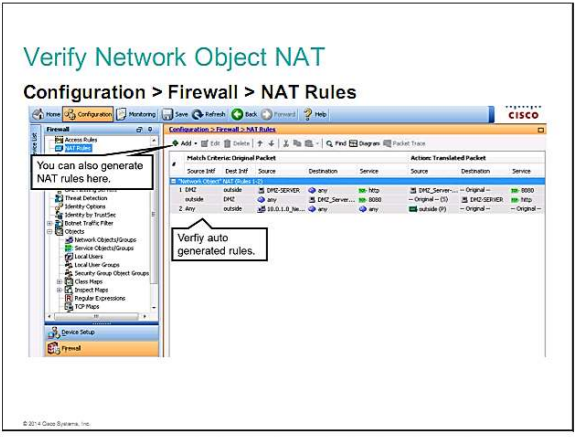
To configure static NAT using network object NAT on the Cisco ASA device using command line interface, use the commands that are described in the table.

Commands	Description
object network 10.0.1.0_Network	Creates the network object and enter network object group configuration mode
subnet 10.0.1.0 255.255.255.0	Specifies IP address of the network object
description Inside host network	Specifies description for the network object
nat (inside,outside) dynamic interface	Configures dynamic NAT for the network object

https://t.me/learningnets

Verify Network Object NAT

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



You can create auto generated NAT rules in the Cisco Adaptive Security Device Manager by navigating to **Configuration > Firewall > NAT Rules**. In the example, one static and one dynamic rules are created, as specified by the configuration scenario.

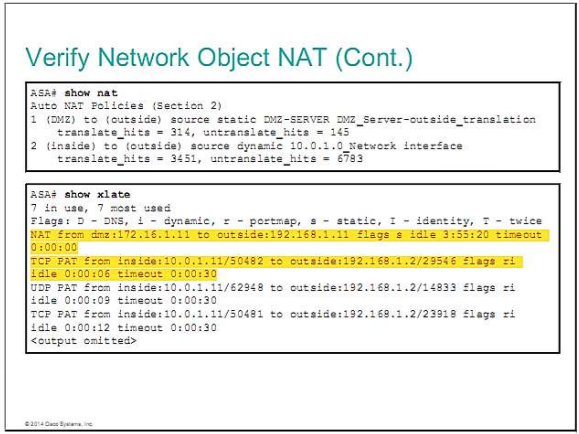
You can also configure network object NAT rules in this Cisco ASDM panel. The procedure is the same as describe in the previous topic.

Verify Network Object NAT (Cont.)

Verification Commands	Description
show nat	Displays statistics of NAT policies.
show xlate	Displays information about NAT sessions (xlates).

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

To verify network object NAT using command line, use the **show nat** and **show xlate** commands.



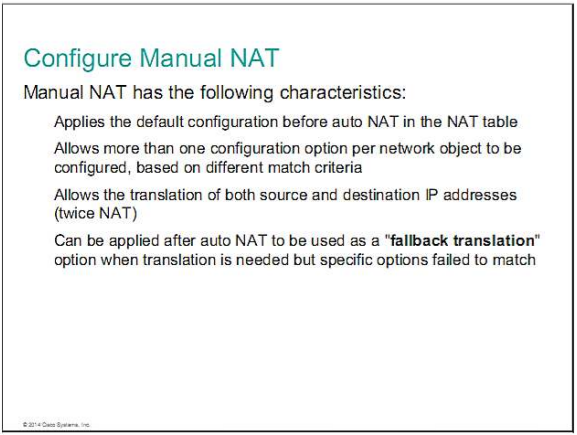
You can display the NAT table and statistics of NAT rules using the **show nat** command. In the example, static NAT and dynamic NAT with PAT rules are configured.

Use the **show xlate** command to see information about NAT sessions and how the configured NAT rules are being used on the Cisco ASA. The example in the figure shows a static auto NAT translation, which is identified by the "s" flag. The example also shows a dynamic PAT translation, which is identified by the tag "PAT" and the "r" and "i" flags.

https://t.me/learningnets

Configure Manual NAT

This topic describes how to configure twice NAT or manual NAT on the Cisco Adaptive Security Appliance.



In some situations, the NAT configuration may need more options than auto NAT provides. Other situations may need to specify exceptions to the auto NAT rules. Both of these situations can be managed using manual NAT configurations, which allow more options and are checked before the auto NAT section in the NAT table.

Manual NAT has the following characteristics:

- The default configuration is applied before the auto NAT section (section 2) in the NAT table.
- You are allowed to configure more than one option per network object, based on different match criteria.
- You can translate both the source and destination IP addresses, a characteristic that is referred to as twice NAT.
- By applying manual NAT after the auto NAT section, you can use it as a fallback translation option when translation is needed but specific options failed to match.

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

Configure Manual NAT (Cont.)

To configure Cisco ASA manual NAT, complete these tasks:

1. Add manual NAT rule
2. Specify original packet addresses
3. Specify translated packet addresses and NAT type

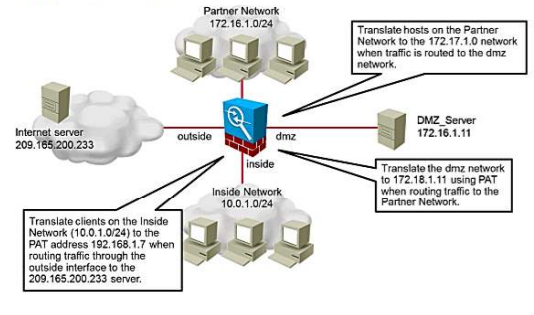
© 2014 Cisco Systems, Inc.

When implementing Cisco ASA manual NAT, you will complete the following tasks:

1. Add manual NAT rule
2. Then specify original source and destination IP address of a packet that requires translation.
3. Then specify translated source and destination IP address of a packet and select NAT type.

Configure Manual NAT (Cont.)

Configuration Scenario



© 2014 Cisco Systems, Inc.

This figure shows the scenario that is used for the configuration tasks in this topic.

https://t.me/learningnets

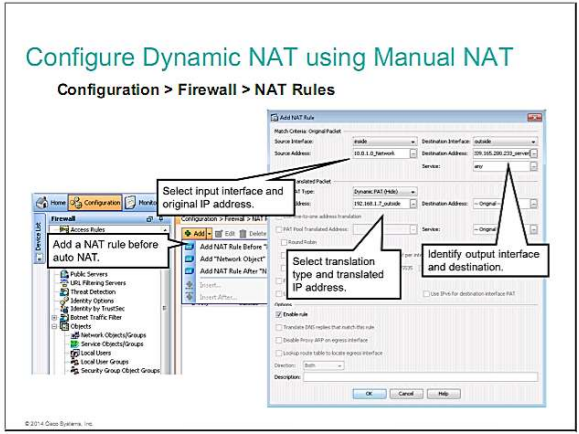
You will configure a policy-based NAT rule, which will translate clients on the inside network using dynamic PAT to 192.168.1.2 when they communicate with the server at 209.165.200.233. You will also configure twice NAT for communication between the DMZ network and Partner network, because both networks use overlapping IP address space.

This configuration scenario assumes that routing between all involved networks has been preconfigured on the Cisco ASA security appliance and that the access rules allow all the required communication between hosts.

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

Configure Dynamic NAT Using Manual NAT

This topic describes how to configure dynamic NAT using manual NAT on the Cisco Adaptive Security Appliance.

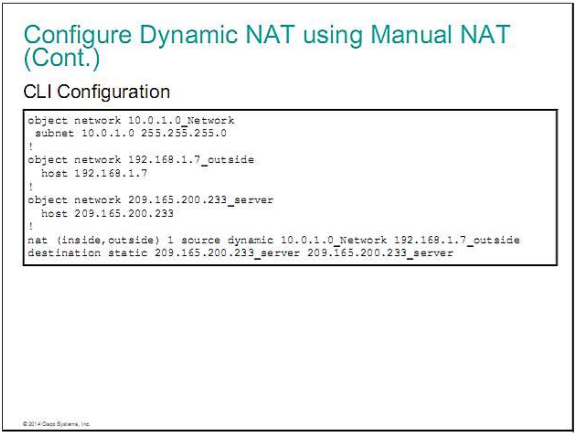


Based on the configuration scenario for this topic, you configure PAT to translate clients on the inside network to 192.168.1.7 when they are routing through the outside interface to the server at 209.165.200.233. Follow these steps to configure this translation using Cisco Adaptive Security Device Manager:

1. Choose **Configuration > Firewall > NAT Rules**.
2. From the Add drop-down menu, choose **Add NAT Rule Before "Network Object" NAT**. The Add NAT Rule dialog box appears.
3. From the Source Interface drop-down list, choose the interface that is the input interface for the translation. In the example, the inside interface is selected.
4. From the Source Address field in the Match Criteria: Original Packet area, click the ellipsis (…) button to choose the network object that identifies the source. In the example, 10.0.1.0_network is selected.
5. From the Destination Interface drop-down list, choose the interface that is the output interface for this translation. In the example, the outside interface is selected.
6. From the Destination Address field in the Match Criteria: Original Packet area, click the ellipsis (…) button to choose the network object that identifies the destination of the translation. In the example, 209.165.200.233_server is selected.
7. From the Source NAT Type drop-down list, choose the type of translation. **Dynamic PAT (Hide)** is selected in the example.
8. From the Source Address field in the Action: Translated Packet area, click the ellipsis (…) button to choose the object to use for the translation addresses. In the example, 192.168.1.7_outside is selected.
9. Ensure that the **Enable Rule** check box is checked (which is the default) to enable this rule. Optionally, you can enter a description about the translation rule.

https://t.me/learningnets

10. Click **OK** to close the Add NAT Rule window and click **Apply** to apply the changes.



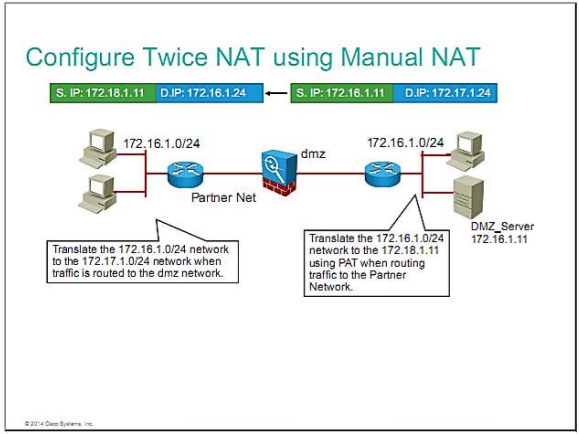
To configure dynamic NAT using manual NAT on the Cisco ASA device using command line interface, use the commands that are described in the table.

Commands	Description
object network 10.0.1.0_Network subnet 10.0.1.0 255.255.255.0	Creates the network object for the original source addresses.
object network 192.168.1.7_outside host 192.168.1.7	Creates the network object for the translated IP address.
object network 209.165.200.233_server host 209.165.200.233	Created the network object for the destination IP address.
nat (inside,outside) 1 source dynamic 10.0.1.0_Network 192.168.1.7_outside destination static 209.165.200.233_server 209.165.200.233_server	Configures dynamic manual NAT rule.

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

Configure Twice NAT Using Manual NAT

This topic describes how to configure twice NAT using manual NAT on the Cisco Adaptive Security Appliance.



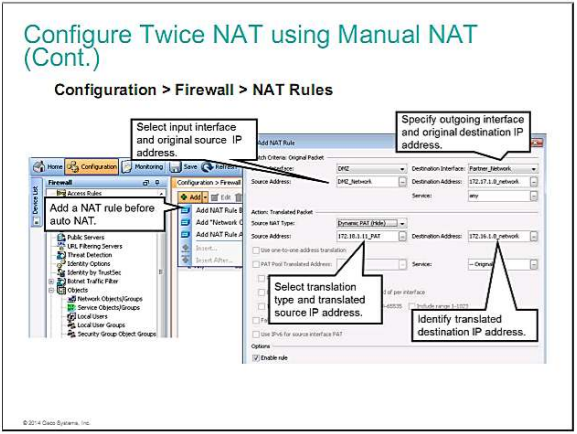
To this point, all the examples in this lesson were for inside NAT. Inside NAT translates IP addresses of hosts on input interfaces when they communicate with hosts on output interfaces. Outside NAT translates IP addresses of hosts on output interfaces when they communicate with hosts on input interfaces.

In some situations, you must configure both inside and outside NAT on the Cisco ASA security appliance to provide connectivity between overlapping address spaces. For the configuration scenario, two networks use the same IP address space of 172.16.1.0/24. Without NAT, when a host on the DMZ network attempts to access a host on the overlapping Partner Network, the Cisco ASA security appliance never receives the packet because the host attempts to directly forward the packet on the local LAN.

To solve this problem, configure inside and outside NAT to translate overlapping IP addresses by translating the Partner Network to a new address space and the DMZ network to another address space. Configuring both translations in the same NAT rule is referred to as twice NAT.

As shown in the figure, the DMZ server uses the 172.17.1.24 destination IP address to connect to the 172.16.1.24 host in the Partner Network. The Cisco ASA security appliance translates the 172.17.1.24 local destination address to the 172.16.1.24 global destination address. The security appliance also translates the 172.16.1.11 local source address to the 172.18.1.11 global address.

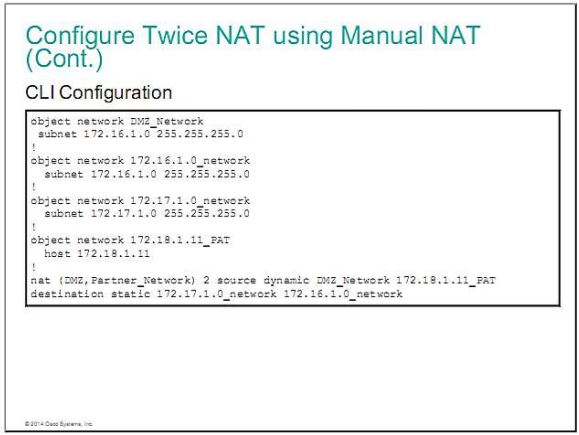
https://t.me/learningnets



Based on the configuration scenario for this topic, you configure twice NAT to translate source and destination IP addresses of traffic from the DMZ network to the Partner network. Follow these steps to configure this translation using Cisco Adaptive Security Device Manager:

1. Choose **Configuration > Firewall > NAT Rules**.
2. From the Add drop-down menu, choose **Add NAT Rule Before "Network Object" NAT**. The Add NAT Rule dialog box appears.
3. From the Source Interface drop-down list, choose the interface that is the input interface for the translation. In the example, the DMZ interface is selected.
4. From the Source Address field in the Match Criteria: Original Packet area, click the ellipsis (…) button to choose the network object that identifies the source. In the example, DMZ_Network is selected.
5. From the Destination Interface drop-down list, choose the interface that is the output interface for this translation. In the example, the Partner_Network interface is selected.
6. From the Destination Address field in the Match Criteria: Original Packet area, click the ellipsis (…) button to choose the network object that identifies the destination of the translation. In the example, 172.17.1.0_network is selected. Hosts in the DMZ network will have to use destination IP addresses from this network in order to communicate with hosts in the Partner network.
7. From the Source NAT Type drop-down list, choose the type of translation. **Dynamic PAT (Hide)** is selected in the example.
8. From the Source Address field in the Action: Translated Packet area, choose an object that will be used for the translation addresses. In the example, 172.18.1.11_PAT is selected.
9. From the Destination Address field in the Action: Translated Packet area, click the ellipsis (…) button to choose the network object that identifies the translation of the destination IP address. In the example, 172.16.1.0_network is selected. Destination IP addresses from the 172.17.1.0/24 network will be translated into the 172.16.1.0 network when traffic is routed to the Partner network.
10. Ensure that the **Enable Rule** check box is checked (which is the default) to enable this NAT rule.
11. Click **OK** to close the Add NAT Rule window and click **Apply** to apply the changes.

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



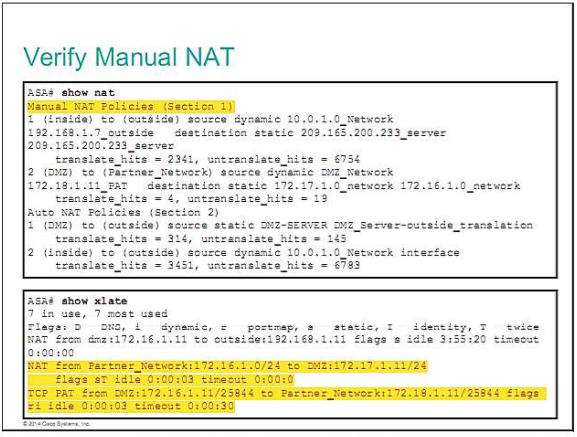
To configure twice NAT on the Cisco ASA device using command line interface, use the commands that are described in the table.

Commands	Description
object network DMZ_Network subnet 172.16.1.0 255.255.255.0	Creates the network object for the original source IP addresses (DMZ network as seen from the DMZ network).
object network 172.16.1.0_network subnet 172.16.1.0 255.255.255.0	Creates the network object for the translated destination IP address (Partner network as seen from the Partner network).
object network 172.17.1.0_network subnet 172.17.1.0 255.255.255.0	Creates the network object for the original destination IP address (Partner network as seen from the DMZ network).
object network 172.18.1.11_PAT host 172.18.1.11	Creates the network object for the translated source IP addresses (DMZ network as seen from the Partner network).
nat (DMZ,Partner_Network) 2 source dynamic DMZ_Network 172.18.1.11_PAT destination static 172.17.1.0_network 172.16.1.0_network	Configures dynamic twice NAT rule. Source IP addresses are translated using dynamic PAT, while destination IP addresses are always translated using dynamic NAT.

https://t.me/learningnets

Verify Manual NAT

This topic describes how to verify manual NAT on the Cisco Adaptive Security Appliance.



You can display the NAT table and statistics of NAT rules using the **show nat** command. In the example, the first section of the NAT table shows the configured manual NAT rules. The first one is policy-based rule that translated inside hosts to 192.168.1.7 IP address when they communicate with the server at 209.165.200.233. The second rule is the twice NAT rule, which translates source and destination IP addresses of traffic from the DMZ network to the Partner network.

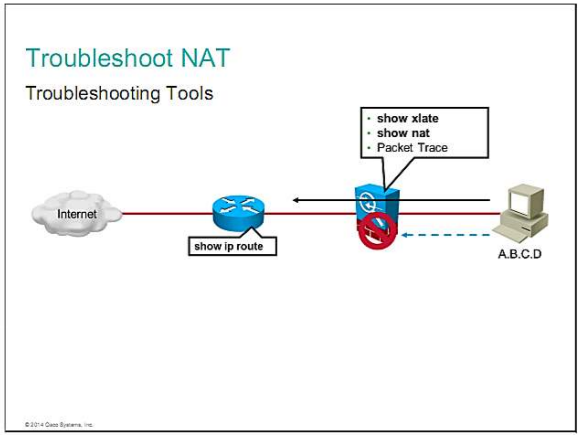
The second section of the NAT table displays auto (network object) NAT rules that were configured in the previous topics.

Use the **show xlate** command to see information about NAT sessions and how the configured NAT rules are being used on the Cisco ASA. The example in the figure shows the twice NAT translation, which consists of two translations. The first one is static translation, which translates destination IP addresses of traffic from the DMZ network to the Partner network. The second one is dynamic translation, which translates source IP addresses of traffic from the DMZ network to the Partner network. The static NAT is marked with s and T flags, while the dynamic translation is marked with r and i flags.

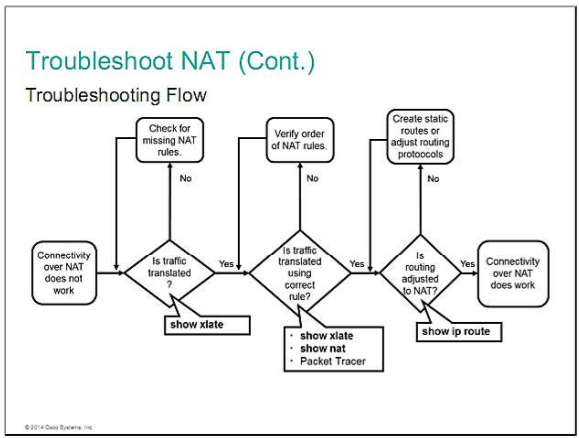
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Troubleshoot NAT

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



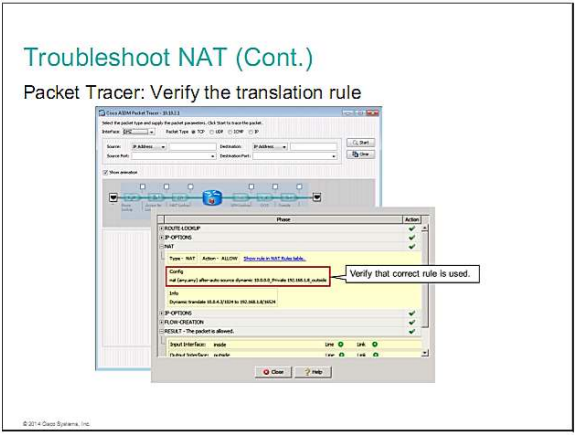
To troubleshoot NAT, you must troubleshoot activity on the ASA, while generating traffic from or to the local host that is subject to translation. The figure shows some common commands and tools that you can use when troubleshooting the connectivity over the NAT-enabled ASA. You may also need to check the configuration of other routers in the network, if possible.



https://t.me/learningnets

The flowchart in the figure shows the recommended troubleshooting task flow that you should use when troubleshooting NAT. Use the following troubleshooting steps:

1. First, verify whether the traffic with which you are having problems is being translated at all. Use the **show xlate** command to look for translations. If traffic is not being translated, check for misconfigured or missing **nat** commands.
2. If traffic is being translated but it is not being translated using the correct NAT rule, check for overlapping NAT rules. Remember that the NAT table is read from top to bottom. If there are conflicting rules, traffic may be matching on the incorrect rule. Examine the NAT table using the **show nat** command.
3. If the traffic is translated using correct NAT rule, but returning traffic does not come back to the ASA, verify routing configuration on the neighboring routers to determine that the addresses you are translating to (the global addresses) are properly routed to the ASA.

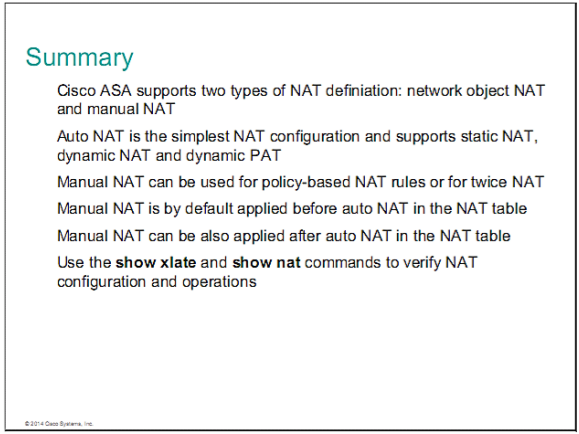


You can use the Cisco Packet Tracer tool to verify which rule is matched for the translation. Expand the **NAT** section to view the rule that is being used. To view the rule in the NAT configuration window of Cisco Adaptive Security Device Manager, click the **Show Rule in NAT Rules Table** link.

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

Summary

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



https://t.me/learningnets

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

Lesson 3

Deploying Cisco IOS Software Network Address Translation

Cisco IOS NAT and PAT are mechanisms that you can use to conserve registered IPv4 addresses in large networks, resolve overlapping addressing scenarios, and simplify IPv4 address management tasks. NAT and PAT translate IPv4 addresses within private internal networks to legal IPv4 addresses for transport over public external networks, such as the Internet, without requiring a registered subnet address. Incoming traffic is translated back for delivery within the inside network.

This translation of IPv4 addresses eliminates the need for host renumbering and allows the same IPv4 address range to be used in multiple intranets. This lesson describes how to configure, verify, and troubleshoot NAT and PAT on Cisco IOS Software routers.

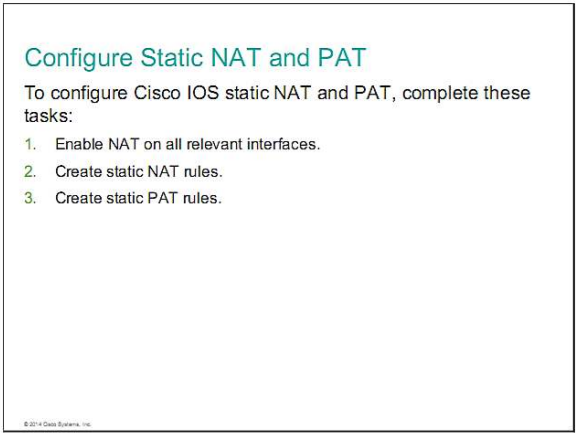
Upon completing this lesson, you will be able to:

- Configure static NAT and PAT on Cisco IOS Software routers
- Verify static NAT and PAT on Cisco IOS Software routers
- Configure dynamic NAT and PAT on Cisco IOS Software routers
- Configure policy-based dynamic NAT with PAT on Cisco IOS Software routers
- Verify dynamic NAT and PAT on Cisco IOS Software routers
- Troubleshoot NAT on Cisco IOS Software routers

https://t.me/learningnets

Configure Static NAT and PAT

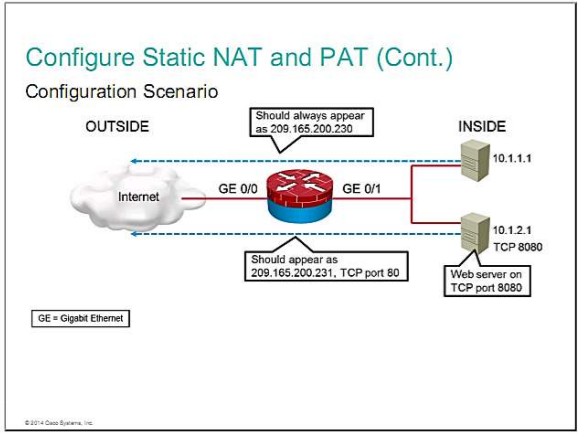
This topic describes how to configure static NAT and PAT on Cisco IOS Software routers.



To configure static NAT or PAT on a Cisco IOS Software router, you must perform the following configuration tasks:

1. Enable NAT on all interfaces that will potentially forward traffic that requires address translation, and tag the interfaces as belonging to either the inside or outside NAT domain.
2. Create static NAT rules for hosts in Cisco IOS Software.
3. Create static PAT rules for services in Cisco IOS Software.

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



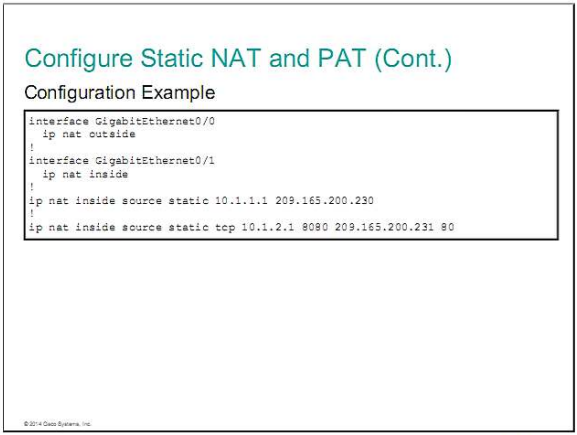
This figure presents the configuration scenario for the configuration tasks. The router acts as a NAT gateway and connects to the outside NAT domain with its GigabitEthernet0/0 interface and to the inside NAT domain with its GigabitEthernet0/1 interface.

You will create a static NAT rule for the host in the inside network, with the real IP address of 10.1.1.1. This host should appear as 209.165.200.230 to the outside network.

Additionally, you will create a static PAT rule for the web server service that runs on TCP port 8080 on the host with the real IP address of 10.1.2.1 in the inside network. This service should be available in the outside network at the IP address of 209.165.200.231, on TCP port 80.

The steps in the configuration sequence assume that the networks in the outside NAT domain route all traffic to addresses in the 209.165.200.0/24 network to the Cisco IOS router, and that the router is configured with IP addresses and IP routing features that enable connectivity between the two networks.

https://t.me/learningnets



To configure static NAT on a Cisco router, use the commands that are described in this table:

Commands	Description
interface GigabitEthernet0/0 **ip nat outside**	Enables NAT and tags the interface to outside hosts as "NAT outside"
interface GigabitEthernet0/1 **ip nat inside**	Enables NAT and tags the interface to inside hosts as "NAT inside"
ip nat inside source static 10.1.1.1 209.165.200.230	Creates a one-to-one address-based mapping
ip nat inside source static tcp 10.1.2.1 8080 209.165.200.231 80	Creates a one-to-one address- and port-based mapping

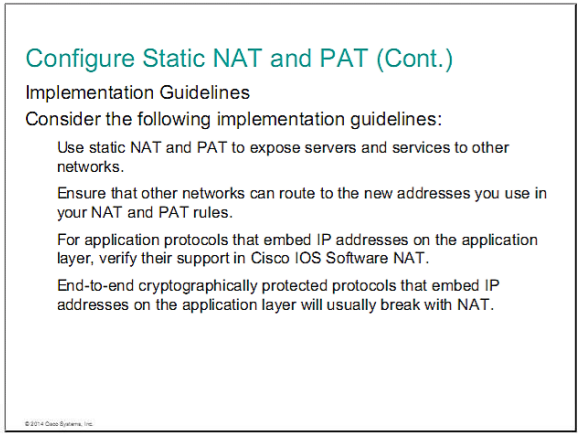
In the first task of this configuration sequence, you will enable NAT on all router interfaces where you expect traffic that requires translation to be forwarded over, and tag them as belonging to the NAT inside or NAT outside domain. In this example, these are the GigabitEthernet0/0 (outside NAT domain) and GigabitEthernet0/1 (inside NAT domain) interfaces.

Use the **ip nat outside** command to enable NAT on the GigabitEthernet0/0 router interface and tag it as an outside NAT domain interface. Use the **ip nat inside** command to enable NAT on the GigabitEthernet0/1 router interface and tag it as an inside NAT domain interface.

In the second configuration task, you will create a static NAT translation for the host with the real IP address of 10.1.1.1. Use the **ip nat inside source static** command to translate the real (local) IP address of 10.1.1.1 to the 209.165.200.230 (global) address.

Finally, in the third configuration task, you will create static PAT translation for the service that is running on the host with the real IP address of 10.1.1.1, on port 8080. Use the **ip nat inside source static tcp** command to specify the local IP address and port, and the global IP address and port for this TCP-based service.

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



When implementing static NAT or PAT using Cisco IOS Software, consider the following guidelines:

Use static NAT or PAT mostly to expose servers and specific services to other networks.

When translating addresses, ensure that the other network can route to the translated (global) addresses of local hosts.

Before deploying applications over a NAT gateway, ensure that the application is NAT compatible, or that the Cisco IOS Software NAT features provide special handling for the application.

If you use end-to-end cryptography between hosts, and the applications they use embed IP addresses on the application layer (for example, FTP), these applications will fail when NAT is used in the path between hosts because the NAT gateway cannot translate the embedded (encrypted) IP address. Remove the end-to-end cryptographic protection, if it is feasible and not risky, or bypass the NAT gateway with these sessions.

https://t.me/learningnets

Verify Static NAT and PAT

This topic describes how to verify static NAT and PAT on Cisco IOS Software routers.

Verify Static NAT and PAT

Verification Commands	Description
show ip nat translations	Displays active NAT or PAT translations
show ip nat statistics	Displays the statistics of the NAT feature

© 2014 Cisco Systems, Inc.

To display active NAT translations, use the **show ip nat translations** command..

To display NAT statistics, use the **show ip nat statistics** command.

Verify Static NAT and PAT (Cont.)

```
Router# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 209.165.200.230:80 10.1.1.1:80        209.165.201.233:1148
209.165.201.233:1148
tcp 209.165.200.231:80 10.1.2.1:8080      209.165.201.233:1162
209.165.201.233:1162
--- 209.165.200.230    10.1.1.1           ---                ---
tcp 209.165.200.231:80 10.1.2.1:8080      ---                ---
```

```
Router# show ip nat statistics
Total active translations: 2 (2 static, 0 dynamic; 1 extended)
Outside interfaces:
  GigabitEthernet0/0
Inside interfaces:
  GigabitEthernet0/1
Hits: 656547  Misses: 0
CEF Translated packets: 57348952347, CEF Punted packets: 7434
Expired translations: 0
Dynamic mappings:
```

© 2014 Cisco Systems, Inc.

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

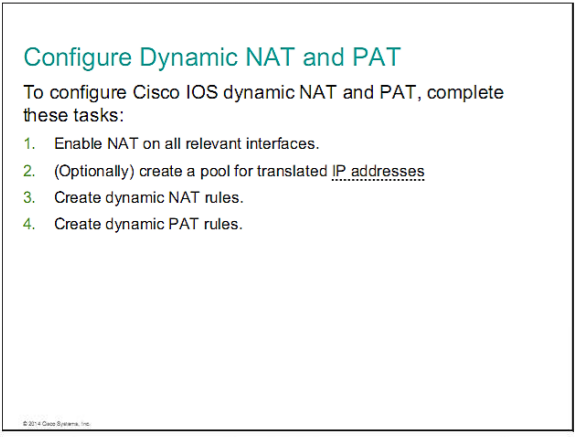
You can use the **show ip nat translations** command to show static NAT or PAT translations. These translations will appear in the translation table even if there is no traffic matching them (the last two entries in the table). In the example, two static translations can also be seen for actual traffic. The first one is static NAT translation, which translates local IP address of 10.1.1.1 to 209.165.200.230. The second one is a static NAT with PAT translation which translates local IP address of 10.1.2.1 and local TCP port 8080 to translated IP address of 209.165.200.231 and port 80

Use the **show ip nat statistics** command to display the statistics of the Cisco IOS Software NAT feature. These counters will indicate if traffic is being translated by NAT, and if NAT is enabled on the correct interfaces.

https://t.me/learningnets

Configure Dynamic NAT and PAT

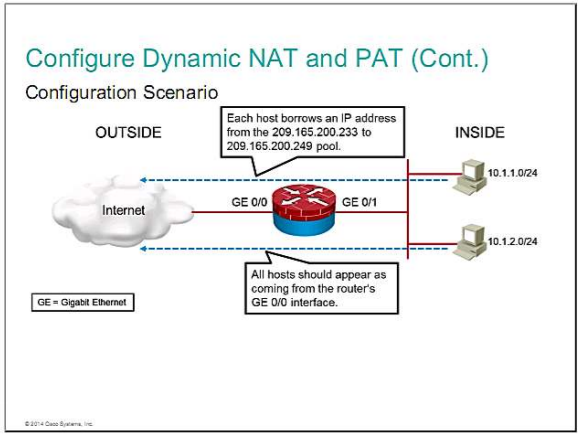
This topic describes how to configure dynamic NAT and PAT on Cisco IOS Software routers.



To configure dynamic NAT or PAT on a Cisco IOS Software router, you must perform the following configuration tasks:

1. Enable NAT on all interfaces that will potentially forward traffic that requires address translation.
2. Optionally create a pool of IP address(es) that will be used to translate traffic that requires address translation. Instead of using a pool of IP addresses, you can also configure hosts to translate into an IP address of a router's interface.
3. Create dynamic NAT rules for hosts.
4. Create dynamic PAT rules for hosts and networks.

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

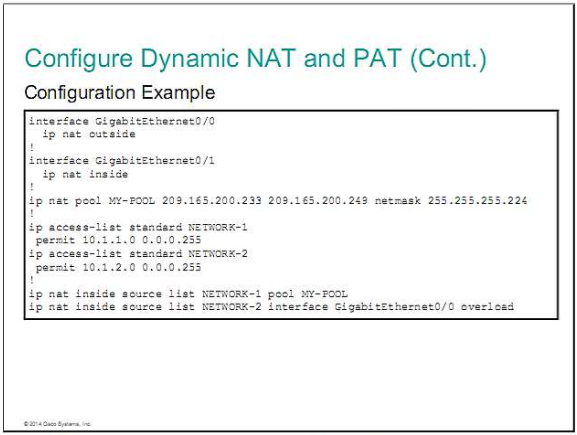


This figure presents the configuration scenario for the configuration tasks. You will create a dynamic NAT rule for the 10.1.1.0/24 subnet in the inside NAT domain. Hosts in the 10.1.1.0/24 subnet should appear with addresses from the 209.165.200.233 to 209.165.200.249 range in the outside NAT domain. You will create temporary one-to-one translations, where each communicating host in the 10.1.1.0/24 subnet will obtain its own temporary address to which to translate. Note that the pool is too small to provide global addresses to all hosts in the local 10.1.1.0/24 subnet. This may not be a problem because not all hosts in the 10.1.1.0/24 subnet communicate with the outside NAT domain at the same time.

Next, you will create a dynamic PAT rule for the 10.1.2.0/24 subnet in the inside NAT domain. Hosts in this network should appear as the single IP address of the router's GigabitEthernet0/0 interface in the outside NAT domain. Since only one IP address is available for translations, dynamic NAT with PAT will be used in this example.

The steps in the configuration sequence assume that the outside NAT domain routes all traffic to addresses in the 209.165.200.0/24 network to the Cisco IOS router and that the router is configured with IP addresses and IP routing features, therefore enabling connectivity between the two domains.

https://t.me/learningnets



In the first task of this configuration sequence, you will enable NAT on all router interfaces in the same manner as in the previous topic. In this example, use the **ip nat outside** command to enable NAT on the GigabitEthernet0/0 and place it in the outside NAT domain, and the **ip nat inside** command to enable NAT on the GigabitEthernet0/1 interface and place it in the inside NAT domain.

In the second configuration task, you will define a named NAT pool of global addresses using the **ip nat pool** command, and specify the range of global IP addresses available to this pool, and network mask of the network IP addresses will translate to.

In the third configuration task, you will create a dynamic NAT translation rule for the local 10.1.1.0/24 subnet, and translate these hosts to global addresses from a dynamic address pool.

Start by defining a standard Cisco IOS Software ACL, matching (permitting) local hosts in the 10.1.1.0/24 subnet, using the **ip access-list standard** command.

Using the **ip nat inside source list** command, reference the standard ACL to specify the local address range, and reference the named pool to specify the global addresses to which local hosts will be translated one-to-one, using temporary addresses from the named pool.

In the fourth configuration task, you will create a dynamic PAT translation rule for the local 10.1.2.0/24 subnet, and translate these hosts to a single global IP address.

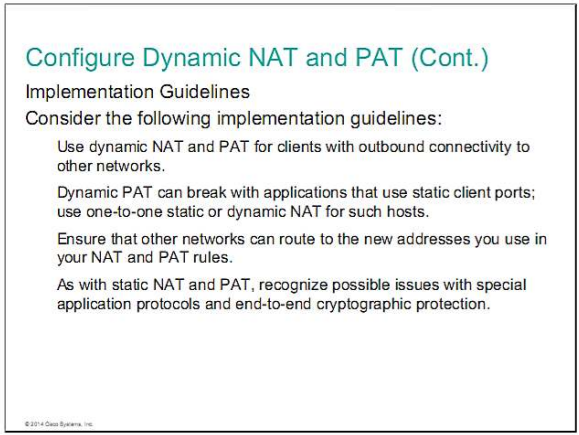
Start by defining a standard Cisco IOS Software ACL, matching (permitting) local hosts in the 10.1.2.0/24 subnet, using the **ip access-list standard** command.

Using the **ip nat inside source list interface** command, reference the standard ACL to specify the local address range, and reference the router's interface to which local hosts will be translated. At the end of the **ip nat inside source list** command, add the **overload** keyword to specify a many-to-one PAT translation for this rule.

To configure dynamic NAT on the Cisco router, use the commands that are described in this table:

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

Commands	Description
interface GigabitEthernet0/0 **ip nat outside**	Enables NAT and tags the interface to outside hosts as "NAT outside"
interface GigabitEthernet0/1 **ip nat inside**	Enables NAT and tags the interface to inside hosts as "NAT inside"
ip nat pool MY-POOL 209.165.200.233 209.165.200.249 netmask 255.255.255.224	Creates a NAT pool with a range of IP addresses
ip access-list standard NETWORK-1 **permit 10.1.1.0 0.0.0.255** **!** **ip access-list standard NETWORK-2** **permit 10.1.2.0 0.0.0.255**	Creates an ACL to match the source network
ip nat inside source list NETWORK-1 pool MY-POOL	Creates a NAT rule that translates the source network to the pool
ip nat inside source list NETWORK-2 interface GigabitEthernet0/0 overload	Creates a NAT rule that translates the source network to the overloaded router's interface



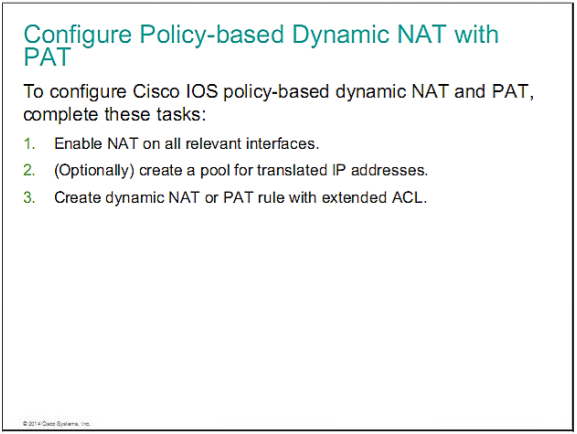
When implementing static NAT or PAT using Cisco IOS Software, consider the following guidelines:

- Use dynamic NAT or PAT mostly to provide clients with outbound connectivity to other networks.
- As with static NAT, ensure that the other networks can route to the translated (global) addresses of local hosts.
- As with static NAT, ensure application compatibility and cryptography issues before deploying applications over a NAT gateway.

https://t.me/learningnets

Configure Policy-Based Dynamic NAT with PAT

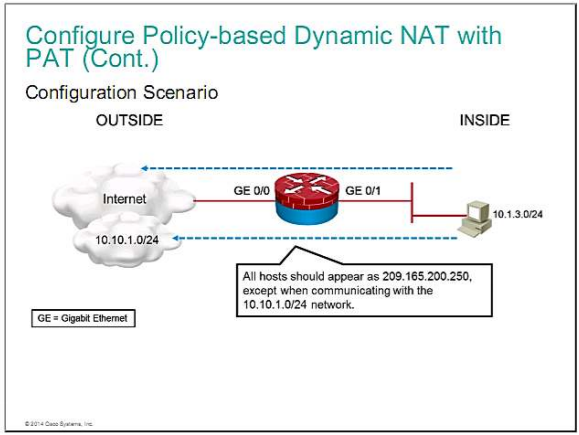
This topic describes how to configure policy-based dynamic NAT with PAT on Cisco IOS Software routers.



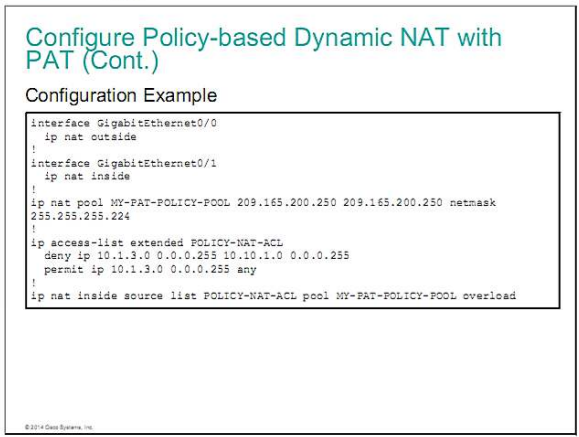
To configure dynamic NAT or PAT on a Cisco IOS Software router, you must perform the following configuration tasks:

1. Enable NAT on all interfaces that will potentially forward traffic that requires address translation.
2. Optionally create a pool of IP address(es) that will be used to translate traffic that requires address translation. Instead of using pool of IP addresses, you can also configure hosts to translate into IP address of a router's interface.
3. Create dynamic NAT or PAT rules for hosts. This time you have to reference an extended ACL, because you have to specify also destination of traffic that require translation.

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



This figure presents the configuration scenario used in upcoming configuration tasks. You will create a policy dynamic NAT rule for hosts in the 10.1.3.0/24 subnet in the inside NAT domain. These hosts should appear as the single global IP address 209.165.200.250 in the outside NAT domain, but only when they do not communicate with the 10.10.1.0/24 subnet in the outside NAT domain, for example, a business partner network reachable over a VPN.



In the first task of this configuration sequence, you will enable NAT on all router interfaces in the same manner as in the previous topic. In this example, use the **ip nat outside** command to enable NAT on the GigabitEthernet0/0 and place it in the outside NAT domain, and the **ip nat inside** command to enable NAT on the GigabitEthernet0/1 interface and place it in the inside NAT domain.

https://t.me/learningnets

In the second configuration task, you will define a named pool of global addresses using the **ip nat pool** command, and specify the single global IP addresses available to this pool by using the same starting and ending IP address.

In the final configuration task, you will create a dynamic policy PAT translation rule for the local 10.1.3.0/24 subnet, and translate these hosts to a single global IP address, except when the 10.1.3.0/24 subnet is exchanging traffic with the 10.10.1.0/24 subnet in the outside NAT domain.

Start by defining an extended ACL, not matching (denying) traffic between hosts in the 10.1.3.0/24 subnet and hosts in the 10.10.1.0/24 subnet, and matching (permitting) traffic between hosts in the 10.1.3.0/24 subnet and any other hosts using the **ip access-list extended** command. Then, define a named pool of global addresses using the **ip local pool** command, and specify a single global IP address inside this pool.

Using the **ip nat inside source list** command, reference the extended ACL to specify the flows subject to NAT, and reference the named pool to specify the global address to which local hosts will be translated. Add the **overload** keyword to specify a many-to-one PAT translation for this rule.

To configure policy-based dynamic NAT on the Cisco router, use the commands that are described in this table:

Commands	Description
interface GigabitEthernet0/0 **ip nat outside**	Enables NAT and tags the interface to outside hosts as "NAT outside"
interface GigabitEthernet0/1 **ip nat inside**	Enables NAT and tags the interface to inside hosts as "NAT inside"
ip nat pool MY-PAT-POLICY-POOL 209.165.200.250 209.165.200.250 netmask 255.255.255.224	Creates a NAT pool
ip access-list extended POLICY-NAT-ACL **deny ip 10.1.3.0 0.0.0.255 10.10.1.0 0.0.0.255** **permit ip 10.1.3.0 0.0.0.255 any**	Creates an ACL to match the source and destination networks
ip nat inside source list POLICY-NAT-ACL pool MY-PAT-POLICY-POOL overload	Creates a NAT rule that translates the specified flows to the pool

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

Verify Dynamic NAT and PAT

This topic describes how to verify dynamic NAT and PAT on Cisco IOS Software routers.

Verify Dynamic NAT and PAT

Verification Commands	Description
show ip nat translations	Displays active NAT or PAT translations
show ip nat statistics	Displays the statistics of the NAT feature

© 2014 Cisco Systems, Inc.

To display active NAT translations, use the **show ip nat translations** command..

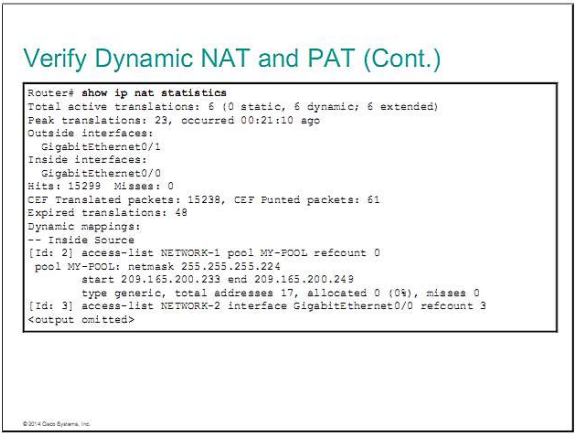
To display NAT statistics, use the **show ip nat statistics** command.

Verify Dynamic NAT and PAT (Cont.)

```
Router# show ip nat translations
Pro Inside global          Inside local   Outside local  Outside global
icmp 209.165.200.251:2     10.1.3.2:2     10.12.1.5:2    10.12.1.5:2
tcp  209.165.200.251:1183  10.1.3.2:1183  10.12.1.4:23   10.12.1.4:23
 <output omitted >
```

© 2014 Cisco Systems, Inc.

https://t.me/learningnets

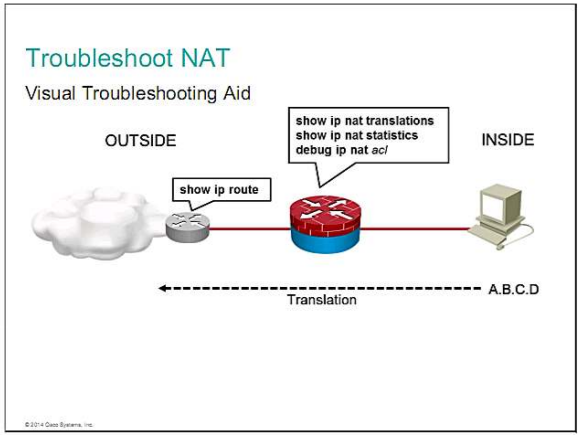


As with static NAT and PAT, you can use the **show ip nat translations** and **show ip nat statistics** commands to verify your configuration and NAT operation. Note that no dynamic translations will appear in the translation table until traffic forwarded over the NAT gateway triggers their creation. In the example, two dynamic translations can be seen. The first one is for ICMP traffic from the 10.1.2.3 host to 10.12.1.5 host, and the other one is for Telnet traffic from the 10.1.2.3 host to 10.12.1.4 host.

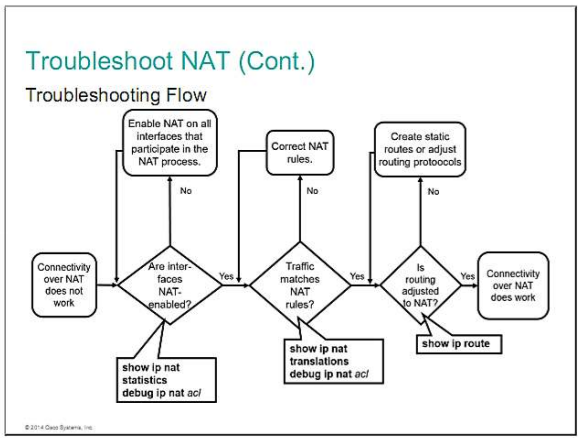
©2014 Cisco Systems, Inc.
https://t.me/learningnets

Troubleshoot NAT

This topic describes how to troubleshoot NAT on Cisco IOS Software routers.



In order to troubleshoot issues related to the Cisco IOS Software NAT feature, you can use a set of Cisco IOS Software CLI verification and debugging features. This figure shows some common commands and features that you may find useful during the troubleshooting session. Typically, you will examine why a particular session cannot be established through a NAT-enabled router. You may also need to check the configuration of other routers in the network.

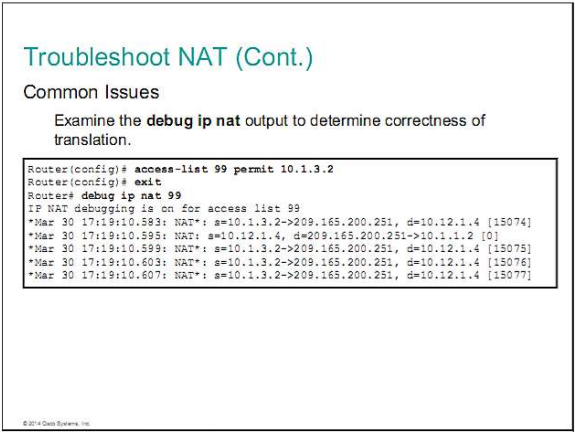


https://t.me/learningnets

The figure shows the recommended task flow for troubleshooting access through a NAT-enabled router. Follow these steps, and use the provided commands to troubleshoot events where a host appears to have connectivity issues due to implemented NAT or PAT rules:

1. Using the **show ip nat statistics** command, verify that all interfaces that should forward translated traffic are NAT-enabled and assigned the correct inside or outside NAT domain role. You may also use the **debug ip nat** command to see which packets undergo translation based on current rules.
2. Use an ACL with the **debug ip nat** command in busy environments to avoid information overload and router performance issues.
3. If appropriate interfaces are NAT-enabled, then, based on the configuration, clearly define what NAT is supposed to achieve. You might determine that there is a problem with the NAT rule configuration. Examine your configuration: use the **show ip nat translations** command to determine if the correct translations exist in the translation table, and the **debug ip nat** command to see which packets match the configured translation rules.
4. Verify that routing in your network is adjusted to support NAT. In the network that you are translating to, verify routes on neighboring devices, and throughout the entire routing domain (if possible), to determine that the addresses you are translating to (the global addresses) are properly routed to the NAT gateway.

If all these steps do not resolve your issue, you may need to deploy troubleshooting tools that are beyond the scope of this course.

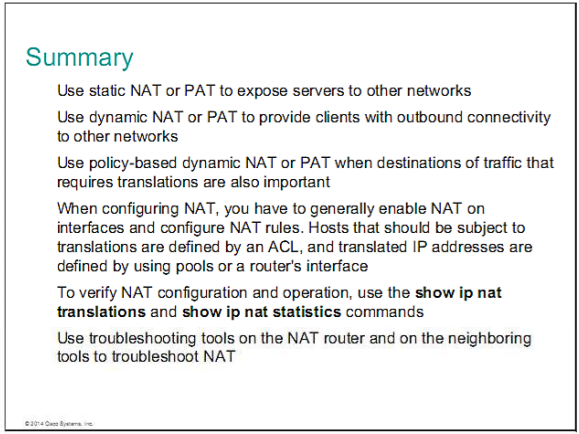


This printout shows a typical output of the **debug ip nat** command, showing the processing of each individual packet inside the NAT feature on the router. In this example, you can observe the translation of the source address (s=) in the first line, indicating the translated (global) address as well. You can use this as a tool to verify correct translation of a specific flow that can be triggered during the troubleshooting process.

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

Summary

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



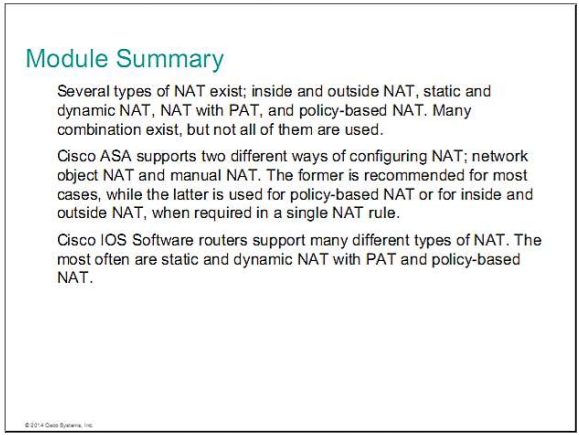
https://t.me/learningnets

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

Module Summary

Overview

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



https://t.me/learningnets

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

Module Self-Check

Questions

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

1. Which is a benefit of NAT? (Source: Introducing Network Address Translation)

   A. NAT provides for outside devices to access the real IP of internal hosts
   B. NAT mitigates the depletion of public IPv4 addresses
   C. NAT allows you to use global IP addresses in your internal network space
   D. NAT was developed migrate networks to a new address scheme

2. What are three benefits of Inside NAT? (Choose three.) (Source: Introducing Network Address Translation)

   A. There is no need to readdress internal networks
   B. It allows for translation of embedded IP addresses
   C. Conserves IPv4 addresses
   D. It provides mutual connectivity with overlapping IP address
   E. It works with all encryption systems

3. Which two types of NAT are supported on the Cisco ASA? (Choose two.) (Source: Deploying Cisco ASA Network Address Translation)

   A. Access NAT
   B. Host NAT
   C. Manual NAT
   D. Object, or Auto NAT

https://t.me/learningnets

4. Which is true of a static Network Object NAT configuration? (Source: Deploying Cisco ASA Network Address Translation)

   A. Source address translation must be mapped to a specific input or output interface
   B. It is the simplest NAT to configure
   C. Traffic direction must be defined
   D. Service port information cannot be configured

5. Which is true of a Manual NAT configuration? (Source: Deploying Cisco ASA Network Address Translation)

   A. The default configuration is applied before the auto NAT section in the NAT table
   B. Only one option per network object can be configured
   C. It can only translate the destination IP address
   D. It must be configured as outside NAT

6. What is the first step you must perform when configuring NAT on a Cisco IOS router? (Source: Deploying Cisco IOS Software Network Address Translation)

   A. Specify the source IP address
   B. Modify routing tables, if needed
   C. Create a pool of IP addresses that will be used to translate traffic
   D. Enable NAT on the desired interfaces

7. When configuring policy-based NAT, which type of access control list should be configured to match both the source and destination IP addresses? (Source: Deploying Cisco IOS Software Network Address Translation)

   A. Dynamic ACL
   B. Standard ACL
   C. Reflexive ACL
   D. Extended ACL

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

Answer Key

1. B

2. A, C, D

3. C, D

4. B

5. A

6. D

7. D

https://t.me/learningnets

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

Glossary

Term	Definition
AAA	authentication, authorization, and accounting. Pronounced "triple a."
ABR	area border router. Router located on the border of one or more OSPF areas that connects those areas to the backbone network. ABRs are considered members of both the OSPF backbone and the attached areas. They therefore maintain routing tables describing both the backbone topology and the topology of the other areas.
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).
AES	Advanced Encryption Standard.
AP	access point. A node on a wireless network that allows other wireless devices to connect to a wired network.
ARP	Address Resolution Protocol. Internet protocol that is used to map an IP address to a MAC address. Defined in RFC 826.
AS	autonomous system. A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided by areas. An autonomous system must be assigned a unique 16-bit number by the IANA.
BGP	Border Gateway Protocol. Interdomain routing protocol that replaces EGP. BGP exchanges reachability information with other BGP systems. It is defined by RFC 1163.
BPDU	bridge protocol data unit. Spanning Tree Protocol hello packet that is sent out at configurable intervals to exchange information among bridges in the network.
CAM	content-addressable memory.
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.
CoA	Change of Authorization.
CoPP	Control Plane Policing.
CoS	class of service. An indication of how an upper-layer protocol requires a lower-layer protocol to treat its messages. In SNA subarea routing, CoS definitions are used by subarea nodes to determine the optimal route to establish a given session. A CoS definition comprises a virtual route number and a transmission priority field. Also called ToS.
CPPr	Control Plane Protection
dACL	downloadable access control list.
DAI	Dynamic ARP Inspection.

https://t.me/learningnets

Term	Definition
DDoS	distributed denial of service
DES	Data Encryption Standard. Standard cryptographic algorithm developed by the U.S. National Bureau of Standards.
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.
DMZ	demilitarized zone.
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.
DTP	Dynamic Trunking Protocol.
EAP	Extensible Authentication Protocol. Framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences.
EAPOL	Extensible Authentication Protocol over LAN
EBGP	Exterior Border Gateway Protocol.
EIGRP	Enhanced Interior Gateway Routing Protocol. Advanced version of IGRP developed by Cisco. Provides superior convergence properties and operating efficiency, and combines the advantages of link-state protocols with those of distance vector protocols.
FIB	forwarding information base
FlexAuth	flexible authentication. A set of features that allows IT administrators to configure the sequence and priority of IEEE 802.1X, MAC authentication bypass (MAB), and switch-based web authentication (local WebAuth).
FPM	Flexible Packet Matching.
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.
GARP	Gratuitous Address Resolution Protocol.
GCM	Galois Counter Mode.
GET	Group Encrypted Transport.
Gigabit Ethernet	Standard for a high-speed Ethernet, approved by the IEEE (Institute of Electrical and Electronics Engineers) 802.3z standards committee in 1996.
GMAC	Galois Message Authentication Code.

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

Term	Definition
GUI	graphical user interface. A user environment that uses pictorial as well as textual representations of the input and the output of applications and the hierarchical or other data structure in which information is stored. Such conventions as buttons, icons, and windows are typical, and many actions are performed using a pointing device (such as a mouse). Microsoft Windows and the Apple Macintosh are prominent examples of platforms using a GUI.
HMAC	Hash-based Message Authentication Code. HMAC is a mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function (for example, MD5 and SHA-1) in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function.
HMAC-MD5	Hashed Message Authentication Code-Message Digest 5 (RFC 2104). A keyed version of MD5 that enables two parties to validate transmitted information using a shared secret.
HRZ	Highly Restricted Zone
HSRP	Hot Standby Router Protocol. Provides high network availability and transparent network topology changes. HSRP creates a hot standby router group with a lead router that services all packets sent to the hot standby address. The lead router is monitored by other routers in the group. If it fails, one of the standby routers inherits both the lead position and the hot standby address.
HTTPS	Hypertext Transfer Protocol Secure
IB	in-band
IBGP	Interior Border Gateway 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.
IDS	intrusion detection system.
IEEE	Institute of Electrical and Electronics Engineers. Professional organization whose activities include the development of communications and network standards. IEEE LAN standards are the predominant LAN standards today.
IGP	interior gateway protocol. Internet protocol used to exchange routing information within an autonomous system. Examples of common Internet IGPs include IGRP, OSPF, and RIP.

https://t.me/learningnets

Term	Definition
IP address	32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address. CIDR provides a new way of representing IP addresses and subnet masks. Also called an Internet address.
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.
IPSG	IP Source Guard
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.
ISE	Cisco Identity Services Engine.
ISP	Internet service provider. Company that provides Internet access to other companies and individuals.
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.

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

Term	Definition
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.
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.
LDP	Label Distribution Protocol. A standard protocol between MPLS-enabled routers to negotiate the labels (addresses) used to forward packets. This protocol is not supported in Cisco IOS Release 12.0. The Cisco proprietary version of this protocol is the Tag Distribution Protocol (TDP).
MAB	MAC authentication bypass.
MAC	Media Access Control. Lower of the two sublayers of the data link layer defined by the IEEE. The MAC sublayer handles access to shared media, such as whether token passing or contention will be used.
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.
MACsec	Media Access Control Security. MACsec encryption provides MAC-layer encryption over wired networks using OOB methods for encryption keying.
man-in-the-middle	Form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association.
MD5	Message Digest 5. A one-way hashing algorithm that produces a 128-bit hash. Both MD5 and Secure Hash Algorithm (SHA) are variations on MD4 and are designed to strengthen the security of the MD4 hashing algorithm. Cisco uses hashes for authentication within the IPsec framework. Also used for message authentication in SNMP v.2. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness.
MDA	Multi-Domain Authentication

https://t.me/learningnets

Term	Definition
MIB	Management Information Base. Database of network management information that is used and maintained by a network management protocol, such as SNMP or CMIP. The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.
MKA	MACsec Key Agreement.
MMP	Mobile Multiplexing Protocol.
MPP	Management Plane Protection.
MQC	modular QoS CLI. Command line structure that allows modular configuration of QoS configuration elements to provide independence between classification and policy.
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.
NDAC	Network Device Admission Control
NetFlow	A feature of some routers that allows them to categorize incoming packets into flows. Because packets in a flow often can be treated in the same way, this classification can be used to bypass some of the work of the router and accelerate its switching operation.
NMS	network management system. System responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer, such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.
NSEL	NetFlow Secure Event Logging
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.
OOB	out-of-band.
OSI	Open Systems Interconnection. International standardization program created by ISO and ITU-T to develop standards for data networking that facilitate multivendor equipment interoperability.
OSI	Open Systems Interconnection. International standardization program created by ISO and ITU-T to develop standards for data networking that facilitate multivendor equipment interoperability.

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

Term	Definition
OSPF	Open Shortest Path First. Link-state, hierarchical IGP routing algorithm proposed as a successor to RIP in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing. OSPF was derived from an early version of the IS-IS protocol.
OTP	one-time password
OZ	Operations Zone
PACL	port access control list.
PAT	port address translation. Translation method that allows the user to conserve addresses in the global address pool by allowing source ports in TCP connections or UDP conversations to be translated. Different local addresses then map to the same global address, with port translation providing the necessary uniqueness. When translation is required, the new port number is picked out of the same range as the original following the convention of Berkeley Standard Distribution (SD).
PAZ	Public Access Zone
PIN	places in the network
PMK	Pairwise Master Key
PVLAN	private VLAN.
PXE	Preboot Execution Environment
PZ	Public Zone
QoS	quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.
RADIUS	Remote Authentication Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.
RBAC	role-based access control. Form of identity-based access control where the system entities that are identified and controlled are functional positions in an organization or process.
REZ	Restricted Extranet Zone
RFC	Request for Comments. Document series that is used as the primary means for communicating information about the Internet. Some RFCs are designated by the IAB as Internet standards. Most RFCs document protocol specifications, such as Telnet and FTP, but some RFCs are humorous or historical. RFCs are available online from numerous sources.
RIB	routing information base
RIP	Routing Information Protocol. A distance-vector routing protocol that uses hop count as a routing metric.
RPF	Reverse Path Forwarding

https://t.me/learningnets

Term	Definition
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.
RZ	Restricted Zone
SA	security association. Instance of security policy and keying material applied to a data flow.
SAP	Session Announcement Protocol.
SAZ	Special Access Zone
SGA	Security Group Access.
SGACL	security group access control list.
SG-FW	Security Group Firewalls
SGT	security group tag.
SGTACL	Security Group Tag/Security Group ACL
SHA-1	Secure Hash Algorithm 1. Algorithm that takes a message of less than 264 bits in length and produces a 160-bit message digest. The large message digest provides security against brute-force collision and inversion attacks. SHA-1 [NIS94c] is a revision to SHA that was published in 1994.
SIEM	Security Information and Event Management.
SMS	short message service
SMTP	Simple Mail Transfer Protocol. Internet protocol providing email services.
SNMP	Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.
SPAN	Switched Port Analyzer. SPAN is a feature that is available on switches based on Cisco IOS and NX-OS Software that allows traffic received on a port or VLAN to be copied to another port for analysis. It is also referred to as "port mirroring."
SSH	Secure Shell Protocol. Protocol that provides a secure remote connection to a router through a TCP application.
SSL	Secure Socket Layer. Encryption technology for the Web used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.
SSO	single sign-on.
STCP	Stream Control Transmission Protocol

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

Term	Definition
STP	Spanning Tree Protocol. Bridge protocol that uses the spanning-tree algorithm, enabling a learning bridge to dynamically work around loops in a network topology by creating a spanning tree. Bridges exchange BPDU messages with other bridges to detect loops, and then remove the loops by shutting down selected bridge interfaces. Refers to both the IEEE 802.1 Spanning Tree Protocol standard and the earlier Digital Equipment Corporation Spanning Tree Protocol upon which it is based. The IEEE version supports bridge domains and allows the bridge to construct a loop-free topology across an extended LAN. The IEEE version generally is preferred over the Digital version.
SUS	Software Update Services
SYN	synchronization.
TACACS+	Terminal Access Controller Access Control System Plus. Proprietary Cisco enhancement to TACACS. Provides additional support for authentication, authorization, and accounting.
TCP	Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.
Telnet	Standard terminal emulation protocol in the TCP/IP protocol stack. Telnet is used for remote terminal connection, enabling users to log into remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC 854.
TLS	Transport Layer Security. A future IETF protocol to replace SSL.
TOC	Threat Operation Center
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.
uRPF	Unicast Reverse Path Forwarding.
VLAN	virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.
VoIP	Voice over IP. The capability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. In VoIP, the DSP segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323.

https://t.me/learningnets

Term	Definition
VPN	virtual private network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses tunneling to encrypt all information at the IP level.
VRF	A VPN routing/forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.
VTP	VLAN Trunking Protocol.
VTY	virtual terminal line
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.
WebAuth	web authentication.
ZIP	Zone Information Protocol. AppleTalk session layer protocol that maps network numbers to zone names. ZIP is used by NBP to determine which networks contain nodes that belong to a zone.
3DES	Triple Data Encryption Standard.

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