CISCO

CCNA Security
Portable Command Guide

All the CCNA Security 640-554 commands
in one compact, portable resource

ciscopress.com

Bob Vachon

CCNA Security
Portable Command Guide

Bob Vachon

Cisco Press

800 East 96th Street
Indianapolis, IN 46240 USA

CCNA Security
Portable Command Guide

Bob Vachon

Warning and Disclaimer

This book is designed to provide information about the CCNA Security (640-554 IINS) exam and the commands needed at this level of network administration. Every effort has been made to make this book as complete and as accurate as possible, fitness is implied.

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

Trademark Acknowledgments

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

Feedback Information

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

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

Corporate and Government Sales

Cisco Press offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales.

For more information please contact: U.S. Corporate and Government Sales

1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the U.S. please contact: International Sales international@pearsoned.com

Contents at a Glance

Contents

CHAPTER 7   Securing Management Access with AAA   77

About the Author

Bob Vachon is a professor in the Computer Systems Technology program at Cambrian College in Sudbury, Ontario, Canada, where he teaches networking infrastructure courses. He has worked and taught in the computer networking and information technology field since 1984. He has collaborated on various CCNA, CCNA Security, and CCNP projects for the Cisco Networking Academy as team lead, lead author, and subject matter expert. He enjoys playing the guitar and being outdoors, either working in his gardens or white-water canoe tripping.

About the Technical Reviewer

Jim Lorenz is an instructor and a senior training developer for the Cisco Networking Academy Program. He holds a bachelor's degree in computer information systems and has over 20 years of experience in networking and IT. Jim has developed course materials, including content, labs, and textbooks for the CCNA and CCNP curricula. Most recently he coordinated lab development for the CCNA Security course.

Dedications

This book is dedicated to my students. Thanks for reminding me why I do this stuff. I also dedicate this book to my beautiful wife Judy and daughters Lee-Anne, Joëlle, and Brigitte who, without their support and encouragement, I would not have been involved in this project.

Acknowledgments

I would like to start off with a big thanks to my friend Scott Empson for involving me with this project. Your *Portable Command Guide* series was a great idea and kudos to you for making it happen.

Thanks to the team at Cisco Press. Thank you Mary Beth for believing in me and to Drew and Mandie for making sure I got things done right and on time. Also thanks to my friend Jim for keeping me in check.

Special thanks to my Cisco Networking Academy family. A big thanks to Jeremy and Rob for involving me in these very cool projects. You guys keep me young.

Finally, a great big thanks to the folks at Cambrian College for letting me have fun and do what I love to do...teach!

Command Syntax Conventions

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

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).

- *Italics* indicate arguments for which you supply actual values.

- Vertical bars (|) separate alternative, mutually exclusive elements.

- Square brackets [ ] indicate optional elements.

- Braces { } indicate a required choice.

- Braces within brackets [{ }] indicate a required choice within an optional element.

Introduction

Welcome to CCNA Security! Scott Empson had an idea to provide a summary of his engineering journal in a portable quick reference guide. The result is the *Portable Command Guide* series. These small books have proven to be very valuable for anyone studying for Cisco certifications or as a handy quick reference resource for anyone tasked with managing Cisco infrastructure devices.

The *CCNA Security Portable Command Guide* covers the security commands and GUI steps needed to pass the 640-554 IINS (Implementing Cisco IOS Network Security) certification exam. The guide begins by summarizing the required fundamental security concepts. It then provides the CLI commands and the Cisco Configuration Professional GUI screenshots required to secure an ISR. Examples are included to help demonstrate the security-related configuration.

The last section of the book focuses on securing a network using an Adaptive Security Appliance (ASA). It provides the CLI commands and the ASA Security Device Manager (ASDM) GUI screenshots required to secure an ASA 5505. Again, examples are included to help demonstrate the security-related configuration.

I hope that you learn as much from reading this guide as I did when I wrote it.

Networking Devices Used in the Preparation of This Book

To verify the commands in this book, I had to try them out on a few different devices. The following is a list of the equipment I used in the writing of this book:

- Cisco 1841 ISR running Cisco IOS advanced IP services software release 12.4(20)T1 and the Cisco Configuration Professional GUI version 2.6

- Cisco ASA 5505 running Cisco Adaptive Security Appliance software version 8.4(2) with a Base License and the ASA Security Device Manager (ASDM) GUI version 6.4(5)

Who Should Read This Book

This book is for those people preparing for the CCNA Security (640-554 IINS) exam, whether through self-study, on-the-job training and practice, study within the Cisco Academy Program, or study through the use of a Cisco Training Partner. There are also some handy hints and tips along the way to make life a bit easier for you in this endeavor. It is small enough that you will find it easy to carry around with you. Big, heavy textbooks might look impressive on your bookshelf in your office, but can you really carry them all around with you when you are working in some server room or equipment closet somewhere?

Organization of This Book

The parts of this book cover the following topics:

- **Part I, "Network Security Fundamentals"**—Introduces network security-related concepts and summarizes how security policies are implemented using a lifecycle approach. It also summarizes how to build a security strategy for borderless networks.

- **Part II, "Protecting the Network Infrastructure"**—Describes how to secure the management and data planes using the IOS CLI configuration commands and CCP.

- **Part III, "Threat Control and Containment"**—Describes how to secure an ISR against network threats using the IOS CLI configuration commands and CCP to configure ACLs, zoned-based firewall, and IOS IPS.

- **Part IV, "Secure Connectivity"**—Describes how to secure data as it traverses insecure networks using cryptology and virtual private networks (VPNs). Specifically, site-to-site IPsec VPNs are enabled using the IOS CLI configuration commands and CCP.

- **Part V, "Securing the Network Using the ASA"**—Describes how to secure a network using an ASA data as it traverses insecure networks using cryptology and virtual private networks (VPNs). Specifically, remote access SSL VPNs are enabled using the IOS CLI configuration commands and CCP.

Networking Security Concepts

The chapter covers the following topics:

Basic Security Concepts

- Assets, Vulnerabilities, Threats, and Countermeasures
- Confidentiality, Integrity, and Availability
- Data Classification Criteria
- Data Classification Levels
- Classification Roles

Threat Classification

- Preventive, Detective, and Corrective Controls
- Risk Avoidance, Transfer, and Retention

Drivers for Network Security

- Evolution of Threats
- Tracking Threats

Malicious Code: Viruses, Worms, and Trojan Horses

- Anatomy of a Worm
- Mitigating Malware and Worms

Threats in Borderless Networks

- Hacker Titles
- Thinking Like a Hacker
- Reconnaissance Attacks
- Access Attacks
- Password Cracking
- Denial-of-Service Attacks

Principles of Secure Network Design

- Defense in Depth

Basic Security Concepts

Assets, Vulnerabilities, Threats, and Countermeasures

Four terms are associated with security management:

Asset	Anything of value to an organization that must be protected
Vulnerability	A weakness in a system or its design that could be exploited by a threat
Threat	A potential danger to information or network functionality
Countermeasure	A protection that mitigates a potential threat or risk

Confidentiality, Integrity, and Availability

To provide adequate protection of network assets, three things must be guaranteed:

Confidentiality	Only authorized users can view sensitive information.
Integrity	Only authorized users can change sensitive information. It can also guarantee the authenticity of data.
Availability (system and data)	Authorized users must have uninterrupted access to important resources and data.

Data Classification Criteria

Factors when classifying data include the following:

Value	The number one criteria and is based on the cost to acquire, develop, and replace.
Age	The importance of data usually decreases with time.
Useful life	The amount of time in which data is considered valuable and must be kept classified.
Personal association	Data that involves personal information of users and employees.

Data Classification Levels

Data classification terms commonly used by government and military include the following:

Unclassified	Data that has little or no confidentiality, integrity, or availability requirements, and therefore little effort is made to secure it.
Sensitive but unclassified (SBU)	Data that could prove embarrassing if it is revealed, but no great security breach would occur.
Confidential	Data must be kept secure.

Secret	Data for which significant effort is made to keep it secure. Few individuals have access to this data.
Top secret	Data for which great effort and sometimes considerable cost is made to guarantee its secrecy. Few individuals on a need-to-know condition have access to top-secret data.

Data classification terms commonly used by the public sector include the following:

Public	Data that is available publicly, such as on websites, publications, and brochures
Sensitive	Data that is similar to SBU data and that might cause some embarrassment if revealed
Private	Data that is important to an organization and an effort is made to maintain the secrecy and accuracy of this data
Confidential	Data that companies make the greatest effort to keep secure, such as trade secrets, employee data, and customer information

Classification Roles

Roles related to data include the following:

Owner	Person responsible for the information
Custodian	Person in charge of performing day-to-day data maintenance, including securing and backing up the data
User	Person using the data in accordance to established procedures

Threat Classification

Three categories of threat classification exist:

Administrative	Policy and procedure based, including change/configuration control, security training, audits, and tests
Technical	Controls that involve hardware and software
Physical	Controls for protecting the physical infrastructure

Preventive, Detective, and Corrective Controls

Incident and exposure management entails the following five categories:

Preventive	Preventing the threat from coming in contact with a vulnerability, such as using a firewall, physical locks, and a security policy
Detective	Identifying that the threat has entered the network or system using system logs, intrusion prevention systems (IPSs), and surveillance cameras

Corrective	Determining the underlying cause of a security breach and then mitigating the effects of the threat being manifested, such as updating virus or IPS signatures
Recovery	Putting a system back into production after an incident
Deterrent	Discouraging security violations

Risk Avoidance, Transfer, and Retention

Countermeasures to managing risk can be categorized as follows:

Risk avoidance	Avoid activity that could carry risk.
Risk reduction	Involves reducing the severity of the loss or the likelihood of the loss from occurring.
Risk sharing or transfer	Involves sharing the burden of loss or the benefit of gain with another party.
Risk retention or acceptance	Involves accepting the loss, or benefit of gain, from a risk when it occurs.

Drivers for Network Security

Key factors to consider when designing a secure network include the following:

- Business needs
- Risk analysis
- Security policy
- Industry best practices
- Security operations

Evolution of Threats

Threats have evolved in the following manner over the years:

First generation (early 1990s)	Threats took days to propagate and targeted individual computers and networks using macro viruses, email viruses, spam, denial-of-service (DoS) attacks, and limited hacking.
Second generation (early 2000s)	Threats were propagated in hours and targeted multiple networks using network DoS, blended threats (worm + virus + Trojan horses), turbo worms, and widespread hacking.
Third generation (late 2000s)	Threats took minutes to propagate and targeted regional networks using infrastructure hacking, Adobe Flash compromises, distributed DoS (DDoS), and worms and viruses with damaging payloads.

Next generation (Early 2010s)	Threats now propagate in seconds and target global networks, websites, critical infrastructure services, and consumer electronics and include virtualization exploits, memory scraping, hardware hacking, and IPv6-based attacks.

Tracking Threats

Various organizations classify and keep track of threats, including the following:

- **CAPEC (Common Attack Pattern Enumeration and Classification):** http://capec.mitre.org
- **MAEC (Malware Attribute Enumeration and Characterization):** http://maec.mitre.org/
- **OWASP (Open Web Application Security Project):** https://www.owasp.org
- **WASC TC (Web Application Security Consortium Threat Classification):** http://www.webappsec.org/
- **ISC (Internet Storm Center):** http://isc.sans.org/

Malicious Code: Viruses, Worms, and Trojan Horses

The following highlights common types of malicious code (malware) that can be used by hackers:

Viruses	Infectious malicious software that attaches to another program to execute a specific unwanted function on a computer. Most viruses require end-user activation and can lay dormant for an extended period and then activate at a specific time or date. Viruses can also be programmed to mutate to avoid detection.
Worms	Infectious malware, worms are self-contained programs that exploit known vulnerabilities with the goal of slowing a network. Worms do not require end-user activation. An infected host replicates the worm and automatically attempts to infect other hosts by independently exploiting vulnerabilities in networks.
Spyware	Spyware is typically used for financial gain and collects personal user information, monitoring web-browsing activity for marketing purposes, and routing of HTTP requests to advertising sites. Spyware does not usually self-replicate but can be unknowingly installed on computers.
Adware	Refers to any software that displays advertisements, whether or not the user has consented sometimes in the form of pop-up advertisements.
Scareware	Refers to a class of software used for scamming unsuspecting users. They can contain malicious payloads or be of little or no benefit. A common tactic involves convincing users that their systems are infected by viruses and then providing a link to purchase fake antivirus software.

Trojan horses	These are applications written to look like something else such as a free screensaver, free virus checker, and so on. When a Trojan horse is downloaded and opened, it attacks the end-user computer from within. Trojan horses may be created to initiate specific types of attacks, including the following: ■ Remote access ■ Data sending (key logging) ■ Destructive ■ Security software disabler ■ Denial of service

Anatomy of a Worm

Upon successful exploitation, the worm copies itself from the attacking host to the newly exploited system and the cycle begins again.

Most worms have the following three components:

Enabling vulnerability	A worm installs itself using an exploit mechanism (email attachment, executable file, Trojan horse) on a vulnerable system.
Propagation mechanism	After gaining access to a device, the worm replicates itself and locates new targets. It spreads without human intervention and scans for other hosts to infect.
Payload	Any malicious code that results in some action. Most often, this is used to create a back door to the infected host.

Mitigating Malware and Worms

The primary means of mitigating malware is antivirus software. Antivirus software helps prevent hosts from getting infected and spreading malicious code. It requires much more time (and money) to clean up infected computers than it does to purchase antivirus software and maintain antivirus definition updates.

Worms are more network based than viruses and are more likely to have infected several systems within an organization. The security staff response to a worm infection usually involves the following four phases:

Containment	The goal is to limit the spread of infection and requires segmentation of the infected devices to prevent infected hosts from targeting other uninfected systems. Containment requires using incoming and outgoing access control lists (ACLs) on routers and firewalls at control points within the network.
Inoculation	The goal is to deprive the worm of any available targets. Therefore, all uninfected systems are patched with the appropriate vendor patch. The inoculation phase often runs parallel to or subsequent to the containment phase.

Quarantine	The goal is to track down and identify the infected machines. Once identified, they are disconnected, blocked, or removed from the network and isolated for the treatment phase.
Treatment	Infected systems are disinfected of the worm. This can involve terminating the worm process, removing modified files or system settings that the worm introduced, and patching the vulnerability the worm used to exploit the system. In severe cases, the system may need to be re-imaged.

Threats in Borderless Networks

Possible adversaries to defend against attacks include the following:

- Nations or states
- Terrorists
- Criminals
- Government agencies
- Corporate competitors
- Disgruntled employees
- Hackers

Hacker Titles

Various hacker titles include the following:

Hackers	Individuals who break into computer networks to learn more about them. Most mean no harm and do not expect financial gain.
White hat and blue hat	Names given to identify types of good hackers. White hats are ethical hackers such as individuals performing security audits for organizations. Blue hats are bug testers to ensure secure applications.
Crackers	Hackers with a criminal intent to harm information systems or for financial gain. They are sometimes called "black hat hackers."
Black hat and gray hat	Names given to identify types of crackers. Black hat is synonymous with crackers, and gray hats are ethically questionable crackers.
Phreakers	Hackers of telecommunication systems. They compromise telephone systems to reroute and disconnect telephone lines, sell wiretaps, and steal long-distance services.
Script kiddies	Hackers with very little skill. They do not write their own code but instead run scripts that are written by more skilled attackers.
Hacktivists	Individuals with political agendas who attack government sites.

Thinking Like a Hacker

The following seven steps may be taken to compromise targets and applications:

Step 1	Perform footprint analysis	Hackers generally try to build a complete profile of a target company's security posture using a broad range of easily available tools and techniques. They can discover organizational domain names, network blocks, IP addresses of systems, ports, services that are used, and more.
Step 2	Enumerate applications and operating systems	Special readily available tools are used to discover additional target information. Ping sweeps use Internet Control Message Protocol (ICMP) to discover devices on a network. Port scans discover TCP/UDP port status. Other tools include Netcat, Microsoft EPDump and Remote Procedure Call (RPC) Dump, GetMAC, and software development kits (SDKs).
Step 3	Manipulate users to gain access	Social engineering techniques may be used to manipulate target employees to acquire passwords. They may call or email them and try to convince them to reveal passwords without raising any concern or suspicion.
Step 4	Escalate privileges	To escalate their privileges, a hacker may attempt to use Trojan horse programs and get target users to unknowingly copy malicious code to their corporate system.
Step 5	Gather additional passwords and secrets	With escalated privileges, hackers may use tools such as the pwdump and LSADump applications to gather passwords from machines running Windows.
Step 6	Install back doors	Hacker may attempt to enter through the "front door," or they may use "back doors" into the system. The backdoor method means bypassing normal authentication while attempting to remain undetected. A common backdoor point is a listening port that provides remote access to the system.
Step 7	Leverage the compromised system	After hackers gain administrative access, they attempt to hack other systems.

Reconnaissance Attacks

This is where the initial footprint analysis and discovery of applications and operating systems are done. Reconnaissance is analogous to a thief surveying a neighborhood for vulnerable homes to break into.

Reconnaissance attacks typically involve the unauthorized discovery and mapping of systems, services, or vulnerabilities using the following:

Internet information queries	Uses readily available Internet tools such as WHOIS, which is widely used for querying databases that store the registered users or assignees of an Internet resource.
Ping sweeps	Method is used to discover a range of live IP addresses.
Port scanners	An application program designed to probe a target host for open ports and identify vulnerable services to exploit.
Packet sniffers	An application program that can intercept, log, and analyze traffic flowing over a network (also referred to as a packet analyzer, network analyzer, or protocol analyzer).

Access Attacks

The goal of access attacks is to discover usernames and passwords to access various resources. The following are common methods to conduct an access attack:

Blended threats	Blended threats are attack mechanisms that combine the characteristics of viruses, worms, Trojan horses, spyware, and others. If the threat is succssfully initiated, the access attack attempts to gather user information.
Phishing	Phishing attacks masquerade as a trustworthy entity to get unsuspecting users to provide sensitive information (and are usually used for identity theft). The attacks are usually carried out using email, instant messaging, or phone contact. The message usually directs users to enter details at the hacker's website. *Spear phishing* is when a phishing attack is directed at a specific user.
Pharming	Pharming is an attack aimed at redirecting the traffic of a website to another website. Such attacks are usually conducted by exploiting a vulnerable Domain Name System (DNS) server.
Man-in-the-middle attacks	In a man-in-the-middle attack, a hacker positions himself between a user and the destination. The actual implementation can be carried out in a variety of ways, including using network packet sniffers or altering routing and transport protocols. This type of attack is used for session hijacking, theft of information, sniffing and analyzing network traffic, corrupting data flows, propagating bogus network information, and for DoS attacks.
IP and MAC address spoofing	In IP address spoofing attacks, a hacker forges IP packets with trusted IP source addresses. MAC address spoofing similarly forges trusted host MAC addresses on a LAN. The attacks are commonly used to create a man-in-the-middle situation.
Trust exploitation	Trust exploitation refers to when a hacker has compromised a target and that host is trusted by another host (new target).

Password Cracking

Hackers can capture passwords using Trojan horse programs, key loggers, or packet sniffers. In addition, they can attempt to crack passwords using the following methods:

Word lists	Programs use word lists; phrases; or other combinations of letters, numbers, and symbols that are often used as passwords. Programs enter word after word at high speed until they find a match.
Brute force	This approach relies on power and repetition, comparing every possible combination and permutation of characters until it finds a match. It eventually cracks any password, but it may be very time-consuming.
Hybrid cracking	Some password crackers mix a combination of techniques and are highly effective against poorly constructed passwords.

Denial-of-Service Attacks

DoS attacks send extremely large numbers of requests over a network or the Internet. These excessive requests cause the target device to run suboptimally. Consequently, the attacked device becomes unavailable for legitimate access and use. By executing exploits or combinations of exploits, DoS attacks slow or crash applications and processes.

Types of attacks to compromise availability include the following:

Botnets	Describes a collection of compromised systems running worms, Trojan horses, or backdoors under a common command and control infrastructure. The originator of a botnet controls the group of computers remotely.
Denial of service (DoS)	A DoS attack sends an extremely large number of requests over a network or the Internet to a server or edge device with the intent to overwhelm the target, making it unavailable for legitimate access and use. This is the most publicized form of attack and among the most difficult to eliminate.
Distributed DoS (DDoS)	A DDoS attack enlists a network of botnets that contains a remotely controlled agent, or zombie, attack program. A master control mechanism provides direction and control. When the zombies receive instructions from the master agent, they each begin generating malicious traffic that is aimed at the victim.
Other attacks	Other attacks to compromise availability include TCP synchronization (SYN) floods, ICMP floods, cutting electrical power, or sabotaging the computer environment.

Principles of Secure Network Design

Guidelines to secure a network infrastructure include the following:

Defense in depth	Architecture uses a layered approach to create security domains and separate them by different types of security controls.
Compartmentalization	Architecture segments the network where different assets with different values are in different security domains, be it physical or logical. Granular trust relationships between compartments would mitigate attacks that try to gain a foothold in lower-security domains to exploit high-value assets in higher-security domains.
Least privilege	Principle applies a need-to-know approach to trust relationships between security domains. This results in restrictive policies, where access to and from a security domain is allowed only for the required users, applications, or network traffic. Everything else is denied by default.
Weakest link	Architecture uses a layered approach to security, with weaker or less-protected assets residing in separated security domains. Humans are often considered to be the weakest link in information security architectures.
Separation and rotation of duties	Concept of developing systems where more than one individual is required to complete a certain task to mitigate fraud and error. This applies to information security controls, and it applies to both technical controls and human procedures to manage those controls.
Mediated access	Principle is based on centralizing security controls to protect groups of assets or security domains such as using firewalls, proxies, and other security controls to act on behalf of the assets they are designed to protect, and mediate the trust relationships between security domains.
Accountability and traceability	Architecture should provide mechanisms to track the activity of users, attackers, and even security administrators. It should include provisions for accountability and non-repudiation. This principle translates into specific functions, such as security audits, event management and monitoring, forensics, and others.

Defense in Depth

Defense in depth provides a layered security approach by using multiple security mechanisms. The security mechanisms should complement each other but not depend on each other. The use of this approach can eliminate single points of failure and augment weak links in the system to provide stronger protection with multiple layers.

Recommendations for a defense-in-depth strategy include the following:

Defend in multiple places	Threat vectors can occur from various locations. Therefore, an organization must deploy protection mechanisms at multiple locations to resist all classes of attacks. Includes defending the networks and infrastructure, enclave boundaries, and the computing environment.
Build layered defenses	All products have inherent weaknesses. Therefore, an effective countermeasure is to deploy multiple defense mechanisms between the adversary and the target.
Use robust components	Specify the security robustness based on the value of the asset to be protected. For instance, deploy stronger mechanisms at the network boundaries than at the user desktop.
Employ robust key management	Deploy robust encryption key management and public key infrastructures that are highly resistant to attack.
Deploy intrusion detection/ prevention systems (IDSs/ IPSs)	Deploy infrastructures to detect and prevent intrusions and to analyze and correlate the results and react accordingly.

Implementing Security Policies Using a Lifecycle Approach

The chapter covers the following topics:

Risk Analysis

- Quantitative Risk Analysis Formula
- Quantitative Risk Analysis Example
- Regulatory Compliance

Security Policy

- Standards, Guidelines, and Procedures
- Security Policy Audience Responsibilities
- Security Awareness

Secure Network Lifecycle Management

- Models and Frameworks
- Assessing and Monitoring the Network Security Posture
- Testing the Security Architecture

Incident Response

- Incident Response Phases
- Computer Crime Investigation
- Collection of Evidence and Forensics
- Law Enforcement and Liability
- Ethics

Disaster-Recovery and Business-Continuity Planning

Risk Analysis

Risk needs to be framed, assessed, monitored, and responded to. Risk, compliance, and security policies are major components of security architectures. The primary purpose of risk analysis is to quantify the impact of an individual potential threat.

There are two types of risk analysis:

Quantitative risk analysis	Uses a mathematical model using an estimated value for an asset multiplied by the likelihood of a threat being realized. Quantitative risk analysis provides an actual monetary figure of expected losses, which is then used to estimate an annual cost. The resulting numbers can also be used to justify proposed countermeasures.
Qualitative risk analysis	Uses a scenario model. Can be performed in a shorter period of time and with less data. Qualitative risk assessments are descriptive versus measurable. Qualitative risk assessments may precede a quantitative analysis.

Quantitative Risk Analysis Formula

Risk management is based on its building blocks of assets and vulnerabilities, threats, and countermeasures. Quantitative analysis relies on specific formulas to determine the value of the risk decision variables. Figure 2-1 displays the quantitative risk analysis formula.
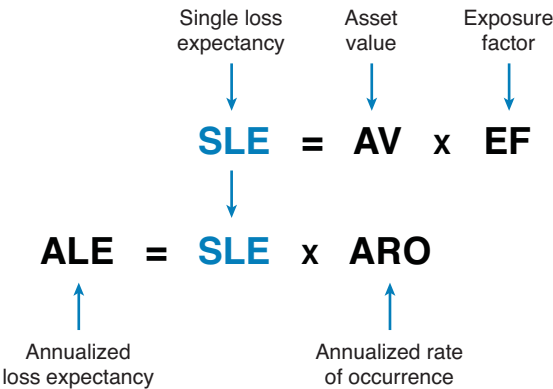
Figure 2-1 Quantitative Risk Analysis Formula

Quantitative risk analysis terms include the following:

Asset value (AV)	This estimated value includes the purchase price, the cost of deployment, and the cost of maintenance.
Exposure factor (EF)	This estimates the degree of destruction that may occur. It is represented as a percentage that a realized threat could have on an asset.
Single loss expectancy (SLE)	This calculation represents the expected loss from a single occurrence of the threat. The SLE is defined as the AV x EF.

Annualized rate of occurrence (ARO)	This is the estimated frequency that a threat is expected to occur. It is the number of times that one may reasonably expect the risk to occur during one year. This estimate is very difficult and is usually based on past experience.
Annualized loss expectancy (ALE)	This is the expected financial loss that an individual threat may cause. The ALE is a monetary value derived from the formula SLE x ARO. This number is used to justify the least-cost security measures.

Quantitative Risk Analysis Example

An administrator of a data center must provide a projection for a flood disaster. Assume that the overall value of a data center is $10,000,000 (AV). It is estimated that 60% (EF) of the data center would be destroyed in the event of a flood (risk):

- SLE = AV x EF
- SLE = $10,000,000 x 60% = $6,000,000

The SLE assigns a monetary value for a single occurrence. It represents the organization's potential loss amount if a specific threat exploits a vulnerability.

The ALE is the total amount of money that the organization will lose in 1 year if nothing is done to mitigate the risk. It is often used to justify the lowest-cost security measure. If the likelihood of a flood occurring is estimated at once in 100 years (1/100), the ARO equals 1%:

- ALE = SLE x ARO
- ALE = $6,000,000 x 1% = $60,000

The ALE provides a value that the organization can work with to budget the cost to establish controls or safeguards to prevent this type of damage.

Regulatory Compliance

The current regulatory landscape is broader and more international. Compliance regulations define not only the scope and parameters for the risk and security architectures of an organization, but also the liability for those who do not comply.

The following are compliance regulations, their geographic scope, and which organizations a regulation applies to:

Regulation	Geographic Boundary	Description
DMCA	U.S.	The Digital Millennium Copyright Act (DMCA) protects against copyright infringement. It heightens the penalties for copyright infringement on the Internet.

Regulation	Geographic Boundary	Description
FISMA	U.S.	The Federal Information Security Management Act (FISMA) of 2002 requires that the U.S. government federal agencies, service organizations, and affiliated parties be subject to yearly cyber security audits.
GLB	U.S.	The Gramm-Leach-Bliley (GLB) Act (also known as the Financial Services Modernization Act of 1999) applies mostly to banks, investment companies, and insurance agencies and governs the collection, disclosure, and protection of consumer information.
HIPAA	U.S.	The Health Insurance Portability and Accountability Act (HIPAA) of 2000 includes a set of national standards for healthcare transactions that provide assurances that the electronic transfer of confidential patient information will be as safe as, or safer than, paper-based patient records.
SOX	U.S.	The Sarbanes-Oxley (SOX) Act of 2002 governs the accounting and reporting practices of publicly traded companies in the United States. It was created in response to accounting scandals, including those affecting Enron, Tyco International, Peregrine Systems, and WorldCom.
PIPEDA	Canada	The Personal Information Protection and Electronic Documents Act governs how private-sector organizations collect, use, and disclose personal information in the course of commercial business.
NERC	North America	The North American Electric Reliability Corporation (NERC), a nonprofit corporation that seeks to ensure the reliability of the North American bulk electric power system, applies to users, owners, and operators in that system.
EU Data Protection Directive	European Union	This act contains eight "data protection principles" that specify how personal data is securely collected, maintained, and disposed of. It applies to all organizations operating in the 27 member countries.
Safe Harbour Act	European Union	It prohibits European firms from transferring personal data to overseas jurisdictions with weaker privacy laws.
Basel II	Global	An international standard with which banking regulators must comply. It requires them to put aside enough capital to guard against risk. It applies to all internationally active banks with assets of more than $250 billion.

Security Policy

A security policy is a set of objectives for the company, rules of behavior for users and administrators, and requirements for system and management that collectively ensure the security of network and computer systems in an organization.

It is a "living document," meaning that the document is never finished and is continuously updated as technology and employee requirements change. One document will not likely meet the needs of the entire audience of a large organization.

The audience of the security policy should be employees, contractors, suppliers, or customers who have access to your network.
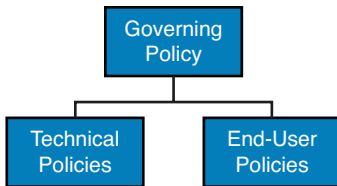
Figure 2-2   Comprehensive Security Policy Components

Figure 2-2 displays a common corporate policy structure for most organizations:

Governing policy	It details the company's overall security policy philosophy. It defines information security concepts at a high level, describes why they are important, and details the organization's stand. It supports the technical and end-user policies.
Technical policies	Security staff creates technical policies to implement the security requirements outlined in the governing policy. These policies describe what the security staff does but do not dictate how the security staff performs its functions.
End-user policies	Documents contain security policies important to end users.

Technical policies can be categorized as follows:

General policies	Define the use of equipment, computing services, and security guidelines. May include an acceptable use policy (AUP), account access policy, password policy, acquisition policy, audit policy, and information sensitivity policy.
Remote-access policies	Defines the standards for connecting to the organization network from an external host or network. Typically include a virtual private network (VPN) security policy.
Network policies	Define standards to secure all wired and wireless networks data ports. May also include general network access polices and policies to access routers, switches, servers, and extranets.

| Email policies | Define standards to protect the email infrastructure of the organization. May also include an automatic forwarding of email policy and spam policy. |
| Other policies | Other categories may include telephony policies, application use policies, and wireless policies. |

Standards, Guidelines, and Procedures

Security policies establish a framework within which to work, but they are usually too general to be of much use to individuals responsible for implementing these policies.

Therefore, more detailed documents exist, including the following:

Standards	Allow IT staff to be consistent by specifying the use of technologies. They are usually mandatory and help provide consistency, uniformity, and efficiency.
Guidelines	These are best practices that provide a list of suggestions on how things can be done better. They are similar to standards, but are more flexible and are not usually mandatory.
Procedures	Documents include the details of implementation, usually with step-by-step instructions and graphics.

Figure 2-3 provides a hierarchical view of the information security policy framework.
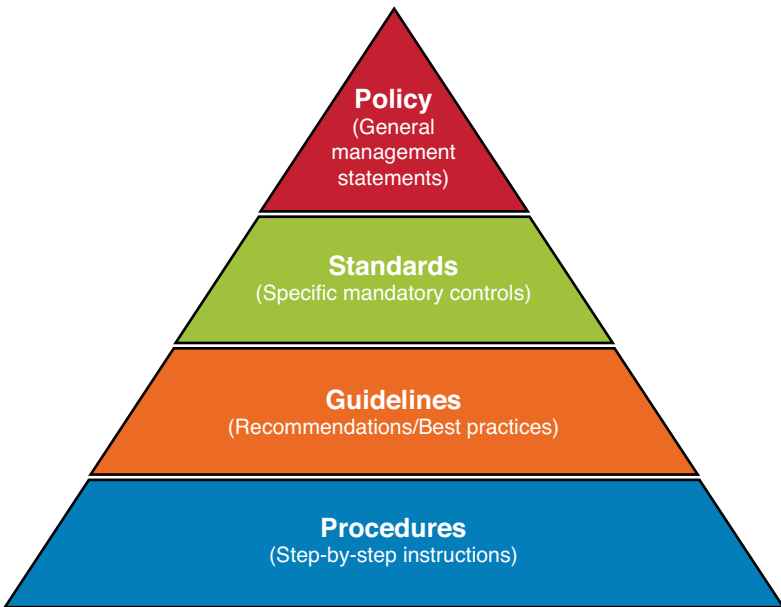
Figure 2-3 Information Security Policy Framework

Security Policy Audience Responsibilities

Key individuals in an organization responsible for the security policy are as follows:

Senior management (CEO)	Is ultimately responsible
Senior security IT management (CSO, CIO, CISO)	Are responsible for the security policy
Senior security IT staff	Have input on the security policy and possibly draft sections of the security policy.
Security IT staff	Are responsible for implementing the security policy
End-users	Are responsible for complying with the security policy

Security Awareness

An effective computer security awareness and training program requires proper planning, implementation, maintenance, and periodic evaluation. In general, a computer security awareness and training program should encompass the following seven steps:

1. Identify program scope, goals, and objectives.
2. Identify training staff.
3. Identify target audiences.
4. Motivate management and employees.
5. Administer the program.
6. Maintain the program.
7. Evaluate the program.

Secure Network Lifecycle Management

The lifecycle approach may also help you understand the framing of information security.
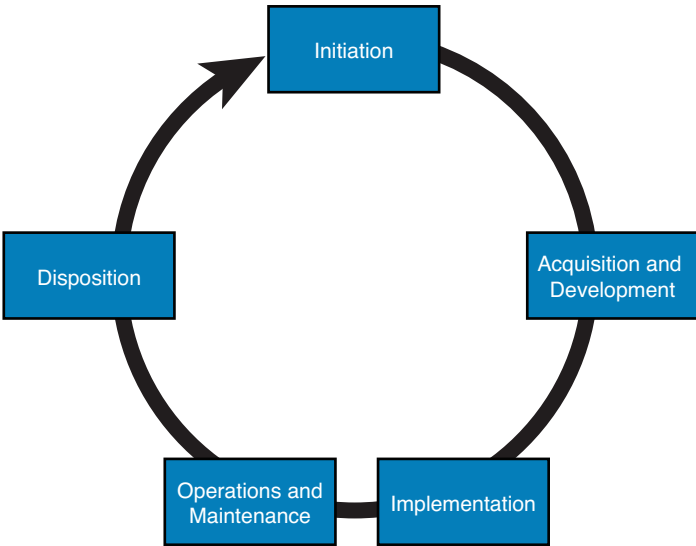
Figure 2-4   Secure Network Lifecycle

Figure 2-4 illustrates the five phases of the lifecycle approach. The five-phase approach gives context to the process of designing, creating, and maintaining security architectures. It is based on Publication 800-64 revision 2 of the NIST.

When applied to information security, these phases are used as follows:

Initiation	Includes security categorization and a preliminary risk assessment steps.
Acquisition and development	Includes steps such as risk assessment, security functional requirements analysis, security assurance requirements analysis, cost considerations and reporting, security planning, security control development, developmental security test and evaluation, and other planning components.
Implementation	These security tasks include inspection and acceptance, system integration, security certification, and security accreditation steps.
Operations and maintenance	Includes configuration management and control and continuous monitoring steps.
Disposition	Includes information preservation, media sanitization, and hardware- and software-disposal steps.

Models and Frameworks

The following frameworks and models are alternatives to the lifecycle approach and provide similar security architecture guidance:

Control Objectives for Information and Related Technology (COBIT)	Includes best practices from a consensus of experts that focus on IT controls and IT metrics, which is useful for IT governance and audits. These good practices help optimize IT-enabled investments, ensure service delivery, and provide a measure against which to judge when things do go wrong.
ISO 27000 Standards	Includes a comprehensive set of controls comprising best practices in information security. It is also a certified and globally recognized information security standard that focuses on risk identification, assessment, and management.
Information Technology Infrastructure Library (ITIL)	Includes a set of eight practice guidebooks covering most aspects of IT service management.
National Institute of Standards and Technology (NIST)	The NIST 800 series provides detailed documents on how to secure a networked infrastructure. It is also available for free and is used for FISMA.

Assessing and Monitoring the Network Security Posture

The security posture should be assessed at multiple points of the lifecycle. By assessing all aspects of the networked business environment, it is possible to determine the ability of the organization to detect, defend against, and respond to network attacks.

Key assessment activities include the following:

Security posture assessment	Consists of a thorough assessment of the network devices, servers, desktops, and databases. Analyzes the effectiveness of the network security against recognized industry best practices to identify the relative strengths and weaknesses of the environment and document specific vulnerabilities that could threaten the business.
Internal assessment	Consists of a controlled network attack on internal systems, applications, and network devices and is used to identify steps that are needed to prevent intentional attacks or unintentional mistakes from trusted insiders to effectively secure valuable information assets.
External assessment	The goal is to quantify the security risk that is associated with Internet-connected systems.
Wireless assessment	Tests the wireless network within the organization and identifies risks and exposures that are associated with a wireless deployment.

Security posture assessment analysis and documentation	Quantifies the security posture of the organization network by using metrics and graphs. The report should explain methods that would likely be used to compromise network devices and systems. It should also prioritize the vulnerabilities and recommend actions to correct the security risks and detail remediation steps to prevent future exploitation.

Testing the Security Architecture

The security infrastructure should be tested within the context of risk management. Some testing techniques are predominantly manual, and other tests are highly automated. Staff that conducts the security testing should have significant security and networking knowledge.

Many types of testing techniques are available, including the following:

- Network and vulnerability scanning
- Password cracking
- Log review
- Integrity checkers, virus checking
- War dialing and war driving
- Penetration testing

Incident Response

Risk cannot be completely eliminated, which makes incident response critical.

Incident Response Phases

The incident response process has several phases:

Preparation	Involves getting ready before an incident happens. Prepare the facilities and team contact information. Define the tools required and know how to use them. Define prevention procedures.
Detection and analysis	Define the threat vector, analyze and implement tools for log and error correlation.
Containment, eradication, and recovery	After an incident has been detected, it must be contained before it can spread. All containment strategies should also include steps to eradicate the threat and vulnerabilities, or at least mitigate them, and steps to recover operating systems, hardware components, and productive time.
Post-incident activity	A very crucial step, document what happened and how it was mitigated. This should provide insight for future incidents.

Computer Crime Investigation

To successfully prosecute computer crimes, investigators must prove three things:

Motive	Did they have a reason to commit the crime?
Opportunity	Were they available to commit the crime?
Means	Were they capable of committing the crime?

Collection of Evidence and Forensics

In response to security breaches, the infected system must be immediately isolated. Dump the memory to disk and create multiple master copies of the hard drive.

These master copies are usually locked in a safe for investigators who will use working copies for both the prosecution and the defense.

Law Enforcement and Liability

Most countries have three basic categories of laws:

Criminal	Concerned with crimes, and its penalties usually involve the risk of fines or imprisonment or both.
Civil	Civil law focuses on correcting wrongs that are not crimes, such as a company infringing on a patent.
Administrative	Involves government agencies enforcing regulations, such as paying employees their due vacation pay.

Organizations are required to practice due diligence and due care. While laws may make it difficult to prosecute intrusions, this does not diminish liability issues on the part of the organization. Companies can be found liable for not properly protecting their systems from being compromised (data breach, data leakage).

Ethics

Ethics is a standard that is higher than the law. It is a set of moral principles that govern civil behavior. Individuals who violate the code of ethics can face consequences such as loss of certification, loss of employment, and even prosecution by criminal or civil courts.

Disaster-Recovery and Business-Continuity Planning

Disaster recovery is the process of regaining access to the data, hardware, and software necessary to resume critical business operations after a natural or human-induced disaster or the unexpected or sudden loss of key personnel.

A disaster-recovery plan is part of business-continuity planning and requires extensive planning. The goal is to define objectives for the recovery of host computing systems that run the applications that support the business processes. Terms associated with business continuity include the following:

Maximum tolerable downtime (MTD)	Total amount of time the system owner or authorizing official is willing to accept for an outage or disruption.
Recovery time objective (RTO)	RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission, or business processes.
Recovery point objective (RPO)	The point in time, prior to a disruption or system outage, to which mission or business process data can be recovered after an outage.

Building a Security Strategy for Borderless Networks

The chapter covers the following topics:

Cisco Borderless Network Architecture

- Borderless Security Products

Cisco SecureX Architecture and Context-Aware Security

- Cisco TrustSec
- TrustSec Confidentiality
- Cisco AnyConnect
- Cisco Security Intelligence Operations

Threat Control and Containment

Cloud Security and Data-Loss Prevention

Secure Connectivity Through VPNs

Security Management

Cisco Borderless Network Architecture

Traditional approaches to network security used well-defined borders to protect inside networks from outside threats and malware. Employees used corporate computers secured with antivirus and personal firewalls. Perimeter-based networks were protected using network-scanning devices (firewalls, web proxies, and email gateways).

Today, network borders are dissolving as users want to access to resources from any locations, on any type of endpoint devices, using various connectivity methods. Cisco has addressed this with the Borderless Network Architecture, which integrates the following components:

| Borderless end zone | The zone offers deployment flexibility and strong security services in multiple dimensions as users connect to the network. End-user access is based on the security posture of the connecting endpoint using the Cisco AnyConnect SSL VPN Client. Infrastructure protection is provided using firewalls, intrusion prevention systems (IPSs), web security, and email security. |

Borderless Internet	Implemented by performing Layer 2 through Layer 7 scanning engines that are managed by enterprises and cloud providers. Scanning engines assume the role of firewalls, intrusion detection/prevention systems (IDSs/IPSs), network proxies, and web gateways.
Borderless data center	Layers virtualized components on top of existing infrastructure components to provide security solutions for the cloud.
Policy management layer	The security policy is managed in central locations and then enforced throughout the network based on context-specific variables. It provides the following: ■ Access policy (who, what, when, where, and how) ■ Dynamic containment policy ■ Policy for on and off premise

Borderless Security Products

The architectural approach to security found in the Borderless Network Architecture results in distinct categories of Cisco products, technologies, and solutions:

■ SecureX and context-aware security

■ Threat control and containment

■ Cloud security and data-loss prevention

■ Secure connectivity through VPNs

■ Security management

Cisco SecureX Architecture and Context-Aware Security

To respond to the evolving security needs of today's borderless network environments, Cisco developed the SecureX architecture. It is a new context-aware security architecture that enforces security policies across the entire distributed network, not just at a single point in the data stream.

The architecture starts with a solid network technology foundation that ensures the network infrastructure is not compromised in any way. It has security enforcement elements in the form of appliances, modules, or cloud services built on top. This architecture can deal with the full spectrum of devices, ranging from the traditional corporate PC or Mac, all the way to next-generation mobile devices such as iPads, Androids, or Cisco Cius. With Cisco AnyConnect, security is enforced in the network by tethering these myriad devices into the security infrastructure at the most optimal point and attaching seamlessly.

The components of the SecureX strategy include the following:

- Context awareness
- Cisco TrustSec
- Cisco AnyConnect
- Cisco Security Intelligence Operations (SIO)

Figure 3-1 illustrates the components of the SecureX strategy.
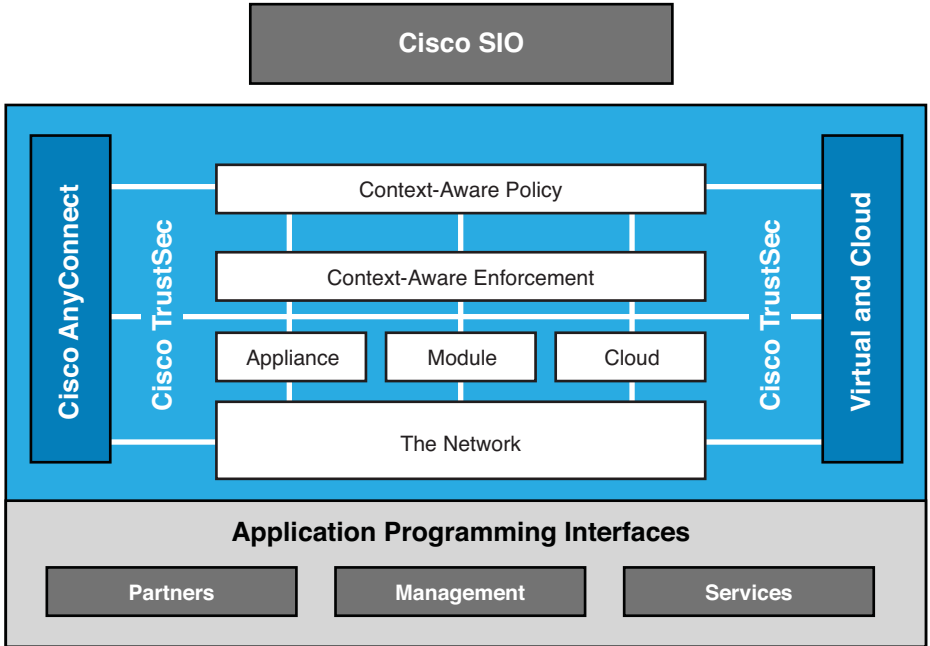
Figure 3-1   Cisco SecureX Components

Components of the Cisco SecureX strategy include the following:

Context-aware policies	Allows enforcement elements such as infrastructure devices to use user information (for example, user identity, security posture of the connecting device, the point of access to the network) to define the access policy.
Cisco TrustSec	TrustSec is an intelligent and scalable access control solution that mitigates security access risks across the entire network to provide access to anyone, anywhere, anytime.
Cisco AnyConnect Client	AnyConnect Client provides for secure connectivity across a broad set of PC- and smartphone-based mobile devices. The enforcement devices provide posture assessment, access control services, and policy enforcement.

Cisco Security Intelligence Operations (SIO)	SIO correlates data of almost a million live data feeds from deployed Cisco email, web, firewall, and IPS solutions to provide real-time insight into the global threat environment. Information is shared with Cisco customers and devices on demand.

Cisco TrustSec

TrustSec is an umbrella term that encompasses the Cisco next-generation Network Access Control (NAC) framework, including the following:

- Policy-based access control
- Identity-aware networking based on roles
- Data confidentiality
- Data integrity

It does so by incorporating the following technologies:

- IEEE 802.1x (Dot1x)
- Cisco NAC Appliance
- Profiling technologies
- Guest services
- Security group tags (SGTs) and security group ACLs (SGACLs)
- MACSec (802.1AE)
- Access Control Server (ACS)
- Identity Services Engine (ISE)

When user TrustSec identities are not based on IP addresses or usernames, they are role based. When users authenticate, their privileges are based on their SGT and SGACL.

Cisco ISE combines the functionality of other Cisco products—such as the Cisco Secure Access Control Server (SACS) for authentication, authorization, and accounting (AAA) services, and Network Admission Control (NAC)—into this next-generation policy server.

TrustSec Confidentiality

TrustSec implementation follows this process:

1. A user connects to a switch using 802.1X. The switch relays the authentication credentials to an ISE. The ISE authenticates the user and assigns the user an SGT.

2. Traffic from the authenticated user is tagged with its specific SGT. Network devices along the data path read this tag and enforce its associated policy by restricting access to predetermined network destinations and resources. The devices do so by using SGACLs.

3. TrustSec can also provide data confidentiality by using MACSec. For example, if a policy requires that data should be secured, Cisco TrustSec understands this policy and dynamically encrypts the user data.

Cisco AnyConnect

Cisco AnyConnect protects mobile employees on PC-based or smartphone platforms using an SSL or IP Security (IPsec) virtual private network (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 AnyConnect provides the following:

- Device support regardless of device type (for example, PC, laptop, smart phone, tablet, or PDA)

- Multifunctional security by combining multiple security controls in one client application

- Consistent experience by providing an always-on intelligent connection for seamless experience and performance

Cisco Security Intelligence Operations

Cisco Security Intelligence Operations (SIO) is a security intelligence center that baselines the current global state of threats and provides the network with valuable information to detect, prevent, and react to threats. It operates as an early-warning system by correlating threat information from the SensorBase, analyzed by the Threat Operations Center. This information is then provided to enforcement devices such as Cisco Adaptive Security Appliance (ASA), Integrated Services Router (ISR), and IPS device for real-time threat prevention.

Threat Control and Containment

The Cisco threat control and containment solution regulates network access, isolates infected systems, prevents intrusions, and protects critical business assets. This solution counteracts malicious traffic before it affects a business.

Threat prevention products include the following:

Cisco ASAs	The Adaptive Security Appliance devices provide proven firewall services and integration of VPN and IPS technologies.
Cisco ISRs	Integrated Services Routers provide network security controls using zone-based policy firewall (ZPF), IOS IPS, and VPN technologies.
Cisco IPS	Intrusion prevention is provided using dedicated appliances or is integrated into ASA and ISR devices. These IPS sensors support a variety of IPS technologies, including signature-based, anomaly-based, policy-based, and reputation-based techniques.

Cloud Security and Data-Loss Prevention

Adding to the complexity of securing a network is the fact that many modern network designs now incorporate cloud computing. Threats in cloud computing include the following:

- Abuse of cloud computing

- Account or service hijacking

- Data loss in the cloud

- Unsecure interfaces and application programming interfaces (APIs)

- Malicious insiders

Administrators, because they are ultimately responsible for data residing on networks over which they have no control, must also consider the consequences if the cloud environment is not properly secured.

Two following traditional key services must now be secured in the cloud:

Securing web access	Cisco ScanSafe Web Security is a cloud-based solution that analyzes every web request to determine whether content is malicious, inappropriate, or acceptable based on the defined security policy.
	Cisco IronPort Web Security integrates web-usage controls, data security, and reputation and malware filtering. It applies Cisco SIO and global threat technology, combats sophisticated web-based threats with layered security technology, and supports built-in management for visibility of threat-related activity.
Securing email access	Cisco IronPort Email Security provides spam protection, data-loss prevention, virus defense, and email encryption. It also helps minimize downtime, and simplifies corporate email system administration while offering insight into mail system operation.

Secure Connectivity Through VPNs

There are two VPN-based solutions to implement secure connectivity:

Secure communications for remote access	Provides secure customizable access to corporate networks and applications by establishing an SSL or IPsec VPN tunnel between the remote host and central site
Secure communications for site-to-site connections	Provides secure site-to-site IPsec VPN access between two or more sites

Security Management

Cisco network management systems help automate, simplify, and integrate a network to reduce operational costs; improve productivity; and achieve critical functions such as availability, responsiveness, resilience, and security.

The hierarchy of tools available for security management is as follows:

Device managers	Web interface tool that simplifies the configuration and monitoring of a single device.
Cisco Configuration Professional (CCP)	A GUI-based device management tool for ISRs. It simplifies the configuration, monitoring, and troubleshooting of LAN/WAN interfaces, routing, firewall settings, IPS, VPN, and unified communications.
Cisco ASA Security Device Manager (ASDM)	A GUI-based device management tool for ASAs that provides the similar features found in CCP.
Cisco Security Manager	An enterprise-level application solution to configure and manage thousands of firewalls, routers, switches, IPS sensors, and other security solutions. Scalability is provided using intelligent policy-based management techniques that simplify administration.

This page intentionally left blank

Network Foundation Protection

The chapter covers the following topics:

Threats Against the Network Infrastructure

Cisco Network Foundation Protection Framework

Control Plane Security

- Control Plane Policing

Management Plane Security

- Role-Based Access Control
- Secure Management and Reporting

Data Plane Security

- ACLs
- Antispoofing
- Layer 2 Data Plane Protection

Threats Against the Network Infrastructure

Common vulnerabilities and threats against a network infrastructure include the following:

Vulnerabilities	■ Design errors
	■ Protocol weaknesses
	■ Software vulnerabilities
	■ Device misconfiguration
Threats	■ Trust exploitation
	■ Login, authentication, and password attacks
	■ Routing protocol exploits
	■ Spoofing
	■ Denial of service (DoS)
	■ Confidentiality and integrity attacks

The impact of those threats and vulnerabilities includes the following:

Impact	
	■ Exposed management credentials
	■ High CPU usage
	■ Loss of protocol keepalives and updates
	■ Route flaps and major network transitions
	■ Slow or unresponsive management sessions
	■ Indiscriminate packet drops

Cisco Network Foundation Protection Framework

The Cisco Network Foundation Protection (NFP) framework provides an umbrella strategy for infrastructure protection forming the foundation for continuous service delivery.

NFP logically divides a router and Catalyst switches into three functional areas:

Control plane	Provides the ability to route data correctly. Traffic consists of device-generated packets required for the operation of the network itself, such as Address Resolution Protocol (ARP) message exchanges or Open Shortest Path First (OSPF) protocol routing advertisements.
Management plane	Provides the ability to manage network elements. Traffic is generated either by network devices or network management stations using tools such as Telnet, Secure Shell (SSH), Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), Network Time Protocol (NTP), or Simple Network Management Protocol (SNMP).
Data plane (forwarding plane)	Provides the ability to forward data. Typically consists of user-generated packets being forwarded to another end station. Most traffic travels through the router via the data plane. Data plane packets are typically processed in fast-switching cache.

Figure 4-1 provides a conceptual view of the NFP framework.
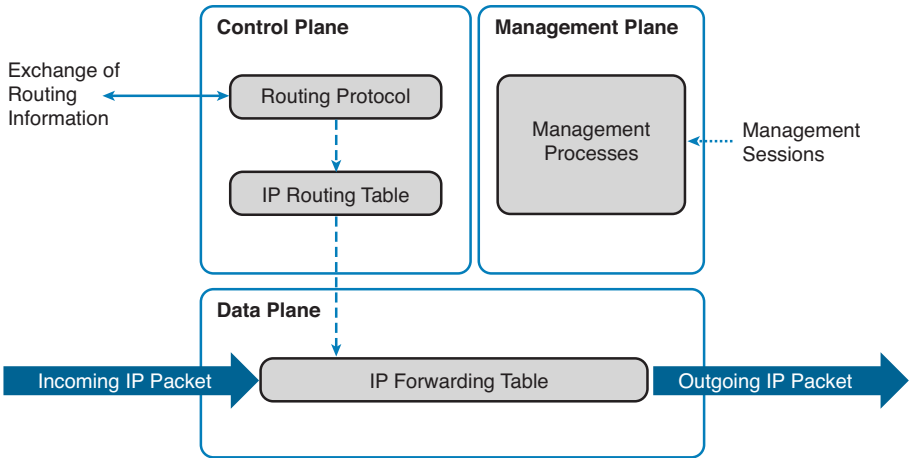
Figure 4-1   NFP Planes

Each of these planes must be protected to provide network availability and ensure con-
tinuous service delivery. The Cisco NFP framework provides the tools and techniques to
secure each of these planes.

Control Plane Security

Control plane security can be implemented using the following features:

Cisco AutoSecure	Cisco AutoSecure provides a one-step device lockdown fea-ture to protect the control plane and the management and data planes. It is a script that is initiated from the command-line interface (CLI) to configure the security posture of routers and disables nonessential system processes and services. It first makes recommendations to address security vulnerabilities and then modifies the router configuration.
Routing protocol authentication	Neighbor authentication prevents a router from accepting fraud-ulent routing updates. Most routing protocols support neighbor authentication.
CoPP	Control Plane Policing (CoPP) is used on higher-end Cisco devices with route processors. It is a Cisco IOS feature designed to enable users to manage the flow of traffic managed by the route processor of their network devices.

Control Plane Policing

CoPP is designed to prevent unnecessary traffic from overwhelming the route processor. The CoPP feature treats the control plane as a separate entity with its own ingress (input) and egress (output) ports. Because the CoPP feature treats the control plane as a separate entity, a set of rules can be established and associated with the ingress and egress ports of the control plane.

CoPP consists of the following features:

CoPP	Control Plane Policing lets users configure a QoS filter that manages the traffic flow of control plane packets. This protects the control plane against reconnaissance and DoS attacks.
CPPr	Control Plane Protection is an extension of CoPP but allows a finer policing granularity. For example, CPPr can filter and rate-limit the packets that are going to the control plane of the router and discard malicious and error packets (or both).
Control Plane Logging	The Control Plane Logging feature enables logging of the packets that CoPP or CPPr drop or permit. It provides the logging mechanism that is needed to deploy, monitor, and troubleshoot CoPP features efficiently.

Management Plane Security

Management plane security can be implemented using the following features:

Login and password policy	Restrict device accessibility. Limit the accessible ports and restrict the "who" and "how" methods of access.
Role-based access control	Ensure access is only granted to authenticated users, groups, and services. Role-based access control (RBAC) and authentication, authorization, and accounting (AAA) services provide mechanisms to effectively authenticate access.
Authorize actions	Restrict the actions and views that are permitted by any particular user, group, or service.
Secure management access and reporting	Log and account for all access. Record who accessed the device, what occurred, and when it occurred.
Ensure the confidentiality of data	Protect locally stored sensitive data from being viewed or copied. Use management protocols with strong authentication to mitigate confidentiality attacks aimed at exposing passwords and device configurations.
Present legal notification	Display legal notice developed with legal counsel.

Role-Based Access Control

RBAC restricts user access based on the role of the user. Roles are created for job or task functions and assigned access permissions to specific assets. Users are then assigned to roles and acquire the permissions that are defined for the role.

In Cisco IOS, the role-based CLI access feature implements RBAC for router management access. The feature creates different "views" that define which commands are accepted and what configuration information is visible. For scalability, users, permissions, and roles are usually created and maintained in a central repository server. This makes the access control policy available to multiple devices using it.

The central repository server can be a AAA server such as the Cisco Secure Access Control System (ACS) to provide AAA services to a network for management purposes.

Secure Management and Reporting

The management network is a very attractive target to hackers. For this reason, the management module has been built with several technologies designed to mitigate such risks.

The information flow between management hosts and the managed devices can be out-of-band (OOB) (information flows within a network on which no production traffic resides) or in-band (information flows across the enterprise production network, the Internet, or both).

Data Plane Security

Data plane security can be implemented using the following features:

Access control lists	Access control lists (ACLs) perform packet filtering to control which packets move through the network and where.
Antispoofing	ACLs can be used as an antispoofing mechanism that discards traffic that has an invalid source address.
Layer 2 security features	Cisco Catalyst switches have integrated features to help secure the Layer 2 infrastructure.

ACLs

ACLs are used to secure the data plane in a variety of ways, including the following:

Block unwanted traffic or users	ACLs can filter incoming or outgoing packets on an interface, controlling access based on source addresses, destination addresses, or user authentication.
Reduce the chance of DoS attacks	ACLs can be used to specify whether traffic from hosts, networks, or users can access the network. The TCP intercept feature can also be configured to prevent servers from being flooded with requests for a connection.

Mitigate spoofing attacks	ACLs enable security practitioners to implement recommended practices to mitigate spoofing attacks.
Provide band-width control	ACLs on a slow link can prevent excess traffic.
Classify traffic to protect other planes	ACLs can be applied on vty lines (management plane). ACLs can control routing updates being sent, received, or redistributed (control plane).

Antispoofing

Implementing the IETF best current practice 38 (BCP38) and RFC 2827 ingress traffic filtering renders the use of invalid source IP addresses ineffective, forcing attacks to be initiated from valid, reachable IP addresses which could be traced to the originator of an attack.

Features such as Unicast Reverse Path Forwarding (uRPF) can be used to complement the antispoofing strategy.

Layer 2 Data Plane Protection

The following are Layer 2 security tools integrated into the Cisco Catalyst switches:

Port security	Prevents MAC address spoofing and MAC address flooding attacks
DHCP snooping	Prevents client attacks on the Dynamic Host Configuration Protocol (DHCP) server and switch
Dynamic ARP inspection (DAI)	Adds security to ARP by using the DHCP snooping table to minimize the impact of ARP poisoning and spoofing attacks
IP source guard	Prevents IP spoofing addresses by using the DHCP snooping table

Protecting the Network Infrastructure Using CCP

The chapter covers the following topics:

Cisco Configuration Professional

Cisco Configuration Professional Express

- Connecting to CCP Express Using the GUI

Cisco Configuration Professional

- Configuring an ISR for CCP Support
- Installing CCP on a Windows PC
- Connecting to an ISR Using CCP

CCP Features and User Interface

- Application Menu Options
- Toolbar Menu Options
- Toolbar Configure Options
- Toolbar Monitor Options

Using CCP to Configure IOS Device-Hardening Features

- CCP Security Audit
- CCP One-Step Lockdown

Using the Cisco IOS AutoSecure CLI Feature

- Configuring AutoSecure via the CLI

Cisco Configuration Professional

Cisco Configuration Professional (CCP) is a Windows-based GUI application that is used to easily and reliably deploy, manage, and monitor Cisco Integrated Services Router (ISR) and ISR-G2 routers without requiring knowledge of the Cisco IOS command-line interface (CLI).

Advantages of CCP include the following:

Productivity	Can be used to get a router up and running quickly.
Simplicity	Provides easy-to-use wizards for routing and security configurations.
Cost savings	The GUI is intuitive and therefore has a low learning curve for a technician.
Reliability	Relies on best-practice configurations that are approved by the Cisco Technical Assistance Center (TAC).
Increased uptime	Provides easy-to-comprehend charts to monitor router status and troubleshoot wide area network (WAN) and virtual private network (VPN) connectivity issues.
License management	Simplifies ISR-G2 license management.
Facilitates hardware integration	Facilitates the integration of hardware-based functionality by using Cisco Services-Ready Engine (SRE) modules.

There are two versions of CCP:

CCP Express	This is a lightweight version of CCP that is embedded in flash of the router and can be used to configure initial interface and minimal security features.
CCP	This is a full-featured version that is used to organize and manage multiple routers using a standalone application that is installed on a host.

Cisco Configuration Professional is available for free and can be downloaded from http://www.cisco.com/go/ciscocp.

Cisco Configuration Professional Express

You can use Cisco CP Express for the initial router deployment. Routers shipped with CCP have CCP Express embedded in flash memory and a factory default router configuration.

> **NOTE:**   For example, on a Cisco 1841 router, the CCP Express filename in flash is cpexpress.tar, and the default factory router configuration is cpconfig-18xx.cfg.

The factory default preconfigures the following settings:

Router hostname	The router hostname is *yourname*.
Domain name	The domain name is *yourdomain.com*.
RSA keys	The router generates the non-exportable 1024-bit RSA keys.
Username	A privilege level 15 local database entry (cisco / cisco).
Interface Fa 0/0	An active interface with IP address 10.10.10.1 /29.
HTTP and HTTPS	Web access is enabled using local authentication from hosts with IP address 10.10.10.2–.6.
Banners	A login banner and user EXEC banner.
Console and vty	Local authentication for console and vty (Telnet/SSH).

CAUTION: The default username and password can be used only once. Another privilege level 15 local database entry must be configured; otherwise, you will be locked out once you log out.

Connecting to Cisco CP Express Using the GUI

Follow these steps to connect to Cisco CP Express on a router with default factory settings.

NOTE: The default factory configuration enables the router Fast Ethernet 0/0 (or Gigabit Ethernet 0/0) interface with IP address 10.10.10.1/29. Smaller Cisco routers (Cisco 815–1812) are Dynamic Host Control Protocol (DHCP) clients and attempt to obtain IP addressing automatically from an upstream device.

1. Connect the PC to the Fast Ethernet 0/0 (or Gigabit Ethernet 0/0) interface.
2. Configure the PC IP address **10.10.10.2 /29** on the host.
3. Open a browser window and enter the IP address **10.10.10.1** to connect to the router and start CCP Express.
4. When prompted for authentication, use the username **cisco** and password **cisco.**

Next, the Cisco CP Express Startup Wizard guides you through the remaining configuration (see Figure 5-1).
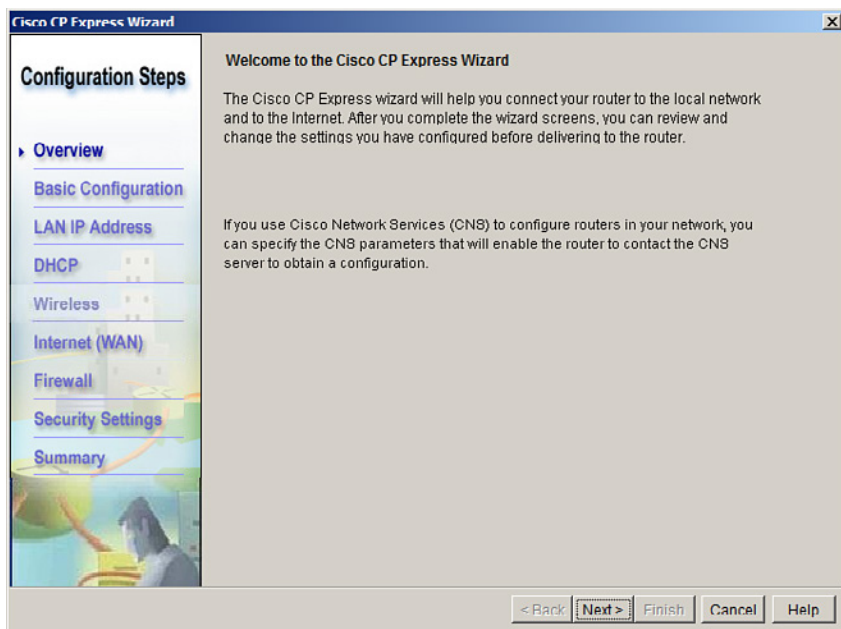
Figure 5-1   Cisco CP Express Startup Wizard

Click **Next** to display the Cisco CP Express Startup Wizard's Basic Configuration screen (see Figure 5-2).
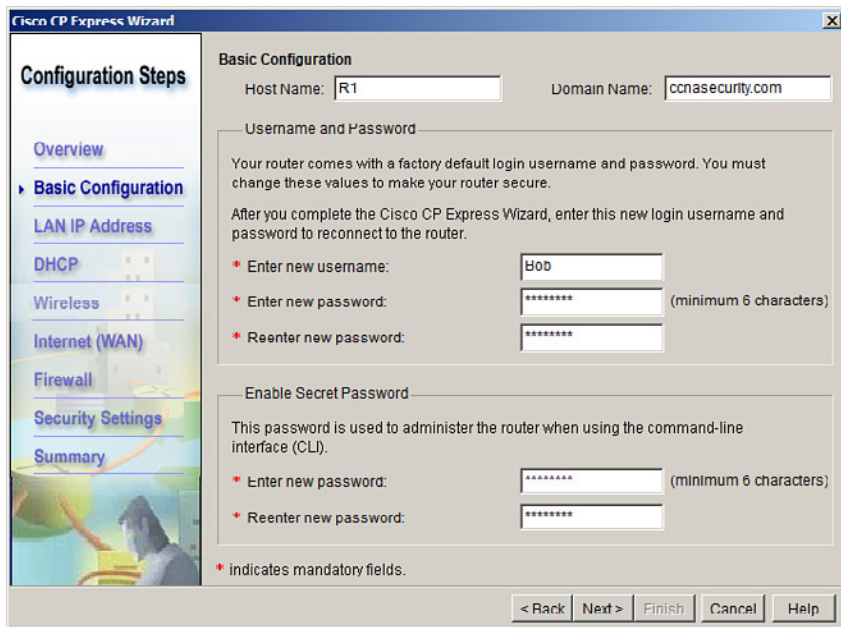
Figure 5-2   Cisco CP Express Startup Wizard Basic Configuration

After you configure the mandatory settings and clicking **Next**, the Startup Wizard guides you through the following:

Router provisioning	The screen prompts you on how you want to configure CCP.
LAN interface configuration	Identify the LAN interface IP address. The default IP address should be changed from 10.10.10.1/29.
DHCP server configuration	Enable DHCP server services on the LAN interface.
WAN configuration	Identify the LAN interface IP address.
NAT	Configure Network Address Translation (NAT) settings.
Default route	Create a default route.
Firewall settings	Enable the IOS firewall features.
Security settings	Select which security features to set.

Figure 5-3 shows an example of a main screen of Cisco CP Express after the router has been configured and reloaded.
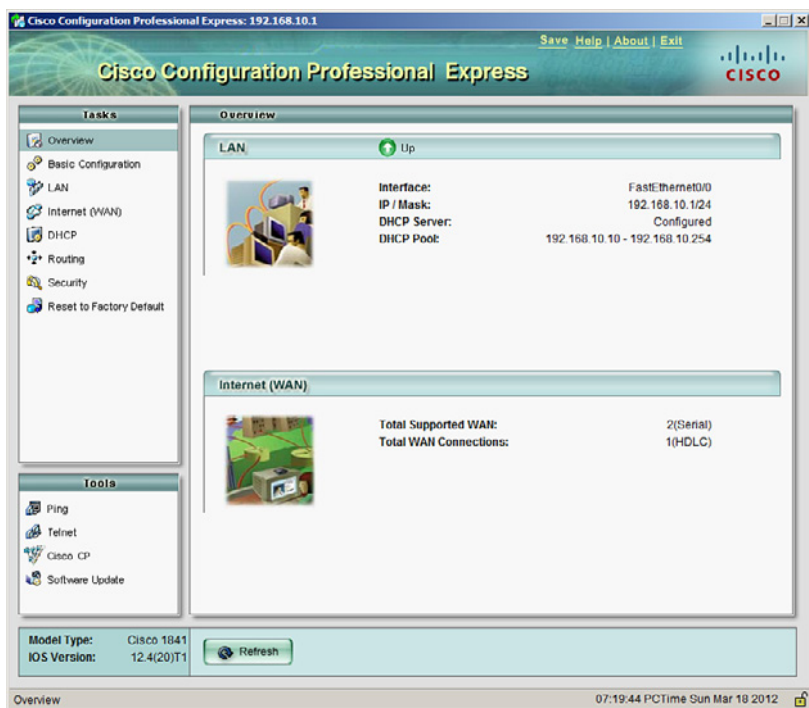
Figure 5-3   Cisco Configuration Professional Express

NOTE: You should use CCP Express only if you have minimal security, simple routing needs, and no requirement for voice support.

NOTE: CCP Express is fairly intuitive and therefore is not explored any further here.

Cisco Configuration Professional

The preferred way to configure an ISR using a GUI is with the Windows-based CCP application. CCP is installed locally on a PC and provides rich configuration capabilities to configure security features for data and voice.

NOTE: Only CCP configuration options are explored throughout the remainder of this portable command guide.

Configuring an ISR for CCP Support

A router must be configured to support a CCP connection. An ISR with default factory settings is configured to do so.

If an ISR no longer has the factory default configuration, you must initially configure the following to support a CCP session:

`Router(config)#`**`username`** `name` **`privilege`** `15` **`secret`** `password`	Creates a local user database username and password
`Router(config)#`**`hostname`** `hostname`	Sets the hostname of the router
`Router(config)#`**`interface`** `interface number`	Moves to interface configuration mode
`Router(config-if)#`**`ip address`** `ip-address subnet-mask`	Sets the IP address and mask
`Router(config-if)#`**`no shutdown`**	Enables the interface, although optional since the interface was already enabled
`Router(config-if)#`**`exit`**	Returns to global configuration mode
`Router(config)#`**`ip http server`**	Enables the HTTP service on the router
`Router(config)#`**`ip http secure-server`**	Enables HTTPS service on the router if the router IOS image supports crypto
`Router(config)#`**`ip http authentication local`**	Enables HTTP authentication using the local database

Router(config)#**ip http timeout-policy idle 60 life 86400 requests 10000**	Configures the HTTP timeout policy
Router(config)#**line vty 0 4**	Enters vty line mode for all five vty lines
Router(config-line)#**privilege level 15**	Sets the privilege level to the highest level
Router(config-line)#**transport input telnet ssh**	Allows only Telnet and SSH protocols access to VTY lines
Router(config-line)#**login local**	Enables authentication using the local database

Installing CCP on a Windows PC

You can download CCP for free from Cisco.com. Once downloaded, unzip the file and run the .exe file. The installation consists of accepting a license agreement and selecting the installation folder.

The host PC requires the following minimal settings:

- Internet Explorer 6.0 or later
- Java Runtime Environment Version 1.6.0_11 or later
- Adobe Flash Player Version 10 or later, with Debug set to **No**
- Memory 1GB DRAM, 2GB recommended
- Screen resolution 1024 x 768

NOTE: When the installation is complete, you have the option to run CCP for the first time. To successfully connect to an ISR using CCP, your router must have a supporting configuration.

Connecting to an ISR Using CCP

Follow these steps to connect to an ISR from a Windows host using CCP. The following assumes that the router still has the default factory configuration.

NOTE: The default factory configuration enables the router Fast Ethernet 0/0 (or Gigabit Ethernet 0/0) interface with IP address 10.10.10.1/29. Smaller Cisco routers (Cisco 815–1812) are DHCP clients and attempt to obtain IP addressing automatically from an upstream device.

1. Connect the PC to the Fast Ethernet 0/0 (or Gigabit Ethernet) 0/0 interface.
2. Configure the PC IP address **10.10.10.2 /29** on the host.
3. Launch the preinstalled CCP application by choosing the Windows **Start >**

All Programs > Cisco Configuration Professional > Cisco Configuration Professional. Otherwise, double-click the Cisco Configuration Professional icon on your desktop.

4. In the Manage Community dialog box, enter the IP address or hostname and the username and password information for the devices that you want to configure. In the Select / Manage Community window, enter the router IP address **10.10.10.1**, username **cisco**, and password **cisco.** Check the **Connect Securely** box if the image supports crypto.

NOTE: If you enter the default username **cisco** and default password **cisco**, the Change Default Credentials dialog box opens. For security reasons, you must change the default credentials to new credentials.

CAUTION: If you do not change the default username and passwords, you cannot log back in to the router after you log out.

5. Click **OK** to continue. The Change Default Credentials window appears and you must enter a new local database entry.

6. Click **OK** to continue. The Community View page appears (see Figure 5-4).
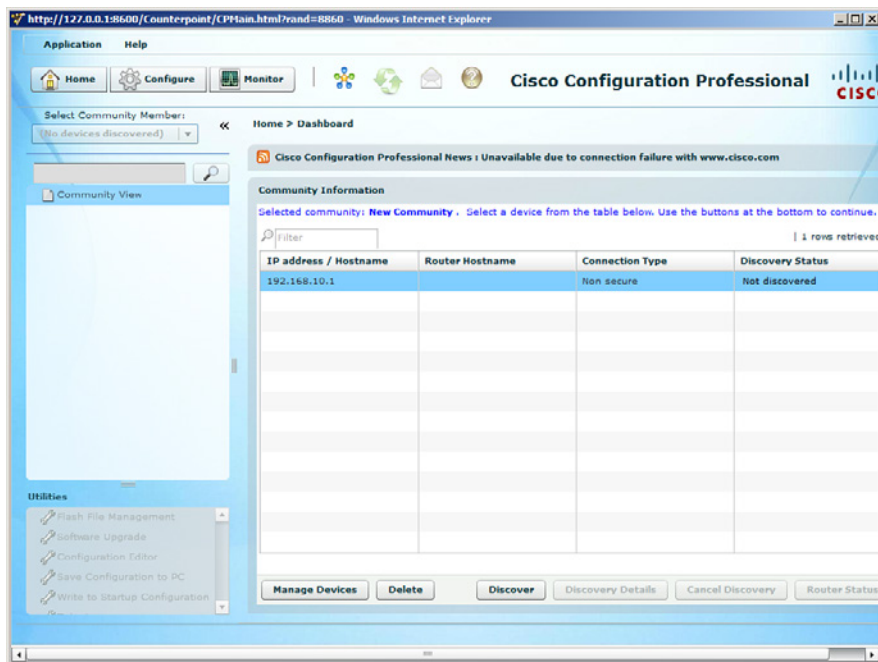
Figure 5-4   Community View Screen

On the Community View page, you have the following options:

Manage Devices	Used to add or edit community members
Delete	Used to remove a device from the community
Discover	Used to discover device information for a specific highlighted device
Discover Details	Displays device information while CCP is discovering it and, after it has been discovered, also displays errors if discovery fails
Router Status	Provides a summary view of hardware, software, and feature availability of the highlighted device

CCP Features and User Interface

CCP provides a single GUI to configure and easily manage the networking features of up to 10 ISRs per community. Figure 5-5 shows the CCP GUI layout.
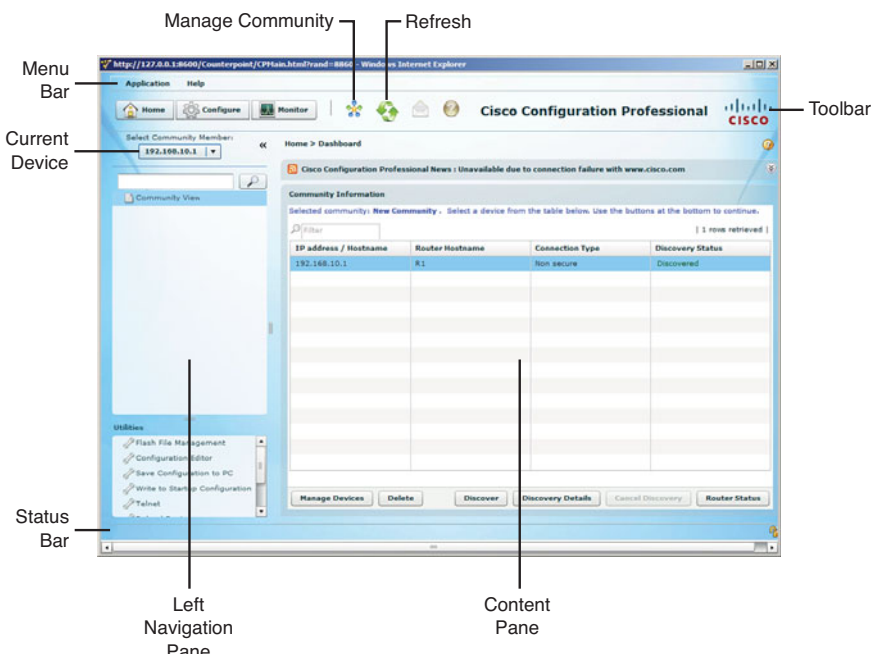
Figure 5-5 CCP GUI Window Layout

The CCP main screen contains the following components:

Menu bar	Contains an Application menu and Help menu.
Toolbar	Provides quick links to the Home, Configure, Monitor, Manage Community, Refresh, Email, and Help options.
Current device	The device listed can be configured or monitored.
Status bar	Displays when a secure connection is enabled.

Left navigation pane	Scalable panel to select the features to configure and monitor.
Content pane	Main workspace to configure features or view reports.

Application Menu Options

The Application menu options include the following:

Manage Community	Create a new community or choose an existing community.
Setup New Device	Start the New Device Setup Wizard to configure basic settings.
Create User Profile	Start the User Profile Creation Wizard to configure role-based access control (RBAC) and restrict user features.
Import User Profile	Import previously created user profiles.
Options	Set user preferences.
Template	Create, edit, or apply a configuration template.
Work Offline	Use CCP without being connected to a device.

Toolbar Menu Options

The toolbar provides the following options:

Home	Displays a summary view of the Community View page, allowing you to add, edit, and discover devices and to view the discovery and router status of each device.
Configure	Displays the features in the left navigation pane that can be configured on the selected device.
Monitor	Displays the router and security features in the left navigation pane that you can monitor for a chosen device.
Manage Community	Opens the Manage Community dialog box where you can add a new community or edit an existing community. A device must be in a community before it can be configured. Up to 10 devices can be discovered within the community.
Refresh	Rediscovers the selected device in the Select Community Member drop-down menu or rediscovers and reloads the current feature.
Help	Provides help content and is equivalent to the Menu Bar **Help > Help Contents** option.

Toolbar Configure Options

Click **Configure** on the toolbar to display the following options:

Interface Management	Includes the Cisco CP Connection Wizard that guides you through LAN and WAN configurations
Router	Contains features such as date/time, router access, DHCP, DNS, static routing, RIP, OSPF, EIGRP routing, AAA, ACL, Object Groups, router properties, NAT, QoS, and router provisioning
Security	Contains security-related features, including security audit and One-Step Router Lockdown features, VPN services, firewall services, intrusion prevention system (IPS), and security management

Toolbar Monitor Options

Click **Monitor** on the toolbar to display the following options:

Router	Displays various monitoring options, including interface status, logging, QoS status, and performance routing status.
Security	Displays various monitoring options, including firewall, VPN, IPS, NAC, and 802.1x status.
Traffic Monitoring	Monitoring options include link usage, link throughput, and traffic volume.

Using CCP to Configure IOS Device-Hardening Features

CCP Security Audit

Use the Security Audit Wizard to test a router configuration to determine whether any potential security problems exist in the configuration. The wizard also displays a screen that lets you determine which of those security problems you want to fix. Once determined, the Security Audit Wizard makes the necessary changes to the router configuration to fix those problems.

To perform the security audit, follow these steps:

1. On the toolbar, navigate to **Configure > Security > Security Audit** (see Figure 5-6).
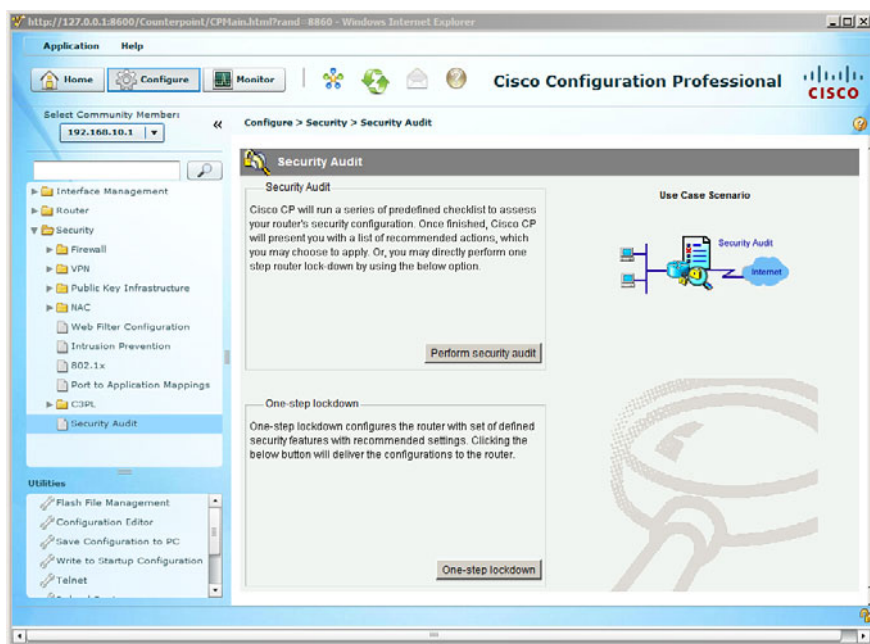
Figure 5-6   Security Audit Screen

2. Click **Perform Security Audit**. The Welcome page of the Security Audit Wizard opens.

3. Click **Next**. The Security Audit Interface Configuration page appears.

4. Select the **inside (trusted)** and **outside (untrusted)** interfaces and click **Next**.

5. The Security Audit Wizard tests the router configuration against Cisco recommended best practices to determine whether possible security problems exist. A report screen appears and lists the test results. If you want to save this report to a file, click **Save Report**. Otherwise, click **Close**.

6. The Security Audit Wizard now lists each security problem identified and provides the option to fix. As well, each problem is hyperlink to an explanation. Select which problems to fix and click **Next**.

7. The Summary screen now displays which services will be altered. Click **Finish**.

8. Finally, the Deliver Configuration to Device window lists the commands that will be sent to the router. Click **Deliver** to apply the changes.

CCP One-Step Lockdown

The One-Step Lockdown option tests your router configuration against Cisco-recommended best practices to determine whether possible security problems exist, and it automatically makes necessary configuration changes to correct problems it finds. Changes are made automatically and without prompting the user to select components to fix.

Navigate to **Configure > Security > Security Audit > One-Step Lockdown**.

Using the Cisco IOS AutoSecure CLI Feature

AutoSecure is a Cisco IOS CLI feature that, like CCP, lets you more easily configure security features on your router so that your network is better protected. CCP implements almost all the configurations that AutoSecure provides.

The following AutoSecure features are not implemented in this version of CCP One-Step Lockdown:

Disabling Network Time Protocol (NTP)	AutoSecure disables NTP if it is not necessary. Otherwise, NTP is configured with message digest 5 (MD5) algorithm authentication. CCP does not support disabling NTP.
Configuring authentication, authorization, and accounting (AAA)	If AAA is not configured, AutoSecure configures local AAA and prompts for configuration of a local username and password database on the router. CCP does not support AAA configuration.
Setting selective packet discard (SPD) values	CCP does not set SPD values.
Enabling TCP intercepts	CCP does not enable TCP intercepts.
Configuring antispoofing access control lists (ACLs) on outside interfaces	AutoSecure creates three named ACLs to prevent antispoofing source addresses. CCP does not configure these ACLs.

Configuring AutoSecure via the CLI

To configure AutoSecure via the CLI, follow these steps:

1. In privileged EXEC mode, enter **auto secure**. A banner explaining what AutoSecure does appears.

2. Answer if the device is connected to the Internet.

3. Answer how many interfaces are facing the Internet.

4. Identify which interface is facing the Internet.

5. Enter a security banner.

6. Enter the privileged EXEC password.

7. Enter the enhanced login features.

8. Answer if SSH should be configured.

9. Configure the context-based access control (CBAC) firewall feature.

10. Apply the configuration to the running configuration.

This page intentionally left blank

Securing the Management Plane

The chapter covers the following topics:

Planning a Secure Management and Reporting Strategy

Securing the Management Plane

- Securing Passwords
- Securing the Console Line and Disabling the Auxiliary Line
- Securing VTY Access with SSH
- Securing VTY Access with SSH Example
- Securing VTY Access with SSH Using CCP Example
- Securing Configuration and IOS Files
- Restoring Bootset Files

Implementing Role-Based Access Control on Cisco Routers

- Configuring Privilege Levels
- Configuring Privilege Levels Example
- Configuring RBAC via the CLI
- Configuring RBAC CLI Example
- Configuring Superviews
- Configuring a Superview Example
- Configuring RBAC Using CCP Example

Network Monitoring

- Configuring a Network Time Protocol Master Clock
- Configuring an NTP Client
- Configuring an NTP Master and Client Example
- Configuring an NTP Client Using CCP Example
- Configuring Syslog
- Configuring Syslog Example
- Configuring Syslog Using CCP Example
- Configuring SNMP
- Configuring SNMP Using CCP Example

Planning a Secure Management and Reporting Strategy

Small networks are relatively easy to manage and monitor. However, device management and monitoring can be challenging on a large network, especially considering the number of infrastructure devices generating syslog data.

You must decide whether the network management data flows over an in-band (over the production network) or out-of-band (over a separate network) network.

Consider the following in-band management guidelines:

- Typically appropriate for smaller networks.

- Network information flows over a production network.

- Apply only to devices that need to be managed or monitored.

- Use secure protocols such as IPsec, Secure Shell (SSH), or Secure Sockets Layer (SSL) when possible.

- Decide whether the management channel needs to be open at all times.

Consider the following out-of-band (OOB) management guidelines:

- Typically implemented in larger networks.

- Network information does not flow over the production network.

- Provides the highest level of security.

- Eliminates the risk of passing unsecure management protocols over the production network.

NOTE: Regardless of which network management method you choose, you must secure the management plane.

NOTE: You can implement both in-band and OOB simultaneously.

Securing the Management Plane

Securing the management plane includes the following:

- Enforcing a secure password policy

- Securing console, vty, and auxiliary lines

- Securing and archiving configurations

- Enabling logging to record changes in real time, on demand, and scheduled reports

- Using Network Time Protocol (NTP) to keep clocks synchronized because it can identify the order in which a specified attack occurred

- Choosing appropriate logging levels for each device while ensuring that the right data is being captured

- Implementing a change management policy

NOTE: The focus of this chapter is on securing the management plane.

Securing Passwords

Keep the following in mind when enforcing a password policy:

- Change passwords often.

- Include alphanumeric characters, uppercase and lowercase characters, symbols, and spaces.

- Password-leading spaces are ignored; all spaces after the first character are not ignored.

- Do not use dictionary words.

- Encrypt all passwords.

- Passwords should have a minimum of 10 characters.

`Router(config)#`**`service password-`** **`encryption`**	Encrypt all plaintext passwords to level 7.
`Router(config)#`**`security passwords`** **`min-length`** *`length`*	Enforce a minimum password length for all new passwords. Existing passwords are not affected. Length can be from 1 to 16. Ten characters or more are recommended.
`Router(config)#`**`enable secret`** *`password`*	Encrypt the privileged EXEC mode (enable) password using message digest 5 (MD5) algorithm.

Securing the Console Line and Disabling the Auxiliary Line

`Router(config)#`**`username`** *`name`* **`privilege`** *`level`* **`secret`** *`password`*	Create a local user database entry and encrypt the password. **TIP:** Always create the local user database accounts before enabling authentication.
`Router(config)#`**`line console 0`**	Enter line console config mode.
`Router(config-line)#`**`login local`**	Authenticate using the local database. This method is stronger than using the **`password`** and **`login`** combination because it requires a username.

`Router(config-line)#`**`exec-timeout`** *`minutes seconds`*	Set the inactivity timer interval to 5 minutes. Default is 10 minutes.
`Router(config-line)#`**`line aux 0`**	Enter line auxiliary mode.
`Router(config-line)#`**`no exec`**	Disable the auxiliary port.

Securing VTY Access with SSH

`Router(config)#`**`hostname`** *`name`*	A hostname other than Router must be configured.
`Router(config)#`**`username`** *`name`* **`privilege`** *`level`* **`secret`** *`password`*	Create a local user database entry and encrypt the password.
`Router(config)#`**`ip domain name`** *`name`*	Configure a domain name. Required to implement SSH. The IOS also accepts the hyphenated command **`ip domain-name.`**
`Router(config)#`**`crypto key generate rsa general-keys modulus`** *`modulus`*	Generate the general usage RSA keys that SSH requires. Required to implement SSH.
`Router(config)#`**`ip ssh version`** **`[1｜2]`**	Specify the version of SSH to enable. Choosing **`1`** only runs SSHv1. Choosing **`2`** only runs SSHv2. By default, SSH runs in compatibility mode, which means that both version 1 and 2 are supported. To return to compatibility mode, enter the command **`no ip ssh version.`** **NOTE:** SSHv1 has known security issues. Therefore, it is recommended to use SSHv2 whenever possible.
`Router(config)#`**`ip ssh time-out`** *`seconds`*	(Optional) The number of seconds to wait for the SSH client to respond during the negotiation phase. Default is 120 seconds.
`Router(config)#`**`ip ssh authentication-retries`** *`integer`*	(Optional) Limit the number of login attempts. Default is 3.
`Router(config)#`**`login block-for`** *`seconds`* **`attempts`** *`tries`* **`within`** *`seconds`*	Configure enhanced vty login.
`Router(config)#`**`line vty 0 4`**	Enter line vty mode.
`Router(config-line)#`**`login local`**	Authenticate using the local database. **NOTE:** This command is available only if AAA is not enabled.

`Router(config-line)#`**`transport`** **`input ssh`**	Only allow incoming SSH sessions.
`Router(config-line)#`**`access-class`** *`ACL-number`*	Apply an access control list (ACL) to specify who can access the vty line.

Securing VTY Access with SSH Example

`Router(config)#`**`hostname R1`**	Change the hostname from Router.
`R1(config)#`**`username Bob privilege 15 secret`** **`cisco123`**	Create a local user database entry and encrypt the password.
`R1(config)#`**`ip domain-name ccnasecurity.com`**	Configure the required domain name.
`R1(config)#`**`crypto key generate rsa`** **`general-keys modulus 1024`**	Generate the general usage RSA keys that SSH requires. Required to implement SSH.
`R1(config)#`**`ip ssh version 2`**	Only allow SSH Version 2.
`R1(config)#`**`ip ssh time-out 60`**	Configure an SSH timeout period of 60 seconds.
`R1(config)#`**`ip ssh authentication-retries 2`**	Limit the number of login attempts.
`R1(config)#`**`login block-for 60 attempts 3`** **`within 30`**	After three failed login attempts within a 30-second time span, do not display the login prompt for 60 seconds.
`R1(config)#`**`line vty 0 4`**	Enter line vty mode.
`R1(config-line)#`**`login local`**	Authenticate using the local database.
`R1(config-line)#`**`transport input ssh`**	Only allow incoming SSH sessions.
`R1(config-line)#`**`access-class ADMIN-IN in`**	Only permit users defined in the ACL ADMIN-IN to access the vty lines.

To SSH from a host, an SSH client such as PuTTY, OpenSSH, or TeraTerm is required.

To SSH from another router using the command-line interface (CLI), use the following command:

`R3#`**`ssh –l Bob 10.1.1.1`** `Password:`	The administrator on R3 is connecting to R1.

> **NOTE:** Use the `show ssh` command to display the SSH connection's status. Use the `show ip ssh` command to display the SSH version and SSH configuration data.

Securing VTY Access with SSH Using CCP Example

Choose **Configure > Router > Router Access > VTY** to open the VTY information screen (see Figure 6-1).
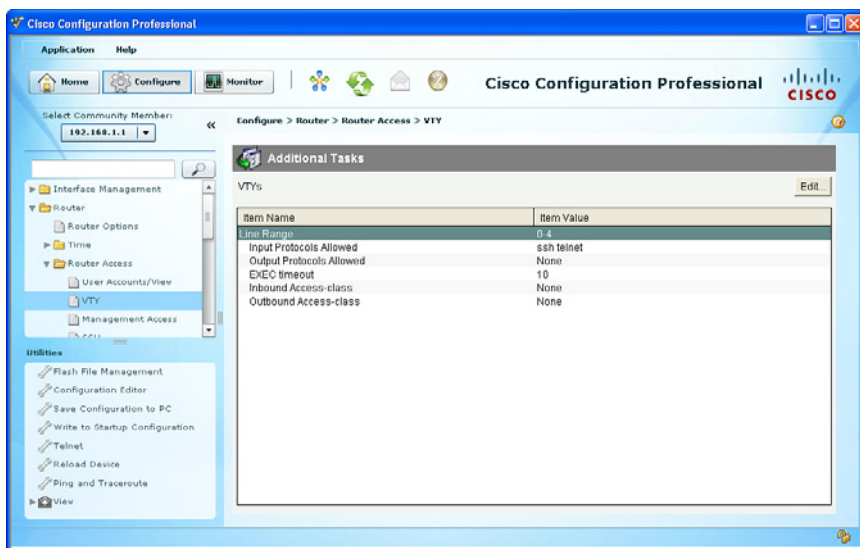
Figure 6-1 VTY Information Screen

Click **Edit** to change the vty parameters.

In the example in Figure 6-2, the vty interface is set with an executive timeout of 5 minutes (the default is 10) and accepts only incoming SSH connections from hosts identified in the ADMIN-IN ACL. The ACL specified must be preconfigured on the router.
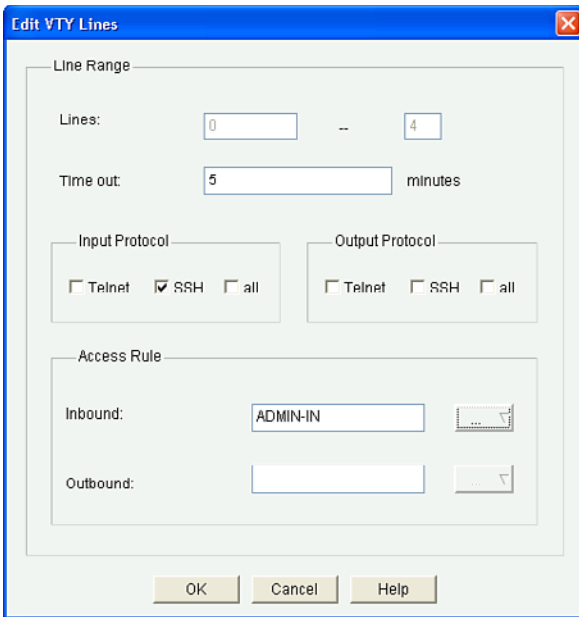
Figure 6-2   Edit VTY Lines Dialog

NOTE: Additional options are available when authentication, authorization, and accounting (AAA) is enabled.

Click **OK** and Cisco Configuration Professional (CCP) displays the Deliver Configuration to Device summary window, as shown in Figure 6-3. The window displays the CLI commands that will be configured on the router.
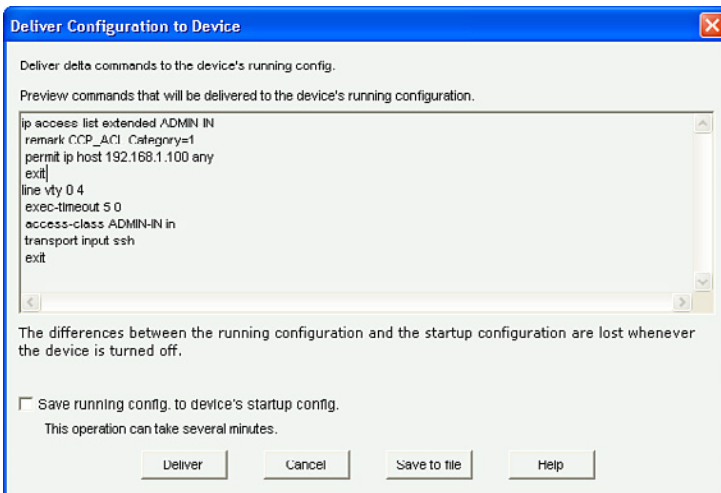
Figure 6-3   Deliver Configuration to Device Summary Window

Click **Deliver** to commit the configuration changes. CCP displays the revised VTY information screen, as shown in Figure 6-4.

Figure 6-4　Revised VTY Information Screen

Securing Configuration and IOS Files

Securing the router configuration and IOS image files is critical. The Cisco IOS Resilient Configuration feature secures working copies of these files by creating bootset files that cannot be erased from a router.

The following example secures the IOS image and configuration file on an 1841 Integrated Services Router (ISR).

`R1(config)#`**`secure boot-image`**
 	
`Jul  1 09:02:03.639: %IOS_RESILIENCE-`
`5-IMAGE_RESIL_ACTIVE: Successfully`
`secured running image`
	Secure the IOS image by hiding it in flash. It can be seen only when in ROMMON mode.

`R1(config)#`**`secure boot-config`**
 	
`Jul  1 09:02:12.563: %IOS_RESILIENCE-`
`5-CONFIG_RESIL_ACTIVE: Successfully`
`secured config archive`
`[flash:.runcfg-20120701-`
`090211.ar]`
	Take a snapshot of the router running configuration and securely archive it in flash. It can be seen only when in ROMMON mode.

`R1#`**`show secure bootset`**
 	
`IOS resilience router id FHK1028517C`
 	
`IOS image resilience version 12.4 acti-`
`vated at 09:02:03 UTC Sun Jul 1 2012`
 	
`Secure archive flash:c1841-advipser-`
`vicesk9-mz.124-20.T1.bin type is image`
`(elf) []`
 	
`  file size is 37081324 bytes, run size`
`is 37247008 bytes`
 	
`  Runnable image, entry point 0x8000F000,`
`run from ram`
 	
`IOS configuration resilience version 12.4`
`activated at 09:02:12 UTC Sun Jul 1 2012`
 	
`Secure archive flash:.`
`runcfg-20120701-090211.ar type is config`
 	
`configuration archive size 3160 bytes`
	Display the status of Cisco IOS image and configuration resilience. This step is important to verify that the Cisco IOS image and configuration files have been properly backed up and secured.
	
	Of importance to note are the location and filenames of both files (for example, flash:c1841-advipservicesk9-mz.124-20.T1.bin and flash:.runcfg-20120701-090211.ar).

Restoring Bootset Files

To restore a primary bootset from a secure archive after the router has been tampered with (by an NVRAM erase or a disk format), you must complete four steps.

The following example walks through the process of restoring bootset files to an ISR with a corrupt IOS that boots to ROMMON mode.

`Router#`**`reload`** `Proceed with reload? [confirm]`	Reload the router. Press **Enter** to continue.
`rommon 1 > `**`dir flash:`**	Enter ROMMON mode and display the bootset files.
`rommon 2 > `**`boot c1841-advipser-`** **`vicesk9-mz.124-20.T1.bin`**	Boot the router using the listed image.
`Router(config)#`**`secure boot-config`** **`restore flash:.runcfg-20120701-090211.`** **`ar`**	Restore the secure configuration to the archive found in flash.

Implementing Role-Based Access Control on Cisco Routers

Configuring Privilege Levels

`Router(config)#privilege` *mode* {`level` *level command* | `reset` *command*}	Assign commands to a custom privilege level between level 2 and 14.
	There are 16 privilege levels. Level 0 is entry level, level 1 is for user EXEC access, and level 15 is privileged EXEC mode. Levels 2–14 are customizable.
`Router(config)#enable secret level` *level password*	Assign a password to the custom privilege level.
`Router>enable` *level*	Enter a custom privilege level.

> **NOTE:**   Use the `show privilege` command to display the current privilege level.

Configuring Privilege Levels Example

`R1(config)#privilege exec level 5 ping`	Add the `ping` command to level 5.
`R1(config)#privilege exec level 5 reload`	Add the `reload` command to level 5.
`R1(config)#enable secret level 5` `cisco12345`	Configure an enable password to enter level 5.
`R1>enable 5` `Password:`	The user logs in with privilege level 5.
	Along with the regular user EXEC commands, the level 5 user also has the `ping` and `reload` available.
`R1#show privilege` `Current privilege level is 5`	Verify the privilege level.

Configuring RBAC via the CLI

`Router(config)#aaa new-model`	Enable AAA. AAA must be configured before you can enable a view.
`Router#enable view` `Password:`	Enter root view. Required to configure and alter views. Use the enable password when prompted.

`Router(config)#`**`parser view`** *`view-name`*	Create a view in global configuration mode. There is a maximum limit of 15 views in total excluding the root.
`Router(config-view)#`**`secret`** *`password`*	Assign a password to the view. This is a required step.
`Router(config-view)#` **`commands`** *`parser-mode`* {**`include`** | **`include-exclusive`** | **`exclude`**} [**`all`**] [**`interface`** *`interface-name`* | *`command`*]	Assign commands to the current view. Views contain commands.
`Router#`**`enable view`** *`view-name`*	Enter and verify a view.

NOTE: Use the `show parser view` command to verify the current view. Root can also use the command `show parser view` to display all configured views.

Configuring RBAC via the CLI Example

`R1(config)#`**`aaa new-model`**	Enable AAA.
`R1#`**`enable view`** `Password:`	Enter root view.
`R1(config)#`**`parser view SHOWVIEW`**	Create a view called **SHOWVIEW**.
`R1(config-view)#`**`secret cisco123`**	Assign a password to the view.
`R1(config-view)#`**`commands exec include show`**	This view can use all `show` commands from privileged EXEC mode.
`R1(config-view)#`**`commands exec include ping`**	This view can use the `ping` command.
`R1#`**`enable view SHOWVIEW`** `Password:`	Log in to the SHOWVIEW view to verify it.

Configuring Superviews

`Router(config)#`**`parser view`** *`view-name`* **`superview`**	Create a superview in global configuration mode. A superview can only contain other views. A superview cannot contain commands.
`Router(config-view)#`**`secret`** *`password`*	Assign a password to the view. This is a required step.
`Router(config-view)#`**`view`** *`view-name`*	Assign an existing view to the superview. Multiple views can be assigned to a superview.
`Router#`**`enable view`** *`view-name`*	Enter and verify a view.

Configuring a Superview Example

| ```
R1(config)#parser view JR-ADMIN
superview
``` | Create a superview called **JR-ADMIN**. |
`R1(config-view)#secret cisco12345`	Assign a password to the view.
`R1(config-view)#view SHOWVIEW`	Assign the SHOWVIEW view to the superview.
`R1(config-view)#view VERIFYVIEW`	Assign the VERIFYVIEW view to the superview.
| ```
R1#show parser view all
Views/SuperViews Present in System:
 SHOWVIEW
 VERIFYVIEW
 JR-ADMIN *
-------(*) represent superview-------
R1#
``` | Show all views. |
| ```
R1#enable view JR-ADMIN
Password:
``` | Enable a view. The JR-ADMIN superview has access to the commands listed in the other views. |
| ```
R1#show parser view
Current view is 'JR-ADMIN'
``` | Verify which view you are in. |
| ```
R1#show parser view all
                    ^
% Invalid input detected at '^' marker.
``` | **NOTE:** The `show parser view all` command is available only to the root view. |

Configuring RBAC Using CCP Example

In this example, a user named JR-ADMIN is assigned privilege level 1 and made a member of the preset CCP_Monitor view.

Choose **Configure > Router > Router Access > User Accounts/View**.

Figure 6-5 displays the contents of the local database.

Figure 6-5   User Accounts/View Information Screen

From this screen, you can add, edit, or delete a user. To create a new user with a lower privilege level, click **Add**. The Add an Account dialog opens (see Figure 6-6).

Figure 6-6   Add an Account Dialog

> **NOTE:** Protocols that require the retrieval of clear-text passwords, such as Challenge Handshake Authentication Protocol (CHAP), cannot be used with MD5-encrypted passwords.

A user can be assigned a privilege level and associated with one of four preset RBAC views, as shown in Figure 6-7.

Figure 6-7 Preset RBAC Views

CCP_Administrator	User has complete access to CCP and can perform all operations supported by CCP.
CCP_Monitor	User can monitor all features supported by CCP but cannot deliver configurations.
CCP_Firewall	User can only use the CCP Firewall and Monitor features and configure firewalls and ACLs using the Firewall Wizard, Firewall Policy view, and ACL editor.
CCP_EasyVPN_Remote	User can only use the CCP Easy VPN Remote features to create Easy VPN Remote connections and edit them.

Choose a view and click **OK**.

> **NOTE:** When choosing a view other than the CCP_Administrator, you are prompted to enter the view password.

CCP displays the CLI configuration commands. Click **Deliver** to commit the configuration changes.

Figure 6-8 shows the new user JR-ADMIN.

Figure 6-8 Revised User Account/View Information Screen

Network Monitoring

Network monitoring includes using syslog and Simple Network Management Protocol (SNMP) features. Regardless, all devices can be synchronized using NTP.

Configuring a Network Time Protocol Master Clock

Time synchronization between devices is critical. Devices should be synchronized with a public time server on the Internet or with an internal time source.

You can configure a router to be an NTP master clock source when other sources are not available.

Router(config)#**ntp master** *stratum*	Configure the router to be the NTP master.
	The stratum number is optional and is the number of hops away from an authoritative time source, such as an atomic clock.
Router(config)#**ntp authenticate**	Enable NTP authentication.
Router(config)#**ntp authentication-key** *key-number* **md5** *key-value*	Define the NTP key and password and encrypt it using MD5.
Router(config)#**ntp trusted-key** *key-number*	Identify the trusted key on the master.
	To synchronize, an NTP client must provide the correct trusted key and password.

Configuring an NTP Client

Client(config)#**ntp server** *ntp-server-address*	Enable Router to be the master clock to which peers will synchronize.
Client(config)#**ntp authentication-key** *key-number* **md5** *key-value*	Define the NTP key and password and encrypt it using MD5.
Client(config)#**ntp trusted-key** *key-number*	Identify the trusted key on the master.

NOTE: Other NTP-related commands are also available.

Configuring an NTP Master and Client Example

The following example configures R1 to be the master NTP clock:

R1#**clock set 9:00:00 july 1 2012**	Set the local device clock.
R1(config)#**ntp master 1**	Enable R1 to be the master clock to which clients will synchronize.

R1(config)#**ntp authentication-key 1 md5 cisco123**	Specify the NTP password and encrypt it using MD5. In this example, a peer router must authenticate with the password cisco123.
R1(config)#**ntp trusted-key 51**	Identify the trusted key on the master. A peer must also provide the correct trusted key in its NTP packets.
R1(config)#**ntp authenticate**	Enable NTP authentication.

The following example configures R3 to be the NTP client:

R3(config)#**ntp server 10.1.1.1**	Enable R1 to be the master clock with which peers will synchronize.
R3(config)#**ntp authentication-key 1 md5 cisco123**	Specify the NTP password and encrypt it using MD5. In this example, a peer router must authenticate with the password cisco123.
R3(config)#**ntp trusted-key 51**	Identify the trusted key on the master. A peer must also provide the correct trusted key in its NTP packets.

> **NOTE:**   It may take up to 2 minutes for the device clock to synchronize with the NTP master.

You can verify the clock settings using the `show clock`, `show ntp associations`, and `show ntp status` commands.

Configuring an NTP Client Using CCP Example

In this example, the time is set on R1 and it is configured as the NTP master via the CLI. Then R1 is specified, using CCP, as the NTP server to NTP client router R3.

> **NOTE:**   You must use the CLI to configure a router as an NTP master. CCP can be used only to configure an NTP client.

To configure R3 to be an NTP client, choose **Configure > Router > Time > NTP and SNTP**, and then click **Add**. The Add NTP Server Detail window opens (see Figure 6-9).

Figure 6-9   Add NTP Server Details Window

In this example, the clock as been set on R1, and it is being configured as the NTP master.

> **NOTE:**   Use the routing table to identify the source interface that connects to the master NTP server.

Click **OK** to complete the entry. The NTP server should now be displayed as shown in Figure 6-10.

Figure 6-10   Revised NTP Information Screen

Configuring Syslog

Log messages can be sent to one of the following locations:

Console	Useful when modifying or testing the router while connected to the console, but messages are not stored.
VTY lines	Useful when accessing a device remotely, but messages are not stored.

Buffer	Messages are stored in the router memory but lost when it is rebooted or the buffer is full. Use the `show logging` command to view logging messages.
Syslog	Very useful message logging facility, which sends log messages to servers. The server provides a central long-term log storage capability for all networking devices.
SNMP server	Specific router events can be trapped and forwarded to an external SNMP server.

NOTE: To reduce the CPU load, disable logging to the console using the `no logging console` and instead send logging information to the local log buffer.

NOTE: When telnetting to a router, use the `terminal monitor` command to view log messages.

Router log messages typically contain time stamps, log messages, severity levels, and message text. Cisco router log messages fall into one of eight levels.

0	LOG_EMERG	Emergencies, such when the router is unusable
1	LOG_ALERT	A condition that should be corrected immediately, such as a corrupted system database
2	LOG_CRIT	Critical conditions, such as hard device errors
3	LOG_ERR	Errors such as invalid memory size
4	LOG_WARNING	Warning messages, such as the crypto operation failed
5	LOG_NOTICE	Conditions that are normal but important
6	LOG_INFO	Informational messages, such as when a packet is denied
7	LOG_DEBUG	Messages that contain information normally of use only when debugging a program

Syslog requires a syslog server and a syslog client:

`Router(config)#service timestamps`	Enable time stamps on debug and logging messages.
`Router(config)#logging host [ip-address | hostname]`	Identify the syslog server address or hostname.
`Router(config)#logging trap level`	Limit messages logged to the syslog servers based on severity. Default is 0–6.

Router(config)#**logging source-interface** *interface-type interface-number*	Specify that syslog packets contain the IP address of a specific interface, regardless of which interface the packet uses to exit the router.
Router(config)#**logging on**	On by default, it sends messages to the buffer, vty lines, and syslog server.

Use the `show logging` command to display the state of system logging (syslog) and the contents of the standard system logging buffer.

Configuring Syslog Example

Router R1 is configured to send level 5 messages to a syslog server located at 192.168.1.100:

R1(config)#**service timestamps**	Enable time stamps on debug and logging messages.
R1(config)#**logging host 192.168.1.100**	Identify the syslog server IP address.
R1(config)#**logging trap 5**	Limit log messages to severity level 0–5.
R1(config)#**logging source-interface loopback 0**	Always specify the Lo0 interface as the source interface from this router.

Configuring Syslog Using CCP Example

To enable syslog logging using CCP, choose **Configure > Router > Logging**.

The Logging information screen will display, as shown in Figure 6-11.

Figure 6-11   Logging Information Screen

To enable syslog logging and add a syslog server, click **Edit**.

The Logging dialog appears, as shown in Figure 6-12. Enter the syslog server information. You can enable a logging buffer and configured it separately.

Figure 6-12   Logging Dialog

In this example, informational (level 6) messages will be forwarded to a syslog server located at IP address 192.168.1.100. As well, debugging (level 7) messages will be sent to the router memory buffer.

After configuring these settings, click **OK**.

CCP displays the CLI configuration commands. Click **Deliver** to commit the configuration changes.

CCP now displays the syslog settings, as shown in Figure 6-13.

Logging	
Property	**Value**
Syslog	Enabled
Syslog Server1	192.168.1.100
Logging to Buffer	Enabled
Buffer Size	4096
Logging Level	debugging (7)
Host Logging Level	informational (6)

Figure 6-13 Revised Syslog Information Screen

> **NOTE:** Use the `show logging` command to view logging settings and logging information sent to the memory buffer.

To monitor logging information with CCP, choose **Monitor > Router > Logging**, as shown in Figure 6-14. You can choose the logging information to view from the drop-down list.

Figure 6-14 Monitoring Syslog Screen

Configuring SNMP

SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. SNMP is used to capture (trap) log information, but can also be configured to get information as needed and to send configuration changes to a device.

> **NOTE:**   Three versions of SNMP are available: SNMPv1 (legacy), SNMPv2, and SNMPv3. SNMPv3 is the most secure. Use SNMPv2 only if SNMPv3 is not supported.

> **NOTE:**   To send SNMP messages to an SNMP server, SNMPv1 and SNMPv2 use read-only community strings to authenticate with a server. To authenticate configuration changes from an SNMP server, SNMP uses read-write community strings.

> **TIP:**   Change the default names of the read-only and read-write community strings.

Configuring SNMP Using CCP

To enable syslog logging using CCP, choose **Configure > Router > SNMP**. The SNMP informational screen will display, as shown in Figure 6-15.

Figure 6-15   SNMP Information Screen

To configure the settings and enable SNMP, click **Edit**.

The SNMP Properties dialog appears, as shown in Figure 6-16. Enter the syslog server information. You can enable the logging buffer and configure it separately.

Figure 6-16   SNMP Properties Dialog

After configuring these settings, click **OK**. CCP displays the CLI configuration commands shown in Figure 6-17.

Click **Deliver** to commit the configuration changes.

Figure 6-17   Deliver Configuration to Device Summary Window

CCP now displays the configured SNMP properties, as shown in Figure 6-18.

Figure 6-18   Revised SNMP Information Screen

Securing Management Access with AAA

This chapter covers the following topics:

Authenticating Administrative Access

- Local Authentication
- Server-Based Authentication
- Authentication, Authorization, and Accounting Framework

Local AAA Authentication

- Configuring Local AAA Authentication Example
- Configuring Local AAA Authentication Using CCP Example

Server-Based AAA Authentication

- TACACS+ Versus RADIUS
- Configuring Server-Based AAA Authentication
- Configuring Server-Based AAA Authentication Example
- Configuring Server-Based AAA Authentication Using CCP Example

AAA Authorization

- Configuring AAA Authorization Example
- Configuring AAA Authorization Using CCP

AAA Accounting

- Configuring AAA Accounting Example

Cisco Secure ACS

- Adding a Router as a AAA Client
- Configuring Identity Groups and an Identity Store
- Configuring Access Service to Process Requests
- Creating Identity and Authorization Policies

Authenticating Administrative Access

Local Authentication

Administrative access to console, vty, and AUX lines and to HTTP access can be authenticated locally using the following:

Line passwords	Easy to implement using the `password` and `login` commands, but this is the least-secure method and very vulnerable to brute-force attacks. There is also loss of accountability because the password can be shared.
Local authentication	Implemented to improve security because the user must now provide a username and password, which are compared to entries in the local device database.
Self-contained AAA (local AAA)	This method is similar to local authentication but can provide backup methods of authentication.

NOTE   Authenticating locally is not very scalable.

Server-Based Authentication

A more scalable method is to use a server-based solution using one of the following methods:

Cisco Secure Access Control Server (ACS) for Windows Server	The AAA services on the router contact an external Cisco Secure ACS Windows Server for user and administrator authentication.
Cisco Secure Access Control System	The Cisco ACS 5.2 software runs either on a dedicated Cisco 1121 Secure Access Control System (CSACS-1121) appliance, or on a VMware server.
Cisco Identity Services Engine (ISE)	A dedicated appliance that consolidates features of Cisco ACS and Network Admission Control (NAC) to provide AAA, profiling, posture, and guest management. It is a component of the Cisco TrustSec solution and Cisco SecureX Architecture.

Authentication, Authorization, and Accounting Framework

Authentication, authorization, and accounting (AAA) is a standards-based framework that you can implement to control who is permitted to access a network (authenticate), what they can do while they are there (authorize), and audit what actions they performed while accessing the network (accounting).

Local AAA Authentication

The following are the general steps to configure a Cisco router to support local AAA authentication:

1. Add usernames and passwords to the local router database.

2. Enable AAA globally on the router using the `aaa new-model` command.

3. Configure authentication policies using the `aaa authentication` command and specified method lists.

4. (Optional) Configure authorization policies using the `aaa authorization` command and specified method lists.

5. (Optional) Configure accounting policies using the `aaa accounting` command and specified method lists.

6. Confirm and troubleshoot the AAA configuration.

> **NOTE**   Other variations of the `aaa authentication` command include `aaa authentication ppp`, `aaa authentication enable`, and `aaa authentication dot1x`.

> **NOTE**   Other configurable parameters include `aaa authentication banner`, `aaa authentication username-prompt`, `aaa authentication password-prompt`, and `aaa authentication fail-message`.

`Router(config)#username` `username` `privilege` `level` `secret` `password`	Add a username and password to the local security database.
`Router(config)#aaa new-model`	Enable AAA.

Router(config)#**aaa authentication login** {**default** | *list-name*} {*method1* [*method2...*]}	Defines the login authentication method to use when accessing console, vty, and AUX lines. A **default** list applies to all lines; a *list-name* can be defined and applied to specific lines.
	If a *list-name* is defined, the **login authentication** *list-name* command must be applied to the line.
	You can specify up to four methods. The additional methods of authentication are used only if the previous method returns an error, not if it fails.
	Method choices include **local**, **local-case**, and **enable.**
	NOTE Passwords are always case sensitive. The **local-case** method makes the password and username case sensitive.

Optional **aaa authentication** commands include the following::

Router(config)#**aaa authentication username-prompt** *text-string*	Replace the default Username: prompt. If this text string contains spaces, it must be enclosed in double quotes.
Router(config)#**aaa authentication password-prompt** *text-string*	Replace the default Password: prompt. If this text string contains spaces, it must be enclosed in double quotes.
Router(config)#**aaa local authentication attempts max-fail** *number*	Secure AAA user accounts by locking out accounts that have exceeded the maximum number of failed attempts specified.
	Account stays locked until it is cleared by an administrator with the **clear aaa local user lockout** {**username** *username* | **all**} command.

Configuring Local AAA Authentication Example

R1(config)#**username ADMIN privilege 15 secret cisco123**	Create an entry in the local database.
	NOTE Always configure at least one local database entry before enabling AAA.
R1(config)#**aaa new-model**	Enable AAA.

R1(config)#**aaa authentication login** default **local-case**	All lines automatically enforce the default login policy and require case-sensitive username and password access.
R1(config)#**aaa authentication login** VTY-IN **local-case enable**	Command specifies a list called VTY-IN using the **local-case** method, which makes the username and password case sensitive. If no local database has been configured, use the enable password.
R1(config)#**aaa authentication username-prompt "Enter your Username: "**	Replace the default Username: prompt.
R1(config)#**aaa authentication password-prompt "Enter your Password: "**	Replace the default Password: prompt.
R1(config)#**aaa local** authentication **attempts max-fail 8**	Lock out the account after eight failed attempts.
R1(config)#**line console 0**	Enter line console mode.
R1(config-line)#**login authentication** VTY-IN	Applies the VTY-IN list-name to the interface. **TIP** Use **login authentication default** to disable the list-name method.

Configuring Local AAA Authentication Using CCP Example

The first step of configuring local AAA authentication is to enable AAA.

Choose **Configure > Router > AAA > AAA Summary** to open the AAA Summary screen (see Figure 7-1).

Figure 7-1 AAA Summary Screen

Click **Enable AAA**.

The Enable AAA dialog box appears, as shown in Figure 7-2.

Clicking **Yes** enables AAA and automatically configures local authentication on the console line. It also configures the vty lines for local authentication, authorization to use the EXEC shell, and accepts the privilege level of the user (if configured).

> **NOTE**   Clicking **No** does not enable AAA.

Figure 7-2 Enable AAA Dialog Box

Click **Yes**.

Figure 7-3 displays the revised AAA(Enabled) screen.

Figure 7-3   Revised AAA(Enabled) Screen

AAA is now enabled and the revised settings are displayed in the AAA Summary screen. It now states that there is one authentication policy and one authorization policy.

To alter the method list of the default authentication login policy, choose **Configure > Router > AAA > Authentication Policies > Login**. The Authentication Policies Login screen opens, as shown in Figure 7-4.

Figure 7-4   Authentication Policies Login Screen

From this screen, you can add a new method list, edit the selected method list, or simply delete the method list.

NOTE: Click **Edit** to add or remove a method or to change the order of the meth-
ods.

To add a new authentication policy, choose **Add**. The Add a Method List for
Authentication Login dialog appears, as shown in Figure 7-5.

In this example, the new method list name is VTY-IN, and once applied to a line, it will
authenticate the user by requiring a case-sensitive username and password. If a local user
database has no entries, it defaults to the enable password. If no enable password is con-
figured, the user is denied access.

Figure 7-5   Add a Method List for Authentication Login Dialog

NOTE: This creates the command-line interface (CLI) command `aaa`
`authentication login VTY-IN local-case enable.`

Cisco Configuration Professional (CCP) displays the CLI configuration command. Click
Deliver to commit the configuration changes.

To apply VTY-IN, choose **Configure > Router > Router Access > VTY > Edit**. The
Edit VTY Lines dialog will appear (see Figure 7-6).

Figure 7-6   Edit VTY Lines Dialog

> **NOTE:**   This creates the CLI command `login authentication VTY-IN`.

Click **OK**.

CCP displays the CLI configuration command. Click **Deliver** to commit the configuration changes.

Figure 7-7 shows the revised vty lines screen.

Figure 7-7   Revised VTY Lines Screen

Server-Based AAA Authentication

Maintaining a local authentication database for each Cisco device in a large network is not feasible. Large networks require a AAA server-based solution. Routers communicate with AAA servers, which can be installed on a Windows server or on dedicated appliances such as the Cisco 1121 Secure Access Control System (ACS) or the Cisco Identity Services Engine (ISE).

When users connect to a router, they are prompted for a username and password. The router passes the credentials to the Cisco Secure ACS (server or engine). The Cisco Secure ACS authenticates the user.

TACACS+ Versus RADIUS

Routers communicate with AAA servers using either TACACS+ or RADIUS protocols to implement AAA functions:

	TACACS+	RADIUS
Standard	Cisco proprietary	RFCs 2865, 2866, 2867, and 2868
Transport protocol	TCP port 49	UDP ports 1645 or 1812 for authentication and UDP ports 1646 or 1813 for accounting
Confidentiality	Encrypts the entire body of the packet, but leaves a standard TCP header	Encrypts only the password in the Access-Request packet from the client to the server
Functionality	Uses the AAA architecture separating authentication, authorization, and accounting	Combines authentication and authorization
Customization	Provides authorization of router commands on a per-user/group basis	Can pass a privilege level down to the router, which can then be used locally for command authorization
Accounting	Captures limited information	Captures more detailed information
Deployment	Common in Cisco deployments and where multiprotocol support is required	Popular in VoIP installations and to support 802.1x

NOTE: Depending on the solution chosen, the configuration commands differ slightly.

NOTE: RADIUS will eventually be replaced by DIAMETER.

The following are the general steps to configure a Cisco router to support server-based authentication:

1. Configure the AAA servers and groups.

2. Enable AAA globally on the router.

3. Configure authentication policies using the `aaa authentication` command and specified method lists.

4. (Optional) Configure authorization policies using the `aaa authorization` command and specified method lists.

5. (Optional) Configure accounting policies using the `aaa accounting` command and specified method lists.

6. Confirm and troubleshoot the AAA configuration.

Configuring Server-Based AAA Authentication

The first step of configuring server-based authentication is to configure AAA server objects:

`R1(config)#tacacs-server host` `{host-name	host-ip-address}` `[key string] [port [integer]]` `[single-connection] [timeout` `[seconds]]`	Specify a TACACS+ host. Key, port number, single connection, and time-out are all optional. **NOTE:** The encryption key can be configured separately using the `tacacs-server key` command. **TIP:** When connecting to Cisco Secure ACS, use the `single-connection` keyword. It is more efficient because it allows the server to handle a higher number of TACACS operations. The time-out specifies the amount of time that the router waits for the server to reply before retransmitting. Default is 5 seconds.
`R1(config)#radius-server host` `{host-name	host-ip-address}` `[auth-port port-number] [acct-port` `port-number] [key password]`	Specify a RADIUS host. Port numbers and key are optional. **NOTE:** If `auth-port` and `acct-port` are not specified, the default value of `auth-port` is 1645 and the default value of `acct-port` is 1646. **NOTE:** You can configure the encryption key separately using the `radius-server key` command.

Optionally, servers can be grouped together. This feature enables you to select a subset of the configured server hosts and use them for a particular service:

`Router(config)#`**`aaa group server radius`** *`group-name`*	Group existing RADIUS server hosts and use them for a particular service.
`Router(config-sg-radius)#`**`server`** *`ip-address`* [**`auth-port`** *`port-number`*] [**`acct-port`** *`port-number`*]	Configure the IP address of the RADIUS server for the group server.
`Router(config)#`**`aaa group server tacacs+`** *`group-name`*	Group existing TACACS+ server hosts and use them for a particular service.
`Router(config-sg-tacacs+)#`**`server`** *`server-ip`*	Configure the IP address of the TACACS+ server for the group server. **NOTE:** You can use this command repeatedly too add multiple servers to a group.

Finally, configure the login authentication method list to use the identified servers:

`Router(config)#`**`aaa authentication login`** {**`default`** | *`list-name`*} {*`method1`* [*`method2`* ...]}	Defines the default login authentication method to use when accessing lines. Server-based method choices include the following: ■ **`group radius`** ■ **`group tacacs+`** ■ **`group`** *`group-name`* **NOTE:** It is recommended to add the local router database as a fallback method, in case communication to the AAA servers fails.

Configuring Server-Based AAA Authentication Example

The first step of configuring AAA servers is to configure AAA server objects:

`R1(config)#`**`username ADMIN privilege 15 secret cisco123`**	Create an entry in the local database.
`R1(config)#`**`aaa new-model`**	Enable AAA.
`R1(config)#`**`radius-server host 192.168.1.101 auth-port 1812 acct-port 1813 key cisco123`**	Specify a RADIUS server and use UDP port numbers 1812 and 1813 and key cisco123.

R1(config)#**radius-server host 192.168.1.102 auth-port 1812 acct-port 1813 key cisco123**	Specify a RADIUS server and use UDP port numbers 1812 and 1813 and key cisco123.
R1(config)#**aaa group server radius RADIUS-SERVERS**	Create a RADIUS server group.
R1(config-sg-radius)#**server 192.168.1.101**	Add a RADIUS server to the server group.
R1(config-sg-radius)#**server 192.168.1.102**	Add another RADIUS server to the server group.
R1(config)#**tacacs-server host 192.168.1.103 single-connection key cisco123**	Specify a TACACS server and use a single connection and key cisco123.
R1(config)# **aaa authentication login default group RADIUS-SERVERS group tacacs+ local**	By default, all logins are to consult the first server listed in the group RADIUS-SERVERS. If it is not reachable, the second RADIUS server in the RADIUS-SERVERS group is consulted. If it is not reachable, the TACACS+ server is consulted. Finally, if the TACACS+ server is not reachable, the local database is consulted.

Configuring Server-Based AAA Authentication Using CCP Example

The first step of configuring AAA servers is to configure AAA server objects.

Choose **Configure > Router > AAA > AAA Servers and Groups > Servers** to open the AAA Server screen (see Figure 7-8).

Figure 7-8   AAA Servers Screen

Initially, no servers are listed. You can configure global TACACS+ and RADIUS server settings such as timeout, password, and source interface. Otherwise, you can add a server.

To add a server, click **Add**. The Add AAA Server dialogs open (see Figure 7-9).

You may add a RADIUS or a TACACS+ server separately.

Figure 7-9   Add AAA Server Dialogs

NOTE: RADIUS servers allow the definition of custom authorization and accounting ports.

NOTE: The optional server settings (timeout and authentication key) override global settings (if configured).

NOTE: The default timeout is 5 seconds.

In this example, two RADIUS servers and a TACACS+ server were added. Figure 7-10 shows the IP address, server type, and other parameters for each server.

Figure 7-10   Revised Add Servers Screen

Servers can be added to server groups to group AAA servers and provide modularity in high-availability scenarios.

Choose **Configure > Router > AAA > AAA Servers and Groups > Groups** to open the Add AAA Server Groups dialog (Figure 7-11).

Figure 7-11   Add AAA Server Group Dialog

In this example, two RADIUS servers are being added to a group called
RADIUS-SERVERS.

Click **OK**.

CCP displays the CLI configuration command. Click **Deliver** to commit the configura-
tion changes.

Figure 7-12 displays the revised AAA Server Groups screen.

Figure 7-12   Revised AAA Server Groups Screen

To have the AAA authentication refer to a RADIUS and a TACACS+ server, you must
alter the AAA authentication method list.

Choose **Configure > Router > AAA > Authentication Policies > Login** to open
the Authentication Policies Login screen as previously seen in Figure 7-4. From the
Authentication Login dialog, you can add, edit, or delete an existing policy. We will edit
the default policy.

Select **Default** and click **Edit** to open the Edit a Method List for Authentication Login
window (see left hand side of Figure 7-13).

Figure 7-13   Edit a Method List for Authentication Login Window

To add the RADIUS and TACACS+ servers, click **Add**.

The Select Methods List(s) for Authentication Login windows appears as shown in the right hand side of Figure 7-13. You can configure up to four authentication methods. Select the server method to use.

In this example, **group tacacs+** and **group RADIUS-SERVERS** are selected. Click **OK** and the new entries are displayed as shown in the left of Figure 7-14.

Figure 7-14   Revising the Edit a Method List for Authentication Login Window

> **NOTE:**   The order of the method list is important. Select the method and click **Move Up** or **Move Down**, accordingly.

In the example on the right, the ISR will consult with the RADIUS servers identified in the group. For instance, assuming there are two RADIUS servers in the group, the ISR would consult the first server listed to validate the authentication credentials. If it is not reachable, the second RADIUS server in the RADIUS-SERVERS group will be consulted. If it is not reachable, the TACACS+ server will be consulted. Finally, if it the TACACS+ server is not reachable, the local database will be consulted.

Click **OK**. CCP displays the CLI configuration command `aaa authentication login default group RADIUS-SERVERS group tacacs+ local`.

Click **Deliver** to commit the configuration changes.

AAA Authorization

Authorization policies set parameters that restrict administrative EXEC access to the routers or user access to the network.

> **NOTE**   Authorization and accounting rules follow a similar approach using method lists to define the location of the authorization permissions and the accounting logs.

`Router(config)#`**`aaa authorization {exec`** `|` **`network`** `|` **`commands`** `level}` `{`**`default`** `|` `list-name}` `{method1 [method2 ...]}`	Defines the authorization policy to use when accessing lines: ■ **exec** is used to authorize whether the user is allowed to run an EXEC shell. ■ **network** is used to authorize network-related service requests, such as PPP. ■ **command** is used to implement authorization for all commands for a specific privilege level.

Configuring AAA Authorization Example

`R1(config)#`**`aaa authorization exec default group tacacs+`**	EXEC command authorization will be provided by the TACACS+ server.

Configuring AAA Authorization Using CCP

To view the summary of authorization configured on the router, choose **Configure > Router > AAA > Authorization Policies > Authorization Policies**. The Authorization Policies Summary screen opens, as shown in Figure 7-15.

Figure 7-15 Authorization Policies Summary Screen

NOTE You can configure authorization for EXEC mode commands, user network access, and Secure Sockets Layer (SSL) web authentication. This section focuses on the EXEC mode commands.

To add or edit the AAA authorization, choose **Configure > Router > AAA > Authorization Policies > EXEC Command Mode**.

The Exec Authorization screen opens, as shown in Figure 7-16.

Figure 7-16   EXEC Authorization Screen

From here, you can add, edit, or delete the authorization policy.

In this example, you edit the current default authorization policy and add the RADIUS server group and TACACS+ server to the local method.

Click = **Edit** to open the Edit a Method List for Exec Authorization dialog (see Figure 7-17).

Figure 7-17   Edit a Method List for Exec Authorization Dialogs

Initially, the Edit a Method List for Exec Authorization dialog displays only the local method. The figure on the right is the completed method list in the correct order.

Click **OK**. CCP displays the CLI configuration command `aaa authorization exec default group RADIUS-SERVERS group tacacs+ local`.

Click **Deliver** to commit the configuration changes.

Figure 7-18 displays the revised AAA authorization screen.

Figure 7-18   Revised Exec Authorization Screen

AAA Accounting

Cisco Secure ACS serves as a central repository for accounting information, essentially tracking events that occur on the network. This stored information can prove very helpful for management, security audits, capacity planning, and network-usage billing.

Method lists for accounting define the way accounting will be performed and the sequence in which these methods are performed. AAA supports six different types of accounting: network, connection, exec, system, command, and resource:

`Router(config)# aaa accounting {system	network	exec	commands level} {default	list-name} {start-stop	wait-start	stop-only	none} [method1 [method2]]`	Define the accounting method to use for a specific service. It keeps track of requested services for billing or security purposes. ■ **system** tracks system-level events such as reloads. ■ **network** tracks network-related service requests such as PPP. ■ **exec** tracks EXEC shell sessions. ■ **commands** tracks all commands at the specified privilege level.

Configuring AAA Accounting Example

`R1(config)#aaa accounting exec default start-stop group tacacs+`	The router sends a start accounting notice at the beginning of the requested event and a stop accounting notice at the end of the event.

Cisco Secure ACS

Cisco Secure Access Control Server (ACS) 5.3 for Windows provides a centralized identity networking solution and simplified user management experience across all Cisco devices and security management applications.

Before Cisco Secure ACS Version 5, users were made part of a group and used group-based policies. Since ACSv5, rule-based policies are implemented, providing a flexible approach that can match a variety of access conditions.

In Cisco Secure ACS, you can define network device groups (NDG), which are sets of devices. These NDGs provide logical grouping of devices, for example, by device location or type, which you can use in policy conditions.

To configure Cisco Secure ACS for device administration, follow these steps:

1. Add a router as a AAA client.

2. Configure identity groups and an identity store.

3. Configure access service to process requests.

4. Create identity and authorization policies.

Adding a Router as a AAA Client

To add a router as a AAA client, navigate to the Network Resources option on the menu on the left and click the **Network Device Groups** branch.

Figure 7-19 displays an example of adding a switch to a group using the Add Network Devices as AAA Clients screen.

Figure 7-19   Add Router as a AAA Client

Configuring Identity Groups and an Identity Store

In this example, users and groups are stored in the Cisco Secure ACS database. To view, add, edit, or delete users, choose **Users and Identity Stores > Internal Identity Store > Users**.

Figure 7-20 shows an example of the Internal Users screen.

Figure 7-20   Internal Users Screen

Selecting a user and clicking **Edit** opens the Edit a User Account screen (see
Figure 7-21), which displays the specific fields associated with a user.

Figure 7-21   Edit a User Account Screen

Configuring Access Service to Process Requests

Policies consist mainly of rules that determine the action of the policy. You create access
services to define authentication and authorization policies for requests. A global service
selection policy contains rules that determine which access service processes an incom-
ing request.

Access services contain the authentication and authorization policies for requests. You can create separate access services for different use cases (for example, device administration and wireless network access).

When you create an access service, you define the type of policies and policy structures that it contains (for example, policies for device administration or network access).

To create an access policy navigate to **Access Policies > Access Services > Default Device Admin > Identity**.

Creating Identity and Authorization Policies

When you create an access service for network access authorization, it creates a session authorization policy. You can then add and modify rules to this policy to determine the access permissions for the client session.

To manage an authorization policy, navigate to **Access Policies > Access Services > Default Device Admin > Authorization**.

This page intentionally left blank

Securing the Data Plane on Catalyst Switches

This chapter covers the following topics:

Common Threats to the Switching Infrastructure

- Layer 2 Attacks
- Layer 2 Security Guidelines

MAC Address Attacks

- Configuring Port Security
- Fine-Tuning Port Security
- Configuring Optional Port Security Settings
- Configuring Port Security Example

Spanning Tree Protocol Attacks

- STP Enhancement Features
- Configuring STP Enhancement Features
- Configuring STP Enhancements Example

LAN Storm Attacks

- Configuring Storm Control
- Configuring Storm Control Example

VLAN Hopping Attacks

- Mitigating VLAN Attacks
- Mitigating VLAN Attacks Example

Advanced Layer 2 Security Features

- ACLs and Private VLANs
- Cisco Integrated Security Features
- Secure the Switch Management Plane

Common Threats to the Switching Infrastructure

Layer 2 and Layer 3 switches are targets of attack and must be secured. If a Layer 2 switch is compromised, Layers 3–7 are also affected.

Layer 2 Attacks

Layer 2 Attack	Attack Description	Catalyst Switch Mitigation Solution
MAC address attacks	There are two types of attacks: ■ MAC spoofing attacks ■ MAC address table attacks	■ Configure port security.
STP manipulation	Attackers attempt to disrupt STP network by introducing rogue switch.	■ Configure PortFast. ■ Configure BPDU guard. ■ Configure root guard.
LAN storms	Also called broadcast storms and are caused by the following: ■ Protocol stack error ■ Misconfiguration ■ DoS attack	■ Configure storm control.
VLAN attacks	There are two types of attacks: ■ VLAN hopping ■ Double tagging VLAN hopping	■ Disable trunking and DTP on access ports. ■ Explicitly configure trunk ports and change Native VLAN. ■ Secure unused ports.

NOTE: This chapter focuses on the Catalyst switch mitigation solutions.

Layer 2 Security Guidelines

■ Use port security where possible for access ports.

■ Enable STP attack mitigation (PortFast, BPDU guard, and root guard).

■ Set all user ports to nontrunking (unless you are using Cisco VoIP).

■ Disable all unused ports and put them in an unused VLAN.

■ Always use a dedicated native VLAN for trunk ports.

■ Do not use default VLAN 1 for anything.

■ Manage switches in as secure a manner as possible (for example, Secure Shell [SSH], out-of-band [OOB] access, and permit lists).

- Selectively use Simple Network Management Protocol (SNMP) and treat community strings like root passwords.
- Use Cisco Discovery Protocol only where necessary—it is useful with IP phones.

MAC Address Attacks

MAC address table attack	Enables an attacker to sniff frames by overwhelming a switch MAC address table with fake addresses. Once full, the switch floods all unknown unicast frames. The attacker can then capture all traffic or spoof one of the learned MAC addresses.
MAC address spoofing	Attacker spoofs another interface MAC address and sends a gratuitous Address Resolution Protocol (ARP) request to the target switch in an attempt to make it forward frames back to the attacker host.

NOTE: Configure port security to mitigate MAC address attacks.

Configuring Port Security

To configure port security on an access port, follow these steps:

1. Configure an interface as an access port.
2. Enable port security on the port.

`Switch(config-if)#`**`switchport mode access`**	A required step, this sets the interface to access mode (as opposed to trunk mode). **NOTE:** A port cannot be secured while in the default dynamic auto mode.
`Switch(config-if)#`**`switchport port-security`**	Enable port security and assign the current MAC address to the port. Port-security defaults include the following: - Only one MAC address can be assigned. - Port violation action is shut down. **NOTE:** Defaults can be altered if required.

> **NOTE:**   Use the `show port-security` command to view security settings and status and the `show port-security [interface` *interface-id*`]` address command to display all secure MAC addresses configured on all switch interfaces.

When a port violation occurs, such as the maximum number of MAC addresses connected is exceeded, error log messages such as `%PM-4-ERR_DISABLE` and `%PORT_SECURITY-2-PSECURE_VIOLATION` are generated and the port status is changed from `Secure-up` to `Secure-shutdown`. When a port is error-disabled, it is effectively shut down, and no traffic is sent or received on the port. The port is error-disabled and must be manually reset by the network administrator using a `shutdown` and `no shutdown` sequence. This should be done after the offending host has been removed; otherwise, the violation will be triggered again.

Fine-Tuning Port Security

If required, you can alter the default maximum number of secure MAC addresses and the port violation action:

`Switch(config-if)#`**`switchport port-security maximum`** *value*	Set the maximum number of secure MAC addresses for the interface. The default is 1, but the range is 1 to 132. **NOTE:** Configure a maximum value of 2 or 3 when connecting an IP phone and host to a switch port.
`Switch(config-if)#`**`switchport port-security violation {protect | restrict | shutdown | shutdown vlan}`**	Configure the port action when the number of MAC addresses exceeds the defined maximum. Default is `shutdown`. `shutdown` disables the port and generates syslog and SNMP messages. `restrict` drops violating traffic and generates syslog and SNMP messages, while traffic from allowed MAC addresses is permitted to pass normally. `protect` drops violating traffic, while traffic from allowed MAC addresses is permitted to pass normally. `shutdown vlan` drops violating traffic for the offending VLAN instead of shutting down the entire port.

> **TIP:**   Configure `shutdown` rather than `restrict` or `protect`.

NOTE: Instead of manually resetting an error-disabled port using the `shutdown` and `no shutdown` sequence, you can implement a dynamic port auto-recovery solution.

Configuring Optional Port Security Settings

Optionally, you can configure the following port security settings:

- Statically assign the secure MAC addresses to the port or enable the switch to dynamically learn the secure MAC addresses and add them to the running configuration.

- Enable the switch to automatically recover an error-disabled port after a specified amount of time.

- Enable address aging (if required).

MAC addresses can be explicitly assigned to the port manually or learned dynamically:

`Switch(config-if)#`**`switchport`** **`port-security mac-address`** *`mac-address`*	Manually assign the MAC addresses connecting to the port. Repeat the command for each secure MAC address.
`Switch(config-if)#`**`switchport`** **`port-security mac-address sticky`**	Enable the switch to dynamically learn the connected MAC addresses until the maximum is reached. Learned MAC addresses are added to the running configuration.

NOTE: Manually entering each secure MAC address is not a scalable solution.

You can also configure a switch to autorecover error-disabled ports after a specified amount of time:

`Switch(config)#`**`errdisable recovery`** **`cause psecure-violation`**	Enable dynamic error recovery of an error-disabled port. Default is 300 seconds.
`Switch(config)#`**`errdisable recovery`** **`interval`** *`seconds`*	Specify how long a port will remain disabled before it is reenabled.
	TIP: Disconnect the offending host; otherwise, the port will remain disabled, and the violation counter will be incremented.

NOTE: Use the `show errdisable recovery` command to display the error-disabled recovery timer information.

By default, when port security is enabled, the first address is added indefinitely as port aging is disabled. If required, you can enable port aging, making the switch periodically refresh the address:

`Switch(config-if)#`**`switchport port-security`** **`aging {static | time`** *`minutes`* **`| type {absolute |`** **`inactivity}}`**	Remove secure MAC addresses on a secure port without manually deleting the existing address in the startup-config.
	`absolute` (default) removes the address after the specified time. Existing addresses are refreshed or new addresses are added.
	`inactivity` removes the address only if they are inactive for the specified time.

NOTE: You should configure aging only if required. Use the **`no switchport port-security aging static`** interface configuration command to disable aging.

Configuring Port Security Example

Figure 8-1 shows the topology for the configuring port security example.

On the access port:
-Enable port security.
-Set the maximum MAC addresses to 2.
-Set the port violation to shutdown.
-Specify the two MAC addresses.
-Enable automatic recovery after 15 minutes.

Fa0/3

R3   S3   IP

aa-aa-aa-aa-aa-aa   bb-bb-bb-bb-bb-bb

Figure 8-1   Network Topology for the Configuring Port Security Example

`S3(config)#`**`interface fa0/3`**	Enter interface configuration mode.
`S3(config-if)#`**`switchport mode access`**	Configure the port as an access port.
`S3(config-if)#`**`switchport port-security`**	Enable port security allowing only one MAC addresses on the port.
`S3(config-if)#`**`switchport port-security maximum 2`**	Change the maximum number of MAC addresses to 2.

S3(config-if)#**switchport port-security violation shutdown**	If a violation occurs, error-disable the port and generate messages.
S3(config-if)#**switchport port-security mac-address aaaa.aaaa.aaaa**	Manually configure the IP phone MAC address.
S3(config-if)#**switchport port-security mac-address bbbb.bbbb.bbbb**	Manually configure the host MAC address.
S3(config)#**errdisable recovery cause psecure-violation**	Enables dynamic error recovery of an error-disabled port.
S3(config)#**errdisable recovery interval 900**	Change the default time to wait from 300 seconds to 900 seconds.

NOTE: Configure MAC address notification using the global configuration command **mac address-table notification** to generate MAC address learning and aging logging messages.

NOTE: Although only a single port is used in this example, port security is typically enabled on all user-facing ports.

Spanning Tree Protocol Attacks

Redundant Layer 2 topologies eliminate single points of failure, but they are more susceptible to broadcast storms, multiple frame copies, and MAC address table instability problems.

Spanning Tree Protocol (STP) is a Layer 2 protocol that provides a loop-free redundant network topology by placing certain ports in the blocking state. A hacker could manipulate STP to conduct an attack by changing the topology of a network (for example, by connecting a rogue switch in an attempt to take over as the root and have all traffic for the immediate switched domain flow through it).

NOTE: Configure the STP enhancement features PortFast, BPDU guard, and root guard features to mitigate STP manipulation attacks.

STP Enhancement Features

PortFast	- Feature minimizes the time an access port must wait for spanning tree to converge. - The Layer 2 access port immediately transitions from the blocking to the forwarding state, bypassing the listening and learning states. - It should be enabled on user-facing access ports.

BPDU guard	■ Feature protects the switched network from the potential problems caused by the receipt of bridge protocol data units (BPDUs) on user-facing ports.
	■ If a BPDU is received, the port transitions to error-disabled mode and blocks all traffic.
	■ The port must be reset manually and therefore provides a secure response to invalid configurations.
	■ It should be enabled on user-facing access ports to prevent rogue switch installations.
Root guard	■ Feature enforces the placement of root bridges and limits the switch ports out of which the root bridge may be negotiated.
	■ If an incoming BPDU advertises a lower bridge ID than the current bridge, the port transitions to a root-inconsistent state (blocked).
	■ The port recovers as soon as the offending BPDUs cease.
	■ It should be configured on user-facing ports and switch ports that connect to switches (but which should not be the root bridge).

NOTE: Another STP enhancement is the BPDU filter feature, which stops the sending and receiving of BPDUs on a port. However, you should not configure this if BPDU guard is enabled.

NOTE: BPDU guard and root guard are similar, but their impact is different. BPDU guard disables the port, and it must be enabled manually. Root guard disables the port but recovers once the offending device ceases to send superior BPDUs.

Configuring STP Enhancement Features

You can enable PortFast globally or individually on an access port:

`Switch(config)#`**`spanning-tree portfast default`**	Globally enable the PortFast feature on all ports.
	NOTE: You must explicitly disable PortFast on switched ports leading to switches because they may create Layer 2 loops.
`Switch(config-if)#`**`spanning-tree portfast`**	Enable PortFast on the specified port.

NOTE: Use the `show running-config [interface` *interface-id*`]` command to verify that PortFast is enabled.

You can enable BPDU guard globally or individually on an access port:

`Switch(config)#`**`spanning-tree portfast`** **`bpduguard default`**	Globally enable BPDU guard on all PortFast-enabled ports
`Switch(config-if)#`**`spanning-tree bpduguard`** **`enable`**	Enable BPDU guard on the specified port

> **NOTE:** Use the `show spanning-tree summary` and the `show spanning-tree summary totals` commands to display STP state information.

You can enable root guard on either an access port or a switch port that connects to another switch (but which should never be the root bridge).

`Switch(config-if)#`**`spanning-tree guard root`**	Enable root guard on the specified port

> **NOTE:** To verify, use the `show spanning-tree inconsistentports` command.

You can also configure a switch to autorecover BPDU guard error-disabled ports after a specified amount of time:

`Switch(config)#`**`errdisable`** **`recovery cause bpduguard`**	Enable the timer to recover from the BPDU guard error-disabled state

> **NOTE** Use the `show errdisable recovery` command to display the error-disabled recovery timer information.

Configuring STP Enhancements Example

Figure 8-2 shows the topology for the configuring STP enhancements example.

Figure 8-2   Network Topology for the Configuring STP Enhancements Example

`S3(config)#interface Fa0/1`	Enter interface configuration mode.
`S3(config-if)#spanning-tree guard root`	Enable root guard on this port. This prevents anything connected to this port from ever becoming the root.
`S4(config)#interface Fa0/3`	Enter interface configuration mode.
`S4(config-if)#spanning-tree portfast`	Enable PortFast.
`S4(config-if)#spanning-tree bpduguard enable`	Enable BPDU guard on this port.
`S4(config-if)#spanning-tree guard root`	Enable root guard on this port.
`S4(config)#errdisable recovery cause bpduguard`	Enable the timer to recover from the BPDU guard error-disabled state.

LAN Storm Attacks

A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Causes include errors in the protocol stack implementation, mistakes in network configurations, or users issuing a denial-of-service (DoS) attack.

The storm control feature monitors predefined suppression-level thresholds. When the rising threshold is reached, the port is blocked and will only resume normal forwarding when the traffic rate drops below the falling threshold (if configured) or below the rising threshold.

Configuring Storm Control

You can enable storm control globally or individually on an access port:

`Switch(config-if)#`**`storm-control`** `{{`**`broadcast`** `|` **`multicast`** `|` **`unicast`**`}` **`level`** `{`*`level`* `[`*`level-low`*`]` `|` **`bps`** *`bps`* `[`*`bps-low`*`]` `|` **`pps`** *`pps`* `[`*`pps-low`*`]}}` `|` `{`**`action`** `{`**`shutdown`** `|` **`trap`**`}}`	Enable storm control on Layer 2 ports and Etherchannels to monitor the rate of received traffic. Broadcast, multicast, and unicast traffic can be monitored. **`level`** `{`*`level`* `[`*`level-low`*`]` specifies the rising and falling suppression levels as a percentage (to two decimal places) of total bandwidth of the port. **`level bps`** `{`*`bps`* `[`*`bps-low`*`]` specifies the rising and falling levels in bits per seconds. **`level pps`** `{`*`pps`* `[`*`pps-low`*`]` specifies the rising and falling levels in packets per second. The action taken can be ■ **`shutdown`**: Disables the port during the storm ■ **`trap`**: Sends an SNMP trap during a storm

NOTE: By default, unicast, broadcast, and multicast storm control are disabled on the switch interfaces; that is, the suppression level is 100 percent.

Configuring Storm Control Example

This example shows how to enable broadcast address storm control on a port to a level of 25 percent. When the broadcast traffic exceeds 25 percent of the total available bandwidth, the switch drops all broadcast traffic until the end of the traffic storm control interval:

`S1(config-if)#`**`storm-control broadcast level 25`**	Enable storm control on Layer 2 interfaces to monitor the rate of received traffic.

VLAN Hopping Attacks

Spoofing DTP messages	Attacker sends spoofed Dynamic Trunking Protocol (DTP) messages in an attempt to establish a trunk link with the switch. If successful, the attacker can send traffic tagged with the target VLAN and have the switch deliver the packets to the destination.

Attach a rogue switch	Attacker connects an unsanctioned rogue switch and attempts to enable trunking with the target switch. If successful, the attacker can then access all the VLANs on the victim switch from the rogue switch.
Double-tagging (double-encapsulated) VLAN hopping attack	Attacker embeds a hidden 802.1Q tag inside the already tagged 802.1Q frame. If successful, the frame can go to a VLAN that the original 802.1Q tag did not specify.

Mitigating VLAN Attacks

On the trunk links, explicitly enable trunking and disable DTP:

`Switch(config-if)#`**`switchport mode trunk`**	Explicitly enable trunking on the link.
`Switch(config-if)#`**`switchport nonegotiate`**	Disable DTP and prevent DTP frames from being generated.

On the trunk links, switch the native VLAN to a dedicated VLAN:

`Switch(config-if)#`**`switchport trunk native vlan`** *`vlan`*	Change the native VLAN to a dedicated VLAN with no other traffic on it

On the nontrunk links, disable trunking:

`Switch(config-if)#`**`switchport mode access`**	Configures port as an access port. This also disables trunking on the interface.

Assign all unused ports to a dedicated unused VLAN and disable the ports:

`Switch(config-if)#`**`switchport mode access`**	Configures port as an access port. This also disables trunking on the interface.
`Switch(config-if)#`**`switchport access vlan`** *`vlan`*	Assign the port to an unused VLAN.
`Switch(config-if)#`**`shutdown`**	Disable the port.

Mitigating VLAN Attacks Example

Figure 8-3 shows the topology for the mitigating VLAN attacks example.

Root bridge

Figure 8-3   Network Topology for the Mitigating VLAN Attacks Example

`S3(config)#interface range Fa0/1 - 2`	Configure the two trunking ports, Fa0/1 and Fa0/2.
`S3(config-range-if)#switchport mode trunk`	Explicitly enable trunking.
`S3(config-range-if)#switchport nonegotiate`	Disable DTP.
`S3(config-range-if)#switchport trunk native vlan 88`	Assign the native VLAN to VLAN 88. VLAN 88 is not used for any other traffic.
`S3(config-range-if)#interface Fa0/3`	Change to interface Fa0/3.
`S3(config-if)#switchport mode access`	Disable trunking.
`S3(config)#interface range Fa0/4 - 24`	Configure all other unused ports.
`S3(config-range-if)#switchport mode access`	Disable trunking on all unused ports.
`S3(config-range-if)#shutdown`	Disable all unused ports.

Advanced Layer 2 Security Features

Additional switch security features include the following:

- Access control lists (ACLs) and private VLANs
- Cisco integrated security features
- Secure management plane security features

NOTE: Configuration of these features is beyond the scope of this book.

ACLs and Private VLANs

Port-based ACLs for Layer 2 ports	You can apply security policies on individual switch ports.
Private VLANs	Private VLANs restrict traffic between hosts in a common segment by segregating traffic at Layer 2, turning a broadcast segment into a nonbroadcast multiaccess-like segment.
Private VLAN edge	Private VLAN edge provides security and isolation between switch ports, which helps ensure that users cannot snoop on other users' traffic.

Cisco Integrated Security Features

Cisco integrated security features are easy-to-use tools to effectively prevent potentially damaging Layer 2 security threats. Features include the previously covered port security and DHCP snooping, dynamic ARP inspection, and IP source guard.

DHCP snooping	Prevents malicious users from spoofing a Dynamic Host Configuration Protocol (DHCP) server and sending out bogus addresses. This feature is used by other primary security features to prevent a number of other attacks, such as ARP poisoning.
Dynamic ARP inspection	Dynamic ARP inspection (DAI) helps ensure user integrity by preventing malicious users from exploiting the unsecure nature of the ARP protocol.
IP source guard	IP source guard prevents a malicious user from spoofing or taking over another user's IP address. It does so by creating a binding table between the client's IP and MAC address, port, and VLAN.

Secure the Switch Management Plane

Just as the management plane is secured on Cisco routers, the Layer 2 switching man-

agement plane must also be secured. You can use many of the same tools to secure the management plane on Catalyst switches.

Secure management plane tools include (but are not limited to) the following:

Secure management protocols	SSH and SNMPv3 provide network security by encrypting administrator traffic during SSH and SNMP sessions.
SPAN support	Bidirectional data support on the Switched Port Analyzer (SPAN) port allows Cisco Intrusion Detection System (IDS) to take action when an intruder is detected.
AAA	TACACS+ and RADIUS authentication facilitates centralized control of the switch and restricts unauthorized users from altering the configuration.
RBAC	With role-based access control (RBAC), multilevel security on console access prevents unauthorized users from altering the switch configuration.
MAC notifications	MAC address notification allows administrators to be notified of users added to or removed from the network.
Multidomain authentication	This feature allows an IP phone and a PC to authenticate on the same switch port while placing them on appropriate voice and data VLANs.

This page intentionally left blank

Securing the Data Plane in IPv6 Environments

This chapter covers the following topics:

Overview of IPv6

- Comparison Between IPv4 and IPv6
- The IPv6 Header
- ICMPv6
- Stateless Autoconfiguration
- IPv4-to-IPv6 Transition Solutions
- IPv6 Routing Solutions

IPv6 Threats

- IPv6 Vulnerabilities

IPv6 Security Strategy

- Configuring Ingress Filtering
- Secure Transition Mechanisms
- Future Security Enhancements

Overview of IPv6

Comparison Between IPv4 and IPv6

IP Service	IPv4	IPv6
IP header	Consists of a 20-byte field containing multiple fields.	Consists of a 40-byte field containing fewer fields, making it simpler, and provides better routing efficiency.
Addressing range	Requires a 32-bit dotted-decimal address to provide 4.3×10^9 (4.3 billion) addresses.	Requires a 128-bit hexadecimal address to provide 3.4×10^{28} addresses with multiple scopes.
Address types	Includes unicast, multicast, and broadcast addresses.	Includes unicast, multicast, and anycast addresses. No broadcast addresses means that it is not susceptible to broadcast storms.

IP Service	IPv4	IPv6
Autoconfiguration	Supports stateful configuration (Dynamic Host Configuration Protocol, DHCP).	Supports stateless autoconfiguration or stateful configuration (DHCPv6).
Security	IPsec must be configured.	IPsec is a mandatory part of the stack, but it still has to be configured.
Mobility	Mobility is not built in, but it supports mobile IP.	Mobile IP is built in, with optimized routing.
Quality of service (QoS)	Supports differentiated service and integrated service.	Supports differentiated service and integrated service, but the header compresses better because of fewer fields.
IP multicast	Heavy application use.	Heavy application and protocol stack use.
ICMP	Mostly used to provide messaging information.	Used extensively to provide messaging and protocol functions.

The IPv6 Header

The IPv6 header is twice as big as the IPv4 header (40 bytes versus 20 bytes). However, IPv6 has fewer fields and is simpler, as shown in Figure 9-1.

Figure 9-1   IPv4 Versus IPv6 Header

Some IPv4 fields no longer exist in IPv6, although three of these IPv4 fields have kept the same name and are identical in nature. Four fields have had their name and position changed but serve a similar function to IPv4. There is also a new QoS field in IPv6.

Like the IPv4 Protocol field, the IPv6 Next Header identifies the extension header and is not of fixed length. It can contain additional information such as a hop-by-hop list of destinations, routing header (RH), IPsec information, and more. All extension headers are daisy-chained, each header pointing to the next header until they reach the transport layer data. This arrangement allows an IPv6 packet to be customized with features and functionality (for example, TCP, UDP, ICMPv6).

> **NOTE**   Attackers can use these extension headers for malicious purposes.

ICMPv6

Internet Control Message Protocol (ICMP) has a greater role in IPv6.

ICMP Message Type	ICMPv4	ICMPv6
Connectivity checks	✓	✓
Information/error messaging	✓	✓
Fragmentation needed notification	✓	✓
Address assignment		✓
Address resolution		✓
Router discovery		✓
Multicast group management		✓
Mobile IPv6 support		✓

ICMPv6 is used for neighbor and router discovery.

ICMPv6 Message	Type	Description
Neighbor solicitation (NS)	135	Similar to the IPv4 Address Resolution Protocol (ARP), it is sent by a host to determine the link-layer address of a neighbor. Used to verify that a neighbor is still reachable. An NS is also used for duplicate address detection (DAD).
Neighbor advertisement (NA)	136	A response to an NS message. A node may also send unsolicited an NA to announce a link-layer address change.
Router advertisement (RA)	134	RAs contain prefixes that are used for address configuration including a hop limit value, maximum transmission unit (MTU) value, and so on. RAs are sent either periodically or in response to an RS message.
Router solicitation (RS)	133	When a host is booting, it sends out an RS requesting routers to immediately generate an RA rather than wait for their next scheduled time.

NOTE: Attackers may manipulate ICMPv6 for malicious purposes.

Stateless Autoconfiguration

Stateless autoconfiguration enables plug-and-play configuration of an IPv6 device without the use of a server. It uses the Neighbor Discovery Protocol (NDP), which is based on ICMP Version 6 (ICMPv6) protocol messaging. NDP uses the ICMPv6 RS and RA messages.

NOTE: NDP replaces ARP and suffers from the same lack of authentication as ARP and DHCP on IPv4 networks.

IPv4-to-IPv6 Transition Solutions

Many transition mechanisms enable smooth integration of IPv4 and IPv6. Other mechanisms that allow IPv4 nodes to communicate with IPv6 nodes are available. All these mechanisms are applied to different situations.

The three most common techniques to transition from IPv4 to IPv6 are as follows:

Dual stack	A host is configured with an IPv4 and IPv6 network address. As a result, the node and its corresponding routers have two protocol stacks.
Tunneling	**Manual IPv6-over-IPv4 tunneling** is an integration method in which an IPv6 packet is encapsulated within the IPv4 protocol. This method requires dual-stack routers.
	Dynamic 6to4 tunneling is a method that automatically establishes the connection of IPv6 islands through an IPv4 network.
	Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunneling is an automatic overlay tunneling mechanism that uses the underlying IPv4 network as a data link layer for IPv6.
	Teredo tunneling is an IPv6 transition technology that provides host-to-host automatic tunneling instead of gateway tunneling.
Proxying and translation (NAT-PT)	This translation mechanism sits between an IPv6 network and an IPv4 network. The job of the translator is to translate IPv6 packets into IPv4 packets and vice versa.

IPv6 Routing Solutions

IPv6 supports static routes, Routing Information Protocol next generation (RIPng), Open Shortest Path First Version 3 (OSPFv3) Protocol, Intermediate System-to-Intermediate System Protocol (IS-IS) for IPv6, Multiprotocol Border Gateway Protocol Version 4 (MP-BGP4), and Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6. You must configure the **ipv6 unicast-routing** before an IPv6-capable routing protocol or an IPv6 static route will work.

NOTE: Neighbor routers are identified by their next-hop link-local addresses and therefore do not use global unicast addresses.

IPv6 Threats

IPv6 is no more or less secure than IPv4. Many similarities exist between them, and therefore they share similar threats, including the following:

- Attacks against the physical or data link layers
- Attacks against routers and other networking devices
- Application layer attacks
- Denial-of-service (DoS) attacks using IPv6-specific attack tools such as 6tunneldos or 4to6ddos
- Reconnaissance attacks
- Sniffing or eavesdropping using IPv6 tools such as Snort, TCPdump, or Wireshark
- Unauthorized access
- Spoofed packets (that is, forged addresses and fields using Scapy6, sendIP, Packit, or Spak6)
- Man-in-the-middle attacks

Other slightly modified IPv6 threats include the following:

- LAN-based attacks against NDP
- Attacks against DHCP or DHCPv6
- DoS attacks against routers (for example, hop-by-hop extension headers)
- Fragmentation (IPv4 routers performing fragmentation versus IPv6 hosts using a fragment extension header)
- Packet amplification attacks (IPv4 uses broadcast; IPv6 uses multicast.)

Threats that are unique to IPv6 include the following:

- Reconnaissance attacks, although more difficult but possible using IPv6 tools such as Parasit6, Fakeroute6, or Scapy6
- Attacks against ICMPv6
- Extension header (EH) attacks
- Autoconfiguration attacks
- Attacks on transition mechanisms
- Mobile IP attacks
- IPv6 protocol stack attacks

NOTE: IPv6 is a relatively new protocol and therefore is subject to bugs in the stack.

IPv6 Vulnerabilities

New vulnerabilities for IPv6 include the following:

Reliance on multicast and ICMPv6	■ Multicasting facilitates reconnaissance. (For example, FF02::1 is all hosts, FF02::2 is all routers.) ■ ICMPv6 is a vehicle for autoconfiguration, subject to spoofing and multiple exploits.
Header extensions	■ Hosts process routing headers (RHs), which can be exploited (for example, routing header for source routing and reconnaissance). ■ There already exist RH-based amplification attacks.
Tunneling	■ Encapsulating IPv6 over IPv4 bypasses firewalls and other inspection systems not ready for IPv6. ■ Most IPv4/IPv6 transition mechanisms have no authentication built in. ■ Dual stack is typically automatically enabled on hosts.
DoS amplification attacks	■ Routing loops are created to consume resources or amplify the packets that are sent to a victim such as when an attacker creates a feedback loop between two routers by spoofing a packet with the RH containing multiple A to B statements. ■ NDP can be used to amplify a network scan by sending NS messages to all the hosts in the LAN segment, using the FF02 multicast address.
Pivoting attacks	■ Combines multiple previously mentioned techniques.

IPv6 Security Strategy

IPv6 is mostly IPv4 with larger addresses, and no significant difference exists between IPv4 and IPv6 with respect to security. In some cases, IPv6 is slightly more secure, and in other cases IPv6 is slightly less secure. Security techniques and devices do exist to enforce a security policy for the IPv6 traffic and should be used.

The lack of IPv6 training for network and security staff is probably the biggest threat for operation.

Configuring Ingress Filtering

Deny bogon addresses	Filter bogon addresses because they are commonly found as the source addresses of distributed DoS (DDoS) attacks. The term *bogon addresses* refers to traffic with a source IP address from a reserved IP address space, and it should be filtered by an Internet service provider.
MAC address table attack	Filter multicast packets at your perimeter based on their scope.

Filter incoming traffic	Only receive packets that have a destination address within your allocated block from an Internet service provider and multicast group address or link-local address for NDP.
Filter ICMPv6 messages	Granularly filter ICMPv6 messages at the perimeter. (Remember, ICMPv6 is needed for protocol operations such as NDP.)
Drop packets with unknown extension headers	Drop RH0 packets and unknown extension headers at the perimeter and throughout the interior of the network.

Secure Transition Mechanisms

Secure dual stack	Prefer dual stack as the transition mechanism, but secure IPv4 and IPv6 equally.
Implement IPsec VPN tunnels	When tunnels are used to send sensitive traffic over a public network, they should be secured by adding IPsec authentication and confidentiality that can prevent both the injection/sniffing attacks and unauthorized access.
Do not allow tunnels through perimeter unless required	Terminate tunnels at the edge and do not permit host-to-host tunnels.

Future Security Enhancements

Consider current and future security enhancements:

Secure Neighbor Discovery (SeND)	Combines NDP with crypto features. The SeND protocol enhances NDP with address ownership proof, message protection, and router authorization.
RA-Guard	RA-Guard blocks router advertisement and router redirect ICMP packets from Layer 2 ports.

NOTE: IPv6 security will now be included in other chapters.

This page intentionally left blank

Planning a Threat Control Strategy

This chapter covers the following topics:

Threats

- Trends in Information Security Threats

Threat Control Guidelines

- Threat Control Design Guidelines

Integrated Threat Control Strategy

- Cisco Security Intelligence Operations

Threats

The time from knowledge of a vulnerability to the release of an exploit has decreased. Some exploits are designed to have global impact within minutes. Some exploits are also persistent and are difficult to eradicate.

Trends in Information Security Threats

Motivation	The attack motivation is no longer for fame and notoriety. Motivation now includes insidious reasons such as for political and financial reasons aimed at economic espionage and money-making activities.
Targeted	Attacks are now targeted with mutating and stealth features.
Application layer	Threats are consistently focusing on the application layer such as known web browser vulnerabilities and looking for new web programming errors.
Social engineering	Users are the weakest link, and social engineering sites are a huge source of information. Increasingly, attackers are not only trying to steal an identity, but also trying to assume the identity of the user.
Borderless	Attackers are also targeting mobile platforms because data is in more places. You must now protect the device, protect the network, and protect the cloud.

Threat Control Guidelines

General threat control guidelines include the following:

- Policies and processes must change from a reactive process to a formal proactive process.

- Mitigation technologies must be able to react to attacks with little or no human intervention.

- End users must be made aware of threats and involved in mitigating them.

Threat Control Design Guidelines

Formalize the process	- Use a layered security approach. - Consider risk management concepts. - Apply policies for both the outside and inside networks. - Maintain logging and monitoring functions.
Distributed security intelligence	- Sensors should be embedded in network elements, operating systems, and applications. - The network of sensors needs to be integrated and provide relevant and actionable dynamic security information. - To provide a greater threat coverage, accuracy, and proactive protection, sensors in the field feed a central location that distributes the information to other sensors.
Security intelligence analysis	- Security intelligence management (that is, event management and incident management) requires a central approach to analysis and correlation. - Include correlation with third parties and external sources. - This analysis should result in relevant threat information that should be automatically distributed to security devices and controls in a timely manner.
Incident response	Incident response should be automated and dynamic, providing the end user the means to respond and mitigate.
Application layer visibility	- Application layer inspection is critical. - Authenticate users and devices. - Monitor and filter application data. - Provide detailed logging.

Integrated Threat Control Strategy

Application awareness	Implement application inspection mechanisms, such as the following: ■ Application Inspection and Control (AIC) ■ Modular Policy Framework (MPF) ■ Network-Based Application Recognition (NBAR) ■ Flexible Packet Matching (FPM)
Application-specific gateways	Implement gateways geared toward the inspection and analysis of specific application traffic, including the following: ■ Cisco IronPort web and email security appliances ■ ScanSafe web security technologies
Integrated threat control and containment	Provide a multidimensional approach to detecting, mitigating, and responding to threats using integrated deployment options, including the following: ■ Integrated Services Routers (ISRs) ■ Cisco Adaptive Security Appliances (ASAs) ■ Intrusion prevention system (IPS) sensors
Cisco Security Appliances	Provide a firewalling service available in various form factors, including the following: ■ Cisco IOS routers ■ Cisco ASA ■ Network modules added to the Catalyst 6500 switch
Cisco IPS	Provide a threat control mechanism available in various form factors, including the following: ■ Cisco IOS IPS (limited version) ■ A dedicated appliance (Cisco 4200) ■ Cisco ASA 5500 series, ISR G2s, and network modules added to the Catalyst 6500
Security management	Provide a comprehensive approach to event management using security management tools such as the following: ■ Cisco Configuration Professional (CCP) ■ Cisco IPS Device Manager (IDM) ■ Cisco Security Manager (CSM)

Cisco Security Intelligence Operations

Global correlation can be accomplished using the Cisco Security Intelligence Operations (SIO) Center, which baselines the current global state of threats such as malware outbreaks, current vulnerabilities, and zero-day attacks. It provides the network system with valuable information to detect, prevent, and react to threats by correlating threat information from the SensorBase. It then feeds this information to enforcement elements for live threat prevention.

Configuring ACLs for Threat Mitigation

This chapter covers the following topics:

Access Control Lists

- Mitigating Threats Using ACLs
- ACL Design Guidelines
- ACL Operation

Configuring ACLs

- ACL Configuration Guidelines
- Filtering with Numbered Extended ACLs
- Configuring a Numbered Extended ACL Example
- Filtering with Named Extended ACLs
- Configuring a Named Extended ACL Example
- Configuring an Extended ACL Using CCP Example

Enhancing ACL Protection with Object Groups

- Network Object Groups
- Service Object Groups
- Using Object Groups in Extended ACLs
- Configuring Object Groups in ACLs Example
- Configuring Object Groups in ACLs Using CCP Example

ACLs in IPv6

- Mitigating IPv6 Attacks Using ACLs
- IPv6 ACLs Implicit Entries
- Filtering with IPv6 ACLs
- Configuring an IPv6 ACL Example

Access Control List

Access control lists (ACLs) provide packet filtering for routers and firewalls to protect internal networks from the outside world and to filter traffic leaving the inside network.

ACL criteria could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information.

CAUTION: Hackers can sometimes successfully evade basic ACLs.

Mitigating Threats Using ACLs

You can use ACLs to mitigate multiple threats, including the following:

- IP address spoofing (inbound and outbound)
- Denial-of-service (DoS) TCP SYN attacks by blocking external attacks
- DoS TCP SYN attacks using TCP intercepts
- DoS smurf attacks
- Filtering Internet Control Message Protocol (ICMP) messages (inbound, outbound, and traceroute)
- Securing vty access

NOTE: This chapter focuses on using ACLs for threat-mitigation purposes.

ACL Design Guidelines

- Base the ACL on the security policy.
- Write out what the ACL is required to do and consider potential problems it may cause.
- Build a library of common ACLs.
- Test the ACL in a lab environment and then apply it to the production network.

ACL Operation

ACL statements operate in a sequential, logical order and evaluate packets from the top down, one statement at a time:

- If a packet header and an ACL statement match, the rest of the statements in the list are skipped and the packet is permitted or denied as determined by the matched statement.
- If a packet header does not match an ACL statement, the packet is tested against the next statement in the list.
- This matching process continues until the end of the list is reached.
- A final implied statement matches all other packets and results in a deny instruction.

NOTE: Each statement in an ACL is referred to as an access control entry (ACE).

ACLs operate in two directions:

Inbound ACLs	Incoming packets are processed before they are routed to an outbound interface.
Outbound ACLs	Incoming packets are routed to the outbound interface, and then they are processed through the outbound ACL.

> **NOTE:**   Inbound ACLs are usually more efficient because they do not perform routing lookups on denied packets. Only permitted packets are processed for routing.

Routers support two types of ACLs:

Standard ACL	- Filters IP packets based on source address only. - ACLs can be numbered or named. - Valid number ranges include 1–99 and 1300–1999.
Extended ACL	- Filters IP packets based on protocol, source and destination addresses, source and destination UDP and TCP ports, and ICMP and Internet Group Management Protocol (IGMP) message types. - ACLs can be numbered or named. - Valid number ranges include 100–199 and 2000–2699.

> **NOTE:**   Numbered ACLs are configured using the `access-list` global configuration command. You cannot edit numbered ACLs using this command. New ACL entries are appended to the end of the ACL.

Standard and extended ACLs can be named. Named ACLs are useful because they provide a hint as to the purpose of the ACL. Names can be alphanumeric but must begin with an alphabetic character. In addition, names cannot contain spaces or punctuation.

> **NOTE:**   Named ACLs are configured using the `ip access-list` global configuration command.

> **TIP:**   Use uppercase letters to make the named ACL stand out in the configuration.

> **TIP:**   You can edit numbered and named ACLs using the `ip access-list` command.

Configuring ACLs

ACL Configuration Guidelines

Three Ps	■ Only one ACL per interface, per protocol (Layer 3), per direction can be configured.
Directional filtering	■ Consider the direction flow of data before creating an ACL.
Order of ACL statements	■ Place the more specific ACE statements at the beginning and generic ACE statements near the end.
Implicit deny	■ Every ACL has a hidden deny all ACE at the end of it. ■ There must be at least one permit ACE; otherwise, all traffic will be denied.
Standard ACL limitation	■ Can only filter by source address. ■ Whenever possible, use an extended ACL instead.
Standard ACL placement	■ Typically place standard ACLs as close to the destination as possible.
Extended ACL placement	■ Typically place extended ACLs as close to the source being filtered.
ACLs are stateless	■ Consider deploying zoned-based policy firewall (ZFW) instead.
Modifying numbered ACLs	■ You can modify numbered ACLs by using the `ip access-list` command.
Router-generated packets	■ Router-generated packets are not subject to ACL filtering on the router generating the packet.

NOTE: This section focuses on extended ACLs.

Filtering with Numbered Extended ACLs

`Router(config)#`**`access-list`** *`access-`* *`list-number`* {**`permit`** | **`deny`**} *`protocol`* *`source source-wildcard`* [*`operator port`*] *`destination destination-wildcard`* [*`operator port`*] [**`established`**] [**`log`**]	Define an extended ACL. Valid numbers are between 100–199 and 2000–2699. **NOTE:** Parameters will vary depending on the protocol of ACL being configured.
`Router(config)#`**`interface`** *`type number`*	Specify the interface type and number and enter interface configuration mode.
`Router(config-if)#`**`ip access-group`** *`access-list-number`* {**`in`** | **`out`**}	Apply the specified extended access list to the interface.

Configuring a Numbered Extended ACL Example

Figure 11-1 displays the network topology for the numbered extended ACL example.

Figure 11-1   Network Topology for Numbered Extended ACL Example

`R1(config)#`**`access-list 100`**	Define extended ACL 100.
`R1(config)#`**`access-list 100 remark Basic`** **`anti-spoofing ACL`**	Document the purpose of the ACL.
`R1(config)#`**`access-list 100 deny ip`** **`209.165.200.224 0.0.0.31 any`**	Deny incoming traffic with the source address the same as the internal subnet.
`R1(config)#`**`access-list 100 permit ip`** **`any host 209.165.200.254 eq 80`**	Permit HTTP web traffic to reach the server.
`R1(config)#`**`interface serial 0/0/0`**	Enter interface configuration mode for the serial interface.
`R1(config-if)#`**`ip access-group 100 in`**	Apply ACL 100 incoming on the outside serial interface.

Filtering with Named Extended ACLs

`Router(config)#`**`ip access-list extended`** {`access-list-number` | `access-list-name`}	Define a named ACL. The command can also be used to edit a numbered ACL.
`Router(config-ext-nacl)#`**`permit`** `protocol` `source source-wildcard` [`operator port`] `destination destination-wildcard` [`operator port`] [**`established`**] [**`log`**]	Define the **`permit`** statement.
`Router(config-ext-nacl)#`**`deny`** `protocol` `source source-wildcard` [`operator port`] `destination destination-wildcard` [`operator port`] [**`log`**]	Define the **`deny`** statement. **NOTE** Parameters will vary depending on the ACL protocol being configured.
`Router(config)#`**`interface`** `type number`	Specify the interface type and number and enter interface configuration mode.
`Router(config-if)#`**`ip access-group`** `access-list-name` {**`in`** | **`out`**}	Apply the specified ACL to the interface.

Configuring a Named Extended ACL Example

`R1(config)#`**`ip access-list extended`** **`ACL-IN`**	Define an extended ACL named ACL-IN.
`R1(config-ext-nacl)#`**`remark Basic`** **`anti-spoofing ACL`**	Document the ACL.
`R1(config-ext-nacl)#`**`permit ip`** **`209.165.200.224 0.0.0.31 any eq 80`**	Permit HTTP web traffic to reach the server.
`R1(config-ext-nacl)#`**`permit ip any`** **`host 209.165.200.254`**	Permit traffic to reach the server.
`R1(config-ext-nacl)#`**`interface serial`** **`0/0/0`**	Apply ACL-IN to the serial interface.
`R1(config-if)#`**`ip access-group`** **`ACL-IN in`**	Apply the ACL incoming on the outside interface.

NOTE: To verify the ACLs, use the `show access-lists`, `show ip access-lists`, and `show ip interfaces` commands.

TIP: Append the `log` keyword at the end of an ACE to generate a system message (106100) every time a flow meets the ACE criteria. Display the number of hits using the `show access-lists` or `show ip access-lists` command.

Configuring an Extended ACL Using CCP Example

In Cisco Configuration Professional (CCP), rules define how the router will respond to a particular kind of traffic. There are various types of rules, such as access rules, Network Address Translation (NAT) rules, IPsec rules, default rules, external rules, and rules with syntax that CCP does not support, called unsupported rules. ACLs are used to help define and enforce rules.

ACLs can be used to classify traffic. This chapter focuses on ACLs applied to interfaces for filtering purposes.

Use the ACL Editor screen to create, edit, or delete rules.

Choose **Configure > Router > ACL > ACL Editor** to display the ACL Editor screen shown in Figure 11-2.

Figure 11-2   ACL Editor Screen

The ACL Editor is most commonly used to define the traffic that you want to permit or deny entry to your LAN or exit from your LAN. The upper portion of the screen lists the access rules that have been configured on this router. The lower portion of the window lists the rule entries associated with the selected rule. A rule entry consists of criteria that incoming or outgoing traffic is compared against and the action to take on traffic matching the criteria. If traffic does not match the criteria of any of the entries in this box, it is dropped.

To add a new access rule, click **Add**.

The Add a Rule dialog appears, as shown on the left side in Figure 11-3.

Figure 11-3   Add a Rule Dialogs

From this window, you can define a standard or extended ACL, provide a brief description, define the rule entry, and associate the rule with an interface.

To add a rule entry, click **Add**.

The Add an Extended Rule Entry dialog appears, as shown on the right side of Figure 11-3. From this window, you can define specifics of the ACE, such as the action to perform the source and destination host/subnet, the protocol to filter, and whether to log entries.

Complete the access rule requirements, and then click on **OK** to return to the Add a Rule window shown on the left side of Figure 11-4.

The configured rule entry now appears in the Rule Entry window. Keep adding rule entries until the access rule policy is complete.

> **NOTE:**   An access rule should have at least one `permit` statement.

After configuring all ACEs, define the interface to which to apply this new rule.

Click **Associate** and the Associate with an Interface dialog appears, as shown on the right side of Figure 11-4.

Figure 11-4   Associate with an Interface Window

Select the interface, specify the direction, and click **OK** to return to the Add a Rule dialog.

> **NOTE:**   If another rule is already associated with the interface, an information box appears. Either cancel the operation or continue by appending the rule entries to the rule that is already applied to the interface.

Review the rule, and when done, click **OK**.

CCP displays the command-line interface (CLI) configuration commands. Click **Deliver** to commit the configuration changes.

The Access Rules information screen displays the newly created rule.

> **NOTE:**   Multiple rules can appear in this screen. Select the rule to view the specifics associated to it.

> **NOTE:**   To view log entries, click **Monitor > Security > Firewall Status**.

Enhancing ACL Protection with Object Groups

Object grouping is used to bundle addresses and services inside of ACLs. ACEs can then refer to the object group instead of having to enter an ACE for each object. Object groups provide a simple and intuitive mechanism for configuring and managing large ACLs that frequently change. It also reduces ACL configuration size and makes ACLs easier to manage. Cisco IOS routers support network and service object groups.

Network Object Groups

A network object group is a group of any of the following objects:

- Hostnames, IP addresses, or subnets
- Ranges of IP addresses
- Existing network object groups

`Router(config)#`**`object-group network`** `nw_grp_id`	Create a network object group.
`Router(config-network-group)#`**`description`** *`description-text`* | **`host`** {*`host-address`* | *`host-name`*} | *`network-address`* {**`/nn`** | *`network-mask`*} | **`range`** *`host-address1 host-address2`* | **`any`** | **`group-object`** *`nested-object-group-name`*	From network object configuration mode, define the specifics of the network object. **NOTE** Options are optional.

Here is a command syntax breakdown of the `object-group network` options:

`Router(config-network-group)#`**`description`** *`description-text`*	Add a description up to 200 characters.
`Router(config-network-group)#`**`host`** {*`host-address`* | *`host-name`*}	Identify a host IP address or name of the host.
`Router(config-network-group)#`*`network-address`* {**`/nn`** | *`network-mask`*}	Identify a subnet object. The default network mask is /32.
`Router(config-network-group)#`**`range`** *`host-address1 host-address2`*	Identify a range of host IP addresses.
`Router(config-network-group)#`**`any`**	Identify any host IP address in the range 0.0.0.0–255.255.255.255.
`Router(config-network-group)#`**`group-object`** *`nested-object-group-name`*	Specify a nested (child) object group to be included in the current (parent) object group.

Service Object Groups

A service object group is a group of any of the following objects:

- Top-level protocols (such as TCP, UDP, or ESP)

- Source and destination protocol ports (such as Telnet or SNMP)
- ICMP types (such as echo, echo-reply, or host-unreachable)
- Existing service object groups

`Router(config)#`**`object-group service`** `svr_grp_id`	Create a service object group.
`Router(config-service-group)#`**`description`** *`description-text`* `|` *`protocol`* `{`*`protocol-number`* `|` *`protocol`*`}` `|` `[`**`tcp`** `|` **`udp`** `|` **`tcp`**-`udp` `[`**`source`** `{{`**`eq`**`]` `|` **`lt`** `|` **`gt`**`}` *`port1`* `|` **`range`** *`port1 port2`*`}]` `[{[`**`eq`**`]` `|` **`lt`** `|` **`gt`**`}` *`port1`* `|` **`range`** *`port1 port2`*`}]]` `|` **`icmp`** *`icmp-type`* `|` **`group-object`** *`nested-object-group-name`*	From service object configuration mode, define the specifics of the service object. **NOTE** Options are optional.

Here is a command syntax breakdown of the **`object-group service`** options:

`Router(config-network-group)#` **`description`** *`description-text`*	Add a description up to 200 characters.
`Router(config-service-group)#`*`protocol`* `{`*`protocol-number`* `|` *`protocol`*`}`	Identify an IP protocol number or name.
`Router(config-service-group)#`**`tcp`** `|` **`udp`** `|` **`tcp`**-`udp` `[`**`source`** `{{`**`eq`**`]` `|` **`lt`** `|` **`gt`**`}` *`port1`* `|` **`range`** *`port1 port2`*`}]` `[{[`**`eq`**`]` `|` **`lt`** `|` **`gt`**`}` *`port1`* `|` **`range`** *`port1 port2`*`}]`	Specify parameters for TCP, UDP, or both.
`Router(config-service-group)#`**`icmp`** *`icmp-type`*	Specify the decimal number or name of an ICMP type.
`Router(config-service-group)#`**`group-object`** *`nested-object-group-name`*	Specify a nested (child) object group to be included in the current (parent) object group.

TIP: To get help with configuration options, use the question mark (**?**) character.

NOTE: Object groups are not supported in standard ACLs or for use with IPsec but can be used in extended ACLs for quality of service (QoS) match criteria, Cisco IOS firewall features, Dynamic Host Configuration Protocol (DHCP), multicast traffic, and many other features that use extended ACLs.

NOTE: You cannot delete an object group that is being used within an ACL.

Using Object Groups in Extended ACLs

Object groups can be used in most extended ACL operations. On an IPv4 ACL, apply object groups by including the **`object-group`** command followed by the appropriate object group name:

`Router(config)#`**`ip access-list extended`** `{access-list-number	access-list-name}`	Define a named ACL. The command can also be used to edit a numbered ACL.
`Router(config-ext-nacl)#`**`permit`** `{protocol |` **`object-group`** `service-object-group-name}` [**`object-group`** `source-network-object-group-name`] [**`object-group`** `destination-network-object-group-name`]	Define the **`permit`** statement.
`Router(config-ext-nacl)#`**`deny`** `{protocol |` **`object-group`** `service-object-group-name}` [**`object-group`** `source-network-object-group-name`] [**`object-group`** `destination-network-object-group-name`]	Define the **`deny`** statement.

TIP: To get help with configuration options, use the question mark (**?**) character.

NOTE: The preceding syntax has been simplified to highlight the use of object groups in an extended ACL.

NOTE: An ACE can contain a mixture of object groups and individual objects, such as specific protocols, networks, or services.

NOTE: After an object group is applied to an ACE, the object group cannot be deleted nor emptied. If additional objects are appended to the object group after it has been applied to the ACE, there is no need to reapply the object group to the ACE. The ACE automatically adjusts to include any newly appended objects.

Configuring Object Groups in ACLs Example

In this example, only the outside hosts are allowed web and email access to the two corporate servers. Network object groups are used to identify outside and inside groups of objects, and a service object group identifies the services available. The required access policy is defined using one ACE in an extended ACL.

NOTE: Without object groups, the following configuration would require multiple ACEs instead of one. Additional outside hosts, servers, or services can easily be added without altering the ACE in the ACL.

Figure 11-5 shows the network topology for the using objects in ACLs example.

Figure 11-5   Network Topology for the Using Object Groups in ACLs Example

Create a network object group identifying the outside posts.

R1(config)#**object-group network OUTSIDE-HOSTS**	Create a network object group identifying the outside hosts.
R1(config-network-group)#**host 209.165.201.1**	Identify a specific host.
R1(config-network-group)#**range 209.165.202.129 209.165.202.130**	Identify a range of hosts.
R1(config-network-group)#**exit**	Return to global configuration mode.

> **NOTE:**   Alternatively, the range of hosts could have been identified using the network subnet 209.165.202.128 /30.

Create a network object group identifying the corporate servers:

R1(config)#**object-group network SERVERS**	Create a network object group identifying the inside servers.
R1(config-network-group)#**209.165.200.252 /30**	Identify a subnet of servers.
R1(config-network-group)#**exit**	Return to global configuration mode.

Create a service object group identifying web and email services:

`R1(config)#`**`object-group service SERVER-APPS`**	Create a service object group called SERVER-APPS.
`R1(config-service-group)#`**`tcp www`**	Specify HTTP traffic.
`R1(config-service-group)#`**`tcp smtp`**	Specify email traffic.
`R1(config-service-group)#`**`exit`**	Return to global configuration mode.

Create an extended ACL that combines all the defined objects into one ACE:

`R1(config)#`**`ip access-list extended ACL-IN`**	Define an extended ACL named ACL-IN.
`R1(config-ext-nacl)#`**`permit object-group SERVER-APPS object-group OUTSIDE-HOSTS object-group SERVERS`**	Permit HTTP and SMTP traffic from the outside hosts to the internal servers.
`R1(config-ext-nacl)#`**`exit`**	Return to global configuration mode.

Apply the extended ACL to the outside interface:

`R1(config)#`**`interface serial 0/0`**	Enter interface configuration mode for the serial interface.
`R1(config-if)#`**`ip access-group ACL-IN in`**	Apply the ACL incoming on the outside interface.

> **NOTE:**   To verify the object group, use the `show ip access-list` or `show object-group` commands.

Configuring Object Groups in ACLs Using CCP Example

To use object groups in ACL rules, start by creating either a network object or a service object group.

To configure a network group object, choose **Configure > Router > ACL > Object groups > Network Object Group**.

This opens the Network Object Groups screen shown in Figure 11-6.

Figure 11-6   Network Object Groups Summary Screen

From this screen, you can create, edit, or delete a network object group.

To add a new network object, click **Create**.

This opens the Create Network Object Group window shown in Figure 11-7. In this window, specify the network object group name, description, and add the network object members.

> **TIP:**   Use the Type of Member drop-down box to display how objects can be identified.

When done, click **OK**.

Figure 11-7   Create Network Object Group Window

CCP displays the CLI configuration commands. Click **Deliver** to commit the configuration changes.

Repeat the procedure for the SERVERS network object group. Once complete, the Network Object Groups summary should appear as shown in Figure 11-8.

Figure 11-8   Revised Network Object Groups Summary Screen

Next you configure the service group object.

To configure a service group object, choose **Configure > Router > ACL > Object groups > Service Object Group** and click **Create** to open the Create Service Object Group window shown in Figure 11-9.

Figure 11-9   Create Service Object Group Window

After the specifics for the SERVER-APPS service object group have been configured, click **OK**. CCP displays the CLI configuration commands. Click **Deliver** to commit the configuration changes.

Once complete, the Service Object Groups summary should appear as shown in Figure 11-10.

Figure 11-10   Revised Service Object Groups Summary Screen

Next, associate the object groups with the incoming ACL.

Choose **Configure > Router > ACL > ACL Editor**.

To add a new access rule, click **Add**. The Add a Rule dialog appears, as shown on the left side of Figure 11-11.

Figure 11-11 Add a Rule Dialogs

Click **Add** to open the Add an Extended Rule Entry window and identify the
OUTSIDE-HOSTS network object group as the source, the **SERVER** network object
group as the destination, and choose the **SERVER-APPS** service object group for the
protocol and service.

Click **OK** to return to the Add a Rule dialog, and then click **Associate** to open the
Associate with an Interface window. Choose the **outside** serial interface and click **OK**.
Review the rule, and when done, click **OK**.

CCP displays the CLI configuration commands. Click **Deliver** to commit the configura-
tion changes.

The revised Access Rules information screen displays the newly created rule, as shown
in Figure 11-12.

Figure 11-12 Revised Access Rules Screen

ACLs in IPv6

Packet filtering in IPv6 is similar to packet filtering in IPv4. A strategy to prevent common attacks between the two protocol stacks, such as reconnaissance and spoofing attacks, typically starts with ACLs trying to match malicious traffic.

Mitigating IPv6 Attacks Using ACLs

IPv6 ACLs can help mitigate the following threats, among others:

- Header extension threats, for instance, amplification attacks based on Routing Header (RH)

- Threats based on misuse and abuse of ICMPv6

- Reconnaissance based on multicast IPv6 addresses

- Threats that exploit tunneling solutions such as those used in IPv6 migration environments

NOTE: Some threats require a combined approach using both protocol stacks, specifically those that exploit dual-stack environments.

IPv6 ACLs Implicit Entries

Each IPv6 ACL implicitly appends three lines: two permit entries to enable IPv6 neighbor discovery (ND) and the traditional rule that implements a default deny policy:

```
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any
```

CAUTION: It might be desirable to log all implicitly denied packets by explicitly configuring the `deny ipv6 any any log` ACE. A common mistake is to forget the two implicit ND ACEs, which result in ND issues. The solution is to explicitly add all three implicit lines, in the correct order, at the end of the ACL.

Filtering with IPv6 ACLs

`Router(config)#`**`ipv6 access-list`** *`access-list-name`*	Define an IPv6 ACL, and enter IPv6 access list configuration mode. IPv6 ACL names cannot contain a space or quotation mark or begin with a numeral.

`Router(config-ipv6-acl)#`**`permit`** `protocol` {`source-` `ipv6-prefix`**`/`**`nn` | **`any`** | **`host`** `source-ipv6-address` | **`auth`**} [`operator` [`port-number`]] {`destination-ipv6-prefix`**`/`**`nn` | **`any`** | **`host`** `destination-ipv6-address` | **`auth`**} [`operator` [`port-number`]] [**`dest-option-type`** [`doh-number` | `doh-type`]] [**`dscp`** `value`] [**`flow-label`** `value`] [**`fragments`**] [**`log`**] [**`log-input`**] [**`mobility`**] [**`mobility-type`** [`mh-number` | `mh-type`]] [**`reflect`** `name` [**`timeout`** `value`]] [**`routing`**] [**`routing-type`** `routing-num-` `ber`] [**`sequence`** `value`] [**`time-range`** `name`]	Specify the permit condition for an IPv6 ACL.
`Router(config-ipv6-acl)#`**`deny`** `protocol` {`source-ipv6-` `prefix`**`/`**`nn` | **`any`** | **`host`** `source-ipv6-address` | **`auth`**} [`operator` [`port-number`]] {`destination-ipv6-prefix`**`/`**`nn` | **`any`** | **`host`** `destination-ipv6-address` | **`auth`**} [`operator` [`port-number`]] [**`dest-option-type`** [`doh-number` | `doh-type`]] [**`dscp`** `value`] [**`flow-label`** `value`] [**`fragments`**] [**`log`**] [**`log-input`**] [**`mobility`**] [**`mobility-type`** [`mh-number` | `mh-type`]] [**`routing`**] [**`routing-type`** `routing-number`] [**`sequence`** `value`] [**`time-range`** `name`] [**`undetermined-transport`**]	Specify the deny condition for an IPv6 ACL.
`Router(config)#`**`interface`** `type number`	Specify the interface type and number and enter interface configuration mode.
`Router(config-if)#`**`ipv6 traffic-filter`** `access-list-` `name` {**`in`** | **`out`**}	Apply the specified IPv6 access list to the interface.
`Router(config)#`**`line vty 0 4`**	Enter line vty mode.
`Router(config-line)#`**`ipv6 access-class`** `access-list-` `name` {**`in`** | **`out`**}	Apply an IPv6 ACL to specify who can access the vty lines.

NOTE: See Cisco.com for more information on the IPv6 ACL parameters.

Configuring an IPv6 ACL Example

Figure 11-13 displays the network topology for the IPv6 ACL example.

Figure 11-13   Network Topology for the IPv6 ACL Example

`R1(config)#`**`ipv6 access-list IPV6-ACL-IN`**	Define an IPv6 ACL.
`R1(config-ipv6-acl)#`**`remark Basic anti-spoofing ACL`**	Document the ACL.
`R1(config-ipv6-acl)#`**`deny 2001:db8:2c80:1000::0/64 any`**	Deny incoming traffic with the source address the same as the internal network address.
`R1(config-ipv6-acl)#`**`permit any 2001:db8:2c80:1000::1/128`**	Permit traffic to reach the server.
`R1(config-ipv6-acl)#`**`interface serial 0/0`**	Enter interface configuration mode for the serial interface.
`R1(config-if)#`**`ipv6 traffic-filter IPV6-ACL-IN in`**	Apply the IPV6-ACL-IN ACL incoming on the outside interface.

This page intentionally left blank

Configuring Zone-Based Firewalls

This chapter covers the following topics:

Firewall Fundamentals

- Types of Firewalls

Firewall Design

- Firewall Policies
- Firewall Rule Design Guidelines
- Cisco IOS Firewall Evolution

Cisco IOS Zone-Based Policy Firewall

- Cisco Common Classification Policy Language
- Zone-Based Policy Firewall Design Considerations
- Default Policies, Traffic Flows, and Zone Interaction
- Configuring an IOS ZFW
- Configuring an IOS ZFW Using the CLI Example
- Configuring an IOS ZFW Using CCP Example
- Configuring NAT Services for ZFWs Using CCP Example

Firewall Fundamentals

A firewall is a software or hardware system that acts as a barrier between an internal (trusted) network and an external (untrusted) network.

Specifically, firewalls must

- Be resistant to attacks
- Be the only transit point between two networks
- Enforce the security policy access control

Types of Firewalls

There are different types of firewalls, including the following:

Network Address Translation (NAT) firewall	Hides inside (usually private) IP addresses by translating them to outside (usually public) IP addresses.
Packet-filtering firewall	Filters packets at Layer 3 (and 4). Filtering is stateless, which means it does not keep track of traffic flows. This also makes them vulnerable to spoofing attacks.
Stateful firewall	Performs the same function as packet-filtering firewalls but also keeps track of the state of network connections (that is, TCP and UDP sequence numbers) traveling across it.
Application gateway firewall (proxy firewall)	Typically a server filtering information at Layers 3, 4, 5, and 7. It can adapt if a protocol requires additional dynamic ports (for example, FTP, H.323).

NOTE: Other firewall solutions exist, including host-based (server and personal) firewalls; Layer 2 transparent firewalls; and hybrid firewalls, which are a combination of the various firewall types.

NOTE: Stateful packet filtering is the focus of this chapter.

Firewall Design

Best practices for firewall design include the following:

- Position firewalls at security boundaries to separate security domains.
- Use firewalls as a key security control, but not the only one.
- Implement a variety of firewall technologies to provide comprehensive, multilayer access control.
- Ensure that physical access to the firewall is controlled.
- Regularly monitor firewall logs and implement an event management strategy.
- Practice change management for firewall rule creation and configuration changes.

Firewall Policies

Access rules are typically implemented using access control lists (ACLs). When defining access rules, you can use multiple criteria as a starting point:

Rules based on service control	Determines the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic based on IP address and TCP port number. It may provide proxy software that receives and interprets each service request before passing it on. It may host the server software itself, such as a web or mail service.

Rules based on direction control	Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.
Rules based on user control	Controls access to a service according to which user is attempting to access it. This feature is usually applied to users inside the firewall perimeter (local users). It may also be applied to incoming traffic from external users. The latter requires some form of secure authentication technology, such as that provided in IP Security (IPsec).
Rules based on behavior control	Controls how particular services are used. For example, the firewall may filter email to eliminate spam, or it may enable external access to only a portion of the information on a local web server.

NOTE: Firewall rule design usually follows a hybrid approach, combining all these criteria and following a restrictive-access approach.

Firewall Rule Design Guidelines

When creating firewall rules, use the following guidelines:

- Use a restrictive approach for all interfaces and all directions of traffic to permit the required traffic flows and deny everything else.

- Be paranoid and assume that malicious traffic could come from any security domain, even the most trusted ones.

- Balance access control, performance, and rule maintenance. Specific and granular rules provide more control but also result in longer rule sets and increased change management and maintenance challenges.

- Exercise care with the use of "any" keywords matching sources, destinations, and ports because they may allow unwanted traffic.

- For a given access requirement, more specific rules should be at the top, and more generic rules should be at the bottom. The top-down processing order demands this approach to prevent shadow rules when creating exceptions to a given access policy.

- Filtering impossible packets is a common practice. An example is antispoofing rules that are aimed at blocking private IPv4 address spaces in the source address of inbound Internet packets.

- Auditing and change management are crucial. Obsolete rules tend to clutter the rule set and cause breaches to the access policy.

Cisco IOS Firewall Evolution

Firewall technology has evolved as follows:

- Packet filtering using ACLs

- Context-Based Access Control (CBAC) (also referred to as Classic Firewall)

- Cisco IOS Zone-Based Policy Firewall (ZFW)

NOTE: The focus of this chapter will be on ZFW.

Cisco IOS Zone-Based Policy Firewall

A ZFW assigns interfaces to zones. An inspection policy is applied to traffic moving between the zones using the Cisco Common Classification Policy Language (C3PL). Zones establish the security borders where traffic is subjected to policy restrictions as it crosses to another region of your network.

NOTE: The C3PL structure is similar to the modular quality of service (QoS) CLI (MQC) structure.

Cisco Common Classification Policy Language

To create firewall policies, complete the following tasks:

Task	Specifics
Define match criteria (class map).	Contains multiple `match` statements to filter traffic based on an access group (ACL), Layer 4 protocol (for example, TCP, UDP, and ICMP), Layer 7 protocol (HTTP, SMTP, FTP), or another nested class map.
Associate actions to the match criteria (policy map).	Contains class maps that are evaluated in order of configuration and assigned actions of inspect, permit, drop, or drop and log. All unclassified traffic matches the default class, known as class-default, with a default action to drop traffic.
Attach the policy map to a zone pair (service policy).	Identify the source and destination zone pair and assign a service policy to it.

ZFW Design Considerations

- The default policy between zones is to deny all.
- Interfaces belonging to the same zone permit access between them.
- A zone pair permits a unidirectional firewall policy between a source and destination zone.
- An interface can be assigned to one zone only.
- An interface pair can be assigned only one policy.
- A self zone is a system-defined zone that does not have any interfaces as members and applies to traffic directed to the router or traffic that is generated by the router.

Default Policies, Traffic Flows, and Zone Interaction

The following rules govern interface behavior for the traffic moving between zone member interfaces:

- A zone must be configured before you can assign interfaces to the zone.

- You can assign an interface to only one security zone.

- Traffic is implicitly allowed to flow by default among interfaces that are members of the same zone.

- To permit traffic to and from a zone member interface, a policy allowing or inspecting traffic must be configured between that zone and any other zone.

- Traffic cannot flow between a zone member interface and any interface that is not a zone member. You can apply `pass`, `inspect`, and `drop` actions only between two zones.

- Interfaces that have not been assigned to a zone function as classical router ports and might still use classical stateful inspection (CBAC) configuration.

- If you do not want an interface to be part of the ZFW, assign it to a "pass all" policy between it and any other target zone.

NOTE: All active interfaces should be a member of a zone.

The following rules govern interface behavior when the self zone (that is, to/from the router) is involved in the traffic flow:

- All traffic to and from a given interface is implicitly blocked when the interface is assigned to a zone, except traffic to or from other interfaces in the same zone and traffic to any interface on the router.

- All the IP interfaces on the router are automatically made part of the self zone when a ZFW is configured. The self zone is the only exception to the default deny-all policy. All traffic to any router interface is allowed until traffic is explicitly denied.

- The only exception to the deny-by-default approach is the traffic to and from the router itself. This traffic is permitted by default. You can configure an explicit policy to restrict such traffic.

NOTE: Interface ACLs are still relevant and are applied before a ZFW when they are applied inbound. Interface ACLs are applied after a ZFW when they are applied outbound.

Configuring an IOS ZFW

To configure basic interzone policies using the IOS command-line interface (CLI), follow these steps:

1. Create security zones.

2. Create a Layer 3/4 or Layer 7 class map and match traffic.

3. Create the policy map, identify the class map, and associate an action.

4. Identify zone pairs and assign a service policy.

5. Assign interfaces to zones.

> **NOTE:** LAN and WAN configurations must be completed before configuring the ZFW.

Create the security zones:

`Router(config)#`**`zone security`** `zone-name`	Create a security zone.

Create a Layer 3 and Layer 4 inspection type class map:

`Router(config)#`**`class-map type inspect`** `{`**`match-any`** `|` **`match-all`**`}` `class-map-name`	Creates a Layer 3 and Layer 4 inspect type class map.
`Router(config-cmap)#`**`match access-group`** `{`*`access-group`* `|` **`name`** `access-group-name}`	Configure the match criteria on the basis of a preconfigured ACL.
`Router(config-cmap)#`**`match protocol`** `protocol`	Configure the match criteria on the basis of a specified protocol.
`Router(config-cmap)#`**`match service`** `{`**`any`** `|` **`text-chat`**`}`	Configure the match criteria for any supported instant messenger protocol.
`Router(config-cmap)#`**`match class-map`** `class-map-name`	Nest traffic classes within one another.

> **NOTE:** You can also use the `description` command to document the zone.

(Optionally) Create a Layer 7 inspect type class map:

`Router(config)#`**`class-map type inspect`** `protocol-name {`**`match-any`** `|` **`match-all`**`}` `class-map-name`	Create a Layer 7 (application-specific) inspect type class map. **NOTE:** Command parameters will vary depending on the protocol.
`Router(config-cmap)#`**`match`** `protocol-parameters`	**NOTE:** The `match` parameters will vary depending on the protocol.

Configure an action using a policy map:

`Router(config)#`**`policy-map type inspect`** *`policy-map-name`*	Create a Layer 3 and Layer 4 inspect type policy map.
`Router(config-pmap)#`**`class type inspect`** *`class-map-name`*	Identify the class map. **NOTE:** You can also configure `class` `class-default`.
`Router(config-pmap-c)#`{**`drop`** | **`inspect`** | **`pass`**}	Assign an action. **NOTE:** `drop` denies the traffic matching the traffic class. **NOTE:** `inspect` permits and statefully tracks the sessions of the traffic class. **NOTE:** *`pass`* statelessly permits packets between zones.

Identify zone pairs and assign a service policy:

`Router(config)#`**`zone-pair security`** *`zone-pair-name`* **`source`** {*`source-zone-name`* | **`self`** | **`default`**} **`destination`** {*`destination-zone-name`* | **`self`** | **`default`**}	Create a zone pair that permits a unidirectional firewall policy between a pair of security zones. **NOTE:** `self` specifies the system-defined zone. Indicates whether traffic will be going to or from a router. **NOTE:** `default` specifies the name of the default security zone. Interfaces without configured zones belong to the default zone.
`Router(config-sec-zone-pair)#` **`service-policy type inspect`** *`policy-map-name`*	Assign the service policy to the zone pair.

Assign interfaces to zones:

`Router(config)#`**`interface`** *`type number`*	Specifies the interface type and number.
`Router(config-if)#`**`zone-member`** **`security`** *`zone-name`*	Attach the interface to the specified security zone.

Configuring an IOS ZFW Using the CLI Example

Figure 12-1 displays the network topology for the IOS ZFW example.

Figure 12-1   Network Topology for the IOS ZFW Example

R1(config)#**zone security PRIVATE**	Create the inside security zone called PRIVATE.
R1(config-sec-zone)#**exit**	Return to global configuration mode.
R1(config)#**zone security INTERNET**	Create the inside security zone called INTERNET.
R1(config-sec-zone)#**exit**	Return to global config mode.
R1(config)#**class-map type inspect match-any TRAFFIC**	Create a class map called TRAFFIC.
R1(config-cmap)#**match protocol http**	Match HTTP services.
R1(config-cmap)#**match protocol smtp**	Match SMTP services.
R1(config-cmap)#**match protocol ftp**	Match FTP services.
R1(config-cmap)#**exit**	Return to global configuration mode.
R1(config)#**policy-map type inspect MY-POLICY**	Create a service policy called MY-POLICY.
R1(config-pmap)#**class type inspect TRAFFIC**	Identify the class map TRAFFIC.
R1(config-pmap-c)#**inspect**	Inspect all traffic.
R1(config-pmap-c)#**exit**	Return to policy-map configuration mode.
R1(config-pmap)#**exit**	Return to global configuration mode.
R1(config)#**zone-pair security IN-TO-OUT source PRIVATE destination INTERNET**	Create a zone pair identifying the source (PRIVATE) and destination (INTERNET) zones.

`Router(config-sec-zone-pair)#service-` `policy type inspect MY-POLICY`	Assign the service policy MY-POLICY for all traffic travelling from the source to the destination.
`R1(config-sec-zone-pair)#exit`	Return to global configuration mode.
`R1(config)#int fa0/0`	Enter interface Fa0/0 configuration mode.
`R1(config-if)#zone-member security` `INTERNET`	Assign the interface to be a member of the INTERNET zone.
`R1(config-if)#exit`	Return to global configuration mode.
`R1(config)#int fa0/1`	Enter interface Fa0/1 configuration mode.
`R1(config-if)#zone-member security` `PRIVATE`	Assign the interface to be a member of the PRIVATE zone.

NOTE: Use the `show zone security` and the `show zone-pair security` commands to verify the configuration.

NOTE: The preceding example was based on a fairly simple security policy. You can use Cisco Configuration Professional (CCP) to implement more comprehensive security policies.

Configuring an IOS ZFW Using CCP Example

To configure basic interzone policies using CCP, follow these steps:

1. Start the Basic Firewall Wizard.

2. Select trusted and untrusted interfaces.

3. Review and verify resulting policies.

4. (Optional) Enable logging.

5. View firewall status and activity.

6. (Optional) Modify basic policy objects.

NOTE: LAN and WAN configurations must be completed before using the Firewall Wizard.

Use the Basic Firewall Wizard to configure a basic firewall. Choose **Configure > Security > Firewall > Firewall > Create Firewall > Basic Firewall** to open the Basic Firewall Wizard. Figure 12-2 shows the Basic Firewall Wizard screen.

Figure 12-2   Basic Firewall Wizard Screen

Click the **Launch the Selected Task** button. The wizard displays the window shown in Figure 12-3.

Figure 12-3   Basic Firewall Configuration Wizard Window

NOTE: You can enable the Basic Firewall Wizard to provide three levels of basic security.

After reading the default policies that will be applied, click **Next** to display the Basic Firewall Interface Configuration window (Figure 12-4).

Figure 12-4   Basic Firewall Interface Configuration Window

The Basic Firewall Interface Configuration window is displayed listing the current active interfaces.

Identify the inside and outside interfaces.

> **CAUTION:**   The interface that CCP is connected through must be an inside interface. If CCP is connected using an outside interface, check the **Allow Secure Cisco CP Access from the Outsides Interfaces** check box. The wizard will display a screen on which you can specify a host IP address or a network address.

NOTE: A warning dialog box appears if an interface is not assigned to a zone.

Click **Next** to continue.

The Basic Firewall Security Configuration window appears, as shown in Figure 12-5.

The wizard provides the three preconfigured application security policies from the most restrictive (High Security) to the least restrictive (Low Security).

Figure 12-5   Basic Firewall Security Configuration Window

High Security	Option provides the highest level of security and makes the router
	■ Drop instant messaging and peer-to-peer traffic
	■ Inspect HTTP and email traffic and drops noncompliant traffic
	■ Permits TCP and UDP return traffic initiated by inside users
Medium Security	Option tracks the use of applications on the network and the router:
	■ Identifies instant messaging and peer-to-peer traffic
	■ Inspects HTTP traffic and email traffic for protocol compliance
	■ Permits TCP and UDP return traffic initiated by inside users
Low Security	Option provides the lowest level of security and makes the router:
	■ Permit TCP and UDP return traffic initiated by inside users

TIP: Use the slider and click the **Preview Commands** button.

NOTE: Regardless of which option is chosen, CCP generates a substantial configuration. For example, the high level generates nearly 300 commands, and the lowest level generates well over 100 commands.

Select the security level and click **Next**. CCP opens the Basic Firewall Domain Name Server Configuration window shown in Figure 12-6.

Figure 12-6   Basic Firewall Domain Name Server Configuration Window

Enter the primary (and secondary) DNS server IP address and click **Next**.

NOTE: The primary DNS server must be configured.

The wizard then displays the Firewall Configuration Summary window. Use the scroll bar to review the commands that will be configured.

Use the **Back** button to edit a selected choice. Otherwise, click **Finish**.

CCP then displays the CLI configuration commands. Click **Deliver** to commit the configuration changes.

When the commands are delivered, you return to the Firewall screen shown in Figure 12-7.

Figure 12-7   Firewall Screen Showing the Edit Firewall Policy Tab

From this screen, you can modify the access and inspection rules that are displayed. For instance, you can add a new zone policy or add a rule for new traffic or for existing traffic. You can also edit an existing policy or delete it.

> **NOTE:**   Use the **Configure > Security > Firewall > Firewall Components** navigation option to add or change zones, zone pairs, and C3PL objects (class maps, policy maps, and policy assignments).

To monitor the firewall status, choose **Monitor > Security > Firewall Status**, as shown in Figure 12-8.

From this screen, you can verify the firewall configuration and view how many connection attempts have been denied and the log entries, including the time and the reason for the log entry.

> **NOTE:**   For firewall log entries to be collected, logging must be enabled to obtain firewall logging messages with a logging level of debugging (7).

Figure 12-8   Monitor Firewall Status Screen

You can also view firewall logs by navigating to **Monitor > Router > Logging > Firewall Log Screen** and opening the Monitor Router Logging Firewall Log screen (see Figure 12-9).

Figure 12-9   Monitor Router Logging Firewall Log Screen

From this screen, you can display the log messages generated by the firewall and the top attack ports and attackers.

Configuring NAT Services for ZFWs Using CCP Example

You can add NAT to ZFW configurations by applying NAT rules at the interface level for interfaces that belong to zones.

> **NOTE:**   Although NAT can also be implemented using the CLI, the focus of this example is only on using CCP.

In this example, Port Address Translation (PAT) is configured. Trusted hosts on the inside zone are translated dynamically, using PAT, to the IP address on the router's untrusted interfaces, in this example Fast Ethernet 0/0.

The first step is to access and run the basic NAT Wizard by navigating to **Configure > Router > NAT > Create NAT Configuration**.

This opens the Create NAT Configuration screen shown in Figure 12-10.

Figure 12-10   Create NAT Configuration Wizard Screen

You have two NAT Wizard options:

Basic NAT	Choose if you want to connect your network to the Internet (or the outside) and your network has hosts but no servers.
Advanced NAT	Choose if you want to connect your network to the Internet (or the outside) and your network has hosts and servers and the servers must be accessible to outside hosts (hosts on the Internet).

Choose **Basic NAT** and click the **Launch the Selected Task** button. The wizard displays the NAT Wizard welcome window shown in Figure 12-11.

Figure 12-11   NAT Wizard Welcome Window

After reading the default policies that will be applied, click **Next**.

The Basic NAT Wizard interface configuration window opens, as shown in Figure 12-12.

Figure 12-12   Basic NAT Wizard Interface Configuration Window

Select the **outside** and the **inside** interfaces and click **Next**.

The wizard then displays the NAT Summary window. Review the commands that will be configured.

Use the **Back** button to edit a selected choice. Otherwise, click **Finish**.

CCP then displays the CLI configuration commands. Click **Deliver** to commit the configuration changes.

When the commands are delivered, you return to the NAT screen.

Configuring Cisco IOS IPS

This chapter covers the following topics:

IDS and IPS Fundamentals

- Types of IDS and IPS Sensors
- Types of Signatures
- Types of Alarms

Intrusion Prevention Technologies

- IPS Attack Responses
- IPS Anti-Evasion Techniques
- Managing Signatures
- Cisco IOS IPS Signature Files
- Implementing Alarms in Signatures
- IOS IPS Severity Levels
- Event Monitoring and Management
- IPS Recommended Practices

Configuring IOS IPS

- Creating an IOS IPS Rule and Specifying the IPS Signature File Location
- Tuning Signatures per Category
- Configuring IOS IPS Example
- Configuring IOS IPS Using CCP Example
- Signature Tuning Using CCP

IDS and IPS Fundamentals

An intrusion detection system (IDS) sensor captures packets in real time, processes them, and can respond to threats, but it works on copies of data traffic to detect suspicious activity by using signatures. An IDS allows malicious traffic to pass before it can respond.

An intrusion prevention system (IPS) sensor works in line in the data stream to provide protection from malicious attacks in real time. An IPS responds immediately and does not allow malicious traffic to pass.

NOTE: This chapter focuses on IPS.

Types of IPS Sensors

IPS sensors can be deployed as follows:

IPS 4200 Sensor	As a dedicated IPS appliance available in multiple form factors
Network modules	As a network module installed in an Integrated Services Router (ISR), an Adaptive Security Appliance (ASA), or a high-end Catalyst switch
Cisco IOS IPS	Integrated in the IOS of an ISR and some Layer 3 switches

Types of Signatures

IDS and IPS technologies use signatures to detect the following general patterns of misuse:

Atomic pattern	An attempt is made to access a specific port on a specific host, and malicious content is contained in a single packet.
Composite pattern	A sequence of operations that are distributed across multiple hosts over an arbitrary period (event horizon).

Types of Alarms

Attacks can generate the following four types of alarms:

True positive	Occurs when an IDS or IPS signature is correctly fired and an alarm is generated when offending traffic is detected
True negative	Occurs when the sensor does not fire an alarm when it captures and analyzes network traffic that is normal
False positive	Alarm that is triggered by normal traffic or a benign action
False negative	Occurs when an alarm is not triggered when offending traffic is detected

NOTE: True positives and true negatives are expected IDS and IPS alarms.

CAUTION: False positives must be tuned; false negatives must be corrected.

Intrusion Prevention Technologies

Multiple detection technologies are typically used to provide an effective intrusion detection architecture:

Signature-based IPS	■ Signatures are a set of rules installed on an IPS sensor. ■ As sensors scan network packets, they use signatures to detect known attacks and respond with predefined actions. ■ Sensors can modify existing signatures and define new ones.
Policy-based IPS	■ Policies are created and configured on the IPS sensor based on the network security policy. ■ Any traffic that is detected outside the policy will generate an alarm and/or will be dropped.
Anomaly-based IPS (profile-based detection)	■ Sensors generally look for network traffic that deviates from the norm. ■ Statistical baselining is when normal behavior is defined based on traffic patterns, traffic and protocol mix, traffic volumes, and other criteria. ■ Protocol anomaly baselining focuses on traffic that deviates from protocol standards.
Reputation-based IPS	■ Technique uses reputation analysis for various traffic descriptors, such as IP addresses, URLs, Domain Name System (DNS) domains, and others. ■ This usually translates into reputation filters that round up a signature-based system by filtering known malicious sources, destinations, or application components. ■ The approach generally requires communication between the sensor and the source of the reputation information. ■ Sources can be local to the device, enterprise knowledge, and even global knowledge.

NOTE: There are advantages and disadvantages to each intrusion detection technique. It is recommended to strike a balance between these methods and combine them to improve the accuracy, sensitivity, relevancy, and precision of your IPS.

IPS Attack Responses

When an IPS sensor detects malicious activity, it can choose from any or all of the following actions:

Deny attacker inline	■ Action terminates the current packet and future packets from the attacker address for a specified period. ■ The sensor maintains a list of the attackers currently being denied by the system, and these entries can be manually removed from the list or wait for the sliding timer to expire.
Deny connection inline	■ Action terminates the current packet and future packets on this TCP flow.
Deny packet inline	■ Action terminates the packet.
Log attacker packets	■ Action starts IP logging on packets that contain the attacker address and sends an alert to the Event Store, even if the Produce Alert action is not selected.
Log pair packets	■ Action starts IP logging on packets that contain the attacker and victim address pair and sends an alert to the Event Store, even if the Produce Alert action is not selected.
Log victim packets	■ Action starts IP logging on packets that contain the victim address and sends an alert to the Event Store, even if the Produce Alert action is not selected.
Produce alert	■ Action writes the event to the Event Store as an alert.
Produce verbose alert	■ Action includes an encoded dump of the offending packet in the alert and is written to the Event Store.
Request block connection	■ Action sends a request to a blocking device to block this connection.
Request block host	■ Action sends a request to a blocking device to block this attacker host.
Request SNMP trap	■ Action sends a Simple Network Management Protocol (SNMP) notification and an alert to the Event Store, even if the Produce Alert action is not selected.
Reset TCP connection	■ Action sends TCP resets to hijack and terminate the TCP flow.

NOTE: You can use the reset TCP connection action with deny packet and deny connection actions. However, deny packet and deny flow actions do not automatically cause TCP reset actions to occur.

NOTE: Cisco IOS IPS does not support all of these actions.

IPS Anti-Evasion Techniques

Attackers use multiple IPS evasion techniques to allow them to deploy exploits using a stealth approach that often renders IPS sensors unable to detect and prevent intrusion.

Evasion Method	Evasion Description	Anti-Evasion Feature
Traffic fragmentation	Attacker fragments malicious traffic, hoping to avoid detection or filtering by confusing the network IPS sensor reassembly methods, bypassing the network IPS sensor if it does not perform any reassembly at all, or reordering split data if the network IPS sensor does not correctly order it in the reassembly process.	Complete session reassembly in string and service engines
Traffic substitution and insertion	Attacker substitutes payload data with other data in a different format but with the same meaning.	Data normalization (de-obfuscation) in service engines
Protocol-level misinterpretation	Attacker causes the IPS sensor to misinterpret the end-to-end meaning of network protocols. Consequently, the sensor either ignores traffic that should not be ignored or vice versa.	IP Time to Live (TTL) analysis TCP checksum validation
Timing attacks	Attacker evades detection of correlating signatures by performing their actions more slowly, to not exceed the event horizon.	Increase configurable intervals or use third-party for correlation
Encryption and tunneling	Attacker has already established a secure session with the target network or host. The sensor captures the encrypted data but is unable to decrypt it and cannot perform meaningful analysis.	Generic routing encryption (GRE) tunnel inspection
IPS resource exhaustion	Attacker uses specialized tools to create a tremendous number of alarms that consume the resources of the IPS device and prevent attacks from being logged.	Smart dynamic event summarization

NOTE: The mitigation techniques vary depending on the IPS sensor.

Managing Signatures

Cisco IPS relies on signature micro-engines to support IPS signatures. All the signatures in a signature micro-engine are scanned in parallel, which increases efficiency and results in higher throughput. Each signature micro-engine does the following:

- Categorizes a group of signatures with a set of acceptable ranges or sets of values
- Uses router memory to compile, load, and merge signatures

Signature Micro-Engine	Description
ATOMIC-IP Engine	Signatures that examine simple packets, such as Internet Control Message Protocol (ICMP) and User Datagram Protocol (UDP). The ATOMIC engine does not store persistent protocol-based state data across packets; instead, it can trigger a signature from the analysis of the header (Layers 3 and 4) of a single packet.
Service Engines	Signatures that examine the many services that are attacked.
STRING Engines	STRING engines are generic pattern-matching inspection engines for ICMP, TCP, and UDP protocol packets. They use a regular expression engine that can combine multiple patterns into a single pattern-matching table, allowing for a single search through the data.
MULTI-STRING Engine	Inspects Layer 4 protocol packets in a flexible pattern-matching manner.
Other	Internal engine to handle miscellaneous signatures.

Cisco IOS IPS Signature Files

The Cisco IOS IPS signature files must be downloaded from Cisco.com (CCO login required). Two versions of signature files are available, and the file required depends on whether IPS is configured using the command-line interface (CLI) or using Cisco Configuration Professional (CCP). Specifically, if configuring IPS using

- **CLI:** Download IOS-S*xxx*-CLI.pkg (*xxx* = signature version number).
- **CCP:** Download sigv5-SDM-S*xxx*.zip.

You must also download the realm-cisco.pub.key.txt file because it must be used to generate an RSA crypto key and load the public signature on the router for signature decryption.

Implementing Alarms in Signatures

Consider the following when implementing signatures:

- The level assigned to the signature determines the alarm severity level.
- The alarm severity levels are informational, low, medium, and high.
- Make the severity level of the signature the same as the severity level of the alarm.
- Tune your signatures to recognize intrusion patterns out of character with your network traffic patterns.

IOS IPS Severity Levels

Informational	Activity that triggers the signature is not considered an immediate threat, but the information that is provided is useful information.
Low	Abnormal network activity is detected that could be perceived as malicious, but an immediate threat is not likely.
Medium	Abnormal network activity is detected that could be perceived as malicious, and an immediate threat is likely.
High	Attacks that are used to gain access or cause a denial-of-service (DoS) attack are detected, and an immediate threat is extremely likely.

Event Monitoring and Management

Consider the following when implementing event monitoring and management:

- The two key functions of event monitoring and management are to provide real-time event monitoring and management and for analysis based on archived information (reporting).

- Multiple protocols are available for alarm generation, including Security Device Event Exchange (SDEE), syslog, and SNMP.

- Event monitoring and management can be hosted on a single server or on separate servers for larger deployments.

- Archiving is important for forensics and compliance.

- A hierarchical approach of local, enterprise, and global event management is recommended.

NOTE: SDEE is an application-level communication protocol that is used to exchange IPS messages between IPS clients and IPS servers. SDEE is always running, but it does not receive and process events from IPS unless SDEE notification is enabled. If SDEE notification is not enabled and a client sends a request, SDEE responds with a fault response message, indicating that notification is not enabled.

Local correlation	Device-level correlation is accomplished with products such as CCP, IPS Device Manager, or IPS Manager Express.
Enterprise intelligence	Gathered using Cisco Security Manager (CSM). Third-party Security Information and Event Management (SIEM) systems (for example, ArcSight, netForensics, Splunk) can be used for more specialized event management and forensics capabilities.
Global intelligence	Global security intelligence correlation is the responsibility of the Cisco Security Intelligence Operations (SIO), cloud-based service that connects global threat information, reputation-based services, and sophisticated analysis to Cisco network security devices to provide stronger protection with faster response times.

For event management, you can use the SDEE protocol and a syslog-based approach to send Cisco IOS IPS alerts. The sensor generates an alarm when an enabled signature is triggered. Alarms are stored on the sensor. A host can pull the alarms from the sensor using SDEE. Pulling alarms from a sensor allows multiple hosts to subscribe to the event "feed" to allow a host or hosts to subscribe on an as-needed basis.

IPS Recommended Practices

- Use a combination of detection technologies.

- Take advantage of multiple form factors to deploy a distributed and cost-effective IPS architecture.

- Plan the IPS architecture carefully, using a "places in the network" approach, and considering the different levels of risk for the different assets you are trying to protect.

- Enable anti-evasion techniques.

- Take advantage of local, enterprise, and global correlation.

- Use a risk-based approach to improve accuracy and simplify management.

- When deploying a large number of sensors, automatically update signature packs instead of manually upgrading every sensor.

- Place the signature packs on a dedicated FTP server within the management network.

- Tune the IPS architecture on a regular basis.

NOTE: IPS capabilities vary depending on the IPS form factor. Refer to the proper documentation for each IPS sensor product for specific platform details.

Configuring IOS IPS

To configure basic IPS using the IOS CLI, complete these steps:

1. Create an IOS IPS configuration directory in flash.

2. Copy the Cisco IOS IPS signature package to flash.

3. Configure an IOS IPS crypto key.

4. Create an IPS rule and specify the location of the IPS signature file.

5. Enable SDEE and logging event notification.

6. Modify signature categories.

7. Assign the IPS rule to an interface.

NOTE: Download the latest signature package (IOS-S*xxx*-CLI.pkg) and crypto file (realm-cisco.pub.key.txt), the latter of which contains the public key from Cisco.com (CCO login is required).

Create an IOS IPS directory in flash:

`Router#`**`mkdir flash:`***`dir-name`*	Create a directory in flash.
	NOTE: You could specify other locations.

Copy the Cisco IOS IPS signature package to flash using one of the following methods:

`Router#`**`copy ftp://`***`myuser:my-pass@ftp-server`***`/`** **`IOS-S`***`xxx`***`-CLI.pkg flash:`***`dir-name`* **`idconf`**	Copy from an FTP server to the directory in flash.
`Router#`**`copy tftp://`***`tftp-server`***`/IOS-S`***`xxx`***`-CLI.`** **`pkg flash:`***`dir-name`* **`idconf`**	Copy from a TFTP server to the directory in flash.
`Router#`**`copy usbflash0:/IOS-S`***`xxx`***`-CLI.pkg`** **`flash:`***`dir-name`* **`idconf`**	Copy from the USB drive to the directory in flash.

NOTE: Add the `idconf` parameter at the end to initiate the compiling process after the copy is complete.

NOTE: The preceding list shows only common examples. Other methods are available.

To create the RSA crypto key, copy and paste the following:

- Open the realm-cisco.pub.key.txt text file and select the entire contents.
- Copy the text and paste it in global configuration mode.

NOTE: The router executes all the commands from the text file and creates the RSA key. Use the `show running-config | section crypto key pubkey-chain rsa` command to verify the configuration.

Creating an IOS IPS Rule and Specifying the IPS Signature File Location

`Router(config)#`**`ip ips name`** *`ips-name`* [**`list`** *`acl`*]	Create an IPS rule name. **`list`** *`acl`* is optional and specifies an extended or standard ACL to filter the traffic that will be scanned. All traffic that is permitted by the ACL is subject to inspection by the IPS. Traffic that is denied by the ACL is not inspected by the IPS.

`Router(config)#ip ips` `config location flash:`*dir-* *name*	Specify the IPS signature file location. The IPS signature file location is used to restore the IPS configuration in cases such as router reboots or IPS becoming disabled or reenabled. Files, such as signature definitions, signature-type definitions, and signature category information, are written in Extensible Markup Language (XML) format, compressed, and saved to the specified IPS signature location.

NOTE: The IPS does not load the signatures until the rule is applied to an interface.

Enable SDEE and logging event notification:

`Router(config)#ip http server`	Enable the HTTP server (required).
`Router(config)#ip ips notify sdee`	Enable IPS SDEE event notification.
`Router(config)#ip ips notify log`	Enable logging.

Tuning Signatures per Category

Router memory and resource constraints prevent a router from loading all Cisco IOS IPS signatures. Therefore, only load a selected set of signatures that are defined by the categories.

TIP: The larger the number of signatures, the larger the amount of memory consumed. Therefore, retire signatures that are irrelevant to your network to save router memory.

All signatures are pregrouped into categories; the categories are hierarchical. An individual signature can belong to more than one category. Top-level categories help to define general types of signatures.

TIP: Because the categories are applied in a top-down order, you should first retire all signatures, followed by unretiring specific categories.

`Router(config)#`**`ip ips`** **`signature-category`**	Enter IPS category configuration mode to tune Cisco IOS IPS signature parameters on the basis of a signature category.
`Router(config-ips-category)#`**`category`** {**`all`** | **`ios_ips`** [**`basic`** | **`advanced`**] }	Specify the signature category to change, and enter IPS category action mode. **NOTE:** Many other categories and sub-categories exist (for example, **`attack`**, **`dos, ddos email, p2p`**). For a list of supported top-level categories, use the router CLI help (**`?`**). **NOTE:** IOS IPS processes **`category`** commands in the order listed in the configuration.
`Router(config-ips-category-action)#`**`retired`** {**`false`** | **`true`**}	Specify whether a signature or signature category definition should be saved in the router memory. **`false`** unretires all signatures within a given category. **`true`** retires all signatures within a given category. **NOTE:** Retired signatures are not scanned by Cisco IOS IPS and therefore do not fire alarms. **NOTE:** To return to the default action, use the **`no retired`** command.
`Router(config-ips-category-action)#`**`event-action`** *action*	Change router actions for a specified signature category. Actions include the following: ■ **`deny-attacker-inline`** ■ **`deny-connection-inline`** ■ **`deny-packet-inline`** ■ **`produce-alert`** ■ **`reset-tcp-connection`** **NOTE:** Event actions associated with a category can be entered separately or on a single line. **NOTE:** To verify the event-action configuration, use the **`show ip ips signatures`** command.

`Router(config-ips-category-action)#`**`alert-severity {high | medium | low | informational}`**	(Optional) Change the alert severity rating for a given signature or signature category. **NOTE:** To return to the default action, use the `no alert-severity` command.
`Router(config-ips-category-action)#`**`fidelity-rating`** *`rating`*	(Optional) Changes the signature fidelity rating for a signature given category.
`Router(config-ips-category-action)# exit`	Return to IPS category mode.
`Router(config-ips-category)#`**`exit`** `Do you want to accept these changes? [confirm]`	After signature-based changes are complete, you are prompted to confirm whether or not the changes are acceptable. Confirming the changes instructs IOS IPS to compile the changes for the signature and modify memory structures to reflect the change and save the changes to the IPS location specified.

CAUTION: Do not unretire the `all` category because it contains all the signatures in a signature release. The IOS IPS cannot compile and use all the signatures at one time; if it were to do so, it would run out of memory.

NOTE: Use the `show ip ips` command to display IPS configuration information. Use the `show ip ips signature-category [config]` command to display IPS signature parameters by signature category.

Apply the IPS rule to a desired interface and specify the direction:

`Router(config-if)#`**`ip ips`** *`ips-name`* **`{in | out}`**	Apply the IPS rule to an interface. The router loads the signatures and builds the signature engines when IPS is applied to the first interface: `in` inspects only incoming traffic. `out` inspects only outgoing traffic. **NOTE:** The command can be repeated to configure incoming and outgoing traffic.

NOTE: The router prompt disappears while the signatures are loading and the signature engines are building. It reappears after these tasks are complete.

NOTE: Building the signature engine can take several minutes depending on the router platform and how many signatures are being loaded. It is recommended that you enable logging messages so you can monitor the engine building status.

NOTE: The process creates six files in the IPS directory: router-sigdef-default. xml, which contains all the factory default signature definitions; router-sigdef-delta. xml, which contains signature definitions that have been changed from the default; router-sigdef-typedef.xml, which is a file that has all the signature parameter defini- tions; router-sigdef-category.xml, which has all the signature category information, such as category ios_ips basic and advanced; router-seap-delta.xml, which contains changes made to the default Signature Event Action Processor (SEAP) parameters; and router-seap-typedef.xml, which contains all of the SEAP parameter definitions.

(Maintenance) To periodically update the signature package after the IPS has been con- figured, use this command:

`Router#`**`copy`** `url` **`idconf`**	Load a signature package to the identified IPS directory.
	`url` specifies the location from which the router loads the signature file (for example, FTP, TFTP, USB, rcp).

NOTE: Use the `clear ip ips configuration` to remove all IPS configuration entries and release dynamic resources. Use the `clear ip ips statistics` com- mand to reset statistics on packets analyzed and alarms sent.

NOTE: Configure automatic signature updates using the `ip ips auto-update` command. Updates can be configured to run on the basis of a preset time.

Configuring IOS IPS Example

1. Create an IOS IPS configuration directory called **IPS-DIR** in flash.
2. Copy the Cisco IOS IPS signature package from a USB drive to flash.
3. Configure an IOS IPS crypto key.
4. Create an IPS rule called **MY-IPS** and specify the location of the IPS file.
5. Enable SDEE event notification.
6. Retire the **all** signature category and then unretire the **ios-basic** and the **ids_evasion** categories. Change the **ids_evasion** default event notification.
7. Assign the IPS rule to inspect inbound traffic on the Fast Ethernet 0/0 interface.

Figure 13-1 shows the network topology for the IOS IPS example.

Figure 13-1   Network Topology for the IOS IPS Example

R1#**mkdir IPS-DIR** Create directory filename [IPS-DIR]? Created dir flash:/IPS-DIR	Create a directory to store the IPS signature file.
R1#**copy usbflash0:/IOS-S614-CLI.pkg flash:/IPS-DIR idconf** Destination filename [/IPS-DIR/IOS-S614-CLI.pkg]? Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCC CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC <Output omitted> 14219010 bytes copied in 35.528 secs (400220 bytes/sec)R1#	Copy the signature from the USB drive to the IPS-DIR directory.

Configure the IOS IPS RSA crypto key. Copy the contents of the realm-cisco.pub.key.
txt file to global configuration.

Create an IOS IPS rule and specify the IPS signature file location:

R1(config)#**ip ips name MY-IPS**	Create an IPS rule name.
R1(config)#**ip ips config location flash:IPS-DIR**	Specify the IPS signature file location.
R1(config)#**ip http server**	Enable the HTTP server service.
R1(config)#**ip ips notify sdee**	Send events to SDEE.
R1(config)#**ip ips signature-category**	Enter IPS category configuration mode.
R1(config-ips-category)#**category all**	Change signature parameters for the all category.
R1(config-ips-category-action)#**retired true**	Retire the all category.
R1(config-ips-category-action)#**exit**	Return to IPS category configuration mode.
R1(config-ips-category)#**category ios_ips basic**	Change signature parameters for the ios_ips basic category.
R1(config-ips-category-action)#**retired false**	Unretire the signatures.
R1(config-ips-category-action)#**exit**	Return to IPS category configuration mode.
R1(config-ips-category)#**category attack ids_evasion**	Change signature parameters for the ids_evasion category.
R1(config-ips-category-action)#**event-action produce-alert**	Write the event to the Event Store as an alert.
R1(config-ips-category-action)#**event-action deny-packet-inline**	Terminate the packet.
R1(config-ips-category-action)#**event-action reset-tcp-connection**	Terminate the TCP flow.
R1(config-ips-category-action)#**end** Do you want to accept these changes? [confirm]**y**	Exit IPS configuration mode and confirm the signature changes.

`R1(config-ips-category-action)#interface` `fa0/0`	Move to interface configuration mode.

`R1(config-if)#ip ips MY-IPS in`
 	
`*Jan 14 17:16:02.319: %IPS-6-`
`ENGINE_BUILDS_STARTED:  12:16:02 Ne`
 	
`<output omitted>`
	Apply the IPS rule MY-IPS to inbound traffic on the Fast Ethernet 0/0 interface.
	
	NOTE: You could also apply the MY-IPS IPS rule inbound on the inside interface.

NOTE: The preceding is a simple example for implementing IOS IPS. Cisco Configuration Professional (CCP) can also be used to implement and manage an IPS policy.

Configuring IOS IPS Using CCP Example

To support the configuration of IPS using CCP, the host must be running Java JRE Version 6 (or later), and the Java heap must be increased to 256 MB by configuring the runtime parameter –Xmx256m.

NOTE: You can download latest JRE version from Oracle Corporation at http://www.oracle.com/.

To increase the Java heap, from the PC Start menu click **Control Panel > Java** to open the Java Control Panel window. In the Java Control Panel window, display the **Java** tab and click the **View** button to enter or change the Java applet runtime settings. Figure 13-2 shows the window and the required change.

Figure 13-2   Java Runtime Environment Settings Window

NOTE: The actual method of change may vary between versions of JRE.

The figure displays the Runtime Parameter –Xmx256m being configured. Click **OK** to accept the change, and then start CCP.

> **CAUTION:**   The host may require a reboot if CCP still does not recognize the new Java parameter.

To configure basic IPS using CCP, complete these steps:

1. Download the latest Cisco IOS IPS signature package and public crypto key.

2. Launch IPS Rule Wizard to configure Cisco IOS IPS.

3. Verify that Cisco IOS IPS configuration and signatures are properly loaded.

4. Tune signatures.

5. Verify alarms.

You have a few options to download the IOS signature package and public crypto key:

- Log in to Cisco.com and download it manually to the host.

- Download it using CCP by choosing **Configure > Security > Advanced Security > Intrusion Prevention > Edit IPS > Download**.

- Download it automatically using CCP by choosing **Configure > Security > Advanced Security > Intrusion Prevention > Edit IPS > Auto Update**.

> **NOTE:**   In this example, the required files have been downloaded locally to the host.

To launch the IPS Policies Wizard, choose **Configure > Security > Advanced Security > Intrusion Prevention** to open the Intrusion Prevention System (IPS) screen (see Figure 13-3).

Figure 13-3   Intrusion Prevention System (IPS) Screen

From this screen, you can enable IPS or edit an IPS configuration.

The **Security Dashboard** option allows you to keep your router updated with signatures for the latest security threats. The Security Dashboard displays the latest top threats from Cisco if the status of the associated signatures indicates that they are available for deployment or are under investigation. Some of the top threats in the table are associated with signatures that can be deployed to your router.

To enable IPS, click the **Launch the Selected Task** button. The wizard opens the window shown in Figure 13-4.

Figure 13-4   IPS Policies Wizard Welcome Window

NOTE: An SDEE dialog boxes might appear. Read the information and click **OK** for each dialog box.

After reading the welcome screen, click **Next**.

The Select Interfaces window then opens, as shown in Figure 13-5.

Figure 13-5   Select Interfaces Window

In this example, check the **Inbound** check box for Fast Ethernet0/0 and Fast Ethernet0/1. Then click **Next**.

> **NOTE:**   Checking **Inbound** on both interfaces allows IPS to monitor attacks on the router from the internal and external networks.

The Signature File and Public Key window opens, as shown in Figure 13-6.

From this window, you can specify the location of the signature file and configure the public key.

Figure 13-6   Signature File and Public Key Window

You can download the signature file from Cisco.com, or you can identify the location of the signature file. In this example, the file is located on the host. Therefore, click the ellipsis (**...**) to open the Specify Signature File dialog.

Choices of location include the following:

- Located on the router flash or USB

- Located on a remote FTP, HTTP, HTTPS, RPC, SCP, or TFTP server

- Located on the host

NOTE: If the signature package file is located on a remote server, select the protocol to be used and enter the path to the file. For example, if the signature file IOS-S614-CLI.pkg is located at 10.10.10.5 and the FTP protocol will be used, select **FTP** as the protocol, and enter **10.10.10.5/IOS-S614-CLI.pkg.**

NOTE: If the signature file is located on the PC, click **Browse**, navigate to the folder containing the file, and select the filename. You must choose a CCP-specific package of the format sigv5-SDM-S*xxx*.zip (for example, sigv5-SDM-S609.zip).

In this example, the signature file is located on the host. Click **Browse**, navigate to the folder, and select the **sigv5-SDM-Sxxx.zip** file, as shown in Figure 13-7.

Figure 13-7 Specify Signature File Dialog

Click **OK**.

In the Configure Public Key section of the Signature File and Public Key window, enter **realm-cisco.pub** in the Name field.

Next, open the realm-cisco.pub.key.txt file that was previously downloaded from Cisco.com. Copy the text after the phrase "named-key" into the Name field. For example, if the line of text including the name is "named-key realm-cisco.pub signature," copy **realm-cisco.pub** to the Name field.

Next, copy the text between the phrase "key-string" and the word "quit" into the Key field. The revised Signature File and Public Key window should then look something like what is shown in Figure 13-8.

Figure 13-8   Revised Signature File and Public Key Window

Click **Next**.

After several seconds, the Config Location and Category window opens. This is used to specify where to store the signature information.

To specify the location, click the ellipsis (**...**) button next to Config Location to open the Add Config Location dialog.

Then, click the ellipsis (**...**) button next to Directory Name, navigate to the directory location, and then click **OK** to return to the Add Config Location dialog.

Router memory and resource constraints might prevent using all the available signatures. Therefore, there are two categories of signatures in the Choose Category section: Basic and Advanced.

In this example, we will choose **Basic**.

Figure 13-9 shows the revised Config Location and Category window.

Figure 13-9   Revised Config Location and Category Window

Click OK to display the Summary window.

Use the **Back** button to edit a selected choice. Otherwise, click **Finish**.

CCP then displays the CLI configuration commands. Click **Deliver** to commit the configuration changes.

> **NOTE:**   It may take several minutes for the router to compile the signatures.

Once the commands are delivered, you return to the IPS window with the Edit IPS tab selected, as shown in Figure 13-10.

Figure 13-10   Edit IPS Screen

Verify the configuration by checking which interface and in what direction the Cisco IOS IPS is enabled.

Under the Edit IPS tab, select **Signatures**. Verify the signature numbers and start planning your resource preservation strategy based on the router model.

Signature Tuning Using CCP

IPS signature tuning helps manage resources. Signatures can be retired or unretired and enabled or disabled. To do so, choose **Edit IPS > Signatures** and highlight the signature. Then, click **Enable**, **Disable**, **Retire**, or **Unretire**, based on your needs.

To change the action that is associated with a signature, highlight the signature, right-click, choose **Actions**, and then select or deselect the actions to be associated with this signature.

> **NOTE:**   A yellow icon appearing for the signature in the column next to Enabled means that changes have been made to the signature but have not yet been applied.

This page intentionally left blank

VPNs and Cryptology

This chapter covers the following topics:

Virtual Private Networks

- VPN Deployment Modes

Cryptology = Cryptography + Cryptanalysis

- Historical Cryptographic Ciphers
- Modern Substitution Ciphers
- Encryption Algorithms
- Cryptanalysis

Cryptographic Processes in VPNs

- Classes of Encryption Algorithms
- Symmetric Encryption Algorithms
- Asymmetric Encryption Algorithm
- Choosing an Encryption Algorithm
- Choosing an Adequate Key Space

Cryptographic Hashes

- Well-Known Hashing Algorithms
- Hash-Based Message Authentication Code

Digital Signatures

Virtual Private Networks

A virtual private network (VPN) is as an encrypted connection between private networks over a public network such as the Internet.

VPN solutions may be classified based on the following:

| **Deployment mode** | ▪ Site-to-site VPN |
| | ▪ Remote-access VPN |

OSI layer	■ Layer 2 VPN (legacy protocols such as Frame Relay or ATM)
	■ Layer 2 VPN (Multiprotocol Label Switching [MPLS] VPN)
	■ Layer 3 VPN (IP Security [IPsec] and Multiprotocol Label Switching [MPLS] Layer 3 VPN)
	■ Layer 7 VPN (Secure Sockets Layer [SSL] VPN)
Underlying technology	■ IPsec VPN
	■ SSL VPN
	■ MPLS VPN
	■ Other Layer 2 technologies such as Frame Relay or ATM
	■ Hybrid VPNs combining multiple technologies

NOTE: This book focuses on site-to-site IPsec VPNs using Cisco IOS Integrated Services Routers (ISR) and on remote-access SSL VPNs using the Adaptive Security Appliance (ASA).

VPN Deployment Modes

Site-to-site VPNs	■ Connects entire networks to each other.
	■ VPN hosts do not require VPN client software.
	■ VPNs send and receive normal TCP/IP traffic through a VPN "gateway" such as a Cisco ISR or an ASA.
	■ The VPN gateway is responsible for encapsulating and encrypting outbound traffic over the Internet to a peer VPN gateway.
	■ Upon receipt, the peer VPN gateway decrypts the content and relays the packet toward the target host inside its private network.
Remote-access VPNs	■ VPN securely connects telecommuters, mobile users, and extranet consumer-to-business over the Internet.
	■ Hosts may require a preinstalled VPN client (for example, Cisco VPN Client or Cisco AnyConnect) or access the target site using Hypertext Transfer Protocol Secure (HTTPS).
	■ The client encapsulates and encrypts that traffic and sends it over the Internet to the target VPN gateway.
	■ The VPN gateway behaves as it does for site-to-site VPNs.

NOTE: VPNs implement cryptographic protocols to secure the VPN network traffic.

Cryptology = Cryptography + Cryptanalysis

Cryptology is the science of creating and breaking secret codes. It consists of the following:

Cryptography	- The science of creating secret codes to ensure confidentiality - Involves encryption and hashing, which provides authentication/integrity
Cryptanalysis	The science of breaking (cracking) secret codes

Historical Cryptographic Ciphers

Cryptography use ciphers to secure data. A cipher is an algorithm for performing encryption and decryption using a series of well-defined steps that are followed as a procedure. Ciphers are commonly classified as transposition or substitution based.

In transposition-based ciphers, characters are "permuted" or rearranged. A simple example is encrypting HELLO by reversing the letters to produce OLLEH. Other examples include the Scytale, Rail Fence, and Grilles ciphers.

> **NOTE:** Some modern algorithms, such as the Data Encryption Standard (DES) and the Triple Data Encryption Standard (3DES), still use transposition as part of the algorithm.

Substitution ciphers include the following:

Substitution (monoalphabetic)	- Substitute one character for another (for example, A=C, B=D, C=E). - Examples: Caesar cipher, Affine cipher, Atbash cipher.
Polyalphabetic	- Based on substitution, using multiple substitution alphabets. - Examples: Vigenère cipher, Autokey cipher.
One-time pads	- A substitution cipher that combines the text letter with a special key material character. - For example, the Vernam cipher key must be random, as long as the data can only be used once. - Key distribution is challenging because the source and destination must have the same key. - One-time pads are no longer practical, but the concept still applies in modern encryption algorithms such as DES and AES.

> **NOTE:** Another type of substitution ciphers is the polygraphic cipher (for example, Playfair cipher).

Modern Substitution Ciphers

Modern substitution ciphers are categorized by the process they follow to encrypt text:

Block ciphers	■ Referred to as "block-by-block cipher" because it operates on large blocks of digits with a fixed, unvarying transformation.
	■ Padding is used to keep the data size a multiple of the block size.
	■ The ciphertext is generally longer than the plaintext.
	■ The block size varies by algorithm. (DES has 8 bytes.)
	■ Examples: DES, 3DES, AES, Twofish.
Stream ciphers	■ Referred to as "bit-by-bit cipher," in which each plaintext digit is encrypted one at a time with the corresponding digit of the key stream, to give a digit of the cipher-text stream.
	■ Stream ciphers operate on smaller units of plaintext (bits).
	■ The size of the message does not typically change.
	■ The transformation of smaller plaintext units varies depending on encryption requirements.
	■ Examples: RC4, SEAL.

Encryption Algorithms

Encryption is the process of disguising a message in such a way as to hide its original contents. Plaintext (that is, the readable message) is converted to ciphertext (the unreadable, "disguised" message).

Encryption provides confidentiality because only authorized entities can read the original message.

> **NOTE:**   Historically, confidentiality was provided by the secrecy of the algorithm (method) used. Secrecy in modern encryption lies in the secrecy of the key used, not in the algorithm.

Encryption can provide confidentiality at various OSI layers, such as the following:

- Encrypt data link layer data using proprietary link-encrypting devices.
- Encrypt network layer data using protocols such as those in the IPsec protocol suite.
- Encrypt session layer data using a protocol such as SSL or Transport Layer Security (TLS).
- Encrypt application layer data, such as secure email, secure database sessions (Oracle SQL*Net), and secure messaging (Lotus Notes sessions).

NOTE: Both IPsec and SSL are used to set up a VPN. An IPsec VPN is application independent and requires a specialized IP stack on the end system or in the packet path that includes IPsec. An SSL-based VPN supports only web-based applications, but the SSL software is included with all Internet browsers.

Cryptanalysis

Cryptanalysis is the practice of breaking codes to obtain the meaning of encrypted data. One of the following methods may be used to decrypt ciphertext:

Brute-force attack	■ Attacker tries every possible key with the decryption algorithm knowing that eventually one of the keys will work.
	■ All encryption algorithms are vulnerable to this attack.
	■ On average, a brute-force attack succeeds about 50 percent of the way through the keyspace (the set of all possible keys).
	■ Choose a keyspace large enough so that it takes too much time (and money) to accomplish a brute-force attack.
Ciphertext-only attack	■ Attacker obtains several ciphertext messages.
	■ Attacker uses statistical analysis to deduce the key used to encrypt the messages.
	■ These kinds of attacks are no longer practical today because modern algorithms are resistant to statistical analysis.
Known-plaintext attack	■ Attacker obtains several ciphertext messages and also knows something about the plaintext underlying that ciphertext.
	■ Attacker uses a brute-force attack to try keys until decryption with the correct key produces a meaningful result.
	■ Modern algorithms with enormous keyspaces make it unlikely for this attack to succeed.
Chosen-plaintext attack	■ Attacker chooses the data and observes the ciphertext output.
	■ A chosen-plaintext attack is more powerful than a known-plaintext attack because the attacker gets to choose the plaintext blocks to encrypt, allowing the attacker to choose plaintext that might yield more information about the key.
	■ This attack might not be very practical because it is often difficult or impossible to capture both the ciphertext and plaintext.

Chosen-ciphertext attack	■ Attacker chooses the ciphertext and observes the cleartext output.
	■ This attack might not be very practical because it is often difficult or impossible to capture both the ciphertext and plaintext.
Man-in-the-middle attack	■ Attacker knows a portion of the plaintext and the corresponding ciphertext.
	■ The plaintext is encrypted with every possible key, and the results are stored.
	■ The ciphertext is then decrypted by using every key until one of the results matches one of the stored values.

Cryptographic Processes in VPNs

Cryptography provides key services to VPN technologies and solutions:

Confidentiality	The assurance that no one can read a particular piece of data except the receivers explicitly intended
Integrity	The assurance that data has not been altered in transit, intentionally or unintentionally
Authentication	The assurance the other entity is who he, she, or it claims to be
Key management	The generation, exchange, storage, safeguarding, use, vetting, and replacement of keys

VPN services use a combination of cryptographic technologies and algorithms to accomplish their goals. For example, in site-to-site VPNs, IP packets use the following:

- Symmetric encryption algorithms to encrypt the payload, with keys negotiated by key management protocols
- Asymmetric encryption algorithms to create digital signatures and authenticate the VPN peers
- Hashing functions to provide checksum-type integrity checks

NOTE: This combination of algorithms and cryptographic methods negotiates the security settings to accomplish confidentiality, integrity, and authentication.

Classes of Encryption Algorithms

There are two classes of encryption algorithms, which differ in their use of keys:

Symmetric encryption algorithms	■ Referred to as *private-key* or *secret-key* encryption. ■ A sender and receiver must share a secret key. ■ Typical key-length range is 40–256 bits. ■ They are usually quite fast (wire speed). ■ Algorithms are based on simple mathematical operations. ■ Encryption techniques include block ciphers, stream ciphers, and message authentication codes (MAC). ■ Examples: DES, 3DES, AES, and RC.
Asymmetric encryption algorithms	■ Referred to as *public-key* encryption. ■ Use different keys to encrypt and decrypt data. ■ Typical key length is 512–4096 bits. ■ These algorithms are relatively slow because they are based on difficult computational algorithms. ■ Examples: RSA, ElGamal, ECDH, and DH.

Symmetric Encryption Algorithms

Well-known symmetric encryption algorithms include the following:

Data Encryption Standard (DES)	■ Block cipher that encrypts 64-bit data blocks. ■ Fixed-length 64-bit key. (Only 56 bits are used for encryption.)
Triple Data Encryption Standard (3DES)	■ Applies DES three times using three different keys. ■ Key 1 (56 bits) encrypts data. ■ Key 2 (56 bits) decrypts data. ■ Key 3 (56 bits) encrypts data. ■ Key sizes of 168 bits and 112 bits (if key 1 = key 3).
Advanced Encryption Standard (AES)	■ Block cipher with variable block and key lengths. ■ It is stronger, faster, and more efficient than 3DES and is suitable for high-throughput, low-latency environments. ■ Key sizes of 128-, 192-, or 256-bit keys.

Rivest ciphers	▪ Widely deployed family of algorithms, including the following:
	▪ RC2: Designed as alternative to DES.
	▪ RC4: Popular algorithm used in SSL.
	▪ RC6: Designed as alternative to AES.
	▪ Variable block and key sizes.

Asymmetric Encryption Algorithm

Asymmetric algorithms are substantially slower than symmetric algorithms. Their design is based on computational problems, such as factoring extremely large numbers or computing discrete logarithms of extremely large numbers.

Because they lack speed, asymmetric algorithms are typically used in low-volume cryptographic mechanisms, such as digital signatures and key exchange. However, the key management of asymmetric algorithms tends to be simpler than that of symmetric algorithms because usually one of the two encryption or decryption keys can be made public.

NOTE: Asymmetric encapsulation is covered later in more detail.

Choosing an Encryption Algorithm

Two main criteria to consider when selecting an encryption algorithm are as follows:

Is the algorithm trusted by the cryptographic community?	▪ Most new algorithms are broken very quickly.
	▪ Algorithms that have resisted attacks for a number of years are preferred.
	▪ Examples: DES, 3DES, AES, IDEA, and RC4.
Does the algorithm adequately protect against brute-force attacks?	▪ If the algorithm is trusted, no shortcut exists to break it, and the attacker must search through the keyspace to guess the correct key.
	▪ Use adequate key lengths to satisfy the confidentiality requirements of the organization.

Choosing an Adequate Keyspace

	Symmetric Key	**Asymmetric Key**	**Hash**
Protection up to 3 years	80	1248	160
Protection up to 10 years	96	1776	192
Protection up to 20 years	112	2342	224
Protection up to 30 years	128	3248	256
Protection against quantum computers	256	15424	512

NOTE: Notice the comparatively short symmetric key lengths. However, do not directly compare the key length of asymmetric and symmetric algorithms; the underlying design of the two algorithm families differs greatly.

NOTE: An 80-bit symmetric key is considered equal to a 1024-bit key using the RSA algorithm. A 112-bit symmetric key is considered equal to a 2048-bit key using the RSA algorithm. A 128-bit symmetric key is considered equal to a 3072-bit key using the RSA algorithm.

Cryptographic Hashes

Cryptographic hashes are based on one-way functions that are used for integrity assurance. They hash arbitrary data into a fixed-length digest known as a fingerprint.

NOTE: Hashing alone does not add security to the message. It only prevents the message from being changed accidentally, such as by a communication error.

Well-Known Hashing Algorithms

Message digest algorithm 5 (MD5)	▪ Popular, ubiquitous hashing algorithm ▪ Collision-resistant one-way function, which means that two messages with the same hash are very unlikely to occur ▪ 128-bit message digest
Secure Hash Algorithm 1 (SHA-1)	▪ Although slower than MD5, it is the stronger algorithm. ▪ 160-bit message digest
Secure Hash Algorithm 2 (SHA-2)	▪ Available as SHA-224, SHA-256, SHA-384, and SHA-512 ▪ Should be used rather than SHA-1 ▪ Adopted by U.S. federal government as a secure hash standard

Hash-Based Message Authentication Codes

Hash-based Message Authentication Codes (HMAC) use existing hash functions and add a secret key as input to the hash function to provide integrity assurance and authentication. Only parties who have access to that secret key can compute the digest of an HMAC function.

NOTE: HMACs defeat man-in-the-middle attacks.

Cisco technologies use two well-known HMAC functions:

- Keyed MD5, based on the MD5 hashing algorithm
- Keyed SHA-1, based on the SHA-1 hashing algorithm

Cisco products use hashing for entity authentication, data integrity, and data authenticity purposes, such as the following:

- IPsec gateways and clients use MD5 and SHA-1 in HMAC mode to provide packet integrity and authenticity.
- Cisco IOS images use MD5 to verify the integrity of downloaded images and router passwords.
- Cisco routers use hashing with secret keys to add authentication to routing protocols.

Digital Signatures

Digital signatures are commonly used in the following situations:

- To provide a unique proof of the data source, which can only be generated by a single party, such as with contract signing in e-commerce environments
- To authenticate a user by using the private key of that user and the signature it generates
- To prove the authenticity and integrity of public key infrastructure (PKI) certificates
- To provide a secure time stamp, such as with a central trusted time source

Digital signatures provide three basic security services in secure communications:

Authenticity of digitally signed data	Digital signatures authenticate a source, proving that a certain party has seen and has signed the data in question.
Integrity of digitally signed data	Digital signatures guarantee that the data has not changed from the time it was signed.
Nonrepudiation of the transaction	The recipient can take the data to a third party, and the third party accepts the digital signature as a proof that this data exchange did take place. The signing party cannot repudiate that it has signed the data.

To achieve these goals, digital signatures have the following properties:

The signature is authentic.	The signature convinces the recipient of the document that the signer signed the document.
The signature is not forgeable.	The signature is proof that the signer, and no one else, signed the document.
The signature is not reusable.	The signature is a part of the document and cannot be moved to a different document.
The signature is unalterable.	After a document is signed, it cannot be altered.
The signature cannot be repudiated.	The signature and the document are physical things. Signers cannot claim later that they did not sign it.

NOTE: The next chapter covers digital signatures.

This page intentionally left blank

Asymmetric Encryption and PKI

This chapter covers the following topics:

Asymmetric Encryption

- Public Key Confidentiality and Authentication
- RSA Functions

Public Key Infrastructure

- PKI Terminology
- PKI Standards
- PKI Topologies
- PKI Characteristics

Asymmetric Encryption

Asymmetric algorithms are based on complex mathematical formulas, and therefore computation takes more time than symmetric algorithms.

Examples of public key encryption algorithms are the Rivest, Shamir, and Adleman (RSA) algorithm; Digital Signature Algorithm (DSA); Diffie-Hellman (D-H); ElGamal; and elliptic curve cryptography (ECC).

Public Key Confidentiality and Authentication

Asymmetric algorithms use a public key and a private key. Both keys are capable of encryption. However, the complementary matched key is required for decryption.

For example, if a public key encrypts the data, the matching private key decrypts the data. The opposite is also true. If a private key encrypts the data, the corresponding public key decrypts the data.

Asymmetric cryptography is used to accomplish confidentiality and authentication.

Public Key Confidentiality	**Confidentiality = Public Key (Encrypt) + Private Key (Decrypt)**
	▪ The public key is used to encrypt; the corresponding private key is used to decrypt.
	▪ Because the private key is only present on one system, confidentiality is achieved in communicating with that system.
	▪ This scenario is often used for key exchange.
Public Key Authentication	**Authentication = Private Key (Encrypt) + Public Key (Decrypt)**
	▪ The private key is used to encrypt; the corresponding public key is used to decrypt.
	▪ Because the private key is only present on one system, authentication is assured when its public key decrypts the message.

RSA Functions

RSA is one of the most common asymmetric algorithms because it is easy to implement. It is very flexible because it has a variable key length that allows speed to be traded for the security of the algorithm if necessary. An RSA key is usually 512–2048 bits long. The security of RSA is based on the difficulty of factoring very large numbers, which is breaking large numbers into multiplicative factors. RSA is substantially slower than Digital Encryption Standard (DES) and is typically used only to protect small amounts of data within the context of confidentiality.

RSA is mainly used for two services:

▪ To ensure confidentiality of data by performing encryption, usually for small amounts of data such as session keys

▪ To perform authentication of data or nonrepudiation of data, or both, by generating digital signatures

Public Key Infrastructure

A public key infrastructure (PKI) ensures confidentiality, integrity, and authentication in an enterprise and is based on the fundamentals of asymmetric encryption. PKI solutions are based on digital certificates and a trusted third-party trust model.

PKI uses the power of private and public keys, digital signatures, and trust models that are derived from asymmetric encryption. PKI provides services that include identity management, software code signing, encrypted file systems, email, virtual private networks (VPNs), and others.

The PKI is a set of technical, organizational, and legal components. Those components are needed to establish a system that enables large-scale use of public key cryptography to provide authenticity, confidentiality, integrity, and nonrepudiation services.

PKI Terminology

Public key infrastructure (PKI)	■ A service framework needed to support large-scale public key-based technologies.
Certificates	■ Electronic document that binds a name of a user or an organization to a public key certificate (digital certificate).
	■ Digital certificates are digitally signed by a CA.
	■ The certificate can be used to verify that a public key belongs to an individual or organization.
Certificate authority (CA)	■ A certificate authority (that is, a trusted third party) binds public keys with respective user identities.
	■ It digitally signs and publishes the public keys associated with an organization.
	■ Commercial CAs (for example, VeriSign) charge for services and are trusted by most web browsers.
	■ Some service providers provide public CAs and do not charge for services.
	■ CAs can also be implemented by an organization or a government for its users.
Registration authority (RA)	■ PKI servers that help CAs by performing key management tasks and therefore offloading the CA.
	■ They are like proxies of the CA.
	■ They minimize CA exposure to the network.

NOTE: Certificates are commonly used at the application layer for Secure Sockets Layer (SSL), Transport Layer Security (TLS), Secure MIME (S/MIME), and Pretty Good Privacy (PGP). Cisco devices can use certificates for the initial key exchange (IKE) in IPsec VPNs and in 802.1x authentication using Extensible Authentication Protocol-TLS (EAP-TLS).

PKI Standards

PKI requires interoperability with other technologies from different PKI vendors. The Internet Engineering Task Force (IETF) has formed the PKIX Working Group that is dedicated to promoting and standardizing PKI for the Internet.

Solutions include the following

X.509	▪ A well-known ITU-T standard that defines basic PKI standard formats for public key certificates and certificate revocation lists (CRL).
	▪ X.509 Version 3 (X.509v3) defines the digital certificate format that is used extensively in SSL website authentication, email agents, and IPsec VPNs for initial key exchange.
Public-Key Cryptography Standards (PKCS)	▪ RSA standards that define formats for the secure exchange of data, including the following: ▪ PKCS #1: RSA Cryptography Standard ▪ PKCS #3: DH Key Agreement Standard ▪ PKCS #7: Cryptographic Message Syntax Standard ▪ PKCS #8: Private-Key Information Syntax Standard ▪ PKCS #10: Certification Request Syntax Standard ▪ PKCS #12: Personal Information Exchange Syntax Standard ▪ PKCS #13: Elliptic Curve Cryptography Standard ▪ PKCS #15: Cryptographic Token Information Format Standard

PKI Topologies

Simple (single-root) PKI	▪ Issues all the certificates to the end users. ▪ The benefit in such a setup is simplicity. ▪ VPNs that are managed by a single organization often use this topology.
Hierarchical CA topology	▪ Involves multiple hierarchical CAs within an organization. ▪ CAs can issue certificates to end users and to subordinate RAs, which in turn issue their certificates to end users or other CAs. ▪ The main benefits are increased scalability and manageability. ▪ Trust decisions can now be hierarchically distributed to smaller branches.
Cross-certified CAs	▪ Involves multiple flat, single-root CAs that establish trust relationships horizontally by cross-certifying their own CA certificates.

PKI Characteristics

- To authenticate each other, users have to obtain the digital certificate of the CA and their own digital certificate. These steps require the out-of-band verification of the processes.

- Public key systems use public and private asymmetric keys. Whatever is encrypted using one key can only be decrypted using the other key providing nonrepudiation.

- Key management is simplified because two users can freely exchange the certificates, and the validity of the received certificates is verified using the public key of the CA, which the users already have in their possession.

- Because of the strength of the algorithms, you can set a very long lifetime for the certificates, typically measured in years.

This page intentionally left blank

IPsec VPNs

This chapter covers the following topics:

IPsec Protocol

- IPsec Protocol Framework
- Encapsulating IPsec Packets
- Transport Versus Tunnel Mode
- Confidentiality Using Encryption Algorithms
- Data Integrity Using Hashing Algorithms
- Peer Authentication Methods
- Key Exchange Algorithms
- NSA Suite B Standard

Internet Key Exchange

- IKE Negotiation Phases
- IKEv1 Phase 1 (Main Mode and Aggressive Mode)
- IKEv1 Phase 2 (Quick Mode)
- IKEv2 Phase 1 and 2
- IKEv1 Versus IKEv2

IPv6 VPNs

IPsec Protocol

The IP Security (IPsec) protocol is an open standard that provides the following:

Confidentiality	■ Confidentiality is provided using encryption algorithms.
	■ Data encryption prevents third parties from reading the data transmitted over public or wireless networks.
	■ Encryption algorithms: Digital Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES), or Software-optimized Encryption Algorithm (SEAL).

Data integrity	■ Data integrity is provided using hashing algorithms. ■ Hashing algorithms validate that the received data has not been altered. ■ Hashing algorithms: message digest algorithm 5 (MD5) or Secure Hash Algorithm (SHA).
Authentication	■ Authentication is defined by the Internet Key Exchange (IKE) protocol. ■ IKE authenticates users and devices. ■ Authentication methods: pre-shared keys (PSK) or digital certificates.
Antireplay protection	■ Antireplay verifies that each packet is unique and not duplicated.

IPsec Protocol Framework

IPsec identifies the framework to support secure network communication over a virtual private network (VPN). Figure 16-1 illustrates the IPsec framework and optional algorithms.

Figure 16-1   IPsec Framework

Encapsulating IPsec Packets

There are two main IPsec framework protocols:

Authentication Header (AH)	■ AH provides data authentication and integrity. ■ However, it does not provide confidentiality. ■ AH provides integrity and authentication of the payload using either HMAC-MD5 or HMAC-SHA-1. ■ AH is IP protocol 51.
Encapsulating Security Payload (ESP)	■ ESP provides confidentiality by encrypting the payload using DES, 3DES, or AES. ■ ESP can also provide integrity and authentication of the payload using either HMAC-MD5 or HMAC-SHA-1. ■ ESP can also enforce antireplay protection by requiring that a receiving host set the replay bit in the header to indicate that the packet has been seen. ■ ESP is IP protocol number 50.

NOTE: This chapter focuses on ESP, along with other important IPsec protocols.

Transport Versus Tunnel Mode

ESP and AH can be used in two different modes:

Transport mode	■ Security is provided only for the transport layer and above. ■ Transport mode protects the payload of the packet but leaves the original IP address in the clear. ■ ESP transport mode is used between hosts.
Tunnel mode	■ Tunnel mode provides security for the complete IP packet. ■ The original packet is encrypted and then encapsulated in another IP packet. ■ ESP tunnel mode is used between a host and a security gateway or between two security gateways.

NOTE: The focus in this book is on tunnel mode.

Confidentiality Using Encryption Algorithms

The following are some of the encryption algorithms and key lengths that IPsec can use:

Data Encryption Standard (DES) algorithm	■ DES uses a 56-bit key symmetric key cryptosystem.
Triple Data Encryption Standard (3DES) algorithm	■ 3DES is a symmetric key cryptosystem. ■ A variant of DES that processes blocks of data 3 times, each time with an independent 56-bit encryption key.
Advanced Encryption Standard (AES)	■ AES is a symmetric key cryptosystem that provides stronger security than DES and is computationally more efficient than 3DES. ■ It offers key lengths of 128 bits, 192 bits, and 256 bits.
Software-optimized Encryption Algorithm (SEAL)	■ SEAL is a stream cipher that uses a 160-bit key for encryption.
Rivest, Shamir, and Adleman (RSA)	■ RSA is an asymmetrical key cryptosystem. ■ It uses a key length of 512 bits, 768 bits, 1024 bits, or larger. ■ It is not used for data encryption but instead is used during the peer-authentication phase.

NOTE: SEAL and RSA algorithms are beyond the scope of this chapter.

Data Integrity Using Hashing Algorithms

The following are some of the Hash-based Message Authentication Code (HMAC) algorithms and key lengths that IPsec can use:

HMAC-Message Digest 5 (HMAC-MD5)	■ HMAC-MD5 uses a 128-bit shared-secret key. ■ The message and 128-bit shared-secret key are combined and run through the HMAC-MD5 hash algorithm. ■ The hash is appended to the original message and is forwarded to the remote end.
HMAC-Secure Hash Algorithm 1 (HMAC-SHA-1)	■ HMAC-SHA-1 uses a 160-bit secret key. ■ The message and the 160-bit shared-secret key are combined and run through the HMAC-SHA-1 hash algorithm. ■ The hash is appended to the original message and is forwarded to the remote end.

| HMAC-Secure Hash Algorithm 2 (HMAC-SHA-2) | ■ SHA-2 HMAC algorithms are the strongest algorithms. |
| | ■ The SHA-2 family is based on SHA-1 and adds the SHA-256 bit hash algorithm and SHA-384 bit hash algorithm. |

Peer Authentication Methods

Pre-shared keys (PSK)	■ Peers authenticate each other by comparing preconfigured secret keys.
	■ The PSK is combined with other information to create the authentication key.
RSA signatures	■ Peers authenticate each other using digital certificates.
	■ The sending peer creates an encrypted hash using their private key, attaches it to a message, and forwards it.
	■ The remote peer decrypts the hash using the public key and compares it with a recomputed hash.
RSA encrypted nonces	■ Peers authenticate each other using RSA-generated random numbers (called nonces).
	■ Public keys must be manually copied to each peer as part of the configuration process.
	■ This method is the least popular.
Elliptical Curve Digital Signature Algorithm (ECDSA)	■ ECDSA is the method used for the Digital Signature Standard (DSS).
	■ ECDSA improves the communication efficiency:
	■ It is quicker than similar-strength RSA operations.
	■ It is smaller than RSA signatures.

Key Exchange Algorithms

Encryption algorithms require a symmetric shared-secret key to perform encryption and decryption. These algorithms are used within IKE to establish session keys. The following public key exchange methods are available in Cisco IOS Software:

Diffie-Hellman (DH)	■ Provides a way for two peers to establish a shared-secret key, which only they know, even though they are communicating over an unsecure channel.
	■ Examples:
	■ For DES, use DH1 (768-bit key).
	■ For 3DES, use DH2 (1024-bit key).
	■ For AES, use DH5 (1536-bit key), DH14 (2048-bit key), DH15 (3072-bit key), or DH16 (4096-bit key).
ECDH	■ A variant of the DH protocol using elliptic curve cryptography (ECC).
	■ For ECDH, use DH19 (256-bit ECDH key), DH20 (384-bit ECDH key), or DH24 (2048-bit ECDH key).

NOTE: DH groups determine the strength of the key that is used in the key exchange process. Higher group numbers are more secure, but they require additional time to compute the key.

NSA Suite B Standard

The National Security Agency (NSA) as part of its Cryptographic Modernization Program has identified a globally recognized set of cryptography standards referred to as Suite B. As described in RFC 4869, Suite B cryptography secures information traveling over networks using four well-established, public-domain cryptographic algorithms:

- Encryption uses AES with 128-bit or 256-bit keys.
- Hashing (digital fingerprinting) uses SHA-2.
- Digital signatures use the ECDSA.
- Key exchange uses the Elliptic Curve Diffie-Hellman (ECDH) method.

Internet Key Exchange

IPsec requires the IKE protocol to negotiate security associations (SA), which are agreements between two peers engaging in an IPsec exchange. IKE is also responsible for the automatic key generation and key refresh.

There are two versions of the IKE protocol: IKEv1 and IKEv2.

IKEv2 was created to overcome some of the limitations of IKEv1. It is more reliable, flexible, and simpler than IKEv1 because it requires fewer transactions to establish SAs. It also provides mobility, allowing mobile users to roam without disconnecting their IPsec session.

IKE Negotiation Phases

To establish an IPsec VPN tunnel, IKEv1 and IKEv2 both require two negotiation phases.

IKE Phase 1	■ Goal is to establish an IKE SA.
	■ Phase can be completed in *main mode* or in *aggressive mode*.
	■ Two IPsec peers perform the initial negotiation of SAs.
	■ SA negotiations are bidirectional; data may be sent and received using the same encryption key.
IKE Phase 2	■ Goal is to establish an IPsec SA.
	■ Phase is also called *quick mode*.
	■ SAs are negotiated by the IKE process Internet Security Association and Key Management Protocol (ISAKMP).
	■ In this phase, the SAs that IPsec uses are unidirectional, and therefore a separate key exchange is required for each data flow.

IKEv1 Phase 1 (Main Mode and Aggressive Mode)

The basic purpose of IKEv1 Phase 1 is to negotiate IKE policy sets, authenticate the peers, and set up a secure channel between the peers.

IKEv1 Phase 1 operates in either main mode or aggressive mode:

Main mode	■ Negotiation exchanges six messages between peers.
	■ These exchanges define what encryption and authentication protocols are acceptable, how long keys should remain active, and whether perfect forward secrecy (PFS) should be enforced.
Aggressive mode	■ Negotiation exchanges three messages between peers.
	■ The initiator passes all data that is required for the SA.
	■ The responder sends the proposal, key material, and ID and authenticates the session in the next packet.
	■ The initiator replies by authenticating the session.

NOTE: Main mode protects the identity of the peers, whereas aggressive mode does not. The use of main mode or aggressive mode is a tradeoff between performance and security.

IKE Phase 1 main mode includes three, two-message exchanges:

First message exchange	■ Peers negotiate and agree upon the algorithms and hashes that will be used to secure the subsequent IKE exchanges.
	■ The responder chooses the best-suited proposal and then sends that proposal to the initiator.
Second message exchange	■ Peers use the DH key exchange algorithm to generate a shared secret key that is used to encrypt all the other encryption and authentication keys.
	■ This negotiation results in one single bidirectional ISAKMP SA.
Third message exchange	■ The third exchange authenticates an ISAKMP session.
	■ The peer is authenticated using PSK, digital signature, or public key encryption.

IKEv1 Phase 2 (Quick Mode)

The purpose of IKE Phase 2 is to negotiate (and renegotiate) the IPsec security parameters (called transform sets) and establish IPsec SAs. It also periodically renegotiates IPsec SAs. IKE Phase 2 has one mode, called quick mode.

After IKE Phase 1 is complete, quick mode uses three messages to negotiate a shared IPsec transform, derives shared-secret keying material that the IPsec security algorithms will use, and establishes IPsec SAs. Quick mode also exchanges nonces that are used to generate new shared-secret key material and prevent replay attacks from generating false SAs.

IKEv2 Phase 1 and 2

IKE Phases 1 and 2 are enhanced by IKEv2. IKEv2 simplifies the initial exchange of messages, thus reducing latency and increasing the connection establishment speed. IKEv2 includes all the functionality of IKEv1, including the two negotiation phases:

IKEv2 Phase 1	■ Negotiation exchanges four messages between peers.
	■ The first two messages flow in the clear on the network while the other two messages are encrypted.
IKEv2 Phase 2	■ Negotiation exchanges two messages between peers.
	■ The Phase 2 SA contains the keys that are used to encrypt and decrypt IPsec packets on the host, authenticate IPsec packets on the host, or both.

IKEv1 Versus IKEv2

Fewer RFCs	■ IKEv1 is defined in five RFCs.
	■ IKEv2 is defined in RFC 5996.
Simplified message exchange	■ IKEv1 exchanges nine messages (Phase 1 = 6, Phase 2 = 3).
	■ IKEv2 exchanges six messages (Phase 1 = 4, Phase 2 = 2).
Security	■ IKEv1 may be susceptible to denial-of-service (DoS) attacks.
	■ IKEv2 is more immune to DoS attacks because it does not process a request until it determines the requester.
NAT traversal	■ The encapsulation of IKE and ESP in UDP port 4500 enables these protocols to pass through a device or firewall performing Network Address Translation (NAT).
Reliability	■ IKEv2 uses sequence numbers and acknowledgments and mandates some error-processing logistics and shared state management.
Support for EAP	■ IKEv2 can leverage existing authentication infrastructure and credential databases such as Extensible Authentication Protocol (EAP).
Mobility	■ IKEv2 can implement MOBIKE (Mobility and Multihoming Protocol), which allows for Layer 3 roaming by changing the peer's IP address without reestablishing all SAs with the VPN gateway.

IPv6 VPNs

IPsec is native to IPv6. However, IPv6 does not mandate that IPsec be used for all IPv6 communications. In IPv4, AH and ESP were IP protocol headers. IPv6 uses the extension header approach, and therefore ESP uses the next-header value of 50 and AH uses the next-header value of 51.

IPv6 supports the latest cryptography suites (Suite B and beyond), and the mobility enhancements that are found in IKEv2 are key.

This page intentionally left blank

Configuring Site-to-Site VPNs

This chapter covers the following topics:

Site-to-Site IPsec VPNs

- IPsec VPN Negotiation Steps
- Planning an IPsec VPN
- Cipher Suite Options

Configuring IOS Site-to-Site VPNs

- Verifying the VPN Tunnel
- Configuring a Site-to-Site IPsec VPN Using IOS Example
- Configuring a Site-to-Site IPsec VPN Using CCP Example
- Generating a Mirror Configuration Using CCP
- Testing and Monitoring IPsec VPNs
- Monitoring Established IPsec VPN Connections Using CCP

Site-to-Site IPsec VPNs

Organizations of all kinds often deploy site-to-site virtual private networks (VPNs) when implementing a corporate network across public and private networks. Internet-based VPN environments and Multiprotocol Label Switching (MPLS) VPN environments benefit from the flexibility of deployment and standards-based implementation of cryptographic mechanisms.

The choice of device terminating VPNs becomes a key factor in implementing site-to-site VPNs. Organizations benefit from leveraging their existing network elements and using an integrated approach to VPN deployments. This lesson highlights the use of Cisco IOS routers as site-to-site VPN termination points in IP Security (IPsec) environments.

IPsec VPN Negotiation Steps

IPsec VPN negotiation can be broken down into five steps, including Phase 1 and Phase 2 of Internet Key Exchange (IKE):

1. An IPsec tunnel is initiated when a host sends "interesting" traffic to a destination host. Traffic is considered interesting when it travels between the IPsec peers and meets the criteria that are defined in the crypto ACL.

2. The interesting traffic initiates IKE Phase 1 between the peer routers. The IPsec peers negotiate the established IKE security association (SA) policy. Once the peers are authenticated, a secure tunnel is created by using Internet Security Association and Key Management Protocol (ISAKMP).

3. The peers then proceed to IKE Phase 2. The IPsec peers use the authenticated and secure tunnel to negotiate IPsec SA transforms. The negotiation of the shared policy determines how the IPsec tunnel is established.

4. The IPsec tunnel is created, and data is transferred between the IPsec peers based on the IPsec parameters that are configured in the IPsec transform sets.

5. The IPsec tunnel terminates when the IPsec SAs are deleted or when their lifetime expires.

Planning an IPsec VPN

When planning to deploy a site-to-site IPsec VPN, remember the following:

Verify connectivity between peers.	Ensure that IP protocols 50 (ESP) and 51 (AH) and UDP port 500 (ISAKMP) traffic are permitted and not blocked by an access control list (ACL).
Define interesting traffic.	Define which traffic will trigger a VPN session (interesting traffic) and which traffic will travel outside the tunnel (non-interesting traffic).
Determine the cipher suite requirements.	Choose a cipher that suits the network security policy of the organization.
Manage monitoring, troubleshooting, and change.	Consider all three areas in the planning process.

Interesting traffic is defined by crypto ACLs in site-to-site IPsec VPN configurations. Crypto ACLs perform these functions:

Outbound	Selects outbound traffic that IPsec should protect. Traffic that is not selected is sent in plaintext.
Inbound	If you want, you can create inbound ACLs to filter and discard traffic that should have been protected by IPsec.

NOTE: Traffic matching a permit action in the ACL is protected and sent through the VPN. Traffic matching a deny action in the ACL is sent outside the VPN in cleartext.

Cipher Suite Options

The following compares weaker options to stronger options:

Parameter	Weakest	Strongest
Encryption algorithm	Digital Encryption Standard (DES)	Advanced Encryption Standard (AES)
Hash algorithm	Message digest algorithm 5 (MD5)	Secure Hash Algorithm 2 (SHA-2)
Authentication method	Pre-share key (PSK)	Rivest, Shamir, Adleman (RSA) Signature
Key exchange	Diffie-Hellman (DH) group 1	DH group 5
IKE SA lifetime	86,400 seconds	< 86,400 seconds

Configuring IOS Site-to-Site VPNs

To configure a site-to-site VPN using the IOS command-line interface (CLI), complete the following steps:

1. Create an IKE policy and configure the required Phase 1 parameters.

2. Specify the PSK and identify the peer address (or hostname).

3. Create the IPsec policy required for Phase 2.

4. Create the crypto map and configure crypto map specifics.

5. Identify interesting traffic using an extended ACL.

6. Apply the crypto map to an interface.

7. Verify the tunnel.

NOTE: Some of these steps can be done out of order.

Create an IKE policy.

`Router(config)#`**`crypto isakmp`** **`policy`** `priority`	Define an IKE policy to specify the parameters to be used during an IKE negotiation to create the IKE SA.
	`priority` uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 10,000, with 1 being the highest priority and 10,000 the lowest.

NOTE: You can configure multiple IKE policies. When the IKE negotiation begins, it tries to find a common policy configured on both peers, starting with the highest-priority policies as specified on the remote peer.

NOTE: Use the `show crypto isakmp policy` command to verify the IKE settings.

Configurable IKE parameters include the following:

- Authentication (default = RSA signatures)
- Encryption (default = 56-bit DES)
- Hash (default = SHA-1)
- DH group (default = 768-bit DH)
- IKE SA lifetime (default = 86400 seconds [1 day])

Configure IKE policy Phase 1 parameters:

`Router(config-isakmp)#` `authentication {pre-share	rsa-encr	` `rsa-sig}`	Set the authentication method for the IKE policy.
`Router(config-isakmp)#encryption {des	3des` `	aes aes-bit}`	Set the encryption algorithm for the IKE policy. **NOTE** Encryption options may vary depending on IOS image.
`Router(config-isakmp)#hash {md5	sha}`	Set the hashing algorithm for the IKE policy.
`Router(config-isakmp)#group {1	2	5}`	Set the DH group to use for the IKE policy.
`Router(config-isakmp)#lifetime seconds`	Configure the maximum amount of time an IKE SA can exist before it expires. Time values are from 60 to 86400 seconds (1 minute to 24 hours).

NOTE: If a parameter is not configured, the default value will be used for that parameter.

Specify the PSK and identify the peer address (or hostname):

`Router(config)#`**`crypto isakmp key`** *`pre-shared-key`* {**`address`** *`address`* | **`hostname`** *`hostname`*}	Set the PSK for the remote peer and identify the peer by IP address or hostname. (Domain Name System [DNS] must be enabled.)

> **NOTE:**   This PSK must be identical on both peers.

> **NOTE:**   Use the `show crypto isakmp key` command to list PSKs.

Create the IPsec policy required for Phase 2:

`Router(config)#`**`crypto ipsec transform-set`** *`transform-name transform1`* [*`transform2`*] [*`transform3`*] [*`transform4`*]	Define the IPsec transform set and settings. A transform set specifies one or two IPsec security protocols (either Authentication Header [AH], Encapsulation Security Protocol [ESP], or both) and specifies which algorithms to use with the selected security protocol.

You may specify up to four *transforms*:

- ESP encryption transform set options include `esp-des`, `esp-3des`, or `esp-aes`.
- ESP authentication transform set options include `esp-md5-hmac` or `esp-sha-hmac`.
- (Optional) AH options transform set includes `ah-md5-hmac` or `ah-sha-hmac`.
- (Optional) IP compression transform set option is `comp-lzs`.

> **NOTE:**   You can specify just an ESP encryption transform set or the ESP encryption transform set and an ESP authentication transform set.

> **NOTE:**   When configuring AES encryption options, you must also specify a key length (128 bits, 192 bits, or 256 bits).

> **NOTE:**   After you issue the `crypto ipsec transform-set` command, you are put into the crypto transform configuration mode. While in this mode, you can change the mode to tunnel or transport. (Tunnel is the default.)

NOTE: Changes to transform sets are not applied to existing SAs but are used in subsequent negotiations to establish new SAs. To force the settings sooner, clear all or part of the SA database by using the `clear crypto sa` command.

NOTE: Use the `show crypto ipsec transform-set` command to verify the IPsec settings.

Create the crypto map specifics:

Router(config)#**crypto map** *map-name sequence-number* **ipsec-isakmp**	Define the site-to-site IPsec VPN crypto map settings.

NOTE: Other options are available, but the focus of this chapter is on IPsec and ISAKMP crypto map definitions.

Configurable site-to-site VPN crypto map parameters include the following:

- Identify the remote peers.
- Identify the transform set to use.
- Identify interesting traffic.

NOTE: Other options can be configured, but these are typical for site-to-site VPNs.

Configure crypto map specifics:

Router(config-crypto-map)# **description** *description*	Add the description to the crypto map.
Router(config-crypto-map)#**set peer** *peer-ip*	Specify an IPsec peer. **NOTE:** You can identify multiple peers using separate commands.
Router(config-crypto-map)#**set transform-set** *transform-name1* [*transform-name2 ... transform-name6*]	Specify which transform sets can be used with the crypto map entry. **NOTE:** You can identify up to six transform sets in one command.
Router(config-crypto-map)#**match address** *crypto-acl*	Assign an extended access list to a crypto map entry that will be used by IPsec to determine which traffic should be protected by crypto and which traffic does not need crypto protection. **NOTE:** Traffic that is permitted by the access list will be protected. Traffic that is denied by the access list will not be protected in the context of the corresponding crypto map entry.

Identify interesting traffic using an extended access control list (ACL). The ACL identifies when source traffic going to a destination network should enable the VPN tunnel. The extended ACL can be numbered or named.

> **NOTE:**   The extended ACLs between peers should be reciprocal (for example, on Peer-A, source-A to destination-B and on Peer-B, source-B to destination-A).

Apply the crypto map to an interface:

`Router(config)#`**`interface`** `type number`	Specify the interface type and number.
`Router(config-if)#`**`crypto map`** `crypto-map-name`	Apply a previously defined crypto map set to an interface.

Verifying the VPN Tunnel

To verify the site-to-site VPN configuration, use the following commands.

To verify IKE phase status, use these commands:

`Router#`**`show crypto isakmp policy`**	Display configured IKE policies.
`Router#`**`show crypto isakmp sa`** [**`active`**]	Display the status of the IKE phase 1 SAs.

> **NOTE:**   The `show crypto isakmp sa` command displays the state and status of Phase 1. A state of QM_IDLE is considered normal for an established Phase 1 tunnel.

To verify IKE Phase 2 status, use these commands:

`Router#`**`show crypto isakmp transform-set`**	Display configured IPsec transform sets.
`Router#`**`show crypto map`**	Display configured crypto maps.
`Router#`**`show crypto ipsec sa`**	Display established IPsec tunnels.

To test a tunnel, complete these steps:

1. Clear the IPsec SAs using the `clear crypto sa` command.

2. Issue the `show crypto ipsec sa` command to verify that the counters have been cleared.

3. Create interesting traffic using an extended ping such as `ping` `destination-network-ip` **`source`** `source-network-ip`.

4. Issue the `show crypto ipsec sa` command to verify that the counters have increased.

Configuring a Site-to-Site IPsec VPN Using IOS Example

This example establishes a site-to-site VPN between R1 and R3, protecting traffic that travels between the two LAN segments. A strong cipher suite is required, using PSKs, AES 128-bit, and SHA.

Figure 17-1 shows the network topology for the site-to-site VPN example.

Figure 17-1 Network Topology for Site-to-Site IPsec VPN Example

Create IKE policy 1 and configure the required Phase 1 parameters:

R1(config)#**crypto isakmp policy 1**	Define the IKE policy settings.
R1(config-isakmp)#**authentication pre-share**	Set the authentication method for the IKE policy.
R1(config-isakmp)#**encr aes 128**	Set the encryption algorithm for the IKE policy.
R1(config-isakmp)#**hash sha**	Set the hashing algorithm for the IKE policy.
R1(config-isakmp)#**group 5**	Set the DH group to use for the IKE policy.
R1(config-isakmp)#**lifetime 86400**	Set the IKE SA expiration timer to 24 hours.
R1(config-isakmp)#**exit**	Return to global configuration mode.

Specify the PSK and identify the peer address (or hostname):

R1(config)# **crypto isakmp key cisco123 address 209.165.202.129**	Set the PSK for the R3 peer.

Create the IPsec policy required for Phase 2:

`R1(config)#`**`crypto ipsec transform-set R1-to-R3-SET esp-sha-hmac esp-aes 128`**	Define the IPsec transform set and settings.
`R1(cfg-crypto-trans)#`**`exit`**	Return to global configuration mode.

Create the crypto map specifics:

`R1(config)#`**`crypto map R1-to-R3-MAP 1 ipsec-isakmp`**	Define the site-to-site IPsec VPN crypto map settings.
`R1(config-crypto-map)#`**`description Create a site-to-site VPN when going from R1 LAN to R3 LAN`**	Document the crypto map.
`R1(config-crypto-map)#`**`set transform-set R1-to-R3-SET`**	Identify the transform set to use with this crypto map.
`R1(config-crypto-map)#`**`set peer 209.165.202.129`**	Identify the peer to use with this crypto map.
`R1(config-crypto-map)#`**`match address VPN-ACL`**	Identify the crypto ACL to use with this crypto map.
`R1(config-crypto-map)#`**`exit`**	Return to global configuration mode.

Create the crypto ACL to identify interesting traffic:

`R1(config)#`**`ip access-list extended VPN-ACL`**	Create a named extended ACL.
`R1(config-ext-nacl)#`**`remark IPSec Rule`**	Provide ACL documentation.
`R1(config-ext-nacl)#`**`permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255`**	Identify the interesting traffic.
`R1(config-ext-nacl)#`**`exit`**	Return to global configuration mode.

Apply the crypto map to an interface:

`R1(config)#`**`interface s0/0/0`** `R1(config-if)#`**`crypto map R1-to-R3-MAP`**	Specifies the interface type and number.

Configuring a Site-to-Site IPsec VPN Using CCP Example

You can use CCP wizards to simplify the process of configuring the site-to-site VPN.

Launch the Site-to-Site Wizard for R1 and choose **Configure > Security > VPN > Site-to-Site VPN** to display the VPN screen (see Figure 17-2).

Figure 17-2   VPN Screen

From this screen, you can create a site-to-site VPN or edit a VPN configuration.

The Create Site to Site VPN tab includes two types of wizard:

Create a Site to Site VPN	This option enables you to create a VPN network connecting two routers.
Create a Secure GRE Tunnel (GRE-over-IPsec)	This option enables you to configure a generic routing encapsulation (GRE) protocol tunnel between your router and a peer device.

Select **Create a Site to Site VPN** and click the **Launch the Selected Task** button.

The wizard displays the window shown in Figure 17-3.

Figure 17-3   Site-to-Site VPN Wizard Window

The wizard provides two configuration options:

Quick Setup	■ Cisco Configuration Professional (CCP) automatically provides a default IKE policy, a default transform set, and a default IPsec rule.
	■ Quick setup is best suited when both peers are Cisco CCP routers.
	■ Quick setup configures Triple Digital Encryption Standard (3DES) encryption (or DES).
	■ If AES or SEAL is required, use the Step by Step Wizard.
Step by Step Wizard	■ Configure a site-to-site VPN using parameters that you specify.
	■ The result is a custom configuration for the VPN, allowing the use of any of the CCP settings available.
	■ The Step by Step Wizard enables you to specify stronger encryption than the Quick Setup Wizard allows.

Select the **Step by Step Wizard** and click **Next**.

The VPN Connection Information opens, as shown in Figure 17-4.

Figure 17-4   VPN Connection Information Window

In this window, identify the IP address or hostname of the remote site that will terminate the VPN tunnel that you are configuring. Specify the router interface to use, and enter the PSK that both routers will use to authenticate each other.

> **NOTE:**   The PSK must be the same on each VPN peer. Question marks (?) and spaces must not be used in the PSK. The PSK can contain a maximum of 128 characters. Optionally, you can configure digital certificates as the authentication option.

Click **Next** to continue.

The IKE Proposals window opens, as shown in Figure 17-5.

Figure 17-5   IKE Proposals Window

This window lists the default IKE policy and all other IKE policies configured. The local router uses the IKE policies that are listed in this window to negotiate authentication with the remote router.

> **NOTE:**   The peer devices must both use the same policy.

From this window, you can add or edit an IKE policy.

> **NOTE:**   The CCP default policy is read-only and cannot be edited.

To add an IKE policy that is not included in this list, click **Add**.

> **NOTE:**   Adding a new policy creates a new line with a higher priority number in the IKE policy list.

The Add IKE Policy dialog opens, as shown in Figure 17-6.

Figure 17-6 Add IKE Policy Dialog

The Add IKE Policy dialog appears as shown on the left of Figure 17-6. The priority can be altered and the cipher suite can be defined. You can also define the key lifetime.

After the new IKE policy has been configured, as shown in the right of Figure 17-6, click **OK**, and the revised IKE Proposals window now displays the new policy, as shown in Figure 17-7.

Figure 17-7 Revised IKE Proposals Window

Click **Next** to continue.

The Transform Set window opens, as shown in Figure 17-8.

Figure 17-8   Transform Set Window

The next step is to define the transform sets, which identify the cipher suite for IPsec Phase 2. A transform describes a particular security protocol with its corresponding algorithm that the peers agree to use for protecting a particular data flow.

CCP displays the default transform set and any additional transform sets that have been configured on this router.

> **NOTE:**   The CCP default policy is read-only and cannot be edited.

> **NOTE:**   Not all routers support all transform sets (encryption types). Unsupported transform sets will not appear in the screen.

> **NOTE:**   Not all IOS images support all the transform sets that CCP supports. Transform sets unsupported by the IOS image will not appear in the screen.

A list of all configured transform sets is available in the Select Transform Set drop-down menu. Choosing one enables you to view the settings and add entries to the transform set. Clicking **Add** creates the transform set in the Add Transform Set window. You can also edit nondefault transform sets.

To add an IPsec transform set that is not included in this list, click **Add**.

The Add Transform Set dialog opens, as shown in Figure 17-9.

Figure 17-9 Add Transform Set Dialog

> **NOTE:** The types of ESP encryption available depend on the router. Depending on the type of router you are configuring, one or more of these encryption types might not be available.

The Add Transform Set dialog appears as shown on the left of Figure 17-9. You must name the transform set (no spaces) and select ESP encryption and integrity algorithms.

> **NOTE:** Clicking the **Show Advanced >>** button enables you to select AH, transport, or tunnel mode (tunnel is the default) and compression.

After the new transform set has been configured, as shown on the right of Figure 17-9, click **OK**, and the revised Transform Set window now displays the new policy, as shown in Figure 17-10.

Figure 17-10 Revised Transform Set Window

Click **Next** to continue.

The Traffic to Protect window opens.

From this window, you define interesting traffic that this VPN protects.

The VPN can protect traffic between

- Specified subnets
- Traffic that is specified in an IPsec rule

NOTE: An IPsec rule provides more granularity because you can specify multiple subnets and hosts.

Figure 17-11 shows a revised Traffic to Protect window.

Figure 17-11   Revised Traffic to Protect Window

Click **Next** to continue.

The summary of the configuration displays, enabling you to review and accept the configuration.

You can review the configuration in this window and use the **Back** button to make changes if you want, or you can click **Finish** to complete the wizard.

> **NOTE:** A testing option is available by checking the **Test VPN Connection After Configuring** check box. The results of the test are shown in another window.

Use the **Back** button to edit a selected choice. Otherwise, click on **Finish**.

CCP then displays the CLI configuration commands. Click **Deliver** to commit the configuration changes.

Once the commands are delivered, you return to the VPN screen with the Edit Site to Site VPN tab selected, as shown in Figure 17-12.

Figure 17-12   Revised VPN Screen

You can verify the VPN configuration with the **Edit Site Site VPN** option. Use this window to manage the VPN connections to remote systems.

The Status column shows the status of the connection, which is indicated by the intuitive icons.

You can also create, edit, and delete VPN connections and reset existing connections.

The Generate Mirror and Test Tunnel buttons are also available in this window. Site-to-site VPNs require both sides to be configured with matching policies. Usually, the same process that is configured by the wizard has to be replicated on the other peer.

CCP provides these two convenient features to help configure the remote peer and test the tunnel.

> **NOTE:** Click **Test Tunnel** after each peer has been configured.

Generating a Mirror Configuration Using CCP

To generate a mirror configuration that you can use as a template for the other peer, click the **Generate Mirror** button. The resulting configuration provides identical IPsec policy names, IKE policies, and transform sets.

To generate a template configuration for the peer VPN router, choose **Configure > Security > VPN > Site-to-Site VPN > Edit Site-to-Site VPN**.

Select the VPN connection that you want to use as a template, and click **Generate Mirror**.

CCP displays the Generate Mirror dialog shown in Figure 17-13.

Figure 17-13   Generate Mirror Dialog

> **CAUTION:**   Do not apply the mirror configuration to the peer device without editing! This configuration is a template that requires additional manual configuration. Use it only as a starting point to build the configuration for the VPN peer.

The suggested configuration for the identified peer device appears on the Generate Mirror dialog.

Click **Save** to display the Windows Save File dialog, and save the file as a text file.

Open the resulting text file using a text editor such as Notepad and make any needed changes to the template configuration. Figure 17-14 highlights sections of a sample configuration that should be verified or altered.

Figure 17-14   Generated Text File in Notepad

NOTE: The mirror configuration does not apply the crypto map to the peer interface. Therefore, the `crypto map` *crypto-name* command must be configured on the peer VPN interface.

Finally, copy and paste the edited configuration to the remote peer global configuration. The VPN tunnel should now be tested.

Testing and Monitoring IPsec VPNs

Navigate to **Configure > Security > VPN > Site-to-Site VPN > Edit Site-to-Site VPN** to open the VPN screen shown in Figure 17-12.

Click the **Test Tunnel** button, and then click **Start**. CCP generates interesting traffic and enables the VPN tunnel. CCP displays status messages indicating the results of the test, as shown in Figure 17-15.

Figure 17-15   VPN Troubleshooting Window

TIP: Click **Details** to see detailed results.

When prompted to enable debugging, click **Yes**.

This opens another VPN Troubleshooting window, as shown in Figure 17-16.

Figure 17-16   VPN Troubleshooting Window

Enter an IP address on the destination network and click **Continue**.

Eventually, CCP reports on the VPN status. If successful, a message appears indicating that the VPN tunnel is up. Otherwise, an error message appears. Troubleshoot as necessary.

> **TIP:**   If an error is generated, compare each peer's running configuration.

Monitoring Established IPsec VPN Connections Using CCP

CCP monitoring is streamlined by using the **VPN Status** option shown in Figure 17-17.

Choose **Monitor > Security > VPN Status**.

Figure 17-17   VPN Status Screen

This window displays a tree of VPN connections that are possible on the router, including all types of VPNs (remote access, site to site, and others).

> **NOTE:**   Site-to-site tunnels are displayed as IPsec tunnels.

This group displays statistics about each IPsec VPN that is configured on the router. Each row in the table represents one IPsec VPN. This window showcases the Monitoring Tunnel and Test Tunnel options, which are essential to the troubleshooting process.

> **TIP:**   You have to click **Update** to refresh the IPsec tunnel table and display the most current data from the router.

This page intentionally left blank

This chapter covers the following topics:

Adaptive Security Appliance

- ASA Models

- Routed and Transparent Firewall Modes

- ASA Licensing

Basic ASA Configuration

- ASA 5505 Front and Back Panel

- ASA 5510 Front and Back Panel

- ASA Security Levels

- ASA 5505 Port Configuration

- ASA 5505 Deployment Scenarios

- ASA 5505 Configuration Options

Adaptive Security Appliance

Cisco offers firewall solutions using a firewall-enabled Integrated Services Router (ISR) or using the Cisco Adaptive Security Appliance (ASA) comprehensive firewall solution. The ASA is a primary component of the Cisco Secure Borderless Network and provides superior scalability, a broad range of technology and solutions, and effective always-on security.

The ASA combines the following features into one platform:

Stateful firewall	■ An ASA provides stateful firewall services tracking the TCP or UDP network connections traversing it.
	■ Only packets matching a known active connection are allowed by the firewall; others are rejected.
VPN concentrator	■ The ASA supports IPsec and Secure Sockets Layer (SSL) remote access and IPsec site-to-site virtual private network (VPN) features.

Intrusion prevention	■ Most ASA models support basic intrusion prevention system (IPS) features.
	■ Advanced threat control is provided by adding the Cisco Advanced Inspection and Prevention Security Services Module (AIP-SSM) and Cisco Advanced Inspection and Prevention Security Services Card (AIP-SSC).
Virtualization	■ A single ASA can be partitioned into multiple virtual devices called security contexts.
	■ Each context is an independent device, with its own security policy, interfaces, and administrators.
	■ Most IPS features are supported except VPN and dynamic routing protocols.
High availability	■ Two ASAs can be paired into an active/standby failover configuration to provide device redundancy.
	■ One ASA is the primary (active) device, while the other is the secondary (standby) device.
	■ Both ASAs must have identical software, licensing, memory, and interfaces.
Identity firewall	■ The ASA can provide access control using Windows Active Directory login information.
	■ Identity-based firewall services allow users or groups to be specified instead of being restricted by traditional IP address-based rules.
Threat control	■ Along with integrated IPS features, additional antimalware threat control capabilities are provided by adding the Content Security and Control (CSC) module.

NOTE: This section focuses on the ASA firewall and remote-access VPN features.

ASA Models

There are six ASA models, ranging from the basic 5505 branch office model to the 5585 data center version. The choice of ASA model will depend on an organization's requirements, such as maximum throughput, maximum connections per second, and budget:

ASA 5505	■ Small business, branch office, and enterprise teleworker solution providing a maximum of 150-Mbps throughput
ASA 5510	■ Small, medium-sized business and branch office solution providing a maximum of 300-Mbps throughput
ASA 5520	■ Branch solution providing a maximum of 450-Mbps throughput
ASA 5540	■ Medium-sized, large enterprise and service-provider network solution providing a maximum of 650-Mbps throughput

ASA 5550	■ Campus, enterprise edge, and data center solution providing a maximum of 1.2-Gbps throughput
ASA 5585	■ Large enterprise and data center solution providing a maximum of 40-Gbps throughput

NOTE: For the Cisco ASA 5505, the default DRAM memory is 256 MB (upgradable to 512 MB), and the default internal flash memory is 128 MB.

NOTE: This section focuses on the ASA 5505.

Routed and Transparent Firewall Modes

Two firewall modes of operation are available on ASA devices:

Routed mode	■ The traditional mode for deploying a firewall.
	■ Two or more interfaces that separate Layer 3 networks.
	■ The ASA is a router hop in the network and can perform Network Address Translation (NAT) between connected networks.
	■ Routed mode supports multiple interfaces, and each interface is on a different subnet and requires an IP address on that subnet.
Transparent mode	■ The ASA functions like a Layer 2 device.
	■ Also referred to as a *bump in the wire* or a *stealth firewall*.
	■ The ASA requires only one management IP address configured in global configuration mode.
	■ Transparent mode does not support dynamic routing protocols, VPNs, quality of service (QoS), or Dynamic Host Control Protocol (DHCP) Relay.

NOTE: This section focuses on routed mode.

ASA Licensing

The ASA 5505 security appliance comes preinstalled with either a Base license or a Security Plus license, the latter supporting a higher connection capacity, full demilitarized zone (DMZ) capabilities, VLAN trunking, and high-availability features.

You can verify license information using the `show activation-key` or the `show version` command:.

```
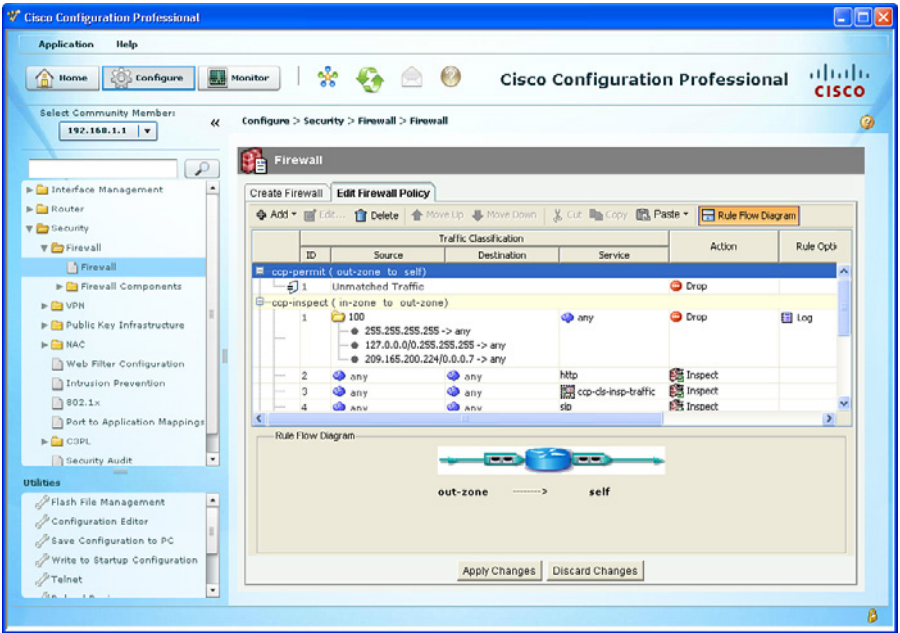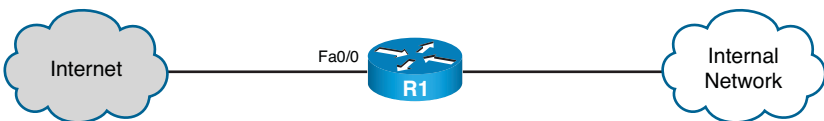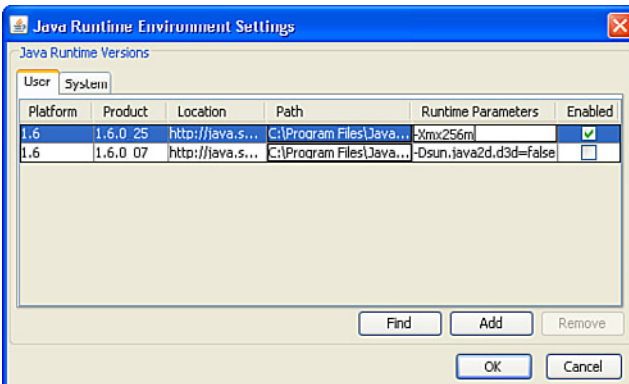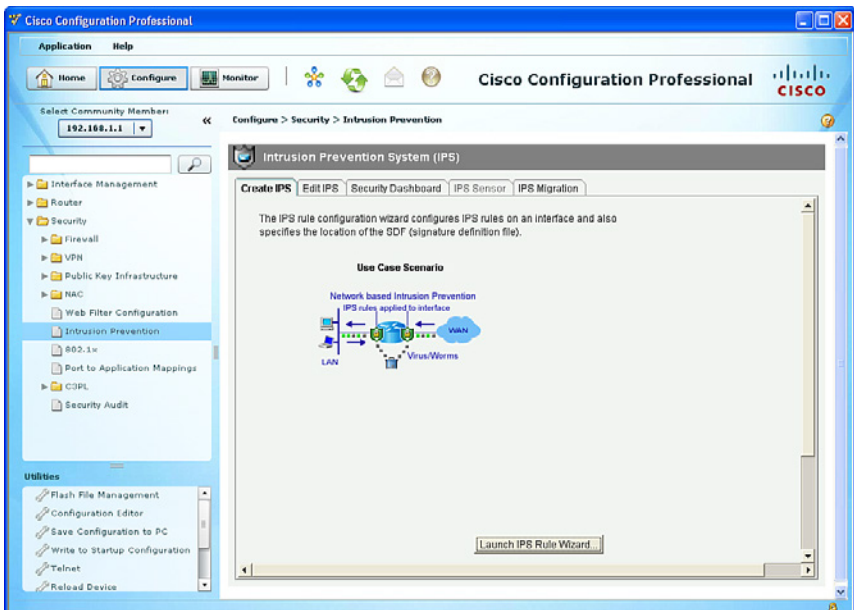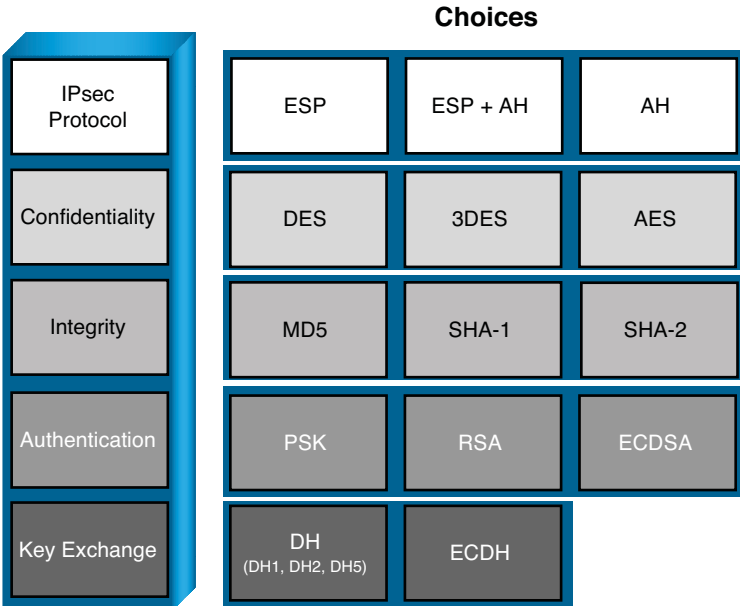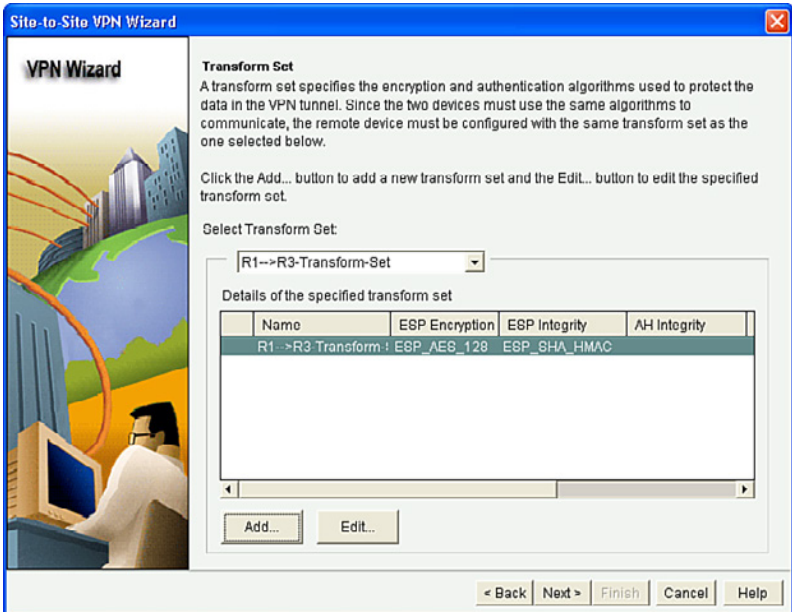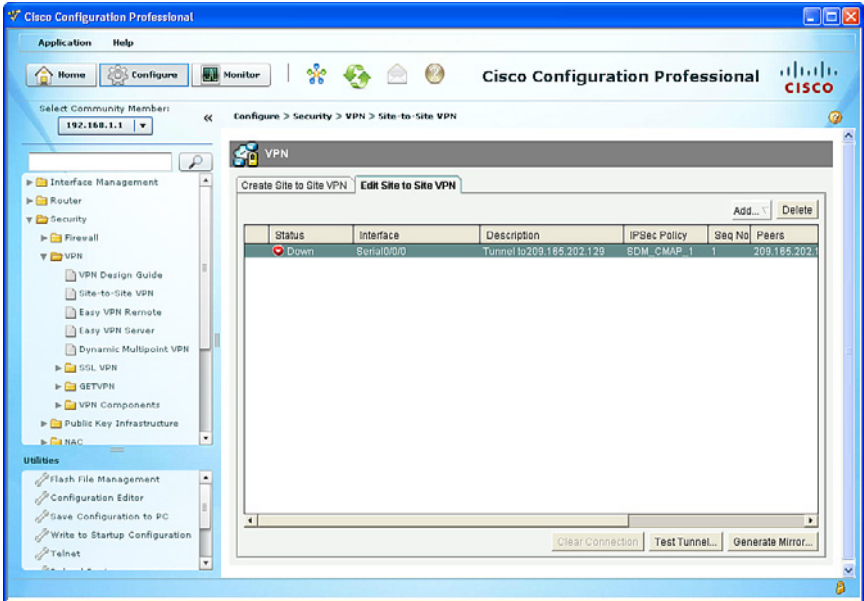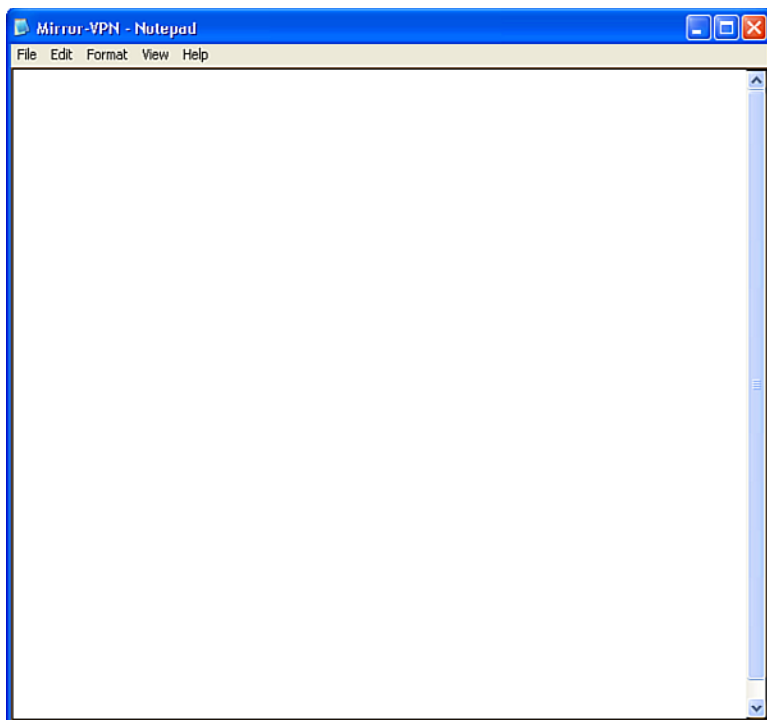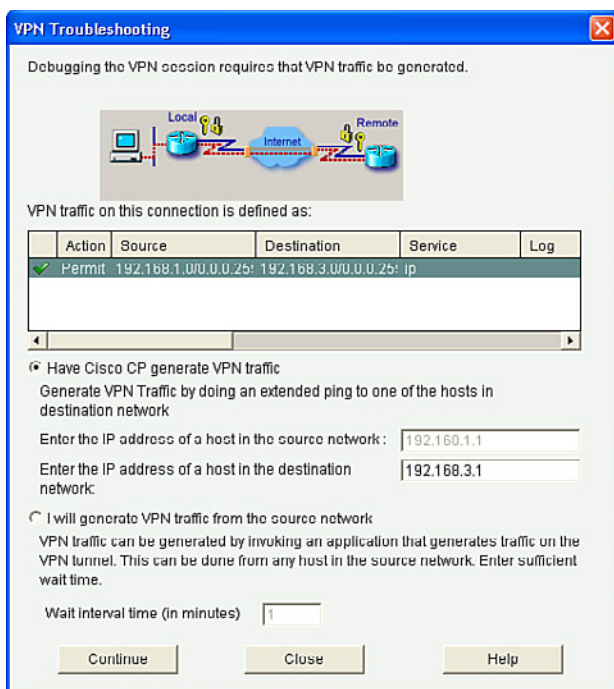ciscoasa# show version

<Output omitted>
```

```
Licensed features for this platform:
Maximum Physical Interfaces     : 8              perpetual
VLANs                           : 3              DMZ Restricted
Dual ISPs                       : Disabled       perpetual
VLAN Trunk Ports                : 0              perpetual
Inside Hosts                    : 10             perpetual
Failover                        : Disabled       perpetual
VPN-DES                         : Enabled        perpetual
VPN-3DES-AES                    : Enabled        perpetual
AnyConnect Premium Peers        : 2              perpetual
AnyConnect Essentials           : Disabled       perpetual
Other VPN Peers                 : 10             perpetual
Total VPN Peers                 : 25             perpetual
Shared License                  : Disabled       perpetual
AnyConnect for Mobile           : Disabled       perpetual
AnyConnect for Cisco VPN Phone  : Disabled       perpetual
Advanced Endpoint Assessment    : Disabled       perpetual
UC Phone Proxy Sessions         : 2              perpetual
Total UC Proxy Sessions         : 2              perpetual
Botnet Traffic Filter           : Disabled       perpetual
Intercompany Media Engine       : Disabled       perpetual


This platform has a Base license.


Serial Number: JMX15364077
Running Permanent Activation Key: 0x970bc671 0x305fc569 0x70d21158
0xb6ec2ca8 0x8a003fb9
Configuration register is 0x41 (will be 0x1 at next reload)
Configuration last modified by enable_15 at 10:03:12.749 UTC Fri Sep 23
2011
ciscoasa#
```

> **NOTE:**   Additional optional licenses (for example, AnyConnect Premium license) or time-based (for example, Botnet Traffic Filter license) can be purchased.

> **NOTE:**   Preinstalled licenses combined with additional licenses create a permanent license that needs to be activated using the `activation-key` command. The product activation key is purchased from a Cisco account representative.

Basic ASA Configuration

ASA 5505 Front and Back Panel

Figure 18-1 shows the front panel of the ASA 5505.

Figure 18-1   ASA 5505 Front Panel

The front panel of the ASA 5505 features as numbered in Figure 18-1 are as follows:

1	**USB port**	■ Can be used to enable additional services and capabilities.
2	**Speed and link activity LEDs**	■ When the 100-Mbps LED is a solid green, it indicates 100 Mbps; otherwise, it indicates 10 Mbps. ■ A solid LINK/ACT LED indicates an established network link, and a blinking LED indicates network activity.
3	**Power LED**	■ Solid green indicates that the appliance is powered on.
4	**Status LED**	■ A blinking green LED indicates that the system is booting and power-up tests are running. ■ Solid green indicates that the system tests passed and the system is operational. ■ Solid amber indicates that the system tests failed.
5	**Active LED**	■ Green indicates that the Cisco ASA is providing failover.
6	**VPN LED**	■ Solid green indicates that a VPN tunnel is active.
7	**SSC LED**	■ Solid green indicates that a Security Services Card (SSC) is present in the SSC slot.

Figure 18-2 shows the back panel of the ASA 5505.

Figure 18-2   ASA 5505 Back Panel

The back panel of the ASA 5505 features as numbered in Figure 18-2 are as follows:

1	**Power connector**	■ Requires a 48 VDC adapter.
2	**SSC slot**	■ Can add IPS features using the Cisco Advanced Inspection and Prevention Security Services Card (AIP-SSC).
3	**Console port**	■ To initially configure the appliance.
4	**Lock slot**	■ To physically secure the appliance.
5	**Reset button**	■ The Reset button is disabled by default.
6	**USB ports**	■ A total of three USB ports can be used to enable additional services and capabilities (two USB ports on the back and one on the front).
7 - 8	**Eight-port Fast Ethernet switch**	■ Each port can be grouped to create up to three separate VLANs (or zones) to support network segmentation and security. ■ Ports 6 and 7 are Power over Ethernet (PoE) ports.

ASA 5510 Front and Back Panel

The ASA 5510 supports 300-Mbps throughput and 9,000 firewall connections per second capacity, making it very suitable for most office deployments. Cisco ASA 5510, 5520, 5540, and 5550 are all one-rack units (1RUs). Each of these has an expansion slot for security-services modules (SSMs). The front panel of the ASA 5510 features Power, Status, Active, VPN, and Flash LEDs. The ASA 5510 front panel and back panel are highlighted in Figure 18-3.

Figure 18-3   ASA 5510 Front and Back Panel

The back panel of the ASA 5510 features as numbered in Figure 18-3 are as follows:

1	SSM	■ The SSM can be used to add the following: ■ 4-Port Gigabit Ethernet Security Services Module (4GE SSM) ■ Advanced Inspection and Prevention Security Services Module (AIP-SSM) ■ Series Content Security and Control Security Services Module (CSC-SSM)
2	USB ports	■ Two USB ports can be used to enable additional services and capabilities.
3	OOB management interface	■ A dedicated Fast Ethernet out-of-band (OOB) management interface.
4	Four Fast Ethernet interfaces	■ By default, interfaces Fa0/0 through Fa0/2 are enabled, but the Fa0/3 is disabled. ■ The OOB interface could also be used as a fifth Fast Ethernet port (ASA software must support).
5	Flash card slot	■ Provides storage for system images and configuration files.
6	LED indicators	■ Power, Status, Active, VPN, and Flash LED indicators.
7	Management ports	■ A console port for the initial configuration. ■ An auxiliary port could be used for OOB management.

ASA Security Levels

The building blocks of ASA security are assigning interfaces to security levels to distinguish between inside (trusted) and outside (untrusted) networks:

- Security levels define the level of trustworthiness of an interface.
- The higher the level, the more trusted the interface.

- The security level numbers range between 0 (untrustworthy) to 100 (very trust-worthy).

- Each operational interface must have a name and a security level from 0 (lowest) to 100 (highest) assigned.

Figure 18-4 illustrates the default ASA security policy.

Figure 18-4   Default ASA Security Policy

The default security policy on an ASA 5505 is as follows:

- Traffic that is sourced from the Inside network (security level 100) and going into either the DMZ (security level 50) or the Outside network (security level 0) is allowed and inspected. Return traffic is allowed due to the stateful packet inspection.

- Traffic sourced from the DMZ network and going into the Inside network is denied.

- Traffic that is sourced from the Outside network and going into either the DMZ or the Inside network is denied by default.

NOTE: Any exception to this default behavior requires the configuration of access control lists (ACLs) to explicitly permit traffic from an interface with a lower security level to an interface with a higher security level (for example, Outside to DMZ).

ASA 5505 Port Configuration

The ASA 5510 devices or later have Layer 3 routed interfaces. The interfaces are enabled by assigning an IP address, interface name, and security level.

The ASA 5505 is configured differently than higher models because it does not have any Layer 3 interfaces. It comes with an integrated eight-port Layer 2 Fast Ethernet switch. Each port is individually assigned to a specific VLAN. All Layer 3 parameters (that is, IP address, interface name, and security level) must be configured for the VLAN interface also known as a switch virtual interface (SVI). Switch ports on the same VLAN can communicate with each other using hardware switching.

ASA 5505 Deployment Scenarios

The ASA 5505 is commonly used as an edge security device that connects a small business to an ISP to access the Internet. It can be deployed as follows:

Small branch deployment	■ The ASA 5505 can be deployed with 2 security zones:
	  ■ VLAN 1 with security level 100 for inside hosts
	  ■ VLAN 2 with security level 0 for the Internet connection

Small business deployment	■ The ASA 5505 can be deployed with 3 security zones:
	  ■ VLAN 1 for the inside network connecting workstations
	  ■ VLAN 2 for the outside network connecting to the Internet
	  ■ VLAN 3 for the DMZ connecting to a company web servers

Enterprise deployment	■ The ASA 5505 can be used by telecommuters and home users to connect to a centralized location using a VPN.

ASA 5505 Configuration Options

ASA devices can be configured and managed using either the

- Command-line interface (CLI) required for initial ASA deployment and maintenance
- Adaptive Security Device Manager (ASDM) GUI

NOTE: ASDM simplifies the deployment and maintenance of an ASA.

This page intentionally left blank

This chapter covers the following topics:

Adaptive Security Device Manager

- Accessing ASDM
- Factory Default Settings
- Resetting the ASA 5505 to Factory Default Settings
- Erasing the Factory Default Settings
- Setup Initialization Wizard

Installing and Running ASDM

- Running ASDM

ASDM Wizards

- The Startup Wizard
- VPN Wizards
- Advanced Wizards

Adaptive Security Device Manager

Cisco Adaptive Security Device Manager (ASDM) is a Java-based GUI tool that facilitates the setup, configuration, monitoring, and troubleshooting of Cisco Adaptive Security Appliances (ASA).

> **NOTE:** ASDM is now preloaded in flash memory on any ASA Versions 7.0 and later.

ASDM can be

- Run from a browser as a Java Web Start application that is dynamically downloaded from the ASA flash, allowing an administrator to configure and monitor that ASA device
- Downloaded from flash and installed locally on a host as an application, allowing an administrator to use ASDM to configure and manage multiple ASA devices

Accessing ASDM

ASDM access requires connecting to a management interface that has some minimal configurations to communicate over the network.

The management interface depends on the model of ASA:

- On an ASA 5505, the management switch port can be any port, except for Ethernet 0/0.

- On an ASA 5510 and later, the management interface is Management 0/0. However, another Fast Ethernet interface can also be used.

The minimal configuration can be provided on an ASA 5505 using any of the following methods:

Restore factory default settings	■ The ASA can be reset to provide a basic configuration that is sufficient for a small office/home office (SOHO) deployment. ■ The configuration includes two preconfigured VLAN networks, Dynamic Host Configuration Protocol (DHCP), and Network Address Translation (NAT) services.
Setup Initialization Wizard	■ The ASA interactively guides an administrator to config-ure the basic security settings to access ASDM. ■ Additional HTTP settings must be configured to access the ASDM.
CLI configuration	■ Configure all parameters using the command-line interface (CLI).

NOTE: The next chapter covers the CLI configuration method.

Factory Default Settings

The ASA 5505 with a Base license ships with the following default factory settings:

- A default hostname of ciscoasa.

- Console or enable passwords, which are blank.

- An inside VLAN 1 interface that includes the Ethernet 0/1 through 0/7 switch ports. The VLAN 1 IP address and mask are 192.168.1.1 and 255.255.255.0.

- An outside VLAN 2 interface that includes the Ethernet 0/0 switch port. VLAN 2 derives its IP address from the ISP using DHCP.

- The default route that is derived from DHCP.

- All inside IP addresses to be translated when accessing the outside using interface Port Address Translation (PAT).

- The HTTP server to support ASDM access.

- An internal DHCP server to provide addresses between 192.168.1.5 and 192.168.1.36 for hosts that connect to a VLAN 1 interface.

> **NOTE:**   You can change these settings manually using the CLI or interactively using either the CLI Setup Initialization Wizard or by using the ASDM Startup Wizard.

> **NOTE:**   The Reset button on the ASA 5505 is disabled and inoperable by default.

Resetting the ASA 5505 to Factory Default Settings

You can restore the ASA to its factory default configuration by using the following:

`ciscoasa#`**`config t`**	Enter global configuration mode.
`ciscoasa(config)#`**`config factory-default`**	Reset the ASA to factory default settings. **NOTE:** A warning appears stating that the boot system configuration (startup configuration) will be cleared. **NOTE:** The ASA loads a default configuration into the running configuration.
`ciscoasa(config)#`**`reload save-config noconfirm`**	Save the configuration and then reload the ASA without asking for confirmation.

Erasing the Factory Default Settings

`ciscoasa#`**`write erase`**	Erase the startup-configuration file.
`ciscoasa(config)#`**`reload noconfirm`**	Reload the ASA without confirmation.

Setup Initialization Wizard

When the default factory settings are erased and an ASA is reloaded, the ASA Setup Initialization Wizard prompts will eventually appear asking `Pre-configure Firewall now through interactive prompts [yes]?`

Answering **`no`** cancels the Setup Initialization Wizard, and the ASA displays its default prompt. In this case, you must manually configure the ASA via the CLI.

Pressing **Enter** accepts the default **`[yes]`**, and the ASA will interactively guide an administrator to configure basic ASA features, including the following:

- Firewall mode
- Enable password
- Enable password recovery
- Time and date settings
- Inside IP address and mask
- ASA device name
- Domain name

> **NOTE:**   The security appliance displays the default values in brackets ([ ]) before prompting the user to accept or change them. To accept the default input, press **Enter.**

When the interactive portion of the Setup Initialization Wizard completes, the security appliance displays the summary of the new configuration and prompts the user to save or reject the settings:

- Answering `yes` saves the configuration and displays the configured hostname prompt.

- Answering `no` restarts the Setup Initialization Wizard. Any changes previously made become the new default settings enabling an administrator to correct a misconfigured setting.

The Setup Initialization Wizard provides most of the settings for ASDM. However, the HTTP service must be enabled.

To allow access to ASDM, enable HTTPS connections from any host on the inside network:

ciscoasa#**http server enable**	Enable HTTP services.
ciscoasa(config)#**http** *ip-address network-mask interface-name*	Identify a host or hosts that can access the ASA HTTP server using ASDM.

> **NOTE:**   To remove and disable the ASA HTTP server service, use the global configuration command `clear configure http.`

Installing and Running ASDM

The ASDM interface can be accessed from any workstation with an IP address included in the HTTP trusted network list.

> **TIP:**   Before attempting to establish a secure ASDM connection to the ASA, verify that IP connectivity exists between the workstation and the Cisco ASA.

With a factory default configuration

- A host on the 192.168.1.0/24 network can connect to the ASA default management IP address of 192.168.1.1 using ASDM.

- The host must establish a connection through a browser to the inside interface IP address using the HTTPS protocol.

A security certificate window may appear. Depending on the browser settings, select **Yes** or click on **Continue to This Website** to continue to the ASDM launcher window.

The ASDM launcher appears, as shown in Figure 19-1.

Figure 19-1   Cisco ASDM Launcher Screen

The ASDM launcher window provides three choices:

Install ASDM Launcher and Run ASDM	▪ Install ASDM as an application on the Windows host.
	▪ The advantage is that the application can be used to manage several ASA devices.
	▪ An Internet browser will no longer be required to start ASDM.
Run ASDM	▪ Run ASDM as a Java Web Start application.
	▪ The advantage is that the ASDM is not locally installed.
	▪ An Internet browser is required to establish a connection.
Run Startup Wizard	▪ Run the ASDM Startup Wizard.
	▪ Similar to the Setup Initialization Wizard, it provides step-by-step windows to help initially configure the ASA.

NOTE: The recommended choice is to install ASDM locally on the host. For security reasons, you might want to simply run ASDM.

Running ASDM

Selecting the **Run ASDM** option opens an ASDM authentication window.

If you are starting ASDM for the first time after running a Startup Wizard, leave the fields empty. If Secure Shell (SSH) has been configured, a local database username and password should be used.

When authentication is successful, the ASDM Home page appears, as shown in Figure 19-2.

Figure 19-2   ASDM Home Page

The Cisco ASDM Home page is updated every 10 seconds and provides a quick view of the operational status of the ASA. The ASDM GUI includes the following elements:

Menu bar	■ Provides quick access to files, tools, wizards, and help.
Toolbar	■ Provides easy navigation of Cisco ASDM.
	■ From the toolbar, an administrator can access the Home, Configuration, and Monitoring views and can save, refresh, navigate between views, and access Help.
Device List button	■ Opens a dockable page that lists other ASA devices.
	■ Use this page to switch to another device running the same version of ASDM.
	■ When managing only one ASA device, the Device List page is hidden and must be opened using the Device List button.

Status bar	■ Displays the time, connection status, user, memory status, running configuration status, privilege level, and SSL status at the bottom of the application window.

The Home page also displays two to four tabs:

Device Dashboard	■ (Default) Provides a view of important information about the ASA, such as the status of interfaces, the OS version, licensing information, and performance-related information.
Firewall Dashboard	■ (Default) Provides security-related information about traffic that passes through the ASA, such as connection statistics, dropped packets, and scan and syn attack detection.
Intrusion Prevention	■ Appears only if an Intrusion Prevention System (IPS) module or card is installed. ■ The additional tab displays status information about the IPS software.
Content Security	■ Appears only if a Content Security and Control Security Services Module (CSC-SSM) is installed in the ASA. ■ The Content Security tab displays status information about the CSC-SSM software.

The Configuration and Monitoring views also feature a dockable navigation pane that you can maximize, restore, or make float so that it can be moved, hidden, or closed. The navigation pane of the Configuration view displays the following tabs:

- Device Setup
- Firewall
- Remote-Access VPN
- Site-to-Site VPN
- Device Management

The navigation pane of the Monitoring view displays the following tabs:

- Interfaces
- VPN
- Routing
- Properties
- Logging

NOTE: The options listed in the navigation pane will vary depending on the view and tab that is selected.

ASDM Wizards

Cisco ASDM offers several wizards to help simplify the configuration of the appliance:

- Startup Wizard
- Virtual private network (VPN) wizards
- Advanced wizards

The Startup Wizard

The Startup Wizard guides the administrator through the initial configuration of the ASA and helps to define basic settings.

Choose either **Wizards > Startup Wizard** or **Configuration > Device Setup > Startup Wizard** to open the configuration startup wizard screen (see Figure 19-3).

Figure 19-3   Configuration Startup Wizard Screen

After the Startup Wizard page appears, click the **Launch Startup Wizard** button.

> **NOTE:**   The actual number of steps in the wizard may vary depending on the specific ASA model and modules installed. However, most ASA models can be configured in a nine-step process.

After the Startup Wizard has been launched, follow these steps:

1. The Starting Point window (also referred to as the Welcome window) is displayed and provides a choice to Modify an Existing Configuration or to Reset the Configuration to Factory Defaults.

2. In the Basic Configuration window, complete the basic ASA management configuration consisting of a hostname, domain name, and privileged EXEC password. Optionally, this step also allows the administrator to deploy the ASA for a remote worker.

3. In the Interface Selection window, create the VLAN switch interfaces. This and other VLAN-related steps are specific to the ASA 5505 model. The Startup Wizard for the ASA 5510 and later models provides steps to configure the Fast Ethernet routed interfaces as needed without the need for VLANs.

4. In the Switch Port Allocation window, map the physical Layer 2 switch ports to the logically named VLANs in the previous step. By default, all switch ports are assigned to VLAN 1 (Inside).

5. In the Interface IP Address Configuration window, identify the inside and outside IP addresses for the defined VLANs. Note that these addresses could also be created using DHCP or PPPoE.

6. The DHCP window allows the administrator to enable the DHCP service for inside hosts. All DHCP-related options are defined in this window.

7. The Address Translation (NAT/PAT) window allows the administrator to enable PAT or NAT.

8. In the Administrative Access window, specify which host or hosts are allowed to access the ASA using HTTPS/ASDM, SSH, or Telnet.

9. The final window is the Startup Wizard Summary. Review the proposed configuration. You can make changes by clicking the **Back** button or save by clicking the **Finish** button.

VPN Wizards

The various VPN wizards enable an administrator to configure basic site-to-site and remote-access VPN connections and assign either pre-shared keys or digital certificates for authentication.

To launch a VPN wizard from the menu bar, click **Wizards** and choose **VPN Wizards** (see Figure 19-4).

Figure 19-4 Available VPN Wizards

To complement the wizards, ASDM also provides the ASDM Assistant. To view the remote-access ASDM Assistant, choose **Configurations > Remote Access VPN > Introduction**, as shown in Figure 19-5.

Figure 19-5   Remote-Access ASDM Assistant

Advanced Wizards

Three other wizards are available in ASDM:

High Availability and Scalability Wizard	■ Guides an administrator to configure failover with high availability and VPN cluster load balancing. ■ VPN cluster mode requires two ASA devices establishing VPN sessions to the same destination network and performing load balancing.
Unified Communication Wizard	■ Used to configure the ASA to support the Cisco Unified Communications Proxy feature.
Packet Capture Wizard	■ Used to configure and run captures for troubleshooting errors and for validating a NAT policy. ■ The captures can use access lists to limit the type of traffic captured, the source and destination addresses and ports, and one or more interfaces. ■ The wizard runs one capture on each of the ingress and egress interfaces. ■ Captures can be saved to a host and examined in a packet analyzer.

NOTE: The three wizards listed here are beyond the scope of this chapter and so are not explored further.

Configuring Cisco ASA Basic Settings

This chapter covers the following topics:

ASA Command-Line Interface

- Differences Between IOS and ASA OS

Configuring Basic Settings

- Configuring Basic Management Settings
- Enabling the Master Passphrase

Configuring Interfaces

- Configuring the Inside and Outside SVIs
- Assigning Layer 2 Ports to VLANs
- Configuring a Third SVI

Configuring the Management Plane

- Enabling Telnet, SSH, and HTTPS Access
- Configuring Time Services

Configuring the Control Plane

- Configuring a Default Route

Basic Settings Example

- Configuring Basic Settings Example Using the CLI
- Configuring Basic Settings Example Using ASDM

ASA Command-Line Interface

The Adaptive Security Appliance (ASA) command-line interface (CLI) is a proprietary OS that has a similar look and feel to the router IOS. Like a Cisco IOS router, the ASA recognizes the following:

- Abbreviation of commands and keywords
- Using the Tab key to complete a partial command
- Using the help key (**?**) after a command to view additional syntax

Differences Between IOS and ASA OS

Unlike an ISR, the ASA

- Can execute any ASA CLI command regardless of the current configuration mode prompt and does not require or recognize the `do` IOS CLI command

- Can provide additional help listing a brief command description and syntax by using the EXEC command `help` followed by the CLI command (for example, `help reload`)

- Interrupts `show` command output by simply using the letter **Q** (unlike the **Ctrl+C** (**^C**) IOS CLI key sequence)

Although the ASA CLI uses many of the same commands as IOS, there are also many different ASA commands. The following partial list highlights common IOS router commands and the equivalent ASA CLI command:

IOS Router Command	Equivalent ASA Command
`enable secret` *password*	`enable password` *password*

`line con 0`
` password` *password*
` login`
	`passwd` *password*

`ip route`	`route outside`
`show ip interfaces brief`	`show interfaces ip brief`
`show ip route`	`show route`
`show vlan`	`show switch vlan`
`show ip nat translations`	`show xlate`
`copy running-config startup-config`	`write` [`memory`]
`erase startup-config`	`write erase`

NOTE: The listed IOS router commands are not available on an ASA device.

Configuring Basic Settings

To configure settings on an ASA 5505, follow these steps:

1. Configure basic management settings (that is, hostname, domain name, and enable password).

2. Enable the master passphrase.

3. Configure the Inside and Outside switch virtual interfaces (SVIs).

4. Assign Layer 2 ports to VLANs.

5. Enable Telnet, SSH, and HTTPS access.

6. Configure time services.

7. Configure a default route.

> **NOTE:**   Assume that the ASA startup configuration file has been erased and the device has been reloaded.

Enter privileged EXEC and then global configuration mode:

`Pre-configure Firewall now through` `interactive prompts [yes]?` **`no`**	At the Setup Initialization Wizard prompt, enter **no** to exit the wizard.
`ciscoasa>` **`enable`** `Password:`	Enter privilege EXEC mode. When prompted for the password, press **Enter**. **NOTE:** The default is no enable password. **NOTE:** If the ASA device is booted using the default factory settings, the password is cisco.
`ciscoasa#` **`configure terminal`**	Enter ASA global configuration mode.

> **NOTE:**   The first time global configuration mode is accessed, a message prompting you to enable the Smart Call Home feature appears. This feature offers proactive diagnostics and real-time alerts on select Cisco devices.

Configuring Basic Management Settings

Configure hostname, domain name, and privileged EXEC password:

`ciscoasa(config)#` **`hostname`** *`ASA-hostname`*	Configure the ASA hostname.
`ciscoasa(config)#` **`domain-name`** *`ASA-domain-name`*	Configure a domain name.
`ciscoasa(config)#` **`enable password`** *`password`*	Configure the privileged EXEC mode password. **NOTE:** There is no secret option.

Enabling the Master Passphrase

The master passphrase must be configured and enabled to encrypt all user passwords:

ciscoasa(config)# **key config-key password-encryption** [*new-passphrase* [*old-passphrase*]]	Create or change an existing master passphrase. **NOTE:** The passphrase must be 8 [nd] 128 characters in length, and all characters except a backspace and double quote are accepted. **NOTE:** If a new passphrase is not included in the command, the ASA prompts for it. **NOTE:** To change the passphrase, you must first enter the old pass-phrase.
ciscoasa(config)# **password encryption aes**	Enable password encryption.

NOTE: To determine whether password encryption is enabled, use the `show password encryption` command.

NOTE: Interfaces must be configured before Telnet, SSH, HTTPS, and static routes are configured.

Configuring Interfaces

On ASA 5510 and later, routed Ethernet interfaces are directly configured with IP configurations, much like an Integrated Services Router (ISR). However, the ASA 5505 has an integrated eight-port Layer 2 switch, and therefore IP configurations are accomplished by

- Configuring the inside and outside SVIs by assigning interface name, security level, and IP address
- Assigning Layer 2 ports to the inside and outside SVI VLANs
- (Optional) Configuring a third SVI if required

Configuring the Inside and Outside SVIs

ciscoasa(config)# **interface vlan** *vlan-id*	Create an SVI.

ciscoasa(config-if)# **nameif** {**inside** | **outside** | *name*}	Assign a name to the SVI interface. **NOTE:** Using the name **inside** automatically assigns a security level of 100. **NOTE:** Using the name **outside** automatically assigns a security level of 0.
ciscoasa(config-if)# **security-level** *level*	Assign or change the SVI security level. **NOTE:** All SVIs must be assigned a security level value. **NOTE:** Security levels are automatically assigned for inside and outside interfaces.
ciscoasa(config-if)# **ip address** *ip-address netmask*	Assign an IP address and mask to the SVI. **NOTE:** The ASA could also obtain its IP address and default route if it is configured as a Dynamic Host Configuration Protocol (DHCP) client or PPP over Ethernet (PPPoE) client.

NOTE: By default, an SVI is active and does not require the `no shutdown` command.

Assigning Layer 2 Ports to VLANs

The Layer 2 ports must be assigned to a VLAN.

NOTE: By default, all ports are members of VLAN 1.

Therefore, to change the default VLAN assignment, you must configure the Layer 2 port with the following commands:

ciscoasa(config)# **interface** *interface/number*	Specify a Layer 2 physical port.
ciscoasa(config-if)# **switchport access vlan** *vlan-id*	Change the VLAN assignment of the port from the default of VLAN 1.
ciscoasa(config-if)# **no shutdown**	Enable physical port.

NOTE: The Layer 2 port must be enabled and therefore requires the `no shutdown` command.

> **NOTE:** To verify VLAN settings, use the `show switch vlan` command. To verify interface settings, use the `show interface` or `show int ip brief` command.

> **NOTE:** ASA Fast Ethernet interfaces are designated as Ethernet x/x (for example, E0/0).

Configuring a Third SVI

An ASA 5505 with the Security Plus license automatically supports the creation of additional VLANs to create other zones such as a demilitarized zone (DMZ) zone. However, an ASA 5505 with a Base license only supports a third, *restricted* SVI that is limited from initiating contact to another specified VLAN.

Use the following to configure a third VLAN SVI on an ASA 5505 with a Base license:

`ciscoasa(config)# interface interface/number`	Specify a Layer 2 physical port.
`ciscoasa(config-if)# no forward interface vlan vlan-id`	Limit the interface from initiating contact to another VLAN. **NOTE:** The `vlan-id` argument specifies the VLAN ID to which this VLAN interface cannot initiate traffic. **NOTE:** You must configure this command before the interface is named. **NOTE:** Configure this command on the third SVI after the inside and outside VLAN interfaces have been configured.

Configuring the Management Plane

Enabling Telnet, SSH, and HTTPS Access

The ASA can be configured to accept Telnet connections from a single host or a range of hosts on the inside network. Use the following commands to enable the Telnet service:

`ciscoasa(config)# passwd password`	Configure the Telnet / SSH password.
`ciscoasa(config)# telnet ip-address subnet-mask interface-name`	Identify which inside hosts can telnet to which ASA interface.
`ciscoasa(config)# telnet timeout minutes`	Alters the default EXEC timeout of 5 minutes.

Alternatively, Telnet can be configured to use authentication, authorization, and accounting (AAA) authentication:

`ciscoasa(config)# username` *name* `password` *password*	Create a local database entry.
`ciscoasa(config)# aaa authentication telnet console LOCAL`	Configure Telnet to refer to the local database for authentication.

Secure Shell (SSH) is also supported, but it requires AAA authentication to be enabled. Use the following commands to enable SSH support:

`ciscoasa(config)# aaa authentication ssh console LOCAL`	Configure SSH to refer to the local database for authentication. **NOTE:** The `LOCAL` keyword is case sensitive and is a predefined server tag.
`ciscoasa(config)# crypto key generate rsa modulus` *modulus*	Generates the RSA key required for SSH encryption. **NOTE:** Valid modulus values include 512, 768, 1024, and 2048. Higher modulus values are recommended.
`ciscoasa(config)# ssh` *ip-address* *subnet-mask* *interface-name*	Identify which inside hosts can SSH to which ASA interface.
`ciscoasa(config)# ssh timeout` *minutes*	Alters the default exec timeout of 5 minutes.

NOTE: To verify the SSH configuration, use the `show ssh` command.

Enable HTTPS services on the ASA:

`ciscoasa(config)# http server enable`	Enable the ASA HTTP server.
`ciscoasa(config)# http` *ip-address* *network-mask* *interface-name*	Identify a host or hosts that can access the ASA HTTP server using ASDM.

NOTE: To remove and disable the ASA HTTP server service, use the `clear configure http` global configuration command.

Configuring Time Services

To configure the local system clock, use the following command:

`ciscoasa(config)# clock set` `hh:mm:ss month day year`	Manually sets the clock via the CLI.

> **NOTE:**   To verify the clock setting, use the `show clock` command.

Alternatively, you can configure the ASA to use Network Time Protocol (NTP) services. Use the following global configuration commands to securely configure and enable NTP:

`ciscoasa(config)# ntp server ip-address`	Identify the NTP server address.
`ciscoasa(config)# ntp authentication-key` `key-number md5 password`	Configure the NTP key and password.
`ciscoasa(config)# ntp trusted-key` `key-number`	Identify the trusted key.
`ciscoasa(config)# ntp authenticate`	Enable NTP authentication.

> **NOTE:**   To verify the NTP configuration and status, use the `show ntp status` and `show ntp associations` commands.

Configuring the Control Plane

Configuring a Default Route

If an ASA is configured as a DHCP or PPPoE client, it most probably is getting a default route provided by the upstream device. Otherwise, the ASA requires a default static route to be configured:

`ciscoasa(config)# route interface-name` `0.0.0.0 0.0.0.0 next-hop-ip-address`	Create a default static route.

> **NOTE:**   To verify the route entry, use the `show route` command.

Basic Settings Example

In this example, you

- Configure basic management settings.
- Configure and enable the master passphrase.

- Create the inside network SVI (VLAN 1) and assign it an IP address, create the outside network SVI (VLAN 2) and assign it an IP address, and create a limited DMZ network SVI (VLAN 3) and assign it an IP address and a security level.

- Assign interface Ethernet 0/1 to VLAN 1, E0/0 to VLAN 2, and E0/2 to VLAN 3.

- Enable Telnet, SSH, and HTTPS access and NTP time services.

- Configure a default route to the ISP.

Figure 20-1 shows the network topology for the ASA basic settings example.

Figure 20-1   Network Topology for the ASA Basic Settings Example

Configuring Basic Settings Example Using the CLI

`ciscoasa(config)# hostname ASA-1`	Name the ASA.
`ASA-1(config)# domain-name ccnas.com`	Configure the domain name.
`ASA-1(config)# enable password cisco123`	Configure the privileged EXEC password.
`ASA-1(config)# key config-key password-encryption cisco123`	Configure the master passphrase key.
`ASA-1(config)# password encryption aes`	Enable the master passphrase.
`ASA-1(config)# interface vlan 1`	Define the inside SVI (VLAN 1).
`ASA-1(config-if)# nameif inside` `INFO: Security level for "inside" set to 100 by default.`	Name the inside SVI. It defaults to a security level of 100.
`ASA-1(config-if)# ip address 192.168.1.1 255.255.255.0`	Assign the inside interface IP address.
`ASA-1(config-if)# interface vlan 2`	Define the outside SVI (VLAN 2).

`ASA-1(config-if)#` **`nameif outside`**
`INFO: Security level for "outside" set`
`to 0 by default.`
	Name the outside SVI. It defaults to a security level of 0.

`ASA-1(config-if)#` **`ip address`** **`209.165.200.226 255.255.255.248`**	Assign the outside interface IP address.
`ASA-1(config-if)#` **`interface vlan 3`**	Define the DMZ SVI (VLAN 3).
`ASA-1(config-if)#` **`no forward`** **`interface vlan 1`**	Disable forwarding to interface VLAN 1, denying the DMZ server the ability to communicate with the inside users. **NOTE:** Required because of the Base license restriction.

`ASA-1(config-if)#` **`nameif dmz`**
`INFO: Security level for "dmz" set to`
`0 by default.`
	Name the DMZ SVI. It defaults to a security level of 0.

`ASA-1(config-if)#` **`security-level 70`**	Change the security level to 70.
`ASA-1(config-if)#` **`ip address`** **`192.168.2.1 255.255.255.0`**	Assign the DMZ interface an IP address.
`ASA-1(config-if)#` **`exit`**	Return to global configuration mode.
`ASA-1(config)#` **`interface e0/1`**	Configure interface Ethernet 0/1.
`ASA-1(config-if)#` **`switchport access`** **`vlan 1`**	Assign it to VLAN 1.
`ASA-1(config-if)#` **`no shut`**	Enable the physical port.
`ASA-1(config-if)#` **`interface e0/0`**	Configure interface Ethernet 0/0.
`ASA-1(config-if)#` **`switchport access`** **`vlan 2`**	Assign it to VLAN 2.
`ASA-1(config-if)#` **`exit`**	Enable the physical port.
`ASA-1(config-if)#` **`interface e0/2`**	Configure interface Ethernet 0/2.
`ASA-1(config-if)#` **`switchport access`** **`vlan 3`**	Assign it to VLAN 3.
`ASA-1(config-if)#` **`exit`**	Return to global configuration.
`ASA-1(config)#` **`password cisco123`**	Create a Telnet / SSH password.
`ASA-1(config)#` **`telnet 192.168.1.10`** **`255.255.255.255 inside`**	Identify which inside host can connect to the ASA using Telnet.
`ASA-1(config)#` **`telnet timeout 4`**	Change the default EXEC timeout from 5 minutes to 4 minutes.

`ASA-1(config)# username admin` `password cisco123`	Create a local database entry.
`ASA-1(config)# aaa authentication ssh` `console LOCAL`	Enable AAA authentication for SSH using the local database.
`ASA-1(config)# crypto key generate rsa` `modulus 1024`	Create the crypto key required for SSH.
`ASA-1(config)# ssh 192.168.1.10` `255.255.255.255 inside`	Identify which inside host can connect to the ASA using SSH.
`ASA-1(config)# ssh timeout 4`	Change the default EXEC timeout from 5 minutes to 4 minutes.
`ASA-1(config)# http server enable`	Enable the HTTP server services.
`ASA-1(config)# http 192.168.1.10` `255.255.255.255 inside`	Identify which inside host can connect to the ASA using HTTP.
`ASA-1(config)# ntp server` `209.165.200.225`	Identify the authoritative NTP source.
`ASA-1(config)# ntp authentication-key` `51 md5 cisco123`	Specify the key number and password.
`ASA-1(config)# ntp trusted-key 51`	Identify which key to trust.
`ASA-1(config)# ntp authenticate`	Enable NTP authentication.
`ASA-1(config)# route outside 0.0.0.0` `0.0.0.0 209.165.200.225`	Create a default route to the ISP router.
`ASA-1(config)# exit`	Return to privileged EXEC.

`ASA-1# write`
`Building configuration...Cryptochecksum:`
`aaf03f93 9f6c40c3`
	Save the running configuration.

Configuring Basic Settings Example Using ASDM

To configure the hostname, domain name, enable, and Telnet passwords, choose **Configuration > Device Setup > Device Name/Password**.

The Device Name/Password screen is shown in Figure 20-2.

Figure 20-2   Device Name/Password Screen

From this screen, you can configure the following:

- The hostname (appears in the command-line prompt and is also used in system messages)
- The domain name (appended as a suffix to unqualified names)
- The Telnet password (sets the login password, which by default is set to cisco)
- The Telnet password (applies to Telnet and SSH access)

> **NOTE:**   Optionally, you can create a master passphrase to encrypt all passwords. To do so, choose **Configuration > Device Management > Advanced > Master Passphrase**.

To configure the Layer 3 interfaces, choose **Configuration > Device Setup > Interfaces** to open the Interfaces screen (see Figure 20-3).

Figure 20-3   Interfaces Screen

In this window, you can create or edit the ASA inside, outside, and DMZ interfaces.

To configure the Layer 2 ports, choose **Configuration > Device Setup > Interfaces > Switch Ports** tab, as shown in Figure 20-4. In this window, Layer 2 ports can be enabled and associated with a specific VLAN interface.

Figure 20-4   Switch Ports Tab

To configure management access for Telnet and SSH services, choose **Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH**, as shown in Figure 20-5.

Figure 20-5 ASDM/HTTPS/Telnet/SSH Screen

In this window, an administrator can identify which host or networks can have access to the ASA via ASDM/HTTPS, Telnet, or SSH.

To change the system time, choose **Configuration > Device Setup > System Time > Clock** to open the Clock screen (see Figure 20-6).

Figure 20-6 System Time Clock Screen

From this screen, you can manually configure the time zone, date, and time. The time is displayed in the status bar in the bottom-right corner.

To configure NTP, choose **Configuration > Device Setup > System Time > NTP** to open the NTP screen (see Figure 20-7).

Figure 20-7   System Time NTP Screen

In this window, you can add, edit, or delete an NTP server. When adding a server, you can configure the IP address and authentication parameters. Time derived from an NTP server overrides any time set manually.

To configure a default static route, choose **Configuration > Device Setup > Routing > Static Routes** to open the Static Routes screen (see Figure 20-8).

Figure 20-8   Static Routes Screen

In this window, you can enter or edit the static and default static routes.

This page intentionally left blank

Configuring Cisco ASA Advanced Settings

This chapter covers the following topics:

ASA DHCP Services

- DHCP Client
- DHCP Server Services
- Configuring DHCP Server Example Using the CLI
- Configuring DHCP Server Example Using ASDM

ASA Objects and Object Groups

- Network and Service Objects
- Network, Protocol, ICMP, and Service Object Groups
- Configuring Objects and Object Groups Example Using ASDM

ASA ACLs

- ACL Syntax
- Configuring ACLs Example Using the CLI
- Configuring ACLs with Object Groups Example Using the CLI
- Configuring ACLs with Object Groups Example Using ASDM

ASA NAT Services

- Auto-NAT
- Dynamic NAT, Dynamic PAT, and Static NAT
- Configuring Dynamic and Static NAT Example Using the CLI
- Configuring Dynamic NAT Example Using ASDM

AAA Access Control

- Local AAA Authentication
- Server-Based AAA Authentication
- Configuring AAA Server-Based Authentication Example Using the CLI
- Configuring AAA Server-Based Authentication Example Using ASDM

Modular Policy Framework Service Policies

- Class Maps, Policy Maps, and Service Policies

- Default Global Policies

- Configuring a Service Policy Example Using ASDM

ASA DHCP Services

You can configure the ASA as follows:

DHCP client	An interface is configured to receive its IP address and Dynamic Host Configuration Protocol (DHCP)-related information from an upstream device.
DHCP server	The Adaptive Security Appliance (ASA) provides IP addresses and DHCP-related information to inside hosts.

DHCP Client

Instead of manually configuring an IP address on a switch virtual interface (SVI), you can configure the ASA as a DHCP client:

`ciscoasa(config-if)# ip address dhcp [setroute]`	Requests an IP address from the upstream device.
	The `setroute` keyword automatically installs a default route to the upstream device.

> **NOTE:** Alternatively, you can configure the ASA as a PPP over Ethernet (PPPoE) client connecting to an upstream digital subscriber line (DSL) device by using the `ip address pppoe [setroute]` command.

DHCP Server Services

Use the following commands to configure an ASA as a DHCP server:

`ciscoasa(config)# dhcpd address [start-of-pool]-[end-of-pool] inside`	Define the pool of IP addresses and assign the pool to inside users. > **NOTE:** The `start-of-pool` and `end-of-pool` IP addresses are separated by a required hyphen (-).

ciscoasa(config)# **dhcpd enable** *interface-name*	Enable the DHCP server service (daemon) on the specified interface of the ASA. **NOTE:** The inside interface is usually configured to provide DHCP services by using the **dhcpd enable inside** command.

NOTE: For the ASA 5505, the maximum number of DHCP client addresses varies depending on the license. If the limit is 10 hosts, the maximum available DHCP pool is 32 addresses. If the limit is 50 hosts, the maximum available DHCP pool is 128 addresses. If the number of hosts is unlimited, the maximum available DHCP pool is 256 addresses.

Use the following commands to manually configure DHCP options:

ciscoasa(config)# **dhcpd domain** *domain-name*	Configure the DNS domain name.
ciscoasa(config)# **dhcpd dns** *dns-ip-address*	Configure the DNS domain name.
ciscoasa(config)# **dhcpd wins** *wins-ip-address*	Configure a WINS server address (if applicable).
ciscoasa(config)# **dhcpd lease** *seconds*	Configure the lease time in seconds. The default is 3600 seconds (1 hour).
ciscoasa(config)# **dhcpd option** *value*	Configure the DHCP option code. Option code is in the range 0 [nd] 255.

NOTE: If the ASA outside interface is configured as a DHCP client, you can use the **dhcpd auto_config outside** global configuration command to redistribute DHCP options learned from the upstream device to the DHCP clients on the inside interface.

Configuring DHCP Server Example Using the CLI

Figure 21-1 shows the network topology for the DHCP server example.

Figure 21-1   DHCP Server Topology Example

ASA-1(config)# **dhcpd address 192.168.1.11-192.168.1.30 inside**	Define the pool of IP addresses and assign the pool to inside users.
ASA-1(config)# **dhcpd enable inside**	Enable the DHCP server service (daemon) on the inside interface of the ASA.
ASA-1(config)# **dhcpd domain ccnas.com**	Define the domain name for DHCP clients.
ASA-1(config)# **dhcpd dns 209.165.200.225**	Define a Domain Name Service (DNS) server to DHCP clients.
ASA-1(config)# **dhcpd lease 7200**	Configure the lease time in seconds. The default is 3600 seconds (1 hour).

NOTE: To verify DHCP settings, use the `show dhcpd state` to display the current DHCP state for inside and outside interfaces, the `show dhcpd binding` command to display the current DHCP bindings of inside users, and the `show dhcpd statistics` command to display the current DHCP statistics.

NOTE: To clear the DHCP bindings or statistics, use the `clear dhcpd binding` or `clear dhcpd statistics` command.

Configuring DHCP Server Example Using ASDM

To enable DHCP server services, choose **Configuration > Device Management > DHCP > DHCP Server**. ASDM opens the DHCP Server screen (see Figure 21-2).

Figure 21-2   DHCP Server Screen

In this window, you can modify the general DHCP settings.

To enable DHCP services to inside users, click the inside interface and click the **Edit** button. ASDM then opens the Edit DHCP Server dialog, shown in Figure 21-3.

> **NOTE:**   Remember to click the **Apply** button any time a change is made.

Figure 21-3 Edit DHCP Server Dialog

Complete the DHCP settings and click **OK** to return to the DHCP Server screen, as shown in Figure 21-4.

Figure 21-4 Revised DHCP Server Screen

Remember to click **Apply** to send the configuration to the ASA device.

ASA Objects and Object Groups

Objects make it easier to maintain configurations. When an object is modified, the change automatically applies to all rules that use the specified object. Objects are used in Network Address Translation (NAT), access lists, and nested into other object groups.

The ASA supports the following:

Objects	- An object identifies an IP address/mask or a protocol (and a port). - An object can be reused in several configurations. - The ASA supports network objects and service objects. - Objects are created using the `object` {`network` | `service`} `object-name` command.
Object groups	- Object groups are used to group objects. - Objects can be attached or detached from multiple object groups. - You can create network, protocol, and Internet Control Message Protocol (ICMP)-type objects groups created using the `object-group` {`network` | `protocol` | `icmp-type`} `group-name` command. - You can also create service object groups by using `object-group service` `group-name` [`tcp` | `udp` | `tcp-udp`].

Network and Service Objects

A network object contains a single IP address/mask pair that can be identified using a host, subnet, or range of addresses.

Use the following commands to create or edit a network object:

`ciscoasa(config)# object network object-name`	Create or edit a network object and enter network object configuration mode.
`ciscoasa(config-network-object)# {host ip_addr | subnet net_addr net_mask | range ip_addr_1 ip_addr_2}`	Assign the IP address to the named object. You can configure a host address, a subnet, or a range of addresses.

NOTE: Use the `no` form of any of these three commands to remove a network object.

NOTE: There can only be one statement in the network object. Entering a second IP address/mask pair will replace the existing configured statement.

NOTE: The `description` command could be used to document the object.

NOTE: The `clear config object network` command erases all network objects.

NOTE: To verify, use the `show running-config object` command.

A service object contains a protocol and optional source and/or destination port.

Use the following commands to create or edit a service object:

`ciscoasa(config)# object service` `object-name`	Create or edit a service object and enter service object configuration mode.

Use the following command to identify specific services:

`ciscoasa(config-service-object)# service {protocol | icmp icmp-type | icmp6 icmp6-type | {tcp | udp} [source operator port] [destination operator port]}`	Specify an IP protocol name or number. You can optionally configure specific source or destination ports. **NOTE:** The `protocol` argument specifies an IP protocol name or number. **NOTE:** The `tcp` and `udp` keywords specify the protocol. **NOTE:** The `icmp` keyword is used to identify a specific ICMP type. **NOTE:** The `source` keyword specifies the source port, while the `destination` keyword specifies the destination port. **NOTE:** The `operator port` argument specifies a single TCP/UDP port number. Valid keyword operators include `eq`, `neq`, `lt`, `gt`, and `range`. The default operator is `eq` when none is specified.

NOTE.   Use the `no` form of any of these three commands to remove a service object.

NOTE: There can be multiple `service` statements in the service object. Additional `service` commands are appended to the configuration.

NOTE: The `clear config object service` command erases all service objects.

NOTE. To verify, use the `show running-config object` command.

NOTE: You cannot remove an object group or make an object group empty if it is used in a command.

Network, Protocol, ICMP, and Service Object Groups

Use the following commands to create a network object group:

`ciscoasa(config)# object-group` `network` *group-name*	Create or edit a network object group and enter network object group configuration mode.

Use the following commands to identify specific hosts or network object groups:

`ciscoasa(config-network-object-group)#` `network-object host` *ip-addr*	Assign an IP address to the named object.
`ciscoasa(config-network-object-group)#` `group-object` *group-name*	Assign an object group to the named object. **NOTE:** This allows for logical grouping of the same type of objects and construction of hierarchical object groups for structured configuration.

NOTE: Multiple hosts, networks, and objects can be added to a network object group.

NOTE: A network object group cannot be used to implement NAT. A network object is required to implement NAT.

A protocol-based object group combines IP protocols into one object.

Use the following commands to create a protocol object group:

`ciscoasa(config)# object-group` `protocol` *group-name*	Create or edit a protocol object group and enter protocol object group configuration mode.

Use one of the following commands to identify a protocol or other protocol object groups:

`ciscoasa(config-protocol-object-group)#` **`protocol-object`** *`protocol`*	Define the protocols in the group. **NOTE:** The *`protocol`* parameter is the IP protocol numeric identifier (1 [nd] 254) or a keyword identifier (for example, **`icmp, tcp, udp,`** or **`ip`** to include all IP protocols).
`ciscoasa(config-protocol-object-group)#` **`group-object`** *`group-name`*	Assign an object group to the named object.

Use the following commands to create an ICMP object group:

`ciscoasa(config)#` **`object-group icmp-type`** *`group-name`*	Create or edit an ICMP object group and enter ICMP group object configuration mode.

Use one of the following commands to identify a protocol or other protocol object groups:

`ciscoasa(config-icmp-object-group)#` **`icmp-object`** *`icmp-type`*	Define the ICMP types in the group. Enter the command for each type.
`ciscoasa(config-icmp-object-group)#` **`group-object`** *`group-name`*	Assign an object group to the named object.

A service-based object group is used to group TCP, UDP, or TCP and UDP ports into an object. The ASA enables the creation of a service object group that can contain a mix of TCP services; UDP services; ICMP-type services; and any protocol such as Encapsulation Security Protocol (ESP), generic routing encryption (GRE), and TCP.

Use the following commands to create a service object group:

`ciscoasa(config)#` **`object-group service`** *`group-name`*	Create or edit a service group object and enter service object group configuration mode.

Use one of the following commands to identify a protocol or other protocol object groups:

`ciscoasa(config-service-object-group)#` **`port-object eq`** *`service`*	Add a port object to a service object group. Specify the decimal number or name of a TCP or UDP port for a service object.
`ciscoasa(config-service-object-group)#` **`group-object`** *`group-name`*	Assign an object group to the named object.

Configuring Objects and Object Groups Example Using ASDM

To configure a network object or a network object group in ASDM, choose
Configuration > Firewall > Objects > Network Objects/Groups. ASDM shows the
Network Object/Groups screen shown in Figure 21-5.

Figure 21-5   Network Objects/Groups Screen

From this window, the administrator can add, edit, or delete a network object or a net-
work object group. To add a network object or a network object group, click **Add**, as
shown in Figure 21-6.

Figure 21-6   Adding a Network Object or Network Object Group

To configure service objects, service object groups, ICMP object groups, or protocol object groups, choose **Configuration > Firewall > Objects > Service Objects/Groups**. ASDM opens the Service Objects/Groups screen, as shown in Figure 21-7.

Figure 21-7   Service Objects/Groups Screen

From this window, the administrator can add, edit, or delete a service object or a service object groups, ICMP object groups, or protocol object groups. Figure 21-8 shows the objects that can be added.

Figure 21-8   Adding a Service, ICMP, and Protocol Objects

ASA ACLs

Many similarities exist between ASA access control lists (ACLs) and IOS ACLs. For example, both

- Are made up of access control entries (ACEs)
- Are processed sequentially from top down
- Have an implicit deny any at the end
- Follow the rule of only one ACL per interface, per protocol, per direction

ASA ACLs differ from IOS ACLs as follows:

- ASA ACLs use a network mask rather than a wildcard mask (for example, 0.0.0.255).
- ASA ACLs are named rather than numbered. There are no numbered standard and extended ACLs, although you could name one with a number.
- By default, interface security levels apply access control without an ACL configured.

NOTE: Traffic from a more-secure interface (such as security level 100) is allowed to access less-secure interfaces (such as level 0). Traffic from a less-secure interface is blocked from accessing more-secure interfaces and requires an ACL to permit traffic to a higher security level.

The ASA supports five types of access lists:

Extended	■ Most common type of ASA ACL
	■ Filters on source/destination port and protocol
Standard	■ Used for routing protocols, not firewall rules
	■ Cannot be applied to interfaces to control traffic
IPv6	■ Used to support IPv6 addressing
Webtype	■ Used for clientless Secure Sockets Layer (SSL) virtual private networks (VPNs)
Ethertype	■ Specifies network layer protocol and only used with transparent firewall mode

NOTE: Use the `help access-list` privileged EXEC command to display the syntax for all of the ACLs supported on an ASA platform.

NOTE: This section focuses on extended ACLs.

ACLs on a security appliance can be used for the following:

Through-traffic packet filtering	■ Traffic is passing through the appliance from one interface to another interface.
	■ The configuration requires an ACL to be defined and then applied to an interface.
To-the-box traffic packet filtering	■ Traffic (for example, Telnet, or SSH, Simple Network Management Protocol [SNMP]) is destined for the appliance.
	■ It filters traffic destined to the ASA management plane.
	■ It is completed in one step but requires an additional set of rules to implement access control.
	■ Also known as a management access rule.

ACL Syntax

You can use many options with ACLs. However, for most needs, a more useful and condensed version of the syntax is as follows:

| `ciscoasa(config)# access-list id extended {deny \| permit} protocol`
`{source_addr source_mask} \| any \| host src_host \|`
`interface src_if_name`
`[operator port [port]`
`{dest_addr dest_mask} \| any \| host dst_host \|`
`interface dst_if_name`
`[operator port [port]]}` | Create an extended ACL.

NOTE: The `interface` keyword is used for to-the-box filtering.

NOTE: Explanation of all ACL syntax is beyond the scope of this chapter. |

> **NOTE:** Use the `help access-list` command to view complete syntax information.

> **NOTE:** To verify ACLs, use the `show access-list` and `show running-config access-list` commands.

> **NOTE:** To erase a configured ACL, use the `clear configure access-list id` command.

After you configure an ACL to identify traffic allowed or denied by the ASA, the next step is to apply the ACL to an interface in either the inbound or the outbound direction.

Apply the ACL as follows:

```ciscoasa(config-if)# access-group acl-id {in | out} interface interface-name [per-user-override | control-plane]```	Applies the ACL to the interface. **NOTE:** The `control-plane` keyword is used for to-the-box filtering.

NOTE: To allow connectivity between interfaces with the same security levels, the `same-security-traffic permit inter-interface` global configuration command is required.

NOTE: To enable traffic to enter and exit the same interface, such as when encrypted traffic enters an interface and is then routed out the same interface unencrypted, use the `same-security-traffic permit intra-interface` global configuration command.

Configuring ACLs Example Using the CLI

PC-A and PC-B are external hosts that require access to the two internal servers. Each server provides web and email services.

Figure 21-9 shows the network topology for the ACL example.

Figure 21-9 ACL Topology Example

`ASA-1(config)# `**`access-list ACL-IN remark Permit PC-A -> Server A for HTTP / SMTP`**	Enter a remark.
`ASA-1(config)# `**`access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.131 eq http`**	Permit PC-A HTTP access to SVR-1.
`ASA-1(config)# `**`access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.131 eq smtp`**	Permit PC-A email access to SVR-1.
`ASA-1(config)# `**`access-list ACL-IN remark Permit PC-A -> Server B for HTTP / SMTP`**	Enter a remark.
`ASA-1(config)# `**`access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.132 eq http`**	Permit PC-A HTTP access to SVR-2.
`ASA-1(config)# `**`access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.132 eq smtp`**	Permit PC-A email access to SVR-2.
`ASA-1(config)# `**`access-list ACL-IN remark Permit PC-B -> Server A for HTTP / SMTP`**	Enter a remark.
`ASA-1(config)# `**`access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.131 eq http`**	Permit PC-B HTTP access to SVR-1.
`ASA-1(config)# `**`access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.131 eq smtp`**	Permit PC-B email access to SVR-1.
`ASA-1(config)# `**`access-list ACL-IN remark Permit PC-B -> Server B for HTTP / SMTP`**	Enter a remark.
`ASA-1(config)# `**`access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.132 eq http`**	Permit PC-B HTTP access to SVR-2.
`ASA-1(config)# `**`access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.132 eq smtp`**	Permit PC-B email access to SVR-2.
`ASA-1(config)# `**`access-list ACL-IN extended deny ip any any log`**	Configure the implicit `deny` statement to log all failures.
`ASA-1(config)# `**`access-group ACL-IN in interface outside`**	Apply the ACL to all incoming traffic on the outside interface.

Configuring ACLs with Object Groups Example Using the CLI

`ASA-1(config)# object-group protocol TCP`	Create a protocol object group called **TCP**.
`ASA-1(config-protocol)# protocol-object tcp`	Match all TCP traffic.
`ASA-1(config-protocol)# exit`	Return to global configuration.
`ASA-1(config)# object-group network Internet-Hosts`	Create a network object group called **Internet-Hosts**.
`ASA-1(config-network)# network-object host 209.165.201.1`	Identify a network host (PC-A).
`ASA-1(config-network)# network-object host 209.165.201.2`	Identify a network host (PC-B).
`ASA-1(config-network)# exit`	Return to global configuration.
`ASA-1(config)# object-group network Internal-Servers`	Create a network object group called **Internal-Servers**.
`ASA-1(config-network)# network-object host 209.165.202.131`	Identify a server host (SVR-1).
`ASA-1(config-network)# network-object host 209.165.202.132`	Identify a server host (SVR-2).
`ASA-1(config-network)# exit`	Return to global configuration.
`ASA-1(config)# object-group service HTTP-SMTP tcp`	Create a service object group called **HTTP-SMTP**.
`ASA-1(config-service)# port-object eq smtp`	Identify Layer 4 services (SMTP).
`ASA-1(config-service)# port-object eq www`	Identify Layer 4 services (HTTP).
`ASA-1(config-service)# exit`	Return to global configuration.
`ASA-1(config)# access-list ACL-IN remark Only permit PC-A / PC-B -> servers`	Enter an ACL remark.
`ASA-1(config)# access-list ACL-IN extended permit object-group TCP object-group Internet-Hosts object-group Internal-Servers object-group HTTP-SMTP`	Permit the Internet-Hosts object services identified in TCP when going to the Internal-Servers object for services identified in HTTP-SMTP.
`ASA-1(config)# access-list ACL-IN extended deny ip any any log`	Configure the implicit `deny` statement to log all failures.
`ASA-1(config)# access-group ACL-IN in interface outside`	Apply the ACL to all incoming traffic on the outside interface.

Configuring ACLs with Object Groups Example Using ASDM

To open the Access Rules screen, choose **Configuration > Firewall > Access Rules**. ASDM then opens the Access Rules screen, as shown in Figure 21-10.

Figure 21-10   Access Rules Screen

From this screen, all ACL rules are displayed. You can add, edit, and delete rules.

To add a rule, highlight the interface you want to add a rule to and click **Add** to open the Add Access Rule dialog shown in Figure 21-11.

Figure 21-11   Add Access Rule Dialog

To edit a rule, highlight an existing rule and click **Edit** to open the Edit Access Rule dialog shown in Figure 21-12.

Figure 21-12   Edit Access Rule Dialog

A useful feature in the Access Rules screen is the Diagram option. Clicking **Diagram** in the Access Rules screen opens a graphical representation of the highlighted policy, as shown in Figure 21-13.

Figure 21-13   Access Rules Diagram

ASA NAT Services

Like IOS routers, the ASA supports the following Network Address Translation (NAT) and Port Address Translation (PAT) deployment methods:

Inside NAT	■ Typical NAT deployment method where the ASA translates the internal host address to a global address. ■ The ASA restores return traffic to the original inside IP address.
Outside NAT	■ Deployment method used where traffic from a lower-security interface is destined for a higher-security interface. ■ This method may be useful to make a host on the outside appear as one from a known internal IP address.
Bidirectional NAT	■ Both inside NAT and outside NAT are used together.

Auto-NAT

The Auto-NAT feature has simplified the NAT configuration as follows:

1. Create a network object.

2. Identify hosts networks to be translated.

3. Define the `nat` command parameters.

The following are the three steps in a simple PAT configuration:

```
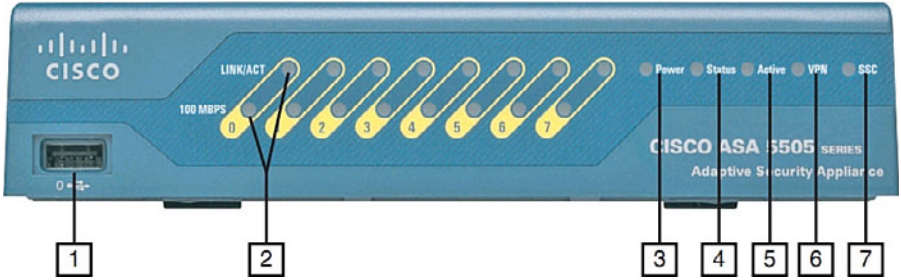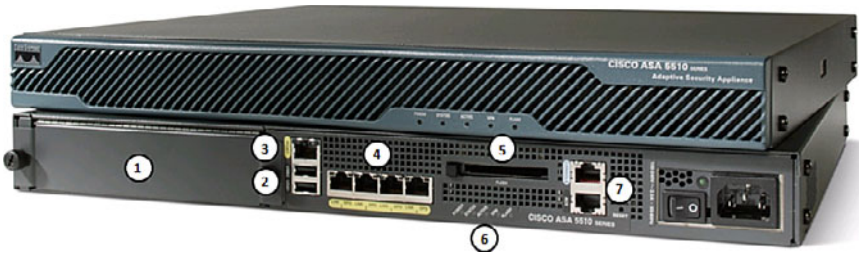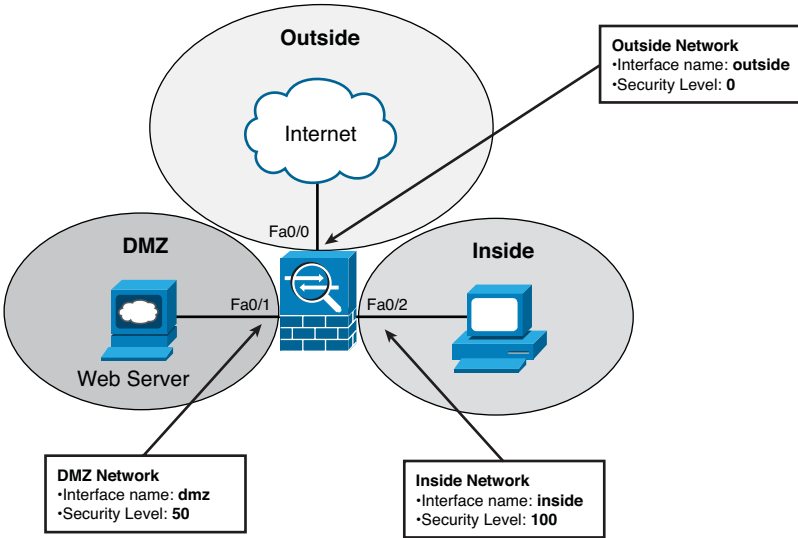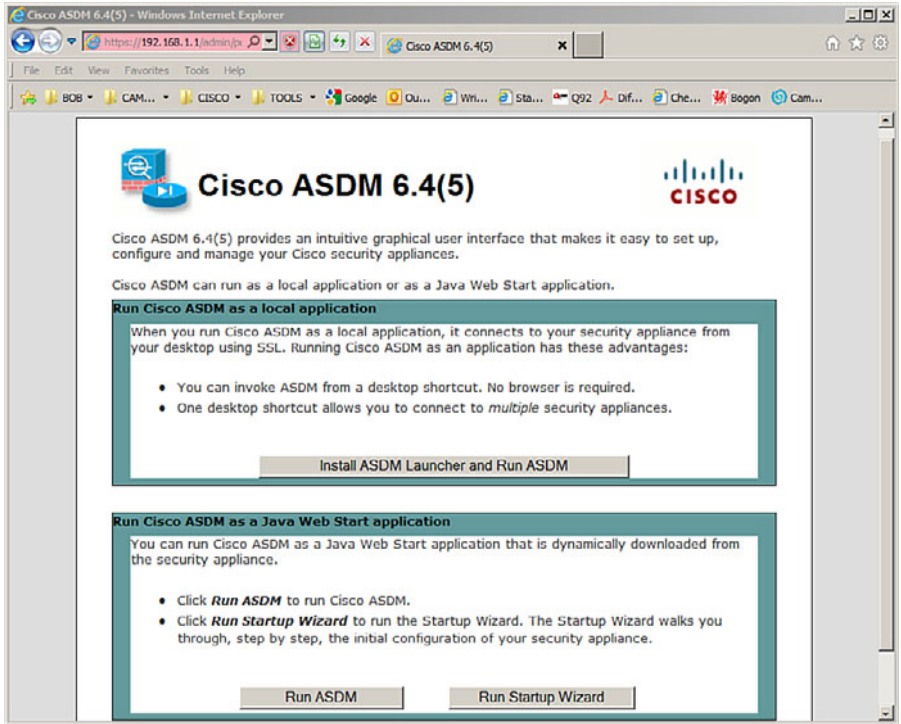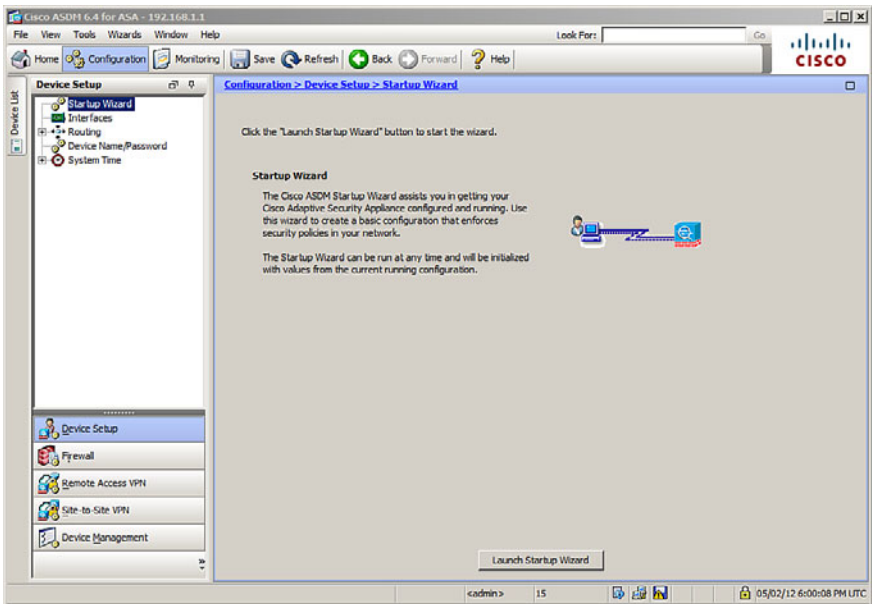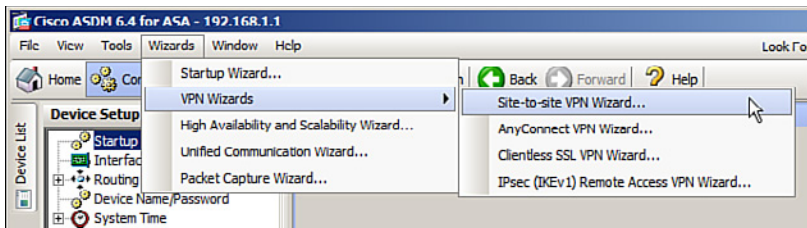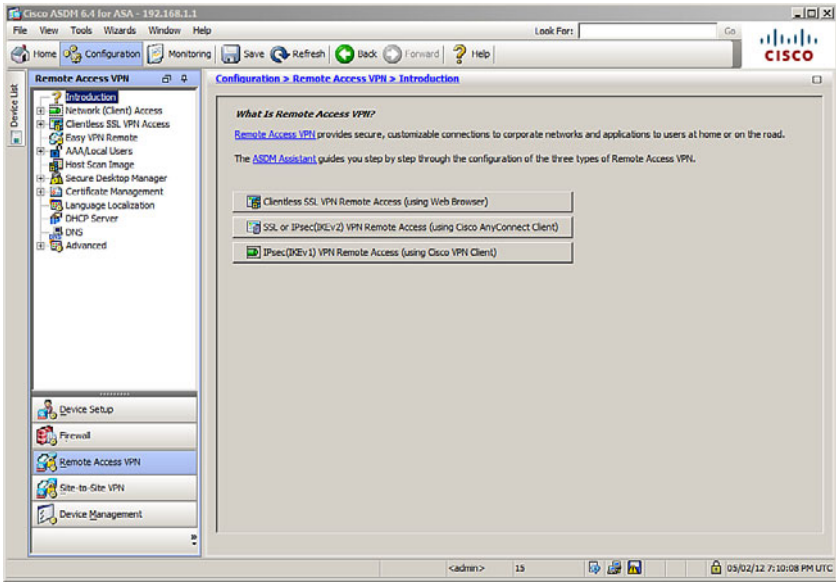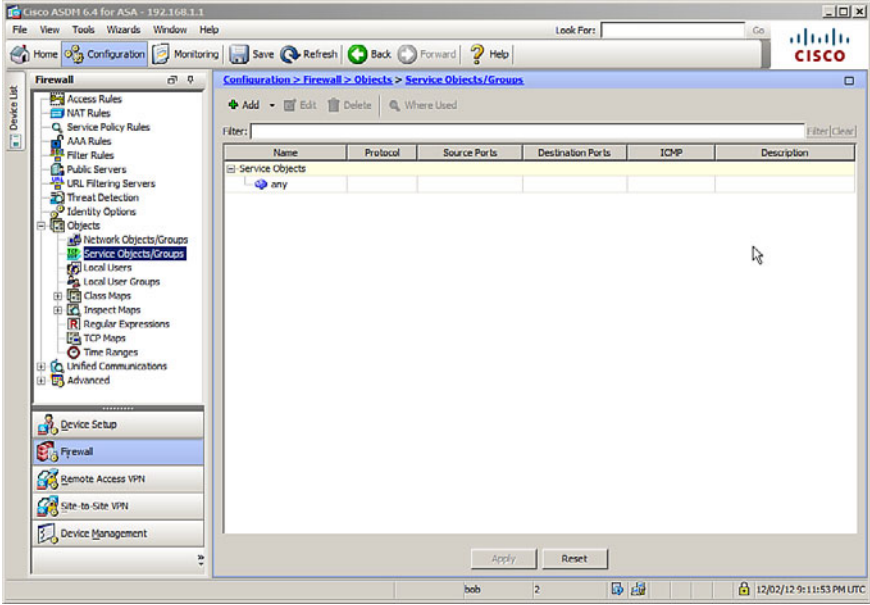ASA-1(config)# object network NAT-CFG
ASA-1(config-network-object)# subnet 192.168.1.0 255.255.255.224
ASA-1(config-network-object)# nat (inside,outside) dynamic interface
```

> **NOTE:**   Before ASA Version 8.3, NAT was configured using the `nat`, `global`, and `static` commands.

> **NOTE:**   The `global` and `static` commands are no longer recognized.

Dynamic NAT, Dynamic PAT, and Static NAT

Cisco ASA supports the following common types of NAT:

Dynamic NAT	■ Many-to-many translation.
	■ Typically deployed using inside NAT.
Dynamic PAT	■ Many-to-one translation.
	■ Usually an inside pool of addresses to overload an outside interface or outside address deployed using inside NAT.
Static NAT	■ A one-to-one translation.
	■ Usually an outside address mapping to an internal server deployed using outside NAT.
Twice-NAT	■ ASA Version 8.3 NAT feature that identifies both the source and destination address in a single rule (`nat` command).
	■ Used when configuring remote-access IPsec and SSL VPNs.
	■ Twice-NAT is beyond the scope of the chapter.

Dynamic NAT requires two network objects to be configured:

- The first network object identifies the pool of public IP addresses to translate to.
- The second network object binds inside addresses to the first network object.

Create a network object to identify the pool of public IP addresses.

`ciscoasa(config)# object network public-pool-obj`	Create a network object and enter network object configuration mode.
`ciscoasa(config-network-object)# {host ip_addr | subnet net_addr net_mask | range ip_addr_1 ip_addr_2}`	Identify the public IP pool of IP addresses using a host address, a subnet, or a range of addresses.

Create the network object that identifies the inside hosts and enable Dynamic NAT:

`ciscoasa(config)# object network nat-object-name`	Create a network object and enter network object configuration mode.
`ciscoasa(config-network-object)# {subnet net_addr net_mask | range ip_addr_1 ip_addr_2}`	Identify the inside IP pool of IP addresses using a subnet or a range of addresses.
`ciscoasa(config)# nat (real-ifc, mapped-ifc) dynamic public-pool-object`	Enable NAT to dynamically translate traffic from `real-ifc` to `mapped-ifc` using the `public-pool` network object. **NOTE:** The parentheses and comma (,) are required.

Dynamic PAT only requires one network object to be configured.

Create a network object that identifies the inside hosts and enable Dynamic NAT:

`ciscoasa(config)# object network pat-obj-name`	Create a network object and enter network object configuration mode.
`ciscoasa(config-network-object)# {subnet net_addr net_mask | range ip_addr_1 ip_addr_2}`	Identify the inside IP pool of IP addresses using a subnet or a range of addresses.

`ciscoasa(config)# ` **`nat (`**`real-ifc`**`,`**`mapped-ifc`**`)`** **`dynamic [`**`interface`** | ** `ip-address`**`]`**	Enable NAT to dynamically overload the outside inter-face IP address or overload a specified IP address. **NOTE:** The parenthe-ses and comma (,) are required. **NOTE:** PAT could also be configured to over-load a public pool of address if configured with the **`pat-pool`** *`mapped-obj`* parameter.

Static NAT maps an inside IP address to an outside public address such as to provide access to web servers by outside hosts. Static NAT requires one network object and an ACL to permit outside hosts access to the internal IP address.

Create a static NAT network object:

`ciscoasa(config)# ` **`object network`** `static-` `nat-obj-name`	Create a network object and enter network object configu-ration mode.
`ciscoasa(config-network-object)# ` **`host`** `ip_addr`	Identify the inside host IP address.
`ciscoasa(config)# ` **`nat (`**`real-ifc`**`,`**`mapped-ifc`**`)`** **`static`** `mapped-ip-addr`	Enable NAT to statically map an inside address to an out-side address. **NOTE:** The parenthe-ses and comma (,) are required.
`ciscoasa(config)# ` **`access-list`** `acl-id` **`extended`** **`permit ip any host`** `inside_host`	Create an extended ACL to permit outside users access to the internal IP address.
`ciscoasa(config-if)# ` **`access-group`** `acl-id` **`interface outside`**	Apply the ACL to allow incoming static NAT traffic.

> **NOTE:** Use the **`show run object`** command to display the network object, and use the **`show run nat`** command to display the NAT running configuration.

Configuring Dynamic and Static NAT Example Using the CLI

Translate inside users to a public pool and permit outside users access to SVR-1. Figure 21-14 shows the network topology for the NAT example.

Figure 21-14   NAT Topology Example

ASA-1(config)# **object network NAT-POOL**	Create the public pool network object.
ASA-1(config-network-object)# **range 209.165.200.240 209.165.200.246**	Assign the outside public pool IP addresses.
ASA-1(config-network-object)# **exit**	Return to global configuration mode.
ASA-1(config)# **object network NAT**	Create the Dynamic NAT object.
ASA-1(config-network-object)# **subnet 192.168.1.0 255.255.255.224**	Identify the inside hosts to translate from.
ASA-1(config-network-object)# **nat (inside,outside) dynamic NAT-POOL**	Dynamically translate traffic inside users to the NAT-POOL network object.
ASA-1(config)# **object network DMZ-NAT**	Create the static NAT network object.
ASA-1(config-network-object)# **host 192.168.2.3**	Identify the inside SVR-1 IP address.
ASA-1(config-network-object)# **nat (dmz,outside) static 209.200.165.227**	Statically map the public IP address to the identified SVR-1 address.
ASA-1(config-network-object)# **exit**	Return to global configuration mode.
ASA-1(config)# **access-list PCB->SVR1 permit ip any host 192.168.2.3**	Create an ACL permitting outside users to access the inside SVR-1 server.
ASA-1(config)# **access-group PCB->SVR1 in interface outside**	Apply the ACL to the outside interface.

NOTE: Unlike IOS ACLs, the ASA ACL `permit` statement must permit access to the internal private demilitarized zone (DMZ) address. External hosts access the server using its public static NAT address, and the ASA translates it to the internal host IP address and applies the ACL.

Configuring Dynamic NAT Example Using ASDM

To configure Dynamic NAT in ASDM, first configure the public pool network object. Choose **Configurations > Firewall > Objects > Network Objects/Groups** to open the Network Objects/Groups screen, as shown in Figure 21-15.

Figure 21-15 Network Objects/Groups Screen

Click **Add > Network Object** to display the Add Network Object dialog shown in Figure 21-16. Complete the public pool object.

Figure 21-16 Add Network Object Dialog

Next, create the Dynamic NAT network object.

Click **Add > Network Object** a second time, and click the drop-down NAT arrows to display the configurable NAT parameters.

Then do the following:

- Enter the NAT network object name.
- Identify the inside network address and subnet mask.
- Check the **Add Automatic Address Translation Rules** box.
- Identify the type of NAT as Dynamic (other options include Dynamic PAT and Static).
- Click the **Translated Addr** ellipsis (**...**) to open the Browse Translated Addr window.
- Select the public pool network object name and click **OK**.

Figure 21-17 shows the revised Add Network Object window.

Figure 21-17   Revised Add Network Object Dialog

Review the settings and click **OK** to complete the NAT configuration.

To view the NAT configuration, choose **Configuration > Firewall > NAT Rules**.

AAA Access Control

You can configure Cisco ASA to authenticate using the following:

Local user database	■ Local authentication, authorization, and accounting (AAA) stores usernames and passwords locally on the ASA and users authenticate against the local database.
	■ Ideal for small networks that do not need a dedicated AAA server.
Server-based authentication	■ Server-based AAA authentication is a much more scalable method than local AAA authentication.
	■ It uses an external database server resource leveraging RADIUS or TACACS+ protocols.

NOTE: Both methods are commonly used to provide a fallback mechanism.

Local AAA Authentication

ciscoasa(config)# **username** *name* **password** *password* **[privilege** *priv-level***]**	Create a local user account.

NOTE: To erase a user from the local database, use the `clear config username` [*name*] command.

NOTE: To view all user accounts, use the `show running-conf username` command.

Enable AAA authentication for the privilege EXEC mode, HTTP, SSH, or Telnet access:

ciscoasa(config)# **aaa authentication enable console LOCAL**	Enable AAA authentication for the privileged EXEC mode using the local database.
ciscoasa(config)# **aaa authentication http console LOCAL**	Enable AAA authentication for HTTP access using the local database.
ciscoasa(config)# **aaa authentication ssh console LOCAL**	Enable AAA authentication for SSH access using the local database.
ciscoasa(config)# **aaa authentication telnet console LOCAL**	Enable AAA authentication for Telnet access using the local database.

Server-Based AAA Authentication

Server-based AAA authentication is a much more scalable solution that uses an external database server resource leveraging RADIUS or TACACS+ protocols.

Server-based AAA authentication lets you do the following:

- Create a TACACS+ or RADIUS AAA server group.
- Ad a AAA server and parameters to the AAA server group.
- Configure server-based AAA authentication.

ciscoasa(config)# **aaa-server** *server-tag* **protocol** [**tacacs+** | **radius**}	Create a TACACS+ or RADIUS AAA server group. **NOTE:** Other protocols include **http-form, kerberos, ldap, nt,** and **sdi.** All are beyond the scope of this chapter.
ciscoasa(config-aaa-server-group)# **aaa-server** *server-tag* [(*interface-name*)] **host** {*server-ip* | *name*} [*key*]	Identify a AAA server and parameters to be part of the AAA server group.
ciscoasa(config)# **aaa authentication** {**enable** | **http** | **ssh** | **telnet**} **console** *server-tag* [**LOCAL**]	Enable server-based AAA authentication.

NOTE: To erase all AAA server configurations, use the **clear config aaa-server** command.

NOTE: To view all user accounts, use the **show running-conf aaa-server** command.

Configuring AAA Server-Based Authentication Example Using the CLI

Figure 21-18 shows the network topology for the server-based AAA authentication example.

Figure 21-18   Server-Based AAA Authentication Topology

`ASA-1(config)# username admin password cisco123 privilege 15`	Create a local user account for fallback purposes.
`ASA-1(config)# aaa-server TACACS-SVR protocol tacacs+`	Create a AAA server group using the TACACS+ protocol.
`ASA-1(config-aaa-server-group)# aaa-server TACACS-SVR (inside) host 192.168.1.5 cisco123`	Identify a server and password key.
`ASA-1(config-aaa-server-host)# exit`	Return to global configuration mode.
`ASA-1(config)# aaa authentication enable console TACACS-SVR LOCAL`	Enable privilege EXEC to use server-based AAA authentication with the local database for fallback.
`ASA-1(config)# aaa authentication http console TACACS-SVR LOCAL`	Enable HTTP to use server-based AAA authentication with the local database for fallback.
`ASA-1(config)# aaa authentication ssh console TACACS-SVR LOCAL`	Enable SSH to use server-based AAA authentication with the local database for fallback.
`ASA-1(config)# aaa authentication telnet console TACACS-SVR LOCAL`	Enable Telnet to use server-based AAA authentication with the local database for fallback.

Configuring AAA Server-Based Authentication Example Using ASDM

For fallback reasons, create a local user account. Choose **Configurations > Device Management > Users/AAA > User Accounts** to open the User Accounts screen shown in Figure 21-19.

Figure 21-19   User Accounts Screen

The screen shows the currently configured user accounts. You can edit, add, or delete user accounts. Click **Add** to open the Add User Account window shown in Figure 21-20.

Figure 21-20   Add User Account Window

Complete the entry and click **OK** to return to the User Accounts screen.

Click **Apply** to commit the changes to the ASA device.

Next, configure the AAA server group. Choose **Configuration > Device Management > Users/AAA > AAA Server Groups** to open the AAA Server Groups screen shown in Figure 21-21.

Figure 21-21   AAA Server Groups Screen

From this screen you can add, edit, or delete AAA server groups.

Click **Add** to open the ADD AAA Server Group dialog shown in Figure 21-22, and create a new AAA server group.

Figure 21-22   Add AAA Server Group Dialog

Complete the entry and click **OK**. The new server group is now displayed in the AAA Server Group screen.

Next, click **Add** in the Servers in the Selected Group portion of the dialog to open the Add AAA Server dialog (see Figure 21-23), and complete the entry to add the new AAA server.

Figure 21-23   Add AAA Server Screen

Click **OK** to continue. The new server is now displayed in the AAA Server Group screen.

Click **Apply** to commit the changes to the ASA device.

Finally, enable AAA authentication with the local database fallback by choosing **Configuration > Device Management > Users/AAA > AAA Access > Authentication**. ASDM will display the AAA Access Authentication screen shown in Figure 21-24.

Figure 21-24   AAA Access Authentication Screen

Edit the screen to enable server-based AAA authentication for the Enable, HTTP, Serial, SSH, and Telnet access, as shown in Figure 21-25.

Figure 21-25   Revised AAA Access Authentication Screen

Click **Apply** to commit the changes to the ASA device.

Modular Policy Framework Service Policies

Modular Policy Framework (MPF) configuration defines a set of rules for applying firewall features to the traffic that traverses the ASA. You can use MPF for the following:

- Advanced application layer traffic inspection by classifying at Layers 5 [nd] 7
- Rate-limiting
- Traffic inspection and quality of service (QoS)

Cisco MPF uses these three configuration objects to define modular, object-oriented, hierarchical policies, as illustrated in Figure 21-26.

Figure 21-26   Modular Policy Framework

> **NOTE:**   Although the MPF syntax is similar to the IOS Cisco Modular QoS CLI (MQC) syntax and Cisco Common Classification Policy Language (C3PL) syntax, the configurable parameters differ. For instance, the ASA provides more configurable actions and support for Layer 5–7 inspections.

To configure MPF on an ASA, you must complete four steps:

1. Optionally configure extended ACLs to identify specific granular traffic.
2. Configure the class map to identify traffic.
3. Configure a policy map to apply actions to those class maps.
4. Configure a service policy to attach the policy map to an interface.

Class Maps, Policy Maps, and Service Policies

Create a class map to identify specific Layer 3/4 traffic:

`ciscoasa(config)# ` **`class-map`** `class-map-name`	Create a Layer 3 or 4 class map and enter class-map configuration mode.

`ciscoasa(config)# `**`class-map`** **`type management`** `class-map-name`	Create a Layer 3 or 4 class map for to-the-box traffic and enter class-map configuration mode. **NOTE:** Two other variations of the command include the `class-map type inspect` command, which is used to define special actions for application inspection traffic, and the `class-map type regex` command to use with regular expressions (for example, to match specific URLs). Both are beyond the scope of this chapter.

NOTE: The names `class-default` and any name that begins with `_internal` or `_default` are reserved.

Define the traffic to include in the class by matching one of the following characteristics:

`ciscoasa(config-cmap)# `**`match any`**	Match all traffic to which you want to apply actions.
`ciscoasa(config-cmap)# `**`match access-list`** `acl-id`	Match packets specified by an extended ACL. **NOTE:** Other `match` keywords include `dscp, flow, port, precedence, rtp,` and `tunnel-group`. All are beyond the scope of this chapter.

NOTE: The `description` keyword could be used to document the class map.

NOTE: Unless otherwise specified, include only one `match` command in the class map.

NOTE: To display information about the class map configuration, use the `show running-config class-map` command

NOTE: To remove all class maps, use the `clear configure class-map` command.

Create a policy map to assign actions to traffic configured in Layer 3/4 class maps:

`ciscoasa(config)# policy-map` `p-map-name`	Specify a name for this policy map (up to 40 characters in length). **NOTE:** Another variation of the command is `policy-map type inspect p-map-name` command. The command is beyond the scope of this chapter.

Identify the class map:

`ciscoasa(config-pmap)# class` `class-map-name`	Assign a class map to a policy map where you can assign actions to the class map traffic and enter config policy map class mode. **NOTE:** The class name `class-default` is a reserved name.

NOTE: The `description` keyword could be used to document the policy map.

Assign one of the following actions:

`ciscoasa(config-pmap-c)# set connection`	Configure connection parameters.
`ciscoasa(config-pmap-c)# police {input | output} rate-bps`	Rate-limit traffic for this class.
`ciscoasa(config-pmap-c)# inspect protocol`	Configure protocol inspection services. **NOTE:** There are many different `protocol` keywords, including `dns, ftp, http, icmp, ipv6,` and more. All are beyond the scope of this chapter.

NOTE: Other configurable policy map actions that are beyond the scope of this chapter include `priority, service-policy, shape, ips, flow-export,` and more.

The service policy enables the policy map globally on all interfaces or on a specific interface:

`ciscoasa(config)# service-policy` `p-map-name [global | interface intf]`	Enable a set of policies globally or apply them on an interface.

Default Global Policies

By default, the ASA configuration includes a policy that matches all default application inspection traffic and applies inspection to the traffic on all interfaces (a global policy).

The global policy consists of the following MPF framework:

- A default class map called `inspection_default` that matches a special a keyword `default-inspection-traffic` that includes all common protocols.

- A global policy map called `global_policy` that assigns protocol inspection action to the `inspection_default` class map.

- A global service policy that enables the policy map `global_policy` globally.

The default class map matches common TCP/UDP traffic:

`ciscoasa(config)# class-map inspection_default`	Edit the default class map and enter class-map configuration mode.
`ciscoasa(config-cmap)# match default-inspection-traffic`	Special keyword to match the default ports for all inspections. **NOTE:** Matches specific common traffic including DNS (UDP 53), FTP (TCP 21), HTTP (TCP 80), ICMP, SMTP (TCP 25), TFTP (UDP 69), and more.

NOTE: There is also a global class map called `class-default` that matches all remaining traffic. This is a special class map that is applied implicitly at the end of all Layer 3 and 4 policy maps and essentially tells the ASA to not perform any actions on all other traffic.

The global policy map is called `global_policy`:

`ciscoasa(config)# policy-map global_policy`	Enter global policy map.
`ciscoasa(config-pmap)# class inspection_default`	Specify the action for the default class map.

The service policy applies it globally to all interfaces

`ciscoasa(config)# service-policy global_policy global`	Enable a set of policies globally.

The default policy configuration includes the following commands:

```
class-map inspection_default
 match default-inspection-traffic
!
```

```
policy-map type inspect dns preset_dns_map
 parameters
   message-length maximum client auto
   message-length maximum 512
policy-map global_policy
 class inspection_default
   inspect dns preset_dns_map
   inspect ftp
   inspect h323 h225
   inspect h323 ras
   inspect ip-options
   inspect netbios
   inspect rsh
   inspect rtsp
   inspect skinny
   inspect esmtp
   inspect sqlnet
   inspect sunrpc
   inspect tftp
   inspect sip
   inspect xdmcp
!
service-policy global_policy global
```

Configure Service Policy Example Using ASDM

To configure a service policy using ASDM, choose **Configuration > Firewall > Service Policy Rules** and click **Add**. ASDM then opens the Service Policy Rules screen shown in Figure 21-27.

Figure 21-27   Service Policy Rules Screen

Configuring Cisco ASA SSL VPNs

This chapter covers the following topics:

Remote-Access VPNs

- Types of Remote-Access VPNs

ASA SSL VPNs

- Client-Based SSL VPN Example Using ASDM
- Clientless SSL VPN Example Using ASDM

Remote-Access VPNs

Enterprise users are requesting support for their mobile devices, including smart phones, tablets, notebooks, and a broader range of laptop manufacturers and operating systems.

This shift has created a challenge for IT security. The solution is the use of Secure Sockets Layer (SSL) virtual private networks (VPNs) to secure access for all users, regardless of the endpoint from which they establish a connection.

Both Cisco Integrated Services Routers (ISR) and Adaptive Security Appliances (ASA) provide IPsec and SSL VPN capabilities. However, an ASA can support up to 10,000 concurrent sessions per device. The ASA is usually the choice when supporting a large remote networking deployment.

Types of Remote-Access VPNs

The ASA supports three types of remote-access VPNs:

Clientless SSL VPN	■ Clientless SSL VPN remote access (using a web browser).
	■ Browser-based VPN, which lets users establish a secure, remote-access VPN tunnel to the ASA.
	■ After authentication, users access a portal page and can access specific supported internal resources.

Client-based SSL or IPsec VPN	■ SSL or IPsec (IKEv2) VPN remote access (using Cisco AnyConnect Client). ■ Provides full-tunnel SSL VPN connection but requires a VPN client, such as the Cisco AnyConnect VPN client to be installed on the host. ■ The AnyConnect client can be manually preinstalled on the host or downloaded on-demand to a host via a browser. ■ After authentication, the user's PC is assigned an internal IP address and can access network resources as though they were on the local network.
IPsec (IKEv1) VPN	■ IPsec (IKEv1) VPN remote access (using Cisco VPN client).

ASA SSL VPN

ASA SSL VPNs can be configured using the following:

- ASDM VPN Assistant
- ASDM VPN Wizard

To open the ASDM VPN Assistant, choose **Configurations > Remote-Access VPN > Introduction**, as shown in Figure 22-1.

Figure 22-1   ASDM VPN Assistant Screen

Alternatively, start the VPN Wizard using the menu bar: **Wizards > VPN Wizards > AnyConnect VPN Wizard** (see Figure 22-2).

Figure 22-2   Choosing the AnyConnect VPN Wizard

Client-Based SSL VPN Example Using ASDM

In this example, the ASA is configured to support client-based SSL VPN. Remote users can establish SSL connection using the Cisco AnyConnect client.

Figure 22-3 shows the network topology for the client-based SSL VPN example.

Figure 22-3   Client-Based SSL VPN Topology Example

Use the VPN Wizard by choosing **Wizards > VPN Wizards > AnyConnect VPN Wizard**. The VPN Wizard Introduction window then opens, as shown in Figure 22-4. Click **Next** to continue.

Figure 22-4   AnyConnect VPN Connection Setup Wizard's Introduction Window

Next, the wizard shows the Connection Profile Identification window, as shown in Figure 22-5.

Figure 22-5   Connection Profile Identification Window

Configure a connection profile name for the connection and identify the interface to which outside users will connect.

Click **Next** to continue to display the VPN Protocol window shown in Figure 22-6.

Figure 22-6   VPN Protocols Window

Select how the traffic will be protected. The choices are SSL and IPsec. You can also configure a third-party certificate.

Uncheck IPsec, leave the SSL VPN protocol checked, and click **Next** to continue.

The Client Images window opens.

If a host does not have the AnyConnect VPN client preinstalled, they can download it from the ASA device. The Client Images window is where you specify the client file's location.

To identify the location and AnyConnect Client version, click **Add** to open the Add AnyConnect Client Image windows, as shown on the left side of Figure 22-7. Click **Browse Flash** to open the window, as shown on the right side of Figure 22-7, and navigate to the desired AnyConnect Client version.

Figure 22-7   Adding AnyConnect Client Image Windows

Three AnyConnect versions are available (Linux, MAC OS, and Windows). Select the client version and click **OK** to display a revised Client Images window, as shown in Figure 22-8.

Figure 22-8   Revised Client Images Window

NOTE: Repeat the process to add other client images.

Click **Next** to continue.

The Authentication Methods window opens, as shown in Figure 22-9.

Figure 22-9   Authentication Methods Window

You can add the location of the AAA authentication server.

Click **New** to enter the location of the AAA server. If a server is not identified, the local database is used.

To add a new user, enter the username and password and then click **Add**.

Click **Next** to continue.

The Client Address Assignment window opens, as shown in Figure 22-10.

Figure 22-10   Client Address Assignment Window

Create a new pool of private inside addresses that the remote users will be assigned once authenticated.

The IP address pool configuration is required for successful client-based SSL VPN connectivity. Without an available IP address pool, the connection to the security appliance will fail.

You can choose a preconfigured IP address pool from the Address Pool drop-down menu. Otherwise, click **New** to create a new one.

Click **Next** to continue and display the Network Name Resolution Servers window, as shown in Figure 22-11.

Figure 22-11   Network Name Resolution Servers Window

Enter the Domain Name System (DNS)-related information.

Click **Next** to continue.

The NAT Exempt window opens, as shown in Figure 22-12.

Figure 22-12   NAT Exempt Window

If Network Address Translation (NAT) is configured on the ASA, a NAT exemption rule must be created for the configured IP address pool. Like IPsec, SSL client address pools must be exempt from the NAT process because NAT translation occurs before encryption functions.

Check the **Exempt VPN Traffic from Network Address Translation** check box, and then click **Next**.

Click **Next** and an information screen on how to launch AnyConnect will open.

Click **Next** again and the VPN Wizard displays a summary of the configured selection, as shown in Figure 22-13.

Figure 22-13   Summary of the Client Images

Review the information displayed. If correct, click **Finish**. Otherwise, click **Back** and correct the misconfiguration.

The configuration is then committed to the ASA, and the AnyConnect Connection Profiles screen opens, as in Figure 22-14.

Figure 22-14 AnyConnect Connection Profiles Screen

From this screen, you can specify enable client access on the interfaces you select, and you can select, add, edit, and delete connections (tunnel groups). You can also specify whether you want to allow a user to select a particular connection at login.

To verify the configuration, you must do the following from a remote host:

1. Open a web browser and enter the login URL for the SSL VPN into the Address field.

2. If the ASA requests confirmation that this is a trusted site, accept and proceed.The ASA performs a series of compliance checks, platform detection, and finally selects/downloads the software package. A security warning displays if AnyConnect must be installed. If the AnyConnect Client must be downloaded, ActiveX must be installed and configured to trust the ASA. It is important that the security appliance is added as a trusted network site. After the client completes the autodownload, the web session automatically launches the Cisco AnyConnect SSL VPN Client.

Clientless SSL VPN Example Using ASDM

In this example, the ASA is configured to support clientless SSL VPN. Remote users require access to specific applications that do not need a full-tunnel SSL VPN. For this reason, the remote host uses a secure web browser connection to access select network resources.

Use the VPN Wizard by choosing **Wizards > VPN Wizards > Clientless SSL VPN Wizard**. The Clientless SSL VPN Connection window opens, as shown in Figure 22-15. Click **Next** to continue.

Figure 22-15   Clientless SSL VPN Connection Introduction Window

The SSL VPN Interface window appears, as shown in Figure 22-16.

Figure 22-16   SSL VPN Interface Window

Configure a connection profile name for the connection and identify the interface to which outside users will connect.

> **NOTE:**   By default, the ASA uses a self-signed certificate to send to the client for authentication. Optionally, you may configure the ASA to use a third-party certificate to connect clients.

> **NOTE:**   The SSL VPN Interface screen provides links in the Information section. These links identify the URLs that need to be used for the SSL VPN service access (login) and for Cisco ASDM access (to access the Cisco ASDM software download).

Click **Next** to continue and display the User Authentication window, as shown in Figure 22-17.

Figure 22-17   User Authentication Window

Identify how remote users will authenticate. You can configure authentication using a AAA server by checking the radio button. Click **New** to enter the location of the AAA server.

Alternatively, the local database can be used. To add a new user, enter the username and password and then click **Add**.

Once complete, click **Next** to continue and open the Group Policy window, as shown in Figure 22-18.

Figure 22-18   Group Policy Window

Identify a group policy that will be associated with the authenticated remote user.

> **NOTE:** If you are configuring a new policy, the policy name cannot contain any spaces.

By default, the created user group policy inherits its settings from the DfltGrpPolicy.

> **NOTE:** You may modify these settings after the wizard has been completed by navigating to the **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Group Policies**.

Click **Next** to continue.

The Bookmark List window appears, as shown in Figure 22-19. A bookmark list is a set of URLs that is configured to be used in the clientless SSL VPN web portal. If bookmarks are already listed, use the Bookmark List drop-down menu, choose the bookmark you want, and click **Next** to continue with the SSL VPN Wizard.

Figure 22-19   Bookmark List Window

To add bookmarks, click **Manage** and then **Add** to open the Add Bookmark List dialog shown in Figure 22-20.

Figure 22-20   Add Bookmark List Dialog

Click **Add** again to open the Add Bookmark dialog shown in Figure 22-21.

Figure 22-21   Add Bookmark Dialog

Add the bookmark and URL and keep clicking **OK** until you return to the Bookmark List window.

Click **Next** to continue. The Summary screen will open.

Review the information displayed. If correct, click **Finish**. Otherwise. click **Back** and correct the misconfiguration.

The configuration is then committed to the ASA, and the AnyConnect Connection Profiles screen opens.

To verify the configuration, open (from a remote host) a web browser and enter the login URL for the SSL VPN into the Address field.

The ASA SSL web portal web page will open listing the various bookmarks previously assigned to the profile.

> **NOTE:**   The browser URL must use Hypertext Transfer Protocol Secure (HTTPS) to connect to the SSL VPN.

This page intentionally left blank

Create Your Own Journal Here

Even though we have tried to be as complete as possible in this reference guide, invariably we will have left something out that you need in your specific day-to-day activities. That is why this section is here. Use these blank lines to enter your own notes, making this reference guide your own personalized journal.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____