

Implementing Cisco IOS Network Security—Volume 1

I. Course Introduction

- A. Overview/Learner Skills and Knowledge
- B. Course Goal and Objectives
- C. Course Flow
- D. Additional Resources
 - 1. Cisco Glossary of Terms

II. Introduction to Network Security Principles

- A. Overview/Module Objectives

III. Examining Network Security Fundamentals

- A. Overview/Objectives
- B. The Need for Network Security
- C. Network Security Options
 - 1. Basic Security Assumptions
 - 2. Basic Security Requirements
 - 3. Confidentiality
 - 4. Integrity
 - 5. Availability
- D. Data Classification
- E. Security Controls
- F. Response to a Security Breach
- G. Laws and Ethics
 - 1. Laws
 - 2. Ethics
 - 3. Liability
 - 4. Policy
- H. Summary

IV. Examining Network Attack Methodologies

- A. Overview/Objectives
- B. Adversaries, Motivations, and Classes of Attack
- C. How Hackers Think
- D. The Principles of Defense in Depth
- E. IP Spoofing Attacks
- F. Confidentiality Attacks
- G. Integrity Attacks
- H. Availability Attacks
- I. Best Practices to Defeat Network Attacks
- J. Summary

V. Examining Operations Security

- A. Overview/Objectives
- B. Secure Network Lifecycle Management
- C. Principles of Operations Security
- D. Network Security Testing
- E. Disaster Recovery and Business Continuity Planning
- F. Summary

VI. Understanding and Developing a Comprehensive Network Security Policy

- A. Overview/Objectives
- B. Security Policy Overview
- C. Policies, Standards, and Procedures
- D. Roles and Responsibilities
- E. Risk Management
- F. Principles of Secure Network Design

- G. Security Awareness
- H. Summary

VII. Building Cisco Self-Defending Networks

- A. Overview/Objectives
- B. Changing Threats and Challenges
- C. Building a Cisco Self-Defending Network
- D. Cisco Integrated Security Portfolio
- E. Summary
- F. Module Summary
 - 1. References

VIII. Perimeter Security

- A. Overview/Module Objectives

IX. Securing Administrative Access to Cisco Routers

- A. Overview/Objectives
- B. Cisco IOS Security Features
- C. Introducing the Cisco Integrated Services Router Family
 - 1. Cisco 800 Series Integrated Services Routers
 - 2. Cisco 1800 Series Integrated Services Routers
 - 3. Cisco 2800 Series Integrated Services Routers
 - 4. Cisco 3800 Series Integrated Services Routers
- D. Configuring Secure Administrative Access
- E. Setting Multiple Privilege Levels
- F. Configuring Role-Based CLI Access
- G. Securing the Cisco IOS Image and Configuration Files
- H. Configuring Enhanced Support for Virtual Logins
 - 1. Delays between Successive Login Attempts
 - 2. Login Shutdown When DoS Attacks Are Suspected
 - 3. Generation of System Logging Messages for Login Detection
- I. Configuring Banner Messages
- J. Summary

X. Introducing Cisco SDM

- A. Overview/Objectives
- B. Cisco SDM Overview
- C. Supporting Cisco SDM and Cisco SDM Express
 - 1. Additional Preparation for Existing Routers
- D. Launching Cisco SDM Express
- E. Launching Cisco SDM
- F. Navigating the Cisco SDM Interface
- G. Cisco SDM Wizards
- H. Summary

XI. Configuring AAA on a Cisco Router Using the Local Database

- A. Overview/Objectives
- B. AAA Overview
- C. Introduction to AAA for Cisco Routers
- D. Using Local Services to Authenticate Router Access
- E. Configuring Local Database Authentication Using AAA
- F. Troubleshooting AAA on Cisco Routers
- G. Summary

XII. Configuring AAA on a Cisco Router to Use Cisco Secure ACS

- A. Overview/Objectives
- B. Cisco Secure ACS Overview
 - 1. Cisco Secure ACS for Windows

2. Cisco Secure ACS Solution Engine
 3. Cisco Secure ACS Express 5.0
 4. Cisco Secure ACS View 4.0
- C. TACACS+ and RADIUS Protocols
 - D. Installing Cisco Secure ACS for Windows
 1. Third-Party Software Requirements
 2. Network and Port Prerequisites
 - E. Configuring the Server
 - F. Configuring TACACS+ Support on a Cisco Router
 - G. Troubleshooting TACACS+
 - H. Summary

XIII. Implementing Secure Management and Reporting

- A. Overview/Objectives
- B. Planning Considerations for Secure Management and Reporting
- C. Secure Management and Reporting Architecture
- D. Using Syslog Logging for Network Security
- E. Using Logs to Monitor Network Security
- F. Using SNMP
- G. Configuring an SSH Daemon for Secure Management and Reporting
- H. Enabling Time Features
- I. Summary

XIV. Locking Down the Router

- A. Overview/Objectives
- B. Vulnerable Router Services and Interfaces
- C. Management Service Vulnerability
- D. Performing a Security Audit
- E. Locking Down a Cisco Router
- F. Limitations and Cautions
- G. Summary
- H. Module Summary
 1. References

Implementing Cisco IOS Network Security—Volume 2

I. Network Security Using Cisco IOS Firewalls

- A. Overview/Module Objectives

II. Introducing Firewall Technologies

- A. Overview/Objectives
- B. Firewall Fundamentals
 1. Firewall Examples
- C. Firewalls in a Layered Defense Strategy
- D. Static Packet Filtering Firewalls
- E. Application Layer Gateways
- F. Dynamic or Stateful Packet Filtering Firewalls
- G. Other Types of Firewalls
- H. Cisco Family of Firewalls
- I. Developing an Effective Firewall Policy
- J. Summary

III. Creating Static Packet Filters Using ACLs

- A. Overview/Objectives
- B. ACL Fundamentals
- C. ACL Wildcard Masking
 1. Example: Wildcard Masking Process for IP Subnets
 2. Example: Wildcard Masking Process to Match a Single IP Address

- 3. Example: Wildcard Masking Process to Match Any IP Address
- D. Using ACLs to Control Traffic
 - 1. Example: Numbered Standard IPv4 ACL—Deny a Specific Subnet
 - 2. Example: vty Access
- E. ACL Considerations
- F. Configuring ACLs Using SDM
- G. Using ACLs to Permit and Deny Network Services
- H. Summary

IV. Configuring Cisco IOS Zone-Based Policy Firewall

- A. Overview/Objectives
- B. Zone-Based Policy Firewall Overview
- C. Configuring Zone-Based Policy Firewalls Using the Basic Firewall Wizard
- D. Manually Configuring Zone-Based Policy Firewalls Using Cisco SDM
- E. Monitoring a Zone-Based Policy Firewall
- F. Summary
- G. Module Summary
 - 1. References

V. Site-to-Site VPNs

- A. Overview/Module Objectives

VI. Examining Cryptographic Services

- A. Overview/Objectives
- B. Cryptology Overview
 - 1. Cryptology
 - 2. The Process of Encryption
 - 3. Application Examples
 - 4. Cryptanalysis
 - 5. Encryption Algorithm Features
- C. Symmetric and Asymmetric Encryption Algorithms
 - 1. Encryption Algorithms and Keys
 - 2. Symmetric Encryption Algorithms
 - 3. Asymmetric Encryption Algorithms
- D. Block and Stream Ciphers
 - 1. Block Ciphers
 - 2. Stream Ciphers
- E. Encryption Algorithm Selection
 - 1. Choosing an Encryption Algorithm
- F. Cryptographic Hashes
- G. Key Management
 - 1. Key Management Components
 - 2. Keyspaces
 - 3. Key Length Issues
 - 4. Example
- H. Introducing SSL VPNs
- I. Summary

VII. Examining Symmetric Encryption

- A. Overview/Objectives
- B. Symmetric Encryption Overview
- C. DES Features and Functions
 - 1. DES Modes of Operation
 - 2. Guidelines
- D. 3DES Features and Functions
- E. AES Features and Functions
 - 1. The Rijndael Cipher

- 2. AES vs. 3DES
- 3. AES Availability in the Cisco Product Line
- F. SEAL Features and Functions
 - 1. Restrictions for SEAL
- G. Rivest Ciphers Features and Functions
- H. Summary

VIII. Examining Cryptographic Hashes and Digital Signatures

- A. Overview/Objectives
- B. Overview of Hash Algorithms and HMACs
- C. MD5 Features and Functions
- D. SHA-1 Features and Functions
- E. Overview of Digital Signatures
- F. DSS Features and Functions
- G. Summary

IX. Examining Asymmetric Encryption and PKI

- A. Overview/Objectives
- B. Asymmetric Encryption Overview
- C. RSA Features and Functions
- D. DH Features and Functions
- E. PKI Definitions and Algorithms
 - 1. PKI Terminology
 - 2. PKI Components
 - 3. Certificate Classes
- F. PKI Standards
- G. Certificate Authorities
- H. Summary

X. Examining IPsec Fundamentals

- A. Overview/Objectives
- B. VPN Overview
- C. Cisco VPN Product Family
- D. Introducing IPsec
- E. IPsec Advantages
- F. IPsec Protocol Framework
- G. IKE Protocol
 - 1. IKE Phase 1
 - 2. IKE Phase 1 Example
 - 3. IKE Phase 2
- H. Summary

XI. Building a Site-to-Site IPsec VPN

- A. Overview/Objectives
- B. Site-to-Site IPsec VPN Operations
- C. Configuring IPsec
- D. Site-to-Site IPsec Configuration—Step 1
- E. Site-to-Site IPsec Configuration—Step 2
- F. Site-to-Site IPsec Configuration—Step 3
- G. Site-to-Site IPsec Configuration—Step 4
- H. Site-to-Site IPsec Configuration—Step 5
- I. Verifying the IPsec Configuration
- J. Summary

XII. Configuring IPsec on a Site-to-Site VPN Using Cisco SDM

- A. Overview/Objectives
- B. Introducing the Cisco SDM VPN Wizard Interface

- C. Site-to-Site VPN Components
- D. Using the Cisco SDM Wizards to Configure Site-to-Site VPNs
 - 1. Quick Setup
 - 2. Step-by-Step Setup
 - 3. Defining What Traffic to Protect
- E. Completing the Configuration
 - 1. Testing the Tunnel Configuration and Operation
 - 2. Monitoring Tunnel Operation
 - 3. Advanced Monitoring
 - 4. Troubleshooting
- F. Summary
- G. Module Summary
 - 1. References

XIII. Network Security Using Cisco IOS IPS

- A. Overview/Module Objectives

XIV. Introducing IPS Technologies

- A. Overview/Objectives
- B. Introducing IDS and IPS
- C. Types of IDS and IPS Systems
- D. Intrusion Prevention Technologies
- E. Host and Network IPS
- F. Introducing Cisco IPS Appliances
- G. Introducing Signatures
- H. Examining Signature Micro-Engines
- I. Introducing Signature Alarms
- J. IPS Best Practices
- K. Summary

XV. Configuring Cisco IOS IPS Using Cisco SDM

- A. Overview/Objectives
- B. Cisco IOS IPS Features
- C. Configuring Cisco IOS IPS Using Cisco SDM
- D. Configuring IPS Signatures
- E. Monitoring IOS IPS
- F. Verifying IPS Operation
- G. Summary
- H. Module Summary
 - 1. References

Implementing Cisco IOS Network Security—Volume 3

I. LAN, SAN, Voice, and Endpoint Security Overview

- A. Overview/Module Objectives

II. Examining Endpoint Security

- A. Overview/Objectives
- B. What Is Endpoint Security?
- C. Buffer Overflows
 - 1. Basics of a Typical Buffer Overflow Exploit
 - 2. Worm
 - 3. Virus
 - 4. Trojan Horse
- D. IronPort
- E. Cisco NAC Products
- F. Cisco Security Agent

- G. Endpoint Security Best Practices
- H. Summary

III. Examining SAN Security

- A. Overview/Objectives
- B. What Is a SAN?
- C. SANs Fundamentals
- D. SAN Security Scope
- E. Summary

IV. Examining Voice Security

- A. Overview/Objectives
- B. VoIP Fundamentals
- C. Voice Security Threats
- D. Spam over IP Telephony
- E. Fraud
- F. SIP Vulnerabilities
- G. Defending Against VoIP Hacking
- H. Summary

V. Mitigating Layer 2 Attacks

- A. Overview/Objectives
- B. Basic Switch Operation
- C. Mitigating VLAN Attacks
- D. Preventing STP Manipulation
 - 1. Mitigating STP Vulnerabilities
- E. CAM Table Overflow Attacks
- F. MAC Address Spoofing Attacks
- G. Using Port Security
- H. Additional Switch Security Features
- I. Layer 2 Best Practices
- J. Summary
- K. Module Summary
 - 1. References

Security Policies

Overview/Outline

Acceptable Use Policy Template

- 1.0 Purpose
- 2.0 Scope
- 3.0 Policy
- 4.0 Enforcement
- 5.0 Definitions
- 6.0 Revision History

Acquisition Assessment Policy Template

- 1.0 Purpose
- 2.0 Scope
- 3.0 Policy
- 4.0 Enforcement
- 5.0 Definitions
- 6.0 Revision History

Information Sensitivity Policy Template

- 1.0 Purpose
- 2.0 Scope

- 3.0 Policy
- 4.0 Enforcement
- 5.0 Definitions
- 6.0 Revision History

Password Policy

- 1.0 Purpose
- 2.0 Scope
- 3.0 Policy
- 4.0 Enforcement
- 5.0 Definitions
- 6.0 Revision History

Wireless Communications Policy Template

- 1.0 Purpose
- 2.0 Scope
- 3.0 Policy
- 4.0 Enforcement
- 5.0 Definitions
- 6.0 Revision History

Router Security Policy Template

- 1.0 Purpose
- 2.0 Scope
- 3.0 Policy
- 4.0 Enforcement
- 5.0 Definitions
- 6.0 Revision History

Switch Security Policy Template

- 1.0 Purpose
- 2.0 Scope
- 3.0 Policy
- 4.0 Enforcement
- 5.0 Definitions
- 6.0 Revision History

Acceptable Encryption Policy

- 1.0 Purpose
- 2.0 Scope
- 3.0 Policy
- 4.0 Enforcement
- 5.0 Definitions
- 6.0 Revision History

Implementing Cisco IOS Network Security—Lab Guide

Overview/Outline

Lab 1-1: Embedding a Secret Message Using Steganography

- A. Activity Objective
- B. Visual Objective
- C. Required Resources
- D. Job Aids
- E. Task 1: Create a Secret Message
- F. Task 2: Embed the Message into an Image File
- G. Task 3: Reveal the Embedded Message

Lab 1-2: Scanning a Computer System Using Testing Tools

- A. Activity Objective
- B. Visual Objective
- C. Required Resources
- D. Job Aids
- E. Task 1: Find an IP Address
- F. Task 2: Complete a Simple Scan of a Host

Lab 1-3: Scanning a Network Using Testing Tools

- A. Activity Objective
- B. Visual Objective
- C. Required Resources
- D. Job Aids
- E. Task 1: Complete a Network Scan

Lab 2-1: Securing Administrative Access to Cisco Routers

- A. Activity Objective
- B. Visual Objective
- C. Required Resources
- D. Command List
- E. Job Aids
- F. Task 1: Configure Password Minimum Length
- G. Task 2: Configure the Enable Secret Password
- H. Task 3: Configure the Console Port, Auxiliary Port, and vty Line-Level Passwords
- I. Task 4: Encrypt Clear Text Passwords
- J. Task 5: Test Administrative Access Security
- K. Task 6: Configure Role-Based CLI Access
- L. Task 7: Configure Enhanced Username Password Security
- M. Task 8: Enhanced Virtual Login Features
- N. Task 9: Secure Cisco IOS Image and Configuration Files

Lab 2-2: Configuring AAA on Cisco Routers to Use the Local Database

- A. Activity Objective
- B. Visual Objective
- C. Required Resources
- D. Command List
- E. Job Aids
- F. Task 1: Configure the Local Database Using Cisco SDM
- G. Task 2: Configure a AAA Authentication Profile Using Cisco SDM
- H. Task 3: Test a AAA Authentication Profile
- I. Task 4: Examine Authentication Using the Debug Command

Lab 2-3: Configure AAA on Cisco Routers to Use Cisco Secure ACS

- A. Activity Objective
- B. Visual Objective
- C. Required Resources
- D. Command List
- E. Job Aids
- F. Task 1: Verification of Cisco Secure ACS for Windows Installation and Configuration
- G. Task 2: Configure a Cisco Secure ACS to Use the Internal Database for Authentication
- H. Task 3: Configure a Cisco Router to Use Cisco Secure ACS for Authentication
- I. Task 4: Configure Cisco Secure ACS to Use the Window Server External Database For Authentication
- J. Task 5: Configure a Cisco Router to Use Cisco Secure ACS for Authorization
- K. Task 6: Configure a Cisco Router to Use Cisco Secure ACS for Accounting

Lab 2-4: Implementing Secure Management and Reporting

- A. Activity Objective
- B. Visual Objective
- C. Required Resources
- D. Command List
- E. Job Aids
- F. Task 1: Configure Router for Syslog
- G. Task 2: Configure Router for SSH
- H. Task 3: Configure the Router for NTP

Lab 2-5: Using Cisco SDM One-Step Lockdown and Security Audit

- A. Activity Objective
- B. Visual Objective
- C. Required Resources
- D. Command List
- E. Job Aids
- F. Task 1: Perform Security Audit
- G. Task 2: Review Issues Presented by Security Audit
- H. Task 3: Fix Security Problems
- I. Task 4: One-Step Lockdown
- J. Task 5: Review Router Configurations

Lab 3-1: Creating Static Packet Filters Using ACLs

- A. Activity Objective
- B. Visual Objective
- C. Required Resources
- D. Command List
- E. Job Aids
- F. Task 1: Apply a Standard ACL to Secure the VTYS
- G. Task 2: Use Extended ACLs to Secure Common Services
- H. Task 3: Verify ACL Operations

Lab 3-2: Configuring a Cisco IOS Zone-Based Policy Firewall

- A. Activity Objective
- B. Visual Objective
- C. Job Aids
- D. Required Resources
- E. Command List
- F. Task 1: Create a Zone-Based Policy Firewall Using Cisco SDM
- G. Task 2: Verify a Zone-Based Policy Firewall Configuration
- H. Task 3: Test the Zone-Based Policy Firewall
- I. Task 4: Remove the Zone-Based Policy Firewall

Lab 4-1: Configuring a Site-to-Site IPsec VPN

- A. Activity Objective
- B. Visual Objective
- C. Required Resources
- D. Command List
- E. Job Aids
- F. Task 1: Launch the Cisco SDM Site-to-Site VPN Wizard
- G. Task 2: Verify the VPN Connection
- H. Task 3: Remove the VPN Connection

Lab 5-1: Configuring Cisco IOS IPS

- A. Activity Objective
- B. Visual Objective
- C. Required Resources
- D. Command List



- E. Job Aids
- F. Task 1: Run the Cisco SDM IPS Rule Wizard
- G. Task 2: Enable Cisco IOS IPS
- H. Task 3: Configure Signature Settings
- I. Task 4: Configure Global Settings
- J. Task 5: Monitor IPS

Lab 6-1: Using Cisco Catalyst Switch Security Features

- A. Activity Objective
- B. Visual Objective
- C. Required Resources
- D. Command List
- E. Job Aids
- F. Task 1: Secure Trunks
- G. Task 2: Secure Access Ports Using BPDU Guard and Port Security

Answer Key

- Lab 1-1: Embedding a Secret Message Using Steganography
- Lab 1-2 Answer Key: Scanning a Computer System Using Testing Tools
- Lab 1-3 Answer Key: Scanning a Network Using Testing Tools
- Lab 2-1 Answer Key: Securing Administrative Access to Cisco Routers
- Lab 2-2 Answer Key: Configuring AAA on Cisco Routers Using the Local Database
- Lab 2-3 Answer Key: Configuring AAA on Cisco Routers to Use Cisco Secure ACS
- Task 4: Configure Cisco Secure ACS to Use the Windows Server External Database For Authentication
- Task 4: Configure Cisco secure ACS to Use the Windows Server External Database For Authentication
- Lab 2-4 Answer Key: Implementing Secure Management and Reporting
- Lab 2-5 Answer Key: Using Cisco SDM One-Step Lockdown and Security Audit
- Lab 3-1 Answer Key: Creating Static Packet Filters Using ACLs
- Lab 3-2: Configuring a Cisco IOS Zone-Based Policy Firewall
- Lab 4-1 Answer Key: Configure a Site-to-Site IPsec VPN
- Lab 5-1: Configuring Cisco IOS IPS
- Lab 6-1: Using Cisco Catalyst Switch Security Features