

642-552 Securing Cisco Network Devices (SND)

- **Course Number:** 642-552
- **Length:** 1 Day(s)

Course Overview

This course is part of the training for the Cisco Certified Security Professional, Cisco Firewall Specialist, Cisco IPS Specialist, and Cisco VPN Specialist certifications.

Prerequisites

Before attending this course, students must have a Cisco Certified Network Associate (CCNA) certification. Candidates must also have:

- Working knowledge of the Windows operating system
- Working knowledge of Cisco IOS networking and concepts

Audience

This course is intended for those who wish to attain the Cisco Certified Security Professional, Cisco Firewall Specialist, Cisco IPS Specialist, or Cisco VPN Specialist certifications.

Course Outline

- Course Introduction
- Chapter 1 Introduction to Network Security Policies
- Building Cisco Self-Defending Networks
- Threat Evolution
- Port 80 Applications Blur the Network Perimeter
- The SQL Slammer Worm: 30 Minutes After “Release”
- Network Effects of the SQL Slammer Worm
- Cisco Self-Defending Network Strategy
- Evolving a Cisco Self-Defending Network
- ATD Products, Services, and Architecture Example
- Cisco Integrated Security Portfolio
- Cisco Self-Defending Network
- Chapter 1a Review
- Understanding the Requirement for a Secure Network Policy
- Closed Networks
- Open Networks
- Threat Capabilities - More Dangerous and Easier to Use
- Size of the Problem
- Network Security Challenge
- E-Business Challenge
- Converging Dynamics
- Information Assurance - CIA

- Information Assurance - Typical Network Architecture
- Hackers, Motivations, and Classes of Attack
- Integrity
- The Human Aspect
- Technology
- Operations
- Defense in Depth
- Layered Approach
- Network Security Design Factors
- Secure the Network
- Monitor Security
- Test Security
- Improve Security
- Network Security Infrastructure
- Chapter 1b Review
- Introducing Network Attack Mitigation Techniques
- Installation Risk Assessment
- Common Threats to Physical Installations
- Hardware Threat Mitigation
- Environmental Threat Mitigation
- Electrical Threat Mitigation
- Maintenance - Related Threat Mitigation
- Reconnaissance Attacks
- Packet Sniffers
- Packet Sniffer Attack Mitigation
- Port Scans and Ping Sweeps
- Port Scan and Ping Sweep Attack Mitigation
- Internet Information Queries
- Access Attacks
- Password Attacks
- Demo - Password Attacks
- Password Attack Example
- Password Attack Mitigation
- Trust Exploitation
- Trust Exploitation Attack Mitigation
- Port Redirection
- Buffer Overflow Attack Mitigation
- Demo - Buffer Overflow
- IP Spoofing
- IP Spoofing - Technical Discussion
- IP Spoofing - Types of Attack
- Man-in-the-Middle Attacks
- Demo - Man In The Middle
- IP Spoofing Attack Mitigation
- DoS Attacks
- TCP SYN Flooding DoS Attack

- DDoS Attacks
- DDoS Example
- DoS and DDoS Attack Mitigation
- Worm, Virus, and Trojan Horse Attacks
- Anatomy of a Worm Attack
- Mitigating Worm Attacks
- Containing Virus and Trojan Horse Attacks
- Application Layer Attacks
- Application Layer Attack Mitigation
- Configuration Management
- Configuration Management Recommendations
- Management Protocols
- Management Protocol Best Practices
- Determining Network Vulnerabilities
- Chapter 1c Review
- Thinking Like a Hacker
- Step 1: Footprinting and Fingerprinting
- Defeat Footprinting
- Step 2: Enumeration
- Step 3: Social Engineering
- Step 4: Privilege Information
- Step 5: Gather Additional Passwords and Secrets
- Step 6: Maintaining Access
- Step 7: Leverage the Compromised System
- Best Practices to Defeat Hackers
- Chapter 1d Review
- Designing a Secure Network Life - Cycle Model
- Secure Network Design Factors
- Typical Business Goals
- Secure Network Life Cycle
- PDIOO Applied to the Secure Network Life Cycle
- Secure Network Planning Phase
- Secure Network Design Phase
- Secure Network Implement Phase
- Secure Network Operation Phase
- Secure Network Optimize Phase
- Disposal of Secure Network Components
- Principles of Secure Network Design
- Selected Principles for IT Security
- Chapter 1e Review
- Developing a Comprehensive Security Policy
- What are the Assets?
- Why Do You Need a Security Policy?
- What Does a Security Policy Do?
- Who Uses the Security Policy?
- Comprehensive Security Policy

- Governing Policy Comes from the Top
- Technical and User Policies
- Types of Technical Policies
- Security Policy Development
- Developing a Security Policy Plan Phase
- Developing a Security Policy Design Phase
- Assigning Risk to Network Components
- Identify Types of Users
- Security Analysis Matrix
- Developing a Security Policy - Implement Phase
- Developing a Security Policy - Operate Phase
- Operate Phase Security Monitoring
- Operate Phase Incident Response
- Developing a Security Policy Optimize Phase
- Managing Security Changes
- What Makes a Good Security Policy?
- Chapter 1f Review
- Chapter 2 - Securing the Perimeter
- Applying a Security Policy for Cisco Routers
- Role of Routers in Networks
- Threats to and Attacks on Routers
- Router Security Principles
- How Routers Enforce Perimeter Security Policy
- Filtering Packets with a Router
- Local and Remote Administrative Access
- Keeping Up-to-date
- Logging
- Conceptual Basis for a Router Security Policy
- Creating a Security Policy for a Router
- Applying Cisco IOS Security Features
- Chapter 2a Review
- Introducing Cisco SDM
- Cisco SDM Overview
- Starting Cisco SDM
- Files Required to Run Cisco SDM from a Router
- Launching Cisco SDM Express
- Launching Cisco SDM
- Navigating the Cisco SDM Interface
- Cisco SDM Wizards in Configuration Mode
- Configuration Mode Advanced Configuration
- Monitor Mode
- Chapter 2b Review
- Configuring AAA Functions on the Cisco IOS Router
- AAA Model - Network Security Architecture
- Implementing Cisco AAA
- Implementing Authentication Using Local Services

- Implementing Authentication Using External Servers
- TACACS+ and RADIUS AAA Protocols
- Authentication Methods and Ease of Use
- Authentication - Remote PC Username and Password
- Authentication - Token Cards and Servers
- AAA Example - Authentication via PPP Link
- Authenticating Router Access
- Router Local Authentication Configuration Process
- Enable AAA Globally Using the aaa new - model Command
- aaa authentication Commands
- aaa authentication login Command
- aaa authentication ppp Command
- aaa authentication enable default Command
- Authentication for Lines and Commands
- aaa authorization Command
- aaa accounting Command
- Troubleshooting AAA Using debug Commands
- Troubleshooting AAA Using the debug aaa Command
- Troubleshooting AAA Using tdebug aaa accounting
- Configuring AAA with Cisco SDM
- Demo - Authentication
- Chapter 2c Review
- Disabling Unused Cisco Router Network Services and Interfaces
- Vulnerable Router Services and Interfaces
- What You Need to Do
- Management Service Vulnerabilities
- Locking Down a Router with Cisco AutoSecure
- Locking Down a Router with Cisco SDM
- Limitations and Cautions
- Demo - Auto Secure
- Chapter 2d Review
- Implementing Secure Management and Reporting
- Considerations for Secure Management and Reporting
- Architecture of Secure Management and Reporting
- In-Band Management Considerations
- Secure Management and Reporting
- Implementing Log Messaging for Security
- Syslog Systems
- Cisco Log Severity Levels
- Log Message Format
- Using Logs to Monitor Network Security
- SNMPv1 and SNMPv2 Architecture
- Community Strings
- SNMP Security Models and Levels
- SNMPv3 Architecture
- SNMPv3 Operational Model

- Configuring an SSH Server for Security
- Enabling Syslog Logging With Cisco SDM
- Enabling SNMP with Cisco SDM
- Enabling NTP with Cisco SDM
- Enabling SSH with Cisco SDM
- Demo - SSH
- Chapter 2e Review
- Defending the Network Perimeter with Cisco Products
- Cisco IOS Router Security
- Cisco Secure ACS
- Cisco Secure ACS Product Summary
- Chapter 2f Review
- Chapter 3 - Securing LAN and WLAN Devices
- Applying Security Policies to Network Switches
- Why Worry About Layer 2 Security?
- Domino Effect
- Switches Are Targets
- Securing Network Access at Layer 2
- Protecting Administrative Access
- Password Encryption
- Password Guidelines
- Protecting the Management Port
- Turning Off Unused Network Services
- Shutting Down Interfaces
- Chapter 3a Review
- Mitigating Layer 2 Attacks
- VLAN Hopping by Switch Spoofing
- VLAN Hopping by Double Tagging
- Mitigating VLAN Hopping Network Attacks
- STP Attack
- bpdu-guard and guard root Commands
- Spoofing the DHCP Server
- DHCP Snooping
- ARP Spoofing: Man-in-the-Middle Attacks
- Mitigating Man-in-the-Middle Attacks with DAI
- DAI in Action
- MAC Learning
- CAM Learns MAC B Is on Port 2
- CAM Table Is Updated Flooding Stops
- Intruder Launches macof Utility
- The CAM Table Overflows
- MAC Address Spoofing Attack
- Using Port Security to Mitigate Attacks
- Port Security Fundamentals
- Port Security Configuration
- Port Security Defaults

- Configuring Port Security on a Cisco Catalyst Switch
- Port Security Configuration Script
- Verify the Configuration
- Layer 2 Best Practices
- Demo - Switch Port Security
- Chapter 3b Review
- Using Cisco Catalyst Switch Security Features
- Switching Infrastructure and Security
- Identity - Based Networking Services
- VLAN ACL
- Private VLAN
- Notification of Intrusions
- Rate Limiting
- Switched Port Analyzer
- Management Encryption
- Chapter 3c Review
- Securing Wireless LANs
- Wireless LANs Extend Wired LANs
- Comparing WLANs with LANs
- WLAN Characteristics
- Typical WLAN Components and Topologies
- Cisco Unified Wireless Network
- Threats to WLANs
- Evolution of WLAN Security
- Open Access Phase - SSID
- Initial Phase - WEP
- 802.11 Open Authentication
- 802.11 Shared Key Authentication
- Basic 802.11 Security Issues
- Exploits of 802.11 Security Vulnerabilities
- Enhanced 802.11 Security
- Interim Phase - WPA
- Present Phase - WPA2
- 802.1x for WLANs
- 802.1x EAP Deployment Comparison
- 802.1x Advantages for WLANs
- "Present" Phase - WLAN IDS
- Demo - Private VLANs
- Chapter 3d Review
- Chapter 4 - Configuring a Cisco IOS Firewall
- Introducing Firewall Technologies
- What Is a Firewall?
- Evolution of Firewall Technologies
- Static Packet Filtering Firewalls
- Static Packet Filtering Example
- Pros and Cons of Packet Filters

- Circuit Level Firewall
- Application Layer Firewall
- Application Layer Proxy Firewall
- Application Level Proxy Firewall
- Proxy Server Communication Process
- Limitations and Uses of Application Layer Firewalls
- Stateful or Dynamic Packet Filtering
- Stateful Filtering
- Limitations and Uses of Stateful Firewalls
- Cut-Through Proxy Firewall Communication Process
- Implementing NAT on a Firewall
- Network Address Translation
- Port Address Translation
- Configuring NAT with Cisco SDM
- Limitations and Uses of NAT
- Application Inspection Firewall
- Application Inspection Firewall Operation
- Application Inspection Firewalls
- Content Filtering Using Websense
- Firewalls in a Layered Defense Strategy
- Chapter 4a Review
- Building Static Packet Filters with Cisco ACLs
- Access Control Lists
- Standard and Extended ACLs
- Identifying ACLs
- Enable Turbo ACLs
- Guidelines for Developing ACLs
- Applying ACLs to Inbound and Outbound Interfaces
- Applying ACLs to Interfaces
- Traffic Filtering with ACLs
- Reference Network Topology
- vty Filtering
- SNMP Service Filtering
- RIPv2 Route Filtering
- IP Address Spoof Mitigation Inbound
- IP Address Spoof Mitigation Outbound
- DoS TCP SYN Attack Mitigation Blocking External Access
- DoS Smurf Attack Mitigation
- Filtering ICMP Messages Inbound
- Filtering ICMP Messages Outbound
- Filtering UDP Traceroute Messages
- Basics of DDoS Attacks
- DDoS Attack Mitigation Trin00
- DDoS Attack Mitigation Stacheldraht
- DDoS Attack Mitigation Trinity v3
- DDoS Attack Mitigation SubSeven

- Combining Access Functions
- ACL Caveats
- Chapter 4b Review
- Configuring a Cisco IOS Firewall with the Cisco SDM Wizard
- Choosing the Type of Firewall You Need
- SDM Firewall Wizard Help Screens
- Step-by-Step Help Screens
- Basic Firewall
- Creating an Advanced Firewall
- Configuring Firewall Inspection Rules
- Application Security Configuration
- Advanced Firewall Configuration Summary
- Delivering the Commands to the Router
- Editing a Firewall Policy
- Editing the Application Security Policy
- Editing Firewall Global Settings
- Chapter 4c Review
- Defending Your Network with the Cisco Firewall Product Family
- Cisco Firewall Product Family
- Cisco IOS Firewall Features
- When to Use a Cisco IOS Firewall
- Cisco PIX 500 Series Security Appliances
- Cisco PIX 500 Series Security Appliances Features
- Cisco Catalyst 6500 Series Firewall Services Module
- Cisco ASA 5500 Series Adaptive Security Appliances
- Adaptive Solution with Converged Security Services
- Migrating from Cisco PIX to Cisco Security Appliance
- Best Practices for Firewall Policy Development
- Demo - Access List
- Chapter 4d Review
- Chapter 5 - Securing Networks with Cisco IOS IPS
- Introducing IDS and IPS
- Defining IDS and IPS
- IDS and IPS Common Characteristics
- IDS and IPS Operational Differences
- Comparing IDS and IPS Solutions
- Placement of IDS and IPS Sensors
- Types of IDS and IPS Sensors
- Cisco IOS IPS Attack Responses
- Event Monitoring and Management
- Security - MARS IPS Monitoring System
- HIPS Features
- HIPS Operation Details
- Cisco HIPS Deployment
- NIPS Features
- Cisco NIPS Deployment

- Comparing HIPS and Network IPS
- HIPS and Network IPS Monitoring
- IPS Signature Operational Characteristics
- Attack Methods, IPS Signature Types, and Capabilities
- Signature Definition Files
- Memory Requirements of Pre-Built SDFs
- Distributed Threat Mitigation with Intrusion Prevention System
- Benefits of DTM with Cisco IOS IPS Software
- Signature Micro-Engines
- Supported Signature Micro-Engines
- Signature Micro-Engine and SDF Build Failures
- Cisco Signature Alarm Types
- Support for SDEE and Syslog
- Viewing SDEE Alarm Messages
- Implementing Alarms in Signatures
- Chapter 5a Review
- Configuring Cisco IOS IPS
- Cisco IOS IPS Intrusion Detection Technology
- Primary Benefits of the Cisco IOS IPS Solution
- Cisco IOS IPS Signature Features
- Using Cisco SDM to Configure Cisco IOS IPS
- Using Cisco SDM GUI to Create IPS Rules
- Using Cisco SDM GUI to Edit Existing IPS Rules
- Launching the IPS Rule Wizard
- Confirming IOS IPS on Interfaces
- Configuring Signatures Using Cisco SDM
- Importing Signature Definition Files
- Configuring Global Settings
- Saving the Cisco IOS IPS Configuration
- Chapter 5b Review
- Defending Your Network with the Cisco IPS Product Family
- Cisco IPS Platforms
- Throughput on Cisco IOS Routers
- Performance and Limitations of Platforms
- Performance and Limitations of Cisco ASA 5500 Series
- Relative Positioning of Cisco IPS Sensors
- Cisco IPS Management Software
- CSA Architecture
- Application, Kernel, and Interceptors
- CSA Interceptors
- CSA Features
- Cisco IPS Selection Considerations
- IPS Configuration Best Practices
- Accommodating Network Growth
- Scaling HIPS Systems
- Chapter 5c Review

- Chapter 6 - Building IPsec VPNs
- Introducing IPsec VPNs
- Introducing Ipsec
- Internet Key Exchange
- IKE Communication Negotiation Phases
- IKE: Other Functions
- ESP and AH Header
- Transport and Tunnel Mode
- Message Authentication and Integrity Check Using Hash
- MD5 and SHA-1
- Symmetric vs. Asymmetric Encryption Algorithms
- Symmetrical Key Encryption Algorithms
- DH and RSA Asymmetric Encryption Algorithms
- PKI Certificates
- PKI Message Exchange
- PKI Credentials
- Chapter 6a Review
- Building a Site-to-Site IPsec VPN Operation
- Site-to-Site IPsec VPN
- Site-to-Site IPsec Configuration
- Site-to-Site IPsec Configuration - Phase 1
- Site-to-Site IPsec Configuration - Phase 2
- Site-to-Site IPsec - Apply VPN Configuration
- Site-to-Site IPsec - Interface Access List
- Chapter 6b Review
- Configuring IPsec Site-to-Site VPN Using Cisco SDM
- Introducing the Cisco SDM VPN Wizard Interface
- Site-to-Site VPN Components
- Launching the Site-to-Site VPN Wizard
- Quick Setup
- Step-by-Step Setup
- Connection Settings
- IKE Proposals
- Transform Set
- Option 1: Single Source and Destination Subnet
- Option 2: Using an ACL
- Review the Generated Configuration
- Test Tunnel Configuration and Operation
- Monitor Tunnel Operation
- Advanced Monitoring
- Troubleshooting
- Chapter 6c Review
- Building Remote Access VPNs
- Cisco Easy VPN Components
- Remote Access Using Cisco Easy VPN
- Cisco Easy VPN Remote Connection Process

- Cisco Easy VPN Tasks for the Cisco Easy VPN Server Wizard
- Starting the Cisco Easy VPN Server Wizard
- Choosing an Interface for Terminating IPsec
- Configuring IKE Policies
- Configuring IPsec Transform Sets
- Configuring a Group Policy Local Router Configuration
- Configuring a Group Policy External Location via RADIUS
- Configuring a Local User Database: User Authentication
- Configuring Local Group Policies
- Configuring Local Group Policy Parameters
- Confirming Configuration Settings
- Testing the Cisco Easy VPN Server Configuration
- Managing Cisco Easy VPN Server Connections
- Editing, Cloning, or Deleting Group Policies
- Creating or Editing a Local Pool for IP Addresses
- Cisco VPN Client Software
- Configuring Cisco Easy VPN Remote
- Managing Cisco Easy VPN Remote Connections
- Chapter 6d Review
- Course Closure