Securing Cisco Network Devices

Length
5 days

Format
Lecture/lab

Version
1.0

Course Description

SND v1.0 is a five-day, entry-level network security course offered as a prerequisite to the Cisco Qualified Specialist curriculum. You will learn how to recognize network threats and vulnerabilities and implement basic mitigation measures.

SND introduces the products and solutions that form the basis of the Cisco security portfolio. You will secure network devices at Layers 2 and 3 using the CLI and web-based GUIs. Devices include routers, switches, access control servers, IPS sensors, and VPN concentrators.

Who Should Attend

This course is designed for network professionals who need to deploy Cisco security solutions including VPN, IDS sensors, and PIX firewalls.

Recommended Prerequisites

- CCNA certification or equivalent knowledge
- Basic knowledge of the Windows operating system
- Familiarity with networking and security terms and concepts

Related Courses

- Introduction to Cisco Networking Technologies (INTRO)
- Interconnecting Cisco Network Devices (ICND)
- Securing Networks with Cisco Routers and Switches (SNRS)

SND

Learning Objectives

After completing this course, you will be able to:

- Describe the products in the Cisco security portfolio and explain how they mitigate security threats to a network
- Describe the security features available for a Cisco Layer 2 device in a secure network
- Implement security on a Cisco IOS router
- Describe and configure Cisco IPS and HIPS
- Configure and verify basic remote access on a Cisco VPN Concentrator
- Implement a Cisco PIX security appliance

Cisco Partner Learning Solutions

Securing Cisco Network Devices

Course Outline

Module 1: Introduction to Network Security Policies

Lesson 1: Understanding the Requirement for a Network Security Policy

Need for Network Security
Balancing Network Security Requirements
Assuring the Availability and Protection of Information
Adversaries, Hacker Motivations, and Classes of Attack
Information Assurance
Principles of Defense in Depth
Network Security Process
Network Security Design Factors

Lesson 2: Introducing Network Attack Mitigation Techniques

Mitigating Physical and Environmental Threats
Reconnaissance Attacks and Mitigation
Access Attacks and Mitigation
IP Spoofing Attacks and Mitigation
DoS Attacks and Mitigation
Worm, Virus, and Trojan Horse Attacks and Mitigation
Application Layer Attacks and Mitigation
Management Protocols and Vulnerabilities
Determining Network Vulnerabilities

Lesson 3: Thinking Like a Hacker

Step 1: Footprint Analysis
Step 2: Enumerate Information
Step 3: Manipulate Users to Gain Access
Step 4: Escalate Privileges
Step 5: Gather Additional Passwords & Secrets
Step 6: Install Back Doors and Port Redirectors
Step 7: Leverage the Compromised System
Best Practices to Defeat Hackers

Lesson 4: Designing a Secure Network Life-Cycle Model

Components of Network Security Design
Secure Network Life-Cycle Management
Planning a Secure Network
Designing a Secure Network
Implementing a Secure Network
Operating a Secure Network
Optimizing a Secure Network
Disposing of Secure Network Components
Principles of Secure Network Design

Lesson 5: Developing a Comprehensive Security Policy

Why Do You Need a Security Policy?
What Does a Security Policy Do and Who Uses It?
Components of a Comprehensive Security Policy
Developing a Security Policy Using the PDIOO Model
Developing a Security Policy—Plan Phase
Developing a Security Policy—Design Phase
Developing a Security Policy—Implement Phase
Developing a Security Policy—Operate Phase
Developing a Security Policy—Optimize Phase
What Makes a Good Security Policy?

Lesson 6: Building Cisco Self-Defending Networks

Changing Threats and Challenges
Building a Cisco Self-Defending Network
Adaptive Threat Defense
Cisco Integrated Security Portfolio

Module 2: Securing the Perimeter

Lesson 1: Applying a Security Policy for Cisco Routers

Role of Routers in Networks
Router Security Principles
How Routers Enforce a Perimeter Security Policy
Local and Remote Administrative Access
Maintaining the Most Recent Versions of Cisco IOS Software
Logging
Conceptual Basis for a Router Security Policy
Creating a Security Policy for a Router
Applying Cisco IOS Security Features

Lesson 2: Securing Administrative Access to Cisco Routers

Configuring Router Passwords
Setting a Login Failure Rate
Setting Timeouts
Setting Multiple Privilege Levels
Configuring Role-Based CLI
Securing the Cisco IOS Image and Configuration Files
Configuring Enhanced Support for Virtual Logins
Configuring Banner Messages

CISCO PARTNER
Learning Solutions

Securing Cisco Network Devices

Course Outline

Module 2: Securing the Perimeter (Cont.)

Lesson 3: Introducing Cisco SDM
Cisco SDM Overview
Starting Cisco SDM and Cisco SDM Express
Launching Cisco SDM Express
Launching Cisco SDM
Navigating the Cisco SDM Interface
Cisco SDM Wizards

Lesson 4: Configuring AAA Functions on the Cisco IOS Router
Identification and Authentication
Introduction to AAA for Cisco Routers
Authenticating Remote Access
TACACS+ and RADIUS AAA Protocols
Authentication Methods
Point-to-Point Authentication Protocols
Authenticating Router Access
Configuring AAA for Cisco Routers
Troubleshooting AAA for Cisco Routers
Configuring AAA with Cisco SDM

Lesson 5: Disabling Unused Cisco Router Network Services and Interfaces
Vulnerable Router Services and Interfaces
Management Service Vulnerabilities
Locking Down Your Router with Cisco AutoSecure
Limitations and Cautions

Lesson 6: Implementing Secure Management and Reporting
Secure Management and Reporting Planning Considerations
Secure Management and Reporting Architecture
Using Syslog Logging for Network Security
Using Logs to Monitor Network Security
Using SNMPv3
Configuring an SSH Server for Secure Management and Reporting
Enabling Management Features

Lesson 7: Defending the Network Perimeter with Cisco Products
Cisco IOS Security Features
Introducing the Cisco Integrated Services Router Family
Identity Solutions

Module 3: Securing LAN and WLAN Devices

Lesson 1: Applying Security Policies to Network Switches
Basic Switch Operation
Switches Are Targets
Securing Network Access to Layer 2 LAN Switches
Protecting Administrative Access to Switches
Protecting Access to the Management Port
Turning Off Unused Network Interfaces and Services

Lesson 2: Mitigating Layer 2 Attacks
Mitigating VLAN Hopping Attacks
Preventing STP Manipulation
Mitigating DHCP Server Spoofing with DHCP Snooping
Mitigating ARP Spoofing with DAI
CAM Table Overflow Attacks
MAC Address Spoofing Attacks
Using Port Security to Prevent Attacks
Configuring Cisco Catalyst Switch Port Security
Layer 2 Best Practices

Lesson 3: Using Cisco Catalyst Switch Security Features
Security Features in Cisco Catalyst Switches
Identity-Based Networking Services
VLAN ACLs
Private VLANs
MAC Address Notification
Rate Limiting
SPAN for IPS
Management Encryption

Lesson 4: Securing WLANs
Introducing WLANs
Threats to WLANs
Evolution of 802.11 Security Features
Service Set Identifier
Wired Equivalent Privacy
Enhanced Methods for WLAN Threat Mitigation
WLAN IDS

Securing Cisco Network Devices

Course Outline

Module 4: Cisco IOS Firewall Configuration

Lesson 1: Introducing Firewall Technologies

Explaining a Firewall
Evolution of Firewall Technologies
Static Packet Filtering Firewalls
Circuit Level Firewalls
Application Layer or Proxy Firewalls
Dynamic or Stateful Packet Filtering Firewalls
Cut-Through Proxy Process
Implementing NAT on a Firewall
Application Inspection Firewall
Firewalls in a Layered Defense Strategy

Lesson 2: Building Static Packet Filters with Cisco ACLs

Access Control Lists
Cisco ACLs
Applying ACLs to Router Interfaces
Using ACLs to Filter Traffic
Filtering Router Service Traffic
Filtering Network Traffic to Mitigate Threats
Mitigating DDoS Attacks with ACLs
Combining Access Functions
Caveats

Lesson 3: Configuring a Cisco IOS Firewall with the Cisco SDM Firewall Wizard

Cisco SDM Firewall Wizard Tasks
Configuring a Basic Firewall
Configuring an Advanced Firewall
Configuring Firewall Inspection Rules
Application Security Policy Configuration
Delivering the Configuration to the Router
Editing Firewall Policies and ACLs

Lesson 4: Defending Your Network with the Cisco Security Appliance Product Family

Introducing the Cisco Security Appliance Product Family
Cisco IOS Firewall Features
When to Choose a Cisco IOS Firewall Solution
Introducing Cisco PIX 500 Series Security Appliances
Introducing Cisco ASA 5500 Series Adaptive Security Appliances
Developing an Effective Firewall Policy

Module 5: Securing Networks with Cisco IOS IPS

Lesson 1: Introducing IDS and IPS

Introducing IDS and IPS
Types of IDS and IPS Sensors
Intrusion Prevention Technologies
HIPS and Network IPS
Introducing Signatures
Examining SDFs and Signature Micro-Engines
Introducing Signature Alarms

Lesson 2: Configuring Cisco IOS IPS

Cisco IOS IPS Features
Configuring Cisco IOS IPS Using Cisco SDM
Using the Cisco SDM GUI for IPS
Configuring IPS Rules
Configuring IPS Signatures
Configuring Global Settings
Delivering the Configuration to the Router

Lesson 3: Defending Your Network with the Cisco IPS Product Family

Network IPS Solutions
HIPS Solutions
Positioning IPS Solutions
IPS Best Practices

Module 6: Building IPsec VPNs

Lesson 1: Introducing IPsec VPNs

IPsec Overview
Internet Key Exchange
IKE: Other Functions
ESP and AH Protocols, Transport and Tunnel Modes
Message Authentication and Integrity Check
Symmetric vs. Asymmetric Encryption Algorithms
PKI Environment

CISCO PARTNER Learning Solutions

Securing Cisco Network Devices

Course Outline

Module 6: Building IPsec VPNs (Cont.)

Lesson 2: Building a Site-to-Site IPsec VPN Operation
Site-to-Site IPsec VPN Operations
Configuring IPsec
Site-to-Site IPsec Configuration—Phase 1
Site-to-Site IPsec Configuration—Phase 2
Site-to-Site IPsec Configuration—Apply VPN Configuration
Site-to-Site IPsec Configuration—Interface Access List

Lesson 3: Configuring IPsec Site-to-Site VPNs Using Cisco SDM
Introducing the Cisco SDM VPN Wizard Interface
Site-to-Site VPN Components
Launching the Site-to-Site VPN Wizard
Connection Settings
IKE Proposals
Transform Set
Defining What Traffic to Protect
Completing the Configuration

Lesson 4: Building Remote-Access VPNs
Cisco Easy VPN
Configuring Cisco Easy VPN Server
Managing Cisco Easy VPN Server Connections
Configuring Cisco Easy VPN Remote

Lesson 5: Defending Your Network with the Cisco VPN Product Family
Secure Connectivity—VPN Solutions
Secure Connectivity—Cisco VPN Product Family
Secure Connectivity—VPN Product Positioning
Cisco VPN Best Practices

Lab 1-1: Discovering Network Vulnerabilities and Threats

Case Study 1-1: Developing a Comprehensive Network Security Policy

Lab 2-1: Securing Administrative Access to Cisco Routers

Lab 2-2: Configuring AAA for Cisco Routers

Lab 2-3: Using Cisco SDM Security Audit

Case Study 3-1: Using Cisco Catalyst Switch Security Features

Lab 4-1: Configuring a Cisco IOS Firewall

Lab 5-1: Configuring Cisco IOS IPS

Lab 6-1: Configuring Site-to-Site IPSec VPNs

Lab 6-2: Configuring a Remote-Access VPN Client