Securing Networks with Cisco Routers and Switches

Length
5 days

Format
Lecture/lab

Version
3.0

Course Description

SNRS 1.0 is a 5-day, lab-intensive course that provides the knowledge and skills needed to secure Cisco IOS router and switch networks. You will learn how to secure the network using Cisco IOS and CatOS security features, configure the Cisco IOS Firewall, implement secure tunnels, and complete a security audit.

Who Should Attend

This course is designed for network professionals tasked with designing and deploying Cisco security features in a Cisco IOS-based internetwork. It is also recommended for anyone pursuing Cisco Certified Security Professional (CCSP), Cisco Security Specialist certifications, or the Information Systems Security (INFOSEC) Professional certification.

Recommended Prerequisites

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

Related Courses

- Introduction to Cisco Networking Technologies (INTRO)
- Interconnecting Cisco Network Devices (ICND)
- Securing Cisco Network Devices (SND)

SNRS

Learning Objectives

After completing this course, you will be able to:

- Configure, operate, and troubleshoot Cisco Secure ACS for Windows Server
- Install, maintain and troubleshoot Cisco IOS Firewall including Authentication Proxy, Context Based Access Control (CBAC) and Intrusion Prevention System (IPS)
- Implement IPSec VPNs using IOS Routers in site to site and remote access configurations, including using digital certificates
- Use the Cisco Security Device Manager (SDM) to complete a wide range of configuration tasks on an IOS router

CISCO PARTNER
Learning Solutions

Securing Networks with Cisco Routers and Switches

Course Outline

Module 1: Layer 2 Security

Lesson 1: Examining Company ABC Unsecured

Company ABC Unsecured
Attacks and Vulnerabilities
Attacks on Company ABC

Lesson 2: Examining Layer 2 Attacks

Types of Layer 2 Attacks
CAM Table Overflow Attack
Port Security
Verifying Port Security
VLAN Hopping Attacks
STP Vulnerabilities
MAC Spoofing: Man-in-the-Middle Attacks
PVLAN Vulnerabilities

Lesson 3: Configuring DHCP Snooping

DHCP Starvation and Spoofing Attacks
Understanding DHCP Snooping
Mitigating DHCP Attacks
DHCP Snooping Configuration Guidelines
Enabling and Configuring DHCP Snooping
Verifying DHCP Snooping

Module 2: Trust and Identity

Lesson 1: Implementing Identity Management

Cisco Secure ACS for Windows Overview
Authentication, Authorization, and Accounting
Authentication
Authorization
Accounting
TACACS+
RADIUS
Configuring AAA to Work with External AAA Servers
Cisco Secure ACS as a AAA Server
Cisco Secure ACS for Microsoft Windows Architecture
Administering Cisco Secure ACS
Installing Cisco Secure ACS
Creating an Installation
Adding an Administrator
Working in Cisco Secure ACS
Network Access Profiles
Configuring Cisco Secure ACS NAPs
Creating a NAP
Configuring Profile-Based Policies
Troubleshooting Cisco Secure ACS

Lesson 2: Implementing Cisco IBNS

Cisco IBNS Overview
Port-Based Access Control
IEEE 802.1x
Selecting the Correct EAP
802.1x and Port Security
802.1x and VLAN Assignment
802.1x and Guest VLANs
802.1x and Restricted VLANs
Configuring 802.1x

Module 3: Cisco Network Foundation Protection

Lesson 1: Introducing Cisco NFP

Cisco NFP Overview
Cisco IOS Tools for a Secure Infrastructure

Lesson 2: Securing the Control Plane

Router Control Plane
Tools for Securing the Control Plane
Overview of CPPr
CPPr Architecture
Configuring CPPr
Configuring a Port-Filter Policy
Configuring a Queue-Threshold Policy
Verifying CPPr

Lesson 3: Securing the Management Plane

The Management Plane
Tools for Securing the Management Plane
Cisco MPP Feature
Securing the Management Plane
Verifying MPP

Lesson 4: Securing the Data Plane

Data Plane Attacks
Data Plane Protection
Flexible Packet Matching
Configuring FPM
Verifying FPM
Troubleshooting FPM

Securing Networks with Cisco Routers and Switches

Course Outline

Module 4: Secured Connectivity

Lesson 1: Introducing IPsec
IPsec Overview
Authentication Header
Encapsulating Security Payload
Internet Key Exchange
Internet Security Association and Key Management Protocol
Other Protocols and Terminology
IPsec Configuration Task List

Lesson 2: Examining Cisco IOS VPNs
IPsec VPN Deployment Options
Fully Meshed IPsec VPNs
Hub-and-Spoke IPsec VPNs
Characteristics
Benefits
Restrictions
Dynamic Multipoint VPNs
Cisco Easy VPN
WebVPN

Lesson 3: Implementing IPsec VPNs Using Pre-Shared Keys
Configuring IPsec
Preparing for IPsec
Planning the IKE Policy
Planning the IPsec Policy
Configuring ISAKMP
Configure Pre-Shared Keys
Configuring IPsec Policies
Applying Crypto Maps to Interfaces
Testing and Verifying IPsec
Troubleshooting

Lesson 4: Implementing IPsec VPNs Using PKI
Examining Cisco IOS PKI
Digital Signatures
Examining SCEP
Configuring IPsec VPN Using Digital Certificates
Testing and Verifying IPsec

Lesson 5: Configuring GRE Tunnels
Examining GRE Tunnels
Deploying GRE
Configuring a GRE Tunnel
Verifying GRE Tunnels
Configuring GRE Tunnels and Encryption

Lesson 6: Configuring a DMVPN
Dynamic Multipoint VPN
DMVPN Configuration Tasks
Configuring ISAKMP and IPsec
IPsec Profiles
Routing Protocols
Configuring the Hub in a Spoke-to-Spoke DMVPN
Configuring a Spoke for the Spoke-to-Spoke DMVPN
Verifying DMVPN

Lesson 2: Generating Reports
Types of Reports
How to Generate an Events by Severity Report
How to Generate an Events by Group Report
How to Generate a Group Detail Report
How to Generate a Host Detail Report
How to Generate a Policy Detail Report
How to View the Audit Trail

Lesson 7: Configuring Cisco IOS SSL VPN (WebVPN)
Overview of Cisco IOS SSL VPN (WebVPN)
Clientless Access
Thin-Client Access
Tunnel Mode Access
WebVPN Configuration Tasks
AAA Configuration for WebVPN
DNS Configuration for WebVPN
Certificates and Trustpoints for WebVPN
WebVPN Configuration
Verifying WebVPN Functionality
Troubleshooting WebVPN

Lesson 8: Configuring Easy VPN Remote Access
Introduction to Cisco Easy VPN
Configuring Cisco Easy VPN Server
Configuring Cisco VPN Client v4.x
Create New Client Connection Entries

Securing Networks with Cisco Routers and Switches

Course Outline

Module 5: Adaptive Threat Defense

Lesson 1: Configuring Cisco IOS Firewall Firewalls
Cisco IOS as a Firewall
Cisco IOS Firewall Feature Set
Cisco IOS Classic Firewall
Cisco IOS Authentication Proxy
Cisco IOS IPS

Lesson 2: Configuring Cisco IOS Classic Firewall
Cisco IOS Classic Firewall
Cisco IOS Classic Firewall Process
Cisco IOS Classic Firewall Configuration Tasks
Configuring IP ACLs for Cisco IOS Classic Firewall
Defining Inspection Rules
Example Configurations
Granular Protocol Inspection
Applying the Inspection Rule to an Interface
Audit Trails and Logging
Verifying Cisco IOS Classic Firewall
Removing Cisco IOS Classic Firewall

Lesson 3: Configuring Cisco IOS Zoned-Based Policy Firewall
Legacy Stateful Inspection
Cisco IOS Zone-Based Policy Firewall Overview
Zones
Security Zone Firewall Policies
Configuring a Cisco IOS Zoned-Based Policy Firewall
Verifying Cisco IOS Zone-Based Policy Firewall

Lesson 4: Configuring Cisco IOS Firewall Authentication Proxy
Cisco IOS Firewall Authentication Proxy
AAA Server Configuration
Cisco IOS Firewall Authentication Proxy Configuration

Lesson 5: Configuring Cisco IOS IPS
Cisco IOS IPS
Signature Micro-Engines
Signatures and SDFs
Deploying IOS IPS
Cisco IOS Firewall IPS Configuration
Configure Logging via Syslog or SDEE
Upgrading to the Latest SDF
Verifying IPS Configuration

Lesson 6: Examining Company ABC Secured
Company ABC Secured

Securing Networks with Cisco Routers and Switches

Course Labs

Lab 1-1: Configure Layer 2 Security

Lab 1-2: Configure DHCP Snooping

Lab 2-1: Configure Cisco Secure ACS as a AAA Server

Lab 2-2: Configure 802.1x Port-Based Authentication

Lab 3-1: Configure Cisco NFP

Lab 4-1: Configure a Site-to-Site VPN Using Pre-Shared Keys

Lab 4-2: Configure a Site-to-Site VPN Using PKI

Lab 4-3: Configure a GRE Tunnel to a Remote Site

Lab 4-4: Configure a DMVPN

Lab 4-5: Configure a Cisco IOS SSL VPN (WebVPN)

Lab 4-6: Configure Cisco Easy VPN Remote Access

Lab 5-1: Configure Cisco IOS Classic Firewall

Lab 5-2: Configure Cisco IOS Application Policy Firewall

Lab 5-3: Configure a Cisco IOS Zone-Based Policy Firewall

Lab 5-4: Configure Cisco IOS Firewall Authentication Proxy on a Cisco Router

Lab 5-5: Configure a Cisco Router with Cisco IOS IPS