Cisco CCNA Security Day

About This Course

Cisco Certified Network Associate Security (CCNA Security) validates associate-level knowledge and skills required to secure Cisco networks. With a CCNA Security certification, a network professional demonstrates the skills required to develop a security infrastructure, recognize threats and vulnerabilities to networks, and mitigate security threats. The CCNA Security curriculum emphasizes core security technologies, the installation, troubleshooting and monitoring of network devices to maintain integrity, confidentiality and availability of data and devices, and competency in the technologies that Cisco uses in its security structure.

Required Exams

Implementing Cisco Network Security (210-260)

Audience Profile

The CCNA Security certification is for IT professionals looking to expand upon and document their existing skills in CISCO technology. This course is intended for students seeking to earn their CCNA Security certification and who need an expert instructor to guide them throughout the training and exam preparation process.

Course Objectives

The CCNA Security course helps you master the following topics:

* Security concepts and threats
* Implementing AAA using IOS and ISE
* Bring Your Own Device (BYOD)
* VPN technology and cryptography
* IP security
* Implementing IPsec site-to-site VPNs
* Implementing SSL remote-access VPNs using Cisco ASA
* Securing Layer 2 technologies
* Network Foundation Protection (NFP)
* Securing the management, data, and control planes
* Understand, implement, and configure Cisco firewall technologies
Outline

Part I Fundamentals of Network Security

Chapter 1 Networking Security Concepts

Foundation Topics

Understanding Network and Information Security Basics

  - Network Security Objectives
  - Confidentiality, Integrity, and Availability
  - Cost-Benefit Analysis of Security
  - Classifying Assets
  - Classifying Vulnerabilities
  - Classifying Countermeasures
  - What Do We Do with the Risk?

Recognizing Current Network Threats

  - Potential Attackers
  - Attack Methods
  - Attack Vectors
  - Man-in-the-Middle Attacks
  - Other Miscellaneous Attack Methods

Applying Fundamental Security Principles to Network Design

  - Guidelines
  - Network Topologies
  - Network Security for a Virtual Environment
Chapter 2 Common Security Threats

Foundation Topics

Network Security Threat Landscape

Distributed Denial-of-Service Attacks

Social Engineering Methods

Social Engineering Tactics

Defenses Against Social Engineering

Malware Identification Tools

Methods Available for Malware Identification

Data Loss and Exfiltration Methods

Part II Secure Access

Chapter 3 Implementing AAA in Cisco IOS

Foundation Topics

Cisco Secure ACS, RADIUS, and TACACS

Why Use Cisco ACS?

On What Platform Does ACS Run?

What Is ISE?

Protocols Used Between the ACS and the Router

Protocol Choices Between the ACS Server and the Client (the Router)

Configuring Routers to Interoperate with an ACS Server

Configuring the ACS Server to Interoperate with a Router

Verifying and Troubleshooting Router-to-ACS Server Interactions

Chapter 4 Bring Your Own Device (BYOD)
Foundation Topics

Bring Your Own Device Fundamentals

BYOD Architecture Framework

BYOD Solution Components

Mobile Device Management

MDM Deployment Options

On-Premise MDM Deployment

Cloud-Based MDM Deployment

Part III Virtual Private Networks (VPN)

Chapter 5 Fundamentals of VPN Technology and Cryptography

Foundation Topics

Understanding VPNs and Why We Use Them

What Is a VPN?

Types of VPNs

Two Main Types of VPNs

Main Benefits of VPNs

Confidentiality

Data Integrity

Authentication

Antireplay Protection

Cryptography Basic Components

Ciphers and Keys

Ciphers

Keys

Block and Stream Ciphers
Block Ciphers

Stream Ciphers

Symmetric and Asymmetric Algorithms

Symmetric

Asymmetric

Hashes

Hashed Message Authentication Code

Digital Signatures

Digital Signatures in Action

Key Management

Next-Generation Encryption Protocols

IPsec and SSL

IPsec

SSL

Public Key Infrastructure

Public and Private Key Pairs

RSA Algorithm, the Keys, and Digital Certificates

Who Has Keys and a Digital Certificate?

How Two Parties Exchange Public Keys

Creating a Digital Signature

Certificate Authorities

Root and Identity Certificates

Root Certificate

Identity Certificate
Using the Digital Certificates to Get the Peer's Public Key

X.500 and X.509v3 Certificates

Authenticating and Enrolling with the CA

Public Key Cryptography Standards

Simple Certificate Enrollment Protocol

Revoked Certificates

Uses for Digital Certificates

PKI Topologies

Single Root CA

Hierarchical CA with Subordinate CAs

Cross-Certifying CAs

Putting the Pieces of PKI to Work

ASA's Default Certificate

Viewing the Certificates in ASDM

Adding a New Root Certificate

Easier Method for Installing Both Root and Identity Certificates

Chapter 6 Fundamentals of IP Security

Foundation Topics

IPsec Concepts, Components, and Operations

The Goal of IPsec

The Internet Key Exchange (IKE) Protocol

The Play by Play for IPsec

Step 1: Negotiate the IKEv1 Phase 1 Tunnel

Step 2: Run the DH Key Exchange

Step 3: Authenticate the Peer
What About the User’s Original Packet?

Leveraging What They Have Already Built

Now IPsec Can Protect the User’s Packets

Traffic Before IPsec

Traffic After IPsec

Summary of the IPsec Story

Configuring and Verifying IPsec

Tools to Configure the Tunnels

Start with a Plan

Applying the Configuration

Viewing the CLI Equivalent at the Router

Completing and Verifying IPsec

Chapter 7 Implementing IPsec Site-to-Site VPNs

Foundation Topics

Planning and Preparing an IPsec Site-to-Site VPN

Customer Needs

Planning IKEv1 Phase 1

Planning IKEv1 Phase 2

Implementing and Verifying an IPsec Site-to-Site VPN in Cisco IOS Devices

Troubleshooting IPsec Site-to-Site VPNs in Cisco IOS

Implementing and Verifying an IPsec Site-to-Site VPN in Cisco ASA

Troubleshooting IPsec Site-to-Site VPNs in Cisco ASA

Chapter 8 Implementing SSL VPNs Using Cisco ASA

Foundation Topics
Functions and Use of SSL for VPNs

Is IPsec Out of the Picture?

SSL and TLS Protocol Framework

The Play by Play of SSL for VPNs

SSL VPN Flavors

Configuring Clientless SSL VPNs on ASA

Using the SSL VPN Wizard

Digital Certificates

Accessing the Connection Profile

Authenticating Users

Logging In

Seeing the VPN Activity from the Server

Using the Cisco AnyConnect Secure Mobility Client

Types of SSL VPNs

Configuring the Cisco ASA to Terminate the Cisco AnyConnect Secure Mobility Client Connections

Groups, Connection Profiles, and Defaults

One Item with Three Different Names

Split Tunneling

Troubleshooting SSL VPN

Troubleshooting SSL Negotiations

Troubleshooting AnyConnect Client Issues

Initial Connectivity Issues

Traffic-Specific Issues

Part IV Secure Routing and Switching

Chapter 9 Securing Layer 2 Technologies
Foundation Topics

VLAN and Trunking Fundamentals

What Is a VLAN?

Trunking with 802.1Q

Following the Frame, Step by Step

The Native VLAN on a Trunk

So, What Do You Want to Be? (Asks the Port)

Inter-VLAN Routing

The Challenge of Using Physical Interfaces Only

Using Virtual "Sub" Interfaces

Spanning-Tree Fundamentals

Loops in Networks Are Usually Bad

The Life of a Loop

The Solution to the Layer 2 Loop

STP Is Wary of New Ports

Improving the Time Until Forwarding

Common Layer 2 Threats and How to Mitigate Them

Disrupt the Bottom of the Wall, and the Top Is Disrupted, Too

Layer 2 Best Practices

Do Not Allow Negotiations

Layer 2 Security Toolkit

Specific Layer 2 Mitigation for CCNA Security

BPDU Guard

Root Guard
Chapter 10 Network Foundation Protection

Foundation Topics

Using Network Foundation Protection to Secure Networks

- The Importance of the Network Infrastructure
- The Network Foundation Protection Framework
- Interdependence
- Implementing NFP

Understanding the Management Plane

- First Things First
- Best Practices for Securing the Management Plane

Understanding the Control Plane

- Best Practices for Securing the Control Plane

Understanding the Data Plane

- Best Practices for Protecting the Data Plane
- Additional Data Plane Protection Mechanisms

Chapter 11 Securing the Management Plane on Cisco IOS Devices

Foundation Topics

Securing Management Traffic

- What Is Management Traffic and the Management Plane?
- Beyond the Blue Rollover Cable
- Management Plane Best Practices
Password Recommendations

Using AAA to Verify Users

AAA Components

Options for Storing Usernames, Passwords, and Access Rules

Authorizing VPN Users

Router Access Authentication

The AAA Method List

Role-Based Access Control

Custom Privilege Levels

Limiting the Administrator by Assigning a View

Encrypted Management Protocols

Using Logging Files

Understanding NTP

Protecting Cisco IOS Files

Implementing Security Measures to Protect the Management Plane

Implementing Strong Passwords

User Authentication with AAA

Using the CLI to Troubleshoot AAA for Cisco Routers

RBAC Privilege Level/Parser View

Implementing Parser Views

SSH and HTTPS

Implementing Logging Features

Configuring Syslog Support

SNMP Features
Configuring NTP

Secure Copy Protocol

Securing the Cisco IOS Image and Configuration Files

Chapter 12 Securing the Data Plane in IPv6

Foundation Topics

Understanding and Configuring IPv6

Why IPv6?

The Format of an IPv6 Address

Understanding the Shortcuts

Did We Get an Extra Address?

IPv6 Address Types

Configuring IPv6 Routing

Moving to IPv6

Developing a Security Plan for IPv6

Best Practices Common to Both IPv4 and IPv6

Threats Common to Both IPv4 and IPv6

The Focus on IPv6 Security

New Potential Risks with IPv6

IPv6 Best Practices

IPv6 Access Control Lists

Chapter 13 Securing Routing Protocols and the Control Plane

Foundation Topics

Securing the Control Plane

Minimizing the Impact of Control Plane Traffic on the CPU

Control Plane Policing
Control Plane Protection

Securing Routing Protocols

Implement Routing Update Authentication on OSPF
Implement Routing Update Authentication on EIGRP
Implement Routing Update Authentication on RIP
Implement Routing Update Authentication on BGP

Part V Cisco Firewall Technologies and Intrusion Prevention System Technologies

Chapter 14 Understanding Firewall Fundamentals

Foundation Topics

Firewall Concepts and Technologies

Firewall Technologies

Objectives of a Good Firewall

Firewall Justifications

The Defense-in-Depth Approach

Firewall Methodologies

Static Packet Filtering

Application Layer Gateway

Stateful Packet Filtering

Application Inspection

Transparent Firewalls

Next-Generation Firewalls

Using Network Address Translation

NAT Is About Hiding or Changing the Truth About Source Addresses

Inside, Outside, Local, Global
Chapter 16 Configuring Basic Firewall Policies on Cisco ASA

Foundation Topics

The ASA Appliance Family and Features

- Meet the ASA Family
- ASA Features and Services

ASA Firewall Fundamentals

- ASA Security Levels
- The Default Flow of Traffic

Tools to Manage the ASA

Initial Access

Packet Filtering on the ASA

Implementing a Packet-Filtering ACL

Modular Policy Framework

Where to Apply a Policy

Configuring the ASA

Beginning the Configuration

Getting to the ASDM GUI

Configuring the Interfaces

IP Addresses for Clients

Basic Routing to the Internet

NAT and PAT

Permitting Additional Access Through the Firewall

Using Packet Tracer to Verify Which Packets Are Allowed

Verifying the Policy of No Telnet
Chapter 17 Cisco IDS/IPS Fundamentals

Foundation Topics

IPS Versus IDS

What Sensors Do

Difference Between IPS and IDS

Sensor Platforms

True/False Negatives/Positives

Positive/Negative Terminology

Identifying Malicious Traffic on the Network

Signature-Based IPS/IDS

Policy-Based IPS/IDS

Anomaly-Based IPS/IDS

Reputation-Based IPS/IDS

When Sensors Detect Malicious Traffic

Controlling Which Actions the Sensors Should Take

Implementing Actions Based on the Risk Rating

Circumventing an IPS/IDS

Managing Signatures

Signature or Severity Levels

Monitoring and Managing Alarms and Alerts

Security Intelligence

IPS/IDS Best Practices

Cisco Next-Generation IPS Solutions

Part VI Content and Endpoint Security

Chapter 18 Mitigation Technologies for E-mail-Based and Web-Based Threats
Foundation Topics

Mitigation Technology for E-mail-Based Threats

E-mail-Based Threats

Cisco Cloud E-mail Security

Cisco Hybrid E-mail Security

Cisco E-mail Security Appliance

Cisco ESA Initial Configuration

Mitigation Technology for Web-Based Threats

Cisco CWS

Cisco WSA

Cisco Content Security Management Appliance

Chapter 19 Mitigation Technologies for Endpoint Threats

Foundation Topics

Antivirus and Antimalware Solutions

Personal Firewalls and Host Intrusion Prevention Systems

Advanced Malware Protection for Endpoints

Hardware and Software Encryption of Endpoint Data

E-mail Encryption

Encrypting Endpoint Data at Rest

Virtual Private Networks