Network Masters™
KNOWLEDGE AND TECHNOLOGY TOGETHER

CCNA Security

Course Outline

MODULE I Fundamentals of Network Security

Lesson 1 Networking Security Concepts and Common Principles
Lesson 1.1 Understanding Network And Information Security Basics
Lesson 1.2 Confidentiality, Integrity, And Availability
Lesson 1.3 Classifying Assets
Lesson 1.4 Types of Security Vulnerabilities
Lesson 1.5 Classifying Countermeasures
Lesson 1.6 Attack Methods & Vectors
Lesson 1.7 Applying Fundamental Security Principles To Network Design
Lesson 1.8 Understanding Security Attack Surface in Different Network Topologies
Lesson 2 Common Security Threats
Lesson 2.1 Network Security Threat Landscape
Lesson 2.2 Distributed Denial of Service (DDoS) Attacks
Lesson 2.3 Social Engineering Methods
Lesson 2.4 Man-in-the-middle Attacks
Lesson 2.5 Malware Identification Tools
Lesson 2.6 Data Loss and Exfiltration Methods

MODULE II Virtual Private Networks (VPNs)

Lesson 3 Fundamentals of VPN Technology and Cryptography
Lesson 3.1 Understanding VPNs and Why We Use Them
Lesson 3.2 Cryptography Basic Components
Lesson 3.3 Public Key Infrastructure
Lesson 3.4 Putting the Pieces of PKI to Work
Lesson 4 Fundamentals of IP Security
Lesson 4.1 IPsec Concepts, Components, and Operations
Lesson 4.2 IKE version 1 Fundamentals
Lesson 4.4 IKE version 2 Fundamentals
Lesson 5 Implementing IPsec Site-to-Site VPNs
Lesson 5.1 Configuring IPsec Site-to-Site VPNs in Cisco IOS Devices
Lesson 5.2 Troubleshooting IPsec Site-to-Site VPNs in Cisco IOS Devices
Lesson 5.3 Configuring IPsec Site-to-Site VPNs in Cisco ASA
Lesson 5.4 Troubleshooting IPsec Site-to-Site VPNs in Cisco ASA
Lesson 6 Implementing SSL Remote Access VPNs Using Cisco ASA
Lesson 6.1 Introduction to Clientless SSL VPN
Lesson 6.2 Configuring Clientless SSL VPNs in the Cisco ASA
Lesson 6.3 Introduction to AnyConnect
Lesson 6.4 Installing AnyConnect
Lesson 6.5 AnyConnect for Mobile Devices

Lesson 6.6 Configuring AnyConnect SSL VPN Connections in the Cisco ASA
Lesson 6.7 Troubleshooting SSL VPN in the Cisco ASA

MODULE III Content and Endpoint Security

Lesson 7 Mitigation Technologies for Email-based and Web-based Threats
Lesson 7.1 Introduction to E-mail-Based Threats and Email Security
Lesson 7.2 Cisco Cloud E-mail Security
Lesson 7.3 Cisco Hybrid E-mail Security
Lesson 7.4 Cisco E-mail Security Appliance
Lesson 7.5 Introduction to Cisco Web Security
Lesson 7.6 Cisco Cloud Web Security (CWS)
Lesson 7.7 Cisco Web Security Appliance (WSA)
Lesson 7.8 Cisco Content Security Management Appliance (SMA)
Lesson 8 Mitigation Technology for Endpoint Threats
Lesson 8.1 Antivirus and Anti-malware Solutions
Lesson 8.2 Personal Firewalls And Host Intrusion Prevention Systems
Lesson 8.3 Cisco Advanced Malware Protection (AMP) For Endpoints
Lesson 8.4 Hardware and Software Encryption Of Endpoint Data

MODULE IV Cisco Firewall Technologies and Intrusion Prevention System Technologies

Lesson 9 Understanding Firewall Fundamentals
Lesson 9.1 What is a Firewall and How They are Used
Lesson 9.2 Understanding Stateful vs Stateless Inspection
Lesson 9.3 Network Address Translation (NAT) Overview
Lesson 10 Implementing Cisco IOS Zone-Based Firewalls
Lesson 10.1 Differences between IOS Firewalls and the ASA Firewall Appliance
Lesson 10.2 Basic Configuration and Features
Lesson 10.3 NAT Configuration on the IOS Firewall
Lesson 10.4 Using Cisco Configuration Professional (CCP)
Lesson 11 Configuring Basic Firewall Policies on Cisco ASA
Lesson 11.1 Basic Configuration of the ASA
Lesson 11.2 Introduction to Network Objects and Access Control Policies
Lesson 11.3 NAT Configuration on the ASA
Lesson 11.4 Advanced Deployment Scenarios — High Availability
Lesson 12 Cisco IPS Fundamentals
Lesson 12.1 IPS Inspection vs Firewall Inspection
Lesson 12.2 IPS Deployment Considerations
Lesson 12.3 Tuning the IPS for Inspection - Basics
Lesson 12.4 Tuning the IPS for Inspection - Signatures
Lesson 12.5 IOS IPS Configuration

MODULE V Secure Routing and Switching

Lesson 13 Securing Layer 2 Technologies
Lesson 13.1 L2 Attack and Defense on Cisco Switches
Lesson 13.3 Spanning-Tree Issues and Troubleshooting
Lesson 13.3 All About VLANs
Lesson 13.4 VLAN Security
Lesson 14 Network Foundation Protection
Lesson 14.1 NPF Overview (Management, Control & Data Planes)
Lesson 15 Securing the Management Plane on Cisco IOS Devices
Lesson 15.1 Introduction to the Management Plane & AAA
Lesson 15.2 Protecting Access to IOS
Lesson 15.3 RADIUS vs. TACACS+
Lesson 15.4 Configuring & Troubleshooting AAA
Lesson 15.5 Privilege Levels and Parser Views
Lesson 15.6 Configuring Secure Management Protocols
Lesson 15.7 Using CCP
Lesson 16 Securing the Data Plane
Lesson 16.1 What is IPv6
Lesson 16.2 Security Plan for IPv4 and IPv6
Lesson 16.3 New Threats with IPv6
Lesson 16.4 IPv6 ACLs
Lesson 16.5 Understanding the Data Plane
Lesson 17 Securing Routing Protocols and the Control Plane
Lesson 17.1 Understanding the Control Plan
Lesson 17.2 Control Plane Policing/Protection
Lesson 17.3 IPv6 Routing
Lesson 17.4 Securing Routing Protocols

MODULE VI Secure Access

Lesson 18 Implementing AAA Using IOS and ISE
Lesson 18.1 Compare ACS and ISE
Lesson 18.2 Configuring IOS for Device Admin with ACS
Lesson 18.3 Verifying AAA with IOS and ACS
Lesson 18.4 Network Access Control with ISE
Lesson 18.5 Configuring IOS for Network Access with ISE
Lesson 18.6 Verifying AAA with IOS and ISE
Lesson 19 Bring Your Own Device (BYOD)
Lesson 19.1 What is BYOD
Lesson 19.2 BYOD Architecture and Components
Lesson 19.3 Mobile Device Management