CISCO CCNA SECURITY BOOT CAMP (ACCELERATED)

DURATION: 5 DAYS

COURSE OVERVIEW

In this course, you will learn how to install, operate, configure, and verify a basic IPv4 and IPv6 network, including configuring a LAN switch, configuring an IP router, managing network devices. You will also learn about the design, implementation, and monitoring of a comprehensive security policy using Cisco IOS security features and technologies as examples. You will also learn about security controls of Cisco IOS devices as well as a functional introduction to the Cisco Adaptive Security Appliance (ASA).

This course enables you to perform basic tasks to secure a network using Cisco IOS security features, which are available through web-based GUIs on the Cisco ASA, and the command-line interface (CLI) on Cisco routers and switches.

Site-to-site virtual private network (VPN) configuration is covered on both the Cisco IOS and the Cisco ASA. Modern malware examples are included in this course as are cryptographic techniques using stronger hashing and encryption algorithms. Current versions of Cisco IOS, Cisco ASA, and Cisco AnyConnect are featured.

This is an intensive accelerated class that runs over extended hours and is aimed at those students who already have some networking and security experience.

TARGET AUDIENCE

This is an intensive class and is aimed at students who already have some networking and security experience but who are looking to gain the

knowledge and skills required to attain the Cisco CCNA in Security accreditation or understand the Cisco security on the network.

COURSE OBJECTIVES

After completing this course you should be able to:

1. Understand Network fundamentals and common network security concepts.
2. Build simple LANs
3. Establish Internet connectivity
4. Manage and secure network devices
5. Expand small- to medium-sized networks
6. Understands IPv6 basics
7. Secure routing and switching infrastructure
8. Deploy basic authentication, authorization, and accounting services
9. Deploy basic firewalling services
10. Deploy basic site-to-site and remote access VPN services
11. Advanced security services such as intrusion protection, content security and identity management
12. Develop a comprehensive network security policy to counter threats against information security
13. Configure routers with Cisco IOS software security features, including management and reporting functions
14. Bootstrap the Cisco ASA Firewall for use in a production network
15. Configure the Cisco ASA Firewall for remote access to a Secure Sockets Layer (SSL) VPN
16. Configure a Cisco IOS zone-based firewall (ZBF) to perform basic security operations on a network
17. Configure site-to-site VPNs using Cisco IOS features
18. Configure security features on IOS switches to mitigate various Layer 2 and Layer 3 attacks
19. How a network can be compromised using freely available tools
20. Implement line passwords, and enable passwords and secrets
21. Examine authentication, authorization, and accounting (AAA) concepts and features using the local database as well as Cisco Secure ACS 5.2
22. Configure packet filtering on the perimeter router

COURSE CONTENT

Building a Simple Network

1. Functions of Networking
2. Host-to-Host Communications Model
3. Introducing LANs
4. Operating Cisco IOS Software
5. Starting a Switch
6. Ethernet and Switch Operation
7. Troubleshooting Common Switch Media Issues

Establishing Internet Connectivity

1. TCP/IP Internet Layer
2. IP Addressing and Subnets
3. TCP/IP Transport Layer
4. Functions of Routing
5. Configuring a Cisco Router
6. Packet Delivery Process
7. Enabling Static Routing
8. Basics of ACL

Building a Medium-Sized Network

1. Implementing VLANs and Trunks
2. Routing Between VLANs
3. Using a Cisco IOS Network Device as a DHCP Server
4. Implementing RIPv2

Network Device Management and Security

1. Securing Administrative Access
2. Implementing Device Hardening
3. Configuring System Message Logging
4. Managing Cisco Devices
5. Licensing

Introducing IPv6

1. Introducing Basic IPv6
2. IPv6 Operation
3. Configuring IPv6 Static Routes

Security Concepts

1. Threat scape
2. Threat defense technologies
3. Security policy and basic security architectures
4. Cryptographic technologies

Secure Network Devices

1. Implementing AAA
2. Management protocols and systems
3. Securing the control plane

Layer 2 Security

1. Securing Layer 2 infrastructures
2. Securing Layer 2 protocols

Firewall

1. Firewall technologies
2. Introducing the Cisco ASA v9.2
3. Cisco ASA access control and service policies
4. Cisco IOS zone based firewall

VPN

1. IPsec technologies
2. Site-to-site VPN
3. Client-based remote access VPN
4. Clientless remote access VPN

Advanced Topics

1. Intrusion detection and protection
2. Endpoint protection
3. Content security
4. Advanced network security architectures

Labs:

ICND1

1. Lab 1: Get Started with Cisco CLI
2. Lab 2: Perform Basic Switch Configuration
3. Lab 3: Observe How a Switch Operates
4. Lab 4: Troubleshoot Switch Media and Port Issues
5. Lab 5: Inspect TCP/IP Applications
6. Lab 6: Start with Cisco Router Configuration
7. Lab 7: Configure Cisco Discovery Protocol
8. Lab 8: Configure Default Gateway
9. Lab 9: Exploration of Packet Forwarding
10. Lab 10: Configure and Verify Static Routes
11. Lab 11: Configure and Verify ACLs
12. Lab 12: Configure a Provider-Assigned IP Address
13. Lab 13: Configure Static NAT
14. Lab 14: Configure Dynamic NAT and PAT
15. Lab 15: Troubleshoot NAT
16. Lab 16: Configure VLAN and Trunk
17. Lab 17: Configure a Router on a Stick
18. Lab 18: Configure a Cisco Router as a DHCP Server
19. Lab 19: Troubleshoot DHCP Issues
20. Lab 20: Configure and Verify RIPv2
21. Lab 21: Troubleshoot RIPv2
22. Lab 6: Summary Challenge Lab: 1
23. Lab 7: Summary Challenge Lab: 2
24. Lab 17: Implement IPv6 Static Routing

IINS

1. Lab 1: Exploring Cryptographic Technologies
2. Lab 2: Configure and Verify AAA
3. Lab 3: Configuration Management Protocols
4. Lab 4: Securing Routing Protocols
5. Lab 5: VLAN Security and ACLs on Switches
6. Lab 6: Port Security and Private VLAN Edge
7. Lab 7: Securing DHCP, ARP, and STP
8. Lab 8: Explore Firewall Technologies

9. Lab 9: Cisco ASA Interfaces and NAT
10. Lab 10: Access Control Using the Cisco ASA
11. Lab 11: Exploring Cisco IOS Zone-Based Firewall
12. Lab 12: Explore IPsec Technologies
13. Lab 13: IOS-Based Site-to-Site VPN
14. Lab 14: ASA-Based Site-to-Site VPN
15. Lab 15: Remote Access VPN: ASA and AnyConnect
16. Lab 16: Clientless Remote Access VPN

COURSE PREREQUISITES

Attendees should meet the following prerequisites:

1. Basic computer literacy
2. Basic Internet usage skills
3. Basic address knowledge
4. Working knowledge of the Windows operating system

TEST CERTIFICATION

Recommended as preparation for the following exams:

210-260 - IINS Implementing Cisco Network Security

100-105 - Interconnecting Cisco Networking Devices Part 1 - CCENT Certification

FOLLOW ON COURSES

The following courses are recommended for further study:

ICND2 - Interconnecting Cisco Networking Devices Part 2

SENSS - Implementing Cisco Edge Network Security Solutions

SIMOS - Implementing Cisco Secure Mobility

SITCS - Implementing Cisco Threat Control Systems

SISAS - Implementing Cisco Secure Access Solutions