IMPLEMENTING CISCO NETWORK SECURITY V3.0

DURATION: 5 DAYS

COURSE OVERVIEW

This is a five-day instructor-led course that focuses on the design, implementation and monitoring of a comprehensive security policy, using Cisco IOS security features and technologies. All IOS examples and hands on experience is done using the IOS CLI. IPS is covered at the theoretical level from the perspective of Fire Power technologies. Site-to-Site VPN configuration is covered on both IOS and the Cisco ASA. Modern malware examples are provided, cryptographic techniques use stronger hashing and encryption algorithms, and current versions of IOS, Cisco ASA and Cisco AnyConnect are highlighted.

More labs have been incorporated to ensure the maximum amount of hands on experience possible. There are two types of labs: Discovery and Challenge. A discovery is a guided lab exercise. Explicit directions are provided to the student to guide them through the activity. Along with the directions are scenarios and explanations specifying why the student is implementing the subject technology and the results after configuration are demonstrated.

Challenges, on the other hand, are evaluation labs. The set of tasks is provided to the student, but directions are not provided. There are job aids which the student may utilize, providing information such as IP addresses and command syntax, but no specific description of procedures. An answer key is available for students who wish to verify their techniques. The instructors will of course be on hand to revisit any areas that may need further clarification.

TARGET AUDIENCE

This course is aimed at individuals wishing to gain an understanding of Cisco Security on the network or those looking to obtain the Cisco Certified Network Associate for Security Certification.

COURSE OBJECTIVES

After you complete this course you should be able to:

1. Describe the current threat landscape
2. Secure the management and control planes of network devices
3. Describe threat defense technologies
4. Secure the management and control planes of network devices
5. Configure AAA on Cisco IOS devices

6. Implement secure management for the Cisco ASA and Cisco IOS routers and switches
7. Secure the control plane
8. Secure the management and control planes of network devices
9. Implement layer 2 infrastructure security
10. Implement layer 2 protocol security
11. Configure management access and NAT on the Cisco ASA
12. Configure access control and service policies on the Cisco ASA
13. Describe IPsec
14. Implement a client-based remote access VPN
15. Implement a clientless remote access VPN
16. Describe IDS and IPS
17. Describe endpoint protection
18. Describe content security
19. Describe advanced network security architectures
20.

COURSE CONTENT

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 Infrastructure
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

Challenge Lab 1: Configure AAA and Secure Remote Administration

Challenge Lab 2: Configure Secure Network Management Protocols

Challenge Lab 3: Configure Secure EIGRP Routing

Challenge Lab 4: Configure Secure Layer 2 Infrastructure

Challenge Lab 5: Configure DHCP Snooping and STP Protection

Challenge Lab 6: Configure Interfaces and NAT on the Cisco ASA

Challenge Lab 7: Configure Network Access Control with the Cisco ASA

Challenge Lab 8: Configure Site-to-Site VPN on IOS

Challenge Lab 9: Configure AnyConnect Remote Access VPN on ASA

Challenge Lab 10: Configure Clientless SSL VPN on the ASA

COURSE PREREQUISITES

Attendees should meet the following prerequisites:

ICND1 - Interconnecting Cisco Network Devices Part 1 is required.

TEST CERTIFICATION

Recommended preparation for exams:

210-260 - IINS Implementing Cisco Network Security

Delegates wishing to obtain the CCNA Security Certification will also need to have passed the ICND1 exam or the CCNA Routing and switching composite exam.

FOLLOW ON COURSES

Delegates looking to progress their Cisco Security Certification should consider the following courses.

1. SENSS -Implementing Cisco Edge Network Security Solutions
2. SIMOS - Implementing Cisco Secure Mobility
3. SISAS - Implementing Cisco Secure Access Solutions
4. SITCS - Implementing Cisco Threat Control Systems