IMPLEMENTING CISCO NETWORK SECURITY V3.0
(IINS v3)

Temario

In this course, you will 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 Any Connect are featured.

Pre-requisitos

- Working knowledge of the Windows operating system
- Working knowledge of Cisco IOS networking and concepts
- ICND1 v2.0 - Interconnecting Cisco Networking Devices, Part 1

Dirigido a

- Network designers
- Network, systems, and security engineers
- Network and security managers

Objetivos del curso

After you complete this course you will be able to:

- Common network security concepts
- Secure routing and switching infrastructure
- Deploy basic authentication, authorization, and accounting services
- Deploy basic firewalling services
- Deploy basic site-to-site and remote access VPN services
- Advanced security services such as intrusion protection, content security and identity management
- Develop a comprehensive network security policy to counter threats against information security
- Configure routers with Cisco IOS software security features, including management and reporting functions
- Bootstrap the Cisco ASA Firewall for use in a production network
- Configure the Cisco ASA Firewall for remote access to a Secure Sockets Layer (SSL) VPN
- Configure a Cisco IOS zone-based firewall (ZBF) to perform basic security operations on a network
- Configure site-to-site VPNs using Cisco IOS features
- Configure security features on IOS switches to mitigate various Layer 2 and Layer 3 attacks
- How a network can be compromised using freely available tools

- Implement line passwords, and enable passwords and secrets
- Examine authentication, authorization, and accounting (AAA) concepts and features using the local database as well as Cisco Secure ACS 5.2
- Configure packet filtering on the perimeter router

Contenido del curos

1. **Security Concepts**
    1. Threatscape
    2. Threat defense technologies
    3. Security policy and basic security architectures
    4. Cryptographic technologies

2. **Secure Network Devices**
    1. Implementing AAA
    2. Management protocols and systems
    3. Securing the control plane

3. **Layer 2 Security**
    1. Securing Layer 2 infrastructures
    2. Securing Layer 2 protocols

4. **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

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

6. **Advanced Topics**
    1. Intrusion detection and protection
    2. Endpoint protection
    3. Content security

   4. Advanced network security architectures

7. **Labs**
   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 1: ASA-Based Site-to-Site VPN
   15. Lab 14: Remote Access VPN: ASA and AnyConnect
   16. Lab 15: Clientless Remote Access VPN
   17. Lab 16: Configure AAA and Secure Remote Administration
   18. Lab 17: Configure Secure Network Management Protocols
   19. Lab 18: Configure Secure EIGRP Routing
   20. Lab 19: Configure Secure Layer 2 Infrastructure
   21. Lab 20: Configure DHCP Snooping and STP Protection
   22. Lab 21: Configure Interfaces and NAT on the Cisco ASA
   23. Lab 22: Configure Network Access Control with the Cisco ASA
   24. Lab 23: Configure Site-to-Site VPN on IOS
   25. Lab 24: Configure AnyConnect Remote Access VPN on ASA
   26. Lab 25: Configure Clientless SSL VPN on the ASA

This training prepares students for the following exam(s):

210-260 IINS : Implementing Cisco Network Security (IINS) 3.0