IINS 3.0 - Implementing Cisco IOS Network Security 3.0

(5 Days)

Course Overview:

Implementing Cisco IOS Network Security (IINS) v3.0 is a five-day instructor-led course that is presented by Cisco Learning Partners to end users and channel partner customers. The content focuses on the design, implementation, and monitoring of a comprehensive security policy, using Cisco IOS security features and technologies as examples. The course covers security controls of Cisco IOS devices as well as a functional introduction to the Cisco ASA adaptive security appliance. Using instructor-led discussion, lecture, and hands-on lab exercises, this course allows students to perform basic tasks to secure a small branch office network using Cisco IOS security features that are available through web-based GUIs (Cisco Configuration Professional) and the CLI on Cisco routers, switches, and ASA appliances.

Who will benefit from this course?

The primary audience for this course is as follows:

- Network designers
- Network administrators
- Network engineers
- Network managers
- System engineers

Prerequisites:

The knowledge and skills that a student must have before attending this course are as follows:

- Skills and knowledge equivalent to those learned in *Interconnecting Cisco Networking Devices Part 1* (ICND1)
- Working knowledge of the Windows operating system
- Working knowledge of Cisco IOS networking and concepts

Course Objectives:

Upon completing this course, the student will be able to meet these overall objectives:

- Describe the components of a comprehensive network security policy that can be used to counter threats against IT systems, within the context of a security policy life cycle
- Develop and implement security countermeasures that are aimed at protecting network elements as part of the network infrastructure
- Deploy and maintain threat control and containment technologies for perimeter security in small and midsize networks
- Describe secure connectivity strategies and technologies using VPNs, as well as configure site-to-site and remote-access VPNs using Cisco IOS features

Course Outline:

Module 1: Networking Security Fundamentals

Lesson 1: Introducing Networking Security Concepts

- Describe information security within the context of risk management and its underlying concepts
- Explain the motivation behind networking security, describing the business and security environment of organizations today
- Classify threat vectors according to multiple criteria, in order to define and plan mitigation strategies
- Analyze and compare design principles and considerations for network security

Lesson 2: Understanding Security Policies Using a Life-Cycle Approach

- Describe risk management within the context of business and organizational drivers
- Compare different compliance regulations and describe them as drivers of information security
- Provide a high-level definition of a security policy along with the benefits of creating a sound policy as part of the life-cycle process
- Analyze the benefits of using a life-cycle approach to information and network security
- Describe the assessment phases of the life-cycle approach, comparing and contrasting different methods and considerations
- Describe the testing phases of the life-cycle approach and how they relate to other phases
- Describe the incident response phases of the life-cycle approach, comparing high-level techniques that are commonly used to respond efficiently and effectively to security threats
- Describe the disaster recovery phases of the life-cycle approach and their importance in business continuity

Lesson 3: Building a Security Strategy for Borderless Networks

- Describe the Cisco Borderless Networks Architecture to position it as a framework to present the Cisco security portfolio of products
- Describe the Cisco SecureX Architecture at a high level, highlighting its features and benefits and providing examples of Cisco products that fall within this category
- Describe Cisco threat control and containment products and technologies, illustrating their high-level features and benefits
- Describe Cisco content security products and technologies, illustrating their high-level features and benefits
- Describe Cisco VPN solutions and technologies, illustrating their high-level features and benefits
- Describe security management products and technologies, illustrating their high-level features and benefit

Module 2: Protecting the Network Infrastructure

Lesson 1: Introducing Cisco Network Foundation Protection

- Categorize common threats against the network infrastructure
- Describe Cisco NFP as a framework to develop and implement security controls to protect the network infrastructure
- List and compare security controls that protect the control plane and data plane
- List and compare security controls that protect the management plane

Lesson 2: Protecting the Network Infrastructure Using Cisco Configuration Professional

- Articulate the features and benefits of Cisco Configuration Professional, describing its requirements and installation options
- Demonstrate the Cisco Configuration Professional GUI, showcasing relevant options and features
- Describe the unique components of Cisco Configuration Professional that are used for effective security policy deployment and configuration
- Describe and implement the One-Step Lockdown and audit features that are found on Cisco Configuration Professional

Lesson 3: Securing the Management Plane on Cisco IOS Devices

- Describe the management security features of the Cisco IOS Software on Cisco routers
- Demonstrate the configuration of management access using RBAC
- Describe the support for AAA services on Cisco routers
- Demonstrate the use of Cisco Configuration Professional to configure AAA services
- Compare and contrast different device monitoring options, including SNMP and syslog

Lesson 4: Configuring AAA on Cisco IOS Devices Using Cisco Secure ACS

- Describe the features of the Cisco Secure ACS in the context of a management protection strategy
- Compare and contrast two popular AAA protocols: TACACS and RADIUS
- Demonstrate the configuration of network elements to use AAA authentication and authorization
- Demonstrate the initialization and basic configuration of Cisco Secure ACS acting as a AAA server
- Utilize CLI commands to verify the correct configuration of the router

Lesson 5: Securing the Data Plane on Cisco Catalyst Switches

- Introduce fundamental switching concepts, starting with the building blocks of VLANs and trunking
- Introduce other building blocks of the switch, including spanning tree for high availability
- Revisit and explain security threats that exploit vulnerabilities in the switching infrastructure
- Plan and develop a strategy for protecting the switch data plane
- Describe the Spanning Tree Protocol Toolkit that is found on Cisco IOS routers that prevents STP operations from having an impact on the security posture
- Revisit port security and configure it to illustrate security controls that are aimed at mitigating ARP spoofing and other threats

Lesson 6: Securing the Data Plane in IPv6 Environments

- Explain the need for IPv6 from the general perspective of the transition to IPv6 from IPv4
- List and describe the fundamental features of IPv6, as well as enhancements when compared to IPv4
- Analyze the IPv6 addressing scheme, components, and design principles and configure IPv6 addressing
- Describe the IPv6 routing function
- Evaluate how common and specific threats affect IPv6
- Develop and implement a strategy for IPv6 security

Module 3: Threat Control and Containment

Lesson 1: Planning a Threat Control Strategy

- Evaluate the current state of enterprise security in the presence of evolving threats
- Describe design considerations for a threat protection strategy to mitigate threats as part of a risk management strategy
- Describe how Cisco strategizes threat control and containment

Lesson 2: Implementing Access Control Lists for Threat Mitigation

- List the benefits of ACLs in general
- Describe the building blocks and operational framework of ACLs
- Describe summarizable address blocks in the context of CIDR and VLSM environments, demonstrating how ACL wildcard masks allow for threat mitigation in those environments
- List design considerations when deploying ACLs in general
- Demonstrate the use of Cisco Configuration Professional and the CLI to deploy and verify a threat containment strategy using ACLs
- Demonstrate the use of Cisco Configuration Professional and the CLI to correlate ACL log and alarm information to monitor their impact and effectiveness
- Configure object groups to simplify the implementation of ACLs for threat control
- Configure ACLs in IPv6 environments, highlighting the operational differences with IPv4 ACLs

Lesson 3: Understanding Firewall Fundamentals

- Describe firewall technologies that historically have played, and still play, a role in network access control and security architectures
- Introduce and describe the function and building blocks of NAT
- List design considerations for firewall deployment
- Describe guidelines for firewall ruleset creation

Lesson 4: Implementing Cisco IOS Zone-Based Policy Firewalls

- Introduce and describe the function, operational framework, and building blocks of Cisco IOS zone-based firewalls
- Describe the functions of zones and zone pairs, as well as their relationship in hierarchical policies

- Describe the Cisco Common Classification Policy Language for creating zone-based firewall policies
- List the default policies for the different combinations of zone types
- Demonstrate the configuration and verification of zone-based firewalls using Cisco Configuration Professional and the CLI
- Demonstrate the configuration of NAT services for zone-based firewalls

Lesson 5: Configuring Basic Firewall Policies on Cisco ASA Appliances

- Describe the Cisco ASA family of products, identifying the primary supported features
- Describe the building blocks of Cisco ASA configuration
- Describe the navigation options, features, and requirements of Cisco ASDM
- Describe the use of ACLs on Cisco ASA appliances
- Briefly describe the deployment of policies using the Cisco Modular Policy Framework
- Describe the configuration procedure to deploy basic outbound access control on Cisco ASA appliances using Cisco ASDM

Lesson 6: Understanding IPS Fundamentals

- Discuss the fundamentals of intrusion prevention and compare IDS and IPS
- Describe the building blocks of IPS and introduce the underlying technologies and deployment options
- Describe the use of signatures in intrusion prevention and highlight their benefits and drawbacks
- Discuss the need for IPS alarm monitoring and evaluate the options for event managers
- Analyze the design considerations in deploying IPS

Lesson 7: Implementing Cisco IOS IPS

- Describe the operational framework and requirements of Cisco IOS IPS
- Describe signature files and signature definitions from the operational and maintenance perspectives
- Evaluate scenarios and analyze a strategy for signature tuning
- Describe the options for event management using Cisco IOS IPS
- List the steps to configure Cisco IOS IPS using Cisco Configuration Professional, and implement the configuration using Cisco Configuration Professional wizards
- Implement signature tuning with Cisco Configuration Professional options
- Use Cisco Configuration Professional as an event manager, and monitor IPS operations

Module 4: Secure Connectivity

Lesson 1: Understanding the Fundamentals of VPN Technologies

- Discuss the state of VPN security and the business and technical drivers behind it
- Describe the required components and deployment options for VPNs
- Introduce the use of encryption in VPN deployments
- Introduce symmetric encryption algorithms and describe their use in VPN operations
- Introduce asymmetric encryption algorithms and describe their use in VPN operations
- Introduce hashing mechanisms and describe their use in VPN operations

- Describe the use of cryptographic keys in VPN operations and list the considerations in key management
- Describe how cryptography plays a role in commercial implementations such as IPsec and SSL/TLS

Lesson 2: Introducing Public Key Infrastructure

- Describe the asymmetric cryptography fundamentals behind PKI
- Explain the reasoning and components behind digital signatures and the RSA protocol
- Describe PKI requirements, components, and operations
- List PKI standards and their functions
- Detail the operations of CAs and RAs

Lesson 3: Examining IPsec Fundamentals

- Analyze the architecture of the IPsec protocol
- Detail the role and operational impact of the main IPsec components
- Describe IPsec modes of operation in various scenarios
- Describe the phases of IPsec connectivity
- Overview the operations of IPv6 VPNs

Lesson 4: Implementing Site-to-Site VPNs on Cisco IOS Routers

- Evaluate the requirements and configuration of site-to-site IPsec VPNs
- Use Cisco Configuration Professional to configure site-to-site IPsec VPNs
- Use CLI commands and Cisco Configuration Professional monitoring options to validate the VPN configuration
- Use CLI commands and Cisco Configuration Professional monitoring options to monitor and troubleshoot the VPN configuration

Lesson 5: Implementing SSL VPNs Using Cisco ASA Appliances

- Describe the use cases and operational requirements of SSL VPNs
- Describe the protocol framework for SSL and TLS
- Describe a configuration that is based on deployment options and other design considerations
- Describe the steps to configure Cisco VPN clientless mode on the Cisco ASA appliance, and demonstrate the configuration on Cisco ASDM
- Describe the steps to configure Cisco full tunnel mode on the Cisco ASA appliance, and demonstrate the configuration on Cisco ASDM using the Cisco AnyConnect client