



Securing Networks with ASA Advanced

Length
5 days

Format
Lecture/lab

Version
1.0

Course Description

This course covers the advanced feature set for the ASA 5500 series appliances, including Policy NAT, Advanced Protocol Handling, Dynamic Routing and Switching (DRS), advanced IPsec and SSL VPN configuration, EasyVPN, QoS for VPNs, and the CSC-SSM and AIP-SSM security services modules.

Basic configuration of the ASA appliance is covered in the *Securing Networks with ASA Fundamentals (SNAF)* course.

Who Should Attend

This course is designed for anyone tasked with implementing or maintaining a secure network using Cisco ASA firewalls. Candidates seeking the Cisco CCSP security certification must also take this course.

Recommended Prerequisites

- CCNA certification or equivalent knowledge
- Basic knowledge of the Windows operating system
- Securing Cisco Network Devices (SND)

Related Courses

- Securing Cisco Network Devices (SND)
- Securing Networks with ASA Advanced (SNAA)

SNAA

Learning Objectives

After completing this course, you will be able to:

- Configure policy NAT based on traffic type
- Configure the Layer 7 Modular Policy Framework for advanced protocol handling
- Segment traffic with VLANs
- Configure dynamic routing
- Establish LAN-to-LAN tunnels with digital certificates
- Configure the IPsec VPN client
- Configure remote access using digital certificates
- Configure QoS for VPN traffic
- Configure WebVPN functionality
- Configure clientless SSL VPNs
- Configure the Cisco AnyConnect VPN Client
- Configure Cisco Secure Desktop and DAP for SSL VPN connections
- Inspect and filter traffic with the CSC-SSM service module
- Identify, alert, and defend against attacks with the AIP-SSM security module



Learning
Solutions



Securing Networks with ASA Advanced

Course Outline

Module 1: Advanced NAT

Lesson 1: Applying NAT 0 and Policy NAT

- ACLs
- NAT
- Translation Behavior
- NAT Exemption
- Policy NAT
- Verify and Troubleshoot

Lab: Implementing Advanced NAT

Module 2: Advanced Protocol Handling

Lesson 1: Applying the Cisco Modular Policy Framework

- Cisco Modular Policy Framework Overview
- Configuring the Cisco Modular Policy Framework
- Configuring a Layer 7 Class Map
- Configuring a Regular Expression Class Map
- Configuring a Layer 7 Policy Map
- Verifying the Cisco Modular Policy Framework Configuration

Lesson 2: Handling Advanced Protocols

- Protocol Inspection Overview
- FTP Inspection
- HTTP Inspection
- IM Inspection
- ESMTP Inspection
- DNS Inspection
- ICMP Inspection
- Protocol Inspection Verification

Lab: Configuring Advanced Protocol Inspection

Module 3: Dynamic Routing and Switching

Lesson 1: Switching with VLANs

- Cisco ASA VLAN Operations
- VLAN Configuration
- VLAN Configuration on the Cisco ASA 5505
- VLAN Verification

Lesson 2: Routing with Dynamic Protocols

- Dynamic and Static Routing
- RIP
- OSPF
- EIGRP
- Redistribution
- Verification and Troubleshooting

Lab: Dynamic Routing with EIGRP and OSPF

Module 4: IPsec VPNs

Lesson 1: Understanding IPsec and Digital Certificates

- IPsec Operation
- Digital Certificates and Public-Key Cryptography
- Certificates and Scalability
- Certificate Enrollment Process
- Validating the Certificate
- Certificate Revocation Lists
- Security Appliance Certificate Enrollment Support
- Key Pairs and Trustpoints

Lesson 2: Implementing Site-to-Site VPNs with Digital Certificates

- Site-to-Site VPNs
- Configuring CA Certificates
- Site-to-Site IPsec Connection Profiles
- Modifying Certificate to Connection Mapping
- Hub and Spoke
- Site-to-Site Redundancy
- Verifying Site-to-Site VPNs
- Troubleshooting Site-to-Site VPNs

Lab: Site-to-Site with Digital Certificates



Learning
Solutions



Securing Networks with ASA Advanced

Course Outline

Module 4 (continued)

Lesson 3: Configuring the Cisco VPN Client

- Cisco VPN Client
- Cisco VPN Client Installation
- Digital Certificates with Cisco VPN Client
- Connection Entry
- Advanced Options
- Verify and Troubleshoot Client Configuration

Lesson 4: Implementing Remote-Access VPNs with Digital Certificates

- Remote-Access VPNs
- Configuring a Cisco ASA for Remote Access
- Installing Cisco ASA Certificates
- Defining a Remote-Access Address Pool
- User Policy Attribute Inheritance
- Configuring an IPsec Connection Profile
- Configuring the Certificate to Connection Profile Policy
- Verifying Remote-Access VPNs
- Troubleshooting Remote-Access VPNs

Lab: Remote Access with Digital Certificates

Lesson 5: Configuring Advanced Remote-Access Features and Policy

- Load Balancing
- Reverse Route Injection
- Backup Servers
- Intra-Interface VPN Traffic
- NAT Transparency
- Client Update
- Split Tunneling
- Personal Firewalls

Lesson 6: Configuring the ASA 5505 as a Cisco Easy VPN Hardware Client

- Introduction to Cisco Easy VPN
- Cisco Easy VPN Server Policy
- Cisco Easy VPN Hardware Client

Lab: Cisco ASA 5505 Easy VPN Hardware Client

Lesson 7: Configuring QoS for IPsec VPNs

- QoS Overview
- Cisco ASA QoS
- Configuring QoS for VPNs
- Verifying QoS

Module 5: SSL VPNs

Lesson 1: Understanding SSL VPN Technology

- SSL Overview
- Clientless SSL VPN
- Cisco Secure Desktop

Lesson 2: Configuring Clientless SSL VPNs

- Configuring Clientless SSL VPN
- Verifying Clientless SSL VPN Operation
- Configuring Port-Forwarding SSL VPN
- Verifying Port-Forwarding SSL VPN
- Configuring Additional SSL VPN Features
- Troubleshooting Clientless and Port-Forwarding SSL VPNs

Lab: Clientless SSL VPNs

Lesson 3: Configuring Full Network Access SSL VPNs

- Cisco Full Network Access SSL VPN Overview
- Configuring Cisco AnyConnect SSL VPN
- Verifying VPN Operation
- Configuring Advanced Features
- Configuring Certificate-Based Authentication
- Troubleshooting VPN Client Operation

Lab: SSL VPNs with the Cisco AnyConnect Client

Lesson 4: Cisco Secure Desktop

- Cisco Secure Desktop Overview
- Cisco Secure Desktop Interoperability
- Preparing the Cisco ASA for Cisco Secure Desktop

Lesson 5: Securing the Desktop with Cisco

- Secure Desktop and DAP
- Cisco Secure Desktop Workflow
- Prelogin Assessment
- Secure Session
- Cache Cleaner
- Host Emulation and Keystroke Logger Detection
- Host Scan
- Dynamic Access Policy
- DAP Testing

Lab: Cisco Secure Desktop and Dynamic Access Policy



Learning
Solutions



Securing Networks with ASA Advanced

Course Outline

Module 6: Security Services Modules

Lesson 1: Examining the Cisco SSMs

- Business Challenges
- Cisco SSMs
- CSC-SSM
- AIP-SSM
- AIP-SSM or CSC-SSM

Lesson 2: CSC-SSM: Getting Started

- CSC-SSM Overview
- CSC-SSM Software Loading
- Initial CLI Cisco CSC Configuration
- Initially Configuring the CSC-SSM with the Cisco ASDM CSC Setup Wizard

Lesson 3: AIP-SSM: Getting Started

- AIP-SSM Overview
- AIP-SSM Software Loading
- Initial Cisco IPS ASDM Configuration
- Configure a Cisco IPS Security Policy

Lab: Initializing AIP-SSM



Learning
Solutions