Securing Networks with ASA Foundations

Price: $2,995

Price:	$2,995
Length:	35 Hours (5 days)

Introduction: *Securing Networks with ASA Fundamentals (SNAF)* is a five-day, instructor-led, lab-intensive course. This task-oriented course teaches the knowledge and skills needed to configure, maintain, and operate Cisco ASA 5500 Series Adaptive Security Appliances.

Prerequisites: Students taking this course should have the following skills:

- Skills & knowledge equivalent to Interconnecting Cisco Networking Devices Part 1 & Part 2
- Working knowledge of the Windows operating system
- Familiarity with networking and security terms and concepts

Course Materials: Students will be provided with the following software for use in the classroom:

- Certification lesson guides, workbooks

The above mentioned materials are yours to keep.

Objectives: After completing this course, students will be able to:

- Explain the functions of the three types of firewalls used to secure today's computer networks.
- Describe the technology and features of Cisco security appliances.
- Explain how each appliance protects network devices from attacks and why each is an appropriate choice for the example network.
- Bootstrap the security appliance, prepare the security appliance for configuration via the Cisco Adaptive Security Device Manager (ASDM), and launch and navigate ASDM.
- Use ASDM and the CLI to perform essential security appliance configuration.
- Use ASDM to configure dynamic and static address translations in the security appliance.
- Use ASDM to configure switching and routing on the security appliance.
- Use ASDM to configure access control lists, filter malicious active codes, and filter URLs to meet the requirements of the security policy.
- Use the packet tracer for troubleshooting.
- Use ASDM to configure object groups that meet the requirements of the security policy.
- Use ASDM to configure AAA as needed to meet the requirements of the security policy.
- Use ASDM to configure a modular policy that supports the security policy and to configure protocol inspection to meet the requirements of the security policy.
- Use ASDM and the CLI to configure threat detection to meet the requirements of the security policy.
- Use ASDM to configure the security appliance to support a site-to-site VPN that meets the requirements of the security policy.
- Use ASDM to configure the security appliance to provide secure connectivity using remote access VPNs.
- Configure the security appliance to run in transparent firewall mode as needed to meet the requirements of the security policy.
- Enable, configure, and manage multiple contexts as needed to meet the requirements of the security policy and monitor and manage an installed security appliance.
- Select and configure the type of failover that best suits the network topology.

Securing Networks with ASA Foundations

Price: $2,995

Course Outline

I. Introducing Cisco Security Appliance Technology and Features
- A. Firewalls
- B. Security Appliance Overview

II. Introducing the Cisco ASA and PIX Security Appliance Families
- A. Models and Features of Cisco Security Appliances
- B. ASA Licensing

III. Getting Started with Cisco Security Appliances
- A. User Interface
- B. File Management
- C. Security Appliance Security Levels ASDM Overview and Operating Requirements
- D. Preparing to Use ASDM
- E. Navigating ASDM Windows

III. PC Technician Professional Best Practices
- A. Tools of the trade
- B. Electrical safety
- C. Environmental safety and materials handling

IV. Configuring a Security Appliance
- A. Basic Security Appliance Configuration
- B. Examining Security Appliance Status
- C. Time Setting and NTP Support
- D. Syslog Configuration

V. Configuring Translations and Connection Limits
- A. Transport Protocols
- B. Network Address Translation
- C. Port Address Translation
- D. Static Translations
- E. SYN Cookies and Connection Limits
- F. Connections and Translations

VI. Using ACLs and Content Filtering
- A. ACLs
- B. Malicious Active Code Filtering
- C. URL Filtering
- D. Packet Tracer

VII. Configuring Object Grouping
- A. Overview of Object Grouping
- B. Configuring Object Groups and Using Them in ACLs

VIII. Switching and Routing on Cisco Security Appliances
- A. VLAN Capabilities
- B. Static Routing
- C. Dynamic Routing

IX. Configuring AAA for Cut-Through Proxy
- A. Introduction to AAA
- B. Configuring the Local User Database
- C. Installing Cisco Secure ACS for Windows
- D. Cut-Through Proxy Authentication Configuration
- E. Authentication Prompts and Timeouts
- F. Authorization Configuration
- G. Accounting Configuration

X. Configuring the Cisco Modular Policy Framework
- A. Modular Policy Framework Overview
- B. Class Map Overview
- C. Policy Map Overview
- D. Using ASDM to Configure a Modular Policy
- E. Configuring a Management Policy
- F. Displaying Modular Policy Framework Commands

XI. Configuring Advanced Protocol Handling
- A. Advanced Protocol Handling
- B. Protocol Application Inspection
- C. Multimedia Support

XII. Configuring Threat Detection
- A. Threat Detection Overview
- B. Basic Threat Detection
- C. Scanning Threat Detection
- D. Configuring and Viewing Threat Detection Statistics

XIII. Configuring Site-to-Site VPNs Using Pre-Shared Keys
- A. Secure VPNs
- B. How IPsec Works
- C. Prepare to Configure an IPsec VPN
- D. Configuring a Site-to-Site VPN Using Pre-shared Keys
- E. Modifying the Site-to-Site VPN Configuration
- F. Test and Verify VPN Configuration

Securing Networks with ASA Foundations

Price: $2,995

XIV. Configuring Security Appliance Remote-Access VPNs

A. Introduction to Cisco Easy VPN
B. Overview of Cisco VPN Client
C. Configuring Remote Access VPNs
D. Configuring Users and Groups

XV. Configuring the Cisco ASA Security Appliance for SSL VPN

A. SSL VPN Overview
B. Using the SSL VPN Wizard to Configure Clientless SSL VPN
C. Verifying Clientless SSL VPN Operations

XVI. Configuring Transparent Firewall Mode

A. Transparent Firewall Mode Overview
B. How Data Traverses a Security Appliance in Transparent Mode
C. Configuring Transparent Firewall Mode
D. Monitoring and Maintaining Transparent Firewall Mode

XVII. Configuring Security Contexts

A. Security Context Overview
B. Enabling Multiple Context Mode
C. Configuring Security Contexts
D. Managing Security Contexts

XVIII. Configuring Failover

A. Understanding Failover
B. Configuring Redundant Interfaces
C. LAN-Based Active/Standby Failover Configuration
D. Active/Active Failover Configuration
E. Remote Command Execution

XIX. Managing the Security Appliance

A. Managing System Access
B. Configuring Command Authorization
C. Managing Configurations
D. Managing Images and Activation Keys