

Securing Networks with PIX and ASA (SNPA)

(5 day Instructor-Led Course)

Course Overview

The SNPA course is a five-day, leader-led, lab-intensive course. The course takes a task-oriented approach to teaching the skills to configure, operate, and manage Cisco PIX 500 Series Security Appliances and Cisco ASA 5500 Series Adaptive Security Appliances.

Who Should Attend

- Network engineers who implement and maintain Cisco firewalls
- Channel Partners who sell, implement and maintain Cisco Firewalls
- Resellers who sell, implement and maintain Cisco Firewalls

Prerequisites

Students who attend this advanced course must have experience in configuring Cisco IOS software and have met the following prerequisites:

- Certification as a CCNA or the equivalent knowledge
- Basic knowledge of the Windows operating system
- Familiarity with the networking and security terms and concepts (the concepts are learned in prerequisite training or by reading industry publications)

What You Will Accomplish

After completing the course, the student should be able to:

- Discuss Security Appliance interface security levels
- Configure a Security Appliance for basic network connectivity
- Configure the Security Appliance to send syslog messages to a syslog server
- Describe how the TCP and UDP protocols function with the Security Appliance
- Describe how static and dynamic translations function
- Explain the Security Appliance Port Address Translation (PAT) feature
- Configure and explain the function of ACLs and NAT 0 ACLs
- Configure active code filtering (ActiveX and Java applets)
- Configure the Security Appliance for URL filtering
- Describe the object grouping feature of the Security Appliance and its advantages
- AAA protocols supported by the Security Appliance
- Configure AAA authentication for Security Appliance access
- Define and configure cut-through proxy authentication and tunnel access authentication
- Define and configure AAA accounting
- Install and configure basic Cisco Secure ACS functions
- Describe how the Security Appliance implements FTP and HTTP protocol inspection
- Describe how the Security Appliance implements remote shell (rsh), SQL, SMTP, ICMP, and SNMP protocol inspection
- Identify the tasks and commands to configure Security Appliance IPsec support
- Describe and configure the Easy VPN Server for remote access VPN using the Cisco VPN Client
- Configure WebVPN general parameters, servers, URLs, and port forwarding
- Monitor and maintain transparent firewall mode
- Configure and manage a security context
- Define the Security Appliance hardware failover requirements
- Configure Active/Standby Failover

- Configure Active/Active Failover
- Install ASDM and use it to configure the Security Appliance
- Configure the AIP-SSM setup parameters
- Configure a security policy on an ASA Security Appliance using ASDM
- Configure Telnet and SSH access to the Security Appliance console
- Recover the Security Appliance passwords using general password recovery procedures
- Use TFTP to install and upgrade the software image on the Security Appliance

Certification Preparation

This course helps prepare students for the CCSP® - Cisco Firewall Specialist certification (exam 642-522).

Follow-up Courses

- Cisco Secure Intrusion Detection System (CSIDS)*
- Cisco Secure Virtual Private Networks (CSVPN)**

* Productivity Point delivers Cisco Authorized Training, Sponsored by Element K, A Cisco Learning Solutions Partner.

Course Outline: SNPA

1. Cisco Security Appliance Technology and Features

Introduction to the general functionality provided by firewalls and Security Appliances.

- Firewall Technologies
- Security Appliance Features Overview

2. Cisco PIX Security Appliance and ASA Adaptive Security Appliance Families

Introduction to the Cisco PIX 500 Series Security Appliance family, Cisco ASA 5500 Series Adaptive Security Appliance family, and Firewall Services Module (FWSM).

- Models and Features of Cisco Security Appliances
- PIX Security Appliance Licensing
- ASA Adaptive Security Appliance Licensing
- Cisco Firewall Services Module

3. Getting Started with Cisco Security Appliances

Learn to configure a Security Appliance.

- User Interface
- File Management
- Security Appliance Security Levels
- Basic Security Appliance Configuration
- Examining Security Appliance Status
- Time Setting and NTP Support
- Syslog Configuration

4. Translations and Connections

Discussion of Security Appliance translations and connections, how the Security Appliance processes TCP and User Datagram Protocol (UDP) traffic, and how to configure dynamic and static address translations in a Security Appliance.

- Transport Protocols
- Network Address Translation
- Port Address Translation
- Identity NAT (NAT 0)
- Static Command
- Port Redirection with the Static Command
- TCP Intercept and Connection Limits
- Connections and Translations
- Configuring Multiple Interfaces

5. Access Control Lists and Content Filtering

Discuss how to control access through the Security Appliance using access control lists (ACLs). Learn how to configure the Security Appliance to filter

malicious active code and how to configure URL filtering.

- ACLs
- Time-Based ACLs
- Editing Existing ACLs
- The ICMP Command
- Other ACL Uses

- Malicious Active Code Filtering
- URL Filtering

6. Object Grouping

Learn object grouping concepts and how to use the object-group command to configure object grouping. The various types of object groups are explained, and the use and configuration of nested object groups are covered.

- Configuring Object Groups
- Nested Object Groups
- Applying Object Groups to ACLs

7. Authentication, Authorization, and Accounting

Learn Security Appliance authentication, authorization, and accounting (AAA) and how to configure AAA.

- Introduction to AAA
- Installation of Cisco Secure ACS for Windows 2000
- Security Appliance Access Authentication Configuration
- Using the Local User Database
- Changing Authentication Timeouts
- Security Appliance Cut-Through Authentication Configuration
- Virtual Telnet and Virtual HTTP
- Tunnel Access Authentication Configuration
- Authorization Configuration
- Downloadable ACLs
- Per-User Override
- Accounting Configuration

8. Switching and Routing

Explanation of the virtual local area network (VLAN) capabilities of the Security Appliance and the routing capabilities of the Security Appliance. Discussion of Routing Information Protocol (RIP) and the Open Shortest Path First (OSPF) algorithm in detail and configuration of the Security Appliance to allow multicast traffic.

- VLANs

- AUTHORISED CENTRE** ■ Static and Dynamic Routing
- OSPF
 - Multicasting

9. Modular Policy Framework

Introduction of modular policy framework and explanation of how to configure a modular policy.

- Modular Policy Overview
- Configuring a Class Map
- Configuring a Policy Map
- Configuring a Service Policy

10. Advanced Protocol Handling

Introduction to Security Appliance advanced protocol handling. Describe how to configure protocol inspection to include configuring an inspection modular policy, defining an FTP map, defining an HTTP map, and describing a number of the inspection protocols supported by the Security Appliance.

- Advanced Protocol Handling
- FTP, HTTP, and Protocol Application Inspection
- Configuring Deep Packet Inspection
- Multimedia Support

11. VPN Configuration

Learn the basics of IPSec and Security Appliance virtual private networks (VPNs), with a focus on communications between Security Appliance gateways for site-to-site secure connectivity. Discuss how VPNs function and the tasks necessary to configure VPN connection parameters on the Security Appliance.

- Secure VPNs
- How IPSec Works
- Configure VPN Connection Parameters
- Configuring IKE Parameters
- Configuring Tunnel Groups
- Configuring IPSec Parameters
- Scale Security Appliance VPNs with Digital Certificates

12. Configuring Security Appliance Remote Access Using Cisco Easy VPN

Discuss the Cisco Easy VPN and its two components and modes of operation.

- Introduction to Cisco Easy VPN
- How Cisco Easy VPN Works
- Configuring Users and Groups
- Configuring IKE Mode Config Parameters
- Configuring Dynamic Crypto Maps

- Configuring the Easy VPN Server for Extended Authentication
- Configure Security Appliance Hub-and-Spoke VPNs
- Cisco VPN Client Manual Configuration Tasks
- Working with the Cisco VPN Client

13. Configuring ASA for WebVPN

Define the characteristics of WebVPN and how it compares with traditional VPNs. Discuss the end-user interface and the steps and commands necessary to configure the ASA for WebVPN. As this is a feature unique to the ASA 5500 Series, it is not covered in a hands-on lab.

- WebVPN End-User Interface
- Configure WebVPN General Parameters, Servers, URLs, and Port Forwarding
- Define Email Proxy Servers
- Configure WebVPN Content Filters and ACLs

15. Configuring Security Contexts

Learn the purpose of security contexts and how to enable, configure, and manage multiple contexts.

- Security Context Overview
- Enabling Multiple Context Mode
- Configuring a Security Context
- Managing Security Contexts

16. Failover

Introduction to the Security Appliance failover options and how to configure them. Describe the types of failover supported by the Security Appliance and discusses how to configure active/standby, active/active, and stateful failover.

- Understanding Failover
- Serial Cable-Based Failover Configuration
- Active/Standby LAN-Based Failover Configuration
- Active/Active Failover Configuration

17. Cisco Security Appliance Device Manager

Introduction to the Cisco Adaptive Security Device Manager (ASDM). Learn an overview of ASDM and its operating requirements. Continue with an introduction to the GUI structure and how to

AUTHORISED CENTRE maneuver through the device manager. Learn how to install ASDM and how to configure and monitor a Security Appliance with ASDM.

- ASDM Overview and Operating Requirements
- Navigating ASDM Configuration and Multimode Windows

18. AIP-SSM - Getting Started

Introduction to the Cisco Advanced Inspection and Prevention Security Services Module (AIP-SSM). Learn how to load intrusion prevention system (IPS) software on the AIP-SSM, initialize the AIP-SSM with the setup command, and define an IPS modular policy on a Security Appliance via ASDM. As this is a feature unique to the ASA 5500 Series, it is not covered in a hands-on lab.

- AIP-SSM SW Loading
- Initial IPS ASDM Configuration
- Configure a Security Policy on the ASA Security Appliance

19. Managing Security Appliances

Explain how to secure system access to the Security Appliance and how to configure and use local user authentication and command authorization. Password recovery and file management are also covered.

- Managing System Access
- Managing User Access Levels
- Command Authorization
- Managing Software, Licenses, and Configurations
- Image Upgrade and Activation Keys

21. Configuring PIX Security Appliance Remote Access Using Cisco Easy VPN

22. Firewall Services Module