



Securing Networks with PIX and ASA (SNPA) v 5.0 (Previously CSPFA)

Associated Certifications: CCSP

Exam: 642-522 SNPA

Duration: 5 days, Classroom

Dates: 24th Sept 2007, 29th Oct 2007, 3rd Dec 2007

Cost: £1,795

Who should Attend

Cisco Customers, Channel Partners and System Engineers who sell, implement and maintain Cisco PIX and ASA security appliances.

Pre Requisites

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

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

Course Content

Securing Networks with PIX and ASA (SNPA) v5.0 is an update to SNPA v4.0, an existing five-day instructor-led course. SNPA 5.0 uses Cisco ASA and PIX Security Appliance software version 7.2 to protect network systems from intrusions and security threats. The SNPA 5.0 course introduces the new ASA 5505 and 5550 and covers important new ASA and PIX Security Appliance 7.2 features, which includes new and enhanced inspection engines for application layer protocol inspection; packet tracer; CSC-SSM; resource management for security contexts; enhanced VPN services such as SSL VPN Client and Citrix support for WebVPN. The SNPA 5.0 course takes a task-oriented approach to teaching the skills to deploy, configure, and administer the Cisco ASA and PIX Security Appliances.





Course Objectives

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

- Describe security appliance features, models, components and benefits
- Discuss Adaptive Security
- Configure the PIX Firewall to statically and dynamically translate IP addresses
- Configure the PIX Firewall to control inbound and outbound traffic
- Configure object groups to simplify ACL configuration
- Configure the PIX Firewall to send messages to a Syslog sever
- Explain the routing functionality of the PIX Firewall
- Configure content filtering on the PIX Firewall
- Configure the PIX Firewall as a DHCP client
- Configure special protocol handling on the PIX Firewall
- Configure AAA on the PIX Firewall
- Configure failover on the PIX Firewall
- Configure the PIX Firewall's IDS feature set
- Configure a site-to-site VPN using the PIX Firewall
- Configure a VPN Client-to-PIX Firewall VPN
- Perform password recovery on the PIX Firewall
- Upgrade PIX Firewall software images
- Perform a PIX Firewall activation key upgrade
- Configure command authorisation
- Configure the PIX Firewall to send traps to a SNMP Network Management Station
- Configure the PIX Firewall to permit SNMP traffic
- Configure a secure connection to the PIX Firewall using SSH
- Install the PIX Device Manager and use it to configure the PIX Firewall
- Use the PIX Device Manager to monitor the PIX Firewall
- Install the PIX Management Centre and use it to configure the PIX Firewall
- Install the Auto Update Server and use it to update the PIX Firewall and configuration
- Explain the similarities and differences between the PIX Firewall and the Catalyst 6500 Firewall Services Module
- Perform basic Firewall Services Module configuration

Course Outline

Reviewing Cisco Firewall Technology Features

- Firewalls
- Security Appliance Overview

Cisco PIX and ASA Security Appliance Families

- Cisco Pix Security Appliance Family
- PIX Security Appliance Licensing
- ASA 5500 Adaptive Security Appliance Licensing
- Cisco Catalyst 6500/7600 Firewall Services Module





Getting Started with Cisco Security Appliance

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

Translations and Connections

- Transport Protocols
- Network Address Translation
- Port Address Translation
- Static Command
- TCP Intercept and Connection Limits
- Connections and Translations
- Configuring Multiple Interfaces

Access Control Lists and Content Filtering

- ACLs
- Malicious Active Code Filtering
- URL Filtering

Object Grouping

- Overview of Object Grouping
- Getting Started with Object Groups
- Configure Object Groups
- Configure Nested Object Groups

Authentication, Authorization, and Accounting

- Installation of Cisco Secure ACS for Windows 2000
- Security Appliance Access Authentication Configuration
- Cut-through Proxy Authentication Configuration
- Tunnel Access Authentication Configuration
- Authorization Configuration
- Downloadable ACLs
- Accounting Configuration





Switching and Routing

- Virtual LANS
- Static and Dynamic Routing
- OSPF
- Multicast

Modular Policy Framework

- Modular Policy Overview
- Class-Map
- Policy Map
- Service Policy

Advanced Protocol Handling

- Advanced Protocol Handling
- FTP Application Inspection
- HTTP Application Inspection
- Protocol Application Inspection
- Multimedia Support

Virtual Private Network Configuration

- Enabling a secure VPN
- How IPSec Works
- Configure VPN Connection Parameters
- IPSec Configuration Tasks
- Scale Security Appliance VPNs

Configuring Security Appliance Remote Access Using Cisco Easy VPN

- Introduction to the Cisco Easy VPN
- Overview of the Cisco VPN Client
- How the Cisco easy VPN Works
- Configuring Users and Groups
- 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





Configuring ASA for WebVPN

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

Configuring Transparent Firewall

- Transparent Firewall Mode Overview
- Enabling Transparent Firewall Mode
- Monitoring and Maintaining Transparent Firewall.

Configuring Security Contexts

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

Failover

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

Cisco Security Appliance Device Manager

- Describe ASDM and its Capabilities
- Explain ASDM hardware and software requirements
- Prepare the Security Appliance to use ASDM
- Navigate ASDM configuration windows.
- Navigate ASDM monitor windows
- Navigate ASDM multimode windows.





AIP- Security Services Module – Getting Started

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

Managing Security Appliance

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

