

# Cisco Networks Securing Networks with PIX and ASA (SNPA)

Course:ET933

## Course Description

This course (SNPA) teaches the knowledge and skills needed to configure, maintain, and operate Cisco® PIX® 500 Series security appliances and Cisco ASA 5500 Series adaptive security appliances. SNPA is recommended training for the Cisco Certified Security Professional (CCSP™) certification

## Who should attend?

Cisco customers who implement and maintain Cisco PIX security appliances and ASA security appliances; Cisco channel partners who sell, implement, and maintain Cisco PIX security appliances and ASA security appliances; and Cisco Systems engineers who support the sale of Cisco PIX security appliances and ASA security appliances

## Pre-requisites

- Cisco Certified Network Associate (CCNA) certification
- Working knowledge of the Windows operating system
- Working knowledge of Cisco IOS networking and concepts

## Course Objectives

- Describe the security appliance features, models, components, and benefits
- Discuss Adaptive Security Algorithm (ASA) and ASA security levels
- Configure a security appliance for basic network connectivity and syslog
- Describe how TCP and User Datagram Protocol (UDP) function within the security appliance
- Describe how static and dynamic translations function and Port Address Translation (PAT) feature
- Configure and explain the function of access control lists (ACLs) and Network Address Translation (NAT) ACLs
- Configure active code filtering (ActiveX and Java applets)
- Configure the security appliance for URL filtering
- Define and configure cut-through proxy authentication and tunnel access authentication
- Define and configure AAA accounting
- Describe and configure VPN server and remote using the Cisco VPN client
- Monitor and maintain transparent firewall mode
- Define the security appliance hardware failover requirements
- Install Adaptive Security Device Manager (ASDM) and use it to configure the security appliance
- Configure a security policy on an ASA security appliance using ASDM
- Configure Telnet and SSH access to the security appliance console

## Course Outline

1. Cisco Security Appliance Technology and Features
  - Firewall Technologies
  - Security Appliance Features Overview
2. Cisco PIX and ASA
  - Models of Cisco Security Appliances
  - PIX Security Appliance Licensing
  - ASA Adaptive Security Appliance Licensing
3. Overview Cisco Security Appliances
  - File Management
  - Basic Security Appliance Configuration
  - Time Setting and NTP Support
  - Syslog Configuration
4. Translations and Connections
  - Network Address Translation
  - Port Address Translation
  - Port Redirection with the Static Command
5. ACLs and Content Filtering
  - Time-Based ACLs
  - Editing Existing ACLs
  - URL Filtering
6. Object Grouping
  - Configuring Object Groups
  - Nested Object Groups
  - Applying Object Groups to ACLs
7. AAA
  - Introduction to AAA
  - Installation of Cisco Secure ACS for Windows
  - Using the Local User Database
  - Cut-Through Authentication Configuration
  - Virtual Telnet and Virtual HTTP
8. Switching and Routing
  - VLANs
  - Static and Dynamic Routing
  - OSPF
  - Multicasting
9. Modular Policy Framework
  - Modular Policy Overview
  - Configuring a Class Map
  - Configuring a Policy Map
  - Configuring a Service Policy
10. Advanced Protocol Handling
  - Advanced Protocol Handling
  - FTP, HTTP, and Protocol Application
  - Multimedia Support
11. VPN Configuration
  - Secure VPNs
  - Scale Security Appliance VPNs with Digital Certificates
12. Configuring Security Appliance Remote
  - Configuring Users and Groups
  - Configuring IKE Mode Config Parameters
  - Configuring Dynamic Crypto Maps
  - Hub-and-Spoke VPNs
  - Working with the Cisco VPN Client
13. Configuring ASA for WebVPN
  - WebVPN End-User Interface
  - Configure WebVPN General Parameters, Servers, URLs, and Port Forwarding
  - Configure WebVPN Content Filters and ACLs
14. Configuring Transparent Firewall
  - Transparent Firewall Mode Overview
  - Enabling Transparent Firewall Mode
  - ARP Inspection
  - Firewall Mode
15. Configuring Security Contexts
  - Enabling Multiple Context Mode
  - Configuring a Security Context
  - Managing Security Contexts
16. Failover
  - Serial Cable-Based Failover Configuration
  - Active/Standby LAN-Based Failover
  - Active/Active Failover Configuration
17. Cisco Security Appliance Device Manager ASDM Overview
  - Navigating ASDM Configuration and Multi-mode Windows
18. AIP-SSM - Getting Started
  - AIP-SSM Software Loading
  - Initial IPS ASDM Configuration
  - Configure a Security Policy on the ASA Security Appliance
19. Managing Security Appliances
  - Managing System Access
  - Managing User Access Levels
  - Command Authorization
  - Image Upgrade and Activation Keys

## Labs

- Lab 1: Basic Security Appliance Configuration
- Lab 2: Syslog and NTP
- Lab 3: Translations and Connections
- Lab 4: Access Control Lists (ACLs) and ICMP Filters
- Lab 5: Object Groups
- Lab 6: AAA Authentication and Accounting
- Lab 7: AAA Authorization Using Downloadable ACLs
- Lab 8: Configure Modular Policy Framework
- Lab 9: Advanced Protocol Inspection
- Lab 10: Site-to-Site VPN with Pre-Shared Keys
- Lab 11: Site-to-Site VPN with Digital Certificates
- Lab 12: Remote Access VPN
- Lab 13: Transparent Firewall
- Lab 14: Secure Shell
- Lab 15: Command Authorization
- Lab 16: System Maintenance
- Lab 17: Active/Standby LAN-Based Failover
- Lab 18: Multiple Contexts
- Lab 19: Active/Active LAN-Based Failover

Register Now 02-260-3233  
<http://www.ctt-center.com>

Certifeid Technical Training Center Co.,Ltd

