

## Securing Networks with PIX and ASA

**Duration: 5 Days**    **Course Code: SNPA**

### Overview:

This five day instructor led course covers the new ASA and Pix Security Appliance 7.2 features and incorporates content for the new ASA 5505 and 5550 appliances. This task-orientated course teaches the knowledge and skill needed to describe, configure, verify and manage the PIX and ASA security Appliances.

### Target Audience:

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

### Objectives:

- Describe the general functionality of firewalls and security appliances
- Choose the most appropriate security appliance and licensing for a given scenario
- Configure the security appliance for basic network connectivity
- Perform address translation on a security appliance
- Configure security appliance access control
- Describe and configure the object grouping feature of Cisco security appliances
- Define, configure, and monitor AAA in Cisco security appliances
- Describe and configure the switching and routing functionality that your security appliance provides Describe and configure a security appliance modular policy
- Describe and configure security appliance advanced protocol handling
- Configure Cisco security appliances for VPN connectivity
- Configure security appliances for secure remote access
- Configure the Cisco security appliances to support the WebVPN feature set
- Configure Cisco security appliances to run in transparent firewall mode
- Configure the security appliance to support multiple contexts
- Implement and configure failover in a network
- Configure and monitor security appliances with ASDM
- Initialize a Cisco ASA AIP SSM and CSC SSM
- Secure and upgrade system access to the security appliance and recover from problems

### Prerequisites:

Delegates are required to meet the following prerequisites:

- CCNA certification or the equivalent knowledge
- Basic knowledge of the Windows operating system.
- Familiarity with networking and security terms and concepts.

### Testing and Certification:

Recommended as preparation for exam(s):

- 642-523 SNPA
- This course is part of the Cisco Certified Security Professional Certification and the Cisco Firewall Specialisation.

## Follow-on-Courses:

The following courses are recommended for further study:

- IPS – Implementing Cisco Intrusion Prevention Systems
  - CSVN - Cisco Secure VPN
  - SNRS – Securing Networks with Cisco Routers & Switches.
  - SND – Securing Cisco Network Devices
-

## Content:

### Cisco Security Appliance Technology and Features

- Firewalls
- Security Appliance Overview

### Cisco PIX and ASA Security Appliance Families

- Models and Features of Cisco Security Appliance
- PIX Security Appliance Licensing
- Cisco ASA Security Appliance Licensing

### Getting Started with Cisco 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

### Configuring Translations and Connection Limits

- Transport Protocols
- Network Address Translation
- Port Address Translation
- static Command
- Translation Behavior
- Connections and Translations

### Configuring Cisco ASA Security Appliances for WebVPN

- WebVPN Feature Overview
- WebVPN End-User Interface
- Configure WebVPN General Parameters
- Configure WebVPN Policies
- Configure WebVPN Tunnel Groups
- Configure WebVPN Servers and URLs
- Configure WebVPN E-Mail Proxy Servers
- Configure WebVPN Content Filters and ACLs

### Configuring Transparent Firewall Mode

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

### Configuring Security Contexts

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

### Configuring Failover

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

### Active/Active Failover Configuration

### Using ACLs and Content Filtering

- ACLs
- Malicious Active Code Filtering
- URL Filtering
- Packet Tracer

### Configuring Object Grouping

- Overview of Object Grouping
- Configuring and Using Object Groups

### Configuring Authentication, Authorisation, and Accounting

- Introduction to AAA
- Installation of Cisco Secure ACS for Windows 2000
- Authentication Configuration
- Cut-Through Proxy Authentication Configuration
- Tunnel Access Authentication Configuration
- Authorization Configuration
- Accounting Configuration

### Switching and Routing on Cisco Security Appliances

- VLAN Capabilities
- Static and Dynamic Routing
- Multicasting

### Configuring the Cisco Modular Policy Framework

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

### Cisco ASDM

- ASDM Overview and Operating Requirements
- Preparing for ASDM
- Navigating ASDM Configuration Windows

### Navigating ASDM Multimode Windows

### Introducing Cisco ASA SSMs

- Cisco ASA SSM Overview
- Cisco ASA AIP SSM Overview
- Cisco ASA AIP SSM Software Loading
- Cisco ASA CSC SSM Overview
- Configure a Security Policy on the Cisco ASA Security Appliance

### Managing Security Appliance

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

### Configuring Advanced Protocol Handling

- Advanced Protocol Handling
- Inspection Class Maps and Inspection Policy Maps
- Regular Expressions
- FTP Inspection
- HTTP Inspection
- Instant Messaging Inspection
- ESMTTP Inspection
- DNS Inspection
- Protocol Application Inspection
- Multimedia Support

### Configuring VPNs

- Secure VPNs
- How IPsec Works
- IPsec Configuration Tasks
- Task 1: Prepare to Configure VPN Support
- Task 2: Configure IKE Parameters
- Task 3: Configure IPsec Parameters
- Task 4: Test and Verify VPN Configuration

### Configuring Security Appliance Remote Access Using Cisco Easy VPN

- Introduction to Cisco Easy VPN
- The Cisco Easy VPN Connection Process
- Overview of Cisco Easy VPN Client
- Configuring Cisco VPN Client as Cisco Easy VPN Remote
- Working with the Cisco VPN Client
- Configuring Users and Groups
- Configuring the Cisco Easy VPN Server for Extended Authentication

---

## Further Information:

For More information, or to book your course, please call us on +966 1 488 8484

[info@globalknowledge.com.sa](mailto:info@globalknowledge.com.sa)

[www.globalknowledge.com.sa](http://www.globalknowledge.com.sa)

Global Knowledge, Diplomatic Quarter, Al Fazzari Complex, Riyadh 11494, Kingdom Saudi Arabia