

## Securing Networks with ASA Fundamentals

Duration: 5 Days Course Code: snaf

### Overview:

In this course delegates will gain the knowledge and skills needed to configure, maintain, and operate Cisco ASA 5500 Series Adaptive Security. We have enhanced our delivery of SNAF by adding depth to the existing Cisco-developed hands-on labs. In a topology designed to simulate a typical production network, our advanced hands-on labs guide you through exercises such as executing general maintenance commands, configuring ACLs, and configuring VPN on the Security Appliance.

### Target Audience:

This course may be of interest to the following people: Cisco customers who implement and maintain ASA and PIX Security Appliances Cisco channel partners who sell, implement, and maintain ASA and PIX Security Appliances Cisco systems engineers who support the sale of ASA and PIX Security Appliances

### Objectives:

- At the end of this course delegates the following;
- Functions of the three types of firewalls used to secure today's computer networks
- Technology and features of Cisco security appliances
- How Cisco Adaptive Security Appliances (ASAs) and Cisco PIX Security Appliances protect network devices from attacks and why each is an appropriate choice
- Bootstrap the security appliance, prepare the security appliance for configuration via the Cisco Adaptive Security
- Device Manager (ASDM), and launch and navigate ASDM
- Perform essential security appliance configuration using ASDM and the CLI
- Configure dynamic and static address translations using ASDM
- Configure switching and routing using ASDM
- Use ASDM to configure ACLs, filter malicious active codes, and filter URLs that 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 to meet the requirements of the security policy
- Configure a modular policy that supports the security policy using ASDM
- Use ASDM to configure protocol inspection to meet security policy requirements
- Configure threat detection to meet security policy requirements using ASDM and the CLI
- Using ASDM, configure the security appliance to support a site-to-site VPN that meets policy requirements
- Using ASDM, configure the security appliance to provide secure connectivity using remote access VPNs
- Configure the security appliance to run in transparent firewall mode
- Enable, configure, and manage multiple contexts to meet security policy requirements
- Select and configure the type of failover that best suits the network topology
- Monitor and manage an installed security appliance

### Prerequisites:

Delegates who are looking to attend this course must have the following pre-requisites;

- ICND2 - Interconnecting Cisco Network Devices 2
- IINS - Implementing Cisco IOS Network Security



## Content:

### Introducing Cisco Security Appliance Technology and Features

- Functions of the three types of firewalls that are used to secure modern computer networks
- Technology and features of Cisco security appliances

### Cisco Adaptive Security Appliance and PIX Security Appliance Families

- Cisco ASA security appliance models
- Cisco ASA security appliance licensing options

### Getting Started with Cisco Security Appliances

- Four main access modes
- Security appliance file management system
- Security appliance security levels
- ASDM requirements and capabilities
- Use the CLI to configure and verify basic network settings, and prepare the security appliance for configuration via ASDM
- ASDM
- Verify security appliance configuration and licensing via ASDM

### Essential Security Appliance Configuration

- Configure a security appliance for basic network connectivity
- Verify the initial configuration
- Set the clock and synchronize the time on security appliances
- Configure the security appliance to send syslog messages to a syslog server

### Configuring Translations and Connection Limits

- Function of TCP and UDP protocols within the security appliance
- Function of static and dynamic translations
- Configure dynamic address translation
- Configure static address translation
- Set connection limits

### Using ACLs and Content Filtering

- Configure the basic function of ACLs
- Configure additional functions of ACLs
- Configure active code filtering (ActiveX and Java applets)
- Configure the security appliance for URL filtering
- Use the packet tracer for troubleshooting

### Configuring Object Grouping

- Object grouping feature of the security appliance and its advantages

### Switching and Routing on Security Appliances

- Configure logical interfaces and VLANs
- Configure static routes and static route tracking
- Dynamic routing capabilities of Cisco security appliances
- Configure passive RIP routing

### Configuring AAA for Cut-Through Proxy

- Define and compare AAA
- Install and configure Cisco Secure ACS
- Configure the local user database
- Define and configure cut-through proxy authentication
- Define and configure user authorization using downloadable ACLs
- Define and configure accounting

### Configuring the Cisco Modular Policy Framework

- Cisco Modular Policy Framework feature for security appliances
- Functionality of class maps
- Functionality of policy maps
- Functionality of service policies
- Use ASDM to configure a service policy rule

### Configuring Advanced Protocol Handling

- Need for advanced protocol handling
- How the security appliance implements inspection of common network applications
- Issues with multimedia applications and how the security appliance supports multimedia call control and audio sessions

### Configuring Threat Detection

- Threat detection and statistics
- Configure basic threat detection and scanning threat detection
- Configure and view threat detection statistics

### Configuring Site-to-Site VPNs Using Pre-Shared Keys

- How security appliances enable a secure VPN
- Perform the tasks necessary to configure security appliance IPsec support
- Commands to configure security appliance IPsec support
- Configure a VPN between security appliances

### Configuring Security Appliance Remote

### Configuring Cisco Security Appliances for SSL VPN

- SSL VPN and its purpose
- Use the SSL VPN Wizard to configure a basic clientless SSL VPN connection
- Configure SSL VPN policies
- Verify SSL VPN operations
- Customize the clientless SSL VPN portals

### Configuring Transparent Firewall Mode

- Purpose of transparent firewall mode
- How data traverses a security appliance in transparent mode
- Enable transparent firewall mode
- Monitor and maintain transparent firewall mode

### Configuring Security Contexts

- Purpose of security contexts
- Enable and disable multiple context mode
- Configure a security context
- Manage a security context

### Configuring Failover

- Difference between hardware and stateful failover
- Difference between active/standby and active/active failover
- Security appliance failover hardware requirements
- Configure redundant interfaces
- How active/standby failover works
- Security appliance roles of primary, secondary, active, and standby
- How active/active failover works
- Configure active/standby cable-based and LAN-based failover
- Configure active/active failover
- Use remote command execution

### Managing Security Appliances

- Configure Telnet access to the security appliance
- Configure SSH access to the security appliance
- Configure command authorization
- Recover security appliance passwords using general password recovery procedures
- Use TFTP to install and upgrade the software image on the security appliance

- Configure object groups and use them in ACLs

#### **Access VPNs**

- Cisco Easy VPN
- Cisco VPN Client
- Configure an IPSec Remote Access VPN
- Configure Users and Groups

---

#### **Further Information:**

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 01924 377489

[info@globalknowledge.co.uk](mailto:info@globalknowledge.co.uk)

[www.globalknowledge.co.uk](http://www.globalknowledge.co.uk)

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK