Securing Networks with ASA Fundamentals

Duration: 5 Days Course Code: SNAF

Overview:

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

Prerequisites:

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

- 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
- 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
- Configure object groups and use them in ACLs

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

Further Information:

For More information, or to book your course, please call us on 353-1-814 8200

info@globalknowledge.ie

www.globalknowledge.ie

Global Knowledge, 3rd Floor Jervis House, Millennium Walkway, Dublin 1