Global Knowledge™

ASAE v2.0 - ASA Essentials v2.0

Duration: 5 Days   Course Code: GK5807

Overview:

Gain the essential skills required to configure, maintain, and operate Cisco ASA 5500 Series Adaptive Security Appliances.
During this 5-day virtual course you will have 24-hour access to labs to practice course objectives. You'll receive ten extra ASAE e-lab credits (good for 30 days) to review a topic after class, refine your skills, or get in extra practice-whatever lab activities complete your training.
Audio for this virtual course will be delivered by toll-free integrated telephone conference bridge, rather than VoIP through your computer. To prepare for your class, the following hardware options are recommended:
Wired speakerphone
Wired telephone with headset or handset
Wireless phone/speakerphone handset with headset adapter
Wireless speakerphone

Target Audience:

Network administrators, managers, and coordinators plus anyone who requires fundamental training on the ASA
Security technicians, administrators, and engineers.

Objectives:

- Technology and features of the Cisco ASA
- Cisco ASA product family
- How ASAs protect network devices from attacks
- Bootstrap the security appliance
- Prepare the security appliance for configuration via the Cisco Adaptive Security Device Manager (ASDM)
- Launch and navigate ASDM
- Essential security appliance configuration using ASDM and the command-line interface (CLI)
- Configure dynamic and static address translations
- Configure access policy based on ACLs
- Use object groups to simplify ACL complexity and maintenance
- Use the Modular Policy Framework to provide unique policies to specific data flows
- Handle advanced protocols with application inspection
- Troubleshoot with syslog and tcp ping
- Configure the ASA to work with Cisco Secure ACS 5.2 for RADIUS-based AAA of VPNs
- Implement site-to-site IPsec VPN
- Implement remote access IPsec and SSL VPNs using the Cisco AnyConnect 3.0 Secure Mobility Client
- Work with the 5.x Legacy Cisco IPsec VPN client
- Deploy clientless SSL VPN access, including smart tunnels, plug-ins, and web-type ACLs
- Configure access control policies to implement your security policy across all classes of VPN
- Configure Active/Standby failover for both firewall and VPN high availability

Prerequisites:

- IINS 2.0 - Implementing Cisco IOS Network Security

Follow-on-Courses:

- FIREWALL 2.0 - Deploying Cisco ASA Firewall Solutions
- VPN 2.0 - Deploying Cisco ASA VPN Solutions

Content:

1. Cisco ASA Essentials

- Evaluating Cisco ASA Technologies
- Identifying Cisco ASA Families

2. Basic Connectivity and Device Management

- Preparing the Cisco ASA for Network Integration
- Managing Basic Cisco ASA Network Settings
- Configuring Cisco ASA Device Management Features

3. Network Integration

- Configuring Cisco ASA NAT Features
- Configuring Cisco ASA Basic Access Control Features

4. Cisco ASA Policy Control

- Cisco ASA Modular Policy Framework
- Configuring Cisco ASA Connection Policy

5. Cisco ASA VPN Architecture and Common Components

- Implementing Profiles, Group Policies, and User Policies
- Implementing PKI Services

6. Cisco ASA Clientless Remote Access SSL VPN Solutions

- Deploying Basic Clientless VPN Solutions
- Deploying Advanced Application Access for Clientless SSL VPNs

7. Cisco AnyConnect Remote Access SSL Solutions

- Deploying a Basic Cisco AnyConnect Full-Tunnel SSL VPN Solution

8. Cisco ASA Remote Access IPsec VPNs

- Deploying Cisco Remote Access VPN Clients
- Deploying Basic Cisco Remote Access IPsec VPN Solutions

9. Cisco ASA Site-to-Site IPsec VPN Solutions

- Deploying Basic Site-to-Site IPsec VPNs
- Deploying Advanced Site-to-Site IPsec VPNs

10. Cisco ASA High Availability and Virtualization

- Configuring Cisco ASA Active/Standby High Availability

Labs

- These labs are enhanced versions of what you'll find in Cisco's FIREWALL and VPN courses. Streamlined and built to work with our unique lab topology, these labs give you hands-on practice that is vital to mastering the course c

Lab 1: Prepare the ASA for Administration

- Prepare the ASA for remote administration by both SSH and HTTPS/ASDM
- Access the ASA via its physical console port and reset the configuration to factory defaults
- Use the setup dialog to configure the inside interface Enable ASDM access via HTTP
- Enable SSH from the CLI
- Test SSH access from the Admin-PC
- Install and configure ASDM on the Admin-PC and test initial access with ASDM
- Prepare a persistent self-signed digital certificate for use for ASDM

Lab 2: Fundamental ASA Configuration

- Configure basic ASA settings including static routes
- Configure the Inside, Outside, and DMZ interfaces
- Configure authenticated NTP support, syslog, and SNMP support
- Configure DHCP Server
- Use different features to test the behavior of the ASA

Lab 3: Network Address Translation (NAT)

- Configure object NAT for dynamic PAT
- Configure object NAT for dynamic NAT
- Configure object NAT for static NAT
- Configure twice NAT
- Test and verify the results of the configuration on the communicating host systems and the ASA
- Configure and monitor address translation

Lab 6: Licensing, ACS, and Public CA

- Work with licensing scenario design challenges Configure the ASA and ACS 5.2 integration for AAA
- Configure ACS 5.2 integration with Active Directory
- Create an ACS 5.2 identity sequence and test authentication
- Manually Obtain SSL certificates from a public CA

Lab 7: Basic Clientless SSL VPN

- Enable DNS lookups to facilitate the portal
- Enable and test clientless SSL VPN
- Connection profiles and group policies
- Connection profile lock using ACS 5.2
- Browsing policies for group policies
- Bookmark lists for group policies
- Navigating without using the URL entry field
- Work with WebType ACLs

Lab 8: Clientless SSL VPN - Thin Apps

- Implement and test port forwarding
- Implement and test smart tunnels
- Implement and test SSL VPN plug-ins

Lab 9: Basic AnyConnect Full Tunnel SSL VPN

- Configure address assignment policy and pools
- Enable AnyConnect and upload client to the ASA
- Configure SSL protocols
- Modify Connection profiles and group policies
- Install the AnyConnect client using WebLaunch
- Configure NAT for remote access VPN
- Allow Internet access via Split Tunneling
- Allow Internet access via Hairpin
- Modify local as well as centralized group policy

Lab 10: Remote Access IPSec VPN

- Enable IKEv2 IPSec remote access VPN
- Reset the AnyConnect Client on the Win7-PC
- Download and test the IPSec AnyConnect profile
- Implement IKEv2 with certificate-based authentication
- Enable and test IKEv1 IPSec remote access VPN

Lab 11: IPSec Site-to-Site VPN

- Configure a site-to-site tunnel from HQ to Site1

- Differences between the ASA's translation and connection tables

Lab 4: Basic Access Control

- Object groups
- Configure global policy
- Configure access policy to allow access to public services running on the DMZ-Srv from the outside
- Configure access policy to allow unrestricted access from the Inside network

Lab 5: Basic Protocol Inspection

- Explore the ASA's simple application layer inspection using FTP and HTTP
- Use the modular policy framework to inspect Layer 3 and Layer 4 packet headers
- Control traffic based on information received
- Work with TTL Decrementation and TCP Maps
- Configure the ASA to work with custom dynamic applications

- Use ASDM to configure the building blocks of the tunnel configuration and see how they work together
- Modify the NAT configuration on the ASA to conform with tunnel requirements
- Monitor tunnel status from the CLI, ASDM, and syslog
- Analyze tunnel establishment by following debug messages
- Apply a group policy to prevent systems on at Site1 from reaching the management subnet on the HQ network
- Update the VPN configuration for PKI support

Lab 12: Active/Standby Failover

- Configure two ASAs for Active/Standby failover
- Prepare the primary ASA for failover using ASDM and configure the secondary ASA via the CLI
- Verify failover status and perform a failover scenario to see how services resume when the standby systems assume the active role
- Return the systems back to their base failover state

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.co.uk

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