ASA LAB CAMP 9.5

Course Code: 4278

Hone your ASA v9.x and SFR skills in this hands-on, lab-focused class.

EXCLUSIVE TO GLOBAL KNOWLEDGE - Accelerate your Cisco learning experience with complimentary access to the IT Skills Video On-Demand Library, Introduction to Cybersecurity digital learning course, course recordings, IT Resource Library, and digital courseware.

Learn more

Based on our enhanced SASAC v1.0 and SASAA v2.1 courses, this exclusive, lab-based course, provides you with your own set of equipment, giving you the Adaptive Security Appliance (ASA) 9.x and ASA SFR-based lab experience in just five days. This course provides 29 different lab scenarios using Cisco equipment such as: ASA v9.5, ASA 5515-X NGFW (Next-Generation Firewall SFR), Access Control Server (ACS 5.4), Context Directory Agent (CDA), Catalyst switch, Integrated Services Router (ISR), and ASA 55x5.

A typical day will begin with an informal white board lecture by the instructor, covering topics associated with the day's labs. Afterwards, you will be free to work on the labs at your own pace and to experiment in the lab environment. Of course, the instructor will remain available to assist as needed.

ASA 9.5 labs can be run in any order, any number of times. ASA-SFR labs will be run consecutively. With the exception of two labs that require two pods to work together, no coordination with other students is necessary.

This course includes 30 Cisco e-lab credits. Your e-Lab credits are good for 90 days after your course ends and can be used for additional practice on the course you just completed or to explore technologies from other courses in the Global Knowledge e-Lab portfolio. Learn more.

What You'll Learn

- Fundamental ASA configuration from the CLI and ASDM
- Administrative access using AAA, TACACS+, and Cisco ACS 5.x

- Object (auto) NAT and manual (twice) NAT
- Access control and troubleshooting tools
- Application inspection and control (deep packet inspection)
- ASAv using 9.4 code
- Equal cost multipathing using ASA security zones
- Policy Based Routing on the ASA
- ACL enhancements including forward reference and manual commit
- Using the REST API to configure the ASA
- Configuring BGP support on the ASA using 9.4 code
- Bootstrapping and configuring the SFR 6.0 software module
- Deploying Cisco Context Directory Agent (CDA) with Active Directory
- Features of Cisco ASA 5500-X Series Next-Generation Firewalls (NGFW ASA SFR)
- SFR (FirePOWER Services) software module integration using FirePOWER Management Center 6.0 and access control, intrusion prevention, file policy, network discovery, Active Directory integration, user based access control, DNS, URL, and SSL policy
- Cloud Web Security (ScanSafe) integration
- Threat and botnet detection
- Dynamic routing
- Transparent firewall and bridge groups
- Basic and advanced clientless SSL VPN
- Full tunnel SSL VPN using AnyConnect 3.x Secure Mobility Client
- Remote Access IPsec IKEv2 using AnyConnect 3.x
- Easy VPN remote for the SOHO using ASA 5505
- External AAA authentication of VPN users
- PKI and VPN integration
- Host scan and dynamic access policies (DAP) for VPN
- IPsec VPN site-to-site between ASAs and with IOS router
- ASA and ISE integration for TrustSec Firewall using Security Group Tags
- Active/standby failover
- ASA clustering including local and spanned EtherChannel

Who Needs to Attend

- Network engineers supporting Cisco ASA 9.x implementations

Prerequisites

- Knowledge of the Cisco ASA

ASA LAB CAMP 9.5

Course Code: 4278

CLASSROOM LIVE	$4,895 USD	5 days

Classroom Live Outline

1. Cisco ASA v9.5 Essentials
   - Firewall Technologies
   - Cisco ASA Features, Hardware, and Licenses
2. Basic Connectivity and Device Management
   - Managing the Cisco ASA Boot Process
   - Configuring the Cisco ASA Using the CLI and ASDM
   - Managing the Cisco ASA Basic Upgrade
   - Managing Cisco ASA Security Levels and Interfaces
   - Cisco ASA as DHCP Client and DHCP Server
3. Network Integration
   - Configuring Object (Auto) NAT and Manual NAT
   - Connection Table and Local Host Table
   - Configuring and Verifying Interface and Global ACLs
   - Configuring and Verifying Object Groups and Public Servers
   - Static and Dynamic Routing
   - Multicast Support
4. Cisco ASA Policy Control
   - Cisco Modular Policy Framework (MPF) Overview
   - Configuring Layer 3 and Layer 4 Policies
   - Configuring Layer 5 to Layer 7 Policies including HTTP and FTP inspection
5. Cisco ASA VPN Common Components
   - VPN Types and Components
   - VPN Connection Profiles and Group Policies
   - AAA Including External Policy Storage
   - Dynamic Access Policy for SSL VPN
   - PKI for VPN Including Provisioning Server-Side Certificates
   - Client-Based Certificate Authentication Including SCEP proxy

6. Cisco Clientless VPN Solution
    - Cisco ASA v9.5 Essentials
    - Firewall Technologies
    - Cisco ASA Features, Hardware, and Licenses
7. Basic Connectivity and Device Management
    - Managing the Cisco ASA Boot Process
    - Configuring the Cisco ASA Using the CLI and ASDM
    - Managing the Cisco ASA Basic Upgrade
    - Managing Cisco ASA Security Levels and Interfaces
    - Cisco ASA as DHCP Client and DHCP Server
8. Network Integration
    - Configuring Object (Auto) NAT and Manual NAT
    - Connection Table and Local Host Table
    - Configuring and Verifying Interface and Global ACLs
    - Configuring and Verifying Object Groups and Public Servers
    - Static and Dynamic Routing
    - Multicast Support
9. Cisco ASA Policy Control
    - Cisco Modular Policy Framework (MPF) Overview
    - Configuring Layer 3 and Layer 4 Policies
    - Configuring Layer 5 to Layer 7 Policies including HTTP and FTP inspection
10. Cisco ASA VPN Common Components
    - VPN Types and Components
    - VPN Connection Profiles and Group Policies
    - AAA Including External Policy Storage
    - Dynamic Access Policy for SSL VPN
    - PKI for VPN Including Provisioning Server-Side Certificates
    - Client-Based Certificate Authentication Including SCEP proxy
11. Cisco Clientless VPN Solution
    - Cisco Clientless SSL VPN
    - Basic Cisco Clientless SSL VPN
    - Cisco Clientless SSL VPN Application Access with Application Plug-Ins and Smart Tunnels
    - Client-side Authentication and Authorization Using AAA Server
    - Double Client-side Authentication Using AAA Servers
12. Cisco AnyConnect Full Tunnel VPN Solution
    - Cisco AnyConnect SSL VPN
    - Split Tunneling
    - IP Address Pools and Identity NAT
    - DTLS and TLS Tunnels
    - Cisco AnyConnect Client Configuration Management
    - Trusted Network Detection and Start Before Logon options

- Certificate-Based Server Authentication
- Client Enrollment Methods and Certificate-Based Authentication
- Two-Factor Authentication
- Local Authorization and External Authorization
- AnyConnect Support for IKEv2
- Making IPsec the Primary Protocol for a Host Entry

13. Cisco ASA High Availability and Virtualization
    - EtherChannel and Redundant Interfaces
    - Multiple-Context Mode
14. Cisco Next Generation Firewall
    - Introducing the Cisco ASA 5500-X Series NGFW
    - Introducing the Cisco ASAv
    - Implementing ASA 9.3 and 9.4.1 New Features
    - Introducing the Cisco ASASM
15. Cisco ASA Identity Firewall
    - Describing the Cisco IDFW Solution
    - Setting Up Cisco CDA
    - Configuring Cisco CDA
    - Configuring Cisco ASA IDFW
    - Verifying and Troubleshooting Cisco ASA IDFW
16. Cisco ASA FirePOWER (SFR) Module
    - Installing Cisco ASA 5500-X Series FirePOWER (SFR) Module
    - Managing Cisco ASA FirePOWER Services Module Using Cisco FireSIGHT Management Center
    - Describing the Cisco ASA 5506-X, 5508-X, and 5516-X FirePOWER Services
    - Configuring ASA Firepower Services v6.0 New Features
17. Cisco ASA Cloud Web Security Integration
    - Introducing Cisco ASA with Cisco Cloud Web Security
    - Configuring Cisco ASA with Cisco Cloud Web Security
    - Verifying Cisco ASA with Cisco Cloud Web Security
    - Describing the Web Filtering Policy in Cisco ScanCenter
    - Cisco Cloud Web Security Advanced Malware Protection and Threat Analytics
18. Cisco ASA Cluster
    - Describing Cisco ASA Cluster Features
    - Describing Cisco ASA Cluster Terminology and Data Flows
    - Using the CLI to Configure a Cisco ASA Cluster
    - Using the ASDM to Configure a Cisco ASA Cluster
    - Verifying Cisco ASA Cluster Operations
    - Troubleshooting a Cisco ASA Cluster Operations
    - Describing Cisco ASA v9.1.4 and later Clustering Features
19. Cisco ASA Security Group Firewall and Change of Authorization
    - Cisco Security Group Tagging Overview

- Configuring Cisco ASA Security Group Firewall
- Describing the ASA 9.2.1 and Later Releases SGT Features
- Describing the ASA 9.2.1 and Later Releases Change of Authorization Support

Note: You will be provided with copies of Cisco official courseware for SASAC and SASAA 2.1 in addition to a Global Knowledge ASA Lab Camp guide.?

Classroom Live Labs

SASAC v1 Labs

Lab 1: ASA Administration and Network Integration

- Clear the Existing Configuration
- Take Inventory of the ASA
- Initialize the ASA
- Enable SSH
- Install ASDM
- Configure Interfaces
- Setup Names and Static Routes
- Configure NTP, Syslog, and SNMP
- Configure DHCP Server
- Install CA Root and Identity Certificates

Lab 2: Network Address Translation

- Object NAT (for Dynamic PAT)
- Object NAT (for Dynamic NAT)
- Object NAT (for Static NAT)
- Manual NAT
- NAT Rule Order

Lab 3: Access Control and Troubleshooting

- Create Object Groups
- Configure Global Policy
- Configure Guest Policy
- Configure Outside Policy
- Configure DMZ Policy
- Configure Inside Policy
- Configure ICMP Policy

- Configure uRPF Policy
- Ping TCP
- Packet Tracer

Lab 4: MPF Basic Application Inspections

- Basic HTTP and FTP Inspection
- TTL Decrement and ISN Randomization
- TCP Normalization and Connection Settings
- Custom Application Support
- QoS with Priority Queuing and Policing

Lab 5: MPF Advanced Application Inspections

- Enforcing HTTP RFC Compliance
- Block an Undesirable HTTP Application
- Filter Commands within FTP

Lab 6: Basic Clientless SSL VPN

- Public CA Certificate
- Configure ASA for DNS
- Enable and Test Clientless SSL VPN
- Connection Profiles and Group Policies
- Local Users on the ASA
- Browsing Policies
- Bookmark Lists
- Navigating without URL Entry
- WebType ACLs

Lab 7: Clientless SSL VPN Applications

- Port Forwarding
- Advanced Bookmarks
- VPN Plugins
- Smart Tunnels

Lab 8: External AAA for Clientless SSL VPN

- AAA Options
- External AAA with LDAP
- External AAA with RADIUS and ACS

Lab 9: Basic AnyConnect SSL VPN

- Configure Address Assignment Policy and Pools
- Enable AnyConnect and Upload Client to the ASA
- Configure SSL Algorithms
- Modify Group Policies
- Install AnyConnect Using WebLaunch
- Configure NAT for Remote Access VPN
- Allow Internet Access via Split Tunneling
- Allow Internet Access via Hairpin
- Modify a Local Group Policy

- Configure a Centralized Group Policy

Lab 10: Advanced AnyConnect SSL VPN

- DTLS and TLS Fallback
- Pre-deploy Install of AnyConnect
- AnyConnect XML Profiles
- Certificates with SCEP proxy

Lab 11: IPSec Remote Access VPN

- Enable IKEv2 IPsec remote access VPN
- Test the IPsec AnyConnect Profile
- IKEv2 with SCEP Proxy

Lab 12: Active-Standby High Availability

- Prepare for this Lab
- Prepare the Primary-ASA for Failover via ASDM
- Configure the Failover Prompt
- Prepare the Secondary-ASA for Failover via the CLI
- Turn Failover On and Verify Status
- Test Failover Operation
- Return to a Normal State
- Demonstrate Configuration Replication

SASAA v2.1 Labs

Lab 1: Set Up and Test the ASAv

- Take Inventory of the ASAv
- Initialize the ASAv
- Enable SSH
- Connect via ASDM
- Configure Interfaces
- Setup names & Static Routes
- Configure NTP, and Syslog
- Configure NAT & ACLs
- Configure BGP

Lab 2: Implement New Features in ASA 9.3 and 9.4

- Configure and Monitor the ASAv Using the REST API
- ACL Forward Reference
- ACL Manual Commit
- Policy-Based Routing
- Verify ECMP

Lab 3: Configure the Cisco CDA

- Explore the Cisco CDA CLI
- Work with CDA CLI User Accounts
- Explore the Cisco CDA GUI
- Configure CDA Communications to ASA, AD, and Syslog

Lab 4: Configure ASA IDFW

- Configure ASA to AD Communications
- Configure ASA to CDA Communications
- Set Up ASA User-Identity Options
- Configure Identity-Based Access Control
- Test Identity-Based Access Control

Lab 5: Install and Configure ASA SFR

- Install and Set Up the ASA FirePower (SFR) Module
- Redirect Traffic to the ASA SFR

Lab 6: Configure and Test Firepower Management Center

- Add the ASA SFR to the FMC (FMC)
- Examine the System Configuration, Firepower Setting Policy, and Health Policy
- Edit the Default FMC Network Discovery Rule
- Configure the IPS, File, and Access Control Policies
- Test the Basic SFR IPS Operations
- Test the Basic SFR AMP Operations
- Examine the Firepower Network Discovery Results
- Integrate Firepower with Active Directory
- Configure Identity Policy
- Configure User Based Access Control Policy
- Test User Based Access Control Policy
- Configure Basic Custom Application Detector
- Configure DNS Policy
- Configure SSL Policy
- Examine Other Firepower v6.0 Features

Lab 7: Configure ASA CWS

- Understand the Cloud Web Security Web Filtering Policy
- Download the Cloud Web Security License File
- Configure ASA-to-Cloud Web Security Integration

Lab 8: Configuring Security Group Access

- Configure the ASA for VPN access
- Verify the ISE Server Communicates with Active Directory
- Configure the ISE Server for ASA TrustSec Integration
- Import the PAC File from the ISE Server
- Test Remote Access VPN
- Configure Security Group Access on the ASA
- Verify the SGA Configuration
- Configure the ASA to Impose Layer 2 SGTs

Lab 9: Implement Cisco ASA Clustering

- Configure Spanned EtherChannel Mode on Each ASA
- Configure the Cluster Hostname on the Odd Pod ASA
- Configure the CCL Using a Local EtherChannel on Each ASA

- Configure the Management Interface in Individual Mode (L3) on the Odd Pod ASA
- Configure the Data Interfaces in Spanned EtherChannel (L2) Mode on the Odd Pod ASA
- Configure the Cluster Bootstrap Configurations and Enable Clustering on Each ASA
- Verify and Manage the Cluster Operations Using the CLI
- Verify the Cluster Operations Using ASDM
- Verify HTTP Connections Through the Cluster
- Configure the ASA Firewall Policy on the Master Unit
- Simulate a Master Unit Failure and Observe Results
- ASA Global Knowledge Exclusive Add-On Labs

ASA Global Knowledge Exclusive Add-On Labs

Lab 1: Dynamic Routing

- Configure Non-ASA Devices for EIGRP and OSPF
- Modify the ASA in Preparation for Dynamic Routing
- Configure OSPF on The the ASA
- Configure EIGRP on The the ASA
- Verify Routing Operations
- Enable Route Redistribution and Verify the Results

Lab 2: Threat Detection

- Working with Basic Threat Detection
- Interpreting Threat Detection Statistics
- Configure and Verify TCP Intercept

Lab 3: IKEv1 Site-to-Site VPN (ASA to IOS router)

- Configure the HQ-ASA for Site-to-Site VPN
- Verify an IKEv1 Policy
- Build the Site-to-Site Connection Profile
- Configure NAT Exemption
- Monitor Tunnel Establishment
- Verifying Tunnel Status
- Control Site-to-Site Traffic with a Filter
- Update the VPN Configuration for PKI Support

Lab 4*: Hardware Easy VPN (ASA 5505 to ASA 5515)

- Configure the Easy VPN Server
- Configure the Easy VPN Remote
- Verify Easy VPN Client Mode
- Implement Network Extension Mode
- Work with Extended Authentication Options

Lab 5*: IKEv2 Site-to-Site VPN (ASA to ASA)

- Setup an IKEv2 Site-to-Site VPN
- Verify an IKEv2 Site-to-Site VPN

Lab 6: ACS 5.x and TACACS+ for Administrative Access

- Work with Privilege Level Authorization
- Configure ACS and ASA Communication
- Configure ACS Integration with Active Directory
- Implement User Authentication using TACACS+
- Institute User Authorization using TACACS+
- Add Command Authorization using TACACS+
- Explore Command Accounting using TACACS+

Lab 7: Transparent Firewall

- Configure Transparent Firewall Mode
- Create Bridge Groups, Interfaces, and Management Address
- Test Connectivity through the Security Appliance
- Prepare the ASA for and Launch ASDM
- Define and Test Inbound Policy with ASDM

Lab 8: Host Scan and Dynamic Access Policies and VPN

- Enable Host Scan and Examine Anti-Spyware Software on an Endpoint
- Deploy DAP to Evaluate Endpoint Posture Status
- Deploy Anti-Virus Posture

*ASA Lab Camp Lab v9.5 has two distinctive parts: Hardware Easy VPN and IKEv2 Site-to-Site VPN.?

ASA LAB CAMP 9.5

Course Code: 4278

VIRTUAL CLASSROOM LIVE	$4,895 USD	5 days

Virtual Classroom Live Outline

SASAC v1 Labs

Lab 1: ASA Administration and Network Integration

- Clear the Existing Configuration
- Take Inventory of the ASA
- Initialize the ASA
- Enable SSH
- Install ASDM
- Configure Interfaces
- Setup Names and Static Routes
- Configure NTP, Syslog, and SNMP
- Configure DHCP Server
- Install CA Root and Identity Certificates

Lab 2: Network Address Translation

- Object NAT (for Dynamic PAT)
- Object NAT (for Dynamic NAT)
- Object NAT (for Static NAT)
- Manual NAT
- NAT Rule Order

Lab 3: Access Control and Troubleshooting

- Create Object Groups
- Configure Global Policy
- Configure Guest Policy
- Configure Outside Policy
- Configure DMZ Policy
- Configure Inside Policy
- Configure ICMP Policy
- Configure uRPF Policy

- Ping TCP
- Packet Tracer

Lab 4: MPF Basic Application Inspections

- Basic HTTP and FTP Inspection
- TTL Decrement and ISN Randomization
- TCP Normalization and Connection Settings
- Custom Application Support
- QoS with Priority Queuing and Policing

Lab 5: MPF Advanced Application Inspections

- Enforcing HTTP RFC Compliance
- Block an Undesirable HTTP Application
- Filter Commands within FTP

Lab 6: Basic Clientless SSL VPN

- Public CA Certificate
- Configure ASA for DNS
- Enable and Test Clientless SSL VPN
- Connection Profiles and Group Policies
- Local Users on the ASA
- Browsing Policies
- Bookmark Lists
- Navigating without URL Entry
- WebType ACLs

Lab 7: Clientless SSL VPN Applications

- Port Forwarding
- Advanced Bookmarks
- VPN Plugins
- Smart Tunnels

Lab 8: External AAA for Clientless SSL VPN

- AAA Options
- External AAA with LDAP
- External AAA with RADIUS and ACS

Lab 9: Basic AnyConnect SSL VPN

- Configure Address Assignment Policy and Pools
- Enable AnyConnect and Upload Client to the ASA
- Configure SSL Algorithms
- Modify Group Policies
- Install AnyConnect Using WebLaunch
- Configure NAT for Remote Access VPN
- Allow Internet Access via Split Tunneling
- Allow Internet Access via Hairpin
- Modify a Local Group Policy
- Configure a Centralized Group Policy

Lab 10: Advanced AnyConnect SSL VPN

- DTLS and TLS Fallback
- Pre-deploy Install of AnyConnect
- AnyConnect XML Profiles
- Certificates with SCEP proxy

Lab 11: IPSec Remote Access VPN

- Enable IKEv2 IPsec remote access VPN
- Test the IPsec AnyConnect Profile
- IKEv2 with SCEP Proxy

Lab 12: Active-Standby High Availability

- Prepare for this Lab
- Prepare the Primary-ASA for Failover via ASDM
- Configure the Failover Prompt
- Prepare the Secondary-ASA for Failover via the CLI
- Turn Failover On and Verify Status
- Test Failover Operation
- Return to a Normal State
- Demonstrate Configuration Replication

SASAA v2.1 Labs

Lab 1: Set Up and Test the ASAv

- Take Inventory of the ASAv
- Initialize the ASAv
- Enable SSH
- Connect via ASDM
- Configure Interfaces
- Setup names & Static Routes
- Configure NTP, and Syslog
- Configure NAT & ACLs
- Configure BGP

Lab 2: Implement New Features in ASA 9.3 and 9.4

- Configure and Monitor the ASAv Using the REST API
- ACL Forward Reference
- ACL Manual Commit
- Policy-Based Routing
- Verify ECMP

Lab 3: Configure the Cisco CDA

- Explore the Cisco CDA CLI
- Work with CDA CLI User Accounts
- Explore the Cisco CDA GUI
- Configure CDA Communications to ASA, AD, and Syslog

Lab 4: Configure ASA IDFW

- Configure ASA to AD Communications

- Configure ASA to CDA Communications
- Set Up ASA User-Identity Options
- Configure Identity-Based Access Control
- Test Identity-Based Access Control

Lab 5: Install and Configure ASA SFR

- Install and Set Up the ASA FirePower (SFR) Module
- Redirect Traffic to the ASA SFR

Lab 6: Configure and Test Firepower Management Center

- Add the ASA SFR to the FMC (FMC)
- Examine the System Configuration, Firepower Setting Policy, and Health Policy
- Edit the Default FMC Network Discovery Rule
- Configure the IPS, File, and Access Control Policies
- Test the Basic SFR IPS Operations
- Test the Basic SFR AMP Operations
- Examine the Firepower Network Discovery Results
- Integrate Firepower with Active Directory
- Configure Identity Policy
- Configure User Based Access Control Policy
- Test User Based Access Control Policy
- Configure Basic Custom Application Detector
- Configure DNS Policy
- Configure SSL Policy
- Examine Other Firepower v6.0 Features

Lab 7: Configure ASA CWS

- Understand the Cloud Web Security Web Filtering Policy
- Download the Cloud Web Security License File
- Configure ASA-to-Cloud Web Security Integration

Lab 8: Configuring Security Group Access

- Configure the ASA for VPN access
- Verify the ISE Server Communicates with Active Directory
- Configure the ISE Server for ASA TrustSec Integration
- Import the PAC File from the ISE Server
- Test Remote Access VPN
- Configure Security Group Access on the ASA
- Verify the SGA Configuration
- Configure the ASA to Impose Layer 2 SGTs

Lab 9: Implement Cisco ASA Clustering

- Configure Spanned EtherChannel Mode on Each ASA
- Configure the Cluster Hostname on the Odd Pod ASA
- Configure the CCL Using a Local EtherChannel on Each ASA
- Configure the Management Interface in Individual Mode (L3) on the Odd Pod ASA

- Configure the Data Interfaces in Spanned EtherChannel (L2) Mode on the Odd Pod ASA
- Configure the Cluster Bootstrap Configurations and Enable Clustering on Each ASA
- Verify and Manage the Cluster Operations Using the CLI
- Verify the Cluster Operations Using ASDM
- Verify HTTP Connections Through the Cluster
- Configure the ASA Firewall Policy on the Master Unit
- Simulate a Master Unit Failure and Observe Results
- ASA Global Knowledge Exclusive Add-On Labs

ASA Global Knowledge Exclusive Add-On Labs

Lab 1: Dynamic Routing

- Configure Non-ASA Devices for EIGRP and OSPF
- Modify the ASA in Preparation for Dynamic Routing
- Configure OSPF on The the ASA
- Configure EIGRP on The the ASA
- Verify Routing Operations
- Enable Route Redistribution and Verify the Results

Lab 2: Threat Detection

- Working with Basic Threat Detection
- Interpreting Threat Detection Statistics
- Configure and Verify TCP Intercept

Lab 3: Botnet Traffic Filter

- Configure the Botnet Traffic Filter Using the Dynamic Database
- Configure the Botnet Traffic Filter Using the Static Database

Lab 4: IKEv1 Site-to-Site VPN (ASA to IOS router)

- Configure the HQ-ASA for Site-to-Site VPN
- Verify an IKEv1 Policy
- Build the Site-to-Site Connection Profile
- Configure NAT Exemption
- Monitor Tunnel Establishment
- Verifying Tunnel Status
- Control Site-to-Site Traffic with a Filter
- Update the VPN Configuration for PKI Support

Lab 5*: Hardware Easy VPN (ASA 5505 to ASA 5515)

- Configure the Easy VPN Server
- Configure the Easy VPN Remote
- Verify Easy VPN Client Mode
- Implement Network Extension Mode
- Work with Extended Authentication Options

Lab 6*: IKEv2 Site-to-Site VPN (ASA to ASA)

- Setup an IKEv2 Site-to-Site VPN

- Verify an IKEv2 Site-to-Site VPN

Lab 7: ACS 5.x and TACACS+ for Administrative Access

- Work with Privilege Level Authorization
- Configure ACS and ASA Communication
- Configure ACS Integration with Active Directory
- Implement User Authentication using TACACS+
- Institute User Authorization using TACACS+
- Add Command Authorization using TACACS+
- Explore Command Accounting using TACACS+

Lab 8: Transparent Firewall

- Configure Transparent Firewall Mode
- Create Bridge Groups, Interfaces, and Management Address
- Test Connectivity through the Security Appliance
- Prepare the ASA for and Launch ASDM
- Define and Test Inbound Policy with ASDM

Lab 9: Host Scan and Dynamic Access Policies and VPN

- Enable Host Scan and Examine Anti-Spyware Software on an Endpoint
- Deploy DAP to Evaluate Endpoint Posture Status
- Deploy Anti-Virus Posture

*ASA Lab Camp Lab v9.5 has two distinctive parts: Hardware Easy VPN and IKEv2 Site-to-Site VPN.?

Virtual Classroom Live Labs

SASAC v1 Labs

Lab 1: ASA Administration and Network Integration

- Clear the Existing Configuration
- Take Inventory of the ASA
- Initialize the ASA
- Enable SSH
- Install ASDM
- Configure Interfaces
- Setup Names and Static Routes
- Configure NTP, Syslog, and SNMP
- Configure DHCP Server
- Install CA Root and Identity Certificates

Lab 2: Network Address Translation

- Object NAT (for Dynamic PAT)
- Object NAT (for Dynamic NAT)
- Object NAT (for Static NAT)
- Manual NAT
- NAT Rule Order

Lab 3: Access Control and Troubleshooting

- Create Object Groups
- Configure Global Policy
- Configure Guest Policy
- Configure Outside Policy
- Configure DMZ Policy
- Configure Inside Policy
- Configure ICMP Policy
- Configure uRPF Policy
- Ping TCP
- Packet Tracer

Lab 4: MPF Basic Application Inspections

- Basic HTTP and FTP Inspection
- TTL Decrement and ISN Randomization
- TCP Normalization and Connection Settings
- Custom Application Support
- QoS with Priority Queuing and Policing

Lab 5: MPF Advanced Application Inspections

- Enforcing HTTP RFC Compliance
- Block an Undesirable HTTP Application
- Filter Commands within FTP

Lab 6: Basic Clientless SSL VPN

- Public CA Certificate
- Configure ASA for DNS
- Enable and Test Clientless SSL VPN
- Connection Profiles and Group Policies
- Local Users on the ASA
- Browsing Policies
- Bookmark Lists
- Navigating without URL Entry
- WebType ACLs

Lab 7: Clientless SSL VPN Applications

- Port Forwarding
- Advanced Bookmarks
- VPN Plugins
- Smart Tunnels

Lab 8: External AAA for Clientless SSL VPN

- AAA Options
- External AAA with LDAP
- External AAA with RADIUS and ACS

Lab 9: Basic AnyConnect SSL VPN

- Configure Address Assignment Policy and Pools

- Enable AnyConnect and Upload Client to the ASA
- Configure SSL Algorithms
- Modify Group Policies
- Install AnyConnect Using WebLaunch
- Configure NAT for Remote Access VPN
- Allow Internet Access via Split Tunneling
- Allow Internet Access via Hairpin
- Modify a Local Group Policy
- Configure a Centralized Group Policy

Lab 10: Advanced AnyConnect SSL VPN

- DTLS and TLS Fallback
- Pre-deploy Install of AnyConnect
- AnyConnect XML Profiles
- Certificates with SCEP proxy

Lab 11: IPSec Remote Access VPN

- Enable IKEv2 IPsec remote access VPN
- Test the IPsec AnyConnect Profile
- IKEv2 with SCEP Proxy

Lab 12: Active-Standby High Availability

- Prepare for this Lab
- Prepare the Primary-ASA for Failover via ASDM
- Configure the Failover Prompt
- Prepare the Secondary-ASA for Failover via the CLI
- Turn Failover On and Verify Status
- Test Failover Operation
- Return to a Normal State
- Demonstrate Configuration Replication

SASAA v2.1 Labs

Lab 1: Set Up and Test the ASAv

- Take Inventory of the ASAv
- Initialize the ASAv
- Enable SSH
- Connect via ASDM
- Configure Interfaces
- Setup names & Static Routes
- Configure NTP, and Syslog
- Configure NAT & ACLs
- Configure BGP

Lab 2: Implement New Features in ASA 9.3 and 9.4

- Configure and Monitor the ASAv Using the REST API
- ACL Forward Reference
- ACL Manual Commit

- Policy-Based Routing
- Verify ECMP

Lab 3: Configure the Cisco CDA

- Explore the Cisco CDA CLI
- Work with CDA CLI User Accounts
- Explore the Cisco CDA GUI
- Configure CDA Communications to ASA, AD, and Syslog

Lab 4: Configure ASA IDFW

- Configure ASA to AD Communications
- Configure ASA to CDA Communications
- Set Up ASA User-Identity Options
- Configure Identity-Based Access Control
- Test Identity-Based Access Control

Lab 5: Install and Configure ASA SFR

- Install and Set Up the ASA FirePower (SFR) Module
- Redirect Traffic to the ASA SFR

Lab 6: Configure and Test Firepower Management Center

- Add the ASA SFR to the FMC (FMC)
- Examine the System Configuration, Firepower Setting Policy, and Health Policy
- Edit the Default FMC Network Discovery Rule
- Configure the IPS, File, and Access Control Policies
- Test the Basic SFR IPS Operations
- Test the Basic SFR AMP Operations
- Examine the Firepower Network Discovery Results
- Integrate Firepower with Active Directory
- Configure Identity Policy
- Configure User Based Access Control Policy
- Test User Based Access Control Policy
- Configure Basic Custom Application Detector
- Configure DNS Policy
- Configure SSL Policy
- Examine Other Firepower v6.0 Features

Lab 7: Configure ASA CWS

- Understand the Cloud Web Security Web Filtering Policy
- Download the Cloud Web Security License File
- Configure ASA-to-Cloud Web Security Integration

Lab 8: Configuring Security Group Access

- Configure the ASA for VPN access
- Verify the ISE Server Communicates with Active Directory
- Configure the ISE Server for ASA TrustSec Integration
- Import the PAC File from the ISE Server

- Test Remote Access VPN
- Configure Security Group Access on the ASA
- Verify the SGA Configuration
- Configure the ASA to Impose Layer 2 SGTs

Lab 9: Implement Cisco ASA Clustering

- Configure Spanned EtherChannel Mode on Each ASA
- Configure the Cluster Hostname on the Odd Pod ASA
- Configure the CCL Using a Local EtherChannel on Each ASA
- Configure the Management Interface in Individual Mode (L3) on the Odd Pod ASA
- Configure the Data Interfaces in Spanned EtherChannel (L2) Mode on the Odd Pod ASA
- Configure the Cluster Bootstrap Configurations and Enable Clustering on Each ASA
- Verify and Manage the Cluster Operations Using the CLI
- Verify the Cluster Operations Using ASDM
- Verify HTTP Connections Through the Cluster
- Configure the ASA Firewall Policy on the Master Unit
- Simulate a Master Unit Failure and Observe Results
- ASA Global Knowledge Exclusive Add-On Labs

ASA Global Knowledge Exclusive Add-On Labs

Lab 1: Dynamic Routing

- Configure Non-ASA Devices for EIGRP and OSPF
- Modify the ASA in Preparation for Dynamic Routing
- Configure OSPF on The the ASA
- Configure EIGRP on The the ASA
- Verify Routing Operations
- Enable Route Redistribution and Verify the Results

Lab 2: Threat Detection

- Working with Basic Threat Detection
- Interpreting Threat Detection Statistics
- Configure and Verify TCP Intercept

Lab 3: IKEv1 Site-to-Site VPN (ASA to IOS router)

- Configure the HQ-ASA for Site-to-Site VPN
- Verify an IKEv1 Policy
- Build the Site-to-Site Connection Profile
- Configure NAT Exemption
- Monitor Tunnel Establishment
- Verifying Tunnel Status
- Control Site-to-Site Traffic with a Filter
- Update the VPN Configuration for PKI Support

Lab 4*: Hardware Easy VPN (ASA 5505 to ASA 5515)

- Configure the Easy VPN Server
- Configure the Easy VPN Remote
- Verify Easy VPN Client Mode
- Implement Network Extension Mode
- Work with Extended Authentication Options

Lab 5*: IKEv2 Site-to-Site VPN (ASA to ASA)

- Setup an IKEv2 Site-to-Site VPN
- Verify an IKEv2 Site-to-Site VPN

Lab 6: ACS 5.x and TACACS+ for Administrative Access

- Work with Privilege Level Authorization
- Configure ACS and ASA Communication
- Configure ACS Integration with Active Directory
- Implement User Authentication using TACACS+
- Institute User Authorization using TACACS+
- Add Command Authorization using TACACS+
- Explore Command Accounting using TACACS+

Lab 7: Transparent Firewall

- Configure Transparent Firewall Mode
- Create Bridge Groups, Interfaces, and Management Address
- Test Connectivity through the Security Appliance
- Prepare the ASA for and Launch ASDM
- Define and Test Inbound Policy with ASDM

Lab 8: Host Scan and Dynamic Access Policies and VPN

- Enable Host Scan and Examine Anti-Spyware Software on an Endpoint
- Deploy DAP to Evaluate Endpoint Posture Status
- Deploy Anti-Virus Posture

*ASA Lab Camp Lab v9.5 has two distinctive parts: Hardware Easy VPN and IKEv2 Site-to-Site VPN.?

Oct 21 - 25, 2019 | 8:30 AM - 4:30 PM EST

Nov 18 - 22, 2019 | 9:30 AM - 5:30 PM EST

Dec 2 - 6, 2019 | 11:30 AM - 7:30 PM EST

Dec 9 - 13, 2019 | 8:30 AM - 4:30 PM EST

Feb 3 - 7, 2020 | 8:30 AM - 4:30 PM EST

Mar 16 - 20, 2020 | 8:30 AM - 4:30 PM EST

ASA LAB CAMP 9.5

Course Code: 4278

PRIVATE GROUP TRAINING	5 days

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 9/16/2019 12:32:23 PM