Implementing Core Cisco ASA Security v1.0 (SASAC)

Modality: Virtual Classroom

Duration: 5 Days

CLC: 38 Units

About this course:

Implementing Core Cisco ASA Security (SASAC) v1.0 is a new 5-day ILT class that:

- Covers the Cisco ASA 9.0 / 9.1 core firewall and VPN features
- Offers hands-on labs Cisco ASA Core v1.0 is designed to teach network security engineers working on the Cisco ASA Adaptive Security Appliance to implement core Cisco ASA features, including the new ASA 9.0 and 9.1 features.

Course Objective:

Upon completing this course, the learner will be able to meet these overall objectives:

- Essentials of Cisco ASA
- Basic connectivity and device management
- Network integration
- Configure common features of the Cisco ASA OS
- Cisco ASA policy control
- Core Cisco ASA VPN common components
- Main VPN components
- Cisco clientless VPN solutions
- Cisco AnyConnect full tunnel VPN solution
- Cisco ASA high availability and virtualization options
- Features of Cisco ASA 5500-X Series Next-Generation Firewalls

Audience:

The primary audience for this course is as follows:

- Network engineers supporting Cisco ASA 9.x implementations

Prerequisite:

The knowledge and skills that a learner should have before attending this course are as follows:

- Knowledge of the Cisco ASA
- IINS 2.0 - Implementing Cisco IOS Network Security

Course Outline:

Module 1: Cisco ASA Essentials

- Firewall Technologies
- Cisco ASA Features
- Cisco ASA Hardware
- Cisco ASA Licensing Options
- Cisco ASA Licensing Requirements

Module 2: Basic Connectivity and Device Management

- Managing the Cisco ASA Boot Process
- Managing the Cisco ASA Using the CLI
- Managing the Cisco ASA Using Cisco ASDM
- Navigating Basic Cisco ASDM Features
- Managing the Cisco ASA Basic Upgrade
- Managing Cisco ASA Security Levels
- Configuring and Verifying Basic Connectivity Parameters
- Configuring and Verifying Interface VLANs
- Configuring a Default Route
- Configuring and Verifying the Cisco ASA Security Appliance DHCP Server
- Troubleshooting Basic Connectivity

Module 3: Network Integration

- NAT on Cisco ASA Security Appliances
- Configuring Object (Auto) NAT
- Configuring Manual NAT
- Tuning and Troubleshooting NAT on the Cisco ASA
- Connection Table and Local Host Table
- Configuring and Verifying Interface ACLs
- Configuring and Verifying Global ACLs
- Configuring and Verifying Object Groups
- Configuring and Verifying Public Servers
- Configuring and Verifying Other Basic Access Controls
- Troubleshooting ACLs
- Static Routing
- Dynamic Routing
- EIGRP Configuration and Verification
- Multicast Support

Module 4: Cisco ASA Policy Control

- Cisco MPF Overview
- Configuring and Verifying Layer 3 and Layer 4 Policies
- Configuring and Verifying a Policy for Management Traffic
- Layer 5 to Layer 7 Policy Control Overview
- Configuring and Verifying HTTP Inspection
- Configuring and Verifying FTP Inspection

- Supporting Other Layer 5 to Layer 7 Applications
- Troubleshooting Application Layer Inspection

Module 5: Cisco ASA VPN Common Components

- VPN Definition
- Key Threats to WANs and Remote Access
- VPN Types
- VPN Components
- Cisco ASA VPN Policy Configuration
- Cisco ASA Connection Profiles
- Cisco ASA Group Policies
- Cisco ASA VPN AAA and External Policy Storage
- Cisco ASA User Attributes
- Access Control Methods
- VPN Accounting Using External Servers
- Dynamic Access Policy for SSL VPN
- Using PKI
- Provisioning Server-Side Certificates on the Cisco ASA Adaptive Security Appliance
- CA Servers
- Deploying Client-Based Certificate Authentication
- SCEP Proxy Operations
- Enable Certificate Authentication in Connection Profile
- Configuring Certificate-to-Connection Profile Mappings

Module 6: Cisco Clientless VPN Solution

- Cisco Clientless SSL VPN
- Cisco Clientless SSL VPN Use Cases
- Cisco Clientless SSL VPN Resource Access Methods
- Secure Sockets Layer and Transport Layer Security
- SSL Session Setup and Key Management
- SSL Server Authentication
- SSL Client Authentication
- SSL Transmission Protection
- Basic Cisco Clientless SSL VPN
- Server Authentication in Basic Clientless SSL VPN
- Client-side Authentication in Basic Clientless SSL VPN
- Clientless SSL VPN URL Entry and Bookmarks
- Basic Access Control for Clientless SSL VPN
- Disabling Content Rewriting
- Basic Clientless SSL VPN Configuration Tasks
- Basic Clientless SSL VPN Configuration Scenario
- Configuring Basic Cisco Clientless SSL VPN
- Verify Basic Cisco Clientless SSL VPN
- Troubleshooting Basic Clientless SSL VPN Operations
- Cisco Clientless SSL VPN Application Access Overview
- Application Plug-Ins

- Configuring Application Plug-ins
- Verify Clientless SSL VPN Application Plug-Ins
- Troubleshooting Clientless SSL VPN Application Plug-Ins
- Smart Tunnels
- Configuring Smart Tunnels
- Verifying Smart Tunnels
- Troubleshoot Smart Tunnels
- Client-side Authentication Options
- Client-side Authentication and Authorization Using AAA Server
- Double Client-side Authentication Using AAA Servers
- Troubleshooting Client-side AAA Authentication

Module 7: Cisco AnyConnect Full Tunnel VPN Solution

- Basic Cisco AnyConnect SSL VPN
- SSL VPN Clients Authentication
- SSL VPN Clients IP Address Assignment
- SSL VPN Split Tunneling
- Configuration Scenario
- Configuration Tasks
- Enable AnyConnect SSL VPN
- Define IP Address Pool
- Configure Identity NAT
- Configure Group Policy
- Configure Group Policy: Split Tunneling
- Configure Connection Profile
- Monitor AnyConnect VPN on Client
- Monitor AnyConnect VPN on Server
- Cisco AnyConnect SSL VPN Solution Components
- DTLS Overview
- Parallel DTLS and TLS Tunnels
- Configure DTLS
- Verify DTLS
- Cisco AnyConnect Client Configuration Management
- Managing Cisco AnyConnect Software from Cisco ASA
- Cisco AnyConnect Client Operating System Integration Options
- Deploying Cisco AnyConnect Trusted Network Detection
- Cisco AnyConnect Start Before Logon
- Deploying Cisco AnyConnect Start Before Logon
- Cisco AnyConnect Advanced Authentication Scenarios
- Certificate-Based Server Authentication
- Client Enrollment Methods
- Methods for Revoking Credentials
- Enable Certificate-Based Authentication
- Enable Two-Factor Authentication
- Two-Factor Authentication with Name Pre-Fill
- Local Authorization Overview
- Local Authorization Configuration Procedure

- Configure Local Authorization
- Verify Local Authorization
- External Authorization Scenario
- Configure Authorization Using LDAP/AD
- Verify External Authorization
- Troubleshooting Cisco AnyConnect VPN
- AnyConnect Support for IKEv2
- Internet Key Exchange v1 and v2
- Making IPsec the Primary Protocol for a Host Entry
- IKEv2 Configuration Procedure
- Configure a Cisco AnyConnect IPsec VPN on a Cisco ASA
- Verify and Troubleshoot Cisco AnyConnect IPsec VPN on Cisco ASA

Module 8: Cisco ASA High Availability and Virtualization

- Configuring and Verifying EtherChannel
- Configuring and Verifying Redundant Interfaces
- Troubleshooting EtherChannel and Redundant Interfaces
- Configuring and Verifying Redundant Interfaces
- Troubleshooting EtherChannel and Redundant Interfaces
- Multiple-Context Mode
- Configuring Security Contexts
- Verifying and Managing Security Contexts
- Configuring and Verifying Resource Management
- Troubleshooting Security Contexts

Self Study (optional)

- Active/Active Failover
- Configuring and Verifying Active/Active Failover
- Tuning and Managing Active/Active Failover
- Troubleshooting Active/Active Failover

Lab Outline

- Lab 1: Remote Lab Environment
- Lab 2: ASA Administration and Network Integration
- Lab 3: Network Address Translation
- Lab 4: Access Control and Troubleshooting
- Lab 5: MPF Basic Application Inspections
- Lab 6: MPF Advanced Application Inspections
- Lab 7: Basic Clientless SSL VPN
- Lab 8: Clientless SSL VPN Applications
- Lab 9: External AAA for Clientless SSL VPN
- Lab 10: Lab: Basic AnyConnect SSL VPN
- Lab 11: Advanced AnyConnect SSL VPN
- Lab 12: IPSec Remote Access VPN
- Lab 13: Active-Standby High Availability