# SASAC v1.0 Implementing Core Cisco ASA Security

Cisco Training

**Course Length:** 5
**Course Delivery:** Traditional Classroom • Online Live

**Course Overview**
Cisco ASA Core v1.0 is a new 5-day ILT class that covers the Cisco ASA 9.0 / 9.1 core firewall and VPN features. 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.

**Audience**
Network engineers supporting Cisco ASA 9.x implementations

**Prerequisites**
FIREWALL v1.0 or FIREWALL v2.0 or an equivalent knowledge of the Cisco ASA

**At the end of this CCNA training course, you'll be able to:**

- Explain the core essential features of Cisco ASA 5500-X Series Next-Generation Firewalls
- Describe how to implement Cisco ASA basic connectivity and device management
- Implement basic Cisco ASA network integration
- Describe and implement basic Cisco ASA policy controls
- Describe Cisco ASA common VPN components
- Describe and implement Cisco ASA clientless VPN solutions
- Describe and implement Cisco ASA and Cisco AnyConnect full tunnel VPN solutions

**Outline**
Module 1: Cisco ASA Adaptive Security Appliance Essentials

Lesson 1: Evaluating Cisco ASA Adaptive Security Appliance Technologies

- Firewall Technologies
- Cisco ASA Adaptive Security Appliance Features

Lesson 2: Identifying Cisco ASA Adaptive Security Appliance Models

- Cisco ASA Adaptive Security Appliance Hardware

Lesson 3: Identifying Cisco ASA Adaptive Security Appliance Licensing Options

- Cisco ASA Adaptive Security Appliance Licensing Options
- Cisco ASA Adaptive Security Appliance Licensing Requirements

Lesson 4: Module Summary

Module 2: Basic Connectivity and Device Management

Lesson 1: Preparing the Cisco ASA Adaptive Security Appliance for Network Integration

- Managing the Cisco ASA Adaptive Security Appliance Boot Process
- Managing the Cisco ASA Adaptive Security Appliance Using the CLI
- Managing the Cisco ASA Adaptive Security Appliance Using Cisco ASDM
- Navigating Basic Cisco ASDM Features
- Managing the Cisco ASA Adaptive Security Appliance Basic Upgrade

Lesson 2: Managing Basic Cisco ASA Adaptive Security Appliance Network Settings

- Managing Cisco ASA Adaptive Security Appliance 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

Lesson 3: Module Summary

Module 3: Network Integration

Lesson 1: Configuring Cisco ASA Adaptive Security Appliance NAT Features

- NAT on Cisco ASA Security Appliances
- Configuring Object (Auto) NAT
- Configuring Manual NAT
- Tuning and Troubleshooting NAT on the Cisco ASA Adaptive Security Appliance

Lesson 2: Configuring Cisco ASA Adaptive Security Appliance Basic Access Control Features

- 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

Lesson 3: Configuring Cisco ASA Adaptive Security Appliance Routing Features

- Static Routing
- Dynamic Routing
- EIGRP Configuration and Verification
- Multicast Support

Lesson 4: Module Summary

Module 4: Cisco ASA Adaptive Security Appliance Policy Controls

Lesson 1: Defining the Cisco ASA Adaptive Security Appliance MPF

- Cisco MPF Overview
- Configuring and Verifying Layer 3 and Layer 4 Policies
- Configuring and Verifying a Policy for Management Traffic

Lesson 2: Configuring Cisco ASA Adaptive Security Appliance Advanced Application Inspections

- 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

Lesson 3: Module Summary

Module 5: Cisco ASA Adaptive Security Appliance VPN Common Components

Lesson 1: VPN Overview

- VPN Definition
- Key Threats to WANs and Remote Access
- VPN Types
- VPN Components

Lesson 2: Implementing Profiles, Group Policies, and User Policies

- Cisco ASA VPN Policy Configuration
- Cisco ASA Adaptive Security Appliance Connection Profiles
- Cisco ASA Adaptive Security Appliance Group Policies

- Cisco ASA VPN AAA and External Policy Storage
- Cisco ASA Adaptive Security Appliance User Attributes
- Access Control Methods
- VPN Accounting Using External Servers
- DAP for SSL VPN

Lesson 3: Implementing PKI Services

- 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

Lesson 4: Module Summary

Module 6: Cisco Clientless VPN Solution

Lesson 1: Introducing Clientless SSL VPN

- 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

Lesson 2: Deploying Basic Cisco Clientless SSL VPN on the Cisco ASA Adaptive Security Appliance

- 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
- Verifying Basic Cisco Clientless SSL VPN
- Troubleshooting Basic Clientless SSL VPN Operations

Lesson 3: Deploying Application Access in Cisco Clientless SSL VPN

- 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

Lesson 4: Deploying Client-Side Authentication and Authorization in Clientless SSL VPN

- Client-Side Authentication Options
- Client-Side Authentication and Authorization Using AAA Server
- Double Client-Side Authentication Using AAA Servers
- Troubleshooting Client-Side AAA Authentication

Lesson 5: Module Summary

Module 7: Cisco AnyConnect Full Tunnel VPN Solutions

Lesson 1: Deploying Basic Cisco AnyConnect SSL VPN on Cisco ASA

- Basic Cisco AnyConnect SSL VPN
- SSL VPN Clients Authentication
- SSL VPN Client IP Address Assignment
- SSL VPN Split Tunneling
- Configuration Scenario
- Configuration Tasks
- Enable Cisco AnyConnect SSL VPNs
- Define IP Address Pool
- Configure Identity NAT
- Configure Group Policy
- Configure Group Policy: Split Tunneling
- Configure Connection Profile
- Monitor Cisco AnyConnect VPN on Client Endpoint
- Monitor Cisco AnyConnect VPN on Server

Lesson 2: Deploying Advanced Cisco AnyConnect SSL VPN on Cisco ASA

- 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

Lesson 3: Deploying Advanced Authentication and Authorization in Cisco AnyConnect VPNs

- 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 Prefill
- 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

Lesson 4: Deploying Cisco AnyConnect IPsec/IKEv2 VPNs

- Cisco 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 Appliance
- Verify and Troubleshoot Cisco AnyConnect IPsec VPN on Cisco ASA Appliance

Lesson 5: Module Summary

Module 8: Cisco ASA Adaptive Security Appliance High Availability and Virtualization

Lesson 1: Configuring Cisco ASA Adaptive Security Appliance Interface Redundancy Features

- Configuring and Verifying EtherChannel
- Configuring and Verifying Redundant Interfaces
- Troubleshooting EtherChannel and Redundant Interfaces

Lesson 2: Configuring Cisco ASA Adaptive Security Appliance Active/Standby High Availability

- Failover Overview
- Configuration Choices, Basic Procedures, and Required Input Parameters
- Configuring and Verifying Active/Standby Failover
- Tuning and Managing Active/Standby Failover
- Remote Command Execution
- Troubleshooting Active/Standby Failover

Lesson 3: Configuring Security Contexts on the Cisco ASA Adaptive Security Appliance

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

Lesson 4: Module Summary
Lesson 5: (OPTIONAL) Configuring Cisco ASA Adaptive Security Appliance Active/Active High Availability (Optional/Self-study)

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

**Lab Outline**

Lab 1-1: Accessing the Remote Lab Environment

Task 1: Access the Learning@Cisco-Hosted ASA Remote Lab
Lab 2-1: Configuring the Cisco ASA Adaptive Security Appliance
Task 1: Verify Cisco ASA Adaptive Security Appliance and Cisco ASDM Versions
Task 2: Initialize the Cisco ASA Adaptive Security Appliance from the CLI
Task 3: Launch Cisco ASDM and Test SSH Access
Task 4: Configure and Verify Interfaces
Task 5: Configure System Management Parameters
Lab 3-1: Configuring NAT
Task 1: Configure Object NAT for the Client Network and DMZ Server
Task 2: Configure Manual NAT for the DMZ Server and Client Network
Lab 3-2: Configuring Basic Cisco Access Control Features
Task 1: Troubleshoot Basic Connectivity
Task 2: Configure Network and Service Object Groups
Task 3: Configure Access Lists

Task 4: Configure Public Servers
Task 5: Configure Global Access Lists
Task 6: (Optional) Configure Unicast Reverse Path Forwarding Check

Lab 4-1: Configuring MPF, Basic Stateful Inspections, and QoS
Task 1: Configure ICMP and FTP Inspection
Task 2: Enable TTL Decrement and Disable TCP Initial Sequence Randomization
Task 3: Tune TCP Timeouts, Enable TCP DCD, and Configure TCP Normalization
Task 4: Configure a Priority Queue and Traffic Policing

Lab 4-2: Configuring MPF Advanced Application Inspections
Task 1: Configure HTTP Inspection to Protect the DMZ Server
Task 2: Configure FTP Inspection to Protect the DMZ Server
Task 3: Return the Cisco ASA Security Appliance to the Default Inspection Policies

Lab 6-1: Implementing Basic Clientless SSL VPN on the Cisco ASA
Task 1: Configure the Cisco ASA to Use DNS
Task 2: Enable Clientless SSL VPN Connections
Task 3: Provision an Identity Certificate for the Cisco ASA
Task 4: Configure Local User Authentication
Task 5: Configure Bookmarks and Access Control

Lab 6-2: Configuring Application Access for Clientless SSL VPN on the Cisco ASA
Task 1: Configure Application Access Using Plug-ins
Task 2: Configure Application Access Using Smart Tunnels

Lab 6-3: Implementing External Authentication and Authorization for Clientless SSL VPNs
Task 1: Configure External Authentication Using Microsoft Active Directory
Task 2: Configure External Authorization Using Microsoft Active Directory

Lab 7-1: Implementing Basic Cisco AnyConnect SSL VPN on the Cisco ASA
Task 1: Enable Cisco AnyConnect SSL VPN Connections
Task 2: Configure the VPN IP Address Pool and Identity NAT
Task 3: Configure a VPN User and Create a Connection Profile
Task 4: Configure Group Policy: IP Pool, DNS, and Split Tunneling
Task 5: Test Cisco AnyConnect SSL VPNs

Lab 7-2: Configuring Advanced Authentication for Cisco AnyConnect SSL VPNs
Task 1: Review LDAP and Active Directory Server Settings on the Cisco ASA
Task 2: Deploy Local Authorization for Local VPN Users
Task 3: Deploy External Authorization Using Microsoft Active Directory
Task 4: Deploy a Standalone Cisco AnyConnect Client on the Outside PC

Lab 7-3: Implementing Cisco AnyConnect IPsec/IKEv2 VPNs
Task 1: Deploy Cisco AnyConnect IPsec/IKEv2 VPN with WebLaunch

Lab 8-1: Configuring Active/Standby High Availability
Task 1: Prepare the Secondary Appliance for Failover Configuration via the CLI and Cisco ASDM
Task 2: Configure Active/Standby Failover
Task 3: Configure Standby IP Addresses on the Active Appliance and Test Failover
Task 4: Tune Active/Standby Failover
Task 5: Enable Stateful Active/Standby Failover