



# SASAA v2.0 Implementing Advanced ASA Security

Cisco Training

**Course Length:** 5

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

## Course Overview

This course provides updated training on the key features of the Cisco ASA, including the ASA FirePOWER Services Module and ASA Clustering.

The main changes in SASAA v2.0 compared to SASAA v1.2 include updating the ASA release to 9.4.1. Added new content in the student guide and a new lab to cover some of the new ASA 9.3 and 9.4.1 features, and added content in the student guide on the new ASA 5506-X, 5508-X, and 5516-X. Also made few minor edits in the other modules. The ASA FirePOWER Services Module coverage is still based on the FirePOWER 5.3.1 software version in SASAA v2.0. The optional modules, like the end of life ASA CX, has been removed in SASAA v2.0.

## Audience

Network engineers supporting Cisco ASA 9.x implementations

## Prerequisites

Implementing Core Cisco ASA Security (SASAC) v1.0 or equivalent knowledge of the Cisco ASA

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

Learn how to implement some of the ASA and ASA v features such as Identity Firewall, FirePOWER Services, ASA Cloud Web Security, Clustering and various ASA post 9.2.2 release new features.

## Outline

Module 1: Cisco ASA Product Family

Lesson 1: Introducing the Cisco ASA 5500-X Next-Generation Firewalls

- Cisco ASA 5500-X Series Next-Generation Firewalls
- Cisco ASA 5500-X Series SSDs
- Cisco ASA 5585-X Dual Firewall Support
- Cisco ASA 5506-X, 5508-X, and 5516-X Overview



- Cisco ASA NGE Support
- Cisco ASA FirePOWER Services, CWS, NGFW Services, IPS Modules Comparisons

#### Lesson 2: Introducing the Cisco ASAv

- ASAv Initial 9.2.1 Release Overview
- Deploy the ASAv OVF Template
- ASAv 9.3.2+ KVM Hypervisor Support
- ASAv Digitally Signed Image
- ASAv Management Options
- ASAv 9.3.2+ Smart Licensing
- Verify the ASAv VM Using the CLI
- Verify the ASAv VM Using the ASDM
- ASA 9.2.1 BGP IPv4 Support

#### Lesson 3: Implementing ASA 9.3 and 9.4.1 New Features

- ASA REST API Basics
- ASA ACL Forward Reference and ACL Manual Commit
- ASA CLI Config Backup and Restore
- ASA Policy Based Routing
- ASA Equal Cost Multiple Path Routing
- ASA NSF Support
- ASA 9.4.1+ VXLAN Support
- Other New ASA Features

#### Lesson 4: Introducing the Cisco ASASM

- Cisco ASASM Supported Platforms
- Cisco ASASM Performance Numbers
- Cisco ASASM Architecture
- Cisco ASASM Features Parity
- Cisco ASASM VLAN Interface

### Module 2: Cisco ASA Identity Firewall

#### Lesson 1: Describing the Cisco ASA Identity Firewall Solution

- Cisco ASA Identity Firewall Benefits
- Cisco ASA Identity Firewall Flow
- Cisco ASA Identity Firewall Policies



## Lesson 2: Setting Up Cisco CDA

- Cisco CDA versus Active Directory Agent
- Cisco CDA Hardware Appliance and VM Requirements
- Cisco CDA Installation
- Cisco CDA Setup
- Cisco CDA Application Status Verification
- Cisco CDA CLI Operations
- Cisco CDA GUI

## Lesson 3: Configuring Cisco CDA

- Active Directory Server Configuration
- Cisco ASA Configuration
- Syslog Server Configuration
- Cisco CDA User-Account Configuration
- Cisco CDA GUI Password Policy Configuration
- Cisco CDA Session Timeout Configuration
- IP-to-Identity Mapping Display
- Registered-Device Verification

## Lesson 4: Configuring Cisco ASA Identity Firewall

- Identity-Based Firewall Configuration Tasks
- Active Directory Server Configuration
- Cisco CDA Configuration
- User-Identity Options Configuration Using Cisco ASDM
- User-Identity Option Configuration Using the CLI
- User-Identity-Based Access Rules
- User Object Group Configuration
- FQDN Network Object Configuration
- Identity Firewall with Cut-Through Proxy Use Case
- Identity Firewall with Remote-Access VPN Use Case

## Lesson 5: Verifying and Troubleshooting Cisco ASA Identity Firewall

- Cisco CDA and Active Directory Server Connectivity Test
- Verify User-Identity Operations Using the CLI
- ASA to CDA Connectivity Verifications
- Active Directory Users Verifications
- Verify the Active Directory Groups



*"The Clever Advantage"*

- Memory Usage Verifications
- Identity-Based Firewall Cisco ASDM Monitoring Panes
- Cisco CDA Management with the CLI
- Cisco CDA Live Log Monitoring
- Cisco CDA Troubleshooting

### Module 3: Cisco ASA FirePOWER Services

#### Lesson 1: Installing the Cisco ASA FirePOWER Services Module

- Cisco ASA FirePOWER Services (SFR) Module Overview
- Cisco FireSIGHT Management Center Overview
- Cisco ASA FirePOWER Services Software Module Management Interface
- Cisco ASA FirePOWER Services Module Package Installation
- Cisco ASA FirePOWER Services Module Verification
- Redirect Traffic to Cisco ASA FirePOWER Services Module

#### Lesson 2: Managing the Cisco ASA FirePOWER Services Module Using the FireSIGHT Management Center

- FireSIGHT Management Center VM Installation and Setup
- FirePOWER Services Module and FireSIGHT License Requirements
- Add the FirePOWER Services Module into FireSIGHT
- FireSIGHT Policy Types Overview
- Task Status Monitoring
- System Policy Overview
- Health Policy Overview
- Objects Management Overview
- Network Discovery Overview
- Security Zones Overview
- Active Directory Integration Overview
- SourceFire User Agent Overview
- Access Control Policy Overview
- Intrusion Policy Overview
- FireSIGHT Recommended Rules Overview
- Intrusion Event Impact Levels Overview
- File Policy Overview
- Connection Events Monitoring
- Events Display Time Range
- Switch Workflow
- IPS Events Monitoring
- File Events Monitoring
- Users Monitoring
- Indication of Compromise Overview



*"The Clever Advantage"*

- Context Explorer
- Dashboards
- System Updates

### Lesson 3: Describing the Cisco ASA 5506-X, 5508-X, and 5516-X FirePOWER Services

- ASDM and FirePOWER On-Box FireSIGHT Manager
- ASA FirePOWER Dashboard, Reporting, and Status
- ASA FirePOWER Events Viewer
- Gather ASA FirePOWER Troubleshooting Information for Cisco TAC
- FirePOWER Licensing

## Module 4: Cisco ASA Cloud Web Security

### Lesson 1: Introducing Cisco ASA Cisco Cloud Web Security

- Cisco ASA with Cisco Cloud Web Security
- Cisco Cloud Web Security URL Filtering, AVC, and Reporting Features Overview
- Cisco Cloud Web Security Scanning Processes and Day Zero Outbreak Intelligence Overview
- Cisco ScanCenter
- Cisco ASA Cloud Web Security Licenses

### Lesson 2: Configuring Cisco ASA with Cisco Cloud Web Security

- Cisco ASA and Cloud Web Security Proxy-Server Configuration
- ScanCenter Generation of an Authentication Key for Cisco ASA
- Traffic Redirection from Cisco ASA to Cloud Web Security Proxy Servers
- Cisco ASA and Cloud Web Security Proxy Server User-Identity Configuration

### Lesson 3: Verifying Cisco ASA Cloud Web Security Operations

- Cisco ASA Cloud Web Security Operations Verification Using the CLI
- Cisco ASA Cloud Web Security Operations Verification by Using Cisco ASDM
- Verification of Traffic Redirection from Cisco ASA to Cloud Web Security Proxy Servers
- Cisco ASA Cloud Web Security Syslog Messages
- Cisco ASA Cloud Web Security Operations Verification Using Debug

### Lesson 4: Describing the Web Filtering Policy in Cisco ScanCenter

- ScanCenter Web Filtering Policy Overview



- ScanCenter Web Filtering Policy Configuration
- ScanCenter HTTPS Inspection Configuration Overview
- ScanCenter Web Filtering Reporting

#### Lesson 5: Describing Cisco ASA Cloud Web Security AMP and CTA

- Cisco ASA CWS Advanced Malware Protection Overview
- Cisco Cloud Web Security Cognitive Threat Analytics
- Cisco ASA Cloud Web Security ScanCenter Threats Reporting Overview

### Module 5: Cisco ASA Clustering

#### Lesson 1: Describing Cisco ASA Cluster Features

- Cluster Performance Figures and Supported Platforms
- Cluster Data-Interface Modes
- Cluster Data-Interface Connections
- CCL Functions
- Cluster Master and Slave Unit Election
- Centralized, Distributed, and Unsupported Cisco ASA Features
- Cluster Dynamic-Routing Operations
- Cluster NAT and PAT Operations

#### Lesson 2: Describing Cisco ASA Cluster Terminology and Data Flows

- Cluster Terminology
- TCP Sequence Number Randomization
- TCP Traffic Flows
- Asymmetric UDP Traffic Flows
- Short-Lived Traffic Flows
- Centralized-Feature Traffic Flows
- Traffic Flows with Secondary Connections
- TCP Flow Rebalancing
- Cluster Health-Check Mechanisms
- Clustering with Multi-Context

#### Lesson 3: Using the CLI to Configure a Cisco ASA Cluster

- Cluster Management
- Cluster Configuration with the CLI
- Cluster Interface-Mode Configuration on Each Unit
- CCL Configuration on Each Unit



- Cluster Management Interface Configuration from the Master Unit
- Spanned EtherChannel (Layer 2) Interface Configuration from the Master Unit
- Individual (Layer 3) Interface Configuration from the Master Unit
- Cluster Bootstrap Configuration and Enabling Clustering on Each Unit
- Sample Configuration of a Two-Unit Cluster with Spanned EtherChannel Interface
- Sample Configuration of a Two-Unit Cluster with Individual Interface
- Cluster Configuration Options

#### Lesson 4: Using the ASDM to Configure a Cisco ASA Cluster

- Cisco ASDM Cluster Dashboards
- Cluster Configuration Using Cisco ASDM
- Cisco ASDM High Availability and Scalability Wizard
- Cisco ASDM ASA Cluster Pane

#### Lesson 5: Verifying Cisco ASA Cluster Operations

- Cluster Licensing
- Cluster Interface-Mode Verification
- Cluster Member-Status Verification
- Cluster Health-Status Verification
- Cluster Connections State Table Verification
- Cluster EtherChannel Status Verification
- Cluster Aggregated ACL Hit-Count Verification
- Cluster Memory and CPU Usage Verification
- Cluster Traffic-Distribution Verification
- TCP Flow-Rebalancing Verification
- Cluster Operation Verification Using ASDM

#### Lesson 6: Troubleshooting Cisco ASA Cluster Operations

- Cluster Packet Captures
- Cluster Syslog Messages
- Cluster Debug
- Cluster Crashinfo and Coredump
- Split-Cluster Scenario

#### Lesson 7: Describing Cisco ASA Version 9.1.4 and Later Clustering Features

- More Switches Support for Clustering
- ASA 5500-X Clustering Support (v9.1.4+)



*"The Clever Advantage"*

- 16 Units Cluster with 32 Active Members Port Channel Support (v9.2.1+)
- BGP Support with Clustering (v9.3.1+)
- Cluster Selective Interface Monitoring Support (v9.4.1+)
- Individual Mode Inter-DC Clustering: Routed Firewall Mode Only (v9.1.4+)
- Extended Spanned EtherChannel for Inter-DC Clustering: Transparent Firewall Mode Only (v9.2.1+)
- Split Spanned EtherChannel Inter-DC Clustering: Transparent Firewall Mode Only (v9.2.1+)
- Inter-DC Redundancy with a Split Cluster

## Module 6: Cisco ASA Security Group Firewall and CoA

### Lesson 1: Introducing Cisco Security Group Tagging

- IEEE 802.1X Overview
- Cisco Secure Access Architecture

### Lesson 2: Configuring Cisco ASA Security Group Firewall

- SG Firewall Configuration
- SGACL Operations Monitoring

### Lesson 3: Describing the Cisco ASA 9.2.1 and Later Releases SGT Features

- Cisco ASA 9.2.1 SGT Support for VPN Users
- Cisco ASA 9.3.1 VPN Inline SGT Tagging Support
- Cisco ASA 9.3.1 Inline SGT Tagging Support
- Cisco ASA Inline SGT Tagging Configurations
- Lesson 4: Describing the Cisco ASA 9.2.1 and Later Releases CoA Support
  - RADIUS Change of Authorization Overview
  - ASA CoA Support Overview
  - ASA CoA CLI Configurations
  - ASA CoA ASDM Configurations

### Lab Outline

#### Lab 1: Cisco Learning Lab Remote Access

- Access the Learning@Cisco Hosted ASA Remote Lab

#### Lab 2: Cisco ASAv Basic Setup

- Setup and Test the ASAv



*"The Clever Advantage"*



### Lab 3: Cisco ASA 9.3 and 9.4.1 New Features

- REST API
- ACL Forward Reference
- ACL Manual Commit
- Policy Based Routing
- Equal Cost Multi Path Routing
- Reset the Inside PC Network Connectivity Through the ASA 5512-X Instead of the ASAv

### Lab 4: Cisco CDA Configuration

- Explore the Cisco CDA CLI
- Manage the Cisco CDA CLI User Accounts
- Explore the Cisco CDA GUI
- Configure the Cisco CDA to Communicate with the Active Directory Server, Cisco ASA, and Syslog Server

### Lab 5: Cisco ASA Identity-Based Firewall Configuration

- Configure the ASA to Communicate with the Active Directory Server
- Configure the ASA to Communicate with the CDA
- Configure ASA User-Identity Options
- Configure ASA Identity-Based Access Rules

### Lab 6: Cisco ASA FirePOWER Services Module Installation

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

### Lab 7: Cisco FireSIGHT Management Center Configuration

- Add the ASA FirePOWER Services Module in the Cisco FireSIGHT Management Center
- Edit the Default FireSIGHT Network Discovery Rule
- Configure the File Policy, Intrusion Policy, and Access Control Policy
- Test ASA FirePOWER Basic IPS Operations
- Test ASA FirePOWER Basic AMP Operations
- Examine the FireSIGHT Network Discovery Results
- Integrate FireSIGHT with Microsoft Active Directory
- Setup and Test User Based Access Control Policy
- Verify the Traffic Redirection to the ASA FirePOWER Services Module



*"The Clever Advantage"*

- Disable Traffic Redirection to the ASA FirePOWER Services Module
- Shut Down and Uninstall the ASA FirePower Services Module

#### Lab 8: Cisco ASA Cloud Web Security Configuration

- Configure the Cisco ASA-to-Cloud Web Security Integration

#### Lab 9: Cisco ASA Cluster Configuration

- Configure Spanned EtherChannel Mode on Each ASA in the Cluster (Pod X ASA and Pod X+1 ASA)
- Configure the Cluster Hostname on the Pod X ASA Only
- Configure the CCL Using a Local EtherChannel on Each ASA in the Cluster (Pod X ASA and Pod X+1 ASA)
- Configure the Management Interface in Individual (Layer 3) Mode on the Pod X ASA Only
- Configure the (Inside and Outside) Data Interfaces in Spanned EtherChannel (Layer 2) Mode on the Pod X ASA Only
- Configure the Cluster Bootstrap Configurations on Each ASA in the Cluster (Pod X ASA and Pod X+1 ASA)
- Enable Clustering on the Pod X ASA Only
- Enable Clustering on the Pod X+1 ASA
- Verify and Manage the Cluster Operations Using the CLI
- Verify the Cluster Operations Using the ASDM
- Verify HTTP Connections Through the Cluster and Identify the Owner and Director of a Flow
- Enable ICMP Inspection from the Master Unit
- Simulate a Master Unit Failure and Observe the Results
- Disable the Cluster

To register or for more information call our office **(208) 898-9036** or email [register@leapfoxlearning.com](mailto:register@leapfoxlearning.com)



*"The Clever Advantage"*