IMPLEMENTING ADVANCED CISCO ASA SECURITY (CI-SASAA)

This subtopic provides an overview of how the course is organized. The course contains these components:

• Module 1: Cisco ASA Product Family
• Module 2: Cisco ASA Identity Firewall
• Module 3: Cisco ASA FirePOWER Services
• Module 4: Cisco ASA Cloud Web Security
• Module 5: Cisco ASA Clustering
• Module 6: Cisco ASA Security Group Firewall and CoA
• Lab 1: Cisco Learning Lab Remote Access
• Lab 2: Cisco ASAv Basic Setup
• Lab 3: Cisco ASA 9.3 and 9.4.1 New Features
• Lab 4: Cisco CDA Configuration
• Lab 5: Cisco ASA Identity-Based Firewall Configuration
• Lab 6: Cisco ASA FirePOWER Services Module Installation
• Lab 7: Cisco FireSIGHT Management Center Configuration
• Lab 8: Cisco ASA Cloud Web Security Configuration
• Lab 9: Cisco ASA Cluster Configuration

Course Introduction

The Course Introduction provides learners with the course objectives and prerequisite learner skills and knowledge. The Course Introduction presents the course flow diagram and the icons that are used in the course illustrations and figures. This course component also describes the curriculum for this course, providing learners with the information that they need to make decisions regarding their specific learning path.
• Overview
• Course Goal and Objectives
• Course Flow
• Additional References
• Your Training Curriculum

Module 1: Cisco ASA Product Family

Objective: Describe the Cisco ASA 5500-X Series Next-Generation Firewalls, ASAv, ASA 5506-X, 5508-X, 5516-X, ASASM and implement new ASA 9.4.1 features.

Lesson 1: Introducing the Cisco ASA 5500-X Next-Generation Firewalls
Objective: Describe the Cisco ASA 5500-X Series of next-generation, midrange platforms and the Cisco ASA 5585-X dual firewall mode
This lesson includes these topics:
• 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

Lab 1: Cisco Learning Lab Remote Access
This activity includes these tasks:
• Access the Learning@Cisco Hosted ASA Remote Lab

Lesson 2: Introducing the Cisco ASAv
Objective: Describe the Virtual Cisco ASA (ASAv).
This lesson includes these topics:
• 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

Lab 2: Cisco ASAv Basic Setup
This activity includes these tasks:
• Setup and Test the ASAv

Lesson 3: Implementing ASA 9.3 and 9.4.1 New Features
Objective: Describe some of the other new ASA 9.3 features.
This lesson includes these topics:
• 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

Lab 3: Cisco ASA 9.3 and 9.4.1 New Features
This activity includes these tasks:
• 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

Lesson 4: Introducing the Cisco ASASM
Objective: Describe the Cisco ASASM
This lesson includes these topics:
• 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

Objective: Implement Cisco ASA Identity Firewall policies
Lesson 1: Describing the Cisco ASA Identity Firewall Solution
Objective: Describe the Cisco ASA Identity Firewall feature
This lesson includes these topics:
• Cisco ASA Identity Firewall Benefits
• Cisco ASA Identity Firewall Flow
• Cisco ASA Identity Firewall Policies

Lesson 2: Setting Up Cisco CDA
Objective: Set up the basic network configurations in Cisco CDA
This lesson includes these topics:
• 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
Objective: Configure Cisco CDA to integrate with the Active Directory server, Cisco ASA, and syslog server
This lesson includes these topics:
• 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
Lab 4: Cisco CDA Configuration
This activity includes these tasks:
• 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

Lesson 4: Configuring Cisco ASA Identity Firewall
Objective: Configure the Identity Firewall policies on Cisco ASA
This lesson includes these topics:
• 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
Objective: Verify and troubleshoot Identity Firewall operations
This lesson includes these topics:
• 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
• Memory Usage Verifications
• Identity-Based Firewall Cisco ASDM Monitoring Panes
• Cisco CDA Management with the CLI
• Cisco CDA Live Log Monitoring
• Cisco CDA Troubleshooting

Lab 5: Cisco ASA Identity-Based Firewall Configuration
This activity includes these tasks:
• 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

Module 3: Cisco ASA FirePOWER Services

Objective: Install and set up the Cisco FirePOWER Services Module (SFR)
Lesson 1: Installing the Cisco ASA FirePOWER Services Module
Objective: Install the Cisco ASA FirePOWER Services Module and redirect traffic to it.
This lesson includes these topics:
• 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

Lab 6: Cisco ASA FirePOWER Services Module Installation
This activity includes these tasks:
• Install and Set Up the ASA FirePower (SFR) Services Module
• Redirect Traffic to the ASA FirePOWER Services Module

Lesson 2: Managing the Cisco ASA FirePOWER Services Module Using the FireSIGHT Management Center
Objective: Manage the ASA FirePOWER Services Module using the FireSIGHT Management Center.
This lesson includes these topics:
• 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
• Context Explorer
• Dashboards
• System Updates

Lab 7: Cisco FireSIGHT Management Center Configuration
This activity includes these tasks:
• Add the ASA FirePOWER Services Module in the Cisco FireSIGHT Management Center
• Edit the Default FreSIGHT 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
• Disable Traffic Redirection to the ASA FirePOWER Services Module
• Shut Down and Uninstall the ASA FirePower Services Module

Lesson 3: Describing the Cisco ASA 5506-X, 5508-X, and 5516-X FirePOWER Services
Objective: Describe the ASA 5506-X and 5508-X FirePOWER Services.
This lesson includes these topics:
• 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

Objective: Implement Cisco ASA Cloud Web Security.
Lesson 1: Introducing Cisco ASA Cisco Cloud Web Security
Objective: Describe the Cisco Cloud Web Security feature in Cisco ASA
This lesson includes these topics:
• 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
Objective: Configure Cisco ASA to integrate with Cisco Cloud Web Security
This lesson includes these topics:
• 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
Objective: Verify Cisco ASA Cisco Cloud Web Security operations
This lesson includes these topics:
• 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
Objective: Describe basic web filtering policy configurations in Cisco ScanCenter
This lesson includes these topics:
• 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
Objective: Describe Cisco Cloud Web Security Advanced Malware Protection and Threat Analytics
This lesson includes these topics:
• Cisco ASA CWS Advanced Malware Protection Overview
• Cisco Cloud Web Security Cognitive Threat Analytics
• Cisco ASA Cloud Web Security ScanCenter Threats Reporting Overview

Lab 8: Cisco ASA Cloud Web Security Configuration

This activity includes these tasks:
• Configure the Cisco ASA-to-Cloud Web Security Integration

Module 5: Cisco ASA Clustering

Objective: Implement Cisco ASA Clustering
Lesson 1: Describing Cisco ASA Cluster Features
Objective: Describe a Cisco ASA cluster
This lesson includes these topics:
• 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
Objective: Explain Cisco ASA cluster operations and traffic flows
This lesson includes these topics:
• 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
Objective: Configure a Cisco ASA cluster using the CLI
This lesson includes these topics:
• 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
Objective: Configure a Cisco ASA cluster using Cisco ASDM
This lesson includes these topics:
• 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
Objective:
This lesson includes these topics:
• 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
Objective: Troubleshoot Cisco ASA Cluster operations
This lesson includes these topics:
• 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
Objective:
This lesson includes these topics:
• More Switches Support for Clustering
• ASA 5500-X Clustering Support (v9.1.4+)
• 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+)
• Spilt Spanned EtherChannel Inter-DC Clustering: Transparent Firewall Mode Only (v9.2.1+)
• Inter-DC Redundancy with a Split Cluster

Lab 9: Cisco ASA Cluster Configuration
This activity includes these tasks:
• 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

Module 6: Cisco ASA Security Group Firewall and CoA

Objective: Describe Cisco ASA Security Group Firewall and Change of Authorization Support
Lesson 1: Introducing Cisco Security Group Tagging
Objective: Describe the Cisco Secure Access architecture
This lesson includes these topics:
• IEEE 802.1X Overview
• Cisco Secure Access Architecture

Lesson 2: Configuring Cisco ASA Security Group Firewall
Objective: Describe Cisco ASA SGACL configurations
This lesson includes these topics:
• SG Firewall Configuration
• SGACL Operations Monitoring

Lesson 3: Describing the Cisco ASA 9.2.1 and Later Releases SGT Features
Objective: Describe the Cisco ASA post 9.0 release new SGT features.
This lesson includes these topics:
• 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
Objective: Describe Cisco ASA 9.2.1 and later releases Change of Authorization support
This lesson includes these topics:
• RADIUS Change of Authorization Overview
• ASA CoA Support Overview
• ASA CoA CLI Configurations
• ASA CoA ASDM Configurations