

SASAA (IMPLEMENTING ADVANCED CISCO ASA SECURITY)

Objetivo

Este curso oferece uma formação atualizada sobre as principais características avançadas do Cisco ASA NGFW. Os profissionais ao participarem desse curso serão capazes de: Explicar as características do Cisco ASA 5500-X Series Next-Generation Firewalls, ASASM (Service Module 7600/6500) e Cisco ASAV (Virtualizado); Instalar e configurar produto Cisco ASAV (Virtualizado); Implantar políticas de controle através do recurso denominado "Firewall de Identidade", usando Cisco ASA e Cisco CDA; Instalar e configurar o Módulo SFR Cisco (Firepower Services) e o gerenciamento pelo FireSight; Configurar as novas características como PBR (PolicyBasedRouting), ECMP (Equal Cost Multiple Path Routing) dentre outras; Implantar a integração entre o Cisco ASA e serviço em nuvem Cisco Cloud Web Security; Implantar uma solução em alta disponibilidade utilizando Cisco ASA Cluster; Descrever o suporte do ASA em CoA.

Público Alvo

Este curso é indicado aos profissionais que buscam uma atualização das novas características e aprimoramentos proporcionados ao Cisco Firewall ASA, através da versão de IOS 9.x.

Pré-Requisitos

Para aproveitar ao máximo este curso, é recomendável que os alunos possuam: Conhecimentos básicos do Cisco ASA NFGW, que pode ser obtido pelo curso Firewall 1.0/2.0, ou SAEXS; Conhecimentos básicos em segurança; Conhecimentos básicos em rede; Conhecimento do sistema operacional Microsoft Windows

Carga Horária

40 horas (5 dias).

Conteúdo Programático

- Cisco ASA Product Family
- Cisco ASA 5500-X NGFW
- 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 and IPS

- Introducing the Cisco ASAv
- ASAv Overview

- Deploy ASAv OVF Template
- ASAv KVM Hypervisor Support
- ASAv Digitally Signed Image
- ASAv Management Options
- ASAv Smart Licensing
- Verify ASAv VM using CLI
- Verify ASAv VM using ASDM
- ASAv BGP IPv4 Support

- Implementing ASA 9.3 and 9.4 New Features
- ASA REST API Basics
- ASA ACL Forward Reference and ACL Manual Commit
- ASA CLI Config Backup and Restore
- ASA Policy Based Routing (PBR)
- ASA Equal Cost Multiple Path Routing (ECMP)
- ASA NSF Support
- ASA 9.4.1 VXLAN Support
- Other New Features

- Introducing the Cisco ASASM
- Cisco ASASM Support Platforms
- Cisco ASASM Performance Numbers
- Cisco ASASM Architecture
- Cisco ASASM Features Parity
- Cisco ASASM VLAN Interfaces

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

- 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 Verifications
- Cisco CDA CLI Operations
- Cisco CDA GUI

- 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 Configurations
- IP-To-Identity Mapping Display

Registered-Device Verification

- Configuring Cisco ASA Identity Firewall
- Identity-Based Firewall Configurations Tasks
- Active Directory Server Configuration
- Cisco CDA Configuration
- User Identity Options Configuration Using Cisco ASDM
- User Identity Options 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

- Verify and Troubleshooting Cisco ASA Identity Firewall
- Cisco CDA and Active Directory Server Connectivity Test
- Verify User Identity Operations the CLI
- ASA to CDA Coneectivity 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

- 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 Interfaces
- Cisco ASA FirePower Services Module Package Installation
- Cisco ASA FirePower Services Module Verification
- Redirect Traffic to Cisco ASA FirePower Services Module

- Managing Cisco ASA Firepower using 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
- Context Explorer
- Dashboards
- System Updates

- 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

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

- Configuring Cisco with Cisco Cloud Web Security
- Cisco ASA and Cloud Web Security Proxy-Server Configurations
- 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

- Verifying Cisco ASA Cloud Web Security Operations
- Cisco ASA Cloud Web Security Operations Verification Using the CLI
- Cisco ASA Cloud Web Security Operations Verification Using the 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

- 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

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

Describing Cisco ASA Clustering 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

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

Using the CLI to Configure a Cisco ASA Clustering
Cluster Management
Cluster Configuration with the CLI
Cluster Interface Mode Configuration on Each Unit
CCL Configuration on Each Unit
Cluster Management Interface Configuration from Master Unit
Spanned EtherChannel (Layer 2) Interface Configuration from Master Unit
Individual (Layer 3) Interface Configuration from Master Unit
Cluster Bootstrap Configuration and Enabling Clustering on Each Unit
Sample Configuration of a Two Unit Cluster with Spanned EtherChannel
Sample Configuration of a Two Unit Cluster with Individual Interface
Cluster Configuration Options

Using ASDM to Configure a Cisco ASA Clustering
Cisco ASDM Cluster Dashboards
Cluster Configuration Using Cisco ASDM
Cisco ASDM High Availability and Scalability Wizard
Cisco ASDM ASA Cluster Pane

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 Traffic Distribution Verification
- TCP Flow Rebalancing Verification
- Cluster Operation Verification Using ASDM

- Troubleshooting Cisco ASA Cluster Operations
- Cluster Packets Captures
- Cluster Syslog Messages
- Cluster Debug
- Cluster CrashInfo and Coredump
- Split Cluster Scenario

- Describing Cisco ASA Version 9.1.4 and Later Clustering Features
- More Switches Support Clustering
- ASA 5500-X Clustering Support (9.1.4)
- 16 Units Cluster with 32 Active Members Port Channel Support (9.2.1)
- BGP Support with Clustering (9.3.1)
- Cluster Selective Interface Monitoring Support (9.4.1)
- Individual Mode Inter-DC Clustering Routed Firewall Mode Only (9.1.4)
- Extended Spanned EtherChannel for Inter-DC Clustering, Transparent Firewall Mode Only (9.2.1)
- Split Spanned EtherChannel Inter-DC Clustering, Transparent Firewall Mode Only (9.2.1)
- Inter-DC Redundancy with a Split Clustering

- Introducing Cisco Security Group Tagging
- IEEE 802.1X Overview
- Cisco Secure Access Architecture

- Configuring Cisco ASA Security Group Firewall
- SG Firewall Configuration
- SG ACL Operations Monitoring

- Describing 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

- Describing Cisco ASA 9.2.1 and Later Releases CoA Supported
- Radius Change of Authorization Overview
- ASA CoA Support Overview
- ASA CoA CLI Configurations
- ASA CoA ASDM Configurations

LABS

Lab 1 Cisco ASAv Basic Setup
Setup and Test ASAv

Lab 2 Cisco ASA 9.3 and 9.4.1 New Features
Include these Tasks
REST API
ACL Forward Reference
ACL Manual Commit
Policy Based Routing
Equal Cost Multi Path Routing

Lab 3 Cisco CDA Configuration
Include these Tasks
Explore Cisco CDA CLI
Manage Cisco CDA CLI User Accounts
Explore Cisco CDA GUI
Configure Cisco CDA to Communicate with Active Directory Server, Cisco ASA and Syslog Server

Lab 4 Cisco Identity Based Firewall Configurations
Include these Tasks
Configure ASA to Communicate with Active Directory Server
Configure ASA to Communicate with CDA
Configure ASA User Identity Options
Configure ASA Identity Access Rules

Lab 5 Cisco ASA FirePower Services Module Installation
Include these tasks
Install and Set Up ASA Firepower (SFR) Services Modules
Redirect Traffic to ASA Firepower Services Module

Lab 6 Cisco FireSight Management Center Configuration
Include these tasks:
Add ASA Firepower Services Module in FireSight Management Center
Edit Default FireSight Network Discovery Rule
Configure File Policy, Intrusion Policy and Access Control Policy
Test ASA FirePower Basic IPS Operations
Test ASA FirePower Basic AMP Operations
Examine FireSight Network Discovery Results
Integrate FireSight with Microsoft Active Directory
Setup and Test User Based Access Control Policy
Verify the Traffic Redirection to ASA FirePower Services Module
Disable Traffic Redirection to ASA FirePower Services Module
Shut Down and Uninstall ASA FirePower Services Module

Lab 7 Cisco ASA Cloud Web Security Configuration
Include these tasks

Configure Cisco ASA to Cloud Web Security Integration

Lab 8 Cisco ASA Cluster Configuration

Include these tasks

Configure Spanned EtherChannel Mode on Each ASA

Configure Cluster Hostname

Configure CCL Using Local EtherChannel on Each ASA

Configure The Management Interface In Individual (Layer 3)

Configure The (Inside and Outside) Data Interfaces Spanned EtherChannel (Layer 2)

Configure The Cluster Bootstrap Configurations on Each ASA in Clustering

Verify and Manage Cluster Operations

Verify Cluster Operations Using ASDM

Verify HTTP Connections Through Cluster

Enable ICMP Inspections Form Master Unit

Simulate Master Unit Failure

Disable Cluster