CISCO - ASA ESSENTIALS 3.0

Code: ASAE-30

Length: 5 days

Gain the essential skills required to configure, maintain, and operate Cisco ASA 5500 Series Adaptive Security

Appliances based on ASA Software v9.x. If you need to get up to speed quickly with Cisco's Adaptive Security

Appliance (ASA), this is the course for you. We combined the most important content from Cisco's Authorized FIREWALL v2.0 and VPN v2.0 courses and added additional information on the new features in v9.x software to hone in on the most crucial aspects of the ASA. In just one week, students will cover: Firewall Basics, Network Address Translation (NAT), Access Control Lists (ACLs), Object Groups, Stateful Inspection, Modular Policy

Framework, PKI Integration, Site-to-site and Remote Access VPN (both IPsec and SSL), Active/Standby Failover,

Server-based Authentication, Authorization, and Accounting (AAA) using ACS 5.2 and Cisco Identity Services Engine (ISE). Students will complete their training with high availability failover coverage, including an exclusive demonstration of what happens to firewall connections and VPN sessions during a device failure.

SKILLS GAINED

- Technology and features of the Cisco ASA
- Cisco ASA product family
- How ASAs protect network devices from attacks
- Bootstrap the security appliance
- Prepare the security appliance for configuration via the Cisco Adaptive Security Device Manager (ASDM) • Launch and navigate ASDM
- Essential security appliance configuration using ASDM and the command-line interface (CLI)
- Configure dynamic and static address translations
- Configure access policy based on ACLs
- Use object groups to simplify ACL complexity and maintenance
- Use the Modular Policy Framework to provide unique policies to specific data flows
- Handle advanced protocols with application inspection
- Troubleshoot with syslog and tcp ping
- Configure the ASA to work with Cisco Secure ACS 5.2 for RADIUS-based AAA of VPNs
- Basics of Identity Services Engine (ISE) integration
- Implement site-to-site IPsec VPN
- Implement remote access IPsec and SSL VPNs using the Cisco AnyConnect 3.0 Secure Mobility Client
- Work with the 5.x Legacy Cisco IPsec VPN client
- Deploy clientless SSL VPN access, including smart tunnels, plug-ins, and web-type ACLs
- Configure access control policies to implement your security policy across all classes of VPN
- Configure Active/Standby failover for both firewall and VPN high availability

WHO CAN BENEFIT

- Network administrators, managers, and coordinators
- Anyone who requires fundamental training on the ASA
- Security technicians, administrators, and engineers

CISCO - ASA ESSENTIALS 3.0

PREREQUISITES

It is recommended that prior to taking this course, students have successfully completed the following: IINS v2.0 - Implementing Cisco IOS Network Security

COURSE DETAILS

MODULE 1: CISCO ASA ESSENTIALS

- Lesson 1: Evaluating Cisco ASA Technologies
- Lesson 2: Identifying Cisco ASA Families

MODULE 2: BASIC CONNECTIVITY AND DEVICE MANAGEMENT

- Lesson 1: Preparing the Cisco ASA for Network Integration
- Lesson 2: Managing Basic Cisco ASA Network Settings
- Lesson 3: Configuring Cisco ASA Device Management Features

MODULE 3: NETWORK INTEGRATION

- Lesson 1: Configuring Cisco ASA NAT Features
- Lesson 2: Configuring Cisco ASA Basic Access Control Features

MODULE 4: CISCO ASA POLICY CONTROL

1. Lesson 1: Cisco ASA Modular Policy Framework
2. Lesson 2: Configuring Cisco ASA Connection Policy

MODULE 5: CISCO ASA VPN ARCHITECTURE AND COMMON COMPONENTS

- Lesson 1: Implementing Profiles, Group Policies, and User Policies
- Lesson 2: Implementing PKI Services

MODULE 6: CISCO ASA CLIENTLESS REMOTE ACCESS SSL VPN SOLUTIONS

- Lesson 1: Deploying Basic Clientless VPN Solutions
- Lesson 2: Deploying Advanced Application Access for Clientless SSL VPNs

MODULE 7: CISCO ANYCONNECT REMOTE ACCESS SSL SOLUTIONS

- Lesson 1: Deploying a Basic Cisco AnyConnect Full-Tunnel SSL VPN Solution

MODULE 8: CISCO ASA REMOTE ACCESS IPSEC VPNS

- Lesson 1: Deploying Cisco Remote Access VPN Clients
- Lesson 2: Deploying Basic Cisco Remote Access IPsec VPN Solutions

MODULE 9: CISCO ASA SITE-TO-SITE IPSEC VPN SOLUTIONS

- Lesson 1: Deploying Basic Site-to-Site IPsec VPNs
- Lesson 2: Deploying Advanced Site-to-Site IPsec VPNs

CISCO - ASA ESSENTIALS 3.0

MODULE 10: CISCO ASA HIGH AVAILABILITY AND VIRTUALIZATION

- Lesson 1: Configuring Cisco ASA Active/Standby High Availability

LAB OUTLINE

- Lab 1: Prepare the ASA for Administration
- Lab 2: Fundamental ASA Configuration
- Lab 3: Network Address Translation (NAT)
- Lab 4: Basic Access Control
- Lab 5: Basic Protocol Inspection
- Lab 6: Licensing, ACS, and Public CA
- Lab 7: Basic Clientless SSL VPN
- Lab 8: Clientless SSL VPN - Thin Apps
- Lab 9: Basic AnyConnect Full Tunnel SSL VPN
- Lab 10: Remote Access IPSec VPN
- Lab 11: IPSec Site-to-Site VPN
- Lab 12: Active/Standby Failover