FIREFLY

CONTACT US

Implementing Core Cisco ASA Security

DURATION: 5 DAYS COURSE CODE: SASAC FORMAT: LECTURE/LAB

COURSE DESCRIPTION

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

Offers hands-on labs

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.

WHO SHOULD ATTEND

Network engineers supporting Cisco ASA 9.x implementations

PREREQUISITES

The knowledge and skills that a learner must have before attending this course are as follows: FIREWALL v1.0 or FIREWALL v2.0 or an equivalent knowledge of the Cisco ASA

LEARNING OBJECTIVES

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

COURSE OUTLINE

1. Cisco ASA Adaptive Security Appliance Essentials
   - Evaluating Cisco ASA Adaptive Security Appliance Technologies
   - Identifying Cisco ASA Adaptive Security Appliance Models
   - Identifying Cisco ASA Adaptive Security Appliance Licensing Options
2. Basic Connectivity and Device Management
   - Preparing the Cisco ASA Adaptive Security Appliance for Network Integration
   - Managing Basic Cisco ASA Adaptive Security Appliance Network Settings
3. Network Integration
   - Configuring Cisco ASA Adaptive Security Appliance NAT Features
   - Configuring Cisco ASA Adaptive Security Appliance Access Control Features
   - Configuring Cisco ASA Adaptive Security Appliance Routing Features
4. Cisco ASA Adaptive Security Appliance Policy Controls
   - Defining the Cisco ASA Adaptive Security Appliance MPF
   - Configuring Cisco ASA Adaptive Security Appliance Advanced Application Inspections
5. Cisco ASA Adaptive Security Appliance VPN Common Components
   - VPN Overview
   - Implementing Profiles, Group Policies, and User Policies
   - Implementing PKI Services
6. Cisco Clientless VPN Solutions
   - Introducing Clientless SSL VPN
   - Deploying Basic Cisco Clientless SSL VPN on Cisco ASA
   - Deploying Application Access in Cisco ASA Clientless SSL VPN
   - Deploying Client-side Authentication and Authorization in Clientless SSL VPN
7. Cisco AnyConnect Full Tunnel VPN Solution
   - Deploying Basic Cisco AnyConnect
   - Deploying Advanced Cisco AnyConnect SSL VPN on Cisco ASA
   - Deploying Advanced Authentication and authorization in Cisco AnyConnect VPNs SSL VPN on Cisco ASA
   - Deploying Cisco AnyConnect IPsec/ IKEv2 VPNs
8. Cisco ASA Adaptive Security Appliance High Availability and Virtualization
   - Configuring Cisco ASA Interface Redundancy Features
   - Configuring Cisco ASA Active/Standby High Availability
   - Configuring Security Contexts on the Cisco ASA

DISCOVERY LABS

1: Accessing the Remote Lab Environment
2: Configuring the Cisco ASA Adaptive Security Appliance
3: Configuring NAT
4: Configuring Basic Cisco Access Control Features
5: Configuring MPF, Basic Stateful Inspections, and QoS
6: Configuring MPF Advanced Application Inspections
7: Implementing Basic Clientless SSL VPN on the Cisco ASA
8: Configuring Application Access for Clientless SSL VPN on the Cisco ASA
9: Implementing External Authentication and Authorization for Clientless SSL VPNs
10: Implementing Basic Cisco AnyConnect SSL VPN on the Cisco ASA
11: Configuring Advanced Authentication for Cisco AnyConnect SSL VPNs
12: Implementing Cisco AnyConnect IPsec/IKEv2 VPNs
13: Configuring Active/Standby High Availability