CISCO ASA TRAINING

UPGRADE YOUR KNOWLEDGE

Cisco ASA Training

Course Overview

The Cisco ASA firewall course aims to provide practical skills on security mechanisms, their configuration and troubleshooting in enterprise environments. This course is intended for networking professionals with little experience in Cisco products and technology.

Duration & Module Coverage

Duration: 8 Days (16hrs)

Session Options	Module Coverage
Session Weekdays[4] : 2 hours per day 4 days per week **Session Weekends:** 2 hours per day	**Day 1 - Modules 1** **Day 2 - Module 2** **Day 3 - Module 3** **Day 4 - Module 4** **Day 5 - Module 5** **Day 6 – Module 6** **Day 7 – Module 7** **Day 8 – Module 8**

Learning Goals

By the end of this course participants will be able to:

1. Demonstrate knowledge of the Cisco ASA Firewalls.
2. Understand security technologies used in Cisco ASA Firewall Devices.
3. Configuration and troubleshooting skills of related platforms.

Pre-Requisites

This course is for security professionals looking to work in a Cisco ASA environment. Understanding of basic networking and security is a pre-requisite to attend this training.

Teaching Methodology

This is a very hands-on course where participants carry out practical exercises according to the lab guide provided. The concepts are taught through implementation of real-world use-cases. Our exercises have been carefully designed to replicate scenarios participants will face in real life work conditions.

Who Should Take This Course?

This course is designed for security professionals with knowledge of basic networking looking forward to gain understanding of security technologies offered by Cisco ASA Firewalls and configuration and troubleshooting of related platforms.

Course Content

1. **Introducing ASA**
   - What does a firewall do?
   - Security Appliance Overview
   - Models and features of Cisco Security Appliances
   - Licensing of ASA

2. **Initial Configuration**
   - User Interface
   - File Management
   - Security Appliance security levels
   - ASDM overview and requirements
   - Navigating ASDM windows

3. **ASA Management Features**
   - Basic settings and password encryption
   - Enabling Management Access Methods
   - Authentication, Authorization and Accounting [AAA]
   - Privilege levels and Local User Database
   - Packet Tracer
   - Managing ASA configuration and images

4. **Access Control List and Network Address Translation on ASA 8.2 and 8.4**
   - Interface ACL
   - Global ACL
   - Time Based ACL
   - Object Groups
   - Static and Dynamic NAT
   - Port Address Translation
   - NAT Exemption
   - Auto NAT and Manual NAT

5. **Routing on Cisco ASA**
   - Static Routing
   - EIGRP on ASA
   - OSPF on ASA
   - ASA Multicast Routing Support

6. **Advanced Network Protection**
   - Blocking and Threat level
   - Black list and white list
   - Dynamic Database Updates
   - DNS Inspection

7. **Virtual Private Networks**
   - Encryption, authentication and hashing algorithms
   - IKE Phase 1 and Phase 2
   - Configure IPSec Site-to-Site VPNs
   - Configure Cisco ANYCONNECT VPN
   - Create SSL Web based VPN

8. **High Availability**
   - Implement Stateful ASA Failover
   - Active/Standby Mode
   - Active/Active Mode
   - Dynamic Routing Protocol Failover

Practical Learning Exercises

A lab guide will be provided to each student with requirement scenarios. Along with lab guide required VMs will be provided to set up individual labs for self practice.

A sample scenario would consist of one interface of Cisco ASA appliance connected to internal network, one interface connected to Server farm and one interface connected to the internet.

Similarly there would be scenarios for implementing, verifying and troubleshooting all modules covered in the course.