



**CTREC
HILTON**
IT ACADEMY

BUILDING TRAINING SOLUTIONS
FOR THE IT WORLD

Deploying Cisco ASA Firewall Features 1.0 (FIREWALL)

Days: 5
Format: Instructor-Led
Class Code: FIREWALL

Recommended Course Sequence

Knowledge of prerequisites
noted below.

*Course content is subject to change
without notice.*

Course Description:

The Deploying Cisco ASA Firewall Features (FIREWALL) 1.0 course is a five-day course that aims at providing network security engineers with the knowledge and skills needed to implement and maintain Cisco ASA adaptive security appliance-based perimeter solutions. Successful graduates will be able to reduce risk to the IT infrastructure and applications using Cisco ASA adaptive security appliance features, and provide detailed operations support for the Cisco ASA adaptive security appliance.

Target Student:

This course is intended for:

- Network Security Engineers (NSEs)
- Anyone that currently has their CCNA Security and/or is working towards CCNP Security certification.

Prerequisites:

To fully benefit from this course, students should have the following prerequisite skills and knowledge:

- Working knowledge of the Microsoft Windows operating system
- Knowledge attained from attending

At Course Completion:

After completing this course, students will be able to...

- Evaluate the basic technology, features, and hardware models of the Cisco ASA adaptive security appliance product line
- Implement and maintain basic Cisco ASA adaptive security appliance connectivity and device management plane features
- Implement and maintain data plane access control features of the Cisco ASA adaptive security appliance product family
- Implement and maintain Cisco ASA adaptive security appliance features that integrate it with the local and global routing and switching infrastructure
- Implement and maintain Cisco ASA adaptive security appliance virtualization and high availability features
- Evaluate Cisco ASA adaptive security appliance SSM modules, their major features, and integrate them with the Cisco ASA adaptive security appliance

Deploying Cisco ASA Firewall Features 1.0 (FIREWALL)

Course Outline

Module 1: Introduction to the Cisco ASA Adaptive Security Appliance

Lesson 1: Introducing Cisco ASA Adaptive Security Appliance Technology and Features
<ul style="list-style-type: none">■ Firewalls and Security Domains■ Firewall Technologies■ Overview of Cisco ASA Adaptive Security Appliance Features■ Common Cisco ASA Adaptive Security Appliance Use Cases
Lesson 2: Introducing the Cisco ASA Adaptive Security Appliance Family
<ul style="list-style-type: none">■ Cisco ASA Adaptive Security Appliance Platforms and Models■ Cisco ASA Adaptive Security Appliance Security Services Modules■ Cisco ASA Adaptive Security Appliance Licensing Model■ Basic Cisco ASA Adaptive Security Appliance Hardware Troubleshooting

Module 2: Implementation of Basic Connectivity and Device Management

Lesson 1: Getting Started with the Cisco ASA Adaptive Security Appliance and Cisco ASDM
<ul style="list-style-type: none">■ Managing the Cisco ASA Adaptive Security Appliance Boot Process■ Managing the Cisco ASA Adaptive Security Appliance Using the CLI■ Managing the Cisco ASA Adaptive Security Appliance Using Cisco ASDM■ Navigating Basic Cisco ASDM Features
Lesson 2: Configuring Interfaces and Static Routing
<ul style="list-style-type: none">■ Overview of Basic Configuration Choices, Basic Procedures, and Required Input Parameters■ Managing Cisco ASA Adaptive Security Appliance Security Levels■ Configuring and Verifying Interface Network Parameters■ Configuring and Verifying VLAN Interfaces■ Configuring and Verifying Static Routing■ Configuring and Verifying the Cisco ASA Adaptive Security Appliance DHCP Server■ Troubleshooting Basic Connectivity

Deploying Cisco ASA Firewall Features 1.0 (FIREWALL)

Lesson 3: Configuring Basic Device Management Features

- Overview of Configuration Choices, Basic Procedures, and Required Input Parameters
- Configuring and Verifying Basic Device Management Settings
- Managing Time Settings
- Managing Event and Session Logging
- Managing the Cisco ASA Adaptive Security Appliance File System
- Managing Cisco ASA Adaptive Security Appliance Software and Feature Activation
- Using Other Troubleshooting and Management Tools

Lesson 4: Configuring Management Access

- Overview of Configuration Choices, Basic Procedures, and Required Input Parameters
- Managing Remote Management Channels
- Managing Authentication for Management Access
- Verifying and Troubleshooting AAA for Management Access

Module 3: Deployment of Cisco ASA Adaptive Security Appliance Access Control

Lesson 1: Configuring Basic Access Control

- Overview of Configuration Choices, Basic Procedures, and Required Input Parameters
- Connection Table and Local Host Table
- Configuring and Verifying Interface Access Rules
- Configuring and Verifying Object Groups
- Configuring and Verifying Other Basic Access Controls
- Troubleshooting Basic Access Control

Lesson 2: Using Cisco ASA Adaptive Security Appliance Modular Policy Framework

- Overview of Configuration Choices, Basic Procedures, and Required Input Parameters
- Configuring and Verifying Policies for OSI Layers 3 and 4
- Configuring and Verifying Policies for OSI Layers 5 to 7
- Configuring and Verifying a Policy for Management Traffic

Lesson 3: Tuning Basic Stateful Inspection Features

- Overview of Configuration Choices, Basic Procedures, and Required Input Parameters
- Tuning Basic Inspection of OSI Layers 3 and 4
- Tuning the Cisco ASA Adaptive Security Appliance TCP Normalizer
- Configuring Support for Dynamic Protocols
- Troubleshooting Inspection of OSI Layers 3 and 4 on the Cisco ASA Adaptive Security Appliance

Deploying Cisco ASA Firewall Features 1.0 (FIREWALL)

Lesson 4: Configuring Application Layer Policies
<ul style="list-style-type: none">■ Overview of Configuration Choices, Basic Procedures, and Required Input Parameters■ Configuring and Verifying HTTP Inspection■ Evaluating FTP Inspection■ Evaluating DNS Inspection■ Evaluating ESMTP Inspection■ Evaluating Inspection of Other Protocols■ Troubleshooting Application Layer Inspection
Lesson 5: Configuring Advanced Access Controls
<ul style="list-style-type: none">■ Overview of Configuration Choices, Basic Procedures, and Required Input Parameters■ Configuring and Verifying Cisco TCP Intercept■ Configuring and Verifying the Cisco Botnet Traffic Filter■ Configuring and Verifying Basic Threat Detection■ Configuring and Verifying Advanced Threat Detection■ Configuring and Verifying Scanning Threat Detection
Lesson 6: Configuring Resource Limits and Guarantees
<ul style="list-style-type: none">■ Overview of Configuration Choices, Basic Procedures, and Required Input Parameters■ Configuring and Verifying Connection Limits■ Configuring and Verifying Traffic Policing and Shaping■ Configuring and Verifying Traffic Priority Queuing
Lesson 7: Configuring User-Based Policies (Cut-Through Proxy)
<ul style="list-style-type: none">■ Overview of Configuration Choices, Basic Procedures, and Required Input Parameters■ Configuring and Verifying User Authentication■ Configuring Authentication Prompts and Timeouts■ Configuring and Verifying User Authorization■ Configuring and Verifying User Session Accounting■ Troubleshooting Operation of User-Based Controls

Module 4: Deployment of Cisco ASA Adaptive Security Appliance Network Integration Features

Lesson 1: Deploying Network Address Translation
<ul style="list-style-type: none">■ Overview of Configuration Choices, Basic Procedures, and Required Input Parameters■ Configuring NAT Control■ Configuring and Verifying Dynamic Inside NAT and PAT■ Configuring and Verifying Static Inside NAT and PAT■ Configuring NAT Rules to Bypass Address Translations■ Configuring Outside NAT■ Integrating NAT with Cisco ASA Adaptive Security Appliance Access Control■ Troubleshooting NAT

Deploying Cisco ASA Firewall Features 1.0 (FIREWALL)

Lesson 2: Configuring Cisco ASA Adaptive Security Appliance Transparent Operations

- Overview of Configuration Choices, Basic Procedures, and Required Input Parameters
- Configuring and Verifying Transparent Firewall Mode
- Configuring OSI Layer 3–7 Access Control in Transparent Firewall Mode
- Configuring OSI Layer 2 Access Control in Transparent Firewall Mode
- Troubleshooting Transparent Firewall Operation

Module 5: Deployment of Cisco ASA Adaptive Security Appliance Virtualization and High Availability Features

Lesson 1: Deploying Cisco ASA Adaptive Security Appliance Virtualization Features

- Overview of Configuration Choices, Basic Procedures, and Required Input Parameters
- Configuring and Verifying Security Contexts
- Managing Security Contexts
- Configuring and Verifying Resource Management
- Troubleshooting Security Contexts

Lesson 2: Deploying Cisco ASA Adaptive Security Appliance Redundant Interfaces

- Overview of Configuration Choices, Basic Procedures, and Required Input Parameters
- Configuring and Verifying Redundant Interfaces
- Troubleshooting Redundant Interfaces

Lesson 3: Deploying Active/Standby High Availability Failover

- Overview of Configuration Choices, Basic Procedures, and Required Input Parameters
- Configuring and Verifying Active/Standby Failover
- Tuning and Managing Active/Standby Failover
- Remote Command Execution
- Troubleshooting Active/Standby Failover

Lesson 4: Deploying Active/Active High-Availability Failover

- Overview of Configuration Choices, Basic Procedures, and Required Input Parameters
- Configuring and Verifying Active/Active Failover
- Tuning and Managing Active/Active Failover
- Troubleshooting Active/Active Failover

Deploying Cisco ASA Firewall Features 1.0 (FIREWALL)

Module 6: Integration of Cisco ASA Adaptive Security Appliance Security Service Modules

Lesson 1: Introducing Cisco ASA Adaptive Security Appliance Security Service Modules
<ul style="list-style-type: none">■ Cisco Security Service Modules Overview■ Cisco Content Security Control SSM■ Cisco Advanced Inspection and Protection SSM and SSC
Lesson 2: Integrating the Cisco ASA Adaptive Security Appliance AIP-SSM and AIP-SSC Modules
<ul style="list-style-type: none">■ Cisco AIP-SSM and Cisco AIP SSC Installation■ Managing Cisco ASA AIP-SSM and Cisco ASA AIP SSC Basic Features■ Initializing Cisco ASA AIP-SSM and Cisco ASA AIP SSC■ Configuring Cisco ASA Adaptive Security Appliance Traffic Redirection Policy
Lesson 3: Integrating the Cisco ASA Adaptive Security Appliance CSC-SSM Module
<ul style="list-style-type: none">■ Cisco CSC-SSM Installation■ Managing Cisco CSC-SSM Basic Features■ Initializing Cisco CSC-SSM■ Configuring Cisco ASA Adaptive Security Appliance Traffic Redirection Policy