Deploying Cisco ASA Firewall Features

Duration: 5 Days Course Code: FIREWALL Version: 2.0

Overview:

This five-day course aims to provide network security engineers with the knowledge and skills needed to implement and maintain Cisco ASA adaptive security appliance-based perimeter solutions.
Delegates 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 Audience:

Anyone who implements and maintains Cisco ASA firewalls, Network security specialists and technicians, delegates seeking CCNP Security certification

Objectives:

- **After you complete this course you will be able to:**
- Evaluate the basic firewall technology, features, hardware models, and licensing options of the Cisco ASA security appliance
- Implement and troubleshoot basic Cisco ASA security appliance connectivity and device management plane features
- Configure and verify Cisco ASA security appliance network integration
- Configure and verify Cisco ASA security appliance policy
- Configure and verify high availability and virtualization on Cisco ASA security appliances

Prerequisites:

Attendees should meet the following prerequisites:

- CCNA Security Certification **ICND1** and **IINS** Required.
- Working knowledge of Microsoft Windows OS is an advantage.

Testing and Certification

Recommended preparation for exam(s):

- **642-618** - Deploying Cisco ASA Firewall Solutions

FIREWALL is one of four courses required for the Cisco Certified Network Professional for Security Career Certification

Follow-on-Courses:

The following courses are recommended for further study :

- **SECURE** - Securing Cisco Routers and Switches
- **VPN** - Deploying Cisco ASA VPN Solutions
- **IPS** - Implementing Cisco Intrusion Prevention System

The above courses along with FIREWALL make up the CCNP for Security Certification.

Delegates may also want to consider

- ICISE - Implementing Cisco Identity Services Engine.
- 802.1X - Introduction to 802.1X Operations for Cisco Security Professionals

Content:

Cisco ASA Adaptive Security Appliance Essentials

- Evaluating Cisco ASA Adaptive Security Appliance Technologies
- Identifying Cisco ASA Adaptive Security Appliance Families
- Identifying Cisco ASA Adaptive Security Appliance Licensing Options

Basic Connectivity and Device Management

- Preparing the Cisco ASA Adaptive Security Appliance for Network Integration
- Managing Basic Cisco ASA Adaptive Security Appliance Network Settings
- Configuring Cisco ASA Adaptive Security Appliance Device Management Features

Network Integration

- Configuring Cisco ASA Adaptive Security Appliance NAT Features
- Configuring Cisco ASA Adaptive Security Appliance Basic Access Control Features
- Configuring Cisco ASA Adaptive Security Appliance Routing Features
- Configuring the Cisco ASA Adaptive Security Appliance Transparent Firewall

Cisco ASA Adaptive Security Appliance Policy Control

- Defining the Cisco ASA Adaptive Security Appliance MPF
- Configuring Cisco ASA Adaptive Security Appliance Connection Policy and QoS Settings
- Configuring Cisco ASA Adaptive Security Appliance Advanced Application Inspections
- Configuring Cisco ASA Adaptive Security Appliance User-Based Policies

Cisco ASA Adaptive Security Appliance High Availability and Virtualization

- Configuring Cisco ASA Adaptive Security Appliance Interface Redundancy Features
- Cisco ASA Adaptive Security Appliance Active/Standby High Availability
- Configuring Security Contexts on the Cisco ASA Adaptive Security Appliance
- Configuring Cisco ASA Adaptive Security Appliance Active/Active High Availability

Labs

- Lab 2-1: Preparing the Cisco ASA Adaptive Security Appliance for Network Integration
- Lab 2-2: Configuring the Cisco ASA Adaptive Security Appliance for Secure Network Integration
- Lab 2-3: Configuring Management Features
- Lab 3-1: Configuring NAT
- Lab 3-2: Configuring Basic Cisco Access Control Features
- Lab 3-3: Configuring Transparent Firewall (Optional)
- Lab 4-1: Configuring MPF, Basic Stateful Inspections, and QoS
- Lab 4-2: Configuring MPF Advanced Application Inspections
- Lab 4-3: Configuring Cut-Through Proxy
- Lab 5-1: Configuring Active/Standby High Availability
- Lab 5-2: Configuring Active/Active High Availability

Additional Information:

Recertification:
Cisco professional level certifications (CCNP, CCNP SP Operations, CCNP Wireless, CCDP, CCNP Security, CCNP Voice, and CCIP) are valid for three years. To recertify, pass any 642 exam that is part of the professional level curriculum or pass any CCIE/CCDE written exam before the certification expiration date.

Achieving or recertifying any of the certifications above automatically extends your active Associate and Professional level certification(s) up to the point of expiration of the last certification achieved. For more information, access the Cisco About Recertification page

Further Information:

For More information, or to book your course, please Call/Email us on : - +254 713 027 191

KENYA - training.kenya@clclearningafrica.com

TANZANIA - training.tanzania@clclearningafrica.com

UGANDA - training.uganda@clclearningafrica.com

RWANDA - training.rwanda@clclearningafrica.com

BURUNDI - training.burundi@clclearningafrica.com

ETHOPIA - training.ethopia@clclearningafrica.com