Deploying Cisco ASA Firewall Solutions (FIREWALL) 2.0

Duration 5 Days

COURSE CONTENT

The Deploying Cisco ASA FIREWALL Solutions (FIREWALL) course is part of the curriculum path leading to the Cisco Certified Network Professional Security (CCNP Security) certification. It is a five-day instructor-led course that is aimed at providing you with the knowledge and skills that are needed to implement and maintain perimeter solutions that are based on Cisco ASA security appliances. At the end of the course, you will be able to reduce risk to your IT infrastructure and applications using Cisco ASA security appliance features, and provide detailed operations support for the Cisco ASA security appliance.

WHAT YOU'LL LEARN

- Technology and features of the Cisco ASA
- Cisco ASA product family
- How ASAs and Cisco PIX Security Appliances 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
- Perform essential security appliance configuration using ASDM and the CLI
- Integrate the ASA with Cisco Secure ACS for TACACS+ command authorization
- Integrate the ASA with Cisco Secure ACS for RADIUS network access control
- Configure auto and manual network address translation (NAT)
- Configure access policy based on the Global Access Control List (ACL)
- Configure access policy based on interface 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
- Deep packet inspection of application layer traffic
- Troubleshoot with TCPping, Syslog, Packet Tracer, and packet capture
- Configure access control based on authenticated users
- Configure the security appliance to run in transparent firewall mode
- Enable, configure, and manage multiple contexts to meet security policy requirements
- Select and configure the type of failover that best suits the network topology
- Monitor and manage an installed security appliance

COURSE OBJECTIVES

Upon completing this course, the learner will be able to meet these overall objectives:

- 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

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th

Call us today 0-2634-7993-4

177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

WHO SHOULD ATTEND

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

PREREQUISITES

The knowledge and skills you must have before attending this course are as follows:

- Cisco Certified Network Associate (CCNA) certification or equivalent knowledge
- Cisco Certified Network Associate Security (CCNA Security) certification or equivalent knowledge
- IINS or equivalent knowledge
- Working knowledge of the Microsoft Windows operating system

COURSE OUTLINE

Module 1: Cisco ASA Introduction

- Cisco ASA Technologies
- Cisco ASA Families
- Cisco ASA Licensing Options

Module 2: Basic Connectivity and Device Management

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

Module 3: Network Integration

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

Module 4: Cisco ASA Policy Control

- Defining the Cisco ASA Modular Policy Framework (MPF)
- Configuring Cisco ASA Connection Policy and QoS Settings
- Configuring Cisco ASA Advanced Application Inspections
- Configuring Cisco ASA User-Based Policies

Module 5: Cisco ASA High Availability and Virtualization

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

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th