

## **Securing Networks with ASA Foundation LIVE and ONLINE (SNAF-LAO)**

### **Course Summary**

#### **Description**

This course takes a task-oriented approach to teaching the skills to configure, operate, and manage the Cisco Adaptive Security Appliance product family. Configurations are performed via ASDM. This course covers important new ASA and PIX Security Appliance 8.0 features giving students the knowledge and skills to protect network systems from intrusions and security threats. This course provides an excellent foundation to SNAF.

#### **Objectives**

At the end of this course, students will be able to:

- Explain the functions of the three types of firewalls used to secure today's computer networks
- Describe the technology and features of Cisco security appliances
- Given diagrams of networks protected by Cisco Adaptive Security Appliances (ASAs) and Cisco PIX Security Appliances, explain how each appliance protects network devices from attacks and why each is an appropriate choice for the example network
- Bootstrap the security appliance, prepare the security appliance for configuration via the Cisco Adaptive Security Device Manager (ASDM), and launch and navigate ASDM
- Use ASDM and the CLI to perform essential security appliance configuration
- Use ASDM to configure dynamic and static address translations in the security appliance
- Use ASDM to configure switching and routing on the security appliance
- Use ASDM to configure access control lists, filter malicious active codes, and filter URLs to meet the requirements of the security policy
- Use the packet tracer for troubleshooting
- Use ASDM to configure object groups that meet the requirements of the security policy
- Use ASDM to configure AAA as needed to meet the requirements of the security policy
- Use ASDM to configure a modular policy that supports the security policy
- Use ASDM to configure protocol inspection to meet the requirements of the security policy
- Use ASDM and the CLI to configure threat detection to meet the requirements of the security policy
- Use ASDM to configure the security appliance to support a site-to-site VPN that meets the requirements of the security policy
- Use ASDM to configure the security appliance to provide secure connectivity using remote access VPNs
- Configure the security appliance to run in transparent firewall mode as needed to meet the requirements of the security policy
- Enable, configure, and manage multiple contexts as needed to meet the requirements of the security policy
- Select and configure the type of failover that best suits the network topology
- Monitor and manage an installed security appliance

## Securing Networks with ASA Foundation LIVE and ONLINE (SNAF-LAO)

### Course Summary

#### Topics

- Introducing Cisco Security Appliance Technology and Features
- Introducing the Cisco ASA and PIX Security Appliance Families
- Getting Started with Cisco Security Appliances
- Configuring a Security Appliance
- Configuring Translations and Connection Limits
- Using ACLs and Content Filtering
- Configuring Object Grouping
- Switching and Routing on Cisco Security Appliances
- Configuring AAA for Cut-Through Proxy
- Configuring the Cisco Modular Policy Framework
- Configuring Advanced Protocol Handling
- Configuring Threat Detection
- Configuring Site-to-Site VPNs Using Pre-Shared Keys
- Configuring Security Appliance Remote-Access VPNs
- Configuring the Cisco ASA Security Appliance for SSL VPN
- Configuring Transparent Firewall Mode
- Configuring Security Contexts
- Configuring Failover
- Managing the Security Appliance

#### Audience

- Technicians requiring CCSP Certification or ASA Specialist Certification
- Technicians using or designing networks with Cisco ASA products

#### Prerequisites

- Certification as a CCNA or the equivalent knowledge
- Basic knowledge of the Windows operating system
- Familiarity with the networking and security terms and concepts (the concepts are learned in prerequisite training or by reading industry publications).

#### Duration

Five days