المركـــز العالمـــي للتدريـــب والتطويـــر
International Centre For Training & Development

SECURING NETWORKS with ASA Foundation

Course Introduction:

Securing Networks with ASA Fundamentals (SNAF) is a instructor-led, lab-intensive course. This task-oriented course teaches the knowledge and skills needed to configure, maintain, and operate Cisco ASA 5500 Series Adaptive Security Appliances.

Securing Networks with ASA Fundamentals lessons and labs are now GUI-based, the commands for each configuration task are also presented in the lessons for those who prefer to configure the security appliance via the command line interface (CLI). In SNAF 1.0, learners will have the ability to implement the following:

- Threat detection
- Secure logging
- Remote command execution in failover pairs
- Redundant interfaces
- Modular policy framework enhancements
- Access control list renaming capability
- FTP support for SSL VPN
- Onscreen keyboard for the SSL VPN
- Administrator-defined customization of all SSL VPN user-visible content
- Personal bookmarks for SSL VPN users

Course Objectives:

- 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
- Given a PC, a Cisco 5520 ASA, and a security policy, 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

Who Should Attend?

- Network designers
- Network administrators
- Network engineers
- Network managers
- Systems engineers
- Project Managers
- Cisco customers who implement and maintain Cisco ASA security appliances
- Cisco channel partners who sell, implement, and maintain ASA security appliances
- Cisco engineers who support the sale of ASA security appliances

Course Outline:

- 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

Course Methodology:

A variety of methodologies will be used during the course that includes:

- (30%) Based on Case Studies
- (30%) Techniques
- (30%) Role Play
- (10%) Concepts
- Pre-test and Post-test
- Variety of Learning Methods
- Lectures
- Case Studies and Self Questionaires
- Group Work
- Discussion
- Presentation

Course Fees:

To be advice as per course location. This rate includes participant's manual, Hands-Outs, buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Course Certificate:

International Center for Training & Development (ICTD) will award an internationally recognized certificate(s) for each delegate on completion of training.

Course Timings:

Daily Course Timings:

08:00 - 08:20	Morning Coffee / Tea
08:20 - 10:00	First Session
10:00 - 10:20	Coffee / Tea / Snacks
10:20 - 12:20	Second Session
12:20 - 13:30	Lunch Break & Prayer Break
13:30 - 15:00	Last Session