NETLOGIC TRAINING CENTER

Course Training

Cisco® Deploying Cisco® ASA Firewall Features 2.0 (FIREWALL)

Course Content

This Cisco ASA training workshop is two intensive days filled with hands-on lab exercises where you'll learn how to reset the administrator password (even when you don't know it), how to build a basic firewall configuration from scratch in the command-line and in the GUI. Once you've finished building the configuration, you get lots of hands-on practice in how to manage it. You'll learn how to write and manage access-control lists, how to set up three different kinds of VPNs, a DMZ, and a lot more.

You'll practice backing-up and restoring your configuration files and the firewall's operating system image. We'll show you how to set up centralized logging with a syslog server. You'll practice configuring login banners. You'll configure local usernames and privilege levels, plus you'll practice using Active Directory for authentication. You'll set up a DHCP server for automatic address assignment. You'll practice building three types of VPNs including site-to-site, remote access AnyConnect VPN, and a clientless Web VPN. You'll build a DMZ with a Web server and a print server. You'll even practice port-scanning to test for vulnerabilities.

Course Objective

Upon completion of Cisco ASA training workshop, you'll...

- Practice password recovery techniques for the Cisco ASA security appliance
- Practice two techniques for building a basic firewall configuration from scratch
- Gain an understanding of logging configurations and practice using syslog with the security appliance
- Practice two methods of backing up and restoring device's configurations
- Practice two methods of backing up and restoring your device's software image (operating system), including how to recover the software in a catastrophic fault condition
- Practice configuring and using three methods of remote management
- Gain an understanding of Network Address Translation and Port Address Translation on the ASA Security Appliance and practice using them in your configurations
- Practice configuring three types of banners
- Gain an understanding of Cisco privilege levels and practice configuring local usernames and privilege levels
- Practice configuring your security appliance to authenticate via Windows Active Directory using RADIUS
- Practice building and troubleshooting a DHCP server
- Practice building three types of VPNs including site-to-site, remote access, and a clientless Web VPN
- Gain an understanding of DMZs and practice building one with a Web server
- Practice testing security configurations with a port scanner
- Gain an understanding of filtering techniques and practice blocking Java applets
- Practice building a transparent (layer 2) firewall
- Practice building a route mode (layer 3) firewall

Course Prerequisite

A solid understanding of networking concepts and technologies is highly beneficial. This knowledge can be obtained by enrolling in our Networking Overview for Managers training course. Familiarity with router configurations is also very helpful.

Course Pre-Test

Not Required

Course Details

Day 1

Item	Subject	Details	Personal Lab and devices	Workgroup Lab and devices
1	Understanding firewall fundamentals	• What do firewalls do? • Types of Firewalls • Classification of Firewalls • AAA: Authentication, Authorization, and Accounting • Basics of Encryption including Single Key and PKI • Stateful Inspection Adaptive Security Algorithm • Network Address Translation • An Overview of Cisco Security Appliances • Understanding VLANs • Understanding the Eight Basic Commands on a Cisco ASA Security Appliance • Controlling the Appliance from its Console • Password Recovery	Theory and Lecture	
		Break		
2	Backing Up and Restoring Configurations and Software Images	• Analyzing the Base Configuration of the Security Appliance	Theory and Lecture	
	Summary challenge advance lab for factory default and Basic Firewall configuration	Lab 1 - Factory default ASA firewall - Password Recovery and Initial Configuration - Removing the Existing Configuration - Using the Eight Commands Required to Enable Basic Firewall Functionality - Building a Base Configuration on the ASA - Security Appliance Lab 2 - Analyzing the Base Configuration and Saving It - Backing Up and Restoring the Configuration - Backing Up and Restoring the Software Image	(Lab 1 and Lab 2) **Real Device** ISR router 4321 1 Unit Catalyst 3560-CX 1 Unit Firewall ASA 5506 1 unit Windows AD 1 Unit Syslog Server 1 Unit	

Day 2

Item	Subject	Details	Personal Lab and devices	Workgroup Lab and devices
3	Sending Logging Output to a Syslog Server	• Using syslogd with the Security Appliance	Theory and Lecture	
4	Remote Management Options	• Remote Console Access concept • Telnet • SSH (Secure Shell) • Configuring and Managing Remote Management through ASDM	Theory and Lecture	
		Break		
5	Configuring Logon Banners, Usernames, and Authentication, Authorization, and Accounting (AAA)	• How to Configure a Banner • Configuring Authentication, Authorization, and Accounting (AAA) • Remote Authentication Technologies • Cisco Secure Access Control Server • Installing and Configuring CACS • Authentication of Clients	Theory and Lecture	
	Summary challenge advance lab for Logging , Remote access and authentication	Lab 1 - Sending Logging Output to a Syslog Server Lab 2 - Telnet and Secure Shell (SSH) Lab 3 - Creating Banners on the Security Appliance - Configuring Usernames and Local Authentication - Configuring Privilege Levels on the Security Appliance - Authenticating Through Windows Active Directory	(Lab 1, 2 and Lab 3) **Real Device** ISR router 4321 1 Unit Catalyst 3560-CX 1 Unit Firewall ASA 5506 1 unit Windows AD 1 Unit Syslog Server 1 Unit	

Day 3

Item	Subject	Details	Personal Lab and devices	Workgroup Lab and devices
6	Configuring the Appliance as a DHCP Server	• Understanding DHCP Theory and Operation • Understanding the DHCP commands on the security appliance	Theory and Lecture	
		Break		
7	Access-Control Lists	• The importance of order of entries • The difference between standard and extended lists • Hidden implicit statements in ACLs • Editing ACLs • Re-naming ACLs • Using time-ranges with ACLs • How to use object groups with ACLs	Theory and Lecture	
	Summary challenge advance lab for DHPC and ACL	Lab 1 - Configuring Your DHCP Server on ASA - Verifying ASA DHCP Functionality Lab 2 - Configure ACL basic functionality - Verifying ACL operation	(Lab 1 and Lab 2) **Real Device** ISR router 4321 1 Unit Catalyst 3560-CX 1 Unit Firewall ASA 5506 1 unit Windows AD 1 Unit Syslog Server 1 Unit	

Day 4

Item	Subject	Details	Personal Lab and devices	Workgroup Lab and devices
8	Virtual Private Networking (VPNs)	• Explain PPTP Theory and Operation • Explain L2TP Theory and Operation • Explain IPSec Theory and Operation • Encryption Algorithms • Hashing Algorithms • Authentication Methods • Troubleshooting VPN Connections • Configuring the Cisco AnyConnect VPN Client and Connecting to Your VPN • Creating a Web-Based SSL VPN	Theory and Lecture	
		Break		
9	DMZs (De-Militarized Zones)	• Understanding DMZ concepts • Security Levels • Access Control Lists • Static Routes • Port Scanning	Theory and Lecture	
	Summary challenge advance lab for VPN and DMZ	Lab 1 - Site-to-Site VPNs - Remote Access VPNs - Configuring a Web-Based SSL VPN - Configuring the Cisco AnyConnect Client - Logging Off VPN Users through the ASDM Lab 2 - Configuring a DMZ - Analyzing Potential Vulnerabilities with Port Scanning	(Lab 1 and Lab 2) **Real Device** ISR router 4321 1 Unit Catalyst 3560-CX 1 Unit Firewall ASA 5506 1 unit Windows AD 1 Unit Syslog Server 1 Unit	

Day 5

Item	Subject	Details	Personal Lab and devices	Workgroup Lab and devices
10	Filtering Content	- Configuring Unicast RPF - Fragmented Packets - Intrusion Prevention - URL Filtering - Dynamic Content Filtering	Theory and Lecture	
		Break		
11	Configuring Transparent Mode	- Understanding transparent mode	Theory and Lecture	
	Summary challenge advance lab for Filtering	Lab1 - Filtering Dynamic Java Content Lab 2 - Viewing and changing the mode	(Lab 1 and Lab 2) **Real Device** ISR router 4321 1 Unit Catalyst 3560-CX 1 Unit Firewall ASA 5506 1 unit Windows AD 1 Unit Syslog Server 1 Unit	

Course Post-Test

Not Required

Course Materials

Not include in this class training (but you can requested from sale team)

Course Devices Training (Per 1 Person)

Cisco Catalyst 3560-CX

Cisco Router ISR 4321

Cisco ASA 5506-CX

Windows Server Active Directory

CISCO CERTIFIED SPECIALIST

KIWI part of the solarwinds family