



**Internet
Institute USA**

Cisco Secure PIX Firewall

Cisco Secure PIX Firewall Advanced

This five-day, task-oriented, lab-intensive course teaches the knowledge and skills needed to describe, configure, verify and manage the PIX Firewall product family and the Cisco IOS Firewall feature set.

Coverage includes:

- Identify PIX Firewall features, models, components and benefits
- Describe PIX Firewall installation procedures
- Upgrade software images
- Configure inbound and outbound access through the PIX Firewall
- Configure multiple interfaces on the PIX Firewall
- Configure the PIX Firewall as a DHCP server
- Configure the PIX Firewall as a DHCP client
- Configure the PIX Firewall to send messages to a syslog server
- Perform password recovery
- Configure access control and content filtering on the PIX Firewall
- Configure special protocol handling on the PIX Firewall
- Configure attack guards and SSH Configure AAA on the PIX Firewall
- Configure and test failover using the PIX Firewall
- Configure the IDS feature set
- Configure a site-to-site VPN utilizing the PIX Firewall
- Install PIX Device Manager and use it to configure the PIX Firewall
- Test and verify PIX Firewall operations
- Configure Cisco IOS Firewall Context-based Access Control
- Configure authentication proxy with Cisco IOS software



To register or to check on class schedules, or for additional information, see our Web site at <http://iisatech.com>, or send us email: info@iisatech.com.

- Instructor-led classroom sessions
- Out-of-hours laboratory time
- Course textbook/materials

<http://iisatech.com>

Course Outline

Cisco Secure PIX Firewall Advanced (Exam 642-521)

IIUSA-334 Cisco Secure PIX Firewall Advanced (CSPFA) (5 days)

Prerequisites: A CSPFA student should possess Cisco Certified Network Associate (CCNA) certification or the equivalent knowledge (working knowledge of basic network security and a solid grasp of TCP/IP and fundamental networking concepts), be familiar with encryption technologies: DES, 3DES, RSA, hashing algorithms (MD5/SHA), and IPSec, and have a basic knowledge of the Windows operating system.

Part 1: Network Security and the Cisco PIX Firewall

Reasons for securing network
The four primary types of threats
The three primary methods of attack; The Security Wheel
Cisco AVVID and SAFE overview

Part 2: Cisco PIX Firewall Technology

Firewalls and firewall technologies
PIX Firewall family; The finesse OS
ASA and ASA Security Levels; Cut-through proxy

Part 3: Identify the Cisco PIX Firewall

PIX Firewall 506, 515, 520, 525, and 535 controls, connectors, and LEDs
Proper location for the perimeter network cables

Part 4: Basic Configuration of the PIX Firewall

General maintenance commands
ASA security levels
The six primary commands (nameif, interface, ip address, route, nat, global)
Lab Ex: Configure the PIX Firewall and execute general maintenance commands

Part 5: PIX Firewall Translations

Transport protocols PIX Firewall translations
Access through the PIX Firewall
Lab Ex: Configuring access through the PIX

Part 6: Configuring Multiple Interfaces

Configuring additional interfaces
Lab Ex: Configuring multiple interfaces

Part 7: DHCP Support

Dynamic Host Configuration Protocol
PIX Firewall as DHCP Server and Client
Lab Ex: Configure the PIX Firewall's DHCP server and client features

Part 8: Configuring Syslog messages

Lab Ex: Configuring syslog

Part 9: Access Control Configuration and Content Filtering

Access control through the PIX Firewall
Malicious active code filtering
URL filtering with Websense
Lab Ex: Configure ACLs in the PIX Firewall

Part 10: Advanced Protocol Handling

Advanced protocols; Multimedia support
Lab exercise: Configure and test advanced protocol handling and attack guards

Part 11: Attack Guards and Intrusion Detection

Attack guards; Intrusion detection
Lab Ex: Configure PIX to use IDS signatures

Part 12: AAA Configuration on Cisco PIX Firewall

Intro to AAA Installation of Cisco Secure ACS for WinNT
Authentication configuration; Authorization configuration
Accounting configuration
Troubleshooting the AAA configuration
Lab Ex: Configure AAA on PIX using CSACS on WinNT

Part 13: Failover

Understand failover; Configure failover
Lab Ex: Configure failover

Part 14: Site-to-site VPN Configuration

Explanation of IPSec; Configure PIX Firewall
IPSec; Scale PIX Firewall VPNs
Lab Ex: Configure a PIX Firewall VPN

Part 15: System Maintenance

Password recovery; Image upgrade
Lab Ex: Upgrade the PIX Firewall image

Part 16: Cisco PIX Device Manager

PDM overview; PDM operating requirements
Prepare for PDM; Using PDM
Lab Ex: Install and configure PDM

Part 17: The Cisco IOS Firewall Context-Based Access Control Configuration

Introduction to Cisco IOS Firewall
How CBAC works; Audit trail and alert
Global timeouts and thresholds
Port-to-application mapping; Define inspection rules
Inspection rules and ACLs applied to router interfaces
Test and verify; CBAC

Lab Ex: Configure IOS Firewall on a Cisco router

Part 18: The Cisco IOS Firewall Authentication Proxy Configuration

Introduction to the Cisco IOS Firewall authentication proxy
AAA server configuration; AAA configuration
Authentication proxy configuration; Test and verify configuration
Lab Ex: Configure authentication proxy on a Cisco router

College Credit

This course qualifies for 2.0 college credits at the University of Phoenix. For details, see:

<http://iisatech.com/UoPcredit.html>

Internet Institute USA

2200 North Central Avenue; Suite 103

Phoenix, AZ 85004

602-776-4545 (phone); 480-452-1688(fax)

<http://iisatech.com> • info@iisatech.com