



DATA SHEET

SECURING NETWORKS WITH CISCO PIX AND ASA SECURITY APPLIANCES

This authorized Cisco Systems® course (SNPA) teaches the knowledge and skills needed to configure, maintain, and operate Cisco® PIX® 500 Series security appliances and Cisco ASA 5500 Series adaptive security appliances. SNPA is recommended training for the Cisco Certified Security Professional (CCSP™) certification.

DURATION

Five Days

OBJECTIVES

Upon completion of this course, students will be able to perform the following tasks:

- Describe the security appliance features, models, components, and benefits
- Discuss Adaptive Security Algorithm (ASA) and ASA security levels
- Configure a security appliance for basic network connectivity
- Configure the security appliance to send syslog messages to a syslog server
- Describe how TCP and User Datagram Protocol (UDP) function within the security appliance
- Describe how static and dynamic translations function
- Explain the security appliance Port Address Translation (PAT) feature
- Configure and explain the function of access control lists (ACLs) and Network Address Translation (NAT) 0 ACLs
- Configure active code filtering (ActiveX and Java applets)
- Configure the security appliance for URL filtering
- Describe the object grouping feature of the security appliance and its advantages
- Name the authentication, authorization, and accounting (AAA) protocols supported by the security appliance
- Define and configure cut-through proxy authentication and tunnel access authentication
- Define and configure AAA accounting
- Install and configure the basic Cisco Secure Access Control Server function
- Describe how the security appliance implements FTP and HTTP protocol inspection
- Describe how the security appliance implements remote shell (rsh), Structured Query Language (SQL), Simple Mail Transfer Protocol (SMTP), Internet Control Message Protocol (ICMP), and Simple Network Management Protocol (SNMP) inspection
- Identify the tasks and commands to configure security appliance IP Security (IPSec) support
- Describe and configure the Easy VPN server and remote using the Cisco VPN client
- Configure WebVPN general parameters, servers, URLs, and port forwarding
- Monitor and maintain transparent firewall mode
- Configure and manager a security context
- Define the security appliance hardware failover requirements
- Install Adaptive Security Device Manager (ASDM) and use it to configure the security appliance
- Configure the AIP-SSM setup parameters
- Configure a security policy on an ASA security appliance using ASDM
- Configure Telnet and SSH access to the security appliance console
- Recover the security appliance passwords using general password recovery procedures

- Use Trivial File Transfer Protocol (TFTP) to install and upgrade the software image on the security appliance

TARGET AUDIENCE

Cisco customers who implement and maintain Cisco PIX security appliances and ASA security appliances; Cisco channel partners who sell, implement, and maintain Cisco PIX security appliances and ASA security appliances; and Cisco Systems engineers who support the sale of Cisco PIX security appliances and ASA security appliances.

PREREQUISITES

CCNA® equivalent experience as taught in the Interconnecting Cisco Network Devices (ICND) course. Skills include the following:


- From the command-line interface (CLI), configure a Cisco IOS® Software router and switch, to include navigating, interfaces, VLANs, routing, and so forth
- Configure and enable static and dynamic routing, including Routing Information Protocol (RIP) and Enhanced Interior Gateway Routing Protocol (EIGRP) on a Cisco IOS Software router
- Troubleshoot a Cisco IOS Software device using the appropriate show and debug commands
- Configure standard and extended access lists to manage traffic access

COURSE OUTLINE

- Cisco Security Appliance Technology and Features
- Cisco PIX Security Appliance and ASA Adaptive Security Appliance Families
- Getting Started with Cisco Security Appliances
- Translations and Connections
- Access Control Lists and Content Filtering
- Object Grouping
- Authentication, Authorization, and Accounting
- Switching and Routing
- Modular Policy Framework
- Advanced Protocol Handling
- VPN Configuration
- Configuring Cisco PIX Firewall Remote Access Using Cisco Easy VPN
- Configuring ASA for WebVPN
- Configuring Transparent Firewalls
- Configuring Security Contexts
- Failover
- Cisco Security Appliance Device Manager
- AIP-SSM—Getting Started
- Managing Security Appliances

LAB OUTLINE

- Lab 1: PIX Security Appliance and Executing General Maintenance Commands
- Lab 2: Configuring Access Through the Security Appliance
- Lab 3: ACLs on the Security Appliance
- Lab 4: Object Groups
- Lab 5: AAA on the Security Appliance Using Cisco Secure ACS for Windows 2000
- Lab 6: Configuring and Testing Advanced Protocol Inspection on the Security Appliance

- 
- Lab 7: Security Appliance Site-to-Site VPN
 - Lab 8: Secure VPN Using IPSec Between a Security Appliance and a Cisco VPN Client
 - Lab 9: ASA Security Appliance for WebVPN
 - Lab 10: Security Appliance Transparent Firewall
 - Lab 11: LAN-Based Failover
 - Lab 12: Configuring the Security Appliance with ASDM
 - Lab 13: Initializing the AIP-SSM
 - Lab 14: Managing the Security Appliance

REGISTRATION INFORMATION

For more information about schedules and registration for this course, please contact aeskt_registration@cisco.com.

For more information on Advanced Services Education course offerings, as well as Curriculum Planning Services and custom training options, refer to the AS Education Website at www.cisco.com/go/ndm.

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International
BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratum, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0402R)