



642-521

Cisco Secure Pix Firewall Advanced

Study Guide
Version 1.0

Copyright (c) 2003 Chinatag LLC. All rights reserved.

Important Note Please Read Carefully

This Study guide has been carefully written and compiled by chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website. Our IT certification products start at only **\$7.99**.

Study Tips

This guide will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 180 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedbacks help us improve future versions. Feedback on specific questions should be send to feedback@chinatag.com.

Thanks for purchasing Chinatag products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team
Chinatag LLC.

TABLE OF CONTENTS

List of Tables

List of Acronyms

Introduction

1. Network Security Threats

- 1.1 The Main Types of Network Security Threats
 - 1.1.1 Internal Threats
 - 1.1.2 External Threats
 - 1.1.3 Unstructured Threats
 - 1.1.4 Structured Threats
- 1.2 The Three Main Types of Network Attacks
 - 1.2.1 Reconnaissance Attacks
 - 1.2.2 Access Attacks
 - 1.2.3 Denial-of-Service Attacks (DoS)
- 1.3 The Security Policy
- 1.4 The Security Process
 - 1.4.1 Securing an Environment
 - 1.4.2 Monitoring an Environment for Breaches and Attacks
 - 1.4.3 Testing the Security of an Environment
 - 1.4.4 Improving a Security Policy

2. The Fundamentals of the PIX Firewall

- 2.1 Areas of the Network
 - 2.1.1 The Inside Interface (Trusted)
 - 2.1.2 The Outside Interface (Untrusted)
 - 2.1.3 The Demilitarized Zone
 - 2.1.4 Perimeter Routers
- 2.2 Firewall Filtering Technologies
 - 2.2.1 Packet Filter
 - 2.2.2 Proxy Filter
 - 2.2.3 Stateful Packet Filter
- 2.3 Cisco PIX Firewall Features
 - 2.3.1 Secure Embedded System
 - 2.3.2 Adaptive Security Algorithm (ASA)
 - 2.3.3 Cut-through Proxy

- 2.3.4 URL Filtering
- 2.3.5 Failover/Hot Standby
- 2.3.6 VPN Support

- 2.4 The PIX Firewall's Adaptive Security Algorithm (ASA)
 - 2.4.1 Security Levels

- 2.5 The PIX Firewall Series Models
 - 2.5.1 Cisco PIX 501 Firewall
 - 2.5.2 Cisco PIX 506E Firewall
 - 2.5.3 Cisco PIX 515E Firewall
 - 2.5.4 Cisco PIX 525 Firewall
 - 2.5.5 Cisco PIX 535 Firewall

- 2.6 Cisco PIX Firewall Expansion Cards

- 2.7 Software Licensing

- 2.8 Activation Keys

3. Setting Up the PIX Firewall

- 3.1 Default Configuration

- 3.2 PIX Firewall CLI Administrative Access Modes
 - 3.2.1 Unprivileged Access Mode
 - 3.2.2 Privileged Access Mode
 - 3.2.3 Configuration Access Mode
 - 3.2.4 Monitor Access Mode

- 3.3 PIX Firewall Common Commands

- 3.4 PIX Firewall Basic Commands
 - 3.4.1 The Nameif Command
 - 3.4.2 The Interface Command
 - 3.4.3 The IP Address Command
 - 3.4.4 The Nat Command and the Global Command
 - 3.4.5 The Route Command

- 3.5 PIX Firewall Save and View Commands

- 3.6 Trivial File Transfer Protocol (TFTP)
 - 3.6.1 The Copy Command
 - 3.6.2 Monitor Mode
 - 3.6.3 The Write Net Command
 - 3.6.4 The Write Erase Command
 - 3.6.5 The Configure Net Command



4. Translations and Connections

- 4.1 Transport Protocols (Layer 4)
 - 4.1.1 Transmission Control Protocol (TCP)
 - 4.1.2 User Datagram Protocol (UDP)
- 4.2 Private Address Translations
- 4.3 Translation and Connection Tables
 - 4.3.1 Show and Clear Xlate Table Commands
 - 4.3.2 Show Conn Table Commands
- 4.3 Outbound Traffic
 - 4.4.1 Static Address Translations
 - 4.4.2 Network Address Translation (NAT)
 - 4.4.3 Port Address Translation (PAT)
 - 4.4.4 Utilizing NAT and PAT

5. Traffic Control and Access Control Lists (ACLs)

- 5.1 Controlling Traffic Using the Conduit Command
- 5.2 Controlling Traffic Using Access Lists
 - 5.2.1 The Access-Group Command
 - 5.2.2 The Access-List Command
 - 5.2.3 ICMP ACL Statement
 - 5.2.4 Turbo ACL Statement
 - 5.2.5 Downloading ACLs
- 5.3 Content Filtering
 - 5.3.1 ActiveX Blocking
 - 5.3.2 JAVA Blocking
 - 5.3.3 Websense Filtering
- 5.4 Object Grouping
 - 5.4.1 Network Groups
 - 5.4.2 Service Groups
 - 5.4.3 Protocol Groups
 - 5.4.4 ICMP Type Groups
 - 5.4.5 Showing and Removing Object Commands
 - 5.4.6 Nested Object Groups

6. Basic System Management

- 6.1 Date and Time Setting
 - 6.1.1 Setting the Date and Time Manually

- 6.1.2 Setting the Date and Time Using Network Time Protocol (NTP)
 - 6.1.2.1 Configuring NTP Support on the PIX Firewall
 - 6.1.2.2 Verifying NTP Support on the PIX Firewall

6.2 Methods of Accessing the PIX Firewall

- 6.2.1 Console Port Access
- 6.2.2 Telnet Access
- 6.2.3 Secure Shell (SSH) Access
 - 6.2.3.1 Configuring a Hostname
 - 6.2.3.2 Configuring a Domain Name
 - 6.2.3.3 Creating a Public Key and Private RSA Key
 - 6.2.3.4 Defining IP addresses for SSH Access
 - 6.2.3.5 Verifying SSH Information
- 6.2.4 HTTP PIX Device Manager (PDM) Access

6.3 Dynamic Host Configuration Protocol (DHCP)

- 6.3.1 DHCP Server Feature
 - 6.3.1.1 Configuring and Monitoring the DHCP Server Feature
- 6.3.2 DHCP Client Feature

6.4 Simple Network Management Protocol (SNMP)

- 6.4.1 Configuring SNMP on the PIX Firewall

6.5 The PIX Firewall Logging Commands

7. Advanced PIX Firewall Features including Advanced Protocol Handling

7.1 PIX Firewall Routing

- 7.1.1 Routing Information Protocol (RIP)

7.2 The Fixup Protocol Feature

7.3 File Transfer Protocol (FTP)

7.4 Hypertext Transfer Protocol (HTTP)

7.5 Voice over IP (VoIP)

- 7.5.1 H.323
- 7.5.2 Skinny Client Control Protocol (SCCP)
- 7.5.3 Session Initiation Protocol (SIP)

7.6 Simple Mail Transfer Protocol (SMTP)

7.7 Real Time Streaming Protocol (RSTP)

7.8 SQL*Net Protocol

7.9 Internet Group Management Protocol (IGMP)

7.10 Attack Guards

7.10.1 DNS Guard

7.10.2 Flood Defender

7.10.3 Fragmentation Guard (FragGuard) and Virtual Reassembly

7.10.3.1 The Sysopt Security Fragguard Command

7.10.4 TCP Intercept

7.10.5 Unicast Reverse Path Forwarding (Unicast RPF)

7.11 Shunning

7.12 Intrusion Detection

7.12.1 Configuring the IDS

8. AAA Configuration on the PIX Firewall

8.1 Specifying a AAA Server

8.1.1 Setting up the Server Group

8.1.2 The Local User Database

8.2 Configuring AAA Services

8.2.1 User Session Authentication

8.2.2 Authorization Services

8.2.3 Accounting Services

8.3 AAA and Access Lists

8.4 The Command Level Authorization Feature

8.5 The Privilege Level Feature

9. The PIX Firewall Failover Feature

9.1 Failover Overview

9.2 Replication

9.3 Detecting a Failover

9.4 Cable-based Failover Configuration

9.5 LAN-based Failover Configuration

10. The PIX Firewall and its Virtual Private Network (VPN) Features

- 10.1 IPSec Overview
 - 10.1.1 IPSec's Security Protocols, Components and Modes
 - 10.1.2 Creating an IPSec VPN
- 10.2 Configuring IPSec
 - 10.2.1 Preparing to Configure IPSec VPN Support
 - 10.2.2 Configuring the IKE Parameters
 - 10.2.2.1 Enabling IKE
 - 10.2.2.2 Creating the IKE Policies
 - 10.2.2.3 Configuring Preshared Keys
 - 10.2.2.4 Configuring CAs
 - 10.2.3 Configuring the IPSec Parameters
 - 10.2.3.1 Getting Around Interface ACLs
 - 10.2.3.2 Configuring Crypto Access Lists
 - 10.2.3.3 Configuring Transform Sets
 - 10.2.3.4 Configuring Crypto Maps
 - 10.2.3.5 Applying Crypto Maps to an Interface
 - 10.2.4 Testing, Verifying and Debugging the IPSec Configuration
- 10.3 Configuring the PIX Firewall as an Easy VPN Remote Device
- 10.4 Scaling VPNs
 - 10.4.1 Cisco Secure Policy Manager (CSPM)
 - 10.4.2 CiscoWorks VPN/Security Management Solution (VMS)
- 10.5 Point-to-Point Protocol over Ethernet (PPPoE)

11. Managing and Configuring the PIX Firewall with the PIX Device Manager

- 11.1 PDM Requirements
- 11.2 Installing and Connecting to the PDM
- 11.3 Utilizing the PDM to Configure the PIX Firewall
- 11.4 Creating a Remote Access VPN with the PDM
- 11.5 Creating a Site-to-site VPN with the PDM
- 11.6 The CiscoWorks Management Center

LIST OF TABLES

TABLE 2.1:	The Open System Interconnection (OSI Model)
TABLE 2.2:	Security Levels on the Pix firewall
TABLE 2.3:	Cisco Pix Firewall Models and Default Abilities
TABLE 3.1:	PIX firewalls 501 and 506E Default Configuration Settings
TABLE 3.2:	PIX Firewall Interface Command Options
TABLE 3.3:	PIX firewall NAT Command Options
TABLE 3.4:	PIX firewall Global Command Options
TABLE 4.1:	The xlate Command Options
TABLE 4.2:	The conn Command Options
TABLE 4.3:	The static Command Parameters
TABLE 4.4:	The nat Command Options
TABLE 5.1:	The conduit Command Options
TABLE 5.2:	The access-list Command Options
TABLE 5.3:	ICMP Types
TABLE 5.4:	The filter activex Command Options
TABLE 5.5:	The filter activex Command Options
TABLE 6.1:	The PIX firewall Logging Severity Levels
TABLE 7.1:	The rip Command Options

LIST OF ACRONYMS

AAA	Authentication / Authorization / Accounting
ACL	Access Control List
ACK	Acknowledgement
ACS	Access Control Server
AH	Authentication Header
ARP	Address Resolution Protocol
ASA	Adaptive Security Algorithm
BGP	Border Gateway Protocol
CA	Certificate Authority
CBAC	Context-Based Access Control
CGMP	Cisco Group Management Protocol
CSPM	Cisco Secure Policy Manager
CSACS	Cisco Secure Access Control Server
DES	Data Encryption Standard
DH	Diffie-Hellman Key Agreement
DHCP	Dynamic Host Configuration Protocol
DLSw	Data-link Switching
DNS	Domain Name Service
DoS	Denial of Service
DDoS	Distributed denial-of-service
DST	Daylight Saving Time
3DES	Triple DES
ESP	Encapsulating Security Payload
FO	Failover
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
IANA	Internet Assigned Numbers Authority
IDS	Intrusion Detection System
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol

IKE	Internet Key Exchange
IPSec	IP Security Protocol
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
Kbps	kilobits per second (bandwidth)
LAN	Local Area Network
MD	Message Digest
MD5	Message Digest 5
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
NAT	Network Address Translation
NEM	Network Extension Mode
NMS	Network Management Stations
NTP	Network Time Protocol
OS	Operating System
OSPF	Open Shortest Path First
PAP	Password Authentication Protocol
PAT	Port Address Translation
PDM	PIX Device Manager
PFSS	PIX Firewall Syslog Server
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Authentication Dial-In User Service
RIP	Routing Information Protocol
ROBO	Remote office/branch office
RPF	Reverse Path Forwarding
RSA	Rivest, Shamir, and Adelman
RSH	Remote Shell
RTP	Real-Time Transport Protocol
RTCP	RTP Control Protocol

SA	Security Association
SCCP	Skinny Client Control Protocol
SEP	Scalable Encryption Processing
SHA-1	Secure Hash Algorithm-1
SIP	Session Initiation Protocol
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SOHO	Small Office/Home Office
SPI	Security Parameters Index
SSH	Secure Shell
SSL	Secure Sockets Layer
SYN	Synchronization
TACACS+	Terminal Access Controller Access Control System Plus
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
UR	Unrestricted
VAC	VPN Accelerator Card
VMS	VPN/Security Management Solution
VoIP	Voice over IP
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
XML	Extensible Markup Language
XAUTH	eXtended Authentication

642-521 CCSP Cisco Secure PIX Firewall

Exam Code: 642-521

Certifications:

Cisco Certified Security Professional (CCSP)

Core

Prerequisites:

Knowledge on securing Cisco IOS Networks and some experience and knowledge on VPNs would be beneficial.

About This Study Guide

This Study Guide is based on the exam questions for the 642-521 Cisco Secure PIX Firewall (CSPFA) exam. It presents all the information necessary to pass the 642-521 Cisco Secure PIX Firewall (CSPFA) exam, and is detailed on the particular proficiencies examined in the exam. The Cisco Secure PIX Firewall exam is designed to test your knowledge on configuring, administering and monitoring the Cisco PIX firewall devices. The information provided in this Study Guide is specific to the 642-521 examination, and does not symbolize a complete reference work on the other four areas covered by the CCSP series of exams.

The following topics are covered in this Study Guide: Internal threats, External threats, Unstructured threats, Structured threats, Denial of service (DoS) attacks, Reconnaissance attacks, Access attacks, Cisco security wheel, The Security Policy, The Security Process, Inside Interface, Outside Interface, DMZ Area, Packet filters, Proxy filters, Stateful packet filters, URL filtering, Activation keys, Access modes, Default Interface names, Setting a Telnet password, Password recovery, PIX Firewall CLI Administrative Access Modes, PIX Firewall Common Commands, PIX Firewall Basic Commands, PIX Firewall Save and View Commands, The PIX Firewall Logging Commands, Trivial File Transfer Protocol (TFTP), Transport Protocols, Private Address Translations, Translation and Connection Tables, Controlling Traffic Using the Conduit Command, Controlling Traffic Using Access Lists, Content Filtering, Object Grouping, Basic System Management, Methods of Accessing the PIX Firewall, Dynamic Host Configuration Protocol (DHCP), Advanced PIX Firewall Features including Advanced Protocol Handling, PIX Firewall Routing, Attack Guards, Shunning, Intrusion Detection, Specifying a AAA Server, Configuring AAA Services, AAA and Access Lists, Command Level Authorization, The Failover Feature, Replication, Cable-based Failover Configuration, LAN-based Failover Configuration, IPSec's Security Protocols, Components and Modes, Configuring the IKE Parameters, Configuring the IPSec Parameters, Testing, Verifying and Debugging the IPSec Configuration, Configuring the PIX Firewall as an Easy VPN Remote Device, Scaling VPNs, Point-to-Point Protocol over Ethernet (PPPoE), Managing and Configuring the PIX Firewall with the PIX Device Manager (PDM), Creating a Remote Access VPN with the PDM, Creating a Site-to-site VPN with the PDM

Intended Audience

This Study Guide is targeted specifically for people that have efficiently finished the Cisco Secure PIX Firewall (CSPFA) class or those that have gained knowledge on Firewall devices who now desire to

complete the 642 -521 CCSP Cisco Secure Firewall exam. The information in this Study Guide is specific to that exam. It is not a complete reference work on the other four exam topics. Although our Study Guides are aimed at new comers to the world of IT, the concepts dealt with in this Study Guide are complex. Knowledge of Firewalls would be advantageous.

Note: Because Firewall technology is a vital component in network security, certain information contained in this Study Guide overlaps with content of the other four topics covered by the CCSP series of exams. This Study Guide does not combine all five exam topics.

How To Use This Study Guide

To benefit from this Study Guide we recommend that you:

- Study each chapter carefully until you fully understand the information. This will require regular and disciplined work. Where possible, attempt to implement the information in a lab setup.
- Be sure that you have studied and understand the entire Study Guide before you take the exam.

Good luck!

1. Network Security Threats

Technology, configuration and policy weaknesses can give rise to security problems. By connecting to public media, information is more readily accessible. In addition, technologies have vulnerabilities that can compromise the security of data. Because the vulnerability of data has become more evident, methods of protection against these attacks and threats have been identified and established.

1.1 The Main Types of Network Security Threats

Threats are classified into four types to enable a more profound understanding of them, and to aide the setting up of methods and procedures to guard against them. Threats are classified into the following four types:

- Internal threats
- External threats
- Unstructured threats
- Structured threats

1.1.1 Internal Threats

Internal threats are initiated by users like a displeased employee that has authorized access to the network. These threats can cause substantial losses and a fair amount of damage to a system. Unfortunately, internal threats are not easy to monitor and defend against. In many instances, systems have not been extended to be able to provide evidence, that certain damaging transactions were not authorized.

1.1.2 External Threats

External threats originate from individuals outside the organization. These individuals normally use the Internet or dial-up connections to try and violate security. External threats are hard to defend against as more and more organizations connect to the Internet, and supply external access to network resources. An organization is protected from external threats when they have no Internet or dial-up connection abilities.

1.1.3 Unstructured Threats

Unstructured threats are caused by a person with little honesty, who is usually inadequately skilled to create the threats on their own. The person uses tools that are built already or scripts that are available on the Internet. These persons are referred to as **script kiddies**. They are more motivated by an actual thrill than a premeditated thought on the damages and losses that they can cause.

1.1.4 Structured Threats

Structured threats are carried out by persons that have a premeditated thought on the actual damages and losses that they can cause. Greed, politics, terrorism, racism and criminal payoffs are possible reasons for structured threats. The attackers are highly skilled on network design and security, access procedures, and hacking tools. They have the skills to develop new attack techniques and the ability to modify existing hacking tools.

1.2 The Three Main Types of Network Attacks

Network attacks are classified according to the objective of the attack instead of the motivation of an attacker. The three main types of network attacks are discussed below.

1.2.1 Reconnaissance Attacks

This is an attack with the intent of gathering information on the network. The hacker attempts to map the network to find out what operating systems and address ranges are being used, and to identify any accessible open ports. This information can be gained by using ping sweepers, port scanners and Simple Network Management Protocol (SNMP). A reconnaissance attack normally takes place before an access attack or a denial-of-service attack.

1.2.2 Access Attacks

A hacker using this form of attack has the intent of capitalizing on a weakness in order to obtain access to a system or the network. These attacks originate from individuals that have no access to the organization's resources. Trojan horses and password hacking programs are used to obtain access. When access is obtained, the individual can modify or wipe out data, and add, modify or remove network resources. The attacker could also be able to install some means of 'access granting code' with the intent of using it at some future stage.

The different types of access attacks are listed below:

- **Unauthorized system access** entails the practice of taking advantage of operating systems' vulnerabilities in order to acquire access to a system.
- **Unauthorized privilege escalation** occurs when a lower level user attempts to obtain a higher level of access.
- **Unauthorized data retrieval** involves interpreting, altering and deleting confidential data.

1.2.3 Denial-of-Service Attacks (DoS)

These are attacks with the intent of ultimately denying authorized users access to the entire network. The attacker normally targets specific services and then floods the network with traffic. DoS attacks are the most destructive attacks to organizations that manage business over the Internet. The enormity of a DoS attack can be increased by initiating the attack against a single network from multiple computers or systems. This is known as a **distributed denial-of-service (DDoS)** attack. Network administrators can experience great difficulty in fending off these attacks, because blocking all the attacking computers, can also result in blocking authorized users

1.3 The Security Policy

Establishing a secure network becomes a continuous process as network environments change and expand. Hackers continually detect new weaknesses and security flaws. A clearly defined security policy describes the organization's security objectives, the procedures to be put into practice to protect the organization's data and services, and the penalties for users violating the security policy. The security policy must define roles, responsibilities and also the strategies to be followed when a security violation occurs.

1.4 The Security Process

A security process is a continuous evaluation and modification effort aimed at improving the organization's security position.

1.4.1 Securing an Environment

Tools that tackle various instances of vulnerability can be used to secure the environment. Devices like firewalls, intrusion detection systems, Cisco Secure Access Control Server (CSACS), and AAA servers, can be implemented to offer assistance in securing that the network resources are only available to authorized users. Firewalls can provide an additional layer of security by filtering incoming and outgoing traffic. IPSec that camouflage data moving over a non-secure public media can be employed to protect an organization's network resources. Remember to keep actual network devices in a secure computer room or data center, that is, behind locked doors.

1.4.2 Monitoring an Environment for Breaches and Attacks

By monitoring for security breaches, security administrators are more competent at figuring out the extent to which the environment is secured. Monitoring enables security administrators to proactively detect possible vulnerabilities and to verify that the security policy is being adhered to. Monitoring should take place continuously. Intrusion detection systems like Cisco Secure Intrusion Detection Systems (CSIDS) that offer exceptional monitoring capabilities can be used. Log files provide a means of recording user access data and system configuration changes.

1.4.3 Testing the Security of an Environment

Testing the security of the environment enables security administrators to decide on the efficiency of security implementations, and to verify that the security methods are endorsed by the security policy. Testing can also assist in revealing security defects. Cisco Secure Scanner can be used to test and reveal security defects.

1.4.4 Improving a Security Policy

Cisco's security wheel clearly illustrates that network security is a continuous monitoring, testing and refining process. Improvements such as new security tools or configuration modifications should be made to systems and policies as the need arises. It is good practice to monitor and be clued-up on the most recent threats, vulnerabilities and available tools.

The Cisco Security Wheel

The Cisco Security Wheel illustratively displays the constantly evolving security process. This process aims at securing the environment by securing, monitoring, testing and improving the security policy.

