brainbuzz.com™
Cramsession

Cramsession™ for Cisco Secure Pix Firewall Fundamentals

This study guide will help you to prepare for Cisco exam 9E0-559, Cisco Secure Pix Firewall Fundamentals. Exam topics include Firewall Feature and Installation, PIX Models, Designing Policies, Security Manager, and Security Strategies.

Check for the newest version of this Cramsession
http://cramsession.brainbuzz.com/checkversion.asp?V=2451957&FN=Cisco/cspff.pdf

Rate this Cramsession
http://cramsession.brainbuzz.com/cramreviews/reviewCram.asp?cert=Cisco+CSPFF

Feedback Forum for this Cramsession/Exam
http://boards.brainbuzz.com/boards/vbt.asp?b=656

More Cramsession Resources:

Search for Related Jobs
http://jobs.brainbuzz.com/JobSearch.asp?R=&CSRE

CramChallenge - practice questions
http://www.cramsession.com/signup/default.asp#day

IT Resources & Tech Library
http://itresources.brainbuzz.com

Certification & IT Newsletters
http://www.cramsession.com/signup/

SkillDrill - skills assessment
http://skilldrill.brainbuzz.com

Discounts, Freebies & Product Info
http://www.cramsession.com/signup/prodinfo.asp

Contents:

PIX Firewall Features

- Cut-through proxy
    - Challenges a user initially at the application layer
    - User is authenticated against an industry-standard database based on the Terminal Access Controller Access Control System (TACACS) or Remote Authentication Dial-In User Service (RADIUS)
    - After authentication and the policy check the PIX Firewall shifts the session flow and all traffic thereafter flows directly and quickly between the two parties while maintaining session state
    - Performs dramatically faster than proxy servers

- "Stateful" information
    - Each time a TCP connection is established information about the connection is logged in a stateful session flow table
    - The session flow table contains the source and destination addresses, port numbers, TCP sequencing information, and additional flags for each TCP connection associated with a particular host, and creates a connection object in the PIX Firewall
    - Inbound packets are compared against session flows in the connection table and are permitted through the Cisco PIX Firewall only if an appropriate connection exists to validate their passage

- IP address depletion
    - Mapping between local and global addresses is done dynamically or selectively
    - After a user-configurable timeout period an entry is removed and the global address is freed for use by another inside host
    - Dynamic address allocation is port specific

PIX Firewall Installation

- You need an ASCII terminal or a computer with serial communications software installed - Windows workstation, Macintosh system, or UNIX system

- Using a Macintosh requires a special cable that can be obtained from an Apple computer vendor
- On the computer or terminal you configure its terminal emulation program and also configure the serial port with these settings: 9600 baud, 8 data bits, no parity, and 1 stop bit
- Inside network cable must be connected to the interface connector labeled Ethernet1 or Token1, and outside network cable must be connected to Ethernet0 or Token0
- You can run the PIX Firewall Setup Wizard on a Windows PC connected to the PIX Firewall console port, the PIX Firewall Manager which is an HTTP-based graphical user interface for administering multiple PIX Firewalls on a Windows NT machine connected to the PIX Firewall's inside network, or access the command line interface from a PC or workstation connected to the PIX Firewall console port using a terminal emulator
- At the pixfirewall> prompt, enter the following commands to enter configuration mode:
    - pixfirewall> **enable**
    - Password:
    - pixfirewall# **configure terminal**
- to view the PIX Firewall help: pixfirewall(config)# **?**
- if you are installing PIX Firewall version 4.1 or later and have a Windows NT version 4.0 or later server, you can install the PIX Firewall Manager to monitor one or more local and foreign PIX Firewall units from a single management facility
- Upgrades for PIX can be downloaded from Cisco Connection Online:
    - pix4*nn*.bin--- PIX Firewall binary file
    - rawrite.exe--- conversion utility to create diskette that can be read by the PIX Firewall from the binary file
    - readme.txt
    - relnotes---release notes
- to install 2 PIX Firewall units in a failover configuration, you must connect the serial cable to the primary unit and not the secondary unit

- if your network has a WebSENSE server on any network interface, you can provide URL filtering through the PIX Firewall using the **url-sever** command
- to log FTP commands and WWW URLs when syslog is enabled, use "**show fixup"** to ensure that the **fixup protocol** commands for FTP and HTTP are in the configuration
- **"snmp-server"** command causes the PIX Firewall to send SNMP traps, making the firewall remotely manageable

Failover Configuration

- works by passing control to the Standby unit should the Active unit fail
- supported only between identical PIX Firewall models running the same software version and having the same config
- use the failover command without an argument, after you connect the optional failover cable between your primary firewall and a secondary firewall, to activate the feature
- use "**no failover"** in the configuration file for the PIX Firewall if you will not be using the failover feature
- use "show failover" to verify the status of the connection and to determine which unit is active
- when a failover occurs, each unit changes state - the newly Active unit assumes the IP and MAC addresses of the previously Active unit and begins accepting traffic. The new Standby unit assumes the failover IP and MAC addresses of the unit that was previously the Active unit. Because network devices see no change in these addresses, no ARP entries change and there are no timeouts anywhere on the network
- use "**write memory"** on the Active unit to save configuration changes to Flash memory on both the Active and Standby units
- Configuration changes made on the Standby unit are not replicated on the Active unit
- use the "**write standby"** command to manually save the configuration of the active failover unit to the standby failover unit from RAM to RAM
- Standby unit does not maintain the state information of each connection, and all active connections will be dropped when failover occurs, meaning that client systems must reestablish connections
- syslog messages are generated when a failover occurs
- when a failure is due to a condition other than power loss, failover will begin a series of tests when hello messages are not heard for two consecutive 15-

second intervals – tests include Link Up/Down test, Network Activity test, ARP test and Broadcast Ping test

Private Link

- works by checking packets that arrive at the PIX Firewall inside interface - **"link"** command creates an encrypted path between Private Link-equipped PIX Firewall units
- you can specify up to seven encryption keys - if you want seven keys, enter the **link** command in the configuration seven times
- key-ID and key values must be the same on each side of the Private Link
- after using the **link** command to add or delete link entries you should use "**write memory"** to store the configuration and reboot the PIX Firewall

Established Command

- allows the PIX Firewall to deliver traffic associated with protocols for which the firewall software does not have specific support
- only used in relatively unusual situations
- permitto and permitfrom parameters can be used to control which ports on the inside host can be reached from the outside – to be safe, the **established** command should always be used together with the **permitto** and/or **permitfrom** keywords
- there is no way to designate specific inside hosts to which the established command should or should not apply
- conduits created with the **static** and **conduit** commands allow the administrator to permit access from outside the firewall to selected ports on hosts inside the firewall

Other commands

- http://www.cisco.com/univercd contains a list of PIX Firewall commands and the level of support within the Cisco Secure Policy Manager
- http://www.cisco.com/univercd shows you a complete set of command references
- Command panel
    - Associated with each PIX Firewall node in the Network Topology tree

- Allows you to define device-specific commands that are not supported natively by Cisco Security Manager
- Present status messages about command set downloads, views of the currently published command sets
- Preserve existing command sets that you have defined for active PIX Firewalls
- To publish a new command set to the PIX Firewall and change the existing password, in the **Command** panel click "**Approve Now".** You must then specify the new enable password in the **Enable password** box in the **Enforcement** panel to allow future command sets to be published

Cisco Security Manager

- Process overview:
  - Define your Network Topology - Use the Topology Wizard to define the PIX Firewall, specify the Internet settings, and create required connecting networks. Also define the Cisco Security Manager server, define special hosts, define address hiding rules, and finally define static mapping rules
  - Define and apply your security policies - Populate the Security Policy Enforcement branch, then define and apply security policies
  - Define your logging and notification settings - specify audit event settings and verify PIX Firewall log settings
  - Generate, verify, and publish device-specific command sets - Perform Save and Update operation and Verify the generated command sets, then approve the command sets and publish them to the PIX Firewall
- Cisco Security Manager servers
  - at least one must be defined in the Network Topology tree
  - responsible for generating and distributing network policies
  - also for monitoring network traffic for suspicious activities and reporting

- Policy-based management
    - a high-level network policy enforced universally across your network devices without you having to understand all the device-specific rules and settings - you specify what you want to do without having to know the how-to
- Policy Database
    - proprietary knowledge-based subsystem
    - persistently stores configuration information as well as information and audit records generated by the Cisco Security Manager system
    - configuration information includes network objects, policies, administrative and user authentication accounts, as well as settings for the various Cisco Security Manager architecture subsystems and components
    - when an agent connects to the Policy Database, the agent and the Policy Database authenticate to each other using a bi-directional authentication method with a public-private key handshake
- Policy Enforcement Point PEP
    - identify a network device that accepts a policy from the Policy Distribution Point
    - enforces that policy against the network traffic traversing that network device
- Security policy abstract
    - template that identifies the rules about whether or not you want to allow network services across your network
    - abstract in nature as they are not dependent on the enforcement point - it actually represents a collection of condition branches
    - two states: active and inactive

  - active security policy abstract is applied to network objects within the Security Policy Enforcement branch of the Network Policy tree and are enforced by PEPs
  - inactive security policy abstract is defined under the Security Policy Abstracts branch of the Tools and Services tree and is representing a template for a specific implementation
  - bundled network service - collection of two or more network services

- Condition branch
  - represents a test that a PEP performs against a session request
  - determines whether to allow a particular session
  - comprises one or more conditions terminated by two terminal nodes
  - request is either accepted, rejected, processed by the next condition branch, or passed up to the next policy for further evaluation

- Policy Distribution Point
  - abstract term used to identify an installed subsystem in the Cisco Security Manager architecture
  - accepts intermediate policy descriptions from a Policy Generation Point and translates the policy description into a device-specific command set, then publishes the device-specific command sets to the PEPs

- Policy Monitor Point
  - an installed subsystem in the Cisco Security Manager architecture that monitors event streams produced by one or more PEPs

- Policy inheritance
  - use hierarchical lists of policies - ability is transferred all the way up to the Policy Enforcement branch if the policies below that branch use the "Use Next Policy action"

  - Dominance - an attribute of the lowest node to which a policy is applied
  - if parameters of a session request match two policies within a direct path, the one applied to the lowest node in that path is applied

- Internet node

  - represents the interconnected global network outside the control of the Cisco Security Manager
  - a gateway with a set of access points to the controlled networks where a network packet enters from one access point and leaves out another access point – a cloud
  - cloud network - special type of network that resides inside of a cloud, exists only as part of a cloud but not as a network in the Network Topology tree
  - you must attach at least one network to the Internet, and attach a gateway device to that network as well

- Security Policies Evaluation

  - the most specific security policy in relation to the network object is enforced first - the security policy that references the network object most specifically with the implicit "If Source is" statement is the one that regulates it

- Address hiding

  - Enhances network security by hiding your network's internal structure from external users
  - Permits almost unlimited number of users for one class D network address
  - No need to register IP address from the Internet Network Information Center
  - to define a hiding rule, you map one or more external IP addresses to an internal network address of any class

  - before hiding a network address the Policy Enforcement Point must have a route defined to access that network

- Secure communication

  - supports secure communications between independent web browsers and the reporting agent
  - all communication requests made from a web browser require the user to use a Cisco Security Manager administrative account
  - encryption mechanisms used between Cisco Policy Manager and the reporting agent are different from those used between a web browser and the reporting agent - all Cisco Policy Manager sessions are encrypted using a symmetric algorithm for bulk encryption
  - Cisco Policy Manager uses Microsoft Crypto API to perform encryption
  - session between a web browser and the reporting agent is encrypted using Secure Sockets Layer (SSL) 40-bit

- Troubleshooting

  - Cisco Policy Manager can import and export current configuration information into a flat file rather than storing it in the Policy Database. Apart from troubleshooting, this can act as a supplemental backup scheme for some types configuration information

- 6 key concepts of using Cisco Security Manager:

  - Define network topology from the outside to the inside
  - Keep global view of the network policy rather than a device-specific one
  - Understand the security stance
  - Apply security policies to have them enforced
  - Define logging and notification settings from a global view
  - Define all Cisco Security Manager servers in the network topology

Planning with Cisco Security Manager

- use the Topology Wizard to define the initial outside-to-inside structure - you define from the point of the access router belonging to your Internet service provider down into your network
- Policy Database is examined to determine whether it contains audit records that are older than the values specified in Event Purging - optimal value dependent on the number of audit records being generated versus the amount of disk space available
- address hiding rules map between an external, exposed IP address and an internal network or host address
- network Policy is not synchronized with Policy Database contents
- to ensure external hosts can reach the internal corporate web server and corporate e-mail server, a static translation rule is needed for each host
- static translation rules apply to all forms of IP traffic, and will override address hiding rules for a specific host

Designing Policies

- Instead of defining conduits and outbound, you define security policies that describe what traffic you want to allow into and out of your networks
- Process:
    - populate your Network Topology tree and add the network objects on which you want to enforce security policies to the Security Policy Enforcement branch of the Network Policy tree
    - construct security policies that permit or deny network services to the network objects on which you plan to enforce those security policies
    - instantiate those security policies by applying them in the Security Policy Enforcement tree
- Cisco Security Manager represents security policies, routing information, and other device-specific settings in a way not directly interpretable by a PEP, meaning that a translation process must take place to ensure that the device-specific command sets are generated – use the Save and Update command on the File menu
- you can publish the command to the PIX Firewall by approving them manually - the default publishing method
- you may configure auto publishing as well

Traffic Flow Rulings

- Routes panel
    - identifies the static rules that your Policy Enforcement Points use to route network packets correctly
    - Secure Policy Manager automatically presents all routes marked as "Implicit" on the basis of network interfaces and networks directly connected to a gateway object, and automatically derives all routes marked as "Derived" on the basis of your Network Topology definition
    - derived routing rules are published to the Policy Enforcement Points as part of the generated command sets
    - all static routing rules that have been defined using interfaces other than Cisco Secure Policy Manager are replaced by those routing rules that are defined using Cisco Secure Policy Manager
    - if you define a MANUAL routing rule that overrides a derived routing rule, the derived routing rule will no longer appear in the Routes panel. Also, no command set will be generated to enable that derived route
    - you can delete the MANUAL routing rule to have the derived routing rule generated and distributed as part of the command set
- as dynamic routing rules are updated via router-to-router communications, the dynamic routes are vulnerable to attack
- if you define a static translation rule for a Policy Distribution Point, you can cause a temporary command set publishing problem - the connection to the Policy Enforcement Point is broken after the new command set is published, as it effectively changes the address of the Cisco Secure Policy Manager host. To solve the problem, you can either define a temporary policy that permits the administrative network service from the old Policy Distribution Point address to the administrative network interface on the Policy Enforcement Points that use that Policy Distribution Point. Or you can use the Prologue option in the Command panel for the affected Policy Enforcement Points to specify that you want to accept administrative connections manually from the old IP address used by the affected Policy Enforcement Points

PIX hardware platform and its adaptive Security feature

- contains two Ethernet interfaces, one for inside and one for outside
- when packets arrive at the inside Ethernet, PIX checks to see if previous packets have come from the inside host. If not, a dynamic translation slot is

created in its state table that includes the inside IP address and the new globally unique IP address drawn from the virtual network of up to 64K host addresses. It then changes the IP address, the checksums, and other aspects of the packet and forwards the packet to the outside interface

- when a packet arrives at the outside interface, it must first pass the PIX Firewall Adaptive Security criteria. If passed, PIX removes the destination IP address and the internal IP address is inserted in its place for forwarding to the inside interface
- Adaptive Security (AS) = stateful approach of inspection:
    - allows any TCP connections that originate from the inside network
    - ensures that there is already an FTP control connection between that translation slot and the remote host if an FTP data connection is initiated to a translation slot
    - drops and logs attempts to initiate TCP connections to a translation slot from the outside, as well as source routed IP packets sent to any translation slot on the PIX Firewall
    - allows ICMP of types 0, 3, 4, 8, 11, 12, 17 and 18 and ICMP type 5 and others
    - drops ping requests to dynamic translation slots
    - answers ping requests directed to static translation slots
- exceptions to the previously described rules can be created with the conduit command, and multiple exceptions are possible

PIX Command Guidelines and Summary

- When entering commands, you can:
    - erase characters with the Backspace and Del keys
    - erase a previous word with ^W
    - erase a previous line with ^U
    - redisplay a line with ^R

- Commands

    - Apply - apply an access list
    - access_list – create an access list
    - no access_list – delete an access list
    - show access_list – view the access list
    - arp – adjust the arp setting
    - clear arp-cache - flush the arp cache
    - show config – display current configuration
    - ifconfig – configure Ethernet interface
    - ifstat - interface statistics
    - clear_config - clear flash memory
    - restore – reload config info from flash
    - save - write configuration to flash
    - kill - terminate a login session
    - who – view IP address origination
    - reboot – reboot PIX
    - route – adjust routing table
    - link / no link – enable or disable private link
    - link_stat – show private link status
    - rip / no rip – enable or disable RIP settings
    - loghost – view or assign syslog
    - telnet / no telnet – enable or disable telnet access
    - mem – show the uptime for PIX

Different Models of PIX

- 4 models: PIX Firewall 515-R, PIX Firewall 515-UR, PIX Firewall 520, PIX Firewall 520-DC
- detailed hardware specs can be found at http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pie_ds.htm

PIX Private Link encryption card

- Data Encryption Between Multiple PIX Firewall Systems – for building VPN
- uses Data Encryption Standard (DES) plus incorporates the IETF Authentication Header/Encapsulating Security Payload (AH/ESP) protocols
- up to seven preshared keys can be changed at preset times
- can directly connect up to 256 other sites

PFM PIX Firewall Manager

- To install, you should log into the Windows NT machine locally (not the domain) as "administrator"
- PFM installation needs to create a local SAM (Security Access Management) database for PFM access, which is usually not possible with default PDC or BDC installations
- if after installing the PFM NT keeps on beeping - an application port conflict - a syslog application such as Cisco Works, PIX Firewall Syslog Server [PFSS], or a third-party application may already be listening on UDP 514, or a web server is already occupying the PFM default TCP port 8080. Try to uninstall, find a clean port and reinstall.
- you are suggested not to install PFM on a machine running Internet Information Server (IIS) so as to avoid possible server ports conflicts
- Firewall Manager requires a static IP Address rather than a DHCP one
- the default administrator name is “pixadmin” and the default password is “cisco”, with read/write configuration abilities.
- default user username/password is pixuser/cisco, with read only capability
- User manager on the server allows you to add, change, or delete users to the pixadmins or pixusers groups
- pfm.log is the log file for troubleshooting problems
- if you lose your password..... to use the password recovery procedure, you need the PIX Password Lockout Utility - rawrite.exe, plus one of the following files depending on the PIX software version you are running - nppix.bin (4.3 and earlier releases)/np44.bin (4.4 release)/np50.bin (5.0 release)/np51.bin (5.1 release). A registered user can download these files from Cisco. Also, the user can open a case with Technical Assistance Center (TAC) to obtain the file

Security Strategies

- for Cisco recommended security strategies please visit http://www.cisco.com/warp/public/707/advisory.html

Special Thanks to Michael Yu for contributing material for this Cramsession. Make sure to visit his site at: http://michaelyu.freeservers.com