The CSPFA Cram Sheet

This Cram Sheet contains distilled, key facts about Cisco PIX firewalls. Review this information as the last thing you do before you enter the testing center, paying special attention to those areas in which you feel you need the most review. You can transfer any of these facts from your head onto a blank sheet of paper immediately before you begin your exam.

INTRODUCTION TO NETWORK SECURITY THREATS

- The Security Wheel components are secure, monitor, test, and improve.
- Types of attacks include internal threats, external threats, unstructured threats, and structured threats.
- Types of attacks include reconnaissance attacks, access attacks, denial-of-service (DoS) attacks and distributed denial-of-service (DDoS) attacks.

BASICS OF THE PIX FIREWALL

- The types of firewalls include
  - *Packet filters*—These monitor source and destination layer 3 and 4 information with no session information and are based on ACL.
  - *Proxy servers*—These operate as middlemen, maintaining session connections between themselves and the client and between themselves and the destination systems. They typically run on other multipurpose operating systems.
  - *Stateful packet filters*—These monitor traffic as packet filters do; however, they record the traffic into connection and xlate tables to allow only requested traffic back into the system. The PIX uses stateful packet filters.
- The Adaptive Security Algorithm controls traffic flow through the PIX firewall, performing stateful inspection of packets.
- The PIX firewall supports WebSense and N2H2 content services.
- The security levels include
  - *Security Level 100*—This is the highest level and is set on the inside (trusted) interface.
  - *Security Level 0*—This is the lowest level and is set on the outside (untrusted) interface.
  - *Security Level 50*—This typically is set on the DMZ interface and can access lower security levels but not higher security levels.
- The PIX models are described in the following table.

Model	501	506E	515E	525	535
Throughput	10Mbps	20Mbps	188Mbps	360Mbps	1Gbps+
Interfaces	2	2	6	8	10
Failover	No	No	Yes	Yes	Yes
VAC	No	No	Yes	Yes	Yes

- The PIX 535 interface slots are as follows:

Interface Slots	Bus Speed
Slots 0 and 1	64-bit/66MHz
Slots 2 and 3	64-bit/66MHz
Slots 4 to 8	32-bit/33MHz

- The PIX interface cards are as follows:

PIX-1FE	32-bit/33MHz
PIX-4FE	32-bit/33MHz
PIX-VPN-ACCEL	32-bit/33MHz
PIX-1GE-66	64-bit/66MHz

SETTING UP A PIX FIREWALL

- The firewall modes include
  - *Unprivileged*—Enables you to change the current setting to privileged mode or logout. Its prompt is `pixfirewall>`.
  - *Privileged*—Enables you to view restricted settings on the system. Its prompt is `pixfirewall#`.
  - *Configuration*—Enables you to change system configurations. Its prompt is `pixfirewall(config)#`.
  - *Monitor*—Enables you to upload images over the network. Its prompt is `monitor>`.
- The six basic commands include
  - *`nameif`*—Assigns a name and sets the security level to a hardware ID interface
  - *`interface`*—Sets the interface speed and enables the interface
  - *`ip address`*—Assigns an IP address to a named interface
  - *`nat`*—Creates a NAT ID that defines which local IP addresses will be translated on a specific named interface
  - *`global`*—Creates a global list of addresses to be used by the NAT ID
  - *`route`*—Creates any necessary static routes or defaults routes
- The `show version` command displays flash contents.
- The `passwd` command changes the Telnet password.
- The `copy tftp flash` command copies the images to the flash.

TRANSLATIONS AND CONNECTIONS

- The translation table contains layer 3 IP address mappings and is commonly known as the xlate table. Use the `show xlate` command to display the contents and the `clear xlate` command to clear the contents of the table.
- The connection table contains layer 4 TCP or UDP sessions. Use the `show conn` command to display the contents and the `clear conn` command to clear the contents of the table.
- To allow traffic inbound, you need to use an ACL or a `conduit` with a `static` mapping.
- NAT is dynamic inside to outside layer 3 IP address-to-IP address mapping; PAT is dynamic inside to outside layer 3 plus layer 4 IP address and port-to-IP and port mapping.
- The `static` command is used to create a one-to-one IP address mapping or a one-to-one port to address mapping.
- The `nat 0` command tells the PIX not to perform translation on an IP address as it passes through the firewall. It is commonly used when public addresses are on the inside of a firewall and don't need translating.
- The static or NAT parameter called `max_conns` is used to define the maximum TCP connections permitted.
- The static or NAT `em_limit` parameter sets the maximum number of embryonic or half-open connections, which is used to prevent SYN attacks.

ACCESS CONTROL LISTS AND TRAFFIC CONTROL

- The `conduit` command always needs to be paired with a `static` command.
- Turbo ACLs are very simple to create and work on all models of the PIX except the 501. The 501 does not support Turbo ACLs. Turbo ACLs are typically not used on smaller firewall models because they require too much memory.
- `conduit` or ACL commands always need to be paired with a `static` command to permit traffic initiated from a lower security level interface to reach a higher security level interface.
- The order of the `conduit` and `access-list` commands is as follows:
  - `conduit permit tcp (DESTINATION)(SOURCE)`
  - `access-list 101 permit tcp (SOURCE)(DESTINATION)`
- Interfaces can have only one ACL attached to them in the inbound direction. Use the `access-group` command to attach the ACL to an interface. ACLs also take precedence over conduits.
- When working on large, complex access lists, object groups enable you to save on the number of entries needed to create the access list. The following are the object group types and commands:
  - *`object-group network`*—Defines a group of hosts or subnets. The following commands create a network object-group:

    ```
    (config)# object-group network TheNetworkList
    (config-network)# network-object host 10.0.0.1
    ```

  - *`object-group services`*—Defines a group of TCP and UDP port numbers. The following commands create a service object group:

    ```
    (config)# object-group service ThePortList tcp
    (config-service)# port-object eq telnet
    ```

  - *`object-group protocol`*—Defines a group of IP protocols, such as IP, ICMP, TCP, and UDP. The following commands create a protocol object group:

    ```
    (config)# object-group protocol TheProtocolList
    (config-protocol)# protocol-object tcp
    ```

  - *`object-group icmp-type`*—Defines a group of ICMP messages. The following commands create an ICMP object group:

    ```
    (config)# object-group icmp-type TheICMPList
    (config-icmp-type)# icmp-object echo
    ```

SYSTEM MANAGEMENT

- The SSH uses the username of the PIX firewall and the current Telnet password.
- When you see the period symbol (`.`), the PIX is generating server keys to use for encryption.
- The PIX supports SSH version 1 with up to five connections.
- The `ca zeroize rsa` command clears all RSA-generated keys from flash.
- The `ntp server` command enables you to synchronize the PIX clock with an NTP server.
- The `reload` command is used to reboot the PIX.
- The `logging host` command allows syslog servers to receive system messages.
- The `logging trap` command enables the log levels for syslog traps.

ADVANCED PROTOCOL HANDLING AND PIX FIREWALL FEATURES

- When in standard FTP mode, the inside client initiates the control connections to the FTP server and the server initiates the data connections. You use the `fixup protocol ftp 21` command to allow the PIX to create a dynamic return connection for the data returning from the server.
- When in passive FTP mode, the inside client initiates both the control and data connections, so the ASA will allow return traffic through the PIX without a need for the `fixup protocol ftp 21` command.
- The `show fixup` command displays the active fixup protocols on the PIX firewall.
- The PIX supports the SCCP, Skinny, SIP, and H.323 VoIP protocols.
- RTSP is a real-time audio and video protocol used by several multimedia applications, such as RealPlayer, Cisco IP/TV, Quicktime 4, Netshow, and VDO live. The `fixup protocol rstp` command enables RTSP support for NAT only.
- WebSense and N2H allow URL traffic filtering when fixup protocol HTTP 80 is enabled.
- The `filter URL` command is used to identify which traffic you want to forward to the URL servers.
- The PIX firewall can be a DHCP client and a DHCP server at the same time.
- The `dhcpd dns` command allows you to set only two DNS server IP addresses.
- When configured, PPPoE can connect to the service providers without user interaction.

ATTACK GUARDS AND INTRUSION DETECTION

- DNSGuard prevents DoS and UDP session hijacking by closing the UDP port after the first received DNS response.
- The SYN Floodguard protects hosts from TCP SYN attacks, which are half-open connections (called *embryonic* connections) from hackers.The embryonic limit is a parameter in the `nat` and `static` commands.
- Embryonic connections are half-open, three-way handshake connections that could be left open intentionally by a hacker. If the embryonic limit is reached, TCP intercept on the PIX handles any new handshakes until they are proven to be valid requests. This feature was introduced in version 5.2.
- The `fixup protocol smtp` command inspects SMTP traffic and allows only the following seven commands: `DATA`, `HELO`, `MAIL`, `NOOP`, `QUIT`, `RCPT`, and `RSET`.
- The `shun` command is used for IDS blocking of inbound source traffic.
- The PIX firewall contains a subset of the signatures of a full Cisco IDS system.
- By default, all IDS audit signatures are enabled. If you want to disable them, use the `ip audit signature <number> disable` command.
- The `ip audit interface <if_name> <name>` command applies an audit policy to an interface.
- False positives are alarms triggered by legitimate traffic that matches a pattern of a monitored signature.
- The embryonic parameter is used by the `nat` and `static` commands.

AAA CONFIGURATION

- The `privilege` command is used to assign a specific command to a specific privilege level.
- During the Cisco Secure ACS install, you are prompted for an NAS IP address called `access server name`. This is the IP address of the PIX firewall.
- The cut-through proxy enables you to control standard ports for HTTP, FTP, and Telnet services through the PIX firewall.
- Virtual HTTP is used to prevent caching problems with Web browsers.
- Virtual Telnet can be used when nonstandard port access is needed. HTTP, FTP, and Telnet are the standard ports.
- Named ACLs are shared among several users and are downloaded only once during authentication. Unnamed ACLs are not shared and are downloaded during authentication.
- Downloadable ACL can be performed only with RADIUS protocol, not TACACS+.
- AAA stands for authentication, authorization, and accounting. You cannot have authorization without successful authentication first.
- TACACS+ uses TCP for connections between AAA servers and clients, whereas RADIUS uses UDP connections.
- The AAA command parameter `local` specifies the use of the local database for usernames and passwords.
- The `aaa-server` command specifies the location of the AAA services: local, RADIUS, or TACACS+.
- When users fail authentication, their basic connections are dropped.

FAILOVER

- Non-stateful failover does not replicate xlate and connection table information.
- Stateful failover replicates xlate and connection table information.
- Stateful failover requires an extra LAN interface to interconnect the two firewalls.
- Cable-based configuration requires a special serial cable with one end labeled “primary” and the other end labeled “secondary.”
- LAN-based configuration requires a dedicated switch or hub to interlink the two PIX firewalls. Do not use a crossover cable.
- LAN-based and cable-based failovers both support configuration on the primary firewall and stateful failover.
- When a primary interface fails, the secondary becomes active and inherits the primary’s IP and MAC addresses. The primary moves into a fail or standby state and assumes the secondary firewall’s IP and MAC addresses.
- Failover requires the hardware models, RAM sizes, flash memory sizes, and software versions to be the same.
- Failover is not supported on the 501 or 506 models.
- RAM configuration information is replicated automatically to the standby firewall.
- The `write standby` command can be used to force a replication of the RAM configuration in memory to the standby firewall.
- The `failover active` command is used to enable failover on the PIX firewall.
- Hello messages are sent across all the interfaces and, if two messages are missed, the failover process begins.
- The four failover tests are
  - NIC status
  - ARP
  - Network activity
  - Ping
- The network activity test monitors for traffic for 5 seconds. If no traffic is found, the PIX moves to the next test (the ARP test)—not standby mode.

IPSEC AND VIRTUAL PRIVATE

- Authentication headers (AHs) provide data integrity, anti-replay, and data origin authentication.
- Encapsulating Security Payload (ESP) provides data integrity, anti-replay, data origin authentication, and data confidentiality.
- The maximum number of transformations in the `crypto ipsec transform-set` command is three.
- The `ip local pool` command is used to create a pool of IP addresses used by remote access clients using PPTP or L2TP.
- Internet Key Exchange (IKE) is a hybrid protocol used to exchange keys.
- AH and ESP can both be used at the same time. ESP is performed first and then encapsulated inside the AH.
- The `clear ipsec sa` command is used to delete or clear all the current security associations.
- Security associations can be created using either IKE dynamically or a manual process.

THE PIX DEVICE MANAGER

- The Pix Device Manager (PDM) performs an interactive setup automatically when the PIX firewall has not been configured.
- The PDM is supported on Windows, Linux, and Sun Solaris operating systems.
- When unsupported PDM commands are found, the PIX firewall allows only the monitoring tab to be available.
- The five main configuration areas are Access Rules, Translation Rules, VPN, Host/Networks, and System Properties.
- The auto update configuration settings are configured on the System Properties tab under the Auto Update link.

ADVANCED MANAGEMENT

- Cisco Secure Access Control Server (CSACS) is used to manage AAA services.
- CiscoWorks is an enterprise tool used to monitor, manage, and configure Cisco devices. CiscoWorks’ default port is 1741.
- The CiscoWorks Management Center for PIX Firewalls (PIX MC) uses a Web-based interface for configuring and managing multiple PIX firewalls and Firewall Services Modules (FWSMs).
- The PIX MC provides the capability to group devices with similar attributes. By using the Devices tab, you can create more groups. However, the default group is called Global Group.
- The PIX MC provides mandatory or default rules for groups or devices. Keep the following in mind:
  - *Mandatory rules*—These cannot be overridden, are applied at the group, and are ordered down to a device.
  - *Default rules*—These can be overridden and are ordered from the device up to the enclosing groups.
- The CiscoWorks Auto Update Server (AUS) is used to upgrade device software images and configuration files. The AUS’s default port is 443.
- The Auto Update Server configuration tabs are as follows:
  - *Devices*—Provides summary information
  - *Images*—Displays information about images, PDM images, and configuration files and allows you to add and remove firewall and PDM images
  - *Assignments*—Enables you to change device-to-image and image-to-device assignments
  - *Reports*—Displays reports
  - *Admin*—Performs administrative tasks, such as changing passwords