- The PIX OS Command-Line Interface -

PIX OS Versions

The operating system for Cisco PIX/ASA firewalls is known as the **PIX OS**. Because the PIX product line was acquired and not originally developed by Cisco, PIX OS versions up to **6.0** featured a command-line interface that was similar to, but not exactly like, the Cisco IOS.

Cisco blended features from the Cisco IOS and PIX OS to form **PIX OS 7.0.** While PIX OS 6.0 (and prior) and PIX OS 7.0 are similar, there are key differences, which will be reflected in this guide.

Cisco ASA firewalls support PIX OS 7.0 exclusively.

Basics of the PIX OS CLI

As with the Cisco Router IOS, there are various **modes** in the PIX OS CLI, each of which contains a set of commands specific to the function of that mode.

By default, the first mode you enter when logging into the PIX OS is User mode. User mode appends a ">" after the device hostname:

pixfirewall>

No configuration can be changed or viewed from User mode. Only basic status information can be viewed from this mode, and thus user mode is mostly used to authenticate to higher privileged modes.

Privileged mode allows all configuration files, settings, and status information to be viewed. Privileged mode appends a "#" after the device hostname:

pixfirewall> *enable PASSWORD*
pixfirewall#

Very little configuration can be *changed* directly from Privileged mode. Instead, to actually configure the Cisco device, one must enter **Global Configuration mode:**

pixfirewall# *config terminal*
pixfirewall(config)#

* * *

Basics of the PIX OS CLI (continued)

Unlike the Cisco IOS, no *interface* or *routing* configuration modes existed in PIX OS 6.0 – all configuration was done within Global Configuration mode. In PIX OS 7.0, several sub-modes under Global Configuration exist, very similar to the Cisco IOS. These differences will be highlighted shortly.

Like the Cisco IOS, the PIX OS supports **shortcuts** as long as the command is not ambiguous.

Additionally, the PIX OS supports **context-sensitive help** through the use of the **question mark** (**?).** Typing the question mark (?) at the command prompt provides a list of all commands available at that mode. Typing in a command followed by a question mark provides the options, arguments, and full syntax for that command.

Cisco PIX/ASA firewalls employ the following configuration files:

- **running-config** - stored in **RAM,** contains the *active* configuration
- **startup-config -** stored in **Flash,** contains the *saved* configuration

To view the running-config:

pixfirewall# *show running-config*
pixfirewall# *write terminal*

To view the startup-config:

pixfirewall(config)# *show startup-config*
pixfirewall(config)# *show configure*

To *copy* the running-config to startup-config:

pixfirewall(config)# *write memory*

To *erase* the startup-config:

pixfirewall(config)# *write erase*

Unlike the Cisco IOS, all show commands can be executed directly from Global Configuration mode as well:

pixfirewall(config)# *show running-config*
pixfirewall(config)# *write terminal*

* * *

Basics of the PIX OS CLI (continued)

The enable password protects the PIX/ASA's Privileged mode. To set this encrypted password:

pixfirewall(config)# *enable password PASSWORD*

To set the firewall hostname:

pixfirewall(config)# *hostname MYFIREWALL*
MYFIREWALL(config)#

To restart the firewall:

pixfirewall(config)# *reload*
pixfirewall(config)# *reload noconfirm*

PIX OS "show" Commands

To view version and licensing information:

pixfirewall(config)# *show version*

To view physical and data-link information about interfaces:

pixfirewall(config)# *show interface*

To view IP addresses configured on interfaces:

pixfirewall(config)# *show ip address*

To view memory and CPU information:

pixfirewall(config)# *show memory*
pixfirewall(config)# *show cpu usage*

To troubleshoot connectivity issues using ping:

pixfirewall(config)# *ping 192.168.1.1*

* * *

PIX OS and Time

To set the system time on a PIX/ASA firewall:

pixfirewall(config)# *clock set 11:02:14 jan 10 2003*

To set the timezone:

pixfirewall(config)# *clock timezone EST -5*

To view the time:

pixfirewall(config)# *show clock*

To securely point to a centralized Network Time Protocol (NTP) server:

pixfirewall(config)# *ntp authenticate*
pixfirewall(config)# *ntp authentication-key 1 md5 MYKEY*
pixfirewall(config)# *ntp server 10.1.1.1 key 1 source inside*

PIX Firewall Interfaces

Cisco security appliances protect **trusted** zones from **untrusted** zones.

Like most firewalls, a Cisco PIX/ASA will **permit** traffic from the *trusted* interface to the *untrusted* interface, **without** any explicit configuration. However, traffic from the *untrusted* interface to the *trusted* interface must be **explicitly permitted.**

Thus, any traffic that is not explicitly permitted from the untrusted to trusted interface will be **implicitly denied.**

To control the *trust* value of each interface, each firewall interface is assigned a **security level**, which is represented as a **numerical value** between **0 – 100** on the Cisco PIX/ASA. A **higher** security level is *more trusted*, whereas a **lower** security level is *less trusted***.**

To explicitly allow a *less trusted* interface to communicate with a *more trusted* interface, an **access control list (ACL)** must be used.

* * *

Configuring Firewall Interfaces – PIX OS 6.0

PIX OS 6.0 (and prior) does not support an Interface Configuration Mode – all interface-related configuration is accomplished directly from Global Configuration mode.

To name an interface, and assign it a security level of *75*:

pixfirewall(config)# *nameif ethernet1 OUTSIDE security75*

To change the duplex and speed of an interface:

pixfirewall(config)# *interface ethernet1 100full*

To administratively shutdown an interface:

pixfirewall(config)# *interface ethernet1 100full shutdown*

To assign an IP address to an interface:

pixfirewall(config)# *ip address OUTSIDE 192.168.1.10 255.255.255.0*

Notice when applying Layer-3 configuration, the interface *name* is referenced.

Configuring Firewall Interfaces – PIX OS 7.0

PIX OS 7.0 was redesigned and functions *very* similarly to the Cisco IOS. It provides an Interface Configuration Mode for all related configuration.

To configure an interface on a PIX OS 7.0 device:

asafirewall(config)# *interface GigabitEthernet0/0*
asafirewall(config-if)# *no shutdown*
asafirewall(config-if)# *nameif OUTSIDE*
asafirewall(config-if)# *security-level 75*
asafirewall(config-if)# *ip address 192.168.1.10 255.255.255.0*

The above *GigabitEthernet0/0* interface was taken out of a *shutdown* state, assigned a *name* of *OUTSIDE*, assigned a *security-level* of *75*, and an *ip address* of *192.168.1.10*.

* * *

Configuring the PIX DHCP Server

Cisco PIX/ASA Firewalls support a built-in DHCP server to delegate addresses to hosts. DHCP servers **lease** out IP addresses to DHCP clients, for a specific period of time. There are four steps to this DHCP process:

- When a DHCP client first boots up, it broadcasts a **DHCPDiscover** message, searching for a DHCP server.
- If a DHCP server exists on the local segment, it will respond with a **DHCPOffer,** containing the "offered" IP address, subnet mask, etc.
- Once the client receives the offer, it will respond with a **DHCPRequest**, indicating that it will accept the offered protocol information.
- Finally, the server responds with a **DHCPACK**, acknowledging the clients acceptance of offered protocol information.

To specify the DHCP Pool:

pixfirewall(config)# *dhcpd address 192.168.50.1-192.168.50.50 inside*

To configure DHCP options:

pixfirewall(config)# *dhcpd dns 172.16.1.1 172.16.1.2*
pixfirewall(config)# *dhcpd wins 172.16.1.3 172.16.1.4*
pixfirewall(config)# *dhcpd domain helpme.please*

To specify the DHCP lease length (in seconds, default is **3600**):

pixfirewall(config)# *dhcpd lease 50000*

Finally, the DHCP server must be enabled on the necessary interface:

pixfirewall(config)# *dhcpd enable inside*

* * *

Enabling SSH Access

SSH (Secure Shell) is the preferred method of remoting into a Cisco PIX/ASA device. The traditional method of telnet is inherently insecure, as it sends all passwords/traffic in clear-text.

SSH requires a local username and password configured on the device:

pixfirewall(config)# *username CHARLIE password BROWN*

Next, the authentication policy for SSH must be configured to use the local database:

pixfirewall(config)# *aaa authentication ssh console LOCAL*

The above command creates an *aaa authentication* policy for *ssh*, to provide *console* access if the user successfully authenticates with the *LOCAL* username/password database.

SSH must then be *enabled* on one or more interfaces:

pixfirewall(config)# *ssh 0.0.0.0 0.0.0.0 inside*
pixfirewall(config)# *ssh 0.0.0.0 0.0.0.0 outside*

An SSH timeout can then be specified (value is in minutes):

pixfirewall(config)# *ssh timeout 10*

Finally, the SSH key must be generated. To accomplish this on a PIX OS 6.0 device:

pixfirewall(config)# *ca generate rsa key 2048*

To generate the SSH key on a PIX OS 7.0 device:

asafirewall(config)# *crypto key generate rsa general-keys modulus 2048*

The larger the specified modulus size, the stronger the key. However, a stronger key will take longer to generate.

* * *