Cisco security appliances

Overview

Cisco offers the PIX firewall solution, acquired from Network Translation in 1995, along with the original Centri firewall which ran on the Windows NT® operating system. The Cisco PIX, however, runs its own proprietary system called PIX OS, currently at version 7. The PIX is a packet filtering firewall with stateful inspection, and there are several DPI features in the newer versions which enhance the rules that can be created.

The Cisco PIX is available in a small SOHO unit and a rack-mount form factor. More recently, Cisco introduced some of the PIX functionality in the Cisco ASA. Cisco also offers the FWSM in a blade form factor for the larger chassis router. This has been updated to the same code level as the Cisco PIX.

The Cisco PIX and ASA have numerous features including:

- purpose-built security appliances
- stateful packet inspection
- routed, NAT and bump-in-the-wire operation
- user authentication of connections
- protocol and application inspection engines for Layer 4 through 7
- VPN connectivity for site-to-site and as endpoints
- virtual firewalls
- stateful failover.

PIX versus ASA

Changes to the product range mean Cisco PIX Firewalls have been renamed Cisco PIX Security Appliances. This has resulted in the creation of a security appliance family which includes both the PIX and ASA devices, as well as the Cisco FWSM and the basic Cisco IOS firewall.

The Cisco ASA is not a direct replacement for the Cisco PIX, but an enhancement in technology. With the convergence of the code at version 7, the Binary and ASDM image files support both platforms.

The Cisco ASA supports the following additional features over a Cisco PIX:

- web-based VPN
- VPN load balancing
- upgradeable module slot

- CF card support
- aux port support.

Placing the SSM into the Cisco ASA provides additional services to the host device. The IPS 5.0 software can be supplied in either inline mode or as a more traditional IDS monitoring operation. The SSM device also provides a dedicated Gigabit port for out-of-band management or can be managed as a session across the backplane in a similar fashion to the way 6500 series routers managed routing and switching with IOS and CatOS.

FireWall Service Module

The Cisco FWSM provides an integrated firewall module to be installed in the 6500 and 7600 router chassis. The FWSM has been recently upgraded to run the same version of code as the PIX and ASA.

There are a number of advantages and disadvantages to using the FWSM. The device can support far more connections at faster wirespeed than either the PIX or ASA, but lacks the additional functionality that the ASA now provides, such as IDS, IPS and VPN termination. The FWSM can provide 5Gbit/s throughput and a million concurrent connections. One of the key benefits is support for 1000 virtual interfaces (256 per virtual firewall) and a maximum of 4000 VLANs allowing the unit to scale for any campus organisation. Failover can be configured in Active/Passive or Active/Active for either two cards in one chassis or a card in two chassis for full inter-chassis failover.

Versions of PIX OS

There have been many recent developments to the code that runs on the Cisco PIX. A number resulted from the release of the Cisco ASA and both code trains merged in version 7.

Some of the new features include:

- time-based ACLs
- no NAT requirement
- security contexts
- bump-in-the-wire firewall
- inspection support for FTP, ESMTP, NIS+, RPC, ICMP, H323, GTP, MGCP, RTSP
- modular policy framework
- application firewall enhancements
- Active/Active failover configuration
- SSHv2 support
- SNMP v2c support.

In the past, the Cisco PIX always required NAT configuration, which precluded the implementation of the device in many situations. The newer version of the code introduces the command **nat-control** which can be negated in the usual manner to turn off the NAT requirement.

Modular Policy Framework enhancements have been imported from QoS implementation to bring the class-map, policy-map and service-policy functions to the Cisco PIX and ASA. Changes have also been made to the syslog functionality in version 7 of the code. There are 36 configurable parameters. One of these includes the Event List function which provides a

method for the aggregation of certain types of messages internally before forwarding them to syslog for processing.

Application firewall enhancements improve the filtering of content transmitted using port 80. A number of rules analyse the content to block tunnelling, peer to peer and other malformed HTTP requests.

To determine the version of firewall code running on the device, the command **show version** can be used. This command also displays information about interfaces, licenses and codes.

Firewall# sh ver

Cisco PIX Security Appliance Software Version 7.0(4)

Device Manager Version 5.0(4)

Compiled on Thu 13-Oct-05 21:43 by builders

System image file is “flash:/image”

Config file at boot was “startup-config”

Firewall up 46 mins 56 secs

Hardware: PIX-515E, 64 MB RAM, CPU Pentium II 433 MHz

Flash E28F128J3 @ 0xfff00000, 16MB

BIOS Flash AM29F400B @ 0xfffd8000, 32KB

0: Ext: Ethernet0 : address is 0017.5976.5508, irq 10

1: Ext: Ethernet1 : address is 0017.5976.5509, irq 11

2: Ext: Ethernet2 : address is 000e.0ca9.40c9, irq 11

Licensed features for this platform:

Maximum Physical Interfaces : 3

Maximum VLANs : 10

Inside Hosts : Unlimited

Failover : Disabled

VPN-DES : Enabled

VPN-3DES-AES : Disabled

Cut-through Proxy : Enabled

Guards : Enabled

URL Filtering : Enabled

Security Contexts : 0

GTP/GPRS : Disabled

VPN Peers : Unlimited

This platform has a Restricted (R) license.

Serial Number: 810000000

Running Activation Key: 0x00000000 0x00000000 0x00000000

0x00000000 0x00000000

Configuration last modified by enable_15 at 13:20:29.106 UTC

Thu Jan 4 2007

Configuration using the GUI

The Cisco PIX and ASA security appliances are provided with a graphical management tool, the ASDM. The ASDM replaces the previous graphical tool, the PIX Device Manager. The ASDM can be used to configure, manage and monitor one or more of Cisco's security appliances. It allows for five simultaneous connections, or five per context, 32 in total when using virtual firewall contexts. It requires a Java VM which allows platform-agnostic execution and the traffic is encrypted by DES or 3DES depending on the license installed on the host device.

In the home window, the ASDM provides an overview of the security appliance with general information on the device:

- hostname
- device version
- ASDM version
- firewall mode
- total flash memory
- device uptime
- device type
- context mode
- total memory.

Other panes in the window provide:

- interface status
- VPN status
- system resource allocation
- traffic status

- syslog messages.

Configuration using the CLI

The Cisco PIX and ASA security appliances are based on the command set found in Cisco IOS. They have the same 16 privilege levels and have four administrative access modes. The first access mode is unprivileged, which is shown by the right angled bracket character. This is the first access mode entered when connecting to a device via either the serial console, telnet or SSH.

Firewall>

The second access mode is privileged and is shown by the hash character. Privileged access is enabled by entering the **enable** command and password if set.

Firewall>

Firewall> enable

Firewall#

Configuration mode allows configuration changes to be made to the system and this is shown by the **(config)** flag. Configuration access is granted by the command **configure terminal** (or **conf t**.).

Firewall>

Firewall> enable

Firewall(config)#

The fourth mode is the monitor mode, which allows password recovery and software image update in the event of a problem. Monitor mode is entered as part of the boot sequence and is recognised from the **Monitor>** prompt. **Monitor>**

There is a help system available in IOS to assist entering commands. It is context-sensitive, which allows help to be given on what is currently being entered. Typing the question mark character (**?**) gives a list of the next available options.

Connections to the security appliance can be made through various methods, each requiring slightly different operations.

Configuring a device for the first time requires the use of a serial connection to the console using terminal emulation software. All security appliances will be provided with a suitable cable, called a rollover cable, which needs to be connected to the serial port of the computer. Most modern laptops will require a USB-serial adaptor as they do not have a traditional serial port.

The terminal emulation software should be configured with the settings of 9600 8-N-1 to ensure correct communication. Windows® comes supplied with the HyperTerminal package, although users may prefer TeraTerm. UNIX and Linux systems have many different packages, including cu.