

Cisco PIX

From Wikipedia, the free encyclopedia

Cisco PIX (*Private Internet eXchange*) was a popular IP firewall and network address translation (NAT) appliance. It was one of the first products in this market segment.

In 2005, Cisco introduced the newer Cisco Adaptive Security Appliance (<http://www.cisco.com/c/en/us/products/security/adaptive-security-appliance-asa-software/index.html>) (Cisco ASA), that inherited many of the PIX features, and in 2008 announced PIX end-of-sale.

The PIX technology was sold in a blade, the FireWall Services Module (FWSM), for the Cisco Catalyst 6500 switch series and the 7600 Router series, but has reached end of support status as of September 26, 2007.^[1]

Contents

- 1 PIX
 - 1.1 History
 - 1.2 Software
 - 1.3 Hardware
 - 1.4 Specifications
 - 1.5 Performance specifications
 - 1.6 Expansion cards
- 2 Adaptive Security Appliance (ASA)
 - 2.1 History
 - 2.2 Software
 - 2.3 Hardware
- 3 Security Vulnerabilities
- 4 See also
- 5 Footnotes
- 6 References
- 7 External links

PIX

History

PIX was originally conceived in early 1994 by John Mayes of Redwood City, California and designed and coded by Brantley Coile of Athens, Georgia. The PIX name is derived from its creators' aim of creating the functional equivalent of an IP PBX to solve the then-emerging registered IP address shortage. At a time when NAT was just being investigated as a viable approach, they wanted to conceal a block or blocks of IP addresses behind a single or multiple registered IP addresses, much as PBXs do for internal phone extensions. When they began, RFC 1597 and RFC 1631 were being discussed, but the now-familiar RFC 1918 had not yet been submitted.

The design, and testing were carried out in 1994 by John Mayes, Brantley Coile and Johnson Wu of Network Translation, Inc., with Brantley Coile being the sole software developer. Beta testing of PIX serial number 000000 was completed and first customer acceptance was on December 21, 1994 at KLA Instruments in San Jose, California. The PIX quickly became one of the leading enterprise firewall products and was awarded the Data Communications Magazine "Hot Product of the Year" award in January 1995.^[2]

Shortly before Cisco acquired Network Translation in November 1995, Mayes and Coile hired two longtime associates, Richard (Chip) Howes and Pete Tenereillo, and shortly after acquisition 2 more longtime associates, Jim Jordan and Tom Bohannon. Together they continued development on Finesse OS and the original version of the Cisco PIX Firewall, now known as the PIX "Classic". During this time, the PIX shared most of its code with another Cisco product, the LocalDirector.

On January 28, 2008, Cisco announced the end-of-sale and end-of-life dates for all Cisco PIX Security Appliances, software, accessories, and licenses. The last day for purchasing Cisco PIX Security Appliance platforms and bundles was July 28, 2008. The last day to purchase accessories and licenses was January 27, 2009. Cisco ended support for Cisco PIX Security Appliance customers on July 27, 2013.^[3]

In May 2005, Cisco introduced the ASA which combines functionality from the PIX, VPN 3000 series and IPS product lines. The ASA series of devices run PIX code 7.0 and later. Through PIX OS release 7.x the PIX and the ASA use the same software images. Beginning with PIX OS version 8.x, the operating system code diverges, with the ASA using a Linux kernel and PIX continuing to use the traditional Finesse/PIX OS combination.^[4]

Software

The PIX runs a custom-written proprietary operating system originally called Finese (*Fast Internet Service Executive*), but as of 2014 the software is known simply as PIX OS. Though classified as a network-layer firewall with stateful inspection, technically the PIX would more precisely be called a Layer 4, or Transport Layer Firewall, as its access is not restricted to Network Layer routing, but socket-based connections (a port and an IP Address: port communications occur at Layer 4). By default it allows internal connections out (outbound traffic), and only allows inbound traffic that is a response to a valid request or is allowed by an Access Control List (ACL) or by a *conduit*. Administrators can configure the PIX to perform many functions including network address translation (NAT) and port address translation (PAT), as well as serving as a virtual private network (VPN) endpoint appliance.

The PIX became the first commercially available firewall product to introduce protocol specific filtering with the introduction of the "fixup" command. The PIX "fixup" capability allows the firewall to apply additional security policies to connections identified as using specific protocols. Protocols for which specific fixup behaviors were developed include DNS and SMTP. The DNS fixup originally implemented a very simple but effective security

policy; it allowed just one DNS response from a DNS server on the Internet (known as *outside* interface) for each DNS request from a client on the protected (known as *inside*) interface. "Inspect" has superseded "fixup" in later versions of PIX OS.

The Cisco PIX was also one of the first commercially available security appliances to incorporate IPSec VPN gateway functionality.

Administrators can manage the PIX via a command line interface (CLI) or via a graphical user interface (GUI). They can access the CLI from the serial console, telnet and SSH. GUI administration originated with version 4.1, and it has been through several incarnations:^{[5][6][7]}

- PIX Firewall Manager (PFM) for PIX OS versions 4.x and 5.x, which runs locally on a Windows NT client
- PIX Device Manager (PDM) for PIX OS version 6.x, which runs over https and requires Java
- Adaptive Security Device Manager (ASDM) for PIX OS version 7 and greater, which can run locally on a client or in reduced-functionality mode over HTTPS.

Examples of emulators include PEMU and Dynagen, and with NetworkSims.com ProfSIMs (Networksims) for a simulator.

Because Cisco acquired the PIX from Network Translation, the CLI originally did not align with the Cisco IOS syntax. Starting with version 7.0, the configuration became much more IOS-like. As the PIX only supports IP traffic (as opposed to IPX, DECNet, etc.), in most configuration commands "ip" is omitted. The configuration is upwards-compatible, but not downwards-compatible. When a 5.x or 6.x configuration is loaded on a 7.x platform, the configuration is automatically converted to 7.x formatting, as long as the configuration was using ACLs, versus conduits and "outbounds". This allows for an easy migration from PIX to ASA. PIX OS v7.0 is only supported on models 515, 515(E), 525 and 535. Although the 501 and 506E are relatively recent models, the flash memory size of only 8 MB prevents official upgrading to version 7.x, although 7.x can be installed on a 506E using monitor mode up to version 7.1(2). The 8 MB flash size only allows for installation of the PIX OS software, not the ASDM software (GUI). For the PIX 515(E) to run version >7.0, a doubling of the memory size is required (32->64 MB for restricted and 64->128 MB for Unrestricted/Failover licenses). A 515(E) UR/FO can run 7.0 with 64 MB memory installed, but that is not recommended as larger configuration and session/xlate tables can exceed the available memory.

Cisco ASA includes the capability of detecting and terminating connections via Dead Connection Detection (DCD).^[8]

Hardware

The original NTI PIX and the PIX Classic had cases that were sourced from OEM provider Appro. All flash cards and the early encryption acceleration cards, the PIX-PL and PIX-PL2, were sourced from Productivity Enhancement Products (PEP).^[9] Later models had cases from Cisco OEM manufacturers.

The PIX was constructed using Intel-based/Intel-compatible motherboards; the PIX 501 used an AMD 5x86 processor, and all other standalone models used Intel 80486 through Pentium III processors. Nearly all PIXs used Ethernet NICs with Intel 82557, 82558, and 82559 network chipsets, but some older models are occasionally found with 3COM 3c590 and 3c595 Ethernet cards, Olicom-based Token-Ring cards, and Interphase-based FDDI cards.

Some Intel-based Ethernet cards for the PIX are identified at boot with the designation "mcwa" (*Multi Cast Work Around*). This designation denotes a multicast receive bug in the card's firmware.

Both the PIX 510 and 520 share basic components, such as motherboard, chassis, NICs, flash cards, etc., with the Cisco LocalDirector 416/420/430, the Service Selector Gateway 6510 (SSG-6510), and the Cisco Cache Engine CE2050, though the latter two run VxWorks, rather than a Finesse derivative.

The PIX boots off a proprietary ISA flash memory daughtercard in the case of the NTI PIX, PIX Classic, 10000, 510, 520, and 535, and it boots off integrated flash memory in the case of the PIX 501, 506/506e, 515/515e, 525, and WS-SVC-FWM-1-K9. The latter is the part code for the PIX technology implemented in the Fire Wall Services Module, for the Catalyst 6500 and the 7600 Router.

The PIX535 has a PCI-X 66 MHz/64 bit bus for expansion slots. This results in a much higher cleartext throughput, as the PCI bus is no longer the bottleneck (the PCI bus is 33 MHz and 32 bits, resulting in maximum throughput of 1.2 GBit without overhead taken in account). As the lower Cisco ASA models use a PCI bus, the PIX535 was faster for cleartext than its successor ASA, until the introduction of the ASA5580.

Specifications



PIX 515 with top cover removed