Cisco PIX vs. Checkpoint Firewall

Introduction

Firewall technology ranges from packet filtering to application-layer proxies, to Stateful inspection; each technique gleaning the benefits from its predecessor.

Stateful inspection works at the network layer and does not require a separate proxy for each application. This technology does not suffer from the same degradation in performance as application-level technology (proxies), which involves the extra overhead of transporting data up to the application layer. And on the contrary of packet filters it has the ability to maintain session state and therefore increase the security level of a network transaction.

Checkpoint Firewall-1

Checkpoint FW-1 has been the firewall market leader since shortly after its introduction in 1994/95. Its well-designed GUI interface was, and still is, the best visual interface to any firewall product. This intuitive interface makes FW-1 easy to work with even for those new to firewalls.

FireWall-1 is based upon Stateful Inspection technology, the de facto standard for firewalls. Invented by Check Point, Stateful Inspection provides the highest level of security. FireWall-1's scalable, modular architecture enables an organization to define and implement a single, centrally managed Security Policy. The enterprise Security Policy is defined on a central management server trough a GUI and downloaded to multiple enforcement points (Inspection Modules) throughout the network.
The FireWall-1 Inspection Module is located in the operating system (NT or UNIX operating systems) kernel at the lowest software level. The Inspection Module analyzes all packets before they reach the gateway operating systems. Packets are not processed by any of the higher protocol layers unless FireWall-1 verifies that they comply with the Inspection Module security policy (it examines communications from any IP protocol or application, including stateless protocols, such as UDP and RPC)

PIX Firewall

Originally designed to be a network address translator, Cisco introduced the Private Internet Exchange (PIX) Firewall series in 1994. The PIX Firewall is a high-performance firewall that uses Stateful packet filtering. The PIX Firewall is essentially a firewall appliance"--it has its own integrated hardware/software solution (Intel hardware / proprietary OS). The PIX Firewall is not Unix or NT-based, but is based on a secure, real-time embedded system, known as the Adaptive Security Algorithm (ASA), which offers Stateful inspection technology. ASA tracks the source and destination address,

TCP sequence numbers, port numbers, and additional TCP flags. All inbound and outbound traffic is controlled by applying the security policy to connection table entries, which house the information. Access is permitted through the PIX Firewall only if a connection has been validated or if it has been explicitly configured.

Comparison

PIX and checkpoint FW-1 are using similar technologies in that both use smart packet filtering technologies (Stateful technology).

There are several key differences: one is that FW1 uses a general-purpose operating system while Cisco's PIX uses an embedded operating system. Another is that the PIX is essentially a "diode": you define a security level for an interface, and anything from a higher (internal=100) to a lower (external=0) is allowed while lower (external) to higher (internal) is blocked (with coding for exception); with FW1 there are no native directions, and everything must be coded. (For this reason, FW1 can be found much more flexible)
The license structure on the PIX is per-connection; the license structure on FW1 is per protected host. All other things being equal, maintenance is much easier on the PIX, and performance is higher on the PIX. Cisco has recently released a host-to-LAN encryption solution; FW1 has such a solution for a long time now (SecuRemote for windows boxes). FW1 has extra features such as bandwidth management (floodgate) or content vectoring servers and others (see OPSEC products).

Note that FW1 is developed in a Unix environment. The Unix implementation is more efficient, more mature, and more stable. It is wrong to go with NT unless the client swears he can support NT and is afraid of Unix. Also, comparing FW1 on a switch or on a NOKIA box versus the PIX could be kind of an interesting comparison.

PIX *Pros*:

1) Minimal configuration if you have few or zero internal devices that needs to be accessed directly from the Internet (i.e. web servers on a protected DMZ) and want to allow everything outbound.

2) Complete hardware/software solution, no additional OS vulnerabilities or boot-time errors to worry about.

3) Cisco support, which is generally very good.

4) Performance, probably the best in the business.

5) No special client side software other than telnet, tftp or serial port terminal software.

6) Lots of detailed documentation.

7) Free upgrades

PIX *Cons*:

1) Difficult to manage if you have many servers on a protected DMZ (lots and lots of conduit statements) or many firewalls to manage.

2) Routing limitation in complex network architectures (Need to add a router for EACH segment).

3) Command line (IOS style) based. Cisco GUI manager (PIX Firewall Manager) is currently in its early releases and not as functional as FW-1's.

4) No ability to off-load layer 7 services like: virus scanning, URL filtering, etc. You can filter on outgoing traffic, but the process is not dynamic.

5) Requires a separate syslog server for logging.

6) No source port filtering.

8) No clear documentation (Cisco's documentation is often conflicting, fails to explain which version of the PIX OS a certain configuration will or will not work under, and seems to be constantly changing).

FW-1 *Pros*:

1) Very functional GUI interface.

2) Based on Stateful inspection like PIX, but can off-load layer 7 inspection to other servers if required.

3) Lots of features for complex environments like: large protected DMZ, Windows VPN support, firewall synchronization, bi-directional NAT, etc.

4) Can be used to control bi-directional traffic.

5) Complex logging provided on management station.

FW-1 *Cons*:

1) Must account for OS vulnerabilities as well as FW-1 vulnerabilities.

2) Performance on NT not as good as on Unix or the PIX.

3) Support is only through re-sellers, very expensive (Contracts start at 50% of the price of the original software per year) and needed for products upgrades.

4) OS boot-time errors possibilities.

NB: PIX can filter java but no ActiveX or JavaScript filtering yet. (Although FW-1 can)

Conclusion

In the simplest terms, FW-1 can be considered much more functional than the PIX, while the PIX has better performance and support. If your particular environment requires a lot of functionality, the best choice is the FW-1 solution, although you might want to consider running it on a Unix platform rather than a NT platform. If your environment is pretty simple, PIX is a solid solution with very good performance.

Checkpoint Firewall-1 links

Main site: http://www.checkpoint.com/products/firewall-1/

Public Support: http://www.checkpoint.com/techsupport/

Unofficial FAQ: http://www.phoneboy.com/fw1/ http://www.deathstar.ch/security/fw1/

Unofficial mailing list archive: http://msgs.securepoint.com/fw1/

Cisco PIX firewall links

Main site: http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/

FAQ: http://www.cisco.com/warp/public/110/pixfaq.html

Several useful papers: http://www.cisco.com/warp/public/110/index.shtml#pix

Documentation: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/

Top issues: http://www.cisco.com/warp/public/110/top_issues/pix/pix_index.shtml