- Introduction to PIX/ASA Firewalls -

Cisco Security Appliances

Both Cisco routers and multilayer switches support the IOS firewall set, which provides security functionality. Additionally, Cisco offers dedicated security appliances:

- **PIX (Private Internet eXchange)**
- **ASA (Adaptive Security Appliance)**

PIX firewalls, though still in prevalent use, are being replaced with ASA equivalents.

Cisco security appliances help protect against three categories of attacks:

- **Reconnaissance Attacks –**used to document and map a network's infrastructure, including vulnerabilities.
- **Access Attacks –**used to gain unauthorized access to data or systems.
- **Denial of Service (DoS) Attacks** –used to disrupt access to services, often by crashing or overloading a system.

Cisco security appliances offer features to safeguard against these attacks:

- **Packet Filtering –** permits or denies traffic based on source/destination IP addresses, or TCP/UDP port numbers using Access Control Lists (ACLs),
- **Stateful Packet Inspection –** tracks TCP and UDP sessions in a flow table, using the **Adaptive Security Algorithm.**
- **Proxy –** serves as the "middle-man" for communication, by authenticating users before communication is allowed to occur.

Cisco security appliances employ a proprietary operating system called **Finesse (Fast InterNEt Server Executive).** Cisco did not originally develop this operating system - the PIX product line was acquired when Cisco bought out Network Translation, Inc.

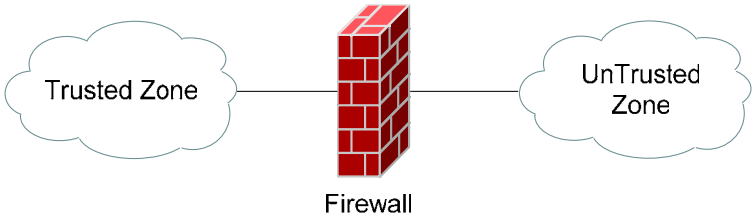
The Finesse operating system is referred to now as the **PIX OS,** and employs a command-line interface that is similar to, but not quite, entirely unlike the Cisco IOS. ☺ Various GUI interfaces are available as well, depending on the PIX OS version, such as the **PIX Device Manager (PDM)** or **Adaptive Security Device Manager (ASDM).**

(Reference: http://en.wikipedia.org/wiki/Cisco_PIX)

* * *

PIX/ASA Security-Levels

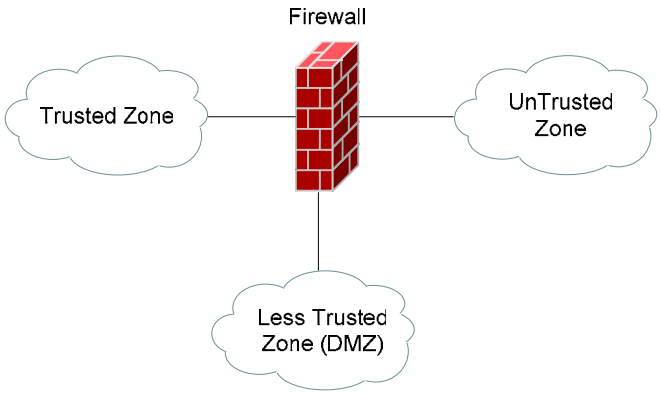
Cisco security appliances protect **trusted** zones from **untrusted** zones.



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.**

A firewall is not limited to only two interfaces, but can contain multiple 'less trusted' interfaces, often referred to as **Demilitarized Zones (DMZ's).**



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. For example, in the above diagram, the Trusted Zone could be assigned a security value of 100, the Less Trusted Zone a value of 75, and the Untrusted Zone a value of 0.

As stated previously, traffic from a *higher* security to *lower* security interface is (generally) allowed by default, while traffic from a *lower* security to *higher* security interface requires explicit permission.

* * *

PIX/ASA Failover

Both PIX and ASA firewalls also support **failover**, providing a redundant environment for high-availability. This failover feature is similar to **HSRP (Hot Standby Routing Protocol)**.

One firewall remains in an **"active"** state, performing all normal firewall functions. Another firewall remains in a **"standby"** state, ready to take over if the primary firewall fails. Only specific PIX/ASA models support failover.

PIX/ASA Licensing

All PIX/ASA firewalls, with the exception of the PIX 506e, support various levels of licensing. For example, the PIX 501 firewall licenses based on the number of users, and supports 10, 25, or 50 concurrent users.

The PIX 506e supports an unlimited numbered of users.

Higher-end PIX/ASA models support three types of licensing:

- **Unrestricted** – allows the maximum number of interfaces and RAM for each model. Supports failover.
- **Restricted** – limits the maximum number of interfaces and RAM. Does not support failover.
- **Failover** – places the PIX/ASA in a "standby" by state, as a backup to an "active" unrestricted PIX/ASA.

Predictably, unrestricted licensing is far more expensive than restricted licensing. Additionally, stronger VPN encryption algorithms (such as AES), may require a specific PIX/ASA license.

All licenses are installed through the use of **activation keys.**

* * *

PIX Firewall Models

The Cisco PIX firewall family consists of five standard models:

- **PIX 501**
- **PIX 506e**
- **PIX 515e**
- **PIX 525**
- **PIX 535**

All PIX models contain a console port for access to the PIX IOS. Higher-end models support faster processors and increased port density. Additionally, the higher-end models support a high number of total connections, IPSEC tunnels, and overall throughput.

- The **PIX 501** is the low-end model of the PIX family. It contains a single WAN port, and an integrated, 10/100 four-port switch that serves as the LAN network. The PIX 501 is intended for home or small offices, with support for 10 IPSEC VPN tunnels.

- The **PIX 506e** is the next model up, and is intended for small branch or remote offices. It contains one integrated LAN port, and one integrated WAN port, and support for 25 VPN tunnels.

Neither the PIX 501 nor the PIX 506e support failover. Both firewalls are also completely integrated; neither offer modular bays for additional ports. Additionally, the PIX 501 and 506e **support up to PIX OS 6.0**, and thus **do not support PIX OS 7.0** or higher.

The following models are modular, and rack-mountable:

- The **PIX 515e** is intended for small to medium sized offices. The PIX 515e supports up to six 10/100 Ethernet interfaces. Each interface is used as either a LAN, WAN, or DMZ port.

- The **PIX 525e** is intended for large or enterprise businesses, and supports a maximum of eight interfaces.

- The **PIX 535** is the highest-end model of the PIX family, with support for 500,000 concurrent connections. A maximum of ten interfaces are supported.

The PIX 515e, 525e, and 535 support **all PIX OS versions, including 7.0**.

* * *

PIX VPN Acceleration

The modular PIX firewalls (**515e** and up) support the installation of **VPN Accelerator Cards (VACs).**

Normally, IPSEC functions are performed in software on the PIX, resulting in suboptimal throughput. VACs improve performance by providing hardware-based IPSEC acceleration. By offloading IPSEC functions onto a VAC card, the PIX IOS can be dedicated to other firewall functions.

In addition to VAC modules, a higher-performance **VAC+ module** is available for modular PIX firewalls.

The PIX 535 contains an integrated VAC, and all ASA firewalls have integrated VPN acceleration.

ASA Firewall Models

The Cisco ASA firewall family currently consists of five standard models:

- **ASA 5505**
- **ASA 5510**
- **ASA 5520**
- **ASA 5540**
- **ASA 5550**

As with the PIX, higher-end ASA models support faster processors and increased port density. Additionally, the higher-end models support a larger number of total connections, memory, IPSEC tunnels, and overall throughput. The link below provides a detailed comparison of each model.

ASA firewalls all operate PIX OS 7.0 or higher.

(Reference: http://www.cisco.com/en/US/products/ps6120/prod_models_comparison.html)

* * *