CN414
Computer Network Security

Week 9:- Firewall Architecture

By

Dr. Piya Techateerawat

Firewall

- **Firewall Architecture**
- Firewall Pro & Cons
- Types of Firewalls
- Firewall Configuration
- Firewall Products
- Firewall Alternatives

Firewall Architecture

- What firewall should be ?

Firewall Architecture

- Principal of an effective firewall are
  - It must act as a door through which all traffic must pass (Both incoming & outgoing)
  - It must allow only authorized traffic to pass
  - It must be immune to penetration or compromise

Firewall Architecture

- The original term of firewall derives from
  - Construction wall that must be able to withstand fire for a prescribed period of time.
  - Therefore, firewall is to provide enough time so that people can either escape or extinguish the fire.

Firewall Architecture

- In term of network,
  - An organization should never connect the company's network or systems to an external network.
  - Never trust the internal or simple protection e.g. company should not relies on filtering rules on router.

Firewall

- Firewall Architecture
- **Firewall Pro & Cons**
- Types of Firewalls
- Firewall Configuration
- Firewall Products
- Firewall Alternatives

Firewall Pro & Cons

- Pros
  - Keeping unwanted an unauthorized traffic from passing (in or out)
  - Efficient method of providing internet access for internal users.
  - It may provides NAT, monitoring attack and maintaining log.

Firewall Pro & Cons

- Cons
  - Single point of failure
  - Security of organization is based on firewall configuration. (Then, people always trust inside)
  - Network Performance.
  - General firewall is static (rule based)

Firewall

- Firewall Architecture
- Firewall Pro & Cons
- **Types of Firewalls**
- Firewall Configuration
- Firewall Products
- Firewall Alternatives

Types of Firewalls

- Categorize firewall based on the level of OSI model at
  - Network level
  - Application level (proxy server)
  - Circuit level (proxy server)

Types of Firewalls

- Network level firewalls
  - Working at network level (OSI Model)
  - It screens or filters packet which pass through.
    - Static packet filtering
    - Dynamic packet filtering/stateful inspection

Types of Firewalls

- Static Packet Filtering
  - A group set of rules to deny/authorize incoming and outgoing packets.
  - These sets are defined by network administrator.
  - These rules are not change on the situation (unless admin changes) so it called “Static”

Types of Firewalls

- Stateful Inspection/Dynamic Packet Filtering
  - The rule can be changed as condition.
  - For example, firewall permits only incoming packet that is corresponding outgoing packets.
  - Or, it only allow in traffic that is response to a request that originated from the inside network.

Types of Firewalls

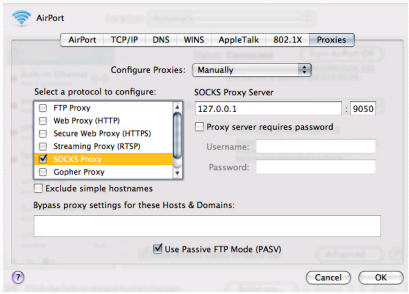
- Proxy Server
  - It acts as “man in the middle”
  - so that there is no direct connection between a client on an internal network and a server on an unstrusted network
  - *Note:* Proxy is not a firewall but only control access which may run on the firewall.

Types of Firewalls

- Application Level Proxy
  - Sometimes referred as application level gateways
  - It act as a gateway between a trusted and untrusted network
  - Typically, the proxy also authenticates the user and authorizes the source and destination addresses to permit or deny the protocol
  - Note: each protocol requires the separated proxies (e.g. HTTP, FTP, ...)

Types of Firewalls

- Circuit Level Proxy
  - A circuit level proxy functions by creating circuit between a client and a server.



Firewall

- Firewall Architecture
- Firewall Pro & Cons
- Types of Firewalls
- **Firewall Configuration**
- Firewall Products
- Firewall Alternatives

Firewall Configuration

- Screening routers
  - Using the router to screen the unstrusted IP
- Bastation Host
  - A selected host to connect with unstrusted network to defend the network

Firewall Configuration

- Dual Home Host
  - It can be imagined as improved version from Bastation Host where host computer is installed with two network cards.
  - One card is connected to the outside network and other connect to inside network

Firewall

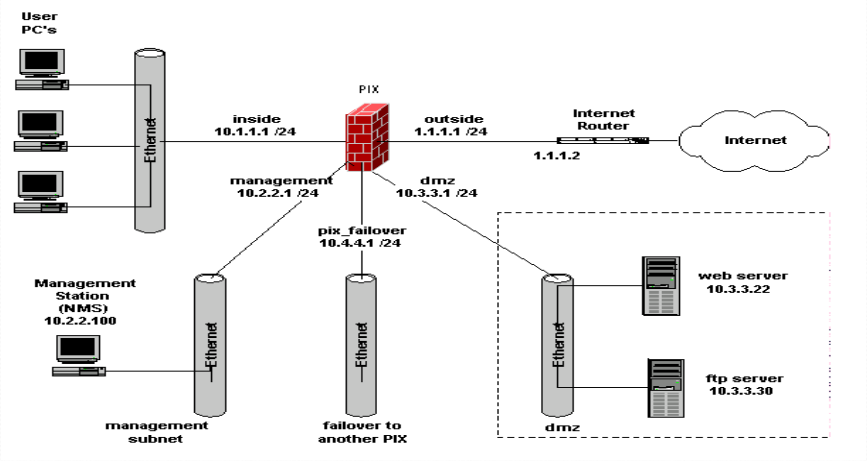
- Firewall Architecture
- Firewall Pro & Cons
- Types of Firewalls
- Firewall Configuration
- **Firewall Products**
- Firewall Alternatives

Firewall Products

Cisco PIX Models

Cisco PIX Model	Rated Throughput	Concurrent Connections	Description
PIX 535	1 Gbps + Up to 95 Mbps 3DES VPN, 2000 IPsec tunnels	500,000	Some models include stateful high-availability capabilities, as well as integrated hardware acceleration for VPN. Modular chassis, up to 10 10/100 Fast Ethernet interfaces or 9 Gigabit Ethernet interfaces.
PIX 525	360 Mbps + Up to 70 Mbps 3DES VPN, 2000 IPsec tunnels	280,000	Some models include stateful high-availability capabilities, as well as integrated hardware acceleration for VPN. Modular chassis, up to 8 10/100 Fast Ethernet interfaces or 3 Gigabit Ethernet interfaces.
PIX 515E	188 Mbps +	125,000	Some models include stateful high-availability capabilities and integrate support for 2,000 IPsec tunnels. Modular chassis, up to six 10/100 Fast Ethernet interfaces.
PIX 506E	20 Mbps +, 16 Mbps 3DES VPN		Compact desktop chassis, two auto-sensing 10Base-T interfaces.
PIX 501	10 Mbps +, 3 Mbps 3DES VPN		Compact plug-n-play security appliance, integrated 4-port Fast Ethernet (10/100) switch and one 10Base-T interface.

Firewall Products



Firewall

- Firewall Architecture
- Firewall Pro & Cons
- Types of Firewalls
- Firewall Configuration
- Firewall Products
- **Firewall Alternatives**

Firewall Alternatives

- TIS firewall Toolkit
  - Trusted Information System's (TIS) firewall toolkit.
  - It contains a set of basic proxies and required functionality for a firewall
- Personal Firewall
  - Microsoft
  - MacAfee
  - Norton

Reference

Accessed @ 18 Nov 2008

- http://stonewall.nist.gov/CONTENT/wall199c.jpg
- http://www.propsunlimited.com/pics/2504.jpg
- http://dltj.org/wp-content/uploads/2008/02/airport-advanced-settings-proxy.png
- http://www.netcraftsmen.net/welcher/papers/pix01.html


Q & A