Bob's Firewall Overview

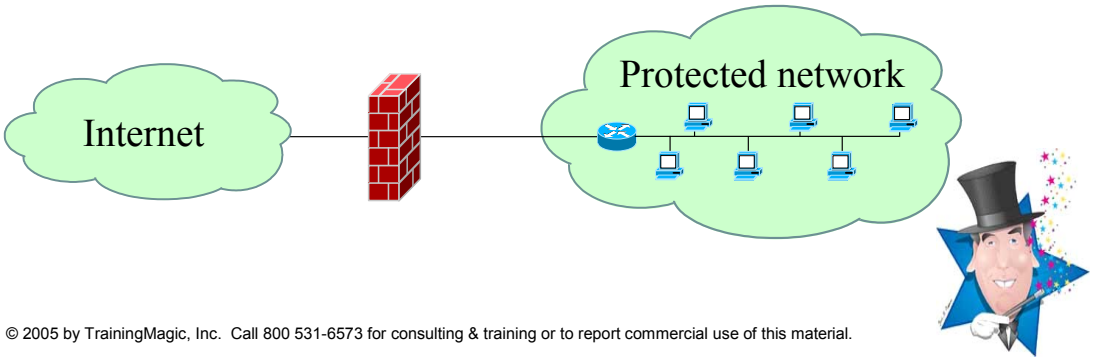
An overview of Firewall Concepts & Technology

Firewalls – Objectives

- Describe the function of a firewall.
- Define a DMZ.
- List the 5 categories of firewalls.
- Compare packet filtering, stateful firewalls, and proxy servers.
- Explain the purpose and operation of an IDS.
- Discuss the techniques used by hackers to penetrate an IDS.
- Compare NAT and NAPT and evaluate their impact on security.

Firewalls defined

- **Dual-homed host.**
- **Like a network guard.**
- **Blocks traffic into, and out of, a network.**
- **There is a performance penalty.**



Firewalls defined

The following comments are from **Internet Firewall Essentials by** *Eric Hall* and can be found at http://www.networkcomputing.com/netdesign/wall2.html:

Almost by definition, a "firewall" provides a filter that incoming or outgoing packets must pass through. If the firewall does something beyond filtering, like checking against a restrictions list, that's great, but it's not necessarily the "definition" of a firewall's function.

Of course, most firewalls do perform some sort of "accept" or "reject" functionality, but that's strictly a matter of implementation. The simplest firewall could just be an Ethernet bridge that you keep powered off, only to be made available when the connection is needed. This would probably work for keeping intruders off of your network, but I doubt you'd enjoy the management interface much. Most firewall products offer much more in the way of actively filtering packets according to certain criteria that you establish.

These filtering firewall products can take many forms. They may be a replacement TCP/IP stack that you load on an existing system, or a software module that exclusively communicates with an existing stack. At the other end of the extreme, the product may be a completely independent operating system written explicitly with Internet security as the objective. There are also application-specific firewall products that only offer protection for certain types of Internet connectivity, such as SMTP or HTTP. There are also hardware-based products that typically fall into the router realm, allowing you to set filters for incoming and outgoing connections. Prices range from free (bundled with the stack or app) to tens of thousands of dollars.

Bastion host

- **A fortified area or position** (Merriam-Webster).
- **Older term: no clear definition.**
- **A firewall that is critical to network security.**
- **Software-based (vs. firmware).**
- **A computer system "hardened" to resist attacks.**

Bastion Host

A Bastion Host is a somewhat older concept, and overtime definitions have become blurred. A Bastion Host is generally thought of as a computer system that has been hardened to resist attack at some critical point of entry, and which is installed on a network in such a way that it is expected to come under attack. Generally, a bastion host uses a general-purpose operating system (e.g., Linux, BSD Unix, WinNT, etc.) rather than a firmware operating system.

Bastion hosts are configured so that all non-essential network services are disabled on them. Usually the only thing the server allows is Internet access. All other services are be disabled, so that intruders can't gain access to the bastion server and from there other computers on the network. The safest way to use bastion hosts is to put them on their own subnet as part of an intranet firewall. By putting them on their own network, if they are broken into, no other intranet resources are compromised.

Firewall placement (1)

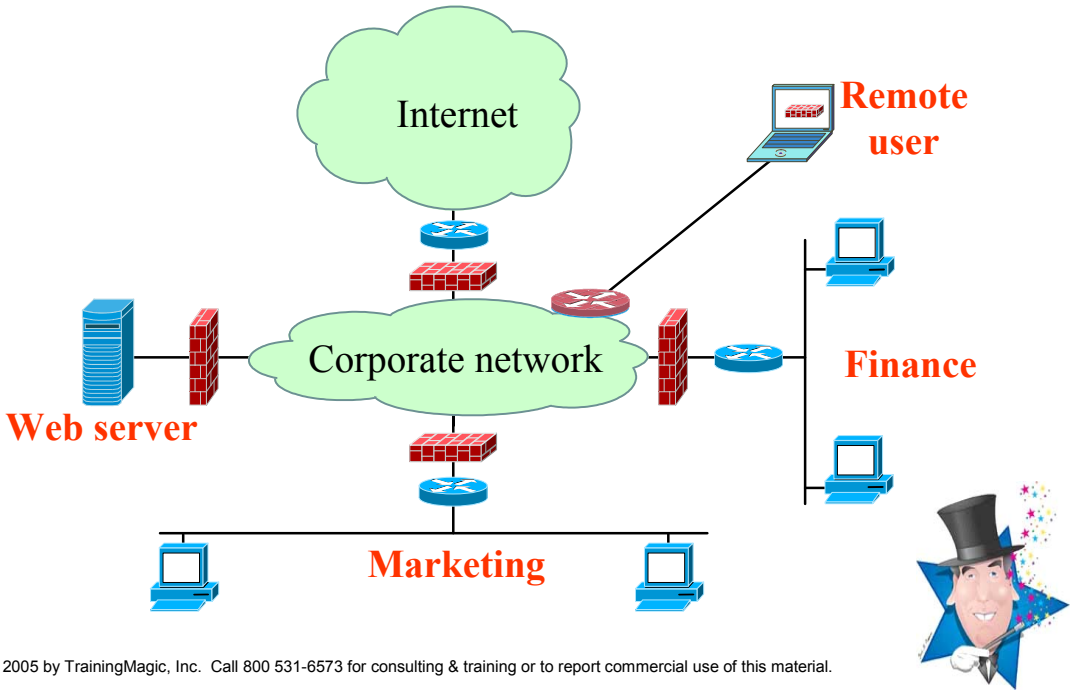
- **Between the Internet and the internal network.**
- **Between different corporate departments.**
- **Between the public web server and the internal network.**
- **On the personal computer.**

Firewall Placement (1)

Proper firewall placement is vital. Improper placement can leave the network with an unguarded "door" to the rest of the world. Firewalls should be placed anywhere the enterprise network has access to an outside computer, an outside network or the Internet. In a simple network, the firewall may be place at a "bottleneck" – the single point of access between the corporate network and the Internet.

Firewalls can also be placed between various areas (or departments) in the enterprise. Firewalls within corporate networks may be connected together to form an "Intranet" without sacrificing security. Software firewalls may be placed on each personal computer – implementing a "belt and suspenders" approach.

Firewall placement (2)

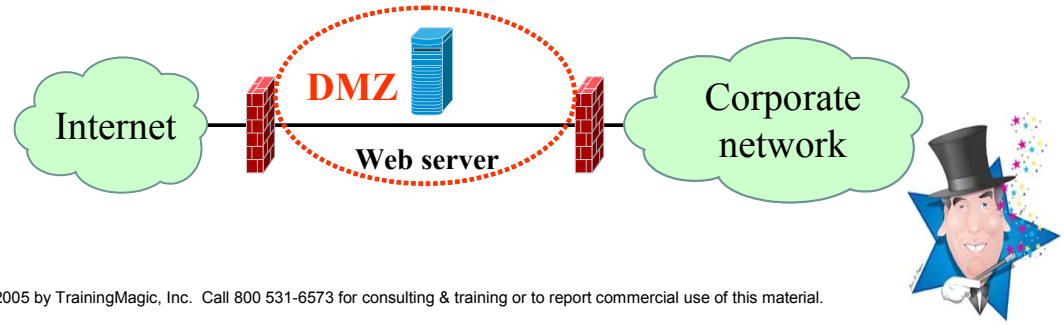


Firewall Placement (2)

Firewalls may be placed at any location in order to police the flow of suspect traffic. This includes between departments, between Remote Access/VPN clients and the intranet, and on connections to the Internet itself.

Demilitarized zones (DMZ)

- **Defense-in-depth**
  - **Multiple layers of security.**
- **Public has limited access to resources.**
- **Server in the DMZ is expendable.**
- **No critical resources located in the DMZ.**
- **AKA Secure Service Network (SSN).**



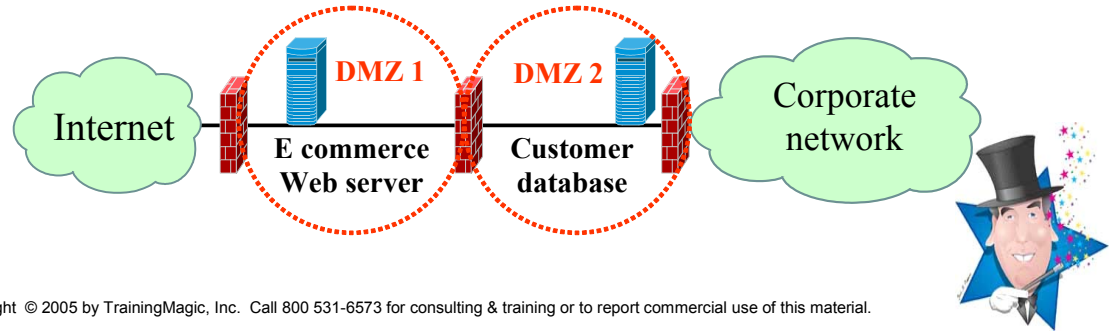
Demilitarized zones (DMZ)

Just like the military term, DMZ stands for Demilitarized Zone. A DMZ is a network added between a protected network and a network with public access in order to provide an additional layer of security. A DMZ can be known by several other names including: “Secure Service Network”, "Perimeter network" or a "Three-homed perimeter network."

A DMZ isolates a computer that is accessing a service from all computers inside the network. Often the external network is the Internet and the service in the DMZ is a web server. The DMZ acts as another layer of defense to make sure that if a hacker penetrates the web server, the internal network is not compromised. The web server might be a bastion host with firewalls on each side. This is an example of the “defense-in-depth” concept.

Multi-tiered DMZs

- **Two or three tiers.**
- **Hackers must get through multiple devices to reach the most sensitive data.**
- **How much protection will you pay for?**
  - **Should every soldier have a tank?**

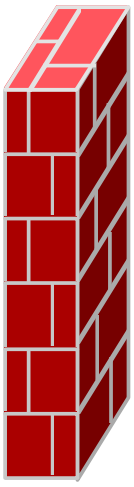


Multi-tiered DMZ

Multiple DMZ's can also be used to isolate particular machines, or services, within a network from other parts of the network. This might be done to keep an E-commerce server isolated from a customer database. An Internet customer accesses the E-commerce web server in DMZ 1. The web server may need data on this customer. The web server retrieves information from the database in DMZ 2. The customer is never in direct contact with the machine that contains the sensitive customer data. However, in the unlikely event that both the E commerce server in DMZ 1 and the customer database in DMZ 2 are compromised, the internal corporate network remains unpenetrated.

Types of firewalls

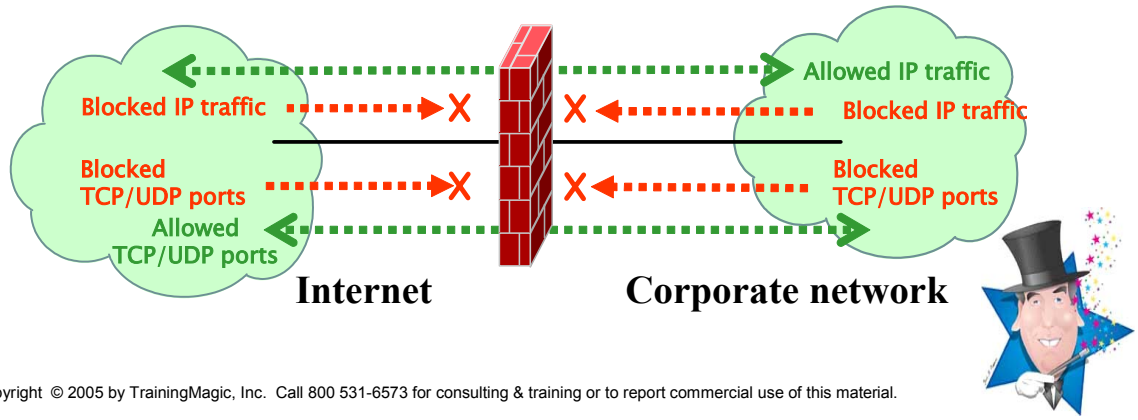
- Software based.
- Hardware based.
- Packet filtering.
- Stateful firewalls.
- Proxy.



Types of Firewalls

Packet filtering overview

- **Restrict or allow IP addresses**
  - **(who is accessing the network).**
- **Restrict or allow TCP/UDP ports**
  - **(what applications are being accessed).**



Packet filtering overview

Packet filtering is a basic building block of network security. In packet filtering, access to a network is controlled by analyzing the incoming and outgoing packets and passing or blocking them based on the source or destination IP address (and/or TCP/UDP ports).

Packet filtering is simple to understand and inexpensive to implement. Furthermore, packet filtering is nearly ubiquitous. Most routers, including Cisco, Juniper, Linksys, and Lucent have packet-filtering functions. All modern operating systems have built in packet filtering firewall capabilities. Every router, switch and PC in the network is a potential filtering point.

Filtering IP

- **Block these IP addresses from the Internet.**
- **Block these IP addresses to the Internet.**
- **What types of addresses?**
  - **Illegal/reserved addresses.**
  - **Broadcast addresses.**
  - **Loopback addresses.**
  - **Known hostile addresses.**

Filtering IP

Most packet filters pass or block packets at either the *network layer* or *transport layer* of the OSI 7 layer reference model. Each packet is examined as it enters the router. The headers are examined and may be blocked based on the following information:

- Some protocols (like ICMP) may be completely blocked.
- Some source or destination addresses may be blocked if they have been identified as “undesirable”.
- Services identified though “well known” TCP/UDP ports can be blocked.

Well known ports (TCP/UDP)

A few well known ports …

Port	*Protocol*	*Service*
21	TCP	FTP control
23	TCP	Telnet
25	TCP	SMTP
53	UDP	DNS
80	TCP	WWW
161	UDP	SNMP

Well known ports

Here are some other well-known ports.

Port/Protocol	Service
7/tcp	Echo
7/udp	Echo
20/tcp	File Transfer [Default Data]
20/udp	File Transfer [Default Data]
22/tcp	SSH Remote Login Protocol
22/udp	SSH Remote Login Protocol
69/tcp	Trivial File Transfer
69/udp	Trivial File Transfer
108/tcp	SNA Gateway Access Server
108/udp	SNA Gateway Access Server
110/tcp	Post Office Protocol - Version 3
110/udp	Post Office Protocol - Version 3
137/tcp	NETBIOS Name Service
137/udp	NETBIOS Name Service
138/tcp	NETBIOS Datagram Service
138/udp	NETBIOS Datagram Service
139/tcp	NETBIOS Session Service
139/udp	NETBIOS Session Service

For a complete listing see: http://www.iana.org/assignments/port-numbers

Filtering TCP/IP

- Used open ports are a necessary evil.
- Unused open ports are an unacceptable vulnerability.
- Firewalls should block all services not explicitly identified for use on the network.
- Another view ⇢

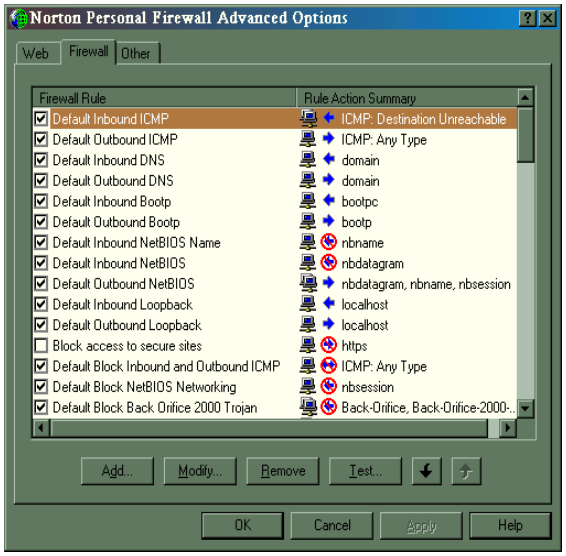
Filtering TCP/IP

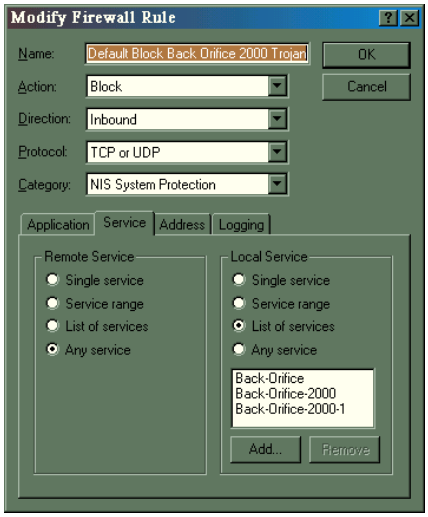
Kesslers "4 P" firewall philosophy

- **Security consultant *Gary Kessler* suggests four levels of filtering.**
- **The Four P's:**
  - *Paranoid* - no connection.
  - *Prudent* - "deny all unless specified".
  - *Permissive* - "allow all unless specified".
  - *Promiscuous* - no protection.

Kessler's "4P" Firewall Philosophy

Sample firewall rules





Sample Firewall rules

Some sample rules taken from **The packet filter: a Basic Network Security tool** which can be found at: http://rr.sans.org/firewall/packet_filter.php:

Ingress – Inbound filtering

1. Block packets destined for services that are not being offered to the Internet.
2. Block addresses that have a source IP address of:
   a. Illegal addresses.
   b. Broadcast address.
   c. RFC1918 reserved addresses – Private networks use these. There should not be any traffic attempting to access your network with these as source addresses. IANA reserved blocks are:
      10.0.0.0 - 10.255.255.255
      172.16.0.0 - 172.31.255.255
      192.168.0.0 - 192.168.255.255
   d. Multicast, if multicast is not being used.
   e. Loopback – 127.0.0.0.
   f. ICMP broadcast per RFC 2644 – This will keep a site from being used as a **smurf amplifier**.
   g. UDP echo.
3. Block packets from outside the filtering device with a source IP address the same as your internal networks. This blocks packets with spoofed IP addresses. This means that you must know what address space is used internally.

Egress – Outbound filtering

1. Block traffic with an invalid source IP address. This keeps a denial of service attack using IP address spoofing from originating on the internal network. The filter should only allow traffic to leave your network with a source IP address that is valid on your internal networks. The purpose here is to keep a denial of service attack from originating on the private network.

Pros and cons of packet filtering

Pro

- **Mature technology.**
  - Well understood
- **Easily integrated into routers and switches.**
- **Good performance.**

Con

- **Complicated rule set.**
- **Attacks can still penetrate through "open" ports.**
- **Can lead to complacency.**

Pros and cons of packet filtering

Packet filtering is a mature technology that is well understood. Both the strengths and weaknesses are published. Packet filtering is nearly ubiquitous and has been integrated into most routers and all modern operating systems. The protection offered by packet filtering, although not perfect, is good.

Among the draw backs of packet filtering are the rule sets that can become cumbersome – especially if individual "hostile" sites are identified and blocked. Finally, because packet filtering can provide a "good" level of protection there can be a tendency to become complacent – ignoring the risk of attacks through open ports (and other vulnerabilities!)

Stateful filtering overview

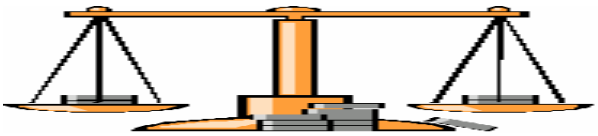
- **Validates based on existing connection.**
  - **Examine each TCP packet for existing connection.**
  - **Must maintain a record for 2 connections per session.**
- **Also blocks unauthorized IP options.**
  - **i.e. Source routing.**

Stateful filtering overview

Stateful firewalls expand the concept of packet filtering process to include multipacket flows. In other words, a stateful firewall tracks if the connection is valid. The connection table tracks individual flows, enabling policy checks that extend across series of packets. For example, TCP ACK packets not preceded by a TCP SYN packet with a correct sequence number can be dropped. Furthermore, if a packet arrives with an inappropriate combination of flags, such as all flags on, all flags off, SYN/FIN, etc., the packet is dropped. Finally, some firewalls (like Cisco PIX) also check TCP sequence numbers; others (like Checkpoint's Firewall-1) do not.

Like ordinary packet filtering, stateful packet inspection works for all applications because its basic functioning is at the Network and Transport layers.

Pros and Cons of Stateful Filtering



Pro

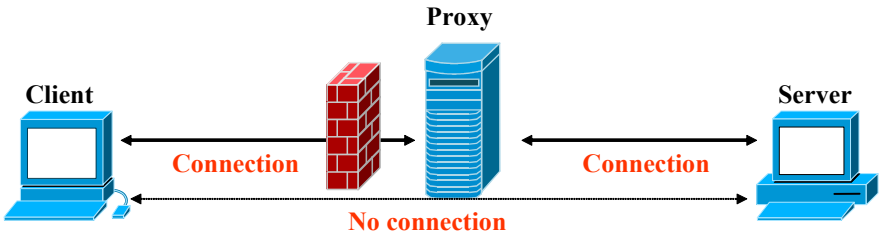
- Better security than simple filtering.
- Block many attacks
  - DOS.
  - Port scanning.
- Can maintain logs of network activity.

Con

- More complicated than filtering.
- More expensive than filtering .
- Increased processing (possible latency).

Pros and Cons of Stateful Filtering

Proxy firewall overview



- **An intermediate device between client and server.**
- **No direct connection between client and server.**
- **Client connects to proxy.**
- **Proxy connects to server.**
- **Difficult for client to cause "mischief" on server.**

Proxy firewall overview

This explanation of proxy servers is from **A Comparison of Packet Filtering Vs Application Level Firewall Technology** by Ernest Romanofski and can be found at: http://rr.sans.org/firewall/app_level.php

A proxy server and a proxy client are two components that are typically implemented as a single executable for each application proxy. A proxy server acts as the end server for all connection requests originated on a trusted network by a real client. Rather than allowing users to communicate directly with the other servers on the Internet, all communication between the internal users on the trusted network and the Internet passes through the proxy server. When the internal user wants to connect to an external service such as FTP or Telnet they send a request to the proxy server for the connection. The proxy server decides whether to permit or deny the request based on an evaluation of a set of rules that is managed for the individual network service. Proxy servers only allow those packets through that comply with the protocol definitions because the servers understand the protocol of the service they are evaluating. The proxy client is the component that talks to the server on the external network on behalf of the real client on the trusted network. The proxy server evaluates a real client's request for a service against the policy rules defined for that proxy and determines whether to approve the request. The proxy server forwards the request to the proxy client if the request is approved. The proxy client contacts the real server on the external network on behalf of the client. The proxy client relays requests from the proxy server to the real server and relays responses from the real server to the proxy server. Then the proxy server relays the requests and responses between the proxy client and the real client.

Proxy services never allow direct connection between the real client on the trusted network and the real server on the external network. Proxy services force all network packets to be examined and filtered for suitability. All communication between the real user and the real service are handled by the proxy service. The proxy service is transparent to the user on the trusted network and the real service on the external network.

Direct/modified connection proxies

- **Two types of "application level" proxies.**
- **Direct connection proxies.**
  - Users connect directly to the proxy server.
  - Users must enter the destination host.
  - Two addresses required for each connection.
- **Modified client proxies.**
  - Use "special" applications on the client PC.
  - Acts like the normal application to user.

Direct/modified connection proxies

Direct/modified connection proxies are specific to a particular application. This turns out to be a powerful advantage since the network manager explicitly defines which applications are authorized and which are not. This type of proxy is also known as an application level proxy. Whether the network is using a direct connection proxy, or a modified client proxy, the internal network is completely isolated from the World Wide Web. When the internal client attempts to connect to the Web, the proxy acts an intermediary. The proxy acts server tot eh client and a client to the server. Finally, some application level firewalls have the ability to maintain a log of all incoming and outgoing traffic.

Invisible proxies

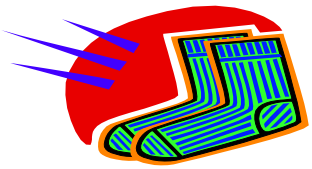
- **No modification of client software.**
- **Invisible to end users.**
- **Translation takes place on proxy server.**
- **Provides compete isolation of users from server applications.**
- **More popular than application level proxies.**
- **AKA "Circuit-level proxies".**

Invisible proxies

Invisible proxies do not modify the client application. Users do not need to have any direct communication with the firewall (or even know that the firewall exists). Invisible proxies are also known as circuit-level proxies. Circuit-level gateways don't access Application-layer information as application proxy firewalls do, so it's not necessary to supply separate proxy processes for each application. The gateway still relays data for a given application between the client and server, but it does not perform any control functions at the gateway level, such as packet processing and filtering. It merely conceals information about the protected network to an outsider, because the connection appears to originate from the firewall system. The best-known implementations of circuit-level gateways employ an IETF standard protocol called SOCKS, which is discussed on the next page.

SOCKS

- **Contraction of SOCKet Security.**
- **Application independent (generic).**
- **Socks protocol is used between the internal client and the proxy server.**
- **Common form of invisible proxy.**



- **RFC 1928.**

SOCKS

SOCKS is a simple, standards based (IETF FRC 1928) and flexible generic application proxy protocol for TCP/IP based networking applications. SOCKS includes two components, the SOCKS server and the SOCKS client. The basic purpose of the protocol is to enable hosts on one side of a SOCKS server to gain access to hosts on the other side of a SOCKS Server, without enabling a direct IP connection. While SOCKS is a generic proxy, generic SOCKS proxy software is required to on the client machine. When an application client needs to connect to an application server, the client connects to a SOCKS proxy server. The proxy server connects to the application server on behalf of the client, and relays data between the client and the application server. For the application server, the proxy server is the client.

Pros and cons of proxies

Pro

- No direct connection between client & server.
- Isolate from Java, Active X, etc.
- Hides network details from outside world.
- Good performance.

Con

- May be slower than other firewall services.
- More complex than other firewall services.
- May be vulnerable to similar bugs as an OS.
- New services may be complex to implement.

Intrusion detection system (IDS)

- **98 % of attacks are not identified by traditional firewalls.**
- **IDS identifies many attacks.**
- **Examines packets for known attack patterns called signatures.**
- **Drop attack packets used in an attack.**
- **Delay can be a problem.**

Intrusion detection system (IDS)

An IDS monitors a computer, or an entire network, for suspicious activity. Suspicious activity is recognized by observing the behavior of a host, or network, and comparing it with the behavior of known attacks. Once an attack is identified, the IDS can respond in a number of ways: notify the network administrator, record the attack, block the attack with the firewall, drop the packets, and/or rest the TCP connection.

IDS signature sets

- **Signatures identify the common elements in an attack.**
- **Some attacks are clear – others require the system to guess!**
- **Example attacks detected:**
  - Buffer overflow
  - Password cracking
  - Port scanning
- **False positives can be annoying.**
- **False negatives can be dangerous.**

IDS signature sets

Intrusion Detection Systems analyze raw network data and look for known patterns in the network, or host, behavior in real time. This pattern is known as an attack signature. Two of the most widely used techniques used to recognize an attack are:

Pattern analysis examines the byte-codes data for known attacks. Some examples that might be detected include: buffer overflow attacks or password cracking attacks.

Frequency analysis examines the frequency with which events that might be attacks occur. Some examples that might be detected include: pings that may be part of a DOS attack or port scans that may be an attempt to footprint the network.

Anti IDS techniques

- **Mask the attack.**
  - Replace characters with Hex equivalent.
  - Example: C:\WINNT\security becomes C:\W%49%4E%4ET\security.
- **Fragment the attack.**
  - Break an attack string into multiple TCP packets.
- **Slow the attack.**
  - Scan the ports of the network over a prolonged period.
- **New techniques.**
  - Coming soon to a network near you!

Anti-IDS techniques

In addition to the techniques mentioned above, an IDS may be susceptible to the following ploys:

Paralyze the IDS by overwhelming it with work. Flooding a network with false attacks can potentially allow you slip a real attack in with out being noticed. Imagine trying to analyze 50,000 attacks, which is genuine? How many people do you have are available to analyze these attacks? This type of attack is really against the people that support IDS – not the system itself.

Another ploy used to confuse the IDS by complicating the request with long URLs. All systems, including the IDS, use sampling techniques that are designed to improve performance by limiting the amount of data sampled in each frame. If a packet is padded with multiple slashes (which some systems interpret as a single slash), hexadecimal letters (as discussed in the slide above), or other techniques, then only a portion of the packet may be read. Because only a portion of the packet is read malicious content may pass though undetected.

Placement of IDS

- **Host based IDS.**
  - Adequate for personal computers.
  - Cannot detect network attacks.
- **Network based IDS.**
  - Must be placed to "see" the entire network.
  - If the firewall is a bottleneck, then IDS can be collocated with the firewall.
  - Distributed "monitors" can combined with a centralized analysis station.

Placement of IDS

Intrusion Detection Systems come in two flavors: host based or network based.

Host based IDS programs reside on the computer that they protect. They can detect attack on a computer that a network based system cannot detect. Examples of attack variables that may be uniquely detected by host based IDS software includes: file corruption, OS modification, registry edits, and CPU usage.

Network based IDS programs usually reside on a dedicated system that may monitor traffic for an entire network. The IDS collects network packets coming into your network and analyzes them to determine if the match any known attacks.

A third approach, offered by some vendors, is called a hybrid approach. In a hybrid IDS there is a dedicated system called a monitor. However, there are also programs reside on all host computers called monitors. This approach combines the strengths of host and network based intrusion detection systems. However, hybrid systems are both more expensive and more complex than either individual system.

NAT defined

- **Network Address Translation (NAT).**
- **Translates a private IP address on the inside of a network to a public IP address.**
- **Allows fewer public IP addresses to service many internal devices.**
- **Hides "real" IP addresses from the public.**
- **Defined in RFC 3022.**

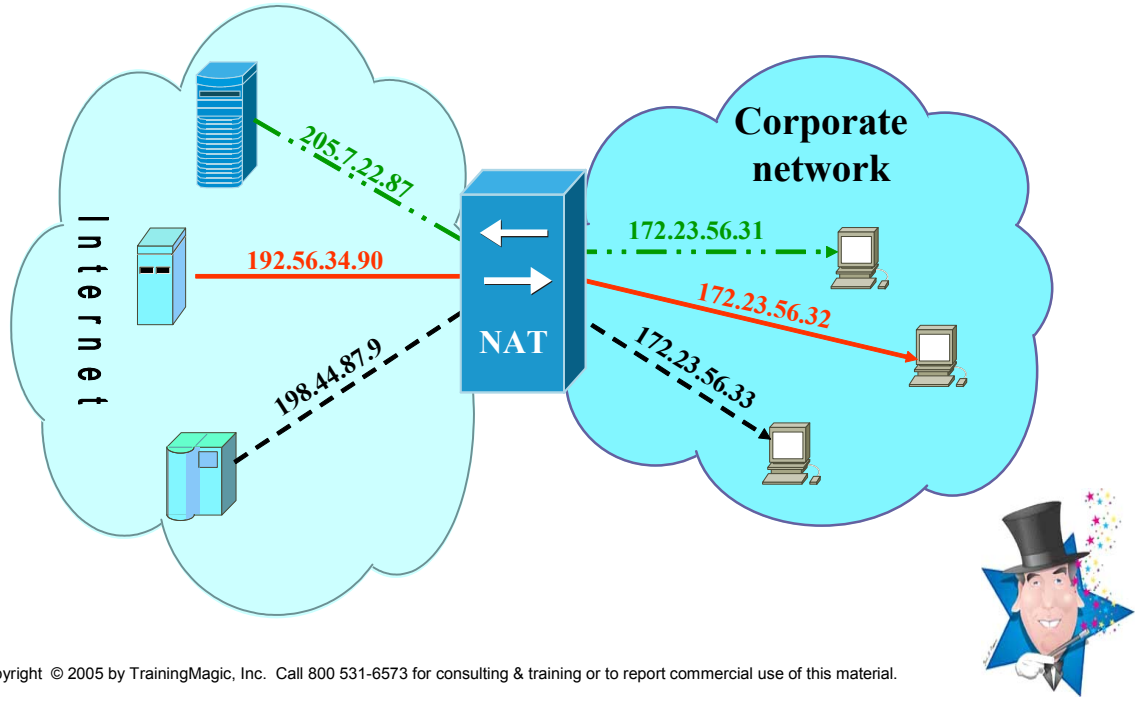
NAT defined

Network address translation is a procedure that translates private IP addresses into public IP addresses. NAT was first introduced in 1994 as defined in RFC 1631 (which has since been replaced with RFC 3022).

When implementing NAT, private IP addresses on the inside of the network are translated into public IP addresses on the outside of the network by a box known as a NAT device. Although there are many reasons that a network administrator might choose to implement NAT (ease of administration and conservation of IP addresses top the list), NAT does provide a measure of security. By using one set of addresses on the public network and a different set of addresses on the inside a hacker has difficulty "mapping" a NAT network.

However, NAT is not a security panacea. NAT leaves a network with several security vulnerabilities: NAT provides no inbound or outbound packet filtering, there is no stateful examination of connections, no logs are maintained of traffic, and all open ports are still connected to the Internet.

Example NAT functions



Example NAT functions

Computer A is assigned a public IP address of 205.7.22.87 and a private IP address of 172.23.56.31. Computer B is also assigned a public IP address of 192.56.34.90 but has a private IP address of 172.23.56.32. How can these computers use the one IP address on the public Internet and a different IP address on the corporate network?

When computer A sends a message out to the Internet it uses the private IP address of 172.23.56.31, and the NAT box translates the private IP address into the public IP address of 192.56.34.90. Again, when computer B sends a message out to the Internet it uses its internal address of 172.23.56.32; the NAT box translates the internal address into the public IP address 192.56.34.90. In the other direction, the NAT performs exactly the opposite function.

NAPT defined

- **Translates a single public IP address to multiple private IP addresses.**
- **An IP address and a TCP/UDP port number is a known as a socket.**
- **Private sockets translated to public sockets.**
- **Hides "real" IP addresses from the public.**
- **Defined in RFC 3022.**

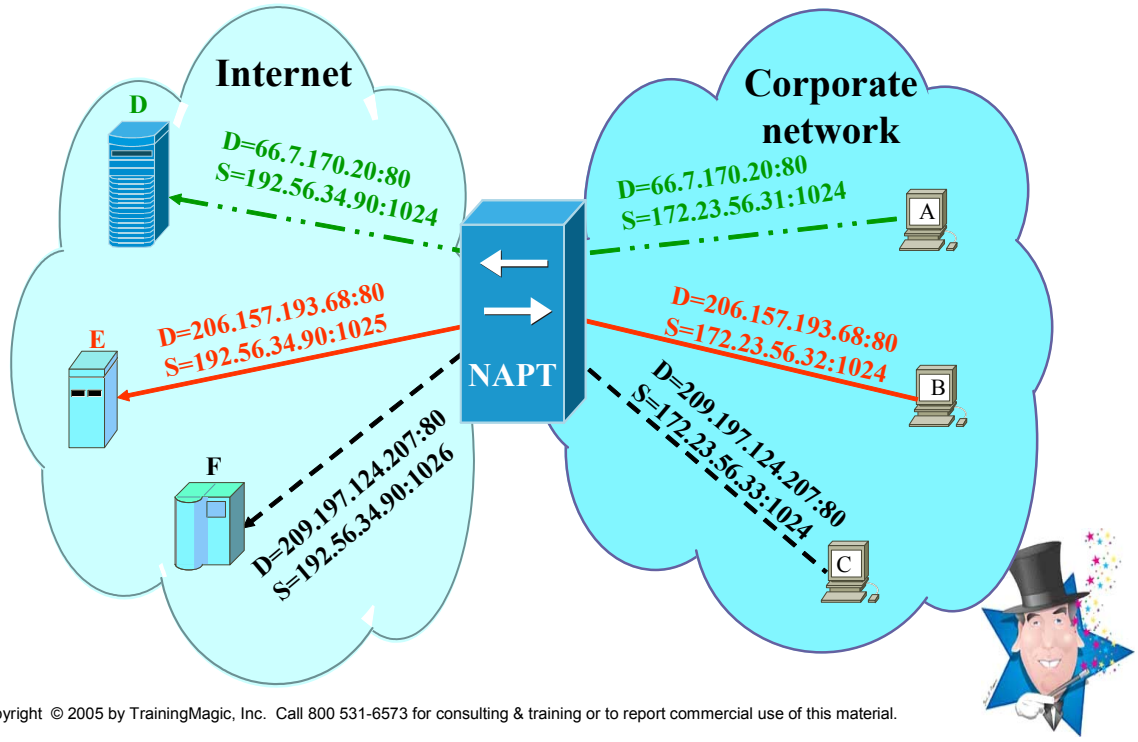
NAPT defined

NAPT translates ***multiple*** IP addresses on a private LAN to one public address on the Internet. In this way, NAPT allows many users to access the Internet with the one IP address assigned by the service provider. In most literature NAPT is simply referred to as NAT or sometimes as PAT (Port Address Translation).

Like NAT, NAPT also provides a measure of added security, since the address of a PC connected to the private LAN is never transmitted on the Internet. In effect, the user is invisible with the PCs "real" IP address hidden behind the DSL router. However, NAPT shares all the security vulnerabilities found in NAT.

How does NATP work? NATP uses Layer 4 identification to translate Layer 3 address. TCP port numbers are used to identify application programs on host computers. However, most TCP port address are not used and NAPT will these "unused" TCP port address to identify different computers on the same network sharing the same public IP address.

Example NAPT functions



Example NAPT functions

In typical NAPT implementations, a single proxy device, such as a Web proxy, router, or other physical device, dynamically creates entries in a NAPT table which correlate internal systems to a single outside address. In this example, the NAPT device itself uses the external address 192.56.34.90. Its internal port has a private address belonging to the 172.23.0.0 corporate network (not shown for simplicity). Devices inside the corporate network typically treat the proxy as a router and simply forward traffic bound for destinations outside their network to it.

When Computer-A attempts to download a web page from Server-D, it's requesting packet contains the target destination and its own internal address which is forwarded to the NAPT device. Upon receipt, the NAPT device forwards a recreated packet with a new source IP address and TCP port number (together, called a socket.) These assigned values are then cached in the NAPT table so that when responses come back to that specific socket, the external address/port values may properly converted back to internal address/port values.

How can multiple computers share the same public IP address? The data streams associated with each computer pair is called a flow. Different flows are distinguished externally by the NAPT device using unique TCP/UDP port numbers. Note that all external flows in the visual bear the same "source" IP address. Yet each has a unique "source" port number.

Security benefits of NAT and NAPT

- **It is difficult to attack an invisible victim!**
- **Both NAT and NAPT hide your network.**
- **Invisibility is not an adequate defense against hackers.**
- **Not a replacement for a firewall.**
- **Many NAT/NAPT devices include a hardware firewall.**

Security benefits of NAT and NAPT

Network Address Translation can provide a level of security of protection as a by-product of the translation process. Through translation, NAT (and NAPT) hides the internal network IP addresses so that external parties never see the actual IP addresses inside the network so it is difficult for bad guys to hack or spoof the network.

However, NAT in and of itself is not an adequate security solution. While NAT helps by hiding all of your hosts, there are still outstanding security issues when using NAT.

The biggest vulnerability with NAT/NAPT exists when an internal host connects to the Internet. Here are four security vulnerabilities, which while not exhaustive, illustrate the weakness of NAT/NAPT: First, if the host connects to a site with malicious code, NAT/NAPT cannot block the packets from that site. Second, NAT/NAPT provides no virus protection. Third, NAT/NAPT does not mask your host information. Theoretically, NETBIOS information could be shared through a NAT/NAPT connection. Finally, nothing in NAT/NAPT protects a host from being used as a zombie machine in DDOS attack.

Risk Evaluation

- **Risk can only be handled in 3 ways:**
  - Transfer the risk (insurance).
  - Reduce the risk (protection).
  - Ignore the risk (foolish).
- **Risk evaluation formulas:**
  - Asset value * exposure factor (percent of loss threatened) = single loss expectancy (SLE).
  - SLE * annualized rate of occurrence (ARO) = annualized loss expectancy (ALE).

Risk evaluation

Security is all about minimizing risk to corporations and individuals. But how much time and money should be spent on security? Some simple formulas can help in making objective business decisions about security expenses.

In assessing security investments, the first step is estimate the value of the risk. Total risk is calculated by estimating the asset value. This should include the value work time, e-commerce activity, customer data, proprietary data, and the value of the company's good name. The asset value is really the cost to replace this information or the value of the lost time.

The next value to estimate is how much of that asset would be lost. In a worst-case scenario, how much of the value of that asset would be lost? The asset value is multiplied times the exposure factor. For example, if the asset being evaluated is a company's e-commerce site that takes in an average of $10,000 an hour. In the worst-case scenario, the e-commerce site could be down due to DOS attack for 5 hours; therefore the worst-case expectancy of a single loss is $50,000.

Is it possible that this could happen to a company more than once a year? If so, then the Single Loss Expectancy (SLE) must be multiplied by the estimate of how often this might happen. This value is known as the annualized rate of occurrence (ARO). The product of these two is known as the annualized loss expectancy (ALE). In our example, if the estimate is that the e-commerce site could be down 6 times a year then the ALE would be $300,000.

Summary

- A firewall blocks certain traffic into and out of a network or a computer.
- A DeMilitarized Zone (DMZ) is:
  - an area isolated from the "secure network" with services available to the public.
- There are five categories of firewalls:
  - Software based.
  - Hardware based.
  - Packet filtering.
  - Stateful firewalls.
  - Proxy servers.

Summary

- Packet filtering blocks or passes traffic on a packet by packet basis.
- Stateful filtering examines traffic based on the state of TCP connections or UDP packets.
- Proxy servers isolate the client from the server.
- An intrusion detection system examines network traffic for known attack patterns.

Summary

- **Hackers attempt to penetrate IDS by:**
  - Masking the attack.
  - Fragmenting the attack.
  - Slow the attack down.
  - Various other techniques.
- **NAT translates an internal private IP address to a public IP address.**
- **NAPT translates many private addresses to a single public IP address.**
- **NAT and NAPT hide network internals from the public.**