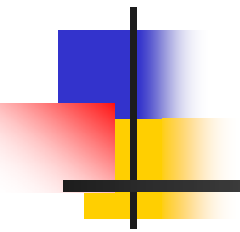
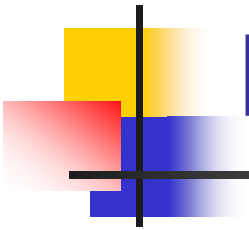
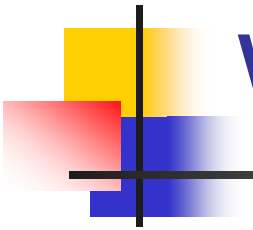


Firewalls



Firewalls

- Typically used to filter packets
- Designed to prevent malicious packets from entering the network or its computers (sometimes called a packet filter)
- Typically located outside the network security perimeter as first line of defense
- The network administrator has the heavy responsibility of configuring the firewalls.



What is a Firewall?

- A firewall is a network device .
- Hardware, software, or a combination.
- The purpose of a firewall is to enforce **a security policy** across its connections.
- To control access to a system, we need firewalls.
- A firewall is a device (usually a router or computer running special software) installed between the internal network of an organization and the rest of the Internet.
- It is designed to forward some packets and filter (not forward) others.

SECURITY POLICIES

- Security policies are a series of rules that define what traffic is permissible and what traffic is blocked or denied.
- These are not universal rules, and there are many different sets of rules for a single company with multiple connections.
- A web server connected to the Internet may be configured only to allow traffic on port 80 for HTTP, and have all other ports blocked.

What can a Firewall Protect Against?

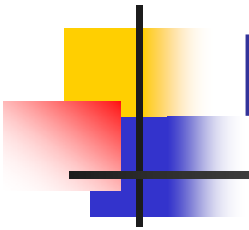
- Generally , firewalls are configured to protect against unauthenticated interactive logins from the “outside” world.
- More elaborate firewalls block traffic from the outside world to the inside, but permit users on the inside to communicate freely with the outside.
- Firewalls provide an important logging and auditing function.
- Often they provide summaries to the administrator about what kinds and amount of traffic passed through it, and how many attempts were made to break in.

Software Firewalls

- Software firewall runs as a program on a local computer (sometimes known as a personal firewall)
  - Enterprise firewalls are software firewalls designed to run on a dedicated device and protect a network instead of only one computer
  - One disadvantage is that it is only as strong as the operating system of the computer

HOW FIREWALLS WORK

- NAT
- Basic packet filtering (Stateless Packet Filtering)
- Stateful Packet Filtering
- ACLs
- Application layer proxies (Proxy Firewalls)



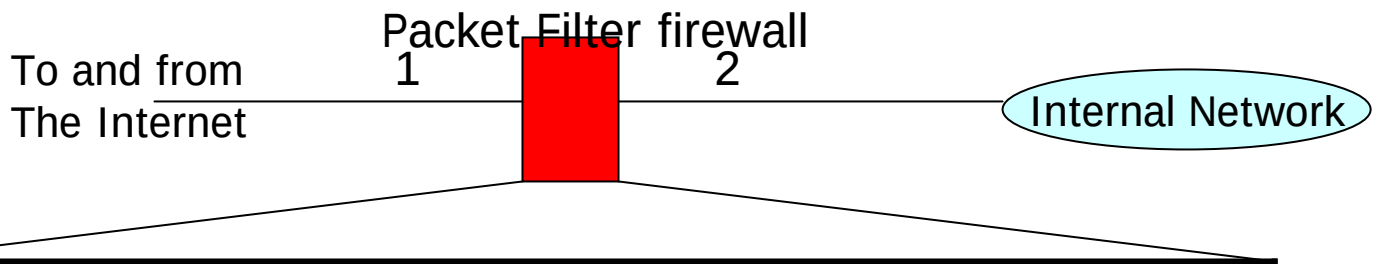
Filtering Firewalls

- Based on packet routing information
- Look at information in the incoming packet's header
- Filter packets in one of two ways:
  - Stateless packet filtering: permits or denies each packet based strictly on the rule base
  - Stateful packet filtering: records state of a connection between an internal computer and an external server; makes decisions based on connection and rule base
- Can perform content filtering to block access to undesirable Web sites

Stateless Packet Filtering

- Forwards or blocks packets based on the information in the network layer and transport layer headers : source and destination IP addresses, source and destination port addresses, type of protocol (TCP or UDP)

Packet-Filter Firewall



Interface	Source IP	Source Port	Destination IP	Destination Port
1	131.34.0.0	*	*	*
1	*	*	*	23 TELNET
1	*	*	194.71.20.8	*
2	*	80 HTTP Server	*	*

Stateful Packet Filtering

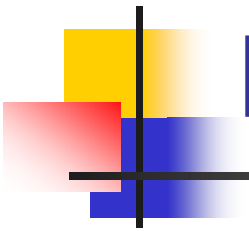
- Records the state of a connection between an internal computer and an external server and makes decisions based on :
  - the connection
  - The rule base
- Records are kept using a state table that tracks every communication channel
- Stateful inspections occur at all levels of the network and provide additional security, especially in connectionless protocols such as UDP and ICMP
- DoS attacks present a challenge because flooding techniques are used to overload the state table and effectively cause the firewall to shut down or reboot

Content Filtering Firewalls

- To block access to undesirable web sites.
- The firewall is linked to an external rule based server, or in some cases these rules are downloaded to the firewall much like updating antivirus signatures.
- These subscription-based servers contain millions of Internet addresses that are updated continuously.

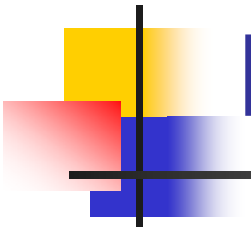
Access Control Lists ACLs

- Switches can perform security functions.
- Switches work by moving packets from inbound connections to outbound connections.
- While moving packets, it is possible to inspect the packet headers and enforce ACLs.
- ACLs act as a series of rules governing whether a packet is allowed or blocked from a connection.
- This is the function of a firewall.



Proxy Firewalls

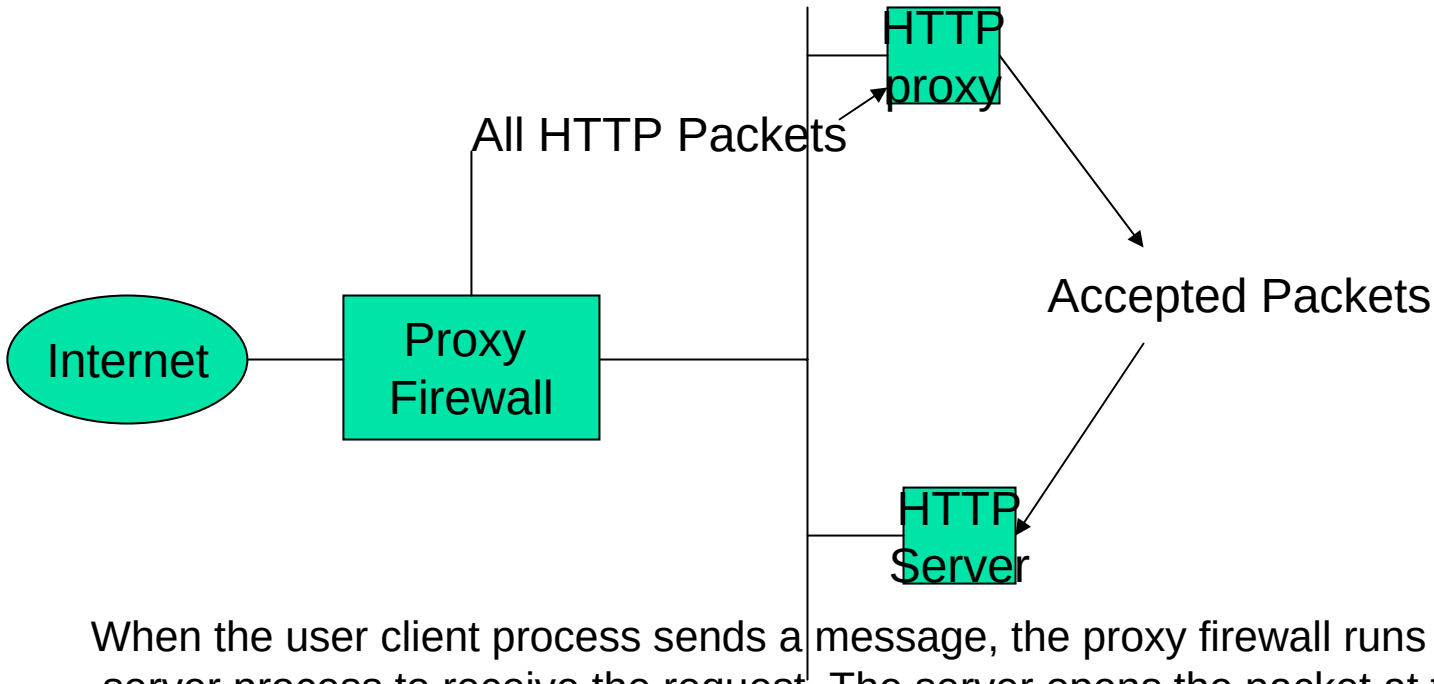
- To filter a message based on the information in the message itself (at the application layer).
- This device can defend against worms better than other kinds of firewalls.
- It does this by reassembling and analyzing packet streams instead of examining individual packets.
- Proxy firewalls can drop packets that contain requests for access to a specific URL or that attempt to access an executable program on a specific URL.



Proxy Firewalls (cont.)

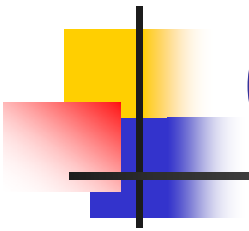
- Provides better security than packet filtering because of the increased intelligence that a proxy firewall offers
- Requests from internal network users are routed through the proxy
- The proxy, in turn, repackages the request and sends it along, thereby isolating the user from the external network
- The proxy can also offer caching, should the same request be made again, and can increase the efficiency of data delivery

Proxy Firewall

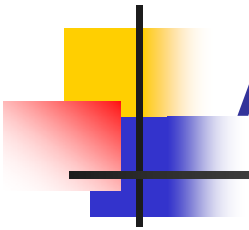


When the user client process sends a message, the proxy firewall runs a server process to receive the request. The server opens the packet at the Application level and finds out if the request is legitimate. If it is, it acts as a client process and sends the message to the real server.

Application Level Firewalls (Proxy Firewalls)



- The firewall serves as a general framework
- Various proxies are plugged into the framework
- Incoming packets are examined
  - And handled by the appropriate proxy
- Programs capable of deep understanding particular kinds of traffic : e.g. HTTP, FTP, etc
- Proxies are specialized

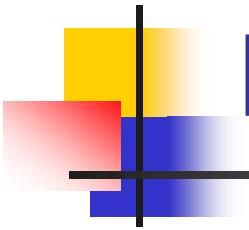


An Example Proxy

- A proxy to audit e-mail
- What might such a proxy do?
  - Allow only e-mail from particular users through
  - Or refuse e-mail from known SPAM sites
  - Or filter e-mail with unsafe inclusions (like executables)

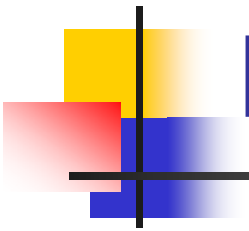
Proxy Firewalls (DUAL - HOMED)

- A proxy firewall with two NICS
- One NIC is connected to the outside network
- The other is connected to the internal network
- The proxy software manages the connection between the two NIC cards
- The setup segregates the two networks from each other and offers increased security
- The proxy function can occur at either the application level or the circuit level
- The circuit level proxy creates a circuit between the client and the server and doesn't deal with the contents of the packets that are being processed



Firewalls and Encryption

- Firewalls provide no confidentiality for data they pass back and forth
- Unless the data is encrypted
- But if the data is encrypted, the firewall can't examine it
- So typically the firewall must be able to decrypt
  - Or only work on unencrypted parts of packets



Firewalls and Viruses

- Firewalls are an excellent place to check for viruses
- Virus detection software can be run on incoming executables
- Requires that firewall knows when executables come in
- And must be reasonably fast
- Again, might be issues with encryption