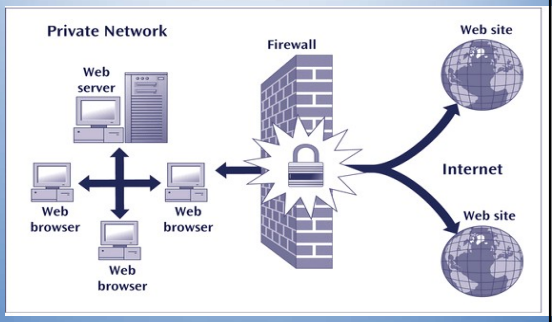
Firewall

A Wall that Protects Over Network

Firewall



What is a Firewall?

- A **check point** of control and monitoring
- Interconnects networks with differing trust
- Imposes restrictions on network services
  - only authorized traffic is allowed
- Auditing and controlling access
  - can implement alarms for abnormal behavior
- Itself immune to penetration
- Provides **perimeter defence**

Introduction

- Firewalls control the flow of network traffic
- Firewalls have applicability in networks where there is no internet connectivity
- Firewalls operate on number of layers
- Can also act as VPN gateways
- Active content filtering technologies

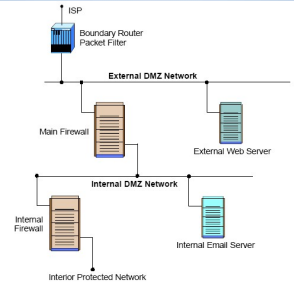
Firewall Environments

- There are different types of environments where a firewall can be implemented.
- Simple environment can be a packet filter firewall
- Complex environments can be several firewalls and proxies

Demilitarized Zone (DMZ) Environment

- Can be created out of a network connecting two firewalls
- Boundary router filter packets protecting server
- First firewall provide access control and protection from server if they are hacked

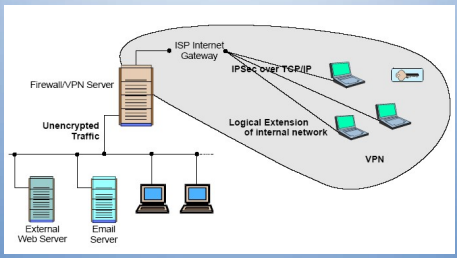
DMZ ENV



VPN

- VPN is used to provide secure network links across networks
- VPN is constructed on top of existing network media and protocols
- On protocol level IPsec (IP Security) is the first choice
- Other protocols are PPTP, L2TP (Layer2TP)

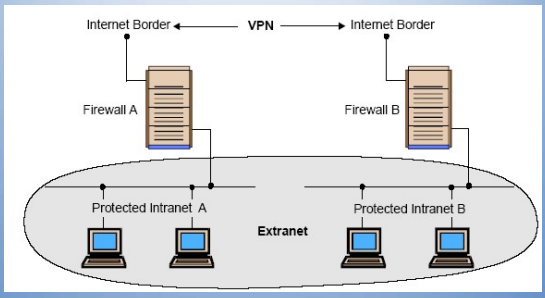
VPN



Intranets

- An intranet is a network that employs the same types of services, applications, and protocols present in an Internet implementation, without involving external connectivity
- Intranets are typically implemented behind firewall environments.

Intranets



Extranets

- Extranet is usually a business-to-business intranet
- Controlled access to remote users via some form of authentication and encryption such as provided by a VPN
- Extranets employ TCP/IP protocols, along with the same standard applications and services

Type is Firewalls

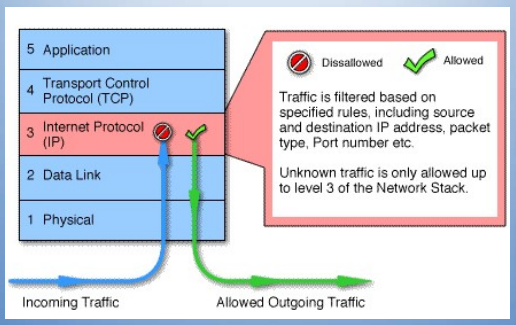
Firewalls fall into four broad categories

- Packet filters
- Circuit level
- Application level
- Stateful multilayer

Packet Filter

- Work at the network level of the OSI model
- Each packet is compared to a set of criteria before it is forwarded
- Packet filtering firewalls is low cost and low impact on network performance

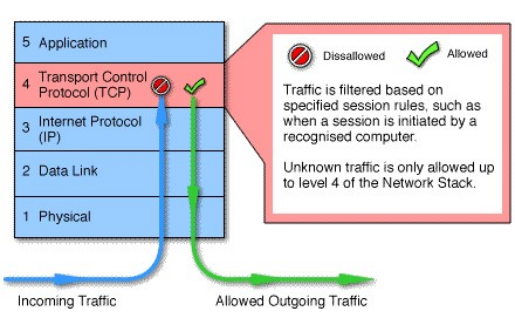
Packet Filtering



Circuit level

- Circuit level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP
- Monitor TCP handshaking between packets to determine whether a requested session is legitimate.

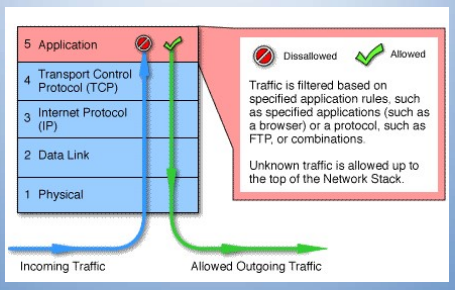
Circuit Level



Application Level

- Application level gateways, also called proxies, are similar to circuit-level gateways except that they are application specific
- Gateway that is configured to be a web proxy will not allow any ftp, gopher, telnet or other traffic through

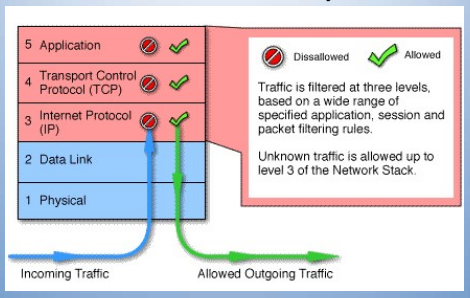
Application Level



Stateful Multilayer

- Stateful multilayer inspection firewalls combine the aspects of the other three types of firewalls
- They filter packets at the network layer, determine whether session packets are legitimate and evaluate contents of packets at the application layer

Stateful Multilayer



General Performance

FIREWALL PERFORMANCE SUMMARY

Technology	Speed	Flexibility	Intelligence
Packet filtering	V. Good	V.Good	Low
Application Proxy	Low	Low	V. Good
Stateful inspection	Good	Good	Good
Circuit gateway	Low	Low	Low

Future of Firewalls

- Firewalls will continue to advance as the attacks on IT infrastructure become more and more sophisticated
- More and more client and server applications are coming with native support for proxied environments
- Firewalls that scan for viruses as they enter the network and several firms are currently exploring this idea, but it is not yet in wide use

Conclusion

- It is clear that some form of security for private networks connected to the Internet is essential
- A firewall is an important and necessary part of that security, but cannot be expected to perform all the required security functions.

Query Session

Ask before it ends