

NETWORK SECURITY

Ch. 8: Defense Mechanism - Firewall



Firewall

- A firewall is a hardware, software, or a combination of both that monitors and filters traffic packets that attempt to either enter or leave the protected private network



Firewall Function

- Packet filtering based
- Application proxy gateways



Firwall policies



- Deny-everything-not-specifically-allowed
- Allow-everything-not-specifically-denied
 - following design goals are derived
 - That all traffic into and out of the protected network must pass through the firewall.
 - That only authorized traffic, as defined by the organizationalsecuritypolicy, in and out of the protected network, will be allowed to pass.
 - That the firewall must be immune to penetration by use of a trusted system with secure operating system.

Policies and Goals are Implemented in A Firewall



- Prevent intruders from entering and interfering with the operations of the organization's network
- Prevent intruders from acquiring proprietary organization information.
- Prevent insiders from misusing the organization resources by restricting unauthorized access to system resources.
- Provide authentication, although care must be taken because additional services to the firewall may make it less efficient.
- Provide end-points to the VPN.




Types of Firewalls

Layer	Firewall service
Application	Application-level gateways, encryption, SOCKS Proxy Server
Transport	Packet filtering (TCP, UDP, ICMP)
Network	NAT, IP-filtering
Data link	MAC address filtering
Physical	May not be available



The First Type

- Packet Inspection Firewalls
 - Are routers that inspect the contents of the source or destination addresses and ports of incoming or outgoing TCP, UDP, and ICMP packets being sent between networks and accept or reject the packet based on the specific packet policies set in the organization's security policy.
 - They based on the following information 
 - Source address
 - Destination address
 - TCP or UDP
 - ICMP
 - Payload
 - Connection initialization and datagram using TCP ACK bit



The Second

- **IP Address Filtering**

- IP address filtering rules are used to control traffic into and out of the network through the filtering of both source and destination IP addresses.

Application	Source IP	Dest IP	Action
HTTP	Any	192.x.x.x	Allow
Telnet	Any	192.x.x.x	Deny
FTP	Any	192.x.x.x	Allow



3rd

- **TCP and UDP Port Filtering**

- Although IP address header filtering works very well, it may not give the system administrator enough flexibility to allow users from a trusted network to access specific services from a server located in the "bad network" and vice versa.
 - Ex: We may not want users from the "bad network" to Telnet into any trusted network host but the administrator may want to let them excess the Web services that is on the same or another machine

Application	Protocol	Dest port	Action
HTTP	TCP	80	Allow
SSL	UDP	443	Deny
Telnet	Tcp	23	allow



4th

- Packet Filtering Based on Initial Sequence Numbers (ISN) and Acknowledgement (ACK) Bits

Sequence Num	Ip dest address	Port	ACK	Action
15	192.x.x.x	80	0	Deny
16	192.x.x.x	80	1	Allow



IPTables

```
Chain INPUT (policy ACCEPT)
target     prot opt source                               destination
```

```
Chain FORWARD (policy ACCEPT)
target     prot opt source                               destination
```

```
Chain OUTPUT (policy ACCEPT)
target     prot opt source                               destination
```



Filtering Rules - Examples

<u>Policy</u>	<u>Firewall Setting</u>
No outside Web access.	Drop all outgoing packets to any IP address, port 80
External connections to public Web server only.	Drop all incoming TCP SYN packets to any IP except 222.22.44.203, port 80
Prevent IPTV from eating up the available bandwidth.	Drop all incoming UDP packets - except DNS and router broadcasts.
Prevent your network from being used for a Smurf DoS attack.	Drop all ICMP packets going to a "broadcast" address (eg 222.22.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP



Access Control List

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all



Demilitarized zone (DMZ)



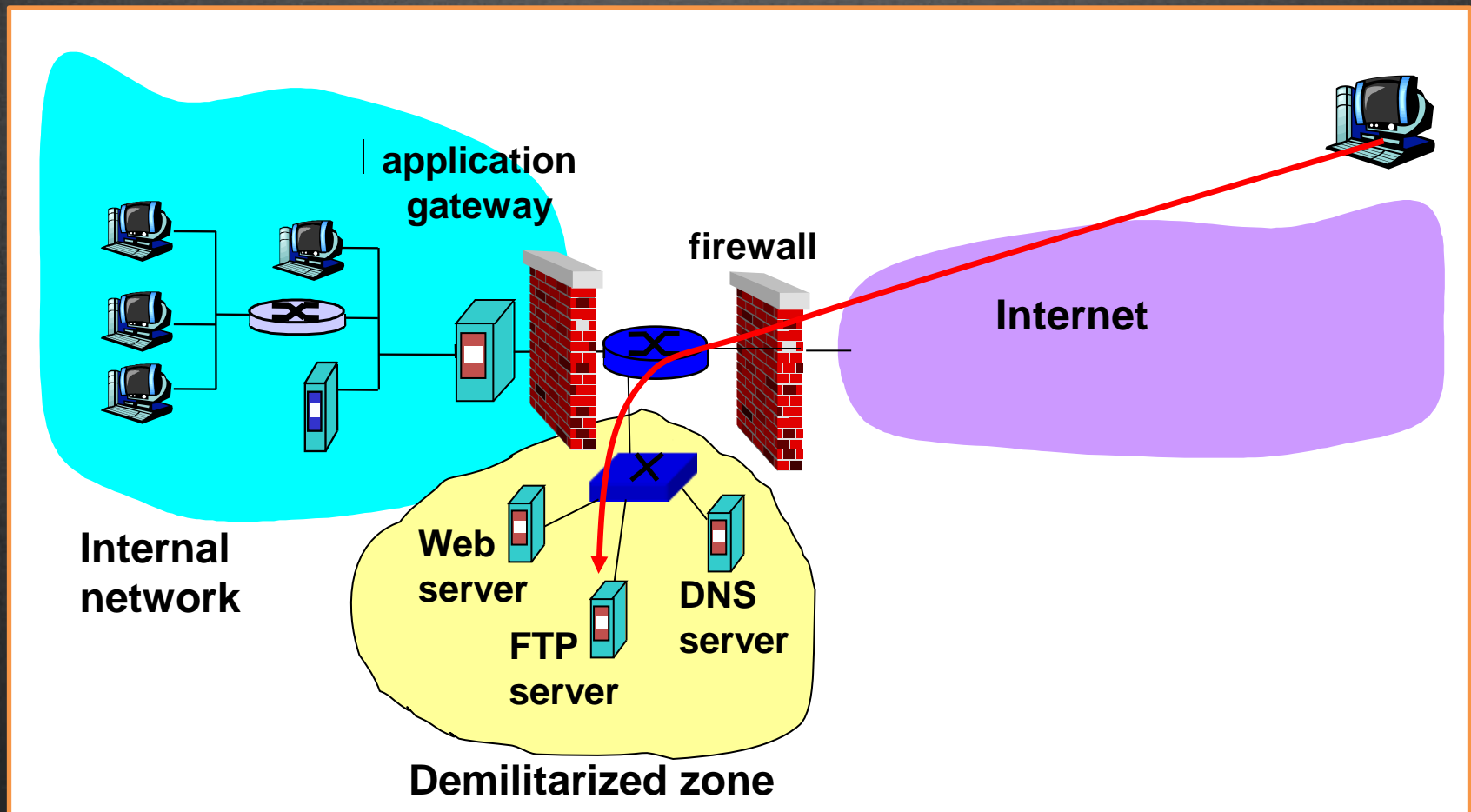


Demilitarized Zone

- Zone of servers / computers that still accessible from the outside network despite implements firewall on its network



Demilitarized Zone (DMZ)





Demilitarized Zone (DMZ)

DMZ Networks

