Chapter Six

Firewall Security

Kanaan Mikeael – University Of Human Developement

Outlines

- Perimeter Security Devices
- what firewalls are?
- why firewalls?
- Software and Hardware firewalls
- characteristics of firewalls
- types of firewall
- firewall toplogy
- firewall rulebases

Firewall

- **Perimeter Security Devices :-**
  - **Routers**
  - **Proxies**
  - **Firewalls**
  - **Firewall Rulebases**

Firewalls

- Firewall means protection a local system or network from network-based security threats while trying access to the outside world via WAN`s or the Internet.

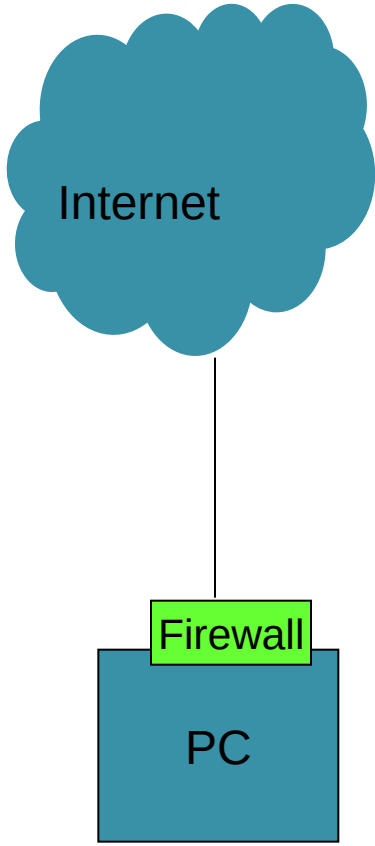
Why Firewalls ?

- Prevent attacks from untrusted networks.
- A choke point of control and monitoring .
- Imposes restrictions on network services .
  - only authorized traffic is allowed
- Provides perimeter defence .

- Firewall Design
  - Software Based Firewall
  - Hardware Based Firewall

Software Firewall

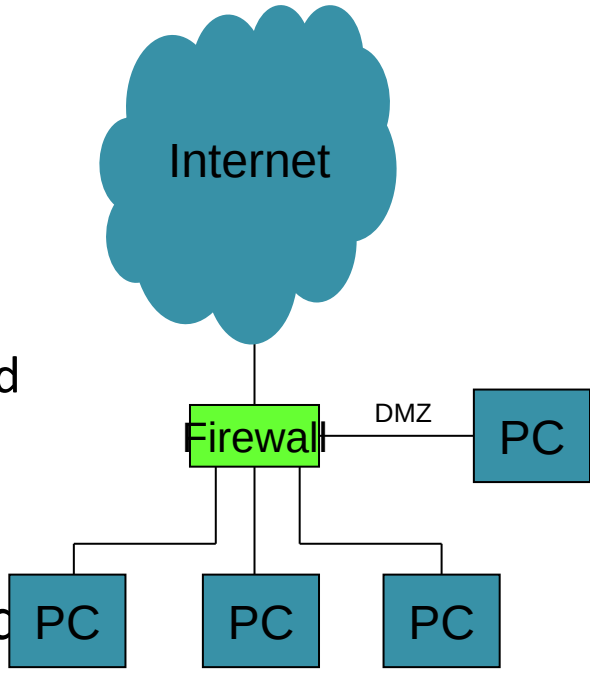
- Software loaded on a PC that performs a firewall function.
  - Protects ONLY that computer
- There are many commercially available software firewall products.



- After loading on a PC, it may have to be configured correctly in order to perform optimally.
- Many operating systems contain a built-in software firewall

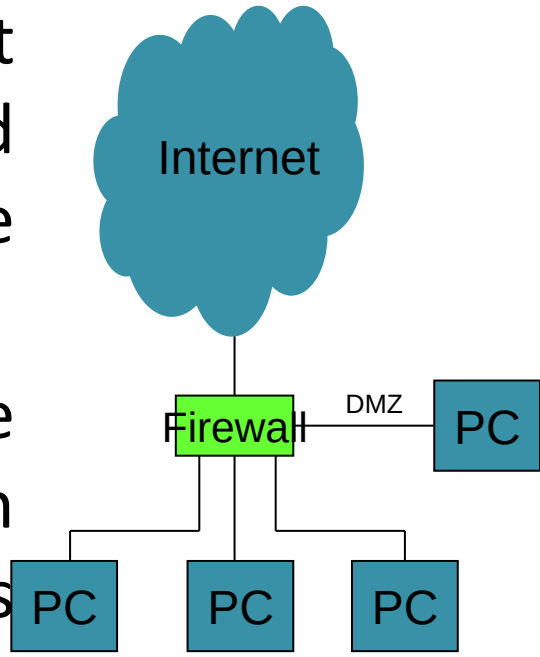
Hardware Firewall

- Hardware device located between the Internet and a PC (or PCs) that performs a firewall function
  - Protects ALL of the computers that it is behind
- May have a subnet region of lesser security protection called a Demilitarized Zone (DMZ).



Hardware Firewall contin …

- Are stand alone devices that contain all of the hardware and software needed to implement the firewall .
- Hardware based firewalls are capable of processing data much more quickly than software bases approach.
  - thus are suitable for organizations operating in a high-bandwidth environment.
  - more expensive .



Hardware Firewall contin …

- There are several commercially available hardware firewall products.

  - Major firewall vendors:

  Checkpoint

  Cisco PIX

- After installation, it may have to be configured correctly in order to perform optimally.

Firewall Characteristics

- Four general techniques:
- Service control
  - Determines the types of Internet services that can be accessed, inbound or outbound
- Direction control
  - Determines the direction in which particular service requests are allowed to flow .

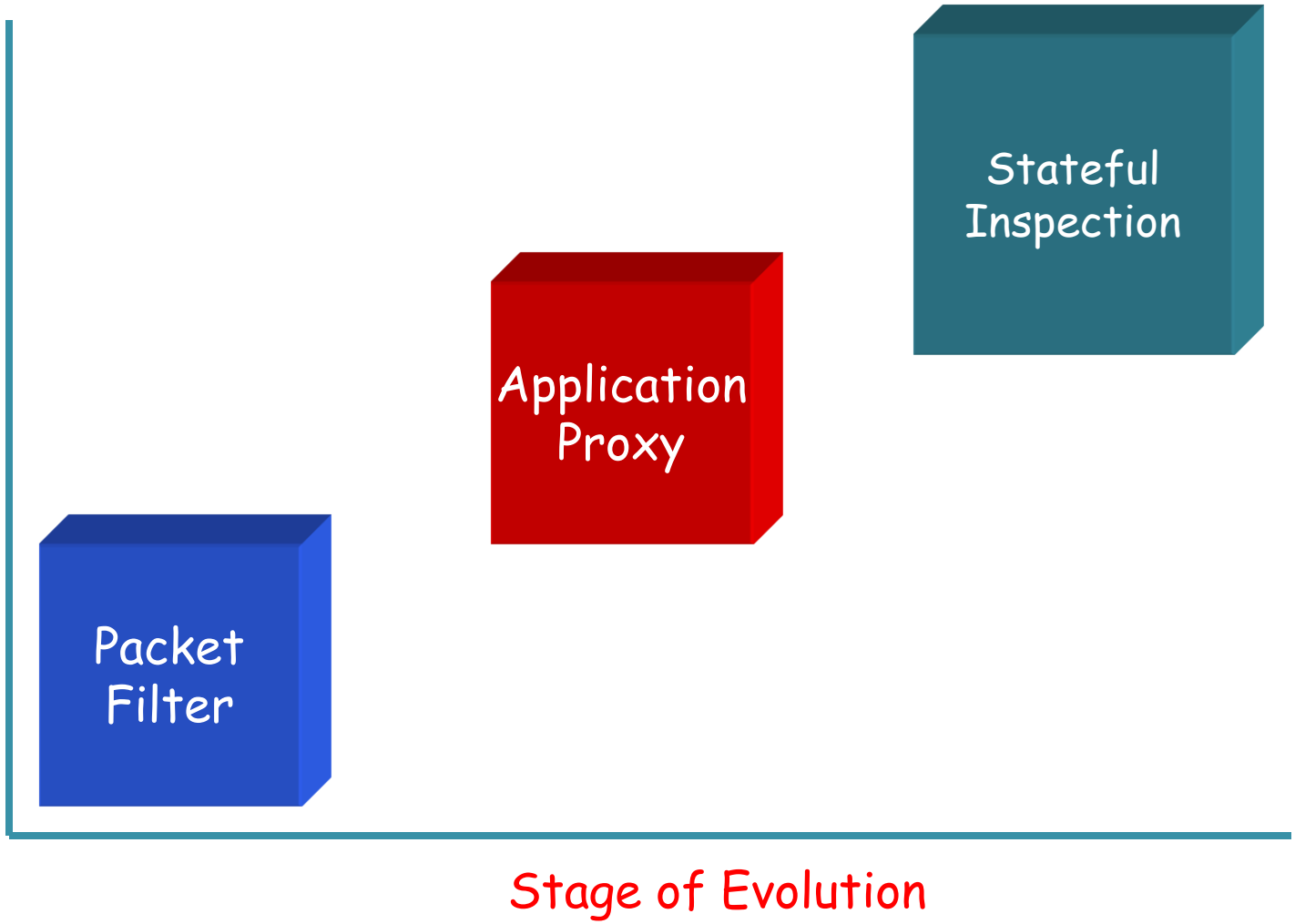
Firewall Characteristics

- User control
  - Controls access to a service according to which user is attempting to access it
- Behavior control
  - Controls how particular services are used (e.g. filter e-mail)

Types of Firewalls

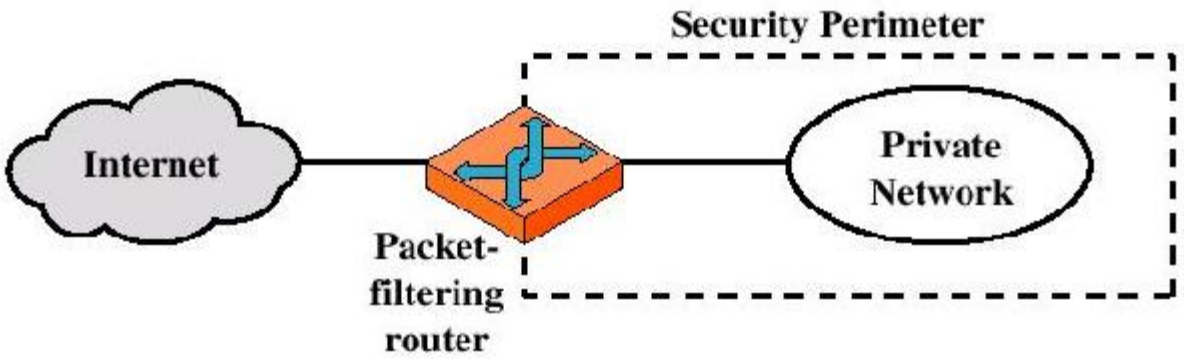
- Three common types of Firewalls:
  - Packet-filtering routers
  - Application-level gateways
  - statefull inspection

Evolution of Firewalls



Types of Firewalls

- Packet-filtering Router



Packet Filtering

- Each inbound(and/or outbound) packet is treated in an isolated manner .
- The firewall reads the packet header and analyzes the routing and protocol information contained within .
- Most common fields may be analyzed are :

  -Source address

  - Destination address

  - Destination port

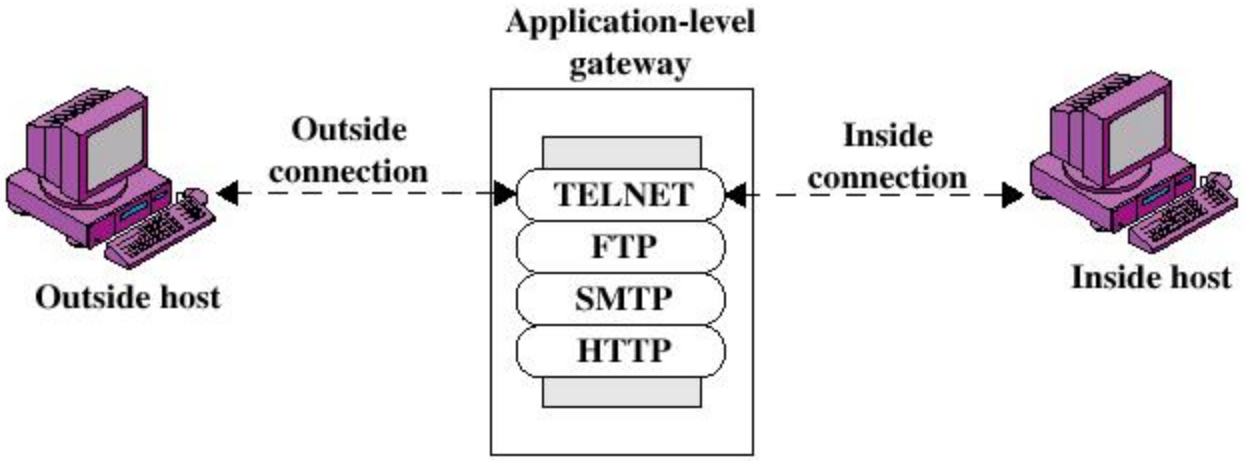
  - Transport Protocol

Packet Filtering Contin…

- Many packet filtering solutions allow us for additional factors, such as the day of the week and the time of the day .
  - for example : we may wish to allow certain types of traffic through the firewall during nonbusiness hours.
  - these capabilities allow us to use our firewall as a performance enhancing device in addition to a perimeter solution device .

Types of Firewalls

- Application-level Gateway



Types of Firewalls

- Application-level Gateway
  - Also called proxy server
  - Acts as a relay of application-level traffic

Types of Firewalls

- Advantages:
  - Higher security than packet filters
  - Only need to scrutinize a few allowable applications
  - Easy to log and audit all incoming traffic
- Disadvantages:
  - Additional processing overhead on each connection (gateway as splice point)

Stateful Packet Filters

- It is the next generation of firewall technology.
- Overcomes the major limitation of packet filtering firewalls (anlayzing each packet individually) .
- Stateful inspection firewall maintain data about open connections .
  - to ensure that packets are part of a legitimate connection initiated by an authorized user .

Stateful Packet Filters Contin …

- When a client requests a web page from a remote server :
  - 1. The client sends a request from a random high-numbered port (say 1423) to port 80 on the destination server .
  - 2. The destination server accepts the connection request and responds to port 1423 on the client from a randomly selected high-numbered port (say 2901).
  - 3. the client and server then communicate using port 1423 on the client and 2901 on the server .

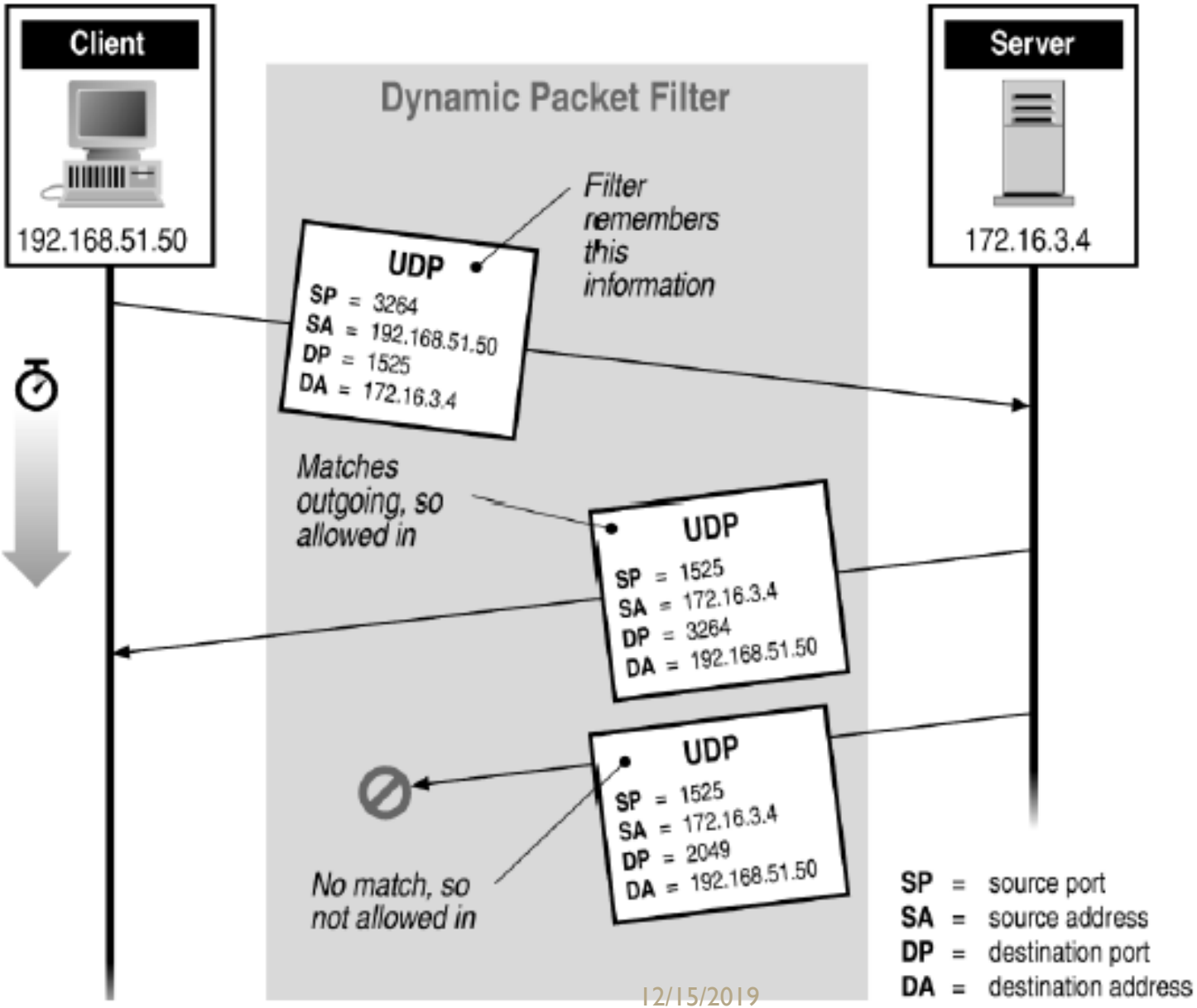
Stateful Packet Filters Contin …

- if we are using packet filtering, we must leave the high-numbered port remain open.
  - this allows remote systems to attempt to initiate communication with protected systems using those high-numbered ports.
  - Stateful inspection firewall contains advanced technology that allows them to track the status of connections.

Stateful Packet Filters Contin …

- When a client sends out an allowable connection request :
  - The firewall actively listens for the response and makes note of the two ports being used by the client and the server.
  - Traffic on those ports is then authorized to pass through the firewall for the duration of the connection.
  - When the firewall observes abnormal signature of a connection, it removes the temporary authorization and traffic between those sockets is again blocked .
  - Same action occur when a connection times out .

Stateful Filtering



Firewall Topology

- Bastion Host

  - places the firewall at the perimeter of the network .

  - incoming/outgoing traffic must pass through the firewall .

  - easiest to implement and most inexpensive.

  - has significant security risk if services are offered to outside world.

Firewall Topology

- Screened Subnet

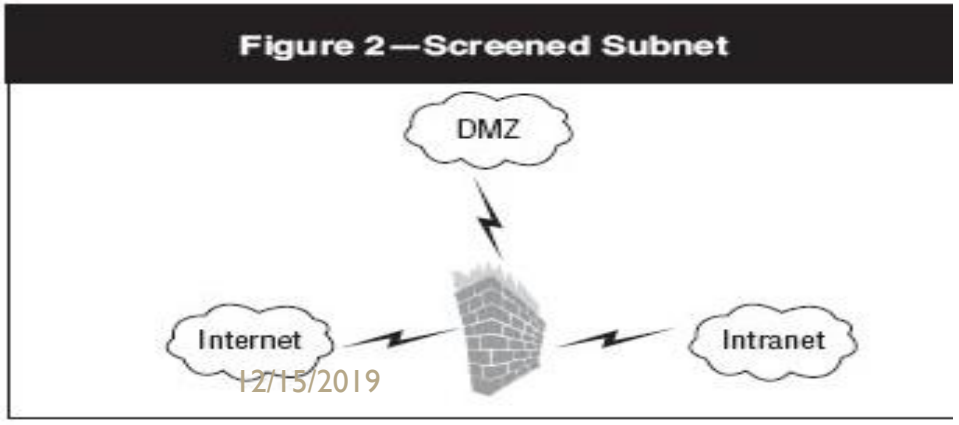
  - also known as demilitarized zone(DMZ) .

  - uses a single firewall with three NIC .

  - provides a middle ground between the internet and the internal network .

  - Administrators place systems on DMZ to provide services to external users(web service, SMTP).

  - chances are less to get access to protcted internal network.



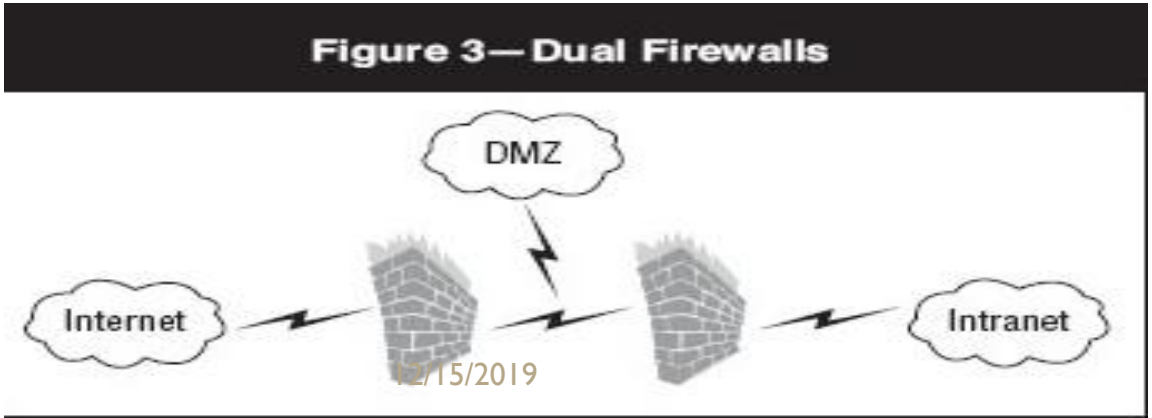
Firewall Topology

- Dual Firwalls

- provides a DMZ network used to house public services.

- uses tow firewall with 2-NIC each to create a middle ground .

- use of tow separate firewall minimize possibility of compromising a firewall itself (firewalls should be vary!) .



Firewall Rulebases

- Is one of the most important components of perimeter security architecture .
- It controls what traffic should be allowed onto the network and what traffic should be blocked.
- Each firewall solution uses a different syntax for rule specification.
- Most rules are of the form :
  - <action> <protocol> from <source_address> <source_port> to <destination_address> <destination_port>

Firewall Rulebases Contin ..

- These fields have at least the following values :
  - <action> may be either deny or allow.
  - <protocol> may be tcp, udp, or icmp.
  - <source_address> and <destination_address> may be an IP address (including network addresses), an IP address range, or the keyword “any” .
  - <source_port> and <destination_port> may be a port number or the keyword “any” .

Firewall Rulebases Contin ..

- Some of functionality types may firewalls do :
  - Drop ability for inbound traffic .
  - Block ability for inbound traffic .
  - Integrate ability with external authentication system.
    - to apply different security restrictions to different classes of users .
  - integration with virtual private network solutions.
  - provisions for (QOS) rules that prioritize certain types of network traffic .

Firewall Rulebases Contin ..

- Special Rules
  - Cleanup Rule
    - "Deny everything that is not explicitly allowed."
    - deny any from any to any any
  - Stealth Rule
    - is designed to protect the firewall itself from external or internal attack .
    - deny any from any any to firewall any, where firewall is the IP address of the firewall itself .

Thank You