University of BRISTOL

Computer System- B Security

Introduction to Network Security

Firewalls

Sanjay Rawat

Firewall Overview

- Introduction to Firewall
- Types of Firewalls
- Firewall configuration and deployment

Firewalls

Firewalls

- *A mechanism used to protect a trusted network from an untrusted network*.

Firewalls

- *A mechanism used to protect a trusted network from an untrusted network*.
- A mechanism to enforce access control policy.

Firewalls

- *A mechanism used to protect a trusted network from an untrusted network*.
- A mechanism to enforce access control policy.
- Software or Hardware based.

Firewalls

- *A mechanism used to protect a trusted network from an untrusted network*.
- A mechanism to enforce access control policy.
- Software or Hardware based.
- Deployed as gatekeeper.

Firewalls

- *A mechanism used to protect a trusted network from an untrusted network*.
- A mechanism to enforce access control policy.
- Software or Hardware based.
- Deployed as gatekeeper.
- Examples: Ipchain/Iptable, Cisco PIX, Juniper, MS ISA.

Firewall’s (in)capabilities

Firewall’s (in)capabilities

✓ Provide a focal point for monitoring.

Firewall’s (in)capabilities

- ✓Provide a focal point for monitoring.
- ✓Provide a central point for access control (who can do what).

Firewall’s (in)capabilities

- ✓Provide a focal point for monitoring.
- ✓Provide a central point for access control (who can do what).
- ✓Limit the damage that a network security problem can do to the overall network.

Firewall’s (in)capabilities

✓Provide a focal point for monitoring.

✓Provide a central point for access control (who can do what).

✓Limit the damage that a network security problem can do to the overall network.

✘ Protect against malicious insiders.

✘ Protect a connection that doesn’t go through it!!

✘ Protect against completely new threats.

✘ Protect against viruses, Trojans etc.

Firewall Deployment

Firewall Deployment

- All traffic from inside to outside, and vice versa, must pass through the firewall.

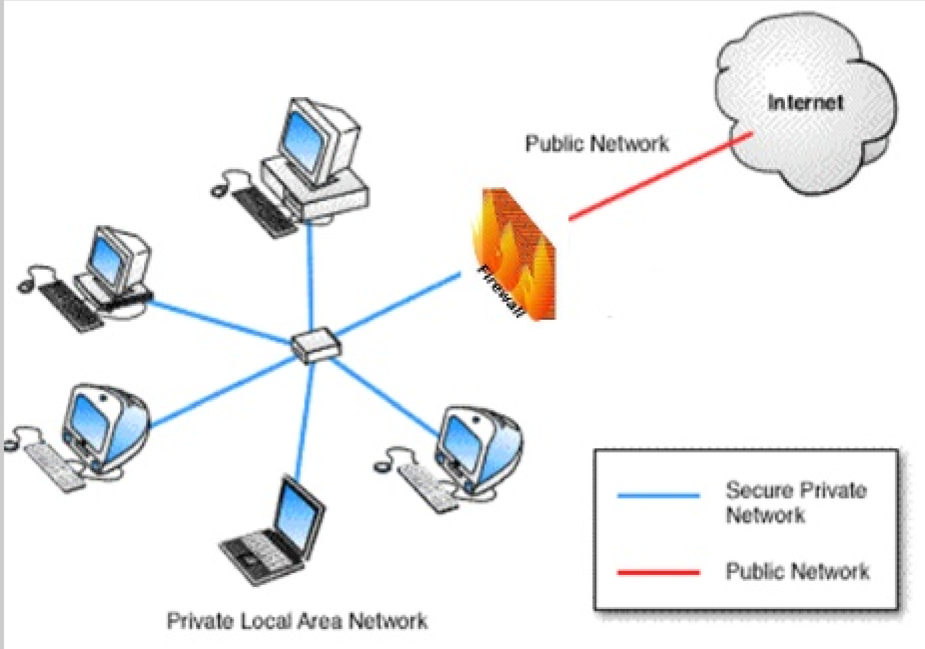
Firewall Deployment

- All traffic from inside to outside, and vice versa, must pass through the firewall.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass

Firewall Deployment

- All traffic from inside to outside, and vice versa, must pass through the firewall.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass
- Ideal Assumption: The firewall itself is immune to penetration. E.g. Cisco iOS vulnerabilities, Juniper Junos vulnerabilities.

Typical Deployment



All images are taken from doc at http://www.vicomsoft.com/learning-center/firewalls/

Generic Techniques for Enforcing policy

Generic Techniques for Enforcing policy

- Service control: Determines the types of Internet services that can be accessed.

Generic Techniques for Enforcing policy

- Service control: Determines the types of Internet services that can be accessed.
- Direction control: Determines the direction in which particular service requests are allowed.

Generic Techniques for Enforcing policy

- Service control: Determines the types of Internet services that can be accessed.
- Direction control: Determines the direction in which particular service requests are allowed.
- User control: Controls access to a service according to which user is attempting to access it. IP based filtering or authentication with IPSec.

Types of firewalls

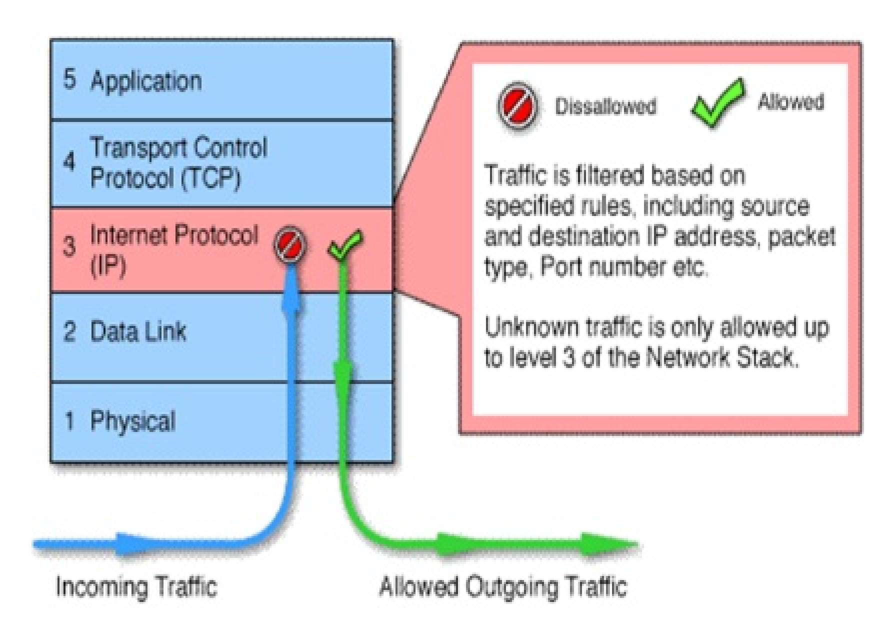
- Packet Filtering Firewall
- Stateful Inspection Firewall
- Application Level Gateway
- Circuit-level gateway

Packet filters

- Works at most up to transport layer, but at individual packet level.
- Stateless
- Fast processing

Packet filters

- Works at most up to transport layer, but at individual packet level.
- Stateless
- Fast processing


5 Application
4 Transport Control Protocol (TCP)
3 Internet Protocol (IP)
2 Data Link
1 Physical
Dissallowed
Allowed
Traffic is filtered based on specified rules, including source and destination IP address, packet type, Port number etc.
Unknown traffic is only allowed up to level 3 of the Network Stack.
Incoming Traffic
Allowed Outgoing Traffic

Example packet filters

Rule No	Action	Src IP	Dst IP	Src Port	Dst Port	Direction	Description
1	Block	IP1	*	*	*	IN	Block packets from IP1
2	Pass	*	IP_SMTP	*	25	IN	Allow packets to mail gateway
3	Pass	*	*	*	*	OUT	Allow outgoing
4	Block	*	*	*	*	IN	Block Everything Else

Problems with Packet filters

- Less visibility in the network stack -> less control.
- Hard to define rules as normal connections are request-response
  - Disallowing incoming traffic will prevent response!

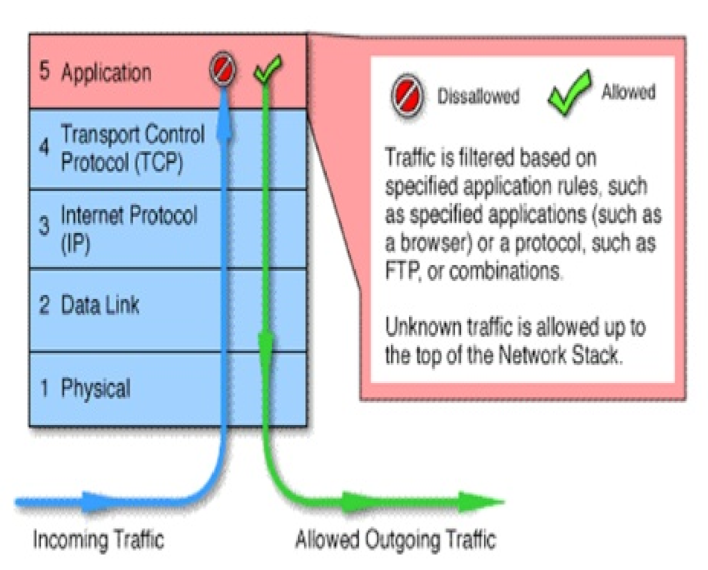
Stateful Inspection

- Keeps session information
- Decision is based on the established connections -> a table of established connection is maintained.
- Fast processing of subsequent packets.

Application gateway (aka Proxy)

- Filters traffic at application layer
- Specific to applications which are configured.
- Works at client-server mode

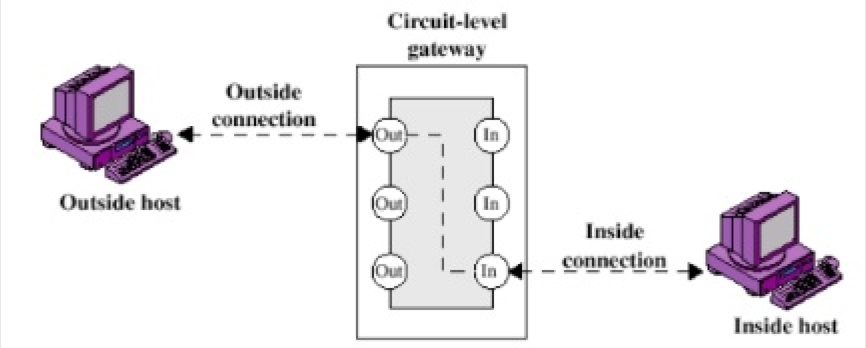
- Offer High level of security
- Have impact on network performance



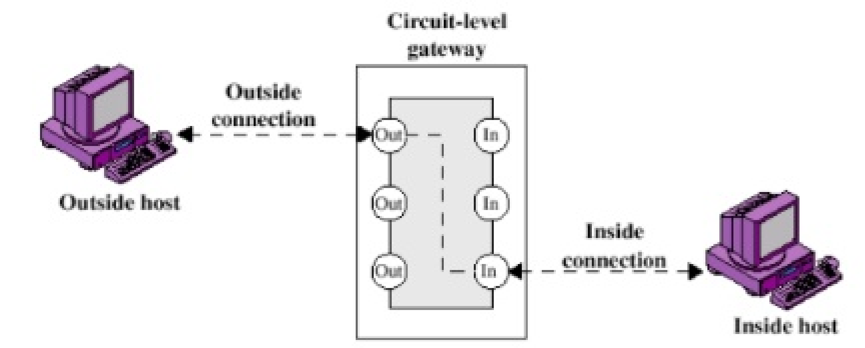
Traffic is filtered based on specified application rules, such as specified applications (such as a browser) or a protocol, such as FTP, or combinations.

Unknown traffic is allowed up to the top of the Network Stack.

Circuit Level gateway

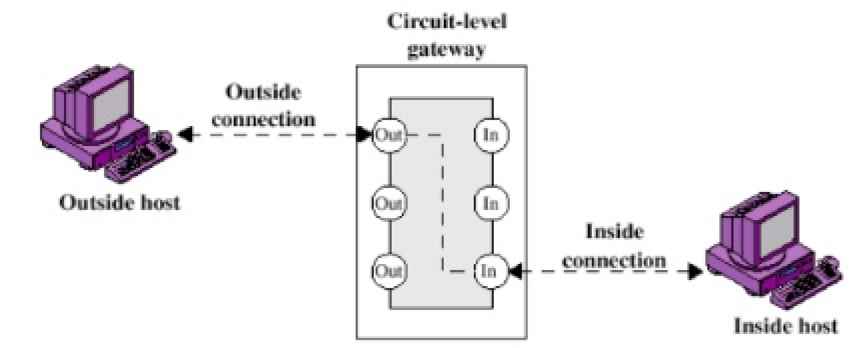


Circuit Level gateway



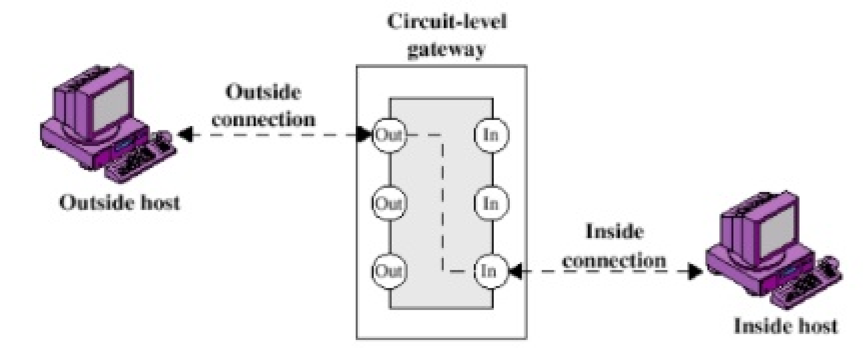
- Client-server mode.

Circuit Level gateway



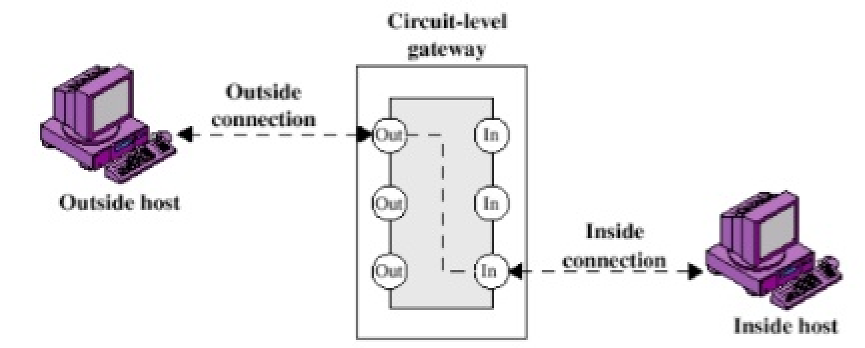
- Client-server mode.
- Always two connections (NAT/PAT).

Circuit Level gateway



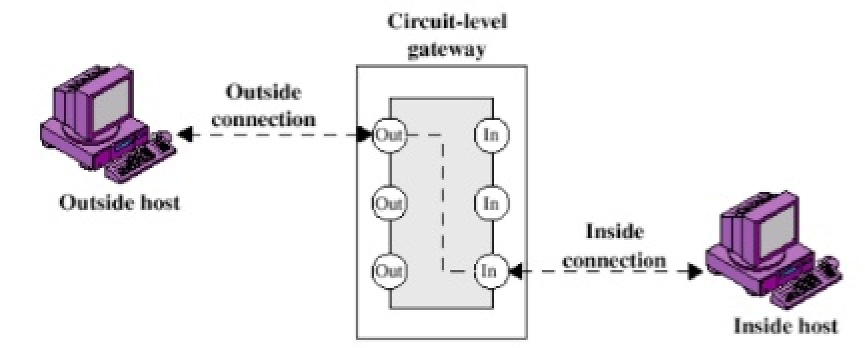
- Client-server mode.
- Always two connections (NAT/PAT).
- Hides internal network!

Circuit Level gateway



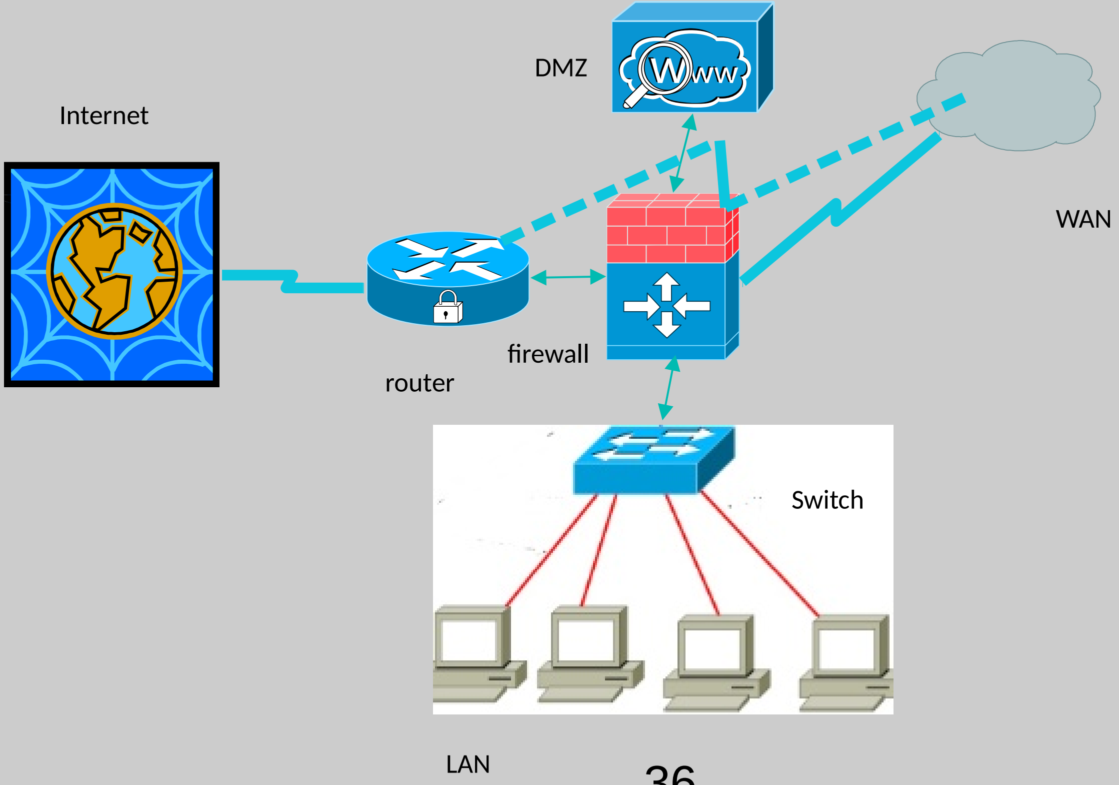
- Client-server mode.
- Always two connections (NAT/PAT).
- Hides internal network!
- Uses SOCKS protocol for client server connection.

Circuit Level gateway



- Client-server mode.
- Always two connections (NAT/PAT).
- Hides internal network!
- Uses SOCKS protocol for client server connection.
- Often used with application gateway.

Our generic design


DMZ
Internet
WAN
router
firewall
Switch
LAN