Firewalls

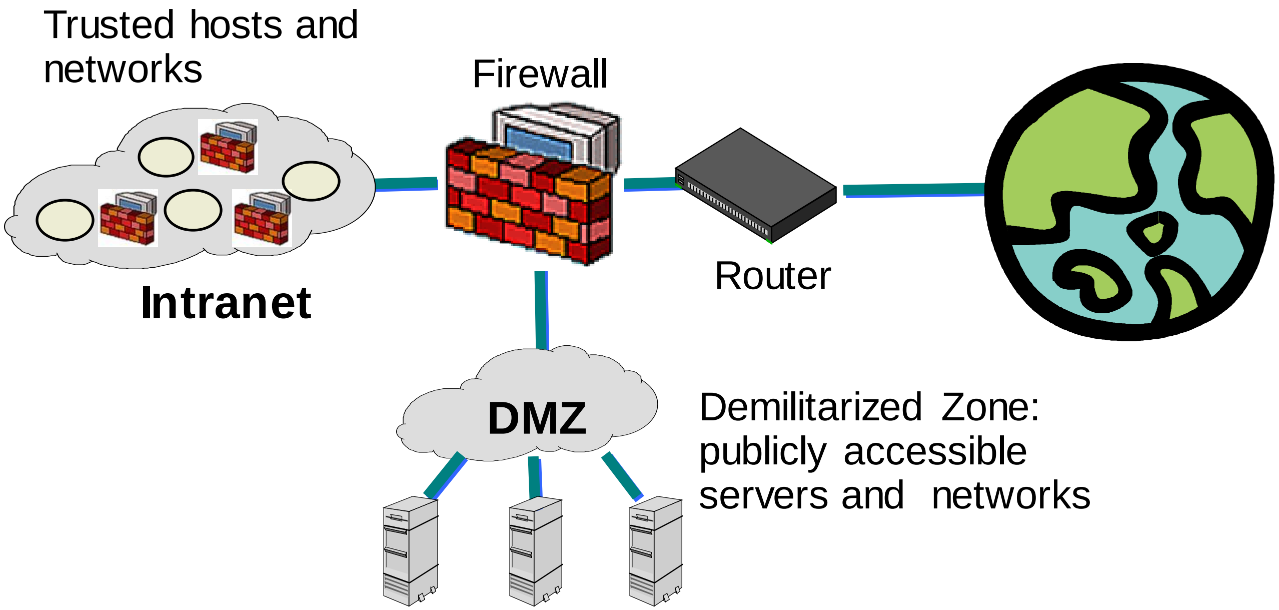
Mridul Sankar Barik

Dept. of Comp. sc. & Engg.

Jadavpur University

Firewalls

- Effective means of protecting a local system or network of systems from network-based security threats while affording access to the outside world via WAN’s or the Internet



Demilitarized Zone: publicly accessible servers and networks

Firewalls

- Placed between the premises network and the Internet/other networks to establish a controlled link
- Goals
  - Protect premises network from attacks originating outside premises network
  - Provide single choke point where security and audit can be imposed

Firewall Characteristics

- Design goals
  - All traffic from inside to outside and vice versa, must pass through the firewall (physically blocking all access to the local network except via the firewall)
  - Only authorized traffic (defined by the local security policy) will be allowed to pass
  - Firewall itself should be immune to penetration

Firewall Locations in the Network

- Between internal LAN and external network
- At the gateways of sensitive subnetworks within the organizational LAN
  - Payroll's network must be protected separately within the corporate network
- On end-user machines
  - Personal firewall

Firewall Characteristics

- Service control
  - Determines the types of services that can be accessed
- Direction control
  - Determines the direction in which particular service requests may be initiated and allowed to flow

Firewall Characteristics

- User control
  - Controls access to a service which is based on user profile
- Behavior control
  - Controls how particular services are used (e.g. filter e-mail to eliminate spams)

Firewall Limitations

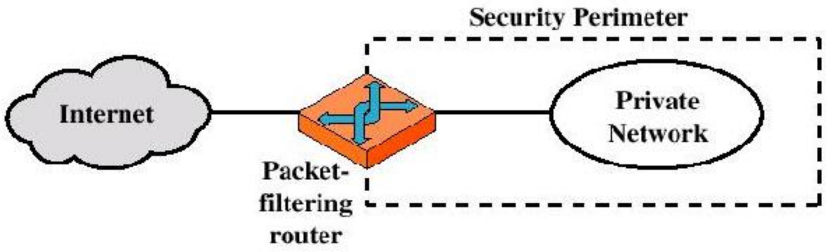
- A Firewall cannot protect against attacks that bypass the firewall
  - Internal systems may have dial out capability to connect to an ISP
  - An internal LAN may support a modem pool that provides dial-in capability for traveling employees and telecommuters
- A Firewall doesn't protect against insider threats
- A Firewall cannot protect against the transfer of virus infected files
  - Laptop, PDA, portable storage device infected outside then used inside
- Improperly secure wireless LAN

Types of Firewalls

- Packet- or session-filtering router (filter)
- Proxy gateway
  - All incoming traffic is directed to firewall, all outgoing traffic appears to come from firewall
  - Application-level: separate proxy for each application
    - Different proxies for SMTP (email), HTTP, FTP, etc.
    - Filtering rules are application-specific
  - Circuit-level: application-independent, "transparent"
    - Only generic IP traffic filtering (example: SOCKS)
- Personal firewall with application-specific rules
  - E.g., no outbound telnet connections from email client

Packet-filtering Router

- For each packet, firewall decides whether to allow it
- Decision must be made on per-packet basis
    - Stateless; cannot examine packet's context (TCP connection, application to which it belongs, etc.)
- To decide, use information available in the packet
    - IP source and destination addresses, ports
    - Protocol identifier (TCP, UDP, ICMP, etc.)
    - TCP flags (SYN, ACK, RST, PSH, FIN)
    - ICMP message type
- Filtering rules are based on pattern-matching
- If a packet doesn't match any rule, default action is taken
    - Discard - prohibit unless expressly permitted
        - more conservative, controlled, visible to users
    - Forward - permit unless expressly prohibited
        - easier to manage/use but less secure



Packet Filtering Example

Goal: Allow inbound and outbound email traffic but block all other traffic

Rule	Direction	Source Address	Destination Address	Protocol	Destination Port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Packet Filtering Example

Goal: Allow inbound and outbound email traffic but block all other traffic

Rule	Direction	Source Address	Destination Address	Protocol	Destination Port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Rule 1: Inbound mail from an external source is allowed

Packet Filtering Example

Goal: Allow inbound and outbound email traffic but block all other traffic

Rule	Direction	Source Address	Destination Address	Protocol	Destination Port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Rule 2: Allow a response to an inbound SMTP connection

Packet Filtering Example

Goal: Allow inbound and outbound email traffic but block all other traffic

Rule	Direction	Source Address	Destination Address	Protocol	Destination Port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Rule 3: Outbound email to an external source is allowed

Packet Filtering Example

Goal: Allow inbound and outbound email traffic but block all other traffic

Rule	Direction	Source Address	Destination Address	Protocol	Destination Port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Rule 4: Allow response to an inbound SMTP connection

Packet Filtering Example

Goal: Allow inbound and outbound email traffic but block all other traffic

Rule	Direction	Source Address	Destination Address	Protocol	Destination Port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Rule 5: Default policy

Packet Filtering Example

Goal: Allow inbound and outbound email traffic but block all other traffic

Rule	Direction	Source Address	Destination Address	Protocol	Destination Port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Problems: Rule 4 allows external traffic to any destination port above 1023

Attacker can open a connection from attacker's port 5150 to an internal web proxy server on port 8080

Packet Filtering Example

Goal: Allow inbound and outbound email traffic but block all other traffic

Rule	Direction	Source Address	Source Port	Destination Address	Protocol	Destination Port	Action
1	In	External	> 1023	Internal	TCP	25	Permit
2	Out	Internal	25	External	TCP	>1023	Permit
3	Out	Internal	>1023	External	TCP	25	Permit
4	In	External	25	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Any	Deny

Solution: Include source port (for rules 2 and 4 source port is 25 and for rules 1 and 3 source port is > 1023

Packet Filtering Example

Goal: Allow inbound and outbound email traffic but block all other traffic

Rule	Direction	Source Address	Source Port	Destination Address	Protocol	Destination Port	Action
1	In	External	> 1023	Internal	TCP	25	Permit
2	Out	Internal	25	External	TCP	>1023	Permit
3	Out	Internal	>1023	External	TCP	25	Permit
4	In	External	25	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Any	Deny

Problem: Attackers can gain access to internal machines by sending packets with a TCP source port number 25

Packet Filtering Example

Goal: Allow inbound and outbound email traffic but block all other traffic

Rule	Direction	Source Address	Source Port	Destination Address	Protocol	Destination Port	Flag	Action
1	In	External	> 1023	Internal	TCP	25		Permit
2	Out	Internal	25	External	TCP	>1023		Permit
3	Out	Internal	>1023	External	TCP	25		Permit
4	In	External	25	Internal	TCP	>1023	ACK	Permit
5	Either	Any	Any	Any	Any	Any		Deny

Solution: Add an ACK flag field

Packet-filtering Router

- Advantages
  - Simplicity
  - Transparency to users
  - High speed
- Disadvantages
  - Difficulty of setting up packet filter rules
  - Cannot prevent attack on application bugs
  - Limited logging functionality
  - Do not support advanced user authentication
  - Vulnerable to attacks on TCP/IP protocol bugs
  - Improper configuration can lead to breaches

Stateful Packet Filtering

- Reviews packet header information but also keeps info on TCP connections
  - Typically have low, "known" port no for server and high, dynamically assigned client port no
  - Simple packet filter must allow all return high port numbered packets back in
  - Stateful inspection packet firewall tightens rules for TCP traffic using a directory of TCP connections
  - Only allow incoming traffic to high-numbered ports for packets matching an entry in this directory
  - May also track TCP seq numbers as well

Stateful Packet Filtering

- Stateless packet filter
  - Admits packets that "make no sense," e.g., dest port = 80, ACK bit set, even though no TCP connection established:

action	source address	dest address	protocol	source port	dest port	flag bit
allow	External	Internal	TCP	80	> 1023	ACK

- Stateful packet filter: track status of every TCP connection
  - Track connection setup (SYN), teardown (FIN): can determine whether incoming, outgoing packets "makes sense"
  - Timeout inactive connections at firewall: no longer admit packets

Stateful Packet Filtering

- ACL augmented to indicate need to check connection state table before admitting packet

action	source address	dest address	proto	source port	dest port	flag bit	check conxion
allow	Internal	External	TCP	> 1023	80	any	
allow	External	Internal	TCP	80	> 1023	ACK	✗
allow	Internal	External	UDP	> 1023	53	---	
allow	External	Internal	UDP	53	> 1023	----	✗
deny	all	all	all	all	all	all	