Firewalls and Intrusion Detection Systems

Computer Networks

Firewalls & IDS Outline

- Firewalls
  - Stateless packet filtering
  - Stateful packet filtering
    - Access Control Lists
  - Application Gateways
- Intrusion Detection Systems (IDS)
  - Denial of Service Attacks

K&R Chapter 8 Outline

8.1 What is network security?

8.2 Principles of cryptography

8.3 Message integrity

8.4 Securing e-mail

8.5 Securing TCP connections: SSL

8.6 Network layer security: IPsec

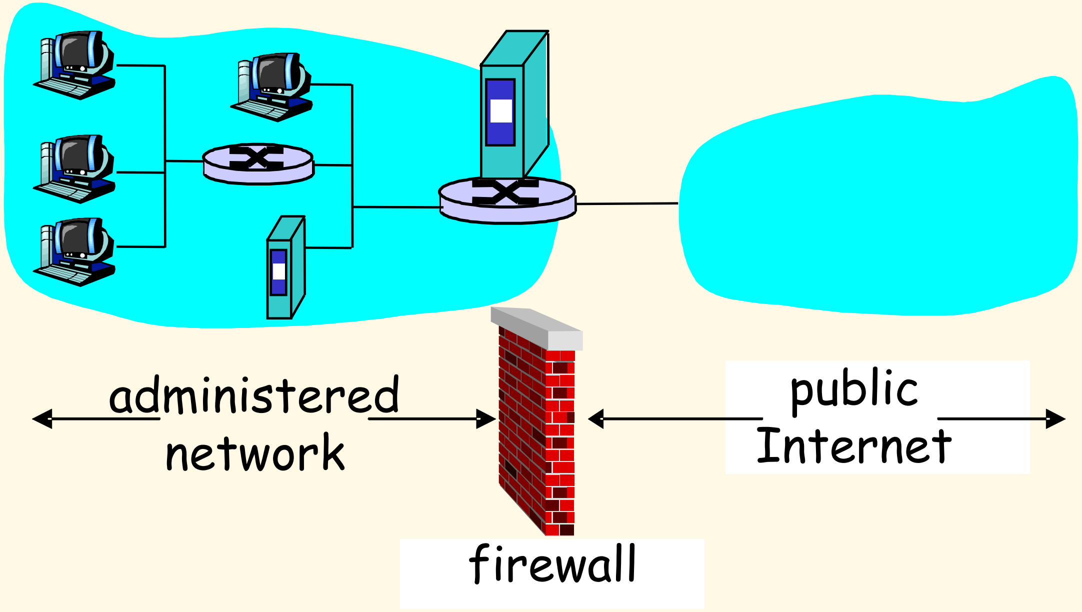
8.7 Securing wireless LANs

8.8 Operational Security: Firewalls and IDS

Firewalls

Firewall

isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others.



Why Firewalls?

prevent denial of service (DoS) attacks:

- SYN flooding: attacker establishes many bogus TCP connections, no resources left for “real” connections.

prevent illegal modification/access of internal data.

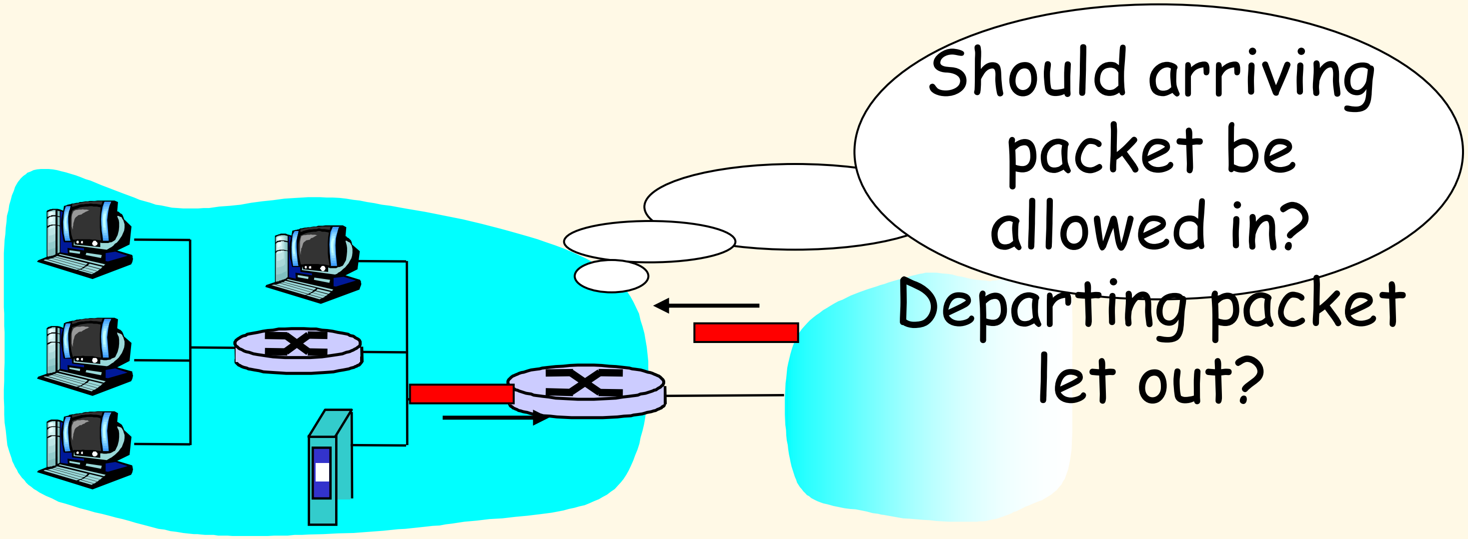
- e.g., attacker replaces CIA’s homepage with something else.

allow only authorized access to inside network (set of authenticated users/hosts)

three types of firewalls:

1. stateless packet filters
2. stateful packet filters
3. application gateways

Stateless Packet Filtering


Should arriving packet be allowed in?
Departing packet let out?

- internal network connected to Internet via router firewall.
- router filters packet-by-packet, decision to forward/drop packet based on:
  - source IP address, destination IP address
  - TCP/UDP source and destination port numbers
  - ICMP message type
  - TCP SYN and ACK bits.

Stateless Packet Filtering: Example

Example 1:

Block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23.

- all incoming, outgoing UDP flows and telnet connections are blocked.

Example 2:

Block inbound TCP segments with ACK=0.

- prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.

Stateless Packet Filtering: More Examples

Policy	Firewall Setting
No outside Web access.	Drop all outgoing packets to any IP address, port 80
No incoming TCP connections, except those for institution's public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent Web-radios 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 130.207.255.255).
Prevent your network from being tracerouted.	Drop all outgoing ICMP TTL expired traffic

Access Control Lists

- **ACL:** table of rules, applied top to bottom to incoming packets: (action, condition) pairs.

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

Stateful Packet Filtering

- stateless packet filter: heavy handed tool
  - 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	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

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

Stateful Packet Filtering

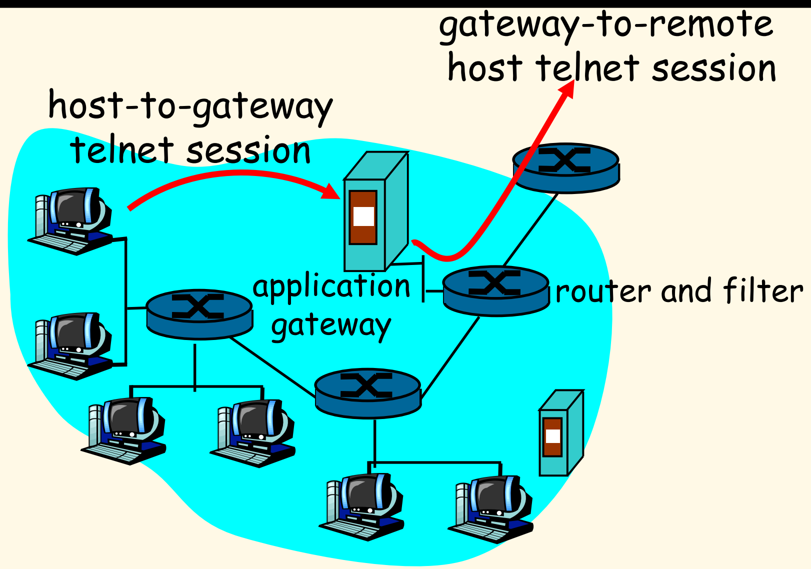
ACL augmented to indicate need to check connection state table before admitting packet.

action	source address	dest address	proto	source port	dest port	flag bit	check conxion
allow	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	

Application Gateways

- Filters packets on application data as well as on IP/TCP/UDP fields.

Example: Allow select internal users to telnet outside.


gateway-to-remote host telnet session
host-to-gateway telnet session
application gateway
router and filter

1. Require all telnet users to telnet through gateway.
2. For authorized users, gateway sets up telnet connection to dest host. Gateway relays data between two connections.
3. Router filter blocks all telnet connections not originating from gateway.

Limitations of Firewalls and Gateways

- IP Spoofing: router can't know if data "really" comes from claimed source.
- If multiple app's. need special treatment, each has own app. gateway.
- Client software must know how to contact gateway.
  - e.g., must set IP address of proxy in Web browser.
- Filters often use all or nothing policy for UDP.
- Tradeoff: degree of communication with outside world, level of security.
- Many highly protected sites still suffer from attacks.

Intrusion Detection Systems (IDS)

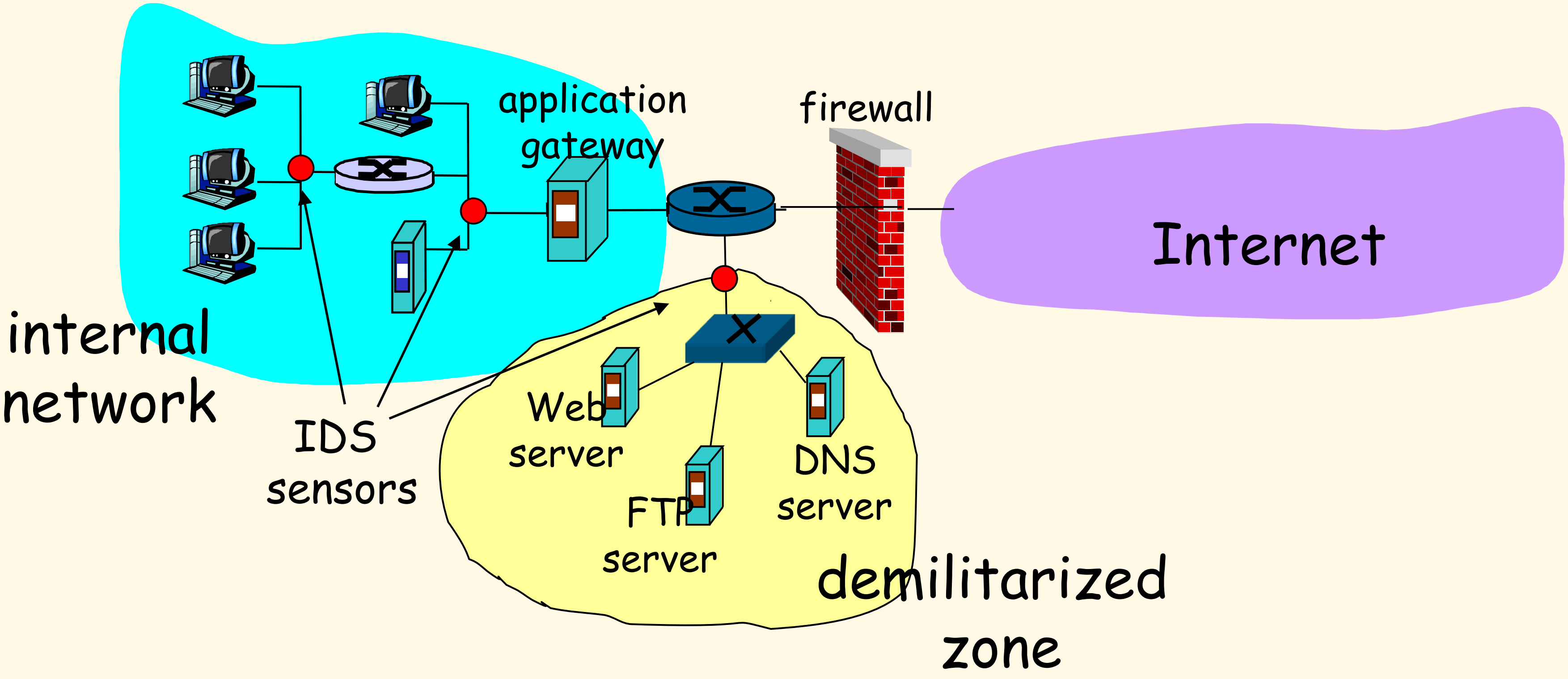
- Packet filtering:
  - operates on TCP/IP headers only.
  - no correlation check among sessions.

IDS: Intrusion Detection System

- Deep packet inspection: look at packet contents (e.g., check character strings in packet against database of known virus, attack strings).
- Examine correlation among multiple packets:
  - port scanning
  - network mapping
  - DoS attack

Intrusion Detection Systems

- Multiple IDS's: employ different types of checking at different locations.



Firewalls & IDS Summary

- Firewalls
  - Stateless packet filtering
  - Stateful packet filtering
    - Access Control Lists
  - Application Gateways
- Intrusion Detection Systems (IDS)
  - Denial of Service Attacks