

Chapter 8 roadmap

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

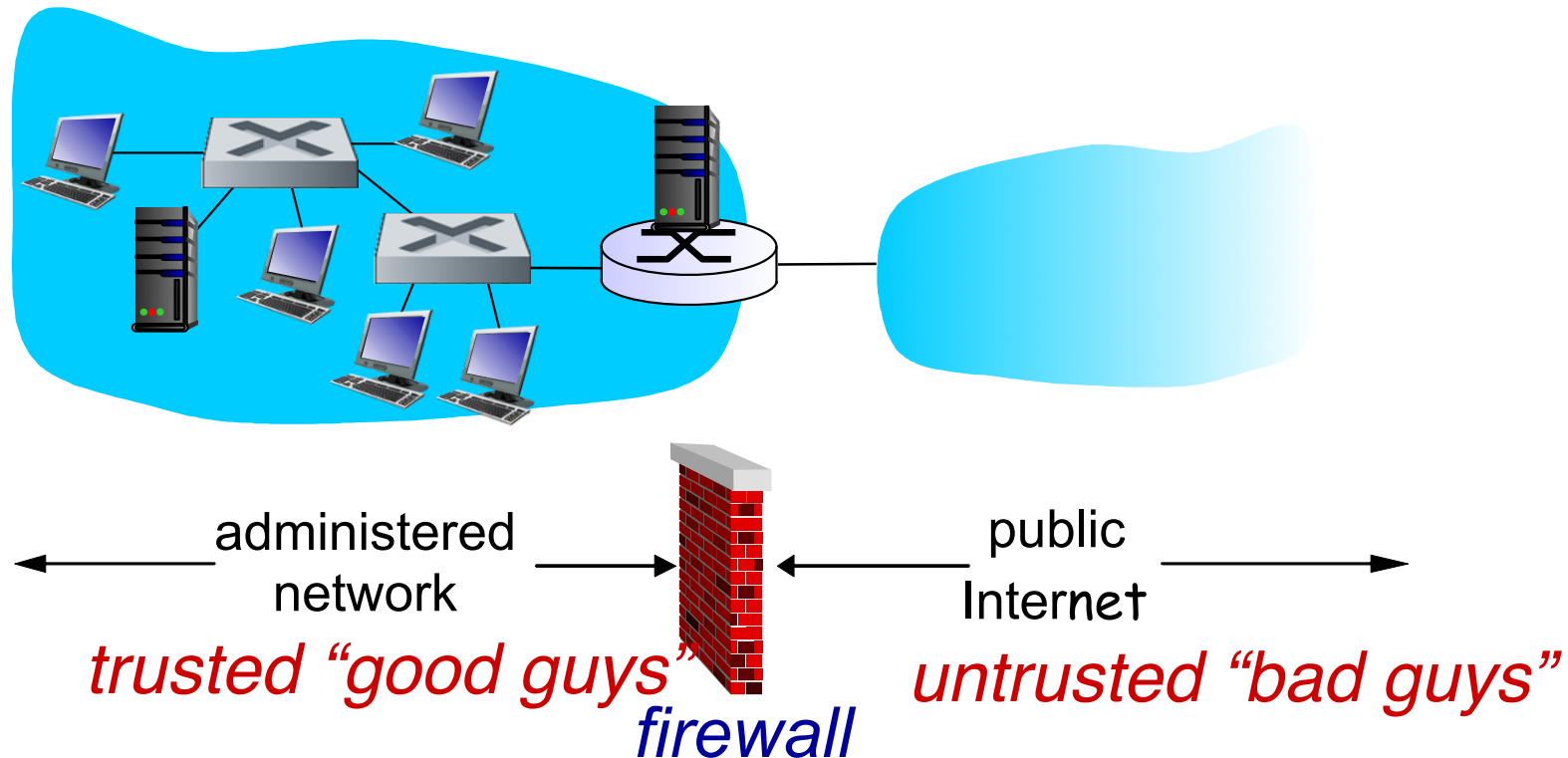
8.7 Securing wireless LANs

8.8 Operational security: firewalls and IDS

Firewalls

firewall

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



Firewalls: why

prevent denial of service 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

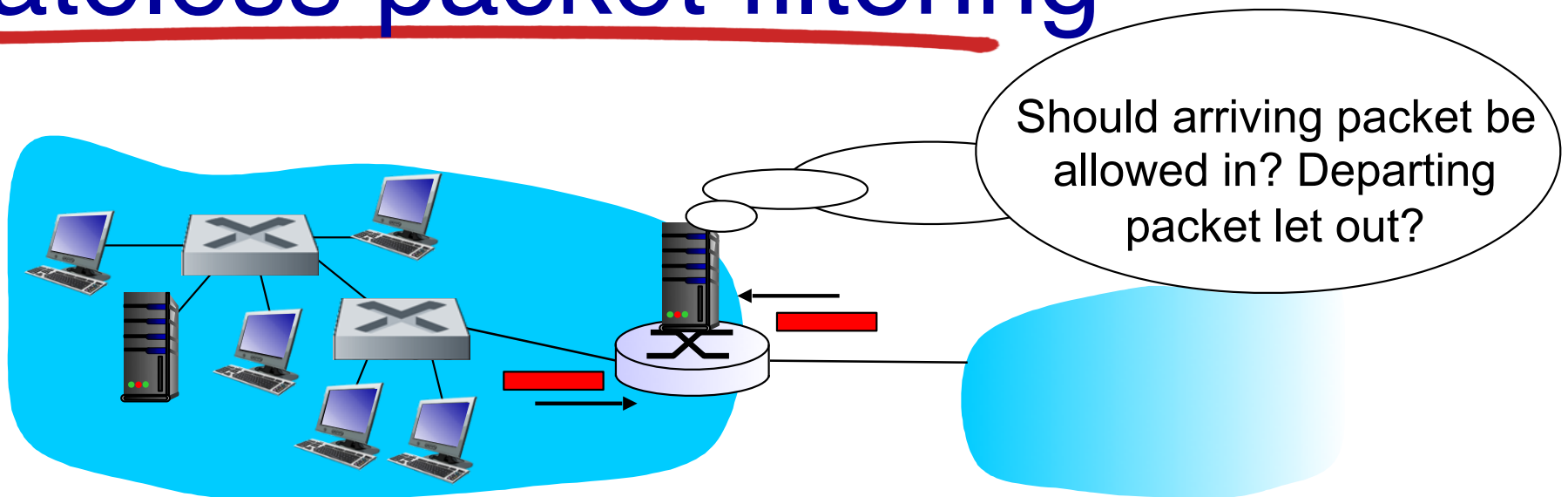
allow only authorized access to inside network

- ❖ set of authenticated users/hosts

three types of firewalls:

- ❖ stateless packet filters
- ❖ stateful packet filters
- ❖ application gateways

Stateless packet filtering



- ❖ 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
 - Protocol type in IP datagram field: TCP, UDP, ICMP, OSPF, ...
 - ICMP message type
 - TCP flag bits: e.g., 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
 - *result:* all incoming, outgoing UDP flows and telnet connections are blocked
- ❖ *example 2:* block inbound TCP segments with ACK=0.
 - *result:* prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.

Stateless packet filtering: more examples

<i>Policy</i>	<i>Firewall Setting</i>
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 (e.g. 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): determine whether incoming, outgoing packets “makes sense”
 - timeout inactive connections at firewall: no longer admit packets

netstat

Active Internet connections (w/o servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	192.168.0.20:45380	waw02s05-in-f46.1:https	ESTABLISHED
tcp	0	160	192.168.0.20:ssh	192.168.0.10:65386	ESTABLISHED
tcp	0	0	192.168.0.20:5901	192.168.0.10:65451	ESTABLISHED
tcp	0	0	192.168.0.20:48723	waw02s05-in-f42.1:https	ESTABLISHED

Active Internet connections (w/o servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	192.168.0.20:45383	waw02s05-in-f46.1:https	ESTABLISHED
tcp	0	0	192.168.0.20:51425	94.232.172.247:http	ESTABLISHED
tcp	0	0	192.168.0.20:39739	108.161.189.160:http	ESTABLISHED
tcp	0	0	192.168.0.20:39738	108.161.189.160:http	ESTABLISHED
tcp	0	0	192.168.0.20:45380	waw02s05-in-f46.1:https	ESTABLISHED
tcp	0	160	192.168.0.20:ssh	192.168.0.10:65386	ESTABLISHED
tcp	0	0	192.168.0.20:34100	waw02s05-in-f35.1:https	ESTABLISHED
tcp	0	0	192.168.0.20:5901	192.168.0.10:65451	ESTABLISHED
tcp	0	0	192.168.0.20:48723	waw02s05-in-f42.1:https	ESTABLISHED
tcp	0	0	192.168.0.20:39742	108.161.189.160:http	ESTABLISHED
tcp	0	0	192.168.0.20:51426	94.232.172.247:http	ESTABLISHED
tcp	0	0	192.168.0.20:39740	108.161.189.160:http	ESTABLISHED
tcp	0	0	192.168.0.20:39743	108.161.189.160:http	ESTABLISHED
tcp	0	0	192.168.0.20:51427	94.232.172.247:http	ESTABLISHED
tcp	0	0	192.168.0.20:39741	108.161.189.160:http	ESTABLISHED

netstat

Active Internet connections (w/o servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	192.168.0.20:45406	waw02s05-in-f46.1:https	ESTABLISHED
tcp	0	0	192.168.0.20:ssh	192.168.0.10:65386	ESTABLISHED
tcp	0	66007	192.168.0.20:5901	192.168.0.10:65451	ESTABLISHED
tcp	1388	0	192.168.0.20:45407	waw02s05-in-f46.1:https	ESTABLISHED

Active Internet connections (w/o servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	1	192.168.0.20:41269	173.194.32.130:https	SYN_SENT
tcp	0	0	192.168.0.20:51464	94.232.172.247:http	ESTABLISHED
tcp	0	160	192.168.0.20:ssh	192.168.0.10:65386	ESTABLISHED
tcp	0	1	192.168.0.20:41270	173.194.32.130:https	SYN_SENT
tcp	0	0	192.168.0.20:5901	192.168.0.10:65451	ESTABLISHED

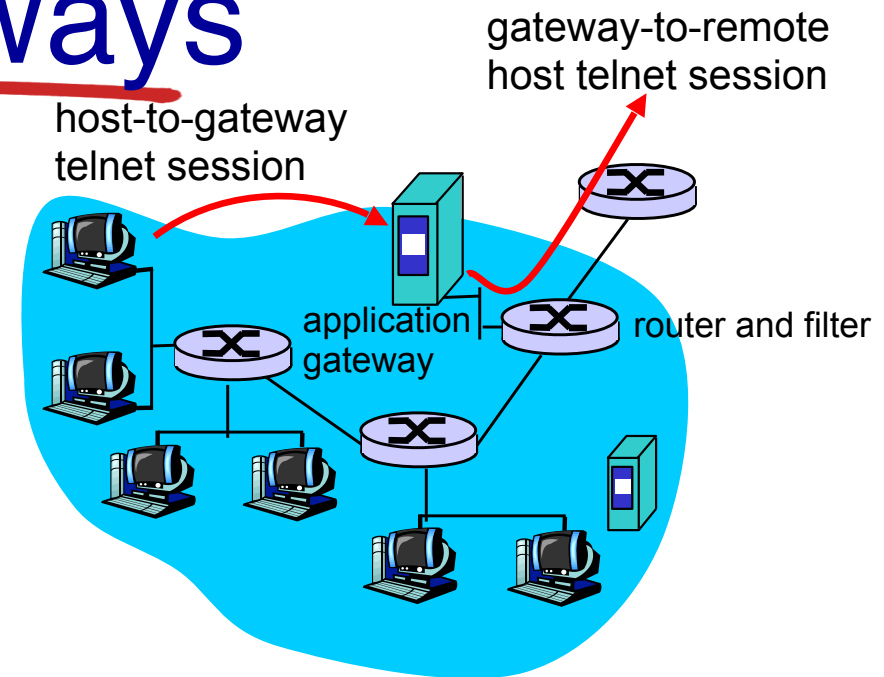
Stateful packet filtering

- ❖ 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	X
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	X
deny	all	all	all	all	all	all	

Application gateways

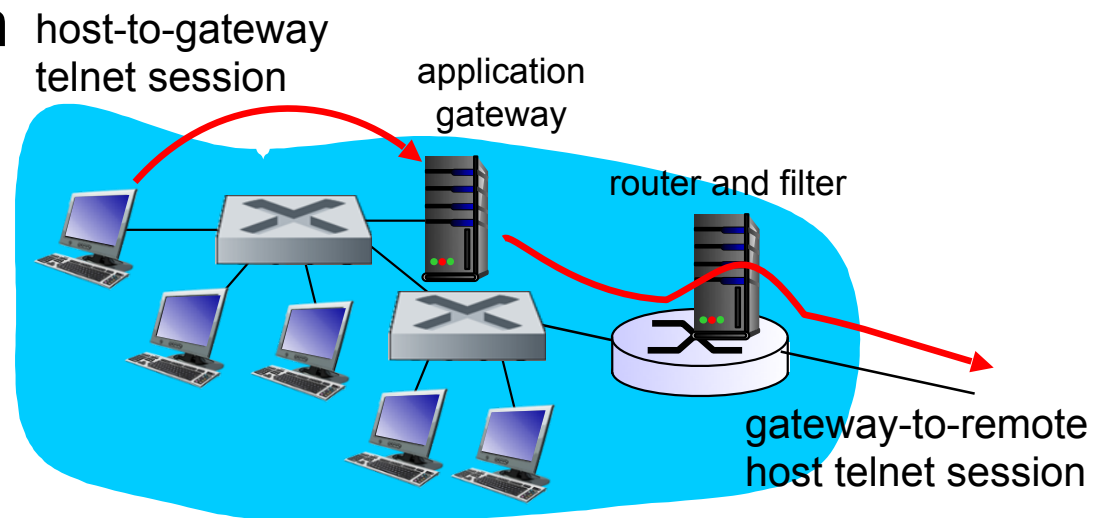
- ❖ filters packets on application data as well as on IP/TCP/UDP fields.
- ❖ *example:* allow select internal users to telnet outside.



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 2 connections
3. router filter blocks all telnet connections not originating from gateway.

Application gateways

- ❖ filter packets on application data as well as on IP/TCP/UDP fields.
- ❖ *example*: allow select internal users to telnet outside



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 2 connections
3. router filter blocks all telnet connections not originating from gateway.

Limitations of firewalls, 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

- ❖ 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 IDSs: different types of checking at different locations

