Computer Networks
COL 334/672

Network Security

Tarun Mangla

Slides adapted from KR

Sem 1, 2024-25

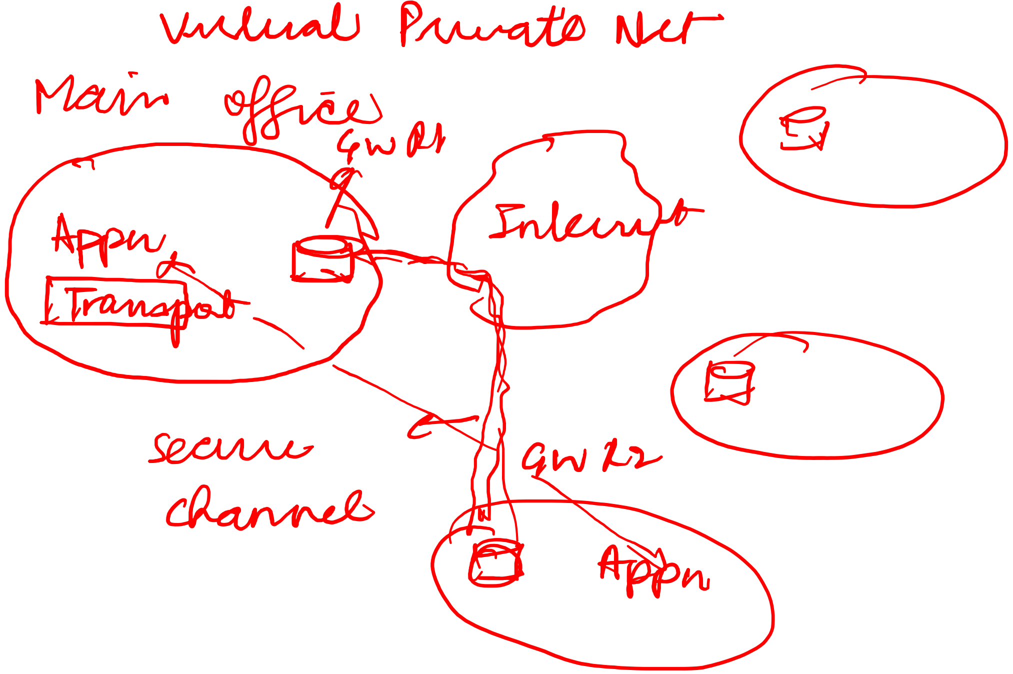
Moodle Quiz

Password: rsa

This Class

- Security for:
  - Email
  - TCP using TLS
  - **Network-layer** / IPSec

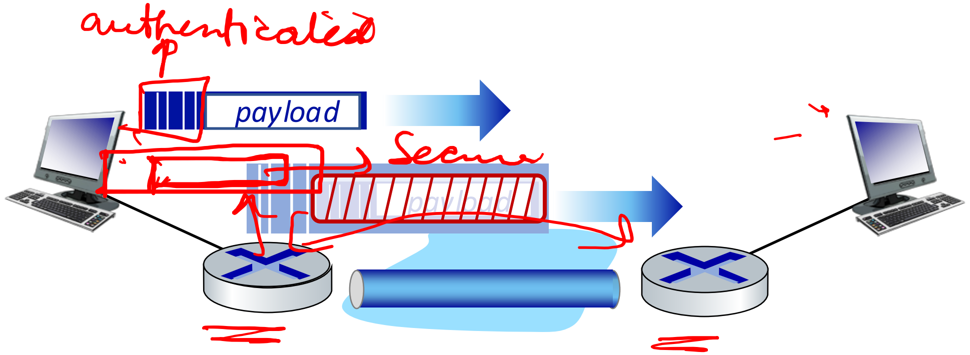
Operational security: firewall and IDS

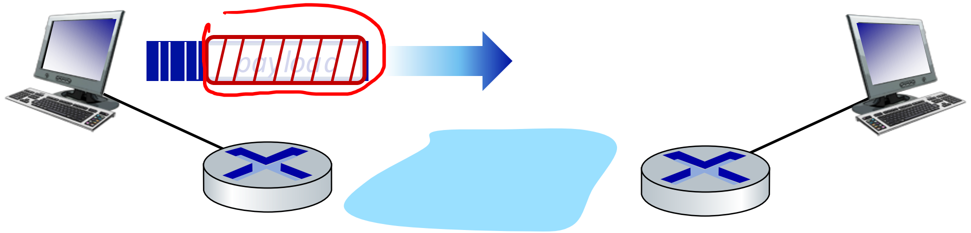


IP Sec

packet

- provides datagram-level encryption, authentication, integrity
  - for both user traffic and control traffic (e.g., BGP, DNS messages)
- two “modes”:





transport mode:

- *only* datagram *payload* is encrypted, authenticated

tunnel mode:

- entire datagram is encrypted, authenticated
- encrypted datagram encapsulated in new datagram with new IP header, tunneled to destination

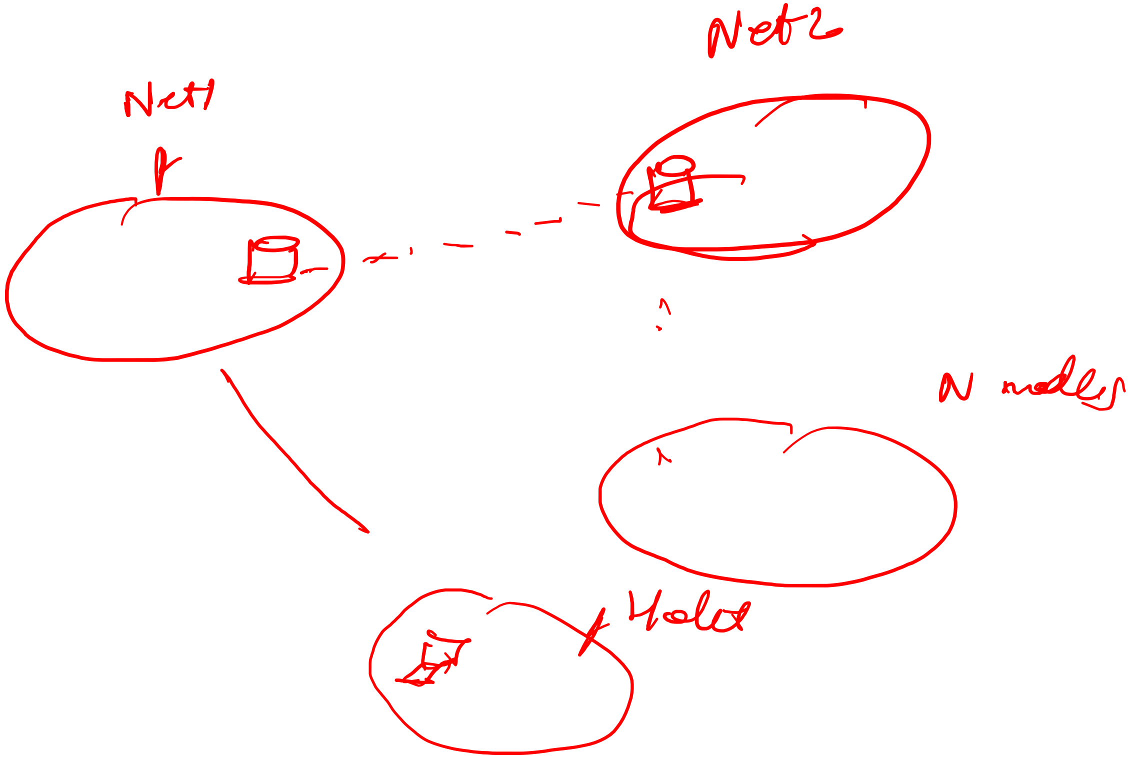
Two IPsec protocols

- Authentication Header (AH) protocol [RFC 4302]
  - provides source authentication & data integrity but *not* confidentiality
- Encapsulation Security Protocol (ESP) [RFC 4303]
  - provides source authentication, data integrity, *and confidentiality*
  - more widely used than AH

IPSec Phases →(ESP)

Public key cryptography to exchange

- How to exchange security keys? →
- How to transmit data? →

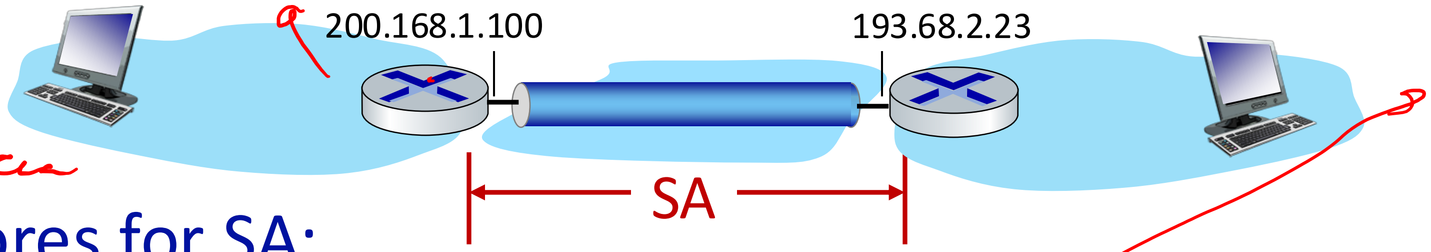


Security associations (SAs)

Internet Key Exchange

- before sending data, security association (SA) established from sending to receiving entity (directional)
- ending, receiving entitles maintain *state information* about SA
  - recall: TCP endpoints also maintain state info
  - IP is connectionless; IPsec is connection-oriented!

SA Database



SPI

Security Associa

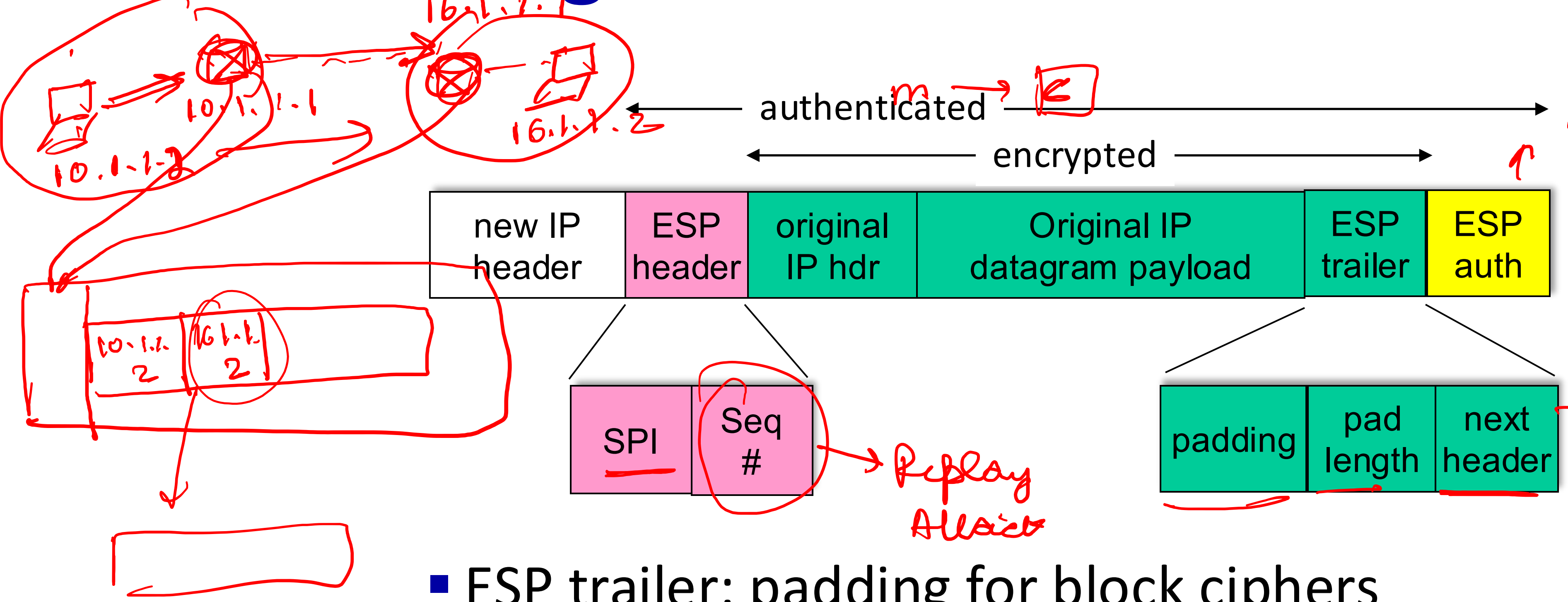
R1 stores for SA:

- 32-bit identifier: *Security Parameter Index (SPI)*
- origin SA interface (200.168.1.100)
- destination SA interface (193.68.2.23)
- type of encryption used
- encryption key
- type of integrity check used
- authentication key

Cipher scheme ← n-bit

Cipher-block encryption

IPsec datagram: Data transmission



Message Authentication Code

tunnel mode ESP

→ protocol UDP / TCP

- ESP trailer: padding for block ciphers
- ESP header:
  - SPI, so receiving entity knows what to do
  - sequence number, to thwart replay attacks
- MAC in ESP auth field created with shared secret key

This Class

- Security for:
  - Email
  - TCP
  - Network-layer

WiFi

/ Kerebros → Protocol

- **Operational security: firewall and IDS**

What is network security?

confidentiality: only sender, intended receiver should "understand" message contents

- sender encrypts message
- receiver decrypts message

authentication: sender, receiver want to confirm identity of each other

message integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

access and availability: services must be accessible and available to users

Why Operational Security?

prevent denial of service attacks:

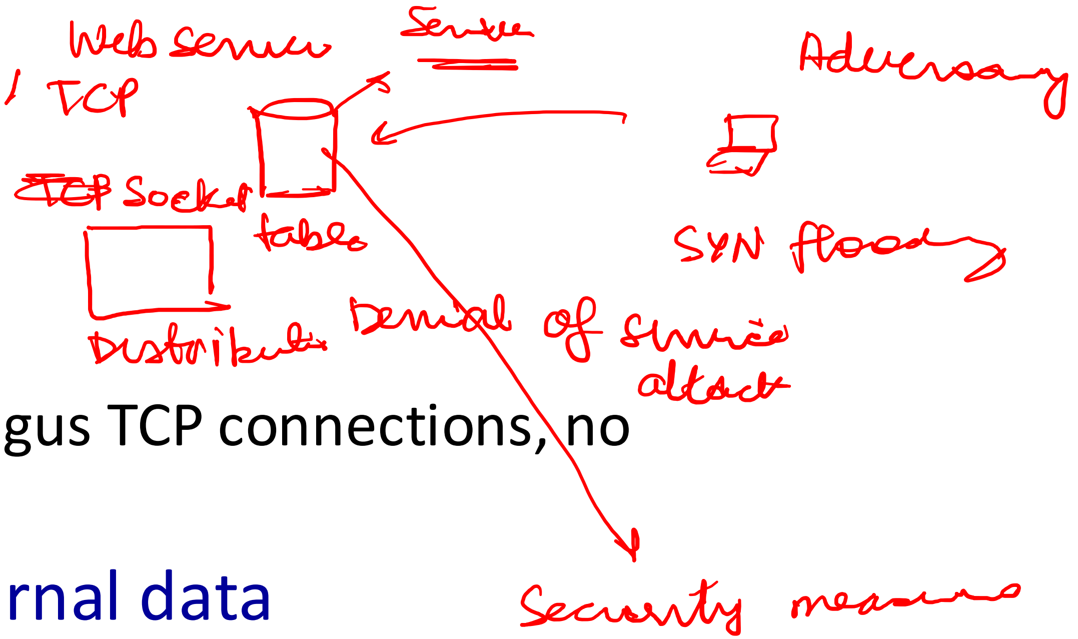
- SYN flooding: attacker establishes many bogus TCP connections, no resources left for "real" connections

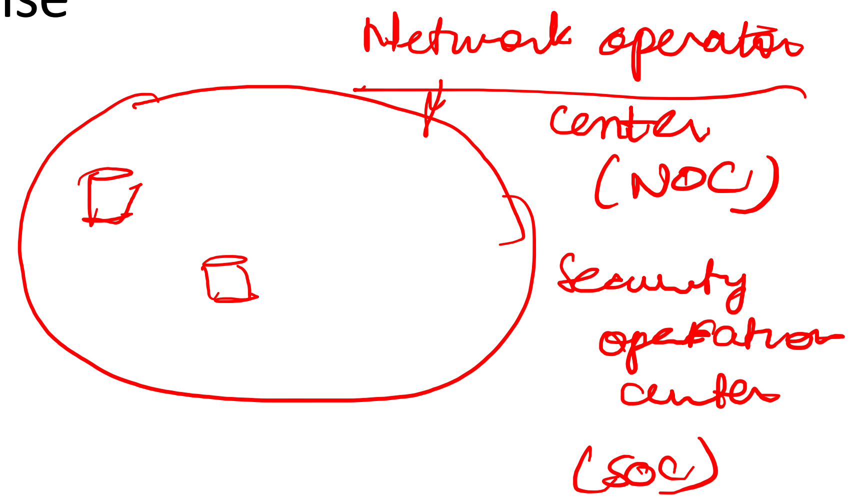
prevent illegal modification/access of internal data

- e.g., attacker replaces homepage with something else

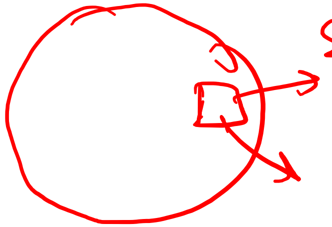
allow only authorized access to inside network

- set of authenticated users/hosts





Firewalls



Single Entry

Guard the entry point

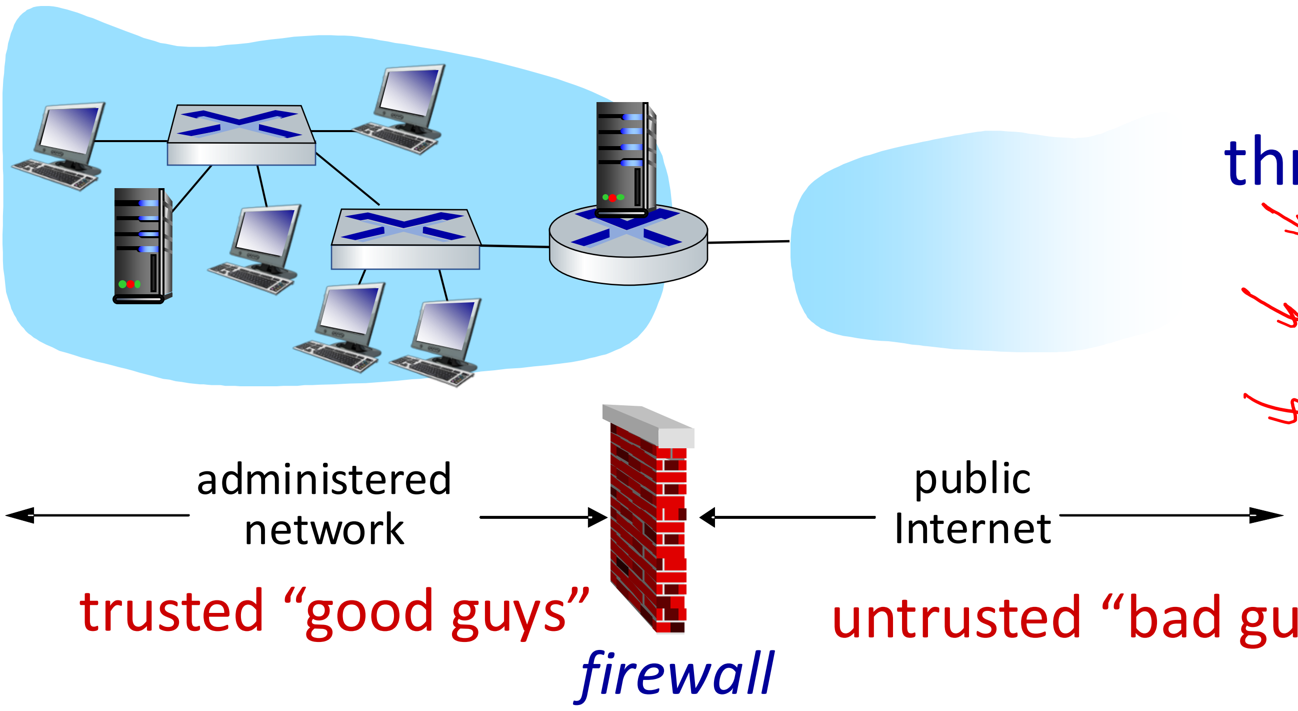
(src, dst)

(5-tuple)

firewall

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

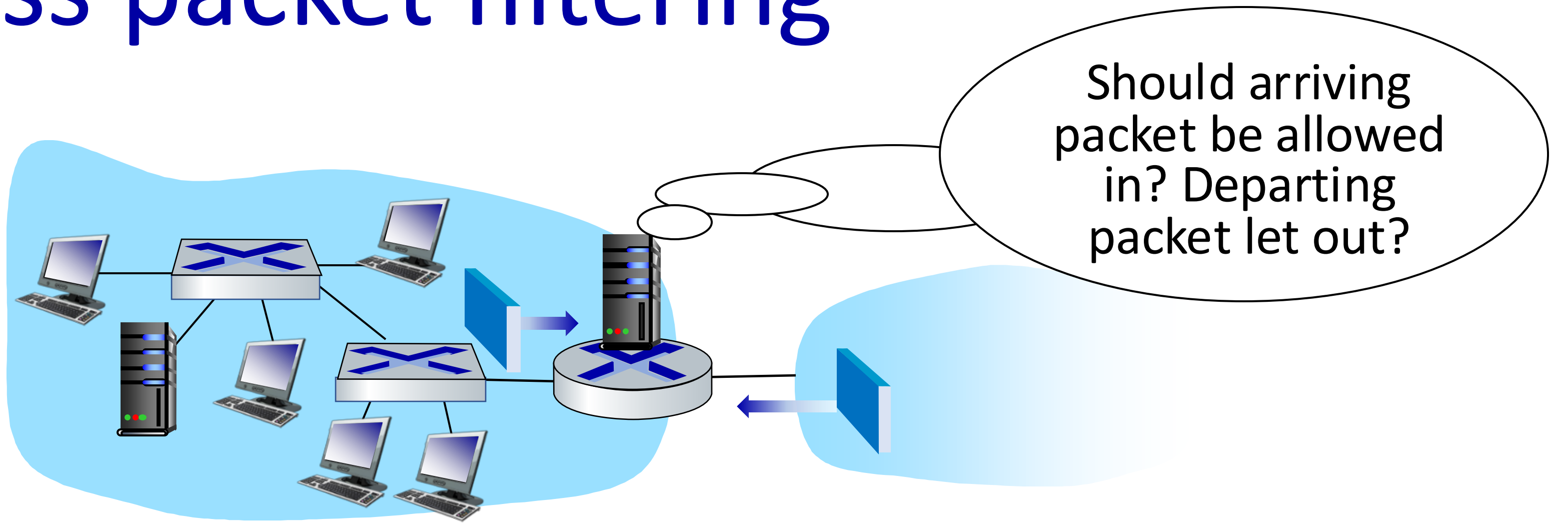
Rules	Action
	Allow
	Block



three types of firewalls:

- stateless packet filters
- stateful packet filters
- application gateways

Stateless packet filtering



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

IP/TCP or UDP

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

Stateless packet filtering: 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 (e.g. 130.207.255.255)
prevent your network from being tracerouted	drop all outgoing ICMP TTL expired traffic

Block UDP Traffic)

Stateless

Access Control Lists

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

Match, Action>

Web Access

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

looks like OpenFlow forwarding!

Connection table

SRC IP	DST IP	SRC POR	DST POR

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

Stateful packet filtering

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

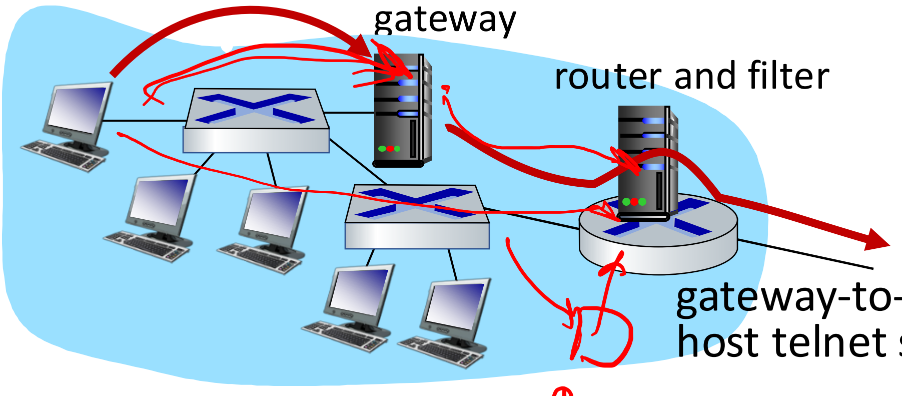
action	source address	dest address	proto	source port	dest port	flag bit	check connection
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	any	X
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	X
deny	all	all	all	all	all	all	

Connection Table

Access to N/w or Appln to some authentication users

Application gateways

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



host-to-gateway telnet session

application gateway

router and filter

gateway-to-remote host telnet session

Proxy for

1. require all users to ssh through gateway.
2. for authorized users, gateway sets up ssh connection to dest host
   - gateway relays data between 2 connections
3. router filter blocks all ssh connections not originating from gateway

Limitations of firewalls, gateways

- IP spoofing: router can't know if data "really" comes from claimed source

Gateway

- if multiple apps 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

Intrusion detection systems

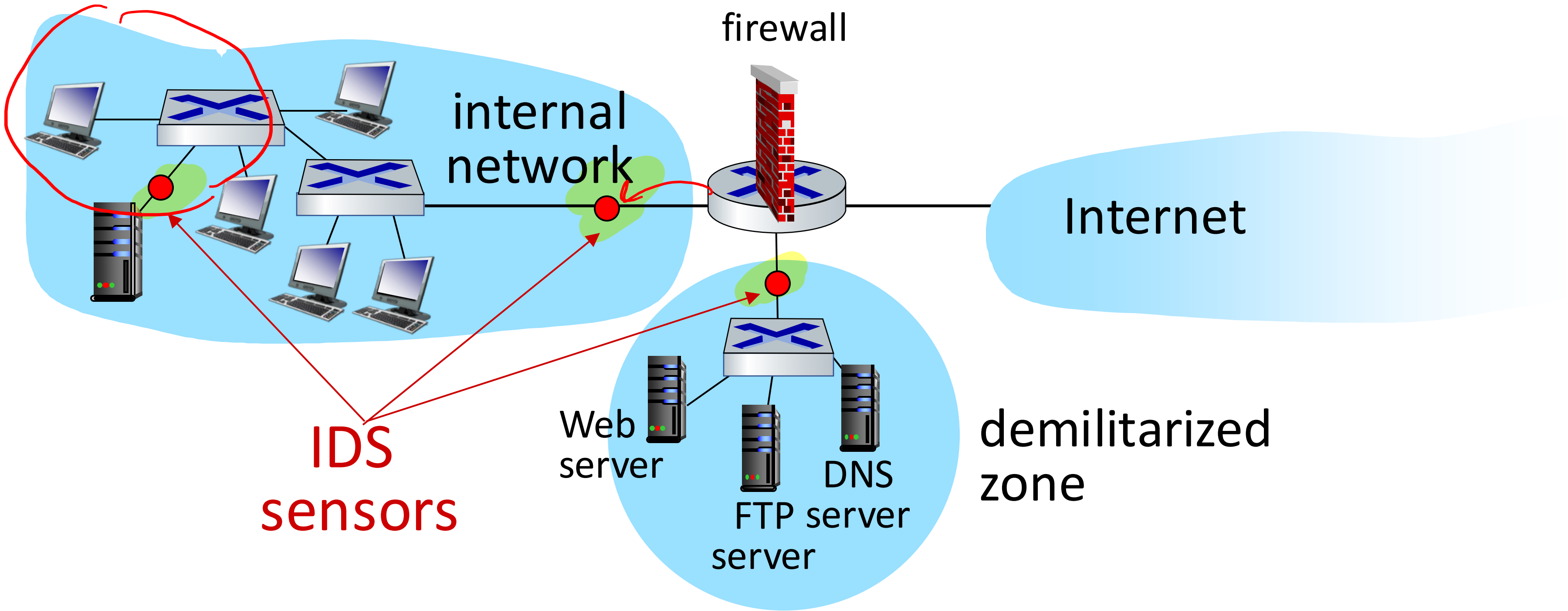
- packet filtering:
  - operates on TCP/IP headers only
  - no correlation check among sessions
- IDS: intrusion detection system
  - deep packet inspection: look at packet contents (e.g., check character strings in packet against database of known virus, attack strings)
  - examine correlation among multiple packets
    - port scanning
    - network mapping
    - DoS attack

SYN flooding

[(Detection logic)] Raise Alarm

Intrusion detection systems

multiple IDSs: different types of checking at different locations



Intrusion Detection System

- Signature-based
  - E.g., detecting “ping sweeps”

```
IDS rule: alert icmp any any -> any any (msg:"Ping Sweep Detected"; itype:8;
threshold:type threshold, track by_src, count 5, seconds 10; sid:1000004;
rev:1;)
```

  - Work well attacks are known
- Anomaly detection-based

Reduce False positive

  - Use Machine learning to model normal behavior of the traffic
  - Tag deviations from normal behavior as malicious

Network Security (summary)

basic techniques……

- cryptography (symmetric and public key)
- message integrity
- end-point authentication

…. used in many different security scenarios

- secure email
- secure transport (TLS)
- IP sec

operational security: firewalls and IDS

Attendance