Computer Networks
COL 334/672

Network Security

Slides adapted from KR

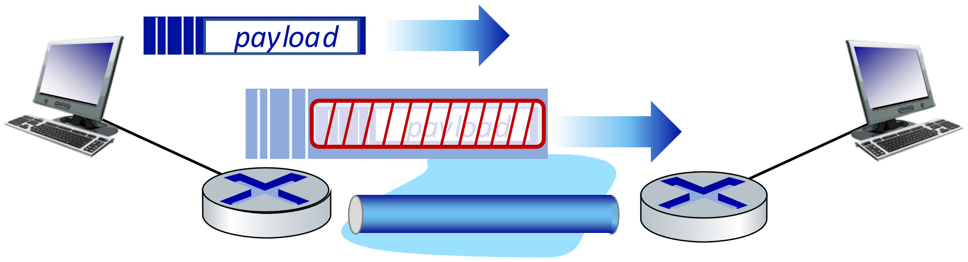
Sem 1, 2025-26

Recap

- Cryptographic techniques
- Securing network protocols
  - Secure Email
  - TLS
- This class
  - IPSec
  - Operational Security: Firewall and IDS

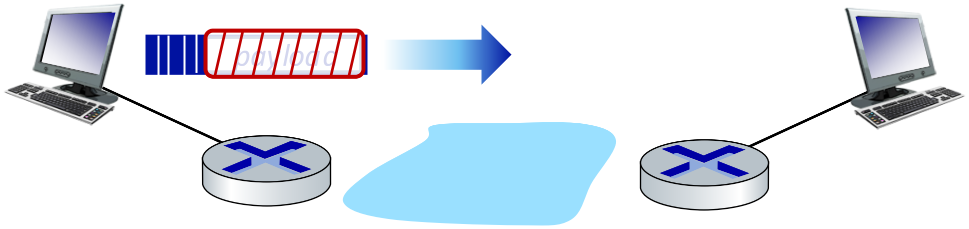
IP Sec

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



tunnel mode:

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



transport mode:

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

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

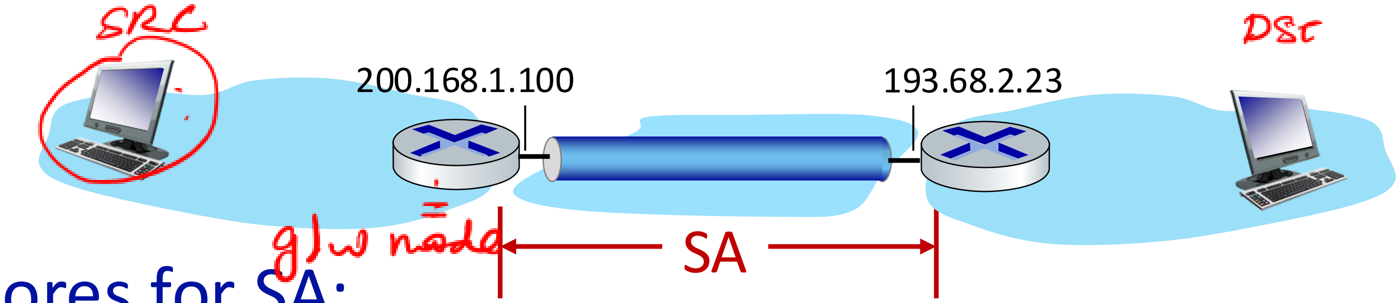
- Phase 1: Exchange security keys (Mutual Authentication)

  IKE

- Phase 2: Secure data communication

Security associations (SAs)

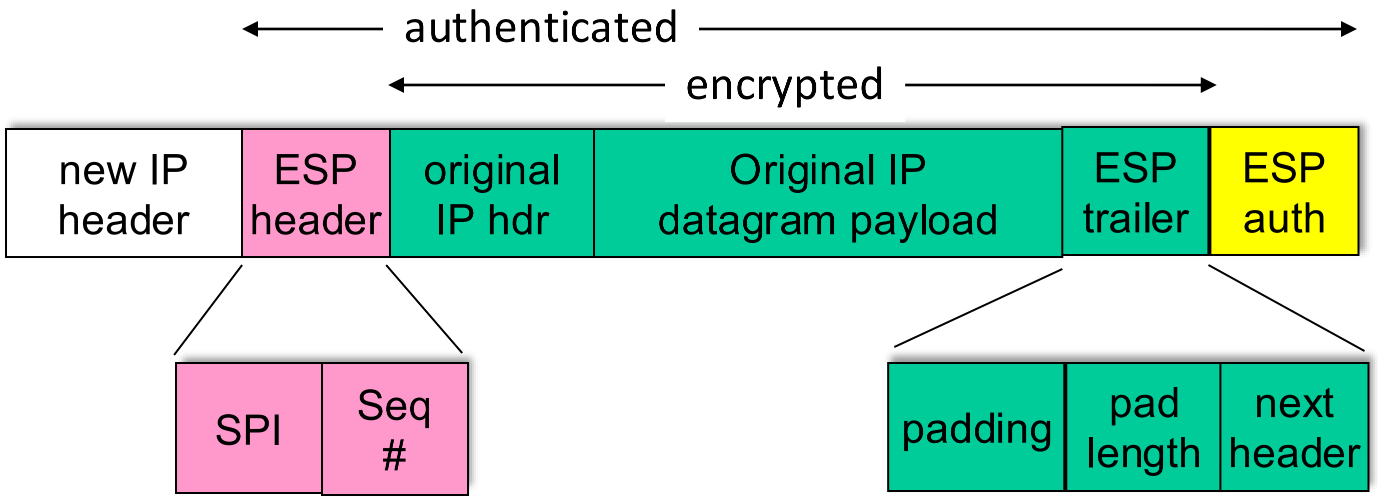
- before sending data, security association (SA) established from sending to receiving entity (directional)
- ending, receiving entities maintain *state information* about SA
  - recall: TCP endpoints also maintain state info
  - IP is connectionless; IPsec is connection-oriented!



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

IPsec datagram: Data transmission

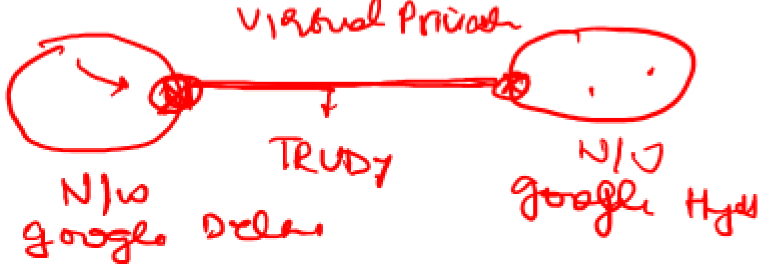


tunnel mode ESP

- 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

OpenVPN works over TLS

implementing VPN



IPsec security databases

All traffic from IP$_1$ to IP$_2$, use IPSec

Mechanism: IPSec

Security Policy Database (SPD)

- policy: for given datagram, sender needs to know if it should use IP sec
- policy stored in security policy database (SPD)
- needs to know which SA to use
  - may use: source and destination IP address; protocol number

SAD: "how" to do it

Security Assoc. Database (SAD)

- endpoint holds SA state in security association database (SAD)
- when sending IPsec datagram, R1 accesses SAD to determine how to process datagram
- when IPsec datagram arrives to R2, R2 examines SPI in IPsec datagram, indexes SAD with SPI, processing
- datagram accordingly.

SPD: "what" to do

Summary: IPsec services

Trudy sits somewhere between R1, R2. she doesn't know the keys

- will Trudy be able to see original contents of datagram? How about source, dest IP address, transport protocol, application port?
- flip bits without detection?
- masquerade as R1 using R1's IP address? (IKE)
- replay a datagram?

Recap

- Cryptographic techniques
- Securing network protocols
  - Secure Email
  - TLS
  - IPSec
- **Operational Security: Firewall and IDS**

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 → software could have faults

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

allow only authorized access to inside network

- set of authenticated users/hosts

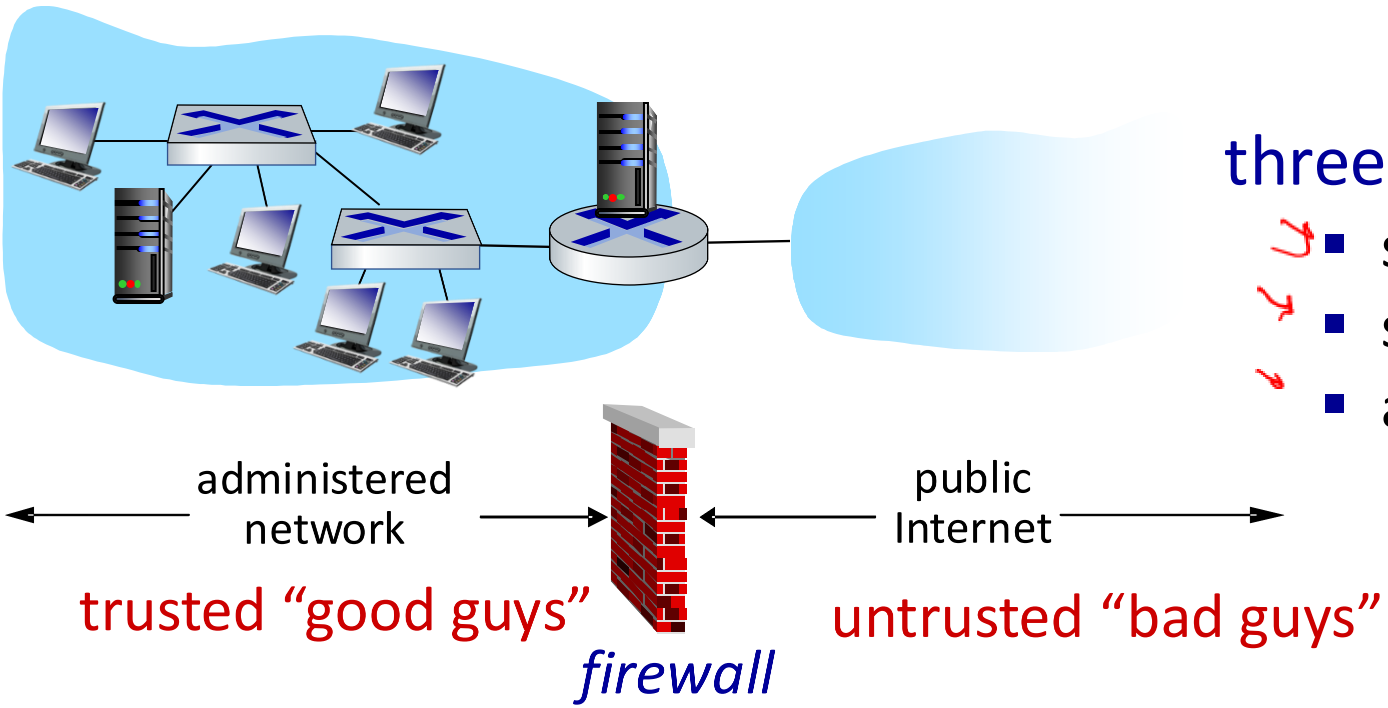
① Firewall

②. Intrusion detection System (IDS)

Firewalls

firewall

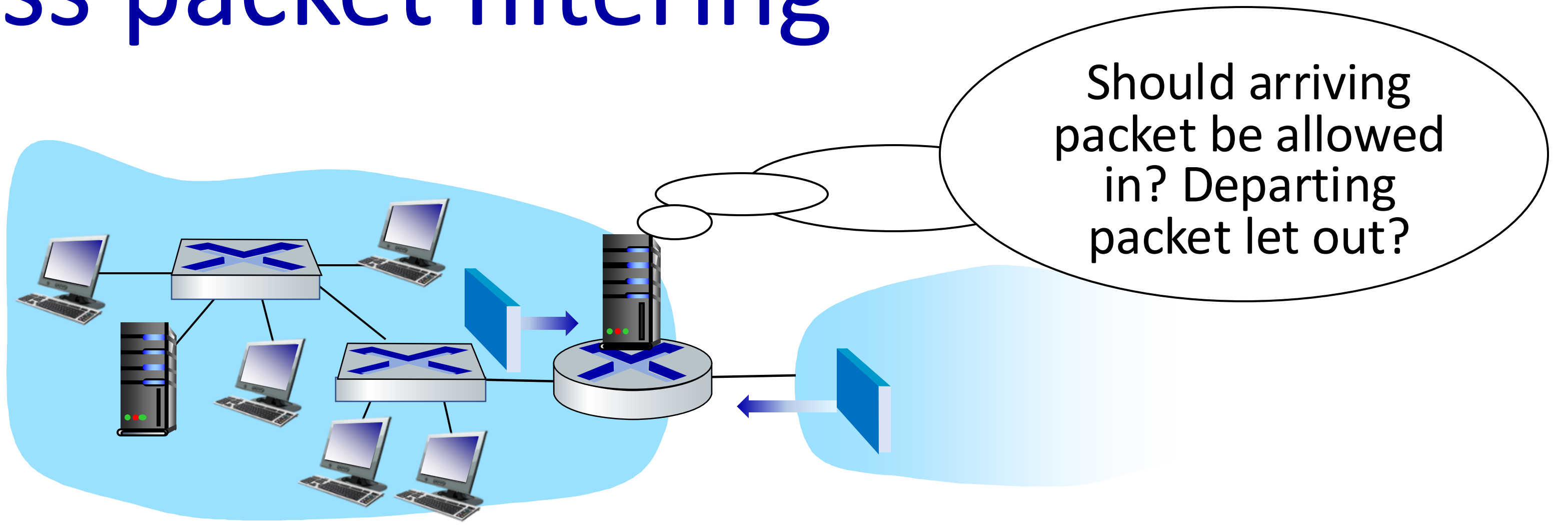
isolates organization’s internal network from larger Internet, allowing some packets to pass, blocking others



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?

- internal network connected to Internet via router firewall

IP | Transport layer header

- 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

Policy	Firewall Setting
no outside Web access	drop all outgoing packets to any IP address, port 80

drop all outgoing

" - " , port 443

Typically Implemented as Access Control Lists

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

flow

my n/w

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!

Stateful packet filtering

SRC IP
Dst IP
80
2456
← IPx

- *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 IPx	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

CONN TABLE

SRC IP	DST IP	SRC PORT	DST PORT

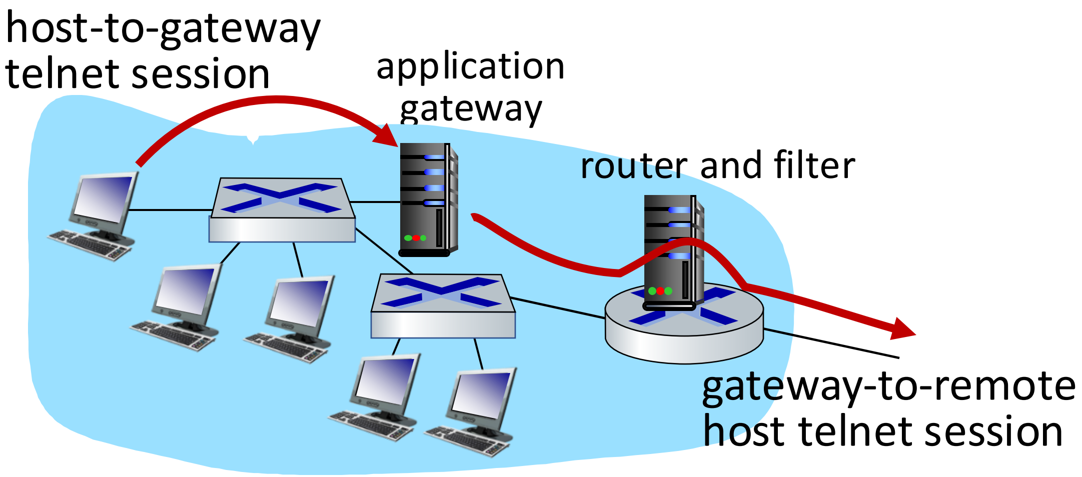
ACL augmented to indicate need to check connection state table before admitting packet

Keep tracks of Seq #s

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	

Application gateways

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



Non Transparent SSH g/w

Transparent g/w

Non-transparent SSH

R

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

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

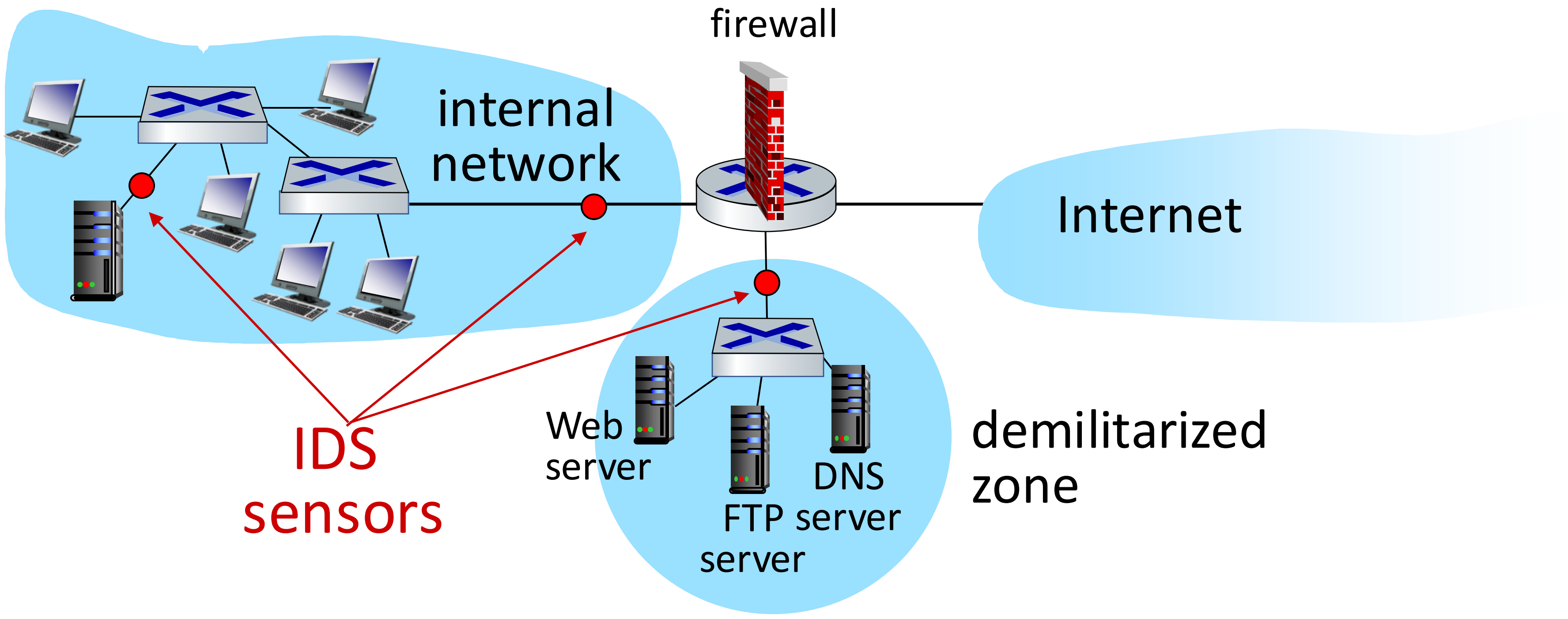
Quiz: Bringing it all together

Throughout this course, you have explored various network protocols. Many system design principles, however, repeat across protocols. Listed below are five such principles. For each principle, provide two examples of network protocols that utilize it.

- **P1**: Modularity for managing a complex system
- **P2**: Hierarchy for managing scale
- **P3**: Soft state to reduce the complexity of managing state across multiple systems
- **P4**: Redundancy for reliability
- **P5**: Indirection, i.e., decouples a name from its actual realization to enable flexibility, scalability

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 when attacks are known
- Anomaly detection-based
  - Use Machine learning to model normal behavior of the traffic
  - Tag deviations from normal behavior as malicious