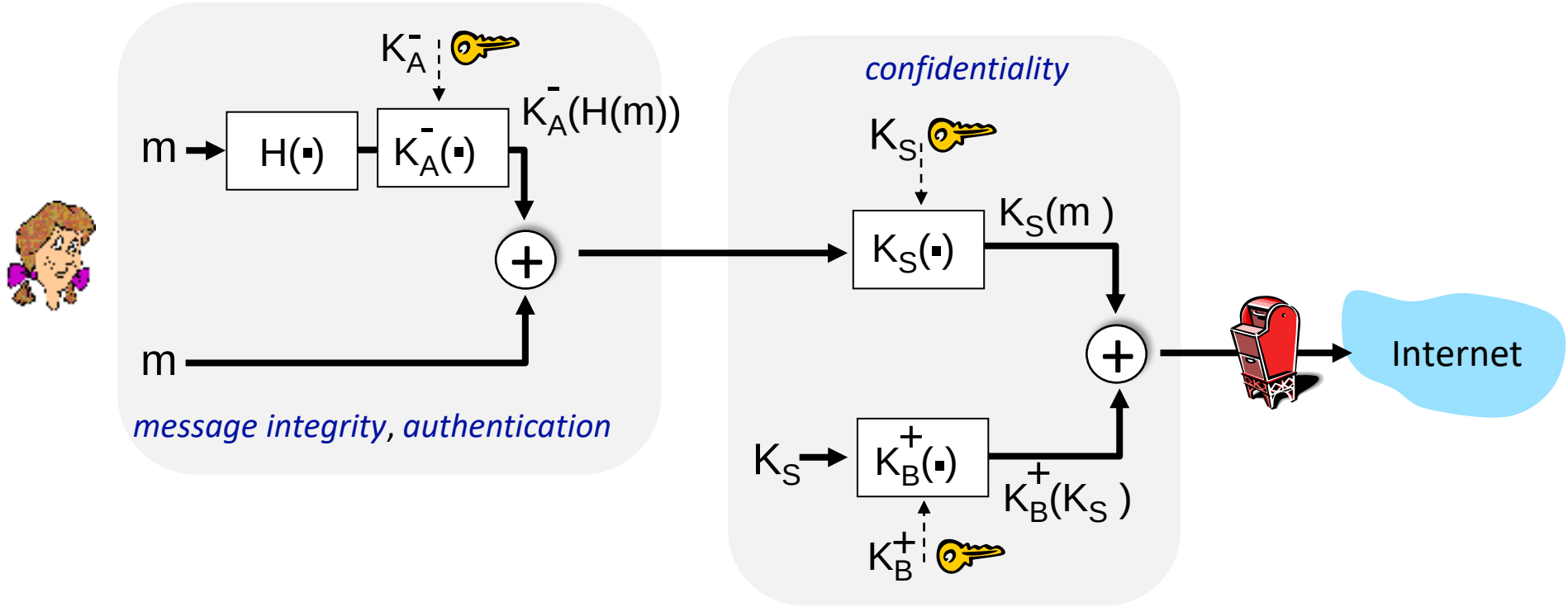
Secure e-mail: integrity, authentication

Alice sends m to Bob, with *confidentiality, message integrity*, *authentication*



Alice uses three keys: her private key, Bob's public key, new symmetric key

What are Bob's complementary actions?

outline

- What is network security?
- Principles of cryptography
- Authentication, message integrity
- Securing e-mail
- **Securing TCP connections: TLS**
- Network layer security: IPsec
- Operational security: firewalls and IDS

Transport-layer security (TLS)

- Two protocols are dominant today for providing security at the transport layer: the Secure Sockets Layer (SSL) protocol and the Transport Layer Security (TLS) protocol.

- The latter is actually an IETF version of the former. We discuss SSL in this section; TLS is very similar.

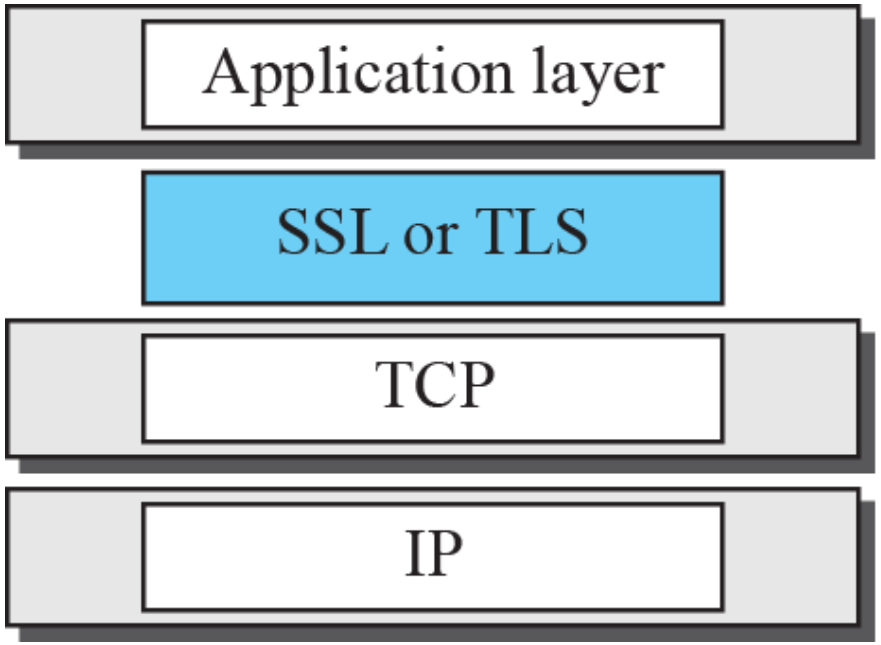
Transport-layer security (TLS)

- widely deployed security protocol above the transport layer
  - supported by almost all browsers, web servers: https (port 443)

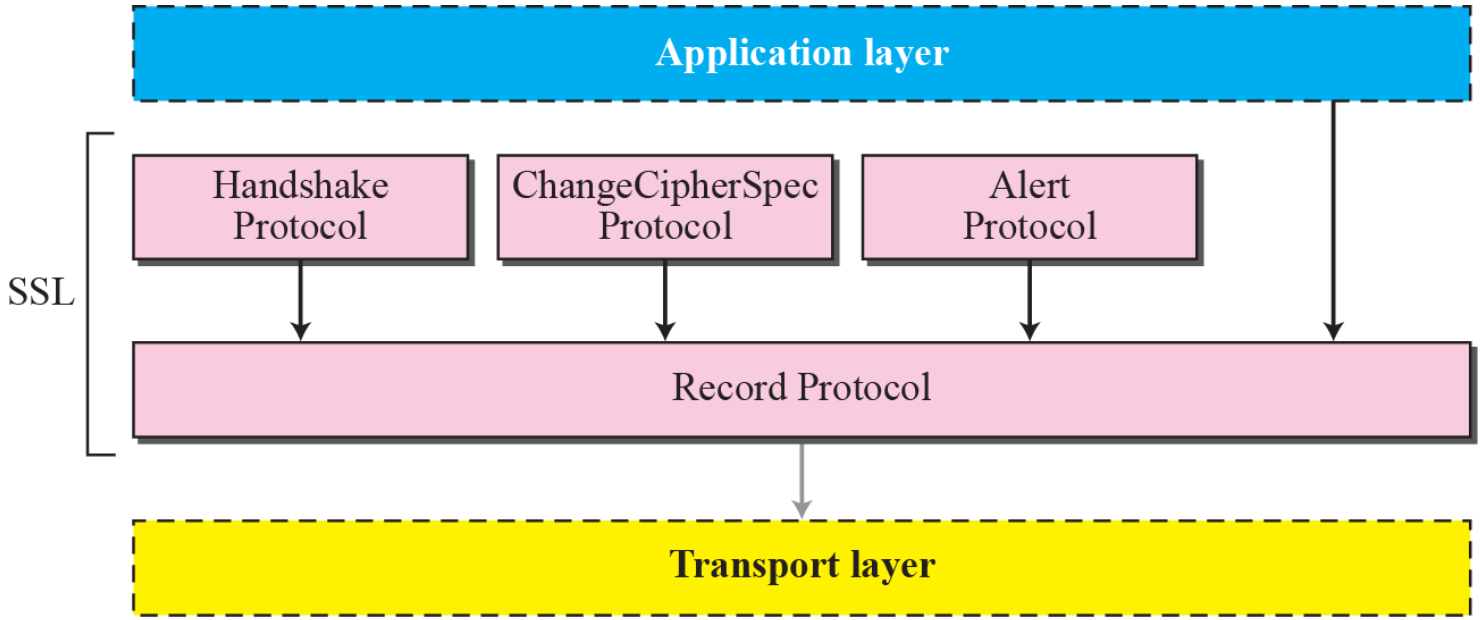
- provides:
  - confidentiality: via *symmetric encryption*
  - integrity: via *cryptographic hashing*
  - authentication: via *public key cryptography*

} *all techniques we have studied!*

Location of SSL and TSL in the Internet mode

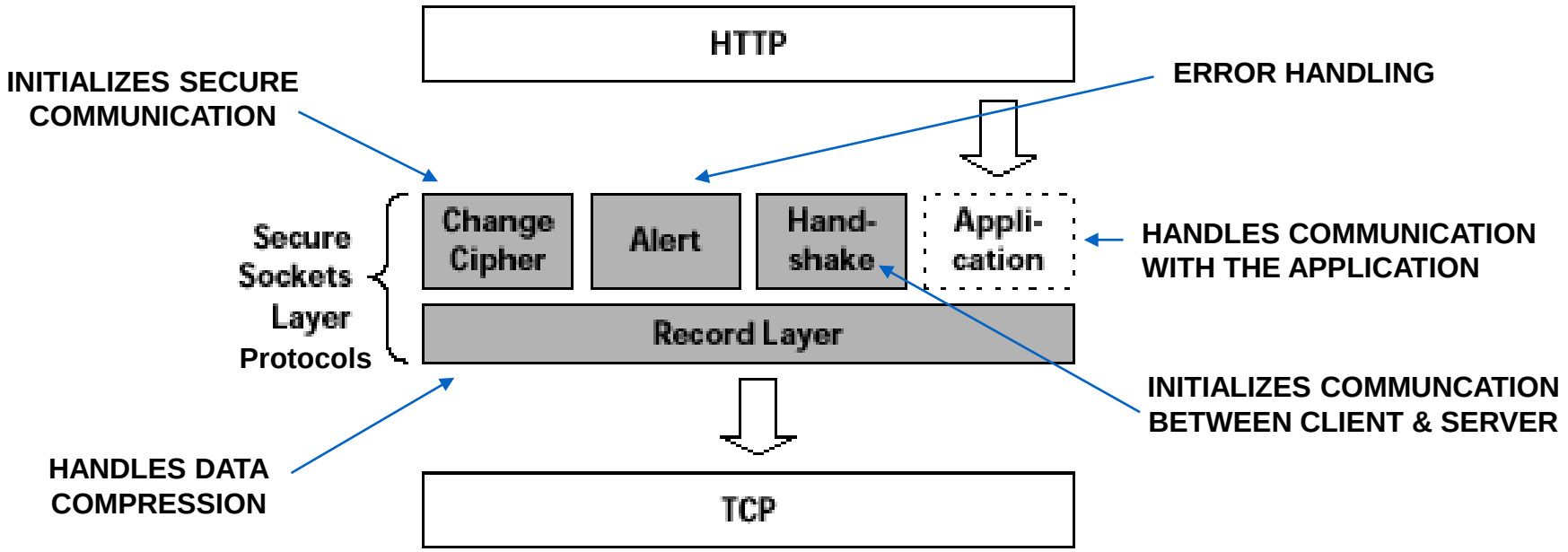


Four SSL protocols



- The **SSL Handshake Protocol (Authentication)** uses the **SSL** Record **Protocol** to exchange a series of messages between an **SSL**-enabled server and an **SSL**-enabled client when they first establish an **SSL** connection.
- SSL Record protocol provides Confidentiality and Integrity.
- **Change cipher spec protocol** is used to change the encryption being used by the client and server.
- Alert Protocol is used to inform the other end, of any irregularity or failure in authentication.

Cont..


HTTP
INITIALIZES SECURE COMMUNICATION
ERROR HANDLING
Change Cipher
Alert
Hand-shake
Appli-cation
HANDLES COMMUNICATION WITH THE APPLICATION
Secure Sockets Layer Protocols
Record Layer
INITIALIZES COMMUNCATION BETWEEN CLIENT & SERVER
HANDLES DATA COMPRESSION
TCP

Handshake protocol

Note

After Phase I, the client and server know the version of SSL, the cryptographic algorithms, the compression method, and the two random numbers for key generation.

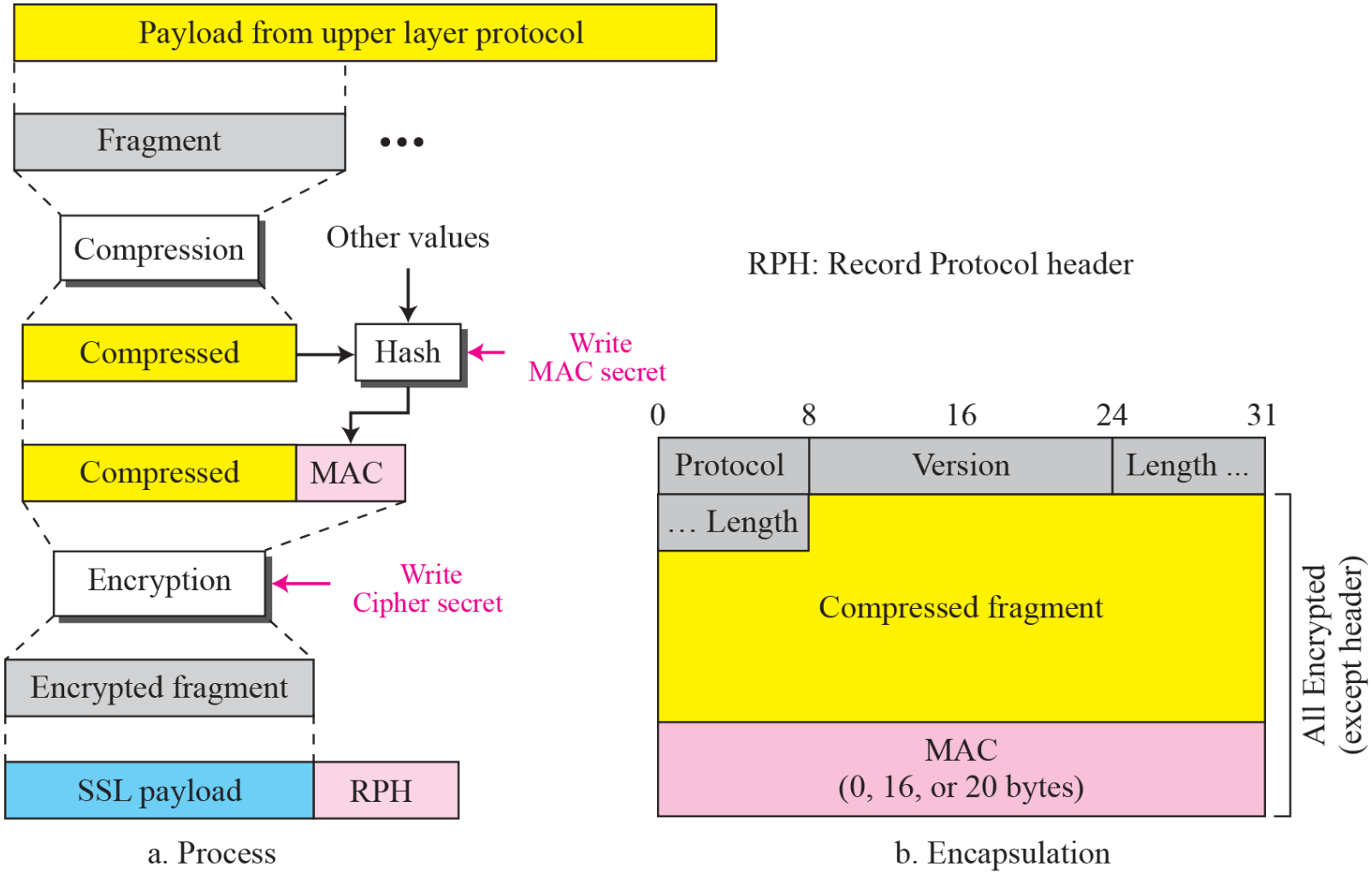
Note

After Phase II, the server is authenticated to the client, and the client knows the public key of the server if required.

Note

After Phase III, The client is authenticated for the serve, and both the client and the server know the pre-master secret.

Processing done by the record protocol

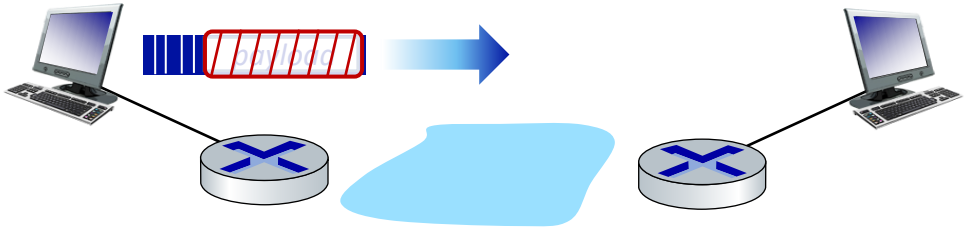


outline

- What is network security?
- Principles of cryptography
- Authentication, message integrity
- Securing e-mail
- Securing TCP connections: TLS
- **Network layer security: IPsec**
- Operational security: firewalls and IDS

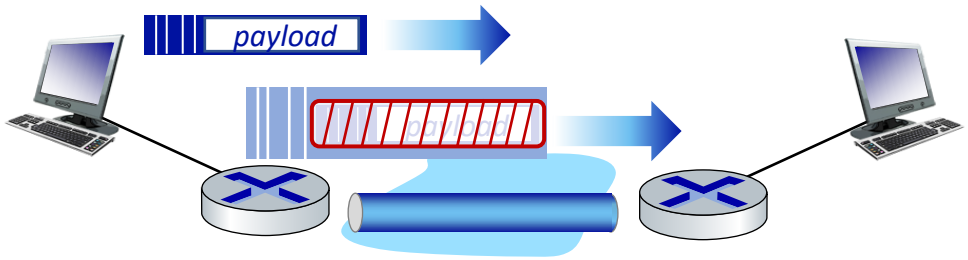
IP Sec

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



transport mode:

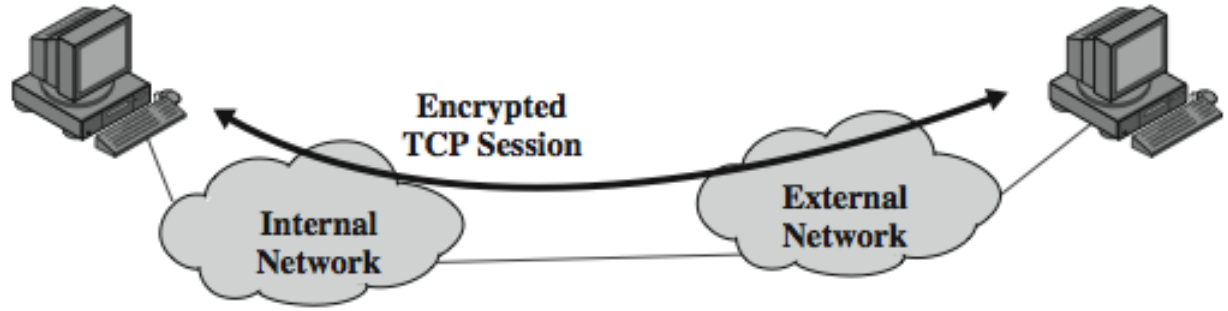
- *only* datagram *payload* is encrypted, authenticated



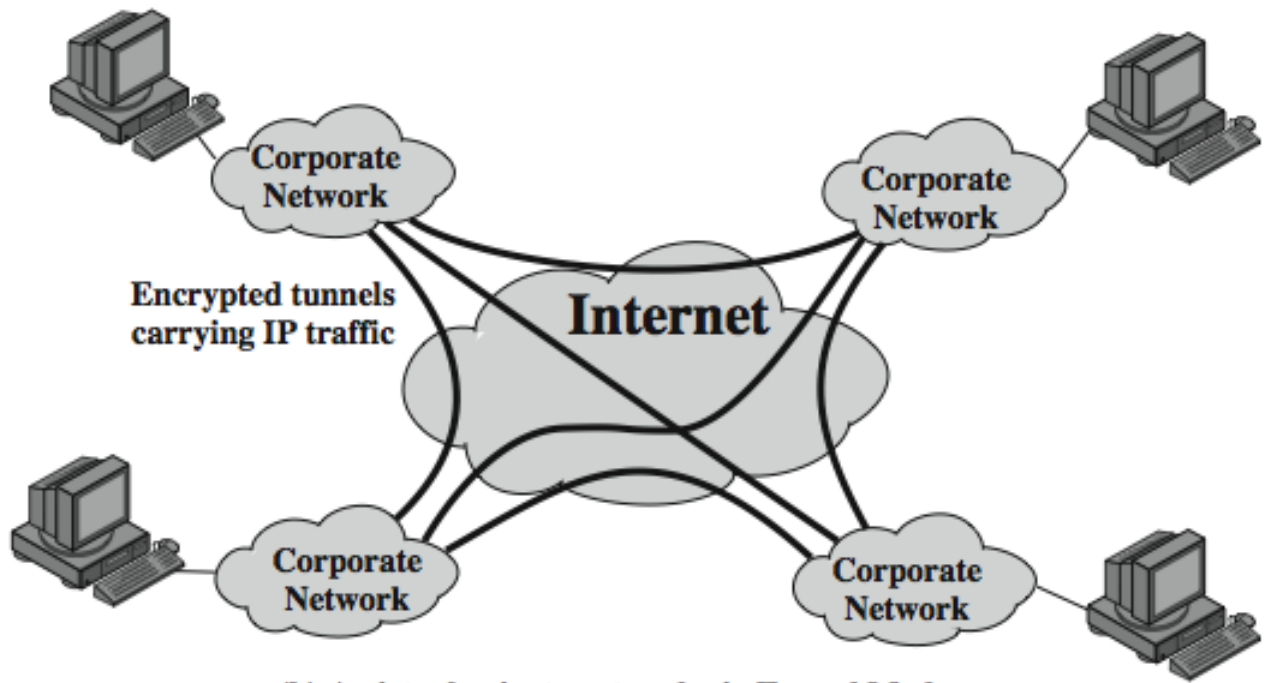
tunnel mode:

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

Transport and Tunnel Modes

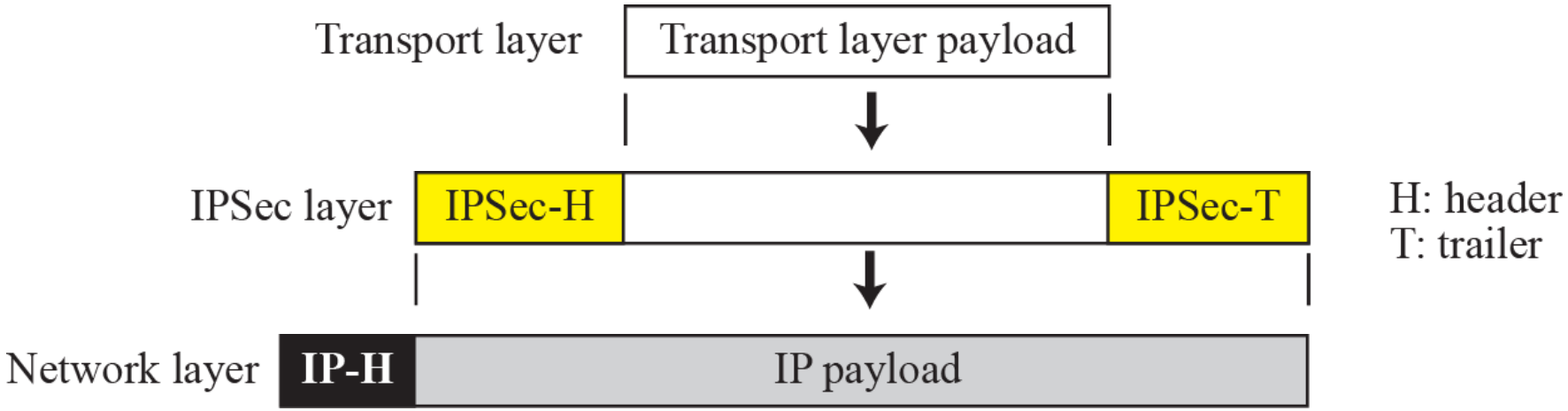


(a) Transport-level security

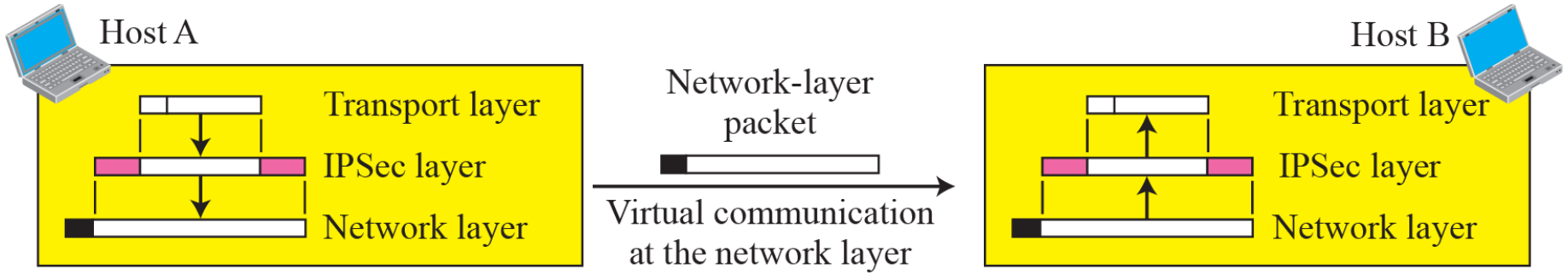


(b) A virtual private network via Tunnel Mode

IPSec in transport mode



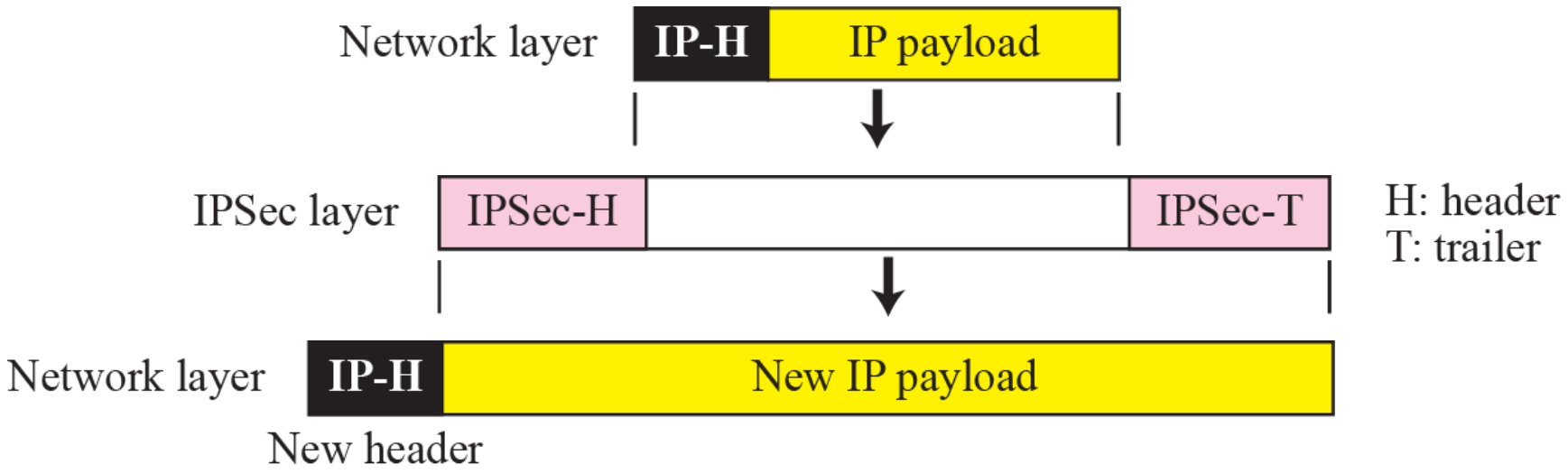
Transport mode in Action



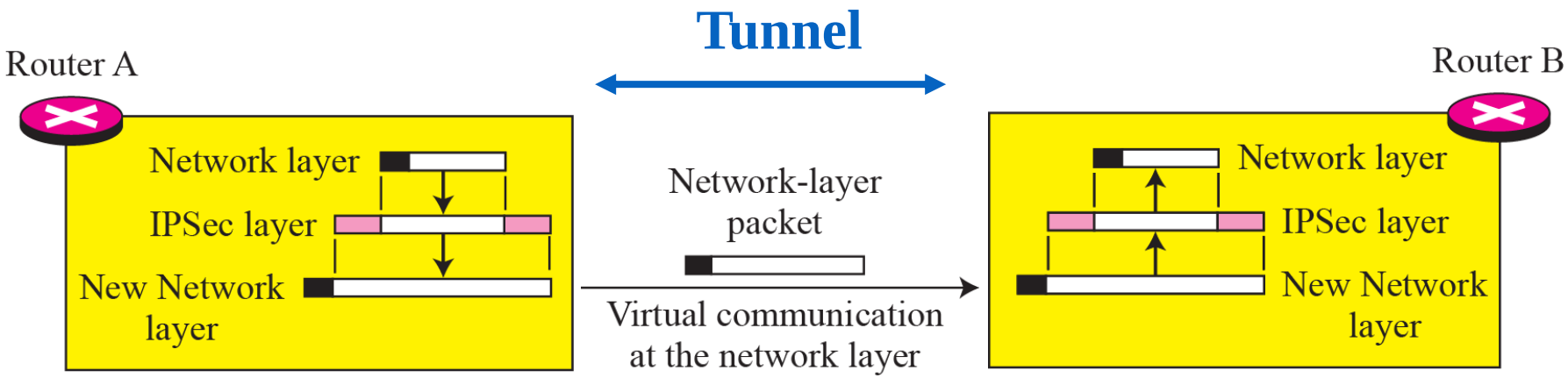
Note

IPSec in transport mode does not protect the IP header; it only protects the information coming from the transport layer.

IPSec in tunnel mode



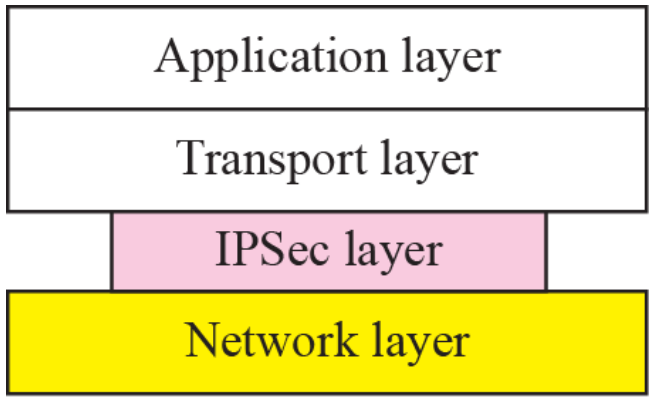
Tunnel-mode in action



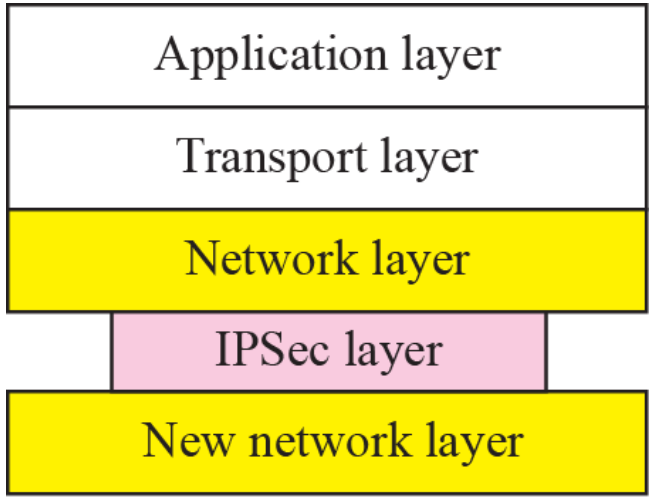
Note

IPSec in tunnel mode protects the original IP header.

Transport mode versus tunnel mode



Transport Mode

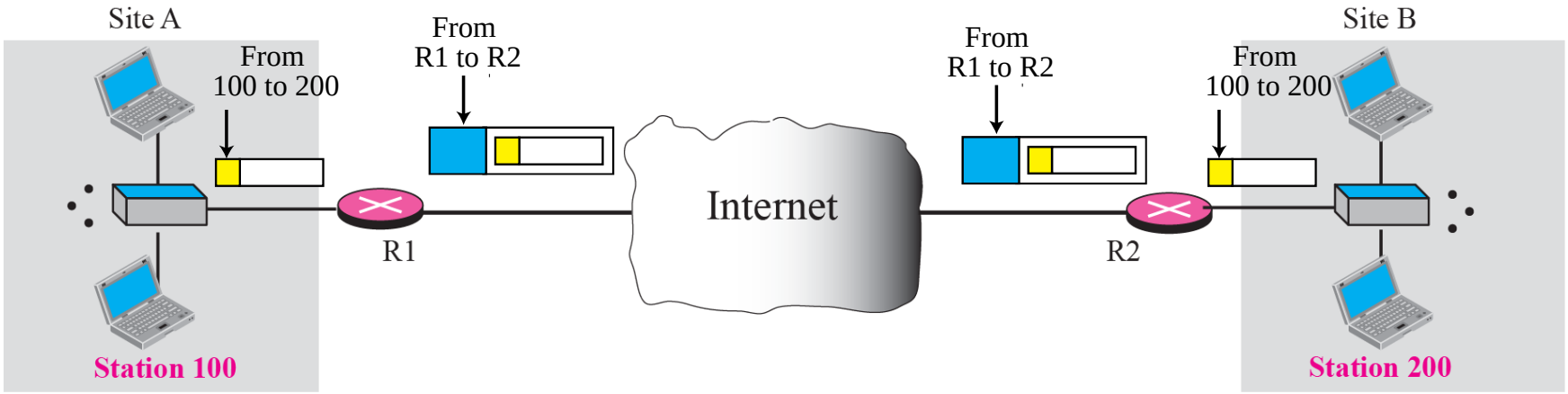


Tunnel Mode

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

Virtual private network



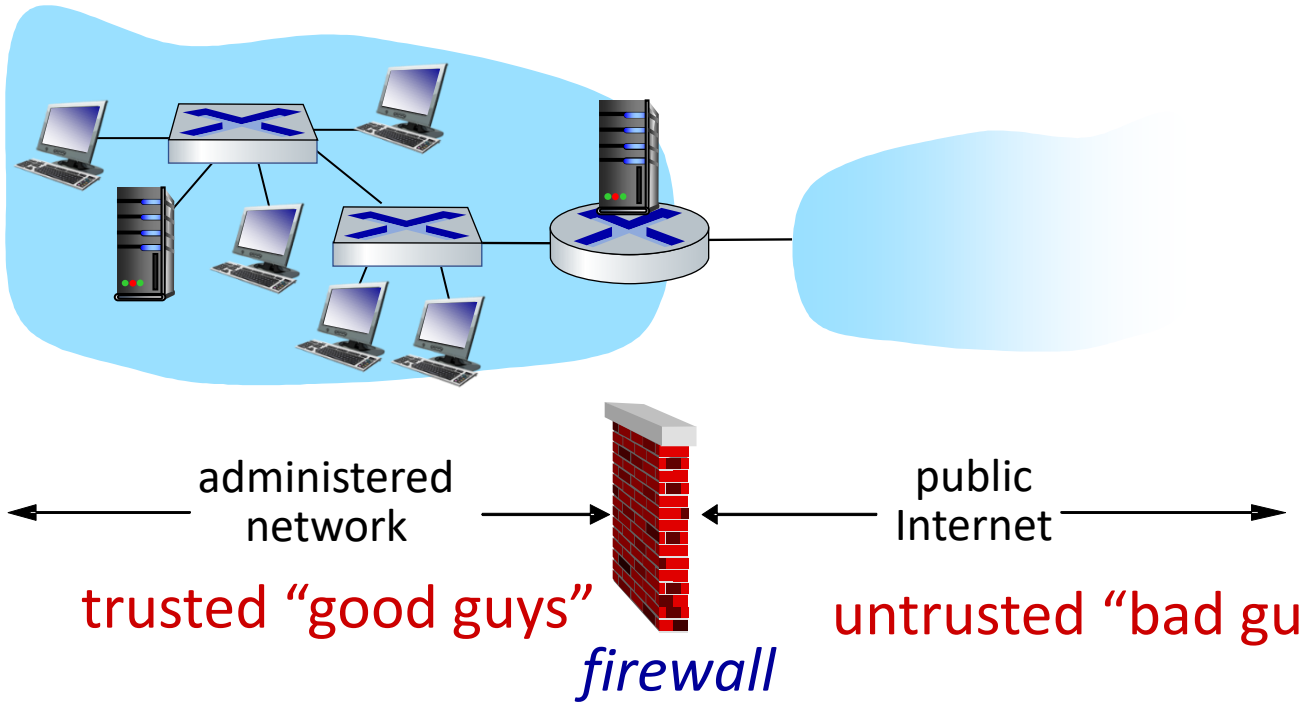
outline

- What is network security?
- Principles of cryptography
- Authentication, message integrity
- Securing e-mail
- Securing TCP connections: TLS
- Network layer security: IPsec
- Security in wireless and mobile networks
- Operational security: firewalls and IDS

Firewalls

firewall

isolates organization's internal network 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

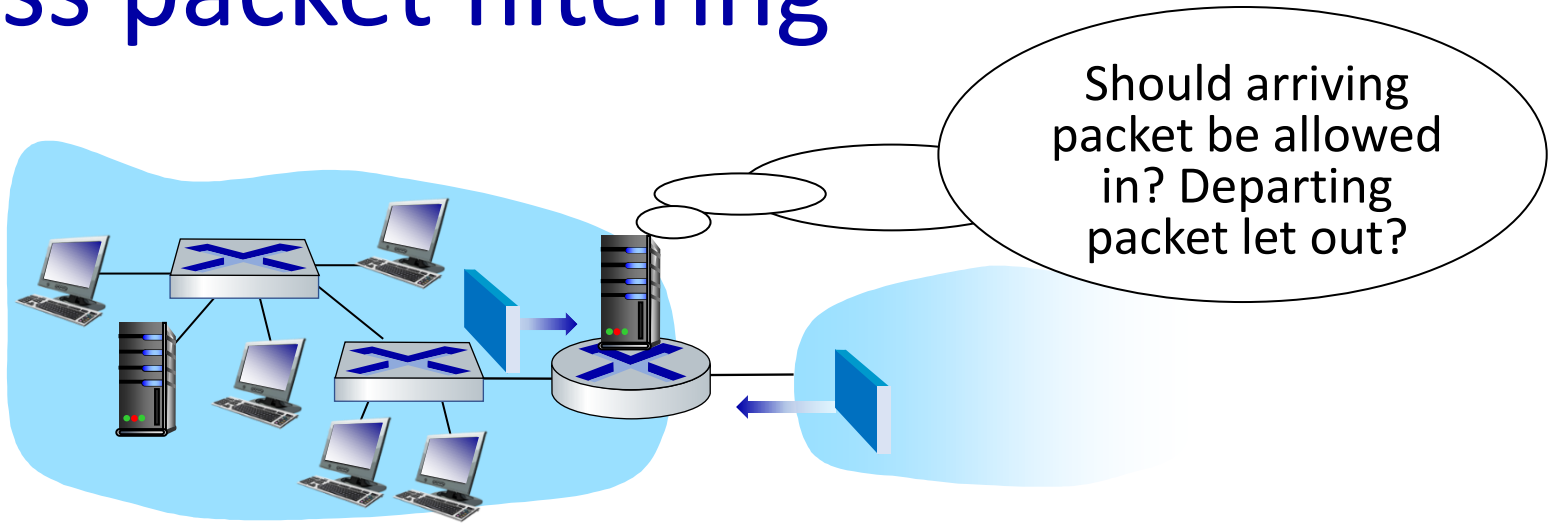
allow only authorized access to inside network

- set of authenticated users/hosts

three types of firewalls:

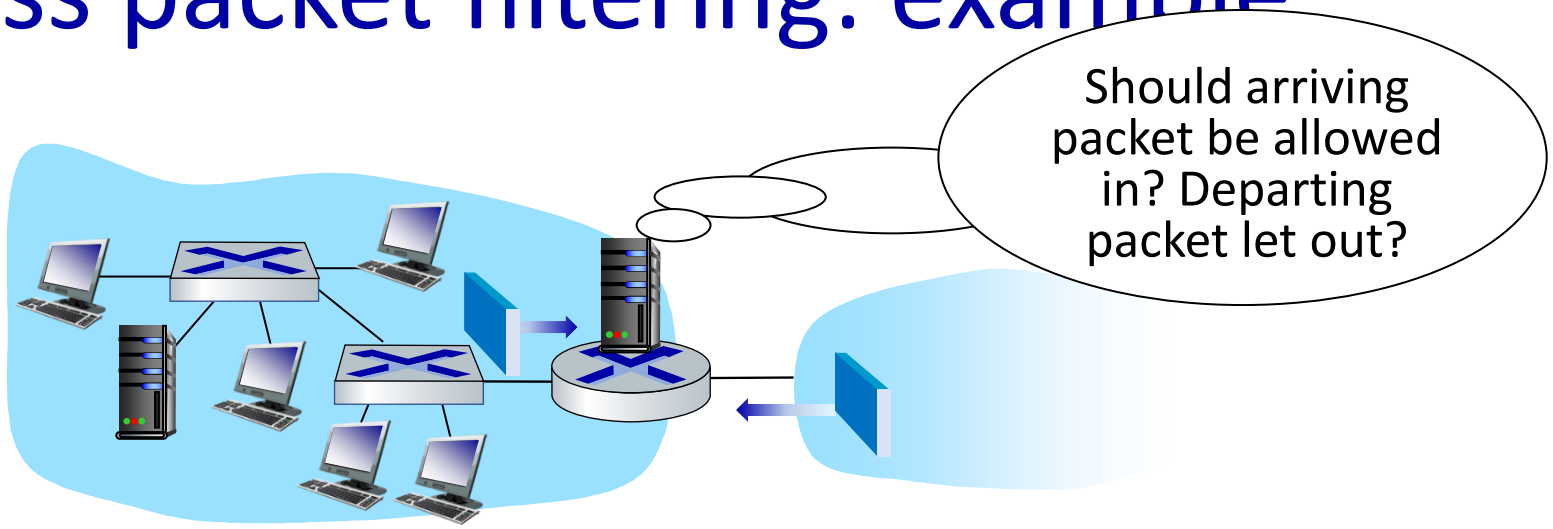
- stateless packet filters
- stateful packet filters
- application gateways

Stateless packet filtering



- internal network connected to Internet via router firewall
- 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: 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

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

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

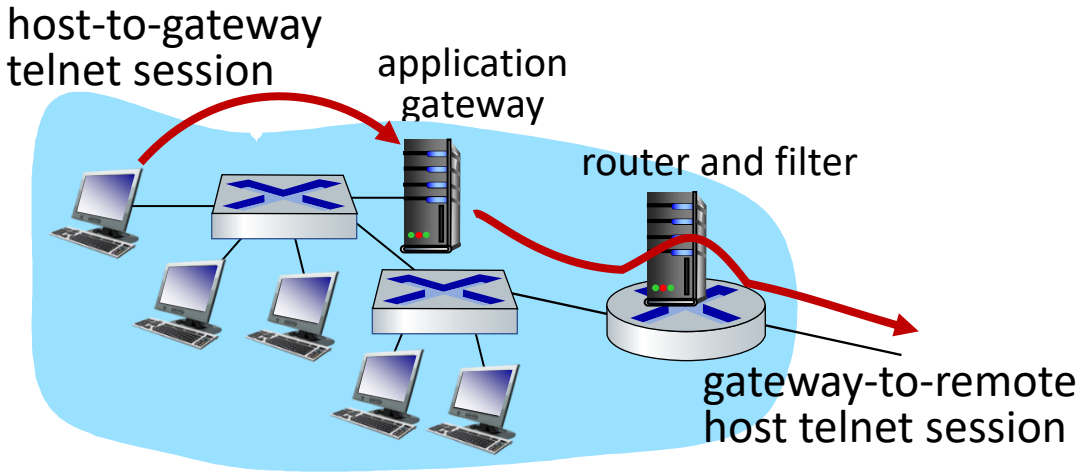
- *stateless packet filter:*
  - admits packets that "make no sense," e.g., dest port = 80, ACK bit set, even though no TCP connection established:

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

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

Intrusion Detection Systems

- Intrusion detection: is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible intrusions (incidents).
- An Intrusion Detection System (IDS): is a network security system designed to identify intrusive or malicious behaviour via monitoring of network activity.
- The IDS identifies suspicious patterns that may indicate an attempt to attack, break in to, or otherwise compromise a system.

IDS vs Firewalls. Firewalls specify policies about what traffic may or may not enter a particular computer network.

An IDS monitors patterns of traffic and signals an alert once it seems that an attack has taken place.

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 Prevention systems

- Intrusion prevention system (IPS): is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.
- IPS evolved from IDS
- Need to stop attacks in real-time
- IDS is cheaper.
- Several Open-Source IDS/IPS
  - Software based
- IPS = EXPENSIVE
  - Hardware based (Application Specific Integrated Circuits (ASIC) & Field-Programmable Gate Array (FPGA))

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