Firewalls

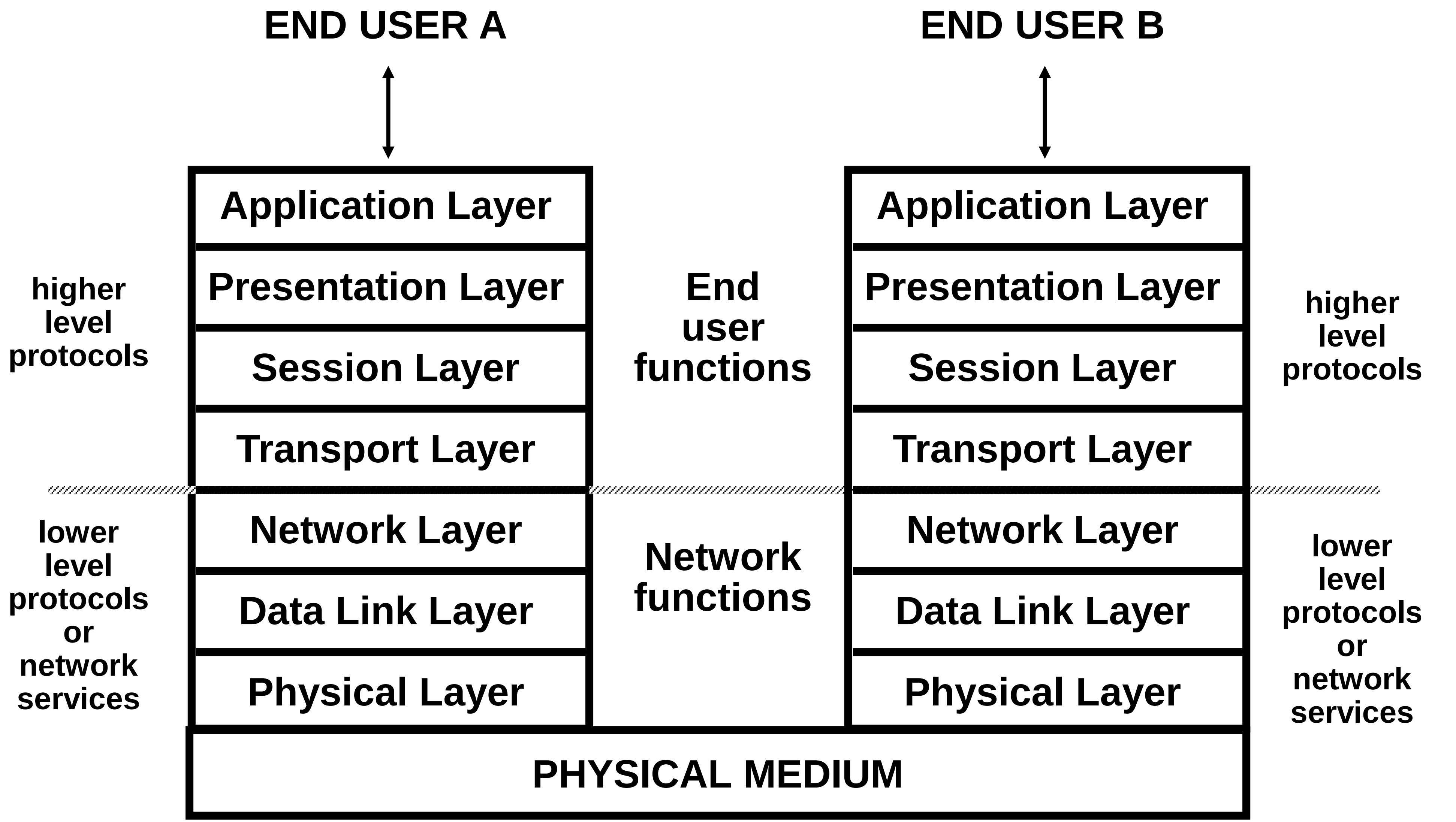
Prof. Ravi Sandhu
Executive Director and Endowed Chair

Lecture 16

ravi.utsa@gmail.com
www.profsandhu.com

TCP/IP Basics

OSI Reference Model



END USER A

END USER B

END USER A		END USER B
Application Layer		Application Layer
Presentation Layer		Presentation Layer
Session Layer		Session Layer
Transport Layer		Transport Layer
Network Layer		Network Layer
Data Link Layer		Data Link Layer
Physical Layer		Physical Layer

PHYSICAL MEDIUM

higher level protocols

End user functions

higher level protocols

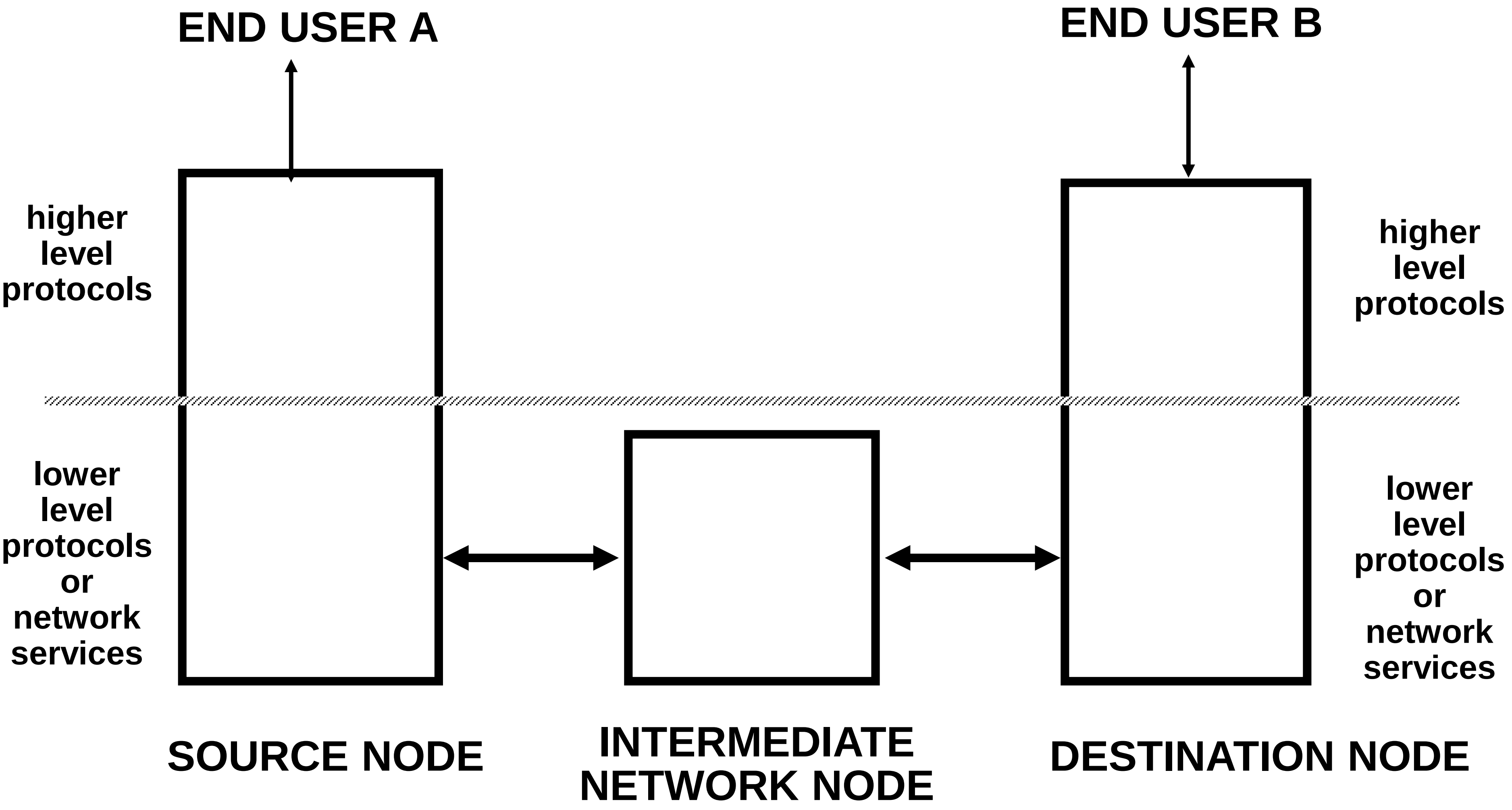
lower level protocols or network services

Network functions

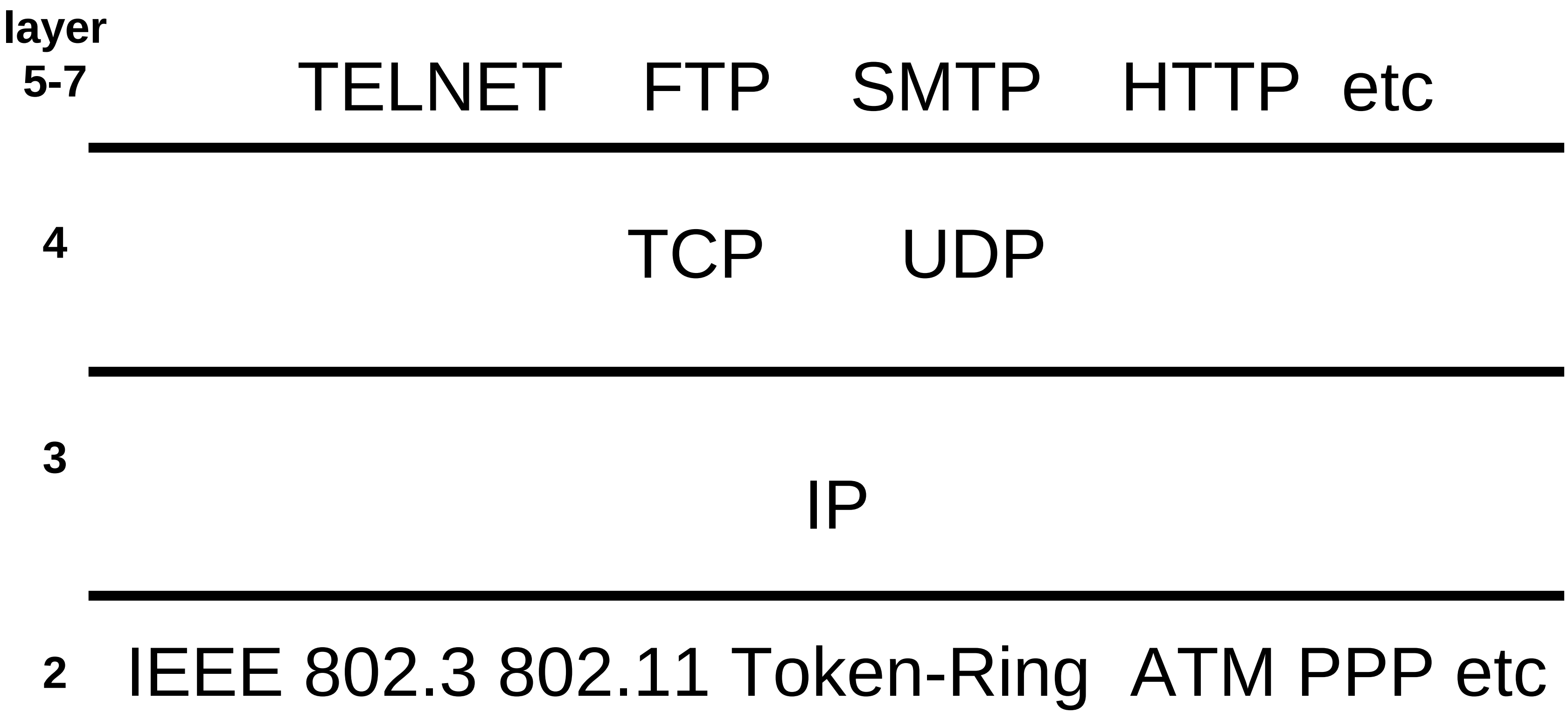
lower level protocols or network services

World-Leading Research with Real-World Impact!

OSI Reference Model


END USER A
END USER B
higher level protocols
higher level protocols
lower level protocols or network services
lower level protocols or network services
SOURCE NODE
INTERMEDIATE NETWORK NODE
DESTINATION NODE

TCP/IP Protocol Stack: Basic Protocols



layer 5-7 TELNET FTP SMTP HTTP etc

4 TCP UDP

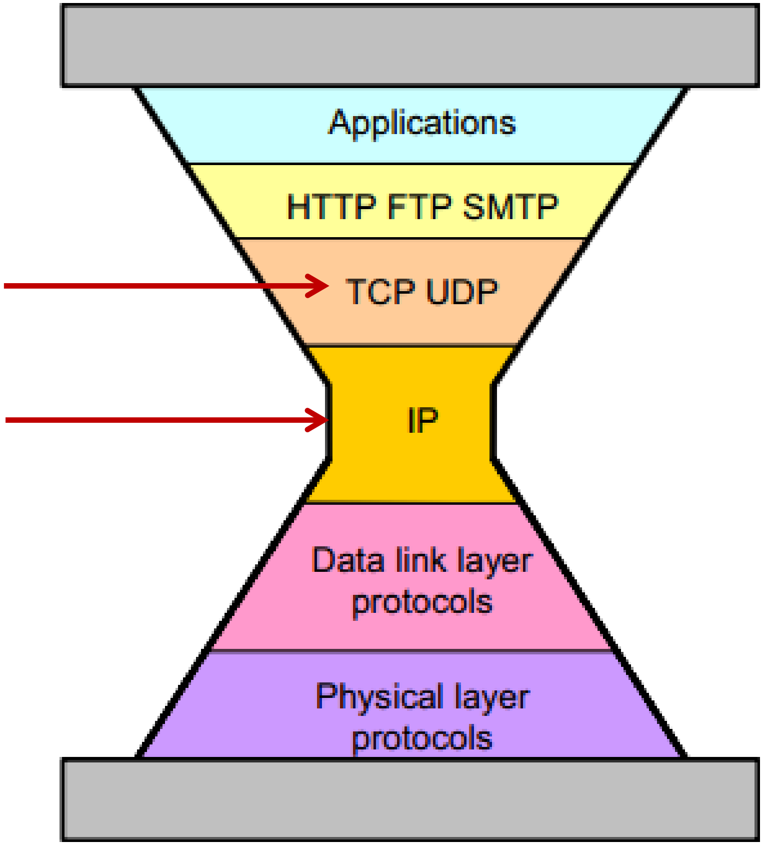
3 IP

2 IEEE 802.3 802.11 Token-Ring ATM PPP etc

TCP/IP Protocol Stack: Basic Protocols

- IP (Internet Protocol)
  - connectionless routing of packets
- UDP (User Datagram Protocol)
  - unreliable datagram protocol
- TCP (Transmission Control Protocol)
  - connection-oriented, reliable, transport protocol
- Application layer protocols
  - TELNET (network virtual terminal)
  - FTP (File Transfer Protocol)
  - SMTP (Simple Mail Transfer Protocol)
  - HTTP (Hyper Text Transfer Protocol)
  - ……

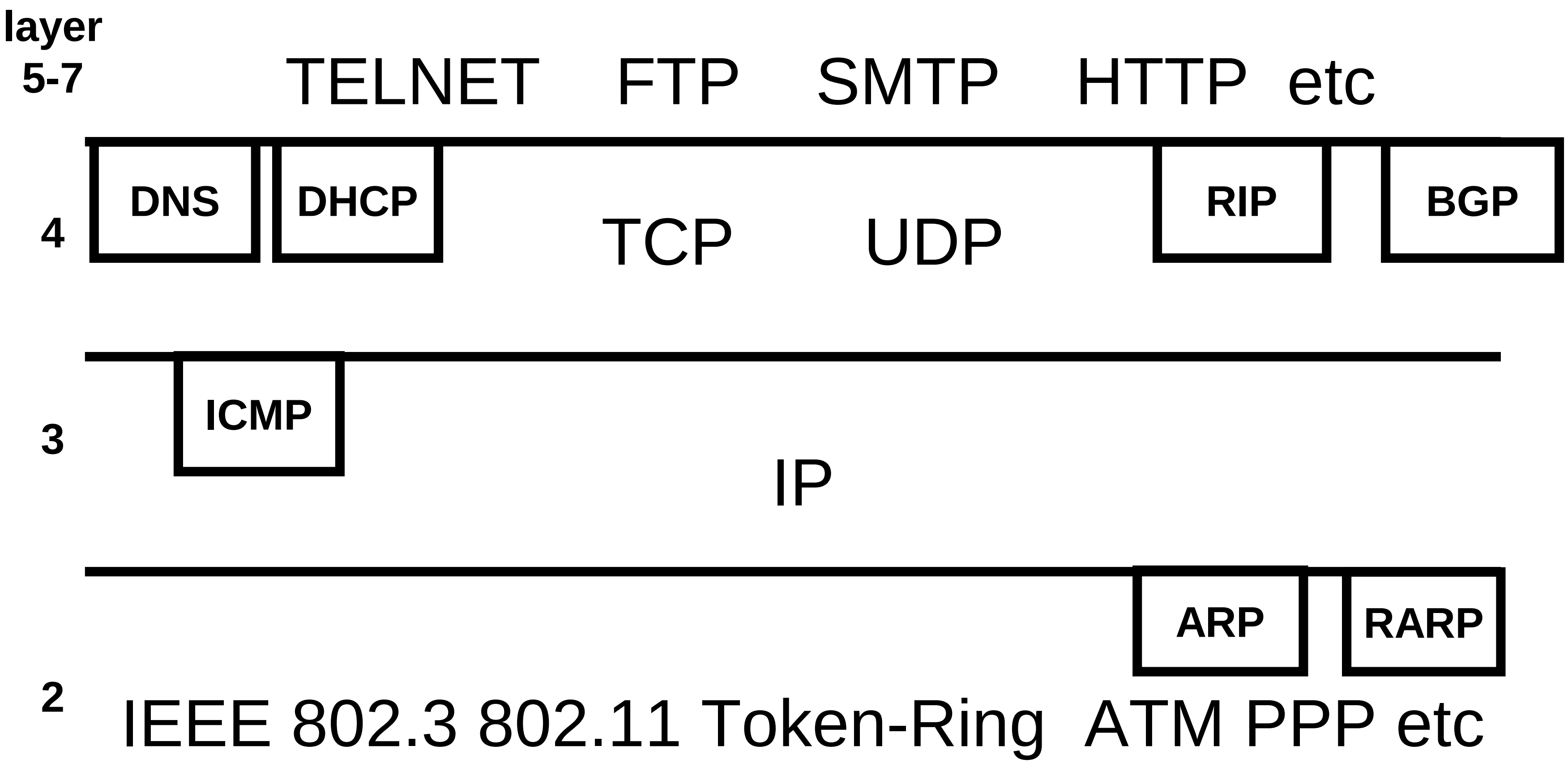
Internet Hourglass Model TCP/IP



TCP RFC 793
Sept. 1981

IPv4 RFC 791
Sept. 1981

TCP/IP Protocol Stack: Infrastructure Protocols



layer 5-7

TELNET FTP SMTP HTTP etc

4

DNS DHCP TCP UDP RIP BGP

3

ICMP IP

2

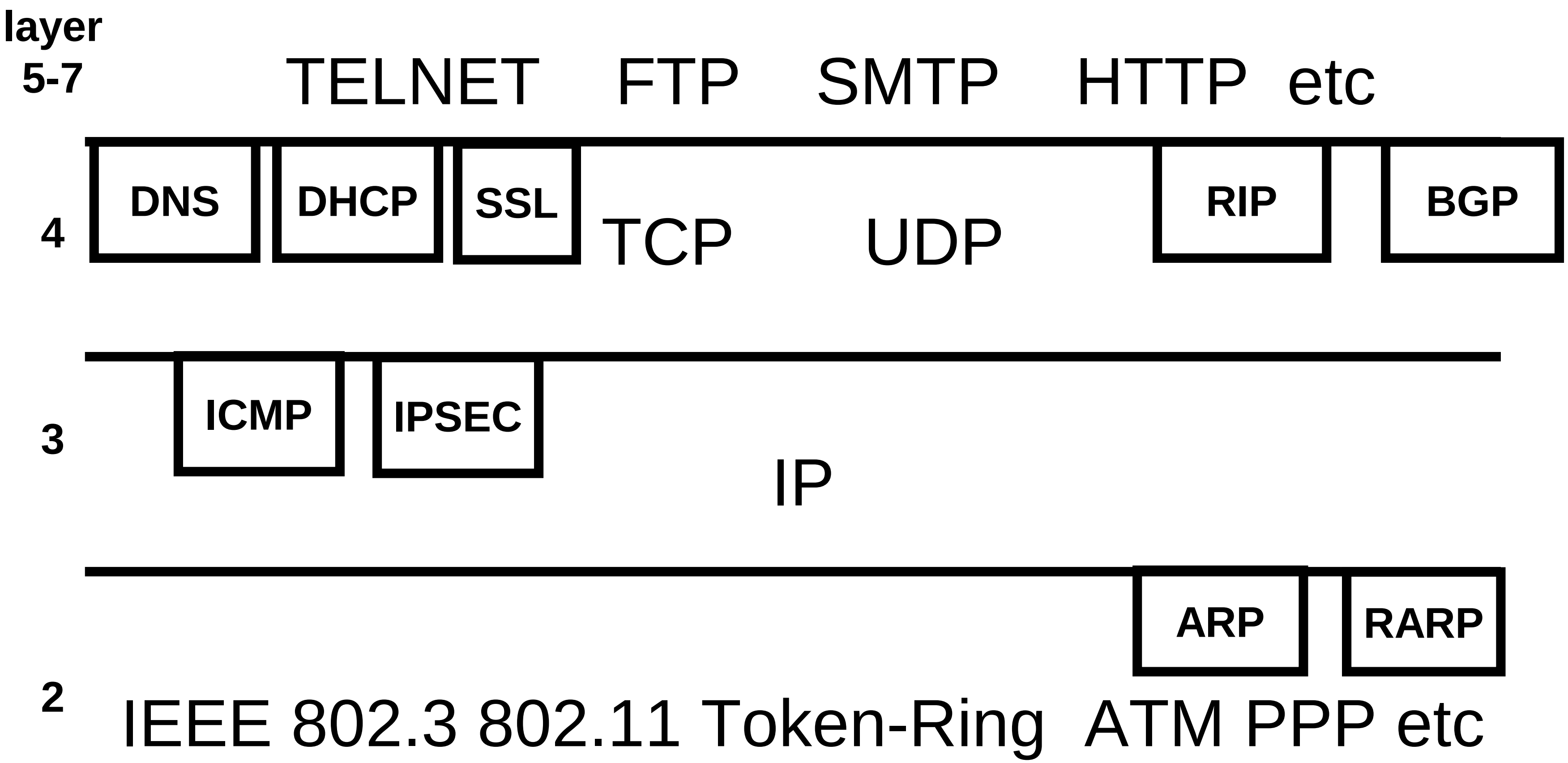
ARP RARP

IEEE 802.3 802.11 Token-Ring ATM PPP etc

TCP/IP Protocol Stack: Infrastructure Protocols

- DNS: Domain Name Service
- DHCP: Dynamic Host Configuration Protocol
- OSPF: Open Shortest Path First
- BGP: Border Gateway Protocol
- ICMP: Internet Control Message Protocol
- ARP: Address Resolution Protocol
- RARP: Reverse Address Resolution Protocol

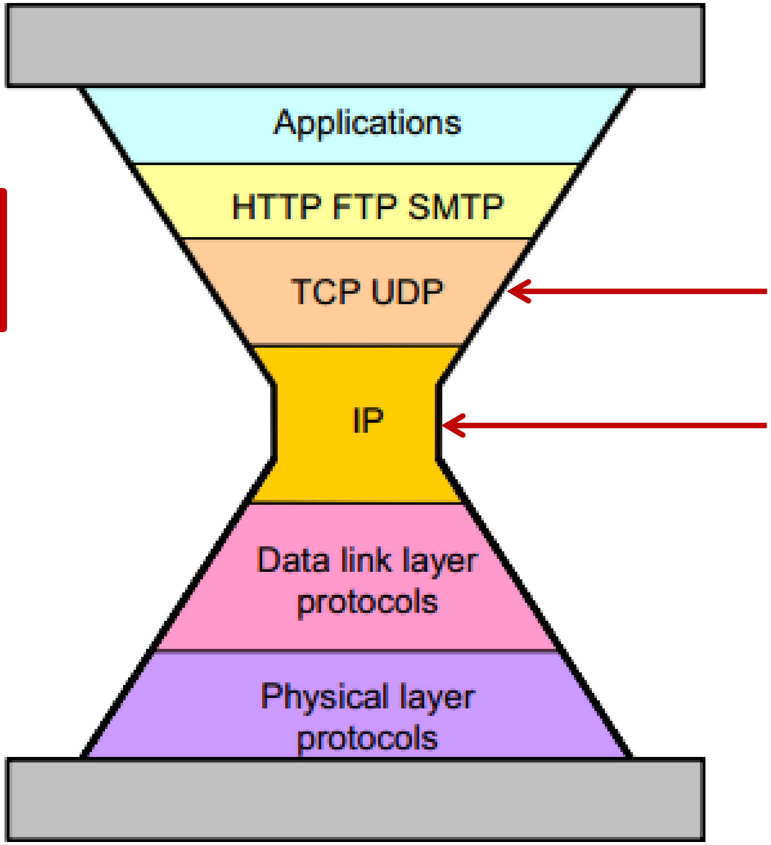
TCP/IP Protocol Stack: Security Protocols



Internet Security Protocols

Dozens of other security protocols

Some successes
Many failures



Half successful

SSL,1994

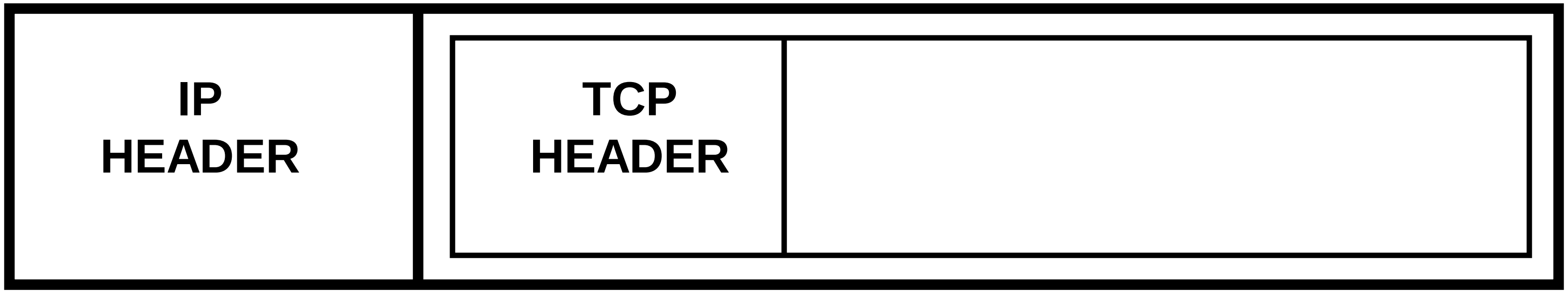
IPsec, 1998

Largely failed

IP v4 Packet

- header
- data
  - carries a layer 4 protocol
    - TCP, UDP
  - or a layer 3 protocol
    - ICMP, IPSEC, IP
  - or a layer 2 protocol
    - IEEE 802.3

TCP Inside IP



IP Header Format

- version: 4bit, currently v4
- header length: 4 bit, length in 32 bit words
- TOS (type of service): unused
- total length: 16 bits, length in bytes
- identification, flags, fragment offset: total 16 bits used for packet fragmentation and reassembly
- TTL (time to live): 8 bits, used as hop count
- Protocol: 8 bit, protocol being carried in IP packet, usually TCP, UDP but also ICMP, IPSEC, IP, IEEE 802.3
- header checksum: 16 bit checksum
- source address: 32 bit IP address
- destination address: 32 bit IP address

IP Header Format

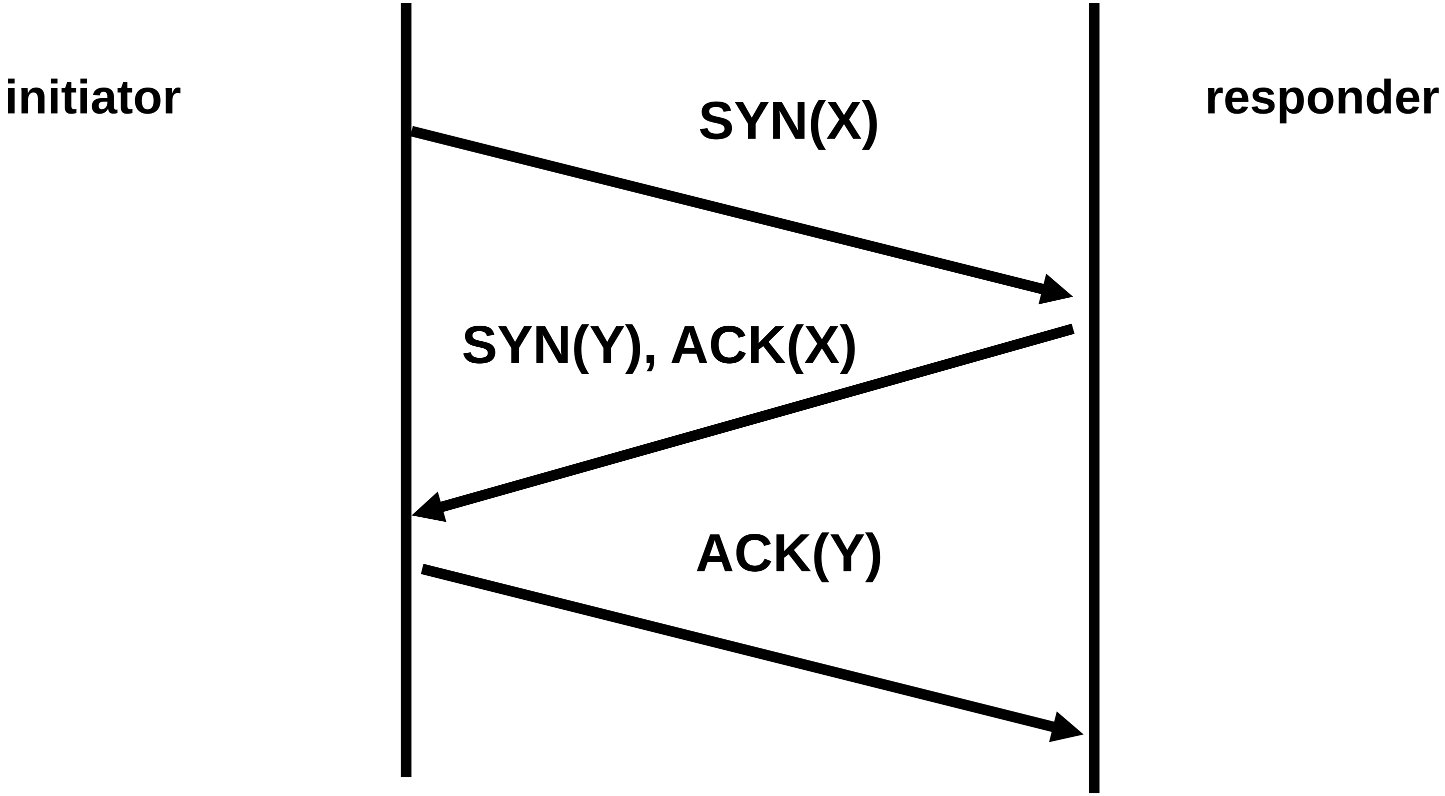
- options
  - source routing
    - enables route of a packet and its response to be explicitly controlled
  - route recording
  - timestamping
  - security labels

TCP Header Format

- source port number
- source IP address + source port number is a socket: uniquely identifies sender
- destination port number
- destination IP address + destination port number is a socket : uniquely identifies receiver
- SYN and ACK flags
- sequence number
- acknowledgement number

TCP/IP Vulnerabilities

TCP 3 Way Handshake



TCP SYN Flooding Attack

- TCP 3 way handshake
  - send SYN packet with random IP source address
  - return SYN-ACK packet is lost
  - half-open connection stays for some time-out period
- Denial of service attack
- Basis for IP spoofing attack

IP Spoofing

- Send SYN packet with spoofed source IP address
- SYN-flood real source so it drops SYN-ACK packet
- guess sequence number and send ACK packet to target
  - target will continue to accept packets and response packets will be dropped

TCP Session Hijacking

- Send RST packet with spoofed source IP address and appropriate sequence number to one end
- SYN-flood that end
- send ACK packets to target at other end

Fundamental Vulnerability

- IP packet carries no authentication of source address
- IP spoofing is possible
- Firewalls do not solve this problem
- Requires cryptographic solutions

IP Spoofing Story

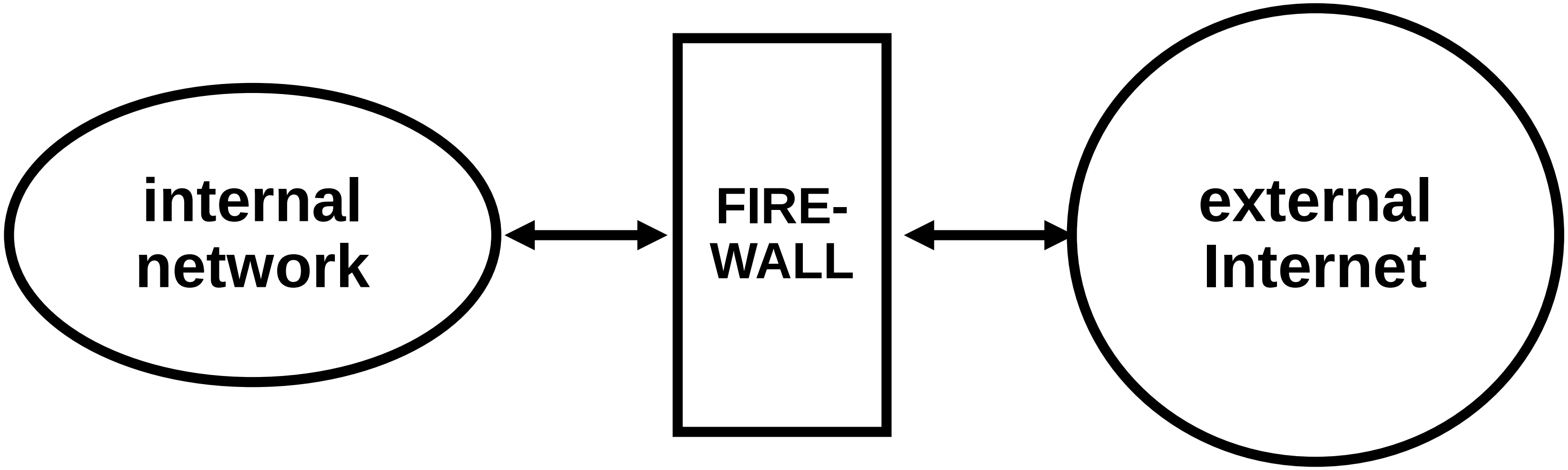
ALLOW GOOD GUYS IN
KEEP BAD GUYS OUT

- IP Spoofing predicted in Bell Labs report ≈ 1985
- Unencrypted Telnet with passwords in clear
- 1st Generation firewalls deployed ≈ 1992
- IP Spoofing attacks proliferate in the wild ≈ 1993
- Virtual Private Networks emerge ≈ late 1990's
- Vulnerability shifts to the client PC
- Network Admission Control ≈ 2000's

- Persists as a Distributed Denial of Service mechanism
- Most of these fixes have not changed or extended IPv4

Firewalls

What is a Firewall?



What is a Firewall?

- all traffic between external and internal networks must go through the firewall
  - easier said than done
- firewall has opportunity to ensure that only suitable traffic goes back and forth
  - easier said than done

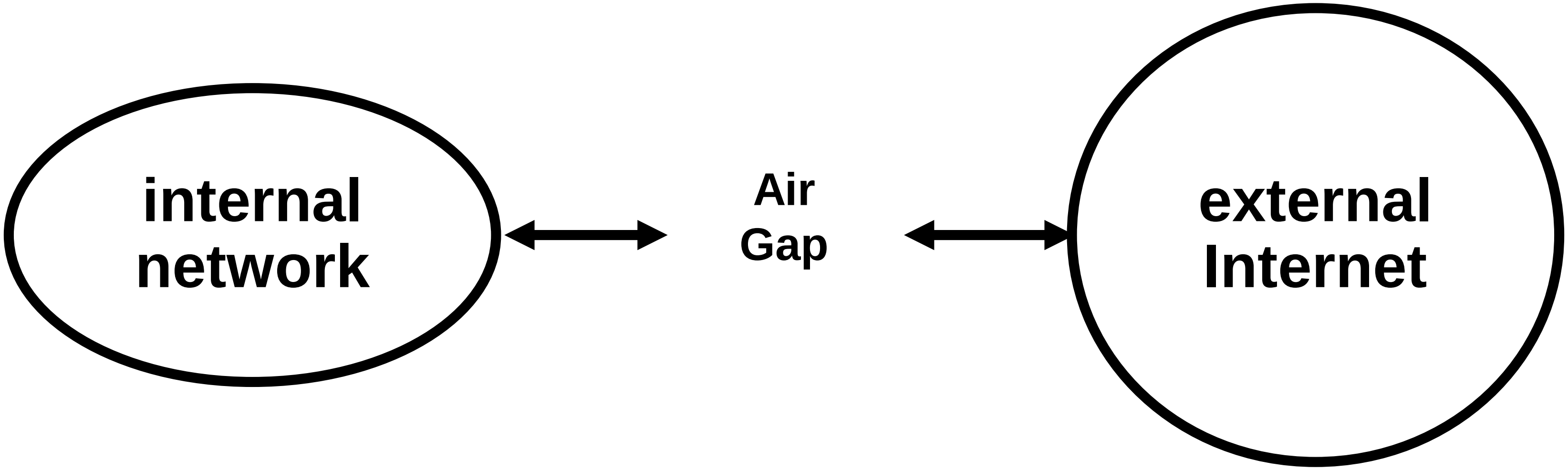
Benefits

- secure and carefully administer firewall machines to allow controlled interaction with external Internet
  - internal machines can be administered with varying degrees of care
- does work

Basic Limitations

- connections which bypass firewall
- services through the firewall introduce vulnerabilities
- insiders can exercise internal vulnerabilities
- performance may suffer
- single point of failure

Ultimate Firewall


internal network

Air Gap

external Internet

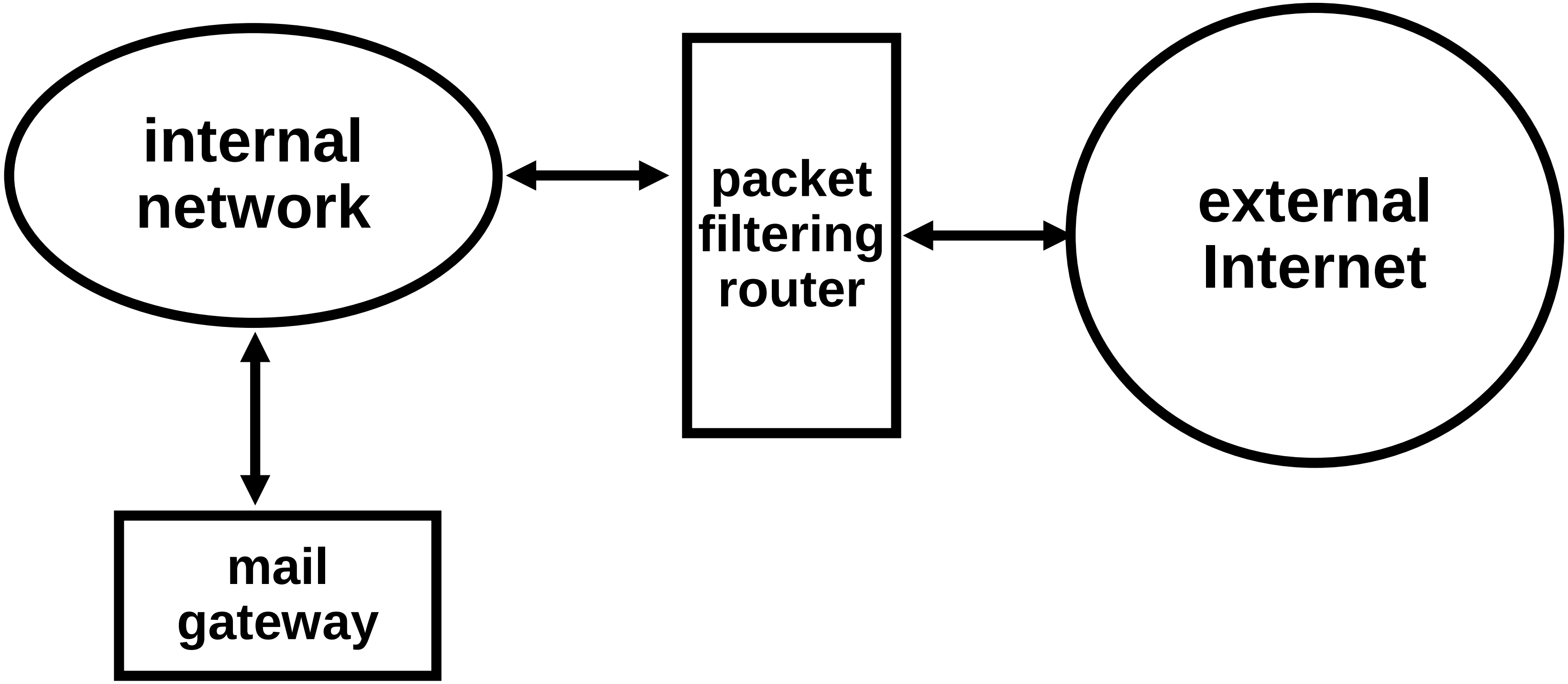
Types of Firewalls

- Packet filtering firewalls
  - IP layer
- Application gateway firewalls
  - Application layer

Packet Filtering Firewalls

- IP packets are filtered based on
  - source IP address + source port number
  - destination IP address + destination port number
  - protocol field: TCP or UDP
  - TCP protocol flag: SYN or ACK
  - TCP/UDP: protocol field

Filtering Routers



Packet Filtering Firewalls

- drop packets based on filtering rules
- static (stateless) filtering
  - no context is kept
- dynamic (stateful) filtering
  - keeps context

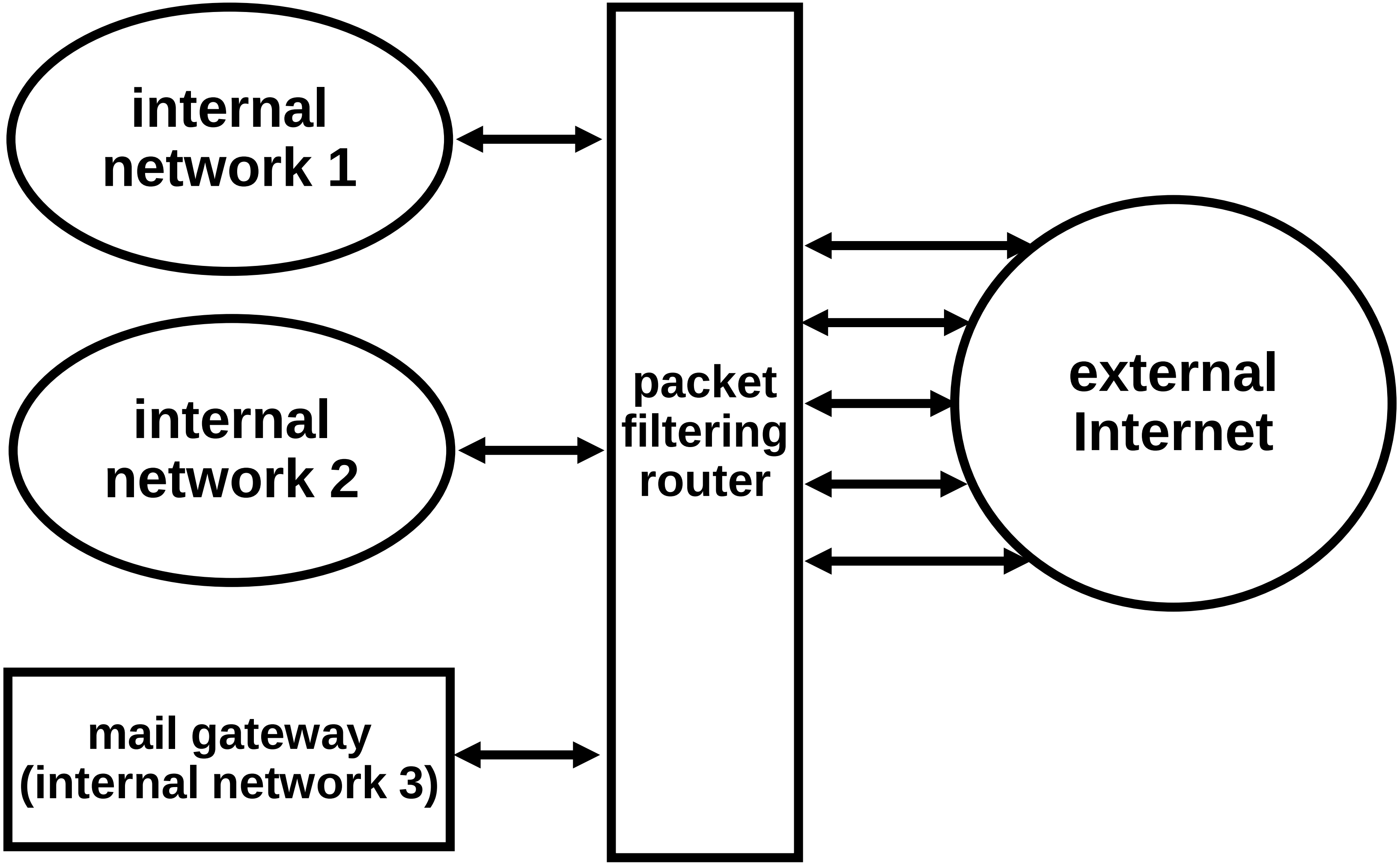
Packet Filtering Firewalls

- Should never allow packet with source address of internal machine to enter from external internet
- Cannot trust source address to allow selective access from outside

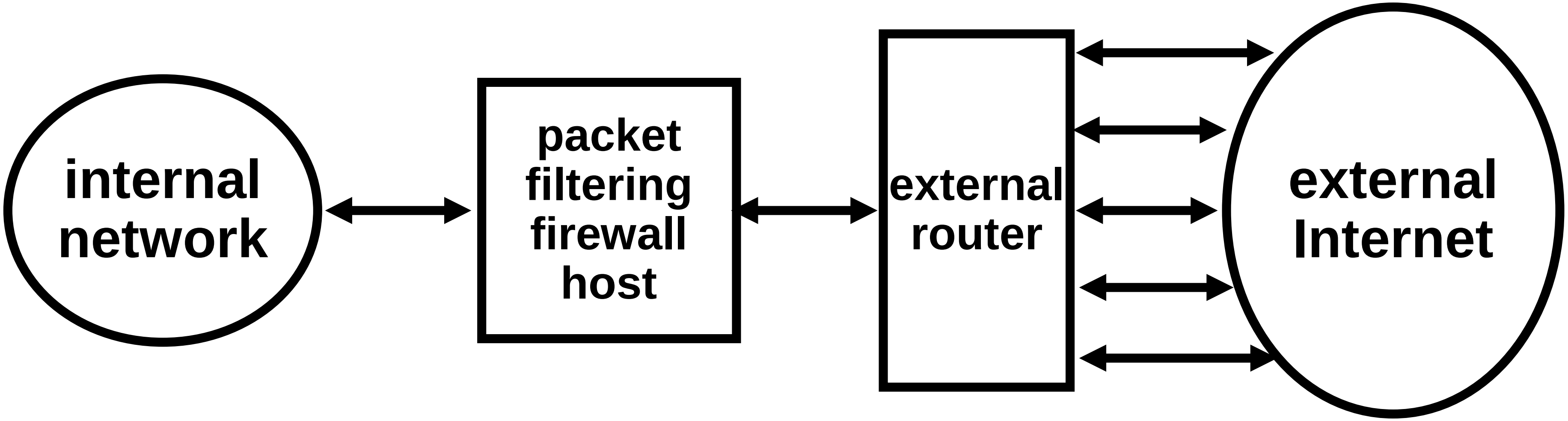
Packet Filtering Firewalls

- packet filtering is effective for coarse-grained controls
- not so effective for fine-grained control
  - can do: allow outgoing ftp from a particular internal host
  - cannot do: allow outgoing ftp from a particular internal user

Filtering Routers

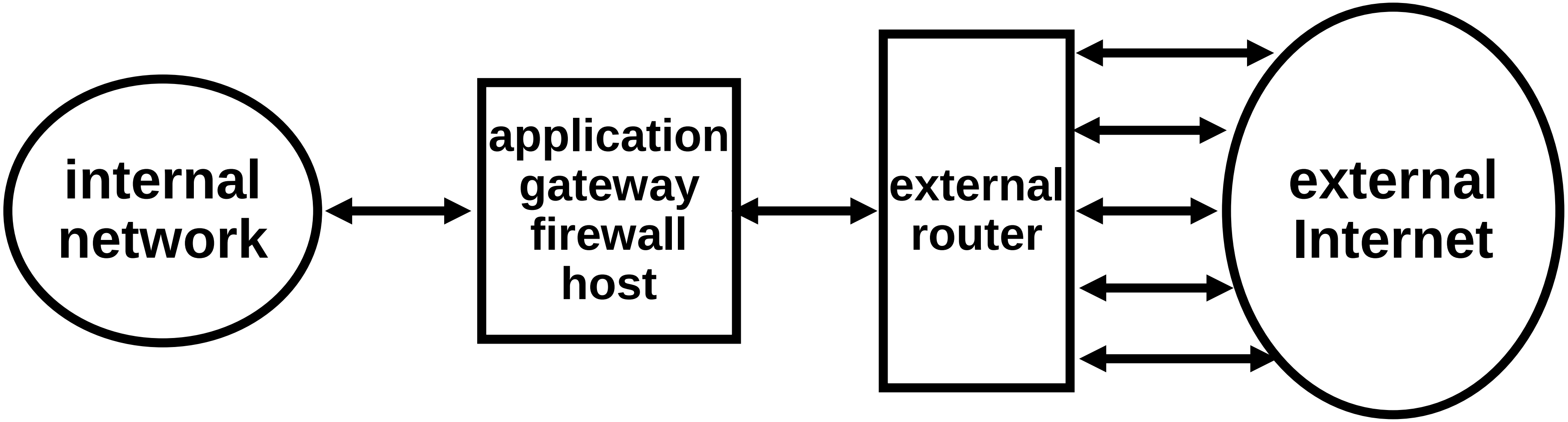


Filtering Host



- ➢ one can use a packet filtering firewall even if connection to Internet is via an external service provider

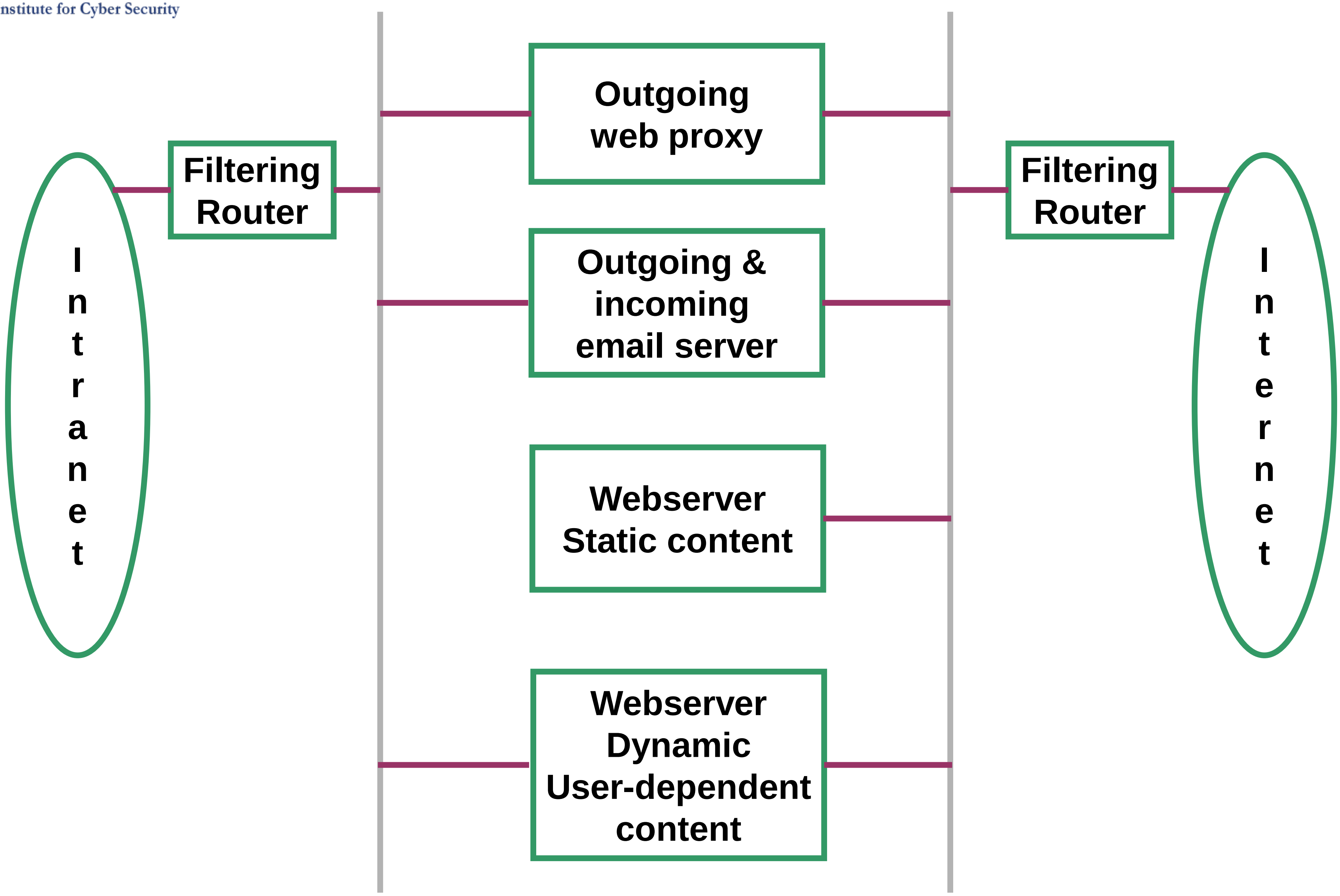
Application Gateway Firewalls



Application Proxies

- have to be implemented for each service
- may not be safe (depending on service)
- typically used for outgoing http requests from internal users

Demilitarized Zone (DMZ)



World-Leading Research with Real-World Impact!