NETWORK

SECURITY

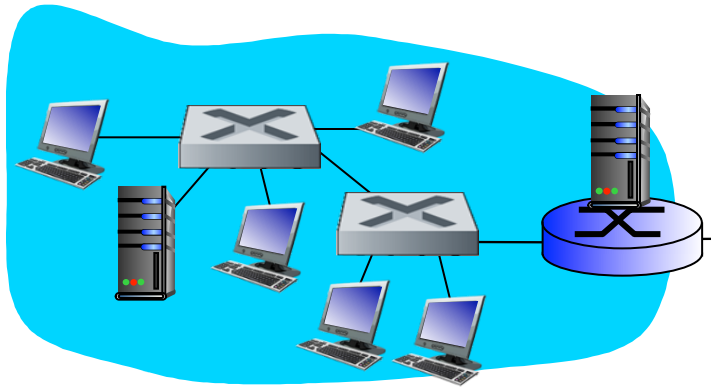
08 FIREWALLS

Contents

Firewalls

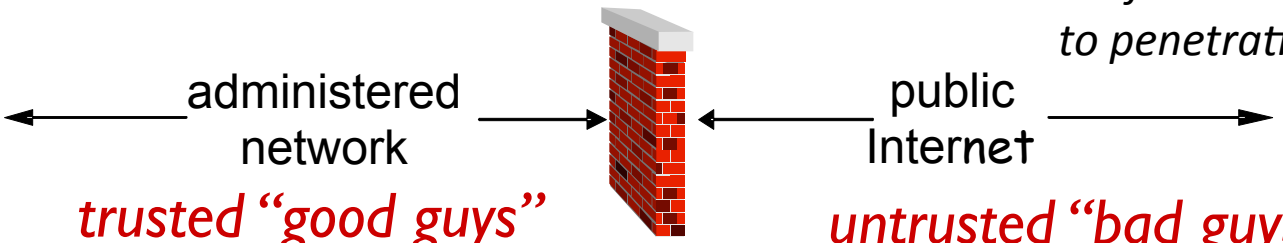
firewall

a collection of components that isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others



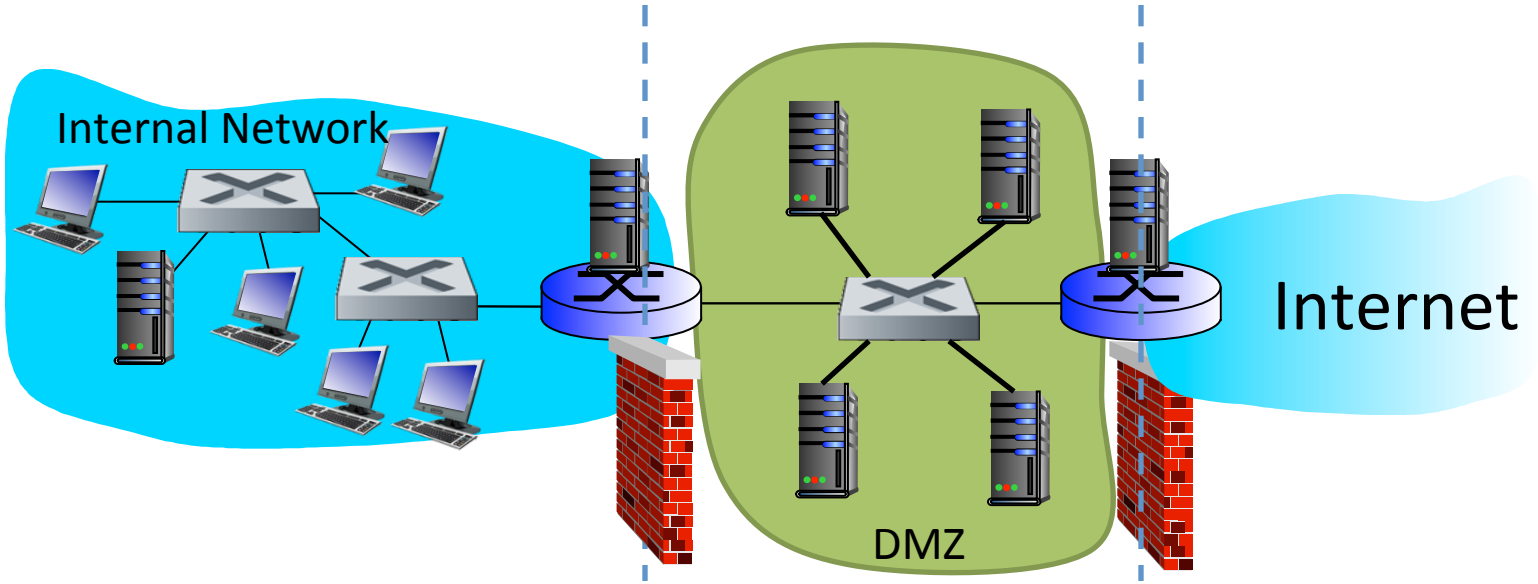
A Firewall has three goals:

1. *All traffic from outside to inside, vice versa, passes through the firewall.*
2. *Only authorized traffic, as defined by the local security policy, will be allowed to pass.*
3. *The firewall itself is immune to penetration.*



firewall

Firewalls: Typical Configuration



- **Demilitarized Zone (DMZ)** is a noncritical yet secure region generally designed at the periphery of the internal and external networks.
- Hosts within DMZ sometimes called as *bastion hosts*.

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

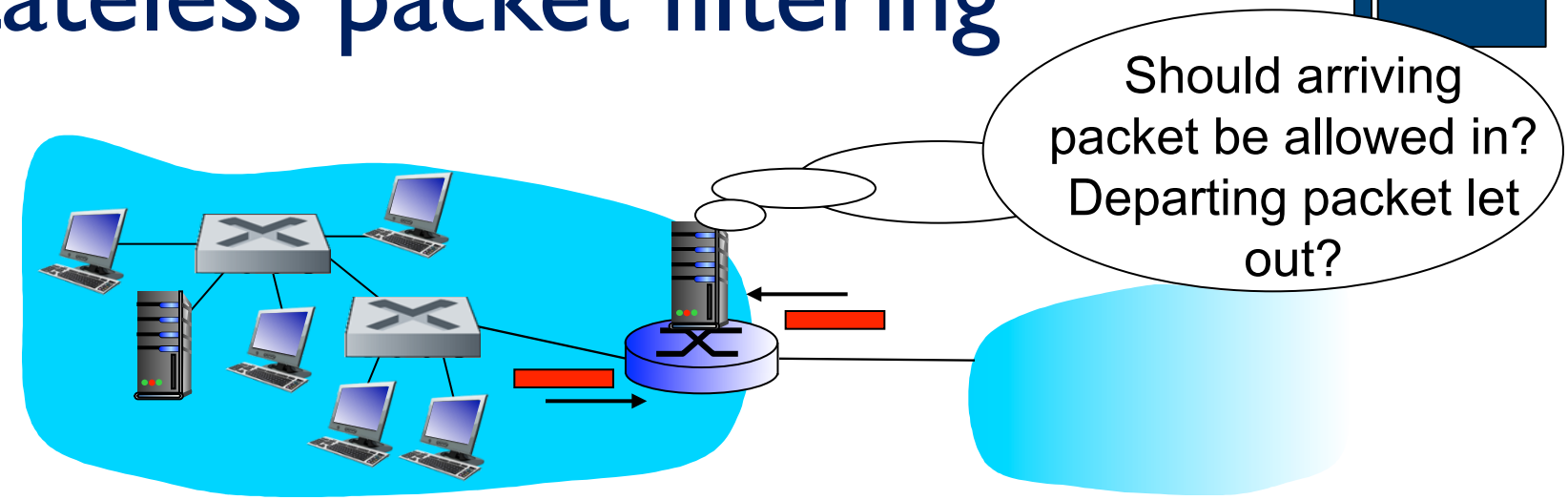
allow only authorized access to inside network

- set of authenticated users/hosts

Categories 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
  - ICMP message type
  - TCP 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: 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:* 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

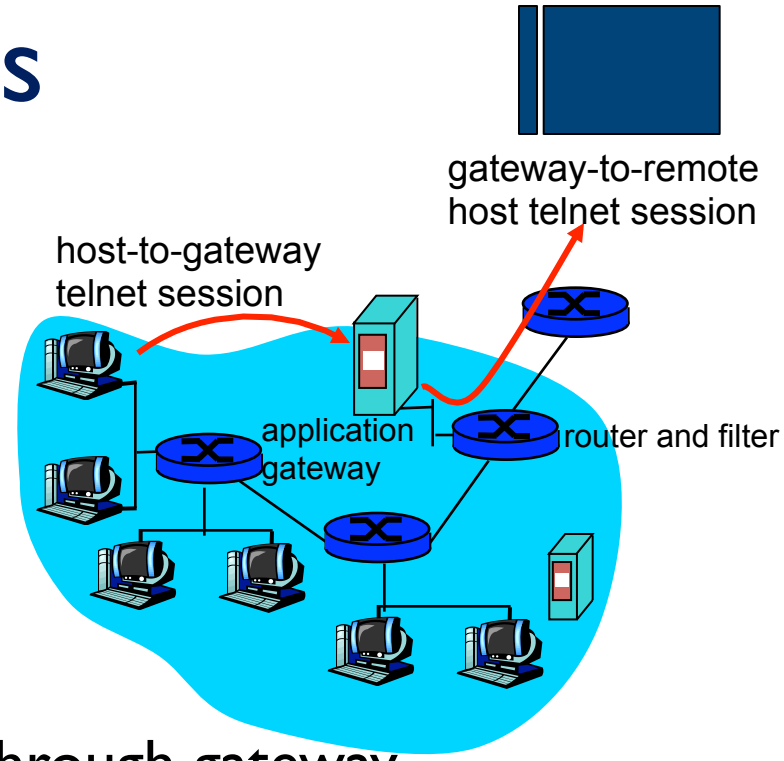
Stateful packet filtering

- 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 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

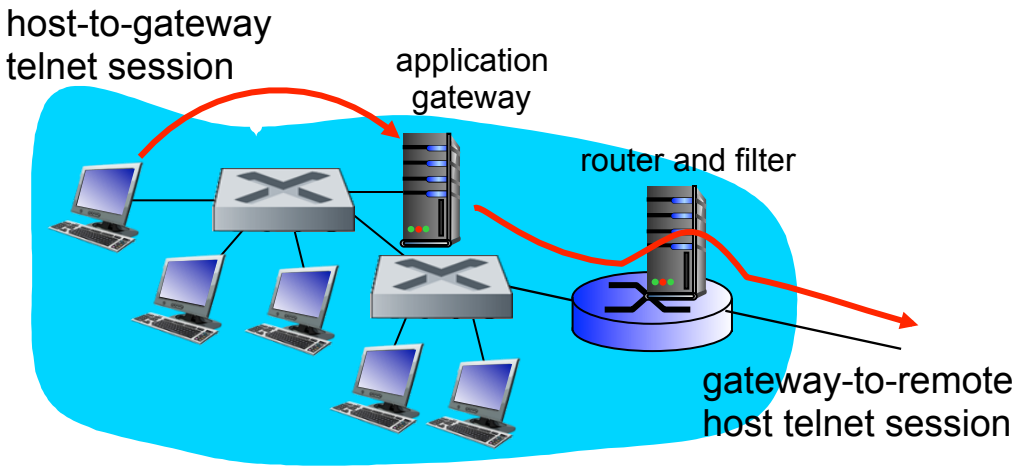
- filters packets on application data as well as on IP/TCP/UDP fields.
- *example:* allow select internal users to telnet outside.



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

Challenges of Firewall Placement

- Consistency
  - Ensuring the firewall sees all the packets of a flow
  - … even if routing changes occur
  - Hard if the firewall lies in the middle of the network
- Efficiency
  - Avoiding wasted bandwidth before traffic reaches firewall
  - Reduces load on the end-host computers
- Scalability
  - Handling the total volume of traffic
  - Maintaining connection and application state

Where Do Firewalls Run?

- On the end host
  - Can include information from application system calls
  - Scalability and customization with a firewall per host
- Just in front of the host(s)
  - Share the firewall between a group of related hosts
  - Reduces traffic and CPU load on the end hosts
- At the gateway to the Internet
  - Share the firewall across an entire organization
  - Avoid wasting resources inside the organization
- On the router itself
  - Avoid the cost of buying and supporting another box

Some of Firewalls

- Personal Firewall
- Distributed Firewall
- Layer 2 Firewall
- Appliance Firewall

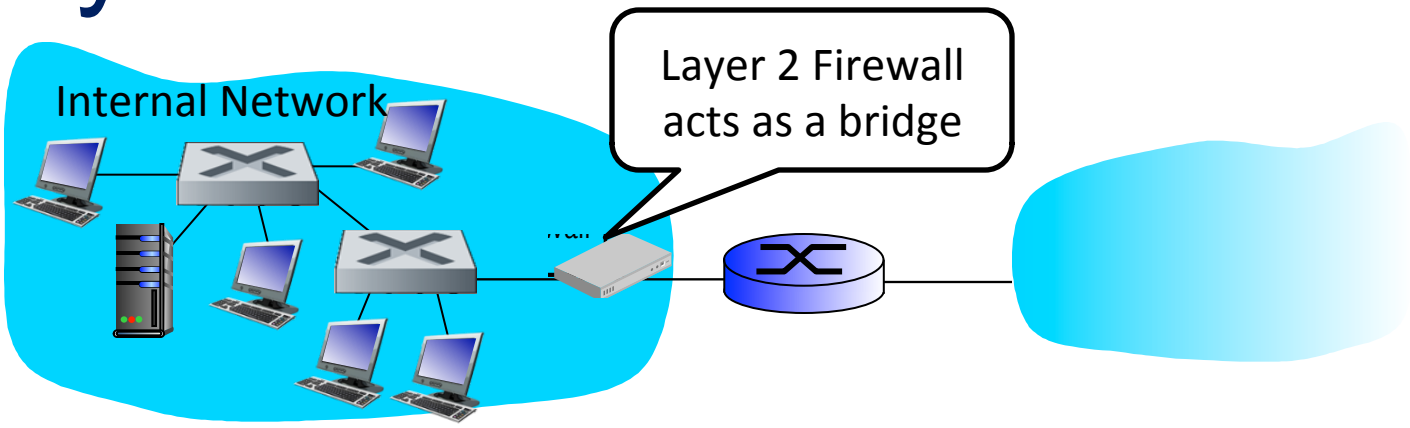
Personal Firewall

- software that runs on your workstation and acts as a packet filtering firewall
- installs kernel-level software that monitors and intercepts network related calls.
  - associate rules with program so that an application can connect to host on the Internet. Example: Web browser on your desktop
- Limitations:
  - runs under a general-purpose OS on desktop.
  - if desktop is compromised by viruses, it may disable personal firewall

Distributed Firewalls

- Improve the conventional firewall design:
  - define the security policy at a central point.
  - enforce the rules at each individual network endpoint (hosts, routers, etc.)
- Three needed components:
  - a language for expressing policies and resolving requests.
  - a mechanism for safely distributing security policies
  - a mechanism that applies the security policy to incoming packets or connections, providing the enforcement part.

Layer 2 Firewall



- Most firewalls typically operate in IP layer.
  - sits in-between internal net and ext. net
- Operate in Layer 2 (link layer)
  - hosts need not be aware of firewall installation
  - allows easy deployment and transparent to IP layer.
  - can be deployed at various point.
- Applicability of Layer 2 Firewall:
  - Prevent ARP spoofing attacks

Appliance Firewall

- What is Appliance Firewall?
  - Integrated hardware solution
  - All softwares, including OS comes pre-loaded on the platform
  - Network “black box” approach to security
- What technologies do they employ?
  - Network Address Translation (NAT)
  - Most use packet filtering rules to determine packet access
  - Some use “stateful inspection” to manage connections
  - Some application proxy support
    - A few allow custom proxy creation *BONUS*