CS 330: Network Applications & Protocols

Network Security

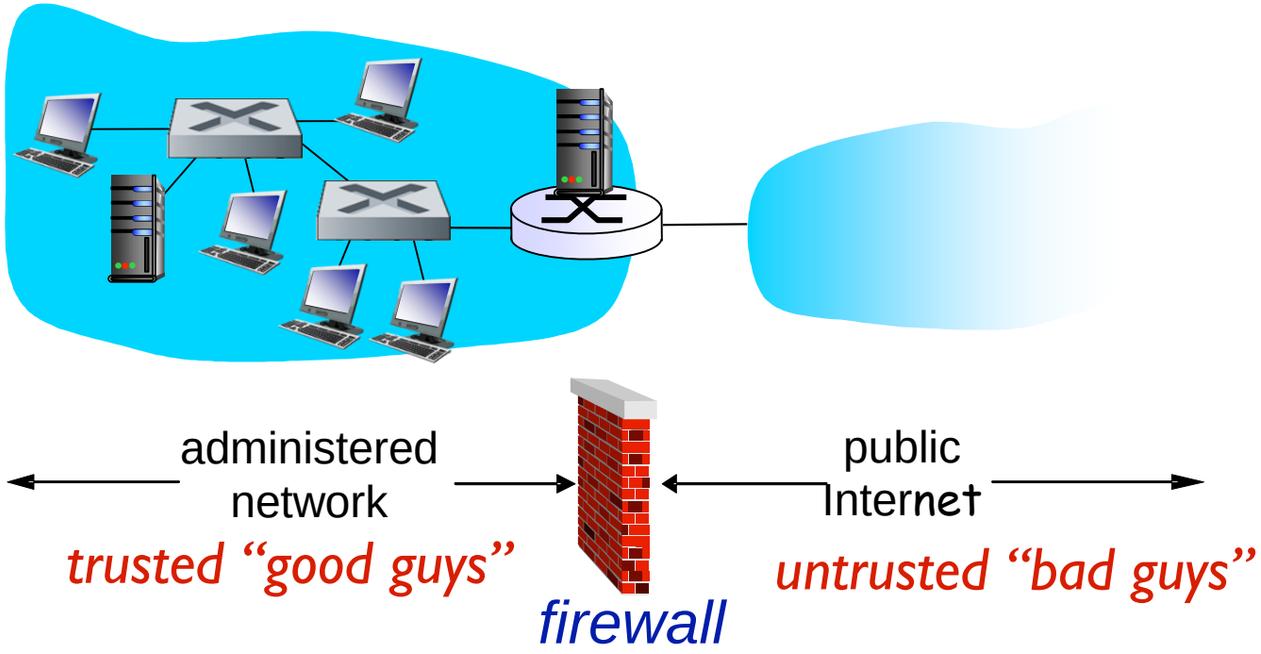
Galin Zhelezov
Department of Physical Sciences
York College of Pennsylvania

Overview of Network Security

- **What is Network Security?**
- **Principles of Cryptography**
- **Message Integrity, Authentication**
- **Operational Security: Firewalls and IDS**

Firewalls

- **Isolate an organization's internal net from larger Internet, allowing some packets to pass, blocking others**

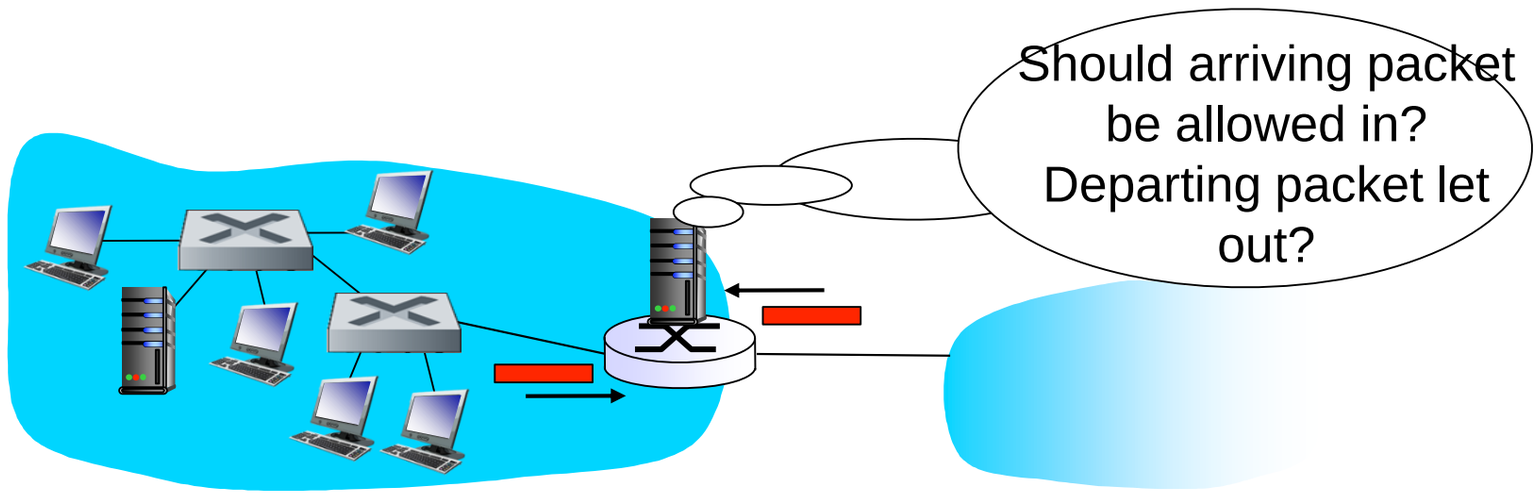


Why Use a Firewall?

- **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**
  - For example, 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**
- **Router filters packet-by-packet, decision to forward/drop packet based on:**
  - Source IP address, destination IP address
  - Protocol type in IP datagram (i.e. TCP, UDP, ICMP, etc.)
  - 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: 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	Destination Address	Protocol	Source Port	Destination 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	Destination Address	Protocol	Source Port	Destination Port	Flag Bit
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

- **Stateful packet filter: tracks 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

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

Action	Source Address	Destination Address	Protocol	Source Port	Destination 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	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	

Stateful Packet Filtering: Connection Table

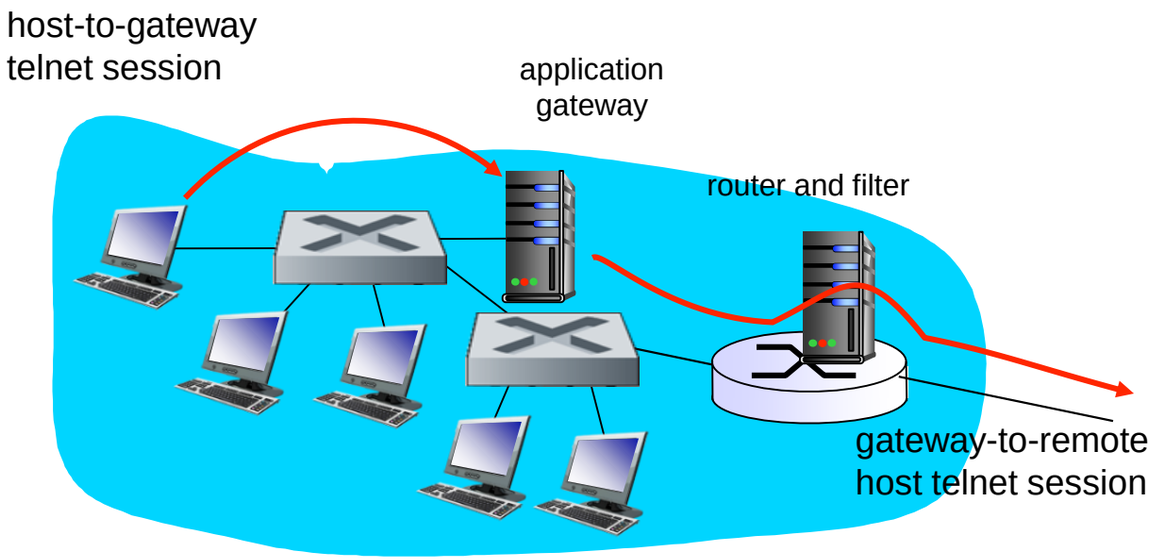
- **Given the following connection table and the previous ACL**

Source Address	Destination Address	Source Port	Destination Port
222.22.1.7	37.96.87.123	12699	80
222.22.93.2	199.1.205.23	37654	80
222.22.65.143	203.77.240.43	48712	80

- **Allow a packet from 37.96.87.123, port 80 to 222.22.1.7, port 12699**
- **Block a packet from 12.1.18.83, port 80 to 222.22.1.7, port 12699**
  - According to the connection table, no connection has been established

Application Gateways

- **Filters packets on application data as well as on IP/TCP/UDP fields**
- **Example, allow select internal users to telnet out of the network**
  - Require all telnet users to telnet through gateway
  - For authorized users:
    - Gateway sets up telnet connection to destination host
    - Gateway relays data between 2 connections
  - Router filter blocks all telnet connections not originating from gateway



Limitations of Firewalls, Gateways

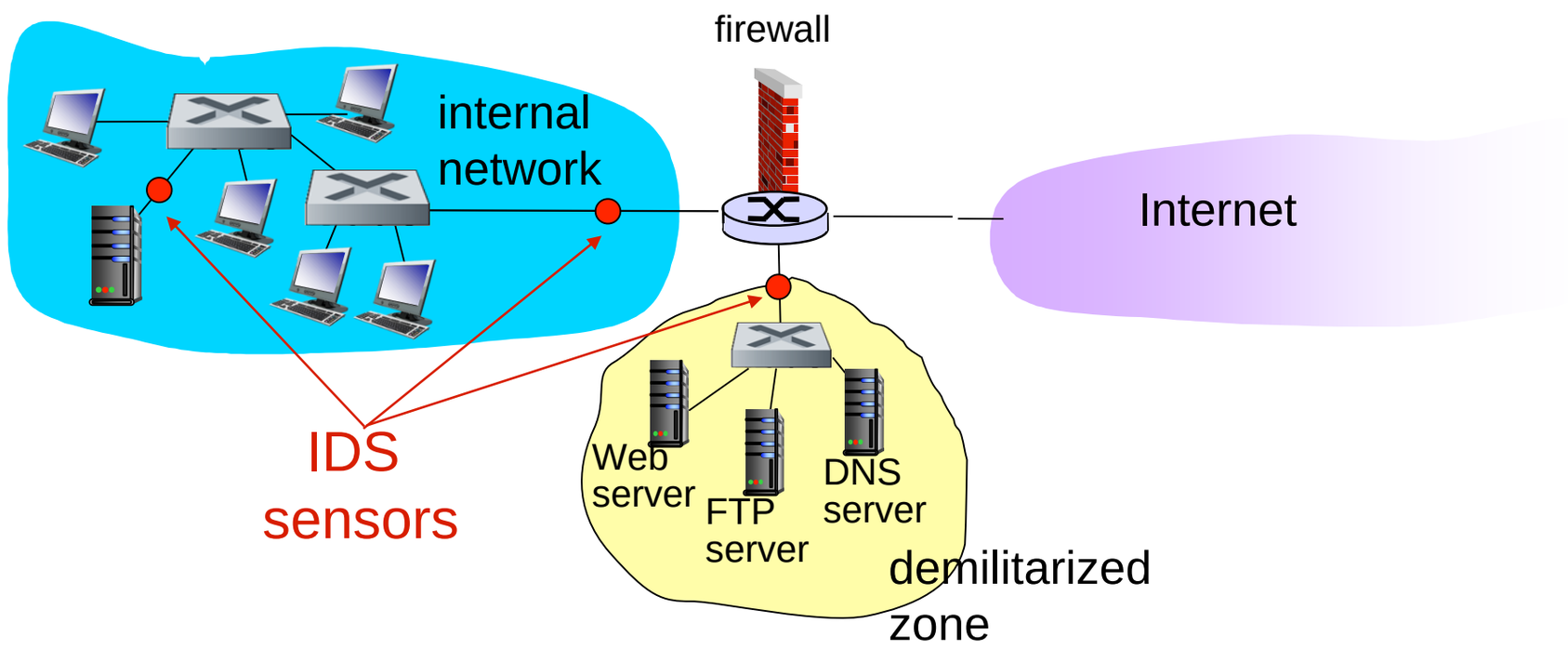
- **IP spoofing - router can't know if data "really" comes from claimed source**
- **If multiple applications need special treatment, each has own application gateway**
- **Client software must know how to contact the application gateway**
  - e.g. must set IP address of proxy in Web browser
- **Filters often use all or nothing policy for UDP**
- **Tradeoff between communication with outside world and security**
- **Many highly protected sites still suffer from attacks**

Intrusion Detection Systems

- **Packet filtering**
  - Operates on TCP/IP headers only
  - No correlation check among sessions
- **IDS: Intrusion Detection System**
  - Perform 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 Detection Systems

- **Multiple IDSs perform different types of checking at different locations**
  - Distribute work load of IDS throughout network
  - IDS may potentially need to scan thousands of signatures that represent known network attacks or viruses



Intrusion Detection Systems

- **Example of an IDS rule:**

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any
  (msg: "ICMP PING NMAP"; dsize: 0; itype:8;)
```

  - Raise an alert for an ICMP packet from any external IP address to any internal IP address that is of ICMP type 8, and has an empty payload
  - Send the alert message, "ICMP PING NMAP"

Network Security (summary)

basic techniques……

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

…. used in many different security scenarios

- secure email
- secure transport (SSL)
- IP sec
- 802.11

operational security: firewalls and IDS