Firewall: Packet Filtering

CSC 154

The Role of A Firewall

- Access control between two or more networks
  - Protect internal network from outside threats
  - Based on hardware and software, perhaps a combination

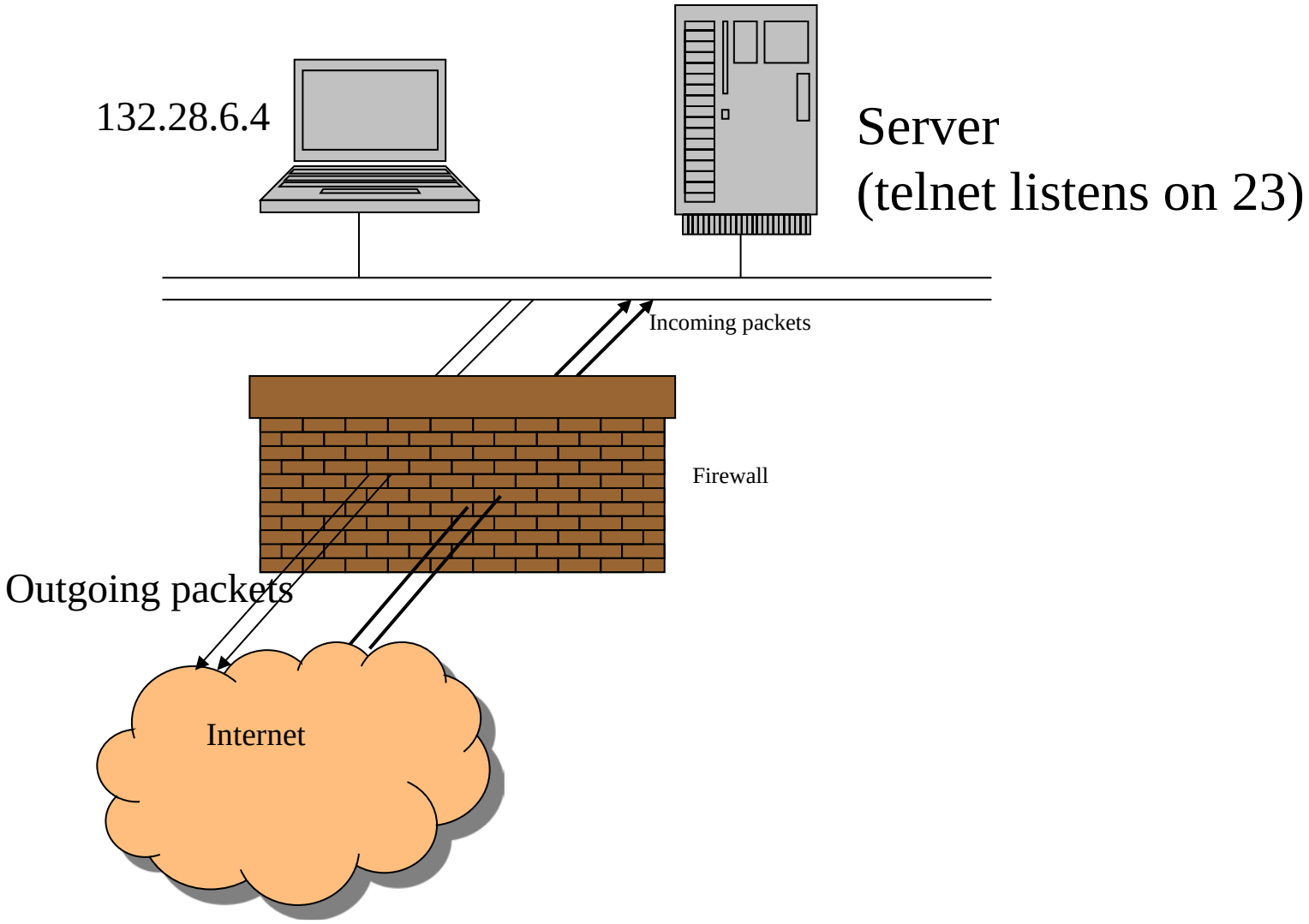
  - keep outsiders from breaking in
  - keep insiders from exposing confidential data
  - enable secure communication between outside network and inside network
    - bidirectional
    - firewall can proxy an internet service
    - block services known to be problematic

Firewall Technologies

- Packet Filtering
- Proxying
- Stateful Packet Filtering

Packet Filtering

- Header Information Checking
  - Rule set of accepting or denying traffic
  - Source IP, destination IP, protocol, source port, destination port, size of packet, sequence #
  - Does not look at contents
- What if spoofed with IP or port?
- Viruses or Trojans
  - Yes, vulnerabilities in firewalls that can be exploited



Examples and explanations in the following slides are from College of IST, PSU

To Be Configured

- 1. No incoming telnet service (request) should be processed
- 2. Outgoing telnet requests are OK
- 3. Computer 132.28.6.4 can not do Telnet
- 4. UDP packets are not allowed

Policy rule	Firewall rule	Direction	Source addr	Dest addr	Type	Source port	Dest port	ACK	action
(1)	A	Incoming	external	internal	TCP	*	23	0	deny
(3)	B	Outgoing	132.28.6.4	external	TCP	*	23	*	deny
(3)	C	Incoming	external	132.28.6.4	TCP	23	*	*	deny
(2)	D	Outgoing	internal	external	TCP	*	23	*	permit
(2)	E	Incoming	external	internal	TCP	23	*	*	permit
(4)	F	Incoming	external	internal	UDP	*	*	*	deny

Explain the 6 firewall rules one-by-one

- Rule A: Denies any incoming TCP packets that attempt to open a Telnet connection
- Rule B: Denies any outgoing Telnet packets from internal client 132.28.6.4 to external telnet server.
- Rule C: Denies incoming packets from external telnet serves
- Rule D and E: Someone from inside firewalls can telnet out, but no one from the outside can telnet in. Connection is established starting from the inside
  - What's the difference between telnet in and telnet out?
  - Telnet in= Internet client and internal server
  - Telnet out= internal client and internet server
- Rule F: Denies any incoming UDP packets

- Firewall rules are processed **sequentially**

Policy rule 1

- Policy rule 1: no incoming telnet service
  - We can enforce this policy rule by a single packet filtering rule which has the following field:
    - RULE #: RULE A
    - FIELD 1: source address
      - External IP (outside IP)
    - Field 2: destination
      - Inside IP (the IP of the internal telnet server)
    - Field 3: direction
      - inbound
    - Field 4: source port -- any port (no restriction)
    - Field 5: dest port -- 23 (telnet server)
    - Field 6: protocol -- TCP
    - Field 7: ACK -- 0
    - Field 8: Action -- deny

Policy rule 2: outgoing telnet requests OK

- To enforce this policy rule, we need TWO packet filtering rules
  - We need two rules because even if an internal employee telnets out, he needs to receives packets from the outside telnet server
  - Rule D: permit outgoing packets to the outside telnet server
    - So the source IP must be an internal IP; the dest IP must be an outside IP; the source port can be any; but the dest port must 23;
    - Direction: outbound
    - Protocol: TCP
    - ACK: 0 or 1 -- we need to allow both otherwise the telnet connection can NOT be established.
  - Rule E: permit incoming packets from the outside telnet server

Policy rule 2 – Rule E

- Rule E: permit incoming packets from the outside telnet server
  - Source IP: outside
  - Dest IP: inside
  - Direction: incoming - inbound
  - TCP
  - Source port: 23
  - Dest port (internal telnet client): any
  - Permit
  - ACK: *
    - Can we set ACK as 1?
      - ACK can NOT be 0 because we do NOT allow an outside telnet server to initiate a connection; actually a Telnet server should NEVER initiate a connection

Policy Rule 3

- Is Rule C redundant?
  - Rule B already specifies host is not able to establish telnet session, so no incoming traffic from a telnet server.
  - If hacker spoofs a packet, and rule C is removed, then the packet goes through
  - Will this packet be a problem for the network?
    - No
    - packet like a car, without rule c, packet will get in, packet will die there, packet will not be processed because no telnet session is established. No damage!

Policy rule 4

- Do you think Rule F is enough to block all UDP Packets?
  - Not enough, resources inside can cause damage to outside
    - if an internal resource gets hacked, it can cause problems for another network. To be safe, have to block all UDP going out.
  - UDP same header information as TCP, there is no way to tell if it is a response or if it is from a session already in progress.
    - UDP no 3 way handshake
  - Worm Slammer show malicious UDP packets can be sent from inside out to outside computers

Rule A and Rule E conflict, how so?

- Rule A blocks incoming requests to create a new TCP session, where Rule E allows already established sessions to continue
  - Process rules in order, fail Rule A first before it gets to E.

- Look at ACK flag

Rule B and Rule D conflict, how so?

- B denies all outgoing telnet packets from an internal server, D does the opposite
  - B trumps D. Rule B will kill packet, if not from the host (132.28.6.4) it will go through rule B.
- Why is the ACK permitting anything in Rule D?
- In Rule B, can we only set ACK as 0?
  - Yes
  - Future packets with ACK 1 die without any meaning

Rule C and Rule E conflict, how so?

- E allows incoming packets, but C denies incoming packets
  - Order matters
  - C is redundant

- Is there a reason to have D and E since they allow everything?
  - Yes, you want to specify what you allow.
  - Usually, packets that go through rule set are denied by default.

Advantages of Packet Filtering

- Easy to setup
  - with routers
  - Many routers support packet filtering
    - No need to buy dedicated hardware
    - No need to require customized software or configurations on client machines, compared with proxying hardware
  - Protect an entire network
    - Strategically place the router
    - A single router is enough
  - Inexpensive
  - Fast
  - transparent to users

Disadvantages of Packet Filtering

- Not that powerful
  - For example, it cannot help to hide the IP addresses of internal servers
- Packet filtering rules tend to be hard to configure and maintain
  - How to set up a set of rules that correctly reflect the security needs of a protected site and manage them is often difficult
  - Packet filtering rules are often difficult to test thoroughly
- Security policies above the network layer are hard to be enforced by packet filtering
  - For example, security policies based on user identities
- Packet filtering firewalls have little logging capability

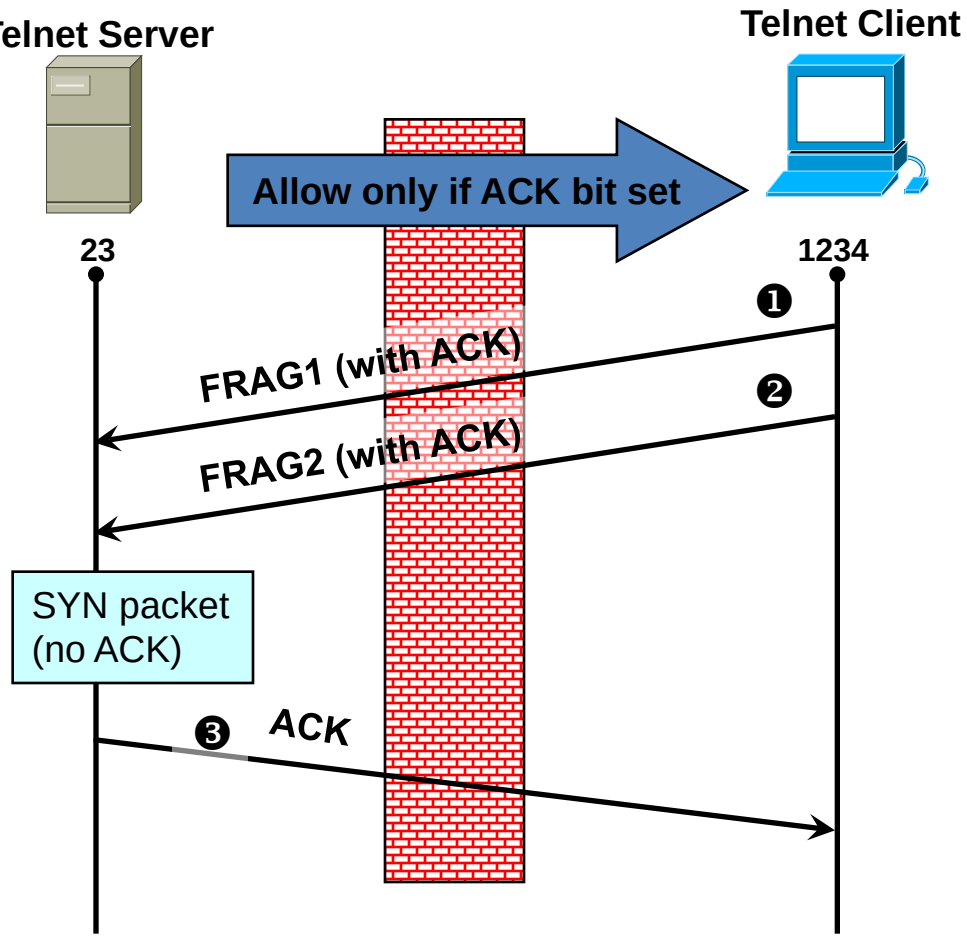
Attacks towards Packet Filtering?

- IP Spoofing Attacks
- Fragmentation Attacks

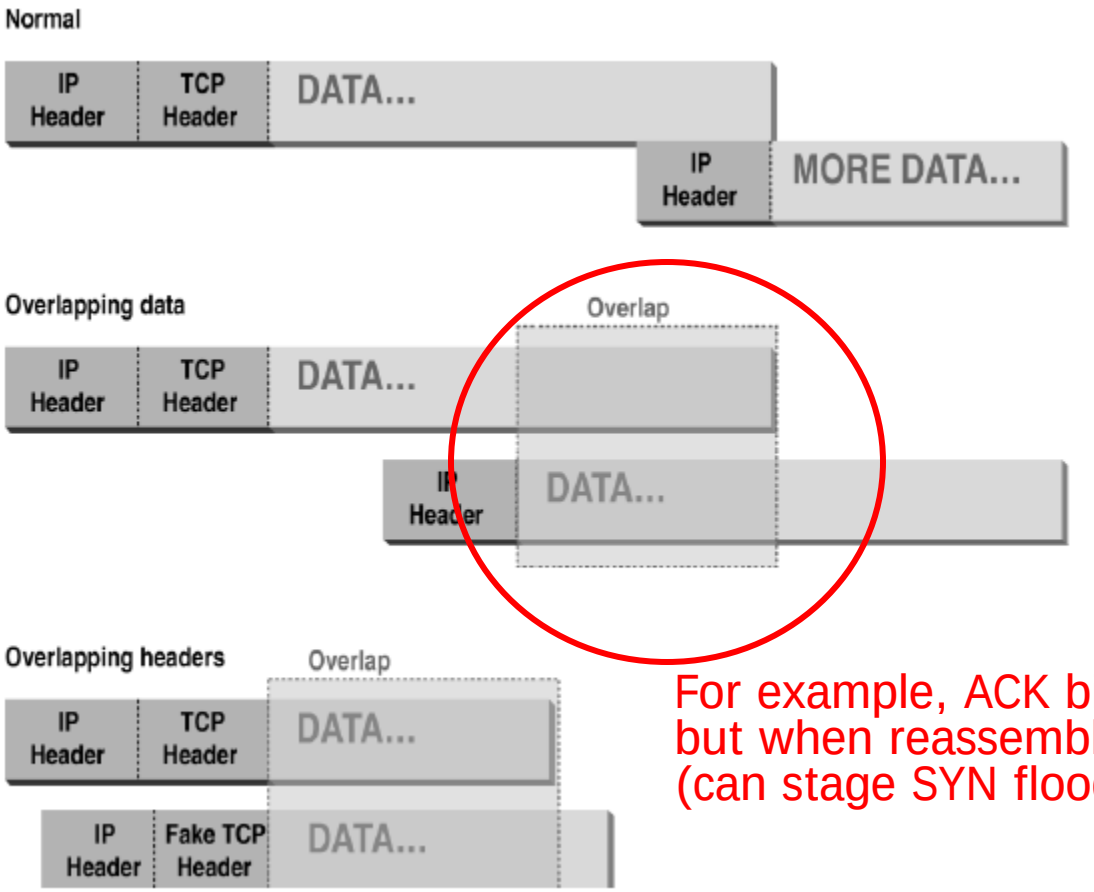
Fragmentation Attack (borrowed from Wenke Lee)

❶,❷ Send 2 fragments with the ACK bit set; fragment offsets are chosen so that the full datagram re-assembled by server forms a packet with the SYN bit set (the fragment offset of the second packet overlaps into the space of the first packet)

❸ All following packets will have the ACK bit set



Abnormal Fragmentation



For example, ACK bit is set in both fragments, but when reassembled, SYN bit is set (can stage SYN flooding through firewall)

The following slides adapted from Shmatikov, UT Austin