Firewalls

firewall

isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others.

Two firewall types:

- packet filter
  - Stateless
  - Stateful
- application gateways

To prevent denial of service attacks:

- SYN flooding: attacker establishes many bogus TCP connections.
- Attacks on specific vulnerabilities of internal services
  - Example: code red
  - Internal web server should have no incoming or outgoing access

Firewalls

- To prevent unwanted modification of internal data.
  - e.g., attacker replaces CIA's homepage with something else
- To prevent intruders from obtaining secret info.
  - Even mundane secret info – network footprint
    - What are the targets?

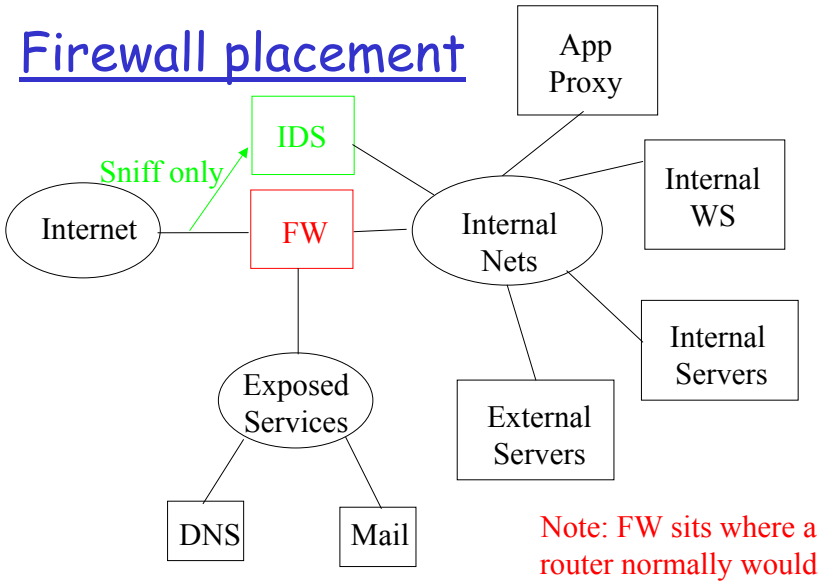
Firewall rules-of-thumb

- To block or not to block
  - Mostly-open?
  - Mostly-closed?
  - The decision should match the purpose of the protected network
- Different hosts need different protection
- Let in only what needs to be let in
  - Rules are destination- and protocol-specific
- Let out only what needs to be let out
  - Minimize exposure of internal hosts behavior
    - N.b. internal addresses may be well-known anyway

Firewall rules-of-thumb

- Block known bad-guys
  - Protocols
  - Hosts
- Special problem for UDP, ICMP
  - Not part of any connection
- When decision is "block"
  - Politely decline? (ICMP Conn Refused)
  - Remain mute?
- Defense in depth
  - Intrusion Detection
  - Host should only run what is needed
  - Host-based firewalls
  - Monitor security bulletins and software security updates

Firewall placement



Note: FW sits where a router normally would

Simple Packet Inspection Filtering

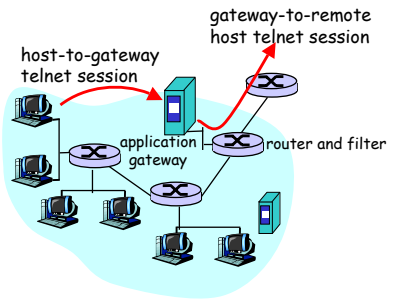
- As described in book
- Internal network is connected to Internet through a router.
- Router manufacturer provides options for filtering packets, based on:
  - source IP address
  - destination IP address
  - TCP/UDP source and destination port numbers
  - ICMP message type
  - TCP SYN and ACK bits
- Ex. Home routers
- Example 1: block incoming and outgoing datagrams with IP protocol field = 17 and block datagrams with either source or dest port = 23.
  - All incoming and outgoing UDP flows and telnet connections are blocked.
- Example 2: Block inbound TCP segments with ACK=0.
  - Prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.

Stateful Packet Filtering

- Ex. Checkpoint FW-1
- Ex. Linux IPTables
- Allow incoming TCP packets for established connections
- Allow incoming UDP or ICMP only in response to previous UDP/ICMP
- Allow traffic at only a certain rate
- Block known bad-guys
  - Protocols
  - Hosts
- Special problem for UDP, ICMP
  - Not part of any connection
- When decision is "block"
  - Politely decline? (ICMP Conn Refused)
  - Remain mute?

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.

Limitations of firewalls and 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.

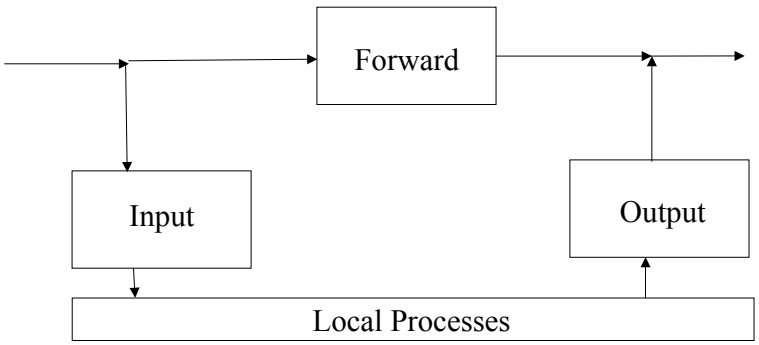
Network Address Translation

- You have only N internet address and you have N+M computers (interesting case N=1)
  - Share! How?
- NAT
  - Router "translates" local addresses in incoming & outgoing packets
- Natural complement to stateful firewall
  - Connection tracking state needed for firewall is similar to that needed for NAT
- Originally
  - Src: 10.0.1.30 Port 2455
  - Dst: 12.18.238.75 Port 80
- After NAT
  - Src: 121.64.32.12 Port 3715
  - Dst: 12.18.238.75 Port 80

Linux Configuration for NAT and Firewall

- Iptables
  - Several different "tables"
    - Filter
    - NAT
    - Mangle – not talking about this one
  - Each table has several built-in "chains"
  - Each chain has several "rules"
  - Each rule has a "match part" and a "target" part
- Filter table chains
  - Input
  - Forward
  - Output
- NAT table chains
  - Prerouting
  - Postrouting
- User-defined chain
  - Add to any table
  - Use as subroutine in pre-defined chains

Filter table chains



NAT table chains

