Firewalls

Firewalls

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

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

Defense in depth

Intrusion Detection

Host should only run what is needed

Host-based firewalls

Monitor security bulletins and software security updates
**Firewall placement**

- **Internet**
  - **FW**
  - **Internal Nets**
  - **Exposed Services**
  - **DNS**
  - **Mail**
  - **Internal WS**
  - **External Servers**

**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

---

**Stateful Packet Filtering**

- Ex. Checkpoint FW-1
- Ex. Linux IPTables
- 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 apps. 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

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

![Diagram of filter table chains](image-url)
NAT table chains

Prerouting → Forward → Postrouting

Input → Output

Local Processes