Network Security

Firewalls

Firewalls Defined
- Separate outside network and inside network
- Selectively forward packets from one network to another
- Keep the badguy's packets out
- Let the goodguy's packets in
- Let everybody's packets get out

Firewall

Local Network → Firewall → Internet

Proxy Function
- Store
- Filter
- Forward

How To Separate?
- Physically
  - Dual Homed Gateway
- Logically
  - Screen Host Gateway

Dual-Homed Gateway

Choose only one of option 1, 2, or 3
**Screened-Host Gateway**

![Diagram of screened-host gateway]

Choose only one of option 1 or 2

---

**Two Generic Filter Categories**

1. Circuit Filters
   – Work at the Data Link and Network OSI layers
2. Application Gateways
   – Transport and Application layers

---

**Filtering Packets**

- Some get through, some don't
- How do you pick?

Depends on:
- What information is available?
- What you want to protect against?

---

**What Information Is Available at the IP level?**

- Always available
  - Source and Destination Addresses
    - Filter traffic from or to IP addresses or ranges of addresses
  - Packet size
    - Can filter out large packets
  - Port requested
    - Can filter out ICMP or FTP, etc.

---

**Ports to Block**

- finger (79)
- telnet (23)
- rlogin (513)
- ftp (21)
- X Windows (177)
- mail (25)
- http (80)
- ICMP (RFC 792)
  - ping
  - redirect
  - traceroute

---

**Using Port Information**

- If TCP port is requested, a TCP-aware filter can use TCP info
- If ICMP is requested and allowed, can filter by ICMP type, e.g. allow `ping`, but disallow `traceroute`
- What if SSL port is selected?
Circuit Gateways
• State-ful filters
  – Who originated?
  – When?
• Where did the last packet come from/go to (route)?

Info at the Application Layer
• Attachment Format
  – File type
  – Viruses
• Access to text in the payload
  – Porn
  – Sex
  – Smack
  – Weed

Pros and Cons
• Circuit Filters
  – Advantage: Simplicity
  – Disadvantage: Limited scope
• Application Filters
  – Advantage: Wide Scope
  – Disadvantages:
    • Complexity
    • Performance

Firewall Features
• Operating System
• Protocols Handled
• Filter Types
• Logging
• Administration
• Simplicity

Some Commercial Firewalls
1. Altavista (DEC)
2. Borderware (Secure Computing Corp)
3. Cyberguard (Cyberguard Corp)
4. Eagle (Raptor Systems)
5. Firewall-1 (Checkpoint Software)
6. Gauntlet (Trusted Info Systems)
7. ON Guard (ON Technology Corp)

Firewalls Cannot:
• Be perfect.
  – Bad stuff will get in/out
• Protect against insiders
Questions?