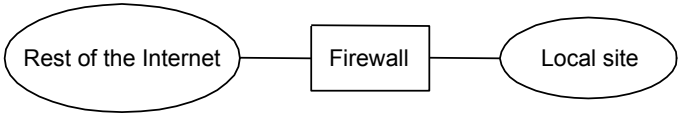
Naptha: A harder but even more insidious attack

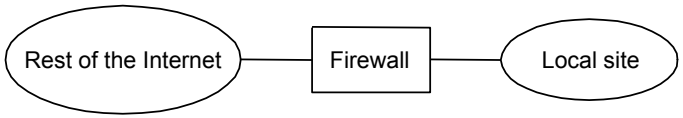
- Another attack based on TCP's fundamentals (not a bug in the OS)
- If you can send arbitrary packets and hear the replies you can create TCP connections in the victim and leave them in any chosen state for arbitrary periods
  - There has to be a return path to the source network address the attacker uses
  - But if the attacker controls any machine on that network there does not have to be a machine at that address
    - Another machine on the network with its interface in promiscuous mode can handle the traffic

Firewalls



- Routing-based
  - Minimum acceptable for good internet citizenship
  - Don't send packets claiming to come from addresses outside the local site
  - Don't accept packets claiming to come from addresses within the local site

Firewalls



- Filter-Based Solution
  - example

    (192.12.13.14, 1234, 128.7.6.5, 80) – incoming packet

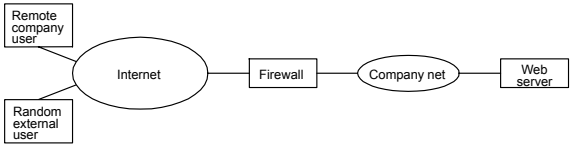
    (*,*, 128.7.6.5, 80) – matching rule
  - default: forward or not forward?
  - how dynamic?

Example Policy

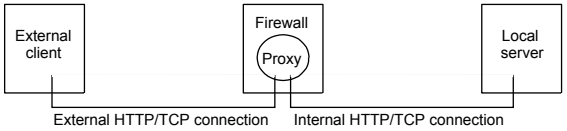
- Default TCP outgoing SYN: allow
  - Default TCP incoming matching outgoing: allow
- Default UDP outgoing: deny
- Default TCP SYN/UDP incoming: deny
- "Deny" is either drop silently or reject with ICMP
- allow TCP incoming to particular ports of particular hosts (webserver port 80, mail server port 25, etc.)
- About 80 rules in all for a modestly complex local/corporate network

Proxy-Based Firewalls

- Problem: complex, data-dependent policy
- Example: web server



- Solution: incoming proxy



- Design: transparent vs. classical
- Limitations: attacks from within

Proxy-based firewalls

- Not shown: a filter policy that says "only traffic to/from the proxy may pass between the local network and the internet
- Proxies may be used for outgoing traffic as well
  - Mail – configuration complexity, logging
  - HTTP – address-based security on web server may require use of an HTTP proxy (e.g. off-campus WSU access to ACM digital library)
  - FTP
  - Telnet
  - Etc.