Firewall

Presentation by:

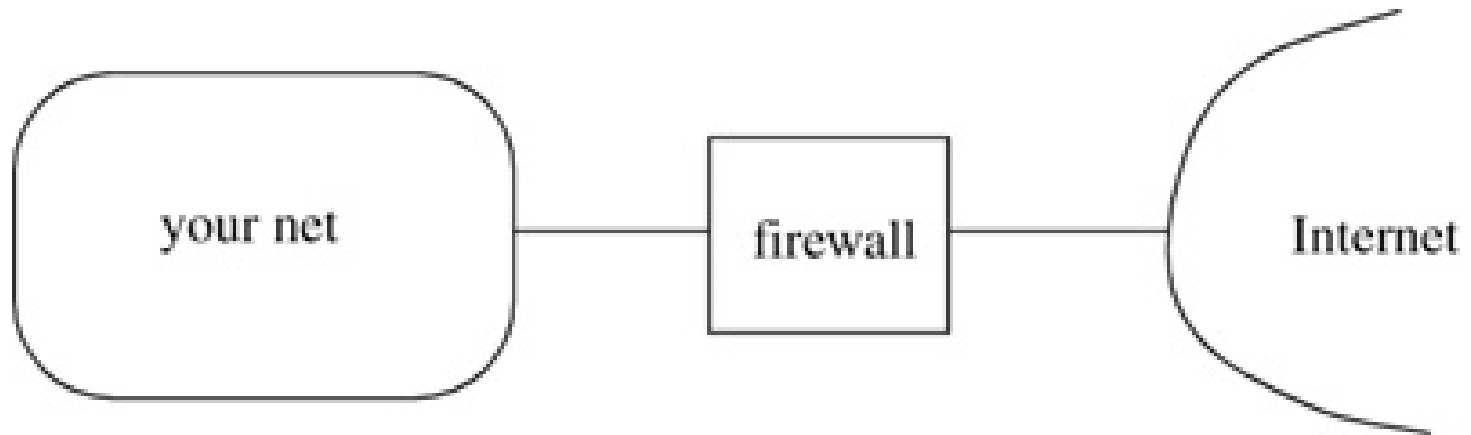V. Balasubramanian

SSN College of Engineering

Firewall

- A firewall is a computer that sits between your internal network and the rest of the network and attempts to prevent bad things from happening (such as internal users sending company secrets outside, or outside people breaking into systems inside)

Example

Other name

- security gateway

Why Firewall is needed?

- internal network are properly secured, meaning that every system in the network has sophisticated authentication, integrity-protected and encrypted communication whenever talking across the network.

- Good passwords

Contd…

- corporate networks are not designed for security, and have survived because they have not been attacked.

- Users want connectivity to the Internet.

- Email, file sharing available to customers located outside your corporate network.

- Internet is a scary place.
- There are spies from unfriendly countries,
- users from competing companies,
- playful undergraduates, press people eager for a juicy scoop, criminals anxious to steal information for profit,

Contd…

- disgruntled ex-employees, and vandals who attempt to compensate for their lack of a social life by annoying others

Example

- A user workstation would only initiate requests to servers on the user's behalf, but most user workstations provide services like remote access to their file systems and configuration databases.

- This makes workstations easier to centrally manage and makes it easier to share files, but every service is a point of attack. Even if the services are properly configured to only serve authorized users, they could be missing bounds checks in their input parsers so that a clever attacker can send an ill-formed request and sometimes get access to things the service
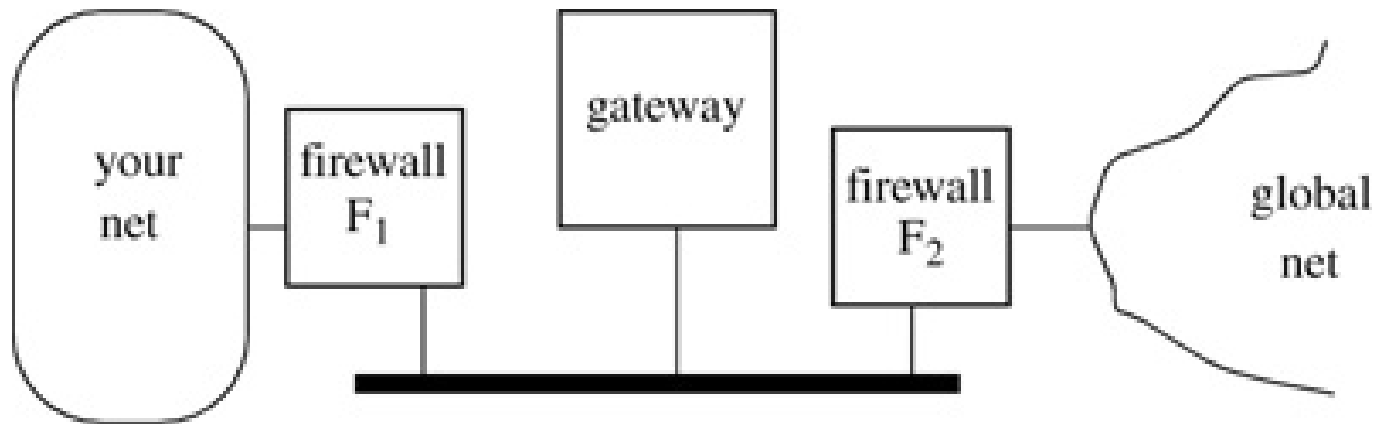
- Firewalls centrally manage access to services in ways that individual systems should.
- They can enforce policies such as systems outside the firewall can't access file services on any systems inside the firewall.
- Firewalls attempt to protect systems inside from attack from outside.

- finger (port 79), which gives information such as who is logged in, or when a specific user last logged in.
- telnet (port 23), which allows someone to log into the system from across a network.

- rlogin (port 513),
- X Windows (port 177),
- ICMP (Internet Control Message Protocol, RFC 792 Ping

Bastion node- Application level gateway

Tunnel