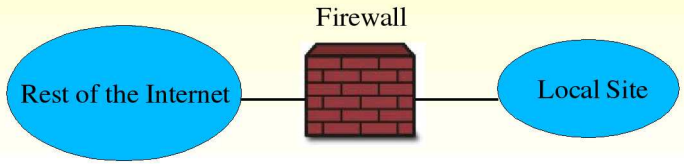
Firewalls

Kameswari Chebrolu
Dept. of Electrical Engineering, IIT Kanpur

Introduction

- Special type of router
- Prevent external users to access certain resources within a site
- Filter out packets based on
  - IP addresses
  - Ports



Need for Firewalls

- Security mechanisms are not widely deployed
  - Implementation is tricky
- Allows system administrator to implement security policy in one center place
  - End-to-end security mechansims require policy to be distributed

Filter-Based Firewalls

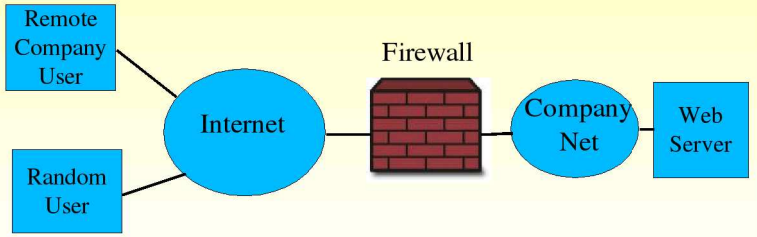
- Configured with a table of ***entries*** that specify what packets will or will not be forwarded
  - Entries denote source, destination IP addresses and port numbers
- Example entry: (*,*,120.89.12.5,80)
  - Drop all packets addressed to port 80 on 120.89.12.5
- One can identify what is allowed or what is disallowed
- Example: (*,*,120.98.1.8,25)
  - Only allow access to port 25 on mail server 120.98.1.8

Proxy

- A process that sits between a client and a server
  - To the client, proxy appears as server
  - To the server, proxy appears as client
- Can implement caching
  - Store frequency accessed content in cache
  - Talks to server only if content not available in cache
- Can implement security as well

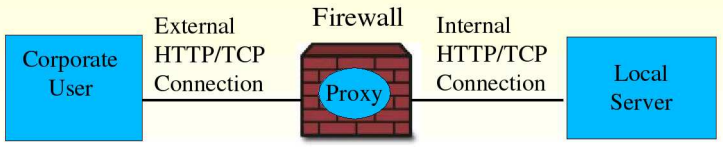
Proxy-Based Firewalls

- Example:
  - Permit access to some of server's web pages to all
  - Restrict access to certain web pages to its corporate users
  - No way to express this as a filter (depends on the URL)



Proxy-Based Firewall Cont...

- Solution: HTTP Proxy
  - Remote users connect to proxy
  - Proxy looks at URL
    - If requested page is allowed to source, proxy acts as in intermediatory
    - If requested page is denied, returns error to sourec



Limitations

- Doesn't protect or isolate internal users
- Impossible to determine who is accessing the network
- Need to move acces protection from the periphery of the network to hosts that initiate access

Summary

- Firewall is nothing but a specialized router that filters packets
- Two types of firewalls: Filter-based, Proxy-based
- Cannot really tell who is accessing the network