Firewall: Proxying and Architectures

CSC 154

slides adapted from Peng Liu, College of IST, Penn State U

Roadmap

- Proxying Firewall
- Firewall Architectures
- Stateful Packet Filtering

Proxy Firewall

- Between users and the internet services
  - Take user requests and forward
  - No direct traffic between networks
  - Logging
  - Access control
  - Hide true network addresses of the internet services
  - Multiple level of security

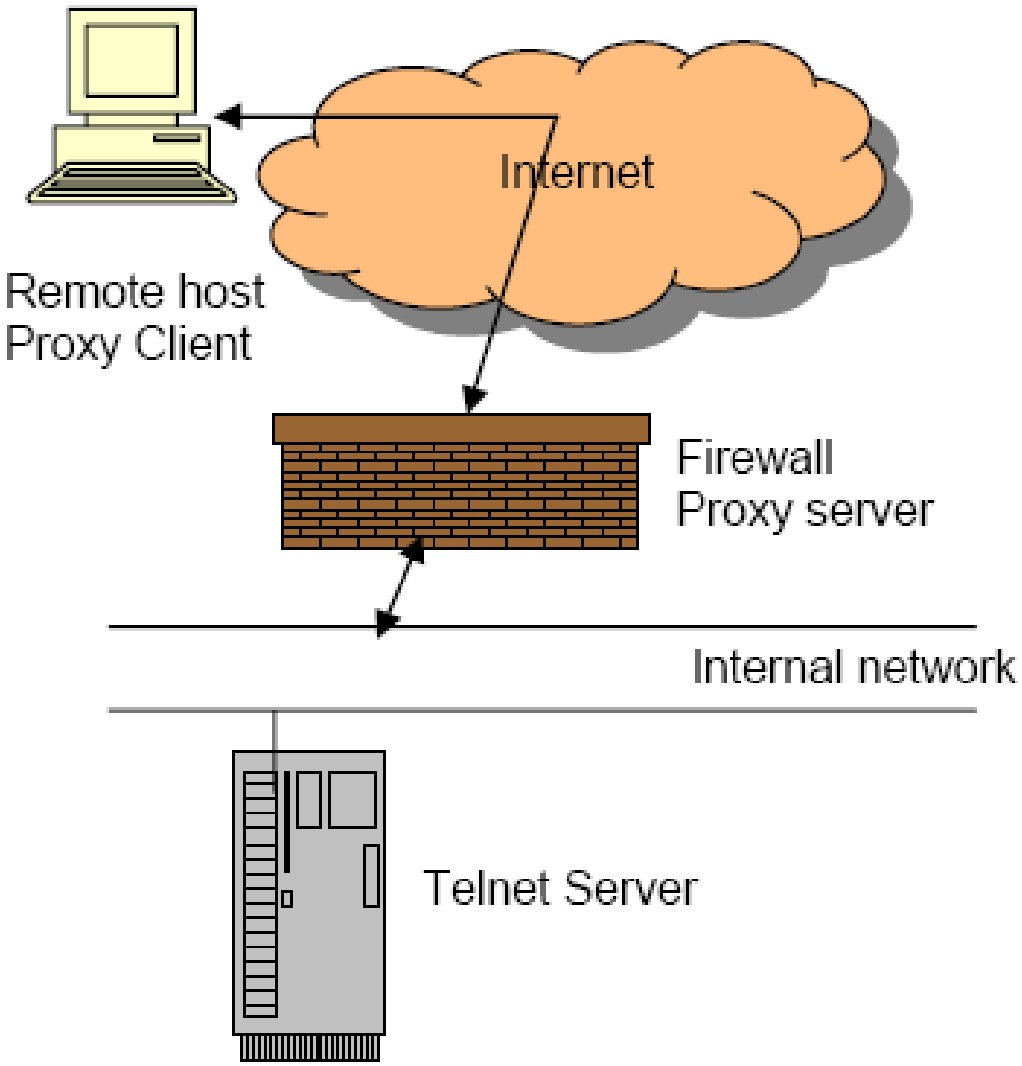
Proxy Firewalls vs. Packet Filtering Firewalls

- Packet filtering firewalls are filters, while proxy firewalls are **decoys**
- Packet filtering firewalls **never** look into packet payload or content, but many proxy firewalls check content
- Packet filtering firewalls are always made of hardware, but many proxy firewalls are **software**
- Packet filtering firewalls work at IP layer, while proxy firewalls work at TCP or application layers

Two Types of Proxy Firewalls

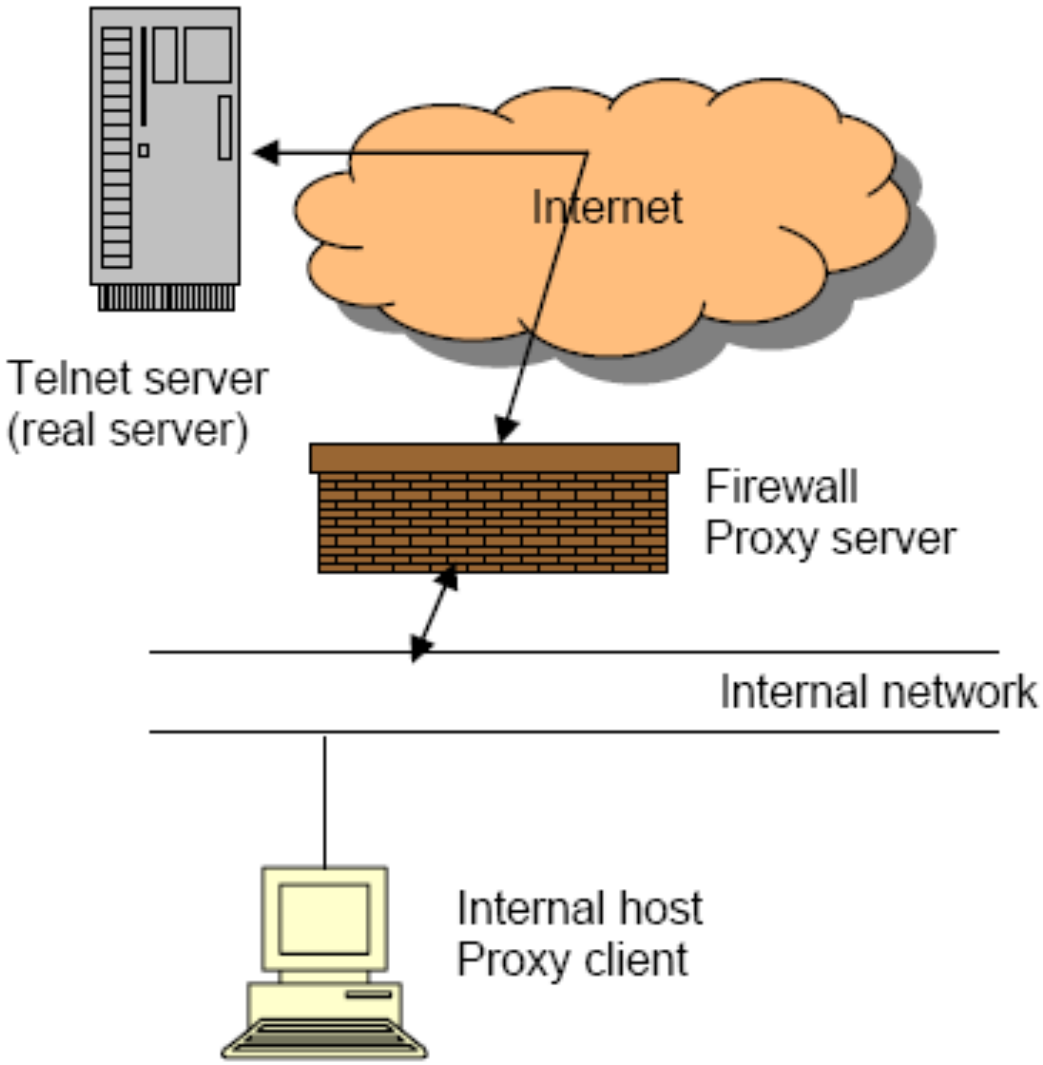
- Application layer proxy firewalls
  - Protect servers
  - Protect clients
  - Need one **separate** proxy firewall software for each Internet service, e.g., HTTP, Telnet, FTP
- TCP layer proxy firewalls
  - One proxy firewall can protect several Internet services

Use a proxy firewall to protect servers



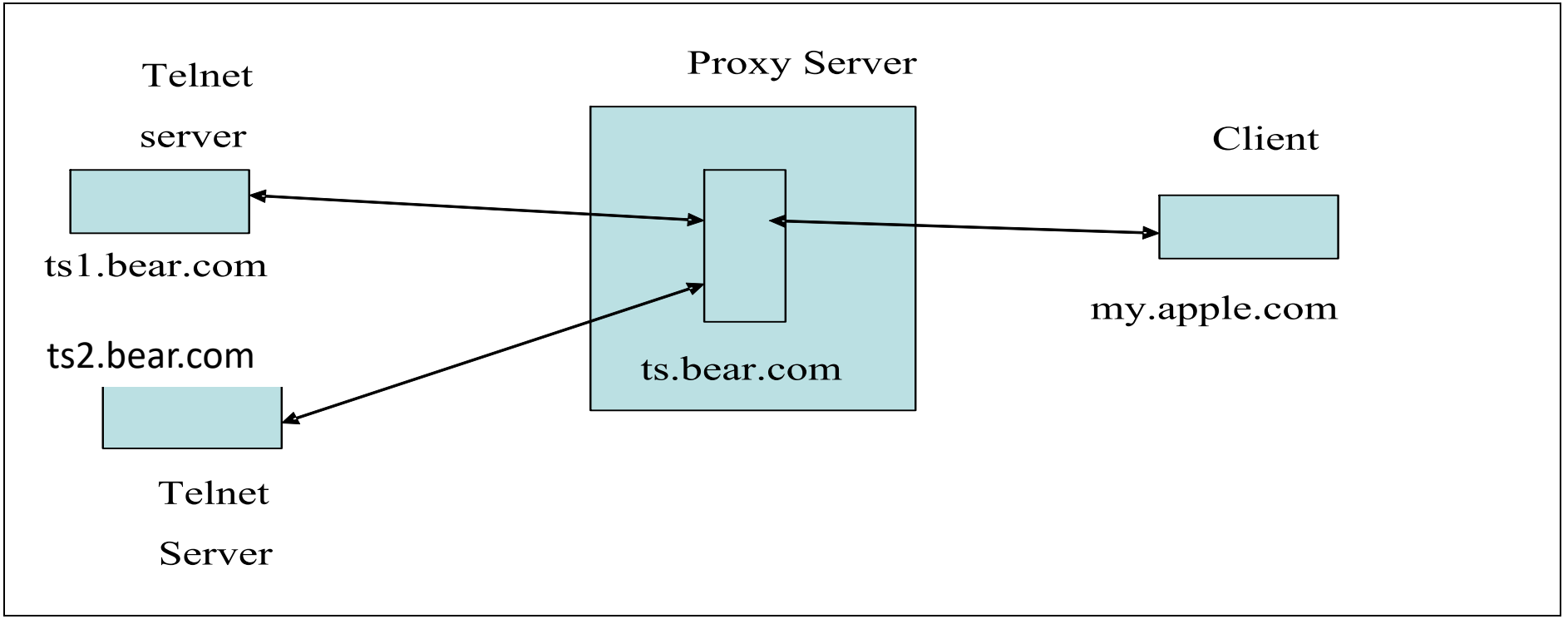
- The proxy firewall gives the remote client the illusion that he is the real Telnet server.

Use a proxy firewall to protect clients



- The proxy firewall gives the remote server the illusion that he is the real Telnet client.

Case Study (1a): risk



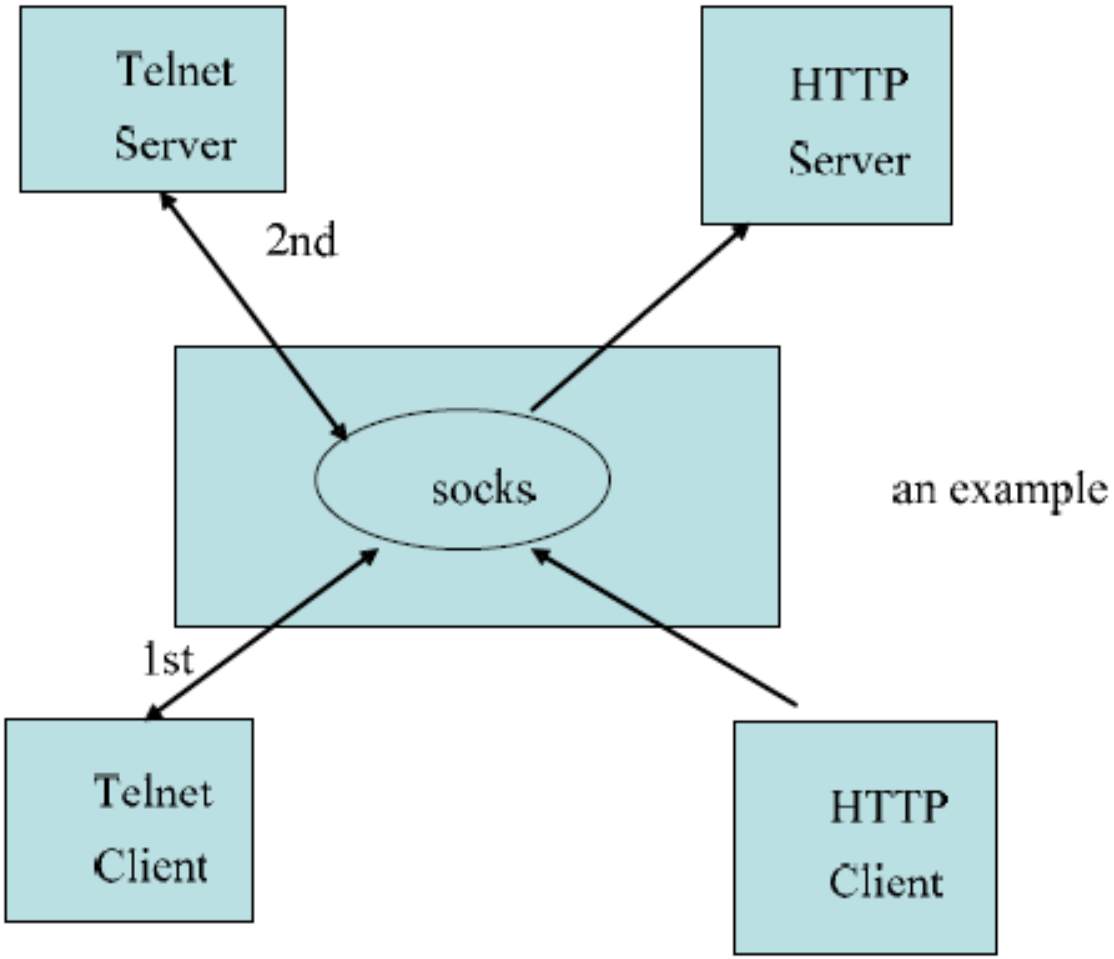
- If the proxy server does not exist or is replaced by a packet filtering firewall, the external client, if malicious, would be able to know the real IP address of the internal Telnet server.
  - This is viewed a major security risk

Case Study (1b): how to get rid of the risk

- Answer: deploy the proxy server
  - The external client would believe that the IP address of this proxy server (decoy) is the IP of the real server

- Issue: the external user will type:
  - % telnet ts.bear.com
  - But how could the proxy know which server the client wants to connect to?
  - Answer: the telnet client software could be slightly modified to ask the user to type in the name of the real server, e.g., ts1.bear.com, after the connection with the proxy is established.
    - An outsider hacker won't have this modified client software installed on this laptop

TCP layer proxy firewalls



One SOCKS proxy firewall can serve multiple Internet services.

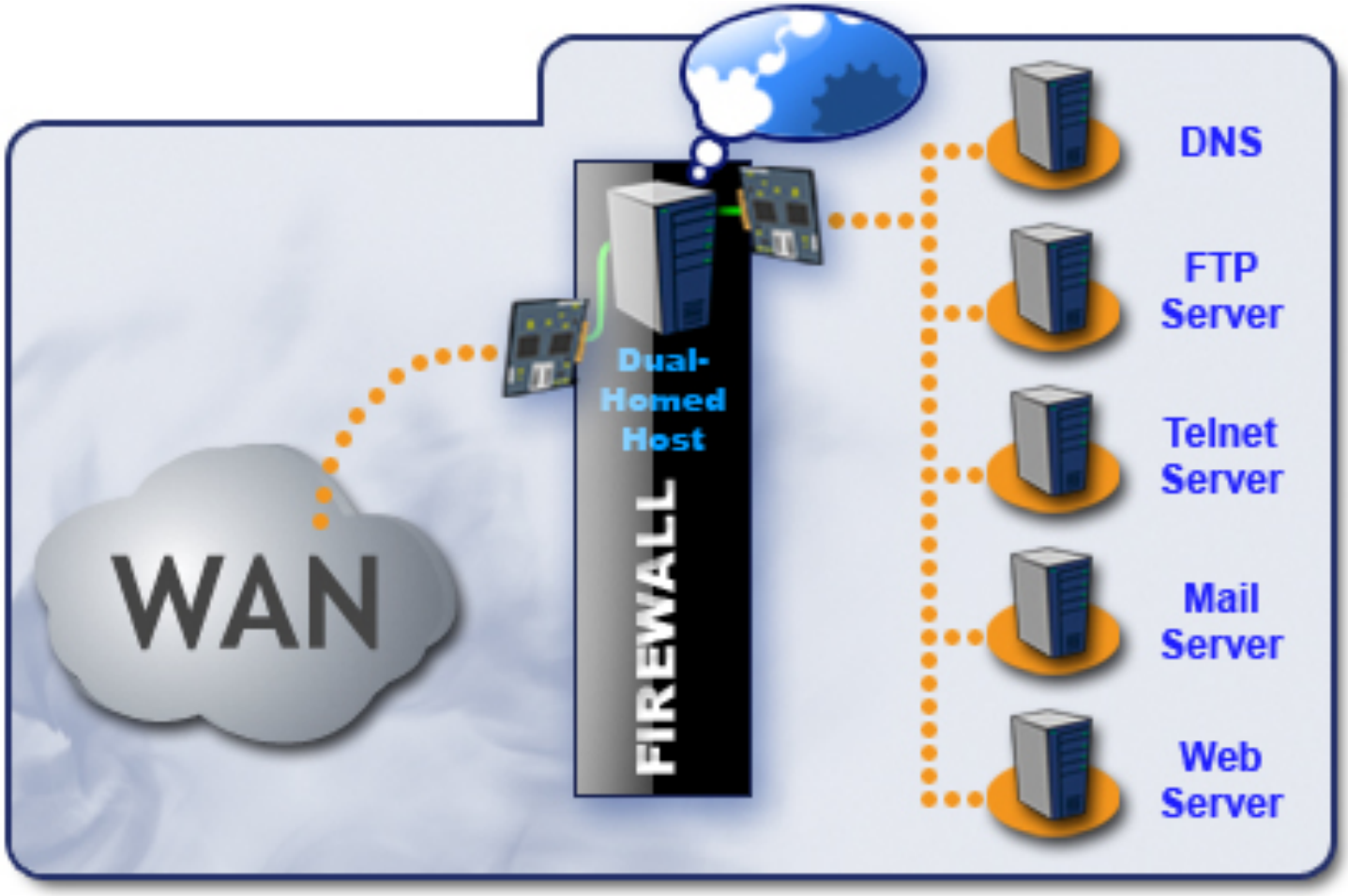
For each service instance between a client and a server, SOCKS proxy will establish **TWO TCP connections**.

SOCKS maintains dozens of TCP connections concurrently.

Firewall Architectures

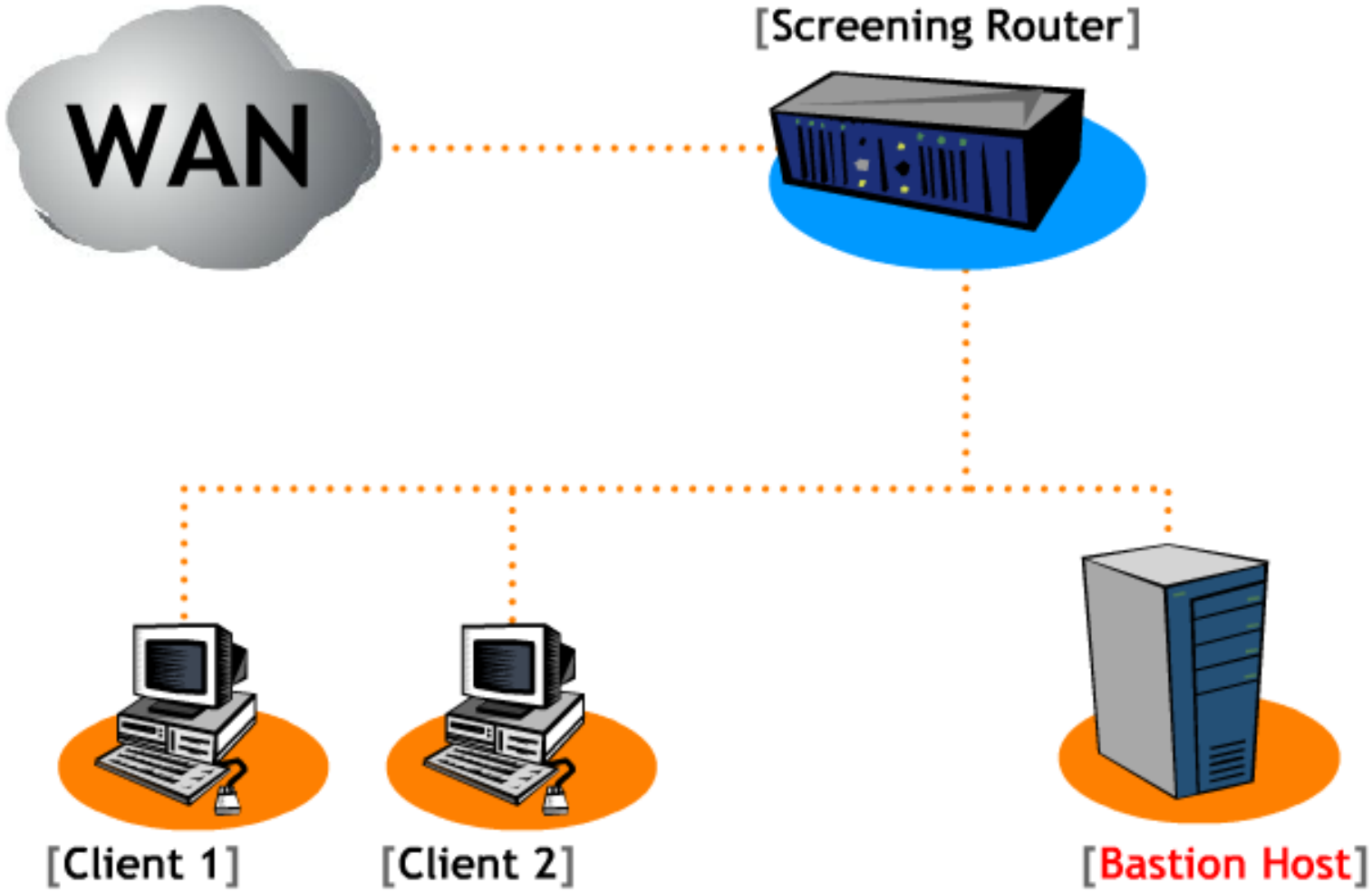
- Dual-Homed Host Firewall
  - Dual-homed host
    - between the internal network and the external network
    - at least two network interface cards (NIC)
    - either an application-layer or a transport-layer proxy
- Screened Host Firewall
  - screening router + bastion host (a proxy)
  - Bastion host is the only system in internal network that have direct connections to/from
- Screened Subnet Firewall
  - screening router + peripheral network + dual-homed host + internal network

Dual-Homed Host Firewall



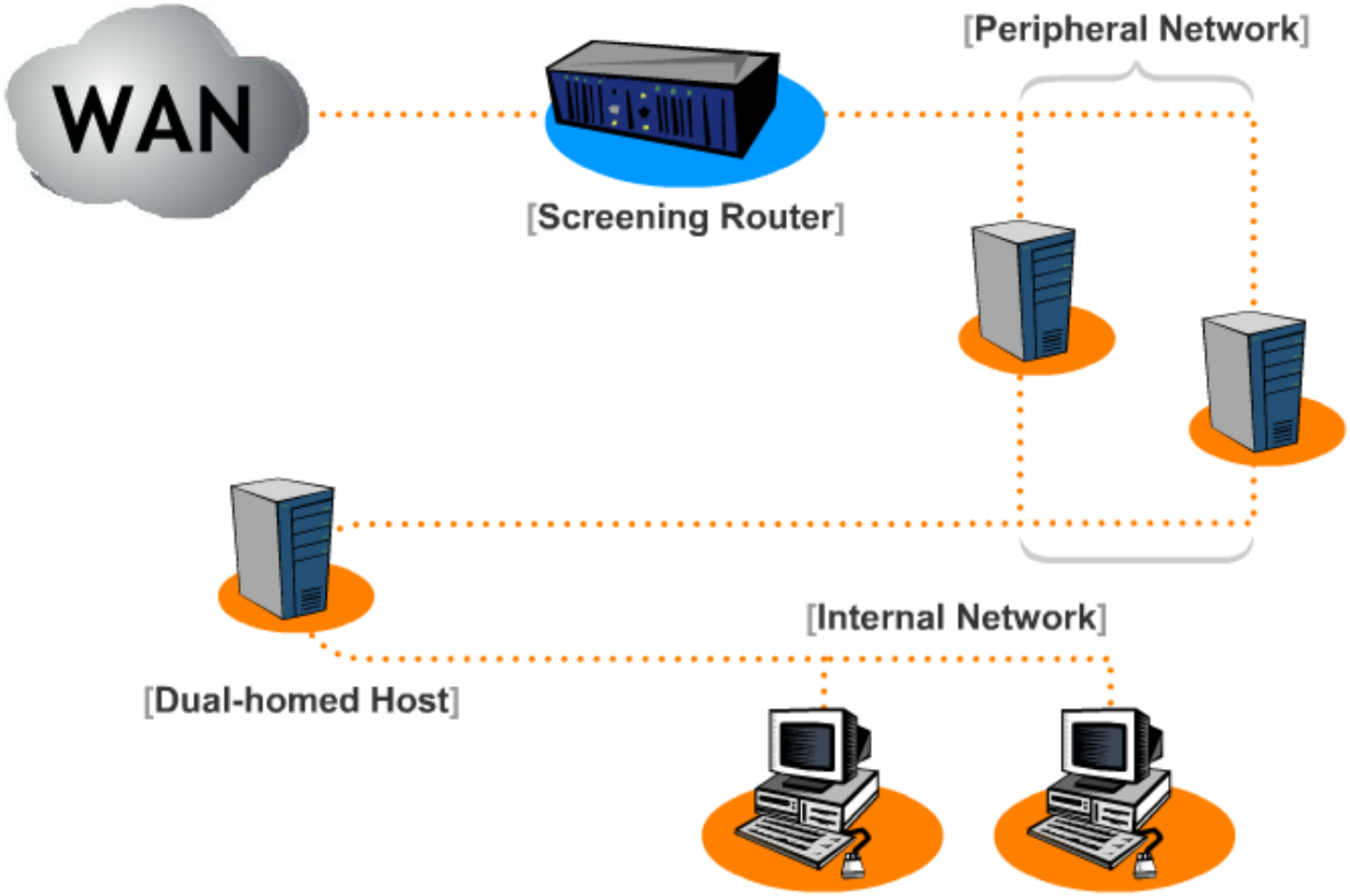
Picture from College of IST, Penn State U

Screened Host Firewall



Picture from College of IST, Penn State U

Screened Subnet Firewall



Picture from College of IST, Penn State U

Questions

- Peripheral network
  - Also called what in real world?

- Why do we need two firewalls?
  - Multiple levels of security
  - Proxy with higher level of security

Principles of the two-layer architecture

- Principle 1: run Internet services within the DMZ so that the internal machines are isolated from the Internet

- Principle 2: when an internal machine (client or server) wants to communicate with a remote machine in the Internet (i.e., the jungle), use a **decoy (proxy server)!**

Stateful Packet Filtering

- For each session or connection, stateful packet filtering maintains a session state table with each entry capturing such “state” information of the session as:
  - How long the connection has lasted so far?
  - How many packets are already seen within the connection?

- The **session state table** contains:
  - Source and dest addresses;
  - Source and dest port numbers;
  - TCP sequence numbers
  - Additional flags
  - The time when a connection was established

Example

- If the firewall can remember the packets, the firewall can pass only the incoming UDP packets that:
  - have been directed to the hosts and ports that sent the outbound packets;

    and
  - are from the hosts and ports that the outbound packets were sent to.

Example Explanation

- The implicit policy rule is:
  - a UDP session can only start from inside;
  - UDP packets can go out but only the corresponding UDP reply packets can come in.
  - This policy rule cannot be enforced without stateful packet filtering

- In the example, the firewall determines whether an incoming packet is a reply packet or not as follows:
  - If a packet is a reply packet, its dest IP address and dest port number must have appeared in a previous UDP packet going out of the firewall as source IP address and source port number;

    and
  - its source IP address and source port number must have appeared in a previous UDP packet going out of the firewall as dest IP address and dest port number

Example

- Packets are dropped if the connection has lasted too long.

Example Explanation

- The rational:
  - a connection lasting too long can be a malicious connection
- The implicit policy rule:
  - any connection lasting longer than the specific threshold should be blocked
  - This policy rule cannot be enforced by static packet filtering
    - stateful packet filtering remembers the time when each connection was started