DRONACHARYA
College of Engineering

**Computer Science & Engineering**

# Data Communication and Computer Networks

( MTCSE-101-A )

# Firewalls

# What is a Firewall?

- A **choke point** of control and monitoring
- Interconnects networks with differing trust
- Imposes restrictions on network services
  - only authorized traffic is allowed
- Auditing and controlling access
  - can implement alarms for abnormal behavior
- Itself immune to penetration
- Provides **perimeter defence**

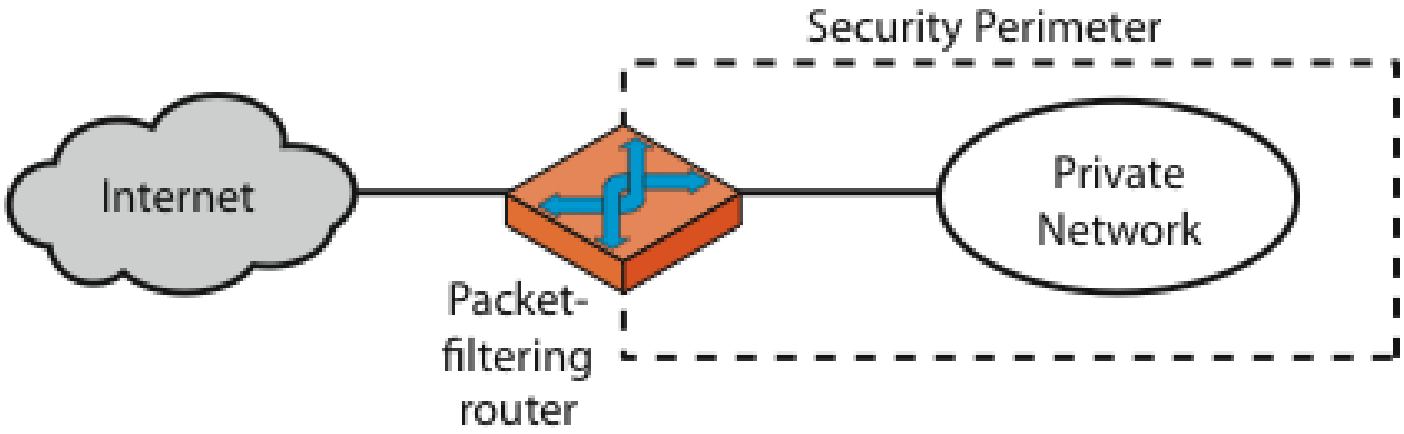
# Classification of Firewall

Characterized by protocol level it controls in

- Packet filtering
- Circuit gateways
- Application gateways

- Combination of above is dynamic packet filter

# Firewalls – Packet Filters




(a) Packet-filtering router

# Firewalls – Packet Filters

- Simplest of components
- Uses transport-layer information only
  - IP Source Address, Destination Address
  - Protocol/Next Header (TCP, UDP, ICMP, etc)
  - TCP or UDP source & destination ports
  - TCP Flags (SYN, ACK, FIN, RST, PSH, etc)
  - ICMP message type
- Examples
  - DNS uses port 53
    - No incoming port 53 packets except known trusted servers

# Usage of Packet Filters

- Filtering with incoming or outgoing interfaces
  - E.g., Ingress filtering of spoofed IP addresses
  - Egress filtering
- Permits or denies certain services
  - Requires intimate knowledge of TCP and UDP port utilization on a number of operating systems

# How to Configure a Packet Filter

- Start with a security policy
- Specify allowable packets in terms of logical expressions on packet fields
- Rewrite expressions in syntax supported by your vendor
- General rules - least privilege
  - All that is not expressly permitted is prohibited
  - If you do not need it, eliminate it

Every ruleset is followed by an implicit rule reading like this.

| action | ourhost | port | theirhost | port | comment |
|---|---|---|---|---|---|
| block | * | * | * | * | *default* |

Example 1:

Suppose we want to allow inbound mail (SMTP, port 25) but only to our gateway machine. Also suppose that mail from some particular site SPIGOT is to be blocked.

# Solution 1:

| action | ourhost | port | theirhost | port | comment |
|---|---|---|---|---|---|
| block | * | * | SPIGOT | * | *we don't trust these people* |
| allow | OUR-GW | 25 | * | * | *connection to our SMTP port* |

# Example 2:

Now suppose that we want to implement the policy "any inside host can send mail to the outside".

# Solution 2:

| action | ourhost | port | theirhost | port | comment |
|---|---|---|---|---|---|
| allow | * | * | * | 25 | *connection to their SMTP port* |

This solution allows calls to come from any port on an inside machine, and will direct them to port 25 on the outside. Simple enough…

So why is it wrong?

- Our defined restriction is based solely on the outside host's port number, which we have no way of controlling.
- Now an enemy can access any internal machines and port by originating his call from port 25 on the outside machine.

What can be a better solution ?

| action | src | port | dest | port | flags | comment |
|---|---|---|---|---|---|---|
| allow | {our hosts} | * | * | 25 | | *our packets to their SMTP port* |
| allow | * | 25 | * | * | ACK | *their replies* |

- The ACK signifies that the packet is part of an ongoing conversation
- Packets without the ACK are connection establishment messages, which we are only permitting from internal hosts

# Security & Performance of Packet Filters

- IP address spoofing
  - Fake source address to be trusted
  - Add filters on router to block
- Tiny fragment attacks
  - Split TCP header info over several tiny packets
  - Either discard or reassemble before check
- Degradation depends on number of rules applied at any point
- Order rules so that most common traffic is dealt with first
- Correctness is more important than speed

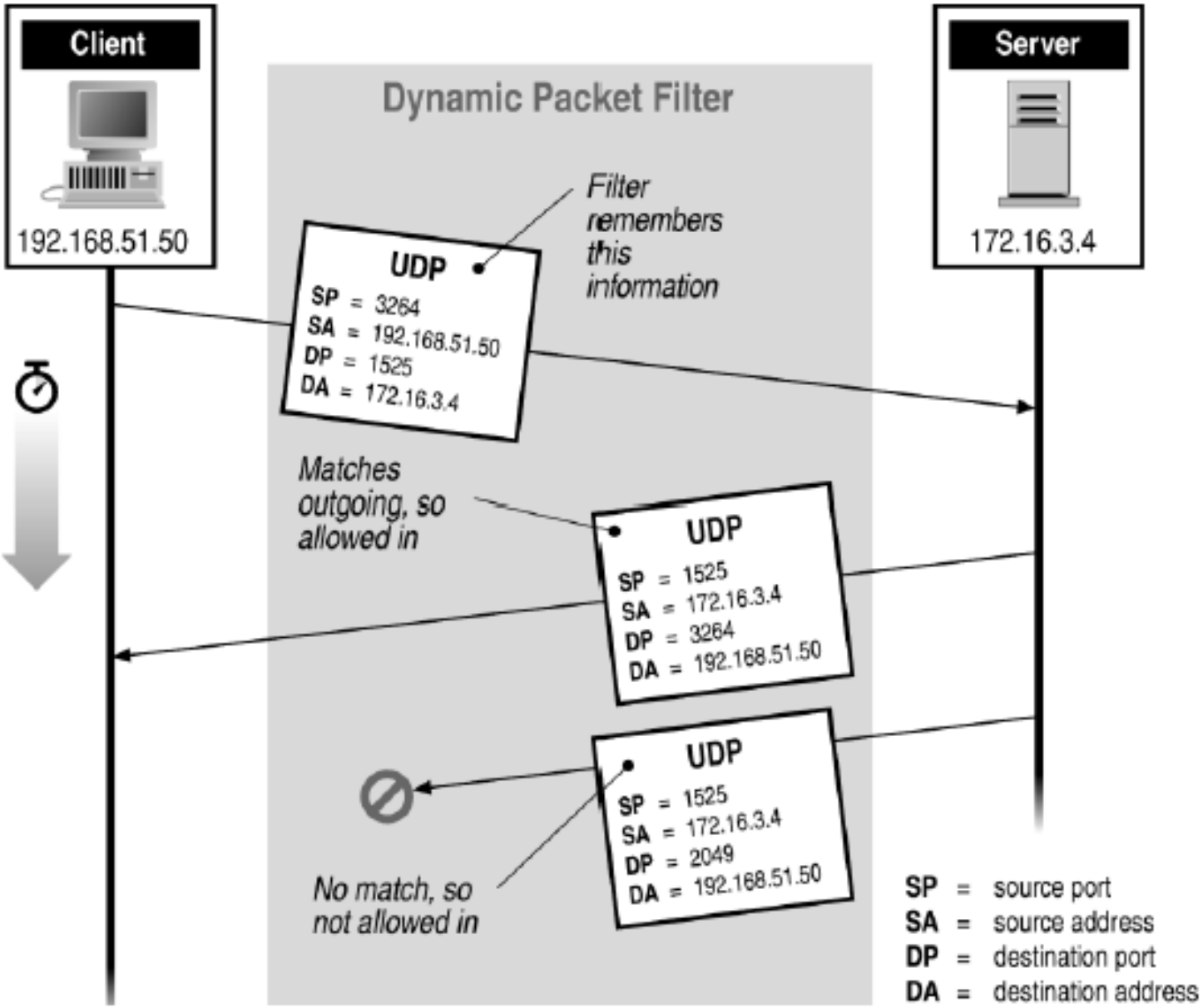
# Port Numbering

- TCP connection
  - Server port is number less than 1024
  - Client port is number between 1024 and 16383
- Permanent assignment
  - Ports <1024 assigned permanently
    - 20,21 for FTP 23 for Telnet
    - 25 for server SMTP 80 for HTTP
- Variable use
  - Ports >1024 must be available for client to make any connection
  - This presents a limitation for stateless packet filtering
    - If client wants to use port 2048, firewall must allow *incoming* traffic on this port
  - Better: stateful filtering knows outgoing requests

# Firewalls – Stateful Packet Filters

- Traditional packet filters do not examine higher layer context
  - ie matching return packets with outgoing flow
- Stateful packet filters address this need
- They examine each IP packet in context
  - Keep track of client-server sessions
  - Check each packet validly belongs to one
- Hence are better able to detect bogus packets out of context

# Stateful Filtering



# Firewall Outlines

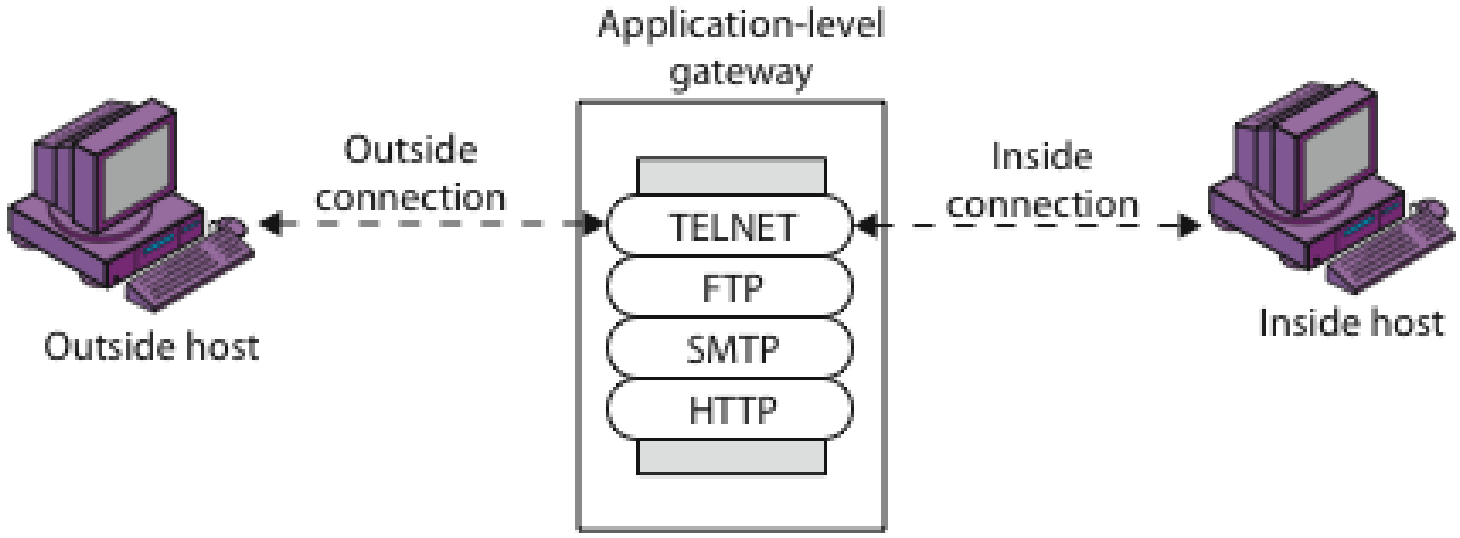
- Packet filtering
- Application gateways
- Circuit gateways

- Combination of above is dynamic packet filter

# Firewall Gateways

- Firewall runs set of proxy programs
  - Proxies filter incoming, outgoing packets
  - All incoming traffic directed to firewall
  - All outgoing traffic appears to come from firewall
- Policy embedded in proxy programs
- Two kinds of proxies
  - Application-level gateways/proxies
    - Tailored to http, ftp, smtp, etc.
  - Circuit-level gateways/proxies
    - Working on TCP level

# Firewalls - Application Level Gateway (or Proxy)

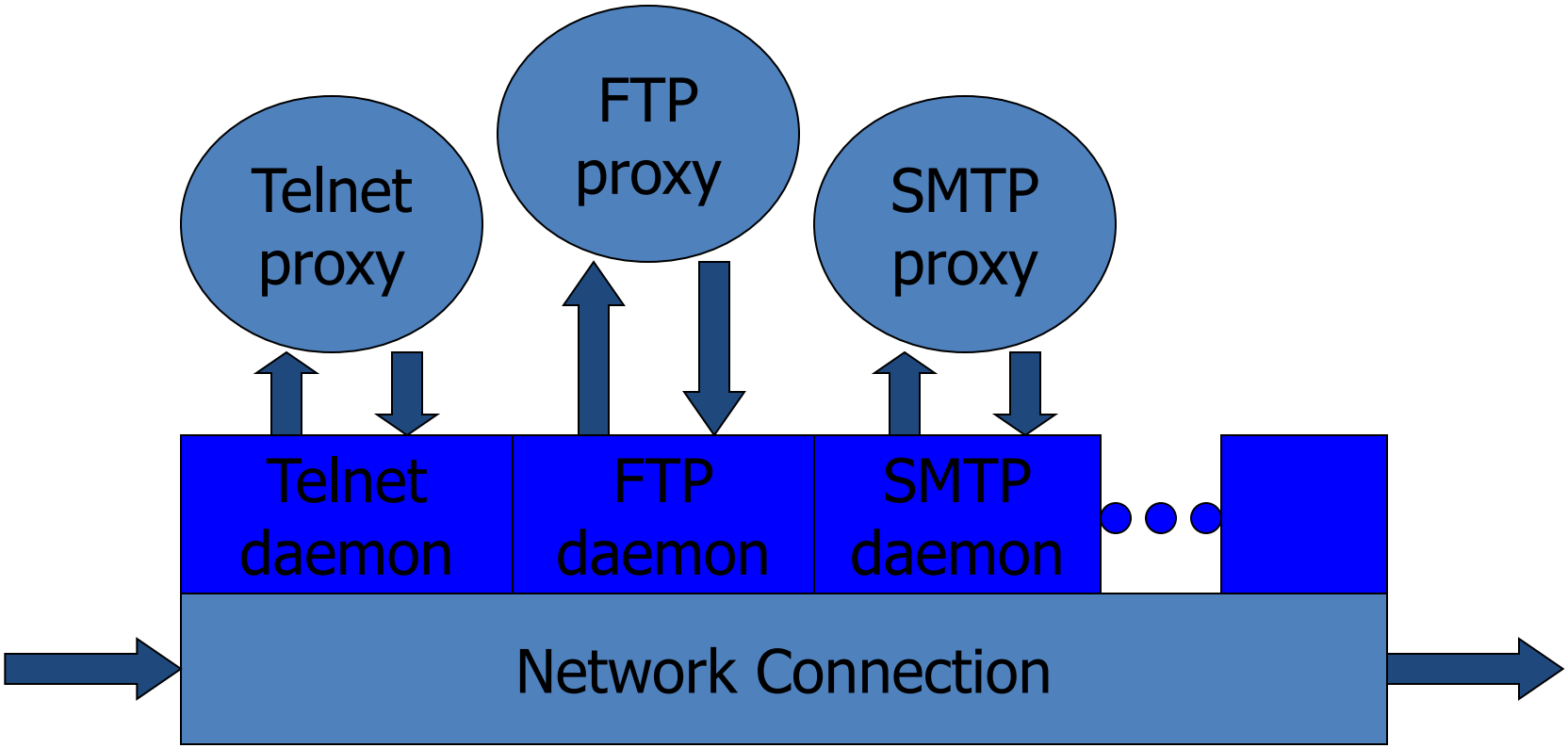



(b) Application-level gateway

# Application-Level Filtering

- Has full access to protocol
  - user requests service from proxy
  - proxy validates request as legal
  - then actions request and returns result to user
- Need separate proxies for each service
  - E.g., SMTP (E-Mail)
  - NNTP (Net news)
  - DNS (Domain Name System)
  - NTP (Network Time Protocol)
  - custom services generally not supported

# App-level Firewall Architecture




Daemon spawns proxy when communication detected …

# Enforce policy for specific protocols

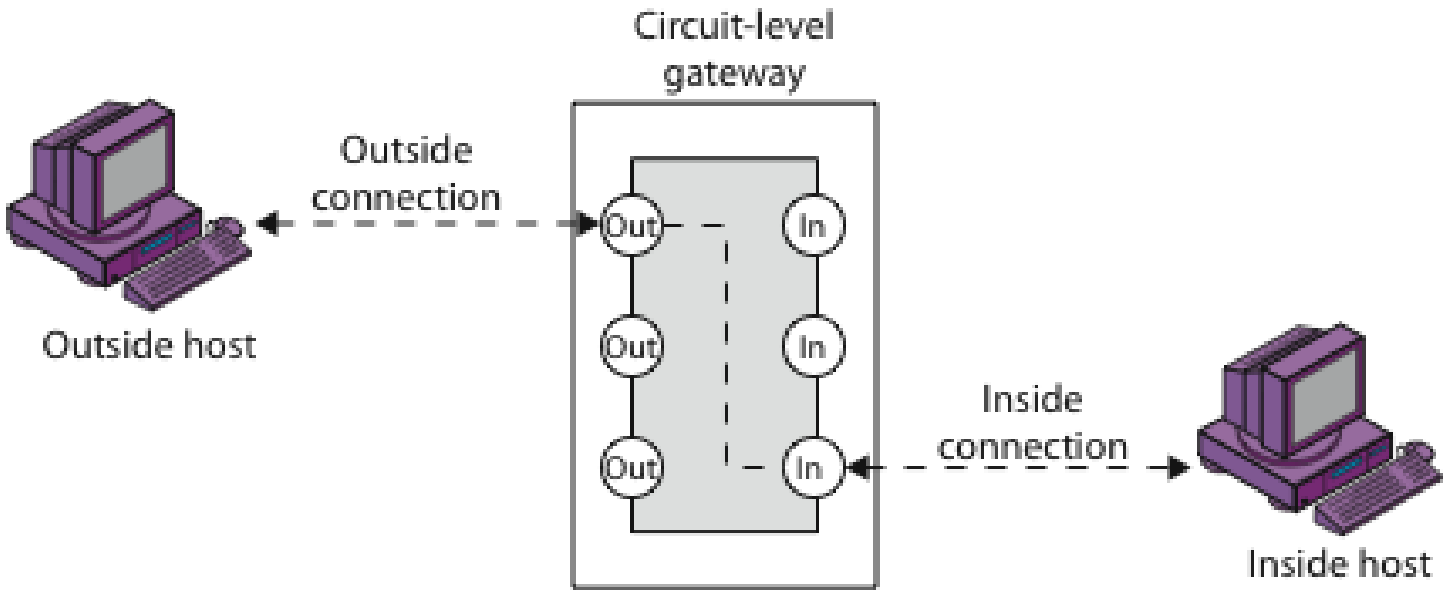
- E.g., Virus scanning for SMTP
  - Need to understand MIME, encoding, Zip archives

# Firewall Outlines

- Packet filtering
- Application gateways
- Circuit gateways

- Combination of above is dynamic packet filter

# Firewalls - Circuit Level Gateway




(c) Circuit-level gateway

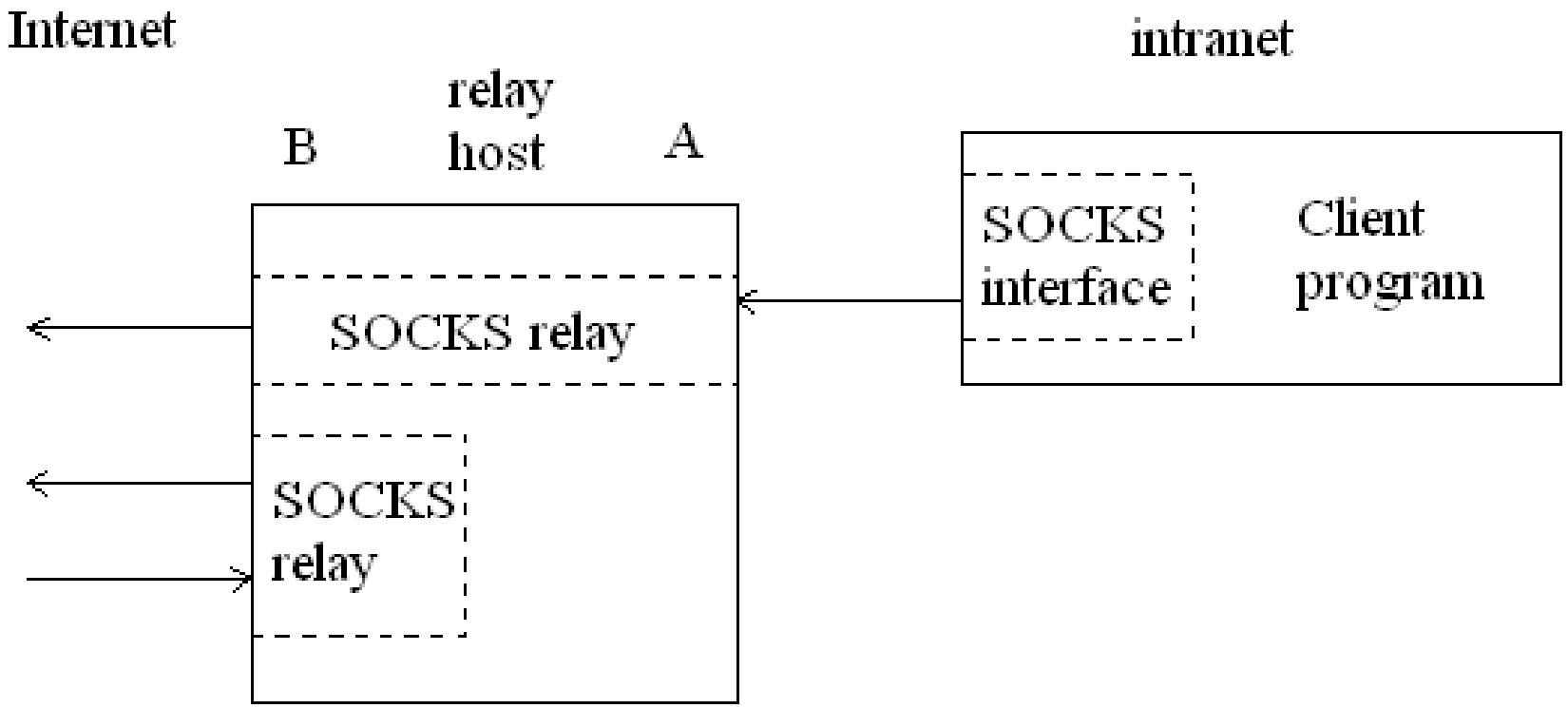
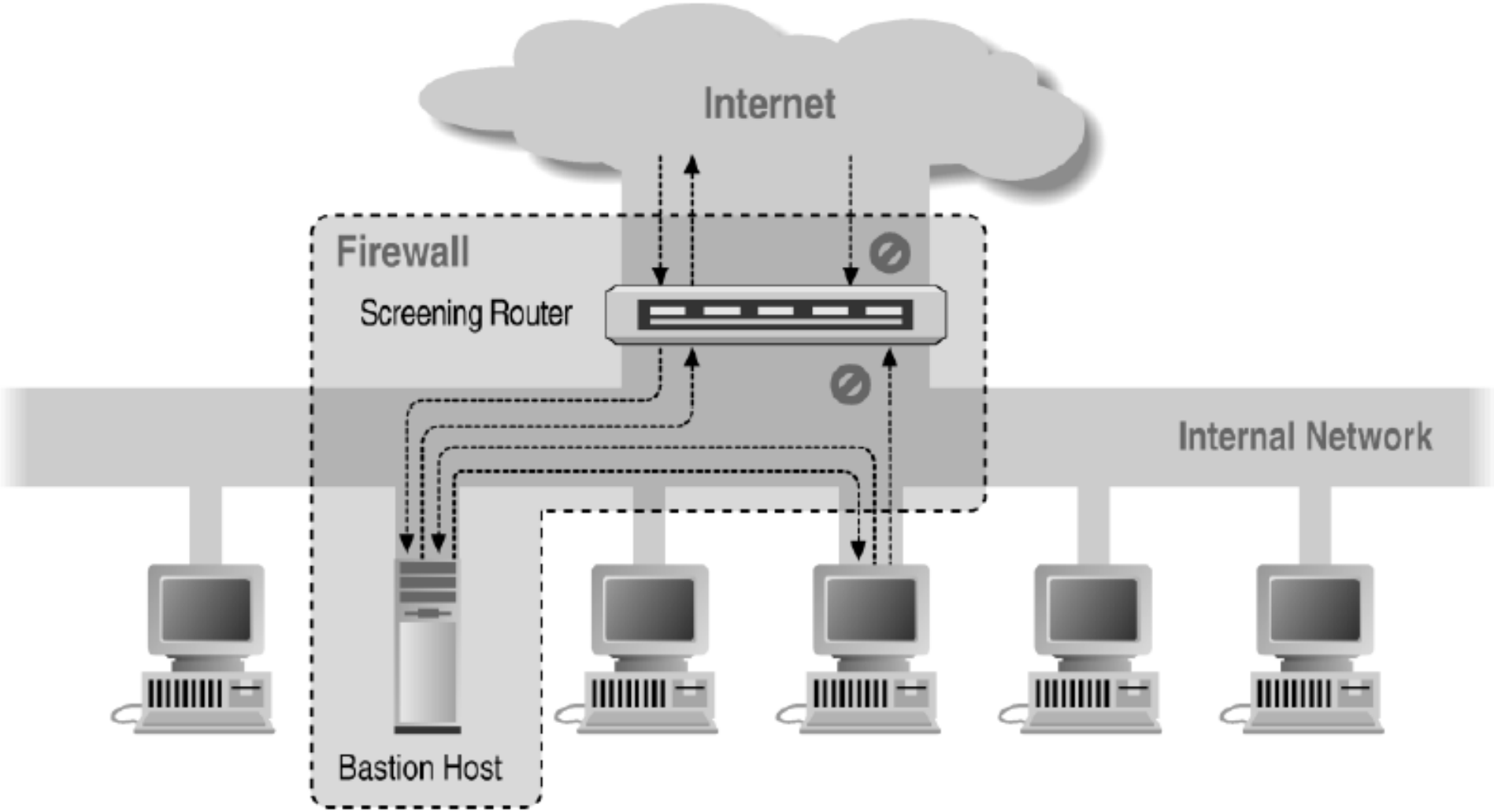



**Figure 9.7:** A typical SOCKS connection through interface A, and rogue connection through the external interface, B.

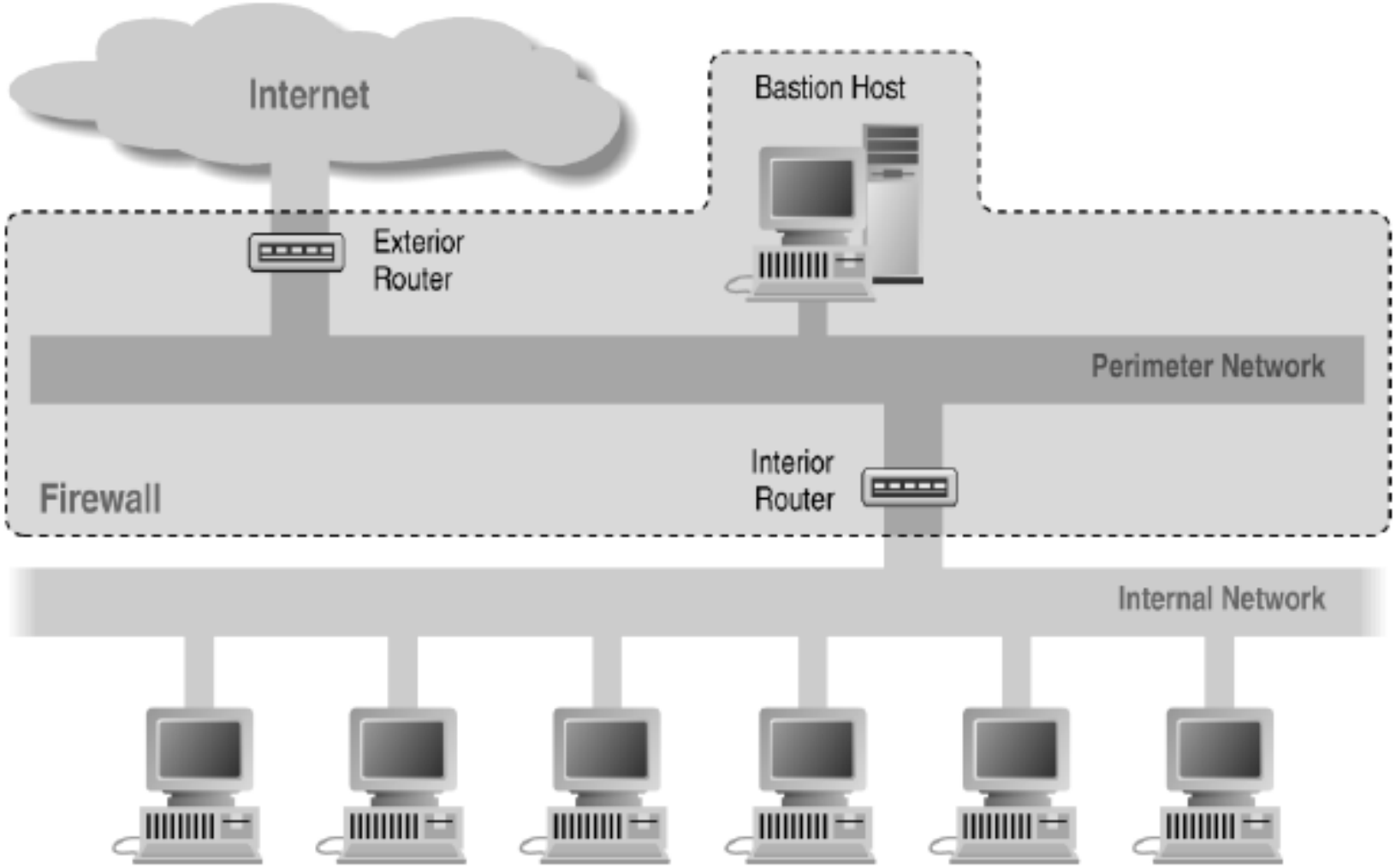
# Bastion Host

- Highly secure host system
- Potentially exposed to "hostile" elements
- Hence is secured to withstand this
  - Disable all non-required services; keep it simple
- Trusted to enforce trusted separation between network connections
- Runs circuit / application level gateways
  - Install/modify services you want
- Or provides externally accessible services

# Screened Host Architecture



# Screened Subnet Using Two Routers



# Firewalls Aren't Perfect?

- Useless against attacks from the inside
  - Evildoer exists on inside
  - Malicious code is executed on an internal machine
- Organizations with greater insider threat
  - Banks and Military
- Protection must exist at each layer
  - Assess risks of threats at every layer
- Cannot protect against transfer of all virus infected programs or files
  - because of huge range of O/S & file types

# Quiz

- In this question, we explore some applications and limitations of a stateless packet filtering firewall. For each of the question, briefly explain how the firewall should be configured to defend against the attack, or why the firewall cannot defend against the attack.
  - Can the firewall prevent a SYN flood denial-of-service attack from the external network?
  - Can the firewall prevent a Smurf attack from the external network? Recall that as we discussed in the class before, the Smurf attack uses the broadcast IP address of the subnet.

- Can the firewall prevent external users from exploiting a security bug in a CGI script on an internal web server (the web server is serving requests from the Internet)?
- Can the firewall prevent an online password dictionary attack from the external network on the telnet port of an internal machine?
- Can the firewall prevent a user on the external network from opening a window on an X server in the internal network? Recall that by default an X server listens for connections on port 6000
- Can the firewall block a virus embedded in an incoming email?
- Can the firewall be used to block users on the internal network from browsing a specific external IP address?