What is a Firewall?

A firewall…

- Can be software or hardware or combination
- Prevents Internet dangers spreading to internal network

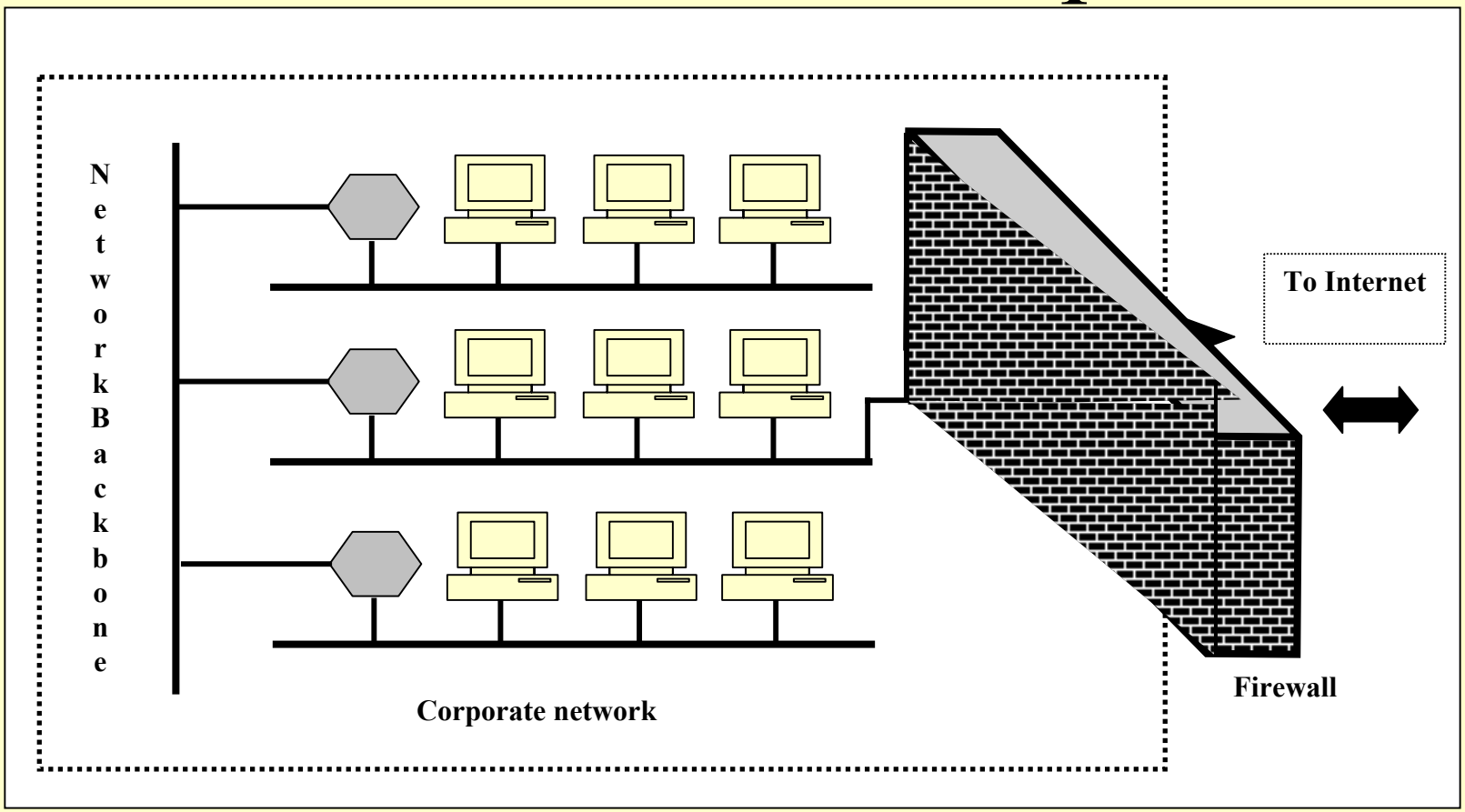
Examples of firewalls:

- Cisco routers
- ipfilter (BSD)
- ipchains/iptables (Linux)
- Windows 2000/NT (limited)

Firewall

- Special type of router
- Controls transmission between internal and external networks
- Decides what to allow/disallow

Firewall Concept



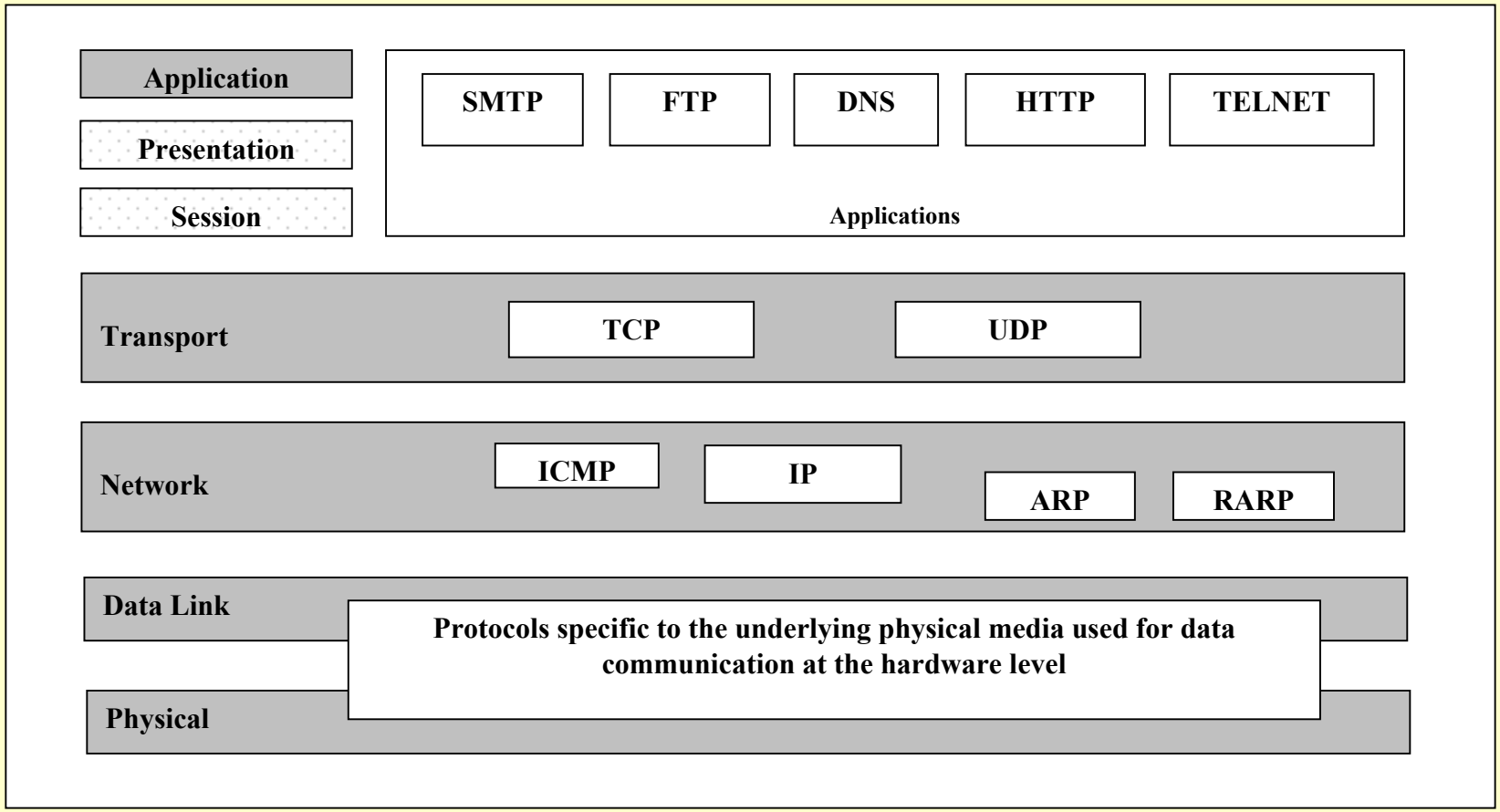
TCP/IP Protocols

- Contains Five Layers
- Top three layers contains many protocols
- Actual transmission at the physical layer
- Reliable transport layer communication
- Establishes a logical connection between the communicating hosts
- Socket-to-socket communication (Socket = Port + IP address)

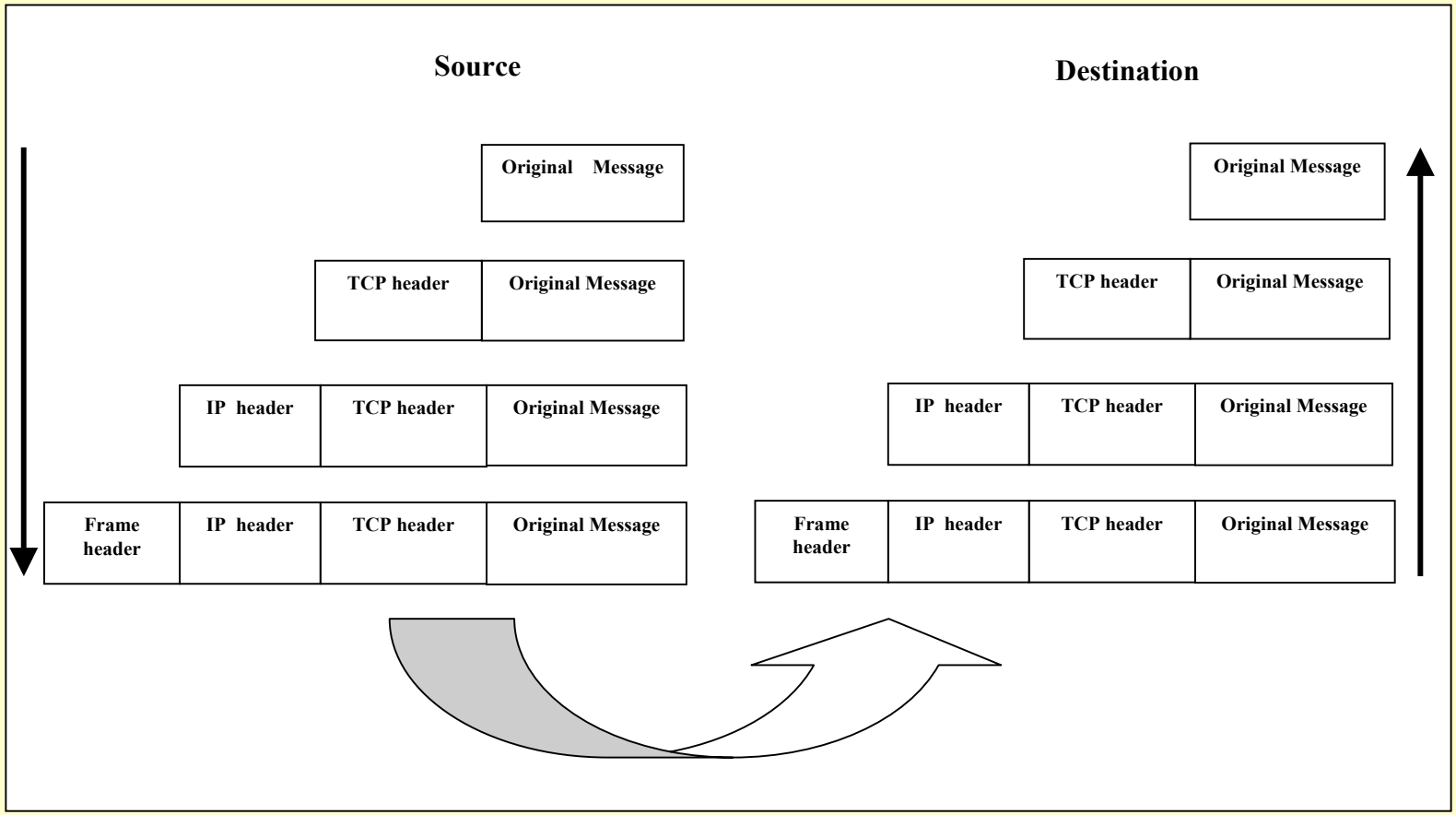
The TCP Protocol

- **TCP is *reliable* because it guarantees that the destination receives:**
  - application data in the order it was sent
  - all application data
  - no duplicates of any application data
- **TCP is *bi-directional***
  - Server can reply to client over the same connection

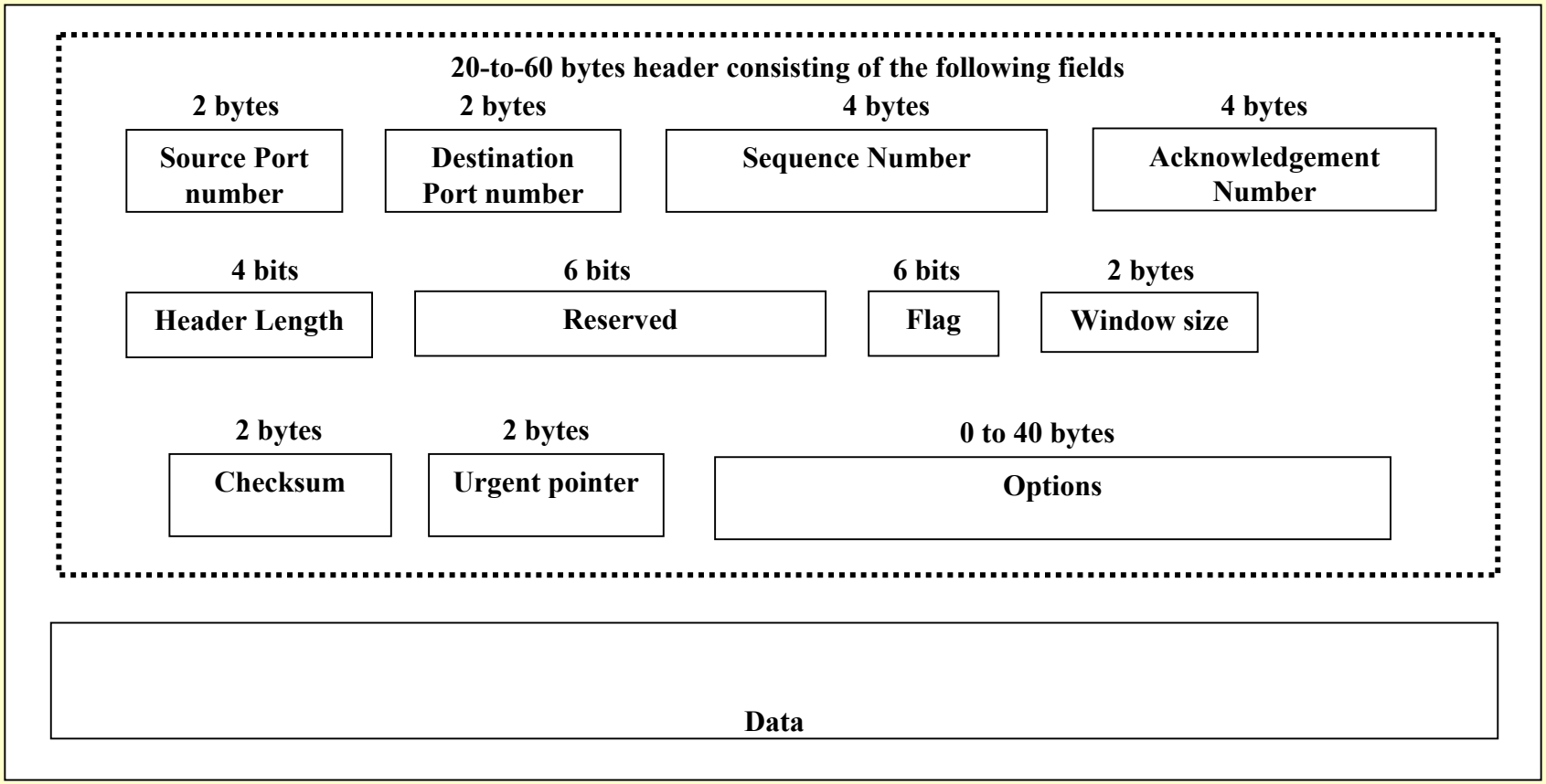
TCP/IP Layers



Message Transfer using TCP/IP



TCP Segment Format



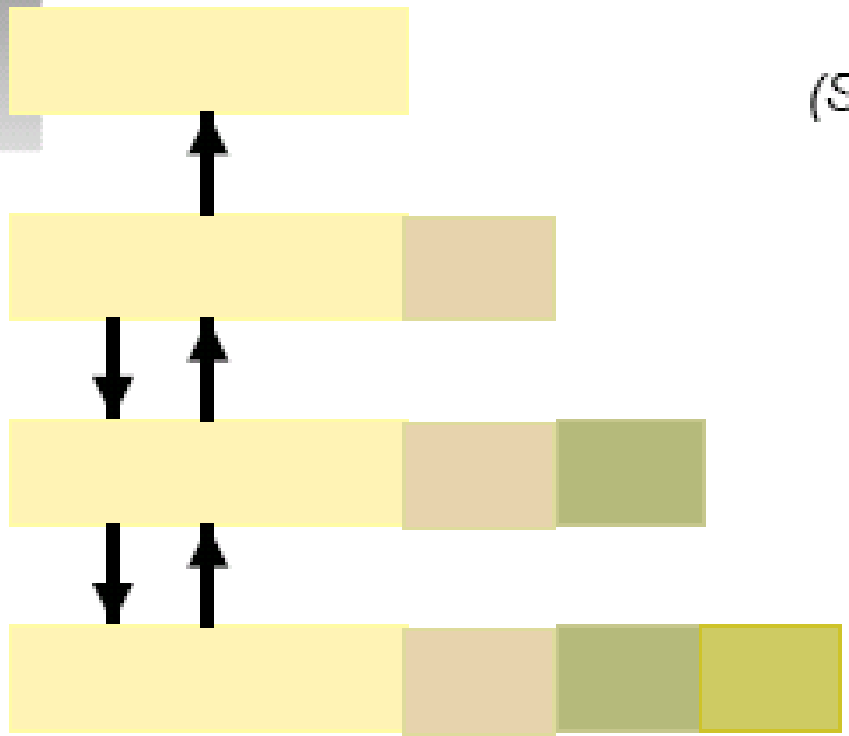
IP

- *Best effort* delivery
- Does not guarantee success
- Leaves error checking to higher layers (e.g. to TCP)

Basics of IP Networking

- Information has to be broken up into *packets* to be transferred across a network.
- Packets can have IP options set
  - IP options are usually useful only for attacks
- Packets consist of information from different layers.
  - IP layer is a common middle ground for the Internet
  - Layers below for transport details
  - Layers above for protocol details

Layers Above and Below IP



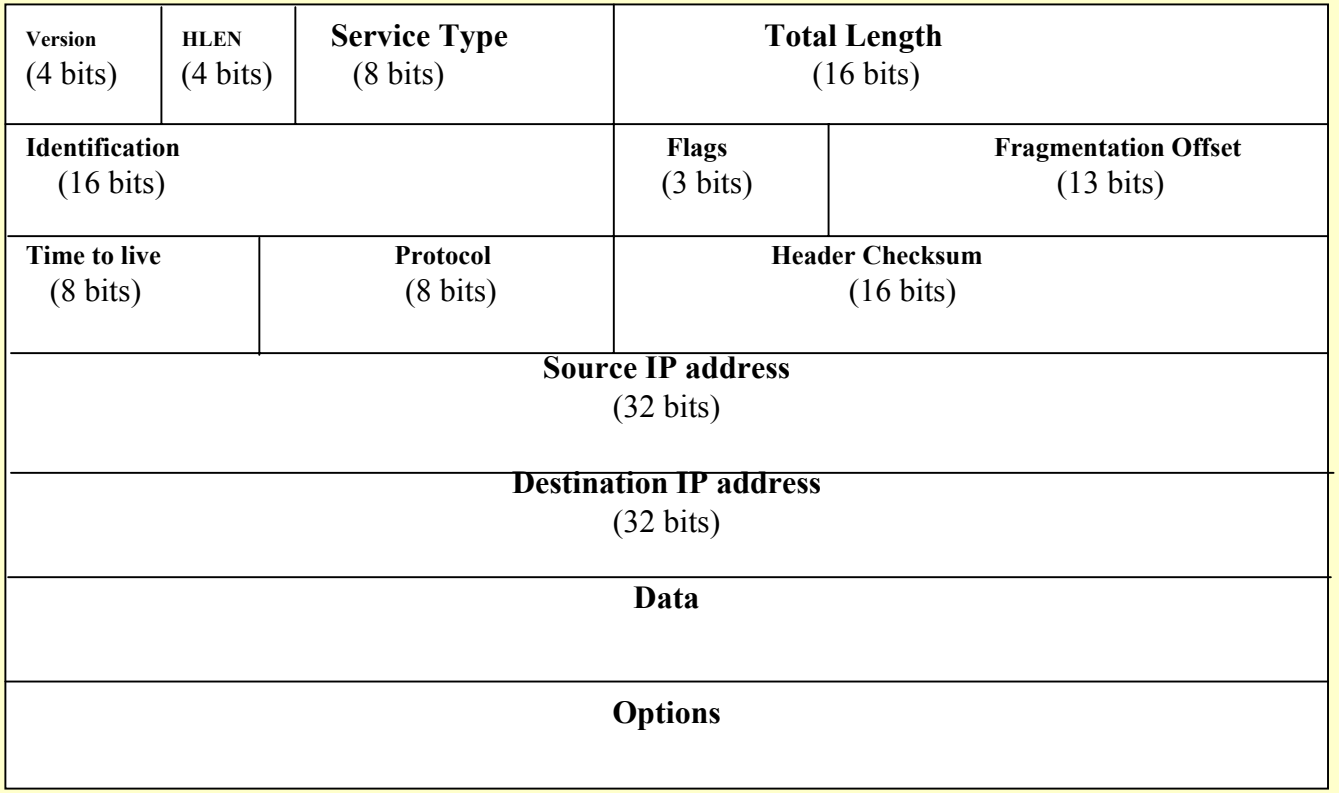
Application Layer
(SMTP, Telnet, FTP, HTTP, etc)

Transport Layer
(TCP, UDP, ICMP, etc)

Internet Layer
(IP)

Network Access Layer
(Ethernet, FDDI, ATP, etc)

IP Datagram Format



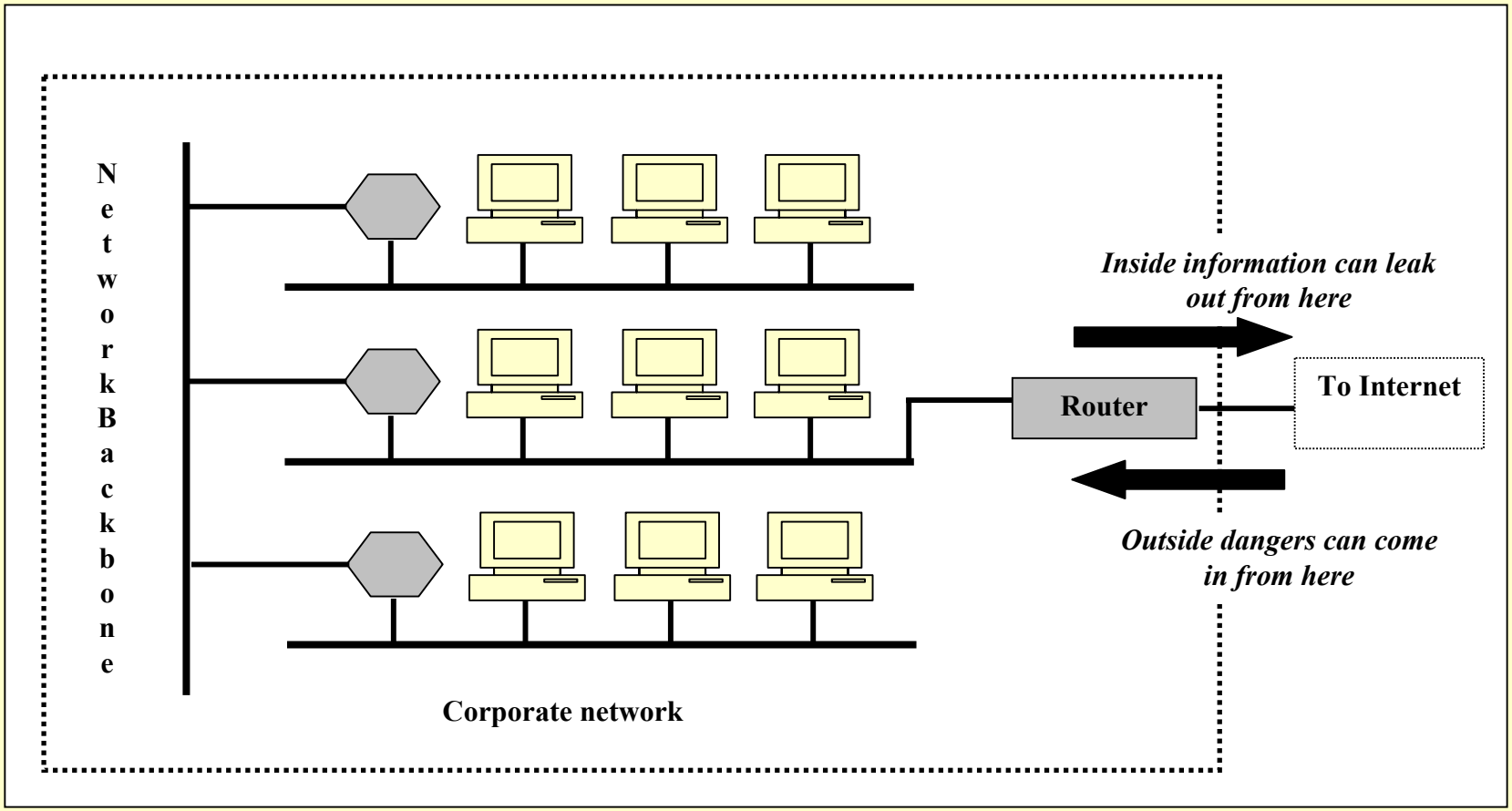
Firewalls and IP

- Firewalls should reject packets with IP options set
- Firewalls should not pass multicast/broadcast destination packets
- Firewalls should not accept multicast/broadcast source addresses
- Firewalls should either reassemble fragments or refuse them

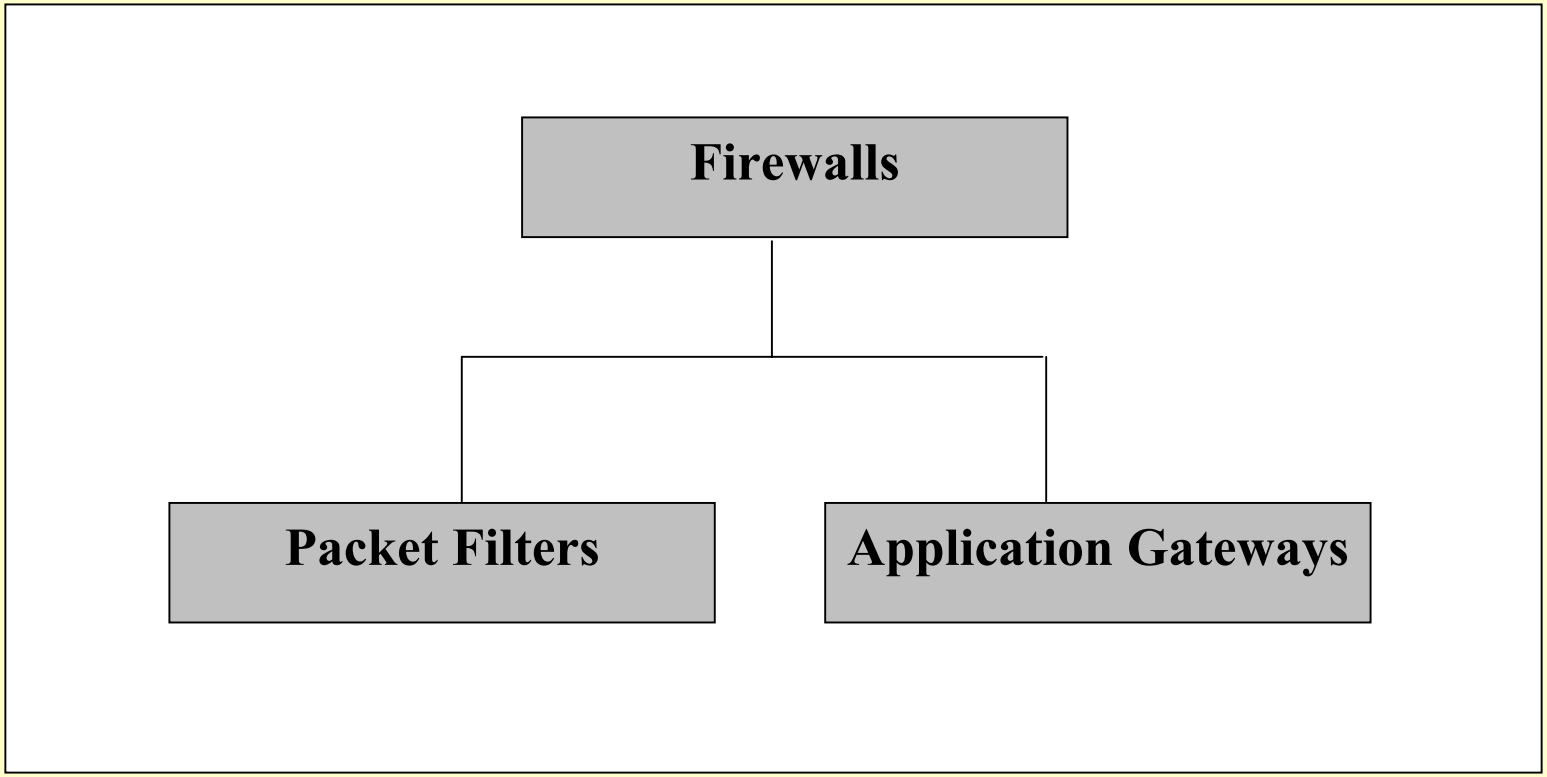
Network Aspects

- Internal network (e.g. LAN)
- External Network (e.g. Internet)
- Threats from the External Network to the Internal Network

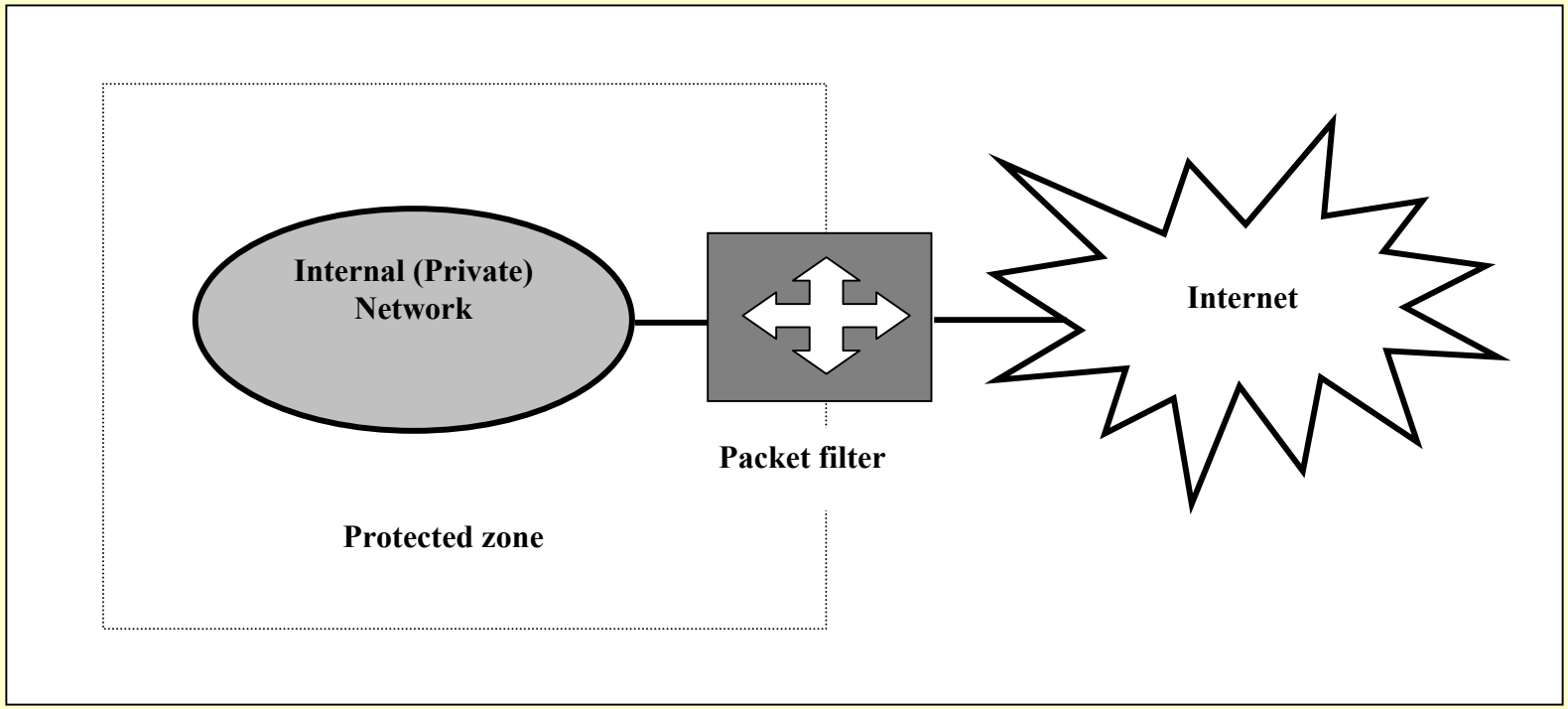
Network Threats



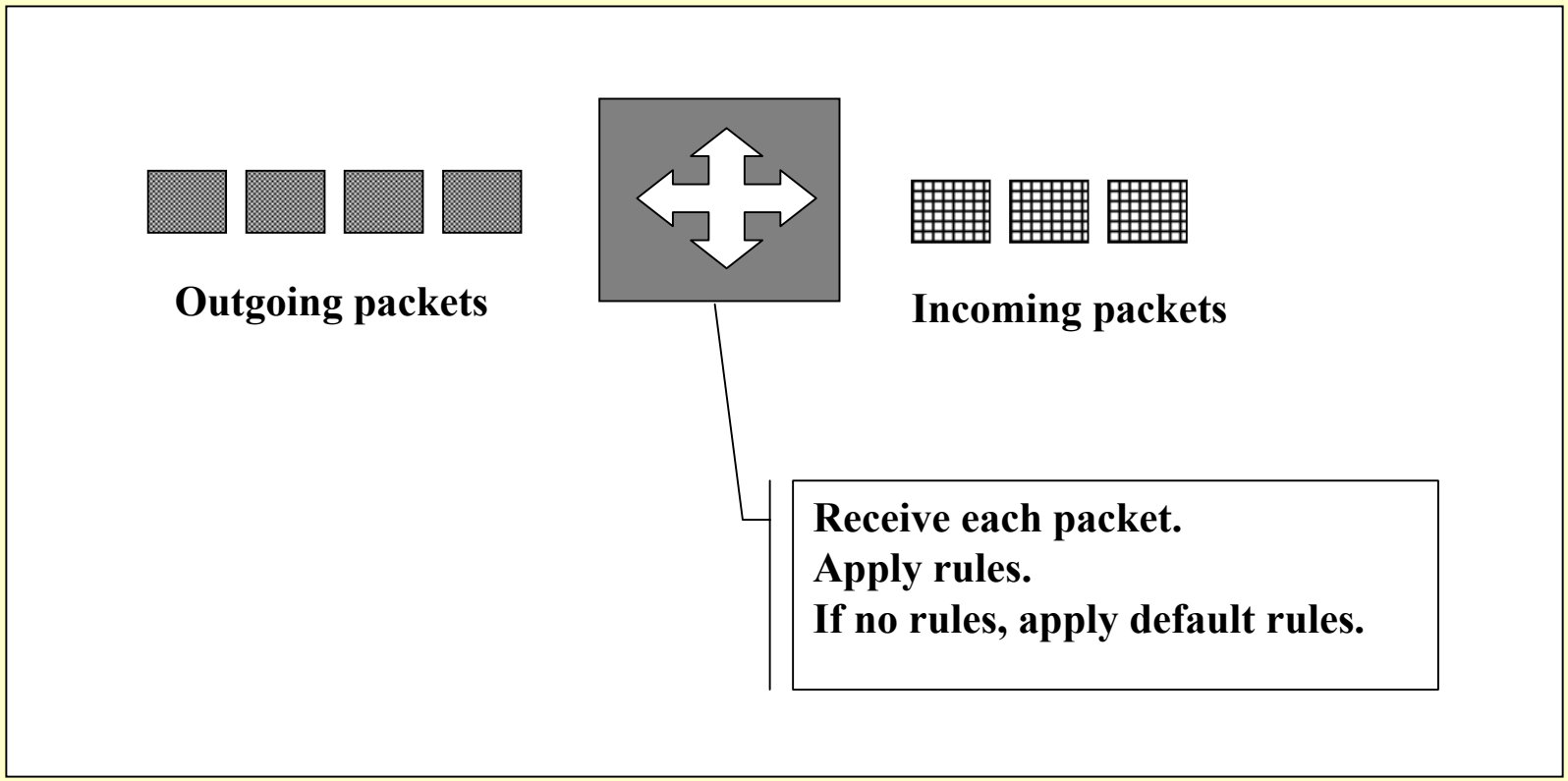
Firewall Types



Packet Filter



Packet Filter Operation



Packet Filtering

- Packet filtering systems selectively route packets between internal and external hosts
- Every IP packet includes information about:
  - source and destination addresses
  - protocol (TCP, UDP, or ICMP)
  - TCP or UDP source and destination ports
  - ICMP message type
  - Packet size
- The packet filtering system also knows:
  - interface packet goes in on
  - interface packet goes out on

Examples of Packet-Filtering Rule Sets

Table 20.1 Packet-Filtering Examples

A

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

B

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

C

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

D

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

E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Packet-Filtering Rule Sets

- Packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header.
- If there is match to one of the rules, that rule is invoked to determine whether to forward or discard the packet.
- If there is no match to any rule, then a default action is taken. Two default policies are possible

There are two fundamental stances that you can take with respect to security

decisions and policies.

1. Default = Discard (The default deny stance)

That which is not expressly permitted is prohibited. Or Specify only what you allow and prohibit everything else.

2. Default = Forward (The default Permit stance)

That which is not expressly prohibited is permitted. Or Specify only what you prohibit and allow everything else.

Examples of Packet-Filtering Rule Sets

Table 20.1 Packet-Filtering Examples

A

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

B

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

C

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

D

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

E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Packet Filtering Examples

- Inbound mail is allowed (port 25 is for SMTP incoming), but only to a gateway host. Mail from an external host, SPIGOT, is blocked because that host has a history of sending massive files in e-mail messages.

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

Packet Filtering Examples

- This is an explicit statement of the default policy. All rule sets include this rule implicitly as the last rule.

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

Packet Filtering Examples

- This rule set is intended to specify that any inside host can send mail to the outside. A TCP packet with a destination port of 25 is routed to the SMTP server on the destination machine.
- The problem is the use of port 25 for SMTP receipt is only default; an outside machine could be configured to have other application linked to port 25.
- As this rule is written, an attacker could gain access to internal machines by sending packets with a TCP source port number of 25.

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

Packet Filtering Examples

- This set of rule take advantage of a feature of TCP connections.
- Once a connection is set up, ACK flag of a TCP segment is set to ack segments sent from the other side.
- This rule states that it allows IP packets where the source IP addr is one of the lists of designated internal hosts & destination TCP port number is 25.
- It allows incoming packets with a source port number of 25 that include ACK flag in the TCP segment.

D

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

Packet Filtering Examples

- This rule set is one approach to handling FTP connections. With FTP, two TCP connections are used: a control connection to set up the file transfer & data connection for actual file transfer.
- The data connection uses a different port number that is dynamically assigned for the transfer.
- Most servers, & hence most attack targets, live on low- numbered ports; ; most outgoing calls tend to use a higher-numbered port, typically above 1023. This rule set allows:

  Packets that originate internally

  Reply packets to a connection initiated by an internal machine

  Packets destined for a high-numbered port on an internal machine

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Advantages of Packet Filtering

- One of the key advantages of packet filtering is that a single, strategically placed packet filtering router can help protect an entire network.
- If only one router connects your site to the Internet, you gain tremendous leverage on network security regardless of the size, by doing packet filtering on that router.
- Simple Packet filtering can be extremely efficient, because simple packet filtering requires paying attention only to a few packet headers, it can be done with very low overhead.

Advantages of Packet Filtering

- Much smaller Delay than Proxying, however,the more work your packet filters do, the slower they will be. If your packet filters behave like proxies, doing complicated data driven operations that require keeping track of multiple packets, they will tend to perform like proxies as well.

- Packet Filtering capabilities are available in many hardware and software routing products , both commercial and freely available over the Internet. Most sites already have packet filtering capabilities available in the routers they use.

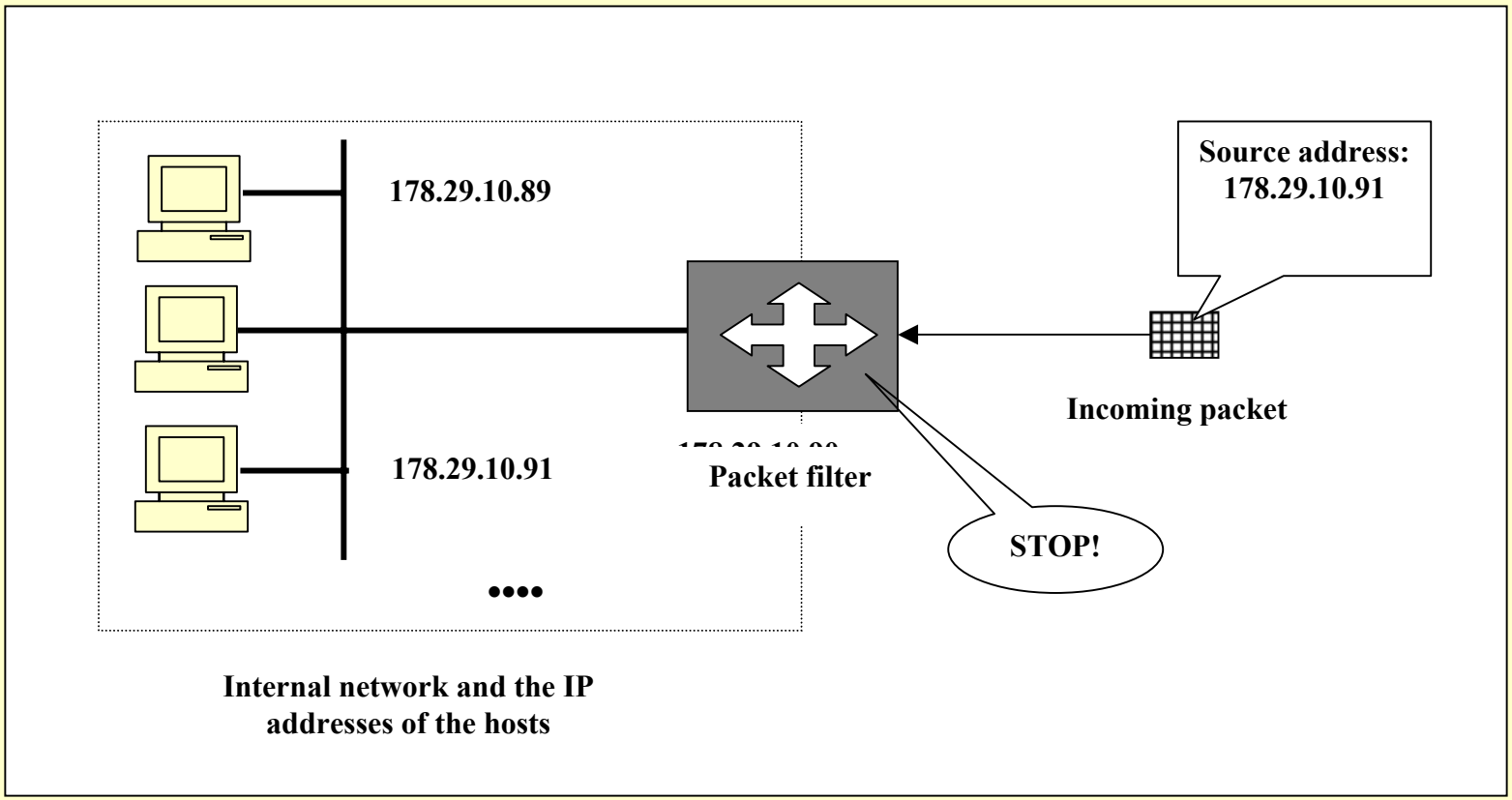
Weaknesses of packet-filter firewalls

- Packet filter firewalls do not examine upper-layer data, it cannot block specific application commands, if it allows a given application, all functions available within that application will be permitted.
- Because of limited information available to the firewall, the logging functionality is limited. Logs normally contain source address, destination address, & traffic type.
- Do not support advanced authentication scheme due to the lack of upper-layer functionality by the firewall.
- Vulnerable to network layer address spoofing. Many packet filter firewalls cannot detect the network packet in which layer 3 addressing is altered

Attacks on Packet Filters

- **IP address spoofing**: Intruder transmits packets from the outside with a source IP address field containing an address of an internal host. Use of a spoofed address will allow penetration of systems that employ simple source address security, in which packets from specific trusted internal hosts are accepted. Countermeasure is to discard packets with an inside source address if the packet arrives on an external interface.
- **Tiny fragment attacks**: Intruder uses IP fragmentation option to create extremely small fragments & force the TCP header information into a separate packet fragment. Attacker hopes that if filtering rules depend on TCP header information, then only the first fragment is examined by the filtering router & that the remaining segments are passed through. A tiny fragment attack can be defeated by discarding all packets where the protocol type is TCP & the IP Fragment Offset is equal to 1.

Packet Filter Defeating IP Spoofing Attack



Attacks: Spoofing

- Spoofed packets have incorrect source addresses
- Spoofing allows attacker to:
  - Intercept the reply
  - Disguise the source of the attack
  - Have victim machine send packets to second victim (*smurf* attack)
  - Have victim send packets to itself until it crashes (*land* attack)

The ICMP Protocol

- ICMP is used for status and control messages:
  - *Echo request* (running `ping`)
  - *Echo response* (responding to `ping`)
  - *Destination unreachable*
  - Others
- `ping` is often used as a prelude to an attack
- ICMP packets are small, but oversized ICMP packets are used in DoS attacks
- ICMP packets can be padded, and thus used as a covert channel
- "Destination unreachable" packets needed for path MTU discovery

Stateful Packet Filtering

A packet filtering system is said to be *stateful* if it keeps track of useful historical facts, such as:

- whether a packet is a response to another packet
- how many other packets have been recently seen to or from the same host
- whether the packet is identifical to a recently seen packet
- whether the packet is a fragment from a larger packet

Stateful Firewall Connection State Table

- In the table, there is an entry for each currently established connection.
- Packet filter will now allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory.

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.212.212	1046	192.168.1.6	80	Established

Other Protocols

The UDP Protocol

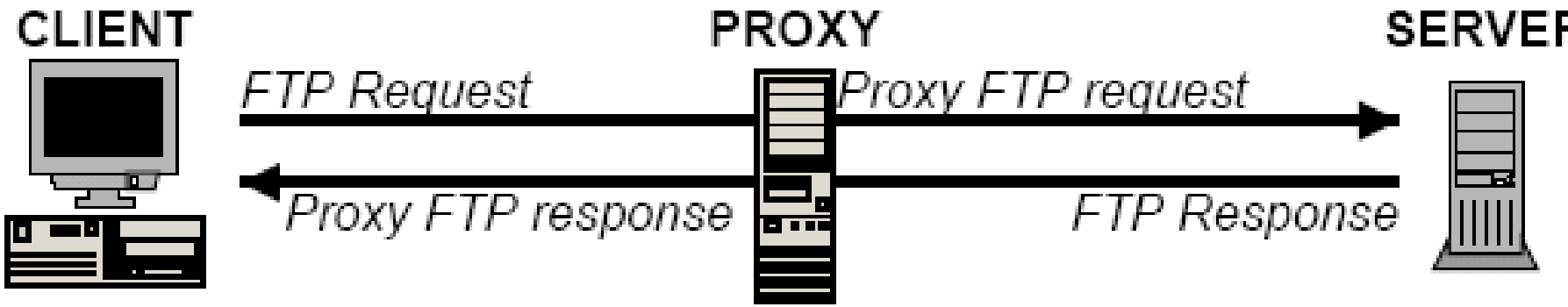
- UDP is not reliable in any of the ways that TCP is reliable.
- Makes UDP more difficult to filter as finely as TCP

Non-IP Protocols

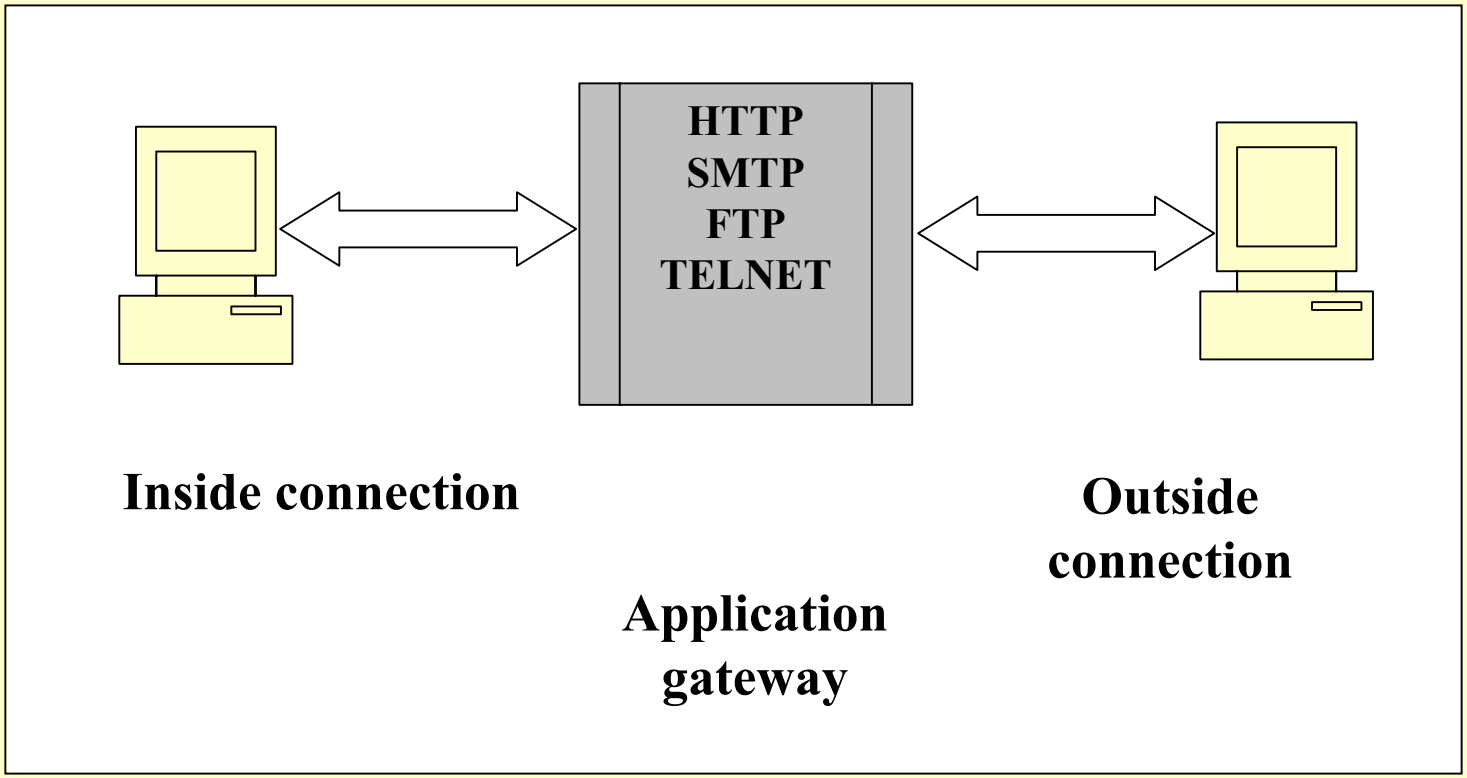
- Examples: Appletalk, IPX
- Non-IP protocols are encapsulated in IP packets across Internet
- Some firewalls can filter non-IP packets, but with less flexibility
- Most firewalls can only either reject all or accept all

Proxies

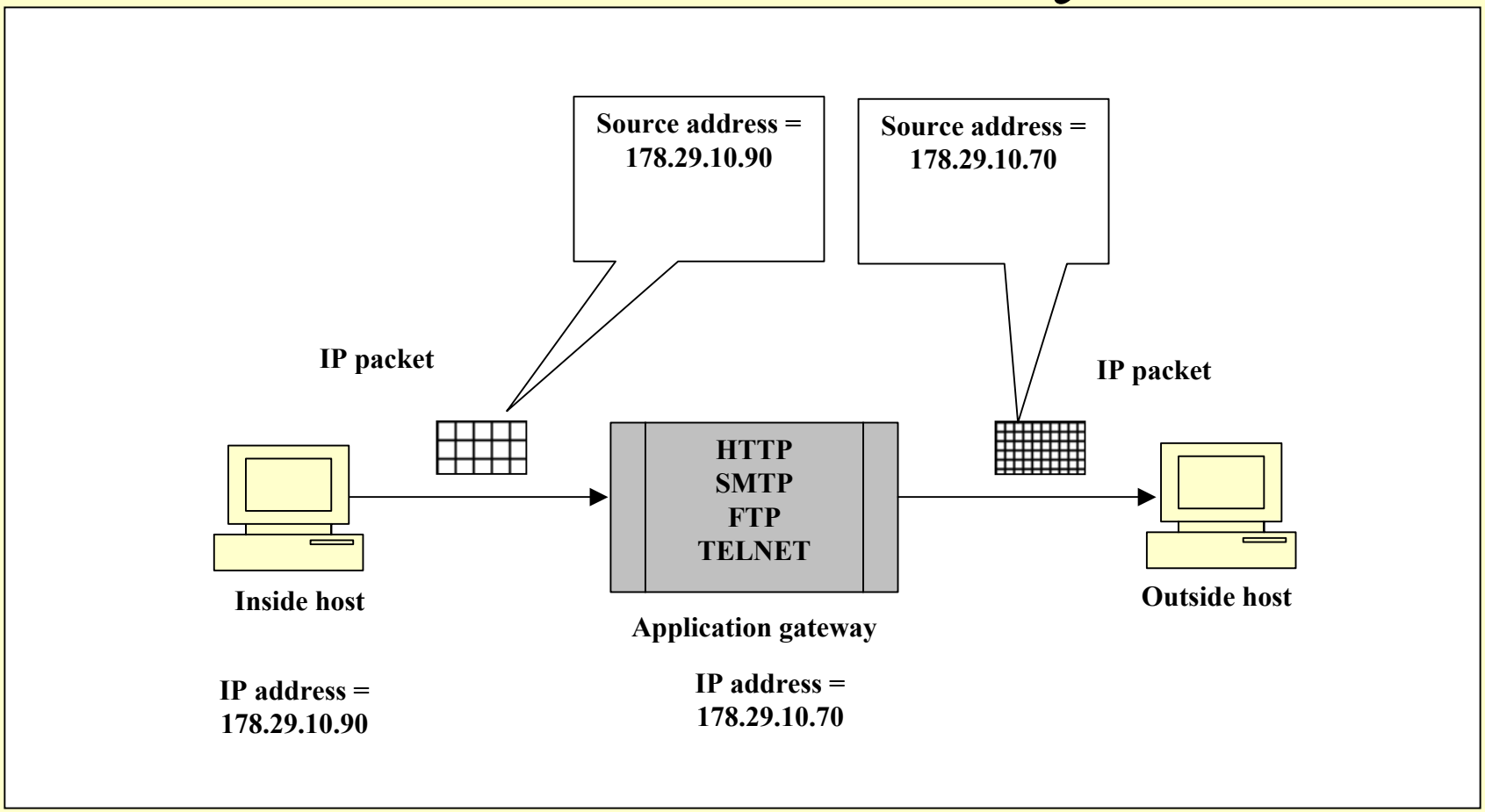
- *proxy*: n. Something or someone who does something on someone else's behalf.
- Proxy servers take requests for services and act as gateways between users and remote machines.



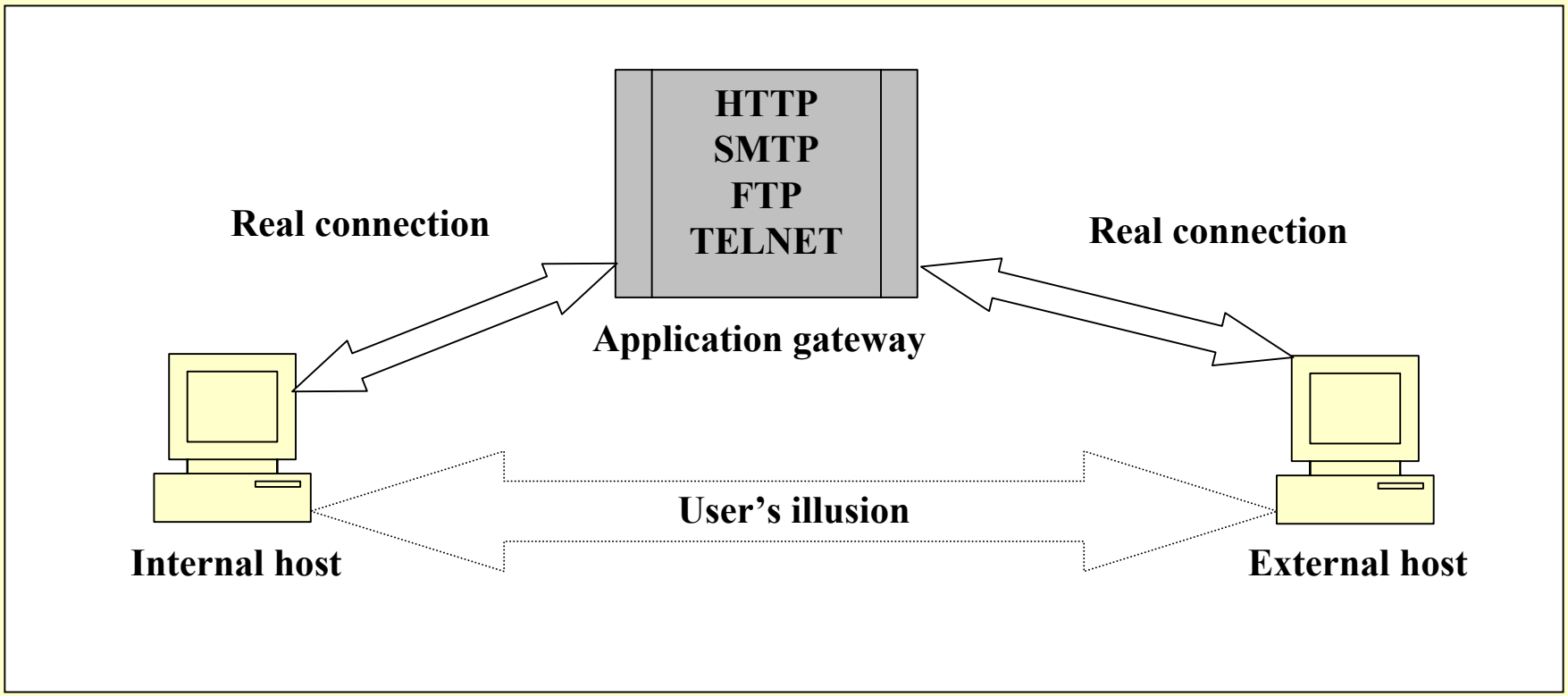
Application Gateway



Circuit Gateway



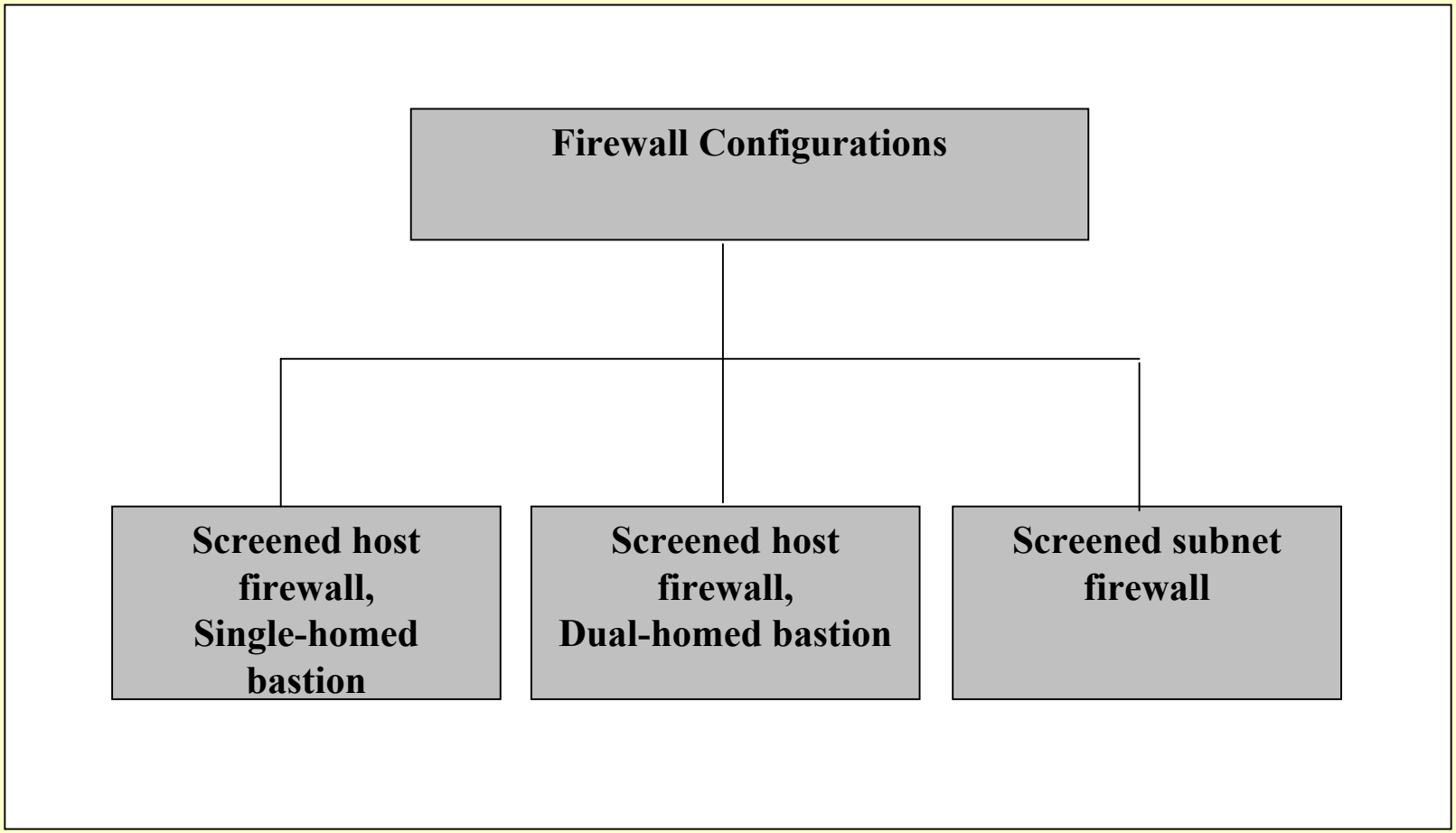
Application Gateway - Illusion



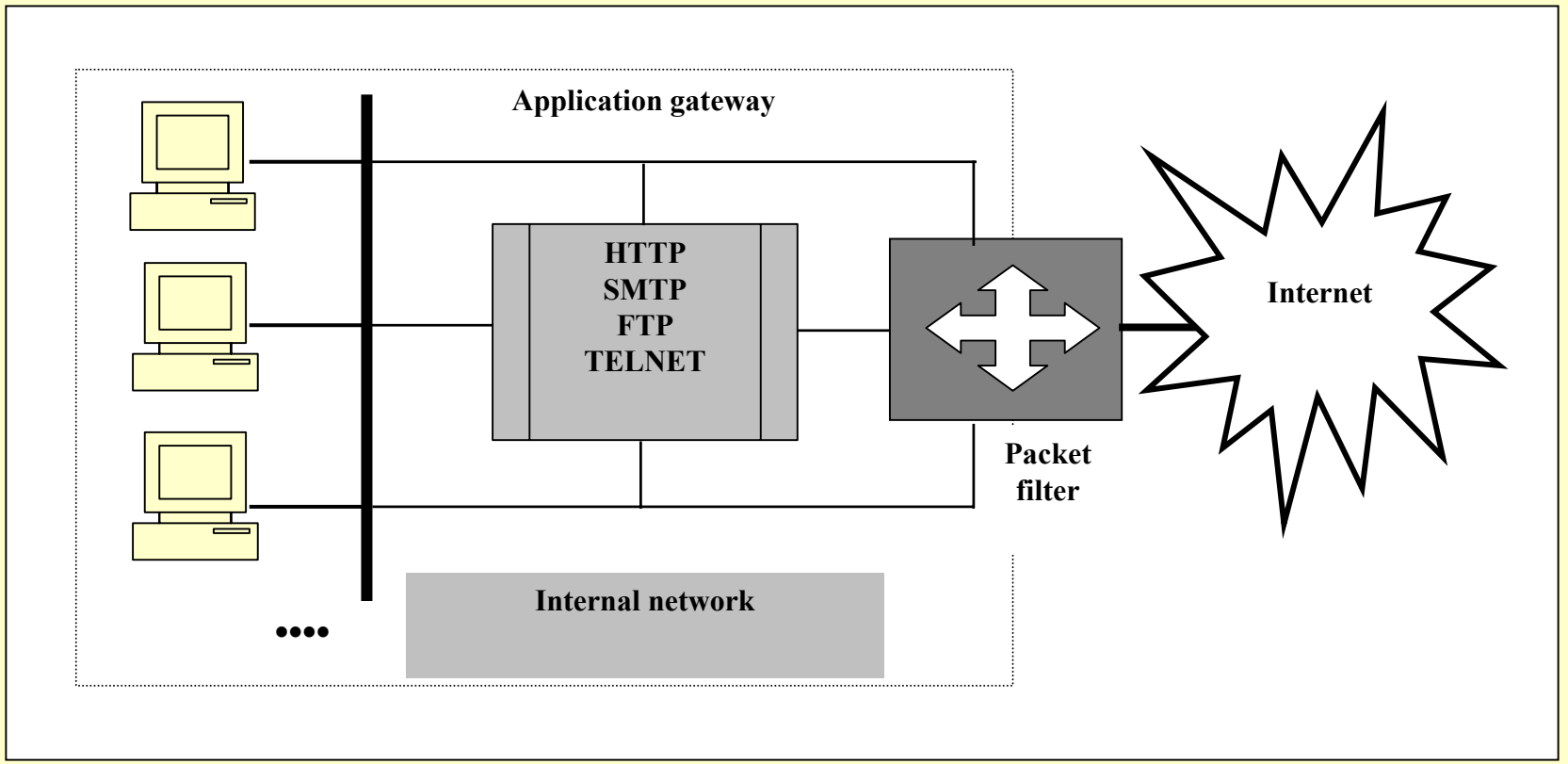
Proxies: Advantages and Disadvantages

- **Advantages:**
  - Proxies are good at logging
  - Proxies can do intelligent filtering
  - Proxies can perform user-level authentication
  - Proxies automatically provide protection for weak or faulty implmentations
- **Disadvantages:**
  - Proxied services are much slower
  - Proxying requires modifications to clients, applications, or procedures

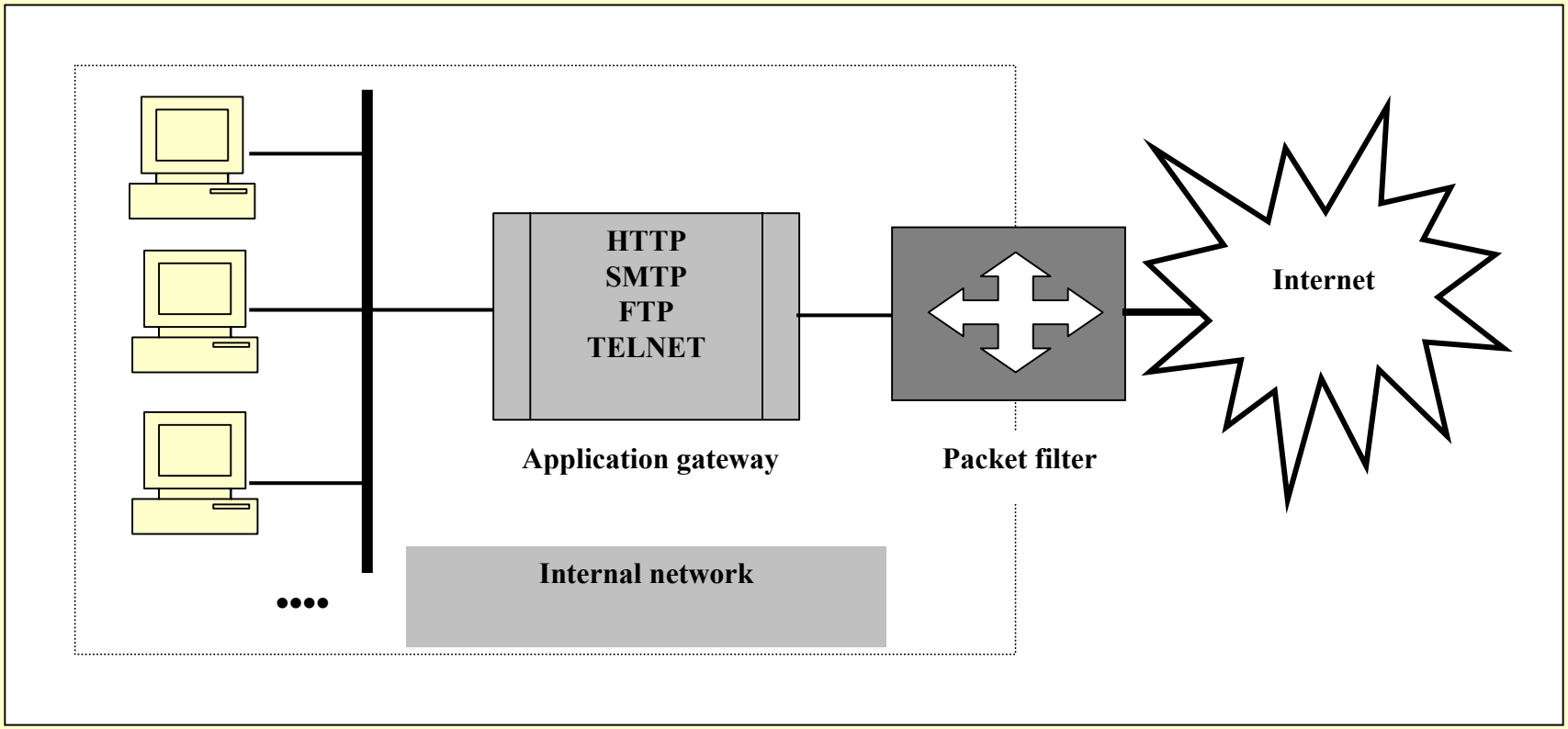
Firewall Configurations



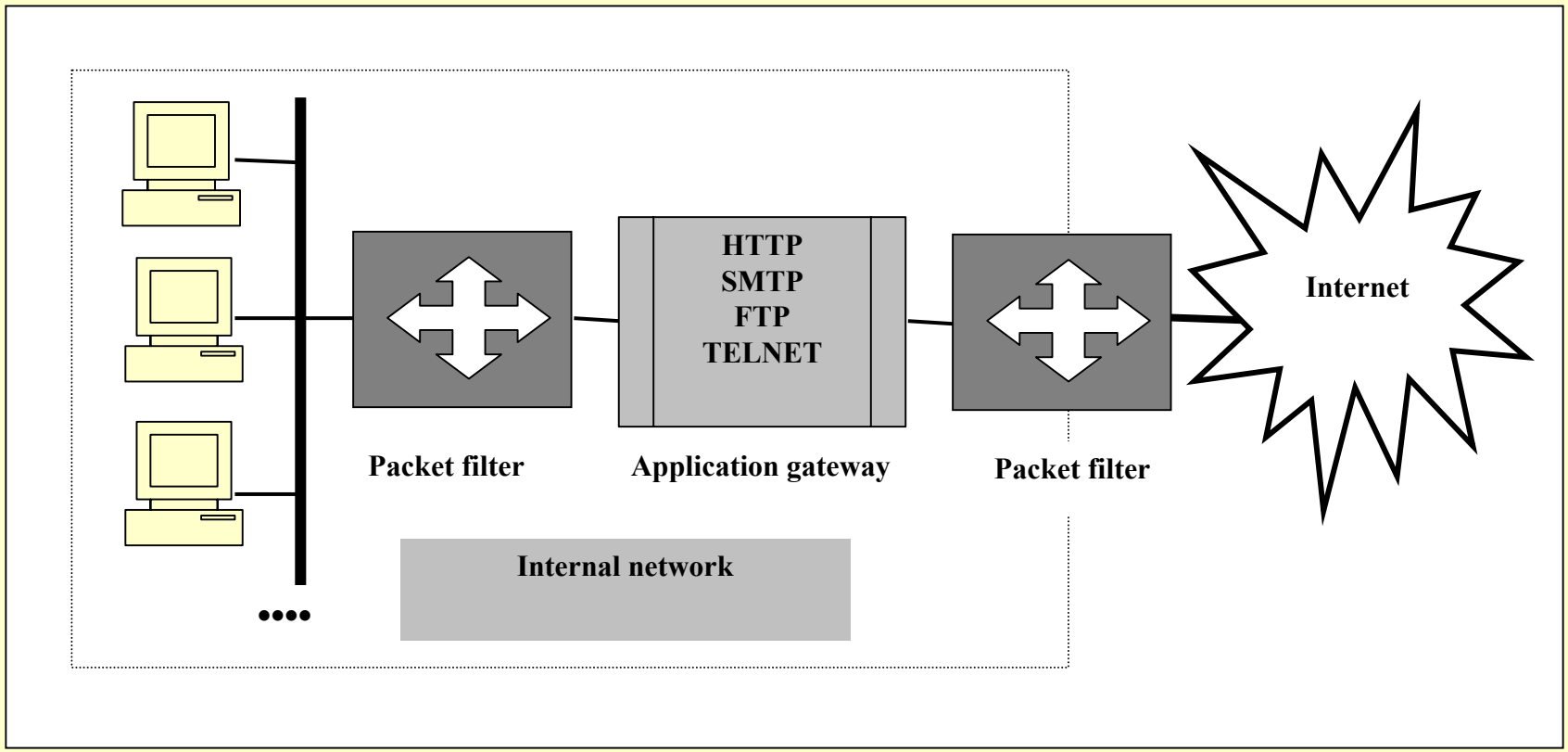
Screened Host Firewall, Single-homed Bastion



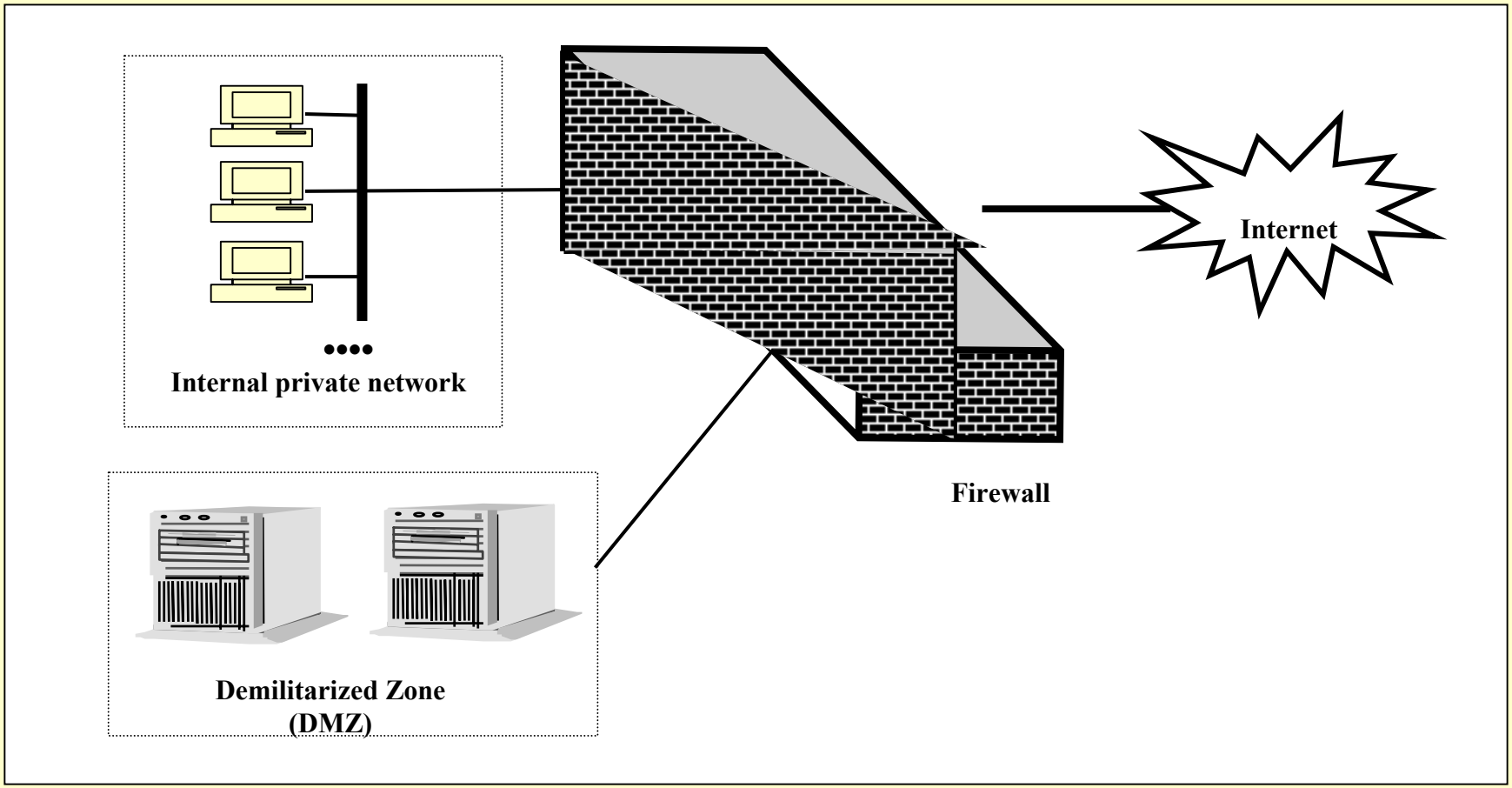
Screened Host Firewall, Dual-homed Bastion



Screened Subnet Firewall



Demilitarized Zone (DMZ)



Firewalls: Advantages

Firewalls can:

- Provide focal point (*choke point*) for security
- Enforce security policy by
  - Limiting services to approved ones
  - Keeping dangerous services to internal network
  - Allowing only specific systems access to specific services
- Log Internet activity efficiently
  - All Internet traffic passes through the firewall
- Limit exposure of the internal network

Firewalls: Disadvantages

Firewalls can't:

- Protect against malicious insiders
- Protect against connections bypassing firewalls
- Protect against completely new threats
- Completely protect against viruses

Firewalls are difficult to configure

- Buggy firewall may be worse than no firewall

Firewalls interfere with the Internet

- Slower connections
- Internet applications must support firewalling

Firewall Architectures

Screening Router Router that also does simple packet filtering

Dual-Homed Host Host that has two network interfaces, each on a different network

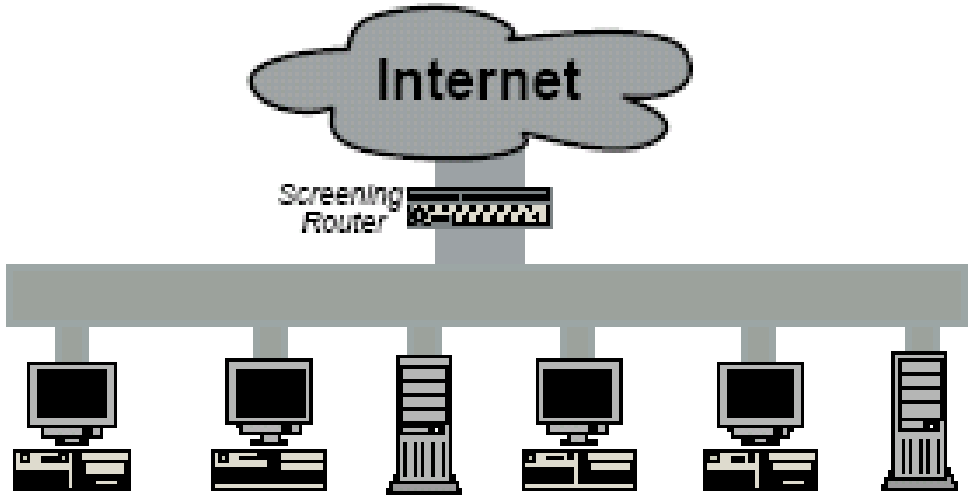
Bastion Host Secure host that provides services between external and internal networks

Perimeter Network An additional network between external and internal network

Interior Router Packet-filtering router that protects internal network from external and perimenter network

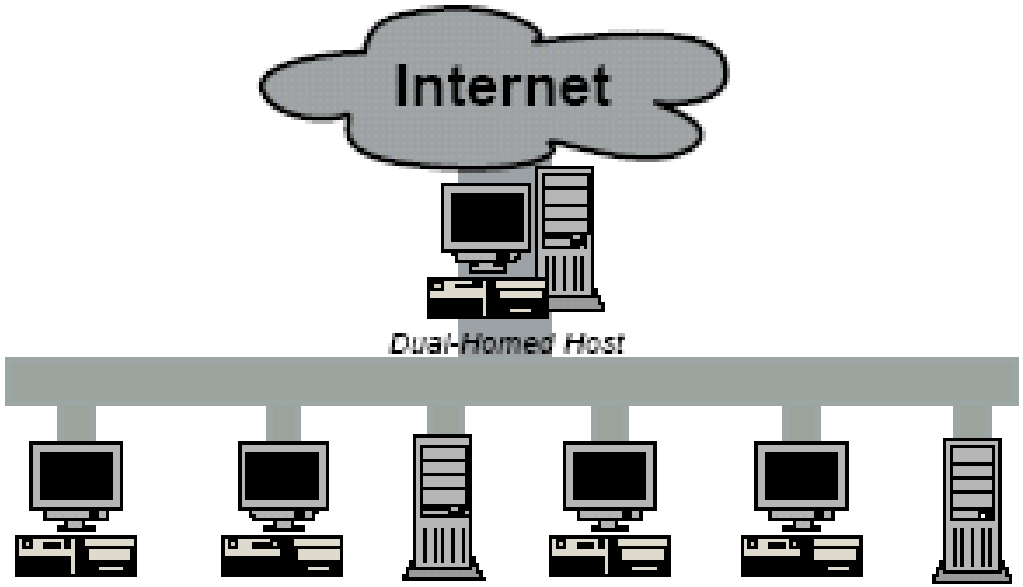
Exterior Router Packet-filtering router that protects internal and perimeter networks from external network

Single-Box Firewall Architecture: Screening Router



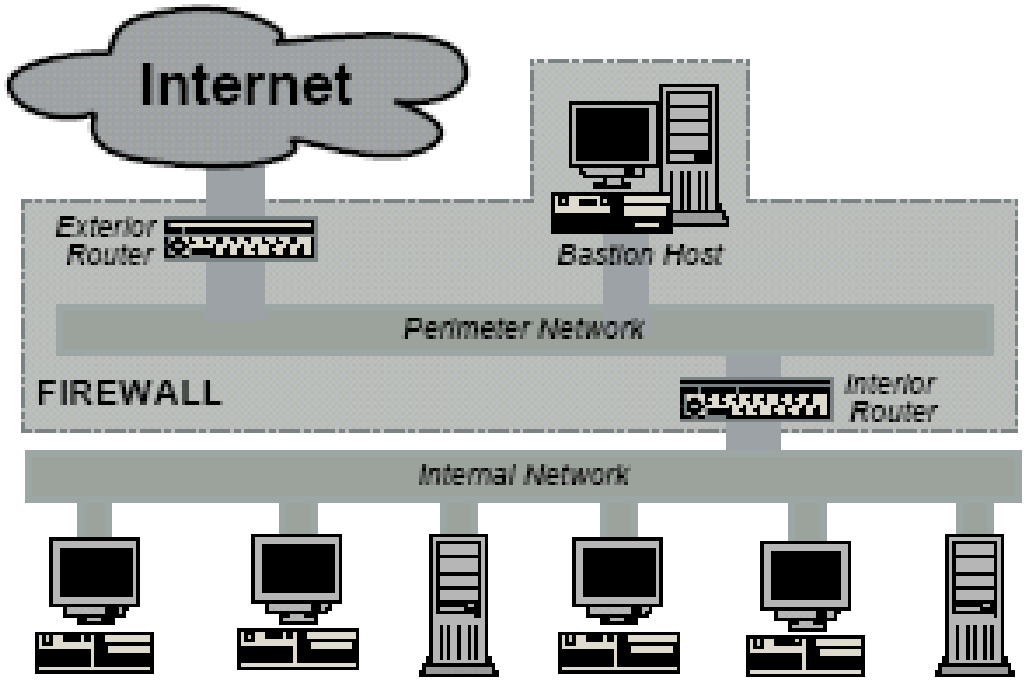
- Simple and low-cost, but not very flexible
- No depth of defense
- Most useful for internal firewalls and networks dedicated to providing services to Internet

Single-Box Firewall Architecture: Dual-Homed Host



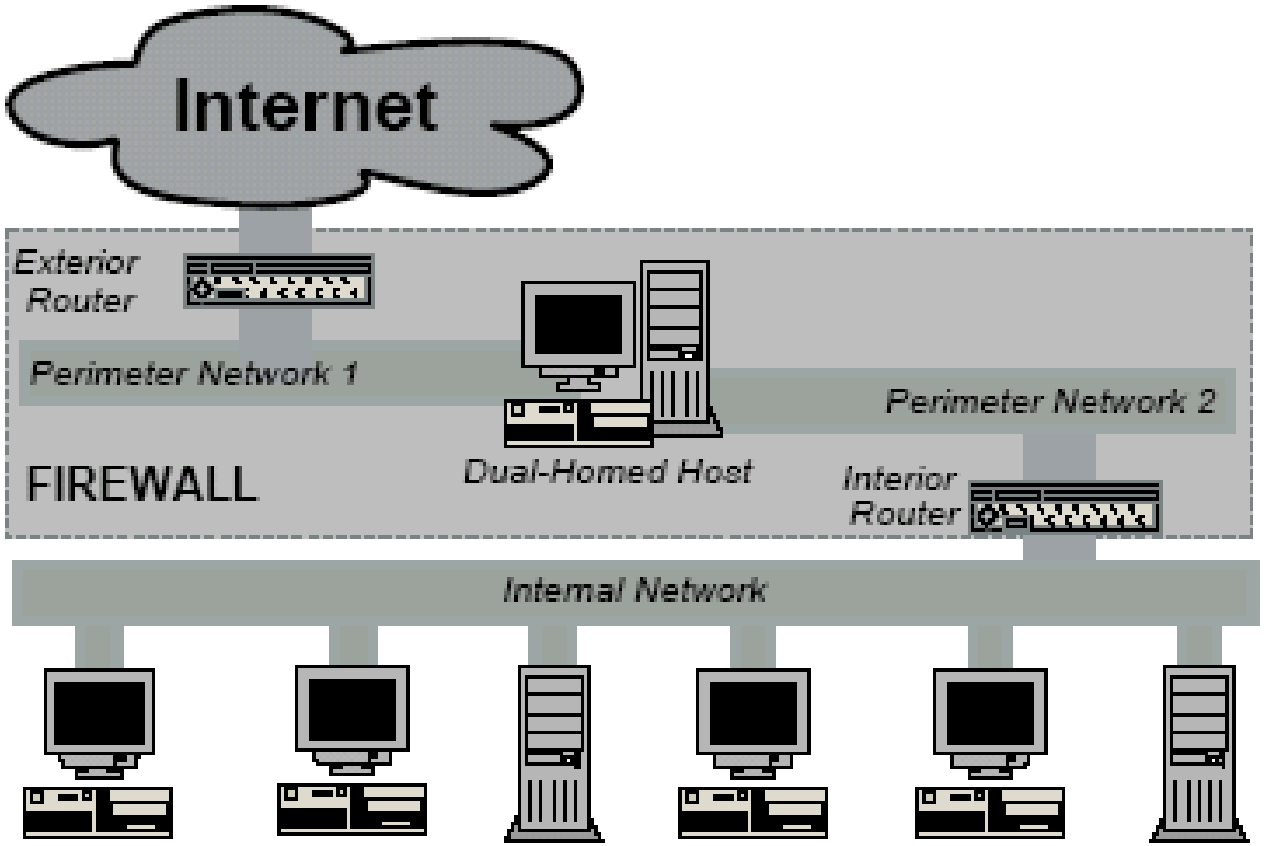
- High level of control, but slow
- Can be crashed, and a single point of failure
- Dangerous to put any services on host

Screened Subnet Firewall Architectures



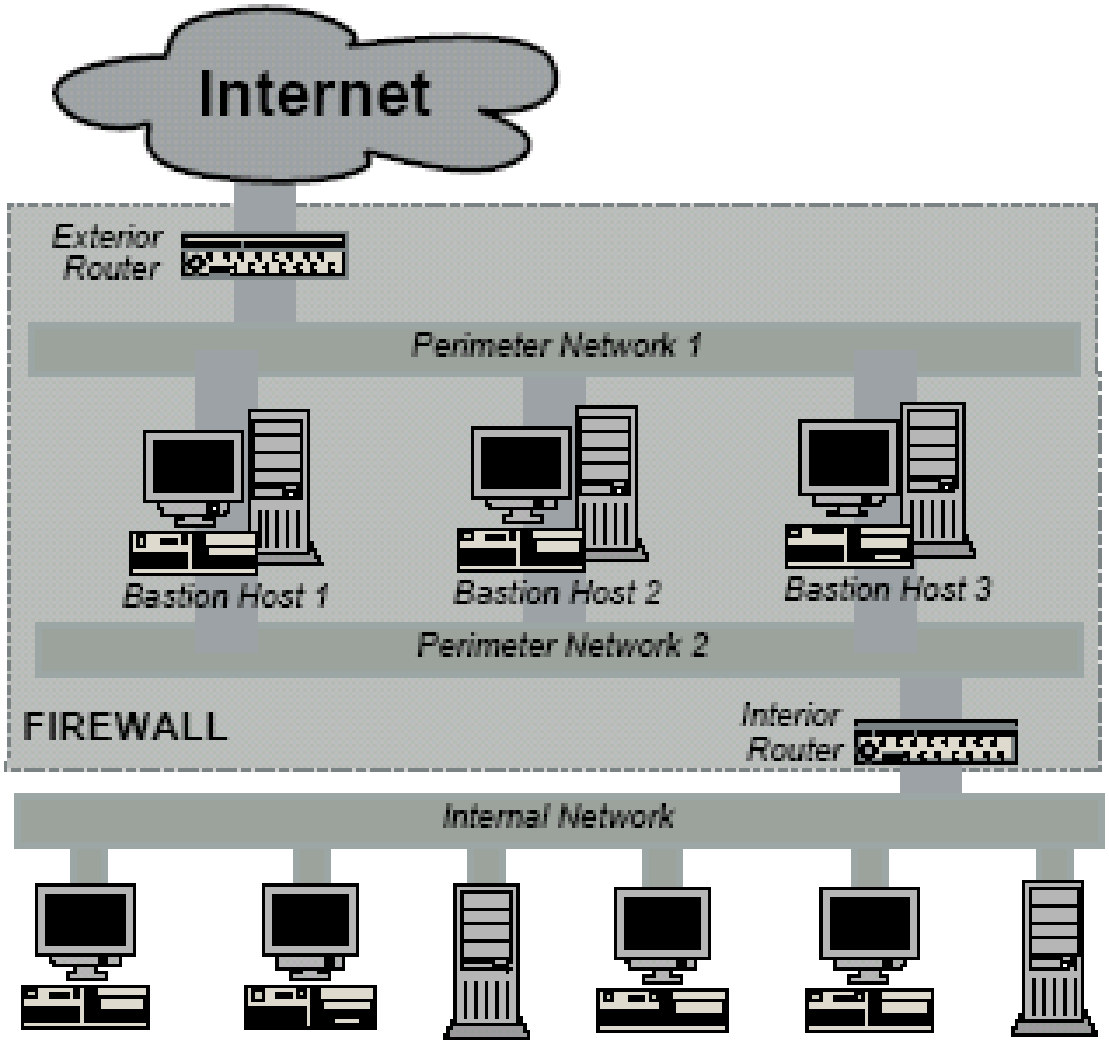
- Breaking into a bastion host: hacker can only snoop perimeter network
- Breaking into internal network requires hacking two routers
- Appropriate for most uses

Split-Screened Subnet Firewall Architectures



- Excellent depth of defense

Another Split-Screened Subnet Firewall Architectures



Intricate Firewall Architecture Example