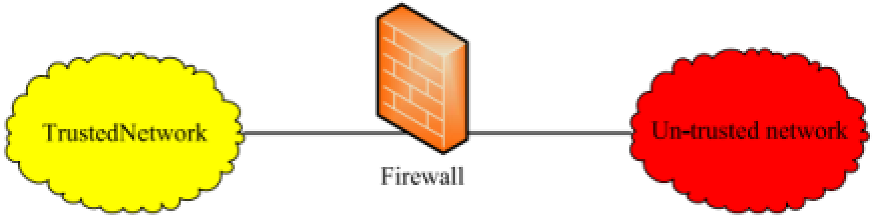
Firewall

Chun-Jen (James) Chung

Arizona State University

What is a Firewall?

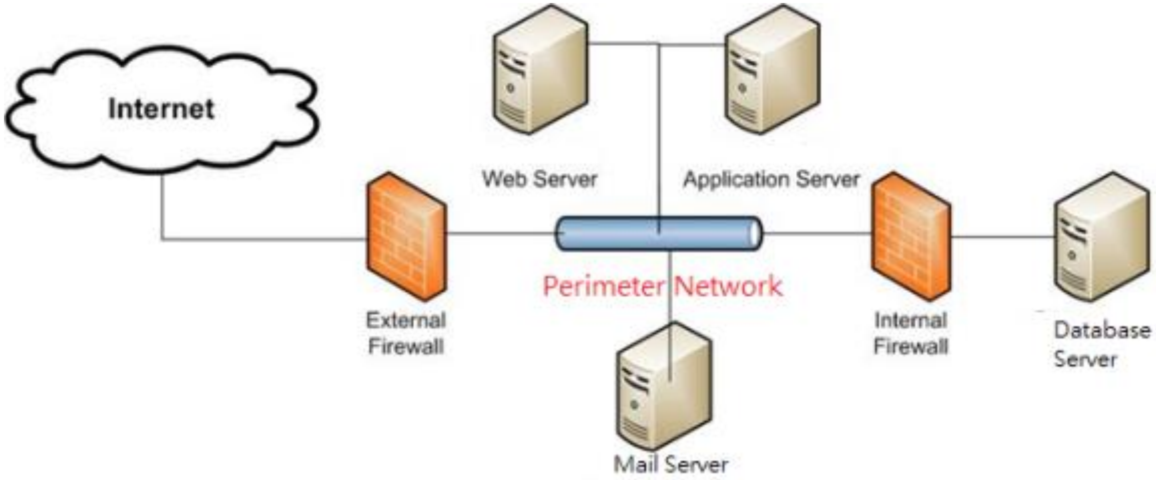
- A component or set of components that **restricts access** between a protected network and the Internet, or between other sets of networks.



- A **choke point** to control and monitor incoming/outgoing traffic.
- Interconnects networks with differing trust.
- Imposes restrictions on network services
  - only authorized traffic is allowed.
- **Auditing** and controlling access.
- Provides **perimeter defense**

Perimeter Network

- A network added between a protected network and an external network, in order to **provide an additional layer of security**.



- A perimeter network is sometimes called a **DMZ** (De-Militarized Zone).

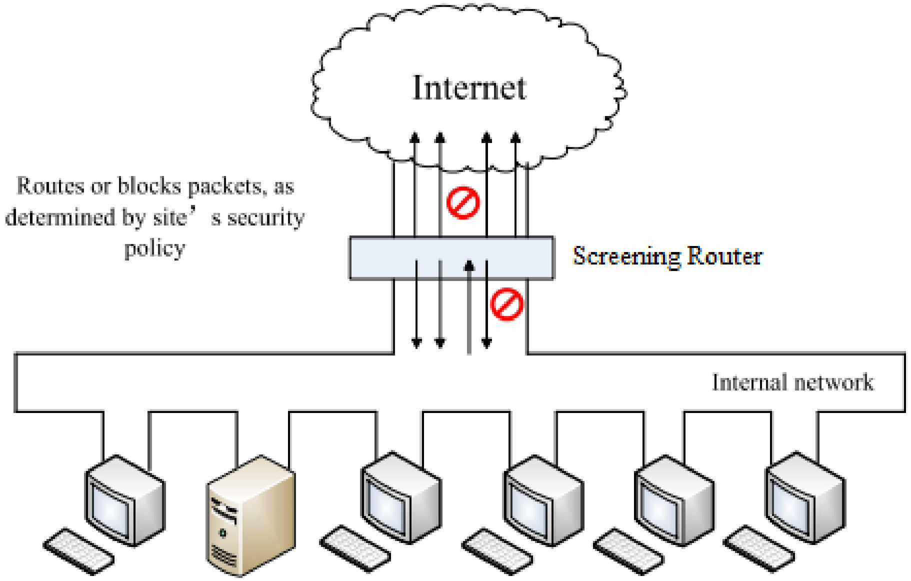
Firewall Architecture

- Single-Box Architecture
  - Screening Router
  - Dual-Homed Host
  - Multiple-Purpose Boxes
- Screened Host Architecture
- Screened Subnet Architecture

D. Brent Chapman & Elizabeth D. Zwicky, “**Building Internet Firewalls**”, O’Reilly, 2000, http://oreilly.com/catalog/fire/chapter/ch04.html

Screening Router

- ***Screening Router***: the type of router used in a packet filtering firewall.
- ***Packet filtering***: selectively routes packets between internal and external hosts according to rules that reflect the organization's network security policy.


Internet
Routes or blocks packets, as determined by site' s security policy
Screening Router
Internal network

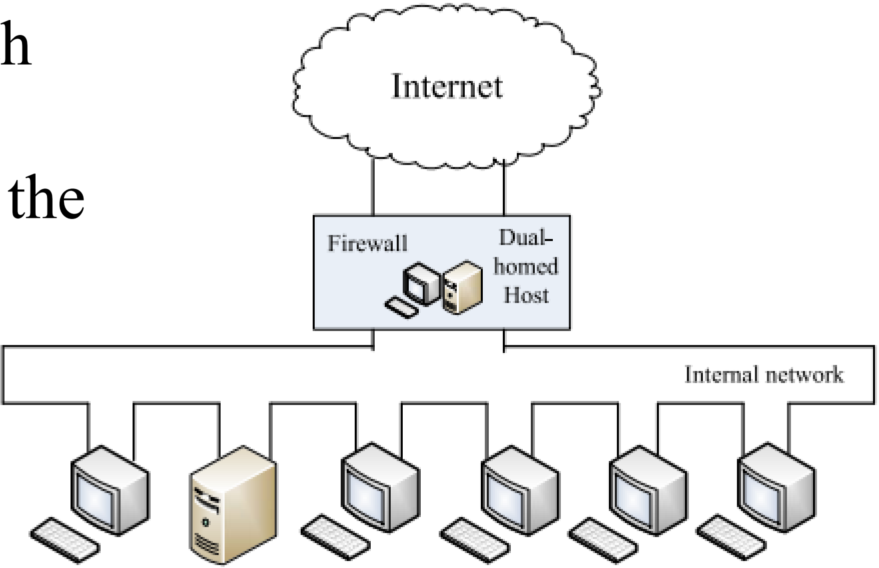
- The screening router passes/rejects an packet based on information contained on the ***packet's header*** (IP addresses and TCP/UDP ports).

Disadvantage of Screening Router

- A little or no logging capability
  - difficult for an administrator to determine whether the router has been compromised or is under attack.
- Packet filtering rules are difficult to test thoroughly
  - may leave a site open to untested vulnerabilities.
- Complex filtering rules may become unmanageable
- Only take care of transport and network layers

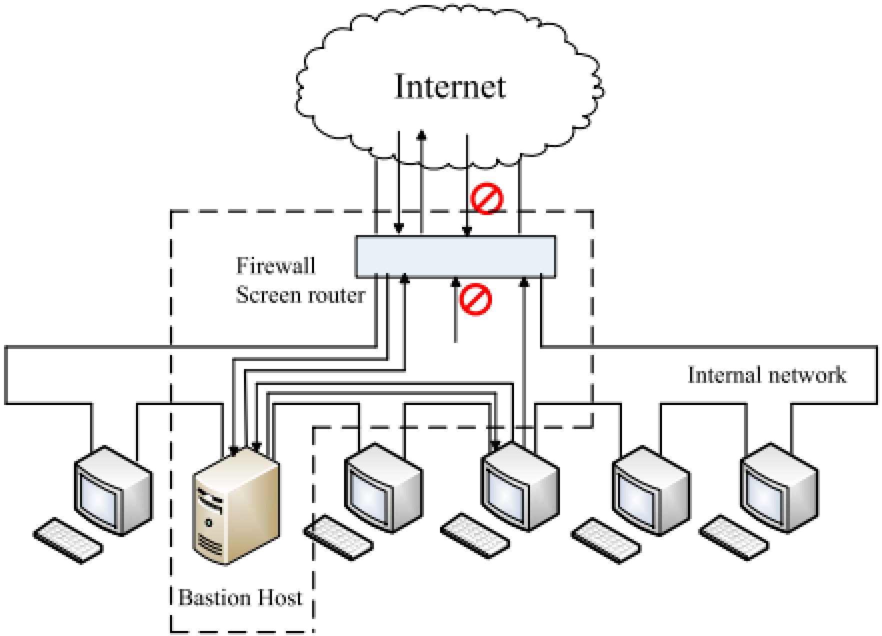
Dual-Homed Host

- ***Dual-homed host*** : a computer with at least two network interfaces.
- It could act as a router, but usually the routing functions are disabled.
  - No external packets can reach to the internal network
- It can only provide services by **proxying** them, or by having users log into the dual-homed host directly.
  - Major issue: user accounts
- Proxying is much less problematic, but may not be available for all services you're interested in.



Screened Host Architecture

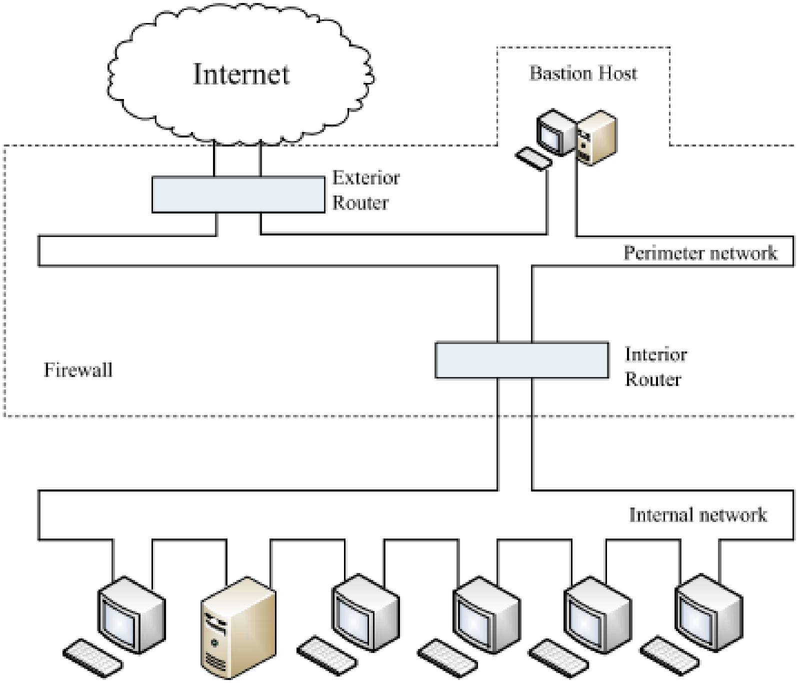
- Two major components:
  - ***Screening router*** provides packet filtering functions
  - ***Bastion host*** is the only system on the internal network that allows the connection from Internet.
- The bastion host thus needs to maintain a high level of host security.



- Screened host architecture provides both better security and better usability than the dual-homed host architecture. Why?

Screened Subnet Architecture

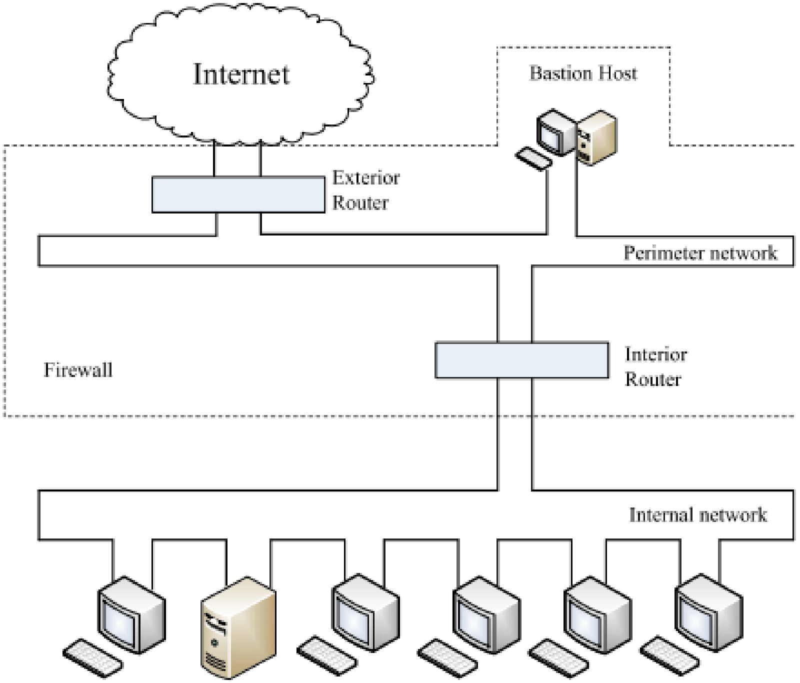
- Screened Subnet: adding a perimeter network (DMZ) that further isolates the internal network from the Internet.
  - Move the bastion host (the most tempting target) to the DMZ.
    - To handle incoming traffic, such as email, FTP, DNS query, and Web request
    - act as a proxy server to allow internal clients to access external servers indirectly.



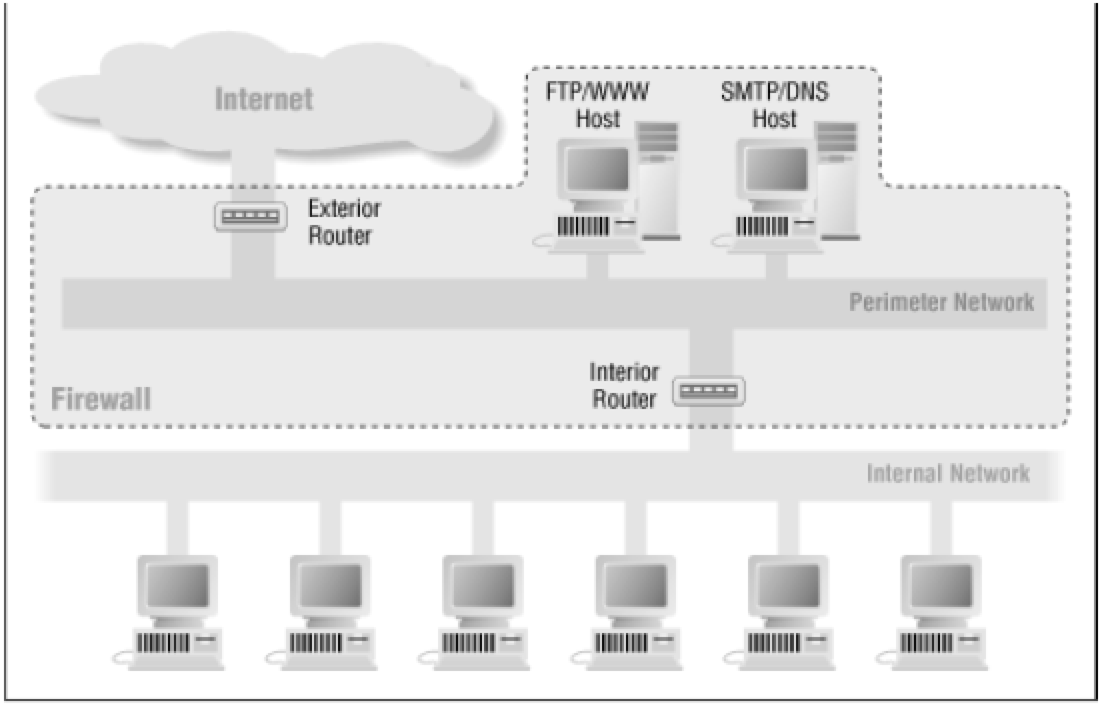
- Outbound services are handled in either of these ways:
  - packet filtering on both the exterior and interior routers (allow access directly).
  - proxy server runs on the bastion host (allow access indirectly).

Interior Router vs. Exterior Router

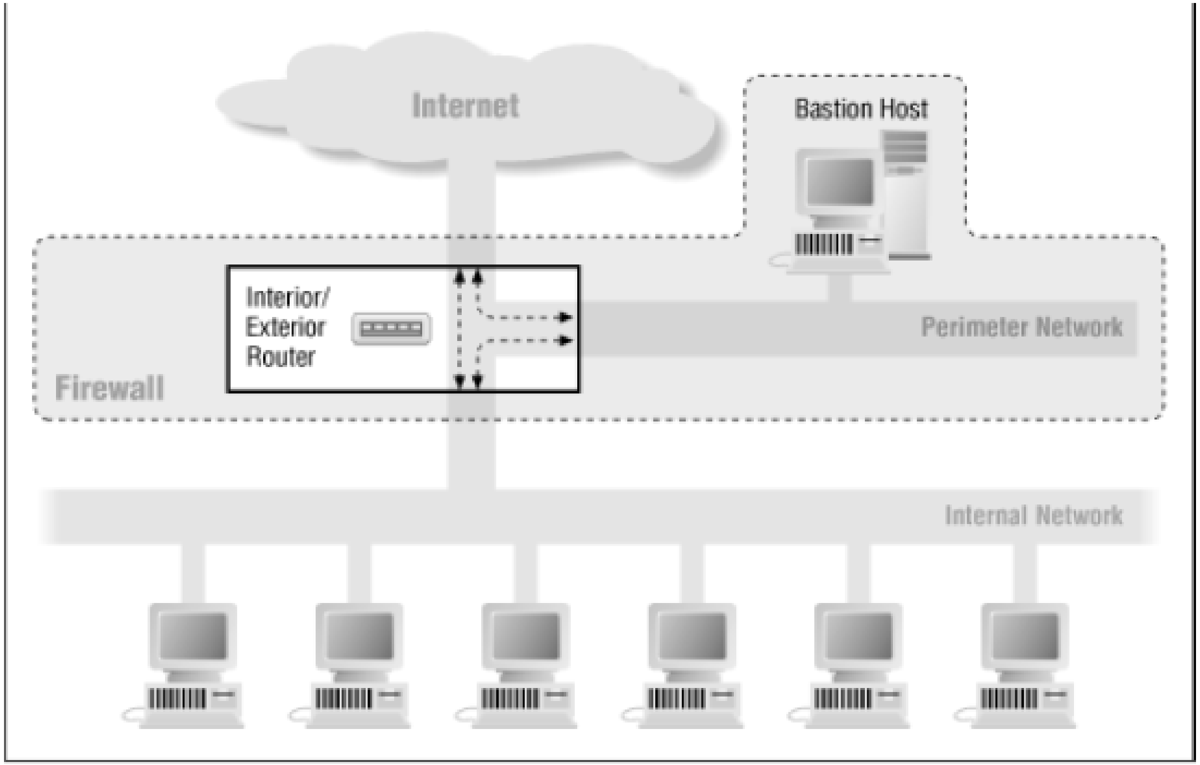
- The exterior router (access router)
  - tend to allow almost anything outbound from the perimeter net, and the generally do very little packet filtering.
  - Special rules to protect the hosts on the perimeter net.
- The interior router (choke router) does most of the packet
  - It allows selected services from the internal to the Internet. These services can safely support and safely provide using packet filtering rather than proxies.



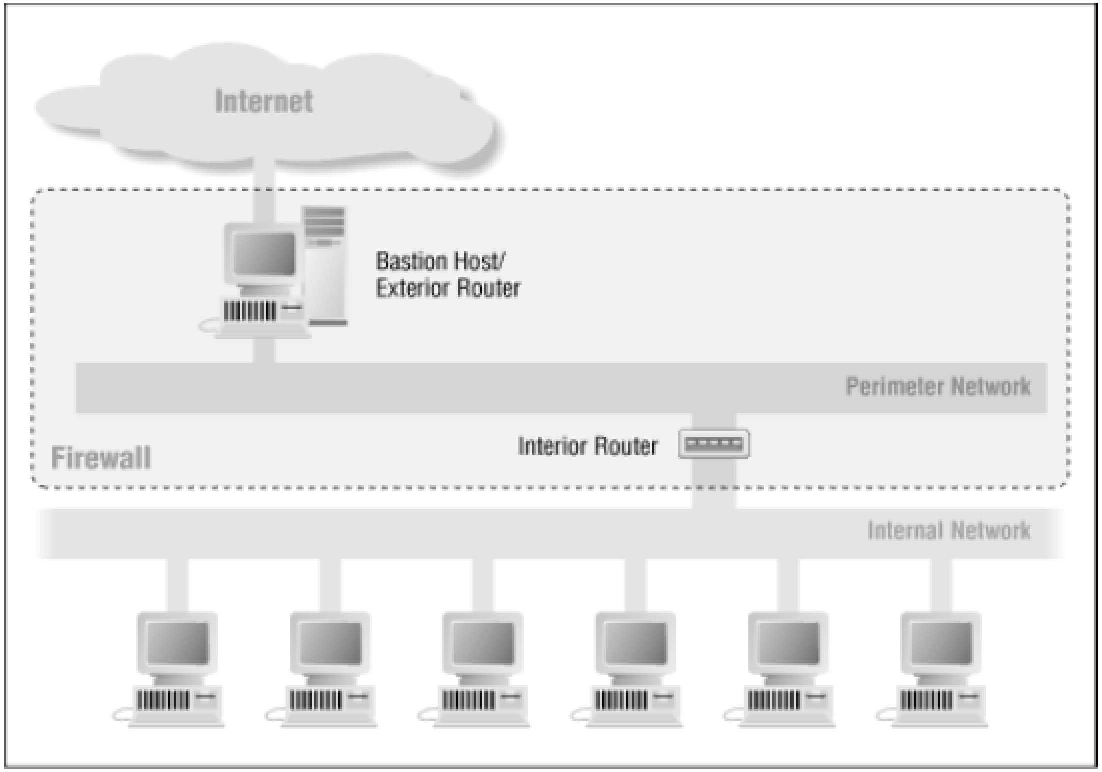
Multiple Bastion Hosts



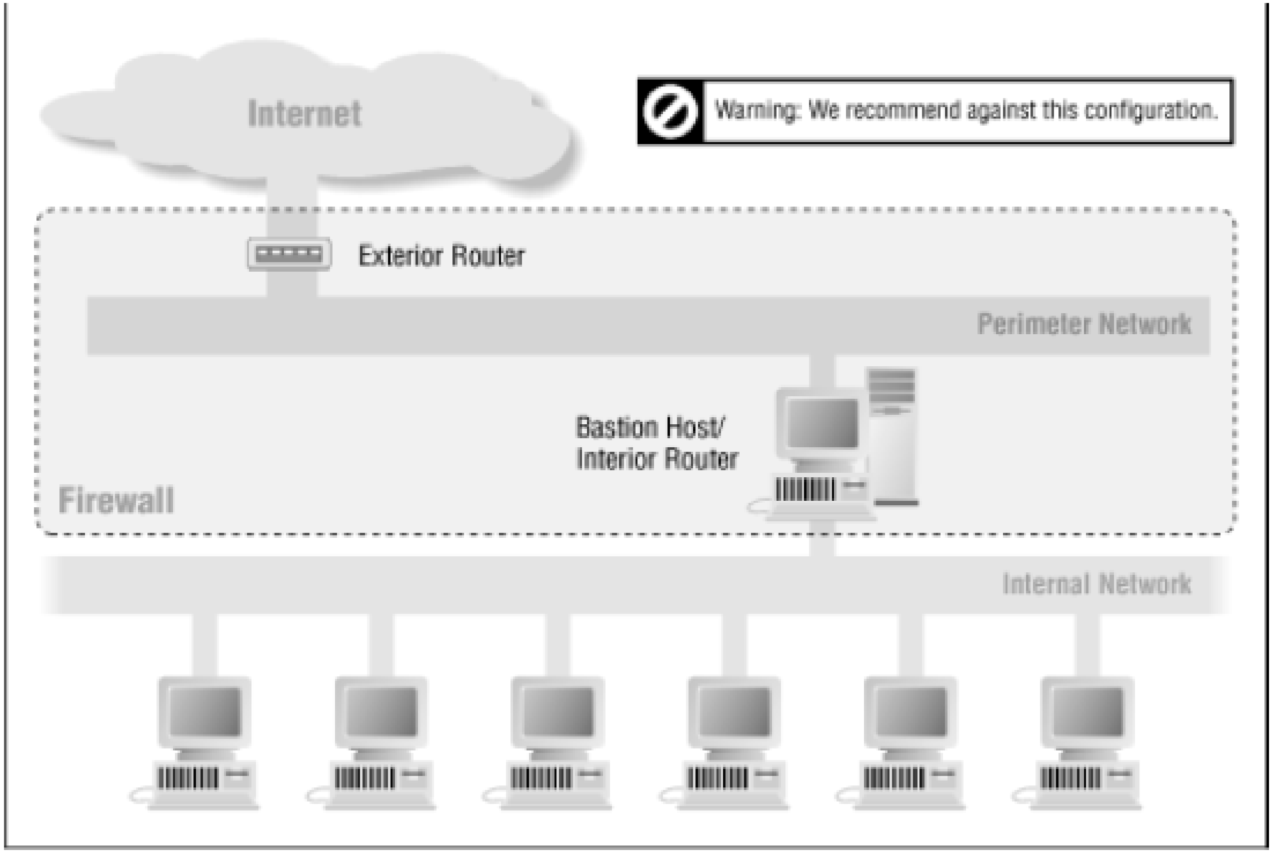
Merge the Interior Router and the Exterior Router



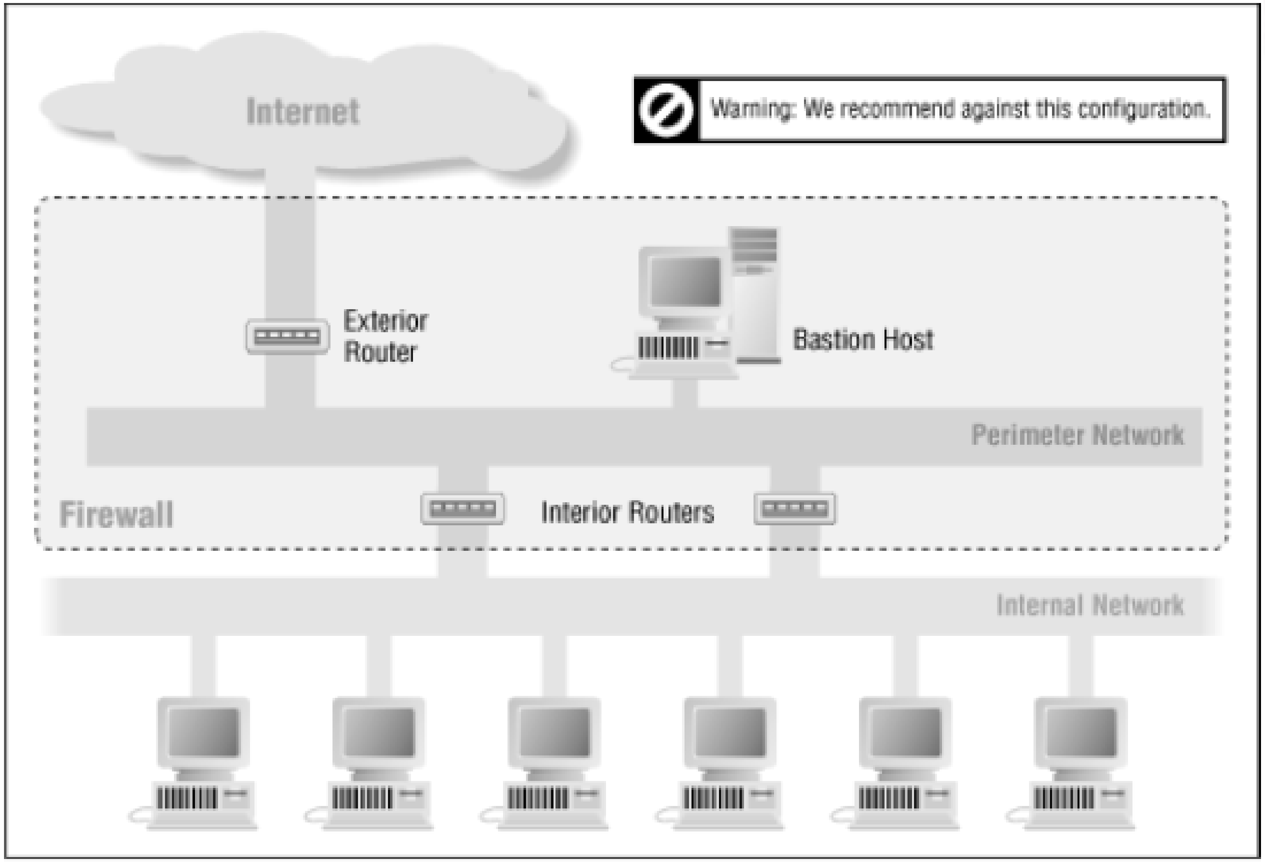
Merge Bastion Host and the Exterior Router



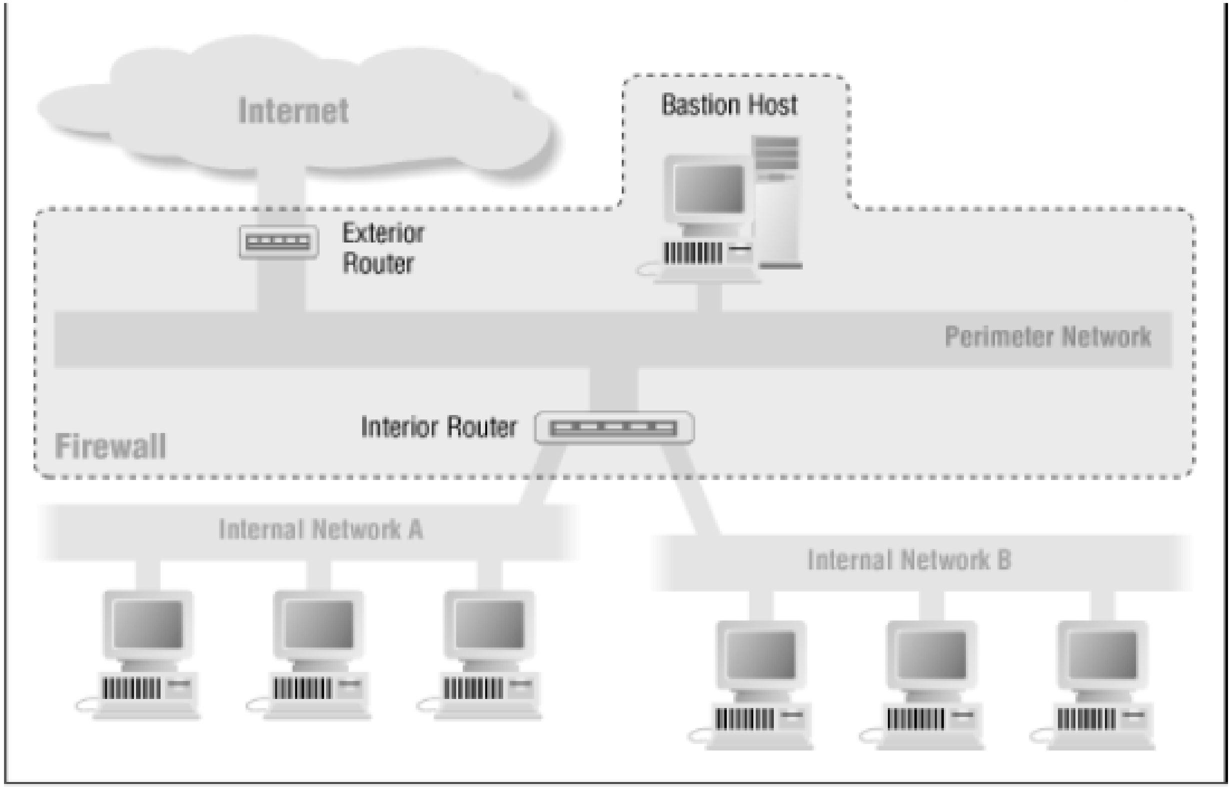
Merge Bastion Host and the Interior Router



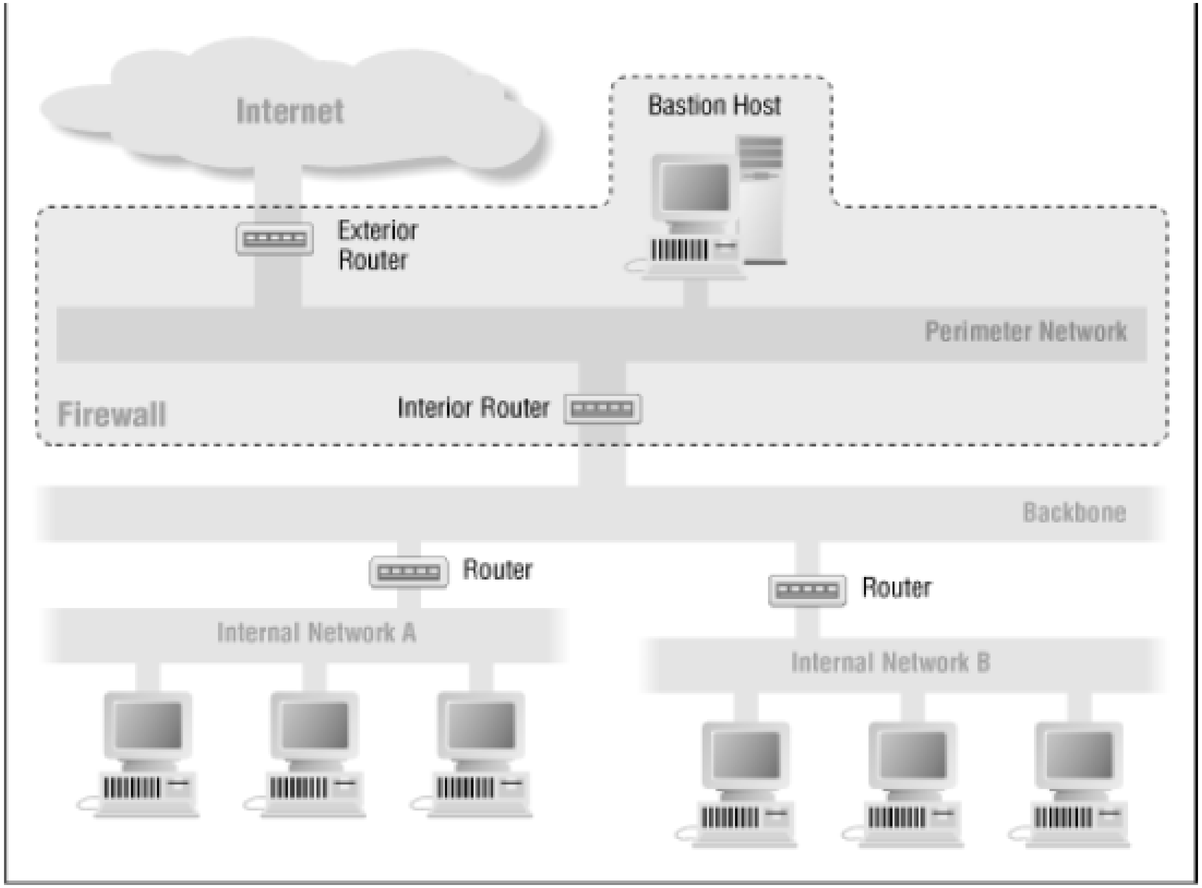
Multiple Interior Router



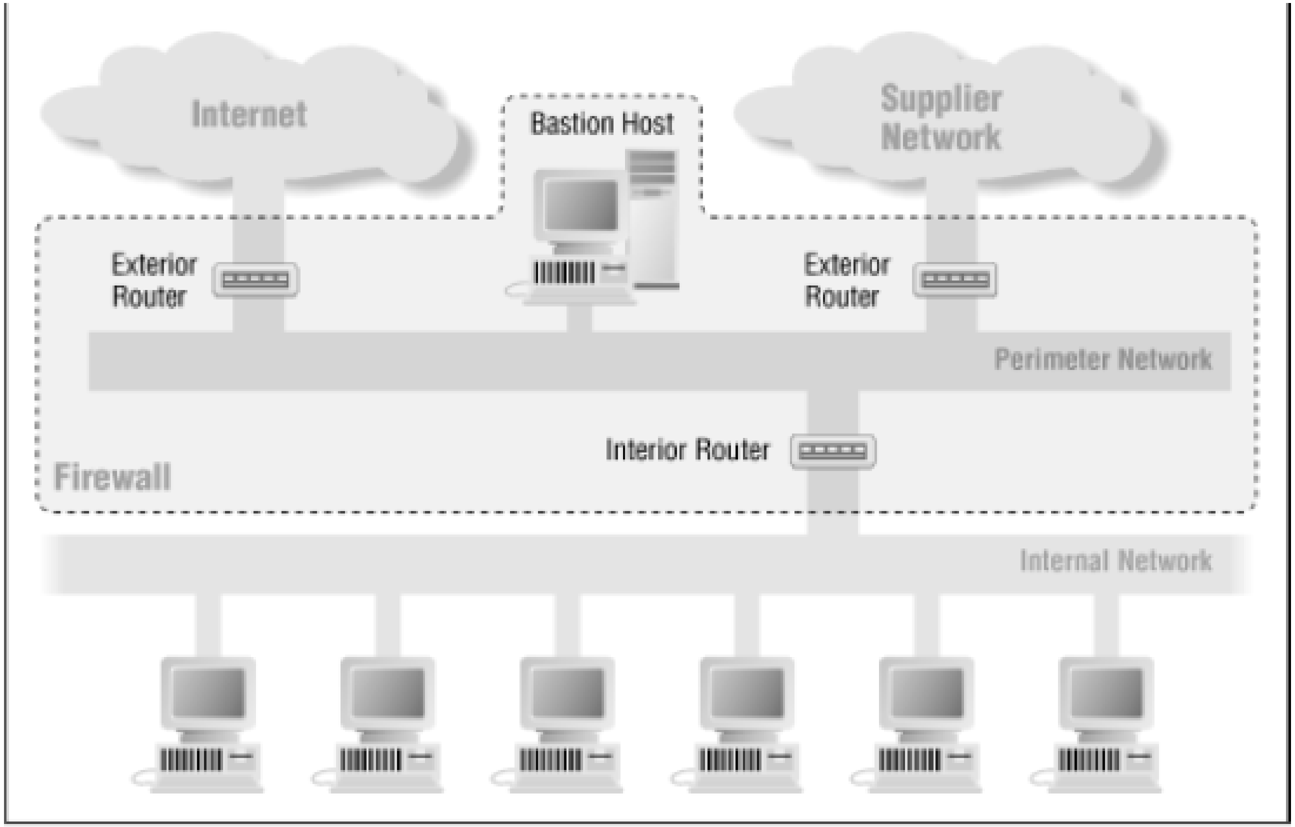
Multiple Internal Networks (separate interfaces in a single router)



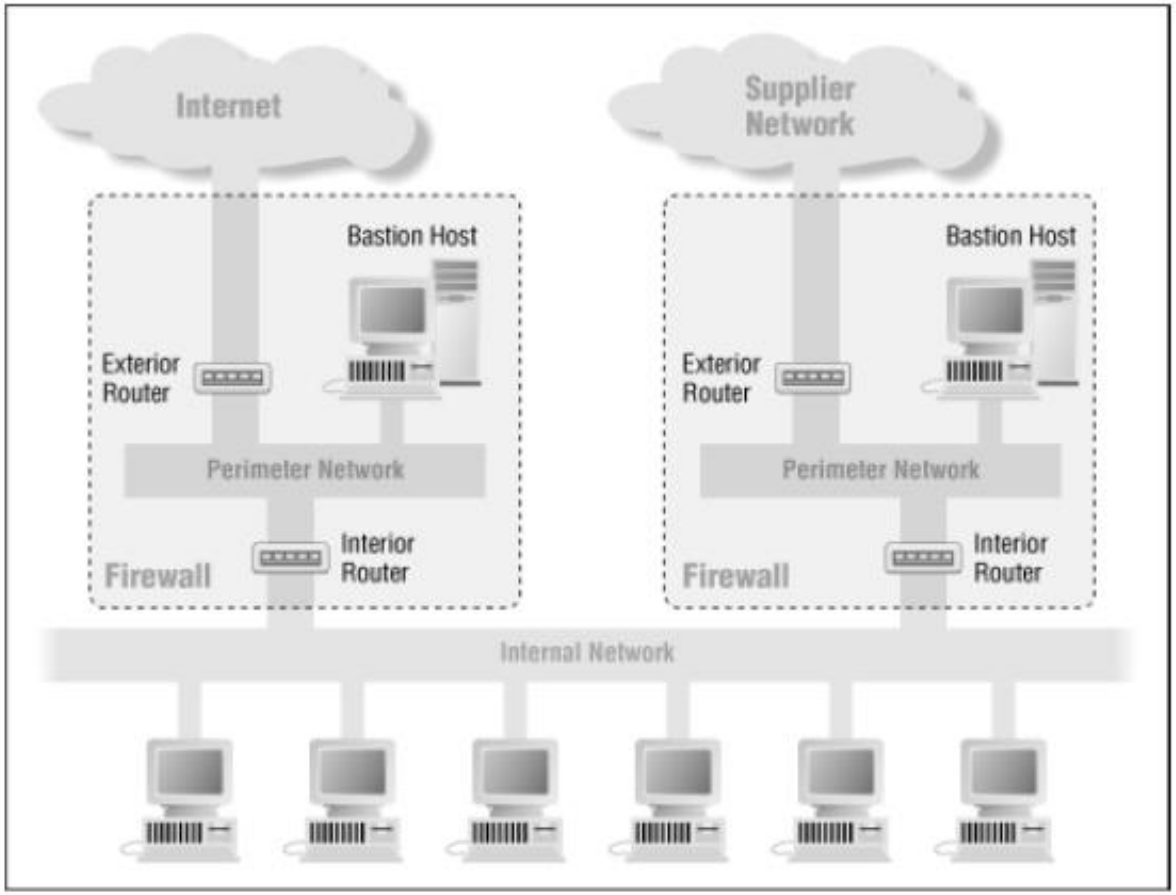
Multiple Internal Networks (backbone architecture)



Multiple Exterior Routers



Multiple Perimeter Networks



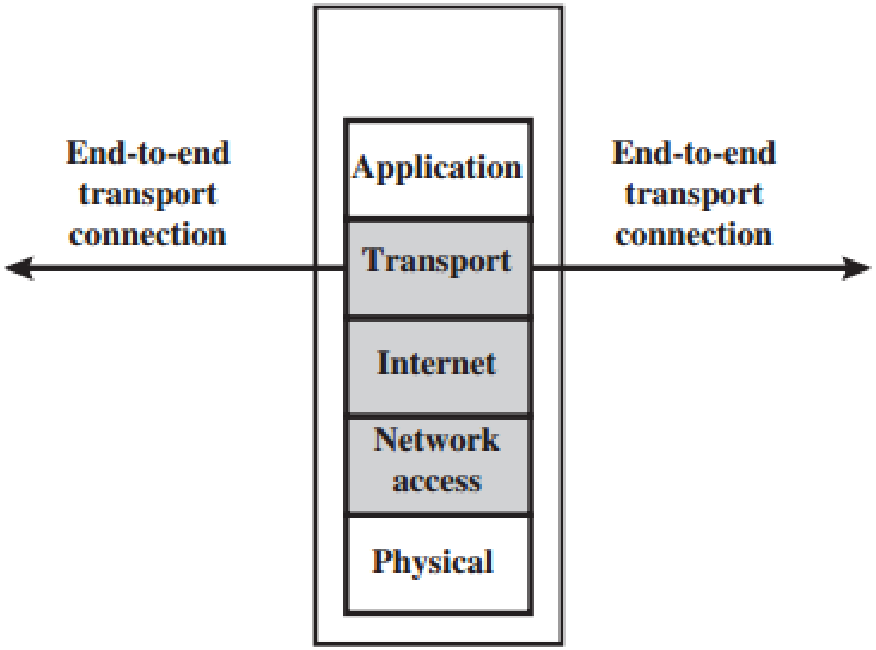
Classification of Firewall

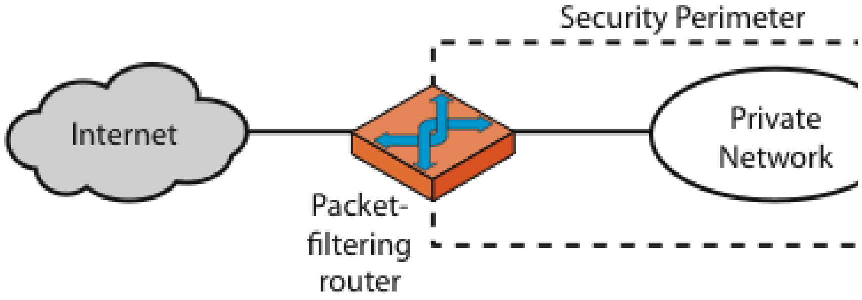
Characterized by **protocol level** it controls in

- Packet filters
- Circuit gateways
- Application gateways
- Dynamic packet filters

Firewalls – Packet Filters

- Packet filtering is generally accomplished using Access Control Lists (ACL) on routers or switches and are normally very fast.


End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection



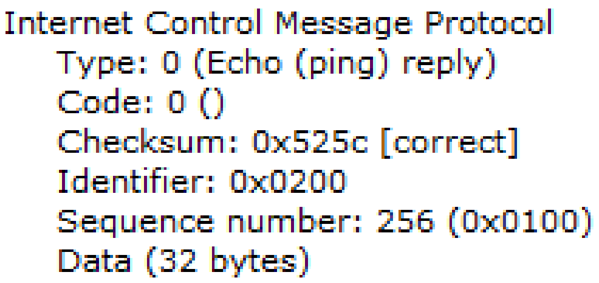
(a) Packet-filtering router

Firewalls – Packet Filters

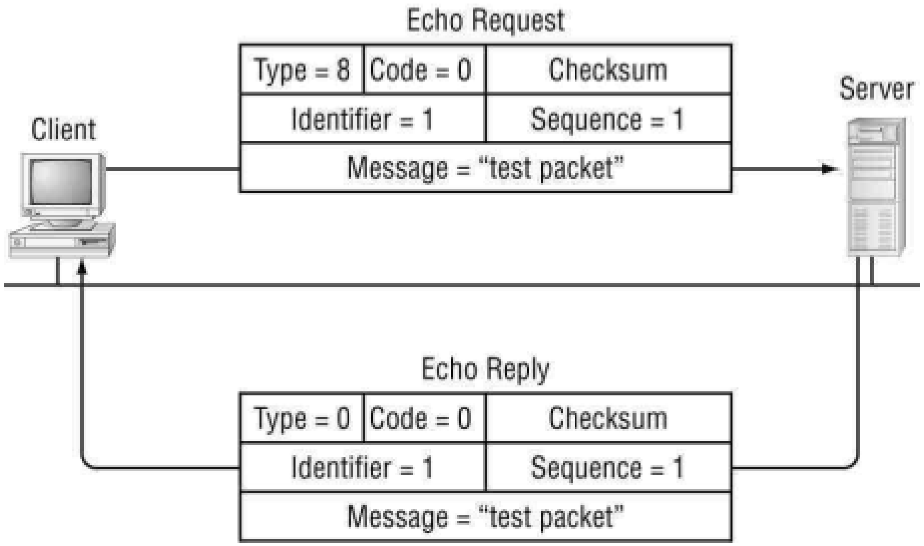
- Simplest, fastest firewall component
- Uses transport-layer information only (no context)
  - IP Source Address, Destination Address
  - Protocol/Next Header (TCP, UDP, ICMP, etc)
  - **TCP or UDP source & destination ports**
  - TCP Flags (SYN, ACK, FIN, RST, PSH, etc)
  - ICMP message type
- Permit or deny according to rules
- Possible default policies
  - that not expressly permitted is prohibited
  - that not expressly prohibited is permitted

ICMP

- Internet Control Message Protocol
  - are typically used for diagnostic or control purposes or generated in response to errors in IP operations.
- Two major types used to Ping
  - Echo Request (8)
  - Echo Reply (0)



```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0 ()
    Checksum: 0x525c [correct]
    Identifier: 0x0200
    Sequence number: 256 (0x0100)
    Data (32 bytes)
```

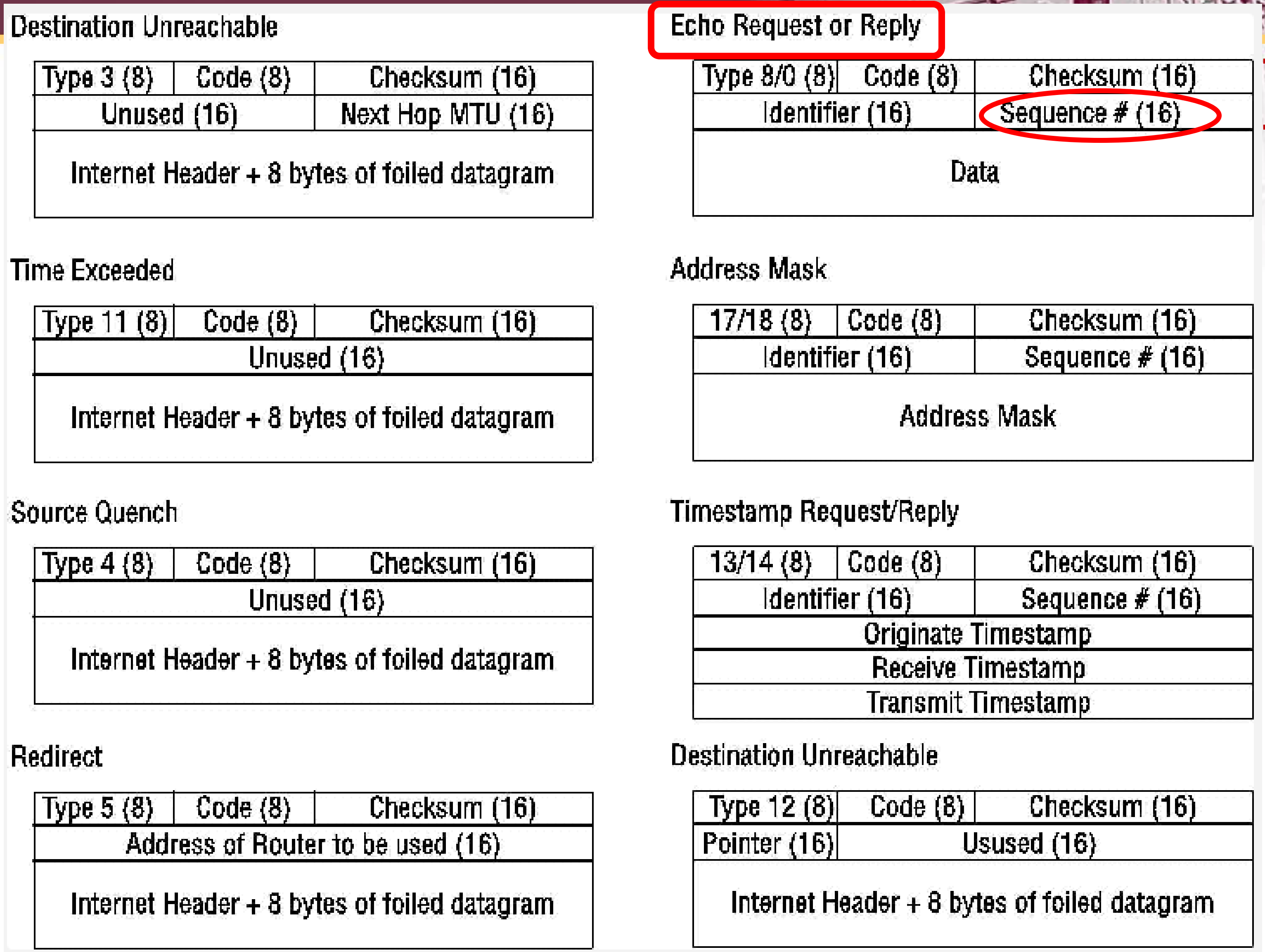


Echo Request

Type = 8	Code = 0	Checksum
Identifier = 1		Sequence = 1
Message = "test packet"		

Echo Reply

Type = 0	Code = 0	Checksum
Identifier = 1		Sequence = 1
Message = "test packet"		



Destination Unreachable

Type 3 (8)	Code (8)	Checksum (16)
Unused (16)		Next Hop MTU (16)
Internet Header + 8 bytes of foiled datagram		

Time Exceeded

Type 11 (8)	Code (8)	Checksum (16)
Unused (16)		
Internet Header + 8 bytes of foiled datagram		

Source Quench

Type 4 (8)	Code (8)	Checksum (16)
Unused (16)		
Internet Header + 8 bytes of foiled datagram		

Redirect

Type 5 (8)	Code (8)	Checksum (16)
Address of Router to be used (16)		
Internet Header + 8 bytes of foiled datagram		

Echo Request or Reply

Type 8/0 (8)	Code (8)	Checksum (16)
Identifier (16)		Sequence # (16)
Data		

8 Bytes

Address Mask

17/18 (8)	Code (8)	Checksum (16)
Identifier (16)		Sequence # (16)
Address Mask		

Timestamp Request/Reply

13/14 (8)	Code (8)	Checksum (16)
Identifier (16)		Sequence # (16)
Originate Timestamp		
Receive Timestamp		
Transmit Timestamp		

Destination Unreachable

Type 12 (8)	Code (8)	Checksum (16)
Pointer (16)	Usused (16)	
Internet Header + 8 bytes of foiled datagram		

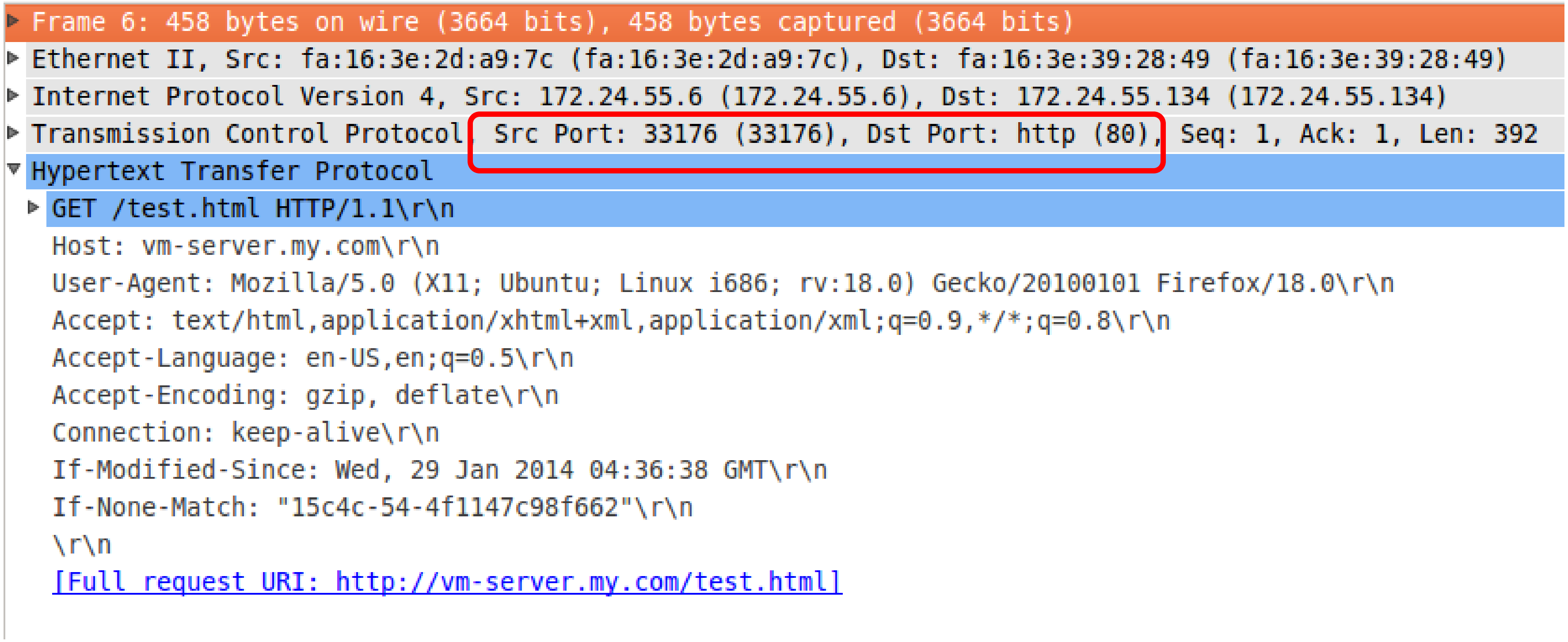
Usage of Packet Filters

- 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

Port Numbering

- TCP connection
  - Server port is number less than 1024
  - Client port is number between 1024 and 16383
- Permanent assignment (common well-known ports)
  - 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

Initial HTTP request for page



```
▶ Frame 6: 458 bytes on wire (3664 bits), 458 bytes captured (3664 bits)
▶ Ethernet II, Src: fa:16:3e:2d:a9:7c (fa:16:3e:2d:a9:7c), Dst: fa:16:3e:39:28:49 (fa:16:3e:39:28:49)
▶ Internet Protocol Version 4, Src: 172.24.55.6 (172.24.55.6), Dst: 172.24.55.134 (172.24.55.134)
▶ Transmission Control Protocol, Src Port: 33176 (33176), Dst Port: http (80), Seq: 1, Ack: 1, Len: 392
▼ Hypertext Transfer Protocol
  ▶ GET /test.html HTTP/1.1\r\n
    Host: vm-server.my.com\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    If-Modified-Since: Wed, 29 Jan 2014 04:36:38 GMT\r\n
    If-None-Match: "15c4c-54-4f1147c98f662"\r\n
    \r\n
    [Full request URI: http://vm-server.my.com/test.html]
```

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

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

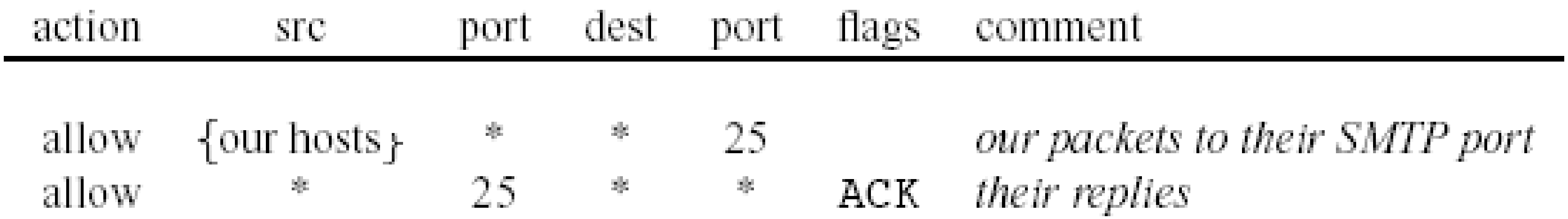
action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

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

- 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.

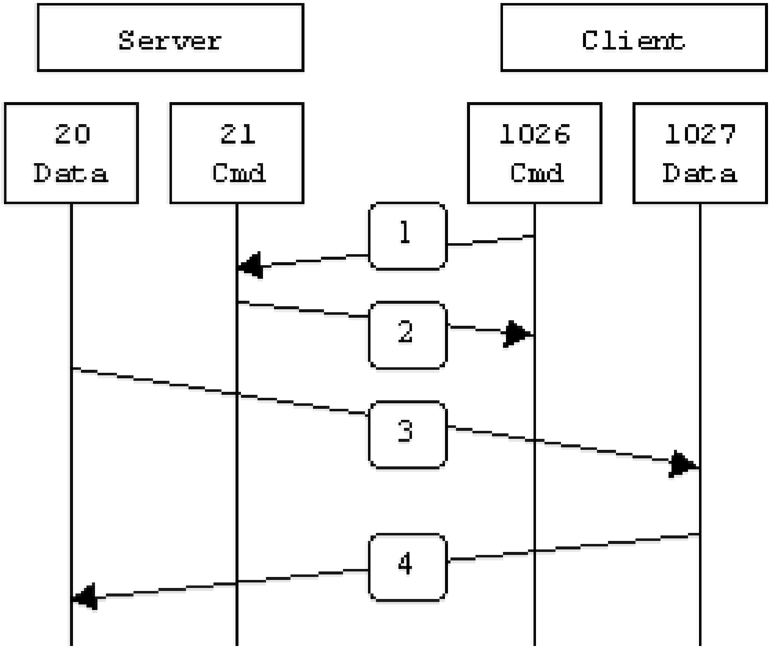
What can be a better solution ?



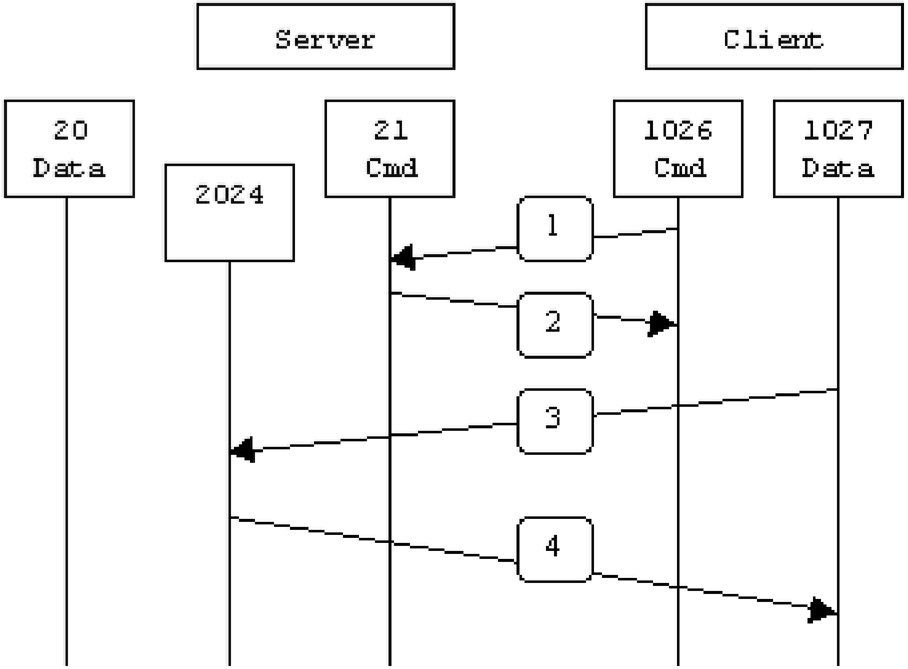
action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		*our packets to their SMTP port*
allow	*	25	*	*	ACK	*their replies*

- 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

Active vs. Passive FTP



Active FTP



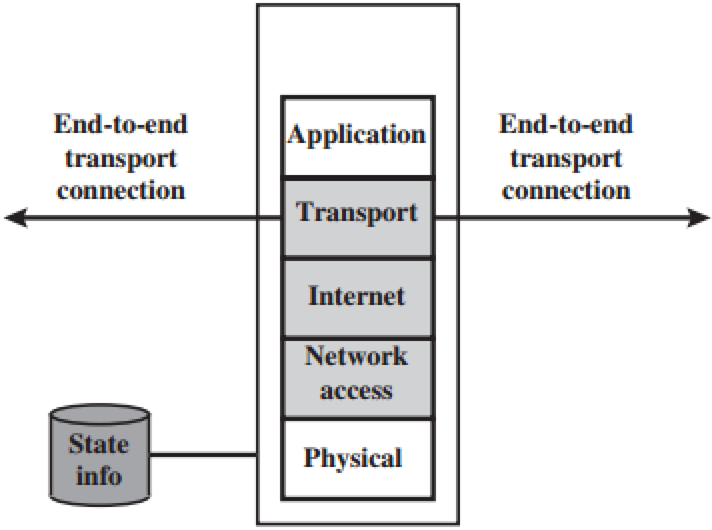
Passive FTP

Attacks on Packet Filters

- IP address spoofing
  - Fake source address to be trusted
  - Solution: add filters on router to block
- Tiny fragment attacks
  - Split TCP header info over several tiny packets
  - Solution: either discard or reassemble before check
- Source routing attacks
  - attacker sets a route other than default
  - block source routed packets

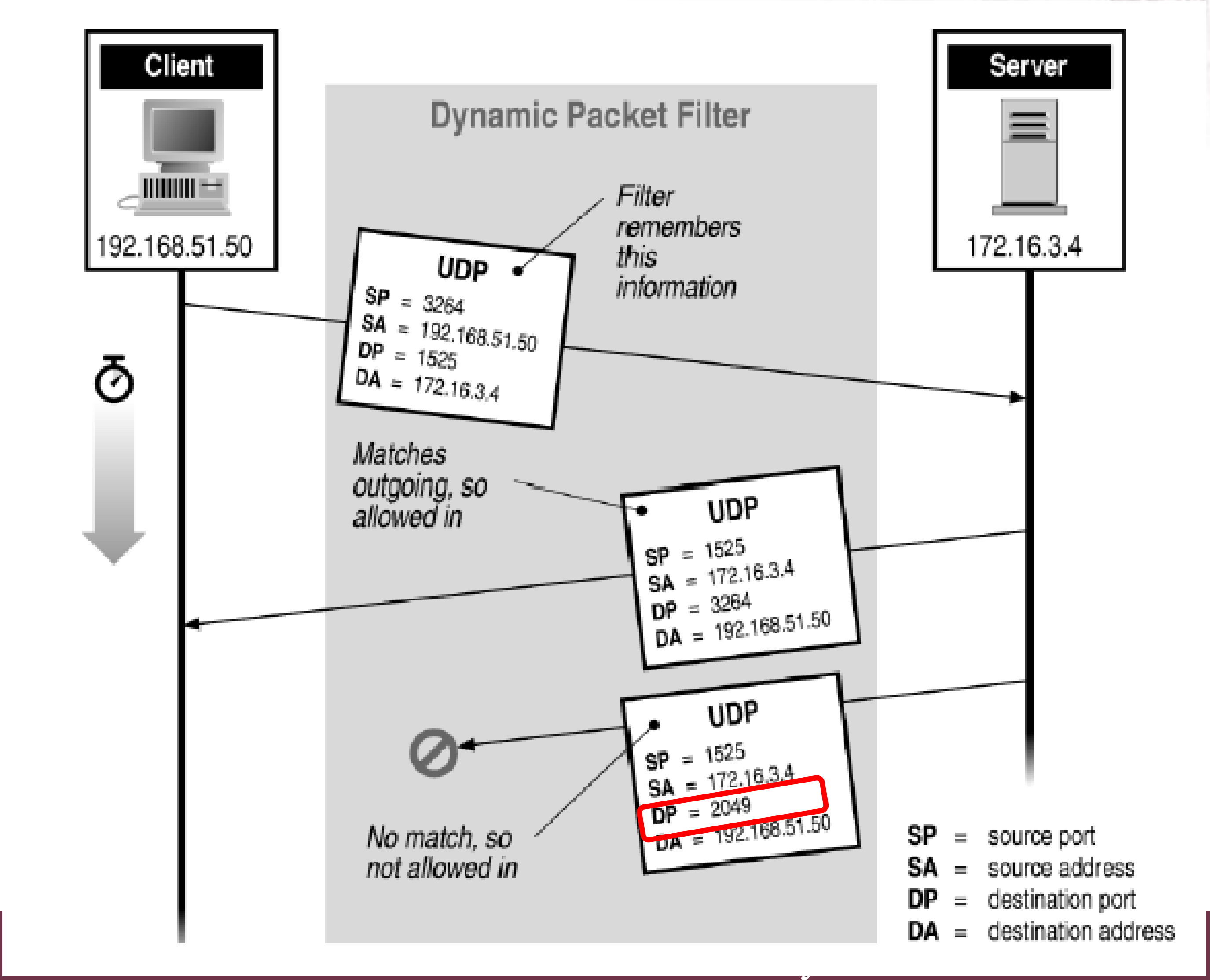
Stateful Packet Filters (iptables)

- Traditional packet filters do not examine higher layer context
  - i.e., matching return packets with outgoing flow
- 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


End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection
State info

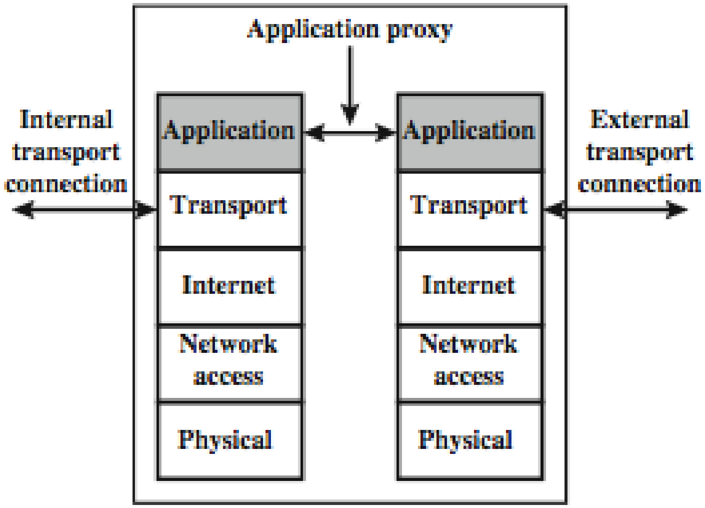
(c) Stateful inspection firewall

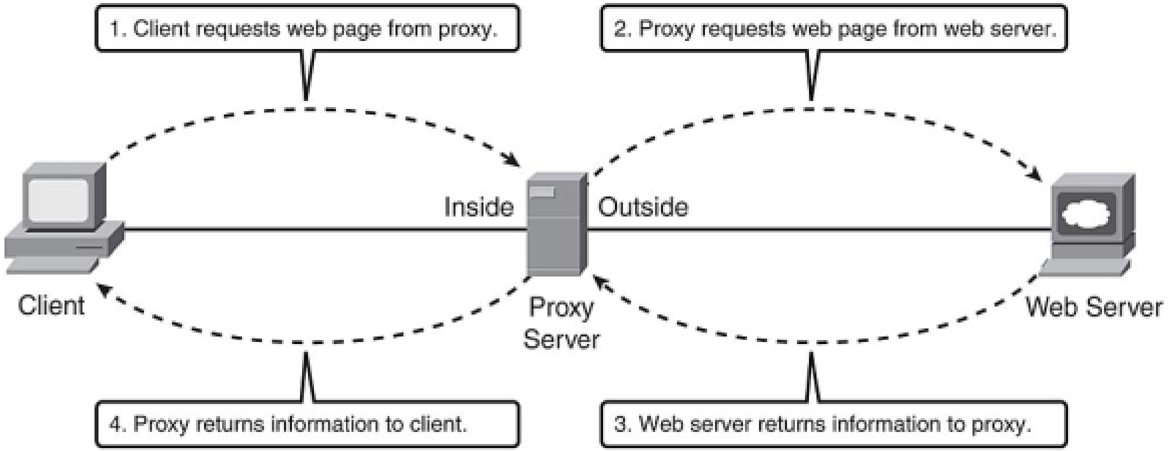
Stateful Filtering



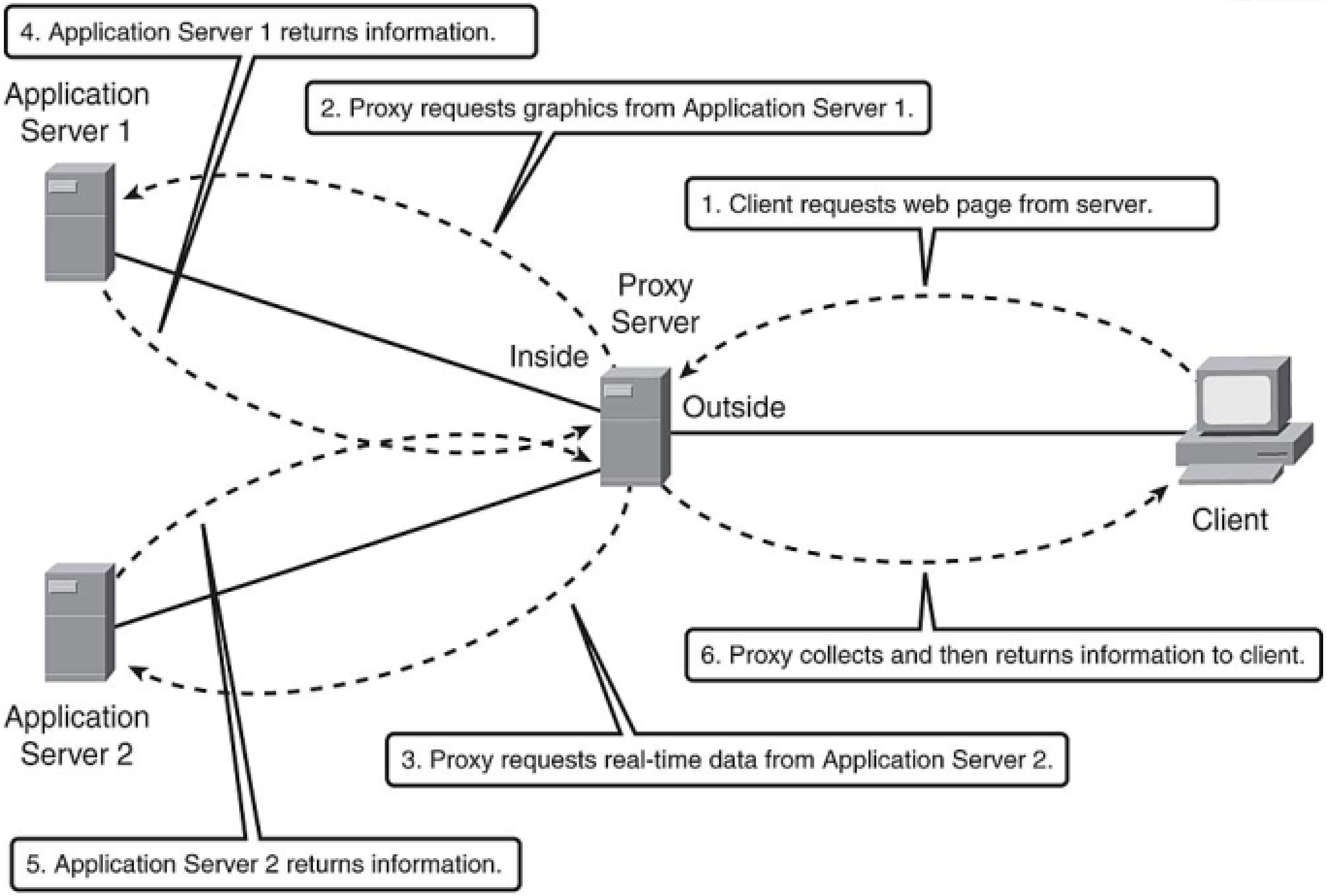
Firewalls - Application Level Gateway (or Proxy)

- Tailored to application layer protocol, e.g., http, ftp, smtp, etc.




1. Client requests web page from proxy.
2. Proxy requests web page from web server.
Inside
Outside
Client
Proxy Server
Web Server
4. Proxy returns information to client.
3. Web server returns information to proxy.

Reverse Proxy



4. Application Server 1 returns information.

2. Proxy requests graphics from Application Server 1.

1. Client requests web page from server.

6. Proxy collects and then returns information to client.

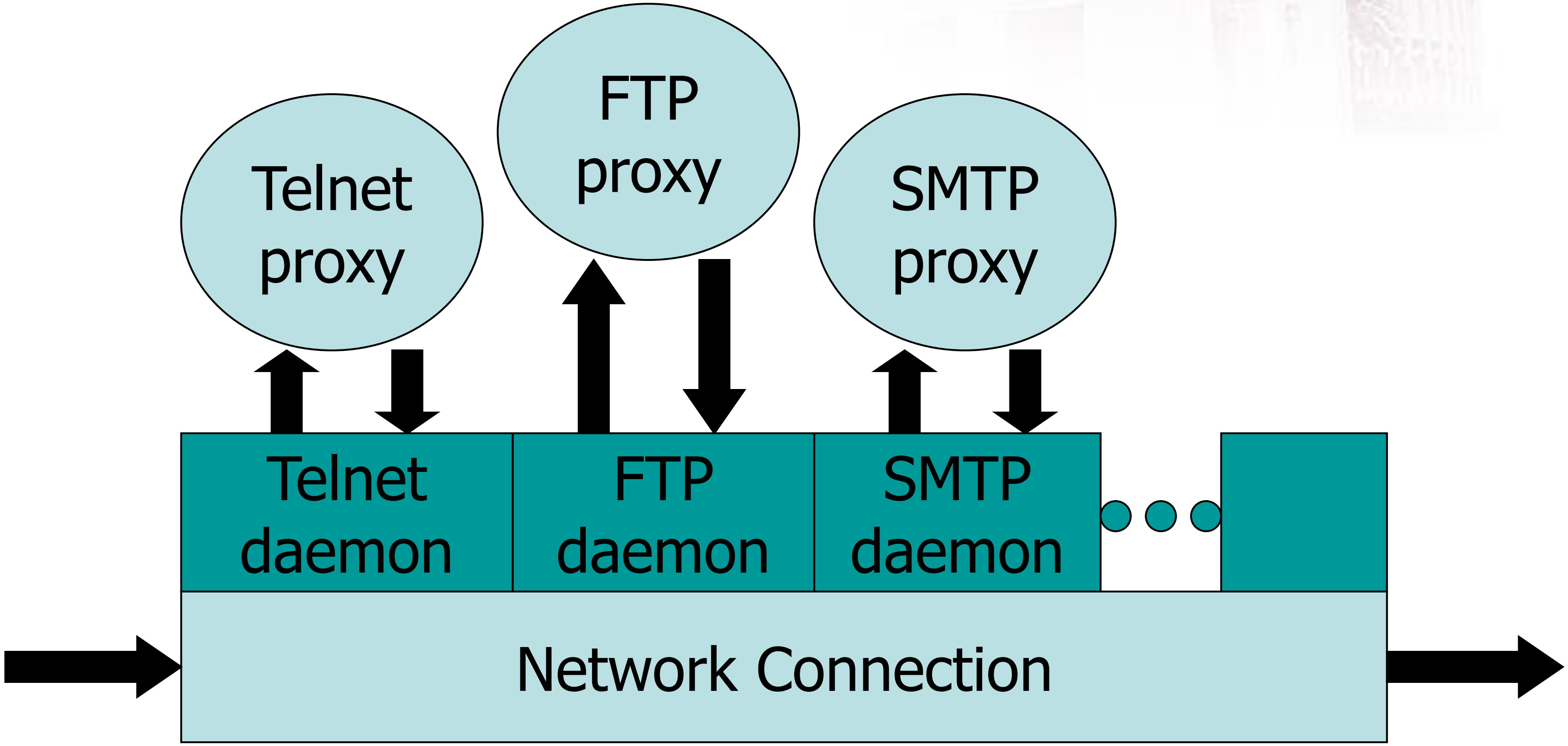
3. Proxy requests real-time data from Application Server 2.

5. Application Server 2 returns information.

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
- Proxy protects clients from malicious and outside attacks, but also make itself vulnerable to application attacks.

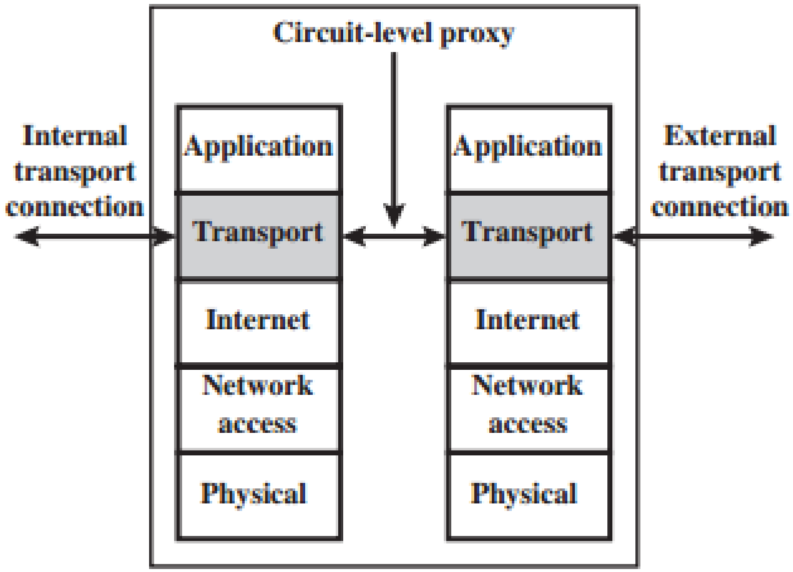
App-level Firewall Architecture

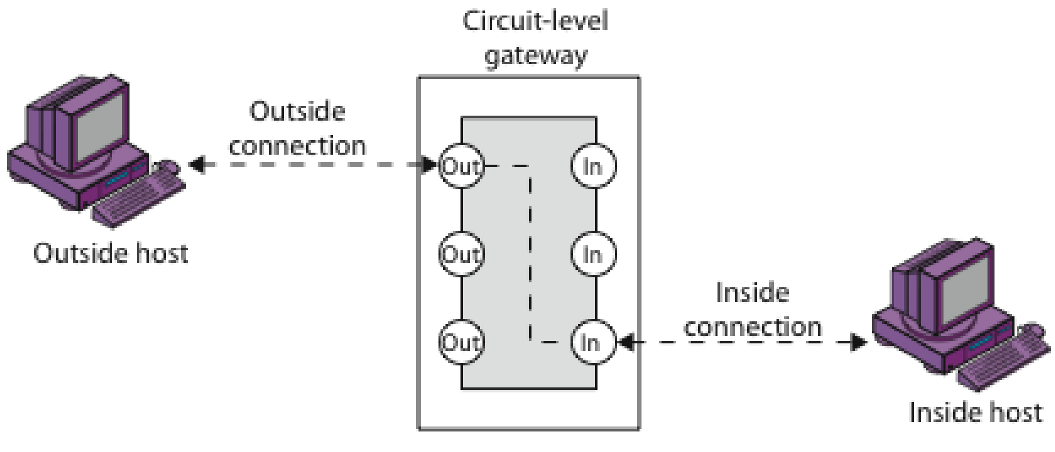


- Daemon spawns proxy when communication detected …
- Additional processing overhead on each connection.

Firewalls - Circuit Level Gateway

- Relay two TCP connections
- Once allowed, it just relays traffic without examining contents
- Typically used for outbound connection from trusted internal users
- SOCKS (socket secure) is commonly used

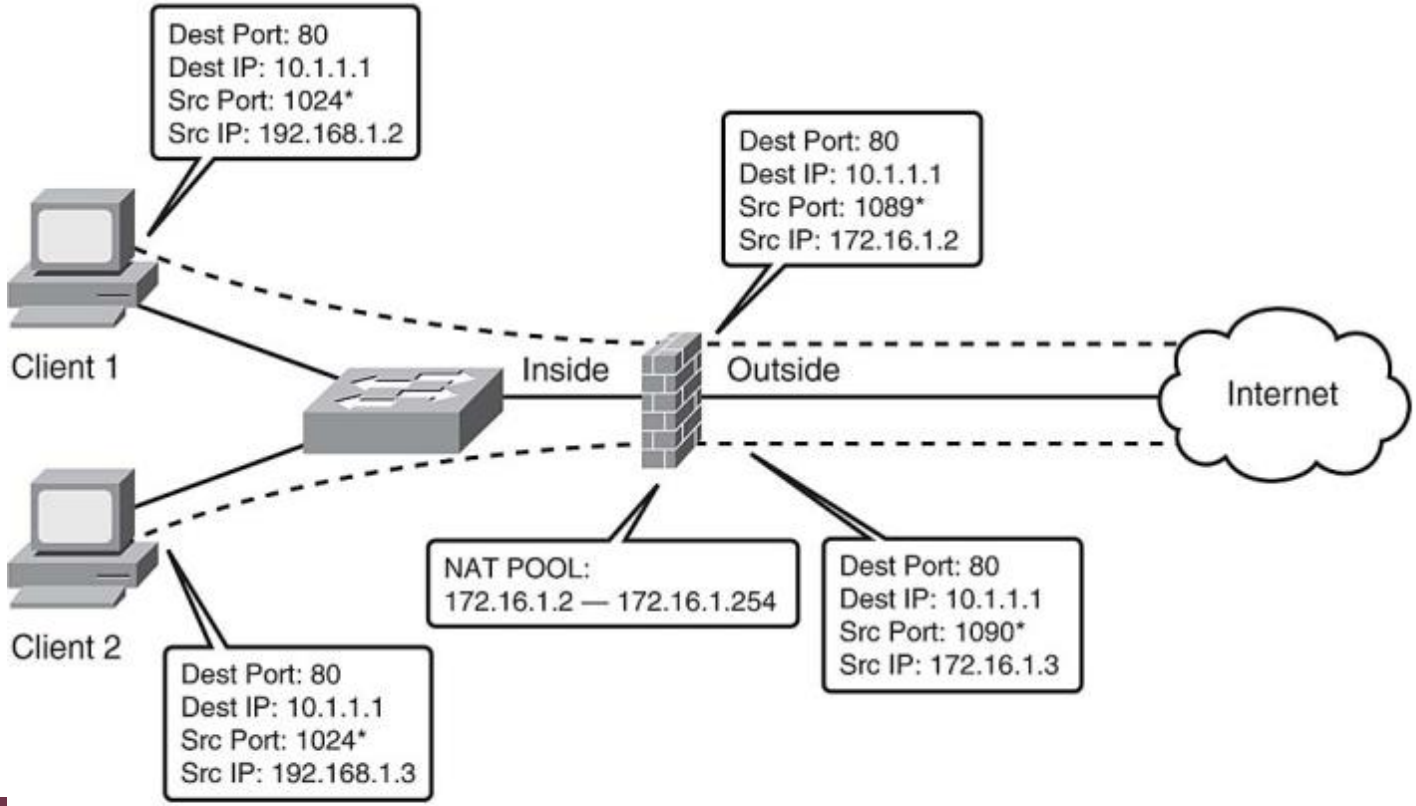




(c) Circuit-level gateway

NAT (Network Address Translation)

- Maps private IP addresses into public IP address
  - One-to-one mapping



Dest Port: 80
Dest IP: 10.1.1.1
Src Port: 1024*
Src IP: 192.168.1.2

Dest Port: 80
Dest IP: 10.1.1.1
Src Port: 1089*
Src IP: 172.16.1.2

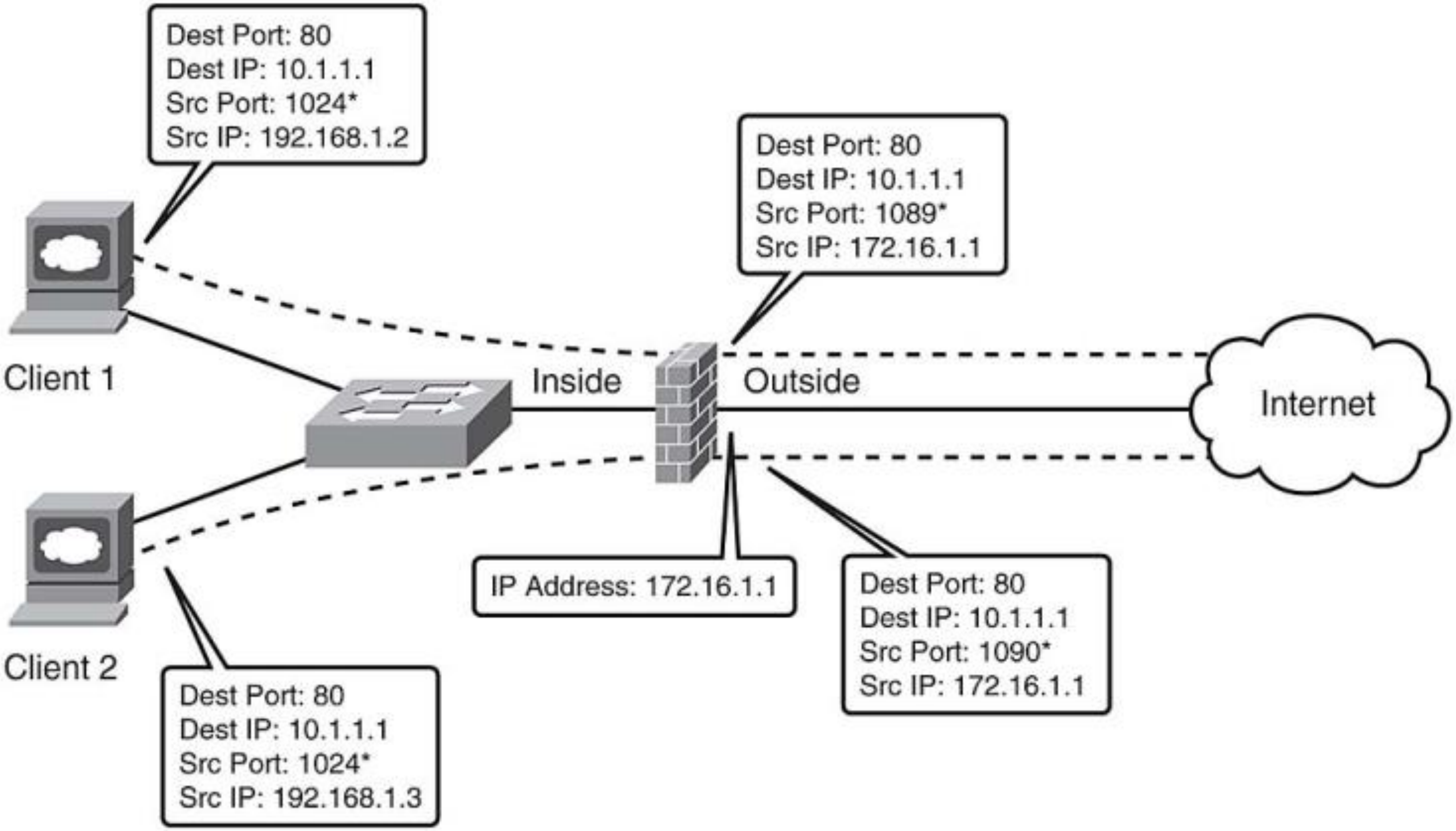
NAT POOL:
172.16.1.2 — 172.16.1.254

Dest Port: 80
Dest IP: 10.1.1.1
Src Port: 1090*
Src IP: 172.16.1.3

Dest Port: 80
Dest IP: 10.1.1.1
Src Port: 1024*
Src IP: 192.168.1.3

PAT (Port Address Translation)

- Maps many private IP address into one public IP address, but different port.


Dest Port: 80
Dest IP: 10.1.1.1
Src Port: 1024*
Src IP: 192.168.1.2
Dest Port: 80
Dest IP: 10.1.1.1
Src Port: 1089*
Src IP: 172.16.1.1
Client 1
Inside
Outside
Internet
Client 2
IP Address: 172.16.1.1
Dest Port: 80
Dest IP: 10.1.1.1
Src Port: 1090*
Src IP: 172.16.1.1
Dest Port: 80
Dest IP: 10.1.1.1
Src Port: 1024*
Src IP: 192.168.1.3