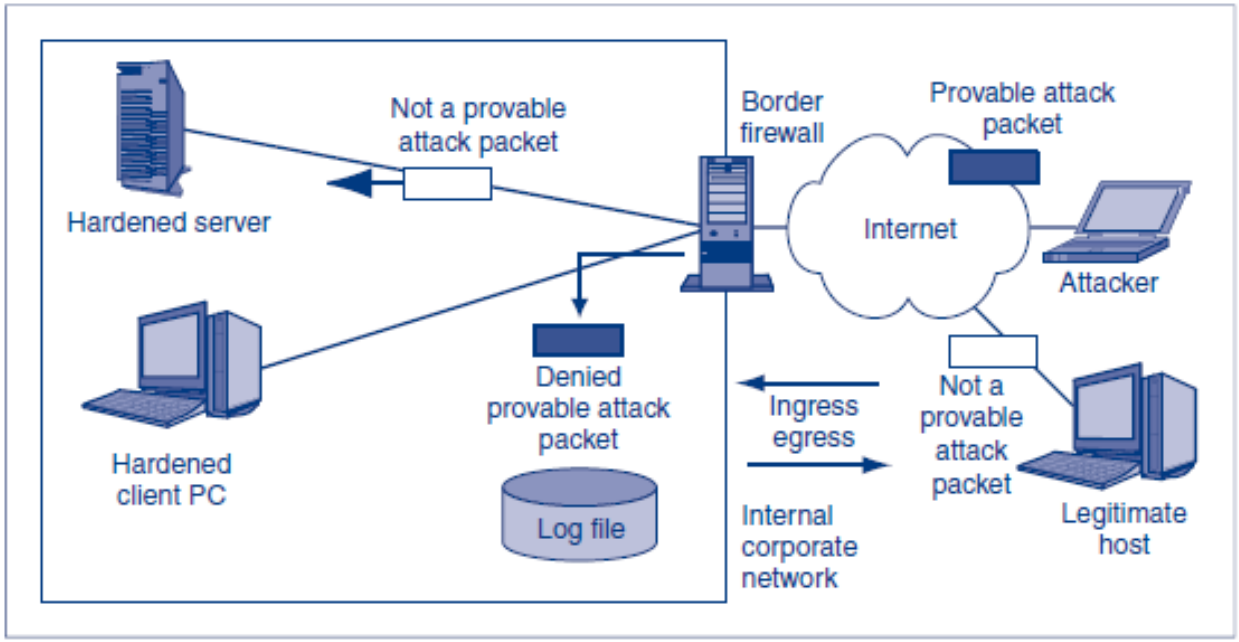
Chapter 15

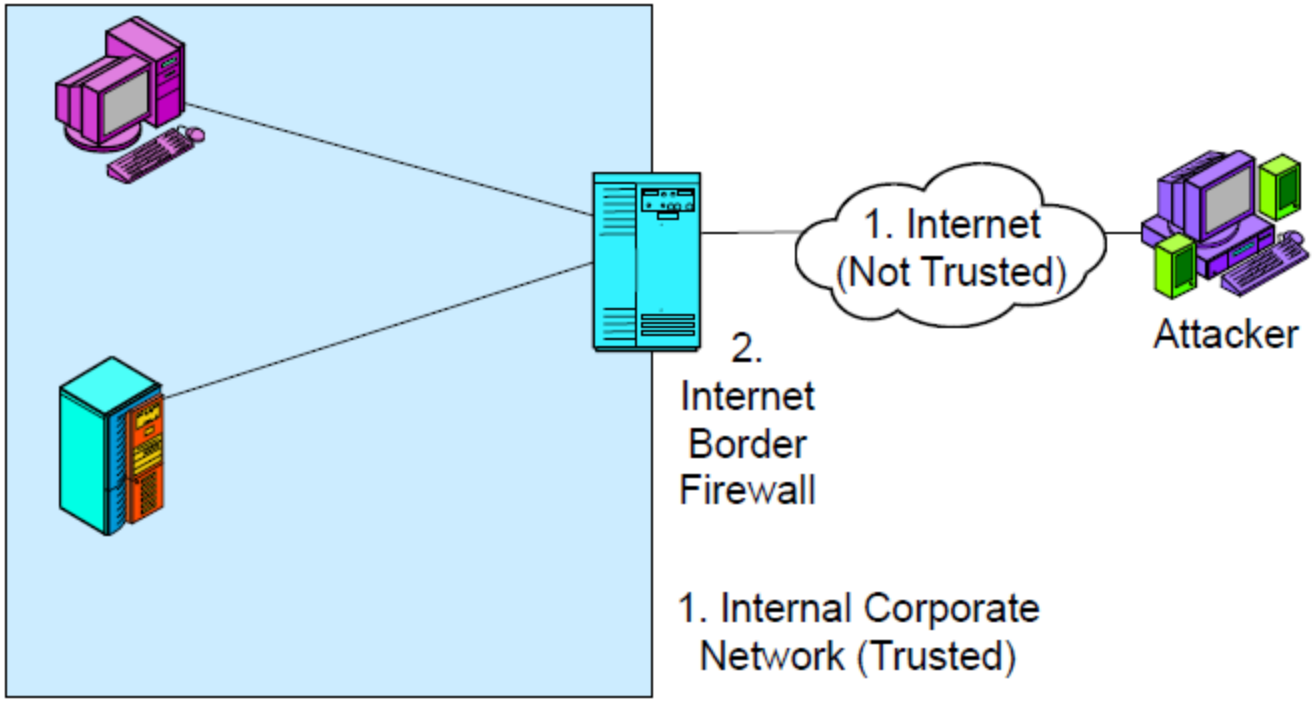
Firewalls, IDS and IPS

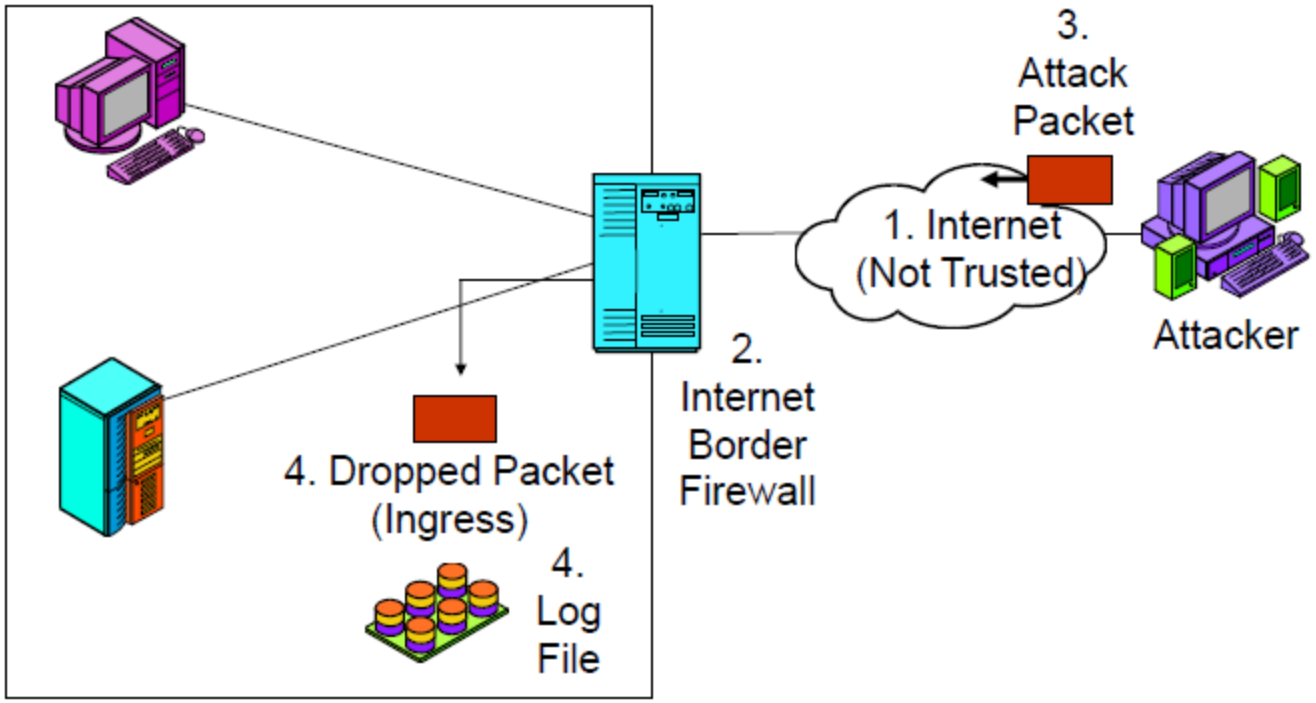
Basic Firewall Operation

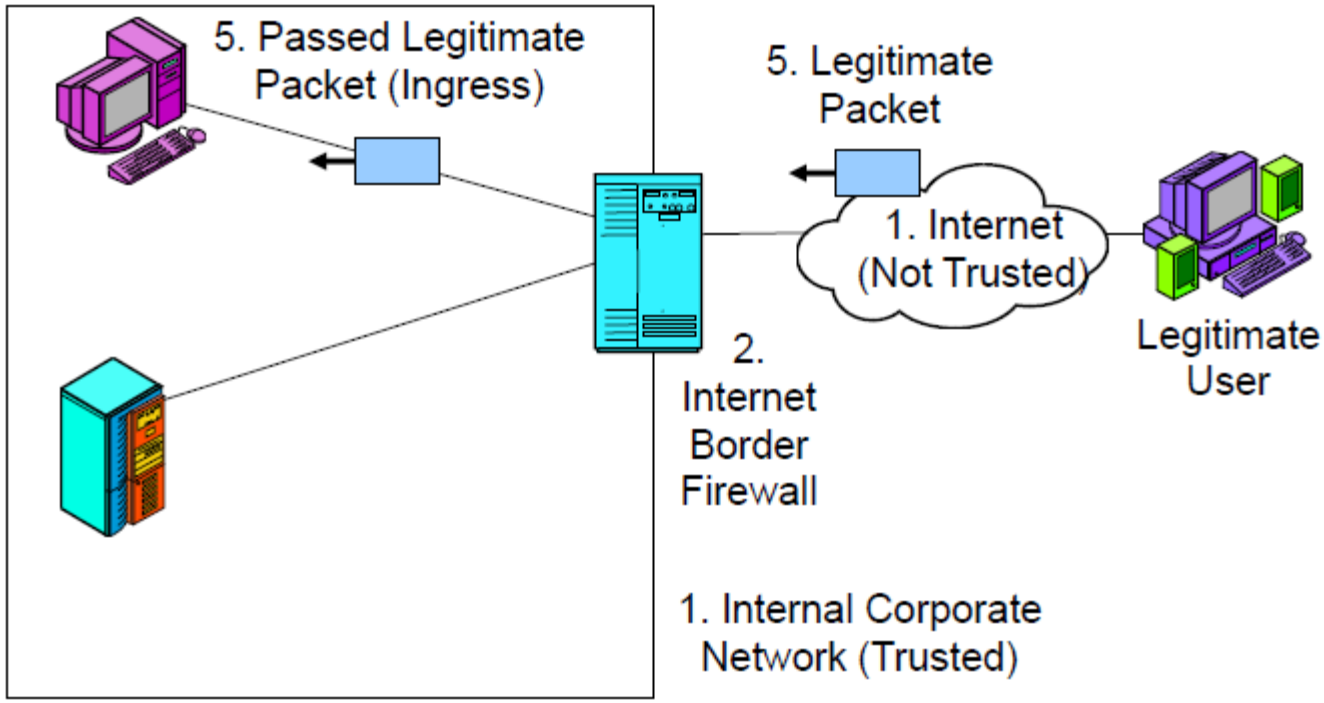


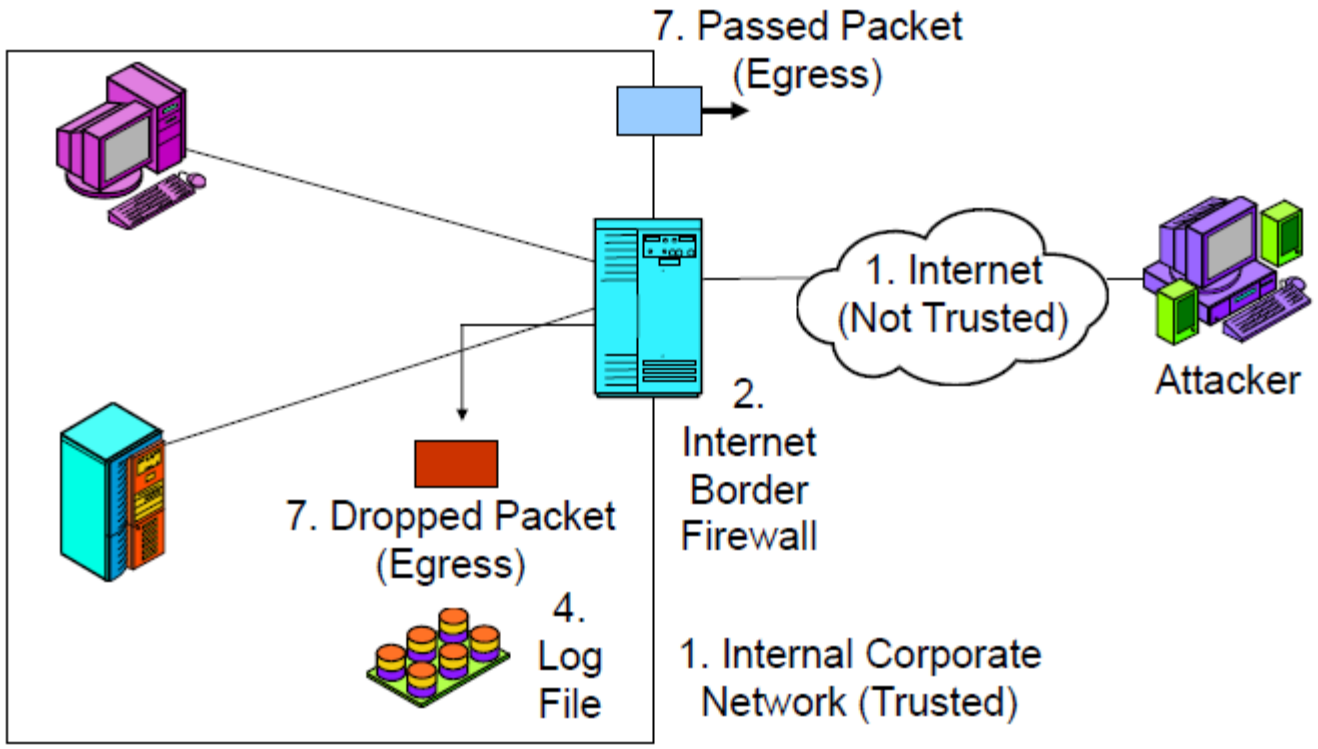
The firewall is a **border firewall.** It sits at the boundary between the corporate site and the external Internet. A firewall examines each packet passing through it.

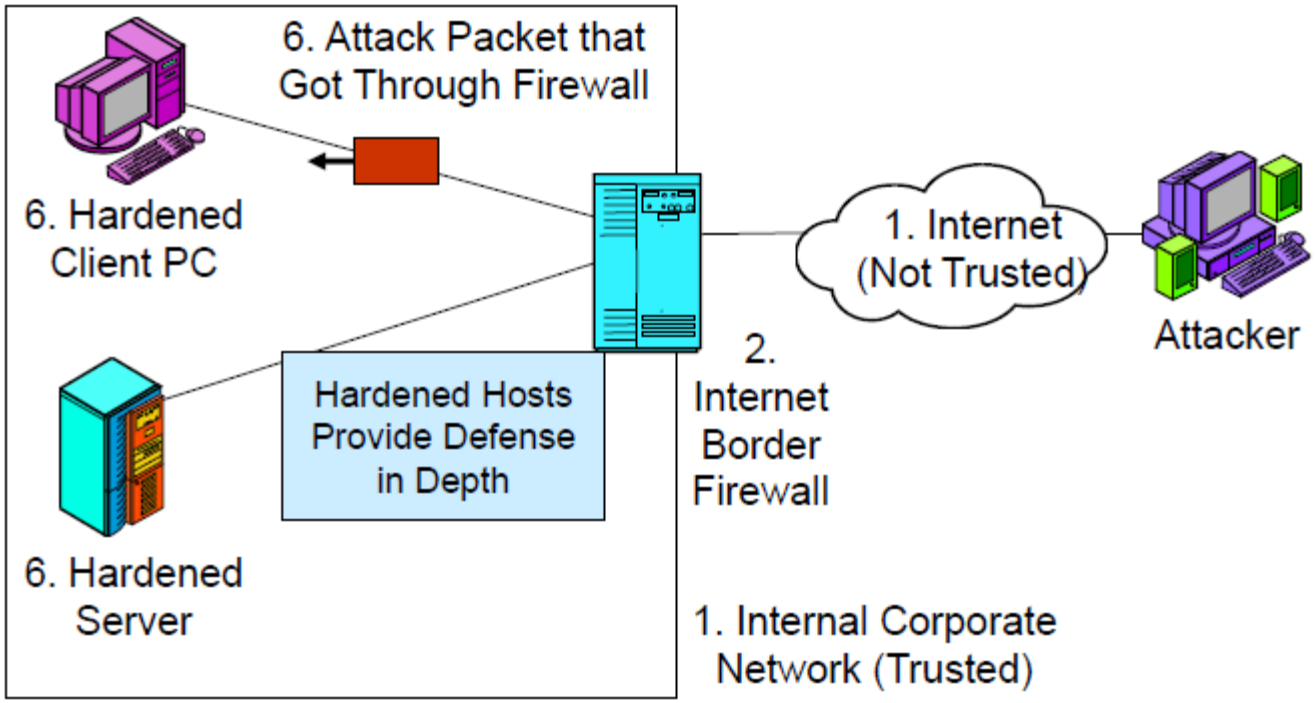
- If the packet is a **provable attack packet**, the firewall drops the packet.
- Firewalls usually record information about each dropped packet in a **log file.** This process is called **logging.**
- If the packet is ***not a provable* attack packet**, the firewall passes the packet on to its destination.
- In firewalls, this is called a **pass/deny decision.**


1. Internet
(Not Trusted)
Attacker
2.
Internet
Border
Firewall
1. Internal Corporate
Network (Trusted)


3.
Attack
Packet
1. Internet
(Not Trusted)
Attacker
2.
Internet
Border
Firewall
4. Dropped Packet
(Ingress)
4.
Log
File


5. Passed Legitimate Packet (Ingress)
5. Legitimate Packet
1. Internet (Not Trusted)
Legitimate User
2. Internet Border Firewall
1. Internal Corporate Network (Trusted)


7. Passed Packet
(Egress)
1. Internet
(Not Trusted)
Attacker
2.
Internet
Border
Firewall
7. Dropped Packet
(Egress)
4.
Log
File
1. Internal Corporate
Network (Trusted)

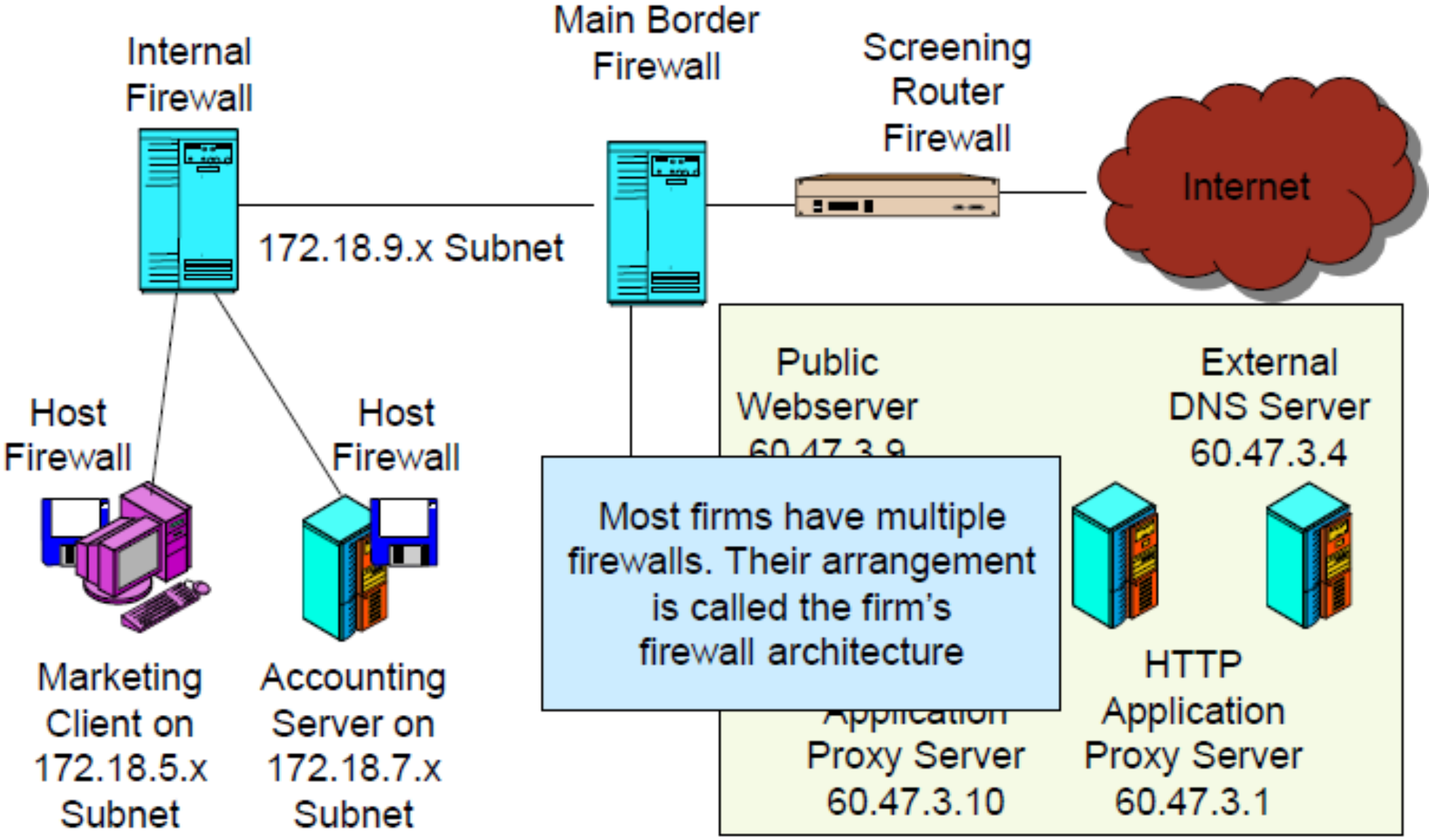

6. Attack Packet that Got Through Firewall
6. Hardened Client PC
1. Internet (Not Trusted)
Attacker
2. Internet Border Firewall
Hardened Hosts Provide Defense in Depth
6. Hardened Server
1. Internal Corporate Network (Trusted)

Ingress and Egress

In **ingress filtering,** the firewall examines packets entering the network from the outside (Internet). The purpose of ingress filtering is to stop attack packets from entering the firm's internal network.

In **egress filtering,** the firewall filters packets when they are leaving the network. This prevents replies to probe packets from leaving the network.

Firewall Architecture (Single Site)



Firewall Principles

- **The Changing Role of Firewalls**
  - In the early 1990s, there was a focus on border security
  - However, some attacks get through the border firewall, and border firewalls provide no protection from internal attackers, attackers who entered the site other than through the Internet, or remote users using VPNs
  - Companies need to employ defense in depth
  - Overall, border firewalls are important but not sufficient.

Firewall Principles (Continued)

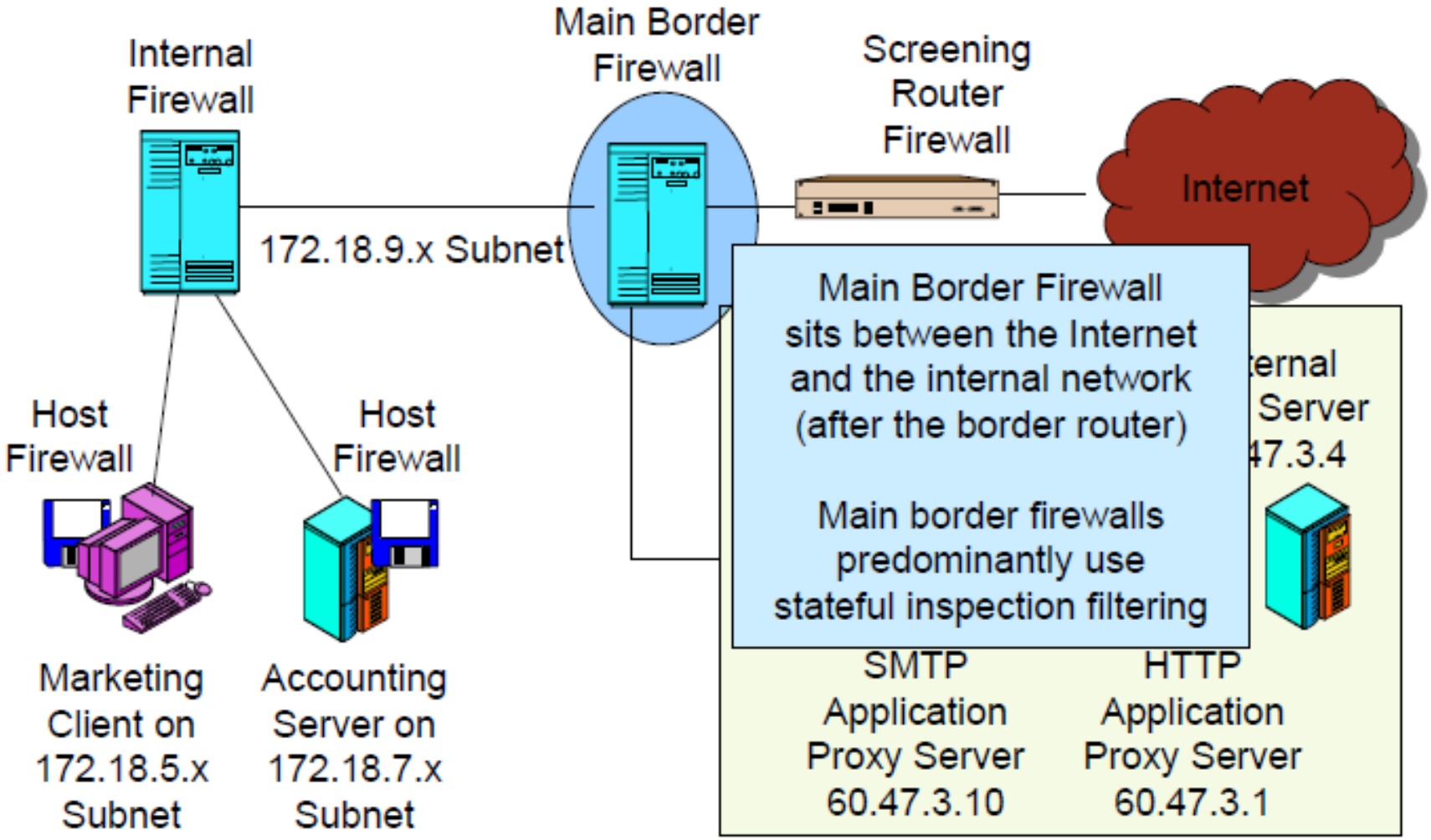
- **Danger of Overload**
  - If a firewall is overloaded and cannot handle the traffic, it drops unprocessed packets
  - This is the safest choice, because attack packets cannot enter the network
  - However, this creates a self-inflicted denial-of-service attack.
  - So firewalls must have the capacity to handle the traffic
  - Some can handle normal traffic but cannot handle traffic during heavy attacks
  - Need to be able to work at wire speed

Firewall Principles (Continued)

- **Firewall Filtering Methods**
  - Firewall Inspection Levels
    - Internet Level
      - Internet and transport layer filtering
      - Attacks and Stateful inspection
      - therefore firewalls began here
      - Static packet inspection
      - Network address translation (NAT)
    - Application Level
      - Attacks growing at the application layer
      - Filter application layer communication
      - Application proxy firewalls
      - Antivirus filtering (general malware filtering)
      - Intrusion prevention systems (also filter internet-level attacks)

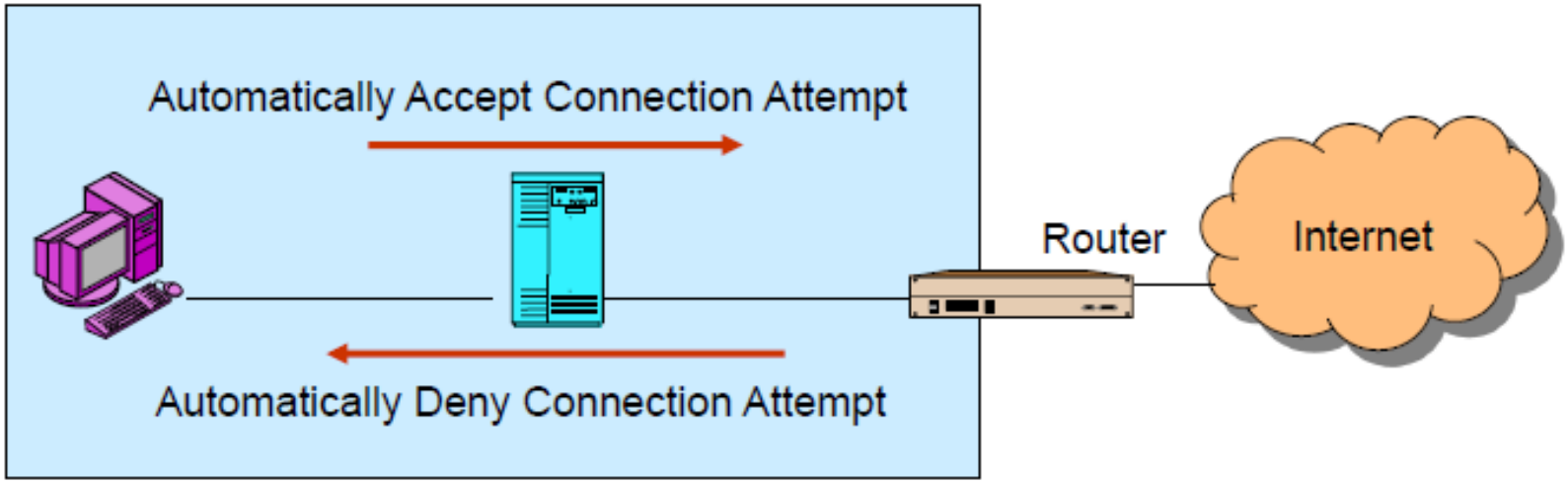
Main Border Firewalls

Firewall Architecture (Single Site)



Opening Connections in Stateful Inspection Firewalls

- **Default Behavior**
  - Permit connections initiated by an internal host
  - Deny connections initiated by an external host
  - Can change default behavior with access control lists (ACLs) for ingress and egress



Permitting Incoming Connections in a Stateful Inspection Firewall

- **Default Behavior Can be Modified by Access Control Lists (ACLs)**
  - Ingress ACL permits some externally-initiated connections to be opened
  - Egress ACL prohibits some internally-initiated connections from being opened
  - On basis of IP address, TCP or UDP port number, and/or IP protocol
  - Sets of **if-then** rules applied in order

Permitting Incoming Connections in a Stateful Inspection Firewall (Ingress ACL)

1. If TCP destination port = 80, Allow Connection
   - *[Pass all HTTP traffic to any webserver. (Port 80 = HTTP)]*
2. If TCP destination port = 25 AND destination IP address = 60.47.3.35, Allow Connection
   - *[Pass all SMTP traffic to a specific host (mail server), 60.47.3.35. Port 25 = SMTP]*
   - Safer than Rule 1
3. Deny ALL
   - *[Deny all other externally-initiated connections]*
   - *(Use the default behavior of stateful inspection firewalls for all other connection-opening attempts)*

Well-Known Port Numbers

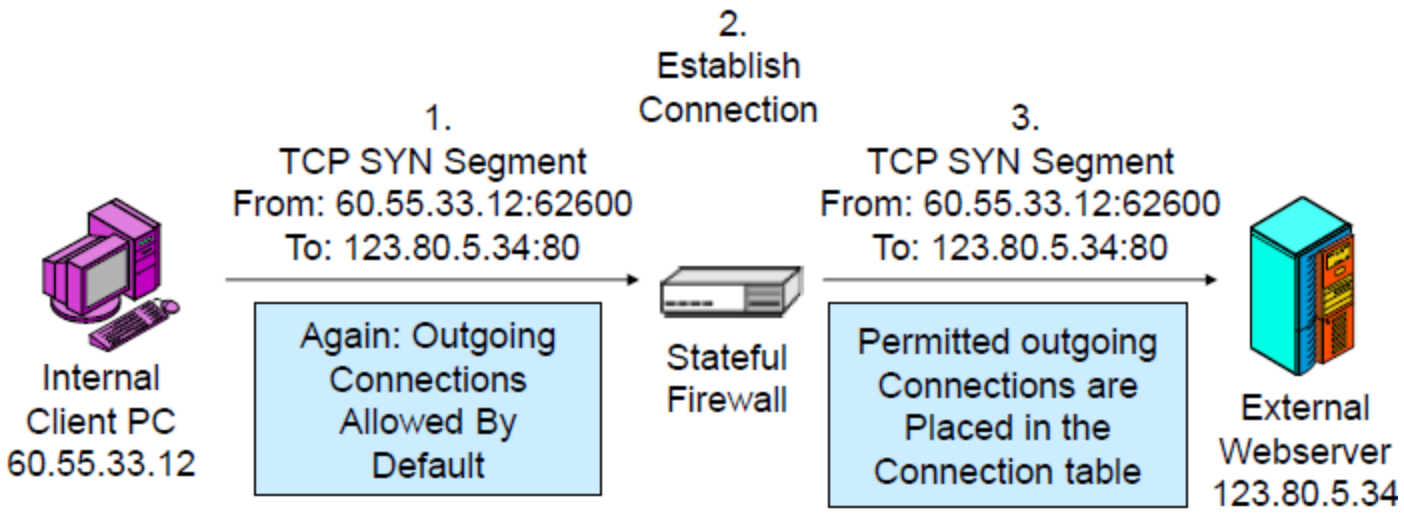
Port Number	Primary Protocol	Application
20	TCP	FTP Data Traffic
23	TCP	Telnet Passwords sent in the clear
25	TCP	Simple Mail Transfer Protocol (SMTP)
53	UDP	Domain Name System (DNS)

Port Number	Primary Protocol	Application
69	UDP	Trivial File Transfer Protocol (TFTP) No login necessary
80	TCP	Hypertext Transfer Protocol (HTTP)
143	TCP	Internet Message Access Protocol (IMAP) for downloading e-mail to client

Main Border Firewall Stateful Inspection I

- **Stateful Firewall Operation**
  - If accept a connection…
  - Record the two IP addresses and port numbers in state table as OK (open)
  - Accept future packets between these hosts and ports with no further inspection
    - This stops most internet-level attacks
    - Does not address application-level attacks

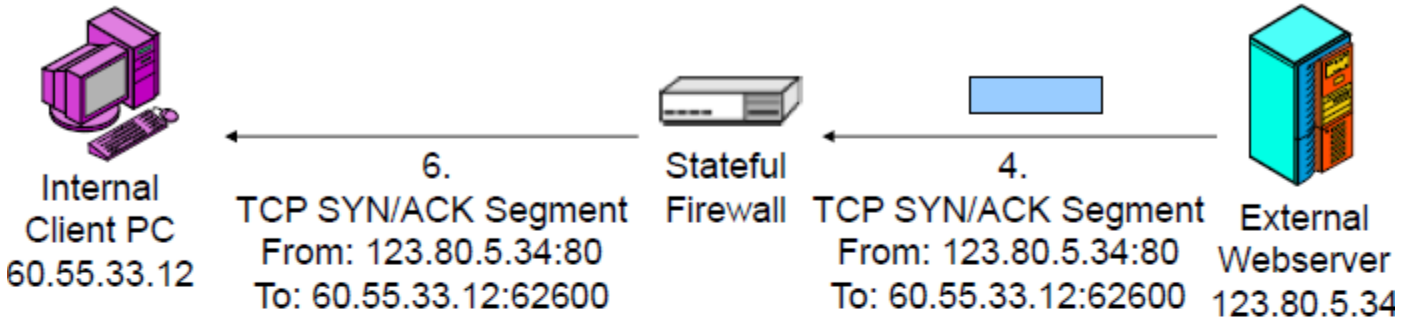
Main Border Firewall Stateful Inspection I (Continued)



Connection Table

Type	Internal IP	Internal Port	External IP	External Port	Status
TCP	60.55.33.12	62600	123.80.5.34	80	OK

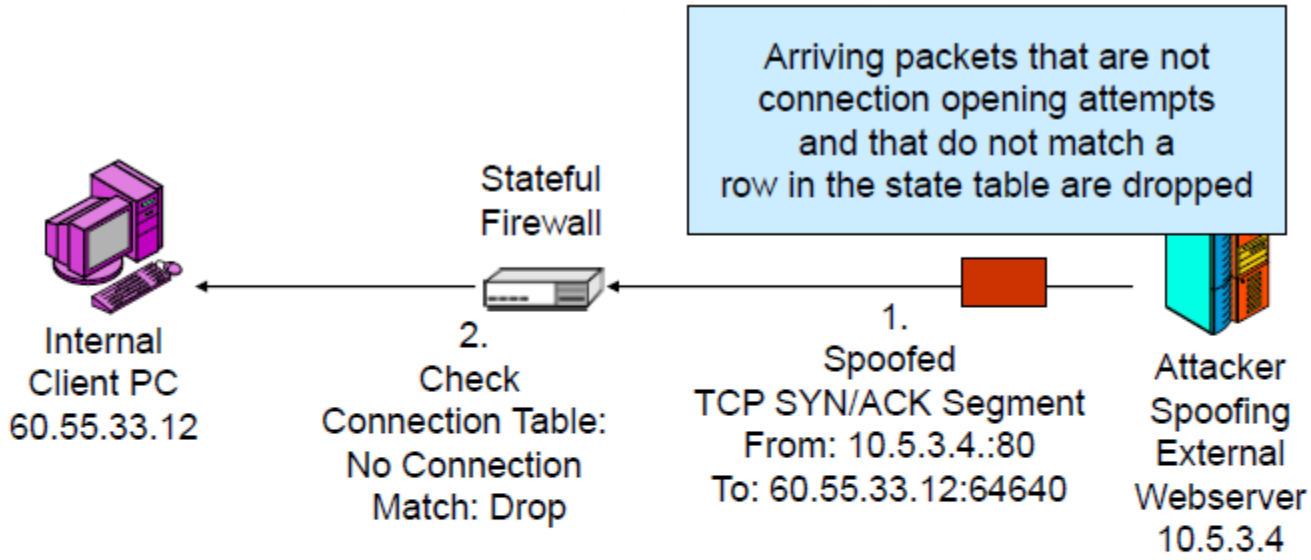
Main Border Firewall Stateful Inspection I (Continued)



Connection Table

Type	Internal IP	Internal Port	External IP	External Port	Status
TCP	60.55.33.12	62600	123.80.5.34	80	OK

Main Border Firewall Stateful Inspection I (Continued)



Connection Table

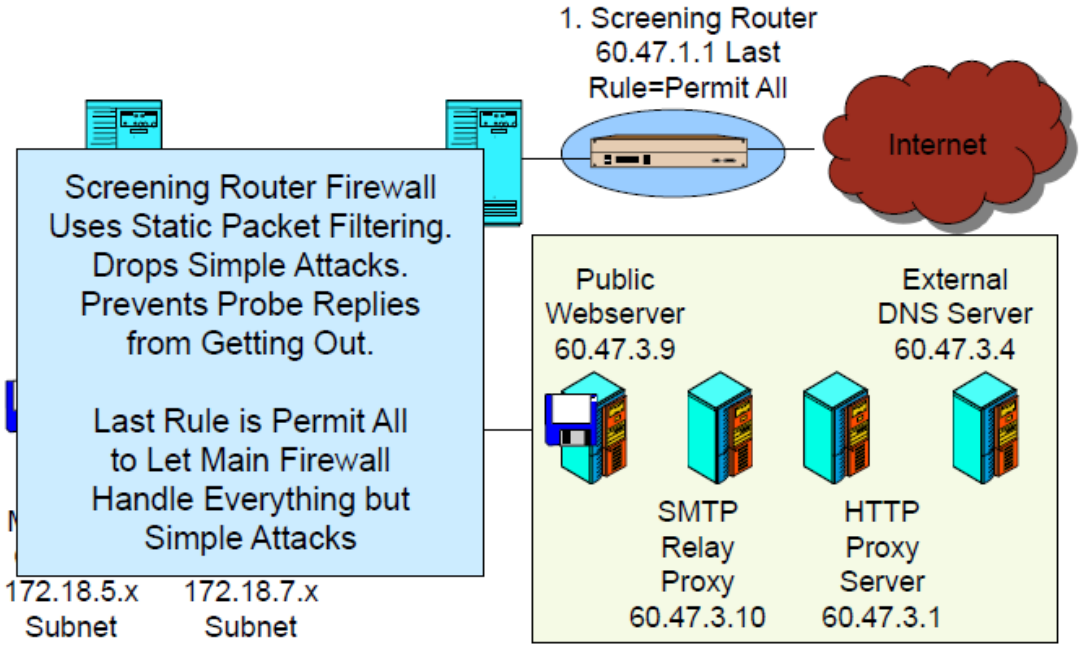
Type	Internal IP	Internal Port	External IP	External Port	Status
TCP	60.55.33.12	62600	123.80.5.34	80	OK
UDP	60.55.33.12	63206	222.8.33.4	69	OK

Stateful Inspection Firewall in Perspective

- **Simplicity and Therefore Low Cost**
  - Connection opening decisions are somewhat complex
  - But most packets are part of approved ongoing connections
  - Filtering ongoing packets is extremely simple
  - Therefore, stateful inspection is fast and inexpensive
- **Low Cost**
- **Safety**
  - Stops nearly all internet-level attacks
  - (Application-level filtering still needed)
- **Dominance for Main Border Firewalls**
  - Nearly all use stateful inspection
- **Beyond Stateful Inspection**
  - Most main border firewalls also use other inspection methods
  - Denial-of-service filtering
  - Limited application content filtering
  - Etc.

Screening Router Firewall

Firewall Architecture (Single Site)



Static packet filtering only filters packets based on administrator defined rules governing allowed ports and IP addresses at the network and transport layers.

Dynamic packet filtering provides a better level of security than static packet filtering since it takes a closer look at the contents of the packet and also considers previous connection states.

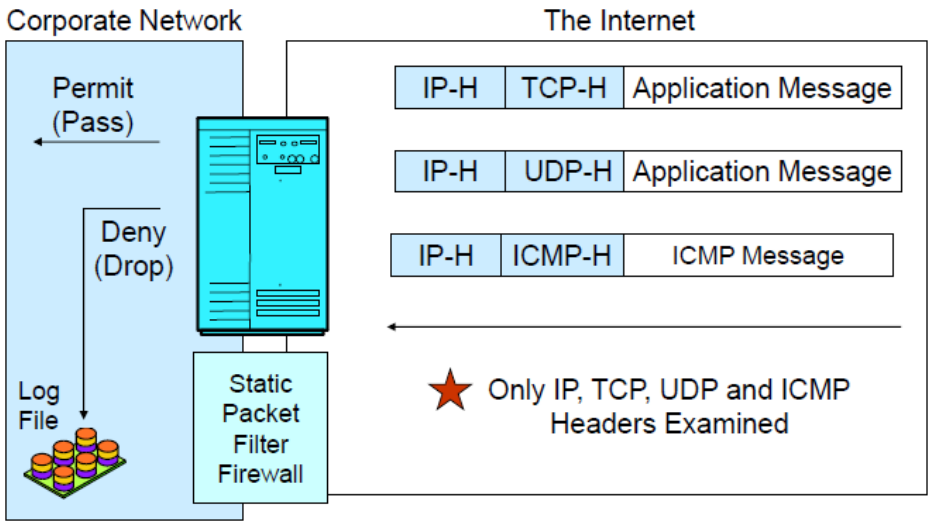
Static Packet Inspection on Screening Router Firewalls

- **Screening Firewall Routers**
  - Add filtering to the border router
  - Filter out many high-frequency, low-complexity attacks
  - For ingress filtering, reduce the load on the main border firewall

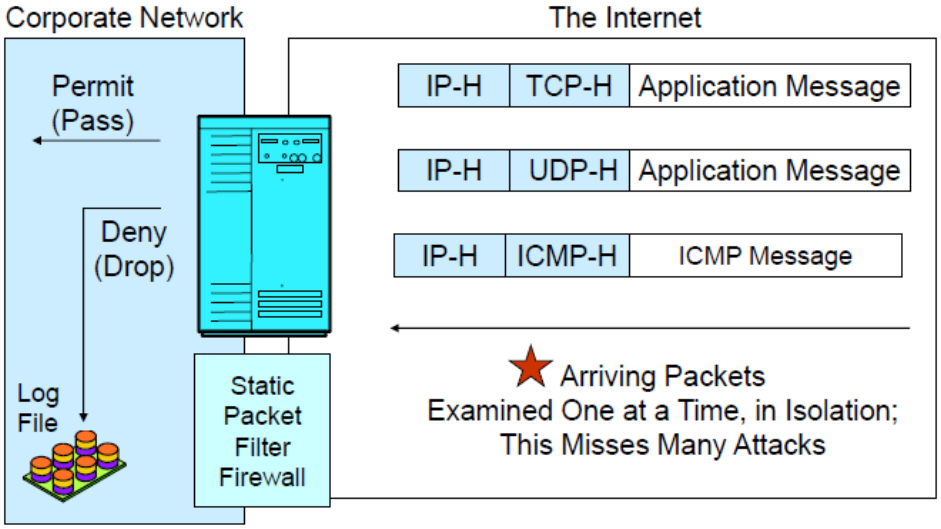
Screening Router Firewalls (Continued)

- **High Cost for Sufficient Performance**
  - Must buy inspection software for the router (expensive)
  - Usually must upgrade router processing speed and memory (expensive)
- **Good Location for Egress Filtering**
  - Stops all replies to probe packets
  - Including those from the border router itself
- **Use Static Packet Filtering**
  - Require complex access control lists (ACLs) Because need an ACL statement for each rule

Static Packet Filter Firewall



ICMP: Internet Control Message Protocol



Screening Firewall Router Ingress ACL

1. If source IP address = 10.*.*.*, DENY *[private IP address range]*

2. If source IP address = 172.16.*.* to 172.31.*.*, DENY *[private IP address range]*

3. If source IP address = 192.168.*.*, DENY *[private IP address range]*

4. If source IP address = 60.47.*.*, DENY *[internal IP address range]*

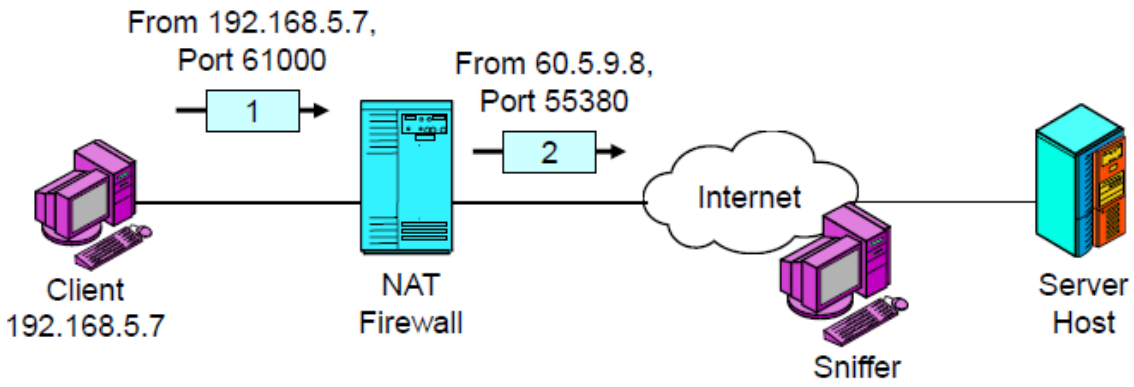
5. If source IP address = 1.33.3.4, DENY *[black-holed IP address of attacker]*

Network Address Translation (NAT)

The problem

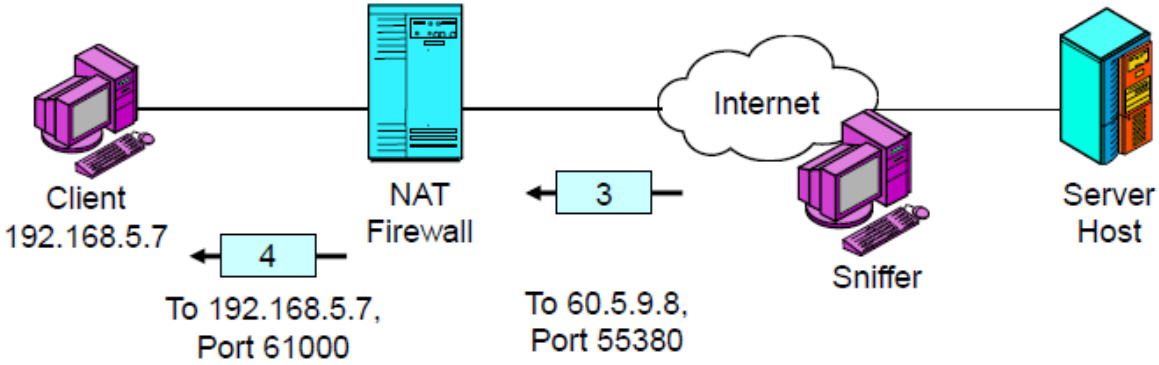
Sniffers on the Internet can read packets to and from organizations

- Detect IP addresses and port numbers of hosts
- Provides considerable information about potential victims without the risks of sending probing attacks
- Solution: Disguise (Hide) IP addresses and port numbers of internal hosts.



Translation Table

Internal		External	
IP Addr	Port	IP Addr	Port
192.168.5.7	61000	60.5.9.8	55380
. . .	. . .	. . .	. . .



Translation Table

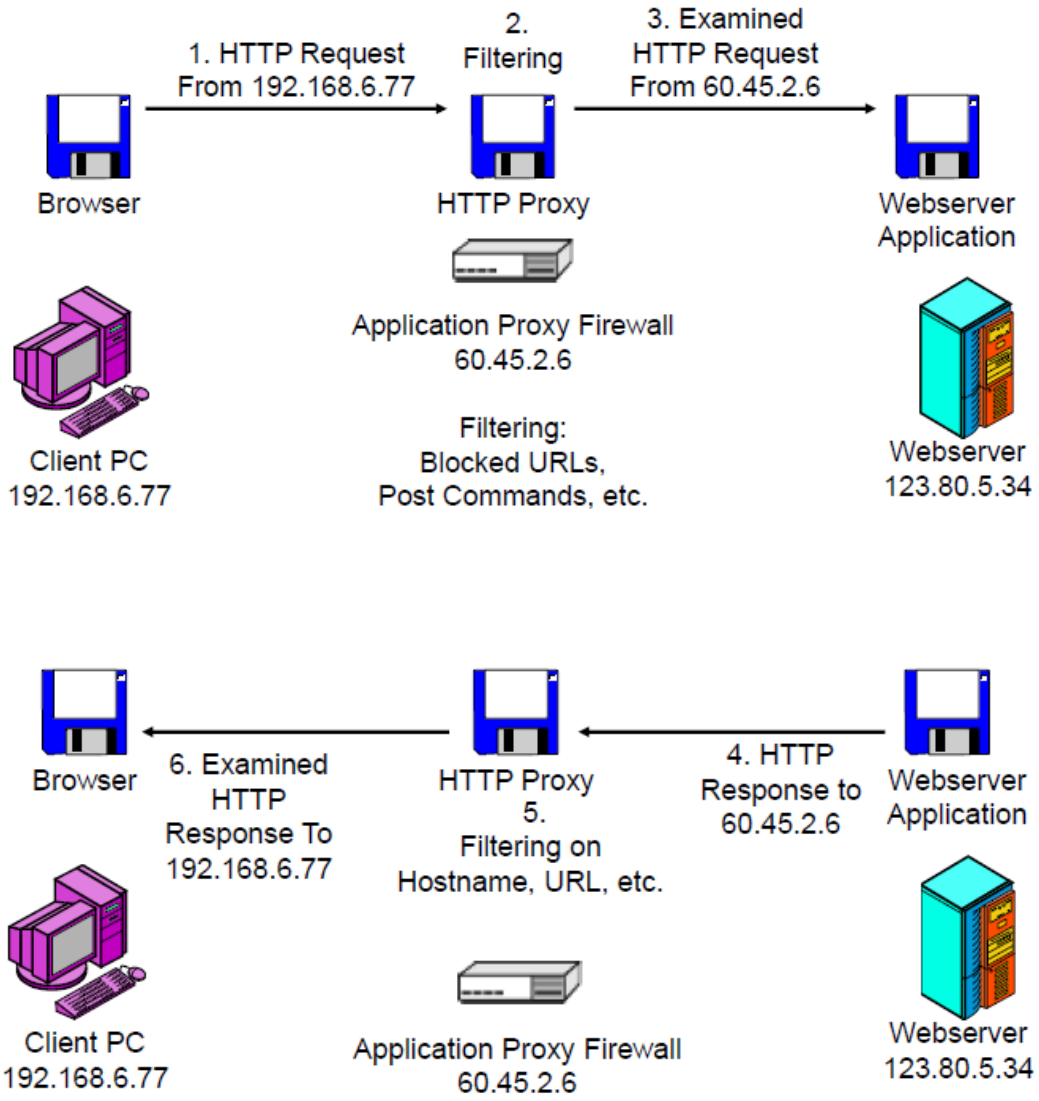
Internal		External	
IP Addr	Port	IP Addr	Port
192.168.5.7	61000	60.5.9.8	55380
. . .	. . .	. . .	. . .

Perspective on NAT

- **Sniffers on the Internet cannot learn internal IP addresses and port numbers**
  - Only learn the translated address and port number
- **By themselves, provide a great deal of protection against attacks**
  - External attackers cannot create a connection to an internal computers
- **Sniffers and NAT**
  - Sniffers can read stand-in IP addresses and port numbers
  - Can send back packets to these stand-in values; NAT will deliver them to the real host
  - However, most sessions too brief to exploit
  - Still a potential danger if sniffers act quickly
- **Box: Using NAT for Address Multiplication**
  - Firm may only be given a limited number of public IP addresses
  - Must use these in packets sent to the Internet
  - May use private IP addresses internally
  - For each public IP address, there can be a separate connection for each possible port
    - Address 60.5.9.8, Port = 2000
    - Address 60.5.9.8, Port = 2001
    - Etc.
  - Each connection can be linked to a different internal IP address
  - Can have thousands of internal IP addresses for each public IP address

Application Proxy Firewalls

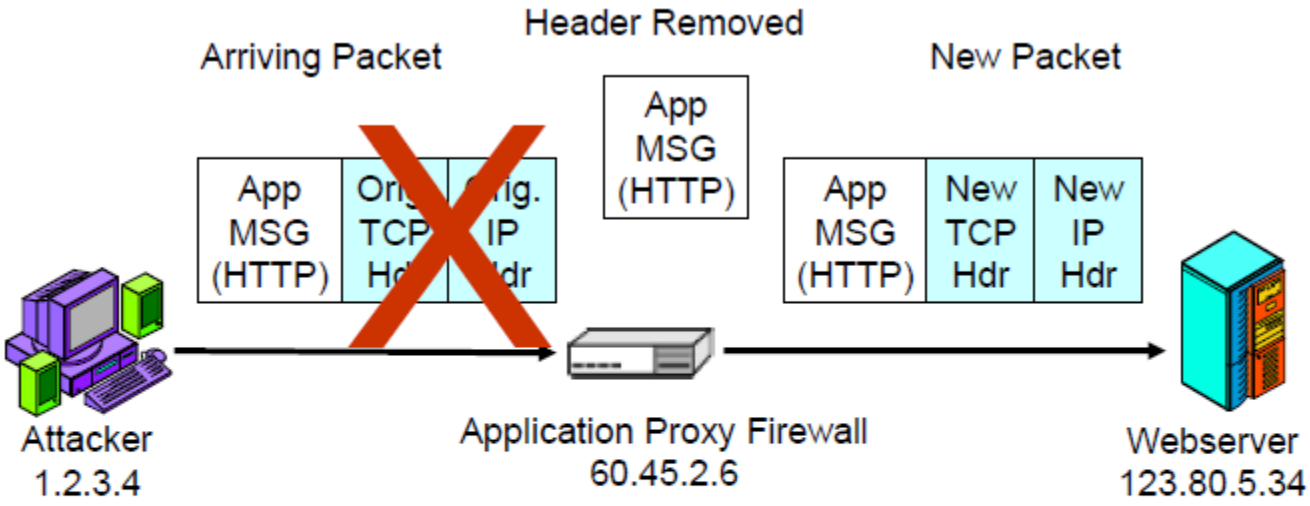
Application Proxy Firewall Operation



Application Proxy Firewall

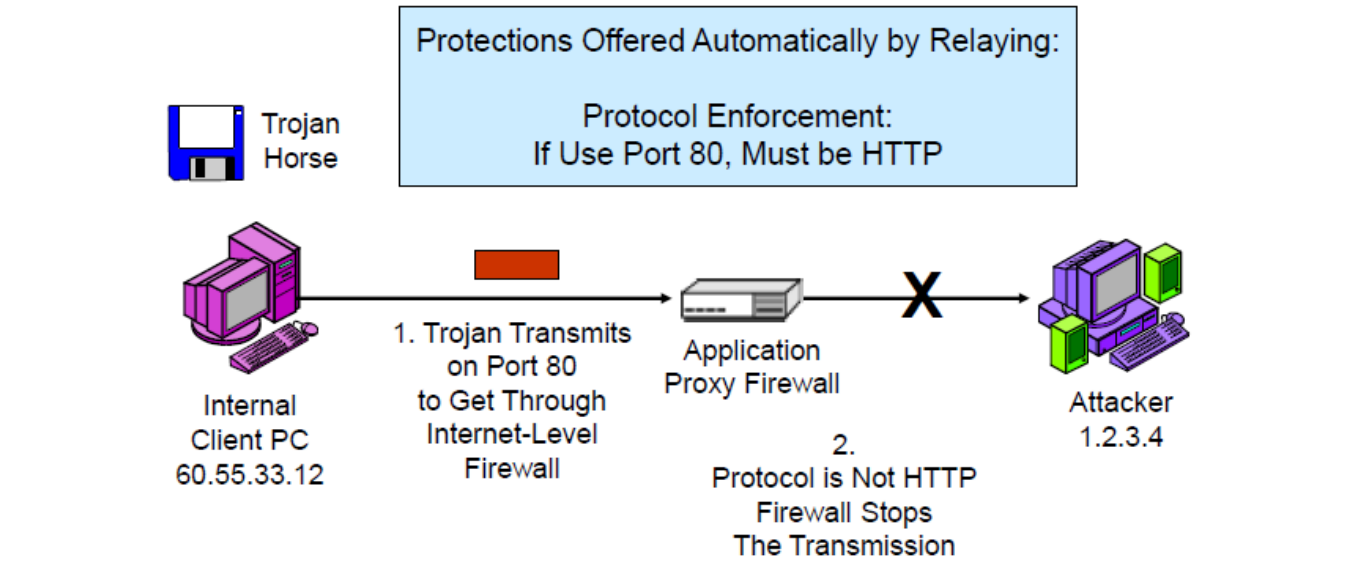
- **Client Server Relaying**
  - Relay operation: Proxy acts as a server to the client and a client to the server.
  - Full protocol support.
  - Slow processing per packet.
- **Core Protections**
  - IP address hiding (sniffer will only see the application proxy firewall's IP address).
  - Packet header destruction.

Core Protections due to Application Proxy Firewall Relay Operation

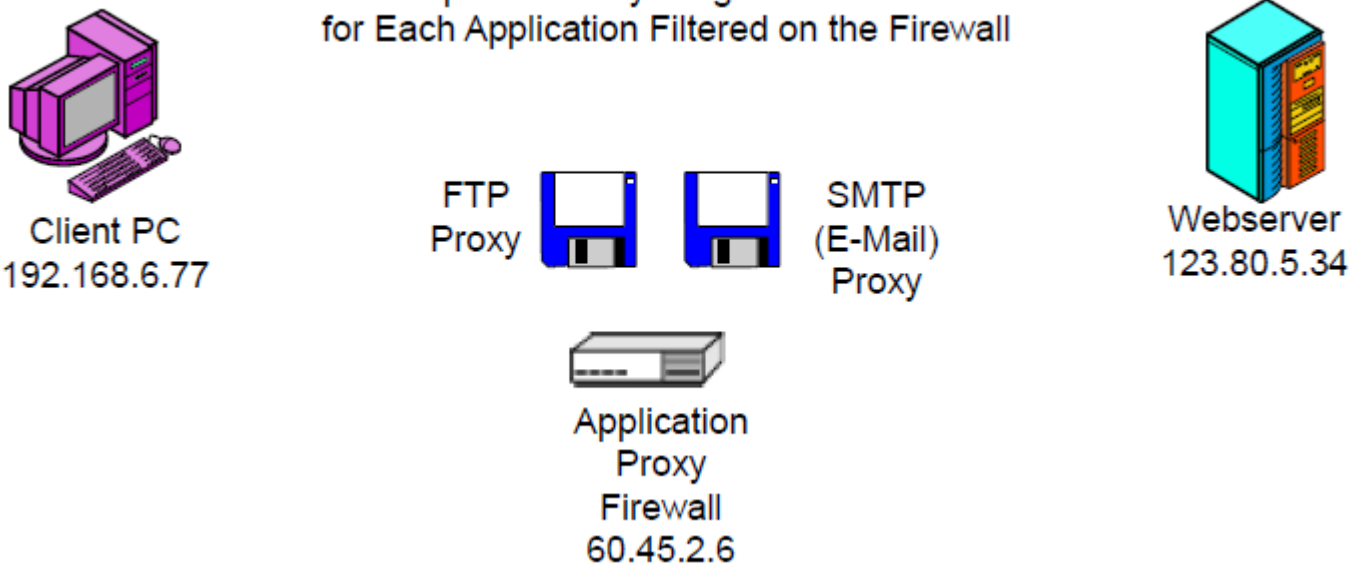


Protections Offered Automatically by Relaying:

Removes Headers from Arriving Packet:
Eliminates Header-Based Attacks



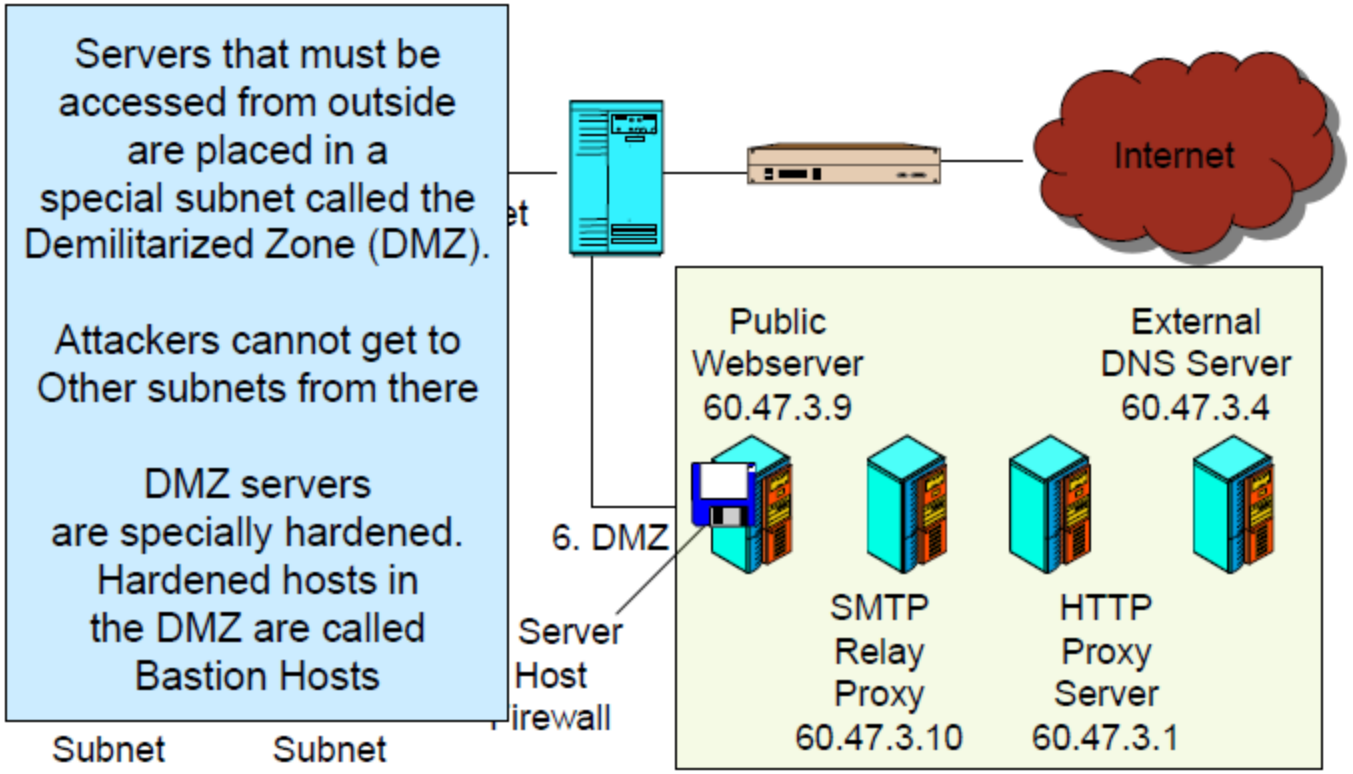
A Separate Proxy Program is Needed
for Each Application Filtered on the Firewall



Application Proxy Firewalls (Continued)

- **Multiple Proxies**
  - Each application to be filtered needs a separate proxy program.
  - Small firms usually use a single application proxy firewall with multiple application proxies.
  - Large firms usually use a single application proxy firewall per proxy.

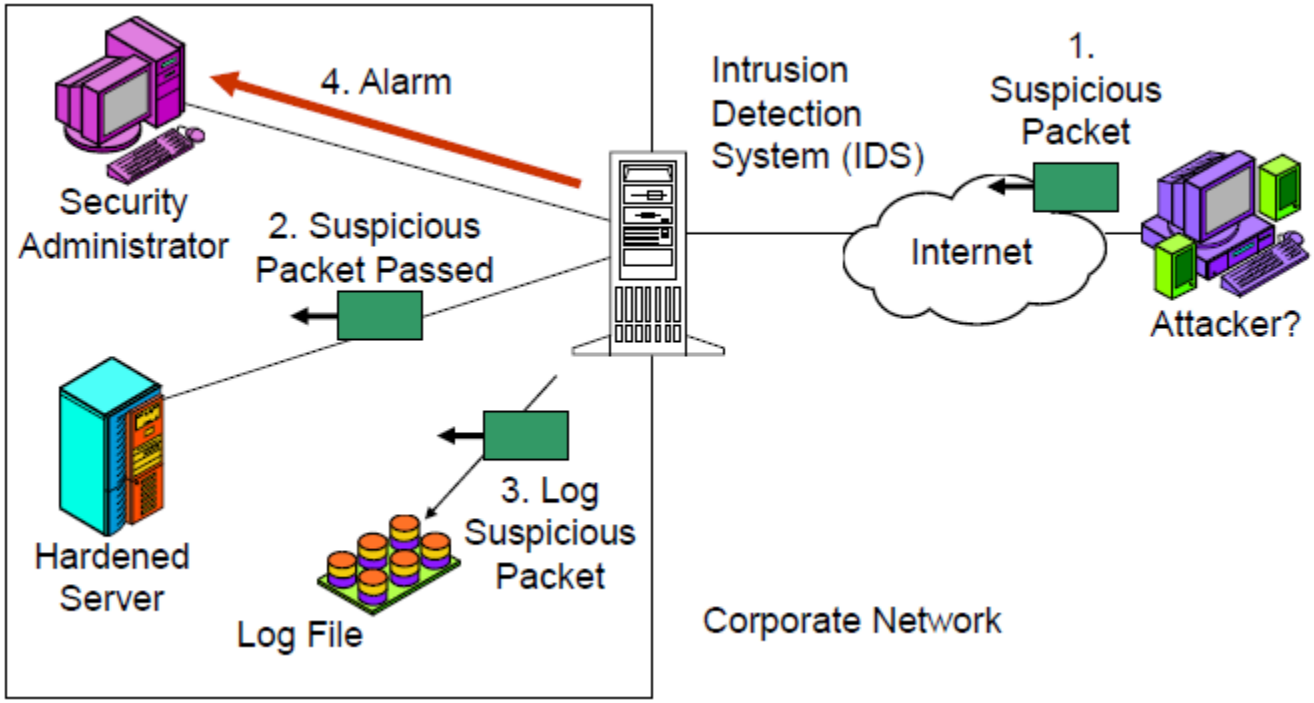
Demilitarized Zone (DMZ)


Servers that must be accessed from outside are placed in a special subnet called the Demilitarized Zone (DMZ).
Attackers cannot get to Other subnets from there
DMZ servers are specially hardened. Hardened hosts in the DMZ are called Bastion Hosts
Internet
Public Webserver 60.47.3.9
External DNS Server 60.47.3.4
6. DMZ
Server
Host
irewall
SMTP Relay Proxy 60.47.3.10
HTTP Proxy Server 60.47.3.1
Subnet
Subnet

- **Demilitarized Zone (DMZ)**
  - Subnet for servers and application proxy firewalls accessible via the Internet
  - Hosts in the DMZ must be especially hardened because they will be attacked by hackers
  - Hardened hosts in the DMZ are called bastion hosts
- **Uses Tri-Homed Main Firewalls**
  - 3 NICs, each attached to a different subnet
  - One subnet to the border router
  - One subnet for the DMZ (accessible to the outside world)
  - One subnet for the internal network
    - Access from the subnet to the Internet is strongly controlled
    - Access from the DMZ is also strongly controlled
- **Hosts in the DMZ**
  - Public servers (public webservers, FTP servers, etc.)
  - Application proxy firewalls
  - External DNS server that only knows host names for hosts in the DMZ

Intrusion Detection Systems (IDSs)
and
Intrusion Prevention Systems (IPSs)

Intrusion Detection System (IDS)



Firewalls, IDSs, and IPSs

	Firewalls	IDSs	IPSs
Drops Packets?	Yes	No	Yes
Logs Packets	Yes	Yes	Yes
Sophistication in Filtering	Medium	High	High
Creates Alarms?	No	Yes	Sometimes

Firewalls, IDSs, and IPSs (Continued)

- **Sophistication in Filtering**
  - Message stream analysis, not just individual packets
  - Reassemble fragmented application messages
  - Deep packet inspection: both internet-level headers and application headers
- **Firewalls Versus IDSs**
  - Firewalls drop packets
  - IDSs only generate alarms
    - Too many false positives (false alarms) to drop suspicious packets safely
- **IDSs versus IPSs**
  - IDSs send alarms
  - IPSs, using the same filtering mechanisms, actually drops suspicious packets with high confidence of being attacks