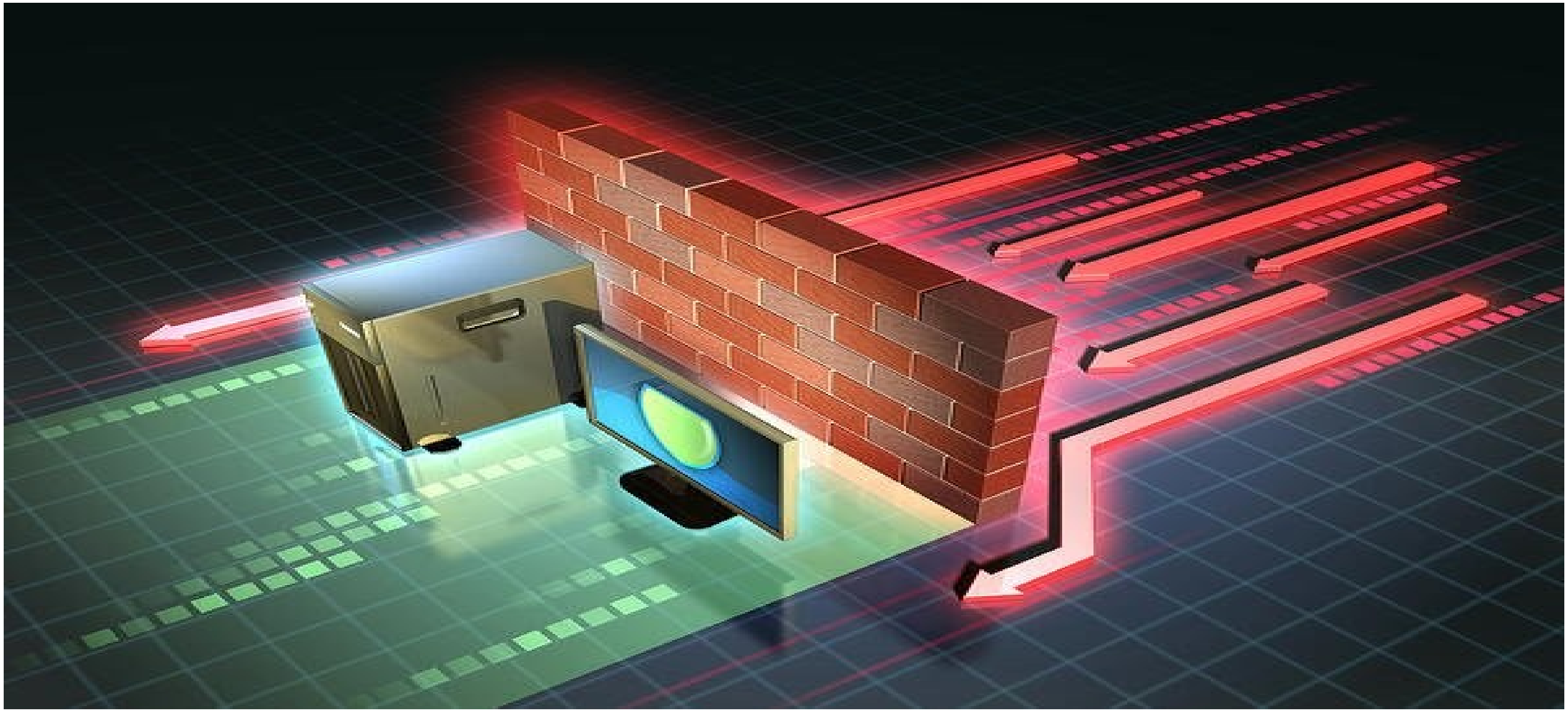


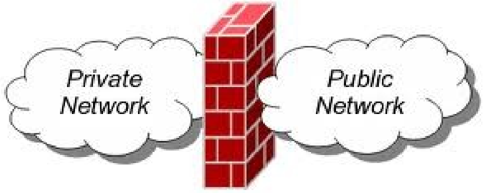
Lecture 12

Firewalls

Trusted and Untrusted Network

- **Trusted networks** are defined as "the networks inside your security perimeter, and are usually the networks you are trying to protect."
- It defines **untrusted networks** as "the network's outside your security perimeter. They are untrusted because they are often beyond your control."
- In other words, **untrusted networks** are those that may offer services or information that you need to access, but because you are not in control of administering these networks, they are "untrusted" in the sense that you limit the communications between them and your network.
- An example of this might be a client network you connect to gain access to certain information. There are also "unknown" networks, which would include any network not specifically defined in your firewall's configuration, which would include the majority of the networks you visit on the Internet.

Firewall



- A firewall is a system designed to prevent unauthorized access to or from a private network.
- You can implement a firewall in either hardware or software form, or a combination of both.
- Firewalls prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets.
- All messages entering or leaving the intranet (i.e., the local network to which you are connected) must pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

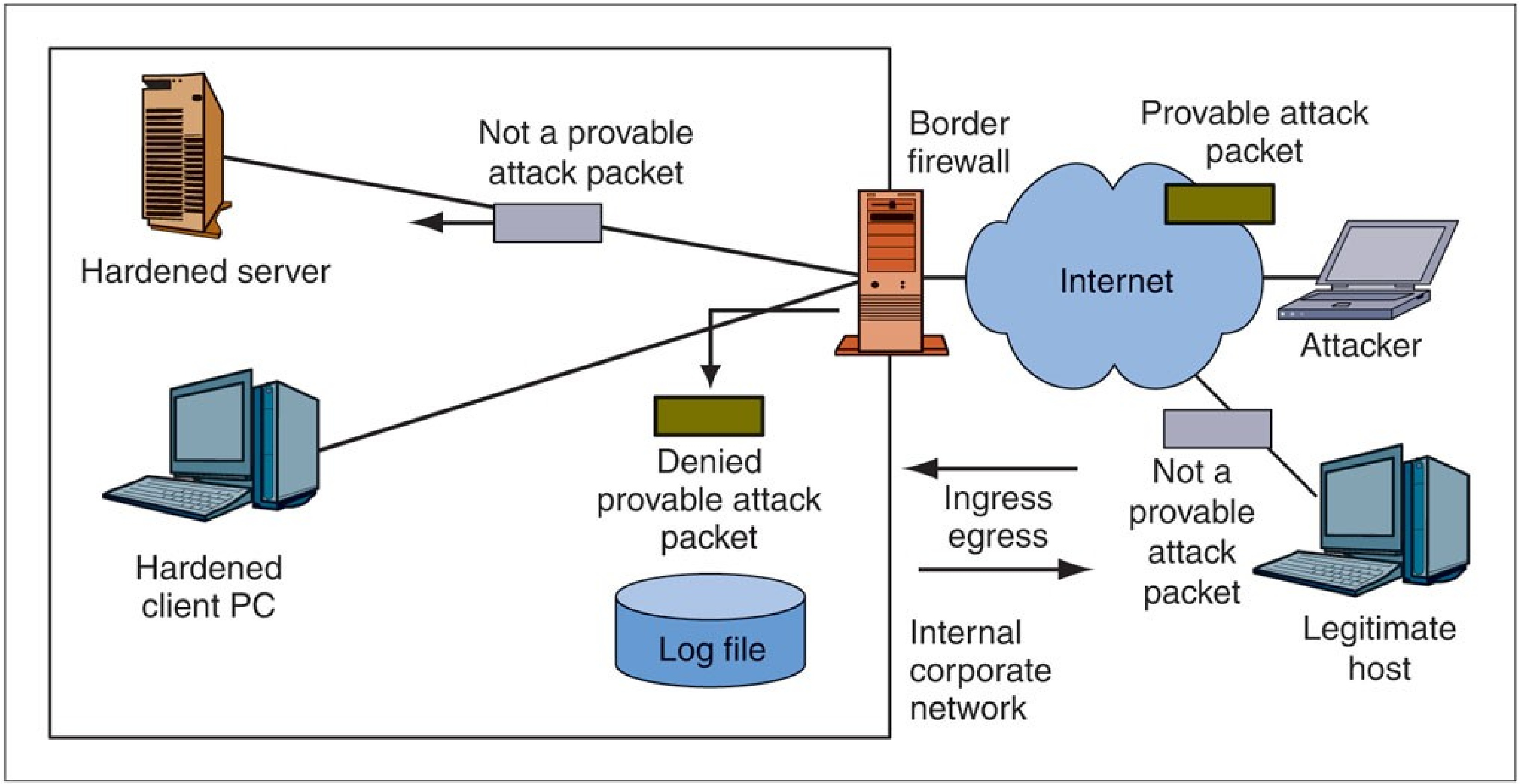
What do Firewalls Protect?

- Data
  - Proprietary corporate information
  - Financial information
  - Sensitive employee or customer data
- Resources
  - Computing resources
  - Time resources
- Reputation
  - Loss of confidence in an organization
  - Intruder uses an organization’s network to attack other sites

Who do Firewalls Guard Against?

- Internal Users
- Hackers
- Corporate Espionage
- Terrorists
- Common Thieves

Basic Firewall Operation



A firewall examines each packet passing through it. If the packet is a **provable attack packet**, the firewall drops the packet. 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**.

Basic Firewall Operation

- The Problem
  - If a firewall cannot filter all of the traffic passing through it, it drops packets it cannot process
  - This is secure because it prevents attack packets from getting through
  - But it creates a self-inflicted denial-of-service attack by dropping legitimate traffic

Basic Firewall Operation

- Firewall Capacity
  - Firewalls must have the capacity to handle the incoming traffic volume
  - Some can handle normal traffic but cannot handle traffic during heavy attacks!
  - They must be able to handle incoming traffic at wire speed—the maximum speed of data coming into each port

Basic Firewall Operation

- Processing Power Is Increasing Rapidly
  - As processing power increases, more sophisticating filtering methods should become possible
  - We can even have unified threat management (UTM), in which a single firewall can use many forms of filtering, including antivirus filtering and even spam filtering. (Traditional firewalls do not do these types of application-level malware filtering.)
  - However, increasing traffic is soaking up much of this increasing processing power

Basic Firewall Operation

- Firewall Filtering Mechanisms
  - There are many types
  - We will focus most heavily on the most important firewall filtering method, stateful packet inspection (SPI)
  - Single firewalls can use multiple filtering mechanisms, most commonly, SPI with other secondary filtering mechanisms

Packet Filtering Firewalls /Static Packet Filtering

- Packet filtering is one of the oldest, and one of the most common types of firewall technologies. Packet filters inspect each packet of information individually, examining the source and destination IP addresses and ports. This information is compared to access control rules to decide whether the given packet should be allowed through the firewall.

- Packet filters consider only the most basic attributes of each packet, and they don't need to remember anything about the traffic since each packet is examined in isolation. For this reason they can decide packet flow very quickly.

- Because every packet of every connection is checked against the access control rules, larger, complex rule bases decrease performance. And because packet filters can only check low-level attributes, they are not secure against malicious code hiding in the other layers. Packet filters are often used as a first defense in combination with other firewall technologies, and their most common implementation today is seen in the access control lists of routers at the perimeters of networks.

Packet Filtering Firewalls /Static Packet Filtering

- Static Packet Filtering
  - This was the earliest firewall filtering mechanism
  - Limits
    - Examines packets one at a time, in isolation
    - Only looks at some internet and transport headers
    - Consequently, unable to stop many types of attacks

Packet Filtering Firewalls /Static Packet Filtering

- Inspects Packets One at a Time, in Isolation
  - If it receives a packet containing a SYN/ACK segment, this may be a legitimate response to an internally initiated SYN segment
    - The firewall must pass packets containing these segments, or internally initiated communications cannot exist
  - However, this SYN/ACK segment could be an external attack

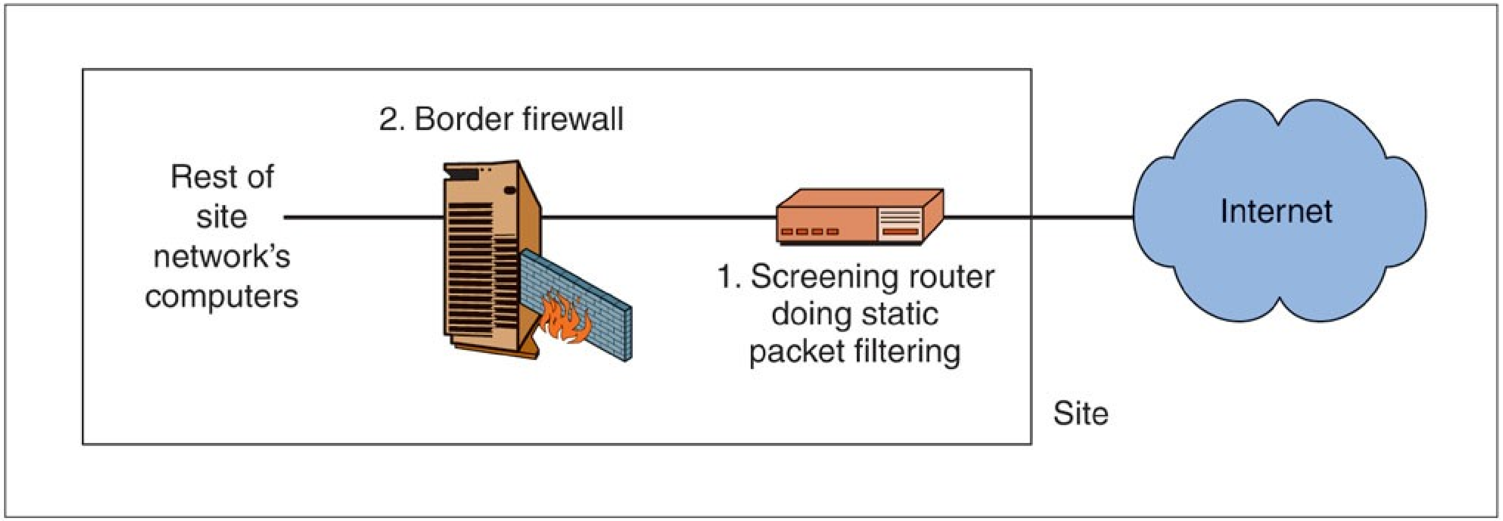
Note: Client requests connection by sending **SYN** (synchronize) message to the server. Server acknowledges by sending **SYN-ACK** (synchronize-acknowledge) message back to the client. Client responds with an **ACK** (acknowledge) message, and the connection is established.

Packet Filtering Firewalls /Static Packet Filtering

- Market Status
  - No longer used as the main filtering mechanism for border firewalls
  - May be used as a secondary filtering mechanism on main border firewalls

Main Border Firewall and Screening Router That Uses Static Packet Filtering

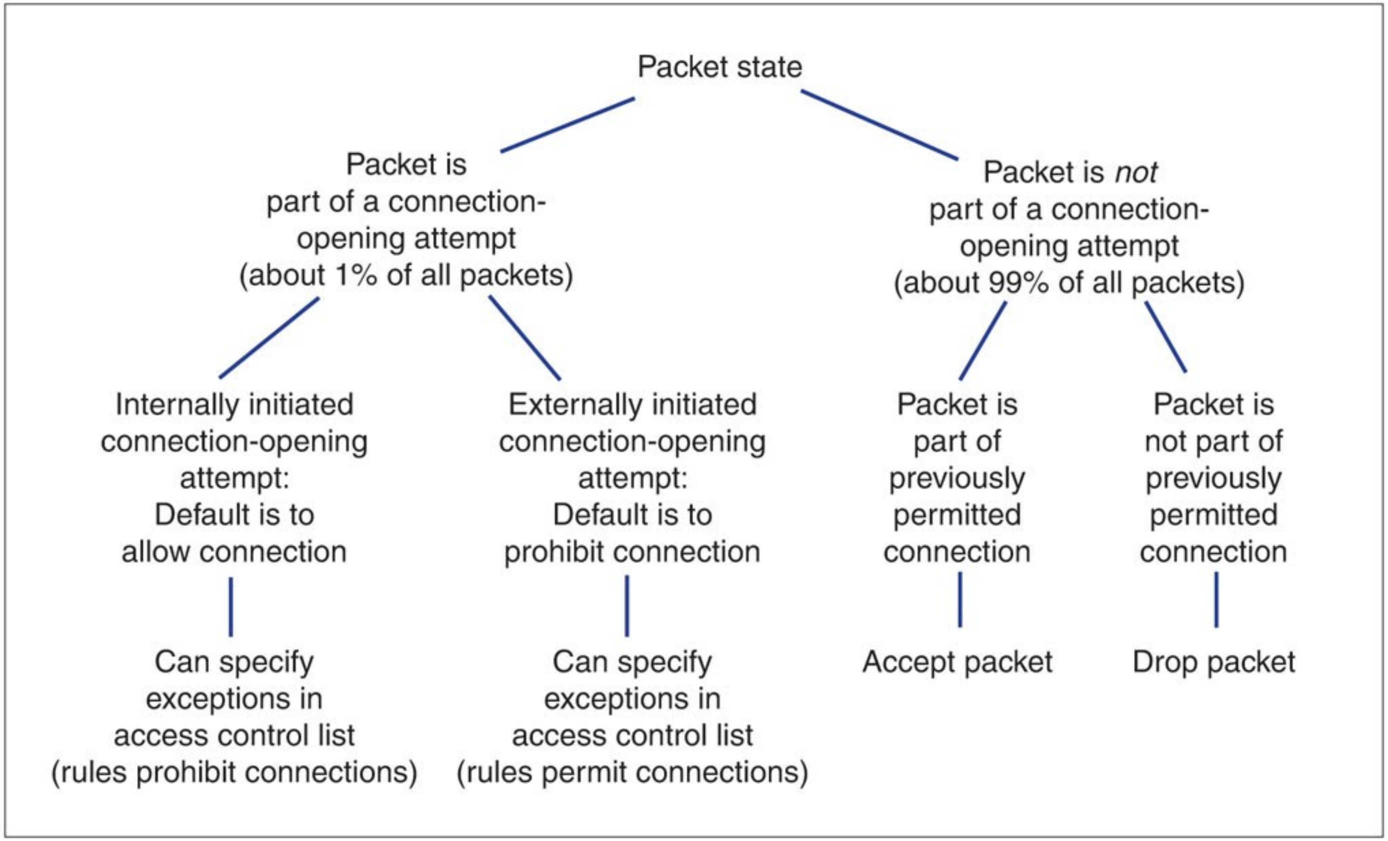
- Market Status
  - Also may be implemented in border routers, which lie between the Internet and the firewall
    - Stops simple, high-volume attacks to reduce the load on the main border firewall


2. Border firewall
Rest of site network's computers
1. Screening router doing static packet filtering
Internet
Site

Stateful Packet Inspection

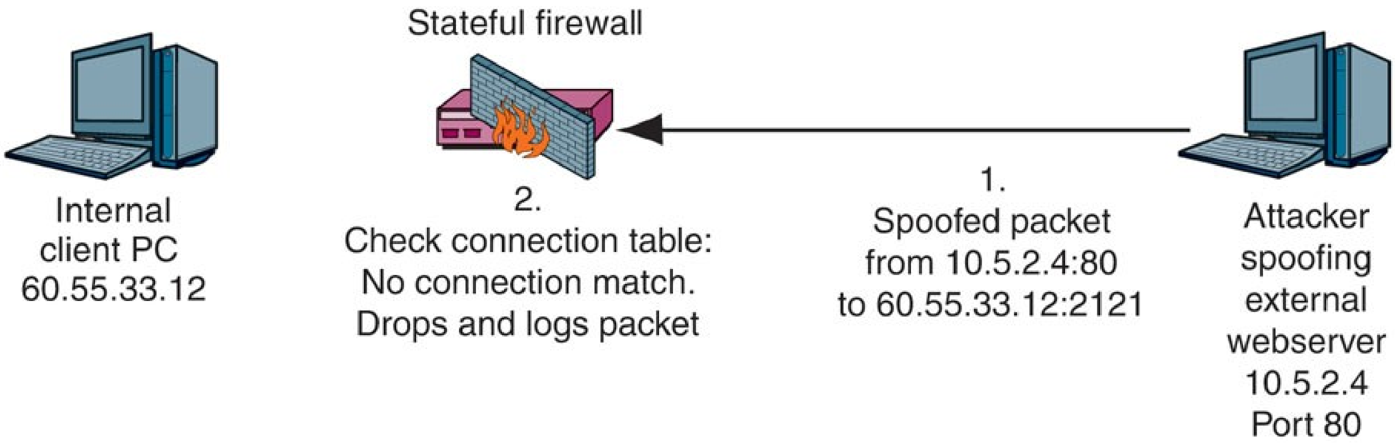
- Nearly all corporate border firewalls today use the stateful packet inspection (SPI) filtering method
    - SPI focuses on connections
        - Persistent conversations between different programs on different computers
- It aims to monitor the active connections on a network. Moreover, the process of stateful inspection determines which network packets should be allowed through the firewall by utilizing the information regarding active connections.
- Stateful inspection keeps track of each connection and constantly checks if they are valid.

States in a Connection


Packet state
Packet is part of a connection-opening attempt (about 1% of all packets)
Packet is *not* part of a connection-opening attempt (about 99% of all packets)
Internally initiated connection-opening attempt: Default is to allow connection
Externally initiated connection-opening attempt: Default is to prohibit connection
Packet is part of previously permitted connection
Packet is not part of previously permitted connection
Can specify exceptions in access control list (rules prohibit connections)
Can specify exceptions in access control list (rules permit connections)
Accept packet
Drop packet

- First, there is an opening state, when the two applications agree to open a connection.
- Afterward, the two applications enter the ongoing communication state.
- For most connections, traffic is dominated by exchanges during the ongoing communication state.
- The two applications communicate back and forth using the same port numbers and other conditions.

Stateful Packet Inspection for a Packet That Does Not Attempt to Open a Connection II



Stateful firewall

Internal
client PC
60.55.33.12

2.
Check connection table:
No connection match.
Drops and logs packet

1.
Spoofed packet
from 10.5.2.4:80
to 60.55.33.12:2121

Attacker
spoofing
external
webserver
10.5.2.4
Port 80

Connection table

Type	Internal IP	Internal Port	External IP	External Port	Status
TCP	60.55.33.12	4400	123.80.5.34	80	OK
UDP	60.55.33.12	3660	1.8.33.4	161	OK

Stateful Packet Inspection

- Access Control List Operation
  - An ACL is a series of rules for allowing or disallowing connections
  - The rules are executed in order, beginning with the first
  - If a rule does not apply to the connection-opening attempt, the firewall goes to the next ACL rule
  - If the rule does apply, the firewall follows the rule, and no further rules are executed
  - If the firewall reaches the last rule in the ACL, it follows that rule

Stateful Packet Inspection

- Ingress ACL’s Purpose
  - The default behavior is to drop all attempts to open a connection from the outside
  - All ACL rules except for the last give exceptions to the default behavior under specified circumstances
  - The last rule applies the default behavior to all connection-opening attempts that are not allowed by earlier rules to be executed by this last rule

Stateful Packet Inspection

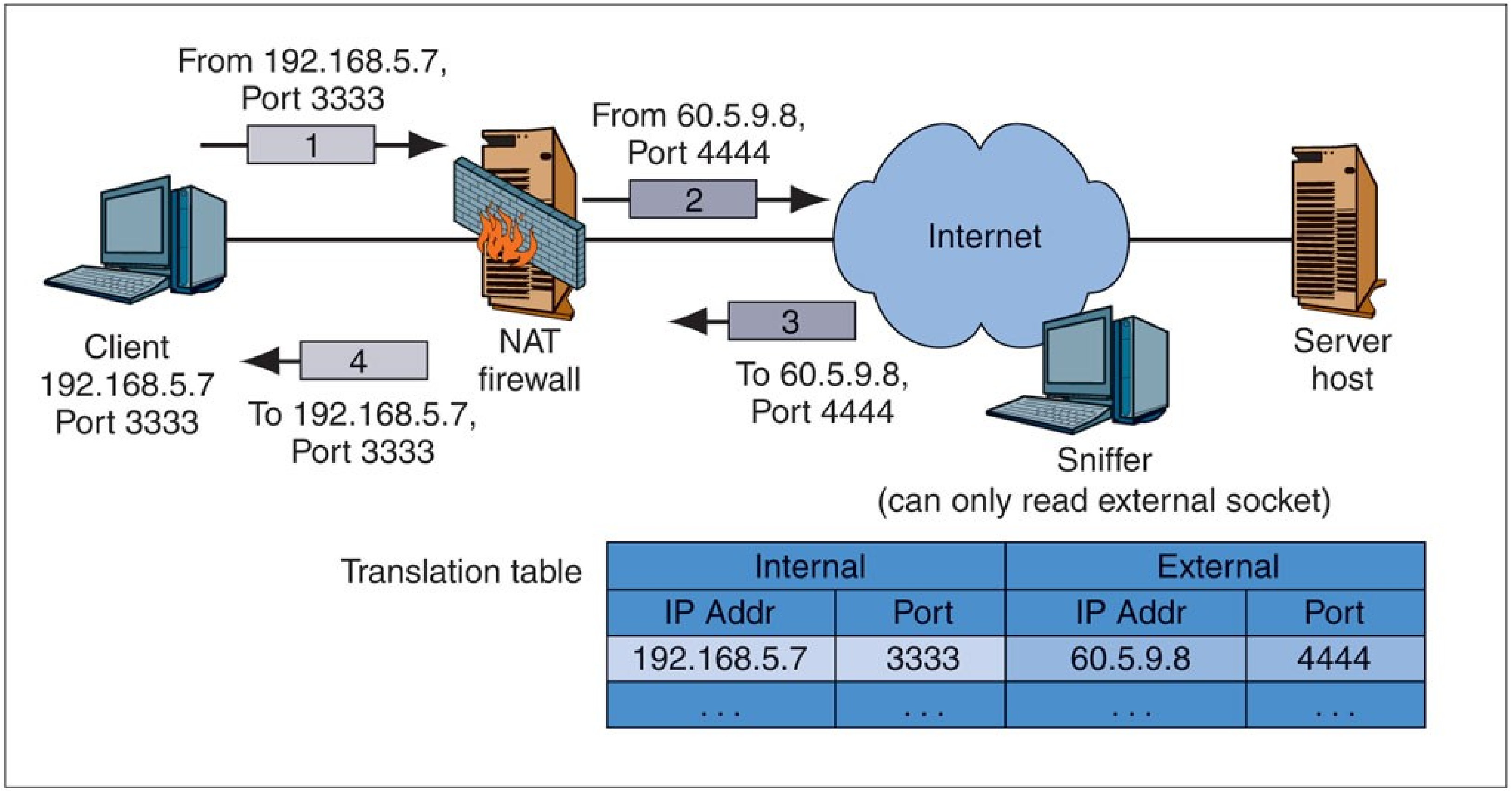
- Simple Ingress ACL with Three Rules

  1. If TCP destination port = 80 or TCP destination port = 443, then Allow Connection [Permits connection to ALL internal webservers]
  2. If TCP destination port = 25 AND IP destination address = 60.47.3.35, then Allow Connection [Permits connections to a SINGLE internal mail server]
  3. Disallow ALL Connections [Disallows all other externally initiated connections; this is the default behavior]

Stateful Packet Inspection

- Low Cost
  - Most packets are not part of packet-opening attempts
  - These can be handled very simply and therefore inexpensively
  - Connection-opening attempt packets are more expensive processes but are rare
- Safety
  - Attacks other than application-level attacks usually fail to get through SPI firewalls
  - In addition, SPI firewalls can use other forms of filtering when needed
- Dominance
  - The combination of high safety and low cost makes SPI firewalls extremely popular
  - Nearly all main border firewalls today use stateful packet inspection

Network Address Translation (NAT)



Internal		External	
IP Addr	Port	IP Addr	Port
192.168.5.7	3333	60.5.9.8	4444
. . .	. . .	. . .	. . .

Network Address Translation (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

Application Level Firewalls

- Application level firewalls are the third firewall technology traditionally seen in the market.
- Also known as application proxies, provide the most secure type of data connection because they can examine every layer of the communication, including the application data.
- To achieve this security proxies, as their name suggests, actually mediate connections. The connection from a client to a server is intercepted by the proxy. If the proxy determines that the connection is allowed, it opens a second connection to the server from itself, on behalf of the original host.
- The data portion of each packet must be stripped off, examined, rebuilt, and sent again on the second connection.
- This thorough examination and handling of packets means that proxy firewalls are very secure and generally slow. Proxies are also limited as firewalls, because they must understand the application layer. As new protocols are developed, new proxies must be written and implemented to handle them.

Intrusion Detection Systems and Intrusion Prevention Systems

- Intrusion Detection Systems (IDSs)
  - Firewalls drop provable attack packets only
  - Intrusion detection systems (IDSs) look for suspicious traffic
  - Sends an alarm message if the attack appears to be serious
  - Problem: Too many false positives (false alarms)
  - Problem: Heavy processing requirements because of sophisticated filtering
  - Packet stream analysis
  - Often, patterns cannot be seen unless many packets are examined

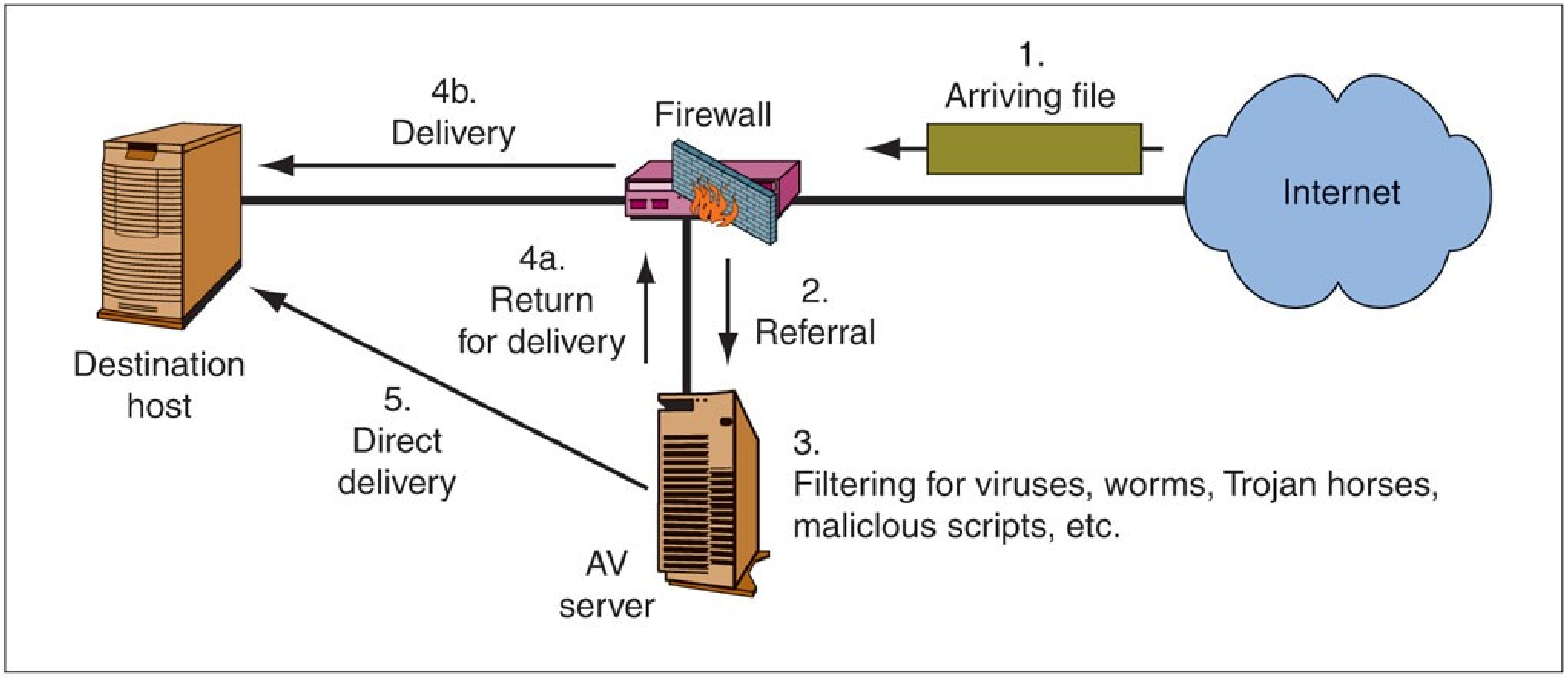
Intrusion Detection Systems and Intrusion Prevention Systems

- Intrusion Prevention Systems (IPSs)
  - Use IDS filtering mechanisms
  - Application-specific integrated circuits (ASICs) provide the needed processing power
  - Attack confidence identification spectrum
  - Somewhat likely,
  - Very likely,
  - Provable
  - Allowed to stop traffic at the high end of the attack confidence spectrum
  - Firm decides which attacks to stop

Intrusion Detection Systems and Intrusion Prevention Systems

- Possible Actions
  - Drop packets
    - Risky for suspicious traffic even with high confidence
  - Bandwidth limitation for certain types of traffic
    - Limit to a certain percentage of all traffic
    - Less risky than dropping packets
  - Useful when confidence is lower

Firewalls and Antivirus Servers



Firewalls normally do not do antivirus filtering. However, firewalls and antivirus filtering servers work together closely. All major firewall vendors have protocols for working with antivirus servers.

Antivirus Filtering and Unified Threat Management

- Traditional Firewalls
  - Do not do antivirus filtering
- Unified Threat Management (UTM) Firewalls
  - SPI
  - Antivirus filtering
  - VPNs
  - DoS protection
  - NAT

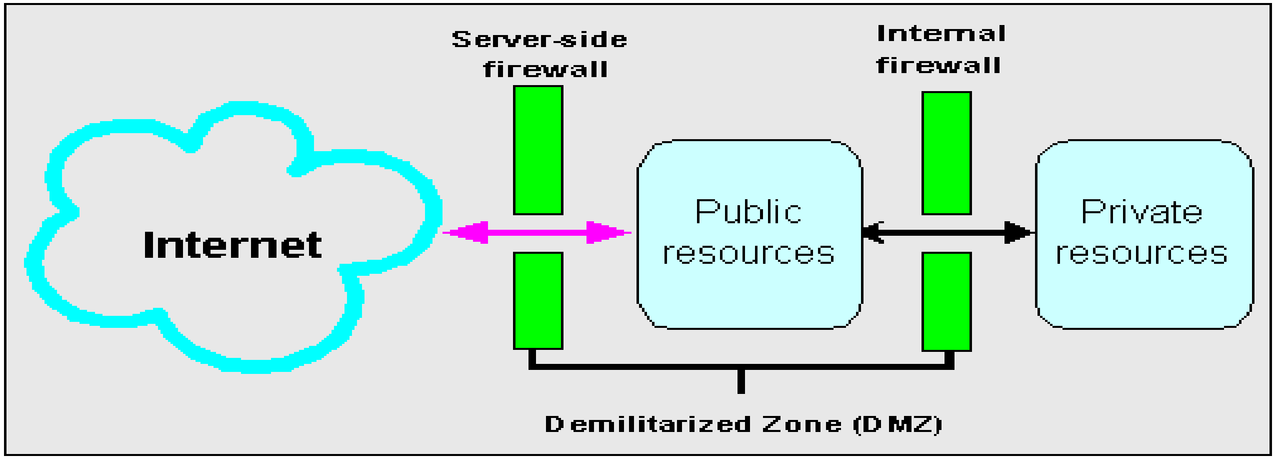
Firewall Architectures

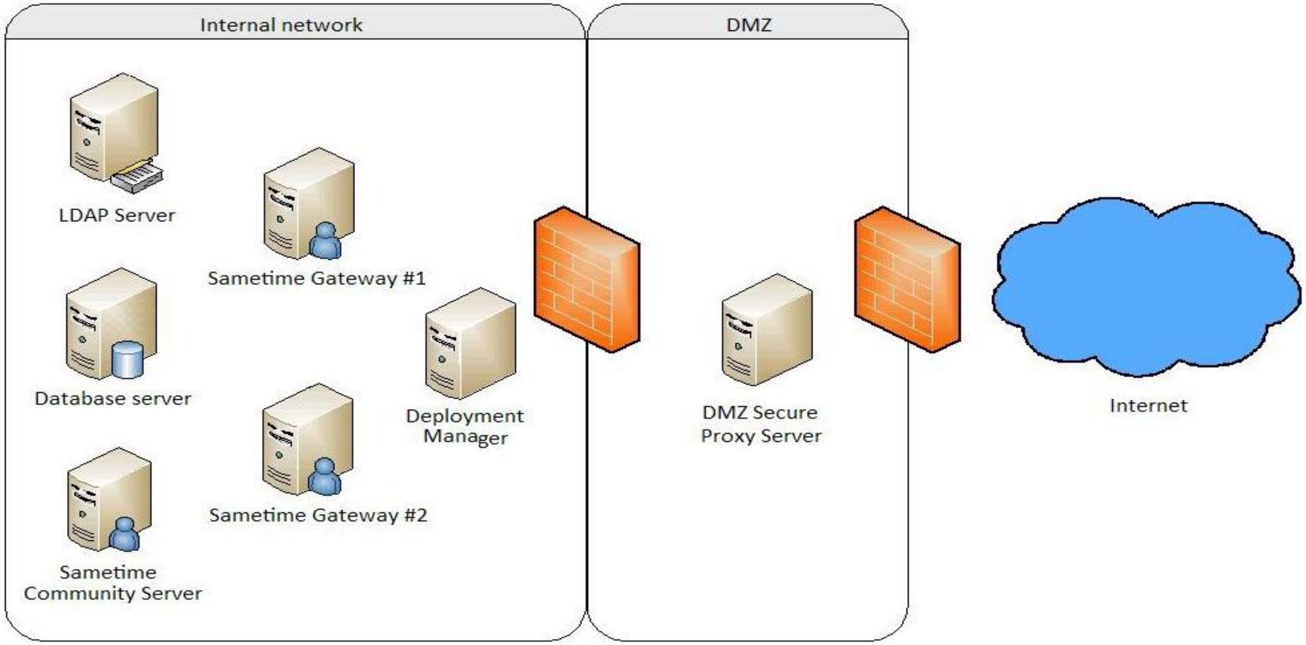
- Most firms have multiple firewalls
  - Main border firewalls
  - Screening border routers
  - Internal firewalls
  - Host firewalls

Firewall Architectures

- Demilitarized Zone (DMZ)
  - Subnet for servers and application proxy firewalls accessible via the Internet
  - This provides an additional layer of security to the LAN as it restricts the ability of hackers to directly access internal servers and data via the Internet.
  - External-facing servers, resources and services are located in the DMZ so they are accessible from the Internet but the rest of the internal LAN remains unreachable.

DMZ (Demilitarized Zone)





Firewall Architectures

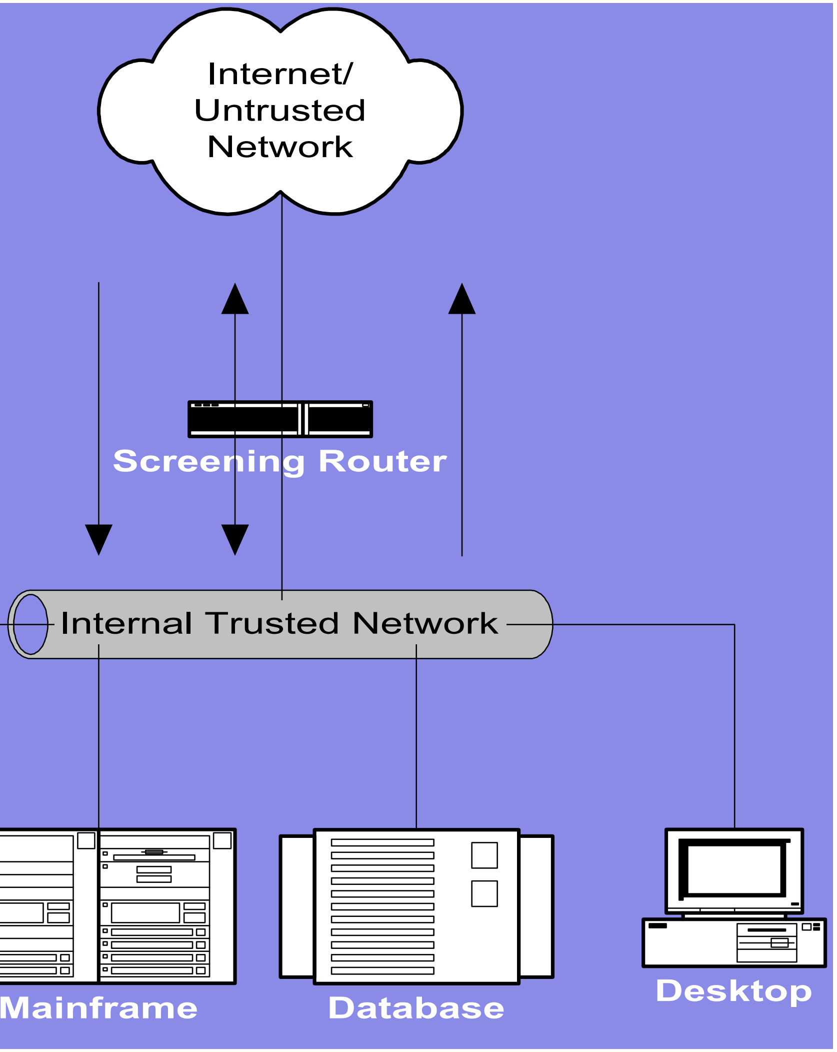
- DMZs Use Multihomed Main Firewalls
  - One subnet to the border router
  - One subnet to the DMZ (accessible to the outside world)
  - One subnet to the internal network
    - Access from the internal subnet to the Internet is nonexistent or minimal
    - Access from the internal subnet to the DMZ is also strongly controlled

Firewall Architectures

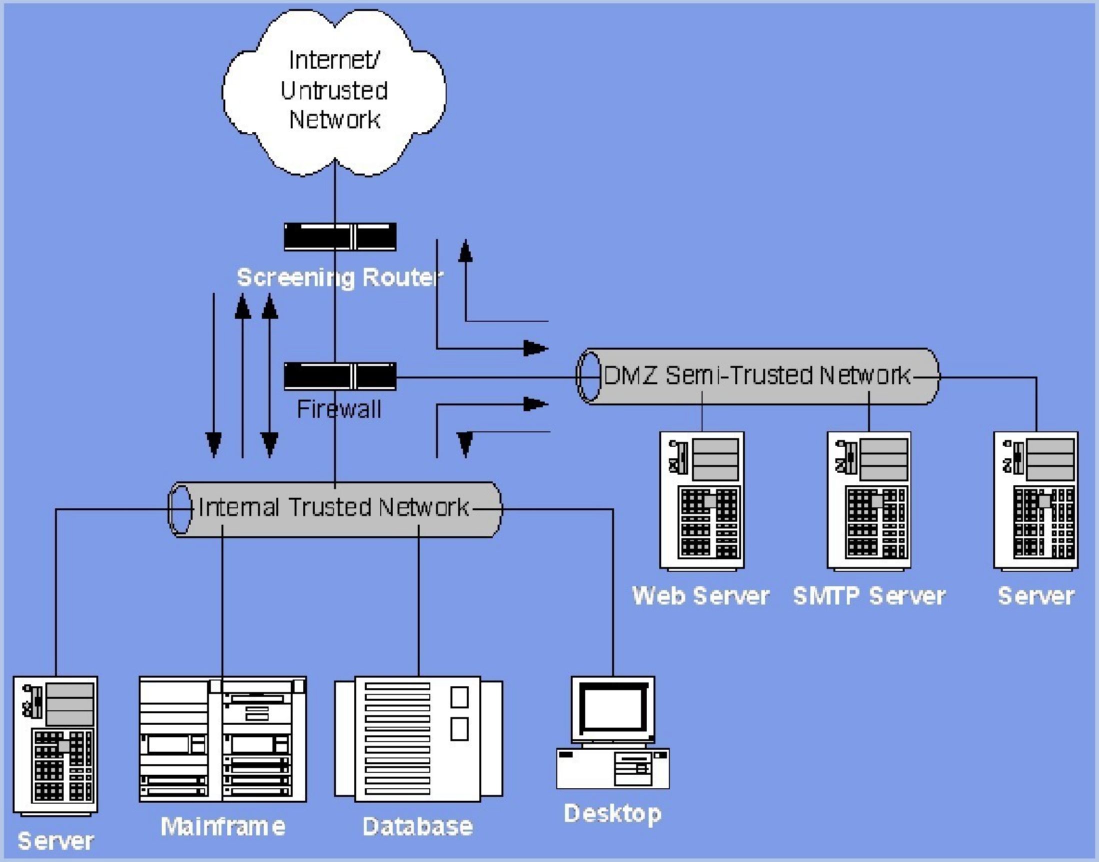
- Hosts in the DMZ
  - Public servers (public webservers, FTP servers, etc.)
  - Application proxy firewalls to require all Internet traffic to pass through the DMZ
  - External DNS server that knows only host names in the DMZ

Screening Router

Routes or blocks packets, as determined by security policy



Multi-Legged Firewall



Multi-Legged Firewall

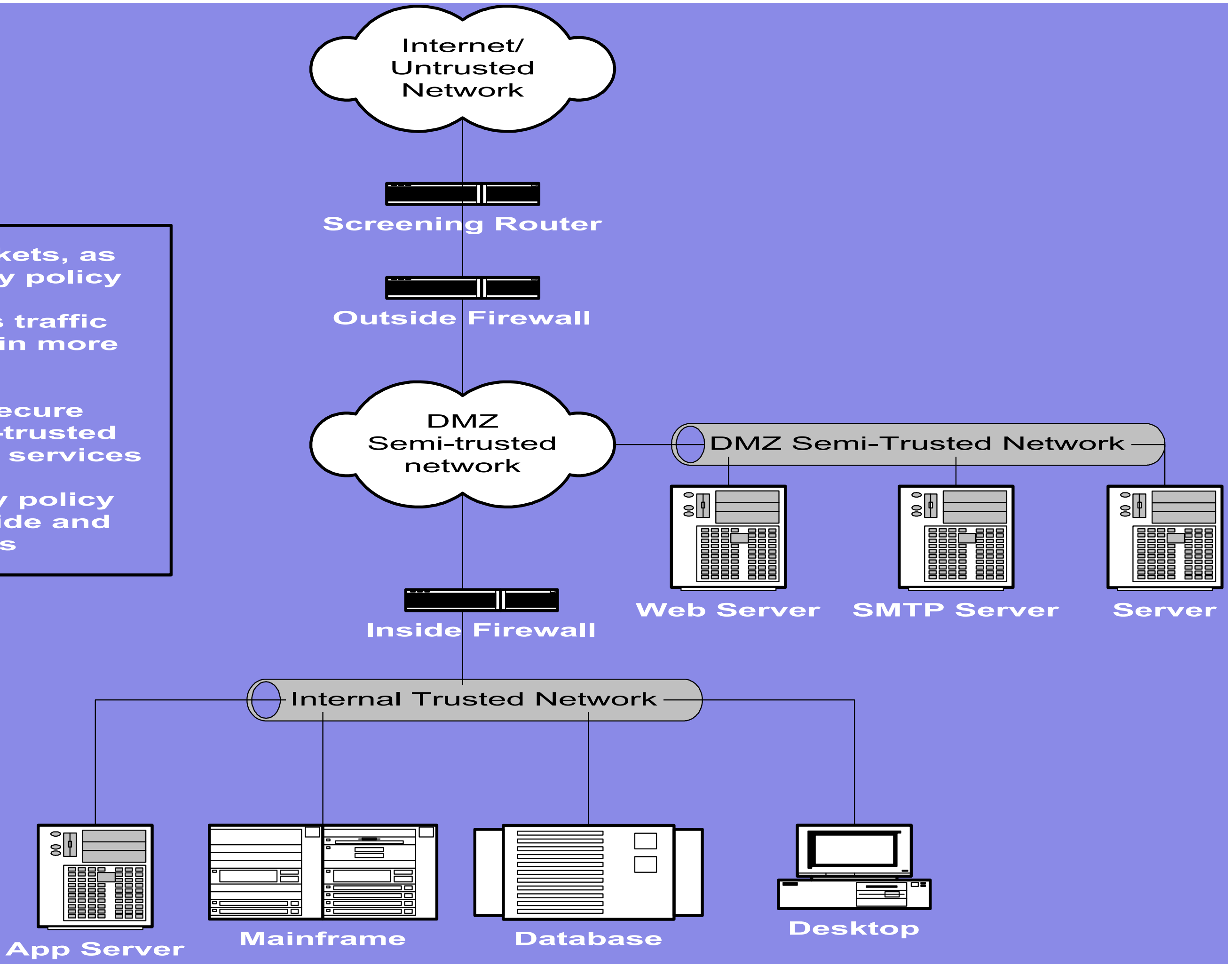
Firewall Sandwich

Routes or blocks packets, as determined by security policy

Firewall then handles traffic additionally to maintain more security

DMZ now offers a secure network to handle un-trusted connections to internet services

Separation of security policy controls between inside and outside firewalls



Internet/ Untrusted Network

Screening Router

Outside Firewall

DMZ Semi-trusted network

DMZ Semi-Trusted Network

Web Server

SMTP Server

Server

Inside Firewall

Internal Trusted Network

App Server

Mainframe

Database

Desktop

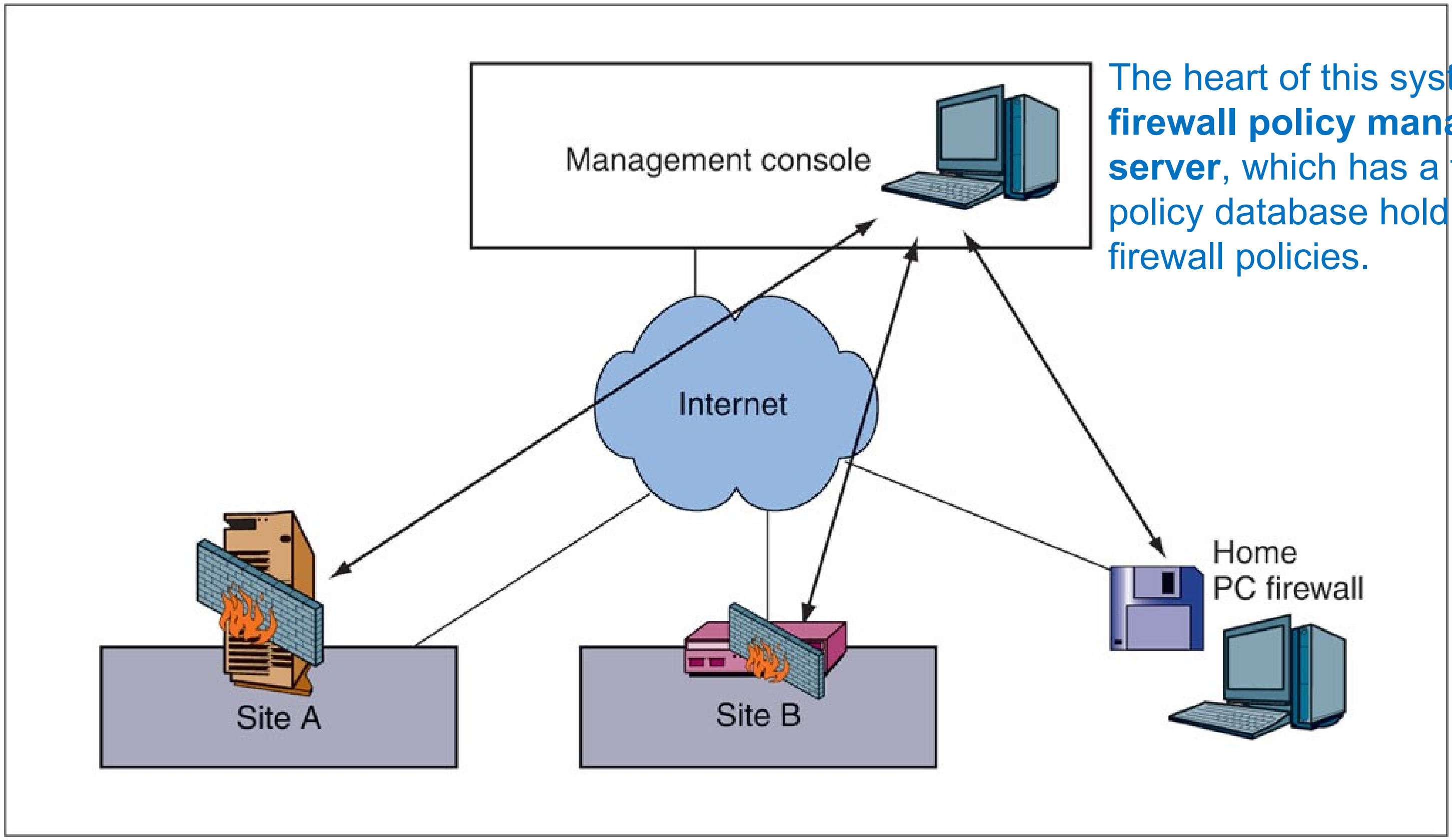
Firewall Management

- Defining Firewall Policies
  - Policies are high-level statements about what to do
  - For example, HTTP connections from the Internet may only go to servers in the DMZ
  - Policies are more comprehensible than actual firewall rules
  - There may be multiple ways to implement a policy

Firewall Management

- Implementation
  - Firewall hardening
  - Central firewall management systems
  - Vulnerability testing after configuration
  - Change authorization and management
  - Reading the firewall logs
  - Attackers can be black holed (have their packets dropped)

Central Firewall Management System



The heart of this system is the **firewall policy management server**, which has a firewall policy database holding the firm’s firewall policies.

Firewall Filtering Problems

- Protecting the Perimeter Is No Longer Possible
  - There are too many ways to get through the perimeter
- Avoiding the Border Firewall
  - Internal attackers are inside the firewall already
  - Compromised internal hosts are inside the firewall
  - Wireless LAN drive-by hackers enter through access points that are inside the site
  - Home notebooks, mobile phones, and media brought into the site
  - Internal firewalls can address some of these threats

Firewall Filtering Problems

- Extending the Perimeter
  - Remote employees must be given access
  - Consultants, outsourcers, customers, suppliers, and other subsidiaries must be given access
  - Essentially, all of these tend to use VPNs to make external parties “internal” to your site
- Most Filtering Methods Use Attack Signature Detection
  - Each attack has a signature
  - This attack signature is discovered
  - The attack signature is added to the firewall

Firewall Filtering Problems

- Problem
  - Zero-day attacks are attacks without warning, and occur before a signature is developed
  - Signature defense cannot stop zero-day attacks
- Anomaly Detection
  - Detects an unusual pattern indicating a possible attack
  - This is difficult, so there are many false positives
  - Shrinking time needed to define signatures
  - Anomaly detection is necessary in today’s firewalls

Firewall

- In Windows 10, Vista, and XP, software firewalls are built into the operating system. Earliest versions of Windows did not have firewalls built in.
- Macintosh computers running macOS 11 also equipped with a built-in firewall.
- Third-party firewall packages also exist, such as Cisco ASA, Palo Alto Networks Next-Gen Firewalls, Fortinet FortiGate, Norton Personal Firewall, Black Ice Protection, and McAfee Personal Firewall.
- Many of these offer free versions or trials of their commercial versions.

Reference

Chapter 6

Corporate Computer Security, 5th Edition Boyle R.J. & Panko R. R. by Pearson

Copyright