Introduction to Cyber Security

Module 4

Network Security

Topics

- Firewalls
- Proxies
- DMZ
- Internet security protocols and standards
- Intrusion detection and prevention

Why Network Security is Important?

- Network security is a broad term that covers a multitude of technologies, devices and processes.
- In its simplest term, it is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies.
- Every organization, regardless of size, industry or infrastructure, requires a degree of network security solutions in place to protect it from the ever-growing landscape of cyber threats today.
- Today's network architecture is complex and is faced with a threat environment that is always changing and attackers that are always trying to find and exploit vulnerabilities.
- These vulnerabilities can exist in a broad number of areas, including devices, data, applications, users and locations.
- For this reason, there are many network security management tools and applications in use today that address individual threats and exploits.

How does Network Security Work ?

- There are many layers to consider when addressing network security across an organization.
- Attacks can happen at any layer in the network security layers model, so our network security hardware, software and policies must be designed to address each area.
- Network security typically consists of three different controls: *physical, technical and administrative.*

- **Physical Network Security**

✓ Physical security controls are designed to prevent unauthorized personnel from gaining physical access to network components such as routers, cabling cupboards and so on.

✓ Controlled access, such as locks, biometric authentication and other devices, is essential in any organization.

Contd…

- **Technical Network Security**

✓ Technical security controls protect data that is stored on the network or which is in transit across, into or out of the network.

✓ Protection is twofold; it needs to protect data and systems from unauthorized personnel, and it also needs to protect against malicious activities from employees.

- **Administrative Network Security**

✓ Administrative security controls consist of security policies and processes that control user behavior, including how users are authenticated, their level of access and also how IT staff members implement changes to the infrastructure.

Types of Network Security

1. Network Access Control
2. Antivirus and Antimalware Software
3. Firewall Protection
4. Virtual Private Networks

Network Access Control

- To ensure that potential attackers cannot infiltrate your network, comprehensive access control policies need to be in place for both users and devices.
- Network access control (NAC) can be set at the most granular level.
- For example, you could grant administrators full access to the network but deny access to specific confidential folders or prevent their personal devices from joining the network.

Antivirus and Antimalware Software

- Antivirus and antimalware software protect an organization from a range of malicious software, including viruses, ransomware, worms and trojans.
- The best software not only scans files upon entry to the network but continuously scans and tracks files.

Firewall Protection

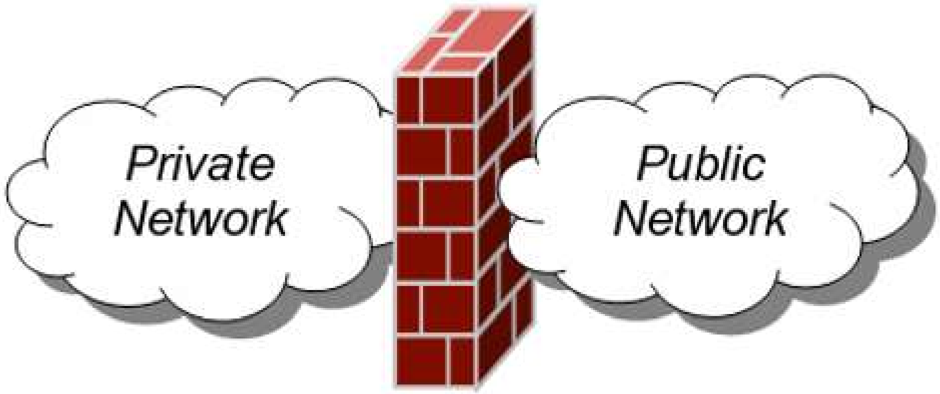
- Firewalls, as their name suggests, act as a barrier between the untrusted external networks and your trusted internal network.
- Administrators typically configure a set of defined rules that blocks or permits traffic onto the network.
- For example, Forcepoint's Next Generation Firewall (NGFW) offers seamless and centrally managed control of network traffic, whether it is physical, virtual or in the cloud.

Virtual Private Networks

- Virtual private networks (VPNs) create a connection to the network from another endpoint or site.
- For example, users working from home would typically connect to the organization's network over a VPN.
- Data between the two points is encrypted and the user would need to authenticate to allow communication between their device and the network.
- Forcepoint's Secure Enterprise SD-WAN allows organizations to quickly create VPNs using drag-and-drop and to protect all locations with our Next Generation Firewall solution.

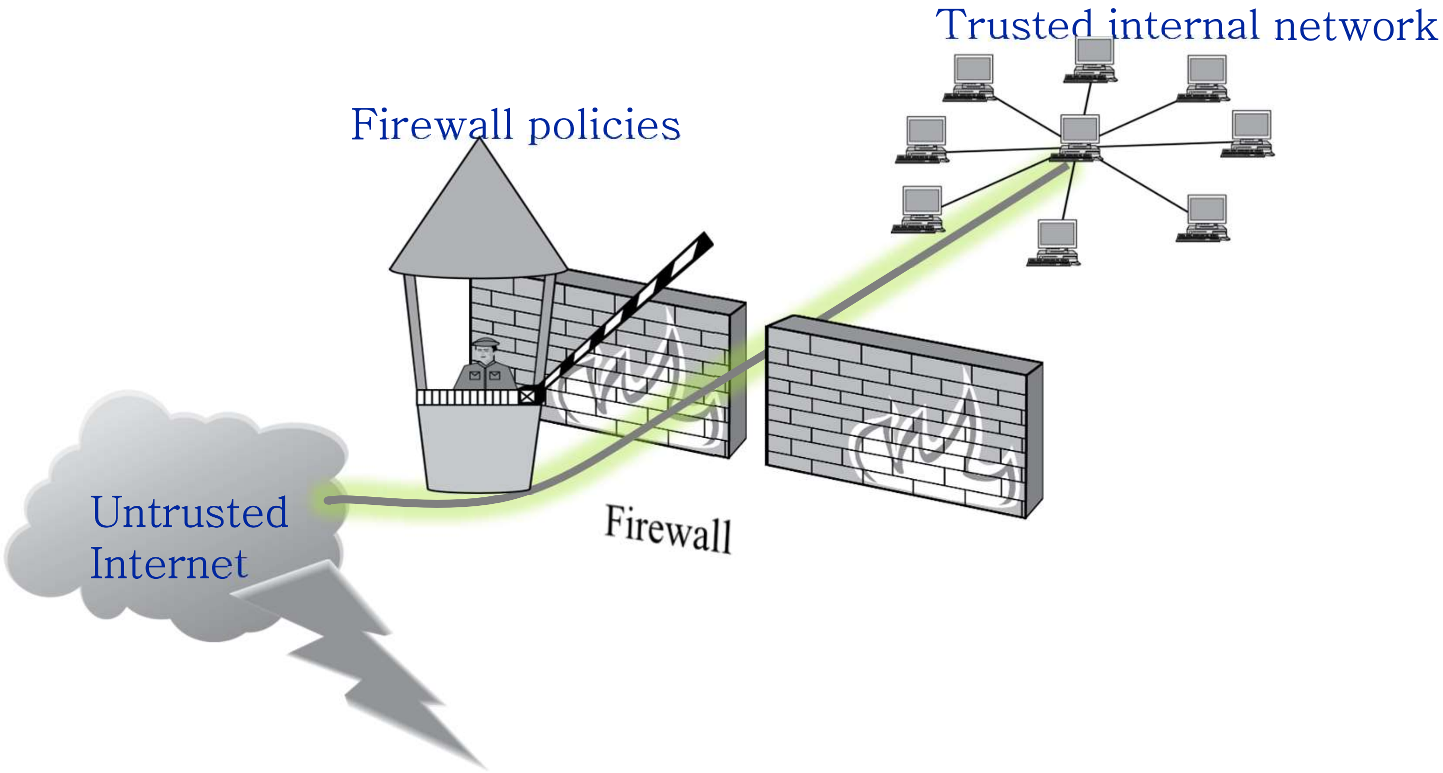
Firewall

- A **firewall** is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system.
- A network firewall is similar to firewalls in building construction, because in both cases they are intended to isolate one "network" or "compartment" from another.



Firewall Policies

- To protect private networks and individual machines from the dangers of the greater Internet, a firewall can be employed to filter incoming or outgoing traffic based on a predefined set of rules called **firewall policies**.



Policy Actions

- Packets flowing through a firewall can have one of three outcomes:
  - **Accepted:** permitted through the firewall
  - **Dropped:** not allowed through with no indication of failure
  - **Rejected:** not allowed through, accompanied by an attempt to inform the source that the packet was rejected
- Policies used by the firewall to handle packets are based on several properties of the packets being inspected, including the protocol used, such as:
  - TCP or UDP
  - **the source and destination IP addresses**
  - **the source and destination ports**
  - the application-level payload of the packet (e.g., whether it contains a virus).

Blacklist and Whitelist

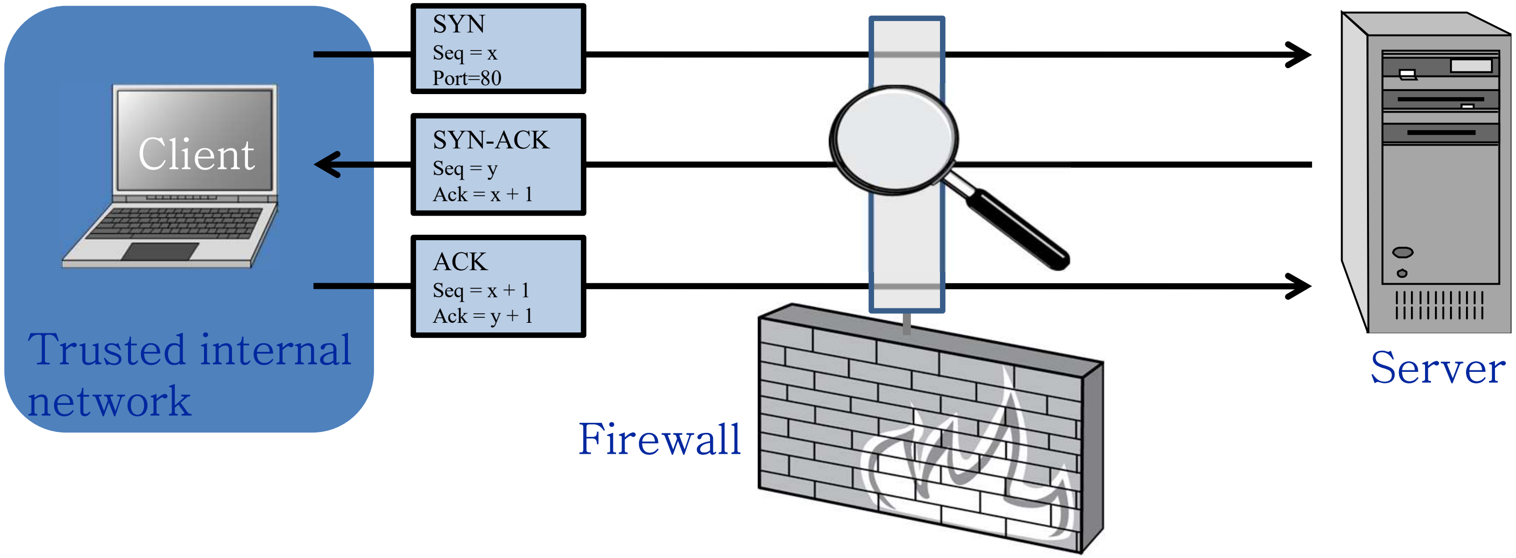
- Two fundamental approaches to creating firewall policies (or rulesets)
- **Blacklist** approach (default-allow)
  - All packets are allowed through except those that fit the rules defined specifically in a blacklist.
  - Pros: flexible in ensuring that service to the internal network is not disrupted by the firewall
  - Cons: unexpected forms of malicious traffic could go through
- **Whitelist** approach (default-deny)
  - Packets are dropped or rejected unless they are specifically allowed by the firewall
  - Pros: A safer approach to defining a firewall ruleset
  - Cons: must consider all possible legitimate traffic in rulesets

Firewall Types

- **packet filters (stateless)**
  - If a packet matches the packet filter's set of rules, the packet filter will drop or accept it
- **"stateful" filters**
  - it maintains records of all connections passing through it and can determine if a packet is either the start of a new connection, a part of an existing connection, or is an invalid packet.
- **application layer**
  - It works like a **proxy** it can “understand” certain applications and protocols.
  - It may inspect the contents of the traffic, blocking what it views as inappropriate content (i.e. websites, viruses, vulnerabilities, ...)

Stateless Firewall

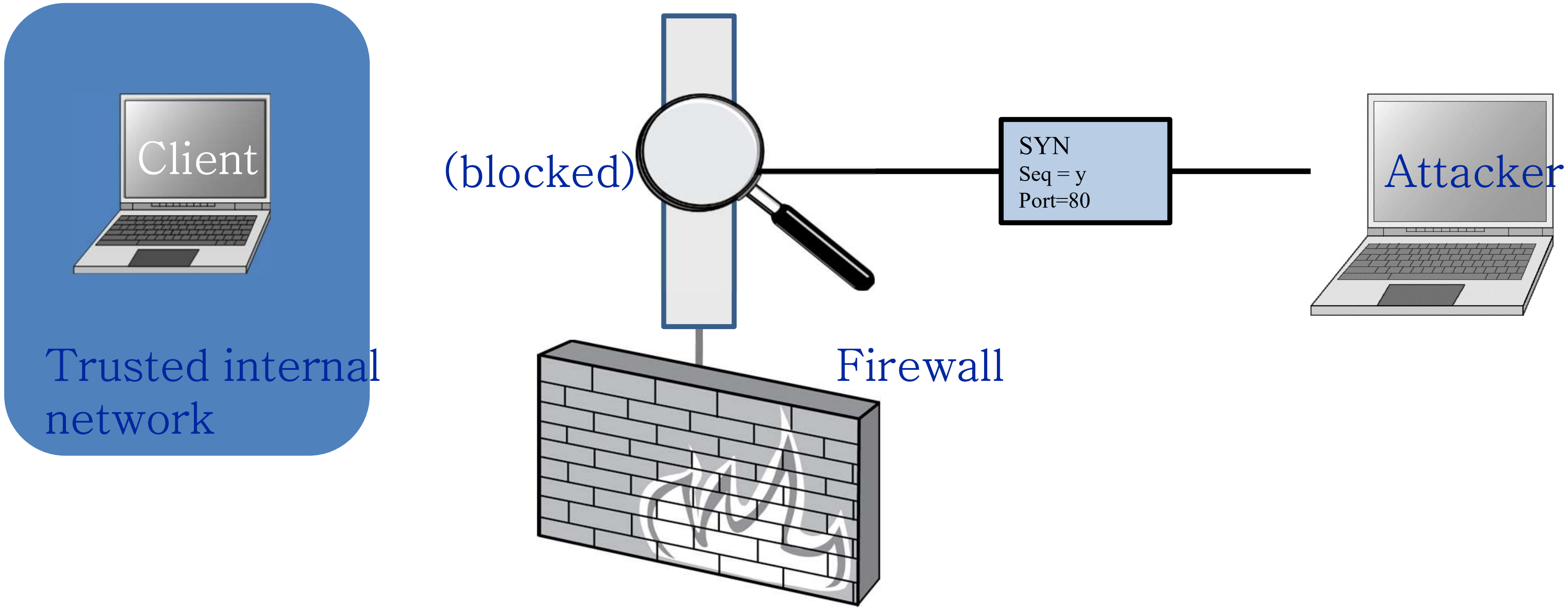
- A stateless firewall doesn't maintain any remembered context (or "state") with respect to the packets it is processing.
- Instead, it treats each packet attempting to travel through it in isolation without considering packets that it has processed previously.



Allow outbound SYN packets, destination port=80
Allow inbound SYN-ACK packets, source port=80

Stateless Restrictions

- Stateless firewalls may have to be fairly restrictive in order to prevent most attacks.



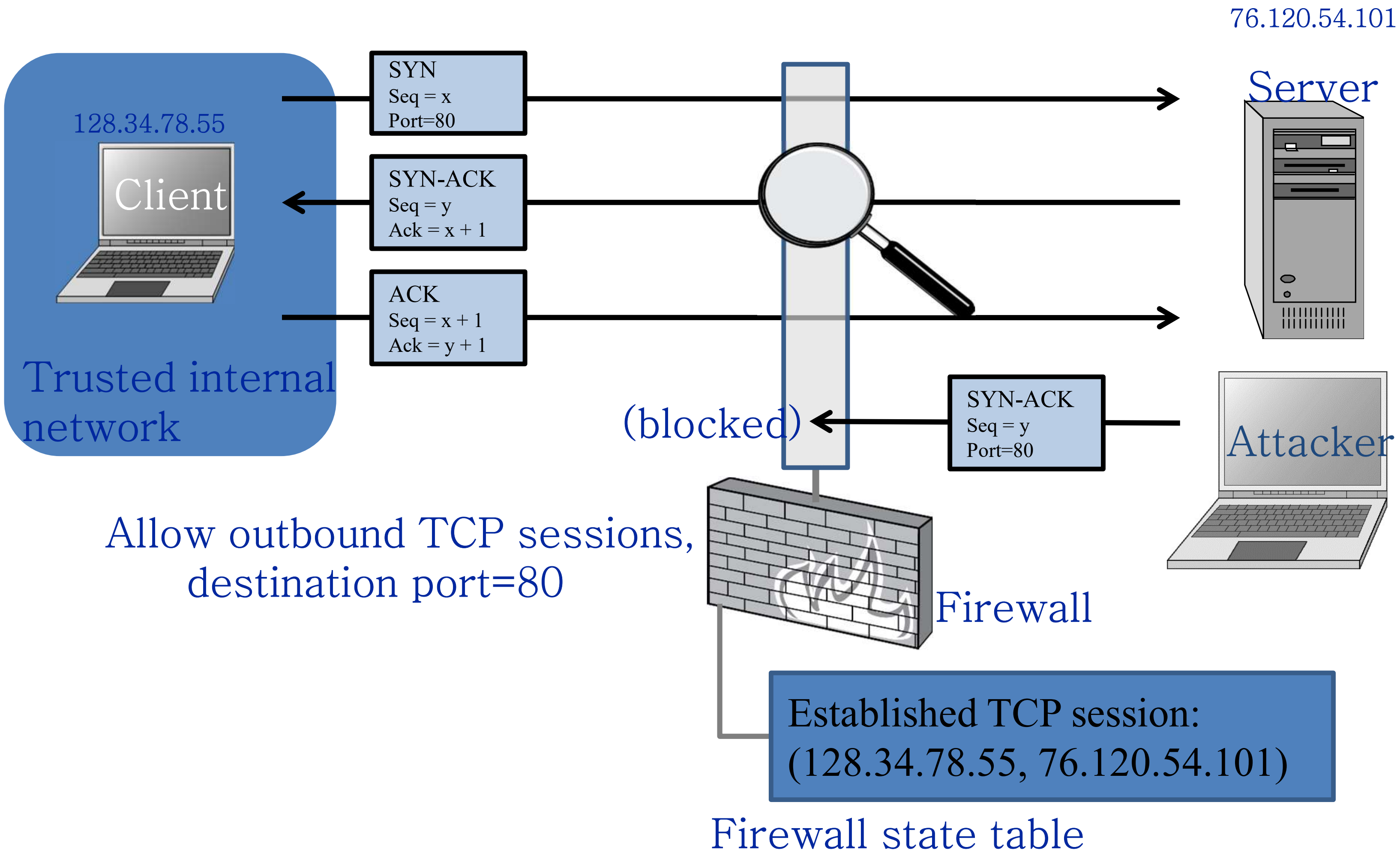
Allow outbound SYN packets, destination port=80
Drop inbound SYN packets,
Allow inbound SYN-ACK packets, source port=80

Stateful Firewall

- **Stateful firewalls** can tell when packets are part of legitimate sessions originating within a trusted network.
- Stateful firewalls maintain tables containing information on each active connection, including the IP addresses, ports, and sequence numbers of packets.
- Using these tables, stateful firewalls can allow only inbound TCP packets that are in response to a connection initiated from within the internal network.

Example

- Allow only requested TCP connections:



Allow outbound TCP sessions, destination port=80

Established TCP session: (128.34.78.55, 76.120.54.101)

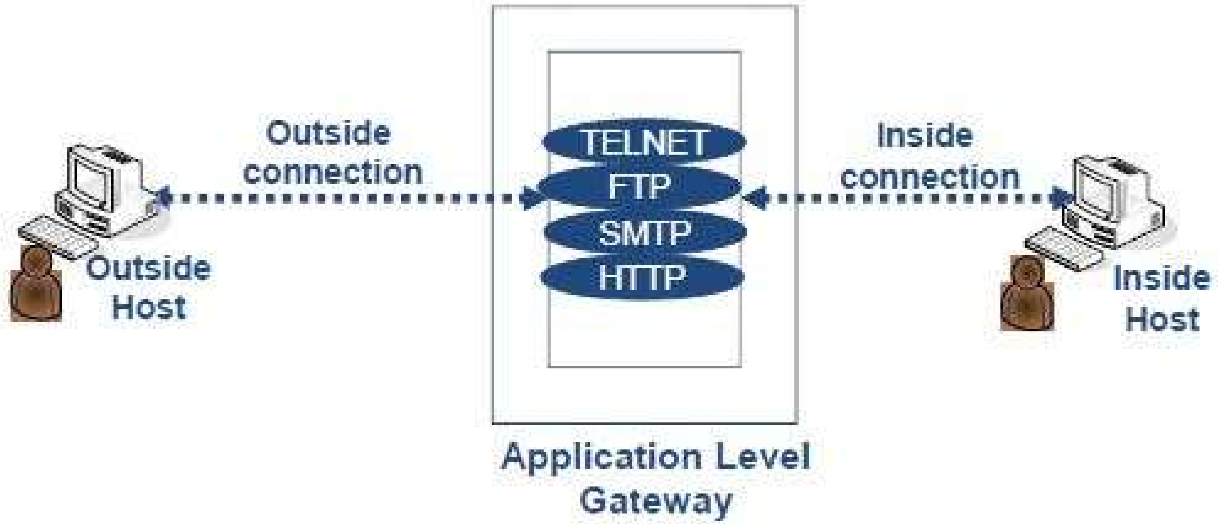
Firewall state table

Contd…

- TCP-based connections are easy to check
  - TCP SYN packet
- UDP-based traffic is not so clear
  - There is no UDP connection set up
  - Treat a UDP session starts when a legitimate UDP packet is allowed through the firewall (such as from inside to outside)
  - Session is defined by (source IP, source port, dest IP, dest port)

Application Level Firewall

- An application firewall is a type of firewall that scans, monitors and controls network, Internet and local system access and operations to and from an application or service.
- This type of firewall makes it possible to control and manage the operations of an application or service that's external to the IT environment.

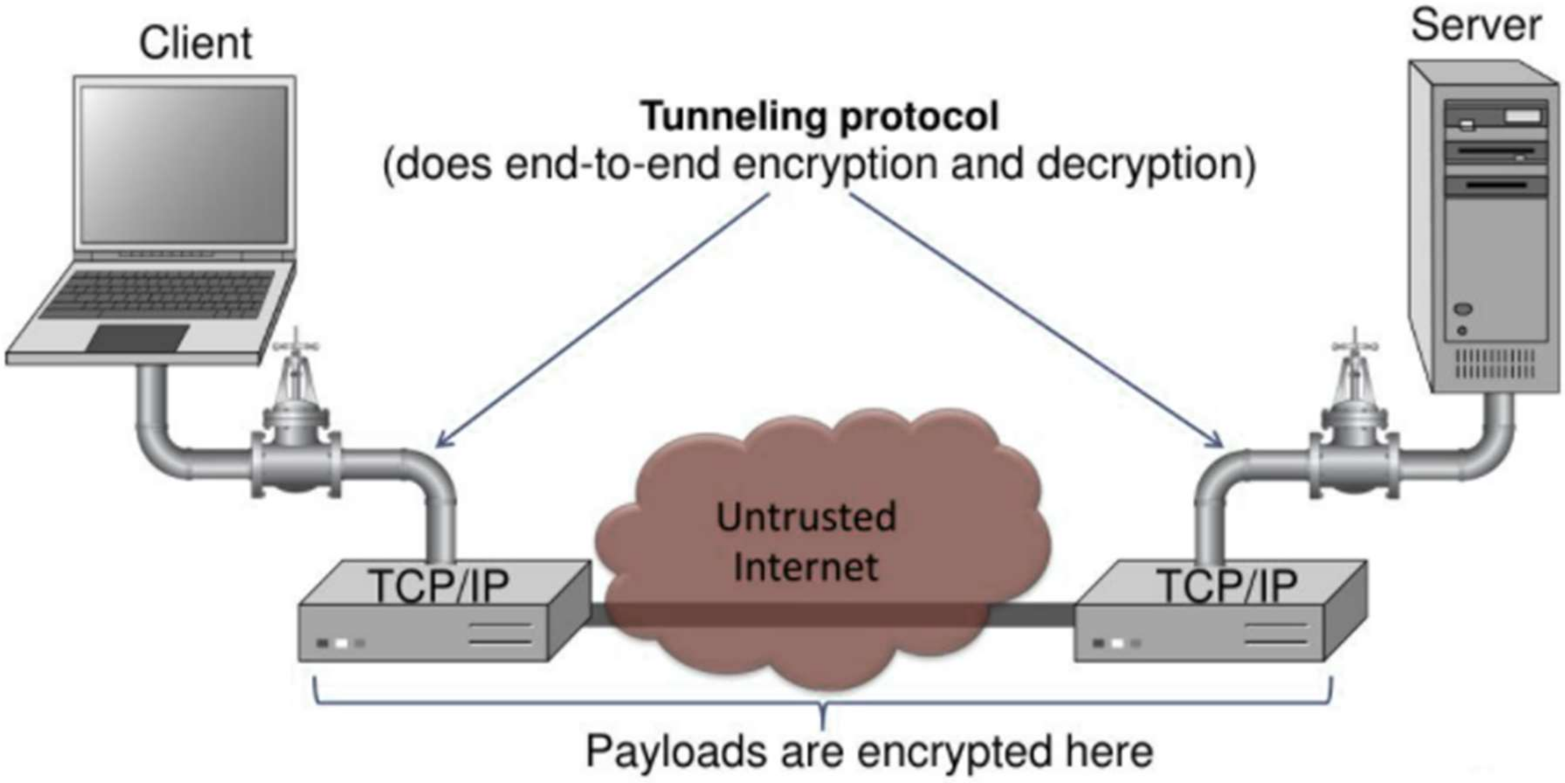


Tunnels

- The contents of TCP packets are not normally encrypted, so if someone is eavesdropping on a TCP connection, he can often see the complete contents of the payloads in this session.
- One way to prevent such eavesdropping without changing the software performing the communication is to use a **tunneling protocol.**
- In such a protocol, the communication between a client and server is automatically encrypted, so that useful eavesdropping is infeasible.

Tunneling Prevents Eavesdropping

- Packets sent over the Internet are automatically encrypted.


Client
Server
Tunneling protocol
(does end-to-end encryption and decryption)
Untrusted Internet
TCP/IP
TCP/IP
Payloads are encrypted here

Intrusion Detection System

- **Intrusion**
  - Actions aimed at compromising the security of the target (confidentiality, integrity, availability of computing / networking resources)

- **Intrusion detection**
  - The identification through intrusion signatures and report of intrusion activities

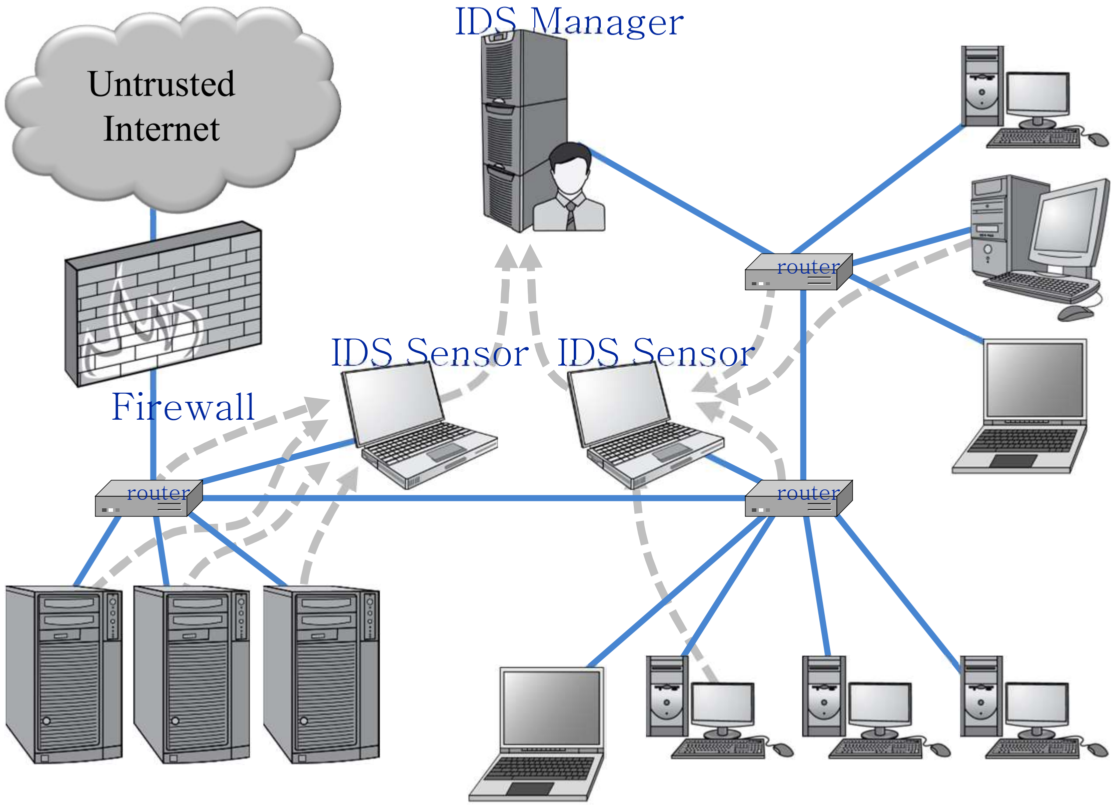
- **Intrusion prevention**
  - The process of both detecting intrusion activities and managing automatic responsive actions throughout the network

IDS Components

- **Sensors**: Sensors are responsible for collecting data.
- **Analyzers**: Analyzers receive input from one or more sensors or from other analyzers. The analyzer is responsible for determining if an intrusion has occurred.
- **User Interface:** The user interface to an IDS enables a user to view output from the system or control the behavior of the system. In some systems, the user interface may equate to a manager, director, or console component.

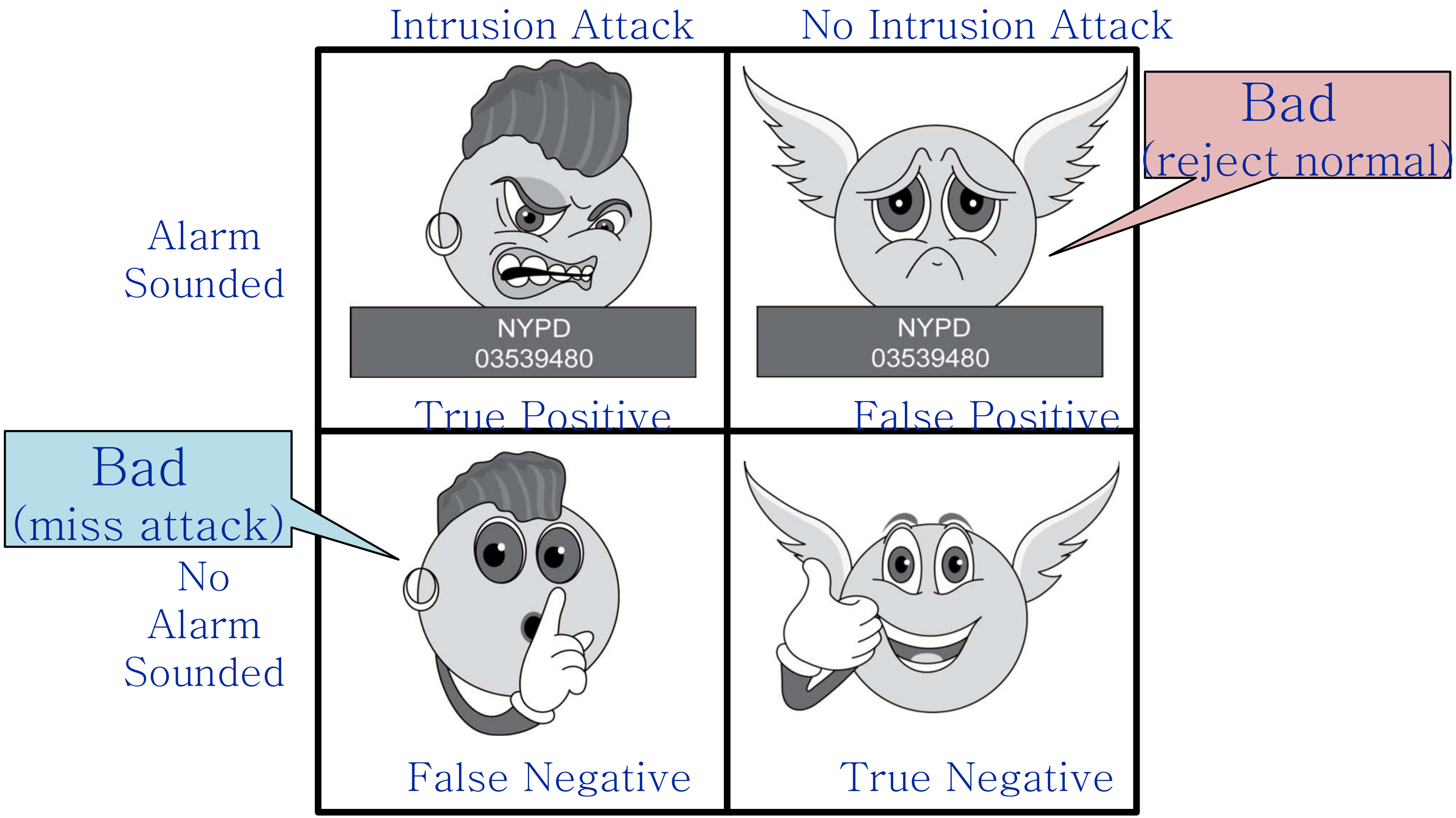
Contd…

- **IDS analyzer (manager)** compiles data from the IDS sensors to determine if an intrusion has occurred.
- If an IDS manager detects an intrusion, then it sounds an **alarm**.



Possible Alarm Outcomes

- Alarms can be sounded (positive) or not (negative).

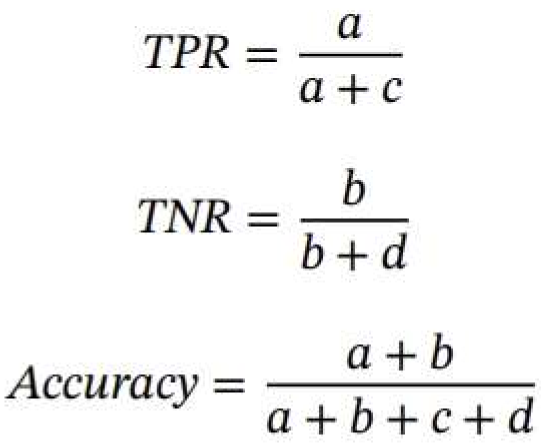


	Intrusion Attack	No Intrusion Attack
Alarm Sounded	True Positive	False Positive
No Alarm Sounded	False Negative	True Negative

Bad (reject normal)

Bad (miss attack)

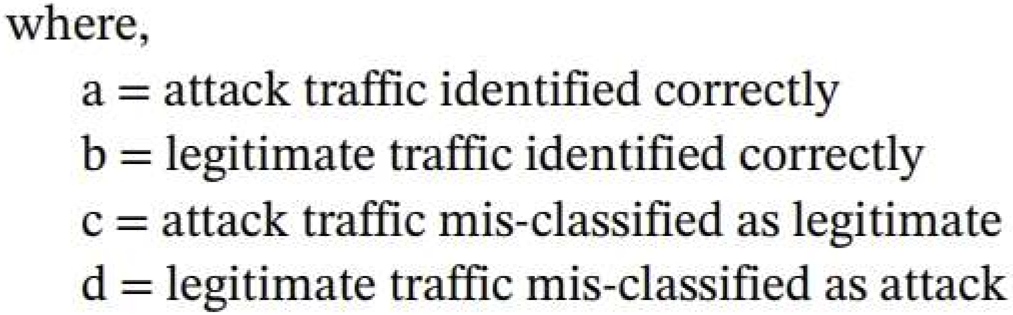
How to calculate the accuracy of an IDS?



$$TPR = \frac{a}{a+c}$$

$$TNR = \frac{b}{b+d}$$

$$Accuracy = \frac{a+b}{a+b+c+d}$$



where,

a = attack traffic identified correctly

b = legitimate traffic identified correctly

c = attack traffic mis-classified as legitimate

d = legitimate traffic mis-classified as attack

TPR: True Positive Rate

TNR: True Negative Rate

Base-Rate Fallacy

- true-positive rate is conflict with false-negative rate.

✓ There is a trade-off

- If # of intrusions << # of all events, the effectiveness of an intrusion detection system can be reduced.
- In particular, the effectiveness of some IDSs can be misinterpreted due to a statistical error known as the base-rate fallacy.
- This type of error occurs when the probability of some conditional event is assessed without considering the "base rate" of that event.

Contd…

- Suppose an IDS has 1% chance of false positives, and 1% of false negatives. Suppose further…
  - An intrusion detection system generates 1,000,100 log entries.
  - Only 100 of the 1,000,100 entries correspond to actual malicious events.
- Among the 100 malicious events, 99 will be detected as malicious, which means we have **1 false negative.**
- Among the 1,000,000 benign events, 10,000 will be mistakenly identified as malicious. That is, we have **10,000 false positives!**
- Thus, there will be 10,099 alarms sounded, 10,000 of which are false alarms. That means false alarm rate is roughly 99%!

Types of IDS

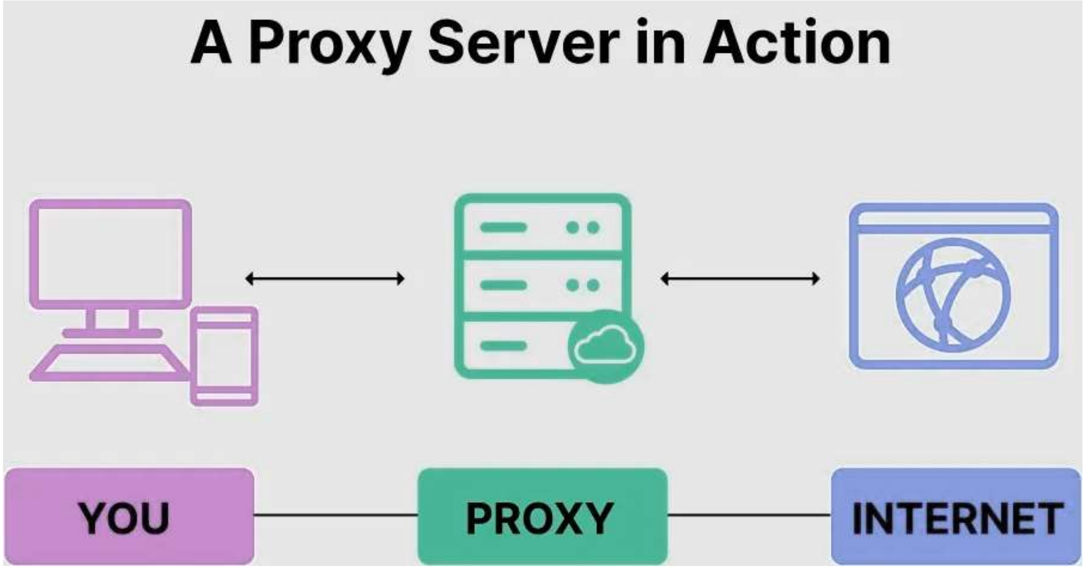
- **Host-based IDS (HIDS)**: Monitors the characteristics of a single host and the events occurring within that host, such as process identifiers and the system calls they make, for evidence of suspicious activity.
- **Network-based IDS (NIDS)**: Monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity.
- **Distributed or hybrid IDS**: Combines information from a number of sensors, often both host and network-based, in a central analyzer that is able to better identify and respond to intrusion activity.

Analysis Approaches

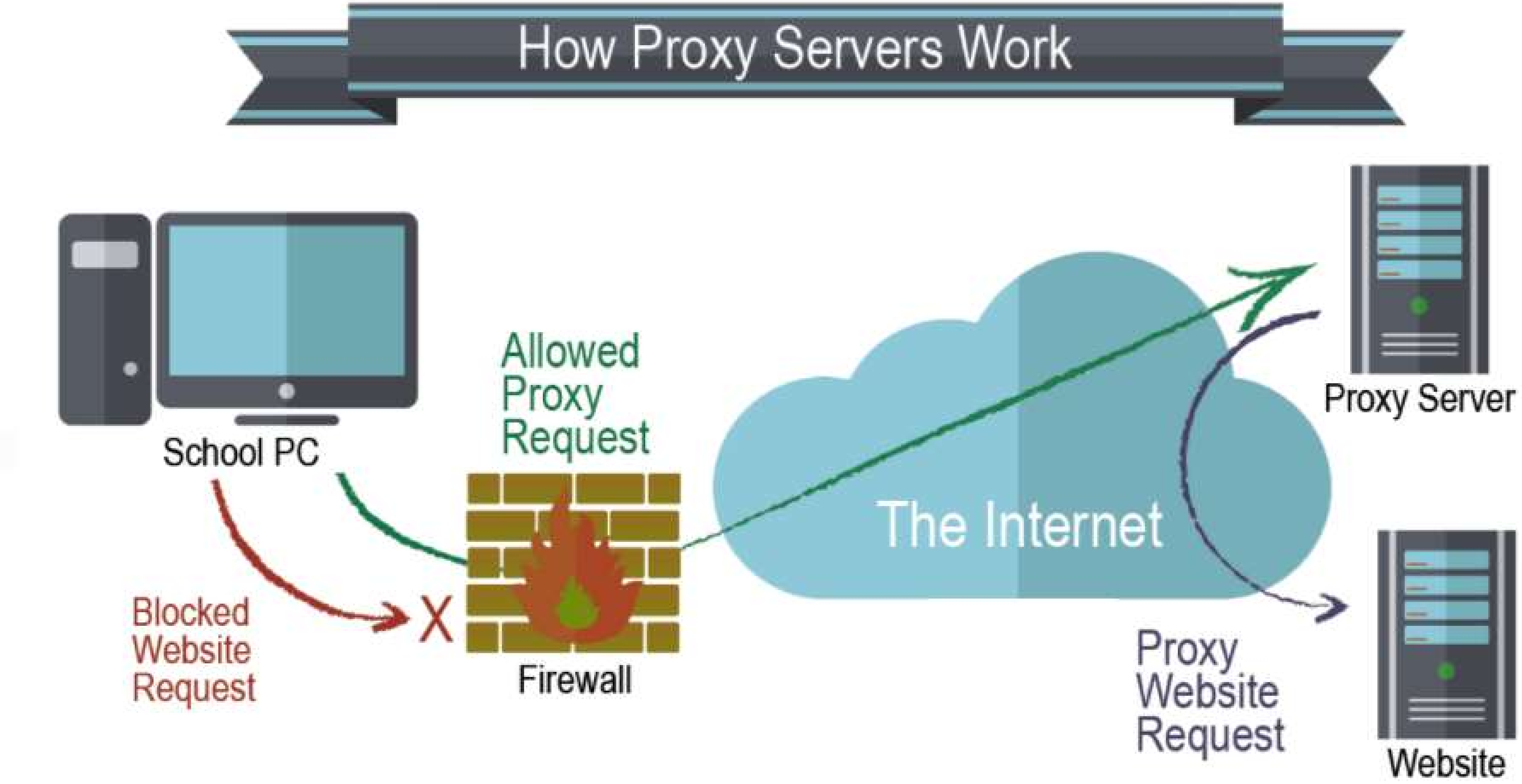
- **Rule/Signature Based Intrusion Detection**
  - Rules and signatures identify the types of actions that match certain known profiles for an intrusion attack
  - Alarm raised can indicate what attack triggers the alarm
  - Problem: Cannot deal with unknown attacks
- **Statistical/Anomaly Based Intrusion Detection**
  - Statistical representation (**profile**) of the typical ways that a user acts or a host is used
  - Determine when a user or host is acting in highly unusual, anomalous ways.
  - Alarm when a user or host deviates significantly from the stored profile for that person or machine
  - Problem: High false positive rate, cannot tell which attack triggers the alarm

Proxy Server

- A proxy server provides a gateway between users and the internet. It is a server, referred to as an "intermediary" because it goes between end-users and the web pages they visit online.
- Because a proxy server has its own IP address, it acts as a go-between for a computer and the internet. Your computer knows this address, and when you send a request on the internet, it is routed to the proxy, which then gets the response from the web server and forwards the data from the page to your computer's browser.



Hide Your Real IP Address Behind a Proxy



Benefits of a Proxy Server

- **Enhanced security:** Can act like a firewall between your systems and the internet. Without them, hackers have easy access to your IP address, which they can use to infiltrate your computer or network.
- **Private browsing, watching, listening, and shopping:** Use different proxies to help you avoid getting inundated with unwanted ads or the collection of IP-specific data.
- **Access to location-specific content:** You can designate a proxy server with an address associated with another country. You can, in effect, make it look like you are in that country and gain full access to all the content computers in that country are allowed to interact with.
- **Prevent employees from browsing inappropriate or distracting sites:** You can use it to block access to websites that run contrary to your organization's principles. Some organizations block social media sites like Facebook.

Types of Proxy Servers

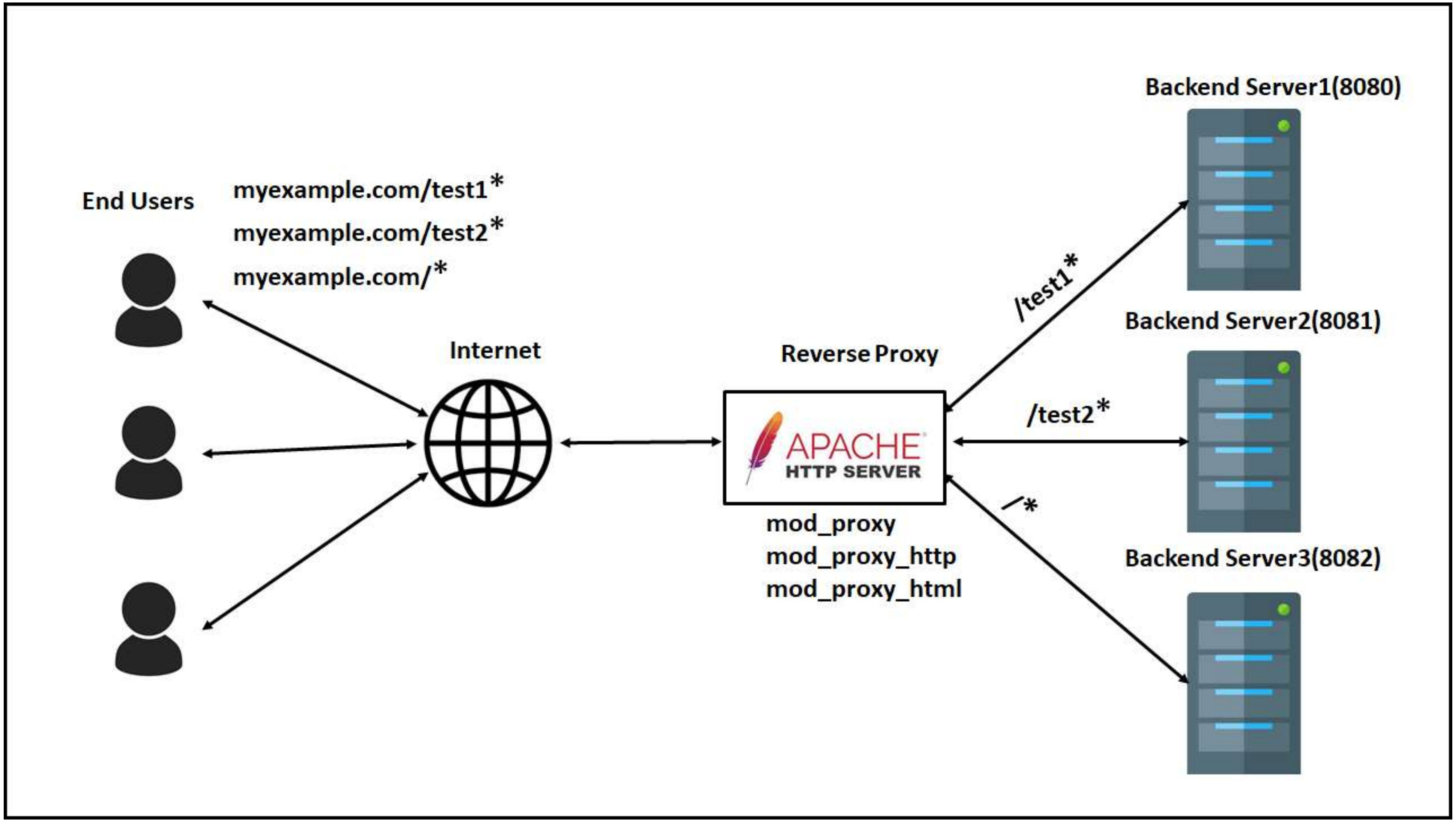
1. Forward Proxies:

- ✓ A forward proxy server sits between the client and an external network. It evaluates the outbound requests and takes action on them before relaying that request to the external resource.
- ✓ Most proxy services that we’re likely to encounter are forward proxies. Virtual Private Networks and Web content filters are both examples of forward proxies.

2. Reverse Proxies:

- ✓ A reverse proxy server sits between a network and multiple other internal resources.
- ✓ A large website might have dozens of servers that collectively serve requests from a single domain.
- ✓ To accomplish that, client requests would resolve to a machine that would act as a load balancer.
- ✓ The load balancer would then proxy that traffic back to the individual servers.
- ✓ Some popular open source reverse proxies are: Varnish, Squid

Contd…



Assignment: Study other types of proxies.

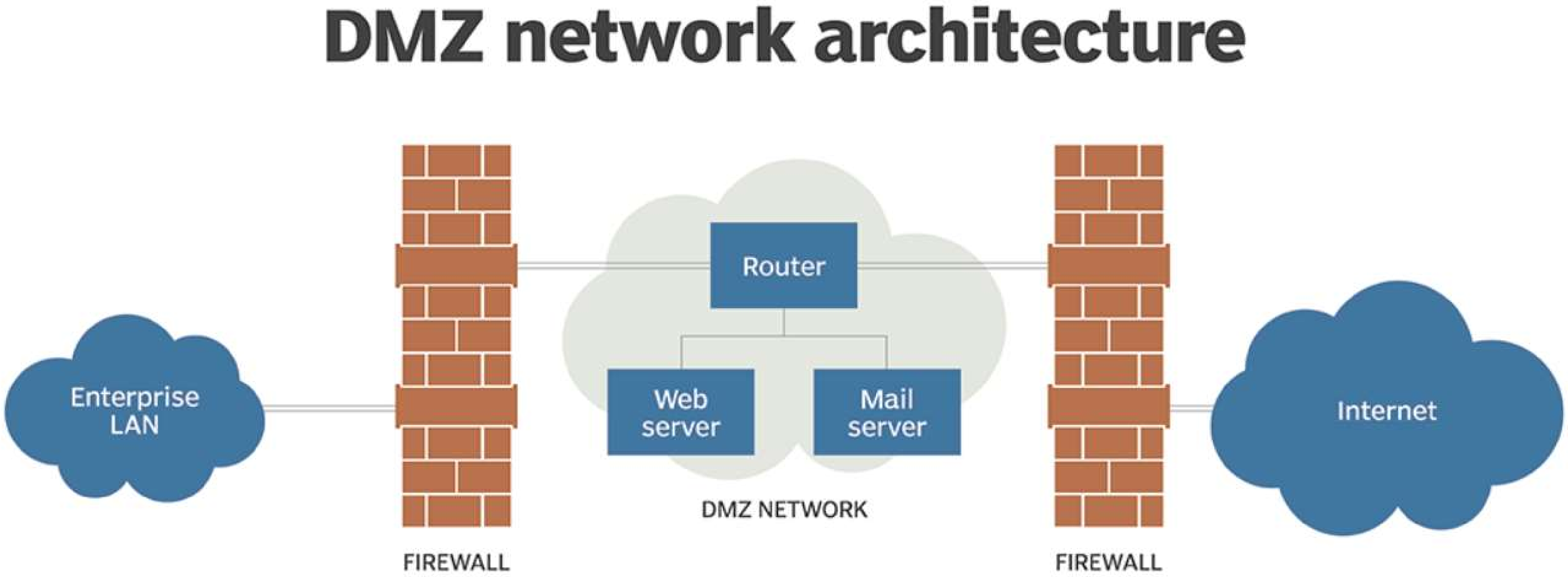
Demilitarized Zone (DMZ)

- In computer networks, a DMZ, or demilitarized zone, is a physical or logical subnet that separates a local area network (LAN) from other untrusted networks -- usually, the public internet.
- DMZs are also known as perimeter networks or screened subnetworks.
- DMZs provide a level of network segmentation that helps protect internal corporate networks. These subnetworks restrict remote access to internal servers and resources, making it difficult for attackers to access the internal network. This strategy is useful for both individual use and large organizations.
- Businesses place applications and servers that are exposed to the internet in a DMZ, separating them from the internal network. The DMZ isolates these resources so, if they are compromised, the attack is unlikely to cause exposure, damage or loss.

How does DMZ Work?

- DMZs function as a buffer zone between the public internet and the private network. The DMZ subnet is deployed between two firewalls. All inbound network packets are then screened using a firewall or other security appliance before they arrive at the servers hosted in the DMZ.
- If better-prepared threat actors pass through the first firewall, they must then gain unauthorized access to the services in the DMZ before they can do any damage. Those systems are likely to be hardened against such attacks.
- Finally, assuming well-resourced threat actors take over a system hosted in the DMZ, they must still break through the internal firewall before they can reach sensitive enterprise resources.

Contd…


DMZ network architecture
Router
Web server
Mail server
DMZ NETWORK
Enterprise LAN
FIREWALL
FIREWALL
Internet

Thank You !!!