Network Firewall

Dr. Risala Tasin Khan

Professor, IIT, JU

Introduction

- A firewall is a security system or network security policy designed to prevent unauthorized access to or from a private network and basically limits access to a network from another network. It isolates an organization's internal network from larger Internet, allowing some packets to pass, blocking others.
- A firewall is the first line of defense for your network.
- The purpose of a firewall is to keep intruders from gaining access to your network.
- Usually placed at the perimeter of network to act as a gatekeeper for incoming and outgoing traffic
- It protects your computer from Internet threats by erecting a virtual barrier between your network or computer and the Internet
- Every business organization that is connected to the Internet needs a firewall to protect the internal network from attacks.

An Internet firewall has the following properties:

- it is a single point between two or more networks where all traffic must pass.
- traffic can be controlled by and may be authenticated through the device.
- all traffic is logged.

How Does a Firewall Works

- A firewall may consist of several pieces of equipments, including a router, a gateway server, and an authentication server.
- Firewalls are setup at every connection to the Internet, therefore subjecting all data flow to careful monitoring.

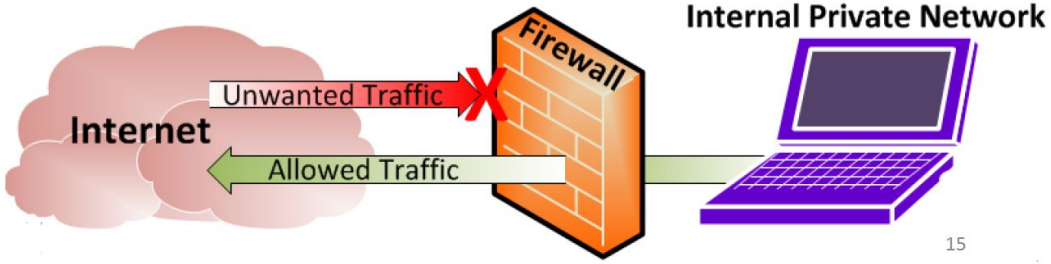
- Firewall examines the traffic sent between two networks

- Data is examined to see if it appears legitimate:
  - if so the data is allowed to pass through
  - If not, the data is blocked
- A firewall allows you to establish certain rules to determine what traffic should be allowed in or out of your private network

- Rules will decide-
  - who can connect to the internet
  - what kind of connections can be made,
  - which or what kind of files can be transmitted in /out.
- Sophisticated logging, auditing, and intrusion detection tools are now part of most commercial firewalls.
- Basically all traffic in and out can be watched and controlled thus giving the firewall installer a high level of security and protection.

Rules and Security Policies

- Traffic blocking rules can be based upon:
  - Words or phrases
  - Domain names
  - IP addresses
  - Ports
  - Protocols (e.g. FTP)
- While firewalls are essential, they can block legitimate transmission of data and programs
- Firewall security policy:
  - What services can be accessed
  - What IP addresses and ranges are restricted
  - What ports can be accessed



Firewall Technologies

- Firewall technologies may be implemented as a
  - Software product running on a server
  - Specialized hardware appliance
- Firewall monitors data packets coming into and out of the network it is protecting
- Packets are filtered by:
  - Source and destination addresses and ports
  - Header information
  - Protocol type
  - Packet type
  - Service
  - Data content – i.e. application and file data content

Basic Types of Firewall

- There are several types of firewall:
  - 1. Host-based Firewall
  - 2. Network-based Firewall
  - 3. Hardware Firewall
  - 4. Software Firewall

1. Host-based Firewall:

- Host-based firewalls are sometimes called “personal” firewalls.
- They are simple, low cost programs or devices intended to protect a single computer.
- A personal firewall controls network traffic to and from a computer, permitting or denying communications based on a security policy.
- **Typically it works as an application layer firewall**.
  - Examples include ZoneAlarm, Norton Personal Firewall, and the Internet Connection Firewall (ICF) built into Windows XP.

Basic Types of Firewalls

2. Network-based Firewall:

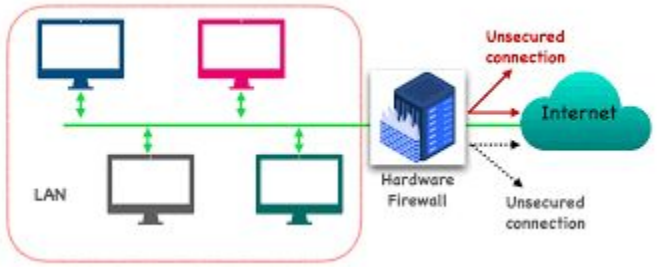
- Network firewalls can protect multiple computers.
- However, not all network firewalls are created equal.
- Some are simple devices or programs that cost little more than personal firewalls.
- Many consumer-grade DSL and cable routers include this type of firewall technology.
- Simple network firewalls perform packet filtering.
- Enterprise firewalls are “all business” type and are designed for large, complex networks.

- They will handle many more users, have faster throughput, and have advanced features.

Basic Types of Firewall

3. Hardware Firewall:

- Hardware firewalls are usually routers with a built in Ethernet card and hub.
- Your computer or computers on your network connect to this router and access the web.
- Hardware firewalls can be purchased as a stand-alone product but more recently hardware firewalls are typically found in broadband routers, and should be considered an important part of your system and network set-up.
- A hardware firewall uses packet filtering to examine the header of a packet to determine its source and destination.
- This information is compared to a set of predefined or user-created rules that determine whether the packet is to be forwarded or dropped.



Basic Types of Firewall

3. Hardware Firewall (continue…):

- Hardware firewalls can be effective with little or no configuration, and they can protect every machine on a local network.
- Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, business networking firewall solutions are available.

- To ensure that your hardware firewall is configured for optimal security and protection, consumers will need to learn the specific features of their hardware firewall, how to enable them, and how to test the firewall to ensure it is doing a good job of protecting your network.
- Hardware firewalls include Cisco PIX, SonicWall, NetScreen, Watchguard, and Symantec's 5400 series appliances (which run their Enterprise Firewall software).

4. Software Firewall:

- For individual home users, the most popular firewall choice is a software firewall.
- Software firewalls are installed on your computer (like any software) and you can customize it; allowing you some control over its function and protection features.
- A software firewall will protect your computer from outside attempts to control or gain access your computer, and, depending on your choice of software firewall, it could also provide protection against the most common Trojan programs or e-mail worms.
- Many software firewalls have user defined controls for setting up safe file and printer sharing and to block unsafe applications from running on your system.
- Additionally, software firewalls may also incorporate privacy controls, web filtering and more.
- The downside to software firewalls is that they will only protect the computer they are installed on, not a network, so each computer will need to have a software firewall installed on it.

4. Software Firewall (continue…):

- Like hardware firewalls, there is a vast number of software firewalls to choose from.
- Because your software firewall will always be running on your computer, you should make note of the system resources it will require to run and any incompatibilities with your operating system.
- A good software firewall will run in the background on your system and use only a small amount of system resources.
- It is important to monitor a software firewall once installed and to download any updates available from the developer.
- Software firewalls include Microsoft ISA Server, CheckPoint FW-1, and Symantec Enterprise Firewall, as well as most personal firewalls.

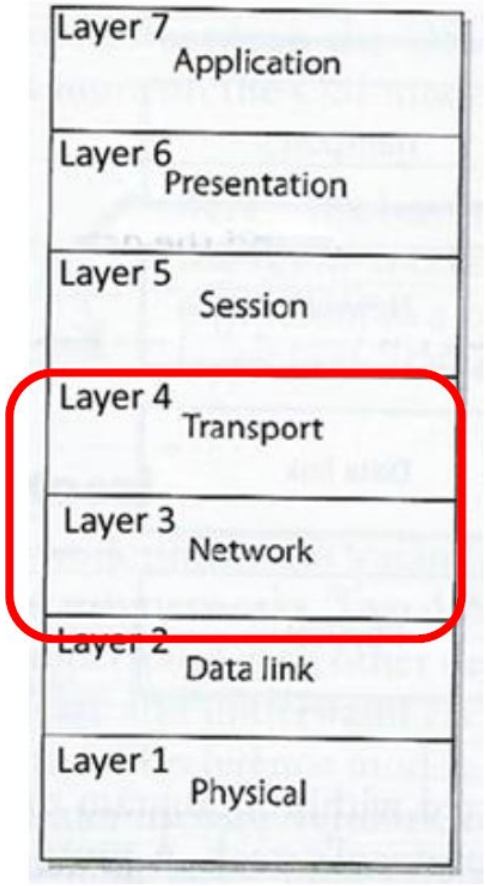
Firewall Techniques

- A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted.
- There are several types of firewall techniques listed below.
  - In practice, many firewalls use two or more of the techniques in concert for better security.

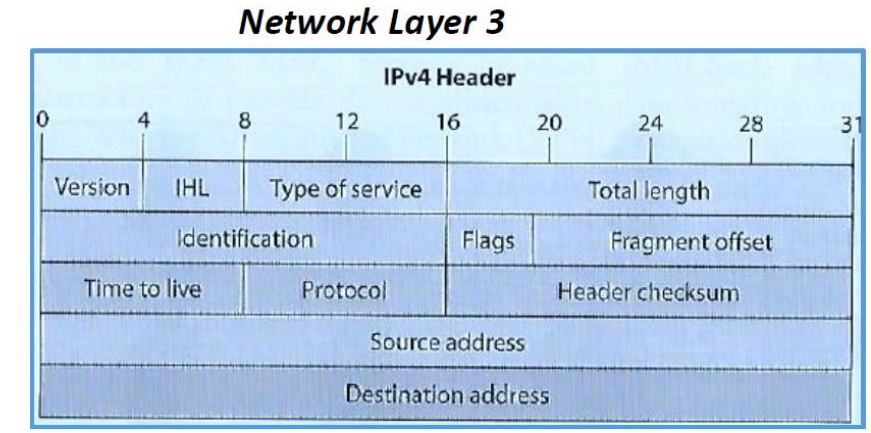
- A. Packet Filtering Firewall
- B. Stateful Inspection Firewall
- C. Proxy Firewall
- D. Next Generation Firewall

Packet Filtering Firewall

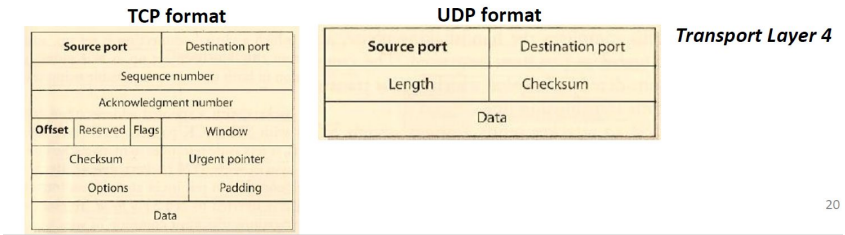
- "First-generation" firewall technology – most basic and primitive
- Capabilities built into most firewalls and routers
  - Configured with **access control lists (ACLs)** which dictate the type of traffic permitted into and out of the network
  - Filters compare protocol header information from network and transport layers with ACLs



Packeting Filtering Firewall (Cont..)



- **Compares ACLS with network protocol header values to determine permit/deny network access based on:**
- 1. Source and destination IP addresses
- 2. Source and destination port numbers
- 3. Protocol types
- 4. Inbound and outbound traffic direction

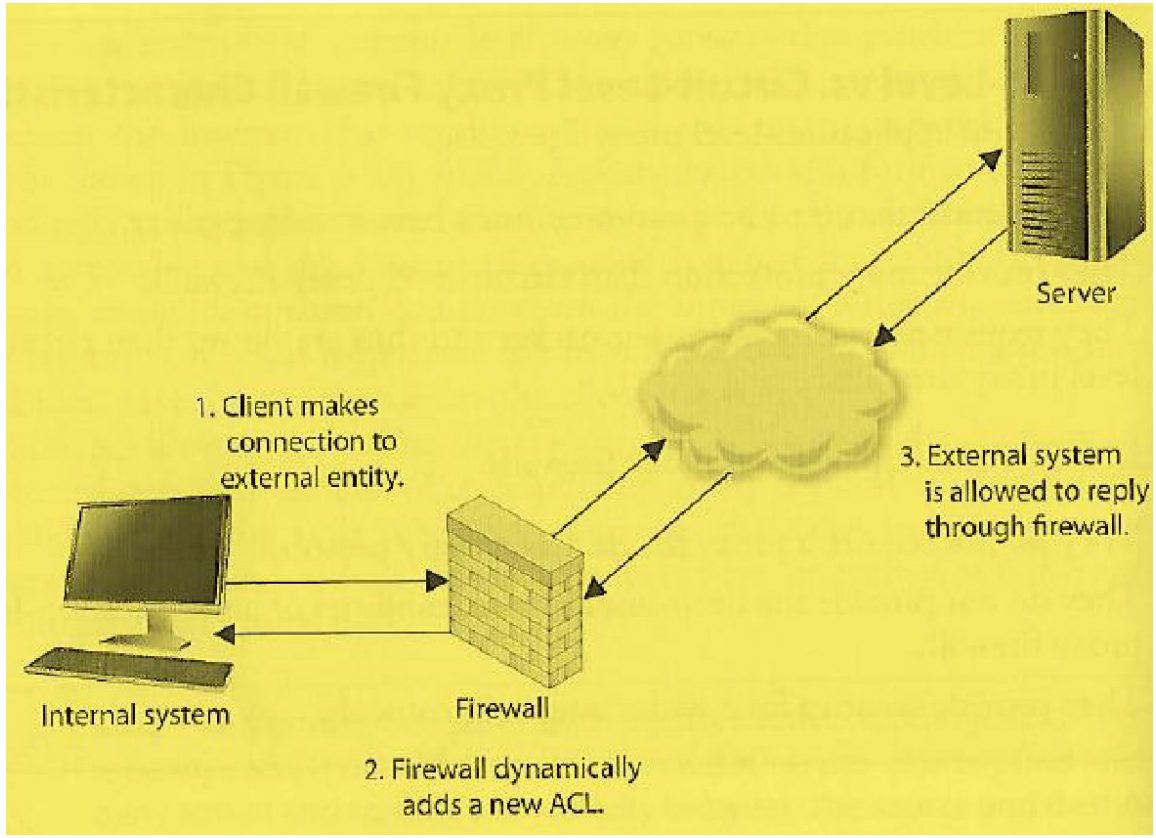


Packet Filtering Firewall (Cont..)

- Packet filtering firewalls: monitor traffic and provide “stateless inspection” of header attribute values (i.e. delivery information) of individual packets
  - …and after the decision to permit or deny access to the network is made the firewall *forgets* about the packets
- **Weakness:**
  - No knowledge of data moving between applications communicating across the network
  - Cannot protect against packet content, e.g. probes for specific software with vulnerabilities and exploit a buffer overflow for example
  - Should not be used to protect an organization’s infrastructure and information assets
- **Strengths:**
  - Useful at the edge of a network to quickly and efficiently strip out obvious “junk” traffic
  - High performance and highly scalable because they do not carry out extensive processing on the packets and are not application dependent
  - First line of defense to block all network traffic that is obviously malicious or unintended for a specific network
  - Typically complemented with more sophisticated firewalls able to identify non-obvious security risks

Dynamic Packet Filtering Firewall

- When an internal system needs to communicate with a computer outside its trusted network it needs to choose an identify its source port so the receiving system knows how/where to reply
- Ports up to 1023 are reserved for specific server-side services and are known as “well-known ports”
- Sending system must choose a randomly identified port higher than 1023 to use to setup a connection with another computer.
- The dynamic packet-filtering firewall creates an ACL that allows the external entity to communicate with the internal system via this high-numbered port.
- The ACLs are dynamic in nature – once the connection is finished the ACL is removed
- The dynamic packet-filtering firewall offers the benefit of allowing any type of traffic outbound and permitting only response traffic inbound

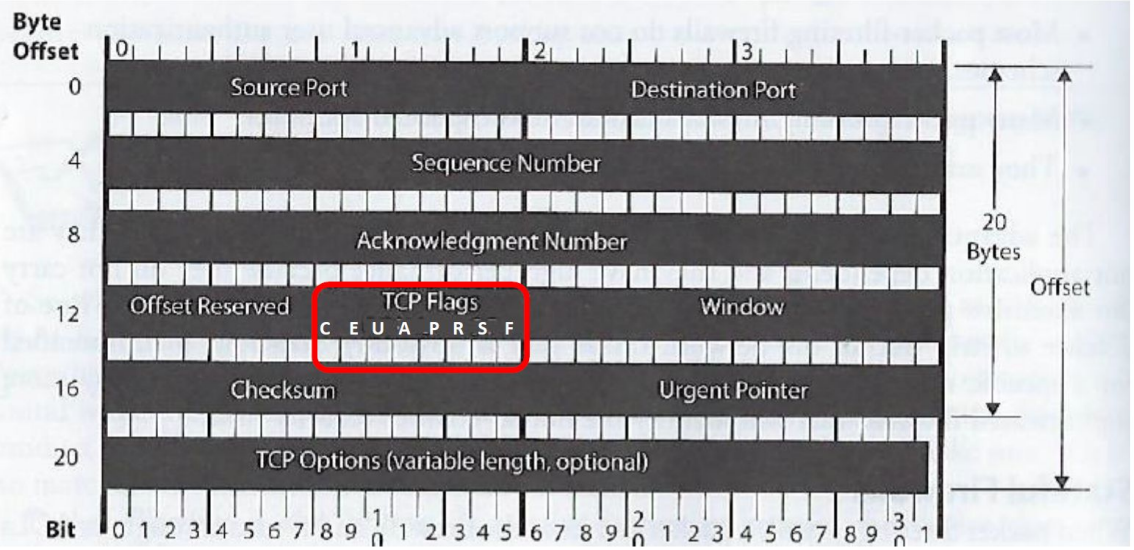


Stateful Inspection Firewall

- This type of firewall remembers and keeps track of what computers say to each other
  - Tracks where packets went until each particular connection between computers is closed
- The firewall uses a “state table” which it updates to track the contents of packets each computer sent to each other
  - Makes sure the sequential process of packet message interchange involved in connection-oriented protocols (e.g. TCP – transmission control protocol) are properly synchronized and formatted
  - *If not an attack is detected and blocked*

Stateful Inspection Example

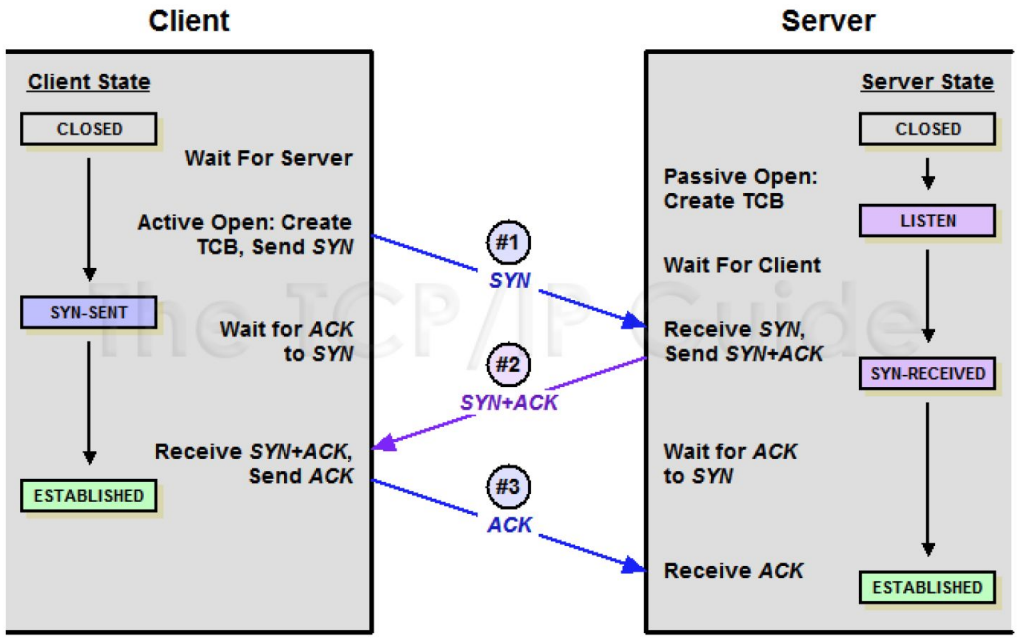
- Determine if all TCP Flags set to 1
  - Attackers send packets with all TCP flags set to 1 with hope that the firewall will not understand or check these values and forward them to the server
  - •Under no circumstances during legitimate TCP connections are all values turned to 1
  - If detected connection is blocked



TCP Flags
C E U A P R S F
Congestion Window
C 0x80 Reduced (CWR)
E 0x40 ECN Echo (ECE)
U 0x20 Urgent
A 0x10 Ack
P 0x08 Push
R 0x04 Reset
S 0x02 Syn
F 0x01 Fin

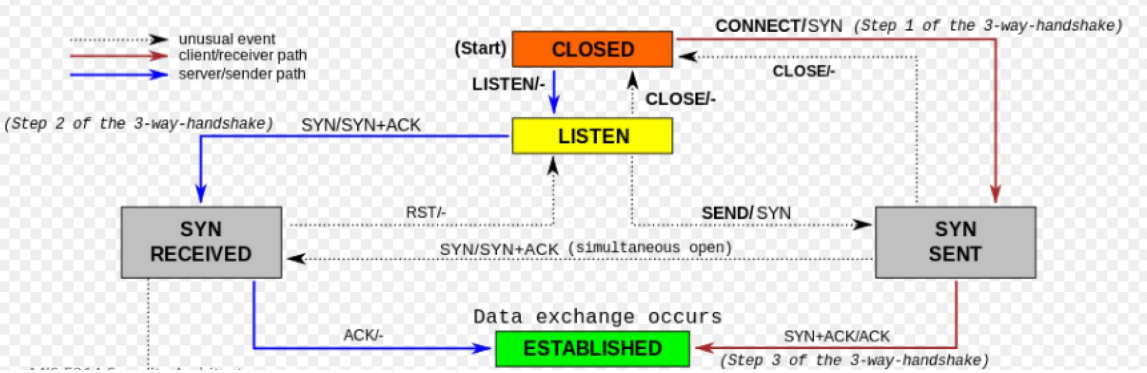
Stateful Inspection Example

- Stateful inspection firewall assures that TCP (connection-oriented protocol) proceeds through a series of states:
- *Stateful firewall keeps track of each of these states for each packet passing through, along with corresponding acknowledgement and sequence numbers.*
- *Out of order acknowledgement and/or sequence numbers can imply a **replay attack** is underway and the firewall will protect internal systems from this activity*



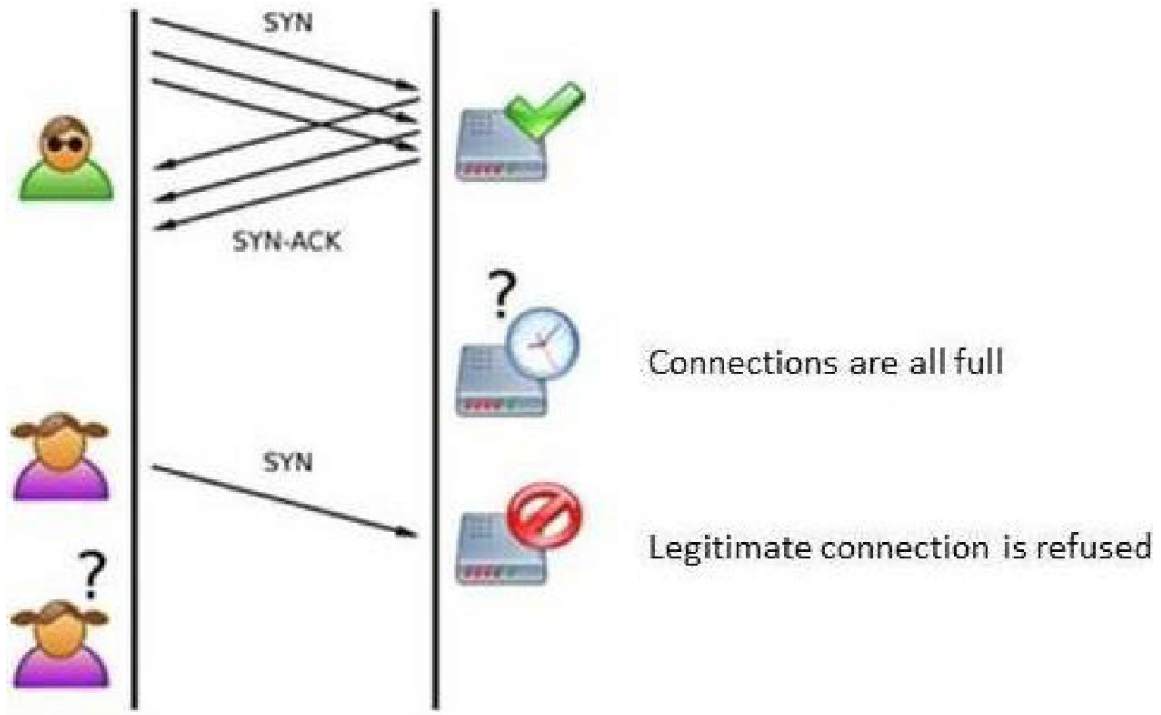
Stateful Inspection Example

- Stateful inspection firewall assures that TCP (connection-oriented protocol) proceeds through a series of states:
  1. LISTEN
  2. SYN-SENT
  3. SYN-RECEIVED
  4. ESTABLISHED
- *Stateful firewall keeps track of each of these states for each packet passing through, along with corresponding acknowledgement and sequence numbers.*
- *If a remote computer sends in a SYN/ACK packet without an internal computer first sending out a SYN packet, this is against protocol rules and the firewall will block the traffic*



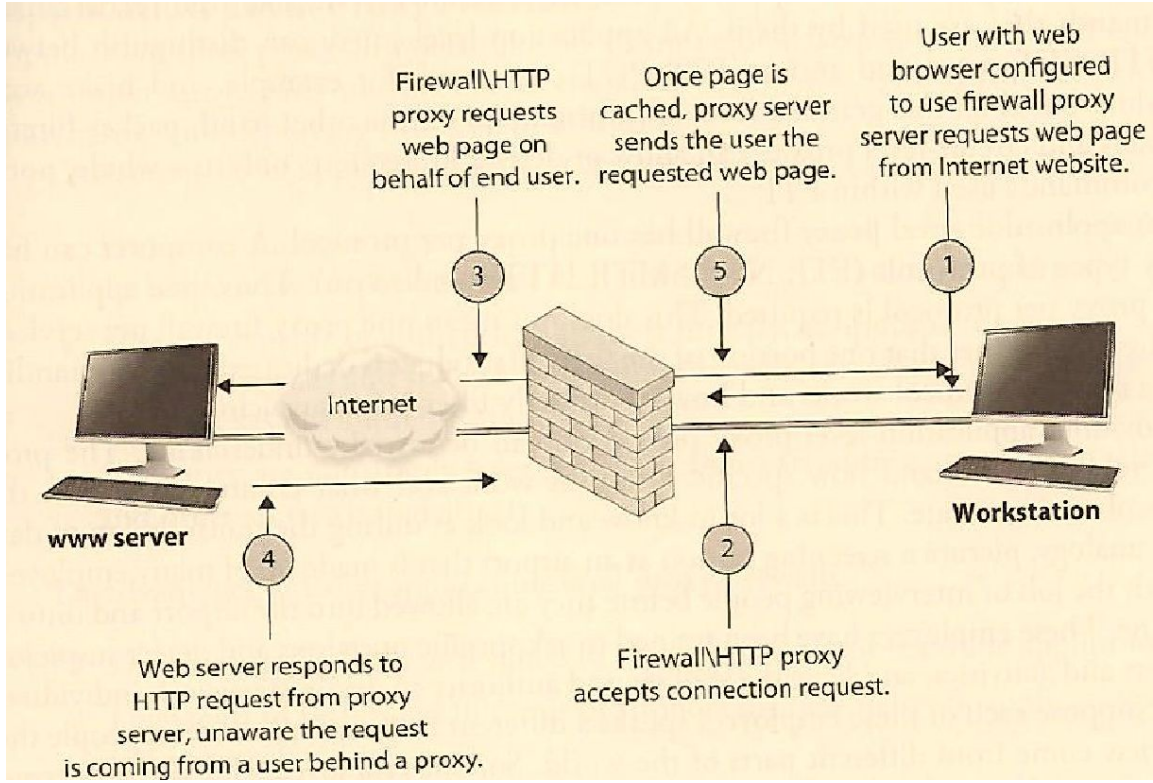
Stateful Inspection Firewall

- **Strength:**
  - Maintains a state table that tracks each and every communication session to validate the session
  - Provides high-degree of security, without introducing a huge performance hit
  - Is scalable and transparent to users
  - **Tracks both connection-oriented protocols (e.g. TCP) and connectionless protocols (UDP and ICMP)**
- **Weakness:**
  - Susceptible to Denial of Service (DoS) attacks aimed at flooding the state table with fake information
  - *Poorly designed stateful firewalls with state-tables filled with bogus information may freeze or reboot*



Proxy Firewall

- Proxy firewall is a “middleman” standing between a trusted and untrusted networks, denying end to end connectivity between source and destination computers
- Puts itself between the pair in both directions intercepting and inspecting each message before delivering it to the intended recipient.
- Applies ACL rules, and also…
  - *Ends the communication session, breaking the communication channel between source and destination, so there is no direct connection between two communicating computers*
  - *Inspects the traffic*
  - *When traffic is “approved” the proxy firewall starts a new session from itself to the receiving system*

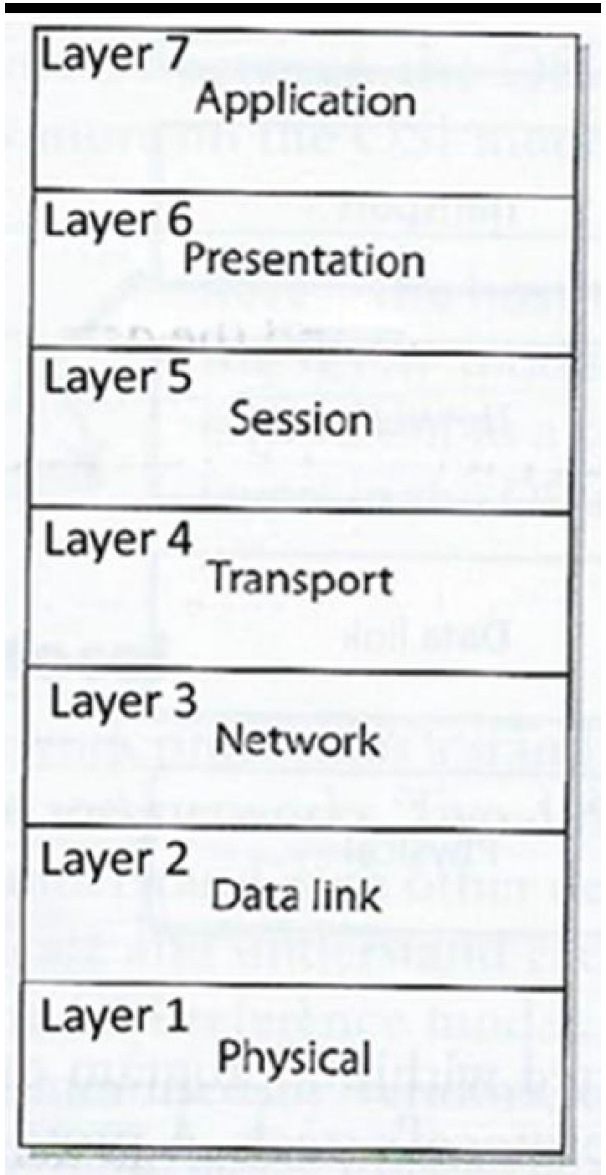


Proxy Firewall (Cont…)

- Two types of proxy firewall is found:
  - Application Level
  - Circuit Level

•**Application-level proxies** work up through Layer 7

- • Understand entire contents of packets, making decisions based on API services, protocols and commands (e.g. FTP PUT and GET commands)
  - A Proxy Firewall will have a series of application-level proxies to detect suspicious data transmission – one proxy per API protocol (i.e. one for FTP, and different ones for SMTP, HTTP, …)



Proxy Firewall (Cont..)

- **Circuit-level gateways (proxies)** work up through the session layer
  - Monitor TCP handshaking between packets to determine whether a requested session is legitimate
  - Information passed to a remote computer appears to have originated from the gateway – hiding information about the protected private network
  - Firewall traffic rules control traffic to/from acknowledged computers only
  - Relatively inexpensive
  - Do not filter content of individual packets like application-level proxies do
  - Only examines network addresses and ports – similar to packet filtering firewalls, but provides proxy services insulating the internal identities and addresses of machines from external devices

Proxy Firewall (cont..)

- Kernel Proxy Firewall is considered a “fifth generation” firewall
- If functions as a proxy – conducting network address translation so it function as a “middleman”
- Creates a dynamic, customized virtual network stacks for each packet that consists of only the protocol proxies needed to examine it
- The packet is evaluated at every layer of the stack simultaneously
    - Data link header
    - Network header
    - Transport header
    - Session layer information
    - Presentation layer information
    - Application layer data
- If anything is determined unsafe the packet is discarded
- Much faster than an application-level proxy because it is optimized to function at the lower level kernel level of the operating system

Next-Generation Firewall

- Combines the best capabilities of the other firewalls
  - Ensures traffic is well-behaved and in accordance with applicable protocols
  - Breaks direct connection between internal and external systems (proxy)
  - Provides dynamic port assignment
- Also includes a signature-based Intrusion Detection System (IPS) engine
  - Able to look for specific indicators of attack even in traffic is well behaved
- Able to use centralized data sources
  - Able to be updated with new attack signatures from cloud aggregators
  - For consistent up to date whitelists, blacklists and policies
  - Can connect to Active Directory to provide URL to IP address translations
- Tend to be expensive – cost of ownership beyond small and medium sized organizations

Summery

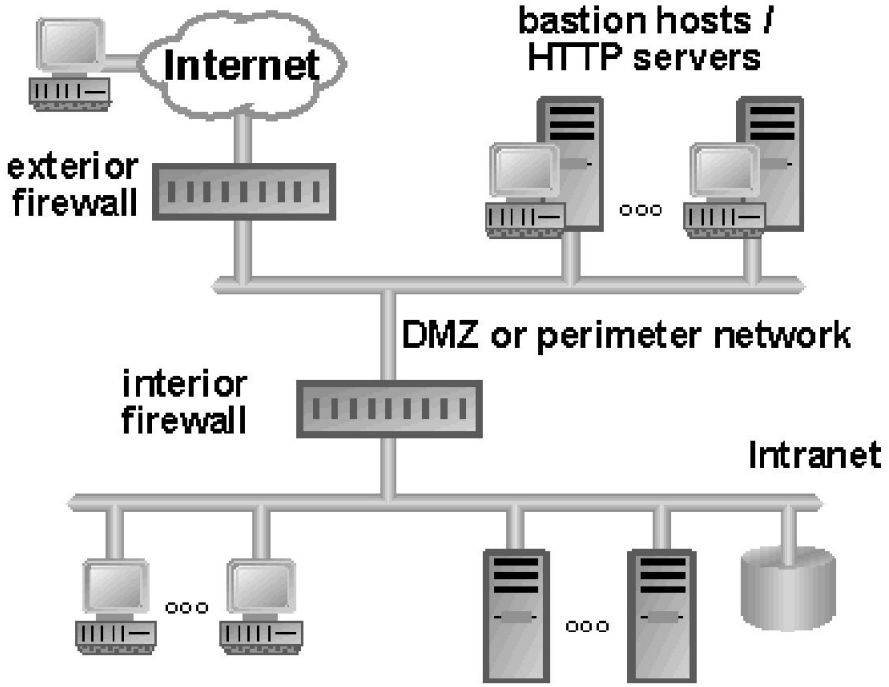
Firewall type	OSI Layer	Characteristics
Packet Filtering	Network Layer	Looks at destination and source addresses, ports, and services requested. Routers use ACLs monitor network traffic
Dynamic Packet Filtering	Network Layer	Allows any permitted type of traffic outbound and only response traffic inbound
Stateful	Network Layer	Looks at the state and context of packets. Keeps track of each conversation using state table
Circuit-level Proxy	Session Layer	Provides proxy services, but looks only at the header packet information (less detailed level of control that application-level proxy)
Application-level Proxy	Application Layer	Looks deep into packets and makes granular access control decisions, It requires one proxy per protocol
Kernal Proxy	Application Layer	Faster than application-level proxy because processing performed in operating system kernel. One network stack created for each packet
Next-generation	Multiple Layers	Very fast and supports high bandwidth. Built-in IPS, able to connect to external services like Active Directory

Some Firewall Architecture Patterns based on firewall placement

1. Bastion host
2. Dual-homed Firewall
3. Screened host
4. Screened Subnet

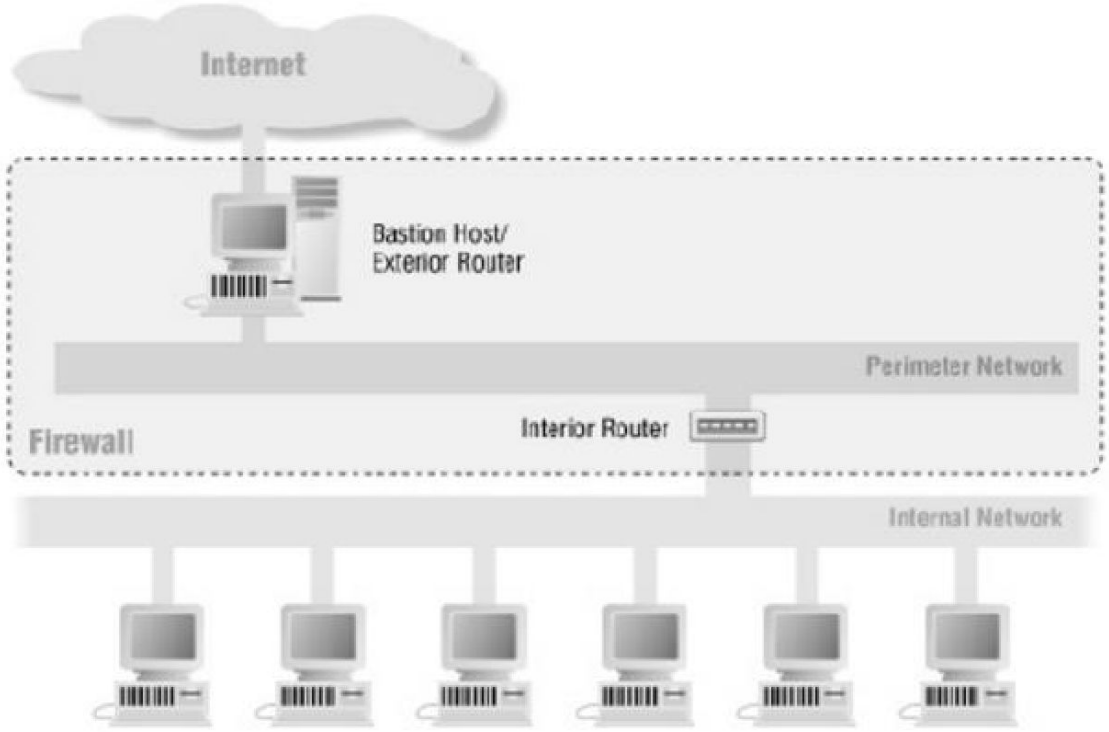
Bastion Firewall

- A **bastion firewall** refers to a specialized and highly secured system designed to act as a primary defense line between an external network (like the internet) and an internal network.
- It acts as a gateway for external users (e.g., remote workers, partners) to access internal resources securely.
- It implements strict policies for allowing or denying traffic based on predefined rules, such as IP addresses or ports.
- As the first point of contact, it is often the target of attacks, such as port scanning or denial-of-service (DoS).
- Its design ensures these attacks do not compromise the internal network.



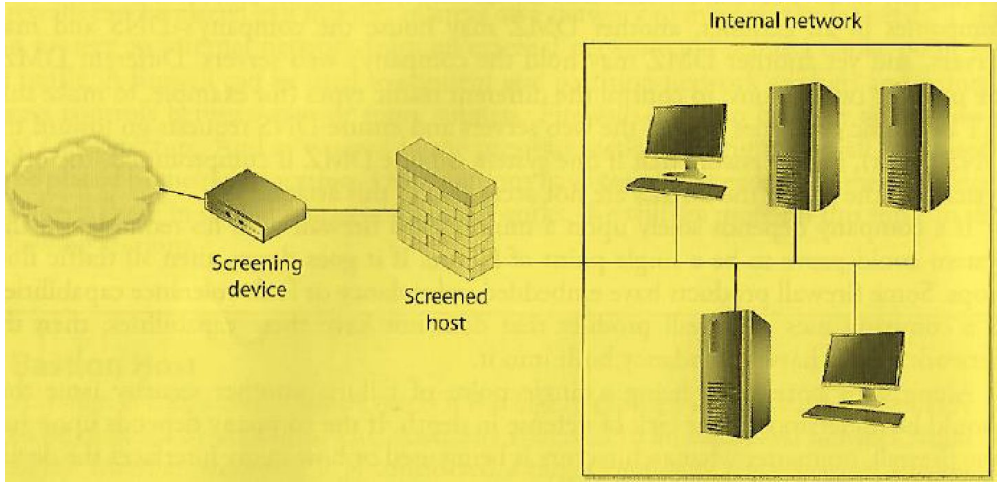
Dual-Homed Firewall Architecture

- A “dual-homed” device has two network interface cards (NICs)
  - Multi-homed devices have multiple NICs.
- Packet comes to the external NIC from an untrusted network and is forwarded up through the firewall software and if not dropped forwarded to the internal NIC.
- Without redundancy, if this goes down the dual-homed firewall becomes a single point of failure.
- One layer of protection lacks “defense in depth”
  - *If an attacker compromises one firewall they can gain direct access to the organizations network resources*



Screened Host Firewall Architecture

- This communicates directly with a perimeter router and the internal network
    1. Traffic from the Internet first passes through a packet filtering router applying ACL rules which filters out (i.e. drops) junk packets
    2. Traffic that makes it past this phase is sent to the screen-host firewall which applies more rules to the traffic and drops the denied packets
    3. Remaining traffic moves to the internal network

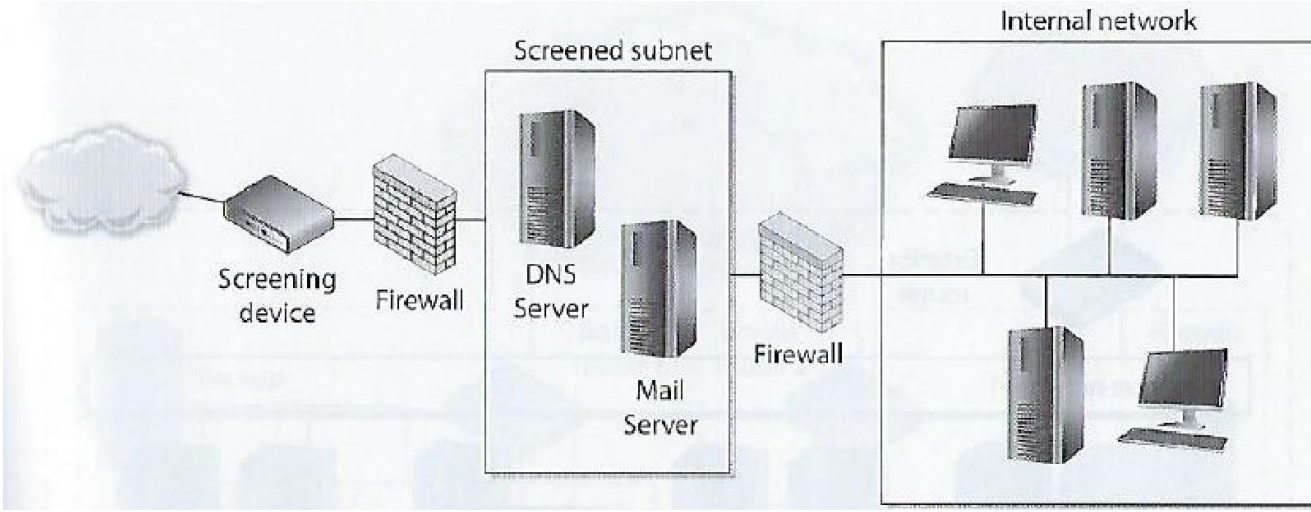


Router provides network-level packet filtering

- Security level is higher than a bastion dual-homed firewall because attacker would need to compromise 2 systems to succeed

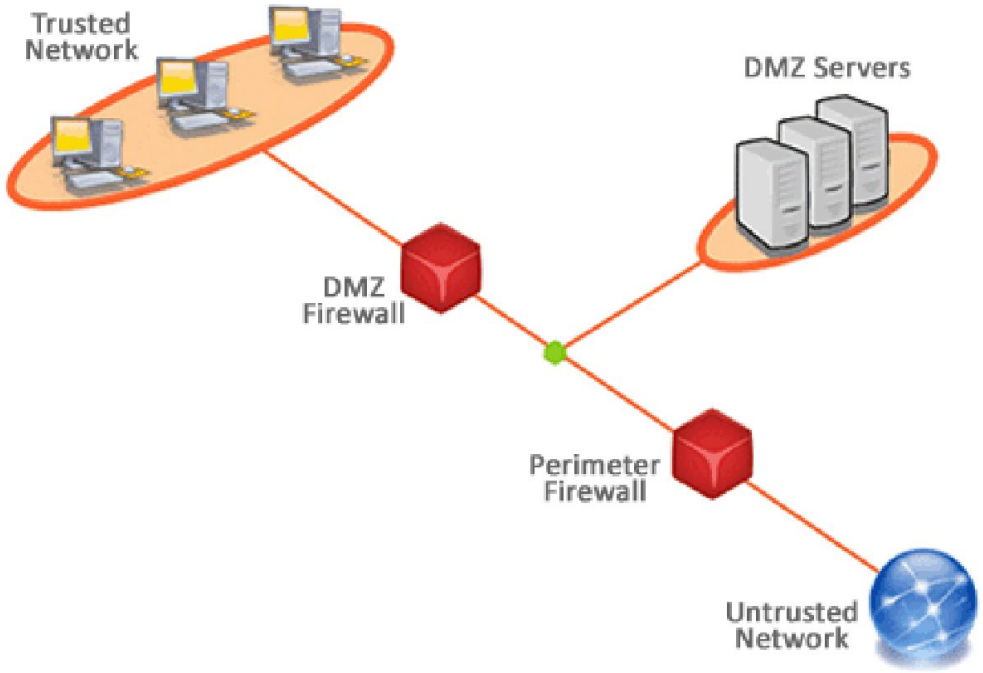
Screened Subnet Architecture

- Adds another layer of depth to the security of the screened-host architecture
- The external firewall screens traffic entering the screened sub-network, instead of firewall redirecting traffic to the internal network
- The second interior firewall also filters the traffic – this creates a screened subnet (i.e. DMZ)
- *Creates a DMZ between 2 firewalls which functions as a small network isolated between trusted internal and untrusted external network*
- 3-devices working together provides more protection than a stand-alone firewall or a screened-host firewall.
- All 3 need to be compromised by an attacker to gain access to the internal network



Demilitarized Zone (DMZ)

- Firewalls are installed to construct DMZ areas which is Network segments that are located between protected and unprotected networks.
- DMZ area provides a buffer zone between the dangerous Internet and valuable assets the organization seeks to protect
- Usually 2 firewalls are installed to form a DMZ
  - May contain mail, file, and DNS (Domain Name System)
  - Servers.
  - Usually contain an Intrusion Detection System sensor which listens for suspicious and malicious behavior
  - Servers in DMZ must be hardened to serve as the first line of protection against attacks coming from the internet



How DMZ Works

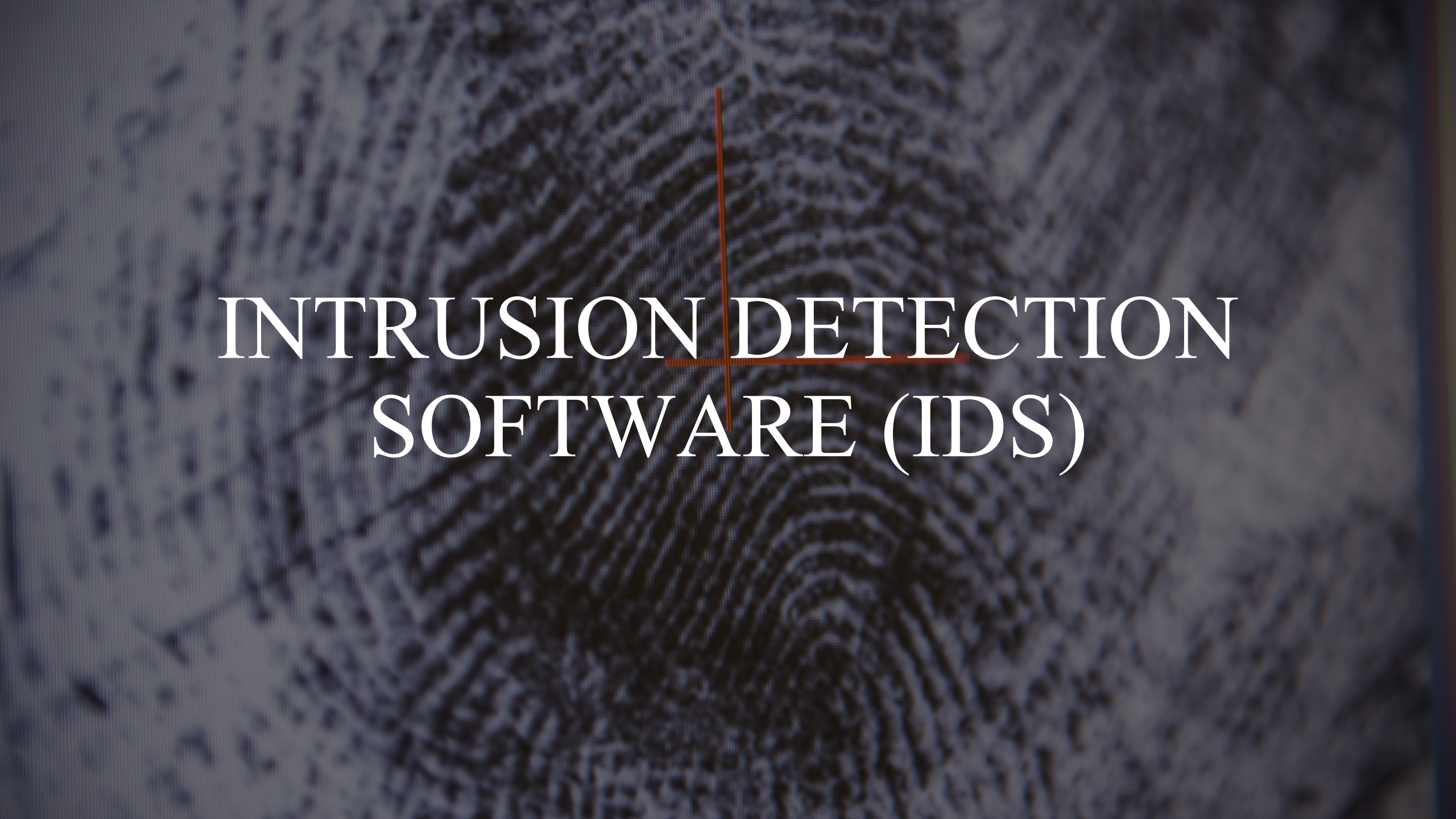
- Incoming requests from the internet (e.g., accessing a website) are directed to servers within the DMZ.
- The external firewall blocks unauthorized traffic while allowing legitimate traffic to reach the DMZ servers.
- If DMZ services (e.g., a web server) need to interact with internal network resources (e.g., a database server), strict rules are applied to control and monitor the connection through the internal firewall.
- Servers in the DMZ are isolated from the internal network. Any compromise within the DMZ does not immediately impact sensitive internal systems.
- Intrusion detection systems (IDS) and logging tools monitor DMZ activity for potential threats.

Firewall Rules

- Good firewall behavior: ***default action is to deny*** any packets explicitly not allowed
  - If no rule in the ACL explicitly implies on an incoming packet can come in, it is dropped
  - Any packet coming in from the Internet containing the source address of an internal host should be dropped
  - Spoofing or masquerading attack reflected in a modified packet header having the source address of a host inside the target network
  - No packet should be permitted to leave that does not contain a source address of an internal host – this is how DDoS zombies work
  - Many companies deny packets with source routing information in the headers which may circumnavigate internal routers and firewalls.
- Firewalls ***not effective "out of the box"***
  - Need to understand internal default rules which may negate user provided rules
  - Can create bottlenecks
  - Need to effectively distribute them throughout the network to control network access points and provide appropriate "defense in depth"
  - Do not protect against malware, complex attack types, sniffers, rogue access points

Common Firewall Rules

- **Stealth rule:**
  - Disallow unauthorized systems from accessing to firewall software
- **Silent rule**
  - Identify and drop “noisy” traffic without logging it to reduce log sizes by not responding to unimportant packets
- **Cleanup rule**
  - A **firewall cleanup rule** is a specific rule, typically configured at the bottom of a firewall's rule set, to handle any network traffic that doesn't explicitly match any of the preceding rules. Its primary purpose is to ensure that all unhandled traffic is dealt with appropriately, either by being explicitly **denied** or **logged and reviewed**.
- **Negate rule**
  - A **firewall negate rule** is a type of rule that uses a **negative condition** to filter traffic. Instead of specifying what traffic to allow or deny directly, a negate rule defines what traffic should **not** match a specific condition.
  - A rule might say, *"Allow all traffic except traffic from IP range X."*


INTRUSION DETECTION
SOFTWARE (IDS)

Introduction

- While firewalls and antivirus are preventive controls, IDSs are access control monitoring devices designed to

  1. Detect a security breach

  2. Aid in mitigating damage caused by hackers breaking into sensitive computer and network systems

- IDS' components

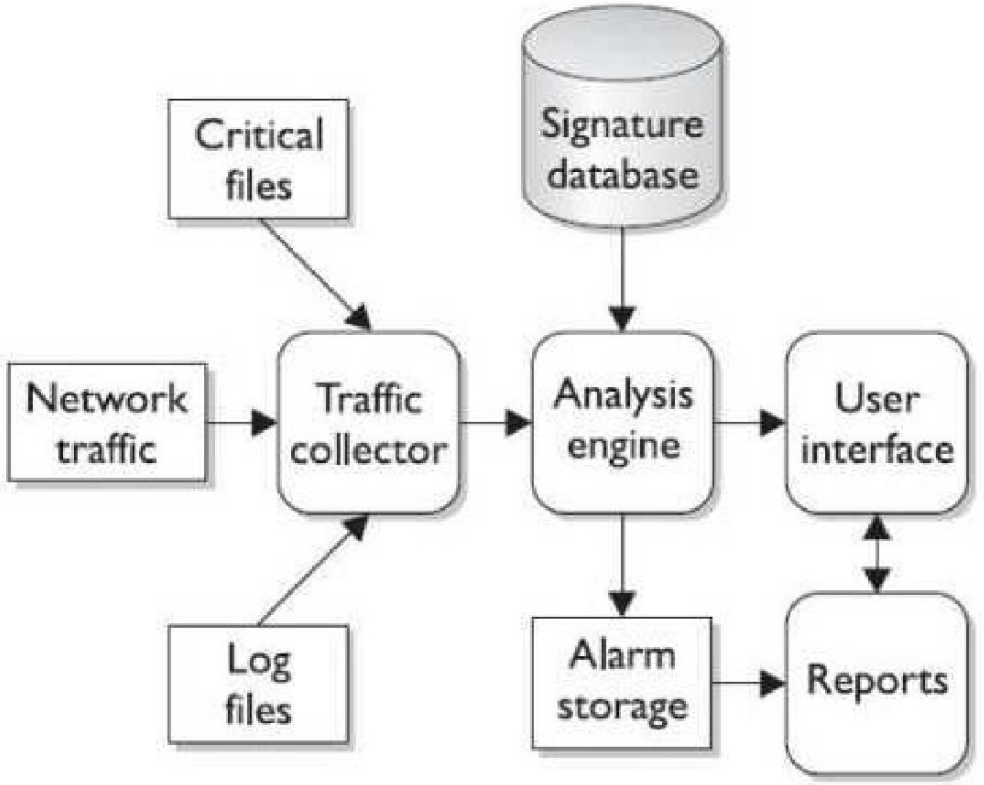
  1. Sensors

  • Collect and send traffic and user activity data to analyzers

  2. Analyzers

  • Look for suspicious activity and if found sends alert to administrator's interface

  3. Administrative interfaces



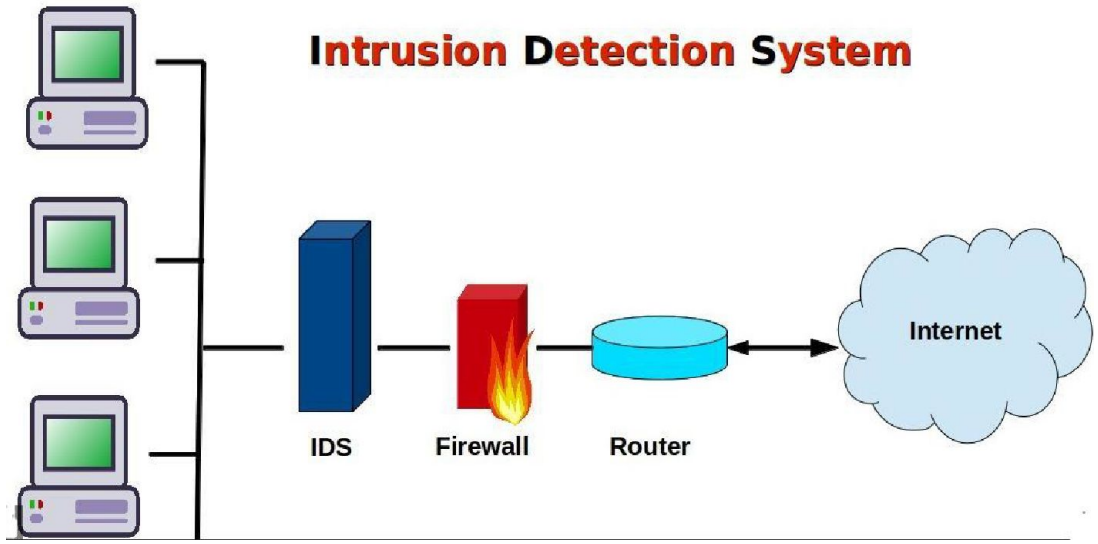
Intrusion Detection Software (Cont..)

Two main types of IDS:

1. Host-based for analyzing activity within a particular computer system.

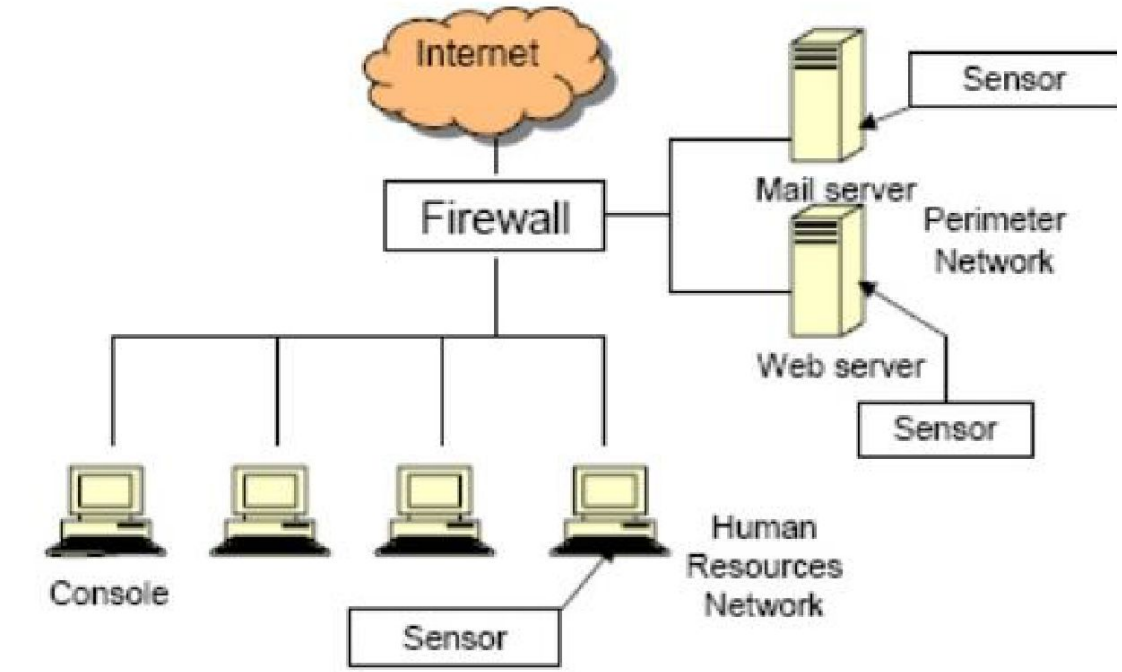
2. Network-based for monitoring network communications.

- IDS can be configured to:
  - Watch for attacks
  - Parse audit logs
  - Terminate a connection
  - Alert administrator as attacks happen
  - Expose a hacker and her/his techniques
  - Illustrate which vulnerabilities need to be addressed

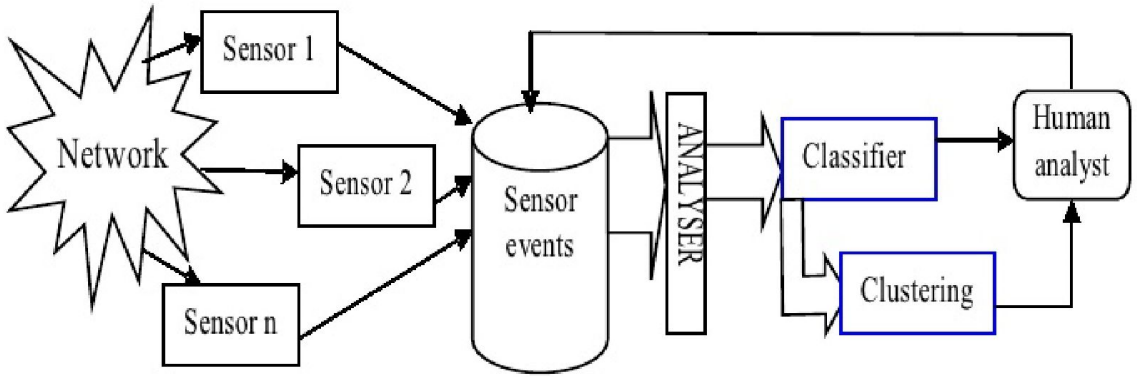


Intrusion Detection Software (Cont..)

- **Host-based IDS (HIDS)**
  - Can be installed to look at the data packets within the higher levels of the OSI stack for anomalous or inappropriate activity on individual servers and/or workstations
  - Usually installed on critical servers (too much administrative overhead to put them everywhere)
  - Make sure users do not put the system at risk by activities such as deleting system files or reconfiguring important settings
  - Does deeper inspection of the packets
  - Does not understand network traffic



- A **Network-Based Intrusion Detection System (NIDS)** is a security solution that monitors and analyzes network traffic to detect unauthorized access, malicious activities, or policy violations.
- By examining network packets, a NIDS identifies potential threats in real time and alerts administrators to take corrective actions.



Key features of NIDS

- **Network Monitoring**:
  - Operates at strategic points in the network, such as behind firewalls or at the boundaries of sensitive systems.
  - Captures and inspects all network traffic passing through its sensors.
- **Threat Detection**:
  - Uses signature-based detection, anomaly detection, or a combination of both to identify malicious behavior:
    - **Signature-Based Detection**: Matches traffic against known attack patterns (e.g., malware signatures).
    - **Anomaly-Based Detection**: Identifies deviations from normal network behavior, potentially indicating new or unknown attacks.
- **Real-Time Alerts**:
  - Notifies security teams about suspicious activity as it happens, enabling timely responses.
- **Passive Operation**:
  - Unlike firewalls, NIDS typically does not block traffic directly. It acts as a monitoring tool and relies on administrators to take action.

How NIDS Works

Placement:

- NIDS sensors are deployed at critical points in the network, such as:
  - At the gateway between the internal network and the internet.
  - Within sensitive network segments.
- These sensors analyze mirrored traffic using techniques like port mirroring or network taps.

Packet Analysis:

- Captures packets and examines headers, payloads, and protocols.
- Matches packet content against threat databases or uses behavioral models to detect anomalies.

Alert Generation:

- When suspicious activity is detected, the NIDS generates alerts and logs details for further analysis.

Types of IDS

- NIDS and HIDS can be one of the following types:

1. Signature-based:

  - Pattern matching, similar to antivirus software
  - Signatures must be continuously updated
  - Cannot identify new attacks

- 2 types
  - Pattern matching: Compares individual packets to signatures
  - Stateful matching: Compares patterns among packets

Types of IDS (Cont..)

2. Anomaly-based (a.k.a. Heuristic-based or Behavior-based):

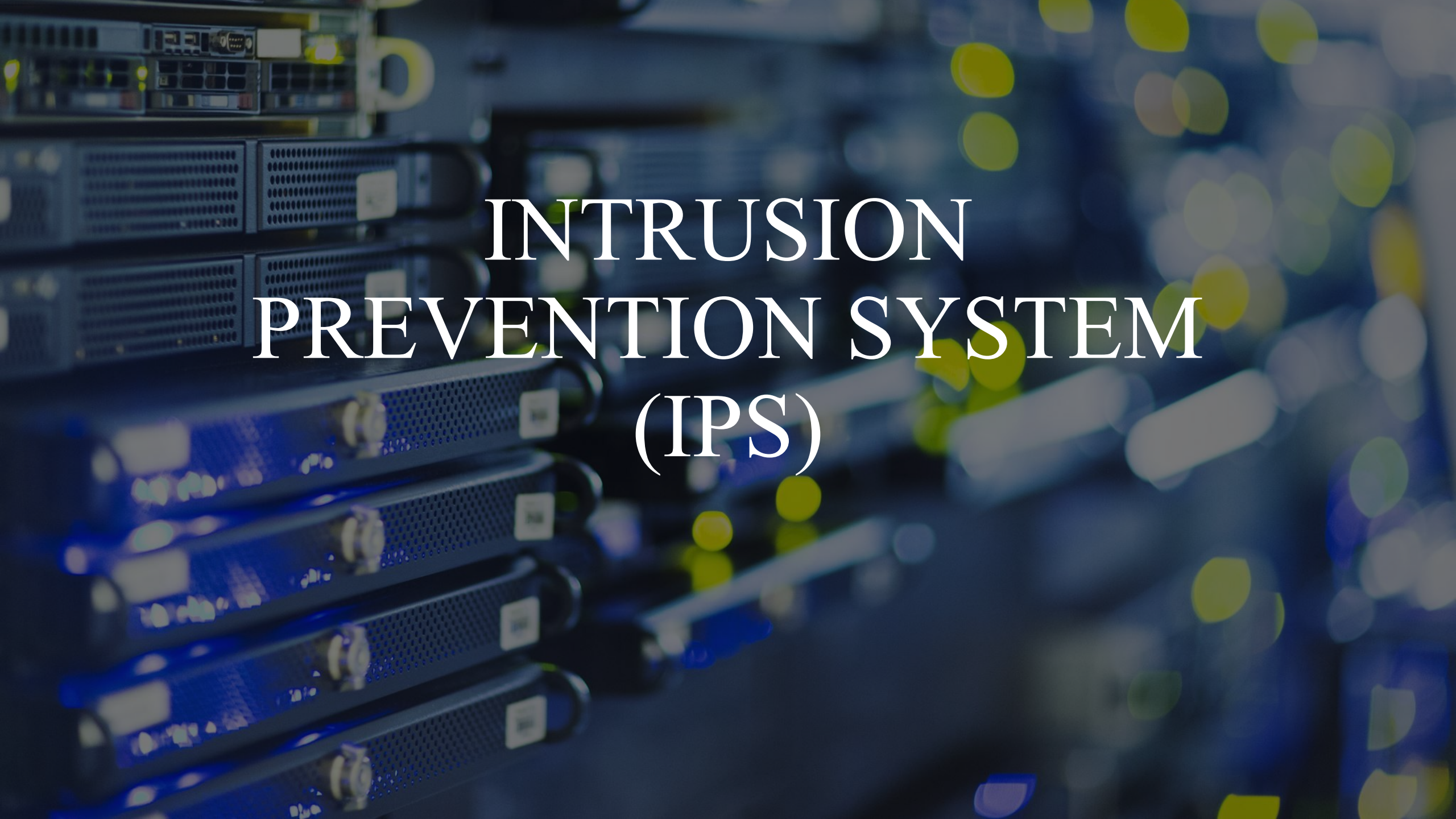
- Behavioral-based system able to learn from “normal activities”
- Can detect new attacks

- 3 Types:
  - Statistical anomaly-based – creates a normal profile used to compare sensed activities
  - Protocol anomaly-based – Identifies incorrect uses that violate protocols (e.g. TCP 3-way handshake)
  - Traffic anomaly-based – Identifies unusual activity in network traffic

Types of IDS (Cont..)

3. Rule-based

- Uses artificial intelligence expert systems that process rules in the form of “If *situation* then *action*” statements to identify combinations of activities within the data of the packets
- *e.g. “IF a root user creates FileA AND FileB IN same directory and there is a call to Administrative ToolK THEN trigger alert”*
- Cannot detect new attacks
- The more complex the rules, the greater the need for processing power to support the software and hardware requirements so the IDS
- does not become a bottleneck and performance problem



INTRUSION PREVENTION SYSTEM (IPS)

- IPS – Detect something bad may be taking place and block traffic from gaining access to target
- *Preventive and proactive response*
- *IPS can be host-based or network-based (like IDS)*
- *Can be content-based (looking deep into packets), conduct protocol analysis or be signature matching*
- *Also can use rate-based metrics to identify suspicious increases in volumes of traffic*
    - *E.g. DoS – flood attack*
    - *Traffic flow anomalies – "slow and low" stealth attack attempting to be undetected*

IDS vs IPS

- Possible responses to a triggered event:
- Disconnect communications and block transmission of traffic
- Block a user from accessing a resource
- Send alerts of an event trigger to other hosts, IDS monitors and administrators