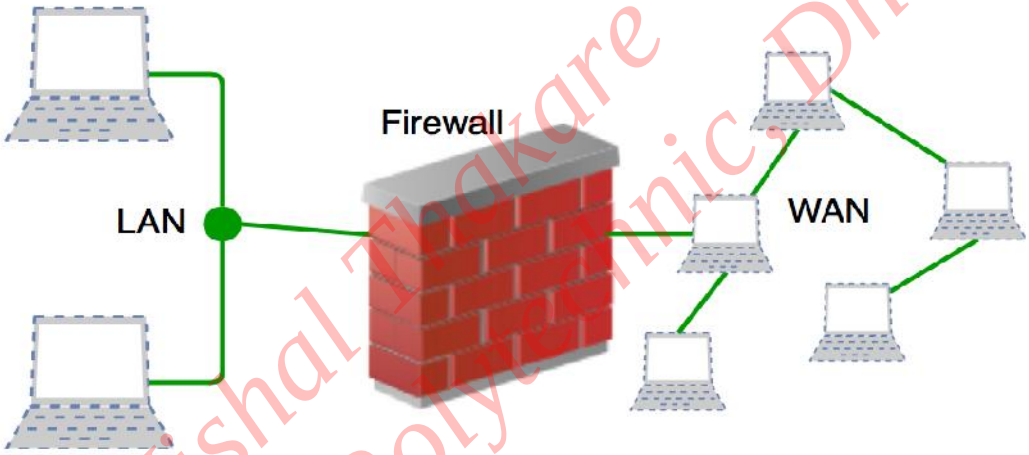
Unit 4 – Firewall and Intrusion Detection System

18 Marks

Firewall and its Need

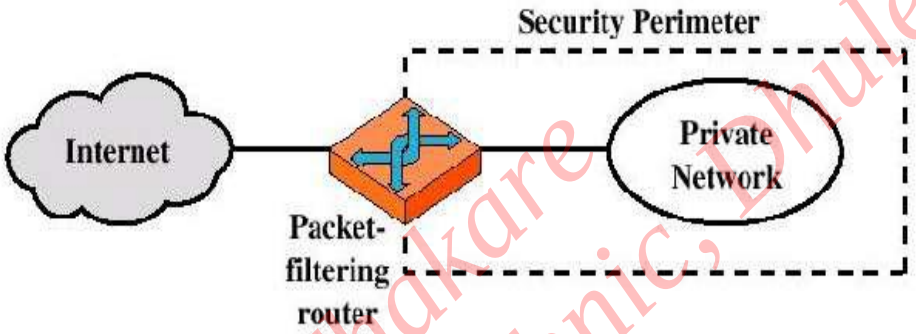


1. A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules.
2. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.
3. Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks.
4. Fig shows the simple firewall between LAN and internet.
5. Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices.
6. Its main purpose is to filter traffic and lower the risk of unauthorized access.
7. It blocks the unwanted contents from the internet that harms to the computer.
8. Firewalls can either be software or hardware.
9. A software firewall is a program installed on each computer and regulates traffic through port numbers and applications.
10. while a physical firewall is a piece of equipment installed between your network and gateway.
11. Firewall logs the suspicious events and alert the administrator about attempts.

Types of firewall

- **Packet Filters**
- **Stateful packet filter**
- **Application level gateways.**
- **Circuit level gateways**.

1) Packet Filter Firewall



1. A packet filtering firewall is the most basic type of firewall.
2. It works at the junction points where devices such as routers work.
3. It monitors network traffic and filters incoming packets based on configured security rules.
4. The firewall performs a simple check of the data packets coming through the router—inspecting information such as the destination and origination IP address, packet type, port number, and other surface-level information without opening up the packet to inspect its contents.
5. If the information packet doesn't pass the inspection, it is dropped.
6. These firewalls are designed to block network traffic based on protocols, an IP address, and a port number if a data packet does not match the established rule-set.
7. It is also called as screening router or screening filter.

Advantages:

1. Its main advantage is its simplicity, one screening router can help to protect the network.
2. It does not require user knowledge or co-operation.
3. Fast in their operating speed.
4. Don't use up a lot of resources.
5. Low cost.

Disadvantages:

1. Some protocols are not well suited for packet filtering.
2. Can be difficult to set up rules.
3. Incapable of filtering at application layer.
4. Can be break by IP address spoofing.
5. No user authentication.

2) Stateful Packet Filter

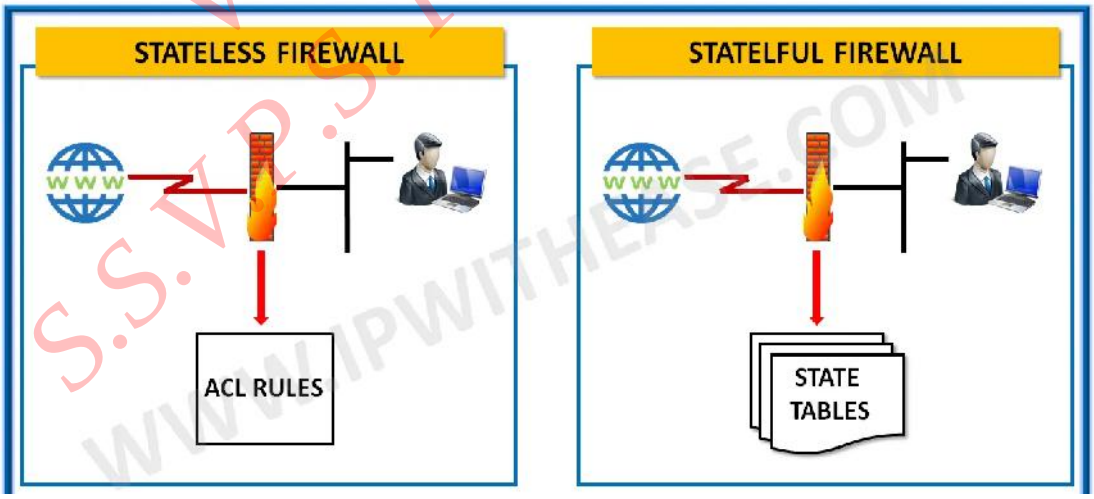
1. A simple packet filter firewall is stateless.
2. It operates on packets on an individual basis and does not store or apply state information.
3. Stateful firewall is also known as 'Dynamic Packet Filters'.
4. It keeps track of the state of active connections and uses this information to decide which packets to allow through it.
5. Stateful Packet Filter
6. That is, it adapts itself to the current exchange of information, unlike the normal packet filters.
7. It keeps track of the state of networks connection travelling across it, such as TCP streams.
8. So the filtering decisions would not only be based on defined rules, but also on packet's history in the state table.

Advantages:

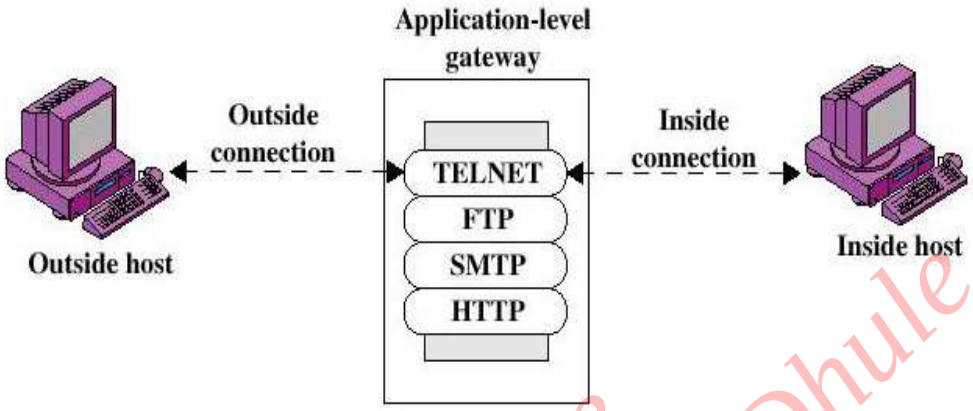
1. The connection table reduces the chance of IP address spoofing.
2. It inspects the packets dynamically.
3. Keep track of the entire session.
4. Inspect headers and packet payloads.

Disadvantages:

1. It does not set up a separate connection on behalf of source.
2. Not as cost-effective as they require more resources.
3. No authentication support.
4. May slow down performance due to high resource requirements.



3) Application Level Gateways



1. They are also called as Proxy firewalls
2. They operate at the application layer as an intermediate device to filter incoming traffic between two end systems That is why these firewalls are called **'Application-level Gateways'**.
3. Unlike basic firewalls, these firewalls transfer requests from clients pretending to be original clients on the web-server.
4. This protects the client's identity and other suspicious information, keeping the network safe from potential attacks.
5. Once the connection is established, the proxy firewall inspects data packets coming from the source.
6. If the contents of the incoming data packet are protected, the proxy firewall transfers it to the client.
7. This approach creates an additional layer of security between the client and many different sources on the network.
8. It works as follows:
   - ❖ **Step-1:** User contacts the application gateway using a TCP/IP application such as HTTP.
   - ❖ **Step-2:** The application gateway asks about the remote host with which the user wants to establish a connection. It also asks for the user id and password that is required to access the services of the application gateway.
   - ❖ **Step-3:** After verifying the authenticity of the user, the application gateway accesses the remote host on behalf of the user to deliver the packets.

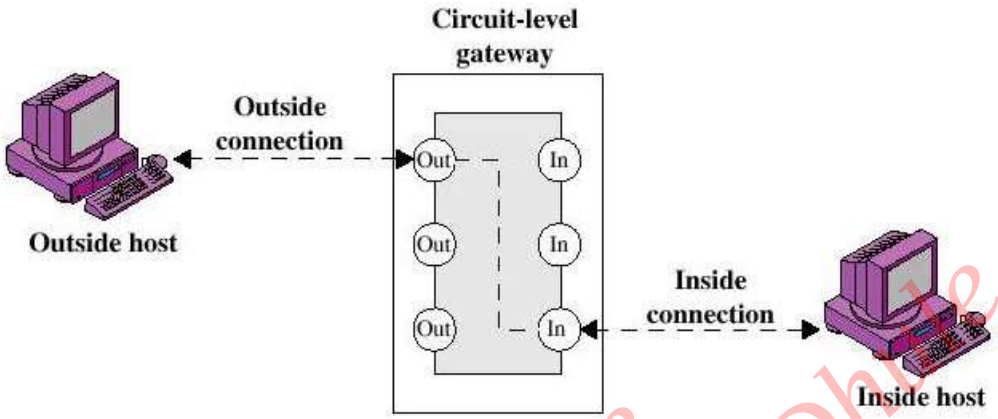
Advantages:

1. They are more secure than packet filter firewalls.
2. Do not allow direct communication between devices.
3. Easy to log and audit all incoming traffic.

Disadvantages:

1. Additional overload on each connection.
2. Require more processing power.

4) Circuit level gateways



1. It works at the **session layer** of the OSI Model.
2. It is the advanced variation of *Application Gateway*.
3. It acts as a virtual connection between the remote host and the internal users by creating a new connection between itself and the remote host.
4. It also changes the source IP address in the packet and puts its own address at the place of source IP address of the packet from end users.
5. This way, the IP addresses of the internal users are hidden and secured from the outside world.
6. It validates the TCP and UDP sessions before allowing a connection through firewall.
7. Once the session has been established, any application can run across that connection, this creates the problem

Advantages:

1. Relatively inexpensive.
2. More efficient traffic processing than application level gateways.

Disadvantages:

1. Protects circuits rather than individual packets.
2. Incapable of content filtering.
3. Once session is validated any application can run across the connection.

Firewall Policies

1. A firewall determines what packet should be accepted, denied or dropped based on its policy.
2. Permissive policies allow all traffic but block certain dangerous services like telnet or SNMP or Port numbers known to be used by an attack.
3. Restrictive policies block all traffic and allow only traffic known to meet a useful purpose such as HTTP, POP3,SMTP and SSH.
4. This is more secure option.
5. A policy is usually represented as an ACL with positive and negative entries.

6. Firewall Policies
7. A typical firewall ruleset could look like:
    - Allow from internal network to internet : HTTP, FTP, SSH, DNS.
    - Allow from anywhere to mail server: SMTP only.
    - Allow from inside to mail server: SMTP, POP3.
    - Allow from mail server to internet: SMTP, DNS.
    - Allow reply packets.
    - Block everything else.

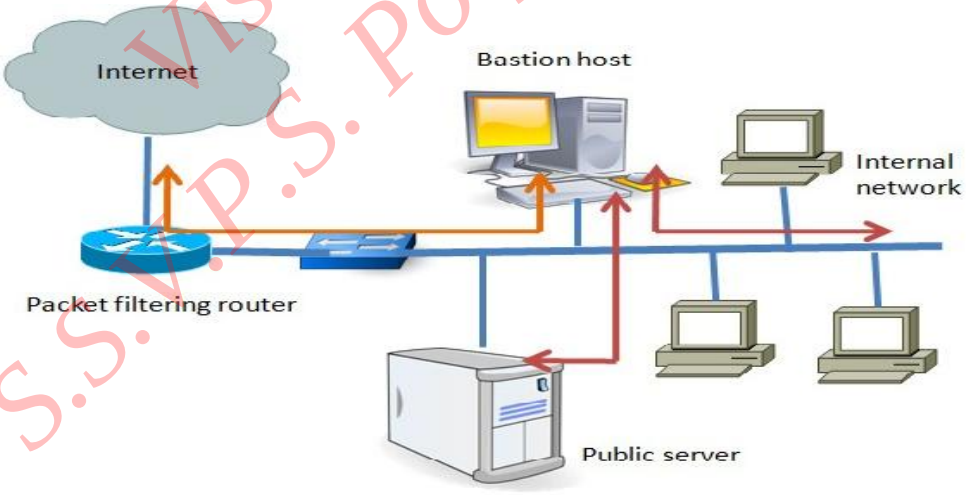
Firewall Configuration

1. Firewall configuration is combination of packet filters and application or circuit gateways.
2. Based on this there are three configurations of firewall.
    1) Screened host firewall, Single homed bastion.
    2) Screened host firewall, Dual homed bastion.
    3) Screened Subnet firewall.

Firewall Configuration/implementations
Bastion host:

1. it is a system identified by the *firewall* administrator as a critical strong point in the network security.
2. It acts as platform for application level or circuit level gateways.

1) Screened Host Firewall Single homed bastion



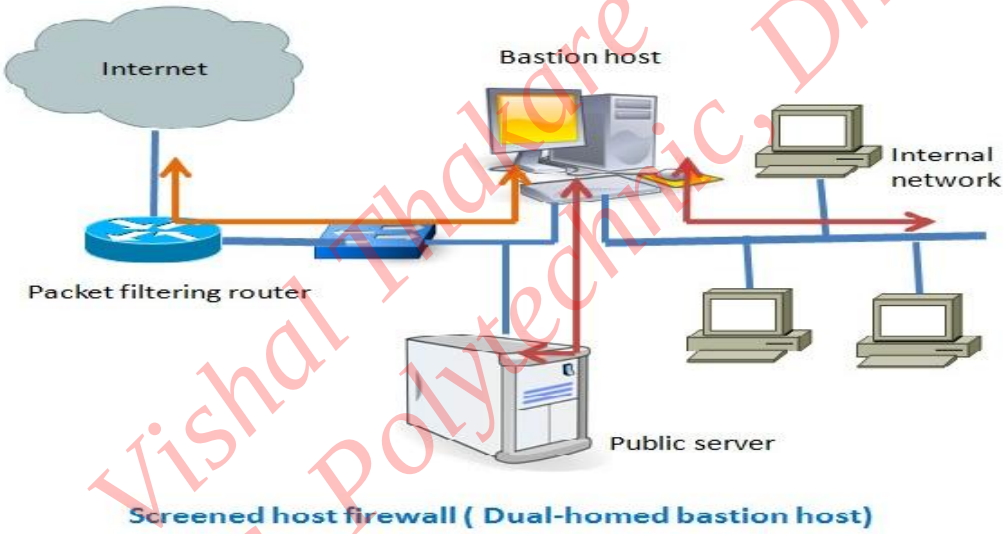
Screened host firewall (single-homed bastion host)

1. In case of single homed bastion host the firewall system consists of a packet filtering router and a bastion host.
2. A bastion host is basically a single computer with high security configuration, which has the following characteristics:

- Traffic from the Internet can only reach the bastion host; they cannot reach the internal network.
- Traffic having the IP address of the bastion host can only go to the Internet. No traffic from the internal network can go to the Internet.

3. This type of configuration can have a web server placed in between the router and the bastion host in order to allow the public to access the server from the Internet.
4. The main problem with the single homed bastion host is that if the packet filter router gets compromised then the entire network will be compromised.
5. To eliminate this drawback we can use the **dual homed bastion host** firewall system.

2) Screened Host Firewall Dual homed bastion



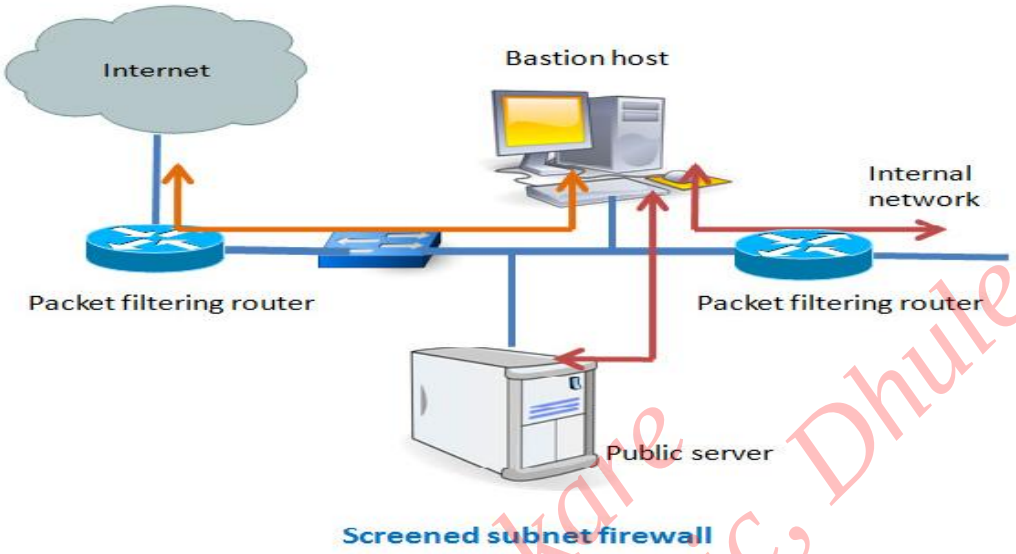
Screened host firewall (Dual-homed bastion host)

3) To eliminate this drawback of single homed bastion, we can use the **dual homed bastion host** firewall system.
4) In this the direct connection between the internal host and the packet filter are avoided.
5) In this configuration a bastion host has two network cards- one is used for internal connection and the second one is used for connection with the packet filter router.
6) In this case, even if, the router got compromised, the internal network will remain unaffected since it is in the separate network zone.

3) Screened Subnet Firewall

1) This is one of the most secured firewall configurations.
2) In this configuration, two packet filtering routers are used and the bastion host is positioned in between the two routers.
3) In a typical case, both the Internet and the internal users have access to the screened subnet, but the traffic flow between the two subnets (one is from bastion host to the internal network and the other is the sub-network between the two routers) is blocked.
4) It provides three layer of defense.

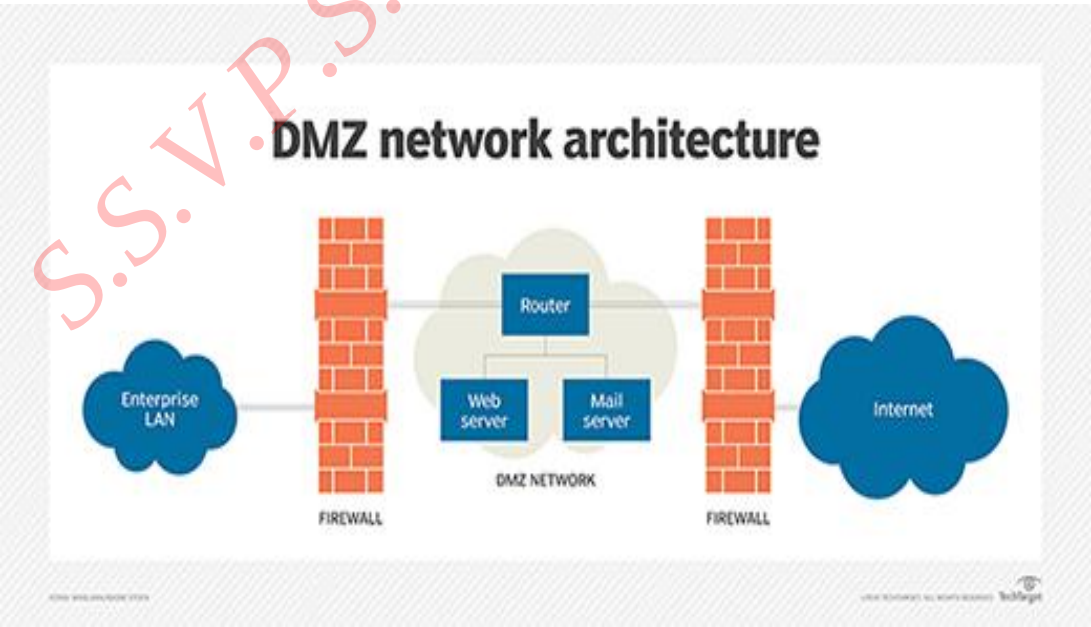
5) Internal network is invisible to the internet.



Limitations of Firewall

1. Firewall cannot protect from malicious insiders.
2. It cannot stop social engineering attacks.
3. It cannot stop attack if traffic bypass through them.
4. A firewall cannot protect from completely new threats.
5. Firewall cannot protect network if the administrator has not correctly set it up.
6. They are only as effective as the rules they are configured to enforce.

DMZ (Demilitarized Zone)

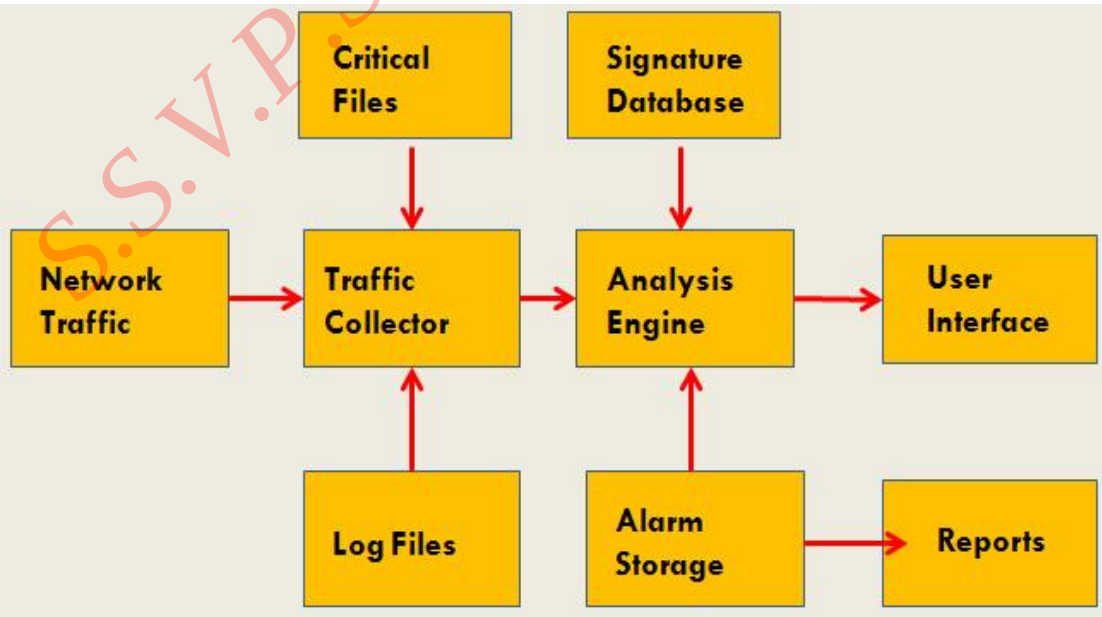


1. In computer networks, a DMZ (demilitarized zone), also sometimes known as a *perimeter network* or a *screened subnetwork*.
2. It is a portion of network that sits between the internal local area network (LAN) and internet.
3. It prevents outside users from getting direct access to a server that has companies data.
4. External-facing servers, resources and services are located in the DMZ.
5. Therefore, they are accessible from the internet, but the rest of the internal LAN remains unreachable.
6. This provides an additional layer of security to the LAN as it restricts a hacker's ability to directly access internal servers and data through the internet.
7. Users of public network outside company can only access the DMZ host.
8. As internal network is not directly connected to DMZ, so if attacker hacked DMZ then internal private network remains protected.

Intrusion Detection System (IDS)

1. An **Intrusion Detection System (IDS)** is a system that monitors the events occurring on a computer system or network and detects the unwanted manipulation or accessing the data by intruders.
2. The main purpose of IDS is to identify suspicious or malicious activity
3. It issues alerts to the system or an administrator when such activity is discovered.
4. It is a software application that scans a network or a system for harmful activity or policy breaching.
5. IDS are mainly divided into two categories depending on monitoring activity.
   - Host based IDS (HIDS)
   - Network Based IDS (NIDS)

Components of Intrusion Detection System (IDS)



1) **Traffic collector:**
   - This component collects activity or event for the IDS to examine.
   - On the HIDS this could be log file, audit logs or traffic coming or leaving a specific system.
   - On NIDS it is a mechanism for copying traffic from the network connection or link.

2) **Analysis Engine:**
   - This component checks the collected network traffic and compares it to known pattern or format stored in signature database.
   - It checks for unauthorized or malicious activity.

3) **Signature Database:**
   - It is the collection of pattern and definitions of known suspicious or malicious activity.

4) **User interface and reports:**
   - This component provides the interface to the user to operate and interact with IDS.
   - It provides alerts to the administrator and provides reports.

A) Host Based IDS (HIDS)

1. Host intrusion detection systems (HIDS) run on independent hosts or devices on the network.
2. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected.
3. HIDS operate in real time mode that looks for activity as it occurs or it can operate in batch mode that looks for activity on a periodic basis.
4. It takes a snapshot of existing system files and compares it with the previous snapshot.
5. Host Based IDS (HIDS)
6. If the analytical system files were edited or deleted, an alert is sent to the administrator.
7. Some host based IDS have ability to cover a specific application by checking logs produced by that application or traffic generated by that application eg: FTP, Web servers.
8. Many HIDS focus on log files produced by local operating systems.
9. HIDS checks the following activities in log file.
   - **Logins at odd hours.**
   - **Login authentication failures.**
   - **Adding new user account.**
   - **Modification or access to system files**
   - **Starting or stopping process.**
   - **Privilege modification**
   - **Use of certain programs.**

Advantages:

- They can be OS specific and have more detailed signature.
- They can check data after it has been decrypted.

- They can be application specific.
- It monitors system activities.

Disadvantages:

- The IDS must have a process or application on every host that is to monitor.
- They can have high cost of purchase and maintain.
- It uses the local system resources.
- It can be disabled by logging on host.

B) Network Based IDS (NIDS)

1. Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network.
2. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks.
3. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator.
4. Network Based IDS (NIDS)
5. It analyze the traffic according to the protocol, type, amount, source, destination, content, etc.
6. The NIDS are designed to monitor the traffic in and out of the organization.
7. An example of an NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying crack the firewall.
8. Network Based IDS (NIDS)
9. The NIDS looks for activities like:
    - **Denial of service attacks.**
    - **Port scans.**
    - **Malicious content in the data packet.**
    - **Trojans, viruses, or worms.**
    - **Brute force attacks.**

Advantages:

- It takes less systems to monitor entire network.
- Maintenance, purchase, and upgrade cost are lower.
- It checks all network traffic and detect attacks.
- Real time detection and quick response.

Disadvantages:

- It has no visibility of what is occurring on individual system.
- It is ineffective when traffic is encrypted.
- High cost of ownership and maintenance.

Vulnerability assessment

1. It checks the security state of the network.
2. Information about open ports, software packages running, network topology, etc. is collected and a prioritized list of vulnerabilities is compiled.
3. Vulnerability assessment products are also known as scanners.

4. They scan the system to determine the weakness in system.
5. There are two categories of vulnerability assessment.
    - **Network vulnerability scanner**
    - **Host vulnerability scanner.**

Network Vulnerability Scanner

1. It operates remotely by examining the network interface on a remote system.
2. It will look for vulnerable services running on that remote machine and report.
3. for example it is well known that rexd is a weak service , a network vulnerability scanner will attempt to connect to the rexd service on the target system.
4. If the connection succeeds, the scanner will report a rexd vulnerability.
5. Since it can be run from a single machine on a network, it can be installed without affecting the other machines.

Host Vulnerability Scanner

1. These scanners are different from network vulnerability scanner in that it is confined entirely to the local operating system.
2. These are the software packages that are installed on particular operating system.
3. Once the software is installed it can be configured to run at any time that is scheduled to run.
4. They do not consume network bandwidth when they run.

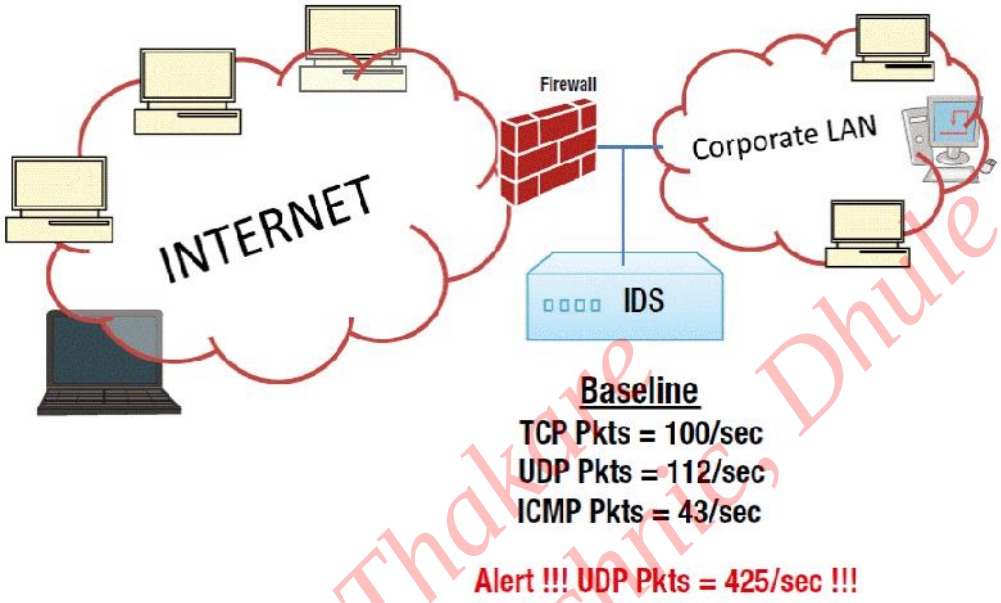
Misuse Detection

1. It looks for attack signatures.
2. Attack signatures are patterns of network traffic or activities in log files that include suspicious behavior.
3. It is widely used because many attacks have clear and distinct signatures.
4. Example signatures might include the number of recent failed login attempts on a sensitive host, certain types of TCP SYN packets, etc.
5. This system analyzes the system or network environment and compare the activity against pattern of known intrusive computer and network behavior.
6. This pattern must be updated over time to include the latest attack patterns similar to antivirus application.
7. The administrator can write their own pattern or signatures according to organizations security policy.
8. This system needs continuous updation to stay ahead of hackers.

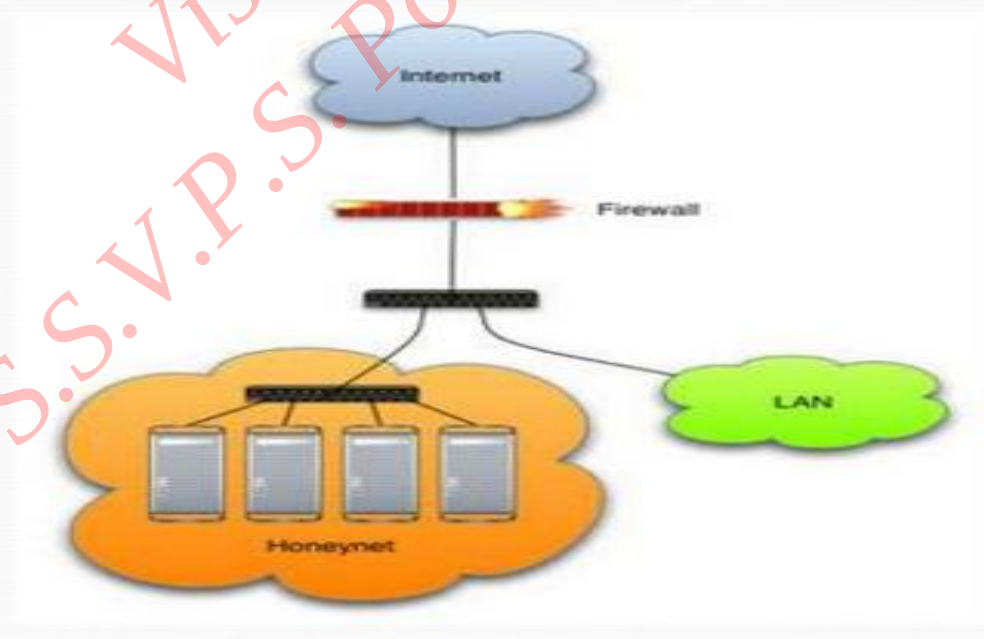
Anomaly Based detection

1. It is also called as behavior-based detection that uses statistical techniques to detect intrusion.
2. In this the normal period of evaluation establishes a performance baseline.
3. Once the baseline is established, this system periodically samples network activity and, using statistical methods, compares the sampled network activity to this baseline.
4. When the measured activity is outside the baseline parameters—exceeding what is called the clipping level
5. Then it sends an alert to the administrator.

6. The baseline data can include variables such as host memory or CPU usage, network packet types, and packet quantities.
7. The advantage of the statistical anomaly-based approach is that the it can detect new types of attacks, since it looks for abnormal activity of any type.



Honeypots



1. A honeypot is a security mechanism that creates a virtual trap to attract attackers.
2. An intentionally compromised computer system allows attackers to exploit vulnerabilities so that we can study them to improve our security policies.

3. We can apply a honeypot to any computing resource from software and networks to file servers and routers.
4. Honeypots are a type of deception technology that allows us to understand attacker behavior patterns.
5. Security teams can use honeypots to investigate cybersecurity breaches to collect information on how cybercriminals operate.
6. They divert the attention of attacker from real network.
7. A group of honeypot is called honeynet.
8. They capture the new viruses for future study.