UNIT - 3

NETWORK SECURITY

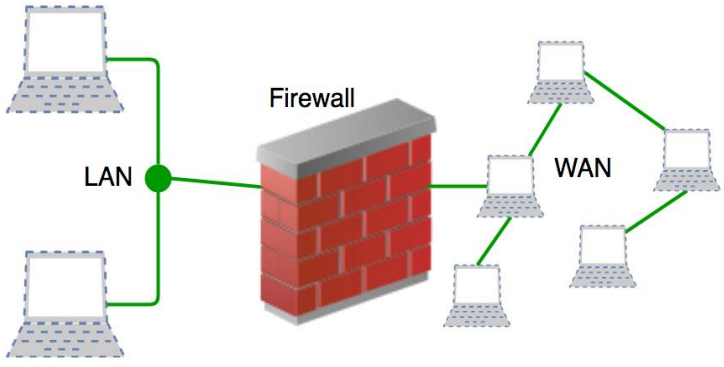
3.1 WORKING PRINCIPLE OF FIREWALLS

3.1.1 Introduction to Firewall

- A Firewall is a hardware or software to prevent a private computer or a network of computers from unauthorized access, it acts as a filter to avoid unauthorized users from accessing private computers and networks. It is a vital component of network security.
- It is the first line of defence for network security.
- A firewall has a set of rules which are applied to each packet.
- The rules decide if a packet can pass, or whether it is discarded.
- It filters network packets and stops malware from entering the user's computer or network by blocking access and preventing the user from being infected.
- A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.
- A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.

• Different kinds of Firewalls:

- Packet filtering / Network Layer
- Circuit switching firewall
- Application-gateway firewalls



3.1.2 Characteristics of Firewall

1) **Physical Barrier:** A firewall does not allow any external traffic to enter a system or a network without its allowance. A firewall creates a choke point for all the external data trying to enter the system or network and hence can easily block access if needed.

2) **Multi-Purpose:** A firewall has many functions other than security purposes. It configures domain names and Internet Protocol (IP) addresses. It also acts as a network address translator. It can act as a meter for internet usage.
3) **Flexible Security Policies:** Different local systems or networks need different security policies. A firewall can be modified according to the requirement of the user by changing its security policies.
4) **Security Platform:** It provides a platform from which any alert to the issue related to security or fixing issues can be accessed. All the queries related to security can be kept under check from one place in a system or network.
5) **Access Handler:** Determines which traffic needs to flow first according to priority or can change for a particular network or system. Specific action requests may be initiated and allowed to flow through the firewall.

3.1.2 Types of Firewalls

1. Packet Filtering Firewall:

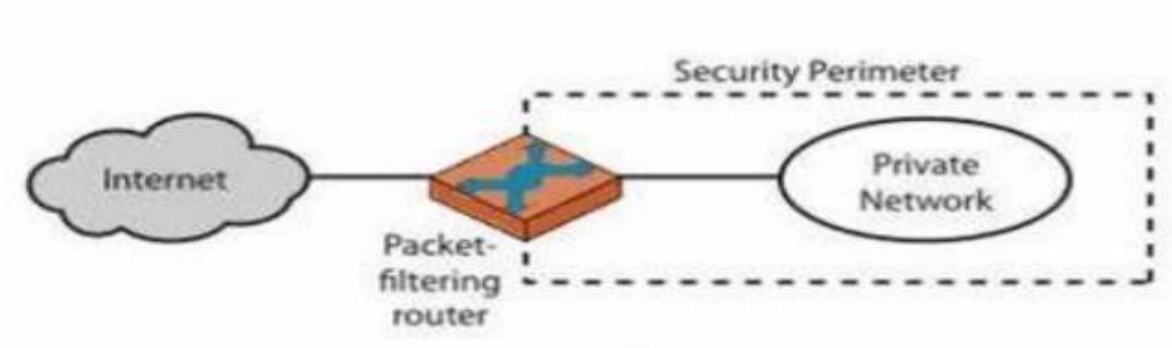
• A packet filtering firewall is the most basic type of firewall.

• It acts like a management program that monitors network traffic and filters incoming packets based on configured security rules.

• These firewalls are designed to block network traffic IP protocols, an IP address, and a port number if a data packet does not match the established rule-set.

• While packet-filtering firewalls can be considered a fast solution without many resource requirements, they also have some limitations.

• Because these types of firewalls do not prevent web-based attacks, they are not the safest.



2. Circuit Switching Firewall:

• Circuit-level gateways are another simplified type of firewall that can be easily configured to allow or block traffic without consuming significant computing resources.

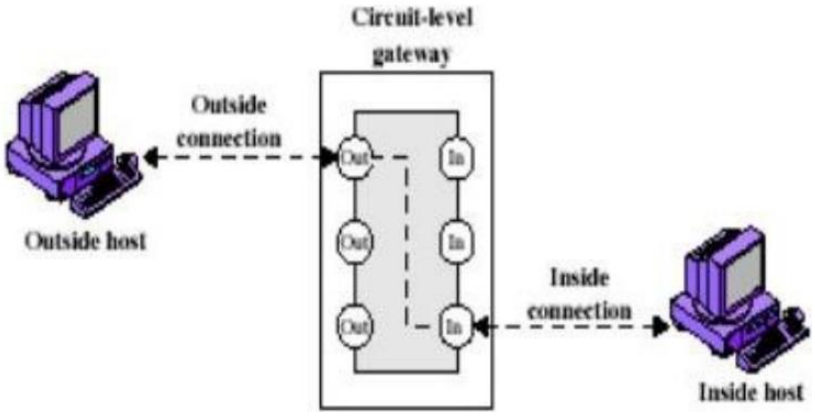
• These types of firewalls typically operate at the session-level of the OSI model by verifying connections and sessions.

• Circuit-level gateways are designed to ensure that the established sessions are protected.

• Like packet-filtering firewalls, these firewalls do not check for actual data, although they inspect information about transactions.

• Therefore, if a data contains malware, but follows the TCP connection, it will pass through the gateway.

• That is why circuit-level gateways are not considered safe enough to protect our systems.



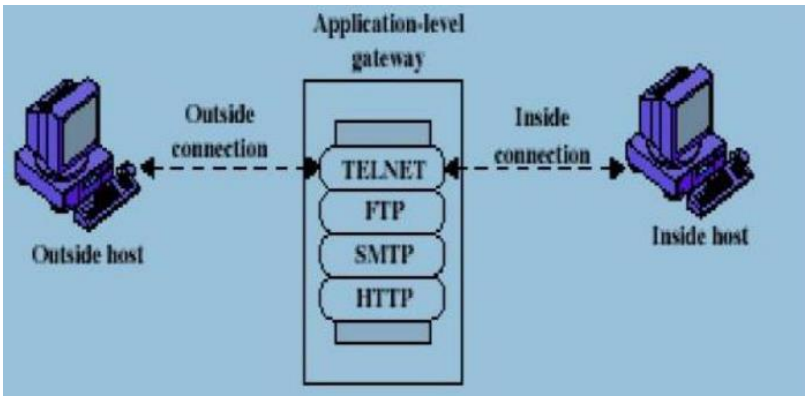
3. Application Gateway Firewall:

• Proxy firewalls operate at the application layer as an intermediate device to filter incoming traffic between two end systems (e.g., network and traffic systems). That is why these firewalls are called 'Application-level Gateways'.

• Unlike basic firewalls, these firewalls transfer requests from clients pretending to be original clients on the web-server. This protects the client's identity and other suspicious information, keeping the network safe from potential attacks.

• Once the connection is established, the proxy firewall inspects data packets coming from the source.

• If the contents of the incoming data packet are protected, the proxy firewall transfers it to the client. This approach creates an additional layer of security between the client and many different sources on the network.



3.1.3 Advantages of Firewall

1) **Blocks infected files:** While surfing the internet we encounter many unknown threats. Any friendly-looking file might have malware in it. The firewall neutralizes this kind of threat by blocking file access to the system.

2) **Stop unwanted visitors:** A firewall does not allow a cracker to break into the system through a network. A strong firewall detects the threat and then stops the possible loophole that can be used to penetrate through security into the system.
3) **Prevents Email spamming:** In this too many emails are sent to the same address leading to the server crashing. A good firewall blocks the spammer source and prevents the server from crashing.
4) **Control of network access:** By limiting access to specified individuals or groups for particular servers or applications, firewalls can be used to restrict access to particular network resources or services.
5) **Monitoring of network activity:** Firewalls can be set up to record and keep track of all network activity. This information is essential for identifying and looking into security problems and other kinds of shady behaviour.

3.1.4 Disadvantages of Firewall

1) **Infected Files:** In the modern world, we come across various kinds of files through emails or the internet. Most of the files are executable under the parameter of an operating system. It becomes impossible for the firewall to keep a track of all the files flowing through the system.
2) **User Restriction:** Restrictions and rules implemented through a firewall make a network secure but they can make work less effective when it comes to a large organization or a company. Even making a slight change in data can require a permit from a person of higher authority making work slow. The overall productivity drops because of all of this.
3) **System Performance:** A software-based firewall consumes a lot of resources of a system. Using the RAM and consuming the power supply leaves very less resources for the rest of the functions or programs. The performance of a system can experiences a drop. On the other hand, hardware firewall does not affect the performance of a system much, because it's very less dependent on the system resources.
4) **Complexity:** Setting up and keeping up a firewall can be time-consuming and difficult, especially for bigger networks or companies with a wide variety of users and devices.
5) **Cost:** Purchasing many devices or add-on features for a firewall system can be expensive, especially for businesses.

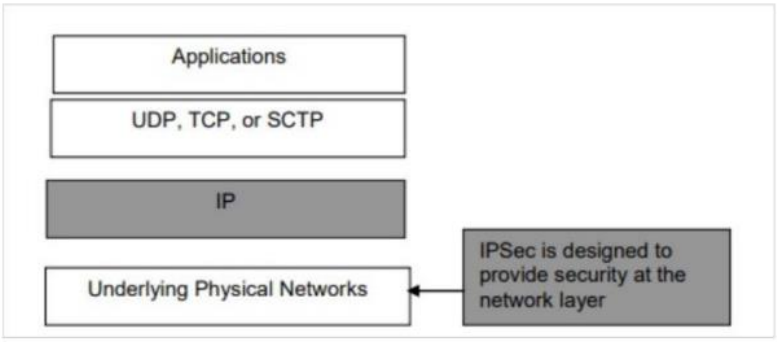
3.2 INTERNET PROTOCOL SECURITY AND ITS USE IN SECURE COMMUNICATION

3.2.1 Introduction

- It Provide security at network layer to the packet.
- It works for both IPv4 and IPv6.
- Applications:
  - Secure branch connectivity
  - Secure remote access

- Intranet and extranet connectivity
- Ecommerce security

- IP Security (IPSec) is a collection of protocols which is designed by Internet Engineering Task Force (IETF) to provide security for a packet at the network level. It helps to create confidential and authenticated and packets for the IP layer as shown in below diagram –

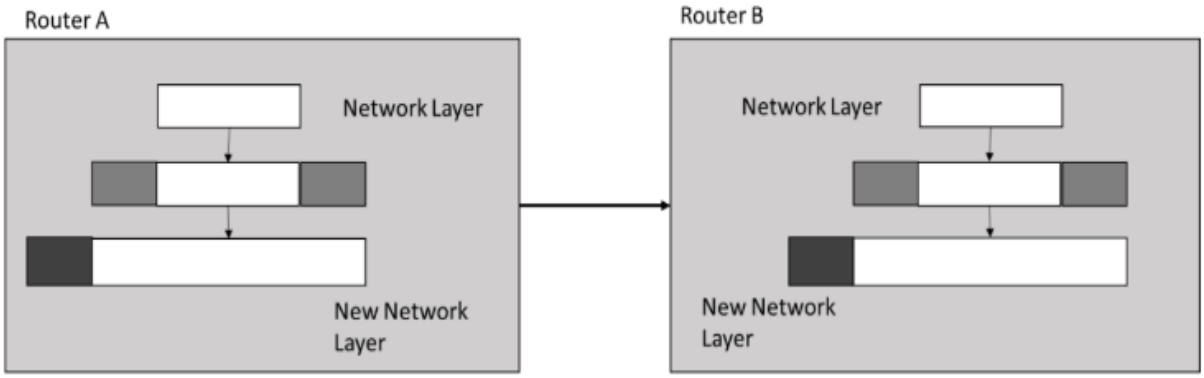


- IPSec protocol aim is to provide security services for IP packets like encrypting sensitive data/packets, authentication, and protection against replay and data confidentiality. It can be configured to operate in two different modes:
  - Tunnel Mode
  - Transport mode.
- The original packet is generated as follows −

IP Header	UDP Header	Data

1. Tunnel Mode

- In tunnel mode, an encrypted tunnel is established between two hosts. Suppose A and B are two hosts and want to communicate with each other using IPsec tunnel mode.
- First, they identify the corresponding proxies, say Pro1 and Pro2 and the logical encrypted tunnel is established between these two proxies.
- A sends its message to Pro1 and the tunnel carries this message to Pro2. Pro2 forwards this message sent by A to B.
- In tunnel mode, it protects the entire IP datagram. It adds the IPSec header and trailer to the Iap datagram and encrypts the whole.
- Then it adds a new IP header to this encrypted datagram.



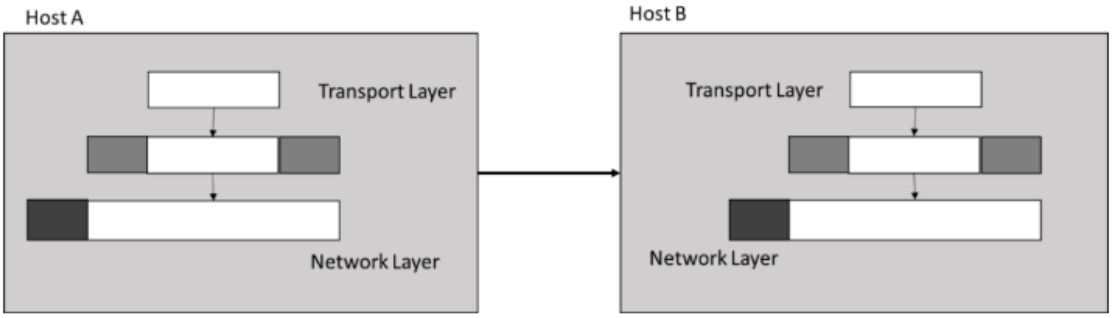
2. Transport mode:

• In transport mode, source addresses and destination addresses are not hidden during transmission.

• They are in plain text form i.e. anyone can read it.

• In transport mode, it takes transport-layer payload, and adds IPSec header and trailer and then encrypt them.

• After that it adds IP header, Thus IP header is not encrypted.



3.2.2 Features of IPSec

1) **Authentication:** IPSec provides authentication of IP packets using digital signatures or shared secrets. This helps ensure that the packets are not tampered with or forged.
2) **Confidentiality:** IPSec provides confidentiality by encrypting IP packets, preventing eavesdropping on the network traffic.
3) **Integrity:** IPSec provides integrity by ensuring that IP packets have not been modified or corrupted during transmission.
4) **Key management:** IPSec provides key management services, including key exchange and key revocation, to ensure that cryptographic keys are securely managed.
5) **Tunneling:** IPSec supports tunneling, allowing IP packets to be encapsulated within another protocol, such as GRE (Generic Routing Encapsulation) or L2TP (Layer 2 Tunneling Protocol).
6) **Flexibility:** IPSec can be configured to provide security for a wide range of network topologies, including point-to-point, site-to-site, and remote access connections.
7) **Interoperability:** IPSec is an open standard protocol, which means that it is supported by a wide range of vendors and can be used in heterogeneous environments.

3.2.3 Advantages of IPSec

1) **Strong security:** IPSec provides strong cryptographic security services that help protect sensitive data and ensure network privacy and integrity.
2) **Wide compatibility:** IPSec is an open standard protocol that is widely supported by vendors and can be used in heterogeneous environments.
3) **Flexibility:** IPSec can be configured to provide security for a wide range of network topologies, including point-to-point, site-to-site, and remote access connections.
4) **Scalability:** IPSec can be used to secure large-scale networks and can be scaled up or down as needed.
5) **Improved network performance:** IPSec can help improve network performance by reducing network congestion and improving network efficiency.

3.2.4 Disadvantages of IPSec

1) **Configuration complexity:** IPSec can be complex to configure and requires specialized knowledge and skills.
2) **Compatibility issues:** IPSec can have compatibility issues with some network devices and applications, which can lead to interoperability problems.
3) **Performance impact:** IPSec can impact network performance due to the overhead of encryption and decryption of IP packets.
4) **Key management:** IPSec requires effective key management to ensure the security of the cryptographic keys used for encryption and authentication.
5) **Limited protection:** IPSec only provides protection for IP traffic, and other protocols such as ICMP, DNS, and routing protocols may still be vulnerable to attacks.

3.2.5 Difference between IPv4 and IPv6

	IPv4	IPv6
Address length	IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
Fields	IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon.
Classes	IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.	IPv6 does not contain classes of IP addresses.
Number of IP	IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.

address		
VLSM	It supports VLSM (Virtual Length Subnet Mask). Here, VLSM means that Ipv4 converts IP addresses into a subnet of different sizes.	It does not support VLSM.
Address configuration	It supports manual and DHCP configuration.	It supports manual, DHCP, auto-configuration, and renumbering.
Address space	It generates 4 billion unique addresses	It generates 340 undecillion unique addresses.
End-to-end connection integrity	In IPv4, end-to-end connection integrity is unachievable.	In the case of IPv6, end-to-end connection integrity is achievable.
Security features	In IPv4, security depends on the application. This IP address is not developed in keeping the security feature in mind.	In IPv6, IPSEC is developed for security purposes.
Address representation	In IPv4, the IP address is represented in decimal.	In IPv6, the representation of the IP address in hexadecimal.
Fragmentation	Fragmentation is done by the senders and the forwarding routers.	Fragmentation is done by the senders only.
Packet flow identification	It does not provide any mechanism for packet flow identification.	It uses flow label field in the header for the packet flow identification.
Checksum field	The checksum field is available in IPv4.	The checksum field is not available in IPv6.
Transmission scheme	IPv4 is broadcasting.	On the other hand, IPv6 is multicasting, which provides efficient network operations.
Encryption and Authentication	It does not provide encryption and authentication.	It provides encryption and authentication.
Number of octets	It consists of 4 octets.	It consists of 8 fields, and each field contains 2 octets. Therefore, the total number of octets in IPv6 is 16.

3.3 VARIOUS TYPES OF IDSs

3.3.1 Introduction

- An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for the harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.
- Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.
- Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once send the warning notifications.

3.3.2 Detection Method of IDS:

Signature-based Method:

- Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects based on the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.
- Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system, but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

Anomaly-based Method:

- Anomaly-based IDS was introduced to detect unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning-based method has a better- generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

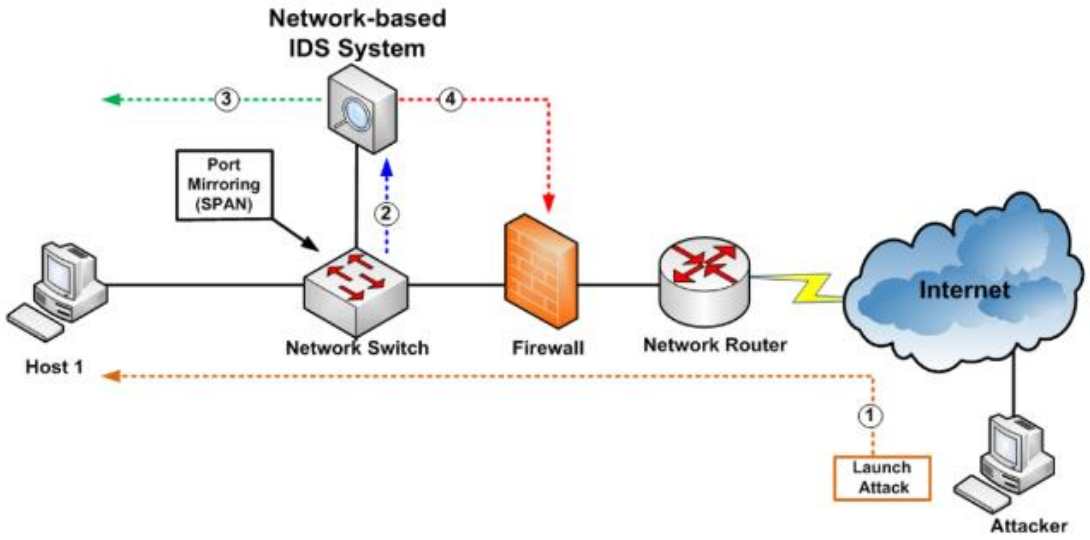
3.3.2 Benefits of IDS

1) **Detects malicious activity:** IDS can detect any suspicious activities and alert the system administrator before any significant damage is done.
2) **Improves network performance:** IDS can identify any performance issues on the network, which can be addressed to improve network performance.
3) **Compliance requirements:** IDS can help in meeting compliance requirements by monitoring network activity and generating reports.
4) **Provides insights:** IDS generate valuable insights into network traffic, which can be used to identify any weaknesses and improve network security.

3.4 DISTINGUISH HOST BASED IDSs & NETWORK BASED IDSs

1) Network Intrusion Detection System (NIDS):

- Network-based IDS is a system for examining network traffic to identify suspicious, malicious, or undesirable behavior.
- NIDS has visibility only into the traffic crossing the network link it is monitoring and typically has no idea of what is happening on individual systems.
- Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. 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. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are to see if someone is trying to crack the firewall.



Advantages of NIDS

- Providing IDS coverage requires fewer systems.
- Deployment, maintenance, and upgrade costs are usually lower.
- NIDS has visibility into all network traffic and can correlate attacks among multiple systems

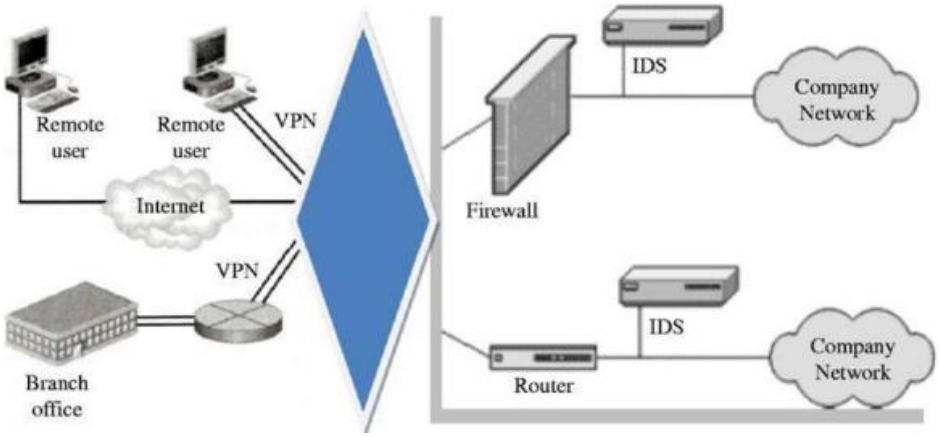
Disadvantages of NIDS

- It is ineffective when traffic is encrypted.
- It cannot see traffic that does not cross it.
- It must be able to handle high volumes of traffic.
- It doesn't know about activity on the hosts themselves.

2) Host Intrusion Detection System (HIDS):

- A host-based intrusion detection system computer system on which it is installed to detect an intrusion and/or misuse and responds by logging the activity and notifying the designated authority.

- Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.



Advantages of HIDS

- They can be very operating system specific and have more detailed signatures.
- They can reduce false positive rates.
- They can examine data after it has been decrypted.
- They can be very application specific.
- They can determine whether an alarm may impact that specific system.

Disadvantages of HIDS

- The IDS must have a process on every system you want to watch.
- The IDS can have a high cost of ownership and maintenance.
- The IDS uses local system resources.
- The IDS has a very focused view and cannot relate to activity around it.
- The IDS, if logged locally, could be compromised, or disabled.

3.5 HIDS AND NIDS COMPONENTS

- Data collectors: Using either agents or an agentless approach, your HIDS deploys sensors that collect data from hosts.
- Data storage: After being collected, the data is usually aggregated and stored in a central location. The data is retained at least as long as is necessary to analyze it, although organizations may also choose to keep the data on hand so they can reference it at a later time if desired.

- Analytics engine: The HIDS uses an analytics engine to process and evaluate the various data sources that it collects. The purpose of analytics is to look for patterns or anomalies, then assess the likelihood that they are the result of security risks or attacks.

3.6 ADVANTAGES AND DISADVANTAGES OF HIDS AND NIDS

Advantages of HIDS:

1) Verifies success or failure of an attack: Since a host-based IDS uses system logs containing events that have actually occurred, they can determine whether an attack occurred or not.

2) Monitors System Activities: A host-based IDS sensor monitors user and file access activity including file accesses, changes to file permissions, attempts to install new executables etc.

3) Detects attacks that a network-based IDS fail to detect: Host based systems can detect attacks that network based IDS sensors fail to detect. For example, if an unauthorized user makes changes to system files from the system console, this kind of attack goes unnoticed by the network sensors.

4) Near real time detection and response: Although host-based IDS do not offer true real-time response, it can come very close if implemented correctly.

5) Lower entry cost: Host based IDS sensors are far cheaper than the network-based IDS sensors.

Disadvantages of HIDS:

1) Host based IDSs are harder to manage, as information must be configured and managed for every host.

2) The information sources for host based IDSs reside on the host targeted by attacks, the IDSs may be attacked and disabled as part of the attack.

3) Host based IDSs are not well suited for detecting network scans or other such surveillance that targets an entire network.

4) Host-based IDSs can be disabled by certain denial-of- service attacks.

Advantages of NIDS:

1) A few well-placed network-based IDS can monitor a large network.

2) The deploying of NIDSs has little impact upon an existing network. NIDSs are usually passive devices that listen on a network wire without interfering with the normal operation of a

3) NIDSs can be made very secure against attack and even made invisible to many attackers.

Disadvantages of NIDS:

1) NIDSs may have difficulty possessing all packets in a large or busy network and, therefore, may fail to recognize an attack launched during period of high traffic.

2) Many of advantages of NIDSs don’t apply to more modern switch-based networks.

3) NIDSs cannot analyse encrypted information. This problem is increasing as organizations and attackers use virtual private network.

4) Most NIDSs cannot tell whether or not an attack was successful; they can only find that an attack was initiated.