System Security

Intruders:

- Intruders are often referred to as hackers and are the most harmful factors contributing to the vulnerability of security.
- Intruders breach the privacy of users and aim at stealing the confidential information of the users.
- The stolen information is then sold to third-party, which aim at misusing the information for their own personal or professional gains.

Intruders are divided into three categories:

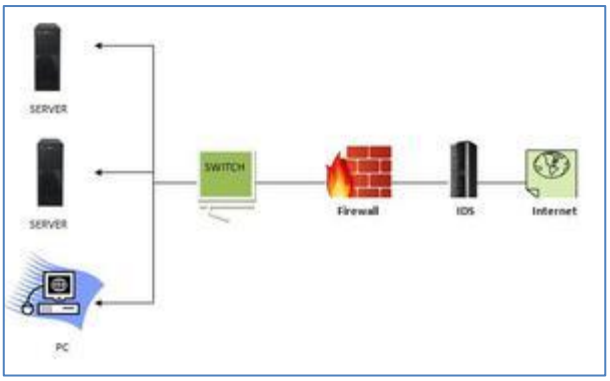
- **Masquerader**: The category of individuals that are not authorized to use the system but still exploit user's privacy and confidential information by possessing techniques that give them control over the system, such category of intruders is referred to as Masquerader. Masqueraders are outsiders and hence they don't have direct access to the system, their aim is to attack unethically to steal data/ information.

- **Misfeasor**: The category of individuals that are authorized to use the system, but misuse the granted access and privilege. These are individuals that take undue advantage of the permissions and access given to them, such category of intruders is referred to as Misfeasor. Misfeasors are insiders and they have direct access to the system, which they aim to attack unethically for stealing data/ information.

- **Clandestine User**: The category of individuals those have supervision/administrative control over the system and misuse the authoritative power given to them. The misconduct of power is often done by superlative authorities for financial gains, such a category of intruders is referred to as Clandestine User. A Clandestine User can be any of the two, insiders or outsiders, and accordingly, they can have direct/ indirect access to the system, which they aim to attack unethically by stealing data/ information.

Intrusion Detection System (IDS):

- A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed.
- It is software that checks a network or system for malicious activities or policy violations.
- Each illegal activity or violation is often recorded either centrally using a SIEM system or notified to an administration.
- IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders.
- It works in the background.



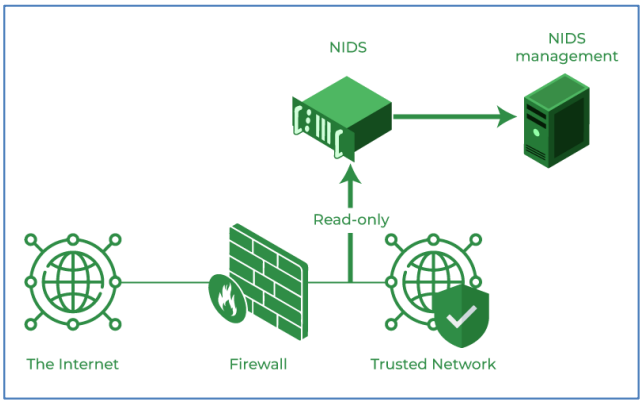
How does an IDS work?

- An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity.
- It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior.
- The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.
- If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator.
- The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.

Classification of Intrusion Detection System:

1.0 Network Intrusion Detection System (NIDS):

- 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.



Advantages of NIDS

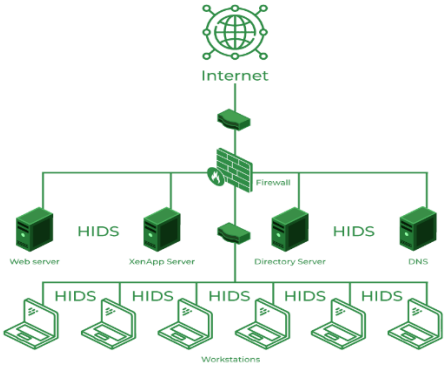
- A well placed network - Based IDS can monitor a large network.
- NIDS just listen to the network; it does not interfere in the network.
- NIDS can be made very secure against attack and made invisible to many attackers.
- Network-based IDS use live network traffic for real time attack detection and also operating system independent.

Disadvantages of NIDS

- It becomes difficult for NIDS to recognize the attack in large or busy network due to high traffic is there in network. It will be difficult for NIDS to analyze.
- NIDS cannot analyze the network if communication is in encrypted format.
- Difficult to detect the whole process of attack, usually detect only the initial level of attack.

2.0 Host Intrusion Detection System (HIDS):

- 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.



☞ **Advantages of HIDS**

- As defined earlier Host-based IDS operate on OS audit trails; they can help detect Trojan horse or other attacks that creates the software integrity violation.
- HIDS analyze most of the encrypted network traffic, which usually encrypted or decrypted by the sender and/or receiver.
- It is able to monitor and detect attack, which is sometimes not possible for Network IDS.

☞ **Disadvantages of HIDS**

- Host-based IDS are difficult to manage, because they generally installed on individual host. Monitoring to individual host is difficult because of different system configuration and log generation.
- W

3.0 Protocol-based Intrusion Detection System (PIDS):

- Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently reside at the front end of a server, controlling and interpreting the protocol between a user/device and the server.
- It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accepting the related HTTP protocol.

4.0 Application Protocol-based Intrusion Detection System (APIDS):

- An application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers.
- It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols.
- For example, this would monitor the SQL protocol explicitly to the middleware as it transacts with the database in the web server.

Hybrid Intrusion Detection System:

- Hybrid intrusion detection system is made by the combination of two or more approaches to the intrusion detection system.
- In the hybrid intrusion detection system, the host agent or system data is combined with network information to develop a complete view of the network system.

Detection Method of IDS

Signature-based Method: Signature-based IDS detects the attacks on the basis of the specific patterns such as the number of bytes or a number of 1s or the number of 0s in the network traffic. It also detects on the basis of 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 the system but it is quite difficult to detect 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 is developed rapidly. In anomaly-based IDS there is the 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 the model. The 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.

Benefits of IDS

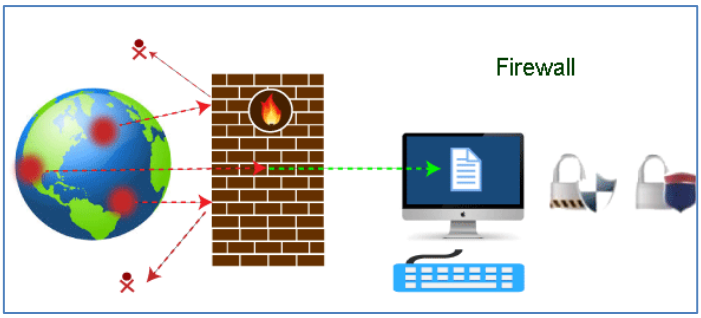
- **Detects malicious activity**: IDS can detect any suspicious activities and alert the system administrator before any significant damage is done.
- **Improves network performance**: IDS can identify any performance issues on the network, which can be addressed to improve network performance.
- **Compliance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

Firewalls

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. Accept : allow the traffic Reject : block the traffic but reply with an "unreachable error" Drop : block the traffic with no reply.

it acts as a filter to avoid unauthorized users from accessing private computers and networks.

The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks.



Need of Firewall

- **Different Requirements**:
- **Outlining Policies**:
- **Identifying Requirements**:
- **Setting Restrictions**:
- **Identify Deployment Location**

Firewall Design Principles

1. Developing Security Policy

Security policy is a very essential part of firewall design. Security policy is designed according to the requirement of the company or client to know which kind of traffic is allowed to pass. Without a proper security policy, it is impossible to restrict or allow a specific user or worker in a company network or anywhere else.

2. Simple Solution Design

If the design of the solution is complex. then it will be difficult to implement it. If the solution is easy. then it will be easier to implement it. A simple design is easier to maintain. we can make upgrades in the simple design according to the new possible threats leaving it with an efficient but more simple structure.

3. Choosing the Right Device

Every network security device has its purpose and its way of implementation. if we use the wrong device for the wrong problem, the network becomes vulnerable. if the outdated device is used for a designing firewall, it exposes the network to risk and is almost useless.

4. Layered Defense

A network defense must be multiple-layered in the modern world because if the security is broken, the network will be exposed to external attacks. Multilayer security design can be set to deal with different levels of threat.

5. Consider Internal Threats

While giving a lot of attention to safeguarding the network or device from external attacks. The security becomes weak in case of internal attacks and most of the attacks are done internally as it is easy to access and designed weakly. Different levels can be set in network security while designing internal security.

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.

Types of Firewalls:

1. **Packet Filters –**

- It is a technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols, and ports.
- This firewall is also known as a static firewall.
-

2. **Circuit-level gateways –**

A circuit-level gateway is a firewall that provides User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) connection security and works between an Open Systems Interconnection (OSI) network model's transport and application layers such as the session layer.

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

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

3. **Application Layer Firewalls –**

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'.

These firewalls can examine application layer (of OSI model) information like an HTTP request. If finds some suspicious application that can be responsible for harming our network or that is not safe for our network then it gets blocked right away.

4. **Software Firewall –**

The software firewall is a type of computer software that runs on our computers. It protects our system from any external attacks such as unauthorized access, malicious attacks, etc. by notifying us about the danger that can occur if we open a particular mail or if we try to open a website that is not secure.

5. **Hardware Firewall –**

A hardware firewall is a physical appliance that is deployed to enforce a network boundary. All network links crossing this boundary pass-through this firewall, which enables it to perform an inspection of both inbound and outbound network traffic and enforce access controls and other security policies.

Advantages of using Firewall

1. **Protection from unauthorized access**: Firewalls can be set up to restrict incoming traffic from particular IP addresses or networks, preventing hackers or other malicious actors from easily accessing a network or system. Protection from unwanted access.
2. **Prevention of malware and other threats:** Malware and other threat prevention: Firewalls can be set up to block traffic linked to known malware or other security concerns, assisting in the defense against these kinds of attacks.
3. **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.
4. **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 behavior.
5. **Regulation compliance:** Many industries are bound by rules that demand the usage of firewalls or other security measures. Organizations can comply with these rules and prevent any fines or penalties by using a firewall.
6. **Network segmentation:** By using firewalls to split up a bigger network into smaller subnets, the attack surface is reduced and the security level is raised.

Disadvantages of using Firewall

1. **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.
2. **Limited Visibility**: Firewalls may not be able to identify or stop security risks that operate at other levels, such as the application or endpoint level, because they can only observe and manage traffic at the network level.
3. **False sense of security**: Some businesses may place an excessive amount of reliance on their firewall and disregard other crucial security measures like endpoint security or intrusion detection systems.
4. **Limited adaptability**: Because firewalls are frequently rule-based, they might not be able to respond to fresh security threats.
5. **Performance impact:** Network performance can be significantly impacted by firewalls, particularly if they are set up to analyze or manage a lot of traffic.
6. **Limited scalability**: Because firewalls are only able to secure one network, businesses that have several networks must deploy many firewalls, which can be expensive.

7. **Limited VPN support:** Some firewalls might not allow complex VPN features like split tunneling, which could restrict the experience of a remote worker.
8. **Cost**: Purchasing many devices or add-on features for a firewall system can be expensive, especially for businesses.

Real-Time Applications of Firewall

1. **Corporate networks**: Many businesses employ firewalls to guard against unwanted access and other security risks on their corporate networks. These firewalls can be set up to only permit authorized users to access particular resources or services and to prevent traffic from particular IP addresses or networks.
2. **Government organizations:** Government organizations frequently employ firewalls to safeguard sensitive data and to adhere to rules like HIPAA or PCI-DSS. They might make use of cutting-edge firewalls like Next-generation firewalls (NGFW), which can detect and stop intrusions as well as manage access to particular data and apps.
3. **Small enterprises**: Small firms may use firewalls to separate their internal networks, restrict access to specific resources or applications, and defend their networks from external threats.
4. **Networks at home:** To guard against unwanted access and other security risks, many home users employ firewalls. A firewall that many routers have built in can be set up to block incoming traffic and restrict access to the network