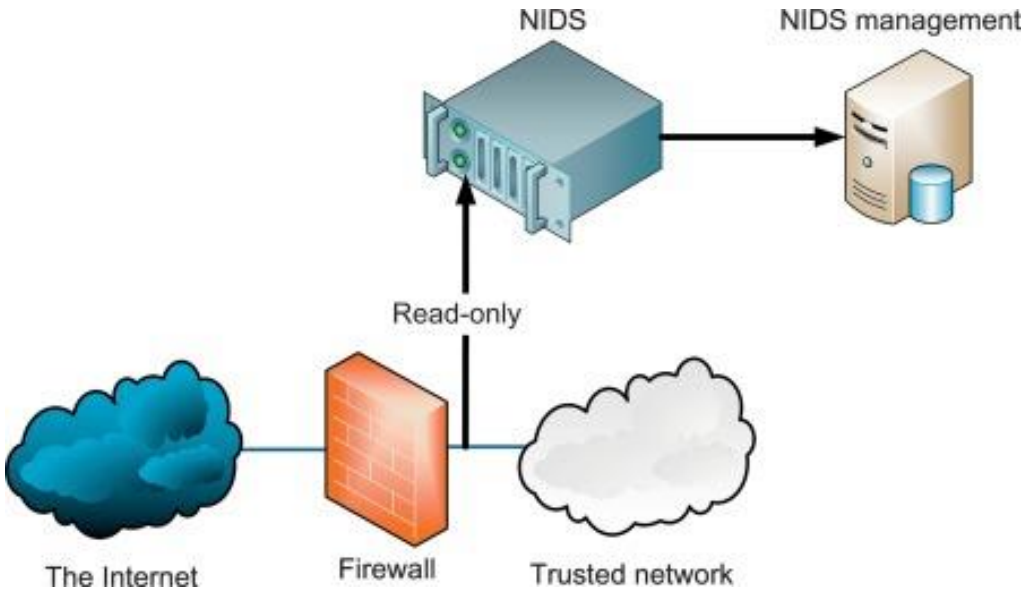
4.3 NETWORK BASED INTRUSION DETECTION SYSTEM

What is NIDS?

- As mentioned, NIDS (Network Intrusion Detection System) is a security technology that monitors and analyzes network traffic for signs of malicious activity, unauthorized access, or security policy violations. The primary function of a NIDS is to detect and alert network administrators of any potential or ongoing attacks on the network.
- NIDS works by examining data packets for specific patterns and behaviors that indicate the presence of an attack. It can detect and alert network administrators of attacks such as DoS (Denial of Service), port scanning, virus and malware infections, and unauthorized access attempts.
- NIDS is an essential component of a comprehensive network security strategy. It helps to identify and respond to threats quickly before they can cause significant damage or compromise sensitive data.



How Does NIDS Work?

- Network-based Intrusion Detection System analyzes the network traffic and looks for behavior patterns indicative of an intrusion or attack. It typically operates in a passive or inline mode, and they use different detection methods to identify network intrusions.
- In passive mode, the NIDS monitors outgoing network traffic without interfering with it. In inline mode, the NIDS can modify network traffic to detect intrusions or block malicious activities. However, the active mode may increase the risk of disrupting legitimate network traffic, and it is usually not recommended.
- When a NIDS detects a potential network threat, it generates an alert. The alert includes information such as the type of attack, the source and destination IP addresses, and the time of the attack. The NIDS may also take action to prevent the attack, such as blocking the source IP address or modifying current network traffic.

Methods of NIDS Detection

- Network Intrusion Detection Systems are designed to detect network-based attacks and intrusions. They use different detection methods to identify suspicious traffic and abnormal behavior. There are three primary detection methods used by NIDS: signature-based detection, anomaly-based detection, and hybrid detection.

1. Signature-Based Detection

- This method compares traffic passing through the network against known attack signatures or patterns. Attack signatures are predefined network traffic patterns associated with specific types of attacks.
- The NIDS alerts the network administrator if the traffic matches a known signature. Signature-based detection is effective at identifying known attacks, but it cannot detect new or unknown attacks.

2. Anomaly-Based Detection

- This method involves detecting traffic that deviates from the normal network behavior. NIDS monitors network traffic and generates an alert if it detects any activity outside the expected range. Anomaly-based detection is useful in detecting new or unknown attacks but can generate many false positives.

3. Hybrid Detection

- This method combines signature-based and anomaly-based detection methods. The NIDS first uses signature-based detection to identify known attacks and then anomaly-based detection to identify unknown attacks. By combining both methods, hybrid detection can provide high accuracy and minimize the false positive rate.

Others

- In addition to these three primary methods, NIDS can use other techniques, such as protocol and heuristic analysis. Protocol analysis involves examining network traffic to detect protocol violations and abnormal behavior. The heuristic analysis involves identifying patterns of behavior that are associated with attacks.

Technologies That a Network-Based Intrusion Detection System Can Monitor

- NIDS systems can monitor network technologies and protocols to detect potential security breaches. Here are some of the technologies that these systems can monitor:

1. Network Protocols

- NIDS systems can monitor network protocols such as TCP/IP, HTTP, FTP, DNS, SMTP, and SNMP to detect anomalous behavior that might indicate a network attack. For example, the system can detect any attempts to exploit vulnerabilities in the protocol to gain unauthorized access.

2. Network Devices

- NIDS systems can monitor network devices such as routers, switches, and firewalls to detect unauthorized access or configuration changes. The system can also detect any attempts to exploit vulnerabilities in the devices to gain access to the network.

3. Applications

- NIDS systems can monitor network applications such as email servers, web servers, and databases to detect any unusual activity that might indicate a security breach. For example, the system can detect attempts to access sensitive information or execute malicious code.

4. Operating Systems

- NIDS systems can monitor the operating systems of network devices and servers to detect any security vulnerabilities or malicious activity. The system can detect any attempts to exploit vulnerabilities in the operating system to gain unauthorized access.

5. Wireless Networks

- NIDS can monitor wireless networks to detect any unauthorized access or malicious activities. The system can monitor the wireless traffic and identify rogue access points, unauthorized connections, or denial of service attacks.

Advantages of Network Intrusion Detection System

- Network Intrusion Detection Systems (NIDS) are essential to network security infrastructure. Here are some of the vital advantages of using NIDS:

- **1. Prevention of Network Attacks**

- NIDS actively monitors the network traffic for any suspicious activities and potential threats. It can detect and block any unauthorized attempts to access the network, such as port scanning, password guessing, and other attacks. By preventing these attacks, NIDS can help maintain network security and prevent data breaches.

2. Identification of Vulnerabilities

- NIDS can scan for vulnerabilities in the network, such as misconfigured devices, outdated software, and unsecured network connections. Once these vulnerabilities are detected, they can be addressed before attackers can exploit them, preventing potential security breaches.

3. Protection of Sensitive Information

- NIDS can help protect sensitive information, such as customer data, financial records, and intellectual property, by monitoring the network for any unauthorized access attempts. If an attempt is detected, NIDS can alert security personnel, who can take appropriate action to prevent data loss or theft.

4. Real-Time Monitoring

- NIDS provides real-time network monitoring, allowing security personnel to respond to any threats or attacks quickly. This quick response can help prevent any potential damage caused by the attack and minimize downtime.

5. Compliance with Regulations

- NIDS can help organizations comply with various regulations such as HIPAA, PCI-DSS, and GDPR, which require organizations to have proper security measures to protect sensitive data.

Limitations of Network Intrusion Detection Systems

1. Need for Frequent Updating

- This is because new attack methods are constantly being developed, and NIDS must be able to detect these new threats. NIDS typically uses signature-based detection methods, which must be updated with new signatures to detect new attacks. If the system is not updated regularly, it may miss new threats.

2. Time-Consuming Process

- NIDS requires extensive configuration to ensure it is tailored to the organization's needs. The configuration of NIDS includes defining the types of traffic that should be monitored, setting the detection thresholds, and configuring the alerting and reporting mechanisms.
- This can be time-consuming and requires a skilled technician to ensure the system is optimized for the organization's needs.

3. Regular Maintenance

- NIDS requires maintenance to ensure that it is functioning properly. This includes monitoring the system to ensure it generates alerts correctly, responds promptly, and addresses any issues. Regular maintenance is essential to ensure that the system functions at peak performance and provides the level of protection the organization requires.

HIDS vs. NIDS

- Host-Based Intrusion Detection Systems are similar in some ways to Network Intrusion Detection Systems, or NIDS, but they are not the same type of solution.
- A NIDS monitors for suspicious activity from the perspective of the network, using data sources like network switch logs. By analyzing this data, a NIDS can look for suspicious activity.
- A HIDS may also monitor network activity, but it does so from the perspective of individual hosts, not centralized networking equipment like switches. In addition, for a HIDS, network data is just one of many data sources used for security analysis purposes.