Unit v

Network Security refers to the **strategies, policies, technologies, and practices** used to **protect the integrity, confidentiality, and availability** of computer networks and data. It defends against **unauthorized access, misuse, modification, or denial of the network and its resources**.

🔑 Goals of Network Security (CIA Triad)

1. **Confidentiality** – Prevent unauthorized access to sensitive information.
2. **Integrity** – Ensure data is accurate and unaltered.
3. **Availability** – Ensure that network resources are available to authorized users when needed.

🛠️ Key Components of Network Security

Component	Function
Firewall	Blocks or allows traffic based on rules.
Antivirus/Anti-malware	Detects and removes malicious software.
Intrusion Detection Systems (IDS)	Monitors network traffic for suspicious activity.
Intrusion Prevention Systems (IPS)	Blocks detected threats automatically.
Virtual Private Network (VPN)	Encrypts traffic between users and network.
Access Control	Ensures only authorized users can access resources.
Network Segmentation	Divides the network to limit threat spread.
Encryption	Protects data during transmission.
Authentication Systems	Validates user identities (e.g., passwords, biometrics).

🧨 Common Network Security Threats

Threat Type	Description
Malware	Viruses, worms, ransomware, spyware, etc.
Phishing	Fake communications to steal data.
Denial-of-Service (DoS/DDoS)	Flooding a network to make it unavailable.
Man-in-the-Middle (MITM)	Intercepting communication between two parties.
SQL Injection	Exploiting databases via user input fields.
Zero-Day Exploits	Attacks using unknown vulnerabilities.

🔐 Techniques for Network Security

- **Strong Passwords and Multi-Factor Authentication (MFA)**
- **Regular Software Updates and Patch Management**
- **Traffic Monitoring and Logging**
- **Security Awareness Training for Users**
- **Backup and Disaster Recovery Planning**

🧱 Layers of Network Security.

1. **Physical Layer Security** – Restrict access to hardware.
2. **Network Layer Security** – Use firewalls, routers, and segmentation.
3. **Application Layer Security** – Protect software and user interfaces.
4. **User Layer Security** – Train users and enforce policies.

📊 Example: Security Policy for a Small Network

- Only allow HTTPS and SSH connections.
- Block unknown IP addresses.
- Encrypt all wireless traffic with WPA3.
- Log and monitor all admin login attempts.
- Use VLANs to separate guest and internal traffic.

SECURITY ATTACKS — Concept in Cybersecurity

Security attacks are **deliberate attempts to breach the confidentiality, integrity, or availability** of an information system or network. These attacks are carried out by individuals (called **attackers** or **threat actors**) to **steal data**, **disrupt services**, **gain unauthorized access**, or **cause damage**.

🔍 Categories of Security Attacks

1. Passive Attacks

These aim to **observe or steal data** without altering it.

Type	Description
Eavesdropping (Sniffing)	Listening to network traffic to steal information like passwords or messages.
Traffic Analysis	Studying communication patterns (like who talks to whom and how often) to gather intelligence.

✅ **Goal**: Stealthy surveillance
❌ **No data alteration**, just information gathering

---

2. Active Attacks

These **disrupt or modify** the target system or data.

Type	Description
Masquerade Attack	Attacker pretends to be an authorized user.
Replay Attack	Old data transmission is fraudulently repeated.
Modification Attack	Data is tampered with during transmission.
Denial of Service (DoS)	System is overwhelmed to make it unavailable.
Man-in-the-Middle (MITM)	Attacker secretly relays and possibly alters the communication.

✅ **Goal**: Change, disrupt, or destroy data or service
❌ **Highly intrusive**

🔐 Based on Objectives — CIA Triad

Objective	Example of Attack
Confidentiality	Eavesdropping, Data Theft
Integrity	Data Tampering, Injection Attacks
Availability	DoS/DDoS Attacks, Ransomware

🧠 Common Examples of Security Attacks

Attack Type	Description
Phishing	Fake emails trick users into revealing personal info.
Malware	Malicious software (e.g., virus, worm, trojan) harms systems.
SQL Injection	Injecting malicious SQL queries to access or destroy databases.
Brute Force	Trying multiple passwords until the correct one is found.
Zero-Day Exploit	Attacks that exploit unknown vulnerabilities before a fix exists.

🛡️ Basic Prevention Measures

- Use **firewalls and antivirus**.
- Enable **multi-factor authentication (MFA)**.
- Regularly **update software and systems**.
- Educate users about **social engineering and phishing**.
- Encrypt sensitive data and use **secure protocols (HTTPS, SSH)**.

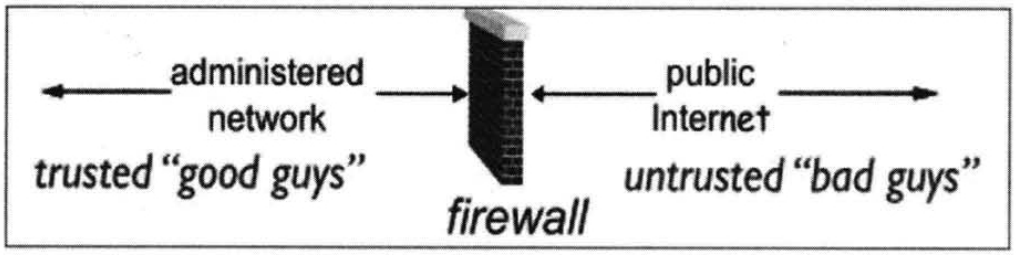
5.6 Firewall.

Almost every medium and large-scale organization has a presence on the Internet and has an organizational network connected to it. Network partitioning at the boundary between the outside Internet and the internal network is essential for network security. Sometimes the inside network (intranet) is referred to as the "trusted" side and the external Internet as the "un-trusted" side.

5.6.1 Types of Firewall

Firewall is a network device that isolates organization's internal network from larger outside network/Internet. It can be a hardware, software, or combined system that prevents unauthorized access to or from internal network.

All data packets entering or leaving the internal network pass through the firewall, which examines each packet and blocks those that do not meet the specified security criteria.



Deploying firewall at network boundary is like aggregating the security at a single point. It is analogous to locking an apartment at the entrance and not necessarily at each door.

Firewall is considered as an essential element to achieve network security for the following reasons –

- Internal network and hosts are unlikely to be properly secured.
- Internet is a dangerous place with criminals, users from competing companies, disgruntled ex-employees, spies from unfriendly countries, vandals, etc.
- To prevent an attacker from launching denial of service attacks on network resource.
- To prevent illegal modification/access to internal data by an outsider attacker.

A **firewall** is a network security device or software that **monitors and controls incoming and outgoing network traffic** based on predetermined security rules.

There are several types of firewalls based on **deployment**, **technique**, and **generation**.

🧱 1. Packet-Filtering Firewall

- **Oldest and simplest** type.
- Works at **Network Layer (Layer 3)**.
- Examines **source/destination IP, port, and protocol**.
- Allows or blocks packets based on rules.

✅ **Fast**
❌ No deep inspection, no state awareness

Example Rule:
Allow TCP traffic from `192.168.1.5:80` to `10.0.0.2:8080`

🔁 2. Stateful Inspection Firewall (Dynamic Filtering)

- Works at **Network and Transport Layers (Layer 3 & 4)**.
- Tracks **connection state** (e.g., TCP handshake).
- Makes decisions based on the **context of traffic** (not just packets).

✅ More secure than packet-filtering
❌ Slower, more resource usage

🔍 3. Proxy Firewall (Application-Level Gateway)

- Works at **Application Layer (Layer 7)**.
- Acts as an **intermediary** between client and server.
- **Inspects entire data payload** (e.g., HTTP, FTP).

✅ High-level filtering, can hide internal IPs
❌ Slower, needs configuration for each app

🧠 4. Next-Generation Firewall (NGFW)

- Combines traditional firewall features with **advanced security**:
  - Deep Packet Inspection (DPI)
  - Intrusion Detection/Prevention (IDS/IPS)
  - Malware filtering
  - Application awareness

✅ Smart, powerful
❌ Expensive, complex configuration

📱 5. Software Firewall

- Runs on **individual devices** (host-based).
- Filters traffic to/from that specific machine.
- Example: **Windows Defender Firewall**

✅ Good for personal computers
❌ Limited scope for enterprise protection

📡 6. Hardware Firewall

- A **physical device** placed at the network perimeter.
- Filters traffic for **entire network**.

✅ Ideal for large networks
❌ More costly than software-only solutions

🌐 7. Cloud Firewall (Firewall-as-a-Service - FWaaS)

- Hosted in the **cloud**.
- Protects cloud-based infrastructure or remote users.
- Managed by a third-party provider.

✅ Scalable, centralized security
❌ Dependent on internet availability

📊 Summary Table

Type	OSI Layer	Use Case	Speed	Complexity
Packet Filtering	Layer 3	Basic filtering	✅ Fast	❌ Simple
Stateful Inspection	Layer 3 & 4	Tracks connection states	⚖️ Medium	⚖️ Medium
Proxy Firewall	Layer 7	Application-specific security	❌ Slower	✅ High
Next-Gen Firewall (NGFW)	Multiple Layers	Enterprise, DPI, threat detection	❌ Slower	✅ High
Software Firewall	Host-based	Personal computers	✅ Fast	✅ Simple
Hardware Firewall	Network perimeter	Organizations	⚖️ Medium	⚖️ Medium
Cloud Firewall (FWaaS)	Cloud layer	Cloud infra & remote security	✅ Fast	✅ Flexible

---

🖼️ Firewall Placement in a Network Diagram

```
plaintext
CopyEdit
                    [Internet / WAN]
                           |
                  [Hardware Firewall]
                           |
        +------------------+------------------+
        |                                     |
   [Web Server]                        [Internal Network]
                                    +--------+--------+
                                    |        |        |
                                [User A] [User B]  [File Server]
```

🔰 Where Each Firewall Works

Firewall Type	Location in Network	Real Example Tools
Packet-Filtering	On a **router** or basic firewall device	iptables (Linux), Cisco Access Control Lists
Stateful Inspection	On **firewall appliance or router**	Cisco ASA, pfSense
Proxy Firewall	Between users and external services	Squid, Blue Coat Proxy
Next-Gen Firewall	At **network perimeter** or data center	Palo Alto NGFW, Fortinet, Check Point
Software Firewall	On **individual computers/servers**	Windows Defender Firewall, UFW (Linux)
Hardware Firewall	As a **dedicated box before internal LAN**	Cisco ASA, SonicWall, Netgear ProSAFE
Cloud Firewall (FWaaS)	Hosted in the **cloud**	Zscaler, Cloudflare Gateway, Azure Firewall

📌 Examples of Usage in the Real World

Use Case	Firewall Type Used
Home PC protection	Software firewall (Windows)
Small office with few users	Hardware firewall + Stateful
Enterprise with apps and users	NGFW + Proxy + IDS/IPS
Cloud apps (AWS, Azure, GCP)	Cloud firewall + NGFW
Blocking specific URLs/apps	Proxy Firewall or NGFW
Allow only TCP port 80 (HTTP)	Packet-filtering firewall

1. **iptables (Linux packet-filtering firewall)**
2. **Windows Defender Firewall (via `netsh`)**
3. **Cisco ASA (Stateful Hardware Firewall)**
4. **pfSense (Web UI-based, briefly explained)**

🧱 1. iptables – Linux Packet Filtering

🔒 Block incoming traffic on port 22 (SSH)

```
bash
CopyEdit
sudo iptables -A INPUT -p tcp --dport 22 -j DROP
```

✅ Allow incoming HTTP traffic on port 80

```
bash
CopyEdit
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

❌ Flush all firewall rules (reset)

```
bash
CopyEdit
sudo iptables -F
```

To make rules permanent, save them using:

```
bash
CopyEdit
sudo iptables-save > /etc/iptables/rules.v4
```

🧰 2. Windows Defender Firewall – Command Line (netsh)

✅ Allow an app (e.g., Chrome)

```
cmd
CopyEdit
netsh advfirewall firewall add rule name="Allow Chrome" dir=in action=allow
program="C:\Program Files\Google\Chrome\Application\chrome.exe" enable=yes
```

❌ Block a specific port (e.g., port 21 - FTP)

```
cmd
CopyEdit
netsh advfirewall firewall add rule name="Block FTP" dir=in action=block
protocol=TCP localport=21
```

🌐 3. Cisco ASA – Stateful Hardware Firewall

✅ Allow HTTP from outside to a web server

```
c
CopyEdit
access-list OUTSIDE_IN extended permit tcp any host 192.168.1.100 eq 80
access-group OUTSIDE_IN in interface outside
```

❌ Deny all ICMP (ping) from outside

```
cisco
CopyEdit
access-list OUTSIDE_IN extended deny icmp any any
access-group OUTSIDE_IN in interface outside
```

Replace `192.168.1.100` with your internal server IP.

🔧 4. pfSense – Web UI Firewall Rules (GUI)

To allow HTTP traffic:

- Go to **Firewall** > **Rules** > **WAN**
- Click **"Add"**
  - Action: `Pass`
  - Protocol: `TCP`
  - Destination Port Range: `80`
  - Destination: Your internal web server IP
- Click **Save** and **Apply Changes**

To block all FTP (port 21):

- Similar steps, but select:
  - Action: `Block`
  - Destination Port Range: `21`

INTRUSION DETECTION SYSTEMS (IDS)

Intrusion detection systems (IDS) are designed to identify suspicious and malicious activity through network traffic. It enables real-time intrusion detection on your network to help optimize intrusion detection. So, let's get to know the meaning of an intrusion detection system and how it works and how it works.

What Is an Intrusion Detection System?

An intrusion detection system definition includes installing a monitoring system that helps detect suspicious activities and issue alerts about them. Depending upon these alerts, a SOC (security operations center) analyst or the incident responder investigates the issue and takes the required steps to eradicate the threat.

While these systems are quite effective for detecting malicious activity, they sometimes generate false alarms. So, organizations need to fine-tune them at the time of installation. This means you need to properly set up the intrusion detection system to identify what normal traffic on the network looks like.

Additionally, the intrusion prevention system also keeps a check on the network packets to detect malicious activity.

Why Are Intrusion Detection Systems Important?

The goal of IDS is to monitor the network assets to detect inappropriate behavior in the network. Attackers continuously develop new exploits and affect techniques that are designed to affect the defense. Some attacks are for obtaining user credentials that grant access to the network and data. A Network Intrusion detection system (NIDS) is important for network security as it allows you to respond to malicious traffic.

An intrusion detection system's prime benefit is ensuring that the respective person is notified when the attack happens. In addition, a network intrusion detection system keeps a check on both inbound and outbound traffic on the network and monitors data traversing between the system and the network.

How Do Intrusion Detection Systems Work?

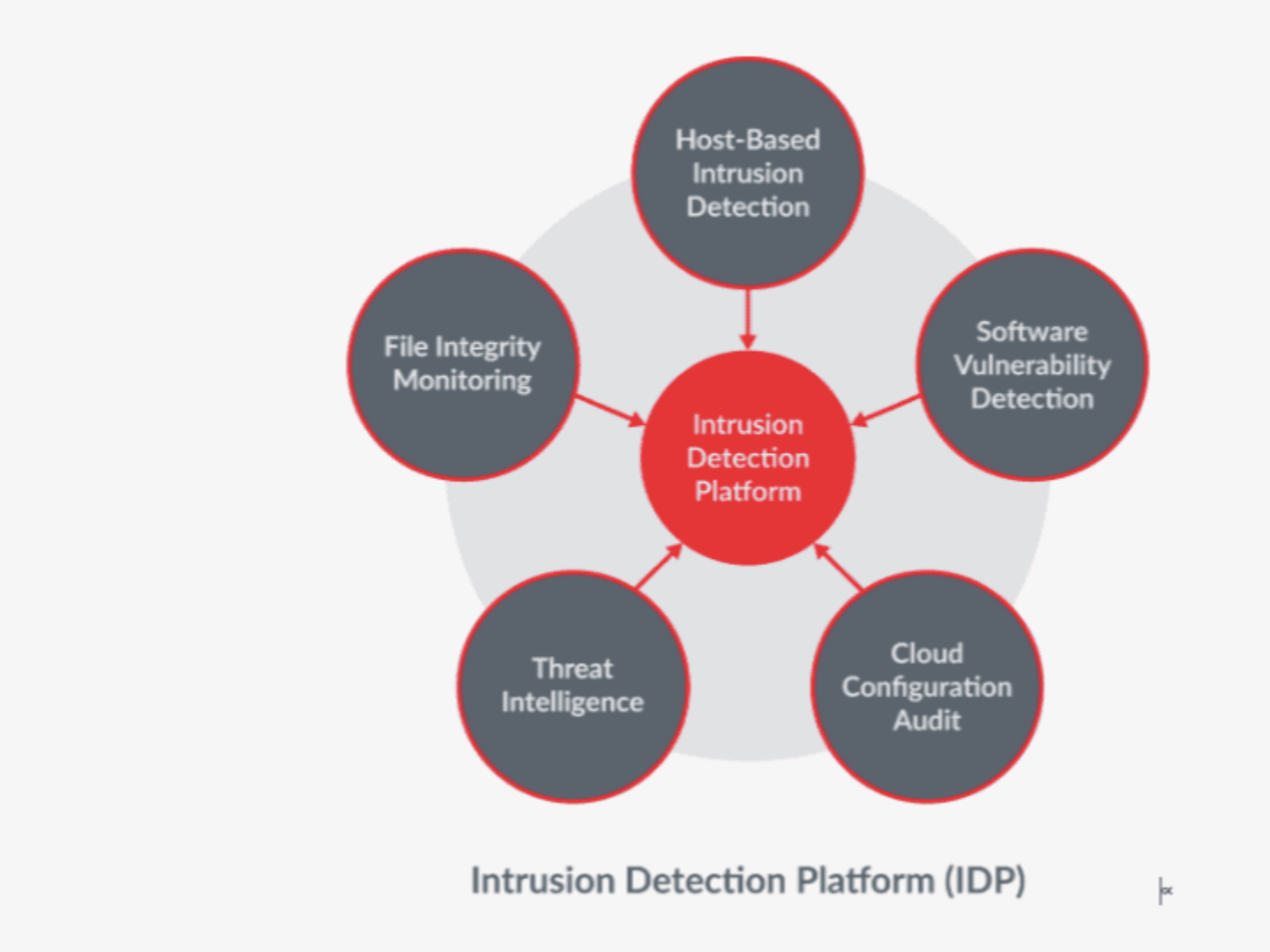
IDS operates through a process where different events on the network are analyzed and monitored to detect incidents of malicious activity or any kind of security violation.

It is placed out from the real-time communication band in your network to work as a detection system. It uses SPAN or TAP port to analyze the copy of inline network packets to ensure that the traffic coming is not malicious.

So, if you set an IDS program, the system will be able to:

- Recognize attack patterns from the network packets
- Monitor the user behavior
- Identify the abnormal traffic activity
- Ensure that user and system activity do not go against security policies

Types of an Intrusion Detection System



[Source]

There are many different types of IDS for protecting computer networks. Below are popular types of intrusion detection systems:

1. Host Intrusion Detection Systems (HIDS):

HIDS host-based intrusion detection system runs on independent devices, i.e., a host on the network monitors the incoming and outgoing packets and alerts the administrator about malicious activity. It takes a snapshot of the existing system files to

identify the abnormalities. If there are any discrepancies among the file sent or if anything got deleted, an alert is sent to the administrator for further investigations.

2. Protocol-Based Intrusion Detection System (PIDS):

PIDS, a Protocol-based Intrusion Detection System, is a system or agent that resides consistently at the front end of the server to control and interpret the protocol between the user and the server. PIDS is for securing the web server by monitoring the HTTPS protocol stream. A typical use of PIDS is at the front end of the web server, keeping a check on the HTTP or HTTPS stream.

3. Application Protocol-Based Intrusion Detection System (APIDS):

An application-based intrusion detection system is a system that stays within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols.

APIDS uses machine language to establish the baseline of the expected system behavior in terms of bandwidth, ports, protocol, and device usage.

4. Hybrid Intrusion Detection System:

A hybrid intrusion detection system results from two or more approaches to the intrusion detection system. In this, the host agent or the system data is combined with the network information to develop a complete view of network systems. This system is quite effective in comparison to other IDS.

Detection Method of IDS Deployment

Any IDS uses different methods for detecting malicious network traffic. Some of them are:

1. Signature Detection:

Signature-based intrusion detection systems use fingerprints of known threats to keep a check on them. Once the malicious traffic or packets are detected, the IDS generates a signature to scan the incoming traffic to detect known malicious patterns. The signature-based IDS can detect the attacks whose patterns are already present in the system but are unable to detect new or unknown malicious or attack network traffic. Example buffer overflow it contains shellcodes.

2. Anomaly Detection:

The anomaly-based intrusion detection system was introduced to detect unknown malicious attacks as new attack methods are developed quickly. This detection method uses machine learning to create a trustful activity model, and anything that comes is compared with that model to detect malicious traffic or patterns. The machine learning-based method has better-generalized property as compared to the signature-based IDS and are trained with the intrusion detection system application and hardware configurations.

3. Hybrid Detection:

This IDS uses both signature-based as well as anomaly-based detection system and enable it to detect potential threats with a minimum error rate.

Benefits of Intrusion Detection Systems

Apart from raising the alarms, the intrusion detection system software also helps in configuring rules, policies, and respective actions to be taken.

Below are the benefits of using an IDS:

1. It keeps a check on the routers, firewalls, key servers, and files and uses its database to raise the alarm and send notifications.
2. Offer centralized management for the correlation of the attack.
3. Act as an additional layer of protection for the company.
4. It analyzes different attacks, identifies their patterns, and helps the administrator to organize and implement effective control.
5. Provide system administrators the ability to quantify the attack.
6. An intrusion detection system in cyber security help detects cyber security problems.

Challenges of Intrusion Detection Systems

There are four key challenges that businesses face when managing IDS systems:

1. Ensuring Effective Deployment:

To ensure a high level of visibility, companies must ensure that their wireless intrusion detection system is optimized and installed correctly. While deploying IDS can be tricky, and if not done properly, it may create vulnerabilities for critical assets.

2. Understanding and Investigating Alerts:

IDS alerts give very little information, which, sometimes, is hard to investigate. You may lag with information like what caused the attack or what further actions are required to oppose a threat. Also, investigating the IDS alerts can be time and resource-intensive, which may require additional information to identify the seriousness of the attack.

3. Managing a High Volume of Alerts:

Since there is the vast majority of attacks are generated by intrusion detection, it may put the burden on internal teams to identify each one of them. Sometimes, these system alerts are false positives, which are hard to screen. Also, some IDS come pre-loaded with some defined alert signatures that are insufficient for many organizations.

4. Knowing How to Tackle Threats:

A common issue that organizations face is the lack of appropriate incident response capability. Identifying a problem is half a thing; knowing how to respond appropriately is a challenging and critical thing. An effective incident response needs an expert who knows how to remediate threats and what procedures are required to address the issue. Sometimes a home intrusion detection system gives false alarms, so keep a check on the type of threats and how you need to handle them.

IDS Vs. Firewall

Installing an intrusion Detection System project and a firewall offers cyber security solutions deployed to protect the network or its end point. IDS is a passive monitoring device that helps detect threats and generate alerts. It enables SOC (security operation center) analysts or incident responders to detect and respond to the threat. An IDS provides no protection to the endpoint.

On the other hand, a firewall is an active protective device and is more like an Intrusion Prevention System (IPS). It performs analysis of the metadata of the network packets and helps block/allow the traffic based on some pre-set rules. This creates a boundary on which some types of traffic or protocols cannot pass.

An IPS is more like an IDS, but the only difference is that it blocks the identified threats instead of raising the alert. This functionality makes IPS more popular among firewalls, and many next-gen firewalls are integrating this functionality.

How To Select An IDS Solution

Once you know what IDS is and its detection, you need to follow these steps to select an IDS solution:

1. Identify the Baseline: To ensure that your IDS works appropriately, set a baseline so you would know what's coming on your network. Keep in mind that every network carries additional traffic, and defining a pre-set initial baseline help prevent false negatives. An intrusion detection system in network security will keep your network protected from firewalls. To ensure that your IDS works appropriately, set up a baseline so that you would know what's coming on your network. Keep in mind that every network carries different traffic, and defining a pre-set initial baseline help prevent false negatives. An intrusion detection system in network security will keep your network protected from firewalls.

2. Define the Deployment: Always deploy the distributed intrusion detection system at the highest point to not overwhelm the system with data. Place it at the edge, behind the firewall, or install multiple ID Sec if you are dealing with a lot of traffic.

3. Test The IDS: Test the system to ensure it detects the potential threats and responds to them properly. Use test datasets or have security professionals do a pen test.

Conclusion:

Keeping in mind the challenges of ongoing system monitoring, maintenance, and alert investigation, many organizations wish to consider having secure network-based intrusion detection systems. A managed IDS service avoids recruiting a dedicated security person and sometimes includes the requisite technology, minimizing the need to maintain capital expenditure.

1. How Do Intrusion Detectors Work?

An intrusion detection system in information security works by scanning the forwarded traffic to detect any malicious activities and known attack patterns.

2. What Are The Major Components Of An Intrusion Detection System?

1. Audit data processor
2. Knowledge base
3. Decision engine
4. Alarm generation
5. Responses

3. What Are The Sensors Used In IDS?

The common application of intrusion detection systems and sensors used are magnetic switches, glass-break sensors, internal monocratic sensors, video motion detectors, glass-break sensors, PIR and microwave sensors, and others in combination.

4. Why Do We Need An Intrusion Detection System?

An IDS or a protocol intrusion detection system gives companies greater visibility across their network, allowing them to meet security regulations.

5. What Is A Perimeter Intrusion Detection System?

A perimeter intrusion detection system uses physical and software technology systems to protect users from unauthorized access and intrusion.

INTRUSION PREVENTION SYSTEM

Intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity. Major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it and attempt to block or stop it.

Intrusion prevention systems are contemplated as augmentation of Intrusion Detection Systems (IDS) because both IPS and IDS operate network traffic and system activities for malicious activity.
IPS typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IPS can also respond to a detected threat by attempting to prevent it from succeeding. They use various response techniques, which involve the IPS stopping the attack itself, changing the security environment or changing the attack's content.

How Does an IPS Work?
An IPS works by analyzing network traffic in real-time and comparing it against known attack patterns and signatures. When the system detects suspicious traffic, it blocks it from entering the network.

Types of IPS
There are two main types of IPS:

1. **Network-Based IPS:** A Network-Based IPS is installed at the network perimeter and monitors all traffic that enters and exits the network.
2. **Host-Based IPS:** A Host-Based IPS is installed on individual hosts and monitors the traffic that goes in and out of that host.

Why Do You Need an IPS?
An IPS is an essential tool for network security. Here are some reasons why:

- Protection against Known and Unknown Threats: An IPS can block known threats and also detect and block unknown threats that haven't been seen before.
- Real-Time Protection: An IPS can detect and block malicious traffic in real-time, preventing attacks from doing any damage.
- Compliance Requirements: Many industries have regulations that require the use of an IPS to protect sensitive information and prevent data breaches.
- Cost-Effective: An IPS is a cost-effective way to protect your network compared to the cost of dealing with the aftermath of a security breach.
- Increased Network Visibility: An IPS provides increased network visibility, allowing you to see what's happening on your network and identify potential security risks.

Classification of Intrusion Prevention System (IPS):
Intrusion Prevention System (IPS) is classified into 4 types:

1. **Network-based intrusion prevention system (NIPS):**
   It monitors the entire network for suspicious traffic by analyzing protocol activity.

2. **Wireless intrusion prevention system (WIPS):**
   It monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.

3. **Network behavior analysis (NBA):**
   It examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, specific forms of malware and policy violations.

4. **Host-based intrusion prevention system (HIPS):**
   It is an inbuilt software package which operates a single host for doubtful activity by scanning events that occur within that host.

Comparison of Intrusion Prevention System (IPS) Technologies:
The Table below indicates various kinds of IPS Technologies:

IPS Technology Type	Types of Malicious Activity Detected	Scope per Sensor	Strengths
Network-Based	Network, transport, and application TCP/IP layer activity	Multiple network subnets and groups of hosts	Only IDPS which can analyze the widest range of application protocols;
Wireless	Wireless protocol activity; unauthorized wireless local area networks (WLAN) in use	Multiple WLANs and groups of wireless clients	Only IDPS able to predict wireless protocol activity
NBA	Network, transport, and application TCP/IP layer activity that causes anomalous network flows	Multiple network subnets and groups of hosts	Typically more effective than the others at identifying reconnaissance scanning and DoS attacks, and at reconstructing

			major malware infections
Host-Based	Host application and operating system (OS) activity; network, transport, and application TCP/IP layer activity	Individual host	Can analyze activity that was transferred in end-to-end encrypted communications

Detection Method of Intrusion Prevention System (IPS):

1. **Signature-based detection:**
   Signature-based IDS operates packets in the network and compares with pre-built and preordained attack patterns known as signatures.

2. **Statistical anomaly-based detection:**
   Anomaly based IDS monitors' network traffic and compares it against an established baseline. The baseline will identify what is normal for that network and what protocols are used. However, It may raise a false alarm if the baselines are not intelligently configured.

3. **State protocol analysis detection:**
   This IDS method recognizes divergence of protocols stated by comparing observed events with pre-built profiles of generally accepted definitions of not harmful activity.

Comparison of IPS with IDS:

The main difference between Intrusion Prevention System (IPS) with Intrusion Detection Systems (IDS) are:

1. Intrusion prevention systems are placed in-line and are able to actively prevent or block intrusions that are detected.
2. IPS can take such actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address.
3. IPS also can correct cyclic redundancy check (CRC) errors, defragment packet streams, mitigate TCP sequencing issues and clean up unwanted transport and network layer options.

Conclusion:

An Intrusion Prevention System (IPS) is a crucial component of any network security strategy. It monitors network traffic in real-time, compares it against known attack patterns and signatures, and blocks any malicious activity or traffic that violates network policies. An IPS is an essential tool for protecting against known and unknown threats, complying with industry

regulations, and increasing network visibility. Consider implementing an IPS to protect your network and prevent security breaches.