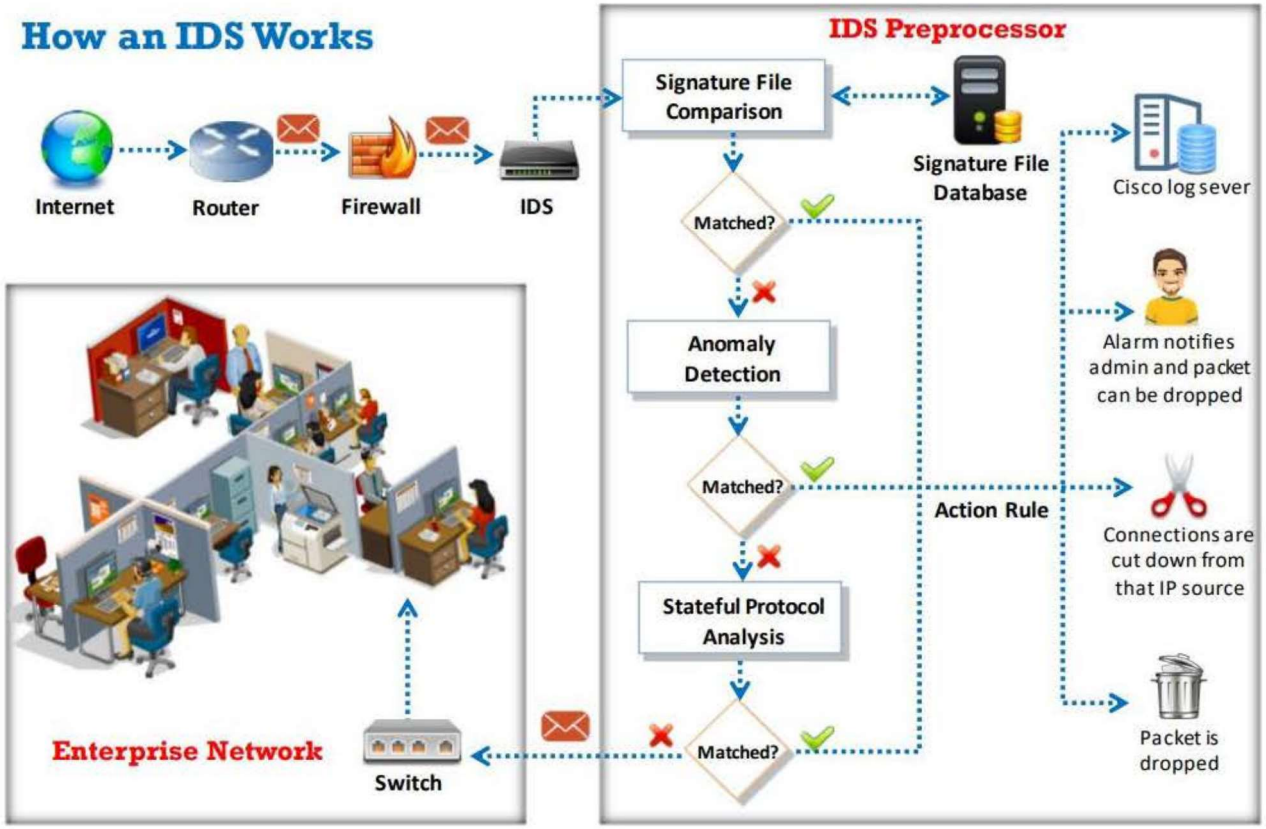
Intrusion Detection System (IDS)

- An intrusion detection system (IDS) is a software system or hardware device that **inspects all inbound and outbound network traffic** for suspicious patterns that may indicate a network or system security breach
- The IDS **checks traffic** for signatures that match known intrusion patterns and **signals an alarm** when a match is found
- Depending on the traffic to be monitored, the IDS is placed **outside/inside the firewall** to monitor suspicious traffic originating from outside/inside the network



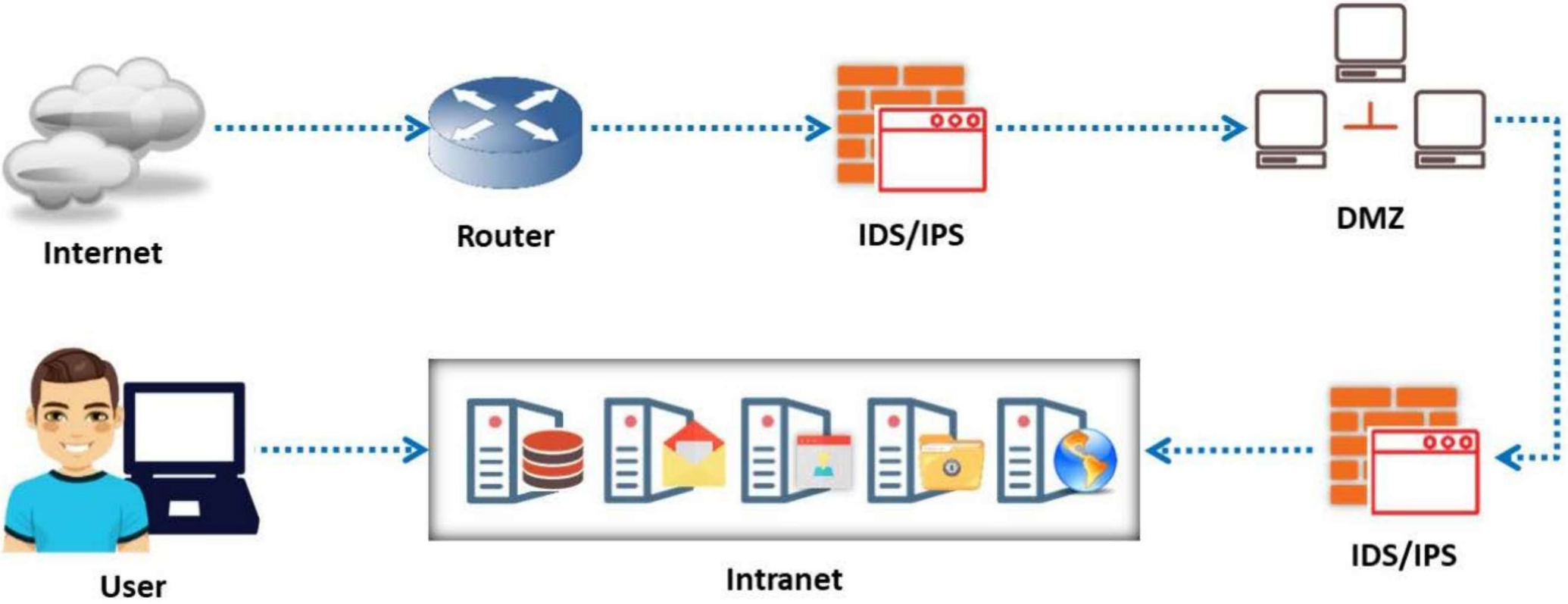


Figure 12.1: Placement of IDS

How an IDS Detects an Intrusion?

Signature Recognition	Signature recognition, also known as misuse detection, tries to **identify events** that indicate an abuse of a system or network resource
Anomaly Detection	It detects the **intrusion based** on the fixed behavioral characteristics of the users and components in a computer system
Protocol Anomaly Detection	In this type of detection, models are built to explore **anomalies** in the way in which vendors deploy the **TCP/IP specification**

General Indications of Intrusions

File System Intrusions

- The presence of new or **unfamiliar files**, or programs
- Changes in **file permissions**
- Unexplained changes in a file's **size**
- **Rogue files** on the system that do not correspond to the master list of signed files
- Missing files

Network Intrusions

- **Repeated probes** of the available services on your machines
- Connections from **unusual locations**
- Repeated login attempts from **remote hosts**
- A sudden **influx of log data**

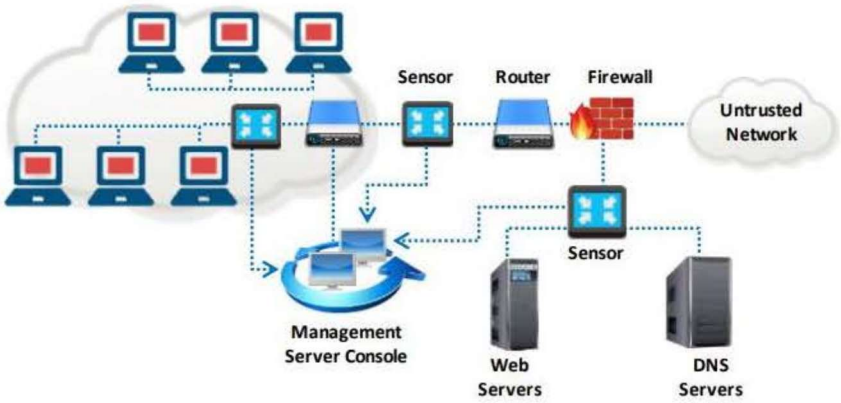
System Intrusions

- **Short** or incomplete logs
- Unusually **slow** system performance
- **Missing** logs or logs with incorrect permissions or ownership
- **Modifications** to system software and configuration files
- Unusual **graphic displays** or text messages
- **Gaps** in system accounting
- System crashes or **reboots**
- **Unfamiliar** processes

Types of Intrusion Detection Systems

Network-Based Intrusion Detection Systems

- These systems typically consist of a **black box** that is placed on the network in a promiscuous mode, listening for patterns indicative of an intrusion
- It detects malicious activity such as **Denial-of-Service attacks**, port scans, or even attempts to crack into computers by monitoring network traffic



Host-Based Intrusion Detection Systems

- These systems usually include auditing for events that occur on a **specific host**
- These are not as common, due to the overhead they incur by having to **monitor each system event**

Types of IDS Alerts

True Positive (Attack - Alert)	An IDS raises an alarm when a **legitimate attack** occurs
False Positive (No Attack - Alert)	An IDS raises an alarm when **no attack** has taken place
False Negative (Attack - No Alert)	An IDS does not raise an alarm when a **legitimate attack** has taken place
True Negative (No Attack - No Alert)	An IDS does not raise an alarm when an **attack** has not taken place