IPS (Intrusion Prevention System)

&

IDS (Intrusion Detection System)

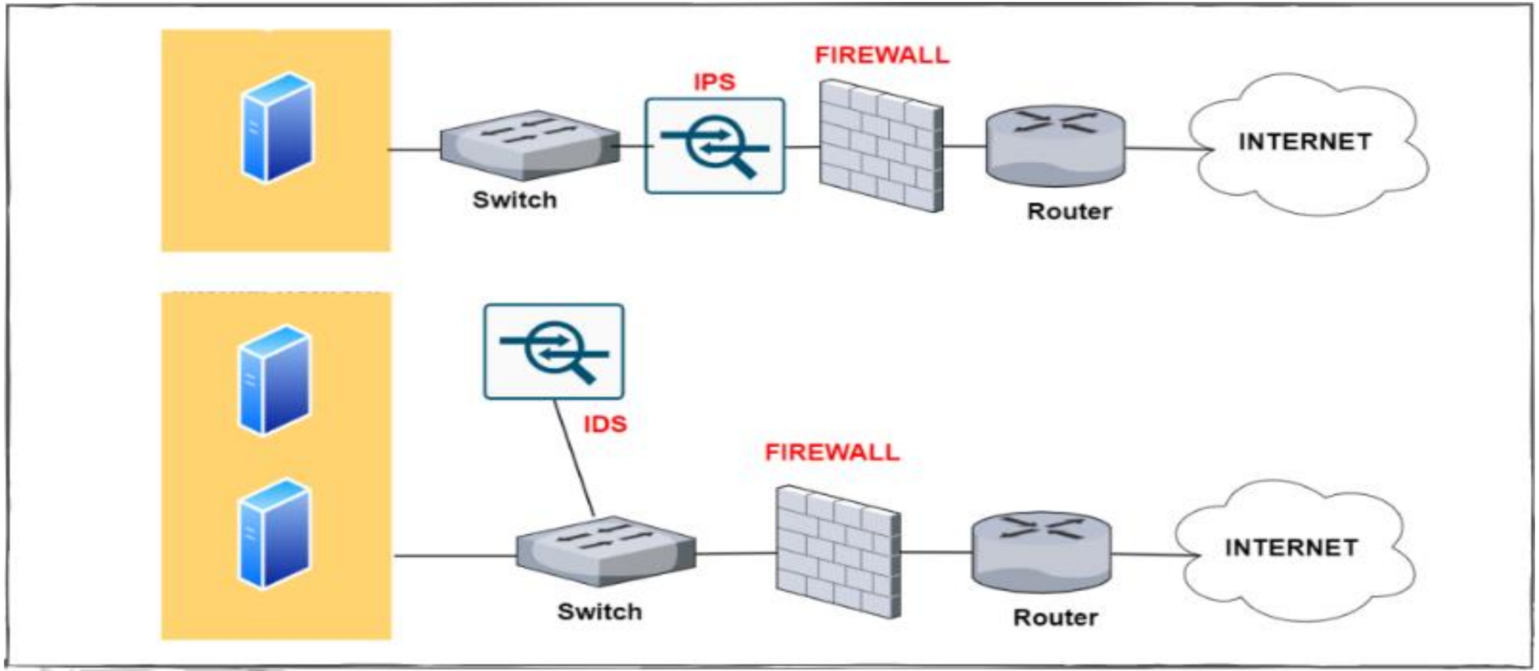
Cyber Security Foundation Course

AGENDA

- Definition
- How IPS\IDS Work
- IPS VS IDS

IPS\IDS Definition

intrusion detection systems (IDS) and intrusion prevention systems (IPS) is a layer 7 Device that constantly watch the network Traffic, identifying possible Attacks or any malicious activities attempting to exploit a known vulnerability., stopping the incidents, and reporting them to security administrators..

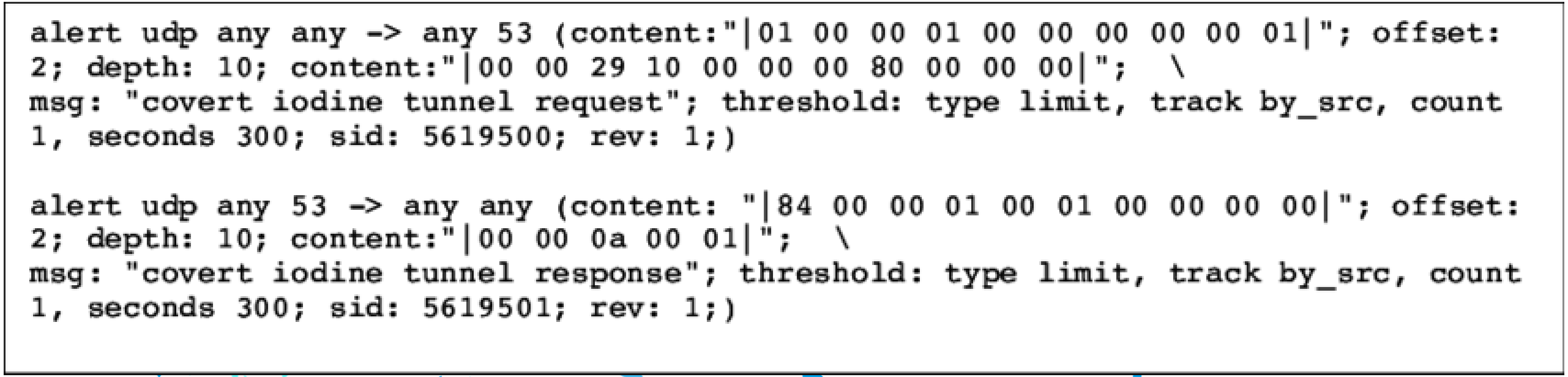


How IPS\IDS Work

- Signature-Based Detection compares signatures against observed events to identify possible incidents. This is the simplest detection method because it compares only the current unit of activity (such as a packet or a log entry, to a list of signatures) using string comparison operations.

- Anomaly-Based Detection compares definitions of what is considered normal activity with observed events in order to identify significant deviations. This detection method can be very effective at spotting previously unknown threats.

- Stateful Protocol Analysis compares predetermined profiles of generally accepted definitions for benign protocol activity for each protocol state against observed events in order to identify deviations.



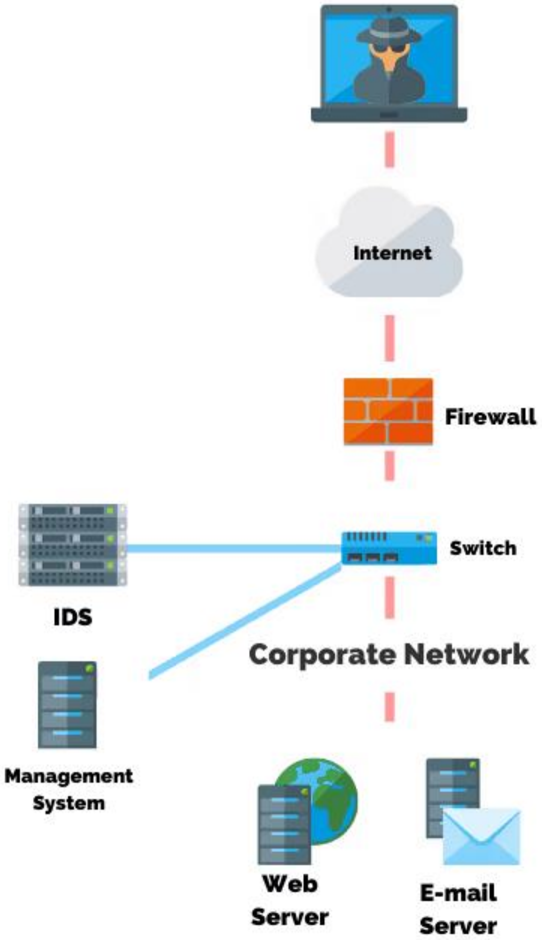
```
alert udp any any -> any 53 (content:"|01 00 00 01 00 00 00 00 00 01|"; offset:
2; depth: 10; content:"|00 00 29 10 00 00 00 80 00 00 00|";  \
msg: "covert iodine tunnel request"; threshold: type limit, track by_src, count
1, seconds 300; sid: 5619500; rev: 1;)

alert udp any 53 -> any any (content: "|84 00 00 01 00 01 00 00 00 00|"; offset:
2; depth: 10; content:"|00 00 0a 00 01|";  \
msg: "covert iodine tunnel response"; threshold: type limit, track by_src, count
1, seconds 300; sid: 5619501; rev: 1;)
```

IPS Vs IDS

	IPS	IDS
Device Action	Prevent Attacks(Take Action and Send Alert)	Detect Attacks(just send alert)
Design	Inline to data communication	Out of band from data communication(Port mirroring or SPAN Port)
Network performance impact	Slow down network performance due to delay caused by inline IPS processing	Does not impact network performance due to non-line deployment of IDS.

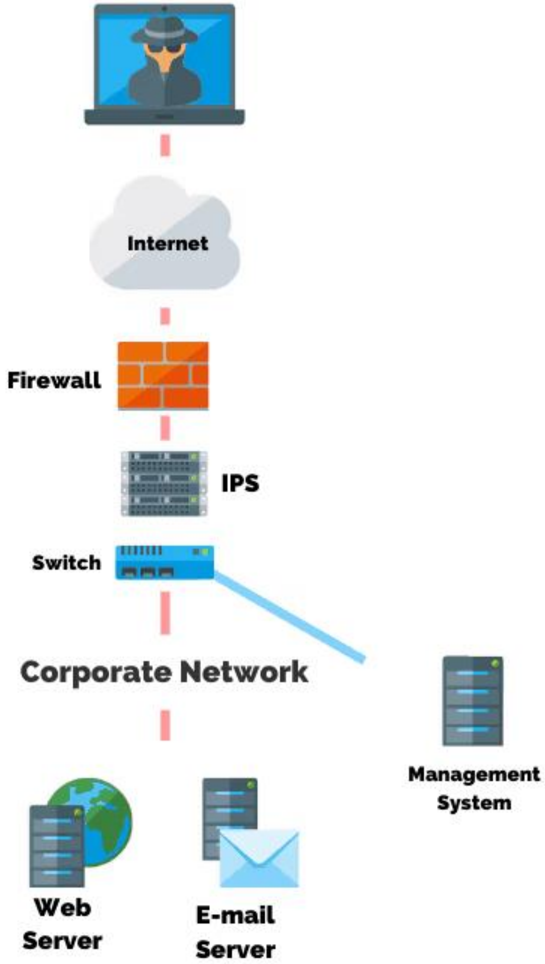
Port mirroring (SPAN Port): is a method of monitoring network traffic. With port mirroring enabled, the switch sends a copy of all network packets seen on one port

Intrusion Detection System (IDS)



VS

Intrusion Prevention System (IPS)



Thanks!

Any questions?