Course 4 Week 1.

Introduction to the TCP/IP Protocol Framework

Stateless Inspection → it does not have a Session table.

- Each packet is inspected one at a time

Browers → TCP Stateless Inspection use Case

→ To protect routing engine resources
→ To control traffic going in or your organization
→ For troubleshooting purposes
→ To control traffic routing
→ To perform QoS/LoS.

Stateful Inspection → has a session IP

Session ID consists of [illegible]
exchanged between parties
during an exchange.

→ Sessions have a number of elemen
→ Source IP addresses
→ the destination IP addres
→ the sorce port
→ identifier.

Firewall Filters → IDS and IPS.
protection
detection

- Intrusion Detection Systems ⇒ An Intrusion Detection System is a network security technology originally built for detecting vulnerability exploits against a targeted application or computer.

→ IPS is a listen-only device.

→ IPS monitors traffic and reports its result to an administrator.

→ Cannot automatically take action

to prevent a detected exploit from taking over the system.

Intrusion Prevention System → is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.

→ It sits directly behind the firewall & active listener.

How does IDS & IPS detect threat?

→ Signature – Based
→ Anomaly – Based
→ Host – Based
→ Network – based

The difference between IPS vs IDS.

Placement of network	IPS	IDS
	direct line of	outside

System type

Detection Mechanism

- Communication. Active
- line of comm (offline) Passive
- 1.) Statistically Anamoly-Based
- Anamoly Based
- 2) Signature detection.

NAT → Network Address translation

→ Remapping one IP Address space into another

→ Additional layer of security

→ Uses different IP from organization.

Nat Gateway for private network.

Types of NAT

Static → Allows one-to-one mapping between local & global

addresses

Dynamic → Address Translation : Maps unregistered IP addresses to registered IP address.

Overloading :

Network Protocols over Ethernet or Local Area Network.

Ethernet bridges has 3 main Fnc

- Forwarding Frame
- Learning MAC Address
- Controlling Traffic.

Layer 2 and Layer 3 Network Addressing.

↳ Matches upon IP