

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

Browsers → TCP Stateless Inspection use case

→ To protect routing engine resources

→ To control traffic going in or out of your organization

→ For troubleshooting purposes

→ To control traffic routing

→ To perform QoS/LOS.

Stateful Inspection → has a session table

→ inspects all packets

Session ID consists of an identifier exchanged between parties during an exchange.

→ Sessions have a number of elements:

→ Source IP addresses

→ the destination IP address

→ the source port

→ Identifier.

Firewall Filter → IDS and IPS.
detection protection.

~ Intrusion Detection Systems → An Intrusion

Detection System is a network security technology originally built for detecting vulnerability exploits against a target application or computer.

→ IDS is a listen-only device.

→ IDS monitors traffic and reports its results 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
- Mailbox-based

The difference between IPS vs IDS.

	IPS	IDS
Placement of Network	direct line of	passive device

System type	Communication	
	Active	Passive
Detection Mechanism	1.) Statistically Anomaly-Based 2.) Signature detection	Anomaly Based.

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 addresses.

Overloading :

Network Protocols over Ethernet &
Local Area Network.

Ethernet bridges has 3 main
Func

- Forwarding Frame
- Learning MAC Addresses
- Controlling Traffic.

Layer 2 and Layer 3 Network
Addressing-
↳ Matches origin IP