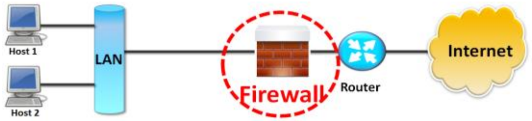
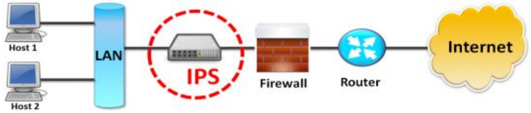
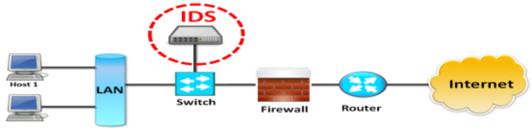
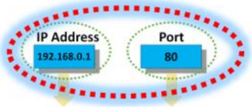
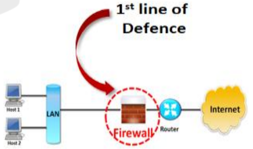
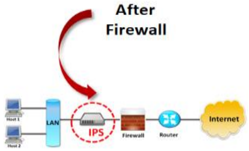
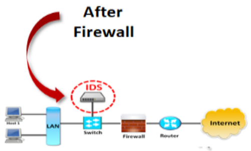
IDS vs IPS vs Firewall

Parameter	FIREWALL	IPS	IDS
	 	 Host 1 Host 2 LAN IPS Firewall Router Internet	 IDS Host 1 Host 2 LAN Switch Firewall Router Internet
Abbreviation For	-	Intrusion Prevention System	Intrusion Detection System
Philosophy	Firewall is a network security device that filters incoming and outgoing network traffic based on predetermined rules	IPS is a device that inspects traffic, detects it, classifies and then proactively stops malicious traffic from attack.	An intrusion detection system (IDS) is a device or software application that monitors a traffic for malicious activity or policy violations and sends alert on detection.
Principle Of Working	Filters traffic based on IP address and port numbers  	Inspects real time traffic and looks for traffic patterns or signatures of attack and then prevents the attacks on detection. Prevents Attacks	Detects real time traffic and looks for traffic patterns or signatures of attack and them generates alerts. Generate Alarms
Configuration Mode	Layer 3 mode or transparent mode	Inline mode , generally being in layer 2	Inline or as end host (via span) for monitoring and detection
Placement	Inline at the Perimeter of Network	Inline generally after Firewall	Non-Inline through port span (or via tap)
Traffic Patterns	Not analyzed	Analyzed	Analyzed
Placement w.r.t Each Other	Should be 1st Line of defense  1st line of Defence LAN Firewall Router Internet	Should be placed after the Firewall device in network  After Firewall LAN IPS Firewall Router Internet	Should be placed after firewall 
Action On Unauthorized Traffic Detection	Block the traffic	Preventing the traffic on Detection of anomaly	Alerts/alarms on detection of anomaly
Related Terminologies	• Stateful packet filtering • permits and blocks traffic by port/protocol rules	• Anomaly based detection • Signature detection • Zero day attacks • Blocking the attack	• Anomaly based detection • Signature detection • Zero day attacks • Monitoring • Alarm

https://ipwithease.com