Cyber Security

Firewalls

2023

NAZGUL ABDINUROVA

SULEYMAN DEMIREL UNIVERSITY

Firewalls - Cyberops

A firewall is a system, or group of systems, that enforces an access control policy between networks. All firewalls share some common properties:

- Firewalls are resistant to network attacks.
- Firewalls are the only transit point between internal corporate networks and external networks because all traffic flows through the firewall.
- Firewalls enforce the access control policy.

Benefits of a firewall

There are several benefits of using a firewall in a network:

- They prevent the exposure of sensitive hosts, resources, and applications to untrusted users.
- They sanitize protocol flow, which prevents the exploitation of protocol flaws.
- They block malicious data from servers and clients.
- They reduce security management complexity by off-loading most of the network access control to a few firewalls in the network.

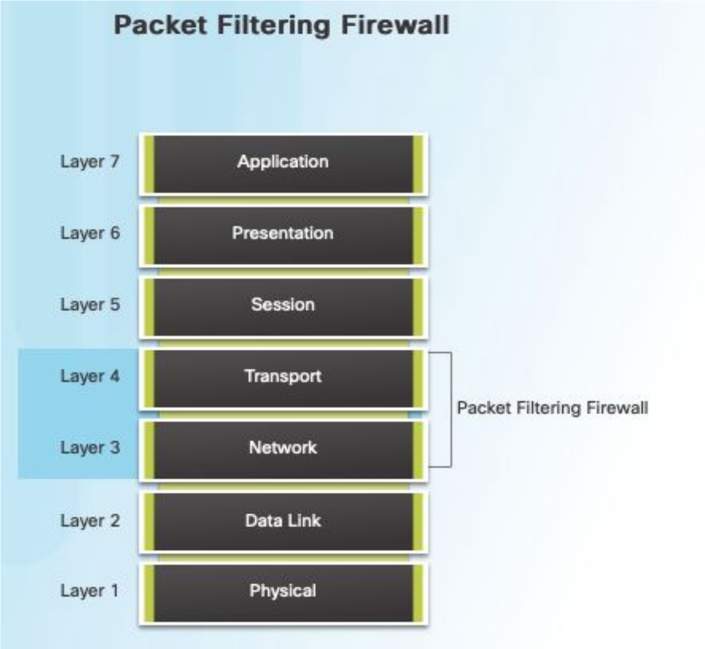
Firewalls - Cyberops

Firewalls also present some limitations:

- A misconfigured firewall can have serious consequences for the network, such as becoming a single point of failure.
- The data from many applications cannot be passed over firewalls securely.
- Users might proactively search for ways around the firewall to receive blocked material, which exposes the network to potential attack.
- Network performance can slow down.
- Unauthorized traffic can be tunneled or hidden as legitimate traffic through the firewall.

Firewall type descriptions

Packet filtering (stateless) firewall - Typically a router with the capability to filter some packet content, such as Layer 3 and sometimes Layer 4 information according to a set of configured rules

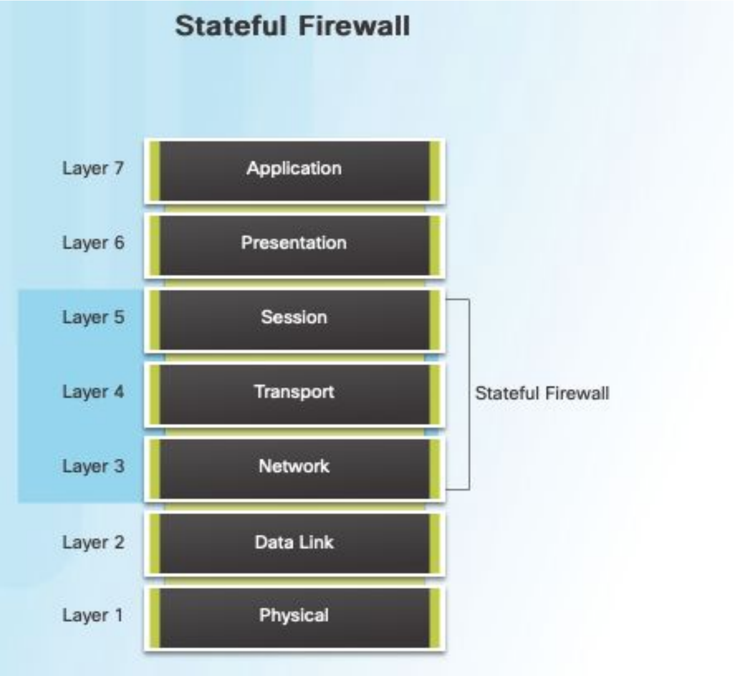


Packet filtering firewall

Packet filtering firewalls are usually part of a router firewall, which permits or denies traffic based on Layer 3 and Layer 4 information. They are stateless firewalls that use a simple policy table look-up that filters traffic based on specific criteria, as shown in the figure. For example, SMTP servers listen to port 25 by default. An administrator can configure the packet filtering firewall to block port 25 from a specific workstation to prevent it from broadcasting an email virus.

Firewall type descriptions

Stateful firewall - A stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection

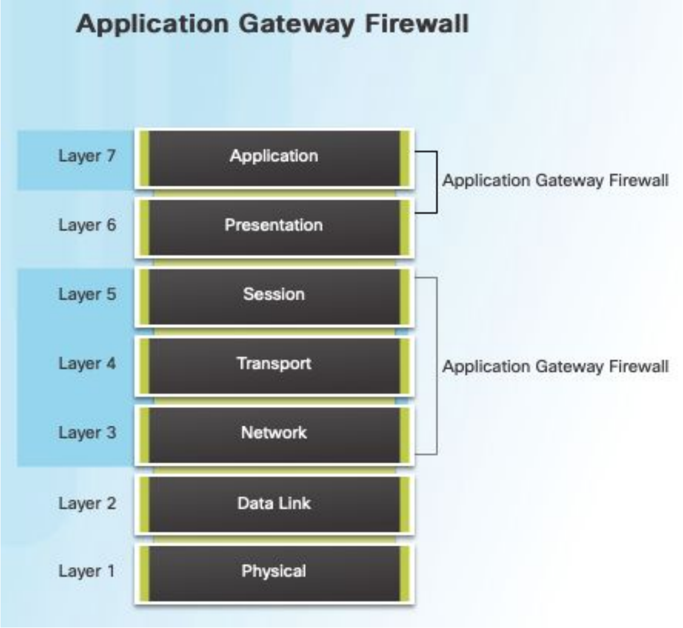


Stateful firewall

Stateful firewalls are the most versatile and the most common firewall technologies in use. Stateful firewalls provide stateful packet filtering by using connection information maintained in a state table. Stateful filtering is a firewall architecture that is classified at the network layer. It also analyzes traffic at OSI Layer 4 and Layer 5, as shown in the figure.

Firewall type descriptions

Application gateway firewall (proxy firewall) – Filters information at Layers 3, 4, 5, and 7 of the OSI reference model. Most of the firewall control and filtering is done in software. When a client needs to access a remote server, it connects to a proxy server. The proxy server connects to the remote server on behalf of the client. Therefore, the server only sees a connection from the proxy server



Other methods of implementing firewalls

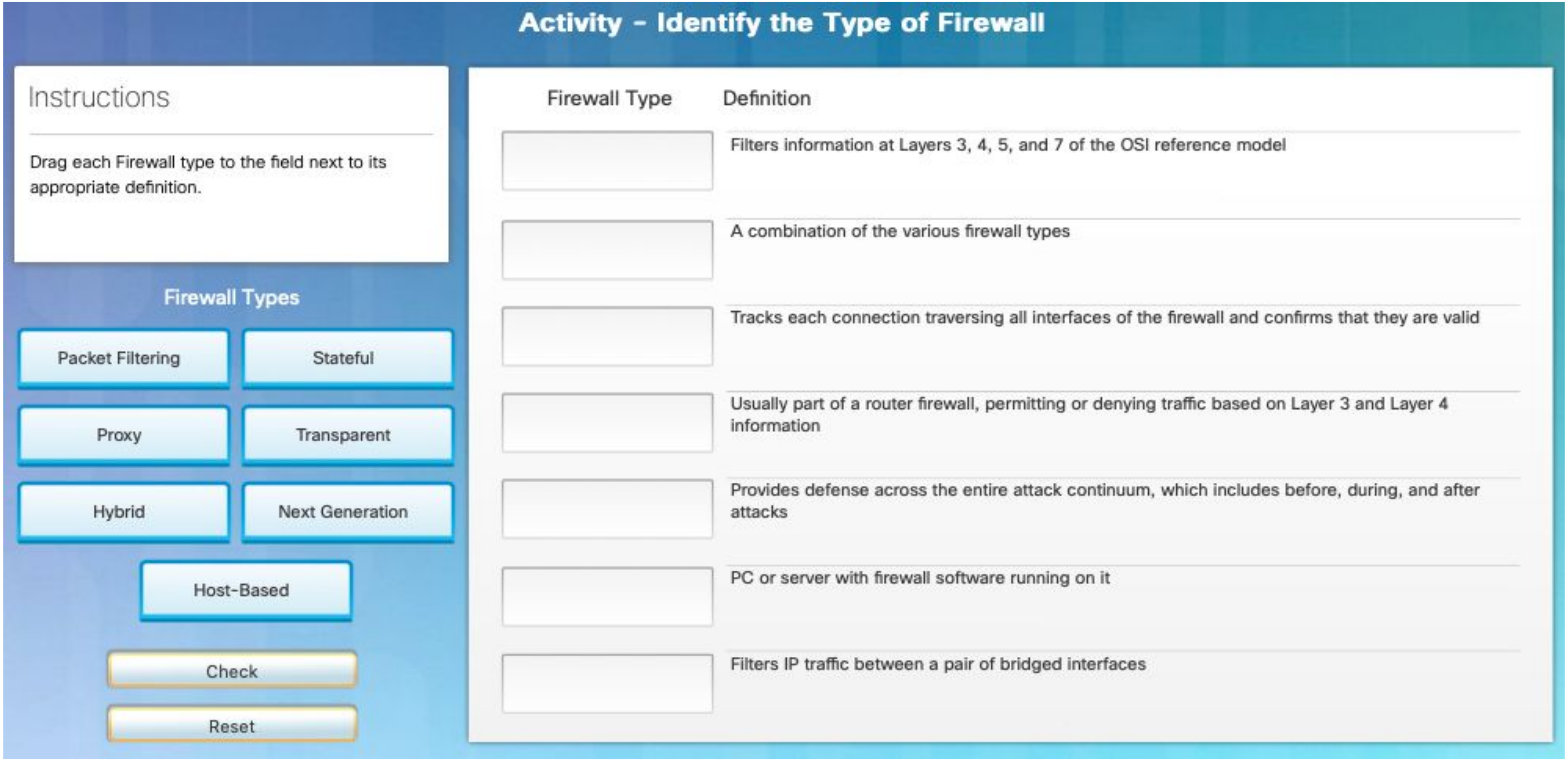
- **Host-based (server and personal) firewall** - A PC or server with firewall software running on it.
- **Transparent firewall** - Filters IP traffic between a pair of bridged interfaces.
- **Hybrid firewall** - A combination of the various firewall types. For example, an application inspection firewall combines a stateful firewall with an application gateway firewall.

Next generation firewall

Next-generation firewalls go beyond stateful firewalls by providing:

- **Standard firewall capabilities like stateful inspection**
- **Integrated intrusion prevention**
- **Application awareness and control to see and block risky apps**
- **Upgrade paths to include future information feeds**
- **Techniques to address evolving security threats**

Task for 5 minutes

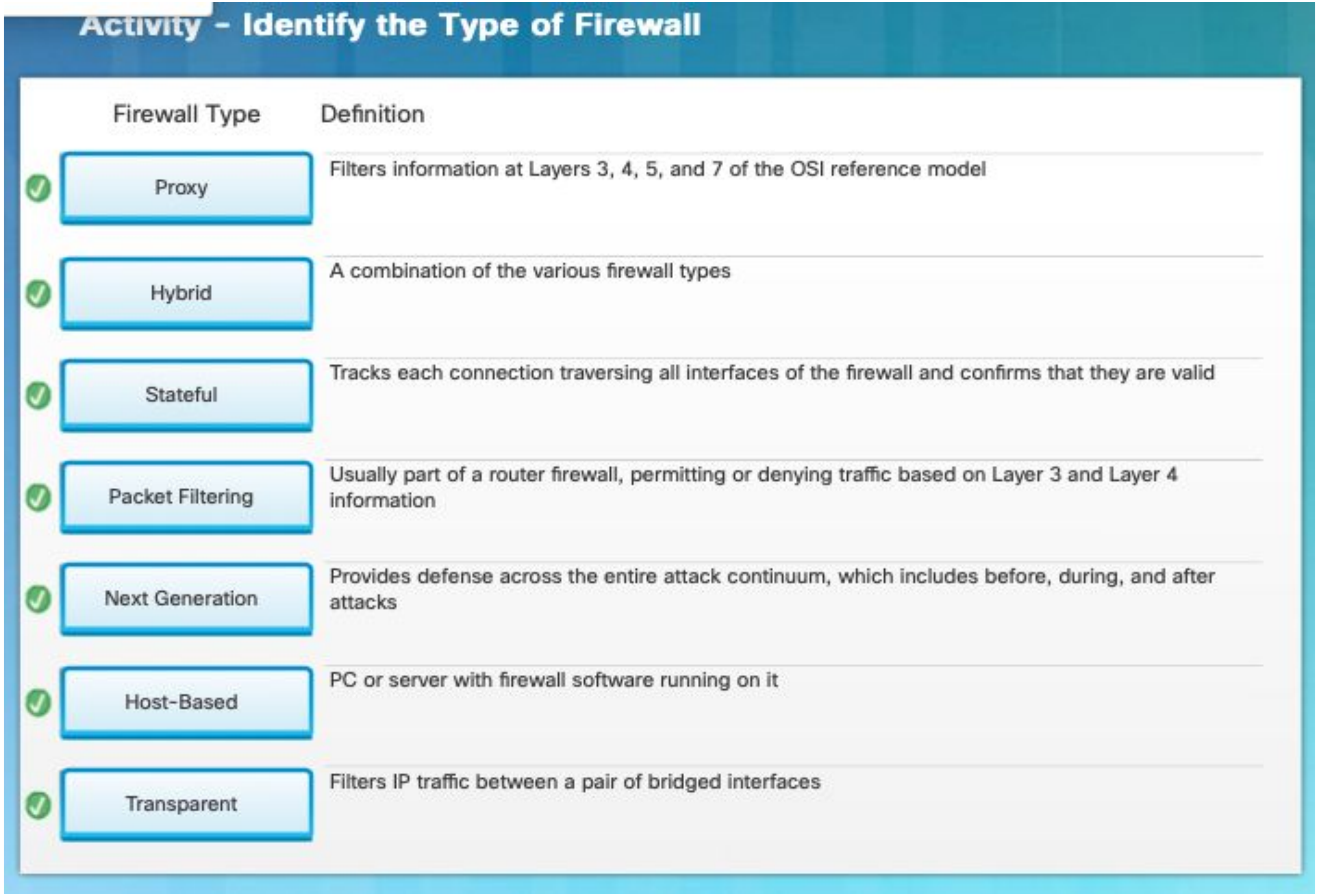


Activity - Identify the Type of Firewall

Instructions

Drag each Firewall type to the field next to its appropriate definition.

Firewall Type	Definition
	Filters information at Layers 3, 4, 5, and 7 of the OSI reference model
	A combination of the various firewall types
	Tracks each connection traversing all interfaces of the firewall and confirms that they are valid
	Usually part of a router firewall, permitting or denying traffic based on Layer 3 and Layer 4 information
	Provides defense across the entire attack continuum, which includes before, during, and after attacks
	PC or server with firewall software running on it
	Filters IP traffic between a pair of bridged interfaces



Activity - Identify the Type of Firewall

	Firewall Type	Definition
✓	Proxy	Filters information at Layers 3, 4, 5, and 7 of the OSI reference model
✓	Hybrid	A combination of the various firewall types
✓	Stateful	Tracks each connection traversing all interfaces of the firewall and confirms that they are valid
✓	Packet Filtering	Usually part of a router firewall, permitting or denying traffic based on Layer 3 and Layer 4 information
✓	Next Generation	Provides defense across the entire attack continuum, which includes before, during, and after attacks
✓	Host-Based	PC or server with firewall software running on it
✓	Transparent	Filters IP traffic between a pair of bridged interfaces

IPS/IDS

- Snort
- Surricata
- Zeek
- *too expensive(~$98k)

Cyberops: Intrusion Prevention and Detection Devices

A networking architecture paradigm shift is required to defend against fast-moving and evolving attacks. This must include cost-effective detection and prevention systems, such as intrusion detection systems (IDS) or the more scalable intrusion prevention systems (IPS). The network architecture integrates these solutions into the entry and exit points of the network.

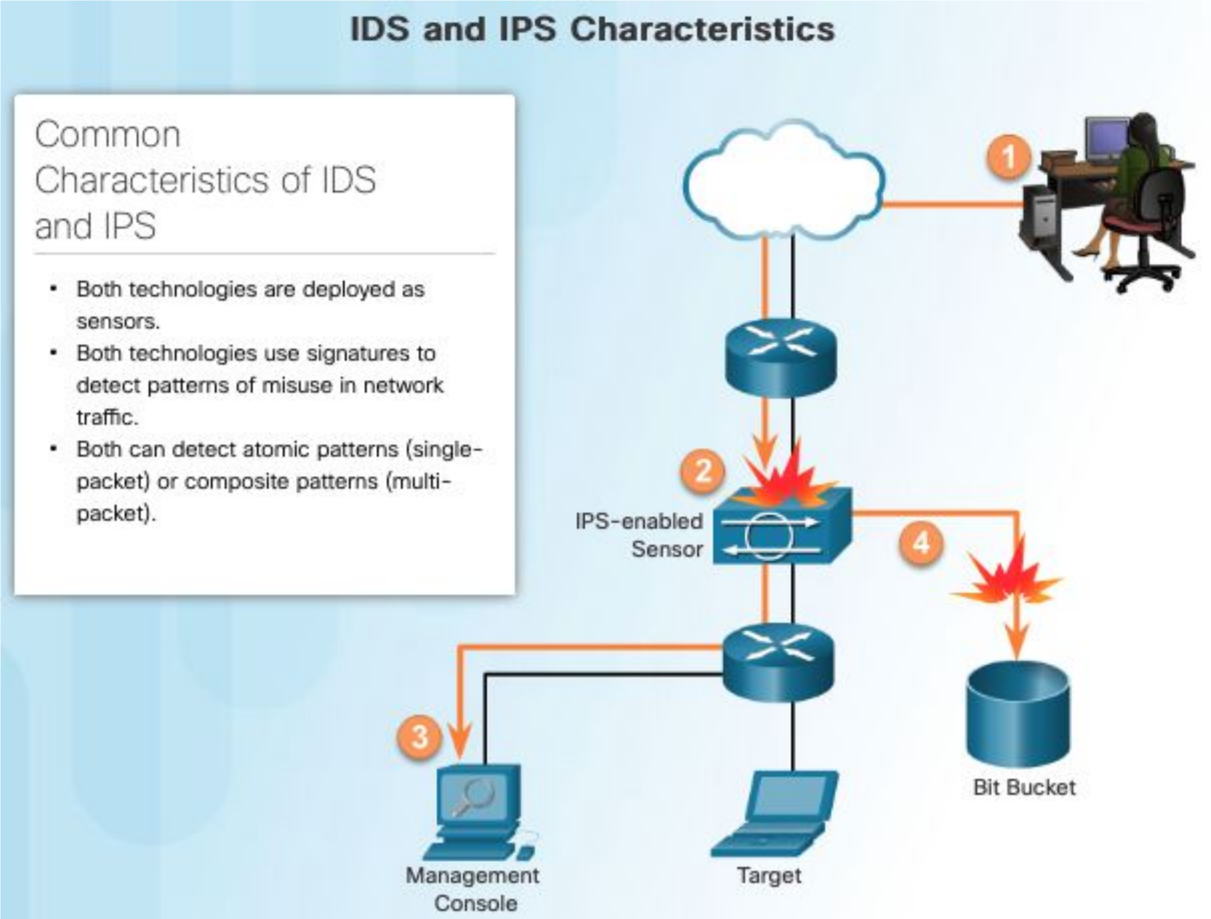
When implementing IDS or IPS, it is important to be familiar with the types of systems available, host-based and network-based approaches, the placement of these systems, the role of signature categories, and possible actions that a Cisco IOS router can take when an attack is detected.

Cyberops: Intrusion Prevention and Detection Devices

IDS and IPS technologies share several characteristics, as shown in the figure. IDS and IPS technologies are both deployed as sensors. An IDS or IPS sensor can be in the form of several different devices:

- A router configured with Cisco IOS IPS software
- A device specifically designed to provide dedicated IDS or IPS services
- A network module installed in an adaptive security appliance (ASA), switch, or router

IDS and IPS technologies use signatures to detect patterns in network traffic. A signature is a set of rules that an IDS or IPS uses to detect malicious activity. Signatures can be used to detect severe breaches of security, to detect common network attacks, and to gather information. IDS and IPS technologies can detect atomic signature patterns (single-packet) or composite signature patterns (multi-packet).

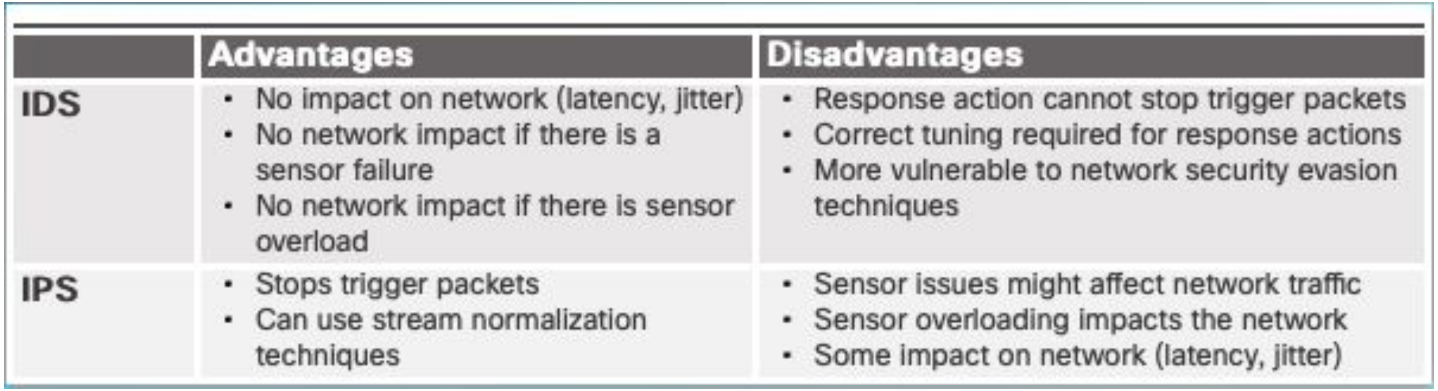


IDS and IPS Characteristics

Common Characteristics of IDS and IPS

- Both technologies are deployed as sensors.
- Both technologies use signatures to detect patterns of misuse in network traffic.
- Both can detect atomic patterns (single-packet) or composite patterns (multi-packet).

Comparing IDS and IPS Solutions



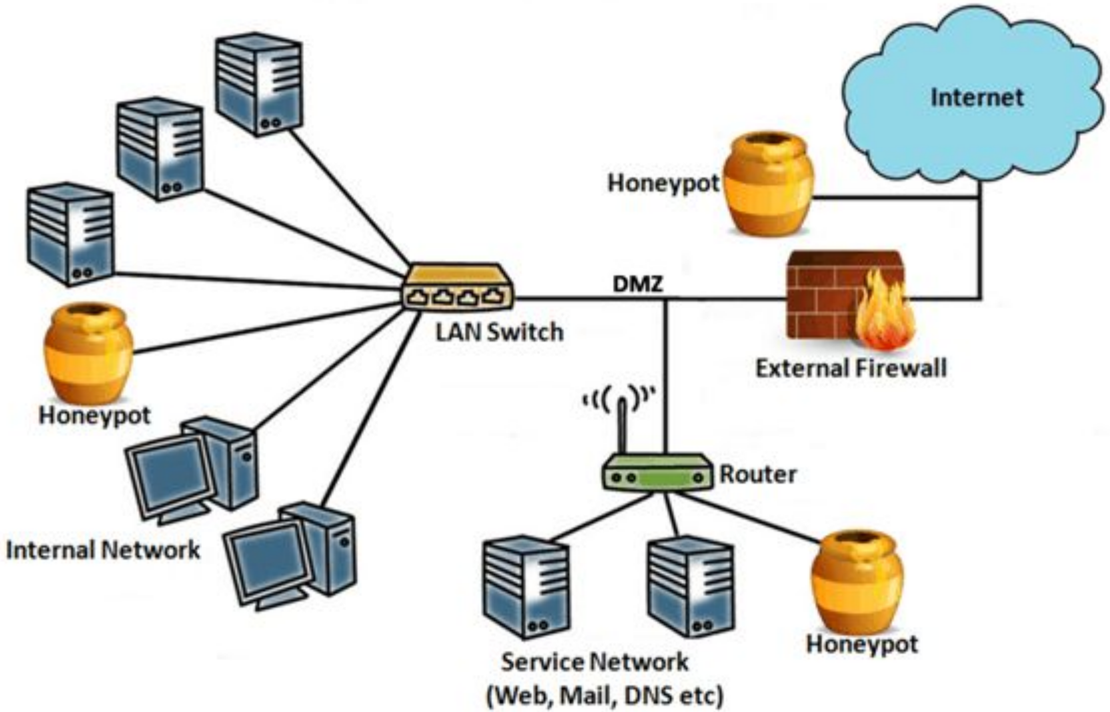
	Advantages	Disadvantages
IDS	• No impact on network (latency, jitter) • No network impact if there is a sensor failure • No network impact if there is sensor overload	• Response action cannot stop trigger packets • Correct tuning required for response actions • More vulnerable to network security evasion techniques
IPS	• Stops trigger packets • Can use stream normalization techniques	• Sensor issues might affect network traffic • Sensor overloading impacts the network • Some impact on network (latency, jitter)

Honeypots

A honeypot is a computer or computer system intended to mimic likely targets of cyber attacks. It can be used to detect attacks or deflect them from a legitimate target. It can also be used to gain information about how cyber criminals operate.

You may not have heard of them before, but honeypots have been around for decades. The principle behind them is simple: Don’t go looking for attackers. Prepare something that would attract their interest — the honeypot — and then wait for the attackers to show up.

Like mice to cheese-baited mouse traps, cybercriminals are attracted to honeypots — not because they’re honeypots. The bad guys think the honeypot is a legitimate target, something worthy of their time. That’s because the bait includes applications and data that simulate a real computer system.


Internet
Honeypot
DMZ
LAN Switch
External Firewall
Honeypot
Router
Internal Network
Service Network
(Web, Mail, DNS etc)
Honeypot

How do honeypots work?

If you, for instance, were in charge of IT security for a bank, you might set up a honeypot system that, to outsiders, looks like the bank’s network. The same goes for those in charge of — or researching — other types of secure, internet-connected systems.

By monitoring traffic to such systems, you can better understand where cybercriminals are coming from, how they operate, and what they want. More importantly, you can determine which security measures you have in place are working — and which ones may need improvement.

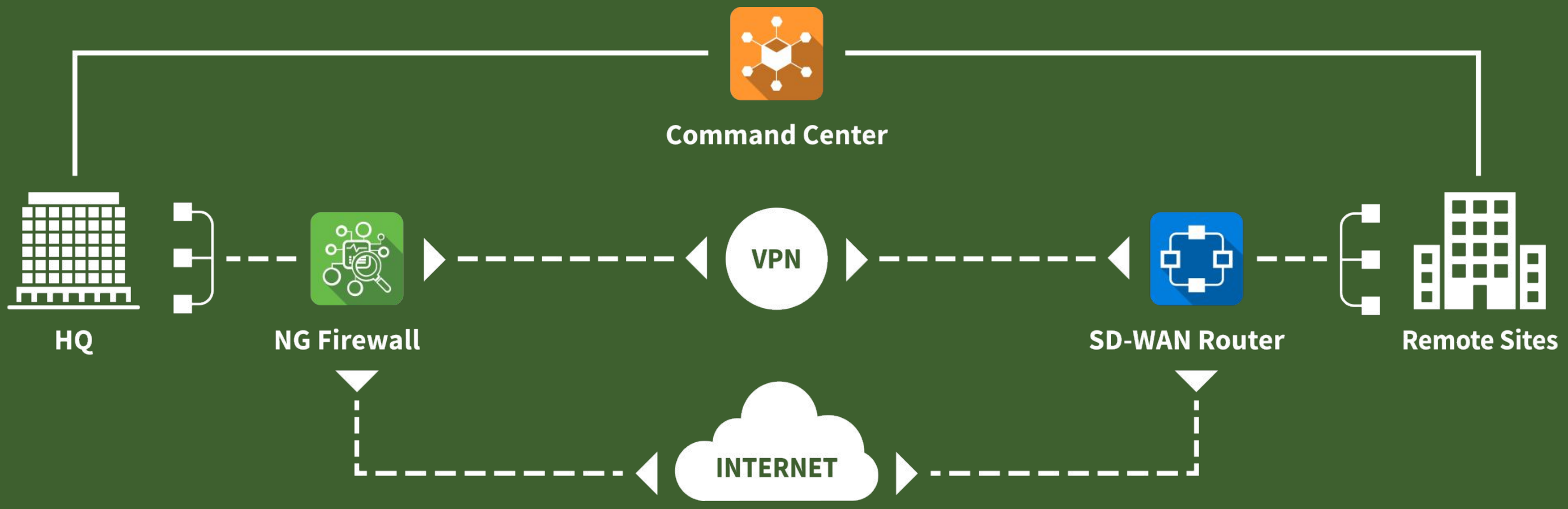
PRACTICAL PART

Firewall

- iptables - administration tool for IPv4 packet filtering and NAT (link for more info)
- Firewalld CentOS
- ufw(ubuntu), example allow/deny

Untangle

Untangle NG Firewall is a Debian-based network gateway with pluggable modules for network applications like spam blocking, web filtering, anti-virus, anti-spyware, intrusion prevention, VPN, SSL VPN, firewall, and more.



WAF - Web Application Firewall

A WAF creates a shield between a web app and the Internet; this shield can help mitigate many common attacks.(cloudflare)

WAF - Web Application Firewall

1. Free, open-source:

- Apache + modsecurity

apt-get install libapache2-mod-security2

/etc/apache2/sites-available/000-default.conf

SecRule on (no sql injection)

WAF - Web Application Firewall

2. Proprietary + expensive:

- Imperva WAF
- Nemesida AI
- PT AF

3. Proprietary + not expensive:

- Cloudflare WAF
- WebTotem
- Sucuri

Honeypots

1. ssh honeypot (collect bruteforce db)
2. https://github.com/internetwache/SSH-Honeypot

   Keygen, ssh

3. wordpress honeypot
   https://github.com/gbrindisi/wordpot

   Change port, run, localhost:81?

SIEM(4000 users-->$1 mln)

Security Information and Event Management (**SIEM**) is a software solution that aggregates and analyzes activity from many different resources across your entire IT infrastructure.

- MaxPatrol SIEM
- Splunk
- Qradar
- LogRhythm
- Rapid7 SIEM
- ELK Stack free
- Graylog
- OSSIM

Antivirus

1. Signature
    a. ClamAV
    b. AVG
    c. Using YARA
2. Proactive(heuristic, behavior)
    a. Avast
    b. Kaspersky
    c. Eset NOD32

Assignment

1. Honeypot:ssh
   a. Show what you see what is being entered on your fake site
2. honeypot:wordpress
   a. Show what you see what is being entered on your fake site
3. apache + modsecurity, show difference before/after configuring secrule