UMPSA
اونيۏرسيتي مليسيا فهڠ السلطان عبدالله
UNIVERSITI MALAYSIA PAHANG
AL-SULTAN ABDULLAH

# Data & Network Security

Chapter 5 - Network Security

# Outline

5.1 Introduction to Network Security

5.2 Use of Cryptography for Data and Network Security

5.3 Architectures for Secure Networks

- 5.3.1 Secure Channels
- 5.3.2 Secure Routing Protocols
- 5.3.3 Secure DNS.

5.4 Defence Mechanisms and Countermeasures:

- 5.4.1 Network Monitoring
- 5.4.2 Intrusion Detection & Prevention
- 5.4.3 Firewalls
- 5.4.4 Spoofing Protection
- 5.4.5 DoS & DDoS Protection
- 5.4.6 Honeypots

# Intrusion Detection & Intrusion Prevention – Requirement

- Sensor
  - IDS and IPS sensors that monitor and analyze network activity.
- Management server
  - Centralized hardware or software product that receives information from all the sensors on the network and performs data analysis. It provides a centralized point of access for all security events detected by the sensors, correlates these events and provides reporting capabilities.
- Database server
  - Stores the security events.
- Console
  - Interface used by security analysts to administer the sensors, apply software updates, and monitor and analyze security events.

# Intrusion Detection & Intrusion Prevention – Requirement

- Spanning port
  - A spanning port makes a copy of all the traffic traversing specific switch ports or VLANs and sends it to the sensor.
  - A spanning configuration is the easiest and cheapest way of getting the traffic to the sensors.
  - It has many limitations:
    - Switches have a limited number of SPAN ports, typically two.
    - Reconfigurations of the spanning port can cause the sensors to stop capturing and monitoring critical traffic.
    - Increase data loss due to an oversubscribed spanning port or overloaded switch backplane.
    - Do not guarantee 100% view of network traffic.

# Intrusion Detection & Intrusion Prevention – Requirement

- Network TAP
  - A network tap deployed inline between the sensor and the network itself decreases the risk of dropped packets by using the existing signals to reconstruct the traffic flows.
  - A network tap is a scalable solution when multiple monitoring tools are required to capture the same traffic;
  - The monitoring tools can be connected directly to the network tap without impacting network traffic.
  - The tap must fail-open in the event of power loss or malfunction.

# Intrusion Detection & Intrusion Prevention – Requirement

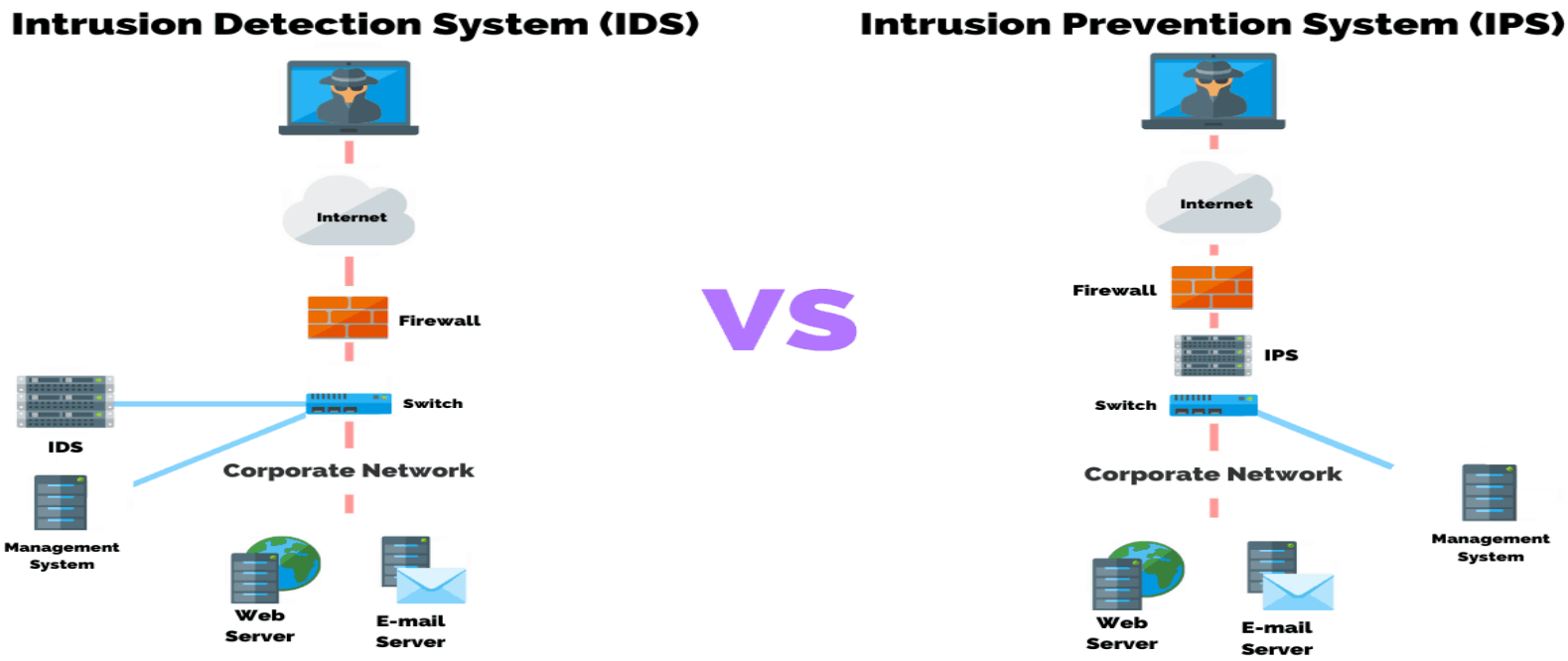
- IDS Load balancer
  - An IDS load balancer is a passive device that aggregates and distributes the traffic received from a spanning port or TAP traffic across multiple sensors.
  - When the output rate of monitored traffic exceeds the throughput of a single sensor, an IDS load balancer can be used to decrease the number of dropped packets and increase visibility.

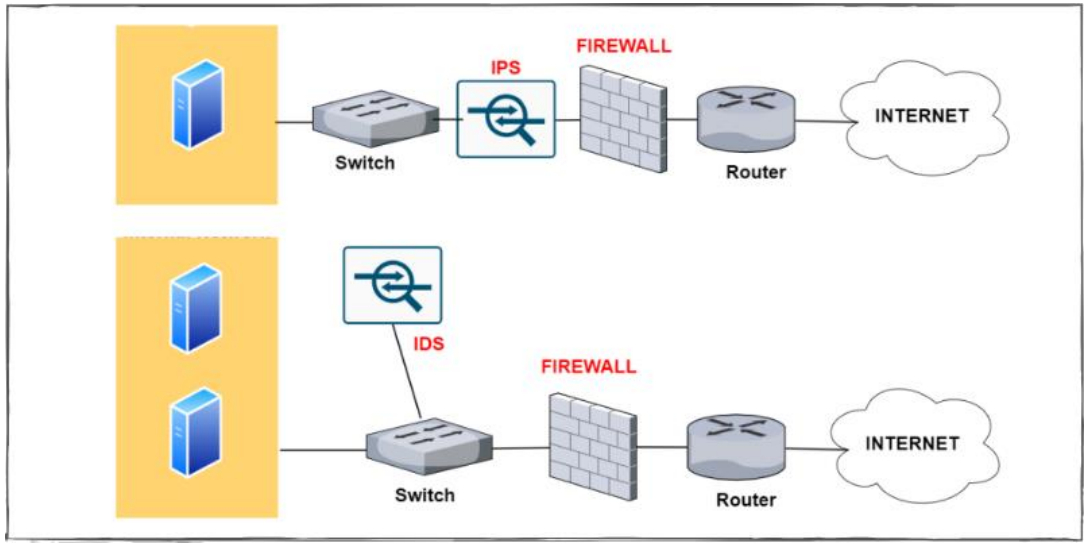
# IDS – IPS ZONE

- Intra Zone
  - Detect lateral movement between systems inside the zone, fraudulent activities executed by end-users exploiting existing trust relationship between systems, or a worm outbreak.

- Inter Zone
  - Detect malicious traffic that may have gotten passed the zone's perimeter firewall.
  - The sensor can act as an auditing device to ensure that the firewall's security policies are working as intended.

# Intrusion Detection vs Intrusion Prevention



McAfee NSP

Trend Micro TippingPoint

Cloudflare

Hillstone NIPS

Darktrace Enterprise Immune System

Securi


Huawei NIP

Entrust IoTrust Identity and Data Security

Cisco Firepower NGIPS

NSFocus NGIPS

H3C SecBlade IPS

## Commercial IDS Products

## 5.4.3 Firewalls

- The firewall is inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter.
- The aim of this perimeter is to protect the premises network from Internet-based attacks and to provide a single choke point where security and auditing can be imposed.
- The firewall may be a single computer system or a set of two or more systems that cooperate to perform the firewall function.

# Firewall

1

Firewalls protect a Network of Computers from being Compromised, Denial of Service and other Attacks from Hackers trying to Intrude the network from outside.

2

Firewall examine all the data packets passing through them to see if they meet the rules defined by the ACL (Access Control List) made by the administrator of the network.

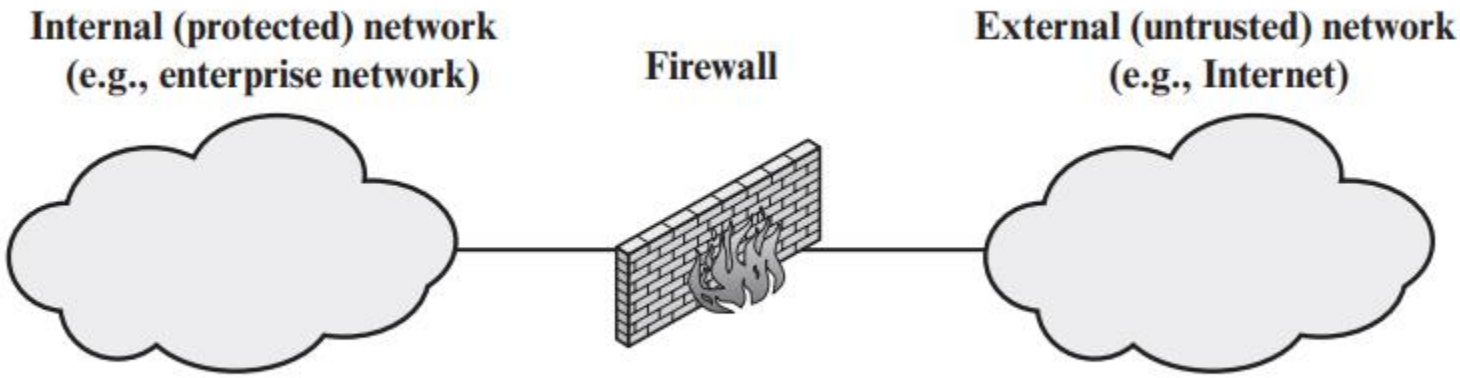
**Only, If the Data Packets are allowed as per ACL, they will be Transmitted over the Connection.**

3

4

A Firewall can be in the form of a Hardware or a Software on a Computer, as well.

# General Model of Firewall




(a) General model

A firewall policy defines **how an organization's firewalls should handle inbound and outbound network traffic** for specific IP addresses and address ranges, protocols, applications, and content types based on the organization's information security policies.


Generally, all **inbound and outbound traffic** not expressly permitted by the firewall policy should be blocked because such traffic is not needed by the organization.

Organizations should **conduct risk analysis** to develop a list of the types of traffic needed by the organization and how they must be secured—including which types of traffic can traverse a firewall under what circumstances.

## Firewall Requirements

**Firewall can filter contents on the basis of Address, Protocols, Packet attributes and State.**

**Firewalls generally only Screen the Packet Headers.**

**Packet Filtering**
Firewalls

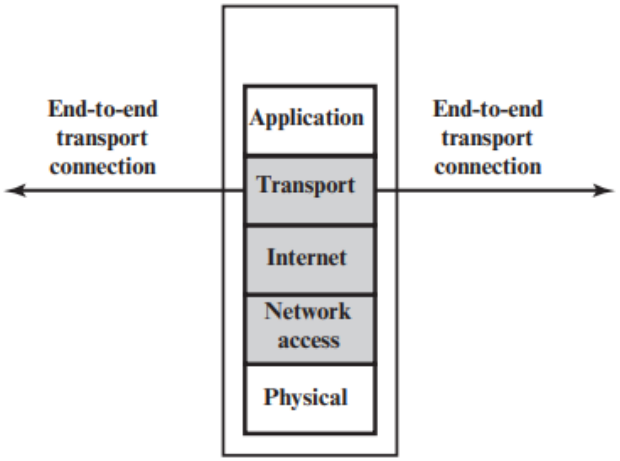
**Circuit Level**
Gateway Firewalls


**Application** level
Gateway Firewalls

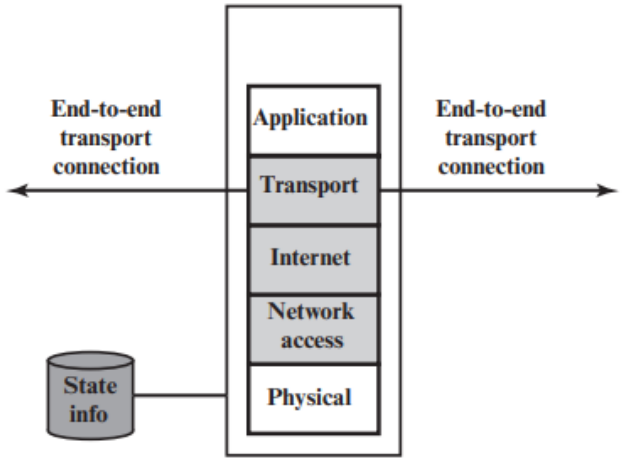
**Stateful** Multilayer Inspection Firewalls

## Types of Firewall

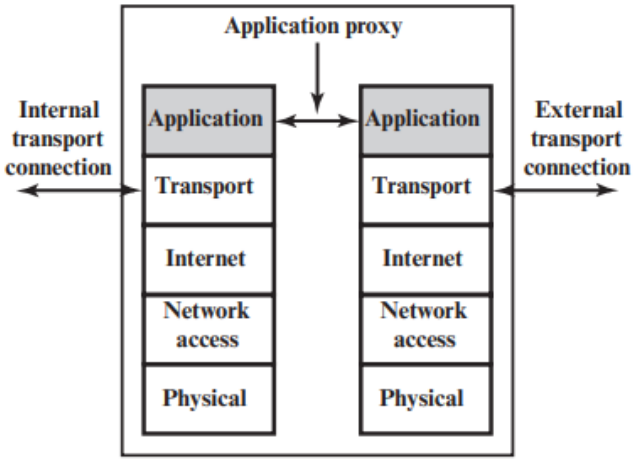
# Types of Firewall based on Layers



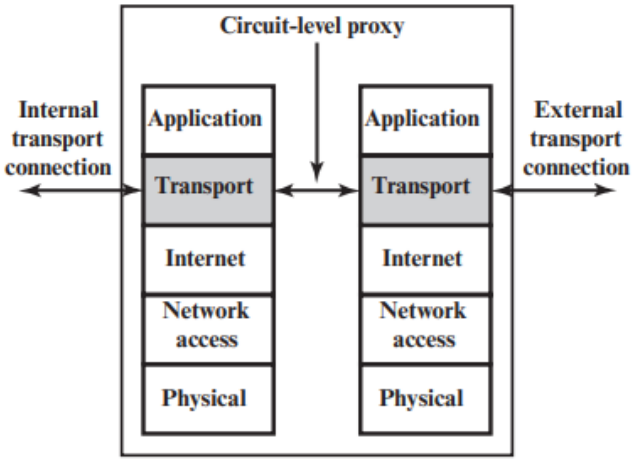

(b) Packet filtering firewall




(c) Stateful inspection firewall




(d) Application proxy firewall




(e) Circuit-level proxy firewall


Packet Filtering Firewalls work on the Basis of Rules defines by **Access Control Lists**. They check all the Packets and screen them against the rules defined by the Network Administrator as per the ACLs. If in case, any packet does not meet the criteria then that packet is dropped and Logs are updated about this information.

**Administrators can create their ACLs on the basis Address, Protocols and Packet attributes.**

*Packet Filtering Firewalls can work only on the Network Layer and these Firewalls do not support Complex rule based models. Also Vulnerable to Spoofing in some Cases.*

## Packet Filtering Firewall

Attacker

Internet

172.16.42.9

Exterior Router

192.168.3.2

Bastion Host

192.168.3.X

Packet

Perimeter Network

192.168.3.1

Interior Router

Source : 10.2.3.1. (Claims to be)

Destination : 10.2.3.2

10.2.3.4

10.2.3.X

Internal Network

10.2.3.1

10.2.3.2

Packet Filtering Firewall

**Circuit level gateways are deployed at the Session layer of the OSI model** and they monitor sessions like TCP three way handshake to see whether a requested connection is legitimate or not.

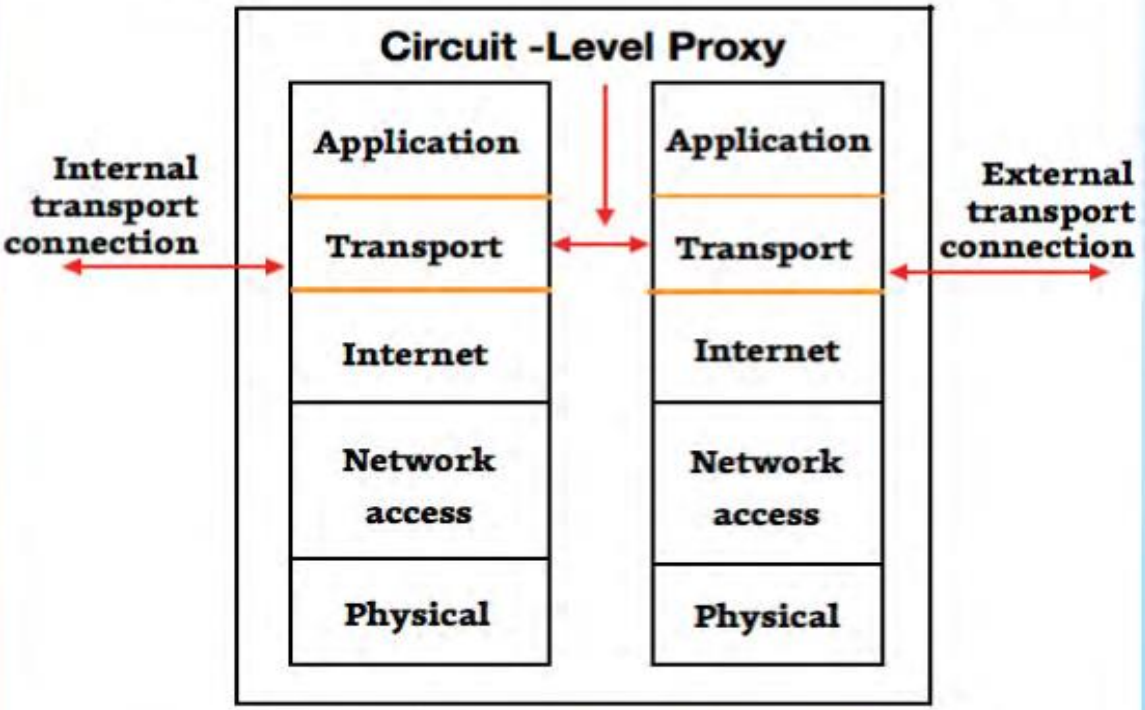
**Major Screening happens before the Connection is Established.**


**Information sent to a Computer outside the network through a circuit level gateway appears to have originated from the Gateway.** This helps in creating a stealth cover for the private network from outsiders.

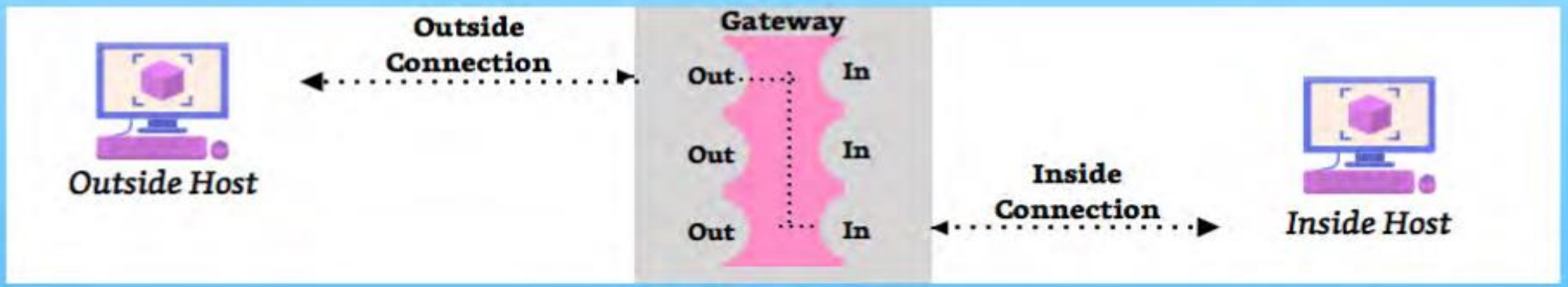
**Circuit level Gateways do not filter Individual Packets.** After Establishing a Connection, an Attacker may take advantage of this.

## Circuit Level Gateway Firewalls

# FireWalls- Circuit Level Gateway




Circuit -Level Proxy Firewall



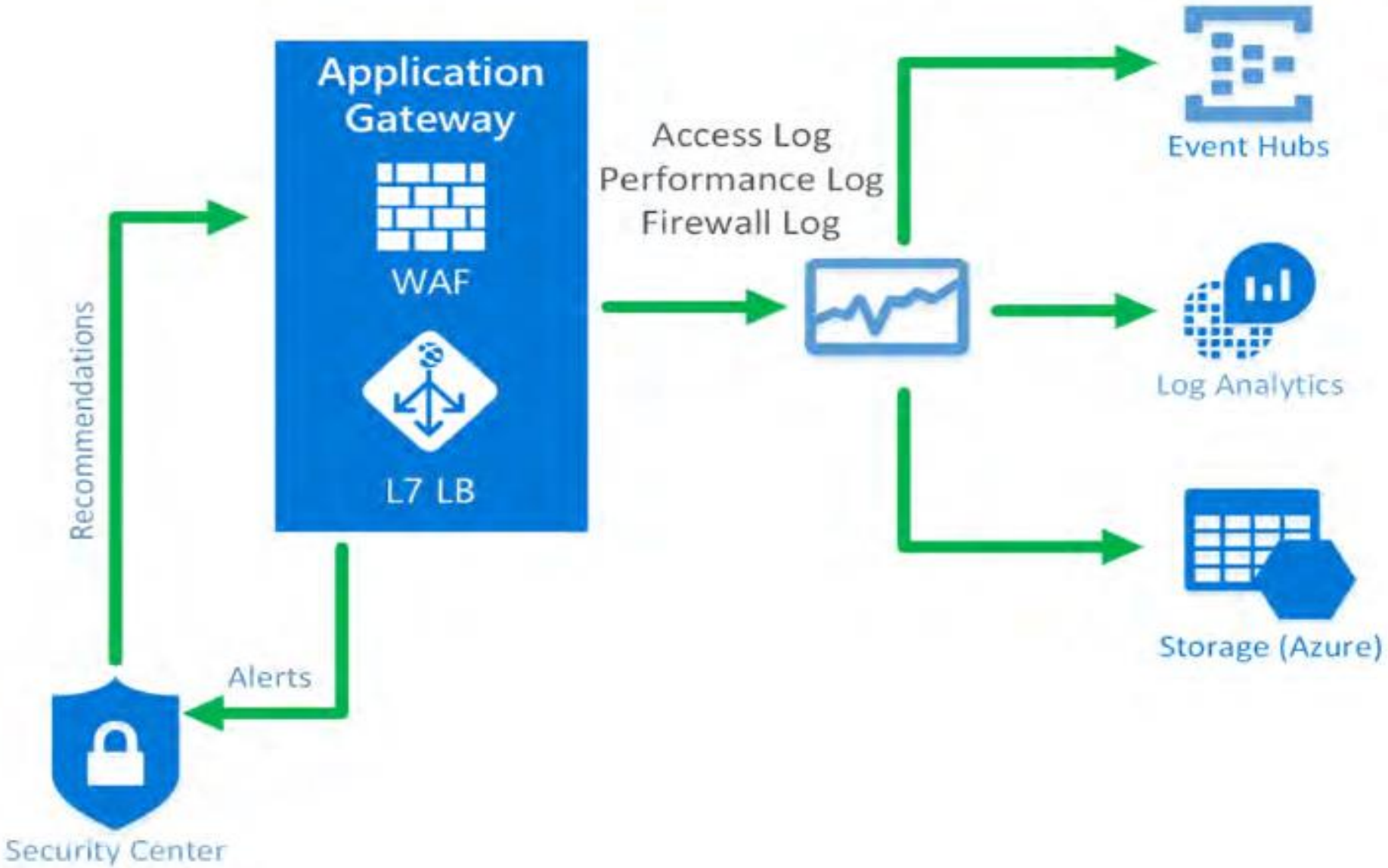

Circuit Level Gateway

Application level gateways work on the **Application layer of the OSI model** and provide protection for a specific Application Layer Procotol. Proxy server is the best example of Application Level Gateways Firewalls.

**Application level gateway would work only for the protocols which is configured.** *For example, if we install a web proxy based Firewall than it will only allow HTTP Protocol Data. They are supposed to understand application specific commands such as HTTP:GET and HTTP:POST as they are deployed on the Application Layer, for a Specific Protocol.*

**Application level firewalls can also be configured as Caching Servers** which in turn increase the network performance and makes it easier to log traffic.

## Application Level Gateway Firewalls




**Application Level Gateway Firewalls**

Stateful inspection improves on the functions of packet filters by **tracking the state of connections and blocking packets** that deviate from the expected state. This is accomplished by incorporating greater awareness of the transport layer.

As with packet filtering, **stateful inspection intercepts packets at the network layer and inspects them** to see if they are permitted by an existing firewall rule, but unlike packet filtering, stateful inspection keeps track of each connection in a state table.

## Stateful Inspection

**Stateful multilayer Inspection Firewall can filter packets at Network layer using ACLs**, check for legitimate sessions on the Session Layers and they also evaluate packets on the Application layer (ALG).

Stateful Multilayer Inspection Firewall can work on a Transparent mode allowing direct connections between the client and the server which was earlier not possible.

*Stateful Multilayer Inspection* ***firewall can also implement algorithms*** *and complex security models which are protocol specific, making the connections and data transfer more secure.*

## Stateful Multilayer Inspection Firewall

## Proxy Based

Proxy-based processes are those in which the security device acts as a proxy for the data's destination. The security device will receive and reconstruct a whole file, and examine it for threats, before passing it on to the eventual destination.

## Stream Based

Stream-based processes are those in which packets are examined as they pass through in a stream.


## Proxy-based threat scanning

**Proxy-based threat scanning uses a proxy Anti-virus engine to extract the stored object data,** and match that data against various known threat signatures contained in the regularly updated threat signature database files. Large amounts of memory and system CPU resources can be consumed performing object file download, re-order and re-assembly, scanning, and object file re-transfer. Plus proxying the TCP session reduces the overall data throughput.

**Nextgen Firewall**

**Firewalls can only work effectively on traffic that they can inspect.** Regardless of the firewall technology chosen, a firewall that cannot understand the traffic flowing through it will not handle that traffic properly—for example, allowing traffic that should be blocked. **Many network protocols use cryptography to hide the contents of the traffic.**

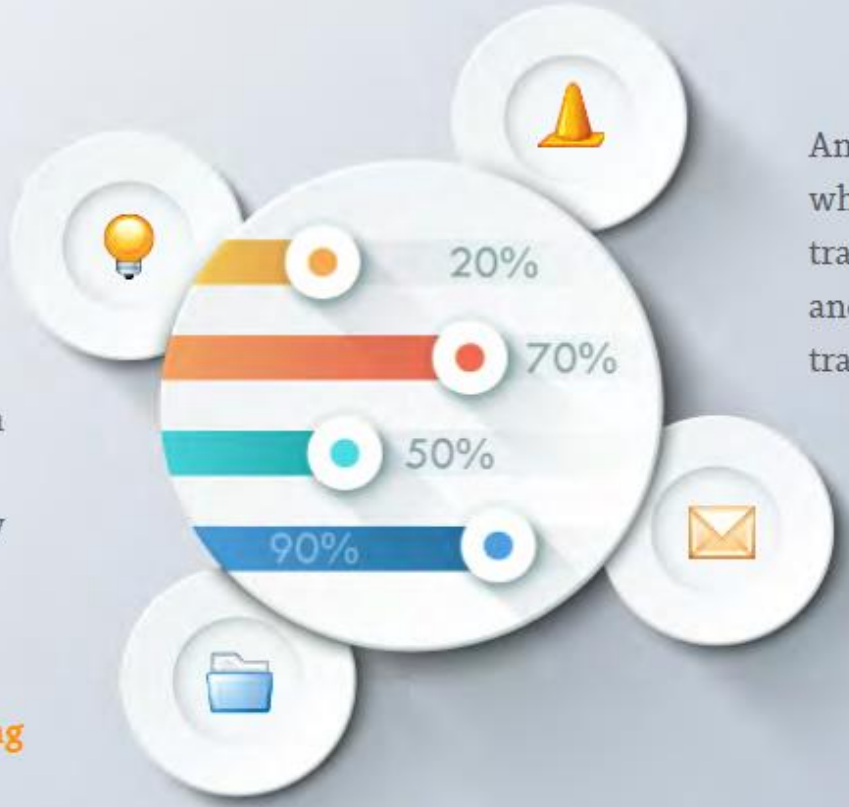
**Firewalls also cannot read application data that is encrypted**, such as email that is encrypted using the S/MIME or OpenPGP protocols, or files that are manually encrypted. Another limitation faced by some firewalls is understanding **traffic that is tunneled**, even if it is not encrypted.

## Limitations of Firewall Inspection

**An organization's firewall policy should be based on a comprehensive risk analysis.**

Firewall policies should be based on blocking all inbound and outbound traffic, with exceptions made for desired traffic.

**Policies should take into account the source and destination of the traffic in addition to the content.**



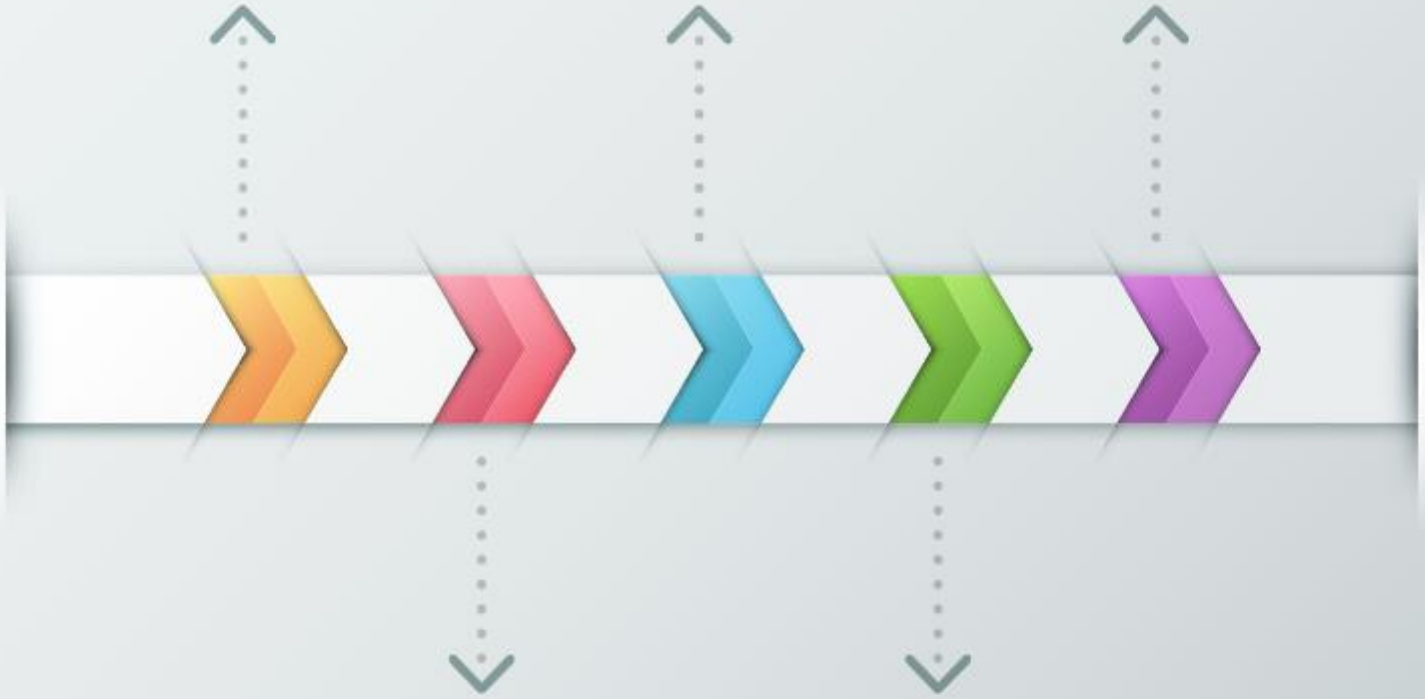

An organization should determine which applications may send traffic into or out of its network and make firewall policies to block traffic for other applications.

- Many types of IPv4 traffic, such as that with invalid or private addresses, should be blocked by default.
- **Organizations should have policies for handling incoming and outgoing IPv6 traffic.**

## Firewall Recommendations

# Firewall Policy Considerations

- Create rulesets that implement the organization's firewall policy while supporting firewall performance.
- Manage firewall architectures, policies, software and other components throughout the life of the firewall solutions.



- Create a firewall policy that specifies how firewalls should handle inbound and outbound network traffic.
- Identify all requirements that should be considered when determining which firewall to implement.

1. pfSense
2. Options_7.10.5.zip OPNSense
3. NG Firewall
4. Smoothwall
5. ufw
6. csf

## Open Source Firewall

# Design Goals of Firewall

1.All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall.

2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies.

3.The firewall itself is immune to penetration. This implies the use of a hardened system with a secured operating system. Trusted computer systems are suitable for hosting a firewall and often required in government applications.

**Network Administrators credentials are compromised and hackers gain access to Firewall dashboards**

Hackers infect the personal laptops of company's employees and spreading the malware to remote office network.

**Weak password policies of configured network devices.**


Hackers attack network with no backups or simple, single location backups.

**Firewalls needs to be updated. Hackers exploit vulnerabilities in Firewalls.**

## How to Hack Firewalls?

- Configure strong authentication credentials
- **Log important system events**
- Use strong encryption where possible


- Run the latest software versions
- **Disable anything that is not used**
- Restrict access to only those that require the access

## Firewall Best Practices


STEP 01

**Do not allow access from any source**

STEP 02

**Do not allow access from any source**

STEP 03

**Do not allow access to any destination**

STEP 04

**Do not allow access to a destination network address**

## Recommendations

STEP 05

Do not allow access to any destination service

STEP 06

Do not allow access to a range of destination services


STEP 07

Do not Reject access

STEP 08

Do not allow any ICMP message types

## Recommendations


STEP 10

**Log all allowed access**

STEP 09

**Log all denied access**

STEP 11

**Do not allow clear-text protocol services**

## Recommendations

## Questions for Discussion

1. How does IDS work?
2. List different types if IDS
3. How do you bypass Firewalls?
4. Compare and contrast different IDS products




# Others Defence Mechanisms and Countermeasures

- Spoofing and DoS Protection
- Honeypots

# 5.4.4 Spoofing Protection

- **Employ Packet Filtering with Deep Packet Inspection**
  - √ Packet filtering analyzes IP packets and blocks those with conflicting source information. This is a good way to eliminate spoofed IP packets because malicious packets will come from outside the network despite what their headers say. Because attackers have developed techniques for evading simple packet filters, most packet-filter systems offer a DPI (Deep Packet Inspection) feature. DPI allows you to define rules based on both the header and the content of network packets, allowing you to filter out many kinds of IP spoofing attacks.
- **Authenticate users and systems**
  - √ If devices on a network use only IP addresses for authentication, IP spoofing can bypass the authentication control. Connections between devices should be authenticated by the individual users or applications, or by using authenticity systems such as mutual certificate auth, IPSec, and domain authentication.

Source : https://www.veracode.com/security/spoofing-attack

# 5.4.4 Spoofing Protection

- **Use Spoofing Detection Software**
  - √ Several programs help detect spoofing attacks, especially ARP spoofing. Consider a tool like NetCut, Arp Monitor, or Arpwatch for ARP spoofing defense. These and other tools can inspect and certify legitimate data before it is received by a target machine can significantly lower the success of spoofing attacks.

- **Use Encrypted and Authenticated Protocols**
  - √ Security experts have developed several secure communications protocols, including Transport Layer Security (TLS) (used by HTTPS and FTPS), Internet Protocol Security (IPSec), and Secure Shell (SSH). When used properly, these protocols authenticate the application or device to which you're connecting, and encrypt data in transit, reducing the likelihood of a successful spoofing attack.

Source : https://www.veracode.com/security/spoofing-attack

# 5.4.5 DoS and DDoS Protection

In general, there are three lines of defence against DoS and DDoS attacks:

- **Attack prevention and pre-emption (before the attack):** These mechanisms enable the victim to endure attack attempts without denying service to legitimate clients.
  - Techniques include enforcing policies for resource consumption and providing backup resources available on demand. In addition, prevention mechanisms modify systems and protocols on the Internet to reduce the possibility of DDoS attacks.
- **Attack detection and filtering (during the attack):** These mechanisms attempt to detect the attack as it begins and respond immediately.
- **Detection involves looking for suspicious patterns of behaviour**. The response involves filtering out packets likely to be part of the attack.

# Best Practices for DoS and DDoS Protection

1. Multi-layered protection – built-on redundancies, traffic monitoring capabilities, business logic flaw detection, and vulnerability management capabilities.
2. Avoid becoming a bot.
3. Recognize attack types – application layer (HTTP flooding), UDP amplification, and DNS flooding.
4. Reduce attack surface exposures – protect critical assets, applications and other resources, ports, protocols, servers, and other entry points from direct exposure to attackers.
5. Fortify network architecture – infrastructure and network capable of handling any thundering surge of a sudden spike in traffic. More bandwidth or resources to cater to client-server request-response.
6. Deploy web application firewall.

Source : https://www.indusface.com/blog/best-practices-to-prevent-ddos-attacks/

# 5.4.6 Honeypots

Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems.

- Divert an attacker from accessing critical systems.
- Collect information about the attacker's activity.
- Encourage the attacker to stay on the system long enough for administrators to respond.

# Honeypot Deployment

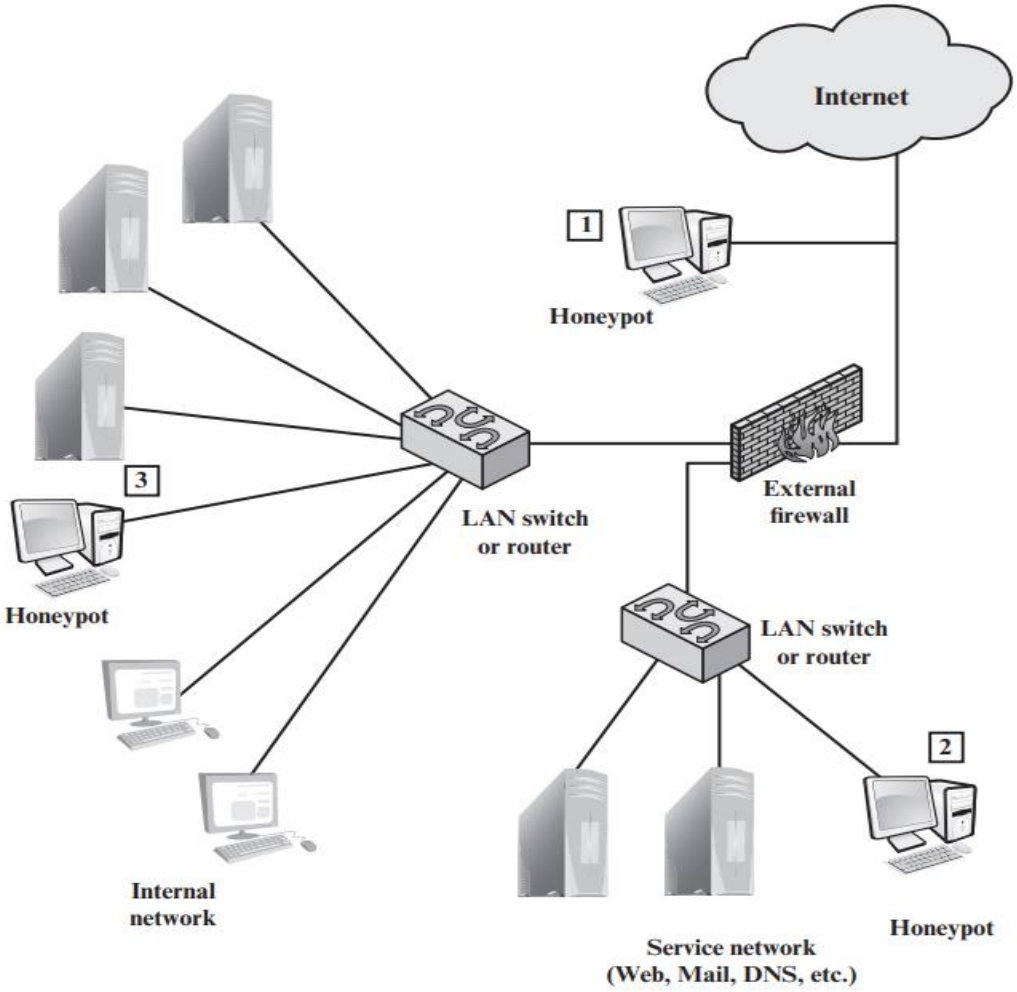



Figure 11.4 Example of Honeypot Deployment

# Continue....

Honeypots can be deployed in a variety of locations:

1. A honeypot outside the external firewall **(location 1)** is useful for tracking attempts to connect to unused IP addresses within the scope of the network.

2. The network of externally available services, such as Web and mail, often called the DMZ (demilitarized zone), is another candidate for locating a honeypot **(location 2).**

3. A fully internal honeypot **(location 3)** has several advantages. Its most important advantage is that it can catch internal attacks. A honeypot at this location can also detect a misconfigured firewall that forwards impermissible traffic from the Internet to the internal network.

# Summary

- Several combinations of technology and application that suit best based on organization requirement is needed to secure the network.
- Cryptography is best suited to secure data on the fly (Internet access) or in a database.
- For network security, deployment of the defence mechanisms and countermeasures is expected to prevent many attacks related to the network environment.
- If not all, at least network security implementation can reduce attacks or minimize the effect of malicious traffic to an acceptable level while maintaining functionality for users' access.

# References


Meier, J. D., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R., & Murukan, A. (2003). Securing Your Network.

Luciana Obregon. (2016), Infrastructure Security Architecture for Effective Security Monitoring

William Stallings. (2017). Network Security Essential.

https://purplesec.us/wp-content/uploads/2019/11/Intrusion-Detection-IDS-VS-Intrusion-Prevention-IPS-What%E2%80%99s-The-Difference.png

https://forum.huawei.com/enterprise/en/comparison-and-differences-between-ips-vs-ids-vs-firewall-vs-waf/thread/763619-867