



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

Learning Outcome

At the end of this chapter, students are able to:

- Understand the network security factors and needs.
- Understand the use of cryptography for data and network security.
- Analyze the defence mechanisms and countermeasures for any related network environment.
- Apply any mechanism to defend the network and its infrastructures from attacks.

5.1 Introduction

- The network is the entry point to your application.
- Provides the first gatekeepers controlling access to your environment's various servers.
- Servers are protected with their operating system gatekeepers, but it is important not to allow them to be deluged with attacks from the network layer.
- In a nutshell, network security involves protecting network devices and the data they forward.
- The basic network components - the router, the firewall, and the switch.

Network Security Model

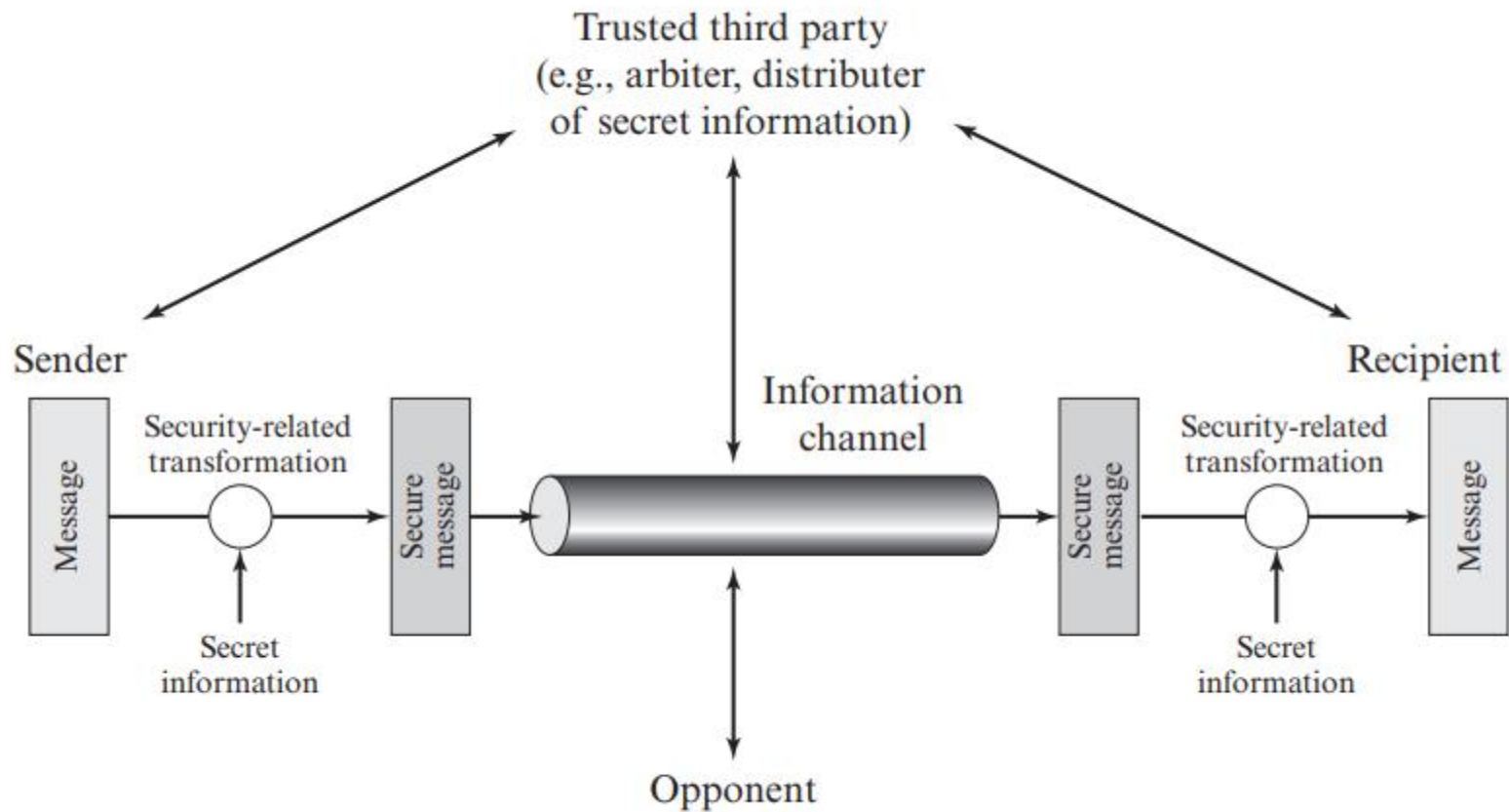


Figure 1.5 Model for Network Security

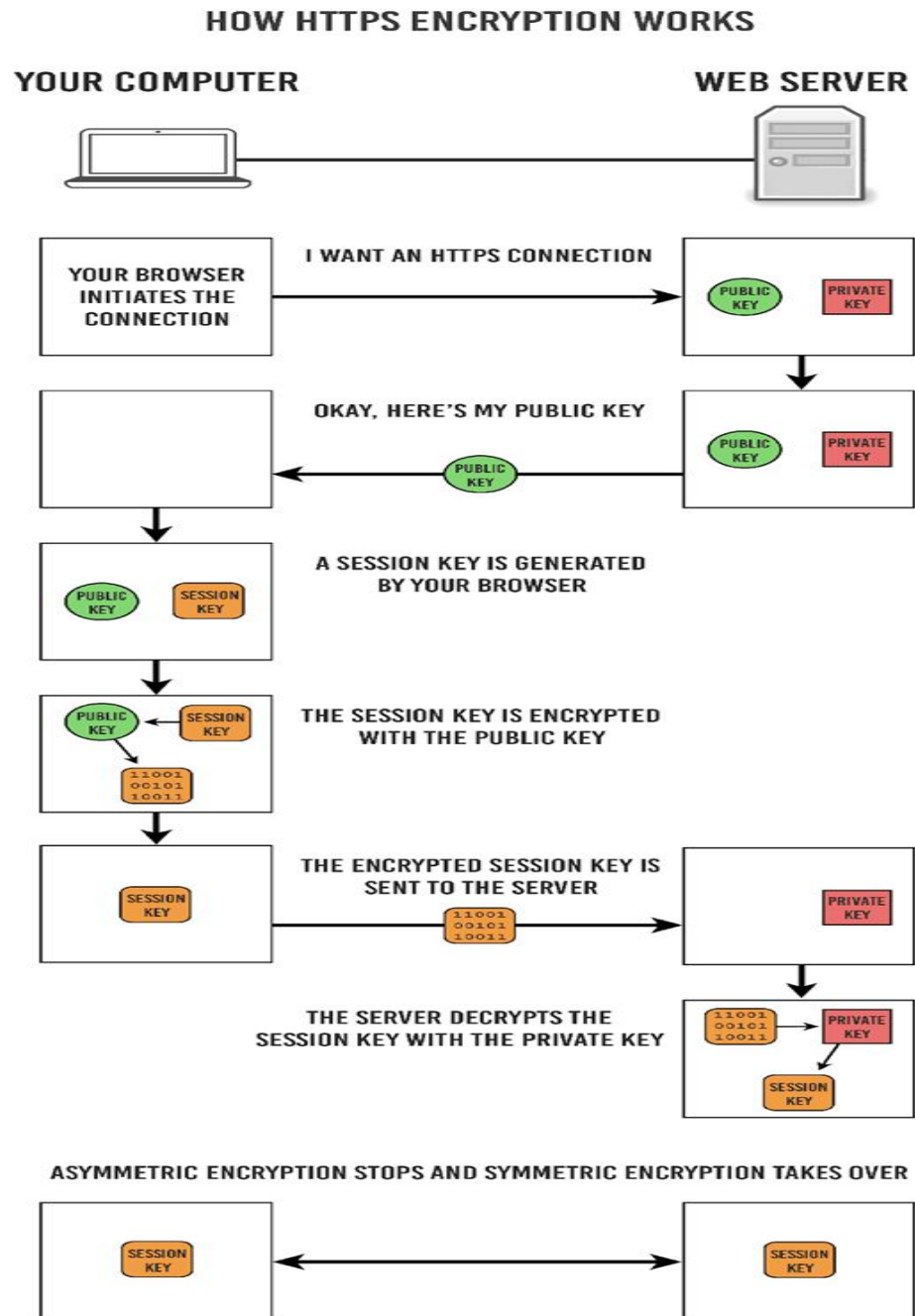
Component of Secure Network

- A security-related transformation on the information to be sent.
- Examples include the encryption of the message, that it is unreadable by the opponent,
- the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.
- Some secret information shared by the two principals and, it is hoped, unknown to the opponent.
- An example is an encryption key used to scramble the message before transmission and unscramble it on reception.

5.2 Use of Cryptography for Data and Network Security

- Protocol for secure Communication
 - Secure HTTP (S-HTTP) – provides for the encryption of protected Web pages transmitted via the Internet between a client and server.
 - Secure Socket Layer (SSL) – use public key encryption to secure a channel over the Internet (Internet Browser)

How HTTPS Work



How SSL Work



5.3 Architectures for Secure Networks

- Factors should be considered to have secure network. The factors are:
 - Topology And Placement Of Hosts Within The Network
 - The Selection Of Hardware And Software Technologies
 - And The careful Configuration Of Each Component

Architectures for Secure Networks

- Some of the typical challenges faced by the network designer include the following:-
 - Securing the network from **Internet launched attacks**
 - Securing **Internet** facing web, DNS and mail servers
 - Containing damage from compromised systems, and preventing internally launched attacks
 - **Securing sensitive** and mission critical internal resources such financial records, customer databases, trade secrets, etc.
 - Building a **framework for administrators** to securely manage the network
 - Providing systems for **logging and intrusion detection**

Secure Channels

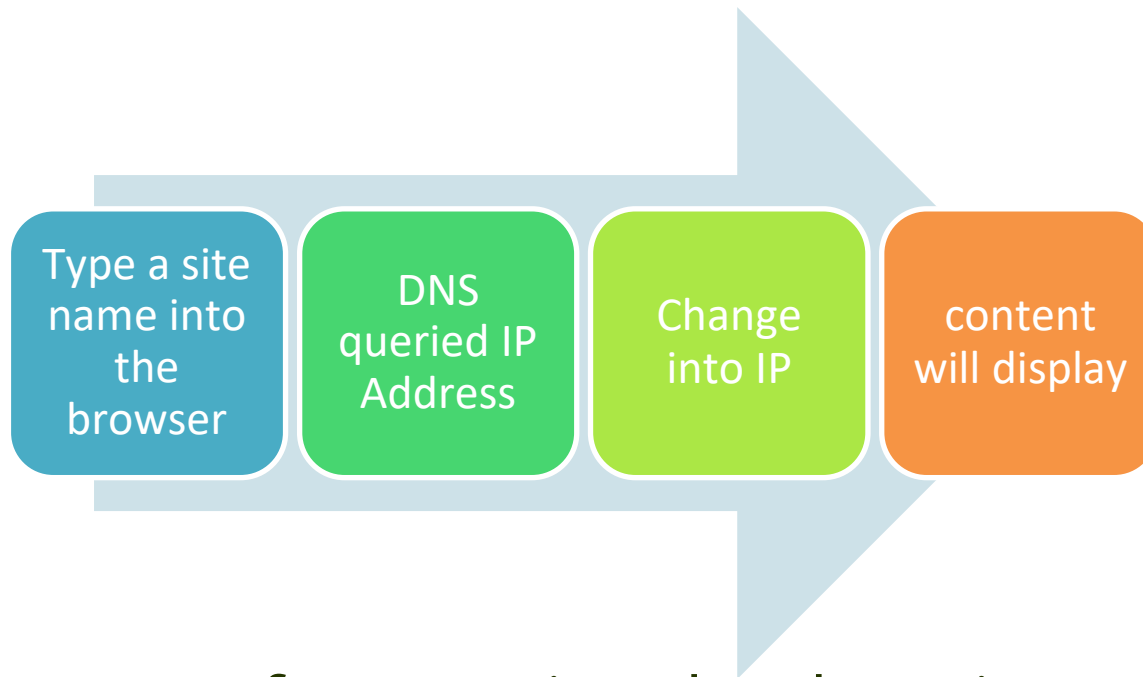
- Channel is a way of communicating with people or getting something done.
- Secure Channel can be defined as a way which authenticates the requester and also provide confidentiality and integrity of data sent across the way.
- Windows Active Directory environments, secure channel provides an encrypted way of communication between clients and [domain controllers](#).
- There are three types of secure channels:
 - communication between clients in a domain and domain controllers.
 - responsible to establish a secure communication between domain controllers of a source domain and domain controllers of a trusted domain.
 - responsible for establishing a secure path between domain controllers in the same domain.

Routing Protocol

- Every network routing protocol performs three basic functions:
 - *discovery* - identify other routers on the network
 - *route management* - keep track of all the possible destinations (for network messages) along with some data describing the pathway of each
 - *path determination* - make dynamic decisions for where to send each network message
- Some of Secure Route Protocol
 - https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook/sec_chap3.html

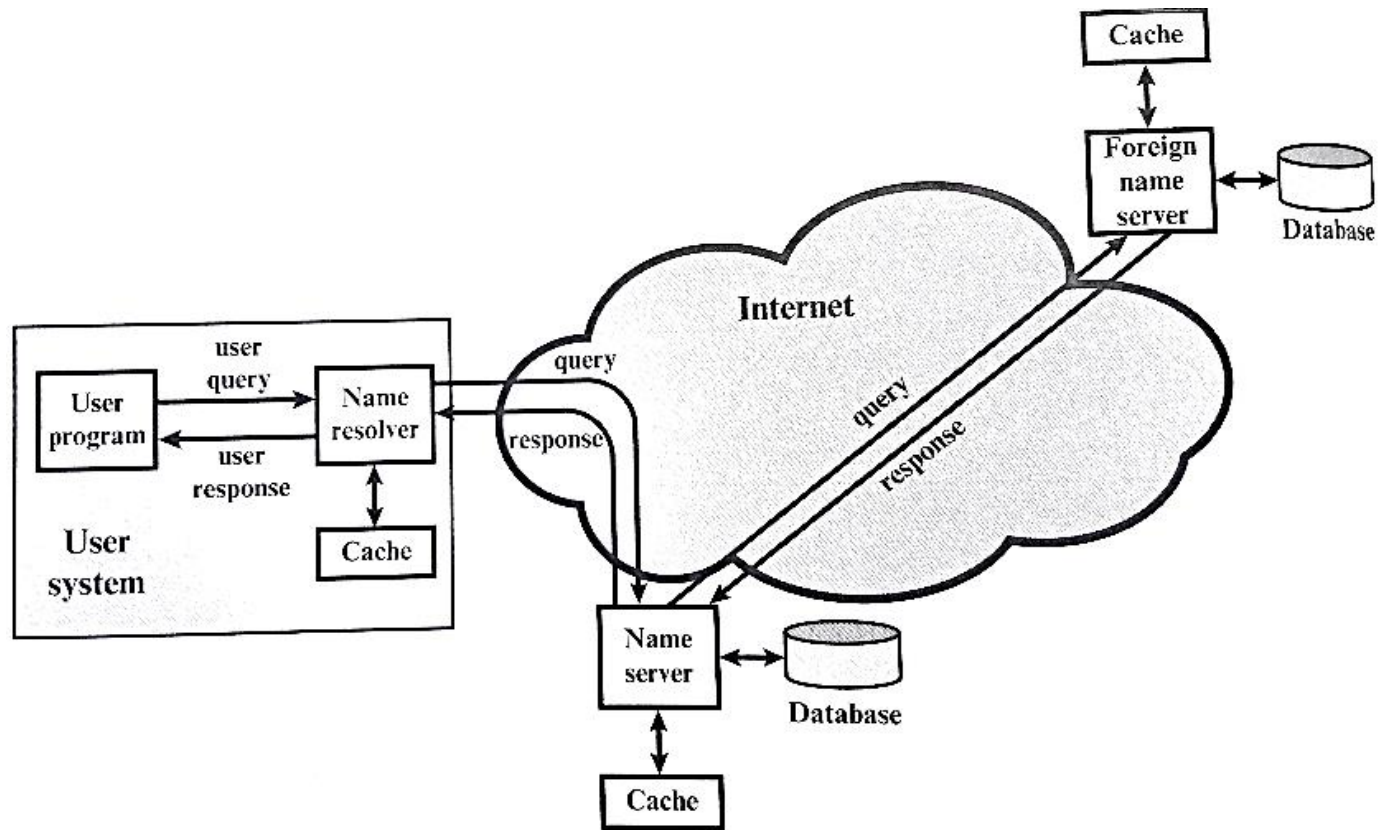
Secure DNS

- The Domain Name System (DNS) is used every time surf the Web.



- The process of converting the domain name to its IP address is called domain-name resolution.

Domain-Name Resolution



Today DNS Offer by Provider

- **Content filtering.** This can be conveniently implemented to block adult sites and other unwanted content, while requiring no software on the computers and devices.
- **Malware and phishing blocking.** This can be performed by the content filtering tool also, to block sites containing viruses, scams and other dangerous content.
- **Protection against botnets.** This blocks communication with known botnet servers so your computer isn't taken over.
- **Advertisement blocking.** This is another type of content filtering, which some DNS services specifically concentrate on.
- **URL typo correction.** For instance, if you typed *gogle.com* it would correct to *google.com*.
- **Botnets-** a group of private computers infected with malicious software and controlled without the knowledge of owner, e.g. send spam messages.

5.4 Defence Mechanisms and Countermeasures

- Network Monitoring
- Intrusion Detection & Prevention
- Firewalls
- Spoofing and DoS Protection
- Honeypots

Defence Mechanisms and Countermeasures

- Many organizations struggle to design and implement adequate network infrastructures to optimize network security monitoring.
- The challenge - often leads to data loss with regards to monitored traffic and security events, increased cost in new hardware and technology needed to address monitoring gaps, and additional Information Security personnel to keep up with the overwhelming number of security alerts.
- Organizations spend a lot of time, effort, and money deploying the latest and greatest tools without ever addressing the fundamental problem of adequate network security design.

5.4.1 Network Monitoring

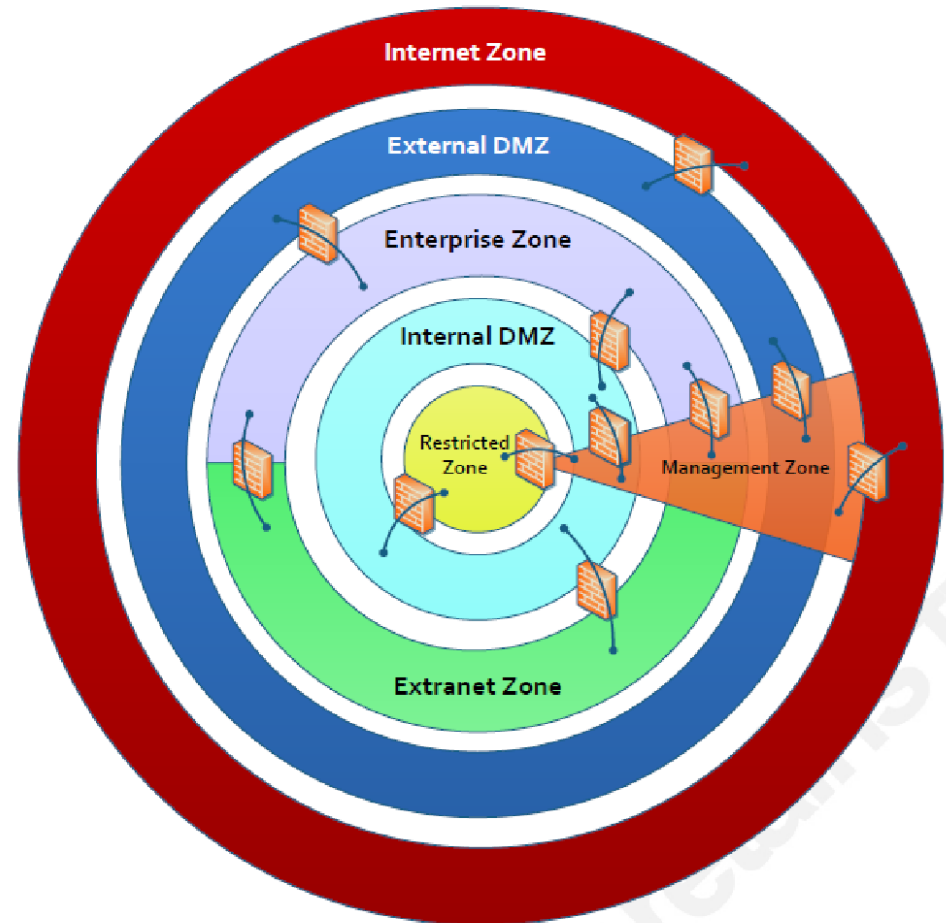
- Information about network performance and user behaviour on the network helps security program managers identify areas in need of improvement as well as pointing out potential performance improvement.
- The visibility should be done for:
 - Logical Network Security Segmentation
 - Security Event Logging

Logical Network Security Segmentation

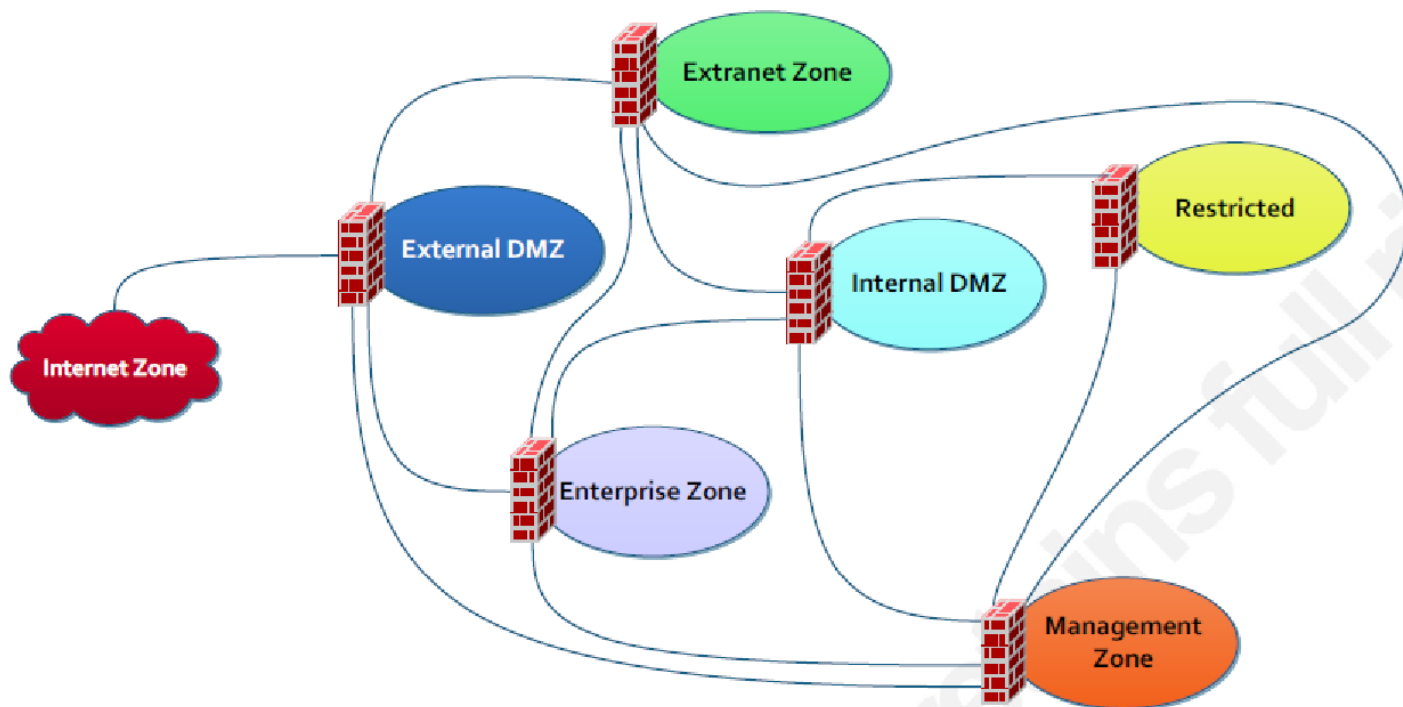
- A network segment, also known as a network security zone, is a logical grouping of information systems in an enterprise network.
- A network security zone has a well-defined perimeter and strict boundary protection.
- The zone is created based on different security requirements.
- Network segmentation is part of a defence-in-depth strategy with the following goals; Limit the scope of regulatory compliance, Reduce data exfiltration(unauthorized data copy/transfer), Reduce attack surface, Compartmentalize systems, Increase availability

Logical Network Security Segmentation: Network Security Zones

- Internet Zone - No Trust
- External DMZ - Low Trust
- Enterprise Zone - Medium Trust
- Extranet Zone - Medium Trust
- Internal DMZ - High Trust
- Management Zone - Highest Trust
- Restricted Zone - Highest Trust



Logical Network Security Segmentation: Rules of Communication



Zones Explanation

- Internet Zone — Internet Zone includes internet, ISPs. It is least trust zone as it contains the threat actors.
- External DMZ — The External DMZ zone is the public facing zone that requires exposure to the Internet. It usually contains the web servers, DNS Server, FTP Servers, Web Proxy Servers, E-mail Gateways. This zone proxies access between systems in the Enterprise Zone and the Internet i.e. all traffic should be funneled through the External DMZ to reach the Internet. The systems deployed in this zone should be tightly controlled and hardened to reduce the attack surface.
- Enterprise Zone — This Zone contains all the end users working inside the Enterprise. Endpoint protection is critical control in this zone to protect the end users.

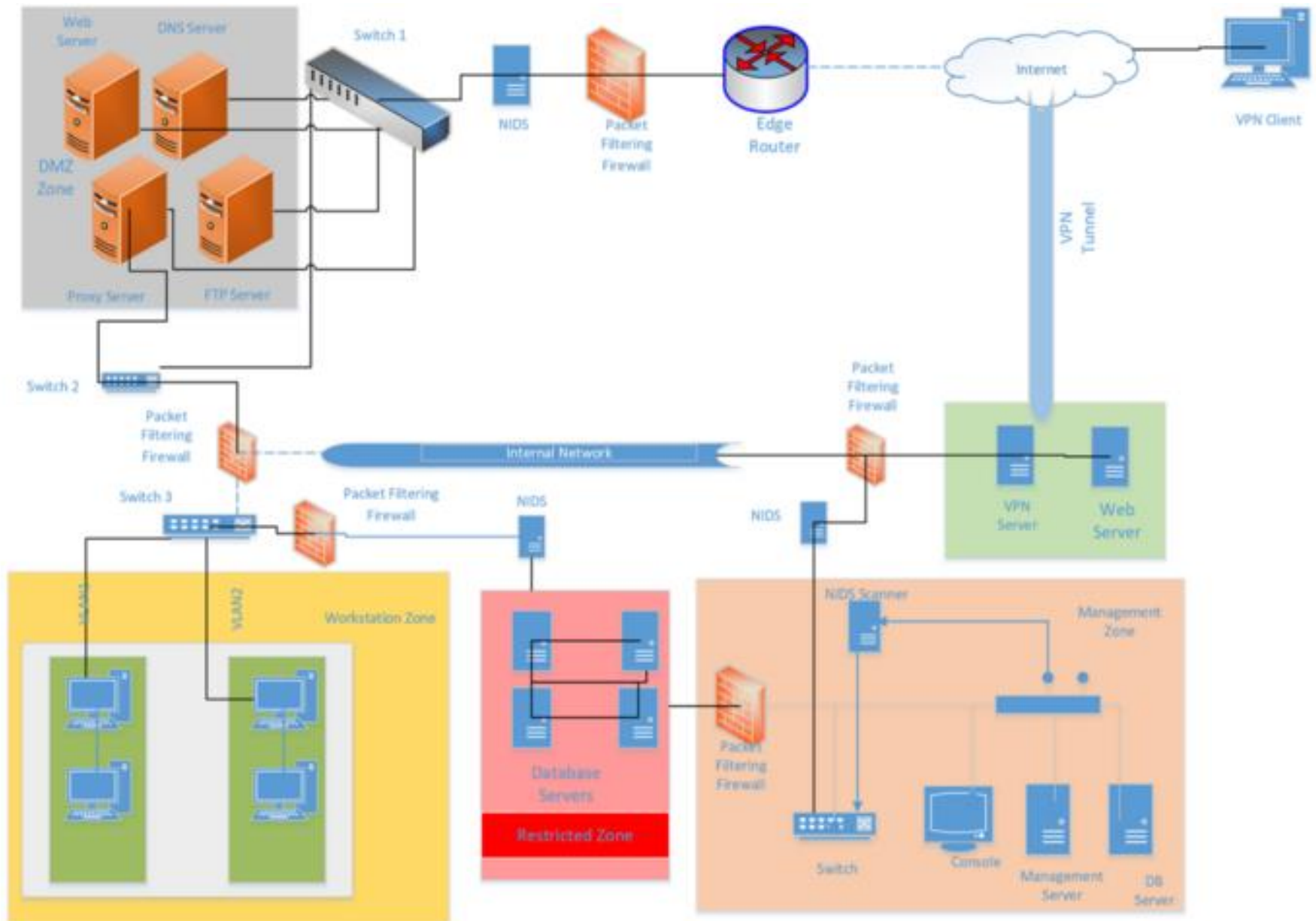
Zones Explanation

- Extranet Zone — This zone connects the Enterprise Network with the highly trusted 3rd party business partners, who can access the Enterprise Zone. Though the traffic between the Extranet Zone and Enterprise Zone is filtered and monitored at the zone's perimeter to allow only business approved traffic to enter and leave the zone. The systems inside this zone are out of the control of the Enterprise and not follow organization's security policies.
- Internal DMZ — Internal DMZ acts as a mediator between Enterprise/Extranet Zone and the Restricted Zone. It usually contains the Internal application servers. So, all the end users must authenticate themselves in this zone before accessing the Restricted Zone.

Zones Explanation

- Restricted Zone — The Restricted zone is the most critical zone for any organization as it contains all the confidential and sensitive data which are accessible to only a few privileged users. That is why it needs the highest-level security at its perimeter. It contains all the database servers.
- Management Zone — This Zone has all the administrative and monitoring systems (performance servers, configuration management servers, log management servers) controlled by the Network administrators, Database administrators, System administrator. The Users of Management Zone have higher privileges to access all the other zones in an Enterprise. This zone needs the highest level of security as needed by the Restricted zone. So, the communication between the Management Zones and the Internet should be restricted to only those destinations, ports, and protocols required to download patches or software upgrades.

Example of Network Segmentation with Devices



Security Event Logging

- A log is a record of events occurring in a computer system or network that triggers a notification, adding it to a local system file or forwarding it to a centralized log management infrastructure for further processing and analysis.
- Is a prime resource for troubleshooting and supporting business goals.
- Log management is the process of generating, gathering, transmitting, storing, analyzing, and disposing of event logs from disparate sources.

What to Log

- Logs can be categorized as follows
 - Security logs
 - Operating system logs
 - Application logs
- In **security log** a minimum, an organization should be collecting as following categories systems:
 - Host-based protection software, Intrusion detection and prevention systems (IDS/IPS), VPN or remote access systems, Web proxy servers, Vulnerability management software, Authentication servers, Routers and layer 3 switches that contain access control lists, Firewalls

What to Log

- **Operating system logs**

- Assist in the investigation of suspicious activities around a particular system.
- OS log - An audit log records both, successful and failed login attempts, account modifications, file access attempts, use of privileges, and security policy changes.

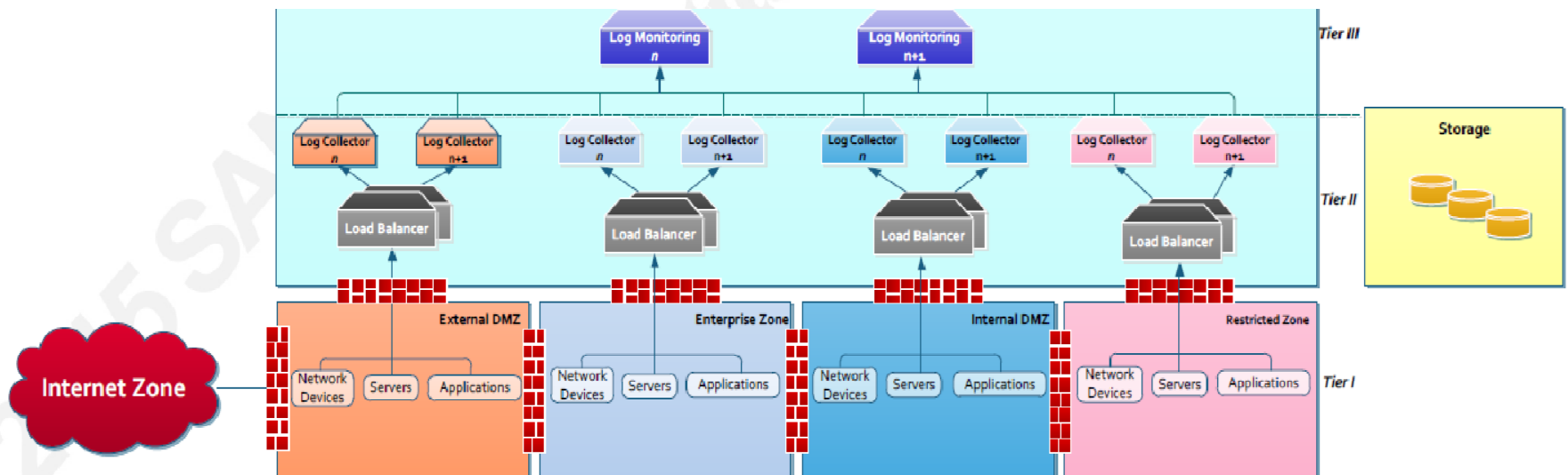
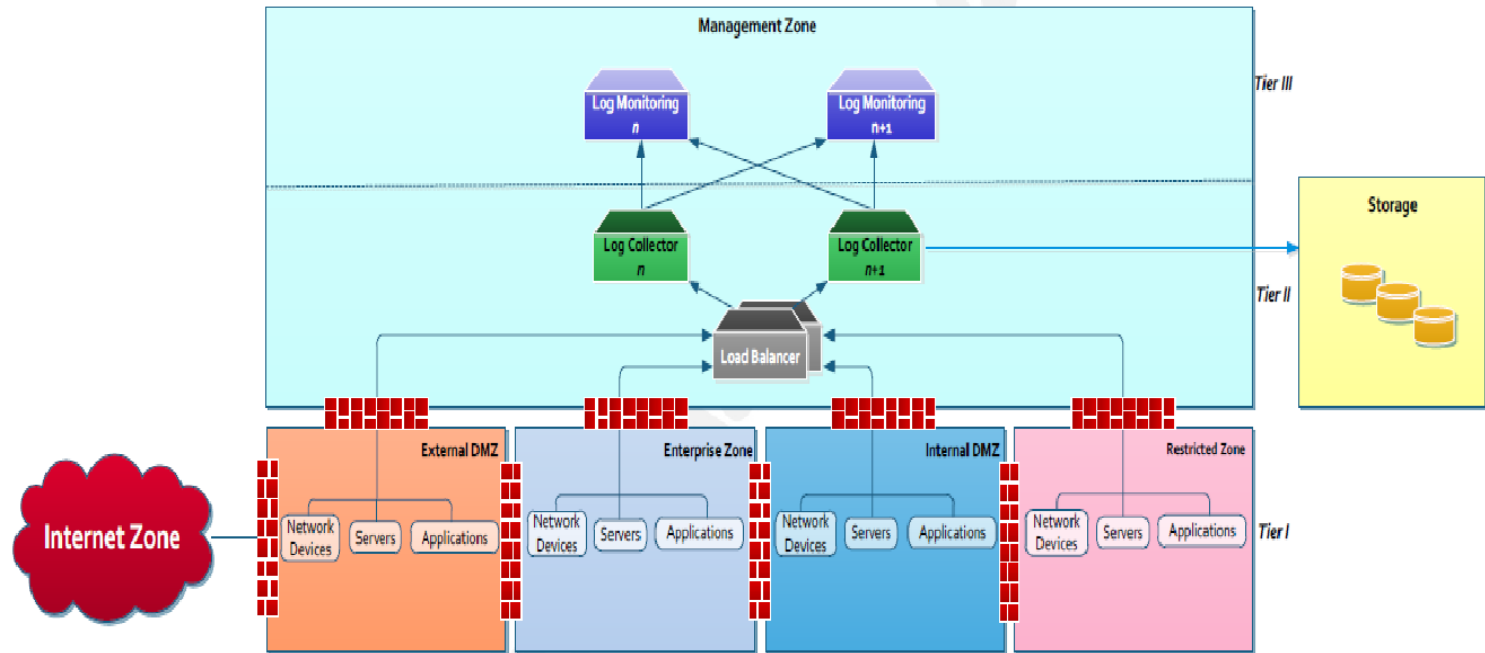
- **Application logs**

- Generate log files and support network protocols such as SYSLOG or SNMP to transfer the logs to a centralized log collector.

Log Management Architecture

- Three tiers log management.
- Tier I: Log generation
 - includes the systems, networks, and applications that generate log data.
- Tier II: Log analysis and storage
 - Consists of the log servers, also known as log collectors, which receive the log data from Tier I.
- Tier III: Log monitoring
 - Includes administrative consoles used to monitor and review the log data.

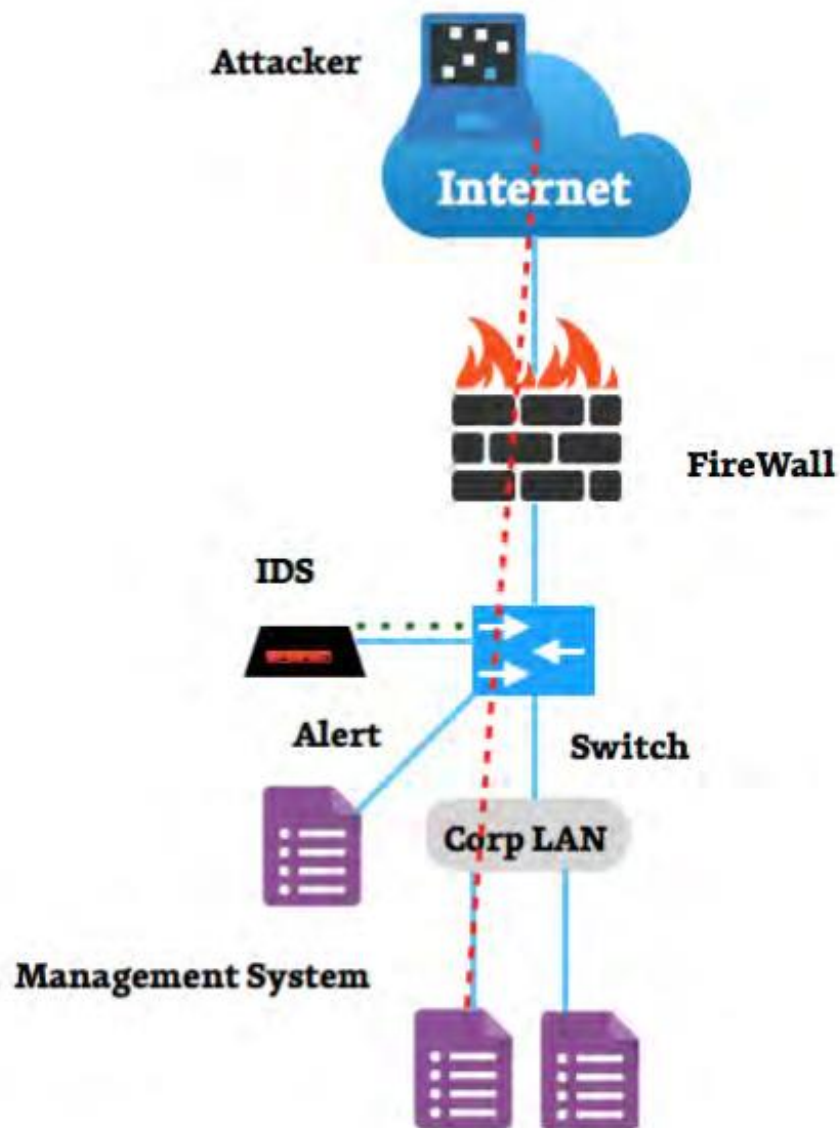
Baseline Log Management Architecture



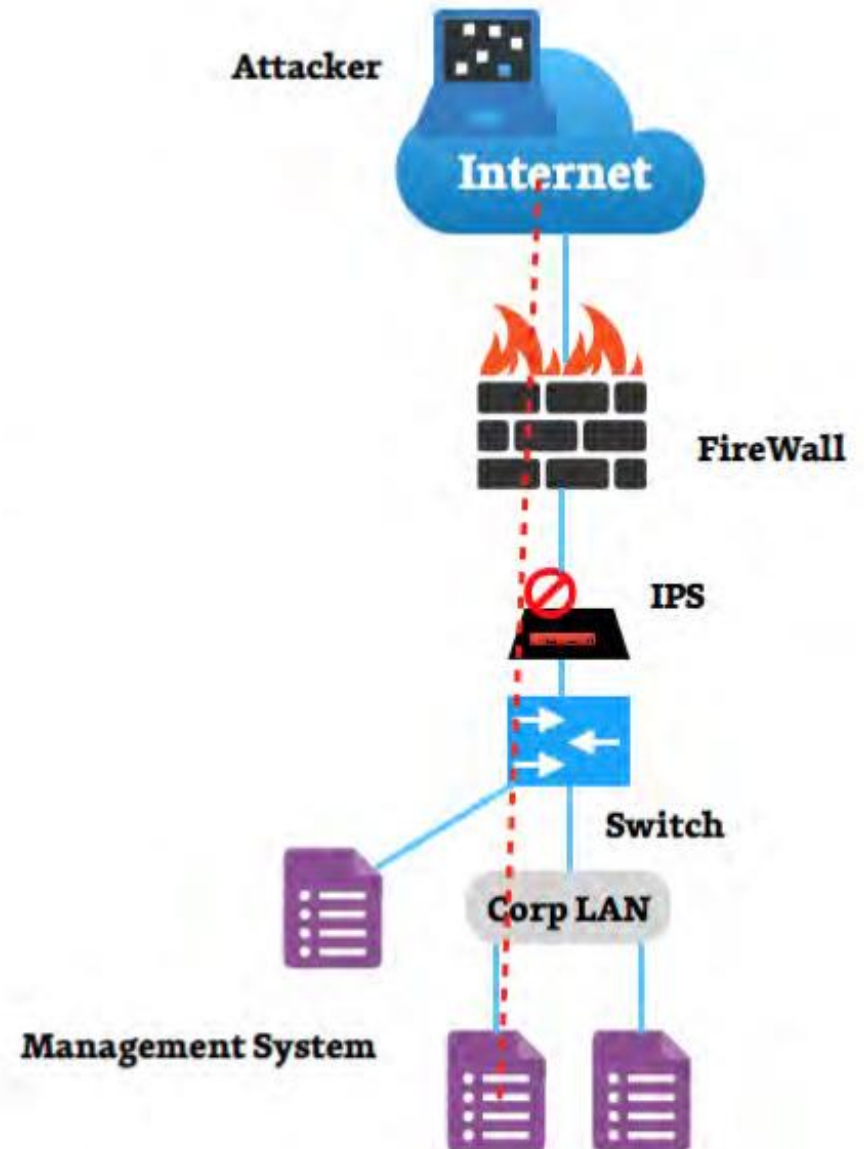
5.4.2 Intrusion Detection & Intrusion Prevention

- Intrusion Detection Systems (IDS) inspect network traffic to identify signs of malicious activity and policy violations, enabling organizations to respond before a threat actor causes significant harm to IT systems.
- Intrusion Prevention Systems (IPS) have the same capabilities of IDS but go a step further by attempting to react to a detected threat to prevent it from being successful.
- The IDS/IPS infrastructure will discuss into two type; Intra-Zone and Inter-Zone.

Intrusion Detection System



Intrusion Prevention System



Intrusion detection is the process of monitoring the events occurring in your network and analyzing them for signs of possible incidents, violations, or imminent threats to your security policies. Intrusion prevention is the process of performing intrusion detection and then stopping the detected incidents.

These security measures are available as:

Intrusion Detection Systems (IDS)

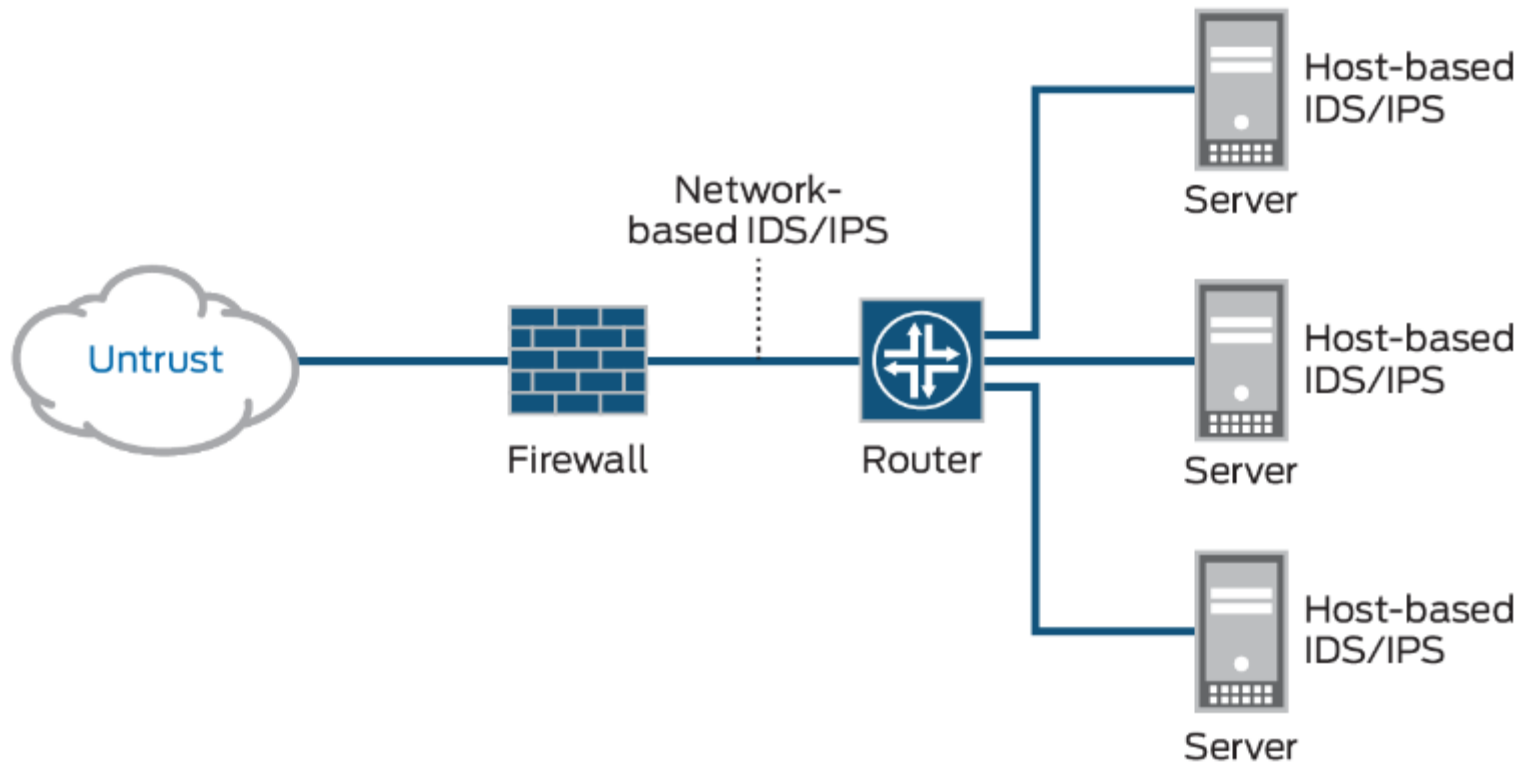
Intrusion Prevention Systems (IPS)



IDS and IPS constantly watch your network, **identifying possible incidents and logging information about them, stopping the incidents**, and reporting them to security administrators.

Any malicious activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms

Intrusion Detection System (IDS)



Intrusion Detection System (IDS)

The three IDS detection methodologies are typically used to detect incidents.

Signature-Based Detection

compares signatures against observed events to identify possible incidents.

This is the simplest detection method because it compares only the current unit of activity (such as a packet or a log entry, to a list of signatures) using string comparison operations.

02



01



01

04



03



03

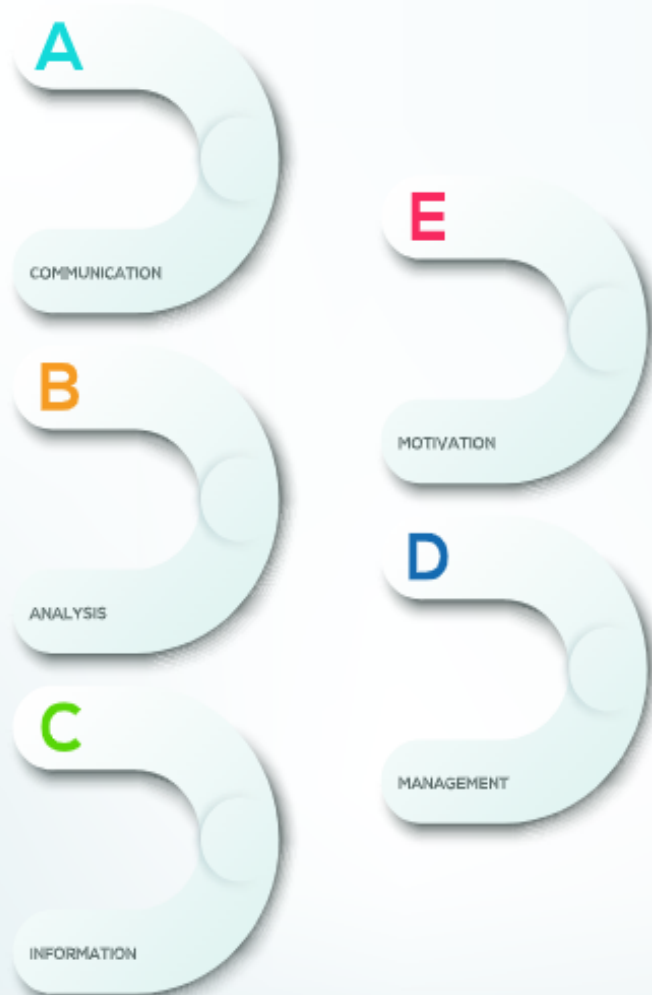
Anomaly-Based Detection

compares definitions of what is considered normal activity with observed events in order to identify significant deviations. This detection method can be very effective at spotting previously unknown threats.

Stateful Protocol Analysis compares predetermined profiles of generally accepted definitions for benign protocol activity for each protocol state against observed events in order to identify deviations.

How Does IDS Work?

Host-based intrusion detection, (HIDS), examine events on a computer on your network rather than the traffic that passes around the system. **HIDS operates by looking at data in admin files on the computer that it protects.** Those files include log files and config files.



HIDS as an agent that monitors whether anything or anyone, whether internal or external, has circumvented the system's security policy.

HIDS agent is installed on every computer on the network.


Host Intrusion Detection Systems (HIDS)

A network-based intrusion detection system (NIDS) is used to **monitor and analyze network traffic** to protect a system from network-based threats.



A NIDS reads all inbound packets and searches for any suspicious patterns. When threats are discovered, based on its severity, the system can take action such as notifying administrators, or barring the source IP address from accessing the network.

Network Intrusion Detection Systems (NIDS)

- 
- OSSEC
 - **Sagan**
 - Security Onion
 - **AIDE**
 - Samhain
 - **Fail2Ban**
 - BSign
 - **Integrit**
 - Systraq
 - Tripwire



- 
- **Snort**
 - Bro
 - **Suricata**
 - Sagan
 - **Security Onion**
 - Open WIPS-NG

Linux - Host Intrusion Detection Systems

Linux - Network Intrusion Detection Systems