Unit -5

Firewall Location and Configuration

Configured to keep organizations protected from data leakage and cyber attacks.

Firewall policy configuration is based on network type, such as public or private, and can be set up with security rules that block or allow access to prevent potential attacks from hackers or malware.

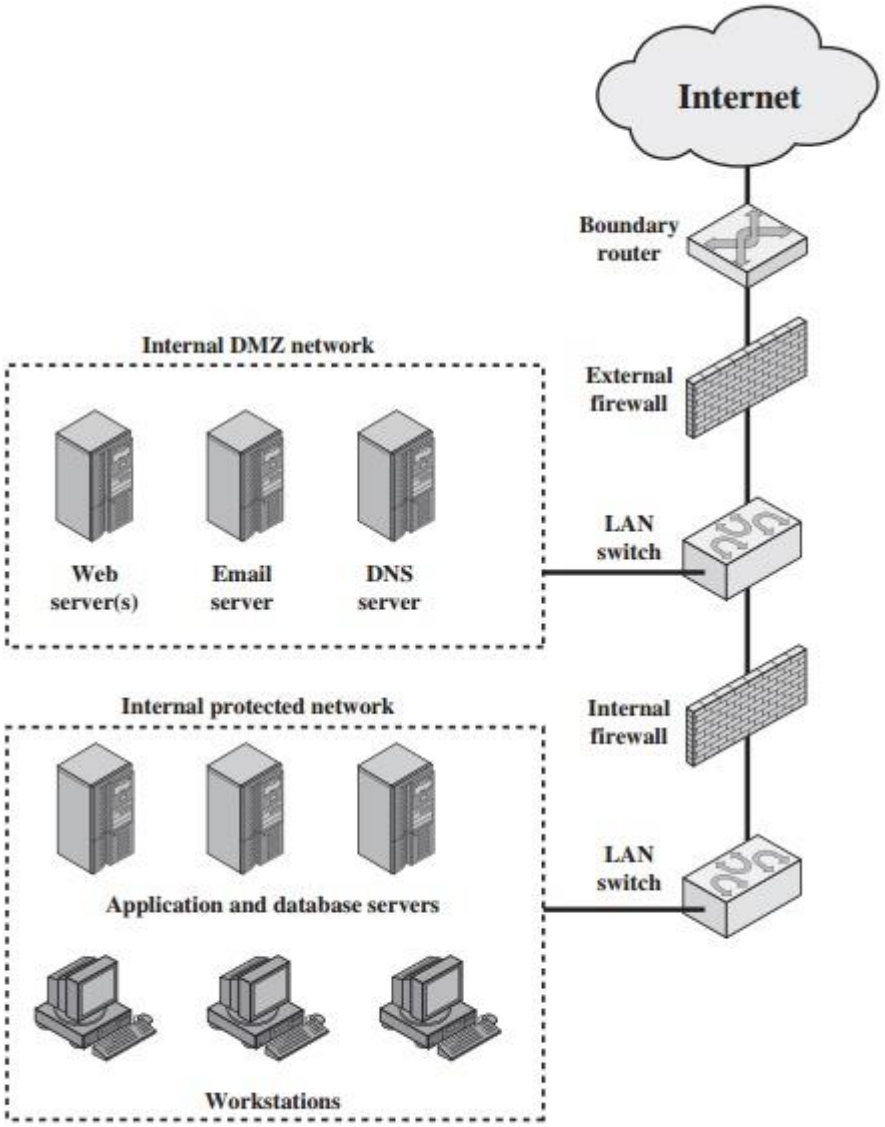


Figure 22.3 Example Firewall Configuration

Unified Threat Management (UTM)

Unified Threat Management (UTM) is the process to tackle the attacks and malware threats on a network.

Purpose of UTM

1. It Known as a Next-Generation Firewall (NGFW).
2. Provide Multiple Security Features into a single device.
3. UTM is also used by service providers for spam email detection, intrusions, filtering traffic, managing devices on the network.

UTM brands (Product) are

- Cisco
- Fortinet
- Sophos
- Netgear
- Huawei
- SonicWall

Examples (Features) of Unified threat management

- Antivirus software
- Firewalls
- Spam Email Detection
- Intrusion Detection
- Leak Prevention
- Anti-Malware
- Virtual Private Network(VPN)

Firewall

1. Network Security Device
2. Prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks.
3. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.
4. Firewalls prevent unauthorized access to networks through software or firmware.

"System which analyzes the filters incoming or outgoing data packet based on pre defined rules".

1. **Hardware Firewall-**Example Broadband Router
2. **Software Firewall-** Called System Firewall

Types of Firewalls

1. Packet Filtering
2. Circuit-level gateways
3. Application Layer Firewalls
4. Cloud Firewall
5. Next-generation Firewalls (NGFW)

Firewall Characteristics

1. Wireless network (Wi-fi) Protection
2. Various protection levels
3. Internet and network access
4. Protection against malware
5. Provide access only to valid data packets
6. Blockage against unauthorized access
7. Allowing to pass authorized traffic that fulfils a set of rules
8. Provision of numerous security policies

Limitations of Firewall

1. Firewalls cannot prevent misuse of passwords.
2. Firewalls cannot secure the system which is already infected.
3. Firewalls cannot stop users from accessing malicious websites.
4. Firewalls cannot protect against the transfer of virus-infected files or software
5. Firewalls cannot protect if security rules are misconfigured.
6. Higher Cost

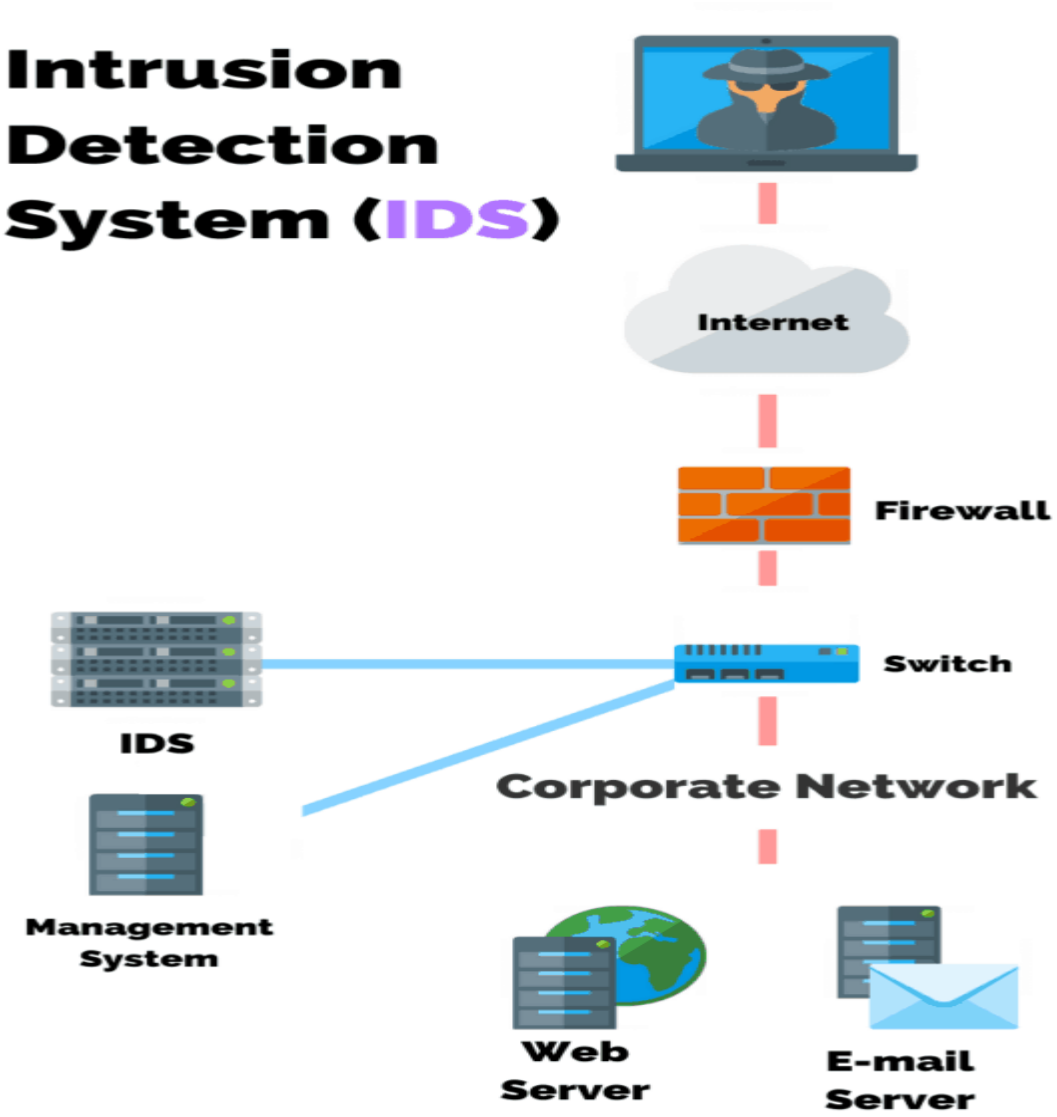
Intrusion Detection System (IDS)	Intrusion Prevention System (IPS)
It is Monitoring System	It is Control System
Only Detect ,Not Prevent	Detect and Prevent
It Need Human or System check the output	Regular Update on database
Not Effect the System Performance	Slow Down Network Performance
Alerting Product	Blocking Product
Detecting Hacking Attacks	Blocking Web Defacement

Intrusion Detection System (IDS)

IDS is used to monitor a network, which then sends alerts when suspicious events on a system or network are detected

1. Network Security
2. Not Effect the System Performance

Intrusion Detection System (IDS) Describes a suspected intrusion once it has happened and then signals on alarm.



An intrusion detection system (IDS) is a device, typically another separate computer that monitors activity to identify malicious or suspicious events.

Method of Intrusion Detection System (IDS)

1. **Signature Based**
2. **Anomaly Based**

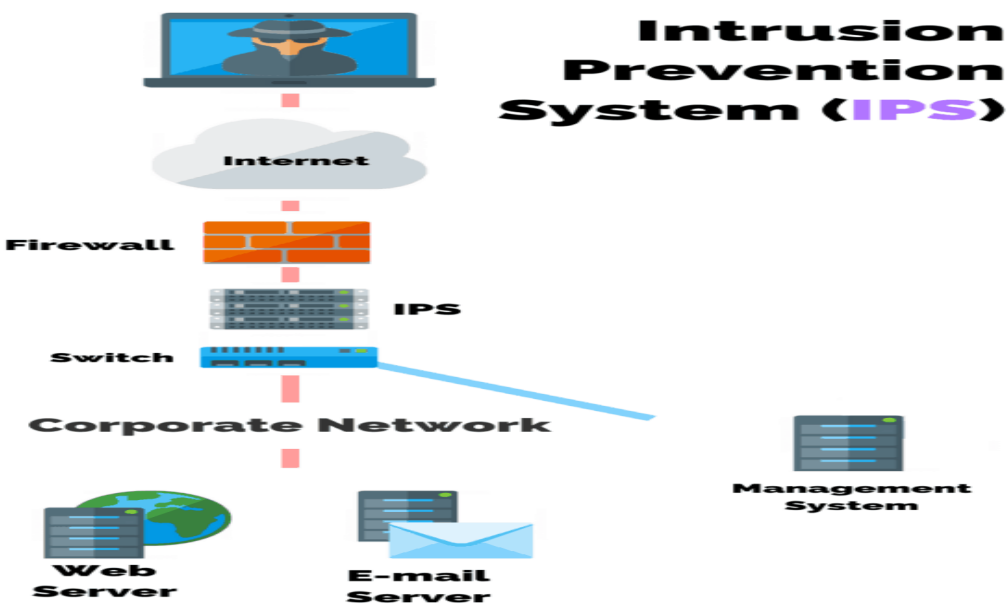
Signature Based	Anomaly Based
Pattern No. of Bytes, 1 and 0	Machine Learning Based Method
Not Detect New Malware	Detect New Malware.
Easily Detect whose Pattern Already Exists	Campare with Model
Slow speed	Fast Speed

Intrusion Prevention System (IPS)

1. Network Security

2. Slow down Network Performance

Intrusion prevention systems (IPS) perform intrusion detection and then go one step ahead and stop any detected threats.



Unit 2

Access Control

Access Control is a data security that enables organization to manage who is authorized to access corporate data and resources.

It is the ability to limit and control the access to host systems and applications via communication links. For this, each entity trying to gain access must first be identified or authenticated, so that access rights can be tailored to the individuals.

Access control systems perform identification, authentication, and authorization of users and entities by evaluating required login credentials that may include passwords, pins, bio-metric scans or other authentication factors.

Access control is a data security procedure that allows organizations to handle who is authorized to access corporate information and resources.

Physical access control: limits access to campuses, building and other physical assets,

Example a proximity card to unlock a door.

Logical access control: limits access to computers, networks, files and other sensitive data.

Example Username and password.

Principles of access control

Three elements (Principles) make up access control: 1.**Identification 2. Authentication 3. Authorization**

There are four main types of access control

Discretionary access control (DAC): In this method, the owner or administrator of the protected system, data, or resource sets the policies for who is allowed access.

Mandatory access control (MAC): In this nondiscretionary model, people are granted access based on an information clearance. A central authority regulates access rights based on different security levels. This model is common in government and military environments.

Role-based access control (RBAC): RBAC grants access based on defined business functions rather than the individual user's identity. The goal is to provide users with access only to data that's been deemed necessary for their roles within the organization. This widely used method is based on a complex combination of role assignments, authorizations, and permissions.

Attribute-based access control (ABAC): In this dynamic method, access is based on a set of attributes and environmental conditions, such as time of day and location, assigned to both users and resources.

Mobile Communication

1 G

- Start Year 1970
- Deployment Year 1980
- Analog Technology
- Voice Call
- 2kbps

2 G

- Start Year 1980
- Deployment Year 1999
- Digital Technology
- Voice Call and Data
- 64kbps

3 G

- Start Year 1990
- Deployment Year 2002
- CDMA Technology
- Voice Call and Data
- 1 mbps to 2 mbps

4 G

- Start Year 2000
- Deployment Year 2009
- WiMax,LTA Technology
- Voice Call ,Data, Video conferencing
- 100 mbps to 1 gbps

5 G

- Start Year 2018
- Deployment Year 2022
- MIMO Technology
- Voice Call ,Data, Video conferencing
- 1 gbps to 20 gbps

Internet speed of NASA 91 gigabits per second

Internet speed of ISRO(India) 14 gigabits per second

Call Rate From 1990 to 2022

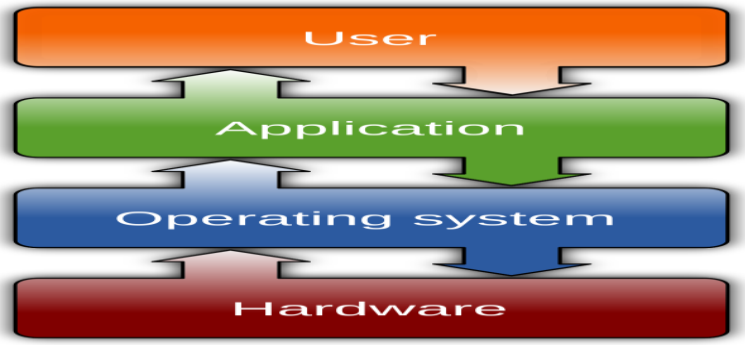
1995 17 Rupees call Charge +SMS Charge Extra

2001 Local 1.80 Rupees/Min

STD Call 3.20 Rupees/Min

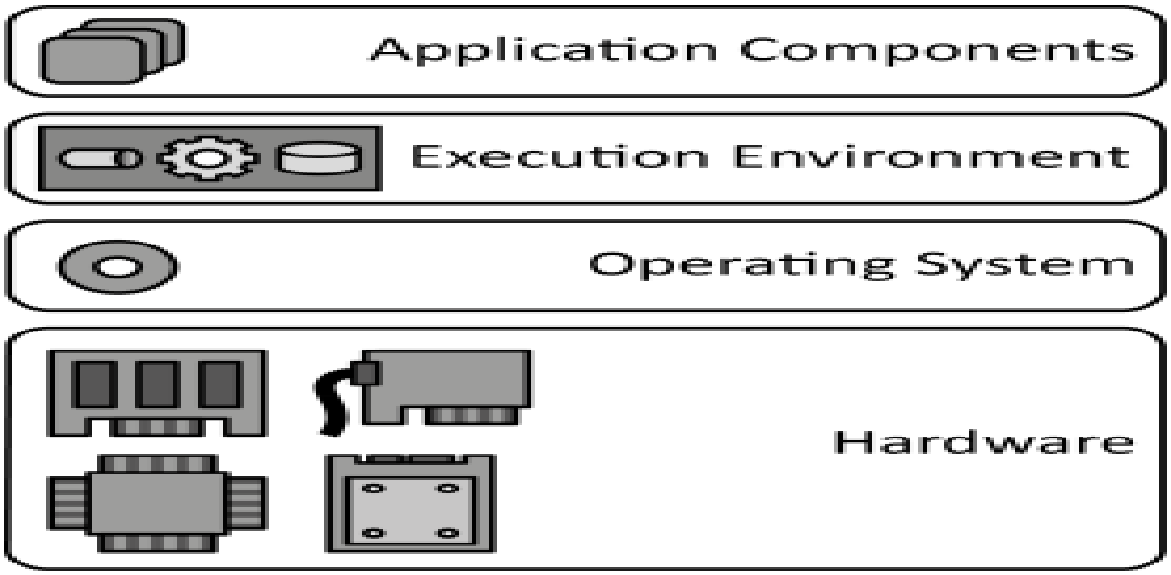
2022 Unlimited Call +100 SMS

Operating Systems and Execution EnvironmentsOperating Systems



Operating Systems and Execution Environment

1. **Data Storage**
2. **Communication**



Trusted Execution Enviíonment (TEE)

1. Security perimeter
2. Only trusted code Execute

Un-Trusted Execution Enviíonment (UEE)

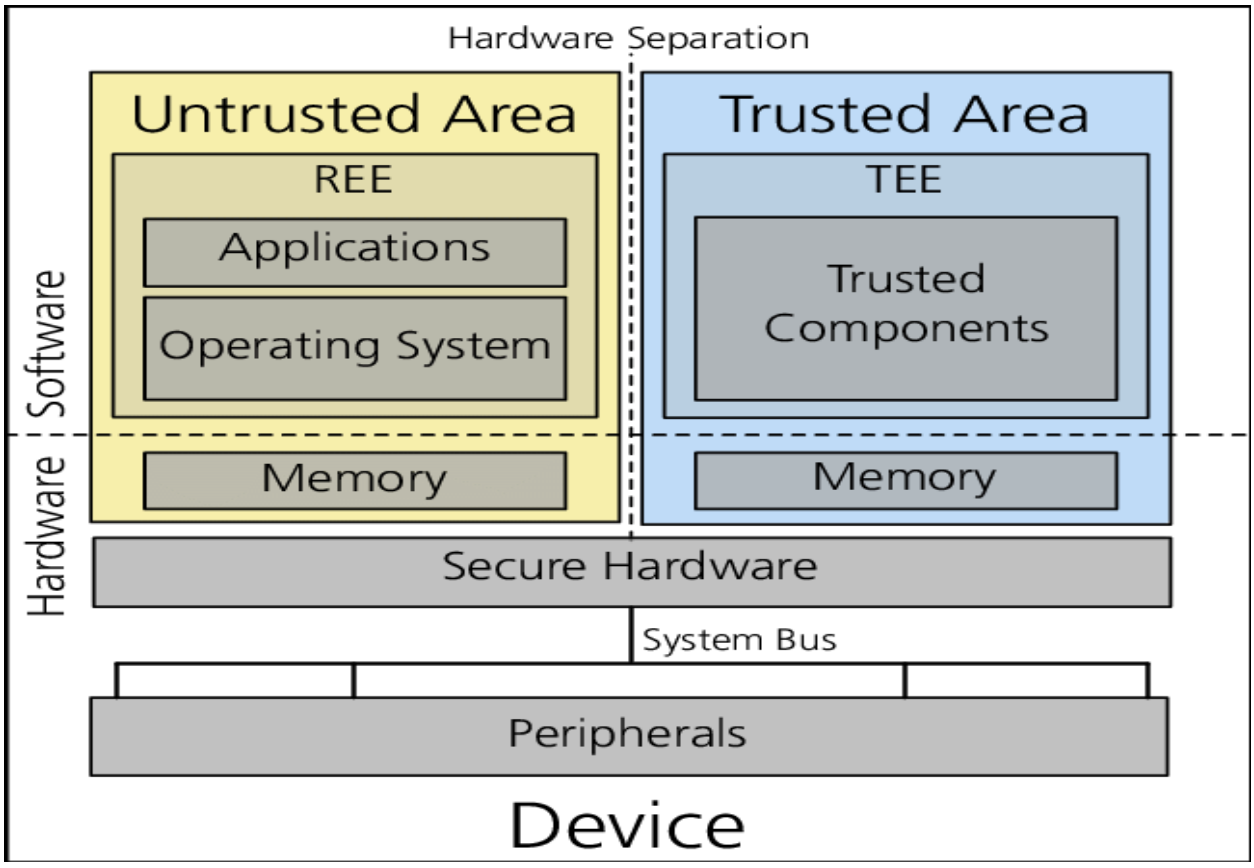
1. Only untrusted code Execute

Embedded operating systems (EOS)

1. Embedded operating systems are designed to be used in embedded computer systems.
2. They are very compact
3. Operate with a limited number of resources
4. Extremely efficient

Tiny operating systems (Tiny OS)

1. Tiny OS is an open-source
2. Flexible and
3. Application-specific operating system
4. Large number of tiny are Used
5. Low-power nodes



Computer security (IT security)

The meaning of the term computer security has evolved in recent years. Before the problem of data security became widely publicized in the media, most people's idea of computer security focused on the physical machine. Traditionally, computer facilities have been physically protected for three reasons:

- To prevent theft of or damage to the hardware
- To prevent theft of or damage to the information
- To prevent disruption of service

Computer security is security applied to computing devices such as computers and smartphones.

Cyber Crime

A cybercrime is a crime that involves a computer or a computer network.The computer may have been used in committing the crime, or it may be the target. Cybercrime may harm someone's security or finances

Example

Email and internet fraud 2. **Phishing scams 3. Online harassment and cyber stalking**

Top 10 Cyber Crime Prevention Tips

1. Use Strong Passwords
2. Secure your computer
3. Be Social-Media Savvy
4. Secure your Mobile Devices.
5. Install the latest operating system updates
6. Protect your Data
7. Secure your wireless network
8. Protect your e-identity
9. Avoid being scammed
10. Call the right person for help

Real-Time Payments

RTP (Real-Time Payments) is a payment processing network used to send money electronically between banks in the United States

Real-Time Payments (RTP) are payments that are initiated and settled nearly instantaneously

Real-Time Payment networks provide 24x7x365 access, which means they are always online to process transfers. This includes weekends and holidays.

List of TOP 5 Countries Highest Payment in Real Time Payment

1. India 2.china 3.Thailand 4.South Korea 5.UK

List of TOP 3 Countries Highest Mobile Phone User

1. China 2. India 3.USA

Digital Payments or E-Payment

- Digital Payment, Sometimes called an Electronic payment
- An E-payment or Electronic Payment system allows customers to pay for the services via electronic methods.
- Without the use of Paper.
- Digital payments are transactions that take place via digital or online modes, with no physical exchange of money involved.

1 Banking Cards

Indians widely use Banking cards, or debit/credit cards, or prepaid cards

2 Unified Payments Interface (UPI)

3 Mobile Wallets

Some popularly used ones include Paytm, Freecharge, Mobikwik, mRupee, Vodafone M-Pesa, Airtel Money, Jio Money, SBI Buddy, Vodafone M-Pesa, Axis Bank Lime, ICICI Pockets, etc.

4 PoS Terminals

PoS(Point of Sale) is known as the location or segment where a sale happens.

5 Internet Banking

NEFT, RTGS, or IMPS are some of the top ways to make transactions via internet banking.

6 Mobile Banking

Digital payment methods, such as IMPS, NEFT, RTGS, IMPS

7 Micro ATMs

List of TOP 5 Countries Highest E-Payment Transaction

1. japan 2.USA 3.India 4.Singapore 5.Indonesia