Network Security Aspects

❖ Security Basics

Network Security refers to the measures taken by any enterprise or organization to secure its computer network and data using both hardware and software systems. This aims at securing the confidentiality and accessibility of the data and network. Every company or organization that handles a large amount of data, has a degree of solutions against many cyber threats.

❖ Benefits of Network Security

Network Security has several benefits, some of which are mentioned below:

1. Network Security helps in protecting clients' information and data which ensures reliable access and helps in protecting the data from cyber threats.
2. Network Security protects the organization from heavy losses that may have occurred from data loss or any security incident.
3. It overall protects the reputation of the organization as it protects the data and confidential items.

❖ Working on Network Security

The basic principle of network security is protecting huge stored data and networks in layers that ensure the bedding of rules and regulations that have to be acknowledged before performing any activity on the data. These levels are:

1. Physical Network Security
2. Technical Network Security
3. Administrative Network Security

These are explained below:

1. Physical Network Security: This is the most basic level that includes protecting the data and network through unauthorized personnel from acquiring control over the confidentiality of the network. These include external peripherals and routers that might be used for cable connections. The same can be achieved by using devices like biometric systems.
2. Technical Network Security: It primarily focuses on protecting the data stored in the network or data involved in transitions through the network. This type serves two purposes. One is protected from unauthorized users, and the other is protected from malicious activities.
3. Administrative Network Security: This level of network security protects user behavior like how the permission has been granted and how the authorization process takes place. This also ensures the level of sophistication the network might need for protecting it through all the attacks. This level also suggests necessary amendments that have to be done to the infrastructure.

❖ Types of Network Security

The few types of network securities are discussed below:

1. Access Control
2. Antivirus and Anti-Malware Software
3. Cloud Security
4. Email Security
5. Firewalls
6. Application Security
7. Intrusion Prevention System(IPS)

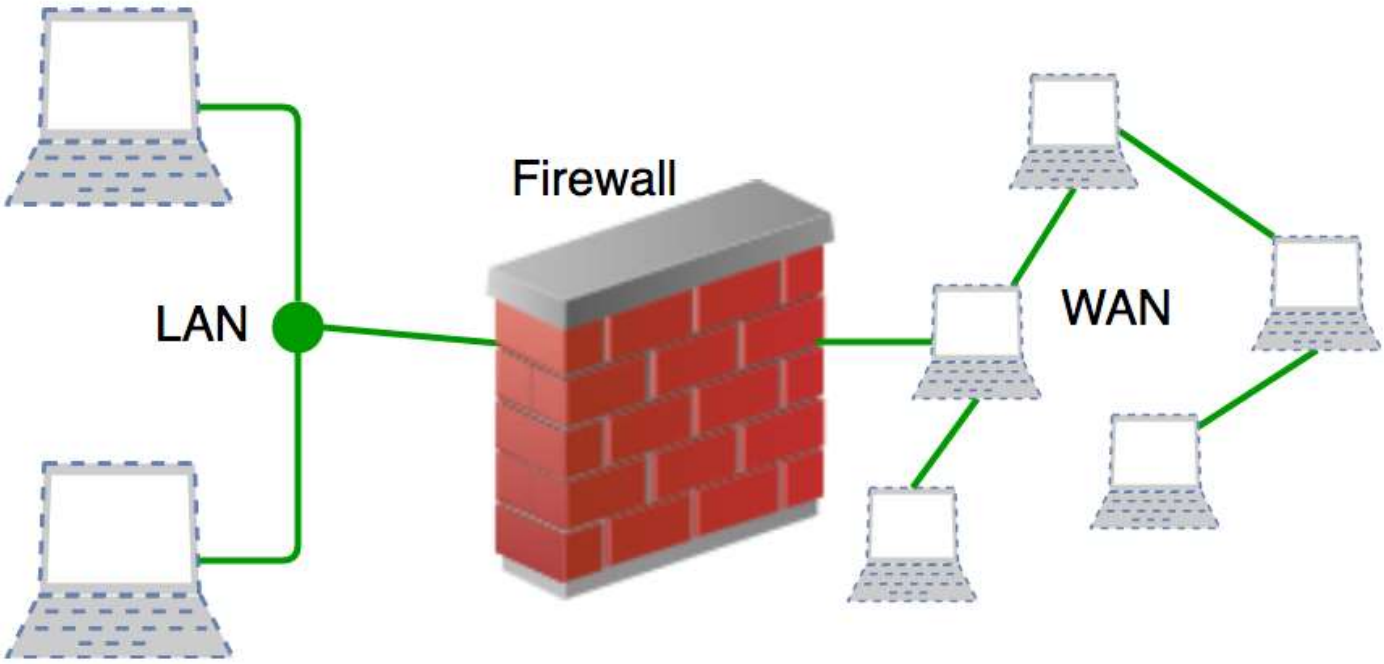
1. **Access Control:** Not every person should have a complete allowance for the accessibility to the network or its data. One way to examine this is by going through each personnel's details. This is done through Network Access Control which ensures that only a handful of authorized personnel must be able to work with the allowed amount of resources.

2. **Antivirus and Anti-malware Software:** This type of network security ensures that any malicious software does not enter the network and jeopardize the security of the data. Malicious software like Viruses, Trojans, and Worms is handled by the same. This ensures that not only the entry of the malware is protected but also that the system is well-equipped to fight once it has entered.

3. **Cloud Security:** Now a day, a lot of many organizations are joining hands with cloud technology where a large amount of important data is stored over the internet. This is very vulnerable to the malpractices that few unauthorized dealers might pertain to. This data must be protected and it should be ensured that this protection is not jeopardized by anything. Many businesses embrace SaaS applications for providing some of their employees the allowance of accessing the data stored in the cloud. This type of security ensures creating gaps in the visibility of the data.

4. **Email Security**: Email Security depicts the services, and products designed to protect the Email Account and its contents safe from external threats. For Example, you generally see, fraud emails are automatically sent to the Spam folder. because most email service providers have built-in features to protect the content.

5. **Firewalls:** A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules accepts, rejects, or drops that specific traffic. Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers.



- **Behavioral analytics:** This method analyses network behaviour and detects and alerts organizations for abnormal activity.

6. **Intrusion Prevention System (IPS):** An intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity. The major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it, and attempt to block or stop it.

❖ Confidentiality

- Confidentiality is the protection of information in the system so that an unauthorized person cannot access it. This type of protection is most important in military and government organizations that need to keep plans and capabilities secret from enemies.
- However, it can also be useful to businesses that need to protect their proprietary trade secrets from competitors or prevent unauthorized persons from accessing the company's sensitive information (e.g., legal, personal, or medical information). Privacy issues have gained an increasing amount of attention in the past few years, placing the importance of confidentiality on protecting personal information maintained in automated systems by both government agencies and private-sector organizations.
- Confidentiality must be well-defined, and procedures for maintaining confidentiality must be carefully implemented. A crucial aspect of confidentiality is user identification and authentication. Positive identification of each system user is essential in order to ensure the effectiveness of policies that specify who is allowed access to which data items.

Threats to Confidentiality: Confidentiality can be compromised in several ways. The following are some of the commonly encountered threats to information confidentiality

- Hackers
- Unauthorized user activity
- Unprotected downloaded files
- Local area networks (LANs)
- Trojan Horses

❖ INTEGRITY:

In the world of information security, integrity refers to the accuracy and completeness of data. Security controls focused on integrity are designed to prevent data from being modified or misused by an unauthorized party. Integrity involves maintaining the consistency and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and precautionary steps must be taken to ensure that data cannot be altered by unauthorized people.

For example, in a data breach that compromises integrity, a hacker may seize data and modify it before sending it on to the intended recipient.

Some security controls designed to maintain the integrity of information include:

1. Encryption
2. User access controls
3. Version control
4. Backup and recovery procedures
5. Error detection software

❖ Availability

Data availability means that information is accessible to authorized users. It provides an assurance that your system and data can be accessed by authenticated users whenever they're needed. Similar to confidentiality and integrity, availability also holds great value.

Availability is typically associated with reliability and system uptime, which can be impacted by non-malicious issues like hardware failures, unscheduled software downtime, and human error, or malicious issues like cyberattacks and insider threats. If the network goes down unexpectedly, users will not be able to access essential data and applications. Information security policies and security controls address availability concerns by putting various backups and redundancies in place to ensure continuous uptime and business continuity.

Your information is more vulnerable to data availability threats than the other two components in the CIA model. Making regular off-site backups can limit the damage caused to hard drives by natural disasters or server failure. Information only has value if the right people can access it at the right time.

Information security measures for mitigating threats to data availability include:

1. Off-site backups
2. Disaster recovery
3. Redundancy
4. Failover
5. Proper monitoring
6. Environmental controls
7. Virtualization
8. Server clustering
9. Continuity of operations planning

THREATS TO SECURITY:

A network threat is a threat to your network and data systems. Any attempt to breach your network and gain access to your data is considered a network threat.

There are different kinds of network threats, and each has a different goal. Some, like distributed denial-of-service (DDoS) attacks, seek to shut down your network or servers by overloading them with requests. While others, such as malware or credential theft, aim to steal your data, spyware will enter your organization's network, where it will lie in wait and collect data.

A security threat Is a malicious act that corrupts or steals data or disrupts the operations of an organization.

❖ Categories of Network Security Threats

Network security threats can be categorized into four main categories:

1. External threats: A network has an external threat when it is caused by an external entity, a person, or even a natural disaster that could negatively disrupt the network. It involves exploiting a weakness, or vulnerability, or causing a loss of data that significantly affects your business operations and network security.

2. Internal threats: This type of threat is posed by malicious insiders, such as disgruntled or improperly vetted employees who are working for a competitor. According to a report from Cybersecurity Insiders published in 2022, 57% of organizations believe that insider attacks have Become more frequent in the recent past.

3. Structured threats: The term structured threats refer to attacks conducted by organized groups of cybercriminals with a clear objective or goal in mind, such as state-sponsored attacks

4. Unstructured attacks: Attacks that are unstructured usually originate from amateurs who de not have a clear objective in mind.

❖ Viruses

A virus is a software programs or pieces of code that is capable of copying itself and infecting a system without the knowledge of the user.

It is a type of malware that spreads from of Computer to another cleaning up its trails as it goes. It can harm other software programs Modifying them and it is a type of malware.

Generally, viruses are attached to the executable (exe) files and when user runs that program viruses spread in the system. They may create mild effects and can cause crash of data software may cause denial-of-service attack. Viruses may infect memory, a floppy disk, a t drive, a backup tape, or any other type of storage.

Types of viruses are as under:

1. Parasitic Virus.
2. Memory Resident Virus.
3. Boot sector Virus.
4. Stealth Virus.
5. Metamorphic Virus.
6. Macro Virus.
7. Resident Virus
8. Multipartite Virus
9. Direct Action
10. Browser Hijacker

The following are the harmful effects of viruses:

1. Erase data
2. Can even control your device

3. Track your keystrokes
4. Hack password or data
5. Damage the hard disk permanently
6. Spam your email list
7. Corrupted files

❖ WORMS

A computer worm is a subset of the Trojan horse malware that can propagate or self-replicate from one computer to another without human activation after breaching a system. Typically, a worm spreads across a network through your internet or LAN (Local Area Network) connection. It does not require any host to spread. Worms can be remorselessly destructive.

Types of Worms are as under

1. P2P-Worm 2. Net-Worm
2. Email-Worm
3. IRC(Internet Relay Chat) –Worm
4. File sharing Worms
5. IM (Instant Messaging) – Worm

The following are the harmful effects of Worms:

1. Performance issues
2. Identity theft can even be caused by worms
3. Delete or change our files
4. Keep us out of important files
5. Hard drive reformatting

Here are some tips on preventing worms:

1. Keep your files safe
2. Update your passwords
3. Software should be updated regularly
4. Use a VPN for torrenting
5. Open attachments and links with caution
6. While browsing, avoid pop-up ads

❖ INTRUDERS

"Intrude" means to put oneself purposefully (intentionally) into a situation or place where one is not welcome or invited. An intruder is unauthorized individual trying to access resources illegally. The main aim of intruders is to gain access to the system and intrude the privacy of the network. Intruders may be insiders or may be outsiders. Intruders' attacks range from the gentle to the serious one. Intruders are mainly classified into three categories:

1. Masquerade: An individual who is not authorized to use the computer but he gets access to the computer system and exploit (misuse or take advantage of) user data and account.
2. Misfeasor: A legal user who accesses data, programs or resources for which he is not authorized.
3. Clandestine user: User who gains administrative access to the system. The masquerade is likely to be an outsider, the misfeasor generally is an insider and clandestine user can be either insider or outsider.

The risk of network intrusion

1. Corruption of Data
2. Financial Loss for the Organization
3. Theft of Data
4. Loss of Reputation
5. Operational Disruption

The following methods are used by hackers to crack passwords:

1. The default password should unlock the system if no changes have been made by the user.
2. Try all possible short passwords to gain access to the system
3. In order to unlock the system, various combinations must be entered, including the user's name, the names of family members, the user's address, and the user's telephone number.
4. Accessing the user's system with Trojan horses.
5. By using the host's connection gateway, you can access the remote user's connection.

What's the best way to detect network intrusions?

- Host Intrusion Detection System (HIDS)
- Application Protocol-based Intrusion Detection System (APIDS)
- Protocol-based Intrusion Detection System (PIDS)
- Network Intrusion Detection System (NIDS)

❖ **INSIDERS**

An insider threat is a malicious threat to an organization that comes from people within the Organization. Insider attacks are typically passive attacks that are harder to detect because they are carried Out by employees, former employees, contractors, partners, or business associates who have inside information about an organization's data, computer systems, and security, Insiders are More dangerous than outside intruders.

Threats related to Insiders:

1. Fraud
2. Theft of confidential information. 3. Theft of intelligent property.
3. Damage of computer system.
4. Corruption, including participation in transnational organized crime

Damages caused by Insiders:

1. Loss of critical data
2. Financial Impact
3. Legal Impact
4. Loss of Reputation
5. Loss of Competitive Edge
6. Intellectual Property Theft
7. Market Value Reduction
8. Increased Expenses

The following steps will help reduce the risk of insider threats:

1. Protect critical assets
2. Enforce policies
3. Increase visibility
4. Promote culture changes
5. Encryption of data

CRIMINAL ORGANIZATIONS

Due to increasing the computer networks and internet uses, criminal organizations turn into the electronic world to misuse.

One difference between criminal group and the "average" hacker is the level of organization is much higher than a simple hacker. They have more money and financial supports compare with hackers. They are done by great amount of planning, a longer period of time to conduct the activity, more financial banking to complete it.

Activities done by Criminal Organizations:

1. Theft of user accounts
2. Blackmail
3. Faking
4. Theft of important credentials
5. Financial fraud

What can be done to prevent cyber-crimes committed by criminal organizations?

1. Updating and enforcing concrete security
2. Keep your personal information private
3. Anti-cybercrime settings 5. Using antivirus software
4. Keep your information secure when visiting unauthorized sites
5. Use virtual private networks B. Keeping your most valuable data secure
6. Back up all data and considerations

❖ TERRORISTS

A cyber terrorist uses Internet networks to conduct violent incidents, such as loss of life or data, to gain political advantage by giving threats to the community. To accomplish their goals, hackers use computer viruses, spyware, malware, ransomware, phishing, and programming language Scripts.

Cyber terrorists might have ethical or religious reasons for wanting to terrorize and others do It for personal reason. Cyber terrorism is sometimes referred to as electronic terrorism or information war.

The following are the Harm caused by Terrorists:

1. Violence
2. Service disruptions
3. Physical damages
4. Psychosocial impacts
5. Economic damages
6. Data breaches:

How to prevent Cyber Terrorism:

1. Ensure all devices are protected with Antivirus
2. Set up multi-factor authentication
3. Choose strong passwords
4. Avoid Phishing scams
5. Shop at safe websites
6. Check website URL

❖ INFORMATION WARFARE

Information warfare is the use and management of information and communication technology (ICT) in order to obtain a competitive advantage over a competitor. It's actually a war against the enemy's information and information processing equipment. Information warfare is also known as cyber warfare, electronic warfare, and cyberattack.

Information warfare targets water, electricity, oil and gas refineries and distribution, banking and Finance, and telecommunications.

Following are seven types of Information Warfare attack

1. Espionage
2. Sabotage
3. Denial-of-service (DoS) Attacks
4. Electrical Power Grid
5. Propaganda Attacks
6. Economic Disruption
7. Surprise Attacks

How to prevent Information Warfare:

1. Mail fence.
2. Digitally sign your emails with OpenPGP signatures to further secure your messages
3. Use of a virtual machine.

Define Firewall.

Firewalls

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.

A firewall is essentially the barrier that sits between a private internal network and the public Internet.

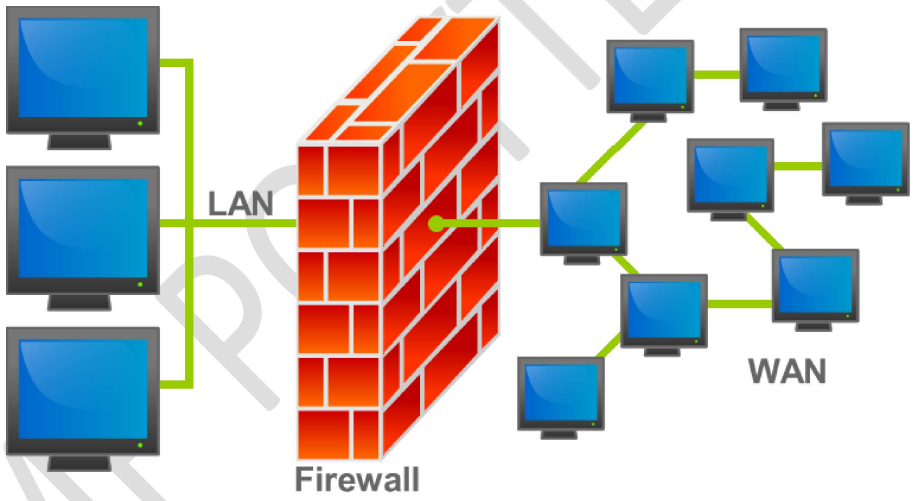
A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.

It is cybersecurity tool that filters network traffic and prevents malicious software from accessing internet on a computer that is infected.

Firewall can be a network security device or software program on a computer .firewall is available in both software and hardware formats.

A hardware firewall is a physical device that set between a computer network and a gateway such as a broadband router.

A software firewall is a simple program installed on computer that's checks port numbers and controls other applications.



Need of firewall

1. Main purpose of firewalls is to prevent malware and network attacks.
2. Preventing application layer attacks acts as a gate keeper.
3. The primary purpose of a firewall is to check if traffic or an incoming connection meets a predefined set of security standards, which is critical for internet security. A good firewall tool can help you adjust the firewall's settings to your needs.

History of firewall

1988---- Packet filter firewall

1989----AT & T Bell labs.—Stateful firewall

1991—DEC –Application layer firewall

1994--- First of stateful firewall appear

2004--- IDC coins the term, Unified Threat Management (UTM)

2009---Next Generation Firewall (NGFW)

Explain firewall with its types and characteristics.

Types of Firewalls

1. **Packet filtering firewall**
   Data is analyzed and distributed in accordance with standard of filter.
2. **Proxy service**
   Network security system that protects and filter message the application layer.
3. **Stateful inspection**
   With dynamic packet filtering, firewall determine which packets should be allowed through based on status of active connection.
4. **Next Generation Firewall(NGFW)**
   Deep Packet inspection firewall with application level inspection.

Firewall can be categorized according to its ability to filter communication between a single node and network or between two or more network

1. Personal firewall
2. Network firewall

Firewall can be classified according to whether they keep track of status of network connections or not

1. Stateful firewall
2. Stateless firewall

Characteristics of firewalls

Major characteristics related to firewall protection are described below.

a. Various protection levels
b. Wireless network (Wi-Fi) Protection
c. Internet and network access
d. Blockage against unauthorized access
e. Protection against malware
f. Provide access only to valid data packets
g. Provision of different configurations
h. Provision of numerous security policies

i. Allowing to pass authorized traffic that fulfils a set of rules
j. Firewall functions like an immune system for malware and unauthorized access; therefore, it ensures a secure system and an OS.

List out advantages and disadvantages of firewall.

Advantages of Firewall

1. Promotes Privacy and Security

Firewalls may play a vital role in corporate security management. It offers enhanced security and privacy from vulnerable services. It stops unauthorized users from accessing a private network that is linked to the Internet. It keeps your data safe and secure. Corporations spend millions of money on protecting their system from outside malware attacks.

2. Monitors Network Traffic

The firewall monitors the data from where it comes in and out of your system. It gives faster response time and the ability to manage larger traffic loads. This regulation has predetermined rules and associated filters. A well-equipped and trained team can provide security to your system based on incoming and outgoing data from the firewall.

3. Prevent Virus Attack

Virus attacks are very dangerous for the computer system, and they could close down all digital operations quickly. Millions of new threats develop every day, and it becomes important to put our guard strong.

It can update its security protocols from a single authorized device. It secures your system from a phishing attack. A firewall can prevent a hacker entirely or deter them from becoming easy targets. Firewalls serve as an important blockade against malicious programs and spyware. It helps you to keep your data safe from the external

Disadvantages of Firewall

1. User Restriction

It is an undisputed fact that a firewall secures the system from unauthorized access, but the firewall is more advantageous to the single user but ineffective for the organization. It damages the organization's productivity and forces the employees to undertake shortcuts, which can lead to serious compromises with security. Employees are not permitted to perform a certain function that is not part of the policies used by the firewall.

2. Cost

Firewall cost depends upon the type of installation. Hardware Firewall is more expensive than software firewalls because for the installation, hardware firewall requires an expert IT professional, and its maintenance is also costly. On another side, an average user can install software firewalls easily.

3. Complex Operations

It becomes very difficult for a large organization to bear the huge maintenance cost of the firewall. A firewall is very efficient in individual cases. A separate team has to be constituted for the firewall's operation and to ensure the other networks remain secure from intrusion. It gives rise to an additional financial burden on the organization.

4. Malware Attack

A firewall secures the system from the simple type of trojans. It cannot secure the system from sophisticated malware that can enter the system in the form of trusted data. This requires installing powerful, sophisticated, and effective anti-malware for quick action.

5. Effect on the Performance

The computer system's performance is affected by the usage of software firewalls. It is a known fact that the RAM (Random Access Memory) and processing power have a vital and important role in giving a good performance, but when a firewall runs in the background, it draws more power from the RAM and processing power. This has an overall impact on the performance of the system.

Explain limitations of firewall.

Limitations of Firewall

- Firewalls cannot prevent misuse of passwords.
- Firewalls cannot protect if security rules are misconfigured.
- Firewalls cannot protect against non-technical security risks, such as social engineering.
- Firewalls cannot stop or prevent attackers with modems from dialing in to or out of the internal network.
- System that are already infected cannot be protected by firewalls

Write a short note on real –time application of firewall.

Real Time Applications of firewall

1. Corporate network: Firewalls allow authorized users to access particular resources or services and block traffic from specific IP address or networks.
2. Government organizations: It is possible that they will make use of cutting edge fire walls such as Next Generation Firewalls (NGFW), which are capable of detecting and stopping instruction as well as managing access to specific apps and data.
3. Service providers: ISPs, cloud service provider and hosting companies use firewalls to safeguard their networks and data of their customers.

4. Small enterprises: These firms may use firewall to separate their internal networks, restrict access to specific applications and resources and protect their networks against external threats.
5. Industrial Control System (ICS): In power plants, water treatment facilities and transportation systems firewall protect control system against unauthorized access and cyber-attacks.

Explain working of firewall.

Working of firewall:

- Firewall system analyzes network traffic according to pre-defined rules. It then filters the traffic and prevents any unreliable or suspicious traffic.
- As a security measure, firewall can allow or block data packets on predefined security rules. Incoming traffic is allowed only via trusted IP addresses, or sources.
- It distinguishes between positive and malicious traffic and either allows or blocks specific data packets according to pre-established security rules.
- Several aspects of packet data are taken into account when deciding these rules such as the sources, destination and content of packet.

Write a short note on design principles of firewall.

Design principles:

1. Design security policy: In firewall design, security policies play a crucial role in identifying what traffic can pass through the firewall. Security policies are created in accordance with the company's or client's requirements. When a security policy is developed properly, it includes instructions for what to do in the event of a security breach. Without it, there is an increase in risk, as security solutions will not be implemented properly.
2. Design of simple solutions: It is difficult to implement a complex solution. If the solution is easy to implement, it is easier to maintain. It is possible to make upgrades to the simple design in response to the new possible threats. The problem with complex design is that they can lead to configuration errors which can open the door to external attacks.
3. Choose the location of the firewalls: It is important to determine the location of your firewall in a strategic manner. In order to order to secure your internal network from your web server, you can use a packet filter firewall at the edge of your network.
4. Selecting the right device: The network becomes vulnerable if we use the wrong device for wrong problem. For example, if and outdated device is used for creating a firewall, the network becomes vulnerable.
5. Adequate throughput: Filters and processing information can significantly reduce throughput, so if you opt for NGFWs choose those that offer at least one gigabit of throughput, which is sufficient for most organizations.
6. Choose a firewall philosophy: All firewall design principles in cybersecurity depends on identification of applications, resources and services that you wish to protect.
7. Be aware of internal threats: The security of a network or device is well protected from external attacks. However, security is weak when attacks are carried out internally as it is easy to gain access to and poorly designed.

8. Communicate according to your preferences: A security policy specifies which people, device and applications are allowed to access your organization's web services and use your network.