**Firewall Design Principles**

A **Firewall** is hardware or software to prevent a private computer or a network of computers from, it acts as a filter to avoid unauthorized users from accessing private computers and networks. It is a vital component of network security. It is the first line of defense for network security. It filters network packets and stops malware from entering the user’s computer or network by blocking access and preventing the user from being infected.

**Characteristics of Firewall**

1. **Physical Barrier:**A firewall does not allow any external traffic to enter a system or a network without its allowance. A firewall creates a choke point for all the external data trying to enter into the system or network and hence can easily block the access if needed.
2. **Multi-Purpose:** A firewall has many functions other than security purposes. It configures domain names and [Internet Protocol](https://www.geeksforgeeks.org/types-of-internet-protocols/)(IP) addresses. It also acts as a network address translator. It can act as a meter for internet usage.
3. **Flexible Security Policies:** Different local systems or networks need different security policies. A firewall can be modified according to the requirement of the user by changing its security policies.
4. **Security Platform:** It provides a platform from which any alert to the issue related to security or fixing issues can be accessed. All the queries related to security can be kept under check from one place in a system or network.
5. **Access Handler:** Determines which traffic needs to flow first according to priority or can change for a particular network or system. specific action requests may be initiated and allowed to flow through the firewall.

**Need and Importance of Firewall Design Principles**

1. **Different Requirements:**Every local network or system has its threats and requirementswhich needs different structure and devices. All this can only be identified while designing a firewall. Accessing the current security outline of a company can help to create a better firewall design.
2. **Outlining Policies:** Once a firewall is being designed, a system or network doesn’t need to be secure. Some new threats can arise and if we have proper paperwork of policies then the security system can be modified again and the network will become more secure.
3. **Identifying Requirements:** While designing a firewall data related to threats, devices needed to be integrated, Missing resources, updating the security devices. All the information collected is combined to get the best results. Even if one of these things is misidentified leads to security issues.
4. **Setting Restrictions:** Every user has its limitations to access different level of data or modify it and it needed to be identified and taken action accordingly. After retrieving and processing data, priority is set to people, devices, and applications.
5. **Identify Deployment Location:** Every firewall has its strengths and to get the most use out of it, we need to deploy each of them at the right place in a system or network. In the case of a packet filter firewall, it needs to be deployed at the edge of your network in between the internal network and webserver to get the most out of it.

**Firewall Design Principles**

**1. Developing Security Policy**

Security policy is a very essential part of firewall design. Security policy is designed according to the requirement of the company or client to know which kind of traffic is allowed to pass. Without a proper security policy, it is impossible to restrict or allow a specific user or worker in a company network or anywhere else. A properly developed security policy also knows what to do in case of a [security breach](https://www.geeksforgeeks.org/top-5-information-security-breaches/). Without it, there is an increase in risk as there will not be a proper implementation of security solutions.

**2. Simple Solution Design**

If the design of the solution is complex. then it will be difficult to implement it. If the solution is easy. then it will be easier to implement it. A simple design is easier to maintain. we can make upgrades in the simple design according to the new possible threats leaving it with an efficient but more simple structure.  The problem that comes with complex designs is a configuration error that opens a path for external attacks.

**3. Choosing the Right Device**

Every network security device has its purpose and its way of implementation. if we use the wrong device for the wrong problem, the network becomes vulnerable. if the outdated device is used for a designing firewall, it exposes the network to risk and is almost useless. Firstly the designing part must be done then the product requirements must be found out, if the product is already available then it is tried to fit in a design that makes security weak.

**4. Layered Defense**

A network defense must be multiple layered in the modern world because if the security is broken, the network will be exposed to external attacks. Multilayer security design can be set to deal with different levels of threat. It gives an edge to the security design and finally neutralizes the attack over the system.

**5. Consider Internal Threats**

While giving a lot of attention to safeguarding the network or device from external attacks. The security becomes weak in case of internal attacks and most of the attacks are done internally as it is easy to access and designed weakly. Different levels can be set in network security while designing internal security. Filtering can be added to keep track of the traffic moving from lower-level security to higher level.

**Advantages of Firewall:**

1. **Blocks infected files:** While surfing the internet we encounter many unknown threats. Any friendly-looking file might have malware in it. The [firewall](https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/)neutralizes this kind of threat by blocking file access to the system.
2. **Stop unwanted visitors:** A firewall does not allow a cracker to break into the system through a network. A strong firewall detects the threat and then stops the possible loophole that can be used to penetrate through security into the system.
3. **Safeguard the IP address:** A network-based firewall like an internet connection firewall(ICF). Keeps track of the internet activities done on a network or a system and keeps the IP address hidden so that it can not be used to access sensitive information against the user.
4. **Prevents Email spamming:** In this too many emails are sent to the same address leading to the server crashing. A good firewall blocks the spammer source and prevents the server from crashing.
5. **Stops Spyware:** If a bug is implanted in a network or system it tracks all the data flowing and later uses it for the wrong purpose. A firewall keeps track of all the users accessing the system or network and if spyware is detected it disables it.

**Limitations:**

1. **Internal loose ends:**Firewall can not be deployed everywhere when it comes to internal attacks. Sometimes an attacker bypasses the firewall through a telephone lane that crosses paths with a data lane that carries the data packets or an employee who unwittingly cooperates with an external attacker.
2. **Infected Files:** In the modern world, we come across various kinds of files through emails or the internet. Most of the files are executable under the parameter of an operating system. It becomes impossible for the firewall to keep a track of all the files flowing through the system.
3. **Effective Cost:** As the requirements of a network or a system increase according to the level of threat increases. The cost of devices used to build the firewall increases. Even the maintenance cost of the firewall also increases. Making the overall cost of the firewall quite expensive.
4. **User Restriction:**Restrictions and rules implemented through a firewall make a network secure but they can make work less effective when it comes to a large organization or a company. Even to make a slight change in data can require a permit from a person of higher authority making work slow. The overall productivity drops because of all of this.
5. **System Performance:**A software-based firewall consumes a lot of resources of a system. Using the RAM and consuming the power supply leaves very less resources for the rest of the functions or programs. The performance of a system can experience a drop. On the other hand hardware firewall does not affect the performance of a system much, because its very less dependent on the system resources.