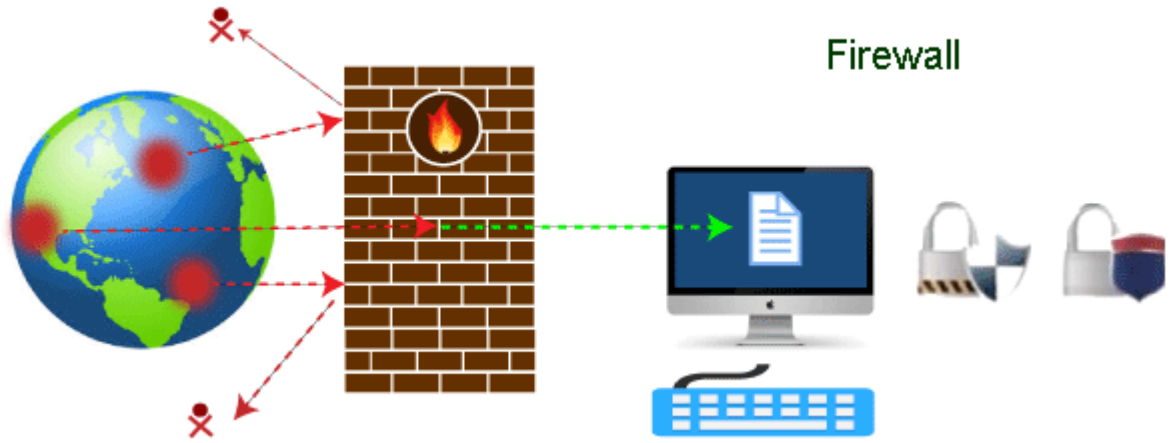
Unit - 9

What is a Firewall?

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).

The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.



Firewall: Hardware or Software

The firewall comes at both levels, i.e., hardware and software, though it's best to have both.

Each format (a firewall implemented as hardware or software) has different functionality but the same purpose.

A hardware firewall is a physical device that attaches between a computer network and a gateway.

For example, a broadband router.

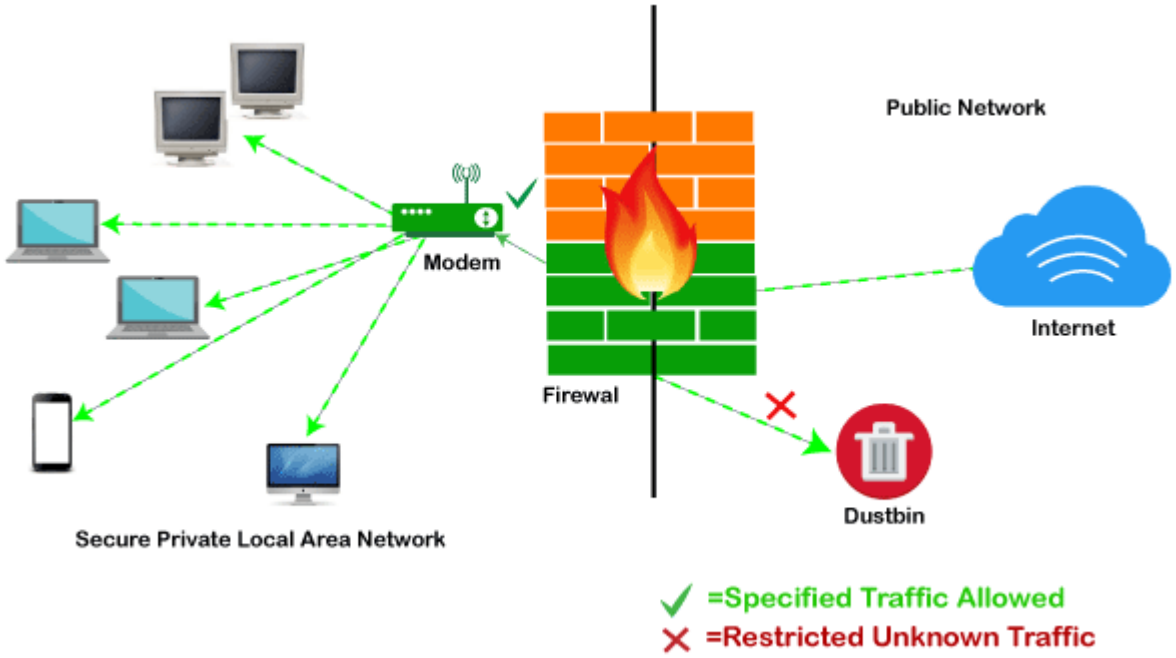
On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software.

Apart from that, there are cloud-based firewalls. They are commonly referred to as FaaS (firewall as a service). A primary advantage of using cloud-based firewalls is that they can be managed centrally.

How does a firewall work?

A firewall system analyzes network traffic based on pre-defined rules. It then filters the traffic and prevents any such traffic coming from unreliable or suspicious sources. It only allows incoming traffic that is configured to accept.

Typically, firewalls intercept network traffic at a computer's entry point, known as a port. Firewalls perform this task by allowing or blocking specific data packets (units of communication transferred over a digital network) based on pre-defined security rules. Incoming traffic is allowed only through trusted IP addresses, or sources.



Types of Firewall

Depending on their structure and functionality, there are different types of firewalls. The following is a list of some common types of firewalls:

- Proxy Firewall
- Packet-filtering firewalls
- Stateful Multi-layer Inspection (SMLI) Firewall
- Unified threat management (UTM) firewall
- Next-generation firewall (NGFW)
- Network address translation (NAT) firewalls

VPN: Virtual Private Network

VPN stands for Virtual Private Network. It refers to a safe and encrypted network that allows you to use network resources in a remote manner. Using VPN, you can create a safe connection over a less secure network, e.g. internet. It is a secure network as it is completely isolated from rest of the internet. The government, businesses, military can use this network to use network resources securely.

How does a VPN work?

A VPN provides a secure, encrypted connection between two points. Before setting up the VPN connection, the two endpoints of the connection create a shared encryption key. This can be accomplished by providing a user with a password or using a key sharing algorithm.

Once the key has been shared, it can be used to encrypt all traffic flowing over the VPN link. For example, a client machine will encrypt data and send it to the other VPN endpoint. At this location, the data will be decrypted and forwarded on to its destination. When the destination server sends a response, the entire process will be completed in reverse.

Types of VPNs

VPNs are designed to provide a private, encrypted connection between two points – but does not specify what these points should be. This makes it possible to use VPNs in a few different contexts:

- **Site-to-Site VPN:** A site-to-site VPN is designed to securely connect two geographically-distributed sites. VPN functionality is included in most security gateways today. For instance a next-generation firewall (NGFW) deployed at the perimeter of a network protects the corporate network and also serves as a VPN gateway. All traffic flowing from one site to the other passes through this gateway, which encrypts the traffic sent to the gateway at the other site. This gateway decrypts the data and forwards it on to its destination.

- **Remote Access VPN:** A remote access VPN is designed to link remote users securely to a corporate network. For instance when the COVID-19 pandemic emerged in 2020, many organizations transitioned to a remote workforce, and set up secure remote access VPNs from the remote clients to connect to critical business operations at the corporate site.

- **VPN as a Service:** VPN as a Service or a cloud VPN is a VPN hosted in cloud-based infrastructure where packets from the client enter the Internet from that cloud infrastructure instead of the client's local address. Consumer VPNs commonly use this model, enabling users to protect themselves while connecting to the Internet via insecure public Wi-Fi and provide some anonymity while accessing the Internet.

Benefits of a VPN

VPNs can provide users and companies with a number of benefits, such as:

- **Secure Connectivity:** A VPN's encrypted connection makes it impossible for a third party to eavesdrop on the connection without knowledge of the secret keys used for encryption and securing the data while in transit.
- **Simplified Distributed Networks:** Any computers accessible from the public Internet need to have public IP addresses – either directly or via Network Address Translation (NAT). A site-to-site VPN simulates a direct connection between the two networks, enabling them to use private IP addresses for internal traffic.
- **Access Control:** Every organization has systems and resources that are designed to only be accessible to internal users. A VPN provides a remote user or site with "internal" access – since the VPN endpoint is inside the network firewall – making it possible to allow access to these resources to authorized remote users without making these resources publicly accessible.

Is a VPN Secure?

A VPN uses cryptography to provide its security and privacy guarantees. In this way, VPNs can meet the three criteria of information security:

- **Confidentiality:** Data privacy is ensured by encrypting all data flowing over the public network.
- **Message Integrity:** Message authentication codes (MACs) ensure that any modifications or errors in transmitted data are detectable. In short, this detects when a message is tampered with or interfered with in some way, either intentionally or unintentionally.
- **Authentication:** The initial authentication and key sharing process proves the identity of both endpoints of the VPN connection, preventing unauthorized use of the VPN.

By providing all of the features of the "CIA triad", VPNs ensure a secure and private connection for their users.

Limitations and Security Risks of VPNs

While VPNs are designed to fill a vital role for the modern business, they are not a perfect solution. VPNs have several limitations that impact their usability and corporate cybersecurity, including:

- **Fragmented Visibility:** VPNs are designed to provide secure point to point connectivity with every VPN user on their own link. This makes it difficult for an organization's security team to maintain the full network visibility required for effective threat detection and response.
- **No Integrated Security:** An organization must deploy additional security solutions behind the VPN to identify and block malicious content and to implement additional access controls.
- **Inefficient Routing:** VPNs can be used in a "hub and spoke" model to ensure that all traffic flows through the organization's centralized security stack for inspection. As remote work and cloud applications become more common, this detour may not be the optimal path between the client and the cloud application or the Internet.
- **Poor Scalability:** As a point-to-point security solution, VPNs scale poorly. For example, the number of site-to-site VPN connections in a fully-connected network grows exponentially with the number of sites. This creates a complex network infrastructure that is difficult to deploy, monitor and secure.
- **Endpoint Vulnerabilities:** Endpoints who have legitimate access to the VPN can sometimes be compromised via phishing and other cyber attacks. Since the endpoint has full access to the VPN resources, so does the threat actor who has compromised the endpoint.