



Firewall

A Guide to understand firewalls

Contents

What is a Firewall ?	2
How does Firewall work ?	3
Firewall types	4
Static packet filtering firewalls:.....	5
Circuit-level gateway firewalls:	6
Proxy firewalls:	6
Next-Generation firewalls(NGFWs):.....	7
Stateful inspection firewalls:.....	9
Virtual firewalls:	9
Unified Threat Management (UTM):	10
Why to use a firewall ?	11
References	12

What is a Firewall ?



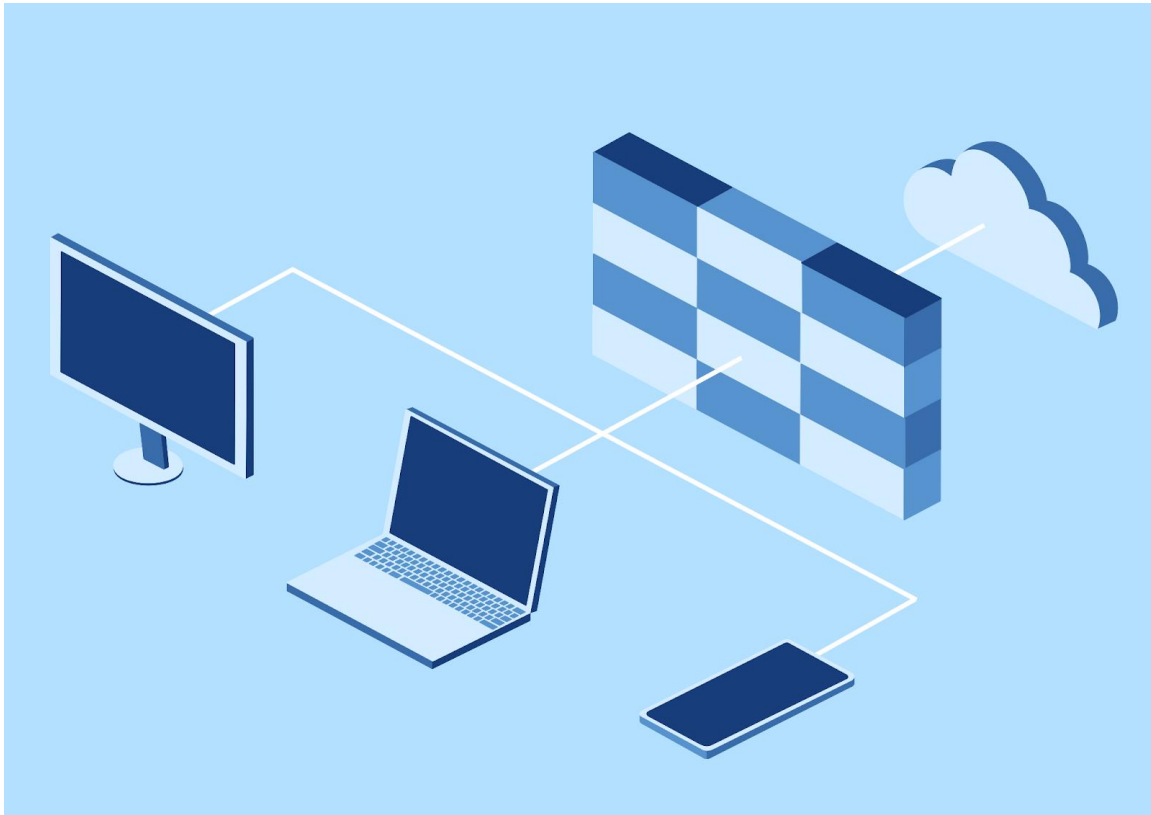
A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

A firewall can be physical hardware, digital software, or a virtual private cloud, it's used in both personal and enterprise level, most operating systems come with a built-in firewall as well.

Firewalls create 'choke points' to funnel web traffic, at which they are then reviewed on a set of programmed parameters and acted upon accordingly. Some firewalls also track the traffic and connections in audit logs to reference what has been allowed or blocked.

Since the internet is not an option nowadays and you or your company interact with it almost frequently in carrying out your daily tasks, then you should consider having a good firewall to guard you from any unwanted threat.

How does Firewall work ?



The data travel through the network as packets, these packets are encapsulated before being transmitted then they decapsulated once they reach their destination, the process of transmitting and receiving the data is what we call network traffic.

A firewall decides which network traffic is allowed to pass through and which traffic is deemed dangerous.

This is done by matching the network traffic against a set of predefined rules in the firewall table. Once the rule is matched, associate action is applied to the network traffic (accept, reject or drop) REJECT sends an error message back to the source indicating a connection failure, while DROP simply ignores the packet without the need for further processing.

From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.

Most traffic which reaches on the firewall(incoming traffic) is one of these three major Transport Layer protocols: [TCP](#), [UDP](#) or [ICMP](#). All these types have a source address and destination address, TCP and UDP have port numbers while ICMP uses type code instead of port number which identifies purpose of that packet.

Firewall types



Firewall types are distinguished by their approach to:

1. Connection tracking
2. Filtering rules
3. Audit logs

We did mention previously that Firewalls can be either software or hardware, in both cases they are categorized by two different ways, the way they filter data or by the system they protect.

When categorized by what they protect, the two types are network-based and host-based. Network-based firewalls guard entire networks and are often hardware. Host-based firewalls guard individual devices known as hosts and are often software.

When categorizing by filtering method, the main types are as follows:

1. Static packet filtering firewalls
2. Circuit-level gateway firewalls
3. Proxy firewalls
4. Next-Generation firewalls(NGFWs)
5. Stateful inspection firewalls
6. Virtual firewalls
7. Unified threat management (UTM)

Static packet filtering firewalls:

Also known as stateless inspection firewalls, operate at the OSI network layer (layer 3). These offer basic filtering by checking all individual data packets sent across a network, based on where they're from and where they're attempting to go.

Since this type of firewalls operates at layer 3 then the Filtering is based on IP addresses, ports, and packet protocols. These firewalls,

at the bare minimum, prevent two networks from directly connecting without permission.

Rules for filtering are set based on a manually created access control list (ACL). These are very rigid and it is difficult to cover unwanted traffic appropriately without compromising network usability. Static filtering requires ongoing manual revision to be used effectively. This can be manageable on small networks but can quickly become difficult on larger ones.

Circuit-level gateway firewalls:

Circuit-level gateways operate on the session level (layer 5). These firewalls check for functional packets in an attempted connection, and if they operate well the firewall will permit a persistent open connection between the two networks. The firewall stops supervising the connection after this occurs.

It is worth to mentions that the ongoing unmonitored connection is dangerous, as legitimate means could open the connection and later permit a malicious actor to enter uninterrupted

Proxy firewalls:

Proxy Firewalls, also known as application-level firewalls (layer 7), are unique in reading and filtering application protocols. These combine application-level inspection, or 'deep packet inspection (DPI)' and stateful inspection.

A proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing

direct connections from outside the network, it essentially looks at and evaluates incoming data. If no problem is detected, the data is allowed to pass through to the user.

The downside to this kind of heavy security is that it sometimes interferes with incoming data that isn't a threat, leading to functionality delays.

Next-Generation firewalls(NGFWs):

A next-generation firewall (NGFW) is a network security device that provides capabilities beyond a traditional, stateful firewall. While a traditional firewall typically provides stateful inspection of incoming and outgoing network traffic, a next-generation firewall includes additional features like application awareness and control, integrated intrusion prevention system (IPS), and cloud-delivered threat intelligence.

Most companies are deploying next-generation firewalls to block modern threats such as advanced malware and application-layer attacks.

According to [Gartner's definition](#), a next-generation firewall must include:

- Standard firewall capabilities like stateful inspection
- Integrated intrusion prevention
- Application awareness and control to see and block risky apps
- Threat intelligence sources
- Upgrade paths to include future information feeds
- Techniques to address evolving security threats

The best next-generation firewalls deliver five core benefits to organizations:

1. Breach Prevention and advanced Security

since preventive measures will never be 100 percent effective, your firewall should also have advanced capabilities to quickly detect advanced malware if it evades your front-line defenses

2. Comprehensive network visibility

You need to monitor what is happening on your network at all times so you can spot bad behavior and stop it fast.

3. Flexible management and deployment options

4. Fast time to detection

The current industry standard time to detect a threat is between 100 to 200 days; that is far too long. A next-generation firewall should be able to:

- Detect threats in seconds
- Detect the presence of a successful breach within hours or minutes

5. Automation and product integrations

NGFW communicates and work together with the rest of your security architecture.

Stateful inspection firewalls:

Stateful inspection firewalls, also called dynamic packet-filtering firewalls, are unique from static filtering in their ability to monitor ongoing connections and remember past ones. These began by operating on the transport layer (layer 4) but nowadays, these firewalls can monitor many layers, including the application layer (layer 7).

Stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

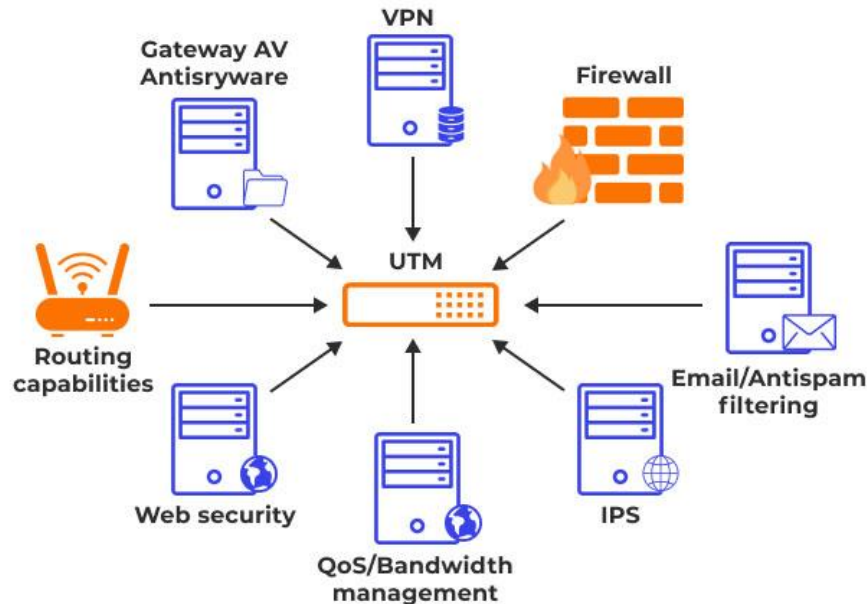
Virtual firewalls:

A virtual firewall is typically deployed as a virtual appliance in a private cloud (VMware ESXi, Microsoft Hyper-V, KVM) or public cloud (Amazon Web Services or AWS, Microsoft Azure, Google Cloud Platform or GCP, Oracle Cloud Infrastructure or OCI) to monitor and secure traffic across physical and virtual networks.

Unified Threat Management (UTM):



UTM A single appliance Blended threats protection



Unified threat management, commonly abbreviated as UTM, is an information security term that refers to a single security solution, and usually a single security appliance, that provides multiple security functions at a single point on the network.

A UTM device typically combines the functions of a stateful inspection firewall with and antivirus, anti-spyware, anti-spam, network firewalling, intrusion detection and prevention, content filtering and leak prevention. Some units also provide services such as remote routing, network address translation (NAT), and virtual private network (VPN). It may also include additional services and often cloud management.

Why to use a firewall ?










It is well known at this point that any small threat can cost big enterprises a lot of time and money, either it is coming from outside or inside its doors, having a good firewall will minimize the risk, it may not give a 100% protection but with choosing the right firewall type and with good customization you can make it difficult to the attacker to damage your data.

You can see below what advantages the firewall can offer you:

1. Protection from unauthorized access
2. Prevention of malware and other threats
3. Control of network access
4. Monitoring of network activity
5. Network segmentation

If you are using the fire wall inside your enterprise or company small or big, it is so important to rise your employees awareness to the possible threats and how you deal with it beside apply a strong security policy, because the firewall won't be enough without what we did mention.

References

-  [What is a Firewall - CISCO](#)
-  [What is a firewall? Definition and explanation](#)
-  [firewall](#)
-  [What is a Firewall? - Checkpoint](#)
-  [Introduction of Firewall in Computer Network](#)
-  [CYBER EDU-What is a Firewall?](#)
-  [What Is a Next-Generation Firewall?](#)
-  [What is Unified Threat Management \(UTM\)?](#)
-  [What is Circuit-Level Gateway?](#)