What is AWS network Firewall?

AWS Network Firewall is a stateful, managed, network firewall and intrusion detection and prevention service for your virtual private cloud (VPC) that you created in Amazon Virtual Private Cloud (Amazon VPC).

With Network Firewall, you can filter traffic at the perimeter of your VPC. This includes filtering traffic going to and coming from an internet gateway, NAT gateway, or over VPN or AWS Direct Connect. Network Firewall uses the open source intrusion prevention system (IPS), Suricata, for stateful inspection. Network Firewall supports Suricata compatible rules.

What are the 2 types of firewalls?

Depending on their construction, firewalls can be classified as software firewalls, hardware firewalls. Each sort of firewall serves a distinct purpose but has the same functionality. However, it is best practice to have both for optimal protection.

Why Are Firewalls Important?

Firewalls are designed with modern security techniques that are used in a wide range of applications. In the early days of the internet, networks needed to be built with new security techniques, especially in the client-server model, a central architecture of modern computing. That's where firewalls have started to build the security for networks with varying complexities. Firewalls are known to inspect traffic and mitigate threats to the devices.

Key Uses of Firewalls

* Firewalls can be used in corporate as well as consumer settings.
* Firewalls can incorporate a security information and event management strategy (SIEM) into cybersecurity devices concerning modern organizations and are installed at the network perimeter of organizations to guard against external threats as well as insider threats.
* Firewalls can perform logging and audit functions by identifying patterns and improving rules by updating them to defend the immediate threats.
* Firewalls can be used for a home network, Digital Subscriber Line (DSL), or cable modem having static IP addresses. Firewalls can easily filter traffic and can signal the user about intrusions.
* They are also used for antivirus applications.
* When vendors discover new threats or patches, the firewalls update the rule sets to resolve the vendor issues.
* In-home devices, we can set the restrictions using Hardware/firmware firewalls.

Functions of Firewall

* The most important function of a firewall is that it creates a border between an external network and the guarded network where the firewall inspects all packets (pieces of data for internet transfer) entering and leaving the guarded network. Once the inspection is completed, a firewall can differentiate between benign and malicious packets with the help of a set of pre-configured rules.
* The firewall abides such packets, whether they come in a rule set or not, so that they should not enter into the guarded network.
* This packet form information includes the information source, its destination, and the content. These might differ at every level of the network, and so do the rule sets. Firewalls read these packets and reform them concerning rules to tell the protocol where to send them.

How Does a Firewall Work?

As mentioned previously, firewalls filter the network traffic within a private network. It analyses which traffic should be allowed or restricted based on a set of rules. Think of the firewall like a gatekeeper at your computer’s entry point which only allows trusted sources, or IP addresses, to enter your network.

A firewall welcomes only those incoming traffic that has been configured to accept. It distinguishes between good and malicious traffic and either allows or blocks specific data packets on pre-established security rules.

These rules are based on several aspects indicated by the packet data, like their source, destination, content, and so on. They block traffic coming from suspicious sources to prevent cyberattacks.

For example, the image depicted below shows how a firewall allows good traffic to pass to the user’s private network.

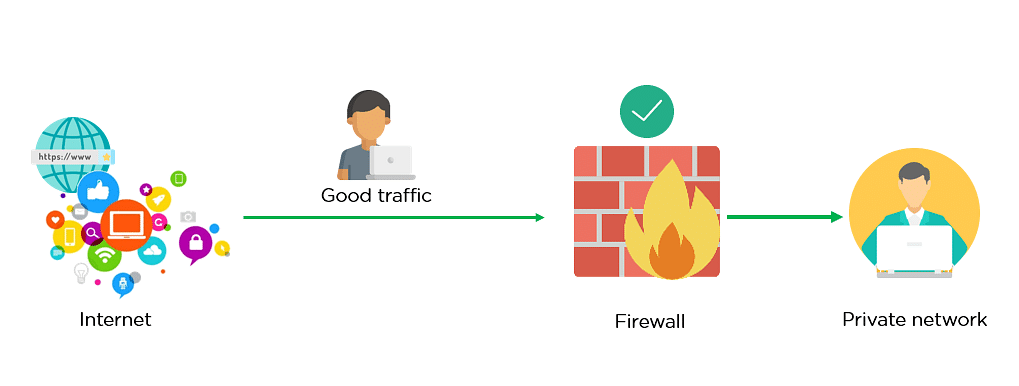


Fig: Firewall allowing Good Traffic

However, in the example below, the firewall blocks malicious traffic from entering the private network, thereby protecting the user’s network from being susceptible to a cyberattack.

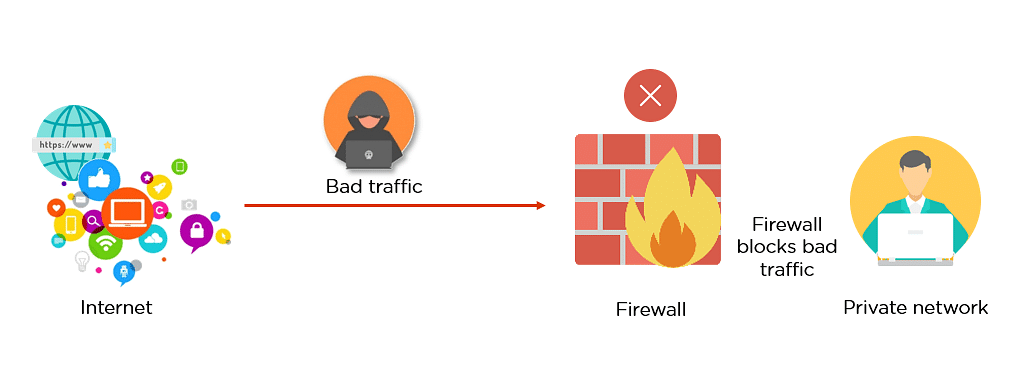


Fig: Firewall blocking Bad Traffic

This way, a firewall carries out quick assessments to detect malware and other suspicious activities.

There are different types of firewalls to read data packets at different network levels. Now, you will move on to the next section of this tutorial and understand the different types of firewalls.

Advantages of Using Firewalls

Now that you have understood the types of firewalls, let us look at the advantages of using firewalls.

* Firewalls play an important role in the companies for security management. Below are some of the important advantages of using firewalls.
* It provides enhanced security and privacy from vulnerable services. It prevents unauthorized users from accessing a private network that is connected to the internet.
* Firewalls provide faster response time and can handle more traffic loads.
* A firewall allows you to easily handle and update the security protocols from a single authorized device.
* It safeguards your network from phishing attacks.

Difference Between a Firewall and Antivirus

Firewall

* A firewall is essential software or firmware in network security that is used to prevent unauthorized access to a network.
* It is used to inspect the incoming and outgoing traffic with the help of a set of rules to identify and block threats by implementing it in software or hardware form.
* Firewalls can be used in both personal and enterprise settings, and many devices come with one built-in, including Mac, Windows, and Linux computers.

Antivirus

* Antivirus is also an essential component of network security. It is basically an application or software used to provide security from malicious software coming from the internet.
* An antivirus working is based upon 3 main actions, Detection, Identification, and Removal of threats.
* Antivirus can deal with external threats as well as internal threats by implementing only through software.

Limitations of a Firewall

* Firewalls are not able to stop the users from accessing the data or information from malicious websites, making them vulnerable to internal threats or attacks.
* It is not able to protect against the transfer of virus-infected files or software if security rules are misconfigured, against non-technical security risks (social engineering)
* It does not prevent misuse of passwords and attackers with modems from dialing in to or out of the internal network.
* Already infected systems are not secured by Firewalls.

More About AWS Firewall: -

https://docs.aws.amazon.com/network-firewall/latest/developerguide/what-is-aws-network-firewall.html