WHY ADVANCED FIREWALL AND WEB GATEWAY SECURITY IS REQUIRED

The threat landscape has changed over the last 5 years, new malicious strains rising to wreak havoc, traditional (and outdated) countermeasures are failing, Machine Learning and Artificial Intelligence is stepping up to the plate to create actionable mediation (and remediation) strategies.

Going back to the basics, a firewall is a network security device that monitors outgoing and incoming traffic. Basically, it's the IT equivalent of a TSA officer (no disrespect intended, of course), checking the passengers as they pass through the airport's security gates.

Firewalls can be physical devices (i.e. hardware firewall), but also be deployed in software form (i.e. Microsoft Windows' Defender Firewall). Firewalls, regardless of form, do more than checking inbound/outgoing traffic – they also ensure that user-defined rules are observed.

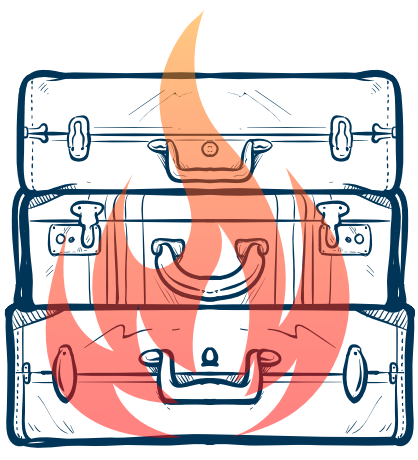
Although the term "firewall" appears to be universal, there are, in fact, several types of firewalls, each designed to address (and overcome) a certain network security challenge. Let's take a close look at the various firewall types.

PACKET-FILTERING FIREWALL

The packet-filtering firewall adds muscle to a multi-device network, such as the ones run by small businesses.

This type of firewall has predetermined rules and policies, which allows it to generate various types of filtering criteria: allowed IP addresses, packet protocol headers, port numbers, and the types of data-bearing packets.

Packet-filtering firewalls are what we call "in-line defences", meaning that they are placed at junction points such as routers or switches.



STATEFUL INSPECTION FIREWALL

Since the entire malware industry is focused on creating variants that circumvent detection grids, there is, indeed, a need for a firewall capable of inspecting the contents of each package.

Enter the stateful inspection firewall, which is, more or less, the IT equivalent of a customs officer, in charge of checking every parcel and suitcase before the owner can retrieve it and go about his business.

HYBRID FIREWALL UTM (UNIFIED THREAT MANAGEMENT)

The epitome of firewall technology, hybrids combine advanced packet-scanning techniques, such as deep-packet inspection, with antivirus antimalware software. A hybrid firewall will inspect every aspect of a web browsing session, right down to the content of each transmitted packet.

More than that, hybrids have the capability of performing deep packet analysis. For instance, they can 'figure out' if the packets came from a legitimate source by piecing together the entire server reply, which is made of many more data packets.

As you would imagine, hybrid firewalls are the go-to solutions if you want to ensure that no malicious packets slip through with built in AV.

However, just like the other types of deep packet inspection firewalls, hybrids can also impact your network's performance. More than that, hybrids can impact your organization's resources as well, since they require front-end maintenance.

ANALYSE AND IMPROVE YOUR NETWORK STRENGTHS

At the most basic level, a UTM security appliance acts as a standard network stateful hardware firewall to restrict access to your network. Other security functions can generally be turned on as options if required.

Typical security functions offered by a UTM security device include:

- Remote access and site-to-site virtual private network (VPN) support
- Secure web gateway functionality (including anti-malware scanning and URL and content filtering)
- A network intrusion prevention system focused on blocking attacks against unpatched
- Windows PCs and servers
- Other UTM security features that are sometimes offered:
- application control
- Intrusion Detection
- Intrusion Prevention
- web application firewalling
- bandwidth management
- data loss prevention (DLP)
- identity-based access control
- load balancing
- DDoS protection
- wireless access management
- email security
- Deep Packet inspection