

Firewall

Types of Firewalls

- **Packet filtering**

A small amount of data is analyzed and distributed according to the filter's standards.

- **Proxy service**

Network security system that protects while filtering messages at the application layer.

- **Stateful inspection**

Dynamic packet filtering that monitors active connections to determine which network packets to allow through the Firewall.

- **Next Generation Firewall (NGFW)**

Deep packet inspection Firewall with application-level inspection.

What Firewalls Do?

A Firewall is a necessary part of any security architecture and takes the guesswork out of host level protections and entrusts them to your network security device. Firewalls, and especially Next Generation Firewalls, focus on blocking malware and application-layer attacks, along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls can react quickly and seamlessly to detect and react to outside attacks across the whole network. They can set policies to better defend your network and carry out quick assessments to detect invasive or suspicious activity, like malware, and shut it down.