Next Generation Firewall
Powered by Cisco Meraki

mother technologies

Next Generation Firewalls (NGFWs) can detect threats up to 60% faster than traditional firewalls, reducing the average threat detection time from 100-200 days to minutes or hours.

The shift to cloud and remote work has made securing business networks much more challenging.	Traditional firewalls only protect on-site assets, leaving remote devices like laptops exposed to threats.	To stay secure, organisations need both On-Net protection for office devices and Off-Net protection for roaming users.

What is a NGFW?

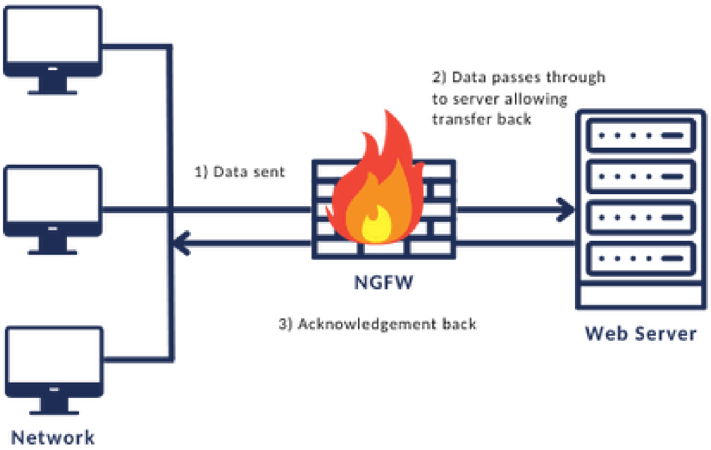
A Next Generation Firewall (NGFW) acts like a digital guard, monitoring and controlling the flow of information in and out of your network.

Smarter than traditional firewalls: Instead of only checking where data is coming from or going to, NGFWs inspect each piece of data to identify the application it belongs to (e.g., email, web browsing) and detect malicious information or suspicious activity.

Advanced inspection: NGFWs block threats like viruses, malware, and unauthorised access attempts.

Access control: They enforce rules on who can access specific parts of the internet and work across multiple locations, including cloud-based services.

Enhanced protection: By doing so, NGFWs provide stronger security against modern cyber threats while giving you more control over how your network is used.



Key Features

Gartner states that Next Generation Firewalls must include:

Stateful Inspection

Also known as Dynamic Packet Filtering, NGFWs must provide Stateful Inspection which is technology common to all traditional firewalls.

Threat Intelligence

Threat Intelligence arms firewalls with the ability to act on threat intelligence feeds from external sources. NGFWs must include upgrade paths to cater for future as well as current information feeds.

Cloud Implementation

In addition to ensuring NGFW prerequisites, Mother recommends that organisations keep NGFW functionality off-box. Simply put, this involves pushing your front-line defences into the cloud as far away from your front door as possible. It destresses your firewall and ensures internet traffic is being screened long before it reaches you.

Deep Packet Inspection

Deep Packet Inspection provides firewalls with application and user-awareness allowing granular control of traffic from unauthorised or high-risk applications.

Integrated Intrusion Prevention

Integrated Intrusion Prevention continuously monitors your network to provide security against unauthorised access and malicious activities.

Evolving Threat Defence

NGFWs must employ techniques to address evolving security threats in addition to those that are recognised and understood.

Benefits of our NGFW

Mother promotes Cisco Meraki MX Next Generation Firewalls for Ironclad security.

The Cisco Meraki MX series are advanced security appliances that go well beyond NGFW prerequisites. They possess a comprehensive suite of secure network and assurance capabilities and are 100% cloud-managed which simplifies their installation and remote management.

✓

Cisco Talos Threat Intelligence – one of the largest commercial threat intelligence teams in the world.

✓

Cisco Advanced Malware Protection (AMP) – comprehensive security before, during and after a malware attack.

✓

Cisco Meraki NGFWs prioritise important applications, optimising network performance through bandwidth management to avoid disruptions from non-business applications.

✓

NGFWs recognise and manage network applications, allowing administrators to set up use rules, prioritise applications, and restrict unauthorised access. This ensures network security and efficient bandwidth use.

✓

World #1 SNORT-based Intrusion Detection & Prevention (IDS & IPS) – a fundamental requirement for PCI compliance.

✓

WAN & Cellular Failover to protect against ISP connection outages.

✓

Auto VPN streamlines secure site-to-site connections, improving communication across offices for more efficient operations and increased data security.

✓

Cisco Meraki NGFWs offer real-time analytics and reporting, giving businesses accurate details about network traffic, security threats, and user activity.