

next firewalls

NEXT GENERATION NETWORK PROTECTION



A next generation firewall is a high-performance network security appliance that adds intrusion prevention, application control, and anti-malware to the traditional firewall-VPN combination.



Anti-spam

Antispam provides a multi-layered approach to detect and filter spam. Dual-pass detection technology can drastically reduce spam volume at the perimeter, giving you unmatched control of email attacks and infections. Fortinet's antispam ranked second highest in security industry tests for effectiveness, earning a 99.98 effectiveness rating.



Anti-virus

Antivirus protects against the latest viruses, spyware, and other content-level threats. It uses industry-leading advanced detection engines to prevent both new and evolving threats from gaining a foothold inside your network and accessing its invaluable content. AV Comparatives awarded our hardware partner its highest award, the Advanced+ rating for file detection and real world protection.



Application Control

Improve security and meet compliance with easy enforcement of your acceptable use policy through unmatched, real-time visibility into the applications your users are running. With Application Control, you can quickly create policies to allow, deny, or restrict access to applications or entire categories of applications.



Web Filtering

Protect your organisation by blocking access to malicious, hacked, or inappropriate websites with Web Filtering. This is the first line of defence against web-based attacks. Protects against malicious or hacked websites, a primary vector for initiating attacks, triggering downloads of malware, spyware, or risky content.



IP Reputation and Anti-botnet Security

Attack signatures change. New bots and worms constantly evolve behaviours. Compromised hosts can remain launch pads for malware indefinitely. A key part of the attack kill chain on an organisation is when the threat communicates with a command & control server – either to download additional threats or to export stolen data. IP and domain address reputation block this communication, neutralising threats.



0800 902 0 902



sales@nextconnex.com



www.nextconnex.com

next firewalls

NEXT GENERATION NETWORK PROTECTION

Firewalls now offer much greater protection options than simply denying access to unrequested traffic. The Next Generation Firewall approach means that you don't have to choose between comprehensive security and network performance.

next connex recommends the use of dual, resilient Next Generation Firewalls to protect customer VPNs with a Unified Threat Management bundle consisting of: Application Control and IPS; Web; Filtering; Anti-virus; Anti-spam and 24x7 support including real-time continuous updates for the term of the contract.

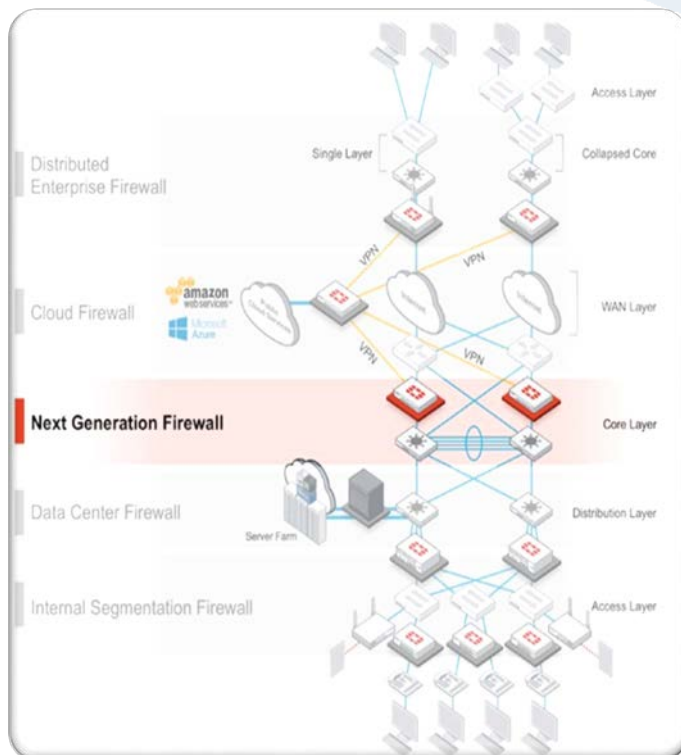
Factors to consider when recommending a centralised or distributed approach to firewalls:

Performance

Performance of a centralised network firewall must be able to meet the needs of many networks and multi-gigabit traffic, while distributed firewalls need only meet the requirements for the individual network segment they protect. Next Generation firewalls provide excellent high performance hardware dedicated to the operation of firewalls, filtering, anti-virus and anti-spam.

Redundancy

Dual, centralised firewalls are located in two separate Data Centres on the Next Connex network so that even if there is a power or equipment failure at one site the network remains protected and available.



Cost

As a result of their needs for performance and redundancy, centralized firewalls have a higher cost per unit than smaller distributed firewalls. Smaller distributed firewalls cost less per unit, but the combined cost of all firewalls to cover an enterprise can often be larger than the cost of the single distributed system and ongoing management and updating are much more time-consuming and prone to error.



0800 902 0 902



sales@nextconnex.com



www.nextconnex.com