Five and a half things that make a firewall *next gen*

Fortinet, leader in high-performance cyber security solutions and a Networks Unlimited reseller partner, has released a white paper titled *5 1/2 things that make a firewall Next Gen*.

Vlad Kochelaevskiy via 123RF

"Network protection can be a difficult balancing act for security vendors and IT administrators alike. How do you achieve very high levels of performance while still ensuring the strongest possible security without impacting end users? After all, as the depth with which network traffic is inspected increases, so too do the demands on the devices at the network's edge," cites the report.

The white paper points out that next generation firewalls (NGFWs) achieve reliable, accurate control of network traffic through increased contextual awareness. That is, the NGFW is aware of the applications generating network traffic, the users of those applications, and the specific content moving across the network.

At the same time, NGFWs have the ability to analyse encrypted traffic on the fly and apply highly intelligent threat detection techniques to actual runtime activity instead of merely comparing traffic characteristics to static lists of threats. "This dynamic, intelligent processing of traffic is what truly differentiates next gen firewalls from their predecessors that relied far more on static, pre-defined rules," state the paper's authors.

So what "five things" exactly makes a *next gen* firewall, *next gen*? And what about the "half a thing" promised in the title? Well, according to Fortinet, the half is that "set of practical considerations that affect buyers of next-gen firewalls. In particular it includes the challenge of delivering the performance needed to handle the additional work of all those great next generation security services. This calls for some specialised hardware and software optimisations."

In summary, **the five important points for administrators evaluating NGFWs for their networks, are listed as**:

1. Application awareness and control

In an age of BYOD and BYOA, it can be a real challenge to know which applications and cloud services are running on your network. Even with complete visibility into the sources of network traffic, distinguishing appropriate business applications from mere time wasters or even malicious apps can be much harder. Next-gen firewalls can not only identify applications and services on the network but provide fine-grained control over quality of service parameters and specific restrictions for network apps.

2. User identity awareness and control

Application awareness and control are powerful features of next-gen firewalls on their own. Combining this with awareness of user identity information, though, creates a whole new degree of granular protection and control that administrators can use to enforce security policies differentiated by role, job function, and organisational unit. Whereas legacy firewalls can only block traffic based on IP address, subnet, or MAC address, NGFWs can easily accommodate the multiple devices with which users may attempt to access network resources.

3. Content security with integrated IPS, antivirus, and web filtering

Next-gen firewalls are able to deliver robust network controls through so-called "deep packet inspection" (DPI). Instead of just inspecting IP header information and blocking or forwarding packets accordingly, DPI involves scanning the actual content of IP packets for a variety of threats and rule violations.

4. SSL Encryption and decryption so threats can't hide in HTTPS traffic

Many legacy firewalls and content filters are foiled by SSL encryption. It isn't hard to block http://facebook.com or even https://facebook.com completely. But what if an organisation wants to allow Facebook access for marketing purposes but block the ability to chat on the secured version of the site? The processing overhead required to decrypt and encrypt secure traffic on the fly and actually inspect its contents is considerable - legacy firewalls (and some NGFWs as well) just aren't up to the task. When secure websites were limited to e-commerce, this wasn't a critical failing.

5. Advanced threat protection and intelligence

Finally, next-gen firewalls include advanced and integrated, intelligent tools that can detect and remediate threats that traditional layers of protection often miss. Although anti-malware, intrusion protection systems, and the like are critical for efficiently stopping many threats at the gateway, an increasing number of highly sophisticated and/or targeted attacks require a different approach altogether.

Practical considerations

"As a value-added distributor of Fortinet we appreciate that for those seeking a NGFW, effective security with excellent performance can be achieved at an affordable price without having to lower performance," says Anton Jacobsz, managing director of Networks Unlimited.

He also refers to the practical considerations, which the white paper discusses, that organisations should note when evaluating new firewalls or looking to move from legacy to next generation protection.

These practical considerations encompass the fact that NGFWs can introduce levels of visibility and control that IT has never enjoyed before. "Administrators should look for clear, easy-to-use dashboards and reports that contribute meaningful metrics and useful information for developing and implementing robust security strategies," mentions the paper. Also, security products are only as good as the intelligence that power them and potential buyers should expect NGFW vendors to employ strong research teams that can quickly respond to new threats and assist customers 24/7/365. Furthermore, third-party testing, in addition to testing in your own environment, are the best ways to really evaluate these products.

Security performance

The paper further says that most administrators have spent a fair amount of time wrestling with policies that balance user trust and empowerment with top-notch security. And NGFWs give IT new capabilities to which users may be especially sensitive, including decryption and scanning of secure web sessions. From a practical perspective, IT will need to accompany the rollout of a new firewall with user training and clear policies. Finally, all of these additional layers of security can place substantial performance demands on a firewall. Potential buyers should ensure that the firewalls they are evaluating have sufficient horsepower for current demands and future requirements.

"Performance isn't part of the classic NGFW definition but it can be the Achilles heel of the NGFW if it isn't properly addressed in both hardware and software optimisations," according to Fortinet.

NGFWs introduce extraordinary new capabilities for network protection and management, states the white paper and concludes that: "no longer just devices for comparing traffic to static lists of threats and attributes, NGFWs intelligently analyse traffic for a variety of known threats as well as telltale signs of potential threats and increasingly include integrated advanced threat protection capabilities."