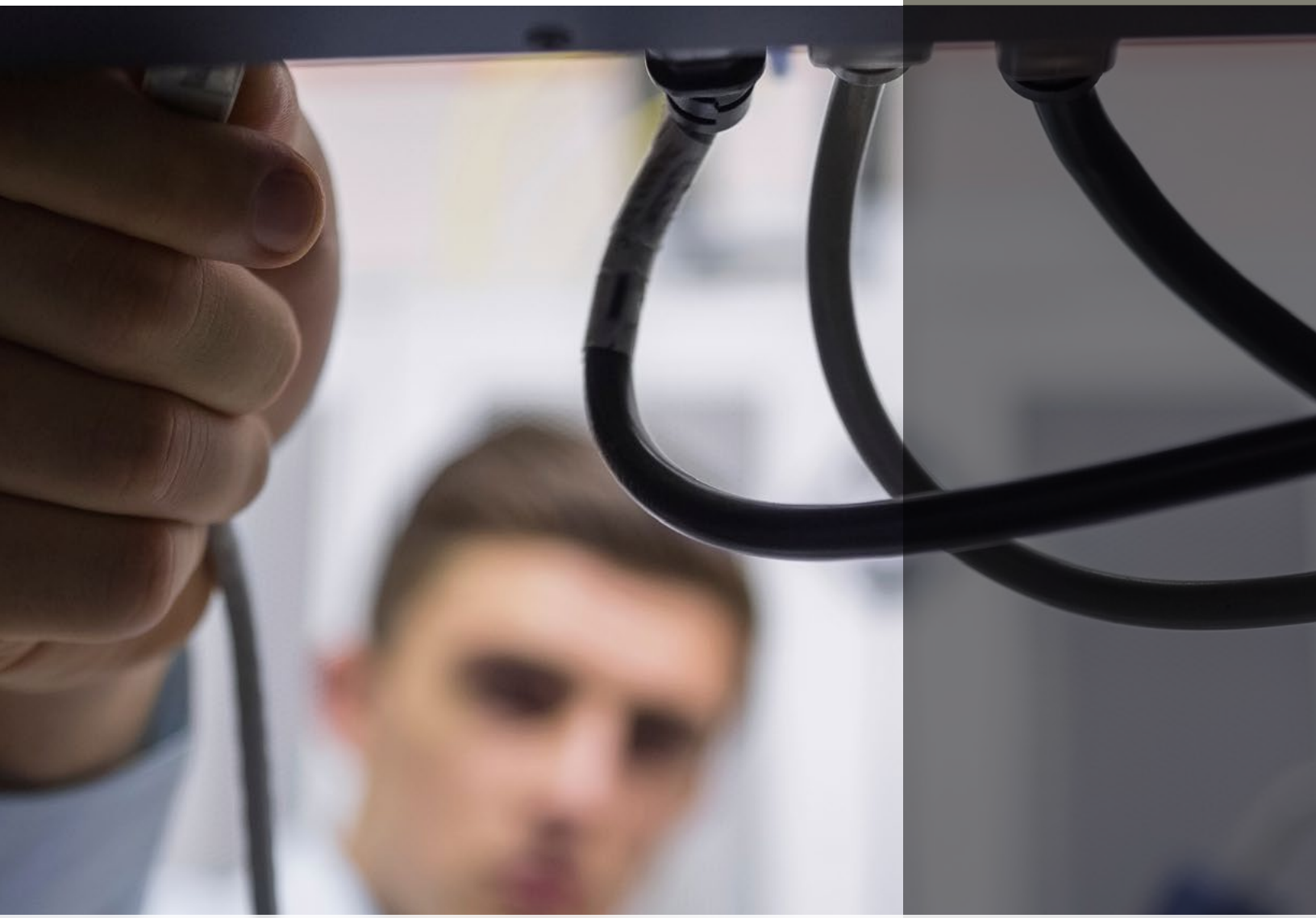
FORTINET

WHITE PAPER



5 ½ Things That Make a Firewall "Next Gen"

5 ½ Things That Make a Firewall "Next Gen"

Table of Contents

Introduction

5 ½ Things That Make a Firewall “Next Gen”

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.

Enter the “Next Generation Firewall” (NGFW). Next gen firewalls achieve reliable, accurate control of network traffic through increased contextual awareness. 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 analyze 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.

These five bullets, of course, are the “five things” that we’ll cover in greater detail throughout this paper. But what of the “half a thing” promised in the title? That is a 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 specialized hardware and software optimizations.

Watch out when evaluating NGFWs, not all of them have the performance to handle the full load of security services they tout.

So what exactly makes a next gen firewall, "next gen"? Read on to find out and discover important points for administrators evaluating NGFWs for their networks.

#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.

For example, YouTube, a well-known bandwidth hog, may be entirely legitimate in business settings but obviously shouldn't interfere with VoIP streams or VDI traffic that should always be given top priority. Peer to peer applications like BitTorrent rarely have business use cases and administrators often want to block them completely. Social media applications may simply be candidates for throttling above certain usage quotas. Consumer-grade file sync and share utilities like Dropbox represent substantial security risks as well as high levels of bandwidth utilization and users should often be prevented from syncing corporate IP to their personal clouds.

Legacy firewalls, on the other hand, lack both application awareness and, often, the ability to efficiently process traffic based on its "state", i.e., attributes that define particular types of persistent connections. These firewalls use administrator-defined or pre-built rules to evaluate traffic instead of built-in application signatures that offer greater flexibility and control. Those peer to peer applications that administrators frequently want to exclude from the network entirely or certain types of malware that send data back to a central server tend to be very good at choosing open ports, making traditional approaches to blocking traffic by port or destination ineffective; application-based blocking will stop the traffic regardless of the port it uses.

#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 organizational 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. Instead of filtering by address, next gen firewalls can filter by identity obtained from an LDAP server or Directory Services. This means that marketing staff, for instance, could access public social media applications while other employees could be limited to sanctioned social business sites.

Ultimately, being able to pinpoint which users are using which applications rather than only being able to identify a particular application's traffic gives administrators high degrees of visibility (and, therefore, control). This has uses far beyond simply allowing a subgroup of users to access Facebook at work. Organizations can use this capability to measure adoption and usage of new applications or to identify areas of potential optimization, e.g., freeing up bandwidth at certain times of the month for critical reporting from a cloud-based ERP system.

#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.

Intrusion prevention systems (IPS), anti-malware, and web filtering all play critical roles in thwarting advanced attacks. Web filtering, for example, may stop a user from visiting a malicious web site in the first place. If it doesn't, integrated IPS and antivirus can stop the exploits and malware that malicious web sites may launch at your organization.

Implementing these technologies at the network's edge provides a powerful additional layer of protection for both users and the network itself, as well as helping administrators ensure that bandwidth is utilized for work instead of objectionable or distracting activities. More importantly, NGFWs add substantial value for administrators by integrating all of these capabilities into a single appliance rather than forcing organizations to maintain multiple appliances for discrete but related functions.

#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 organization 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 ecommerce, this wasn't a critical failing.

Now, however, a growing number of sites ranging from social media to unified communications use SSL by default. Moreover, these sites are now using SSL on all pages rather than selected pages deemed appropriate for encryption. Hackers also use SSL to obscure attacks and websites increasingly use SSL to deliver malicious payloads. All of these factors make SSL inspection a must-have feature.

In fact, the ability to process SSL data in real time is a defining characteristic of the next gen firewall.

#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.

Advanced persistent threats (APTs) are often comprised of several hacking techniques designed to evade detection and gather sensitive data over time. Even deep packet inspection may not catch every element of an APT and zero-day threats, or those that have not yet been identified and added to malware databases, can quickly infect a network relying on signature-based protection alone. NGFWs should be able to identify and submit suspicious or high risk objects to a sandbox (either integrated or cloud-based) where they can be safely and quickly tested for malicious activity and payloads.

#5 1/2: Practical Considerations

The five traits described in this paper characterize a good next gen firewall fairly well. But for organizations evaluating new firewalls or looking to move from legacy to next generation protection, there are several practical considerations also worth noting.

First, 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. These strategies need to carefully balance security requirements with end user productivity. A firewall is only as good as the policies it implements and the human factor in all of this shouldn't be ignored.

Second, security products are only as good as the intelligence that power them. Potential buyers should expect NGFW vendors to employ strong research teams that can quickly respond to new threats and assist customers 24/7/365. Vendors must also offer timely updates, ongoing threat intelligence, and access to sandboxing capabilities to address the latest vulnerabilities.

Next, third-party testing, in addition to testing in your own environment, are the best ways to really evaluate these products. Competing claims and a crowded market make it difficult to distinguish merely adequate IPS, anti-malware, and threat intelligence from highly effective NGFW tools. NSS Labs, AV Comparatives, and VB100 all offer comprehensive third-party test reports.

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. NGFWs with purpose-built ASICs (application-specific integrated circuits) can optimize performance. 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 optimizations.

That said, NGFWs don't need to break the bank. Buyers can achieve highly effective security with excellent performance at an affordable price. Again, third-party testing can provide useful resources for evaluating performance and value.

Conclusion

Next Generation Firewalls introduce extraordinary new capabilities for network protection and management. No longer just devices for comparing traffic to static lists of threats and attributes, NGFWs intelligently analyze traffic for a variety of known threats as well as telltale signs of potential threats and increasingly include integrated advanced threat protection capabilities. NGFWs are aware of the overall context of network traffic and act accordingly. Application, user identity, and content awareness all play into their function, as do performance characteristics that support on-the-fly decryption and encryption and advanced threat intelligence. Effectiveness and performance vary greatly, even from vendor published specifications in many cases. Be sure to validate all such claims with independent third-party tests and/or your own testing before making a strategic security purchase.

About Fortinet

Fortinet is a global leader and innovator in Network Security. Our mission is to deliver the most innovative, highest performing network security platform to secure and simplify your IT infrastructure. We are a provider of network security appliances and security subscription services for carriers, data centers, enterprises, distributed offices and MSSPs. Because of constant innovation of our custom ASICs, hardware systems, network software, management capabilities and security research, we have a large, rapidly growing and highly satisfied customer base, including the majority of the Fortune Global 100, and we continue to set the pace in the Network Security market. Our market position and solution effectiveness has been widely validated by industry analysts, independent testing labs, business organizations, and the media worldwide. Our broad product line of complementary solutions goes beyond Network Security to help secure the extended enterprise.

Fortinet FortiGate NGFWs deliver NSS-Recommended levels of security effectiveness and deliver five times the performance of equivalently priced NGFWs in the industry. FortiGate is the best value on the market with exceptional security and throughput at prices within reach of all organizations.

For more information about Fortinet and their FortiGate line of NGFW products, visit www.fortinet.com.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480