



Top 5 Considerations for Choosing a Next-Generation Firewall:

SonicWALL vs. Palo Alto Networks and Fortinet

Contents

Introducing the Next Generation Firewall	1
Top 5 Considerations When Choosing a NGFW	2
Conclusion	6

Brought to you compliments of



Thanks to Web 2.0 and an explosion of Web-based applications, nearly two-thirds of today's traffic is HTTP and HTTPS. Collaboration, increased productivity and improved insights into customers and prospects are all key benefits of Web 2.0. But with these benefits come new security threats as well as dramatic increases in network bandwidth consumed.

Gone are the days when IT administrators could simply focus on filtering content on a few ports while blocking all others in order to close off all possible attack vectors into their networks. Today's complex IT and threat landscapes require more sophisticated IT controls.

Web-based applications all look the same to legacy firewalls — like legitimate HTTP and HTTPS traffic. But IT managers know better. An important productivity tool for one user may be a threat-laden time-sink for another. However, traditional network security solutions don't have the sophistication and the power to closely scrutinize all traffic and to sort the good from the bad. The result: application chaos.

Gaining control over this application chaos is critical to protecting your network against Web 2.0 threats and preserving bandwidth. But how do you discern the good traffic from the bad? How can you properly identify, catalog and control applications and network bandwidth? Enter the Next Generation Firewall.

Introducing the Next Generation Firewall

According to Gartner, a Next Generation Firewall (NGFW) "is a wire-speed integrated network platform that performs deep inspection of traffic and blocking of attacks." A NGFW includes all standard capabilities found in a first-generation firewall; i.e., Network Address Translation, packet filtering and stateful packet inspection, among other common networking features.

What sets a NGFW apart is application awareness and full network stack visibility. Instead of blocking traffic based only on port or protocol, the NGFW abstracts away from these characteristics and enforces network security policies at the application layer based on traffic fingerprinting through Deep Packet Inspection. Traffic control goes beyond the ability to merely block or allow particular applications and can be used to manage bandwidth or prioritize application level traffic. Deep inspection of traffic allows for enforcement of granular policies for individual application components. For example, you might allow the use of an instant messaging client but disable file sharing.

NGFWs are also characterized by integrated network intrusion prevention capabilities that go beyond simple addition of an intrusion prevention subsystem on top of traditional firewall architecture. NGFWs integrate intrusion prevention as a core piece of the security engine and thus avoid having to pass the same traffic through multiple independent security layers, thereby increasing performance and security.

Another important capability of NGFWs is the dynamic adaptation to changing threats. The device is constantly updated with signatures to identify new threats and stay on top of the evolving malware landscape.

Top 5 Considerations When Choosing a NGFW

Gartner recommends requiring NGFW capabilities from your vendors when you approach your firewall and/or intrusion prevention technology refresh cycle. But as you evaluate NGFWs, you'll notice that some network security vendors claim capabilities that overlap with NGFWs. So what should you look for in a true enterprise-class NGFW? Let's consider five capabilities and how they compare between two popular NGFW vendors and a firewall vendor, respectively: SonicWALL, Palo Alto Networks and Fortinet.

At-a-glance comparison of SonicWALL, Palo Alto Networks and Fortinet

Area	SonicWALL	Palo Alto Networks	Fortinet
Performance	Re-assembly Free Deep Packet Inspection (RFDPI) ensures minimal performance impact with near-zero latency	Limited scalability in performance, low latency	Proxy approach – fundamentally flawed for DPI performance, very high latency, no scalability
Scanning	Scans files of all sizes, SSL-encrypted files and a wide range of protocols	Scans SSL traffic, but shows limitations in file size capabilities	Constrained by file size, protocol and port dependency
Management	Global Management System (GMS) in wide deployment	Management system not in wide deployment	Requires purchase of two additional applications
App Intelligence	Real-time app traffic visualization, wireless endpoint, growing database of app signatures	Real-time app traffic visualization, no wireless controller, lower app signature count	Limited wireless features, no real-time view of traffic
NetFlow/IPFix Reporting	Detailed output on applications, users and other data	Doesn't support NetFlow/IPFix	Doesn't support NetFlow/IPFix

#1. Performance

Gartner states that NGFWs “support in-line, bump-in-the-wire configuration without disrupting network operations.” In other words, they introduce minimal latency. The tight integration of IPS with other capabilities is key to making this happen. A single-pass engine enables seamless policy implementation and enforcement without introducing latency or dropping performance to unacceptable levels. This is important because enabling NGFW services should not bring a network to a standstill.

Fortinet, for example, relies on ASIC technology for stateful packet inspection in its line of firewalls. By the company’s own quoted documentation, the performance of its firewall degrades significantly — in some cases by more than 99% — when Malware Threat Prevention is activated. This is a result of having to proxy each file and each network connection in order to enable Deep Packet Inspection.

There is another option. At the heart of every SonicWALL network security solution is a patented Re-assembly Free Deep Packet Inspection (RFDPI) engine. The RFDPI technology unifies multiple security capabilities into a single, integrated engine to allow extremely high performance Deep Packet Inspection. Packets are scanned once, and the information is shared across all of the NGFW’s security capabilities. As a result, there is nearly zero latency introduced into the network stream and the NGFW benefits are provided at fast network speeds.

SonicWALL’s unique RFDPI design allows it to massively scale across an arbitrary number of cores with linear performance gains, providing a unique set of solutions that can be deployed in diverse environments ranging from branch/small offices to data center networks.

#2. Robust scanning capabilities

Like first-generation firewalls, NGFWs include stateful inspection capabilities. But what sets them apart from their predecessors is the ability to perform deep packet inspection (DPI). Many NGFW companies advertise DPI capabilities, but a close examination of their products shows limitations that minimize protection. Many NGFWs have to proxy files in order to scan them for malware at the gateway. This can severely impact network performance. To avoid bringing the network to halt, some vendors opt to allow packets through without scanning them.

In its documentation, Fortinet states that the performance of its NGFW degrades by 95% when Gateway Antivirus is turned on, which is even worse on its higher end models. This is exacerbated by Fortinet’s proxy approach in which the gateway’s limited memory is quickly exhausted by a few large files or a medium number of smaller files transferred simultaneously. When all memory is consumed, Fortinet firewalls resort to either passing files through without inspection or blocking all files that can’t be inspected.

Some vendors also fail to scan large files or certain protocols. Such is the case for both Fortinet and Palo Alto Networks. Their file scanning capabilities are limited by file size, and they only scan a small portion of protocols for malware.

When evaluating NGFWs, look for one that can:

- Scan files of all sizes for viruses, malware, botnets and other threats
- Decrypt, scan and re-encrypt SSL packets
- Scan a wide range of protocols in addition to raw TCP traffic across all ports

SonicWALL does all three. SonicWALL NGFWs can scan any size file for any threat on any appliance. Because they don’t have file size limitations, SonicWALL NGFWs can scan files

of unlimited size across any port and without security degradation. SonicWALL NGFWs aren't limited by the number of simultaneous files or network streams, so infected files don't have a chance to slip through undetected when the firewall is under heavy load. In addition, SonicWALL NGFWs can apply all security and application control technologies to SSL encrypted traffic, ensuring that this does not become a new malware vector into the network.

Additionally, SonicWALL NGFW users can extend their protection beyond IPS with gateway threat prevention to block viruses, Trojans, worms, bots, keyloggers, spyware and other malware. SonicWALL's RFDPI low-latency engine ensures industry leading DPI performance, and a cloud-based malware identification engine provides an additional layer of content security by tapping the additional threat intelligence available in the SonicWALL GRID security network*.

#3. Ease of management

A scalable and proven distributed management solution is vital to achieving both security and strong ROI as your company begins deploying security to multiple sites. SonicWALL's Distributed Enterprise Global Management System (GMS) currently manages more than 90,000 devices through thousands of customers, VARs and MSSPs. SonicWALL's scalability is proven with customer deployments ranging from a few dozen to several thousand firewalls.

Some vendors, like Palo Alto Networks, have a management platform but lack large scale deployments of their distributed management solution. In fact, SonicWALL has more firewalls under GMS management than Palo Alto Networks has sold in total units worldwide to date. This wide scale deployment is a testament to SonicWALL's ease of management.

Still other vendors lack a cohesive distributed management platform, as in the case of Fortinet. To get the equivalent of SonicWALL GMS, Fortinet users must purchase and run two separate pieces of software — FortiManager and FortiAnalyzer. This complicates the management process and adds to the solution's total cost of ownership (TCO).

#4 Application intelligence, control and visualization

A fundamental benefit of NGFWs is the ability to control applications and optimize what runs on the network. But these capabilities are hindered if the NGFW doesn't:

- extend application intelligence and control to wireless endpoints;
- take into account custom applications;
- provide real-time visualization into the network;
- scan applications against a growing database of signatures.

NGFWs address these capabilities to various degrees. To ensure your network is adequately protected, you need to understand what a specific NGFW can and can't do.

Robust signature database

A NGFW's effectiveness is only as good as the number of applications that it can detect and control. SonicWALL can scan, at the time of this writing, and identify more than 3,500 unique applications and application components, with hundreds of new signatures added daily. Furthermore, SonicWALL NGFW capabilities provide administrators with a comprehensive set of application management capabilities including application bandwidth management, beyond Fortinet's traditional three tools: allow, block or log.

Real-time visualization

You can't control and optimize what you can't see. When evaluating NGFWs, you must consider whether they allow you to see application and user traffic in real-time. SonicWALL provides extensive real-time, integrated, on-box visualization, forensic analysis tools and dashboards. You get a real-time view of exactly which applications are being used, and can correlate this data in order to answer questions such as "Who is using Application A" or "What application is user X using?" At any given time administrators can look at network traffic to understand what is happening on the network. Fortinet has nothing onboard that can provide real-time visual analysis of traffic.

Consideration of custom applications

Although there are many web applications that you want to immediately bring under control on your network, it may not be so easy with your company's custom applications with most NGFWs. But, in order to be truly useful, NGFWs must also be able to identify your company's custom applications and prioritize them over other traffic. SonicWALL includes a built-in Application Signature Generator that allows you to create your own custom signatures based on dozens of traffic attributes or traffic characteristics unique to your application. SonicWALL enables you to bring your custom applications under Application Intelligence & Control immediately and ensure that your core networking tools get the priority that they need.

Wireless endpoint control

Increasingly, companies are experiencing a proliferation of wireless endpoints on the network edge. If this is the case for your company, consider a NGFW's ability to provide powerful application intelligence, control and visualization for wireless users. It does little good to control traffic for only wired users while ignoring the large number of users with laptops who rely solely on the wireless network.

SonicWALL NGFWs can control up to 128 wireless access points while providing application intelligence and control to the WiFi edge. All SonicWALL NGFWs integrate a wireless switch and controller, allowing the provisioning and management of distributed wireless deployments. Further, SonicWALL is able to subjugate all wireless traffic to Application Intelligence and Control policies to maintain wireless bandwidth efficiency. Other wireless features include Lightweight Hotspot Messaging and Wireless Guest Services.

Palo Alto Networks doesn't have an integrated wireless switch controller with NGFW policy controls, and Fortinet firewalls offer significantly fewer wireless features than SonicWALL.

#5 The ability to report via NetFlow and IPFix with Extensions

NetFlow and IPFix are two industry standards for reporting on network traffic flows to external collectors. Traditionally deployed for switches and routers, Netflow exports data such as IP address source and destination, source and destination ports, Layer 3 protocol type and class of service. However, both IPFix and NetFlow Version 9 can be extended to export additional data off the network device such as application data, user data and URL data. SonicWALL NGFWs can export all data that they extract through Application Intelligence and through Deep Packet Inspection through NetFlow/IPFix with extensions to an external collector.

Your NGFW should provide support for NetFlow/IPFix. At the time of this writing, none other than SonicWALL can output such detailed data on applications, users and other attributes to an external collector.

Conclusion

NGFWs promise to help companies regain control over their networks through the integration of intrusion prevention, stateful inspection and deep packet inspection capabilities. But vendors' offerings vary widely in their approach to scanning network traffic. No one that we evaluated offers as much protection as SonicWALL.

SonicWALL provides:

- Application intelligence — Scanning every byte of every packet of all network traffic, SonicWALL provides complete application intelligence and control regardless of port or protocol by determining exactly what applications are being used and who is using them.
- Application control — With new levels of management and ease of use, Application Intelligence, Control and Visualization gives IT administrators granular control of applications and users. Administrators can easily create bandwidth management policies based on logical pre-defined categories (such as social media or gaming), individual applications, or even users and groups.
- Application visualization — To control network use properly, administrators must visualize application traffic and adjust network policy based on critical observations. The SonicWALL Application Flow Monitor provides real-time graphs of applications, ingress and egress bandwidth, web sites visited and all user activity. As a tightly integrated feature of SonicWALL NGFWs, SonicWALL Application Intelligence, Control and Visualization puts the power back into the hands of IT administrators, easily sorting out the good applications from the bad and helping to enhance productivity without compromising security.

For a more detailed analysis of the NGFW market and SonicWALL, download the white paper [Next-Generation Firewall Market Analysis: The SonicWALL Difference](#).

* The SonicWALL GRID Network collaboratively gathers, analyzes and vets cross-vector threat information from millions of business-oriented sources around the world. Reputation-based threat protection information is then distributed securely, anonymously and in real time to improve the overall effectiveness of SonicWALL security solutions. Due to the distributed nature of this network and the use of multiple different data sources, the evaluation from one contributor can be vetted against multiple other contributors, allowing the GRID's collaborative filtering process to be highly accurate and fully self-correcting.