FAQ

Next-Generation Firewalls: Fact and Fiction

Frequently Asked Questions

Introduction

Attackers are increasingly using web-based applications to break into enterprise networks, gain control of devices, and steal valuable information. In an effort to gain control of application use in organizations, and to block web-based attacks, IT managers are deploying a new generation of firewall devices know as next-generation firewalls, or NGFWs. Industry analysts caution, however, that many next-generation firewalls still lack basic network security features and organizations should deploy them only in conjunction with other layers of security for comprehensive protection[1]. This document provides answers to questions that are often asked about NGFWs, and also details important security features that you should consider when choosing the best network security solution for your organization.

Why are so many security vendors claiming to have a next–generation firewall?

Since Gartner published Defining the Next Generation Firewall in 2009, many network security vendors have scrambled to introduce their own version of a NGFW for fear of being left behind in the marketplace. Gartner suggests that NGWF capabilities are necessary to control the increasing number of network threats that are leveraging web-based applications and services.

What is a next–generation firewall anyway?

The term ‘next-generation firewall’ refers to a firewall that offers specific features to address changes in both the way business processes use IT and the ways attacks try to compromise business systems. In order to defend networks against the latest threats, NGFWs should include, at a minimum, an integrated intrusion prevention system (IPS) with deep packet scanning, the ability to identify and control applications running over a network, and the ability to verify a user’s identity and enforce access policies accordingly[1].

Why won’t my stateful firewall block these new attacks?

Stateful firewalls with packet filtering capabilities used to be highly successful at blocking unwanted applications simply because most applications communicated over networks by using specific and unchanging computer ports and protocols. Should an administrator decide that an application was unsafe, they could quickly prevent users from accessing it by modifying the firewall policy to block the associated ports and protocols. However, traditional port-based protection is no longer practical. For example, blocking port 80 (HTTP) would block access to the web entirely, and this is simply not an option for most enterprises today.

Businesses and government agencies are realizing that traditional standalone security solutions such as firewalls, intrusion prevention systems and host-based antivirus are no longer adequate to protect against new, sophisticated attacks. The potential for data loss and damage to corporate networks increases every year as criminals find new ways to penetrate defenses. In addition, as government regulations and legal requirements such as PCI DSS, HIPAA and the HITECH Act begin to hold company executives accountable for their employee's actions, corporate executives and IT professionals alike are becoming more concerned about what their employees are viewing and downloading from the Internet.

I just installed a next-generation firewall. Why are so many attacks still getting through?

In their haste to bring their own version of a NGFW to market, some security vendors have failed to include mature next-generation security features, while other vendors have added NGFW features to platforms that lack sufficient or proven traditional network protections. This has prompted industry analysts to caution that many next-generation firewalls still lack basic network security features, and that organizations should deploy them only in conjunction with other layers of security.

[1] Gartner, Inc., Defining the Next-generation Firewall, October 2009

In order to block all threats, NGFWs must also include traditional packet filtering, network address translation, stateful protocol inspection, and virtual private network (VPN) capabilities[1]. In other words, to deliver the promised protections, NGFWs must be built on a solid, field-proven base of traditional network protections before attempting to add next-generation security features such as application control or an integrated intrusion prevention system.

Why should I care about old security threats?

Once in the wild, viruses, malware and traditional methods of attacking networks and users never go away. Over the past four years, for example, successful malware strains such as the Koobface worm have built a very large attack base through relentless variation and the ability to exploit and spread across multiple social networking platforms. The Koobface virus has leveraged some of the most popular web-based applications including MySpace, Twitter and Facebook[2] to steal personal information and credentials from unsuspecting users.

The Koobface virus is not unique in its success or in its ability to exploit known vulnerabilities for an extended period of time. In fact, many exploits enjoy prolonged lives simply because vendors of widely used applications are reluctant to add user protections, such as strong passwords or SSL encryption, for fear of slowing user acquisition and feature development. This has the effect of placing responsibility for security entirely upon the enterprises and service providers whose employees and customers use these popular web-based applications.

Likewise, many enterprises and end users remain susceptible to a myriad of known attacks due to a simple failure to patch known vulnerabilities, outdated equipment and malware signatures, or a failure to properly setup and deploy security devices. Since many of these vulnerabilities have been known for years, they are well documented, and anyone can download ready-made tools to attack unpatched systems[3]. When developing a security strategy, organizations must plan to protect against not just current threats, but all threats, known and unknown.

Why do I need to control the use of web-based applications in my organization?

In addition to adoption by millions of consumers, many organizations have also integrated social media applications including Twitter feeds, Facebook pages, and YouTube videos into their everyday business practices. These Web 2.0 applications are key to many organizations' marketing and customer support strategies, and can also enable instantaneous, always-on communications between employees, business partners and even temporary contractors, bringing improved productivity.

Unfortunately, allowing these consumer-oriented applications with user-generated content into the enterprise raises a myriad of security concerns. Web 2.0 applications can tunnel through trusted ports, use proprietary encryption algorithms and even masquerade as other applications to evade detection and blocking by traditional firewalls. This makes it much easier to transmit content undetected and unimpeded from inside of a 'secure' enterprise network to the outside world and vice versa. Web 2.0 applications also create a green-field opportunity for a new generation of malware and threats to breach traditional network security firewalls.

Are there other new types of threats I should be concerned about?

Blended threats and Advanced Persistent Threats, or APTs, can use multiple old and new attack methods simultaneously, targeting specific data and even individuals within organizations. Traditional and advanced security measures working together are especially important when defending networks against these new types of multi-faceted and persistent attacks.

[2] Koobface Worm Variant Circulating on Facebook, SC Magazine December 2008; Koobface Variants Explode, SC Magazine, July 2009; New Koobface Campaign Hits Facebook, SC Magazine, June 2011

3 LulzSec Disbands: The Attacks Live On, Infosec Island, June 2011

What are the most important next-generation security features that I should look for?

Application Control

A primary requirement and driver for adoption of next-generation firewalls is application control. In order to prevent data loss and mitigate new threats, organizations must be able to effectively control legacy applications as well as the new breed of Internet-based applications. Next-generation application control must be able to detect, monitor, and control the usage of applications and any associated traffic flows at gateways and at endpoints, regardless of ports and protocols used. In addition, an association must be made between the application and the end user before the proper access rights and security policy can be assigned.

Using the Application Control feature included in FortiGate® platforms, businesses and agencies can detect and restrict the use of applications on their networks and endpoints based on application classification, behavioral analysis, and end user association. Network administrators can define and enforce policies for thousands of applications running on next-generation networks and endpoints. They can detect and control individual features of Web 2.0 applications such as Facebook, Skype, Twitter and Salesforce.com such as allowing chat but disabling the ability to download videos or following links.

Integrated Intrusion Prevention System (IPS)

Deploying updates and patches in large, complex next-generation networks is a complex and time-consuming process. Following a patch release, it can take a large organization weeks or even months to deploy the fix to all affected systems. Fortinet IPS protects networks from both known and zero-day vulnerabilities, blocking attacks that take advantage of unpatched systems.

Fortinet IPS offers a wide range of features that can be used to monitor and block malicious network activity including; predefined and custom signatures, protocol decoders, out-of-band mode (or one-arm IPS mode), packet logging, and IPS sensors. IPS sensors provide a convenient, centralized location to configure and deploy an arsenal of IPS tools. You can install Fortinet intrusion prevention technology, available in all FortiGate and FortiWiFi™ platforms, at the edge of your network or within the network core to protect critical business applications from both external and internal attacks.

Data Loss Prevention (DLP)

Trusted employees can send sensitive data into untrusted zones, either intentionally or by accident. Fortinet DLP uses sophisticated pattern matching techniques and user identity to detect and prevent unauthorized communication of sensitive information and files through the network perimeter. DLP features include fingerprinting of document files and document file sources, multiple inspection modes (proxy and flow-based), enhanced pattern matching, and data archiving.

Numerous communication protocols - including HTTP, HTTPS, FTP, FTPS, email (POP3, POP3S, IMAP, IMAPS, SMTP, and SMTPS), NNTP and instant messaging (AIM, ICQ, MSN, and Yahoo!) – can be monitored for sensitive data. Fortinet DLP can search content based on text strings as well as enhanced pattern matching that includes wild cards and Perl regular expressions. For example, pattern matching can be used to scan network traffic for sensitive personal information such as social security and credit cards numbers.

When a match is found, sensitive content can be blocked, passed or archived, with potential leak notifications generated. DLP can be used to block sensitive information coming into the network or going out. For example, by blocking content often found in spam email messages, DLP can enhance incoming data protection measures.

Web Content Filtering

The Fortinet web content filtering solution begins with traditional URL blocking lists, but goes further by expanding these methods and allowing their use in combination with other Fortinet security functions resident on all FortiGate consolidated security appliances. Fortinet's web content filtering technology enables a wide variety of actions to inspect, rate, and control perimeter web traffic at a granular level. Using Fortinet web content filtering technology, FortiGate appliances can classify and filter web traffic using multiple pre-defined and custom categories.

To accelerate web traffic and content inspection, all FortiGate devices support web cache communication protocol (WCCP) which allows the FortiGate to operate as a router or cache engine. Acting as a router, the FortiGate intercepts web browsing requests from client web browsers and forwards them to the cache engine. The cache engine then returns web content to the client as required. When operating as a WCCP cache server, the FortiGate can communicate with other WCCP routers to cache web content, returning requested content to client web browsers as needed. Fortinet web content filtering is easily accessible through the FortiGate management interface.

Dual-stack IPv4 and IPv6 Support

With the recent exhaustion of the IPv4 address space, many organizations are migrating towards IPv6, the next generation Internet communication protocol. As more content and service providers begin to transition to IPv6, it's essential that organizations deploy network security devices that can deliver the same level of protection for IPv6 content as IPv4. There are mechanisms in place to enable communication between IPv6-only devices and networks with IPv4-only devices and networks.

The two most common are dual-stack and tunnelling:

- Dual-stack is preferable because it allows the security device to process each packet in either IPv4 or IPv6.
- Tunnelling, on the other hand, wraps an IPv6 packet in an IPv4 header, allowing a device to forward a packet but not inspect it. This limited IPv6 support means that it will not be able to inspect the contents for malicious code or unwanted content, allowing unwanted traffic to traverse the network.

FortiGate consolidated security appliances support a dual stack architecture that recognizes and separately routes both IPv4 and IPv6 traffic, providing the same core network security technologies simultaneously for both Internet protocols. Vital network and content protection security features, including routing, are fully supported. Fortinet adopted early support of IPv6, receiving IPv6-Ready and JITC certifications in 2008, both important to global telecommunications carriers. Fortinet also earned the USGv6 certification in 2011, important to the US government and the businesses serving them.

Integrated Secure Wireless Controller

All FortiGate appliances include an integrated wireless controller, consolidating security policies and management of all wired and wireless network traffic into a single pane of glass. The integrated wireless controller provides unmatched visibility and control of both thick FortiWiFi and thin FortiAP™ wireless access points. The same comprehensive threat protection provided for wired networks, including firewall, VPN, intrusion prevention, application control, web filtering, traffic shaping and many other security capabilities, are extended to wireless networks.

Centralized Management

For large installations, FortiManager™ appliances provide centralized policy-based provisioning, configuration, and update management for FortiGate, FortiWiFi, and FortiMail™ appliances as well as FortiClient™ endpoint security agents. By locally hosting security content updates for managed devices and agents, FortiManager appliances minimize web filtering rating request response times and maximize network protection. FortiManager provides a single pane of glass interface to manage and configure all Fortinet appliances.

For additional analysis and reporting capabilities, FortiAnalyzer™ appliances securely aggregate log data from both Fortinet devices and other syslog-compatible devices. Using a comprehensive suite of easily-customizable reports, users can filter and review log records for traffic, event, virus, attack, web content and email data. Information can be mined to determine a user's security stance and assure regulatory compliance. FortiAnalyzer also provides advanced security management functions such as quarantined file archiving, event correlation, vulnerability assessments, traffic analysis, and archiving of email, web access, instant messaging and file transfer content.

How does Fortinet compare with other security vendors?

Table 1: Security vendor feature comparison

	Fortinet	Cisco Systems	Juniper Networks	Check Point	Palo Alto Networks
Performance	Purpose-built FortiASIC processors integrated with custom hardware accelerate firewall, IPS, app control, antivirus and VPN traffic throughput.	No custom security-related ASICs or hardware acceleration.	No custom security-related ASICs or hardware acceleration.	No custom security-related ASICs or hardware acceleration.	Use off the shelf processors (such as Cavium)
Application Control	Full visibility and granular control of more than 1,900 unique apps and protocols including Web 2.0 apps. Inspection of encrypted application traffic including SSL, HTTPS, POP3S, SMTPS and IMAPS.	Limited support of application control across product line.	Limited support of application control across product line.	Requires purchase of separate application control software blade for certain appliances.	More than 1,300 applications controlled.
Intrusion Prevention System	Advanced FortiASIC Security Processor chips accelerate IPS throughput and optimize content inspection for superior performance.	Inferior IPS, firewall and VPN performance.	Inferior IPS, firewall and VPN performance.	Inferior IPS, firewall and VPN performance.	Inferior IPS, firewall and VPN performance. Limited protocol decoders and limited signature coverage.
Security Technologies	Provides complete UTM security functionality on a single platform. All security technologies developed in-house and deployed across all platforms with no extra license fees via the security-hardened FortiOS operating system.	Does not offer complete UTM security functionality on a single platform. Uses third-party OEM agreements for antivirus, antispam, and content filtering (Trend Micro). Primary focus is on networking products, not security.	Does not offer complete UTM security functionality on a single platform. Uses third-party OEM agreements for antivirus (Kaspersky), antispam (Sophos), content filtering (Websense). Different systems run different operating systems such as ScreenOS and JUNOS. Primary focus is on networking products, not security.	Does not offer complete UTM security functionality on a single platform. Uses third-party OEM agreements for antivirus (Kaspersky), content filtering (Websense). Different systems run different operating systems such as SPLAT and Nokia IPSO.	Does not offer complete UTM security functionality on a single platform. Uses third-party OEM agreements for content filtering (BrightCloud & OPSWAT).

(Cont. on page 7)

	Fortinet	Cisco Systems	Juniper Networks	Check Point	Palo Alto Networks
Security Certifications	Most security certifications of any vendor including ICSA, VB100, NSS Labs, FIPS-140, Common Criteria and West Coast Labs.	No ICSA, VB100, or NSS Labs certifications. Primary company focus is on networking products, not security.	No VB100 or NSS Labs certifications.	No ICSA, VB100, NSS Labs, FIPS-140, Common Criteria or West Coast Labs certifications.	No ICSA, VB100, FIPS-140, Common Criteria or West Coast Labs certifications.
Wireless Controller	All FortiGate appliances include an integrated wireless controller with no extra license fees.	Requires purchase of separate license. Not available on all appliances.	Requires purchase of separate license. Not available on all appliances.	Requires purchase of separate wireless controller software blade for certain appliances.	No wireless controller.
Flexibility and Scalability	Full line of purpose-built appliances for small businesses up to large enterprises and service providers. High-end systems are modular to meet security requirements in any size network environment.	Limited appliance line with no modular flexibility.	Separate Juniper and NetScreen appliance lines complicate distributed network security deployments and feature development.	Separate Check Point and Nokia appliance lines complicate distributed network security deployments and feature development. Low-end appliances are from third party source.	Limited appliance line with no modular flexibility. Cannot support large service provider or carrier environments.
Management	Common operating system across all platforms simplifies policy creation and deployment. FortiManager and FortiAnalyzer appliances simplify management and analysis of large installations.	Different products run different operating systems requiring separate management platforms.	Different products run different operating systems requiring separate management platforms.	Different products run different operating systems requiring separate management platforms. Real-time monitoring and reporting require additional licensing.	Management system not in wide deployment.

Conclusion

FortiGate consolidated security physical and virtual appliances from Fortinet are field-proven, purpose-built security platforms that include rock-solid traditional security technologies, as well as protection against next-generation threats such as Advanced Persistent Threats, or APTs, and threats targeting mobile devices. Because Fortinet develops all security technologies in-house (instead of licensing crucial security features from third parties), all FortiGate platforms include finely tuned, hardware-accelerated protective technologies that can integrate new security technologies and scale effortlessly with any size of fast-growing business and any network environment. Fortinet also provides in-depth monitoring and reporting capabilities to alert administrators and users to threats, and to allow further analysis for fine tuning. When combined with FortiGuard Services, FortiGate consolidated security appliances protect your next-generation network and your business against threats now and into the future.

About Fortinet

Fortinet delivers unified threat management and specialized security solutions that block today's sophisticated threats. Our consolidated architecture enables our customers to deploy fully integrated security technologies in a single device, delivering increased performance, improved protection, and reduced costs. Purpose-built hardware and software provide the high performance and complete content protection our customers need to stay abreast of a constantly evolving threat landscape. Our customers rely on Fortinet to protect their constantly evolving networks in every industry and region in the world. They deploy a robust defense-in-depth strategy that improves their security posture, simplifies their security infrastructure, and reduces their overall cost of ownership.

About FortiOS

FortiOS™ is a security-hardened, purpose-built operating system that is the software foundation of FortiGate consolidated security platforms. FortiOS software enables high performance multi-threat security by leveraging the hardware acceleration provided by FortiASIC™ content and network processors. This combination of custom hardware and software gives you the best security and performance possible from a single device. FortiOS helps you stop the latest, most sophisticated, and dynamic threats facing your network today with expert threat intelligence delivered via FortiGuard Security Subscription Services.

FortiOS 4.0 software redefines network security by extending the scope of integrated security and networking capabilities within the FortiGate consolidated security platform. Regardless of the size of your organization, you can benefit from the most comprehensive suite of security and networking services within a single device on the market today.

FortiGuard® Security Subscription Services deliver dynamic, automated updates for Fortinet products. The Fortinet Global Security Research Team creates these updates to ensure up-to-date protection against sophisticated threats. Subscriptions include antivirus, intrusion prevention, web filtering, antispam, vulnerability management, application control, and database security services.

FortiCare™ Support Services provide global support for all Fortinet products and services. FortiCare support enables your Fortinet products to perform optimally. Support plans start with 8x5 Enhanced Support with return and replace hardware support or 24x7 Comprehensive Support with advanced hardware replacement. Options include Premium Support, Premium RMA, and Professional Services. All hardware products include a 1-year limited hardware warranty and a 90-day limited software warranty.

FORTINET®

GLOBAL HEADQUARTERS
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE
Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE
Fortinet Incorporated
300 Beach Road #20-01
The Concourse, Singapore 199555
Tel: +65-6513-3734
Fax: +65-6295-0015

Performance metrics contained herein were attained in internal lab tests under ideal conditions. Network variables, different network environments and other conditions may affect performance results, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding contract with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600.