FORTINET

WHITE PAPER

Powering Security at the Speed of the Business

Why the FortiGate Next-Generation Firewall Is at the Apex of the Industry

Executive Overview

Stolen data fuels a highly profitable cyber-crime economy, one where organizations are under constant attack. In response, network engineering and operations leaders are in search of network and security solutions that increase network visibility, enable immediate threat intelligence sharing, and unlock automated threat protection at all network edges. Fortinet FortiGate next-generation firewall (NGFW) provides real-time and intelligent protection against malware and emerging threats. As part of the Fortinet Security Fabric, FortiGate NGFWs integrate with other Fabric-Ready partner security solutions to improve network visibility and control while simplifying network infrastructure.

Trends Driving NGFW Adoption

In the third quarter of 2018, almost 34,000 new malware variants were detected—a 43% increase over the second quarter and an 129% increase over the first quarter of the year.[1] This trend has continued into 2019, and it poses a serious problem. As threats evolve to become increasingly sophisticated, the risk of a data breach is nearly inevitable at many companies. The median organization in one survey experienced 20 breaches in the past 24 months.[2] Morever, 68% of breaches are not discovered for months or longer.[3] In terms of impact, a 2019 report from Ponemon and Accenture recorded an 11% increase in the number security breaches last year—yielding a 12% higher average cost of cyber crime per company (reaching $13 million USD in 2018).[4] To reduce both exposure and damage caused by a data breach, organizations must re-evaluate their network security strategy.

Network throughput is critical to operational success. Enterprises need security designed to keep up with the digital growth and direction of their network traffic needs. By 2021, global IP traffic is expected to show a five-year compound annual growth rate (CAGR) of 26%, while interconnection bandwidth (for the private exchange of data between businesses) is expected to jump by 48%.[5] Furthermore, encrypted traffic recently hit a new all-time high of over 72% of all network traffic—nearly a 20% increase year-over-year.[6] At the same time, encryption technologies such as secure sockets layer (SSL) and transport layer security (TLS) hide up to 50% of cyberattacks, making inspection of encrypted traffic a non-negotiable feature.[7]

Fortinet NGFWs

- High-performance threat protection
- Validated security effectiveness
- Protection of business-critical applications
- Continuous risk assessment via security rating and workflow and threat intelligence automation
- Integration with the Fortinet Security Fabric
- Enterprise-class security management

Verizon's 2019 Data Breach Investigation Report analyzed more than 41,000 reported security incidents with 2,013 confirmed data breaches.[8]

Network Security Challenges

IT executives consider network security a critical priority, but they also need to reduce the complexity associated with supporting multiple disparate security products. More than three-fourths (77%) of organizations rely on non-integrated point security solutions to some degree—which leaves network defenses vulnerable to cyberattacks.[9] New and evolving compliance requirements further complicate network management in terms of manual workflows for reporting and auditing.

External threat vectors are not the only problems that need to be addressed. With 34% of breaches now attributed to trusted internal users,[10] it has become imperative to segment users, devices, and applications for greater control. With granular access control, a compromised user credential or infected device can easily be isolated, quarantined, or blocked to prevent unauthorized access to sensitive content.

Key NGFW Deployment Requirements

Network engineering and operations leaders need to improve compatibility and shared intelligence across their security solutions. They also need a high level of reliable network performance and open application programming interfaces (APIs) to coordinate and automate responses. Beyond these broader requirements, NGFW evaluation should focus on the following areas:

Highly effective security. A NGFW solution should leverage global threat research and artificial intelligence (AI) as well as local zero-day threat intelligence to reduce the risk of data breaches. A fully featured NGFW solution goes beyond intrusion prevention, application control, and user identity. It should also support capabilities such as web filtering, IP reputation, SSL/TLS inspection, anti-malware protection, and sandboxing to help break the kill chain of attacks.

Visibility and control over network traffic. Establishing transparent visibility across all parts of the distributed organization is essential to securing increasingly complex and distributed networks. A NGFW should use deep inspection to identify applications, users, devices, and threats and then deliver better protection through context-aware policy controls. It should also inspect both clear-text and encrypted traffic to discover things like hidden malware attachments. An effective NGFW solution should also come with single-pane-of-glass management, advanced visualization components, and rich reporting to inform strategic security decisions.

Performance and reliability. NGFW capabilities are only useful if the platform's performance can keep up with normal network operations when all desired NGFW features are enabled. Further, reducing cost and complexity can only be achieved if the NGFW can consolidate traffic from various firewalls or run multiple security services concurrently. To support business continuity and bandwidth requirements, a NGFW platform must deliver highly reliable and resilient firewall capabilities at high-throughput speeds.

Risk mitigation. A truly successful NGFW solution should reduce risks by segmenting network and infrastructure assets in accordance with business intent and continuously evaluating the trust of users and devices. It should provide cost-effective, advanced Layer-7 security for defense in depth.

The Fortinet NGFW Solution

FortiGate NGFWs deliver unparalleled protection, operational ease of use, and the industry's best threat protection in a compact form factor. Powered by AI and machine learning (ML) from FortiGuard Labs, FortiGate NGFWs offer a wide range of integrated security capabilities and services.

- NGFW threat protection
- SSL/TLS inspection
- Intrusion prevention system (IPS)
- URL filtering
- Security rating
- Intent-based segmentation
- IPsec/SSL VPN
- User/device identity and authentication
- Sandboxing
- Networking (LAN, WAN, Wi-Fi)
- Management and reporting

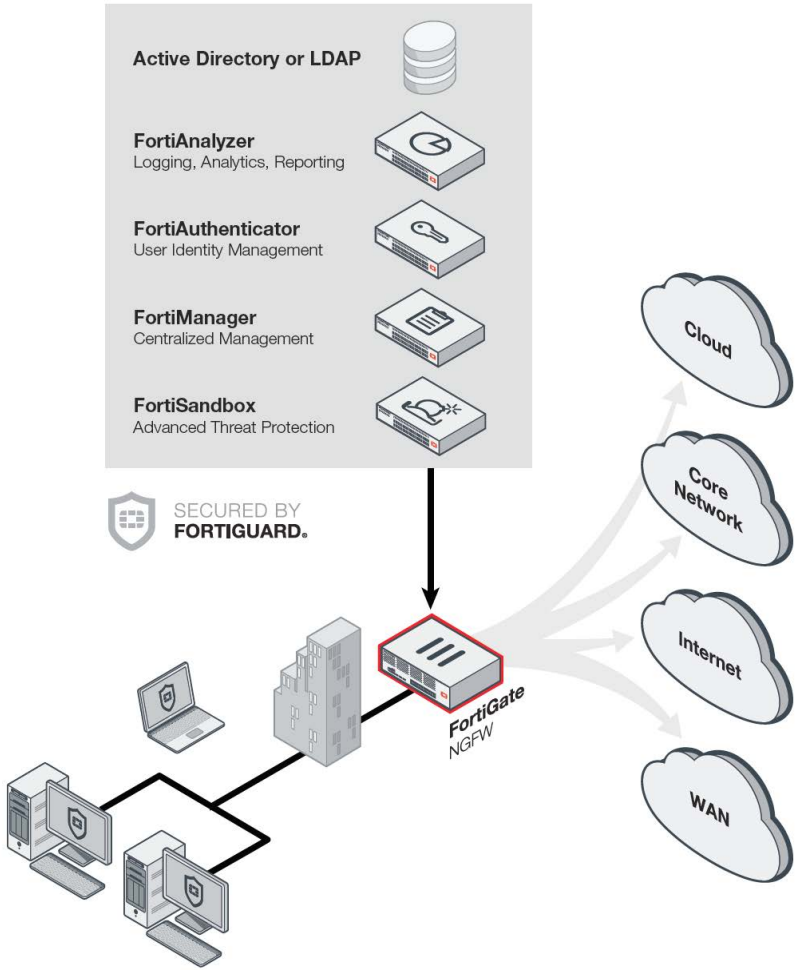

Figure 1: FortiGate NGFW solution deployment.

Active Directory or LDAP

FortiAnalyzer

Analytics-powered security and log management

FortiAuthenticator

User identity management

FortiManager

Automation-driven network management

FortiSandbox

Advanced threat protection

Unparalleled Protection

Effective security solutions keep attacks from damaging organizations—and the more threats blocked, the better. Fortinet technologies are the most validated by independent tests conducted by industry experts. Most recently, FortiGate NGFWs received a "Recommended" rating in NSS Labs 2018 NGFW industry tests by achieving an 100% block rate for live exploits and delivering the lowest-per-protected Mbps total cost of ownership (TCO).[11] FortiGate also delivered high SSL/TLS inspection performance with minimal performance degradation, receiving the best scores in this area among all other tested vendors.

FortiGuard Labs delivers the most advanced threat intelligence to address all phases of the attack lifecycle with top-rated security effectiveness. Threat researchers around the globe keep close watch on the threat landscape 365x24x7. This enables the FortiGuard Labs team to deliver updates to the entire Fortinet Security Fabric ecosystem with some of the fastest response times in the industry.

Increasingly, enterprises look to implement network-based threat protection; however, most network security vendors only offer limited capabilities in this area. In contrast, Fortinet offers an effective, AI-powered threat protection engine that was developed in-house by FortiGuard Labs. Its features include one-to-many signature matching, heuristics, decompression, and emulation. This engine consistently receives ratings from Virus Bulletin, AV-Comparatives, and NSS Labs that are as good or better than other threat protection vendors.[12]

In addition to traditional threat protection, organizations are now also looking to NGFWs for protection from the latest advanced threats. Fortinet FortiSandbox, which earned the coveted NSS Labs Recommendation in the 2018 Breach Detection System and 2017 Breach Prevention System Test,[13] analyzes objects for malicious behavior and is proven effective against zero-day threats. FortiSandbox natively integrates with FortiGate NGFWs and is available as a physical or virtual appliance on-premises, as well as a cloud-based or managed service.

Single-Pane Orchestration, Automation, and Response

The unique, single-platform approach of Fortinet's NGFW solution delivers end-to-end protection that is easy to purchase, deploy, and manage. Single-pane-of-glass security management and visibility helps to simplify the problems of multiple complex consoles. This centralization enables true automation-driven network management with features for flexible deployment. A highly intuitive view of applications, users, devices, threats, cloud service usage, and deep inspection provides unparalleled transparency of what is happening on the network at all times. With this strategic view, one can easily create and manage more granular security policies designed to optimize security and the allocation of network resources.

Figure 2: FortiManager dashboard view.

Using real-time threat intelligence, FortiGate NGFWs enable network engineering and operations leaders to:

- Identify thousands of different applications with application control (including deep application control specific to cloud services) to set up effective application-aware policy enforcement. The FortiGate can inspect SSL/TLS-encrypted and -evasive traffic as well as traffic running on the latest protocols. By integrating this capability with AI-based threat intelligence and sandboxing, FortiGate NGFWs can help uncover both known and unknown malware hidden within applications or encrypted sessions.
- Set granular policies for different types of users with FortiGate user identity management capabilities integrated through Active Directory (AD), Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), Microsoft Exchange, and other authentication sources. This integrated NGFW capability is easily expanded to many more sources for user identity through the addition of Fortinet FortiAuthenticator for large, diverse networks.
- Uniquely identify the type and operating system of devices being used on the network without requiring agents or additional products to set stronger security policies for riskier types of devices.
- Speed incident response with advanced visualization, such as custom threat maps specific to the organization, one-click policies (e.g., device quarantine), and more.
- Reduce administrative workload by leveraging the broadest range of enterprise-class security services. This now includes mobile malware and local sandbox intelligence—all consolidated and managed from a single-pane-of-glass console.

Industry's Fastest Platform

Fortinet purpose-built security processing units (SPUs) drive performance at the heart of the FortiGate platform, delivering industry-leading threat protection and SSL/TLS inspection performance. This level of throughput is needed to deliver on the promise of a great NGFW solution that consolidates multiple security functions on a single appliance—thereby reducing cost and complexity while boosting operational efficiency to keep up with rapidly evolving enterprises.

At the same time, the FortiGate software architecture also leverages parallel path processing to optimize the high-performance hardware and software resources available in packet flow for maximum throughput. As a result, FortiGate NGFWs provide extremely high throughput and exceptionally low latency, while still delivering industry-leading security effectiveness and consolidating functions.

Best-of-Breed Security Reduces Risks and Complexity

Along with new sophisticated threats and escalating breach statistics, organizations simultaneously must manage rapidly evolving network environments that demand more connectivity and greater bandwidth. New and better security solutions are needed—but not at the cost of latency and complexity that impede operations. FortiGate NGFWs deliver the security effectiveness, robustness, and performance needed to secure transforming enterprises without slowing down the business.

[1] "Quarterly Threat Landscape Report Q3 2018," Fortinet, November 2018.

[2] "2018 Security Implications of Digital Transformation Report," Fortinet, July 2018

[3] "The Hidden Dangers of Business Agility" Fortinet, May 2019.

[4] "The Cost of Cybercrime," Accenture and Ponemon, March 6, 2019.

[5] "Bandwith Growth Drives Storage Demand," Forbes, September 24, 2018.

[6] "Encrypted Traffic Reaches A New Threshold," Network Computing, November 28, 2018.

[7] "Study Reveals Hackers Increasingly Use Encryption to Hide Criminal Activity," Lifeline Data Centers, accessed March 21, 2019.

[8] "2019 Data Breach Investigations Report," Verizon, April 2019.

[9] "State of the CIO and Security Report," Fortinet, May 2019.

[10] "2019 Data Breach Investigations Report," Verizon, April 2019.

[11] "Fortinet Receives Recommended Rating in Latest NSS Labs NGFW Report…," Fortinet, July 17, 2018.

[12] "Certifications," Fortinet, accessed May 16, 2019.

[13] "Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests," Fortinet, April 2019.

FORTINET

www.fortinet.com

June 8, 2019 2:20 AM

416367-0-0-EN

D:\Fortinet\White Paper\NGFW SS\WP - NGFW SS V3.1