SOLUTION BRIEF

One Next-Generation Firewall Designed to Protect an Expanding Attack Surface—the FortiGate NGFW

Executive Overview

The widespread adoption of new digital innovations has transformed enterprise networks—adding breakthrough capabilities while at the same time exposing new vulnerabilities. With the rapid proliferation of the mobile workforce, multiple public and private clouds, and Internet-of-Things (IoT) devices, network attack surfaces have dramatically expanded. This makes extended enterprises more difficult to secure. Fortinet next-generation firewall (NGFW) solutions enable broad, integrated, and automated protection against emerging threats and increasing network complexity. It serves as an integral part of the Fortinet Security Fabric—an end-to-end security architecture designed to protect evolving networks.

Fortinet NGFWs

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

Distributed Networks Present a Larger Target for Attack

New technologies are causing enterprise networks to expand. This includes widespread adoption of cloud environments, geographically distributed offices, and a greater number and variety of endpoint devices. Nearly 80% of organizations report they are introducing digital innovations faster than their ability to secure them against cyberattacks.[1]

Threat actors are well aware of this vulnerability. They pinpoint the weakest points across this ever-expanding network surface. They use sophisticated strategies (e.g., multivector or polymorphic attacks) and automated processes to penetrate defenses to then steal sensitive information or to lock down operations in exchange for ransom.

Trying to keep up, network engineering and operations leaders worry about a lack of full visibility into encrypted data as well as control of a network infrastructure that spans applications, data, users, and multiple network edges. At many organizations, a vast number of disconnected point security products operating in silos across the network only increases complexity. The average enterprise uses 75 different security solutions, many of which only address a single attack vector or compliance requirement.[2] This results in a less effective security posture.

Driving the Evolution in Network Security

To improve security effectiveness, network engineering and operations leaders need greater compatibility across the different security solutions deployed across the entire organization. They need security that can share threat intelligence in real time, a high level of reliable network performance at all times, open application programming interfaces (APIs) to coordinate and automate responses, and simplified security management in a single-pane-of-glass console.

Enterprises need to protect the entire expanding attack surface—from IoT to multiple clouds and from users to data. This includes performing secure sockets layer (SSL)/transport layer security (TLS) inspection to detect malware in encrypted flows.

Fortinet FortiGate NGFW solutions address all of these needs by taking a more collaborative and integrated approach across the entire IT infrastructure.

Fortinet FortiGate NGFWs

FortiGate NGFWs simplify security complexity and provide visibility into applications, users, and networks. They utilize purpose-built security processing units (SPUs) and threat intelligence services from FortiGuard Labs to deliver top-rated security and high-performance threat protection (e.g., intrusion prevention, web filtering, anti-malware, application control) for known attacks. The unknown attacks are detected and prevented by Fortinet on-premises and cloud-based advanced threat protection solutions.

As part of the broader Fortinet Security Fabric architecture, FortiGate NGFWs leverage automated, policy-based responses to accelerate time to resolution. When a FortiGate NGFW detects an event, it communicates with the Security Fabric, which determines what information will be shared across the enterprise. For example, when malware is detected in one part of the organization, the Security Fabric shares threat intelligence with the rest of the enterprise IT infrastructure. In another instance, when a policy is created for one security solution, the Security Fabric can contextually apply that same policy across other security solutions in the architecture for consistent and coordinated control.

FortiGate NGFWs allow deployment flexibility that can be tailored to the specific security needs of an enterprise that require either running one or more security features like SSL/TLS inspection, IPS, and antivirus individually or concurrently with minimal performance degradation. All deployed FortiGate devices across the organization's network infrastructure are interconnected via the Security Fabric. This integration provides comprehensive, real-time protection while simplifying deployment and reducing the need for multiple touch points and policies across the enterprise.

Fortinet NGFW Use Cases

- **Reduce complexity.** Consolidate products and services, reduce costs, and maximize return on investment (ROI).
- **Encrypted cloud access.** Achieve transparency and control by inspecting all types of traffic—from clear text to encrypted (SSL/TLS).
- **Visibility and automation.** Gain access to network and security events for contextual visibility while simplifying operations with automated processes.

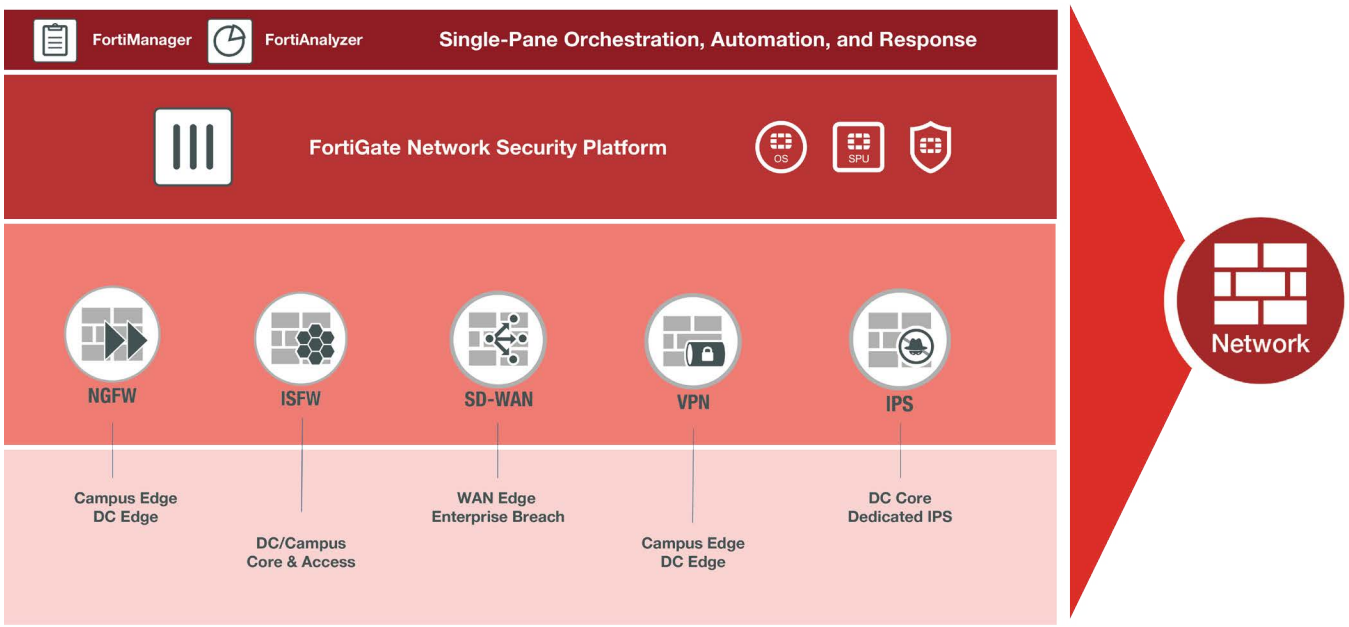

Figure 1: Fortinet next-generation firewall (NGFW) solution.

Industry-Leading Security Effectiveness

Extensive knowledge of the threat landscape combined with the ability to respond quickly at multiple levels is the foundation for providing effective network security. This is why the FortiGuard Threat Intelligence Service—credited with an unprecedented over 700 zero-day threat and vulnerability discoveries[3]—is a crucial enabler of Fortinet world-class NGFW capabilities.

Figure 2: FortiGuard Labs 360 Degrees of Threat Intelligence.

The FortiGuard global threat research team works closely with Fortinet product developers to deliver dynamic security intelligence services. Security updates are instantaneous—automatically and independently validated by third-party research labs. This ensures that the threat intelligence is highly accurate and effective.

One of the primary reasons Fortinet receives consistently high marks in real-world security effectiveness tests, such as those from NSS Labs, Virus Bulletin, and AV-Comparatives,[4] is the combination of in-house research, information from industry sources, and advanced machine-learning capabilities.

Simplify Operations

The unique single-platform approach of the Fortinet NGFW, which includes flexible deployment options, delivers end-to-end protection that is easy to buy, deploy, and manage. Centralized security management and visibility consolidates multiple management consoles into a single pane of glass and unlocks automation-driven management. Specifically, a highly intuitive view of applications, users, devices, threats, cloud service usage,` and deep inspection gives network engineering and operations leaders a better sense of what is happening on their network. With this strategic view, they can easily create and manage more granular policies designed to optimize security and network resources.

Figure 3: FortiManager dashboard view.

Network leaders can transparently observe traffic and set consolidated policies with granular security controls. Network management becomes both automation-driven and analytics-powered via a single-pane-of-glass console for logging, reporting, and central administration.

One NGFW Solution Across the Extended Enterprise

As a foundational part of the Fortinet Security Fabric, FortiGate NGFWs deliver protection that keeps pace with the accelerating demands of high-performance enterprise networking. FortiGate NGFWs feature a purpose-built security processor technology, which provides extremely high throughput and exceptionally low latency while delivering industry-leading security effectiveness and consolidation.

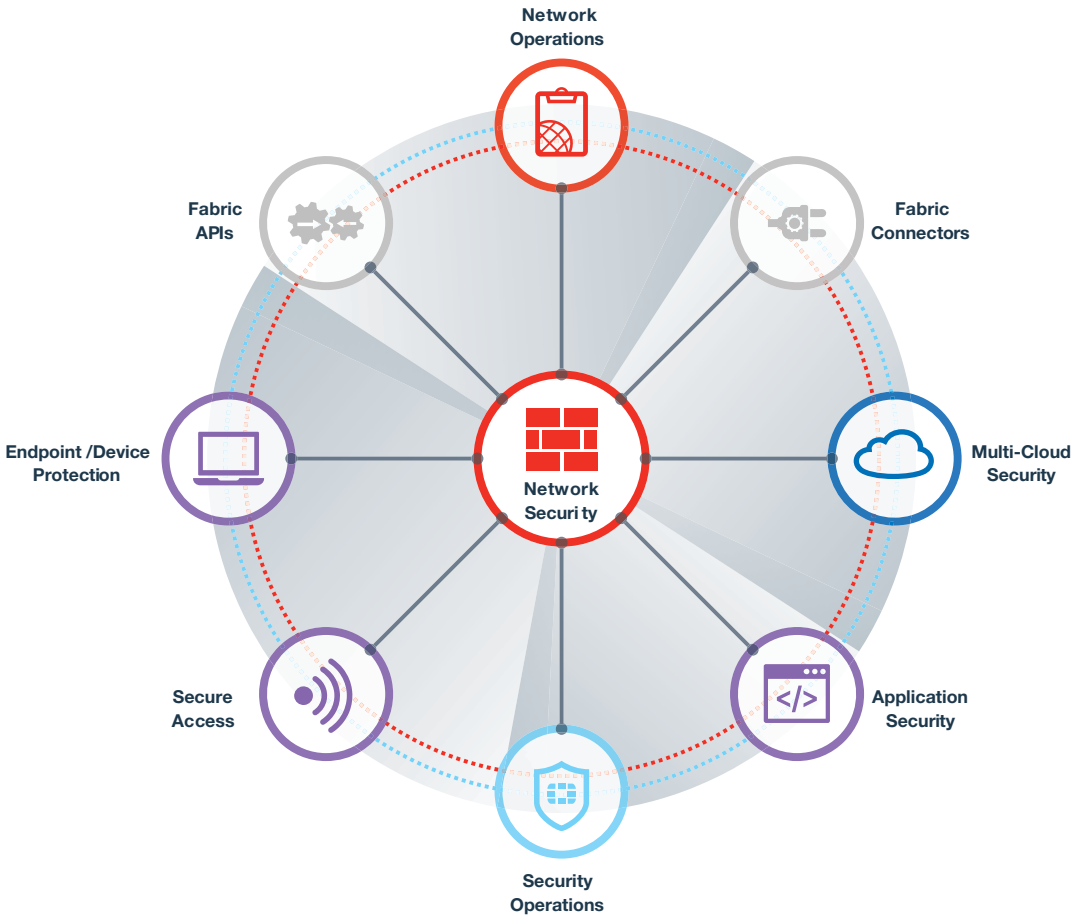

Figure 4: The Fortinet Security Fabric Architecture.

The FortiGate NGFW family includes a set of flexible platforms at various price/performance points that can be deployed at the enterprise edge, data-center edge, or at the branches of a distributed enterprise to provide secure access to multiple clouds. FortiGate NGFWs can also be deployed within the data center as part of an **intent-based segmentation** solution. Intent-based segmentation creates partitions across flat and open networks to reduce the attack surface.

It also applies adaptive access controls that establish continuous trust of users and devices based on user and entity behavior analytics (UEBA).

Enabling a Broad and Dynamic Defense Strategy for the Long Term

Fortinet NGFWs offer universal platform support for all types of deployments—giving network leaders exceptional flexibility across the extended enterprise infrastructure. Managers have the visibility and control they need to counter attackers with a single network security operating system across the entire FortiGate family of solutions.

Additionally, all the FortiGate appliances are interconnected via the Fortinet Security Fabric for automatic distribution of contextual security policies and threat intelligence across an organization.

A single-pane-of-glass dashboard consolidates management views, enhances visibility, and simplifies security policy implementation.

Fortinet Security Scores High in Real-World Security Effectiveness

NSS LABS RECOMMENDED

AV comparatives

vb 100 VIRUS virusbtn.com

ICSA labs CERTIFIED FIREWALL - SMB

COMMON CRITERIA

[1] Kelly Bissell et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture and Ponemon, March 6, 2019.

[2] Kacy Zurkus, "Defense in depth: stop spending, start consolidating," CSO Online, March 14, 2016.

[3] "Zero-Day Research | Fixes Available," FortiGuard Labs, accessed May 16, 2019.

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

FORTINET

www.fortinet.com

June 11, 2019 1:58 AM

D:\Fortinet\Solution Brief\NGFW\SB - NGFW V4

416367-0-0-EN