SOLUTION BRIEF

Hybrid Mesh Firewalls Protect the Expanding Attack Surfaces of Distributed Sites

Executive Summary

The widespread adoption of new digital innovations has transformed enterprise networks—adding breakthrough capabilities while at the same time exposing new vulnerabilities. Network attack surfaces have dramatically expanded with the rapid proliferation of the mobile workforce, multiple public and private clouds, and Internet-of-Things (IoT) devices. Enterprise IT teams must now defend corporate sites that include direct internet access, such as branches and campuses, as well as on-premises data centers, public clouds, and remote sites to support work from anywhere (WFA). This makes extended enterprises more difficult to secure. Fortinet FortiGate Next-Generation Firewalls (NGFWs) are part of a hybrid mesh firewall (HMF) solution that enables broad, integrated, and automated protection against emerging threats and increasing network complexity. FortiGate is 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 the widespread adoption of cloud environments, geographically distributed offices, and a greater number and variety of endpoint devices. Cyberattack damage will amount to about $10.5 trillion annually by 2025, a 300% increase from 2015.[1]

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

Trying to keep up, network engineering and operations leaders worry about a lack of complete visibility into encrypted data and control of a network infrastructure that spans applications, data, users, and multiple network edges. At many organizations, the vast number of disconnected point security products operating in silos across the network only increases complexity. A recent Panaseer report found that the shift to cloud and remote working has driven a 19% increase over the past two years in the number of security tools organizations must manage—from 64 to 76.[2] This results in a less effective security posture, as the same report found that 82% of security leaders have been surprised by a security event, incident, or breach that evaded a control they thought was in place.[3]

Driving the Evolution in Network Security

Network engineering and operations leaders need greater compatibility across the different security solutions deployed across the entire organization to improve security effectiveness. They need security that can share threat intelligence in real time, a high level of reliable network performance, 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 these needs by taking a more collaborative and integrated approach across the entire IT infrastructure.

Fortinet FortiGate NGFWs: Protecting Corporate Sites and Data Centers

FortiGate NGFWs simplify security complexity and provide visibility into applications, users, and networks. Appliances utilize purpose-built security processing units (SPUs) and threat intelligence services from FortiGuard Labs to deliver top-rated security and high-performance threat protection (such as 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 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 to be tailored to the specific security needs of an enterprise that requires 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 touchpoints 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.

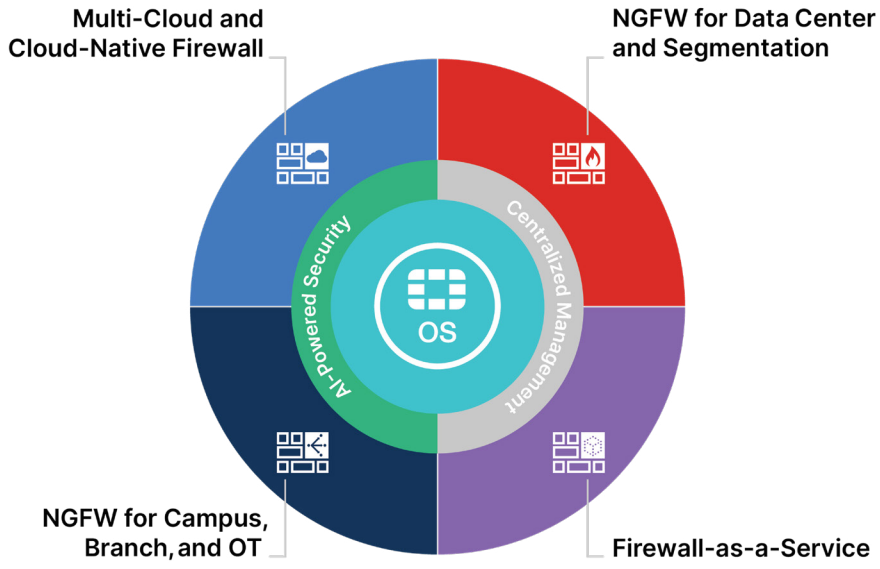

Figure 1: Hybrid Mesh Firewall

Industry-Leading Security Effectiveness

Extensive knowledge of the threat landscape and the ability to respond quickly at multiple levels are the foundations for effective network security. This is why the FortiGuard Threat Intelligence Service—credited with an unprecedented 1,026+ zero-day threat and vulnerability discoveries[4] is a crucial enabler of Fortinet's world-class NGFW capabilities.

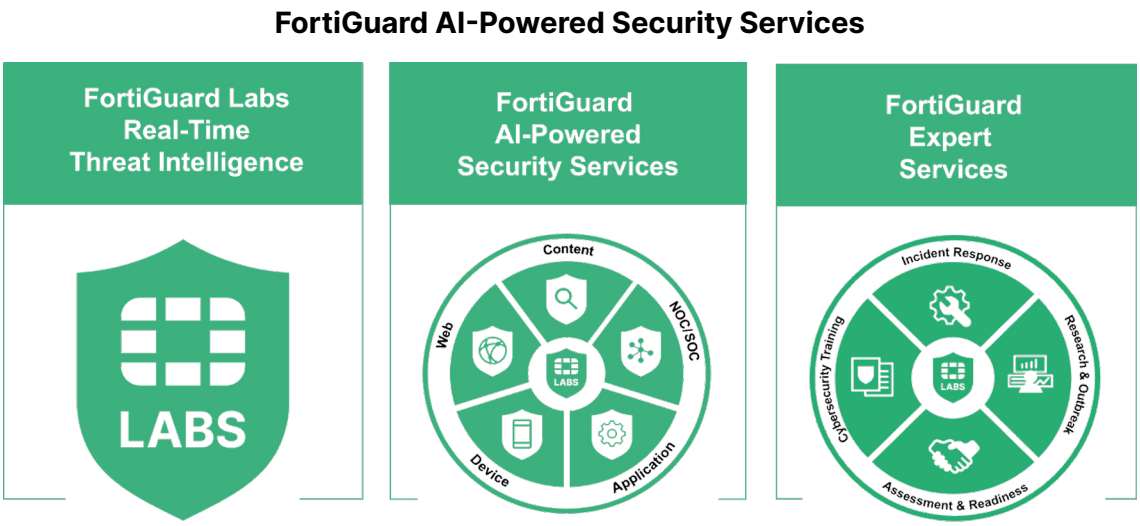

Figure 2: FortiGuard Labs 360 degrees of threat intelligence

The FortiGuard global threat research team collaborates 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.

Fortinet receives consistently high marks in real-world security effectiveness tests, such as those from CyberRatings.org, Virus Bulletin, and AV-Comparatives, due to our combination of in-house research, information from industry sources, and advanced machine-learning capabilities.

Simplify Operations with Centralized and Unified Management

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 consolidate multiple management consoles into a single pane of glass and unlock 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 networks. This strategic view allows them to easily create and manage more granular policies to optimize security and network resources.

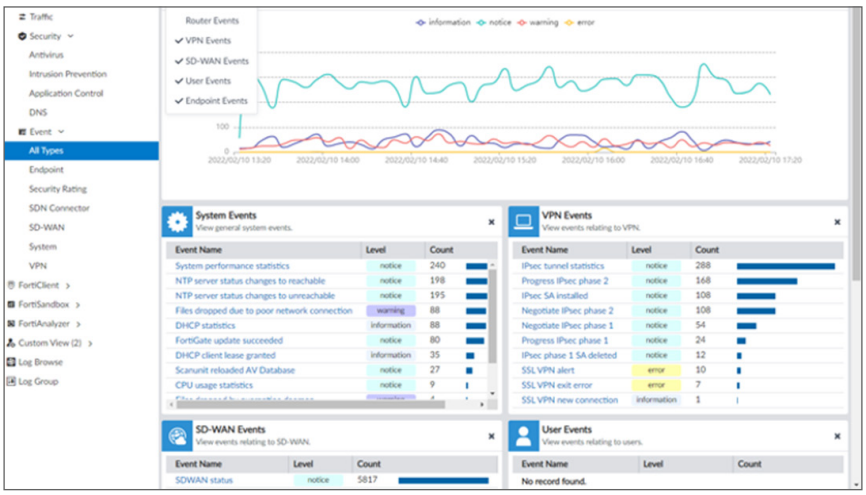

Figure 3: FortiManager dashboard view

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 Hybrid Mesh Firewall Solution across the Extended Enterprise

As a foundational part of a hybrid mesh firewall, FortiGate NGFWs deliver protection that keeps pace with the accelerating demands of high-performance enterprise networking. FortiGate NGFWs feature centralized management that unifies protection across corporate sites such as branches and campuses and on-premises data centers, public clouds, and remote sites for work from anywhere. Every FortiGate NGFW appliance contains purpose-built security processor technology, which provides extremely high throughput and exceptionally low latency while delivering industry-leading security effectiveness and consolidation.

Figure 4: Fortinet Security Fabric

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 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 to automatically distribute contextual security policies and threat intelligence across an organization. FortiGate devices are industry-leading for their security capabilities, rated 99.88% effective against cyber exploits and evasions by CyberRatings.org.[5]

A single-pane-of-glass dashboard consolidates management views, enhances visibility, and simplifies security policy implementation, so you can build a HMF to protect your expanding attack surface across distributed sites, including data centers, public clouds, and remote locations.

[1] Bharath Aiyer, Jeffrey Caso, Peter Russell, and Marc Sorel, New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers McKinsey & Company, October 22, 2022.

[2] Panaseer, 2022 Security Leaders Peer Report, January 2022.

[3] Ibid.

[4] FortiGuard Labs Zero-Day Research, accessed May 31, 2023.

[5] CyberRatings.org, Enterprise Firewall Comparative Report, April 24 2023.

FORTINET

www.fortinet.com

August 7, 2024 6:54 PM / 416367-C-0-EN