FORTINET

WHITE PAPER

Fortinet Delivers Best-of-Breed NGFW Security for Modern Data Centers

NGFW Protection from the Core to the Edge

Executive Overview

Network engineering and operations leaders require integrated security with advanced capabilities designed for protecting hybrid IT data-center environments. Fortinet FortiGate next-generation firewalls (NGFWs) offer a best-of-breed solution that delivers critical risk management against the latest threats, resiliency that ensures business continuity, scalability that extends data-center protection wherever it is needed, and automation and orchestration features that accelerate responsiveness.

Evolving from On-premises to a Hybrid Model

Data-center architectures have evolved from using hard-wired connections that draw direct lines between services into a virtualization-based utility model, where business-critical applications and services are managed using software-defined models. Modern distributed data centers encompass a hybrid IT infrastructure, including Software-as-a-Service (SaaS) applications, compute resources, analytics, and data storage across multiple private and public clouds. These hybrid data centers offer greater agility, flexibility, and scale on demand—as well as an expanded attack surface that requires an equally evolved security strategy.

Security had long been thought of as a mandatory function at the edge of the network: building the strongest possible perimeter defenses to protect the points of entry. But today's threats have changed in every conceivable fashion—in terms of types, their sophistication, and the location (direction) of their attack. Attacks now come from trusted users, devices, and applications that spread malware, both unknowingly and with malicious intent. Hackers that penetrate the perimeter may now roam the network for days or weeks, quietly searching for vulnerabilities and the right opportunity to exfiltrate critical data. Risk exposure can now reach the very core of the data center, where data moves between trusted systems, behind the point products that failed to stop the original perimeter breach.

FortiGate NGFWs Deliver Security to the Core of the Network

To address the challenges of the hybrid IT data center, Fortinet developed FortiGate NGFWs for enterprise data centers. FortiGate NGFWs address the core functions that any enterprise-class firewall must deliver, including policy enforcement, application control services, and intrusion prevention systems (IPS). In addition, FortiGate NGFWs provide granular policy control of users, devices, and applications, as well as secure sockets layer (SSL) and transport layer security (TLS) encryption inspection and sandboxing, all at the network core. The same FortiOS operating system runs across both physical and virtual FortiGate NGFWs to provide advanced threat-protection capabilities across all network locations.

FortiGate NGFWs offer the flexibility to provide protection at the data level as well as at the perimeter. Classifying data to be protected and gaining visibility into the data flow within the data center are both paramount to stopping threats that have been lurking in the network for weeks—bouncing from system to system seeking targets.

FortiGate 7000 Series

FortiGate 7000 series solutions are available in several configurations that enable them to scale with evolving demands and capacities—up to 320 million concurrent sessions. FortiGate 7000 firewalls deliver up to 100 Gbps of SSL/TLS inspection and up to 360 Gbps IPS throughput in a compact form factor. They are flexible enough to be deployed as an L7 NGFW or as an L4 data-center firewall for the edge or internal segments. They allow enterprises to move to IPv6 or run dual-stack IPv4/v6 with no performance penalty.

FortiGate 6000 Series

FortiGate 6000 series solutions offer simplicity and deployment flexibility, including the flexibility to be deployed at the enterprise/cloud edge, in the data-center core, or internal segments. It provides ultrahigh NGFW and threat-protection performance—plus capacity and connectivity to secure vast amounts of network traffic. FortiGate 6000 NGFWs deliver up to 130 Gbps SSL/TLS inspection with minimal performance impact to the network.

Core capabilities and benefits of Fortinet NGFWs include:

FortiGate 3000 Series

FortiGate 3000 series solutions offer L7 advanced security capabilities to enable Intent-based Segmentation and NGFW use cases in the data center. FortiGate 3000 series NGFWs yield up to 30 Gbps threat protection and high SSL/TLS inspection performance (34 Gbps) in a compact appliance. Flexible 10 GbE, 40 GbE, and 100 GbE connectivity offers maximum I/O scalability.

NSS Labs awarded FortiGate a "Recommended" rating for the fifth consecutive year in its annual NGFW industry tests—noting its high-security effectiveness, best-of-breed security with HTTPS inspection, and low TCO.[2]

Performance for exceptional risk management

As a core element of the integrated Fortinet Security Fabric architecture, FortiGate NGFWs are built with dedicated security processors to minimize the impact on network performance for even the most demanding security functions. Because a data-center firewall typically is deployed in the fastest portion of the network, dedicated processors are essential for advanced L7 security. Fortinet's outstanding security performance offers headroom that even anticipates the fact that enterprises are rapidly migrating to a 100 Gbps network core. FortiGate NGFWs include solutions with multiple 100 GbE interfaces and a stateful firewall throughput of more than 1 Tbps.

Resiliency and scalability

FortiGate NGFWs use N+1 redundancy clustering to ensure system real-time failover in the event of a component failure. They provide a fully redundant architecture to eliminate any single point of failure in L4 data-center firewall deployments and the lowest possible latency for time-sensitive applications such as financial use cases. Built with carrier-grade hardware and software, FortiGate NGFWs deliver five-nines (99.999%) reliability and superior mean time between failure (MTBF). FortiGate NGFWs also provide protection and detection regardless of the location of digital assets—which is essential for securing data and applications across a distributed, hybrid infrastructure.

Data-center security must also scale to address ever-increasing traffic flows—including both unencrypted and encrypted data. With as much as 60% of encrypted traffic containing hidden malware,[1] data centers become vulnerable to threats moving secretly in encrypted data flows within the network. Mitigating this requires security that inspects the vast amounts of encrypted traffic moving between users and systems as well as across systems without impacting application performance. Here, FortiGate NGFWs offer high-performance inspection of both unencrypted and encrypted workflows (including TLS version 1.3). Purpose-built security processors provide the power required to address SSL key exchange, IPS signature matching, and Suite B cryptography without a performance penalty.

Automation and orchestration

An integrated security architecture provides the foundation for intelligent automation and orchestration across the hybrid IT infrastructure. As part of the Fortinet Security Fabric, FortiGate NGFWs maximize return on investment (ROI) through point product consolidation. Existing security solutions can connect to FortiGate NGFWs through open APIs, enabling workflow automation, orchestration, and synchronized security that protect against unpatched applications and ever-changing DevOps environments. This comprehensive integration is enriched by indicators-of-compromise (IOCs) visibility that uses both current and past logs for threat detection via consolidated single-pane-of-glass monitoring and management.

FortiGate NGFWs also provide automated compliance reporting, audits, and orchestration that help network engineering and operations leaders comply with evolving government and industry regulations, as well as security standards such as the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS). Further, the Fortinet Security Rating Service (which is part of both the 360 Protection Bundle and Enterprise Protection Bundle) helps organizations proactively manage and improve their overall security posture and detect risks before they lead to compromises.[3]

FortiGate and the Fortinet Security Fabric

FortiGate NGFWs provide not only best-in-class NGFW functionality but they also operate as a core element in the Fortinet Security Fabric, a comprehensive security architecture used to protect the enterprise.

In a nutshell, the Fortinet Security Fabric ties together all security elements to deliver three key attributes:

- **Broad** visibility of the entire digital attack surface
- **Integrated** artificial intelligence (AI)-driven breach prevention
- **Automated** operations, orchestration, and security responses

The Security Fabric integrates solutions beyond the enterprise firewall, including cloud security, advanced threat protection, application security, secure access, and security operations—all managed and coordinated from a single interface. This unified approach allows for seamless management and threat-intelligence sharing across all components of the security architecture.

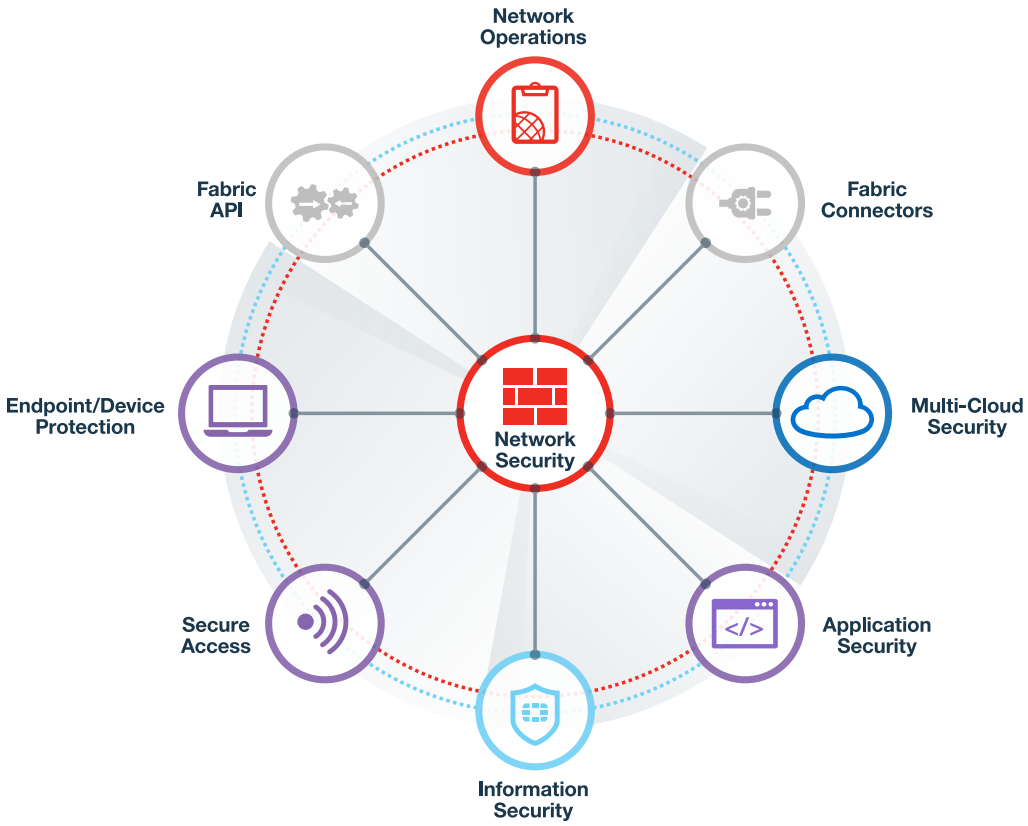

Figure 1: The Fortinet Security Fabric enables multiple security technologies to work seamlessly across all network environments. This helps to eliminate security gaps and accelerate responses to attacks.

Traditional security approaches are geared toward the deployment of point products that address specific security elements—often aspects of the expanded attack surface. This leads to environments where individual products perform their function but do not share information or a common management interface. Comprehensive protection against the latest threats and vulnerabilities requires seamless visibility across all elements of the security infrastructure. For example, when malware is detected by a FortiGate NGFW in one network location, that information is instantly shared across the entire Security Fabric. This enables the rest of the network to have immediate situational awareness to respond to concurrent attacks across other parts of the organization.

Security Designed for Distributed, Hybrid Data Centers

The advanced threat landscape requires greater focus and attention than ever from security network engineering and operations leaders. And with modern data centers demanding ever-increasing levels of performance and bandwidth, these same leaders cannot compromise between security and meeting user demand for access. But there is good news: FortiGate firewalls deliver the highest level of performance and the most advanced threat-intelligence and threat-protection capabilities. They address the perfect storm of threat volume and speed, which can overwhelm all but the highest-performing solutions.

[1] Omar Yaacoubi, "The hidden threat in GDPR's encryption push," PrivSec Report, January 8, 2019.

[2] "Certifications," Fortinet, accessed July 19, 2019.

[3] "Proactive, Actionable Risk Management with the Fortinet Security Rating Service," Fortinet, February 14, 2019.

August 5, 2019 12:02 PM

wp-fortinet-delivers-best-of-breed-ngfw

440460-0-0-EN