SOLUTION BRIEF

FortiGate NGFWs Provide Proactive and Transformative Data-Center Security for Business Continuity

Executive Summary

Businesses today demand unrivaled availability and resiliency in their data centers, but this is challenged by an attack surface that is rapidly expanding and a sophisticated and evolving advanced threat landscape. With FortiGate E-Series next-generation firewalls (NGFWs), organizations can deliver five-nines availability and superior mean time between failures (MTBF), while inspecting all network traffic—encrypted and unencrypted. FortiGate E-Series NGFWs simplify complex security processes resulting from a proliferation of point security solutions. They also provide L7 advanced security by adapting to any segmentation using dynamic objects—all accomplished with single-pane-of-glass visibility and centralized control.

FortiGate E-Series NGFWs

- Best security efficacy as measured by third-party entities
- Best price/performance for encryption inspection and threat protection
- Lowest TCO to maximize business value
- Open APIs—integration with third-party orchestration/automation systems
- Five-nines (99.999%) reliability and a carrier-grade OS (form-factor agnostic)

As Data Centers Evolve, Security Must Keep Pace

Digital transformation (DX) has evolved the nature of the data center from a defensible, on-premises infrastructure to an increasingly distributed hybrid IT environment that combines virtual, on-premises, and cloud elements. These new distributed data centers offer greater agility and new capabilities—where applications are consumed by business users and public users alike (such as in healthcare where both staff and patients require access to services).

But along with the expanded capabilities, the risk of cyberattacks also increases. Combining distributed, cloud-ready data centers with outdated security tools (which were originally designed only for on-premises environments) expands the network attack surface and increases the chances of application outages and disruption to critical infrastructure. The effects of this can be extremely damaging to a business—with the average infrastructure failure costing as much as $100,000 per hour and the hourly damages associated with a critical application failure running between $500,000 and $1 million, according to IDC.[1]

Alongside a growing number of security breaches, the total cost of cyber crime per company reached $13.0 million in 2018—an increase of 12% from 2017.[2]

Adapting an Integrated Security Ecosystem

To ensure continuous operations, network engineering and operations leaders first need to effectively manage risks by protecting critical business applications and services, regardless of their location. They need to build a scalable and resilient network security architecture that can withstand adverse network security conditions within and across a distributed hybrid IT infrastructure.

In addition to the above, they need to move away from relying on isolated point security products that have proliferated as the attack surface has expanded, in favor of an architectural strategy that streamlines operations to reduce both capital expenditure (CapEx) and operating expenditure (OpEx). Indeed, more than three-fourths (77%) of organizations rely on nonintegrated point security solutions to some degree within their organization. This adds cost and complexity while leaving networks vulnerable to cyberattacks.[3] In response, security integration simplifies operations and enables automated workflows, which in turn allows technical security resources to focus on more critical business outcomes and optimizations.

Enabling Effective Data-Center Segmentation

To manage risks, organizations must reduce the attack surface. This can be achieved in part through network segmentation, helping to isolate workloads from one another to secure them individually, while restricting lateral (east-west) movement of malicious intrusions to the network. Segmentation for distributed data centers must be sufficiently flexible to address a broad selection of use cases. The solution must provide scalability, resiliency, and availability across a hybrid IT architecture to maintain business continuity.

However, segmentation by itself does not offer mechanisms to inspect content for threats. Therefore, organizations need an NGFW solution that can adapt to various segmentation techniques and communicate with third-party security solutions to share threat intelligence and provide automated threat protection.

Proactive Security Features for Expanding Risk Exposures

The **FortiGate E-Series NGFWs**, which are an integrated part of the Fortinet Security Fabric, address these evolving data-center security requirements. Specifically, integrated threat intelligence from FortiGuard Labs is included with the FortiGate E-Series NGFWs to prevent known attacks plus artificial intelligence (AI)-driven detection of unknown attacks (via FortiSandbox). This collective threat intelligence is shared in real time across all of the parts of the security infrastructure, thus helping organizations to improve their risk posture.

Core capabilities of the FortiGate E-Series NGFWs offer network engineering and operations leaders the best choice for several different reasons:

Risk management

FortiGate E-Series NGFWs are designed for deep integration into third-party technologies and platforms in multivendor infrastructures. Fabric Connectors and Fabric-Ready Partner compatibility enable two-way communications and threat-intelligence sharing. FortiGate NGFWs can adapt to any segmentation strategy (absorbing network changes using dynamic objects) and they provide L7 advanced security with a very high fidelity. Indeed, third-party testing shows that FortiGate NGFWs provide industry-leading security efficacy.[4]

FortiGate NGFWs have received five consecutive "Recommended" ratings from NSS Labs in its annual NGFW industry tests.[5]

Resiliency and scalability

Data centers demand maximum availability and resiliency. FortiGate E-Series NGFWs achieve five-nines availability and superior MTBF by applying N+1 redundancy clustering (to ensure system backup in the event of a component failure), in addition to carrier-grade hardware and software.

Network security must also scale to protect all traffic—both unencrypted and encrypted. Inspecting encrypted traffic is a requisite, with 72% of network traffic now with secure sockets layer (SSL)/transport layer security (TLS) encryption.[6] With upwards of 50% of cyberattacks using SSL/TLS encryption to infiltrate networks or exfiltrate data, employing SSL/TLS inspection is a requisite.[7] But with many NGFWs experiencing serious performance degradation when SSL/TLS inspection is turned on, this incurs substantial increases in CapEx and OpEx.

FortiGate NGFWs deliver high-performance inspection of both unencrypted and encrypted workflows (including TLS version 1.3). Specifically, they deliver industry-best price/performance for SSL inspection and one of the best total cost of ownership (TCO) per protected megabit per second (Mbps)—even when SSL/TLS inspection is activated.[8]

Automation and orchestration

As an essential part of the Fortinet Security Fabric architecture, FortiGate NGFWs maximize business value through point product consolidation and integration. Existing security solutions integrate with FortiGate NGFWs through open APIs, enabling workflow automation, orchestration, and synchronized security to protect against unpatched applications and ever-changing DevOps environments. This comprehensive integration is enriched by indicators of compromise (IOCs) visibility into current and past logs for threat detection via single-pane-of-glass monitoring and management.

FortiGate NGFWs also enable network engineering and operations teams to keep pace with new and evolving government and industry regulations, as well as adherence to security standards such as those from the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS) through automated compliance reporting, audits, and orchestration. In addition, the Fortinet Security Rating Service[9] (which is part of both the 360 Protection Bundle and Enterprise Protection Bundle) allows network engineering and operations leaders to proactively manage and improve their overall security posture over time, while simultaneously detecting risks before they cause problems.

Securing an Expanding Data-Center Attack Surface

As data centers become increasingly distributed across hybrid IT environments, network engineering and operations leaders must ensure availability for business continuity. First, they must adopt an integrated security architecture for features such as shared threat intelligence, advanced segmentation, and access control. Second, they need resilient security that manages risks while scaling as traffic demands increase. Finally, they require automation and orchestration of security workflows to reduce cost.

The FortiGate E-Series NGFWs meet all three of these requirements, providing a cornerstone to any security approach—an integrated security offering that adapts to the changing shape and nature of the data center. This ensures industry-leading protection while simplifying operations and reducing TCO.

[1] Kevin O'Connor, "Is Your Disaster Recovery Plan Up to Date?," CIO, April 18, 2016.

[2] "Ninth Annual Cost of Cybercrime Study," Accenture and Ponemon Institute, March 6, 2019.

[3] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, May 23, 2019.

[4] "Certifications," Fortinet, accessed July 12, 2019.

[5] Ibid.

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

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

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

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

July 17, 2019 8:21 AM

452438-0-0-EN

D:\Fortinet\Solution Brief\RED SB\FortiGate E-Series SS\FA - Solution Brief - FortiGate E-Series SS