SOLUTION BRIEF

How to Achieve Optimal Internal Segmentation with FortiGate NGFWs and the Fortinet Security Fabric

Executive Summary

As network traffic shifts from corporate data centers to multiple clouds, attack surfaces are increasing exponentially. Internet of Things (IoT), mobile-first, and other digital transformation (DX) initiatives are adding to network vulnerabilities. To protect their digital assets, network engineering and operations leaders need to go beyond perimeter-based network security to implement a defense-in-depth strategy with Internal Segmentation. This involves defining security zones inside the network—and policies controlling access to those zones—based on business logic.

A key tenet of Internal Segmentation is the ability to enforce access control policies by deploying next-generation firewalls (NGFWs) wherever they are needed. This solution guide explains why Fortinet FortiGate NGFWs—including the new FortiGate E-Series and F-Series—are the best choices for this role. Their high-performance Layer 7 inspection, powered by purpose-built security processing units (SPUs), and the industry's lowest total cost of ownership (TCO) per protected Mbps are strong starting points. Organizations can derive even greater value from the fact that FortiGate solutions integrate seamlessly into the unique artificial intelligence (AI)-enabled Fortinet Security Fabric.

Fortinet's Innovative Approach to Internal Segmentation

With the Fortinet Security Fabric, organizations can intelligently segment users, devices, and applications, regardless of their location—whether on-premises or in multiple clouds. Using innovative features of the Fortinet Security Fabric operating system (FortiOS), network operators can define dynamic and granular access control policies. Through integration with multiple verified trust assessment sources, the Security Fabric establishes and maintains accurate trust levels for users, devices, and applications. Physical and virtual FortiGate NGFWs, deployed throughout the network, enforce these policies through high-performance, Layer 7 inspection of both encrypted and clear-text traffic.

Other components of the Security Fabric, FortiSandbox AI-driven sandboxing and AI-powered FortiGuard threat intelligence, detect and mitigate unknown threats and share the threat information with all other Security Fabric components.

Recommended by NSS Labs

In extensive testing during the NSS Labs 2018 NGFW Group Test, Fortinet NGFWs achieved the following:

- High SSL/TLS inspection performance with the lowest performance degradation of all products, demonstrating efficacy across all cipher suites and emergent ciphers tested
- 100% blocking of live exploits being used or that have been used in various attack-related campaigns[1]
- Lowest TCO per protected Mbps among the participating vendors

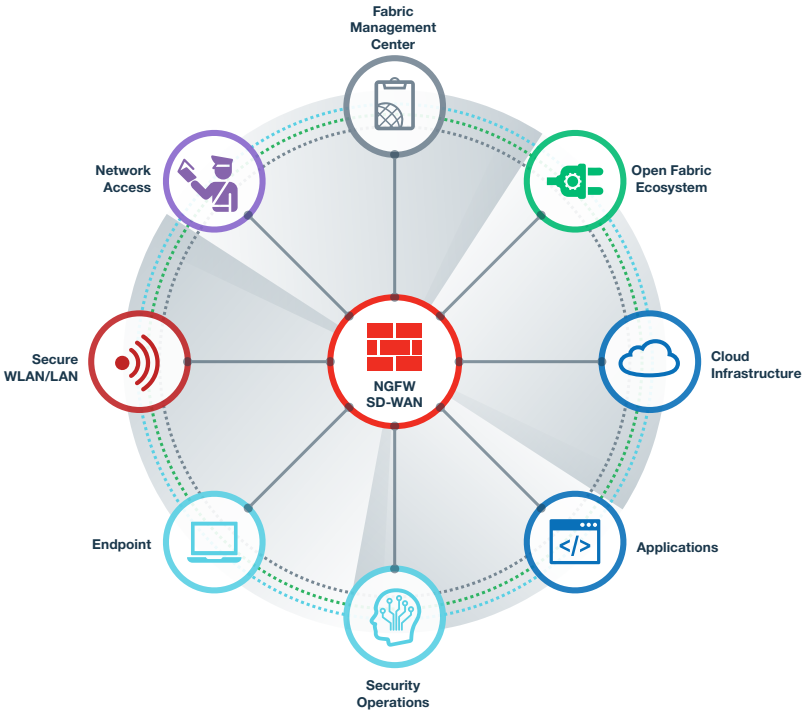

Figure 1: The Fortinet Security Fabric enables multiple security technologies to work seamlessly together, across all environments and supported by a single source of threat intelligence. This eliminates security gaps in the network and hastens responses to attacks and breaches.

Advantages of FortiGate NGFWs for Internal Segmentation

The access control policies defined through Internal Segmentation are meaningful only if they can be enforced. That means deploying security components on every segment and inspecting every packet that comes through. The security checks must be rigorous, without impeding network performance. Also, they must permit or deny access based on up-to-date threat intelligence and trust information. Fortinet NGFWs rise to these challenges, with several technological and operational advantages:

High performance to make deep inspection practical

As the majority of internet traffic is now encrypted, it is essential to inspect secure sockets layer (SSL) and transport layer security (TLS)-encrypted traffic as well as clear text. Powered by Fortinet patented parallel-path SPUs, FortiGate NGFWs eliminate the trade-off between rigorous inspection and network performance. For example, in independent tests, FortiGate E-Series firewalls delivered SSL/TLS inspection performance (at Layer 7) that is more than four times higher than that of competing solutions.[2] This minimizes performance degradation when SSL/TLS inspection and other security services—including intrusion prevention system (IPS) inspection, antivirus protection, email and web filtering, and data leak protection—are performed concurrently. Figure 2 shows the performance specifications for two of the FortiGate E-Series NGFWs.

FortiGate FG-1800F	
Threat Protection	9 Gbps
SSL/TLS Inspection Throughput	15 Gbps
Network Interfaces	Multiple 40 GE QSFP+, multiple 25GE, 10 GE SFP28/SFP+, two 10GE SFP+ HA, multiple 1 GE SFP, multiple 1 GE RJ45

FortiGate 3400E	
Threat Protection	23 Gbps
SSL/TLS Inspection Throughput	30 Gbps
Network Interfaces	Multiple 100 GE, 40 GE, QSFP28, multiple 10 GE SFP+/SFP

Figure 2: The high-performance FortiGate E-Series firewalls are the core of an enterprise Internal Segmentation solution.

Low TCO to enable ubiquitous deployment

In extensive testing during the NSS Labs 2018 NGFW Group Test, Fortinet NGFWs achieved the lowest TCO per protected Mbps among the participating vendors, making Fortinet an ideal platform for the defense-in-depth strategy that network engineering and operations leaders need.[3] Also, with the high performance of the FortiGate NGFWs, there is less of a need to deploy multiple appliances in parallel to avoid SSL/TLS inspection latency, as is the case with competing firewalls. Fewer firewalls covering the same attack surface leads to lower CapEx and ongoing management requirements.

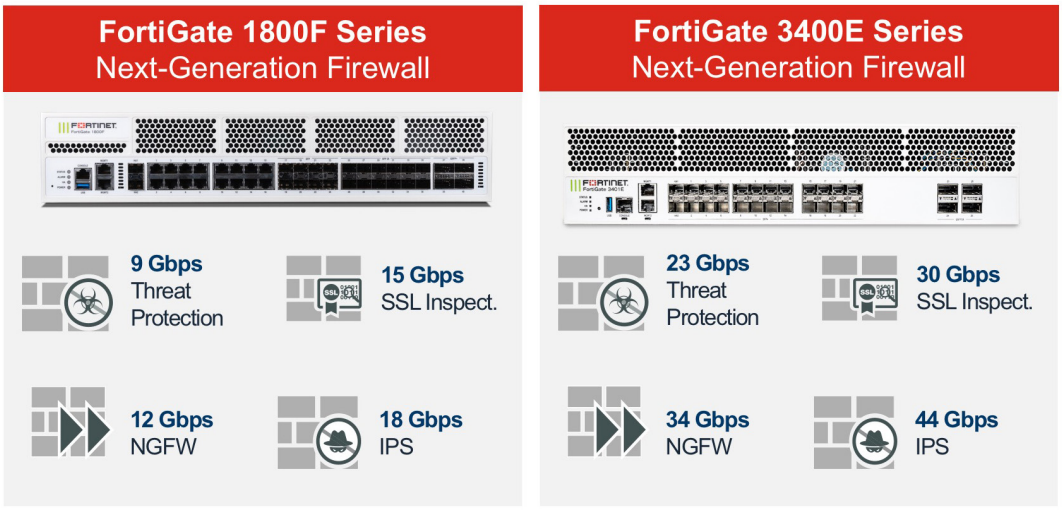

Figure 3: Fortinet NGFWs offer high port densities, a variety of form factors, and the best price/performance for threat protection, SSL/TLS inspection, and IPS. This lowers the TCO of enforcing Internal Segmentation access policies.

Access policies driven by business logic and maintained through continuous trust monitoring

Fortinet provides centralized, dynamic policy controls and enforcement based on business logic that is created using user and application groups. It is also enforced irrespective of the location of the users and applications.

In particular, the Fortinet asset tagging feature, introduced with FortiOS release 6.0, allows the tagging of users, devices, and applications across an organization's entire network (Figure 4). This feature can easily evolve to support creation of security policies that are based more on business logic than traditional IP and port-based policies. This results in consistent enforcement of security policies and improved operational efficiencies. FortiGate NGFWs can also permit or deny access to network resources when risk and trust assessments change as a result of suspicious user, application, or device behavior.

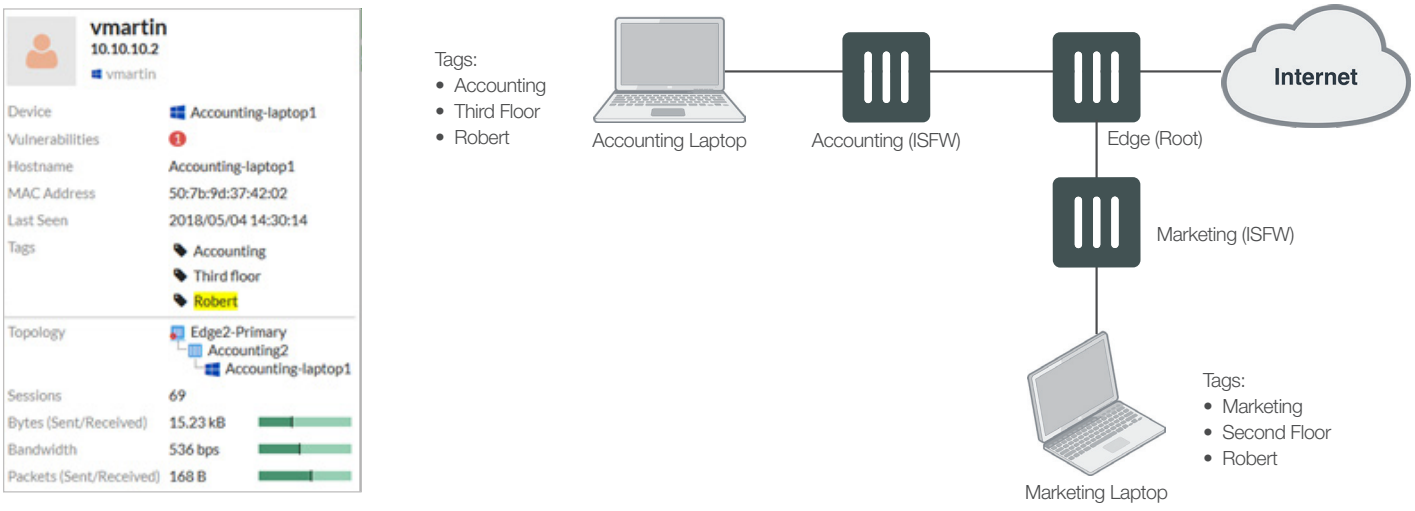

Figure 4: Once business-logic tags are defined and applied, they can be used to enforce access policies throughout the Fortinet Security Fabric.

Trust can also be continuously monitored by Fortinet Identity and Access Management capabilities within the Security Fabric using FortiAuthenticator or by a third-party trust engine, allowing organizations to dynamically adjust and enforce security policies. At the same time, the FortiNAC network access control solution enables network engineering and operations leaders to manage network access—from devices, to users, to applications.

FortiGate NGFWs establish and monitor trust on multiple levels:

- Business logic
- Orchestration (Fabric Connectors to third-party trust engines)
- User identity
- Network address

A Broad, Integrated, and Automated Internal Segmentation Solution

Beyond noting the robust feature set and performance specifications of the FortiGate NGFWs, network operations and engineering leaders need to demonstrate to their executives that their Internal Segmentation solution improves risk management and overall security posture. They also need to show that any Internal Segmentation solutions they deploy will complement existing networking technologies rather than overlapping or replacing them. The following features of the Fortinet Security Fabric meet both of these objectives:

Proactive, actionable risk management and compliance

The Fortinet Security Rating Service, which is included in the 360 Protection Bundle and Enterprise Protection Bundle subscription services, provides dashboards that allow security teams to prioritize vulnerability patching as well as tools to automate configuration changes (Figure 5).[4] The results can be reported to executive management, boards of directors, and auditors, helping the organization understand how its security posture is changing over time. Further, automated dashboards communicate risk management to different personas, providing a clear view of the organization's overall security posture as compared with peer organizations.

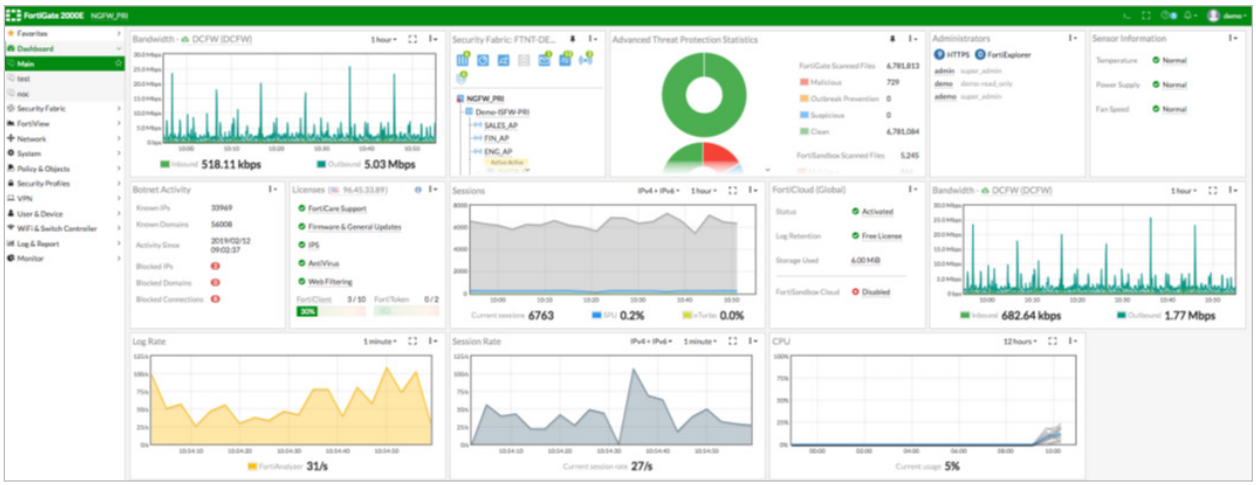

Figure 5: The Fortinet Security Rating Service dashboard.

The Security Rating Service also helps organizations run compliance checks to satisfy auditors' requirements and meet Center for Internet Security (CIS) and National Institute of Standards and Technology (NIST) cybersecurity standards. By continually analyzing and reporting on changes to network topology, the service simplifies identification and remediation of high-risk and noncompliant devices and provides action plans and progress reports for both technical- and management-level stakeholders. Customers can also implement the real-time Security Rating Service across every FortiGate deployment with FortiManager and achieve aggregated reporting with FortiAnalyzer.

Easier integration with trust and threat-intelligence services

Making sense of disaggregated threat alerts from different vendors and technologies can be a major challenge for cybersecurity professionals.[5] FortiGate NGFWs employ Fortinet Fabric Connectors as integration points to Fabric-Ready Partners. For third-party security products not currently part of the Security Fabric, organizations can easily and quickly build their integrations using REST APIs. Fabric Connectors integrate with third-party trust-monitoring engines to continually gather proactive threat intelligence from outside sources. FortiGate devices can then enforce the outside trust engine verdict on the network (Figure 6).

Integrated Third-Party Threat Protection

The FortiGate NGFWs leverage Fabric Connectors to seamlessly integrate with external security ecosystems, sharing threat intelligence quickly for automated remediation.

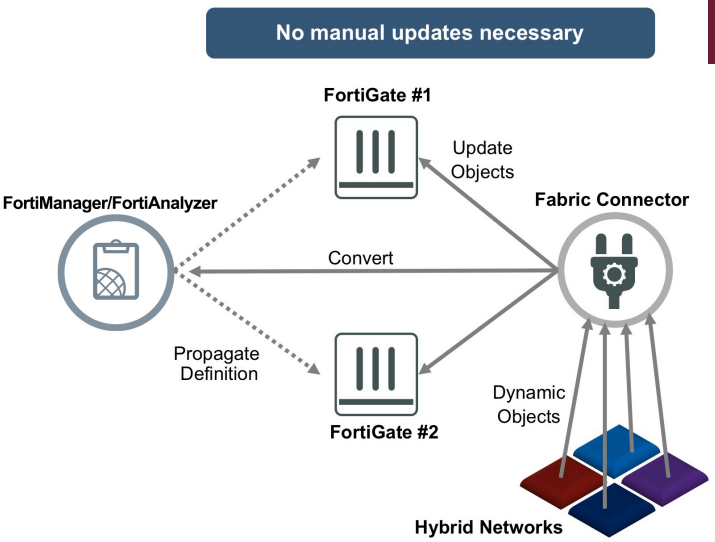

Figure 6: Fabric Connectors provide open, API-based integration and orchestration of FortiGate NGFWs with multiple trust-monitoring engines.

Complements other segmentation solutions

Fortinet Internal Segmentation is designed to fill the gaps in existing segmentation solutions, without replacing or reconfiguring existing network management software. Fortinet provides high-performance advanced (Layer 7) security and network access control for prevalent segmentation solutions (e.g., micro-segmentation with VMware NSX [Figure 7] and application-segmentation with Cisco ACI). Customers can complement their existing segmentation solutions with robust and granular security controls.

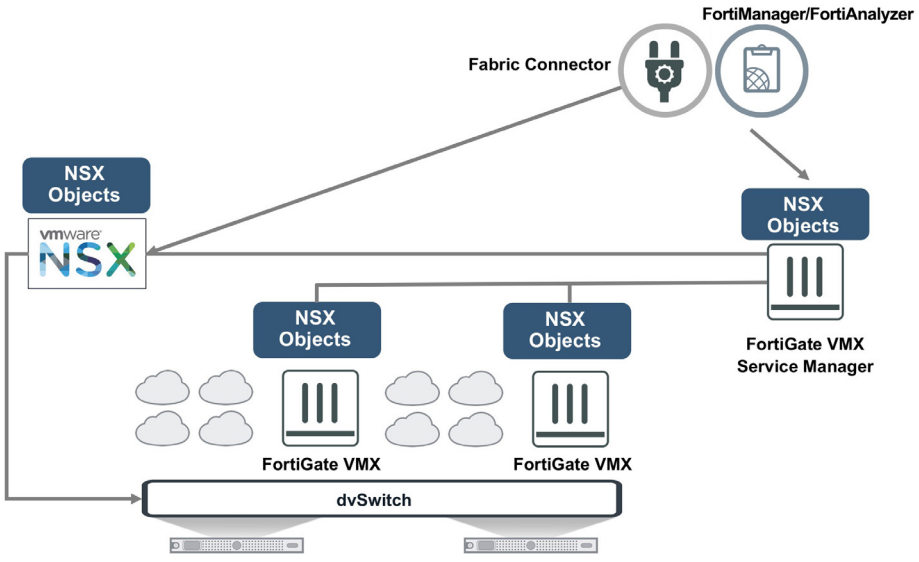

Figure 7: Fabric Connectors provide open, API-based integration and orchestration of FortiGate NGFWs with multiple trust-monitoring engines.

Acing Internal Segmentation with FortiGate and the Fortinet Security Fabric

Recognizing that threats will find ways to penetrate network perimeter defenses, Internal Segmentation helps organizations mitigate east-west (lateral) threats. It achieves this through granular and dynamic access control, continuous trust assessment, end-to-end visibility across IT and OT spaces and into encrypted and nonencrypted flows, and automated threat protection. Fortinet helps network engineering and operations leaders implement effective Internal Segmentation at an unmatched price-performance ratio.

Fortinet solutions seamlessly expand to the new edges of the network, deliver unparalleled performance and reliability, and provide centralized controls and comprehensive visibility across the entire attack surface. The benefits are improved risk management, protection of critical business applications and services, compliance with industry regulations and data privacy rules, and higher operational efficiency with effective security posture management.

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

[2] Based on Fortinet testing.

[3] Thomas Skybakmoen, "Next Generation Firewall Comparative Report: Total Cost of Ownership (TCO)," NSS Labs, July 17, 2018.

[4] "Proactive, Actionable Risk Management with the Fortinet Security Rating Service," Fortinet, April 5, 2019.

[5] Kirsten Bay, "The security tech stack is out of control, here is what to do about it," CSO Online, October 11, 2017.

March 11, 2020 3:24 PM

361436-0-0-EN

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2019:sb-red-ibs-network-leader-ph:sb-red-ibs-network-leader Folder:sb-red-ibs-network-leader