SOLUTION BRIEF

Powering Advanced Research with Scalable, Robust Security in Hyperscale Data Centers

The adoption of digital innovation is forcing the world's largest enterprise organizations to implement hyperscale architectures. These architectures are designed to meet unprecedented business demands generated by the requirements for enormous capacity and astronomical performance. While other industries require hyperscale data centers, pharmaceutical and oil and gas companies are two prevalent example sectors with advanced research foci that see increased business value by implementing a hyperscale architecture.

Securing these data centers requires hyperscale-enabled firewalls that offer high-performance Layer 4 security and the ability to transfer massive datasets. These "elephant flows"—where a single session consumes a large amount of bandwidth—enable organizations to achieve business outcomes faster while capitalizing on existing investments.

FortiGate next-generation firewalls (NGFWs), based on the Fortinet seventh-generation network processor (NP7), provide these capabilities, allowing advanced research institutions to apply access controls while maintaining high performance and supporting high-speed traffic encryption while transferring large datasets in hyperscale environments. The FortiGate NGFWs that are powered by NP7 also protect against volumetric attacks with hardware-accelerated distributed denial-of-service (DDoS) protection. Additionally, these NP7-based FortiGate NGFWs are very efficient when it comes to power usage without sacrificing performance, resulting in compact and cost-effective hyperscale firewalls.

FortiGate 1800F series helps secure hyperscale architectures:

- Support for 40 Gbps flows
- IPsec encryption at high speeds of 65 Gbps
- High-density I/O in a compact form factor—2RU
- Efficiency—low power consumption

Introduction

Digital innovation fuels modern research institutions in significant ways. They increasingly require processing of massive datasets in order to achieve their business goals, enabling them to establish a dominant position in the market they play and subsequently increase shareholder value.[1]

These institutions are adopting hyperscale architectures that can meet unprecedented business demands through enormous capacity and astronomical performance to deliver business outcomes faster.[2] The pharmaceutical industry, for example, is transitioning to the use of machine learning (ML) and artificial intelligence (AI) to more accurately determine the impact of drugs upon test subjects and to perform simulations regarding the possible impact of new medicine.[3] Their overarching goals are faster discovery and bringing better, safer, and more cost-effective drugs to the market—all ahead of their competition. In doing so, they can garner market share and competitive advantage.

Similarly, the oil and gas industry requires high-throughput connections to share massive amounts of exploration information (datasets) across different sites.[4] These datasets are used for AI and ML analytics and discovery that is directly tied to the business outcome, such as adding more capacity and serving a larger market than they are currently able to do. And larger markets mean larger market share, which potentially means more revenue.

Today's accelerated research demands different network and security requirements than have ever been envisioned. Many of these organizations have invested in routing and switching infrastructures capable of carrying 100 Gbps flows. These flows can handle extremely large files of research data in an efficient manner. Yet, in their quest for security, organizations with hyperscale data centers often struggle to source firewalls that can support single data flows at 100 Gbps throughput. As a result, these organizations often do not implement security at network entry and exit points—a significant challenge for network engineering and operations leaders.

Hyperscale Architectures Require Hyperscale Security

Organizations now realize that foregoing security is no longer a sustainable or viable business strategy. However, not all NGFWs implement Layer 4 security, and many struggle to achieve 10 Gbps throughput on a single flow, leaving much of an organization's bandwidth investment unused. Historically, organizations have been forced to make a tradeoff between security and taking full use of their WAN investment.

The Fortinet NP7-powered hyperscale NGFW provides a solution to this problem. These hyperscale NGFWs implement Layer 4 security policy, achieve access control (viz., who is allowed versus not allowed), and prevent volumetric attacks. They also provide high-performance firewall throughput, support high-throughput single data sessions, and allow organizations to achieve faster time to market.

Of particular note is the enhanced capabilities resulting from the NP7, which dramatically increases the FortiGate NGFW's Layer 4 performance. Specifically, the Fortinet NP7 security processing unit (SPU) has multiple very high-speed ports that are capable of handling traffic flows at 40 Gbps. This support for multiple, parallel 40 Gbps flows can dramatically increase the rate of data transfer, providing up to 195 Gbps throughput between research centers. Massive datasets can be broken up and transferred over parallel connections, or multiple large datasets can be sent at once. This delivers significant business and productivity impact, as researchers no longer need to wait for network flows to complete or schedule them during off hours. This ultimately equates to faster time to market and increased capacity.

High-performance Layer 4 NGFW Eliminates Performance/Security Tradeoff

Beyond a higher firewall port capacity, securing hyperscale architectures requires an NGFW to process network traffic and enforce security policies at wide-area network (WAN) speeds. This enables the NGFW to enforce strong access control policies on the network link as well as on the device responsible for inter-site communications. As a result, organizations can ensure that valuable network bandwidth is used solely for legitimate business purposes.

The FortiGate 1800F series is the first line of FortiGate NGFWs built using the NP7. FortiGate 1800F series NGFWs incorporate a firewall with a maximum throughput of 195 Gbps. This represents a 13x improvement on the industry average (see security compute rating in figure 1).

High-speed IPsec Processing Supports Compliance

Data protection regulations like the EU's General Data Protection Regulation (GDPR) require strict security controls on protected data. For organizations transmitting sensitive data that contains patient or subject information (e.g., pharmaceutical research data) over network connections, these regulations mandate the use of IPsec or similar encryption mechanisms to achieve data privacy.

Once again, the FortiGate 1800F series NGFWs with NP7 processors provide the answer, as they are capable of processing IPsec traffic at 60 Gbps. When processed at this speed, encryption protocols do not encumber network performance, obviating concerns that compliance will conflict with research activities.

Low Power Consumption

When processing massive network traffic flows, power efficiency is a significant concern. For example, achieving 60 Gbps IPsec transmission using a cluster of Intel CPUs consumes 2,380 watts.[5]

In response, the Fortinet NP7 processor is optimized to provide extremely high performance with low power consumption. For example, achieving the same IPsec throughput on NP7 consumes only 20 watts, less than 1% of the consumption of Intel CPUs. These significant efficiency gains enable research institutions to deploy the security that they need in hyperscale architectures without significant additional expense or overhead. And as most organizations now have green computing objectives,[6] this reduction in power consumption enables them to reduce the carbon footprint of their network security infrastructure.

Industry's Best Security Compute Rating

Specification	FortiGate 1801F	Industry Average	Security Compute Rating	PA-3260	SG-5600	FPR-2130
Firewall	195 Gbps	150 Gbps	13x	10 Gbps	25 Gbps	10 Gbps
IPsec VPN	60 Gbps	4.3 Gbps	14x	4.8 Gbps	6.5 Gbps	1.5 Gbps
Threat Protection	10 Gbps	3.74 Gbps	2.7x	4.7 Gbps	2.78 Gbps	N/A
SSL Inspection	15 Gbps	0.735 Gbps	20x	N/A	N/A	0.735 Gbps
Concurrent Sessions	12M	2.73M	4x	3M	3.2M	2M
Sessions per Second	500k	114k	4x	118k	185k	40k

Figure 1: Comparison of NP7-based FortiGate 1801F with industry-average security benchmarks.

Security Compute Rating: Benchmark (performance multiplier) that compares FortiGate NGFW performance versus the industry average of competing products across various categories that fall within the same price band.

Comparing the NP7-based FortiGate 1800F series with similarly priced competitors reveals that the FortiGate 1800F series offers double-digit improvements over the industry average for several key security benchmarks. For the core capabilities required for security in hyperscale architectures, the FortiGate 1801F outperforms competitors in all areas.

By providing the industry's best price/performance, the NP7-based FortiGate 1800F series enables organizations to deploy a firewall solution that can scale to meet their business needs while maximizing return on investment (ROI). With full solution integration, the organization needs to purchase, deploy, and maintain fewer standalone appliances, reduce cost, complexity, and benefits from a lower overall total cost of ownership (TCO).

The FortiGate 1800F series also enables security-driven networking. As an integral component of the Fortinet Security Fabric, they are powered by AI-driven FortiGuard and FortiSandbox security services. This provides protection from known attacks, detection of unknown attacks, and the delivery of automated threat protection.

FortiGate 1800F Series

- The FortiGate 1800F series NGFW is an integral part of the Fortinet Security Fabric.
- The FortiGate 1800F series NGFW also offers the industry's best-of-breed security services like secure sockets layer (SSL) inspection and an intrusion prevention system (IPS) that are validated by third-party entities like NSS Labs.[7]

Hyperscale Security Begins with Fortinet

Most NGFWs are incapable of securing 40 Gbps network flows commonly used by advanced research institutions, as well as other organizations, to transfer large datasets. This creates a problem for these institutions as new data privacy laws, like the GDPR and California Consumer Privacy Act (CCPA), mandate the protection of sensitive data at all times.

The NP7-based FortiGate 1800F series is capable of securing these 40 Gbps network flows, placing Fortinet at the forefront of providing security in hyperscale environments. This empowers the largest global enterprise organizations to meet the challenges of unprecedented scale, performance, and application delivery while providing the required level of security.

[1] Rajiv Kohli and Nigel P. Melville, "Digital innovation: A review and synthesis," John Wiley & Sons Ltd., January 29, 2018.

[2] "Hyperscale Data Center Count Passed the 500 Milestone in Q3," Synergy Research Group, October 17, 2019.

[3] Kumba Sennaar, "AI in Pharma and Biomedicine—Analysis of the Top 5 Global Drug Companies," Emerj, November 22, 2019.

[4] "Exploring the impact of artificial intelligence on offshore oil and gas," Offshore Technology, May 15, 2019.

[5] Based on Fortinet internal research.

[6] "Data Centers 'Going Green' To Reduce A Carbon Footprint Larger Than The Airline Industry," Data Economy, January 27, 2017.

[7] "Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests October 2019," Fortinet, October 14, 2019.

FORTINET

www.fortinet.com

February 4, 2020 9:30 AM

581677-0-0-EN

D:\Fortinet\Solution Briefs\red solution briefs\Elephant Flows\sb-FA-powering-advanced-research-with-scalable-robust-security