SOLUTION BRIEF

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

Executive Summary

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.

NP7 powered FortiGate NGFWs:

- Support for 40 Gbps and 100 Gbps Elephant flows
- IPsec encryption at high speeds to encrypt these Elephant flows
- Multiple 40 Gbps and 1000 Gbps interfaces in a compact form factor

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 that can reach 40 Gbps or 100 Gbps throughput. As a result, these organizations often do not implement security at network edges that are involved in the transfer of such large data sets—creating a significant challenge for network security 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 provide resilience against volumetric attacks. They also provide high-performance firewalling, as well as support for high-throughput single data sessions (a.k.a Elephant flows), and allow organizations to analyze data faster using AI/ML techniques and 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 100 Gbps. This support for multiple, parallel 100 Gbps flows can dramatically increase the rate of data transfer, providing more than a Tbps throughput between research centers. 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.

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 industry's most innovative NP7-powered FortiGate NGFWs provide the answer, as they are capable of processing IPsec traffic at very high throughput rate and can encrypt these elephant flows. 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

By providing the industry's best price/performance, the NP7-powered FortiGate NGFWs 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).

Hyperscale Security Begins with Fortinet

Most NGFWs are incapable of supporting more than 10 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 NGFWs are capable of supporting up to 100 Gbps Elephant 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.

NP7 powered FortiGate NGFWs:

- Integral part of Security Fabric providing visibility and protection across the entire attack surface
- Reduce cost and complexity by eliminating the need of point products
- Managed by Fortinet's single pane-of-glass management, the Fabric Management Center

[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.

FORTINET

www.fortinet.com

April 12, 2021 10:42 AM

sb-FA-powering-advanced-research-with-robust-security-in-hyperscale

581677-A-0-EN