SOLUTION BRIEF

Protecting Hyperscale Data Centers from Ransomware and Volumetric DDoS Attacks

Executive Summary

Enterprises are adopting hybrid IT, Industrial Internet of Things (IIoT), and 5G to improve operational agility. These tools help them build composable and scalable architectures that interconnect distributed branches, campuses, on-premises data centers, and multi-clouds into a unified network. And yet, amid this change, the enterprise on-premises data center remains an essential component of most networks. Its role is vital because it protects applications, data, and workloads that can't be moved to the cloud but still need to be consumed by employees, customers, and partners.

At the same time, the data center infrastructure is also becoming more distributed, significantly expanding its attack surface. Point security products deployed in different parts of the network create security gaps that reduce visibility and increase the potential for breaches and attacks. Without a holistic security strategy that can seamlessly span distributed environments, blind spots emerge. The resulting disjointed security is unable to provide a holistic view of the attack surface or effectively stop and contain increasingly sophisticated attacks, such as ransomware and distributed denial-of-service (DDoS).

To complicate things further, most data center security policies are focused on north-south data flows. By applying essential Layer 4 protection at the edge, they aim to create airtight perimeter protection. But most data center traffic flows east-west, across the data center, especially across distributed data center environments. This means perimeter-focused security measures are ineffective if threat actors launch sophisticated ransomware or volumetric DDoS attacks (in fact, these attacks are increasingly being combined) to overwhelm the foundation of your security.

Fortinet Advanced Innovations Protect Today's Hybrid Environments at Scale

Leveraging our 20+ years of innovation, Fortinet provides solutions with consistent enterprise-class protection and optimal user experience across—and between—all network edges. And Fortinet also converges networking and security, including branch and secure access service edge (SASE) technologies, into a single solution, extending protections and visibility that enable interoperability and scalability across complex, hybrid environments.

Because of these innovations, the FortiGate Next-Generation Firewall (NGFW) has received the highest score in Gartner's Enterprise Data Center Use Case[1] four times in a row and maintained a leadership position in its Network Firewall Magic Quadrant[2] for the last several years.

These accolades are partly because Fortinet NGFWs are powered by application-specific integrated circuit (ASIC) chips custom designed for today's high performance, scalability, and connectivity requirements, rather than the general-purpose processors used by other vendors. These patented security processing units (SPUs) are custom-built for network acceleration (NP7) and content inspection offloading (CP9), delivering parallel path processing for unmatched Level 4 to Level 7 performance. They also include hardware-accelerated anti-DDoS capabilities to prevent volumetric attacks—all in a single FortiGate platform managed through an easy-to-use, single-pane-of-glass console.

The NP7 offers the following unique and unparalleled capabilities:

- Ultrafast speeds are delivered by offloading user connections from the CPU using innovative FastPath acceleration. FortiGate NGFWs deliver up to 10 million connections per second, resulting in enhanced network performance.
- The NP7 also offers anomaly-based intrusion prevention, checksum offload, and packet defragmentation. Its multilayered protection starts with anomaly checking at the packet level

to ensure that each packet has not been compromised. Next, a sophisticated set of interface-based anomaly protection, DDoS protection, policy-based intrusion protection, firewall FastPath, and behavior-based methods are employed to prevent DDoS attacks from spreading to the rest of the system.

- Anti-DDoS mitigation is also embedded in the NP7's hardware, ensuring business continuity and service availability in case of a DDoS attack. Its anti-DDoS hardware acceleration policy offloads the processing of IPv4/IPv6, interface, and access control list (ACL) policies from the CPU for efficiency and performance, making the NP7 very effective at detecting and preventing volumetric attacks.
- The NP7 can also secure high-performance data center interconnect (DCI) to build data recovery (DR) sites and replication. The NP7 stores session and Internet Protocol security (IPsec) security association keys, performs all necessary encryption and decryption, and accelerates all sessions. It delivers Suite B IPsec throughput of up to 310 Gbps in a compact form factor.

Security Beyond the Edge

Today's NGFWs must also support dynamic, secure segmentation with automated internal segmentation firewall (ISFW) capabilities. ISFW prevents the lateral spread of threats and establishes strong compliance and application access control combined with a broad defense-in-depth portfolio of fully integrated solutions to root out and terminate malicious activity.

But today's networks are also highly dynamic, adapting to changing bandwidth and application requirements. The scalable segmentation such environments require is only possible because NP7-powered FortiGate platforms also support virtual extensible local area network (VXLAN) termination and re-origination combined with essential Layer 4 firewall rules. These help enterprises build hybrid IT architectures that connect legacy physical database domains to virtualized application and web server domains, helping organizations achieve agility and on-demand scalability.

Full Threat Protection

Complete threat protection is achieved by consolidating all required best-of-breed security functions within a single FortiGate NGFW. NP7-powered FortiGate solutions reach up to 500+ Gbps of throughput, helping organizations realize optimal total cost of ownership (TCO).

FortiGate NGFWs designed for the data center combine the industry-leading performance of the FortiGate product portfolio with the coordinated and actionable threat intelligence of FortiGuard Security Services from FortiGuard Labs to deliver the following benefits:

- Enables seamless user experience because Fortinet NGFWs are powered by the industry's only SPUs. Handles unprecedented customer traffic loads with hyperscalability and ultrafast performance.
- Protects applications and infrastructure hosted at the data center edge with hardware-assisted IPv4 or IPv6 DDoS metering controls to prevent volumetric-based flooding attacks.
- Applies stringent controls to enforce access control lists at both the physical network interface and in-build host protection engine to limit packets per second for various packet types, helping to make the NGFW more robust and resilient.
- Protects any workload, anywhere, anytime by building hyperscale secure networking that weaves security into the networking of hybrid IT architectures.
- Consolidates and eliminates point products by running multiple industry-leading FortiGuard services on a single platform to achieve optimal TCO.
- Extends security across the entire attack surface with actionable, coordinated, and fully automated threat protection.
- Simplifies operations, automates workflows, and saves time with an easy-to-use, single-pane-of-glass management system that can cover the entire distributed Fortinet Security Fabric, including support for over 300 ecosystem partners.

Today's agile networks and hybrid data center environments allow organizations to compete effectively in today's digital marketplace. But to do so, they need security solutions designed to see, scale, and adapt to dynamic changes and defend against advanced threats, such as ransomware and DDoS attacks. Fortinet FortiGate solutions, built on an integrated platform and powered by the industry's only custom security processors, enable organizations to build the networks they need without compromising the security those environments require.

[1] "Analyst Report: 2023 Gartner Critical Capabilities for Network Firewalls," Fortinet, May 2023.

[2] "Fortinet is a Leader in the 2023 Gartner Magic Quadrant for Network Firewalls," Fortinet, March 2023.

June 9, 2023 8:08 AM

1280968-A-0-EN