SOLUTION BRIEF

Selecting your High-Performance VPN Solution

5 Reasons Why the FortiGate Next-Generation Firewall Is The Best Choice

Executive Summary

Digital technologies are fundamentally transforming the economic and business processes and the way businesses operate. They transport massive amounts of customer and corporate data, applications usage data for advanced analytics, and telemetry data to identify attacks across geographical boundaries. Services and applications are consumed from multiple public clouds that complement existing private clouds and require data to travel back and forth from the enterprise networks.

As the speed of business accelerates, the real-time propagation of this massive amount of customer, application, and network data in motion pushes network boundaries further, requiring high-speed transports. Regulatory compliance mandates and customer SLAs require that the data in motion must be protected at matching speeds from eavesdropping and breaches as it traverses network boundaries by using high-performance crypto VPNs.

As security experts consider how to provide comprehensive data-in-motion security for their businesses—including access control, data confidentiality, privacy, and breach prevention—they face a confusing array of point products. A particular product may provide great data-in-motion security but would typically not also have the best threat protection. Alternately, it could provide excellent threat protection but offer mediocre data-in-motion security.

FortiGate Next-Generation Firewalls (NGFWs), running the powerful FortiOS operating system, offer ultralow latency crypto VPNs that are enabled by custom security processors to deliver the best of both data-in-motion security and network-wide threat protection at high speeds. This results in product consolidations, footprint reductions, and lowered capital and operational expenditures.

This guide provides a comprehensive overview of key crypto VPN use cases and features that are offered by FortiGates to protect data in motion. FortiGates come in both physical and virtual form factors to meet the varying needs of enterprises' price and performance points.

Additionally, a competitive comparison of the FortiGate 3960E compact NGFW with other lead offerings is presented to showcase how the industry's highest-performance IPsec crypto VPN product can also deliver the best threat protection performance. Armed with this data, security architects can approach their CISOs with a compelling security solution.

Digitally Transformed Networks Need Consolidated Services at High Performance

Adapting to the new digital economy requires organizations to retool their networks so that computing and network infrastructure evolve to become the prominent sources of frontline business value delivered directly to customers, business partners, employees, and other stakeholders.

Digital transformation introduces new risks that previous generations of security solutions are not able to address effectively because they are unable to simultaneously offer encryption and threat protection at high scale and speed. They also tend to lack seamless integration with more prevailing advanced Border Gateway Protocol (BGP) routing.

To protect digitally transformed and geographically dispersed networks from the rising tide of sophisticated threats, organizations need a modern security architecture that offers consolidated crypto VPN and threat protection, without compromising performance. Sharing threat intelligence across all security devices using encrypted tunnels not only provides data confidentiality but also results in automated, high-performance threat protection. The security architecture should also secure multi-cloud transports and software-defined wide-area networks (SD-WANs).

FortiGate—Redefining Security Rules at the Enterprise Edge

Customer and corporate data must also be protected as it moves across applications, devices, and geographical boundaries. This means that security needs to seamlessly extend to the farthest reaches of the network and must also be found at every point of data interaction to ensure data privacy, confidentiality, and origin authentication.

This is why the lack of comprehensive security that protects data in motion and provides threat protection is recognized as one of the biggest obstacles to digital transformation today, and it is highlighting the limitations of current security implementations to IT leaders. The multiple security solutions they have "bolted onto" their networks over the years are difficult to manage, unable to share threat intelligence, and are not able to meet the rising needs of encrypted traffic to securely transmit data at very high speeds. FortiGate NGFWs are an integral component of the Fortinet Security Fabric, and are unique in that they leverage hardware-based acceleration to deliver predictable performance at high speeds and include diverse and feature-rich crypto VPN solutions.

A comparison of the FortiGate 3960E with other offerings reveals a clear lead for the FortiGate in several key areas of specifications. (See Table 1.)

Following are some of the top areas of differentiation for FortiGate crypto VPN solutions.

Specification	FortiGate 3960E	Industry products (with similar pricing)
IPsec VPN Throughput	280 Gbps	10-26 Gbps
Gateway-to-Gateway VPN Tunnels	40,000	15,000
Client-to-Gateway VPN Tunnels	200,000	15,000
SSL Inspection	30 Gbps	<6.5 Gbps
Threat Inspection	13.5 Gbps	4-20 Gbps

Figure 1: FortiGate 3960E vs. Industry Average Spec Comparison.

1. High-Performance Crypto VPNs

High-performance encryption/decryption is critical to transport large volumes of data to reduce latency and enable enhanced user experience and match the attack speed of adversaries to effectively thwart data-in-motion breaches. Leading NGFWs include both data-in-motion security and threat-protection capabilities. When reviewing vendor data sheets, it's important to compare side-by-side performance of both crypto VPN performance and NGFW threat protection—checking to make sure the test shows results of when all security controls are enabled.

The FortiGate 3960E delivers IPsec crypto VPN throughput at speeds up to 280 Gbps, ensuring minimal degradation of network performance even with multiple services running. That's 17 times the performance of Palo Alto Networks and 11 times the performance of Checkpoint Software; 28 times faster than Cisco. At this time, Palo Alto Networks and Checkpoint Software don't publish their IPsec Gateway-to-Gateway tunnels scale. The FortiGate 3960E offers 13 times more Client-to-Gateway IPsec crypto VPN tunnels than Cisco.

2. Diverse VPN Solution

FortiGates offer next-generation Suite B-enabled crypto VPN solutions to match the varying array of network designs, ranging from scalable SSL-based remote access solutions to high-performance, multi-cloud, site-to-site networks that are deployed as policy-based or route-based IPsec VPNs. A route-based VPN creates a virtual IPsec network interface that applies encryption or decryption as needed to any traffic that interface carries. Routebased VPNs are also known as interface-based VPNs. A policybased VPN is implemented through a special IPsec VPN firewall policy that applies encryption to traffic accepted by the policy. Integration with the Security Fabric allows secure communication of FortiTelemetry data over encrypted IPsec Site-to-Site VPN tunnels between FortiGates. FortiOS-based crypto VPNs are also compatible with FortiOS traffic optimization, traffic shaping, high availability, BYOD (device identification), and endpoint control.

3. Multi-Cloud Security

Organizations are opening up their branch networks to ride on business-class. Internet and leverage one cloud provider for specific functionality, another for application or for cost. To effectively utilize the cloud, critical data is being exchanged and processed across a variety of cloud-based applications. To preserve data privacy, ensure confidentiality, prevent breaches, and achieve compliance, organizations need to deploy scalable and high-performance crypto VPN solutions that extend from the private cloud and terminate at the doorstep of multiple cloud providers.

4. Secure SD-WAN

SD-WAN allows enterprise branches to access corporate resources from private or public clouds over inexpensive Internet transports as an alternative to expensive MPLS circuits. While this can enable significant cost savings, it can open the door to new threats and may lack access control.

To maintain compliance and achieve robust security, enterprises need to employ crypto VPNs over public Internet transports to achieve data confidentiality, privacy, breach prevention, and threat protection by matching the scale and performance needs of every branch. FortiGates are the only NGFWs that offer secure SD-WAN solutions to build massively scaled IPsec crypto VPN-based networks connecting geographically dispersed branches to enterprise resources that are located on-premises and in the cloud.

5. Crypto VPNs Configured at VDom Level For Better Security

As enterprises adopt rich customer experiences and allow Internet access at every branch, they need to separate the guest Wi-Fi traffic from the corporate traffic. In addition, the enterprise branches that offer ATM and credit card processing services not only encrypt financial traffic using crypto VPN but also separate it from their regular corporate traffic to achieve PCI compliance. To separate traffic, enterprises opt for VLANs that are not able to establish a distinct security policy per VLAN. FortiOS virtual domain (VDOM) offers much better implementation of security policy that allows granular control and configuration of crypto VPN and threat protection features on a per-VDOM level to achieve compliance, threat isolation, and better security.

The Industry-Leading FortiGate High-Performance IPSec Crypto VPN Is The Right Choice for Today's Enterprises

FortiGates provide a full range of high-speed crypto VPN solutions to protect data in motion and seamless integration with scalable routing. They offer data in motion and granular access control at high speeds across devices, applications, and geographical boundaries.

These powerful NGFWs combine broad visibility, threat intelligence sharing, and high-performance threat protection all in a single system to meet the rising needs of high-performance networks.

FORTINET®

www.fortinet.com

September 7, 2019 2:39 AM

485411-0-0-EN

D:\Fortinet\Solution Briefs\red solution briefs\Refresh\sb-selecting-your-high-performance-vpn-solution