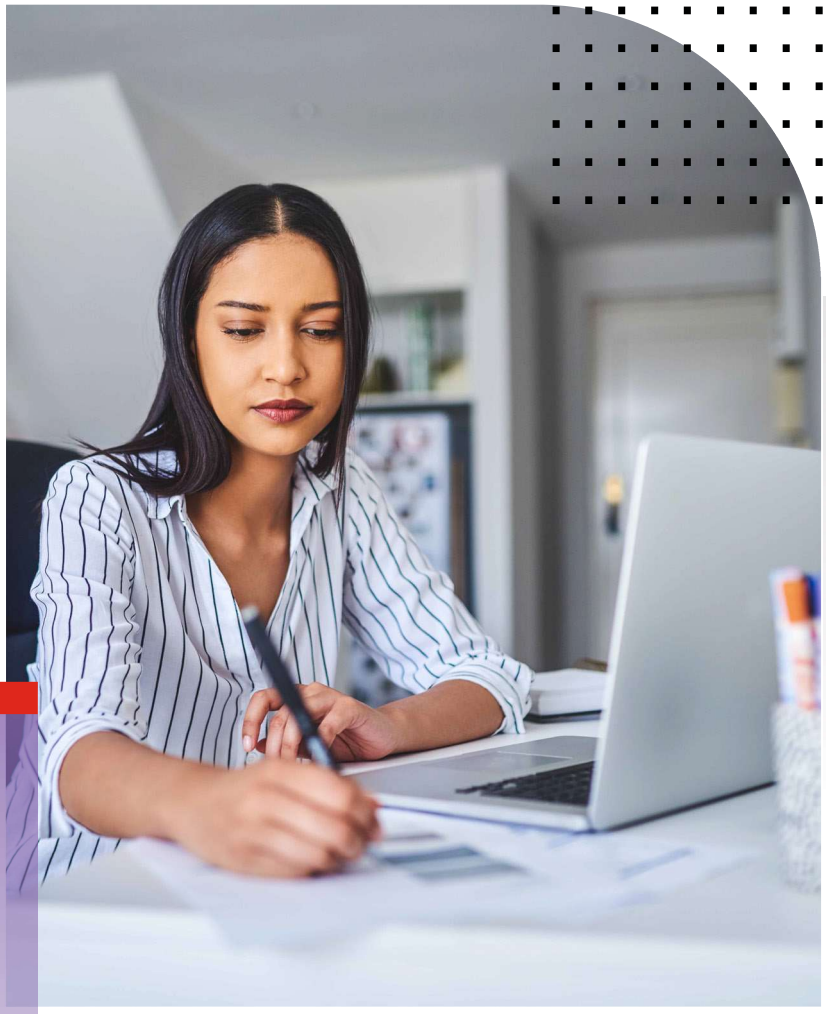
WHITE PAPER

7 Critical Considerations for Firewall Performance in the Era of Secure Remote Work



Executive Summary

7 Critical Considerations for Firewall Performance in the Era of Secure Remote Work

The COVID-19 pandemic has forced organizations to press remote worker programs into action, often with hard lessons learned along the way. All organizations in today's world must be able to adapt to changing business conditions with little advance notice, and ensure secure remote work is part of a robust business continuity plan.

This is not so easy. Organizations wrestling with a remote workforce are learning the limits of outdated integrated firewall and virtual private network (VPN) solutions when it comes to performance and scalability. Many have already seen firsthand that traditional firewalls simply cannot scale across multiple applications required for secure telework—putting further burden on IT teams to upgrade firewalls or install completely separate appliances to keep pace.

Next-generation firewalls (NGFWs) must be able to provide performance and advanced capabilities at an agreeable cost—and with the ability to scale to meet future demands of distributed teams. The pandemic will not be the last time teams are asked to be at their best in a remote-first environment.

When Price Isn't Meeting Performance

Teams have been talking about NGFW performance for a generation, so why is it still an issue? The truth is that most security solutions are unable to provide speed and scale at a price most companies can afford, largely because many of the security vendors behind those solutions have themselves not invested in cost-effective technologies for building them. As a result, most organizations are left with little choice but to purchase traditional firewalls with limited performance and minimal headroom for scalability.

Say a typical business bought firewalls planning for about 5, maybe 10 percent of their remote workers. When the number of remote workers ballooned to more than 90 percent during the pandemic, many more resources are then consumed for remote VPN client connections, greatly affecting capacity on the firewall. So, consider that under "normal" circumstances, underperforming firewalls are less than ideal, hampering network throughput, among other drawbacks. During a critical event, however—or during the kind of seismic shifts companies experience as they embrace digital innovation—many firewalls become bottlenecks and productivity drops.

Imagine a financial services firm that can't keep pace with its competitors because its transaction latency has tripled. Or the already stressed IT team at a large ecommerce organization flooded with complaints because trying to securely support tens of millions of user connections per second has slowed those connections to a crawl. Or organizations focused on genome research or restricted-access government needs, suddenly wondering if they'll never be able to securely transfer huge datasets (so-called "elephant flows") again?

These can feel like unique challenges tied to only a few industries or verticals. But what isn't unique—whether during a pandemic or another similarly massive change in working conditions whose next phase isn't certain—is that organizations of all sizes are challenged by increasing time to service as a result of underperforming firewalls. A poor NGFW investment can slow productivity, harm business continuity, and threaten security.

What to Look for When Evaluating NGFW Performance

NGFWs play an important role in threat protection and preserving business continuity. Security teams use NGFWs to monitor the IT environment, everywhere from the network edge to the data center, and gain visibility into users, endpoint devices, applications, and security threats across networks.

The following seven considerations should guide the evaluation of NGFW performance.

1. **IPsec VPN performance**

   Teleworking employees have access to sensitive company data. Protecting this against compromises requires the ability to ensure that a remote employee connection to the company network is secure. This is provided through an encrypted session to not only ensure the confidentiality and integrity of sensitive company data in transit but also ensure that all traffic between the employee and the public internet is monitoted and protected by the organization's existing cybersecurity infrastructure. Bringing a very large remote workforce online to maintain productivity levels and maintain

business continuity requires the support for a very large number of secure connections called IPsec or secure sockets layer (SSL) VPN tunnels. Equally important is the aggregated performance of the system. The NGFW should be able to sustain the user connections and the encrypted traffic load irrespective of the location of the users.

2. Threat protection performance

How well does your NGFW perform when running full threat protection? Ideally, an NGFW can sustain performance with full threat protection—meaning firewalling, intrusion prevention, antivirus, and application control—turned on. In three or so decades of firewall technology, at least one thing has remained constant: vendors that speak ambiguously about threat protection performance. Insist on real numbers and a close reading of documented performance claims.

3. SSL inspection capacity

A majority of enterprise network traffic is now encrypted, and bad actors are continuing to take advantage by inserting malware into encrypted packets. SSL decryption and inspection can offset these security risks by intercepting malware, but SSL inspection comes at a downside: reduced throughput. And too much reduction puts the traditionally tense relationship between security and business productivity once again in conflict. All NGFWs receive some impact in throughput with SSL turned on, but the best have predictable performance with minimal degradation in speed.

4. Price vs. performance

Many NGFW vendors increase the size of their firewalls to boost performance, and increase the price to match that size. The best NGFW solutions, however, combine price and performance with an eye toward a smaller technology footprint. Years ago, teams were often forced to choose price or performance when it came to total cost of ownership (TCO). But big leaps in disruptive firewall technology, underpinned by world-class network processors that can achieve unprecedented levels of performance, have made the TCO conversation a happy one.

5. Credible third-party validation

No organization making an investment as important as an NGFW should rely on vendor documentation or word of mouth alone. Recognized third-party evaluators such as Gartner and NSS Labs provide detailed validation of NGFW solutions, and their consultation is highly recommended.

6. Easy, single-pane-of-glass management

It's a frequent productivity killer: security teams that have to toggle between multiple dashboards to assess vulnerabilities, respond to threats, and ensure system resiliency. But gone now is the era when teams couldn't include their NGFW in management consoles for other parts of the infrastructure. Teams should insist on single-pane-of-glass management combining NGFW as part of a broad, integrated security architecture that enables sharing of threat information across network devices and receiving of threat intelligence automatically.

7. Future-proofing

As IT continues to evolve from cost center to business enabler, all organizations are embracing digital innovation in some form. Digital innovation initiatives drag, however, when organizations add complexity and introduce performance challenges because they haven't integrated their solutions, right-sized their investment, or planned for future state activities. This includes NGFW integration. Ensuring an NGFW that not only provides performance at agreeable cost and scale but can also anticipate future demands will ensure organizations maximize their investments in network security for superior return on investment—today and tomorrow.

FORTINET®

www.fortinet.com

May 11, 2021 6:41 AM

D:\Fortinet\2021 Rebranded templates\White paper\May\Refresh\7 Critical Considerations for Firewall Performance\wp-7-critical-considerations-5112021\wp-7-critical-considerations-5112021

665637-A-0-EN