SOLUTION BRIEF

Don’t Diverge—Converge

Using FortiGate NGFW to Protect Your Business

Introduction

Digital acceleration is driving the adoption of hybrid IT architectures. These new hybrid environments blend data centers, campuses, branches, home offices, and multi-cloud environments into a dynamic, interconnected networking environment. When implemented correctly, a hybrid network provides critical services that traditional IT cannot offer, such as operational agility, hyperscale, and location independence. These, in turn, allow organizations to compete more effectively in today’s digital economy through improved productivity, more efficient supply-chain systems, increased customer and partner engagements, and optimized user experience.

However, effectively implementing digital acceleration requires rethinking security. While hybrid networks enable organizations to implement critical new business applications, processes, and services, they also significantly increase the attack vectors and surface. And hybrid networks not only have more locations, devices, applications, and services to protect. They are also in a state of constant flux. So, in addition to offering security everywhere, those protections also need to dynamically adapt to constantly shifting business requirements.

Where do you start?

Everything starts with visibility. In security parlance, what is not seen is unknown—and could be malicious. As a result, visibility must span every new potential attack vector, including applications, local and remote networks, new devices, mobile users, and workflows that span environments. But this is easier said than done. How do you achieve broad visibility, especially into encrypted network flows providing critical communications, without impacting network performance or user experience?

Encrypted Traffic Is the New Epicenter of Harm—Your Blind Spot Is the Bad Actors’ Sweet Spot

95% of web traffic is now encrypted[1], which means we have already transitioned to what is often referred to as “always-on SSL.” Secure Sockets Layer (SSL)—or more specifically Transport Layer Security (TLS), the successor to SSL—is now a requisite for anyone wishing to transmit email and data over the internet safely and securely. But there is a twist. These encrypted channels are also a perfect conduit for hiding criminal activity, such as delivering malware or exfiltrating stolen data.

The challenge is that few next-generation firewall (NGFW) solutions—the tool most commonly tasked with inspecting traffic—are able to inspect encrypted traffic in real time. Because they do not include Fortinet’s unique security processors (SPUs)—custom ASICs designed specifically to offload performance-heavy security processing—most solutions slow dramatically, impacting network performance and user experience. And only Fortinet can inspect encrypted streaming video in real time, which has become today’s primary collaboration tool.

The Perils of Implicit Trust

Another critical challenge of most legacy networks is that they operate from a position of implicit trust. Users and devices inside the perimeter are assumed to be reliable and secure, and, therefore, free to access data and resources. Unfortunately, such unfettered access to the critical resources distributed across today’s hybrid networks is a security risk. Malicious actors that breach the network—through unprotected home offices or compromised public access points—are free to look for data to steal and resources to corrupt or hold for ransom. And when trusted users fall victim to phishing attacks or mistakenly execute malicious software code, it can create a perfect storm for hackers to hop from network to network and application to application without being detected.

This issue is compounded when uninspected encrypted traffic is combined with this implicit trust model. This deadly combination allows bad actors to infiltrate networks via encrypted streams, move freely across the network looking for data to steal or resources to corrupt, and then leave undetected.

How Should Organizations Address These Two Challenges? It Starts with Deep SSL Inspection

With the average cost of a cybersecurity breach now pinned at $4.2 million[2], enterprises must focus on the emerging security issues targeting their hybrid IT networks. SSL encryption is at a critical crossroads, providing essential protections for organizations and criminals. Enterprises must address the cybersecurity challenges of SSL encryption by implementing real-time SSL decryption and traffic inspection systems. This is the only way to differentiate between legitimate traffic and that being used by bad actors to hide their malicious attacks and communications.

However, less than half of deployed NGFW solutions have their SSL decryption and inspection functions enabled. And one of the primary reasons is the performance impact these services have on their network. Studies show performance can be impacted by nearly 80 percent when inspecting SSL or TLS traffic. Side-by-side comparisons show that even those vendors touting firewall performance take an enormous hit when inspecting traffic. That's why turning on SSL decryption turns off most companies.

FortiGate NGFWs simplify security complexity and provide full high-fidelity visibility into applications, users, and networks. This unique capability starts with the industry's only purpose-built security processing units (SPUs). They provide the industry's fastest rate of deep inspection, even for traffic other vendors won't even touch, like streaming video. And this technology is further enhanced with AI/ML-powered threat intelligence services from FortiGuard Labs to deliver the industry's top-rated coordinated security and highest-performance threat protection—including intrusion prevention, web filtering, anti-malware, and application control—to combat both known and zero-day attacks.

Recent tests were performed in partnership with Keysight labs. The Keysight BreakingPoint tool was used to measure performance degradation for the FortiGate 7121F during deep inspection of SSL and TLS 1.3 traffic. But threat protection must also include a combination of application control, IPS, and anti-malware features running concurrently—something that virtually no vendors do when publishing their encryption inspection performance numbers. The tests were performed with all logs enabled and used industry-standard 64 KB HTTPS objects to replicate a real-world environment.

And to ensure that the FortiGate 7121F underwent the most rigorous performance tests, these tests were also performed without session resumptions—unlike many tests conducted by competitors. As is customary with SSL inspection, the most compute-heavy portion of any connection is the start of a session, when keys are negotiated. Session resumption is a trick used in testing to allow a firewall to leverage already-negotiated keys, thereby reducing their impact on performance.

The results were staggering. The FortiGate 7121F achieved 300 Gbps of Threat Protection throughput—the highest in the industry using a single NGFW system. It also demonstrated industry-leading results of setting up 625,000 sessions per second.

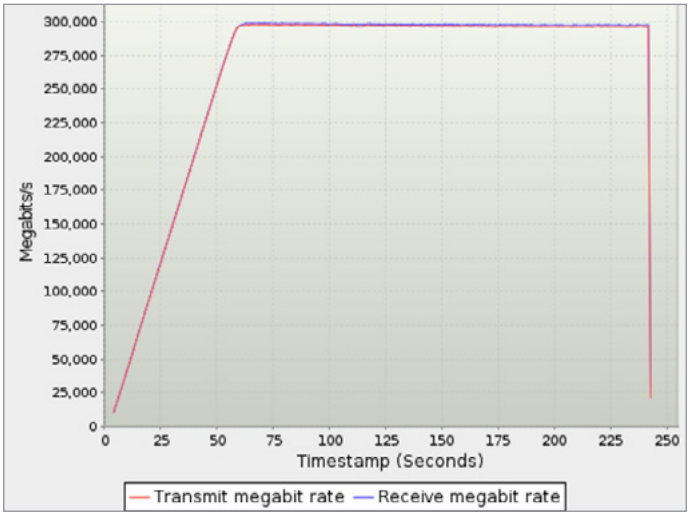


Figure 1: 7.19.2 Application data throughput.

The above image is from our BreakingPoint test report showing stable 300 Gbps Threat Protection throughput. In the following image, below, note the clear separation of management and data plane functions, with FortiGate 7121F GUI responding quickly even when the data plane is under high CPU load with logging enabled for full visibility of encrypted traffic:

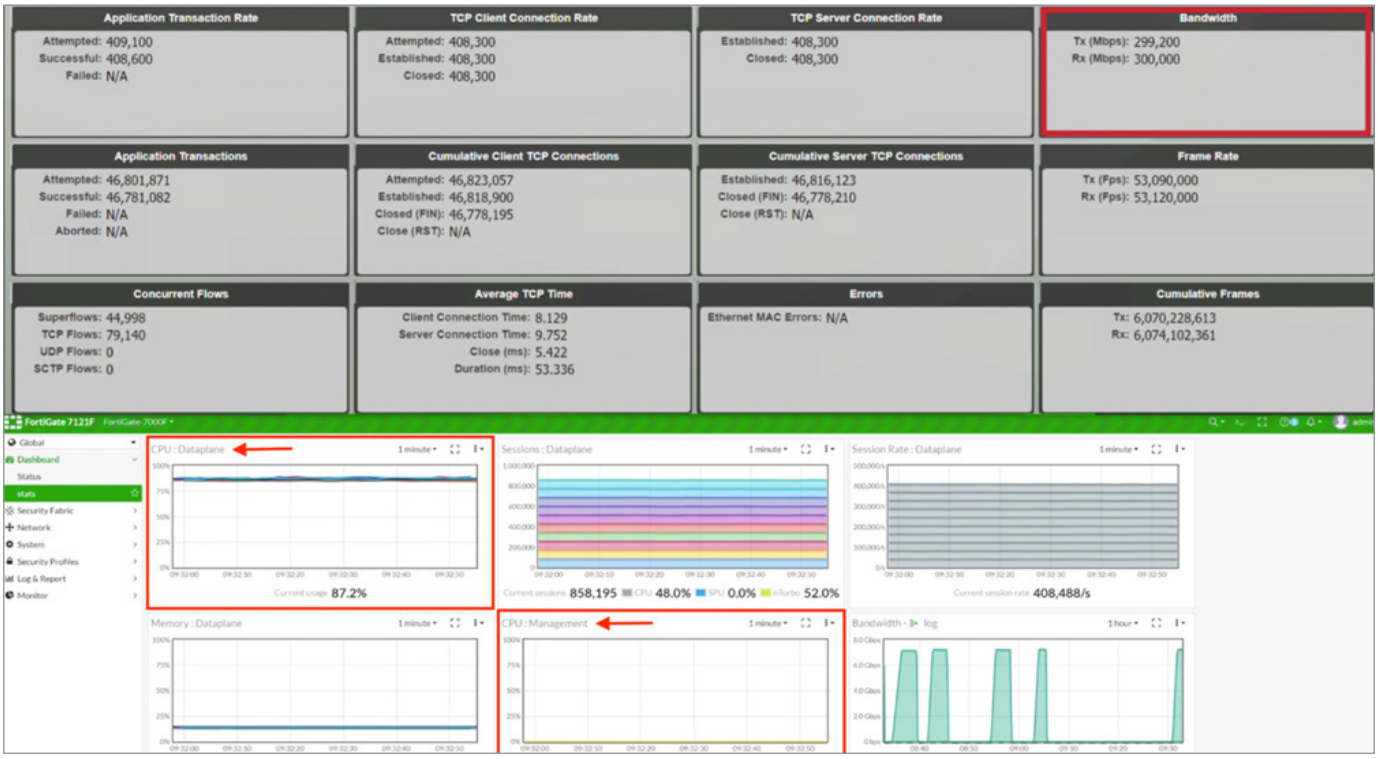


Figure 2: FortiGate 7121F chart table.

This next image shows the FortiGate 7121F maintaining a stable 625,000 connections per second (CPS) with no application transaction failures.

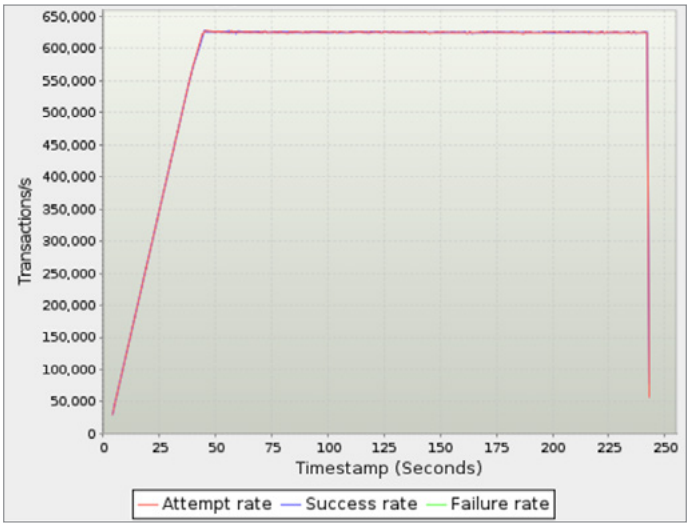


Figure 3: 7.19.9 Application transaction rates.

Note that the same management and data plane separation was conducted here in the Connection per Second test:

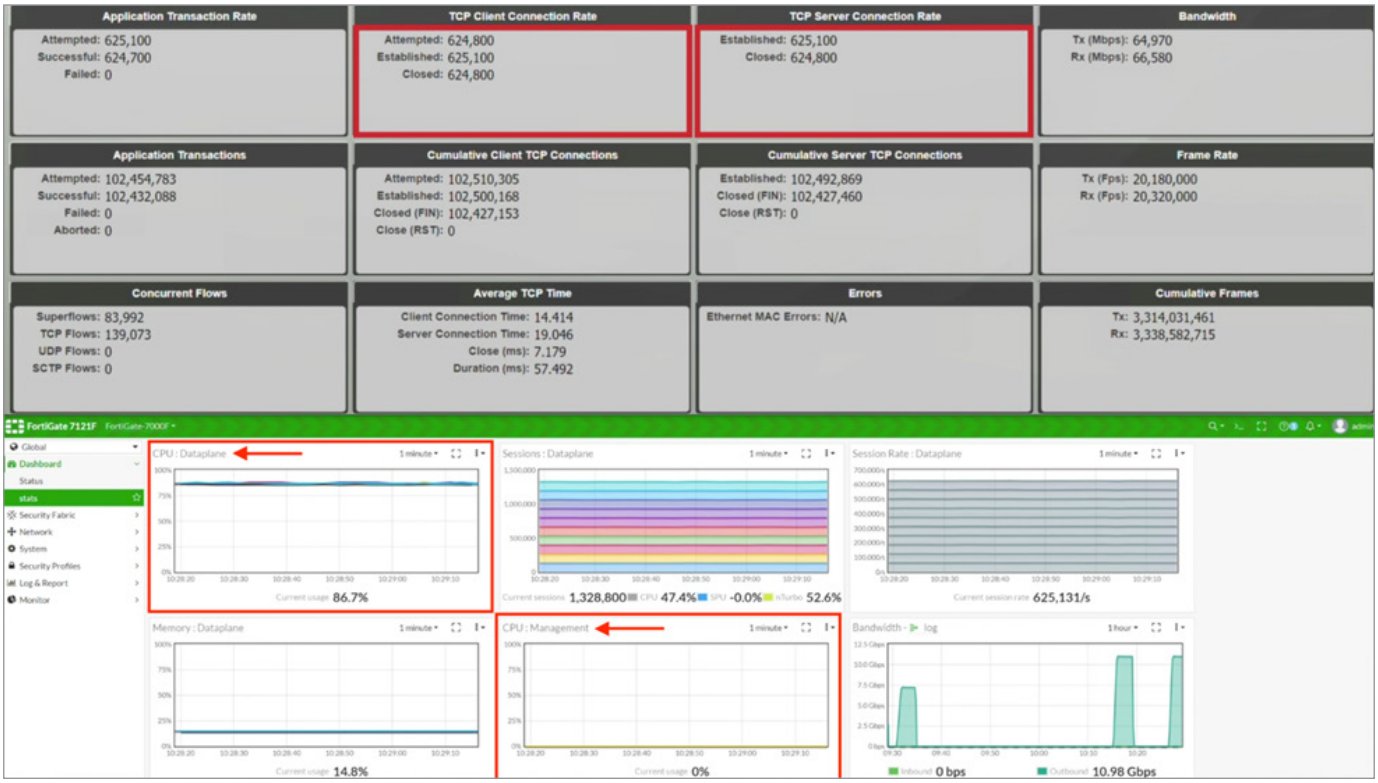


Figure 4: FortiGate 7121F and BreakingPoint performance testing for SSL deep inspection.

The detailed test video can be found here.

World-class Web, Video, and DNS Security Performance

The FortiGate platform leverages AI/ML-powered FortiGuard services to protect data and applications against web-based attacks. FortiGuard's massive web content rating and URL databases, and AI-enabled analysis environments, power our accurate web and video filtering services. They enable us to provide granular services across web and video categories to quickly and accurately log, allow, or block traffic. This function also extends to DNS security to protect against malicious domain block attack tactics, like DNS tunneling, C2 server identification, and Domain Generation Algorithms. FortiGate's web security function also blocks unauthorized attempts to communicate with compromised remote (C2) servers to receive malicious commands or send extracted data.

In tests of the new FortiGate 7121F's web security functions, the Keysight BreakingPoint APS-M1010 controller was used to simulate users accessing websites leveraging a 64k object payload. The test ran for 10 minutes with no drop. It resulted in 1.14 Tbps of throughput performance, even with application control running concurrently with the AI/ML-powered FortiGuard Web Filtering service. It also demonstrated 2M connections per second, with all traffic logged at the rate of 23 Gbps to maintain visibility and active intelligence.

This image from the BreakingPoint test report shows 2M TCP connections per second with no transaction failures:

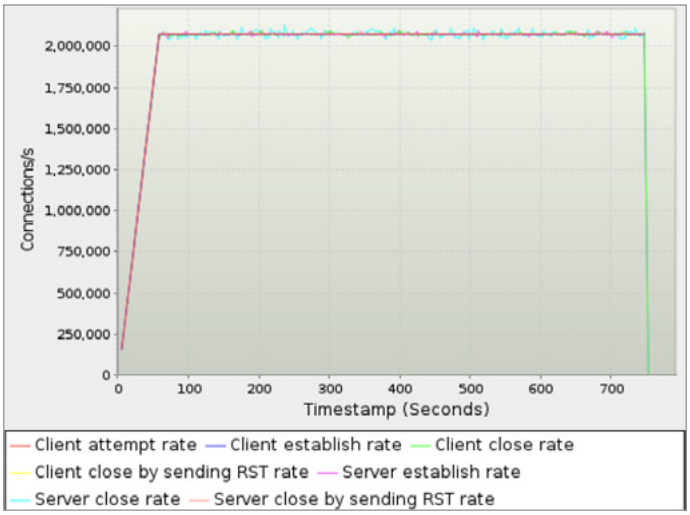


Figure 5: 7.19.14 TCP connection rate.

Remarkably, 1.14 Tbps of HTTP throughput at the same time was possible even with URL filtering and application control enabled:

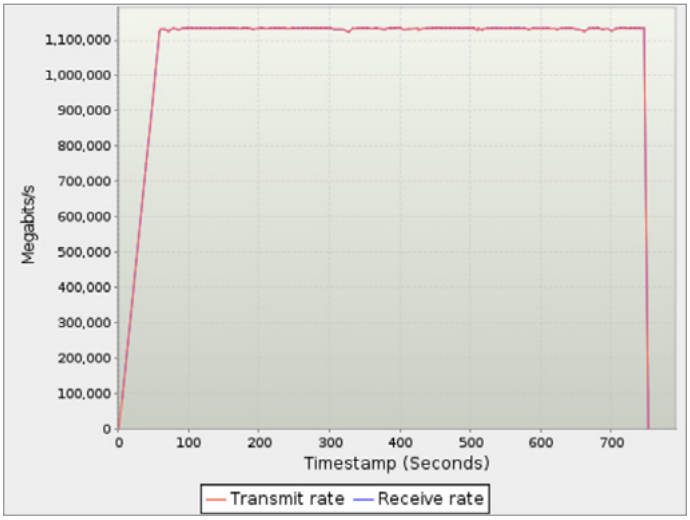
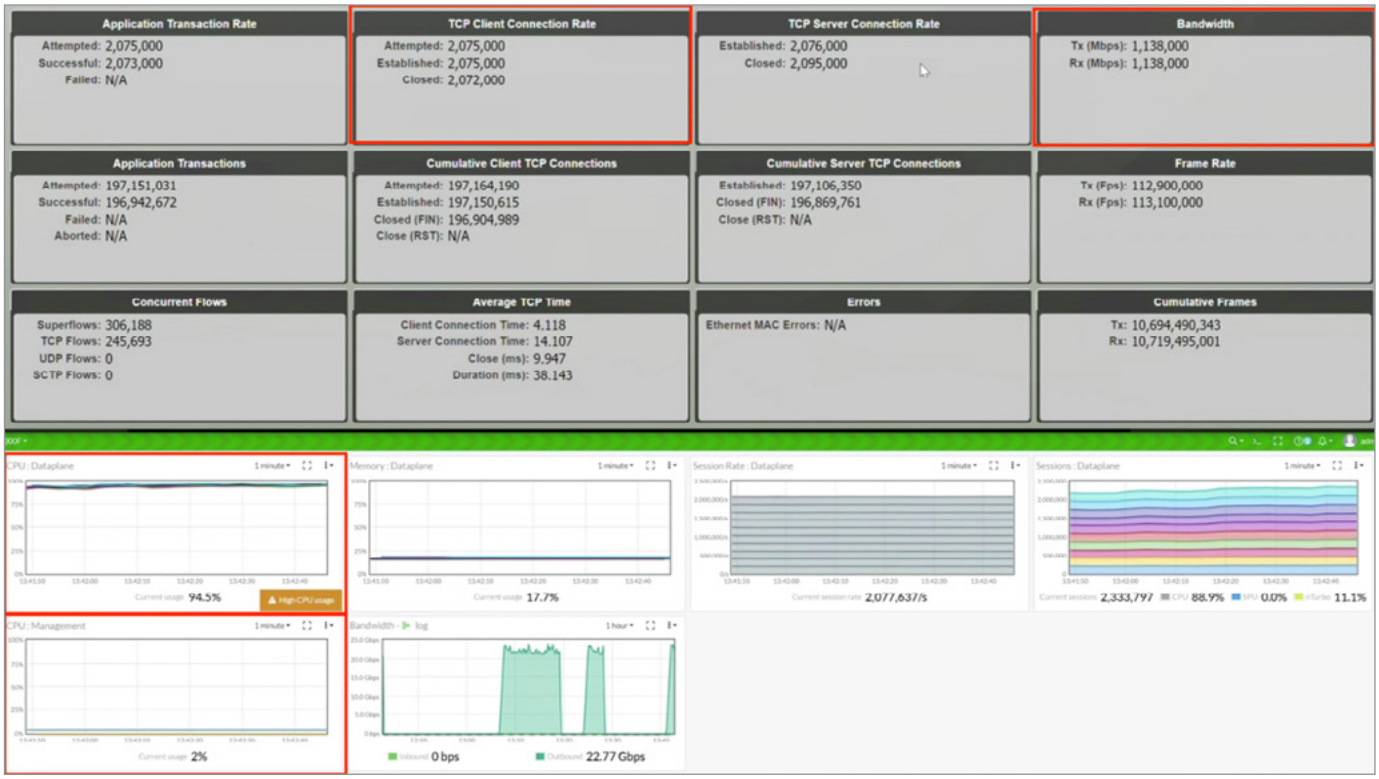


Figure 6: 7.19.4 Super flow data throughput.

The overall performance for URL Filtering with application control shows two powerful Key Performance Indicators (KPIs) for both CPS and Throughput:



The Industry's Highest Threat Performance

A second test was run to highlight FortiGate 7121F performance with Threat Protection enabled (Application Control, IPS, and Anti-Malware) while simultaneously testing security efficacy when the device is under heavy load. This is a crucial test case that many customers should use when comparing different vendors' performance and security efficacy. The test was run with an HTTP 64K payload for easy comparison.

The FortiGate 7121F delivered 639 Gbps of throughput, the industry's highest threat protection performance, even with traffic logging enabled for full traffic visibility and actionable intelligence. The following image is from the BreakingPoint test:

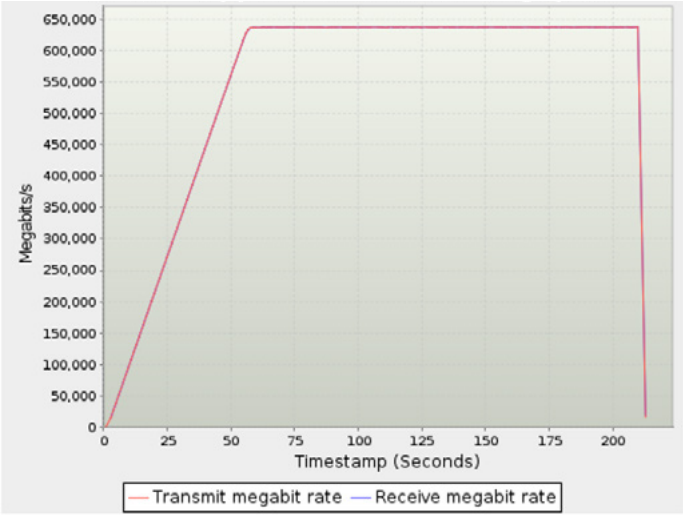
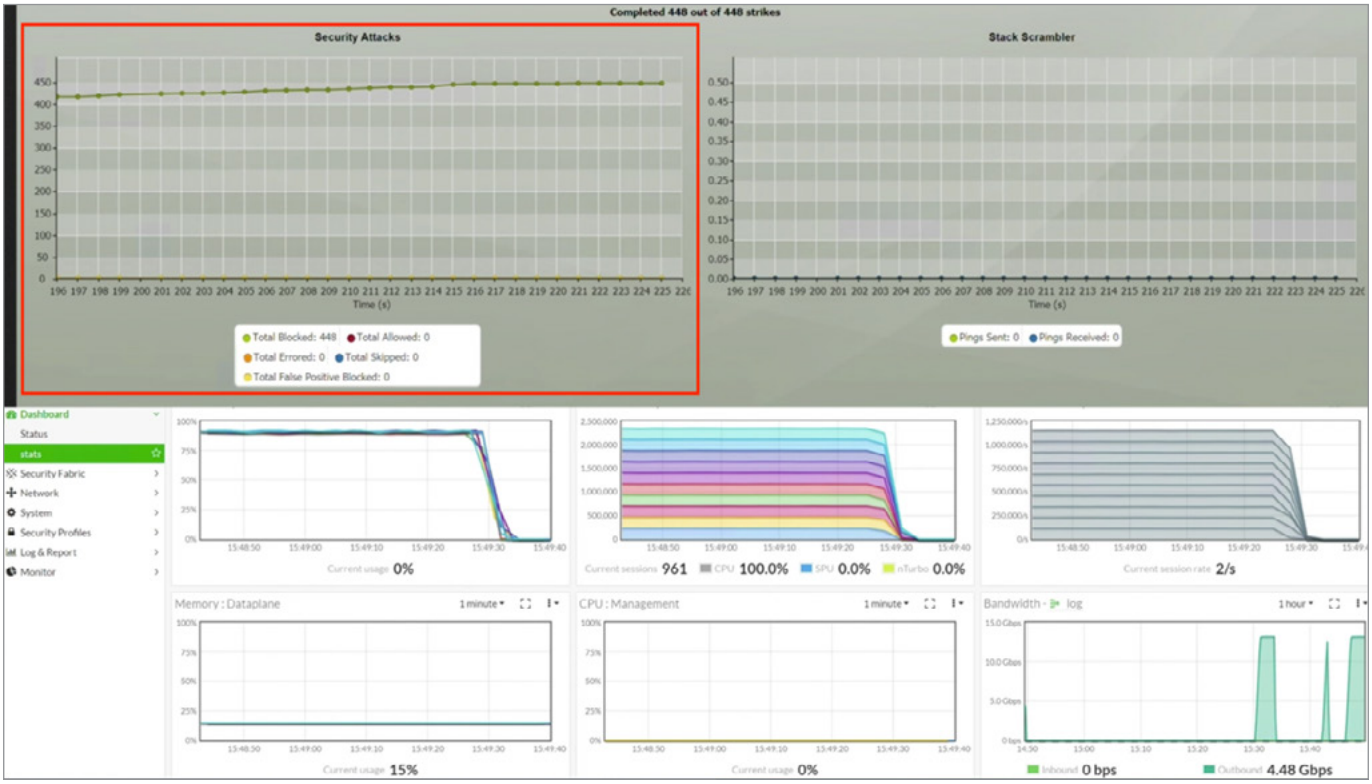


Figure 7: 7.19.2 Application data throughout.

As you can see, all security attacks were successfully blocked:



FortiGate 7121F Breaking Point Test Summary	Traffic Type	Performance Highlights
Threat Protect with SSL Deep Inspection	HTTPS 64 KB	300 Gbps throughputs
Threat Protect with SSL Deep Inspection	HTTPS 1B	625,000 connections per second
Threat Protect with Security Attacks Blocked	HTTP 64 KB	639 Gbps throughput
Application Control with URL Filtering	HTTP 64 KB	1.14 Tbps throughput and 2M connections per second

Building a Zero Trust Strategy with FortiGate's Built-in ZTNA

Performance inside the network is critical. But for organizations dealing with a hybrid workforce that divides their time between home, the office, and travel, delivering consistent security to any user or device in any location is vital. The new hybrid workforce has also exposed the shortcomings of traditional virtual private networks that never paid attention to implicit trust beyond user authenticating for the VPN connection. Over the past two years, criminals have successfully exploited this weakness to hijack VPN connections to access corporate networks and resources.

Fortinet's Zero Trust Network Access (ZTNA) solution changes all that while simplifying secure connectivity and reducing the attack surface. Built natively into the FortiOS that powers the FortiGate security platform on-premises as well as Fortinet's cloud-delivered service, Fortinet can extend the power and protection of ZTNA to remote users and their home offices. It can also easily be extended to retail stores and remote offices using FortiGate's natively integrated SD-WAN capabilities for better application steering, secure application access and use, and optimal user experience.

To start, we strongly recommend having the performance of your existing solutions tested today using the correct benchmarking tool and KPIs that matter to your business. Once that is done, we can provide you with the industry's most comprehensive performance metrics compared across vendors.

Placing a FortiGate NGFW solution at the core of your organization's network security allows you to build a zero-trust strategy for consistent convergence of networking and security across all edges and the consolidation of security functions—including secure access—to simplify operations. And at the same time, deliver the industry's highest throughput so you can maintain peak performance to meet your data and user experience requirements without compromising on protection.

[1] "HTTPS encryption on the web," Google Transparency Report, February 19, 2022.

[2] Abi Tyas Tunggal, "What is an Attack Vector? 16 Common Attack Vectors in 2022," UpGuard, January 14, 2022.

FORTINET®

www.fortinet.com

March 24, 2022 4:09 AM
1538813-0-0-EN