Decoding Network Security

Don't Be Fooled by Cryptic Information from Vendors Touting Cheap Firewalls

Making network security purchases solely based on datasheet "speeds and feeds" is a common mistake. Datasheets can include misconceptions and disingenuous advertising, which don't mesh with real-world requirements and low risk tolerance. Transparency in performance testing and truth in advertising arm you with the most accurate data to ensure you can make the right decisions. This document will aid in guiding you through the firewall purchase, focusing on whether the listed performance holds up in the real world with crucial security features enabled. Gaps in security result in unwarranted risks, higher total cost of ownership (TCO), and impaired business agility.

Dig Deeper into Performance

Understanding stated datasheet performance numbers and how they are derived is crucial for informed buying. Ask the vendor to explain their testing methodology and how they derived the advertised performance. Consider the firewall's operational mode (sometimes referred to as Flow Mode, Proxy Mode, Stream Mode, etc.), the traffic mix composition (not just the name of the mix), packet type and size, CPU utilization realized, and other figures as proven by that methodology.

> **Through 2020, 99% of firewall breaches will be caused by simple firewall misconfigurations, not flaws.**[1]
>
> **-Gartner**

When evaluating a datasheet, dig deeper into feature performance:

- **Application control:** Consider whether the application control, also called App-ID, is native to the platform or bolted on. It should also be able to withstand application port-hopping. Identify if the product has to run in a special mode to build application-based rules or to build multiple applications into a single rule for firewall rule consolidation. If so, ensure this functionality doesn't come at the cost of other critical security features.
- **SSL inspection:** Nearly 80% of north-south traffic is SSL-encrypted, and encryption is a well-used evasion technique among threat actors. Despite it being a recommended best practice—only a fraction of organizations implement SSL decryption to inspect this traffic. You should understand what ciphers and key sizes a vendor uses in SSL inspection tests. Some may test with keys as small as 256 bits to game the system, whereas 2048-bit keys are common in the real world. Furthermore, some vendors may publish an SSL inspection performance value higher than their Threat Protection value—does that make sense? Most importantly: If SSL inspection is tested only using App-ID, or only IPS, is that relevant to how you plan to deploy it?
- **IDS/IPS:** Determine how IPS and IDS capabilities were configured during testing. IPS should be configured to inspect all critical-, high-, medium-, and low-severity vulnerabilities. If the vendor includes rate-based signatures, these should be enabled as well. You should also check for any "intelligent mode" or "adaptive scanning" features enabled during tests, as these often improve performance at the cost of security.
- **File blocking:** Compliance best practices, such as PCI DSS, recommend file blocking, often called data loss prevention (DLP), to secure customer data, sensitive corporate information, and financial records. It should be enabled during performance testing just as it would be in your production environment.
- **Antivirus (AV):** A critical component of threat prevention is the ability to inspect traffic for malicious files. Network security vendors may provide multiple AV inspection modes, including performance-tuning options. Understand whether or not these features were enabled during testing, as tuning for performance often compromises security efficacy.
- **Logging:** In a production environment, logging would be enabled for visibility of threats, incident response and forensics, detection of emerging patterns of activity, deployment of machine learning tools, and more. Find out if logging was enabled during testing. IMPORTANT: Does your solution include on-box logging with retention, or do you need to upgrade to a model that includes storage at an additional cost?

> **"We have such a broad range of security needs, yet the Palo Alto Networks platform allows me to manage them with simplicity and efficiency. With the types of advanced threats we face today, I'm not sure we could provide the necessary protections without it."**
>
> **-Ada County**

Other critical factors that will impact performance measurements are:

- **Traffic mix:** Traffic mixes matter. Every organization has a unique set of network traffic mix variables. Check if the vendor changed testing methodology to an undisclosed "enterprise traffic mix" that may have drastically improved IDS/IPS performance. Understanding the traffic mix of your environment contextually frames performance testing compared to a generic lab mix.
- **Generally available OS:** Find out if the vendor used a software build that does not have general availability (GA) during testing. If so, the results of that test are only relevant if you also plan to deploy non-GA software in your mission-critical production deployment.
- **Operational mode:** Some vendors' products have as many as eight different inspection modes, each with unique features, and always with a compromise of security efficacy for performance. Make sure performance numbers are measured in the most secure mode, as that's the one you'll use in your production environment.

What Are They Not Telling You?

Some security vendors may tout third-party certifications to legitimize their security solution. These test reports provide insight that can influence a purchase decision, much like Consumer Reports may when shopping for the next family vehicle, or the ultimate big screen TV.

The latest NSS Labs Next Generation Firewall (NGFW) Group Test report showed that a firewall vendor based in Sunnyvale, California, missed 31 evasions. Of all named vendors, this one scored the lowest in Security Effectiveness. However, the vendor also came in among the lowest TCO in the test. Our key takeaway here is that this vendor places more importance on price than on security. What's your priority: low costs or effective protection?

1. "Technology Insight for Network Security Policy Management," Gartner, February 21, 2019, https://www.gartner.com/en/documents/3902564/technology-insight-for-network-security-policy-managemen.

Palo Alto Networks came in with the highest Security Effectiveness score of 97.9% by blocking 1,783 of the 1,784 exploits and all 406 evasions.

Reading the reports in their entirety, including the typically included customer feedback (sometimes called "Strengths and Cautions") will provide far more insight into the overall product value than a chart full of dots.

How Are the Test Results Meaningful to Your Organization and Unique Business Needs?

No independent organization, such as NSS Labs or Gartner, can present the true TCO of an organization's security architecture. All they can do is analyze and present the TCO of a product in a lab environment.

Although HTTP 64K is typically considered an industry standard component of the traffic test, the actual traffic mix itself is not. Threat Protection is one key metric of your traffic mix, but based on the traffic mix, the results will vary widely. For example, that same Sunnyvale, California-based firewall vendor uses its "Enterprise Mix" to derive datasheet numbers. This traffic mix is considerably different from the very conservative traffic mix that Palo Alto Networks uses to derive our datasheet numbers. NSS Labs also uses a different traffic mix for testing.

Ultimately, the only important traffic mix is yours.

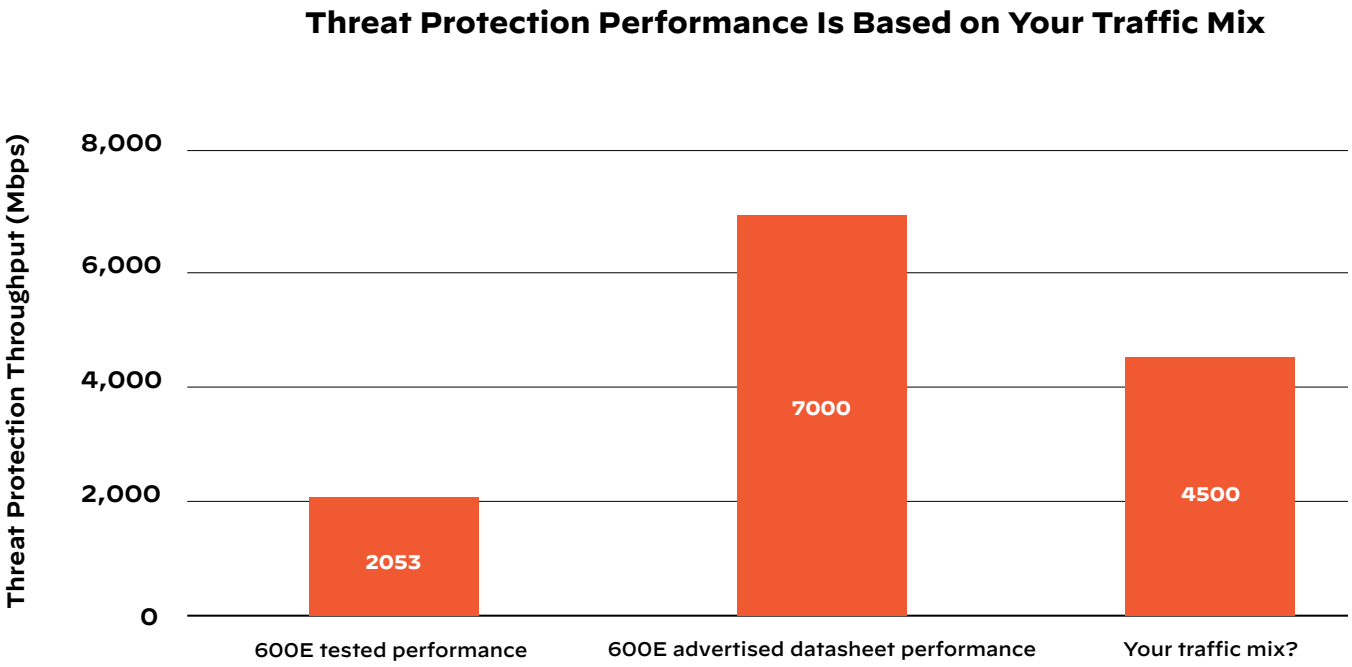

Figure 1: "Threat Protection" performance by traffic mix

This Sunnyvale-based firewall vendor makes substantial claims about its firewall appliance, SSL inspection, and Threat Protection performance in datasheets while touting a cheap price tag. We recently tested the vendor's 600E firewall appliance, which advertises 7 Gbps Threat Protection and 8 Gbps of SSL inspection throughput. To determine how they stacked up to our firewall appliances, first we tested the 600E on our own test harness, using the exact testing methodology we use for our own datasheet information. Then, we tested our Next-Generation Firewall appliance using the "Enterprise Traffic Mix." The results were interesting, albeit predictable.

When testing the 600E ourselves, we saw a 50% average reduction in Threat Protection performance (Firewall, IPS, Application Control, and Malware Protection enabled). When testing the inverse—our Next-Generation Firewall on this vendor's test harness—we observed an average 50% **increase** in performance with those same features enabled. This is important as it perfectly illustrates how significant traffic mix is with respect to datasheet numbers. In production environments, the most important factor is your organization's traffic mix.

Here are a few key questions to consider when shopping for a Next-Generation Firewall:

- Does the vendor provide the next-generation firewall with the highest security efficacy (no missed evasions in the latest NSS Labs test)?
- Are all signatures enabled all the time? Or will you need to juggle signature databases and modes to fine-tune for performance?
- Will you need to purchase, learn, deploy, and manage additional helper products to achieve industry standard best practices?

Test for Real-World Scenarios—The Proof of Concept

The most accurate way to determine a datasheet's accuracy is to put the vendor to the test. Testing that doesn't represent real-world deployments is of little value—if your deployed products don't perform as promised, you may be forced to disable critical security features to recoup performance. This exposes your organization to avoidable risk, prompts more hardware purchases, and introduces operational complexity that drives up costs.

A proof of concept lets you accurately test next-generation firewalls as well as related services and subscriptions, either on their own or against one another in your real-world, operational environment. This gives you an accurate representation of real-world deployment scenarios.

Top 10 Benefits of a POC

1. Understand the firewall's performance in your enterprise, with your unique traffic mix.
2. Demonstrate whether the firewall is right-sized for your traffic mix and security needs.
3. Understand how the firewall will scale as your business needs grow to maximize your ROI.
4. Get hands-on administrative experience to understand day-to-day operations and usability.
5. Experience operational consistency between GUI and CLI.
6. Easily leverage network and threat visibility and intelligence without needing to purchase helper products.
7. Experience consistent firewall and management platform GUI with operations at scale to increase efficiency, reduce errors, and reduce overall TCO.
8. Validate performance needs and security in your unique environment.
9. Test advanced features like SSL inspection and automation to understand how the platform can be customized and how it responds.
10. Test integration with your specific business requirements.

Palo Alto Networks Firewalls Are Made in the US—Why Is This Important?

Why not ship off the manufacturing and engineering to China as many security vendors do? At Palo Alto Networks, we pride ourselves on providing premium security products that not only deliver the highest levels of security, but are also developed and manufactured with the highest standards of supply chain integrity.

The manufacturing process introduces a variety of vulnerable stages, making it vital to have practices and processes in place to prevent potential exposure and keep the product and IP secure. Next-Generation Firewall hardware design and development are both done in one place: our United States corporate headquarters in Santa Clara, California. Our hardware manufacturing is done in Milpitas, California, a mere 10 miles from our headquarters.

Palo Alto Networks implements both internal and external security controls based on various well-established standards, including, but not limited to, those from the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO), particularly ISO 27001.

If a firewall manufacturer is willing to falsify their country of origin records, what's next?

Bloomberg Businessweek disrupted the cybersecurity world with a bombshell claim that Supermicro motherboards in servers, used by major tech firms, contained stealthily implanted chips the size of a grain of rice that allowed Chinese hackers to spy into those networks. The NSA dismissed it as a false alarm. The DEF CON hacker conference awarded Bloomberg two Pwnie Awards for "most overhyped bug" and "most epic fail," and no follow-up reporting has confirmed its premise.[2]

> **A Sunnyvale, California-based firewall vendor intentionally falsified their manufacturing country of origin documents and mislabeled Chinese-made firewalls that were sold to US government end users.**
>
> **– US Department of Justice, 2019[3]**

WIRED followed up with a report stating that a tiny, tough-to-detect spy chip could easily be planted in a company's hardware supply chain. It was demonstrated that it didn't require a state sponsored spy agency to pull it off, just a motivated hardware hacker with the right access and as little as $200 worth of equipment.[4]

2. "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," Bloomberg Businessweek, October 4, 2018, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.
3. "Sunnyvale-Based Network Security Company Agrees To Pay $545,000 To Resolve False Claims Act Allegations," April 12, 2019, https://www.justice.gov/usao-ndca/pr/sunnyvale-based-network-security-company-agrees-pay-545000-resolve-false-claims-act.
4. "Planting Tiny Spy Chips in Hardware Can Cost as Little as $200," Wired, October 10, 2019, https://www.wired.com/story/plant-spy-chips-hardware-supermicro-cheap-proof-of-concept.

At the CS3STHLM security conference, security researcher Monta Elkins demonstrated how he created a proof-of-concept version of that hardware hack in his basement. With only a $150 soldering tool, a $40 microscope, and some $2 chips ordered online, Elkins was able to alter a Cisco firewall in a way that he says most IT admins wouldn't notice, yet would give a remote attacker deep control.

> **"It's not magical. It's not impossible. I could do this in my basement."**
>
> **- Monta Elkins, FoxGuard**

Who's There to Guarantee Your Success?

Palo Alto Networks is the only security platform provider that offers a 24/7, J.D. Power award-winning Technical Support Center to ensure your cutover goes off without incident. At Palo Alto Networks, your security is our utmost priority. We'll explore your investment fully without introducing unexpected operational complexity, costs, or risks.

Hidden Costs Associated with Critical Subscriptions and Features Lurk Behind Promises of an Interwoven Security Fabric

In today's threat landscape, some vendors' all-in-one fabric approaches fall short of hitting the mark when it comes to delivering the security efficacy and operational efficiency your organization requires. It's more important than ever to invest in an innovative, comprehensive, and cohesive security platform that offers the right integrated tools and technologies. This solution set should provide comprehensive, scalable, and highly focused security protection to your ever-changing business needs as they scale from firewall appliances and VMs, to the cloud, endpoints, IoT, and beyond. No other security vendor offers a more comprehensive and effective security solution than Palo Alto Networks.

> **"Palo Alto Networks next-generation firewalls enable us to simply enforce both network-layer and application-layer policy in a single rule … We can now make all changes from one place, including bandwidth management and firewall control, in near-real time, with most of the work being automated."**
>
> **- Bank Central Asia**

With breaches happening at alarming rates, cost is only one of many variables to consider when evaluating your security platform provider—the top priority should be security. Beyond this, you need to be aware of limitations due to products that are not truly integrated and difficult to manage.

Cobbled-together offerings that are not truly integrated often introduce hidden costs with added complexity.

Will you have to pay for additional subscriptions or products for features that should come natively with your firewall, such as visibility into applications based on users? Are these potential costs included up front and transparent based on the services and requirements you need?

Palo Alto Networks offers a technology-agnostic view into the true economic value of various security offerings. We believe security investments should provide a quantified bottom-line impact. Don't be surprised by hidden costs!

Rely on customer views and proof-of-concept testing to validate ease of operations. Palo Alto Networks is consistently referenced by customers as simple to operate.

Contact your Palo Alto Networks sales representative to discuss how Palo Alto Networks can help reduce complexity and lower your operational expenses while providing better security to secure your enterprise.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com