Decoding Network Security Datasheets

Don't Be Fooled by Cryptic Information

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 high requirements and low risk tolerance. Transparency in performance testing and truth in advertising arm you with the most accurate data and ensure you can make the right decisions.

Dig Deeper into Performance

Understanding stated performance numbers and how they are derived is crucial for informed buying. If it's unclear how a vendor derived advertised performance, ask the vendor to explain their testing methodology. 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**

1. "Technology Insight for Network Security Policy Management," Gartner, February 21, 2019, https://drive.google.com/open?id=1rkO9GVLSZBhRIoNT8EWyTIFl4aSoXMqh

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 all north-south traffic is SSL encrypted, and encryption is a well-used evasion technique for threat actors, yet only a fraction of customers implement SSL decryption to inspect this traffic. SSL decryption is an industry-recommended best practice. You should understand what ciphers a vendor uses in SSL inspection tests as well as the key lengths used. Some vendors may test with keys as small as 256 bits to game the system, whereas 2048-bit keys are common in the real world. Most importantly: determine if threat prevention features were enabled during performance tests.
- **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 bring performance benefits at the cost of security.
- **File blocking:** Compliance best practices recommend file blocking, a.k.a. 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:** Find out if logging was enabled during testing. In a production environment, you'd certainly have it enabled for visibility of threats, incident response and forensics, detection of emerging patterns of activity, deployment of machine learning tools, and more.

"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 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 for your environment contextually frames performance testing compared to a generic 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.

Future-Proof Your Investment

Some vendors sell application-specific integrated circuit (ASIC) technology while others promote software or a blend of software innovation and programmable hardware. The proven combination is a balance of the right hardware and mature software. As new industry-standard features or protocols are released, the ability to drive these features without losing performance is critical. If you can't effectively push new features and protocols to existing hardware, your hardware lifecycle is shortened and your network becomes more vulnerable.

Test for Real-World Scenarios

The most accurate way to determine if a datasheet is accurate 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

You should never have to decide between security and performance.

For more information please review 10 Things to Test Before Buying Your Next-Generation Firewall.

Contact your Palo Alto Networks account team today to discuss how the Security Operating Platform® can help reduce complexity and save money with lower operational expenses while providing better security across your network, clouds, and endpoints.

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

© 2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.
panw-decoding-network-security-ds-031120