5 Critical Mistakes When Evaluating a Next-Generation Firewall

The firewall is the foundation of enterprise data security. All firewalls are not created equal, though, and no two organizations have the same needs, risks, and data flow. You need a firewall to protect against today's advanced attacks while preserving the performance and uptime critical to foster innovation and growth.

If you're in the market for a new firewall, we'll assume you understand the many benefits of next-generation firewall technology and that a next-generation firewall is the way to go. That said, how can you be sure you're choosing the right next-generation firewall to meet your organization's specific networking, performance, and security needs for the present and future?

Test It Before You Buy It

Testing a next-generation firewall in your environment—with your traffic and data, for your specific use cases—will demonstrate whether that firewall is the right choice for your organization's unique needs. With that in mind, here are five critical mistakes to avoid when evaluating a new next-generation firewall and selecting the perfect fit.

1. Incorrectly Sizing the Firewall

Avoid relying solely on datasheets and other "performance on paper" summaries as they are inaccurate points of comparison for firewalls. There are fundamental differences in features and offerings from one firewall vendor to the next. For example, one vendor might measure consolidated threat prevention features (e.g., intrusion prevention systems [IPS], antivirus, command and control, URL filtering) in terms of performance impact, while another might highlight performance impact based solely on best-in-class IPS capabilities in a standalone box.

To ensure accurate "apples to apples" firewall comparisons, you should size capabilities to your organization's real-world environments' requirements (e.g., IPS, application control, advanced malware detection) and your traffic mix. When doing so, it's critical to account for performance impact that may result from enabling other features in the future.

In addition, advanced capabilities, such as TLS/SSL decryption, will vary in performance impact depending on processing logistics. Some vendors decrypt using the hardware form factor while others decrypt using software—each with varying effects on performance. Further, threat response performance should only be compared with all required signatures activated. Carefully read the documentation for out-of-the-box collections of signatures to determine actual coverage. Performance often continues to degrade with the introduction of additional signatures. Some further considerations:

- Avoid trade-offs between security and performance. You should never have to decide between enabling a feature or signature and crippling your performance.
- Accurately map to your requirements for throughput and traffic composition. It is difficult for anyone to argue against testing the actual traffic to be secured. Simulators can't represent custom applications, real-world usage scenarios, or shadow IT.

2. Choosing a Firewall in a Silo

Several teams within IT count on the firewall to enable them to do their jobs effectively and efficiently, and they all have different needs and priorities:

- **Networking teams** prioritize hassle-free integration with current architecture, ease of use and deployment, and network performance and uptime.
- **Security teams** focus on seamless integration with existing security controls, better overall security, and threat prevention versus detect-and-respond tactics.
- **Security operations teams** work best with single-pane management and automation for security features and capabilities.
- **Data center teams** need automated features and capabilities, segmentation/microsegmentation of hybrid cloud environments, scalability to meet evolving needs, and single-pane management.
- **Application teams** want simple, fast, and secure application development and deployment.

In a typical evaluation scenario, the firewall vendor works directly with the networking team to evaluate and implement a firewall. Accounting only for the needs of the networking team is a critical mistake, though—one with potentially dire results for other teams that rely on the firewall. For example, the networking team usually isn't concerned with security and may very well prefer an option that doesn't account for the scope of security your business demands. Both the security and security operations teams should be engaged early to provide input on the level of threat prevention and other security capabilities required. For the sake of overall business efficiency and success, your organization should account for the varying needs of all key stakeholders when choosing a new firewall.

3. Buying Into Roadmap Features and Promises

Purchasing a firewall based on the promise of future roadmap features is risky. First, there is a high probability that timelines will slip, affecting business development, innovation, and execution of projects and initiatives in progress. Second, there is no guaranteeing the stability, maturity, or functionality of upcoming features before significant testing. New features may also require major operating system version upgrades across all firewalls and connected management devices, the complexity of which can outweigh the benefits.

Instead, you should look at past behavior to predict whether roadmap promises will be fulfilled. Evaluate your next firewall purchase as part of a trusted and tested platform, verifying that core, required features are available at the time of purchase. Furthermore, you'll benefit from selecting a next-generation firewall platform that can be easily updated with new security innovations, comprehensive threat information, data analysis, and signatures. This way, security teams can solve the most challenging security use cases with the best technology available, without the cost or operational burden of deploying new infrastructure for each new function.

4. Failing to Account for Ease of Integration and Scalability

A new firewall should enhance your IT infrastructure without complex integration. It should easily integrate with your current ecosystem without forcing you to replace other infrastructure components with products from the same vendor—particularly in cases where integration is still relatively complex even after those replacements. Often, once you've successfully migrated to a single vendor, management issues and complexities persist between individual networking and security devices.

You can avoid the age-old vendor lock-in hook by choosing a firewall vendor with a strong community of technology partners to ensure seamless integration with your ecosystem from both networking and security perspectives. In addition, you should not be forced to manage the integration efforts of a new security platform—that should be the vendor's responsibility.

Scalability as business requirements change is also a key factor when choosing a new firewall. A vendor that uses cloud architecture for innovation and design can scale much more quickly without the need to frequently update hardware on the network edge. In addition, the on-demand nature of the cloud inherently offers greater agility, higher performance, and much faster access to innovative technologies. This results in a higher likelihood of compatibility with future technology and new applications, better overall support, and easier integration with your network.

5. Choosing a Firewall with Multiple Management Experiences

Some firewall vendors promise your networking and security teams will be able to "leverage the same skill set" if you switch to their firewall. Unfortunately, this is often not true even when switching between products from the same vendor (e.g., stateful inspection firewall to next-generation firewall). When it comes to networking and security, resources and expertise are often scarce. It's counterproductive to choose a firewall vendor that employs completely different design frameworks and management user interfaces from one product generation to another, complicating deployment and introducing steep learning curves.

Avoid the compounding effects of maintaining multiple management interfaces during phased hardware refreshes. This way, if you choose to migrate to a single vendor, integration and management will be easy. If you choose not to, make sure the firewall vendor you choose offers a vast ecosystem of strategic technology partners who can offer expert help in terms of manpower and knowledge.

Run a Proof of Concept

To maximize performance, security, and your return on investment (ROI) while avoiding these five critical mistakes, run a proof of concept (POC). This will allow you to accurately test next-generation firewalls, along with their affiliated services and subscriptions—either on their own or up against one another—in your real-world, operational IT environment, whether physical, virtual, containerized, or hybrid. A POC gives you tangible proof points and evidence to ensure the firewall you choose will provide your business with the ideal balance of network performance and security.

To set up a POC, get in touch with your Palo Alto Networks sales representative.

Not ready for a POC? Check out these other tools and these resources to learn more about our products and get hands-on experience:

- 10 Things to Test in Your Future Next-Generation Firewall
- Next-Generation Firewall Buyer's Guide
- Our Customers Succeed Around the World (customer feedback)

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

5-critical-mistakes-when-evaluating-a-next-generation-firewall-b-100520