WEI CYBERSECURITY

INSIGHTS | TECH BRIEF

Centralized Management of Palo Alto Networks NGFWs

Enterprise security requires a multilayered cybersecurity strategy to combat today's sophisticated threats. While a defense-in-depth strategy requires multiple integrated tools, the next-generation firewall (NGFW) remains the cornerstone of effective protection. NGFWs serve as the first line of defense for all your sites, offering advanced threat prevention, application-level visibility, and intelligent network segmentation. They not only protect against known threats but also leverage machine learning and behavioral analytics to identify and mitigate emerging risks. Without properly placed NGFWs, your organization's digital assets stand dangerously exposed to potential attacks.

The Leader in NGFWs

WEI partner Palo Alto Networks continues to demonstrate innovative leadership in the cybersecurity industry. Recently recognized as a Leader in the Forrester Wave™: Enterprise Firewall Solutions, Q4 2024 report,[1] the company's next-generation firewalls achieved the highest score in the Current Offering category and ranked second in the Strategy category. Says Forrester:

> *"Precision AI, Palo Alto Networks proprietary AI system, automates tasks with data from ML, deep learning and AI models to enhance platform experience."*

This isn't the first time Forrester has credited Palo Alto Networks line of NGFWs. According to the Forrester Total Economic Report dated January 2024,[2] Palo Alto Networks customers experienced a total savings of $2.5 million thanks to the increased security and operational efficiency of its NGFW products. Other notable quantified benefits included:

- 50% reduction in the likelihood of data breaches
- 60% decrease in time required for handling security incidents
- 229% return on investment (ROI) over a three-year period

Palo Alto Networks Vision for Integrated Security

The Forrester report highlighted another significant benefit: Palo Alto Networks customers were able to reassign 50% of their full-time security professionals to higher-value initiatives. This was made possible by management efficiencies gained through vendor consolidation and the use of a common platform. Palo Alto Networks customers benefit from integration

paloalto NETWORKS

across the company's comprehensive security ecosystem. This integration is particularly impressive given the diverse range of NGFW models offered. Their extensive portfolio includes:

- **Ruggedized Solutions**

  The PA-220R: An ML-Powered NGFW designed for harsh industrial environments like manufacturing plants and energy facilities.

- **Campus and Internet Edge**

  The PA-3400 Series: Delivers up to 25 Gbps throughput in a compact 1U design, ideal for internet edge and campus environments.

- **High-Performance Data Centers**

  The PA-7000 Series: ML-Powered NGFWs providing robust security and up to 200 Gbps throughput, tailored for high-speed data centers and service providers.

Of course, Palo Alto Networks offers numerous models beyond these, catering to diverse enterprise needs. A notable example is the PA-5400 Series, a 2U datacenter appliance line. This series includes the recently launched PA-5445, which delivers 2.5X threat performance and 50% higher session capacity.

With such a diverse array of platforms deployed across an expanding enterprise, a critical question arises: How can organizations effectively gain comprehensive visibility into all these different NGFW platforms? The answer is Strata™ Cloud Manager and Panorama®. Let's dive in.

Central Management with Panorama

For over a decade, Panorama, Palo Alto Networks centralized management platform, has provided unified control, visibility, and policy management across distributed network security infrastructures. Imagine having the ability to manage up to 5,000 firewalls from a single interface. This includes firewalls dispersed across cloud and on-premises environments that can span multiple geographic regions throughout the world. This exceptional scalability is Panorama's hallmark. Available as either a virtual or physical appliance, Panorama offers management capabilities for your on-prem or private cloud environments with capabilities that include:

- Manage updates, licenses, and content across all firewalls from a single interface.
- Push configurations to firewalls grouped by business function, geographic location, or custom criteria.
- Apply consistent security policies, and monitor threats across both cloud and on-premises firewalls from a single interface.
- Gain real-time insights into applications, URLs, threats, data files, and traffic patterns using an interactive interface with graphical views of network and threat activity.
- Create shared policies and templates for consistent security controls across all firewalls worldwide.

Security vulnerabilities often stem from human error rather than technology failures. With research showing that over 95%[3] of firewall breaches originate from misconfigurations, Panorama addresses this critical vulnerability through intelligent automation. It continuously monitors security policies, identifies potential configuration errors, and enables automated remediation workflows, while reducing complexity at the same time.

Strata Cloud Manager: The New Kid on the Block

While Panorama remains the preferred choice for large, established on-premises deployments, Palo Alto Networks has another management solution called Strata Cloud Manager (SCM). For organizations embracing cloud-first strategies, Strata Cloud Manager delivers a SaaS-based approach to network security management that complements Panorama's robust capabilities. Here are some of the ways that SCM is different than Panorama:

- Goes beyond firewall management by offering AI-powered analytics, automated workflows, and real-time threat intelligence across multiple security layers.
- SCM is a cloud-based SaaS solution that manages both NGFWs and Prisma Access (SASE) from a single interface.

- Uses machine learning and AI-driven security analytics to proactively detect threats and optimize security operations.
- Ideal for large-scale, hybrid, and multi-cloud environments, providing elastic scalability via the cloud.

In other words, SCM is an AI-driven platform designed for broader security operations beyond the management of NGFW deployments. SCM enhances security and operational efficiency through proactive health monitoring and AI-driven security posture management. But what does all that mean? How about this:

> *With SCM, security teams can forecast deployment health and proactively identify capacity bottlenecks up to seven days in advance[4] with predictive analytics to prevent operational disruptions!*

The platform's AI-powered analysis of policies and configurations against industry and Palo Alto Networks best practices to significantly bolster an organization's security posture. For instance, it detects misconfigurations and policy gaps that attackers could exploit and then assists in remediating them. In fact, every month, Strata Cloud Manager shares 715.5K misconfigurations for resolution.

With automated recommendations and workflows, organizations can optimize security configurations, eliminate risks, and maintain continuous compliance without manual intervention. For compliance-focused organizations, SCM continuously monitors firewall configurations against key frameworks such as NIST, CIS, and PCI DSS, to ensure adherence to security standards across the entire infrastructure. Not only does SCM's intelligent automation reduce mean time to remediation, but it also allows security teams to shift from reactive firefighting to strategic planning. Now they can harness SCM's advanced analytics to make data-driven decisions that strengthen overall cybersecurity posture while demonstrating measurable security outcomes to stakeholders.

Bringing It All Together

Cyberthreats are only going to get more sophisticated as time moves forward. This means IT leaders must simplify and strengthen security operations through centralized firewall management. Whether your organization needs to manage thousands of NGFWs with Panorama or leverage AI-powered automation with Strata Cloud Manager, Palo Alto Networks offers the solutions to enhance security visibility, reduce risks, and optimize IT operations.

Talk to WEI today

Are you ready to unify firewall management and improve your security posture? WEI's security engineers can provide a live demo of Panorama or Strata Cloud Manager, helping you determine the right fit for your IT environment.

Contact WEI today to schedule a consultation and experience the benefits of centralized firewall management firsthand.

Sources:

1. Forrester Research. (2024, Q4). The Forrester Wave™: Enterprise firewalls, Q4 2024. Palo Alto Networks. Retrieved from https://start.paloaltonetworks.com/forrester-wave-firewall-2024.html

2. Forrester Consulting. (2024, January). The total economic impact™ of Palo Alto Networks next-generation firewalls. Palo Alto Networks. Retrieved from https://start.paloaltonetworks.com/rs/531-OCS-018/images/TEI%20of%20PANW%20NGFW%20-%20FINALv20240119.pdf?version=0

3. Forbes Technology Council. (2024, December 17). The consequences of network security complexity. Forbes. Retrieved from https://www.forbes.com/councils/forbestechcouncil/2024/12/17/the-consequences-of-network-security-complexity/

4. Palo Alto Networks. (2024a). Strata Cloud Manager data sheet. Palo Alto Networks. Retrieved from https://www.paloguard.com/datasheets/strata-cloud-manager-ds.pdf

About WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. We go further.

WEI is an expert in business technology improvement, helping clients optimize their technology environments and work efficiently. WEI works with clients to understand goals, integrate strategy with technology solutions, and leverage their current IT environment into one company-wide model to increase utilization and efficiencies around their unique business processes.