

Palo Alto Networks ML-Powered Next-Generation Firewalls and Network Perception NP-View

The Importance of Protecting Mission-Critical Assets on the Path to Cyber Resiliency

Benefits of the Integration

- Retrieve configuration files from Palo Alto Networks ML-Powered Next-Generation Firewalls (NGFWs) or Panorama network management systems (Panorama) devices.
- Analyze firewall configurations to identify potential configuration risks and vulnerabilities.
- Alert key users of potential risk situations in near-real time.
- Review an interactive visual representation of the network topology and cyber risks.

The Challenge

Your cyber resiliency journey starts with establishing a clear baseline. Then you can verify if your risk mitigation controls align with what you'd expect. In order to do this, you will need an accurate view of the network architecture and cyber-security posture. This information can then be used to set up continuous monitoring so you can decrease your response time and adapt quickly to disruptions.

While performing regular reviews of your compliance metrics is important for your organization, accessing that data and analyzing it can be time-consuming, tedious, and limited depending on where you are looking. As cybersecurity risks grow, reviews need to become more comprehensive and frequent and need to be managed in a way that will not overburden security and audit teams.

Network assessment automation is a foundation of cyber resiliency that enables security and audit teams to transition from point-in-time spot-checking to real-time verification.

Network Perception: NP-View

NP-View, combined with Palo Alto Networks NGFWs and Panorama, provides a comprehensive, independent audit platform to track and verify system changes and provide network visibility. NP-View provides auditors with assessment reports and network engineers with proactive alerts to help identify potential network risk. NP-View's read-only approach isolates the assessment team from the management systems, providing a secure barrier to prevent accidental system changes. NP-View's comprehensive connectivity path analysis allows for the assessment of each network path and

visibility into the nearest neighbors with steppingstone analysis to identify system vulnerabilities.

Palo Alto Networks NGFWs and Panorama

Palo Alto Networks NGFWs offer a prevention-focused architecture that's easy to deploy and operate. The machine learning (ML)-powered NGFWs inspect all traffic, including all applications, threats, and content, and tie that traffic to the user, regardless of location or device type. Automation reduces manual effort, so your security team can replace disconnected tools with tightly integrated innovations, focus on what matters most, and enforce consistent protection. The user, application, and content—the elements that run your business—become integral components of your enterprise security policy. As a result, you can align security with your business policies and write rules that are easy to understand and maintain.

Panorama™ empowers you with easy-to-implement, consolidated policy creation and centralized management features. Manage your network security with a single security rule base for firewalls, threat prevention, URL filtering, application awareness, user identification, sandboxing, file blocking, access control, and data filtering. This crucial simplification, along with App-ID™ technology-based rules, dynamic security updates, and rule usage analysis, reduces administrative workload and improves your overall security posture.

Palo Alto Networks and Network Perception NP-View

The integration between Palo Alto Networks NGFWs and Network Perception NP-View provides network engineers, network security and compliance analysts with an easy review of firewall access rules and object groups. The integration provides automatic identification of configuration risks and the information needed to establish a configuration change review process. NP-View's audit assistants allow the compliance team to verify cybersecurity regulations, best practices and prepare audit-ready artifacts.

For visual learners, NP-View provides the networking team with a topology map of their architecture. The topology can be used to identify and label critical cyber assets, critical network zones and review which devices are protecting which network zones.

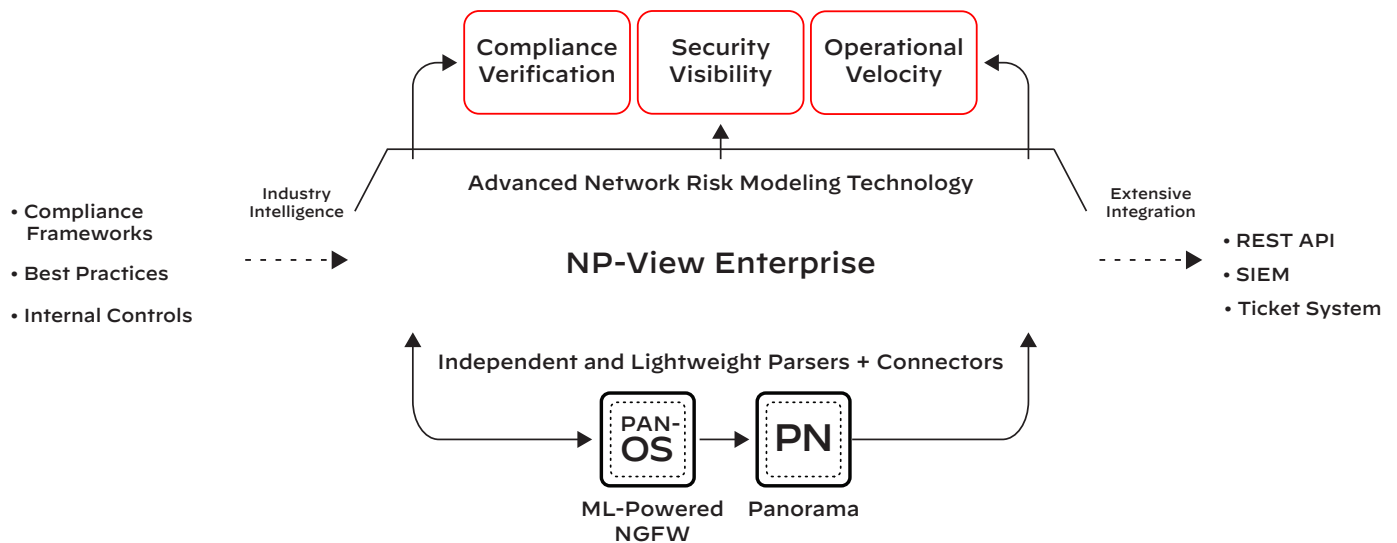


Figure 1: The NP-View and Palo Alto Networks integration

Use Case 1: Verify Configurations for Compliance

Challenge

A mission-critical OT application has a network of 1,200 high-availability NGFW pairs connected to Panorama. The internal audit team needs to collect information to perform a compliance review.

Solution

NP-View policy review provides compliance analysts with automated capabilities to easily collect and review cyber assets with their firewall access rules and object groups. Audit assistants provide automatic identification and reporting of configuration risks and remediation recommendations.

Use Case 2: Network Architecture Review

Challenge

A mission-critical IT facility is replacing its legacy network with 500 NGFWs connected to Panorama. The network architecture team wants to evaluate the network rules for potential risks before going live.

Solution

NP-View architecture review provides the networking team with capabilities for easy creation and visualization of an accurate topology of the network architecture. The topology can be used for evaluating the architecture for potential risks before the configurations are pushed into production by Panorama.

About Network Perception

Network Perception protects industrial control systems by ensuring network access security as the first line of perimeter defense. Our monitoring software provides complete network transparency and continuous mapping to better support cybersecurity compliance and enable greater cyber resiliency. For more information, visit www.network-perception.com.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. For more information, visit www.paloaltonetworks.com.



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

© 2022 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. parent_pb_network-perception_022822

© 2022 Network Perception.