

Palo Alto Networks and Keysight Technologies

Detect & Respond to New Threats Across On-Prem & Public/Private Cloud

Benefits

- Speed configuration and safeguard networks from link, power, and device outages.
- Increase resilience by automatically blocking or redirecting traffic in case of maintenance or other interruptions.
- Respond to threats faster with increased uptime using integrated high availability architecture.
- Network visibility fabric collects data to ensure comprehensive data delivery to Palo Alto Networks Next-Generation Firewalls.
- Integrated mitigation techniques between network visibility and cybersecurity can accelerate remediation.

and public and hybrid clouds. Vision NPBs remove unwanted data, mask personally identifiable information (PII), and offload decryption of transport layer security (TLS) and secure sockets layer (SSL) traffic from firewalls and other inline solutions. Bypass switches—which can be up and running within minutes—protect security devices, links, and networks from outages and promote rapid deployment of new monitoring tools as your network scales.

Palo Alto Networks

Palo Alto Networks ML-Powered NGFWs inspect all traffic at Layer 7, including all applications, threats, and content, and tie that traffic to the user, regardless of location or device type. The 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 as well as write rules that are easy to understand and maintain.

NGFWs offer a prevention-focused architecture that is easy to deploy and operate. Automation reduces manual effort so your security teams can replace disconnected tools with tightly integrated innovations, focus on what matters, and enforce consistent protection everywhere.

Palo Alto Networks and Keysight

The integration between Palo Alto Networks and Keysight creates a highly intelligent and integrated framework for scaling cybersecurity across your hybrid network. Security begins with end-to-end visibility, including packet-level data needed to spot anomalies and perform drill-down analysis to identify and contain threats. Keysight's intelligent visibility architecture captures, aggregates, and processes packet-level data from networks and clouds for use in monitoring, analysis, and forensics efforts. In addition to this comprehensive data delivery platform, Keysight bypass switches include a specific heartbeat packet for Palo Alto Networks ML-Powered NGFWs to speed deployment and provide reliability for a security operation that depends on uptime for protection. This tightly integrated solution promotes insightful threat hunting and real-time incident response while improving security resilience—the ability of the network to return to a normal state after detecting a breach.

The Challenge

Cybersecurity is a moving target, and time is of the essence. With many disparate parts and a lack of collaboration among selected vendors in your network, the fight against cyber threats could be an uphill battle for on-premise and public/private cloud networks. Integrated solutions and intelligence sharing within your monitoring infrastructure are paramount in defending against advanced persistent threats. Palo Alto Networks ML-Powered Next-Generation Firewall (NGFW) and Keysight provide an intelligent, scalable framework for detecting and responding to new threats, deploying new defenses, and staying a step ahead of today's fast-changing threat landscape.

Keysight's Network and Cloud Visibility

Keysight provides intelligent visibility across hybrid networks to optimize threat hunting, incident response, forensics, troubleshooting, and resilience. Visibility proves vital to delivering a secure, high-quality user experience. Keysight's taps, Vision series of network packet brokers (NBP), and bypass switches ensure that Palo Alto Networks ML-Powered NGFWs and other analysis solutions receive all—and only—the data they need from the network, including data centers, branch offices,

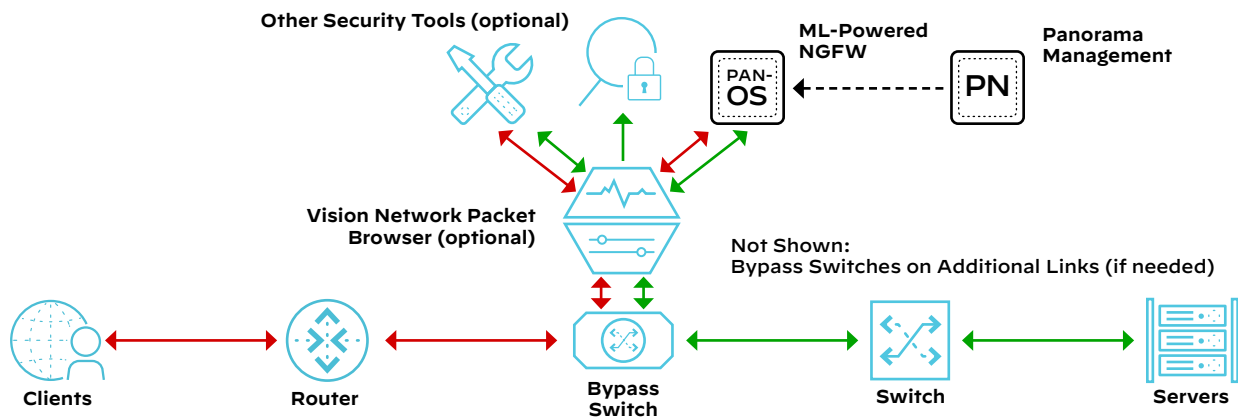


Figure 1: Sample Palo Alto Networks – Keysight joint deployment

Use Case 1: Identifying Cyberthreats and Attacks in Hybrid Environments

Challenge

Users and applications are now spread across on-premise, virtual, and cloud resources, making it difficult to have all the data to identify threats and attacks in a consistent and scalable way.

Solution

Keysight’s visibility architecture feeds Palo Alto Networks solutions with reliable real-time data, whether it’s on-prem, or in a hybrid cloud environment. The visibility fabric captures packet-level data and network traffic and load balances traffic across multiple Palo Alto Networks appliances for optimal use of resources. The integration combines security with network visibility to accommodate higher-speed traffic and rising traffic volumes, prevent network and application downtime, and add real-time application and threat intelligence.

Use Case 2: Preventing and Recovering from Outages

Challenge

Upgrading, maintaining, or dealing with failed inline security devices can result in having to take the network down for maintenance, resulting in lost service availability.

Solution

Deploying Keysight bypass switches with NGFWs safeguards availability and gives IT teams the flexibility to have tools fail open or fail closed so traffic can continue to flow in the event of link or power failure. Bypass switches send pre-configured “heartbeat” packets to Palo Alto Networks appliances to automatically verify and update status. When updating or deploying new devices, the bypass switch allows tools to be brought inline or taken out of service at any time without disruption to live network traffic.

About Keysight

Keysight Technologies, Inc. (NYSE: KEYS) is a leading technology company that helps enterprises, service providers and governments accelerate innovation to connect and secure the world. More information is available at www.keysight.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

© 2021 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_sb_keysight_071921

© 2021 Keysight Technologies