# Palo Alto Networks and Niagara Networks

## Combining Network Security Monitoring, Flexible Deployments, and High-Availability

### Benefits of the Integration

- Uninterrupted network uptime during power loss and security appliance updates
- Non-disruptive security scale and performance optimization using traffic offloading, load-sharing, aggregation, and flow replication
- Automation of fail-safe scenarios and unconstrained network security architecture
- Enhanced ROI with improved IT efficiency and scale at all data traffic rates up to 100 GB

## The Challenge

Enterprises seek to reduce the risk of security attacks and outages. This necessitates implementing a combination of products that can always protect and address threats, as well as enable highly flexible monitoring and high availability capabilities. Next-Generation Firewalls (NGFWs) safeguard mission-critical applications and data through a security foundation across physical and virtual environments, while enabling threat protection and control. To optimally provide such capabilities, NGFWs must seamlessly collect network data to inspect traffic and monitor threats, while operating flawlessly without inserting a single point of failure into the network.

## Niagara Networks

Niagara Networks enables NetOps and SecOps teams to share a visibility platform and seamlessly administer security solutions and other data networks services while ensuring performance and availability.

The Niagara BypassP2™ product line provides carrier-grade protection from network outages resulting from power loss, inline security appliance failure, or any other networking anomalies. Niagara's technology enables intelligent inline deployments, at all interface rates up to 100 GB, forwarding only relevant high-priority traffic to the firewall and load balancing between firewall appliances.

The N2 series is Niagara Networks flagship multi-purpose modular Network Packet Broker (NPB). It provides a single platform for enabling non-stop availability for the full range of visibility adaptation scenarios. The NPB series is designed to support a wide variety of modules, including fail-safe bypass, network taps, data processing, and interfaces (up to 100 GB/s) that enterprises can customize to create a robust and flexible carrier-grade deployment.

## Palo Alto Networks

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

NGFWs inspect all traffic—applications, threats, and content—and tie that traffic to the user, regardless of location or device type. 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 as well as write rules that are easy to understand and maintain.

## Palo Alto Networks and Niagara Networks

### Use Case No. 1: Uninterrupted Network Uptime

#### Challenge

NetOps teams tend to have various traffic engineering designs that complicate threat detection deployments and involve intensive CAPEX and OPEX spending. NetOps often design symmetric and asymmetric routing in a perimeter network with inline traffic that traverses multiple NGFWs. It's challenging to synchronize asymmetric traffic between inline security appliances that are a part of the same threat prevention domain. However, state synchronization between firewalls is imperative in such scenarios, and inflexible configurations can block traffic from the existing network, resulting in lost service continuity and downtime.

### Response

Niagara Networks N2 modular NPB product series and bypass solution overcomes this challenge by enabling advanced bypass state synchronization between Palo Alto Networks NGFWs. Advanced bypass state synchronization across network segments enables asymmetric routing across NGFW systems with complete automation of fail-safe scenarios and unconstrained network security architectures. In light of flexible solution offering, NetOps and SecOps teams can simplify their design and implementation workflows, streamline joint operations, and optimize security with an always-on high availability model.

## Use Case No. 2: Automation of Fail-Safe Protection for Unconstrained Network Security

### Challenge

Mobility, cloud, and streaming video services continue to disrupt network architectures and drive capacity expansions. As bandwidth growth continues to drive demand for higher performance in the mission-critical network edge, data centers, and large enterprises, customers require scalability and speed beyond the capabilities of any single inline cybersecurity tool. As the attack surface continues to expand, the scalability of inline cybersecurity tools and preservation of high availability architectures become a challenge. Threat inspection must be future-proofed to meet elastic demand and scale in a manageable and pay-as-you-grow model.

### Response

Niagara Networks N2 modular NPB product series and bypass solution overcomes this challenge by enabling advanced load balancing for Palo Alto Networks NGFWs, resulting in an elastic cybersecurity architecture. As a load balancing solution, it ensures business continuity while enabling pervasive visibility and resilient threat prevention. Advanced load balancing ensures NGFWs can protect inline traffic flow and sessions, even in the most complex traffic distribution scenarios. The combination of deep visibility into data flows at any traffic rate and load balancing based on intelligent criteria enables NetOps and SecOps teams to easily and efficiently add and administer a scalable cybersecurity architecture, while reducing operational expenses and downtime.

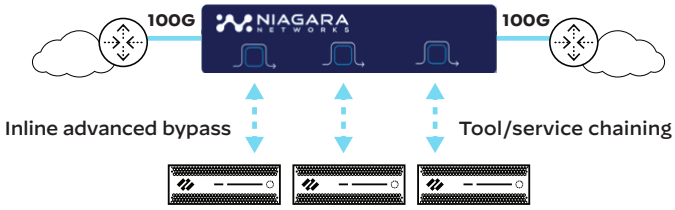


**Figure 1: Niagara Networks advanced load balancing for Palo Alto Networks NGFWs**

## About Niagara Networks

Niagara Networks is a Silicon Valley based company that provides high-performance, high-reliability network visibility and traffic delivery solutions for the world's most demanding service provider and enterprise environments.

Their solutions are installed in the world's most prominent networks, empowering security and network operations centers with end-to-end visibility and actionable traffic intelligence across physical and virtual networks. For more information, visit www.niagaranetworks.com.

## About Palo Alto Networks

Palo Alto Networks, the world's largest cybersecurity company, 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. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

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