Palo Alto Networks and Niagara Networks Partnership

Technology Segment: Network Monitoring and Availability

The Palo Alto Networks Technology Partner Program includes a select group of partners that deliver solutions or products that interoperate with the next-generation firewall.

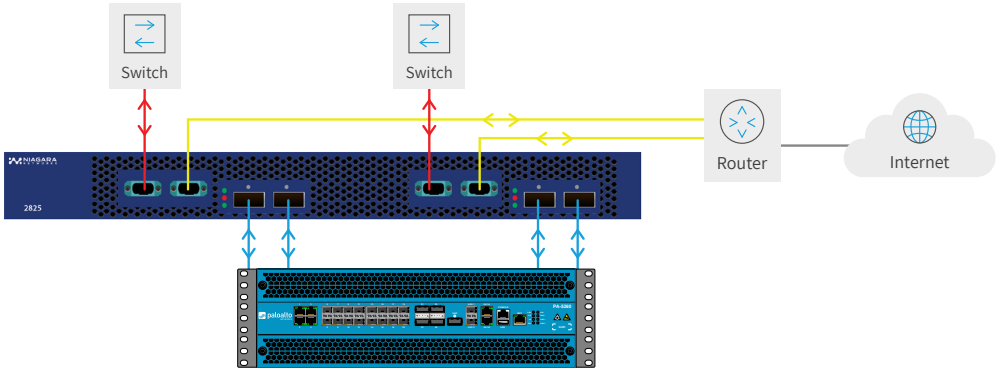
Highlights

- Bypass system assures connection integrity achieving high-availability network
- Inline threat prevention without impacting network reliability
- Telco Grade bypass system with dual power supplies, AC/DC support, and removable fans
- Allows update of inline devices without network downtime
- Supports 1Gb, 10Gb, 40Gb, 100Gb fiber SM, MM and copper networks
- Supports PA-7000 Series, PA-5200 Series, PA-5000 Series, PA-3200 Series, PA-3000 Series, PA-2000 Series, PA-800 Series

Solution Overview

On mission critical network segments, customers may prefer to deploy a tap/bypass switch to maintain network continuity to mitigate the risks of scheduled or unscheduled downtime of an inline appliance for configuration changes, maintenance, or repair.

Palo Alto Networks next-generation firewall with Niagara Networks network packet broker. The figure depicts bypass switch functionality, enabling inline deployment protection. Network traffic from the Router (yellow lines) goes into the Niagara's bypass switch, and from there forwarded to the next generation firewall. Inspected traffic returns from the firewall to the bypass switch, and from there to the Switch (red lines).



Palo Alto Networks™ has partnered with Niagara Networks to preserve the network connectivity and maintain communication at all times, even in the event of planned or unplanned device outage. The combination of Palo Alto Networks next-generation firewall and Niagara Networks Bypass P^2 technology provides transparent inline full threat prevention without reducing and compromising the reliability of the network.

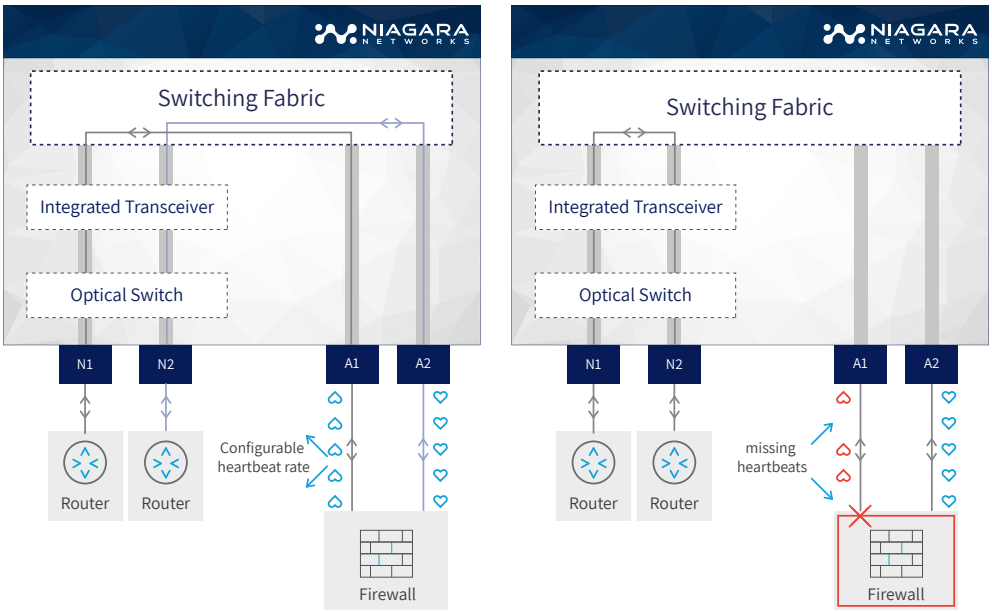
The Palo Alto Networks Technology Partner Program includes a select group of partners that deliver solutions or products that interoperate with the next-generation firewall.

When Palo Alto Networks next-generation firewall is configured in “Virtual Wire” mode to work with the Niagara Networks line of external bypass switches, hybrid network packet brokers or bypass switch modules, it can function as an inline security appliance without the risk of network interruption. The Niagara unit provides protection from network outages resulting from power or inline appliance failure, or any other reasons.

Niagara Networks Bypass P^2 consists of 2 bypass technologies for keeping the traffic flowing on the network:

The first mode consists of an intelligent active mechanism that senses the firewall path by sending a configurable heartbeat, which can be unidirectional or bidirectional. If the heartbeat is lost, the system automatically reroutes the traffic activity until the firewall is back online. The intelligent active bypass mode preserves the link and the transition is made seamlessly.

The second mode consists of a passive bypass technology that senses the power supply to the system. Upon detection of power outage, the Niagara Networks Bypass system will fail open, making sure that the network connectivity stays intact.



Left diagram depicts Normal inline Operation Mode with Heartbeat on datapath to firewall. Right diagram depicts firewall failure detection when Heartbeat is missing, and consequent bypass

Table: Niagara Networks bypass switching capabilities

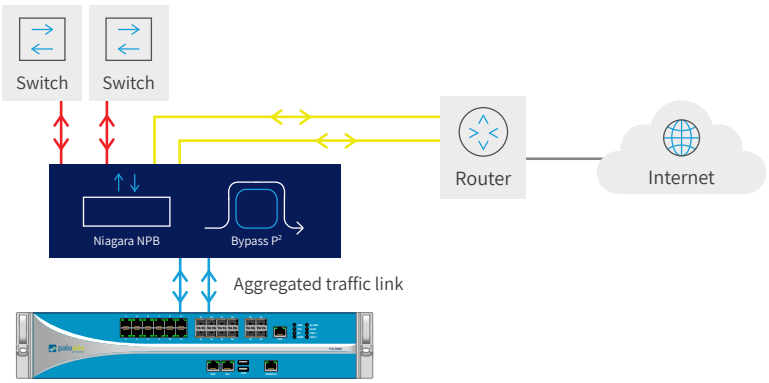
Bypass Switch Type	Niagara Networks Model	Data Rates	Bypass	Active/ Standby	Loadbalance	Filter	Information
External Bypass	2818 2825	1/10 Gb (SM/MM) 1/10/40/100 Gb (SM/MM/RJ45)	✓	✓	-	-	includes integrated tap ports
	3299	1 Gb (SM/MM/RJ45)					includes 10Gb aggregation ports
Hybrid Network Packet Broker	2804	1/10 Gb (SM/MM)	✓	✓	✓	✓	
Bypass Module in modular platfrom	2845/2847	1/10/40/100 Gb (SM/MM/RJ45)	✓	✓	✓	✓	2845/2847 Modular multi-purpose visibility nodes

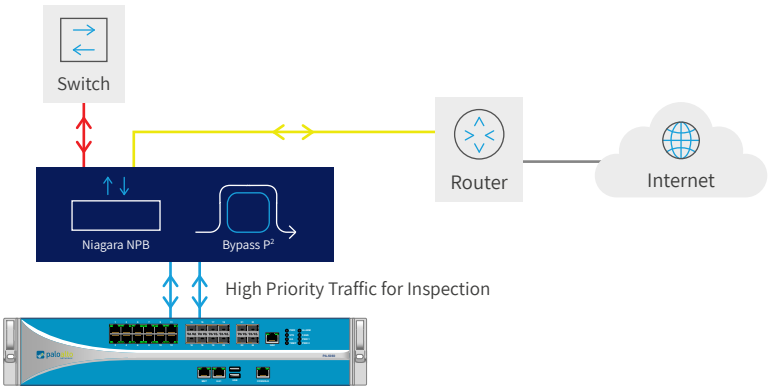
Deployment Use Cases

The following diagrams illustrate various useful deployment scenarios of Palo Alto next generation fire wall and Niagara Network bypass switch technology. More complex deployments can be created by combining the use cases depicted.

Inline deployment of multiple aggregated network traffic link

In this deployment use case, multiple network links are aggregated and only one link is forwarded to the next generation firewall. This saves on firewall resources for an optimized deployment.



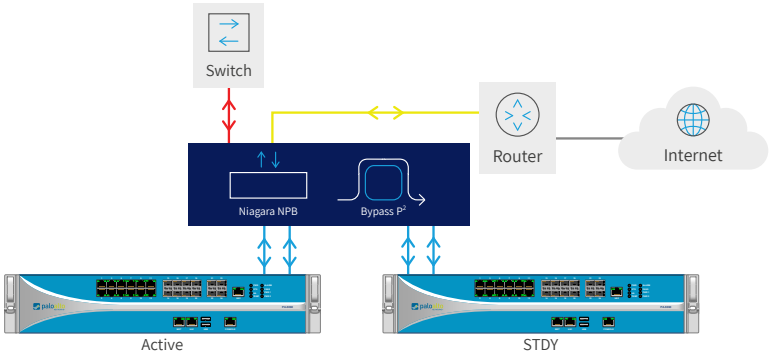


Inline deployment, forwarding only relevant high priority traffic to the firewall

In this deployment use case, users can configure that only traffic of interest will be forwarded to the firewall. The rest of the traffic bypassed directly without going through the firewall. This saves on firewall resources for an optimized deployment where not all traffic needs to be processed by the next generation firewall.

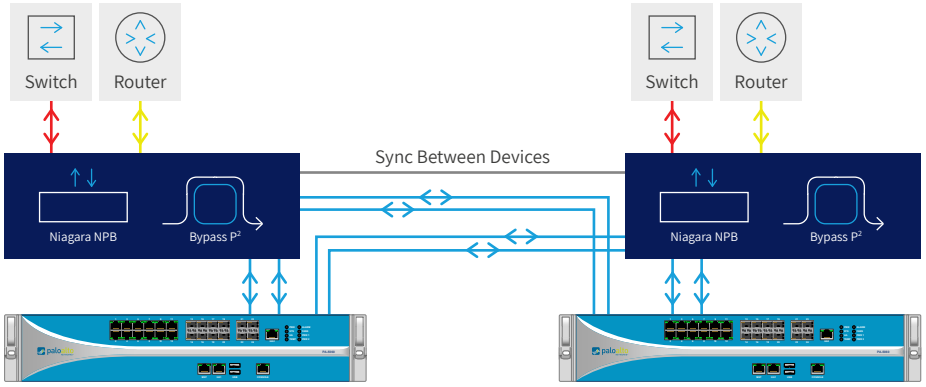
Inline deployment, load balancing network traffic between firewall devices

In this deployment use case, we want to load balance the network traffic between multiple firewalls. Alternatively, we can designate one firewall as 'primary' and the other firewall as 'secondary'. Network traffic will be forwarded to the standby/secondary firewall only on failure of the active/primary firewall. This enables us to efficiently deploy firewalls in redundancy mode.



Inline deployment, double resiliency

In this deployment use case, we want to ensure link redundancy, bypass switch redundancy and firewall redundancy. A control link between the two Niagara devices serves to synchronize bypass segment states and status.



About Palo Alto Networks

Palo Alto Networks™ (NYSE: PANW) is the network security company. Its innovative platform allows enterprises, service providers, and government entities to secure their networks and safely enable the increasingly complex and rapidly growing number of applications running on their networks. The core of Palo Alto Networks' platform is its Next-Generation Firewall, which delivers application, user, and content visibility and control integrated within the firewall through its proprietary hardware and software architecture. Palo Alto Networks' products and services can address a broad range of network security requirements, from the data center to the network perimeter, as well as the distributed enterprise, which includes branch offices and a growing number of mobile devices. Palo Alto Networks' products are used by more than 9,000 customers in over 100 countries.

For more information, contact techpartners@paloaltonetworks.com | www.paloaltonetworks.com

About Niagara Networks

Niagara Networks provides high performance network visibility solutions for seamless administration of security solutions, performance management and network monitoring. Niagara Networks products provide advantages in terms of network operation expenses, downtime, and total cost of ownership.

A former division of Interface Masters, Niagara Networks provides all the building blocks for an advanced Visibility Adaptation Layer at all data rates up to 100Gb, including Taps, bypass elements, packet brokers and a unified management layer. Thanks to its integrated in-house capabilities and tailor-made development cycle, Niagara Networks are agile in responding to market trends and in meeting the customized needs of service providers, enterprise, data centers, and government agencies.

NIAGARA NETWORKS

150 E Brokaw Road
San Jose, CA 95112, USA

www.niagaranetworks.com
sales@niagaranetworks.com

Tel: +1 408 622 0354
Fax: +1 408 213 7529