SOLUTION BRIEF

Fortinet and Niagara Networks Security Solution

Broad, Integrated, and Automated Solution for Eradicating Blind Spots and Identifying Imminent Threats

Executive Summary

Niagara Networks and Fortinet recently established a technology partnership to offer comprehensive solutions that dramatically reduce deployment complexity, risk, and effort. The combined solution offers complete visibility into network flows and eliminates network downtime by optimizing the number of tools required and ensuring highly available networks for continuous threat monitoring and remediation.

Challenges

Enterprise networks are exceedingly multifaceted and business-critical and require the elimination of the risks of both security attacks and outages as critical imperatives. This necessitates implementing solutions that can continuously protect and address threats as well as enable highly-flexible monitoring and high availability capabilities to ensure attacks are exposed anywhere and anytime they arise.

Joint Solution Description

To provide a uniform security foundation across physical and virtual environments, and enable next-generation threat protection and control, NGFW systems must be able to seamlessly collect the network data required to inspect traffic and monitor threats and operate flawlessly without inserting a single point of failure into the network.

Niagara Networks complements Fortinet's FortiGate Next-Generation Firewall with the PacketMaster™ N2 modular Network Packet Broker (NPB) series. The NPB platform provides a single multi-purpose platform for enabling non-stop availability for the full range of visibility adaptation scenarios. The NPB platform supports a variety of modules that can be customized to meet the challenges for creating a robust visibility adaptation layer.

Deploying FortiGate NGFW with Niagara PacketMaster™ NPB provides the following benefits:

Network bypass: Eliminates single point of failure scenarios by redirecting the network traffic to bypass an inline FortiGate NGFW system in the event of a power outage or planned, or unplanned inline tool events that could disrupt network traffic.

Load balancing: Optimizes network security scalability and processing capability of Fortinet NGFW appliance by allowing the pooling of tools to inspect more traffic. Load balancing also allows matching of traffic data rates to the number and capacity of in-place NGFW systems, thereby simplifying network security architecture design.

Packet deduplication: Deduplicates redundant packets before forwarding to NGFW devices. This substantially reduces the traffic volume and optimizes the NGFW efficiency.

Joint Solution Benefits

- In-line NGFW/IPS/DDoS always-on and flexible security architectures
- Uninterrupted network uptime during power loss and security appliance updates
- Optimal performance using traffic offloading, load balancing, aggregation, and flow replication
- Enhanced ROI with improved efficiency and scale

FORTINET Fabric-Ready

Packet slicing: This feature reduces the volume of data forwarded to Fortinet NGFW devices by reducing the packet length based on user-configurable options. Packet slicing is a deterministic capability of the NPB hardware-based Packetron module which removes any risk of jitter or packet drop.

Data masking: NPB enables the Fortinet NGFW deployments to forward and share data traffic across departments, while at the same time providing them with a tool to mask private and confidential user information, such as the password contained in the data which minimizes the risk of privacy breaches.

Application filtering: Identification of applications and layer 7 protocols often require deep packet inspection (DPI) and analysis. The NPB Application filtering performs deep packet inspection for supporting policy-based application-level filtering of traffic to Fortinet NGFW systems.

NetFlow generation: NPB systems generate NetFlow/IPFIX-based metadata reports for forwarding to Fortinet NGFW systems. As a result, the generation of metadata is offloaded from firewall systems optimizing their aggregate performance.

Actionable Agile Security Module (AASM): The intelligent policy-triggered capabilities of the N2 modular NPB system enable trigger actions to be undertaken based on the status and state of the Fortinet NGFW system. Trigger-based policy capabilities include traffic-steering, load balancing, routing traffic via different ports, deactivating links, performing fail-over of traffic, and more.

Diagram of Joint Solution

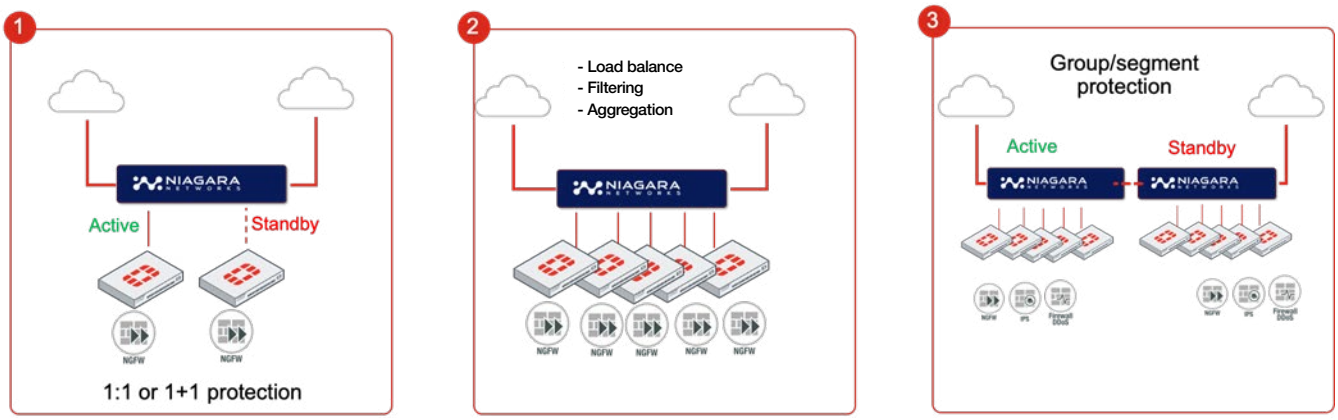

Figure 1: Niagara NPB/bypass provides nonstop availability for FortiGate solutions.

Use Case: Pervasive visibility and resilient threat monitoring

- The Niagara NPB provides bypass functionality for the high availability of FortiGate NGFW services. This enables NGFW software upgrades to be completed without network downtime as well as fast failover recovery in the event of unplanned NGFW failure.
- The NPB monitors NGFW availability and health by sending a heartbeat packet at designated intervals. If a certain number of these packets are not returned to the NPB within the timeout period, the NPB will consider the NGFW system in failure mode and instantly begin routing traffic around it to keep data flowing. The Niagara N2 NPB is also configured to fail open in the case of a power failure.
- In the event of an NGFW failure, traffic may be redistributed across healthy NGFW systems using N2 NPB load-sharing capabilities. Specifically, physical or logical bypass functionality can seamlessly divert the traffic destined for the failed NGFW device. The NPB bypass capability thus ensures business continuity while enabling pervasive visibility and resilient threat monitoring.

Niagara Networks N2 Network Packet Broker (NPB)/Bypass

N2 series is Niagara Network's 2nd generation advanced packet broker with a universal modular platform. the N2 series provides a single multi-purpose platform that covers all of the visibility adaptation scenarios in your network. The N2 series can be populated with a wide range of high density, high versatility, processor-accelerated modules. With a modular design, it supports advanced FabricFlow technology, capabilities, and features including network tap, bypass, packet broker and packet processing applications. Available in both a 1U and 2U form factor.

Fortinet FortiGate Next-Generation Firewall

FortiGate Next-Generation Firewalls (NGFWs) utilize purpose-built security processors and threat intelligence security services from AI-powered FortiGuard labs to deliver top-rated protection and high-performance inspection of clear-texted and encrypted traffic.

Next-generation firewalls reduce cost and complexity with full visibility into applications, users and networks while providing the best of breed security. As an integral part of the Fortinet Security Fabric, next-generation firewalls can communicate within Fortinet's comprehensive security portfolio as well as third-party security solutions in a multivendor environment to share threat intelligence and improve security posture.

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.

Our solutions are installed in the world's most prominent networks, empowering Security and Network Operations Centers (SOC/NOC) with end-to-end visibility and actionable traffic intelligence across physical and virtual networks.

www.niagaranetworks.com

April 3, 2020 2:06 AM

618260-0-0-EN

D:\Fortinet\Solution Briefs\grey solution briefs\Niagara Networks\sb-FA-fortinet-and-niagara-networks-422020\sb-FA-fortinet-and-niagara-networks-422020