

Case Study

International Financial Institution Optimizes Data Centers' Security with Performance, Reliability and Scalability Using Niagara Networks' data center gatekeeper platforms.

In-line Next Generation Firewalls and Intrusion Prevention Systems Run at the Speed of Business

Challenge

The true cost of security has usually been considered the most important factor in terms of impact on network performance and limitations or trade-offs on network reliability, scalability and flexibility. One of the top ten largest banks and financial services companies in North America decided that they could achieve the highest standards of security without making such trade-offs for over 20 of their data centers deployed globally. As a leading bank, they needed top security to combat the relentless threats and attack environment along with the speed and agility needed

to provide frictionless transactions and information exchange. They also wanted to ensure that the addition of ultra-scalable inline threat detection FireEye platforms and Cisco Sourcefire Intrusion Prevention Systems (IPS) will not introduce new points of failure that could impair the network, cause downtime or reduce flexibility. The agility and ability to ensure future growth and changes without significant disruption or complexity was also a must-have requirement.

Solution

The bank turned to Niagara Networks to add multiple N2 Series Modular platforms that included Network Packet Brokers and hybrid TAP/Bypass Switch/Network Packet Broker modules. The security team designated Niagara's solution as the gatekeeper that will serve as the primary platform at the edge of the data center that will connect, protect and scale the entire inline security stack of threat detection cybersecurity elements. The platform provides easy deployment points for the security solutions combined with a policy and logic-based environment to manage the solutions for high availability and resilience. These policy and logic rules can be easily created to adapt to any security or networking sandbox or failure scenarios or simply take any security devices off-line for maintenance. The platform also enables tools or services chaining configurable in any logical order and maintained without additional cabling. The Niagara Networks solutions are designed for carrier-grade networks, providing the highest levels of performance and reliability.

The empowered data center gatekeeper solution of Niagara Networks decreased CAPEX costs by 50% since the multi-functional platform could do more with the performance and flexibility the bank needed. It reduced the number of visibility elements required while providing efficient aggregation and filtering at the TAP level. As a result, less equipment needed to be deployed and had fewer devices to manage. The ease of implementation and simplified administration also lowered OPEX costs through a significant reduction of resources required by the networking and security teams to manage their network.

The security team designated Niagara's solution as the gatekeeper that will serve as a primary platform at the edge of the data center that will connect, protect and scale the entire in-line security stack of threat detection cybersecurity elements.

The Niagara Networks solution performs intelligent aggregation and filtering of tapped or inline data traffic, including five tuple anchors for granular selection and traffic optimization. It provides a significant power multiplier to network architects and security teams by efficiently accessing any or all specific required data in real-time with optimal and simple implementation closer to the source, consequently reducing any bottlenecks and latency while allowing for better utilization of the available bandwidth to the inline security stack. Such a powerful and flexible solution enables CAPEX savings of over 50% by reducing the number of visibility elements and efficient aggregation at the TAP level.

Niagara Networks also offers a single pane of glass platform to provision the visibility infrastructure with the Niagara Visibility Controller (NVC) that can support great scalability through a simple point and click management GUI. It adds another value by further reducing operational expenses, architectural limitations and complexity by enabling design, capacity planning, implementation and management of hundreds and thousands of visibility elements without the need for complex command line interface (CLI) configurations and extensive training.

Value Proposition

- Reduced CAPEX by 50% as well as ongoing reductions to OPEX due to the need for less deployment solutions and the ease of deploying and managing implementations
- Highly reliable, always-on inline security – inline bypass for any scenario and traffic rates
- Carrier-grade solution for Active/Standby 1:1 data center edge
- Load balancing per flow and policy-based complex actionable rules
- Offload the demands of traffic filtering on each IPS by performing it centrally on the Niagara appliances
- Complete management of tool chaining with logical flow of operations maintained
- Ability to easily add additional inline or out-of-band security or networking solutions
- Rich policy and logic management with simple GUI-based management
- Complete management of tool chaining with logical flow of operations maintained
- Ability to easily add additional inline or out-of-band security or networking solutions
- Rich policy and logic management with simple GUI-based management



“Niagara Networks enabled us to adapt the most advanced security solutions without compromising network performance, reliability or the ability to fluidly scale for future growth and needs. The powerful visibility appliances make deployments easy and greatly reduce the work in managing and maintaining solutions.”

Financial Institution Operations Architect

