– Bricata & Niagara Networks provide transparent intrusion prevention –

Next Generation Intrusion Prevention System with Bricata

Challenge

Using innovative technology, Bricata provides a deep, multi-vector cyber threat defense system to protect your network. Based on multi-threaded processing for unparalleled throughput speeds, Bricata's Next Generation Intrusion Prevention System (NGIPS) delivers double the detection performance for more timely threat prevention in a single appliance, supports cloud-based configurations, and comes in at roughly half the cost of traditional IPS solutions. With 80% of breaches occurring within networks' perimeter, Bricata's core level security stops threats where they occur. Niagara Networks is a leading vendor in the bypass and network monitoring market. Providing industry leading price performance solutions, Niagara Networks' enables 1Gb, 10Gb, 40Gb and 100G networks to be protected against any possible outage, such as power failures, planned maintenance, or unexpected outages. Using Bricata's Next Generation Intrusion Prevention System, with Niagara Networks' bypass technology, transparent intrusion prevention can be achieved without reducing or compromising the reliability of the network.

Solution Benefit Summary

- Plug & Play, User friendly Web GUI/Management
- Scalable Enterprise Grade Visibility & Security Solution
- Ensures Comprehensive Network Access, Visibility and uptime
- Support for 10G & 1G Network TAP, Filtering, Mirroring, Aggregation, Load Balancingand Speed Conversion between Network Links & Monitoring/Security Tools
- Continuous Monitoring and Breach Detection
- Comprehensive Network Forensics
- Software based Sensors can be deployed on commodity hardware or in virtual environments
- Detection via Analytics, Signature, Behavioral and File Analysis
- Query and Visualize Network Traffic
- Network Analytics, Reporting and Alerting
- Cost-Effective Solution

Proposed Architecture

All appliances that are placed inline on a network present a single point of failure, which could potentially cause network downtime. This can be caused by power failure, or a number of other possible risks. By connecting a Niagara Networks' bypass system to a Bricata security appliance, the potential point of failure is effectively eliminated, ensuring consistent and complete network uptime. Niagara Networks' bypass solutions provide the required network protection by making sure the network stays intact, at all times.

The Niagara Networks line of Niagara External Bypass units are easily configured to work with Bricata's line of NGIPS, with zero configuration required on the Niagara Networks unit ('Plug and play').

If there is a network failure due to an unexpected Bricata NGIPS outage, the Niagara Bypass unit will detect this failure and re-route all network traffic to bypass the NGIPS, keeping the traffic flowing on the network. The Niagara Networks Bypass system consists of 2 bypass technologies:

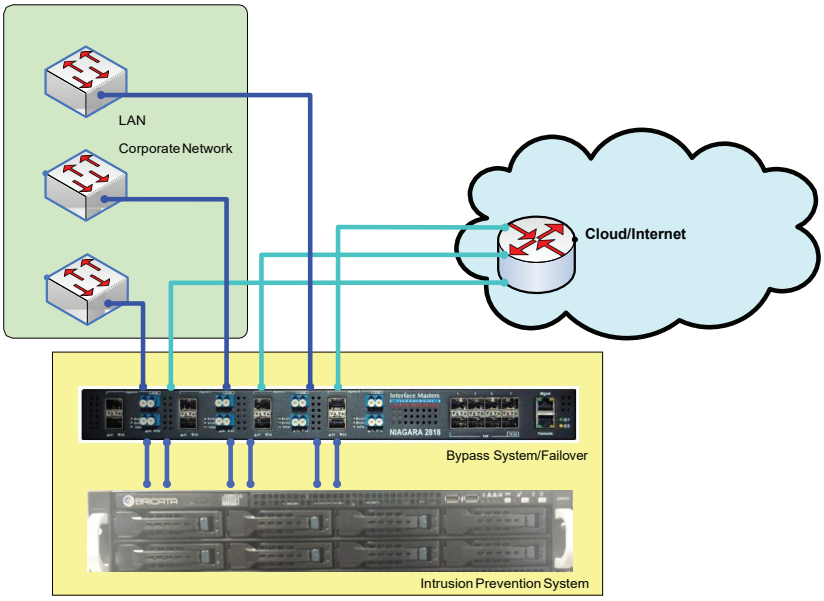
- The first mode consists of an intelligent 'active' mechanism that senses the NGIPS path by sending a configurable heartbeat, which can be unidirectional or bidirectional. If the heartbeat is lost, the system automatically reroutes the traffic 'actively', until the NGIPS is back inline. The intelligent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

- The second mode consists of a passive bypass technology that senses the system's power supply. Upon detection of power outage, the system fails-open, making sure the network connectivity stays intact.

The Niagara Bypass unit can also be configured to prevent traffic from flowing if it detects any kind of failure in Bricata's NGIPS. This feature is useful for networks that have redundant paths. The networking devices on the network can detect if traffic is not flowing on the route where the Niagara Bypass unit is present, and will then reroute the traffic using the backup path.

It is also possible to configure the Niagara Bypass unit to operate in "TAP" mode. In this mode, a copy of the network traffic will be sent to the Bricata's NGIPS for inspection, and the bypass switch will not expect traffic to be returned to the network. In this mode, the traffic is unidirectional.

The Niagara Bypass units will send out a layer 2 Ethernet frame heartbeat (by default) in order to verify appliance health. The Bricata's NGIPS will forward this heartbeat from its input port to its output port with no configuration in "Virtual Wire" mode.



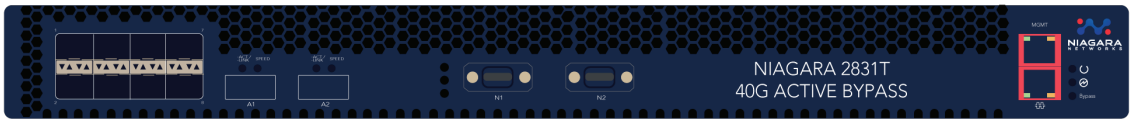
Application Diagram - Niagara Networks and Bricata

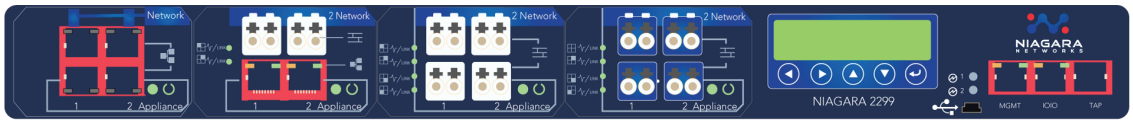
In addition to its basic functions, the Niagara bypass units can be used along with Bricata's Intrusion Prevention systems in multiple other cases. For example, a second Bricata's Intrusion Prevention System can be connected to a segment on the Niagara bypass unit and can be configured for redundancy in case the primary Bricata appliance falls.

Niagara Networks Niagara External Bypass Units are available in many different models to accommodate many different types of networks. Following is a list of available configurations:

- 1 – 4 segments. Each segment contains 2 network ports and 2 appliance ports.
- 1 Gigabit SX/LX/Copper
- 10 Gigabit SX/LX
- 40 Gigabit

Niagara Bypass Switches





About Bricata

Bricata is a leading developer of innovative, high-throughput network security and data protection solutions. Our Bricata ProAccel Appliances are based on Next Generation Intrusion Prevention Systems (NGIPS) technology, enabling both small and large enterprises to secure and protect data and networks cost effectively, without sacrificing performance or creating bottlenecks that inhibit productivity. Using our high-speed solutions to automate the capture, analysis and disposition of threats to network security at the core, Bricata offers more efficient threat protection across network and cloud-based devices. Built on the open source Suricata engine, and augmented with proprietary software and hardware to make it faster, more reliable and more user friendly, Bricata delivers double the throughput and detection performance in a single appliance at roughly half the cost of traditional IPS solutions. Now deployed across both the public and private sectors, Bricata's security products are enabling its clients to do more with less, providing the means for customers to minimize the time, risk and expense of maintaining a reliable intrusion prevention infrastructure so that they can be more productive, competitive and compliant at a dramatically reduced cost. Read more: www.bricata.com

About Niagara Networks

Niagara Networks is a Network Visibility industry leader, with emphasis in 1/10/40/100 Gigabit systems including Network TAPs, External Bypass Switches, and Network Packet Brokers that integrate with monitoring systems, inline networking appliances, IPS, UTM, Load Balancing, WAN acceleration, and other mission-critical IT and security appliances. Formerly part of Interface Masters, a Silicon Valley based network solutions company, Niagara Networks recently spun off from Interface Masters to focus on its core competencies, and developed an independent company identity.

Niagara Networks offers the highest port-density systems, the most complete hybrid systems, and the highest quality and feature-rich Bypass Solutions in the market. Niagara's unique and modular designs, innovative next generation Network Visibility technology, including the 100 Gigabit-capable Network Packet Broker with hybrid functionality, and the ability to tailor systems to exact customer specifications, allow it to lead the industry with high quality, innovative products and exceptional service. For more information, please go to: www.niagaranetworks.com

NIAGARA
NETWORKS

USA
+1 408 622 0354
+1 408 213 7529
sales@niagaranetworks.com
150 E. Brokaw Rd., San Jose, Ca 95112

EMEA
+44 20 3514 2567
+1 408 213 7529
emea@niagaranetworks.com