

- DAMBALLA & NIAGARA NETWORKS PROVIDE ROBUST NETWORK VISIBILITY AND SECURITY THREAT DETECTION SOLUTION -

Comprehensive Network Monitoring and Breach Detection

Damballa, a leader in Security Threat Detection and Niagara Networks, a leader in Network Visibility Solutions, have partnered to ensure a complete network security solution that provides visibility into to all network traffic and so there is full coverage across single and multi-network link deployments.

The joint Damballa and Niagara Networks solution offers a cost-effective way to provide highly granular network visibility, deep packet inspection, netflow & traffic monitoring, content inspection, endpoint analysis, and behavioral classification to detect complex, evolving and varied threats in real time. Together, Damballa and Niagara Networks provide a plug-and-play passive network security solution that ensures network access and uptime, with intuitive and comprehensive user interface, reporting, and notifications.

Challenge

Infections can be hidden on end points, servers, and other key network nodes in an Enterprise and subtly propagated throughout mission-critical networks. Detecting these vulnerabilities and threats in the first place before they infect a network is difficult enough, but once they have infiltrated the network it becomes even more challenging. A solution is required that can detect behavioral patterns and discrepancies and identify malicious communication to react to known and unknown threats as they happen.

Solution

Together, Damballa and Niagara Networks provide a scalable solution that provides Network Visibility at 1G and 10G Critical Network links and can provide access to the appropriate network traffic for identification of Security breaches, advanced threats, endpoint threat behavior, and endpoint compromise.

The Network TAP ports of the Niagara 2804 connect to each side of one or multiple bi-directional 1G or 10G network links and transparently pass network traffic while ensuring network uptime in case of any power failure, link loss, or software crash via fail-to-wire protection. The Packet Broker ports (1G/10G flexible SFP+ ports) provide the ability to load balance, aggregate, filter, and/or mirror the tapped Network traffic to one or multiple Damballa Failsafe® Sensors. Damballa Failsafe® takes a multi-faceted approach using a multitude of detection techniques that analyzes network behavior, malicious content and applies threat intelligence. The integrated solution provides a seamless passive network monitoring and visibility solution tailored to protect enterprises, service providers, governments, and institutions.

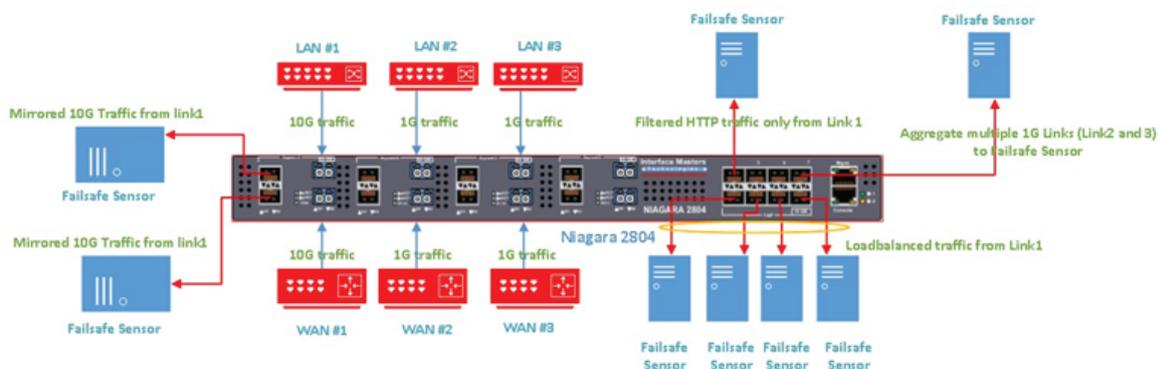
SOLUTION BENEFIT SUMMARY

- 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 Balancing and 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

Solution Applications

Common applications of the Niagara Networks Niagara 2804 and Damballa Failsafe® Sensor solution are:

- Niagara 2804 provides session-based load balancing and network speed conversion which enables 10G Network links to be monitored by Damballa Failsafe® Sensors. With the Niagara 2804 in place, an enterprise can simply connect 10G Network links into the Niagara 2804 and load balance any 10G feed to a series of Damballa Failsafe® Sensors, while maintaining session integrity
- Niagara 2804 provides ability to Filter 10G traffic based on IP, MAC, Port, Protocol, VLAN ID, or create a user defined byte and then send only the traffic that is relevant to the Damballa Failsafe® Sensor for processing, enabling the Sensor to focus on the types of network traffic that pose a threat to the network and drop the rest.
- Niagara 2804 provides the capability to take in a 10G or 1G network feed and mirror that traffic to multiple Damballa Failsafe® Sensors (or a Damballa Failsafe® Sensor and other brands of monitoring or security devices) to provide in depth or multi-layered analysis on the same critical network link
- Niagara 2804 can enable multiple 1G or 10G network links to be tapped and aggregated to a Damballa Failsafe® Sensor for analysis and monitoring. An example would be tapping the marketing, accounting, engineering, and operations 1G network links and aggregating the traffic via the Niagara 2804 and sending the traffic to a Damballa Failsafe® Sensor.



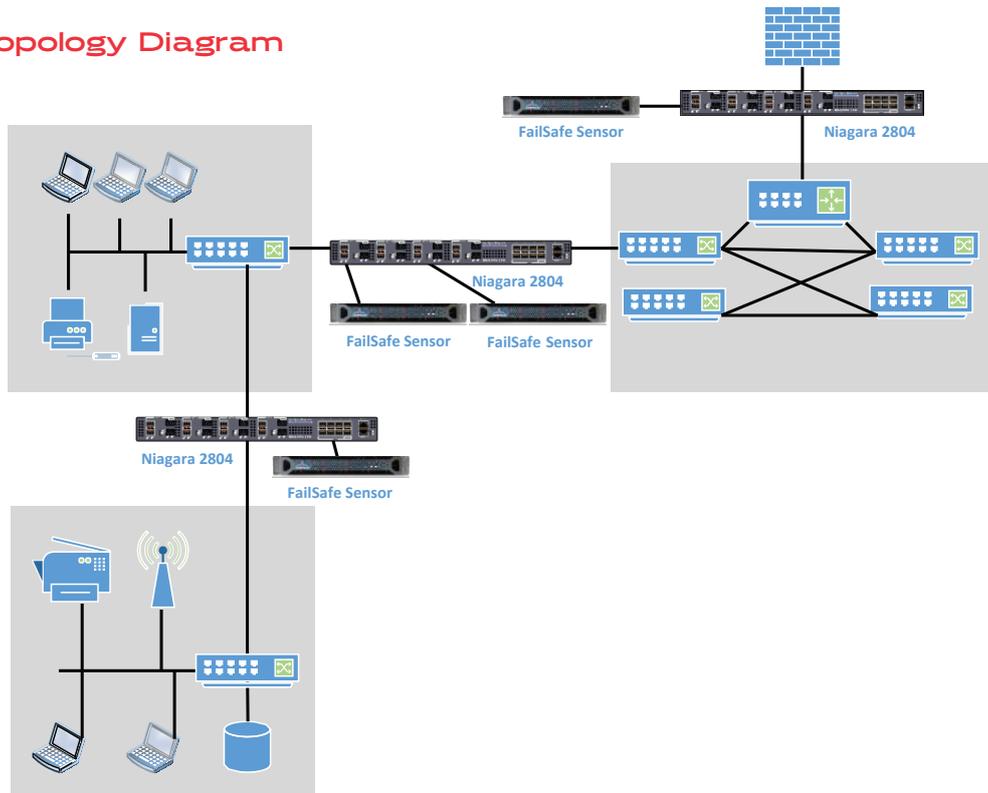
Application Diagram – Interface Masters Niagara 2804 and Damballa Failsafe Sensor

Deployment Options

The Solution can be passively deployed at any strategic network point including:

- Core/BackBone
- Site to Site
- Edge
- Distribution
- Corporate Backhaul
- DataCenter/Central Office
- Access
- Remote Office
- DMZ

Network Topology Diagram



Example Network Topology Diagram

About Damballa

Damballa was founded in 2006 by pioneering data scientists from the Georgia Institute of Technology who were conducting Ph.D.-level research around malicious network communications. They quickly realized that security controls designed to stop attackers at the perimeter would not measure up to advanced methods. Their work caught the interest of ISPs, mobile carriers and forward-thinking large enterprises. Concepts developed in the University lab were put operationalized in live networks and Damballa was born. Damballa delivers advanced threat protection for active threats that bypass traditional security layers, rapidly discovering infections with certainty and pinpointing compromises that represent the highest risk to a business. For more information, please go to www.damballa.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



USA	EMEA
+1 408 622 0354	+44 20 3514 2567
+1 408 213 7529	+1 408 213 7529
sales@niagaranetworks.com	emea@niagaranetworks.com
150 E. Brokaw Rd., San Jose, Ca 95112	

