**Damballa & Interface Masters provide Robust Network Visibility and Security Threat Detection Solution**

*Comprehensive Network Monitoring and Breach Detection with Damballa Failsafe® and Niagara 2804 Network Tap/Packet Broker*

Damballa, a leader in network monitoring of advanced threats, and Interface Masters, a leader in Network Visibility and Uptime Solutions have partnered to ensure a complete network security solution that provides visibility into to all network traffic so there is full coverage across single and multi-network link deployments.

The joint Damballa and Interface Masters 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 Interface Masters 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**

Damballa and Interface Masters 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 PacketBroker 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 Failsafe sensors, which uses multiple detection techniques. The integrated solution provides a seamless passive network monitoring and visibility solution tailored to protect enterprises, service providers, governments, and institutions.

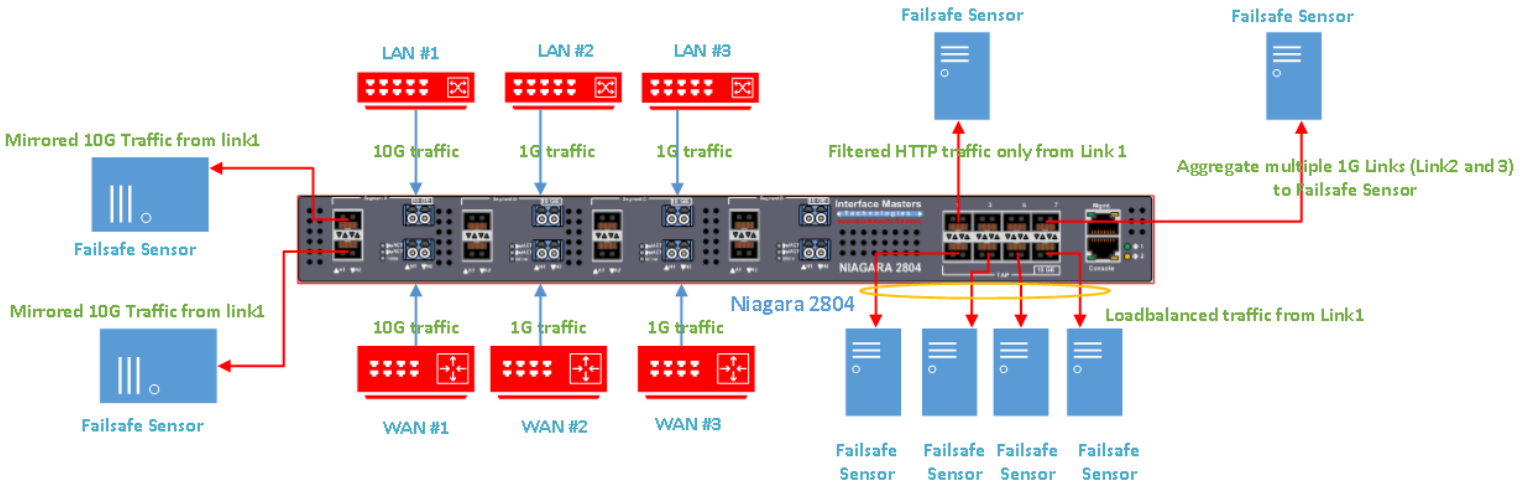
**Solution Benefit Summary**

- 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
- Access to Damballa Threat Discovery Center's (TDC) unmatched Worldwide Internet visibility
- Analyze network behaviors, malicious content and threat actor / APT activity
- Pass information to an Case Analyzer which corroborates evidence automatically
- Verify true positive infections and apply 9 factor risk-ranking
- Present response teams with prioritized workflow for immediate action
- Cost-effective solution

## Solution Applications

Common applications of the Interface Masters Niagara 2804 and Damballa Failsafe® Sensor solution are as follows:

- 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 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 Failsafe sensor.

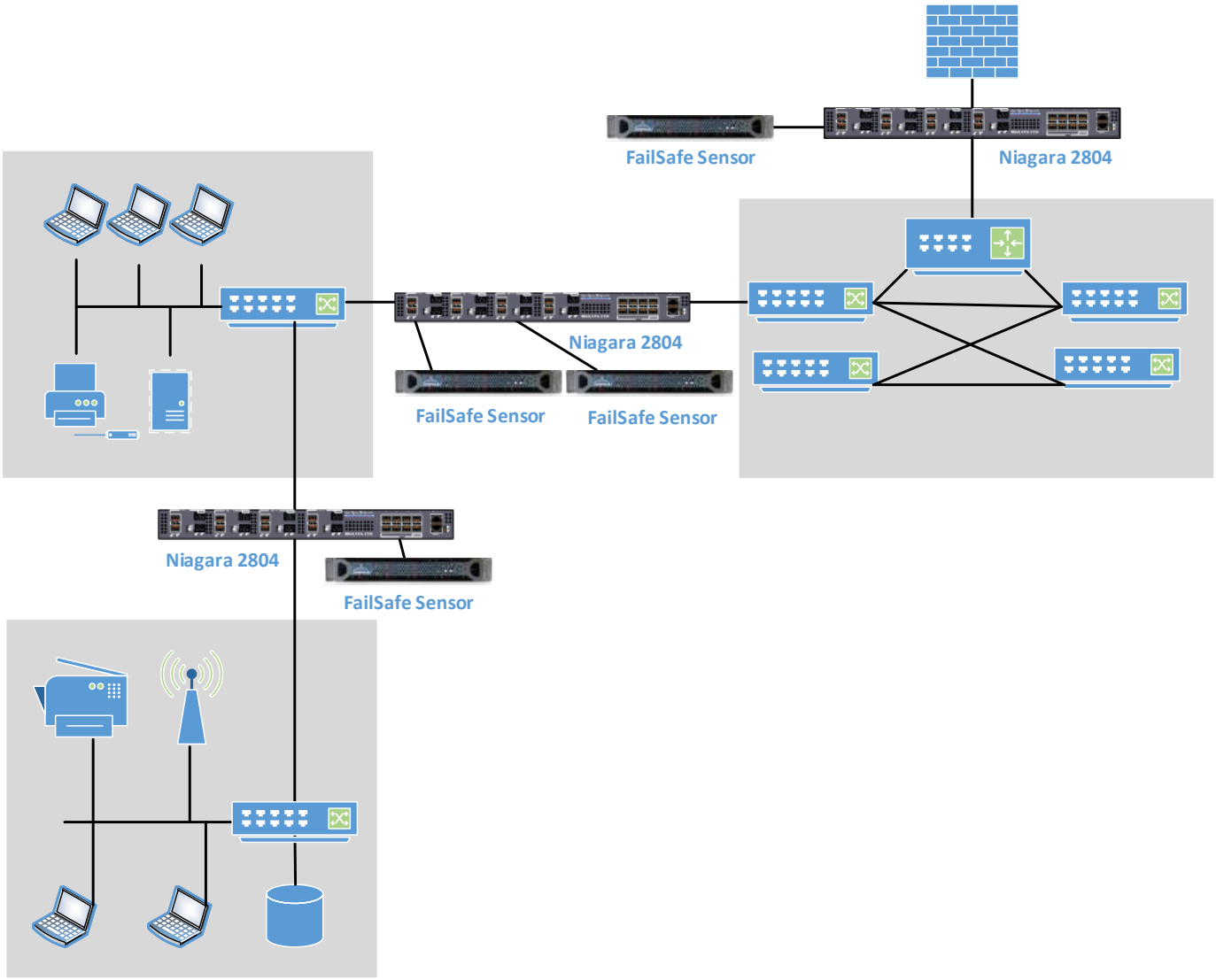



**Application Diagram – Interface Masters Niagara 2804 and Damballa Failsafe Sensor**

**Deployment Options**

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

- DNS, Proxy and Egress
- Core/Backbone
- Distribution
- Access
- Edge
- DMZ
- Site to Site
- Corporate Backhaul
- Remote Office
- Data Center/Central Office




**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 Interface Masters Technologies**

Interface Masters Technologies is a leading vendor in the network monitoring and visibility market including External Bypass and Failover Switches, PacketMaster® Network Packet Broker, Passive TAP, and Active TAP, based in the heart of the Silicon Valley. Interface Masters' expertise lies in Gigabit, 10GbE, 40GbE and 100GbE networking solutions that integrate with monitoring, inline networking, IPS, UTM, Load Balancing, WAN acceleration, and other mission-critical IT and security appliances. Company Headquarters are located in San Jose, CA with satellite offices in Hong Kong and Europe. For more information, please go to http://www.interfacemasters .com/