ReversingLabs & Interface Masters provide Comprehensive Network Visibility and Cyber Security Threat Detection

Complete Network Monitoring and File Extraction and Inspection Solution with ReversingLabs N1000 Network File Flow Sensor appliance and Niagara 2804 Network Tap/Packet Broker

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

The joint ReversingLabs and Interface Masters solution offers a cost-effective way to provide highly tuned network visibility, file extraction and inspection, event logging and analysis, email alerting, malware identification and integration with SIEMs/Syslog servers. Together, ReversingLabs and Interface Masters ensure a plug-and-play passive network security solution that provides detailed network visibility while providing maximum network uptime, an intuitive and comprehensive user interface, reporting and alerts.

Solution Benefit Summary

- Plug & Play, Web GUI/Management
- Scalable Enterprise grade visibility & security solution
- Comprehensive Network Access, Visibility & Uptime
- 10G & 1G Network TAP, Filtering, Mirroring, Aggregation, Loadbalancing & Speed Conversion between Network Links & Monitoring/Security Tools
- File Extraction, Inspection & Classification
- File Reputation Knowledgebase
- Unknown Threat analysis, reporting
- Integration with SIEM/Log Aggregation Systems
- Malware Identification
- Network Analytics, reporting and alerting

Challenge

Network Security Breaches are happening ever more frequently despite an increase in adoption of traditional and specialty network security devices. The reason is traditional Anti-Virus Scanners, IDS/IPS and Firewalls are not able to keep up with the evolution and sophistication of Modern Security Threats. In addition, many specialty dynamic analysis solutions create a "sandbox" environment to observe the behavior of security threats but even these systems, while being able to identify and mitigate many threats, still cannot keep up with the volume and multi-directional network challenges and subtlety of modern threats. Lastly, even with monitoring/security devices in place, the growth of bandwidth is forcing network security infrastructure to become overloaded and vulnerable to over-subscription (even dropped packets). A solution is needed that can provide sound security functionality and ensure full network visibility and uptime, while providing the appropriate network packets to the appropriate security/monitoring tool.

Solution

Together, ReversingLabs and Interface Masters deliver a flexible solution that provides Network Visibility at 1G and 10G Critical Network links and enables access to the appropriate network traffic for file analysis (based on file attributes), malware identification, unknown threat classification, and file reputation grading.

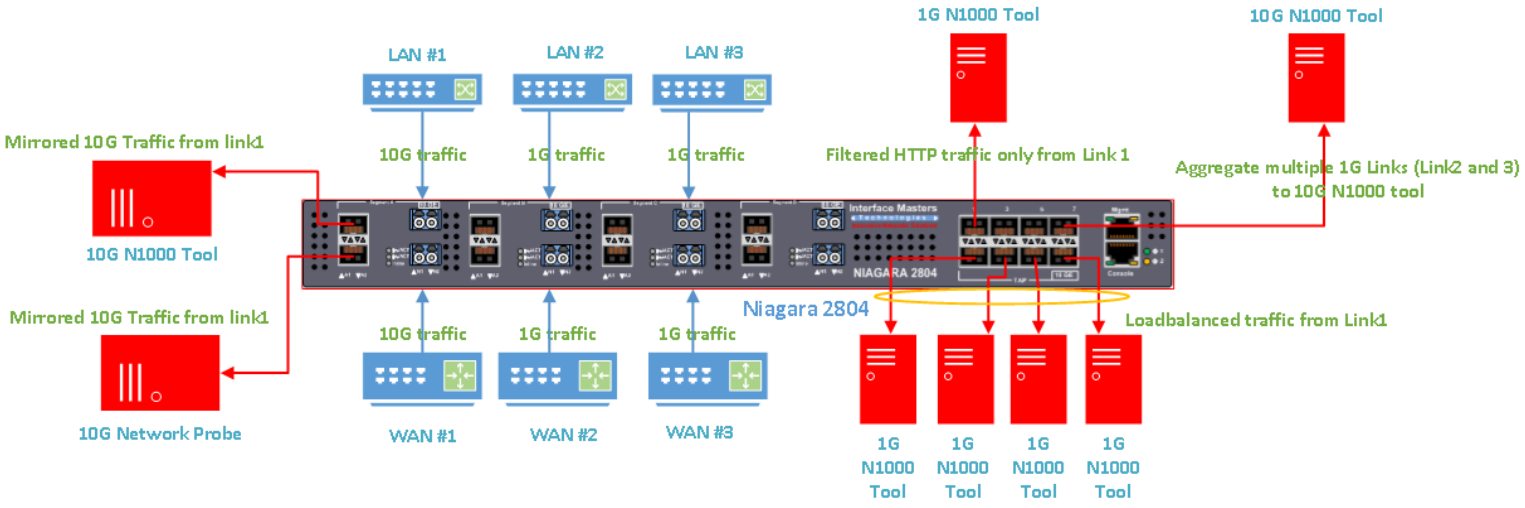
The Network TAP ports of the Niagara 2804 connect to each side of one or multiple bi-directional 1G or 10G network links and transparently pass network traffic while ensuring network uptime in case of any power failure, link loss or software crash via fail-to-wire protection. The PacketBroker ports (that come in 1G/10G flexible SFP+ ports) provide the ability to loadbalance, aggregate, filter and/or mirror the tapped Network traffic to one or multiple ReversingLabs N1000 appliances. N1000 appliances provide functions including threat analysis, file ranking and attribute assessment, advanced reporting and logging and integration with SIEMs and other Analytics tools. The integrated offering provides

a seamless passive network monitoring and visibility solution tailored to protect enterprises, service providers, governments and institutions.

Solution Applications

Common applications of the Interface Masters Niagara 2804 and ReversingLabs N1000 solution are as follows:

- Niagara 2804 provides session based loadbalancing and network speed conversion that enables 10G Network links to be monitored by an N1000 10G or 1G Appliance. With the Niagara 2804 in place, an enterprise can simply connect 10G Network links into the Niagara 2804 and loadbalance any 10G feed to a series of 1G or several 10G N1000 Appliances, 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 N1000 Appliance for processing, enabling the Sensor to focus on the types of network traffic that pose a threat to the network and drop the rest. An example would be to take in a 10G feed and filter out HTTP Traffic or Port 80 traffic and send only that traffic via a "PacketMaster" port to a port on a N1000 Appliance
- Niagara 2804 provides the capability to take in a 10G or 1G network feed and mirror that traffic to multiple N1000 Appliances (or an N1000 Appliance 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 10G N1000 Appliance 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 10G N1000 Appliance.

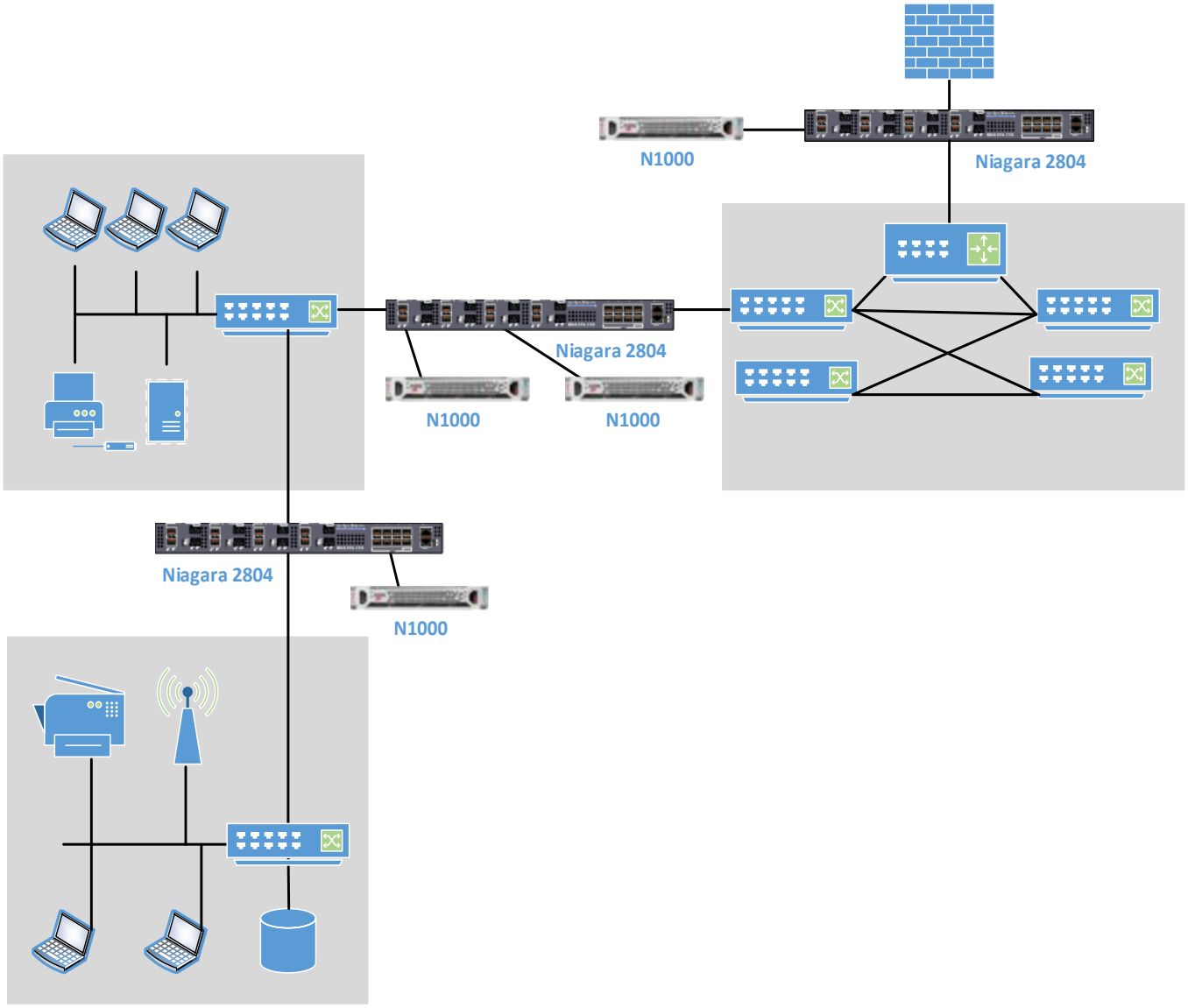


Application Diagram – Interface Masters Niagara 2804 and Reversing Labs N1000 Appliance

Deployment Options

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

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



Example Network Topology Diagram

About ReversingLabs

ReversingLabs was formed in 2009 to combat the next generation of intelligent cyber threats with a simple mission: to use experience and expertise from the security world to provide state of the art solutions for organizations to protect all their digital assets. ReversingLabs customers include antivirus vendors, security vendors, government agencies, and commercial enterprises. More information is available at http://www.reversinglabs.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. More information is available at http://www.interfacemasters .com/