– ReversingLabs & Niagara Networks Provide Comprehensive Network Visibility and CyberSecurity Threat Detection –

Complete Network Monitoring, File Extraction and Inspection Solution

ReversingLabs, a leader in Security Advanced Threat Detection and Niagara Networks, a leader in Network Visibility and Uptime Solutions, have partnered together to offer 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 Niagara Networks 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 Niagara Networks provide a passive, plug-and-play network security solution to ensure detailed network visibility and maximum network uptime, with an intuitive and comprehensive user interface, reporting, and alerts.

Solution Benefit Summary

- Plug & Play, User friendly Web GUI/Management
- Scalable Enterprise Grade Visibility & Security Solution
- Ensures Comprehensive Network Access for Visibility
- Maximizes network uptime
- 10Gb & 1Gb Network
- TAP
- Filtering
- Mirroring
- Aggregation
- Load Balancing
- Speed Conversion between Networks
- Cost-Effective Solution

Applications

- Breach Detection
- Network Forensics
- Software Sensors in Virtual Environments
- Signature & Behavioral Analytics
- Network Analytics & Reporting

Challenge

Network Security Breaches are happening ever more frequently, despite an increased adoption of traditional and specialty network security devices. The breaches occur because traditional Anti-Virus Scanners, IDS/IPS, and Firewalls are not able to keep up with the evolution and sophistication of modern security threats.

In response, many specialty dynamic analysis solutions create a 'sandbox' environment which enables security teams to observe attacks in real time , and to integrate with SIEMs and other Analytics tools. The integrated offering provides protection against security threats, but even these systems, while being able to identify and mitigate many of the threats, still cannot keep up with the subtlety, volume, and multi-directional network challenges of modern threats. Even with monitoring/security devices in place, the growth of bandwidth is forcing network security infrastructure to become overloaded and vulnerable to oversubscription (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 applicable security/monitoring tool.

Solution

Together, ReversingLabs and Niagara Networks deliver a flexible solution that provides Network Visibility at 1Gb and 10Gb 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 1Gb or 10Gb 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 (that come in 1G/10Gb flexible SFP+ ports) provide the ability to load balance, 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 solution provides a passive, seamless network monitoring and visibility solution that is tailored to protect enterprises, service providers, governments and institutions.

Solution Applications

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

- Niagara 2804 provides session-based load balancing and network speed conversion that enables 10Gb network links to be monitored by an N1000 10Gb or 1Gb appliance. With the Niagara 2804 in place, an enterprise can simply connect 10Gb network links into the Niagara 2804 and load balance any 10Gb feed to a series of 1Gb or several 10Gb N1000 appliances while maintaining session integrity.
- Niagara 2804 provides ability to filter 10Gb 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 ignore the rest. An example would be to take in a 10Gb feed, filter out HTTP Traffic or Port 80 traffic and send only that traffic via a Niagara Packet Broker port, to a port on a N1000 appliance.
- Niagara 2804 provides the capability to take in a 10Gb or 1Gb 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 1Gb or 10Gb network links to be tapped and aggregated to a 10Gb N1000 appliance for analysis and monitoring. An example would be tapping the marketing, accounting, engineering and operations 1Gb network links, then aggregating the traffic using the Niagara 2804 and sending that traffic to a 10Gb N1000 appliance.

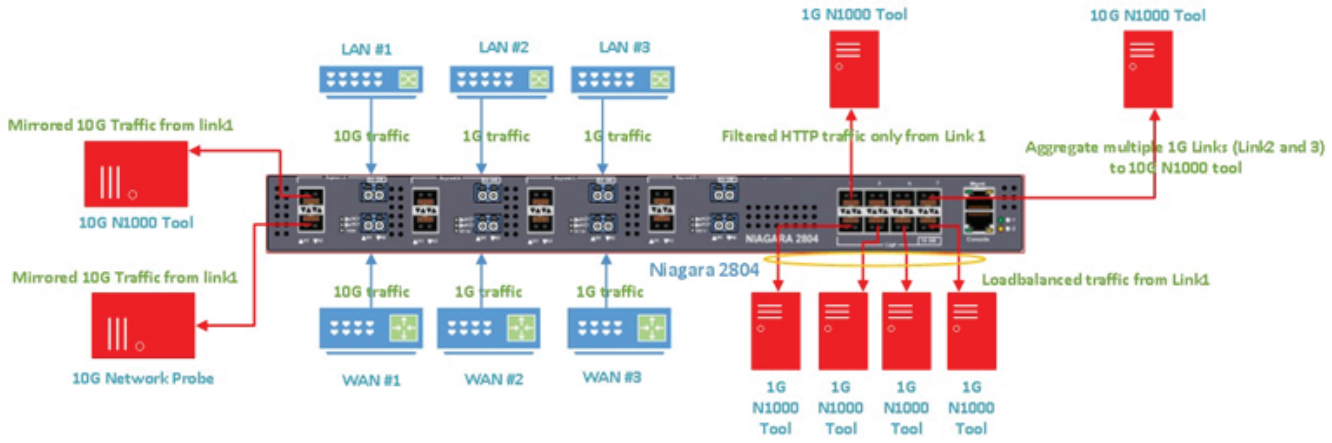

Figure 1, Niagara2804 and ReversingLabs N1000

Deployment

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

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

Application Diagram

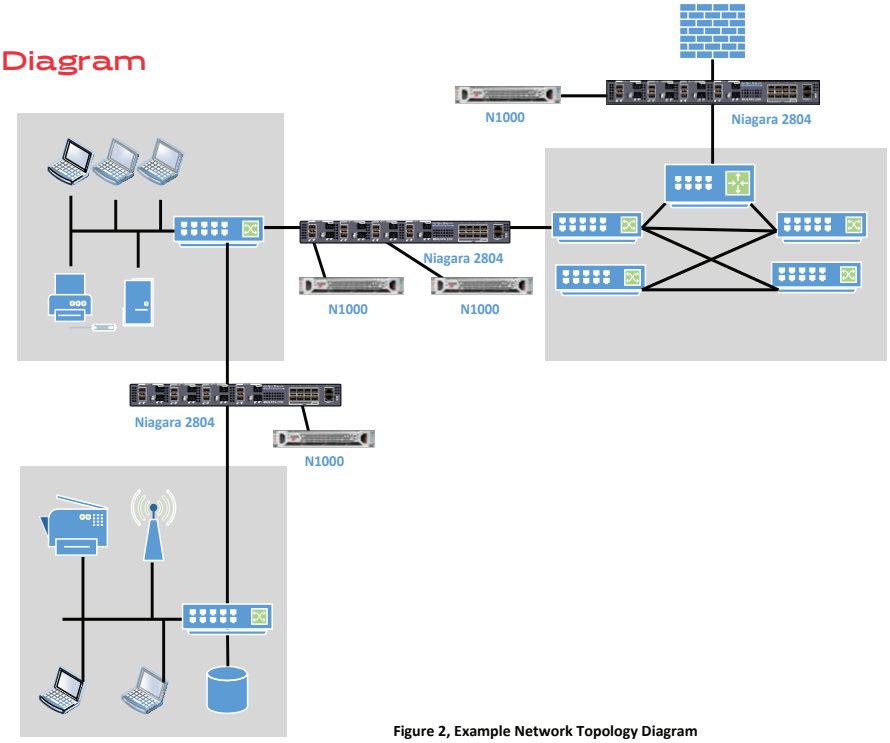

Figure 2, Example Network Topology Diagram

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: www.reversinglabs.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
+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