aria CYBERSECURITY SOLUTIONS

DATASHEET

Myricom nVoy Series 10 Gb Packet Recorder

KEY FEATURES

- Two capture ports, each supporting 1 or 10 Gb
- 10 Gb/s packet recording to disk, in pcap file format, with zero packet loss
- On-the-fly indexing and compression/decompression
- Web configuration and management
- Packet indexes accessed through a command line or an API
- Optional pcap re-injection into the network

The Myricom nVoy Series Packet Recorder enables security operations engineers to not only build next-generation intrusion detection systems (IDS), but also isolate and record accesses to an organization's critical business data including personally identifiable information (PII), enterprise resource planning (ERP), and intellectual property (IP).

The nVoy Packet Recorder makes it easy to record and index up to 10 Gb network traffic. Users can take advantage of these recordings to address issues such as compliance, forensics, and reducing the duration of incident investigation. Additionally, the Packet Recorder is fully backed by a customer support team that specializes in cyber incident response technologies.

Compliance

Some businesses demand an accurate, time-stamped record of specific conversations. Regulated industries, including financial, government, and retail must meet compliance requirements. They must also provide detailed auditing, outlining cyber-breach details, including such items as dates, times, and extent of data loss. The nVoy Packet Recorder's timestamp accuracy meets strict MiFID II specifications for recording financial transactions in automated trading. With many other regulations in effect, including HIPPA, SOX, and PCI DSS organizations need to be prepared to support these and others as they come online such as the European Union's 2018 GDPR data privacy regulation, which specifies cyber breach notification within 72 hours of any suspected intrusion.

Effective, Efficient Rapid Incident Response

Every day, numerous alert logs are generated from firewalls or other security tools, such as next-generation IPS/IDS or SIEMs, highlighting suspicious activity. However, these alerts only provide basic metadata information. While this is a good starting point, it doesn't provide enough detail for efficient, effective forensic analysis for incident investigation. With the nVoy Packet Recorder, security teams are able to capture, index, and timestamp packet-level traffic related to your most critical data and assets at the packet level. Having this detail at your disposal enables your forensic tools to improve reporting on the suspicious activity.

For example, perhaps you need to fill in the gap between two distinct incidents. You can use the metadata to determine the start and end points. However, it is the recorded data that will give you the details on what has actually transpired. Or, it may be the case that you want to take data provided from a current alert and search on whether this type of suspicious activity has occurred in the past. The alert log will allow you to isolate the search parameters, and through the recorded data your forensic tools can identify any previous points in time.

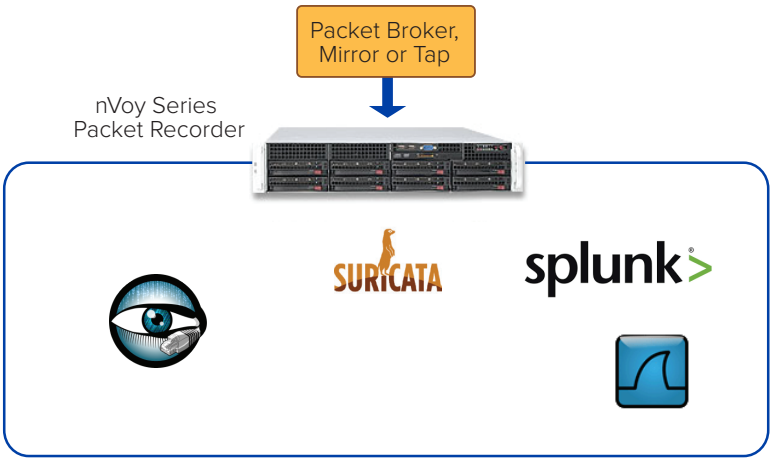
In addition, utilizing the optional nVoy AIR application, alerts targeting critical assets triggers the Packet Recorder to automatically generate an extraction file of all conversations associated with that alert. This streamlines the process and eliminates the need for manual efforts, thus reducing the risk and cost associated with manual incident investigation.

Performance

The nVoy Packet Recorder, built on the proven performance of ARIA Cybersecurity Solutions Myricom ARC Series of network adapters, captures packets at 1 or 10G speeds without drops and with extremely accurate nanosecond timestamp capability. It runs on a server that we have carefully tuned for optimal performance as a complete system (adapter, BIOS, operating system, and application software).

Of equal importance is the ability to locate and identify an area of interest quickly and effectively. Searching through large amounts of stored data for a pattern, session, or even IP addresses can present a significant challenge. The nVoy Packet Recorder creates on-the-fly index trees to retrieve packets in parallel while recording at line rate. You can search on a time basis or with an accelerated packet filter in BPF notation, or a combination of both.

Extracted packets are formatted as pcap files for further analysis in your favorite tool. An API is also available to access the indexes, allowing advanced users to develop their own search and extraction tools.



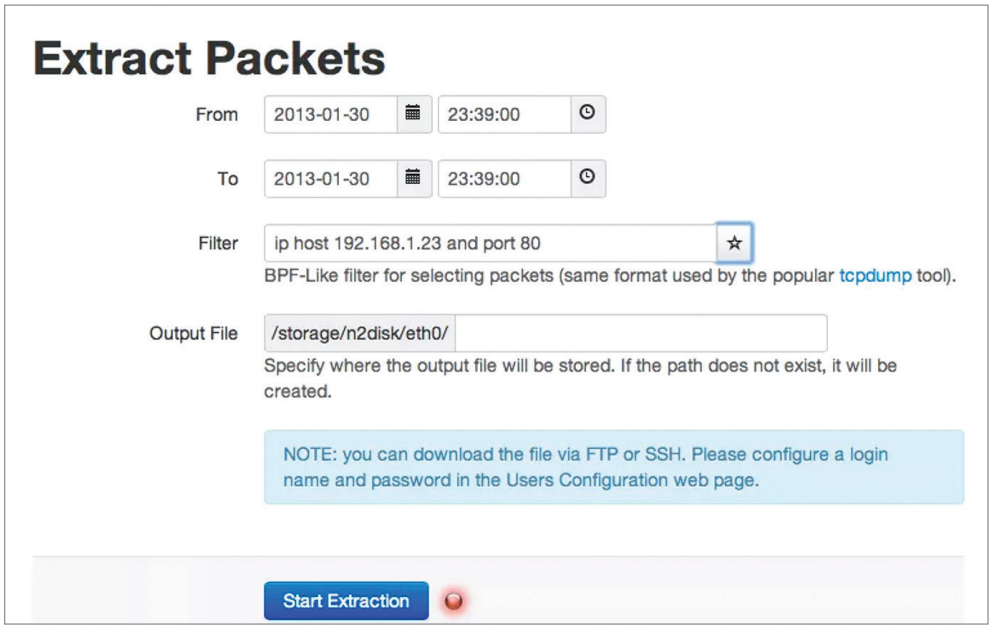
The nVoy Packet Recorder has the capacity to host multiple analysis applications sharing the same packet stream.

Real-time compression

Real-time pcap compression can be enabled upon packet capture to reduce the effective written data and extend the capture window within the same device. Certain network traffic patterns better lend themselves to compression, such as High Frequency Trading (HFT) related traffic.

Web Interface

A powerful and easy-to-use, web-based interface is provided for capture and recording configuration, system management, and packet retrieval.



The user interface simple and powerful specification of packets to be extracted based on capture time and or BPF-like filtering.

nVoy Packet Recorder Configurations

	nVoy Recorder 10 Gbit
Form Factor	2U Rackmount
Sustained Capture	Up to 14.88 Mpps
Capture ports	2 x 1/10G SFP/SFP+ but the combined bandwidth to disk is limited to 10Gb/Sec
Standard Storage Capacity	24 x 1.2 = 28.8TB
Hardware	Dual CPU with hardware RAID and Myricom ARC Series 2-port adapter
Software	10G packet capture and recording license
Timestamp Accuracy	± 50 ns
Packet extraction Filtering	Allows filtering content by IP source address, IP destination address, protocol and or application.
Management Port	RJ45 modular connector supporting up to 1 Gbit Ethernet
Additional Storage Capacity	Drives larger than 1.2 TB are available. Or add additional drive-only storage expansion boxes.
Configuration and Management	Web Interface
Warranty	3 years hardware, 1 year software maintenance

Contact Us Today: sales@ariacybersecurity.com or (978) 954-5038

ABOUT ARIA CYBERSECURITY SOLUTIONS

ARIA Cybersecurity Solutions recognizes that better, stronger, more effective cybersecurity starts with a smarter approach. Our solutions provide new ways to monitor all internal network traffic, while capturing and feeding the right data to existing security tools to improve threat detection and surgically disrupt intrusions. Customers in a range of industries rely on our solutions each and every day to accelerate incident response, automate breach detection, and protect their most critical assets and applications. With a proven track record supporting the Department of Defense and many intelligence agencies in their war on terror, and an award-winning portfolio of security solutions, ARIA Cybersecurity Solutions is committed to leading the way in cybersecurity success.

ARIA Cybersecurity Solutions • 175 Cabot St, Suite 210 • Lowell, MA O1854

Connect with Us: ariacybersecurity.com / Linkedin / Twitter / Blog

aria CYBERSECURITY SOLUTIONS ariaSDS nVoy SECURITY APPLIANCES Myricom NETWORK ADAPTERS