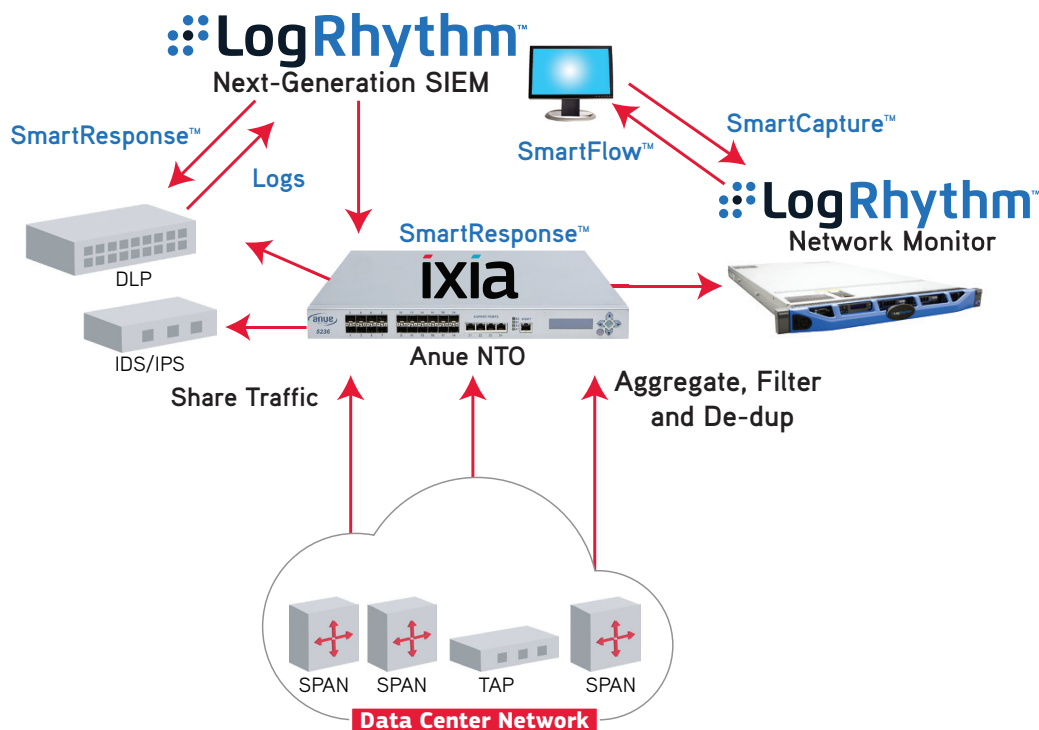




Ixia and Network Monitor from LogRhythm Combat Advanced Security Threats



Highlights

The Ixia Anue Net Tool Optimizer (NTO) provides complete access to network data feeds that LogRhythm's Network Monitor identifies, captures, and analyzes for real-time security threats. Leveraging LogRhythm's SmartCapture™ capability, the solution also delivers access to full packet data without the extensive storage requirements of traditional solutions. The Anue NTO from Ixia complements the LogRhythm Network Monitor by extending access to every network feed needed for analysis. The joint solution provides complete visibility into network traffic in a highly scalable system that is easy to deploy.

Joint Solution Benefits

- Full network visibility – Anue NTO extends access to data feeds from anywhere in the network for analysis by the LogRhythm Network Monitor, including true application identification and SmartFlow™ generation, a collection of Layer 7 metadata attributes of each network session.
- Intelligent Capture – Integrating Anue NTO with the SmartCapture™ capability of the LogRhythm Network Monitor solution allows for a rules-based selective packet capture of full network sessions for packet level analysis when necessary, without the extensive storage requirements of traditional packet recorder solutions.

- Simplified deployment – The solution is flexible enough to work in any network environment and can share access with monitoring and security tools that are already deployed.
- Easily scalable – Additional 1G, 10G, 40G, or 100G Anue NTO ports can be added to meet bandwidth requirements, and traffic can be load-balanced across multiple LogRhythm Network Monitors.
- Maximum efficiency – The Anue NTO filters and removes unneeded duplicate traffic so that the LogRhythm solution can operate at full efficiency.

Solution

The Ixia Anue Net Tool Optimizer (NTO) works in concert with the LogRhythm Network Monitor to ensure that the LogRhythm solution has access to the data it needs to provide application-level network session analysis with deep packet inspection and full packet capture. The Anue NTO passively directs out-of-band network traffic from multiple network access points – SPAN ports or TAPs – to LogRhythm Network Monitor for analysis. Traffic is aggregated from all needed access points in the network to provide comprehensive visibility and to address shortages in monitoring access points. LogRhythm's Network Monitor performs deep packet inspection, classifying applications, generating rich, searchable metadata and Layer 7 SmartFlow™, and performing SmartCapture™ to intelligently record full packet

captures for sessions relevant to high priority security threats. This integrated solution provides complete visibility into forensic security data, without the extensive storage requirements or reliance on packet-level analysis of traditional packet recording products.

LogRhythm Network Monitor Solution

True enterprise security intelligence requires real-time awareness and understanding of all data traversing your network. The LogRhythm Network Monitor provides application level (e.g. OSI layer 7) network session analysis with deep packet inspection and full session packet capture, delivering enterprise-wide visibility into all network activity. By analyzing each individual packet from every session and applying multiple recognition methodologies, Network Monitor identifies over 1,700 applications and derives a rich set of fully searchable metadata, SmartFlow™, providing extensive event context from the entire session. In addition, LogRhythm Network Monitor retains full-session packet capture in either continuous capture, or selectively with SmartCapture™, for additional forensics.

LogRhythm Network Monitor provides critical visibility for detecting and responding to today's advanced threats, enabling organizations to:

- Baseline network behavior to immediately pinpoint abnormal activity
- Detect unauthorized or suspicious application activity
- Expedite network forensic investigations
- Perform full-session packet capture for advanced packet-level analysis
- Prevent sensitive data loss
- Monitor application bandwidth consumption

The Anue NTO Efficiently Directs Traffic to Security, Network, and Application Monitoring Tools

The Anue NTO provides LogRhythm Network Monitor access to all necessary network feed data. The NTO sits between the access points in the network that require monitoring, and the LogRhythm Network Monitor. The Anue NTO aggregates traffic from multiple SPANs/TAPs in the network and directs it to any security or monitoring appliance including LogRhythm. This approach provides efficient access to asymmetric traffic across large heterogeneous networks. The Anue NTO filters out duplicate and other traffic that does not need analysis, prior to consuming resources on monitoring appliances.

The Anue NTO can share traffic from a network access point with multiple monitoring tools. This capability eliminates the common SPAN/TAP shortages that occur when another tool is attached to a needed access point. Additionally, by removing duplicate packets, the Anue NTO can enhance the throughput and storage capacity of the monitoring appliance.

Anue's intuitive control panel makes the NTO easy to set up and use. Simply drag-and-drop a virtual connection between SPANs/TAPs and tools to make a live connection.

About Ixia's Network Visibility Solutions

Ixia's Anue Net Tool Optimizer (NTO) provides complete network visibility into physical and virtual networks, improves network security and optimizes monitoring tool performance. The Anue NTO ensures that each monitoring tool gets exactly the right data needed for analysis. This improves the way you manage your data center and maximizes return on investment. Our customers include large enterprises, service providers, educational institutions and government agencies.

For additional information:

Toll Free: (877) 268-3269

EMEA: +44 (0) 1189 076 204

APAC: +852-2824-8850

Email: visibility@ixiacom.com

About LogRhythm

LogRhythm is the largest and fastest growing independent Security Information and Event Management (SIEM) provider in the world. The company's patented and award-winning Security Analytics platform and Network Monitor product empower organizations around the globe to detect breaches and the most sophisticated cyber threats of today, faster and with greater accuracy than ever before. LogRhythm also provides unparalleled compliance automation and assurance as well as IT intelligence to Global 2000 organizations, government agencies and mid-sized businesses worldwide.

For additional information:

Phone: (866) 384-0713

Email: info@logrhythm.com

Ixia Worldwide Headquarters

26601 Agoura Rd.
Calabasas, CA 91302

(Toll Free North America)

1.877.367.4942

(Outside North America)

+1.818.871.1800

(Fax) 818.871.1805

www.ixiacom.com

Ixia European Headquarters

Ixia Technologies Europe Ltd
Clarion House, Norreys Drive
Maidenhead SL6 4FL
United Kingdom

Sales +44 1628 408750

(Fax) +44 1628 639916

Ixia Asia Pacific Headquarters

21 Serangoon North Avenue 3
#04-01
Singapore 554864

Sales +65.6332.0125

Fax +65.6332.0127