TECHNICAL SOLUTIONS BRIEF

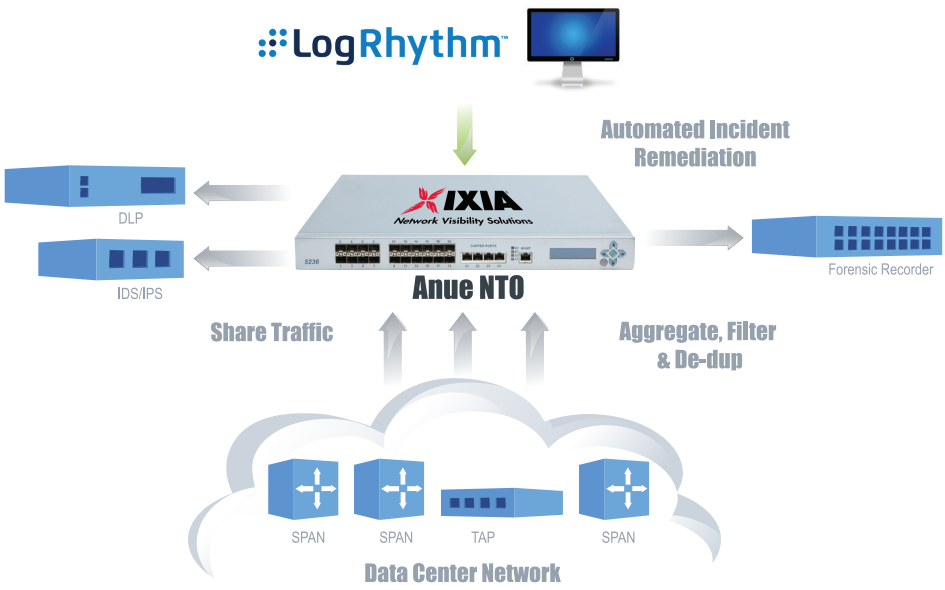
Automatically Trigger Packet Capture from LogRhythm to Accelerate Incident Remediation

The Ixia Anue Net Tool Optimizer® automates packet capture to speed root cause analysis

SOLUTION

The Ixia-Anue Net Tool Optimizer™ (NTO™) works in concert with a LogRhythm Smart**Response**™ plug-in and your security tools (forensic recorders, IPS/IDS, DLP and malware analyzers) to protect your network. The Anue NTO passively directs out-of-band network traffic from multiple access points (SPANs or TAPs) in the network to security tools for analysis. Traffic is aggregated from all necessary access points in the network to provide comprehensive visibility.

The Anue NTO's Automated Response Technology complements LogRhythm's ability to detect, analyze and respond to security threats. When an anomaly or security threat is detected in LogRhythm, a LogRhythm Smart**Response**™ plug-in can be triggered to signal the Anue NTO solution to automatically send the right traffic to a forensic recorder or other security probe. Incident remediation can begin the instant an anomaly is detected by enabling immediate capture of relevant packet-level detail or other critical information. The joint solution speeds root-cause analysis, eliminates time-consuming manual steps and simplifies compliance.



HIGHLIGHTS

Security appliances are only as useful as the data they collect. The integrated Anue Systems and LogRhythm solution automatically sends the right traffic to the right tool at the right time to ensure proper collection. By automating out-of-band traffic monitoring based on the alerting and correlation capabilities of LogRhythm, security threats can be resolved before they become problems.

JOINT SOLUTION BENEFITS

- Accelerates root cause analysis by capturing relevant packet-level detail
- Simplifies compliance reporting
- Provides security tools the right data at the right time from anywhere in the network to maximize coverage
- Eliminates time-consuming and error-prone manual processes
- Compatible with any security tool – forensic recorder, IDS/IPS, DLP, or malware analyzer
- Easy to deploy using LogRhythm's currently available Smart**Response**™ plug-in for Anue

Ixia's Network Visibility Solutions • 8310 N. Capital of Texas Highway • Building 2, Suite 300 • Austin, TX 78731
www.ixiacom.com • Email: visibility@ixiacom.com
Toll Free: (877) 268-3269 • U.S.: (512) 600-7171 • EMEA: +44 (0) 1189 076 204 • APAC: +852-2824-8850

May 2013

IXIA | Anue

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

The Anue NTO provides security and monitoring tools access to all necessary network traffic. The NTO sits between the access points in the network that require monitoring and security appliances. Simultaneously, the Anue NTO aggregates traffic from multiple SPANs/TAPs in the network and directs it to any security or monitoring appliance. This approach provides efficient access to asymmetric traffic across large heterogeneous networks. The Anue NTO filters out traffic, which 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 any security appliance or forensic recorder.

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.

LogRhythm Log Management and Security Information & Event Management

LogRhythm is an enterprise-class big data security analytics platform that seamlessly combines Log Management & SIEM 2.0, File Integrity Monitoring, and Host Activity Monitoring into a single integrated solution. It is designed to address an ever-changing landscape of threats and challenges, with a full suite of high-performance tools for security, compliance, and operations. LogRhythm delivers comprehensive, useful and actionable insight into what is really going on in and around an enterprise IT environment.

LogRhythm's SIEM 2.0 platform delivers:

- Fully Integrated Log & Event Management
- Advanced Correlation and Pattern Recognition
- File Integrity/Host Activity Monitoring
- Powerful, Rapid Forensics
- Intelligent, Process-Driven Smart**Repsonse**™
- Ease-of-use and Simplified Management

Automated Response Technology

The Anue NTO's unique Automated Response Technology allows users to efficiently monitor more of their network without requiring additional staff or budget. Automation can adjust your monitoring configuration proactively in response to changes in the network. The integrated Anue Systems and LogRhythm solution uses the technology to automatically send the right traffic to the right security tool at the right time based on triggers from LogRhythm SIEM security alerts.

Common automation applications include:

- Redirect suspicious traffic to specific monitoring tools for analysis
- Activate unused tools to distribute network monitoring bandwidth more effectively
- Prevent network tool oversubscription by automatically filtering data when network throughput crosses predetermined thresholds
- Use available Anue LogRhythm Smart**Response**™ Remediation plugin to trigger the Anue NTO and redirect network traffic to specific monitoring tools

Once automation is configured on your NTO and LogRhythm, you will have "always on" visibility into your dynamic network. So the next time network traffic spikes at 3:00AM, you can relax knowing that your NTO will take care of the early troubleshooting tactics for you.

ABOUT IXIA'S NETWORK VISIBILITY SOLUTIONS

The Ixia 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 leader in cyber threat defense, detection and response. The company's SIEM 2.0 security intelligence platform delivers the visibility, insight and response capabilities required to detect and address the mutating cyber threat landscape. LogRhythm also provides unparalleled compliance automation and assurance as well as operational intelligence to Global 2000 organizations, government agencies and MSSPs worldwide. For additional information please visit http://www.logrhythm.com