



Slash MTTR by Automatically Triggering Packet Captures from IBM Tivoli Netcool/OMNIBus

The Anue Net Tool Optimizer™ automates incident remediation to speed root cause analysis

HIGHLIGHTS

Packet based monitoring and security appliances are only as useful as the data they receive. The integrated Anue Systems' Net Tool Optimizer™ and IBM Tivoli Netcool/OMNIBus solution automatically sends the right traffic to the right packet capture appliance at the right time. By automating out-of-band monitoring traffic flow based on the alerting and correlation capabilities of IBM Tivoli Netcool, issues can be resolved before they become a problem.

JOINT SOLUTION BENEFITS

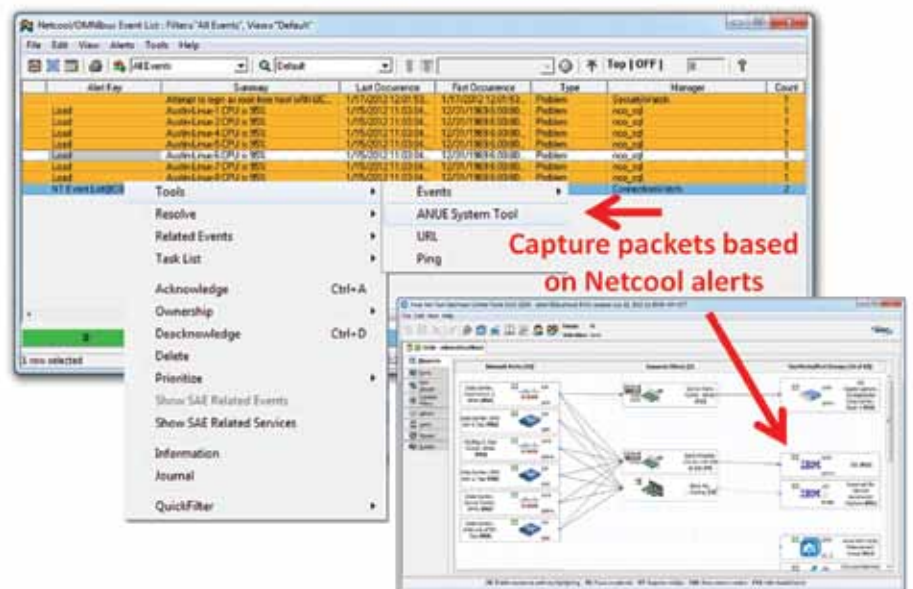
- Accelerate root cause analysis by capturing the required packets
- Simplify compliance reporting
- Provide monitoring and security tools the right data at the right time from anywhere in the network to maximize coverage
- Eliminate time consuming and error prone manual steps
- Compatible with any packet based monitoring, troubleshooting, security or recording tool.
- Easy to deploy from IBM Tivoli Netcool/OMNIBus using a right mouse click or alert triggers

SOLUTION

The Anue Net Tool Optimizer™ (NTO) works in concert with IBM Tivoli® Netcool®/OMNIBus operations management software and your packet capture tools (forensic recorders, protocol analyzers and IPS/IDS) to monitor and troubleshoot your network.

The Anue NTO passively directs out-of-band network traffic from multiple access points (SPAN ports or TAPs) in the network to packet capture tools for recording and analysis. Traffic is aggregated from all needed access points in the network to provide comprehensive visibility.

The Anue NTO's Automated Response Technology complements the IBM Tivoli Netcool/OMNIBus product's ability to detect, analyze and respond to network issues. When IBM Tivoli Netcool/OMNIBus detects an anomaly, the Anue NTO can automatically, or via a right mouse click from Netcool/OMNIBus, send the right traffic to a forensic recorder or other monitoring probe. Incident remediation can begin the instant an anomaly occurs with the benefit of having all the required packet information. The joint solution speeds root cause analysis, eliminates time consuming manual steps and simplifies compliance.



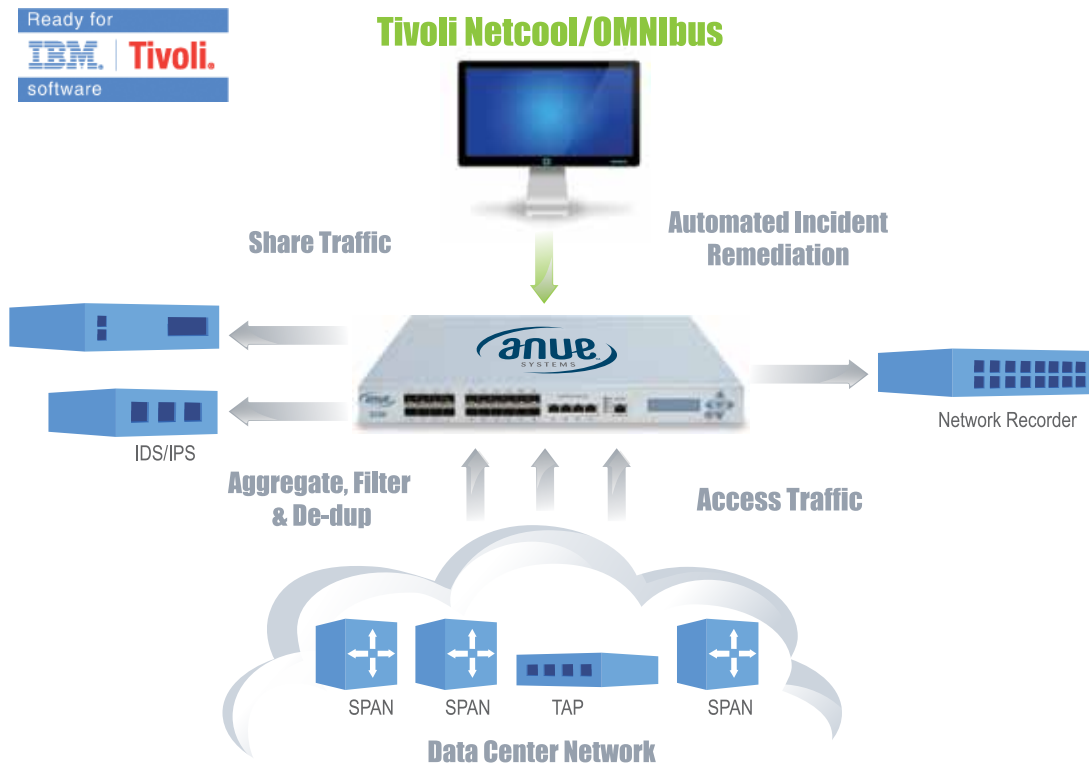


■ **THE ANUE NTO EFFICIENTLY DIRECTS TRAFFIC TO SECURITY AND APPLICATION MONITORING TOOLS**

The Anue NTO provides monitoring and security 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 SPAN ports and TAPs in the network and directs it to any 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 port and TAP shortages that occur when another tool is attached to a needed access point. Additionally, by removing duplicate packets, the Anue NTO enhances the throughput and storage capacity of any monitoring 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 SPAN ports/TAPs and tools to make a live connection.





ABOUT ANUE SYSTEMS

Anue Systems (anuesystems.com) helps network engineers and scientists monitor and test complicated networks. The Anue Systems Net Tool Optimize™ provides complete network visibility into physical and virtual networks, improves network security, and optimizes monitoring tool efficiency. The Anue patented filtering technology and industry leading, easy-to-use control panel help network engineers minimize network downtime and maximize return on monitoring tool investment. Anue's Test and Measurement division provides Network Emulation products that simulate real world conditions for the testing and deployment of large networks. Founded in 2002, Anue customers include the world's largest data centers, enterprise networks, service providers, and government agencies.

CONTACT INFORMATION

Anue Systems Inc.

8310 N. Capital of Texas Highway
Building 2, Suite 300
Austin, TX 78731

www.anuesystems.com

Email: solutions@anuesystems.com

Toll Free: (877) 268-3269

U.S.: (512) 600-7171

EMEA: +44 (0) 1189 076 204

APAC: +852-2824-8850



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' NTO and IBM Tivoli Netcool/OMNIbus solution uses the technology to automatically send the right traffic to the right packet capture tool at the right time based on triggers from IBM Tivoli Netcool/OMNIbus alerts.

Common automation applications include:

- Redirect suspicious traffic to specific monitoring tools for analysis
- Activate unused tools to effectively distribute network monitoring bandwidth
- Prevent network tool oversubscription by automatically filtering data when network throughput crosses predetermined thresholds
- Configure IBM Tivoli Netcool/OMNIbus or Security Incident and Event Management (SIEM) systems to trigger the Anue NTO and redirect network traffic to specific monitoring tools

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

OPERATIONS MANAGEMENT SOFTWARE THAT ENABLES AROUND-THE-CLOCK ADMINISTRATION AND AUTOMATION

IBM Tivoli Netcool/OMNIbus operations management software consolidates complex IT and network operation management tasks. The solution improves service availability and resiliency with real-time service management for data centers, network operations centers and IT domains.

- Delivers a central point of real-time service management for business applications, network devices, Internet protocols and security devices
- Enables you to identify and resolve the most critical problems with automated event correlation, isolation and resolution capabilities
- Consolidates data in operational silos into real-time Web dashboard views with customizable displays of events, service views and operational indicators
- Supports current and evolving standards and uses approved cryptographic providers to help ease security audits
- Utilizes customizable lightweight agents to collect business and technology events from more than 1,000 sources in real time