APPLICATION NOTE

IXIA®
Network Visibility Solutions

Maximize the Coverage and Effectiveness of Malware Analyzers with Ixia's Anue Net Tool Optimizer®

Malware, zero-day attacks and targeted advanced persistent threat (APT) attacks are pressing concerns for enterprises, service providers and governments. Advanced malware and APT solutions complement IPS/IDS and firewall solutions and provide an effective solution against advanced threats.

Unfortunately, security and network organizations are often constrained in their ability to deploy malware analyzers. Obstacles such as limited traffic access, ever increasing bandwidths, and tighter budgets may mean you are forced to monitor fewer points in the network. As a result, the traffic carrying the threat may not be analyzed.

However, there is a solution. Combining Ixia's Anue Net Tool Optimizer® (NTO) with a malware analyzer allows you to:

- **Monitor and secure more of your network**
- **Reduce the time to detect and address security issues**

This scalable joint solution captures and analyzes network traffic to accurately and efficiently monitor networks of any size. The Anue NTO passively directs traffic from multiple access points – SPANs or TAPs - in the network to the malware detectors for analysis. Traffic is aggregated from all needed access points in the network to provide comprehensive visibility.

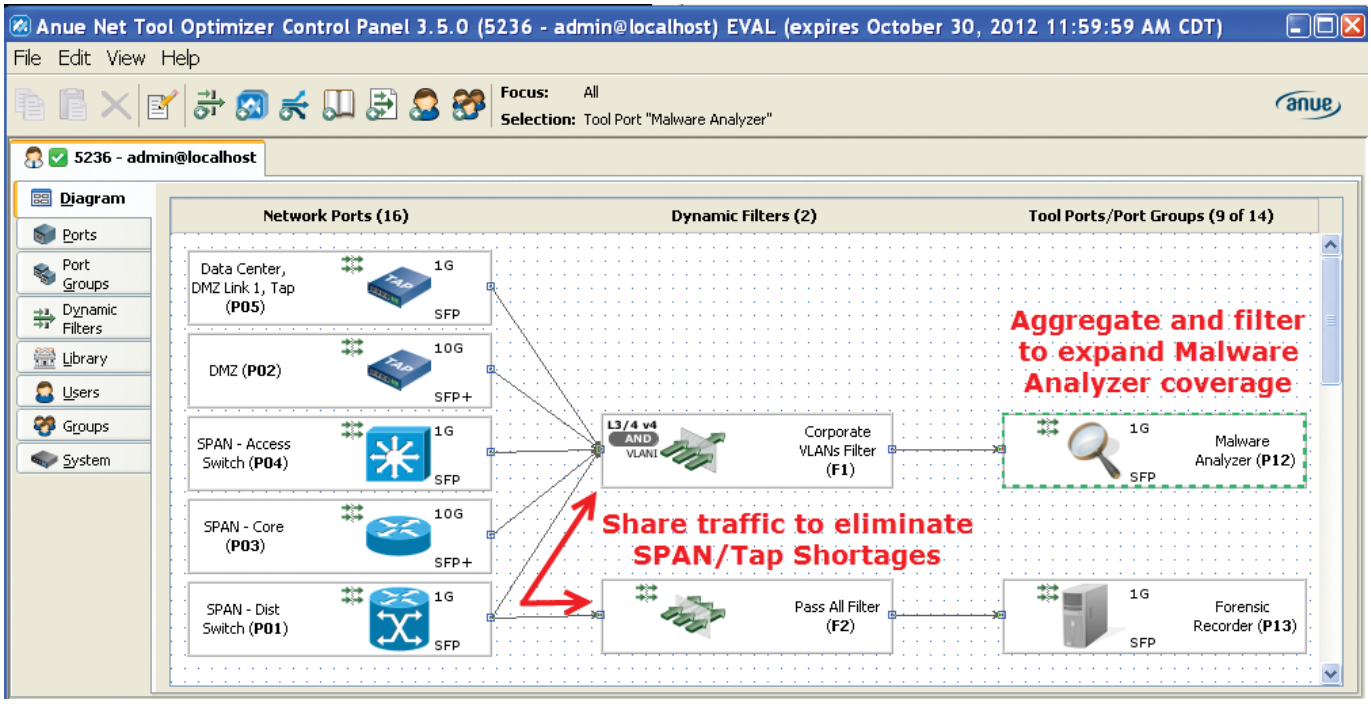

FIGURE 1: The Anue NTO's drag-and-drop control panel is used to direct traffic to the malware analyzer. In this example, the analyzer is monitoring five links in an asymmetric network. Traffic is being filtered so that the 1G analyzer can monitor 23G of traffic. The distribution switch SPAN traffic is being shared with the analyzer and a forensic recorder.

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

September 2012 Document No. 915-6544-01

IXIA®
Network Visibility Solutions

Monitor and Secure More of Your Network

Combining a malware analyzer with the Anue NTO allows more of your network to be monitored and secured. This is achieved in four ways.

Aggregate and Load Balance to Increase Visibility

The Anue NTO aggregates and load balances across multiple points in your network. Since many links run only at a fraction of their total bandwidth the majority of the time, they can be aggregated into a single input on a malware analyzer. If traffic exceeds the capacity of a single malware analyzer, the NTO's load balancing capability allows traffic to be distributed evenly across multiple detector input ports, or even multiple malware analyzer appliances, while keeping sessions intact and maximizing usage of the analyzers.

Filter and De-Duplicate to Monitor High Bandwidths

Users have the option to selectively filter what traffic is sent to the malware analyzer or slice all or a portion of the payload. For example, the NTO can provide only TCP/IP information, or filter on critical protocols or conversations. Filtering also allows a 1G analyzer to monitor one or more 10G links. In addition, duplicate packets can be removed to maximize the usage of the malware analyzers' throughput capacity. Since 50-80 percent of traffic from a normally configured SPAN port is unneeded duplicate packets, this significantly increases capacity of the analyzer.

Share Limited SPAN/TAP Ports to Provide Access

The Anue NTO allows traffic from a network access point to be shared with multiple monitoring tools. This eliminates the SPAN/TAP shortages that can commonly occur when the malware appliance is prevented from getting access to needed traffic because another tool is already attached to a needed access point.

Use Alerts from Your SIEM to Automate Malware Analysis

The Anue NTO allows malware analyzers to dynamically connect to different locations in the network based on when and where threats are detected. By setting specific triggers on protocols or events, the NTO will connect the analyzer to the traffic stream only when specific events occur. This automatic monitoring reconfiguration can be changed quickly and easily by the user if a new problem or threat emerges. Triggers to send traffic to the malware analyzer can be based on a wide range of sources including events detected by Security Incident and Event Management (SIEM) products or network management system alerts.

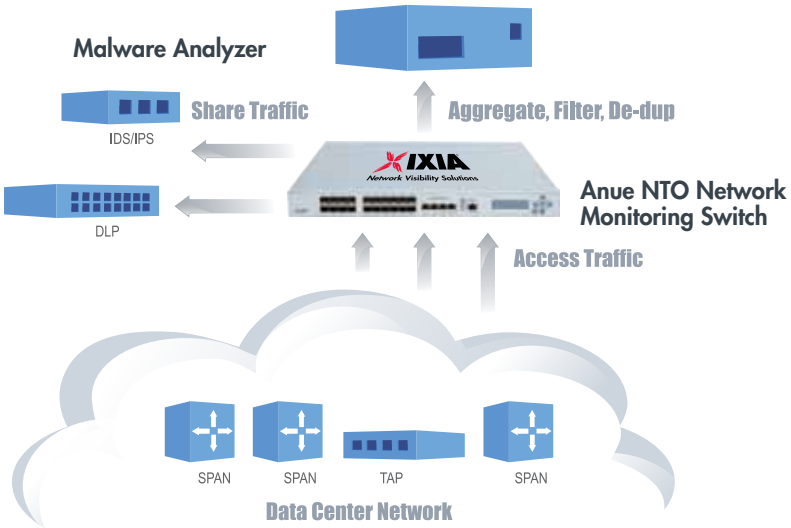

FIGURE 2: The Anue NTO sits between SPAN/TAP ports in the network and the malware analyzer. Out-of-band traffic is passively aggregated, filtered, de-duplicated and shared to provide the analyzer complete visibility.

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

September 2012 Document No. 915-6544-01

IXIA®
Network Visibility Solutions

Reduce the Time to Detect and Resolve Security Issues

Speed is critical to the success of detecting and resolving threats. The joint Anue NTO and malware analyzer solution reduces time to resolution in three ways.

Quickly Get Your Analyzer the Data it Needs

The straightforward control panel of the Anue NTO lets you tap into the traffic you need quickly, without digging into your network diagrams and navigating a complex command line interface. This system also greatly reduces the risk that you'll accidentally stop traffic flow to or stop monitoring a key device in the network. Better yet, the Anue NTO can be automatically directed by your SIEM to send traffic from any location in your network to the malware analyzer.

Avoid Lengthy Change Control Delays

In some cases, you need to monitor the same port that is being used by another piece of network monitoring gear, such as protocol analyzer. The Anue NTO allows you to do that with a few mouse clicks - without interfering with the protocol analyzer's data stream. Getting the packets you need without working out some sort of arrangement with the networking team or waiting for a change control window could save hours and mean the difference in detecting and stopping a threat. The Anue NTO's access control ensures that access to tools and traffic adheres to company policies.

Automatically Trigger Forensic Recorder Packet Captures

It is often helpful to capture and analyze all the packets associated with a threat when troubleshooting. The problem is that most companies do not have enough forensic recorders to capture packets at every point in the network. And it always seems that the threat occurs in the locations that you do not have a recorder deployed. The Anue NTO's can automatically connect a forensic recorder to the right location in the network and only capture the packets associated with the threat based on an alert from a SIEM or malware analyzer.

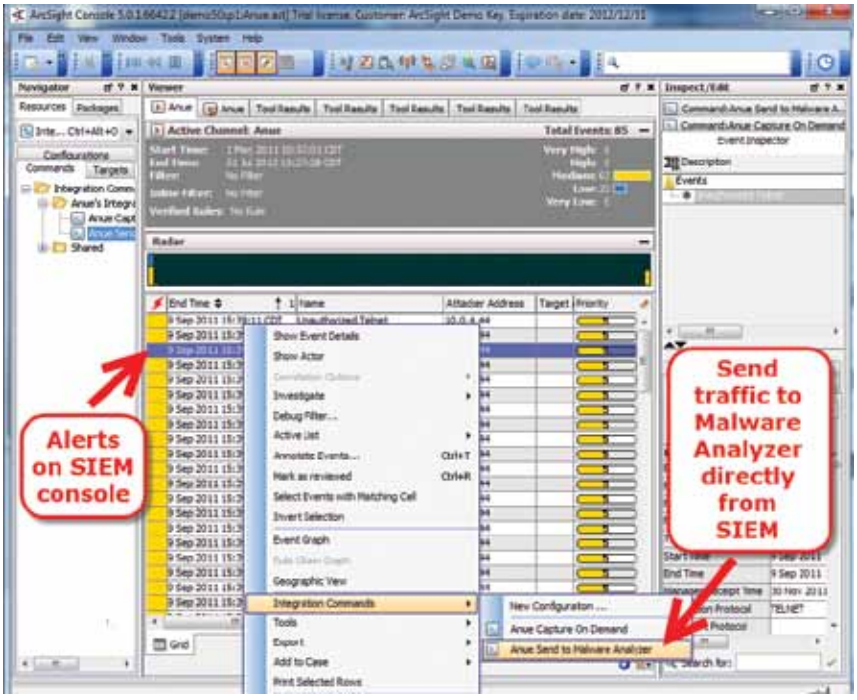

FIGURE 3: The Anue NTO's automation capability allows traffic relating to a specific alert to be sent to a malware analyzer directly from a Security Incident and Event Management (SIEM) console or an automated SIEM alert trigger. This allows the malware analyzer to always be connected to the right location in the network.

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

September 2012 Document No. 915-6544-01