Technical Note:
Integrating IXIA Network Visibility Solutions (NVS) with IBM QRadar SIEM

Using Ixia NVS Automation API

Table of Contents
Overview 1
Integration Pre-Requisites 2
Test the Integration 3
Appendix A – IBM QRadar Right-Click Menu Customization 5
Appendix B – Ixia Integration Script Editing 6

IXIA Network Visibility Solutions

This material is for informational purposes only and subject to change without notice. It describes Ixia’s present plans to develop and make available to its customers certain products, features and functionality. Ixia is only obligated to provide those deliverables specifically included in a written agreement between Ixia and the customer. © Keysight Technologies, 2017
Integration Guide for IBM QRadar

Overview

Ixia Network Visibility Solutions (NVS) work in concert with IBM Security QRadar SIEM (Security Information and Event Management) and Packet Recorder/Analysis tools to better troubleshoot security issues. The Ixia Net Tool Optimizer (NTO) passively directs out-of-band network traffic from multiple access points (SPANs or TAPs) in the network to monitoring tools for analysis. Traffic is aggregated from all needed access points in the network to provide comprehensive visibility. Ixia NVS’s Automated Response Technology complements IBM QRadar’s ability to detect, analyze and respond to security events. When QRadar detects an event or creates an event as a result of correlating events, the Ixia NTO unit can automatically send the right traffic to a packet recorder/analyzer or other tool.

Remediation can begin the instant an issue occurs with the benefit of having all the required packet information. Some example use cases include; investigation of Rogue IP, DOS analysis, troubleshooting of specific host, and investigating traffic behavior. The joint solution speeds root-cause analysis, eliminates time consuming manual steps, and simplifies compliance.

This document describes the methodology for integrating Ixia NTO with IBM QRadar SIEM, providing an example integration scenario from our testing environment. The Guide is meant to assist customers with Ixia – QRadar Integration options

(Expertise in IBM QRadar and Ixia NTO is required to complete the integration setup)

ASIDE: Contact Greg Copeland for further guidance and assistance with integration – gcopeland@ixiacom.com
Integration Pre-Requisites

- Ixia NTO version 3.9 or newer is installed, configured, and connected to Network and Tool ports (see Ixia documentation)
  o Make note of the following; the IP address of the NTO, username/password for NTO, Names of NTO Network & Tool Ports that you wish to integrate with
- IBM QRadar SIEM version 7.2 MR1 or newer is installed and is configured with data sources to monitor security events (see IBM QRadar documentation)
- It is assumed there is a Packet Analyzer connected to the NTO Tool Port which you are using for this integration.
- Edit /opt/qradar/conf/arielRightClick.properties on QRadar server to include Ixia menus
  o see Appendix A for further details
- Obtain the following Ixia Integration perl scripts and place them on IBM QRadar SIEM Console (PATH shown is default integration directory created in our demo environment, PATH in customer environment may vary)
  /opt/anue/createIpFilter.pl
  /opt/anue/deleteIpFilter.pl
  o contact gcopeland@ixiacom.com for samples of the integration files
- Edit the Ixia Integration files to work specific to the customer environment
  o see Appendix B for further details

Integration Background:
  o The Integration makes calls from the QRadar SIEM, to the Ixia NTO’s RESTful WebAPI
  o The WebAPI calls are wrapped in Perl scripts, Perl comes included with the QRadar install file and is installed by default in /usr/bin directory
  o The scripts make use of the following Perl modules, which are also included by default in the QRadar install; JSON::Syck; Data::Dumper, strict
  o It is assumed the defaults for Perl have been left unchanged

Notes:

Since differences will exist in Customer’s IBM QRadar / Ixia NTO environment, it is recommended to test in QA environment before putting into production. See also Ixia NTO Guide, Ixia NTO Web API User Guide & IBM QRadar Documentation – Note: Full instruction on QRadar is beyond the scope of this document; consult a QRadar Subject Matter Expert for further assistance
Test the Integration

- Launch the Ixia NTO (formerly known as Anue NTO) GUI Interface and login with appropriate credentials (note: do not log in with the same user account specified in your perl scripts)
- Click the Diagram Tab

**Usage Scenario – Ixia NTO filters packets, related to selected QRadar Event, by IP Address and forwards those packets to an analyzer for further investigation**

The Integration instructs the Ixia NTO to automatically create connection(s) from the Network to the Monitoring Tool (in this example a Packet Analyzer). A filter is automatically applied so that only Packets for the IP Address specified in the right-clicked QRadar SIEM event are forwarded from the network to the monitoring tool.

- Here is an example of the Ixia NTO configuration Before Integration is triggered, i.e.no packets are being sent to the waiting Packet Analyzer (in our demo system this analyzer is named QRadar-Packets)

- Launch the QRadar web interface and login with appropriate admin user credentials
  - Click the Log Activity Tab
  - Select an Event from list for which you are interested in capturing relevant packets
  - Right Click the Source IP or Destination IP field of the Event
  - Choose the “Plugin Options” menu item
    - then choose the “Create Ixia IP Filter” item
      (see next page)
Return to the Ixia NTO GUI and note response to the Right-Click
- IBM QRadar Right Click triggers the Ixia NTO (traffic for this IP is filtered and automatically forwarded from the Network Ports which you specified in the integration script, to the QRadar-Packets analyzer tool also specified in the integration script)

QRadar will also generate an acknowledgment of the Packet Capture filtering

There is now a packet trail available on the Packet Analyzer related to the right-clicked QRadar event(s). Root cause analysis of the packet data related to the QRadar Security Event can begin immediately.
- The filtered packet capture can be left in place for as long as needed to conduct root cause analysis on the security issue. When finished, delete the Ixia NTO filter as follows:
  - From IBM QRadar Log Activity, return to the event used earlier to create the Filter
  - **Right Click** the Source IP or Destination IP address (the same address as used to create the Filter before)
  - Choose the “Plug-In Options” menu item
    - then choose the “Delete Ixia IP Filter” item
  - Returning to the Ixia NTO Diagram you will observe the IP Filter has been removed, and packets are no longer being forwarded to the QRadar-Packets Analyzer
  - QRadar will also generate an acknowledgement of the NTO Filter removal

Appendix A – IBM QRadar Right-Click Menu Customization
A. using SSH, log into IBM QRadar as the root user:
   - username: root
   - password: <password>

B. edit (or if it doesn’t exist create it) arielRightClick.properties file in the /opt/qradar/conf directory on the QRadar SIEM server.

C. using a text editor add the following lines to customize the right-click menu in QRadar (/opt/anue/ PATH assumes directories specified in the pre-requisites section were used)

D. save your edited arielRightClick.properties file to /opt/qradar/conf directory

E. from the SSH shell - restart the web services in QRadar
   - service tomcat restart

Appendix B – Ixia Integration Script Editing

Open the /opt/anue/createlpFilter.pl script with text editor, and you will need to edit as follows:

1. Replace value for $ipAddress to match that of the Ixia NTO you are integrating with
2. Replace values $userID and $passwd with valid credentials for the Ixia NTO unit you are integrating with *(note: do not use the same account used for Ixia NTO GUI access)*
   - *Note: credentials will be passed over the wire within HTTPS*
3. Replace values for @networkPortNames to match those on the NTO you are integrating with. These are the physical ports connected to the relevant SPAN and TAPs in your network
   - Note: all Names in the script must match port names from the NTO exactly, and are case sensitive
   - Note: be sure to leave the comma off the last entry in the array
4. Replace value for @toolPortNames to match that of NTO you are integrating with, this is the physical port which your Packet Analyzer is connected to.
   - Note: the Name in the script must match the port name in the NTO exactly, and is case sensitive
   - Note: don’t put a comma after the tool port entry

5. *save your edited createlpFilter.pl file to /opt/anue directory*

Open the /opt/anue/deletelpFilter.pl script with text editor, and you will need to edit as follows:

1. Replace value for $ipAddress to match that of the Ixia NTO you are integrating with
2. Replace values $userID and $passwd with valid credentials for the Ixia NTO unit you are integrating with *(note: do not use the same account used for Ixia NTO GUI access)*
   - *Note: credentials will be passed over the wire within HTTPS*
3. save your edited `deletelpFilter.pl` file to `/opt/anue` directory