Introduction

Overview

NetFlow Logic Network Metrics Content Pack for VMware vRealize Log Insight is designed to deliver next generation, real-time, network resource management power to network and security analysts. NetFlow Optimizer™ (“NFO”) is a middleware that processes massive amount of flows to stream summarized and meaningful syslog events into vR Log Insight. The events are available for immediate indexing and correlation. NetFlow Logic Network Metrics Content Pack provides visualization and reporting capabilities. The operators benefit from detailed visibility to their entire network and being able to address many IT use cases including bandwidth monitoring, capacity planning, congestion troubleshooting, and cyber security using threat intelligence lists.

This manual is intended for network and security analysts who use the Content Pack to monitor and investigate problems. For additional NFO information please visit www.netflowlogic.com.

Dashboards

Dashboard: Select Device >

This dashboard relies on syslog messages generated by the following NFO Module packaged in Network Traffic and Devices Monitor Module Set:

- 10067: Top Traffic Monitor

This Module is enabled by default when you install NFO.

Top Devices by Traffic

Displays network devices with most traffic in your network. It is useful for real time or historical network utilization and bandwidth monitoring.

The “Select Device >” dashboard consists from one widget, which allows to select a device and look at network traffic details for this particular device. To do this you need to right-click on a device (a bar) in the widget and the pop-up menu will appear. Please select “Other Dashboard >” and a target dashboard name in the sub-menu. You will get Traffic Monitoring, Visitors by Country, or Virtual to Physical Analytics for the selected device.
Dashboard: Traffic Monitoring

This dashboard relies on syslog messages generated by NFO Module “10067: Top Traffic Monitor”.

This dashboard has the following widgets.

**Top Traffic by Source IP**

**Top Traffic by Destination IP**
Top Traffic by Protocol

Top Traffic by Port by Protocol

Top In-interfaces by Traffic

Top Out-interfaces by Traffic
Dashboard: Visitors by Country

This dashboard relies on syslog messages generated by NFO Module “10040: Visitors by country”. Make sure this Module is enabled and configured to see data in this dashboard.

Egress traffic by country

Ingress traffic by country
Egress traffic bytes by country

Ingress traffic bytes by country

Egress traffic flow_count by country

Ingress traffic flow_count by country
Dashboard: Cyber Threat Statistic

This dashboard relies on syslog messages generated by the following NFO Modules packaged in Security Module Set:

- 10053: Threat Feeds Traffic Monitor
- 10050: Botnet C&C Traffic Monitor
- 10052: Host Reputation Monitor (shown in Malicious Hosts widgets)

Make sure these Modules are enabled and configured to see data in this dashboard.

Threat Feeds

This widget shows traffic to and from IP addresses found in the known threat lists:

- [http://www.dshield.org/feeds/suspiciousdomains_High.txt](http://www.dshield.org/feeds/suspiciousdomains_High.txt)
- [http://feeds.dshield.org/block.txt](http://feeds.dshield.org/block.txt)
**Threat Feeds – details**

<table>
<thead>
<tr>
<th>timestamp</th>
<th>nfi_src_ip</th>
<th>nfi_flow_count</th>
<th>nfi_exp_ip</th>
<th>nfi_dest_port</th>
<th>nfi_dest_ip</th>
<th>nfi_bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-10-23</td>
<td>16.8.5.7</td>
<td>1</td>
<td>16.8.5.34</td>
<td>58165</td>
<td>58.169.78.38</td>
<td>772</td>
</tr>
<tr>
<td>2015-10-22</td>
<td>58.169.78.38</td>
<td>2</td>
<td>16.8.5.34</td>
<td>22</td>
<td>16.8.5.7</td>
<td>148</td>
</tr>
<tr>
<td>2015-10-22</td>
<td>16.8.5.7</td>
<td>1</td>
<td>16.8.5.24</td>
<td>48005</td>
<td>58.169.78.38</td>
<td>772</td>
</tr>
<tr>
<td>2015-10-22</td>
<td>58.169.78.38</td>
<td>4</td>
<td>16.8.5.24</td>
<td>22</td>
<td>16.8.5.7</td>
<td>312</td>
</tr>
<tr>
<td>2015-10-22</td>
<td>16.8.5.7</td>
<td>1</td>
<td>16.8.5.24</td>
<td>54813</td>
<td>58.169.78.38</td>
<td>93</td>
</tr>
<tr>
<td>2015-10-22</td>
<td>58.169.78.38</td>
<td>1</td>
<td>16.8.5.24</td>
<td>53559</td>
<td>58.169.78.38</td>
<td>61</td>
</tr>
</tbody>
</table>

View more results in Interactive Analytics.

**Botnet Command & Control (Emergingthreats.net)**

This widget shows traffic to and from IP addresses found in the known threat list:


**Malicious Hosts (AlienVault Reputation)**

This widget shows traffic to and from IP addresses found in the known threat list:


**Malicious Hosts (AlienVault Reputation) – details**

<table>
<thead>
<tr>
<th>timestamp</th>
<th>nfi_src_ip</th>
<th>nfi_flow_count</th>
<th>nfi_exp_ip</th>
<th>nfi_dest_port</th>
<th>nfi_dest_ip</th>
<th>nfi_bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-12-02</td>
<td>117.27.159.70</td>
<td>1</td>
<td>10.0.5.24</td>
<td>22</td>
<td>18.0.5.7</td>
<td>150</td>
</tr>
<tr>
<td>2014-12-02</td>
<td>10.0.5.7</td>
<td>2</td>
<td>10.0.5.24</td>
<td>14802</td>
<td>122.225.195.200</td>
<td>154</td>
</tr>
<tr>
<td>2014-12-02</td>
<td>122.225.195.200</td>
<td>1</td>
<td>10.0.5.24</td>
<td>22</td>
<td>18.0.5.7</td>
<td>150</td>
</tr>
<tr>
<td>2014-12-02</td>
<td>10.0.5.7</td>
<td>1</td>
<td>10.0.5.24</td>
<td>58100</td>
<td>122.225.195.200</td>
<td>52</td>
</tr>
<tr>
<td>2014-12-02</td>
<td>10.0.5.7</td>
<td>3</td>
<td>10.0.5.24</td>
<td>46883</td>
<td>62.259.53.52</td>
<td>238</td>
</tr>
</tbody>
</table>

View more results in Interactive Analytics.
Dashboard: Virtual to Physical Analytics

This dashboard relies on syslog messages generated by the following NFO Modules packaged in VMware Module Set:

- 10164: Top Host:VM Pairs Monitor
- 10167: Top VM:Host Traffic Monitor

Total traffic by VXLAN

This chart shows total traffic in bytes by each observed VXLAN ID.
Traffic by VXLAN over time

This chart shows traffic over time in bytes by each observed VXLAN ID over time.

Top VM Host pairs traffic on same hosts
This chart shows total traffic in bytes of the top VM pairs residing on the same hosts.

VM pair is defined as:
Client VM = nfi_vm_src_ip
Client host = nfi_host_src_ip

Server VM = nfi_vm_dest_ip
Server host = nfi_host_dest_ip

Top VM Host pairs traffic on different hosts

This chart shows total traffic in bytes of the top VM pairs residing on different hosts.

VM pair is defined as:
Client VM = nfi_vm_src_ip
Client host = nfi_host_src_ip

Server VM = nfi_vm_dest_ip
Server host = nfi_host_dest_ip
Top VM Host pairs traffic combined

This chart shows traffic over time in bytes by each observed VXLAN ID over time.

Top VM talkers by host

This chart shows top VM talkers by host.

VM is identified by nfi_vm_src_ip
Host is identified by nfi_host_src_ip

Top VM listeners by host

This chart shows top VM listeners by host.
VM is identified by \texttt{nfi\_vm\_dest\_ip}
Host is identified by \texttt{nfi\_host\_dest\_ip}

**Top VM talkers by VXLAN**

This chart shows top VM talkers by VXLAN.

VM is identified by \texttt{nfi\_vm\_src\_ip}

**Top VM listeners by VXLAN**

This chart shows top VM listeners by VXLAN.

VM is identified by \texttt{nfi\_vm\_dest\_ip}
Dashboard: Host Pairs

This dashboard relies on syslog messages generated by the following NFO Module packaged in Network Traffic and Devices Monitor Module Set:

- 10164: Top Host:VM Pairs Monitor
Resources

Getting help

NetFlow Logic Support:
https://www.netflowlogic.com/connect/support/