NetFlow:
Troubleshooting
Network & Security Problems
with Flows

Presented by Christina Klam at NJEDge Conference 2016. 2016-11-18
NetFlow

- Developed and patented at Cisco® Systems in 1996
- NetFlow is now the primary network accounting technology in the industry
- Answers questions regarding IP traffic: who, what, where, when, and how
- Provides a detailed view of network behavior
- Insight into the network without minimizing the need for DPI (Deep Packet Inspection)
NetFlow

De-facto term although flow data comes in other forms:

Juniper® (Jflow)

3Com/HP® , Dell® , and Netgear® (s-flow)

Huawei® (NetStream)

Alcatel-Lucent® (Cflow)

Ericsson® (Rflow)
Flow Record Creation

Flow-cache (inactive)
Flow Record Creation

If only INACTIVE flows are sent

AND

Active Flow-cache default timeout = 30 min

Does this mean you have to wait 30 minutes to see traffic from an active connection???
Flow Record Creation

Change the timeout value to 1 minute (v5) or 1 second (v9+)

`ip flow-cache timeout active 1`

* If this is a busy router, change it to something less frequent.
<table>
<thead>
<tr>
<th>NetFlow Version</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Original</td>
</tr>
<tr>
<td>5</td>
<td>Standard and most common</td>
</tr>
<tr>
<td>7</td>
<td>Specific to Cisco Catalyst 6500 and 7600 Series Switches</td>
</tr>
<tr>
<td></td>
<td>Similar to Version 5, but does not include AS, interface, TCP Flag &amp; TOS information</td>
</tr>
<tr>
<td>8</td>
<td>Choice of eleven aggregation schemes</td>
</tr>
<tr>
<td></td>
<td>Reduces resource usage</td>
</tr>
<tr>
<td>9</td>
<td>Flexible, extensible file export format to enable easier support of additional fields &amp; technologies; coming out now MPLS, Multicast, &amp; BGP Next Hop</td>
</tr>
</tbody>
</table>
Version 5

Static set of fields or tuples
Version 5: Ingress Only
Version 9

● Version 5 fields + ...

● Up to a total of 128 fields

  ○ Type of service (ToS)

  ○ Packet and byte counts

  ○ Start and end timestamps

  ○ Layer 2: VLANs, mac addresses

  ○ Application

  ○ Routing information (MPLS, next-hop address, source autonomous system (AS) number, destination AS number, source prefix mask, destination prefix mask)
Version 9: Ingress & Egress
Version 9

Dynamic set of fields

Template
Fields being sent
Flow Exporter Scrutinizer:

Client: Flow Monitor IPV4-FLOW
Exporter Format: IPFIX (Version 10)
Template ID : 256
Source ID : 22
Record Size : 38

Template layout

<table>
<thead>
<tr>
<th>Field</th>
<th>ID</th>
<th>Ent.ID</th>
<th>Offset</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4 source address</td>
<td>8</td>
<td></td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>ipv4 destination address</td>
<td>12</td>
<td></td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>transport source-port</td>
<td>7</td>
<td></td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>transport destination-port</td>
<td>11</td>
<td></td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>ip tos</td>
<td>5</td>
<td></td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>ip protocol</td>
<td>4</td>
<td></td>
<td>13</td>
<td>1</td>
</tr>
<tr>
<td>interface input snmp</td>
<td>10</td>
<td></td>
<td>14</td>
<td>4</td>
</tr>
<tr>
<td>interface output snmp</td>
<td>14</td>
<td></td>
<td>18</td>
<td>4</td>
</tr>
<tr>
<td>counter bytes long</td>
<td>1</td>
<td></td>
<td>22</td>
<td>8</td>
</tr>
<tr>
<td>counter packets long</td>
<td>2</td>
<td></td>
<td>30</td>
<td>8</td>
</tr>
</tbody>
</table>
Client: Option options application-name
Exporter Format: NetFlow Version 9
Template ID : 258
Source ID : 22
Record Size : 87
Template layout

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Offset</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>v9-scope system</td>
<td>1</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>application id</td>
<td>95</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>application name</td>
<td>96</td>
<td>8</td>
<td>24</td>
</tr>
<tr>
<td>application description</td>
<td>94</td>
<td>32</td>
<td>55</td>
</tr>
</tbody>
</table>
IPFIX: Vendor Templates

- Not flow technology.
- IANA standard for both sflow and netflow flow technology.
- Allows for variable length fields that can be used for URLs, messages, etc.
- Like with flexible v9, the templates allows for specifying just the information you need.
  - Templates are sent by router every 20 packets
  - Templates explains the info being sent
If Netflow and SNMP had a baby

- Push technology like snmptrap and syslog
- Allows for unique elements across vendors.
- Each vendor has an unique enterprise number -- usually same used in SNMP.
- Like SNMP MIBS without the need for compiling and uses less bandwidth.

IPFIX
IPFIX Templates: AVC & NBAR

- Applications Downstream
- Applications Upstream
- Applications by Wireless Host
- Applications by Wireless Host with DSCP
- Clients per AP
- Clients per SSID
- Hosts by SSID
- Hosts with MAC
- Hosts with User Name
- SSID List
- Usage by SSID and AP
- User and Controller Details

<table>
<thead>
<tr>
<th>Application</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1   ssl (Type: 13 ID: 453)</td>
<td></td>
</tr>
<tr>
<td>2   youtube (Type: 13 ID: 82)</td>
<td></td>
</tr>
<tr>
<td>3   video-over-http (Type: 13 ID:...</td>
<td></td>
</tr>
<tr>
<td>4   binary-over-http (Type: 13 ID:...</td>
<td></td>
</tr>
<tr>
<td>5   secure-http (Type: 3 ID: 443)</td>
<td></td>
</tr>
<tr>
<td>6   internet-video-streaming (Typ...</td>
<td></td>
</tr>
<tr>
<td>7   http (Type: 3 ID: 80)</td>
<td></td>
</tr>
<tr>
<td>8   dns (Type: 3 ID: 53)</td>
<td></td>
</tr>
<tr>
<td>9   unknown (Type: 13 ID: 1)</td>
<td></td>
</tr>
<tr>
<td>10  rtsp (Type: 3 ID: 554)</td>
<td></td>
</tr>
</tbody>
</table>
Resource Impact

● As most vendors are moving v9 & IPFIX to silicon, there is a much smaller hit to the CPU.
  ○ For vendors who do the flow via software, they may be sticking with sFlow

● Exporting NBAR instead of source and destination can reduce the number of flows as well. With NBAR alone, you lose the source and destination if the flow is not also coming from somewhere else.
NBAR only Topology

Src/Dst

NBAR only

Src/Dst
3 Ingredients for Configuration

Record

Monitor

Export
Flow Record: Layer3+

match ipv4 source address
match ipv4 destination address
match ip protocol
match ip tos
match transport source-port
match transport destination-port
match interface input
match interface output
match flow direction
collect routing source as
collect routing destination as
collect routing next-hop address ipv4
collect transport tcp flags
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
Flow Record: Layer 2

- Source and destination MAC addresses
- Source VLAN ID
- EtherType from the Ethernet frame

Apply to INGRESS interfaces:
1. Switch ports in access mode
2. Switch ports in trunk mode
3. Layer 2 port channels

Cannot be applied to VLANs, egress interfaces, or Layer 3 interfaces such as VLAN interfaces.
Flow Export

- Netflow Version {5,9,IPFIX}
- IP of the collector
- Protocol (UDP or SCTP)
- Port Number
- Source interface
- DSCP
Flow Export

Cisco and others tend to use UDP: NetFlow is UDP port 2055, but other ports like 9555 or 9995, 9025, and 9026 can also be used. UDP port 4739 is the default port used by IPFIX.
IPFIX prefers Stream Control Transmission Protocol (SCTP) as its transport protocol.

SCTP is a transport level protocol. “...[i]t is message-oriented like UDP and ensures reliable, in-sequence transport of messages with congestion control like TCP; it differs from these in providing multi-homing and redundant paths to increase resilience and reliability.”
Flow Monitor
Flow Monitor

Examples of some Neflow collectors

- Plixar Scrutinizer
- NFSEN
- NTOP
- Cisco Stealthwatch
- CFLOW
- PRTG
- Arbor Peakflow
Flow Monitor

Criteria for selecting a netflow collectors

- Can it read the v9/ipfix templates?
- Can it read NBAR?
- Cost
- Ease of searching and reporting
Apply it to an interface
IF YOU WALK ON SNOW
YOU CANNOT HIDE YOUR FOOTPRINTS

GEORGE HERBERT

PICTUREQUOTES.com
Netflow Give OSI Layer Visibility

Layer 1: Interface and Traffic flow by bit/bytes/packets

Layer 2: MAC Address

Layer 3: Source & Destination IP

Layer 4 & 5: Protocol (TCP, UDP, ICMP) & Port Number

Layer 6 & 7: NBAR/Application/URLs
Netflow: Top Destinations

![Netflow Graph]

**Inbound Results**

<table>
<thead>
<tr>
<th>Source</th>
<th>Percent</th>
<th>Bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>cistar_vmmfs.itg.ias.edu</td>
<td>47.55%</td>
<td>1.012 Gb/s</td>
</tr>
<tr>
<td>fas_svm2_vmmfs.sns.ias.edu</td>
<td>6.73%</td>
<td>143.260 Mb/s</td>
</tr>
<tr>
<td>fas_svm1.ias.edu</td>
<td>3.49%</td>
<td>74.318 Mb/s</td>
</tr>
<tr>
<td>oceanrvb_vmmfs.itg.ias.edu</td>
<td>3.24%</td>
<td>68.911 Mb/s</td>
</tr>
<tr>
<td>wc1.net.ias.edu</td>
<td>3.18%</td>
<td>67.714 Mb/s</td>
</tr>
<tr>
<td>fas_svm2_vmmfs.ias.edu</td>
<td>2.10%</td>
<td>44.637 Mb/s</td>
</tr>
<tr>
<td>vc1_vmmf_sns.ias.edu</td>
<td>1.60%</td>
<td>34.096 Mb/s</td>
</tr>
<tr>
<td>fas_svm2_av.sns.ias.edu</td>
<td>1.56%</td>
<td>33.226 Mb/s</td>
</tr>
<tr>
<td>fas_node1_rep.sv.sns.ias.edu</td>
<td>1.07%</td>
<td>22.747 Mb/s</td>
</tr>
<tr>
<td>130.156.232.210</td>
<td>1.05%</td>
<td>23.421 Mb/s</td>
</tr>
<tr>
<td><strong>Other</strong></td>
<td></td>
<td>604.605 Mb/s</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td>2.126 Gb/s</td>
</tr>
</tbody>
</table>
Netflow: What is cistern doing?
Reporting

BYOD
BRING YOUR OWN DEVICE

Amazon Music

Netflix

AWS

Skype

Amazon

Instant Video
Netflow: Top Applications

Results

<table>
<thead>
<tr>
<th>Application</th>
<th>Packets</th>
<th>Percent</th>
<th>Bps</th>
</tr>
</thead>
<tbody>
<tr>
<td>sal (Type: 13 ID: 453)</td>
<td>1.863 k/s</td>
<td>19.36 %</td>
<td>13.763 M/s</td>
</tr>
<tr>
<td>youtube (Type: 13 ID: 82)</td>
<td>1.053 k/s</td>
<td>14.51 %</td>
<td>10.315 M/s</td>
</tr>
<tr>
<td>video-over-http (Type: 13 ID: 432)</td>
<td>734.980 p/s</td>
<td>9.14 %</td>
<td>6.495 M/s</td>
</tr>
<tr>
<td>binary-over-http (Type: 13 ID: 431)</td>
<td>621.090 p/s</td>
<td>7.99 %</td>
<td>5.682 M/s</td>
</tr>
<tr>
<td>internet-video-streaming (Type: 13 ID: 574)</td>
<td>589.179 p/s</td>
<td>7.29 %</td>
<td>5.185 M/s</td>
</tr>
<tr>
<td>secure-http (Type: 3 ID: 443)</td>
<td>380.841 p/s</td>
<td>4.71 %</td>
<td>3.346 M/s</td>
</tr>
<tr>
<td>http (Type: 3 ID: 80)</td>
<td>402.197 p/s</td>
<td>4.38 %</td>
<td>3.116 M/s</td>
</tr>
<tr>
<td>dropbox (Type: 3 ID: 17500)</td>
<td>322.881 p/s</td>
<td>3.50 %</td>
<td>2.486 M/s</td>
</tr>
<tr>
<td>ftp (Type: 3 ID: 554)</td>
<td>374.105 p/s</td>
<td>3.30 %</td>
<td>2.343 M/s</td>
</tr>
<tr>
<td>dns (Type: 3 ID: 53)</td>
<td>252.387 p/s</td>
<td>2.44 %</td>
<td>1.734 M/s</td>
</tr>
</tbody>
</table>
Netflow: Patterns

DPI Reports » Applications

From 2016-10-14 20:00 to 2016-11-13 19:00 in auto (1d) Intervals

Results

<table>
<thead>
<tr>
<th>Application</th>
<th>Packets</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>bittorrent (Type: 13 ID: 69)</td>
<td>17,096 p/s</td>
<td>100.00 %</td>
</tr>
</tbody>
</table>
Voice and Video Traffic Monitoring and Reporting

Rich media traffic monitoring must go beyond traditional usage metrics. Excessive jitter or packet loss are often telltale signs of a voice and video issue, but where on the network was the problem introduced? Where did the DSCP value change and why wasn’t the traffic prioritized correctly? Voice and video traffic monitoring often needs to be done campus-wide and, ideally, when quality of service slips, thresholds are breached, notifications are triggered, and if configured, traffic is rerouted. Does your company have the solution to investigate and accurately report on all of this recorded information on an end-to-end or hop-by-hop basis?
Netflow Security
NetFlow cannot see payloads
Neither will you DPI if the packet is encrypted.

Keeping netflows requires far less storage that your IDS.
Compliance

● Recognize unauthorized host access
● Detect malicious and suspicious network activity
● Leverage third-party integrations for threat mitigation to remediate security policy violations
● **HIPPA, RIAA**
● Continuously monitor hosts and network activity to identify intrusions
● Conduct forensic analysis for security incidents: Who, what, when, how long
Title: Last Week Tonight with John Oliver
Timestamp: 2016-11-07T23:07:29Z
IP Address: 192.16.204.250
Port: 23945
Type: BitTorrent
Torrent Hash: 2b9b91ca32f082e3f7d6c7af60e8a51d0eb9a465
Filesize: 309 MB

Diagnosing Compliance: RIAA
Infringement
Compliance

- Recognize unauthorized host access
- Detect malicious and suspicious network activity
- Leverage third-party integrations for threat mitigation to remediate security policy violations
- HIPPA, RIAA
- Continuously monitor hosts and network activity to identify intrusions
- **Conduct forensic analysis for security incidents:** Who, what, when, how long
Diagnosing Vectors of Infection

What is the malware doing?
Diagnosing Vectors of Infection

What is the malware doing?

Who else has it?
Diagnosing Vectors of Infection

What is the malware doing?

Who else has it?

How long has it been active on the network?
Diagnosing Vectors of Infection

What is the malware doing?

Who else has it?

How long has it been active on the network?

What is the malware pattern?
Diagnosing Vectors of Infection
Questions?

How is netflow being used at your institution?

Presented by Christina Klam at NJEDge Conference 2016. 2016-11-18
NetFlow: Troubleshooting Network & Security Problems with FloWS

Presented by Christina Klam at NJEDge Conference 2016. 2016-11-18