Flow-Based Network Monitoring using nProbe and ntopng

Simone Mainardi, PhD
@simonemainardi
mainardi@ntop.org
Agenda

• About ntop
• Flow-based network monitoring, beyond SNMP
• nProbe: NetFlow/IPFIX/sFlow probe and collector
• ntopng: Web-Based visualization
About ntop

• Private company devoted to development of Open Source network traffic monitoring applications.

• R&D Italy, Sales Switzerland.

• ntop (circa 1998) is the first app we released and it is a web-based network monitoring application.
Some Products we Developed [1/2]

• Our software is powering many commercial products...
Some Products we Developed [2/2]

• ...and allows packets to be received and transmitted at 1/10 Gbit line rate with no loss, any packet size on Intel-based commodity NICs.

• So we accelerate not just our applications but also third party open source solutions including:

![SNORT logo](image1)
![ostinato logo](image2)
![WIRESHARK logo](image3)
Product Lines

• Open Source (https://github.com/ntop)
  ◦ ntopng: Web-based monitoring application
  ◦ PF_RING: Accelerated RX/TX on Linux
  ◦ nDPI: Deep Packet Inspection Toolkit

• Proprietary
  ◦ PF_RING ZC: 1/10/40/100 Gbit Line rate.
  ◦ nProbe: 10G NetFlow/IPFIX Probe
  ◦ nProbe Cento: flows+packets+security
  ◦ n2disk/disk2n Network-to-disk and disk-to-network.
  ◦ nScrub: Software DDoS Mitigation
Motivation

• Without measurements we cannot evaluate the results, introduce improvements, quantify the success of our policies.

“If you can’t measure it, you can’t improve it”
(Lord Kelvin, 1824 – 1907)

“If you can’t measure it, you can’t manage it”
(Peter Drucker, 1909 – 2005)
Network Monitoring with Check_MK
SNMP

- Basic measurements
  - Bytes in/out, interface status, interface speed
- Ability to set thresholds
  - “if the interface goes above X Bps for Y secs then…”
- Visibility on the troubles but…
  - What is the cause?
  - Who is the bad guy?
Active Measurements

- PINGs, HTTP(s) requests, DNS queries
- Ptolemaic view
  - Measurements depend on the observation point
- Are the measurements really representative of users’ quality of experience (QoE)?
What is missing today?

• Network traffic visibility

• Device-to-traffic binding

• Distributed service availability and performance
  • Network traffic visibility to pretend to be the end-user
  • Measurements that are representative of the users’ QoE
Available Monitoring Technologies

- Fortunately, several technologies come into play when it comes to provide visibility into the network traffic
  - Switches: sFlow
  - Routers: NetFlow v5/v9, IPFIX, NetFlow Lite
Monitoring From Scratch

- Sometimes it is necessary to start the monitoring from raw packets, for example when
  - NetFlow/sFlow is not available
  - Custom measurements are needed (eg., RTT, Network Latency, DPI)
  - An extra piece of software (a **probe**) is required to process the packets and translate them into something actionable
  - The **probe** can be fed with packets from
    - Switch mirror ports
    - Network TAPs
Compressing Raw Packets

• All the monitoring technologies available are inherently connected by the necessity to “compress” packets into actionable summaries that preserve the basic properties of the network communications

• Often impractical to work with raw network packets

• Network packets are still important for providing evidence or troubleshooting problems (“pcap or it didn't happen!”) but they are “too raw” and take too much storage space.

• Network flow analysis is a good way to “compress packets”: sFlow do it with sampling, NetFlow with stateful connection-based packet classification.
Network Flows: What Are They?

• “A flow is a set of packets with a set of common packet properties” (e.g. common IP address/port).

• All the packets of a web session can be summarized in a flow

  • “host 1.2.3.4 fetched website www.ntop.org served by host 6.7.8.9 in $S$ seconds [with network latency $X$ ms [and application latency $Y$ ms [and …]]]”

• Other examples of network flows are a Skype/VoIP call, an FTP file transfer, an SSH session, etc.
## Packets vs Flow

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Source P</th>
<th>Destination P</th>
<th>Protocol</th>
<th>Length</th>
<th>Host</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10:55:45</td>
<td>192.168.1.110</td>
<td>212.1.42.233</td>
<td>80</td>
<td>62241</td>
<td>TCP</td>
<td>78</td>
<td>80 → 62241 [SYN] Seq=0 W...</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>66</td>
<td>62241 → 80 [ACK] Seq=1 Ac...</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>66</td>
<td>HTTP/1.1 200 OK [Unreas...</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>1506</td>
<td>Continuation</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>1506</td>
<td>Continuation</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>1506</td>
<td>Continuation</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>1506</td>
<td>Continuation</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>1506</td>
<td>Continuation</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>1506</td>
<td>Continuation</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>1506</td>
<td>Continuation</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>1506</td>
<td>Continuation</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>1506</td>
<td>Continuation</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>1506</td>
<td>Continuation</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>1506</td>
<td>Continuation</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>66</td>
<td>62241 → 80 [ACK] Seq=561 ...</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>66</td>
<td>62241 → 80 [ACK] Seq=561 ...</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>66</td>
<td>62241 → 80 [ACK] Seq=561 ...</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>66</td>
<td>62241 → 80 [ACK] Seq=561 ...</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>66</td>
<td>62241 → 80 [ACK] Seq=561 ...</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>66</td>
<td>62241 → 80 [ACK] Seq=561 ...</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>1506</td>
<td>Continuation</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>1506</td>
<td>Continuation</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>10:55:45</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>1506</td>
<td>Continuation</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>10:56:00</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>1506</td>
<td>Continuation</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>10:56:00</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>1506</td>
<td>Continuation</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>10:56:01</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>1506</td>
<td>Continuation</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>10:56:01</td>
<td>212.1.42.233</td>
<td>192.168.1.110</td>
<td>62241</td>
<td>80</td>
<td>TCP</td>
<td>66</td>
<td>80 → 62241 [ACK] Seq=1493...</td>
<td></td>
</tr>
</tbody>
</table>

### Application: HTTP
- **L4 Proto:** TCP
- **Client:** 192.168.1.110:62241
- **Server:** www.magazin.com:80
- **Duration:** 16 sec
- **Breakdown:** 0 bit/s
- **Total Bytes:** 16.89 KB
- **Info:** /schluesselanhaenger-key...
SNMP vs Flow

Visibility provided by SNMP
What to Expect from Flows

• PC/services that are heavily using the network (Top Talkers) — Who’s making the network slow?

• Highlight the sources and destinations of network traffic — There’s a file transfer going on to a Chinese host

• Application protocols used (Skype, HTTP, Email) — Someone is watching Netflix at work!

• Advanced reporting (billing and accounting) — What was the amount of bandwidth consumed over the past week?

• Legitimate but unauthorized/suspicious traffic (eg. Tor or VPN)
What NOT to Expect from Flows

• Non-IP traffic (e.g. NetBIOS, AppleTalk).

• L2 information (e.g. interface up/down state changes)

• Filtered traffic (e.g. firewall policy counters).

• Per-link statistics (e.g. link usage, congestion, delay, packet loss).
What Pieces are Needed?

- A collector
  - To speak sFlow/NetFlow with switches and routers
- A probe
  - To generate flows out of network TAPs and port mirrors
- Least but not last, a good tool for visualization and analysis…
nProbe

- NetFlow v5/v9/IPFIX, NetFlow-Lite and sFlow collector
- 10Gbps+ probe with DPI
- Extensible (support plugins)
- Convert flow format (sFlow-to-NetFlow/IPFIX) or version (e.g. v5 to v9)
- Ability to export to Kafka, MySQL, ElasticSearch, Text Files, Syslog, JSON, ZMQ, …
Collector vs Probe Mode

Probe

Collector

NICs

NetFlow v5/v9
IPFIX
sFlow

Check_MK Conference #4 May 2nd-4th 2018
© 2018 - ntop.org
Deep Packet Inspection with nDPI

• nProbe in collector mode performs Deep Packet Inspection (DPI) using the opensource library nDPI

• Supported protocols (> 240) include:
  • P2P (Skype, BitTorrent)
  • Messaging (Viber, Whatsapp, MSN, The Facebook)
  • Multimedia (YouTube, Last.gm, iTunes)
  • Conferencing (Webex, CitrixOnLine)
  • Streaming (Zattoo, Icecast, Shoutcast, Netflix)
  • Business (VNC, RDP, Citrix, *SQL)
nProbe Downstream Export

- ntopng
- ØMQ
- ntopng
- elastic
- MySQL
- Apache Kafka
- NetFlow v5/v9
  IPFIX collectors
- syslog
- {json

Check_MK Conference #4 May 2nd-4th 2018
© 2018 - ntop.org
Flow Analysis with ntopng

- ntopng is a monitoring tool capable of harvesting nProbe-generated data for visualization and analysis

- Web-based HTML5 Graphical User Interface
Main ntopng Features

- Embedded alerting system with several external endpoints including nagios, email and slack
- Grafana datasource
- Ready for Wireshark, Vagrant, Docker
- Support for NetFlow/sFlow/SNMP
- Passive/Active Network Device Discovery
- Traffic Behavior Analysis
## SNMP Monitoring

### SNMP Devices

<table>
<thead>
<tr>
<th>Device IP</th>
<th>Chart</th>
<th>Device Name</th>
<th>Description</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.2.224</td>
<td><img src="image1" alt="chart" /></td>
<td>nbox-demo</td>
<td>Linux nbox-demo 3.13.0-108-generic #155-Ubuntu SMP Wed Jan 11 16...</td>
<td>Disable Polling, Delete</td>
</tr>
<tr>
<td>192.168.2.169</td>
<td><img src="image2" alt="chart" /></td>
<td>192.168.2.169</td>
<td>ProCurve J9019B Switch 2510B-24, revision Q.11.17, ROM Q.10.02 (...</td>
<td>Disable Polling, Delete</td>
</tr>
<tr>
<td>192.168.2.110</td>
<td><img src="image3" alt="chart" /></td>
<td>ubuntu12</td>
<td>Linux ubuntu12 3.13.0-117-generic #164-precise1-Ubuntu SMP Mon A...</td>
<td>Disable Polling, Delete</td>
</tr>
<tr>
<td>170.168.2.34</td>
<td><img src="image4" alt="chart" /></td>
<td>Cisco DPC3928SL DOCSIS 3.0 1-PORT Voice Gateway &lt;</td>
<td></td>
<td>Disable Polling, Delete</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux snmp 2.6.39 #1 SMP PREEMPT Fri Jul 28 11:15:39 CEST 2017 i...</td>
<td>Disable Polling, Delete</td>
</tr>
</tbody>
</table>

Showing 1 to 7 of 7 rows
# SNMP Interfaces Slicing & Dicing

## Interfaces

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>VLAN</th>
<th>Speed</th>
<th>Status</th>
<th>In Bytes</th>
<th>Out Bytes</th>
<th>In Discards</th>
<th>Interface Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>25</td>
<td>1</td>
<td>1 Gbit</td>
<td>Up</td>
<td>88.18 GB</td>
<td>1001.33 GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>1</td>
<td>100 Mbit</td>
<td>Up</td>
<td>1.04 TB</td>
<td>42.63 GB</td>
<td></td>
<td>ethernetCsmacd</td>
</tr>
<tr>
<td>15</td>
<td>15</td>
<td>1</td>
<td>100 Mbit</td>
<td>Up</td>
<td>2.28 GB</td>
<td>29.94 GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>19</td>
<td>1</td>
<td>100 Mbit</td>
<td>Up</td>
<td>1.71 GB</td>
<td>26.23 GB</td>
<td></td>
<td>softwareLoopback</td>
</tr>
<tr>
<td>21</td>
<td>21</td>
<td>1</td>
<td>100 Mbit</td>
<td>Up</td>
<td>340.65 MB</td>
<td>9.26 GB</td>
<td></td>
<td>propVirtual</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>1</td>
<td>100 Mbit</td>
<td>Up</td>
<td>167.48 MB</td>
<td>635.18 MB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4152</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HP ProCurve Switch software loopback interface</td>
</tr>
<tr>
<td>57</td>
<td>DEFAULT_VLAN</td>
<td>1</td>
<td>100 Mbit</td>
<td>Up</td>
<td>0 Bytes</td>
<td>0 Bytes</td>
<td>55 days, 7 h, 17 min, 11 sec</td>
<td></td>
</tr>
</tbody>
</table>

Showing 1 to 8 of 8 rows
SNMP and Flow Collection: Connecting the Dots [1/2]

- ntopng for each flow exporter device is able to detect if there is a corresponding SNMP device configured and glue them up.
SNMP and Flow Collection: Connecting the Dots [2/2]
Know What’s Wrong: Alerts [1/3]

Extensible Thresholds on Traffic/SNMP/NetFlow…

Time Period

<table>
<thead>
<tr>
<th>Threshold Type</th>
<th>Host Lucas-iMac Thresholds</th>
<th>Local Hosts Common Thresholds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity time delta (seconds)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traffic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Layer 2 bytes delta (sent + received)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Traffic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Layer 2 bytes delta (sent + received) for DNS detected traffic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flows</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flows delta (as client + as server)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Idle Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Idle time since last packet seen (seconds)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P2P Traffic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Layer 2 bytes delta (sent + received) for peer-to-peer detected traffic</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Know What’s Wrong: Alerts [2/3]

Open Issues

Engaged Alerts

Past Issues

Flow Issues

Engaged Alerts

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Duration</th>
<th>Severity</th>
<th>Alert Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sat May 6 13:03:03 2017</td>
<td>2 min, 4 sec</td>
<td>Error</td>
<td>Threshold Cross</td>
<td>Threshold active crossed by host [65 &gt; 1]</td>
</tr>
</tbody>
</table>

Showing 1 to 1 of 1 rows

Who

What

When

How Long
Know What’s Wrong: Alerts [3/3]

• External Alerts Endpoints

• Slack and Email

• Nagios via NSCA client

• Nagios will intercept all alerts that are explicitly declared as passive services

<table>
<thead>
<tr>
<th>ntopng-host</th>
<th>NtopngAlert</th>
<th>?</th>
<th>OK</th>
<th>12-23-2015 15:25:50</th>
<th>0d 17h 27m 59s</th>
<th>1/1</th>
<th>Alert for host Y!</th>
</tr>
</thead>
<tbody>
<tr>
<td>NtopngAlert_192.168.1.15_min_bytes</td>
<td>?</td>
<td>OK</td>
<td>12-23-2015 09:13:22</td>
<td>0d 6h 47m 34s</td>
<td>1/1</td>
<td>OK, alarm deactivated</td>
<td></td>
</tr>
<tr>
<td>NtopngAlert_192.168.2.0/24</td>
<td>?</td>
<td>OK</td>
<td>12-23-2015 11:02:34</td>
<td>0d 4h 33m 4s</td>
<td>1/1</td>
<td>OK, alarm deactivated</td>
<td></td>
</tr>
<tr>
<td>NtopngAlert_192.168.70.0/24_min_egress</td>
<td>?</td>
<td>WARNING</td>
<td>12-23-2015 15:33:01</td>
<td>0d 0h 6m 5s</td>
<td>1/1</td>
<td>Threshold egress crossed by network 192.168.70.0/24 [1180 &gt; 10]</td>
<td></td>
</tr>
<tr>
<td>NtopngAlert_192.168.70.0/24_min_ingress</td>
<td>?</td>
<td>WARNING</td>
<td>12-23-2015 15:33:01</td>
<td>0d 0h 2m 5s</td>
<td>1/1</td>
<td>Threshold ingress crossed by network 192.168.70.0/24 [11241211 &gt; 10]</td>
<td></td>
</tr>
</tbody>
</table>
Take Home

- SNMP is OK but it’s better if it can be enriched with network traffic
- Network traffic can be compressed with into meaningful representations called flows
- Flow can be collected from sFlow/NetFlow devices or generated with a network probe
  - nProbe
    - 10+ Gbps probe
    - NetFlow v5/v9/IPFIX collector
  - ntopng
    - Web-based GUI for visualization and analysis
    - Able to collect monitored traffic from remote nProbes
    - Present and past host activities visualization, including ability to alert on suspicious behaviors
Thank you!

Simone Mainardi, PhD
@simonemainardi
mainardi@ntop.org