ntopng 2023: News & Updates

Matteo Biscosi
Nicolò Maio
What Changed

Main Focus/Changes:

<table>
<thead>
<tr>
<th>Last Year</th>
<th>Now</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alerts &amp; Checks</td>
<td>Cybersecurity</td>
</tr>
<tr>
<td>Behavior Analysis</td>
<td>Traffic Analysis</td>
</tr>
<tr>
<td>Historical Flows (ClickHouse)</td>
<td>Historical Flows (Improvements)</td>
</tr>
<tr>
<td>Integrations</td>
<td>Integrations</td>
</tr>
<tr>
<td></td>
<td>User Interface</td>
</tr>
</tbody>
</table>
New ntopng Model Available: Enterprise XL

XL Model:

• Increased the maximum number of exporters (reaching 1024 total exporters)
• Increased the maximum number of monitored interfaces (up to 64)
• Support to Host Flow Sankey & other features...
User Interface Refactoring: Charts (2/2)

![Graph and table showing network metrics for different interfaces and metrics, including average, 95th percentile, max, min, and total values for byte rates.](image)

- **eno1 - Sent**: 164.31 Kbps, 1.12 Mbps, 1.98 Mbps, 0.00 bps, 420.75 MB
- **eno1 - Rcvd**: 170.33 Kbps, 90.77 Kbps, 12.60 Mbps, 0.00 bps, 436.15 MB
- **eno1 - TLS**: 5.83 Kbps, 11.16 Kbps, 31.49 Kbps, 0.00 bps, 14.94 MB
- **eno1 - WebCheckinNew**: 107.90 Kbps, 684.34 Kbps, 2.10 Mbps, 0.00 bps, 276.29 MB
- **eno1 - Github**: 79.92 Kbps, 291.37 bps, 9.09 Mbps, 0.00 bps, 204.64 MB

---

**ntopConf'23**

Sept, 21-22 · Pisa
New Dashboard... (1/2)
New Dashboard... (2/2)

A different Dashboard based on:

- Model (Pro, Enterprise M, ...)
- Configuration (ClickHouse enabled or not)

In the near future: ability to create custom dashboards from ntopng UI
... & Traffic Report (1/2)
...& Traffic Report (2/2)

Now it can:

- Be Printed / Uploaded / Downloaded
- Sent via E-Mail!
- Different Reports available
- A lot more in the future...
New Report Available

There is a new daily report auto-2023-Sep-15-1894728886 available in ntopng for interface tcp://127.0.0.1:6666c under the Reports section. A retention time of 30 days is configured in the ntopng Preferences, it is recommended to download and backup the report.

Check it out!

Go to Report
Historical Flows

User Interface Refactoring... (1/2)
Historical Flows
User Interface Refactoring... (2/2)

• Changed tables:
  • More Flexible (resizable columns)
  • A lot more Fast
  • Configurable (choose which column to display)

• Added many new Presets (Queries):
  • Top Sender/Receiver Network
  • Top Sender/Receiver Country
  • ...
...Historical Flows Aggregation (1/3)...

Have less information but more Data!

Keeping all last month Flows in the Database could cost a lot of disk

Just keep an aggregation of flows (compact similar flows in a single entry) in order to be able to keep more data
Historical Flows Aggregation (2/3)

Switch Between Normal &...
...Historical Flows Aggregation (2/3)...

```
<table>
<thead>
<tr>
<th>Actions</th>
<th>Begin</th>
<th>End</th>
<th>Protocol</th>
<th>Application</th>
<th>Flow</th>
<th>Avg Score</th>
<th>Total Flows</th>
<th>Pkts</th>
<th>Total Bytes</th>
<th>Cli ASN</th>
<th>Srv ASN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>13:22:32</td>
<td>13:22:32</td>
<td>TCP</td>
<td>TLS.Unknown</td>
<td>192.168.2.222</td>
<td>10</td>
<td>1</td>
<td>1,140</td>
<td>1.01 MB</td>
<td>36459 (GitHub, Inc.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>13:22:34</td>
<td>13:56:26</td>
<td>TCP</td>
<td>SSH</td>
<td>192.168.2.222</td>
<td>7</td>
<td>7</td>
<td>1,322</td>
<td>152.28 KB</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>13:22:35</td>
<td>13:57:22</td>
<td>TCP</td>
<td>Unknown</td>
<td>127.0.0.1</td>
<td>7</td>
<td>7</td>
<td>52,222</td>
<td>7.0 MB</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>13:22:38</td>
<td>13:57:23</td>
<td>TCP</td>
<td>Unknown</td>
<td>127.0.0.1</td>
<td>7</td>
<td>7</td>
<td>8,338</td>
<td>1.43 MB</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>13:22:57</td>
<td>13:23:32</td>
<td>TCP</td>
<td>TLS.Unknown</td>
<td>192.168.2.222</td>
<td>10</td>
<td>2</td>
<td>180</td>
<td>73.6 KB</td>
<td>8075 (Microsoft Corp)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>13:22:57</td>
<td>13:32:07</td>
<td>UDP</td>
<td>DNS.Microsoft365</td>
<td>127.0.0.1</td>
<td>16</td>
<td>64</td>
<td>64</td>
<td>11.4 KB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
...Historical Flows Aggregation (3/3)...

99.6 GB vs 629.1 MB

Compression of data:
2.5B vs 14.2M Flows

Database Table Records:
- Flows Table Size: 99.6 GB
- Hourly Flows Table Size: 629.1 MB
- Alert Tables Size: 6.9 MB (Flow Alerts are included in the Flow Table Size)

ClickHouse

ClickHouse Flows/Alerts Data Retention
Number of days to keep raw (unaggregated) flows (if enabled) and alerts. Default: 30 days.

15 days of data vs 60 days of data!
Export flows from multiple ntopng towards:

- A single/stand-alone ClickHouse instance
- A ClickHouse Cluster

A ClickHouse cluster can provide redundancy, capacity, and performance
... & more Traffic Analysis

Many new pages to analyze the traffic and to understand what's happening:

- Live Flows Aggregation
- Asset Map
- Ports Analysis
- Host Sankey
- Networks
- Inactive Local Hosts
- ...
... & more Traffic Analysis
... & more Traffic Analysis
... & more Traffic Analysis
... & more Traffic Analysis
... & more Traffic Analysis

<table>
<thead>
<tr>
<th>Actions</th>
<th>Host</th>
<th>Name</th>
<th>MAC Address</th>
<th>Manufacturer</th>
<th>First Seen</th>
<th>Last Seen</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>192.168.2.240@384</td>
<td>[Test vlan]</td>
<td>28:B1:33:00:59:4D</td>
<td>SHINEMAN(SHENZHEN) Tech. Cor., Ltd.</td>
<td>08/23/2023 16:00:44</td>
<td>08/23/2023 16:00:45</td>
</tr>
<tr>
<td></td>
<td>192.168.2.225@384</td>
<td>[Test vlan]</td>
<td>00:E0:E0:1A:34:56</td>
<td>Silicom, Ltd.</td>
<td>08/23/2023 15:46:59</td>
<td>08/23/2023 15:47:07</td>
</tr>
<tr>
<td></td>
<td>192.168.2.225</td>
<td></td>
<td>00:E0:E0:1A:34:56</td>
<td>Silicom, Ltd.</td>
<td>09/14/2023 11:20:21</td>
<td>09/14/2023 11:20:24</td>
</tr>
<tr>
<td></td>
<td>192.168.2.222@3828</td>
<td></td>
<td>00:25:90:D4:CC:F9</td>
<td>Super Micro Computer, Inc.</td>
<td>09/01/2023 10:16:19</td>
<td>09/01/2023 10:16:19</td>
</tr>
<tr>
<td></td>
<td>192.168.2.222@3822</td>
<td></td>
<td>00:25:90:D4:CC:F9</td>
<td>Super Micro Computer, Inc.</td>
<td>08/25/2023 13:00:51</td>
<td>08/25/2023 13:00:52</td>
</tr>
<tr>
<td></td>
<td>192.168.2.222@3671</td>
<td></td>
<td>00:25:90:D4:CC:F9</td>
<td>Super Micro Computer, Inc.</td>
<td>09/01/2023 10:00:14</td>
<td>09/01/2023 10:00:15</td>
</tr>
<tr>
<td></td>
<td>192.168.2.222@3608</td>
<td></td>
<td>00:25:90:D4:CC:F9</td>
<td>Super Micro Computer, Inc.</td>
<td>08/30/2023 09:00:34</td>
<td>08/30/2023 09:01:01</td>
</tr>
<tr>
<td></td>
<td>192.168.2.222@3533</td>
<td></td>
<td>00:25:90:D4:CC:F9</td>
<td>Super Micro Computer, Inc.</td>
<td>08/30/2023 08:19:22</td>
<td>08/30/2023 08:19:23</td>
</tr>
<tr>
<td></td>
<td>192.168.2.222@3522</td>
<td></td>
<td>00:25:90:D4:CC:F9</td>
<td>Super Micro Computer, Inc.</td>
<td>08/22/2023 16:45:01</td>
<td>08/22/2023 16:45:03</td>
</tr>
</tbody>
</table>
... & more Traffic Analysis

and many more...
Vulnerability Scan (1/5)

- Analyze hosts in a network to discover vulnerabilities
- Discover open ports
- Manually or periodically scan single or multiple hosts
# Vulnerability Scan (2/5)

<table>
<thead>
<tr>
<th>Actions</th>
<th>Host</th>
<th>Host Name</th>
<th>Scan Type</th>
<th>CVEs</th>
<th>TCP Ports</th>
<th>Last Scan Duration</th>
<th>Last Scan Date</th>
<th>Periodicity</th>
<th>Last Scan Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>192.168.1.1</td>
<td>h388x.homenet.telecomitalia.it</td>
<td>CVE</td>
<td>3</td>
<td>6</td>
<td>02:24</td>
<td>12:19:29</td>
<td>Nightly</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>192.168.1.6</td>
<td>host-004.homenet.telecomitalia.it</td>
<td>CVE</td>
<td></td>
<td></td>
<td>00:02 sec</td>
<td>11:18:57</td>
<td>Nightly</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>192.168.1.10</td>
<td>host-002.homenet.telecomitalia.it</td>
<td>CVE</td>
<td>1,729</td>
<td>3</td>
<td>00:34 sec</td>
<td>11:26:05</td>
<td>Nightly</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>192.168.1.16</td>
<td></td>
<td>CVE</td>
<td></td>
<td></td>
<td>00:02 sec</td>
<td>12:16:55</td>
<td>Nightly</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>192.168.1.28</td>
<td>peppeasusi7.homenet.telecomitalia.it</td>
<td>CVE</td>
<td>5,518</td>
<td>3</td>
<td>00:08 sec</td>
<td>11:17:19</td>
<td>Nightly</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>192.168.1.30</td>
<td></td>
<td>CVE</td>
<td></td>
<td></td>
<td>00:02 sec</td>
<td>12:09:50</td>
<td>Nightly</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>192.168.1.88</td>
<td></td>
<td>CVE</td>
<td></td>
<td></td>
<td>00:02 sec</td>
<td>12:07:33</td>
<td>Nightly</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>192.168.1.110</td>
<td></td>
<td>CVE</td>
<td></td>
<td></td>
<td>02:00</td>
<td>11:16:27</td>
<td>Nightly</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>192.168.1.164</td>
<td></td>
<td>CVE</td>
<td></td>
<td></td>
<td>00:02 sec</td>
<td>12:08:17</td>
<td>Nightly</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>192.168.1.60</td>
<td></td>
<td>CVE</td>
<td></td>
<td></td>
<td>00:02 sec</td>
<td>11:13:39</td>
<td>Nightly</td>
<td>Success</td>
</tr>
</tbody>
</table>

Showing page 1 of 4: total 37 rows
Vulnerability Scan (3/5)

- Download/Show Scan Report
- Schedule Periodic Scan
- Show CVEs (Vulnerabilities)
- Scan Hosts on specific ports
Vulnerability Scan Report of 192.168.2.172 at 11:17:45

22/tcp open ssh Dropbear sshd 2013.60 (protocol 2.0)

Vulnerability Scan Report:

[CVE-2012-0929] Use-after-free vulnerability in Dropbear SSH Server 0.52 through 2012.54, when command restriction and public key authentication are enabled, allows remote attackers to cause a denial of service via unknown vectors, as demonstrated by a certa.

[CVE-2009-3340] Unspecified vulnerability in FreeSSH 1.2.4 allows remote attackers to cause a denial of service via unknown vectors, as demonstrated by a certa.

[CVE-2008-3234] sshd in OpenSSH 4 on Debian GNU/Linux, and the 20070303 OpenSSH snapshot, allows remote authenticated users to obtain access to arbitrary SELinux.

[CVE-2006-5794] Unspecified vulnerability in the sshd Privilege Separation Monitor in OpenSSH before 4.5 causes weaker verification that authentication has been completed.


[CVE-2002-0460] Bitvise WinSSHD before 2002-03-16 allows remote attackers to cause a denial of service (resource exhaustion) via a large number of incomplete close requests.

80/tcp open http ATEN/Supermicro IPMI web interface

Vulnerability Scan Report:

[CVE-2013-4785] The web interface for Dell iDRAC 6 firmware 1.7, and possibly other versions, allows remote attackers to modify the CLP interface for arbitrary command.


[CVE-2013-3633] The web interface on Siemens Scalance X200 IRT switches firmware before X-200IRT 5.1.0 relies on client-side privilege checks, which allows.


[CVE-2013-3508] The Foundation webapp admin interface in GroundWork Monitor Enterprise 6.7.0 uses the nagios account as the owner of writable files under /usr/local.

[CVE-2013-3457] Absolute path traversal vulnerability in the web interface in Cisco Finesse allows remote attackers to read directory contents via a direct request.

[CVE-2013-3440] Multiple cross-site scripting (XSS) vulnerabilities in the administrative web interface in Cisco Unified Operations Manager allow remote attack.


[CVE-2013-3088] VMware vCenter Server Appliance (vCSA) 5.1 before Update 1 allows remote authenticated users to create or overwrite arbitrary files, and consequ.
Vulnerability Scan (5/5)

<table>
<thead>
<tr>
<th>Actions</th>
<th>Port</th>
<th>Service Name</th>
<th>CVEs</th>
<th>Count</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>22</td>
<td>ssh</td>
<td>52,767</td>
<td>23</td>
<td>192.168.2.225, 192.168.2.221, 192.168.2.222, 192.168.2.222, 192.168.2.106, 192.168.2.153...</td>
</tr>
<tr>
<td></td>
<td>80</td>
<td>http</td>
<td>53,402</td>
<td>16</td>
<td>192.168.2.221, 192.168.2.106, 192.168.2.167, 192.168.2.120, 192.168.2.133...</td>
</tr>
<tr>
<td></td>
<td>443</td>
<td>https</td>
<td>42,569</td>
<td>12</td>
<td>192.168.2.221, 192.168.2.167, 192.168.2.120, 192.168.2.133, 192.168.2.60...</td>
</tr>
<tr>
<td></td>
<td>3000</td>
<td>remoteware-cl</td>
<td>485</td>
<td>6</td>
<td>192.168.2.222, 192.168.1.60, 192.168.2.240, 192.168.2.178, 192.168.2.134...</td>
</tr>
<tr>
<td></td>
<td>5900</td>
<td>rfb</td>
<td>41,952</td>
<td>5</td>
<td>192.168.2.120, 192.168.2.133, 192.168.2.158, 192.168.2.172, 192.168.2.83</td>
</tr>
<tr>
<td></td>
<td>9090</td>
<td>websm</td>
<td>59</td>
<td>4</td>
<td>192.168.2.221, 192.168.2.240, 192.168.2.134, 192.168.2.75</td>
</tr>
<tr>
<td></td>
<td>9000</td>
<td>cslinter</td>
<td>474</td>
<td>4</td>
<td>192.168.2.39, 192.168.1.110, 192.168.2.178, 192.168.2.134</td>
</tr>
<tr>
<td></td>
<td>53</td>
<td>domain</td>
<td>204</td>
<td>4</td>
<td>192.168.2.60,h388x.homenet.telecomitalia.it, 192.168.2.1, 192.168.2.59</td>
</tr>
<tr>
<td></td>
<td>23</td>
<td>telnet</td>
<td>10,632</td>
<td>3</td>
<td>192.168.2.106, 192.168.2.169, 192.168.2.237</td>
</tr>
<tr>
<td></td>
<td>135</td>
<td>epmap</td>
<td>5,518</td>
<td>3</td>
<td>peppeasus7.homenet.telecomitalia.it, 192.168.1.30, 192.168.1.16</td>
</tr>
</tbody>
</table>

Showing page 1 of 4: total 40 rows
Local Traffic Rules (1/3)

Monitoring SNMP devices / Hosts / Interfaces to unveil changes in traffic:

- Check periodically (every 5 mins, 1 hour, or 1 day) timeseries.
- Multiple metrics to check available (Traffic, Apps, Score, ...)
- When a configured Threshold is exceeded

↓

Trigger an alert

(Available only from Enterprise L license)
### Local Traffic Rules (2/3)

<table>
<thead>
<tr>
<th>Target</th>
<th>Type</th>
<th>Metric</th>
<th>Check Frequency</th>
<th>Last Measurement</th>
<th>Threshold</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>eno1</td>
<td>Interface</td>
<td>Score</td>
<td>Hourly</td>
<td>506290</td>
<td>&lt; 3 GB</td>
<td></td>
</tr>
<tr>
<td>eno1</td>
<td>Interface</td>
<td>Traffic</td>
<td>5 Minutes</td>
<td>2.82 MB</td>
<td>&lt; 125.00 Kbps</td>
<td></td>
</tr>
<tr>
<td>192.168.2.1</td>
<td>Host</td>
<td>DNS</td>
<td>5 Minutes</td>
<td>7.60 Mbps</td>
<td>&lt; 1 GB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Host</td>
<td>Traffic</td>
<td>5 Minutes</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**What to Monitor:**
- Score
- Traffic
- DNS
- Traffic

**Check Frequency:**
- Hourly
- 5 Minutes

**Threshold:**
- < 3 GB
- < 125.00 Kbps
- < 1 GB

**Notes:**
- Trigger an alert when a local host exceeds the specified traffic amount.
- To add a new rule, click the '+' symbol on the right side above the table (next to the search).
- To remove a rule, click on the 'Actions' column button and then click onto 'Delete' on the row you want to remove.
Local Traffic Rules (3/3)
Integrations

Before:
• Discord
• Elasticsearch
• E-Mail
• Fail2Ban
• Slack
• Syslog
• Teams
• Telegram
• Webhook

Now:
• Discord
• Elasticsearch
• E-Mail
• Fail2Ban
• Mattermost
• PagerDuty
• Slack
• Syslog
• Teams
• Telegram
• TheHive
• Webhook
Integrations

• PagerDuty is one of the most commonly used software solutions for managing notifications

• TheHive a widely known platform for managing cybersecurity alerts

• Mattermost one of the most used business chat platforms
TheHive

Sending notifications to TheHive the Alert Entities count will increase
Incidents on All Teams

<table>
<thead>
<tr>
<th>Status</th>
<th>Priority</th>
<th>Urgency</th>
<th>Title</th>
<th>Created</th>
<th>Service</th>
<th>Assigned To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Triggered</td>
<td>--</td>
<td>High</td>
<td>[System]: Process</td>
<td>on Aug 16, 2023 at 5:33 PM</td>
<td>ntopng_service</td>
<td>Nicolo' Maio</td>
</tr>
<tr>
<td>Triggered</td>
<td>--</td>
<td>High</td>
<td>[Flow]: Known Proto on Non Std Port</td>
<td>on Aug 16, 2023 at 5:29 PM</td>
<td>ntopng_service</td>
<td>Nicolo' Maio</td>
</tr>
<tr>
<td>Triggered</td>
<td>--</td>
<td>High</td>
<td>[Flow]: Known Proto on Non Std Port</td>
<td>on Aug 16, 2023 at 5:29 PM</td>
<td>ntopng_service</td>
<td>Nicolo' Maio</td>
</tr>
<tr>
<td>Triggered</td>
<td>--</td>
<td>High</td>
<td>[Flow]: Known Proto on Non Std Port</td>
<td>on Aug 16, 2023 at 5:29 PM</td>
<td>ntopng_service</td>
<td>Nicolo' Maio</td>
</tr>
</tbody>
</table>
nEdge

ntopng inline, designed to solve a few problems:

- Bind devices to users
- Specify per-user application protocol policies
- Protect the network from malware and connections
- Make sure that the available Internet bandwidth is shared evenly
nEdge Updates

- Added support for multi-LAN
- Added support for VLANs
- Added handling of DHCPd Service
- Improved RADIUS AUTH
- Added RADIUS ACCT
https://github.com/ntop/ntopng