ntop 2Q23 Webinar
## Highlights

<table>
<thead>
<tr>
<th>Title</th>
<th>Speaker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction, OT Monitoring, Aggregated Flows, Zoom/Teams Monitoring, OpenAPI</td>
<td>Luca Deri</td>
</tr>
<tr>
<td>SNMP Devices/Host Traffic Rules, Server Port Analysis</td>
<td>Nicolò Maio</td>
</tr>
<tr>
<td>Live vs Inactive Monitoring, New GUI: Tables and Charts</td>
<td>Matteo Biscosi</td>
</tr>
<tr>
<td>Smart Recording, Suricata/Zeek at 100Gbit, New Licensing Model</td>
<td>Alfredo Cardigliano</td>
</tr>
<tr>
<td>Open Discussion</td>
<td></td>
</tr>
</tbody>
</table>
NTOPCONF ’23

Call for Paper Deadline JUNE 30TH, 2023
SEPTEMBER 21 (TRAINING)-22 (CONFERENCE), 2023

https://www.ntop.org/ntopconf2023/
SCADA/OT Monitoring
Introduction

• ntopng/nProbe have been used in SCADA/OT monitoring for a while.
  ◦ November 2020: Added support IEC 60870-5-104
  ◦ ntopConf 2022: M. Scheu shown how to use ntop tools for monitoring critical infrastructures.
  ◦ Leading OT monitoring companies use ntop tools inside their products.
Ntop and OT/Scada [1/2]

• Ntop tools are not “vertical” tools OT-only but are designed to solving “generic monitoring” problems including:
  ◦ Active/Passive Asset Discovery and Management.
  ◦ Traffic Monitoring.
  ◦ Behavioural Traffic Analysis.
  ◦ Anomaly and vulnerability detection.
  ◦ Threat Intelligence
Ntop and OT/Scada [2/2]

- OT/Scada is supported “à la ntop way” namely
  - Add support in nDPI
    - 44 Modbus
    - 244 DNP3
    - 245 IEC60870
    - 331 TuyaLP
    - 332 TPLINK_SHP
    - 334 BACnet
  - Implement nProbe Plugin (below ModbusTCP)
    - Extend ntopng
ntopng and OT/Scada

• ntopng is able to detect, report and alert
  ◦ Unusual error messages
  ◦ Unsupported function calls
  ◦ Function calls that have not been used before
  ◦ Unknown function codes
  ◦ Abnormal protocol behaviour
  ◦ Unexpected state transition
  ◦ Values outside of defined ranges
  ◦ Changes in frequency / periodicity
### OT/Scada Behavioural Checks

<table>
<thead>
<tr>
<th>Name</th>
<th>Interface</th>
<th>Category</th>
<th>Severity</th>
<th>Description</th>
<th>Values</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC Invalid Command Transition</td>
<td>🍀</td>
<td>🌟</td>
<td>Notice</td>
<td>Trigger an alert when a command to/from command or measure to/from command IEC transition is detected</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEC Invalid Transition</td>
<td>🍀</td>
<td>🌟</td>
<td>Notice</td>
<td>Trigger an alert when an invalid IEC transition is detected</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEC Unexpected TypeID</td>
<td>🍀</td>
<td>🌟</td>
<td>Notice</td>
<td>Trigger an alert when an unexpected TypeID is detected in IEC 104 protocol</td>
<td>9, 13, 36, 45, 46, 48, 30, 103, ...</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Interface</th>
<th>Category</th>
<th>Severity</th>
<th>Description</th>
<th>Values</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>ModbusTCP Invalid Transition</td>
<td>🍀</td>
<td>🌟</td>
<td>Notice</td>
<td>Trigger an alert when an invalid ModbusTCP transition is detected</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ModbusTCP Too Many Exceptions</td>
<td>🍀</td>
<td>🌟</td>
<td>Error</td>
<td>Trigger an alert when a flow reports a number of exceptions exceeding the specified threshold</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ModbusTCP Unexpected Function Code</td>
<td>🍀</td>
<td>🌟</td>
<td>Error</td>
<td>Trigger an alert when an unexpected ModbusTCP Function code is detected</td>
<td>3, 6, 16</td>
<td></td>
</tr>
</tbody>
</table>
Transition/State Monitoring

### Function Codes

<table>
<thead>
<tr>
<th>Function</th>
<th>Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read Holding Registers (3)</td>
<td>1,102</td>
</tr>
<tr>
<td>Write Multiple Registers (16)</td>
<td>6</td>
</tr>
</tbody>
</table>

### Registers

<table>
<thead>
<tr>
<th>Register</th>
<th>Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1,105</td>
</tr>
<tr>
<td>1</td>
<td>1,089</td>
</tr>
<tr>
<td>2</td>
<td>1,089</td>
</tr>
<tr>
<td>7</td>
<td>1,089</td>
</tr>
<tr>
<td>8</td>
<td>1,089</td>
</tr>
<tr>
<td>3</td>
<td>1,089</td>
</tr>
<tr>
<td>5</td>
<td>1,089</td>
</tr>
<tr>
<td>6</td>
<td>1,089</td>
</tr>
<tr>
<td>4</td>
<td>1,089</td>
</tr>
<tr>
<td>9</td>
<td>1,089</td>
</tr>
</tbody>
</table>

### Function Code Transitions

- **Write Multiple Registers** → **Read Holding Registers**

### Exceptions

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>16</td>
</tr>
</tbody>
</table>
# Behavioural Learning

## Traffic Behaviour

### Learning Period
Configure the learning period for behavioural traffic analysis.

<table>
<thead>
<tr>
<th>Hours</th>
<th>Days</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

### Service Status During Learning
The default status of a new discovered service when the Service Map is learning.

<table>
<thead>
<tr>
<th>Undecided</th>
<th>Allowed</th>
<th>Denied</th>
</tr>
</thead>
</table>

### Service Status Post Learning
The default status of a new discovered service when the Service Map has finished the learning.

### IEC60870 Learning Period
Configure the learning period for IEC60870 and ModbusTCP traffic analysis. Default: 6 hours.

<table>
<thead>
<tr>
<th>Hours</th>
<th>Days</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6</td>
</tr>
</tbody>
</table>

### ModbusTCP Learning Period
Configure the learning period for ModbusTCP traffic analysis. Default: 6 hours.

<table>
<thead>
<tr>
<th>Hours</th>
<th>Days</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>
## Alerts

<table>
<thead>
<tr>
<th>Action</th>
<th>Date/Time</th>
<th>Score</th>
<th>Application</th>
<th>Alert</th>
<th>Flow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12:04:21</td>
<td>100</td>
<td>TCP:Modbus</td>
<td>ModbusTCP Too Many Exceptions</td>
<td>172.16.203.200:2634 ⇔ 172.16.203.5:502</td>
<td>1 Exceptions</td>
</tr>
<tr>
<td></td>
<td>12:04:21</td>
<td>100</td>
<td>TCP:Modbus</td>
<td>ModbusTCP Invalid Function Code</td>
<td>172.16.203.200:2634 ⇔ 172.16.203.5:502</td>
<td>Function Code 'Write Multiple Re...</td>
</tr>
<tr>
<td></td>
<td>12:04:21</td>
<td>200</td>
<td>TCP:Modbus</td>
<td>ModbusTCP Invalid Function Code</td>
<td>192.168.3.201:54047 ⇔ 192.168.3.30:502</td>
<td>Function Code 'Read Coils (1)' de...</td>
</tr>
</tbody>
</table>

⚠️ Alert: ModbusTCP Invalid Function Code | 172.16.203.200:3343 ⇔ 172.16.203.5:502 | Overview

<table>
<thead>
<tr>
<th>Alert</th>
<th>ModbusTCP Invalid Function Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol / Application</td>
<td>TCP:Modbus</td>
</tr>
<tr>
<td>Date/Time</td>
<td>12:05:46</td>
</tr>
<tr>
<td>Score</td>
<td>200</td>
</tr>
<tr>
<td>Description</td>
<td>Function Code 'Write Single Register (6)' detected</td>
</tr>
<tr>
<td>Other Issues</td>
<td>ModbusTCP Too Many Exceptions</td>
</tr>
<tr>
<td>Traffic Info</td>
<td><strong>Client to Server Traffic</strong>: 82.15 KB</td>
</tr>
<tr>
<td></td>
<td><strong>Main Direction</strong>: Server → Client</td>
</tr>
<tr>
<td></td>
<td><strong>Server to Client Traffic</strong>: 139.95 KB</td>
</tr>
</tbody>
</table>
Aggregated Flows
ClickHouse Historical Flows

• ntopng has the ability to:
  ◦ Dump historical flows into ClickHouse.
  ◦ Correlate flows with alerts.
  ◦ Download (n2disk is required) flows with traffic traces.
• Historical flows can be heavy (hundred of million/day) and exhaust disk space.
• What if we can aggregate flows, save disk space, and still have the ability to have accurate “Top X” and alert correlation?
Aggregated Flows [1/2]
Aggregated Flows [2/2]

• Typical savings ratio: 133M vs 648K (1:200)

Processed 12,934,942 records [133,967,482 records/sec].

• Flexible Settings

- ClickHouse Aggregated Flows Data Retention
  Number of days to keep aggregated flows informations (it must be larger than unaggregated flows retention). Default: 60 days.

- ClickHouse Limit Aggregated Flows
  Number of maximum aggregated flow entries to insert every hourly dump.

- ClickHouse Minimum Aggregated Flow Traffic
  Discard aggregated flows whose size is less than the specified value (in Kbytes).

- Include Alerted Flows
  Include all alerted flows in aggregated flows.

• Next Step: Aggregate Alerts
Zoom and MS Teams Monitoring
Zoom/MS Teams Monitoring [1/2]

• nDPI has been enhanced...

- 38 Skype_TeamsCall TCP Acceptable VoIP
- 125 Skype_Teams UDP Acceptable VoIP
- 189 Zoom TCP Acceptable Video
- 250 Teams TCP Safe Collaborative

• nProbe has been Enhanced to handle STUN/RTP flows with “non-standard”

```plaintext
[NFv9 57626] [IPFIX 35632.154] [Len 4] %RTP_IN_JITTER
[NFv9 57627] [IPFIX 35632.155] [Len 4] %RTP_OUT_JITTER
[NFv9 57628] [IPFIX 35632.156] [Len 4] %RTP_PKT_LOST
[NFv9 57629] [IPFIX 35632.157] [Len 4] %RTP_OUT_PKT_LOST
[NFv9 57902] [IPFIX 35632.430] [Len 4] %RTP_IN_PKT_DROP
[NFv9 57903] [IPFIX 35632.431] [Len 4] %RTP_OUT_PKT_DROP
[NFv9 57632] [IPFIX 35632.160] [Len 4] %RTP_PKT_TYPE
[NFv9 57630] [IPFIX 35632.158] [Len 4] %RTP_OUT_PKT_TYPE
[NFv9 57631] [IPFIX 35632.159] [Len 4] %RTP_IN_MAX_DELTA
[NFv9 57632] [IPFIX 35632.160] [Len 4] %RTP_OUT_MAX_DELTA
[NFv9 57820] [IPFIX 35632.348] [Len 64 varlen] %RTP_SIP_CALL_ID
[NFv9 57906] [IPFIX 35632.434] [Len 4] %RTP_MOS
[NFv9 57842] [IPFIX 35632.370] [Len 4] %RTP_IN_MOS
[NFv9 57904] [IPFIX 35632.432] [Len 4] %RTP_OUT_MOS
[NFv9 57908] [IPFIX 35632.436] [Len 4] %RTP_R_FACTOR
[NFv9 57843] [IPFIX 35632.371] [Len 4] %RTP_IN_R_FACTOR
[NFv9 57905] [IPFIX 35632.433] [Len 4] %RTP_OUT_R_FACTOR
[NFv9 57853] [IPFIX 35632.381] [Len 4] %RTP_IN_TRANSIT
[NFv9 57854] [IPFIX 35632.382] [Len 4] %RTP_OUT_TRANSIT
[NFv9 57852] [IPFIX 35632.380] [Len 4] %RTP_RTT
```

- RTP jitter (ms * 1000)
- RTP jitter (ms * 1000) Packet lost in stream (src->dst)
- RTP jitter (ms * 1000) Packet discarded by Jitter Buffer (src->dst)
- RTP payload type
- RTP payload type
- Max delta (ms*100) between consecutive pkts (src->dst)
- Max delta (ms*100) between consecutive pkts (dst->src)
- SIP call-id corresponding to this RTP stream
- RTP pseudo-MOS (value * 100) (average both directions)
- RTP pseudo-MOS (value * 100) (src->dst)
- RTP pseudo-MOS (value * 100) (dst->src)
- RTP pseudo-R_FACTOR (value * 100) (average both directions)
- RTP pseudo-R_FACTOR (value * 100) (src->dst)
- RTP pseudo-R_FACTOR (value * 100) (dst->src)
- RTP Transit (value * 100) (src->dst)
- RTP Transit (value * 100) (dst->src)
- RTP Round Trip Time (ms)
Zoom/MS Teams Monitoring [2/2]

• And ntopng too…

---

### Skype_TeamsCall Flows

<table>
<thead>
<tr>
<th>Serial</th>
<th>Application</th>
<th>Proto</th>
<th>Client</th>
<th>Server</th>
<th>Duration</th>
<th>Score</th>
<th>Breakdown</th>
<th>Actual Thpt</th>
<th>Total Bytes</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>STUN.Skype_T</td>
<td>UDP</td>
<td>imacm1</td>
<td>192.168.1.128</td>
<td>&lt; 1 sec</td>
<td>50</td>
<td>Client</td>
<td>0 bps</td>
<td>726.86 KB</td>
<td>Audio Stream</td>
</tr>
<tr>
<td></td>
<td>STUN.Skype_T</td>
<td>UDP</td>
<td>imacm1</td>
<td>50004</td>
<td>&lt; 1 sec</td>
<td>50</td>
<td>Server</td>
<td>0 bps</td>
<td>400.04 KB</td>
<td>Screen Sharing Stream</td>
</tr>
<tr>
<td></td>
<td>STUN.Skype_T</td>
<td>UDP</td>
<td>imacm1</td>
<td>50004</td>
<td>&lt; 1 sec</td>
<td>50</td>
<td>Server</td>
<td>0 bps</td>
<td>400.04 KB</td>
<td>Screen Sharing Stream</td>
</tr>
<tr>
<td></td>
<td>STUN.Skype_T</td>
<td>UDP</td>
<td>imacm1</td>
<td>50004</td>
<td>&lt; 1 sec</td>
<td>50</td>
<td>Server</td>
<td>0 bps</td>
<td>400.04 KB</td>
<td>Screen Sharing Stream</td>
</tr>
<tr>
<td></td>
<td>STUN.Skype_T</td>
<td>UDP</td>
<td>imacm1</td>
<td>50004</td>
<td>&lt; 1 sec</td>
<td>50</td>
<td>Server</td>
<td>0 bps</td>
<td>400.04 KB</td>
<td>Screen Sharing Stream</td>
</tr>
<tr>
<td></td>
<td>STUN.Skype_T</td>
<td>UDP</td>
<td>imacm1</td>
<td>50004</td>
<td>&lt; 1 sec</td>
<td>50</td>
<td>Server</td>
<td>0 bps</td>
<td>400.04 KB</td>
<td>Screen Sharing Stream</td>
</tr>
<tr>
<td></td>
<td>STUN.Skype_T</td>
<td>UDP</td>
<td>imacm1</td>
<td>50004</td>
<td>&lt; 1 sec</td>
<td>50</td>
<td>Server</td>
<td>0 bps</td>
<td>400.04 KB</td>
<td>Screen Sharing Stream</td>
</tr>
<tr>
<td></td>
<td>STUN.Skype_T</td>
<td>UDP</td>
<td>imacm1</td>
<td>50004</td>
<td>&lt; 1 sec</td>
<td>50</td>
<td>Server</td>
<td>0 bps</td>
<td>400.04 KB</td>
<td>Screen Sharing Stream</td>
</tr>
</tbody>
</table>

---

**Flow: 192.168.1.29:50014 → 82.51.138.80:59225 | Overview**

**Flow Peers [ Client / Server ]**


**Protocol / Application**

UDP / STUN.Skype_TeamsCall (VoIP) [Confidence: DPI] [Audio Stream]
Finally… OpenAPI
Presentation Outline

- SNMP Devices Rules
- Host/Network Interface Rules
- Server Ports Analysis Page

PS: All the features displayed on this presentation are available only from Enterprise L license or superior.

Nicolo’ Maio
maio@ntop.org
SNMP Devices Rules [1/3]

• Monitoring several SNMP devices in order to unveil changes and changed trends in traffic, can be difficult.

• SNMP Devices Rules enables the creation of periodic checks (for all or a selected SNMP device) at a specific frequency (5 mins, 1 hour, or 1 day).

• The triggered rules will emit a “Threshold Crossed” alert when a SNMP Device exceeds (up or down) the specified threshold (Packets, Bytes or Interface Errors).

• Available only from Enterprise L license or superior.
SNMP Devices Rules [2/3]

- Select the SNMP device
- Select the SNMP device port
- Select the metric
- Select the check frequency
- Select the rule threshold

**NOTES**
- Device: select the SNMP Device to be analyzed
- Interface: select the interface of the SNMP device that needs to be analyzed.
- Metric: select the metric to be analyzed (e.g., errors -> the SNMP metric errors)
- Frequency: select the frequency of the analysis (e.g., 5 Min -> analyzed every 5 minutes)
- Threshold: select the type of threshold (Volume, Throughput or Percentage), lowerbound or upperbound, and the threshold that, if exceeded, is going to trigger an alert
- Percentage Threshold: is calculated between the last two frequency checks (e.g., <1% with frequency 5 Min -> if the difference between precedent frequency and the last 5 minutes check is lower than 1% trigger and alert)
SNMP Devices Rules [3/3]

<table>
<thead>
<tr>
<th>Device IP</th>
<th>SNMP Interface</th>
<th>SNMP Device Name</th>
<th>Counts</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.2.237</td>
<td>X435-24P-4S Port 2</td>
<td>X435-24P-4S</td>
<td>1</td>
<td>Metric: Bytes (RX/TX) / Unit: Volume / Value: 0 Bytes / Threshold: &lt; 1 GB</td>
</tr>
<tr>
<td>192.168.2.237</td>
<td>X435-24P-4S Port 7</td>
<td>X435-24P-4S</td>
<td>1</td>
<td>Metric: Bytes (RX/TX) / Unit: Volume / Value: 0 Bytes / Threshold: &lt; 1 GB</td>
</tr>
<tr>
<td>192.168.2.237</td>
<td>X435-24P-4S Port 15</td>
<td>X435-24P-4S</td>
<td>1</td>
<td>Metric: Bytes (RX/TX) / Unit: Volume / Value: 0 Bytes / Threshold: &lt; 1 GB</td>
</tr>
<tr>
<td>192.168.2.237</td>
<td>X435-24P-4S Port 14</td>
<td>X435-24P-4S</td>
<td>1</td>
<td>Metric: Bytes (RX/TX) / Unit: Volume / Value: 0 Bytes / Threshold: &lt; 1 GB</td>
</tr>
<tr>
<td>192.168.2.237</td>
<td>X435-24P-4S Port 15</td>
<td>X435-24P-4S</td>
<td>1</td>
<td>Metric: Bytes (RX/TX) / Unit: Volume / Value: 0 Bytes / Threshold: &lt; 1 GB</td>
</tr>
</tbody>
</table>
Host/Interface Rules [1/3]

• Same as SNMP Rules but for hosts and interfaces.
• Frequency of 5 mins, 1 hour or 1 day.
• The triggered rules will emit a “Threshold Crossed” alert when a Host or a Network Interface exceeds (up or down) the specified threshold (Traffic, Score or Specific Application Traffic).
• Available only from Enterprise L license or superior.
Host/Interface Rules [2/3]

In case of Rule Type Host indicate the Host, Otherwise select an Interface

Select the metric

Select the check frequency

Select the rule threshold

NOTES
- Target: insert the IP of a Local Host to be analyzed or a * (meaning that all Local Hosts has to be analyzed) or select a local network interface
- Metric: select the metric to be analyzed (e.g. DNS -> the DNS traffic)
- Frequency: select the frequency of the analysis (e.g. 5 Min -> analyzed every 5 minutes)
- Threshold: select the type of threshold (Volume, Throughput or Percentage), lowerbound or upperbound, and the threshold that, if exceeded, is going to trigger an alert
- Percentage Threshold: is calculated between the last two frequency checks (e.g. <1% with frequency 5 Min -> if the difference between precedent frequency and the last 5 minutes check is lower than 1% trigger and alert)
In Actions menu the edit and delete rule options are present.
Server Ports Analysis [1/2]

- Monitoring available host services is not simple with live traffic view. On the other hand it is important to keep an eye on new or disappeared server port (service map).
- In order to enable it, start selecting a Network Protocol, then an Application Protocol and the server port.
- The page displays many server local host details including:
  - Host IP
  - Host Name
  - MAC address
  - Manufacturer
  - Host Total Score
  - Host Total Flows
  - Host Total Traffic.
- Available only from Enterprise L license or superior.
Server Ports Analysis [2/2]

Select the Protocol

Select the Application

Select the Server port
Behavior Analysis
&
Inactive Hosts
Behavior Analysis (1/2)

• Use algorithms to understand and foresee the behaviors of hosts and interfaces

• See the actual value and the lower/upper bound of the foreseen value
Behavior Analysis (2/2)

The value exceeds the lower or upper bound

↓

Trigger the corresponding alert
Inactive Hosts Analysis (1/2)

• Which Host is active and which is inactive?
• When was active the last time on the net?
• Which MAC address did it have?
• First time in ntopng that inactive data are shown (usually only live data are present)
Inactive Hosts Analysis (2/2)

### Local Hosts

<table>
<thead>
<tr>
<th>Actions</th>
<th>IP Address</th>
<th>VLAN</th>
<th>MAC Address</th>
<th>Name</th>
<th>First Seen</th>
<th>Last Seen</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>192.168.2.209</td>
<td>00:0C:29:22:E5:66</td>
<td>fe80:20cc29ff:fe22:e566</td>
<td></td>
<td>08:00:15</td>
<td>08:00:16</td>
</tr>
<tr>
<td></td>
<td>192.168.2.209</td>
<td>00:0C:29:22:E5:66</td>
<td>192.168.2.209</td>
<td></td>
<td>08:00:16</td>
<td>08:00:17</td>
</tr>
<tr>
<td></td>
<td>192.168.2.209</td>
<td>00:0C:29:22:E5:66</td>
<td>192.168.2.209</td>
<td></td>
<td>08:00:16</td>
<td>08:00:17</td>
</tr>
<tr>
<td></td>
<td>192.168.2.209</td>
<td>00:0C:29:22:E5:66</td>
<td>192.168.2.209</td>
<td></td>
<td>08:00:16</td>
<td>08:00:17</td>
</tr>
</tbody>
</table>

Showing page 1 of 1: total 7 rows.
ntopng New UI
Timeseries (1/2)
Timeseries (1/2)

• Lowered loading time (4/5 s ~> below 1 s)
• More responsive
• More user friendly
Tables Refactoring (1/3)
Tables Refactoring (2/3)

- Reworked tables (homeproduct)
- Hastened loading
- Change the length of columns
- Remove/Add columns
Tables Refactoring (3/3)

Click between columns and you can change the length of the columns.
Smart Recording
Continuous Recording

• In most cases it’s not possible to predict when a network event occurs
• In order to drill down up to the packet level:
  ◦ We need to record traffic 24/7
  ◦ On-demand capture is not an option
Data Retention

• Data retention depends on traffic rate and storage size

• Example:

<table>
<thead>
<tr>
<th>Traffic rate</th>
<th>10 Gbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data on disk</td>
<td>1,2 GB/s</td>
</tr>
<tr>
<td>Data on disk</td>
<td>4 TB/h</td>
</tr>
<tr>
<td>Data on disk</td>
<td>100 TB/day</td>
</tr>
</tbody>
</table>

• 10x at 100 Gbps
Saving Space

• Packet compression: save up to 5% on Internet traffic (more on LAN traffic)
• Packet slicing: good if interested in headers only
• BPF filtering: difficult to predict
• L7 filtering: good to discard or shunt unwanted traffic (e.g. encrypted, compressed, multimedia)
Not all traffic is alike

• What if our storage does not satisfy the desired data retention, even after filtering?

• Assumption: traffic matching Network events is more important than the rest of the traffic

• What we need is:
  ◦ Prioritize selected traffic (e.g. security alerts)
  ◦ Smart data recycling: delete traffic which is not matching any event first
Smart Data Retention

• Process Network events generated by ntopng
• Use a 1st level storage to implement continuous recording with a short data retention (cache)
• Use a 2nd level storage to archive traffic for Network events with a longer data retention (archive)
Continuous Recording
Continuous Recording

PCAP Data

Start
Continuous Recording

PCAP Data

Start
Continuous Recording

PCAP Data

Start
Continuous Recording

Start -> PCAP Data -> Max Window Size
Continuous Recording

Max Window Size

PCAP Data

Start
Continuous Recording

PCAP Data

Start

Event
Continuous Recording
Continuous Recording

PCAP Data

Start

Event
Smart Recording

- Archive
- Cache
- Start
Smart Recording

Start

Cache

Archive
Smart Recording
Smart Recording

- Archive
- Cache
- Start
- Event
Smart Recording
Smart Recording
Smart Recording

Start → Archive → Cache → Event → Smart Recording
Smart Recording

- Archive
- Cache
- Start
- Event

Smart Recording
Smart Recording
Smart Recording

(Much Wider) Window Size

Archive

Cache

Start

Event
Suricata and Zeek at 100 Gbit
IDS Acceleration

IDS/IPS
Suricata, Zeek, ...
IDS Acceleration

IDS/IPS
Suricata, Zeek, ...

PF_RING
IDS Acceleration

IDS/IPS
Suricata, Zeek, ...

SURICATA

PF_RING ZC

NVIDIA ConnectX

ntop Webinar - June 20th, 2023 © ntop.org
IDS Acceleration

IDS/IPS
Suricata, Zeek, ...

PF_RING FT
L7 Filtering

Discard TLS, Netflix, Youtube, Spotify, ...

PF_RING

NVIDIA
ConnectX
Suricata and Zeek On Demand

IDS/IPS
Suricata, Zeek, ...

Discard all traffic by default
Suricata and Zeek On Demand

IDS/IPS
Suricata, Zeek, ...

SURICATA

PF_RING

NVIDIA
ConnectX

ntopng
Enterprise
Suricata and Zeek On Demand

IDS/IPS
Suricata, Zeek, ...

PF_RING

NVIDIA ConnectX

100 Gbit

ntopng
Enterprise

Flows

nProbe Cento

ntop Webinar - June 20th, 2023 © ntop.org
Suricata and Zeek On Demand
Suricata and Zeek On Demand

IDS/IPS
Suricata, Zeek, ...

PF_RING

Selected Traffic

Ban/Unban Events

Hardware Rules

Full Traffic

NVIDIA ConnectX

ntopng Enterprise

ntop Webinar - June 20th, 2023 © ntop.org
Cloud License
Remote Traffic Analysis

- Remote Probe
- Flows
- Centralized Collector

- nProbe
- ntopng
Remote Traffic Analysis

SPAN or TAP → Packets → Remote Probe → nProbe

Flows → Centralized Collector → ntopng

ntop Webinar - June 20th, 2023 © ntop.org
Remote Traffic Analysis

NetFlow
IPFIX
sFlow

Remote Probe

nProbe

Flows

Centralized Collector

ntopng
Remote Traffic Analysis

Remote Probe -> nProbe License

nProbe

Flows

Centralized Collector -> ntopng License

ntopng
With Many Probes

nProbe License A  nProbe License B  nProbe License C  nProbe License D

nProbe  nProbe  nProbe  nProbe

Flows

ntopng

ntopng License
With (Optional) Encryption

- nProbe License A
- nProbe License B
- nProbe License C
- nProbe License D

Public Key

Encrypted Flows

Public Key

Private Key

ntopng

ntopng License
Cloud License

No per-probe license key required

nProbe → ntopng
nProbe → ntopng
nProbe → ntopng
nProbe → ntopng
Cloud License

Secure (Encrypted Export) by design

nProbe

Cloud Public Key

nProbe

Cloud Public Key

nProbe

Cloud Public Key

nProbe

Cloud Public Key

ntopng

ntopng Cloud License
Bundle vs Cloud License

• Bundle
  ◦ single key unlocking ntopng, nProbe, n2disk (they must run on the same box)

• Cloud
  ◦ automatically unlocks remote nProbe instances
  ◦ Designed for Service Providers
    • License the on-Cloud box and forget about System IDs on the probe side (just distribute the public key)
  ◦ Anyone interested in early adoption? Contact us!
NTOPCONF '23

SEPTEMBER 21 (TRAINING)-22 (CONFERENCE), 2023

Submission Deadline
JUNE 30TH, 2023