nDPI-based Traffic Enforcement

Merging Visibility and Cybersecurity

Luca Deri <deri@ntop.org>
@lucaderi
20+ Years of OpenSource
Presentation Goals

• Show how nDPI can be used for both visibility and security.

• Present ntop work on traffic enforcement and show how this is integrated in the ecosystem.

• Demonstrate ntop tools on popular security-oriented platforms such as OPNsense and pfSense.
20+ Years of Network Monitoring

• Increased speed:
  ◦ 10Gbit is now commodity for companies.
  ◦ 100 Gbit is standard for ISPs.

• Monitoring Protocols
  ◦ Still NetFlow and sFlow, just at higher speed.

• Monitoring Metrics
  ◦ Bytes and packets are still the main metrics for many network vendors.
Cybersecurity and Network Observability

• Observability: The ability to ask any question about your network, including security.

• Cybersecurity is an important piece of observability as this is unfortunately a popular topic in the news.

• Backbone: volumetric attacks (DDoS) and BGP traffic monitoring/hijacking are two popular attacks and many mitigation solutions are already in place.

• Edge/Enterprise: traditional ntop playgoing and where most network threats happen.
Cybersecurity and Network Edge

• As edge network speed is increasing, security threats on customer networks can propagate the issue to the core.

• Data centers with unhealthy customer traffic can affect neighbours and decrease the whole network reputation score.

• Limiting traffic observability to bandwidth usage is no longer wise: it is time to monitor customer traffic in an unobtrusive way in order to report users threats they have not detected, mitigate issues (as you do with DDoS) and implement a healthier Internet.
Welcome to nDPI

• In 2012 we decided to develop our own GNU LGPL DPI toolkit order to build an open source DPI layer.

• Protocols supported exceed 250+ and include:
  ◦ P2P (BitTorrent)
  ◦ Messaging (Viber, Whatsapp, Telegram, Facebook)
  ◦ Multimedia (YouTube, Last.gm, iTunes)
  ◦ Conferencing (Skype, Webex, Teams, Meet, Zoom)
  ◦ Streaming (Zattoo, Disney, Netflix)
  ◦ Business (VNC, RDP, Citrix)
  ◦ Gaming
nDPI Traffic Analysis

Layer 4 Protocol

TCP / HTTP

Layer 7 Protocol

Good or Bad?
nDPI in Cybersecurity

- Analyses **encrypted** traffic to detect issues hidden but un-inspectable payload content.
- Extracts metadata from selected protocols (e.g. DNS, HTTP, TLS..) and matches it against known algorithms for detecting selected threats (e.g. DGA hosts, Domain Generated Algorithm, JA3, blacklists…).
- Associates a “**risk**” with specific flows to identify communications that are affected by security issues.
nDPI: Flow Risks

- HTTP suspicious user-agent
- HTTP numeric IP host contacted
- HTTP suspicious URL
- HTTP suspicious protocol header
- TLS connections not carrying HTTPS (e.g. a VPN over TLS)
- Suspicious DGA domain contacted
- Malformed packet
- SSH/SMB obsolete protocol or application version
- TLS suspicious ESNI usage
- Unsafe Protocol used
- Suspicious DNS traffic
- TLS with no SNI
- XSS (Cross Site Scripting)
- SQL Injection

- Arbitrary Code Injection/Execution
- Binary/.exe application transfer (e.g. in HTTP)
- Known protocol on non standard port
- TLS self-signed certificate
- TLS obsolete version
- TLS weak cipher
- TLS certificate expired
- TLS certificate mismatch
- DNS suspicious traffic
- HTTP suspicious content
- Risky ASN
- Risky Domain Name
- Malicious JA3 Fingerprint
- Malicious SHA1 Certificate
- Desktop of File Sharing Session
- TLS Uncommon ALPN

Legenda: Clear Text Only, Encrypted/Plain Text, Encrypted Only
nDPI Encrypted Traffic Analysis


TCP 10.9.25.101:49165 <-> 144.91.69.195:80 [byte_dist_mean: 95.694525][byte_dist_std: 25.418150][entropy: 0.000000][total_entropy: 0.000000][score: 0.9943][proto: 7/HTTP][cat: Web/5][203 pkts/11127 bytes <-> 500 pkts/706336 bytes][Goodput ratio: 1/96][5.18 sec][Host: 144.91.69.195][bytes ratio: -0.969 (Download)][IAT c2s/s2c min/avg/max/stddev: 0/0 23/9 319/365 49/37][Pkt Len c2s/s2c min/avg/max/stddev: 54/54 55/1413 207/1514 11/134][URL: 144.91.69.195/solar.php][StatusCode: 200][ContentType: application/octet-stream][UserAgent: pwtyyEKZhGatwn3jmCcBLb0veCVpc][Risk: ** Binary application transfer **][PLAIN TEXT (GET /solar.php HTTP/1.1)]

Trickbot Traffic
nDPI in Wireshark

https://sharkfesteurope.wireshark.org
From Flow Risk To Score [1/4]

- Flow traffic analysis is too granular and it needs to be consolidated into:
  - Network Interface
  - Host/Network/Customer.
  - ASN/country

- In essence that is the pillar for creating a (client/server) numerical score that can be quickly used to spot issues (network, security...).
## From Flow Risk To Score [2/4]

<table>
<thead>
<tr>
<th>Id</th>
<th>Risk</th>
<th>Severity</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>XSS attack</td>
<td>Severe</td>
<td>250</td>
</tr>
<tr>
<td>2</td>
<td>SQL injection</td>
<td>Severe</td>
<td>250</td>
</tr>
<tr>
<td>3</td>
<td>RCE injection</td>
<td>Severe</td>
<td>250</td>
</tr>
<tr>
<td>4</td>
<td>Binary application transfer</td>
<td>Severe</td>
<td>250</td>
</tr>
<tr>
<td>5</td>
<td>Known protocol on non standard port</td>
<td>Low</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>Self-signed Certificate</td>
<td>Medium</td>
<td>50</td>
</tr>
<tr>
<td>7</td>
<td>Obsolete TLS version (&lt; 1.1)</td>
<td>Medium</td>
<td>50</td>
</tr>
<tr>
<td>8</td>
<td>Weak TLS cipher</td>
<td>Medium</td>
<td>50</td>
</tr>
<tr>
<td>9</td>
<td>TLS Expired Certificate</td>
<td>High</td>
<td>100</td>
</tr>
<tr>
<td>10</td>
<td>TLS Certificate Mismatch</td>
<td>High</td>
<td>100</td>
</tr>
<tr>
<td>11</td>
<td>HTTP Suspicious User-Agent</td>
<td>Medium</td>
<td>50</td>
</tr>
<tr>
<td>12</td>
<td>HTTP Numeric IP Address</td>
<td>Low</td>
<td>10</td>
</tr>
<tr>
<td>13</td>
<td>HTTP Suspicious URL</td>
<td>High</td>
<td>100</td>
</tr>
<tr>
<td>14</td>
<td>HTTP Suspicious Header</td>
<td>Medium</td>
<td>50</td>
</tr>
<tr>
<td>15</td>
<td>TLS (probably) not carrying HTTPS</td>
<td>Low</td>
<td>10</td>
</tr>
<tr>
<td>16</td>
<td>Suspicious DGA domain name</td>
<td>High</td>
<td>100</td>
</tr>
<tr>
<td>17</td>
<td>Malformed packet</td>
<td>Low</td>
<td>10</td>
</tr>
<tr>
<td>18</td>
<td>SSH Obsolete Client Version/Cipher</td>
<td>Medium</td>
<td>50</td>
</tr>
<tr>
<td>19</td>
<td>SSH Obsolete Server Version/Cipher</td>
<td>Medium</td>
<td>50</td>
</tr>
<tr>
<td>20</td>
<td>SMB Insecure Version</td>
<td>Medium</td>
<td>50</td>
</tr>
<tr>
<td>21</td>
<td>TLS Suspicious ESNI Usage</td>
<td>Medium</td>
<td>50</td>
</tr>
<tr>
<td>22</td>
<td>Unsafe Protocol</td>
<td>Low</td>
<td>10</td>
</tr>
<tr>
<td>23</td>
<td>Suspicious DNS traffic</td>
<td>Medium</td>
<td>50</td>
</tr>
<tr>
<td>24</td>
<td>SNI TLS extension was missing</td>
<td>Medium</td>
<td>50</td>
</tr>
<tr>
<td>25</td>
<td>HTTP suspicious content</td>
<td>Medium</td>
<td>50</td>
</tr>
<tr>
<td>26</td>
<td>Risky ASN</td>
<td>Medium</td>
<td>50</td>
</tr>
<tr>
<td>27</td>
<td>Risky domain name</td>
<td>Medium</td>
<td>50</td>
</tr>
<tr>
<td>28</td>
<td>Possibly Malicious JA3 Fingerprint</td>
<td>Medium</td>
<td>50</td>
</tr>
<tr>
<td>29</td>
<td>Possibly Malicious SSL Cert. SHA1 Fingerprint</td>
<td>Medium</td>
<td>50</td>
</tr>
<tr>
<td>30</td>
<td>Desktop/File Sharing Session</td>
<td>Low</td>
<td>10</td>
</tr>
<tr>
<td>31</td>
<td>Uncommon TLS ALPN</td>
<td>Medium</td>
<td>50</td>
</tr>
</tbody>
</table>
## From Flow Risk To Score [3/4]

**TCP 192.168.149.129:43535 <-> 51.83.238.219:80**
- [proto: 91.252/TLS.AnyDesk][cat: RemoteAccess/12][2942 pkts/175103 bytes <-> 4001 pkts/2618640 bytes][Goodput ratio: 9/92][55.97 sec][bytes ratio: -0.875 (Download)][IAT c2s/s2c min/avg/max/stddev: 0/0 19/14 7028/7028 153/126][Pkt Len c2s/s2c min/avg/max/stddev: 54/60 60/654 1514/1514 50/618][Risk: ** Known protocol on non standard port **** TLS (probably) not carrying HTTPS **** SNI TLS extension was missing **** Desktop/File Sharing Session **][Risk Score: 80]
- [TLSv1.2][JA3C: 201999283915cc31ce6b15472ef3332][JA3S: 107030a763c7224285717f11569a17f3][Issuer: CN=AnyNet Root CA, O=philandro Software GmbH, C=DE][Subject: C=DE, O=philandro Software GmbH, CN=AnyNet Relay][Certificate SHA-1: 9E:08:D2:58:A9:02:CD:4F:E2:4A:26:B8:48:5C:43:0B:81:29:99:E3][Firefox][Validity: 2018-11-18 02:14:23 – 2028-11-15 02:14:23][Cipher: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384][Plen Bins: 0,7,17,2,1,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,3,0,0,33,0,0,0,29,0,0]

<table>
<thead>
<tr>
<th>Detected Risk</th>
<th>Risk Score Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS (probably) not carrying HTTPS</td>
<td>10</td>
</tr>
<tr>
<td>SNI TLS extension was missing</td>
<td>50</td>
</tr>
<tr>
<td>Desktop/File Sharing Session</td>
<td>10</td>
</tr>
<tr>
<td><strong>Flow Score Total</strong></td>
<td><strong>80</strong></td>
</tr>
</tbody>
</table>
### From Flow Risk To Score [4/4]

<table>
<thead>
<tr>
<th>Name</th>
<th>Category</th>
<th>Description</th>
<th>Values</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blacklisted Country</td>
<td></td>
<td>Trigger an alert when hosts contact or are contacted by the specified countries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blacklisted Flow</td>
<td></td>
<td>Trigger an alert when a blacklisted host or domain is detected</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Exfiltration</td>
<td></td>
<td>Trigger alerts when a possible data-exfiltration activity is detected</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Application Not Allowed</td>
<td></td>
<td>Trigger an alert when an unusual application is detected for a device. Rules can be configured here</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Data Exfiltration</td>
<td></td>
<td>Trigger alerts when a DNS data exfiltration activity is detected</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Elephant Flows</td>
<td></td>
<td>Trigger an alert when a flow exchanges more than the configured bytes volume. The remote to Local direction indicated in...</td>
<td>&gt; 1 GB (L2R), &gt; 1 GB (R2L)</td>
<td></td>
</tr>
<tr>
<td>External Alert</td>
<td></td>
<td>Receives flow alerts from external endpoints (e.g. Sufi)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP Numeric IP Host</td>
<td></td>
<td>HTTP Numeric IP Host</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP Suspicious Header</td>
<td></td>
<td>HTTP Suspicious Header</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP Suspicious URL</td>
<td></td>
<td>HTTP Suspicious URL</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Showing 1 to 10 of 53 rows
Score At Work

All Hosts

<table>
<thead>
<tr>
<th>IP Address</th>
<th>VLAN</th>
<th>Flows</th>
<th>Score</th>
<th>Name</th>
<th>Seen Since</th>
<th>Breakdown</th>
<th>Throughput</th>
<th>Total Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>250</td>
<td>9853</td>
<td>111,320</td>
<td></td>
<td>03:19</td>
<td>34.75 kbit/s</td>
<td>642.7 KB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>250</td>
<td>10254</td>
<td>102,650</td>
<td></td>
<td>09:44:37</td>
<td>47.07 kbit/s</td>
<td>168.32 KB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>250</td>
<td>2231</td>
<td>73,816</td>
<td></td>
<td>09:44:04</td>
<td>18.98 kbit/s</td>
<td>64.26 MB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>250</td>
<td>823</td>
<td>52,938</td>
<td></td>
<td>09:44:03</td>
<td>4.03 kbit/s</td>
<td>21.6 MB</td>
<td></td>
</tr>
</tbody>
</table>

- Number of detected flows
- MAC address list
- Number of remote hosts
- Number of local hosts
- (Active) flows with errors
- (Active) flows with warnings
Score-based Alerts

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Score</th>
<th>Flow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:50:26</td>
<td>120</td>
<td>192.168.1.252:51110</td>
<td>TLS Version: TLSv1</td>
</tr>
<tr>
<td>15:50:26</td>
<td>320</td>
<td>192.168.1.252:51111</td>
<td>Suspicious DGA Domain [<a href="http://www.e5r5p57kbsfmr3j3plz.com">www.e5r5p57kbsfmr3j3plz.com</a>]</td>
</tr>
<tr>
<td>15:50:26</td>
<td>320</td>
<td>192.168.1.252:51112</td>
<td>Suspicious DGA Domain [<a href="http://www.4ynamic3ntop.tun">www.4ynamic3ntop.tun</a> eidl.com]</td>
</tr>
<tr>
<td>15:50:26</td>
<td>146</td>
<td>192.168.1.252:139</td>
<td>Unsafe Protocol</td>
</tr>
<tr>
<td>15:50:26</td>
<td>320</td>
<td>192.168.1.252:0175</td>
<td>Suspicious DGA Domain [<a href="http://www.p5.7bzevox.co">www.p5.7bzevox.co</a>]</td>
</tr>
<tr>
<td>15:50:26</td>
<td>120</td>
<td>192.168.1.252:51113</td>
<td>TLS Version: TLSv1</td>
</tr>
<tr>
<td>15:50:26</td>
<td>120</td>
<td>192.168.1.252:0170</td>
<td>TLS Version: TLSv1</td>
</tr>
<tr>
<td>15:50:26</td>
<td>120</td>
<td>192.168.1.252:5185</td>
<td>TLS Version: TLSv1</td>
</tr>
<tr>
<td>16:00:26</td>
<td>20</td>
<td>192.168.1.1:17600</td>
<td>Remote to Remote</td>
</tr>
<tr>
<td>16:00:26</td>
<td>20</td>
<td>192.168.1.1:17650</td>
<td>Remote to Remote</td>
</tr>
</tbody>
</table>
Score-based Behaviour Analysis
Visualising Cybersecurity: Bubbles

Victim

Attacker

Score as Attacker: 143,620
Score as Victim: 340

Score as Victim: 2000
Score as Attacker: 143,620
Lateral Movement
# Beaconing Detection

## Table

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Client</th>
<th>Server</th>
<th>Port</th>
<th>Observations</th>
<th>Frequency</th>
<th>Last Seen</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP</td>
<td>Luca's iMac</td>
<td></td>
<td></td>
<td>144</td>
<td>3 sec</td>
<td>00:02 ago</td>
<td></td>
</tr>
<tr>
<td>TCP:Google</td>
<td>Luca's iMac</td>
<td></td>
<td>4070</td>
<td>3</td>
<td>120 sec</td>
<td>00:33 ago</td>
<td></td>
</tr>
<tr>
<td>TCP:IMAPS</td>
<td>Luca's iMac</td>
<td></td>
<td>993</td>
<td>3</td>
<td>120 sec</td>
<td>01:04 ago</td>
<td></td>
</tr>
<tr>
<td>TCP:IMAPS</td>
<td>Luca's iMac</td>
<td></td>
<td>993</td>
<td>3</td>
<td>121 sec</td>
<td>01:03 ago</td>
<td></td>
</tr>
<tr>
<td>TCP:IMAPS</td>
<td>Luca's iMac</td>
<td></td>
<td>993</td>
<td>3</td>
<td>120 sec</td>
<td>01:04 ago</td>
<td></td>
</tr>
</tbody>
</table>
From Visibility to Enforcement [1/2]

• In 2018 we have introduced nEdge (online version of ntopng) whose goal was to create a comprehensive, one-click solution, for enforcing traffic policies.
From Visibility to Enforcement [2/3]

Router with NAT

Transparent Bridge

WiFi Router with NAT

Container-based
nEdge Limitations

• Complete Linux distribution: it reconfigures the system to transparently setup everything in one click. Cons: many people want to enrich visibility without adding a new, stand-alone, traffic enforcement component.

• Designed for small/mid-size companies with one/twin Internet link. Cons: distributed networks require multiple instances that need to be configured individually.

• Linux-centric solution Cons: non-Linux platforms are not supported.
Making nProbe Inline [1/3]

- nProbe is a nDPI-aware passive network probe available for Windows, MacOS, Linux, FreeBSD systems.
# Making nProbe Inline: Linux [2/3]

```
# Transparent Bridge
LAN="eth1"
WAN="eth2"
BRIDGE="br0"

iptables -t mangle -A PREROUTING -j CONNMARK --restore-mark
iptables -t mangle -A PREROUTING -m mark --mark 2 -j DROP
iptables -t mangle -A POSTROUTING -j CONNMARK --save-mark

tc qdisc del dev $WAN root 2>/dev/null

tc qdisc add dev $WAN root handle 1: htb default 100

tc class add dev $WAN parent 1: classid 1:1 htb rate "$WAN_SPEED"kbit ceil "$WAN_SPEED"kbit


tc class add dev $WAN parent 1: classid 1:11 htb rate "$STANDARD_BANDWIDTH_POOL"kbit ceil "$WAN_SPEED"kbit burst 15k

tc class add dev $WAN parent 1: classid 1:13 htb rate "$LOW_BANDWIDTH_POOL"kbit ceil "$WAN_SPEED"kbit burst 15k


tc qdisc add dev $WAN parent 1:11 handle 11: sfq perturb 10

tc qdisc add dev $WAN parent 1:13 handle 13: sfq perturb 10


tc filter add dev $WAN parent 1:11 protocol ip handle 51 flow hash keys nfct-src divisor 254


tc filter add dev $WAN parent 1:13 protocol ip handle 53 flow hash keys nfct-src divisor 254

```

In-Kernel Bypass
Making nProbe Inline: FreeBSD [3/3]
## Making nProbe Inline: Performance

<table>
<thead>
<tr>
<th>Device</th>
<th>Vanilla Linux Bridge Only</th>
<th>Linux nProbe IPS</th>
<th>Vanilla FreeBSD Bridge Only</th>
<th>FreeBSD nProbe IPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low End (APU2)</td>
<td>550 Mbps</td>
<td>600 Mbps</td>
<td>1 Gbps</td>
<td>120 Mbps</td>
</tr>
<tr>
<td>Intel E3</td>
<td>10 Gbps / 1.8 Mpps</td>
<td>10 Gbps / 2.4 Mpps</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IPS Configuration: Stand Alone [1/2]

• nProbe IPS enabled with --ips-mode <conf file>
• JSON-based configuration language.

### Pool definition ###

```json
{ "pool": { "id":1, "name": "my pool 1", "ip": [ "192.168.0.1/24", "10.0.0.0/8", "2a03:b0c0:2:0:360:4001/48" ], "mac": [ ] },
  "policy": { "id":1 } }
{ "pool": { "id":2, "name": "my pool 2", "mac": [ "e8:06:88:ff:fe:e4", "02:81:27:b5:f9:f3", "00:01:01:e4:ba:2c" ], "ip": [ "172.16.0.0/16" ] },
  "policy": { "id":2 } }
{ "pool": { "id":3, "name": "my pool 3", "ip": [ "131.114.0.0/16" ], "mac": [ ] },
  "policy": { "id": 3 } }
```

### Policy definition ###

# Continents: Africa / Asia-Pacific / Europe / North America / South America

# Root

```json
{ "policy": { "id": 0, "name": "root rule", "default_marker": "pass", "flow_risk": { "risks": [ 12 ], "marker": "drop" },
  "markers": { "categories": { "Video": "drop" },
              "protocols": { "TLS": "pass" }},
  "countries": { "IT": "pass", "CN": "drop" },
  "continents": { "Asia": "drop" }}}
```

# Rule definition (son of rule 0)

```json
{ "policy": { "id": 1, "root": 0, "name": "my rule 1", "default_marker": "pass", "markers": { "protocols": { "HTTP": "pass" },
  "countries": { "IT": "pass", "CN": "drop" },
  "continents": { "Asia": "drop" }},
  "hostnames": [ "fundingchoicesmessages.google.com": "pass", "www.gstatic.com": "drop", "www.youtube.com": "pass" ]}}
```

# Subrule of rule 1 with more restrictions

```json
{ "policy": { "id": 2, "root":1, "name": "my subrule 2 (son of rule 1)", "default_marker": "drop", "markers": { "protocols": { "53": "pass" }},
  "hostnames": [ "fundingchoicesmessages.google.com": "pass", "www.gstatic.com": "drop", "www.youtube.com": "pass" ]}}
```
IPS Configuration: ntopng Driven [2/2]

- ntopng can be used to
  - Configure nProbe in a graphical fashion.
  - Trigger host blocks based on score and behaviour.

```bash
ntopng -i tcp://192.168.1.10:1234
-1 tcp://192.168.1.30:1234
--zmq-publish-events "tcp://*:9999"
```

```bash
nprobe --zmq "tcp://*:1234" --zmq-publish-events tcp://192.168.1.10:9999
```

```bash
nprobe --zmq "tcp://*:1234" --zmq-publish-events tcp://192.168.1.10:9999
```

```bash
nProbe (192.168.1.20)
n Probe (192.168.1.30)
```
nProbe IPS Mode: (Some) Use Cases

• Drop unwanted protocols (e.g. Tor).
• Block “unclean” traffic (e.g. TLS traffic with self-signed certificates, HTTP traffic with suspicious SQL injection).
• Shape protocols that take a lot of bandwidth (e.g. BitTorrent).
• Prevent specific hosts from being accessed by specific countries or region (e.g. my core servers can be accessed only from USA).
• Drop traffic from/to hosts that have been marked as malware.
• Assign fair bandwidth (Linux only) to protocols by preventing specific protocols (e.g. Netflix or YouTube) to monopolize the bandwidth.
• Block traffic from advertisement servers (similar to PiHole) or blacklisted hosts.
nProbe IPS Mode: Licensing

• Completely stand-alone solution: no cloud access.
• Free add-on to nProbe: no price change or extra license necessary.
• Existing users can update free of charge. No cost licenses for no-profit and education.

<table>
<thead>
<tr>
<th>nProbe Version</th>
<th>Max number of Rules/Pools in IPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pro</td>
<td>4</td>
</tr>
<tr>
<td>Enterprise S</td>
<td>8</td>
</tr>
<tr>
<td>Enterprise M</td>
<td>32</td>
</tr>
<tr>
<td>Enterprise L</td>
<td>256</td>
</tr>
</tbody>
</table>
nProbe IPS Mode: Open Items

• Current software is available in the dev branch and it will be released in the next nProbe stable version (due late June, early July).

• Enforce traffic based on Service and Periodicity map (currently it is only score-based).

• Improve network discovery so that we can create policies for device families and enforce them automatically.

• Your feedback....
Acknowledgements