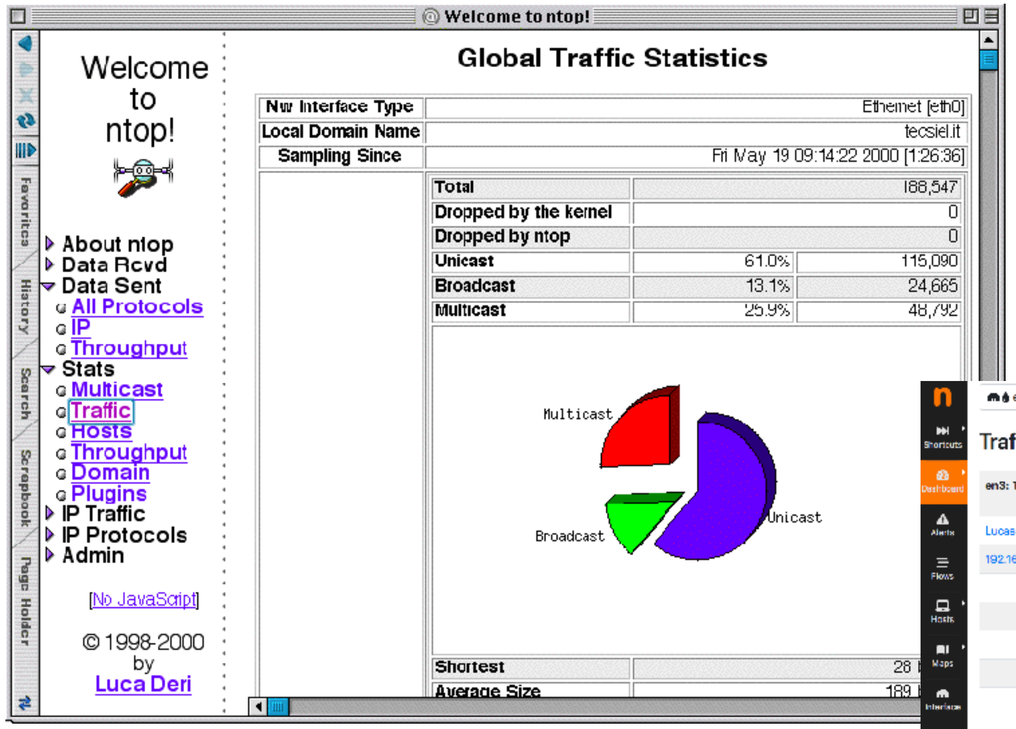
nDPI-based Traffic Enforcement

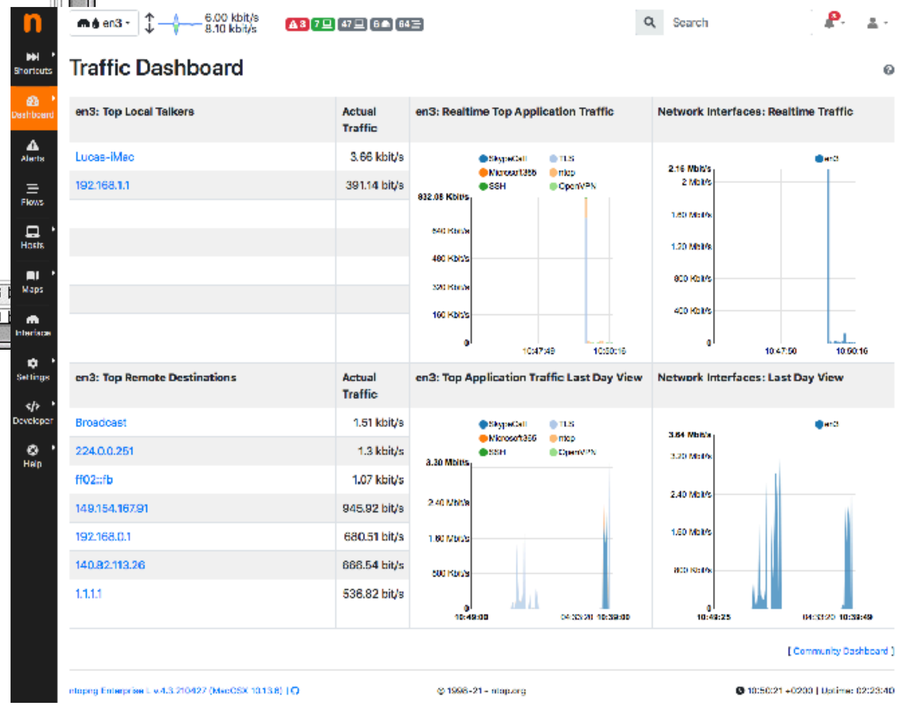
Merging Visibility and Cybersecurity

Luca Deri <deri@ntop.org>
@lucaderi

ntop

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.

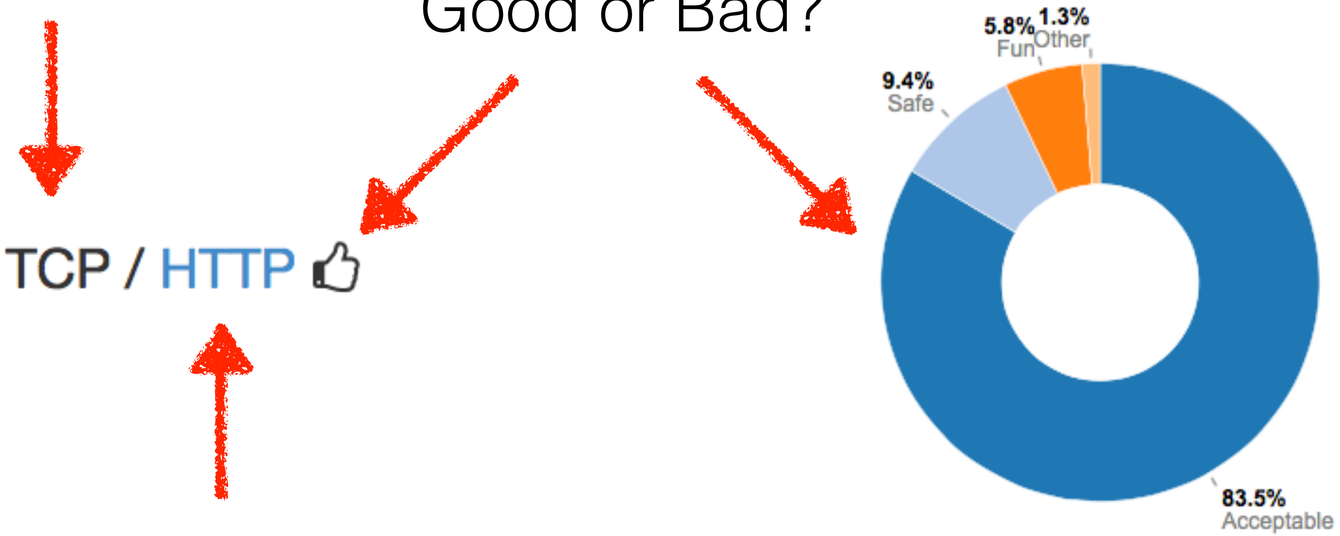
Welcome to nDPI

- 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

Good or Bad?



Layer 7 Protocol

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

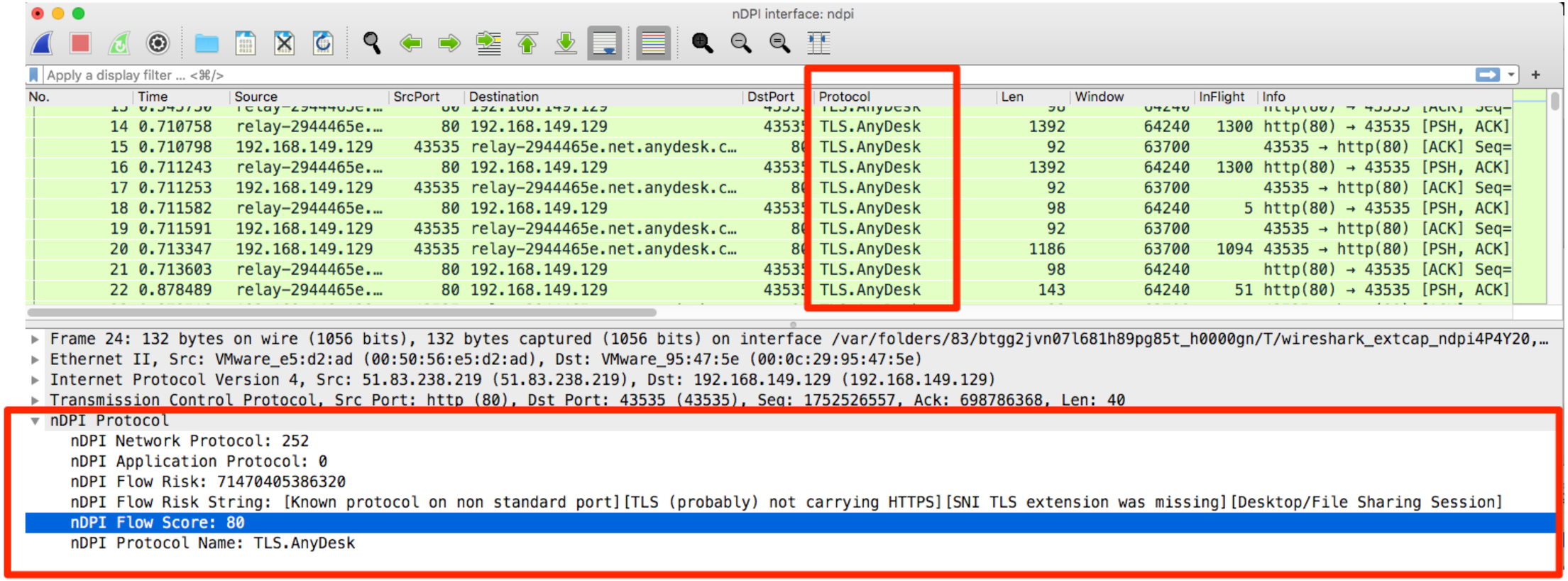
```
TCP 10.9.25.101:49184 <-> 187.58.56.26:449 [byte_dist_mean: 124.148883][byte_dist_std:
58.169660][entropy: 5.892724][total_entropy: 7124.302784][score: 0.9973][proto: 91/TLS]
[cat: Web/5][97 pkts/36053 bytes <-> 159 pkts/149429 bytes][Goodput ratio: 85/94][111.31
sec][bytes ratio: -0.611 (Download)][IAT c2s/s2c min/avg/max/stddev: 0/0 1129/662
19127/19233 2990/2294][Pkt Len c2s/s2c min/avg/max/stddev: 54/54 372/940 1514/1514
530/631][Risk: ** Self-signed Certificate **** Obsolete TLS version (< 1.1) **][TLSv1]
[JA3S: 623de93db17d313345d7ea481e7443cf][Issuer: C=AU, ST=Some-State, O=Internet Widgits
Pty Ltd][Subject: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd][Certificate SHA-1:
DD:EB:4A:36:6A:2B:50:DA:5F:B5:DB:07:55:9A:92:B0:A3:52:5C:AD][Validity: 2019-07-23 10:32:39
- 2020-07-22 10:32:39][Cipher: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA]

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: pwtyyEKzNtGatwnJjmCcBLbOveCVpc][Risk: ** Binary application transfer **][PLAIN
TEXT (GET /solar.php HTTP/1.1)]
```

Trickbot Traffic

nDPI in Wireshark

SharkFest'21 Virtual EUROPE Online • June 14-18

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]

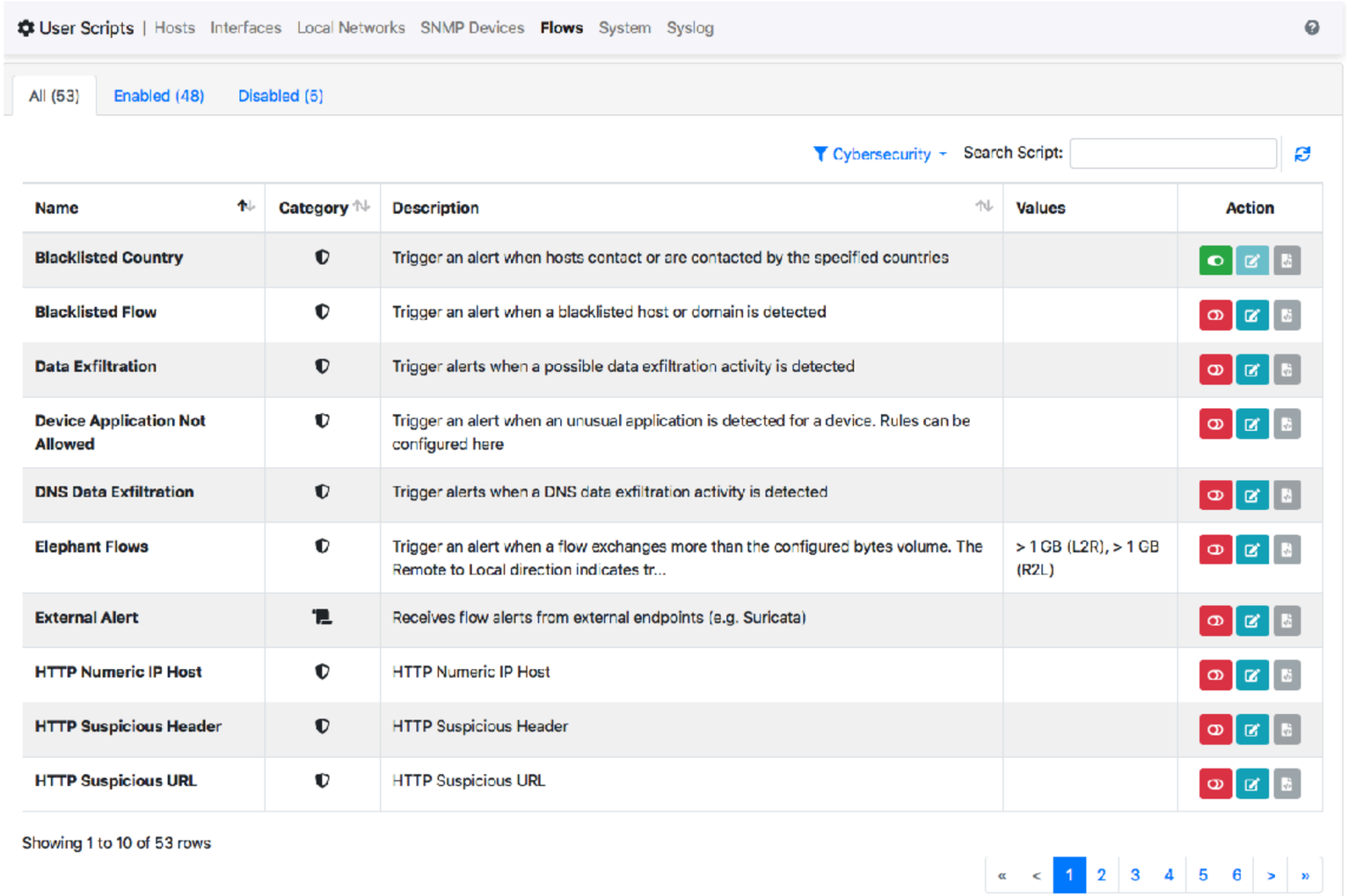
Id	Risk	Severity	Score
1	XSS attack	Severe	250
2	SQL injection	Severe	250
3	RCE injection	Severe	250
4	Binary application transfer	Severe	250
5	Known protocol on non standard port	Low	10
6	Self-signed Certificate	Medium	50
7	Obsolete TLS version (< 1.1)	Medium	50
8	Weak TLS cipher	Medium	50
9	TLS Expired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

From Flow Risk To Score [3/4]

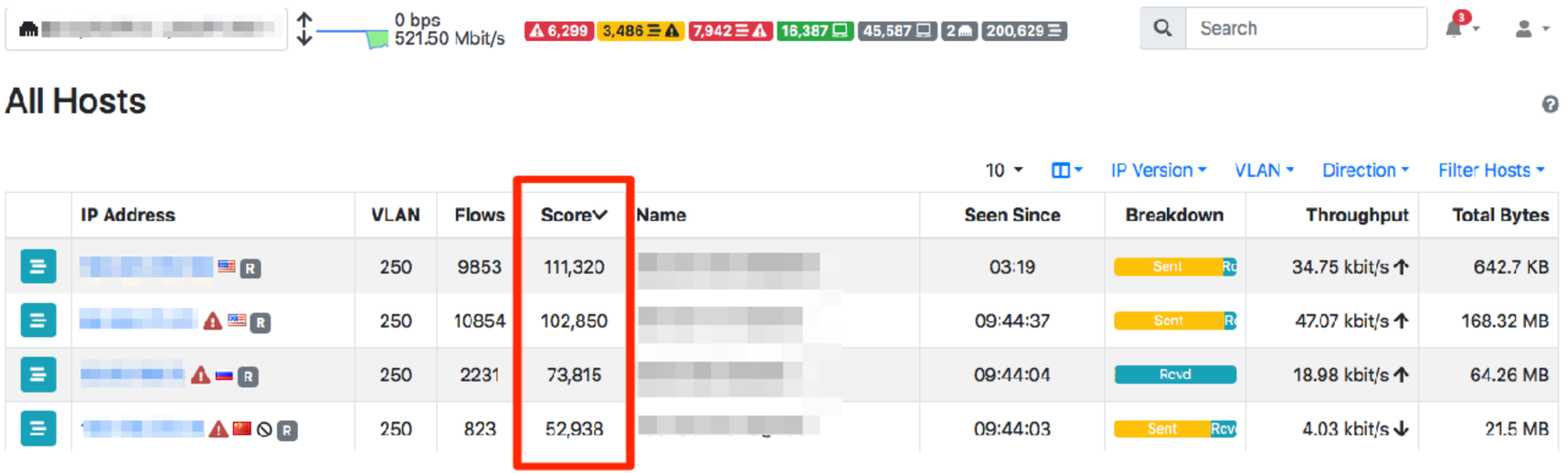
TCP 192.168.149.129:43535 <-> 51.83.238.219:80 [proto: 91.252/**TLS.AnyDesk**][cat: RemoteAccess/12][2942 pkts/175103 bytes <-> 4001 pkts/2618640 bytes][Goodput ratio: 9/92][55.97 sec][bytes ratio: -0.875 (Download)][IAT c2s/s2c min/avg/max/stddev: 0/0 19/14 7028/7028 153/126][Pkt Len c2s/s2c min/avg/max/stddev: 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: 201999283915cc31cee6b15472ef3332][JA3S: 107030a763c7224285717ff1569a17f3][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: 0,7,17,2,1,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,3,0,0,33,0,0,0,0,29,0,0]

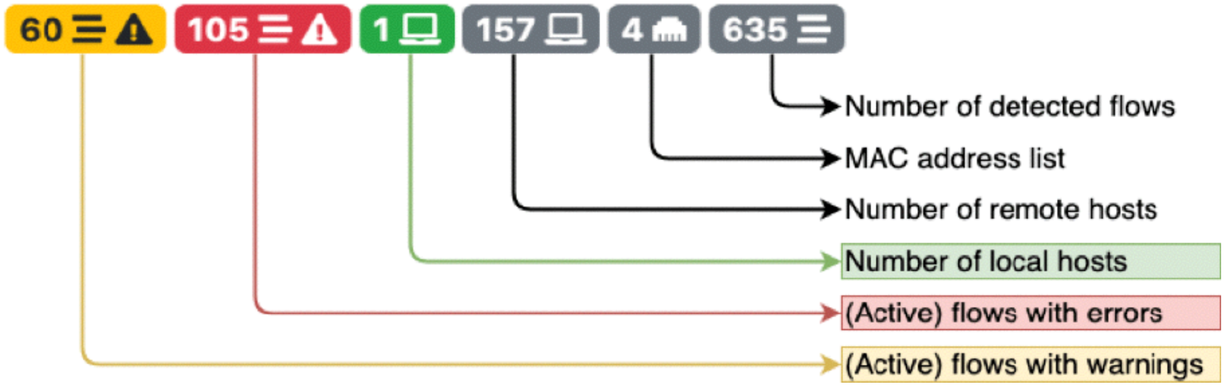
Detected Risk	**Risk Score Value**
TLS (probably) not carrying HTTPS	10
SNI TLS extension was missing	50
Desktop/File Sharing Session	10
Flow Score Total	80

From Flow Risk To Score [4/4]

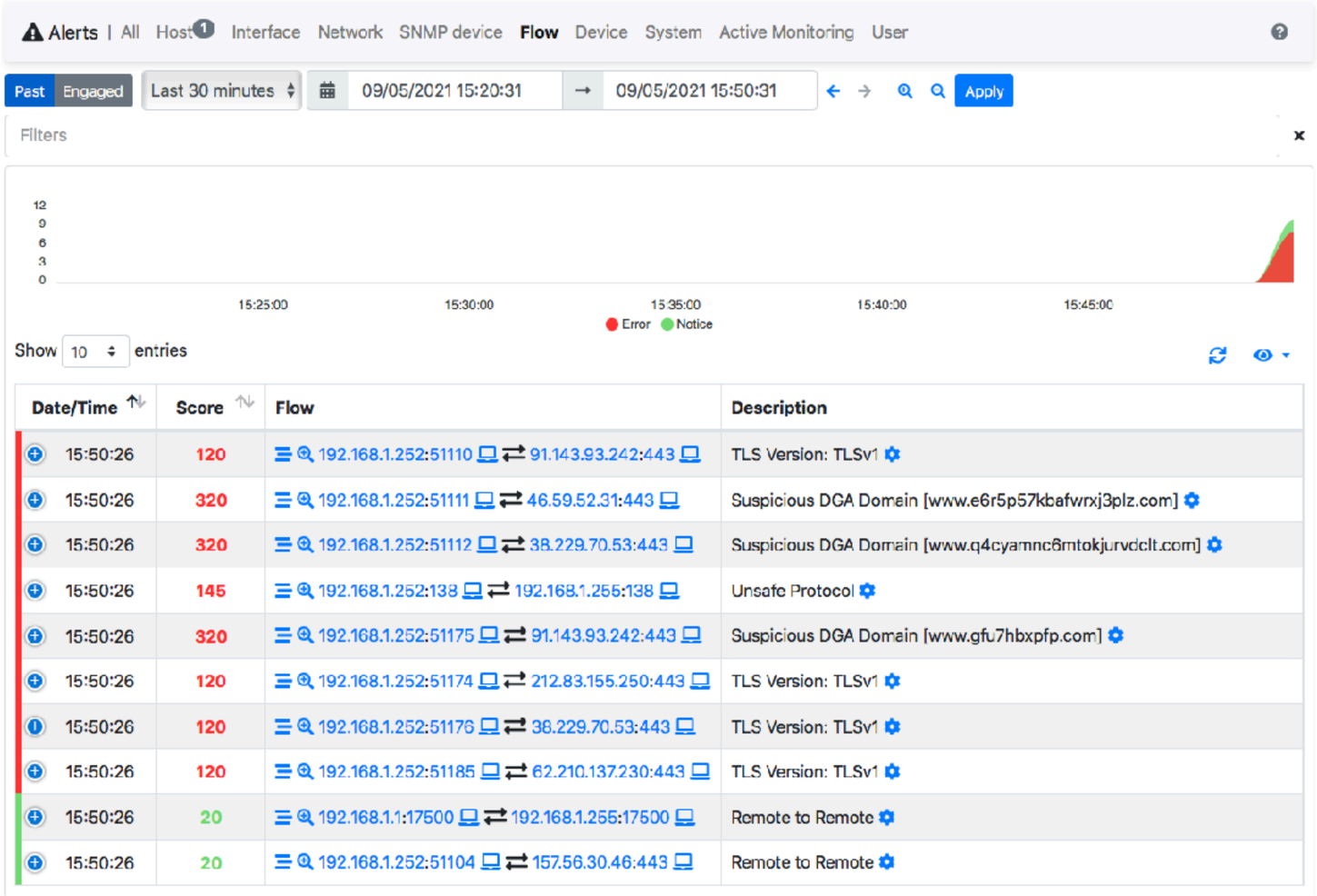


Score At Work



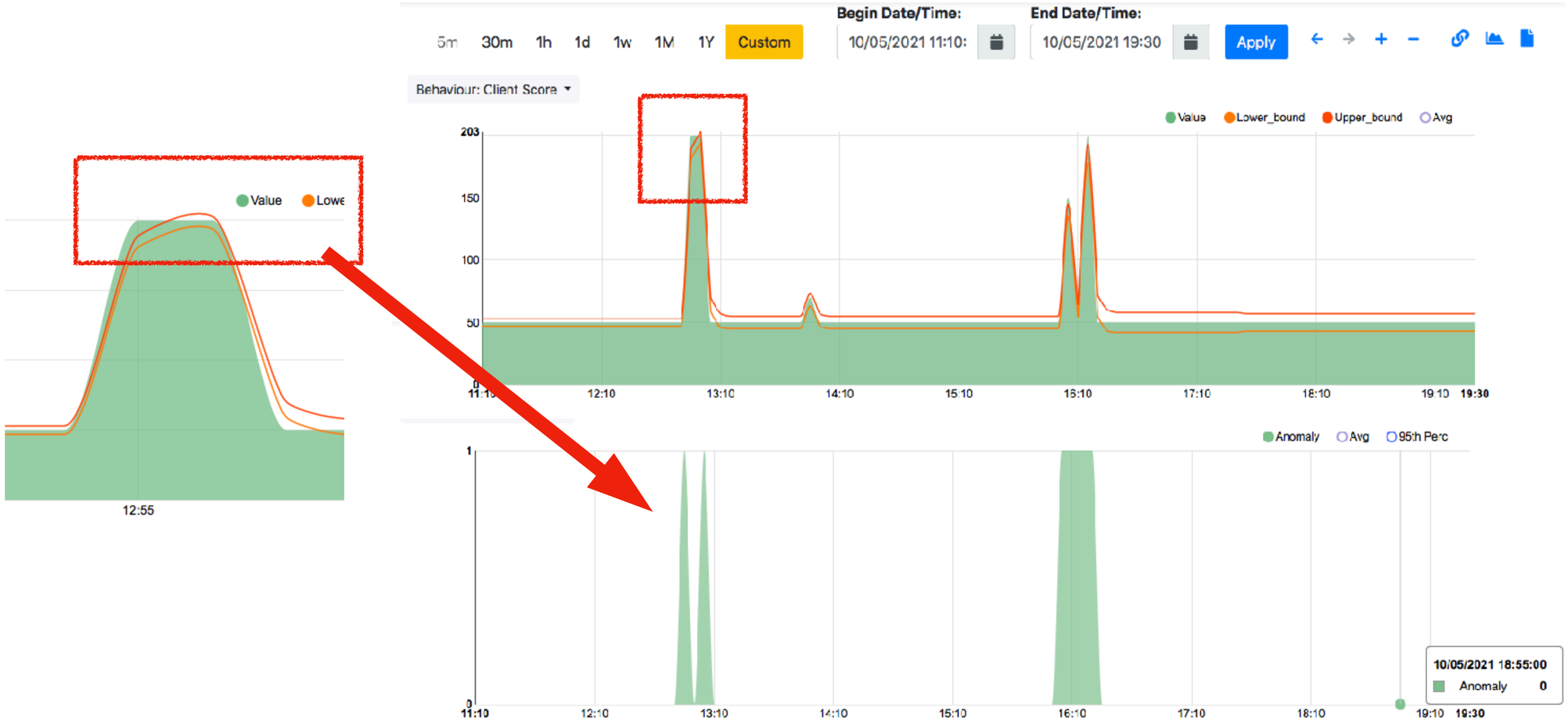


Score-based Alerts

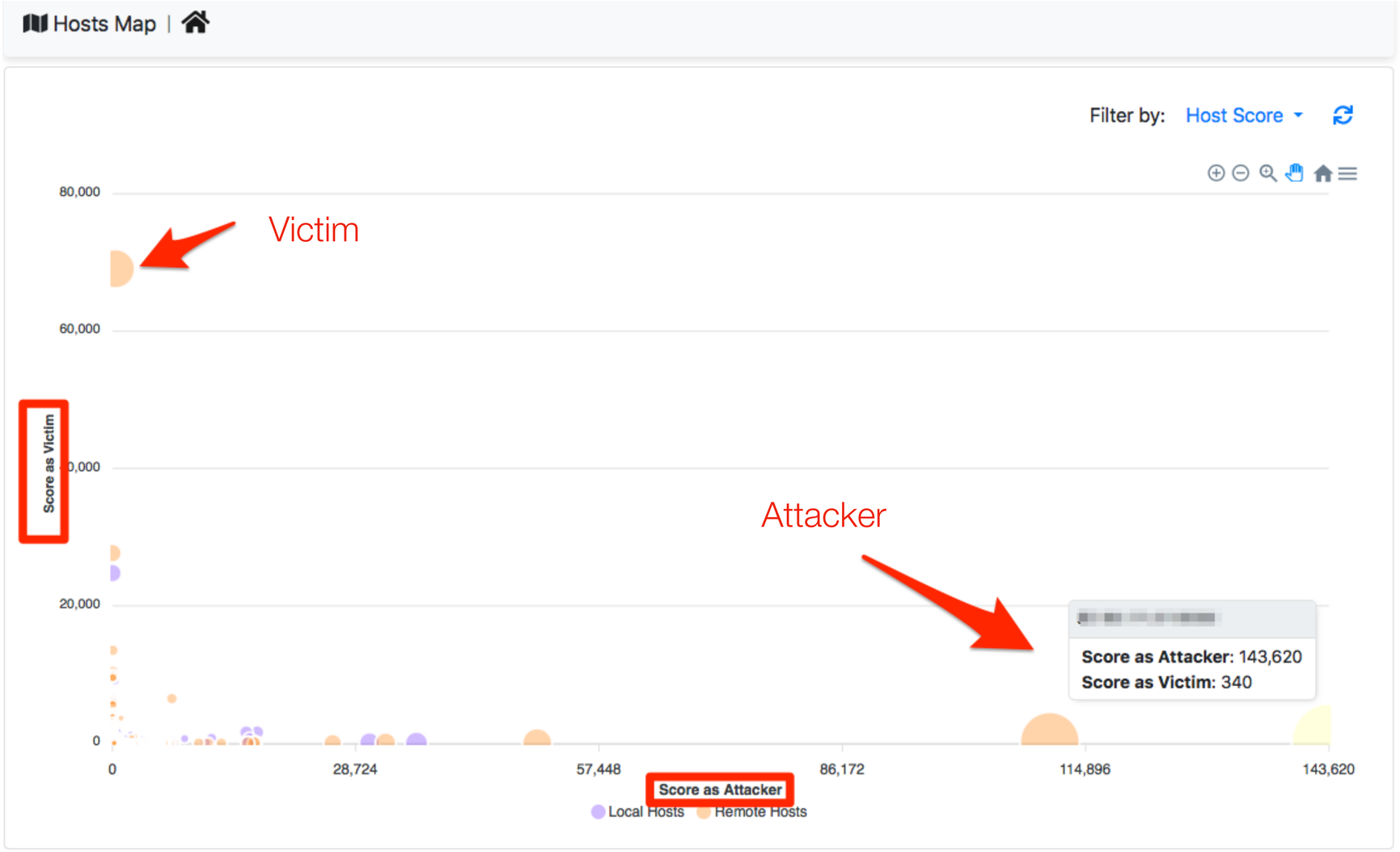


Date/Time	Score	Flow	Description
15:50:26	120	192.168.1.252:51110 91.143.93.242:443	TLS Version: TLSv1
15:50:26	320	192.168.1.252:51111 46.59.52.31:443	Suspicious DGA Domain [www.e6r5p57kbafwrxj3plz.com]
15:50:26	320	192.168.1.252:51112 38.229.70.53:443	Suspicious DGA Domain [www.q4cyamnc6mtokjurvdclt.com]
15:50:26	145	192.168.1.252:138 192.168.1.255:138	Unsafe Protocol
15:50:26	320	192.168.1.252:51175 91.143.93.242:443	Suspicious DGA Domain [www.gfu7hbxpfp.com]
15:50:26	120	192.168.1.252:51174 212.83.155.250:443	TLS Version: TLSv1
15:50:26	120	192.168.1.252:51176 38.229.70.53:443	TLS Version: TLSv1
15:50:26	120	192.168.1.252:51185 62.210.137.230:443	TLS Version: TLSv1
15:50:26	20	192.168.1.1:17500 192.168.1.255:17500	Remote to Remote
15:50:26	20	192.168.1.252:51104 157.56.30.46:443	Remote to Remote

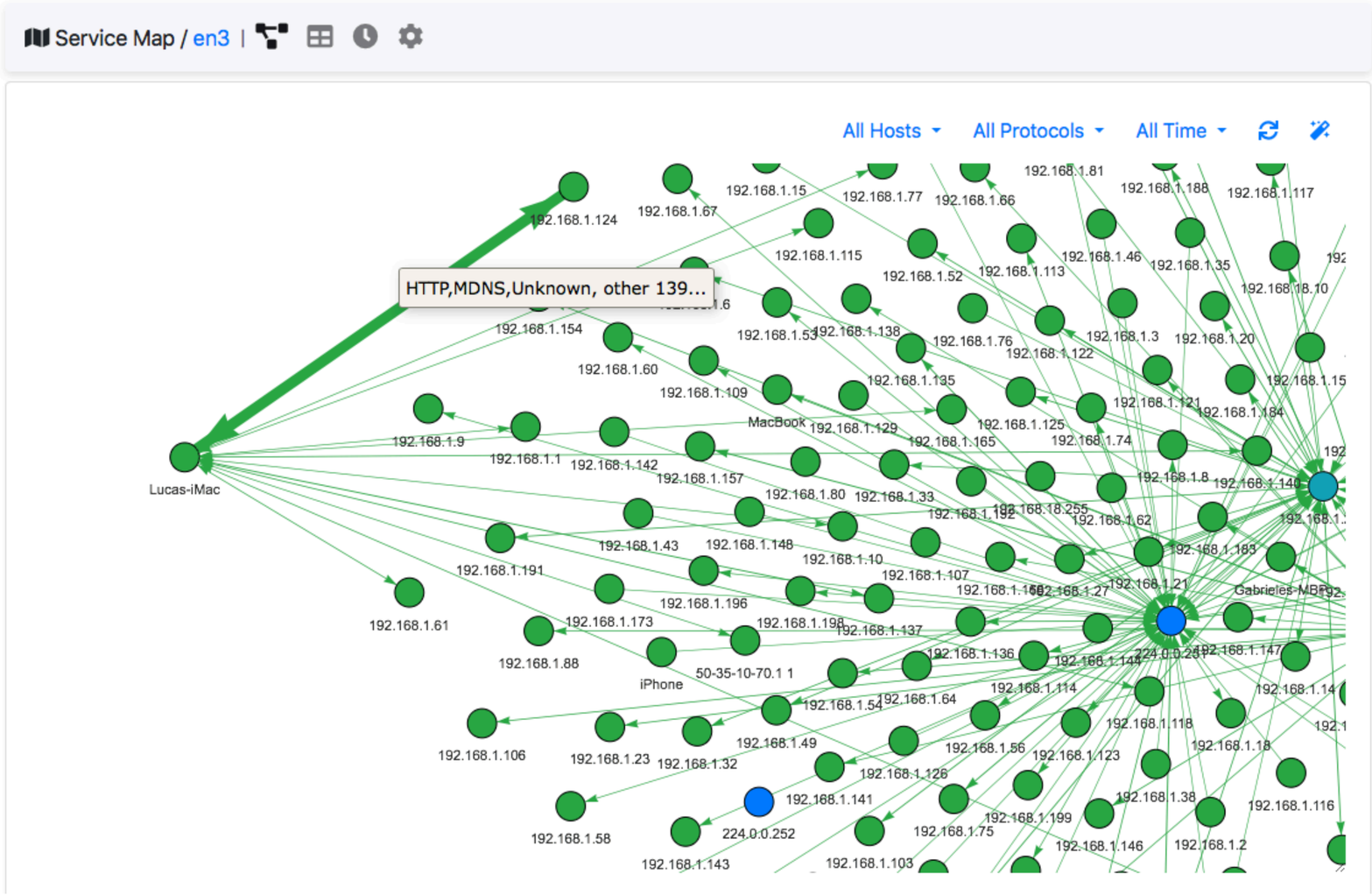
Score-based Behaviour Analysis



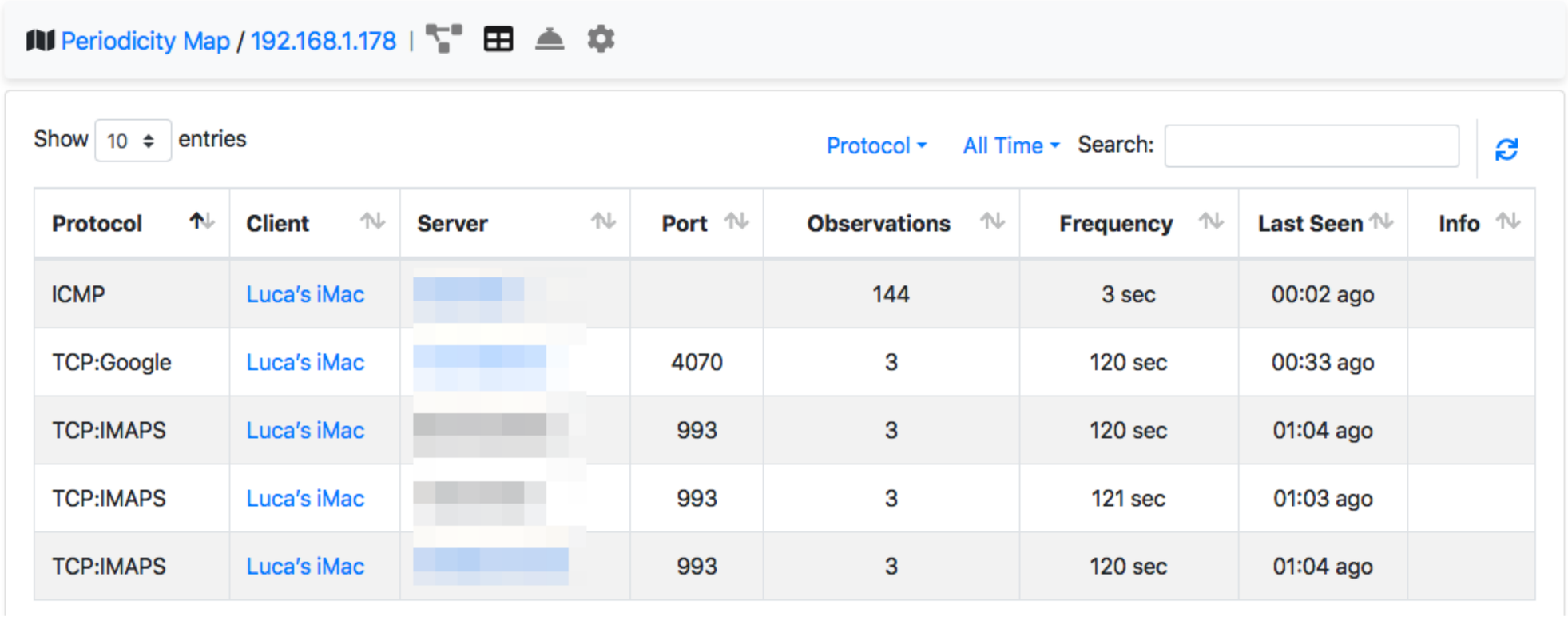
Visualising Cybersecurity: Bubbles



Lateral Movement



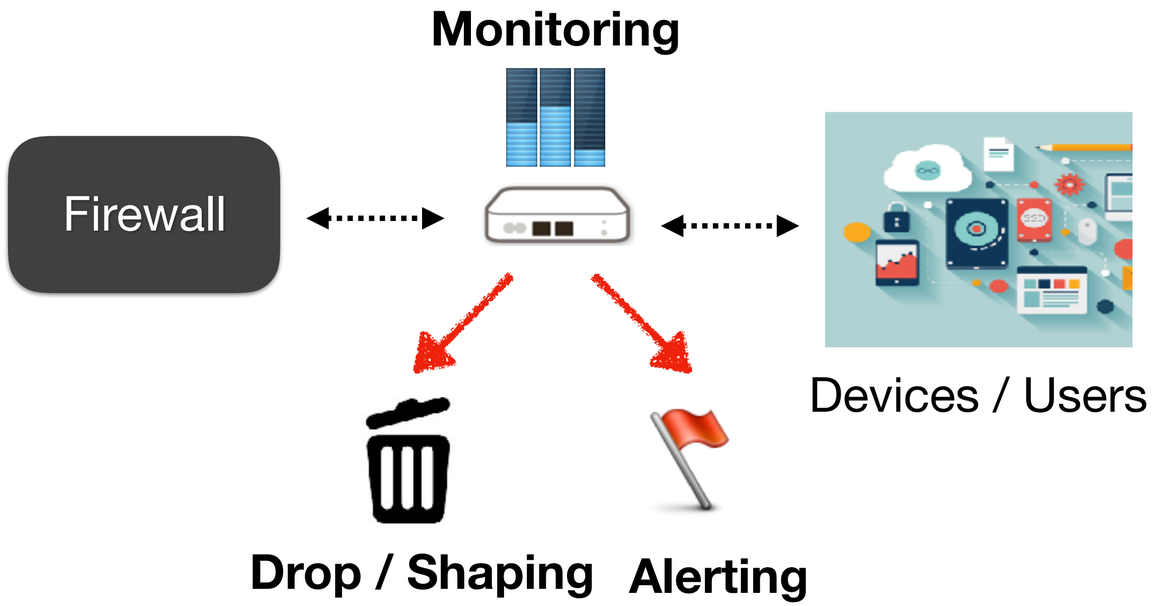
Beaconing Detection



Protocol	Client	Server	Port	Observations	Frequency	Last Seen	Info
ICMP	Luca's iMac			144	3 sec	00:02 ago	
TCP:Google	Luca's iMac		4070	3	120 sec	00:33 ago	
TCP:IMAPS	Luca's iMac		993	3	120 sec	01:04 ago	
TCP:IMAPS	Luca's iMac		993	3	121 sec	01:03 ago	
TCP:IMAPS	Luca's iMac		993	3	120 sec	01:04 ago	

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.



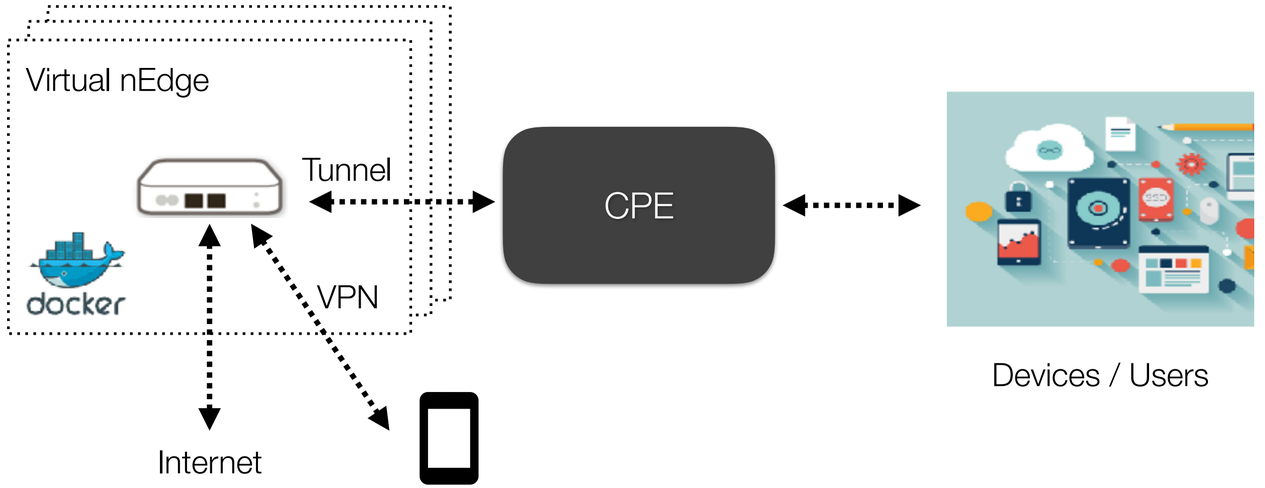
From Visibility to Enforcement [2/3]

Router with NAT

Transparent Bridge

WiFi Router with NAT

Container-based

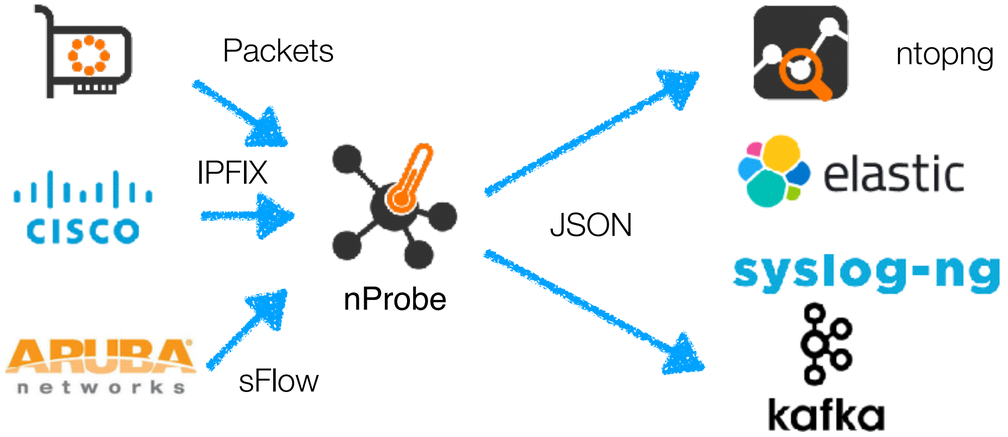


nEdge Limitations

- 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.

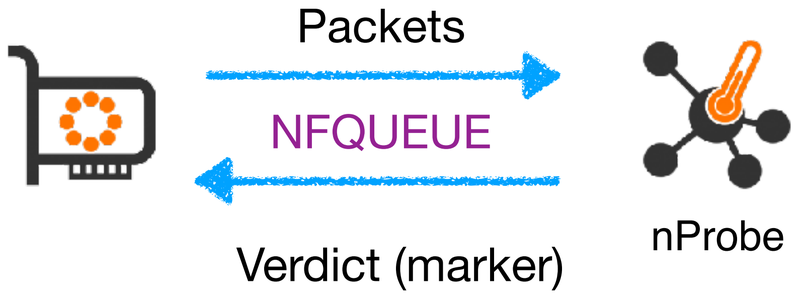
Making nProbe Inline [1/3]

- nProbe is a nDPI-aware passive network probe available for Windows, MacOS, Linux, FreeBSD systems.




```
[NFv9 57590][IPFIX 35632.118][Len 2] %L7_PROTO                    Layer 7 protocol (numeric)
[NFv9 57591][IPFIX 35632.119][Len 16 varlen] %L7_PROTO_NAME       Layer 7 protocol name
[NFv9 57973][IPFIX 35632.501][Len 16 varlen] %L7_PROTO_CATEGORY   Layer 7 protocol category
[NFv9 57981][IPFIX 35632.509][Len 4] %L7_PROTO_RISK               Layer 7 protocol risk (bitmap)
[NFv9 57982][IPFIX 35632.510][Len 64 varlen] %L7_PROTO_RISK_NAME  Layer 7 protocol risk (string)
[NFv9 57999][IPFIX 35632.527][Len 2] %L7_RISK_SCORE               Layer 7 flow risk score
```

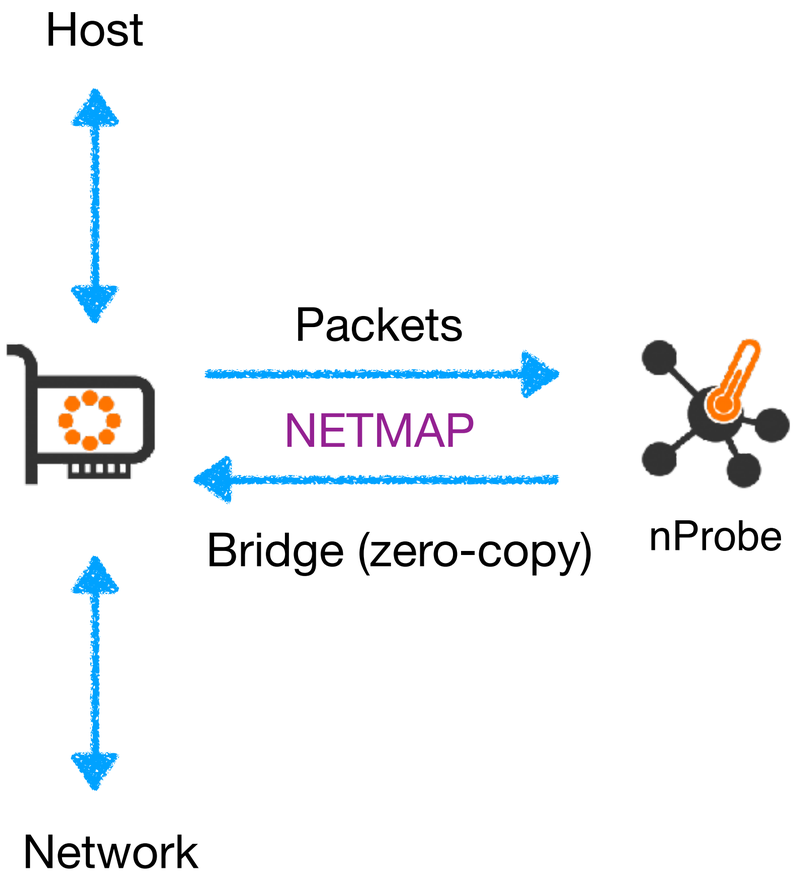
Making nProbe Inline: Linux [2/3]




```
# 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 qdisc add dev $WAN parent 1:11 handle 11: sfq perturb 10
tc filter add dev $WAN parent 1:11 protocol ip handle 51 flow hash keys nfct-src divisor 254
iptables -t mangle -A POSTROUTING -m mark --mark 1 -j CLASSIFY --set-class 1:11
iptables -t mangle -A POSTROUTING -m mark --mark 1 -j RETURN
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 1:13 handle 13: sfq perturb 10
tc filter add dev $WAN parent 1:13 protocol ip handle 53 flow hash keys nfct-src divisor 254
iptables -t mangle -A POSTROUTING -m mark --mark 3 -j CLASSIFY --set-class 1:13
iptables -t mangle -A POSTROUTING -m mark --mark 3 -j RETURN
iptables -t mangle -A FORWARD -m mark --mark 0 -j NFQUEUE --queue-num 0 --queue-bypass -m physdev --physdev-in $LAN
iptables -t mangle -A FORWARD -m mark --mark 0 -j NFQUEUE --queue-num 0 --queue-bypass -m physdev --physdev-out $WAN
```

In-Kernel Bypass

Making nProbe Inline: FreeBSD [3/3]



Making nProbe Inline: Performance

Device	Vanilla Linux Bridge Only	Linux nProbe IPS	Vanilla FreeBSD Bridge Only	FreeBSD nProbe IPS
Low End (APU2)	550 Mbps	600 Mbps	1 Gbps	120 Mbps
Intel E3	10 Gbps / 1.8 Mpps	10 Gbps / 2.4 Mpps		

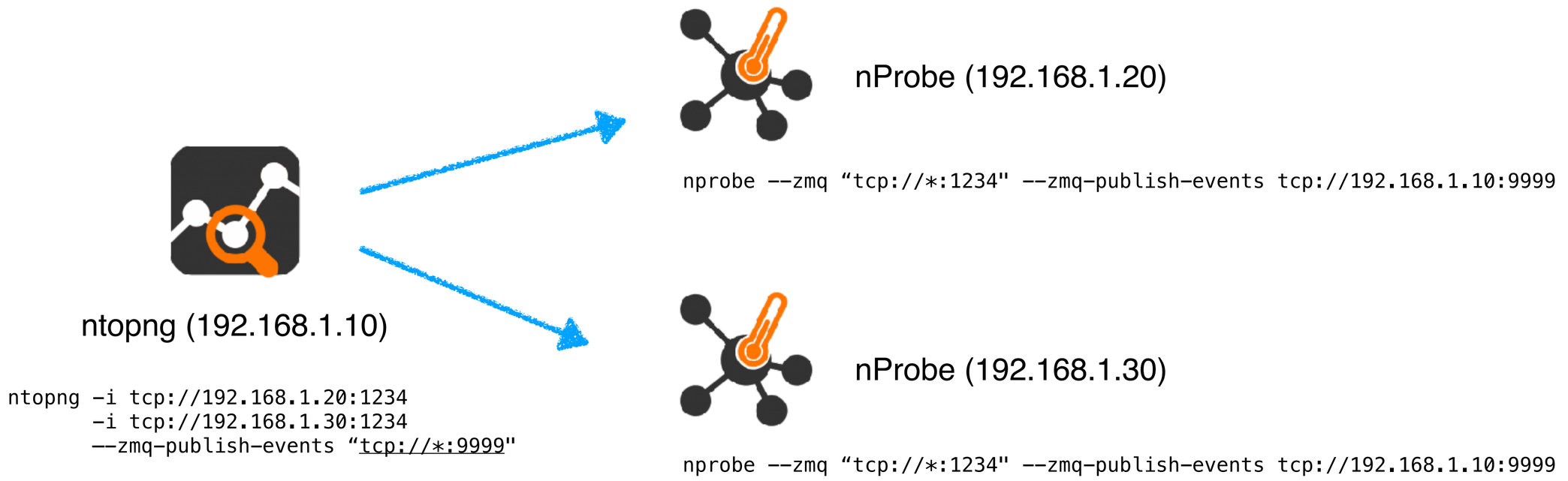
IPS Configuration: Stand Alone [1/2]

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

```
### Pool definition ###
{ "pool": { "id":1, "name": "my pool 1", "ip":  [ "192.168.0.1/24", "10.0.0.0/8", "2a03:b0c0:2:d0::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
{ "policy": { "id": 0, "name": "root rule", "default_marker": "pass", "flow_risk": { "risks": [ 12 ], "marker": "drop" },
"markers": { "categories": { "Video": "drop" }, "protocols": { "TLS": "pass" }}}}

# Rule definition (son of rule 0)
{ "policy": { "id": 1, "root": 0, "name": "my rule 1", "default_marker": "pass", "markers": { "protocols": { "HTTP": "pass" },
"countries": { "IT": "pass", "CN": "drop" }, "continents" : { "Asia" : "drop"}}}}

{ "policy": { "id": 3, "root": 0, "name": "my rule 3", "default_marker": "pass", "markers": { "protocols": { "HTTP": "drop" }}}}

# Subrule of rule 1 with more restrictions
{ "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.



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.

nProbe Version	Max number of Rules/Pools in IPS
Pro	4
Enterprise S	8
Enterprise M	32
Enterprise L	256

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

Horizon 2020 Programme
DG CNECT
Next-generation Internet

NGI TRUST

Silicom Ltd.
Connectivity Solutions

VERXO