ntop MiniConf 2021

Luca Deri <deri@ntop.org>
@lucaderi

2021 In Retrospective

2021 Vision: Visibility + Enforcement

Network Edge

Visibility

Enforcement

Multitenant
(Cloud or On Premise)

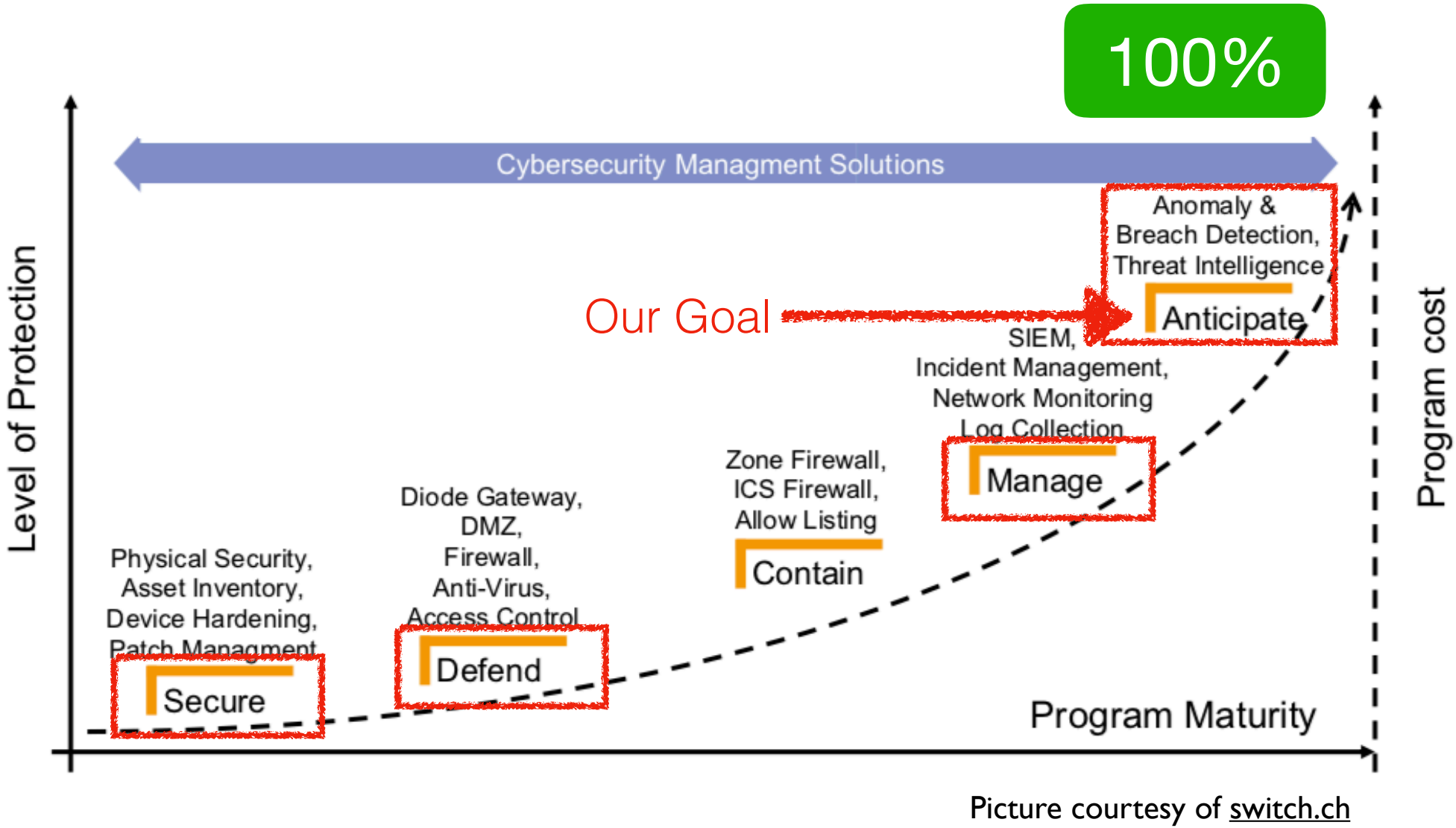
80%

ntop as a Service

80%

- Many of our users are companies that provide visibility and security to their customers.
- Multi-tenancy support in ntopng allows people to have a single ntopng instance that analyses multiple networks/hosts/customers and provide each customer a “restricted view”.
- Various users embed ntop tools in small boxes that they sell/rent to their customers.
- We are adding in ntopng the ability to configure companion services (e.g. nProbe) and configure the system (IP, firewall etc) to let them have a simple turnkey solution without using the nBox interface.
- These are the first step towards a future “ntop as a service”.

2021 Monitoring Goals



Picture courtesy of switch.ch

Roadmap 2022

Planning for 2022

- ntop is well know for:
  - Production of network traffic data.
  - High-speed networking.
  - Data source for OEMs and this party (e.g. CheckMK)
- While we want to continue along this line, we have taken already some direction we want to purse:
  - Cybersecurity
  - Traffic analysis.
  - Data Visualisation.

Plans for 2022: Cybersecurity

- Network traffic is sometimes not enough:
  - Need additional metadata, e.g. via VPN logs Network Access Controllers (NACs).
  - We need to know more about processes that make traffic, and ports used on a system (agent or port scan?).
  - Create a baseline of what a host does and how its behaviour changes. We have started with service and periodicity map in ntopng, but we need to continue as this is just the beginning.

Plans for 2022: Traffic Analysis

- Thanks for nDPI enhancements (see later) we managed to start analysing traffic and produce behavioural alerts.
- The current trend is going towards an increase in number of devices and traffic, making it unfeasible for (skilled) humans to daily spend time to search for anomalies or unexpected situations.
  - We need to automate that.
  - Extends the alerting system to report anomalies, behavioural changes, and outliers.

Plans for 2022: Data Visualisation

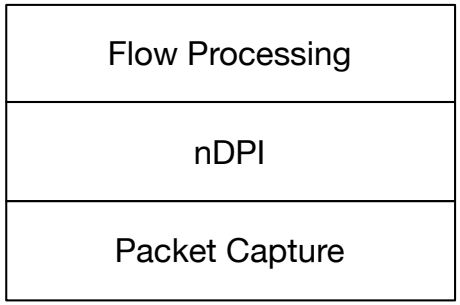
- As you will see later today we have tried to move from table-based data representation to graphics.
- This trend will continue as data exploration is easier when assisted by charts.
- Examples:
  - Last X flows by protocol.
  - Traffic latency/jitter per destination (including alerting when too high).

Update on nDPI

What is nDPI?

- nDPI is an open source DPI toolkit on top of which ntop tools compute statistics. It:
  - Decodes the initial flow packets detecting the application protocol (e.g. Google Maps).
  - 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).

nProbe



What's new in nDPI 4.0 ?

- 2.5x Speeeeeed Bump.
  - v3.4 - nDPI throughput: 1.29 M pps / 3.35 Gb/sec
  - v4.0 - nDPI throughput: 3.35 M pps / 8.68 Gb/sec
- Several improvements with encrypted traffic analysis (QUIC and TLS).
- 14 new protocols, 30 existing protocols vastly improved.
- Various improvements and fixes.

nDPI 4.x: 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

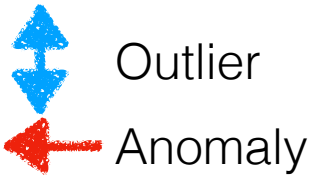
- TLS Certificate Validity Too Long
- Suspicious TLS Extension
- TLS Fatal Alert
- Suspicious Protocol traffic Entropy
- Clear-text Credentials Exchanged
- DNS Large Packet
- DNS Fragmented Traffic
- Invalid Characters Detected

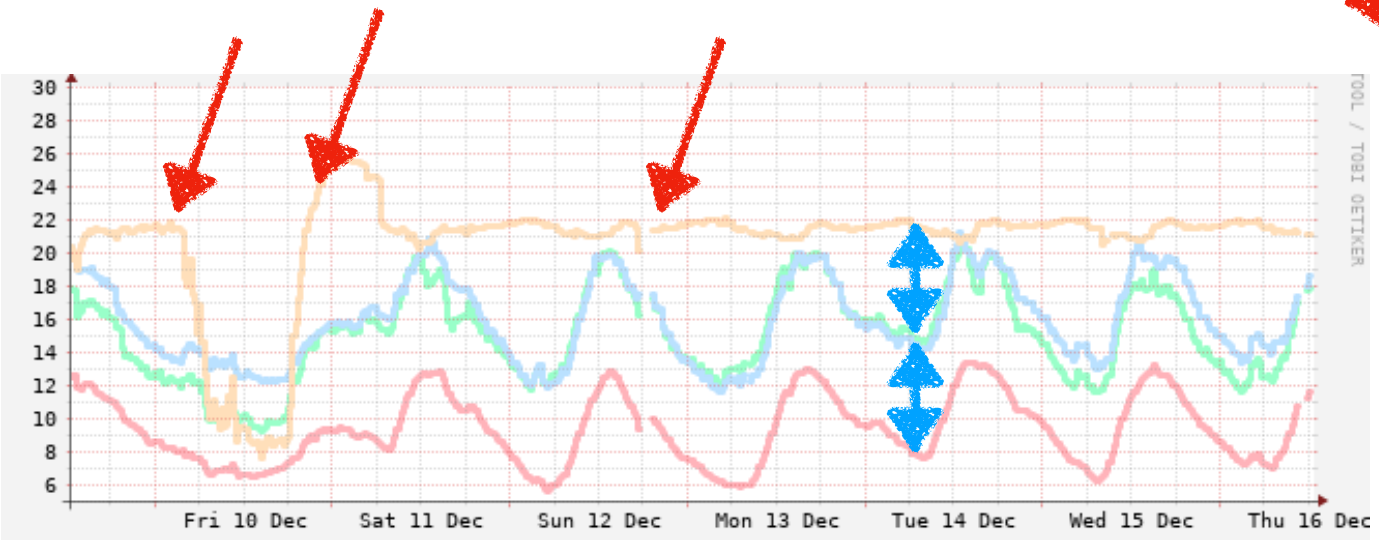
Legenda: Clear Text Only, Encrypted/Plain Text, Encrypted Only

4.x

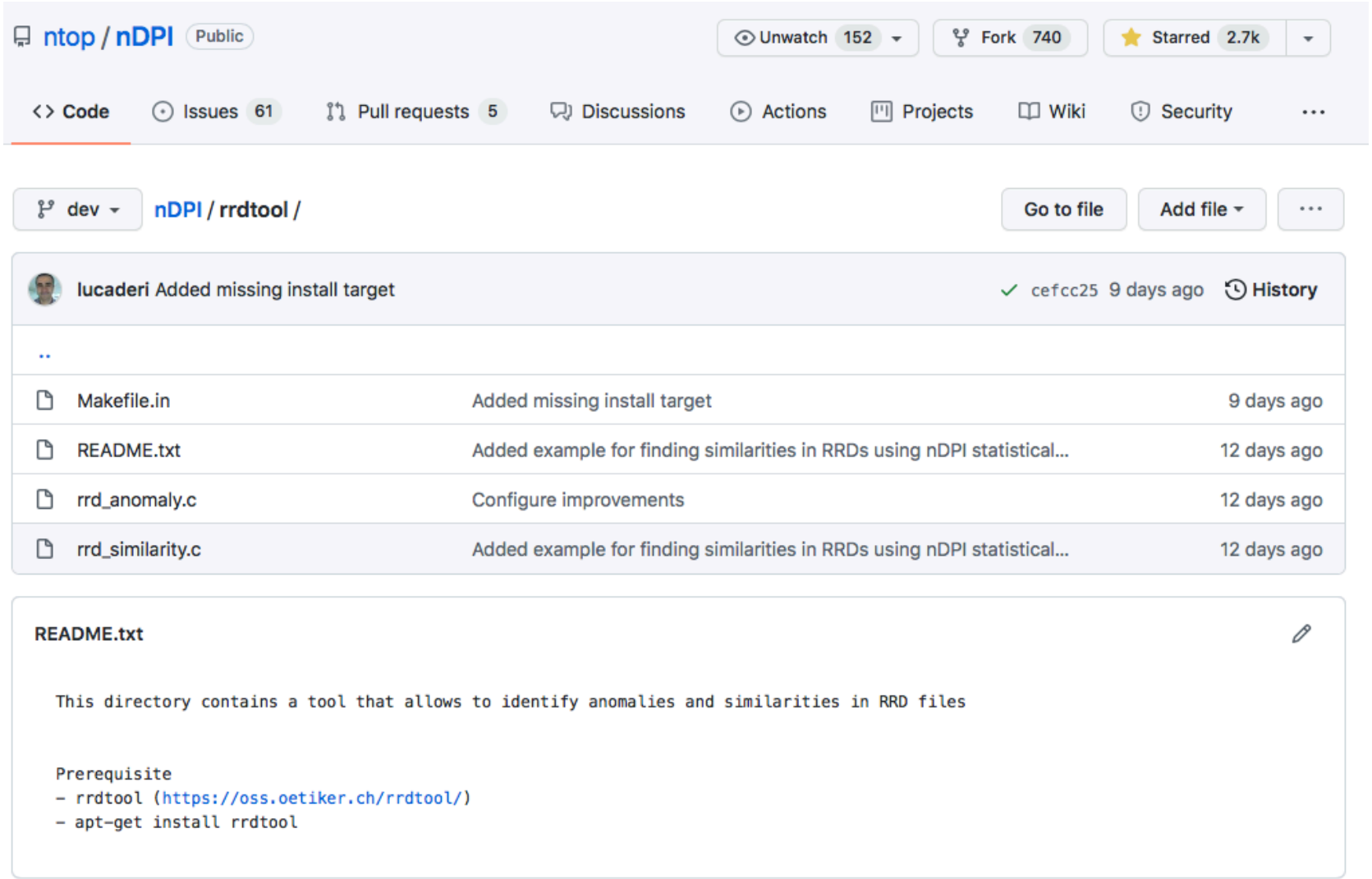
nDPI 4: New APIs for Data Analysis

- Jitter calculation
- Timeseries forecasting: single, double, triple (Holt-Winters) exponential smoothing.
- Improved data binning support





4.1.x Ongoing Work



Update on nProbe

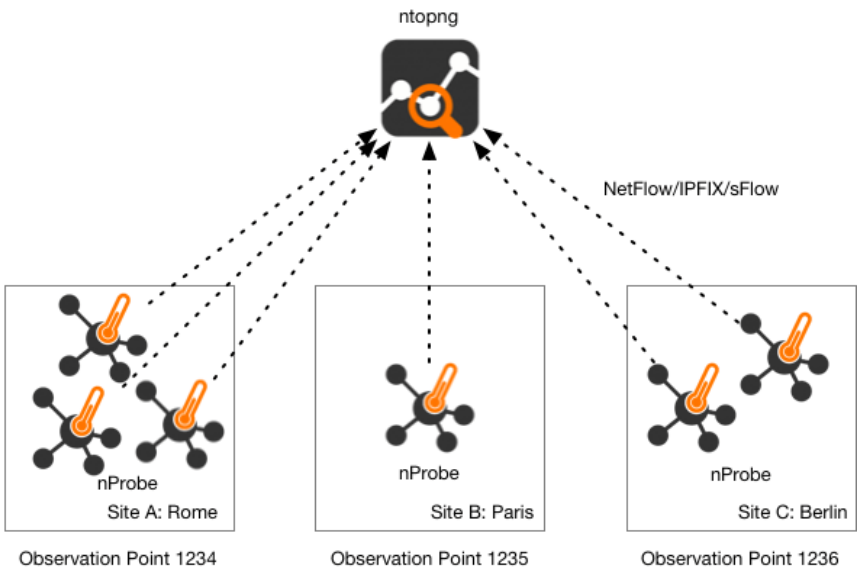
What is nProbe?

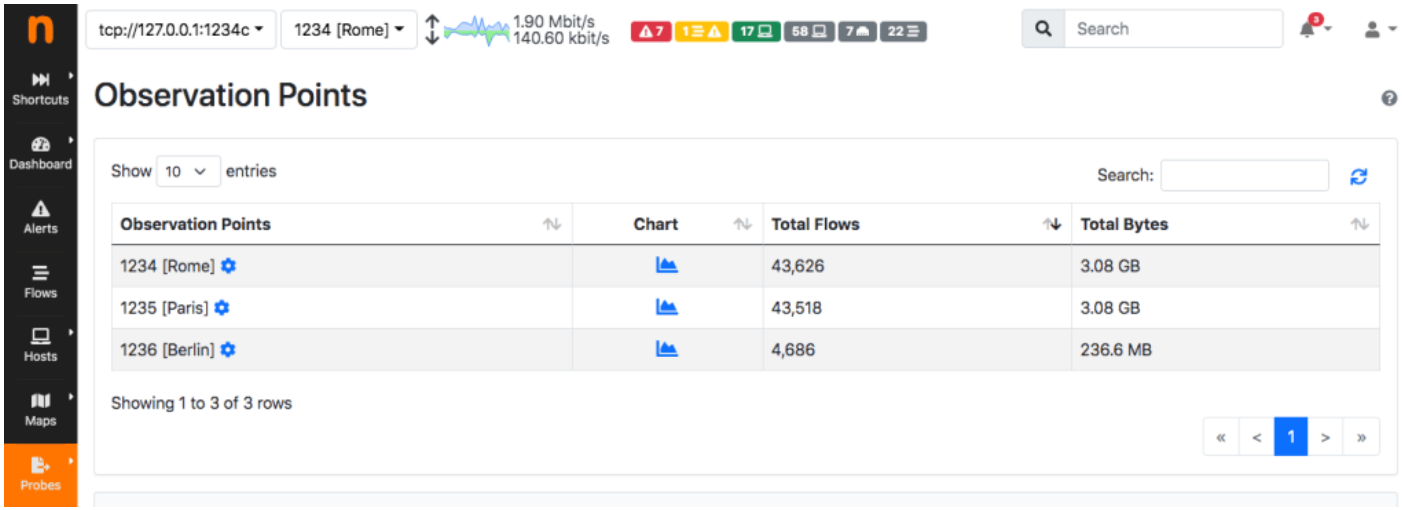
- nProbe is an extensible NetFlow/IPFIX/sFlow application able to:
  - Capture packets and turn them into flows that are exported in NetFlow/IPFIX format to external collectors, or JSON to ntopng via ZMQ .
  - Collect flows and re-export them (proxy mode).
  - Collect flows and dump them to disk, external consumers (Kafka, ElasticSearch, Syslog, TCP streaming).
  - Fully nDPI-based and extensible via plugin architecture (e.g. VoIP, Email, DNS, HTTP, 3G/4G, Radius…)

What's new in nProbe 9.6?

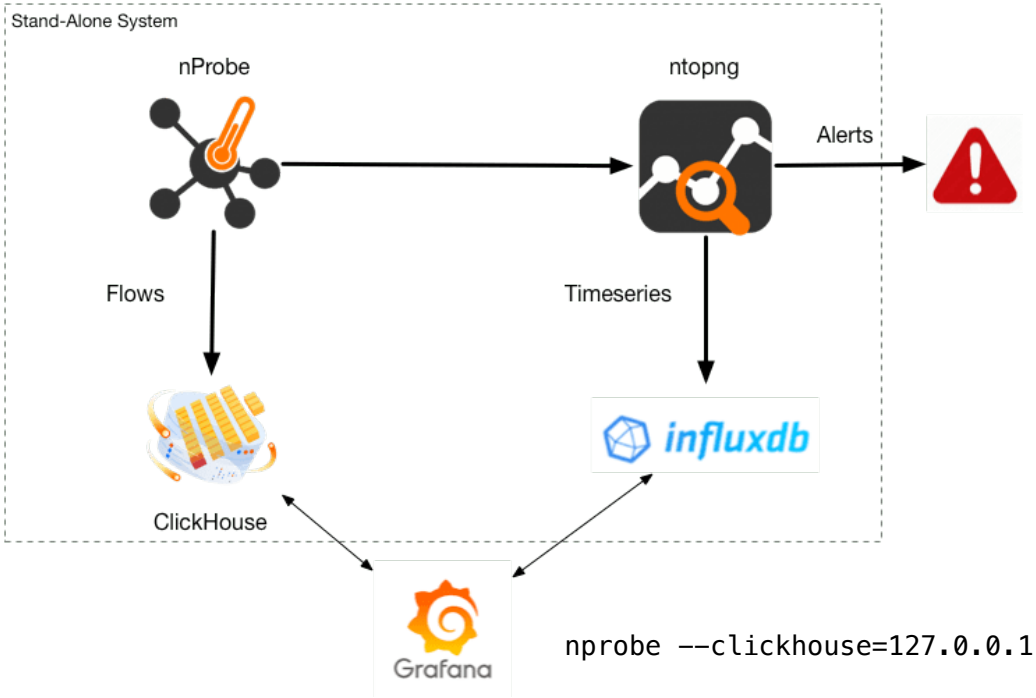
- Support for FreeBSD/OPNsense/pfSense.
- IPS Mode: Linux (based on Netfilter) and FreeBSD/OPNsense/pfSense (based on Netmap).
- Added support for dumping flows at high speed into ClickHouse DB.
- Cloud Monitoring: Added ability to read Amazon AWS VPC Log Files and turn them into flows.

nProbe 9.6: Observation Points





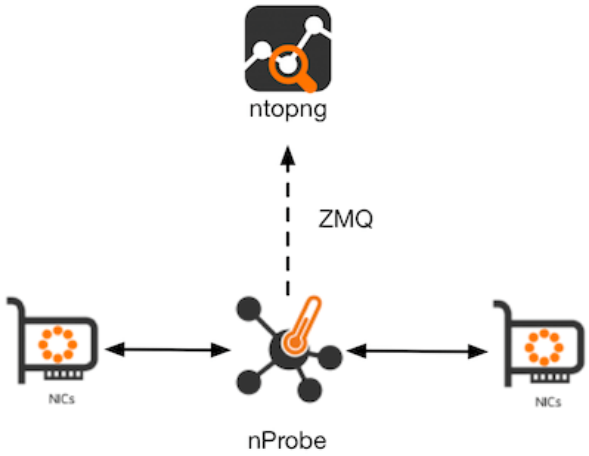
nProbe 9.6: ClickHouse




```
nprobe --clickhouse=127.0.0.1:ntop::default:helloworld
```

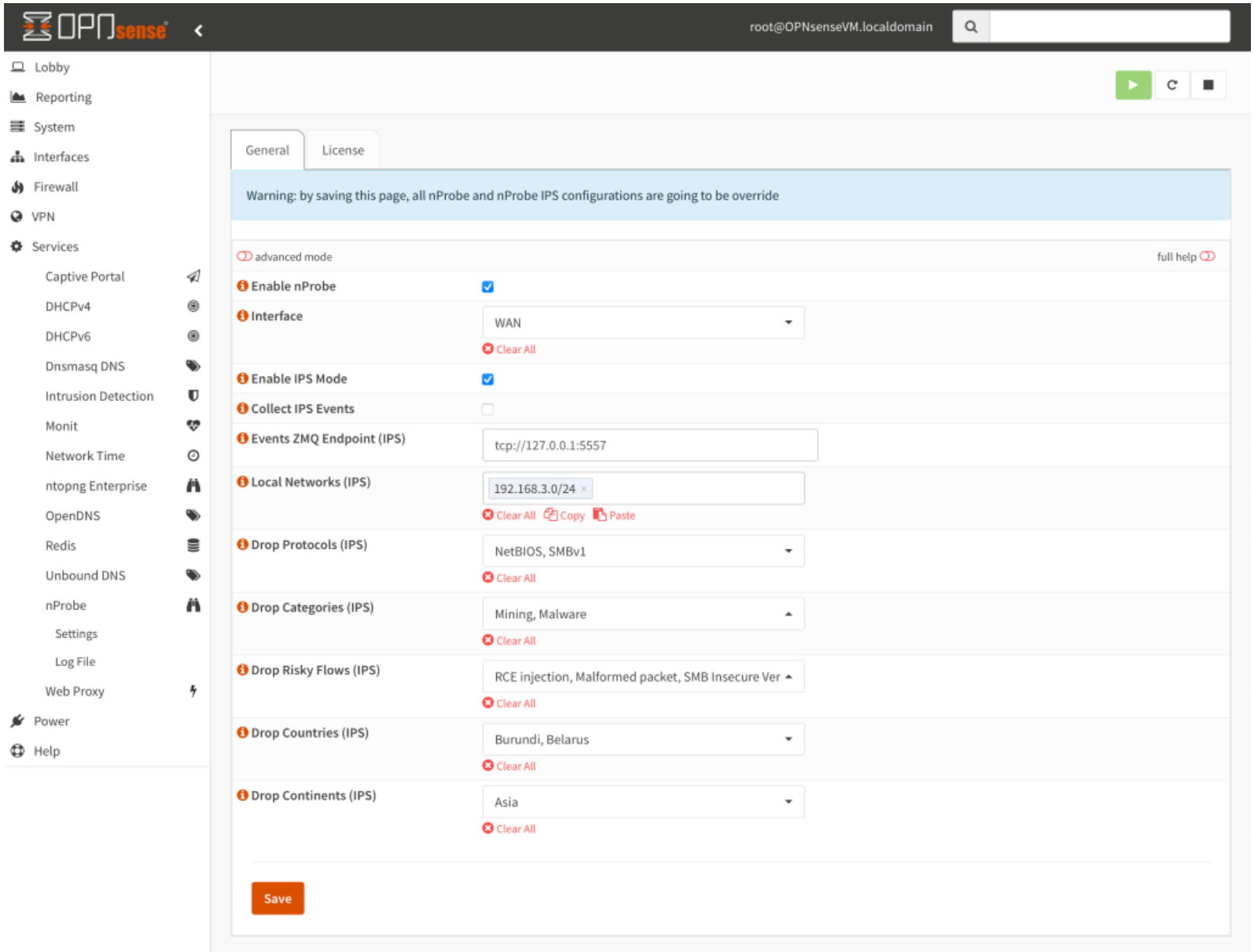
Test Case (Single nProbe Instance)	Performance Fps (Flows/sec)
nProbe dumping to ClickHouse, no NetFlow Export	125 Kfps
nProbe with NetFlow Export only	300 Kfps
nProbe speaking to ntopng via ZMQ, no NetFlow Export	183 Kfps
nProbe dumping to ClickHouse, speaking to ntopng via ZMQ, no NetFlow Export	77 Kfps
nProbe dumping to ClickHouse, speaking to ntopng via ZMQ, with NetFlow Export	74 Kfps

nProbe 9.6: IPS Mode [1/3]




```
# Pool definition
{"pool":{"id":1,"name":"my pool 1","ip": [ "131.114.0.0/16"], "mac": [ ]},"policy": {"id": 1} }
{"pool":{"id":2,"name":"my pool 2","ip": [ "192.168.1.0/24"], "mac": [ ]},"policy": {"id": 2} }

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

# Policy definition
{"policy":{"id":0,"name":"root policy rule", "default_marker": "pass", "markers": { "countries": { "IT": "pass",
"CN": "drop", "US": "pass" } } } }
{"policy":{"id":1,"root":0,"name":"my rule 1", "markers": { "categories": { "Network": 7, "Download-FileTransfer-
FileSharing": 8, "DataTransfer": 8, "VPN": 8, "Video": 9, "Music": 9, "Streaming": 9, "Media": 9 }, "protocols":
{ "DNS": "drop" }, "countries": { "IT": "drop", "CN": "drop", "US": "pass" }, "asn" : { }, "continents" : { "Asia" :
"drop"} } , "default_marker": "pass"  } }
{"policy":{"id":2,"root":0,"name":"my rule 2", "markers": { "categories": { "Video": "pass" }, "flow_risk":
{ "risks": [12], "marker": "drop" }, "protocols": { "DNS": "drop" }, "countries": { "IT": "pass", "US": "pass" },
"asn" : { "34984" : "drop" } }, "default_marker": "pass"  } }
#{"policy":{"id":2,"root":0,"name":"my rule 2", "markers": { "categories": { "Video": "drop" }, "protocols": { "DNS":
"drop" }, "countries": { "IT": "pass", "US": "pass" } }, "default_marker": "pass"  } }

### GeoIP ###

{ "geoip": { "asn": ".GeoLite2-ASN.mmdb", "city": "GeoLite2-City.mmdb" }}
```

nProbe 9.6: IPS Mode [2/3]



nProbe 9.6: IPS Mode [3/3]

Device	Vanilla Linux Bridge Only	Linux nProbe IPS	Vanilla FreeBSD Bridge Only	FreeBSD nProbe IPS
PC Engines APU2	550 Mbps	600 Mbps	1 Gbps	120 Mbps
Intel E3	10 Gbps / 1.8 Mpps	10 Gbps / 2.4 Mpps		

Plans for nProbe Post 9.6 [1/2]

- Added ability to collect syslog and turn it into flows.
- Currently only FortiNet is supported

```
<189>logver=602091234 timestamp=1638540274 tz="UTC+1:00"
devname="MY_FORTI" devid="FG100ETK18008770" vd="root" date=2021-12-03
time=15:04:34 logid="0000000013" type="traffic" subtype="forward"
level="notice" eventtime=1638540275032390407 tz="+0100"
srcip=192.168.100.97 srcport=52449 srcintf="port6" srcintfrole="lan"
dstip=10.0.7.17 dstport=389 dstintf="DMZ_TO_INT" dstintfrole="dmz"
sessionid=52036420 proto=17 action="accept" policyid=5
policytype="policy" poluuid="ae1d6816-710c-51eb-6ff3-75abf3490362"
service="LDAP_UDP" dstcountry="Reserved" srccountry="Reserved"
trandisp="noop" duration=180 sentbyte=234 rcvdbyte=189 sentpkt=1
rcvdpkt=1 appcat="unscanned" mastersrcmac="24:56:88:ad:12:2d"
srcmac="56:88:16:ad:27:19" srcserver=0 dsthwvendor="Microsoft"
dstosname="Windows" dstswversion="10" masterdstmac="24:56:88:ad:
12:2d" dstmac="24:56:88:ad:12:2d" dstserver=0
```

Plans for nProbe Post 9.6 [2/3]

- Implement basic EDR (EndPoint Detection and Response) able to:
  - Map open ports and report differences.
  - Add process/user/container info to exported flows.
  - Ability to work in IPS mode blocking
    - Unwanted apps (e.g. apps not part of a package).
    - Apps started from unusual directories (e.g. /tmp).
    - Invalid user/application combination (e.g. user luca cannot start ssh)

Plans for nProbe Post 9.6 [3/3]

- Planned availability: Spring 2022

```
# cat /tmp/2021/09/22/22/49.flows
IPV4_SRC_ADDR|IPV4_DST_ADDR|INPUT_SNMP|OUTPUT_SNMP|IN_PKTS|IN_BYTES|FIRST_SWITCHED|LAST_SWITCHED|
L4_SRC_PORT|L4_DST_PORT|TCP_FLAGS|PROTOCOL|SRC_PROC_NAME|SRC_PROC_PID|DST_PROC_NAME|DST_PROC_PID|
FLOW_VERDICT
192.168.1.187|192.168.1.178|0|0|17|6564|1632343764|1632343765|22|56218|24|6||0|/usr/sbin/sshd|2910|0
192.168.1.178|192.168.1.187|0|0|17|884|1632343764|1632343765|56218|22|16|6|/usr/sbin/sshd|2910||0|0
192.168.1.178|192.168.1.187|0|0|9|612|1632343767|1632343768|49372|22|24|6|/usr/sbin/sshd|2910||0|0
192.168.1.187|192.168.1.178|0|0|5|504|1632343767|1632343768|22|49372|24|6||0|/usr/sbin/sshd|2910|0
192.168.1.187|192.168.1.178|0|0|11|3648|1632343767|1632343768|22|56218|24|6||0|/usr/sbin/sshd|2910|0
192.168.1.178|192.168.1.187|0|0|11|572|1632343767|1632343768|56218|22|16|6|/usr/sbin/sshd|2910||0|0
192.168.1.187|192.168.1.1|0|0|2|116|1632343768|1632343768|44199|53|0|17||0|/usr/bin/traceroute.db|4909|2
192.168.1.1|192.168.1.187|0|0|1|106|1632343768|1632343768|53|44199|0|17|/usr/bin/traceroute.db|4909||0|2
192.168.1.187|192.168.1.178|0|0|9|3264|1632343771|1632343771|22|56218|24|6||0|/usr/sbin/sshd|2910|0
192.168.1.178|192.168.1.187|0|0|9|468|1632343771|1632343771|56218|22|16|6|/usr/sbin/sshd|2910||0|0
192.168.1.178|192.168.1.187|0|0|4|244|1632343772|1632343772|49372|22|24|6|/usr/sbin/sshd|2910||0|0
192.168.1.187|192.168.1.178|0|0|3|296|1632343772|1632343772|22|49372|24|6||0|/usr/sbin/sshd|2910|0
```