Enterprise Network Visibility with ntopng

Simone Mainardi
mainardi@ntop.org

Agenda

- Defining the goals of network visibility
- Getting the data
- Use-cases: troubleshooting and security with ntopng

ntop: Our Tools

- Open Source (https://github.com/ntop)
  - ntopng: Web-based network visibility
  - PF_RING: Accelerated RX/TX on Linux
  - nDPI: Deep Packet Inspection Toolkit
  - nIndex: Flow-database
- Proprietary
  - PF_RING ZC: 1/10/40/100 Gbit Line rate.
  - nProbe: 10G NetFlow/IPFIX Probe
  - nProbe Cento: flows+packets+security
  - n2disk/disk2n Network-to-disk and disk-to-network.
  - nScrub: Software DDoS Mitigation

ntop + Würth Phoenix

- ntop and Würth Phoenix are long-term partners
  - nBox: Network visibility appliances tailored on the needs of every customer
  - nBox Recorder: Network visibility + traffic recording up to 40 Gbps
  - NetEye: Unified Monitoring e System Management
- Currently partnering to integrate ntopng Enterprise in NetEye4

Defining the Goals of Network Visibility

- Network visibility per se is a broad term
- One should define which are the goals
- It should be clear why money and time should be invested for this purpose

North-South vs East-West Visibility

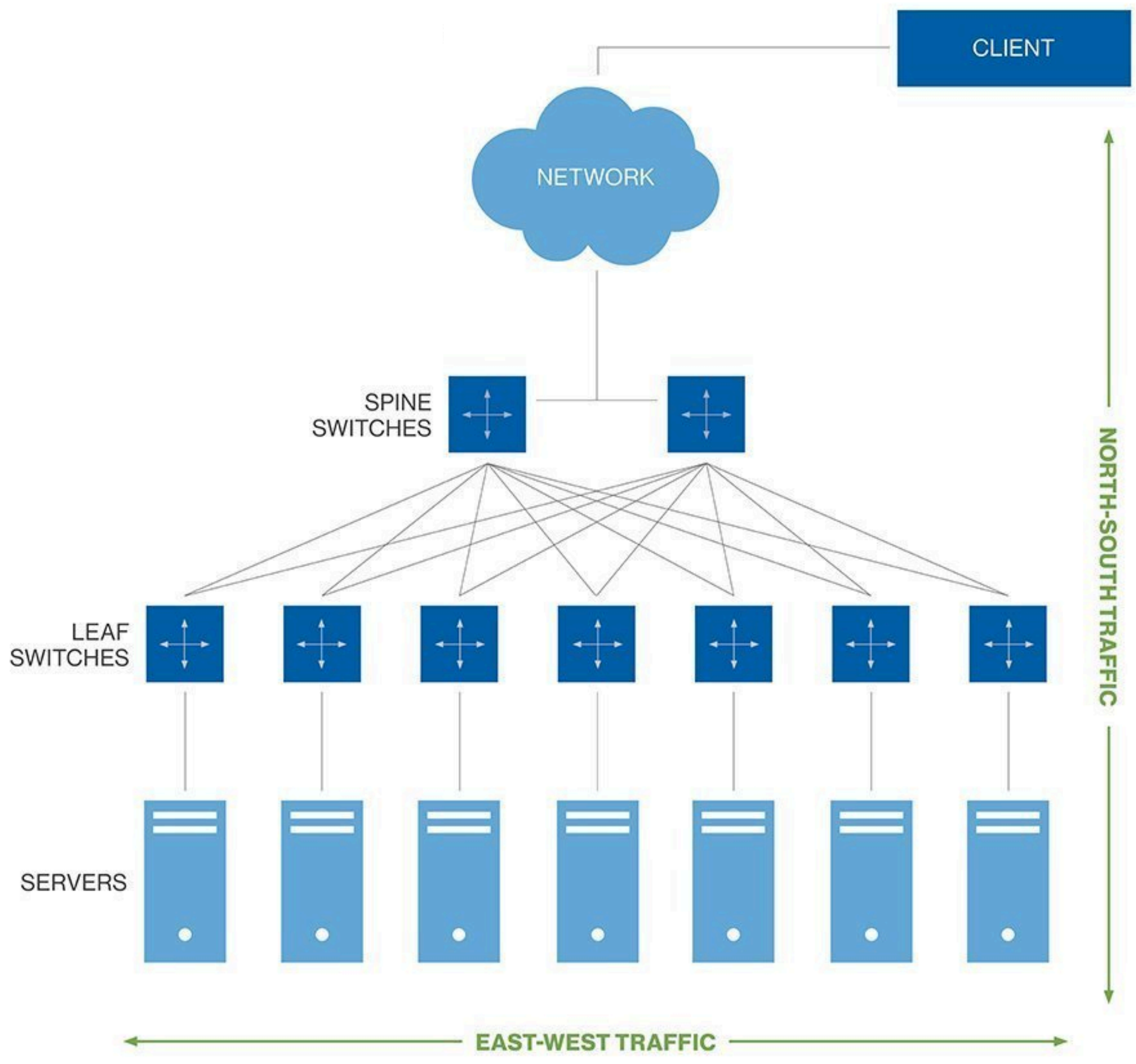


image credits: https://searchnetworking.techtarget.com/definition/east-west-traffic

North-South Visibility

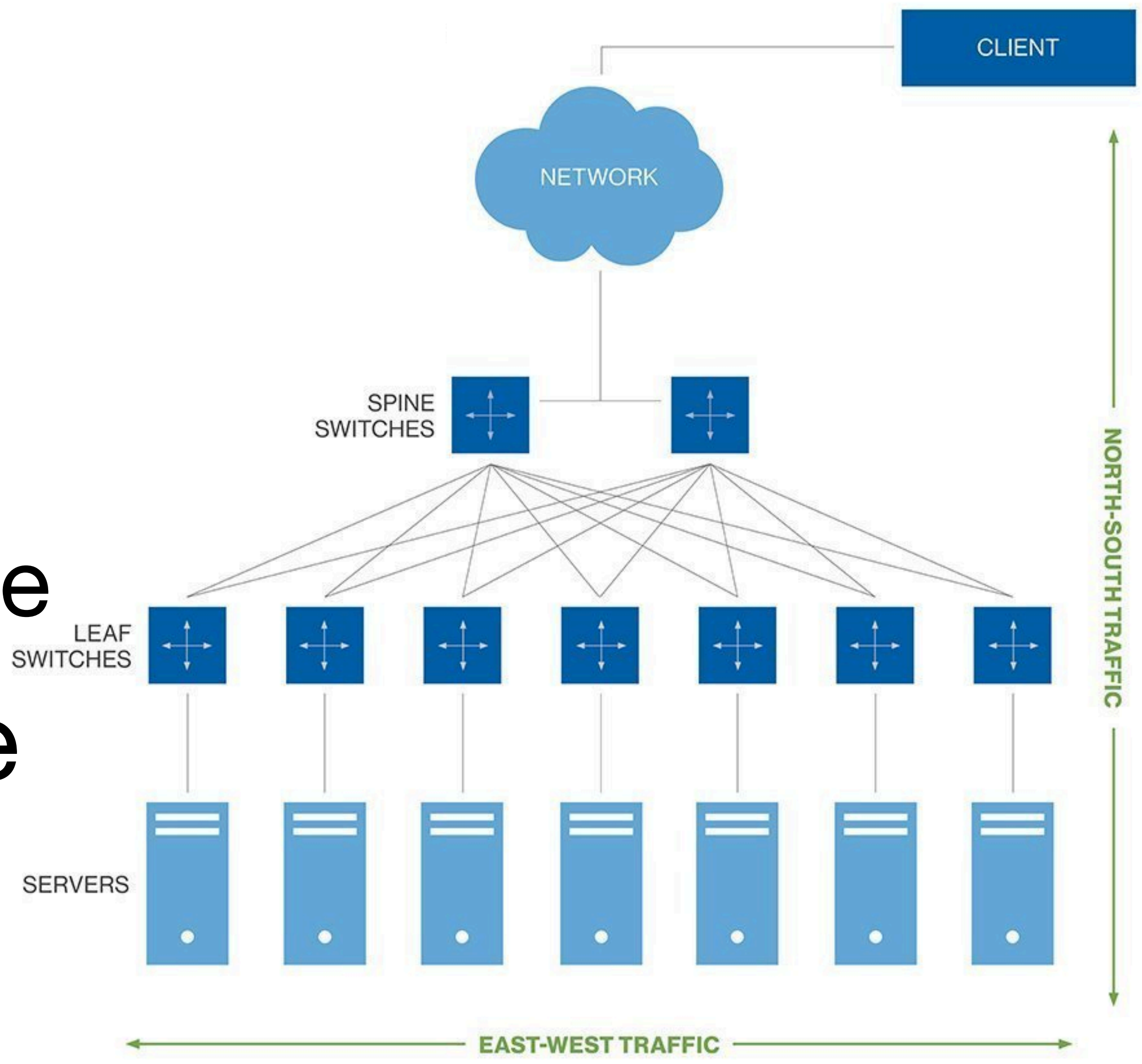
- Visibility of the traffic that moves between the data center and a location outside of the data center
  - *“I'm paying for an International MPLS link and I want to understand how this bandwidth is used”*
  - *“I want protection against data exfiltration”*
  - *“Are there any compromised hosts talking with the Internet? Where are they located?”*

East-West/Lateral Visibility

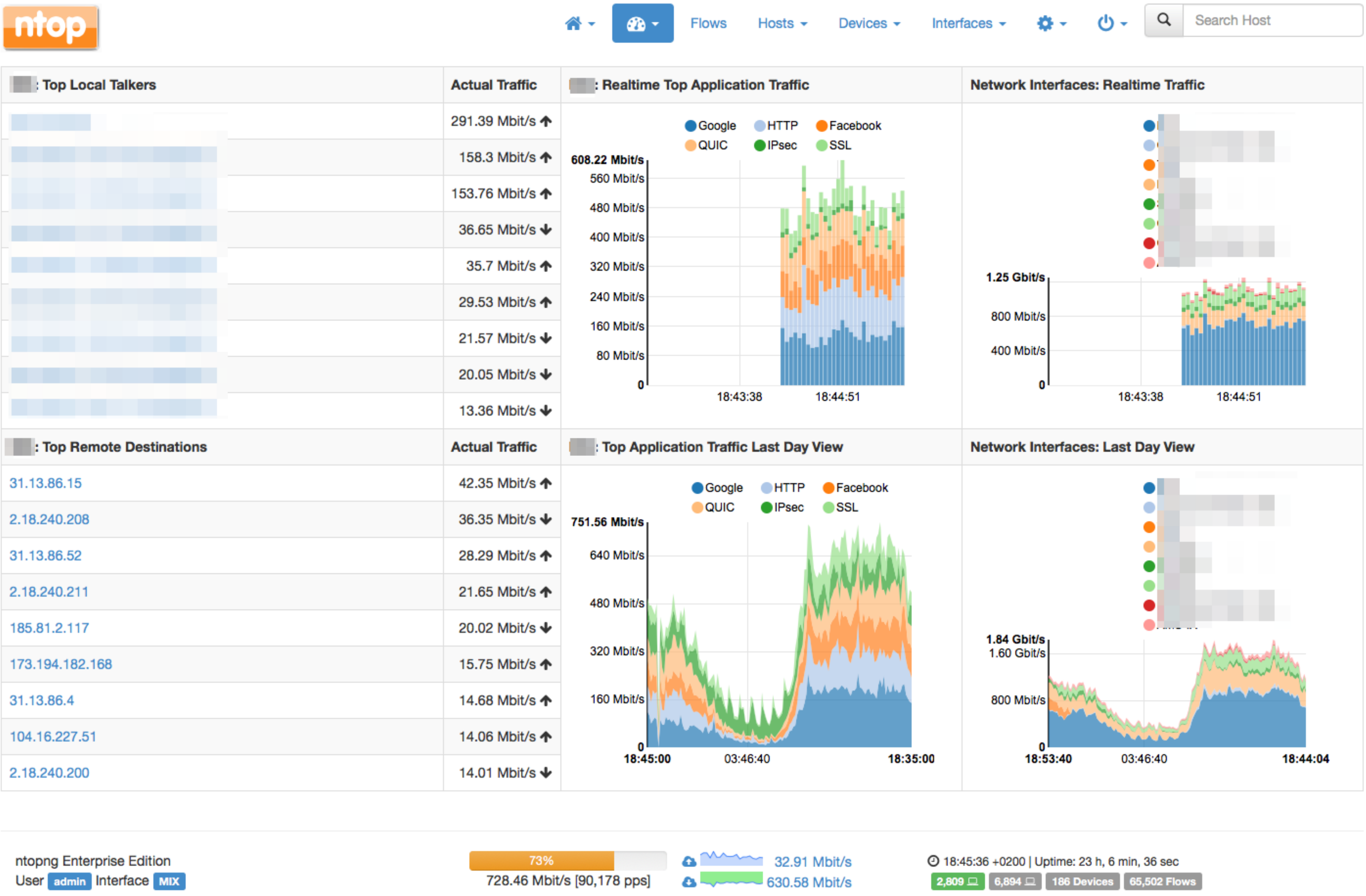
- Visibility of the traffic that moves within a data center (typically bypassing firewalls)
  - *“I need to understand the traffic exchanged between the web and the database server”*
  - *“I know that MySQL performs poorly with a latency above 300ms”*
  - *“I want to verify implemented micro-segmentation policies (e.g., PLCs can only talk to other PLCs)”*

Network Data Sources

- Counters
  - SNMP, sFlow
- Packets
  - Mirror/SPAN, TAP, sFlow
- Flows
  - NetFlow, IPFIX - via nProbe
- Connect the datasource to ntopng



Network Visibility with ntopng



[redacted]: Top Local Talkers	Actual Traffic
[redacted]	291.39 Mbit/s ↑
[redacted]	158.3 Mbit/s ↑
[redacted]	153.76 Mbit/s ↑
[redacted]	36.65 Mbit/s ↓
[redacted]	35.7 Mbit/s ↑
[redacted]	29.53 Mbit/s ↑
[redacted]	21.57 Mbit/s ↓
[redacted]	20.05 Mbit/s ↓
[redacted]	13.36 Mbit/s ↓

[redacted]: Realtime Top Application Traffic

Network Interfaces: Realtime Traffic

[redacted]: Top Remote Destinations	Actual Traffic
31.13.86.15	42.35 Mbit/s ↑
2.18.240.208	36.35 Mbit/s ↓
31.13.86.52	28.29 Mbit/s ↑
2.18.240.211	21.65 Mbit/s ↑
185.81.2.117	20.02 Mbit/s ↓
173.194.182.168	15.75 Mbit/s ↑
31.13.86.4	14.68 Mbit/s ↑
104.16.227.51	14.06 Mbit/s ↑
2.18.240.200	14.01 Mbit/s ↓

[redacted]: Top Application Traffic Last Day View

Network Interfaces: Last Day View

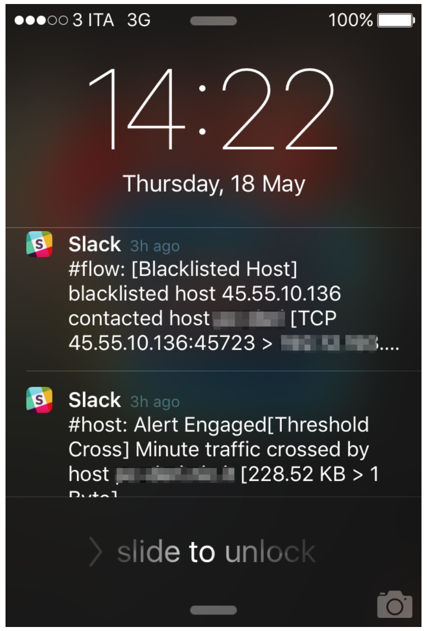
ntopng Enterprise Edition
User admin Interface MIX

73%
728.46 Mbit/s [90,178 pps]

32.91 Mbit/s
630.58 Mbit/s

18:45:36 +0200 | Uptime: 23 h, 6 min, 36 sec
2,809 | 6,894 | 186 Devices | 65,502 Flows

Main ntopng Features



●●●○○ 3 ITA 3G 100%

14:22

Thursday, 18 May

Slack 3h ago
#flow: [Blacklisted Host] blacklisted host 45.55.10.136 contacted host [redacted] [TCP 45.55.10.136:45723 > [redacted]....

Slack 3h ago
#host: Alert Engaged[Threshold Cross] Minute traffic crossed by host [redacted] [228.52 KB > 1

slide to unlock

- Embedded alerting system with external endpoints (Slack, Email, Icinga2, NetEye4, …)
- InfluxDB Support influxdata
- Malware detection (Emerging Threats, Cisco Thalos, …)
- Ready for openstack CLOUD SOFTWARE WIRESHARK VAGRANT docker elastic NetEye
- Deep Packet Inspection with nDPI
- Support for NetFlow/sFlow/SNMP
- Passive/Active Network Device Discovery

ntopng Editions: Matrix

Community

- Realtime traffic and L7 applications visibility
- Historical charts for hosts, networks, ASes, VLANs, host pools
- Historical top talkers (sources and destinations)
- Threshold- and anomaly-based alerts
- Geolocation
- Network discovery and devices inventory

Professional

everything in Community plus

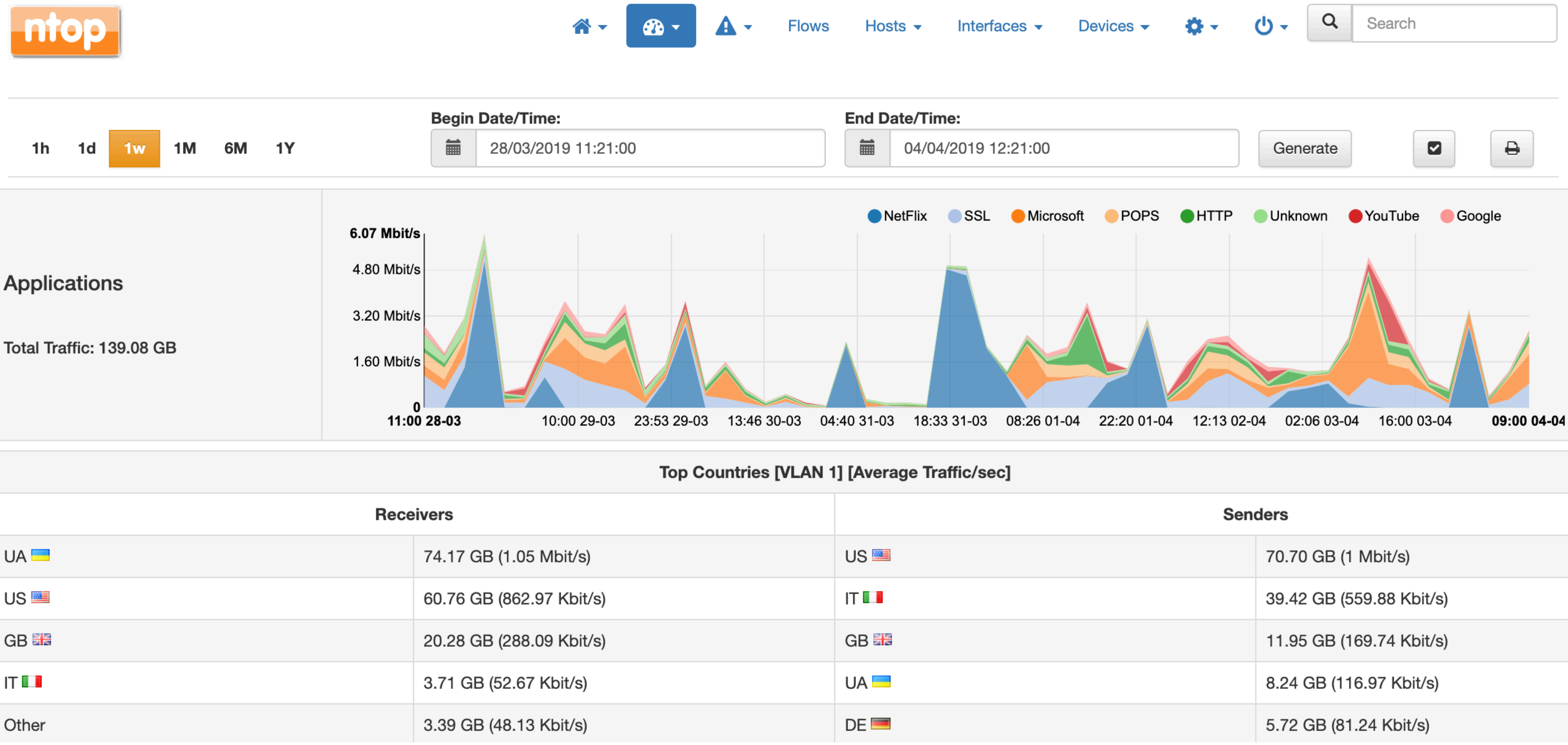
- Extended realtime visibility with dashboards
- Rich historical flows drill-down and export with nIndex
- SNMP v1/v2c
- Custom BPF-based traffic profiles

Enterprise

everything in Professional plus

- Alerts dashboard
- SNMP v1/v2c with historical charts
- Netflow/sFlow devices ports monitoring (via nProbe)
- Continuous Traffic Recording
- Advanced network activity reports generation

“I'm paying for an International MPLS link and I want to understand how this bandwidth is used” [1/2]



Begin Date/Time: 28/03/2019 11:21:00

End Date/Time: 04/04/2019 12:21:00

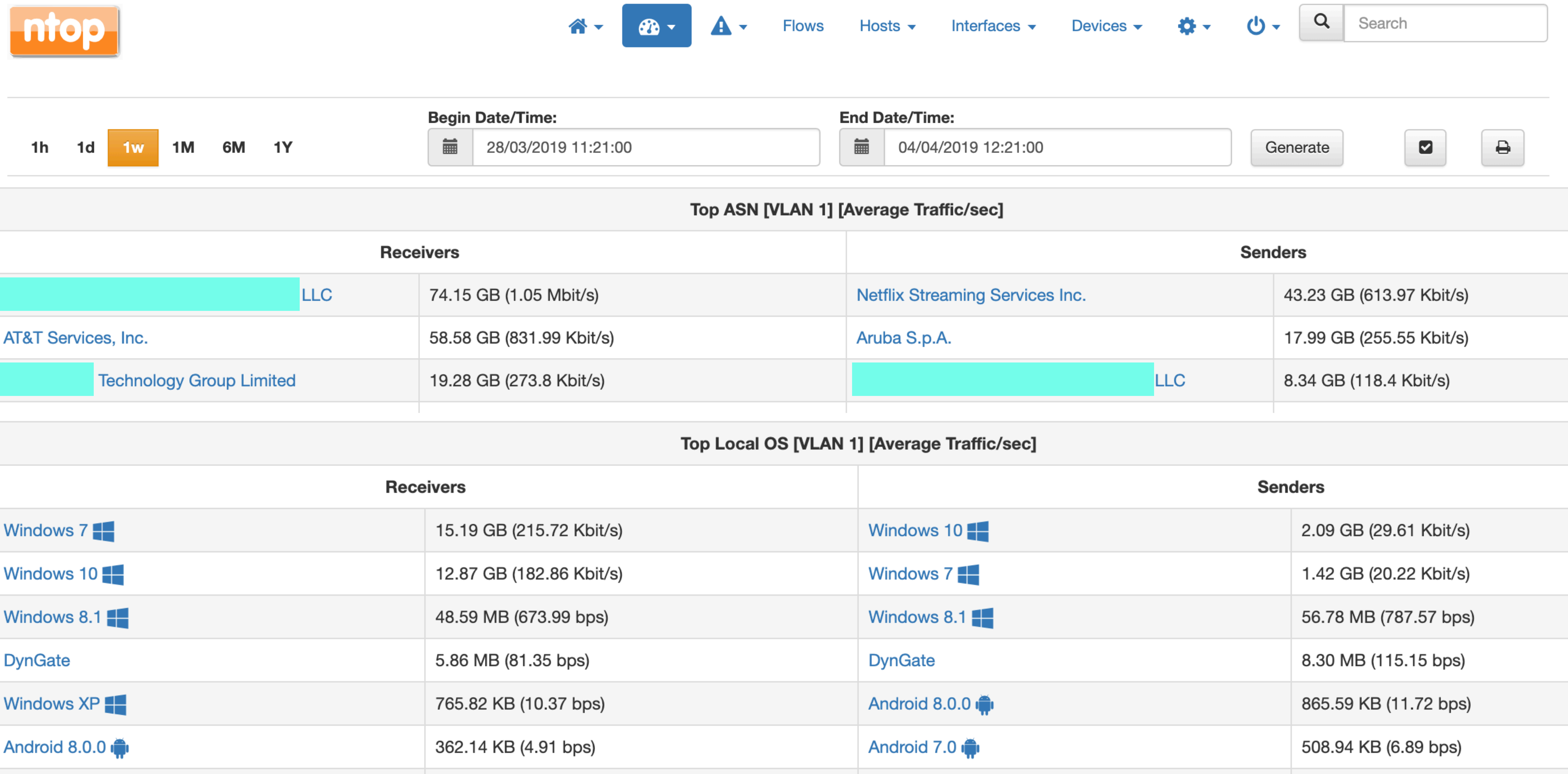
Applications

Total Traffic: 139.08 GB

Top Countries [VLAN 1] [Average Traffic/sec]

Receivers		**Senders**	
UA	74.17 GB (1.05 Mbit/s)	US	70.70 GB (1 Mbit/s)
US	60.76 GB (862.97 Kbit/s)	IT	39.42 GB (559.88 Kbit/s)
GB	20.28 GB (288.09 Kbit/s)	GB	11.95 GB (169.74 Kbit/s)
IT	3.71 GB (52.67 Kbit/s)	UA	8.24 GB (116.97 Kbit/s)
Other	3.39 GB (48.13 Kbit/s)	DE	5.72 GB (81.24 Kbit/s)

"I'm paying for an International MPLS link and I want to understand how this bandwidth is used" [2/2]



Begin Date/Time: 28/03/2019 11:21:00

End Date/Time: 04/04/2019 12:21:00

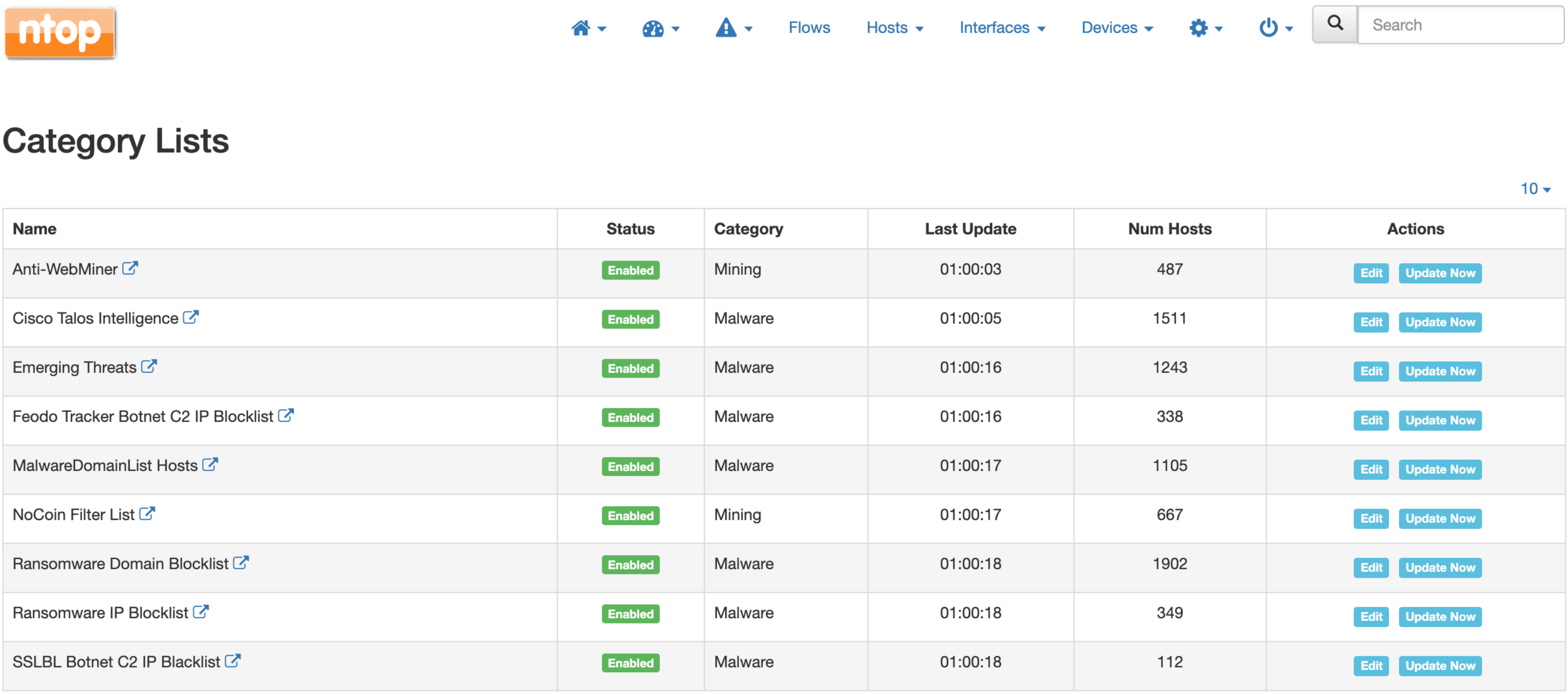
Top ASN [VLAN 1] [Average Traffic/sec]

Receivers		Senders	
[redacted] LLC	74.15 GB (1.05 Mbit/s)	Netflix Streaming Services Inc.	43.23 GB (613.97 Kbit/s)
AT&T Services, Inc.	58.58 GB (831.99 Kbit/s)	Aruba S.p.A.	17.99 GB (255.55 Kbit/s)
[redacted] Technology Group Limited	19.28 GB (273.8 Kbit/s)	[redacted] LLC	8.34 GB (118.4 Kbit/s)

Top Local OS [VLAN 1] [Average Traffic/sec]

Receivers		Senders	
Windows 7	15.19 GB (215.72 Kbit/s)	Windows 10	2.09 GB (29.61 Kbit/s)
Windows 10	12.87 GB (182.86 Kbit/s)	Windows 7	1.42 GB (20.22 Kbit/s)
Windows 8.1	48.59 MB (673.99 bps)	Windows 8.1	56.78 MB (787.57 bps)
DynGate	5.86 MB (81.35 bps)	DynGate	8.30 MB (115.15 bps)
Windows XP	765.82 KB (10.37 bps)	Android 8.0.0	865.59 KB (11.72 bps)
Android 8.0.0	362.14 KB (4.91 bps)	Android 7.0	508.94 KB (6.89 bps)

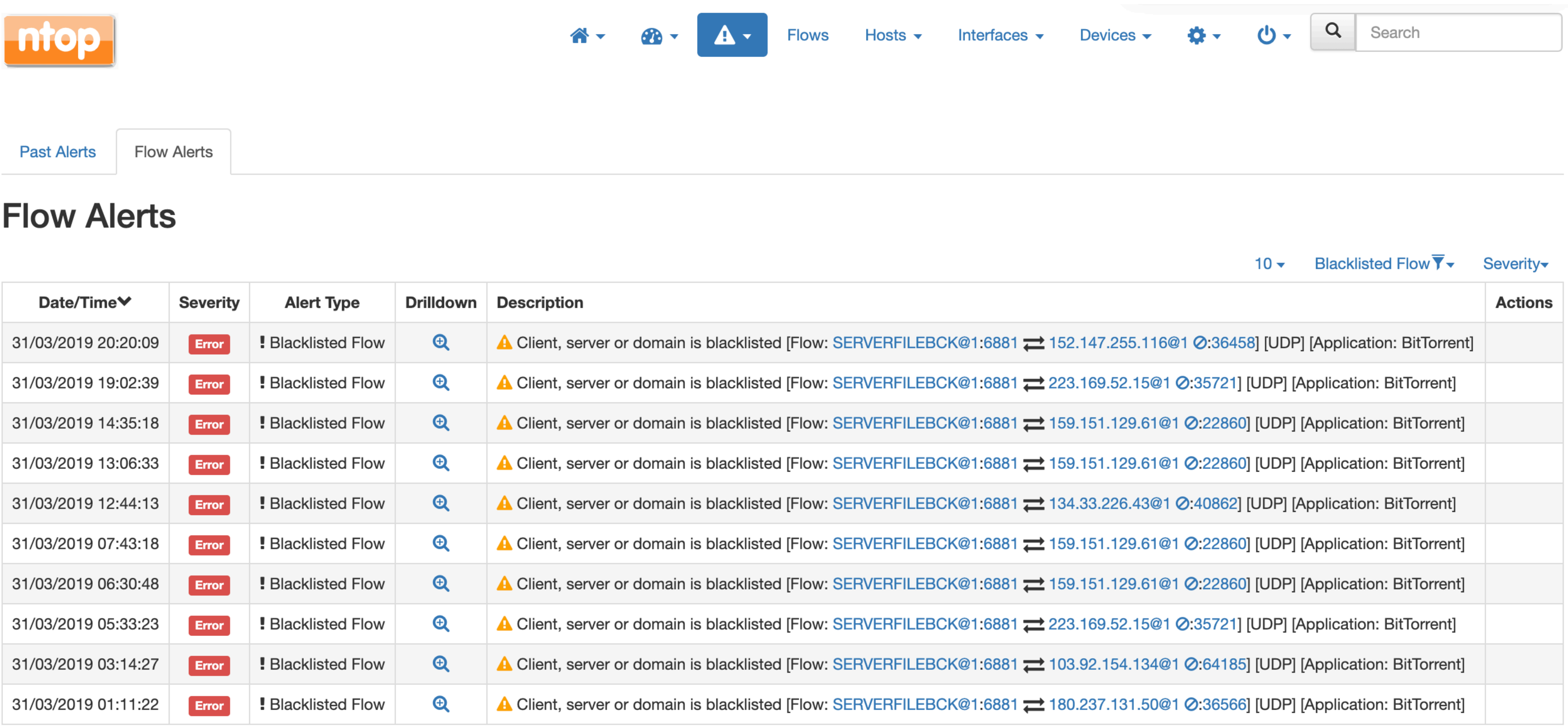
“I want to detect compromised hosts talking with the Internet” [1/2]



Category Lists

Name	Status	Category	Last Update	Num Hosts	Actions
Anti-WebMiner	Enabled	Mining	01:00:03	487	Edit Update Now
Cisco Talos Intelligence	Enabled	Malware	01:00:05	1511	Edit Update Now
Emerging Threats	Enabled	Malware	01:00:16	1243	Edit Update Now
Feodo Tracker Botnet C2 IP Blocklist	Enabled	Malware	01:00:16	338	Edit Update Now
MalwareDomainList Hosts	Enabled	Malware	01:00:17	1105	Edit Update Now
NoCoin Filter List	Enabled	Mining	01:00:17	667	Edit Update Now
Ransomware Domain Blocklist	Enabled	Malware	01:00:18	1902	Edit Update Now
Ransomware IP Blocklist	Enabled	Malware	01:00:18	349	Edit Update Now
SSLBL Botnet C2 IP Blacklist	Enabled	Malware	01:00:18	112	Edit Update Now

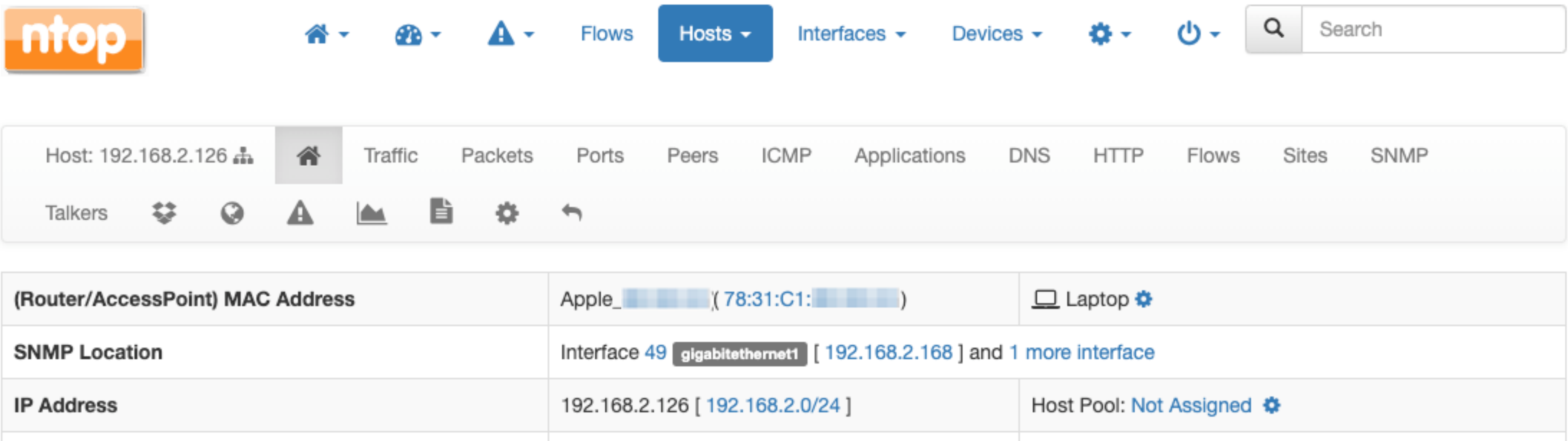
“I want to detect compromised hosts talking with the Internet” [2/2]



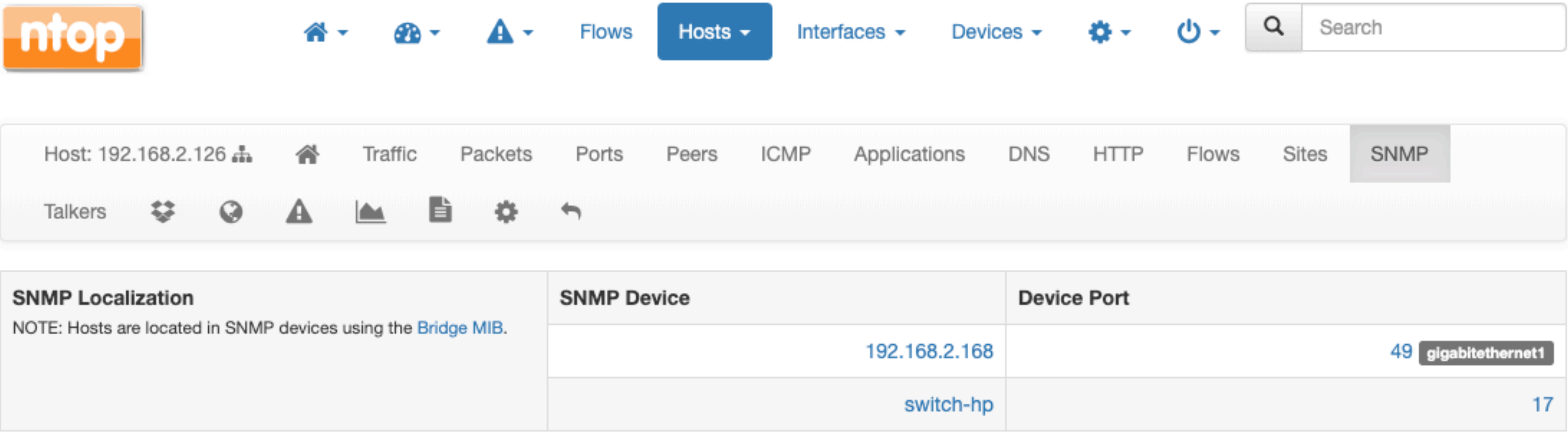
Flow Alerts

Date/Time	Severity	Alert Type	Drilldown	Description	Actions
31/03/2019 20:20:09	Error	! Blacklisted Flow	🔍	⚠ Client, server or domain is blacklisted [Flow: SERVERFILEBCK@1:6881 ⇄ 152.147.255.116@1 ⊘:36458] [UDP] [Application: BitTorrent]	
31/03/2019 19:02:39	Error	! Blacklisted Flow	🔍	⚠ Client, server or domain is blacklisted [Flow: SERVERFILEBCK@1:6881 ⇄ 223.169.52.15@1 ⊘:35721] [UDP] [Application: BitTorrent]	
31/03/2019 14:35:18	Error	! Blacklisted Flow	🔍	⚠ Client, server or domain is blacklisted [Flow: SERVERFILEBCK@1:6881 ⇄ 159.151.129.61@1 ⊘:22860] [UDP] [Application: BitTorrent]	
31/03/2019 13:06:33	Error	! Blacklisted Flow	🔍	⚠ Client, server or domain is blacklisted [Flow: SERVERFILEBCK@1:6881 ⇄ 159.151.129.61@1 ⊘:22860] [UDP] [Application: BitTorrent]	
31/03/2019 12:44:13	Error	! Blacklisted Flow	🔍	⚠ Client, server or domain is blacklisted [Flow: SERVERFILEBCK@1:6881 ⇄ 134.33.226.43@1 ⊘:40862] [UDP] [Application: BitTorrent]	
31/03/2019 07:43:18	Error	! Blacklisted Flow	🔍	⚠ Client, server or domain is blacklisted [Flow: SERVERFILEBCK@1:6881 ⇄ 159.151.129.61@1 ⊘:22860] [UDP] [Application: BitTorrent]	
31/03/2019 06:30:48	Error	! Blacklisted Flow	🔍	⚠ Client, server or domain is blacklisted [Flow: SERVERFILEBCK@1:6881 ⇄ 159.151.129.61@1 ⊘:22860] [UDP] [Application: BitTorrent]	
31/03/2019 05:33:23	Error	! Blacklisted Flow	🔍	⚠ Client, server or domain is blacklisted [Flow: SERVERFILEBCK@1:6881 ⇄ 223.169.52.15@1 ⊘:35721] [UDP] [Application: BitTorrent]	
31/03/2019 03:14:27	Error	! Blacklisted Flow	🔍	⚠ Client, server or domain is blacklisted [Flow: SERVERFILEBCK@1:6881 ⇄ 103.92.154.134@1 ⊘:64185] [UDP] [Application: BitTorrent]	
31/03/2019 01:11:22	Error	! Blacklisted Flow	🔍	⚠ Client, server or domain is blacklisted [Flow: SERVERFILEBCK@1:6881 ⇄ 180.237.131.50@1 ⊘:36566] [UDP] [Application: BitTorrent]	

“Where is a host physically located?”

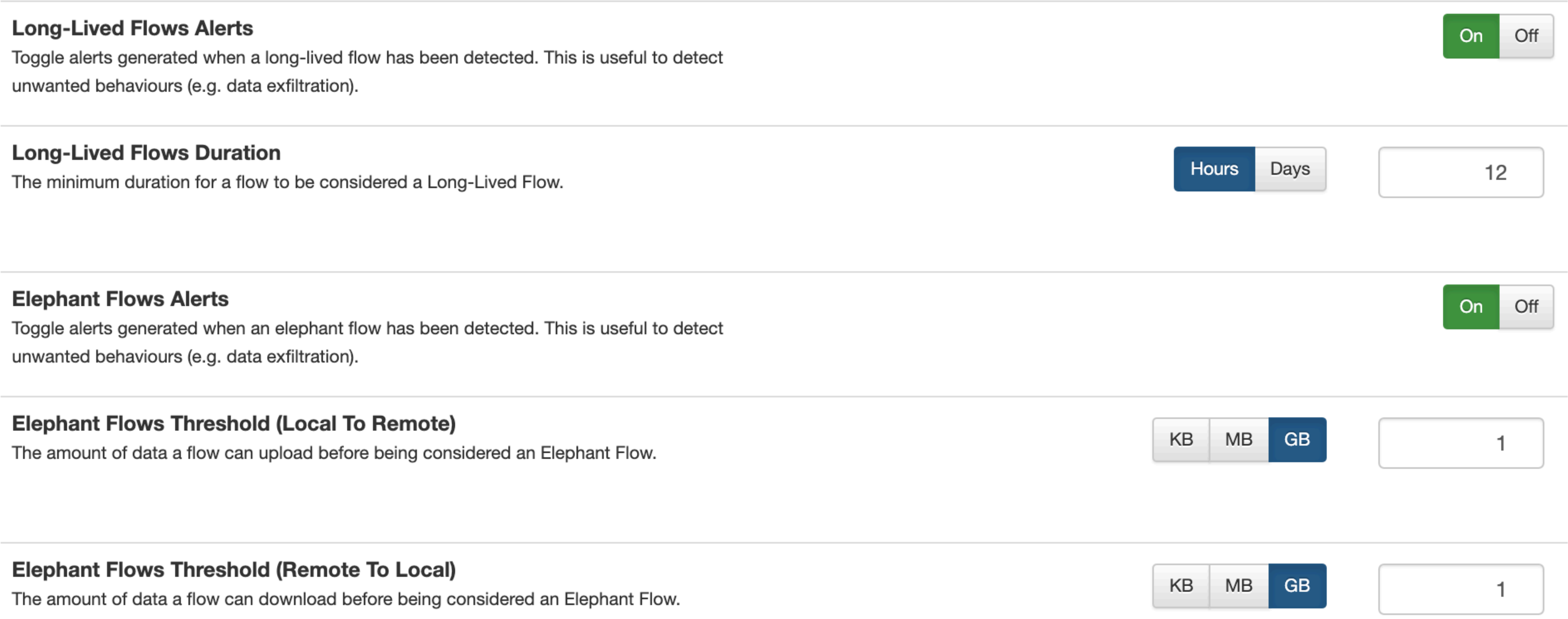


(Router/AccessPoint) MAC Address	Apple_[redacted](78:31:C1:[redacted])	Laptop
SNMP Location	Interface 49 gigabitethernet1 [192.168.2.168] and 1 more interface	
IP Address	192.168.2.126 [192.168.2.0/24]	Host Pool: Not Assigned



SNMP Localization	SNMP Device	Device Port
NOTE: Hosts are located in SNMP devices using the Bridge MIB.	192.168.2.168	49 gigabitethernet1
	switch-hp	17

“I want protection against data exfiltration” [1/2]



Long-Lived Flows Alerts
Toggle alerts generated when a long-lived flow has been detected. This is useful to detect unwanted behaviours (e.g. data exfiltration).
[✓ On] Off

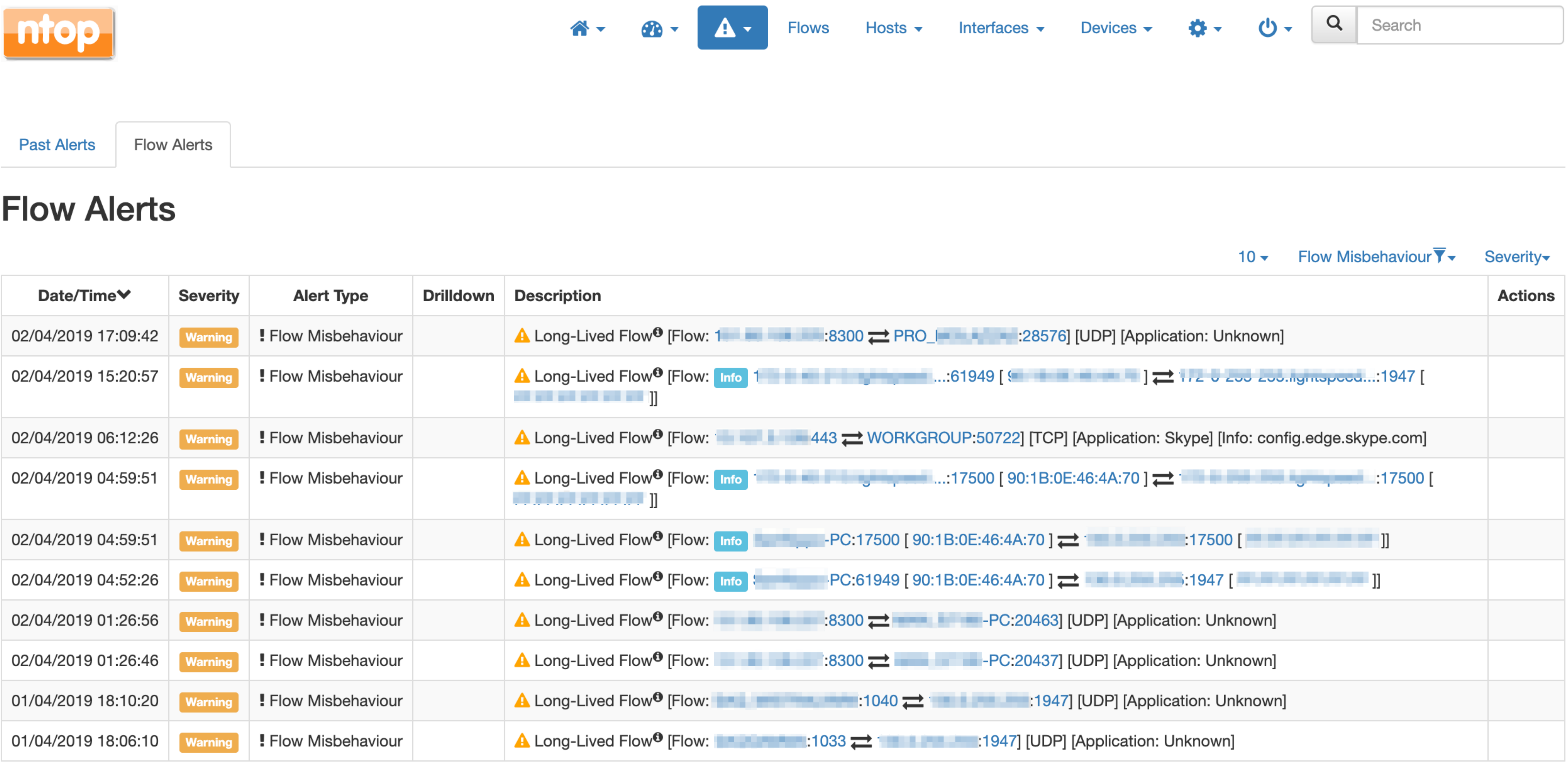
Long-Lived Flows Duration
The minimum duration for a flow to be considered a Long-Lived Flow.
[✓ Hours] Days 12

Elephant Flows Alerts
Toggle alerts generated when an elephant flow has been detected. This is useful to detect unwanted behaviours (e.g. data exfiltration).
[✓ On] Off

Elephant Flows Threshold (Local To Remote)
The amount of data a flow can upload before being considered an Elephant Flow.
KB MB [✓ GB] 1

Elephant Flows Threshold (Remote To Local)
The amount of data a flow can download before being considered an Elephant Flow.
KB MB [✓ GB] 1

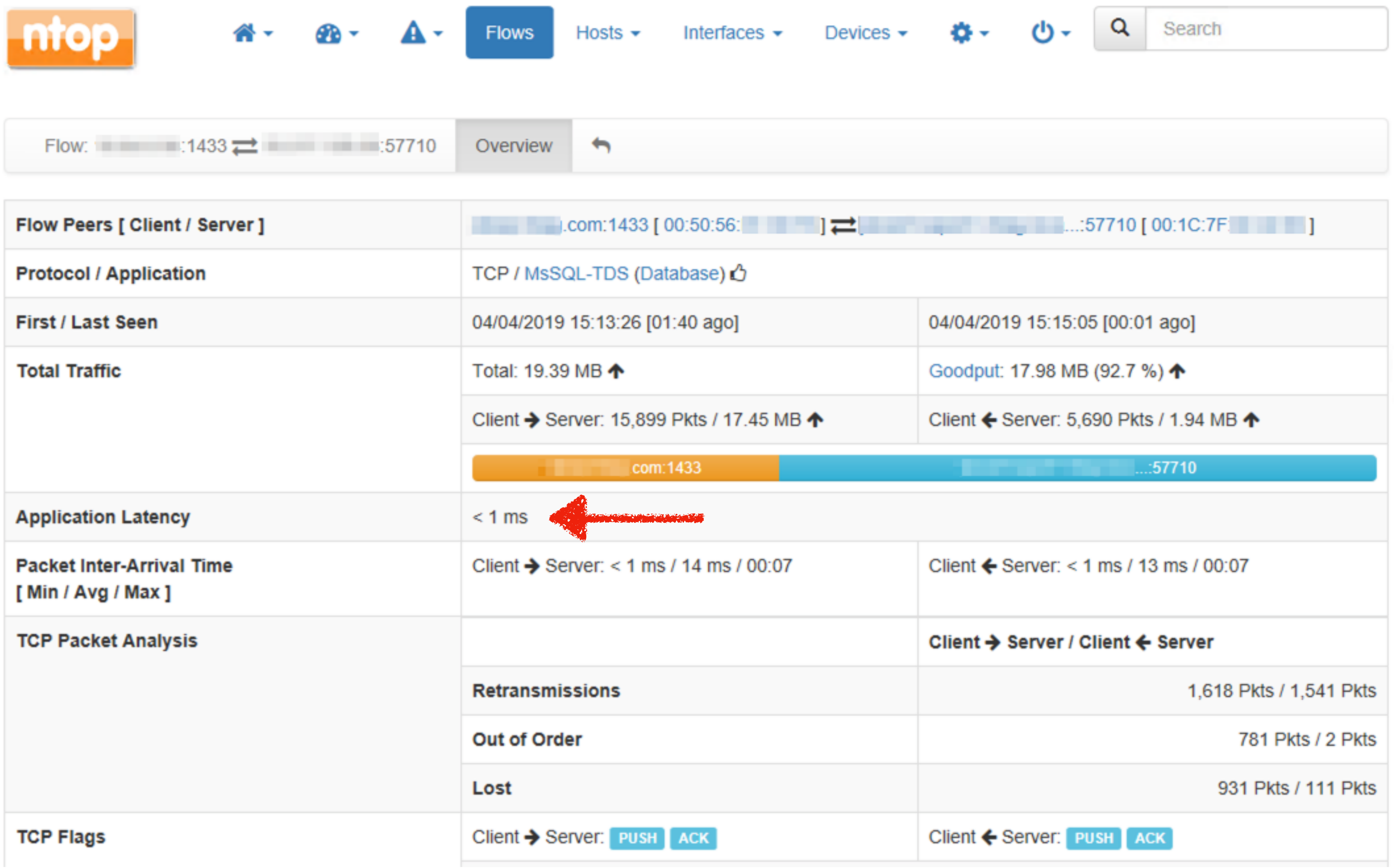
“I want protection against data exfiltration” [2/2]



Flow Alerts

Date/Time	Severity	Alert Type	Drilldown	Description	Actions
02/04/2019 17:09:42	Warning	! Flow Misbehaviour		⚠ Long-Lived Flow🛈 [Flow: [redacted]:8300 ⇄ PRO_[redacted]:28576] [UDP] [Application: Unknown]	
02/04/2019 15:20:57	Warning	! Flow Misbehaviour		⚠ Long-Lived Flow🛈 [Flow: Info [redacted]...:61949 [[redacted]] ⇄ [redacted]...:1947 [[redacted]]]	
02/04/2019 06:12:26	Warning	! Flow Misbehaviour		⚠ Long-Lived Flow🛈 [Flow: [redacted]443 ⇄ WORKGROUP:50722] [TCP] [Application: Skype] [Info: config.edge.skype.com]	
02/04/2019 04:59:51	Warning	! Flow Misbehaviour		⚠ Long-Lived Flow🛈 [Flow: Info [redacted]...:17500 [90:1B:0E:46:4A:70] ⇄ [redacted]:17500 [[redacted]]]	
02/04/2019 04:59:51	Warning	! Flow Misbehaviour		⚠ Long-Lived Flow🛈 [Flow: Info [redacted]-PC:17500 [90:1B:0E:46:4A:70] ⇄ [redacted]:17500 [[redacted]]]	
02/04/2019 04:52:26	Warning	! Flow Misbehaviour		⚠ Long-Lived Flow🛈 [Flow: Info [redacted]PC:61949 [90:1B:0E:46:4A:70] ⇄ [redacted]:1947 [[redacted]]]	
02/04/2019 01:26:56	Warning	! Flow Misbehaviour		⚠ Long-Lived Flow🛈 [Flow: [redacted]:8300 ⇄ [redacted]-PC:20463] [UDP] [Application: Unknown]	
02/04/2019 01:26:46	Warning	! Flow Misbehaviour		⚠ Long-Lived Flow🛈 [Flow: [redacted]:8300 ⇄ [redacted]-PC:20437] [UDP] [Application: Unknown]	
01/04/2019 18:10:20	Warning	! Flow Misbehaviour		⚠ Long-Lived Flow🛈 [Flow: [redacted]:1040 ⇄ [redacted]:1947] [UDP] [Application: Unknown]	
01/04/2019 18:06:10	Warning	! Flow Misbehaviour		⚠ Long-Lived Flow🛈 [Flow: [redacted]:1033 ⇄ [redacted]:1947] [UDP] [Application: Unknown]	

“I know that MySQL performs poorly with a latency above 300ms”



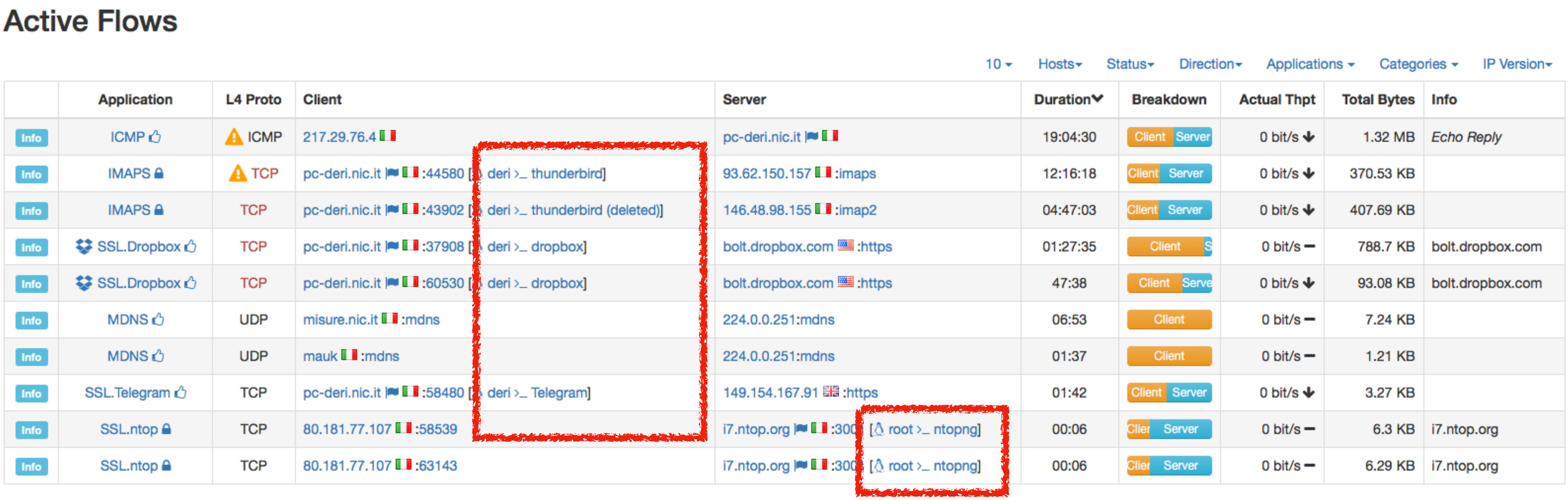
Flow: [redacted]:1433 ⇄ [redacted]:57710

Flow Peers [Client / Server]	[redacted].com:1433 [00:50:56:[redacted]] ⇄ [redacted]...:57710 [00:1C:7F[redacted]]	
Protocol / Application	TCP / MsSQL-TDS (Database)	
First / Last Seen	04/04/2019 15:13:26 [01:40 ago]	04/04/2019 15:15:05 [00:01 ago]
Total Traffic	Total: 19.39 MB ↑	Goodput: 17.98 MB (92.7 %) ↑
	Client → Server: 15,899 Pkts / 17.45 MB ↑	Client ← Server: 5,690 Pkts / 1.94 MB ↑
	[redacted]com:1433	[redacted]...:57710
Application Latency	< 1 ms	
Packet Inter-Arrival Time [Min / Avg / Max]	Client → Server: < 1 ms / 14 ms / 00:07	Client ← Server: < 1 ms / 13 ms / 00:07
TCP Packet Analysis		**Client → Server / Client ← Server**
	Retransmissions	1,618 Pkts / 1,541 Pkts
	Out of Order	781 Pkts / 2 Pkts
	Lost	931 Pkts / 111 Pkts
TCP Flags	Client → Server: PUSH ACK	Client ← Server: PUSH ACK

Towards Containerized Environments

- Open our engine to VM and containers monitoring through eBPF that is now supported in all latest mainstream distributions.
  - Incoming TCP/UDP events are mapped to packets monitored by ntopng.
  - We’ve added user/process/flow integration and implemented process, container, pod’s and user statistics.

Merging Network and System Events



Active Flows

10 ▾ Hosts▾ Status▾ Direction▾ Applications ▾ Categories ▾ IP Version▾

	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	ICMP 👍	⚠ ICMP	217.29.76.4	pc-deri.nic.it	19:04:30	Client Server	0 bit/s ↓	1.32 MB	*Echo Reply*
Info	IMAPS 🔒	⚠ TCP	pc-deri.nic.it :44580 [deri >_ thunderbird]	93.62.150.157 :imaps	12:16:18	Client Server	0 bit/s ↓	370.53 KB	
Info	IMAPS 🔒	TCP	pc-deri.nic.it :43902 [deri >_ thunderbird (deleted)]	146.48.98.155 :imap2	04:47:03	Client Server	0 bit/s ↓	407.69 KB	
Info	SSL.Dropbox 👍	TCP	pc-deri.nic.it :37908 [deri >_ dropbox]	bolt.dropbox.com :https	01:27:35	Client S	0 bit/s —	788.7 KB	bolt.dropbox.com
Info	SSL.Dropbox 👍	TCP	pc-deri.nic.it :60530 [deri >_ dropbox]	bolt.dropbox.com :https	47:38	Client Serve	0 bit/s ↓	93.08 KB	bolt.dropbox.com
Info	MDNS 👍	UDP	misure.nic.it :mdns	224.0.0.251:mdns	06:53	Client	0 bit/s —	7.24 KB	
Info	MDNS 👍	UDP	mauk :mdns	224.0.0.251:mdns	01:37	Client	0 bit/s —	1.21 KB	
Info	SSL.Telegram 👍	TCP	pc-deri.nic.it :58480 [deri >_ Telegram]	149.154.167.91 :https	01:42	Client Server	0 bit/s ↓	3.27 KB	
Info	SSL.ntop 🔒	TCP	80.181.77.107 :58539	i7.ntop.org :300 [root >_ ntopng]	00:06	Clier Server	0 bit/s —	6.3 KB	i7.ntop.org
Info	SSL.ntop 🔒	TCP	80.181.77.107 :63143	i7.ntop.org :300 [root >_ ntopng]	00:06	Clier Server	0 bit/s —	6.29 KB	i7.ntop.org

Final Remarks [1/2]

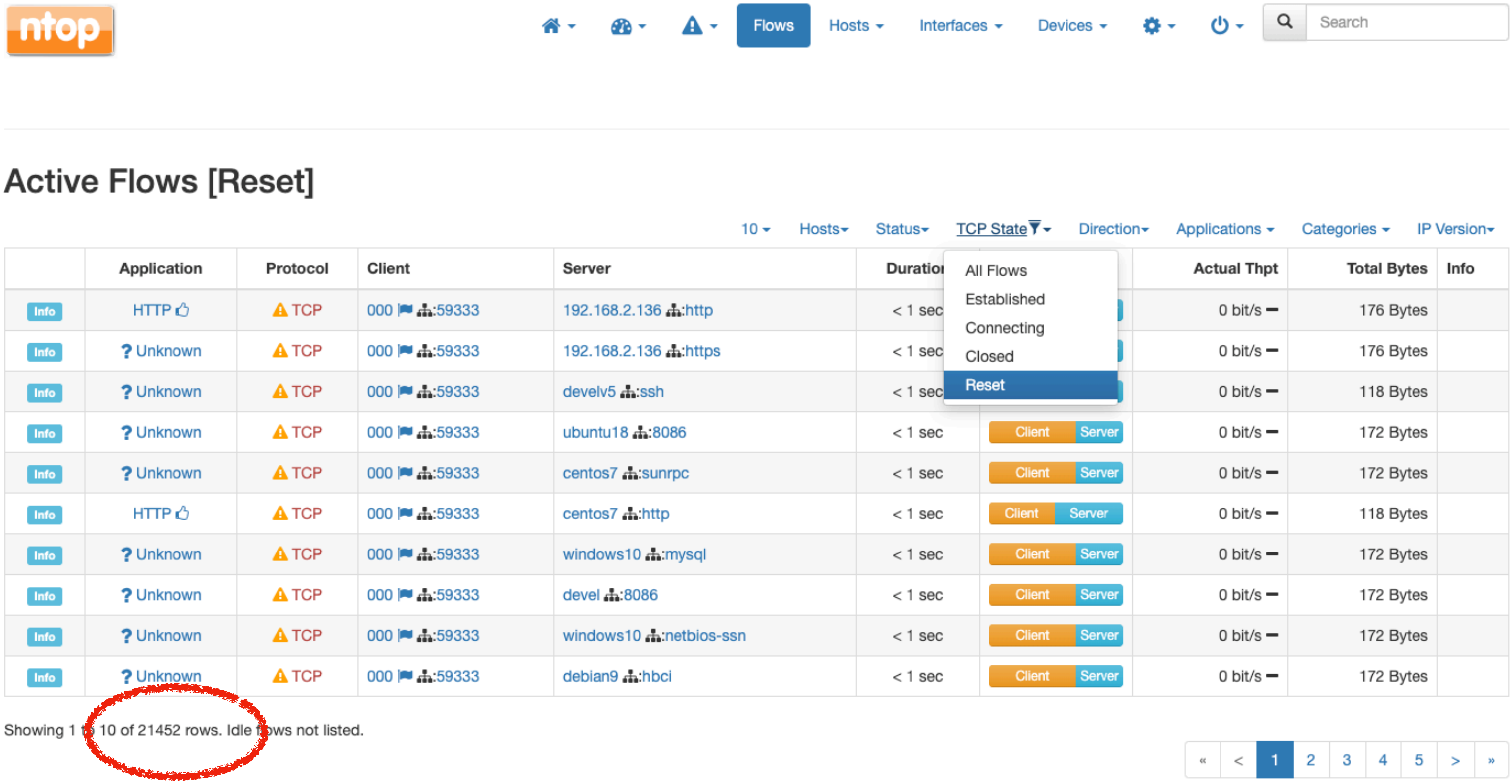
- While ntopng has preserved its open-source monitoring engine designed for simple traffic monitoring, it proves to be enterprise-ready for
  - North-South and East West Visibility
  - Misbehaving/Infected hosts detection
  - Bandwidth usage and allocation
- It can be used as stand-alone solution or as a feed for other monitoring solutions.

Final Remarks [2/2]

- ntop and Würth Phoenix are partnering to integrate ntopng Enterprise and NetEye4
- ntop experience in enterprise network visibility contributes in making NetEye4 one of the most complete **unified monitoring solutions** in the market

Appendix & Backup Material

“Are there any misbehaving hosts in the network?” [1/3]

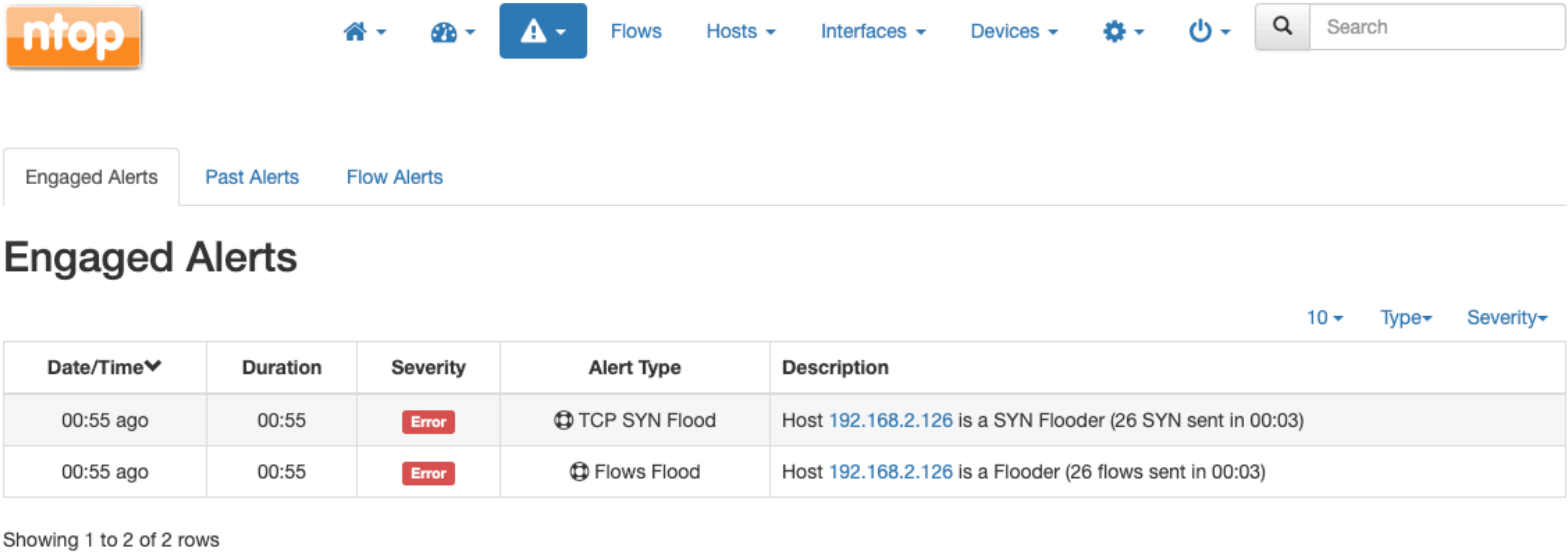


Active Flows [Reset]

	Application	Protocol	Client	Server	Duratio		Actual Thpt	Total Bytes	Info
Info	HTTP	TCP	000 :59333	192.168.2.136 :http	< 1 sec		0 bit/s	176 Bytes	
Info	? Unknown	TCP	000 :59333	192.168.2.136 :https	< 1 sec		0 bit/s	176 Bytes	
Info	? Unknown	TCP	000 :59333	develv5 :ssh	< 1 sec		0 bit/s	118 Bytes	
Info	? Unknown	TCP	000 :59333	ubuntu18 :8086	< 1 sec	Client Server	0 bit/s	172 Bytes	
Info	? Unknown	TCP	000 :59333	centos7 :sunrpc	< 1 sec	Client Server	0 bit/s	172 Bytes	
Info	HTTP	TCP	000 :59333	centos7 :http	< 1 sec	Client Server	0 bit/s	118 Bytes	
Info	? Unknown	TCP	000 :59333	windows10 :mysql	< 1 sec	Client Server	0 bit/s	172 Bytes	
Info	? Unknown	TCP	000 :59333	devel :8086	< 1 sec	Client Server	0 bit/s	172 Bytes	
Info	? Unknown	TCP	000 :59333	windows10 :netbios-ssn	< 1 sec	Client Server	0 bit/s	172 Bytes	
Info	? Unknown	TCP	000 :59333	debian9 :hbci	< 1 sec	Client Server	0 bit/s	172 Bytes	

Showing 1 to 10 of 21452 rows. Idle flows not listed.

"Are there any misbehaving hosts in the network?" [2/3]

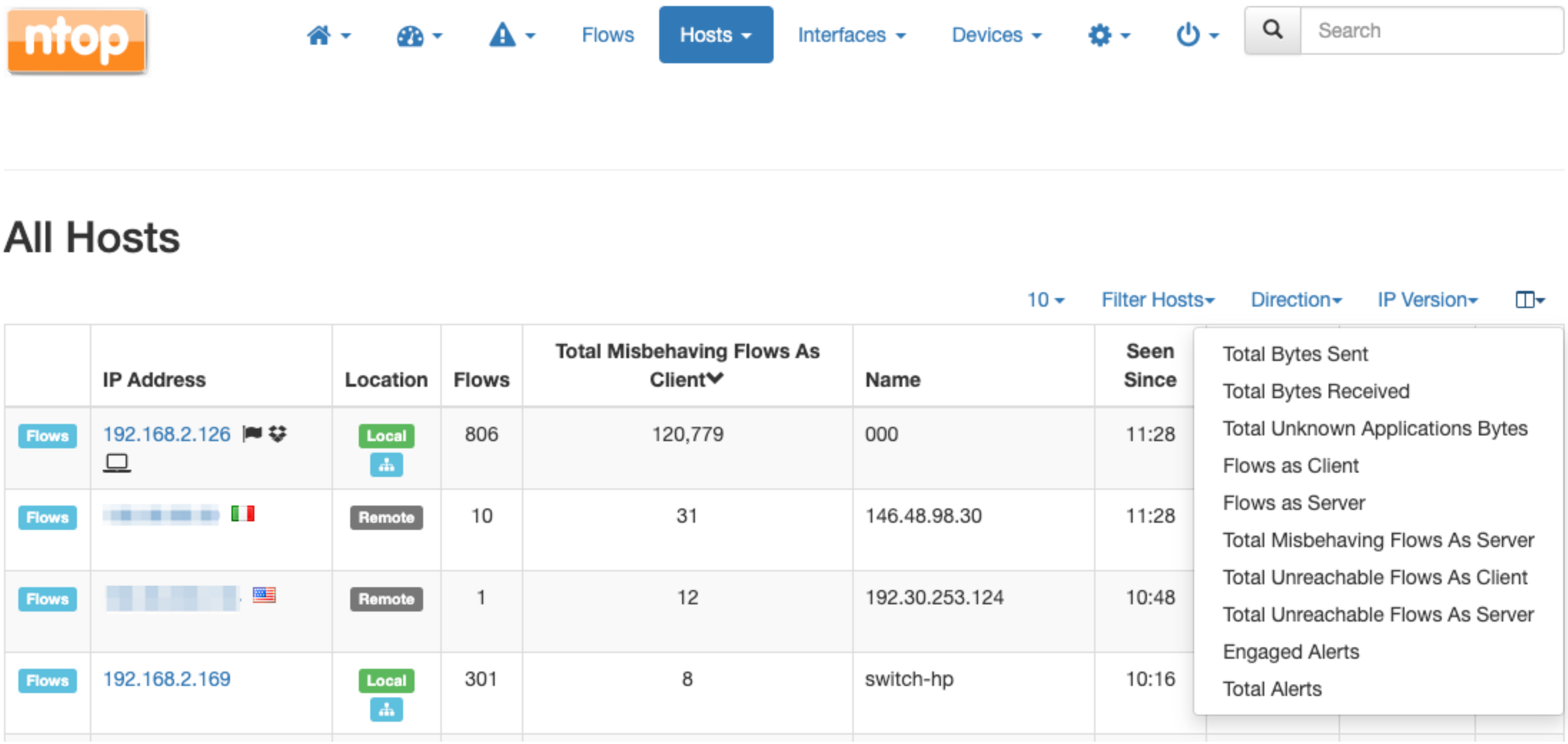


Engaged Alerts

Date/Time	Duration	Severity	Alert Type	Description
00:55 ago	00:55	Error	TCP SYN Flood	Host 192.168.2.126 is a SYN Flooder (26 SYN sent in 00:03)
00:55 ago	00:55	Error	Flows Flood	Host 192.168.2.126 is a Flooder (26 flows sent in 00:03)

Showing 1 to 2 of 2 rows

“Are there any misbehaving hosts in the network?” [3/3]



All Hosts

	IP Address	Location	Flows	Total Misbehaving Flows As Client	Name	Seen Since
Flows	192.168.2.126	Local	806	120,779	000	11:28
Flows	[redacted]	Remote	10	31	146.48.98.30	11:28
Flows	[redacted]	Remote	1	12	192.30.253.124	10:48
Flows	192.168.2.169	Local	301	8	switch-hp	10:16

Active Monitoring

- While passive traffic monitoring is still the core task, we will be expanding active monitoring beyond SNMP aiming at
  - Majoring latency and service availability of remote sites including ping, http(s) and user-scripts.
  - Monitor host services and processes

Big-Data Made Personal

- ntopng currently supports MySQL and Elastic for non time-series data such as flows.
- Since 2016 we're working at a high-speed indexing system, named nIndex, able to perform million inserts/sec while providing sub-second query responses on billion of records on a single node machine.
- nIndex is currently in beta (see -F) but we are close to the first stable release