ntopng and Suricata: Merging Network Visibility and Security

Luca Deri <deri@ntop.org>, @lucaderi
Alfredo Cardigliano <cardigliano@ntop.org>

About ntop

- ntop develops open source network traffic monitoring applications. All code is available at https://github.com/ntop

- ntop is a community: http://t.me/ntop_community

- Part of the Intel Innovator program.

- ntop is also the name of the first app we released in 1998, a web-based network monitoring application (today ntopng).

- Today our tools range from traffic monitoring (ntopng, nProbe), high-speed packet capture (PF_RING), Deep-Packet Inspection (nDPI), traffic recording (n2disk), DDoS mitigation (nScrub), IDS/IPS acceleration.

Network Visibility

- Network visibility ensures that you are able to see everything happening on a network. It includes:
  - Network performance
  - Application performance
  - Devices discovery
- ntopng is a web-based open-source traffic analysis application that aims to provide full network visibility.

Uncorrelated Security Events

- Suricata, as well as other IDS systems, is commonly used to generate alarms when security threats are detected, and produce logs with suspicious network activities.

- There are many tools collecting logs produced by Suricata, and pushing them to system like ElasticSearch. The best they can do is index them and produce statistics: “Tell me how many Policy Violations we got today”.

- Threat detection is typically limited to a single session (see decode-events.c, app-layer-events.c) and it is (mostly) based on signatures matching. Suricata is basically a pure network sensor with no mechanisms for correlating information across multiple flows or hosts.

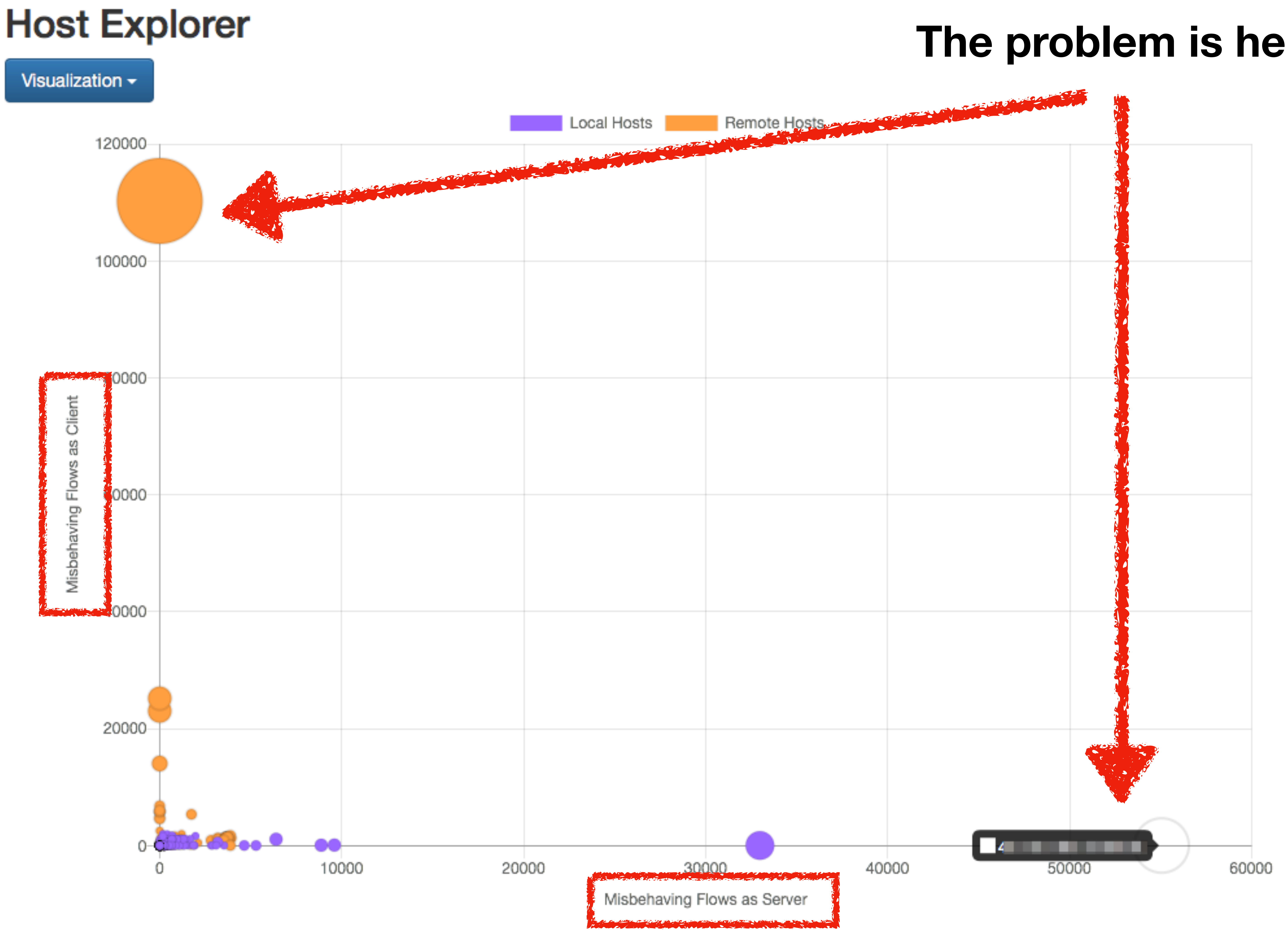
Augmented Security

- Network administrators need a clear picture of the traffic flowing into their network and place security events in the right context.

- Correlating security events with network traffic provides a better visibility of what's going on and the root cause of threats.

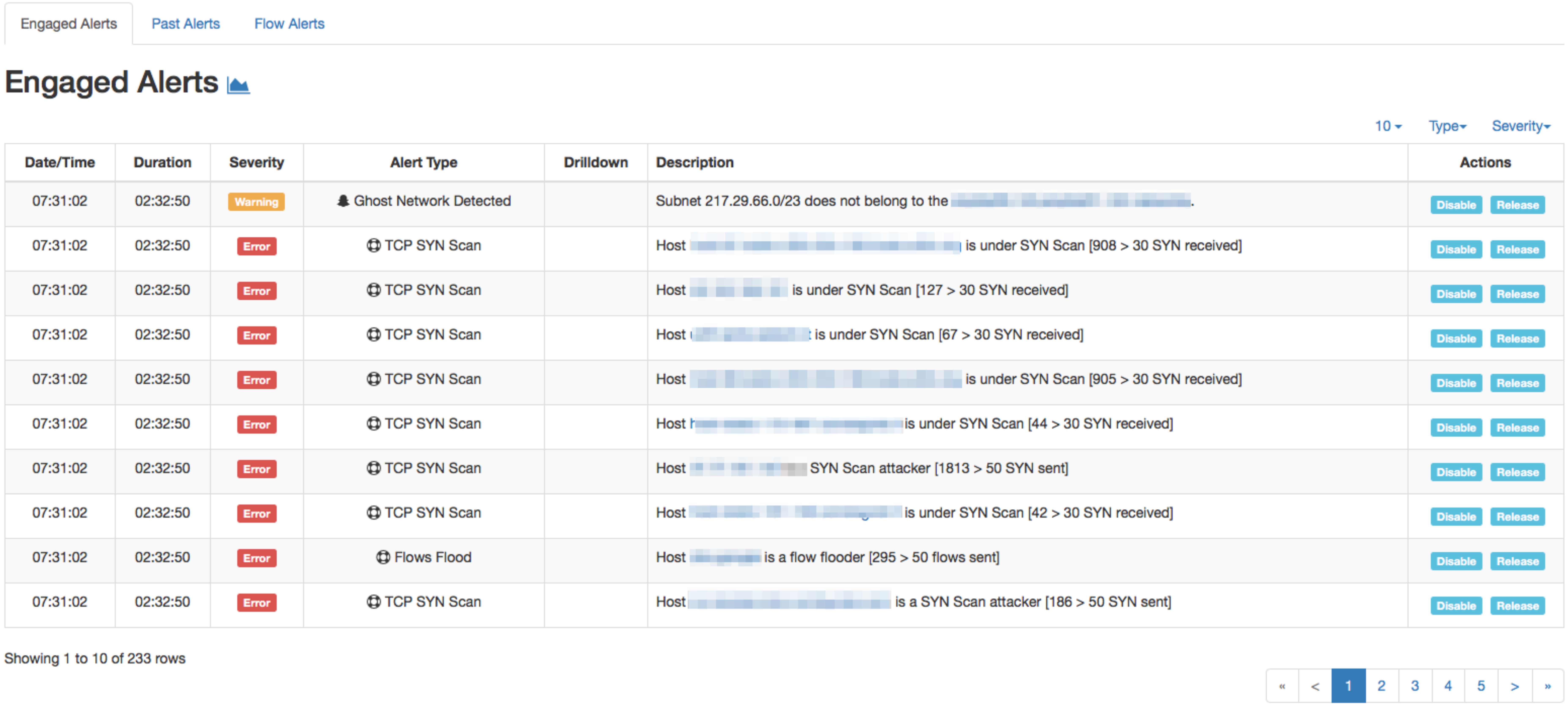
- Single events that can be considered harmless when looking at them individually, could be small pieces of bigger harmful events.

ntopng Troubleshooting [1/2]



The problem is here

ntopng Troubleshooting [2/2]



Engaged Alerts

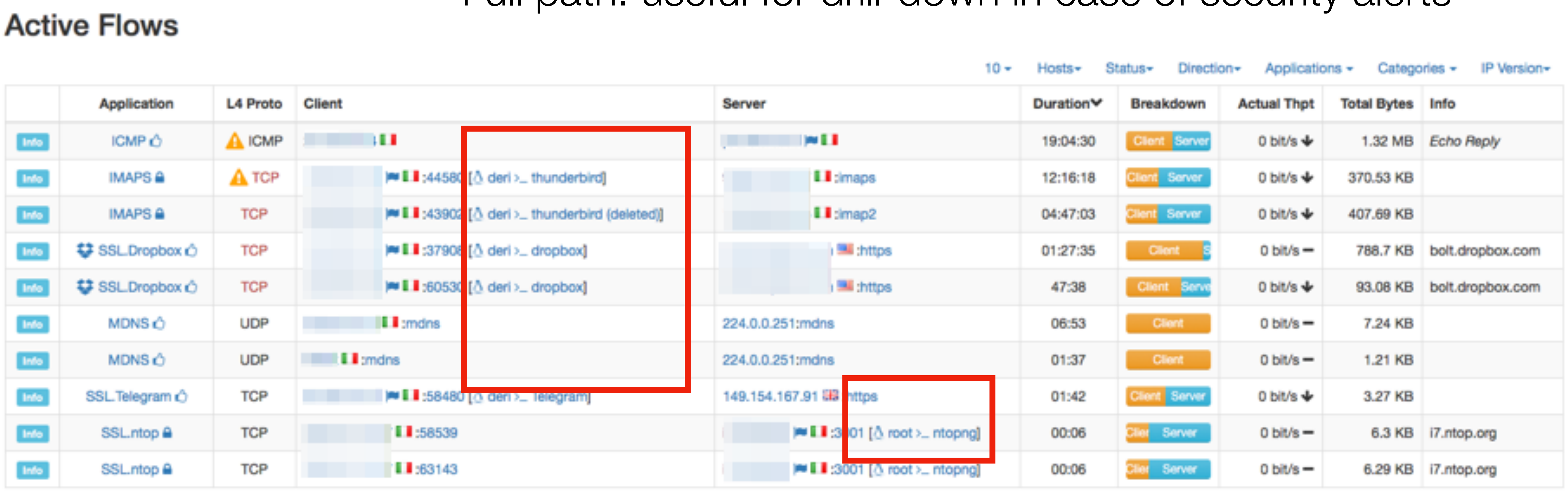
Date/Time	Duration	Severity	Alert Type	Drilldown	Description	Actions
07:31:02	02:32:50	Warning	Ghost Network Detected		Subnet 217.29.66.0/23 does not belong to the [redacted].	Disable Release
07:31:02	02:32:50	Error	TCP SYN Scan		Host [redacted] is under SYN Scan [908 > 30 SYN received]	Disable Release
07:31:02	02:32:50	Error	TCP SYN Scan		Host [redacted] is under SYN Scan [127 > 30 SYN received]	Disable Release
07:31:02	02:32:50	Error	TCP SYN Scan		Host [redacted] is under SYN Scan [67 > 30 SYN received]	Disable Release
07:31:02	02:32:50	Error	TCP SYN Scan		Host [redacted] is under SYN Scan [905 > 30 SYN received]	Disable Release
07:31:02	02:32:50	Error	TCP SYN Scan		Host [redacted] is under SYN Scan [44 > 30 SYN received]	Disable Release
07:31:02	02:32:50	Error	TCP SYN Scan		Host [redacted] SYN Scan attacker [1813 > 50 SYN sent]	Disable Release
07:31:02	02:32:50	Error	TCP SYN Scan		Host [redacted] is under SYN Scan [42 > 30 SYN received]	Disable Release
07:31:02	02:32:50	Error	Flows Flood		Host [redacted] is a flow flooder [295 > 50 flows sent]	Disable Release
07:31:02	02:32:50	Error	TCP SYN Scan		Host [redacted] is a SYN Scan attacker [186 > 50 SYN sent]	Disable Release

Showing 1 to 10 of 233 rows

ntopng Features and Limitations [1/2]

- Host system and containers monitoring through eBPF
- Process, container, POD and user statistics

Full path: useful for drill-down in case of security alerts

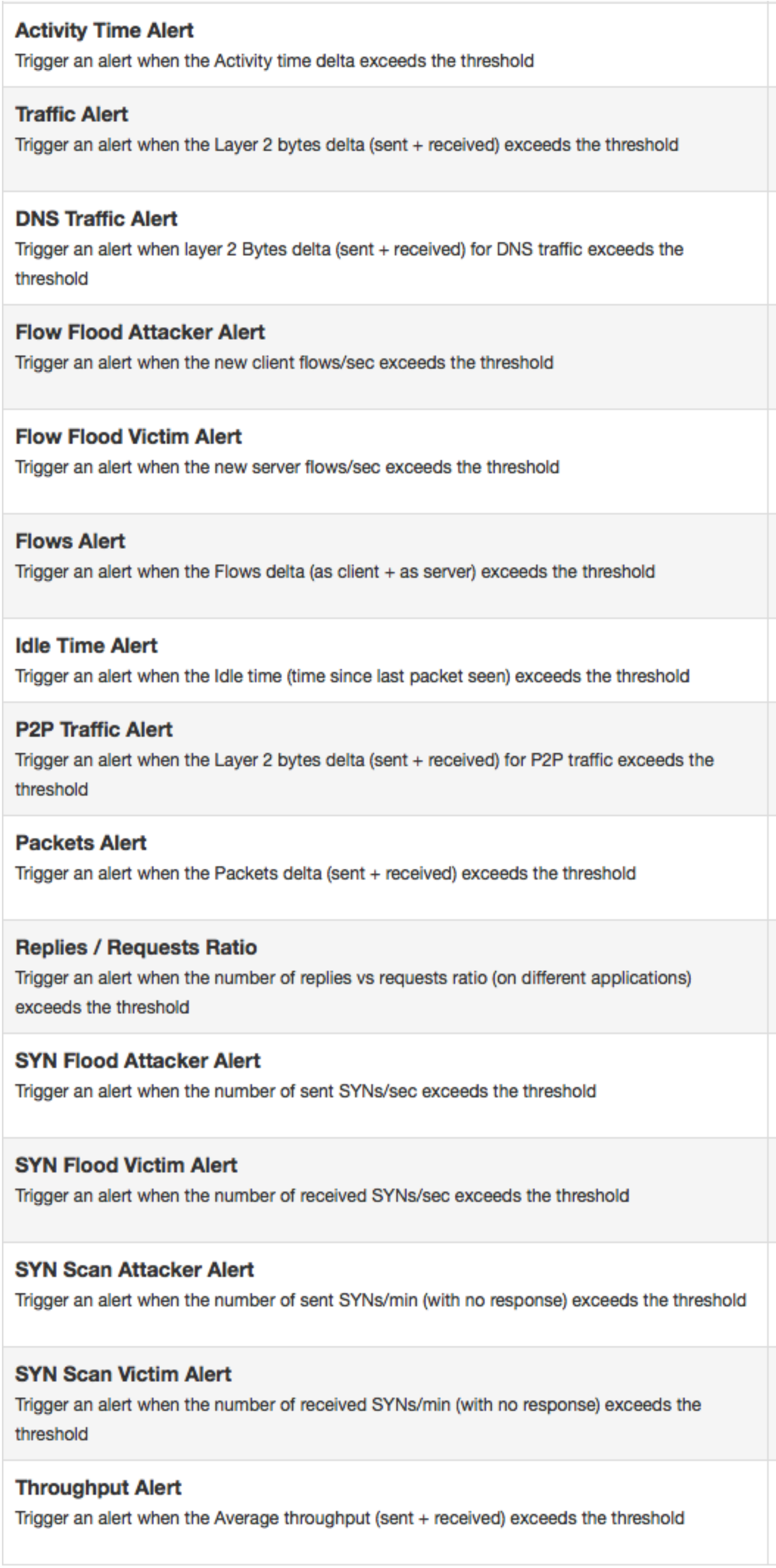


Active Flows

	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	ICMP	⚠ ICMP	[redacted]	[redacted]	19:04:30	Client Server	0 bit/s ↓	1.32 MB	*Echo Reply*
Info	IMAPS	⚠ TCP	[redacted] :44580 [deri >_ thunderbird]	[redacted] :imaps	12:16:18	Client Server	0 bit/s ↓	370.53 KB	
Info	IMAPS	TCP	[redacted] :43902 [deri >_ thunderbird (deleted)]	[redacted] :imap2	04:47:03	Client Server	0 bit/s ↓	407.69 KB	
Info	SSL.Dropbox	TCP	[redacted] :37908 [deri >_ dropbox]	[redacted] :https	01:27:35	Client S	0 bit/s –	788.7 KB	bolt.dropbox.com
Info	SSL.Dropbox	TCP	[redacted] :60530 [deri >_ dropbox]	[redacted] :https	47:38	Client Serve	0 bit/s ↓	93.08 KB	bolt.dropbox.com
Info	MDNS	UDP	[redacted] :mdns	224.0.0.251:mdns	06:53	Client	0 bit/s –	7.24 KB	
Info	MDNS	UDP	[redacted] :mdns	224.0.0.251:mdns	01:37	Client	0 bit/s –	1.21 KB	
Info	SSL.Telegram	TCP	[redacted] :58480 [deri >_ Telegram]	149.154.167.91 :https	01:42	Client Server	0 bit/s ↓	3.27 KB	
Info	SSL.ntop	TCP	[redacted] :58539	[redacted] :3001 [root >_ ntopng]	00:06	Clie Server	0 bit/s –	6.3 KB	i7.ntop.org
Info	SSL.ntop	TCP	[redacted] :63143	[redacted] :3001 [root >_ ntopng]	00:06	Clie Server	0 bit/s –	6.29 KB	i7.ntop.org

ntopng Features and Limitations [2/2]

- ntopng features:
    - Network traffic metrics
    - Anomaly detection
    - Blacklists for malware detection
- It lacks security features including:
    - Threat detection
    - Signatures support
    - File extraction



Activity Time Alert
Trigger an alert when the Activity time delta exceeds the threshold

Traffic Alert
Trigger an alert when the Layer 2 bytes delta (sent + received) exceeds the threshold

DNS Traffic Alert
Trigger an alert when layer 2 Bytes delta (sent + received) for DNS traffic exceeds the threshold

Flow Flood Attacker Alert
Trigger an alert when the new client flows/sec exceeds the threshold

Flow Flood Victim Alert
Trigger an alert when the new server flows/sec exceeds the threshold

Flows Alert
Trigger an alert when the Flows delta (as client + as server) exceeds the threshold

Idle Time Alert
Trigger an alert when the Idle time (time since last packet seen) exceeds the threshold

P2P Traffic Alert
Trigger an alert when the Layer 2 bytes delta (sent + received) for P2P traffic exceeds the threshold

Packets Alert
Trigger an alert when the Packets delta (sent + received) exceeds the threshold

Replies / Requests Ratio
Trigger an alert when the number of replies vs requests ratio (on different applications) exceeds the threshold

SYN Flood Attacker Alert
Trigger an alert when the number of sent SYNs/sec exceeds the threshold

SYN Flood Victim Alert
Trigger an alert when the number of received SYNs/sec exceeds the threshold

SYN Scan Attacker Alert
Trigger an alert when the number of sent SYNs/min (with no response) exceeds the threshold

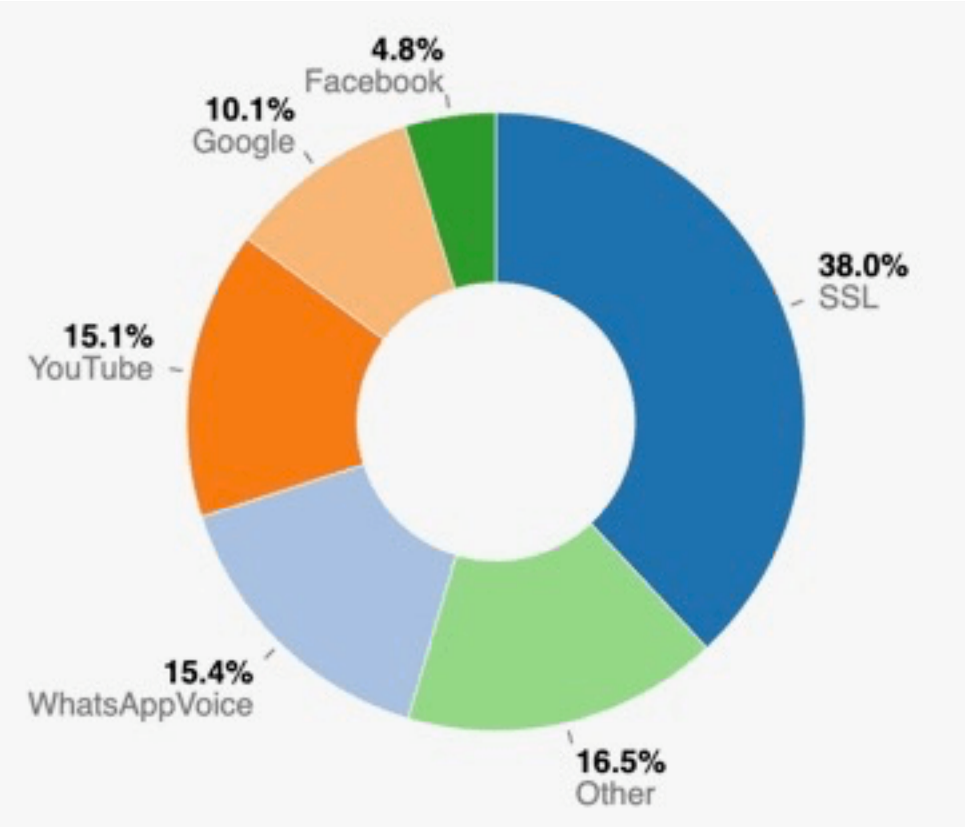
SYN Scan Victim Alert
Trigger an alert when the number of received SYNs/min (with no response) exceeds the threshold

Throughput Alert
Trigger an alert when the Average throughput (sent + received) exceeds the threshold

Suricata Limitations

- It does not use any DPI (Deep Packet Inspection) techniques to identify traffic regardless of the port is uses:
  - Running a service on a non standard port might be invisible to it.

    alert tcp $HOME_NET any -> $EXTERNAL_NET ![25,587,6666:7000,8076] (msg:"ET POLICY IRC Channel JOIN on non-standard port"
  - No information about flows/protocols not dissected by Suricata.



- No encrypted traffic analysis (i.e. Cisco Joy-like technologies) beside protocol fingerprinting: the idea is to be able to decode traffic, but unencrypted traffic is becoming rare, and this has impact on visibility.
- It does not provide any facility that could help users to understand the “big picture” (e.g. ARP scan, DNS negative/positive response ratio, or too many host active flows with respect) as it focuses on per-flow analysis.

Motivation: Unify Visibility and Security [1/2]

- Suricata is a great tool for dissecting selected protocols, extracting key metrics, and emitting alerts based on flow content driven by external rules.

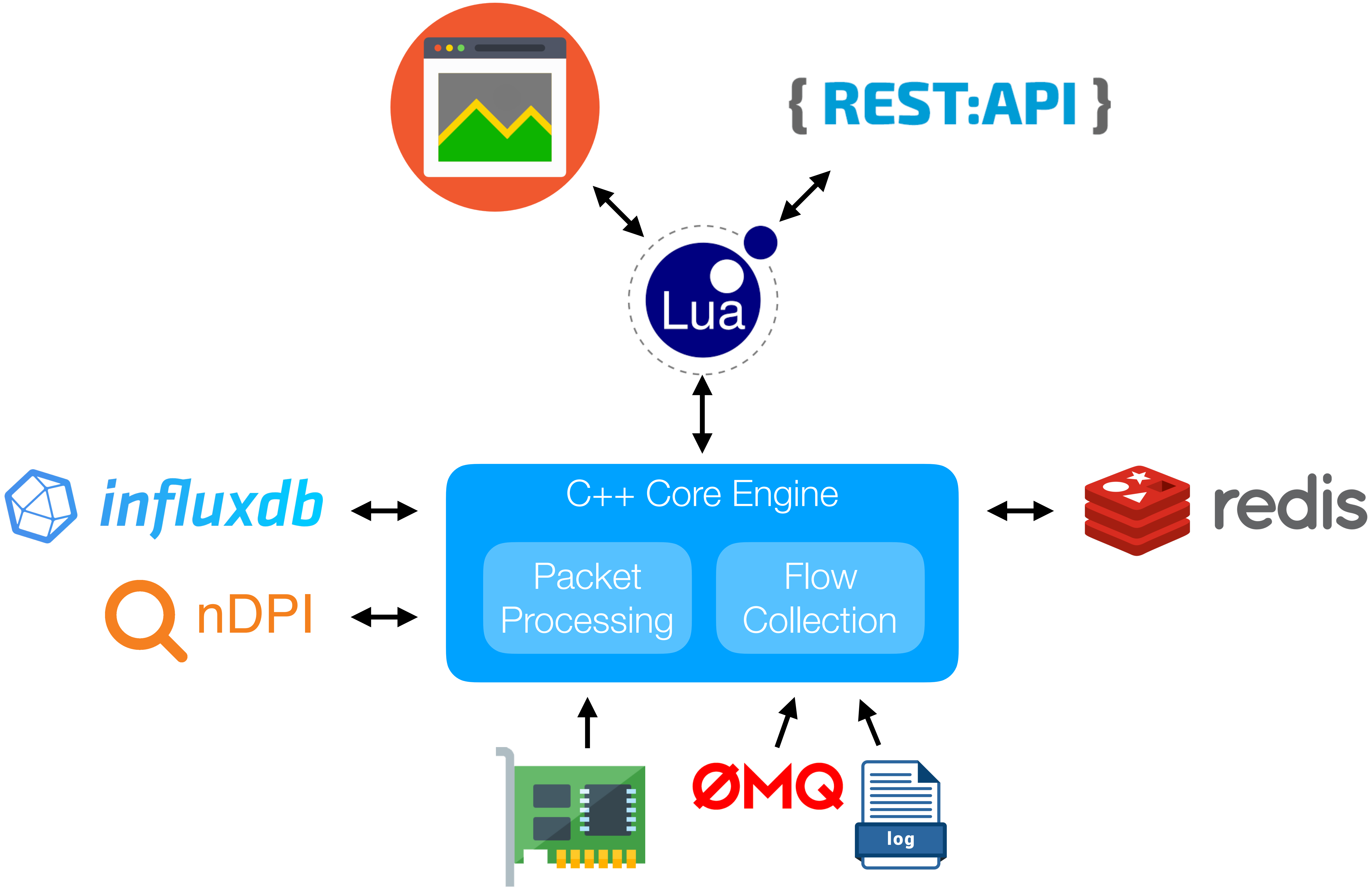
- ntopng is able to collect information from various sources (packets, NetFlow, sFlow), analyse them in a comprehensive format, and emit alerts. All in one place, with minimal requirements.

- What if we can unify these two open source tools into a single tool able to provide the best solution for complementing security and visibility? Seamlessly.

Motivation: Unify Visibility and Security [2/2]

- Benefits for the Suricata community:
  - Provide a web GUI to Suricata. Someone might say: there are many (ELK-based) tools that do that. True but they lack network visibility, require third parties DBs/tools, and are not been designed for networking/security.
  - Enhance Suricata with network metrics not reported by the tool.
  - Provide existing Suricata users with ntop features (e.g. nIndex-based efficient flow-storage or Slack-based alerts).
- Benefits for the ntop community:
  - Add the benefits of signature-based traffic analysis.
  - Merge Suricata traffic alerts with those already handled by ntopng to implement the best of both worlds.

ntopng Architecture

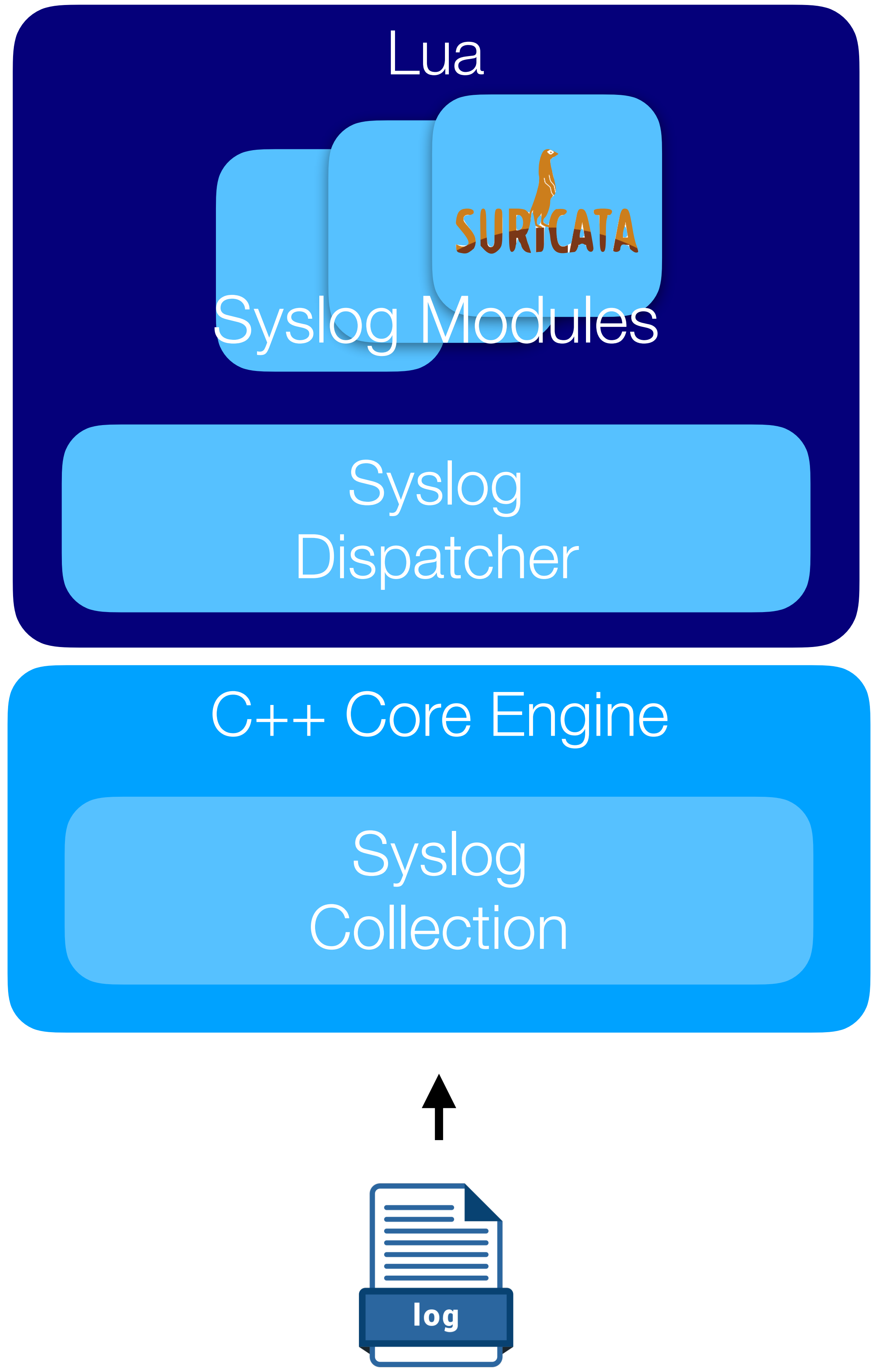


Suricata Eve

- The Suricata EVE output facility outputs events in JSON format.
- Events include:
    - Flow records (à la Netflow)
    - Alerts (signature matches)
    - Application layer metadata (HTTP, DNS, TLS, …)
    - Extracted files information

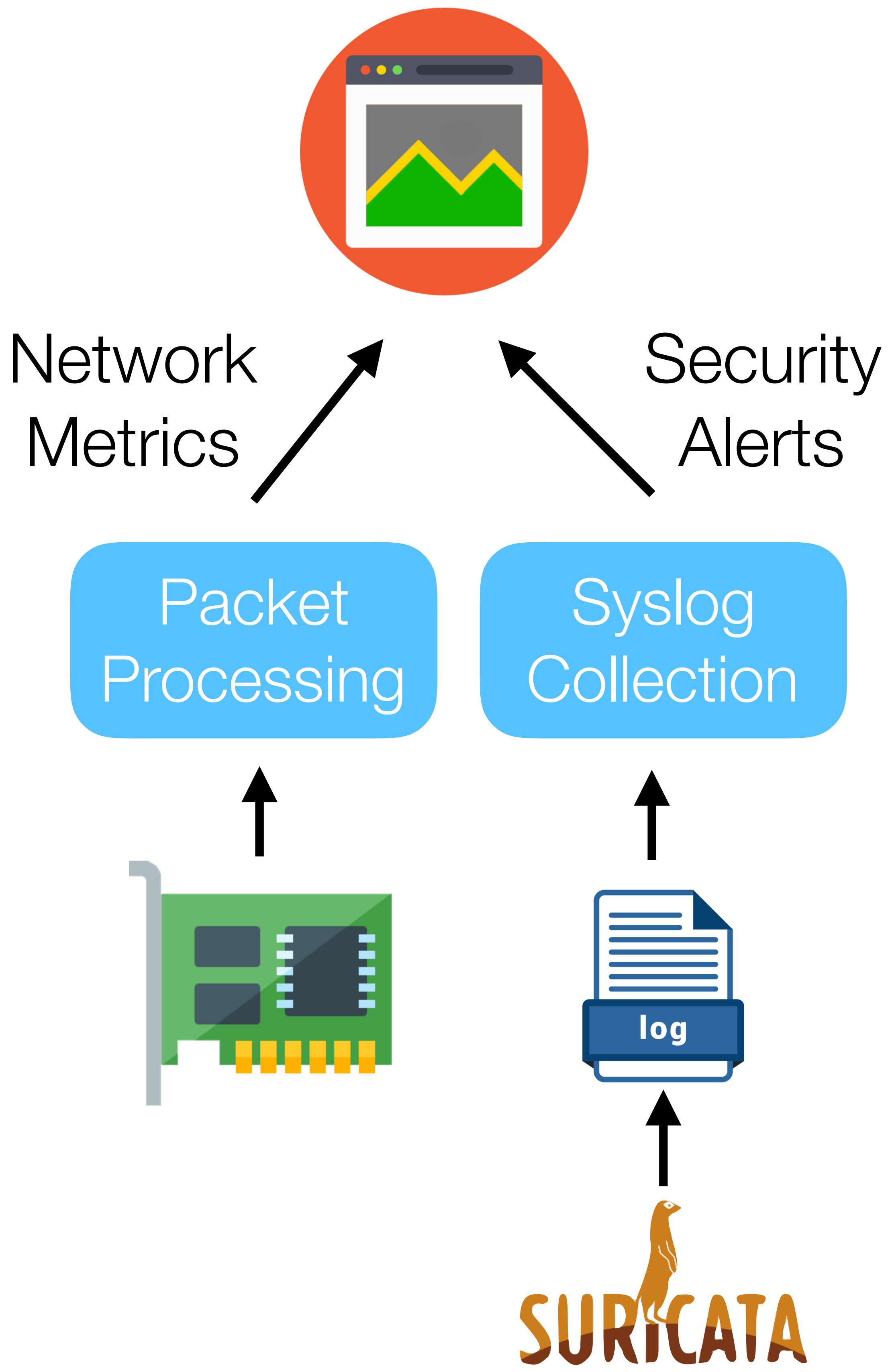
Syslog Collector Interface

- Ntopng implements Syslog-over-TCP ingestion to collect Syslog records from remote clients.
- Syslog records are processed by Lua modules based on the source application.



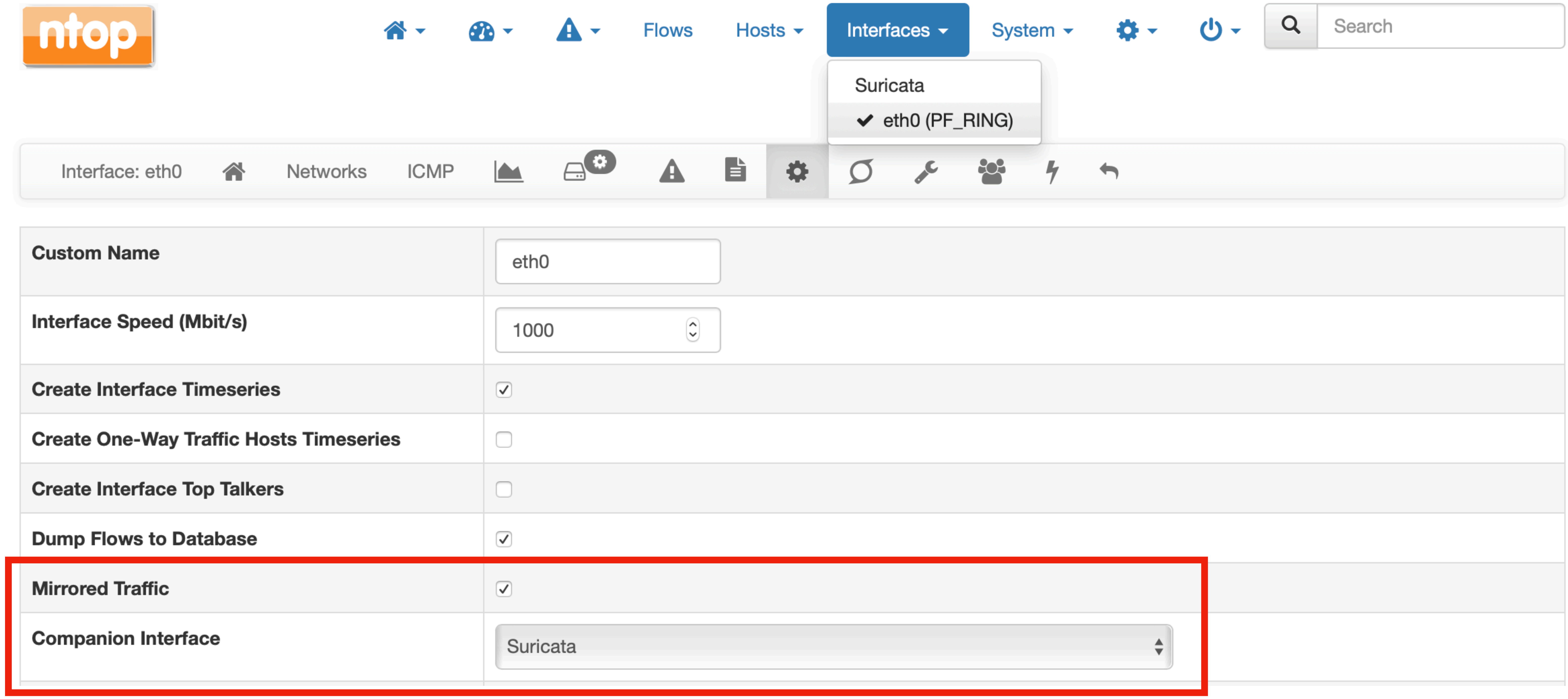
Alerts Ingestion

- Alerts generated by Suricata are collected through a Syslog interface.
- Binding the Syslog interface to a physical interface in ntopng we are able to:
  - Correlate events coming from Suricata with traffic processed by ntopng.
  - See network metrics and alerts (as well as other information coming from Suricata) in the same logical interface.



Configuration

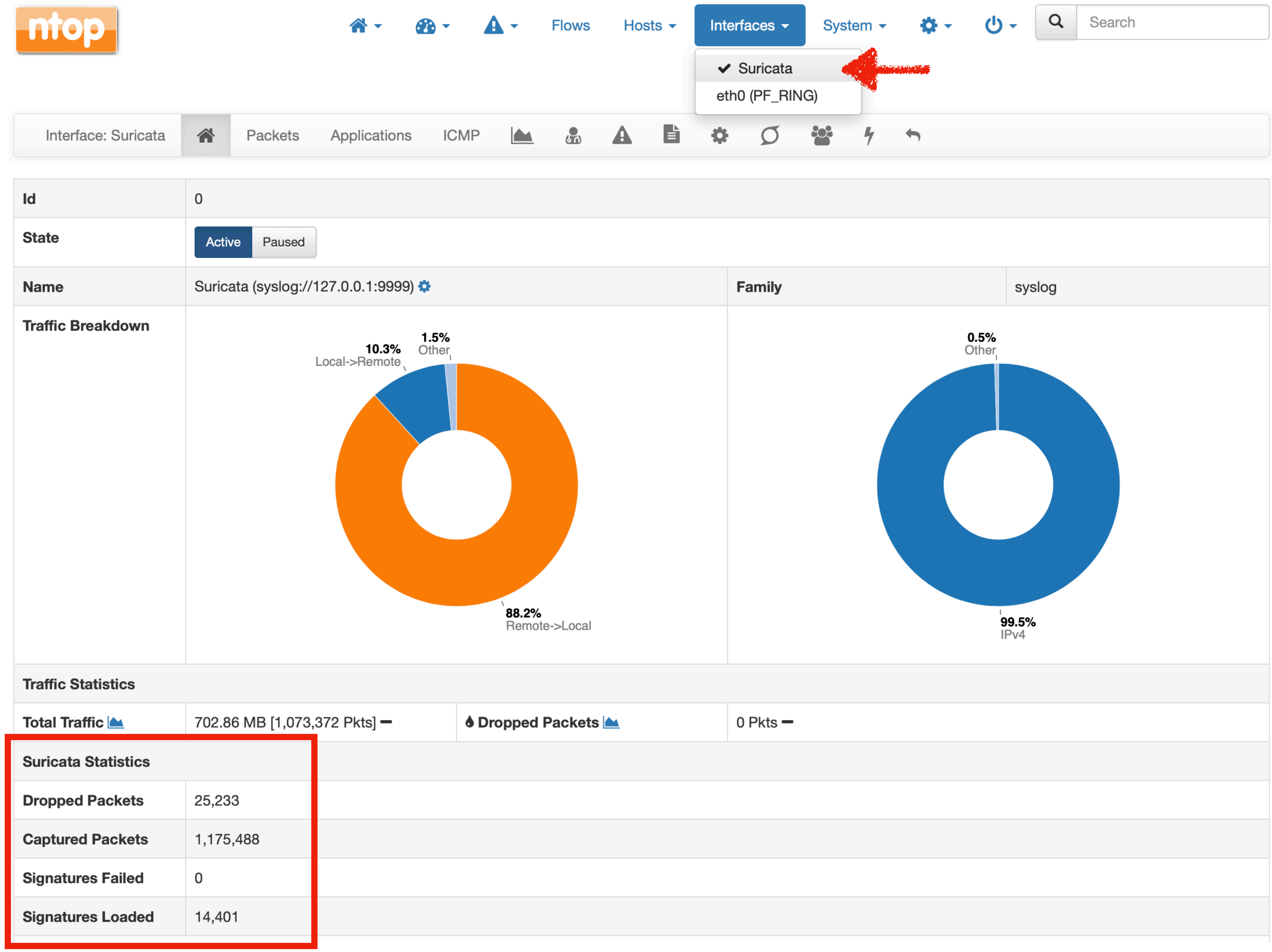
- `ntopng -i eth0 -i syslog://127.0.0.1:9999`



Custom Name	eth0
Interface Speed (Mbit/s)	1000
Create Interface Timeseries	☑
Create One-Way Traffic Hosts Timeseries	□
Create Interface Top Talkers	□
Dump Flows to Database	☑
Mirrored Traffic	☑
Companion Interface	Suricata

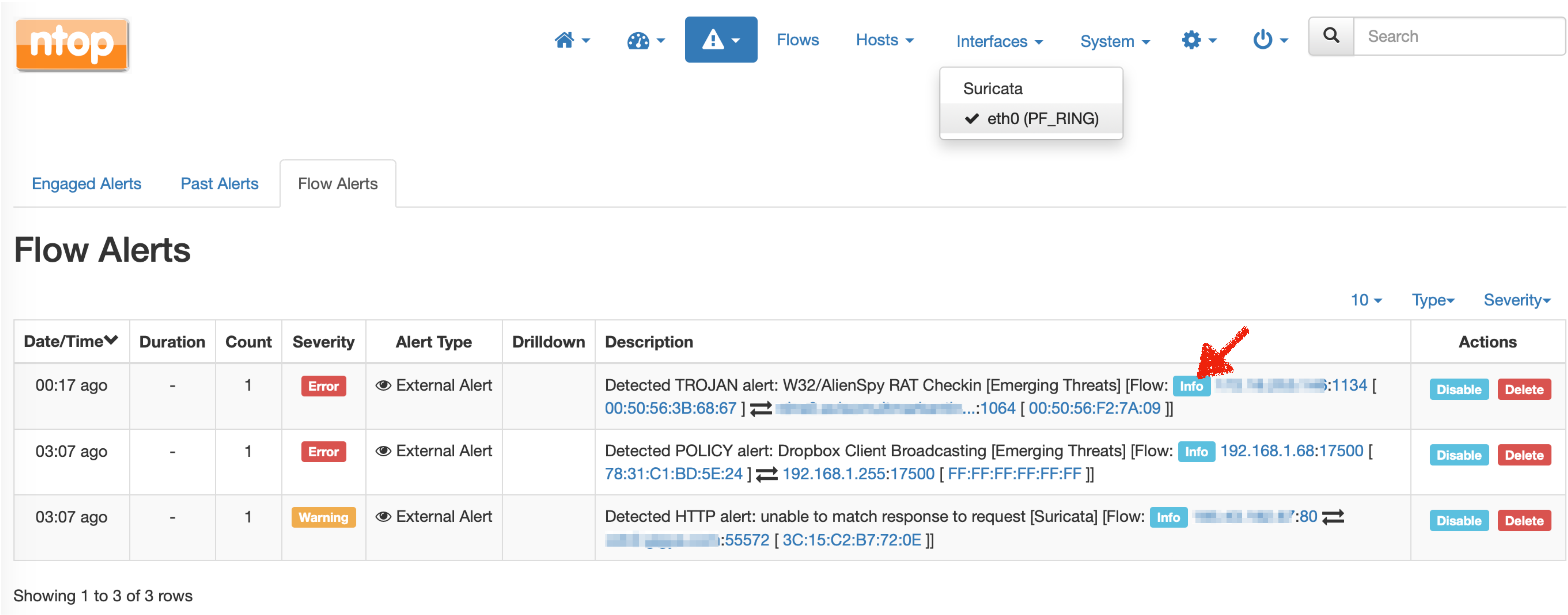
*User's Guide at https://www.ntop.org/guides/ntopng

Suricata (Syslog) Interface



Id	0		
State	Active Paused		
Name	Suricata (syslog://127.0.0.1:9999)	**Family**	syslog
Traffic Breakdown			
Traffic Statistics			
Total Traffic	702.86 MB [1,073,372 Pkts]	**Dropped Packets**	0 Pkts
Suricata Statistics			
Dropped Packets	25,233		
Captured Packets	1,175,488		
Signatures Failed	0		
Signatures Loaded	14,401		

Flow Alerts

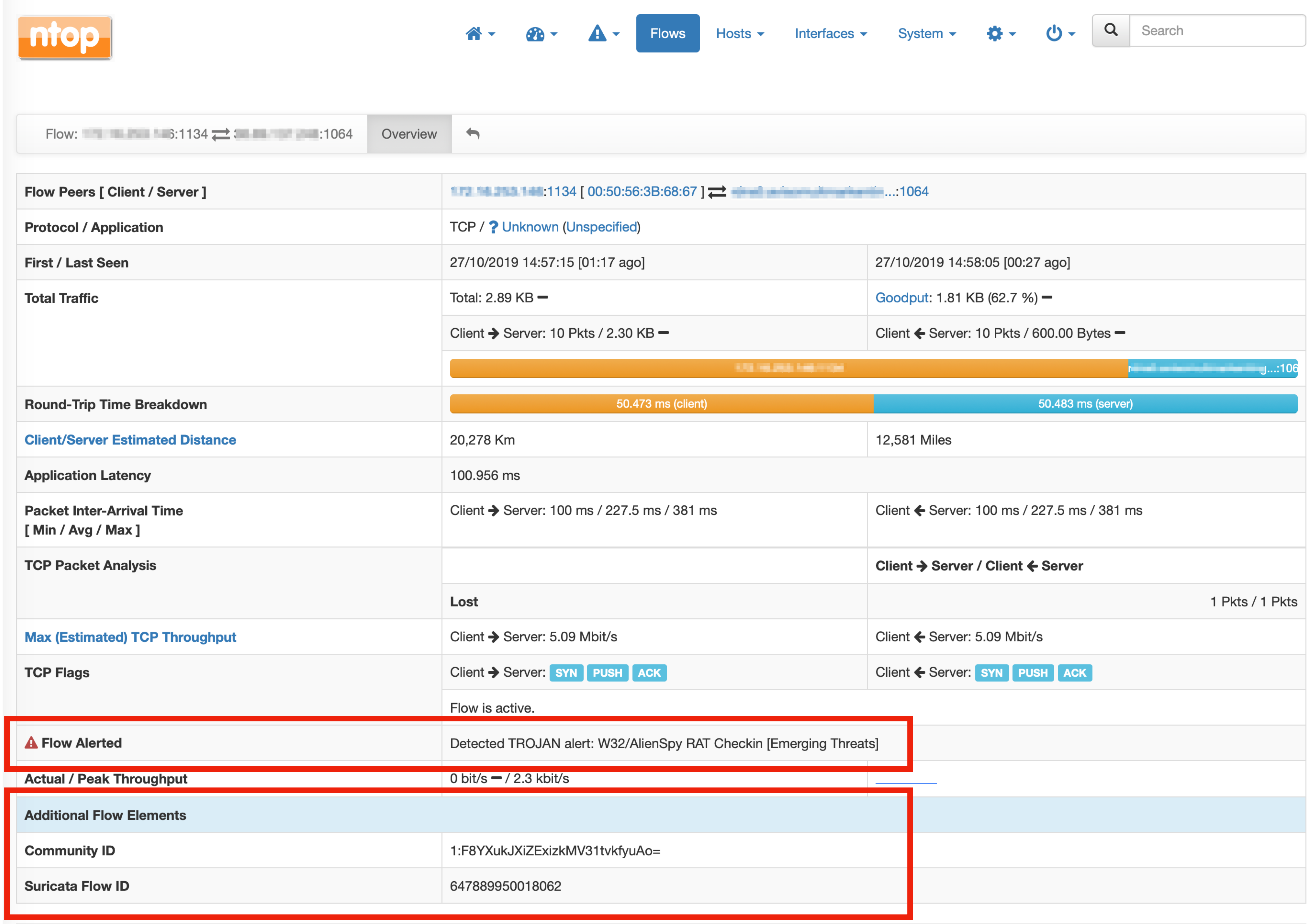


Flow Alerts

Date/Time	Duration	Count	Severity	Alert Type	Drilldown	Description	Actions
00:17 ago	-	1	Error	External Alert		Detected TROJAN alert: W32/AlienSpy RAT Checkin [Emerging Threats] [Flow: Info [redacted]:1134 [00:50:56:3B:68:67] ⇄ [redacted]...:1064 [00:50:56:F2:7A:09]]	Disable Delete
03:07 ago	-	1	Error	External Alert		Detected POLICY alert: Dropbox Client Broadcasting [Emerging Threats] [Flow: Info 192.168.1.68:17500 [78:31:C1:BD:5E:24] ⇄ 192.168.1.255:17500 [FF:FF:FF:FF:FF:FF]]	Disable Delete
03:07 ago	-	1	Warning	External Alert		Detected HTTP alert: unable to match response to request [Suricata] [Flow: Info [redacted]:80 ⇄ [redacted]:55572 [3C:15:C2:B7:72:0E]]	Disable Delete

Showing 1 to 3 of 3 rows

Flow Details



Flow: [redacted]:1134 ⇄ [redacted]:1064

Flow Peers [Client / Server]	[redacted]:1134 [00:50:56:3B:68:67] ⇄ [redacted]...:1064	
Protocol / Application	TCP / ? Unknown (Unspecified)	
First / Last Seen	27/10/2019 14:57:15 [01:17 ago]	27/10/2019 14:58:05 [00:27 ago]
Total Traffic	Total: 2.89 KB —	Goodput: 1.81 KB (62.7 %) —
	Client → Server: 10 Pkts / 2.30 KB —	Client ← Server: 10 Pkts / 600.00 Bytes —
	[redacted]	[redacted]...:106
Round-Trip Time Breakdown	50.473 ms (client)	50.483 ms (server)
Client/Server Estimated Distance	20,278 Km	12,581 Miles
Application Latency	100.956 ms	
Packet Inter-Arrival Time [Min / Avg / Max]	Client → Server: 100 ms / 227.5 ms / 381 ms	Client ← Server: 100 ms / 227.5 ms / 381 ms
TCP Packet Analysis		**Client → Server / Client ← Server**
	Lost	1 Pkts / 1 Pkts
Max (Estimated) TCP Throughput	Client → Server: 5.09 Mbit/s	Client ← Server: 5.09 Mbit/s
TCP Flags	Client → Server: SYN PUSH ACK	Client ← Server: SYN PUSH ACK
	Flow is active.	
⚠ Flow Alerted	Detected TROJAN alert: W32/AlienSpy RAT Checkin [Emerging Threats]	
Actual / Peak Throughput	0 bit/s — / 2.3 kbit/s	
Additional Flow Elements		
Community ID	1:F8YXukJXiZExizkMV31tvkfyuAo=	
Suricata Flow ID	647889950018062	

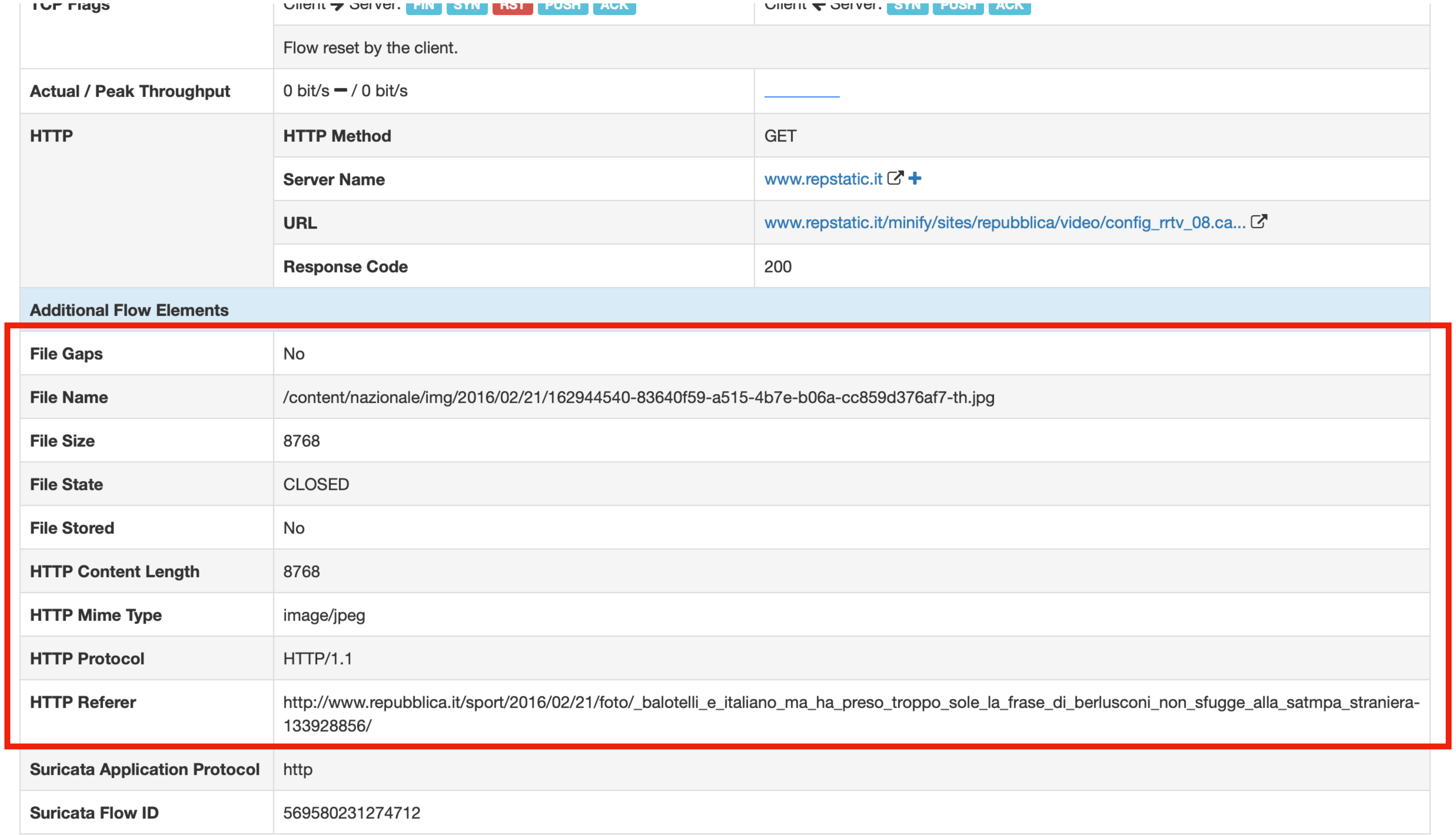
L7 Metadata Ingestion

- Application layer metadata for selected protocols (e.g. HTTP, DNS, TLS, …) are generated by Suricata and collected through the Syslog interface.

- The Suricata protocol parser and stream reassembly engine can also be used to extract and store files to disk (e.g. from HTTP, SMTP, FTP, …).

- All metadata are ingested by ntopng and are used to compute metrics and run analysis (those natively supported) or just listed as "Additional Information".

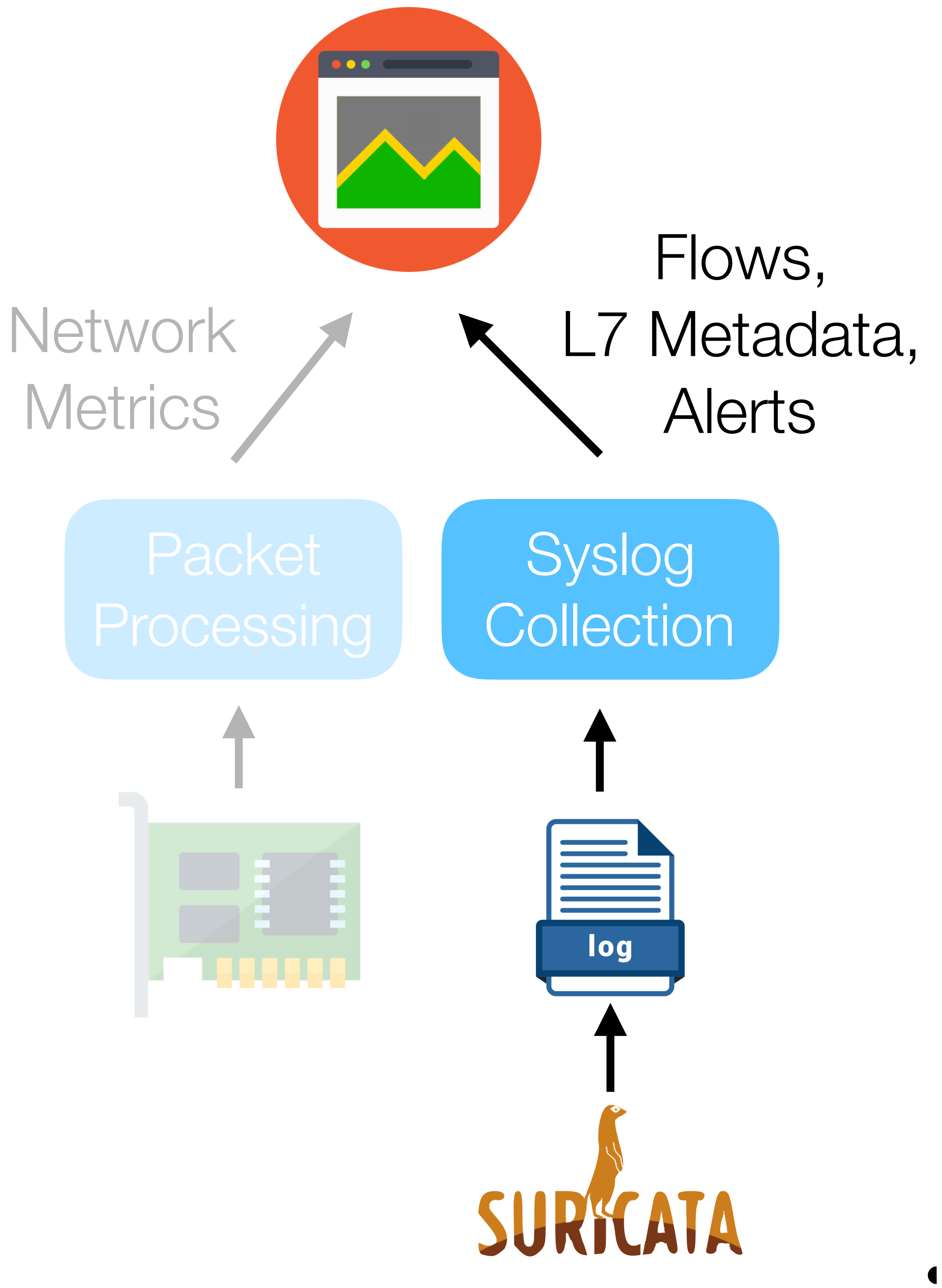
HTTP & File Info



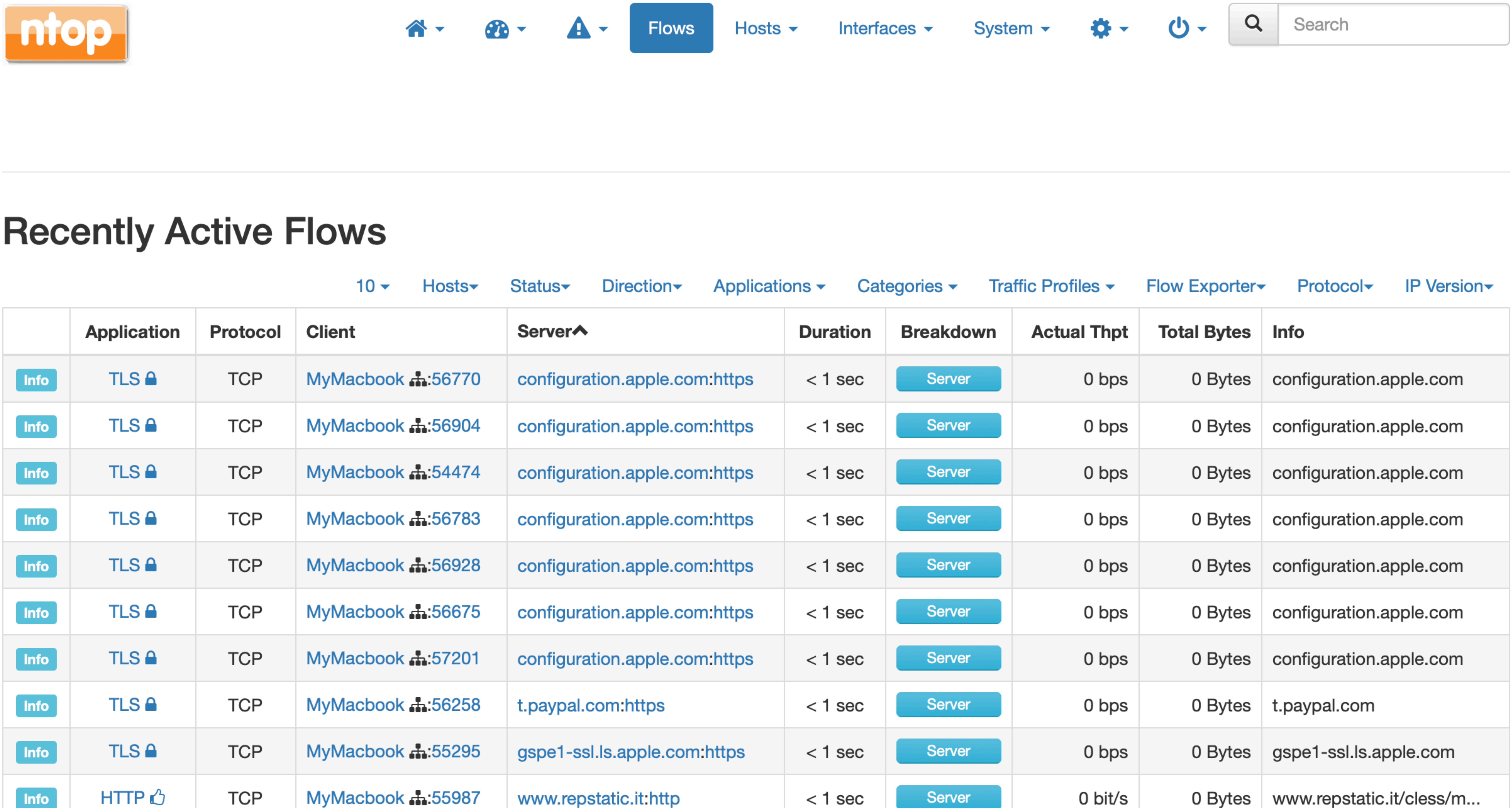
TCP Flags	Client → Server: FIN SYN RST PUSH ACK	Client ← Server: SYN PUSH ACK
	Flow reset by the client.	
Actual / Peak Throughput	0 bit/s — / 0 bit/s	
HTTP	HTTP Method	GET
	Server Name	www.repstatic.it
	URL	www.repstatic.it/minify/sites/repubblica/video/config_rrtv_08.ca...
	Response Code	200
Additional Flow Elements		
File Gaps	No	
File Name	/content/nazionale/img/2016/02/21/162944540-83640f59-a515-4b7e-b06a-cc859d376af7-th.jpg	
File Size	8768	
File State	CLOSED	
File Stored	No	
HTTP Content Length	8768	
HTTP Mime Type	image/jpeg	
HTTP Protocol	HTTP/1.1	
HTTP Referer	http://www.repubblica.it/sport/2016/02/21/foto/_balotelli_e_italiano_ma_ha_preso_troppo_sole_la_frase_di_berlusconi_non_sfugge_alla_satmpa_straniera-133928856/	
Suricata Application Protocol	http	
Suricata Flow ID	569580231274712	

Flow Records Ingestion

- Suricata as a NetFlow-like flow exporter.
- Flow information generated by Suricata are collected through a Syslog interface, together with alerts.
- In this working mode, ntopng collects flows instead of processing packet.
- Drawback: ntopng cannot compute most of the Network metrics as it does not have packets visibility.



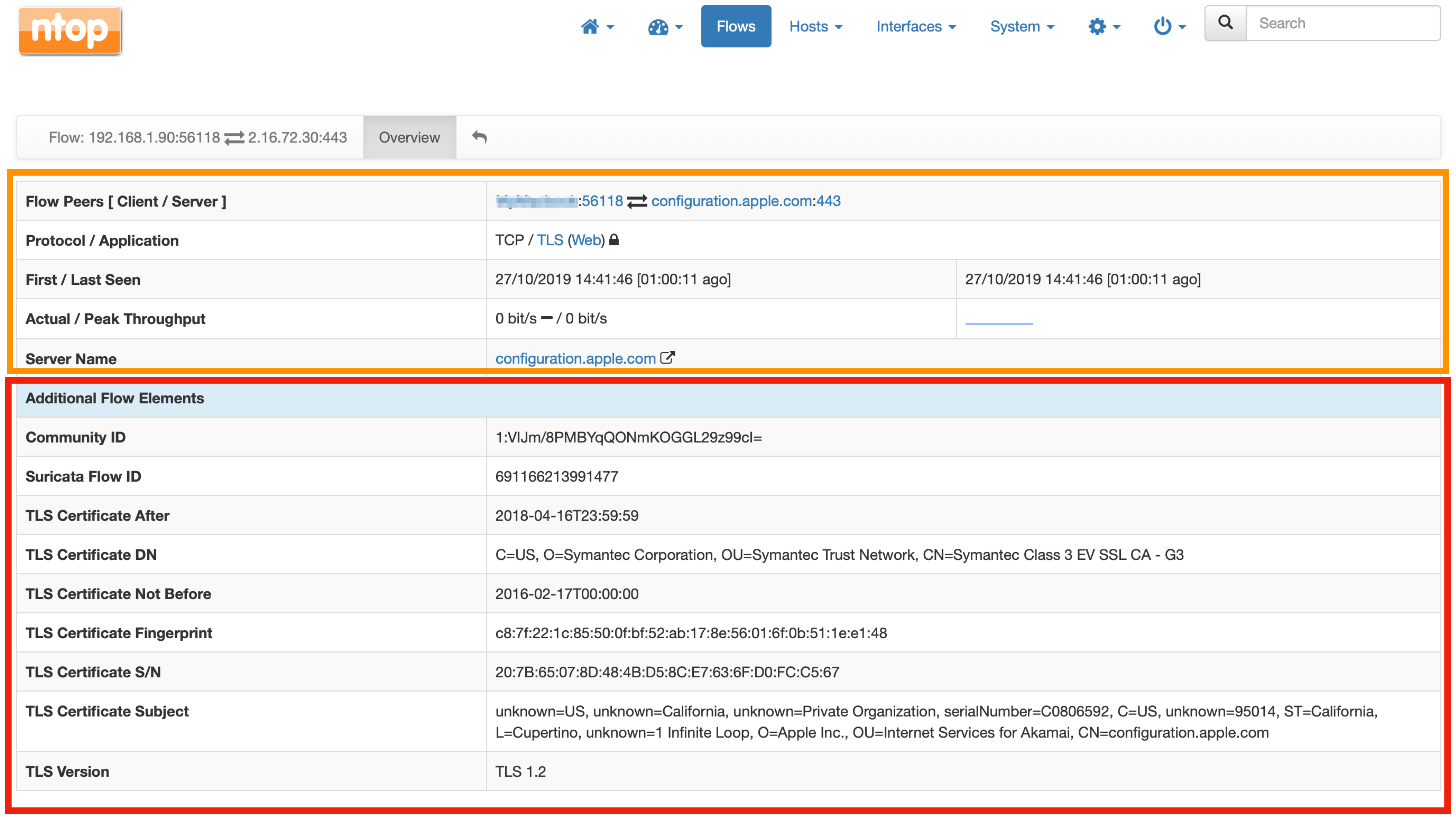
Flows List



Recently Active Flows

	Application	Protocol	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	TLS	TCP	MyMacbook :56770	configuration.apple.com:https	< 1 sec	Server	0 bps	0 Bytes	configuration.apple.com
Info	TLS	TCP	MyMacbook :56904	configuration.apple.com:https	< 1 sec	Server	0 bps	0 Bytes	configuration.apple.com
Info	TLS	TCP	MyMacbook :54474	configuration.apple.com:https	< 1 sec	Server	0 bps	0 Bytes	configuration.apple.com
Info	TLS	TCP	MyMacbook :56783	configuration.apple.com:https	< 1 sec	Server	0 bps	0 Bytes	configuration.apple.com
Info	TLS	TCP	MyMacbook :56928	configuration.apple.com:https	< 1 sec	Server	0 bps	0 Bytes	configuration.apple.com
Info	TLS	TCP	MyMacbook :56675	configuration.apple.com:https	< 1 sec	Server	0 bps	0 Bytes	configuration.apple.com
Info	TLS	TCP	MyMacbook :57201	configuration.apple.com:https	< 1 sec	Server	0 bps	0 Bytes	configuration.apple.com
Info	TLS	TCP	MyMacbook :56258	t.paypal.com:https	< 1 sec	Server	0 bps	0 Bytes	t.paypal.com
Info	TLS	TCP	MyMacbook :55295	gspe1-ssl.ls.apple.com:https	< 1 sec	Server	0 bps	0 Bytes	gspe1-ssl.ls.apple.com
Info	HTTP	TCP	MyMacbook :55987	www.repstatic.it:http	< 1 sec	Server	0 bit/s	0 Bytes	www.repstatic.it/cless/m...

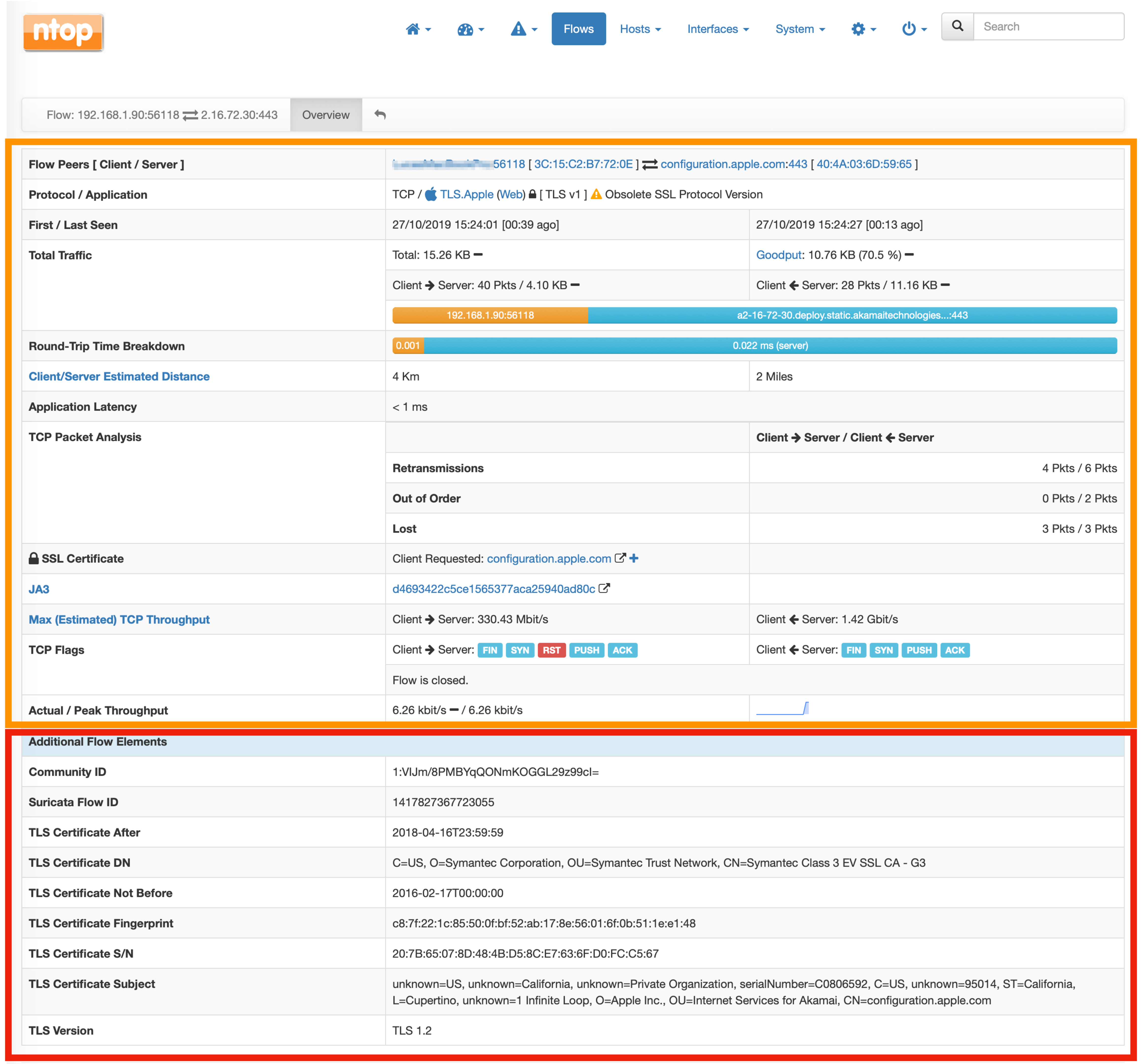
Flow Details w/o Packets



Flow: 192.168.1.90:56118 ⇄ 2.16.72.30:443

Flow Peers [Client / Server]	[redacted]:56118 ⇄ configuration.apple.com:443	
Protocol / Application	TCP / TLS (Web) 🔒	
First / Last Seen	27/10/2019 14:41:46 [01:00:11 ago]	27/10/2019 14:41:46 [01:00:11 ago]
Actual / Peak Throughput	0 bit/s ━ / 0 bit/s	
Server Name	configuration.apple.com	
Additional Flow Elements		
Community ID	1:VlJm/8PMBYqQONmKOGGL29z99cI=	
Suricata Flow ID	691166213991477	
TLS Certificate After	2018-04-16T23:59:59	
TLS Certificate DN	C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL CA - G3	
TLS Certificate Not Before	2016-02-17T00:00:00	
TLS Certificate Fingerprint	c8:7f:22:1c:85:50:0f:bf:52:ab:17:8e:56:01:6f:0b:51:1e:e1:48	
TLS Certificate S/N	20:7B:65:07:8D:48:4B:D5:8C:E7:63:6F:D0:FC:C5:67	
TLS Certificate Subject	unknown=US, unknown=California, unknown=Private Organization, serialNumber=C0806592, C=US, unknown=95014, ST=California, L=Cupertino, unknown=1 Infinite Loop, O=Apple Inc., OU=Internet Services for Akamai, CN=configuration.apple.com	
TLS Version	TLS 1.2	

Flow Details w/ Packets

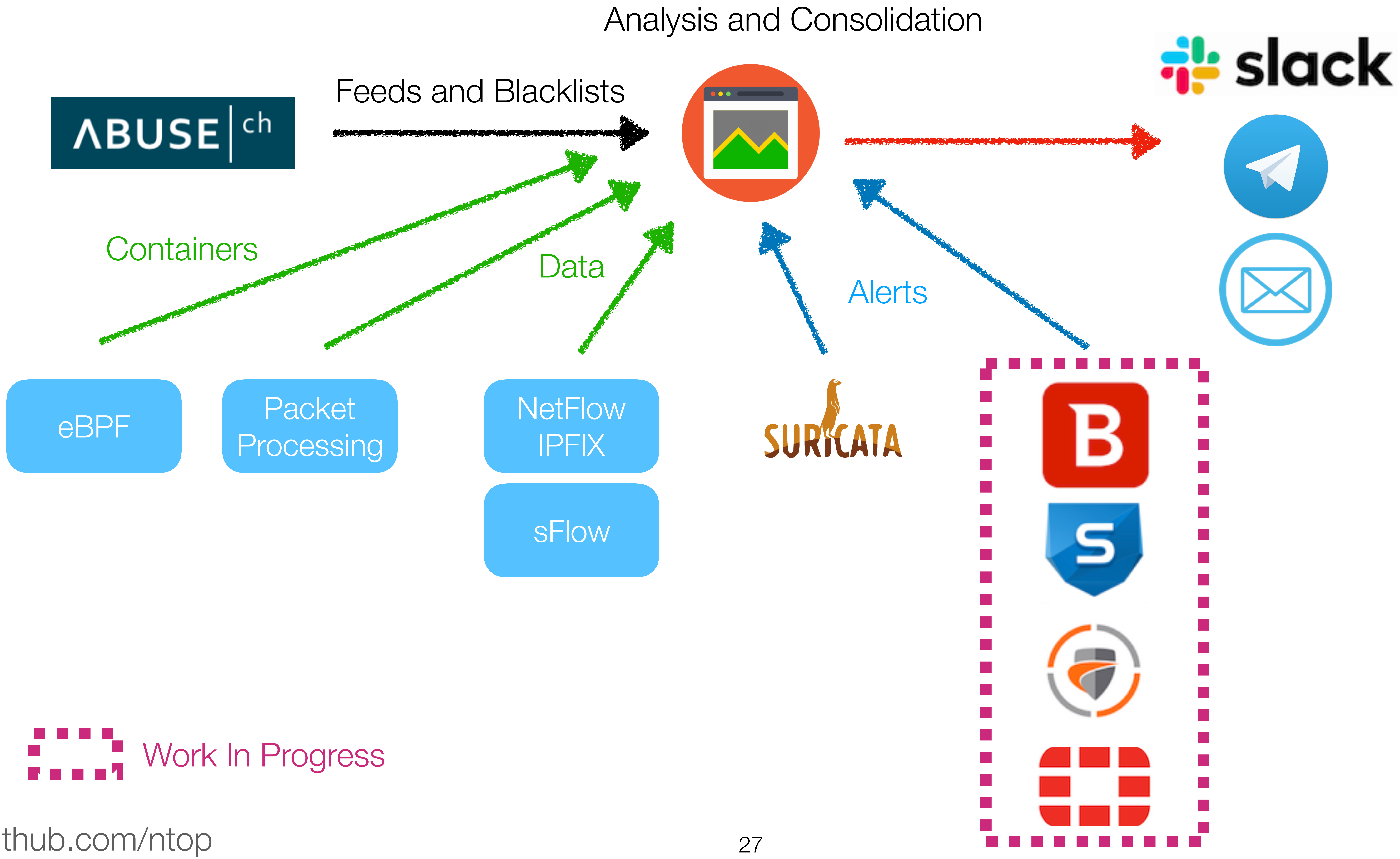


Flow: 192.168.1.90:56118 ⇄ 2.16.72.30:443

Flow Peers [Client / Server]	[redacted]56118 [3C:15:C2:B7:72:0E] ⇄ configuration.apple.com:443 [40:4A:03:6D:59:65]	
Protocol / Application	TCP / TLS.Apple (Web) 🔒 [TLS v1] ⚠ Obsolete SSL Protocol Version	
First / Last Seen	27/10/2019 15:24:01 [00:39 ago]	27/10/2019 15:24:27 [00:13 ago]
Total Traffic	Total: 15.26 KB −	Goodput: 10.76 KB (70.5 %) −
	Client → Server: 40 Pkts / 4.10 KB −	Client ← Server: 28 Pkts / 11.16 KB −
	192.168.1.90:56118 a2-16-72-30.deploy.static.akamaitechnologies...:443	
Round-Trip Time Breakdown	0.001 0.022 ms (server)	
Client/Server Estimated Distance	4 Km	2 Miles
Application Latency	< 1 ms	
TCP Packet Analysis		**Client → Server / Client ← Server**
	Retransmissions	4 Pkts / 6 Pkts
	Out of Order	0 Pkts / 2 Pkts
	Lost	3 Pkts / 3 Pkts
🔒 **SSL Certificate**	Client Requested: configuration.apple.com +	
JA3	d4693422c5ce1565377aca25940ad80c	
Max (Estimated) TCP Throughput	Client → Server: 330.43 Mbit/s	Client ← Server: 1.42 Gbit/s
TCP Flags	Client → Server: FIN SYN RST PUSH ACK	Client ← Server: FIN SYN PUSH ACK
	Flow is closed.	
Actual / Peak Throughput	6.26 kbit/s − / 6.26 kbit/s	

Additional Flow Elements	
Community ID	1:VlJm/8PMBYqQONmKOGGL29z99cI=
Suricata Flow ID	1417827367723055
TLS Certificate After	2018-04-16T23:59:59
TLS Certificate DN	C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL CA - G3
TLS Certificate Not Before	2016-02-17T00:00:00
TLS Certificate Fingerprint	c8:7f:22:1c:85:50:0f:bf:52:ab:17:8e:56:01:6f:0b:51:1e:e1:48
TLS Certificate S/N	20:7B:65:07:8D:48:4B:D5:8C:E7:63:6F:D0:FC:C5:67
TLS Certificate Subject	unknown=US, unknown=California, unknown=Private Organization, serialNumber=C0806592, C=US, unknown=95014, ST=California, L=Cupertino, unknown=1 Infinite Loop, O=Apple Inc., OU=Internet Services for Akamai, CN=configuration.apple.com
TLS Version	TLS 1.2

Ongoing Activities



Analysis and Consolidation

Feeds and Blacklists

Containers

Data

Alerts

eBPF

Packet Processing

NetFlow IPFIX

sFlow

Work In Progress

Final Remarks

- Network security and visibility is now possible.
- Comprehensive merge of Suricata alerting information with ntopng traffic analysis.
- Benefits for the whole open source community, as well the ntopng and Suricata communities.
- Hopefully closer integration using nDPI into Suricata for characterising traffic unknown to Suricata.