High-speed Traffic Analysis Using ntopng: The New Features

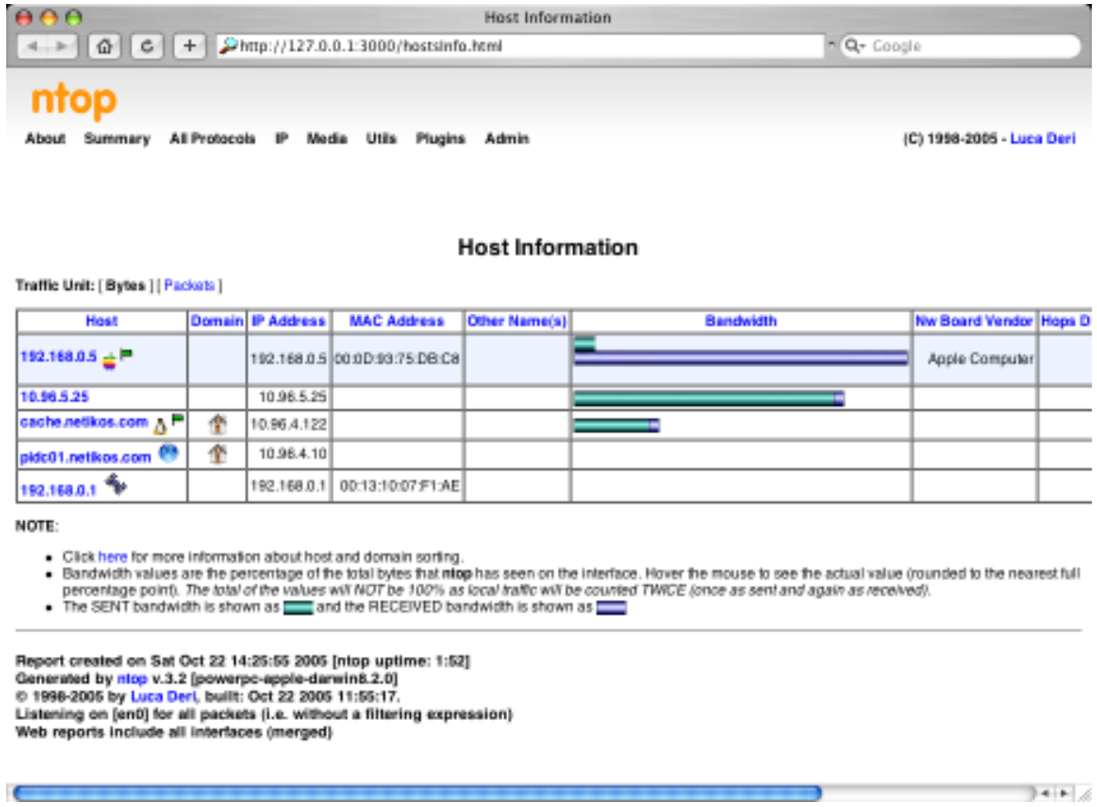
High Speed Traffic Analysen mit ntopng: Die neuen Features

Luca Deri <deri@ntop.org>

© 2015 - ntop.org

Some History

- In 1998, the original ntop has been created.
- It was a C-based app embedding a web server able to capture traffic and analyse it.



- Contrary to many tools available at that time, ntop used a web GUI to report traffic activities.
- It is available for Unix and Windows under GPL.

© 2015 - ntop.org

Towards ntopng 2.0

- Version 1.0: 2013
  - Fresh code, some missing features, initial release.
- Version 1.2: 09/2014
  - Latest stable release, fixed many bugs, some new features.
- Version 2.0: Spring 2015

  - Added support for enterprise customers.
  - Two flavours: Embedded and Standard.
  - Two versions: Community and Professional.

© 2015 - ntop.org

Version 2.0: Main Goals

- One application for network traffic monitoring and control (policy enforcement)
- Ability to scale to hundred thousand hosts (mid/large ISPs)
- Identify network security issues and produce alerts.
- Natively integrated with other enterprise tools (e.g. Nagios) and protocols (e.g. NetFlow/IPFIX/sFlow)

© 2015 - ntop.org

Details Matter [1/2]

ntop

Home | Flows | Hosts | Interfaces | Search Host

Active Flows

10 | Applications

	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	DNS	UDP	192.168.1.92 :62927	192.168.1.1:53	1 sec	Client Server	0 bps	230 Bytes	www.maxmind.com
Info	DNS	UDP	192.168.1.92 :49440	192.168.1.1:53	1 sec	Client Server	0 bps	156 Bytes	github.com
Info	DNS	UDP	192.168.1.92 :63909	192.168.1.1:53	1 sec	Client Server	0 bps	183 Bytes	www.gnu.org
Info	DNS	UDP	192.168.1.92 :64600	192.168.1.1:53	1 sec	Client Server	0 bps	251 Bytes	83.83.175.5.in-addr.arpa...
Info	DNS	UDP	192.168.1.92 :49690	192.168.1.1:53	1 sec	Client Server	0 bps	380 Bytes	fbexternal-a.akamaihd.ne...
Info	DNS	UDP	192.168.1.92 :63467	192.168.1.1:53	1 sec	Client Server	0 bps	186 Bytes	eu-gmtdmp.gd1.mookie1.co...
Info	DNS	UDP	192.168.1.92 :49725	192.168.1.1:53	1 sec	Client Server	0 bps	208 Bytes	a1294.w20.akamai.net
Info	DNS	UDP	192.168.1.92 :63706	192.168.1.1:53	1 sec	Client Server	0 bps	214 Bytes	232.113.194.173.in-addr....
Info	DNS	UDP	192.168.1.92 :64473	192.168.1.1:53	1 sec	Client Server	0 bps	176 Bytes	it.gmads.mookie1.com
Info	Google	TCP	192.168.1.92 :57279	mil01s18-in-f15.1e10... :80	1 sec	Server	0 bps	15.29 KB	

Showing 1 to 10 of 131 rows

« < 1 2 3 4 5 > »

© 2015 - ntop.org

Details Matter [2/2]

ntop

Home | Flows | Hosts | Interfaces | Search Host

Flow: lucas-imac.homenet.telecomitalia.it:64578 ⇄ 93.184.221.133:80 | Overview

Flow Peers	lucas-imac.homenet.telecomitalia.it :64578 ⇄ 93.184.221.133:80	
Protocol	TCP / HTTP	
First / Last Seen	15/03/2015 18:58:19 [19 sec ago]	15/03/2015 18:58:35 [3 sec ago]
Total Traffic Volume	313.43 KB	
Client vs Server Traffic Breakdown	lucas 93.184.221.133:80	
Network Latency Breakdown	24.091 ms (server)	
Client to Server Traffic	155 Pkts / 8.62 KB	
Server to Client Traffic	214 Pkts / 304.82 KB	
TCP Flags	SYN PUSH ACK This flow is active.	
Actual / Peak Throughput	182.24 bps – / 240.89 Kbit/s	
HTTP		
HTTP Method	GET	
Server Name	download.cdn.mozilla.net	
URL	/pub/firefox/releases/36.0.1/update/mac/en-US/firefox-35.0.1-36.0.1.partial.mar	
Response Code	206	

© 2015 - ntop.org

nDPI [1/4]

- ntop develops and maintains nDPI: a GPL DPI toolkit.
- Supported protocols (> 180) include:
  - P2P (Skype, BitTorrent)
  - Messaging (Viber, Whatsapp, MSN, The Facebook)
  - Multimedia (YouTube, Last.gm, iTunes)
  - Conferencing (Webex, CitrixOnLine)
  - Streaming (Zattoo, Icecast, Shoutcast, Netflix)
  - Business (VNC, RDP, Citrix, *SQL)
  - VPN (Tor, IPSEC, PPTP)

© 2015 - ntop.org

nDPI [2/4]

- nDPI identifies the application protocol regardless of the port being used (e.g. it can detect HTTP on ports other than 80).
- nDPI supports encrypted content for identifying HTTPS-based communications.
- ntopng is based on the nDPI layer for protocol recognition and enforcement.

© 2015 - ntop.org

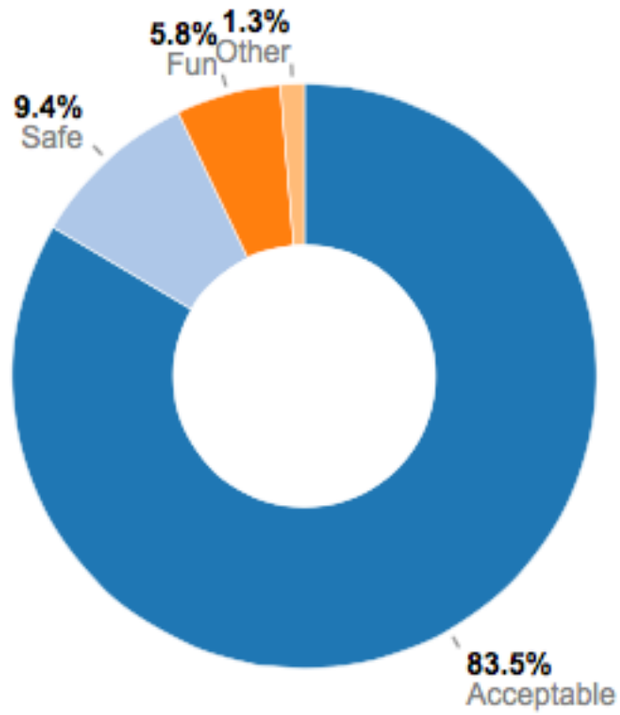
nDPI [3/4]

Layer 4 Protocol

Good or Bad?

Protocol	TCP / HTTP

Layer 7 Protocol



© 2015 - ntop.org

nDPI [4/4]

- Using nDPI you can identify all hosts in your network who do something specific such as listening to music or going to Facebook.

All DropBox Hosts

10 ▾ Filter Hosts▾

IP Address	Location	Alerts	Name	Seen Since	ASN	Breakdown	Throughput	Traffic
192.168.1.92	Local	3	lucas-imac.homenet.telecomitalia...	1 h, 24 min, 25 sec		Rcvd	106.89 Kbit/s	92.63 MB
192.168.1.1	Local	0	alicegate.homenet.telecomitalia...	1 h, 24 min, 22 sec		Sent Rcvd	3.67 Kbit/s	425.7 KB
192.168.1.255	Local	0	192.168.1.255	1 h, 24 min, 12 sec		Rcvd	1.08 Kbit/s	140.81 KB
255.255.255.255	Local	0	Broadcast	1 h, 24 min, 12 sec		Rcvd	0 bps	248.61 KB
108.160.165.54	Remote	0	sjd-ra1-1b.sjc.dropbox.co...	13 min, 30 sec	Dropbox, Inc.	Sent Rcvd	0 bps	32.23 KB

Showing 1 to 5 of 5 rows

© 2015 - ntop.org

Network Health Unveiled [1/3]

Flows to Pay Attention

Active Flows

10 ▾ Applications ▾

	Application	L4 Proto	Client	Server	Duration ▾	Breakdown	Actual Thpt	Total Bytes	Info
Info	Spotify	UDP	lucas-imac.homenet.t... :57621	192.168.1.255:57621	1 h, 10 min, 38 sec	Client	0 bps –	12.01 KB	
Info	DropBox	UDP	lucas-imac.homenet.t... :17500	broadcasthost:17500	1 h, 11 min, 8 sec	Client	0 bps ↓	96.36 KB	
Info	DropBox	UDP	lucas-imac.homenet.t... :17500	192.168.1.255:17500	1 h, 11 min, 8 sec	Client	0 bps ↓	96.36 KB	
Info	Unknown	TCP	lucas-imac.homenet.t... :54679	pc-deri.nic.it :2222	1 h, 10 min, 52 sec	Client Server	0 bps –	126.98 KB	
Info	DropBox	TCP	lucas-imac.homenet.t... :56571	ash-ra1-3a.sjc.dropb... :80	1 h, 9 min, 57 sec	Client Server	0 bps –	170.26 KB	
Info	Unknown	TCP	pc-deri.nic.it :2222	lucas-imac.homenet.t... :54475	1 h, 10 min, 40 sec	Client Server	0 bps –	34.44 KB	
Info	SSH	TCP	lucas-imac.homenet.t... :61281	pc-deri.nic.it :2222	38 min, 28 sec	Client Server	0 bps –	2.26 MB	
Info	SSH	TCP	lucas-imac.homenet.t... :63061	net-93-64-151-231.cu... :2220	22 min, 13 sec	Client Server	21.67 Kbit/s ↓	1.58 MB	
Info	Spotify	TCP	lucas-imac.homenet.t... :50467	lon3-accesspoint-a10... :4070	2 min, 1 sec	Client Server	0 bps –	643.01 KB	
Info	Unknown	TCP	lucas-imac.homenet.t... :49254	webmail3.iit.cnr.it :993	49 sec	Client	1.54 Kbit/s ↑	10.77 KB	

Showing 1 to 10 of 28 rows

« < 1 2 3 > »

© 2015 - ntop.org

Network Health Unveiled [2/3]

(Router) MAC Address	D0:D4:12:C6:73:F5	
IP Address	194.132.198.242	☑ ⚠ Trigger Host Alerts
ASN	Spotify Technology SARL [ASN 43650]	Whois Lookup
Name	lon3-accesspoint-a10.lon3.spotify.com Remote	194.132.198.242 Save Name
First / Last Seen	15/03/2015 19:10:02 [1 min, 39 sec ago]	15/03/2015 19:11:15 [26 sec ago]
Sent vs Received Traffic Breakdown	Sent	Rcvd
Traffic Sent / Received	433 Pkts / 537.55 KB	428 Pkts / 105.31 KB
Flows Active / Total	**'As Client'**	**'As Server'**
	0 / 0	1 / 1
TCP Packets Sent Analysis	**Retransmissions**	0 Pkts
	Out of Order	40 Pkts
	Lost	20 Pkts

© 2015 - ntop.org

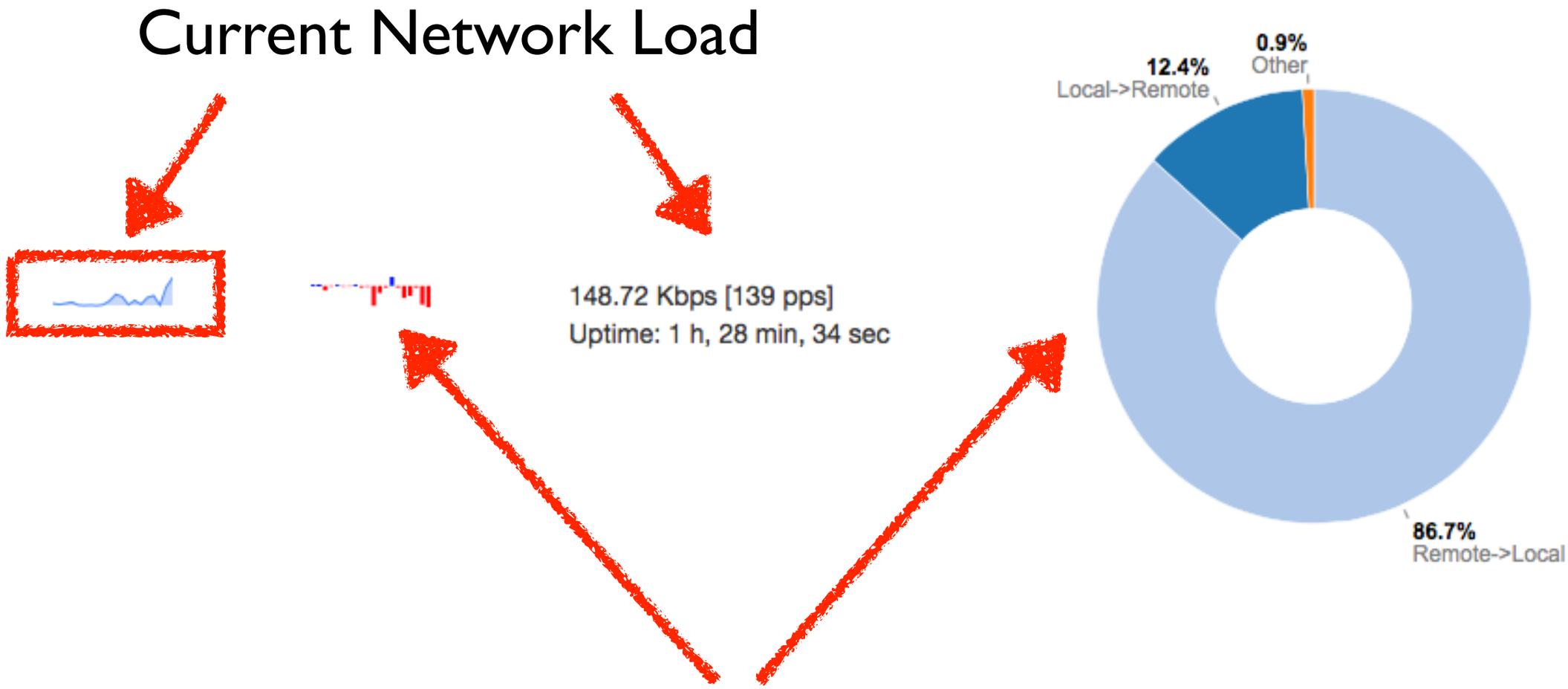
Network Health Unveiled [3/3]

Flow Peers	192.168.30.205:4185 ⇄ 195.22.198.30:80	
Protocol	TCP / Google	
First / Last Seen	09/02/2007 11:54:32 [8 years, 37 days, 10 h, 40 sec ago]	09/02/2007 11:55:52 [8 years, 37 days, 9 h, 59 min, 20 sec ago]
Total Traffic Volume	42.79 KB	
Client vs Server Traffic Breakdown	192.16 — 195.22.198.30:80	
Network Latency Breakdown	1.14 — 27.290 ms (server)	
Client to Server Traffic	20 Pkts / 1.93 KB	
Server to Client Traffic	32 Pkts / 40.85 KB	
TCP Flags	SYN RST PUSH ACK This flow has been reset and probably the server application is down.	
Actual / Peak Throughput	0 bps / 0 bps	
Server Name	m1.2mdn.net	

Do you finally know where is the higher latency: client or server ?

© 2015 - ntop.org

Download or Upload ?



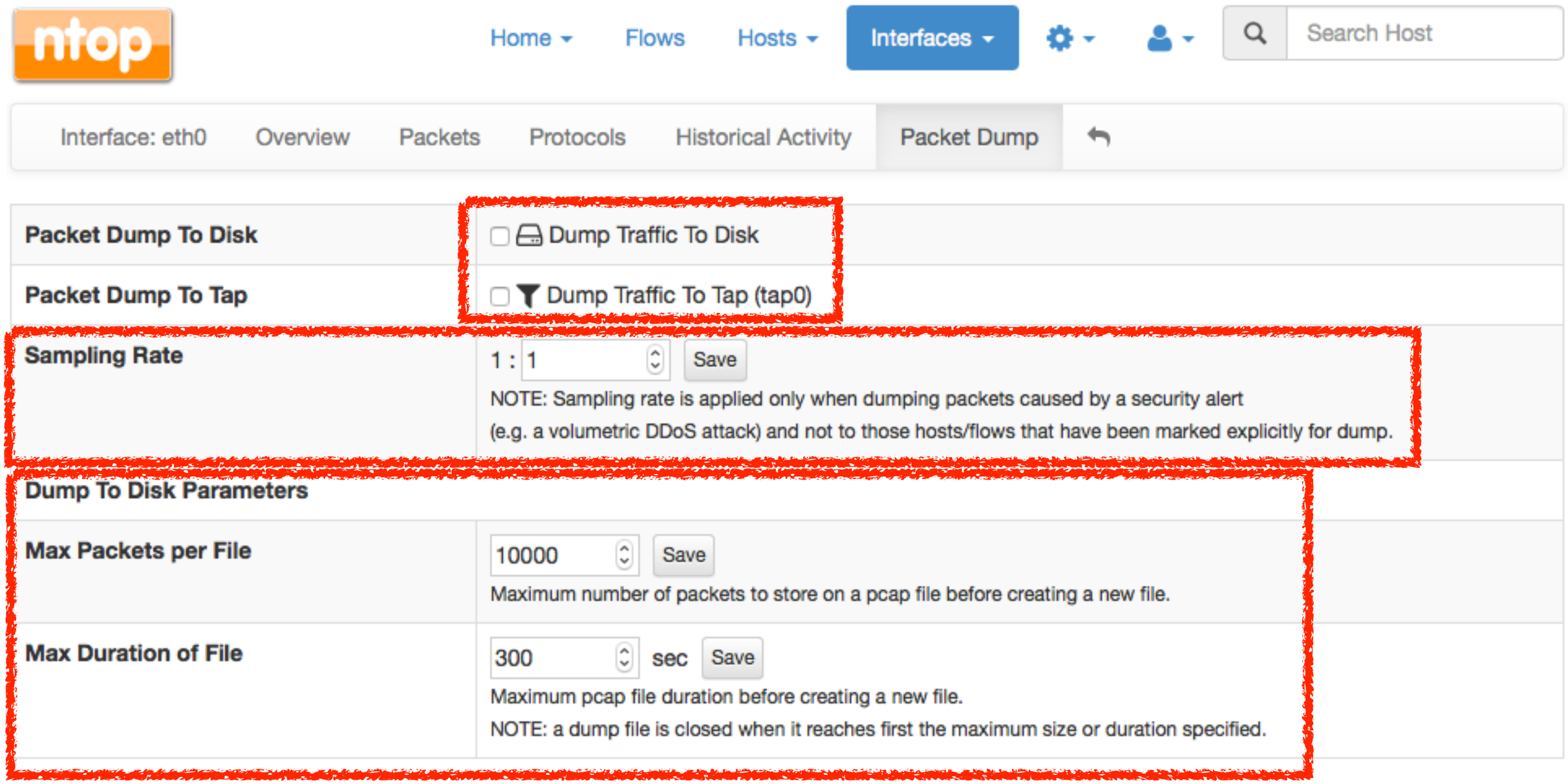
Download or Upload ?

Packets Never Lie [1/3]

- Suppose that for specific hosts (e.g. for which an IDS has reported security issues) you want to save raw packets.
- Suppose that your host is under attack or is attacking somebody (e.g. portscan).
- Suppose that you want to save packets of unknown (i.e. not detected by nDPI) communications for inspection (or for improving nDPI).
- …then you need raw packets (pcap).

© 2015 - ntop.org

Packets Never Lie [2/3]



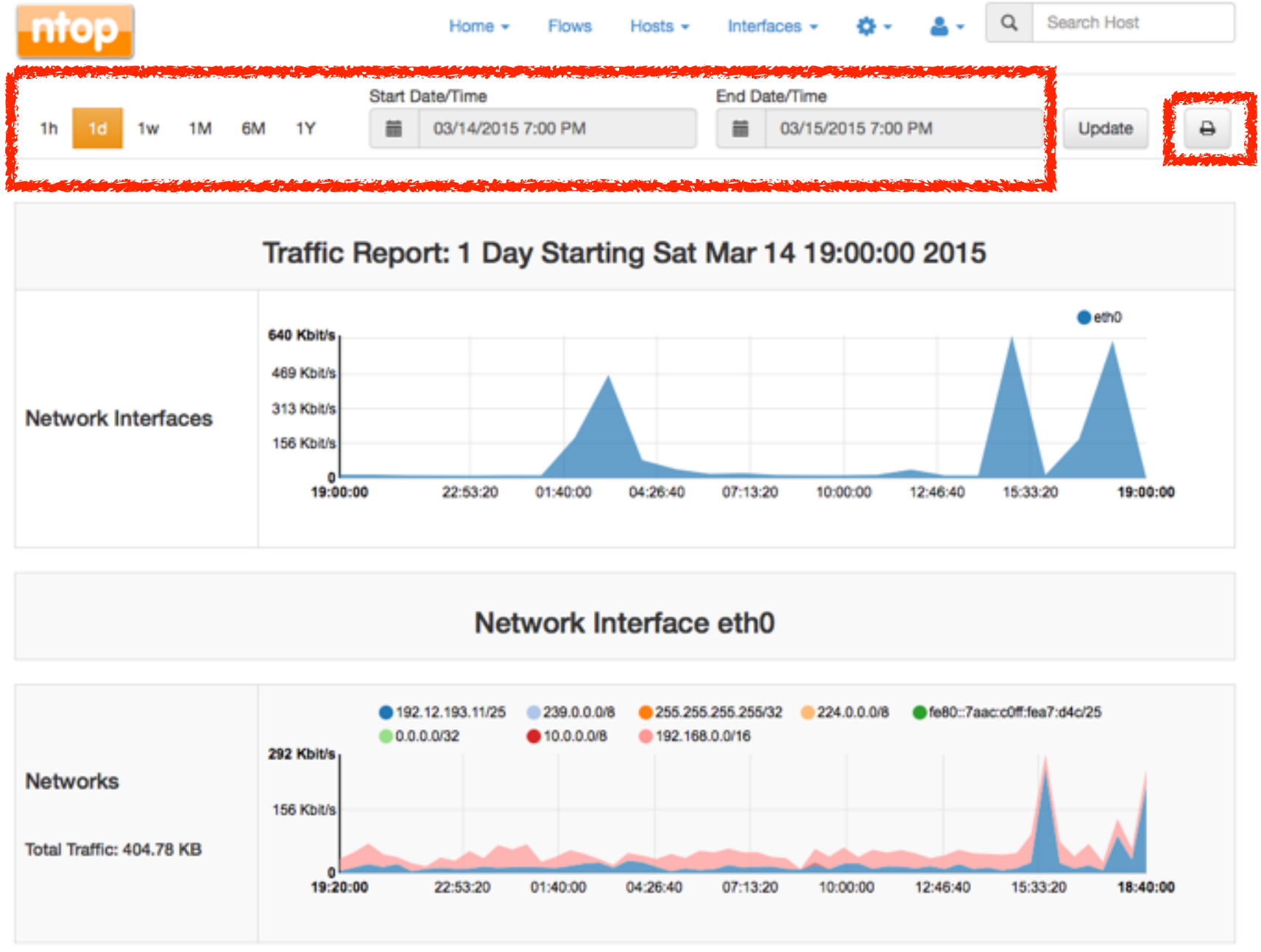
© 2015 - ntop.org

Packets Never Lie [3/3]

- You can now see in realtime what is happening inside ntopng at packet level…
- …and at the same time ntopng generates pcap files for you.

© 2015 - ntop.org

Reports [1/3]



Historical

Print

Reports [2/3]

- Compact, file-system based (no DB is required so it can work with embedded systems), reports

Top Countries [Average Traffic/sec]

Senders		Receivers	
IT	1.06 GB (103 Kbit/s)	IT	912.62 MB (86 Kbit/s)
NL			
US			
FR			
IE			
GB			
CN			
EU			
JP			

Top ASN [Average Traffic/sec]

Senders		Receivers	
0 [Local/Unknown]	599.52 MB (57 Kbit/s)	2597 [Registry of ccTLD it - IIT-CNR]	855.49 MB (81 Kbit/s)
2597 [Registry of ccTLD it - IIT-CNR]	420.16 MB (40 K		
5602 [KPNQwest Italia S.p.a]	393.30 MB (37 K		
137 [Consortium GARR]	304.27 MB (29 K		
200130 [Digital Ocean, Inc.]	27.04 MB (3 Kbi		
3269 [Telecom Italia S.p.a.]	7.27 MB (705 by		
15169 [Google Inc.]	6.84 MB (663 by		
41231 [Canonical Ltd]	6.35 MB (616 by		

Top Local Hosts [Average Traffic/sec]

Senders		Receivers	
pc-deri.nic.it	132.56 MB (13 Kbit/s)	pc-deri.nic.it	794.73 MB (75 Kbit/s)
perseus.nic.it	117.28 MB (11 Kbit/s)	10.255.255.255	121.42 MB (12 Kbit/s)
dhcpc.nic.it	87.14 MB (8 Kbit/s)	dhcpc.nic.it	25.79 MB (2 Kbit/s)
HPM476dw-A23c.local	64.51 MB (6 Kbit/s)	NPIE06A71.local	21.69 MB (2 Kbit/s)
AirPort-Time-Capsule-di-Rera3.local	49.83 MB (5 Kbit/s)	192.168.0.255	15.58 MB (1 Kbit/s)
hpfax-reprint.local	48.92 MB (5 Kbit/s)	hp3005-cs.local	15.36 MB (1 Kbit/s)
NPIAB36C0.local	46.12 MB (4 Kbit/s)	xerox-7760-exm2.local	13.90 MB (1 Kbit/s)
NPI7D6365.local	45.78 MB (4 Kbit/s)	xerox2125.nic.it	11.59 MB (1 Kbit/s)
xerox-7760-exm2.local	44.23 MB (4 Kbit/s)	NPIF967E4.local	10.45 MB (1014 bps)
Time-Capsule-di-Maurizio.local	43.42 MB (4 Kbit/s)	239.255.255.250	8.82 MB (856 bps)
AirPort-Time-Capsule-di-Rera2.local	43.37 MB (4 Kbit/s)	ovpnc.nic.it	6.79 MB (658 bps)

© 2015 - ntop.org

Reports [3/3]

Interactive Talkers

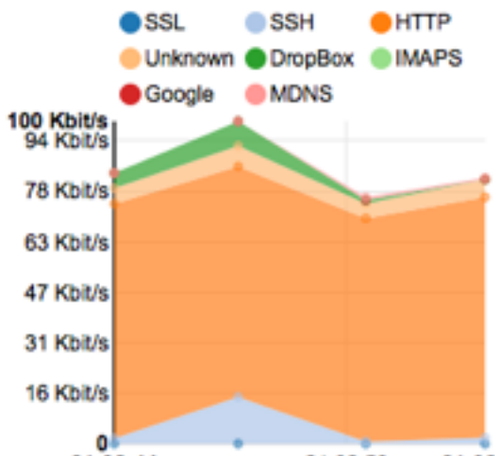
Click to Zoom

© 2015 - ntop.org

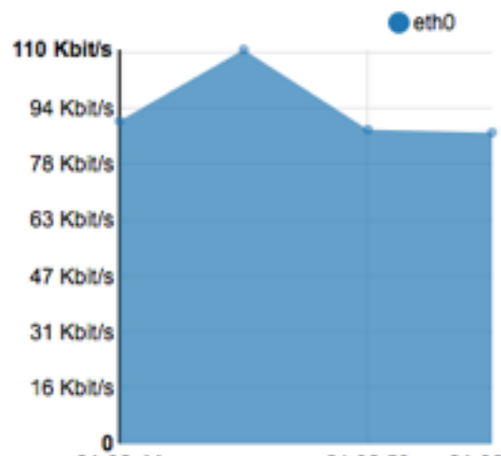
Modular Dashboard

eth0: Top Talkers	Actual Traffic
pc-deri.nic.it	58.49 Kbit/s ↓
host240-180-dynamic.10-79-r.retail.telecomitalia.it	48.55 Kbit/s ↓
115.239.228.11	8.28 Kbit/s ↑
Broadcast	1.56 Kbit/s ↑
192.12.193.127	1.02 Kbit/s ↓
nsresolv1.nic.it	1019 bps ↑
mac-mallia.nic.it	991.8 bps ↑
pc-sideri.nic.it	639.87 bps ↑

eth0: Realtime Top Application Traffic

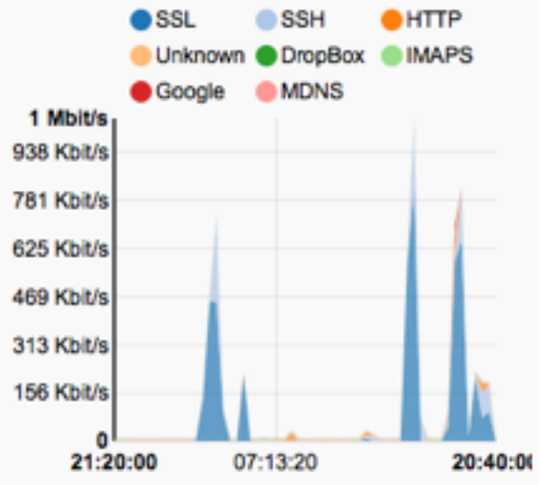


Network Interfaces: Realtime Traffic

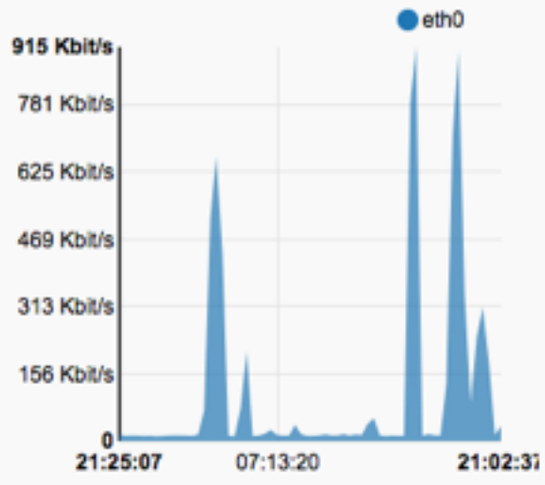


eth0: Top HTTP Site Contacts	Actual	Total
i7.ntop.org	8 ↓	6,966

eth0: Top Application Traffic Last Day View

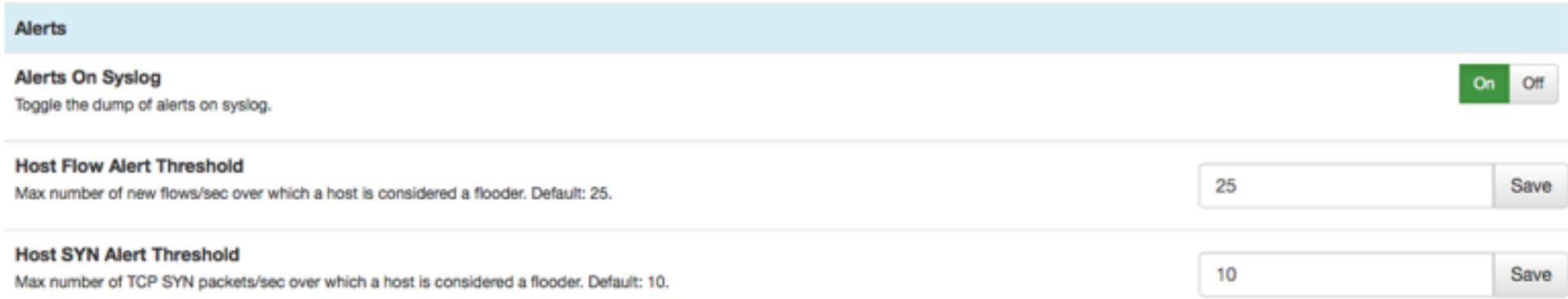


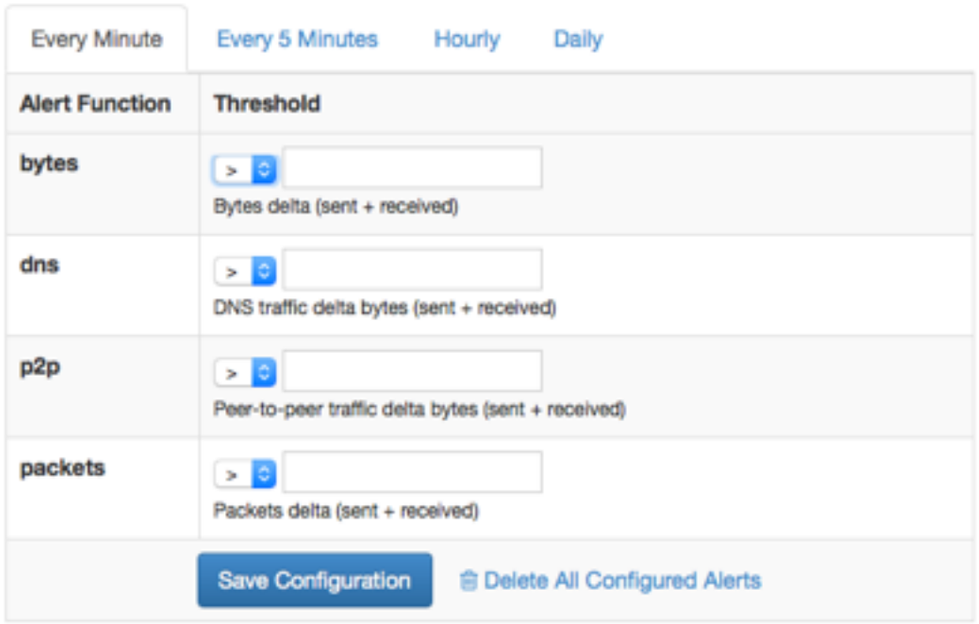
Network Interfaces: Last Day View

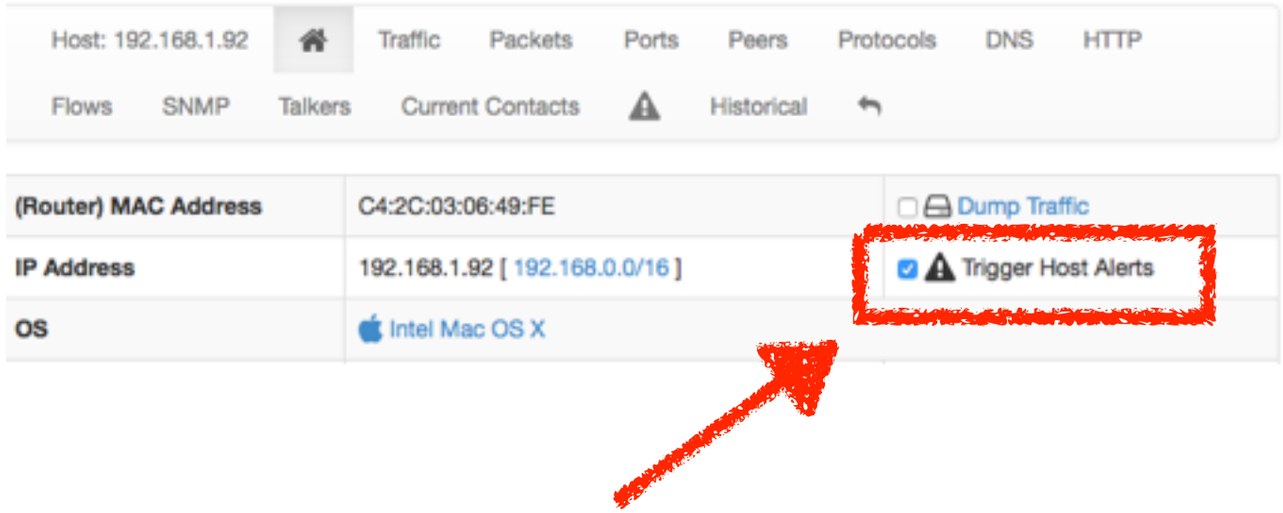


© 2015 - ntop.org

Alerts [1/2]







Per-host Alert Preferences

© 2015 - ntop.org

Alerts [2/2]

Queued Alerts

10

Action	Date	Severity	Type	Description
	Sun Mar 15 20:52:20 2015	Error	TCP SYN Flood	Host 192.168.1.92 is a SYN flooder [68 SYNs sent in the last 3 sec] TCP 192.168.1.92:60970 > 23.50.145.215:443 [proto: 0/Unknown][1/0 pkts][78/0 bytes]
	Sun Mar 15 20:50:05 2015	Error	TCP SYN Flood	Host 192.168.1.92 is a SYN flooder [72 SYNs sent in the last 3 sec] TCP 192.168.1.92:60321 > 37.252.170.95:80 [proto: 0/Unknown][1/0 pkts][78/0 bytes]
	Sun Mar 15 20:49:46 2015	Error	TCP SYN Flood	Host 192.168.1.92 is a SYN flooder [64 SYNs sent in the last 3 sec] TCP 192.168.1.92:60172 > 64.202.112.8:80 [proto: 0/Unknown][1/0 pkts][78/0 bytes]
	Sun Mar 15 20:49:24 2015	Error	TCP SYN Flood	Host 192.168.1.92 is a SYN flooder [95 SYNs sent in the last 3 sec] TCP 192.168.1.92:60003 > 54.235.188.239:80 [proto: 0/Unknown][1/0 pkts][78/0 bytes]
	Sun Mar 15 20:48:51 2015	Error	TCP SYN Flood	Host 192.168.1.92 is a SYN flooder [77 SYNs sent in the last 3 sec] TCP 192.168.1.92:59751 > 23.223.58.13:80 [proto: 0/Unknown][1/0 pkts][78/0 bytes]
	Sun Mar 15 19:14:38 2015	Error	TCP SYN Flood	Host 127.0.0.1 is under SYN flood attack [255 SYNs received in the last 3 sec] TCP 127.0.0.1:51416 > 127.0.0.1:3000 [proto: 0/Unknown][1/0 pkts][68/0 bytes]
	Sun Mar 15 19:14:38 2015	Error	TCP SYN Flood	Host 127.0.0.1 is a SYN flooder [255 SYNs sent in the last 3 sec] TCP 127.0.0.1:51416 > 127.0.0.1:3000 [proto: 0/Unknown][1/0 pkts][68/0 bytes]
	Sun Mar 15 19:14:38 2015	Error	TCP SYN Flood	Host ::1 is under SYN flood attack [255 SYNs received in the last 3 sec] TCP ::1:51415 > ::1:3000 [proto: 0/Unknown][1/0 pkts][88/0 bytes]
	Sun Mar 15 19:14:38 2015	Error	TCP SYN Flood	Host ::1 is a SYN flooder [255 SYNs sent in the last 3 sec] TCP ::1:51415 > ::1:3000 [proto: 0/Unknown][1/0 pkts][88/0 bytes]
	Sun Mar 15 19:13:27 2015	Error	TCP SYN Flood	Host 127.0.0.1 is under SYN flood attack [115 SYNs received in the last 3 sec] TCP 127.0.0.1:51123 > 127.0.0.1:3000 [proto: 0/Unknown][1/0 pkts][68/0 bytes]

Showing 1 to 10 of 328 rows

« < 1 2 3 4 5 > »

© 2015 - ntop.org

SNMP

Host: 192.168.1.92 | Traffic | Packets | Ports | Peers | Protocols | DNS | HTTP | Flows | SNMP | Talkers

Current Contacts | Historical

SNMP Community	public Save Community
SysDescr	Darwin Lucas-iMac.local 14.1.0 Darwin Kernel Version 14.1.0: Thu Feb 26 19:26:47 PST 2015; root:xnu-2782.10.73~1/RELEASE_X86_64 x86_64
SysUptime	57 min, 32 sec
SysContact	Administrator
SysName	Lucas-iMac.local
SysLocation	Right here, right now.
SysServices	76

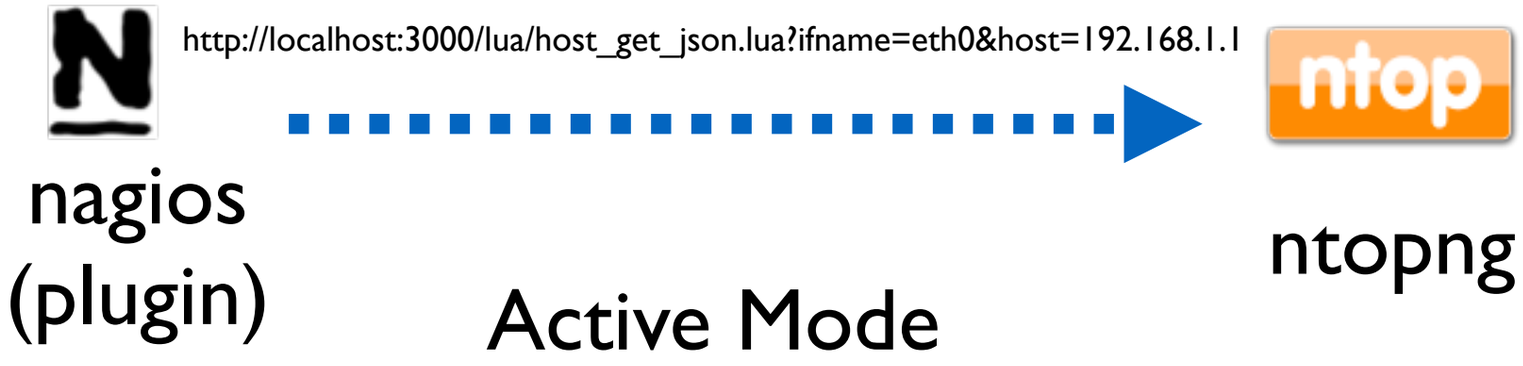
Id	Name	Type	MTU	Speed	Mac Address	Status	In Bytes	Out Bytes	In Discards	Last Change
1	lo0	softwareLoopback	16384			Up	507.95 MB	507.95 MB	0	0
2	gif0	ieee80212	1280			Down	0 Bytes	0 Bytes	0	0
3	stf0	hippiInterface	1280			Down	0 Bytes	0 Bytes	0	0
4	en0	ethernetCsmacd	1500	1 Gbit	00:2C:03:06:49:FE	Up	555.39 MB	102.56 MB	0	0
5	en1	ethernetCsmacd	1500		00:30:62:56:00:1C	Down	0 Bytes	0 Bytes	0	0
6	fw0	ieee1394	4078	10 Mbit		Up	0 Bytes	346 Bytes	0	0
7	p2p0	ethernetCsmacd	2304	10 Mbit	00:30:62:56:00:1C	Down	0 Bytes	0 Bytes	0	0

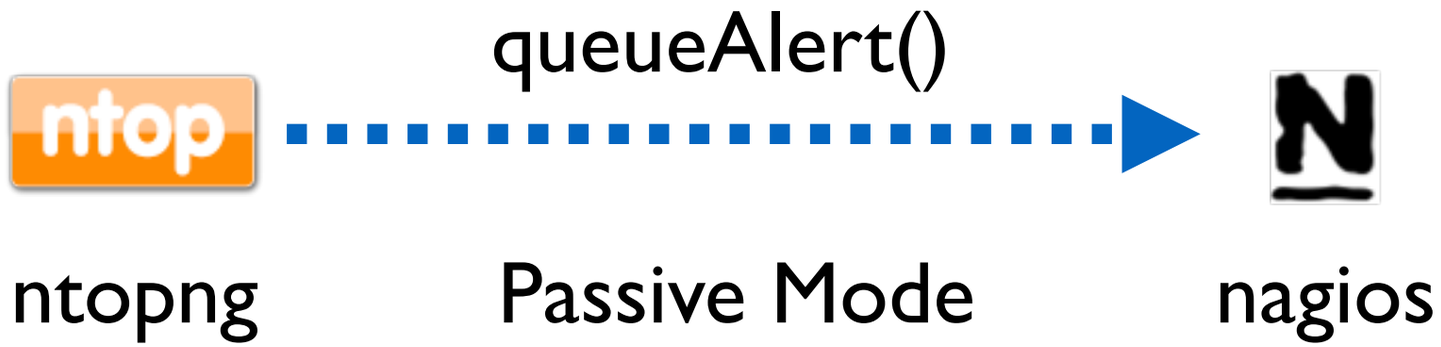
© 2015 - ntop.org

Nagios [1/2]

- ntopng can be used by nagios as:
  - Data source (e.g. give me the traffic of host X)
- ntopng can use nagios for:
  - Sending alerts and state changes.

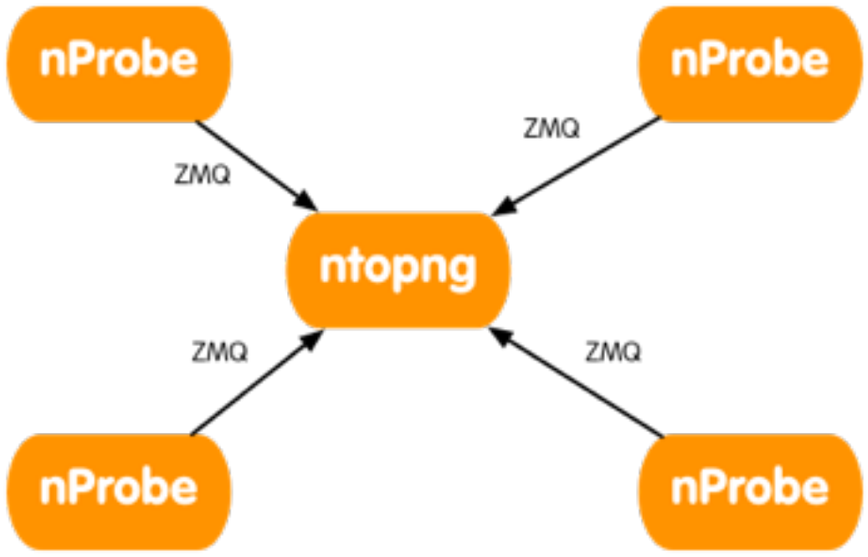
Nagios [2/2]

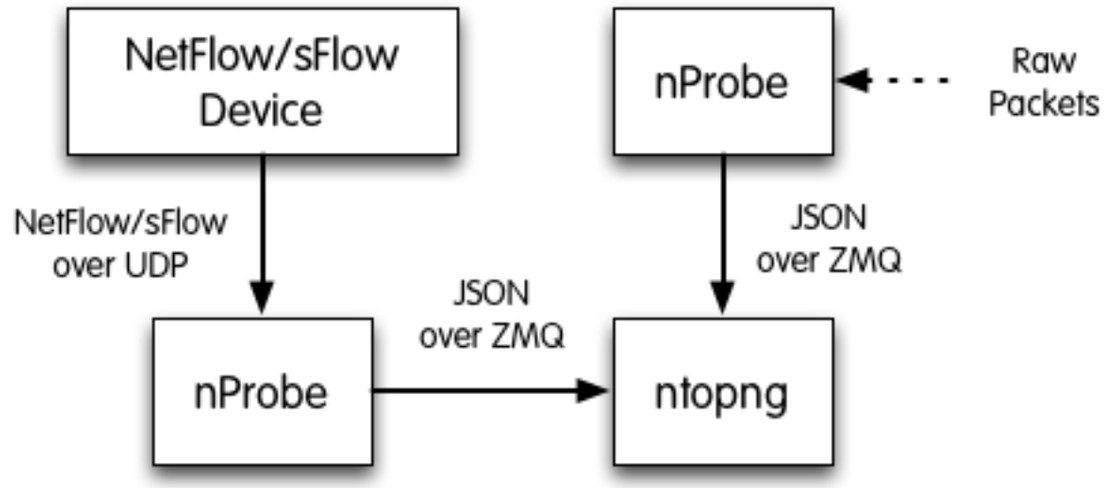

http://localhost:3000/lua/host_get_json.lua?ifname=eth0&host=192.168.1.1
nagios
(plugin)
Active Mode
ntopng


queueAlert()
ntopng
Passive Mode
nagios

NetFlow/IPFIX/sFlow Collection

- Flow collection is implemented using nProbe.
- Flows are converted to JSON and sent over ØMQ.
- {“8”:"192.12.193.11","12":"192.168.1.92","15":"0.0.0.0","10":0,"14":0,"2":5,"1":406,"22":1412183096,"21":1412183096,"7":3000,"11":55174,"6":27,"4":6,"5":0,"16":2597,"17":0,"9":0,"13":0,"42":4}

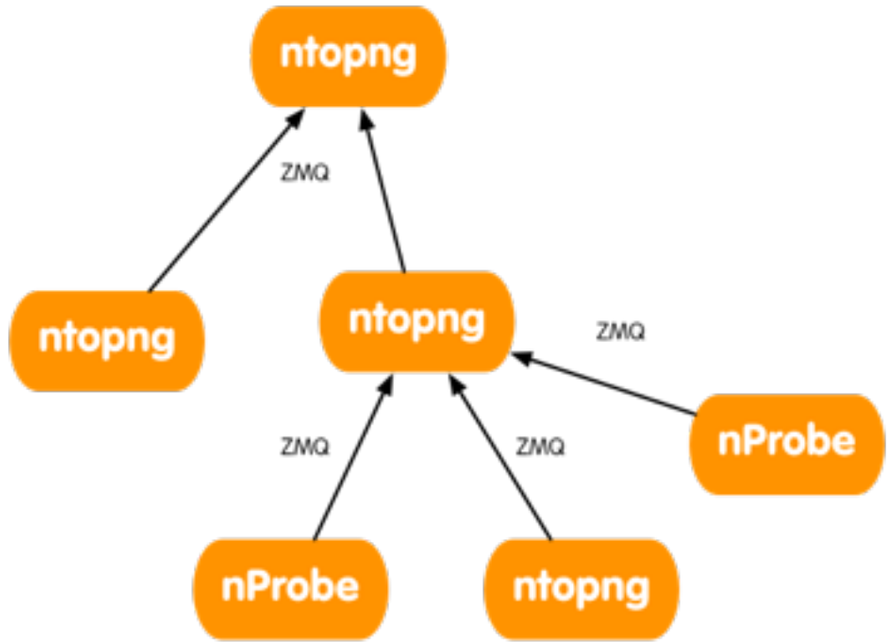




© 2015 - ntop.org

Multi-Tenancy

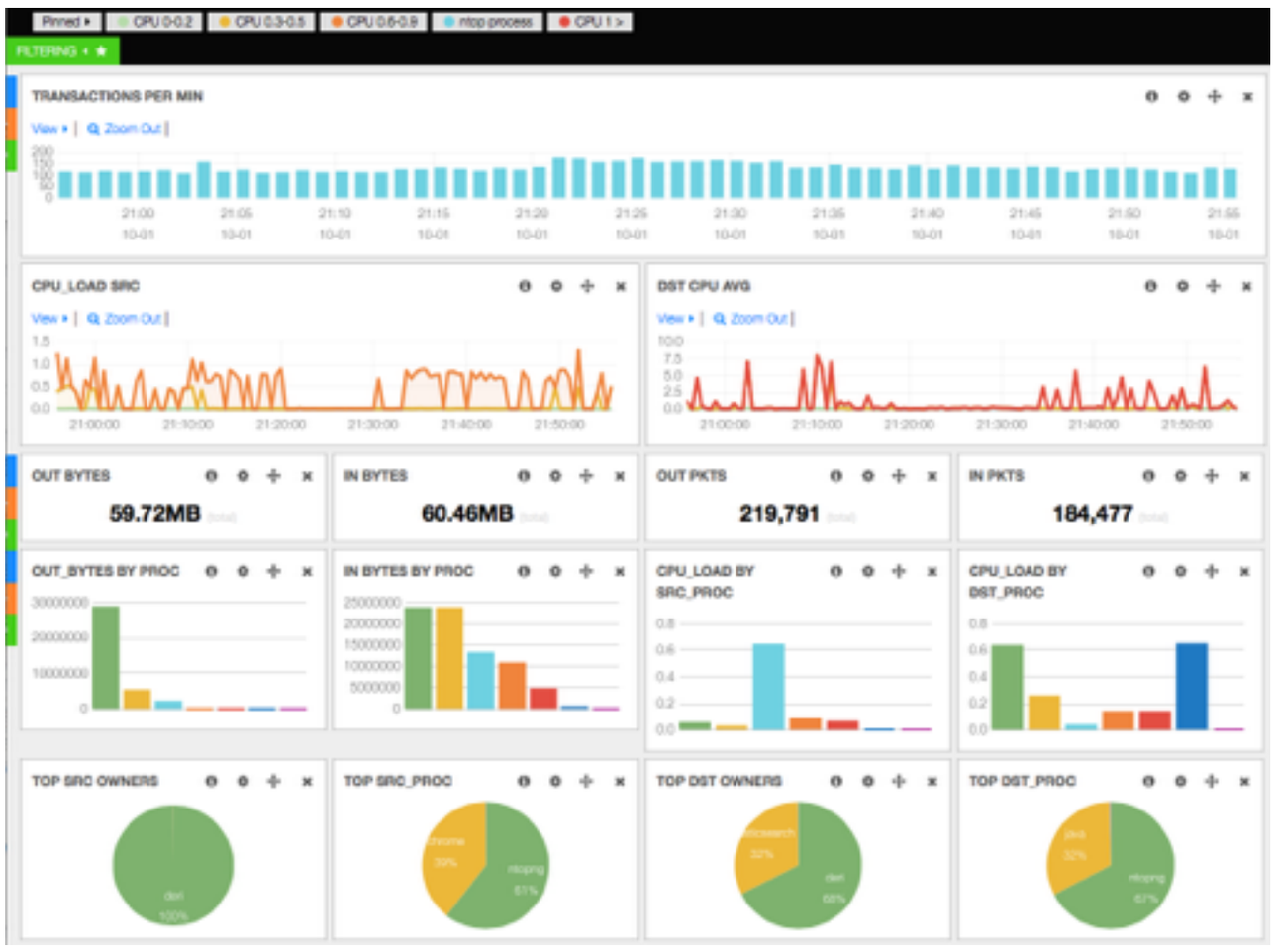
- ntopng has natively the ability to create multi-tenancy topologies using the same ØMQ used for flow collection.
- It is possible to create complex father-son topologies where the top ntopng instance receives data from the bottom instances.



© 2015 - ntop.org

Big Data with ElasticSearch

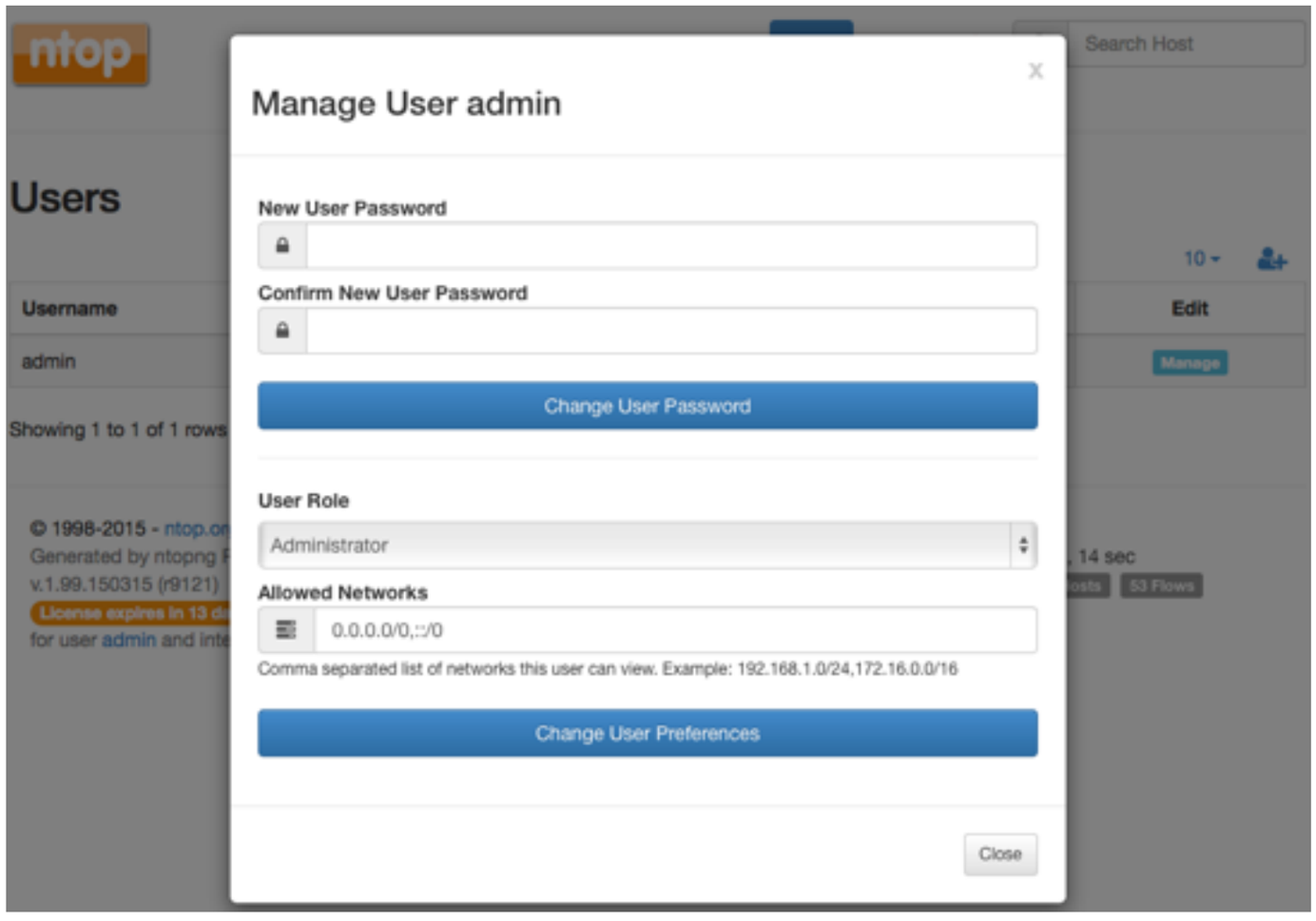
- ntopng can natively export flows information into ElasticSearch, a popular big data database.
- Using applications such as Kibana it is possible to visualise in realtime data exported di ntopng.



© 2015 - ntop.org

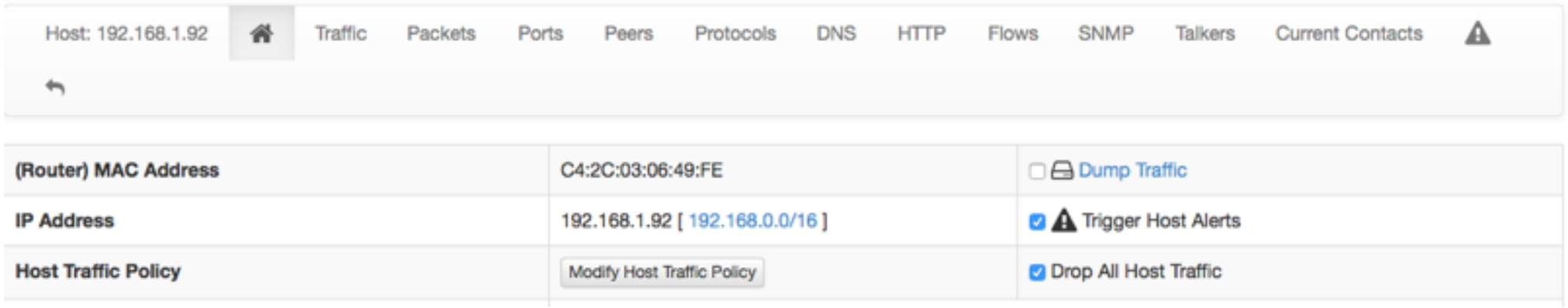
Multi User Support

- ISPs can use ntopng to show their users only the portion of the hosts that matter them.



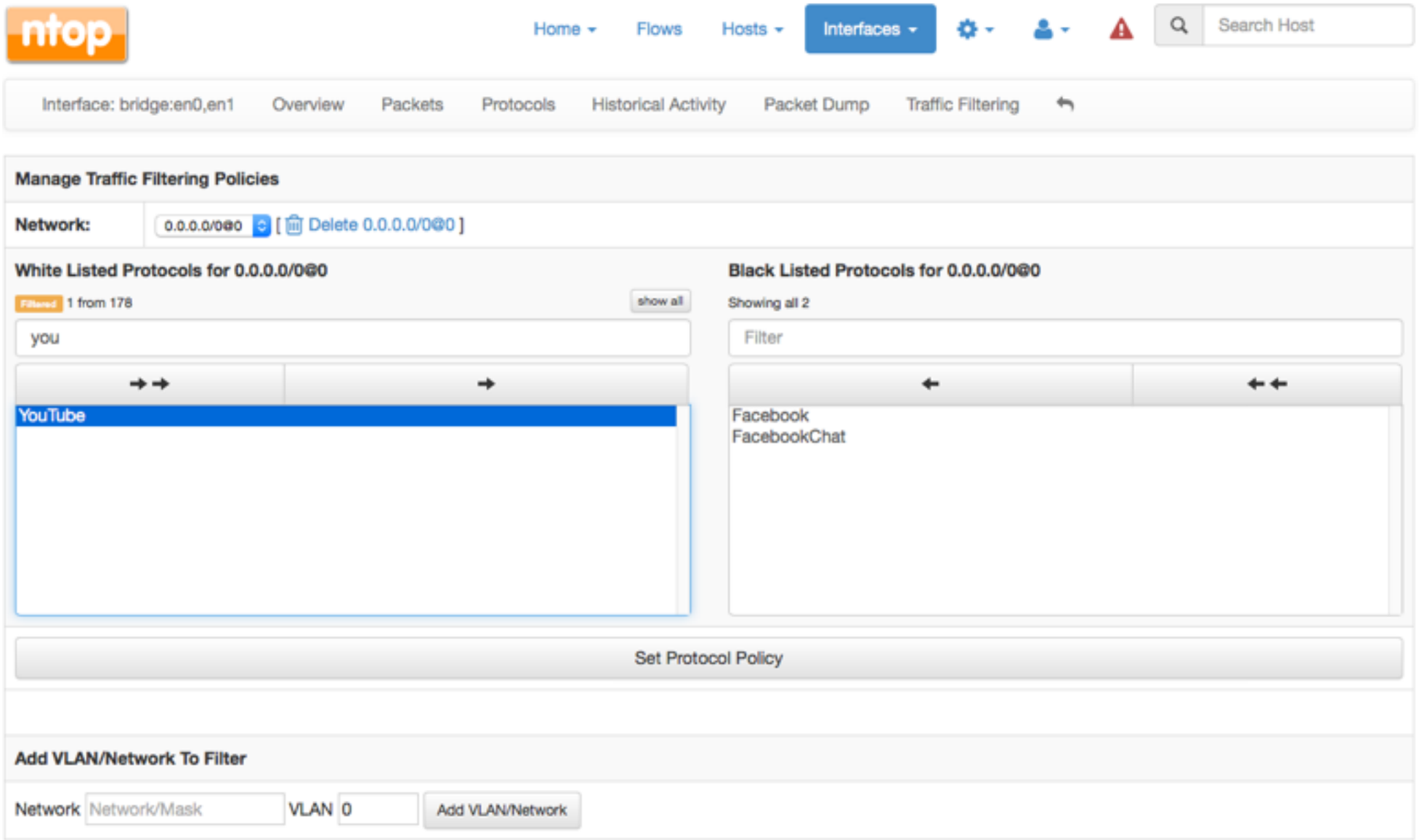
Layer-7 Traffic Enforcement [1/2]

ntopng
(Bump-In-The-Wire)



© 2015 - ntop.org

Layer-7 Traffic Enforcement [2/2]



© 2015 - ntop.org

Final Remarks

- We believe that open-source traffic network monitoring should be simple and cheap.
- Commodity hardware, with adequate software, can now match the performance and flexibility that markets require. With the freedom of open source.
- ntopng is available under GNU GPLv3 from http://www.ntop.org/.

© 2015 - ntop.org