Network Security Using ntopng

Understanding Host Behaviour [1/2]

- Security attacks can originate from both local and remote hosts.
- It is important to characterise host behaviour in order to detect invalid traffic patterns and thus react.
- Typical misbehaved hosts include:
  - Multiple (low bandwidth) egress connections.
  - Connections with hosts on countries unlikely to be contacted.
  - Use of unfriendly protocols such as SSL connections with self-signed certificates.

Understanding Host Behaviour [2/2]

- Host behaviour is the result of the combination of flow traffic analysis.

SSL Certificate	Client Requested: luca.ntop.org	Server Certificate: shop.ntop.org Certificates don't match
Max (Estimated) TCP Throughput	Client → Server: 91.57 Kbit	Client ← Server: 1.49 Mbit
TCP Flags	Client → Server: FIN SYN PUSH ACK	Client ← Server: FIN SYN PUSH ACK
	This flow is completed and will expire soon.	
Flow Status	SSL Certificate Mismatch	

IPv6 Address Assignment

- IPv6 hosts can configure themselves automatically using the Neighbour Discovery Protocol in ICMPv6 discovery messages.
- To find out unwanted advertisers do:

ICMPV6

Active ICMPV6 Flows

10 Hosts Applications IP Version

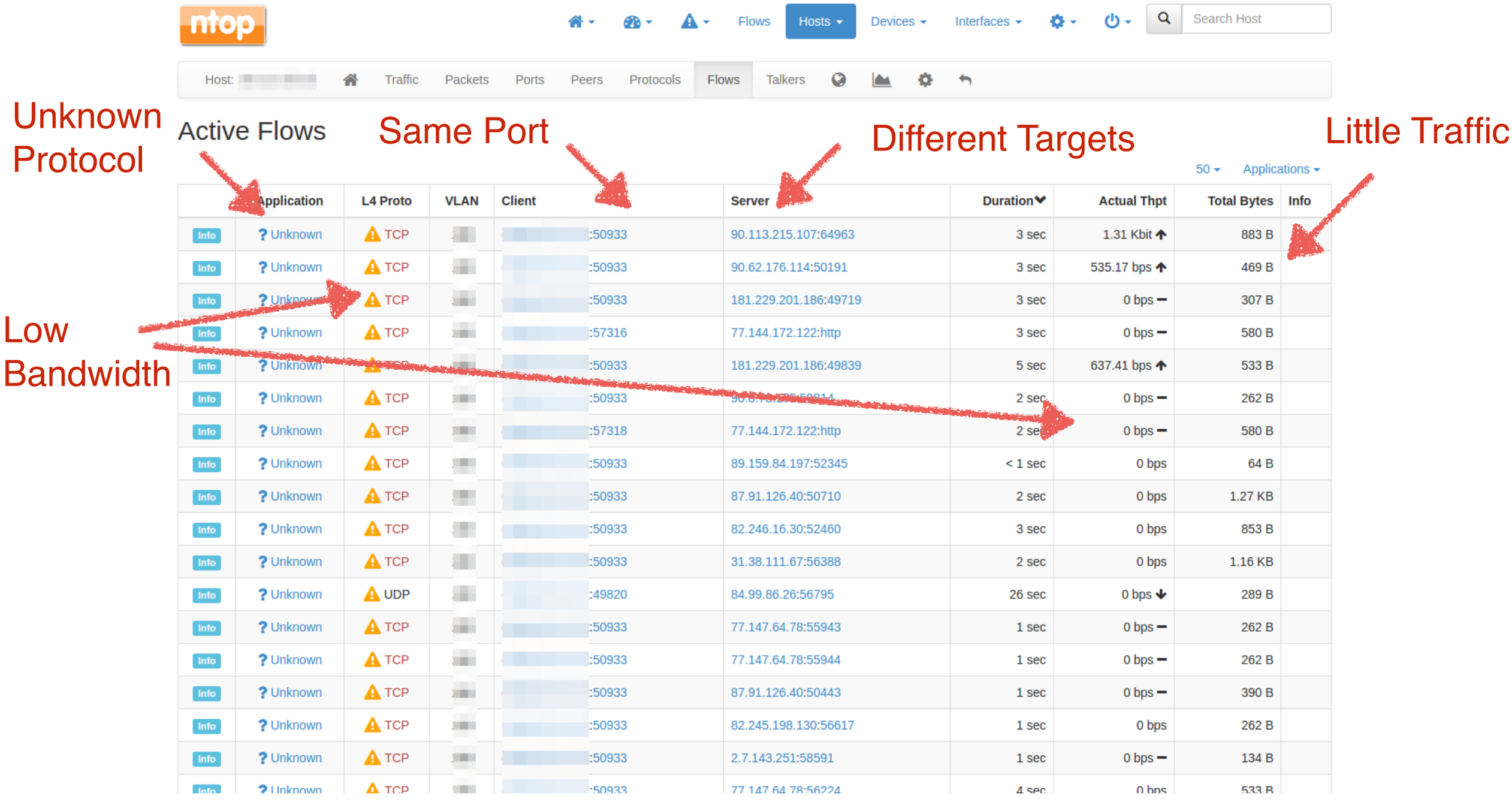
	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	ICMPV6	IPv6-ICMP			< 1 sec	Client	0 bps	86 B	Neighbor Solicitation
Info	ICMPV6	IPv6-ICMP	fe80::8aa2:5eff:fee6...	ff02::1	1 sec	Client	0 bps	172 B	Neighbor Advertisement
Info	ICMPV6	IPv6-ICMP		ff02::1	1 min, 10 sec	Client	0 bps	430 B	Neighbor Advertisement
Info	ICMPV6	IPv6-ICMP	fe80::f6b5:2f00:fc:a...		< 1 sec	Client	0 bps	78 B	Neighbor Advertisement
Info	ICMPV6	IPv6-ICMP	fe80::226:88ff:fe7f:...	ff02::1	1 min, 10 sec	Client	0 bps	430 B	Neighbor Advertisement
Info	ICMPV6	IPv6-ICMP		ff02::1	1 sec	Client	0 bps	172 B	Neighbor Advertisement

Showing 1 to 6 of 6 rows

Detecting Command & Control [1/2]

- In case an internal (external accesses are mediated by firewall devices and thus are more difficult) host is infected, such host can run an Internet robot (a.k.a. bot) for running automatic tasks over the Internet.
- Malicious use of bots is the coordination and operation of an automated attack on networked computers.
- A typical bot behaviour consists of opening (a) several (b) low-bandwidth (c) client connection over unknown layer-7 protocols to instruct remote bots.

Detecting Command & Control [2/2]



DNS and Infections [1/5]

- The analysis of DNS traffic can be used as a looking glass for spotting infections.
- DGAs (Domain Generation Algorithm) are used i various families of malware to generate rendezvous points for command & control (see previous slide).
- In literature, the first malware using DGAs was Kraken (2008).
- Crypto-locker apps often use DGAs for this purpose.

DNS and Infections [2/5]

- Usually DGAs take as input a seed that is used to generate many pseudo-random domain names.
- The malware keep generating domain names up until there is one registered that is used to connect to the "malware network".
- ntopng can analyse DNS traffic and spot these problems. Note that when we see DNS traffic for DGAs we might have been victim of an attack.

DNS and Infections [3/5]

Examples of DGAs

```
<IP resolver> <GEO Resolver> <DNS Request>
a.b.c.d    IT    Turin    afupelalikovacah.com.mydomain.it
a.b.c.d    IT    Turin    epolowypuvugijys.com.mydomain.it
a.b.c.d    IT    Turin    uzowawibehezojil.com.mydomain.it
a.b.c.d    IT    Turin    yfohizihifozoral.com.mydomain.it
a.b.c.d    IT    Turin    epolowypuvugijys.com.mydomain.it
a.b.c.d    IT    Turin    uzowawibehezojil.com.mydomain.it
a.b.c.d    IT    Turin    yfohizihifozoral.com.mydomain.it
a.b.c.d    IT    Turin    ibpirauljhskybqlfdqnvtpz.ru.mydomain.it
a.b.c.d    IT    Turin    krmfbypgavgoxklrscbmvolq.ru.mydomain.it
a.b.c.d    IT    Turin    tkvnjzxlrjnwgeavcnflfsohgkb.ru.mydomain.it
a.b.c.d    IT    Turin    qusspxmese.mydomain.it
a.b.c.d    IT    Turin    sxievblqv.mydomain.it
a.b.c.d    IT    Turin    amsssmy.mydomain.it
a.b.c.d    IT    Turin    qkbmzxwcshedyprksckrukbnfz.ru.mydomain.it
a.b.c.d    IT    Turin    riolnodfogydy.mydomain.it
a.b.c.d    IT    Turin    ufqqzkphnpx.mydomain.it
a.b.c.d    IT    Turin    oxctpbjzfvf.mydomain.it
```

```
def generate_domain(year, month, day):
    """Generates a domain name for the given date."""
    domain = ""

    for i in range(16):
        year = ((year ^ 8 * year) >> 11) ^ ((year & 0xFFFFFFF0) << 17)
        month = ((month ^ 4 * month) >> 25) ^ 16 * (month & 0xFFFFFFF8)
        day = ((day ^ (day << 13)) >> 19) ^ ((day & 0xFFFFFFFE) << 12)
        domain += chr(((year ^ month ^ day) % 25) + 97)

    return domain
```

DNS and Infections [4/5]

- The best approach is start analysing DNS traffic

Select DNS

Queries

Active DNS Flows

10 Hosts Applications IP Version

	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	DNS	UDP	:54666	:domain	< 1 sec	Cli Server	0 bps	941 B	xml2.corriereobjects.it ContentServer
Info	DNS	UDP	:43845	:domain	< 1 sec	Clie Server	0 bps	623 B	xml.corriereobjects.it ContentServer
Info	DNS	UDP	:53835	:domain	< 1 sec	Clie Server	0 bps	547 B	www.trovoaste.it Generic
Info	DNS	UDP	:43740	:domain	< 1 sec	Clie Server	0 bps	461 B	www.dday.it FreeTime
Info	DNS	UDP	:60289	:domain	1 sec	Clie Server	0 bps	563 B	www.corriere.it News
Info	DNS	UDP	:45126	:domain	< 1 sec	Clie Server	0 bps	716 B	vivimilano.corriere.it News
Info	DNS	UDP	:48302	:domain	< 1 sec	Clie Server	0 bps	523 B	video.corriere.it News
Info	DNS	UDP	:39114	:domain	< 1 sec	Clie Server	0 bps	559 B	vicenza.corriere.it News
Info	DNS	UDP	:57737	:domain	< 1 sec	Clie Server	0 bps	555 B	verona.corriere.it News
Info	DNS	UDP	:57524	:domain	< 1 sec	Clie Server	0 bps	559 B	venezia.corriere.it News

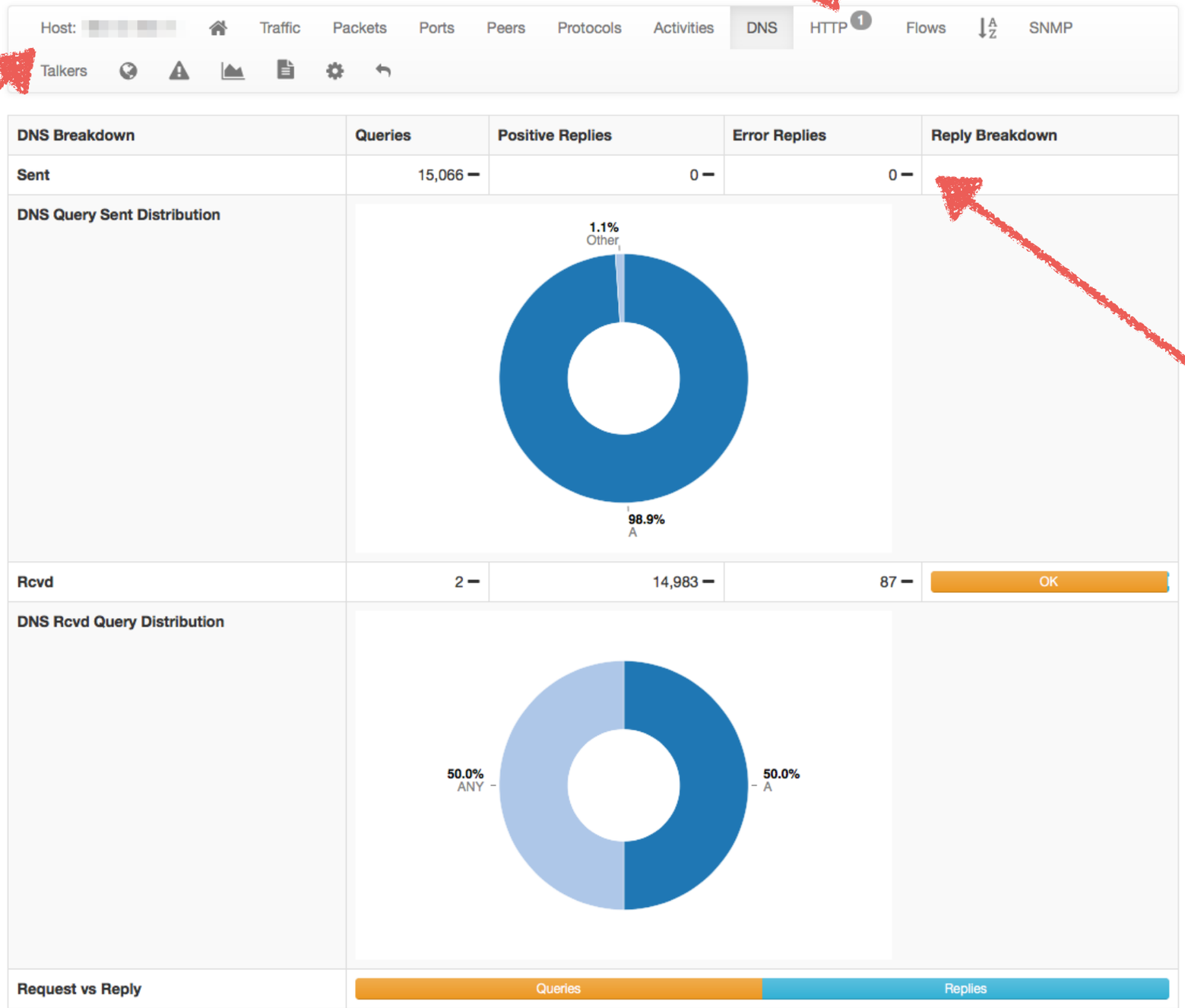
Showing 1 to 10 of 70 rows

« < 1 2 3 4 5 > »

DNS and Infections [5/5]

Select DNS

Drill-down on
a specific host



Analyse Replies

MAC/ARP Monitoring and Scanning [1/2]

- ARP (Address Resolution Protocol) is not used just to bind MAC addresses to IPs, but also for monitoring device presence (e.g. in DHCP networks).
- However it can also be used for scanning networks (e.g. with nmap, fing and other tools).

MAC/ARP Monitoring and Scanning [1/2]

All Layer 2 Devices

ARP Stats

10 ▾ Filter MACs▾ Manufacturer▾

MAC Address	Manufacturer	Hosts	ARP Sent▾	ARP Received	Seen Since	Breakdown	Throughput	Traffic
80:2A:A8:8D:69:2C	Ubiquiti Networks Inc.	269	38	8	4 min, 32 sec	Sent Rc	9.1 Kbit	4.36 MB
C4:2C:03:06:49:FE	Apple, Inc.	1	10	8	4 min, 32 sec	Se Rcvd	8.75 Kbit	4.37 MB
CC:2D:8C:F6:C7:39	LG ELECTRONICS INC	1	5	2	4 min, 30 sec	Sent R	95.88 bps	14.62 KB
54:4E:90:BA:EC:84	Apple, Inc.	2	5	0	2 min, 16 sec	Sent	361.17 bps	10.22 KB
AC:87:A3:16:3E:30	Apple, Inc.	1	0	0	4 min, 6 sec	Sent	0 bps	2.61 KB
80:2A:A8:8D:2B:EE	Ubiquiti Networks Inc.	1	0	0	3 min, 30 sec	Sent	0 bps	228 B
26:A4:3C:FF:4C:D7	n/a	0	0	0	2 min, 24 sec	Sent	0 bps	468 B
28:57:BE:E3:D7:CF	Hangzhou Hikvision Digital Technology Co.,Ltd.	1	0	0	4 min, 31 sec	Sent	0 bps	13.6 KB
24:A4:3C:FE:4C:D7	Ubiquiti Networks Inc.	1	0	0	2 min, 22 sec	Sent	0 bps	1.45 KB

Showing 1 to 9 of 9 rows

Hosts Monitoring

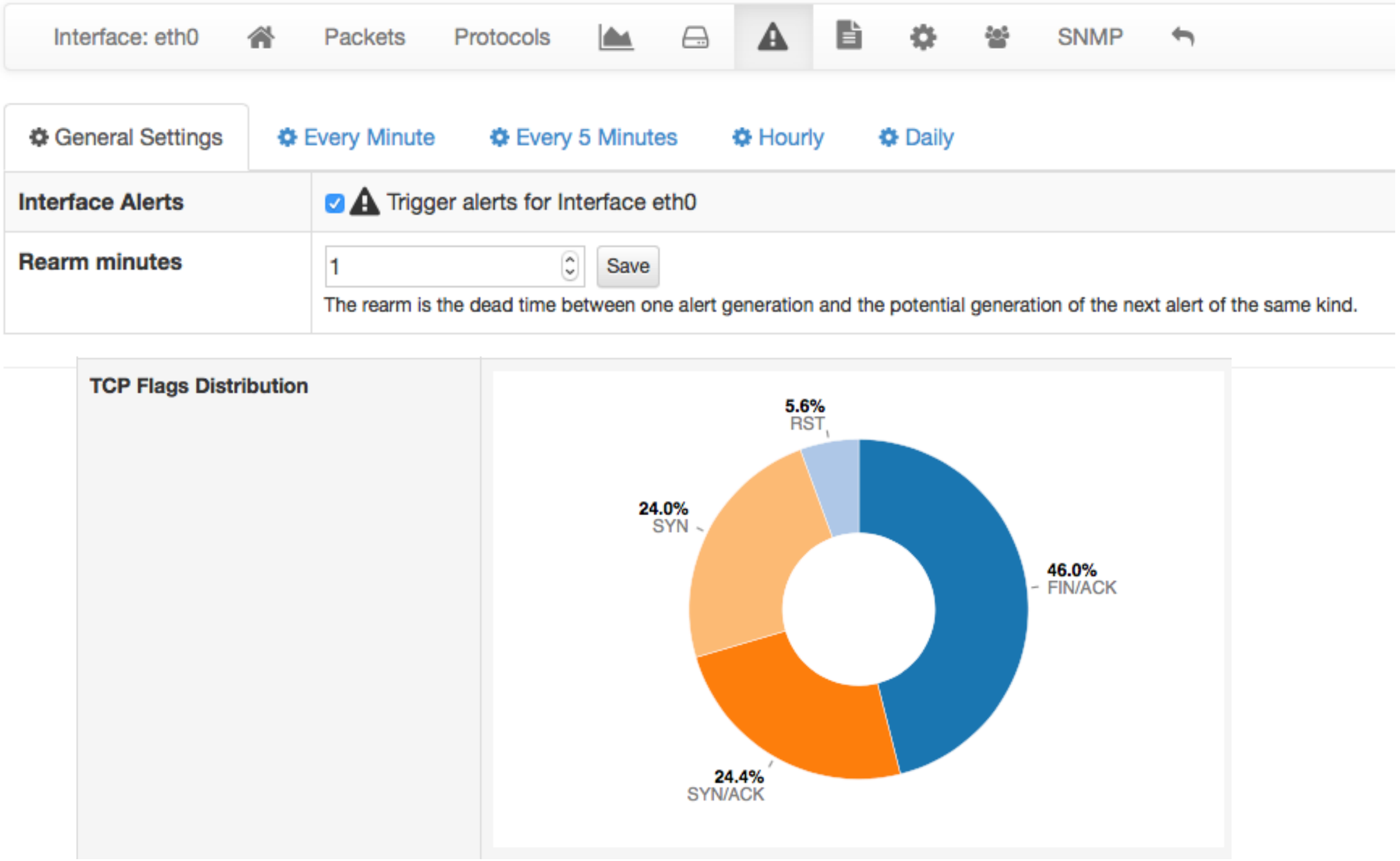
Mac: 80:2A:A8:8D:69:2C

MAC Address	80:2A:A8:8D:69:2C (Ubiquiti_8D:69:2C) [Show Hosts]	80:2A:A8:8D:69:2C Save
First / Last Seen	02/04/2017 19:28:54 [4 min, 35 sec ago]	02/04/2017 19:33:26 [3 sec ago]
Sent vs Received Traffic Breakdown	Sent Rcvd	
Traffic Sent / Received	5,111 Pkts / 3.71 MB	4,558 Pkts / 666.24 KB
Address Resolution Protocol	**ARP Requests**	**ARP Replies**
	38 Sent / 0 Received	0 Sent / 8 Received

Detecting TCP Flags-based Attacks [1/2]

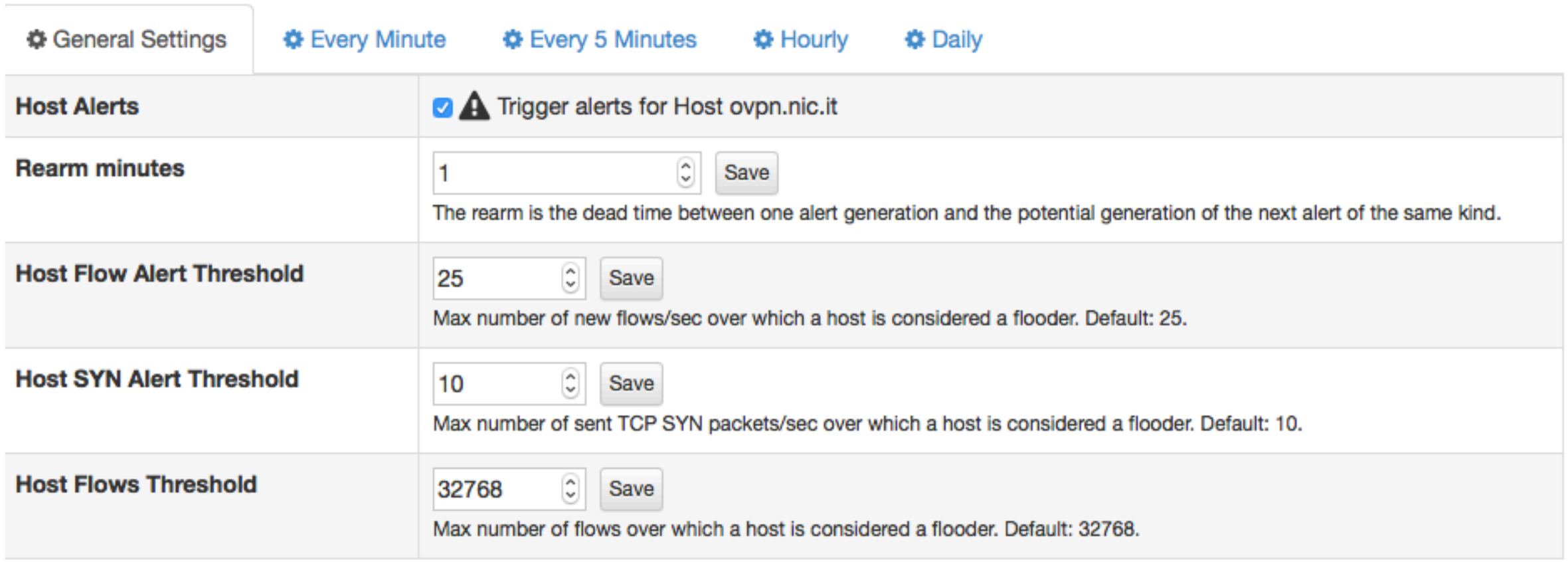
- TCP flags distribution can indicate source of problems as in theory you should have a 1:1 ratio for:
  - SYN vs SYN|ACK
  - ICMP ECHO Request vs ECHO Reply
  - ARP Request vs ARP Reply
- TCP FIN vs RST distribution analysis is an interesting parameter for detecting scans.
- ntopng keeps these statistics and it allows alerts to be generated based on these values.

Detecting TCP Flags-based Attacks [2/2]



Detecting Scans

- ntopng has native detection of scans that can be used to detect them regardless of their nature such as SYN scan and Slowloris (low goodput).



ICMP Traffic Monitoring [1/2]

- ICMP messages are useful for detecting traffic anomalies:
  - ICMP Redirect: MITM, asymmetric path
  - Destination unreachable: network scan?
  - Port unreachable: service scan or a service previously up is now down?
- ntopng is able to monitor ICMP messages and to report issues via alarms it generates on hosts and interfaces.

ICMP Traffic Monitoring [2/2]

ICMP Message	Packets Sent	Last Sent Peer	Packets Received	Last Rcvd Peer	Breakdown	Total
Neighbor Advertisement	4 Pkts		0 Pkts		Sent	4 Pkts
Neighbor Solicitation	0 Pkts		4 Pkts		Rcvd	4 Pkts

ICMP Message	Packets Sent	Last Sent Peer	Packets Received	Last Rcvd Peer	Breakdown	Total
Destination Port Unreachable	103 Pkts		3 Pkts		Sent	106 Pkts
Echo Request	0 Pkts		1 Pkts		Rcvd	1 Pkts
Echo Reply	1 Pkts		0 Pkts		Sent	1 Pkts

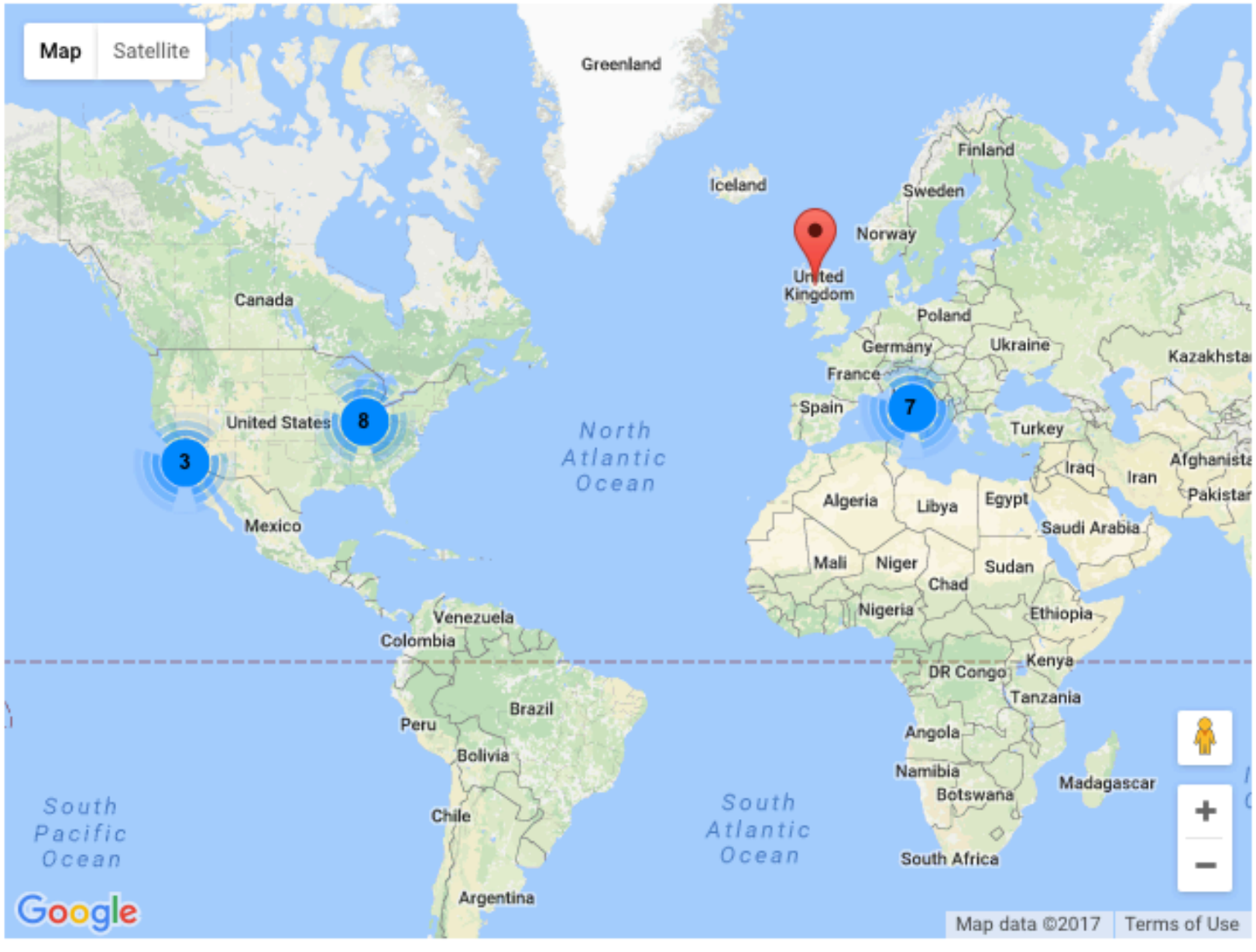
Traffic Geolocation [1/2]

- Traffic geolocation is useful for enforcing security rules. Examples:
  - A child iPad is not supposed to access remote countries outside its domain of knowledge
  - A video-surveillance camera can be accessed only by specific ASs/Countries

- ntopng has the ability to geolocate traffic and emit alerts based on continents (i.e. alert if my PC is accessed any Asia or Oceania)

Traffic Geolocation [2/2]

Hosts GeoMap



Monitoring Copyrighted Content [1/4]

University Toolkit

From Wikipedia, the free encyclopedia

University Toolkit is a software package developed by the MPAA for University system administrators to track and log what types of, and how much, traffic goes through their network, and over the internet provided by the University. The toolkit was available for free at www.universitytoolkit.org until a developer for Ubuntu (the operating system which the toolkit is based on) contacted the MPAA and requested that it be taken down,[1] citing GPL violations, stating that under the GPL, any software must have its source code released under the GPL as well. The MPAA has not released the source code to University Toolkit, despite it being supposedly based entirely on open-source software, specifically snort and ntop.

References [edit]

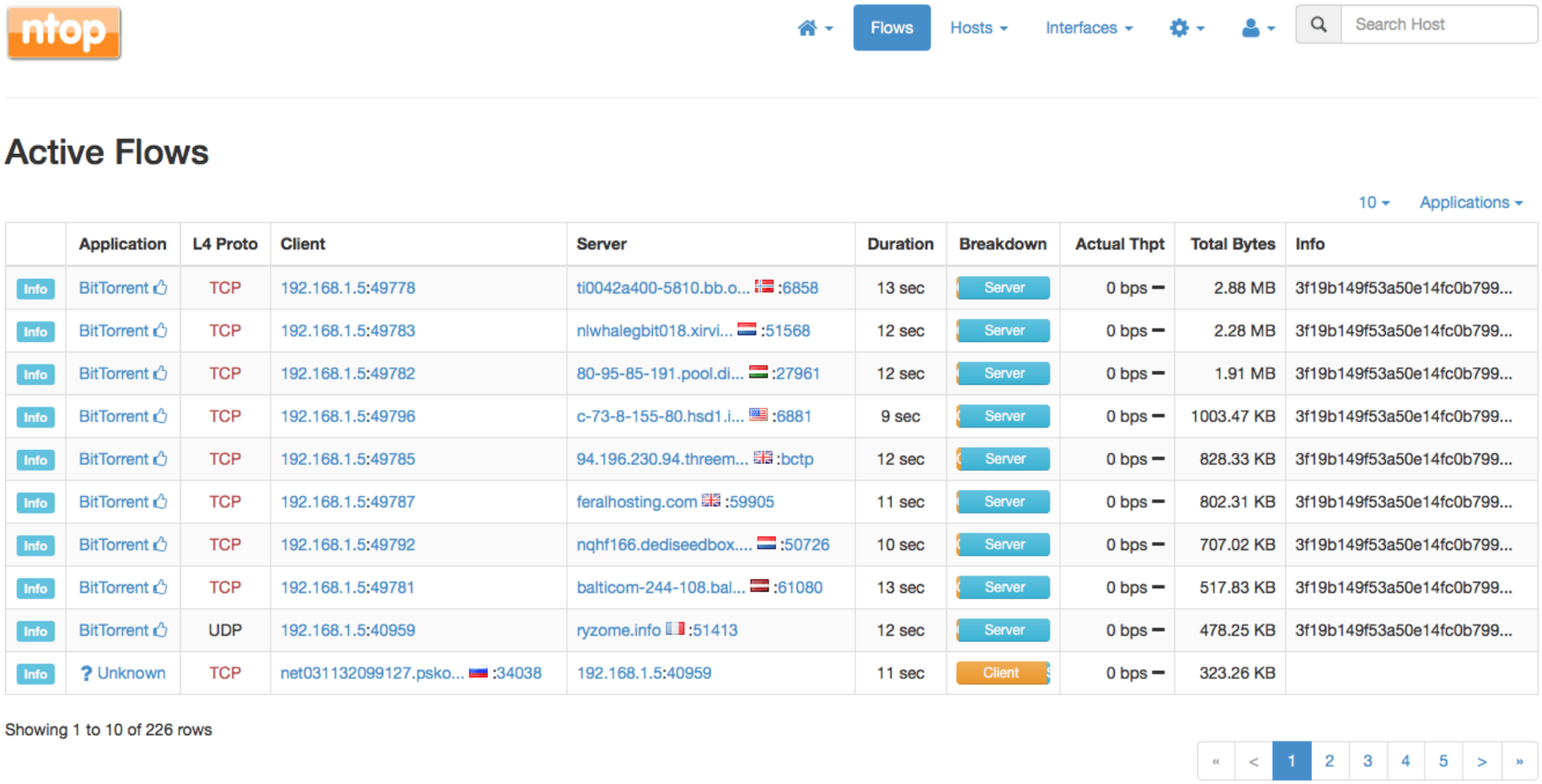
1. ^ mjg59: Spot the difference

External links [edit]

- http://blog.washingtonpost.com/securityfix/2007/11/mpaa_university_toolkit_opens_1.html

Monitoring Copyrighted Content [2/4]

- ntopng has the ability to detect L7 protocols by means of nDPI and thus to detect for instance BitTorrent traffic



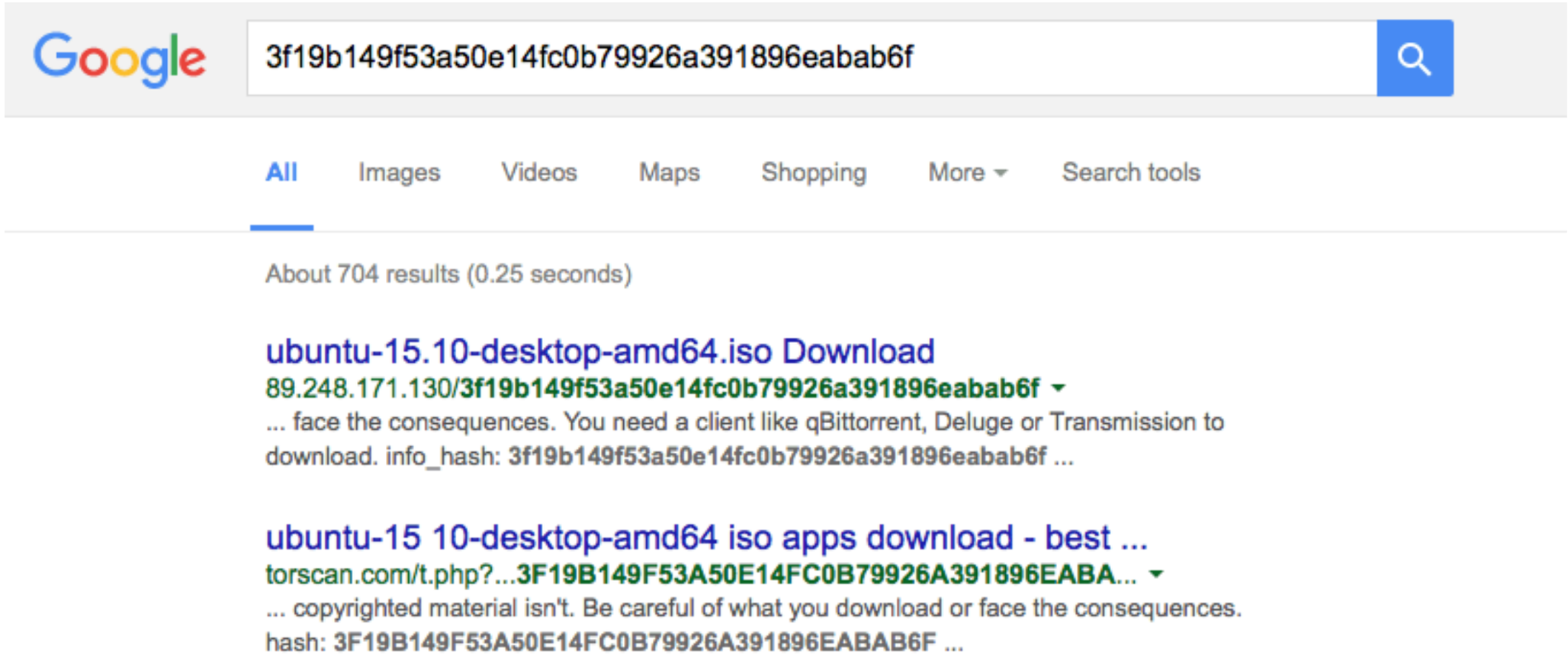
Monitoring Copyrighted Content [3/4]

ntop | Flows | Hosts | Interfaces | Search Host

Flow: 192.168.1.5:40959 ⇄ ryzome.info:51413 | Overview

Flow Peers	192.168.1.5:40959 ⇄ ryzome.info:51413	
Protocol	UDP / BitTorrent (37)	
First / Last Seen	28/02/2016 09:03:49 [18 min, 26 sec ago]	28/02/2016 09:04:01 [18 min, 14 sec ago]
Total Traffic	Total: 478.25 KB	Goodput: 456.56 KB (95.5 %)
Client vs Server Traffic Breakdown	192 ryzome.info:51413	
Client to Server / Server to Client Traffic	185 Pkts / 12.63 KB	344 Pkts / 465.62 KB
Actual / Peak Throughput	0 bps / 0 bps	
BitTorrent hash	3f19b149f53a50e14fc0b79926a391896eabab6f	
Dump Flow Traffic		

Monitoring Copyrighted Content [4/4]



NOTE: This information can be logged onto the database for historical activity tracking.

Unknown vs Unknown

- Unknown traffic does not always mean nDPI needs to be extended to detect a new protocol.
- It can also indicate that there are activities that are worth to be analysed more in detail.

Looking Glass: Unknown Traffic Volume

10 ▾ Criteria ▾ IP Version ▾

Upload Volume
Download Volume
Incoming Flows Count
Outgoing Flows Count

IP Address	VLAN	Alerts	Name	Seen Since	Unknown Traffic Volume	Breakdown	Th	
	0	0		1 h, 43 min, 12 sec	342.8 KB	Rcvd	3	
	0	0		1 h, 43 min, 12 sec	44.83 KB	Sent Rcvd	3	
	0	0		1 h, 42 min, 52 sec	0 B	Sent	5.98 Kbit ↓	3.56 MB
	0	0		1 h, 42 min, 52 sec	0 B	Sent	0 bps ↓	1.52 MB
	0	0		1 h, 42 min, 51 sec	0 B	Sent	540.69 bps ↓	841.73 KB
	0	0		1 h, 42 min, 52 sec	0 B	Sent	0 bps ↓	721.85 KB
	0	0		1 h, 42 min, 51 sec	0 B	Sent	0 bps ↓	1.55 MB
	0	0		1 h, 42 min, 52 sec	0 B	Sent	0 bps ↓	1.54 MB
	0	0		1 h, 42 min, 51 sec	0 B	Sent	0 bps ↓	1.52 MB
	0	0		1 h, 42 min, 51 sec	0 B	Sent	0 bps ↓	1.52 MB

One-way Traffic

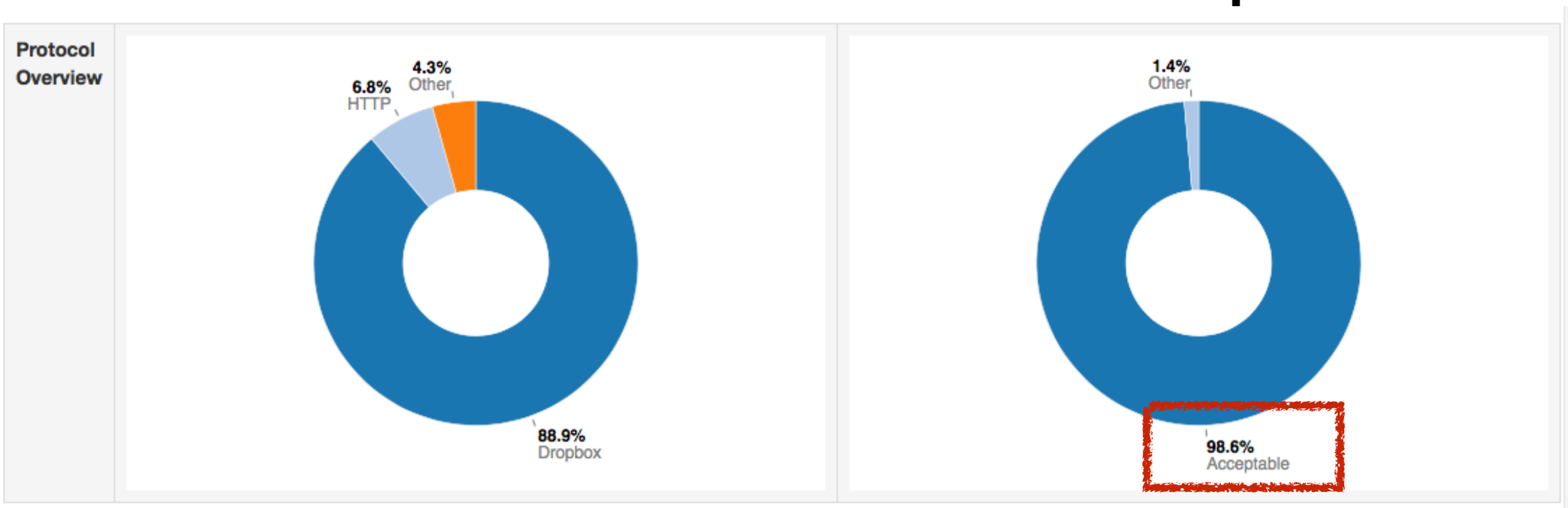
- One way traffic can be a good source of information for understanding suspicious activities based on destination and protocol:
  - Multicast traffic can be exploited for disclosing sensitive information (e.g. SSDP, MDNS)
  - TCP traffic is by nature bi-directional, so one-way TCP flow might indicate activities such as probing or service unavailability.
- The flows menu can display one-way flows and spot these situations.

Suspicious Activities Detection

- nDPI can detect over 200 protocols including those that are considered potentially malicious.
- The list includes protocols such as Tor or even long-term acceptable protocols such as SSH or SSL that in certain scenarios can hide something more dangerous such as a VPN.
- Selecting specific protocols (e.g. TOR) in the flow list and sorting them for duration, can enable this analysis.

Characterising Host Risk Factor [1/2]

- Every host can have a security risk associated, depending on the type and nature of traffic it performs.
- nDPI has the ability to cluster layer-7 protocols in families and thus characterise them up.



Characterising Host Risk Factor [2/2]

- However risks are coming not just from traffic that a host makes, but also from ingress traffic.
- As previously said with one-way traffic, this is a good source of understanding the security risk factor a host has associated.

SIP	0 B	7.06 KB	Rcvd	7.06 KB	0 %
SNMP	4.5 M	MB	Sent Rcvd	8.67 MB	1.54 %
SSH	593.4 KB	11 MB	Sen Rcvd	4.69 MB	0.83 %
SSL	3.26 MB	.17 MB	Sent Rcvd	7.43 MB	1.32 %
Skype	0 B	11.54 KB	Rcvd	11.54 KB	0 %
Tor	37.34 KB	58.7 KB	Sent Rcvd	96.04 KB	0.02 %

What do we need to hide here?

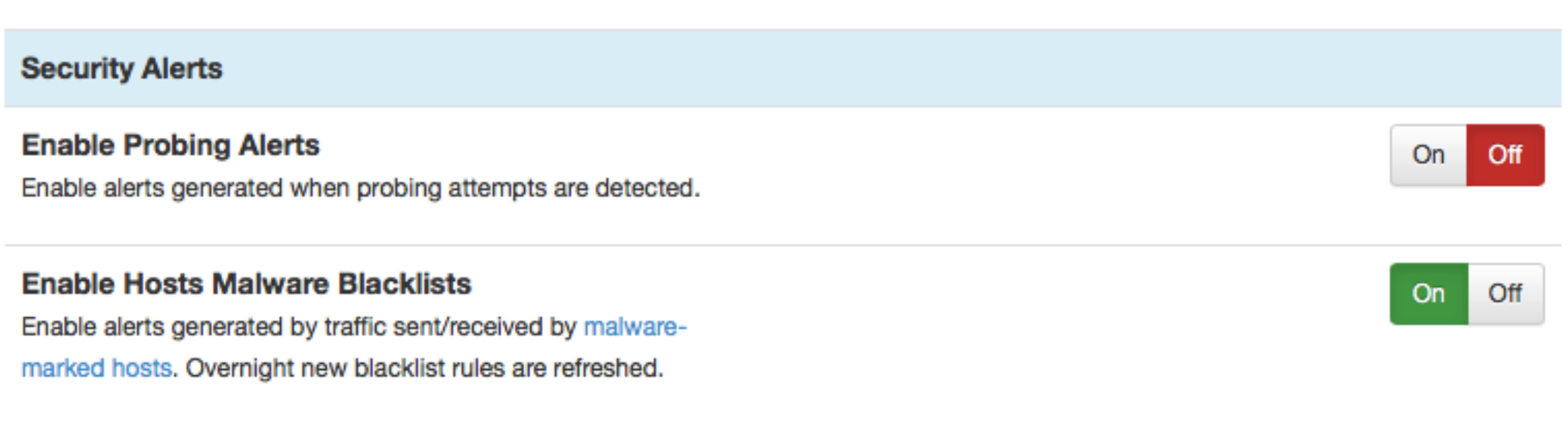
Ingress but no egress traffic: service scan?

Malware Detection [1/3]

- IDSs have been traditionally used to detect security threats but as traffic is becoming more and more encrypted they are falling short.
- A simple way to effectively monitor malware, is by means of IP blacklists.
- You can configure ntopng to do nightly download of malware hosts and enforce them in ntopng.
- If you use ntopng in monitor mode an alert is reported, in inline-mode instead the communication against such hosts are disabled.

Malware Detection [2/3]

- Step 1: Enable Malware hosts detection in preferences.



https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt

- Step 2: See the generated alerts for an overview of malware activities.

Malware Detection [3/3]

Engaged Alerts | Past Alerts | Flow Alerts

Flow Alerts

10 ▾ Type▾ Severity▾

Actions	Date/Time	Severity	Alert Type	Description
	Thu Feb 16 07:39:38 2017	Error	☹ Blacklist Host	blacklisted 71.6.146.185 contacted host [redacted] [TCP 71.6.146.185:49717 > [redacted]:902 [proto: 0.0/Unknown][1/1 pkts][60/54 bytes][SYN ACK RST]]
	Thu Feb 16 08:39:19 2017	Error	☹ Blacklist Host	blacklisted 93.174.93.30 contacted host [redacted] [TCP 93.174.93.30:29162 > [redacted]:5900 [proto: 0.0/Unknown][1/0 pkts][62/0 bytes][SYN]]
	Thu Feb 16 09:01:50 2017	Error	☹ Blacklist Host	blacklisted 185.35.62.185 contacted host [redacted]ri [TCP 185.35.62.185:60205 > [redacted]:1911 [proto: 0.0/Unknown][1/1 pkts][60/54 bytes][SYN ACK RST]]

Engaged Alerts | Past Alerts | Flow Alerts

Past Alerts

10 ▾ Type▾ Severity▾

Actions	Date/Time	Duration	Severity	Alert Type	Description
	Thu Feb 16 07:39:04 2017	-	Error	⊘ Malware Detected	Blacklisted host found 71.6.146.185@0
	Thu Feb 16 08:39:15 2017	-	Error	⊘ Malware Detected	Blacklisted host found 93.174.93.30@0
	Thu Feb 16 09:01:48 2017	-	Error	⊘ Malware Detected	Blacklisted host found 185.35.62.185@0

Characterising User Traffic [1/5]

- Network administrators should not look at user traffic content as this falls outside of their tasks.
- However detecting (and blocking/shaping/setting a quota) specific protocols not suitable for business usage (e.g. Netflix) can be acceptable.
- Cloud-based services such as Google Drive or DropBox can be prohibited in certain environments so network administrators need a way to know what users are doing (not the data content they are exchanging).

Characterising User Traffic [2/5]

- While nDPI is enough for known what hosts are using what protocols…

All Dropbox Hosts

10 ▾ Filter Hosts▾ IP Version▾

IP Address	Location	Flows	Alerts	Name	Seen Since	ASN	Breakdown	Throughput	Traffic
	Local Host	161	0		2 h, 30 min, 8 sec		Rcvd	Rcvd	41.29 Kbit ↓
	Local Host	2	0		2 h, 30 min, 6 sec		Sent	Sent	0 bps –
	Local Host	4	0		2 h, 29 min, 48 sec		Sent	Sent	0 bps ↓

- …inappropriate content (e.g. in schools or public places) cannot be enforced this way as the protocol is generic (e.g. HTTP) but the content is not.

Characterising User Traffic [3/5]

FlashStart
LA PROTEZIONE INTERNET ITALIANA

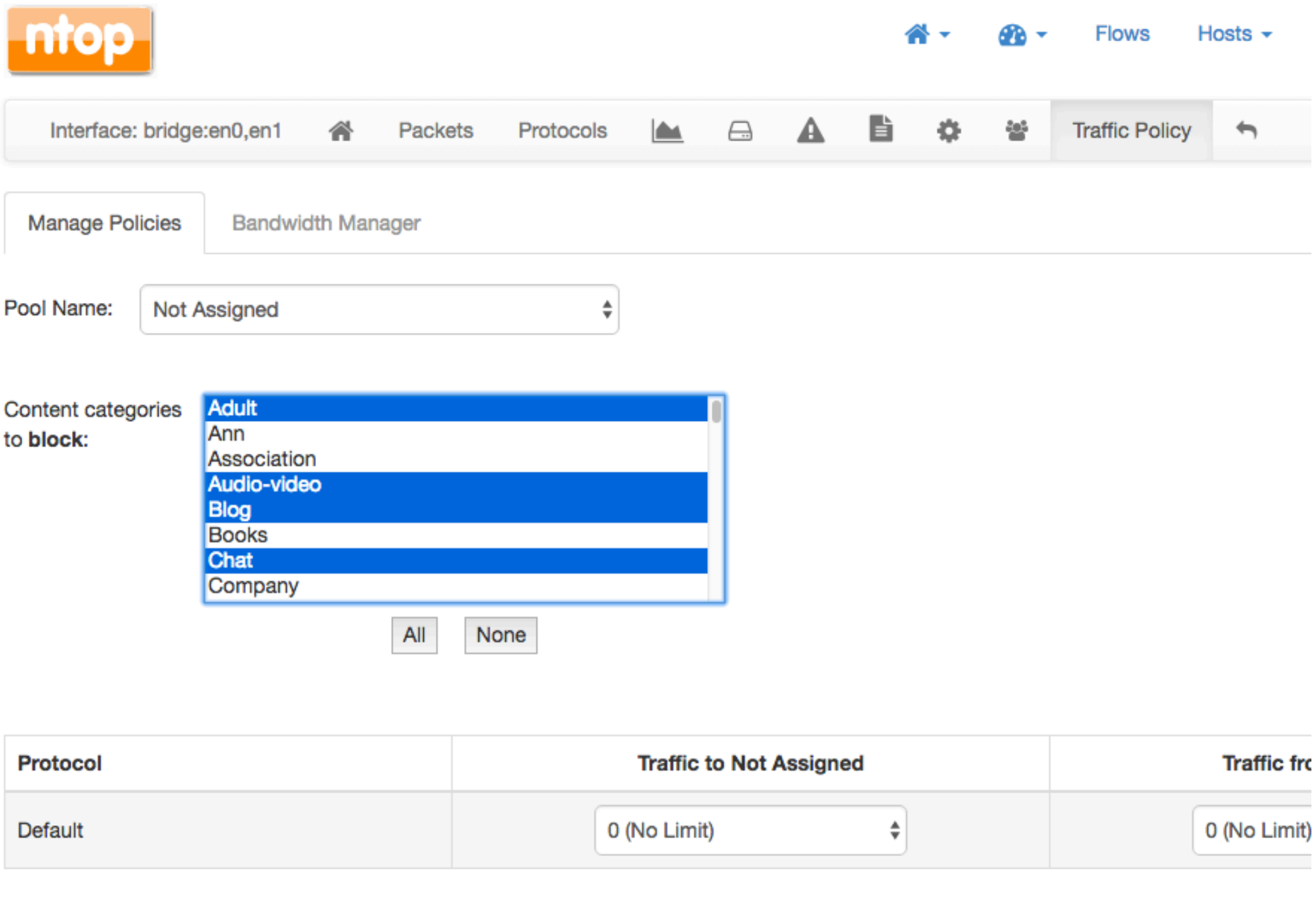
- ntopng has been integrated with a content analysis company to complement layer-7 traffic analysis with content enforcement.
- Go to http://flashstart.ntop.org to get your categorisation key.

Active HTTP Flows

10 Hosts Applications IP Version

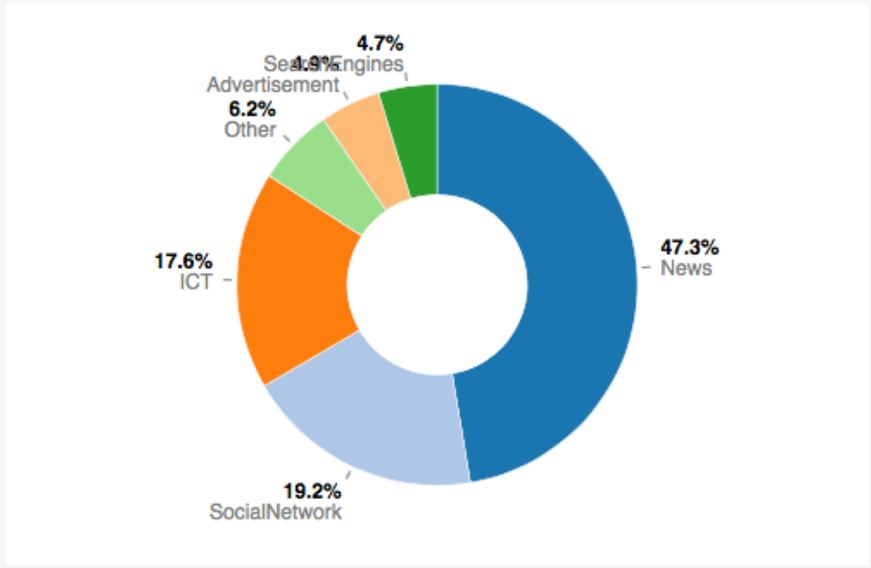
	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	HTTP	TCP	:41620	www.corriere.it:http	2 min, 23 sec	Client Server	0 bps	30.23 KB	/includes2013/SSI/utilit... News
Info	HTTP	TCP	:41618	www.corriere.it:http	2 min, 21 sec	Client Server	0 bps	4.13 KB	/includes_methode/cache/... News
Info	HTTP	TCP	:41616	www.corriere.it:http	2 min, 21 sec	Server	0 bps	33.66 KB	/includes_methode/cache/... News
Info	HTTP	TCP	:36764	images2.corriereobje... :http	2 min, 17 sec	Client	0 bps	4.75 KB	/methode_image/placeh old... ContentServer
Info	HTTP	TCP	:60492	static2.vivimilano.c... :http	2 min, 15 sec	Client	0 bps	2.46 KB	/wp-content/uploads/20 7... News
Info	HTTP	TCP	:60494	static2.vivimilano.c... :http	2 min, 15 sec	Client	0 bps	2.47 KB	/wp-content/uploads/20 7... News
Info	HTTP	TCP	:36838	images2.corriereobje... :http	2 min, 15 sec	Client	0 bps	1.59 KB	/includes2013/LIBS/css a... ContentServer
Info	HTTP	TCP	:60490	static2.vivimilano.c... :http	2 min, 15 sec	Client	0 bps	2.46 KB	/wp-content/uploads/20 7... News
Info	HTTP	TCP	:60496	xml2.corriereobjects... :http	2 min, 15 sec	Client	0 bps	1.62 KB	/tools/3a-col-nav/tablet... ContentServer
Info	HTTP	TCP	:60488	static2.vivimilano.c... :http	2 min, 15 sec	Client	0 bps	2.44 KB	/wp-content/uploads/20 7... News

Characterising User Traffic [4/5]



Characterising User Traffic [5/5]

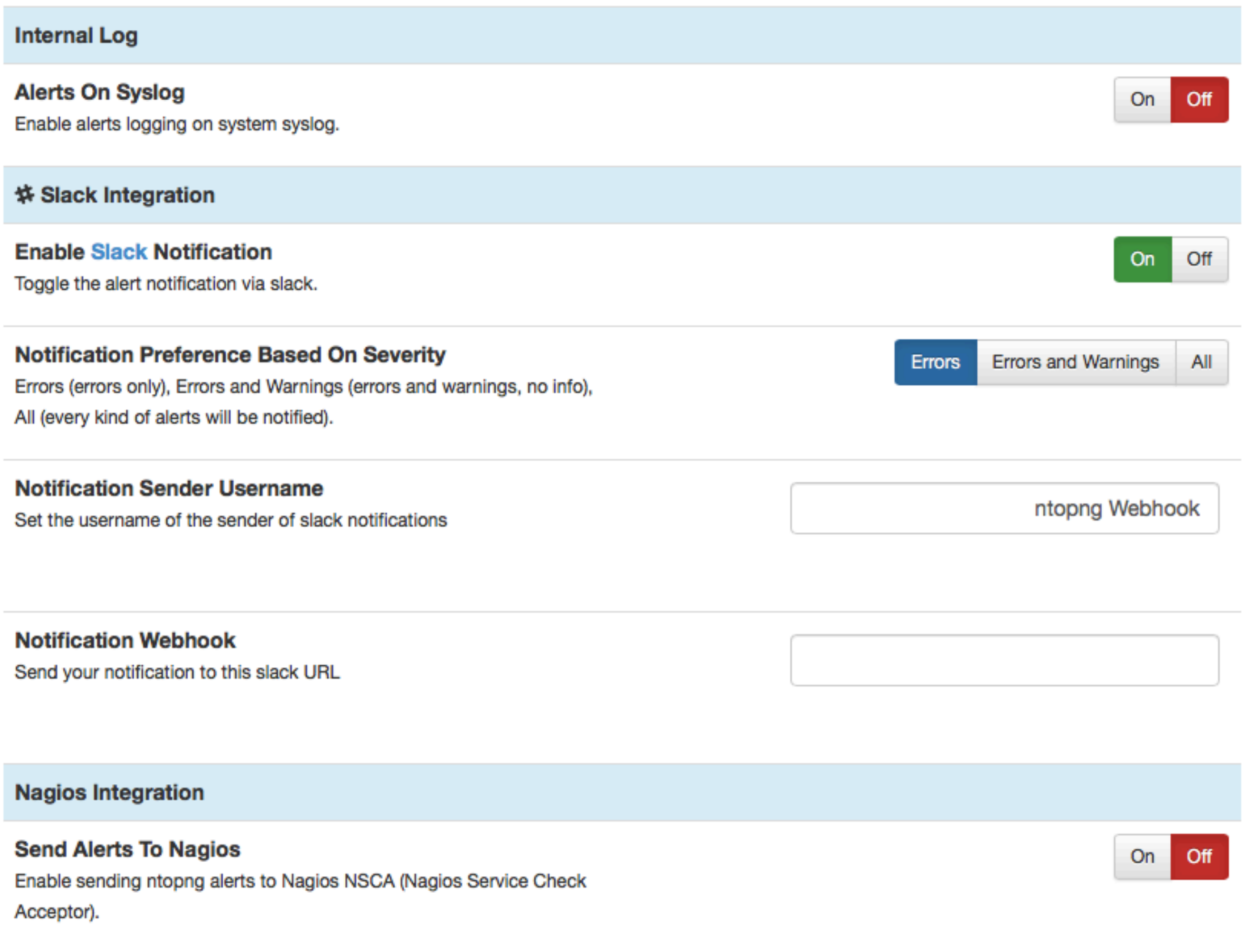
Traffic Categories



10

Traffic Category	Traffic Volume	Traffic %
News	41.77 KB	50.35%
SocialNetwork	17.04 KB	20.54%
ICT	10.58 KB	12.75%
Advertisement	4.2 KB	5.06%
SearchEngines	3.8 KB	4.58%
FreeTime	3.46 KB	4.17%
Webstat	1.79 KB	2.16%
AudioVideo	336 B	0.4%

Alarms On The Go



Conclusions

- Traffic flow analysis and extraction of metadata information are the cornerstones of network security analysis.
- ntopng is able to provide insights not just for traffic monitoring but also from the security viewpoint.
- The nDPI engine allows traffic to be properly classified and bound to applications.
- Traffic categorization allows traffic patterns to be built not just for tagging traffic but also for malware analysis.