Network Traffic and Security Monitoring Using ntopng

Luca Deri <deri@ntop.org>
@lucaderi

Outlook

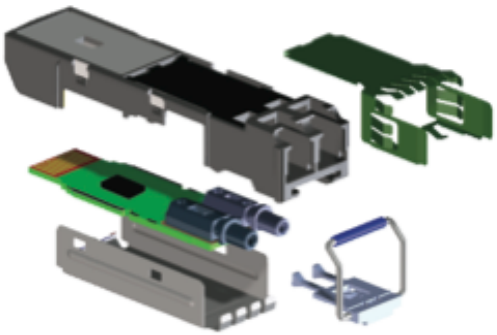
- What are the main activities of ntop.org ?
- ntop's view on network monitoring.
- From ntop to ntopng.
- ntopng architecture and design.
- ntopng as a flow collector
- Exploring system activities using ntopng
- Using ntopng.
- Advanced monitoring with ntopng.
- Future roadmap items.

About ntop.org [1/2]

- ntop develops of open source network traffic monitoring applications.
- ntop (circa 1998) is the first app we released and it is a web-based network monitoring application.
- Today our products range from traffic monitoring, high-speed packet processing, deep-packet inspection, and IDS/IPS acceleration (snort and suricata).

About ntop.org [2/2]

- Our software is powering many commercial products...



Integrated ASIC with JDSU technology

ntop Goals

- Provide better, yet price effective, traffic monitoring solution by enabling users to have increased traffic visibility.
- Go beyond standard metrics and increase traffic visibility by analysing key protocols in detail.
- Promote open-source software, while protecting selected IPRs.
- All commercial ntop tools are available at no cost for research and education.

ntop's Approach to Traffic Monitoring

- Ability to capture, process and (optionally) transmit traffic at line rate, any packet size.
- Leverage on modern multi-core/NUMA architectures in order to promote scalability.
- Use commodity hardware for producing affordable, long-living (no vendor lock), scalable (use new hardware by the time it is becoming available) monitoring solutions.
- Use open-source to spread the software, and let the community test it on unchartered places.

Motivation For Traffic Monitoring

If you can not measure it,
you can not improve it

Lord Kelvin

What Happens in Our Network?

- Do we have control over our network?
- It's not possible to imagine a healthy network without a clear understanding of traffic flowing on our network.
- Knowledge is the first step towards evaluation of potential network security issues.
- Event correlation can provide us timely information bout our network health.

Packets Never Lie

- Packet analysis provide useful information for understanding:
  - Network traffic issues.
  - Network usage not compliant with network policies (note: firewalls cannot help here).
  - Performances less than expected.
  - Potential security flaws.
  - Ongoing (latent) attacks.
  - Data breach

Before We Start: ntopng Installation

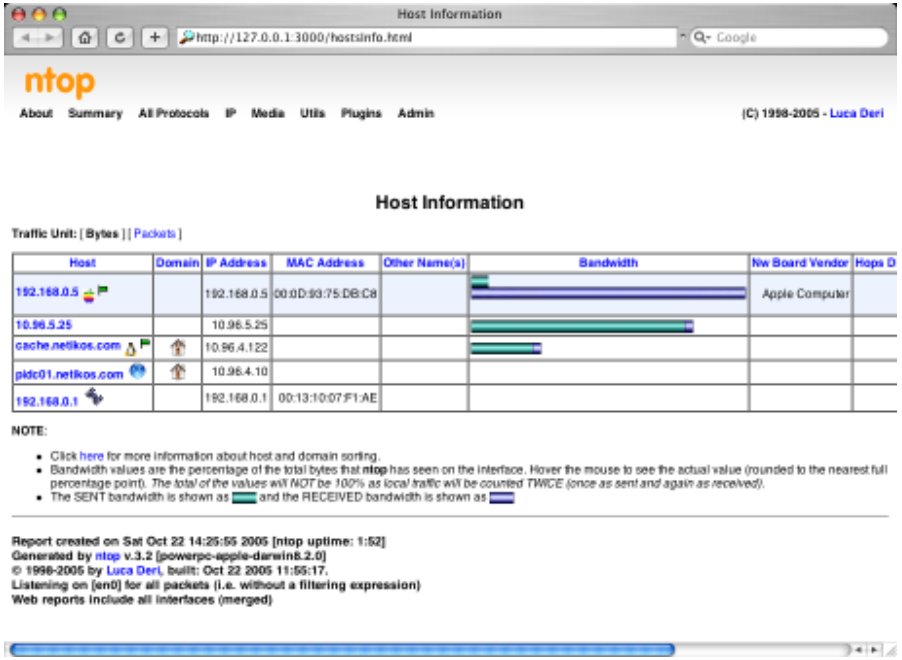
- Source code
  https://github.com/ntop/ntopng

- Distributions
  Ubuntu/Debian, FreeBSD…. (included in the distro)
  OSX (brew)

- Binary Packages (nightly)
  http://packages.ntop.org (Debian/Ubuntu/CentOS, OSX, RaspberryPI/ARM)

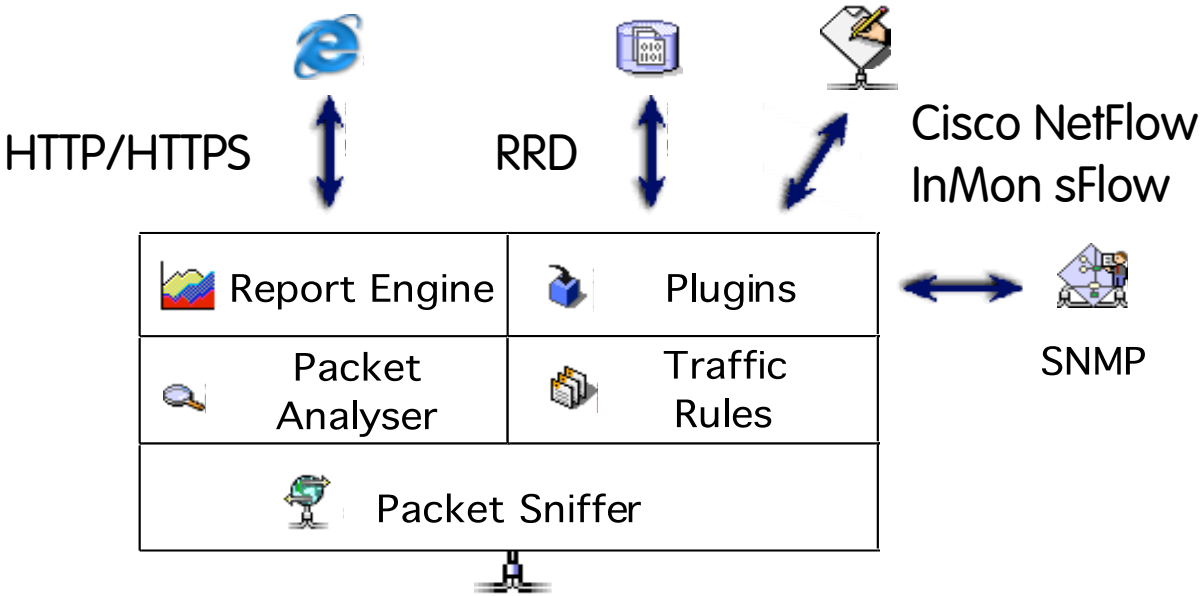
Some History

- 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.

ntop Architecture

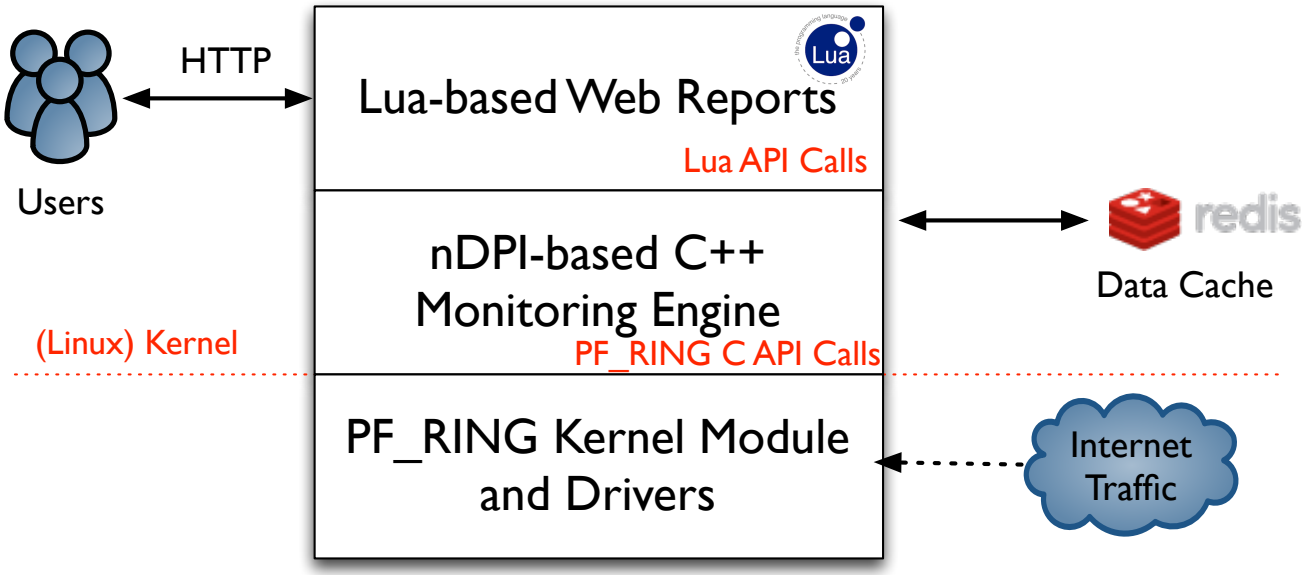


ntopng Design Goals

- Clean separation between the monitoring engine and the reporting facilities.
- Robust, crash-free engine (ntop was not really so).
- Platform scriptability for enabling extensions or changes at runtime without restart.
- Realtime: most monitoring tools aggregate data (5 mins usually) and present it when it's too late.
- Many new features including HTML 5-based dynamic GUI, categorisation, DPI.

ntopng Architecture

- Three different and self-contained components, communicating with clean API calls.



ntopng Monitoring Engine

- Coded in C++ and based the concept of flow (set of packets with the same 6-tuple).
- Flows are inspected with a home-grown DPI-library named nDPI aiming to discover the "real" application protocol (no ports are used).
- Information is clustered per:
  - (Capture) Network Device
  - Flow
  - Host

Local vs Remote Hosts [1/2]

- ntopng keeps information in memory at different level of accuracy in order to save resources for hosts that are not "too relevant".
- For this reason at startup hosts are divided in:
  - Local hosts
    The local host where ntopng is running as well the hosts belonging to some "privileged" IPv4/v6 networks. These hosts are very relevant and thus ntopng keep full statistics.
  - Remote hosts
    Non-local hosts for which we keep a minimum level of detail.

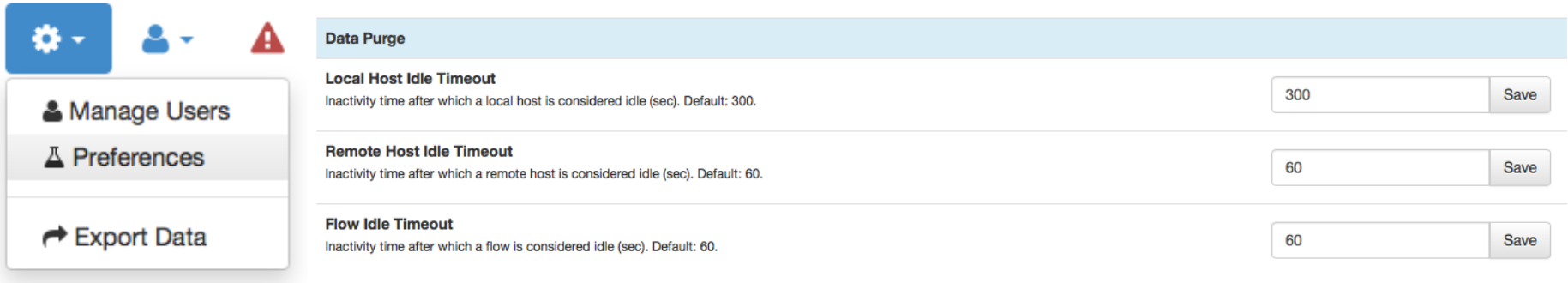
Local vs Remote Hosts [2/2]

- For local hosts (unless disabled via preferences) are kept all L7 protocol statistics, as well basic statistics (e.g. bytes/packets in/out).
- No persistent statistics are saved on disk.
- A system host is the host where ntopng is running and it is automatically considered local as well the networks of its ethernet interfaces.

IP Address	192.12.193.11 [192.12.193.11/32] [Pisa]
ASN	2597 [Registry of ccTLD it - IIT-CNR]
Name	pc-deri.nic.it Local System

Information Lifecycle

- ntopng keeps in memory live information such as flows and hosts statistics.
- As the memory cannot be infinite, periodically non-recent information is harvested.
- Users can specify preferences for data purge:

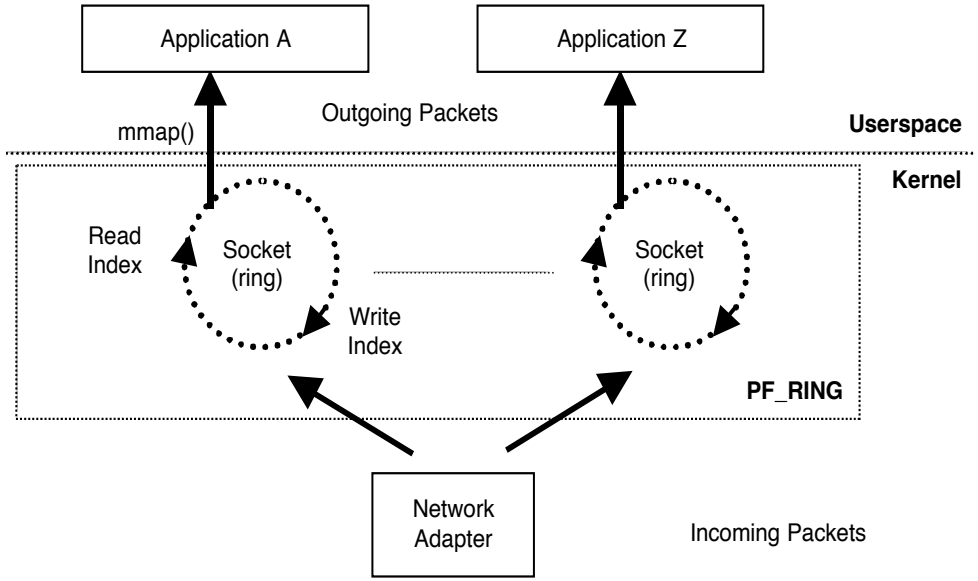


Packet Processing Journey

1. Packet capture: PF_RING (Linux) or libpcap.
2. Packet decoding: no IP traffic is accounted.
3. IPv4/v6 Traffic only:
   - Map the packet to a 6-tuple flow and increment stats.
   - Identify source/destination hosts and increment stats.
   - Use nDPI to identify the flow application protocol
     - UDP flows are identified in no more than 2 packets.
     - TCP Flows can be identified in up to 15 packets in total, otherwise the flow is marked as "Unknown".
4. Move to the next packet.

PF_RING [1/2]

- In 2004 we realised the the Linux kernel was not efficient enough to fulfil our packet capture requirements and thus we have written a in-kernel circular buffer named PF_RING.

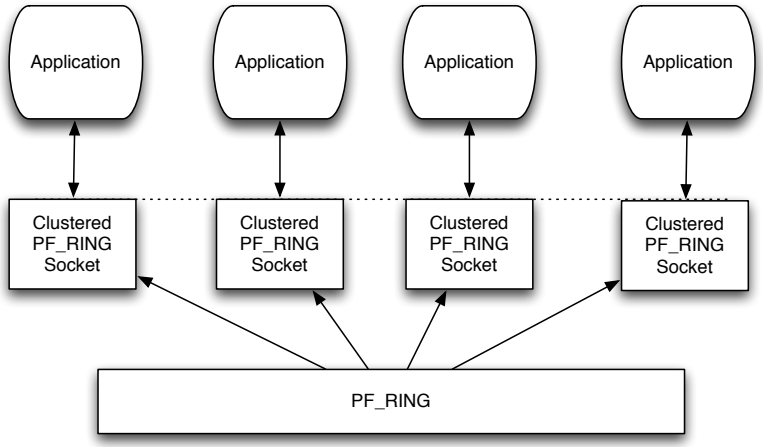


PF_RING [2/2]

- It creates a straight path for incoming packets accessed from user-space applications with memory mapping.
- No need to use custom network cards: any card is supported.
- Transparent to applications: legacy applications need to be recompiled in order to use it (pcap-over-PF_RING).
- Developers familiar with network applications can immediately take advantage of it without having to learn new APIs.
- Acceleration support for many popular open-source applications including Wireshark, Suricata and Snort.

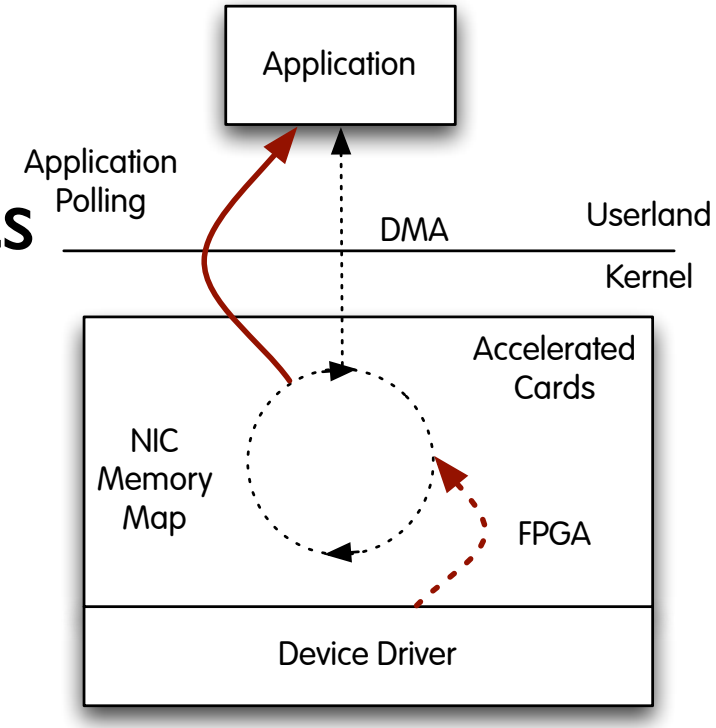
Balancing Traffic with PF_RING

- At high speed on modern multi-core systems, it is a good idea to improve the overall system performance by balancing traffic across cores.
- PF_RING shares ingress packets across multiple consumer applications (e.g. ntopng) by hashing them (tunnels are supported) so that they are balanced to multiple consumer applications via virtual PF_RING network interfaces.



Moving towards 10 Gbit and above [1/2]

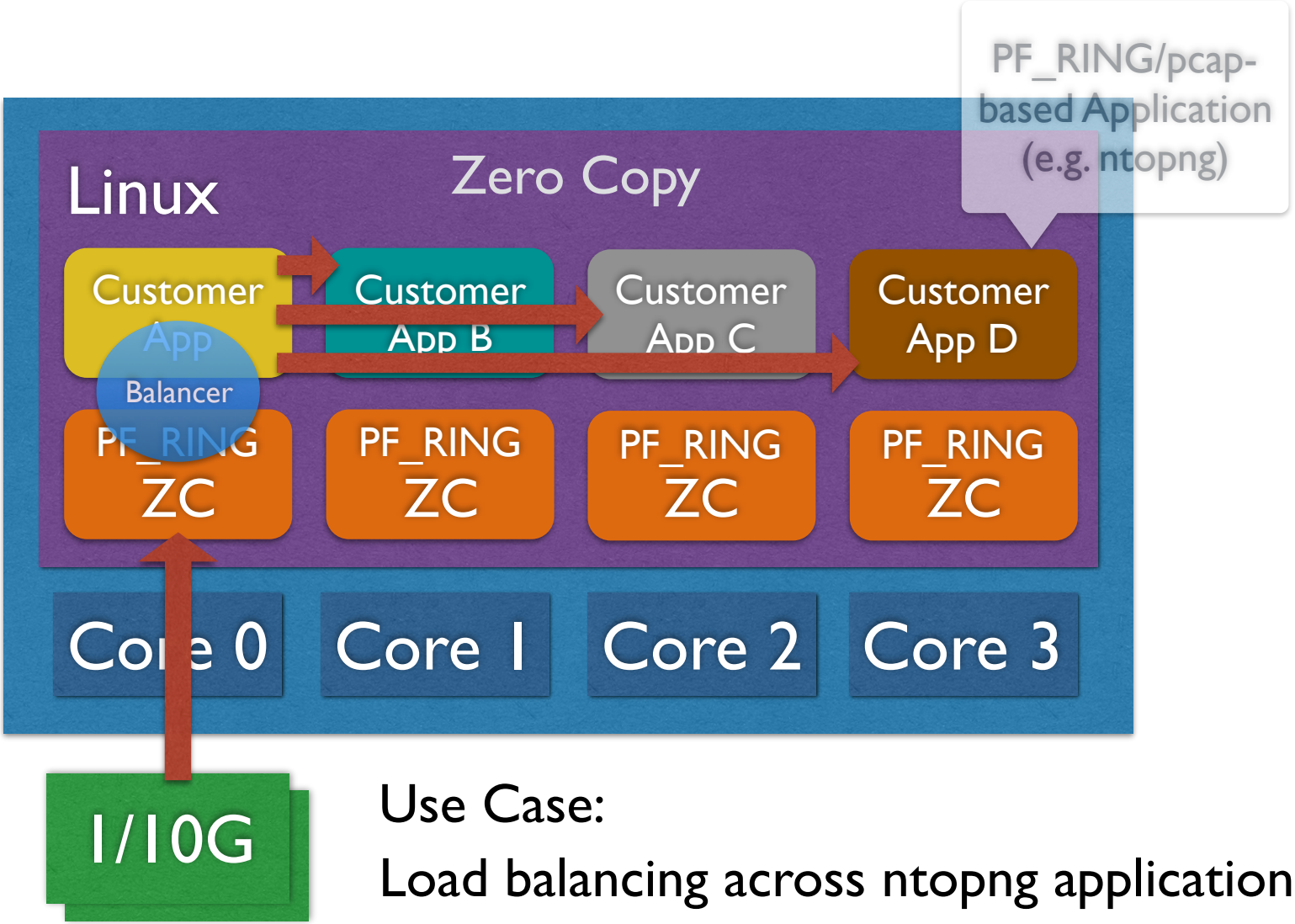
- The original PF_RING is a good solution up to 3/5 Gbit but not above as the cost of packet copy into the ring is overkilling.
- PF_RING ZC (Zero Copy) is an extension that allows packets to be received/transmitted in zero copy similar to what FPGA-accelerated cards (e.g. Napatech) do in hardware.



Moving towards 10 Gbit and above [2/2]

- In ZC a packet is put by the ingress NIC into a shared memory buffer, and it hop across applications (and VMs) by exchanging the buffer pointer (packets don't move).
- Thanks to this solution it is possible to create arbitrary packet processing topologies at multi-10 Gbit line rate using commodity hardware x86 servers and adapters (ZC natively supports Intel ethernet adapters).

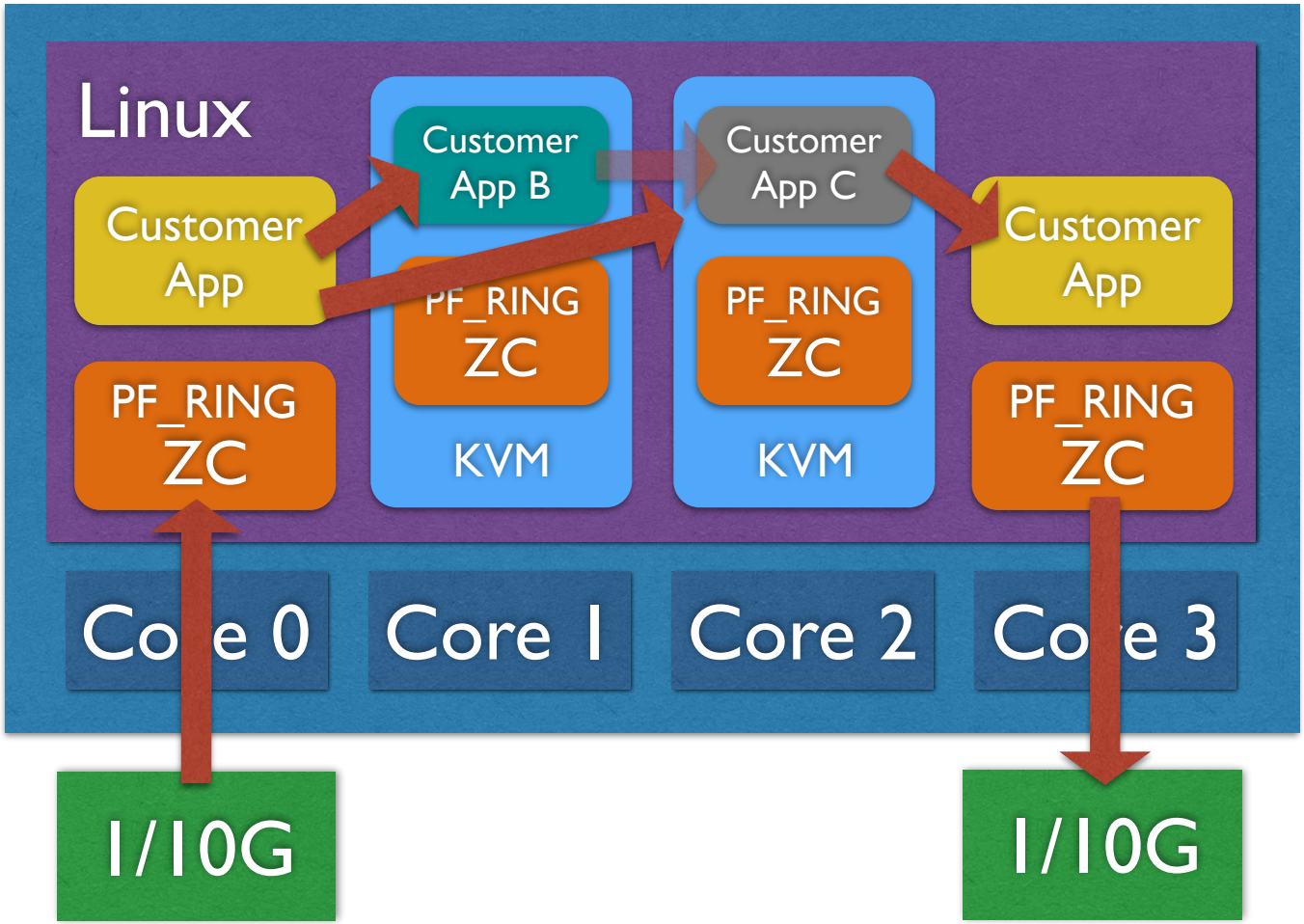
PF_RING ZC Network Topologies [1/2]



Use Case:

Load balancing across ntopng applications.

PF_RING ZC Network Topologies [2/2]



Use Case:

Application pipeline or run multiple apps (e.g. ntopng) in VMs to insulate them.

PF_RING (ZC) and ntopng

- Using PF_RING (ZC) with ntopng has several benefits:
  - ntopng can scale to 10 Gbit and above by spawning several ntopng instances each bound to a (few) core(s).
  - It is possible to send the same packet to multiple apps. For instance it is possible to send the same packet to ntopng (for accounting purposes) and n2disk (ntop's application for dumping packet-to-disk at multi-10G) and/or and IDS (e.g. Suricata and snort).

The need for DPI in Monitoring [1/2]

- Limit traffic analysis at packet header level it is no longer enough (nor cool).
- Network administrators want to know the real protocol without relying on the port being used.
- Selected protocols can be "precisely dissected" (e.g. HTTP) in order to extract information, but on the rest of the traffic it is necessary to tell network administrators what is the protocol flowing in their network.

The need for DPI in Monitoring [2/2]

- DPI (Deep Packet Inspection) is a technique for inspecting the packet payload for the purpose of extracting metadata (e.g. protocol).
- There are many DPI toolkits available but they are not what we looked for as:
  - They are proprietary (you need to sign an NDA to use them), and costly for both purchase and maintenance.
  - Adding a new protocol requires vendor support (i.e. it has a high cost and might need time until the vendor supports it) = you're locked-in.
- On a nutshell DPI is a requirement but the market does not offer an alternative for open-source.

Say hello to nDPI

- ntop has decided to develop its own GPL DPI toolkit in order to build an open DPI layer for ntop and third party applications.
- Supported protocols (> 220) 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)

nDPI Overview

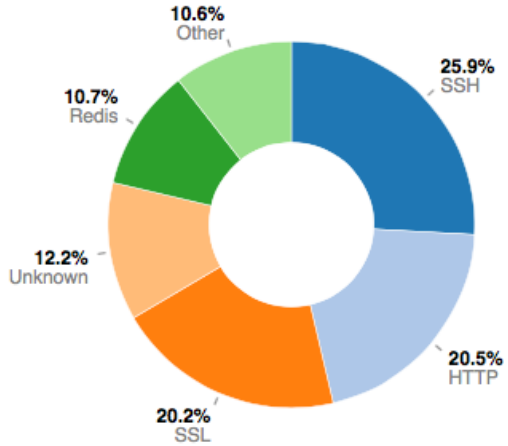
- Portable C library (Win and Unix, 32/64 bit).
- Designed for user and kernel space
  - Linux ndpi-netfilter implements L7 kernel filters
- Used by many non-ntop projects (eg. xplico.org) and part of Linux distributions (e.g. Debian).
- Able to operate on both plain ethernet traffic and encapsulated (e.g. GTP, GRE…).
- Ability to specify at runtime custom protocols (port or hostname - dns, http, https -based).

nDPI on ntopng

- In ntopng all flows are analysed through nDPI to associate an application protocol to them.
- L7 statistics are available per flow, host, and interface (from which monitoring data is received).
- For network interfaces and local hosts, nDPI statistics are saved persistently to disk (in RRD format).

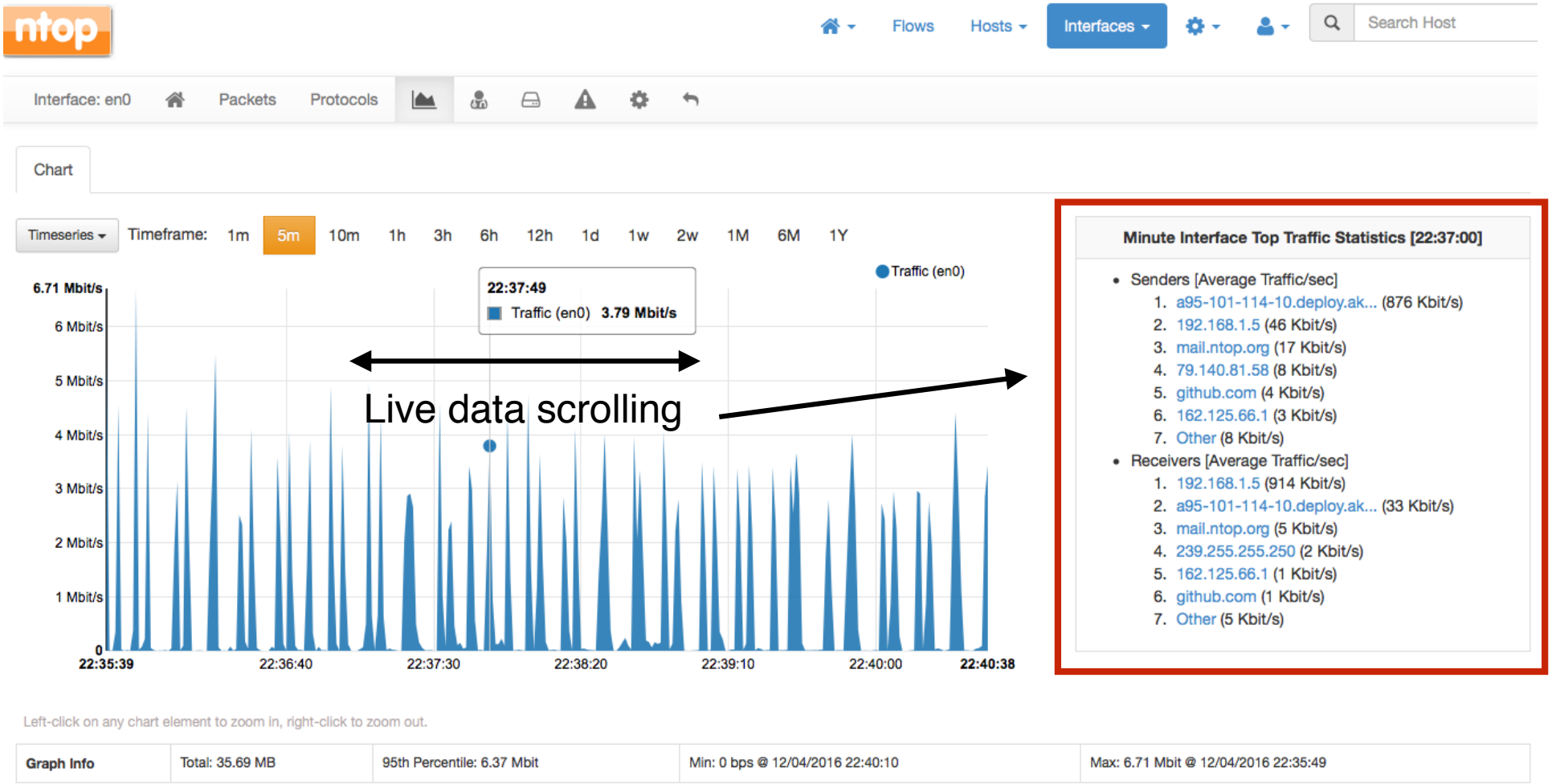
nDPI on ntopng: Interface Report [1/2]

Protocol Overview



Application Protocol	Total (Since Startup)	Percentage
Apple	17.94 KB	0 %
BitTorrent	90.59 KB	0 %
CiscoVPN	560 Bytes	0 %
DCE_RPC	2.65 KB	0 %
DHCP	1.09 MB	0 %
DHCPV6	3.38 KB	0 %

nDPI on ntopng: Interface Report [2/2]



ntopng and Redis [1/2]

- Redis is an open source key-value in-memory database.
- ntop uses it to cache data such as:
  - Configuration and user preferences information.
  - DNS name resolution (numeric to symbolic).
  - Volatile monitoring data (e.g. hosts JSON representation).
- Some information is persistent (e.g. preferences) and some is volatile: ntopng can tell redis how long a given value must be kept in cache.

ntopng and Redis [2/2]

- Redis is also used as a (persistent) queue for requests towards external applications.
  - If configured (-F command line option), periodically flow status is saved onto a redis queue, requests are packed, and send to a remote BigData system.

- In essence Redis is used by ntopng to store information that might take too much memory (if kept on ntopng memory space), or to pile up list of things that are executed periodically or that require interaction with remote applications that might be slow or temporary unavailable.

Lua-based ntopng Scriptability [1/3]

- A design principle of ntopng has been the clean separation of the GUI from engine (in ntop it was all mixed).
- This means that ntopng can (also) be used (via HTTP) to feed data into third party apps such as Nagios or OpenNMS.
- All data export from the engine happens via Lua.
- Lua methods invoke the ntopng C++ API in order to interact with the monitoring engine.

Lua-based ntopng Scriptability [2/3]

- `/scripts/callback/` scripts are executed periodically to perform specific actions.
- `/scripts/lua/` scripts are executed only by the web GUI.
- Example: `http://ntopng:3000/lua/flow_stats.lua`

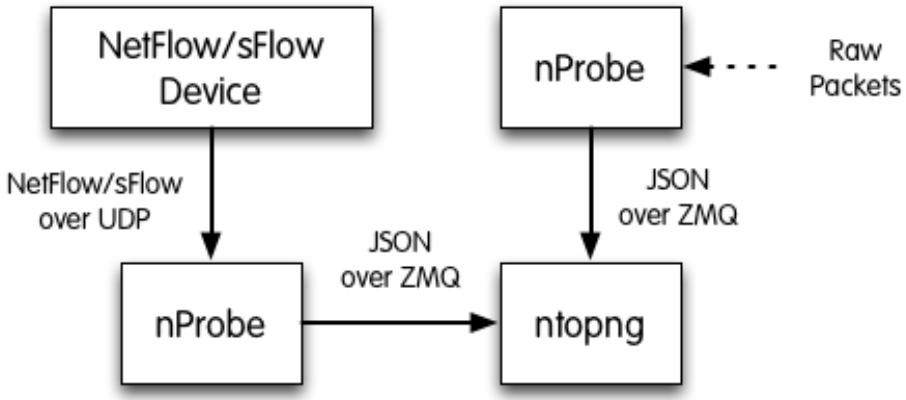
Name	Date Modified	Size
callbacks	Sep 30, 2013 2:15 PM	--
daily.lua	Apr 17, 2013 1:55 PM	29 bytes
hourly.lua	Apr 17, 2013 1:55 PM	29 bytes
minute.lua	Sep 30, 2013 2:15 PM	5 KB
nprobe-collector.lua	Sep 30, 2013 2:15 PM	4 KB
second.lua	Sep 30, 2013 2:15 PM	2 KB
lua	Today 3:58 PM	--
about.lua	Jun 30, 2013 10:27 PM	2 KB
admin	Jun 26, 2013 11:24 PM	--
aggregated_host_details.lua	Sep 30, 2013 2:15 PM	6 KB
aggregated_host_stats.lua	Aug 15, 2013 4:37 PM	442 bytes
aggregated_hosts_stats.lua	Sep 30, 2013 2:15 PM	1 KB
db.lua	Aug 12, 2013 7:48 PM	320 bytes
do_export_data.lua	Sep 30, 2013 2:15 PM	765 bytes
export_data.lua	Sep 4, 2013 7:49 PM	1 KB
find_host.lua	Sep 4, 2013 7:49 PM	2 KB
flow_details.lua	Sep 30, 2013 2:15 PM	7 KB
flow_stats.lua	Aug 15, 2013 4:37 PM	1 KB
flows_stats.lua	Aug 15, 2013 4:37 PM	2 KB
get_aggregated_host_info.lua	Aug 15, 2013 4:37 PM	857 bytes
get_flows_data.lua	Sep 4, 2013 7:49 PM	6 KB
get_geo_hosts.lua	Sep 4, 2013 7:49 PM	2 KB
get_host_activitymap.lua	Sep 30, 2013 2:15 PM	505 bytes
get_host_traffic.lua	Sep 4, 2013 7:49 PM	399 bytes
get_hosts_data.lua	Sep 30, 2013 2:15 PM	6 KB
get_hosts_interaction.lua	Sep 30, 2013 2:15 PM	2 KB

Lua-based ntopng Scriptability [3/3]

- ntopng defines (in C++) two Lua classes:
  - `interface`
    - Hook to objects that describe flows and hosts.
    - Access to live monitoring data.
  - `ntop`
    - General functions used to interact with ntopng configuration.
- Lua objects are usually in "read-only" mode
  - C++ sets their data, Lua reads data (e.g. `host.name`).
  - Some Lua methods (e.g. `interface.restoreHost()`) can however modify the information stored in the engine.

ntopng as a NetFlow/sFlow Collector [1/3]

- The "old" ntop included a NetFlow/sFlow collector. Considered the effort required to support all the various NetFlow dialects (e.g. Cisco ASA flows are not "really" flows), in ntopng we have made a different design choice.



ntopng as a NetFlow/sFlow Collector [2/3]

- nProbe (a home-grown NetFlow/sFlow collector/probe) is responsible for collecting/generating flows and convert them to JSON so that ntopng can understand it.
- The communication ntopng <-> nProbe is over ØMQ a simple/fast messaging system that allows the two peers to be decoupled while:
  - Avoiding "fat" communication protocols such as HTTP.
  - Relying on a system that works per message (no per packet) and handles automatic reconnection if necessary.

ntopng as a NetFlow/sFlow Collector [3/3]

Flows are sent in the following format (gzip+encryption)

- {“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}
- Where:
  - “<Element ID>”: <value> (example 8 = IPV4_SRC_ADDR)

- Contrary to what happens in NetFlow/sFlow ntopng (collector) connects to nProbe (probe) and fetches the emitted flows. Multiple collectors can connect to the same probe. No traffic is created when no collector is attached to the probe.

Flow Collection Setup: an Example

Flow collection/generation (nProbe)

- Probe mode

```
nprobe --zmq "tcp://*:5556" -i eth1 -n
none
```

- sFlow/NetFlow collector mode

```
nprobe --zmq "tcp://*:5556" -i none -n
none --collector-port 2055
```

Data Collector (ntopng)

- `ntopng -i tcp://127.0.0.1:5556`

Flow Collection: Pull vs Poll Mode

- Poll Mode
  - host X> ntopng -i "tcp://Y:1234" --zmq-encrypt-pwd myencryptionkey
  - host Y> nprobe -n none --zmq "tcp://*:1234" --zmq-encrypt-pwd myencryptionkey

- Push Mode
  - host X> ntopng -i "tcp://Y:1234" --zmq-collector-mode --zmq-encrypt-pwd myencryptionkey
  - host Y> nprobe -n none --zmq "tcp://*:1234" --zmq-probe-mode --zmq-encrypt-pwd myencryptionkey

SNMP and Flow Collection [1/4]

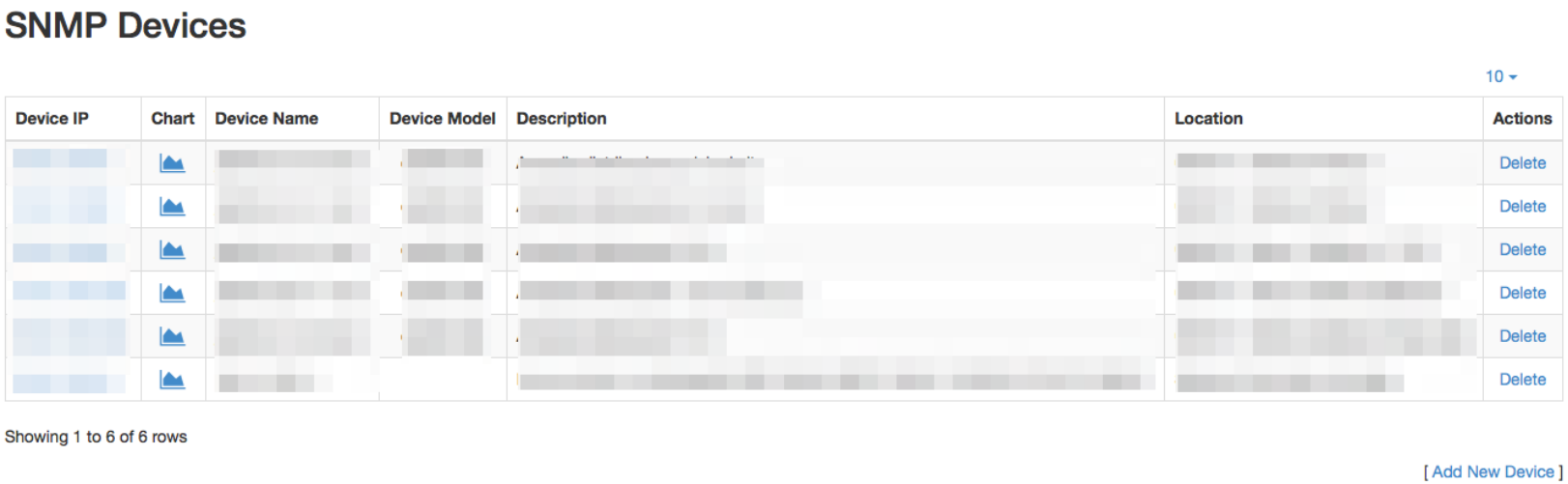
- ntopng allows SNMP MIBs to be queried (MIB-II and Bridge MIB)

Description	[redacted]
ObjectID	1.3.6.1.4.1.8072.3.2.10
Uptime	1 day, 17 h, 58 min, 14 sec
Contact	Me
Name	[redacted]
Location	Sitting on the Dock of the Bay

Interface Index	Chart	Name	Type	MTU	Speed	Mac Address	Status	In Bytes	Out Bytes	In Discards	Port MACs	Last Change
1		lo	softwareLoopback		10 Mbit		Up	1.17 GB	1.17 GB			
2		Intel Corporation Ethern...	ethernetCsmacd	1500	1 Gbit	64:00:6A:63:35:CC	Up	269.12 MB	1.51 GB			
3	-	Intel Corporation 82540E...	ethernetCsmacd	1500		00:0E:0C:2C:0B:B4	Down					
4	-	docker0	ethernetCsmacd	1500		02:42:97:B3:2F:EA	Down					
5		as0t0	other	1500			Up	0 B	832 B			
6		virbr0	ethernetCsmacd	1500		FE:54:00:57:7C:58	Up	1.24 GB	1.35 GB			
7	-	virbr0-nic	ethernetCsmacd	1500		52:54:00:25:C9:88	Down					
11		vnet0	ethernetCsmacd	1500	10 Mbit	FE:54:00:57:7C:58	Up	1.29 GB	1.37 GB			

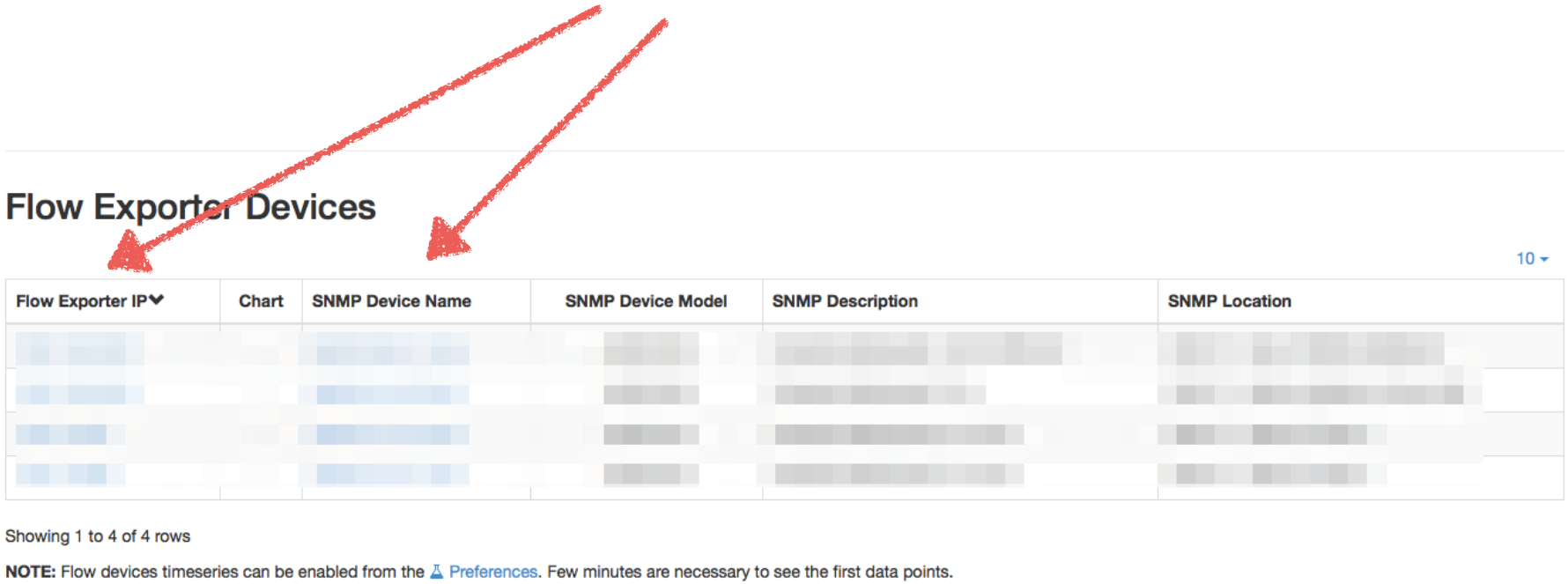
SNMP and Flow Collection [2/4]

- Both NetFlow and sFlow can be glued to SNMP through the InterfaceId
- All necessary is to do, is to define in the SNMP menu the IP address and community of the SNMP-enabled devices



SNMP and Flow Collection [3/4]

- ntopng for each flow exporter device is able to detect if there is a corresponding SNMP device configured and glue them up.



SNMP and Flow Collection [4/4]

- With sFlow there is no need to have SNMP enabled as ntopng is able to collect counter values via ZMQ.
- With NetFlow counters are created accumulating interface values

Flow/SNMP Ratio

Flow Device [redacted]

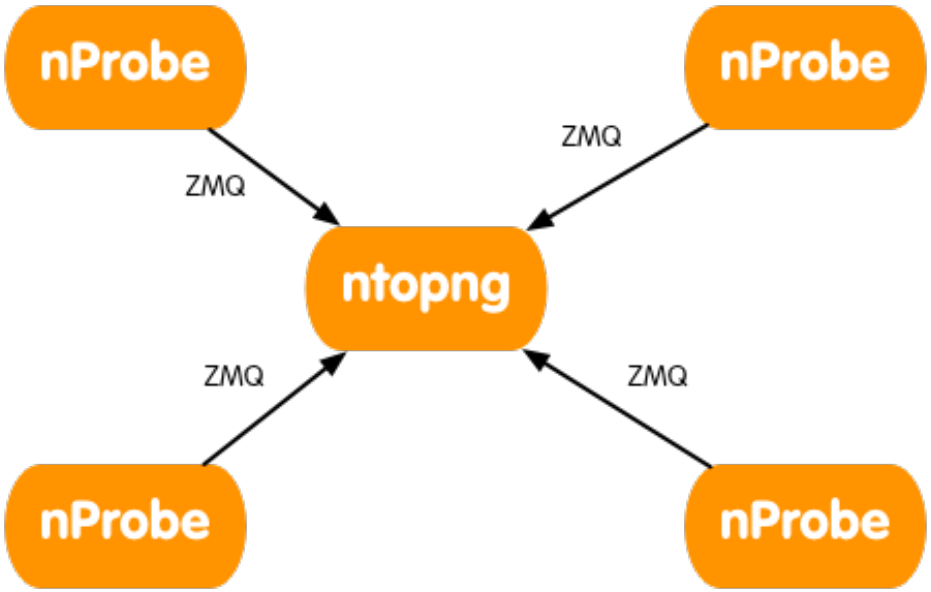
Interface Index	Interface Name	Chart	In Bytes	Out Bytes	Flow/SNMP Ratio
502	ge-0/0/0	-	0 B	104 B	
508	ge-0/0/3	-	0 B	253 B	
530	ge-0/0/17	-	0 B	220 B	
600	ge-0/1/0	-	577 B	0 B	

NOTE:
The Flow/SNMP ratio is a number 0..1 that indicates how much received flows represent the overall traffic. As in flow-based analysis non-IP and layer 2 headers are not accounted, typical ratio values are in the 0.8..0.9 range (i.e. 0.9 means that 90% of the received traffic as observed via SNMP has been reported in flows).
Ratio is computed hourly only if the following conditions are met:

- Device 192.12.193.126 must support SNMP and must be configured in the SNMP devices page.
- SNMP and flow devices timeseries must be enabled from the from the Preferences (Expert View).

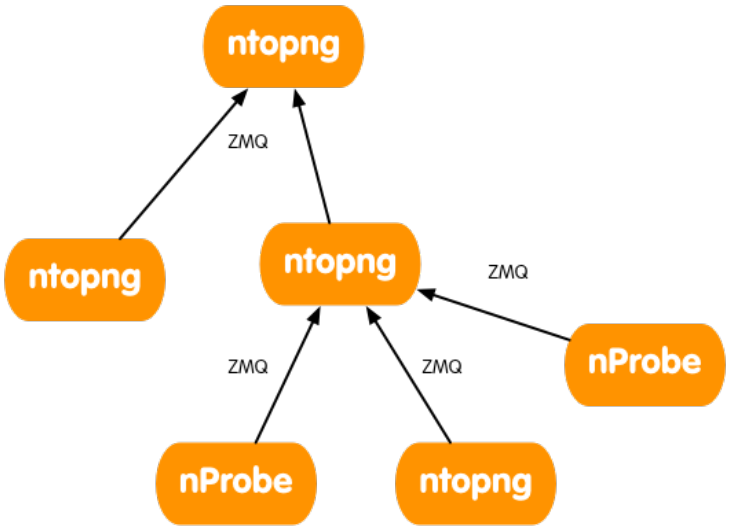
Creating ntopng Clusters [1/3]

- ntopng is not only a flow collector, but it can export flows in the same JSON format used in the received flows.
- This allows complex clusters to be created:



Creating ntopng Clusters [2/3]

- In many companies, there are many satellite offices and a few central aggregation points.
- Using ØMQ (both ntopng and nProbe flows are in the same format) it is possible to create a hierarchy of instances.
- Each node aggregates the traffic for the instances "below" it, so that at each tree layer you have a summarised view of the network activities.



Creating ntopng Clusters [3/3]

Example

- Start the remote nProbe instances as follows
  - `[host1] nprobe --zmq "tcp://*:5556" -i ethX`
  - `[host2] nprobe --zmq "tcp://*:5556" -i ethX`
  - `[host3] nprobe --zmq "tcp://*:5556" -i ethX`
  - `[host4] nprobe --zmq "tcp://*:5556" -i ethX`

- If you want to merge all nProbe traffic into a single ntopng interface do:
  - `ntopng -i tcp://host1:5556,tcp://host2:5556,tcp://host3:5556,tcp://host4:5556`

- If you want to keep each nProbe traffic into a separate ntopng interface do:
  - `ntopng -i tcp://host1:5556 -i tcp://host2:5556 -i tcp://host3:5556 -i tcp://host4:5556`

Managing Alerts [1/2]

- In many situations it is fundamental to set alerts that can signal anomalous conditions
- ntopng handles host/interface/network alerts hooked to multiple metrics
- Metrics include bytes/packets received/generated
- User-submitted alerts are continuously monitored in the background

Managing Alerts [2/2]

Host: 192.168.2.130 | Traffic | Packets | Ports | Peers | Protocols | DNS | HTTP | Flows | SNMP | Talkers

Every Minute | Every 5 Minutes | Hourly | Daily

Uptime: 1 h, 16 min, 12 sec
1 Alert | 86 Hosts | 148 Flows

Alert Function	Threshold
bytes	> 25000000 Bytes delta (sent + received)
dns	> DNS traffic delta bytes (sent + rece
p2p	> Peer-to-peer traffic delta bytes (ser
packets	> Packets delta (sent + received)
Rearm minutes	3 The rearm is the dead time between one alert generation and the potential generation of the next alert of the same kind.

Save Configuration [Delete All Host Configured Alerts]

Queued Alerts

10

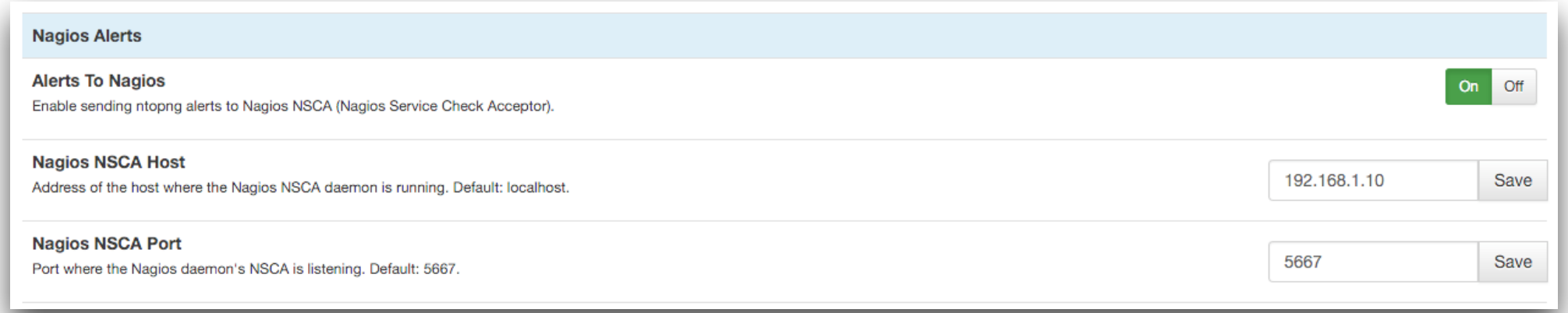
Action	Date	Severity	Type	Description
	Mon Apr 11 18:36:01 2016	Warning	Threshold Cross	Threshold **bytes** crossed by host 192.168.2.130 [1168 > 25]

Showing 1 to 1 of 1 rows

Purge All Alerts

Sending ntopng Alerts to Nagios [1/2]

- Nagios is the de-facto standard in infrastructure monitoring
- ntopng features alert propagation to Nagios



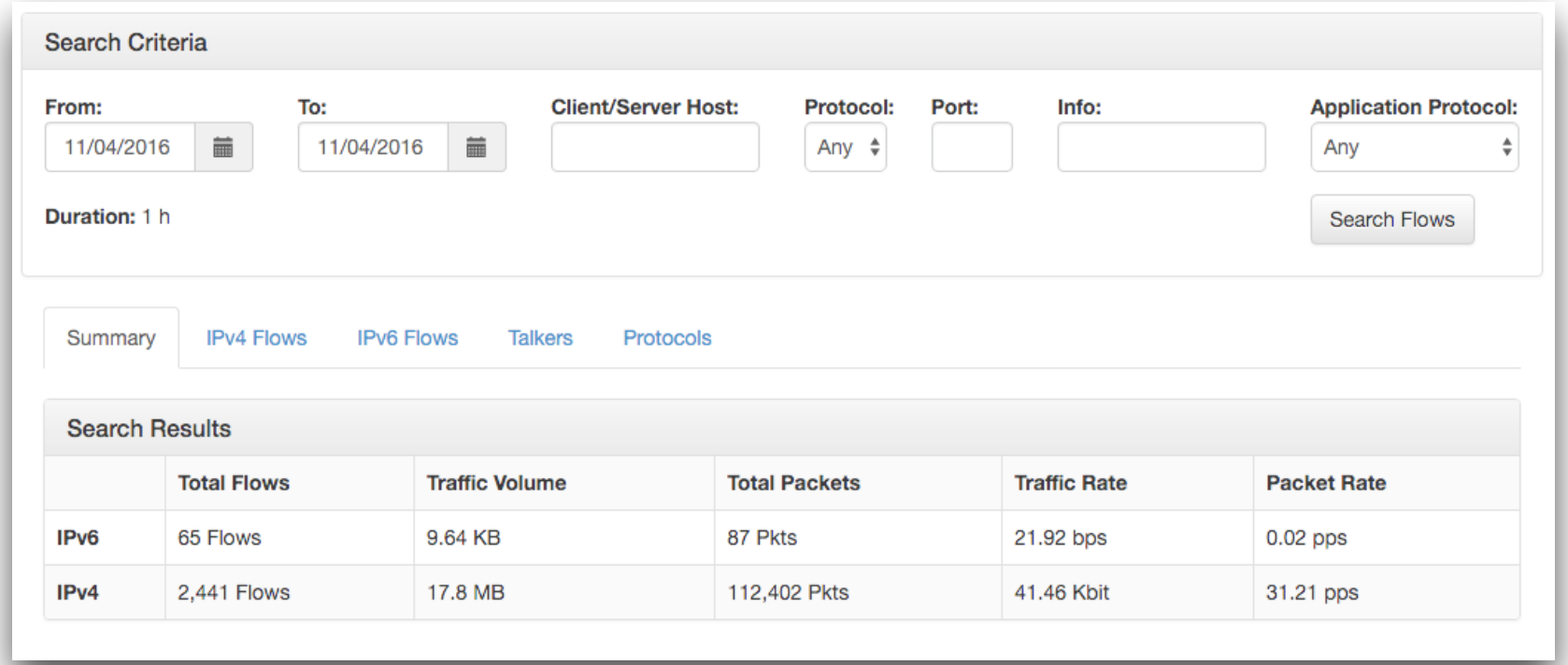
Sending ntopng Alerts to Nagios [2/2]

- Alerts are sent to Nagios via NSCA
- Nagios will intercept all alerts that are explicitly declared as passive services
- Passive service description format is:
  - NtopngAlert_<host/network/interface>_<timespan>_<metric>

ntopng-host	NtopngAlert	?	OK	12-23-2015 15:25:50	0d 17h 27m 59s	1/1	Alert for host Y!
	NtopngAlert_192.168.1.15_min_bytes	?	OK	12-23-2015 09:13:22	0d 6h 47m 34s	1/1	OK, alarm deactivated
	NtopngAlert_192.168.2.0/24	?	OK	12-23-2015 11:02:34	0d 4h 33m 4s	1/1	OK, alarm deactivated
	NtopngAlert_192.168.70.0/24_min_egress	?	WARNING	12-23-2015 15:33:01	0d 0h 6m 5s	1/1	Threshold egress crossed by network 192.168.70.0/24 [1180 > 10]
	NtopngAlert_192.168.70.0/24_min_ingress	?	WARNING	12-23-2015 15:33:01	0d 0h 2m 5s	1/1	Threshold ingress crossed by network 192.168.70.0/24 [11241211 > 10]

Historical Flow Navigation [1/2]

- ntopng can send (-F) network flows to MySQL
- a built-in database explorer retrieves such flows and allows them to be navigated and searched



	Total Flows	Traffic Volume	Total Packets	Traffic Rate	Packet Rate
IPv6	65 Flows	9.64 KB	87 Pkts	21.92 bps	0.02 pps
IPv4	2,441 Flows	17.8 MB	112,402 Pkts	41.46 Kbit	31.21 pps

Historical Flow Navigation [2/2]

Summary | IPv4 Flows | IPv6 Flows | Talkers | Protocols

IPv6 Top Flows [11/04/2016 17:56:35 - 11/04/2016 18:56:35]

5

	Application	L4 Proto	Client	Server	Begin	End	Bytes	Avg Thpt
Info	? Unknown	UDP	simones-macbook-pro.loca...:mdns	ff02::fb:mdns	11/04/2016 18:22:02	11/04/2016 18:22:03	811 B	3.24 Kbit
Info	? Unknown	UDP	simones-macbook-pro.loca...:mdns	ff02::fb:mdns	11/04/2016 18:22:02	11/04/2016 18:22:03	811 B	3.24 Kbit
Info	? Unknown	UDP	fe80::3e15:c2ff:feb7:720...:mdns	ff02::fb:mdns	11/04/2016 18:39:30	11/04/2016 18:39:30	613 B	4.9 Kbit
Info	? Unknown	UDP	fe80::b675:eff:fe92:8917...:dhcpv6-client	ff02::1:2:dhcpv6-server	11/04/2016 18:50:40	11/04/2016 18:50:43	324 B	648 bps
Info	? Unknown	UDP	fe80::b675:eff:fe92:8917...:dhcpv6-client	ff02::1:2:dhcpv6-server	11/04/2016 18:41:55	11/04/2016 18:41:58	324 B	648 bps

Showing 1 to 5 of 65 rows

« < 1 2 3 4 5 > »

Download flows: IPv4 IPv6 Extract pcap:

Bulk download and full pcap extraction options

Historical Talkers [1/2]

- Top Talkers can be automatically extracted from flows
- Every top talker can be clicked to inspect its peers
- Every peer can be clicked to inspect L7 application protocols

Historical Talkers [2/2]

Summary | IPv4 Flows | IPv6 Flows | Talkers | Protocols

Interface en4

50

Host Name	IP Address	Total Traffic	Total Packets	Ingress Traffic	Ingress Packets	Egress Traffic	Egress Packets	Flows
192.168.2.130	192.168.2.130	18.27 MB	119,364	9.02 MB	86,911	9.25 MB	32,453	2,320

Summary | IPv4 Flows | IPv6 Flows | Talkers | Protocols

Interface en4 / Talkers with 172.217.16.5

50

Host Name	IP Address	Total Traffic	Total Packets	Traffic Sent	Packets Sent	Traffic Received	Packets Received	Flows
192.168.2.130	192.168.2.130	1.68 MB	3,317	0 B	0	1.68 MB	3,317	12

Summary | IPv4 Flows | IPv6 Flows | Talkers | Protocols

Interface en4 / Talkers with 172.217.16.5 / Applications between 172.217.16.5 and 192.168.2.130

50

Application	Traffic Volume	Packets	Flows
Quic	1.68 MB	3,317	12

Historical Applications [1/2]

- Top Applications can be automatically extracted from flows as well
- Every top application can be clicked to inspect hosts that have used it
- Every host can be clicked to inspect peers that have used a given application to communicate with the host

Historical Applications [2/2]

Chart | IPv4 Flows | IPv6 Flows | Talkers | Protocols

Interface en4

protocols all — Select saved...

host peers by protocol all — Select saved...

50

Application	Traffic Volume	Packets	Flows
AppleiTunes	471 B	2	1
IGMP	600 B	10	10
NTP	1.05 KB	12	6

Chart | IPv4 Flows | IPv6 Flows | Talkers | Protocols

Interface en4 / AppleiTunes talkers

protocols all — Select saved...

host peers by protocol all — Select saved...

50

Host Name	Address	Traffic Volume	Packets	Flows
192.168.2.130	192.168.2.130	471 B	2	1

Chart | IPv4 Flows | IPv6 Flows | Talkers | Protocols

Interface en4 / AppleiTunes talkers / AppleiTunes talkers with 192.168.2.130

protocols all — Select saved...

host peers by protocol all — Select saved...

50

Host Name	Address	Traffic Volume	Packets	Flows
jake.unipi.it	131.114.18.19	471 B	2	1

ntopng and Big Data

- Using SQLite to save flows persistently is good when flows are not too many and the system that runs ntopng has storage.
- For large deployments or disk-less systems (e.g. ARM-based PCs) it is desirable to upload flows on remote, cloud-based, systems able to scale with the number of flows.
- In essence ntopng has been opened to what is currently defined as "big data" systems that can scale with data in volume and speed.

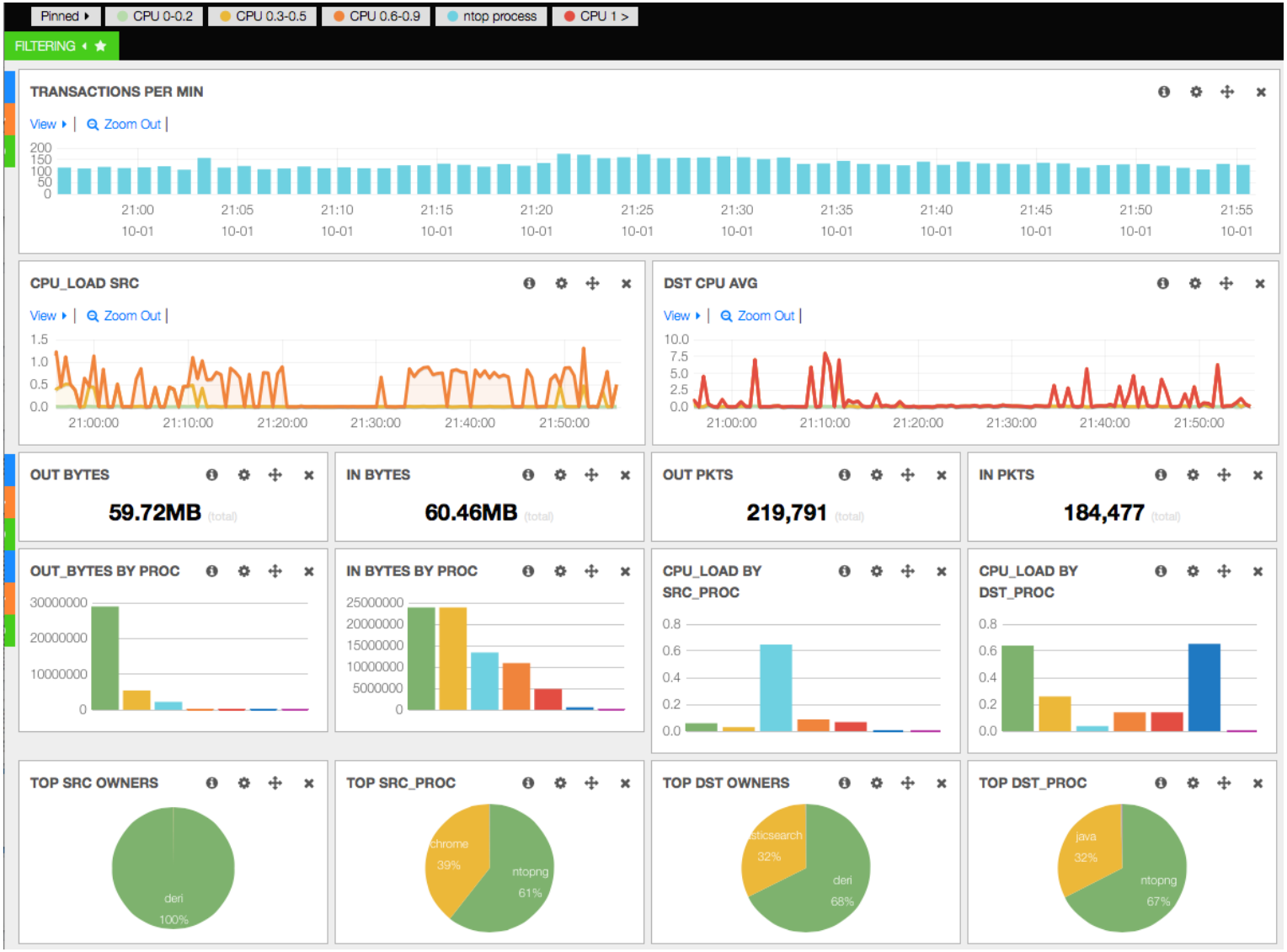
Integrating ntopng with ElasticSearch [1/2]

- An emerging Big Data system is ElasticSearch that is used by a large community because of its flexibility and user interface (Kibana) that allow visual applications to be developed in minutes.
- Although we do not want to bind ntopng only with ES, we believe that its integration is a good starting point for:
  - Opening ntopng to the Big Data world.
  - Allowing people to use ntopng as data source and let them use ES for long-term data storage and develop custom dashboards using Kibana.

Integrating ntopng with ElasticSearch [2/2]

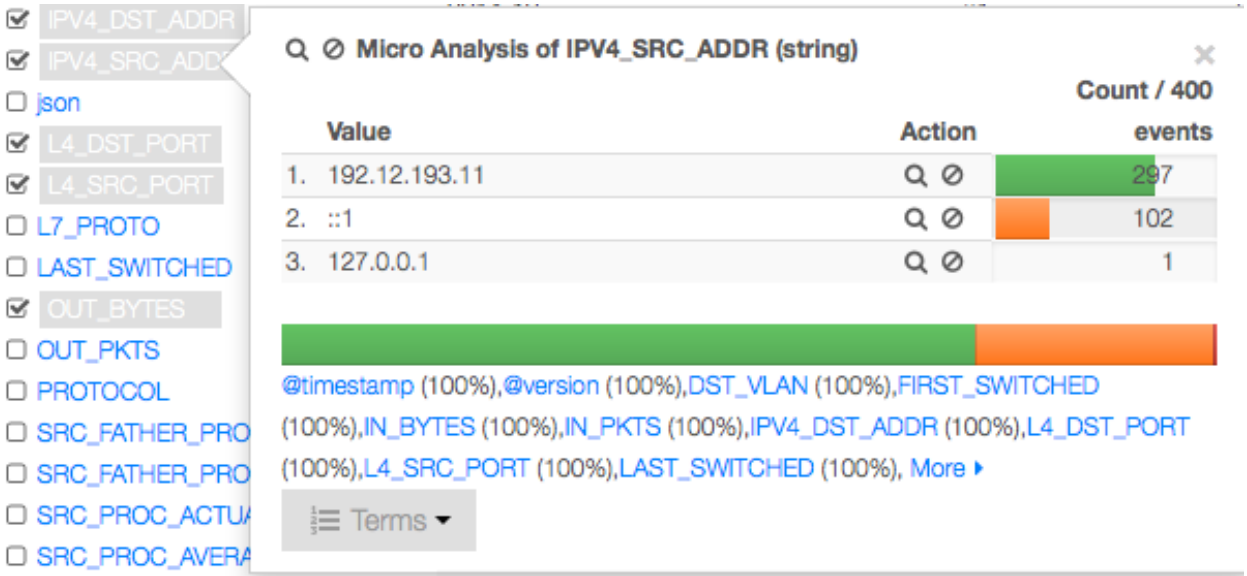
- ntopng dumps exported flows in JSON format onto a Redis queue enriched with some specified ES attributes (e.g. @timestamp that specifies the time such flow has been exported).
- As soon as there is a minimum number of flows in queue, a ntopng thread packs them together and sends them to ES using the ES bulk API.
- ES indexes the received flows and make them available to external applications such as the Kibana dashboard.

ntopng Process Dashboard in Kibana [1/2]



ntopng Process Dashboard in Kibana [2/2]

- The GUI refreshes automatically as new data arrive and users can drill down data or visualise raw flows.



View: **Table** / JSON / Raw

Field	Action	Value
@timestamp		2014-10-01T20:00:25.021Z
@version		1
DST_VLAN		0
FIRST_SWITCHED		1412193584
IN_BYTES		40
IN_PKTS		1
IPV4_DST_ADDR		192.12.192.104
IPV4_SRC_ADDR		192.12.193.11
L4_DST_PORT		1234
L4_SRC_PORT		55451
LAST_SWITCHED		1412193584
OUT_BYTES		60
OUT_PKTS		1
PROTOCOL		6
SRC_FATHER_PROC_NAME		init
SRC_FATHER_PROC_PID		1
SRC_PROC_ACTUAL_MEMORY		1467872
SRC_PROC_AVERAGE_CPU_LOAD		0
SRC_PROC_NAME		ntopng
SRC_PROC_NUM_PAGE_FAULTS		0
SRC_PROC_PEAK_MEMORY		1533796
SRC_PROC_PID		13058
SRC_PROC_USER_NAME		deri

What's Next on Big Data and ntopng

- We believe that the big data world is still very liquid and it is not clear what the emerging technology will be.
- We believe ntopng should be just a data source without being tightly integrated with any external tool (ntopng speaks JSON and HTTP so we can cover most of them pretty easily).
- We are experimenting with other big data technologies (e.g. druid.io) and we plan to open it to all the emerging technologies available.

ntopng on Virtual Environments

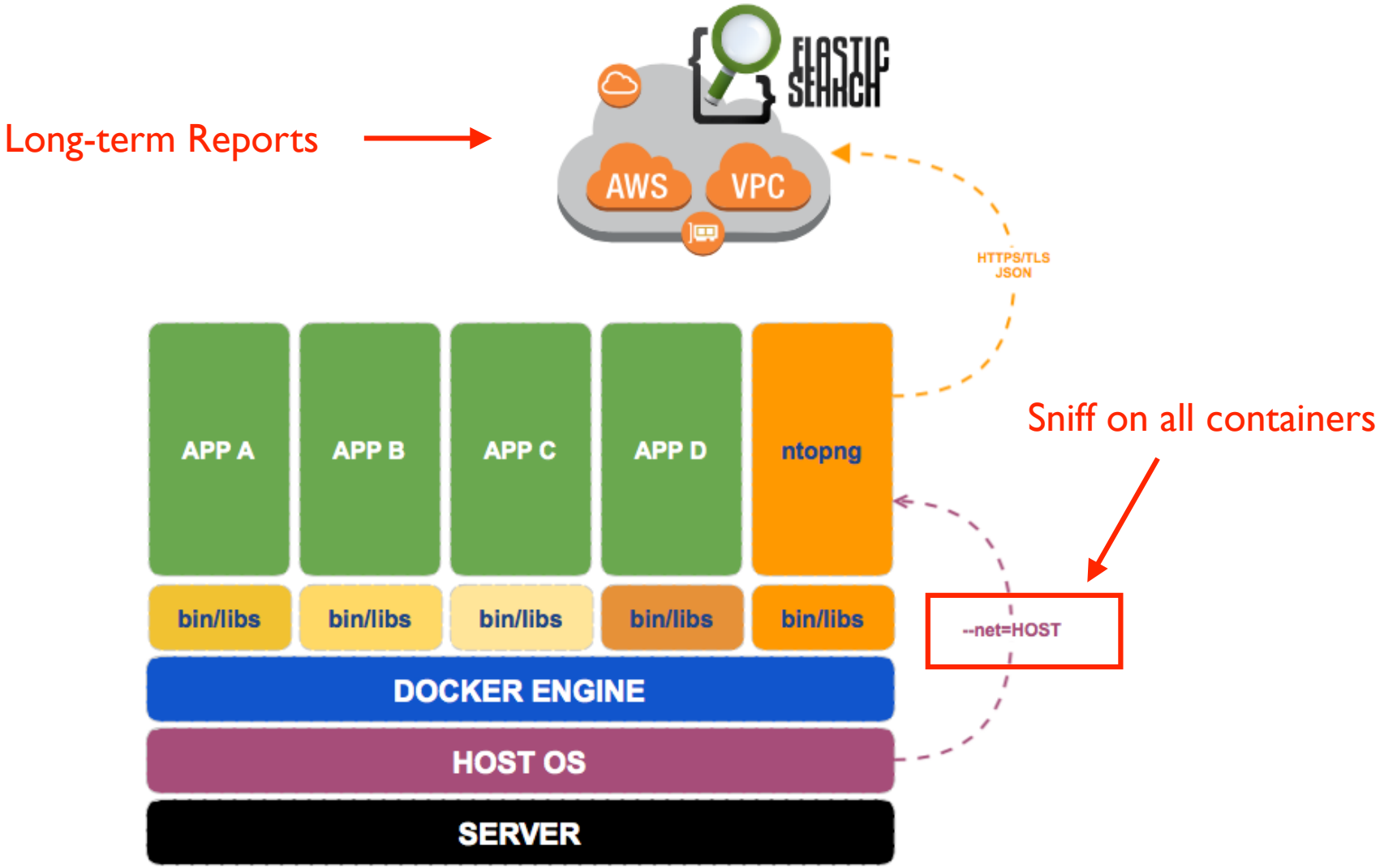
- ntopng has been packaged for major Linux distributions such as Debian/Ubuntu, CentOS/RedHat and also FreeBSD and OSX (brew): installation couldn't be simpler.
- However the current trend is going towards virtualised environments (not just VMs such as VMware) and IaaS (Infrastructure as a Service) and thus we need to support them.

ntopng on Docker [1/5]

- In essence there are two types of virtualisation:
  - Virtual Machine: emulation of a particular computer system, including its devices (network, storage, USB etc).
  - Operating-system level virtualisation: run multiple isolated user-space instances (often called containers) that look like a real server.

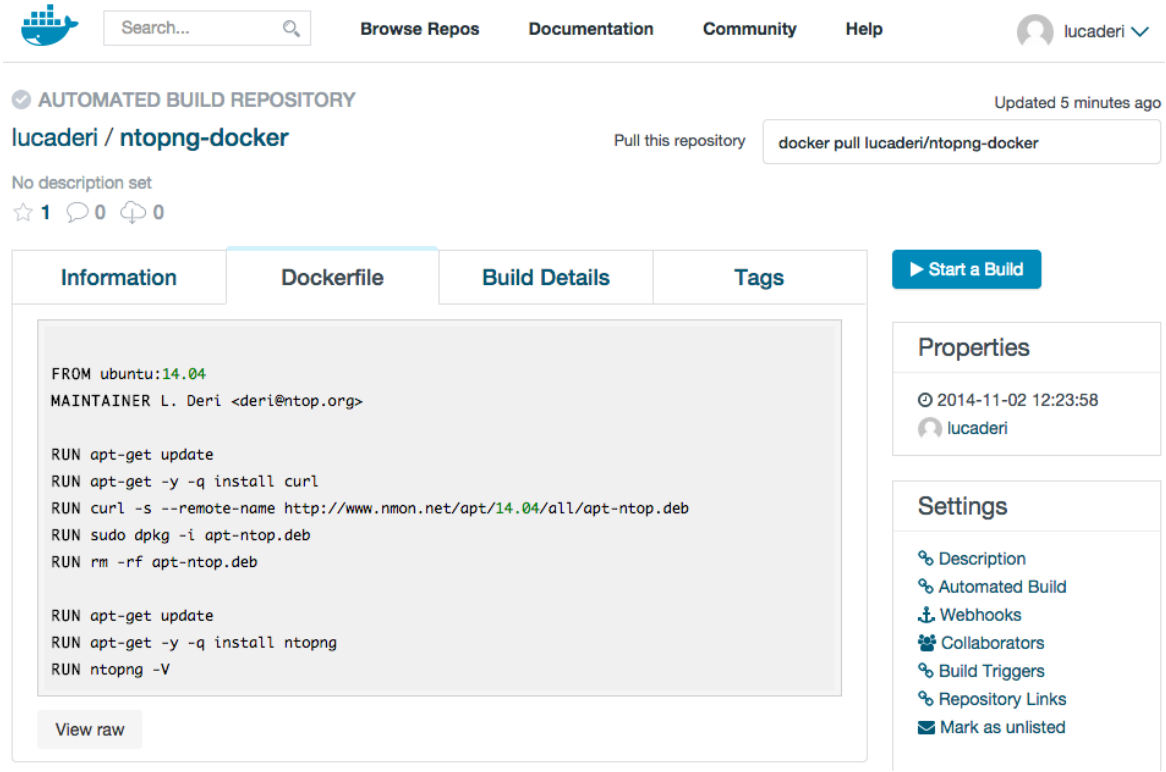
- Docker is an open-source software that automates the deployment of applications inside software containers. Each container runs within a single Linux instance without the overhead of starting VMs.

ntopng on Docker [2/5]



ntopng on Docker [3/5]

- A ntopng container allows you to run ntopng on a clean and isolated environment.
- Building a dock can be done in a few clicks on hub.docker.com

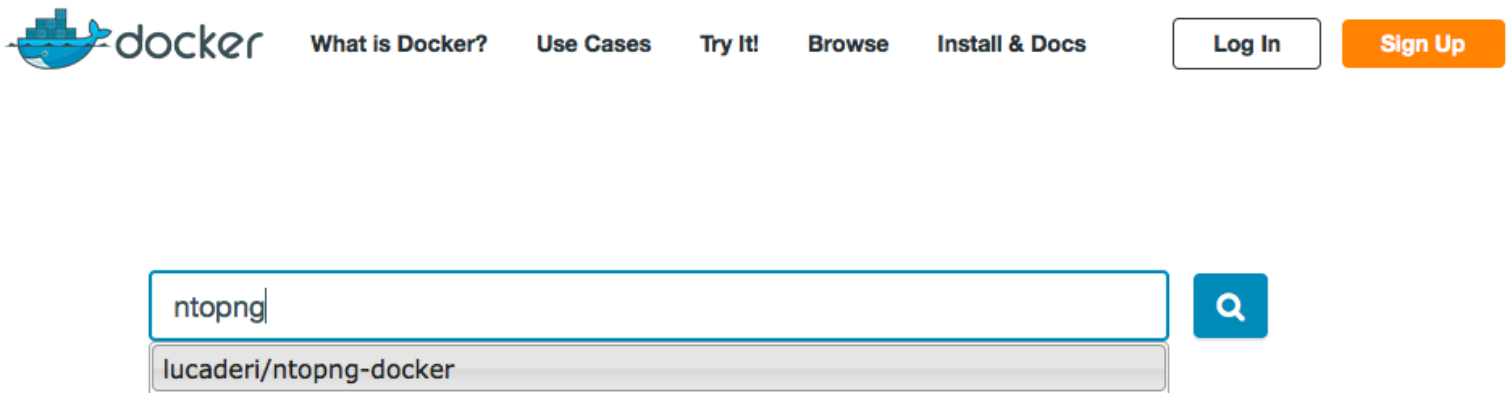


ntopng on Docker [4/5]

- Install docker (http://docs.docker.com/installation/ubuntulinux/)

```
$ sudo apt-get update
$ sudo apt-get install docker.io
$ sudo ln -sf /usr/bin/docker.io /usr/local/bin/docker
$ sudo sed -i '$acomplete -F _docker docker' /etc/bash_completion.d/docker.io
$ source /etc/bash_completion.d/docker.io
$ sudo sh -c "echo deb https://get.docker.com/ubuntu docker main > /etc/apt/sources.list.d/docker.list"
$ sudo apt-get update
$ sudo apt-get install lxc-docker
```

- Go do docker.com and search for ntopng



ntopng on Docker [5/5]

- Pull the ntopng container

```
root@ubuntu:/home/deri# docker pull lucaderi/ntopng-docker
Pulling repository lucaderi/ntopng-docker
8077c18a90a8: Download complete
511136ea3c5a: Download complete
d497ad3926c8: Download complete
ccb62158e970: Download complete
e791be0477f2: Download complete
…
e072f31bb2a5: Download complete
9e52f4c92f80: Download complete
ecc46895937f: Download complete
3a3f2545e225: Download complete
4f1229fadea7: Download complete
5b5364929cbf: Download complete
Status: Downloaded newer image for lucaderi/ntopng-docker:latest
```

- Run ntopng on a container

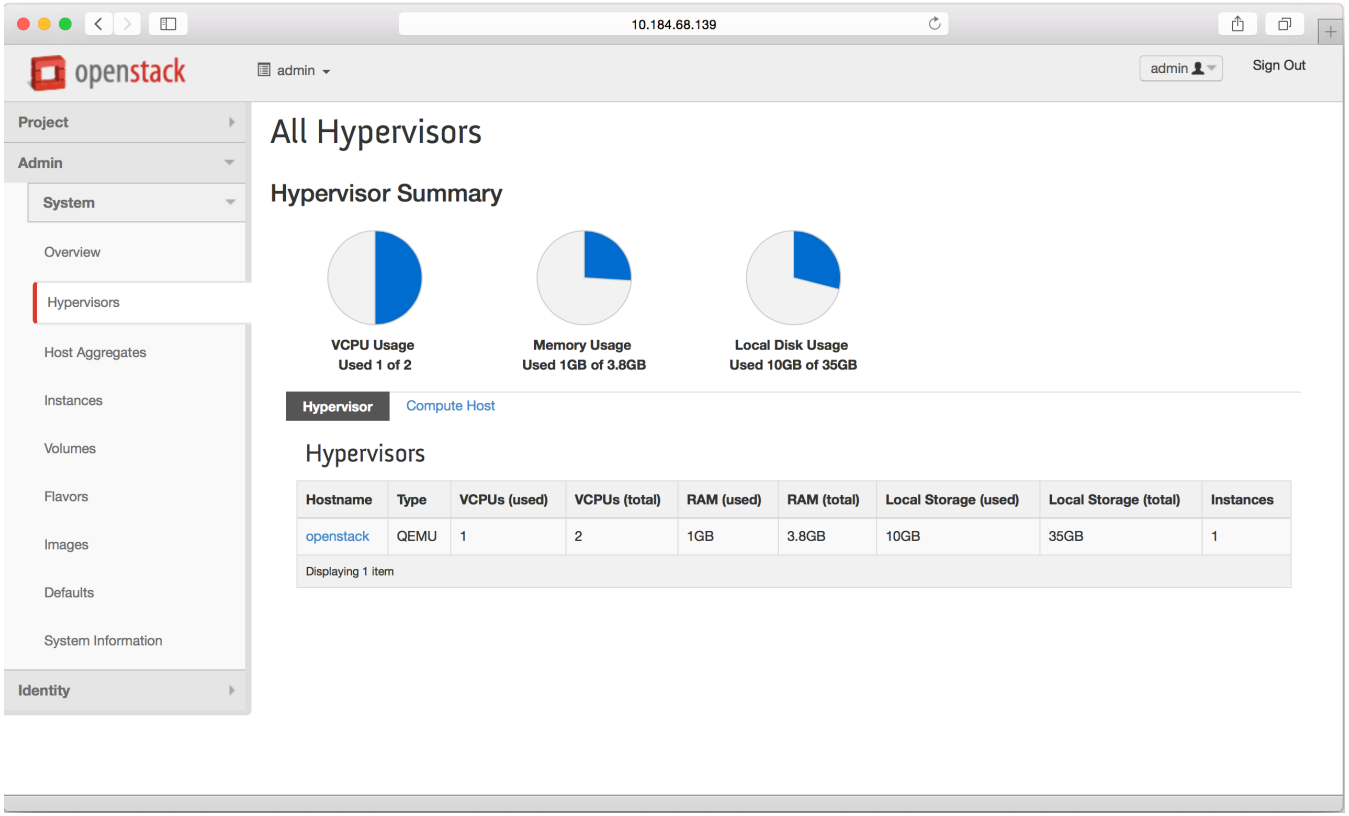
```
root@ubuntu:/home/deri# docker run --net=host --name ntopng -t -i lucaderi/ntopng-docker ntopng -v
….
02/Nov/2014 12:55:20 [main.cpp:183] PID stored in file /var/tmp/ntopng.pid
02/Nov/2014 12:55:20 [HTTPserver.cpp:374] HTTPS Disabled: missing SSL certificate /usr/share/ntopng/httpdocs/ssl/ntopng-cert.pem
02/Nov/2014 12:55:20 [HTTPserver.cpp:376] Please read https://svn.ntop.org/svn/ntop/trunk/ntopng/README.SSL if you want to enable SSL.
02/Nov/2014 12:55:20 [HTTPserver.cpp:420] Web server dirs [/usr/share/ntopng/httpdocs][/usr/share/ntopng/scripts]
02/Nov/2014 12:55:20 [HTTPserver.cpp:423] HTTP server listening on port 3000
02/Nov/2014 12:55:20 [main.cpp:231] Working directory: /var/tmp/ntopng
02/Nov/2014 12:55:20 [main.cpp:233] Scripts/HTML pages directory: /usr/share/ntopng
02/Nov/2014 12:55:20 [Ntop.cpp:218] Welcome to ntopng x86_64 v.1.2.2 (r8539) - (C) 1998-14 ntop.org
```

ntopng on OpenStack [1/8]

- OpenStack is a technology that allows to deploy and control resources on a data center (VMs, storage, networking).
- Our interest in OpenStack is manyfold:
  - Create an OpenStack VM image for enabling people to easily deploy ntop monitoring apps on datacenter.
  - Exploit ntop's PF_RING open-source packet processing technology for bringing packets in 0-copy at 10 Gbit on a VM managed by OpenStack. This is to enable efficient traffic monitoring on a data center.

ntopng on OpenStack [2/8]

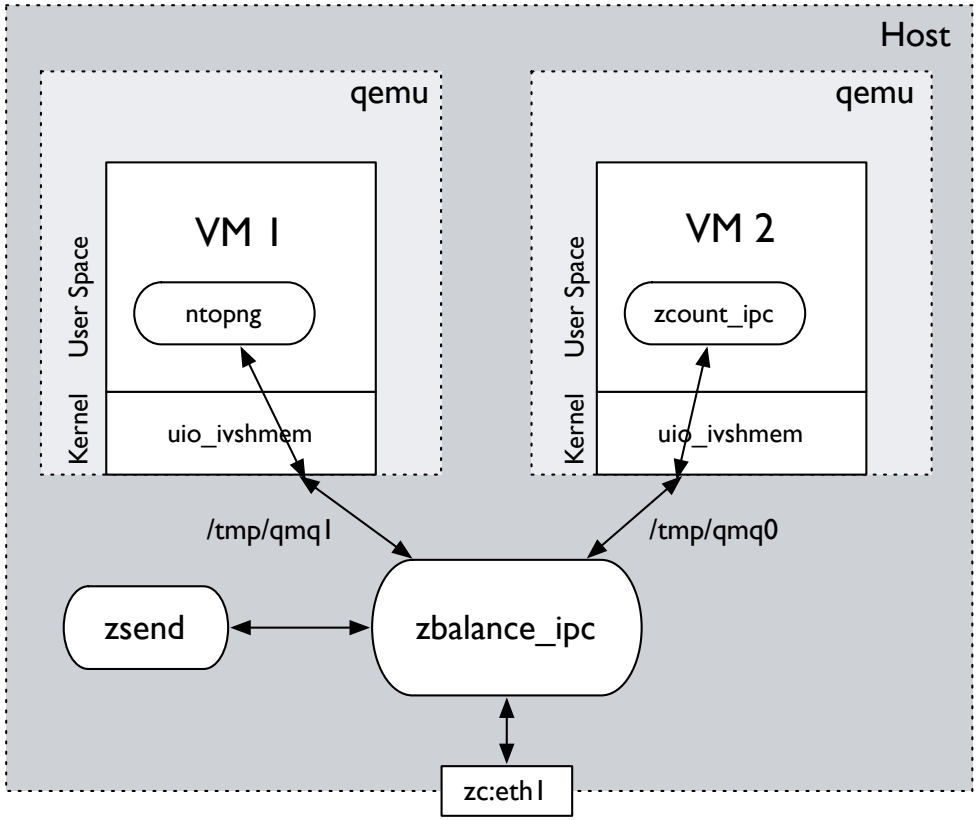
- In OpenStack, VMs are KVM-based and are managed though the OpenStack controller.



ntopng on OpenStack [3/8]

- Through OpenStack we want to be able to deploy VMs with ntopng and attach them to virtual controllers (Open vSwitch) or 0-copy PF_RING ZC-based packet sources.
- With ZC, packets are captured in 0-copy from network adapters and deployed in 0-copy to VMs.
- ZC packets are deployed on the VM using virtual adapters attached dynamically to the VM though a ntop-developed kernel module based on PCI hotplug.

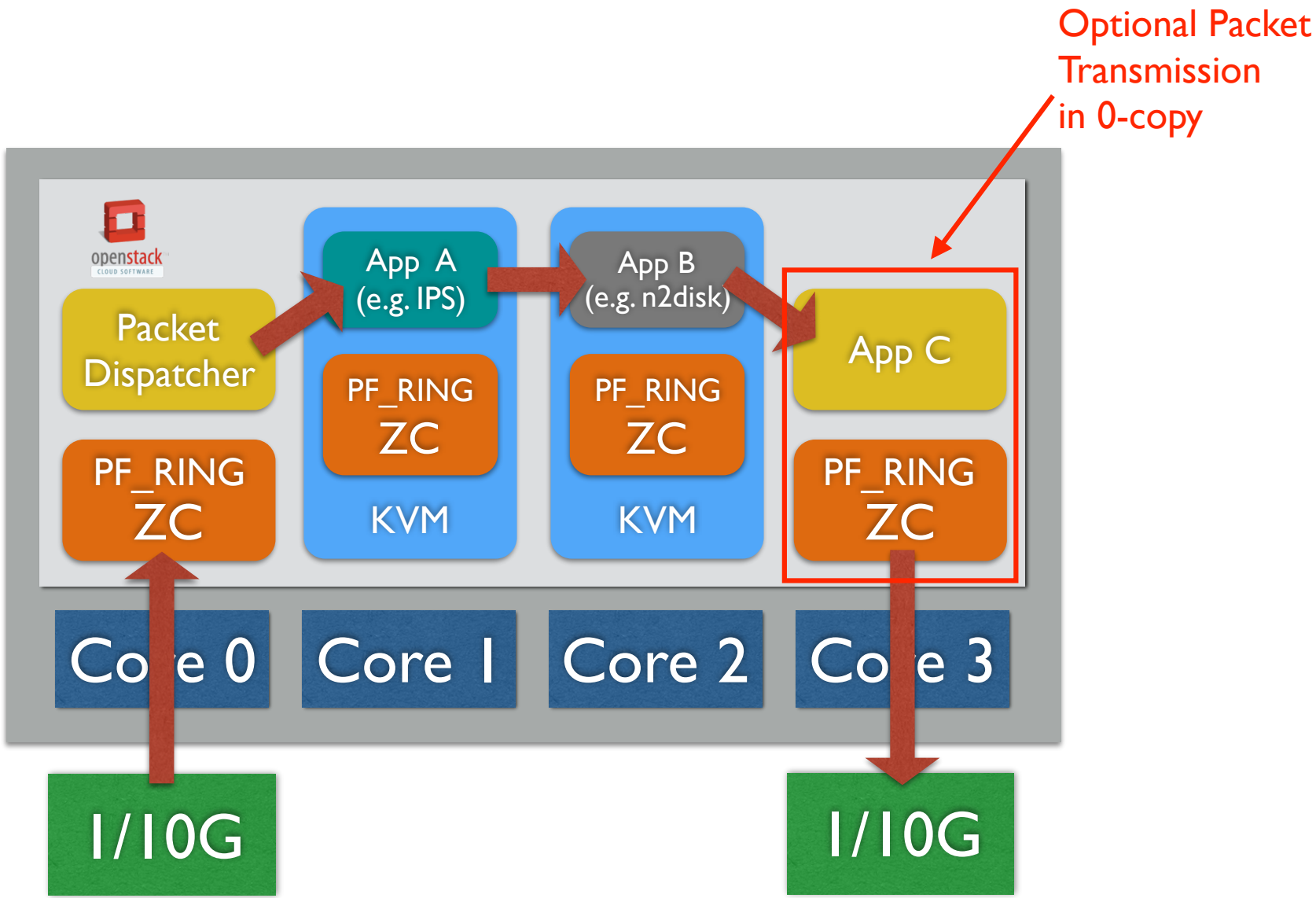
ntopng on OpenStack [4/8]



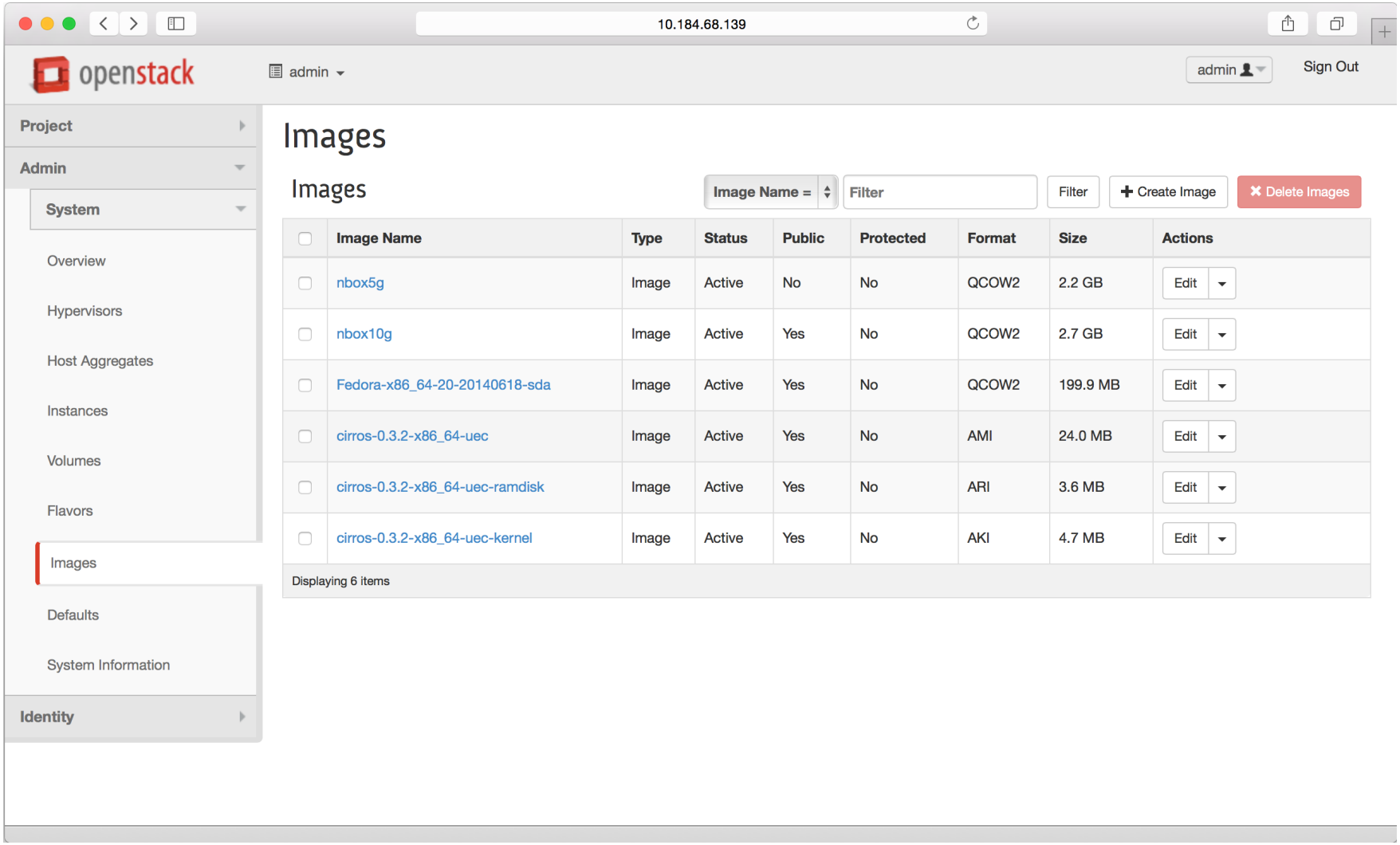

```
(Host) $ ./zbalance_ipc -i zc:eth1 -c 99 -n 2 -m 0 -Q /tmp/qmp0,/tmp/qmp1
(Host) $ ./zsend -c 99 -Q /tmp/qmp0

(VM 1) $ ./ntopng -i zc:99@0 …
(VM 2) $ ./zcount_ipc -i 1 -c 99 -u
```

ntopng on OpenStack [5/8]

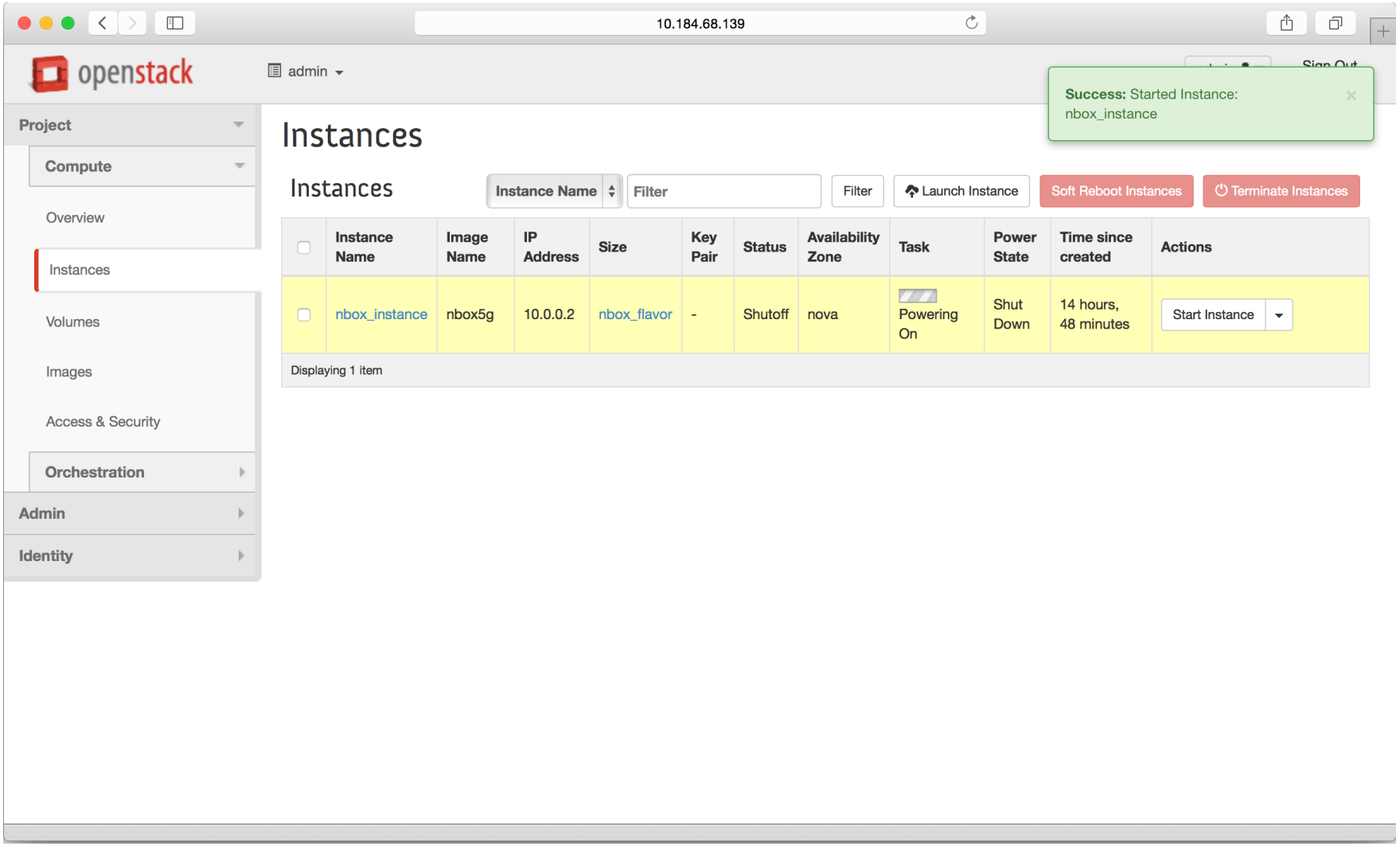


ntopng on OpenStack [6/8]

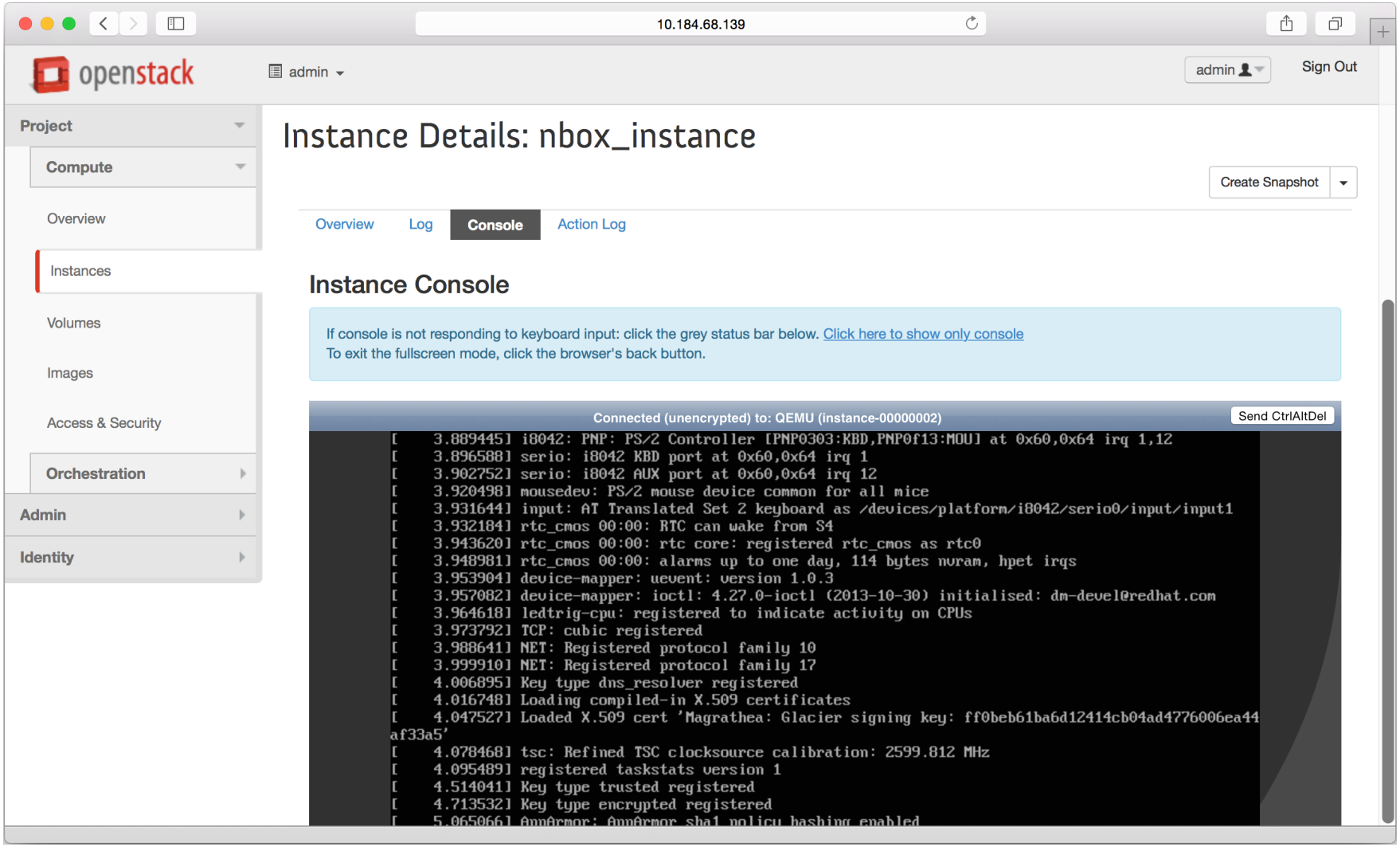


NOTE: OpenStack image available from the ntop web site

ntopng on OpenStack [7/8]



ntopng on OpenStack [8/8]



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]

Unknown Protocol

Same Port

Different Targets

Little Traffic

Low Bandwidth

ntop | Flows | Hosts | Devices | Interfaces | Search Host

Host: | Traffic | Packets | Ports | Peers | Protocols | Flows | Talkers

Active Flows

50 | Applications

	Application	L4 Proto	VLAN	Client	Server	Duration	Actual Thpt	Total Bytes	Info
Info	? Unknown	TCP		:50933	90.113.215.107:64963	3 sec	1.31 Kbit ↑	883 B	
Info	? Unknown	TCP		:50933	90.62.176.114:50191	3 sec	535.17 bps ↑	469 B	
Info	? Unknown	TCP		:50933	181.229.201.186:49719	3 sec	0 bps –	307 B	
Info	? Unknown	TCP		:57316	77.144.172.122:http	3 sec	0 bps –	580 B	
Info	? Unknown	TCP		:50933	181.229.201.186:49839	5 sec	637.41 bps ↑	533 B	
Info	? Unknown	TCP		:50933	[illegible]	2 sec	0 bps –	262 B	
Info	? Unknown	TCP		:57318	77.144.172.122:http	2 sec	0 bps –	580 B	
Info	? Unknown	TCP		:50933	89.159.84.197:52345	< 1 sec	0 bps	64 B	
Info	? Unknown	TCP		:50933	87.91.126.40:50710	2 sec	0 bps	1.27 KB	
Info	? Unknown	TCP		:50933	82.246.16.30:52460	3 sec	0 bps	853 B	
Info	? Unknown	TCP		:50933	31.38.111.67:56388	2 sec	0 bps	1.16 KB	
Info	? Unknown	UDP		:49820	84.99.86.26:56795	26 sec	0 bps ↓	289 B	
Info	? Unknown	TCP		:50933	77.147.64.78:55943	1 sec	0 bps –	262 B	
Info	? Unknown	TCP		:50933	77.147.64.78:55944	1 sec	0 bps –	262 B	
Info	? Unknown	TCP		:50933	87.91.126.40:50443	1 sec	0 bps –	390 B	
Info	? Unknown	TCP		:50933	82.245.198.130:56617	1 sec	0 bps	262 B	
Info	? Unknown	TCP		:50933	2.7.143.251:58591	1 sec	0 bps –	134 B	
Info	? Unknown	TCP		:50933	77.147.64.78:56224	4 sec	0 bps	533 B	

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	Server	0 bps	941 B	xml2.corriereobjects.it ContentServer
Info	DNS	UDP	:43845	:domain	< 1 sec	Server	0 bps	623 B	xml.corriereobjects.it ContentServer
Info	DNS	UDP	:53835	:domain	< 1 sec	Server	0 bps	547 B	www.trovoaste.it Generic
Info	DNS	UDP	:43740	:domain	< 1 sec	Server	0 bps	461 B	www.dday.it FreeTime
Info	DNS	UDP	:60289	:domain	1 sec	Server	0 bps	563 B	www.corriere.it News
Info	DNS	UDP	:45126	:domain	< 1 sec	Server	0 bps	716 B	vivimilano.corriere.it News
Info	DNS	UDP	:48302	:domain	< 1 sec	Server	0 bps	523 B	video.corriere.it News
Info	DNS	UDP	:39114	:domain	< 1 sec	Server	0 bps	559 B	vicenza.corriere.it News
Info	DNS	UDP	:57737	:domain	< 1 sec	Server	0 bps	555 B	verona.corriere.it News
Info	DNS	UDP	:57524	:domain	< 1 sec	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]

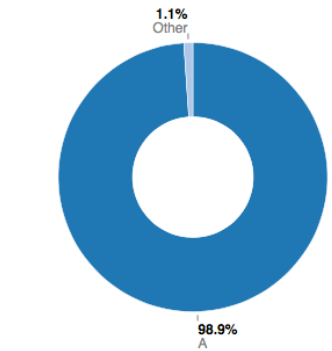
Select DNS

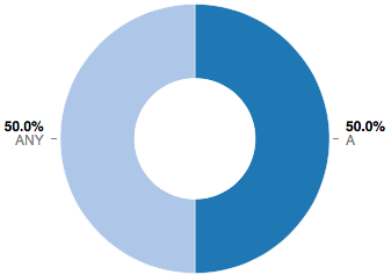
Drill-down on
a specific host

Host: Traffic Packets Ports Peers Protocols Activities DNS HTTP 1 Flows SNMP

Talkers

DNS Breakdown	Queries	Positive Replies	Error Replies	Reply Breakdown
Sent	15,066	0	0	
DNS Query Sent Distribution				
Rcvd	2	14,983	87	OK
DNS Rcvd Query Distribution				
Request vs Reply	Queries		Replies	





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

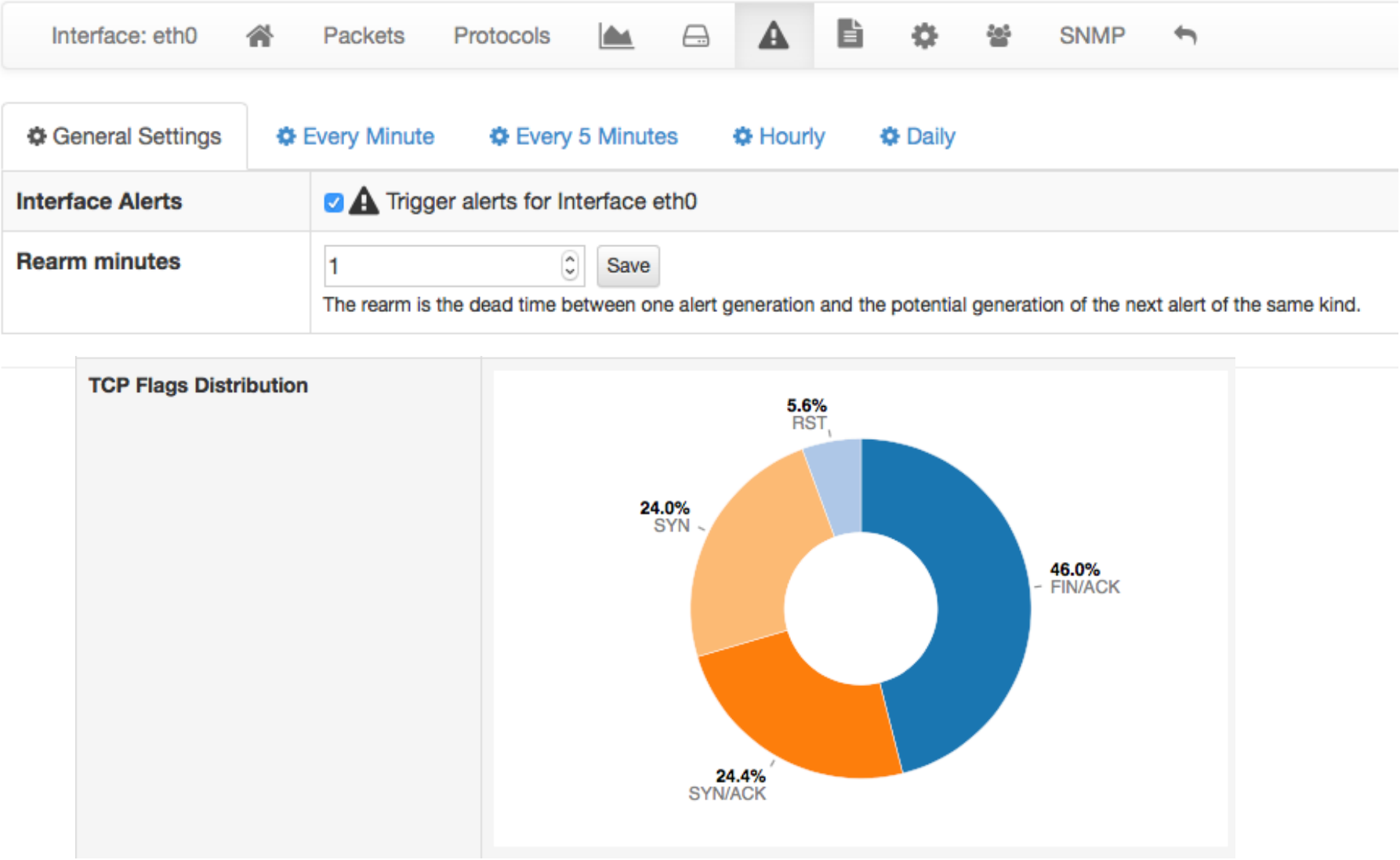
Mac: 80:2A:A8:8D:69:2C

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).

General Settings | Every Minute | Every 5 Minutes | Hourly | Daily

Host Alerts	☑ ⚠ Trigger alerts for Host ovpn.nic.it
Rearm minutes	1 Save The rearm is the dead time between one alert generation and the potential generation of the next alert of the same kind.
Host Flow Alert Threshold	25 Save Max number of new flows/sec over which a host is considered a flooder. Default: 25.
Host SYN Alert Threshold	10 Save Max number of sent TCP SYN packets/sec over which a host is considered a flooder. Default: 10.
Host Flows Threshold	32768 Save Max number of flows over which a host is considered a flooder. Default: 32768.

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

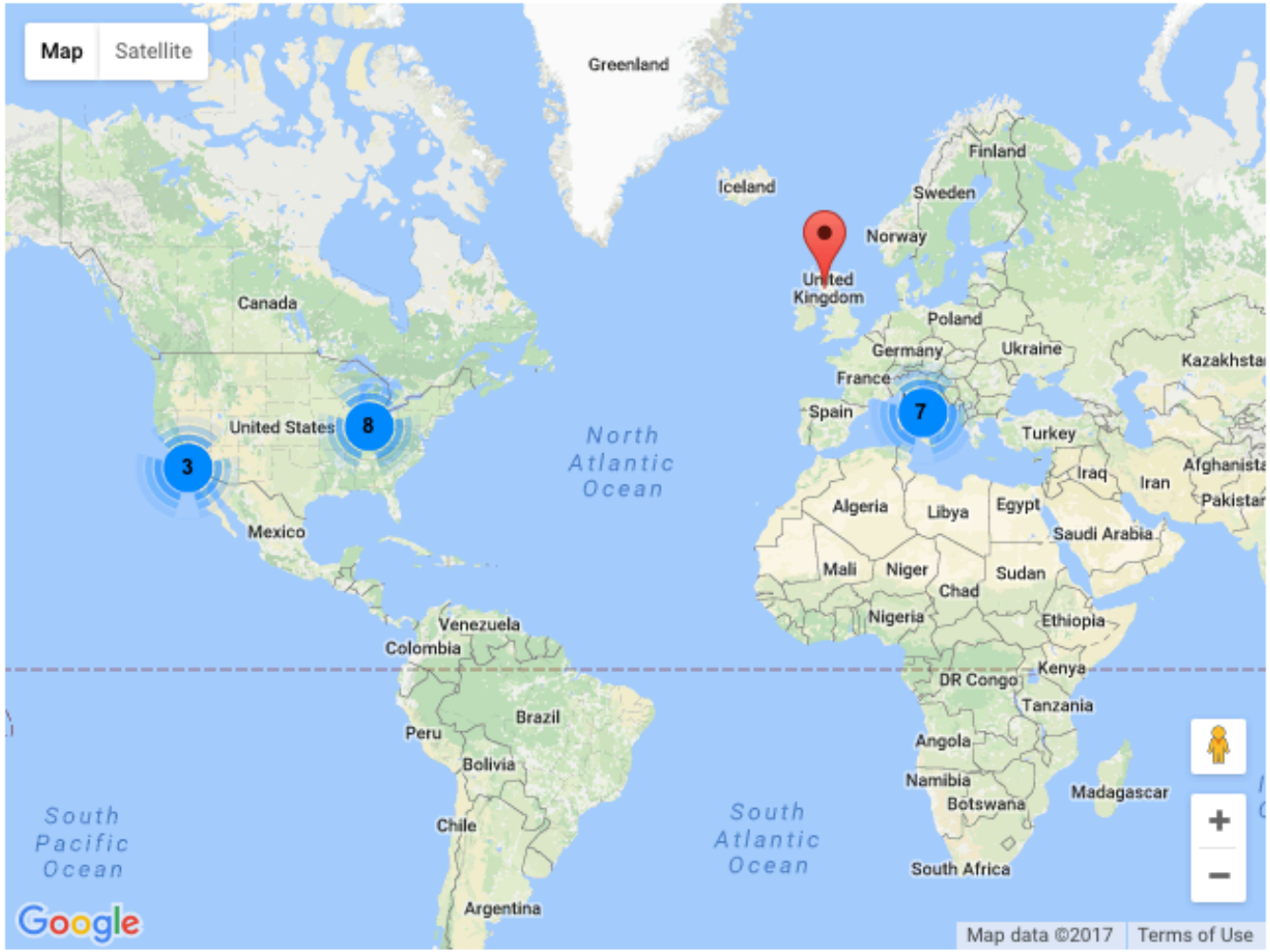
Traffic Geolocation [1/2]

- 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]

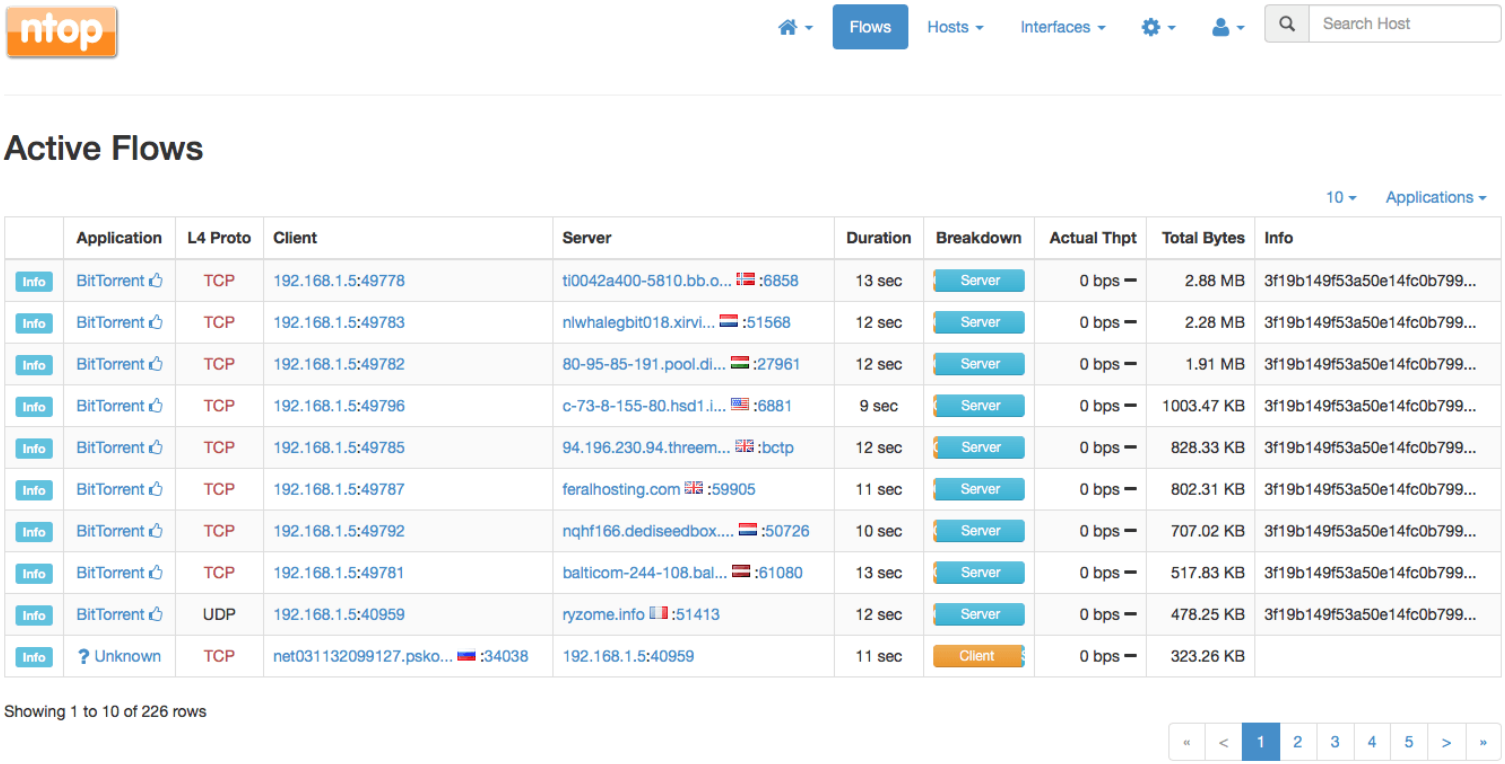
1. ^ mjg59: Spot the difference

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



	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	BitTorrent	TCP	192.168.1.5:49778	ti0042a400-5810.bb.o... :6858	13 sec	Server	0 bps	2.88 MB	3f19b149f53a50e14fc0b799...
Info	BitTorrent	TCP	192.168.1.5:49783	nlwhalegbit018.xirvi... :51568	12 sec	Server	0 bps	2.28 MB	3f19b149f53a50e14fc0b799...
Info	BitTorrent	TCP	192.168.1.5:49782	80-95-85-191.pool.di... :27961	12 sec	Server	0 bps	1.91 MB	3f19b149f53a50e14fc0b799...
Info	BitTorrent	TCP	192.168.1.5:49796	c-73-8-155-80.hsd1.i... :6881	9 sec	Server	0 bps	1003.47 KB	3f19b149f53a50e14fc0b799...
Info	BitTorrent	TCP	192.168.1.5:49785	94.196.230.94.threem... :bctp	12 sec	Server	0 bps	828.33 KB	3f19b149f53a50e14fc0b799...
Info	BitTorrent	TCP	192.168.1.5:49787	feralhosting.com :59905	11 sec	Server	0 bps	802.31 KB	3f19b149f53a50e14fc0b799...
Info	BitTorrent	TCP	192.168.1.5:49792	nqhf166.dediseedbox.... :50726	10 sec	Server	0 bps	707.02 KB	3f19b149f53a50e14fc0b799...
Info	BitTorrent	TCP	192.168.1.5:49781	balticom-244-108.bal... :61080	13 sec	Server	0 bps	517.83 KB	3f19b149f53a50e14fc0b799...
Info	BitTorrent	UDP	192.168.1.5:40959	ryzome.info :51413	12 sec	Server	0 bps	478.25 KB	3f19b149f53a50e14fc0b799...
Info	? Unknown	TCP	net031132099127.psko... :34038	192.168.1.5:40959	11 sec	Client	0 bps	323.26 KB	

Showing 1 to 10 of 226 rows

« < 1 2 3 4 5 > »

Monitoring Copyrighted Content [3/4]

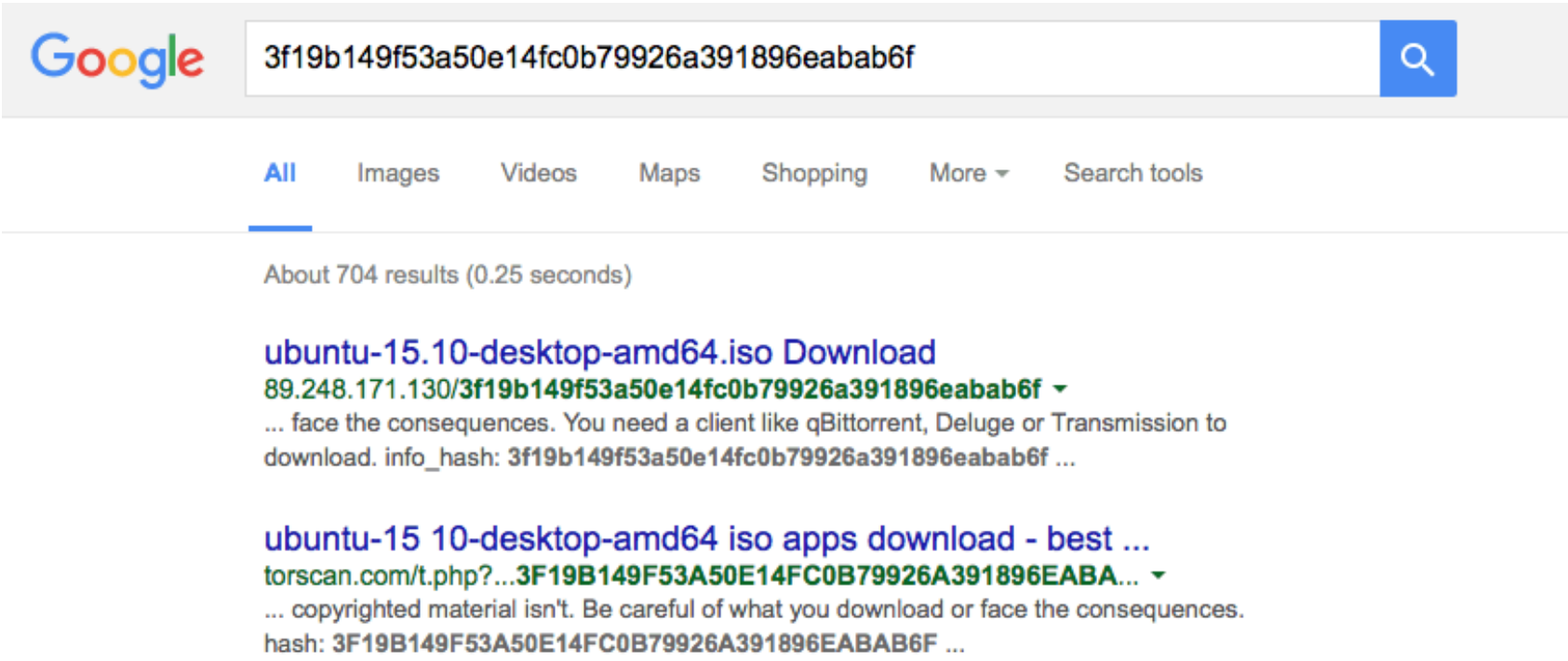
ntop

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

IP Address	VLAN	Alerts	Name	Seen Since	Unknown Traffic Volume	Breakdown	Th	
	0	0		1 h, 43 min, 12 sec	342.8 KB	S Rcvd	3	
	0	0		1 h, 43 min, 12 sec	44.83 KB	Sen 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

Upload Volume
Download Volume
Incoming Flows Count
Outgoing Flows Count

One-way Traffic

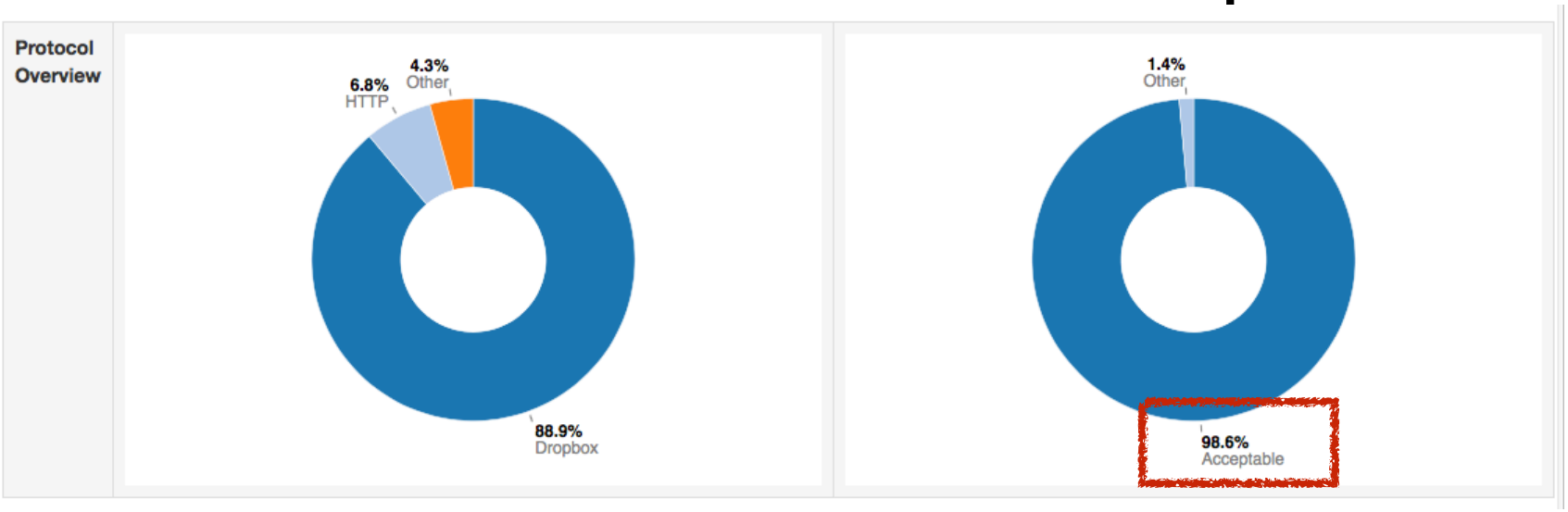
- One way traffic can be a good source of information for understanding suspicious activities based on destination and protocol:
  - Multicast traffic can be exploited for disclosing sensitive information (e.g. SSDP, MDNS)
  - TCP traffic is by nature bi-directional, so one-way TCP flow might indicate 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	1.54 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?

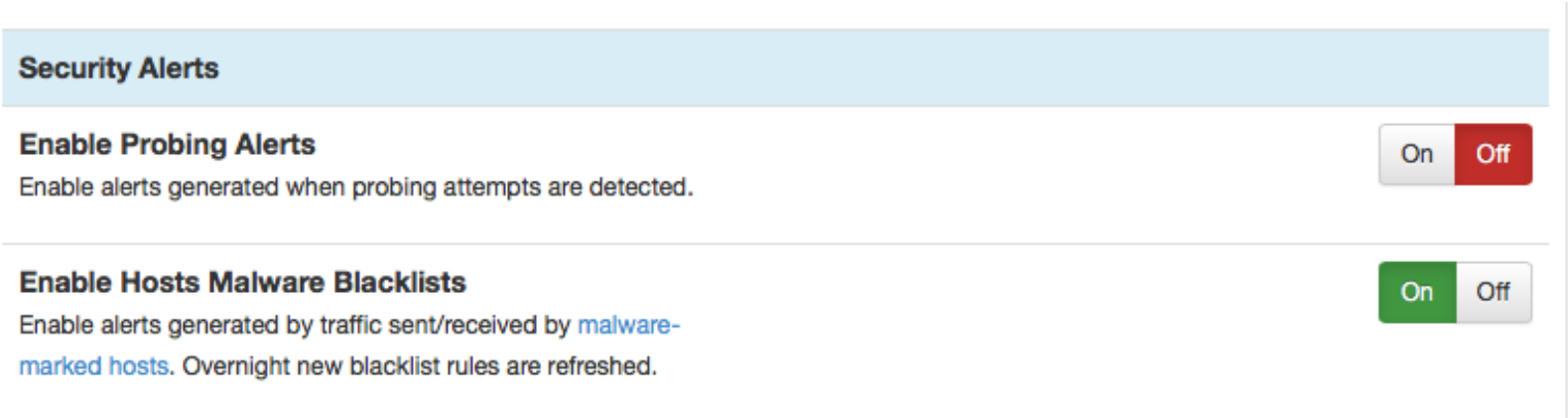
Ingress but no egress traffic: service scan?

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 [TCP 71.6.146.185:49717 > :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 [TCP 93.174.93.30:29162 > :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 ri [TCP 185.35.62.185:60205 > :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

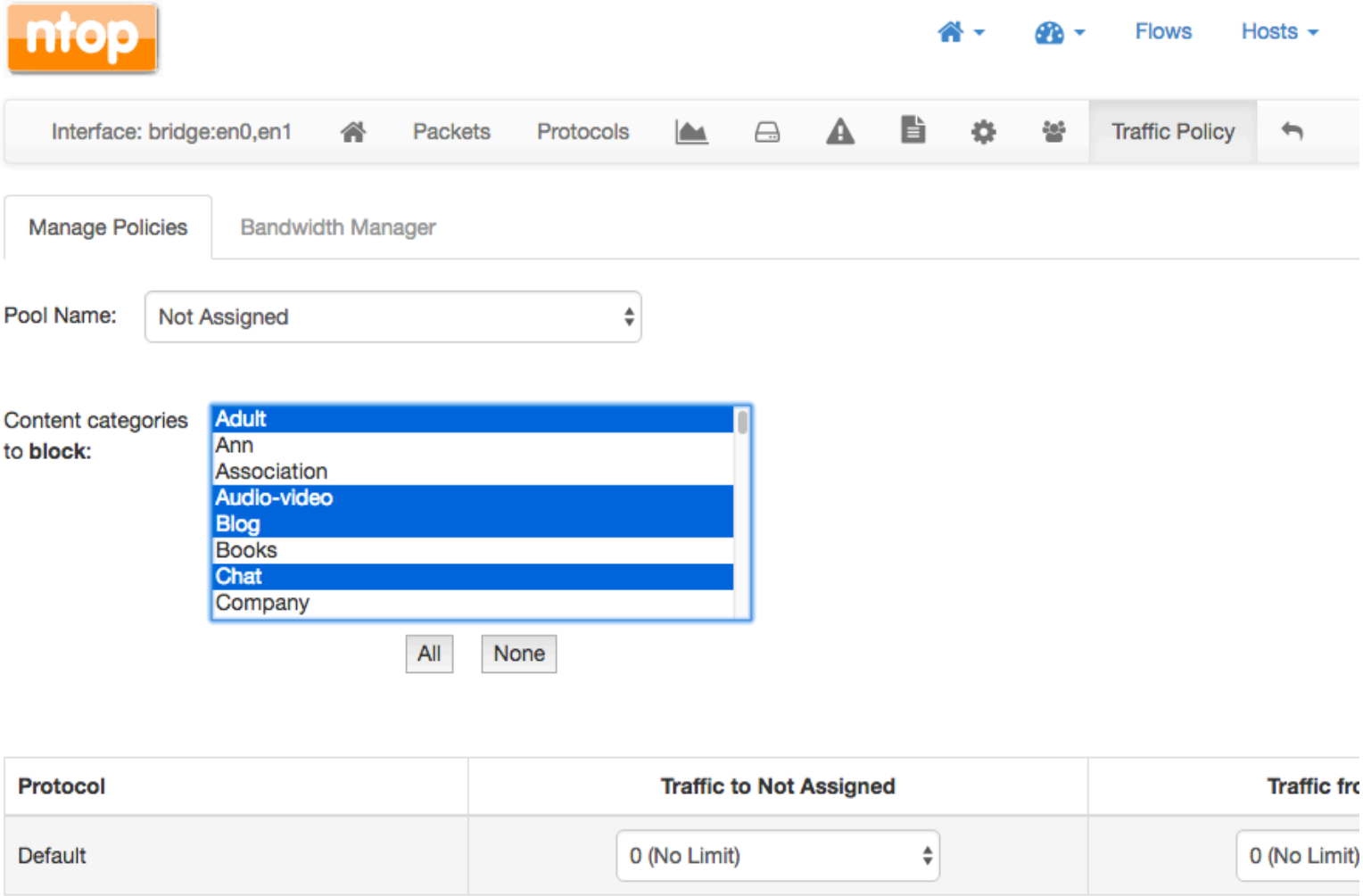
- ntopng has been integrated with a content analysis company to complement layer-7 traffic analysis with content enforcement.
- Go to http://flashstart.ntop.org to get your categorisation key.

Active HTTP Flows

10 Hosts Applications IP Version

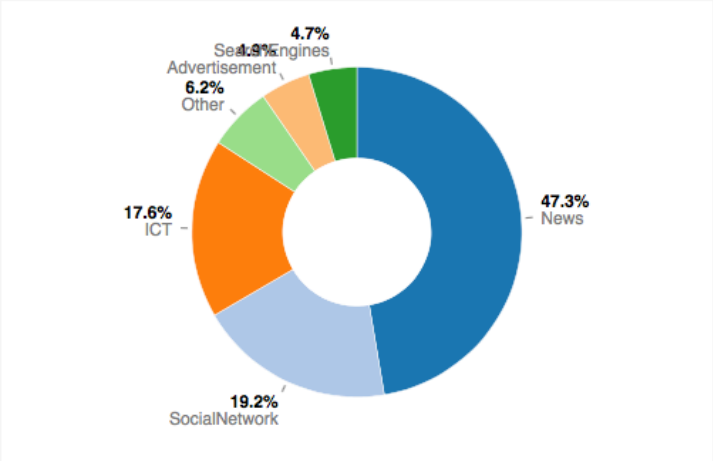
	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	HTTP	TCP	:41620	www.corriere.it:http	2 min, 23 sec	Client Server	0 bps	30.23 KB	/includes2013/SSI/utilit... News
Info	HTTP	TCP	:41618	www.corriere.it:http	2 min, 21 sec	Client Server	0 bps	4.13 KB	/includes_methode/cache/... 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 Server	0 bps	4.75 KB	/methode_image/placehold... ContentServer
Info	HTTP	TCP	:60492	static2.vivimilano.c... :http	2 min, 15 sec	Client Server	0 bps	2.46 KB	/wp-content/uploads/2017... News
Info	HTTP	TCP	:60494	static2.vivimilano.c... :http	2 min, 15 sec	Client Server	0 bps	2.47 KB	/wp-content/uploads/2017... News
Info	HTTP	TCP	:36838	images2.corriereobje... :http	2 min, 15 sec	Client Server	0 bps	1.59 KB	/includes2013/LIBS/cssa... ContentServer
Info	HTTP	TCP	:60490	static2.vivimilano.c... :http	2 min, 15 sec	Client Server	0 bps	2.46 KB	/wp-content/uploads/2017... News
Info	HTTP	TCP	:60496	xml2.corriereobjects... :http	2 min, 15 sec	Client Server	0 bps	1.62 KB	/tools/3a-col-nav/tablet... ContentServer
Info	HTTP	TCP	:60488	static2.vivimilano.c... :http	2 min, 15 sec	Client Server	0 bps	2.44 KB	/wp-content/uploads/2017... 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

Internal Log

Alerts On Syslog
Enable alerts logging on system syslog.
On | Off

Slack Integration

Enable Slack Notification
Toggle the alert notification via slack.
On | Off

Notification Preference Based On Severity
Errors (errors only), Errors and Warnings (errors and warnings, no info), All (every kind of alerts will be notified).
Errors | Errors and Warnings | All

Notification Sender Username
Set the username of the sender of slack notifications
ntopng Webhook

Notification Webhook
Send your notification to this slack URL

Nagios Integration

Send Alerts To Nagios
Enable sending ntopng alerts to Nagios NSCA (Nagios Service Check Acceptor).
On | Off

Staying in Touch

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.

Final Remarks

- Over the past 16 years ntop created a software framework for efficiently monitoring traffic.
- "We have a story to tell you, not just hacks".
- 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/.