Web-Based Traffic Monitoring Using ntopng

Simone Mainardi, PhD
mainardi@ntop.org

Arnhem, The Netherlands • October 17, 2016

ntop meeting

Outlook

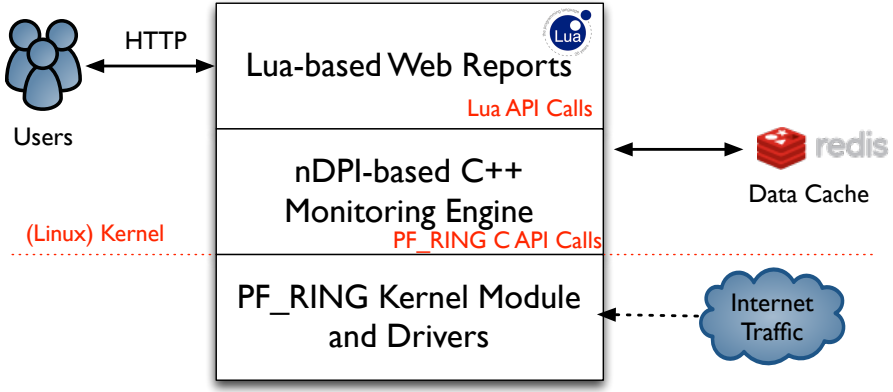
- ntopng architecture and design
- ntopng as a flow collector
- Using ntopng
- Advanced monitoring with ntopng

ntopng Design Goals

- Clean separation between the monitoring engine and the reporting facilities
- Robust, crash-free engine
- 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, categorization, Deep Packet Inspection (DPI)

ntopng Architecture

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



ntopng Monitoring Engine

- Coded in C++ and based on the concept of flow (set of packets with the same 5-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
    - Network
    - High-level Aggregations

Lua-based ntopng Scriptability [1/3]

- A design principle of ntopng is the clean separation of the GUI from engine
- 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`

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

Using ntopng for traffic analysis, troubleshooting, and flow collection

ntop meeting

Using ntopng for traffic analysis, troubleshooting, and flow collection

ntop meeting

Selecting Facebook Traffic

ntop

Flows | Hosts | Devices | Interfaces | Search Host

Active Flows

10 | Applications

	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	SSL.Facebook	TCP	192.168.2.130:64557	scontent-bru2-1.xx.f... :https	9 min, 3 sec	Server	464.94 Kbit ↓	31.57 MB	scontent-bru
Info	SSL.Facebook	TCP	192.168.2.130:60268	scontent-bru2-1.xx.f... :https	22 min, 38 sec	Server	11.59 Kbit ↑	113.02 MB	scontent-bru
Info	SSL.Facebook	TCP	192.168.2.130:58282	www.facebook.com :https	29 min, 18 sec	Client Server	8 Kbit ↑	3.14 MB	www.facebo
Info	Skype	TCP	157.55.56.173 :40007	192.168.2.130:57255	9 min, 9 sec	Client Server	0 bps ↓	35.39 KB	
Info	SSL.WhatsApp	TCP	192.168.2.130:57846	w7.web.whatsapp.com :https	35 min, 48 sec	Client Server	0 bps ↓	58.06 KB	w7.web.whats
Info	SSL.Google	TCP	192.168.2.130:49725	safebrowsing.google.... :https	4 min	Client Server	0 bps —	3.53 KB	safebrowsing.
Info	Skype	TCP	192.168.2.130:50599	40.115.32.252 :50000	2 min, 1 sec	Client Server	0 bps —	23.2 KB	
Info	Skype	TCP	192.168.2.130:50610	40.127.134.228 :50007	2 min, 1 sec	Client Server	0 bps —	9.47 KB	
Info	SSH	TCP	office:ssh	192.168.2.130:54931	58 min, 33 sec	Client Server	0 bps —	27.77 KB	
Info	Unknown	TCP	192.168.2.130:57250	17.172.232.126 :5223	4 sec	Client Serve	0 bps —	704 B	

Showing 1 to 10 of 77 rows

« < 1 2 3 4 5 > »

- All Proto
- Apple
- AppleiCloud
- DNS
- Dropbox
- Facebook
- GMail
- Google
- ICMP
- MDNS
- Microsoft
- SSDP
- SSH
- SSL
- Skype
- Unknown
- WhatsApp

ntop meeting

Analyzing Facebook Traffic

SSL: encrypted Facebook ☺ : fun

DNS: domain Facebook ☺ : fun

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

Active Facebook Flows

10 | Applications

	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	SSL.Facebook ☺	TCP	192.168.2.130:60268	scontent-bru2-1.xx.f... :https	23 min, 17 sec	Server	1.63 Mbit ↑	120.2 MB	scontent-bru2-1.xx.fbcdn...
Info	SSL.Facebook ☺	TCP	192.168.2.130:64557	scontent-bru2-1.xx.f... :https	9 min, 42 sec	Server	671.71 Kbit ↓	35.13 MB	scontent-bru2-1.xx.fbcdn...
Info	SSL.Facebook ☺	TCP	192.168.2.130:58282	www.facebook.com :https	29 min, 59 sec	Client Server	313.92 Kbit ↑	3.54 MB	www.facebook.com
Info	SSL.Facebook ☺	TCP	192.168.2.130:51693	video-bru2-1.xx.fbcd... :https	15 sec	Server	118.14 Kbit ↓	1.39 MB	video-bru2-1.xx.fbcdn.ne...
Info	SSL.Facebook ☺	TCP	192.168.2.130:51696	video-bru2-1.xx.fbcd... :https	1 sec	Client Server	0 bps –	1.44 KB	video-bru2-1.xx.fbcdn.ne...
Info	SSL.Facebook ☺	TCP	192.168.2.130:58308	3-edge-chat.facebook... :https	29 min, 54 sec	Client Server	0 bps ↓	267.3 KB	3-edge-chat.facebook.com...
Info	SSL.Facebook ☺	TCP	192.168.2.130:51692	video-bru2-1.xx.fbcd... :https	1 sec	Client Server	0 bps –	1.44 KB	video-bru2-1.xx.fbcdn.ne...
Info	SSL.Facebook ☺	TCP	192.168.2.130:51695	video-bru2-1.xx.fbcd... :https	1 sec	Client Server	0 bps –	1.44 KB	video-bru2-1.xx.fbcdn.ne...
Info	DNS.Facebook ☺	UDP	192.168.2.130:27276	2-edge-chat.facebook... :domain	< 1 sec	Client Server	0 bps	243 B	2-edge-chat.facebook.com...
Info	SSL.Facebook ☺	TCP	192.168.2.130:51694	video-bru2-1.xx.fbcd... :https	1 sec	Client Server	0 bps –	1.44 KB	video-bru2-1.xx.fbcdn.ne...

Showing 1 to 10 of 13 rows

« < 1 2 > »

certificate name for SSL

A query for DNS

ntop meeting

Inspecting a Facebook Flow

Access to the historical Facebook Flows

Goodput: application level throughput

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

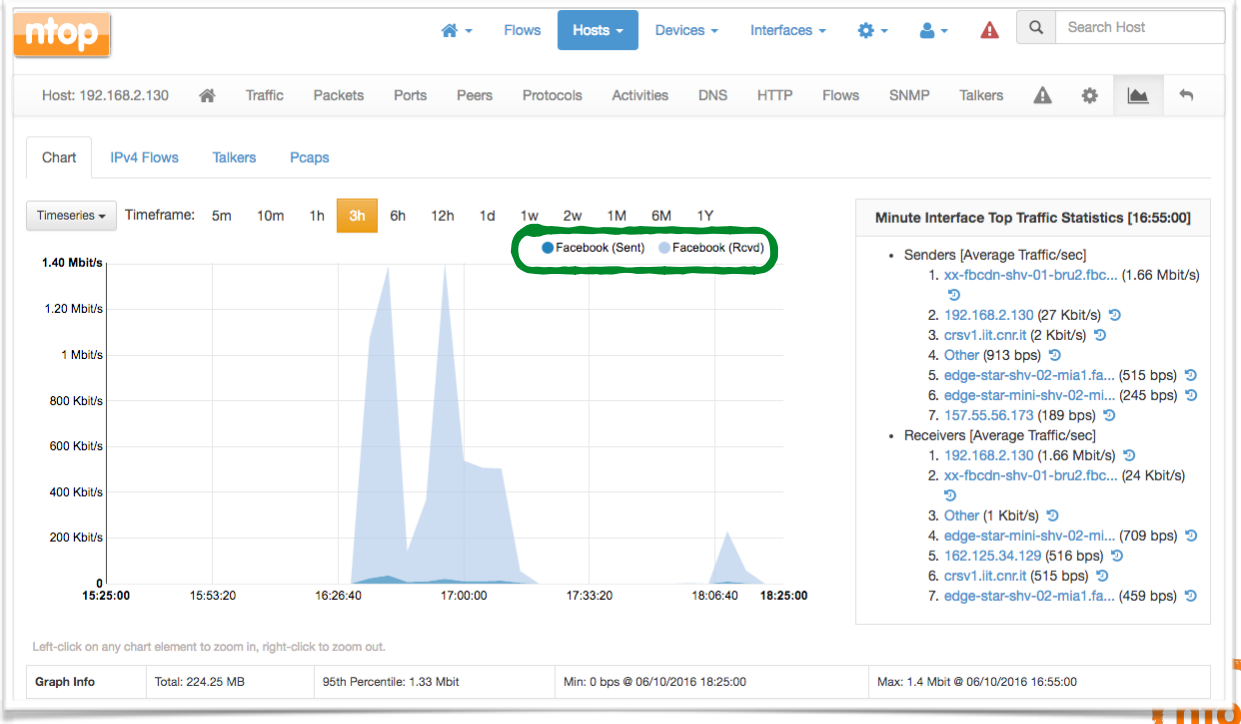
Flow: 192.168.2.130:60268 ⇄ scontent-bru2-1.xx.fbcdn.net:443 | Overview

Flow Peers [Client / Server]	192.168.2.130:60268 [68:5B:35:A7:DE:85] ⇄ scontent-bru2-1.xx.fbcdn.net:443 [04:18:D6:31:EF:5A]	
Protocol	TCP / SSL.Facebook (119)	
First / Last Seen	06/10/2016 15:59:13 [24 min, 3 sec ago]	06/10/2016 16:23:15 [1 sec ago]
Total Traffic	Total: 126.34 MB ↑	Goodput: 118.85 MB (94.1 %) ↑
	Client → Server: 26,244 Pkts / 1.91 MB ↑	Client ← Server: 90,791 Pkts / 124.43 MB ↑
	192 / 179.60.195.12:443	
Network Latency Breakdown	20.966 ms (server)	
Application Latency	45.088 ms	
Packet Inter-Arrival Time [Min / Avg / Max]	Client → Server: < 1 ms / 54 ms / 20 sec	Client ← Server: < 1 ms / 15 ms / 20 sec
TCP Packet Analysis		**Client → Server / Client ← Server**
	Retransmissions	3 Pkts / 5 Pkts
	Out of Order	0 Pkts / 237 Pkts
	Lost	0 Pkts / 35 Pkts
SSL Certificate	scontent-bru2-1.xx.fbcdn.net	
Max (Estimated) TCP Throughput	Client → Server: 778.62 Kbit	Client ← Server: 12.47 Mbit
TCP Flags	Client → Server: SYN PUSH ACK	Client ← Server: SYN PUSH ACK
	This flow is active.	
Flow Status	Normal	
Actual / Peak Throughput	1.12 Mbit ▬ / 16.51 Mbit	

ntop meeting

Historical Facebook Chart

- Layer-7 Application stats are (optionally) stored for local hosts
- Facebook is just one application
- Minute interface top talkers shown as well



Historical Facebook Flows

ntop

Flows | Hosts | Devices | Interfaces | Search Host

Search Criteria

From:	To:	Client/Server Host:	Protocol:	Port:	Info:	Application Protocol:
06/10/2016 15:23:03	06/10/2016 16:23:03	192.168.2.130	Any		scontent-bru2-1.xx.fbcdn.ne	Facebook

Observation Period: 1 h

Search Flows

Summary | IPv4 Flows | Talkers | Pcaps

Search Results

	Total Flows	Traffic Volume	Total Packets	Traffic Rate	Packet Rate
IPv4	26 Flows	194.58 MB	198,601 Pkts	453.27 Kbit	55.15 pps

Application, host, time range, etc.

Results with summary, flows, top talkers, etc

ntop meeting

Historical Facebook Flows

ntop

Flows | Hosts | Devices | Interfaces | Search Host

Search Criteria

From: 06/10/2016 15:23:03 | To: 06/10/2016 16:23:03 | Client/Server Host: 192.168.2.130 | Protocol: Any | Port: | Info: scontent-bru2-1.xx.fbcdn.n | Application Protocol: Facebook

Observation Period: 1 h

Search Flows

Summary | IPv4 Flows | Talkers | Pcaps

5

	Application	L4 Proto	Client	Server	Begin	End	Traffic Sent	Traffic Received	Total Traffic	Info	Avg Thpt
Info	Facebook	TCP	192.168.2.130:60268	xx-fbcdn-shv-01-bru2.fbc...:https	06/10/2016 15:59:13	06/10/2016 16:04:14	572.79 KB	34.91 MB	35.47 MB	scontent-bru2-1.xx.fbcdn.net	985.15 Kbit
Info	Facebook	TCP	192.168.2.130:60268	xx-fbcdn-shv-01-bru2.fbc...:https	06/10/2016 16:19:15	06/10/2016 16:24:16	776.45 KB	33.7 MB	34.46 MB	scontent-bru2-1.xx.fbcdn.net	957.09 Kbit
Info	Facebook	TCP	192.168.2.130:60268	xx-fbcdn-shv-01-bru2.fbc...:https	06/10/2016 16:14:15	06/10/2016 16:19:15	345.23 KB	22.36 MB	22.7 MB	scontent-bru2-1.xx.fbcdn.net	632.69 Kbit
Info	Facebook	TCP	192.168.2.130:60268	xx-fbcdn-shv-01-bru2.fbc...:https	06/10/2016 16:04:14	06/10/2016 16:09:14	242.54 KB	22.44 MB	22.67 MB	scontent-bru2-1.xx.fbcdn.net	631.9 Kbit
Info	Facebook	TCP	192.168.2.130:58466	xx-fbcdn-shv-01-bru2.fbc...:https	06/10/2016 15:59:14	06/10/2016 16:04:14	578.92 KB	19.54 MB	20.11 MB	scontent-bru2-1.xx.fbcdn.net	560.4 Kbit

Showing 1 to 5 of 26 rows

« < 1 2 3 4 5 > »

ntop meeting

Historical Top Facebook Talkers

ntop

Flows | Hosts | Devices | Interfaces | Search Host

Search Criteria

From:	To:	Client/Server Host:	Protocol:	Port:	Info:	Application Protocol:
06/10/2016 15:23:03	06/10/2016 16:23:03	192.168.2.130	Any		scontent-bru2-1.xx.fbcdn.n	Facebook

Observation Period: 1 h

Search Flows

Summary | IPv4 Flows | Talkers | Pcaps

Interface en4 / 192.168.2.130 talkers

Observation period: 1 hour starting on Thursday, October 6th 2016, 3:23:03 pm

10

Host Name	IP Address	Traffic Sent	Traffic Received	Total Traffic	Total Packets	Flows
xx-fbcdn-shv-01-bru2.fbc...	179.60.195.12	224.17 MB	4.86 MB	229.04 MB	234,021	24
157.240.0.35	157.240.0.35	2.31 MB	860.04 KB	3.15 MB	6,021	7
179.60.195.15	179.60.195.15	1.86 MB	96.83 KB	1.96 MB	2,623	25
157.240.0.17	157.240.0.17	72.28 KB	199.45 KB	271.73 KB	1,176	8
131.114.18.19	131.114.18.19	2.02 KB	1.17 KB	3.19 KB	28	14

Showing 1 to 5 of 5 rows

Download flows: IPv4

Extract pcap:

This is the guy that did most Facebook with 192.168.2.130

TXT download or even pcap extraction

ntop meeting

Traffic Analysis: Take Home

- Ability to Inspect Traffic up to the Layer-7
- Realtime flows with information on peers, throughput, TCP status, HTTP requests, SSL/TLS certificates
- Historical charts: bytes, packets per host / network / application protocol / etc
- Ability to record flows and browse / export them according to multiple search criteria.

Using ntopng for traffic analysis, troubleshooting, and flow collection

ntop meeting

Sorting out Network and Security Issues

- Network Issues
  - Application Latency / Round Trip Time / Retransmissions
  - Bandwidth usage
  - Top Talkers / AS / Networks / Countries / OSes etc.
- Security Issues
  - Scans / SYN floods / flow floods
  - post-mortem analyses of trace files to investigate security incidents

Analysing Traces of a Security Incident

- ntopng is able to process pcap trace files and visualise them as if they were live captures
- `ntopng -i /path/to/the/capture.pcap`
- Looking at the issue from an additional perspective
    - Wireshark offers a **packet-centered** view
    - ntopng offers a **flow-centered** view

Getting the Traces

- Incident: http://www.malware-traffic-analysis.net/2016/09/20/index.html
- Trace: 2016-09-20-traffic-analysis-exercise.pcap
- Courtesy of Brad (@malware_traffic malware-traffic-analysis.net)
- What happened?

Skimming the Flows

- Navigate to the flows page
- Sort by total bytes

ntop | Flows | Hosts | Interfaces | Search Host

✔ 2016-09-20-traffic-analysis-exercise.pcap

Flows

HTTP *Host:* contacted

Almost all server-2-client (download?)

Requested GET location

10 | Applications

	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	HTTP	TCP	192.168.8.134:50496	fungasoap.net :http	2 sec	Server	0 bps	191.55 KB	/67SELbosjc358
Info	SSL.Microsoft	TCP	192.168.8.134:50481	v10.vortex-win.data.... :https	1 min, 3 sec	Client Se	0 bps	32.27 KB	v10.vortex-win.data.micr...
Info	SSL.Microsoft	TCP	192.168.8.134:50480	v10.vortex-win.data.... :https	2 sec	Client Se	0 bps	27.01 KB	v10.vortex-win.data.micr...
Info	HTTP.Microsoft	TCP	192.168.8.134:50488	dmd.metaservices.mic... :http	1 min, 39 sec	Client Server	0 bps	24.71 KB	/dms/metadata.svc
Info	SSL	TCP	192.168.8.134:50499	f5xraa2y2ybtrefz.tor... :https	5 sec	Cl Server	0 bps	21.21 KB	f5xraa2y2ybtrefz.tor2web...
Info	SSL.Microsoft	TCP	192.168.8.134:50497	licensing.mp.microso... :https	2 sec	Clie Server	0 bps	14.47 KB	licensing.mp.microsoft.c...
Info	SSL.Microsoft	TCP	192.168.8.134:50486	sqm.telemetry.micros... :https	2 min, 4 sec	Client Server	0 bps	9.13 KB	sqm.telemetry.microsoft....
Info	SSL.Microsoft	TCP	192.168.8.134:50498	iecvlist.microsoft.c... :https	1 sec	Cl Server	0 bps	8.63 KB	iecvlist.microsoft.com
Info	SSL	TCP	192.168.8.134:50494	nexus.officeapps.liv... :https	1 min, 50 sec	Cl Server	0 bps	7.98 KB	nexus.officeapps.live.co...
Info	SSL	TCP	192.168.8.134:50495	nexusrules.officeapp... :https	1 min, 46 sec	Cl Server	0 bps	7.69 KB	nexusrules.officeapps.li...

Showing 1 to 10 of 72 rows

« < 1 2 3 4 5 > »

Googling Around…

ntop

Flows | Hosts | Interfaces | Search Host

Flows

10 | Applications

	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	HTTP	TCP	192.168.8.134:50496	fungasoap.net :http	2 sec	Server	0 bps	191.55 KB	/67SELbosjc358

Google

fungasoap.net

Tutti | Immagini | Notizie | Shopping | Maps | Altro | Strumenti di ricerca

Circa 66.200 risultati (0,51 secondi)

Forse cercavi: ***www.fungasoap***.net

FungaSoap.net
fungasoap.net/ Traduci questa pagina

Locky Distribution Site: fungasoap.net - Ransomware Tracker - Abuse.ch
https://ransomwaretracker.abuse.ch/host/**fungasoap.net/** Traduci questa pagina
Locky Distribution Site: **fungasoap.net**. Threat: Distribution Site. Malware: Locky. Host Status: offline. Blacklist check: Spamhaus DBL: Not Listed. SURBL ...

www.fungasoap.net - FungaSoap.net - Web Site Archive
www.websitarchive.com/www.**fungasoap.net** Traduci questa pagina
03 ago 2016 - World ranking 0 altough the site value is $0. **fungasoap.net** IP is 209.200.244.79 on Apache/2.2.3 (CentOS) server works with 437 ms speed.

Google

67SELbosjc358

Tutti | Maps | Immagini | Video | Notizie | Altro | Strumenti di ricerca

Circa 571 risultati (0,24 secondi)

Обліковий запис VirusTotal Спільноти для JaGui - VirusTotal
https://www.virustotal.com/uk/user/JaGui/ Traduci questa pagina
07 lug 2015 - http://heritagebaptistchurch.ca/**67SELbosjc358** ... http://judgedeborahshallcross.com/**67SELbosjc358** ... http://zheng-du.com/**67SELbosjc358** ...

Dynamoo's Blog: Malware spam: "Order: 28112610/00 - Your ref ...
blog.dynamoo.com/.../malware-spam-order-2811261000-your-... Traduci questa pagina
19 set 2016 - bernardchandran.com/**67SELbosjc358** bobneal.net/**67SELbosjc358** burgeoservise.ru/**67SELbosjc358** dirkdj.nl/**67SELbosjc358**

Locky Distribution Site: puchipuchivirus.com - Ransomware Tracker
https://ransomwaretracker.abuse.ch/host/puchipuchivirus.com/ Traduci questa pagina
2016-09-30 12:02:38. http://puchipuchivirus.com/vvkqo7, Distribution Site, Locky. 2016-09-19 11:12:42. http://puchipuchivirus.com/**67SELbosjc358**, Distribution ...

download - Ransomware Tracker - Abuse.ch
https://ransomwaretracker.abuse.ch/.../LY_DS_URLBL.txt Traduci questa pagina
... http://fungasoap.net/**67SELbosjc358** http://puchipuchivirus.com/**67SELbosjc358** http://burgeoservise.ru/**67SELbosjc358** http://techscape4.com/**67SELbosjc358** ...

Locky Distribution Site: win88id.com - Ransomware Tracker - Abuse.ch
https://ransomwaretracker.abuse.ch/host/win88id.com/ Traduci questa pagina
19 set 2016 - Locky Distribution Site: win88id.com. Threat: Distribution Site. Malware: Locky. URL: http://win88id.com/**67SELbosjc358**. Host Status: offline.

Last 1 reports on IP 117.53.152.232 - urlquery.net - Free url scanner
urlquery.net/report.php?id=1474372193277 Traduci questa pagina
20 set 2016 - URL, bernardchandran.com/**67SELbosjc358**. IP, 117.53.152.232. ASN, AS46015 Exa Bytes Network Sdn.Bhd. Location, Malaysia.

Last 6 reports on ASN: AS46606 Unified Layer - urlquery.net - Free url ...
urlquery.net/report.php?id=1474284169322 Traduci questa pagina
19 set 2016 - URL, knaravan.org/**67SELbosjc358**. IP, 69.89.20.51. ASN, AS46606 Unified Layer. Location, United States. Report completed, 2016-09-19 ...

AV: Trojan[Downloader]/VBS.Agent.bzo | ThreatMiner.org
https://www.threatminer.org/av.php?q.../VBS.Agent.bzo Traduci questa pagina
URL: **/67SELbosjc358**. MD5: 8b79afd000acc50510c847ffe0408201. Filename: OffOrd_55337490-00-3583920-2509.docm. File size: 26466 bytes, 2016-09-21 ...

ntop meeting

Security Incident: Summary

- Reasonable evidence that the host is the victim of locky ransomware
- Ransomware has been downloaded through mail attachment
- no need to use other files (e.g., .eml, .docm, .dll)

Dynamoo's Blog

Malware, spam, scams and random stuff, by Conrad Longmore.

Blogger.com | Dynamoo's Blog | Dynamoo.com | Get Updates on Twitter

Sponsored by..

Monday, 19 September 2016

Malware spam: "Order: 28112610/00 - Your ref.: 89403" leads to Locky

This fake financial spam has a malicious attachment that leads to Locky ransomware.

Subject: Order: 28112610/00 - Your ref.: 89403
From: Melba lochhead (SALES1@krheadshots.com)
Date: Monday, 19 September 2016, 16:05

Dear customer,

Thank you for your order.

Please find attached our order confirmation.

Should you be unable to open the links in the document, you can download the latest version of Adobe Acrobat Reader for free via the following link: http://www.adobe.com/products/acrobat/readstep2.html

Should you have any further questions, do not hesitate to contact me.

Kind Regards,

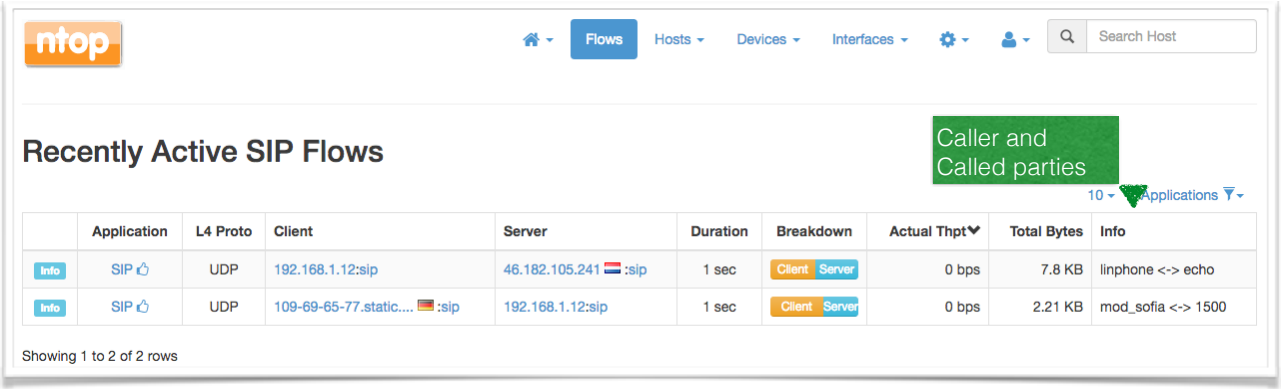
It drops a DLL which had a moderate detection rate earlier. This version of Locky does not communicate with C2 servers, so if you want to block or monitor traffic perhaps you should use the string *67SELbosjc358*.

Monitoring VoIP Calls

- ntopng can be used to visualize VoIP calls
- Visualization of SIP and RTP that are the de-facto standards in the VoIP industry

SIP

- SIP is a signalling protocol used by the call parties to negotiate parameters such as
  - Encoding
  - RTP addresses and Ports
  - etc



A SIP Flow

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

Flow: 192.168.1.12:5060 ⇄ 46.182.105.241:5060 | Overview

Flow Peers [Client / Server]	192.168.1.12:5060 ⇄ 46.182.105.241:5060	
Protocol	UDP / SIP (100)	
First / Last Seen	14/10/2016 19:25:13 [< 1 sec ago]	14/10/2016 19:25:14 [< 1 sec ago]
Total Traffic	Total: 7.80 KB	
	Client → Server: 5 Pkts / 3.96 KB	Client ← Server: 7 Pkts / 3.84 KB
	192.168.1.12:5060	46.182.105.241:5060
Actual / Peak Throughput	0 bps / 0 bps	
SIP Protocol Information		
Call-ID	32145	
Call Initiator ⇄ Called Party	linphone ⇄ echo	
RTP Stream Peers (src ⇄ dst)	192.168.1.12:7078 ⇄ 46.182.105.241:30270 RTP Flow	
Call State	Call Completed	
Additional Flow Elements		
Total number of exported flows	2	

Call-ID

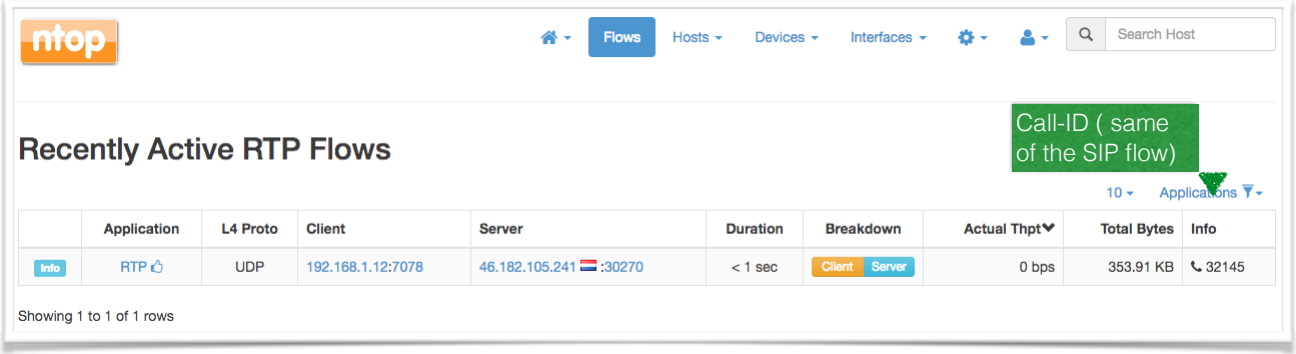
Negotiated RTP Stream Peers

Ability to jump to the RTP Flow

ntop meeting

RTP

- RTP is the transport protocol actually used to carry the voice



An RTP Flow

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

Flow: 192.168.1.12:7078 ⇄ 46.182.105.241:30270 | Overview

Flow Peers [Client / Server]	192.168.1.12:7078 ⇄ 46.182.105.241:30270	
Protocol	UDP / RTP (87)	
First / Last Seen	14/10/2016 17:19:23 [< 1 sec ago]	14/10/2016 17:19:23 [< 1 sec ago]
Total Traffic	Total: 353.91 KB	
	Client → Server: 906 Pkts / 176.95 KB	Client ← Server: 906 Pkts / 176.95 KB
	192.168.1.12:7078	46.182.105.241:30270
Actual / Peak Throughput	0 bps / 0 bps	
RTP Protocol Information		
Round Trip Time	39.995 ms	
SIP Call-ID	32145	
Call Quality Indicators	**Forward**	**Reverse**
Jitter	19.976 ms	19.975 ms
Lost Packets	0 Pkts	0 Pkts
Dropped Packets	0 Pkts	0 Pkts
Max Packet Interarrival Time	10.29 ms	10.29 ms
Payload Type	PCMA	PCMA
(Pseudo) MOS	4.36 Desirable	4.36 Desirable
R-Factor	90.95 Desirable	90.95 Desirable

Call Quality Indicators

ntop meeting

Using ntopng for traffic analysis, troubleshooting, and flow collection

ntop meeting

Flow Collection with ntopng and nProbe

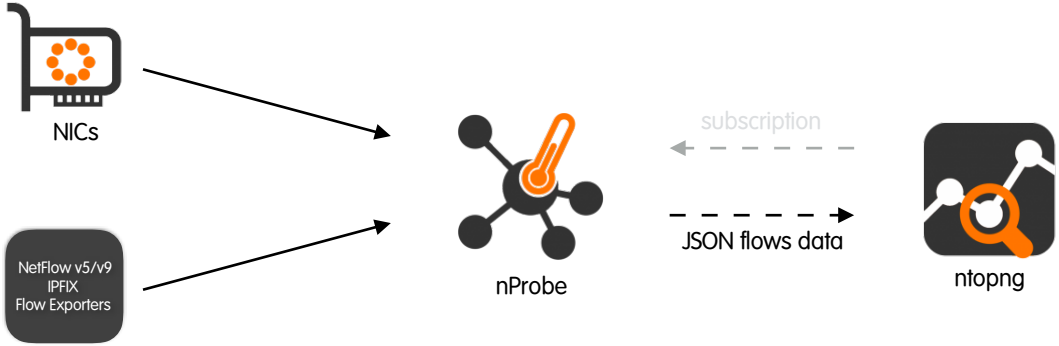
- nProbe (a home-grown NetFlow/sFlow collector/probe) is responsible for collecting/generating flows and convert them to JSON so that ntopng can understand it
- The communication ntopng <-> nProbe is over ØMQ a simple/fast messaging system that allows the two peers to be decoupled while:
    - Avoiding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

ØMQ Communications

- Flows are sent in the following format
  - {"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)
- Multiple collectors can connect to the same probe.
- No traffic is created when no collector is attached to the probe.

Advanced Flow Collection: A Diagram

- nProbe capture packets from NICs and talks with NetFlow/IPFIX/sFlow/etc exporters
- ntopng subscribes with the nProbe for a 'flows' topic
- nProbe periodically (1 second) pushes data for the subscribed topic

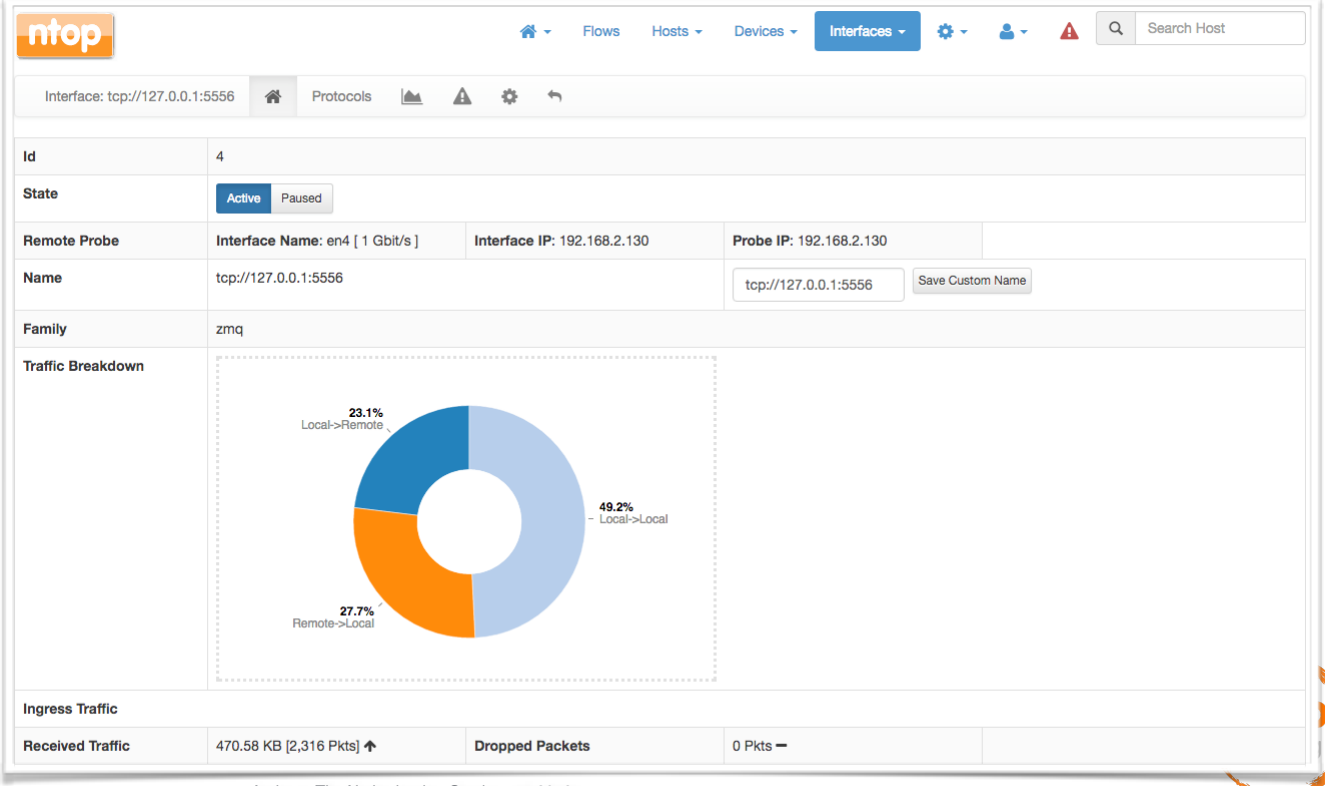


Configuring ntopng and nProbe

- nProbe
  - Packet Capture
    - `./nprobe --zmq "tcp://*:5556" -i en4 -n none`
  - *Flow collection
    - `./nprobe --zmq "tcp://*:5556" -i none -n none --collector-port 2055`
- ntopng
  - `./ntopng -i "tcp://127.0.0.1:5556"`

Visualising the Remote Interface

- Remote probe interface name, speed and ip addresses
- Treated by ntopng as if it was a local interface



Visualising Remotely Monitored Flows

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

Recently Active Skype Flows

5 | Applications

	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	Skype	UDP	192.168.2.130:33807	157.55.235.145 :40010	< 1 sec	Server	276.38 bps	1.11 KB	
Info	Skype	UDP	192.168.2.130:33807	157.56.52.36 :40002	< 1 sec	Client Server	60.18 bps	248 B	
Info	Skype	UDP	192.168.2.130:33807	157.55.56.174 :40007	< 1 sec	Client Serv	56.54 bps	233 B	
Info	Skype	UDP	192.168.2.130:33807	157.55.130.159 :40010	< 1 sec	Client Serv	56.29 bps	232 B	
Info	Skype	UDP	192.168.2.130:33807						

Showing 1 to 5 of 10 rows

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

Flow: 192.168.2.130:17500 ⇄ 192.168.2.255:17500 | Overview

Flow Peers [Client / Server]	192.168.2.130:17500 ⇄ 192.168.2.255:17500	
Protocol	UDP / Dropbox (121)	
First / Last Seen	07/10/2016 16:50:23 [6 min, 11 sec ago]	07/10/2016 16:55:54 [40 sec ago]
Total Traffic	Total: 6.82 KB	
	Client → Server: 24 Pkts / 6.82 KB	Client ← Server: 0 Pkts / 0 Bytes
	192.168.2.130:17500	
Actual / Peak Throughput	154.82 bps / 154.99 bps	

ntop meeting

Flow Collection: Take Home

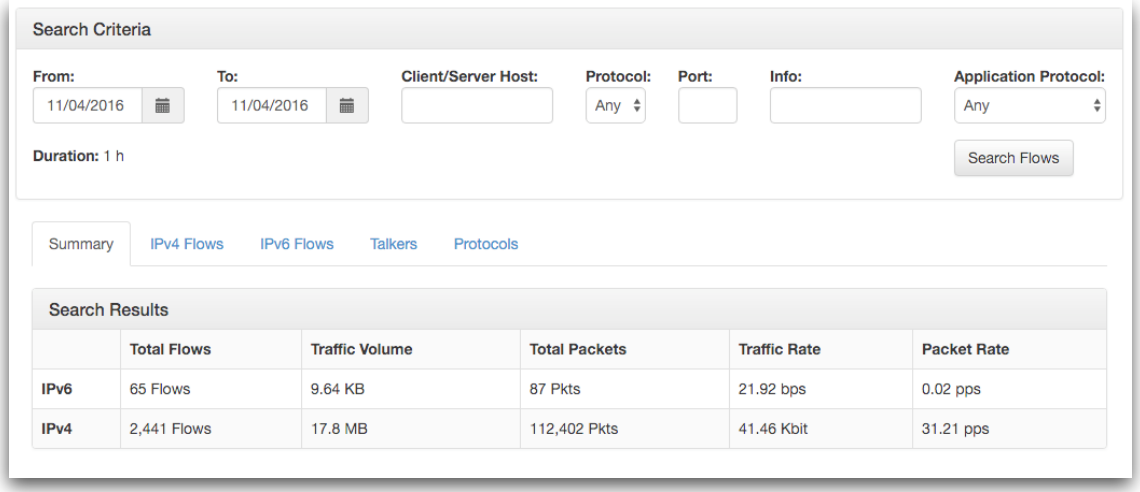
- Flow protocols implementation logic on the nProbe
- ntopng focuses on statistics/aggregation of the received data
- Simple JSON-over-ZMQ flows data nProbe -> ntopng
- Optional support for encryption and compression

Thank You!

Simone Mainardi, PhD
mainardi@ntop.org

Historical Flow Navigation

- 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 Talkers

- 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
- Flows matching inspection criteria can be downloaded at any stage

Drilling Down Historical Talkers [1/2]

Chart | IPv4 Flows | IPv6 Flows | Talkers | Protocols

Interface en4

10

Host Name	IP Address	Traffic Sent	Traffic Received	Total Traffic	Total Packets	Flows
192.168.2.130	192.168.2.130	122.34 MB	27.32 MB	149.66 MB	338,326	17,123

Chart | IPv4 Flows | IPv6 Flows | Talkers | Protocols

Interface en4 / 192.168.2.130 talkers

10

Host Name	IP Address	Traffic Sent	Traffic Received	Total Traffic	Total Packets	Flows
devel	192.168.2.222	54.74 MB	95.36 MB	150.1 MB	954,233	70,473

Chart | IPv4 Flows | IPv6 Flows | Talkers | Protocols

Interface en4 / 192.168.2.130 talkers / Applications between 192.168.2.130 and 192.168.2.222

10

Application	Total Traffic	Packets	Flows
SSL	34.56 MB	202,780	14,671

ntop meeting

Drilling Down Historical Talkers [2/2]

Chart | IPv4 Flows | IPv6 Flows | Talkers | Protocols

Interface en4 / 192.168.2.130 talkers / Applications between 192.168.2.130 and 192.168.2.222

10

Application	Total Traffic	Packets	Flows
SSL	34.56 MB	202,780	14,671

Chart | IPv4 Flows | IPv6 Flows | Talkers | Protocols

Interface en4 / 192.168.2.130 talkers / Applications between 192.168.2.130 and 192.168.2.222 / Application flows

10

	Application	L4 Proto	Client	Server	Begin	End	Traffic	Info	Avg Thpt
Info	SSL	TCP	192.168.2.130:49567	devel:https	24/05/2016 17:54:44	24/05/2016 17:54:47	354.83 KB	test2	726.69 Kbit
Info	SSL	TCP	192.168.2.130:50998	devel:https	24/05/2016 17:55:35	24/05/2016 17:55:35	294.93 KB	test2	2.42 Mbit

ntop meeting

Historical Applications

- 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
- Flows matching inspection criteria can be downloaded at any stage

Drilling Down Historical Applications [1/2]

Chart | IPv4 Flows | IPv6 Flows | Talkers | Protocols

Interface en4

10

Application	Total Traffic	Packets	Flows
SSL	154.05 MB	961,762	70,667
? Unknown	69.76 MB	73,394	157
QUIC			
DropBox			
Google			

Chart | IPv4 Flows | IPv6 Flows | Talkers | Protocols

Interface en4 / DropBox talkers

10

Host Name	Address	Traffic Sent	Traffic Received	Total Traffic	Packets	Flows
192.168.2.130	192.168.2.130	2.56 MB	277.63 KB	2.83 MB	3,981	79
45.58.74.161	45.58.74.161	55.92 KB	1.07 MB	1.13 MB	1,423	4

Chart | IPv4 Flows | IPv6 Flows | Talkers | Protocols

Interface en4 / DropBox talkers / DropBox talkers with 192.168.2.130

10

Host Name	Address	Traffic Sent	Traffic Received	Total Traffic	Packets	Flows
45.58.74.161	45.58.74.161	55.92 KB	1.07 MB	1.13 MB	1,423	4
108.160.173.162	108.160.173.162	52.04 KB	1.04 MB	1.09 MB	1,324	4
ec2-52-21-57-191.compute...	52.21.57.191	10.67 KB	200.5 KB	211.17 KB	241	1

Drilling Down Historical Applications [2/2]

Chart | IPv4 Flows | IPv6 Flows | Talkers | Protocols

Interface en4 / DropBox talkers / DropBox talkers with 192.168.2.130

10

Host Name	Address	Traffic Sent	Traffic Received	Total Traffic	Packets	Flows
45.58.74.161	45.58.74.161	55.92 KB	1.07 MB	1.13 MB	1,423	4
108.160.173.162	108.160.173.162	52.04 KB	1.04 MB	1.09 MB	1,324	4
ec2-52-21-57-191.compute.						

Chart | IPv4 Flows | IPv6 Flows | Talkers | Protocols

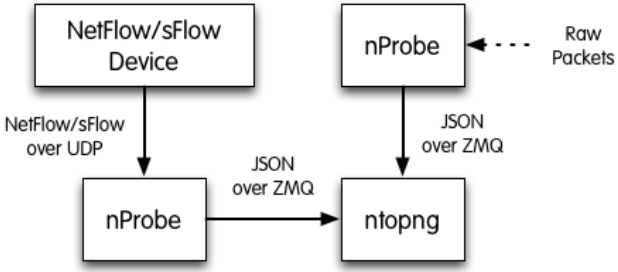
Interface en4 / DropBox talkers / DropBox talkers with 192.168.2.130 / DropBox protocol flows between 192.168.2.130 and 45.58.74.161

10

	Application	L4 Proto	Client	Server	Begin	End	Traffic	Info	Avg Thpt
Info	DropBox	TCP	192.168.2.130:49333	45.58.74.161:https	24/05/2016 18:02:38	24/05/2016 18:02:40	431.58 KB	test2	1.18 Mbit
Info	DropBox	TCP	192.168.2.130:49332	45.58.74.161:https	24/05/2016 18:02:38	24/05/2016 18:02:39	317.04 KB	test2	1.3 Mbit
Info	DropBox	TCP	192.168.2.130:49334	45.58.74.161:https	24/05/2016 18:02:38	24/05/2016 18:02:41	278.95 KB	test2	571.3 Kbit
Info	DropBox	TCP	192.168.2.130:49363	45.58.74.161:https	24/05/2016 18:02:38	24/05/2016 18:02:40	125.96 KB	test2	343.97 Kbit

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.



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`

Advanced Flow Collection with ntopng and nProbe [1/2]

- ntopng uses a poll-mode architecture to fetch flows data from nProbe
- fetched data is pure JSON
- nProbe implements flow protocols (e.g., IPFIX/NetFlow v5-v9-v10 sFlow, etc.) and deals with flow export devices (e.g., routers/switches)

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 considere erfaces.

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 harvest
- Users c

Packet Processing Journey

1. Packet capture: PF_RING (Linux) or libpcap
2. Packet decoding: no IP traffic is accounted
3. IPv4/v6 Traffic only
    1. Map the packet to a 6-tuple flow and increment stats
    2. Identify source/destination hosts and increment stats
    3. Use nDPI to identify the flow application protocol
        1. UDP flows are identified in no more than 2 packets
        2. 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