

# Say Hello To ntopng 4.0

Cybersecurity, Scripting... and a New User Interface

# Agenda

- ntopng 4.0: some numbers
- Motivation
- Main breakthroughs
  - New look-and-feel
  - Cybersecurity-related features
  - Active monitoring
  - Plugins
- Additional features
- Conclusions

# ntopng 4.0: Some Numbers

- **One and half years** after ntopng 3.8
- **Community** 
  - 3,688 files changed
  - 438,746 insertions / 238,350 deletions
- **Pro/Enterprise**
  - 329 files changed
  - 14,904 insertions / 10,273 deletions

# ntopng 4.0: Motivation [1/3]

- Refresh its **look-and-feel**
  - Modern look, customizable, more intuitive, optimized for wide-screens
- Focused on **cybersecurity**
  - Augment network data with security intelligence indicators

# ntopng 4.0: Motivation [2/3]

- **Simplify the analysis of heterogeneous traffic**
  - Ability to create interfaces on-the-fly, matching certain patterns of traffic
- Support for **active monitoring**
  - Don't just passively look at what's on the network
  - Probe the network to make sure it behaves as expected

# ntopng 4.0: Motivation [3/3]

- Make it more **extensible** to **facilitate** community contributions
  - Easier for users and practitioners to extend ntopng functionalities without touching its core

# A Refreshed Look-and-Feel

# The New Web UI

The screenshot illustrates the transition from the original ntopng interface to the new web-based user interface.

**Left Side:** A vertical menu bar on the left contains icons for Dashboard, Alerts, Flows, Hosts, Interface, Settings, Developer, and Help. An orange arrow points from the text "Vertical Menu on the Left" to the top of this menu.

**Top Bar:** The top navigation bar includes a "WAN" dropdown, a status summary (182.20 bit/s, 120.80 Mbit/s), a flow count (9 flows), a device count (41 devices), and a total flow count (5,449 flows). To the right is a search bar and a user profile icon. An orange arrow points from the text "Always-Visible Status Bar" to the top right corner of the dashboard area.

**Traffic Dashboard:** The main content area displays four panels: "WAN: Top Local Talkers", "Actual Traffic" (with a chart showing 17.07 kbit/s up and 11.22 kbit/s down), "WAN: Realtime Top Application Traffic" (chart showing IMAPS, Google, GitHub, and Facebook traffic), and "Network Interfaces: Realtime Traffic" (chart showing Guest Network, Internal Network, WAN, and Office-Sensor traffic).

**Comparison View:** To the right, a separate window shows the same data from the old ntopng interface, highlighting the differences in layout and design.

**Bottom:** The footer includes the ntop logo, version information (ntopng Enterprise Edition v0.9.191114), and system statistics (CPU: 52.10 kHz, RAM: 25.2 ppm, Disk: 00:05:58 -0500 | Usage: 38:57, CPU: 52.10 kHz, RAM: 25.2 ppm, Disk: 00:05:58 -0500 | Usage: 38:57).

Vertical Menu on the Left

# The New Web UI: Skins

The screenshot displays the ntop web interface across three distinct skins, illustrating the visual variety available to users. Each skin maintains a consistent layout with a left sidebar and a main dashboard area.

**Left Sidebar (Common to all skins):**

- WAN: Top Local Talkers
- WAN: Top Remote Destinations
- sFlow: Top Local Talkers
- sFlow: Top Remote Destinations
- Actual Traffic
- WAN: Realtime Top Application Traffic
- Network Interfaces: Realtime Traffic
- WAN: Top Remote Destinations
- Actual Traffic
- WAN: Top Application Traffic Last Day View
- Network Interfaces: Last Day View

**Skin 1 (Dark Skin):** The first skin features a dark background with light-colored text and blue highlights. It includes a navigation bar at the top with links for WAN, sFlow, Alerts, Flows, Hosts, Interface, Settings, Developer, and Help.

**Skin 2 (Light Skin):** The second skin has a light gray background with dark text and orange highlights. It includes a navigation bar at the top with links for WAN, sFlow, Alerts, Flows, Hosts, Interface, Settings, Developer, and Help.

**Skin 3 (White Skin):** The third skin uses a white background with black text and orange highlights. It includes a navigation bar at the top with links for WAN, sFlow, Alerts, Flows, Hosts, Interface, Settings, Developer, and Help.

**Bottom Navigation Bar:**

ntop

© 2020 - ntop.org

9

# Focus on Cybersecurity

# Cybersecurity: Why?

- **Increasingly relevant** in any environment (corporate, SMEs, SOHO, home)
  - Protection of data is fundamental - and now also requested by law
- **Increasingly difficult** as
  - There is no longer a clear line dividing the good from the bad
    - Think to people carrying personal devices at work
  - A large part of the traffic is encrypted
    - Hard to understand what is in it

# ntopng 4.0 and Cybersecurity

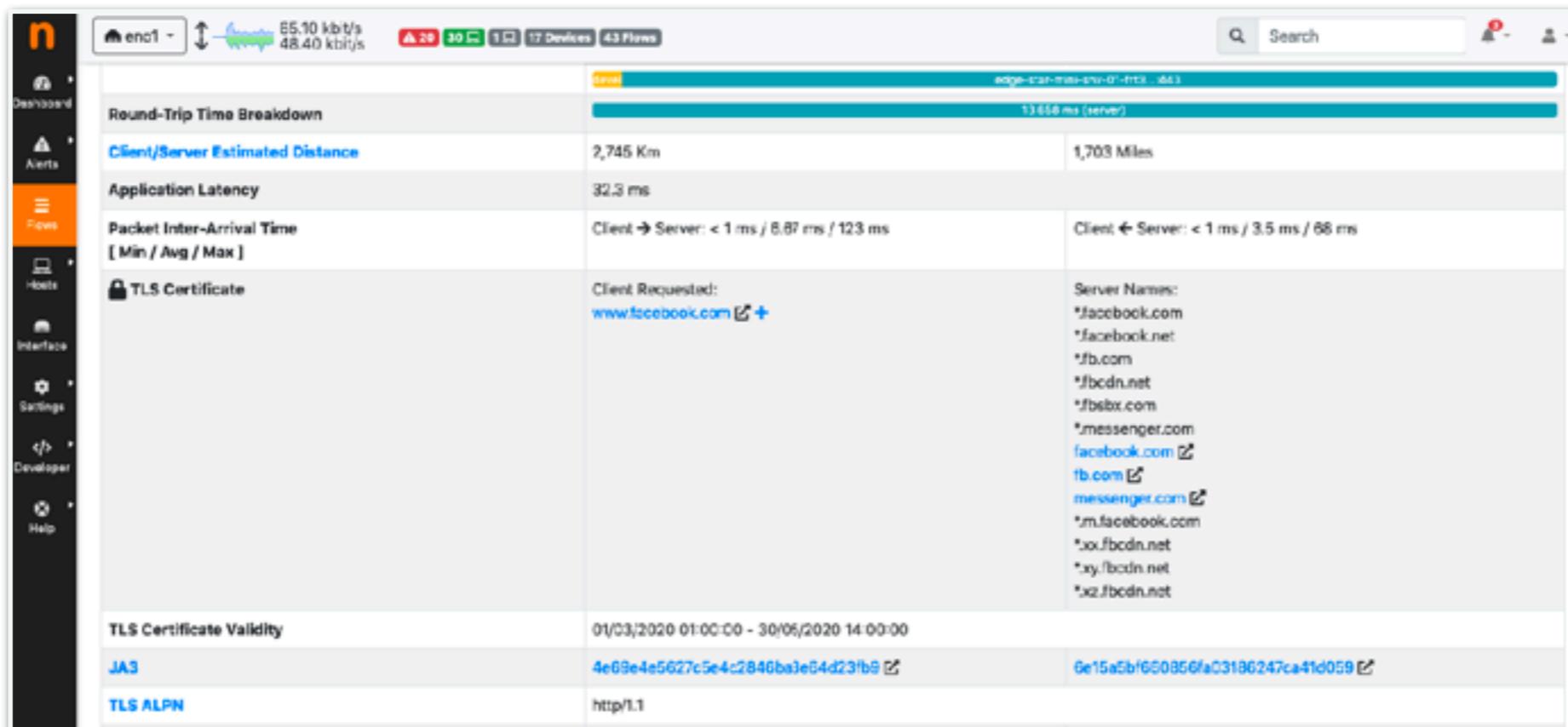
- **Behavioral protocol analyses** for encrypted and non-encrypted protocols, e.g.,
  - A Dropbox flow is uploading data outside the company network
  - A DNS query contains suspicious names
  - A TLS is likely originated by a malware application
- Generate **alerts** when suspicious traffic is found

# Behavioral Protocol Analyses

- Aim is to **assess** (to some extent)
  - How protocols are **(ab)used**
- Encrypted protocols (e.g., TLS) are not decrypted
  - Decryption is unpractical

# TLS Analysis

- Certificates analysis
  - Names, Validity
- Robustness of encryption



# TLS Analysis: Alerts

The screenshot displays two main sections of the ntopng web interface:

**Flow Alerts (Top Section):**

- Header:** Shows interface en0 with 36.10 kbit/s traffic, 145 Flows, and 1 ntopng maintenance expired alert.
- Alert Types:** Engaged Alerts, Past Alerts, Flow Alerts.
- Table:** Shows a single alert entry: Date/Time (26/03/2020 17:59:30), Duration, Count (1), Severity (Error), Alert Type (Potentially Dangerous Protocol), Score (50), Drilldown, Description (TLS Certificate Expired [16/05/2019 13:54:31 - 14/08/2019 13:54:31] [Flow: MACBOOKPRO-5E24:62417 ↔ 167.99.215.164:4434] [TCP] [Application: TLS.ntop] [Info: dati.ntop.org] ⚡), and Actions (Explore, Delete).

**Alert Configuration (Bottom Section):**

- Header:** Shows interface en0 with 203.20 kbit/s traffic, 128 Flows, and 1 ntopng maintenance expired alert.
- Breadcrumbs:** User Scripts / Flows / Config Default.
- Buttons:** All (22), Enabled (19), Disabled (3).
- Search:** Filter Categories (Search Script: tls).
- Table:** Lists four alert configurations:
  - Old TLS Version:** Trigger an alert when an old (and possibly unsecure) TLS version is detected. Action: Disable.
  - TLS Certificate Expired:** Trigger an alert when an expired TLS certificate is detected. Action: Disable.
  - TLS Certificate Issues:** Trigger an alert when a mismatched TLS certificate is detected. Action: Disable.
  - TLS Unsafe Ciphers:** Trigger an alert when unsafe TLS ciphers are detected. Action: Disable.
- Pagination:** Showing 1 to 4 of 4 rows.

# Additional Behavioral Protocol Analyses

The screenshot shows the ntopng web interface with the 'Security' tab selected. The left sidebar includes links for Dashboard, Alerts, Flows, Hosts, Interface, Settings, Developer (which is currently active), and Help. The top header displays network information (en0, 14.70 kbit/s), a maintenance status message ('ntopng maintenance expired'), and summary statistics (24 alerts, 3 flows, 17 hosts, 16 devices, 10 devices). A search bar and a notifications icon are also present.

Name	Category	Description	Values	Action
Blacklisted Country	!	Trigger an alert when hosts contact or are contacted by the specified co...		<a href="#">Disable</a> <a href="#">Edit</a> <a href="#">View</a>
Blacklisted Flow	!	Trigger an alert when a blacklisted host or domain is detected		<a href="#">Disable</a> <a href="#">View</a>
Data Exfiltration	!	Trigger alerts when a possible data exfiltration activity is detected		<a href="#">Disable</a>
Device Application Not Allowed	!	Trigger an alert when an unusual application is detected for a device. R...		<a href="#">Disable</a> <a href="#">View</a>
DNS Data Exfiltration	!	Trigger alerts when a DNS data exfiltration activity is detected		<a href="#">Disable</a>
Elephant Flows	!	Trigger an alert when a flow exchanges more than the configured bytes vo...	> 1 GB (L2R), > 1 GB (R2L). Exce...	<a href="#">Disable</a> <a href="#">Edit</a>
Invalid DNS Query	!	Trigger an alert when a possibly malicious DNS query is detected	sophosxl.net	<a href="#">Disable</a> <a href="#">Edit</a>
Long Lived	!	Trigger an alert when a flow lasts more than the configured duration	> 01:00. Exceptions: Database	<a href="#">Disable</a> <a href="#">Edit</a>
Malicious Signature	!	Trigger an alert when a possibly malicious signature is detected		<a href="#">Disable</a>

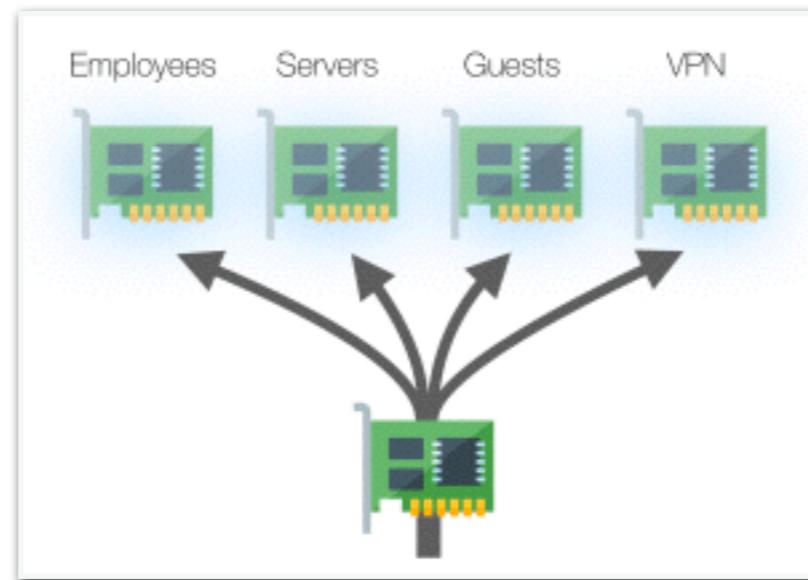
# Simplifying the Analysis of Heterogeneous Traffic

# Sub-Interfaces: Why? [1/2]

- **(Corporate) network traffic** is often **heterogeneous**
  - Employees network
  - Core company servers
  - Guests network
  - ...
- Logical separation done with
  - VLANs
  - Subnets
  - ...

# Sub-Interfaces: Why? [2/2]

- Having all the traffic "mixed" in a single interface not of help for the analysts
  - Hard to tell X and Y apart, difficult to do root-cause analyses
- Need to partition the traffic into meaningful subsets



# Automatic Traffic Partitioning

- Automatically divert the traffic of an interface into logical **sub-interfaces**
- Criteria such as
  - NetFlow/sFlow exporter IP address
  - VLAN ID
  - SNMP Interfaces

# Custom Traffic Partitioning

- Sometimes a single criteria is not enough and custom disaggregation is required
- ntopng 4.0 allows to define sub-interfaces with **BPF-like filters**

The screenshot shows the ntopng web interface with the following details:

- Header:** Shows interface `eno1`, bandwidth usage `59.60 kbit/s` (`515.80 kbit/s`), and various monitoring metrics: `14`, `12`, `1`, `13 Devices`, `62 Flows`.
- Search Bar:** Includes a search icon and a "Search" input field.
- Left Sidebar:** Includes links for `Dashboard`, `Alerts`, `Flows`, `Hosts`, `Interface` (selected), and `Settings`.
- Main Content:** Title `Custom Traffic Disaggregation`. A table lists two sub-interfaces:

Sub-Interface Name	Traffic Filter (nBPF Format)	Action
Guests	<code>(INPUT_SNMP 246 or OUTPUT_SNMP 246) and net 192.168.2.0/24</code>	<a href="#">Edit</a> <a href="#">Delete</a>
Staff	<code>net 192.168.1.0 and SRC_VLAN 234</code>	<a href="#">Edit</a> <a href="#">Delete</a>
- Footer:** Shows `Showing 1 to 2 of 2 rows`.

# Active Monitoring

# Active Monitoring: Why?

- Important hosts in the network
  - Offering critical services
    - Backup
    - VPN
    - NAS
- They must be always available and fully functional

# Active Monitoring in ntopng 4.0

- ntopng 4.0 active monitoring probes hosts on a minute-by-minute basis
- Check **reachability of hosts** and **availability of their services**
  - ICMP/ICMPV6
  - HTTP/HTTPS
- **⚠** Alerts when hosts are unreachable or have high Round Trip Time (**RTT**)

# Monitoring Hosts RTT

The screenshot shows the ntop web interface under the 'System' tab. The main content area displays a table of RTT measurements for various URLs. A modal dialog is open in the bottom right corner for 'Add RTT Record'. The 'Measurement' dropdown is set to 'https'. Other fields in the dialog include 'Host' (ntop.org) and 'RTT Threshold' (> 300 ms). A note at the bottom of the dialog provides information about measurement types.

URL	Chart	RTT Threshold	Last Measurement	Last IP	Measurement Time	Actions
http://ntop.org		25 ms	00:41 ago	178.62.197.130	210.05 ms	<button>Edit</button> <button>Delete</button>
https://ntop.org		300 ms	00:41 ago	178.62.197.130	243.85 ms	<button>Edit</button> <button>Delete</button>
https://one.one.one.one		200 ms	00:41 ago	1.0.0.1	491.48 ms	<button>Edit</button> <button>Delete</button>
icmp6://2001:4860:4860::8888		100 ms				<button>Edit</button> <button>Delete</button>
icmp://127.0.0.1		100 ms	00:41 ago	127.0.0.1	0.05 ms	<button>Edit</button> <button>Delete</button>
icmp://192.168.2.222		100 ms	00:41 ago	192.168.2.222	0.03 ms	<button>Edit</button> <button>Delete</button>

Showing 1 to 6 of 6 rows

Add RTT Record

Measurement: https

Host: ntop.org

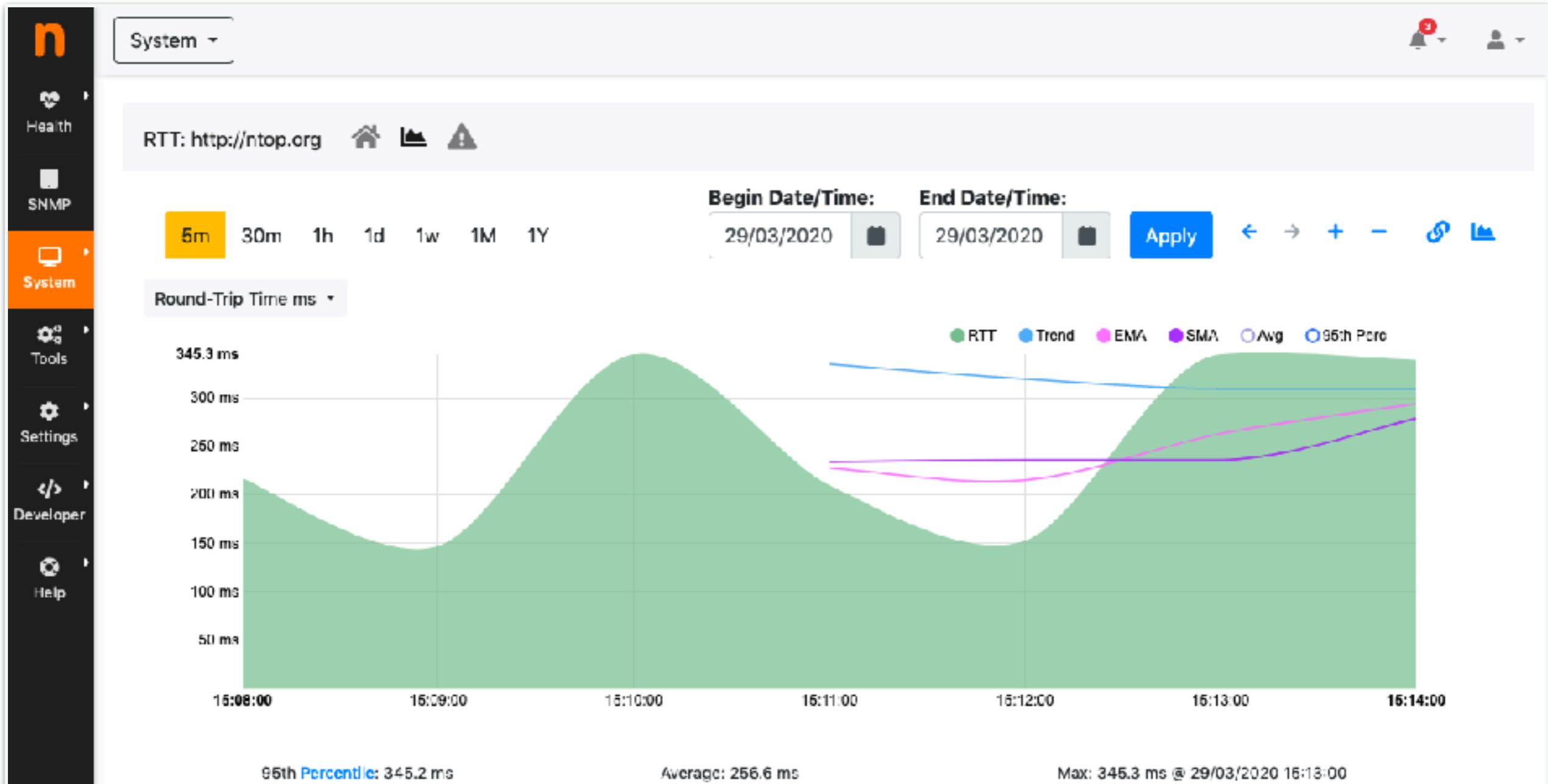
RTT Threshold: > 300 ms

NOTES:

- Measurements icmp and icmp6 ping the host using ICMP and ICMPv6
- Measurements http and https retrieve a web page using HTTP and HTTPS
- An alert is triggered when the RTT is detected to be above the threshold set

Cancel Add

# Historical Host RTT



# RTT-Based Alerts

The screenshot shows the ntop web interface with the following details:

- Header:** System dropdown, Health icon, User icon.
- Breadcrumbs:** RTT, Home, Alert icon.
- Alert Types:** Engaged Alerts (selected), Past Alerts.
- Title:** Engaged Alerts (with a blue exclamation mark icon).
- Filter:** 10, Type (dropdown), Severity (dropdown).
- Table Headers:** Date/Time, Duration, Severity, Alert Type, Drilldown, Description, Actions.
- Table Data:**

Date/Time	Duration	Severity	Alert Type	Drilldown	Description	Actions
01:22 ago	01:22	Warning	! RTT		RTT too high for http://ntop.org (178.62.197.130) [146.95 ms > 25 ms]. <a href="#">Fix</a>	<a href="#">Disable</a> <a href="#">Release</a>
01:22 ago	01:22	Warning	! RTT		RTT too high for https://one.one.one.one (1.1.1.1) [419.44 ms > 200 ms]. <a href="#">Fix</a>	<a href="#">Disable</a> <a href="#">Release</a>
03:23 ago	03:23	Warning	! RTT		Host icmp6://2001:4860:4860::8888 is unreachable. <a href="#">Fix</a>	<a href="#">Disable</a> <a href="#">Release</a>

# Something for the Developers: Extensibility

# ntopng 4.0 Extensibility: Why?

- Ease community contributions
- Desire to turn ntopng into something which is really opensource
- ~~Opensource means being on GitHub~~ 
- ~~Opensource means free~~
- **Opensource means easily extensible** by community contributors

# ntopng 4.0 Extensibility: Plugins

- **Move** most of the **functionalities** from the C/C++ core **to plugins**
  - **Redesign ntopng architecture**
- **Plugins are Lua scripts** executed by ntopng periodically or on an event-driven basis

# Plugin Functionalities

- Plugins are executed
  - **Periodically**: every min/5min/hour/day
  - **On events**: e.g., when a new flow is detected, when a flow goes idle
- A developer can use plugins to "**tap**" into hosts, flows, and other network elements
- **APIs** to interact with the core
  - **Pull** data **from the core**
    - e.g., read host traffic, read nDPI-dissected data
  - **Push** data **into the core**
    - e.g., trigger alerts, set flow statuses

# Other Plugin Functionalities

- **Create Web UI pages** and **write timeseries** - RTT monitoring is implemented with a plugin!
- **Add menu entries**
- **Monitor the status of the host** on top of which ntopng is running
- **Check status and health of ntopng** itself

# Configuring Plugins

The screenshot shows the ntopng web interface with the following details:

- Header:** Shows network traffic statistics: **12.40 kbit/s** up and **23.80 kbit/s** down, **26 Flows**, **8 Flows** (red), **32 Flows** (green), **3 Devices**, **21 Devices**, **36 Flows**.
- Left Sidebar:** Includes links for **Dashboard**, **Alerts**, **Flows**, **Hosts**, **Interface**, **Settings** (selected), and **Developer**.
- Breadcrumbs:** **User Scripts / Hosts / Config office**.
- Table Headers:** **All (16)**, **Enabled (9)** (selected), **Disabled (7)**. Filter Categories and Search Script.
- Table Data:** A list of 16 scripts, including **Traffic Alert**, **SYN Scan Victim Alert**, **SYN Scan Attacker Alert**, **SYN Flood Victim Alert**, **SYN Flood Attacker Alert**, **Score**, **Replies / Requests Ratio**, **Flow Flood Victim Alert**, and **Flow Flood Attacker Alert**. Each row has **Disable**, **Edit**, and **View** buttons.
- Modal Dialog (Traffic Alert):** Shows the configuration for the **Traffic Alert** script. It includes:
  - Enabled:**  Minute:  Bytes
  - 5 Minutes:  Bytes
  - Hourly:  Bytes
  - Daily:  Bytes
- Description:** Trigger an alert when the Layer 2 bytes delta (sent + received) exceeds the threshold.
- Buttons:** **Reset Default**, **Cancel**, **Apply**.

# Plugins: Hands On

- Examples at [https://github.com/ntop/ntopng/tree/  
dev/scripts/plugins](https://github.com/ntop/ntopng/tree/dev/scripts/plugins)
- Docs at <https://www.ntop.org/guides/ntopng/plugins>
- Video at [https://www.youtube.com/watch?  
v=4IjkAhhCH8M](https://www.youtube.com/watch?v=4IjkAhhCH8M)

# Other ntopng 4.0 Functionalities

# Multi-Tenancy [1/2]

- (W)ISP, transit and other Internet providers use ntopng to provide services to their customers
  - Security services
  - Billing
- ntopng 4.0 becomes (really) multi-tenant
  - Admin/non-admin users with different privileges
  - Different users have access to different portions of
    - Traffic
    - Alerts
    - Local Networks

# Multi-Tenancy [2/2]

The screenshot shows the ntopng web interface with the 'Settings' menu item highlighted in orange. On the left, there's a sidebar with icons for Dashboard, Alerts, Flows, Hosts, Interface, Settings (which is active), Developer, and Help. The main content area has a header 'Web Users' with network statistics: eno1 - 11.50 kbit/s up, 53.60 kbit/s down, 18 flows, and 29 hosts. Below this is a table of existing users:

Username	Full Name
maina	maina
alfredo	alfredo
admin	ntopng Administrator

Below the table, it says 'Showing 1 to 3 of 3 rows'. A message at the bottom indicates 'ntopng Enterprise Edition v4.0.200327 | ⓘ'.

A modal dialog box titled 'Add Web User' is open in the center. It contains the following fields:

- Username: customer
- Full Name: Customer One
- Password: (obscured)
- Confirm Password: (obscured)
- User Role: Non Privileged User
- Allowed Interface: Any Interface
- Allowed Networks: 192.168.1.0/24  
Comma separated list of networks this user can view. Examples:  
192.168.1.0/24,172.16.0.0/16
- Allow the user to download live traffic and PCAPs
- Language: English

At the bottom of the dialog is a blue 'Add New User' button.

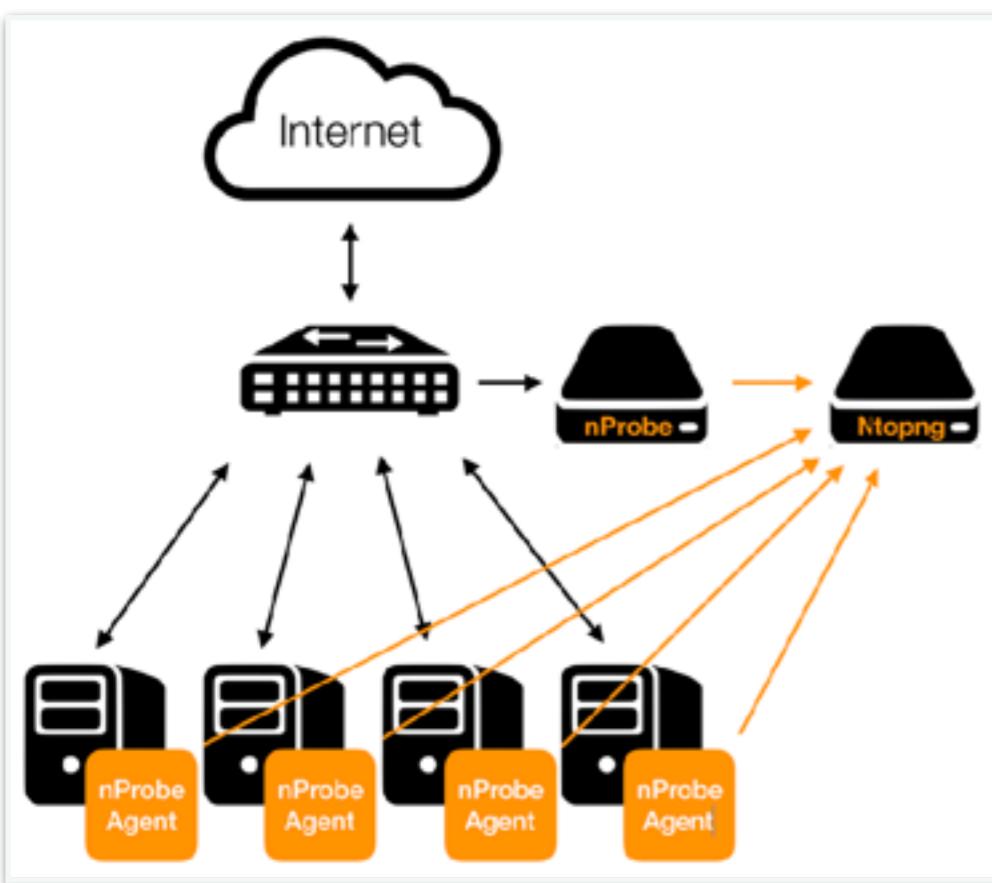
# Multi-Language

- Several languages supported thanks to community contributors
  - English
  - Italian
  - Japanese
  - German
  - Czech
  - Portuguese

# Traffic-to-Process Visibility [1/2]

- **Associate flows with** the originating process and other process metadata
  - Process
  - Process Owner
  - Docker container
  - ...
- ntopng 4.0 integrates with **nprobe-agent**, a packet-less probe capturing designed to capture these associations

# Traffic-to-Process Visibility [2/2]



**Recently Active Flows**

Application	Protocol	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	HTTP [0]	ubuntu18 [59674] [0 root > curl]	123.56.1 [0:80] http	< 1 sec	Server	0 bit/s	0 Bytes	

**Flow Peers [ Client / Server ]** ubuntu18 [59674] ⇨ 123.56.1 [0:80]

**Protocol / Application** TCP / HTTP (Network) [0]

**First / Last Seen** 11/06/2019 11:46:45 [00:30 ago] 11/06/2019 11:46:48 [00:30 ago]

ubuntu18 [59674] → /bin/bash [pid: 59847] ● → /usr/bin/curl [pid: 9273] ● ↗ /bin/bash [pid: 22847]

Legend: Host (blue dot), Process (red dot)

**Client Process Information**

User Name	root
Process PID/Name	/usr/bin/curl [pid: 9273] ↗ /bin/bash [pid: 22847]

**Additional Flow Elements**

Flow exporter IPv4 Address	ubuntu18
TCP_EVENT_TYPE	CLOSE

# Conclusions

- Releasing ntopng 4.0 brings several breakthroughs with its **~0.5 million of new lines of code**
- A **renewed look-and-feel** of the Web UI offers the best experience on wide-screens and guarantee the important information is always visible
- **Strong focus on security** offers augmented visibility and increased protection against cyberthreats
- **Active monitoring** guarantee the network has expected behaviors
- A new **pluggable architecture** makes it more open for community contributions