# Network Flow Monitoring – Integration of ntop & Checkmk

CHECKMK CONFERENCE #6 – MUNICH, APRIL 28, 2020


Alex Wilms
Consultant
tribe29

Jan Justus
CEO
tribe29

Simone Mainardi
Lead Engineer
ntop


tribe29 ntop

# Agenda

1. WHY NETWORK FLOW MONITORING?
2. WHAT IS NTOP?
3. HOW IS NTOP INTEGRATED IN CHECKMK?
4. HOW DO I GET IT?
5. Q&A?!

tribe29 ntop

# Integrate network flow monitoring in Checkmk

## What you already get from Checkmk

- Network performance monitoring & metrics
  - Bandwidth (e.g. bits in/out)
  - Packet rate
  - Error rate
- Network interface status and speed
- (Default) Thresholds / alarming

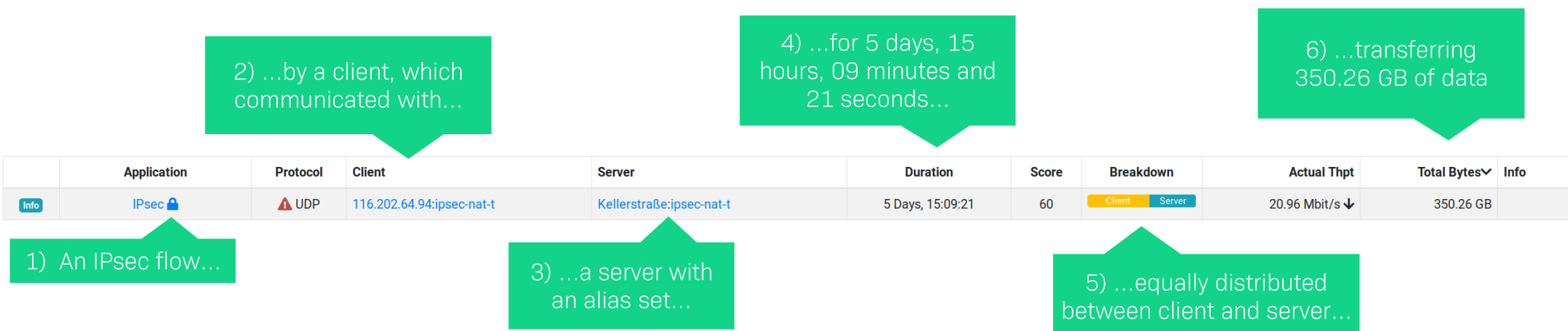
## What you might want to do in addition

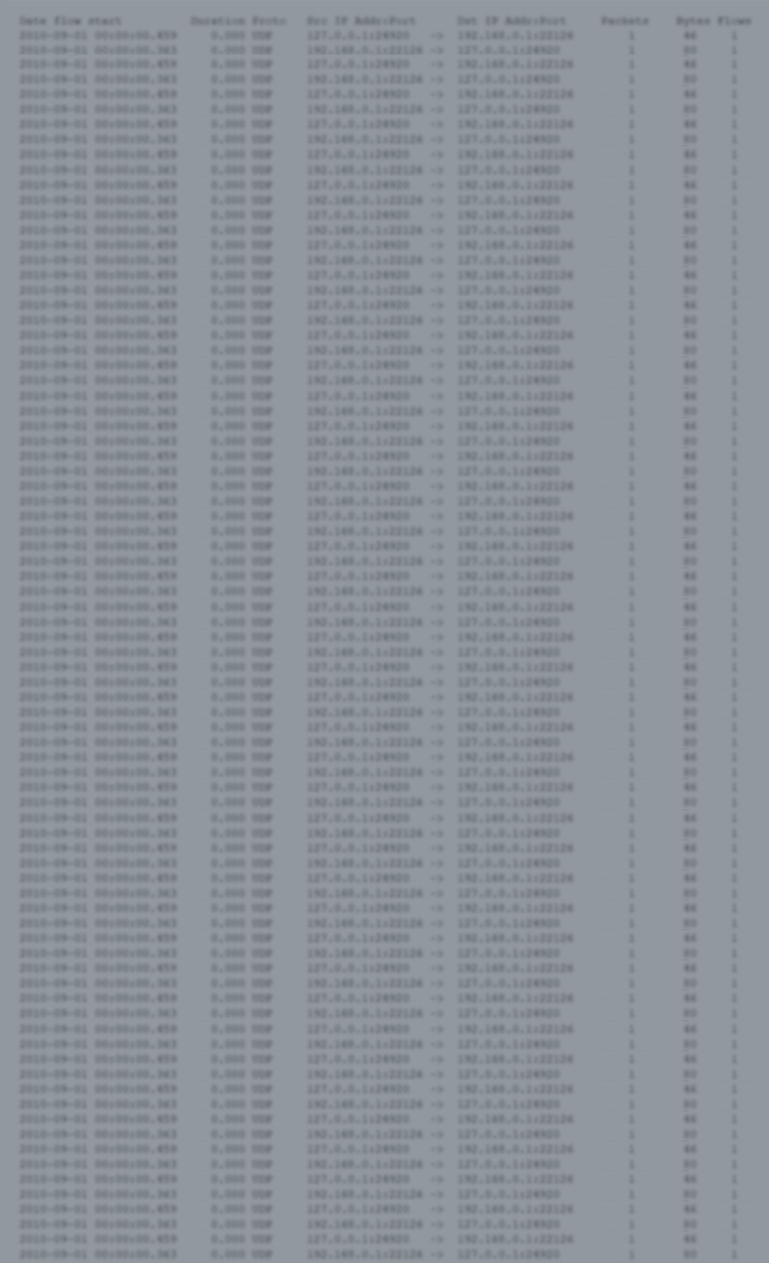
- Deeper root cause analyses (e.g. quick identification of network bottlenecks)
- Network flow analyses (e.g. top talkers, …)
- In-depth performance monitoring (e.g. delay, round-trip-times, …)
- Support threat detection (e.g. quick identification of threats like DDoS attacks)

# Flows – data summarized for a set of packets

A ‘Flow’ is a set of packets with a set of common properties. Vice versa, all packets of e.g. a web session can be summarized in a flow.

Typical flow data tells you that…





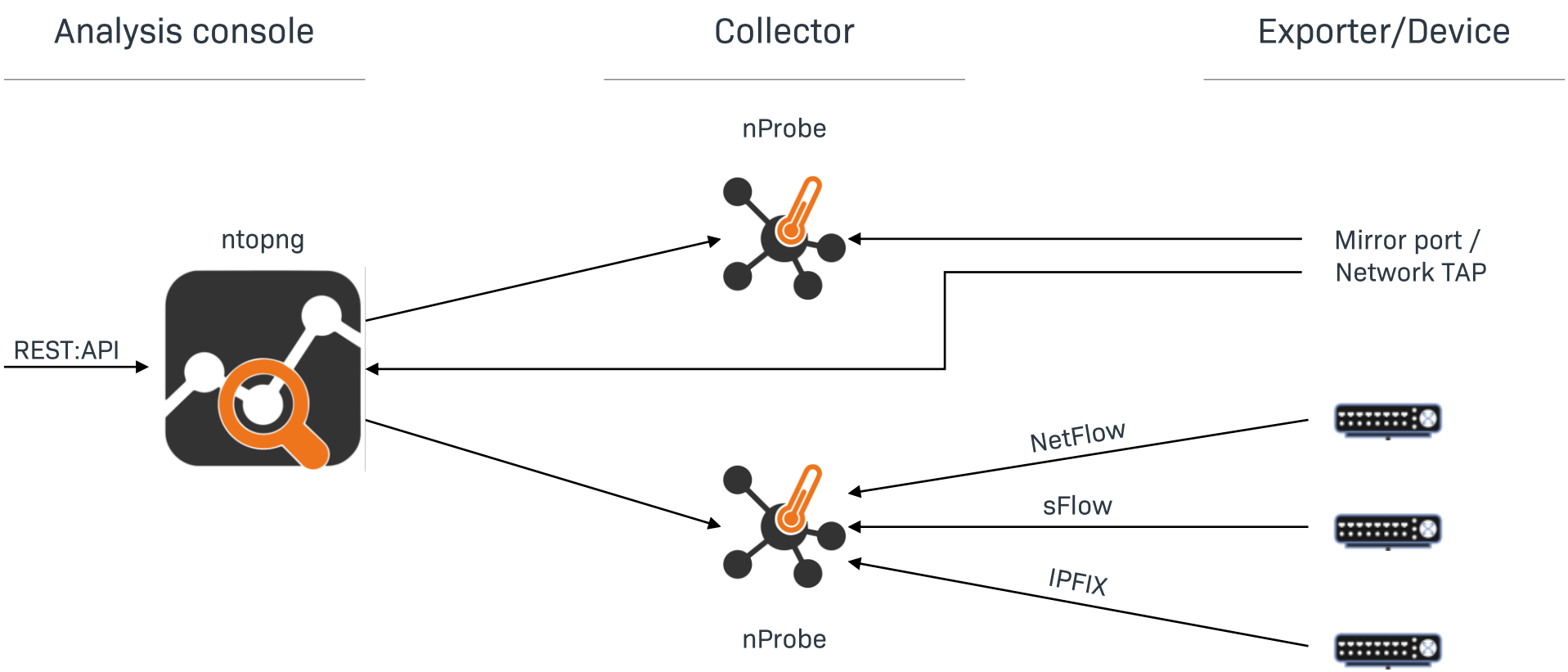
# Various protocols & sources provide flow data

| Switch | Router | Miscellaneous |
| --- | --- | --- |
| • sFlow | • NetFlow v5/v9<br>• NetFlow Lite<br>• IPFIX | • Mirror Port<br>• eBPF |

# ntop – a specialist in network flow analyses (and more!)

- Software company from Pisa, Italy
- Started as open source project in 1998 evolving into fully fledged software solution for network flow analysis, DPI, …
- Independent from third-party companies
- Serving many customers for more than 10 years

# Standard ntop architecture



# Traffic Dashboard

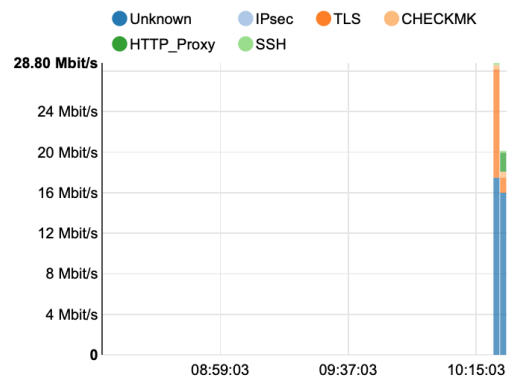
Real-time views: Top applications, top interfaces

| tcp://127.0.0.1:5556: Top Local Talkers | Actual Traffic |
|---|---|
| build-dc14-001.tribe29.com | 27.69 Mbit/s ↑ |
| fw.tribe29.com | 18.36 Mbit/s ↑ |
| review.lan.tribe29.com | 18.24 Mbit/s ↑ |
| build-dc4-001.tribe29.com | 4.6 Mbit/s ↓ |
| monitoring.lan.tribe29.com | 2.06 Mbit/s ↑ |
| support.tribe29.com | 1.26 Mbit/s ↑ |
| 10.1.2.229 | 890.69 kbit/s ↑ |

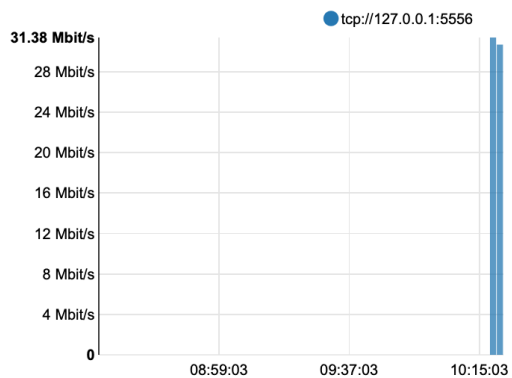
The top talkers

(hosts in your network with largest traffic)

tcp://127.0.0.1:5556: Realtime Top Application Traffic




Network Interfaces: Realtime Traffic

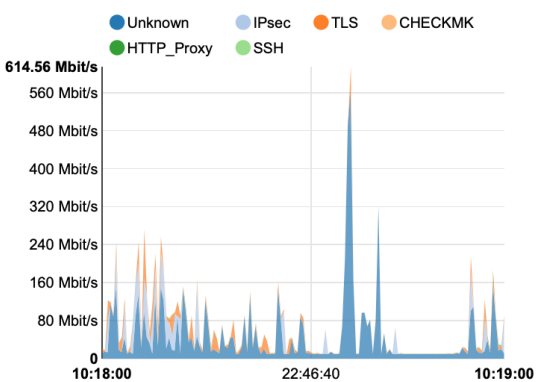



| tcp://127.0.0.1:5556: Top Remote Destinations | Actual Traffic |
|---|---|
| 178.248.246.154 | 4.71 Mbit/s ↑ |
| 192.168.4.100 | 2.29 Mbit/s ↑ |
| 188.193.219.176 | 90.79 kbit/s ↑ |
| 95.216.118.249 | 56.56 kbit/s ↓ |
| tauschzone.de | 44.93 kbit/s ↑ |
| 51.116.156.32 | 19.03 kbit/s ↓ |
| 212.114.227.32 [Kellerstraße] | 5.08 kbit/s ↓ |

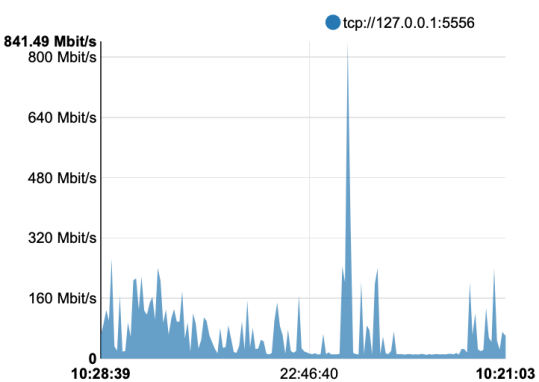
The top remote destinations

(where all the traffic is going)

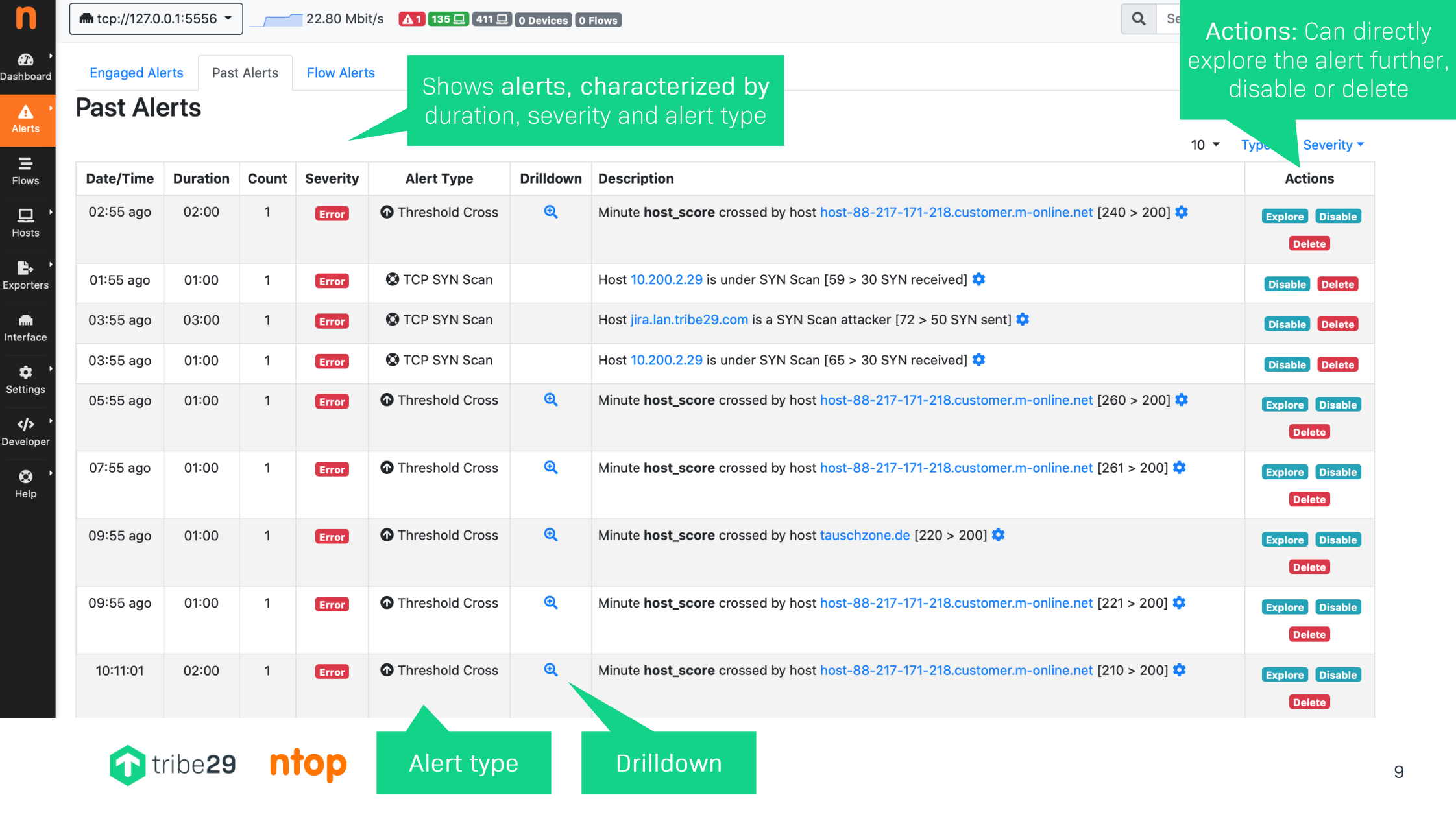
tcp://127.0.0.1:5556: Top Application Traffic Last Day View

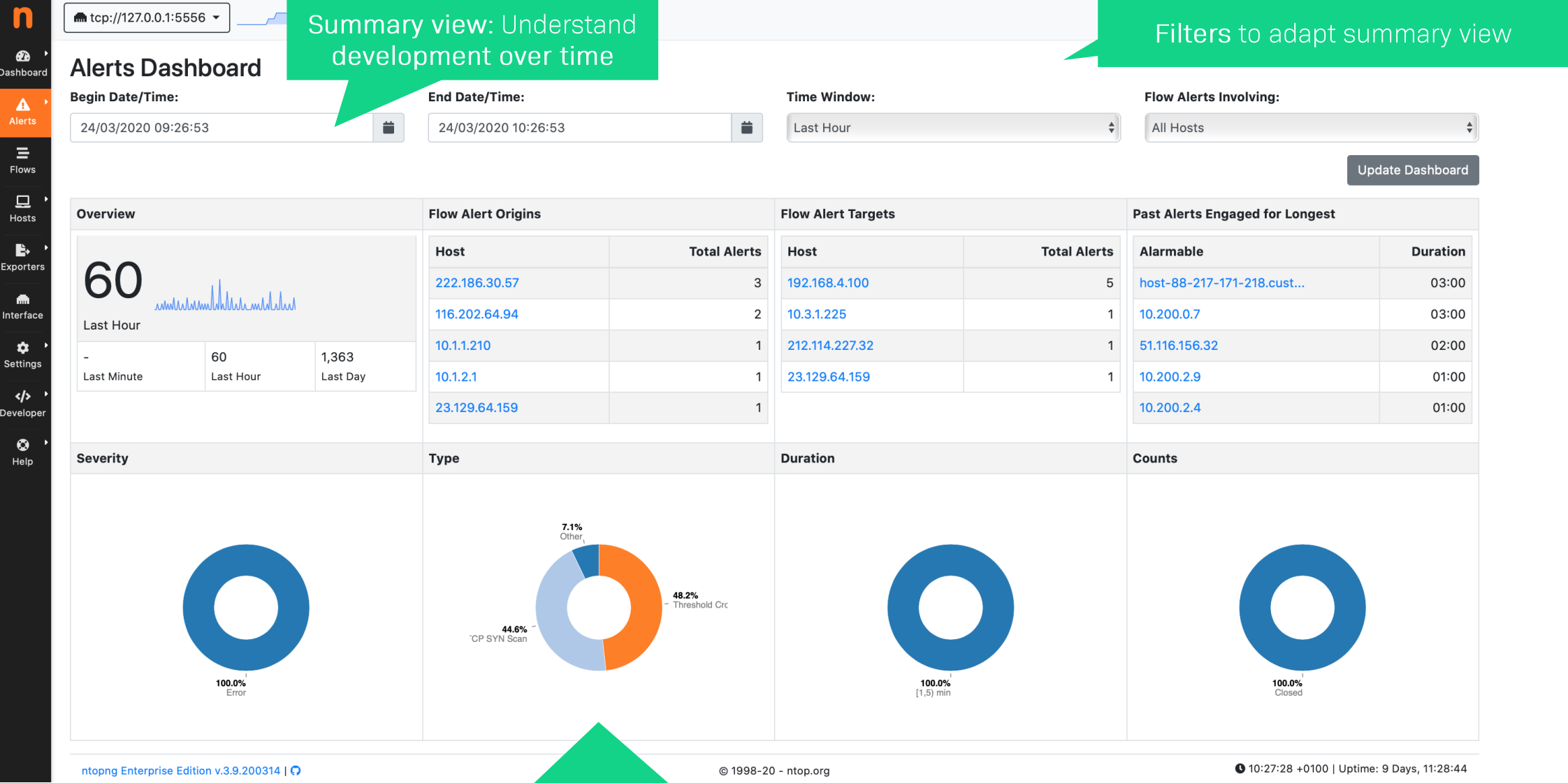



Network Interfaces: Last Day View

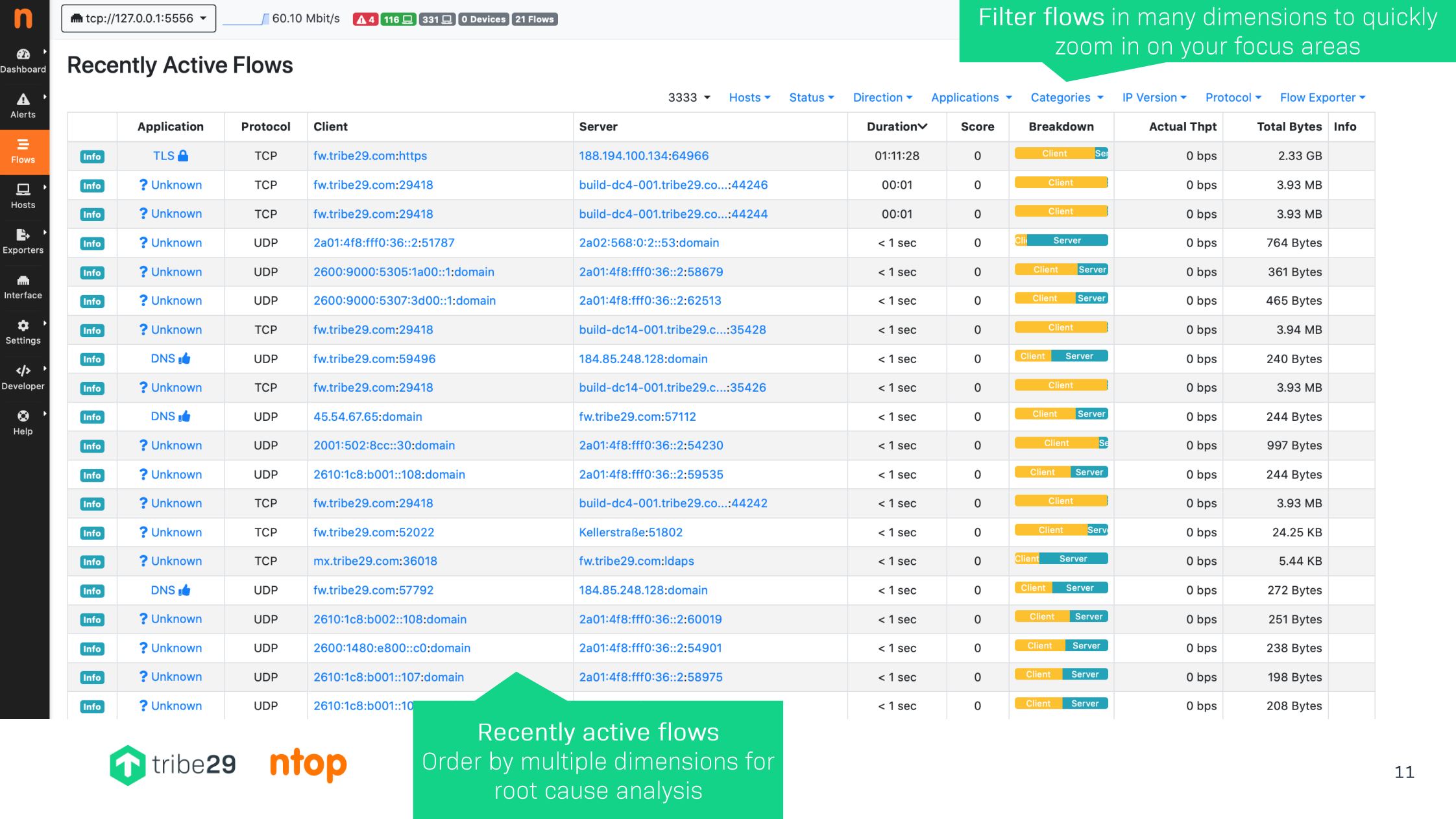



Last Day views: Top applications, top interfaces

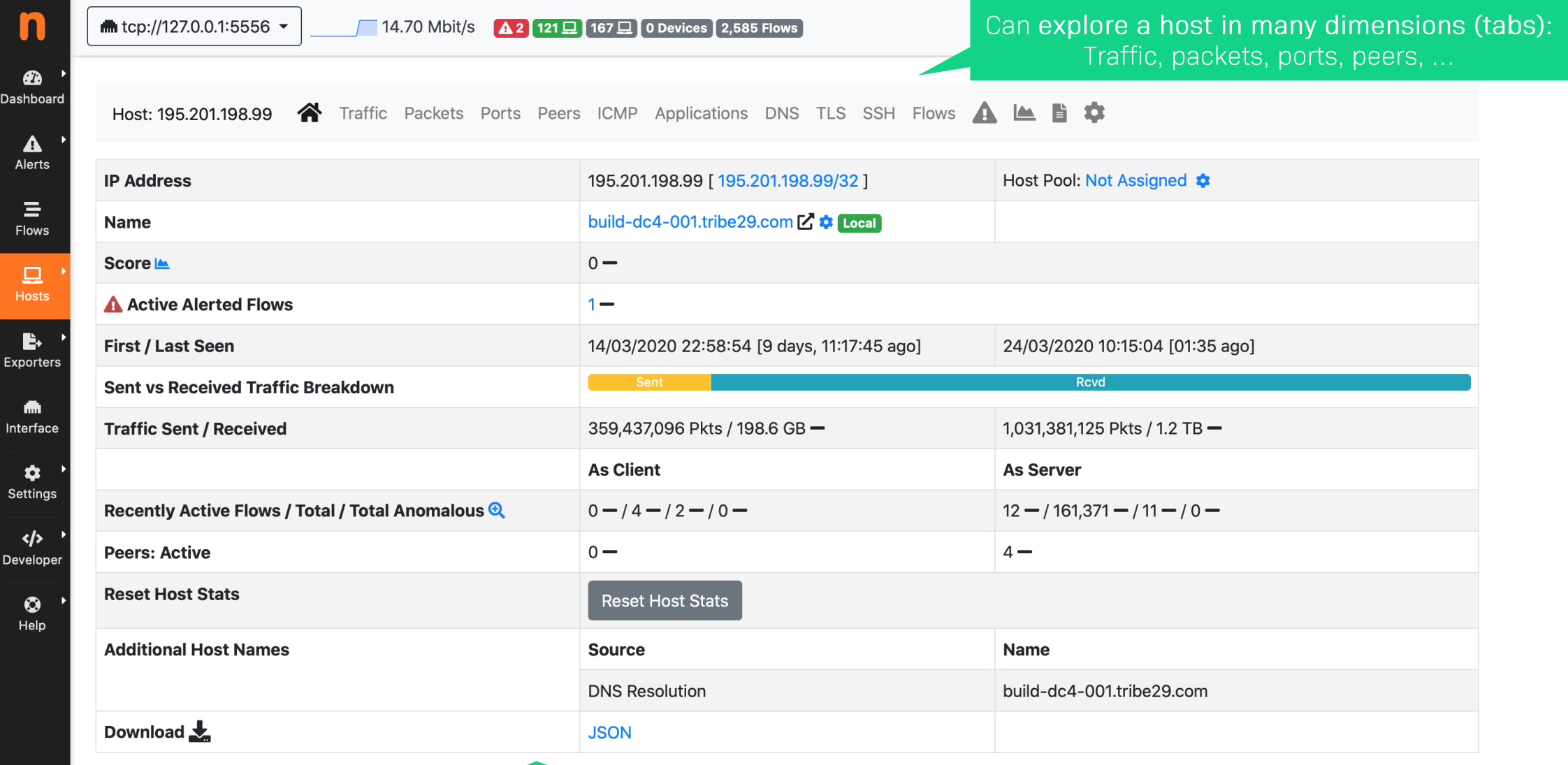

tcp://127.0.0.1:5556
22.80 Mbit/s
1
135
411
0 Devices
0 Flows
Dashboard
Alerts
Flows
Hosts
Exporters
Interface
Settings
Developer
Help
Engaged Alerts
Past Alerts
Flow Alerts
Past Alerts
Shows alerts, characterized by duration, severity and alert type
Actions: Can directly explore the alert further, disable or delete
10
Type
Severity
Date/Time | Duration | Count | Severity | Alert Type | Drilldown | Description | Actions
02:55 ago | 02:00 | 1 | Error | Threshold Cross | Minute host_score crossed by host host-88-217-171-218.customer.m-online.net [240 > 200] | Explore Disable Delete
01:55 ago | 01:00 | 1 | Error | TCP SYN Scan | Host 10.200.2.29 is under SYN Scan [59 > 30 SYN received] | Disable Delete
03:55 ago | 03:00 | 1 | Error | TCP SYN Scan | Host jira.lan.tribe29.com is a SYN Scan attacker [72 > 50 SYN sent] | Disable Delete
03:55 ago | 01:00 | 1 | Error | TCP SYN Scan | Host 10.200.2.29 is under SYN Scan [65 > 30 SYN received] | Disable Delete
05:55 ago | 01:00 | 1 | Error | Threshold Cross | Minute host_score crossed by host host-88-217-171-218.customer.m-online.net [260 > 200] | Explore Disable Delete
07:55 ago | 01:00 | 1 | Error | Threshold Cross | Minute host_score crossed by host host-88-217-171-218.customer.m-online.net [261 > 200] | Explore Disable Delete
09:55 ago | 01:00 | 1 | Error | Threshold Cross | Minute host_score crossed by host tauschzone.de [220 > 200] | Explore Disable Delete
09:55 ago | 01:00 | 1 | Error | Threshold Cross | Minute host_score crossed by host host-88-217-171-218.customer.m-online.net [221 > 200] | Explore Disable Delete
10:11:01 | 02:00 | 1 | Error | Threshold Cross | Minute host_score crossed by host host-88-217-171-218.customer.m-online.net [210 > 200] | Explore Disable Delete
tribe29
ntop
Alert type
Drilldown




tribe29 ntop




tribe29 ntop



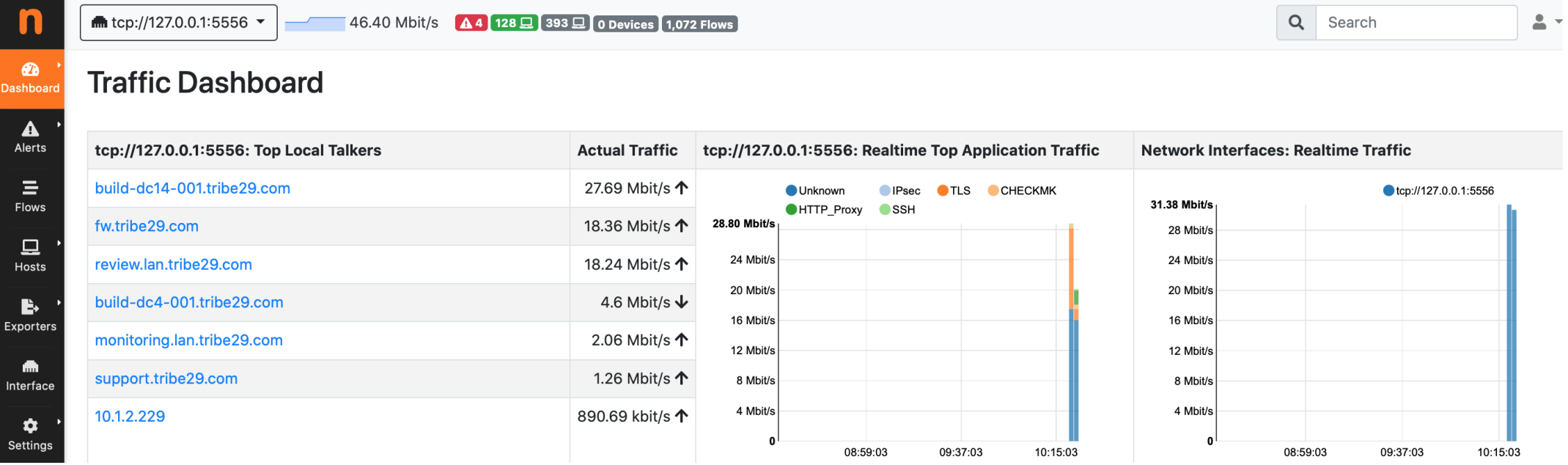

Can explore a host in many dimensions (tabs): Traffic, packets, ports, peers, ...

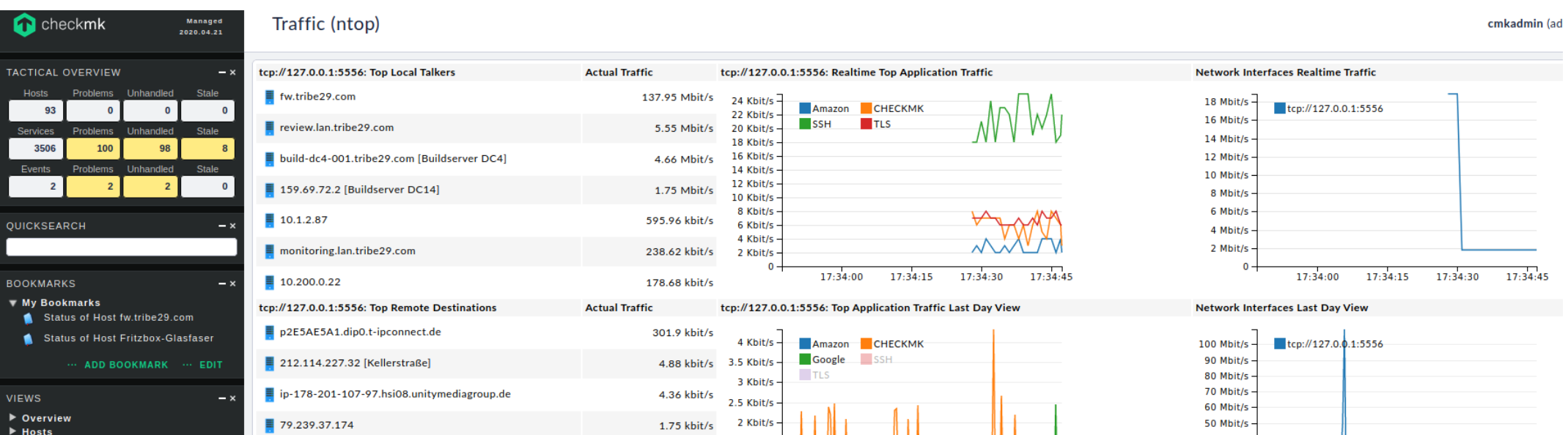
tribe29 ntop

Detailed view of a host in ntop


# Integrations available from Checkmk 1.7

- **Traffic dashboard:** Main dashboard (top talkers etc.) available in Checkmk
- **Alerts**:
  - Provide ntop “detected alerts” list + “alert summary” in Checkmk
  - Allow specific ntop alarms to trigger notifications in Checkmk
- **Flows**: Flow information available in Checkmk
- **Host details**: Relevant ntop data looking at a host in Checkmk
- **ntop graphing building blocks**: Enables specific ntop graphics to be included in views


tcp://127.0.0.1:5556
46.40 Mbit/s
4
128
393
0 Devices
1,072 Flows
Search
Dashboard
Alerts
Flows
Hosts
Exporters
Interface
Settings
Traffic Dashboard
tcp://127.0.0.1:5556: Top Local Talkers
Actual Traffic
build-dc14-001.tribe29.com
27.69 Mbit/s
fw.tribe29.com
18.36 Mbit/s
review.lan.tribe29.com
18.24 Mbit/s
build-dc4-001.tribe29.com
4.6 Mbit/s
monitoring.lan.tribe29.com
2.06 Mbit/s
support.tribe29.com
1.26 Mbit/s
10.1.2.229
890.69 kbit/s
tcp://127.0.0.1:5556: Realtime Top Application Traffic
Unknown
IPsec
TLS
CHECKMK
HTTP_Proxy
SSH
28.80 Mbit/s
24 Mbit/s
20 Mbit/s
16 Mbit/s
12 Mbit/s
8 Mbit/s
4 Mbit/s
0
08:59:03
09:37:03
10:15:03
Network Interfaces: Realtime Traffic
tcp://127.0.0.1:5556
31.38 Mbit/s
28 Mbit/s
24 Mbit/s
20 Mbit/s
16 Mbit/s
12 Mbit/s
8 Mbit/s
4 Mbit/s
0
08:59:03
09:37:03
10:15:03


checkmk
Managed
2020.04.21
Traffic (ntop)
cmkadmin (ad
TACTICAL OVERVIEW
Hosts
Problems
Unhandled
Stale
93
0
0
0
Services
Problems
Unhandled
Stale
3506
100
98
8
Events
Problems
Unhandled
Stale
2
2
2
0
QUICKSEARCH
BOOKMARKS
My Bookmarks
Status of Host fw.tribe29.com
Status of Host Fritzbox-Glasfaser
ADD BOOKMARK
EDIT
VIEWS
Overview
Hosts
Host Groups
tcp://127.0.0.1:5556: Top Local Talkers
Actual Traffic
fw.tribe29.com
137.95 Mbit/s
review.lan.tribe29.com
5.55 Mbit/s
build-dc4-001.tribe29.com [Buildserver DC4]
4.66 Mbit/s
159.69.72.2 [Buildserver DC14]
1.75 Mbit/s
10.1.2.87
595.96 kbit/s
monitoring.lan.tribe29.com
238.62 kbit/s
10.200.0.22
178.68 kbit/s
tcp://127.0.0.1:5556: Realtime Top Application Traffic
Amazon
CHECKMK
SSH
TLS
24 Kbit/s
22 Kbit/s
20 Kbit/s
18 Kbit/s
16 Kbit/s
14 Kbit/s
12 Kbit/s
10 Kbit/s
8 Kbit/s
6 Kbit/s
4 Kbit/s
2 Kbit/s
0
17:34:00
17:34:15
17:34:30
17:34:45
Network Interfaces Realtime Traffic
tcp://127.0.0.1:5556
18 Mbit/s
16 Mbit/s
14 Mbit/s
12 Mbit/s
10 Mbit/s
8 Mbit/s
6 Mbit/s
4 Mbit/s
2 Mbit/s
0
17:34:00
17:34:15
17:34:30
17:34:45
tcp://127.0.0.1:5556: Top Remote Destinations
Actual Traffic
p2E5AE5A1.dip0.t-ipconnect.de
301.9 kbit/s
212.114.227.32 [Kellerstraße]
4.88 kbit/s
ip-178-201-107-97.hsi08.unitymediagroup.de
4.36 kbit/s
79.239.37.174
1.75 kbit/s
tcp://127.0.0.1:5556: Top Application Traffic Last Day View
Amazon
CHECKMK
Google
SSH
TLS
4 Kbit/s
3.5 Kbit/s
3 Kbit/s
2.5 Kbit/s
2 Kbit/s
1.5 Kbit/s
Network Interfaces Last Day View
tcp://127.0.0.1:5556
100 Mbit/s
90 Mbit/s
80 Mbit/s
70 Mbit/s
60 Mbit/s
50 Mbit/s
40 Mbit/s

tcp://127.0.0.1:5556 | 22.80 Mbit/s | 1 | 135 | 411 | 0 Devices | 0 Flows | Search

Dashboard | Alerts | Flows | Hosts | Exporters | Interface

Engaged Alerts | Past Alerts | Flow Alerts

# Past Alerts

10 | Type | Severity

| Date/Time | Duration | Count | Severity | Alert Type | Drilldown | Description | Actions |
|---|---|---|---|---|---|---|---|
| 02:55 ago | 02:00 | 1 | Error | Threshold Cross | | Minute **host_score** crossed by host host-88-217-171-218.customer.m-online.net [240 > 200] | Explore Disable Delete |
| 01:55 ago | 01:00 | 1 | Error | TCP SYN Scan | | Host 10.200.2.29 is under SYN Scan [59 > 30 SYN received] | Disable Delete |
| 03:55 ago | 03:00 | 1 | Error | TCP SYN Scan | | Host jira.lan.tribe29.com is a SYN Scan attacker [72 > 50 SYN sent] | Disable Delete |
| 03:55 ago | 01:00 | 1 | Error | TCP SYN Scan | | Host 10.200.2.29 is under SYN Scan [65 > 30 SYN received] | Disable Delete |

checkmk Managed 2020.04.21

## Interface 116.202.64.94, Host fw.tribe29.com

cmkadmin (admin) 17:18

TACTICAL OVERVIEW

| Hosts | Problems | Unhandled | Stale |
|---|---|---|---|
| 93 | 0 | 0 | 0 |
| **Services** | **Problems** | **Unhandled** | **Stale** |
| 3506 | 101 | 99 | 4 |
| **Events** | **Problems** | **Unhandled** | **Stale** |
| 2 | 2 | 2 | 0 |

QUICKSEARCH

BOOKMARKS

- My Bookmarks
  - Status of Host fw.tribe29.com
  - Status of Host Fritzbox-Glasfaser

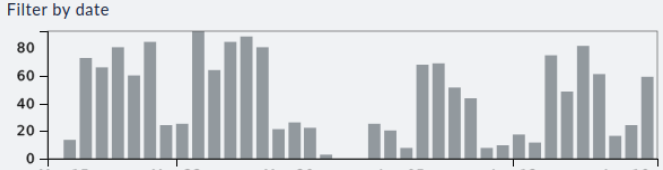
ADD BOOKMARK EDIT

VIEWS

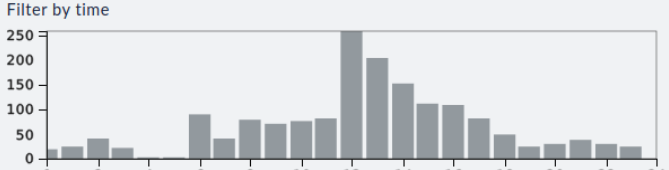
- Overview

Host | Traffic | Packets | Ports | Peers | Apps | Engaged alerts | Past alerts | Flow alerts

Filter by date




Filter by time

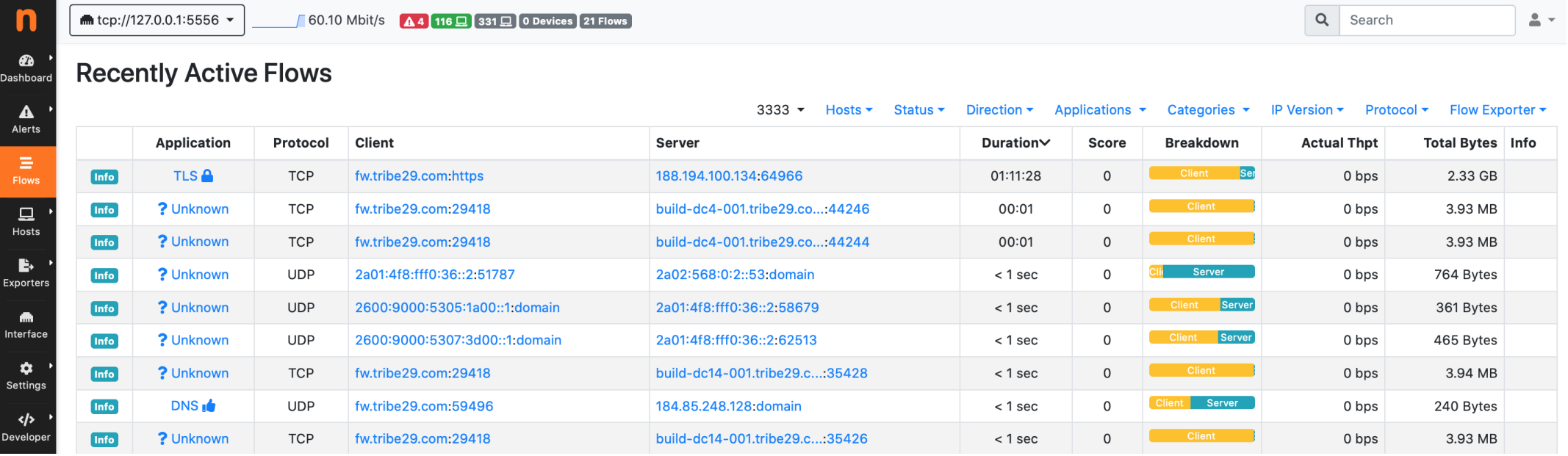


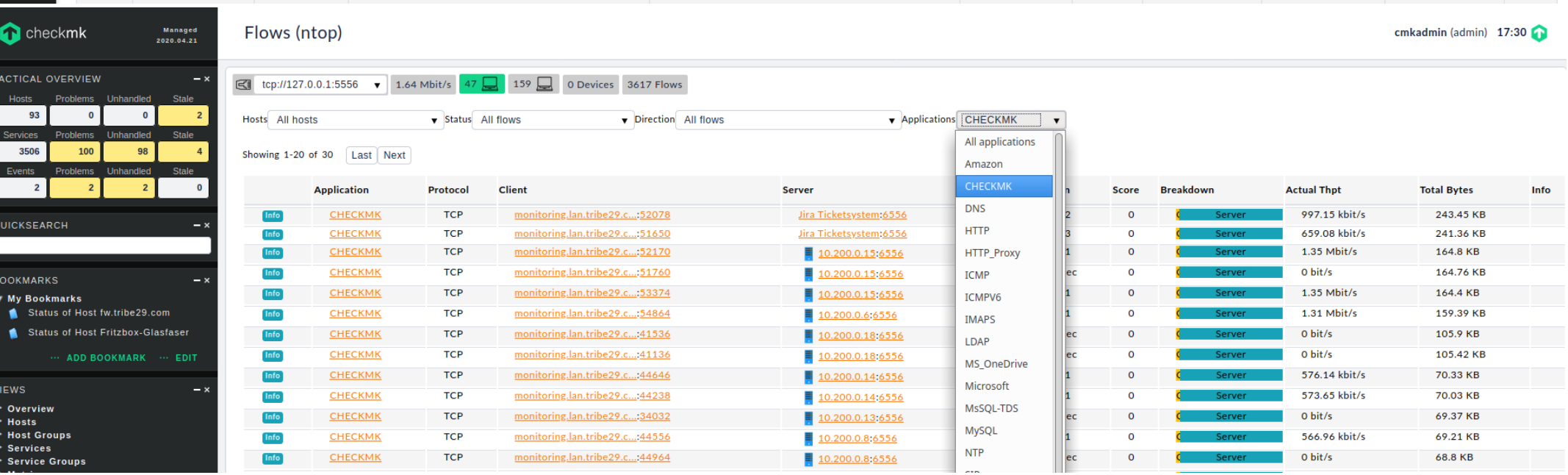

Additional filter options in Checkmk

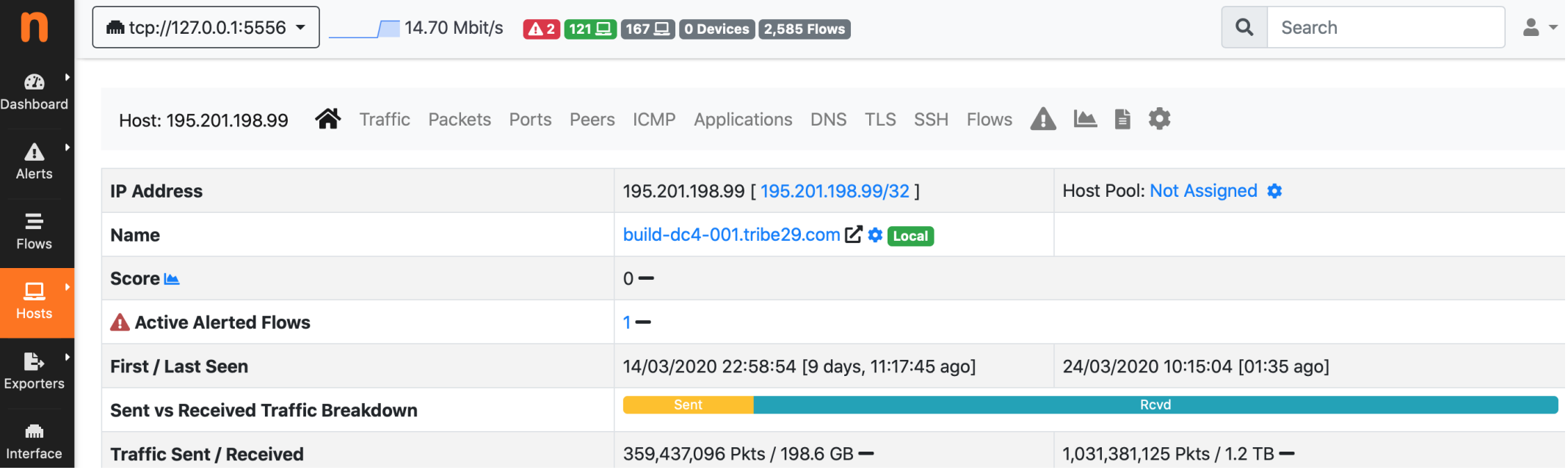
Filter by description | Type: Flow Misbehaviour | Severity: All

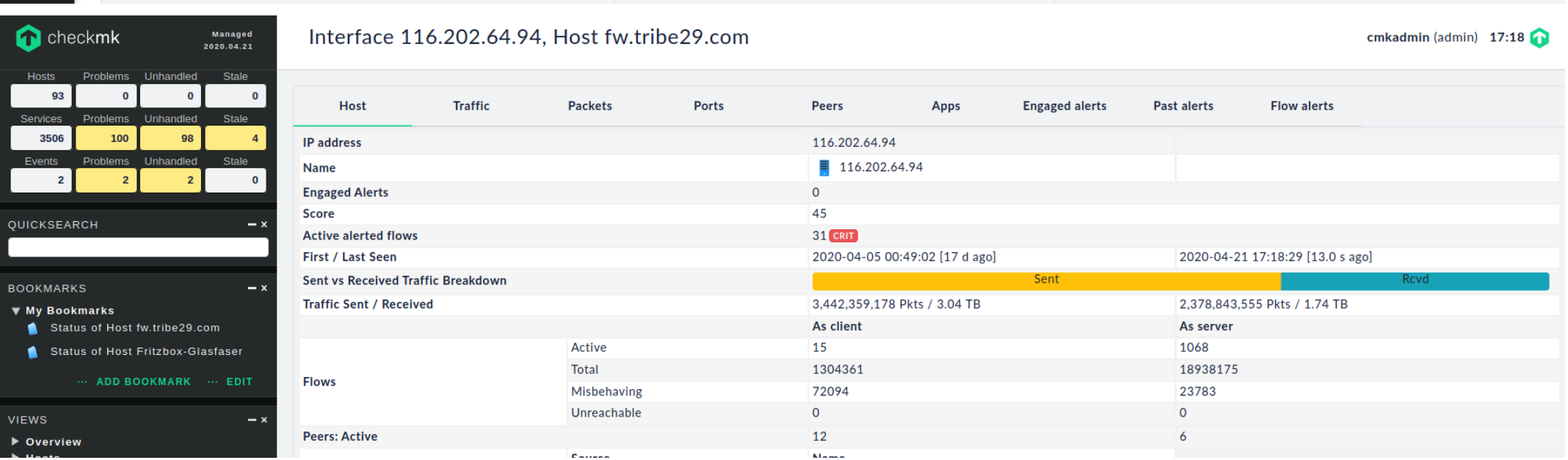
Showing 1-20 of 1661 (filtered Total: 2773 ) Last Next

| Date | Severity | Alert type | Score | Description | Actions |
|---|---|---|---|---|---|
| 21.4.2020 17:17:30 | Error | Flow Misbehaviour | | Elephant Flow (Remote to Local Traffic) [Exceeding 1 GB] [Flow: 116.202.64.94:4500 Kellerstraße:4500] [UDP] [Application: IPsec] | Explore Delete |
| 21.4.2020 17:16:20 | Error | Flow Misbehaviour | | Elephant Flow (Local to Remote Traffic) [Exceeding 1 GB] [Flow: ipbcc26486.dynamic.kabel...:61080 116.202.64.94:443] [TCP] [Application: TLS] | Explore Delete |
| 21.4.2020 17:05:35 | Error | Flow Misbehaviour | | Elephant Flow (Local to Remote Traffic) [Exceeding 1 GB] [Flow: 95.91.254.141:7979 116.202.64.94:443] | Explore Delete |


tcp://127.0.0.1:5556
60.10 Mbit/s
4
116
331
0 Devices
21 Flows
Search
Dashboard
Alerts
Flows
Hosts
Exporters
Interface
Settings
Developer
Recently Active Flows
3333
Hosts
Status
Direction
Applications
Categories
IP Version
Protocol
Flow Exporter
Application
Protocol
Client
Server
Duration
Score
Breakdown
Actual Thpt
Total Bytes
Info
TLS
TCP
fw.tribe29.com:https
188.194.100.134:64966
01:11:28
0
Client
0 bps
2.33 GB
Unknown
fw.tribe29.com:29418
build-dc4-001.tribe29.co...:44246
00:01
3.93 MB
build-dc4-001.tribe29.co...:44244
UDP
2a01:4f8:fff0:36::2:51787
2a02:568:0:2::53:domain
< 1 sec
Server
764 Bytes
2600:9000:5305:1a00::1:domain
2a01:4f8:fff0:36::2:58679
361 Bytes
2600:9000:5307:3d00::1:domain
2a01:4f8:fff0:36::2:62513
465 Bytes
build-dc14-001.tribe29.c...:35428
3.94 MB
DNS
fw.tribe29.com:59496
184.85.248.128:domain
240 Bytes
build-dc14-001.tribe29.c...:35426
3.93 MB


checkmk
Managed
2020.04.21
Flows (ntop)
cmkadmin (admin)
17:30
ACTICAL OVERVIEW
Hosts
Problems
Unhandled
Stale
93
0
0
2
Services
3506
100
98
4
Events
2
2
2
0
UICKSEARCH
OOKMARKS
My Bookmarks
Status of Host fw.tribe29.com
Status of Host Fritzbox-Glasfaser
ADD BOOKMARK
EDIT
IEWS
Overview
Hosts
Host Groups
Services
Service Groups
tcp://127.0.0.1:5556
1.64 Mbit/s
47
159
0 Devices
3617 Flows
Hosts
All hosts
Status
All flows
Direction
All flows
Applications
CHECKMK
Showing 1-20 of 30
Last
Next
Application
Protocol
Client
Server
Score
Breakdown
Actual Thpt
Total Bytes
Info
CHECKMK
TCP
monitoring.lan.tribe29.c...:52078
Jira Ticketsystem:6556
997.15 kbit/s
243.45 KB
monitoring.lan.tribe29.c...:51650
659.08 kbit/s
241.36 KB
monitoring.lan.tribe29.c...:52170
10.200.0.15:6556
1.35 Mbit/s
164.8 KB
monitoring.lan.tribe29.c...:51760
0 bit/s
164.76 KB
monitoring.lan.tribe29.c...:53374
1.35 Mbit/s
164.4 KB
monitoring.lan.tribe29.c...:54864
10.200.0.6:6556
1.31 Mbit/s
159.39 KB
monitoring.lan.tribe29.c...:41536
10.200.0.18:6556
105.9 KB
monitoring.lan.tribe29.c...:41136
105.42 KB
monitoring.lan.tribe29.c...:44646
10.200.0.14:6556
576.14 kbit/s
70.33 KB
monitoring.lan.tribe29.c...:44238
573.65 kbit/s
70.03 KB
monitoring.lan.tribe29.c...:34032
10.200.0.13:6556
69.37 KB
monitoring.lan.tribe29.c...:44556
10.200.0.8:6556
566.96 kbit/s
69.21 KB
monitoring.lan.tribe29.c...:44964
68.8 KB
All applications
Amazon
CHECKMK
DNS
HTTP
HTTP_Proxy
ICMP
ICMPV6
IMAPS
LDAP
MS_OneDrive
Microsoft
MsSQL-TDS
MySQL
NTP


tcp://127.0.0.1:5556
14.70 Mbit/s
2
121
167
0 Devices
2,585 Flows
Search
Dashboard
Alerts
Flows
Hosts
Exporters
Interface
Host: 195.201.198.99
Traffic
Packets
Ports
Peers
ICMP
Applications
DNS
TLS
SSH
Flows
IP Address
195.201.198.99 [ 195.201.198.99/32 ]
Host Pool: Not Assigned
Name
build-dc4-001.tribe29.com
Local
Score
0
Active Alerted Flows
1
First / Last Seen
14/03/2020 22:58:54 [9 days, 11:17:45 ago]
24/03/2020 10:15:04 [01:35 ago]
Sent vs Received Traffic Breakdown
Sent
Rcvd
Traffic Sent / Received
359,437,096 Pkts / 198.6 GB
1,031,381,125 Pkts / 1.2 TB


checkmk
Managed
2020.04.21
Hosts
Problems
Unhandled
Stale
93
0
0
0
Services
Problems
Unhandled
Stale
3506
100
98
4
Events
Problems
Unhandled
Stale
2
2
2
0
QUICKSEARCH
BOOKMARKS
My Bookmarks
Status of Host fw.tribe29.com
Status of Host Fritzbox-Glasfaser
ADD BOOKMARK
EDIT
VIEWS
Overview
Interface 116.202.64.94, Host fw.tribe29.com
cmkadmin (admin)
17:18
Host
Traffic
Packets
Ports
Peers
Apps
Engaged alerts
Past alerts
Flow alerts
IP address
116.202.64.94
Name
116.202.64.94
Engaged Alerts
0
Score
45
Active alerted flows
31
CRIT
First / Last Seen
2020-04-05 00:49:02 [17 d ago]
2020-04-21 17:18:29 [13.0 s ago]
Sent vs Received Traffic Breakdown
Sent
Rcvd
Traffic Sent / Received
3,442,359,178 Pkts / 3.04 TB
2,378,843,555 Pkts / 1.74 TB
As client
As server
Flows
Active
15
1068
Total
1304361
18938175
Misbehaving
72094
23783
Unreachable
0
0
Peers: Active
12
6

# It‘s demo time

# Get network flow monitoring with Checkmk 1.7

## Product

Purchase:

- ntop resold by Checkmk
- Checkmk-ntop integration addon (MKP)

Download:

- Checkmk-ntop integration add-on from Checkmk
- ntop download directly from ntop servers or via appliance option

## Consulting & Support

Checkmk-ntop-integration add-on:

- Checkmk or Checkmk partner

Ntop: Two major options

- 1st/2nd level come in via Checkmk support / Checkmk partner, routed to ntop specialist partner, who delivers support (D, EN, IT). 3rd level from ntop
- Directly from ntop

Our focus: make the experience as much „one-face-to-the-customer“ as possible

tribe29 ntop

# Any questions?

# Thank you

tribe29

ntop

**tribe29 GmbH**
Kellerstraße 29
81667 München
Deutschland

**Web** — tribe29.com
**E-Mail** — mail@tribe29.com