



# EXA8 Applications

June 2019



# The EXA8

**The EXA8 is a compact multi-application device which can be used for aggregation, filtering, and capturing of network traffic in real-time.**

- Captures 100% of all data for real-time analysis as well as historical playback – excellent for troubleshooting
- Captures to USB or SSD
- Capable of performing several other advanced applications like a Sessionmaster
- Able to run 3rd party applications
- Rolling Capture “look back in time capture”

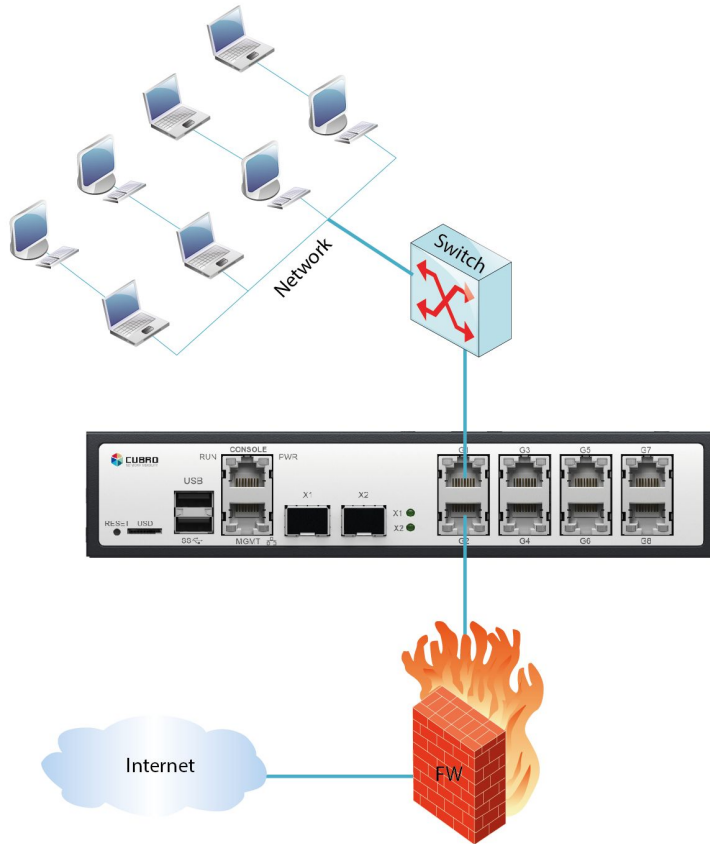


# EXA8 - “the multi-in-one tool”

- 4 link copper TAP
- 4 link aggregator
- Multi-gbit capture tool with 1TB SSD
- Rolling capture with index
- Web GUI protocol analyzer similar to Wireshark
- Netflow support controller & analyzer



# Enterprise Application



## Typical connection in any Enterprise Applications.

The EXA8 can be installed inline up to 4 links, the integrated bypass protects the live links.

- Rolling traffic capture to find security breaches.
- NTOPNG for live analytics of the traffic including DPI
- VoIP Analyzer
- DPI filter to block unwanted applications
- Regex Filter for detection security breaches

# Intuitive Web GUI

EXA8 Device Ports Aggregation Tapping Capture Shell Settings Welcome! admin Sign out CUBRO

## Device Information

Device Model EXA8  
Image Version 1.1.2-2.0  
Serialnumber 124A-18C0007  
Custom Device Label

N/A

Save

## Device Configuration

✓ Save configuration

↺ Restore configuration

✗ Reset configuration

## Device Image



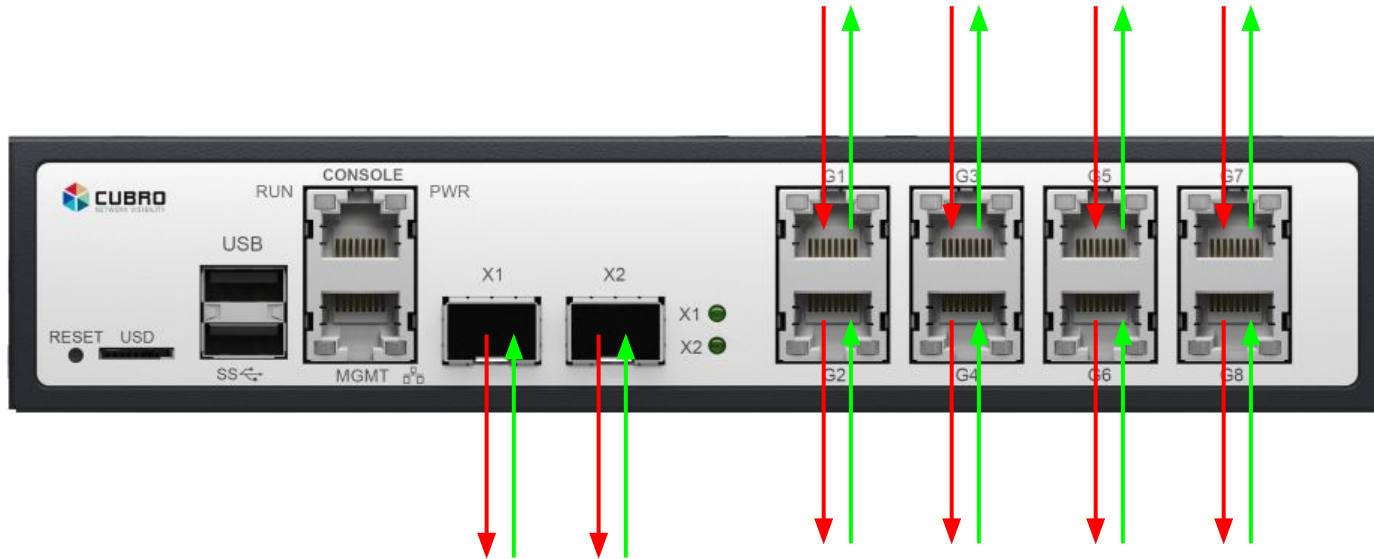
## System Information

CPU - 12% - Temperature 46°C

Disk free 776.45 GiB - used 303.93 MiB - total 818.33 GiB

Memory free 11.43 GiB - used 2.38 GiB - total 15.89 GiB

# The EXA8

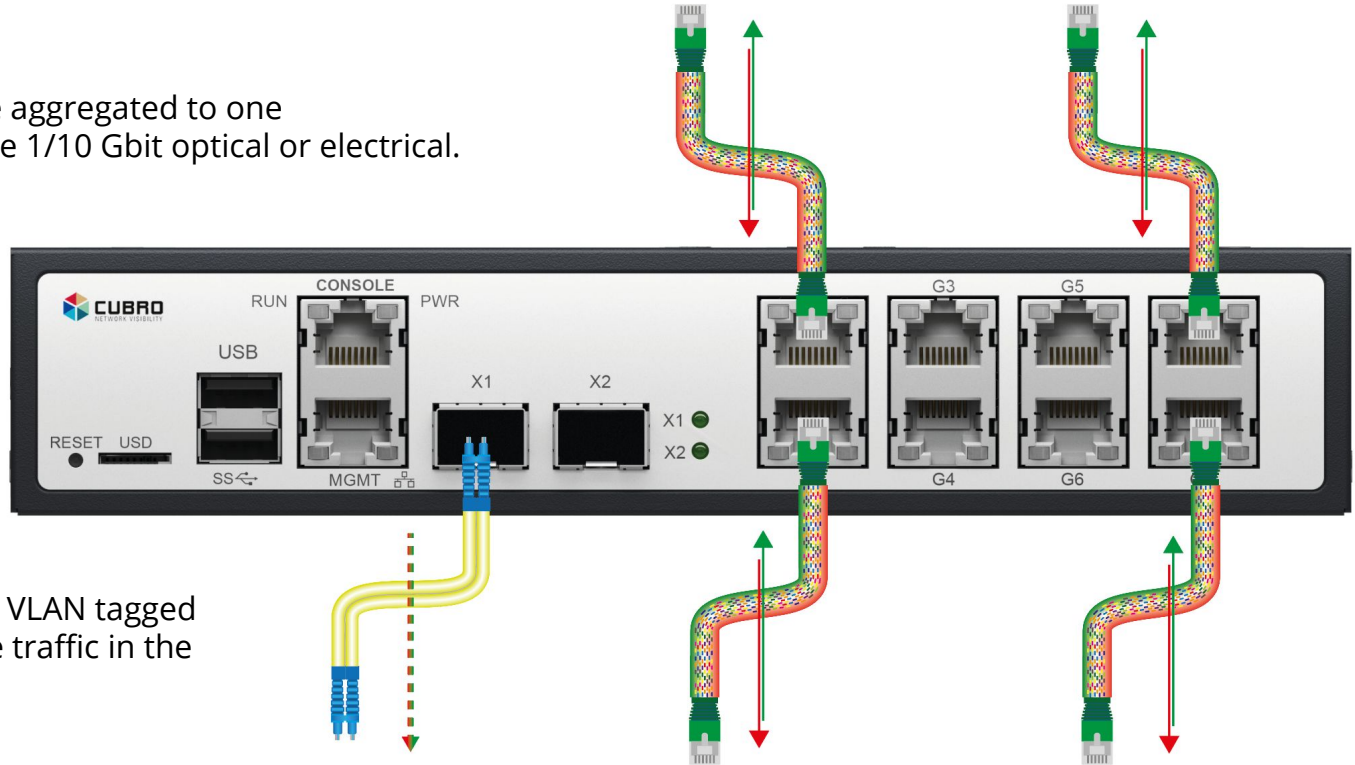


**2 x 1/10 Gbit  
optical/electrical ports  
usable as  
input and output  
(depending on the SFP  
module)**

**4 x 1 Gbit links with  
internal TAP (bypass)**

# Aggregation

Up to 4 links/8 ports can be aggregated to one output. This output could be 1/10 Gbit optical or electrical.



The output traffic can be VLAN tagged per input to separate the traffic in the monitoring tool.



# Aggregation GUI



## Set Tag

| Interface | Tag                |
|-----------|--------------------|
| G1        | <a href="#">10</a> |
| G2        | <a href="#">20</a> |
| G3        | <a href="#">30</a> |
| G4        | <a href="#">40</a> |
| G5        | <a href="#">50</a> |
| G6        | <a href="#">60</a> |
| G7        | <a href="#">70</a> |
| G8        | <a href="#">80</a> |

## Aggregation Tag

| Interface | Tag                         |
|-----------|-----------------------------|
| X1        | <a href="#">10 20 30 40</a> |
| X2        |                             |
| Xv        | <a href="#">60 80</a>       |

Output Interfaces:

X1 and X2 = optical outputs  
Xv = capture interface

## Push Tag

Disabled

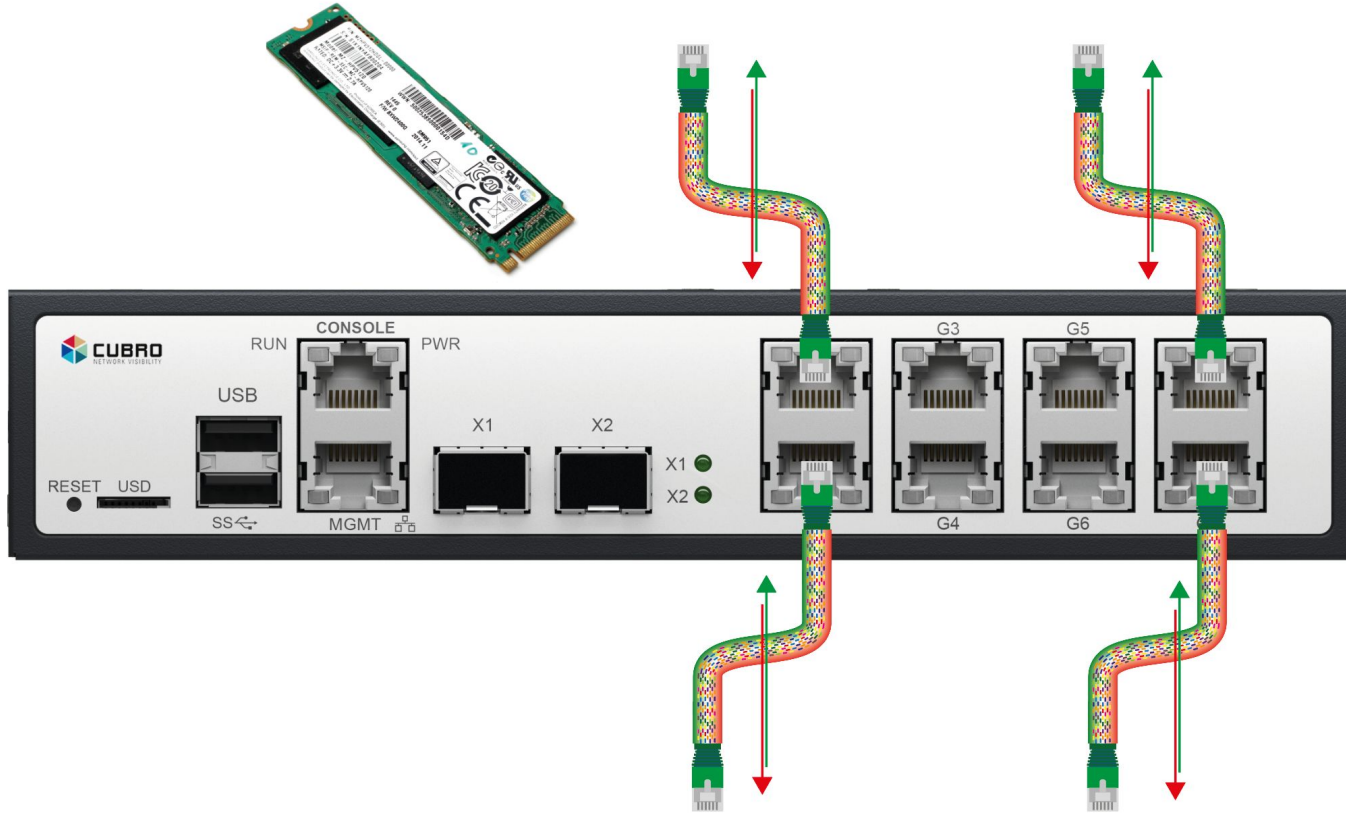
Input Interfaces:

G1 - G2  
G3 - G4  
G5 - G6  
G7 - G8

4 links



# Aggregation & Capture to SSD



# Tapping Session GUI

**Tapping Configuration**









Session  
Select...

Source Interfaces Configuration  
Select...

Destination Interface Configuration  
Select...

Apply

**Active Tapping session**

|   | Tapping Session   | Source Interface(s) | Destination Interface |
|---|-------------------|---------------------|-----------------------|
|  | Tapping Session 1 | G1                  | G2                    |
|  | Tapping Session 2 | G2                  | G1                    |
|  | Tapping Session 3 | G3                  | G4                    |
|  | Tapping Session 4 | G4                  | G3                    |
|  | Tapping Session 5 | G5                  | G6                    |
|  | Tapping Session 6 | G6                  | G5                    |
|  | Tapping Session 7 | G7                  | G8                    |
|  | Tapping Session 8 | G8                  | G7                    |

# Capture GUI

## Capture

PCAP Name

2019-06-06\_15-43-50.pcap






















Custom Filter

custom tcp dump compatible filter string

▶ Start Capture

■ No Capture running

## PCAPs

|   | Filename ↕               | Last Edited ↕              | Filesize ↕ |
|---|--------------------------|----------------------------|------------|
|    | VLAN_test.pcap           | 2019-06-06 03:11:03.244967 | 39.24 KiB  |
|    | VLAN_test (1).pcap       | 2019-06-06 03:11:03.244967 | 39.24 KiB  |
|    | test.pcap                | 2019-06-06 03:11:03.240967 | 7.69 KiB   |
|    | nij-subprocess.pcap      | 2019-06-06 03:11:03.240967 | 24 B       |
|    | logs.pcap                | 2019-06-06 03:11:03.240967 | 5.22 MiB   |
|    | 2019-04-25_16-39-26.pcap | 2019-06-06 03:11:03.124967 | 1.45 KiB   |
|    | 2019-04-29_14-02-43.pcap | 2019-06-06 03:11:03.124967 | 3.45 KiB   |



delete capture file  
download capture file  
start webshare (analyze capture file)

# Custom Filter examples

**Capture**

PCAP Name:  Custom Filter:

Capture running  Stop Capture

**Capture**

PCAP Name:  Custom Filter:

Capture running  Stop Capture

**Capture**

PCAP Name:  Custom Filter:

Capture running  Stop Capture

These filters reduce the captured traffic to save disk space.



# Remote Capture

With the optional built-in Wifi / 2G/3G/4G modem or Iridium satellite modem, the EXA8 is a versatile monitoring platform, that connects various wireless technologies across every point on Earth.

The EXA8 supports a PCIe connector expansion slot as well as holes for an antenna in the enclosure.

One box can do it all - Network connections on multiple interfaces, powerful multi-core CPU, high-performance SSD storage, and the modem support for remote connections.

The powerful CPU gives the user the option to run analysis software at the remote site thus preventing the need to download capture files over a slow connection link.

 **iridium**  
Everywhere

**4G**

**WiFi**

Wifi / 4G Modem / Iridium Modem

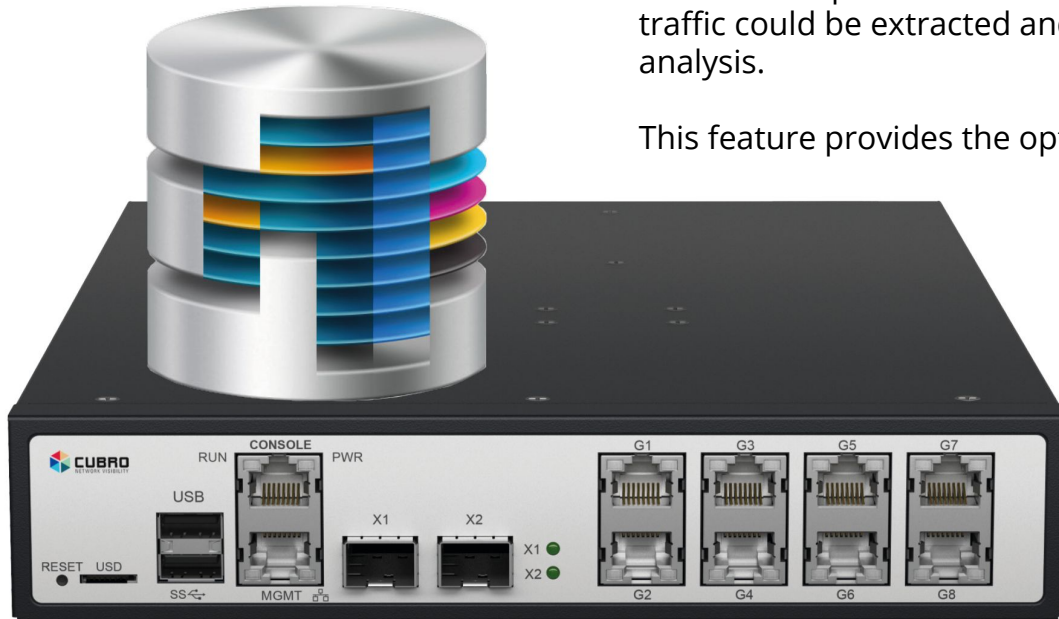


# Rolling Capture & Indexing

Rolling capture is a feature where the EXA8 is endlessly capturing traffic from the configured ports or links. If the reserved disk space is full, the rolling capture overwrites the older capture automatically.

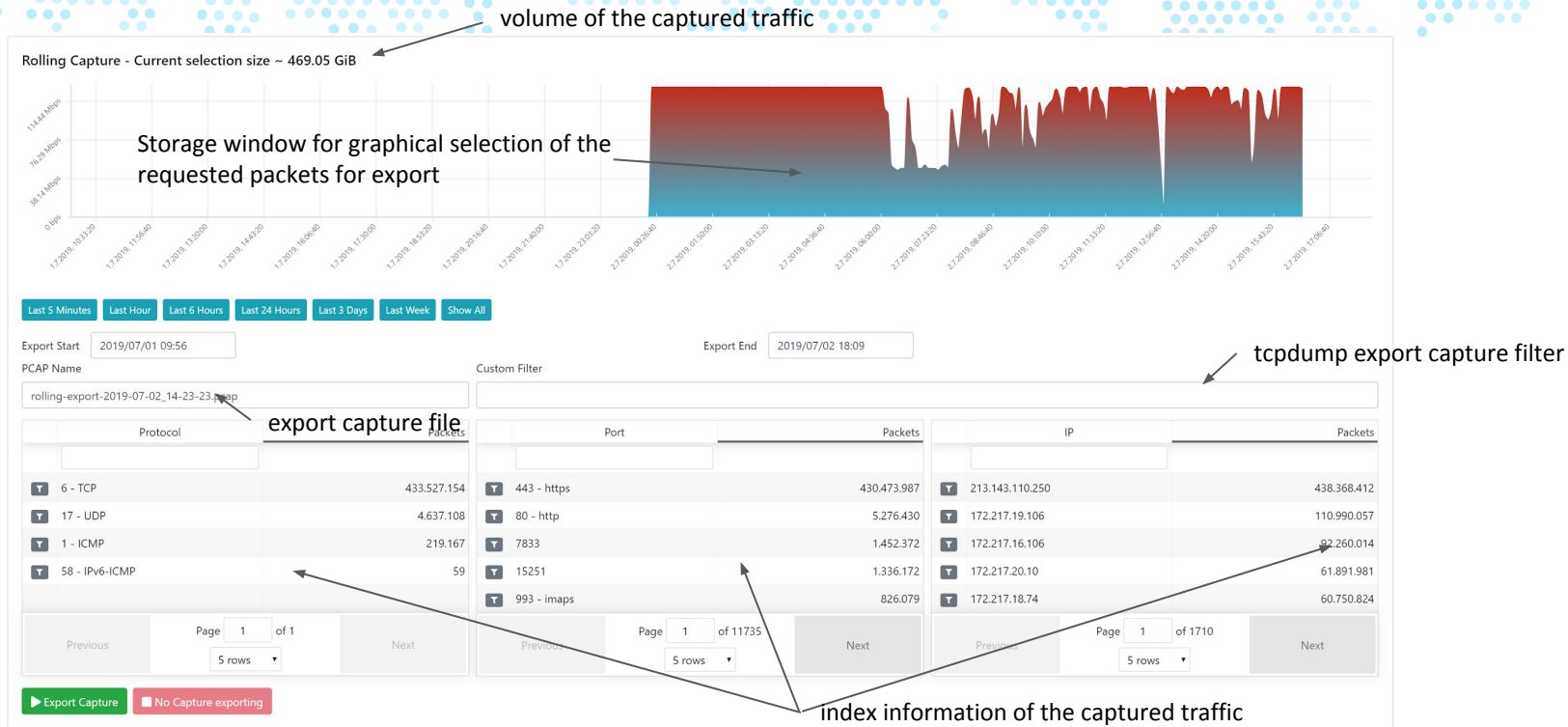
The rolling capture also produces an Index of the captured traffic (time, IP address and port information). With the help of this index the relevant traffic could be extracted and exported in a PCAP file for the purpose of analysis.

This feature provides the option to look back in time and find past events.



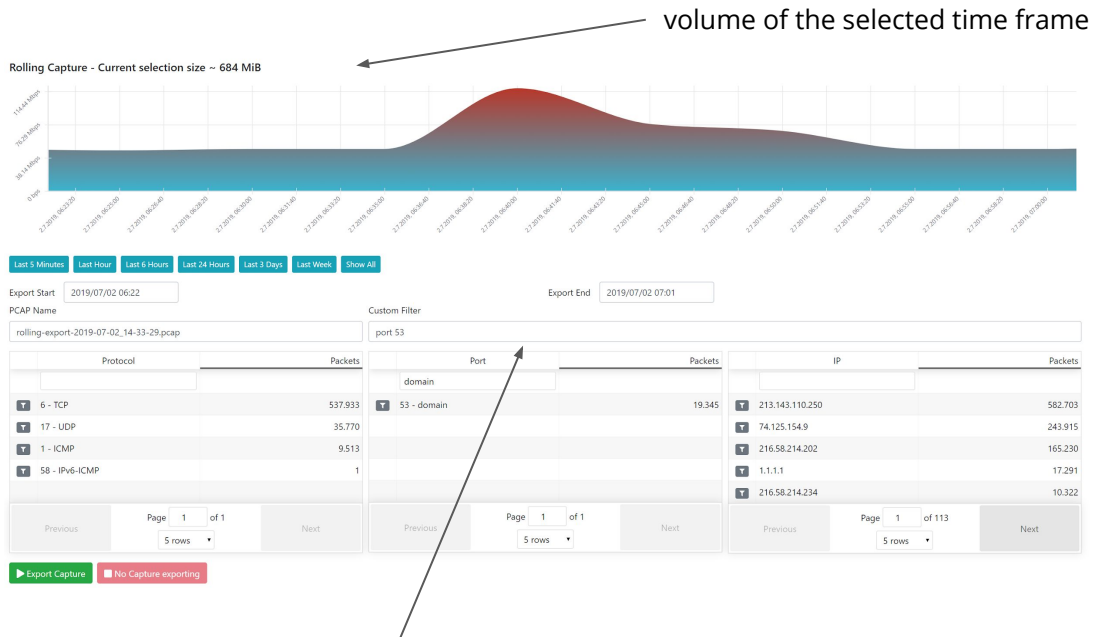


# Rolling Capture & Indexing



The rolling capture runs 24/7 and the user can extract the capture files by time or IP index and convert it to a PCAP for later analysis. There is also an option for a post filter via tcpdump during the export process.

# Rolling Capture & Indexing



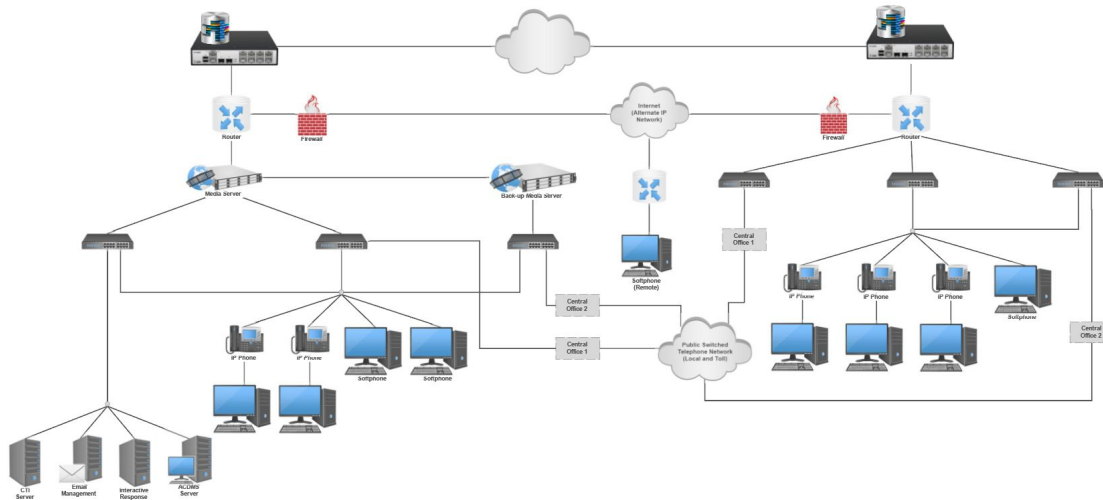
In this example we want to extract only DNS traffic from this time frame

# Rolling Capture & Indexing Use Case

Network troubleshooting is often not that easy because the problem appears only from time to time. In this case a standard capture will not help.

The Cubro Rolling Capture can quickly solve the problem, because the capture is **continuously running**, and when the error happens, the engineer can **look back in time through the capture file**. With the help of the query language you can **extract the right time frame and the relevant traffic filtered by IP address and port**.

In combination with the TAP and remote access, the EXA8 is the perfect **remote site troubleshooting tool**.

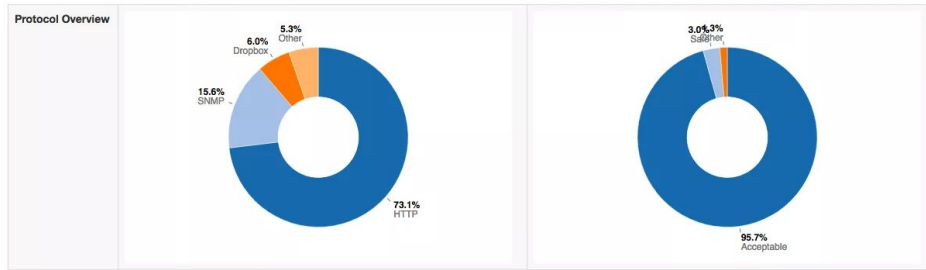


In this example the rolling capture is used on two WAN interfaces to see the behaviour of the WAN at the exact same time when the error event happens.

# Flowanalyzer on EXA8

The EXA8 offers a full featured Flow Analyzer.

This software gives a full online monitoring of the traffic which is connected to EX8



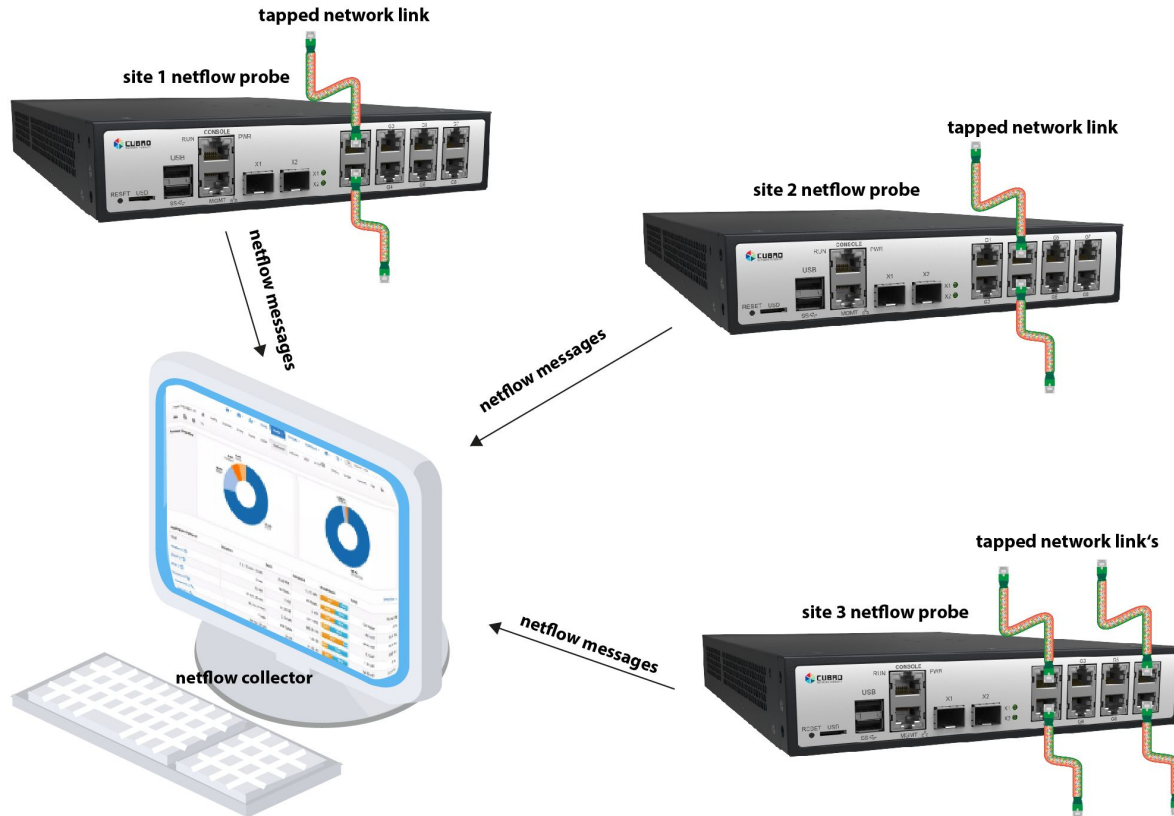
Direction ▾

| Application Protocol | Duration            | Sent     | Received | Breakdown                           | Total           |
|----------------------|---------------------|----------|----------|-------------------------------------|-----------------|
| <b>Total</b>         | 2 h, 10 min, 15 sec | 31.02 MB | 14.13 MB | <span>Sent</span> <span>Recv</span> | 45.15 MB        |
| Amazon               | 5 sec               | 66 Bytes | 60 Bytes | <span>Sent</span> <span>Recv</span> | 126 Bytes 0 %   |
| DHCP                 | 30 sec              | 2 KB     | 2 KB     | <span>Sent</span> <span>Recv</span> | 4.01 KB 0.01 %  |
| DNS                  | 10 min, 35 sec      | 27.32 KB | 57.11 KB | <span>Sent</span> <span>Recv</span> | 84.43 KB 0.18 % |
|                      |                     |          |          | <span>Sent</span> <span>Recv</span> | 2.7 MB 5.99 %   |
|                      |                     |          |          | <span>Sent</span> <span>Recv</span> | 1.91 KB 0 %     |
|                      |                     |          |          | <span>Sent</span> <span>Recv</span> | 54.53 KB 0.12 % |

| Application        | Protocol | Client          | Server                    | Duration | Breakdown     | Actual Thrt | Total Bytes | Info                        |
|--------------------|----------|-----------------|---------------------------|----------|---------------|-------------|-------------|-----------------------------|
| Unknown            | UDP      | 185.69.244.42   | openvpn                   | 01:26    | Client Server | 270.65 kb/s | 7.63 MB     |                             |
| IMAPS.GMail        | TCP      | Buchhaltung-HP  | 74.125.133.109            | 00:14    | Client Server | 38.94 kb/s  | 132.37 KB   |                             |
| WhatsApp           | TCP      | Lukas-iPhone    | 31.13.84.49               | 02:29    | Client Server | 11.35 kb/s  | 52.04 KB    |                             |
| SSL                | TCP      | ptik-pc         | 192.168.0.1               | 10:17    | Client Server | 10.28 kb/s  | 1.43 MB     |                             |
| SSL.GoogleServices | TCP      | etinger-PC      | presence.googleapis.com   | 33:24    | Client Server | 7.07 kb/s   | 360.02 KB   | presence.googleapis.com     |
| Google             | UDP      | openvpn         | music3907-4n-f110.1e100.n | 01:15    | Client Server | 6.04 kb/s   | 40.47 KB    |                             |
| SSL.WhatsApp       | TCP      | etinger-PC      | web.whatsapp.com          | 16:01    | Client Server | 4.64 kb/s   | 125.6 KB    | web.whatsapp.com            |
| SSL.Skype          | TCP      | etinger-PC      | db5-client-s.gateway.mes  | 01:31:49 | Client Server | 4.45 kb/s   | 163.75 KB   | db5-client-s.gateway.mes... |
| SSL.Google         | TCP      | LAPTOP-7UH81FDN | cm.g.doubleclick.net      | 00:09    | Client Server | 4.13 kb/s   | 25.0 KB     | cm.g.doubleclick.net        |
| SSL.Google         | TCP      | BEG-PC          | www.google.at             | 01:15    | Client Server | 3.26 kb/s   | 396.0 KB    | www.google.at               |

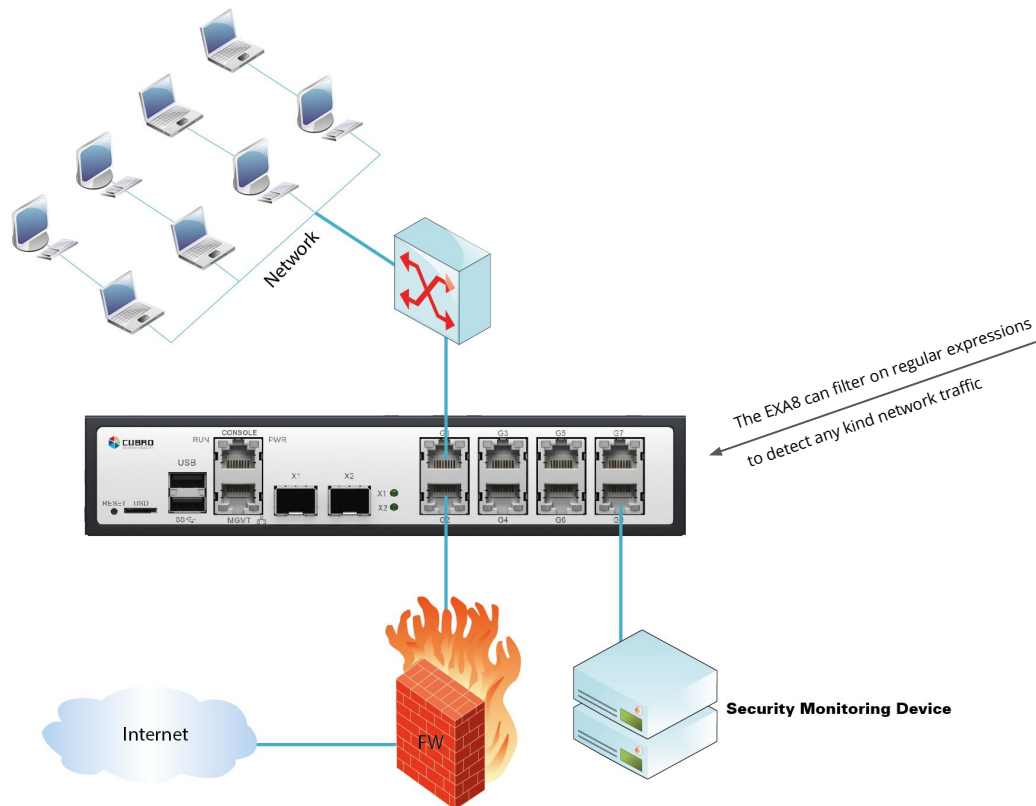
Showing 1 to 10 of 980 rows. Idle flows not listed.

# EXA8 as Netflow Probe

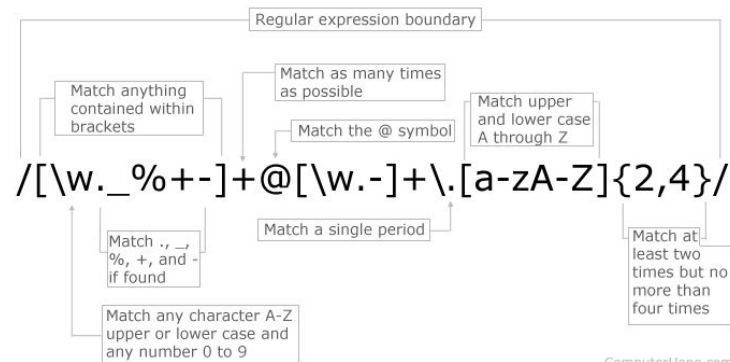


# Regex Filtering EXA8

## Regex filtering: DPI fingerprint filtering for security applications



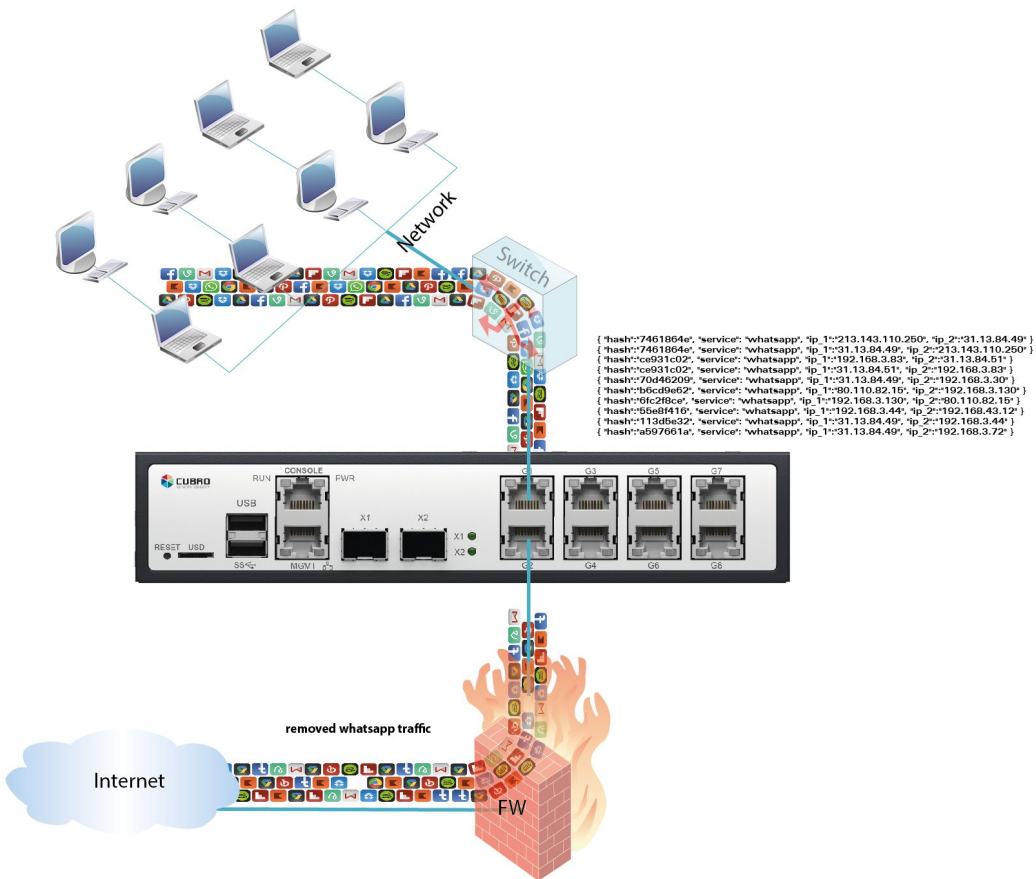
## Regular Expression E-mail Matching Example



ComputerHope.com



# DPI Filtering on EXA8



The EXA8 can be used to block inline any kind of traffic on application level. In this example Whatsapp.

We currently support up to 4000 signatures and applications.



# Quality & Environment Management



Cubro is certified with ISO 9001 for Quality Management to ensure to deliver best product and services



Cubro is certified with ISO 14001 for Managing the efforts to protect our environment.



**Cubro Network Visibility**  
Ghegastraße 1030 Vienna,  
Austria

**Tel.:** +43 1 29826660  
**Fax:** +43 1 2982666399  
**Email:** support@cubro.com

**Cubro Asia Pacific**  
8, Ubi Road 2 #04-12 Zervex  
Singapore 408538

**Tel.:** +65-97255386  
**Email:** jl@cubro.com



**THANK YOU**



**Cubro North America**  
105 Strowger Blvd  
Brockville, Ontario,  
Canada K6V 5K1

**Tel:** 613-213-0222  
**Email:** americas@cubro.com

**Cubro Japan**  
8-11-10-3F, Nishi-Shinjuku,  
Shinjuku,  
Tokyo, 160-0023 Japan

**Email:** japan@cubro.com

