



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



Intuitive Web GUI

The screenshot displays the CUBRO web interface for device management. At the top, a navigation bar includes 'EXA8', 'Device', 'Ports', 'Aggregation', 'Tapping', 'Capture', 'Shell', and 'Settings'. The user is logged in as 'admin' with a 'Sign out' option.

Device Information

Device Model	EXA8
Image Version	1.1.2-2.0
Serialnumber	124A-18C0007
Custom Device Label	<input type="text" value="N/A"/> Save

Device Configuration

[Save configuration](#) [Restore configuration](#) [Reset configuration](#)

Device Image

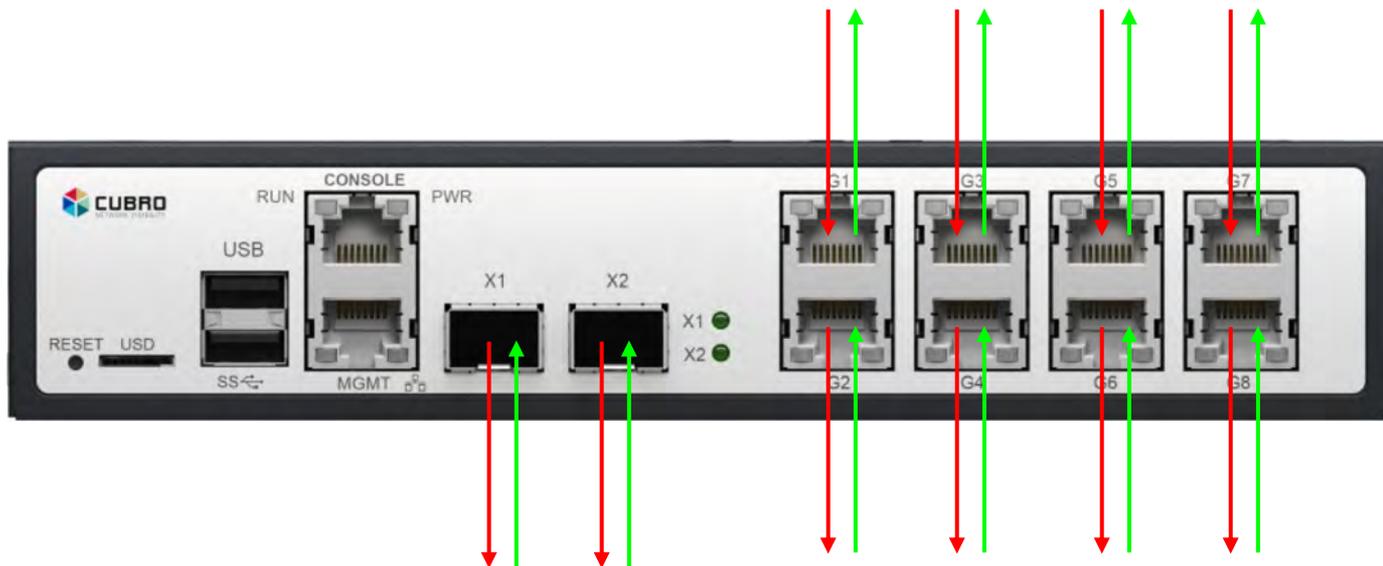
System Information

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

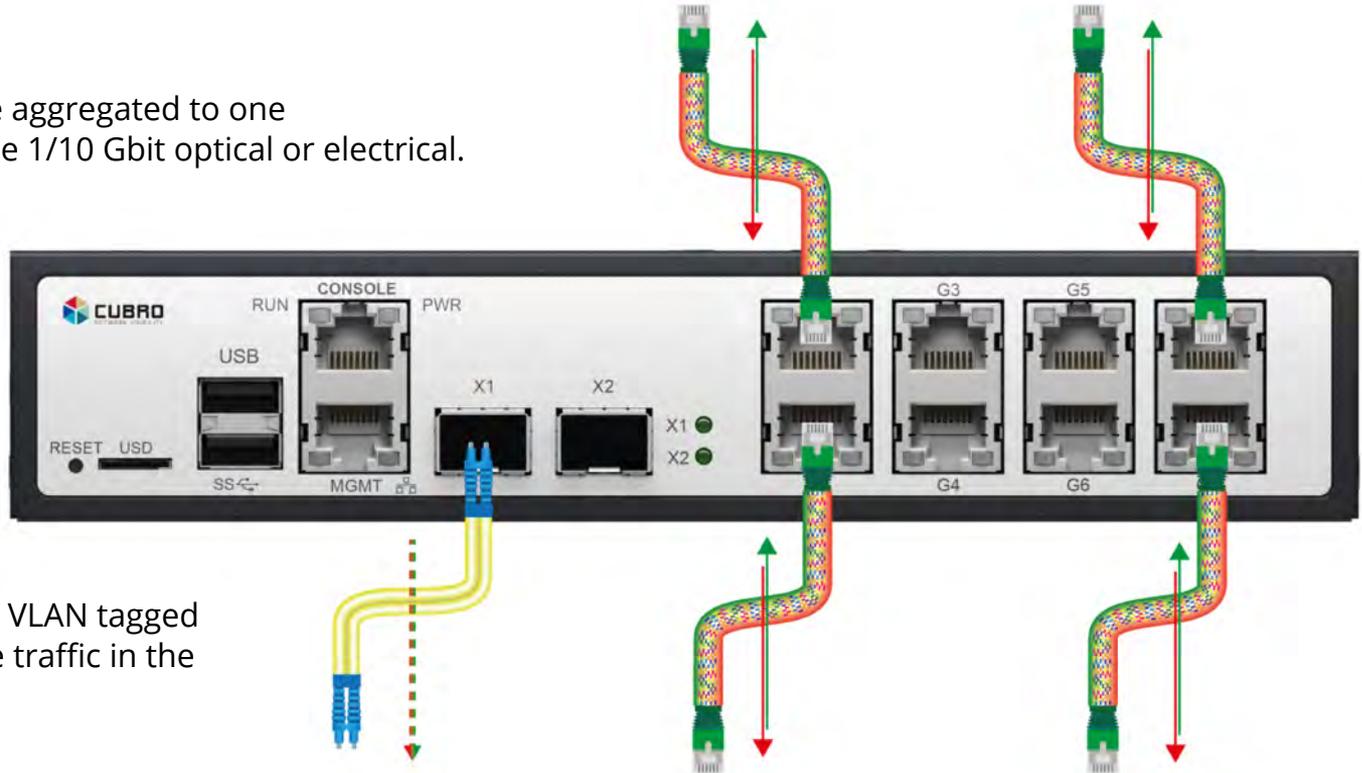


**2 x 1/10 Gbit
optical/electrical ports
usable as
input and output
(depending on the SFP
module)**

**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

The screenshot shows the CUBRO Aggregation GUI for device EXA8. The top navigation bar includes 'Device', 'Ports', 'Aggregation', 'Tapping', 'Capture', 'Shell', and 'Settings'. The main content is divided into two panels: 'Set Tag' and 'Aggregation Tag'.

Set Tag

Interface	Tag
G1	10
G2	20
G3	30
G4	40
G5	50
G6	60
G7	70
G8	80

Aggregation Tag

Interface	Tag
X1	10 20 30 40
X2	
Xv	60 80

Push Tag
 Disabled

Output Interfaces:

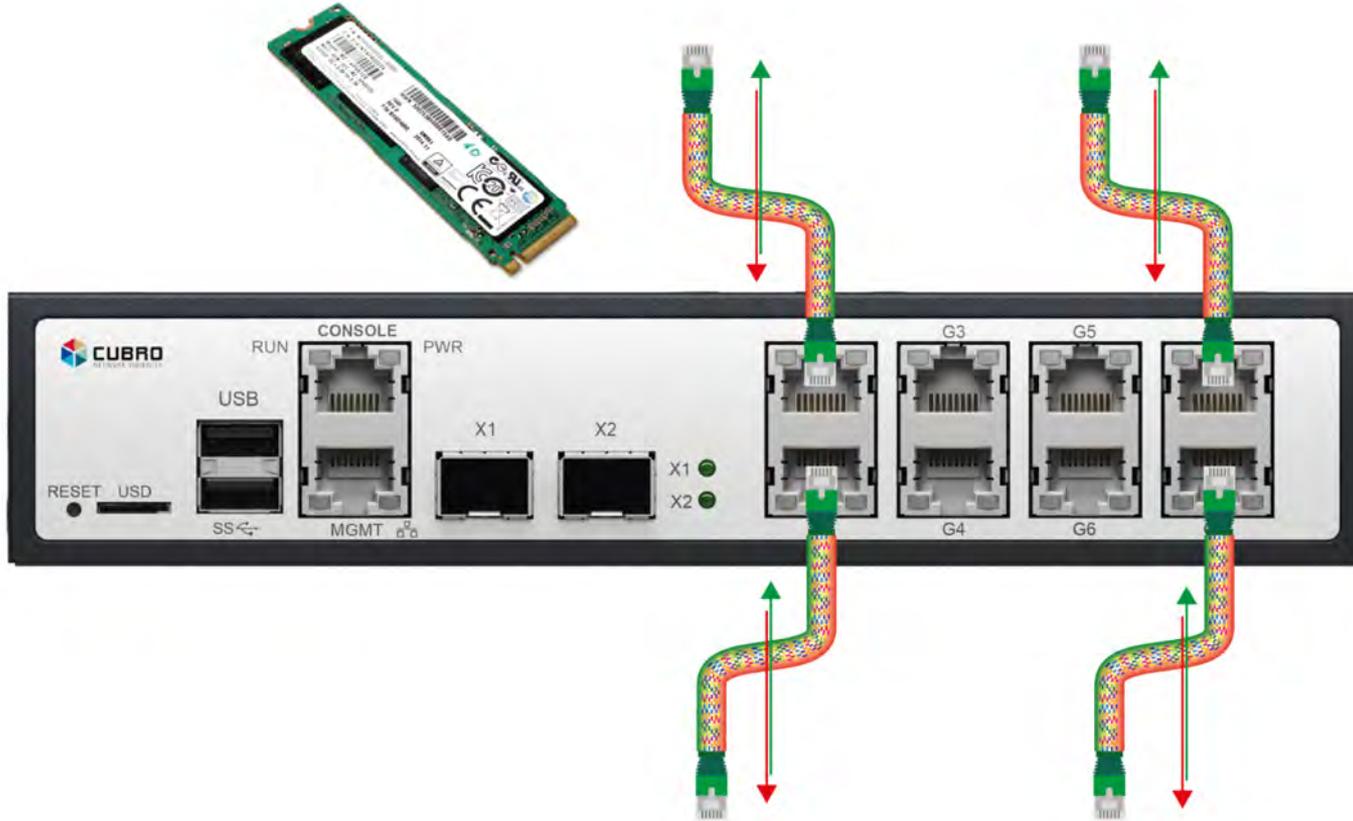
X1 and X2 = optical outputs
Xv = capture interface

Input Interfaces:

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

4 links

Aggregation & Capture to SSD



Tapping Session GUI

Tapping Configuration

Session:

Source Interfaces Configuration: → Destination Interface Configuration:

Active Tapping session

	Tapping Session	Source Interface(s)	Destination Interface
<input type="button" value="Clear"/>	Tapping Session 1	G1	G2
<input type="button" value="Clear"/>	Tapping Session 2	G2	G1
<input type="button" value="Clear"/>	Tapping Session 3	G3	G4
<input type="button" value="Clear"/>	Tapping Session 4	G4	G3
<input type="button" value="Clear"/>	Tapping Session 5	G5	G6
<input type="button" value="Clear"/>	Tapping Session 6	G6	G5
<input type="button" value="Clear"/>	Tapping Session 7	G7	G8
<input type="button" value="Clear"/>	Tapping Session 8	G8	G7

Capture GUI

The screenshot shows the CUBRO Capture GUI. At the top, there is a navigation bar with 'EXAB' and various menu items like 'Device', 'Ports', 'Aggregation', 'Tapping', 'Capture', 'Shell', and 'Settings'. On the right, it says 'Welcome! admin' and 'Sign out' next to the CUBRO logo.

The main section is titled 'Capture' and contains a 'PCAP Name' field with the value '2019-06-06_15-43-50.pcap'. Below this field is a 'Custom Filter' input box, which is pointed to by an arrow from the text 'custom tcp dump compatible filter string'. There are two buttons: a green 'Start Capture' button and a red 'No Capture running' button.

Below the capture configuration is a table titled 'PCAPs' with columns for 'Filename', 'Last Edited', and 'Filesize'. Each row has three small icons (green, blue, red) on the left, which are pointed to by arrows from the text 'delete capture file', 'download capture file', and 'start webshark (analyze capture file)' respectively.

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

custom tcp dump compatible filter string

delete capture file
download capture file
start webshark (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.



Wifi / 4G Modem / Iridium Modem

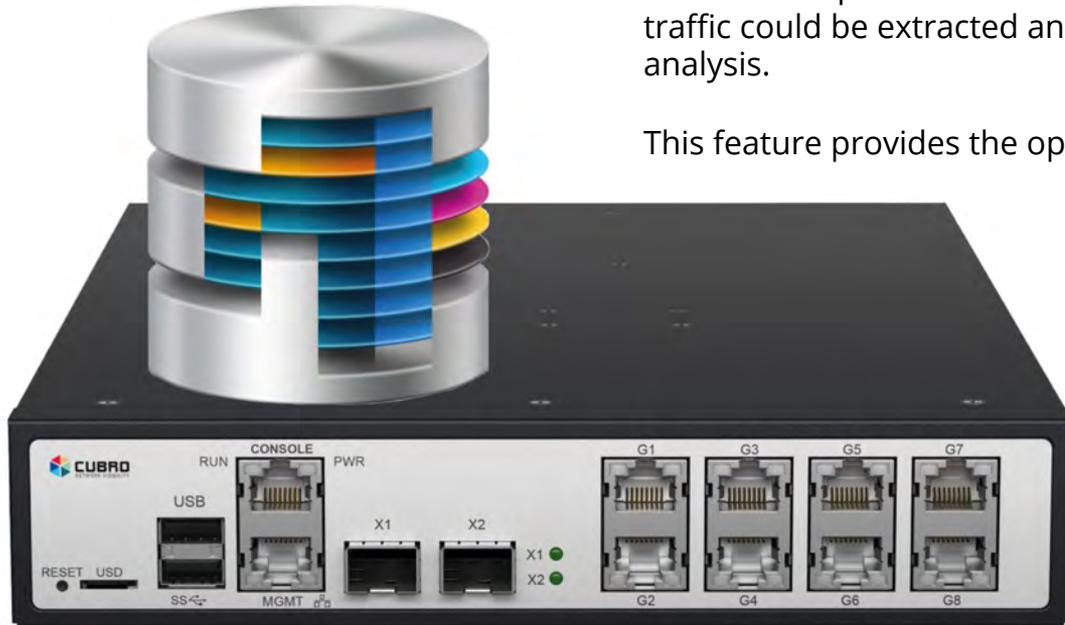


Rolling Capture & Indexing

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



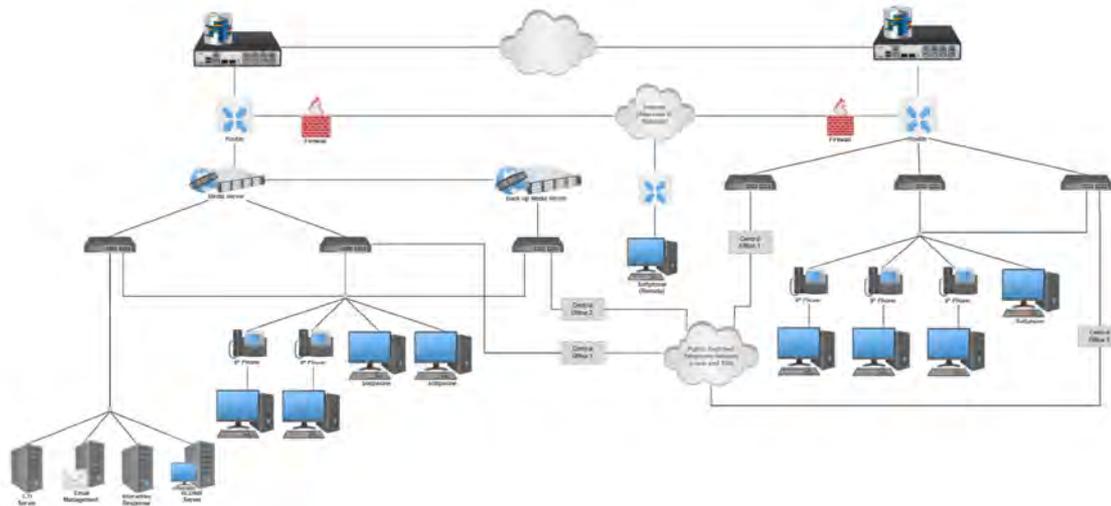
In this example we want to extract only DNS traffic from this time frame

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**.

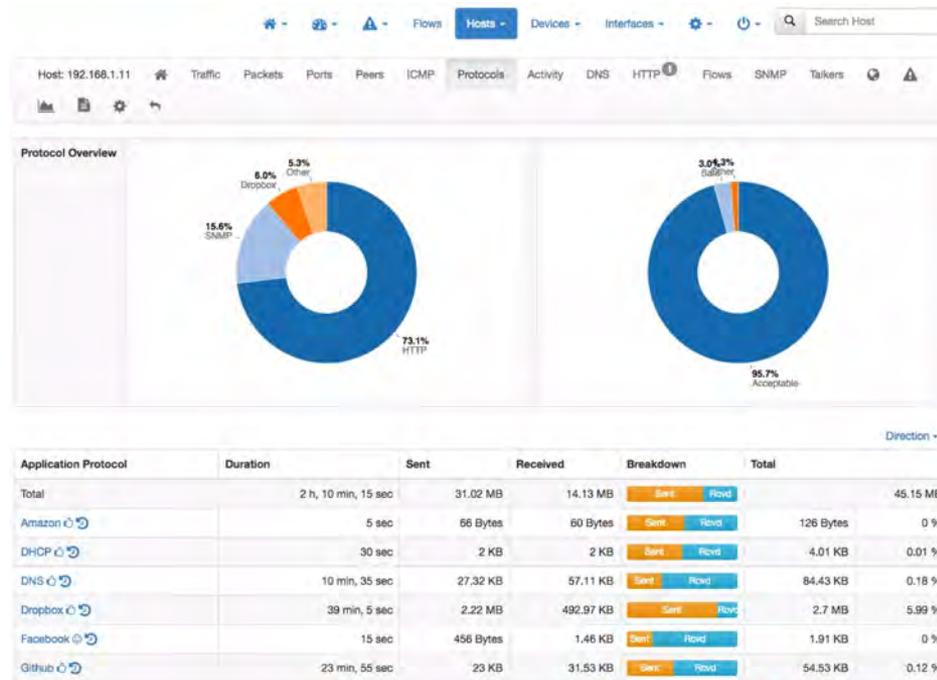


In this example the rolling capture is used on two WAN interfaces to see the behaviour of the WAN at the exact same time when the error event happens.

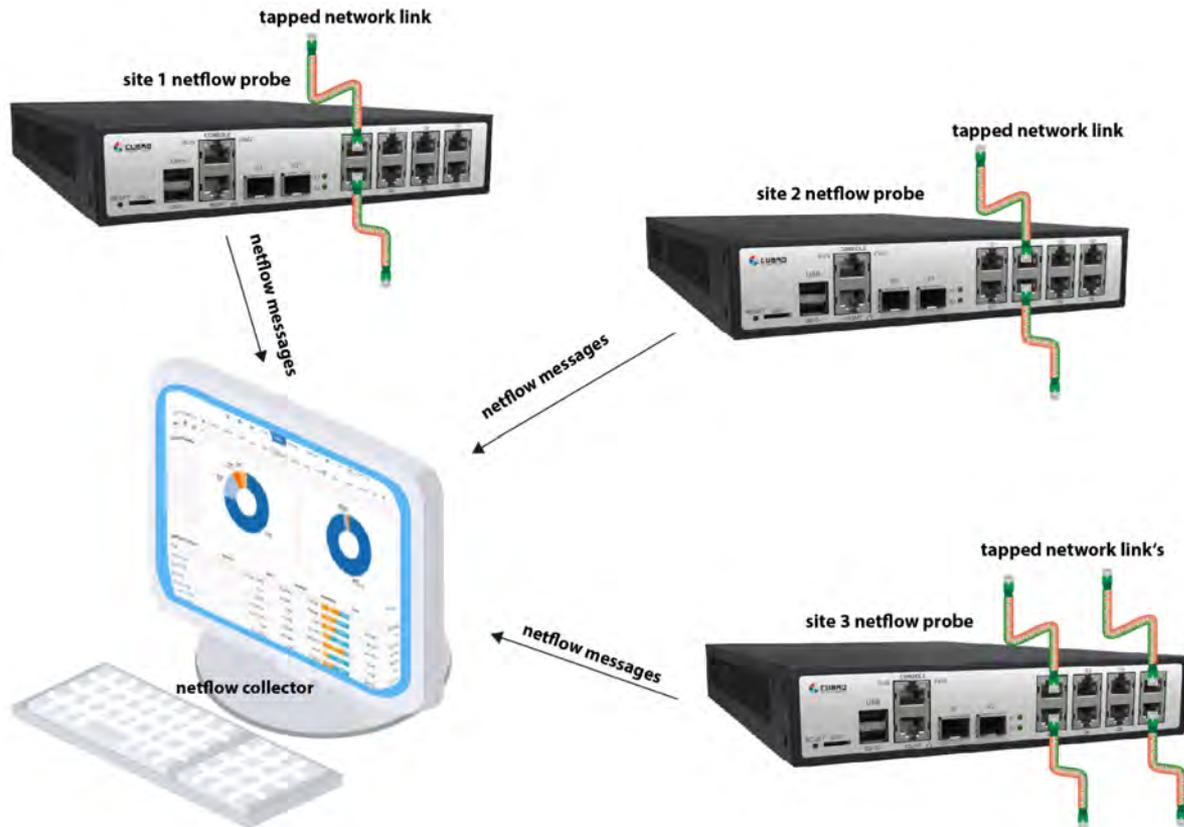
Netflow on EXA8

The EXA8 offers a full featured Netflow analyzer.

The user has the option to run the software in two different modes. The first is as only a Netflow generator. In this case the Netflow messages are sent to an external collector for higher performance and to support multiple probes. The second mode is for one EXA8 to serve as both a probe and collector for an out of the box, turnkey solution.



Multiple Netflow Probes



Software Roadmap for EXA8

Regex filtering: DPI fingerprint filtering for security applications

`[^]*?@[^]*?\. [^]*?`

