CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

DNS Traffic Analysis

Make networks more secure and find problems earlier

Use of Cubro Packetmaster & Sessionmaster for DNS traffic analysis

www.cubro.com

June 2018

DNS

CUBRO

- The domain name system (DNS) is a complex distributed database on which most Internet services rely on.

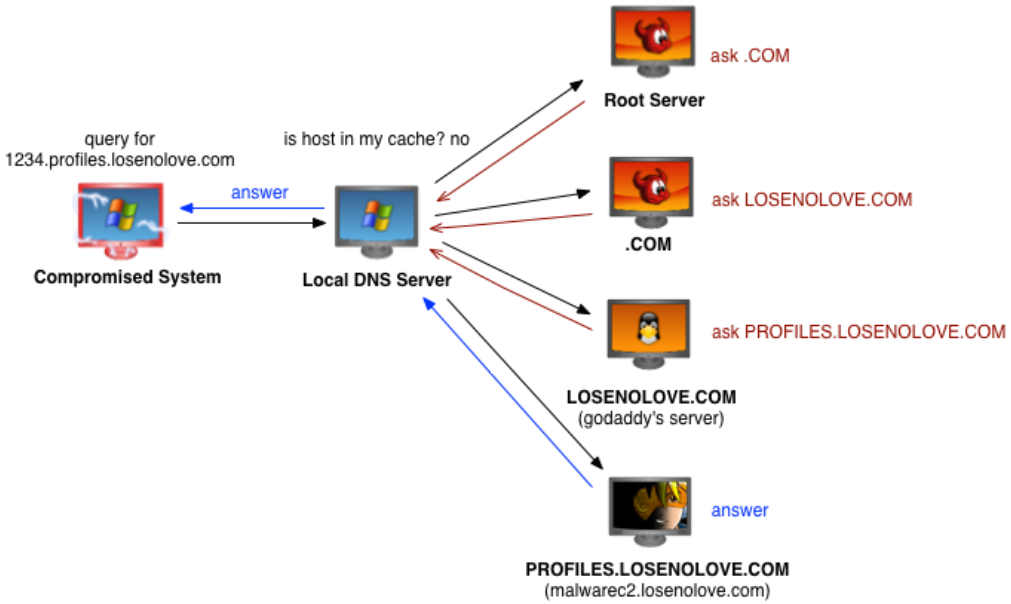
- Its monitoring is critical and it is necessary to continuously monitor DNS traffic for identifying anomalies, measuring performance, and generating usage statistics.

- Such analysis of DNS traffic has a significant application within information security and computer forensics, primarily when identifying insider threats, malware, cyberweapons, and advanced persistent threat (APT) campaigns within computer networks.

- While a primary driver for DNS Analytics is security, another motivation is understanding the traffic of a network so that it can be evaluated for improvements or optimization.

Security Aspects

- Leveraging DNS data to detect new Internet threats has been gaining in popularity in the past few years.



DNS performance

CUBRO

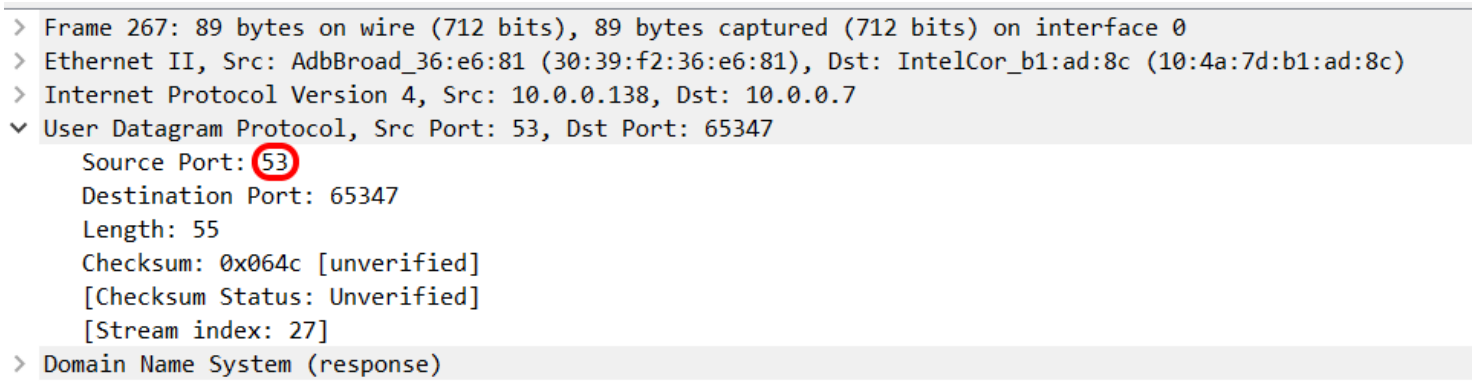
- DNS has a huge impact on overall network performance.
  - DNS is the Achille's heel of the web. It is often forgotten and its impact on performance ignored until it breaks down.

- Typical Problems are:
  - Low performance DNS server
    - too many requests
    - delayed answers
  - Low Time To Live in DNS cache

Monitor DNS traffic and improve performance

How to get access to DNS traffic?

- DNS traffic runs on UDP (or TCP) Port 53.
  - DNS traffic can be extracted by filtering on Port 53.



- **All** Cubro Packetmasters allow filtering up to OSI Layer 4; all Cubro Sessionmasters allow filtering up to Layer 4 AND beyond!
  - Only forward traffic to analysis tools that is really needed.
  - Don´t overload analysis tools
    - ***Make monitoring more efficient and more cost effective***

Make better use of existing monitoring tools

Packetmaster - Easy to use WebGUI

CUBRO

Main Properties

Cookie	○	0x0 – 0xffffffffffffffff
Name	◉ DNS Filter	
Description	Filter DNS Traffic and foward to Port 10	Only available if using name instead of cookie.
Priority	32768	0–65535 (lowest to highest prio.). Higher priority rules are tried first, ea

Match Fields

In-Ports		1 – 54, ranges allowed, e.g. "1, 3-5"
VLAN (802.1Q)	match all traffic (tagged and untagg	
MAC Source (+ /Mask)		e.g. FE:ED:FE:ED:FE:ED
MAC Dest. (+ /Mask)		e.g. FE:ED:FE:ED:FE:ED
Protocol	IP/UDP	Select to see protocol specific fields.
IP Source (+ /Mask or + /CIDR-Num.)		e.g. 1.2.3.4 or 4.3.2.1/255.255.255.1
IP Dest. (+ /Mask or + /CIDR-Num.)		e.g. 1.2.3.4 or 4.3.2.1/255.255.255.1
UDP Source (+ /Mask)	53	e.g. 42 or 3/255 or 0x3/0xff

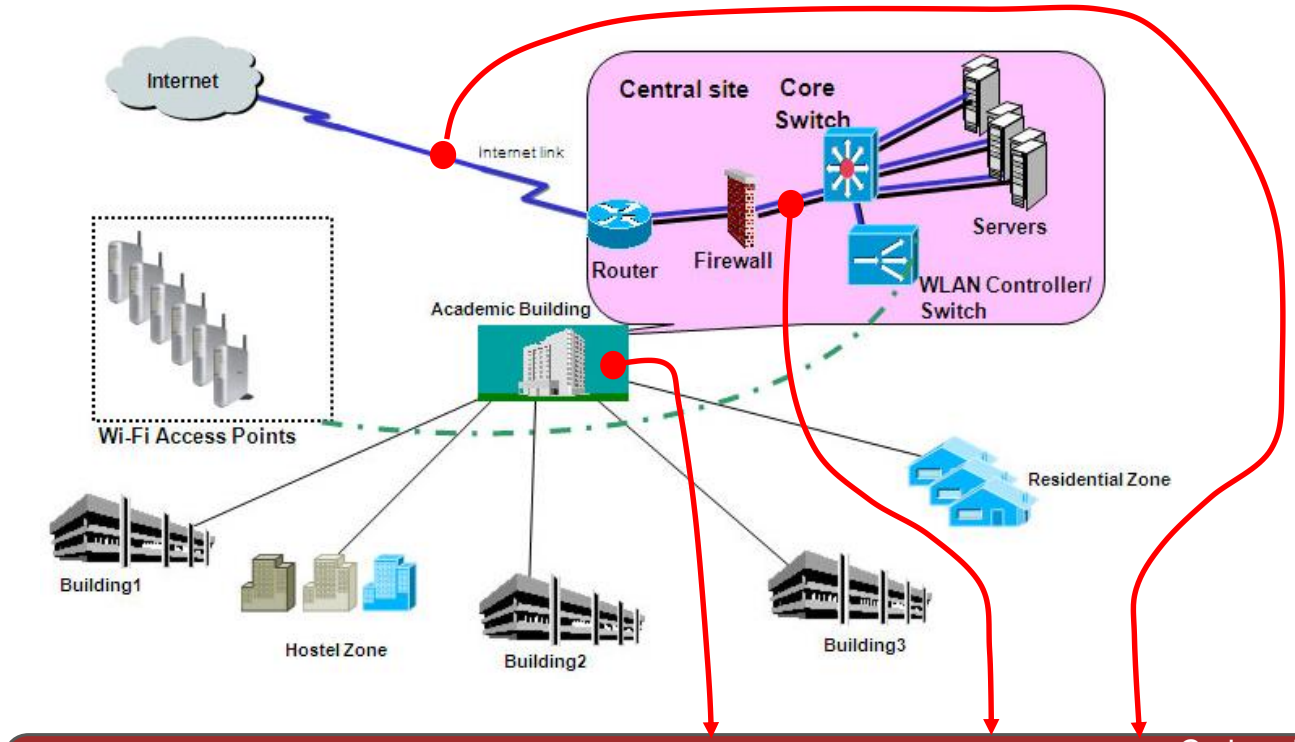
Actions

◉ Standard Actions

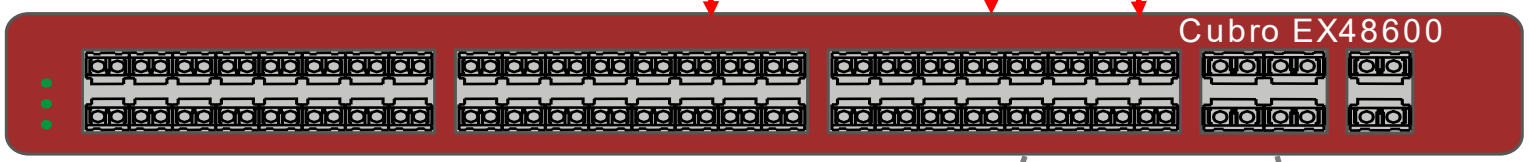
- ○ Drop
- ○ Output to Group
- ◉ Output to Ports: 10 (1 – 54)

Fast, Easy and Flexible

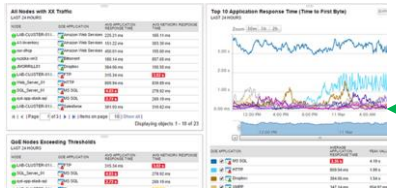
Typical Application Scenario



up to 8000 parallel filters!!!



DNS Traffic only

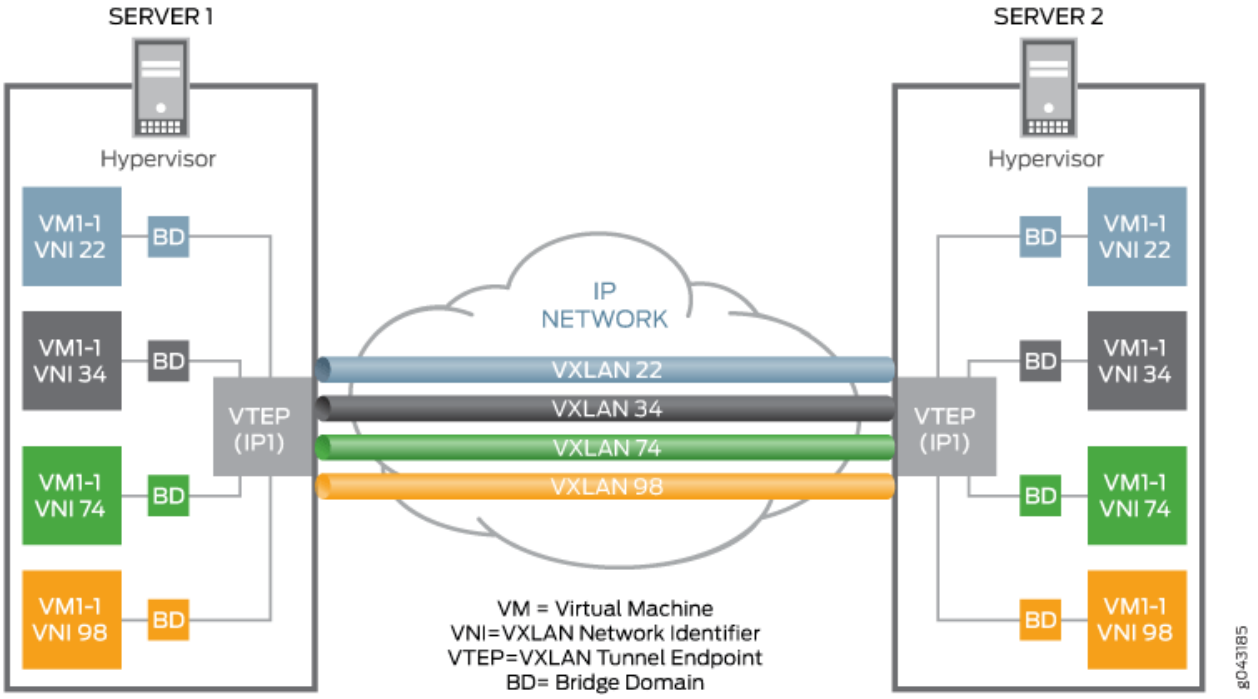


DNS Analysis Tool

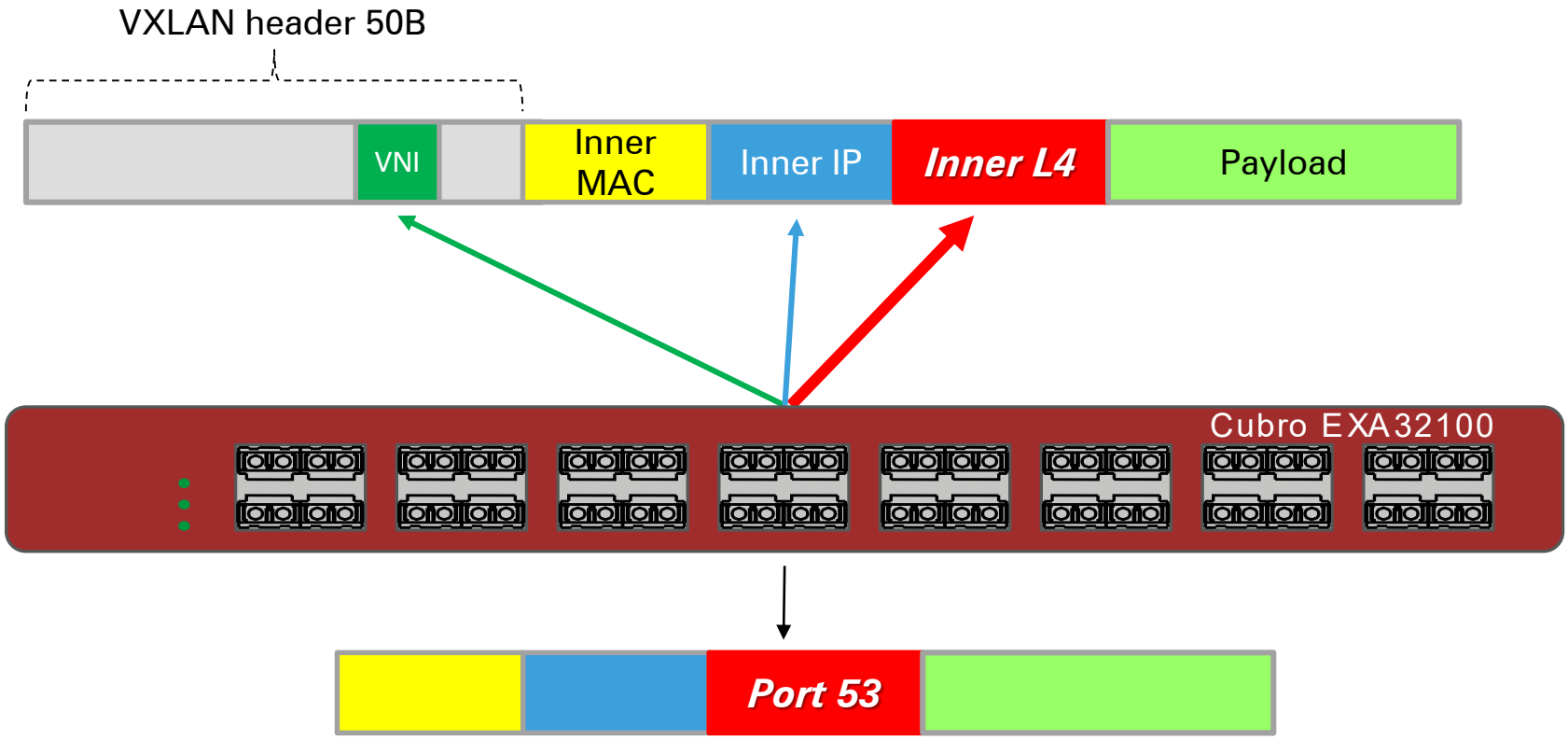
Other Monitoring Tools

Inside VXLAN tunnel

- In data centers, VXLAN is the most commonly used protocol to **create overlay networks** that sit on top of the physical network, enabling the use of a virtual network of switches, routers, firewalls, load balancers, and so on.



VNI, inner IP & inner Port filtering

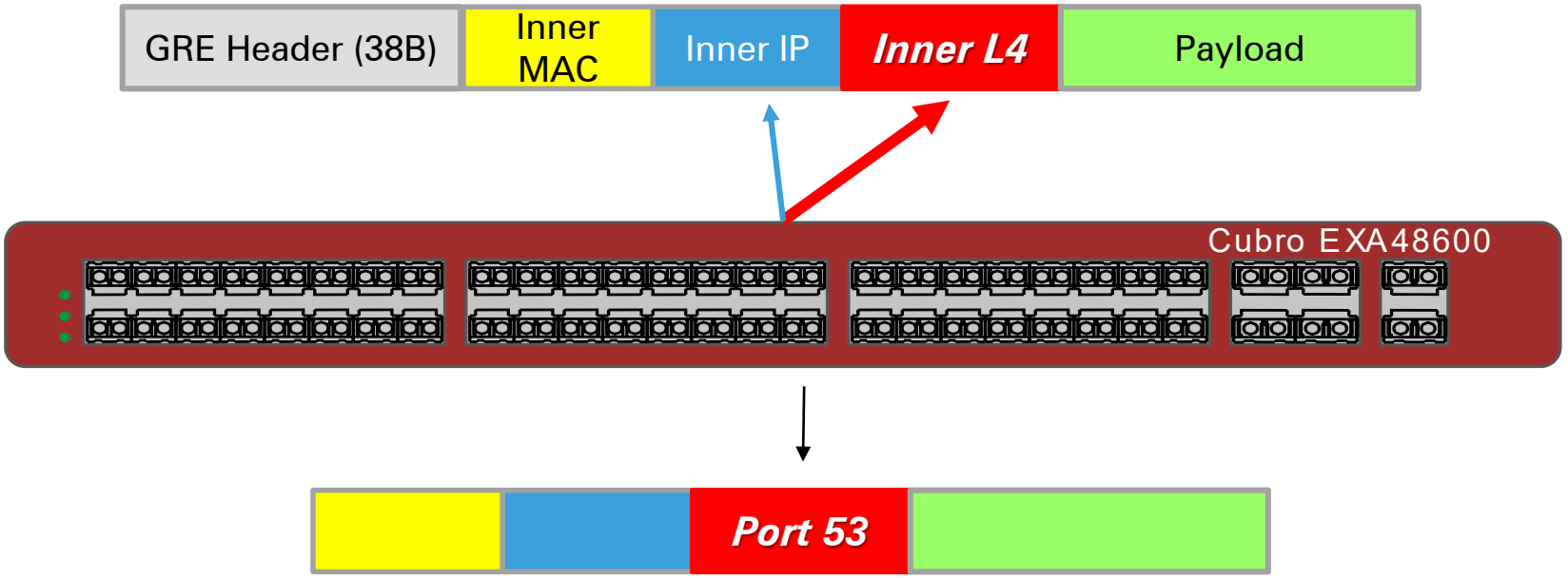


- Allows simultaneous filtering on
  - VXLAN identifier
  - Inner IP source and/or destination
  - **Inner L4** /TCP/UDP) source port and/or destination port –> **filter DNS traffic inside the tunnel**
  - Remove VXLAN header (if monitoring can´t deal with VXLAN header)

Inside GRE tunnel

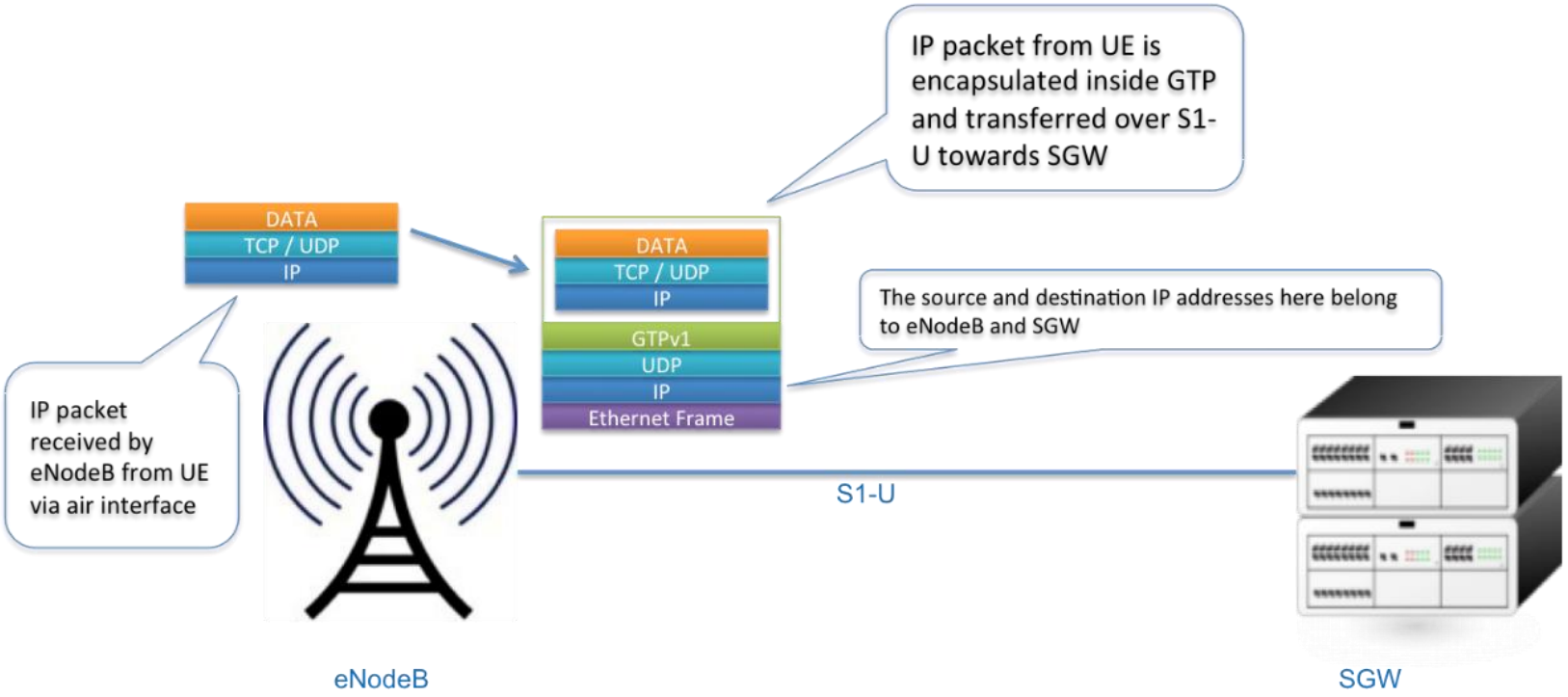
- All Cubro Packetmasters and Sessionmasters allow to remove GRE headers from incoming packets to release monitoring tools.

- Moreover, EXA32100 and EXA48600 allow **direct filtering** of inner IP and inner Port of GRE packets.



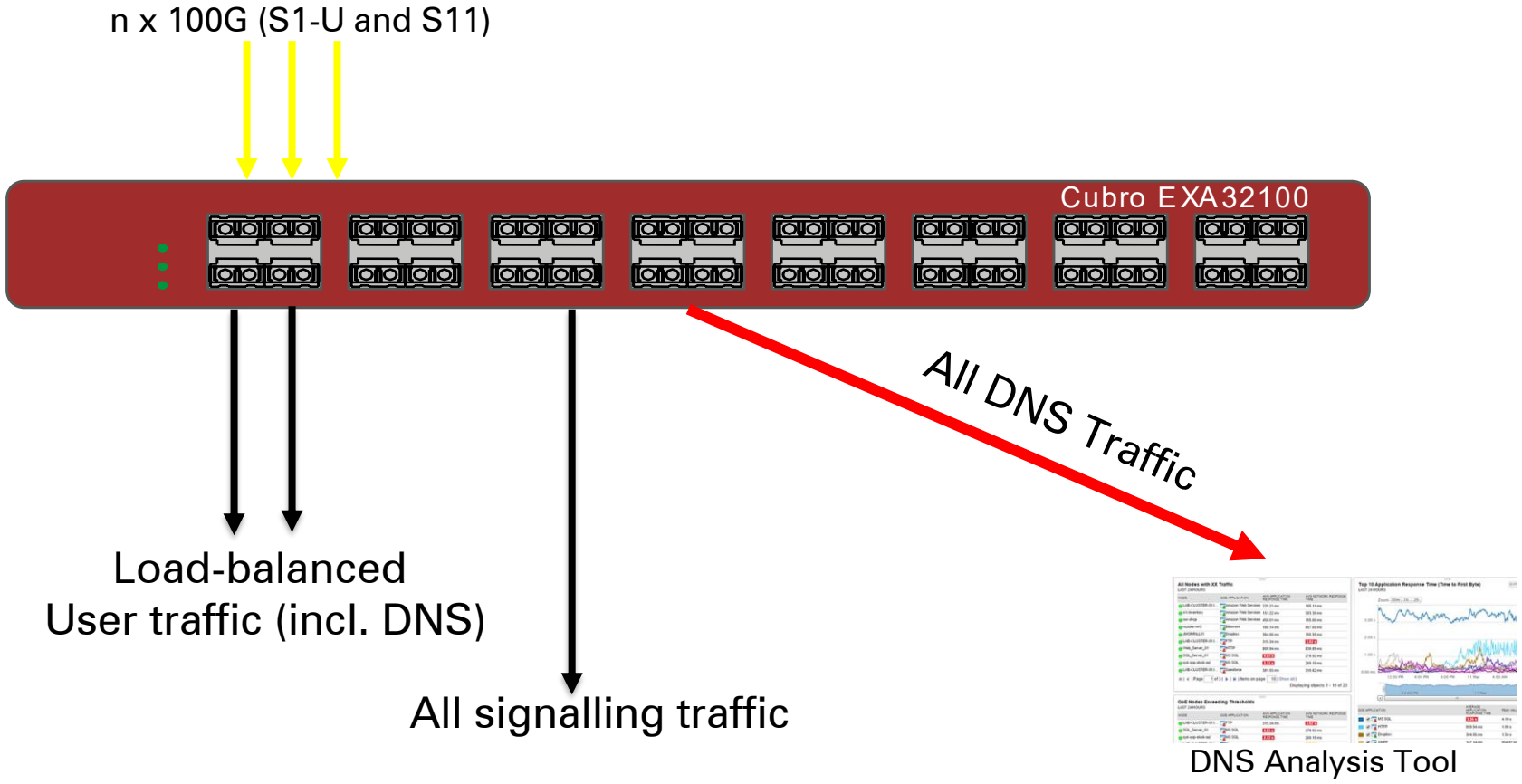
Inside GTP Tunnel (mobile operators)

- GTP is used to transport packet data from the eNodeB to the internet via an IP tunnel.



Inside GTP Tunnel (Mobile Operators)

- EXA48600 and EXA32100 can directly filter inside the tunnel (inner IP = user IP and/or inner TCP/UDP Port).



Summary

- Cubro Packetmaster and Sessionmaster products are the perfect choice to get access to DNS traffic.
  - Regardless if traffic is straight such as IPv4, IPv6 or encapsulated like VXLAN, GRE or GTP.

Thank you

EMEA

Cubro Network Visibility
Ghegastraße 1030 Vienna,
Austria

Tel.: +43 1 29826660
Fax: +43 1 2982666399

Email: support@cubro.com

North America

Cubro US
337 West Chocolate Ave
Hershey, PA 17033

Tel.:717-576-9050
Fax.: 866-735-9232

Email: support@cubro.com

APAC

Cubro Asia Pacific

8, Ubi Road 2 #04-12 Zervex
Singapore 408538

Tel.: +65-97255386

Email: jl@cubro.com

Japan

Cubro Japan

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

Email: japan@cubro.com