Cubro DNS Filtering

APPLICATION NOTE

CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Contents

1. DNS Background
2. Examples of the importance of DNS monitoring
3. Filtering DNS traffic with Cubro Packetmasters
4. VXLAN and DNS filtering
5. GRE and DNS filtering
6. GTP and DNS filtering
7. Summary

Domain Name System (DNS) Background

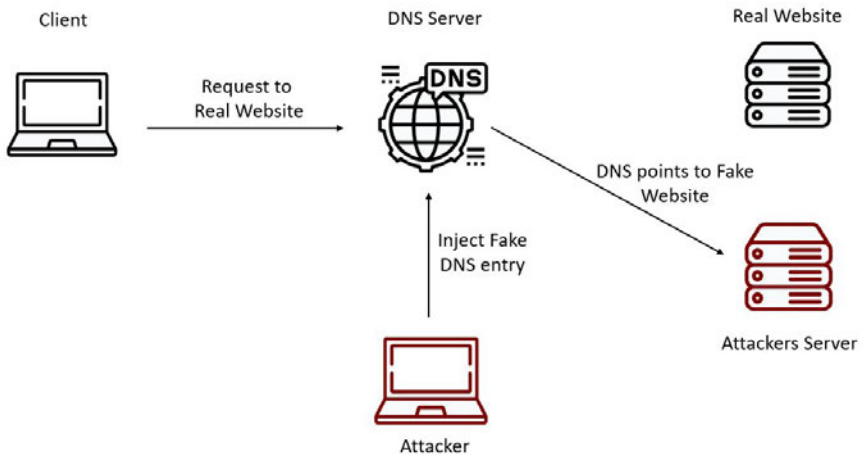
DNS is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. It translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. The purpose of this presentation is to highlight the importance of DNS and how Cubro helps in getting the vital information from the network

- Because of the importance of DNS, its continuous monitoring is critical for identifying anomalies, measuring performance, and generating usage statistics.
- DNS traffic monitoring and analysis has a significant importance within information security and computer forensics, primarily when identifying insider threats, malware, different types of cyber weapons, and advanced persistent threat (APT) campaigns within computer networks. For example attack.mitre.org has documented several DNS attack methods based on DNS poisoning, DNSCalc and Shadow DNS to name a few
- While the primary driver for DNS Analytics is security, another motivation is to understand the traffic of a network to execute either network improvements or optimization.

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

Security

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



DNS poisoning first needs access to the local DNS server and once being inside it changes one or several DNS entries to point to a different destination. This can be spread amongst the DNS servers

DNS Performance

- 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

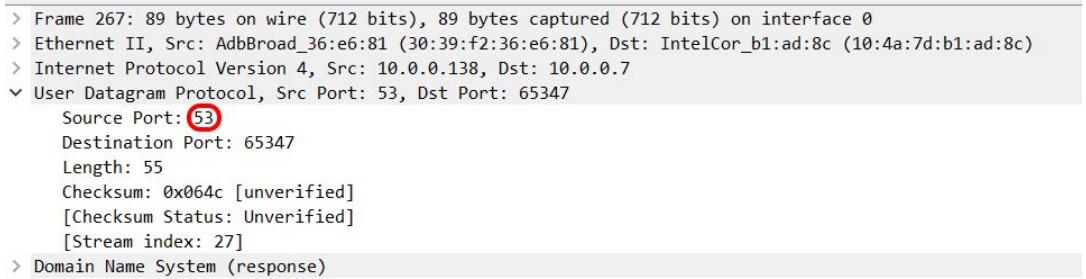
Monitor DNS traffic and improve performance

There are public services that measure the response times of DNS services (for example dnsperf.com). Home users can in many cases change their DNS service to another DNS provider whereas CSPs are using their local cache DNS servers that theoretically can improve the performance. This however is not always the case and therefore it is important to verify the performance

How to get access to DNS traffic?

DNS traffic runs on UDP (or TCP) Port 53 and can be extracted by the port number.

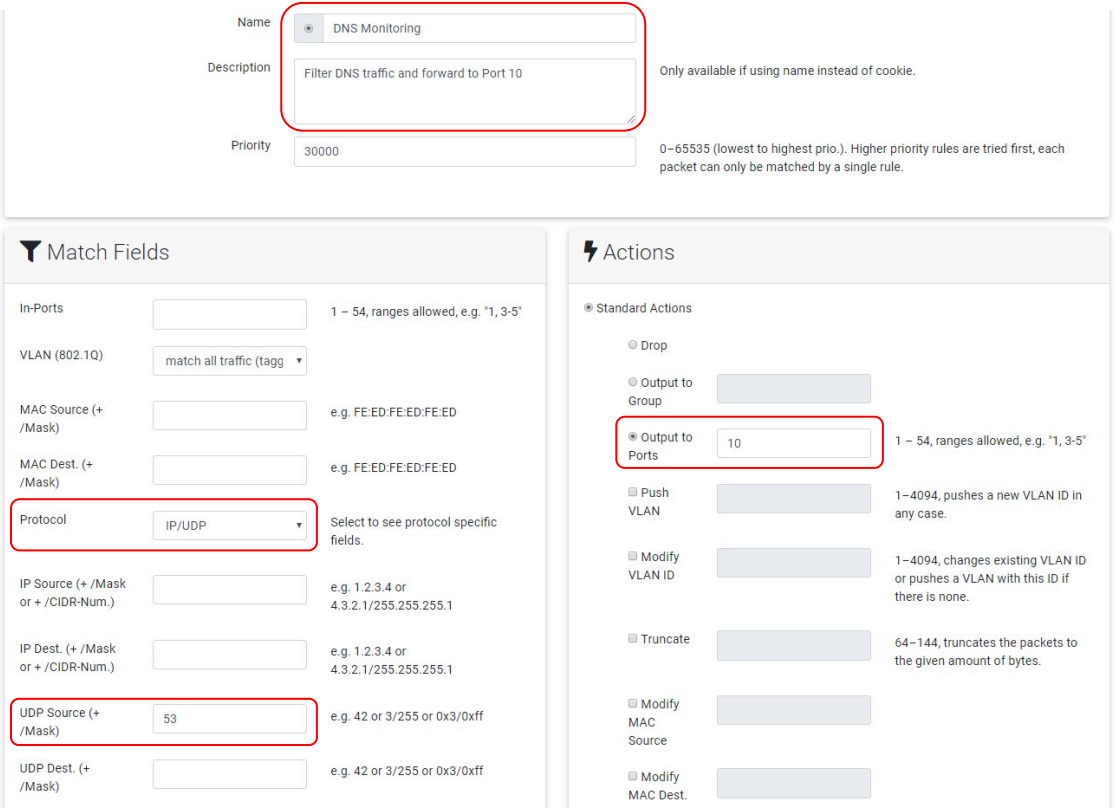
- All Cubro Packetmasters allow filtering up to OSI Layer 4
- All Cubro Sessionmasters allow filtering up to Layer 4 and beyond



Make monitoring more efficient and cost effective

- Only forward traffic that is really needed to analysis tools
- Use load balancing and other methods to avoid overloading analysis tools

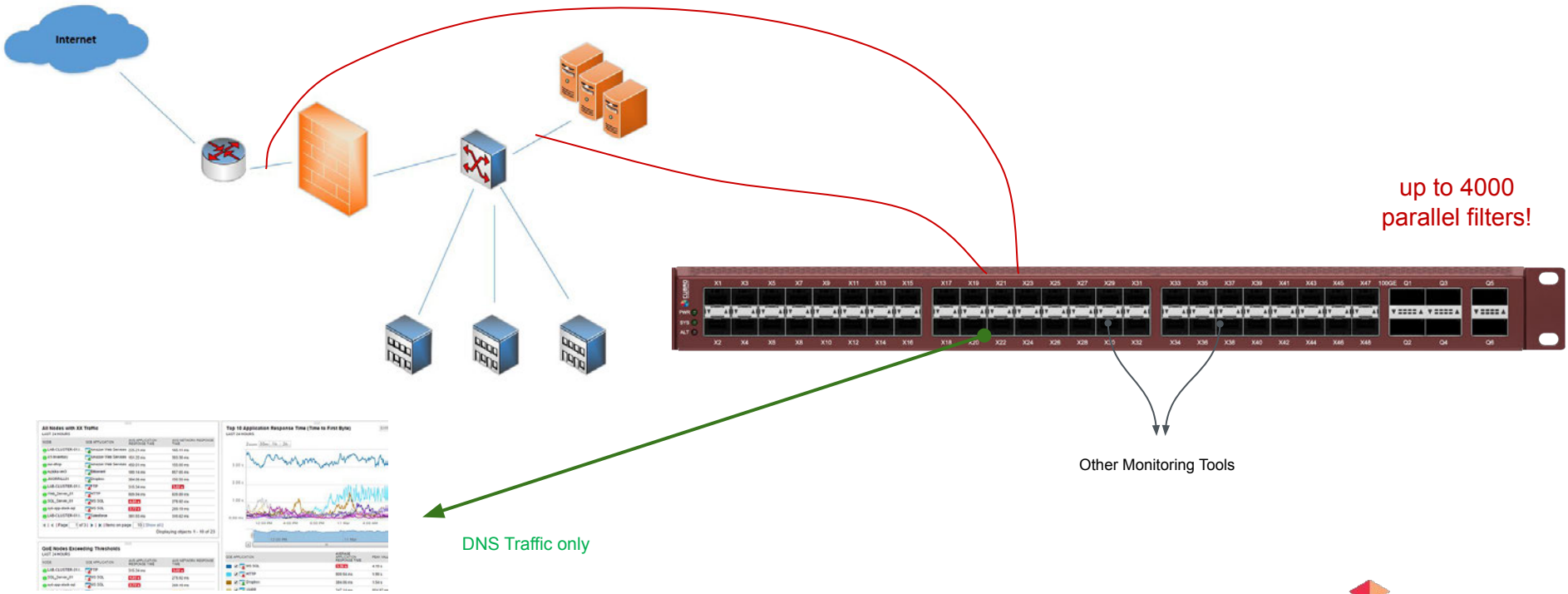
Easy to use WebGUI



Fast, Easy and Flexible

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

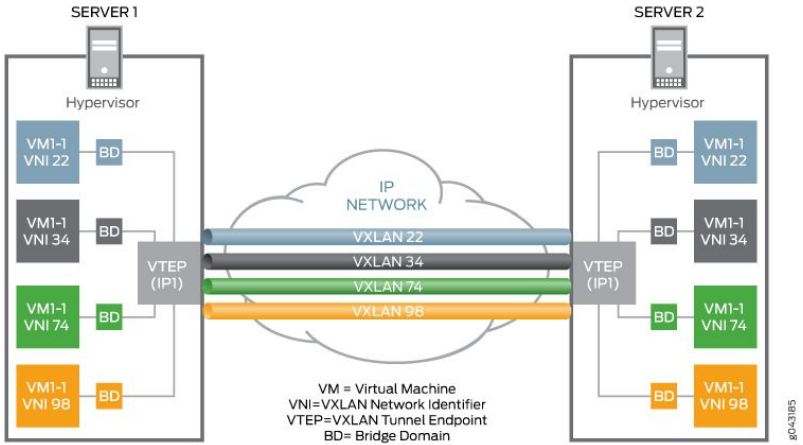
Scenario



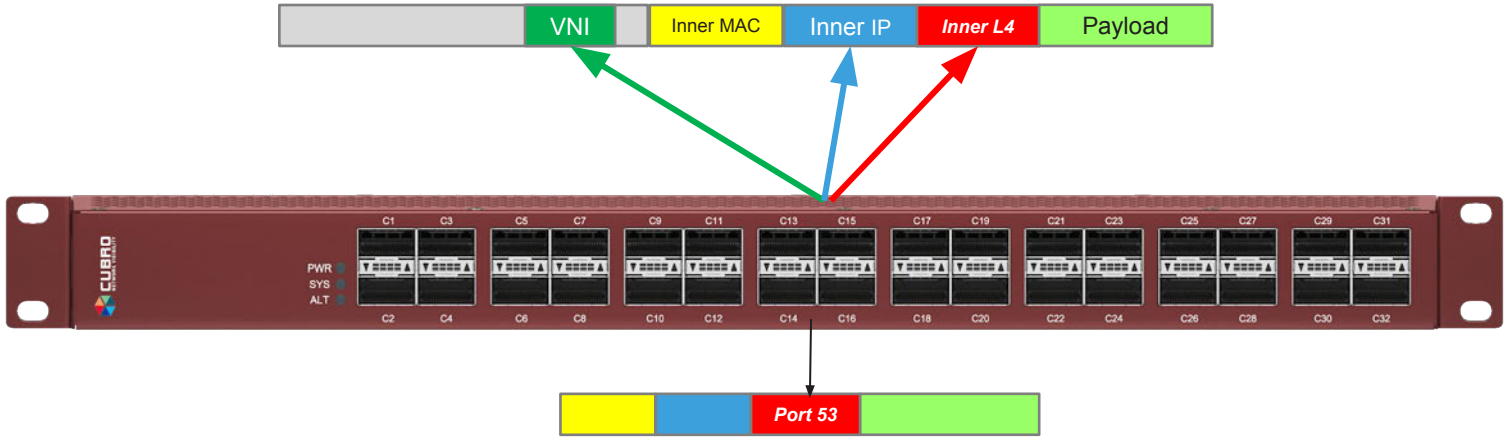
CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

VxLAN Tunnel and DNS

In data centers and in cloudified environments, 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. This raises the question of how to monitor DNS when VXLAN is used.



VXLAN and DNS filtering



Simultaneous filtering

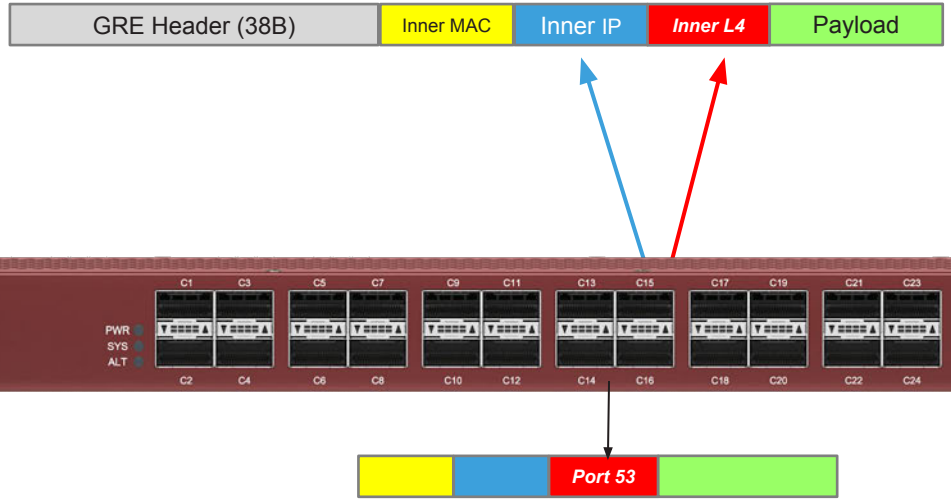
VXLAN identifier (VNI)	Inner IP source and/or destination IP	Inner L4 (TCP/UDP) source port and/or destination port*	Remove VXLAN header

*Filter DNS traffic inside the VXLAN tunnel

**Needed if the monitoring tool cannot understand VXLAN

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

GRE and DNS filtering



Simultaneous filtering

Remove GRE headers

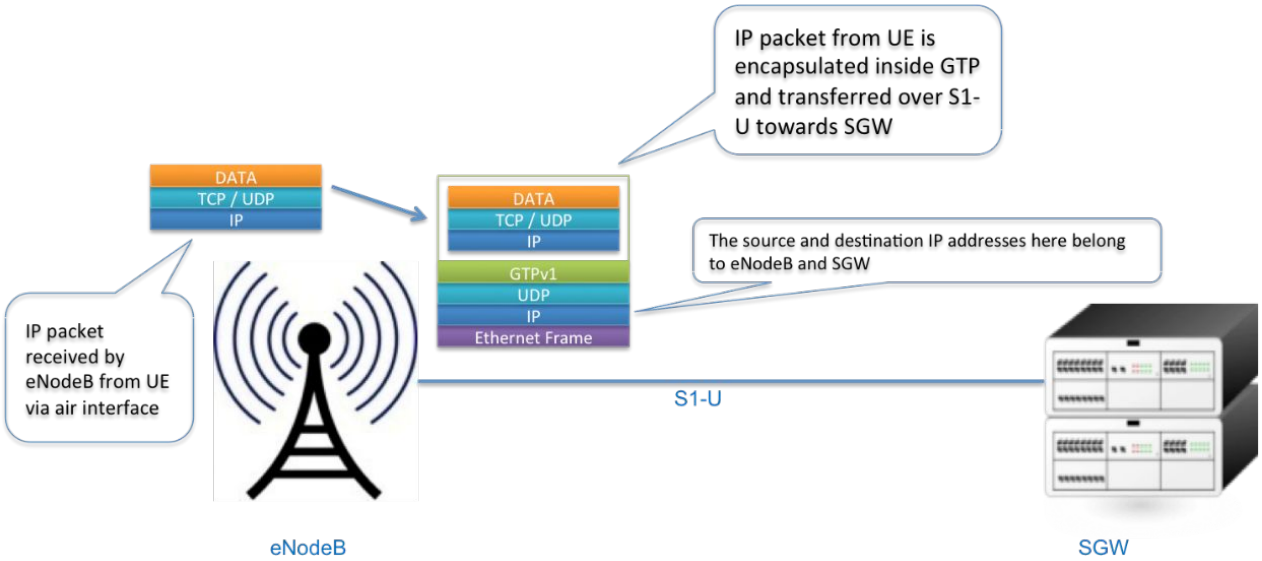
Inner IP source and/or destination IP

Inner L4 (TCP/UDP) source port and/or destination port*

CUBRO NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

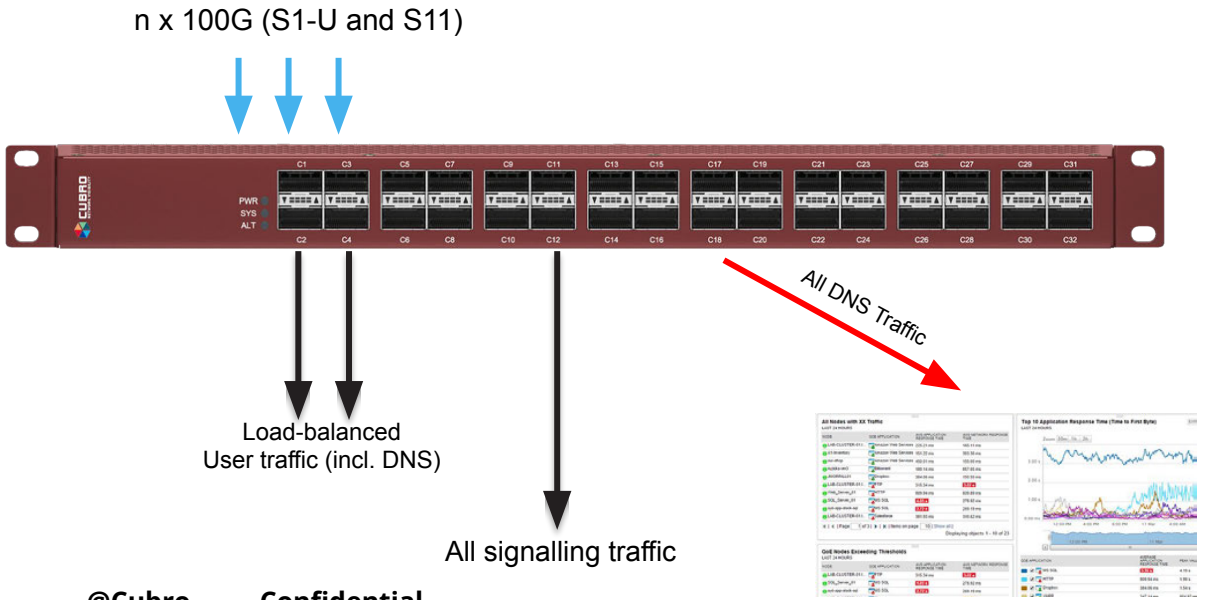
GTP and DNS filtering

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



GTP and DNS filtering

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 have inbuilt capability of inner IP and port filtering thus making them a perfect choice to get access to DNS traffic regardless of whether traffic is plain IPv4, IPv6 or encapsulated using VXLAN, GRE or GTP.


THANK YOU