CUBRO
NETWORK VISIBILITY

# ACHIEVING ACCURATE VISIBILITY IN VXLAN NETWORKS

## APPLICATION NOTE

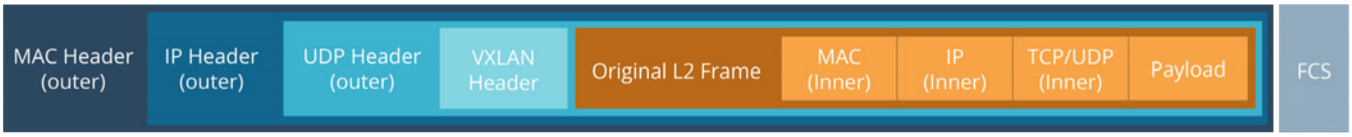
**Published at Cubro, March 2025**
Please refer to the latest version of this document on our website
to ensure you have the most up-to-date information.

## Introduction

Attaining comprehensive visibility into overlay networks while maintaining logical separation of traffic poses a significant challenge. As Network Functions Virtualization (NFV) deployments expand rapidly, the use of Virtual extensible LAN, VXLAN, as the protocol of choice in Leaf-Spine architectures has increased significantly. While VXLAN overlays offer scalability and flexibility, they also introduce complexity and make network visibility challenging since the essential information becomes encapsulated within VXLAN tunnels. Traditional monitoring tools often struggle to process VXLAN-encapsulated traffic, leading to critical gaps in network visibility.

## Challenges of VXLAN Visibility

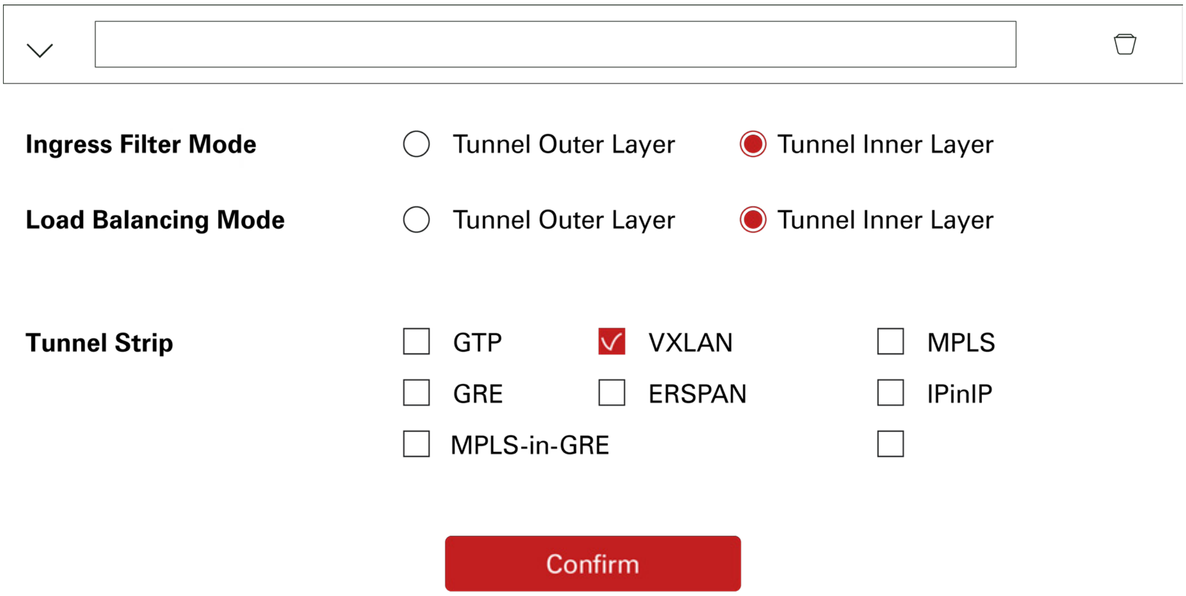
VXLAN encapsulation increases packet size and hides original traffic details inside the tunnel, making monitoring more difficult.



Traditional Layer 2 to Layer 4 monitoring systems cannot interpret VXLAN, which results in an inability to filter or analyze specific traffic within tunnels. The inability to see inside VXLAN tunnels leads to monitoring blind spots, increased operational complexity, and potential security risks.

## Cubro's Technical Solutions for VXLAN Visibility

Cubro's Advanced Network Packet Brokers provide a powerful solution for modern VXLAN networks, offering full support for VXLAN tunnel handling.



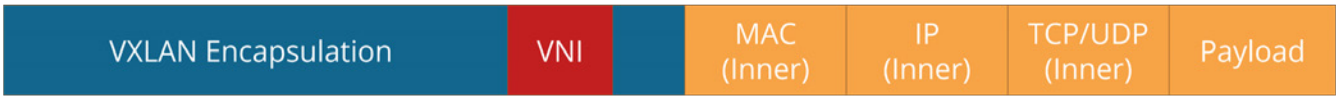
**Ingress Filter Mode** ○ Tunnel Outer Layer ● Tunnel Inner Layer

**Load Balancing Mode** ○ Tunnel Outer Layer ● Tunnel Inner Layer

**Tunnel Strip** □ GTP ☑ VXLAN □ MPLS
□ GRE □ ERSPAN □ IPinIP
□ MPLS-in-GRE □

These features include:

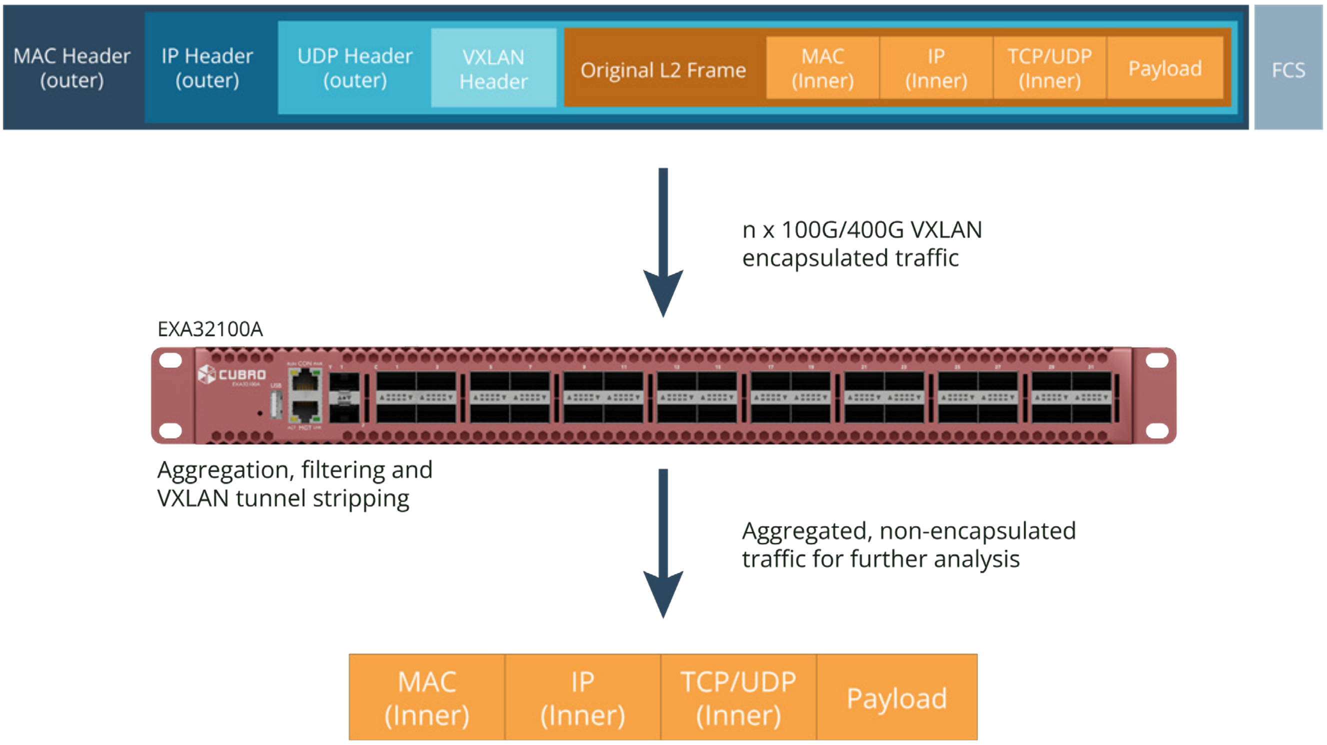
- VXLAN inner tunnel filtering (inner IP and/or inner TCP/UDP port number filtering)
- VXLAN outer tunnel filtering (VXLAN VNI tunnel identifier filtering)
- VXLAN tunnel stripping
- Simultaneous outer and inner VXLAN tunnel filtering, illustrated in the drawing below



These functionalities help monitoring systems by preventing them from being overloaded and ensure that existing monitoring infrastructure remains effective in VXLAN environments.

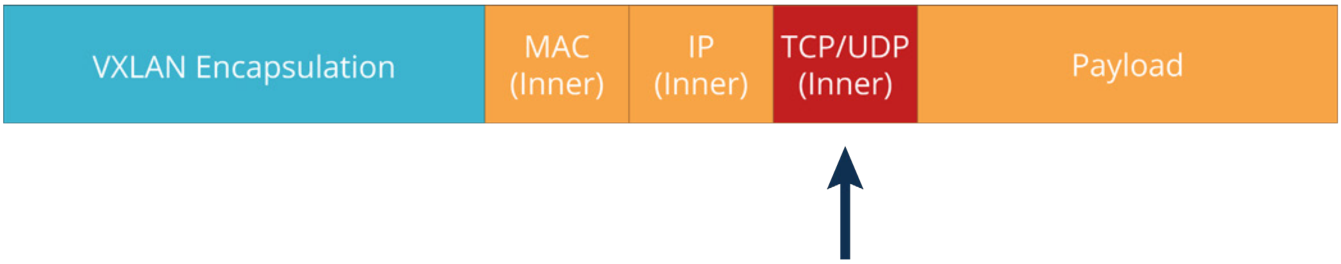
## VXLAN Tunnel Stripping

VXLAN encapsulation adds a 50-byte tunnel header to each packet, which increases packet size and can obscure original traffic details. Most monitoring systems require access to the original packets but are incapable of processing VXLAN tunnel headers. By enabling VXLAN stripping on Cubro's Advanced Packet Brokers, tunnel headers are automatically removed, allowing monitoring systems to receive original traffic without additional user intervention.



## Inner VXLAN Tunnel Filtering

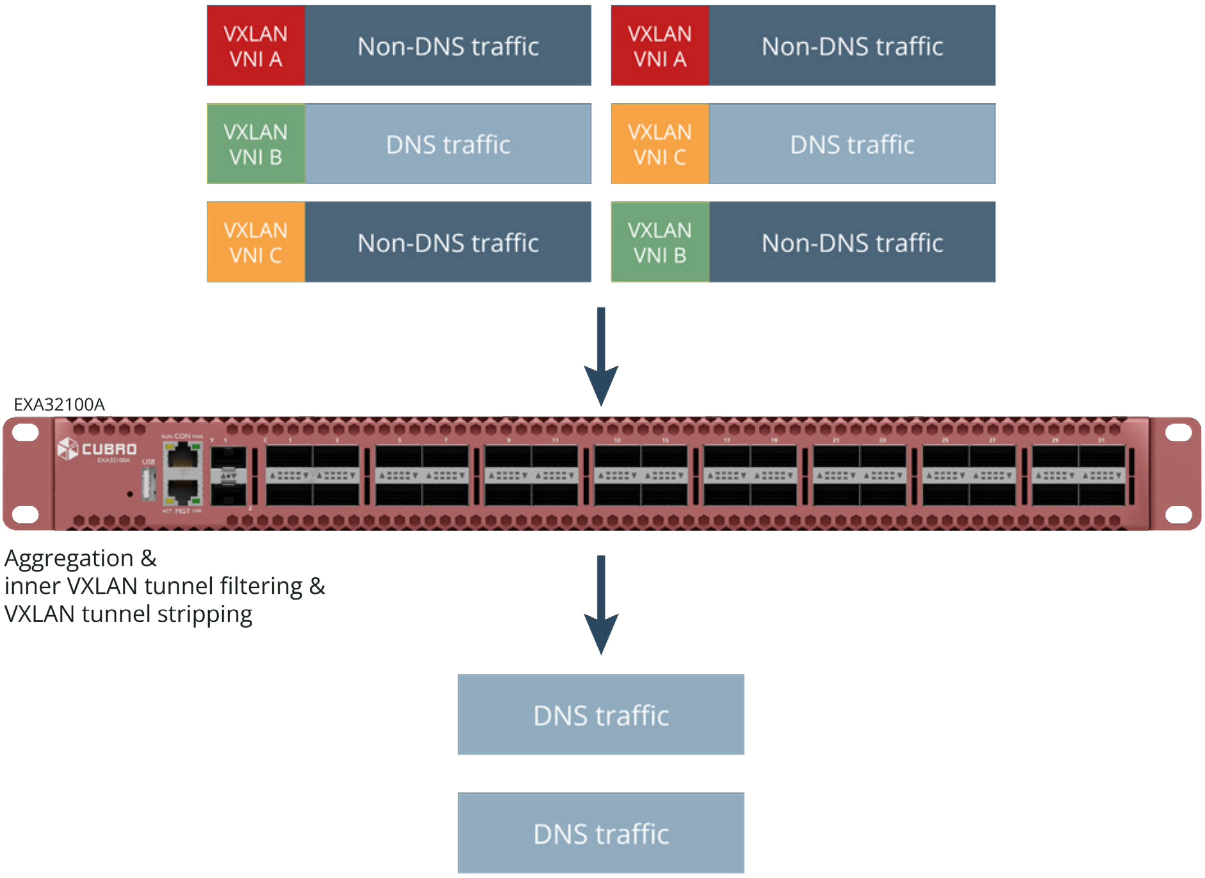
To prevent monitoring systems from becoming overwhelmed, only relevant traffic should be forwarded to them. Traditional Layer 2 to Layer 4 devices can only filter based on outer header information and cannot interpret VXLAN-encapsulated traffic. Advanced Packet Brokers from Cubro allow filtering within VXLAN tunnels to extract and forward only relevant traffic.



Extract relevant information
by filtering on TCP/UDP port number

### For example:

**DNS traffic** using **UDP Port 53** inside single or multiple VXLAN tunnels can be identified and filtered. This ensures that a DNS monitoring system processes only relevant DNS traffic instead of all network traffic, thereby optimizing resource utilization.



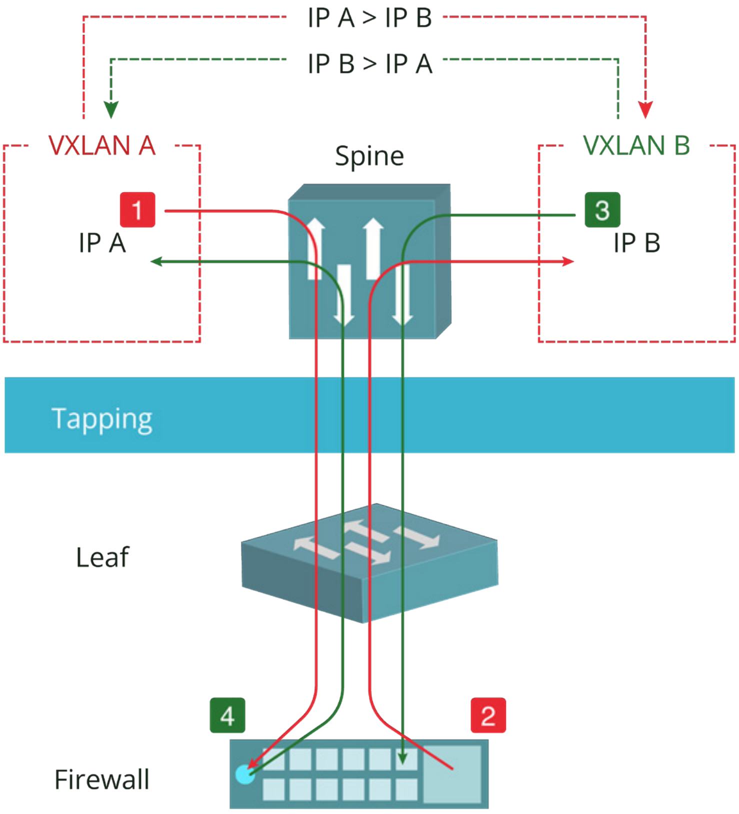
Aggregation &
inner VXLAN tunnel filtering &
VXLAN tunnel stripping

## Combining Outer and Inner VXLAN Tunnel Filtering

Advanced Packet Brokers from Cubro support simultaneous traffic filtering of the outer and inner VXLAN tunnel. In Leaf-Spine architectures, network traffic may become duplicated. When IP address A communicates with IP address B, the tapped traffic might be captured with two copies.

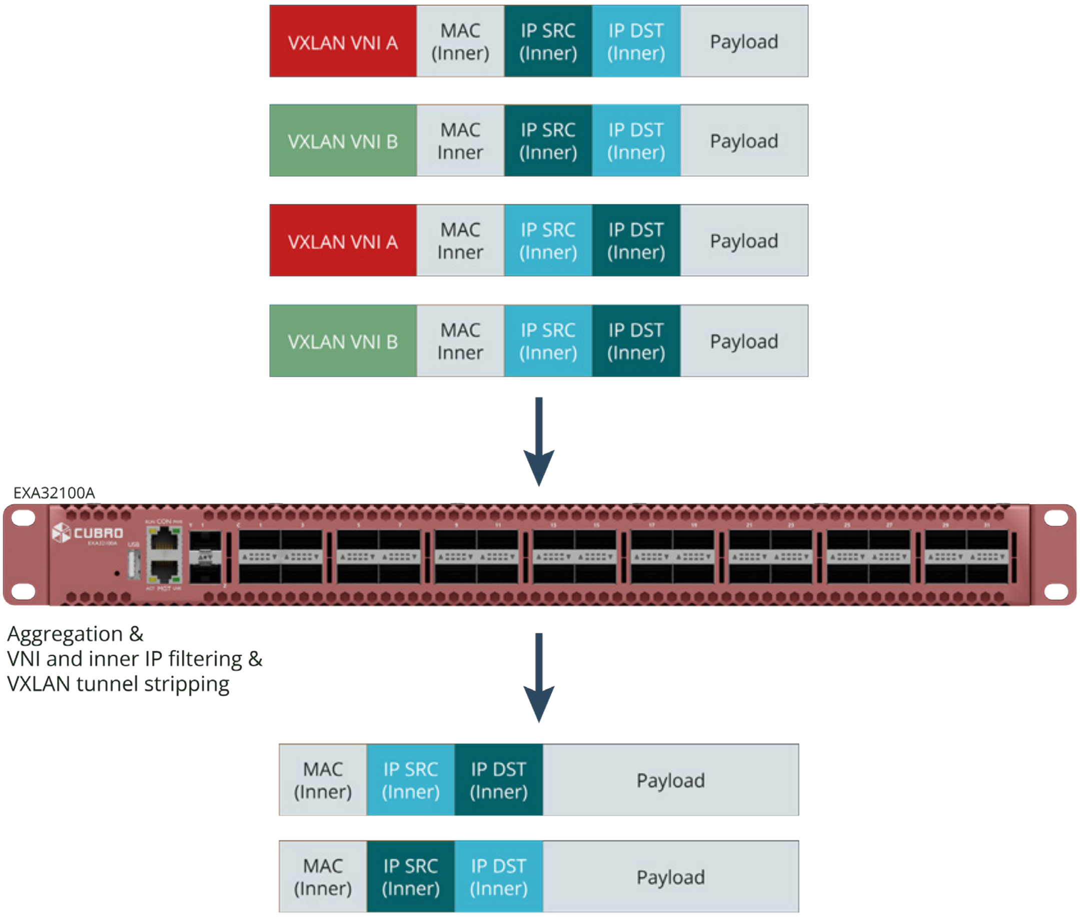
Logically IP address A communicates with IP address B, but physically packets go through spine, leaf and firewall and if firewall allows the packets to go to the destination they go again through leaf and spine before reaching the destination. The tapping point is typically between leaf and spine, thus a duplicate of the traffic is captured.

Cubro packet brokers filter based on VXLAN VNI and inner IP addresses, and therefore, duplicate packets can be eliminated before they reach monitoring systems. The deduplication is performed in the chipset and it operates at terabit-per-second (Tbit/s) speeds, ensuring high-performance network visibility without additional processing overhead.



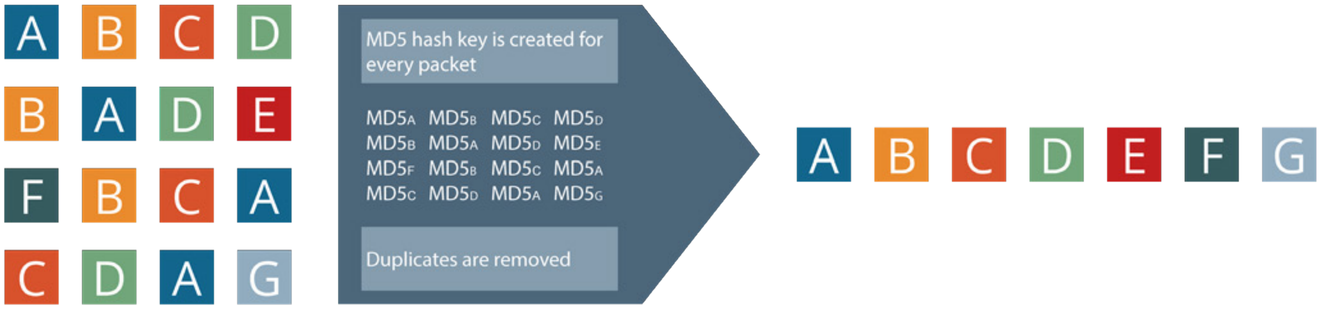
| Packet # | VXLAN | Source IP | DEST IP | Direction | Action |
|---|---|---|---|---|---|
| **1** | **A** | **A** | **B** | spine > leaf > firewall | drop |
| **2** | **B** | **A** | **B** | firewall > leaf > spine | forward |
| **3** | **B** | **B** | **A** | spine > leaf > firewall | forward |
| **4** | **A** | **B** | **A** | firewall > leaf > spine | drop |

The drawing below illustrates how the filtering is executed.



When the network has lots of different VXLAN VNIs, the inputs come from several subnets and from port spanning, it is often difficult to create a filtering rule that would remove duplicate packets. In those cases it may be necessary to use packet comparison based deduplication.

Comparing full packets against each other is not an efficient method since it would consume all available appliance memory very fast. Cubro implementation uses instead a MD5 checksum (hash key) based method for every packet. MD5 algorithm creates a 128-bit hash value that identifies the packet uniquely. MD5 hash keys are compared in the memory and if a matching hash key is found it will be discarded as a duplicate.



Packet comparison even with MD5 checksum cannot be executed on the chipset, it requires a dedicated CPU for processing. An optimized detection window is needed, a time window in which it is assumed that the network has provided packets from all of its domains. Therefore, the downside of packet comparison in addition to cost is increased latency.

## Conclusion

As VXLAN deployments continue to expand, ensuring visibility across overlay and underlay networks is critical. Traditional monitoring solutions struggle to process VXLAN-encapsulated traffic, leading to significant blind spots. Cubro's Advanced Network Packet Brokers provide best-in-class VXLAN visibility by offering tunnel stripping, inner and outer tunnel filtering, deduplication, and advanced flow correlation capabilities. These features empower network operators with the tools needed to maintain accurate visibility while ensuring optimal performance of their monitoring infrastructure.