Cubro & Endace

Enabling Total Visibility and Network History for SDN Data Centers

Cloud technologies, virtualization, multi-tenancy, greater bandwidth requirements, and the need for elevated security have driven a new approach to network and security management. Today, many public and private datacenters are moving to a Software Defined Network (SDN) strategy, where multiple traffic networks are independently “overlaid” based on a leaf-and-spine topology.

With SDN, traditional IP addressing can be configured independently, and applications can be moved from server to server as needs require. Additional application copies can be created when performance needs are high and then deleted when traffic subsides. Network packets now have multiple possible paths through the network to increase overall throughput. This new architecture, and the dynamic nature of the infrastructure, presents new challenges for the datacenter tools used for monitoring, security, and forensics.

Cubro is a leading vendor of network visibility solutions that include network TAPs, Advanced Network Packet Brokers, Bypass Switches and Network Probes, for service providers and private and public sector enterprises worldwide. Cubro has developed unique, industry leading solutions specifically designed to solve many of the new challenges that appear in these networks.

EndaceProbe™ Analytics Platforms capture, index and record network traffic with 100% accuracy while simultaneously providing hosting for a wide variety of network security and performance monitoring applications in Application Dock™, the EndaceProbe’s built-in hosting environment. Customers can extend their network and security monitoring capability by deploying instances of virtual applications anywhere they have EndaceProbes deployed. Customers can scale, expand, and adapt to diverse needs, environments, while comprehensively recording and monitoring everything happening on the network.

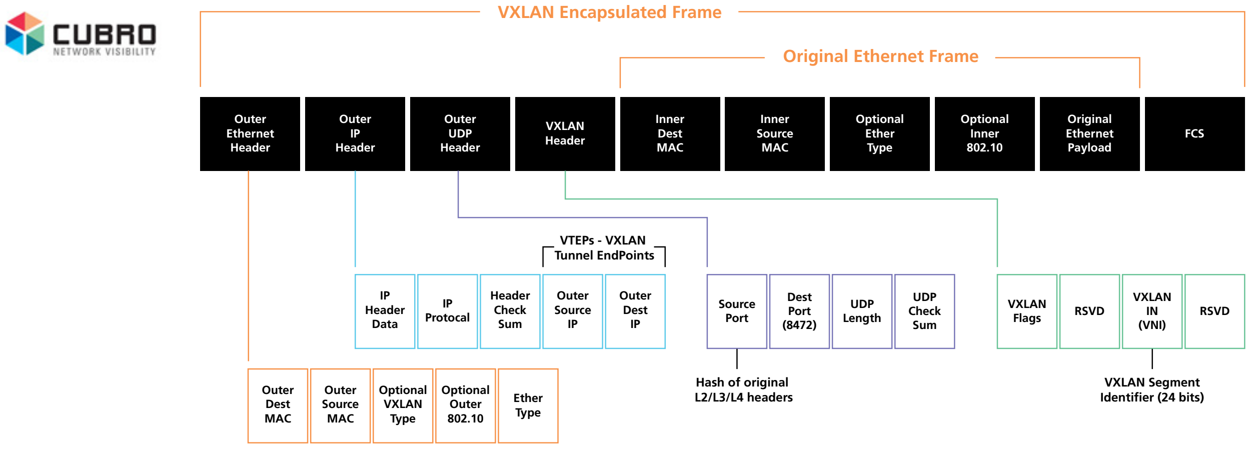
PRODUCTS

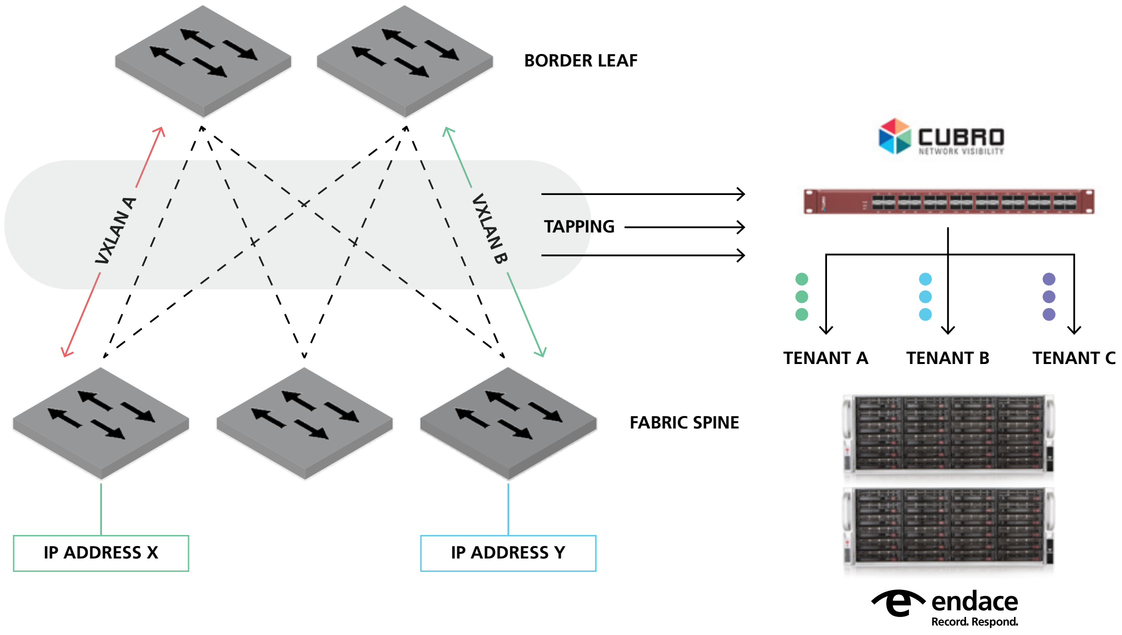
- Cubro TAPs
- Cubro Omnia Packet Brokers
- EndaceProbe Analytics Platforms with EndaceVision and InvestigationManager

BENEFITS

- Eliminate network blind spots with comprehensive visibility into all SDN traffic.
- Ensures security separation between network tenants.
- Brings the power of EndaceProbe platforms to SDNs and the latest cloud technologies:
  - VNI filtering identifies overlays independent of host IPs, which can dynamically change through migration and application scaling
  - Visibility into traffic from overlapping and duplicate IP or MAC address in different Virtual Network Instances.
  - Complete packet capture with Equal Cost Multipath Routing

Virtual Extensible LAN (VXLAN) handling on NP8 is most important on overlay networks





Confidently Accelerate Investigations in Software Defined Data Centers

The challenge of encapsulated traffic has changed significantly in modern data centers. Simple header stripping is ineffective for monitoring because encapsulation headers are critical to understanding the network. Overlay networks can easily share the same IP range: the underlay is transparent to the service running on top of it and because overlays are logically separated by their encapsulation headers there is no reason to ensure overlays are in separate IP ranges. Stripping away the encapsulation headers removes information pertaining to the underlay network and there is no longer a way to guarantee traffic belonged to a given overlay. This not only renders monitoring ineffective but also creates an incorrect view of the network.

Omnia Network Packet Brokers address these challenges of software-defined datacenter environments by filtering on the inner headers of encapsulated traffic, logically identifying and grouping overlays, and performing deduplication, decryption, and session-aware load-balancing for EndaceProbe deployments. Omnia provides full visibility into virtualized and overlay network traffic, giving EndaceProbes unrestricted access to all network traffic. When tapping a leaf and spine architecture, duplicate overlay traffic will inevitably be captured. Cubro can uniquely "deduplicate" overlay traffic by matching the VNI and inner IP source and destination to drop duplicate tunnels. This action is performed at line rate because the filtering is implemented in hardware.

Fast, Accurate Security Investigation and Threat Hunting

SecOps analysts can drill down from alarms or threat indicators in their security tools directly to related network packet data in EndaceVision™ or InvestigationManager™ using the EndaceProbe's powerful API integration. The API uses the IP address and time range of the trigger event to focus the analyst directly on relevant incident data. They can then quickly analyze, dissect, and extract the relevant traffic from amongst petabytes of Network History recorded on the network. Analysts can analyze traffic to microsecond level detail with views filtered by Application, IP, Protocol, Top Talkers, and many other parameters, providing rapid insights and enabling accurate conclusions. Being able to get directly to the related packets with a single click enables security analysts to quickly establish the root cause of issues as they are performing investigations or threat hunting in their environment. They can respond rapidly to security threats, dramatically reducing the time to resolve critical incidents and minimizing the risk of threats escalating to become more serious breaches.

Omnia and the EndaceProbe platform share the ability to host third-party and custom software solutions through Omnia's AppMaster and the EndaceProbe's Application Dock, offering unparalleled flexibility and integration in any environment. Together, Cubro's Omnia line of network packet brokers and EndaceProbe create a powerful solution addressing the monitoring and security challenges of modern data center environments.

Conclusion

Combining Cubro's expertise in overlay visibility with the EndaceProbe's 100% accurate Network History delivers network wide security analytics and always-on recording for definitive evidence that enables SecOps teams the time and forensic data for even the most complex investigations.

Integrating these technologies lets security teams respond to alerts faster and investigate threats with more confidence across both physical and cloud environments and eliminates blind spots created by encrypted traffic. Additionally, the ability to host virtualized tools on the EndaceProbe's Application Dock or Cubro's AppMaster, enables customers to extend their monitoring coverage without additional hardware deployments, leveraging existing hardware to extend traffic monitoring and analysis capability.