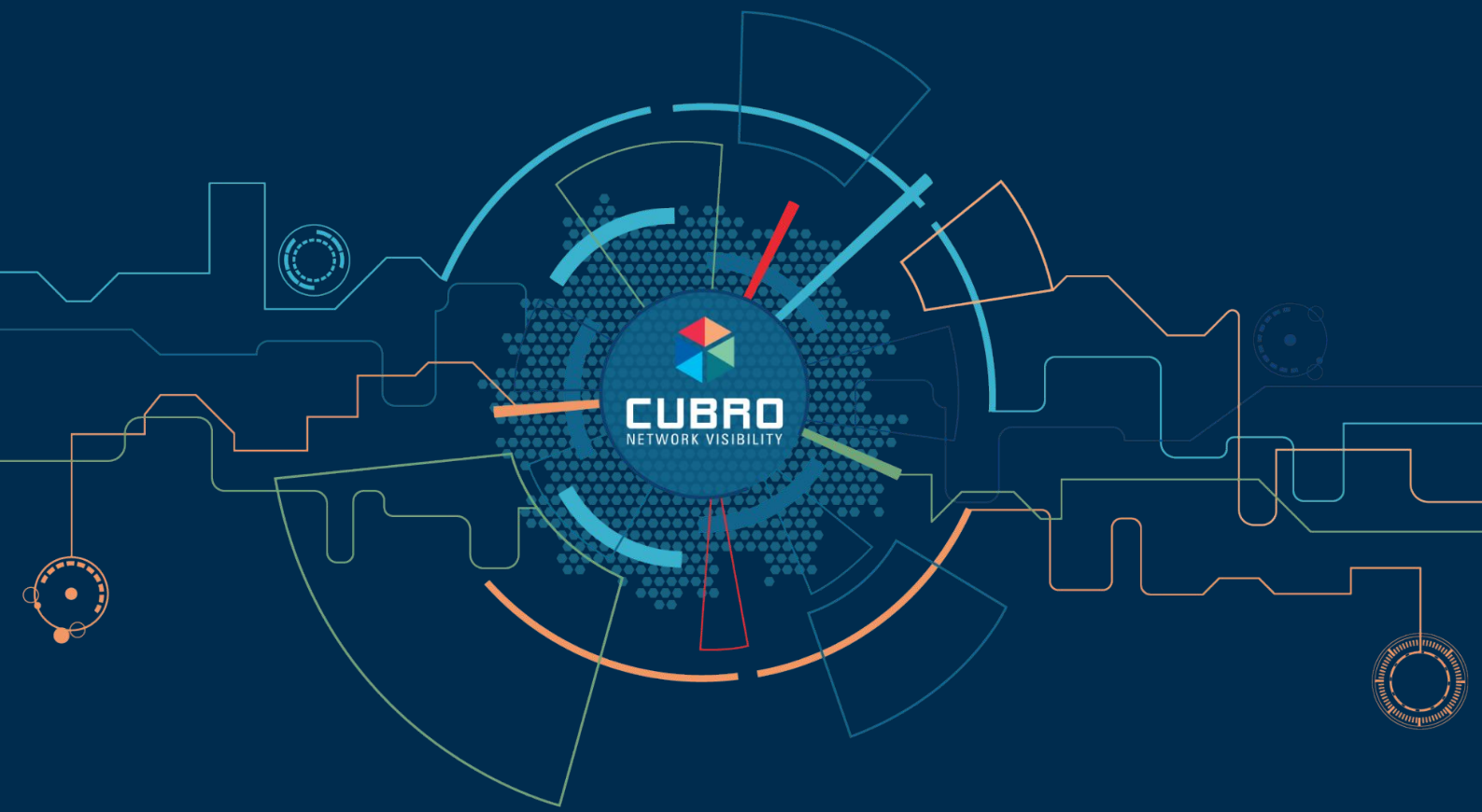


Virtual Tapping for Public and Private Cloud

Application Note

Classification Type: Public

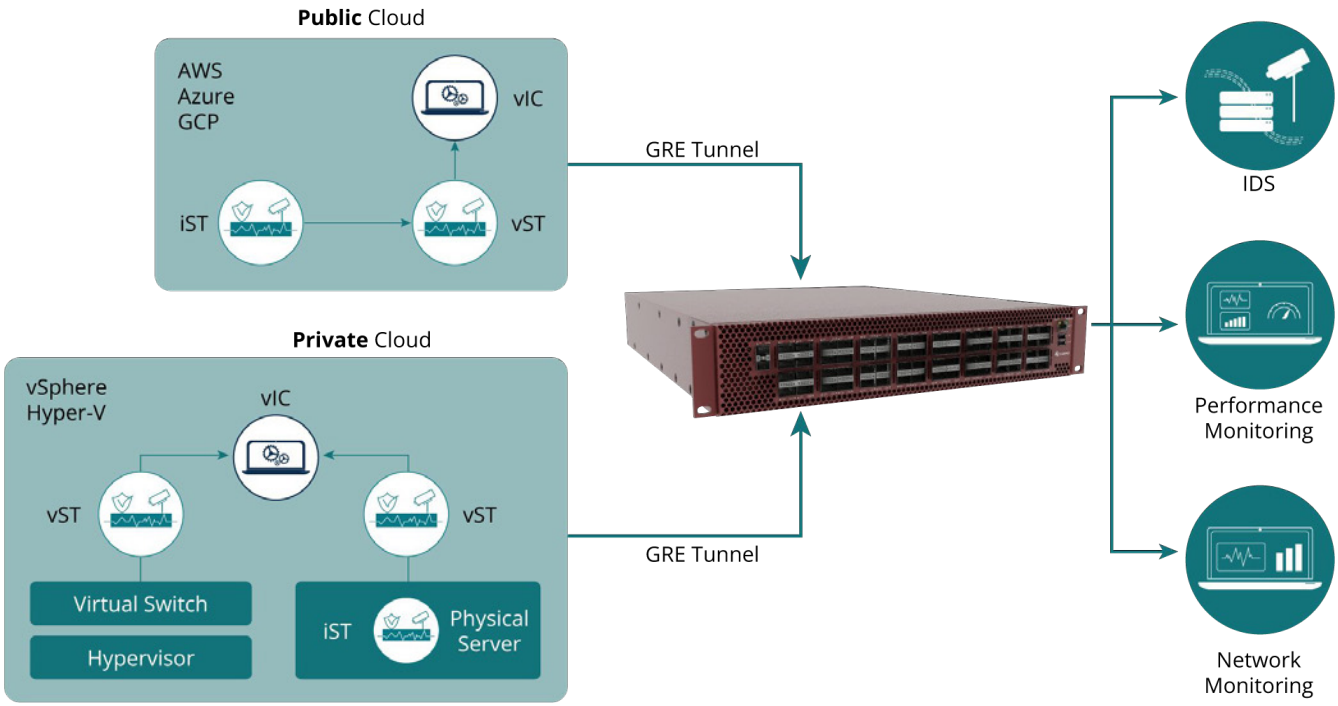
Please refer to the latest version of this document on our website to ensure you have the most up-to-date information.

1. Operational Overview & Industry Challenges

Modern company networks are spread across a mix of on-premises data centers and cloud platforms. To keep critical services running without interruption, systems need to easily move data and computing power wherever they are needed most.

- **Rapidly Growing Data:** Data center network activity is expanding by over 20% every year.
- **Shift to the Cloud:** Roughly 70% of business applications now run in public clouds, while 30% remain on private servers. Managing a mix of both has become the norm.
- **Internal Network Activity:** Over 80% of network traffic stays inside the data center - moving directly between servers or virtual machines rather than entering or leaving the perimeter. Because of this internal ("east-west") flow, monitoring tools must look inside the network, not just watch the front doors ("north-south" traffic).

To get useful insights about system performance without overspending, companies must track and make sense of this data as it moves across these different boundaries.



2. Core Components

1. Virtual Smart Tap (vST):

a. **Deployment:** Installs directly as a lightweight guest virtual machine inside private cloud hypervisors (e.g., VMware vSphere/ESXi, Microsoft Hyper-V) or public cloud compute instances (AWS, Azure, GCP).

b. **Functionality:** Promiscuously monitors all traffic across virtual switches and Docker bridges without forwarding to external hardware.

c. **Tunneling & Forwarding:** Transmits metadata to the controller while backhauling captured raw packet data over GRE tunnels directly to the **Network Packet Broker** where further processing like VXLAN decapsulation is handled.

2. Instance Smart Tap (iST):

d. **Deployment:** Installed as a distributed plug-in on target virtual machines or public cloud instances running application workloads. The iST is also suitable for containers/pods on a Kubernetes platform including Amazon EKS, Azure AKS, Red Hat OpenShift, and VMware Tanzu.

e. **Functionality:** Collects local instance-level compute metrics along with raw network traffic, forwarding these streams to the Virtual Smart Tap for deep inspection.

3. Virtual Information Controller (vIC):

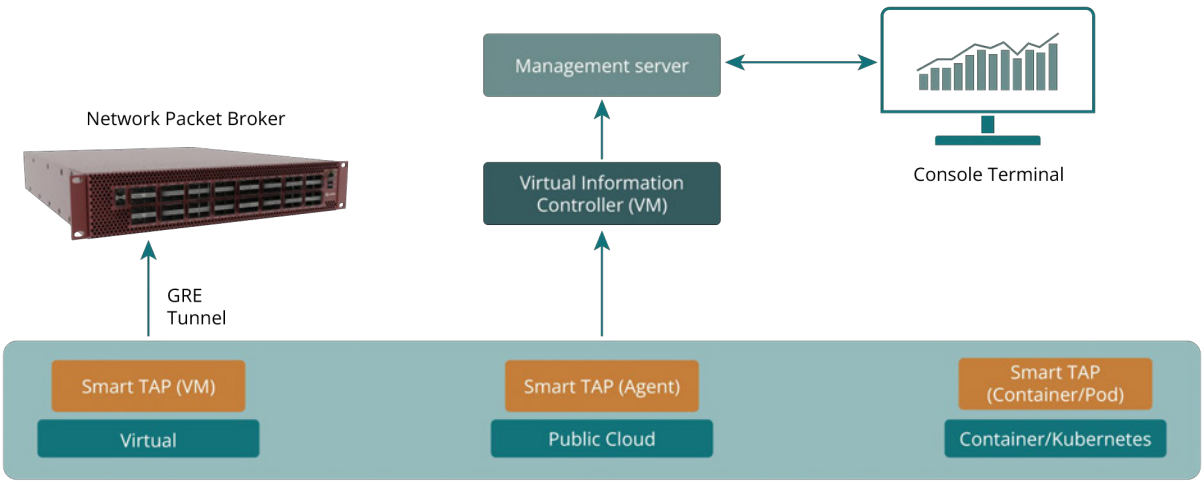
f. **Deployment:** Acts as the central management conduit, running on-premise or within cloud environments.

g. **Integration:** Connects directly with hypervisor management platforms (such as vCenter) to discover infrastructure configurations, retrieve storage and compute stats, and coordinate all deployed Virtual Smart Taps. Performs policy enforcement and provide visibility and management for deployed Virtual Smart Taps.

4. Network Packet Broker (NPB):

h. **Packet Processing:** Receives GRE-tunnelled raw packet streams from distributed virtual taps.

i. **Intelligent Routing:** Filters, aggregates, and directs selected packet streams to target security devices, performance management tools, and Intrusion Detection Systems (IDS).



3. Primary Benefits

- **Agentless Virtual Monitoring:** Collects traffic without requiring software agents on individual guest operating systems, eliminating application-owner approval cycles using native API on private and public cloud.
- **Minimal Resource Footprint:** Lightweight virtual taps consume minimal host computing power while delivering wide-scale coverage across internal networks.
- **Lateral Threat Detection:** Tracks horizontal "east-west" traffic movement to detect malicious behavior, backdoors, and unauthorized outbound connections.
- **Network Virtualization Insights:** Provides full visibility across overlay networks like VMware NSX to support micro-segmentation planning.
- **Rapid Onboarding:** Plug-and-play tap templates enable full operational deployment in less than one hour.
- **Application Dependencies Mapping:** Automated visualization of all virtual, physical and cloud assets and their interdependencies at the application level without any agents.
- **Visibility for workloads on Cloud:** Visibility for private and public cloud deployments regardless of deployment scenarios including containerized (including Kubernetes), VM and Bare-metal.
- **Assured privacy and data security:** The solution can filter and forward only necessary traffic over to the intended tool.
- **Full unmodified packets access:** Packets captured by the virtual tap will be forwarded to the packet broker without any modification ensuring full data fidelity.

Cubro Network Visibility
EMEA USA APAC
support@cubro.com
www.cubro.com