Tech Brief

cCloud™ Visibility Suite for Cloud Visibility and Observability

Full Visibility Stack - Network Packet Acquisition, Replication, Delivery, Capture-to-Storage, and Analytics

Technology Benefits

- **Agentless Cloud Visibility**

  Network-centric visibility and observability without the downsides of using agents

- **Streamed Network Packets**

  Acquire network packets from natively mirrored and custom strategic vantage points to provide real-time visibility to analytics and tools

- **Captured Network Packets**

  Provides stored network packet data enriched with metadata for forensics analysis that can be exported via API, Kafka, and PCAP files

- **Network-Centric Analytics**

  KPIs and other results accessible via API and visualized in customizable dashboards facilitate observability

Business Benefits

- **Strengthen Security Posture**

  Reliably provides network packets to any vendor's NDR, XDR, and MDR security analytics so SecOps and the SOC can detect and respond to security breaches before they become costly and chaotic events

- **Operational Efficiency**

  Pervasive visibility allows you to optimize infrastructure and workload performance, and effectively troubleshoot problems

- **Regulatory Compliance**

  Access data for regulatory record keeping and reporting

The Challenge

Application, workload, and data migration to public cloud infrastructure are common and accelerating. Observability from monitoring and visibility is necessary to know if everything is operating securely and as needed. One of the challenges of gaining observability and visibility into virtualized cloud infrastructure is sharing the infrastructure and responsibilities with the Cloud Service Provider (CSP).

Network-centric requires network instrumentation and telemetry data. Because public cloud infrastructure only exposes virtualized networks, the instrumentation combines native mirroring plus additional software. Monitoring agents are one option, but they are unattractive and generally avoided because they increase the attack surface, induce production resource contention and management burden.

cPacket Networks designed its cCloud Visibility Suite as virtualized visibility fabric appliances versus agents to avoid additional cyberattack surface area and the administrative burden of deploying and managing agents.

Network visibility in public cloud infrastructure varies by CSP from nothing to partial pre-defined and inflexible monitoring via native mirroring services, so instrumenting for monitoring and visibility is required. Doing so poses several challenges:

- Cyber Risk Resilience – often uses agents that require privileged access rights, increasing the attack-surface
- Performance Monitoring and Management – often use agents, virtualized probes, virtualized tapping, and container services that all run in the same namespace. All these production workloads increase contention for CPU, memory, and I/O (much of the I/O traffic is through the virtualized network)
- Manageability – Deploying and maintaining agents, especially at scale, increases patching, orchestration, and health monitoring overhead
- Capturing and storing network packet data – for use as forensic evidence by capturing and storing network packets from specific vantage points
- Analytics – that provide KPIs and actionable insights into the health of the network, Traffic, and utilization patterns and trends, throughput and protocol performance, network services performance

The Technology

Network packets are needed to fuel security solutions, AIOps, and critical IT operations to secure production applications and reduce resource contention in cloud environments that use shared virtualized infrastructure. Virtualized packet brokering with a Gateway Load Balancer (GWLB) and cloud-native packet/traffic mirroring means that network visibility has a lesser impact on VMs and the workloads they run. Cloud-native packet/traffic mirroring replicates network traffic flowing through specific vantage points and makes it available for forwarding to user-defined destinations. Replicated Traffic generated by each mirrored service instance counts against the overall instance bandwidth. Virtual networks also may intermittently stop mirroring packets when there is heavy network traffic, which is a key reason for extending the mirroring services.

Cloud-native monitoring and visibility services include the following (specific services available vary by CSP):

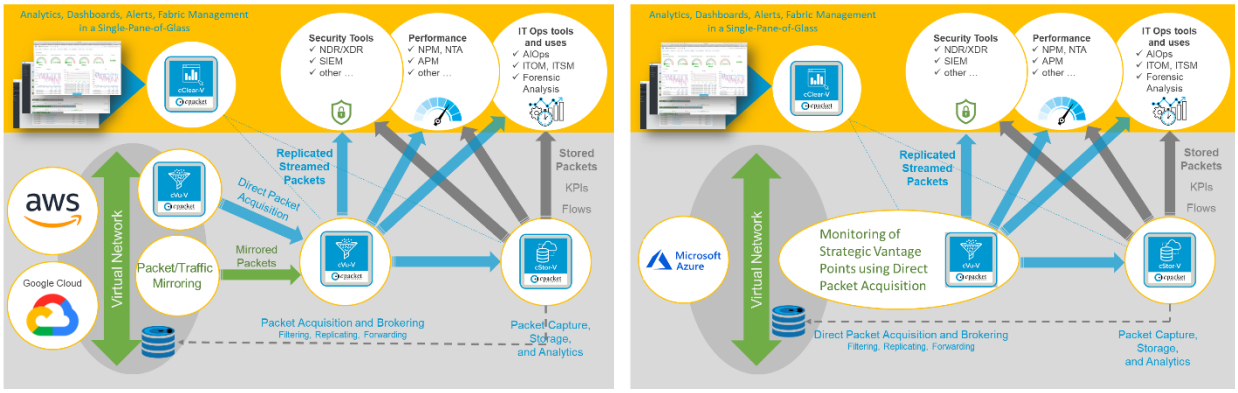
- **Virtual Packet Broker:** a purpose network vendor-designed appliance in the traffic flow provides a dedicated device to handle replication, filtering, and forwarding to network management and security tools. Its direct packet acquisition feature acquires network packets from custom vantage points, which is especially valuable for public cloud infrastructure that does not offer packet/traffic mirroring.
- **Cloud-Native Traffic Mirroring:** a network service provided by the CSP, including AWS VPC Traffic Mirroring and GCP Packet Mirroring. Replicates network traffic directly from the instance's virtual network interface or ENI (Elastic Network Interface). Virtual Machine or instance performance may be impaired due to resource contention of the replication service.
- **Gateway Load Balancing:** a network service provided by the CSP without interfering with application instances and production workloads, including AWS and Azure enabling you to deploy, scale, and manage your virtual appliances for traffic distribution and create redundant data paths to heighten the availability of critical services.
- **Cloud-Native Flow Logs and metrics**: a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data is collected outside of the path of your network traffic, and therefore does not affect network throughput or latency. VPC Flow Logs records a sample of network flows sent from and received by VM instances. These logs can be used for network monitoring, forensics, real-time security analysis, and expense optimization.

The Solution

The cPacket cCloud™ Visibility Suite provides IT teams and the tools they use with a visibility service chain that consists of agentless self-hosted appliances, including virtual packet brokering, packet capture, and network analytics. The cCloud Visibility Suite gives you essential network-centric visibility for cloud and virtualized environments without using agents. Validated images are available for Amazon Web Services (AWS), Google Cloud, and Microsoft Azure. The Visibility Suite includes several self-hosted virtual appliances that provide the benefits that provide streamed and stored network packets that give you high-fidelity visibility into your network's Traffic, behaviors, and performance and, more broadly, into your IT infrastructure apps, and other IT workloads and services. The virtual appliances interoperate with cPacket Networks' appliances for physical networks. The visibility includes either or both streamed and stored network packets that give you high-fidelity visibility into your network's Traffic, behaviors, and performance. It also enables broad observability into your IT infrastructure, applications, and other IT workloads and services.

The cPacket cCloud™ Visibility Suite provides IT teams and their tools with network packets. Using elastic agentless self-hosted virtualized appliances gives them visibility for packet brokering, flow generation, packet capture, and network analytics. The entire physical, virtual, or hybrid visibility fabric from cPacket is unified and managed using the same user interface and workflows using a physical or virtual instance of the cClear® Analytics Engine and Administration Console. The cPacket cCloud Visibility Suite consists of:

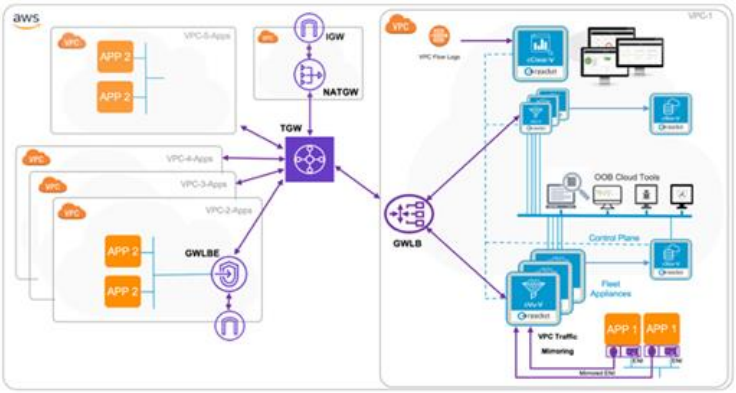
- cClear®-V – Analytics, data visualizations via customizable dashboards, and fabric management all from a single-pane-of-glass
- cStor®-V – Packet capture that provides forensic evidence that can be searched, retrieved, exported to PCAP files, and enables replaying Traffic linked to events up to 10Gbps for stateful and low-latency analysis
- cVu®-V – Virtualized Network Packet Broker (NPB) that performs replication, filtering, and forwarding functions



High-level architectures for cloud visibility for AWS and Google Cloud using mirroring and Direct Packet Acquisition (necessary for Azure)

Amazon Web Services Use Cases:

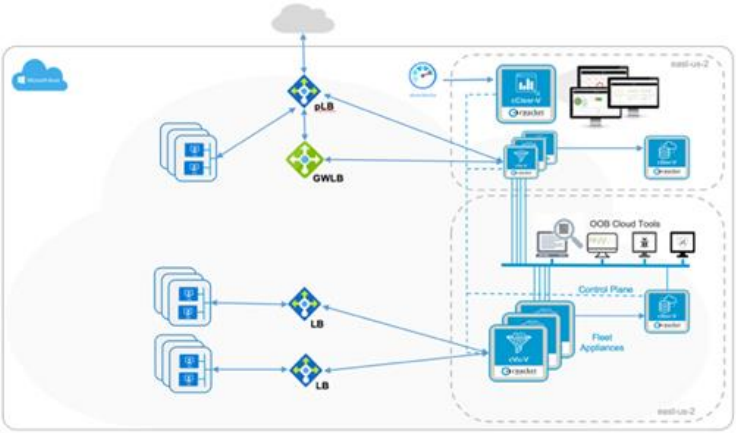
- Cloud Instance Elastic Network Interface ingress and egress mirrored Traffic
- Inter-VPC/Transit Gateway (TGW) flow traffic between Virtual Private Clouds
- North-South Internet Gateway (IGW) monitoring external internet traffic
- Ingest for partner device flows, meta-data, and analytics that are natively available in the cloud platform, including VPC Flow Logs



Cloud Observability for AWS and deployment Use Cases

Microsoft Azure Use Cases:

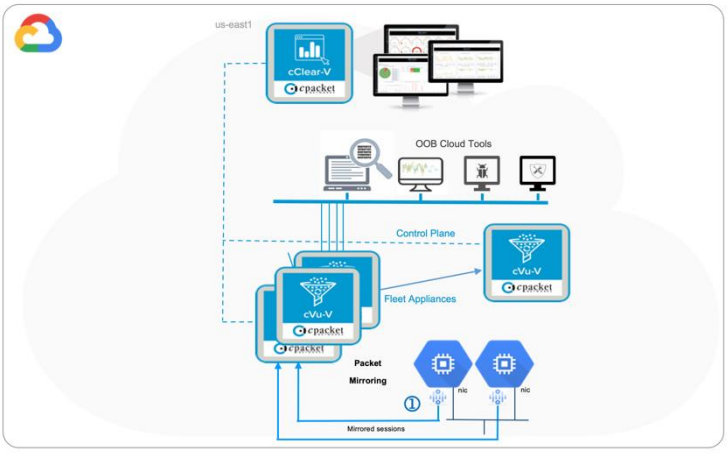
- Virtual Packet Broker with UDRs for Internet and Inter-VNet flow traffic
- North-South Internet Gateway (IGW) monitoring external internet traffic
- Ingest for partner device flows, meta-data, and analytics that are natively available in the cloud platform, including Azure Monitoring



Cloud Observability for Azure and deployment Use Cases

Google Cloud Use Cases:

- Cloud Instance Network Interface ingress and egress packet mirrored Traffic



Cloud Observability for GCP and deployment Use Cases

Summary

Gaining cloud visibility into single-cloud and multi-cloud environments is now possible using the cCloud Visibility Suite. When coupled with the physical appliances, visibility seamlessly extends to hybrid environments.

Key highlights are:

- **Cloud Visibility using Flexible and Multi-Function Network Packet Brokering:** The virtualized NPB provides multiple packet services, including direct acquisition, acquisition from cloud-native packet/traffic mirroring, replication, filtering, and forwarding
- **Network Packet Capture, Storage, and Analytics:** Virtualized network packet capture and analytics provide persistently stored and indexed network packets and network insights with Key Performance Indicators (KPIs) for forensic analysis, including point-in-time visualizations for fast troubleshooting, break-fix resolution, and reducing MTTR
- **Supports Cloud-Native Mirroring, Gateway Load Balancing, and Flow Log Services:** Visibility and observability extends across ingress, egress, and inter-VPC East-West traffic from multiple VPCs

About cPacket Networks

cPacket Networks enables IT through network-aware application performance and security assurance across the distributed hybrid environment. Our AIOps-ready single-pane-of-glass analytics provide the deep network visibility required for today's complex IT environments. With cPacket, you can efficiently manage, secure, and future-proof your network - enabling digital transformation. cPacket solutions are fully reliable, tightly integrated, and consistently simple. cPacket enables organizations around the world to keep their business running. Our cutting-edge technology enables network, application, and security teams to proactively identify issues before negatively impacting the business. The result: increased security, reduced complexity, and increased operational efficiency. Learn more at www.cpacket.com