Tech Brief

cCloud™ Visibility Suite Extends Cloud-Native Traffic Mirroring

Agentless Hybrid-Cloud Network Packet Replication, Forwarding, Capture-to-Storage, and Analytics

Technology Benefits

- **Cloud Traffic Replication and Forwarding to Tools**
  Network-centric visibility and observability without the downsides of using agents and vTAPs

- **Packet Storage for Forensic Analysis**
  Provides stored network packet data enriched with metadata that can be replayed, analyzed, and exported via API, Kafka, and PCAP files for forensic analysis

- **Network-Centric Analytics**
  KPIs and other results accessible via API and visualized in customizable dashboards for observability

Business Benefits

- **Strengthen Security**
  Reliably provides replication and forwarding to any vendor's NDR, XDR, and MDR security analytics. With added Packet Capture Storage responding to security breaches before they become costly and chaotic events

- **Reducing Service Outages**
  Packet capture, storage, and analytics allows you to optimize incident response and improved operation efficiency

- **Accelerating Incident Response**
  Know what's happening and what to do about problems using streamed and stored network packet data plus analytics

The Challenge

New capabilities are being introduced from the Cloud Service Providers (CSPs) to provide access to network packet data for monitoring network traffic to minimize IT security and operational risks. Several network packet acquisition capabilities are provided, including cloud-native mirroring, gateway load balancing, flow logs, and metrics. Each has pros and cons depending on your requirements, and the details vary per CSP, resulting in the need streamed and stored packets to enhance security and service observability tools.

With the shared responsibility for security and service availability in the cloud, access to network packets remains critical to compliance and operational efficiency. However, some architectural and design decisions need to be considered.

Some of these challenges include:

- Security – Cyber Risk Resilience often uses agents that require privileged access rights, increasing the attack-surface
- Incident Response – Capturing and storing network packet data for use as forensic evidence
- Manageability – Deploying and maintaining agents/vTAPs, especially at scale, increases patching, orchestration, and management overhead
- Network Analytics – providing Key Performance Indicators (KPIs) and actionable insights into the health of the network, traffic, utilization patterns and trends, throughput, protocol performance, and network services performance

As more network data from the platform becomes increasingly available, the focus and challenge turn to volume, quality of data, insights, context, reduced time for root cause analysis, and restoring services to an operational state.

The Technology

Cloud-Native Traffic Mirroring is a network observability service currently provided by some CSPs, including AWS VPC Traffic Mirroring and Google Cloud Packet Mirroring. The service replicates network traffic directly from the instance's virtual network interface or ENI (Elastic Network Interface). The mirroring happens on the virtual machine (VM) instance, with production traffic having a higher priority than mirrored traffic when there is traffic congestion. As a result, mirrored traffic is dropped when there is congestion. The production instance performance can be impacted due to resource contention from the replication service, and mirrored traffic consumes bandwidth. For example, if you mirror a network interface with 1 Gbps of inbound traffic and 1 Gbps of outbound traffic, the instance must handle 4 Gbps of traffic (1 Gbps inbound, 1 Gbps mirrored inbound, 1 Gbps outbound, and 1 Gbps mirrored outbound). To limit what traffic is mirrored, you can use filters for ingress vs. egress monitoring. Other considerations include mirroring limitations, service maximums, and some traffic types that are not supported. It's recommended to review the CSP's latest documentation and limits.

Further CSP specific details can be found via the following links:

https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-considerations.html

Google Cloud Packet Mirroring

https://cloud.google.com/vpc/docs/packet-mirroring

The Solution

The cPacket cCloud Visibility Suite provides operational teams with streamed and stored network packets and analytics necessary for network performance management tools, security tools, and to initiate rapid incident response. Extending Cloud-Native Mirroring Services gives you visibility into cyberthreats, traffic, behaviors, and service availability problems. The suite supports cloud-native mirroring by proving a target virtualized Network Packet Broker (NPB) and/or collector appliance, adding packet storage and detailed TCP analytics. The virtualized NPB provides packet acquisition, replication, filtering, and forwarding from the mirroring service. Interface mirroring services use production host resources, so it's recommended to offload replication and distribution to virtual NPB appliances fleet to minimize the impact on your production application. The replication requirements will be determined by the number of security and monitoring tools plus the number of forwarding flows.

The cPacket cCloud^{TM} Visibility Suite consists of:

- cClear$^{®}$-V – Analytics, data visualizations via customizable dashboards, and fabric management all from a single-pane-of-glass
- cStor$^{®}$-V – Virtualized Packet Capture that provides forensic evidence that can be searched, retrieved, exported to PCAP files, and enables forensic analysis and replaying traffic linked to events
- cVu$^{®}$-V – Virtualized Network Packet Broker (NPB) that performs packet acquisition, replication, filtering, and forwarding

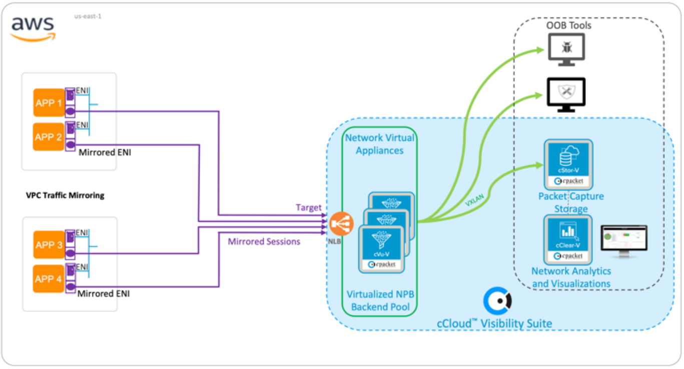

Figure 1: Cloud Observability for AWS VPC Traffic Mirroring

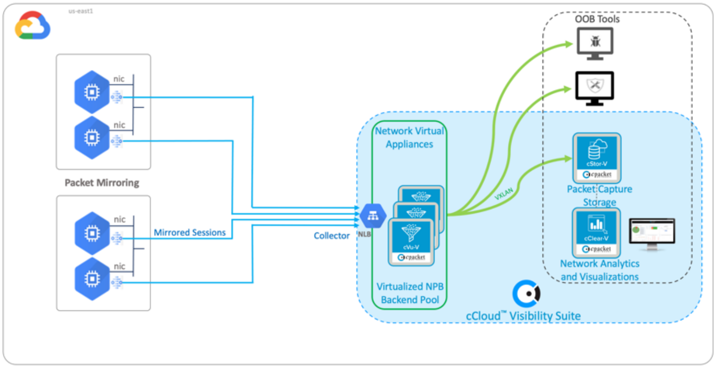

Figure 2: Cloud Observability for GCP Packet Mirroring

The performance of the Cloud-Native Mirroring service depends on the instance size and the supported throughput of the network interface; its throughput will depend on the size of the instance or virtual machine. The Virtualized NPB appliance requires the accelerated interface enabled. The minimum recommended instance to host a cVu$^{®}$-V virtual appliance is 4 vCPUs, 16GB memory, and supports up to 10Gbps. The Virtualized NPB appliance fleet is a set of cVu$^{®}$-V virtual machines behind a Load Balancer that can be scaled up as required. The traffic is distributed to the tools, packet capture appliance(s), and the cClear Analytic Engine that provides the KPIs' visualization, including health, errors, latency, open sessions, round trip time, and retransmissions.

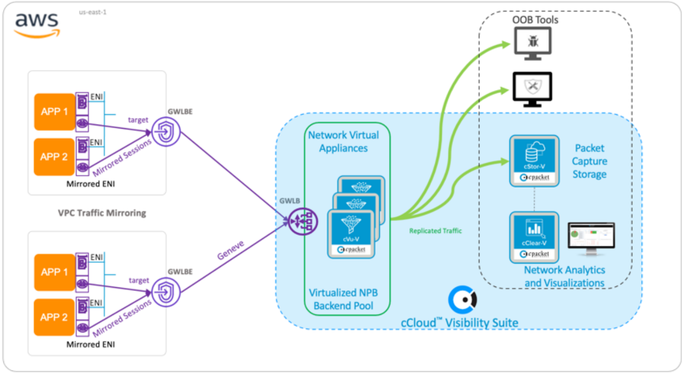

Figure 3: Cloud Observability for AWS VPC Mirroring and GWLBE

The cPacket cCloud Visibility Suite provides streamed and stored network packet data that is easily accessible by the cClear-V Analytics Engine, Wireshark, and other third-party analytics and tools, including direct role-based access and Open API remote querying and streaming to your choice of targets, including Kafka.

Figure 3 shows mirrored traffic from EC2 instances using VPC Traffic Mirroring forwarded to appliances deployed behind an AWS Gateway Load Balancer (GWLB) for traffic monitoring and analysis. Traffic is replicated and forwarded via the mirrored sessions to each GWLB Endpoint (GWLBE) deployed in production subnets containing their workloads.

Summary

Using the cCloud™ Visibility Suite to extend Cloud-Native Mirroring services enhances security, network monitoring, and IT operational effectiveness, reducing production service outages, costs, and MTTR. Agentless acquisition of the desired traffic minimizes impact to the production service and enables offloading the distribution service to a dedicated virtualized NPB appliance fleet strengthening security and accelerating incident response.

Key highlights are:

- Agentless Real-Time Cloud Packet Replication and Forwarding to tools: the Virtualized NPB provides multiple packet services, including acquisition from Cloud-Native Mirroring, replication, filtering, and forwarding to tools enhancing security and forensic analysis
- Network Packet Storage for Forensic Analysis: packet capture provides persistently stored and indexed network packets for forensic analysis
- Network Analytics with Insights with Key Performance Indicators (KPIs): give you insightful real-time and historical views for fast troubleshooting and problem resolution that reduces MTTR

Details about the cClear®-V, cStor®-V, and cVu®-V virtualized appliances are in the respective data sheets that can be viewed using the following links:

https://www.cpacket.com/resources/cclear-datasheet/

https://www.cpacket.com/resources/cstorv/

https://www.cpacket.com/resources/cvu-v-series-datasheet/

About cPacket Networks

cPacket powers hybrid-cloud observability through its Intelligent Observability Platform. It reduces service outages through network-centric application analysis, strengthens cyber security through high-resolution network data for threat detection, and accelerates incident response through network forensic analysis. The result is increased service agility, experience assurance, and transactional velocity for the business. Find out more at www.cpacket.com.