Application Note

cPacket Networks cCloud™ Suite Maximizes Cloud Packet Acquisition

Agentless Hybrid-Cloud Packet Replication to Multiple Tools & Unparalleled Network Observability

www.cpacket.com

Highlights

- Learn about the key limitations of utilizing native Cloud Service Provider mirroring
- Learn how cVu-V can overcome native mirroring limitations while maximizing packet replication
- Learn about the different cCloud deployment options across the various Cloud Service Providers

Native CSP Mirroring Capabilities & Limitations

CSPs (cloud service providers) in recent years have introduced native traffic mirroring capabilities, enabling network traffic from a VM network interface to be replicated and forwarded to a destination endpoint where traffic can be monitored and analyzed. AWS, Azure and Google Cloud all have varying levels of support for traffic mirroring, with Azure Virtual Network Tap, AWS Traffic Mirroring, and Google Cloud Packet Mirroring respectively. While native CSP traffic mirroring solutions are convenient, they are limited in a few key areas:

- Most CSPs lack support for replicating packets from a single interface to multiple out of band tools. While technically supported by AWS, significant caveats exist such as the fact that you're still limited to a single copy of a unique packet and distributing different packets to alternate destinations requires the use of complicated filters and configuration. In addition, the VM source instance will take a significant network performance hit with mirroring enabled and a consumer would be charged per packet stream, or per tool. This leads to an expensive traffic mirroring footprint which underperforms and becomes difficult to scale.

- Current CSP traffic mirroring solutions have documented that mirrored traffic can be dropped during periods of network congestion. Traffic mirroring is a best effort service. Because mirroring consumes bandwidth on the source instance, traffic congestion causes production traffic to take priority over mirrored traffic during such periods. This leads to gaps in visibility and blind spots – for your security tools! Enabling mirroring also doubles the network bandwidth utilization of the VM source instance, potentially degrading performance and limiting instance headroom.

- Scaling to enable mirroring in large enterprise cloud environment with tens to hundreds of mirrored VM workloads across regions and virtual networks becomes challenging, expensive,

and difficult to maintain. Additionally, CSPs native mirroring services each have their own throughput performance and reliability limitations which create additional headaches and decrease network capacity headroom for large cloud deployments.

Maximize Performance and Flexibility with cCloud

cPacket addresses these CSP native mirroring shortcomings with an agentless solution capable of overcoming these limitations while enabling more flexible deployment options in your cloud infrastructure. cVu-V virtual packet broker is capable of being deployed inline, directly in the data path, for packet replication to out of band tools. Alternatively, in scenarios where CSP traffic mirroring is preferred, cVu-V can be utilized in a traffic mirroring target mode, where traffic mirror sessions can forward packets to cVu-V instances behind a load balancer. In either scenario, cVu-V maximizes packet delivery and enhances the overall reliability of packet replication use cases.

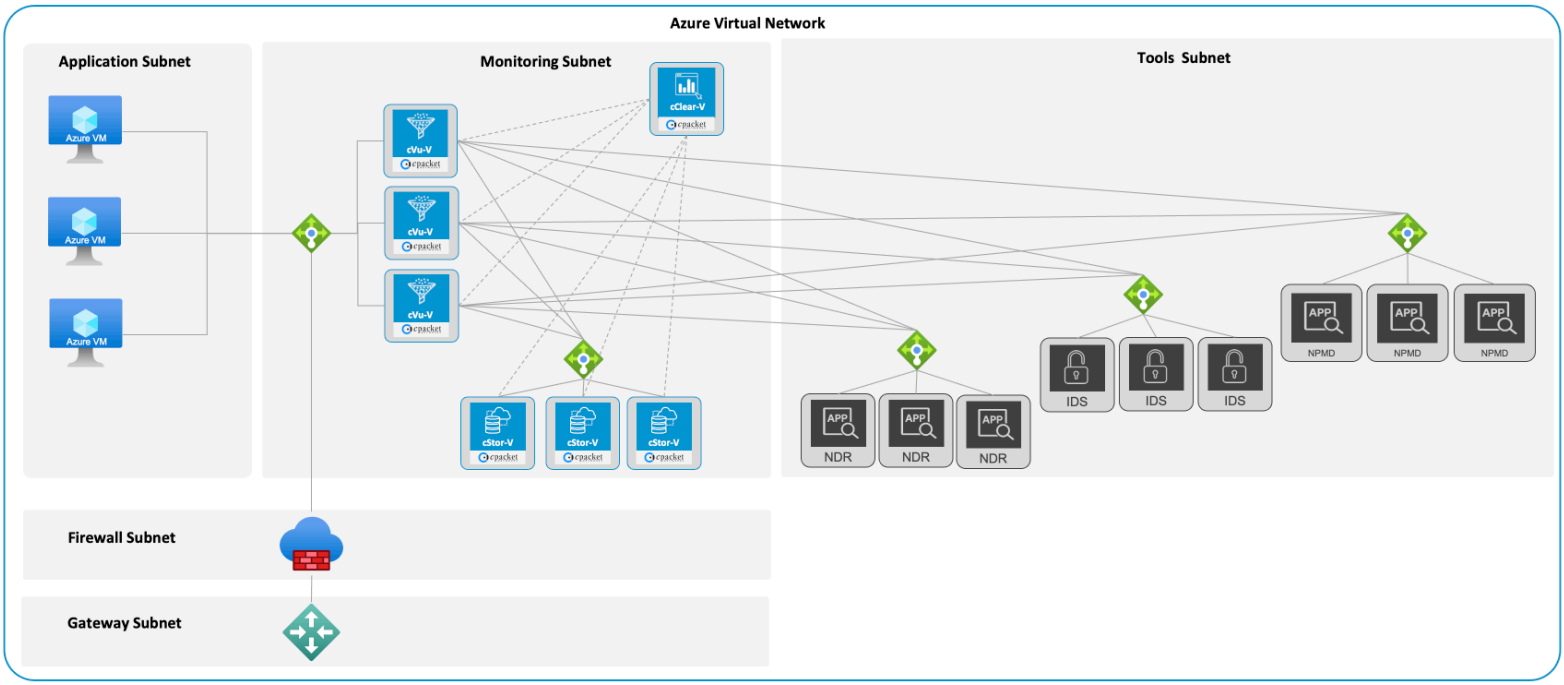
Deploying cVu-V Inline in the Data Path

Deploying cVu-V inline is ideal for security-focused deployments where minimizing packet loss is crucial. Since this scenario deploys cVu-V nodes directly in the data path - achieved via routing changes - it avoids the limitations of native CSP traffic mirroring such as dropping packets during times of congestion and enables the ability to replicate the same packets to more than one security tool or destination, encapsulated in VXLAN.

While the specifics around how we support inline routing and the accompanying tools varies by CSP, the basics of the cCloud deployment remain the same. A load balancer sits in front of a group of cVu-V instances – typically 3 for high availability – and distributes traffic across cVu-V targets. Traffic is diverted via routing changes from the original destination to cVu-V instances for packet replication to toolsets, where traffic is then routed back to the original destination via predefined routes.

Like most inline appliances, this deployment introduces minimal latency - characterized in microseconds - and includes a load balancer with health check capabilities capable of remedying common failures. As an example, in the case of a single unhealthy cVu-V instance, the load balancer will detect such conditions and reroute traffic to available healthy instances. An example Azure VNet deployment is featured below, where cVu-V instances are replicating packets to cStor-V packet

capture and 3 security and performance monitoring toolsets.

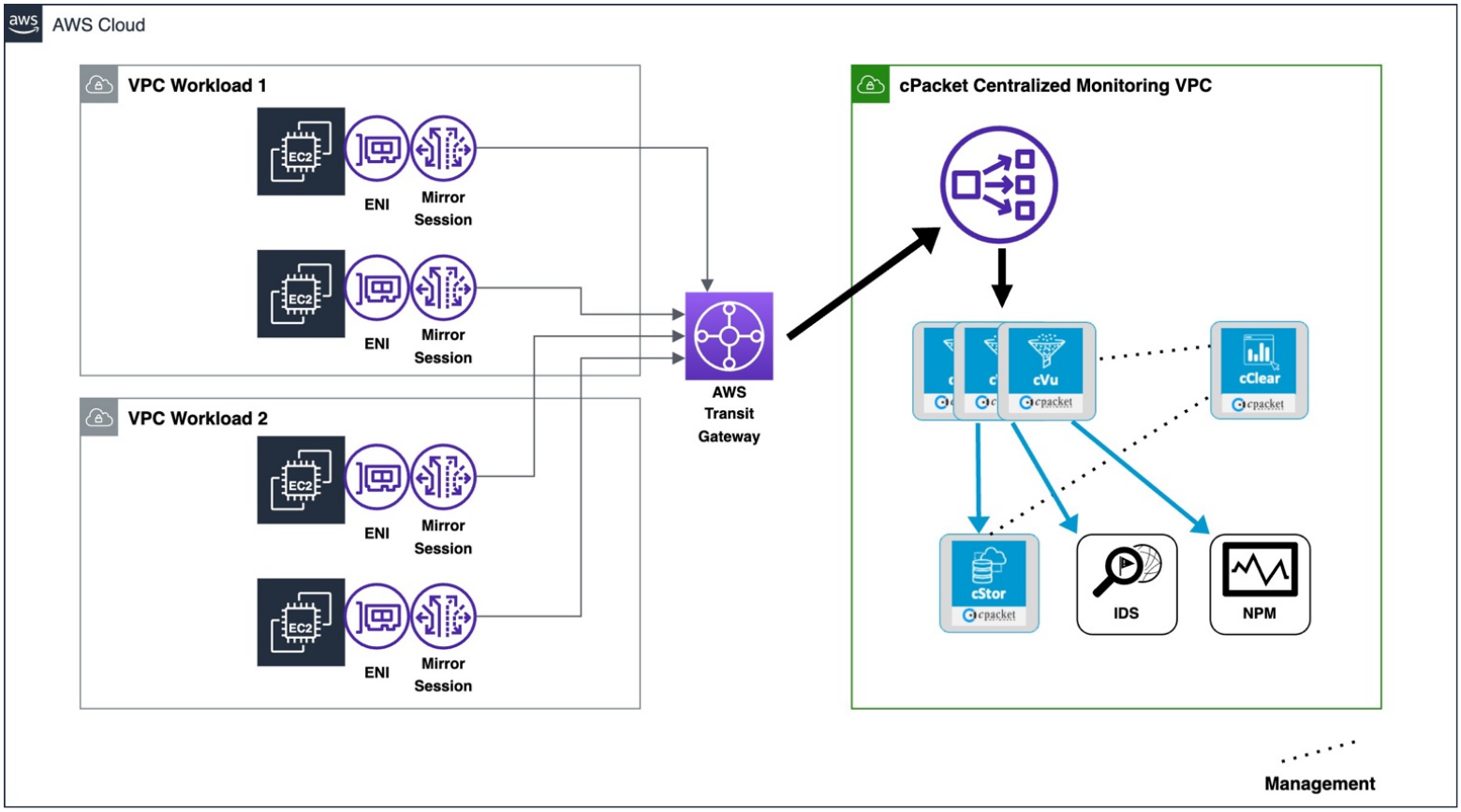


Deploying cVu-V as a Traffic Mirroring Target

In scenarios where native CSP traffic mirroring is preferred or already being utilized, cVu-V can be used as the traffic mirror target or destination for multiple traffic mirror sessions. This can help to centralize your point of packet acquisition, simplifying management of mirror sessions and downstream tool delivery. Traffic mirror sessions can be static or established on-demand for dynamic workloads.

cCloud deployments supporting traffic mirroring are deployed with the same basic principles: a load balancer sits in front of a group of cVu-V instances and distributes traffic across cVu-V targets. However, instead of routing changes to accomplish packet acquisition like in the inline scenario, traffic mirror sessions initiated from a source instance point to the load balancer in front of cVu-V nodes, where traffic is distributed in a high availability fashion.

Deploying cVu-V as a traffic mirroring target centralizes your hub for acquiring packets from one-to-many traffic mirroring sessions, reducing complexity and minimizing points of failure in a cloud environment. It can be used in conjunction with available CSP native mirroring capabilities allowing you to easily replicate to many security and performance monitoring toolsets which require packet-level granularity. An example AWS Traffic Mirroring session is featured below, where 2 external VPCs are mirroring traffic to a centralized monitoring VPC, where traffic is distributed to a combination of cPacket and security/NPM tools.



cCloud Advanced Platform Differentiators

The cCloud suite of products brings so much more than just reliable packet delivery. Continuous packet captures enabled by the cStor-V cloud packet capture node enable extended retention of packet data for security and compliance-focused environments. On-demand packet captures enhance forensic investigation capabilities and incident response. Single pane of glass management using cClear-V gives you management and visibility into your cCloud nodes and offers powerful analytics capabilities, including the most accurate network traffic KPIs, advanced visualizations and reports, unified PCAP retrieval and more.

Lastly, the benefits of an agentless architecture remains a key differentiator for cCloud when evaluating cPacket against the competition. Managing agents becomes a nightmare for large environments, where agents can be deployed in the thousands and require extensive operational investment. Avoid adding another overlay component to your cloud environment and maximize the performance of your cloud workloads by deploying without the use of agents.

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

Please contact cPacket today to get more information. We look forward to hearing from you.