Data Sheet

cPacket cVu®-V Virtualized Network Packet Broker

Network Packet Acquisition, Filtering, Replication, and Delivery for Observability

The cVu-V Virtualized NPB enables you to:

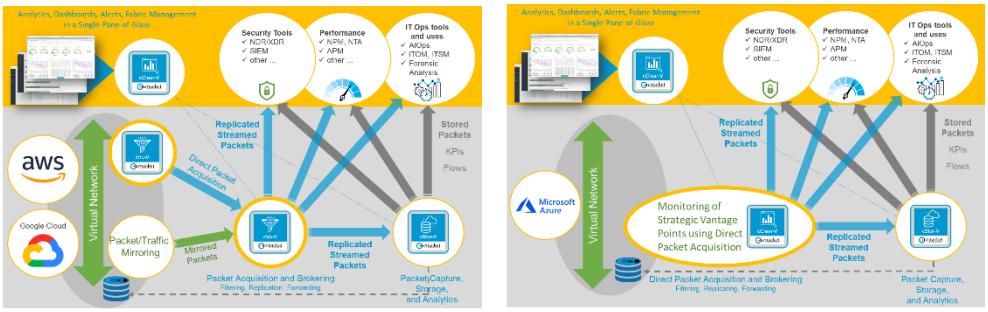
- Strengthen your security posture by delivering network packets to (XDR/NDR) detection and response, SIEM, and other security tools
- Leverage packet data and KPI metrics to efficiently troubleshoot problems, plan capacity, know the health of your network, and understand traffic
- Acquire packets/traffic from custom strategic vantage points in VPC subnets to supplement packets from native mirroring services to maximize visibility and observability
- Contain mirroring costs using packet replication to deliver packets from the same source to multiple targets
- Increase availability of services and workloads by bridging to load balancing services
- Scale to support temporary (elastic) and permanent growth
- Uniformly manage packet brokering nodes across any distributed, single-cloud, multi-cloud, or hybrid network
- Simplify the delivery of network packets to all cPacket Intelligent Observability Platform components, and third-party analytics and IT tools throughout any environment
- Quickly get started leveraging stored network packet data by deploying self-hosted executable images with installation scripts in Amazon Web Services (AWS), Google Cloud, and Microsoft Azure[1]

cVu-V Virtualized Network Packet Broker (NPB)

Streamed and stored network packets are vital for maximizing your network's security posture and observability, IT infrastructure, and application workloads. Streamed network packets also help troubleshoot and isolate network problems and capacity shortcomings and monitor performance vis-a-vis service level agreements. This agentless self-hosted component of the cCloud™ Visibility Suite is the foundation of virtualized Visibility Fabric. It facilitates the availability of network packet data, traffic analytics, and KPI metrics to IT personnel, other cPacket physical and virtualized appliances, and third-party analytics and tools. It delivers filtered and replicated streamed packets to multiple targets from one source. When chained to one or more cStor®-V Virtualized Packet Capture appliances, it facilitates the availability of enriched and indexed stored packets for additional forensic analysis and evidence. It is ready to deploy, use, and scale with[1]:

- Public Cloud Infrastructure: AWS, Azure, Google Cloud
- Hypervisors: VMware ESXi, Microsoft Hyper-V, KVM, Cisco NFVIS

Streamed and stored network packets are essential for Extended/Network Detection and Response (XDR/NDR) security solutions and Network Performance Monitoring.



high-level diagrams of typical deployments in a Public Cloud; direct packet acquisition (necessary when using Azure) streams network packets to one or more target destinations

The cVu-V Virtualized Network Packet Broker (NPB) performs the following functions:

- Unified and centrally managed network packet acquisition from any combination of:
  - Packet/traffic mirroring services
  - VXLAN and other overlay tunnels
  - Custom strategic subnet vantage points in virtual subnets to augment mirrored packets or simulate mirroring where mirroring is unavailable
- Filtering that can tailor and reduce packet stream volume to specific targets
- Replicate and deliver the same packet streams to multiple targets
- Forwarding packet streams to multiple targets simultaneously
- Interoperability with ingress routing and load balancing services

[1] go to www.cpacket.com for the current list of readily supported and validated environments

Key Benefits

Streamed network packets provide visibility, observability, and real-time data to security and performance analytics, other IT Operations tools, and dashboards to:

- Strengthen the security posture using XDR/NDR, SIEM, and other security analytics and solutions
- Assure optimal network performance using actionable insights into patterns, trends, and problems
- Collaboratively isolate and troubleshoot IT problems with the IT team to minimize MTTR, frustration, and stress
- Gain continuous visibility and observability of network health and status using traffic analysis and other analytics
- Contain the cost and reduce the effort of getting packets from the same source to multiple targets at scale
- Implement high-availability service chains using the NPB as a bridge between load balancing and IT services
- Interoperability with third-party security and performance management solutions that require network packets
- Elastically and persistently scale across physical, single-cloud, multi-cloud, and hybrid networks.

IT operations personnel, especially NetOps, AppOps, CloudOps, SRE, and SecOps (security analysts, forensic analysts, red team, blue team, third-party vulnerability, and penetration testers, and the analytics and tools they use) benefit from the rich insights derived from inspecting and analyzing streamed and stored network packets (storing packets requires using the cStor®-V Virtualized Packet Capture Appliance). The packets and insights facilitate detecting cyberthreats and active attacks, validating health, profiling performance, and identifying anomalies and other problems. You can use the cClear® or cClear®-V Analytics Engine, Wireshark, and other third-party applications to visualize packets, traffic, KPI metrics, and insights.

Holistic Visibility into Hybrid, Single-Cloud, Multi-Cloud, and Physical Networks and IT Infrastructure

The virtualized NPB seamlessly delivers streamed packets to cPacket and third-party virtualized and physical components, analytics, and tools. Tight integration with all cPacket Intelligent Observability Platform components allows you to deploy, orchestrate, and manage a holistic monitoring fabric to gain visibility that seamlessly and elastically scales to encompass physical, virtual, single-cloud, multi-cloud, and hybrid IT environments from every packet from every monitored vantage point [2]. Key Performance Indicators (KPIs) and timestamps are available to the cStor/cStor-V appliances for analysis and visualization in dashboards presented by an instance of the cClear/cClear-V Analytics Engine to view and drill into the network packet data to search for specific ports, hosts, etc., to investigate threats and problems.

Comprehensive Visibility from Network Packet Data

Observability, flow data, KPIs, and other analytics results provide visibility and actionable network intelligence from acquired network packets.

Security Posture Strengthening with Network Packets

The virtualized NPB and the streamed network packet data it delivers are essential for implementing Network/Extended Detection and Response (NDR/XDR) as part of your security defenses, especially in environments where a native packet mirroring service is not available. Stored network packet data is also essential for threat hunting, post-breach forensic analysis, and supporting vulnerability and penetration assessments.

Augmenting and Extending Packet Mirroring Services

Filtering and replication extend native packet mirroring services that do not provide these functions. Without the NPB, you would have to orchestrate mirroring sessions to deliver packets to multiple targets, each with a usage-based cost. Management and cost quickly become untenable as the number of vantage points and targets increase, which are among the benefits of having a unified Visibility Fabric with centralized management.

[2] Refer to the cCloud Suite data sheet

Acquiring packets in addition to mirroring extends and increases your overall visibility with a greater granularity from custom vantage points.

Unified Fabric Management and Workflow Simplicity

IT teams only need to learn and use one user interface and type of workflow. Installing and configuring the virtual NPB is straightforward and consistent irrespective of where instances are deployed (which is less burdensome and problematic than using agents).

Versatile Usage

Elastically deploy packet acquisition nodes at strategic vantage points for subsequent replication, forwarding, and analysis to understand threats, breaches, and performance problems. Nodes can be located anywhere within your environment, including branch offices, remote sites, data centers, and public clouds. The cVu-V virtualized NPB can be configured to filter and forward acquired packets to any local, virtual, and cloud-hosted targets (refer to the Technical Specifications for details). In addition to filtering, you can use the configurable deduplication, packet slicing, and header truncation functions to reduce the volume and tailor the packets to meet each receiver's ingestion requirements.

Instances of cVu virtualized and physical appliances can be deployed at strategic vantage points for visibility and packet acquisition that scales across distributed and hybrid environments. When used with the cClear or cClear-V Analytics Engine, network packets from all nodes are combined to present a holistic unified view of the IT environment.

The virtualized NPB can be run in virtualized Network Function Virtualization (NFV) environments in the Single-Root Input/Output Virtualization (SR-IOV) mode to capture/analyze the LAN/WAN traffic. It also interoperates with qualified Cisco ISRv virtual routers for gaining visibility, insights, and observability.

Add self-hosted virtualized NPB instances to meet temporary (elastic) and permanent scaling needs. This flexibility gives you a cost-effective and easy way to monitor traffic at strategic vantage points or for specific periods (e.g., you can use an instance to troubleshoot a particular problem then decommission that instance). Additional flexibility includes typical packet brokering and a unique direct packet acquisition function.

Packet Brokering (Filtering and Replication)

The cVu-V virtual NPB provides packet brokering that streams packets to your choice of targets by replicating and forwarding packets (refer to the Technical Specifications for details). You can use configurable packet filtering to tailor the delivery and thin packet volume. For example, an instance of the cVu-V NPB will filter packets forwarded to an instance of the cStor-V Packet Capture appliance to reduce bandwidth, storage utilization, and related costs.

Direct Packet Acquisition

This mode works with all environments. It is beneficial for environments that do not have native packet/traffic mirroring services because it acquires packets without a native mirroring service. This mode lets you establish custom mirroring at vantage points from your VPC subnets that give you functionality equivalent to packet/traffic mirroring services. It goes beyond fixed mirroring by enabling packet acquisition from vantage points that are strategic or of other interest.

The virtual NPB acts as a network element within a dedicated monitoring subnet when used for packet acquisition. User-Defined Routes direct traffic to replicate the traffic to downstream targets (e.g., tools). The NPB forwards all traffic onto the original path for delivery to its intended destination.

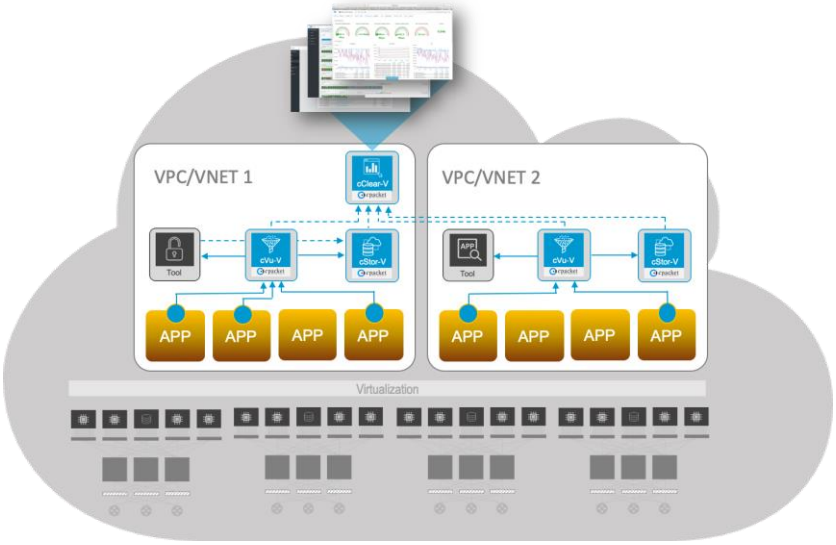
When using this function, the virtual NPB is in the data path, so you should consider deploying multiple instances behind a load balancer capable of validating the health of the virtual NPB to ensure fault-tolerance of the data path.

Open Architecture

The virtualized NPB interoperates with all physical and virtualized appliances of the Intelligent Observability Platform. It also readily interoperates with a vast assortment of third-party services and tools by receiving and transmitting industry-standard network packets.

Deployment and Use Cases

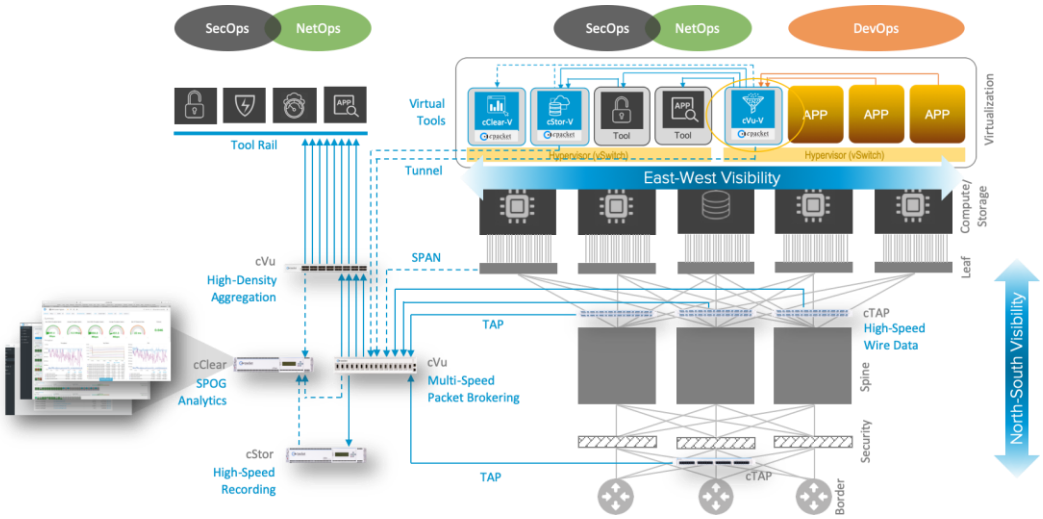
Visibility based on streamed and stored network packets in public cloud infrastructure seamlessly scales across multiple Virtual Private Clouds, Availability Zones, and the entire infrastructure (i.e., a multi-cloud environment). The same applies to hybrid environments that include physical infrastructure.



architectural diagram for comprehensive public cloud visibility

Load balancers (including virtualized load balancing services) have several uses, including enabling parallel paths for fault tolerance and high availability. Each image for a specific public cloud interoperates with the native load balancing service (if available), so you can filter, replicate, and forward traffic behind a load balancer.

You can use the virtualized NPB in on-premises virtualized infrastructure such as branch offices and data centers to acquire packets from DPDK/SR-IOV in direct mode, hypervisor-based virtual-switching with support for VMware Standard/Distributed vSwitch and Open vSwitch (OVS) mode, and overlay tunnels (i.e., VXLAN, ERSPAN).



architectural diagram for complete north-south and east-west visibility in a hybrid environment

Cost-Effective and Flexible Licensing

The cStor-V Virtualized Packet Capture appliance has flexible licensing that allows you to control, contain, and right-size cost. Licensing options include bringing your own usage license (BYOL). The virtual appliances can be instantiated on-demand for timed use (e.g., hourly, weekly, monthly, etc.). The licensing options give you elastic flexibility to deploy software images in your target environments at the scale needed. Refer to the ordering information section for additional details.

Technical Specifications

Key Features:

	cVu-V
Packet Replication	Yes
Flow-based Load Balancing	Yes
Filtering	Yes
Deduplication	Yes*
Packet Slicing	Yes*
Header Truncation	Yes*
VXLAN Encapsulation	Yes
cClear/cClear-V Analytics Engine Integration	Yes
Role-Based Administration	Yes
Software Upgrade/Restore	Yes
Web-based GUI / CLI for System Management	Yes
TACACS+/RADIUS Authentication	Yes

* Roadmap or planned. Check with your cPacket sales representative for the most current product release information.

Performance and Specifications:

	cVu-V
Targets	Up to 10
Monitoring Rate / Instance	Up to 10Gbps
vCPU	4
Memory	16GB
System Disk	40GB
Maximum Monitoring Throughput*	Scalable (Refer to Ordering Information)
Hypervisor Supported	VMware ESXi, MS Hyper-V, KVM, Cisco NFVIS
High-Performance Mode	DPDK/SR-IOV
Public Cloud	AWS, MS Azure, GCP
Cloud Data Mirroring	AWS VPC Traffic Mirroring GCP Packet Mirroring

* Storage scales with machine type selected

Ordering Information

SKU	Description
CP_CCLOUD_CVU_V_SUB-xG (Where X is the capacity. Options 1G, 5G, 1(25G, 50G, 100G, 250G, 500G, 1TB)	cPacket cVu-V virtual appliance up to xGbps aggregate monitoring capacity, 1 year subscription. Deployable on top of VMware ESXi, Microsoft Hyper-V, KVM, Cisco NFVIS, and as part of cCloud BYOL solution in AWS, Google Cloud, and Microsoft Azure. Requires cClear-V subscription. Gold level maintenance included.
CP_CCLEAR_CON	Annual license to connect with cClear appliance or cClear-V software instance at 3% of the list price of the connected device.

For additional information, go to the cCloud Visibility Suite product webpage.

About cPacket Networks

cPacket Networks de-risks IT I&O through network-aware service and security assurance across hybrid and multi-cloud environments. Our AIOps-ready Intelligent Observability Platform provides single-pane-of-glass analytics and deep network visibility required for complex IT environments enabling Fortune 500 organizations worldwide to keep their business running. cPacket solutions are fully reliable, tightly integrated, and consistently simple. Our cutting-edge technology enables network, application, and security teams to proactively identify issues before negatively impacting the business. The result: increased service agility, enhanced experience assurance, and faster transactional velocity. Learn more at www.cpacket.com.