cpacket NETWORKS

Application Note

Troubleshooting Cloud Subnet Traffic with cCloud™ Visibility Suite

Enable Access, Capture, and Analyze Cloud Traffic to Reduce Service Outages

www.cpacket.com

Highlights

- Learn how to Troubleshoot Subnet Connectivity Issues in East-West direction
- Learn how to Quickly Resolve Network Problems for Virtual Machine Latency between Subnets
- Learn how to Replicate, Forward, and Capture Subnet Traffic for Forensic Analysis

Introduction

This Application Note steps you through how to instrument public cloud infrastructure for network visibility to reduce the number and duration of service outages and disruptions. You will see how to investigate and solve multiple operational use cases, subnet connectivity issues, virtual machine latencies between subnets, and captured subnet traffic for detailed forensic analysis. The examples in this document use a Microsoft Azure environment.

Monitoring Cloud Infrastructure Intra East-West Traffic

You need continuous and detailed network-centric visibility to gain cloud network performance metrics. Further instrumentation is required in the cloud environments to provide agentless packet data capture and off-load replication services from the production workloads. Network virtual appliances and Gateway Load Balancer (GWLB) services are available to provide insights into the production network packets. These network visibility services ensure that packets are replicated and delivered to the correct security tools, network performance monitoring tools, and dashboards that are key to effective troubleshooting and helping to reduce service outages.

Agentless Subnet Monitoring

The cCloud Visibility Suite is built for public multi-cloud infrastructure with out-of-the-box support for Amazon Web Services, Microsoft Azure, and Google Cloud. The suite is an integrated set of components that perform packet acquisition, replication, forwarding, packet capture-to-storage, and analytics. Altogether the suite provides vital visibility for cloud infrastructure without the management overhead and additional security risks of placing agents or probes into the production workload host, virtual machine (VM), or application layer.

The cCloud Visibility Suite consists of these components:

cClear®-V Analytics Engine that provides network health, traffic analytics, visualizations, and alerts

cStor®-V Virtualized Network Packet Capture and Storage including PCAP retrieval and forensics

cVu®-V Virtualized Network Packet Broker including packet data acquisition, replication, forwarding, and delivery to analytics, tools, and dashboards

Figure-1 below shows an example of a simple Microsoft Azure environment for subnet monitoring using the suite's virtual appliances for network visibility. Two subnets, "Prod" and "Default" have been created to simulate production East-West traffic with a separate subnet "monitoring" for the tool's infrastructure.

The traffic is routed via User Defined Routes using the Azure Route Table between the subnets. The virtualized network packet brokers provide replication and forwarding services to all packets passing through the Azure Load Balancer. The virtualized packet capture appliance routes packets to storage for historic forensics, replay, and exporting as streams and PCAP files.

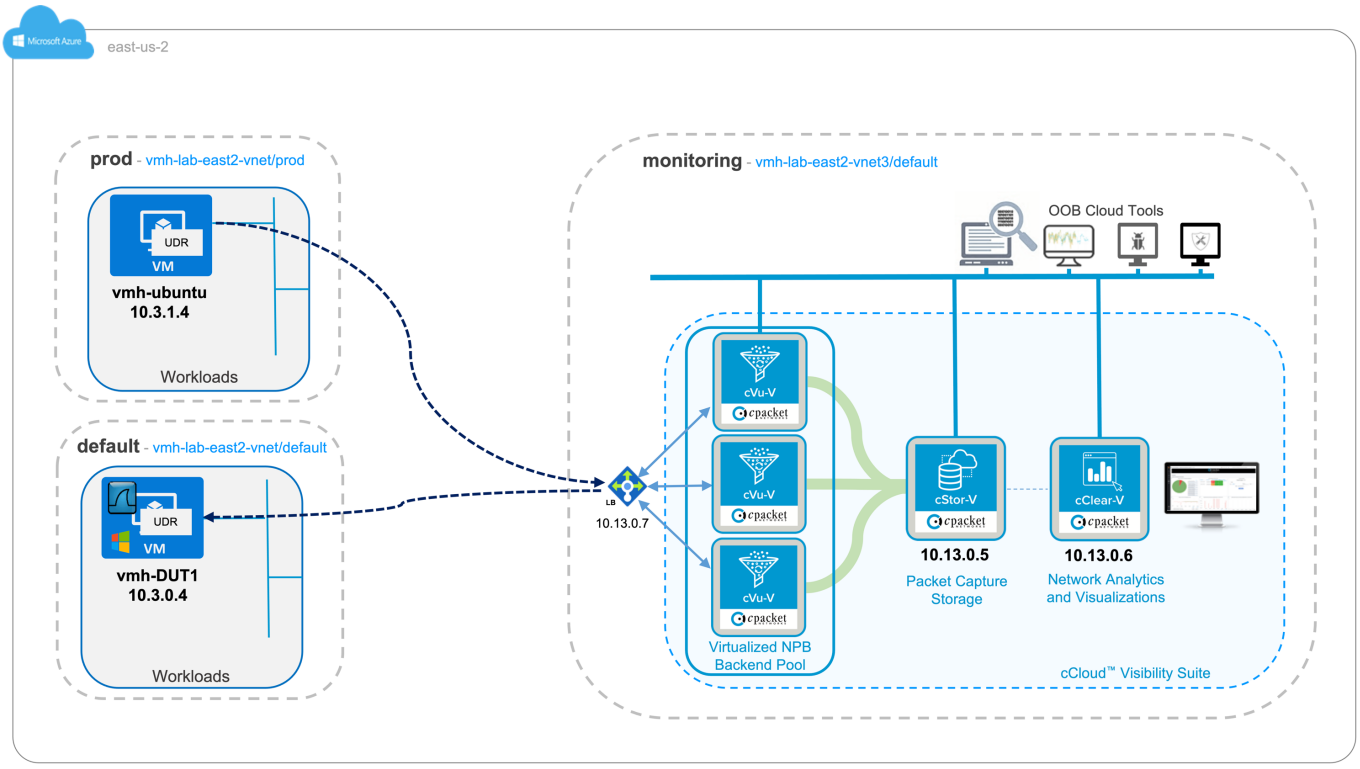

Figure-1 – Cloud Subnet Monitoring Lab Setup Example

You must first have a cloud environment configured and running before deploying any cCloud Visibility Suite components, and set up the following essential functional system prerequisites:

- Access
  - SSH keys
- Storage
  - Resource location created for target VMs
  - Access to cPacket Networks cCloud Visibility Suite vAppliances
- Networking
  - Monitoring Subnet (recommended for tools)
  - Understanding of network topology for routing
  - Route Table configuration
  - Subnet routing must be set up and working
  - Security Policy

Figure-2 shows an example configuration view from the Microsoft Azure Portal:

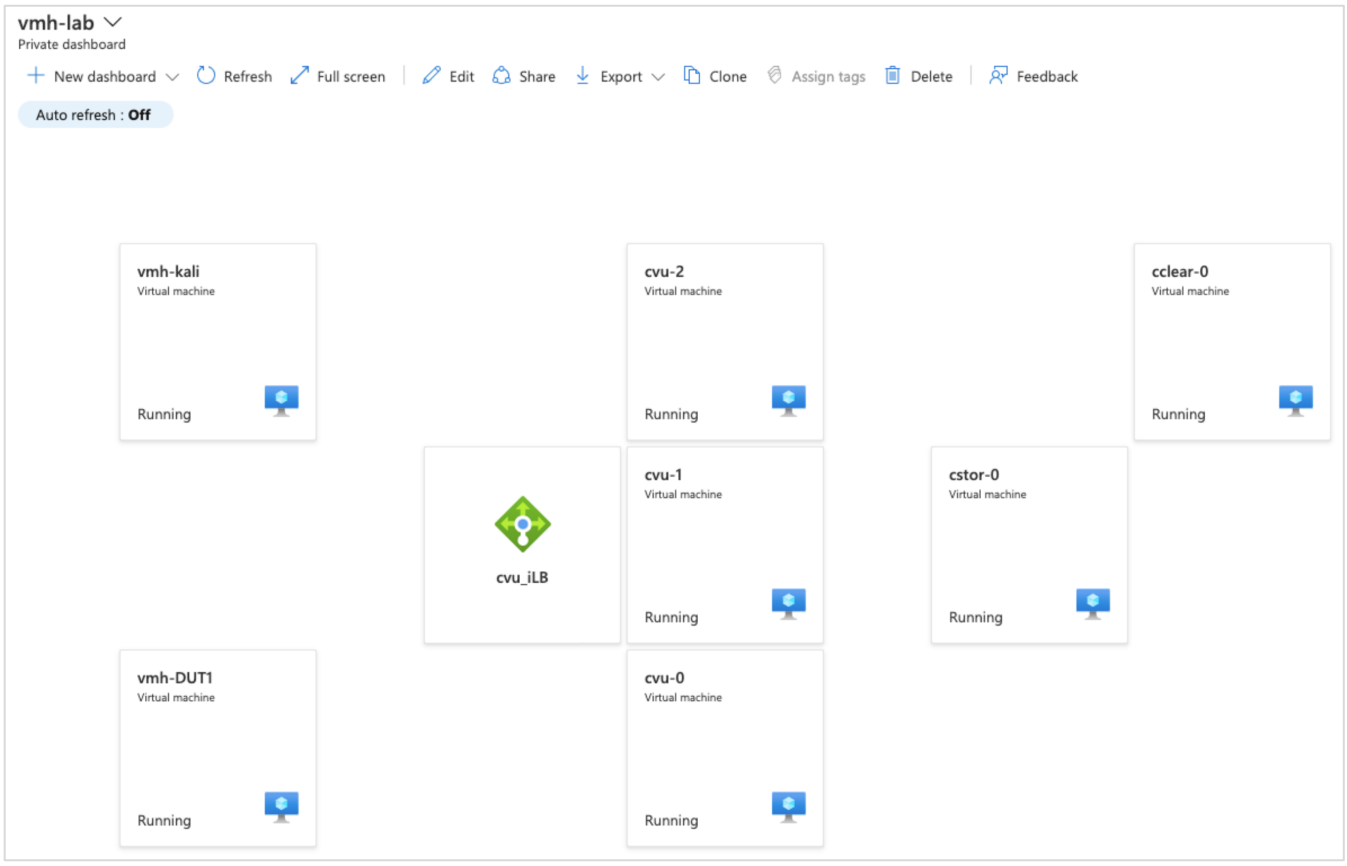

Figure-2 – Microsoft Azure Portal Dashboard View

Figure-3 shows a cClear-V **TCP Health Level 1** dashboard view of the environment's Subnet segments Prod, Default, and Monitoring before generating and injecting network traffic. The Key Performance Indicators (KPIs) in this example are green, indicating that everything monitored is operating normally.

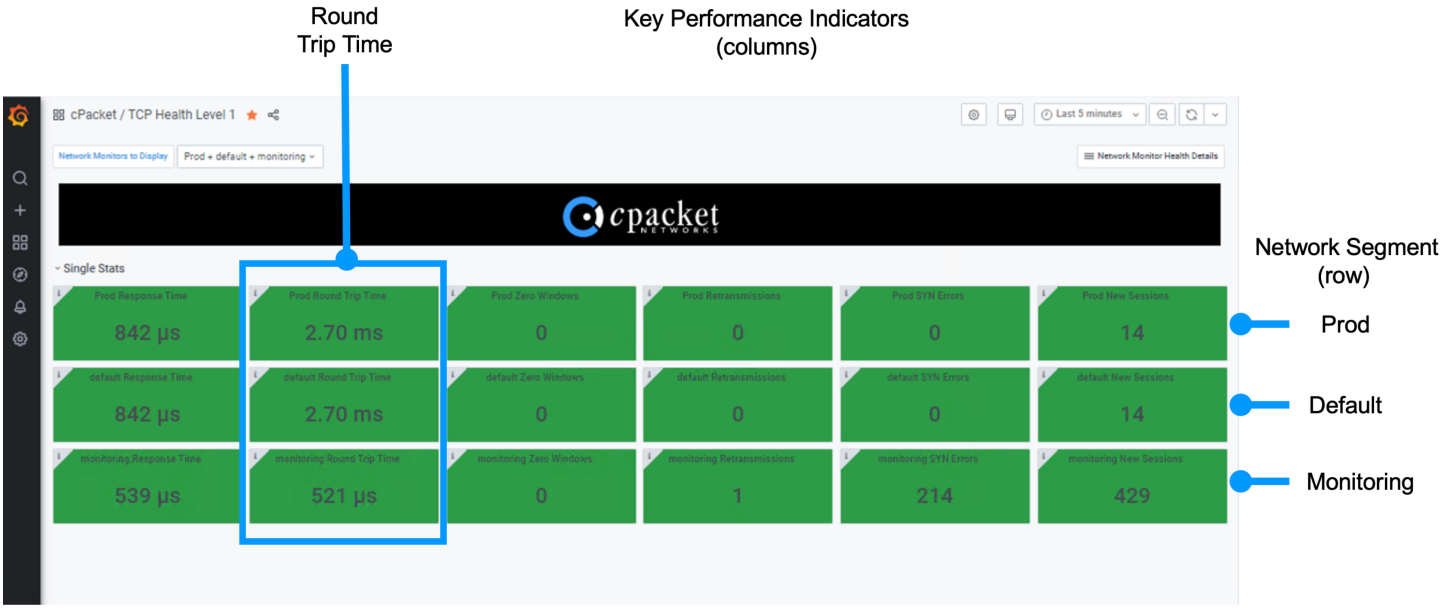

Figure-3 – Dashboard showing TCP Health Level 1 with Normal Operational Status

Use Cases

1 – Isolating Subnet Connectivity (East-West)

Description: – An unknown issue is reported in lab-east2-vnet/default (refer to Figure-1)

Simulation:
- – Source — Host 10.3.0.4 in subnet lab-east2-vnet/prod
- – Traffic Type — Flooding http on port 8080
- – Destination — Host 10.3.1.4 in subnet lab-east2-vnet/default

IT Operational Response: – Need to see network health information, including visualizations of TCP Analytics for the subnet traffic over the last 30-minutes

Workflow: – Directly login to the cClear-V virtual appliance and choose the Network Health Overview dashboard

Select the cClear-V dashboard **Network Health Overview** for a summary view of all Lab traffic. Figure-4 shows that the “New Sessions” KPI has 58268 open sessions. The red status is a visual alert. Click on the Lab network row to drill down to review the subnets details.

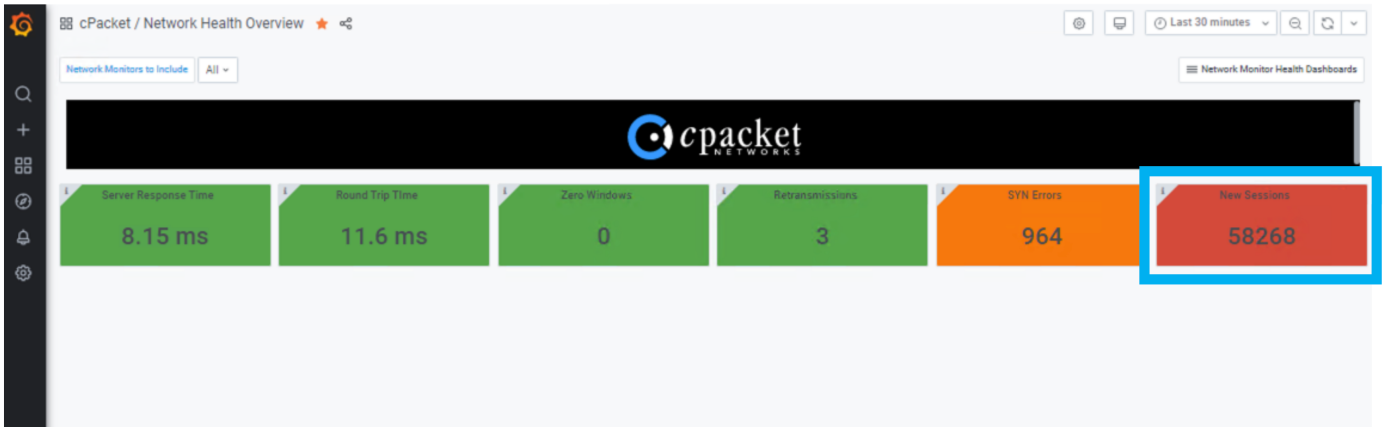

Figure-4 – Network Health Overview Dashboard

Next, Figure-5 shows the cClear-V **TCP Health Level 1** dashboard and each row representing each network segment. Prod and Default subnets show the “New Sessions” KPI and are triggered red, with the Monitoring segment displaying minor counters (orange). Click on the red default New Sessions box for further details

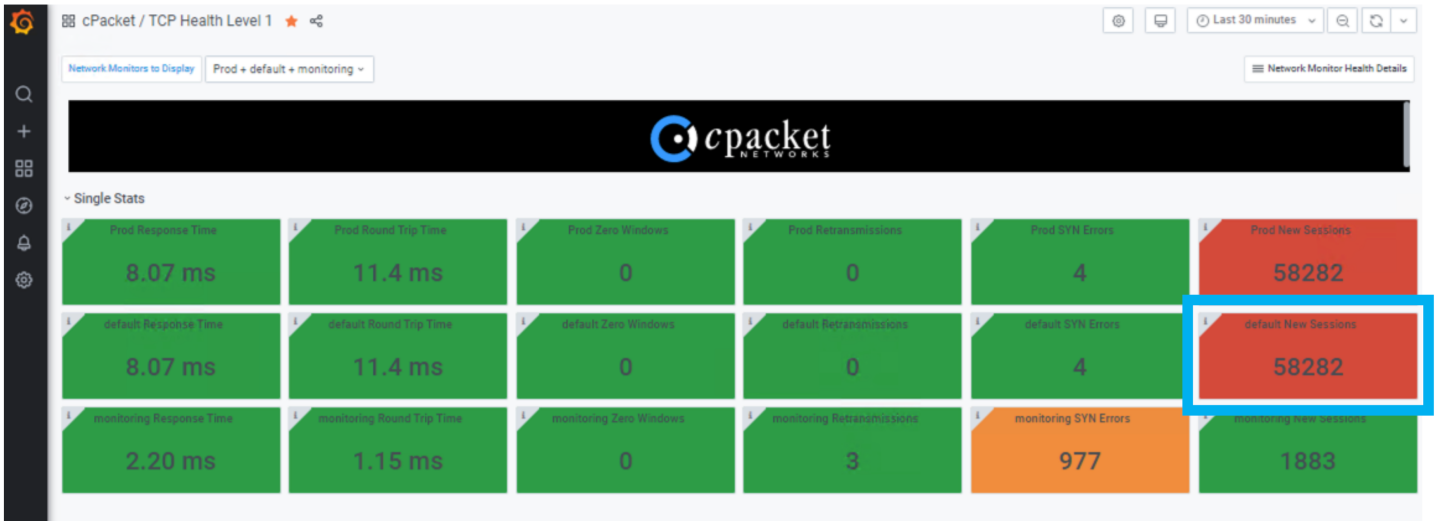

Figure-5 – TCP Health Level 1 Dashboard

Figure-6 below shows the cClear-V **Syn Metrics Network Monitor Level 2** dashboard with details for the “New Sessions by Server” highlighted in red, the destination host IP 10.3.0.4, and the port number 8080 indicating the New Sessions Application.

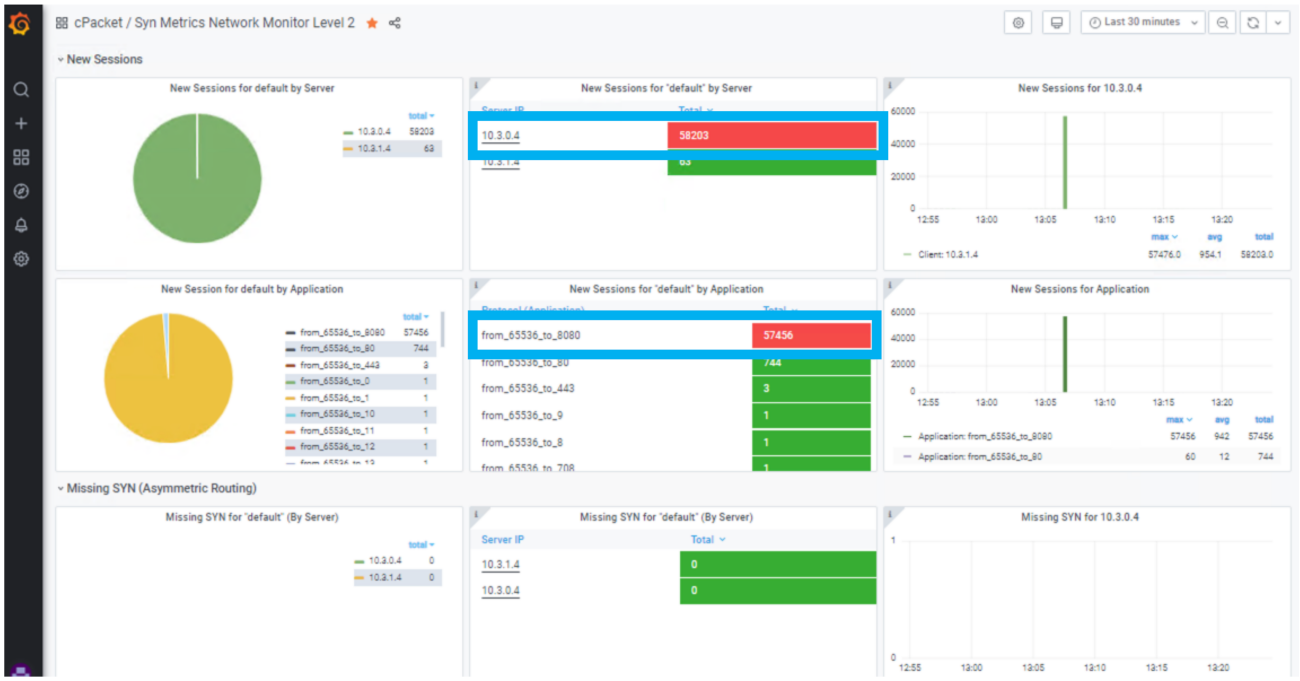

Figure-6 – Network Health Overview Dashboard

Outcome: In this use case, the operator used dashboards presented by the cClear-V Analytics Engine to gain the insights with just a few clicks to isolate the network segment with the issue, the IP addresses involved, and the destination port of the traffic.

2 – Determining Virtual Machine Latency between Subnets

Description: – A latency issue is reported in lab-east2-vnet/default subnet (refer to Figure 1)

Simulation:
- – Source host 10.3.0.4 in subnet lab-east2-vnet/prod
- – Traffic Type Latency impairment injection
- – Destination host 10.3.1.4 in subnet lab-east2-vnet/default

IT Operational Response: – Network Health and TCP Analytics for Latency over the previous 1-hour

Workflow: – Directly login to the cClear-V virtual appliance and choose the Network Health Overview dashboard

Figure-7 shows the cClear-V **Network Health Overview** dashboard in a normal status before inserting traffic. Note: The **Round-Trip Time (RTT)** latency displays **352 microseconds**!

Figure-7 – Network Health Overview Dashboard

Figure-8 shows the cClear-V **Network Health Overview Dashboard** after generating traffic and a 6.08ms RTT using the last 5-minute sample.

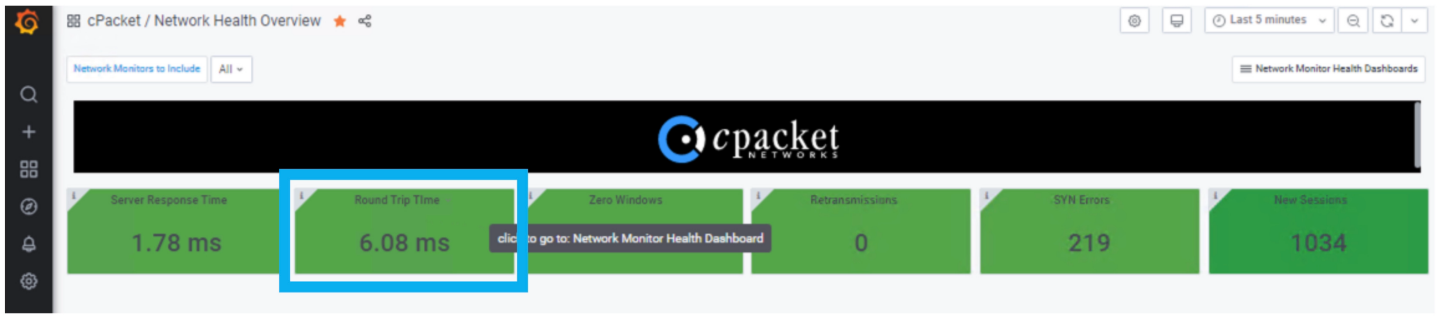

Figure-8 – Network Health Overview Dashboard

Clicking on the KPI RTT will launch the cClear-V **Network Health Level 1** dashboard shown in Figure-9 with the RTT approximately 6ms in the “Default” and “Prod” network segments.

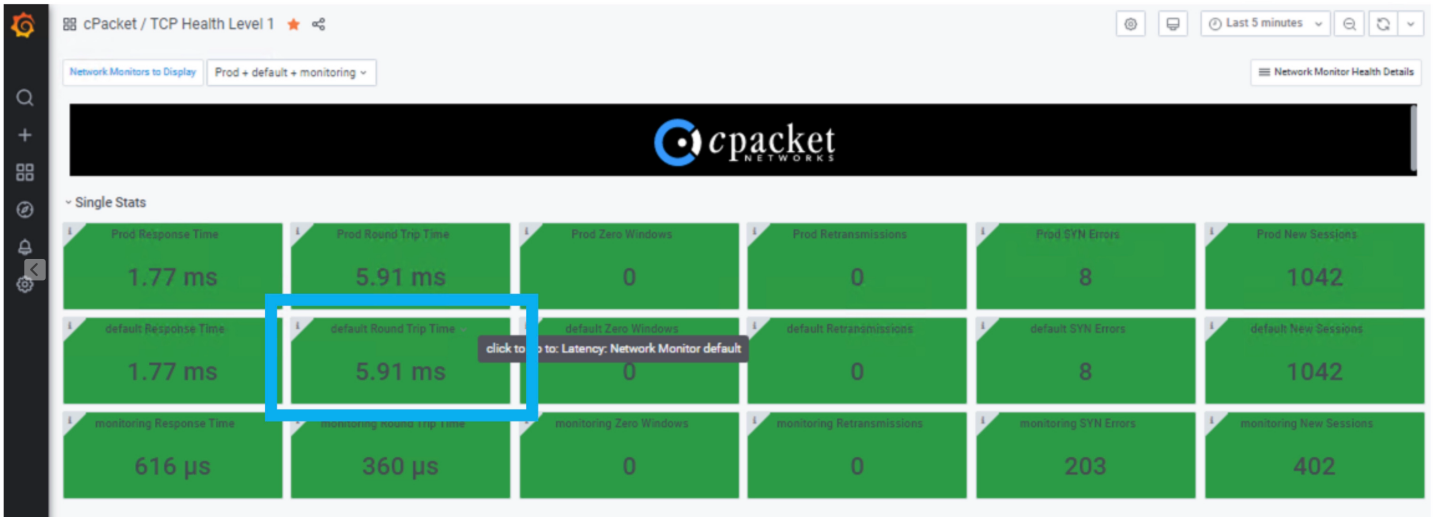

Figure-9 – Network Health Overview Dashboard

Clicking on the RTT will launch the cClear-V **Latency Network Monitor Level 2** dashboard shown in Figure-10. This visualization shows the two network devices involved in the connectivity. While the average latency reported is 4-5ms, the trending graph over the previous hour displays a maximum RTT of 76ms, peaking at 01:17 pm over a 10-minute period. The IP address of 10.3.1.4 is the server of the source impairment injection, with 10.3.0.4 the target webserver responding to HTTP requests.

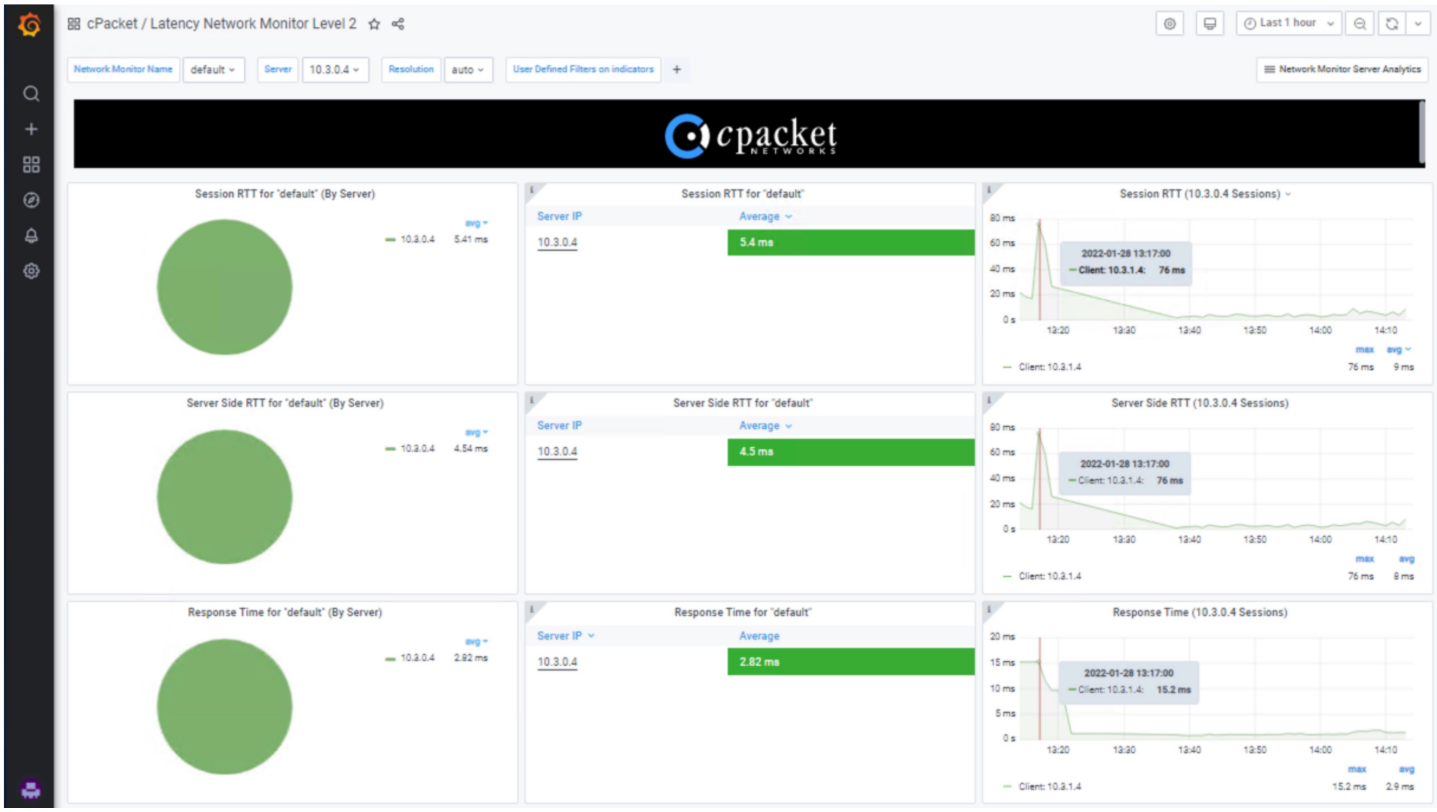

Figure-10 – Network Health Overview Dashboard

Outcome: In this use case, the operator used dashboards presented by the cClear-V Analytics Engine to gain the insights with just a few clicks to review the **RTT data for the immediately preceding hour** and discover when specific hosts were impacted by latency in the network.

3 – Capturing Subnet Traffic for detailed Forensic Analysis

Description:	– An issue is reported in lab-east2-vnet/prod including approximate time (Refer to Figure 1)	
Simulation:	– Source	host 10.3.0.4 in subnet lab-east2-vnet/prod
	– Traffic Type	Flooding http on port 8080
	– Destination	host 10.3.1.4 in subnet lab-east2-vnet/default
IT Operational Response:	– The subnet packets for the last 2 minutes from 12:30 pm are needed	
Workflow:	– Directly login to the cStor-V virtual appliance, group packets for the timeframe needed, export as a PCAP file, and analyze using Wireshark	

Select the "**Data Capture**" tab and chose your options:

Time Selection Mode:	**Start/End**
Start:	**2022-01-26 12:30:00**
Stop:	**2022-01-26 12:32:00**
Download Size:	**Limited**
Maximum Download Size:	**10MB** (first)
cVu Port Filter:	default
Filter Type:	**Fast** (all packets)
Fast Filter:	**default**

Select **Start Download**

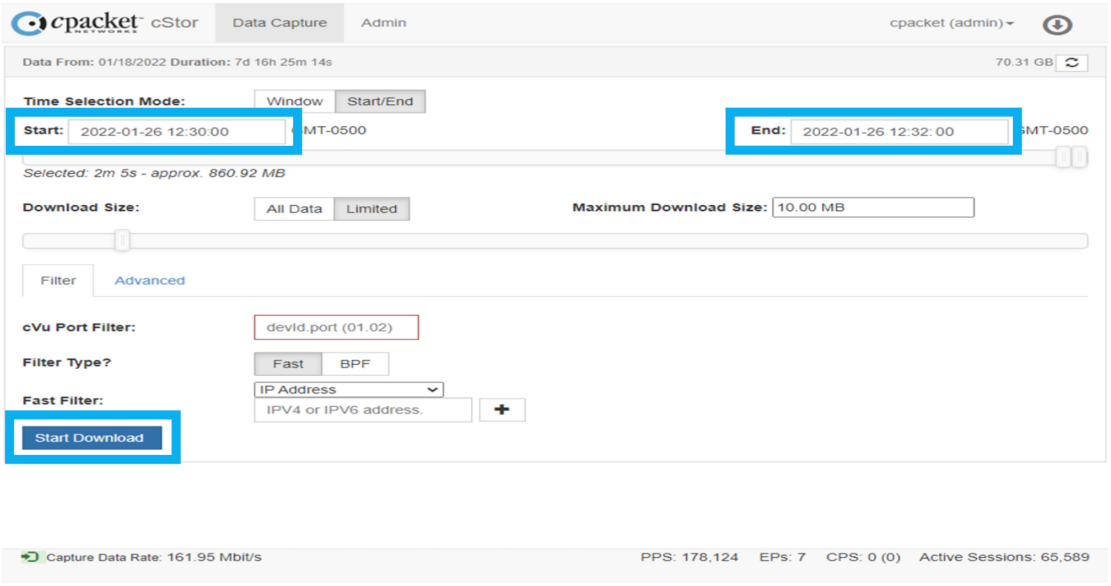

Figure-11 – Analysis of Captured Packets

Click on “**Start Download**” to transfer the PCAP file to your local computer. After the transfer is completed, open it into Wireshark for analysis. Figure-12 shows Wireshark displaying the traffic with the source address 10.3.1.4 generating HTTP traffic to port 8080 on destination 10.3.0.4.

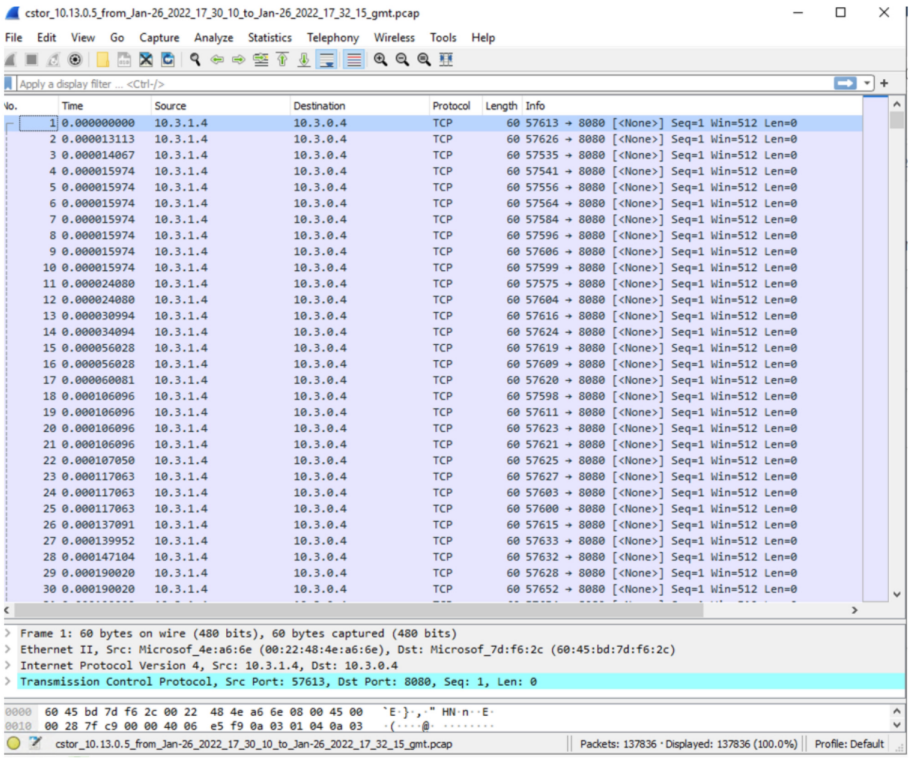

Figure-12– cStor-V PCAP for Forensic Analysis

Outcome: In this use case, the operator selected, grouped, and exported a specific set of captured packets as a PCAP file for analysis using Wireshark. The analysis shows the source 10.3.1.4 generating HTTP traffic on port 8080 to the destination IP 10.3.0.4

Summary for Cloud Subnet Monitoring

This document showed three common use cases where monitoring subnet traffic using the cCloud™ Visibility Suite helps you quickly isolate issues and troubleshoot their causes by analyzing streamed and stored network packets acquired from subnet traffic. These common use cases often result in service outages, poor end-user experiences, and lost productivity. In the first two use cases, the issues and their root causes were determined using the cCloud Visibility Suite network visualizations and dashboards. The third case showed how to directly access the data from the packet capture store for forensic analysis to determine the root cause.

Related Information:
cPacket Intelligent Observability Platform for Azure – Solution Brief