CASE STUDY

Virtual Insights with CloudLens

European ISP extends visibility into virtualized infrastructure

Introduction

End-to-end monitoring and access to data in virtual environments are critically important for software-defined data centers (SDDCs). Security and performance monitoring tools depend on rich network packet data to detect potential threats and track vital quality-of-service (QoS) metrics. With the spread of virtualization, which includes network functions, getting the data to the right tool became more challenging.

Organization

Proximus, the largest internet service provider (ISP) in Belgium, launched its network function virtualization (NFV) initiative in 2018 and has been deploying different telecommunication applications using a cloud infrastructure including virtual IP multimedia subsystems, (vIMS), and software defined wide area networking, (SD-WAN).

Migrating complex physical internet service provider (ISP) networks to a new network with virtualized functions does not happen overnight or even in a month — these projects generally require several years.

Organization:

- Proximus – largest ISP in Belgium

Challenges:

- visibility into virtualized east-west traffic
- reliable traffic analytics and troubleshooting capability
- preserve investment in physical monitoring and visibility

Solutions:

- CloudLens Management Server
- CloudLens vTAP
- Vision ONE NPB
- Vision 7300 NPB

Results:

- faster troubleshooting/ remediation
- end to end visibility including east/west traffic

KEYSIGHT TECHNOLOGIES

Challenge(s)

While deploying these applications, Proximus faced the challenges of providing the same visibility and analytics across physical and virtual functions. For both environments, Proximus deployed several traffic analytics probes. These probes relied on physical taps, tap aggregation switches, and Keysight Vision network packet brokers — Vision ONE, Vision 7300 — in the legacy environment to deliver the duplicated traffic to these probes.

Proximus had to retain the same level of visibility in the new virtual environment as in the current physical one. Network functions ran as virtual machines (VMs) on the same physical server; the east-west traffic did not cross any of the physical links where the physical taps would have been located. Additionally, different IP Multimedia Subsystem (IMS) components were migrated over several years. Having reliable traffic analysis and troubleshooting tools was of vital importance.

A key driver for the migration was to contain the total cost of ownership. Proximus looked for an opportunity to preserve their investments while using their existing monitoring and security tools.

Solution(s)

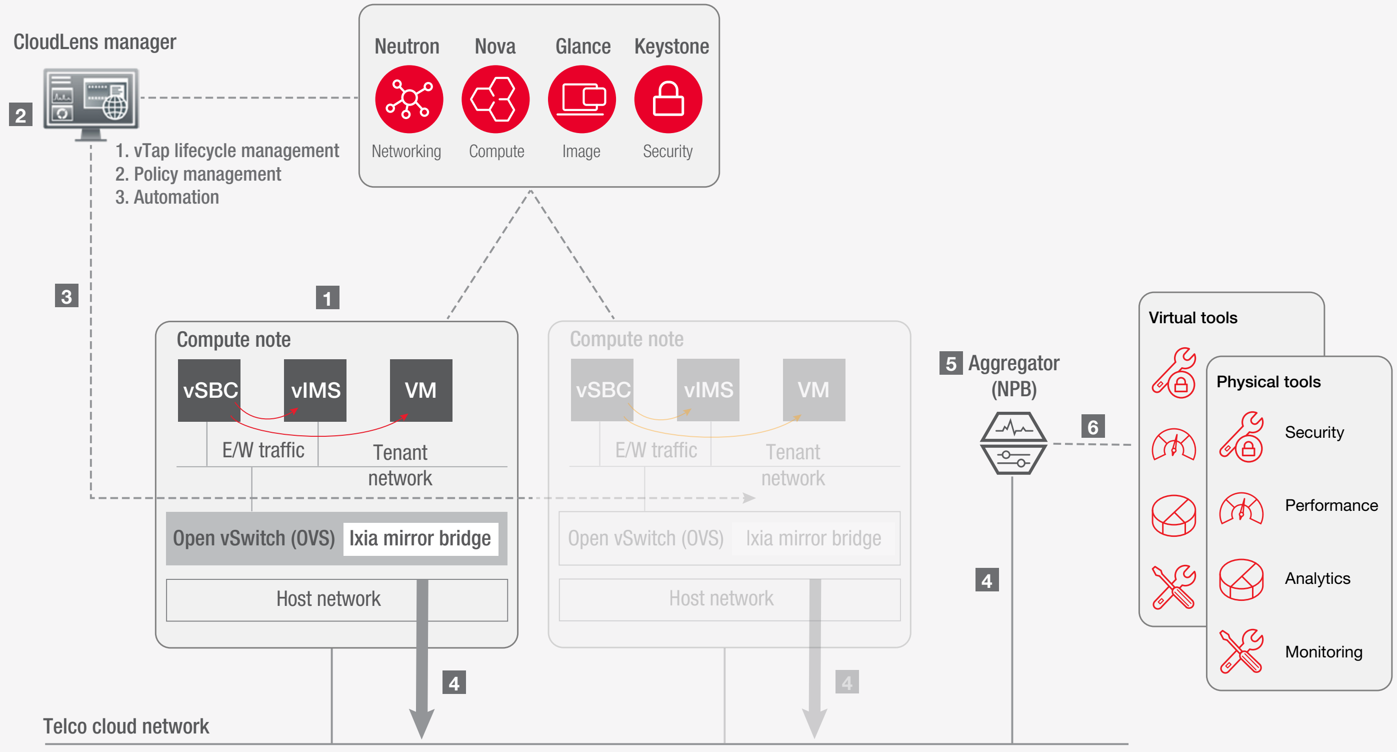
Deploying Keysight CloudLens, our visibility solution for virtualized environments, solved this issue for Proximus. One of the key components, CloudLens vTap, offers virtual tapping and filtering capabilities enabling Proximus to capture traffic from the virtualized environment that formerly fell into a blind spot and forward it to the right destination.

Proximus did not need to change their current processes for support, monitoring, and security. The end-to-end reporting remained the same using a single platform independent of the origin of the traffic – both physical and virtual.

Internal customers using that data would not notice the migration because their daily workflows would not change. This consistency ensured that Proximus could deliver on commitments to customers while ensuring the network's core was ready for any future challenges.

Proximus virtual infrastructure is running on OpenStack / KVM. Proximus deployed Open vSwitch software and CloudLens vTap to mirror the network traffic at the virtual workload or virtual switch level. The virtual taps are deployed to the monitored hosts and managed from the CloudLens management server (CLMS), the central management component that administers the virtual taps and packet capture policies.

The VisionONE network packet broker sanitizes the mirrored network traffic between the virtualized functions via generic routing encapsulation (GRE) tunnel to third-party monitoring and security tools. See figure 1.



1 Virtual application setup

2 Install CloudLens vTap environment

3 Setup traffic mirroring policies

4 Selective mirrored traffic sent to aggregator

5 NetStack, PacketStack, AppStack capabilities

6 Optimized traffic sent to monitoring tools

Figure 1. CloudLens deployment in an OpenStack / KVM environment

Results

Like many organizations, Proximus is migrating many services from physical to virtual environments. Also like many organizations, these migrations can take years to complete. In the interim, the business needs to continue to be able to deliver support, security, and monitoring. Limited visibility into traffic in their virtualized environment and a desire for single pane of glass management provided considerable challenges to the European ISP.

With CloudLens they were able to deploy new services on cloud platforms with confidence, eliminating blind spots that can hide security vulnerabilities, attacks or other network related issues. With CloudLens they were able to regain network visibility into their software-defined data center (SDDC), including challenging virtualized east-west traffic spanning one or even multiple clouds.

Visibility into packet level data gave Proximus valuable insight, enabling them to improve the speed of detection and incident remediation. Continuous validation of security infrastructure helps them ensure their solutions are configured properly and working effectively.

Please visit our website to learn more about CloudLens visibility solution.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT
TECHNOLOGIES