GigaVUE Cloud Suite for OpenStack-based Networks

Intelligent Traffic Visibility for OpenStack

Key Benefits

Traffic acquisition
- Flexibly acquire via VMs, agents or ‘tunnel as a source’ methods including from Nuage and Palo Alto Networks
- Minimize agent overload for simplification and reduced CPU processing
- Obtain comprehensive workload visibility
- Dynamically scale virtual TAP instances up and down as needed
- Quickly bring new revenue generating services on line

Traffic forwarding for network and security operations
- Selectively aggregate, optimize, replicate and distribute
- Service chain multiple GigaSMART apps for ease of operation and reduced traffic flows
- Automatically modify and scale high-performance visibility nodes
- Load balance traffic to tools for improved availability and reduced scaling needs

Management and orchestration
- Centralized management across multiple clouds with tight coupling with OpenStack and other orchestration suites
- Increase architectural flexibility by choosing from multiple tunnel options including VXLAN, L2GRE and ERSPAN
- Simplify traffic orchestration through use of monitoring sessions

Figure 1. Improving visibility in a virtual project using GigaVUE Cloud Suite
The rapid evolution of Infrastructure-as-a-Service (IaaS) brings instant advantages of economies of scale, elasticity and agility to organizations seeking to modernize their IT infrastructures.

The obvious challenges of this approach include the inability to access all traffic in support of threat detection and response, and application and network performance in these environments. Current security and monitoring tools that operate in private clouds such as OpenStack often lack workload visibility.

One approach to this challenge is to adopt what is shown in Figure 1 on the left where agents for each tool are placed within each workload VM for every tool. Such an approach, however, overloads compute instances, increases application and bandwidth costs and forces an architecture redesign when adding new security and monitoring tools. An efficient and optimal solution, in contrast, is to use Gigamon GigaVUE® Cloud Suite as shown on the right in Figure 1 where only one agent per VM is installed or one agent-less virtual TAP is deployed per hypervisor.
GigaVUE Cloud Suite is an intelligent network traffic visibility solution that acquires, optimally processes and distributes selected traffic to security and monitoring tools. This enables enterprises and service providers to extend their security posture and network monitoring to OpenStack and accelerate the time to detect and mitigate threats and operational issues, while helping assure compliance.

### Accelerate Application Migration to the Cloud

Using GigaVUE Cloud Suite for OpenStack, security architects can ensure an effective security posture in the cloud, thereby accelerating the onboarding of applications to OpenStack.

GigaVUE Cloud Suite for OpenStack, as shown in Figure 2, acquires traffic in one of two ways. Either with a single, lightweight agent installed on the workloads, in this case OpenStack instances. Or by installing a single agentless VM on each server that is to be monitored. The platform integrates with OpenStack APIs to discover the cloud infrastructure, deploy visibility nodes in the projects that collect aggregated traffic from all the agents or VMs and apply advanced traffic intelligence prior to sending selected traffic to security and monitoring tools. Visibility nodes may also receive traffic via ‘tunnel as a source’ methods including packets from Nuage-based proxy services and Palo Alto Network devices.

With this solution, organizations can take advantage of:

- **Increased security:** Centralize visibility for security and performance monitoring of all projects in an organization. Network and security operations and incident response teams can use network visibility to rapidly detect and respond to threats, vulnerabilities, compliance violations and operational issues across the infrastructure.
- **Reduced data costs:** Optimize costs with pervasive visibility for security and monitoring without increasing load on compute instances as more security and monitoring tools are deployed. Acquire traffic once from compute instances and leverage traffic intelligence to optimize data to multiple tools. Specifically, with packet deduplication and slicing, over 50 percent reduction in data to tools can be achieved.
- **Operational efficiency:** One common platform for visibility across the entire IT environment enables consistent insight in OpenStack. Acquire network traffic with minimal impact to a VM instance’s utilization and apply traffic intelligence before distributing to multiple tools for analysis.
- **Operational agility:**
  - Rapidly detect changes in projects being monitored
  - Automatic Target Selection®: Automatically extract network traffic of interest anywhere in the infrastructure being monitored without having to specify the specific target compute instances to monitor
  - Flexibility to perform the analysis of traffic anywhere
  - Automate and orchestrate visibility using open REST APIs
  - Optionally choose to obtain workload traffic via tunnel-as-a-source methods including from Nuage and Palo Alto Networks
- **High performance with infinite scalability:** The suite take advantage of DPDK libraries and NIC polling-mode drivers to offload TCP processing and expand performance to gigabit/second levels per instance with an unlimited number of visibility nodes.
GigaVUE Cloud Suite Components

G-νTAP Module
A lightweight agent-like module deployed in an OpenStack VM instance. The module mirrors traffic from the production instance and sends the mirrored traffic via L2GRE or IPsec to GigaVUE H or GigaVUE V series nodes.

G-νTAP VM
A lightweight VM deployed as its own OpenStack VM instance. The VM directs the Open vSwitch (OVS) to mirror traffic from the production instance and send the mirrored traffic via L2GRE or VXLAN to a GigaVUE H or GigaVUE V series node. Note third party orchestration tools are required for full automation.

GigaVUE-FM
The Gigamon Fabric Manager (FM) provides centralized orchestration and management across the entire network infrastructure, including on OpenStack, VMware, and public clouds, such as Microsoft Azure and Amazon AWS. The traffic policies can be configured using a simple drag-and-drop user interface. FM utilizes APIs to send commands and controls to the G-νTAP Modules and V Series visibility nodes.

GigaVUE V Series
Visibility nodes deployed in OpenStack to selectively aggregate, optimize, replicate and distribute traffic of interest to multiple tools located anywhere.

Giga-νTAP Controller and GigaVUE V Series Controller
For flexible deployment models, such as hybrid and multi-project deployments at scale, GigaVUE Cloud Suite leverages a controller-based architecture to proxy the command-and-control APIs while preserving existing Network Address Translation (NAT) or IP addressing schemes.

The G-νTAP Controller is used to proxy commands from GigaVUE-FM to the G-νTAP Modules.

For V Series deployments where these instance(s) reside outside the environment, such as when located on-premise or in separate cloud with no direct connection, a GigaVUE V Series Controller is required to proxy the commands from FM.
Figure 4. Architecture of GigaVUE Cloud Suite for OpenStack using G-vTAP Modules and V Series

Figure 5. Architecture of GigaVUE Cloud Suite for OpenStack using G-vTAP VM and V Series
**Key Features and Benefits**

**Traffic Acquisition**

**Giga-vTAP Module and Controller:**
- Lightweight, deployed per VM instance
- Traffic mirroring
- Traffic passed or dropped based on Layer 2–4 filtering rules
- Traffic forwarded via L2GRE or IPsec to GigaVUE H Series physical nodes or GigaVUE V Series virtual nodes
- GigaVUE-FM integrates with OpenStack APIs and provided to Giga-vTAP agents

- Minimize agent overload: Deploy one agent per OpenStack VM instance vs. one per security tool, which lowers impact on CPU utilization per instance.
- Reduce application downtime: Avoid need to redesign infrastructure to add new tool agents as applications scale out in OpenStack or as more operational tools are added.
- Scalability: Automatically scale agent as instances scale out due to demand.
- Minimize production changes: Optionally use either the production Virtual Network Interface Card (vNIC) or a separate vNIC to mirror the workload traffic. The separate vNIC option allows preservation of application traffic policies.
- Reduce costs: Forward only traffic of interest to reduce application and data egress costs.

**G-vTAP VM**:
- VM deployed as a guest VM on each hypervisor
- Receives copied packets from each of the other VMs through OVS Mirroring
- Provides basic processing including VM/port filtering, white/blacklisting and basic slicing
- Traffic forwarding via L2GRE or IPsec to physical or virtual visibility nodes
- Instantiation and configuration provided by GigaVUE-FM integration with OpenStack APIs

- Single, lightweight VM per hypervisor minimizes impact on compute nodes
- Delivers high-performance traffic throughput per instance.
- Scalability and automation: Automatically scale or move VMs as deployed workloads expand or are relocated
- No need to run special software or changes to kernel modules
- Reduces application downtime — there is no need to redesign applications when adding new tools
- Automatic Target Selection (ATS) automatically extracts traffic of interest from any workload
- Flow Mapping for Selection of Layer 2 to 4 traffic
- Reduce costs: Forward only traffic of interest to reduce application and data egress costs

*Requires the use of third party orchestration tool such as Ansible, Chef or Puppet to automate the process.*
Traffic Forwarding for Network and Security Operations

GigaVUE V Series:
• Core intelligence:
  – Receive and aggregate traffic from multiple OpenStack VM instances or agents over GRE, IPsec or VXLAN tunnels
  – Selectively filter traffic based on Layer 2–4 rules (e.g., IP addresses/subnets, TCP/UDP ports) with Flow Mapping®
  – Load-balance traffic based on Layer 2–4 criteria
• Traffic intelligence:
  – Identify and drop duplicate packets
  – Modify key content in packet headers
  – Mask specific data in packets
  – Slice off packet payload
  – Forward traffic to dedicated NIC or via L2GRE or VXLAN tunnels
• Subscriber intelligence: Sample flows with FlowVUE®
• Supports multiple tunnel options including VXLAN, L2GRE and ERSPAN
• Scale and performance:
  – Service chaining of multiple operations
  – Automatic target selection
  – Automatic scaling
• Access traffic from any application and distribute to any tool, even for different throughput rates of applications and tools
• Offload tools and improve their accuracy, and effectiveness by packet deduplication
• Optimize tools by forwarding only traffic of interest or dropping traffic not of interest
• Spread load across multiple tool instances of same type
• Pinpoint source of traffic
• Maintain regulatory compliance by obfuscating or removing sensitive and private data
• Allow tools to operate more effectively by forwarding less traffic volume and more packets
• Send reliable, unsampled network flow data to tools, such as forensics for analysis
• Increase architectural flexibility by choosing from multiple tunnel options
• Backhaul traffic to physical or virtual nodes over a LAN
• Facilitate meaningful network monitoring without monitoring every user’s or domain’s session
• Selectively reduce traffic bound to monitoring and analytic tools
• Dynamically optimize traffic based on tool needs
• Extract traffic of interest anywhere in the infrastructure being monitored
• Scale to match the number of application instances without lowering performance of visibility node
Management and Orchestration

GigaVUE-FM:
- Centralized Orchestration and Management
  - Define traffic policies using simple drag-and-drop
  - Configure traffic policies using software-defined networking constructs
  - Supports traffic orchestration through use of monitoring sessions
- Automation and integration
  - Automate visibility with OpenStack APIs
  - Integrate tools with visibility using open published REST APIs
- Topology visualization: Automatically discover and display end-to-end topology

See GigaVUE-FM data sheet for more details

*Requires Advanced Features license

- Single-pane-of-glass management, orchestration and visualization across entire infrastructure — public, private and hybrid
- Detect VM instance changes in the OpenStack project and automatically adjust the visibility tier
- Dynamically adjust traffic received or orchestrate new traffic policies
- View the visibility tier and OpenStack VM instances and agents as a topology
- Simplifies traffic orchestration
## Minimum Requirements for GigaVUE Cloud Suite Components

<table>
<thead>
<tr>
<th>SOLUTION COMPONENT</th>
<th>MINIMUM PER VM INSTANCE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>-</td>
<td>Per component choices: • Linux: RPM or Debian package • Windows: Windows Server 2008/2012/2016</td>
</tr>
<tr>
<td>G-vTAP module</td>
<td>2 x vCPU, 4GB RAM, one or more vNICs</td>
<td>vNICs (one or more): • Tunnel IP (traffic to V Series or on prem GigaVUE H Series) • Management IP + vTAP Interfaces</td>
</tr>
<tr>
<td>G-vTAP VM</td>
<td>2 x vCPU, 4GB RAM, one or more vNICs</td>
<td>vNICs (one or more): • Tunnel IP (traffic to V Series or on prem GigaVUE H Series) • Management IP + vTAP Interfaces</td>
</tr>
<tr>
<td>G-vTAP controller</td>
<td>1 x vCPU, 1GB RAM</td>
<td>Command-and-control component for the G-vTAP agents</td>
</tr>
<tr>
<td>GigaVUE V Series node</td>
<td>2 x vCPU, 8GB RAM, 2 x vNICs</td>
<td>Supports up to 500Mbps throughput: • vNIC 1: Data IP (mirrored traffic from G-vTAP) • vNIC 2: – Tunnel IP (traffic to tools or on-premises GigaVUE H Series) – Management IP (commands from the controller)</td>
</tr>
<tr>
<td>GigaVUE V Series controller</td>
<td>1 x vCPU, 1GB RAM</td>
<td>Command-and-control component for the V Series nodes</td>
</tr>
<tr>
<td>GigaVUE-FM</td>
<td>4 x vCPU, 16GB RAM, 40GB root disk</td>
<td>Fabric manager: • Needs to be able to access both the controller types for relaying the commands • Automatically spins up additional V Series nodes based on a predefined configuration in the user interface* For on-premises GigaVUE-FM requirements and ordering information, please refer to the GigaVUE-FM data sheet.</td>
</tr>
</tbody>
</table>

*Based on the number of virtual TAP points, GigaVUE V Series nodes will be auto-launched by GigaVUE-FM.
Ordering Information

GigaVUE Cloud Suite for OpenStack can be purchased as a subscription from Gigamon and pricing is based on daily total volumes of traffic processed with four tiers of traffic processed per day. If usage exceeds the selected tier by an amount over a specified percentage the customer will be automatically moved into a higher tier. Customers receive an unlimited number of G-vTAP Modules or G-vTAP VMs and V Series instances at no additional charges. Traffic throughput rates do not affect charges, only total volumes consumed. The table below lists the SKUs for procurement.

<table>
<thead>
<tr>
<th>PART NUMBER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>VBL-50T-BN-CORE</td>
<td>Volume license with up to 50 TB/day of usage with all CoreVUE apps. Monthly term license with 12-month minimum and includes Elite support.</td>
</tr>
<tr>
<td>VBL-250T-BN-CORE</td>
<td>Volume license with up to 250 TB/day of usage with all CoreVUE apps. Monthly term license with 12-month minimum and includes Elite support.</td>
</tr>
<tr>
<td>VBL-2500T-BN-CORE</td>
<td>Volume license with up to 2.5 PB/day of usage with all CoreVUE apps. Monthly term license with 12-month minimum and includes Elite support.</td>
</tr>
<tr>
<td>VBL-25KT-BN-CORE</td>
<td>Volume license with up to 25 PB/day of usage with all CoreVUE apps. Monthly term license with 12-month minimum and includes Elite support.</td>
</tr>
<tr>
<td>VBL-50T-BN-NV</td>
<td>Volume license with up to 50 TB/day of usage with all NetVUE apps. Monthly term license with 12-month minimum and includes Elite support.</td>
</tr>
<tr>
<td>VBL-250T-BN-NV</td>
<td>Volume license with up to 250 TB/day of usage with all NetVUE apps. Monthly term license with 12-month minimum and includes Elite support.</td>
</tr>
<tr>
<td>VBL-2500T-BN-NV</td>
<td>Volume license with up to 2.5 PB/day of usage with all NetVUE apps. Monthly term license with 12-month minimum and includes Elite support.</td>
</tr>
<tr>
<td>VBL-25KT-BN-NV</td>
<td>Volume license with up to 25 PB/day of usage with all NetVUE apps. Monthly term license with 12-month minimum and includes Elite support.</td>
</tr>
</tbody>
</table>

Note:

- A single OpenStack Virtual Machine Image (OVMI) could have multiple vNICs that can be tapped. For example, if an application uses ten OpenStack instances with two vNICs each, then the total virtual TAP points are 20.
- Licenses are managed and activated from GigaVUE-FM.

Support and Services


For More Information

For more information about the Gigamon Platform or to contact your local representative, please visit: [www.gigamon.com](http://www.gigamon.com).