

Power of Public Cloud Network Traffic Visibility

GigaVUE Cloud Suite for AWS is an intelligent network traffic visibility fabric that acquires, optimizes and distributes selected traffic to security and monitoring tools

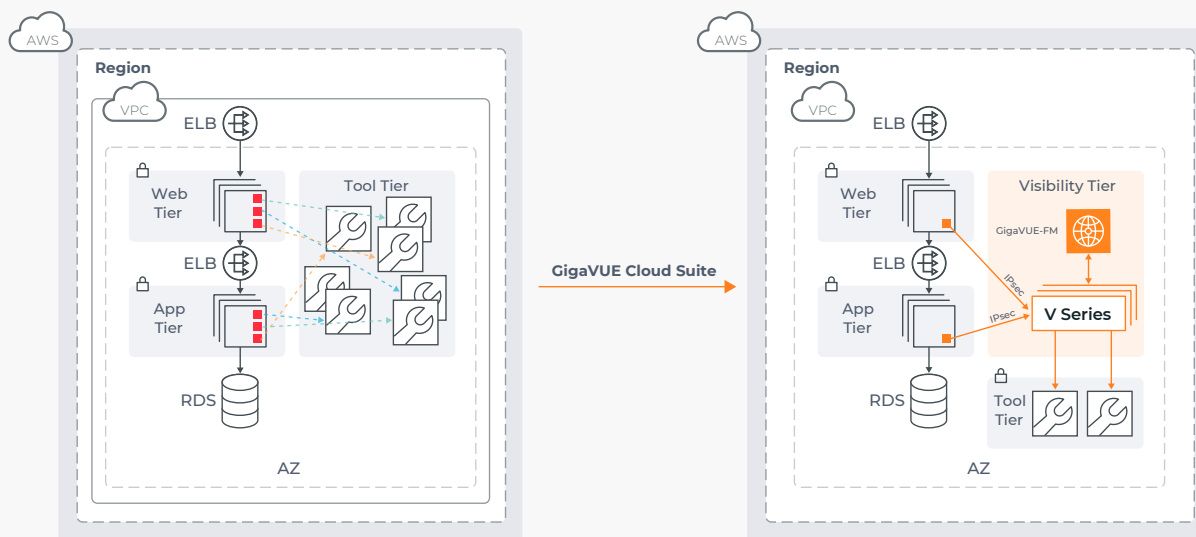


Figure 1. The suite is a cloud native platform and is fully integrated and certified within AWS environments. The solution dramatically simplifies and accelerates traffic acquisition and tool deployment.

Key Features and Benefits

- GigaSMART modules to offload tools from processor intensive tasks including packet slicing, masking and packet deduplication
- Flexible packet acquisition through either agentless AWS VPC traffic mirroring, or through GigaVUE vTAPs that add IPsec security and pre-filtering
- Automatic Target Selection® and Flow Mapping™ to extract traffic of interest anywhere in the infrastructure being monitored
- GigaVUE-FM for centralized orchestration and management of on-prem or cloud traffic with a single pane of glass interface
- Simplified and automated deployment of a dynamic visibility fabric through tight integration with AWS CloudWatch and Ansible
- 100 percent visibility into the entire AWS infrastructure and all VMs of interest
- Dynamic discovery of new workloads and appropriate routing of that new traffic to augment V Series visibility –without any manual action
- Traffic steering, service chain and tool load balancing techniques to simplify traffic distribution among multiple tools and ensure availability
- Comprehensive visibility fabric to acquire and aggregate all traffic and optimally distribute to cloud-based network monitoring and security tools
- High performance GigaSMART processing with V Series nodes that scale as needed
- Ensure visibility across interconnected VPCs and on-premise tools with AWS transit gateway support

Initiating new workloads, or migrating existing ones, into the public cloud introduces new challenges. Organizations must manage, secure and understand all the data now traversing this environment to support security detection/response, application and network performance needs. Traditionally IT had to install one agent per tool on every compute node, and direct that traffic to the tool. This quickly overloaded compute instances, increased bandwidth and forced an architecture redesign when adding new tools.

A better method is to deploy GigaVUE Cloud Suite for AWS. Gigamon helps organizations gain full workload VM visibility into east-west traffic and improve their security posture, while extending current network and application performance monitoring to AWS traffic. Using GigaVUE Cloud Suite for AWS, security architects can ensure an effective security posture in the cloud, thereby accelerating the onboarding of new AWS applications. NetOps teams can also leverage this fabric to troubleshoot degraded user experience, ensure network performance and meet SLAs.

GigaVUE Cloud Suite for AWS, as shown in figure 2, acquires traffic in two ways: Either via AWS VPC traffic mirroring instances, or with a lightweight Gigamon G-vTAP agent installed within the VMs housing Amazon EC2 instances. The Gigamon fabric integrates with Amazon EC2 APIs to discover the cloud infrastructure, deploy visibility nodes in VPCs that collect all the aggregated traffic and apply advanced traffic intelligence and applying load balancing algorithms prior to sending selected traffic to security and monitoring tools. Supports AWS transit gateways to ensure visibility across interconnected VPCs and on-premise tools. This integrated solution enables this suite to automatically remain in sync. With this solution, organizations can take advantage of:

- Increased security: Centralized visibility for security monitoring of all Amazon VPCs in an enterprise. Security operations and incident response teams can use network visibility to rapidly detect and respond to threats, vulnerabilities and compliance violations across the enterprise.
- Reduced data costs: Up to 100% traffic visibility, without increasing load on compute instances, even as new security tools are deployed. Acquire traffic once from compute instances, and leverage traffic intelligence to optimize data to any number of tools.
- Offload tools: Apply multiple GigaSMART applications including packet deduplication, slicing, masking and flow mapping to reduce the processing burden on tools.
- Operational efficiency: One common platform for visibility across the entire IT environment; consistent insight into AWS, along with other public cloud platforms and on-premises infrastructure. Acquire network traffic with minimal impact to Amazon EC2 utilization and apply traffic intelligence before distributing to multiple tools for analysis.
- Operational agility:
 - Rapidly detect changes in Amazon VPCs being monitored
 - Automatic Target Selection®: Automatically extract network traffic of interest anywhere in the infrastructure being monitored, without having to specify the target compute instances to monitor.
 - Ability to automate and orchestrate traffic visibility using open REST APIs.
- Improved performance and scalability: Packets can be processed at multi Gbps rates with the integrated DPDK support and the number of visibility nodes can be expanded to what ever levels required at no extra charge

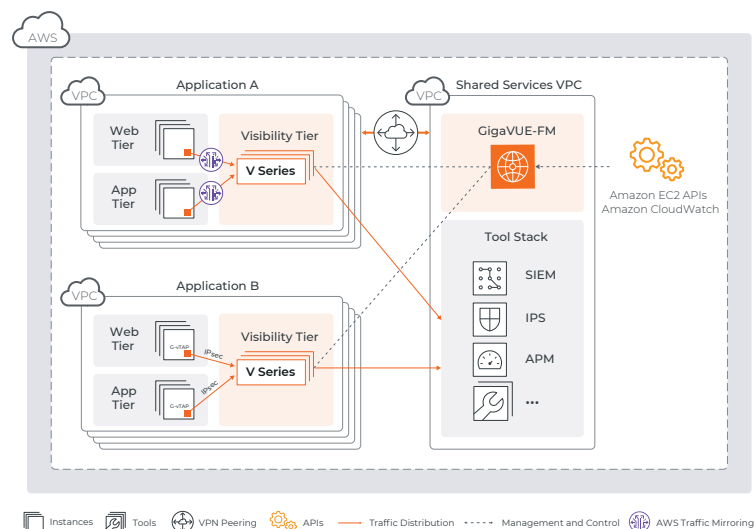


Figure 2. GigaVUE Cloud Suite for AWS supports multiple VPCs and has tight integration with AWS cloud management tools to enable automation. Either AWS's agentless native VPC traffic mirroring or Gigamon's GigaVUE lightweight G-vTAPs can collect all traffic streams.

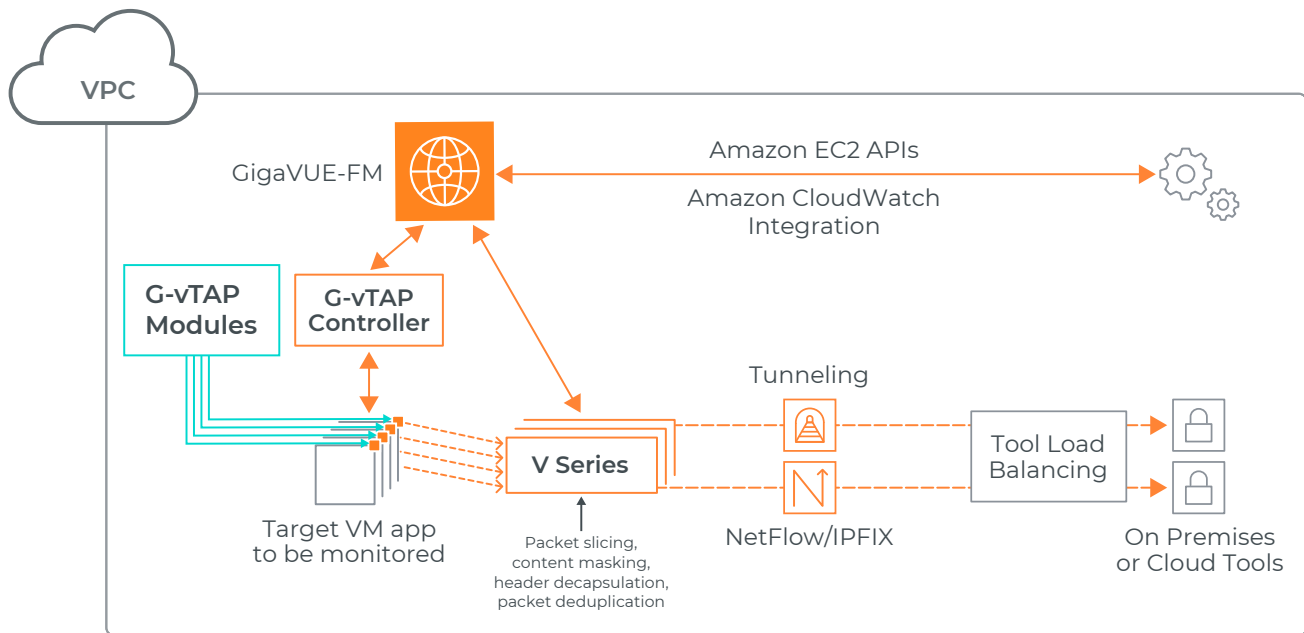


Figure 3. GigaVUE Cloud Suite for AWS is composed of four components: G-vTAP, V Series, Controller and Fabric Manager (FM)

GigaVUE Cloud Suite for AWS

The suite comprises multiple elements that enable traffic acquisition, aggregation, intelligence and distribution, along with centralized single-pane-of-glass orchestration and management.

G-vTAP Module – Lightweight agent deployed in an Amazon EC2 instance to mirror production traffic and send this traffic via IPsec to GigaVUE V Series nodes. Black- or white-listed IP addresses can be optionally pre-filtered out. These agents support a high ‘fan-out’ to send traffic to up to 25 V Series.

GigaVUE V Series – Visibility nodes in AWS aggregate and select traffic of interest, then optimize and distribute acquired traffic to multiple tools located in any VPC. V Series is based on a common architecture for multiple on-premise and cloud environments; supports multiple GigaSMART applications including packet deduplication, packet slicing, masking, flow mapping and tool load balancing. Includes DPDK for high-performance packet processing.

GigaVUE-FM – Provides centralized orchestration and management across the entire enterprise including on-premise, AWS and private clouds (OpenStack, VMware and Nutanix). The traffic policies are configured using a simple drag-and-drop user interface.

G-vTAP Controller and GigaVUE V Series Controller – For hybrid and multi-VPC deployments GigaVUE uses a controller-based design to proxy the command-and-control APIs while preserving existing IP addressing schemes or Network Address Translation (NAT). G-vTAP Controller is required and proxies commands from GigaVUE-FM to the G-vTAP Modules. See Figure 3. For those scenarios where FM does not reside in the same location, such as where it is on-premise or a separate VPC or even different cloud vendor, GigaVUE V Series Controller is used to proxy commands from GigaVUE-FM to the GigaVUE V Series nodes. If FM is deployed in the same location as the V Series, then it is not required.

Key Features and Benefits

G-vTAP Module

Lightweight agent deployed on an EC2. Mirrors traffic and sends via IPsec to GigaVUE V Series.

Minimize Agent Overload

- Requires just one agent per Amazon EC2 instance vs. needing to deploy one per security tool. This approach lowers impact on EC2 CPU utilization.

Reduce Application Downtime

- Avoid the need to redesign infrastructure to add new tool agents as applications scale out in AWS, or as more operational tools are added.

Scale What's Being Monitored

- As EC2 instances scale out due to demand, the agent automatically scales appropriately. This is achieved with the integration between GigaVUE FM, Amazon EC2 APIs and Amazon CloudWatch.

Minimize Production Changes

- Option to use either the production Elastic Network Interface (ENI) or a separate ENI to mirror the workload traffic. The separate ENI option allows IT to preserve application traffic policies.

Reduce Costs

- Pass or Drop rules to filter traffic of interest prior to sending it to the GigaVUE V Series. This reduces application and data egress costs.

GigaVUE V Series

Visibility nodes that aggregate, select, optimize and distribute traffic.

Traffic Aggregation

- Acquire and aggregate traffic from multiple EC2 instances. The traffic is acquired from the EC2 instances using IPsec and via GRE or VXLAN tunnels and support pre-filtering. Alternatively, traffic may be acquired from AWS VPS traffic mirroring instances.

Traffic Intelligence: Select, Optimize and Distribute

- Flow Mapping®: Select Layer 2-Layer 4 traffic of interest with a variety of policies and forward of to specific tools. Criteria can include IP addresses/subnets, TCP/UDP ports, protocols, instance tags etc. Advanced policies using overlapping rules and nested conditions can be specified.
- Other GigaSMART® traffic intelligence functions: Optimize selected traffic by applying applications to remove duplicated packets, slice out superfluous content, sample packet flows, and mask confidential information to reduce tool overload and maintain compliance.
- Distribute optimized traffic to multiple tools anywhere. Supports 5-tuple load balancing to tools to improve tool deployment efficiency and obviate the need for discrete load balancers.

Service Chaining

- Service chain multiple traffic intelligence operations dynamically, based on tool needs.

Elastic Scale and Performance

- Automatic Target Selection: Automatically extract traffic of interest anywhere in the infrastructure being monitored.
 - Automatically scale based on varying number of EC2s, without lowering performance of visibility node.
 - Processes at multi-Gbps rates per instance leveraging DPDK technology
-

GigaVUE-FM

Centralized management and orchestration.

Centralized Orchestration and Management

- Centralized orchestration and single-pane-of-glass visualization across entire infrastructure – public, private and hybrid.
- Traffic policies are defined using simple drag-and-drop user interface.
- Software-Defined Networking constructs are used to configure traffic policies.

Automation

- Tight integration with Amazon APIs detects EC2 changes in the Amazon VPC, and automatically adjusts the visibility tier.
- Open REST APIs published by GigaVUE-FM can be consumed by tools to dynamically adjust traffic received or to orchestrate new traffic policies.

Topology View

- Auto-discovery and end-to-end topology visualization of visibility tier and EC2 instances .

Minimum Requirements for GigaVUE Cloud Suite for AWS

Table 1: Recommended Minimum Compute Specifications

SOLUTION COMPONENT	MINIMUM EC2 INSTANCE TYPE	DESCRIPTION
G-vTAP Module	T2 medium (single or multiple ENI support)	<ul style="list-style-type: none"> • Linux: Available as an RPM or Debian package. • Windows: Available for Windows Server 2008/2012/2016
G-vTAP Controller	T2 Micro	Command-and-Control component for the G-vTAP agents
GigaVUE V Series Node	C4 large (2 ENIs)	<p>c4.large supports high performance throughput</p> <p>ENI 1: Data IP (mirrored traffic from G-vTAP)</p> <p>ENI 2: Tunnel IP (traffic to tools or on prem GigaVUE H/W)</p> <p>ENI 2: Management IP (commands from the controller)</p>
GigaVUE V Series Controller Optional	T2 micro	<p>GigaVUE-FM needs to be able to access both the controller instances for relaying the commands</p> <p>GigaVUE-FM automatically spins up additional V Series nodes based on a pre-defined configuration in the user interface</p> <p>For on-premises GigaVUE-FM requirements and ordering information, please refer to the GigaVUE-FM Data Sheet</p>
GigaVUE-FM	<p>M4 xlarge</p> <p>40GB root disk</p> <p>40GB data disk</p>	<p>GigaVUE-FM needs to be able to access both the controller instances for relaying the commands</p> <p>GigaVUE-FM automatically spins up additional V Series nodes based on a pre-defined configuration in the user interface</p> <p>For on-premises GigaVUE-FM requirements and ordering information, please refer to the GigaVUE-FM Data Sheet</p>

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

Ordering Information, Renewals

GigaVUE Cloud Suite for AWS, with all the solution components, can be consumed using the following:

- AWS Marketplace Metered – GigaVUE Cloud Suite for AWS can be purchased as a subscription from the AWS marketplace and pricing is based on daily total volumes of traffic processed. In this option, AWS meters and charges for the usage of the solution 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, Controllers and V Series instances at no additional charges. Traffic throughput rates do not affect charges, only total volumes consumed.

Table 2: Part Numbers for the Solution

PART NUMBER	DESCRIPTION
VBL-50T-BN-CORE	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
VBL-250T-BN-CORE	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
VBL-2500T-BN-CORE	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
VBL-25KT-BN-CORE	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
VBL-50T-BN-NV	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
VBL-250T-BN-NV	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
VBL-2500T-BN-NV	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
VBL-25KT-BN-NV	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

Note:

- Virtual TAP Point: Any end point from which traffic can be mirrored using the G-vTAP Module, for example, an ENI in an EC2 instance. A single Amazon Machine Image (AMI) could have multiple ENIs that can be tapped. For example, if an application uses ten EC2 instances with two ENIs each, then the total Virtual TAP Points are 20.
- Utilizes a true-forward method when usage exceeds contracted limit. The 95th percentile usage in the prior three months needs to be less than the contracted limit or the next tier pricing is applied.
- Licensing: Licenses are activated from GigaVUE-FM.
- Requires the GigaVUE operating system 5.11 and above.

Support and Services

Gigamon offers a range of support and maintenance services. For details regarding Gigamon’s Limited Warranty and its Product Support and Software Maintenance Programs, visit www.gigamon.com/support-and-services/overview-and-benefits.

Learn More

For more information on GigaVUE Cloud Suite for AWS visit this [website](#). Read the [Solution Brief](#) and requesting a [demo](#).

