GigaVUE Cloud Suite for AWS
Network Visibility into Public Clouds

aws partner network

Advanced
Technology Partner

Networking Competency
Public Sector Partner

Organizations are increasingly migrating to public cloud Infrastructure-as-a Service (IaaS) to take advantage of scale, elasticity and availability.

IaaS cloud providers operate under a shared responsibility model — the cloud provider is responsible for security of the cloud, whereas the IaaS customer is responsible for security in the cloud.

GigaVUE® Cloud Suite resides in the AWS VPCs and aggregates flows from all compute sites, including from AWS traffic mirroring nodes. This suite provides advanced high-performance traffic processing such as removing duplicate packets and optimally distributes and load balances data to the appropriate network monitoring and security tools. This helps ensure effective and comprehensive cloud security.
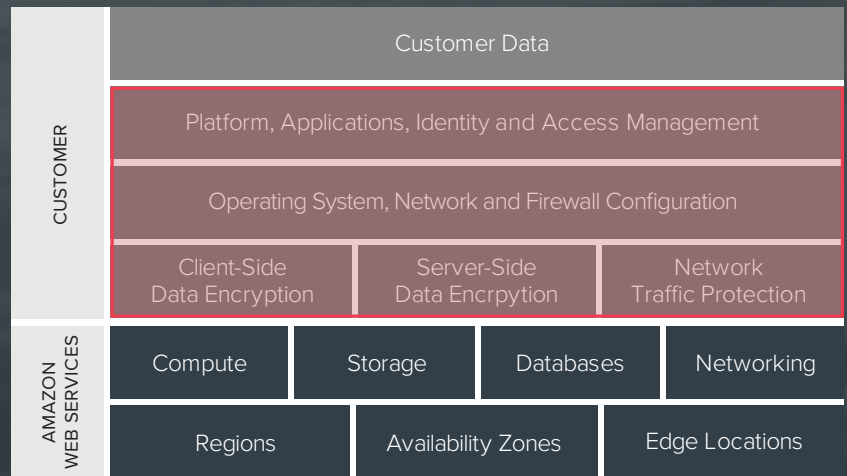
CUSTOMER	Customer Data			
	Platform, Applications, Identity and Access Management			
	Operating System, Network and Firewall Configuration			
	Client-Side Data Encryption	Server-Side Data Encrpytion	Network Traffic Protection	
AMAZON WEB SERVICES	Compute	Storage	Databases	Networking
	Regions	Availability Zones	Edge Locations	

Figure 1: Amazon Web Services (AWS) Shared Security Model

KEY FEATURES

- GigaSMART intelligence – includes packet deduplication, slicing, masking and tool load balancing

- Traffic acquisition with AWS VPC traffic mirroring or with GigaVUE vTAPs with IPsec and pre-filtering

- AWS transit gateway support

- Tight integration of GigaVUE-FM APIs with AWS CloudWatch to instantiate unlimited virtual nodes

- Centralized orchestration and management with a single-pane-of-glass GUI using GigaVUE-FM

KEY BENEFITS

- Delivery of optimized traffic to offload security and networking monitoring tools

- 100 percent visibility into your AWS infrastructure located workloads

- Ensure visibility across interconnected VPCs and on-premise tools

- Simplified and automated deployment of a dynamic visibility fabric with limitless scalability

- Discovery of new workloads, proper traffic direction and adjustment of the visibility tier, all without manual intervention
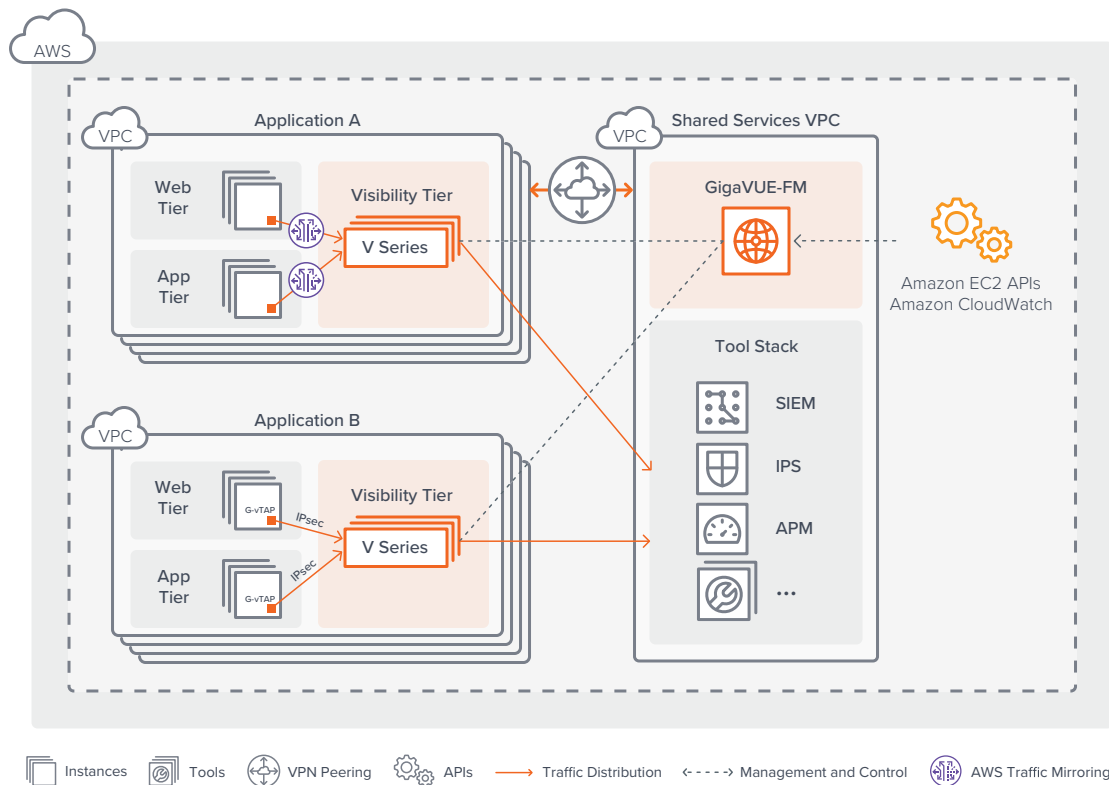
Figure 2: GigaVUE Cloud Suite for AWS

Key Considerations for IT, Cloud and Security Architects

While Amazon ensures protection from the physical data center up to the hypervisor, security and compliance of data and applications rests on IT teams, who must ensure that workloads are deployed securely and perform as required. To automatically and proactively identify and remediate security and performance limitations, accurate visibility into the AWS environment is imperative.

IT, cloud and security architects are responsible for addressing the following questions before they can successfully deploy applications in a public cloud, like AWS:

- As part of the shared responsibility model, how do I assure that AWS is being used securely by everyone in the enterprise?
- How do I run more applications on AWS while meeting the needs for applying compliance and security controls?
- What methods can be used to realize a fully automated environment that dynamically adjusts for workload relocations?
- Can the necessary traffic processing performance levels with proper scalability be assured in the cloud?
- As applications are moved from on-premise to the cloud, can the same traffic processing be applied including payload masking, packet deduplication and tool load balancing?
- Are there effective methods to reduce the cost of backhauling traffic when the tools monitoring traffic in the cloud are on-premises vs. part of a tool tier is in the cloud?

Not addressing these considerations slows down the migration of applications to the cloud, and leaves the organization vulnerable to potential security breaches, with potential impact to reputation and brand.

THE SOLUTION

Gigamon CloudVUE Cloud Suite for AWS delivers automated intelligent network traffic visibility for dynamic workloads running in AWS and enables increased security, operational efficiency and high-performance processing across VPCs. Organizations can optimize costs with up to 100 percent visibility for security without increasing load on compute instances as more security tools are deployed.

Figure 3: Centralized management, automation and straightforward process with AWS and Gigamon Fabric Manager

GigaVUE G-vTAPs

For traffic acquisition, lightweight G-vTAPs are deployed within EC2 instances that mirror traffic to the V Series. Key benefits include:

· Single, lightweight instance minimizes impact on compute nodes

· Reduction in application downtime — there is no need to redesign applications when adding new tools

· Agent filters traffic of interest prior to sending it via IPSec to the GigaVUE V Series to reduce application and data egress costs

GigaVUE V Series Nodes

Traffic aggregation, intelligent high-performance packet processing and distribution occurs within the GigaVUE V Series nodes, which are deployed within the visibility tier (see figure 2). Key benefits include:

· Automatic Target Selection (ATS): Automatically extract traffic from any workload with an agent deployed without explicitly specifying VPCs

· Flow Mapping®: Selection of L2 – 4 traffic

· GigaSMART® intelligence: Packet deduplication, slicing, sample and masking combined with load balancing to optimize traffic sent to tools, reducing tool overload

· Fully interoperable with native AWS VPC traffic mirroring

GigaVUE-FM (Fabric Manager)

Centralized orchestration and management are done by GigaVUE-FM. Tight coupling with Ansible and AWS CloudWatch automatically instantiates, configures and monitors G-vTAP and V Series instances and supports dynamic workload migrations.

· Detect EC2 changes in a VPC and automatically adjust the visibility tier, through pre-built integration with AWS APIs

· Publish REST APIs: Integrate with AWS CloudWatch and third-party systems and tools to dynamically adjust traffic received or to orchestrate new traffic policies

· Auto-discover and visualize end-to-end network topology, including VPC workloads by using an intuitive drag-and-drop user interface

· Eliminate manual processes and errors by automatically identifying each new workload and their associated traffic mirroring via ATS, and then configuring the traffic mirroring to direct traffic to the V Series Nodes

Conclusion

Whether your organization is already using AWS or considering a future migration, GigaVUE Cloud Suite for AWS provides intelligent network traffic visibility for workloads running in the cloud. Integration with AWS APIs automatically deploys a visibility tier in all VPCs, collects aggregated traffic and applies advanced packet processing prior to sending selected traffic to existing security tools. With GigaVUE, organizations can obtain consistent insight into their infrastructure across AWS and their on-premises environment.

For more information on GigaVUE Cloud Suite for AWS, please read the data sheet. Learn more at www.gigamon.com/aws.