Gigamon

Product Brief
Gigamon Visibility Platform for AWS

Introduction

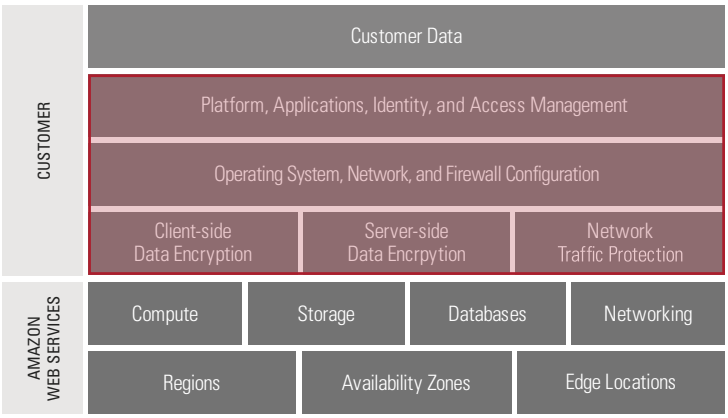
Enterprises are increasingly migrating to public cloud Infrastructure-as-a-service (IaaS) to take advantage of scale, elasticity and availability. To deploy an effective and secure public cloud IaaS strategy, cloud architects and enterprise decision makers need to recognize the security responsibility of the enterprise.

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. Based on this model, security and compliance of data and applications rests on IT, cloud, and security teams, who must ensure that applications and workloads are deployed securely by everyone within the organization. To identify early signs of security anomalies and deviations from expected behavior, accurate visibility into public cloud IaaS network traffic is imperative when implementing an effective multi-tiered security model.

Key Considerations for IT, Cloud and Security Architects

IT, cloud and security architects are responsible for addressing the following questions before they can successfully deploy mission-critical applications in a public cloud, such as Amazon Web Services (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 mission-critical applications on AWS while meeting the needs for applying compliance and security controls?
- If zero-day security vulnerabilities are exploited in software that is yet to be patched, what backstops do I have to detect them?
- How do I detect and respond to security or network anomalies while deploying applications on AWS?
- Are there efficient ways to consolidate network traffic flows to security and monitoring tools?
- 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 in the cloud?



Amazon Web Services Shared Security Model

Failure to address these considerations slows down the migration of mission-critical applications to the cloud and leaves an organization vulnerable to potential security breaches, with severe consequences to reputation and brand.

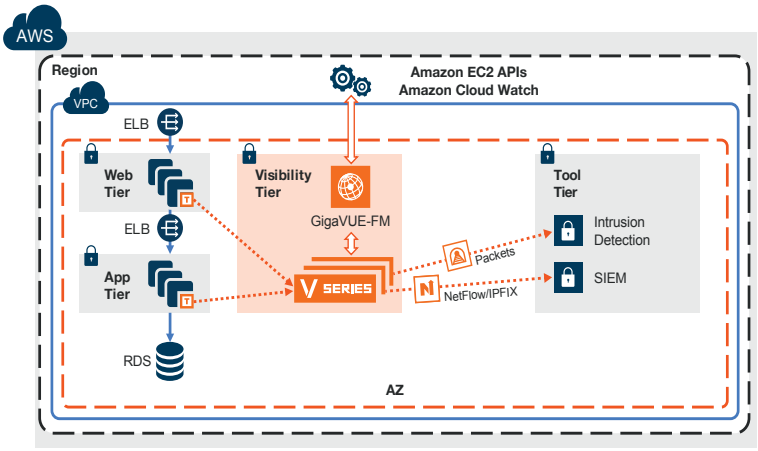
The Solution

The Gigamon Visibility Platform for AWS delivers intelligent network traffic visibility for workloads running in AWS and enables increased security, operational efficiency and scale across Virtual Private Clouds (VPCs). With this solution, organizations can:

- Optimize costs with up to 100% visibility for security without increasing load on compute instances as more security tools are deployed[2]
- Leverage GigaSMART® traffic intelligence to deliver optimized traffic to the right tool, up to 99% reduction in traffic with NetFlow/IPFIX generation[2]

The solution consists of three key components:

- Traffic acquisition using G-vTAP agents
- Traffic aggregation, intelligence and distribution using GigaVUE V Series
- Centralized orchestration and management using GigaVUE-FM



For traffic acquisition, G-vTAP agents, are deployed on EC2 instances that mirror traffic to the V Series.

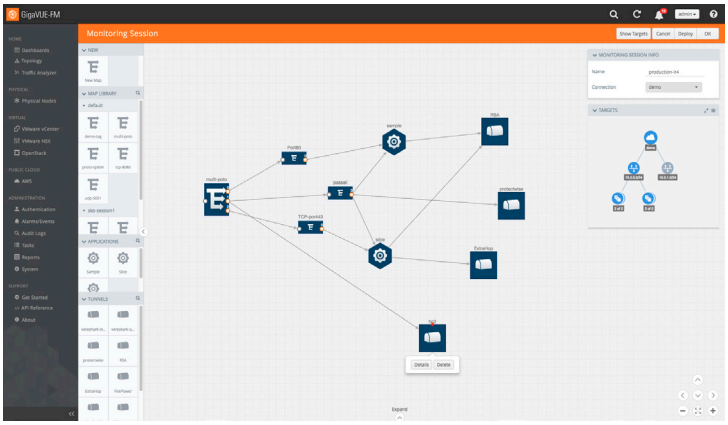
Key benefits include:

- Minimized impact of agent overload
- Reduction in application downtime: there is no need to redesign applications when adding new tools

Traffic aggregation, intelligence and distribution occurs within the GigaVUE V Series visibility nodes, which are deployed within the visibility tier (see figure above).

Key benefits include:

- Automatic Target Selection: automatically extract traffic of interest anywhere without explicitly specifying target VPCs.
- Flow Mapping®: selection of Layer 2 through Layer 4 traffic of interest.
- NetFlow/IPFIX generation: create flow records from network traffic to determine IP source, destination of traffic, etc.
- Header Transformation: modify content in the header (L2-L4) to ensure security and segregation of sensitive information.
- GigaSMART® intelligence: slice, sample and mask packets to optimize traffic sent to tools, reducing tool overload.



Centralized orchestration and management of the Visibility Platform is done by GigaVUE-FM. This single pane of glass creates visibility policies for workloads within AWS.

Key benefits include:

- Tight integration with AWS APIs: detect EC2 changes in a VPC and automatically adjust the Visibility Tier.
- Publish REST APIs: integrate with third-party systems and tools to dynamically adjust traffic received or to orchestrate new traffic policies.
- Drag-and-drop intuitive user interface: auto discover and visualize the end-to-end topology.

Conclusion

Whether your organization is already using AWS or considering a future migration, the Gigamon Visibility Platform provides intelligent network traffic visibility for mission critical workloads. Integration with AWS APIs automatically deploys a visibility tier in all VPCs, collects aggregated traffic, and applies advanced intelligence prior to sending selected traffic to existing security tools. With this platform, organizations can obtain consistent visibility into their infrastructure across AWS and their on-premises environment.

For more information on the Visibility Platform for AWS: Please read the **data sheet**. Learn more at **www.gigamon.com/aws**

[2] *Based on Gigamon internal analysis, November 2017*

2039-03 12/17

Gigamon® 3300 Olcott Street, Santa Clara, CA 95054 USA | +1 (408) 831-4000 | www.gigamon.com