Gigamon

amazon web services | Partner Network
ADVANCED TECHNOLOGY PARTNER
AUTHORIZED PUBLIC SECTOR PARTNER

Solution Overview
Gigamon Visibility Platform for AWS

Background

With the rapid evolution of the public cloud that brings instant advantages of economies of scale, elasticity and agility, IT and data center administrators are re-evaluating their investments to deploy or scale applications on-premise. They either deploy newer applications in the public cloud or use the public cloud for bursty needs to augment the on-premise private cloud. In either case, what enterprises end up with is a hybrid cloud environment. Other enterprises start in the cloud with no physical data center footprint, commonly referred to as a born-in-the-cloud model. Unlike Software-as-a-Service (SaaS) environments, in which application ownership and security of information is the responsibility of the SaaS provider, an Infrastructure-as-a-Service (IaaS), or public cloud environment, places the responsibility of application and information security on the enterprise.

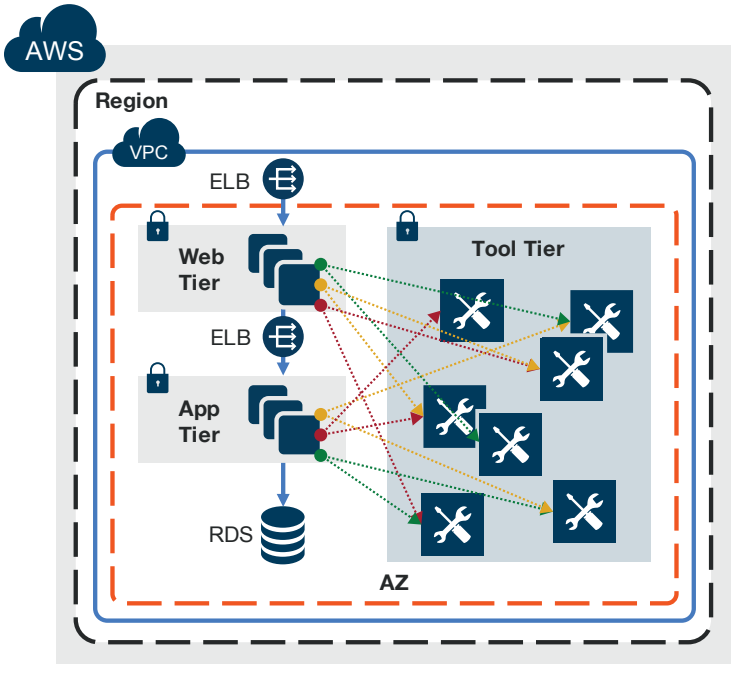
Challenges

How does an enterprise which has migrated or deployed workloads into the public cloud now manage, secure and understand its data traversing the public cloud? The obvious challenges are as follows:

- Inability to access traffic, and by extension, information traversing the public cloud, for analysis
- Deep packet inspection for forensics, advanced threat detection, etc.
- Analysis of North-South [elastic load balancer (ELB) to web tier] and East-West [web tier to app tier or app tier to database] traffic for compliancy, lateral propagation of threats, etc.
- Lack of sufficient tools in the public cloud. While a plethora of security analysis and IT monitoring tools exist for on-premise deployments, many of these tools do not have an equivalent offering in the public cloud
- Increased and varied backhaul costs from the IaaS provider to an enterprise, should an enterprise choose to backhaul traffic from the public cloud infrastructure to the enterprise location where the tools are located

In an on-premise deployment, there are options to get access to traffic from the infrastructure for real-time analysis: TAPs (physical or virtual), SPAN sessions—although TAPs are the favored method to gain reliable, non-intrusive access to mission-critical data in motion—or a network visibility solution can be used. When deploying applications in the public cloud, none of these options are available.

Agent-based monitoring is an option, but that could lead to a very complex architecture, especially if you have multiple tools that need access to the same traffic for inspection and analysis, as depicted below.



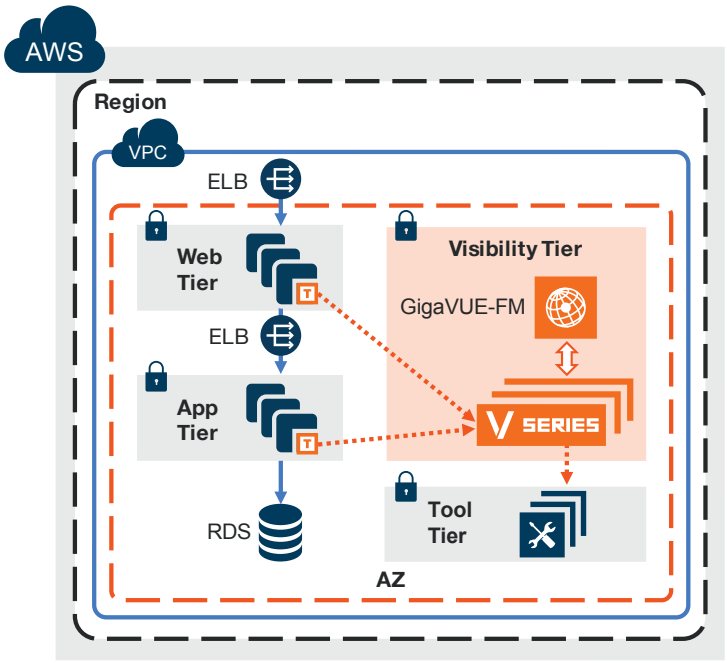
IaaS Visibility Challenges

- Inability to access all traffic
- Discreet vendor monitoring agents per instance
- Impacts workload and VPC performance
- Increases complexity
- Static visibility with heavy disruption

Gigamon Solution

An efficient and optimal solution to overcome these challenges is to use the Gigamon Visibility Platform for AWS, the industry's first pervasive Visibility Platform that provides consistent visibility into data in motion across the entire enterprise: on-premise, remote sites, public, private, and hybrid clouds.

Create a comprehensive visibility tier on an AWS VPC, with one consistent way to access, categorize and consolidate the delivery of network traffic to out-of-band security and performance management tools.



Gigamon Visibility Platform for the Public Cloud

- Provides a consistent way to access network traffic within and across VPCs
- Distributes traffic effectively to multiple tools
- Customizes network traffic to specific tools using policies
- Delivers elastic, on-demand visibility as workloads scale out

Extending the Solution to the Hybrid Cloud and Multi-VPC Deployments

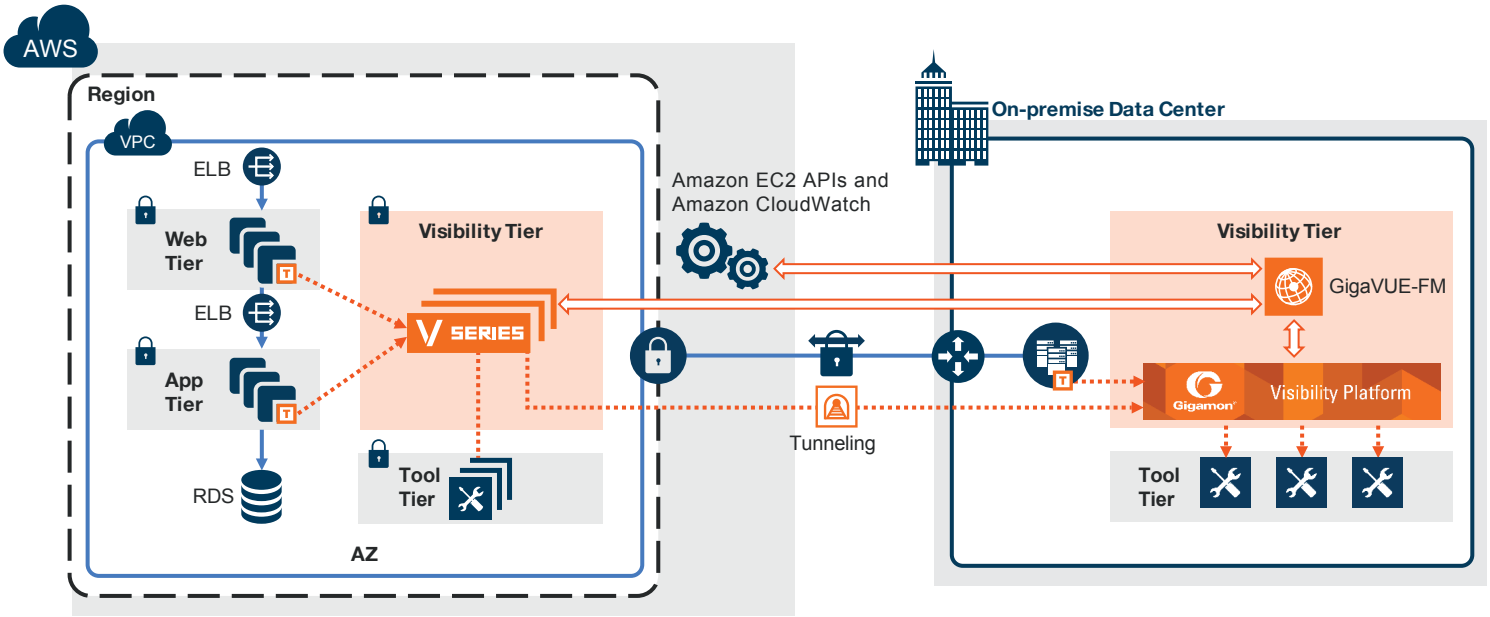
Gigamon's Visibility Platform extends its capabilities to the following real-world, flexible deployment models:

1. Hybrid clouds for large enterprises—providing on-premise visibility, while preserving tool investment.
2. Scale-out public cloud model with multiple VPCs for applications, business units, or tenants.
3. Enterprises with an all-in approach and have migrated and deployed all their applications to the cloud.

Use Case #1: Hybrid Cloud for Large Enterprises

In this use case, an enterprise's on-premise Gigamon Visibility Platform can be extended to the cloud by:

- Integrating with AWS APIs to identify inventory of the EC2 instances, the network configuration, etc.
- Selectively accessing EC2 instance traffic using G-vTAP
- Aggregating and applying traffic intelligence using a service-chained set of GigaVUE V Series nodes
- Optimizing the aggregated traffic by slicing to conserve network backhaul
- Masking the traffic before the backhaul can provide privacy and compliance
- Tunneling the aggregated and optimized traffic to on-premise over existing backhaul connections

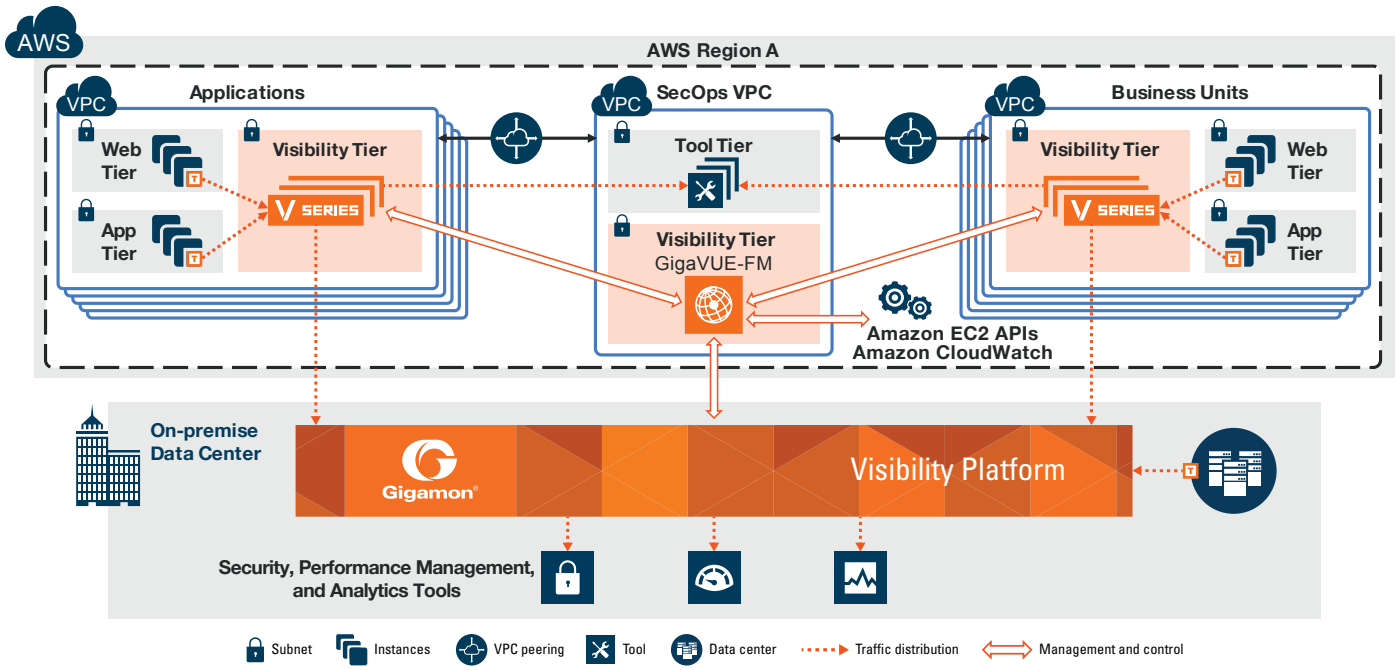


Use Cases #2 & #3: Centralized Visibility for Multi-VPC Deployments (i.e. All-in Cloud Enterprise)

In this combined use case:

- A centralized VPC managed by the SecOps team can be used for security or analytics, removing a need for each VPC to host a separate tool tier
- Enterprises can utilize AWS VPC Peering to save network costs for central traffic inspection and analysis
- Reduces tool proliferation while allowing for effective, centralized visibility for an all-in-the cloud enterprise

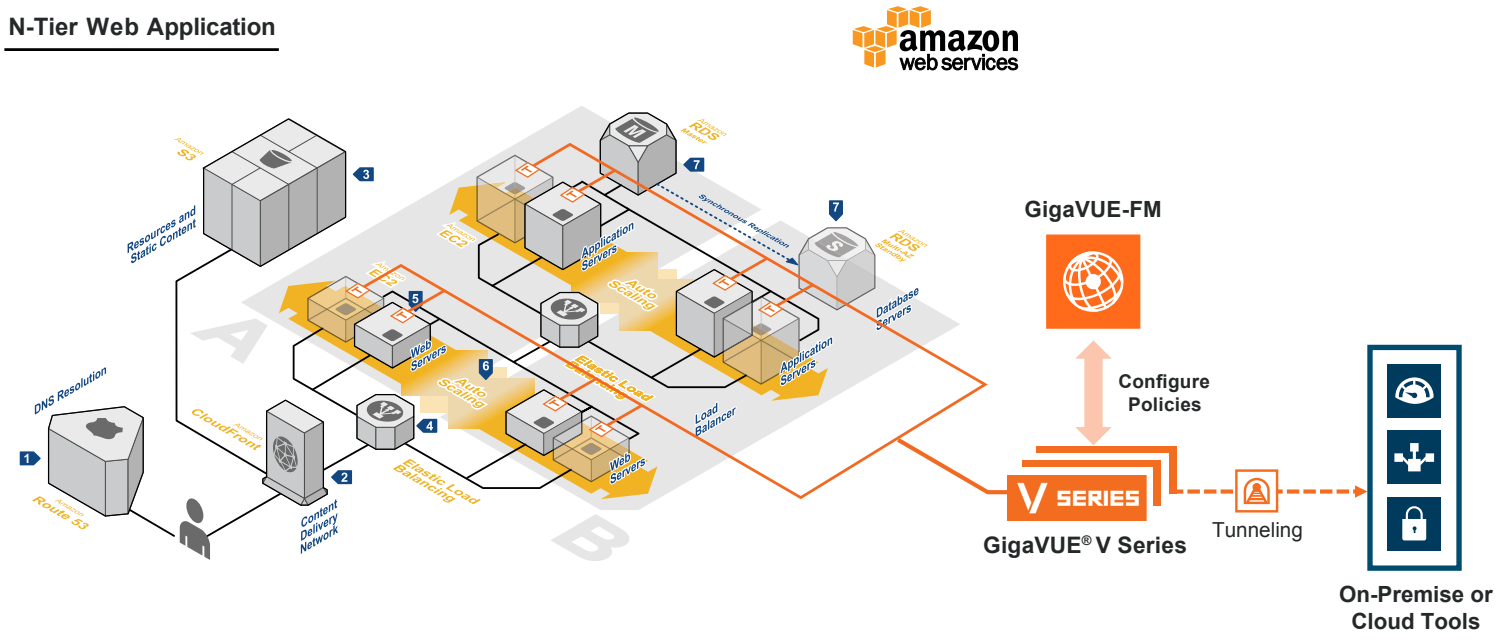
With support for these flexible deployment models, the Gigamon Visibility Platform for AWS provides pervasive visibility into data in motion across the entire enterprise: on-premise, remote sites, public, private, and hybrid clouds.



Features and Benefits

Features	Benefits
Traffic Access (G-vTAP™ Agent)	• A user space agent deployed in the elastic compute cloud (EC2) instance to mirror selected traffic and deliver to GigaVUE® V Series visibility nodes • Single agent that can replace multiple vendor agents to consistently access and forward traffic
Traffic Aggregation and Intelligence (GigaVUE V Series)	• Visibility node [available as an Amazon Machine Image (AMI)] that aggregates traffic from multiple agents • Applies intelligence and optimization to the aggregated traffic – Flow Mapping®—select and filter traffic – Slicing—reduce packet size at a specified offset to conserve network backhaul – Sampling—conserve network backhaul by selecting packet rates, for ex. 1 in 10 or 1 in 100 – Masking—can provide compliancy and privacy of the traffic by masking specific offsets • Distributes optimized traffic to cloud-based tools or backhaul to on-premise Gigamon Visibility Platform using standard IP GRE Tunnels
Orchestration (GigaVUE-FM)	• Centralized management application can be deployed either on-premise or in the cloud • Defines traffic policies using simple drag-n-drop UI • Integrates with AWS APIs for EC2 inventory and network topology • Monitors Amazon CloudWatch events to identify EC2 instance spin-up
Elastic and Automated Visibility (Automatic Target Selection)	• Elastically scales-out GigaVUE V Series nodes based on traffic access points • Automatically selects new EC2 instances as part of traffic policies • Allows for continuous and automated visibility while identifying any lateral propagation of threats

AWS Reference Architecture Example with the Gigamon Visibility Platform



3213-02 03/17

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