PRODUCT BRIEF

GigaSECURE Cloud

For Microsoft Azure

Features and Benefits

- GigaSMART® intelligence: slice, sample and mask packets to optimize traffic sent to tools, reducing tool overload
- Single, lightweight agent minimizes impact on compute instance
- Reduction in application downtime: there is no need to redesign applications when adding new tools
- Tight integration with Azure APIs: detect VM changes in a VNet 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 network topology

Introduction

As enterprises move to the public cloud to take advantage of scale, elasticity, and availability, cloud architects and enterprise decision makers need to recognize the security expectations on the enterprise. Specifically, infrastructure-as-a-service (IaaS) cloud providers operate under a "Shared Responsibility" model – the cloud provider is responsible for security of the cloud, i.e. of the cloud infrastructure whereas the IaaS customer is responsible for security in the cloud, i.e. of the data and applications.

Based on the Shared Responsibility model, security of the data and applications, along with organizational/regulatory compliance, rests on IT/cloud and security architects, who must ensure that applications and workloads are being deployed securely by everyone within the organization. Enterprises who migrate to the cloud typically rely on techniques like workload security, perimeter security, prevention-only solutions, and reliance on identity and access management to mitigate security risks. Today's threat landscape means that prevention only security techniques are insufficient; they need to be complemented with additional detection and response techniques to detect early signs of security anomalies and deviations from expected behavior. For this to happen, organizations need to have accurate network traffic visibility into physical, virtual and cloud network traffic to implement a multi-tiered security model.

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	■	■	■	■
Client & end-point protection	■	■	■	◩
Identity & access management	■	■	◩	◩
Application level controls	■	■	◩	□
Network controls	■	◩	□	□
Host infrastructure	■	◩	□	□
Physical security	■	□	□	□

■ Cloud Customer □ Cloud Provider

Source: Shared responsibilities for different cloud service models.," from document: Shared Responsibilities for Cloud Computing, Microsoft, p. 5. Retrieved September 22, 2017, from http://aka.ms/sharedresponsibility. Copyright 2017.

Key Considerations for IT/Cloud and Security Architects

IT/Cloud and security architects responsible for charting a cloud strategy for their enterprise must address the following questions before they can successfully deploy applications in an IaaS public cloud such as Microsoft Azure:

- As part of the shared responsibility model, how do we assure that Azure is being used securely by everyone in our enterprise?
- How do we run more applications on Azure 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 mechanisms do we have in place to detect them?
- How do we detect and respond to security or network anomalies while deploying applications on Azure?
- How do we extend our enterprise security posture to workloads running in Azure?
- What methods do we have to detect deviations from organization's cloud usage policy in real-time?

Failure to comprehensively address these considerations prevents or slows down the migration of applications to the cloud, and leaves an organization vulnerable to potential security breaches, with adverse consequences to reputation and brand. Thus, a well- defined cloud security architecture that accelerates application migration to the cloud is essential.

The Solution

GigaSECURE Cloud delivers intelligent network traffic visibility for workloads running in Azure and enables increased security, operational efficiency and scale across Virtual Networks (VNets). 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[1]
- Leverage GigaSMART® traffic intelligence to deliver optimized traffic to the right tool, with up to 99% reduction in traffic with NetFlow/IPFIX generation[1]

The solution consists of three key components:

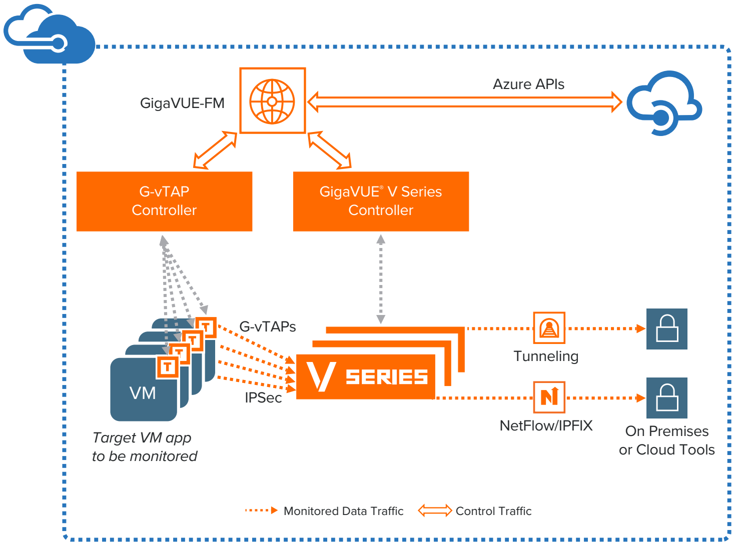
- Traffic acquisition using G-vTAP agents
- Traffic aggregation, intelligence and distribution using GigaVUE® V Series
- Orchestration and management using GigaVUE-FM

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

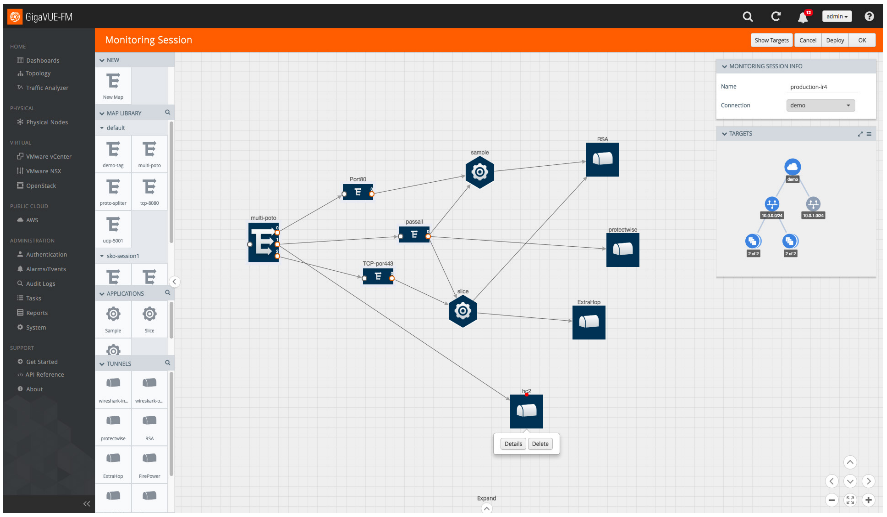
Key benefits include:

- Single, lightweight agent minimizes impact on compute instance
- 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

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



[1] Based on Gigamon internal analysis, November 2017



Name: production-lr4
Connection: demo

Key benefits include:

- Automatic Target Selection: automatically extract traffic of interest from any workload with an agent deployed without explicitly specifying target VNets
- 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 is done by GigaVUE-FM. This single pane of glass creates policies for workloads within Azure.

Key benefits include:

- Tight integration with Azure APIs: detect VM changes in a VNet 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 network topology

Conclusion

Whether already in Azure or considering a future migration to Azure, GigaSECURE Cloud provides intelligent network traffic visibility for mission critical workloads. Enterprises can obtain complete network traffic visibility into virtual machines, an essential requirement for building multi-tiered security stacks. GigaSECURE Cloud integrates with Azure APIs and deploys a visibility tier in VNet that collects aggregated traffic and applies advanced intelligence prior to sending selected traffic to security tools.

With GigaSECURE Cloud, organizations can obtain consistent visibility into their infrastructure across both Azure and their on-premises environment and extend their security posture to Azure.

To learn more visit www.gigamon.com/azure.

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