SOLUTION BRIEF

Fortinet Multidimensional Cloud Workload Protection

Executive Summary

Both applications being developed in the cloud (DevOps) and those being migrated to the cloud must be protected from traditional threats that originate on the public internet as well as new threats that propagate across workloads. Threats also include those that are introduced through cloud management user interface (UI) application programming interfaces (APIs). Fortinet offers multidimensional cloud workload protection for the public cloud by offering solutions—powered by FortiGate VM and FortiClient—that address in-line protection for north-south traffic and host-based protection for east-west traffic. FortiCASB-Cloud enables organizations to protect cloud UIs and APIs by securing unwanted and unsupervised configurations at the cloud account level.

Key Benefits:

- Centralized security policy management for IaaS, at the network level, and at the API level
- Aggregated data visible through single pane of glass using FortiAnalyzer
- Consistent compliance visibility with FortiCASB-Cloud
- Centralized security management visibility across public clouds

Securing Public Cloud Workloads

The public cloud shared responsibility model dictates that cloud providers secure the infrastructure, while customers protect the data and applications they put in that infrastructure. This means that customers are also responsible for correct configuration of cloud services and preventing any abuse of cloud APIs.

With the threat landscape forever more relentless and sophisticated, securing the expanded cloud attack surface is an ongoing challenge. The vast amounts of data stored in public clouds also make them prime targets for hackers. Deploying a reliable next-generation firewall (NGFW) virtual machine (VM) to keep internet-borne threats out of the cloud virtual network is necessary. But this north-south traffic protection is not enough to secure cloud workloads in today's advanced threat environment.

In addition to the above, it is critical to ensure security controls are working and that no security gaps exist. Server-level internal security policy compliance must be maintained to protect east-west traffic. In instances where nefarious activity is detected, real-time alerts to security staff and/or automated responses by the NGFW must occur before damage is done.

Protecting Against Misconfigurations

One of the primary causes of cloud security breaches is misconfigurations. Due to the dynamic nature of DevOps and ongoing application life-cycle management in the cloud, misconfiguration is bound to occur—whether mishaps by DevOps or security staff or the importation of erroneous code. The upside is that misconfigurations can be prevented with continuous configuration monitoring powered by FortiCASB-Cloud.

Fortinet addresses the challenges of cloud workload protection by:

- Stopping internet-borne threats at the perimeter with FortiGate VM
- Ensuring cloud workloads comply with internal security policies with FortiClient
- Avoiding security breaches caused by preventable misconfiguration using FortiCASB-Cloud

Fortinet Multidimensional Cloud Security

Fortinet cloud workload protection provides in-line protection for north-south traffic, host-based protection for east-west traffic, and protection for cloud API and configuration-related risks. Three Fortinet products comprise the integrated, unified, and centrally managed offering:

At the network level. **FortiGate VM** protects cloud virtual networks from internet-originated threats as well as provides inter-cloud secure connectivity. Among other capabilities, FortiGate VM includes antivirus, intrusion prevention (IPS), and application control. Secure IPsec VPN safeguards migration from on-premises data center and private clouds to the public cloud. It also facilitates and protects inter-cloud communications. For threat protection, real-time updates from FortiGuard Labs enable organizations to proactively address advanced threats.

FortiClient software extends security on cloud workloads by securing east-west traffic communications and ensuring servers and systems comply with security policies. It delivers telemetry and compliance for cloud servers and operating systems. When a VM is found to be in noncompliance with security policies or regulations, FortiClient alerts the FortiGate VM so that security policy updates or remediation can be automatically triggered. Additional east-west traffic protections are possible using Fabric-Ready Partner solutions such as those from Tufin and Alcide, which provide east-west protection for emerging technologies like containers and serverless architectures.

At the API level. **FortiCASB-Cloud** is a cloud-based service that accesses the Infrastructure-as-a-Service (IaaS) management APIs to enable visibility into cloud resource usage and control over configurations. It secures from unwanted and unsupervised configurations at the cloud account level. With continuous monitoring across all public cloud environments (Amazon Web Services, Microsoft Azure, Google Cloud Platform), it identifies risks associated with the unsecure provisioning and configuration of public cloud resources. It also offers visibility into APIs to manage and protect them.

Secure Multiple Cloud Dimensions

By combining a powerful NGFW with server-level policy compliance checks and continuous configuration monitoring, organizations can protect cloud workloads across three dimensions. FortiGate VM, FortiClient, and FortiCASB-Cloud work together to close security gaps and offer greater efficiency with centralized management and visibility. In addition, FortiGate VM includes IPsec VPN to secure traffic between clouds, between users and clouds, and between on-premises data centers and clouds.

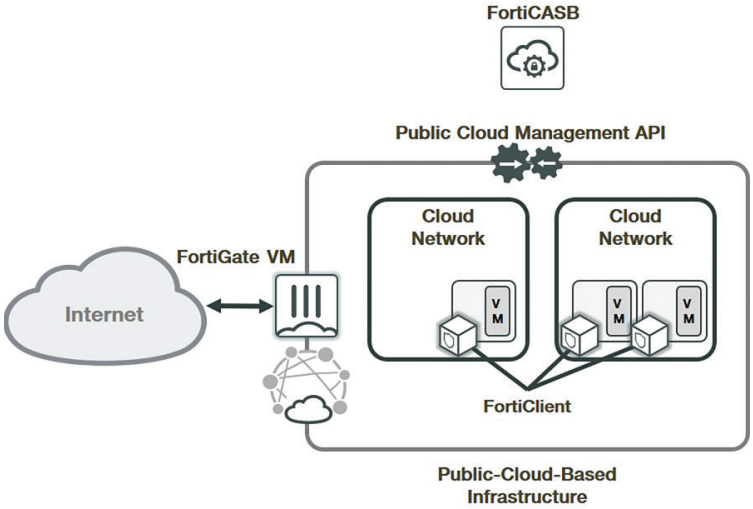

Figure 1. The combination of FortiGate VM, FortiClient, and FortiCASB-Cloud delivers multidimensional workload protection for public clouds.

August 1, 2019 10:55 AM

357731-0-0-EN

C:\Users\cyan\Documents\Creative Services - Misc\Document Edits\SB - Cloud Workload Protection\sb-multidimensional-cloud-workload-protection Folder\sb-multidimensional-cloud-workload-protection