EXTENDING ADVANCED SECURITY FOR GOOGLE CLOUD PLATFORM

Google Cloud Platform (GCP) was designed with security as a core design component. Google uses a variety of technologies and processes to secure information stored on Google servers. Like other public cloud platforms, Google offers customers a great deal of basic security control over their instances running on Google's infrastructure. However, general cloud Infrastructure-as-a-Service (IaaS) does not control security on the operating system, packages, all network connections, inbound and outbound traffic, or applications that are deployed by customers on GCP. It is the customer's responsibility to comply with its own regulation compliance requirements.

FortiGate for Google Cloud Platform extends the consistent and best-in-class enterprise security to secure connectivity for business workload between the on-premises data center and the cloud environment. Business needs seamless security orchestration that scales along with cloud workloads. FortiGate complements native GCP security functions with advanced threat protection.

COMPLEMENTS BASE GCP SECURITY

FortiGate safeguards Google Cloud Platform so developers can deploy the cloud application and data with enterprise grade of next-generation firewall, VPN, IPS, antivirus, etc., beyond the base GCP VPN.

SINGLE PANE OF SECURITY VISIBILITY OF PUBLIC AND HYBRID CLOUDS

FortiGate next-generation firewall along with FortiManager delivers consistent cross-site policy management and visibility in the multicloud infrastructures.

PCI COMPLIANCE-READY SOLUTION

The public cloud adapts the shared responsibility model regardless of which public cloud option you choose. FortiGate's open APIs and consolidated log analytics enable out-of-box PCI compliance reports. Organizations can also bring all log streams into GCP for a more effective threat prevention.

SOLUTION BENEFITS

- Maintains consistent security posture in shared responsibility model from on-premises to the cloud

- Comprehensive advanced security and threat prevention for Google Cloud Platform

- Continuous control and visibility through single pane of policy management

- Mitigates concentration of end-to-end data and risk in consolidated environments within and across clouds

F#RTINET
Fabric-Ready

FORTIGATE ON GOOGLE CLOUD PLATFORM

With Google Cloud Platform VPC, you can provision your GCP resources geographically, connect them to each other, and isolate them from one another in a virtual private cloud (VPC). You can also define or segment fine-grained networking policies within GCP and between GCP and on-premises or other public clouds.

FortiGate virtual firewall is deployed to segment your networks and restrict access to virtual instances. The key FortiGate deployment cases for GCP include:

- Site-to-site VPN
- Firewall high availability
- Multilayered security among VPCs
- Hybrid cloud
- Centralized management with combining use with FortiManager

MULTI-LAYERED SECURITY

HYBRID CLOUD
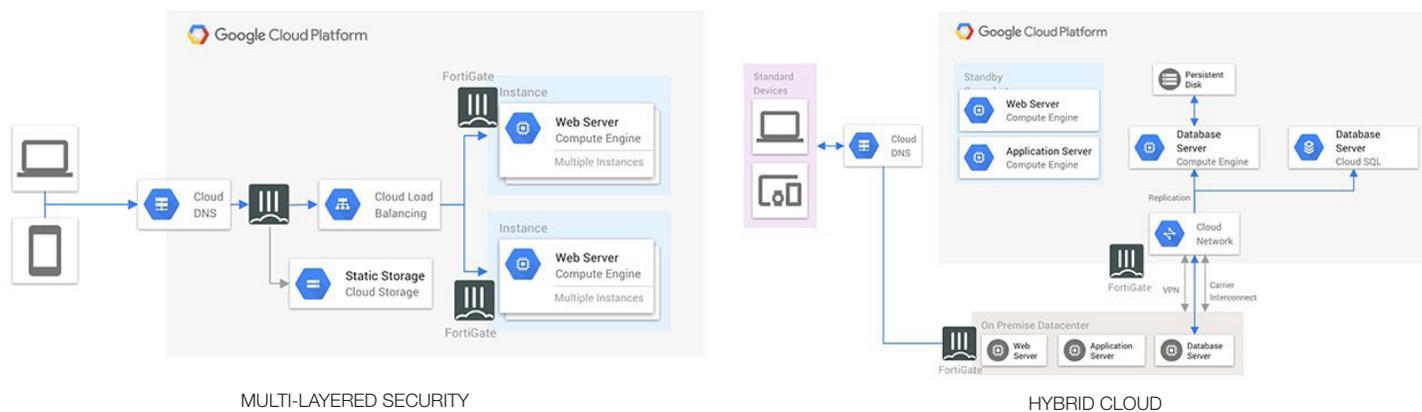
BYOL LICENSING

FortiGate is available in Google Cloud Platform cloud launcher with a bring-your-own-license (BYOL) supporting standard and new V series virtualized instances from VM01/v to VM32/v for both VDOM/non-VDOM configuration.

F⊡RTINET.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

170609-0-A-EN   May 18, 2018 3:15 PM

Mac:Users:susiehwang:Desktop:Susie Projects:2018:SB-Extended-Advanced-Seuicrty-Google:sb-extended-advanced-security-google-platform