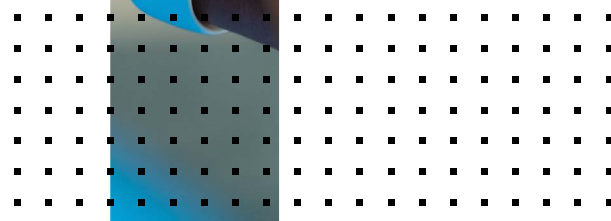
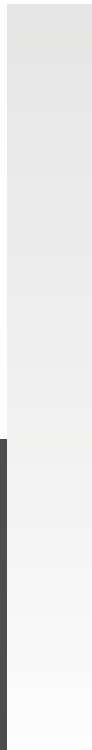
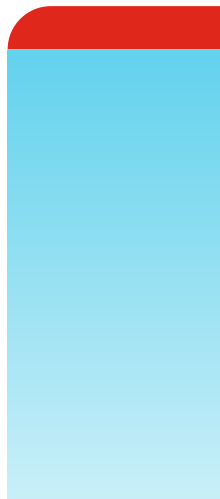


QUICK START DEPLOYMENT GUIDE

# Fortinet Security Solutions for Google Cloud

FortiGate-VM, FortiWeb, FortiManager,  
FortiADC and FortiAnalyzer



# Table of Contents

Fortinet Security Solutions for Google Cloud . . . . .	1
FortiGate-VM, FortiWeb, FortiManager, FortiADC and FortiAnalyzer . . . . .	1
Quick Start Deployment Guide . . . . .	1
Overview . . . . .	4
Fortinet extends advanced security to Google Cloud platform . . . . .	4
Fortinet solutions for Google Cloud. . . . .	4
FortiGate Next-Gen Firewall (NGFW) . . . . .	4
FortiWeb on Google Cloud protects web applications . . . . .	4
FortiWeb Cloud WAF-as-a-Service . . . . .	5
FortiManager provides centralized management for Fortinet devices . . . . .	5
FortiADC on Google Cloud protects web apps . . . . .	5
FortiAnalyzer simplifies SOC operations. . . . .	5
Preparing for deployment . . . . .	6
1. Create a Google Cloud Compute Portal account . . . . .	6
2. Obtain a license . . . . .	6
Licensing options . . . . .	6
3. Determine deployment method. . . . .	7
Architecture . . . . .	8
Deploying on Google Cloud . . . . .	8
FortiGate-VM . . . . .	8
FortiWeb . . . . .	8
FortiManager . . . . .	8
FortiADC . . . . .	8
FortiAnalyzer . . . . .	8
Automate deployments with Terraform. . . . .	9



# Table of Contents

- Use cases ..... 9
  - 1. Peered Security Hub ..... 9
  - 2. Network Security ..... 9
  - 3. Secure SD-WAN ..... 9
  - 4. Application and Web Traffic Security ..... 9
  - 5. High availability (HA) ..... 10
  - 6. SAP ..... 10
  - 7. Auto Scaling ..... 10
  - 8. Container security ..... 10
  - 9. Packet Mirroring ..... 11
- Best practices ..... 12
- FAQ ..... 12
- Additional resources ..... 13



## Overview

The Quick Start Deployment guide provides important guidance for deploying Fortinet's security solutions on Google Cloud. Fortinet products included in the guide are FortiGate-VM, FortiWeb, FortiManager, FortiADC, FortiAnalyzer, and FortiCWP. This Quick Start is for users who want to plan or deploy Fortinet solutions on Google Cloud or deploy a FortiGate-VM trial.

Fortinet extends security to the Google Cloud platform to maintain operational viable and consistent security protection for workloads on Google Cloud, or across hybrid and multi-cloud infrastructures. With Fortinet, Google Cloud customers have the flexibility to run any application on Google Cloud or on-premises, while maintaining consistent security everywhere. The Quick Start Guide assumes familiarity with the Google Cloud platform.

## Fortinet extends advanced security to Google Cloud platform

The Fortinet solution natively integrates security with Google Cloud, offering a comprehensive set of security solutions including deep threat inspection, traffic visibility, and protection of applications and cloud platforms against attacks. Fortinet provides integrated network security, application security, and cloud platform security in one platform.

The [Fortinet Security Fabric](#) offers organizations a comprehensive set of security solutions to address the expanding attack surface that spans hybrid cloud infrastructures. The Security Fabric enables a broad, integrated, and automated cybersecurity framework for all Fortinet security products.

Fortinet provides [Zero-Trust Access](#) solutions for Google Cloud. It delivers automatic secure remote access that verifies who and what is on your network and secures application access regardless of users' location.

## Fortinet solutions for Google Cloud

### FortiGate Next-Gen Firewall (NGFW)

By combining stateful inspection with a comprehensive suite of powerful security features, FortiGate Next Generation Firewall technology delivers complete content and network protection. FortiGate-VM integrates with Google Cloud Network Connectivity Center (NCC) to simplify cloud on-ramp for applications and workloads running on Google Cloud and across multi- and hybrid clouds.

- Using APIs, FortiGate-VM is infrastructure aware, enabling the configuration of high-availability (HA) environments automatically to create failover scenarios.
- FortiGate-VM is purpose-built to achieve superior security efficacy and the industry's best IPS performance. It provides network-based virtual patching for business applications that are hard to patch or can't be patched. This ensures protection against vulnerabilities without interrupting operations. It also provides SSL inspection (including TLS 1.3) to detect hidden malware, ransomware, and other HTTPS-borne attacks.
- NCC bridges a first-party native cloud underlay from Google Cloud with Secure SD-WAN and cloud on-ramp service from Fortinet across hybrid and multi-clouds.

[Licensing](#) – [Deploying on Google Cloud](#) – [Use Cases](#) – [FortiGate - PAYG](#) – [FortiGate - BYOL](#)

### FortiWeb on Google Cloud protects web applications

Many organizations now realize that unprotected web applications are the easiest point of entry for even unsophisticated hackers. Fortinet's multi-layered and correlated approach protects your web apps from the Open Web Application Security Project (OWASP) Top 10 and more. FortiWeb uses AI-based machine learning to continuously model each application to detect anomalies, identify threats, and protect against new vulnerabilities such as Apache Log4j. Our Web Application Security Service from FortiGuard Labs uses information based on the latest application vulnerabilities, bots, suspicious URL and data patterns, and specialized heuristic detection engines to keep your applications safe from malicious cyberattacks.



## FortiWeb Cloud WAF-as-a-Service

FortiWeb is also available as a cloud native SaaS based web application firewall (WAF) that protects web applications & APIs from the OWASP Top 10 threats, zero-day attacks and other application layer attacks.

### *Malicious Sources*

- Denial-of-service (DoS) attacks
- Sophisticated threats such as SQL injection, cross-site scripting, buffer overflows, and cookie poisoning
- Malware uploads and application distributed denial-of-service (DDoS) and other attacks
- Layer 7 load balancing and accelerated SSL offloading for more efficient application delivery

[Licensing](#) – [Deploying on Google Cloud](#) – [Use Cases](#) – [FortiWeb – Cloud WAF-as-a-Service](#)

## FortiManager provides centralized management for Fortinet devices

As the cloud and IoT force networks to evolve, organizations struggle to keep ahead. Too many solutions with varying management tools strain already overworked security teams. A new approach is needed to short-circuit this challenge, one that combines the perspective of both operations and security. FortiManager is the NOC-SOC operations tool that was built with security perspective. It provides a single-pane-of-glass across the entire Fortinet Security Fabric. FortiManager supports next-gen SOC through workflow automation and manages FortiGate NGFW as they scale up and down.

[Licensing](#) – [Deploying on Google Cloud](#) – [Use Cases](#) – [FortiManager - BYOL](#)

## FortiADC on Google Cloud protects web apps

FortiADC is an advanced application delivery controller that optimizes application performance and availability while securing the application both with its own native security tools and by integrating application delivery into the Fortinet Security Fabric.

- Application acceleration, load balancing, and web security, regardless of whether it is used for applications within a single data center or Google Cloud
- One solution for application acceleration, WAF, IPS, SSLi, link load balancing, and user authentication

[Licensing](#) – [Deploying on Google Cloud](#) – [Use Cases](#) – [FortiADC - BYOL](#) – [FortiADC - PAYG](#)

## FortiAnalyzer simplifies SOC operations

FortiAnalyzer offers advanced logging and reporting capabilities, centralized security analytics across the Fortinet Security Fabric, and security automation via Fabric Connectors and application programming interfaces (APIs).

[Licensing](#) – [Deploying on Google Cloud](#) – [Use Cases](#) – [FortiAnalyzer - BYOL](#)



## Preparing for Deployment

Before you can begin to deploy Fortinet's FortiGate-VM, FortiWeb, FortiManager, FortiADC or FortiAnalyzer on Google Cloud, you will need to make sure the following conditions have been met.

### 1. Create a Google Cloud Compute Portal account

### 2. Obtain a license. Choose one of the following:

- Purchase a Fortinet product license for Google Cloud
- Register to receive an evaluation license from the [Fortinet website](#)

### There are two flexible procurement options:

- Bring-your-own-License (BYOL) Licenses are purchased from a Fortinet channel partner for different products are transferrable across platforms.
- Pay-as-you-go (PAYG) can be consumed using a pay-as-you-go (PAYG) on-demand usage model from the Google Cloud Marketplace.

BYOL offers perpetual (normal series and v-series) and annual subscription licensing as opposed to PAYG, which is an hourly subscription available with marketplace listed products. BYOL licenses are available for purchase from resellers or your distributors. BYOL licensing provides the same ordering practice across all private and public clouds, no matter what the platform is. You must activate a license for the first time you access the instance from the GUI or CLI before you can start using various features.

In both BYOL and PAYG, cloud vendors charge separately for resource consumption on computing instances, storage, and so on, without use of software running on top of it.

For BYOL, you typically order a combination of products and services including support entitlement. News-series SKUs contain the VM base and service bundle entitlements for easier ordering. PAYG includes support, for which you must contact Fortinet Support with your customer information.

### Licensing Options

Licensing	FortiGate-VM	FortiManager	FortiAnalyzer	FortiADC	FortiWeb	FortiWeb Cloud WAF-as-a-Service
BYOL	X	X	X	X	X	
PAYG	X			X		
SaaS						X
Flex-VM*	X					

\*Flex-VM is a subscription service to manage VM usage entitlements for FortiGate-VMs.



### 3. Determine deployment method

Three deployment options listed below with links to additional documentation.

A. [Google Cloud Marketplace](#) is a fulfillment platform that provides customers a centralized location to easily discover, subscribe, and deploy Fortinet solutions using a trial and buy experience in just a few clicks. For information regarding the possible deployment methods for FortiGate-VM, FortiWeb, FortiWeb Cloud WAF-as-a-Service, FortiManager, and FortiAnalyzer, visit the links below to the Google Cloud Marketplace.

#### FortiGate-VM

- [BYOL](#)
- [PAYG](#)

#### FortiWeb

- [BYOL](#)

#### FortiWeb Cloud WAF-as-a-Service





#### FortiManager

- [BYOL](#)



#### FortiAnalyzer

- [BYOL](#)

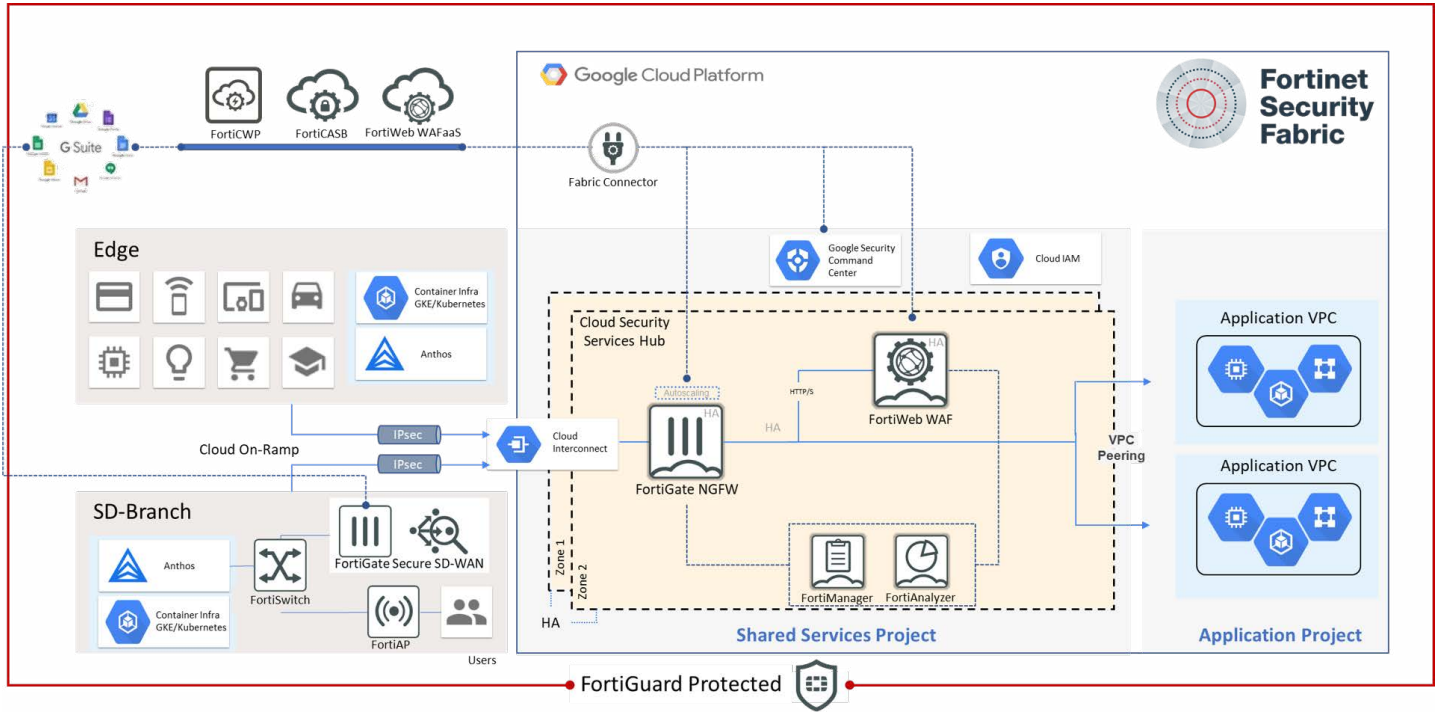
B. Deploy using a deployment image via Google Cloud Compute Engine.

- Links to deployment steps:  [FortiGate-VM](#),  [FortiWeb](#)
-  [FortiGate-VM](#)
  - FortiGate-VM is required to be deployed inline across multiple networks and multiple network interfaces must be assigned to the instance.
  - This deployment method supports up to 8 NICs per instance on the Google Cloud platform.
  - Google Cloud does not allow changing the number of network interfaces after deploying VM instances.
-  [FortiWeb](#)

C. Google Cloud software development kit (SDK) is a method of deploying Fortinet outside of the marketplace product listing and without creating an instance on the Google Cloud Compute Portal.

- Use to assign multiple network interfaces to the VM instance.
- Links to deployment steps:  [FortiGate](#)
-  [FortiGate-VM](#)
  - This deployment method is only applicable for BYOL. The PAYG deployment file will be ready at a later time.

# Architecture



## Deploying on Google Cloud

The links in this section will take you to the Fortinet product located in the [Fortinet document library](#) for additional documentation, links to GitHub and deployment steps.

### FortiGate-VM

- Steps to deploy using [Google Cloud Marketplace](#)
- Deploy custom image using [Google Cloud Web Console](#)
- Deploy using [Google Cloud SDK CLI](#)

### FortiWeb

- Steps to deploy on [Google Cloud Marketplace](#)
- Deploy on [Google Cloud Compute Engine](#)

### FortiWeb Cloud WAF-as-a-Service

- Steps to deploy on [Google Cloud Marketplace](#)

### FortiManager

- Steps to deploy on [Google Cloud Marketplace](#)
- Setting up [FortiManager](#)

### FortiADC

- Deploy on [Google Cloud Compute Engine](#)

### FortiAnalyzer

- Steps to deploy on [Google Cloud Marketplace](#)





# Automate deployments with Terraform

Deploying [Fortigate-VM](#) using terraform

## Use Cases

Fortinet extends security to Google Cloud and provides consistent, enterprise security across a spectrum of use cases:


### 1. Peered Security Hub

A Peered Security Hub architecture provides flexibility of securing up to 150 segments using standard VM04 instances. The hub-and-spoke design puts firewalls in the hub VPC Network and connects all VPC Networks to be inspected for traffic using peering.



Use case	Fortinet solution
Security Hub VPC	FortiGate-VM

### 2. Network Security

Implement scalable and multilayer security using a cloud security services hub. Leverage the scale and flexibility of the Google Cloud infrastructure to build effective and low-friction security solutions.

Use case	Fortinet solution
Hybrid cloud with Google Anthos	FortiGate-VM - FortiWeb
 <a href="#">VPC-to-VPC segmentation</a>	FortiGate-VM
Remote access/VPN	FortiGate-VM

### 3. Secure SD-WAN

The Fortinet  [Secure SD-WAN](#) transforms and secures a WAN. With an  [SD-WAN transit routing setup](#) with Google Network Connectivity Center (NCC), you can route data and exchange border gateway protocol (BGP) routing information between two or more remote sites via GCP.

Use case	Fortinet solution
Distributed enterprise / SD-WAN	FortiGate-VM - FortiManager - FortiAnalyzer - FortiWeb



## 4. Application and Web Traffic Security

Protect business-critical applications from known and unknown threats, including zero-day attacks, botnet attacks, and API attacks. Also mitigate the risk from server vulnerabilities and support compliance with the latest laws, regulations, and standards.

### Use case

Web applications

### Fortinet solution

FortiWeb Cloud WAF-as-a-Service - FortiWeb

## 5. High availability (HA)

Enhance reliability and increase performance of critical enterprise networking components for deployments in Google Cloud.

### Use case

HA

### Fortinet solution

FortiGate-VM

There are two options for high availability (HA) configurations with FortiGate-VM on Google Cloud. The recommended deployment is multiple zones to address zonal failures.

-  [Deploying between multiple zones](#)

## 6. SAP

Using a holistic approach, [Fortinet secures the entire enterprise SAP landscape \(PDF\)](#) to protect against security threats. By leveraging its extensive threat intelligence, a strong portfolio, and state-of-the-art AI/ML security, Fortinet provides comprehensive security across the entire SAP ecosystem.

The single-pane-of-glass management enabled by the Fortinet portfolio provides a complete and consolidated view of security events across on-premises, hybrid, and multi-cloud environments. A consistent security framework protects SAP workloads and all SAP-generated data. Fortinet applies AI for faster threat prevention, detection, and response. The Fortinet security solution for SAP centralizes and automates security controls and analytics—making it easier to manage, respond, and automate the SecOps capabilities.

### Use case

SAP

### Fortinet solution

FortiGate-VM – FortiManager – FortiWeb – FortiADC

## 7. Auto Scaling

You can deploy FortiGate virtual machines (VMs) to support Auto Scaling on Google Cloud. Multiple FortiGate-VM instances can form an Auto Scaling group (ASG) to provide highly efficient clustering at times of high workloads. To provide centralized management and a single pane of glass, FortiManager can manage FortiGate-VM devices as they scale out and in.

### Use case

Auto scaling

### Fortinet solution

FortiGate-VM – FortiManager



## 8. Container security

Kubernetes is a powerful platform for scaling containers in production to meet user demand. However, Kubernetes clusters are quite complex, and the default configuration should be hardened to reduce the attack surface. Here are some of the top security concerns about running Kubernetes clusters in production:

- Misconfigurations & Exposure
- Failed Compliance Audits
- Image Vulnerabilities
- Runtime Threats

### FortiCWP's Container Guardian

FortiCWP's Container Guardian provides deeper visibility into the security posture for container registries and repositories.

Container images are scanned for vulnerabilities during the build process with policy enforcement tools to prevent vulnerability propagation before images are deployed into container registries. Registries are continuously monitored and scanned for new vulnerabilities to provide continuous protection.

Container Guardian performs continuous audits in containers and clusters to detect misconfigurations and other noncompliant security practices with policies to alert IT teams or auto-remediate.

### FortiCWP Container Guardian Benefits

- CIS Benchmarks are ran to identify configuration that is not compliant with best practices which can expand the attack surface of a cluster
- Container image scanning on build requests and regular registry scans identifies vulnerable images
- CI\CD integration with Jenkins provides image scanning when images are created as part of a build request, these requests can be failed based on vulnerabilities found
- Graphical visibility into K8s deployments and also traffic patterns within the cluster and even to internal\external resources outside the cluster

#### Use case

Container security

#### Fortinet solution

FortiCWP

## 9. Packet mirroring

You can utilize the Google Cloud Packet Mirroring feature together with FortiGate-VM one-arm-sniffer mode to detect malicious or infected traffic and alert the administrators. For multiple sensors it's best to use FortiAnalyzer as the correlation and aggregation engine providing single pane of glass insights into the traffic patterns as well as detected threats or compromised VMs.

Fortinet IDS for Google Cloud is an intrusion detection service that provides threat detection for intrusions, malware, spyware, and command-and-control attacks on your network. Cloud IDS works by creating a peered network with mirrored VMs. FortiGate virtual appliances can detect and blocking threats using the FortiLabs-powered IDS/IPS system as well as the built-in antivirus engine.

#### Use case

Packet mirroring

Cloud IDS

#### Fortinet solution

FortiGate-VM – FortiAnalyzer


FortiGate-VM – FortiAnalyzer



## Best Practices

As soon as the FortiGate-VM is connected to the Internet it is exposed to external risks, such as unauthorized access, man-in-the-middle attacks, spoofing, DoS attacks, and other activities from malicious actors. Prior to your deployment, please consider the following best practices to harden your infrastructure:

- Review default settings such as administrator passwords, certificates for GUI and SSL VPN access, SSH keys, open administrative ports on interfaces, and default firewall policies
- Either use the startup wizard or manually reconfigure the default settings to tighten your security from the beginning, thereby securing your network to its full potential
- Set RBAC controls with least access for administrators and manage roles from a centralized source (LDAP, Active Directory, etc.)
- Configure bastion services to limit the scope of administrative network sources

Additional documentation, best practices, training & tutorials can be found here:  [Fortinet Document Library for Cloud](#)

## FAQ

### [FortiGate-VM](#)

#### **What backup retention does FortiGate-VM Cloud provide?**

Backup does not have storage limits. For licensed devices, the retention period is one year. For unlicensed devices, the retention period is seven days.

#### **How does automatic backup work?**

Automatic backup is either per session or day. FortiGate-VM setting changes from FortiOS or FortiGate-VM Cloud trigger backup. If there are no changes to FortiGate-VM settings, FortiGate-VM Cloud does not perform a backup.

#### **What public IP addresses and ports does FortiGate Cloud use?**

FortiGate-VM Cloud uses the TCP ports 80, 443, 514, 541, and UDP ports 5246/5247. IP address ranges differ depending on the region.

#### **How can I receive a daily report by email?**

Ensure that the scheduled report has been generated and that the email address has been added.

### [FortiWeb](#)

#### **What should I do when I upgrade or replace a FortiGate or FortiGate VM under FortiManager?**

Use the following procedure to upgrade the FortiGate or FortiGate-VM OS version (in some cases, the FortiGate-VM license might be new and will have a different serial number):

- Upgrade the version of FortiGate or FortiGate-VM.
- In FortiManager, update the ADOM version on FortiManager.
- Poll from FortiPortal.

**I can see data in the dashboard as a site administrator but not as customer user. How do I fix this?**

Select the User(s) icon on the Customer List page to display the Customer User(s) page and then select the Edit icon for the specific customer user. Check if the customer user has permission to view information related to all sites and the devices associated with those sites.

## Additional Resources

### Google Cloud Resources

- [Google Cloud Security and Privacy Considerations](#)
- [Google Cloud Firewall Rules](#)
- [Google Cloud HA VPN Interoperability Guide for FortiGate](#)

### Fortinet Documentation

-  [Resource Library](#)
- [Customer Service & Support](#)
-  [FortiOS Administration Guide - Google Cloud](#)
-  [FortiManager Administration Guide – Google Cloud](#)
- [Fortinet GitHub Repository](#)
-  [Ports and Protocols](#)
- [FortiGate-VM Open Ports](#)

