



SERVICE DESCRIPTION

FORTIGSLB CLOUD (GLOBAL SERVER LOAD BALANCE AS-A-SERVICE)

1. Introduction

FortiGSLB Cloud is a cloud based Software-as-a-Service providing DNS-based load balancing as described herein (the “Service”). The Service helps the end-customer (the “Customer”) to optimize end-client requests for a specific domain by dynamically distributing workload across Customer’s data centers and different locations. In particular, the Service applies several techniques to:

- Direct internet application traffic to multiple servers behind a single external IP address; and
- Make use of advanced load balancing policies (e.g. Geo-IP, server load) for dynamic selection of preferred pools of servers.

Through the FortiGSLB Cloud web-based portal, the Customer may:

- Define the pools of physical and virtual servers in data centers that will host Customer web applications.
- Manage multiple domains for multiple tenants from multiple organizations from a single place.
- Access the FortiGSLB Cloud’s web dashboard to obtain an analysis on availability, utilization, DNS queries, and services.
- Receive Customer’s application visibility in real time.

2. Service Features and Deliverables

FortiGSLB Cloud platform is managed by Fortinet on a twenty-four (24) hours by seven (7) days a week basis. It is monitored for server availability, service capacity, and network resource utilization.

Fortinet will use reasonable efforts to ensure that the Customer receives as part of the Service:

- A DNS server for Customer usage as DNS name server.
- Reasonable support for Customer’s topology definition, including data centers, locations, primary and backup physical and virtual servers, and pool of servers.
- A “One-Click-DNS” integration of existing FortiADC customers in addition to a hybrid global server load balancing solution with FortiGSLB Cloud.
- Customer’s configured methods to route DNS queries to the appropriate virtual servers.
- Virtual server pool selection method based on pool weight, origin of DNS query, and first available pool.
- Reasonable support of standard DNS zones (RFC 1035).
- Management of the Service’s underlying infrastructure, including scaling and monitoring for availability, required to deliver the Service and meet a Service availability target of 99.99%. For the avoidance of doubt, management of Customer’s or third parties infrastructure is explicitly excluded.
- FortiGSLB Cloud management portal with target availability of 99.99%.
- Visibility on Customer’s traffic and servers through a dashboard displaying status and statistics for monitoring.
- FortiCare™ 24x7 technical support, as outlined in the then-current Fortinet support policies and service description, available on the Support Portal or other site as designated by Fortinet.

3. Customer Requirements and Responsibilities

The Customer agrees for the duration of the Service to be solely responsible for:

- Maintaining a Fortinet ONE unified cloud services login to access to FortiGSLB Cloud.
- Providing and maintaining one (1) or multiple registered domain(s).
- Configuring FortiGSLB Cloud appropriately for use of the Service in accordance with the Service’s then-current documentation, including:
 - Assigning domain names to set virtual servers.
 - Configuring FQDN and zone services.
 - Ensuring that health check policy works as configured by Customer.



- Changing the DNS entry for the virtual service to point to the FortiGSLB Cloud infrastructure as necessary, including when the Customer ceases using the Service.
- Accessing the FortiGSLB Cloud web-based portal through a supported web browser software with appropriate internet connectivity.
- Purchasing and maintaining all required Service entitlements (in accordance with the DNS QPS SKUs and Health Check SKUs listed below) to adequately match or exceed the Customer's present and future usage of the Service. For clarity, the Customer acknowledges and agrees that any usage of the Service above its purchased and active Service entitlements will be automatically blocked and Fortinet shall not be held responsible for any service interruptions and/or degradations of the Company's network, systems, applications, and/or devices or any other damages, consequences, or disruptions caused to Company or third parties as a result of such Service blocking.
- Designating a network security skilled individual who will serve as a single point of contact for liaising with Fortinet for the duration of the Service. This person should be able to assist with determining priorities, responsible for delivery capability and provide the names of the designated contacts.
- Complying with Fortinet's instructions for technical ticket creation.
- Complying with all reasonable requests for technical information to deliver the Service and providing timely updates to open tickets. It should be noted that when a technical ticket is awaiting a Customer response weekly reminders would be automatically initiated for a period of twenty (20) calendar days. The technical ticket will be automatically closed after such period if there is no response from the Customer.
- Providing, at least, fifteen (15) business days' notice to Fortinet for the setup of the Service.

By purchasing the Service, Customer understands and agrees that Fortinet is not required to provide the Service if Customer fails to meet any of the Service requirements as stipulated herein.

4. Scope and Conditions

- The Customer acknowledges and agrees that Fortinet may permanently or temporarily limit or suspend the Service to the Customer at Fortinet's sole discretion in the event that continued provision of the Service to the Customer could compromise the integrity or security of the Service or Fortinet's systems or networks in Fortinet's opinion.
- Customer agrees to use the Service for legitimate and lawful business purposes only. This Service is provided for the Customer internal business use and shall not be resold -or use for the provision of services to third parties. The Service may be terminated without notice in the event that the Customer breaches the aforementioned obligations. Furthermore, Fortinet may notify the relevant authorities should Fortinet discover, regardless of intent, any illegal activity, or activity likely to undermine the integrity of the Service or Fortinet's systems, networks or reputation.
- Any loss of connectivity by the Customer is the responsibility of the Customer and the Service shall be considered to be utilized regardless of such loss or absence of Customer's actual usage of the Service. Availability targets as set forth herein shall be construed as the availability of FortiGSLB Cloud infrastructure, excluding required maintenance, updates or upgrades with: (1) planned downtime where Customer had an ability to plan for such updates or upgrades; and/or (2) regular maintenance downtime.
- Fortinet will use reasonable efforts to perform the maintenance of the Fortinet infrastructure aiming at minimizing or mitigating any Service disruption to the extent reasonably feasible. In particular, Fortinet will use reasonable efforts to provide the Customer with forty-eight (48) hours advanced notice in the event that any planned maintenance activity may cause Service disruption. For any planned maintenance, Fortinet will use reasonable efforts not to perform it between the hours of 8 am and 6 pm in the time zone where the infrastructure subject to maintenance is located, and not for more than eight (8) hours in any given calendar month. Notification will be made through the most appropriate means at the discretion of Fortinet which may include email, portal messages or other means.
- During maintenance activity that requires Fortinet to make the Service unavailable, Fortinet will use reasonable efforts to configure the traffic to bypass and forward it directly to origin web servers to minimize Service availability impact to the extent reasonably possible.
- In the event that the integrity of the Service is at risk, Fortinet may perform emergency maintenance actions at its sole discretion and will use reasonable efforts to inform all affected parties within one (1) hour of the start of the maintenance activity.



- The Customer is responsible for ensuring that their use of the Service is in accordance with all applicable privacy and security laws, and the Customer will ensure it has in place proper controls and processes in this respect.
- The scope of the Service is limited to the services as outlined in this service description. Any request made by the Customer for services beyond the duration or scope of the Services will be provided at Fortinet's discretion and billable at the then-current rate.
- Any Fortinet resource assigned to the Service will work up to eight (8) hours during core business hours of 09:00 am to 6:00 pm in the local time zone where the Service is being performed.
- Unless otherwise specified, the Service will be delivered in English and remotely.
- Activation of the Service takes place in accordance with Fortinet's Service Contract Activation and Grace Period Policy, made available at: <https://www.fortinet.com/corporate/about-us/legal/service-contract-activation-grace-period-policy>.
- The Service is delivered in accordance with any data processing agreement between the parties and Fortinet's Privacy Policy, made available at: <https://www.fortinet.com/corporate/about-us/privacy.html>.
- The Service is subject to the terms of then-current Fortinet's Service Terms & Conditions located at <https://www.fortinet.com/corporate/about-us/legal.html> and Fortinet's then-current privacy policy available at: <https://www.fortinet.com/corporate/about-us/privacy.html> (or any other sites as designated by Fortinet from time-to-time).

5. Eligibility and Purchasing

The Service is available for purchase by a Customer through authorized Fortinet's resellers and distributors globally or AWS cloud marketplace.

When the Service is bought from a Fortinet authorized reseller or distributor, the duration of the Service is three hundred and sixty-five (365) days from activation of the purchased Service entitlement. The Service is offered in different technical capacities based on the amount of DNS queries per seconds (QPS) transferred and Health Checks performed by the Service. Customer may cease using the Service at any time and for any reason, but in no event will Fortinet refund any prepaid subscription fee. All sales are final.

Purchasing Information:

FortiGSLB Cloud Service - 100 QPS (queries per second) Annual Subscription. Includes 24x7 FortiCare. Select Health Checks separately	FC2-10-CGSLB-330-02-DD
FortiGSLB Cloud Service - 500 QPS (queries per second) Annual Subscription. Includes 24x7 FortiCare. Select Health Checks separately	FC3-10-CGSLB-330-02-DD
FortiGSLB Cloud Service - 1000 QPS (queries per second) Annual Subscription. Includes 24x7 FortiCare. Select Health Checks separately	FC4-10-CGSLB-330-02-DD
FortiGSLB Cloud Service - Additional 2 Advanced Health Checks	FC1-10-CGSLB-332-02-DD
FortiGSLB Cloud Service - Additional 10 Advanced Health Checks	FC2-10-CGSLB-332-02-DD
FortiGSLB Cloud Service - Additional 100 Advanced Health Checks	FC4-10-CGSLB-332-02-DD