

FortiOS - Rackspace Cookbook

Version 6.2

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



August 21, 2020

FortiOS 6.2 Rackspace Cookbook

01-620-548068-20200821

TABLE OF CONTENTS

About FortiGate for Rackspace	4
Instance type support	4
Licensing	4
Order types	4
Creating a support account	5
Launching FortiGate on Rackspace	7
Connecting to the FortiGate	7
Building a server behind the FortiGate	7
Accessing a server behind the FortiGate	8
Change log	9

About FortiGate for Rackspace

By combining stateful inspection with a comprehensive suite of powerful security features, FortiGate Next Generation Firewall (NGFW) technology delivers complete content and network protection. This solution is available for deployment on Rackspace.

In addition to advanced features such as an extreme threat database, vulnerability management, and flow-based inspection, features including application control, firewall, antivirus, IPS, web filter, and VPN work in concert to identify and mitigate the latest complex security threats.

Highlights of FortiGate for Rackspace include the following:

- Delivers complete content and network protection by combining stateful inspection with a comprehensive suite of powerful security features.
- IPS technology protects against current and emerging network-level threats. In addition to signature-based threat detection, IPS performs anomaly-based detection, which alerts users to any traffic that matches attack behavior profiles.
- New Docker application control signatures protect your container environments from newly emerged security threats. See [Use Case: FortiGate-VM on a Docker Environment](#).

Instance type support

Rackspace supports only pay-as-you-go for FortiGate-VM deployments.

Licensing

The FortiGate-VM image provided on mycloud.rackspace.com is a PAYG image that does not require licensing. However, you should still create a Fortinet support account and register your FortiGate-VM.

Order types

On Rackspace, there is one order type: pay-as-you-go (PAYG).

With a PAYG subscription, the FortiGate-VM becomes available for use immediately after you create the instance.

To purchase PAYG, all you need to do is launch the product on the Rackspace marketplace. However, you must contact [Fortinet Support](#) with your customer information to obtain support entitlement. See [Creating a support account on page 5](#).



PAYG FortiGate instances do not support the use of VDOMs.



PAYG FortiGate instances do not support additional FortiGate features that require separate licenses.

When using a FortiGate-VM PAYG instance, the GUI may display expiry dates for FortiGuard services. However, these expiries are automatically extended for as long as the PAYG instance's lifespan. You do not need to be concerned about the expiry of FortiGuard services.

Dashboard	>	FortiGuard Distribution Network	
Security Fabric	>	Botnet Domains	Version 2.00480
Network	>	AntiVirus	Licensed - expires on 2021/01/01
System	>	AV Definitions	Version 77.00424
Administrators		AV Engine	Version 6.00144
Admin Profiles		Mobile Malware	Version 77.00424
Firmware		SD-WAN Network Monitor	Not Licensed
Settings		Outbreak Prevention	Licensed - expires on 2021/01/01
HA		Industrial DB	Licensed - expires on 2021/01/01
SNMP		Industrial Attack Definitions	Version 15.00845
Replacement Messages		Security Rating	Licensed - expires on 2021/01/01
FortiGuard	>	Web Filtering	Licensed - expires on 2021/01/01
Feature Visibility		Blacklisted Certificates	Version 1.00261
Certificates		FortiGate Cloud	Not Activated
Policy & Objects	>		
Security Profiles	>		
VPN	>		
User & Authentication	>		
WiFi & Switch Controller	>		
Log & Report	>		

Creating a support account

FortiGate for Rackspace supports the pay-as-you-go (PAYG) licensing model. See [Order types on page 4](#).

To make use of Fortinet technical support and ensure products function properly, you must complete certain steps to activate your entitlement. Our support team can identify your registration in the system thereafter.

First, if you do not have a Fortinet account, you can [create one](#).

To register the PAYG license:

1. Deploy and boot up the FortiGate PAYG instance on the Rackspace cloud and log into the FortiGate GUI management console.
2. On the Dashboard, copy the VM serial number.
3. Go to [Fortinet Service & Support](#) and create a new account or log in with an existing account.
4. Go to *Asset > Register/Activate* to start the registration process.
5. In the *Specify Registration Code* field, enter the serial number, and select *Next* to continue registering the product. Enter your details in the other fields.

6. After completing registration, contact [Fortinet Customer Support](#) and provide your FortiGate instance's serial number and the email address associated with your Fortinet account.

Launching FortiGate on Rackspace

You can deploy the FortiGate NGFW for Rackspace as a virtual appliance in the Rackspace cloud. This section shows you how to install and configure a single instance FortiGate-VM PAYG virtual appliance.

To subscribe to the FortiGate-VM:

1. On the Rackspace mycloud portal, go to *SERVERS > CREATE RESOURCES > Cloud Server*.
2. On the *Create Server* page, name your FortiGate-VM and choose the region. Under *Image*, choose the *Linux/Appliances Image Type*. Next, from *Operating System*, choose *FortiGate VM*.
3. Under *Flavor*, choose a flavor that fits your resource needs. Pay careful attention to the *Network* value. The *Network* value controls throughput in Rackspace cloud. Larger flavors have more throughput.
4. (Optional) Under *Advanced Options*, select an SSH key.
5. Under *Recommended Installs*, select *Configure as gateway*. This automatically configures a cloud network and NAT on your FortiGate-VM.
6. Verify your options, then click *Create Server*. The root admin password displays. Copy the password, then dismiss the dialog.
7. After you create the server, the server details page displays. Wait for the server to show an active status. This usually takes a few minutes.

Connecting to the FortiGate

To connect to the FortiGate:

1. In a browser, go to `https://<IP address>`, where "IP address" is your FortiGate-VM public IP address.
2. Do one of the following:
 - a. Log in using "admin" as the username and the root admin password from [Launching FortiGate on Rackspace on page 7](#) as the password.
 - b. Log in via SSH. Use the username "admin" and the root admin password or an SSH key.

Building a server behind the FortiGate

To build a server behind the FortiGate:

1. From the mycloud portal server creation page, scroll down to *Advanced Options*.
2. Click *Select Networks...*
3. Ensure that *PublicNet* is not selected.
4. Select the cloud network that has the name of your server.
5. (Optional) Enable ServiceNet if you use Rackspace products such as Cloud Backups or Cloud Files.

The server now builds without a public IP address. However, since NAT is configured on the FortiGate-VM, the server can connect outbound to the Internet.

Accessing a server behind the FortiGate

You can access servers behind the FortiGate-VM in a variety of ways:

- Using the FortiGate-VM to forward remote access ports to the server behind the VM
- Configuring VPN on the FortiGate-VM, then connecting to VPN. Once connected to VPN, you can access servers across the VPN via their Cloud Networks (private) IP addresses.
- Using the emergency console available in the mycloud.rackspace.com portal

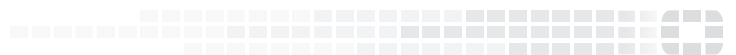
For details about configuring the FortiGate, see the [FortiOS Handbook](#).

Change log

Date	Change Description
2019-11-29	Initial release.
2020-05-15	Updated Order types on page 4 .
2020-08-21	Updated About FortiGate for Rackspace on page 4 subtopics.



FORTINET®



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.