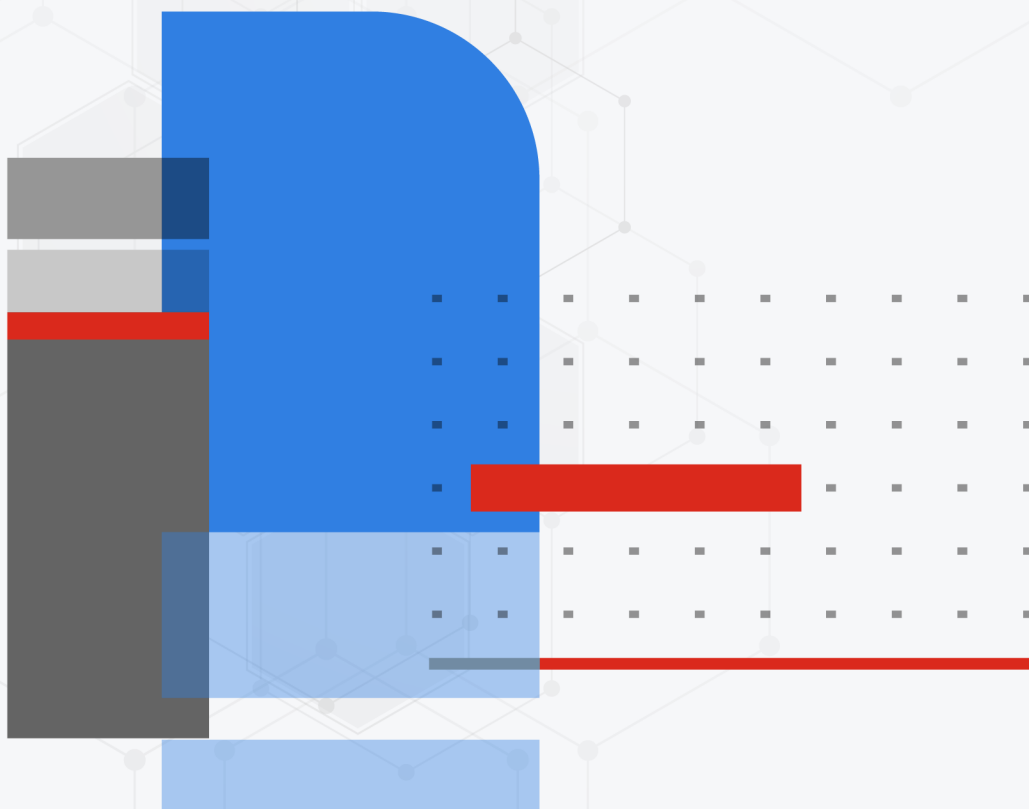




HA on Azure Deployment Guide

FortiMail 7.4.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<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/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



December 21, 2023

FortiMail 7.4.0 HA on Azure Deployment Guide

06-740-978581-20231221

TABLE OF CONTENTS

Change Log	4
Introduction	5
Creating an Azure Resource Load Balancer	6
Adding FortiMail-VM Instances to Azure Backend Pool	12
Monitoring FortiMail-VM Health with Azure Load Balancer	13

Change Log

Date	Change Description
2019-05-25	Initial release.
2023-12-21	Republished.

Introduction

FortiMail units can operate in one of the two HA modes: Active-Passive or Active-Active. For details about HA modes, refer to the [FortiMail Administration Guide](#).

- **Active-Active HA**

Active-Active HA is also called Config-HA. All instances in an HA group can process traffic. Azure load balancer can be used to distribute traffic to all HA members. If one member is down, Azure load balancer will be able to detect it and traffic will be redirected to other healthy members.

- **Active-Passive HA**

Azure load balancer can be used to achieve this Active-Passive HA setup. In an HA group, the primary unit processes traffic while the secondary unit works as a standby and will not process traffic. If the primary unit is down, the secondary unit will take over the role and continue to process traffic. Azure load balancer will be able to detect the healthy status of FortiMail instances and distribute the traffic.



All HA units must have valid licenses to function correctly.

Prerequisites


To configure FortiMail HA cluster on Azure, you need:

- A virtual cloud network.
- A security list.
- Two FortiMail-VM instances. See [FortiMail VM on Azure Deployment Guide](#) for more information.

Creating an Azure Resource Load Balancer


After logging on to the Microsoft Azure Portal <https://portal.azure.com>, go to All services > Load balancing, click the “Create” button to create a new Load Balancer.


[All services](#) > [Load balancing](#)


 **Load balancing** | Load Balancer ⚙️ ...


 <<

+ Create


 Manage view ▾


 Refresh

 Export to CSV

 Open query

 |


 Assign tags

 Overview

Subscription == all

Resource group == all ×

Location == all ×

 Add filter

1. Configure the basic settings

Create load balancer ...

Basics

Frontend IP configuration

Backend pools

Inbound rules

Outbound rules

Tags

Review + create

Azure load balancer is a layer 4 load balancer that distributes incoming traffic among healthy virtual machine instances. Load balancers use a hash-based distribution algorithm. By default, it uses a 5-tuple (source IP, source port, destination IP, destination port, protocol type) hash to map traffic to available servers. Load balancers can either be internet-facing where it is accessible via public IP addresses, or internal where it is only accessible from a virtual network. Azure load balancers also support Network Address Translation (NAT) to route traffic between public and private IP addresses. [Learn more.](#)

Project details

Subscription *

BYOL-DevOps

Resource group *

[Create new](#)**Instance details**

Name *

FortiMail-LoadBalancer

Region *

East US

SKU * ⓘ

- ☒ Standard
- ☐ Gateway
- ☐ Basic



Microsoft recommends Standard SKU load balancer for production workloads.

[Learn more about pricing differences between Standard and Basic SKU](#)

Type * ⓘ

- ☒ Public
- ☐ Internal

Tier *

- ☒ Regional
- ☐ Global

2. Add a frontend IP configuration

Create load balancer ...

Basics **Frontend IP configuration** Backend pools Inbound rules Outbound rules Tags Review + create

A frontend IP configuration is an IP address used for inbound and/or outbound communication as defined within load balancing, inbound NAT, and outbound rules.

+ Add a frontend IP configuration

Name ↑↓

IP address ↑↓

Add a frontend IP to get started

Create load balancer ...

Basics **Frontend IP configuration** Backend pools Inbound rules Outbound rules Tags Review + create

A frontend IP configuration is an IP address used for inbound and/or outbound communication as defined within load balancing, inbound NAT, and outbound rules.

+ Add a frontend IP configuration

Name ↑↓

Add a frontend IP to get started

Add frontend IP address ×

Name *

FortiMail-LB-FrontendIP ✓

IP version

☒ IPv4 ☐ IPv6

IP type

☒ IP address ☐ IP prefix

Public IP address *

Choose public IP address ▼

[Create new](#)

Add a public IP address

Name *

FortiMail-LB-FrontendIP ✓

SKU

☐ Basic ☒ Standard

Tier

☒ Regional ☐ Global

Assignment

☐ Dynamic ☒ Static

Availability zone *

No Zone ▼

OK

Cancel

3. Add a backend pool

You can add FortiMail units into the backend pool at this step or later (see the next section).

Create load balancer ...

Basics Frontend IP configuration **Backend pools** Inbound rules Outbound rules Tags Review + create

A backend pool is a collection of resources to which your load balancer can send traffic. A backend pool can contain virtual machines, virtual machine scale sets, and containers.

+ Add a backend pool

Name	Virtual network	Resource Name	Network interface
Add a backend pool to get started			

Add backend pool ...

Name * FortiMail-LB-BackendPool ✓

Virtual network * ⓘ

Backend Pool Configuration

☒ NIC

☐ IP Address

IP Version

☒ IPv4

☐ IPv6

Virtual machines

You can only attach virtual machines in eastus that have a standard SKU public IP configuration or no public IP configuration. All IP configurations must be on the same virtual network.

4. Create inbound rules

Creating Inbound rules to load balance SMTP traffic to backend FortiMail VMs. Also enable health probe to monitor the health status of the backend FortiMail and proactively redirect the SMTP traffic.

FortiMail-LoadBalancer | Load balancing rules ...

Search (Ctrl+/) « + Add Refresh Give feedback

Filter by name...

Name ↑↓	Load balancing rule ↑↓	Backend pool ↑↓	Health probe ↑↓
FortiMail-LB-rule	FortiMail-LB-rule (TCP/25)	FortiMail-LB-BackendPool	FortiMail-LB-Health

Settings

- Frontend IP configuration
- Backend pools
- Health probes
- Load balancing rules**
- Inbound NAT rules

Add load balancing rule ...

FortiMail-LoadBalancer

i A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name *	FortiMail-LB-rule ✓
IP Version *	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Frontend IP address * ⓘ	FortiMail-LB-FrontendIP ✓
Backend pool * ⓘ	FortiMail-LB-BackendPool ✓
Protocol *	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
Port *	25 ✓
Backend port * ⓘ	25 ✓
Health probe * ⓘ	<div> <div></div> <div>Create new</div> </div>
Session persistence ⓘ	
Idle timeout (minutes) * ⓘ	4
TCP reset	
Floating IP ⓘ	
Outbound source network address translation (SNAT) ⓘ	

Add health probe

Name *

FortiMail-LB-Health ✓

Protocol *

TCP ✓

Port * ⓘ

25 ✓

Interval * ⓘ

5 seconds

Unhealthy threshold * ⓘ

2 consecutive failures

Used by ⓘ

Not used

OK Cancel

Backend pool members

and because it can cause

5. Review and create the load balancer

Create load balancer ...

✓ Validation passed

Basics Frontend IP configuration Backend pools Inbound rules Outbound rules Tags Review + create

Basics

Subscription	BYOL-DevOps
Resource group	
Name	FortiMail-LoadBalancer
Region	East US
SKU	Standard
Tier	Regional
Type	Public

Frontend IP configuration

Frontend IP configuration name	FortiMail-LB-FrontendIP
Frontend IP configuration IP address	To be created

Backend pools

Backend pool name	FortiMail-LB-BackendPool
-------------------	--------------------------

Inbound rules

None

Outbound rules

None

Tags

None

Adding FortiMail-VM Instances to Azure Backend Pool

1. Create FortiMail-VM instances

Follow [FortiMail Azure Quick Start Guide](#) to deploy multiple FortiMail-VM instances on Azure.

2. Configure HA on FortiMail

Log on to your FortiMail-VM instances with URL `https://<Public_IP>/admin`.

Go to *System > High Availability > Configuration* to setup HA between your FortiMail instances. For more details about HA setup, see the section “Using high availability (HA)” in the [FortiMail Administration Guide](#).

3. Add the FortiMail-VM instances to Backend Pool

Now you can add Azure FortiMail VMs to the Backend pool of the pre-created load balancer. Choose the Virtual Network (where the two VMs are deployed) and add them into the Backend pool.

FortiMail-LB-BackendPool ...

FortiMail-LoadBalancer

Name FortiMail-LB-BackendPool

Virtual network * ⓘ

Backend Pool Configuration

IP Version

☒ NIC
☐ IP Address

☒ IPv4
☐ IPv6

Virtual machines

You can only attach virtual machines in eastus that have a standard SKU public IP configuration or no public IP configuration. All IP configurations must be on the same virtual network.

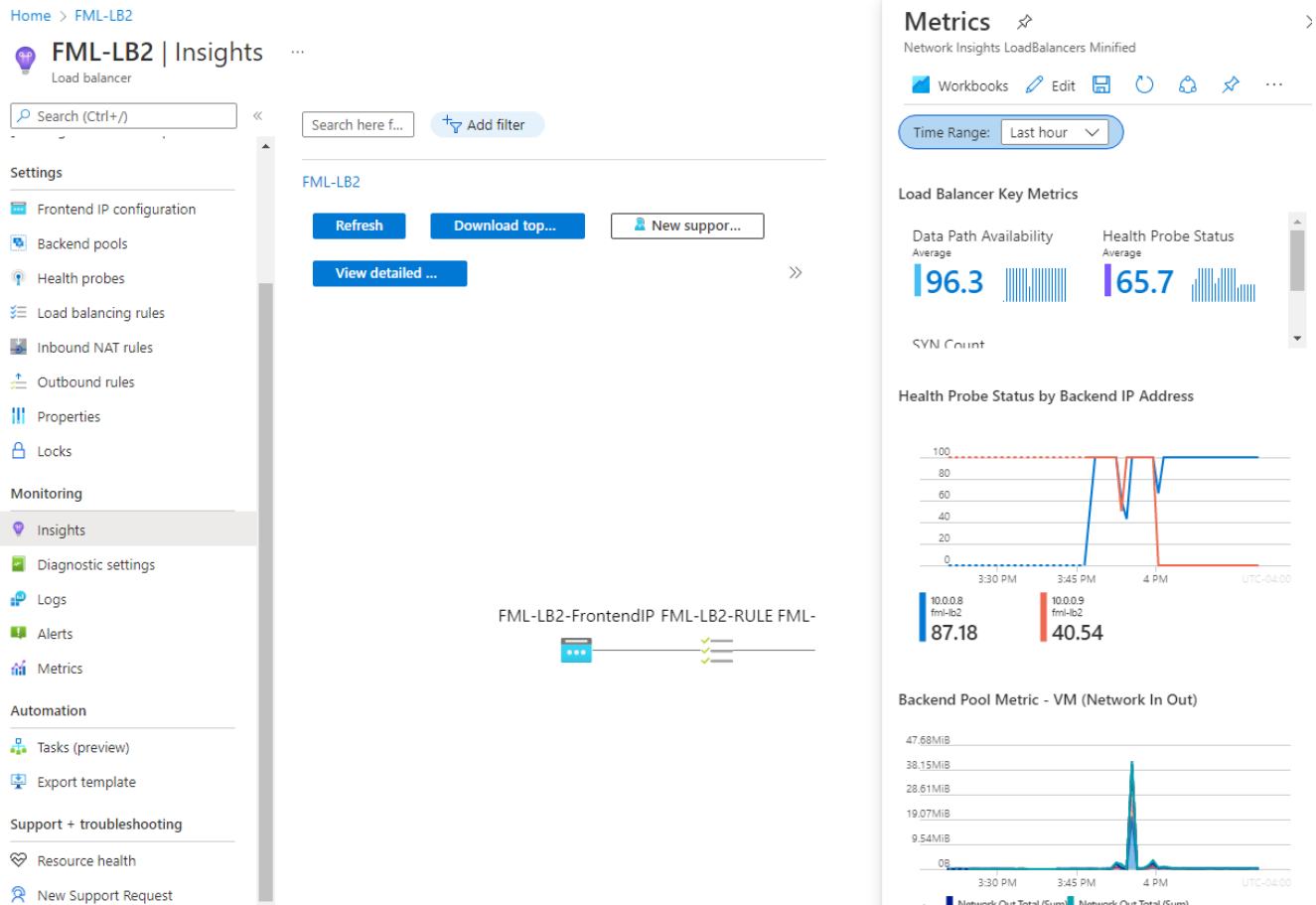
+ Add X Remove

Virtual machine ↑↓ IP Configuration ↑↓ Availability set ↑↓

No virtual machines selected

Monitoring FortiMail-VM Health with Azure Load Balancer

You can monitor the FortiMail HA status with Azure Load Balancer. Refer to the Microsoft Azure Guide for more details about the monitoring and distributing traffic functions.





www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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. 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.