



# FortiWeb KVM Active-Passive HA Cluster with Unicast Heartbeat Setup Guide

**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/training-certification>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



---

## TABLE OF CONTENTS

<b>Prerequisites .....</b>	<b>4</b>
<b>Configuring FortiWeb Active-Passive HA cluster with Unicast Heartbeat .....</b>	<b>5</b>
<b>Failover test .....</b>	<b>7</b>

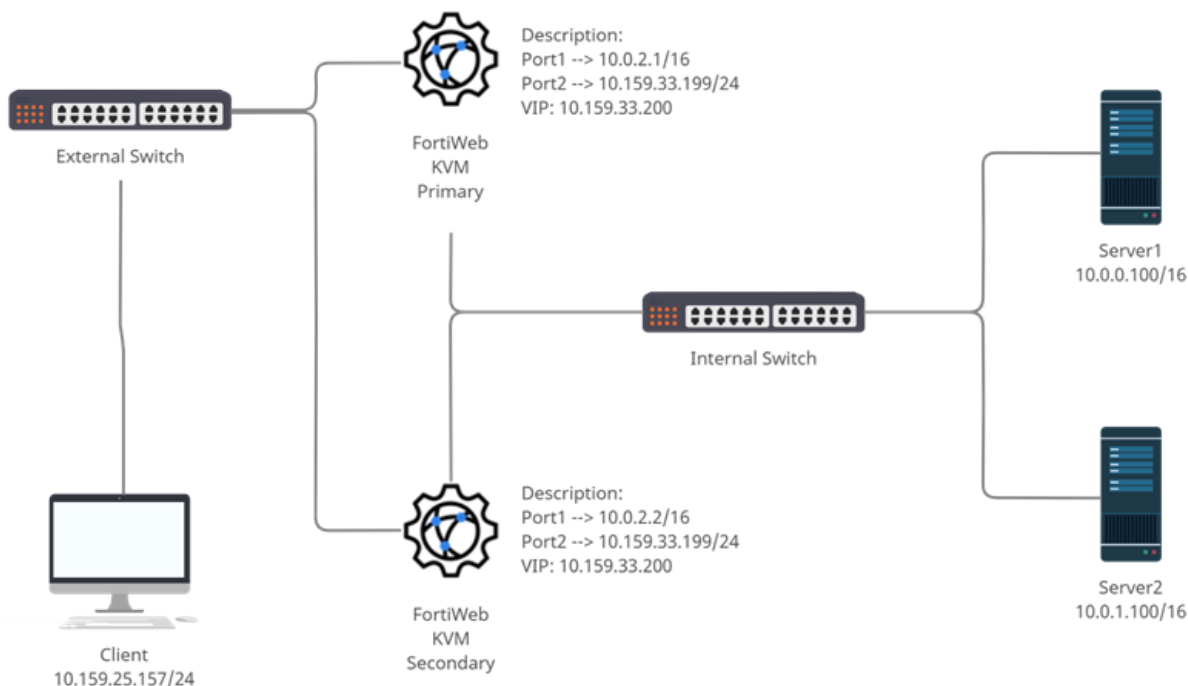
# Prerequisites

In this article, we assume you already have deployed the following:

- Two FortiWeb-VMs running on KVM. The FortiWeb version should be 7.0.1 or higher, and they should be in Reverse Proxy mode.
- Client (Ubuntu 18.04) \* 1
- Server (Ubuntu 18.04) \* 2

In the following sections, we will use an example to illustrate the steps. In this example, there is a server policy configured with VIP 10.159.33.200, and the real servers' IP addresses are 10.0.0.100 & 10.0.1.100.

Refer to the network diagram below.



# Configuring FortiWeb Active-Passive HA cluster with Unicast Heartbeat

1. Log in to either one of the FortiWeb-VM.
2. Go to **System > High Availability > Settings**.
3. Select **Active-Passive** mode in drop down list.
4. Select **UDP Tunnel** for **Network Type**.
5. Set **Group ID** as 18 to avoid HA cluster conflict.
6. Set **Local IP Address** and **Peer IP Address** as **10.0.2.1** and **10.0.2.2**.
7. Select port1 for Reserved Management Interface. UDP unicast requires at least one Reserve interface.

Please note that the **Local IP Address** and **Peer IP Address** should be configured with the IP addresses that are bound to the Reserved Management Interface, otherwise they will be synchronized across the HA nodes in active-passive HA mode.

FortiWeb-KVM FortiWeb

Dashboard > High Availability Configuration

Network >

System > High Availability > Settings

Config >

High Availability >

Settings

Admin >

Maintenance >

Security Fabric >

User >

Policy >

Server Objects >

Application Delivery >

Web Protection >

Bot Mitigation >

API Protection >

DoS Protection >

IP Protection >

Tracking >

Machine Learning >

Log&Report >

High Availability Configuration

Mode: Active-Passive

Device Priority: 2 (0-9)

Override: ☒

Networking Settings

Network Type: UDP Tunnel

Cluster Settings

Group-name:

Group ID: 18

Local IP Address: 10.0.2.1

Peer IP Address: 10.0.2.2

Layer 7 Persistence Synchronization: ☒

Monitor Interface: port2

HA Member

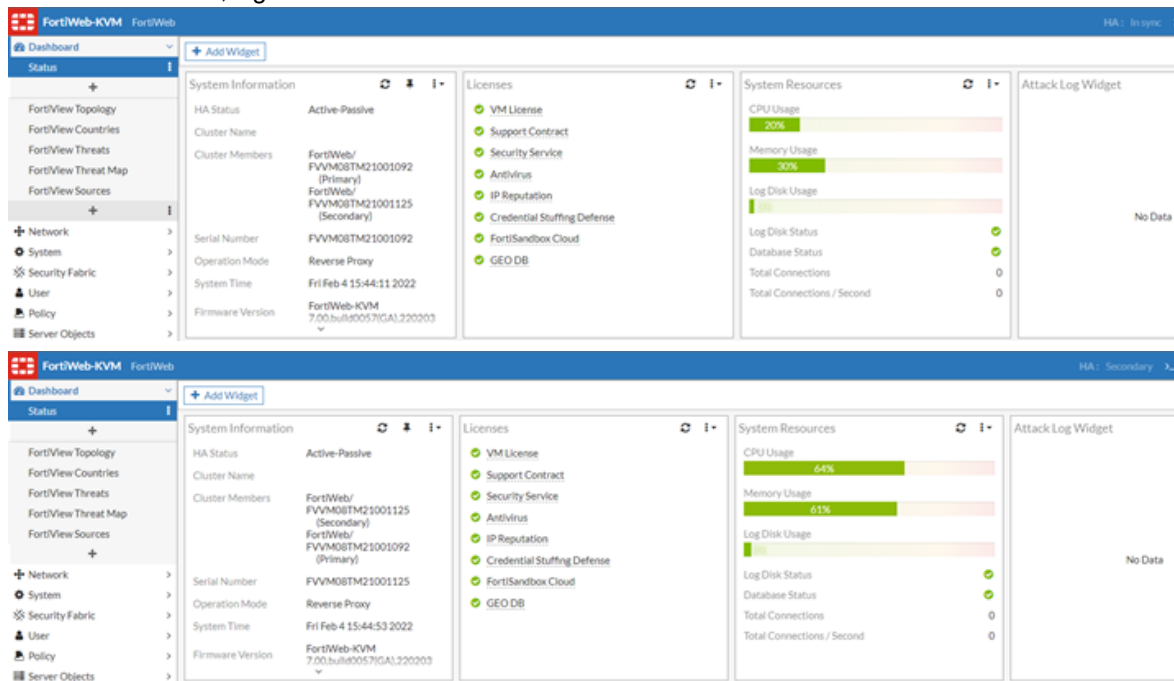
Reserved Management Interface

Interface: port1

Apply

8. Click **Apply**.
9. Configure the second FortiWeb-VM with the same settings, except **Local IP Address** as 10.0.2.2 and **Peer IP Address** as 10.0.2.1, the Device Priority with a different value. The device with a lower priority value will take the primary role.

10. After a few minutes, log in to both of the FortiWeb-VM GUI. You should see the correct HA info.



## CLI Commands

### Primary device:

```
FortiWeb # config system ha
FortiWeb (ha) # set mode active-passive
FortiWeb (ha) # set network-type udp-tunnel
FortiWeb (ha) # set override enable
FortiWeb (ha) # set priority 1
FortiWeb (ha) # set group-id 18
FortiWeb (ha) # set tunnel-local 10.0.2.1
FortiWeb (ha) # set tunnel-peer 10.0.2.2
FortiWeb(ha) # set ha-mamt-status enable
FortiWeb(ha) # set ha-mgmt-interface port1
FortiWeb (ha) # end
```

### Secondary device:

```
FortiWeb # config system ha
FortiWeb (ha) # set mode active-passive
FortiWeb (ha) # set network-type udp-tunnel
FortiWeb (ha) # set override enable
FortiWeb (ha) # set priority 5
FortiWeb (ha) # set group-id 18
FortiWeb (ha) # set tunnel-local 10.0.2.2
FortiWeb (ha) # set tunnel-peer 10.0.2.1
FortiWeb(ha) # set ha-mamt-status enable
FortiWeb(ha) # set ha-mgmt-interface port1
FortiWeb (ha) # end
```

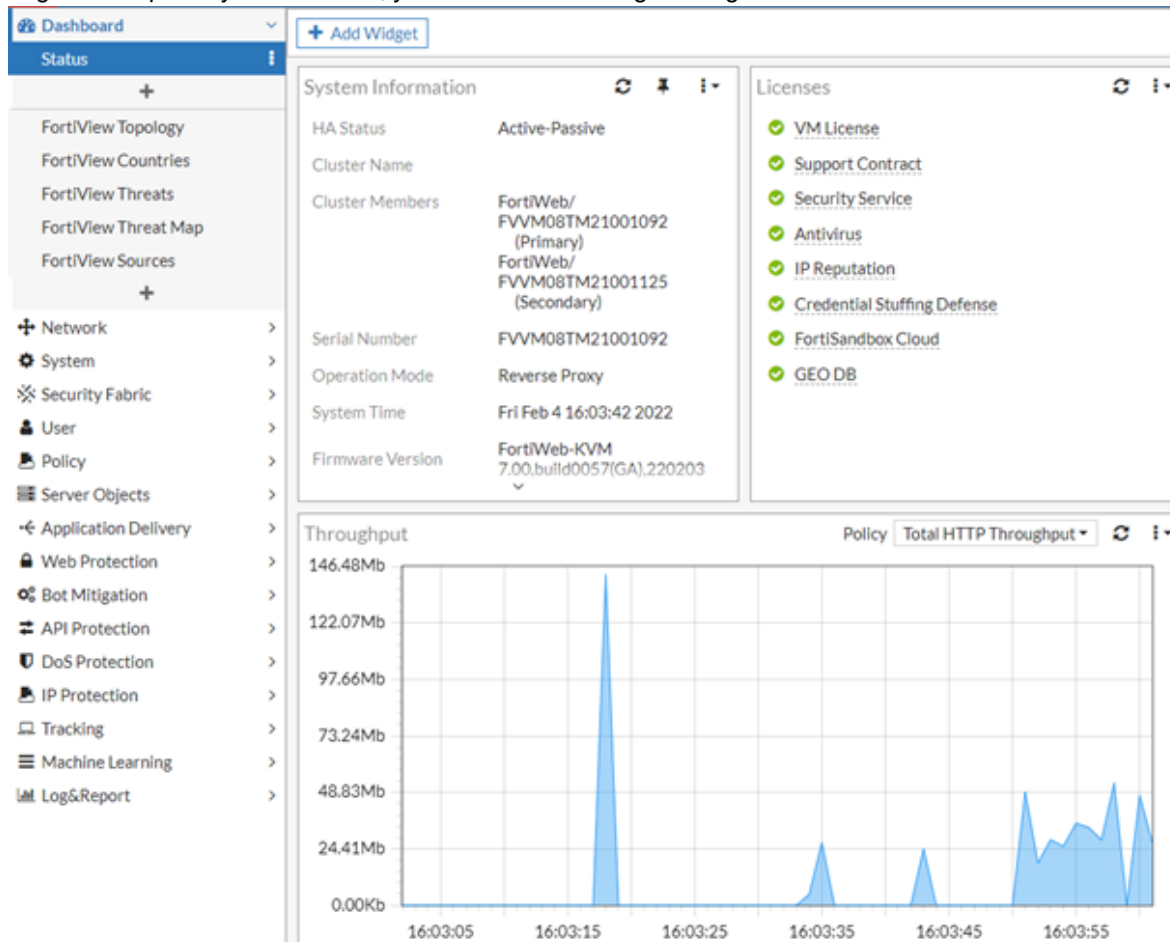
# Failover test

1. From the Client side, request VIP 10.159.33.200.

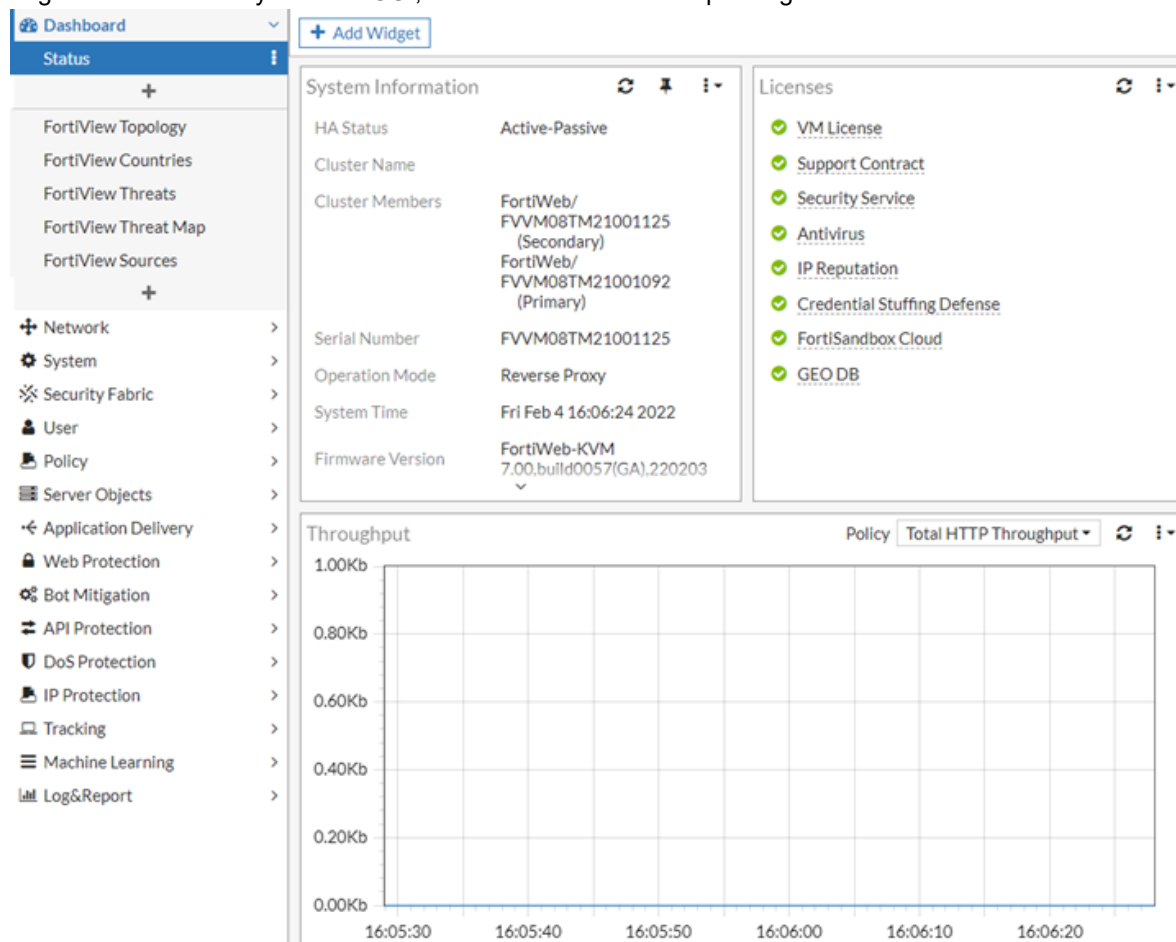
```
root@ubuntu:~# wget http://10.159.33.200:8090/large --limit-rate=4000000
--2022-02-04 16:03:49-- http://10.159.33.200:8090/large
Connecting to 10.159.33.200:8090... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10737418240 (10G)
Saving to: 'large.1'

large.1                                     15[>
165.00M  9.81MB/s
```

2. Log in to the primary device's GUI, you should see traffic go through.



3. Log in to the secondary device's GUI, there should be no traffic passing.

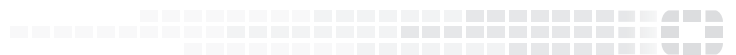


4. Change the Secondary device's priority to 1 so that it could take over as primary device.
5. Log in to the former primary device's GUI. You should see that its role change to secondary and there isn't traffic passing.





**FORTINET®**



Copyright© 2022 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.