# 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

# TABLE OF CONTENTS

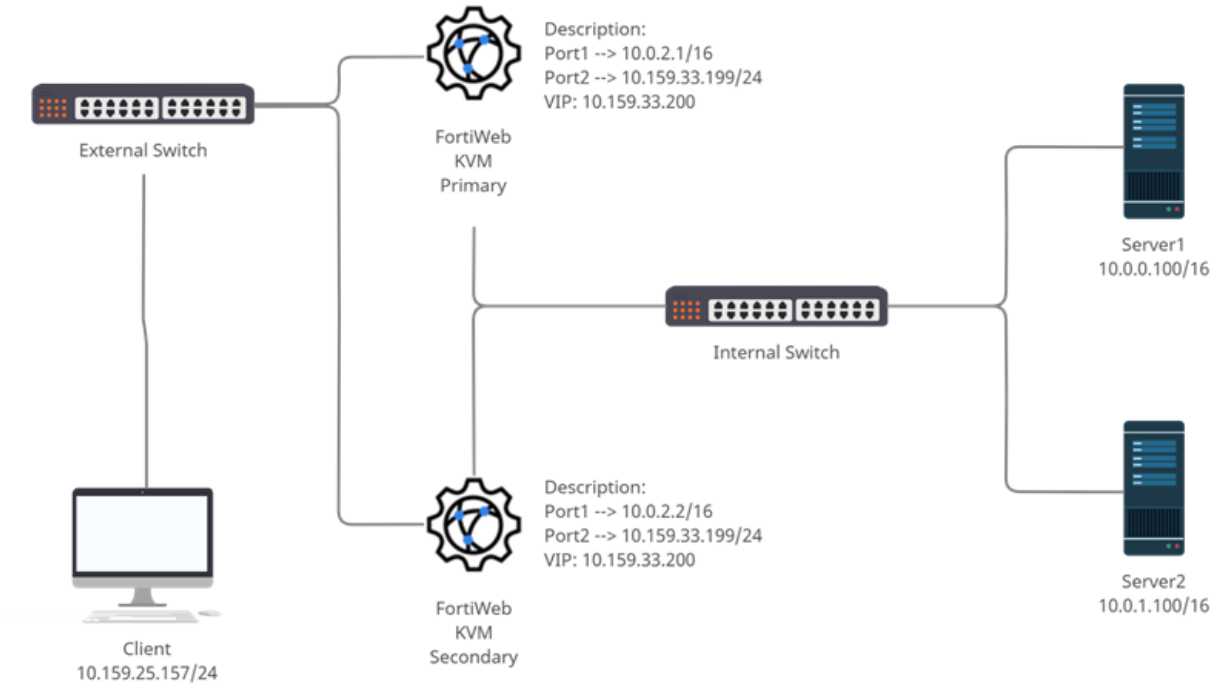
# Prerequisites

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
- Sever (Ubuntu 18.04) * 2

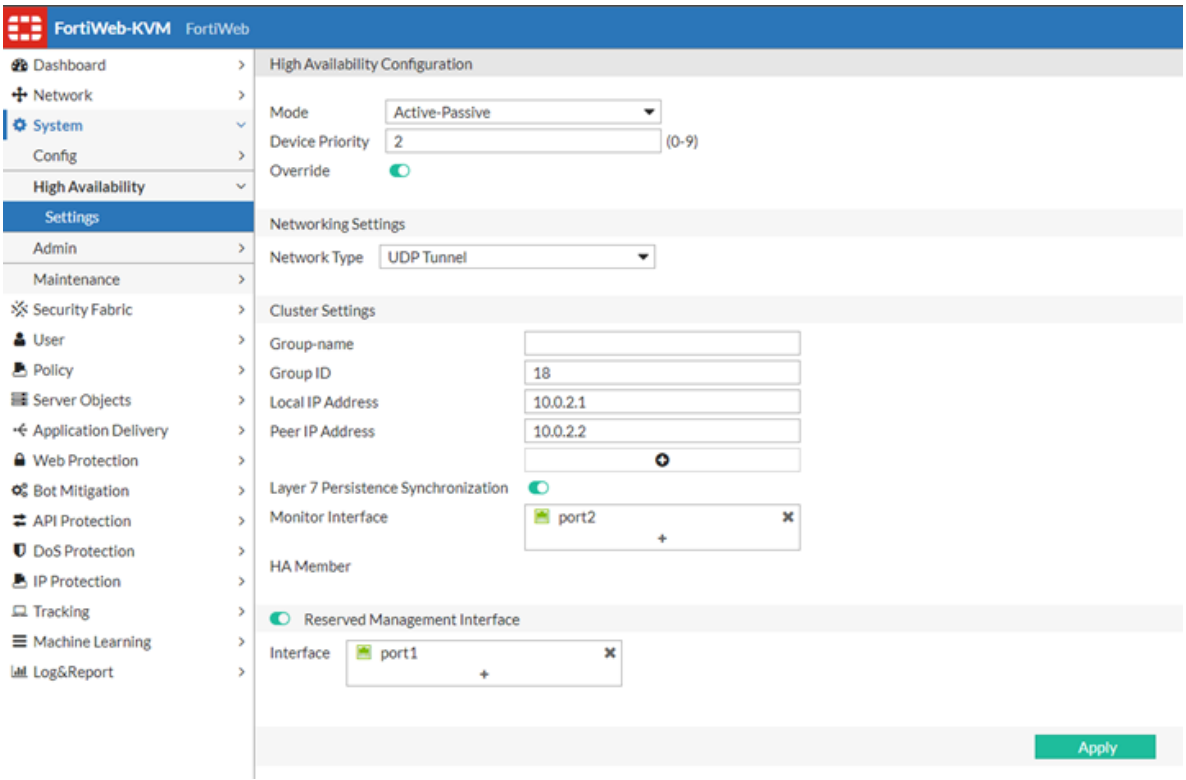
In the following sections, we will use an example to illustrate the steps. In this example, there is a server policy configured with VIP 10.159.33.200, and the real servers' IP addresses are 10.0.0.100 & 10.0.1.100.

Refer to the network diagram below.



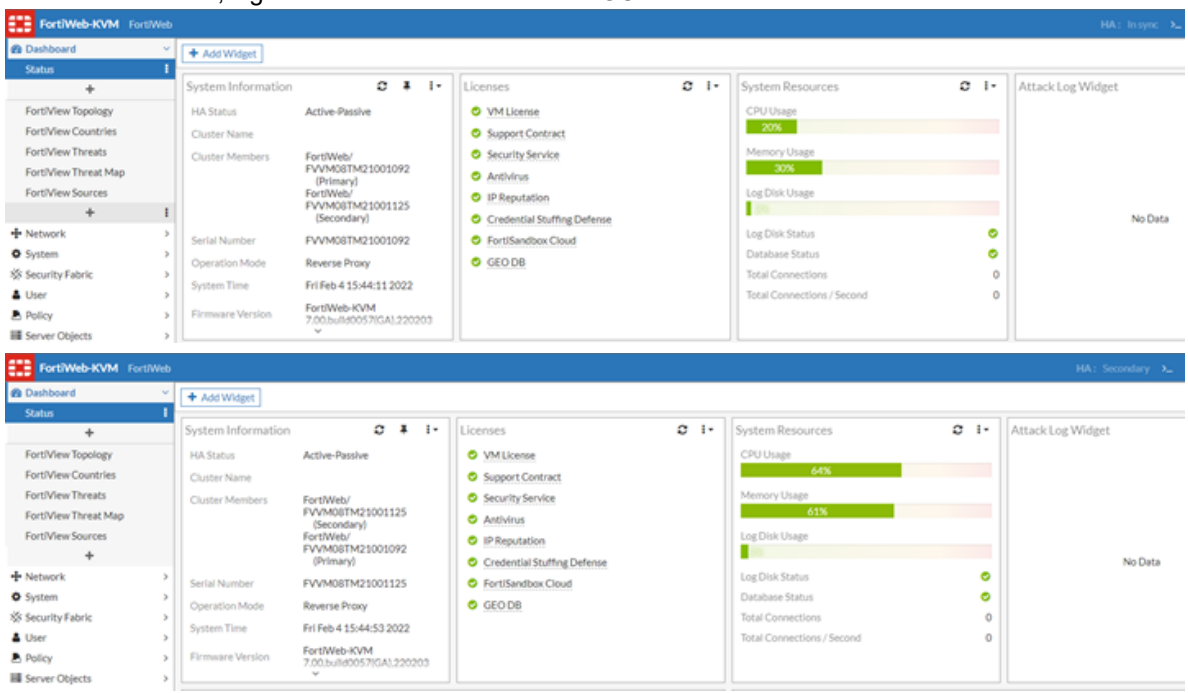
# Configuring FortiWeb Active-Passive HA cluster with Unicast Heartbeat

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.




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
```

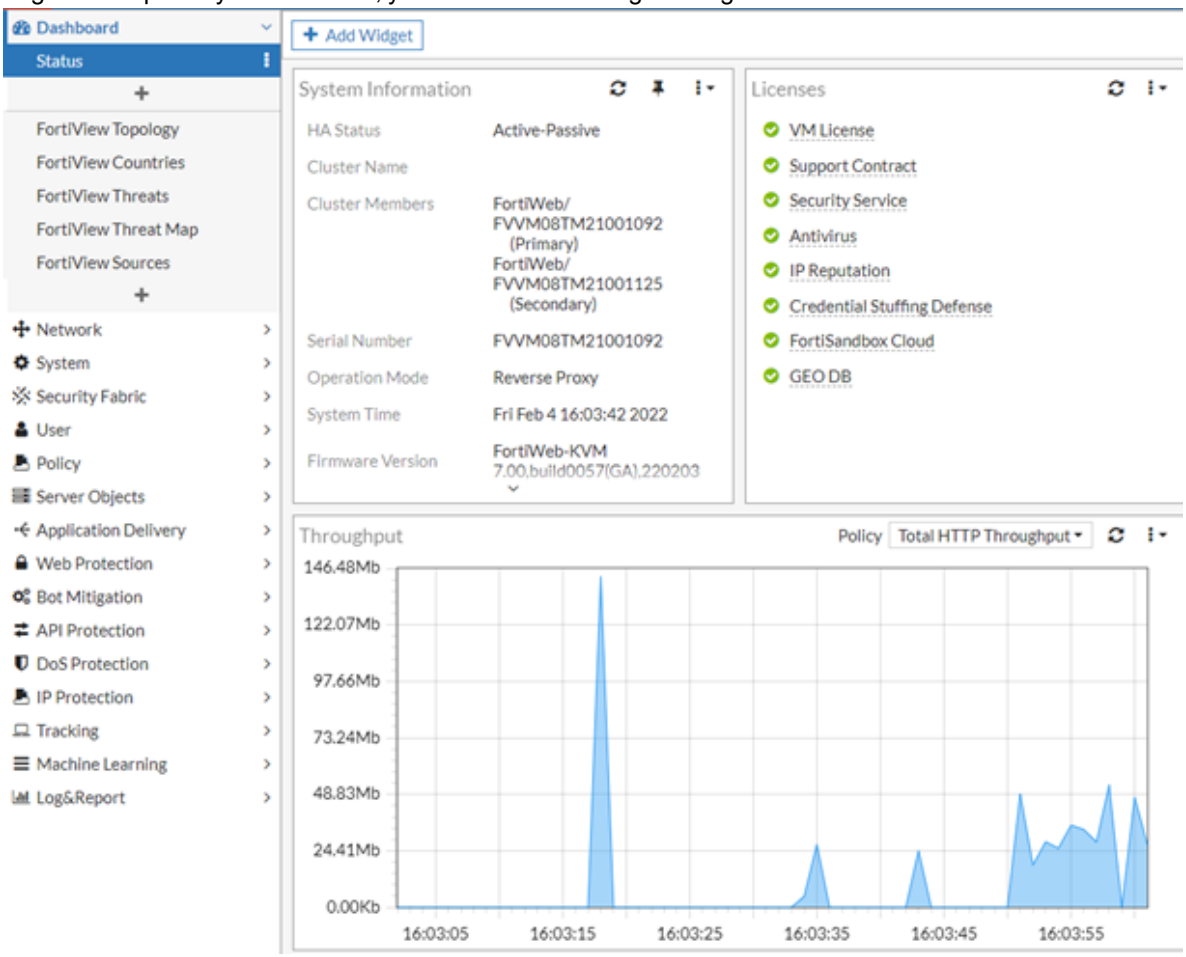
Secondary device:

```
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
```

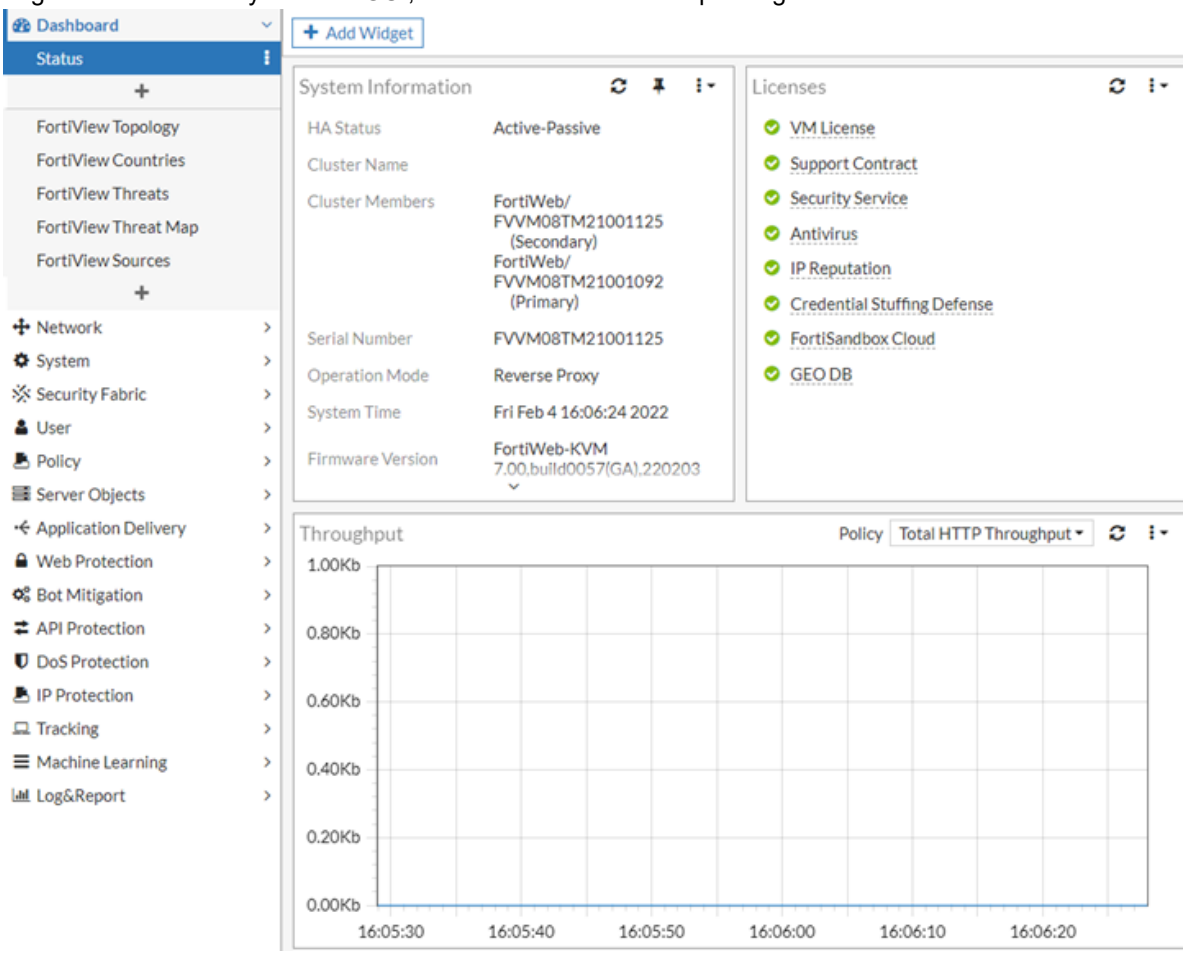
# Failover test

1. From the Client side, request VIP 10.159.33.200.


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.