Configuring HA cluster between two Fortigate units:

A FortiGate HA cluster consists of two to four FortiGate's configured for HA operation. Each FortiGate in a cluster is called a cluster unit. All cluster units must be the same FortiGate model with the same FortiOS firmware build installed. All cluster units must also have the same hardware configuration (for example, the same number of hard disks and so on) and be running in the same operating mode (NAT mode or transparent mode).

Good to know:

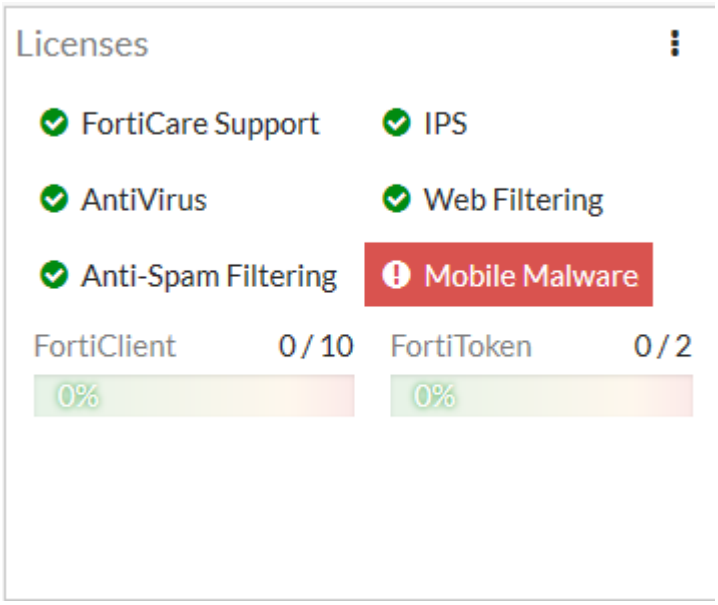
- Make sure your FortiGate interfaces are configured with static IP addresses. If any interface gets its address using DHCP or PPPoE you should temporarily switch it to a static address and enable DHCP or PPPoE after the cluster has been established.
- Make sure the FortiGates are running the same FortiOS firmware version.
- All the FortiGates in a cluster must have the same level of licensing.

Basic configuration steps

Each FortiGate in the cluster must have the same HA configuration. Once the cluster is connected, you can configure it in the same way as you would configure a standalone FortiGate. The following example sets the HA mode to active-passive and the HA password to HA_pass.

Make sure your FortiGate interfaces are configured with static IP addresses. If any interface gets its address using DHCP or PPPoE you should temporarily switch it to a static address and enable DHCP or PPPoE after the cluster has been established.

Make sure both FortiGates are running the same FortiOS firmware version. Register and apply licenses to both FortiGates before adding them to the cluster. This includes licensing for FortiCare Support, IPS, AntiVirus, Web Filtering, Mobile Malware, FortiClient, FortiCloud, and additional virtual domains (VDOMs). All FortiGates in the cluster must have the same level of licensing for FortiGuard, FortiCloud, FortiClient, and VDOMs. FortiToken licenses can be added at any time because they are synchronized to all cluster members.



You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed, third-party certificates are synchronized to the backup FortiGate.

To configure a FortiGate for HA operation - GUI

1. Power on the FortiGate to be configured.

2. Log into the GUI.

3. Locate the System Information Dashboard widget. Click on the System Information dashboard widget and select **Configure settings in System > Settings**.

4. Enter a new Host Name for this FortiGate.
   Changing the host name makes it easier to identify individual cluster units when the cluster is operating.

5. Go to **System > HA** and change the following settings:

   Mode Active-Passive
   Group Name Example_cluster
   HA_pass
   Password
   The password must be the same for all FortiGates in the cluster.

6. You can accept the default configuration for the remaining HA options and change them later, once the cluster is operating.

6. Select **OK**.
   The FortiGate negotiates to establish an HA cluster. When you select **OK** you may temporarily lose connectivity with the FortiGate as the HA cluster negotiates and the

FGCP changes the MAC address of the FortiGate interfaces. To be able to reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate (or just deleting all ARP table entries). You may be able to delete the ARP table of your management PC from a command prompt using a command similar to arp -d.

7. Power off the FortiGate.

8. Repeat this procedure for all of the FortiGates in the cluster.
   Once all of the units are configured, continue by connecting the FortiGate HA cluster below.

To configure a FortiGate for HA operation - CLI

1. Power on the FortiGate to be configured.

2. Log into the CLI.

3. Enter the following command to change the FortiGate host name.

   config system global

   set hostname Example1_host

   end

   Changing the host name makes it easier to identify individual cluster units when the cluster is operating.

4. Enter the following command to enable HA:

   config system ha

   set mode active-passive

   set group-name Example_cluster

   set password HA_pass

   end

   You can accept the default configuration for the remaining HA options and change them later, once the cluster is operating.

   The FortiGate negotiates to establish an HA cluster. You may temporarily lose connectivity with the FortiGate as the HA cluster negotiates and because the FGCP changes the MAC address of the FortiGate interfaces. To be able to reconnect sooner, you can update the ARP table of your management PC by deleting the ARP

table entry for the FortiGate (or just deleting all arp table entries). You may be able to delete the arp table of your management PC from a command prompt using a command similar to arp -d.

5. Power off the FortiGate.

6. Repeat this procedure for all of the FortiGates in the cluster.
   Once all of the units are configured, continue with connecting the FortiGate HA cluster.

Connecting a FortiGate HA cluster

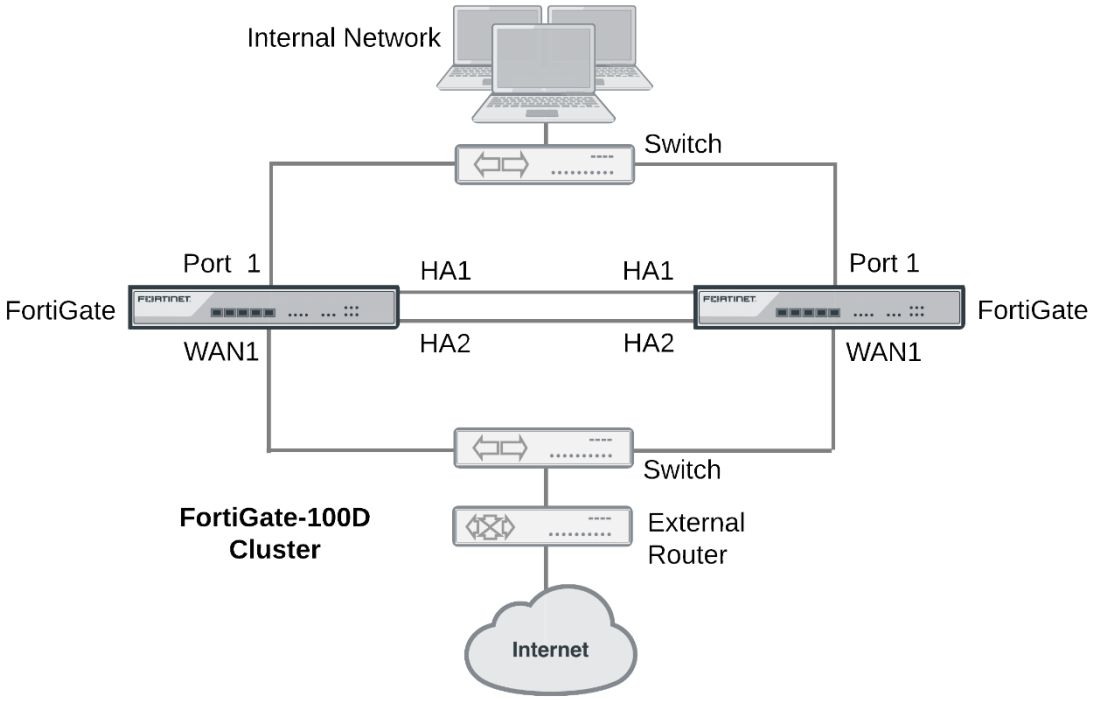
Use the following procedure to connect a cluster. Connect the cluster units to each other and to your network. You must connect all matching interfaces in the cluster to the same switch, then connect these interfaces to their networks using the same switch.

Although you can use hubs, Fortinet recommends using switches for all cluster connections for the best performance.

Connecting an HA cluster to your network temporarily interrupts communications on the network because new physical connections are being made to route traffic through the cluster. Also, starting the cluster interrupts network traffic until the individual cluster units are functioning and the cluster completes negotiation. Cluster negotiation is automatic and normally takes just a few seconds. During system startup and negotiation all network traffic is dropped.

This section describes how to connect the cluster shown below, which consists of two FortiGate-100D units to be connected between the internet and a head office internal network. The wan1 interfaces of the FortiGate connect the cluster to the internet and the internal interfaces connect the cluster to the internal network. The ha1 and ha2 interfaces are used for redundant HA heartbeat links.

Example cluster connections



To connect a FortiGate HA cluster

1. Connect the WAN1 interfaces of each cluster unit to a switch connected to the internet.

2. Connect the Port1 interfaces of each cluster unit to a switch connected to the internal network.

3. Connect the HA1 interfaces of the cluster units together. You can use a crossover Ethernet cable or a regular Ethernet cable. (You can also connect the interfaces using Ethernet cables and a switch.)

4. Connect the HA2 interfaces of the cluster units together. You can use a crossover Ethernet cable or a regular Ethernet cable. (You can also connect the interfaces using Ethernet cables and a switch.)

5. Power on both FortiGates.

   As the cluster units start, they negotiate to choose the primary unit and the subordinate unit. This negotiation occurs with no user intervention and normally just takes a few seconds.

   At least one heartbeat interface should be connected together for the cluster to operate.

   Do not use a switch port for the HA heartbeat traffic. This configuration is not supported.

You could use one switch to connect all four heartbeat interfaces. However, this is not recommended because if the switch fails both heartbeat interfaces will become disconnected.

6. You can now configure the cluster as if it is a single FortiGate.

Verifying the cluster status from the HA Status dashboard widget

The HA Status dashboard widget shows the mode and group names of the cluster, the status of the cluster units and their host names, the cluster uptime and the last time the cluster state changed. A state change can indicate the cluster first forming or one of the cluster units changing its role in the cluster.

The HA Status Dashboard widget also shows if the cluster units are synchronized. Mouse over each FortiGate in the cluster to verify that they both have the same checksum.