How to Configure High Availability CC-Managed CloudGen Firewalls for Virtual Routing

https://campus.barracuda.com/doc/96026380/

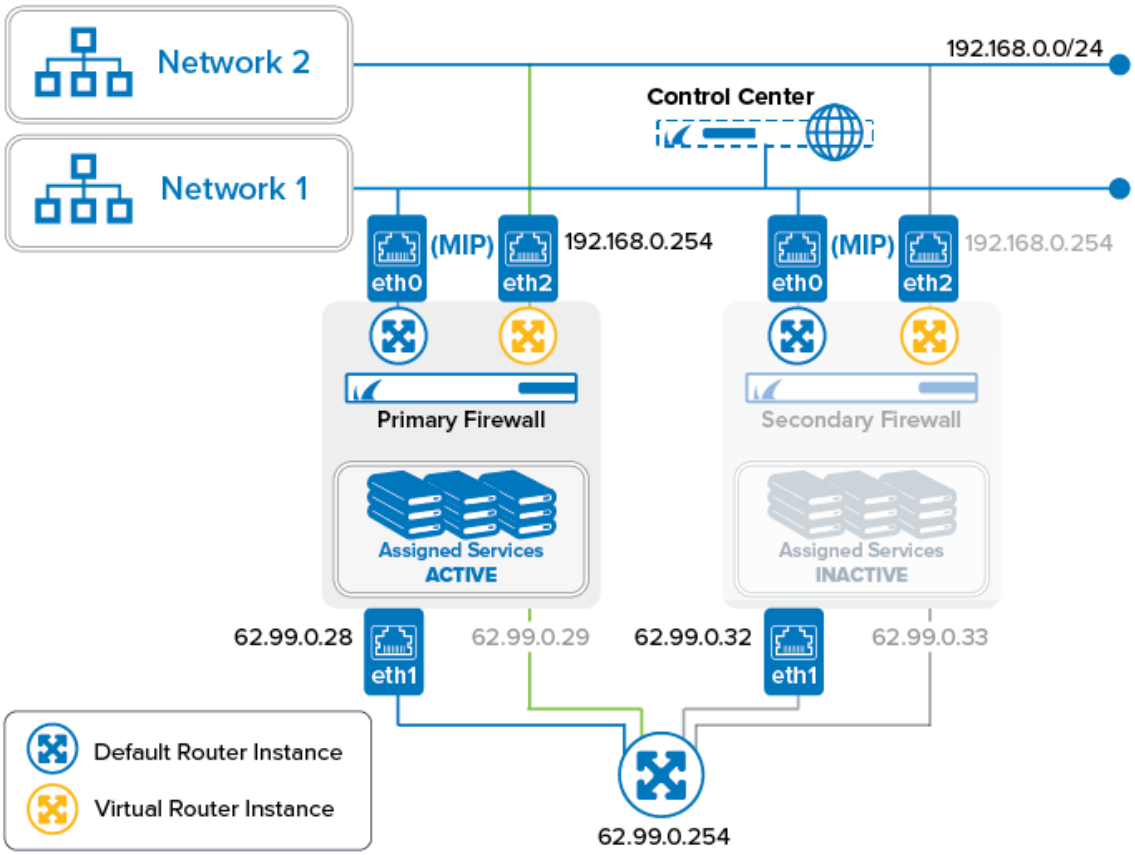
When configuring a virtual router instance for a CC-managed HA pair, the configuration is transparently transferred to the secondary firewall after being completed for the primary firewall. There is no need to make any configuration for the secondary firewall.

Before You Begin

Verify that two firewalls are operating in high availability mode. For more information, How to Set Up a Managed High Availability Cluster from Scratch.

Configuration

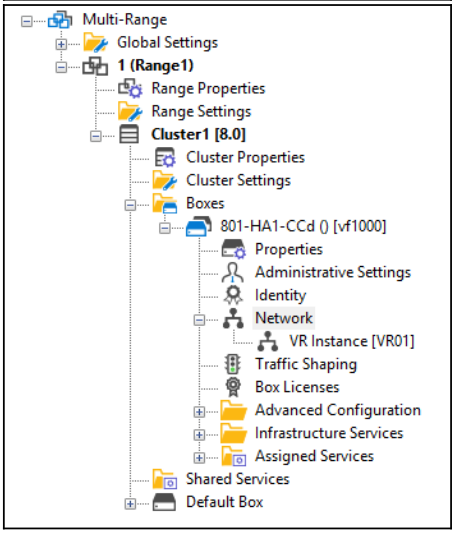
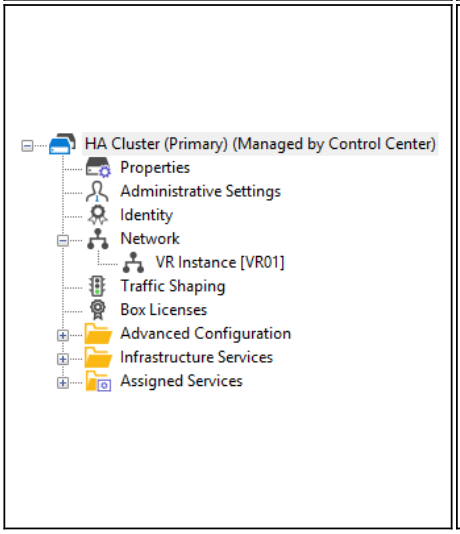
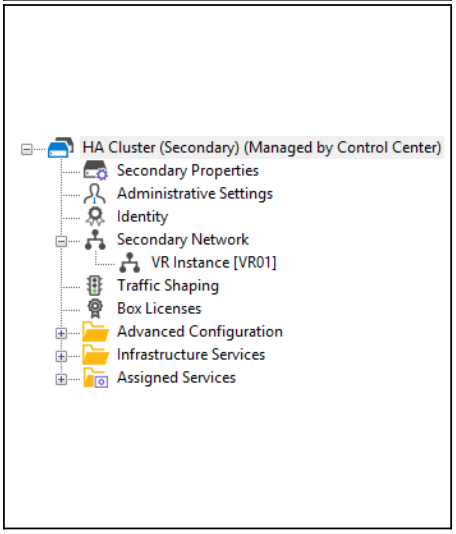
In the following example, an additional virtual instance will be created that routes traffic between a private network (e.g., 192.168.0.0/24) and the Internet. In this setup, the firewall service will be transparent to the additional virtual router instance only if authenticated users are not defined. All other services are not available to the additional virtual router. For more information on which services are available for additional virtual instances, see Virtual Routing and Forwarding (VRF).



Step 1. On the CC, Create a Virtual Router Instance for the Primary Firewall

When creating a router instance for the primary firewall, the configuration will be mirrored to the secondary firewall.

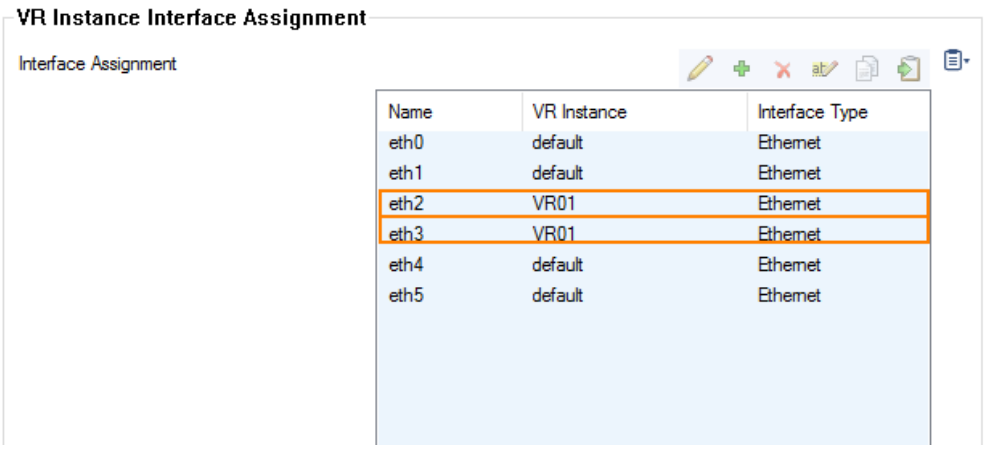
1. Log into the Control Center.
2. Right-click **CONFIGURATION > Configuration Tree > Multi Range > *your range* > *your cluster* > Boxes > *your primary firewall* > Network**.
3. Select **Lock**.
4. Right-click **CONFIGURATION > Configuration Tree > Multi Range > *your range* > *your cluster* > Boxes > *your primary firewall* > Network**.
5. Select **Create VR Instance** from the list.
6. The **Create a new VR Instance** window is displayed.
7. The window for naming the virtual router is displayed.
8. Enter the name for the virtual router, e.g., `VR01`.
9. Click **OK**.
10. Click **Send Changes**.
11. The **Activate Changes** window opens.
12. Click **Activate**.

VR Node configured in Control Center	VR Node on Managed Primary Firewall	VR Node on Managed Secondary Firewall
		

Step 2. Assign Interfaces to the VR Instance

The configuration for the interfaces will be forwarded from the primary to the secondary HA partner.

1. On your Control Center, double-click **CONFIGURATION > Configuration Tree > Multi Range > *your range* > *your cluster* > Boxes > *your primary firewall* > Network**.
2. In the left menu bar, click **Virtual Router**.
3. Click **Lock**.
4. In the **Interface Assignment** list, double-click the first interface to assign the VR Instance, e.g., **eth2**.
5. The **Interface Assignment** window is displayed.
6. For **VR Instance**, select **VR01**.
7. Click **OK**.
8. In the **Interface Assignment** list, double-click the second interface to assign the VR Instance, e.g., **eth3**.
9. The **Interface Assignment** window is displayed.
10. For **VR Instance**, select **VR01**.
11. Click **OK**.
12. Click **Send Changes**.
13. Click **Activate**.

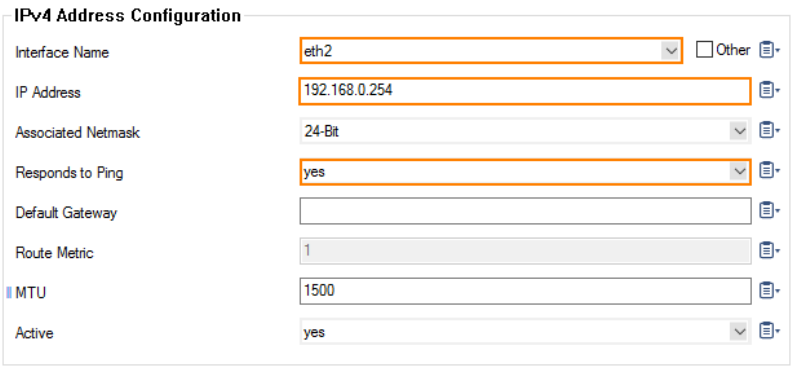


Step 3. Re-activate the New Network Configuration

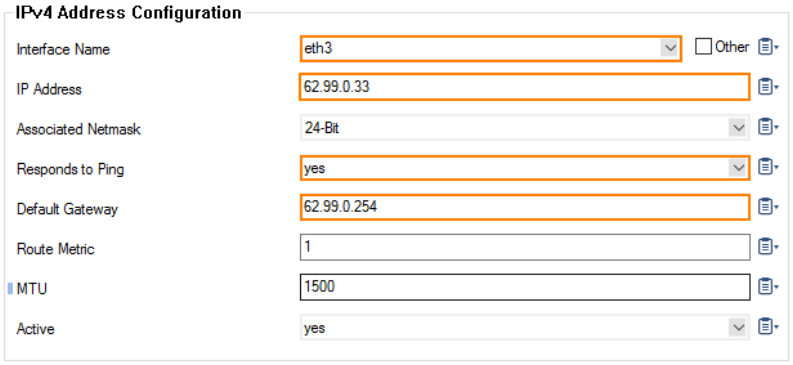
1. Log into your primary firewall.
2. On your primary HA firewall, go to **CONTROL > Box**.
3. In the left menu, click **Network** to expand the menu.
4. Click **Activate new network configuration**.
5. The **Network Activation** window is displayed.
6. Click **Failsafe**.
7. Log into you secondary firewall.
8. On your secondary HA firewall, go to **CONTROL > Box**.
9. In the left menu, click **Network** to expand the menu.
10. Click **Activate new network configuration**.
11. The **Network Activation** window is displayed.
12. Click **Failsafe**.

Step 4. Assign IP Addresses to the Interfaces of the VR Instance

1. On your Control Center, go to **CONFIGURATION > Configuration Tree > Multi-Range > *your range* > *your cluster* > Boxes > *your primary firewall* > Network > VR Instance [*your virtual instance*]**.
2. In the left menu bar, select **IP Configuration**.
3. Click **Lock**.
4. Click **+** to assign the first IP address to the first interface, e.g., eth2 = `192.168.0.254`.
5. The **IPv4 Addresses** window is displayed.
6. Enter the name for the first IP address to interface assignment, e.g., `VRF-to-CLASSROOM1`.
7. Enter the **IPv4 Address Configuration**
    1. **Interface Name** – **eth2**
    2. **IP Address** – Enter the private network address, e.g., `192.168.0.254`.
    3. **Responds to Ping** – **yes**.



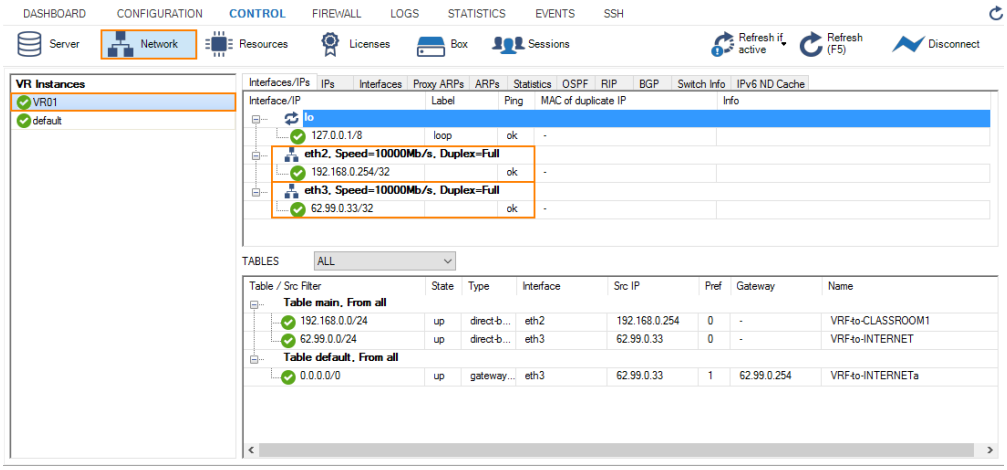
8. Click **OK**.
9. Click **+** to assign the second IP address to the first interface, e.g., eth3 = 62.99.0.33.
10. The **IPv4 Addresses** window is displayed.
11. Enter the name for the second IP address to interface assignment, e.g., `VRF-to-INTERNET`.
12. Enter the **IPv4 Address Configuration**
    1. **Interface Name** – **eth3**
    2. **IP Address** – Enter the private network address, e.g. `62.99.0.33`.
    3. **Responds to Ping** – **yes**.
    4. **Default Gateway** – Enter the IP address for the Internet gateway, e.g., `62.99.0.254`.



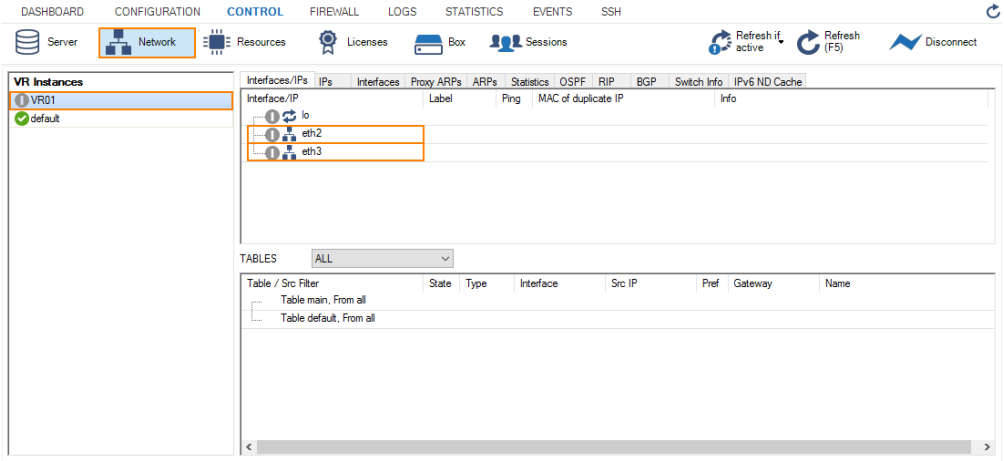
13. Click **OK**.
14. Click **Send Changes**.
15. The **Activate Changes** window opens.
16. Click **Activate**.

Step 5. Verify Your Configuration on Both HA Partners

On the primary firewall, go to **CONTROL > Network** and click **VR01**. In case the primary firewall is the active one, the interfaces with its IP addresses are displayed as configured.



On the secondary firewall, go to **CONTROL > Network.** In case the secondary firewall is the passive one, the VR01 instance is displayed in gray with the assigned IP addresses being invisible.



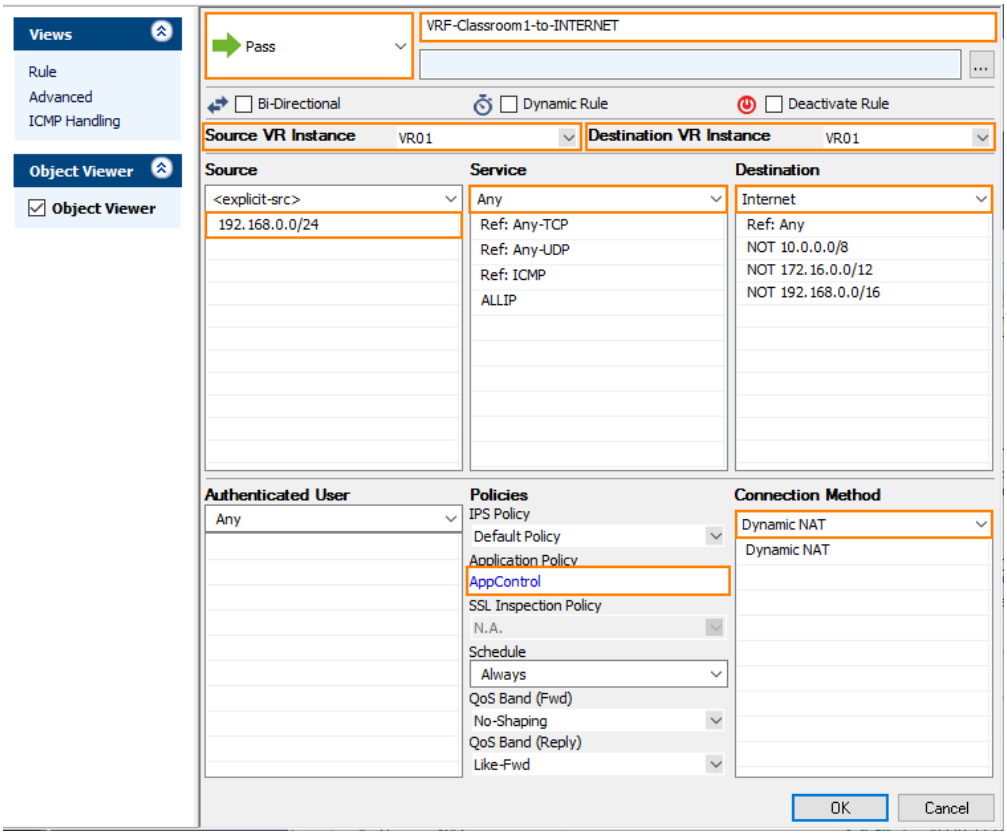
To activate the reverse HA constellation, perform an HA failover. For more information, see How to Perform a Manual High Availability Failover. The upper two images will then be displayed with reversed configuration information accordingly .

Step 6. Create an Access Rule for the Newly Created Virtual Router VR01

To pass traffic from interface eth2 (192.168.0.254/32) to eth3 (62.99.0.29/32), create an access rule and constrain the access rule to the virtual router VR01.

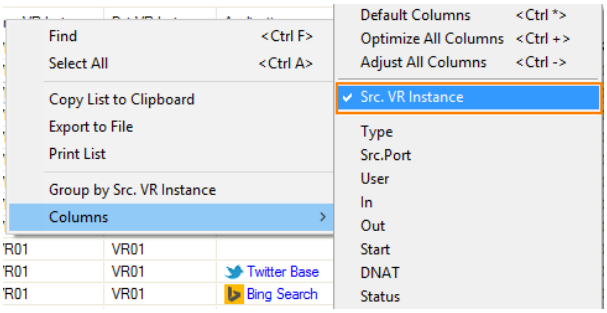
1. On your Control Center, go to **CONFIGURATION > Configuration Tree > Multi-Range > *your range* > *your cluster* > Boxes > *your primary firewall* > Assigned Services > NGFW (Firewall) > Forwarding Rules**.
2. Click **Lock**.
3. Click **+** to add an access rule.
4. For the access rule type, select **Pass**.
5. Enter a name for the access rule. To differentiate between rules that apply to the default router instance, and for a clearer overview, it is recommended to prepend a prefix like 'VRF' or 'VR01' to the name of the access rule, e.g., `VRF-Classroom-to-INTERNET`.

6. **Source VR Instance** – Select the name of the virtual router instance, e.g. **VR01**.
7. **Destination VR Instance** – Select the name of the virtual router instance, e.g. **VR01**.
8. **Source** – Enter the IP address of the source network, e.g., `192.168.0.0/24`.
9. **Service** – Select **Any**.
10. **Destination** – Enter the IP address for the Internet from the list.
11. **Application Policy** – In case you have licensed Application Control, you can activate it now.
12. **Connection Method** – Select **Dynamic NAT**.
13. Click **OK.**
14. Click **Send Changes**.
15. Click **Activate**.



Step 7. Activate Columns to Display the Traffic Flow Through Your Virtual Router Instance

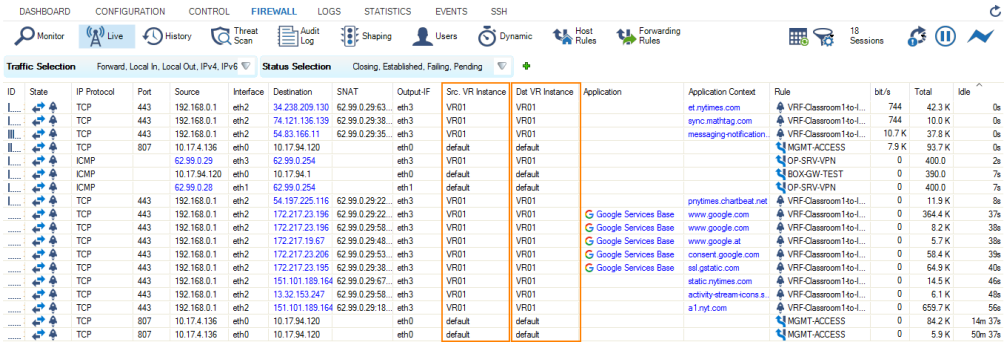
1. On your primary firewall, go to **FIREWALL > Live**.
2. Right-click on any of the column identifiers of the Live view.
3. From the menu, select **Columns -> Src. VR Instance**.
4. Right-click on any of the column identifiers of the Live view.
5. From the menu, select **Columns -> Dst. VR Instance**.



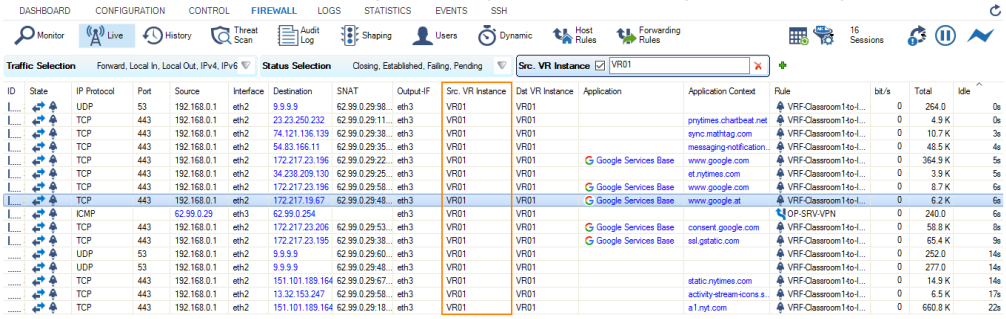
Step 8. Verify that Traffic is Flowing from the Source Network to the Internet

Set up a client with an IP address in the source network (e.g., `192.168.0.1`), and set the default route on the client to the address of the virtual router, e.g., `192.168.0.254`.

1. On your client, open a web browser and go to a website of your choice, e.g., www.nytimes.com
2. On your primary firewall, go to **FIREWALL > Live**.
3. The **Live** view will display a mixture of traffic flowing both through the default router and the virtual router you configured before, e.g., VR01.



4. In order to restrict display output only to the URL you entered before, activate a display filter for the virtual router instance by clicking on the filter symbol in any of the lines showing VR01.



Figures

1. vr_ha_managed_80.png
2. ha_VR_node_created_in_CC.png
3. ha_VR_node_created_on_primary_managed.png
4. ha_VR_node_created_on_secondary_managed.png
5. vrf_HA_primary_network_node_configured.png
6. vrf_HA_configure_primary_interface.png
7. vrf_HA_configure_second_interface.png
8. vrf_HA_configuration_complete_HA1.png
9. vrf_HA_configuration_complete_HA2.png
10. vrf_enter_access_rule_for_vr01.png
11. vrf_select_vr_column_to_display.png
12. vrf_traffic_flowing_through_all_router_instances.png
13. traffic_flowing_only_through_VR01.png