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

https://campus.barracuda.com/doc/77401026/

When configuring VRF for two CC-managed firewalls, the box level configuration for both firewalls must be identical, except for the **Network**, **Box Properties**, and **Licensing** pages. Furthermore, both the names of all virtual router instances and the **VR Instance IDs** must also match each other on both firewalls.

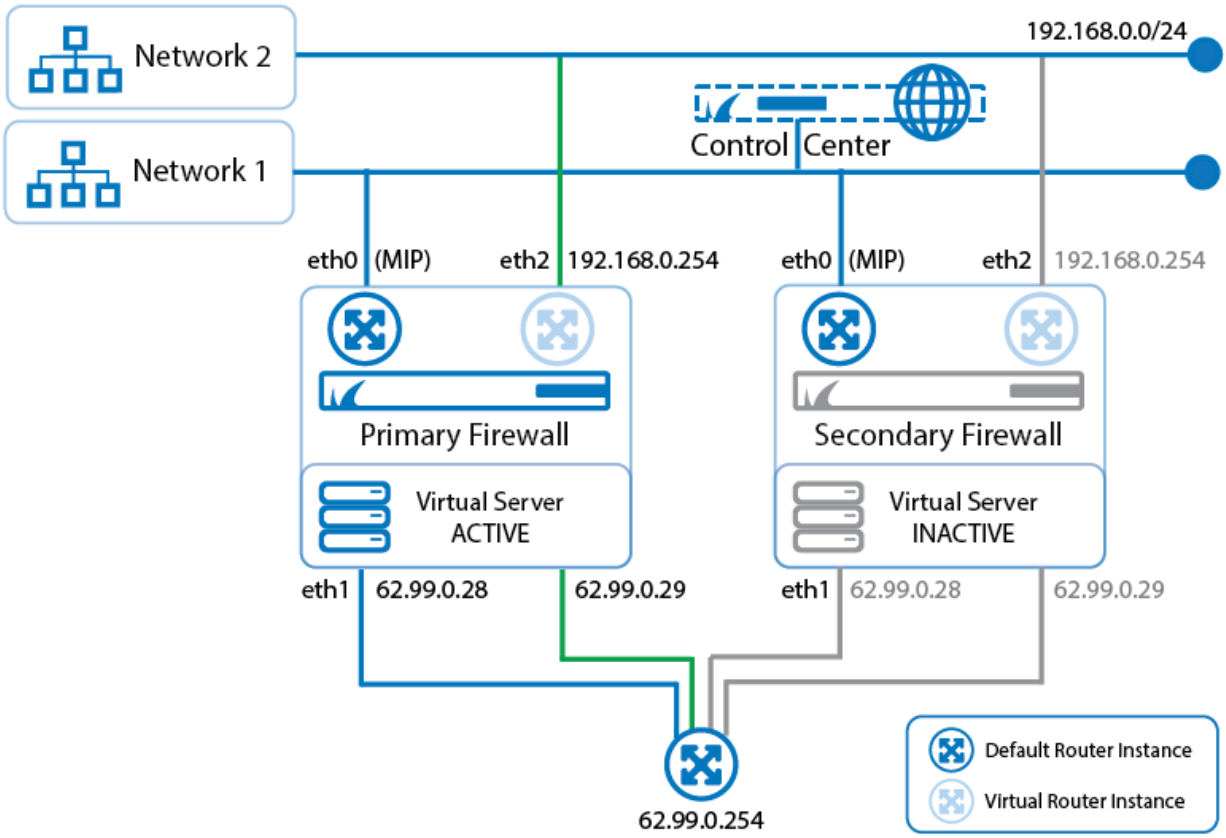
If the names of all virtual router instances and the **VR Instance IDs** do not match each other on both HA boxes, a failover to the secondary firewall will not work!

Before You Begin

Verify that two firewalls are configured to be controlled by the Control Center for operating in high availability mode. For more information, see How to Configure a High Availability Cluster for Managed CloudGen Firewalls.

Verify that your primary firewall is configured for running at least one virtual router instance. For more information, see How to Configure and Activate a Virtual Router Instance with Hardware, Virtual, VLAN, or Bundled Interfaces.

The following example assumes that there is already one virtual router instance configured on the primary firewall that serves as the basis for replicating the configuration to the secondary firewall. The name of the VR Instance is VR01, the ID = 1. In case there are multiple virtual router instances configured, you must execute the following steps for each additional virtual router instance. 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).



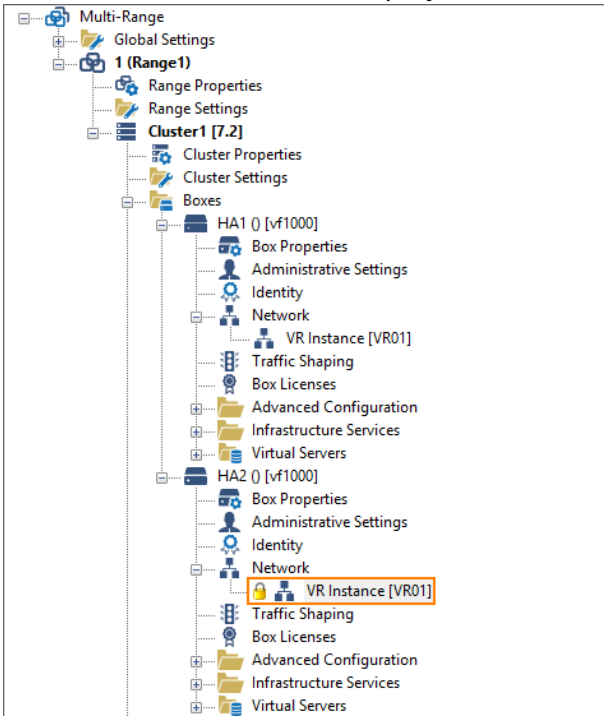
Step 1. Determine the Name and the Virtual Router ID on the Primary Firewall

Because it is important that both HA partners are set up identically also for VRF, both the exact name of the virtual router instance and its ID on the primary HA box must be determined.

1. Go to **CONFIGURATION > Configuration Tree > Multi Range > *your range* > *your cluster* > Boxes > *your primary HA box*** .
2. Click **+** to expand the **Network** node.
3. Double-click **VR Instance[*your virtual router instance*]**.
4. The **VR Instance[*your virtual router instance*]** window opens.
5. Note the name and ID of the virtual router instance of your primary HA box, e.g., name = VR01, ID = 1.

Step 2. Create a Virtual Router Instance on the Secondary Firewall

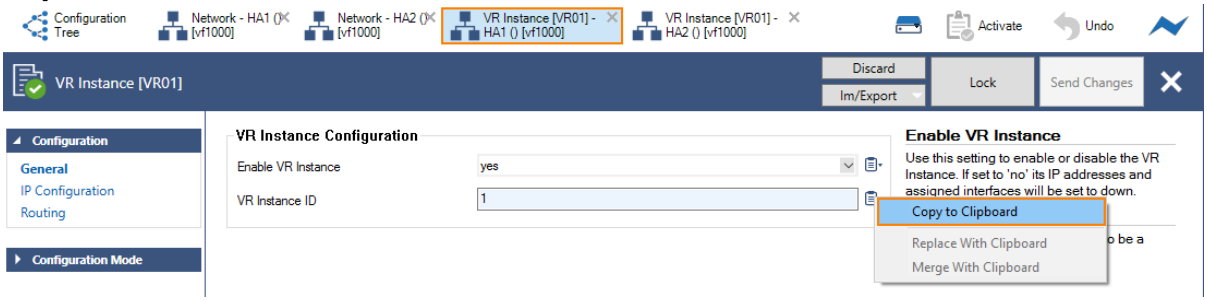
1. Go to **CONFIGURATION > Configuration Tree > Multi Range > *your range* > *your cluster* > Boxes > *your secondary HA box*** .
2. Right-click **Network**.
3. From the menu, select **Lock**.
4. From the menu, select **Create VR Instance**.
5. The window for naming the virtual router is displayed.
6. Enter the same name for the virtual router as on the primary HA box, e.g., VR01 for the name.
7. Click **OK**.
8. In the ribbon bar, click **Activate**.
9. The **Activate Changes** window opens.
10. Click **Activate**.
11. Right-click **VR Instance**.
12. From the menu, select **Lock**.
13. The virtual router node is displayed one hierarchy level below **Network**.



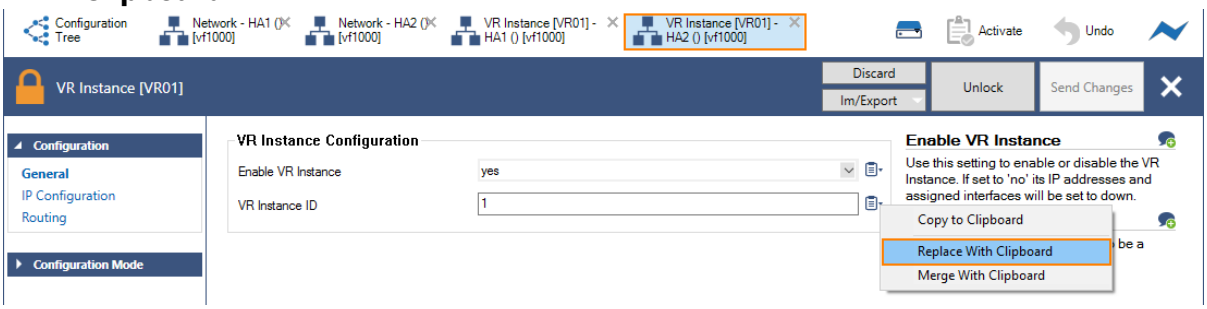
Step 3. Set the ID of the VR Instance on the Secondary Firewall to Match the Value on the Primary Firewall

1. Go to **CONFIGURATION > Configuration Tree > Multi Range > *your range* > *your cluster* > Boxes > *your primary HA box*** .
2. Click **+** to expand the **Network** node of the primary HA box.

3. Double-click **VR Instance [*your virtual instance*]**.
4. In the ribbon bar, select the window **VR Instance [*your virtual instance*] - *your primary HA box*** .
5. Click the **Clipboard** symbol to the right of the **VR Instance ID** edit field and select **Copy to Clipboard**.



6. Go to **CONFIGURATION > Configuration Tree > Multi Range > *your range* > *your cluster* > Boxes > *your secondary HA box*** .
7. Double-click **VR Instance [*your virtual instance*]**.
8. The **VR Instance[*your virtual router instance*]** window opens.
9. Click the **Clipboard** symbol to the right of the **VR Instance ID** edit field and select **Replace With Clipboard**.



10. Click **Send Changes**.
11. The **Activate Changes** window opens.
12. Click **Activate (Keep Locks)**.

Step 4. Transfer all Network Configuration Data from the Primary HA Virtual Router Instance to the Secondary HA Virtual Router Instance

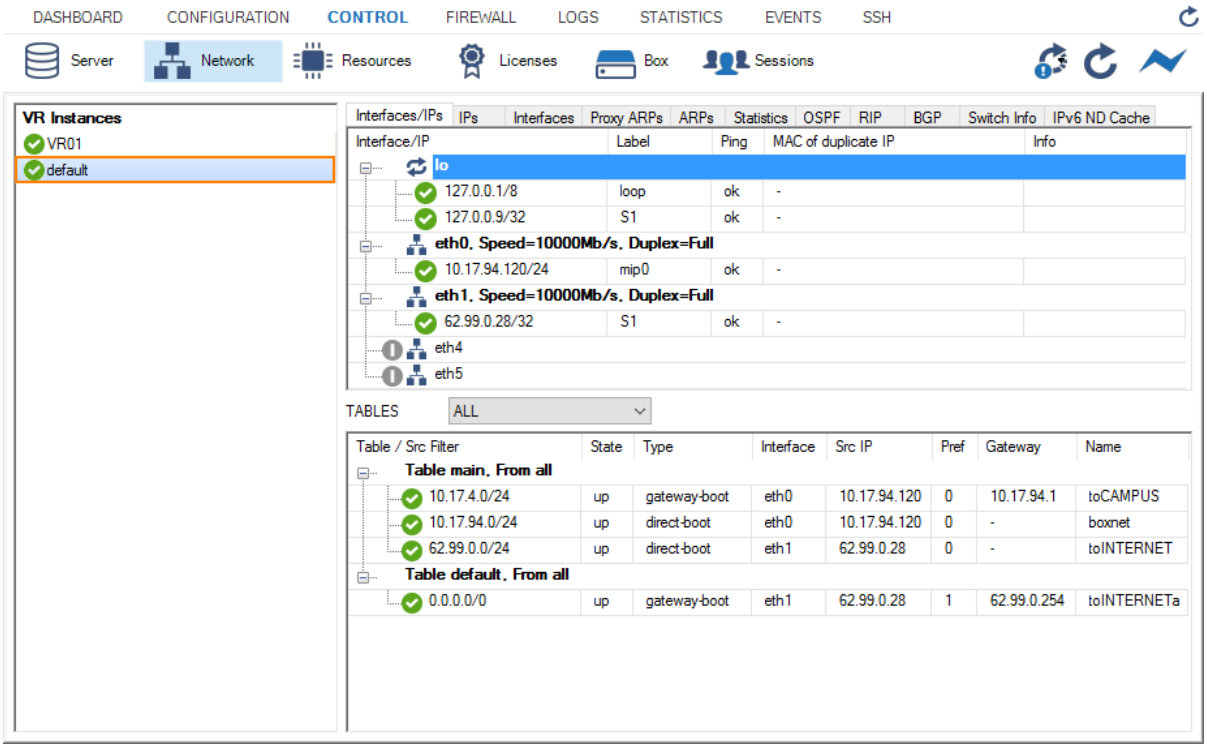
1. In the Ribbon Bar, select **VR Instance [*your virtual instance*] - *your primary HA box*** .
2. Click **IP Configuration**.
3. As in Step 3, transfer all IP addresses from the IPv4 addresses with the clipboard tool to the corresponding list on the secondary HA firewall.
4. (optional) As in Step 3, transfer all routing entries from the IPv4 routing table with the clipboard tool to the corresponding list on the secondary HA firewall.
5. Click **Send Changes**.
6. The **Activate Changes** window opens.
7. Click **Activate**.

Step 5. Re-activate the New Network Configuration

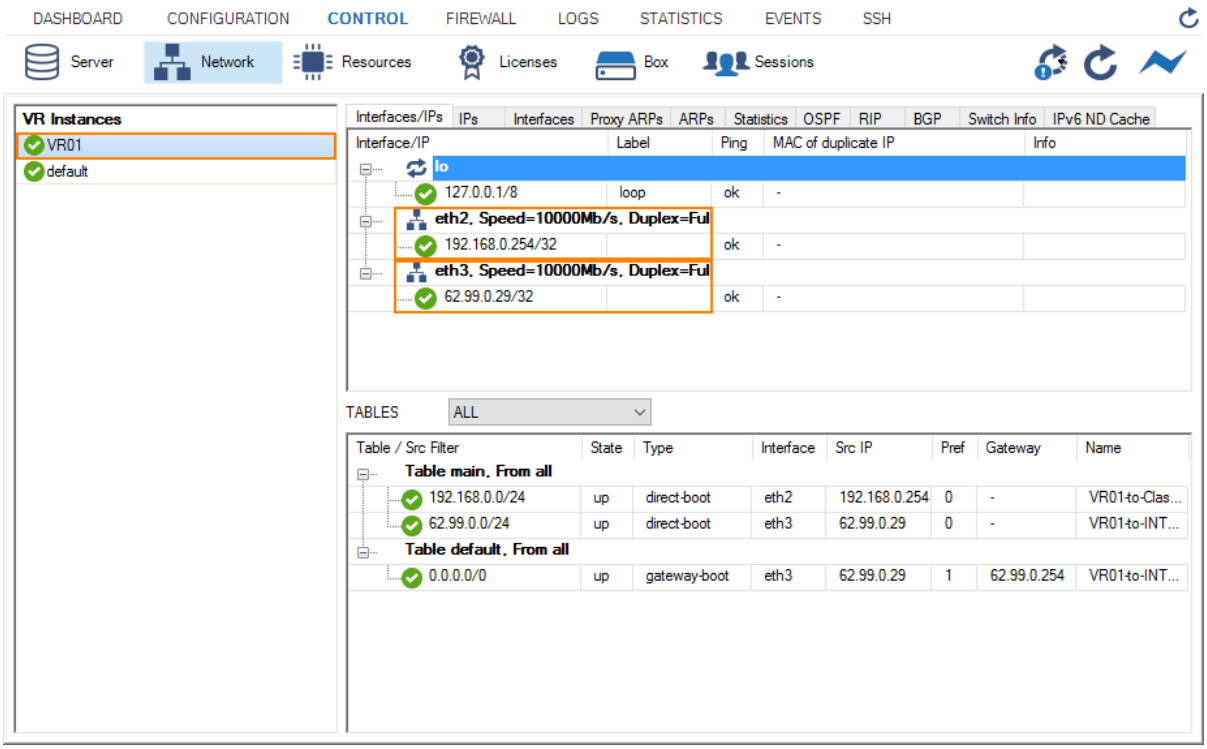
1. On your secondary HA firewall, go to **CONTROL > Box**.
2. In the left menu, click **Network** to expand the menu.
3. Click **Activate new network configuration**.
4. The **Network Activation** window is displayed.
5. Click **Failsafe**.

Step 6. Verify the New Network Configuration

1. On your primary HA box, go to **CONTROL > Network**.
2. In the left column, select **default** to display the network settings for the default router.



3. In the left column, select **VR01** to display the network setting for the virtual router VR01.

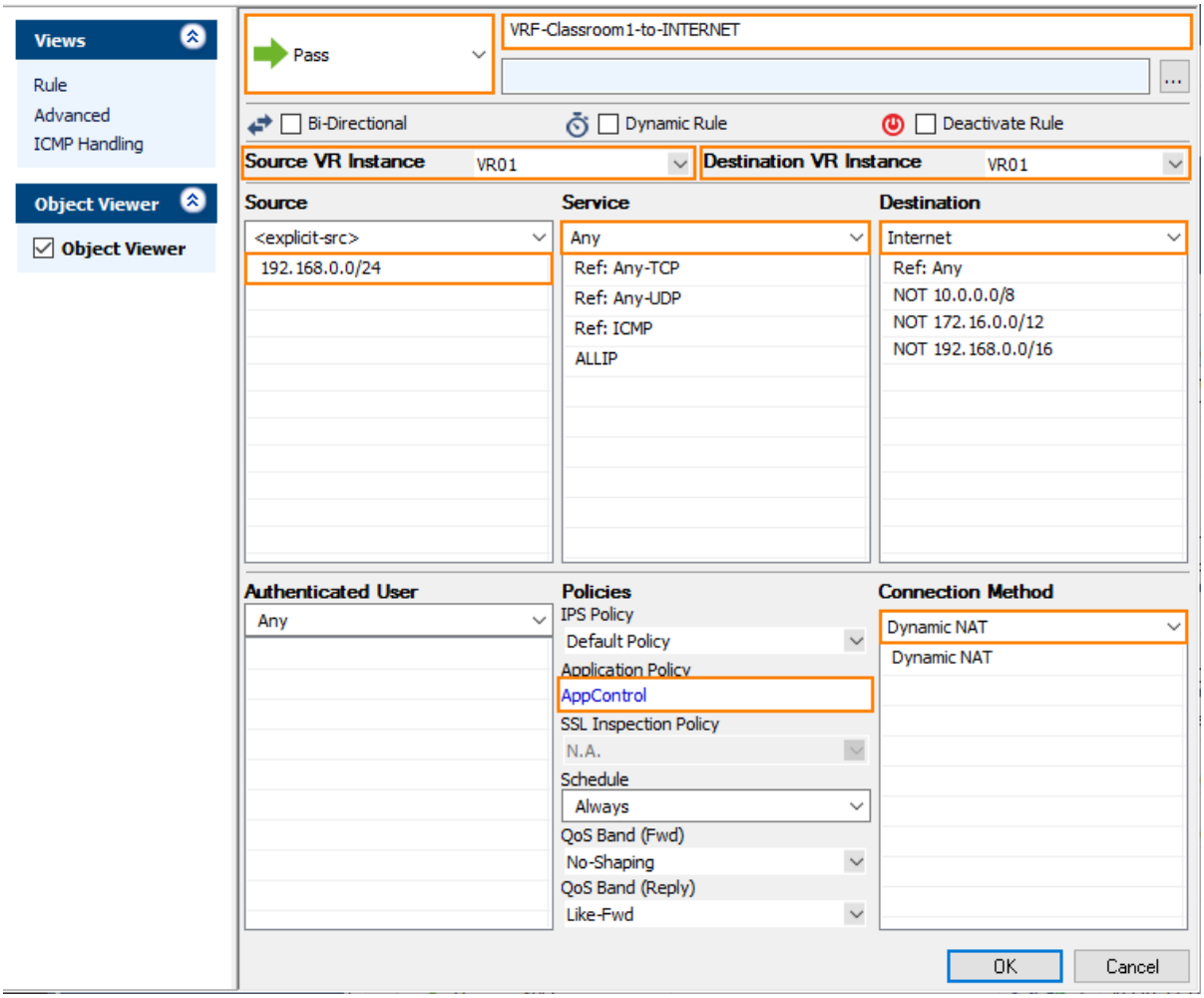


Step 8. Create an Access Rule for the Newly Created Virtual Router VR01

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.

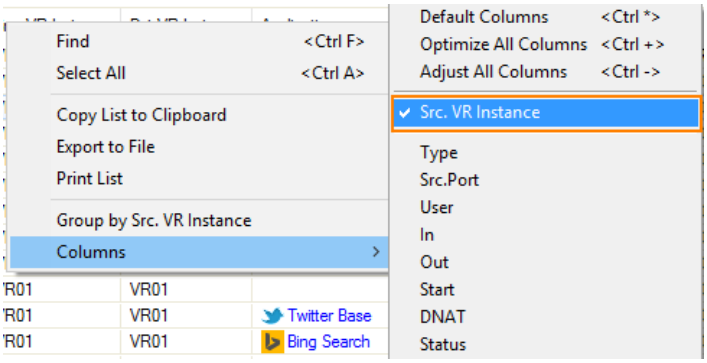
1. Go to **CONFIGURATION > Configuration Tree > Multi Range > *your range* > *your cluster* > Virtual Servers > *your virtual server* > Assigned Services > NGFW (Firewall) > Forwarding Rules**.
2. Click **Lock**.
3. Click **+** to add an access rule.
4. For the access rule type, select **Pass**.
5. Enter a name for the access rule. For a better differentiation between rules that apply to the default router instance and a better 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 that you created in Step 1.
7. **Destination VR Instance** – Select the name of the virtual router instance that you created in Step 1.
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 9. Activate Columns to Display the Traffic Flow Through Your Virtual Router Instance

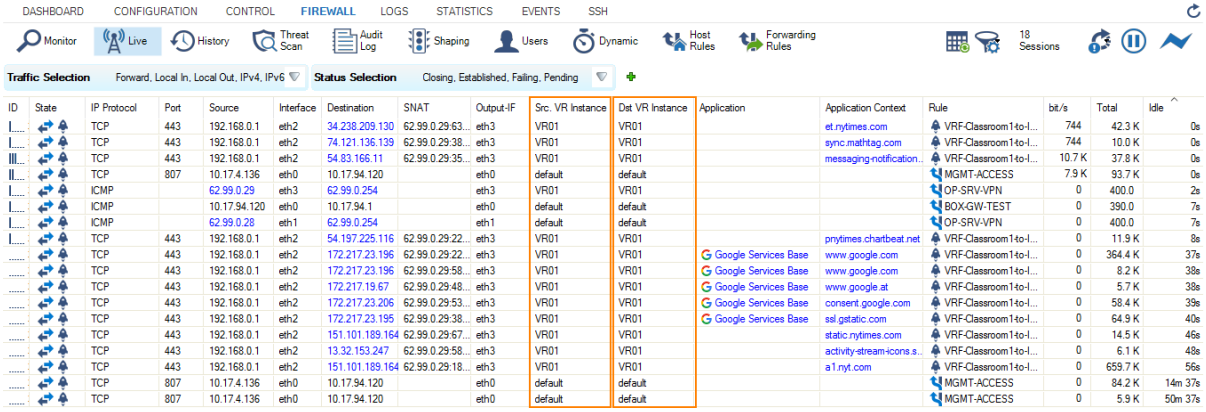
1. Go to **FIREWALL > Live**.
2. Right-click on any of the column identifiers of the Live view.
3. From the menu, select **Columns -> Src. VR Instance**.
4. Right-click on any of the column identifiers of the Live view.
5. From the menu, select **Columns -> Dst. VR Instance**.



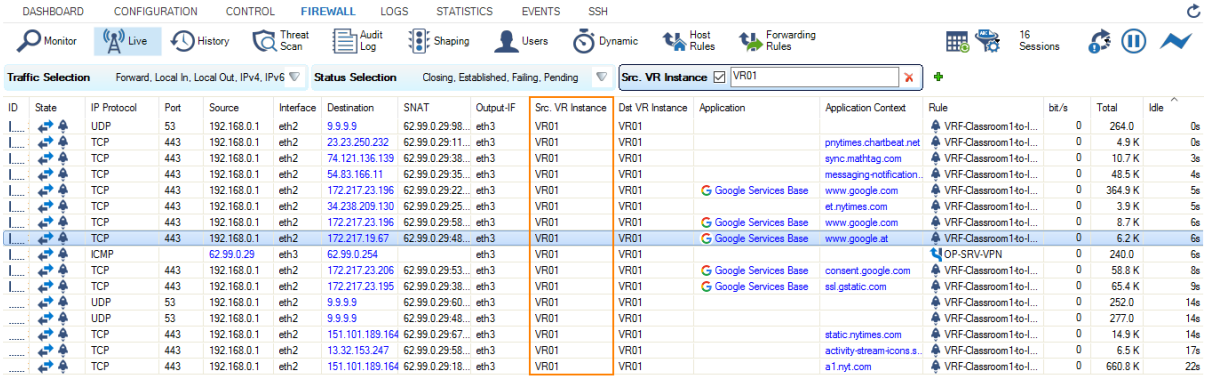
Step 10. Verify that Traffic is Flowing from the Source Network to the Internet

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. 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.png
2. vrf_instance_naming_and_id.png
3. vr_instance_created_on_secondary_ha.png
4. vrf_get_vr_instance_id_from_primary.png
5. vrf_set_vr_instance_id_on_secondary.png
6. vrf_setup_network_overview_default_router.png
7. vrf_setup_network_overview_virtual_router.png
8. vrf_enter_access_rule_for_vr01.png
9. vrf_select_vr_column_to_display.png
10. vrf_traffic_flowing_through_all_router_instances.png
11. traffic_flowing_only_through_VR01.png