How to Configure High Availability Stand-Alone CloudGen Firewalls for Virtual Routing

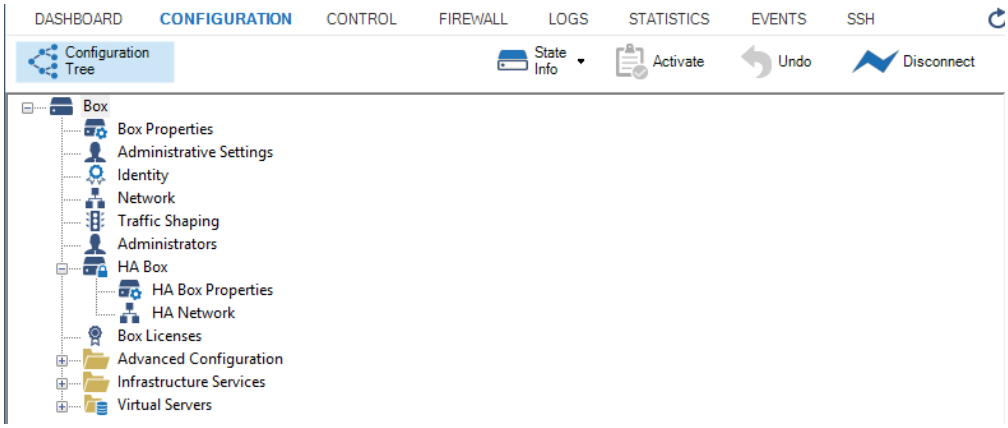
https://campus.barracuda.com/doc/79463121/

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.

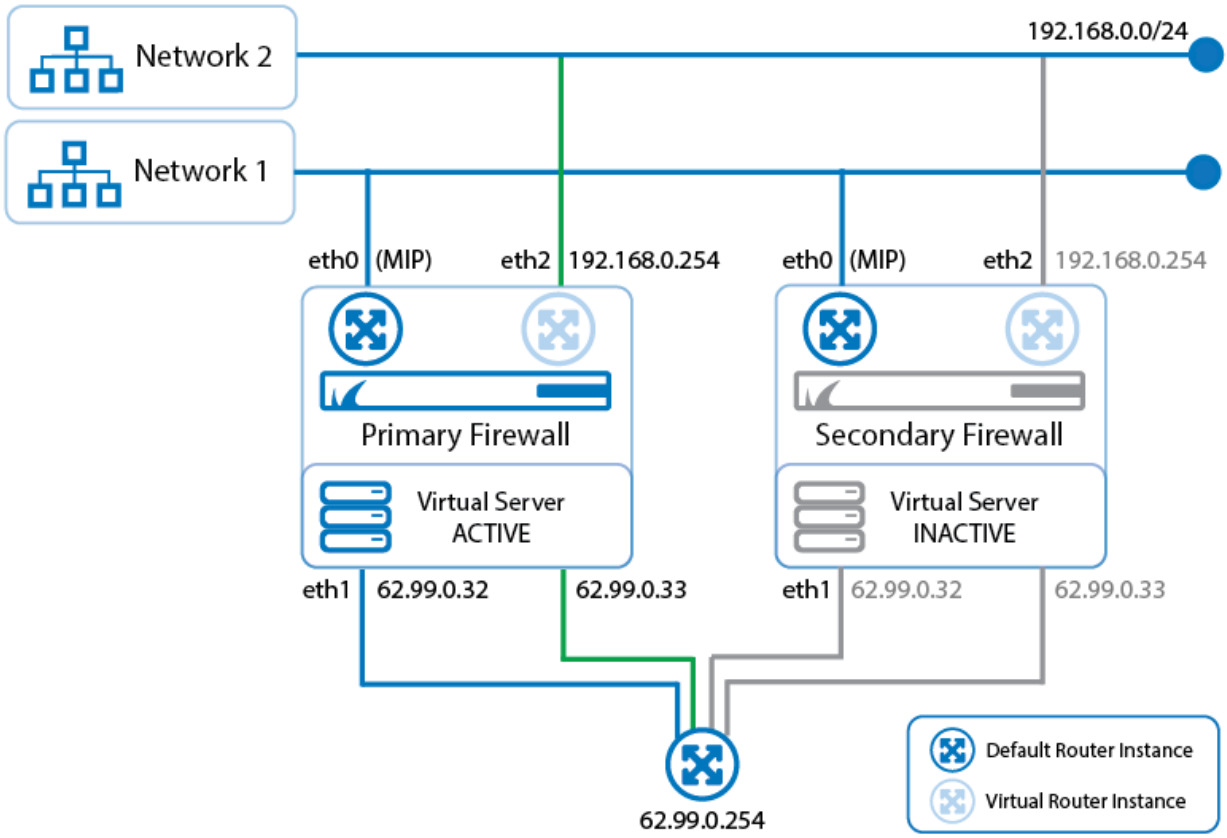
If the names of all virtual router instances and the **VR Instance IDs** do not match each other on both HA boxes, a failover to the secondary firewall will not work!

Before You Begin

Verify that two firewalls are operating in high availability mode. For more information, see How to Configure a High Availability Cluster for Managed CloudGen Firewalls.

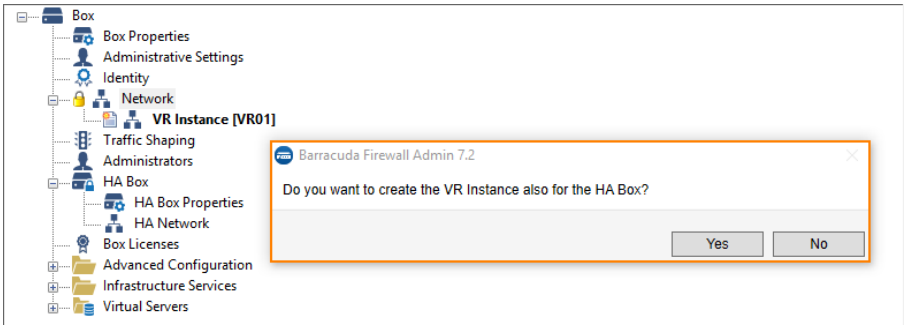


In the following example, an additional virtual instance will be created that routes traffic between a private network (e.g., 192.168.0.0/24) and the Internet. In this setup the firewall service will be transparent to the additional virtual router instance only if authenticated users are not defined. 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).

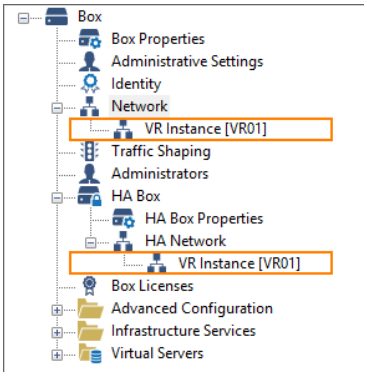


Step 1. Create a Virtual Router Instance on the Primary Firewall

1. Log into the primary firewall.
2. Right-click **CONFIGURATION > Configuration Tree > Box > Network**.
3. Select **Lock**.
4. Right-click **CONFIGURATION > Configuration Tree > Box > 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 for the name.
9. Click **OK**.
10. A dialog window is displayed questioning whether you want to create the VR instance also for the HA box.

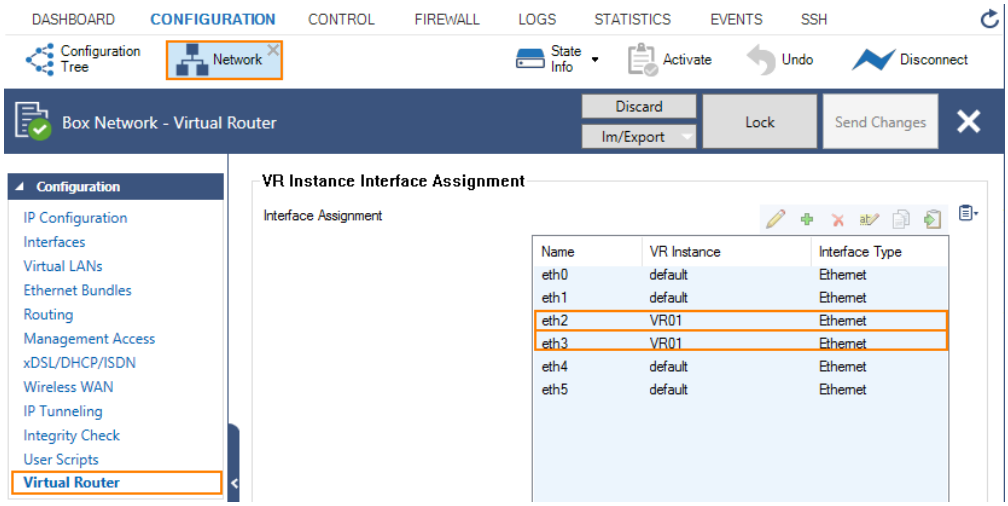


11. Click **Yes**.
12. Click **Send Changes**.
13. The **Activate Changes** window opens.
14. Click **Activate**.



Step 2. Assign Interfaces to the VR Instance on the Primary Firewall

1. The interfaces must be configured both for the primary and secondary HA partner.
2. On your primary firewall, double-click **CONFIGURATION > Configuration Tree > Box > Network**.
3. In the left menu bar, click **Virtual Router**.
4. Click **Lock**.
5. In the **Interface Assignment** list, double-click the first interface to assign the VR Instance, e.g., eth2.
6. The **Interface Assignment** window is displayed.
7. For **VR Instance**, select **VR01**.
8. Click **OK**.
9. In the **Interface Assignment** list, double-click the second interface to assign the VR Instance, e.g., eth3.
10. The **Interface Assignment** window is displayed.
11. For **VR Instance**, select **VR01**.
12. Click **OK**.
13. Click **Send Changes**.
14. Click **Activate**.



Step 3. Assign Interfaces to the VR Instance on the Secondary Firewall

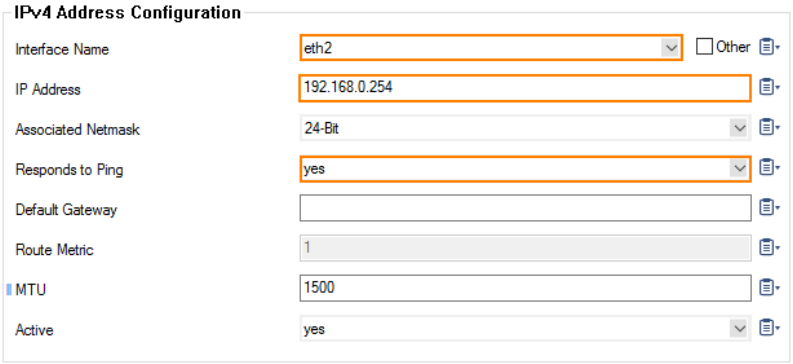
1. Click **CONFIGURATION > Configuration Tree**.
2. Double-click **CONFIGURATION > Configuration Tree > Box > HA Box > HA Network**.
3. Click **Lock**.
4. In the **Interface Assignment** list, double-click the first interface to assign the VR Instance, e.g., eth2.
5. The **Interface Assignment** window 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. The **Activate Changes** window opens.
14. Click **Activate**.

Step 4. Re-activate the New Network Configuration

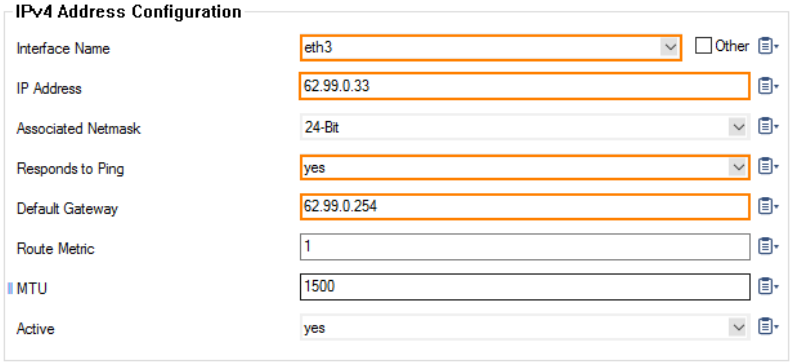
1. On your secondary HA firewall, go to **CONTROL > Box**.
2. In the left menu, click **Network** to expand the menu.
3. Click **Activate new network configuration**.
4. The **Network Activation** window is displayed.
5. Click **Failsafe**.

Step 5. Assign IP Addresses to the Interfaces of the VR Instance on the Primary Firewall

1. Go to **CONFIGURATION > Configuration Tree > Box > 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.



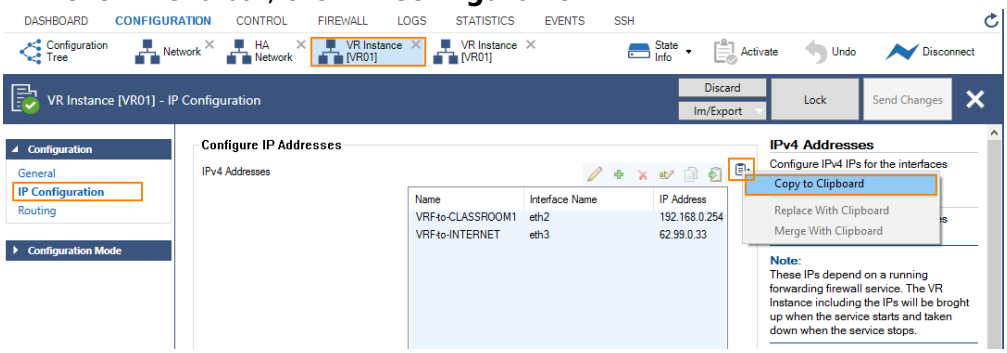
13. Click **OK**.

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

Step 6. Copy the IP Addresses to Interfaces Assignment from the VR Instance from the Primary Firewall to the Secondary Firewall

The VR instance must be configured exactly the same as the primary VR instance.

1. Go to **CONFIGURATION > Configuration Tree > Box > Network > VR Instance [*your virtual instance*]**.
2. Click the **Clipboard** symbol to the right of the **IPv4 Addresses** list and select **Copy to Clipboard**.
3. In the left menu bar, click **IP Configuration**.

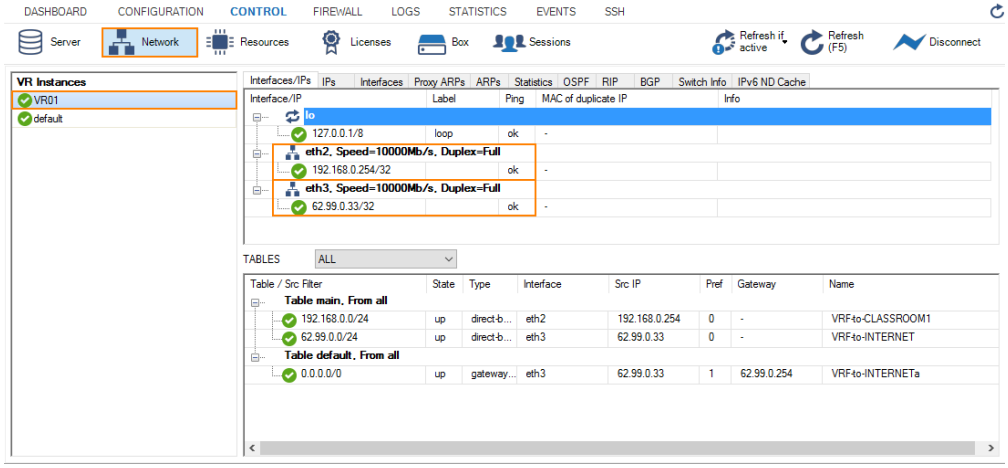


4. Go to **CONFIGURATION > Configuration Tree > Box > HA Box > HA Network > VR Instance [*your virtual instance*]**.
5. Click **Lock**.
6. From the left menu bar, select **IP Configuration**.
7. Click the **Clipboard** symbol to the right of the **IPv4 Addresses** list and select **Replace With Clipboard**.
8. Click **Send Changes**.
9. Click **Activate**.
10. Go to **CONFIGURATION > Configuration Tree > Box > Network > VR Instance [*your virtual instance*]**.
11. In the left menu bar, click **Routing**.
12. Click the **Clipboard** symbol to the right of the **IPv4 Addresses** list and select **Copy to Clipboard**.
13. Go to **CONFIGURATION > Configuration Tree > Box > HA Box > HA Network > VR Instance [*your virtual instance*]**.
14. Click **Lock**.
15. From the left menu bar, select **Routing**.
16. Click the **Clipboard** symbol to the right of the **IPv4 Addresses** list and select **Replace With Clipboard**.
17. Click **Send Changes**.

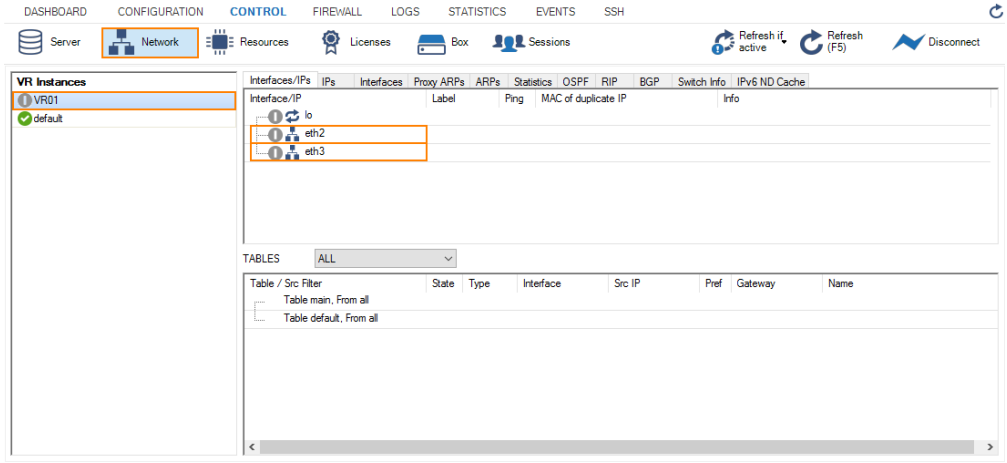
18. The **Activate Changes** window opens.
19. Click **Activate**.

Step 7. Verify Your Configuration on Both HA Partners

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

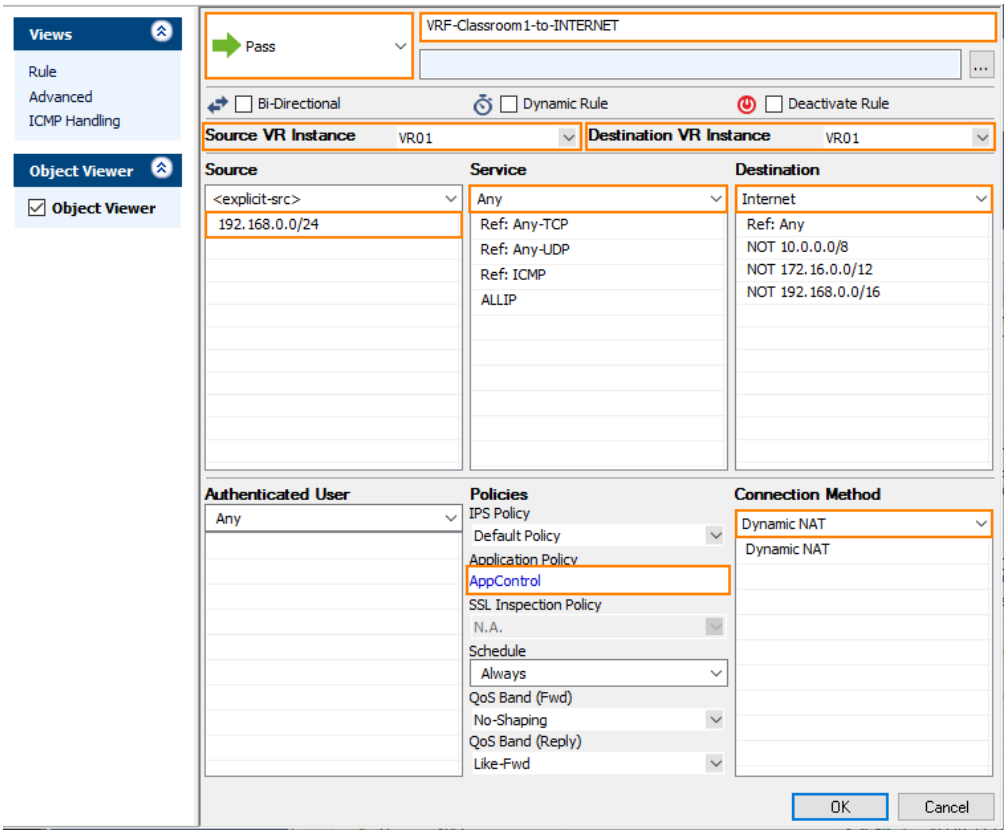


To activate the reverse HA constellation, perform an HA failover. For more information, see How to Perform a Manual High Availability Failover. The upper two images will then be displayed with reversed configuration information accordingly .

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

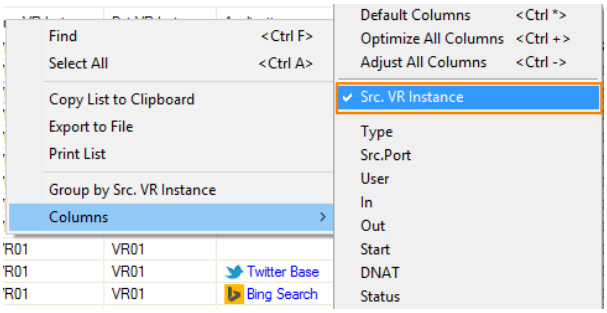
To pass traffic from interface eth2 (192.168.0.254/32) to eth3 (62.99.0.29/32), create an access rule and constrain the access rule to the virtual router VR01.

1. Go to **CONFIGURATION > Configuration Tree > 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, 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 9. Activate Columns to Display the Traffic Flow Through Your Virtual Router Instance

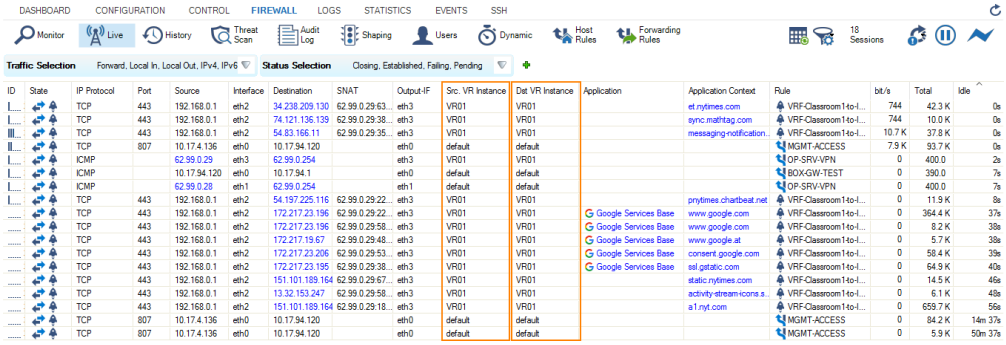
1. Go to **FIREWALL > Live**.
2. Right-click on any of the column identifiers of the Live view.
3. From the menu, select **Columns -> Src. VR Instance**.
4. Right-click on any of the column identifiers of the Live view.
5. From the menu, select **Columns -> Dst. VR Instance**.



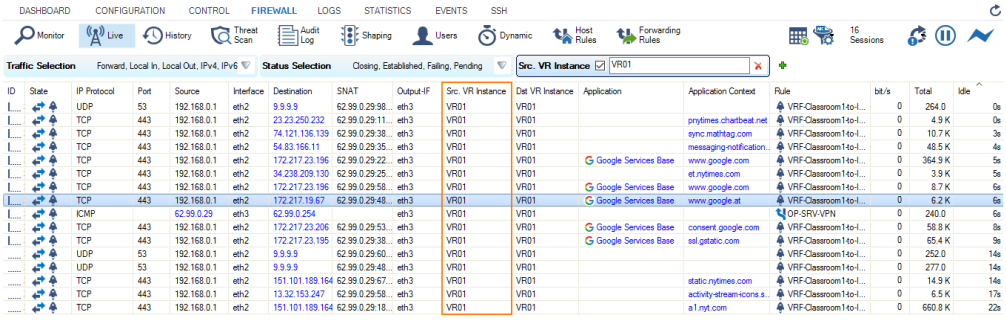
Step 10. Verify that Traffic is Flowing from the Source Network to the Internet

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. vrf_standalone_HA_unconfigured.png
2. vr_ha_standalone.png
3. vrf_standalone_HA_questioning_dialog.png
4. vrf_standalone_HA_both_nodes_created.png
5. vrf_standalone_HA_primary_network_node_configured.png
6. vrf_standalone_HA_configure_primary_interface.png
7. vrf_standalone_HA_configure_second_interface.png
8. vrf_standalone_HA_copy_vri_data_to_clipboard.png
9. vrf_standalone_HA_configuration_complete_HA1.png
10. vrf_standalone_HA_configuration_complete_HA2.png
11. vrf_enter_access_rule_for_vr01.png
12. vrf_select_vr_column_to_display.png
13. vrf_traffic_flowing_through_all_router_instances.png
14. traffic_flowing_only_through_VR01.png