

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

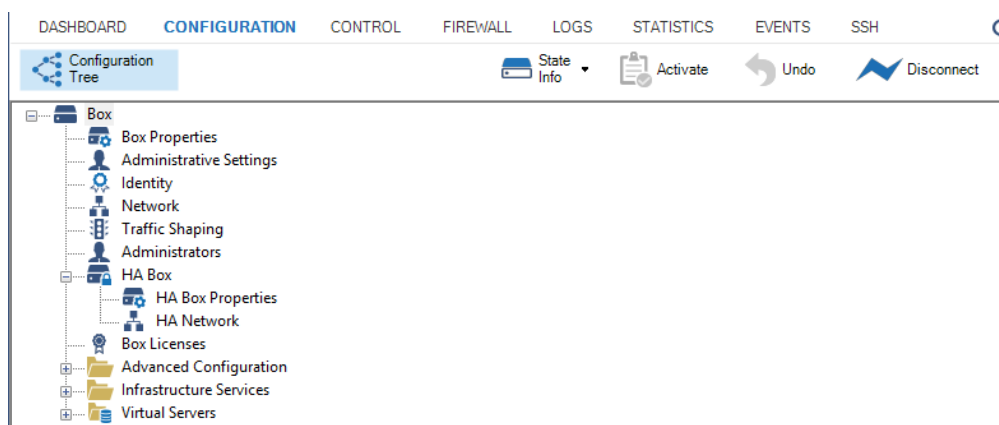
<https://campus.barracuda.com/doc/79463121/>

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.

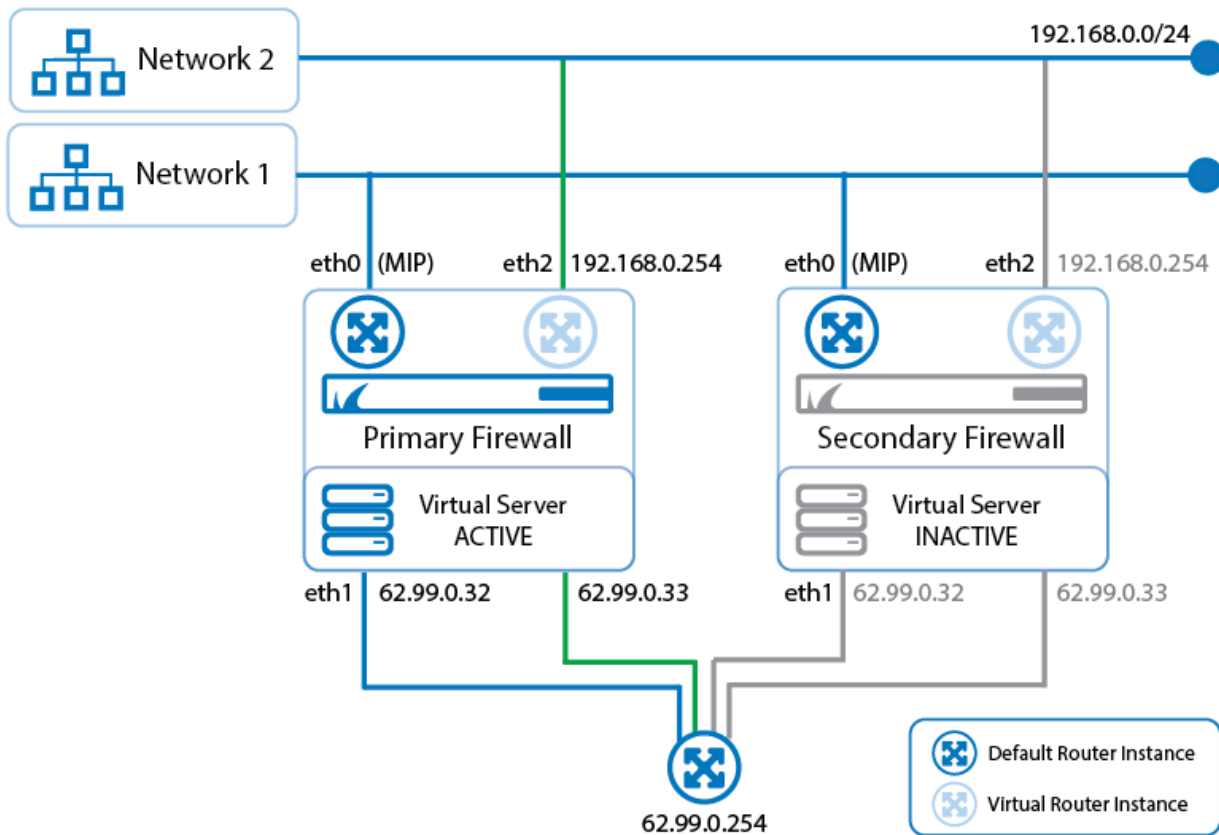
If the names of all virtual router instances and the **VR Instance IDs** do not match each other on both HA boxes, a failover to the secondary firewall will not work!

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](#).

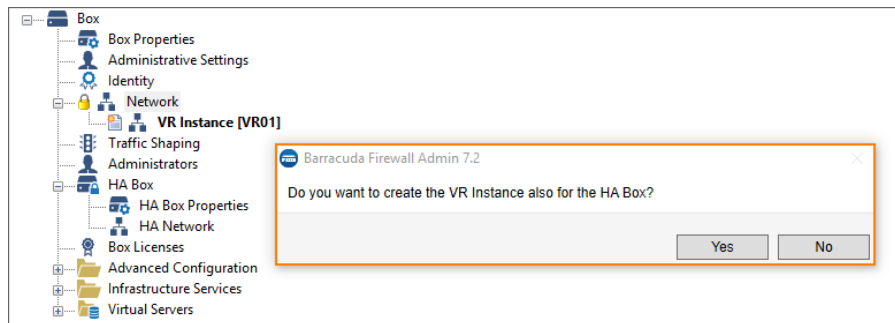


In the following example, an additional virtual instance will be created that routes traffic between a private network (e.g., 192.168.0.0/24) and the Internet. In this setup the firewall service will be transparent to the additional virtual router instance only if authenticated users are not defined.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

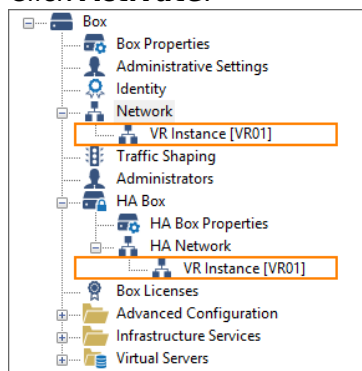


Step 1. Create a Virtual Router Instance on the Primary Firewall

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.

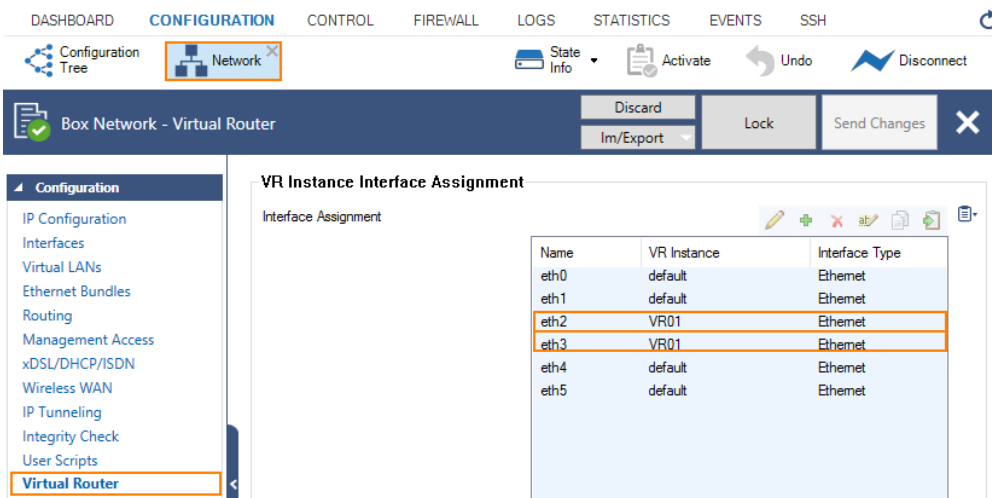


11. Click **Yes**.
12. Click **Send Changes**.
13. The **Activate Changes** window opens.
14. Click **Activate**.



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**.



DASHBOARD **CONFIGURATION** CONTROL FIREWALL LOGS STATISTICS EVENTS SSH

Configuration Tree **Network** State Info Activate Undo Disconnect

Box Network - Virtual Router Discard Im/Export Lock Send Changes X

Configuration

- IP Configuration
- Interfaces
- Virtual LANs
- Ethernet Bundles
- Routing
- Management Access
- xDSL/DHCP/ISDN
- Wireless WAN
- IP Tunneling
- Integrity Check
- User Scripts
- Virtual Router**

VR Instance Interface Assignment

Interface Assignment

Name	VR Instance	Interface Type
eth0	default	Ethernet
eth1	default	Ethernet
eth2	VR01	Ethernet
eth3	VR01	Ethernet
eth4	default	Ethernet
eth5	default	Ethernet

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

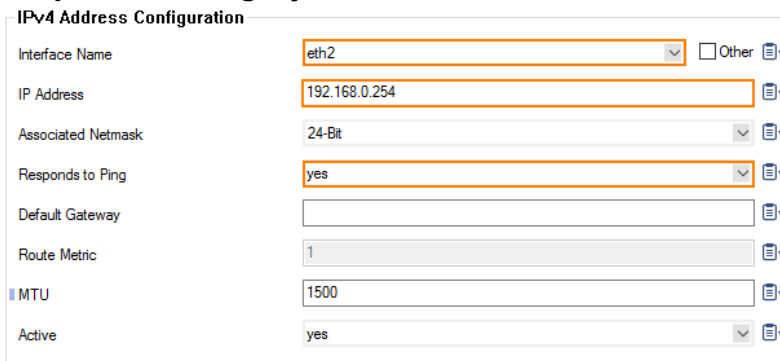
1. Click **CONFIGURATION > Configuration Tree**.
2. Double-click **CONFIGURATION > Configuration Tree > Box > HA Box > HA Network**.
3. Click **Lock**.
4. In the **Interface Assignment** list, double-click the first interface to assign the VR Instance, e.g., eth2.
5. The **Interface Assignment** window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

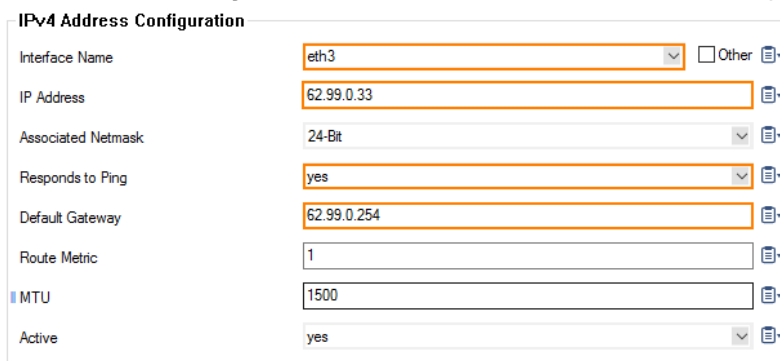
Step 5. Assign IP Addresses to the Interfaces of the VR Instance on the Primary Firewall

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.



The screenshot shows the 'IPv4 Address Configuration' window. The 'Interface Name' dropdown is set to 'eth2'. The 'IP Address' field contains '192.168.0.254'. The 'Associated Netmask' dropdown is set to '24-Bit'. The 'Responds to Ping' dropdown is set to 'yes'. The 'Default Gateway' field is empty. The 'Route Metric' field contains '1'. The 'MTU' field contains '1500'. The 'Active' dropdown is set to '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.



The screenshot shows the 'IPv4 Address Configuration' window. The 'Interface Name' dropdown is set to 'eth3'. The 'IP Address' field contains '62.99.0.33'. The 'Associated Netmask' dropdown is set to '24-Bit'. The 'Responds to Ping' dropdown is set to 'yes'. The 'Default Gateway' field contains '62.99.0.254'. The 'Route Metric' field contains '1'. The 'MTU' field contains '1500'. The 'Active' dropdown is set to 'yes'.

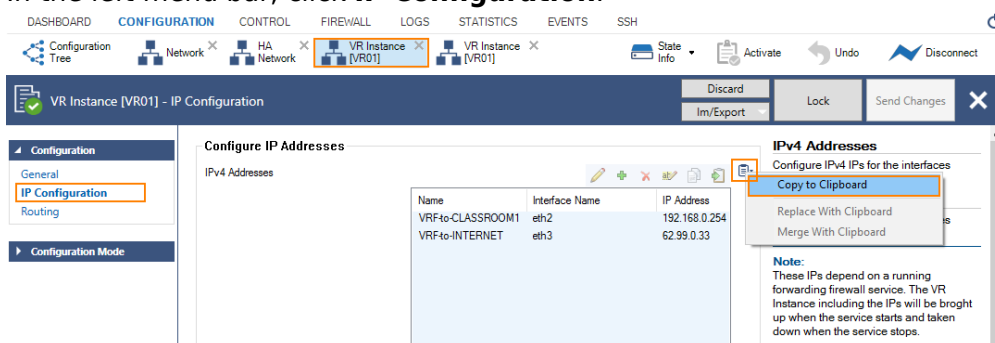
13. Click **OK**.

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**.

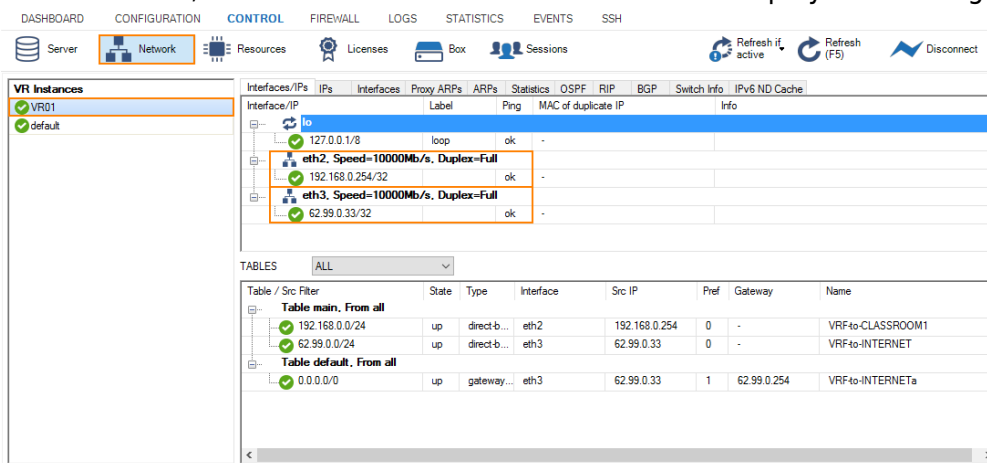


4. Go to **CONFIGURATION > Configuration Tree > Box > HA Box > HA Network > VR Instance [your virtual instance]**.
5. Click **Lock**.
6. From the left menu bar, select **IP Configuration**.
7. Click the **Clipboard** symbol to the right of the **IPv4 Addresses** list and select **Replace With Clipboard**.
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**.

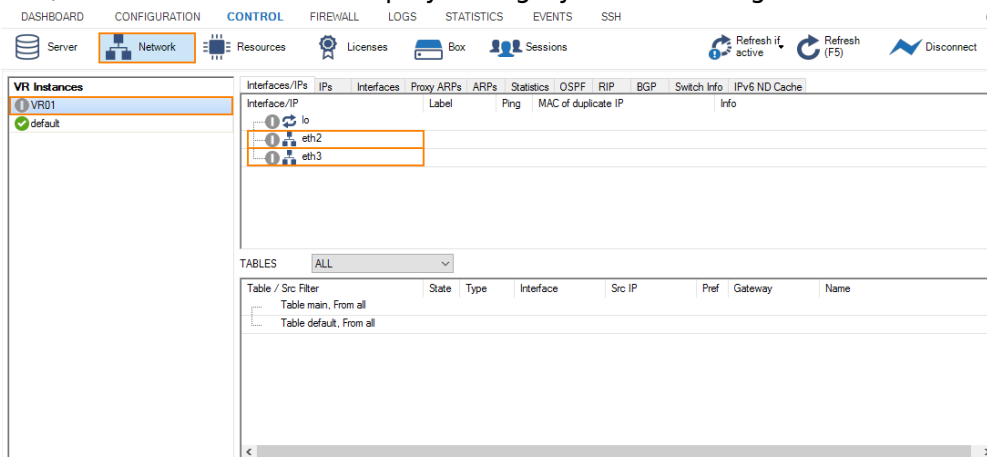
18. The **Activate Changes** window opens.
19. Click **Activate**.

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.

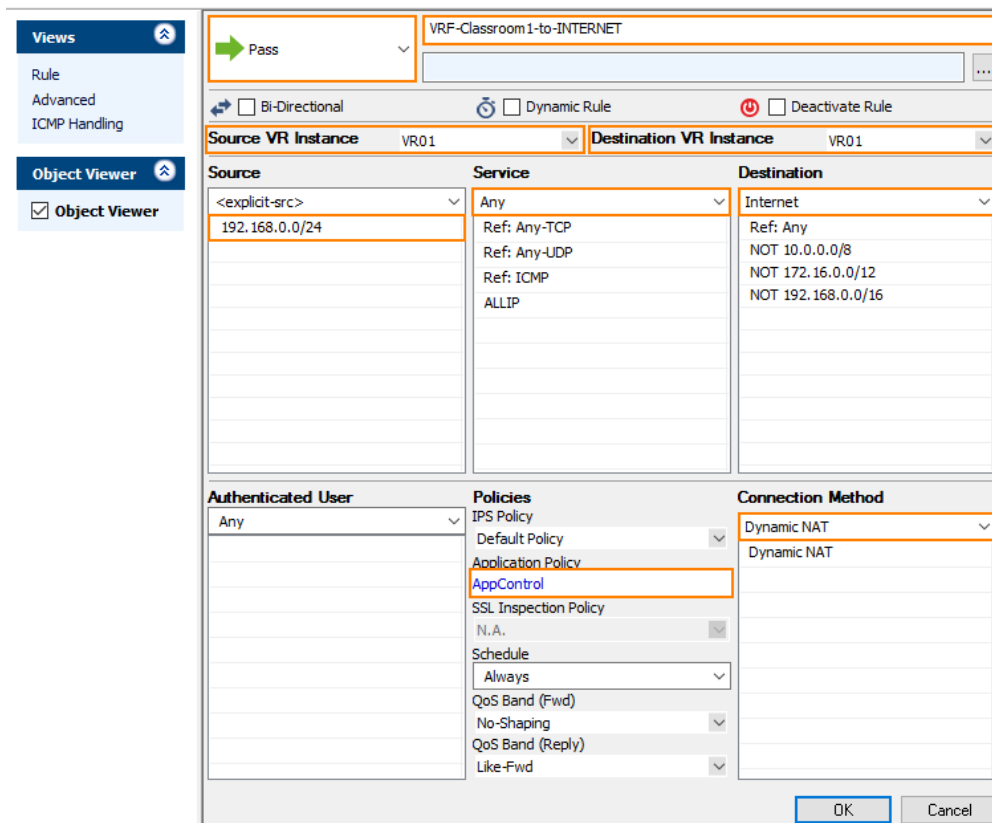


To activate the reverse HA constellation, perform an HA failover. For more information, see [How to Perform a Manual High Availability Failover](#). The upper two images will then be displayed with reversed configuration information accordingly .

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**.



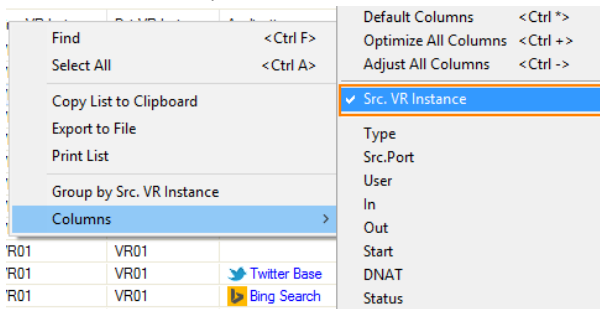
The screenshot shows the configuration for a Forwarding Rule named "VRF-Classroom 1-to-INTERNET". The rule type is "Pass". It is configured for Source VR Instance "VR01" and Destination VR Instance "VR01". The Source is set to "192.168.0.0/24", Service is "Any", and Destination is "Internet". The Connection Method is "Dynamic NAT". The Application Policy is set to "AppControl".

Source	Service	Destination
<explicit-src>	Any	Internet
192.168.0.0/24	Ref: Any-TCP Ref: Any-UDP Ref: ICMP ALLIP	Ref: Any NOT 10.0.0.0/8 NOT 172.16.0.0/12 NOT 192.168.0.0/16

Authenticated User	Policies	Connection Method
Any	IPS Policy Default Policy Application Policy AppControl SSL Inspection Policy N.A. Schedule Always QoS Band (Fwd) No-Shaping QoS Band (Reply) Like-Fwd	Dynamic NAT Dynamic NAT

Step 9. Activate Columns to Display the Traffic Flow Through Your Virtual Router Instance

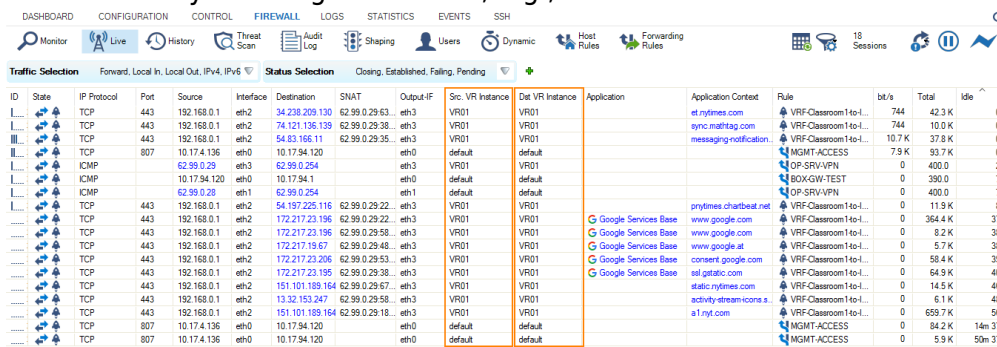
1. Go to **FIREWALL > Live**.
2. Right-click on any of the column identifiers of the Live view.
3. From the menu, select **Columns -> Src. VR Instance**.
4. Right-click on any of the column identifiers of the Live view.
5. From the menu, select **Columns -> Dst. VR Instance**.



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

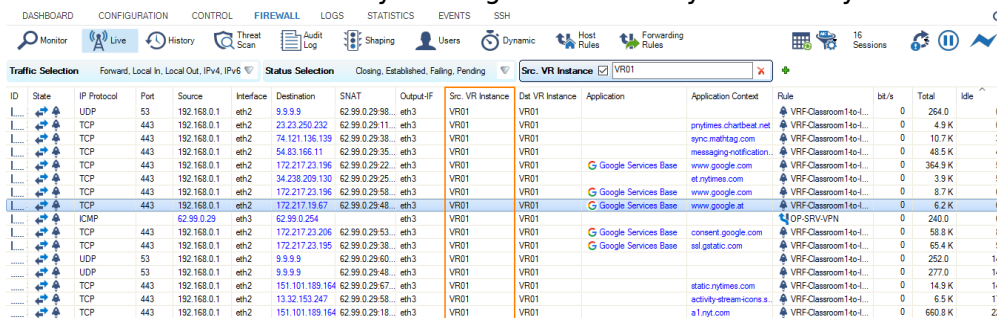
Set up a client with an IP address in the source network (e.g. 192.168.0.1) and set the default route on the client to the address of the virtual router, e.g., 192.168.0.254.

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.



ID	State	IP Protocol	Port	Source	Interface	Destination	SNAT	Output-IF	Src. VR Instance	Det. VR Instance	Application	Application Context	Rule	bit/s	Total	Idle
...	...	TCP	443	192.168.0.1	eth2	34.238.209.130	62.99.0.29.63	eth3	VR01	VR01	et.nytimes.com	et.nytimes.com	VRF-Classroom1-to-I...	744	42.3 K	0s
...	...	TCP	443	192.168.0.1	eth2	74.121.136.139	62.99.0.29.38	eth3	VR01	VR01	sync.mailtag.com	sync.mailtag.com	VRF-Classroom1-to-I...	744	10.0 K	0s
...	...	TCP	443	192.168.0.1	eth2	54.83.166.11	62.99.0.29.35	eth3	VR01	VR01	messaging-notification...	messaging-notification...	VRF-Classroom1-to-I...	10.7 K	37.9 K	0s
...	...	TCP	807	10.174.136	eth0	10.1794.120	62.99.0.29.35	eth3	default	default			MGMT-ACCESS	7.9 K	93.7 K	0s
...	...	ICMP		62.99.0.29	eth3	62.99.0.254		eth0	VR01	VR01			OP-SRV-VPN	0	400.0	2s
...	...	ICMP		10.1794.120	eth0	10.1794.120		eth0	default	default			BOX-GW-TEST	0	390.0	7s
...	...	ICMP		62.99.0.28	eth1	62.99.0.254		eth1	default	default			OP-SRV-VPN	0	400.0	7s
...	...	TCP	443	192.168.0.1	eth2	54.197.225.116	62.99.0.29.22	eth3	VR01	VR01	nytimes.charliebeal.net	nytimes.charliebeal.net	VRF-Classroom1-to-I...	0	11.9 K	8s
...	...	TCP	443	192.168.0.1	eth2	172.217.23.196	62.99.0.29.22	eth3	VR01	VR01	www.google.com	www.google.com	VRF-Classroom1-to-I...	0	364.4 K	37s
...	...	TCP	443	192.168.0.1	eth2	172.217.23.196	62.99.0.29.58	eth3	VR01	VR01	www.google.com	www.google.com	VRF-Classroom1-to-I...	0	8.2 K	35s
...	...	TCP	443	192.168.0.1	eth2	172.217.19.67	62.99.0.29.48	eth3	VR01	VR01	www.google.at	www.google.at	VRF-Classroom1-to-I...	0	5.7 K	38s
...	...	TCP	443	192.168.0.1	eth2	172.217.23.206	62.99.0.29.53	eth3	VR01	VR01	consent.google.com	consent.google.com	VRF-Classroom1-to-I...	0	58.4 K	33s
...	...	TCP	443	192.168.0.1	eth2	172.217.23.195	62.99.0.29.38	eth3	VR01	VR01	ssl.gstatic.com	ssl.gstatic.com	VRF-Classroom1-to-I...	0	64.9 K	40s
...	...	TCP	443	192.168.0.1	eth2	151.101.189.164	62.99.0.29.67	eth3	VR01	VR01	static.nytimes.com	static.nytimes.com	VRF-Classroom1-to-I...	0	14.5 K	46s
...	...	TCP	443	192.168.0.1	eth2	13.32.153.247	62.99.0.29.58	eth3	VR01	VR01	activity-stripe-icons.s...	activity-stripe-icons.s...	VRF-Classroom1-to-I...	0	6.1 K	49s
...	...	TCP	443	192.168.0.1	eth2	151.101.189.164	62.99.0.29.18	eth3	VR01	VR01	a1.nytimes.com	a1.nytimes.com	VRF-Classroom1-to-I...	0	659.7 K	55s
...	...	TCP	807	10.174.136	eth0	10.1794.120		eth0	default	default			MGMT-ACCESS	84.2 K	14m 37s	
...	...	TCP	807	10.174.136	eth0	10.1794.120		eth0	default	default			MGMT-ACCESS	0	5.9 K	50m 37s

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.



ID	State	IP Protocol	Port	Source	Interface	Destination	SNAT	Output-IF	Src. VR Instance	Det. VR Instance	Application	Application Context	Rule	bit/s	Total	Idle
...	...	UDP	53	192.168.0.1	eth2	9.9.9.9	62.99.0.29.98	eth3	VR01	VR01			VRF-Classroom1-to-I...	0	264.0	0s
...	...	TCP	443	192.168.0.1	eth2	23.23.250.232	62.99.0.29.11	eth3	VR01	VR01	nytimes.charliebeal.net	nytimes.charliebeal.net	VRF-Classroom1-to-I...	0	4.9 K	0s
...	...	TCP	443	192.168.0.1	eth2	74.121.136.139	62.99.0.29.38	eth3	VR01	VR01	sync.mailtag.com	sync.mailtag.com	VRF-Classroom1-to-I...	0	10.7 K	3s
...	...	TCP	443	192.168.0.1	eth2	54.83.166.11	62.99.0.29.35	eth3	VR01	VR01	messaging-notification...	messaging-notification...	VRF-Classroom1-to-I...	0	48.5 K	4s
...	...	TCP	443	192.168.0.1	eth2	172.217.23.196	62.99.0.29.22	eth3	VR01	VR01	www.google.com	www.google.com	VRF-Classroom1-to-I...	0	364.9 K	5s
...	...	TCP	443	192.168.0.1	eth2	34.238.209.130	62.99.0.29.25	eth3	VR01	VR01	et.nytimes.com	et.nytimes.com	VRF-Classroom1-to-I...	0	3.9 K	6s
...	...	TCP	443	192.168.0.1	eth2	172.217.23.196	62.99.0.29.58	eth3	VR01	VR01	www.google.com	www.google.com	VRF-Classroom1-to-I...	0	8.7 K	6s
...	...	TCP	443	192.168.0.1	eth2	172.217.19.67	62.99.0.29.48	eth3	VR01	VR01	www.google.at	www.google.at	VRF-Classroom1-to-I...	0	6.2 K	8s
...	...	ICMP		62.99.0.29	eth3	62.99.0.254		eth3	VR01	VR01			OP-SRV-VPN	0	240.0	6s
...	...	TCP	443	192.168.0.1	eth2	172.217.23.195	62.99.0.29.38	eth3	VR01	VR01	consent.google.com	consent.google.com	VRF-Classroom1-to-I...	0	58.8 K	8s
...	...	TCP	443	192.168.0.1	eth2	172.217.23.195	62.99.0.29.38	eth3	VR01	VR01	ssl.gstatic.com	ssl.gstatic.com	VRF-Classroom1-to-I...	0	65.4 K	9s
...	...	UDP	53	192.168.0.1	eth2	9.9.9.9	62.99.0.29.60	eth3	VR01	VR01			VRF-Classroom1-to-I...	0	252.0	14s
...	...	UDP	53	192.168.0.1	eth2	9.9.9.9	62.99.0.29.48	eth3	VR01	VR01			VRF-Classroom1-to-I...	0	277.0	14s
...	...	TCP	443	192.168.0.1	eth2	151.101.189.164	62.99.0.29.67	eth3	VR01	VR01	static.nytimes.com	static.nytimes.com	VRF-Classroom1-to-I...	0	14.9 K	14s
...	...	TCP	443	192.168.0.1	eth2	13.32.153.247	62.99.0.29.58	eth3	VR01	VR01	activity-stripe-icons.s...	activity-stripe-icons.s...	VRF-Classroom1-to-I...	0	6.5 K	17s
...	...	TCP	443	192.168.0.1	eth2	151.101.189.164	62.99.0.29.18	eth3	VR01	VR01	a1.nytimes.com	a1.nytimes.com	VRF-Classroom1-to-I...	0	660.8 K	22s

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_flowng_through_all_router_instances.png
14. traffic_flowng_only_through_VR01.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.