

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.

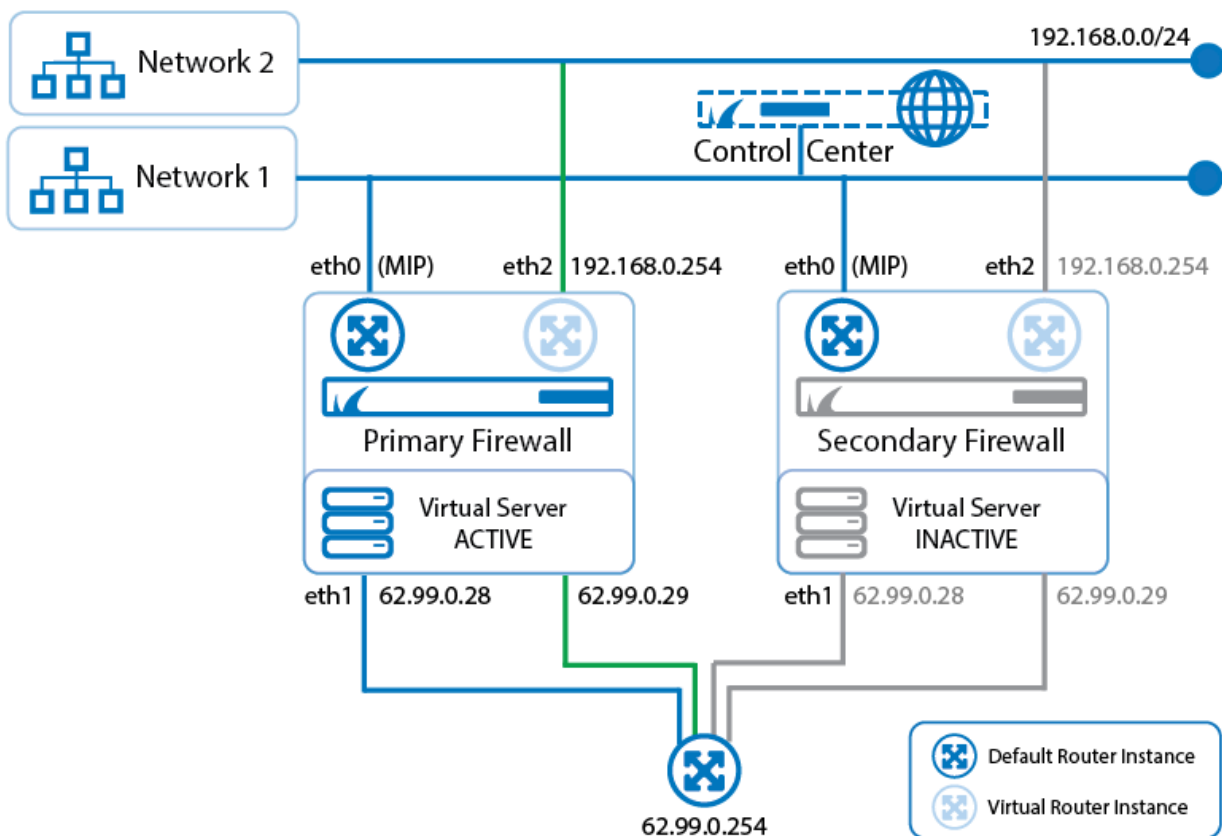
If the names of all virtual router instances and the **VR Instance IDs** do not match each other on both HA boxes, a failover to the secondary firewall will not work!

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

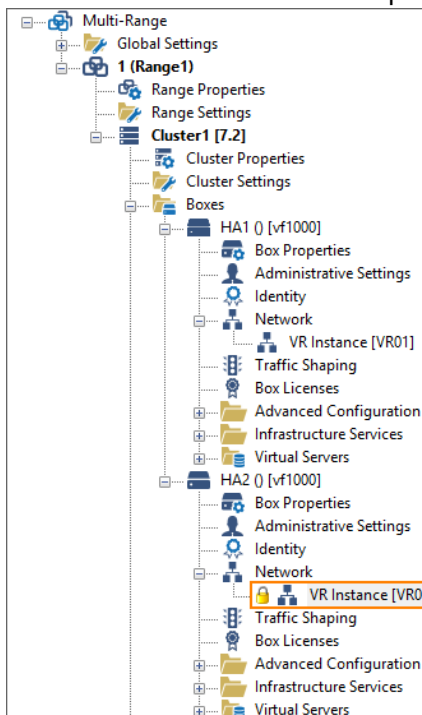
Because it is important that both HA partners are set up identically also for VRF, both the exact name of the virtual router instance and its ID on the primary HA box must be determined.

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

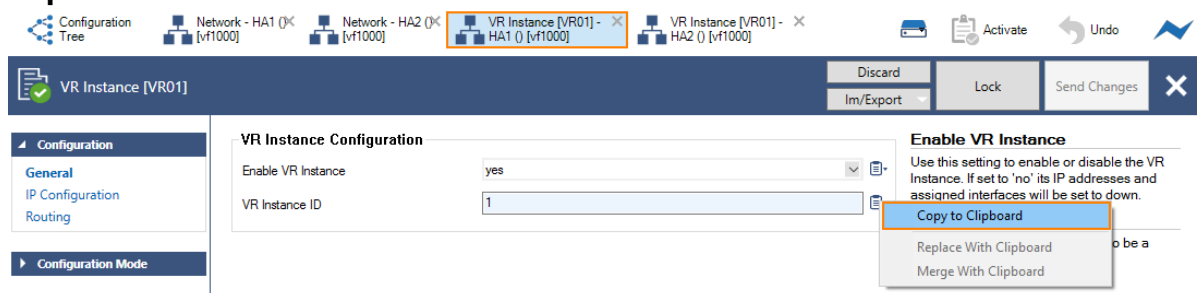
1. Go to **CONFIGURATION > Configuration Tree > Multi Range > your range > your cluster > Boxes > your secondary HA box** .
2. Right-click **Network**.
3. From the menu, select **Lock**.
4. From the menu, select **Create VR Instance**.
5. The window for naming the virtual router is displayed.
6. Enter 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**.



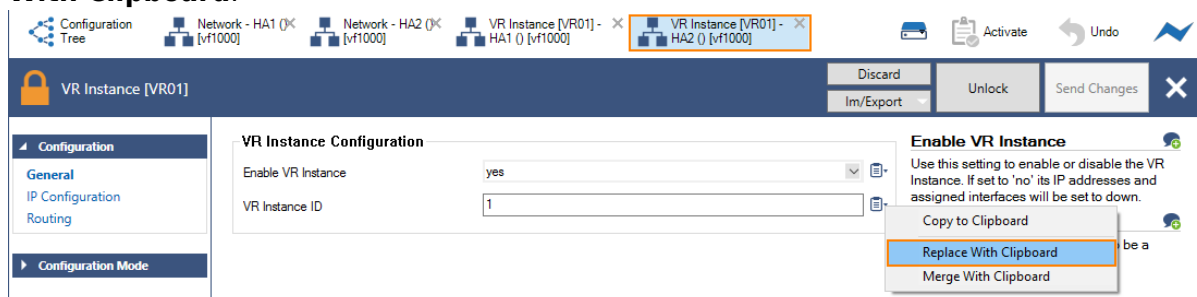
Step 3. Set the ID of the VR Instance on the Secondary Firewall to Match the Value on the Primary Firewall

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

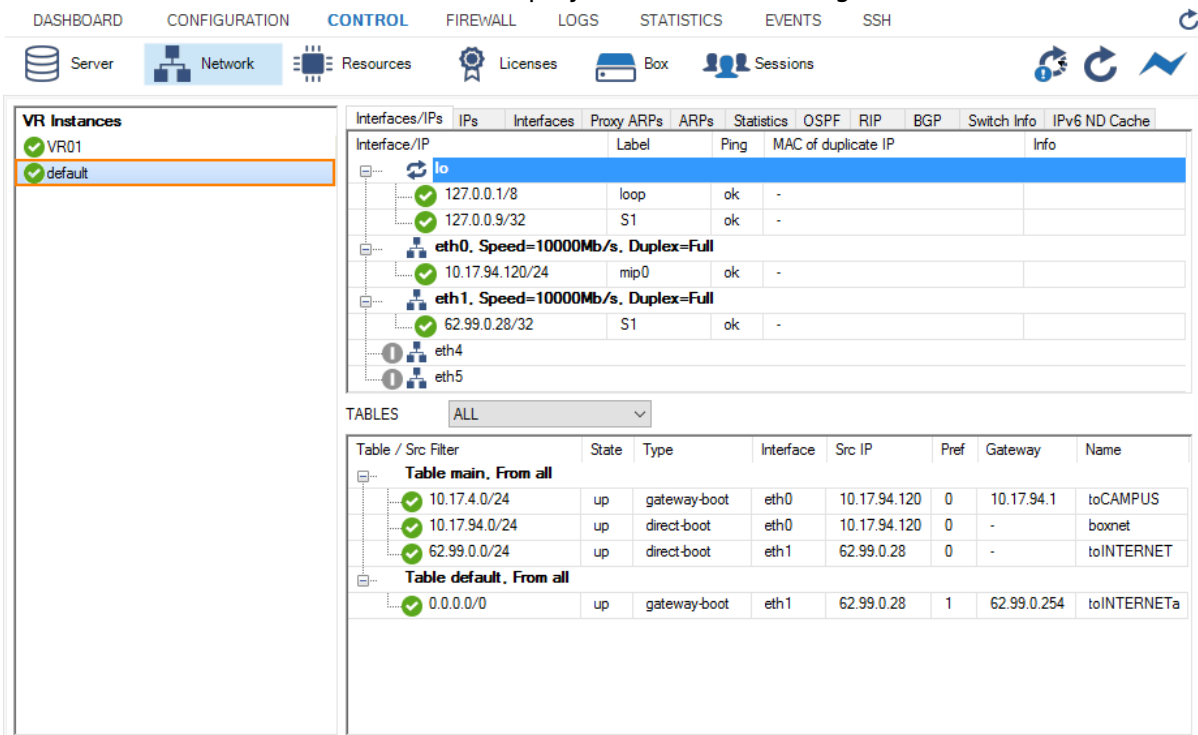
1. In the Ribbon Bar, select **VR Instance [your virtual instance] - your primary HA box**.
2. Click **IP Configuration**.
3. As in Step 3, transfer all IP addresses from the IPv4 addresses with the clipboard tool to the corresponding list on the secondary HA firewall.
4. (optional) As in Step 3, transfer 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.



The screenshot shows the Barracuda CloudGen Firewall web interface. The top navigation bar includes DASHBOARD, CONFIGURATION, CONTROL (selected), FIREWALL, LOGS, STATISTICS, EVENTS, and SSH. Below the navigation bar, there are icons for Server, Network (selected), Resources, Licenses, Box, and Sessions. The main content area is divided into two sections: VR Instances and Interfaces/IPs.

VR Instances: A list showing two instances: VR01 and default, both with green checkmarks indicating they are active.

Interfaces/IPs: A table showing the configuration for the default router. The table has columns for Interface/IP, Label, Ping, and MAC of duplicate IP. The 'lo' interface is highlighted in blue. Below the interface list, there are two tables showing routing information.

TABLES: A dropdown menu set to 'ALL'.

Table / Src Filter	State	Type	Interface	Src IP	Pref	Gateway	Name
Table main. From all							
10.17.4.0/24	up	gateway-boot	eth0	10.17.94.120	0	10.17.94.1	toCAMPUS
10.17.94.0/24	up	direct-boot	eth0	10.17.94.120	0	-	boxnet
62.99.0.0/24	up	direct-boot	eth1	62.99.0.28	0	-	toINTERNET
Table default. From all							
0.0.0.0/0	up	gateway-boot	eth1	62.99.0.28	1	62.99.0.254	toINTERNETA

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

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

Server Network Resources Licenses Box Sessions

VR Instances

- VR01
- default

Interface/IP	Label	Ping	MAC of duplicate IP	Info
lo	127.0.0.1/8	loop	ok	-
eth2	192.168.0.254/32	Speed=10000Mb/s, Duplex=Full	ok	-
eth3	62.99.0.29/32	Speed=10000Mb/s, Duplex=Full	ok	-

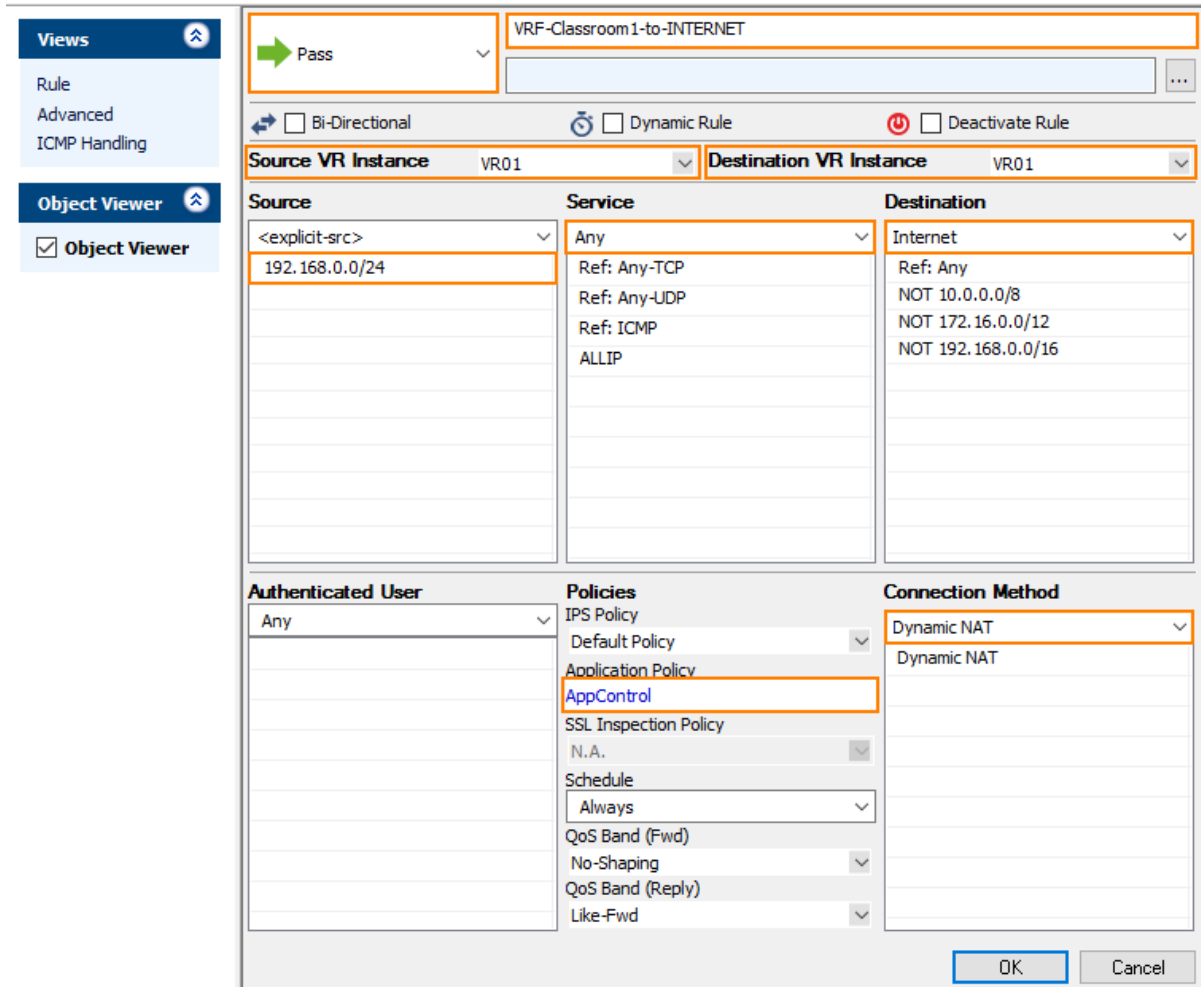
TABLES ALL

Table / Src Filter	State	Type	Interface	Src IP	Pref	Gateway	Name
Table main, From all							
<input checked="" type="checkbox"/> 192.168.0.0/24	up	direct-boot	eth2	192.168.0.254	0	-	VR01-to-Clas...
<input checked="" type="checkbox"/> 62.99.0.0/24	up	direct-boot	eth3	62.99.0.29	0	-	VR01-to-INT...
Table default, From all							
<input checked="" type="checkbox"/> 0.0.0.0/0	up	gateway-boot	eth3	62.99.0.29	1	62.99.0.254	VR01-to-INT...

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**.


The screenshot shows the configuration window for a rule named "VRF-Classroom1-to-INTERNET". The rule is set to "Pass" and is not bi-directional, dynamic, or deactivated. Both the source and destination VR instances are set to "VR01".

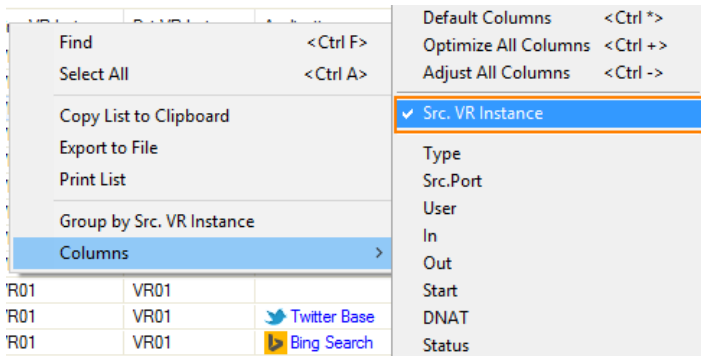
Source	Service	Destination
<explicit-src> 192.168.0.0/24	Any Ref: Any-TCP Ref: Any-UDP Ref: ICMP ALLIP	Internet Ref: Any NOT 10.0.0.0/8 NOT 172.16.0.0/12 NOT 192.168.0.0/16

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

Buttons: OK, Cancel

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

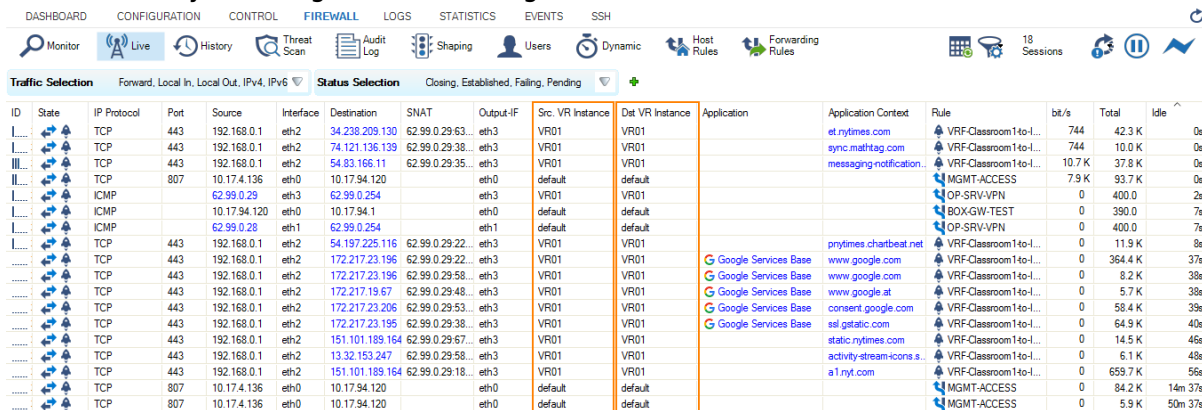
1. Go to **FIREWALL > Live**.
2. Right-click on any of the column identifiers of the Live view.
3. From the menu, select **Columns -> Src. VR Instance**.
4. Right-click on any of the column identifiers of the Live view.
5. From the menu, select **Columns -> Dst. VR Instance**.



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

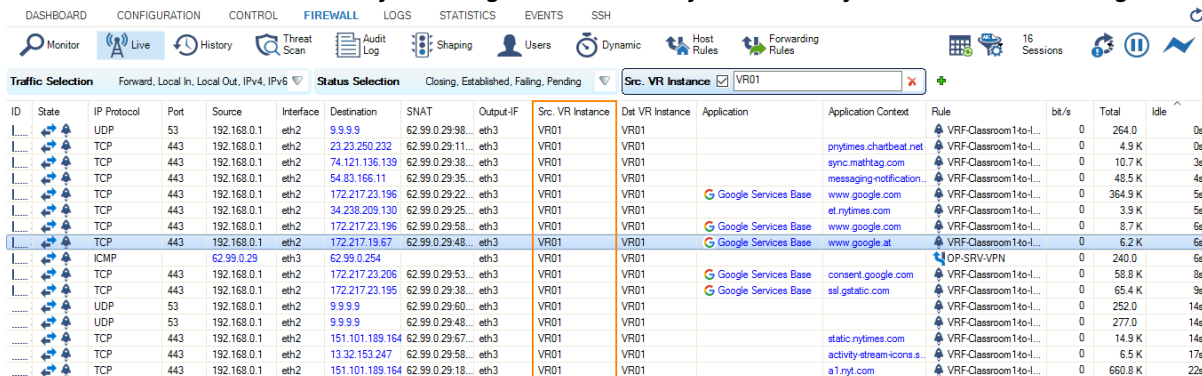
Set up a client with an IP address in the source network (e.g. 192.168.0.1) and set the default route on the client to the address of the virtual router, e.g., 192.168.0.254.

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	Dst 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	VRF-Classroom14o-1...	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.mathtag.com	VRF-Classroom14o-1...	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...	VRF-Classroom14o-1...	10.7 K	37.8 K	0s
...	...	TCP	807	10.17.4.136	eth0	10.17.94.120	62.99.0.29.35...	eth3	default	default		MGMT-ACCESS	VRF-Classroom14o-1...	7.9 K	93.7 K	0s
...	...	ICMP		62.99.0.29	eth3	62.99.0.254		eth3	VR01	VR01		OP-SRV-VPN	VRF-Classroom14o-1...	0	400.0	2s
...	...	ICMP		10.17.4.120	eth0	10.17.94.1		eth0	default	default		BOX-GW-TEST	VRF-Classroom14o-1...	0	390.0	7s
...	...	ICMP		62.99.0.28	eth1	62.99.0.254		eth1	default	default		OP-SRV-VPN	VRF-Classroom14o-1...	0	400.0	7s
...	...	TCP	443	192.168.0.1	eth2	54.197.225.116	62.99.0.29.22...	eth3	VR01	VR01		prytimes.chartbeat.net	VRF-Classroom14o-1...	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	VRF-Classroom14o-1...	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	VRF-Classroom14o-1...	0	8.2 K	38s
...	...	TCP	443	192.168.0.1	eth2	172.217.19.67	62.99.0.29.48...	eth3	VR01	VR01		www.google.at	VRF-Classroom14o-1...	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	VRF-Classroom14o-1...	0	58.4 K	39s
...	...	TCP	443	192.168.0.1	eth2	172.217.23.195	62.99.0.29.38...	eth3	VR01	VR01		ssl.gstatic.com	VRF-Classroom14o-1...	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	VRF-Classroom14o-1...	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.stream-icons.s...	VRF-Classroom14o-1...	0	6.1 K	48s
...	...	TCP	443	192.168.0.1	eth2	151.101.189.164	62.99.0.29.18...	eth3	VR01	VR01		a1.nytimes.com	VRF-Classroom14o-1...	0	659.7 K	56s
...	...	TCP	807	10.17.4.136	eth0	10.17.94.120		eth0	default	default		MGMT-ACCESS	VRF-Classroom14o-1...	0	84.2 K	14m 37s
...	...	TCP	807	10.17.4.136	eth0	10.17.94.120		eth0	default	default		MGMT-ACCESS	VRF-Classroom14o-1...	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	Dst 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-Classroom14o-1...	0	264.0	0s
...	...	TCP	443	192.168.0.1	eth2	23.23.250.232	62.99.0.29.11...	eth3	VR01	VR01		prytimes.chartbeat.net	VRF-Classroom14o-1...	0	4.3 K	0s
...	...	TCP	443	192.168.0.1	eth2	74.121.136.139	62.99.0.29.38...	eth3	VR01	VR01		sync.mathtag.com	VRF-Classroom14o-1...	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...	VRF-Classroom14o-1...	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	VRF-Classroom14o-1...	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	VRF-Classroom14o-1...	0	3.9 K	5s
...	...	TCP	443	192.168.0.1	eth2	172.217.23.196	62.99.0.29.58...	eth3	VR01	VR01		www.google.com	VRF-Classroom14o-1...	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	VRF-Classroom14o-1...	0	6.2 K	6s
...	...	ICMP		62.99.0.29	eth3	62.99.0.254		eth3	VR01	VR01		OP-SRV-VPN	VRF-Classroom14o-1...	0	240.0	6s
...	...	TCP	443	192.168.0.1	eth2	172.217.23.206	62.99.0.29.53...	eth3	VR01	VR01		consent.google.com	VRF-Classroom14o-1...	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	VRF-Classroom14o-1...	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-Classroom14o-1...	0	252.0	14s
...	...	UDP	53	192.168.0.1	eth2	9.9.9.9	62.99.0.29.48...	eth3	VR01	VR01			VRF-Classroom14o-1...	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	VRF-Classroom14o-1...	0	14.7 K	14s
...	...	TCP	443	192.168.0.1	eth2	13.32.153.247	62.99.0.29.58...	eth3	VR01	VR01		activity.stream-icons.s...	VRF-Classroom14o-1...	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	VRF-Classroom14o-1...	0	660.9 K	22s

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_flowng_through_all_router_instances.png
11. 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.