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

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

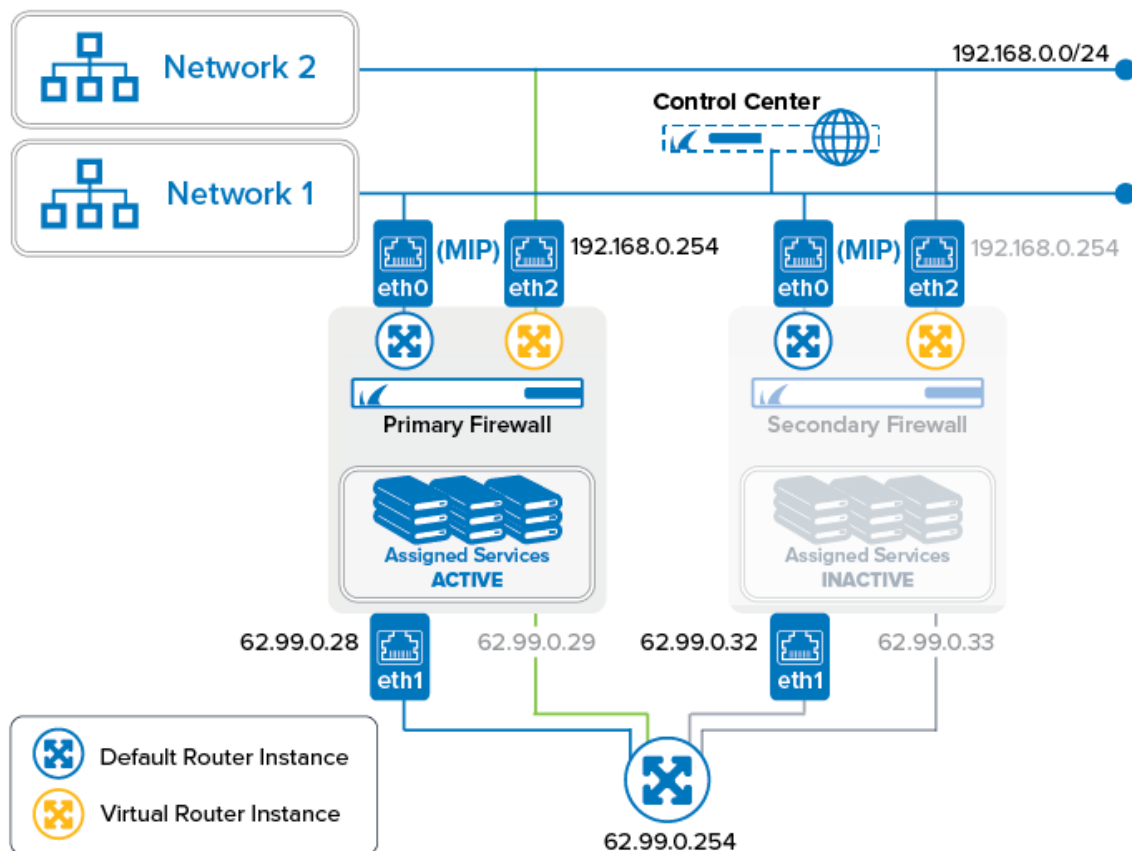
When configuring a virtual router instance for a CC-managed HA pair, the configuration is transparently transferred to the secondary firewall after being completed for the primary firewall. There is no need to make any configuration for the secondary firewall.

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

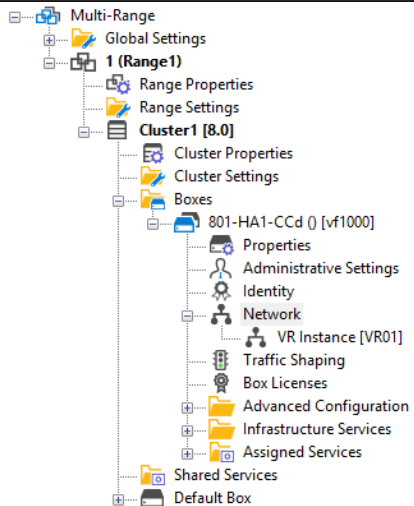
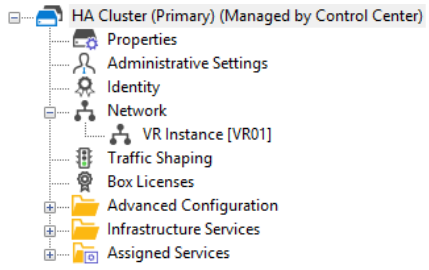
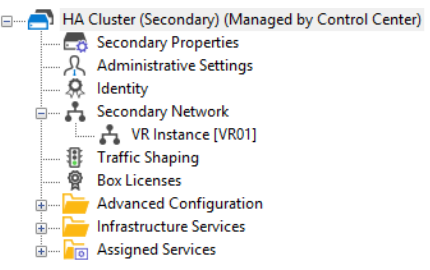
In the following example, an additional virtual instance will be created that routes traffic between a private network (e.g., 192.168.0.0/24) and the Internet. In this setup, the firewall service will be transparent to the additional virtual router instance only if authenticated users are not defined. 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
 <p>Multi-Range Global Settings 1 (Range1) Range Properties Range Settings Cluster1 [8.0] Cluster Properties Cluster Settings Boxes 801-HA1-CCd () [vf1000] Properties Administrative Settings Identity Network VR Instance [VR01] Traffic Shaping Box Licenses Advanced Configuration Infrastructure Services Assigned Services Shared Services Default Box</p>	 <p>HA Cluster (Primary) (Managed by Control Center) Properties Administrative Settings Identity Network VR Instance [VR01] Traffic Shaping Box Licenses Advanced Configuration Infrastructure Services Assigned Services</p>	 <p>HA Cluster (Secondary) (Managed by Control Center) Secondary Properties Administrative Settings Identity Secondary Network VR Instance [VR01] Traffic Shaping Box Licenses Advanced Configuration Infrastructure Services Assigned Services</p>

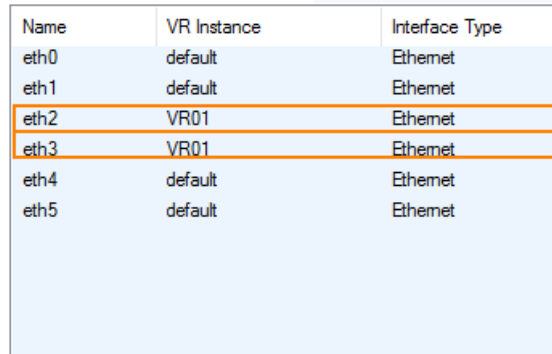
Step 2. Assign Interfaces to the VR Instance

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**.

VR Instance Interface Assignment

Interface Assignment



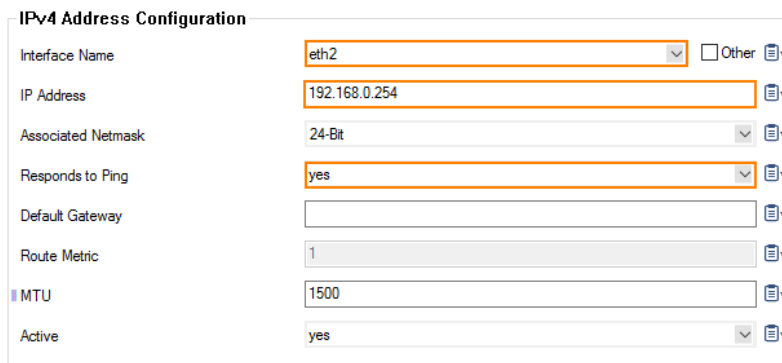
Name	VR Instance	Interface Type
eth0	default	Ethernet
eth1	default	Ethernet
eth2	VR01	Ethernet
eth3	VR01	Ethernet
eth4	default	Ethernet
eth5	default	Ethernet

Step 3. 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 your 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

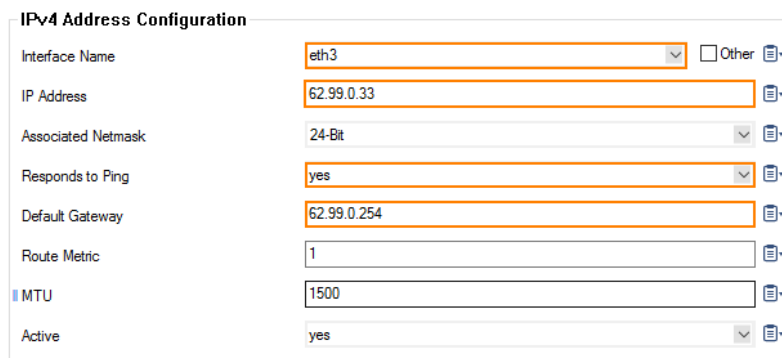
1. On your Control Center, go to **CONFIGURATION > Configuration Tree > Multi-Range > your range > your cluster > Boxes > your primary firewall > Network > VR Instance [your virtual instance]**.
2. In the left menu bar, select **IP Configuration**.
3. Click **Lock**.
4. Click **+** to assign the first 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.



IPv4 Address Configuration

Interface Name	eth2	<input type="checkbox"/> Other
IP Address	192.168.0.254	
Associated Netmask	24-Bit	
Responds to Ping	yes	
Default Gateway		
Route Metric	1	
MTU	1500	
Active	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.



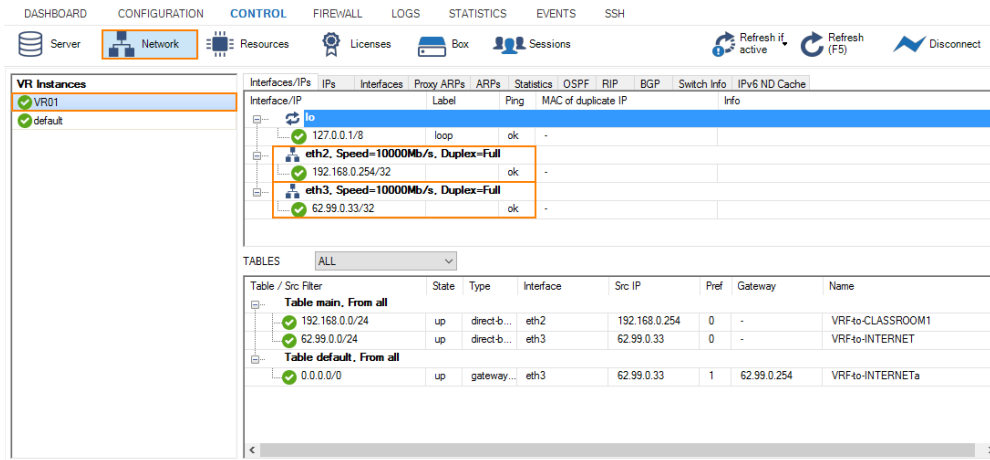
IPv4 Address Configuration

Interface Name	eth3	<input type="checkbox"/> Other
IP Address	62.99.0.33	
Associated Netmask	24-Bit	
Responds to Ping	yes	
Default Gateway	62.99.0.254	
Route Metric	1	
MTU	1500	
Active	yes	

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.



VR Instances

- VR01
- default

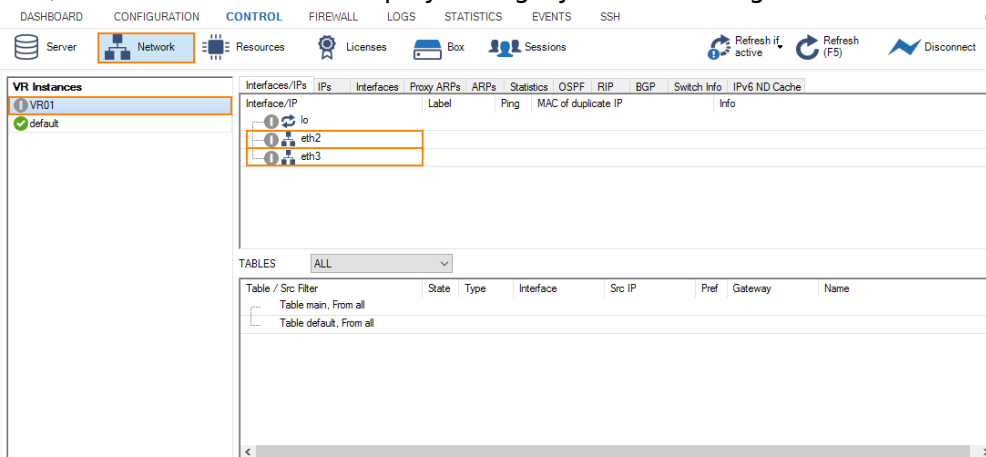
Interfaces/IPs

Interface/IP	Label	Ping	MAC of duplicate IP	Info
127.0.0.1/8	loop	ok	-	
eth2, Speed=10000Mb/s, Duplex=Full		ok	-	
192.168.0.254/32		ok	-	
eth3, Speed=10000Mb/s, Duplex=Full		ok	-	
62.99.0.33/32		ok	-	

TABLES

Table / Src Filter	State	Type	Interface	Src IP	Pref	Gateway	Name
Table main, From all	up	direct-b...	eth2	192.168.0.254	0	-	VRF-to-CLASSROOM1
62.99.0.0/24	up	direct-b...	eth3	62.99.0.33	0	-	VRF-to-INTERNET
Table default, From all	up	gateway...	eth3	62.99.0.33	1	62.99.0.254	VRF-to-INTERNETa

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.



VR Instances

- VR01
- default

Interfaces/IPs

Interface/IP	Label	Ping	MAC of duplicate IP	Info
lo				
eth2				
eth3				

TABLES

Table / Src Filter	State	Type	Interface	Src IP	Pref	Gateway	Name
Table main, From all							
Table default, From all							

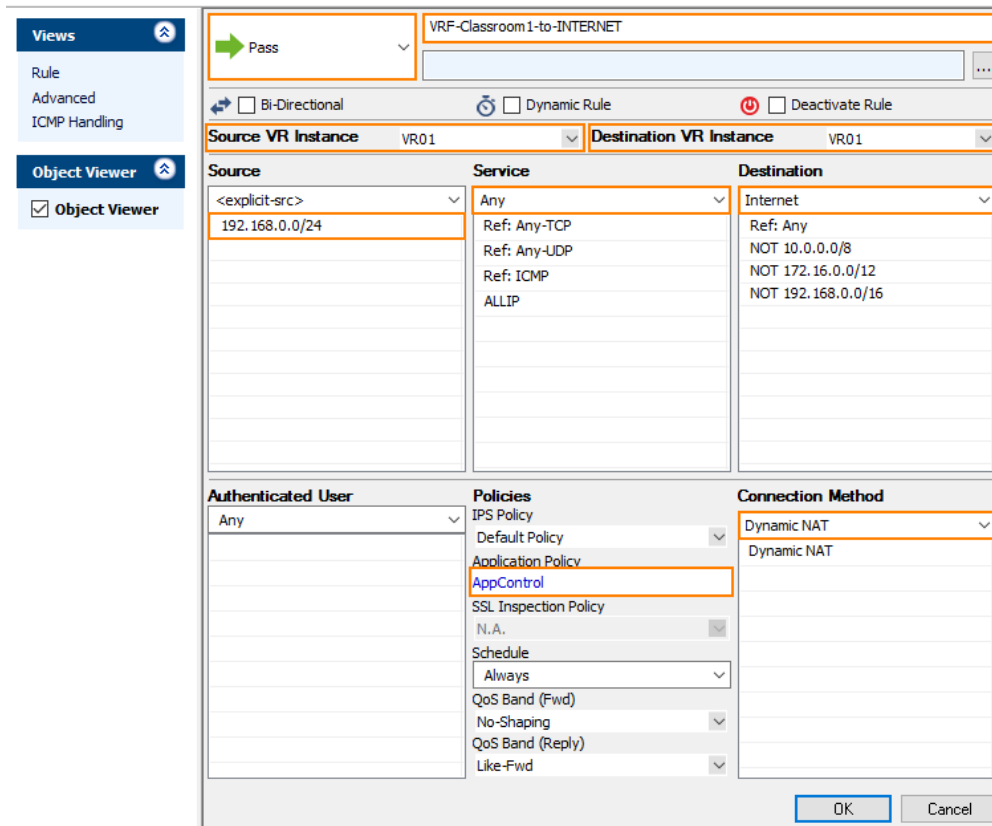
To activate the reverse HA constellation, perform an HA failover. For more information, see [How to Perform a Manual High Availability Failover](#). The upper two images will then be displayed with reversed configuration information accordingly.

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**.



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. The "Source VR Instance" and "Destination VR Instance" are both set to "VR01".

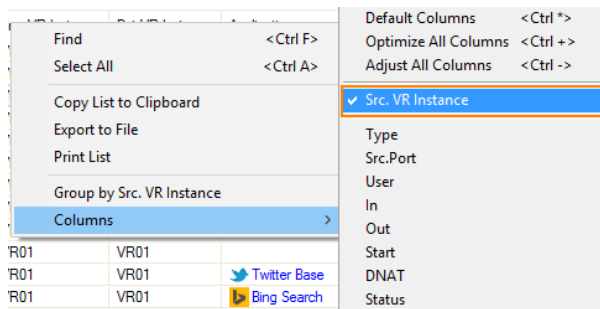
Source	Service	Destination
<explicit-src>	Any	Internet
192.168.0.0/24	Ref: Any-TCP Ref: Any-UDP Ref: ICMP ALLIP	Ref: Any NOT 10.0.0.0/8 NOT 172.16.0.0/12 NOT 192.168.0.0/16

Below the table, the "Authenticated User" is set to "Any". The "Policies" section includes "IPS Policy", "Default Policy", "Application Policy" (highlighted), "AppControl", "SSL Inspection Policy", "N.A.", "Schedule" (set to "Always"), "QoS Band (Fwd)", "No-Shaping", "QoS Band (Reply)", and "Like-Fwd". The "Connection Method" is set to "Dynamic NAT".

Buttons at the bottom: OK, Cancel.

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.

DASHBOARD		CONFIGURATION		CONTROL		RENEWAL		LOGS		STATISTICS		EVENTS		SSH			
Monitor		Live		History		Audit Log		Shaping		Users		Dynamic		Host Rules		Forwarding Rules	
																18 Sessions	
Traffic Selection																	
Forward, Local In, Local Out, IPv4, IPv6																	
Status Selection																	
Closing, Established, Failing, Pending																	

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.

DASHBOARD

CONFIGURATION

CONTROL

FIREWALL

LOGS

STATISTICS

EVENTS

SSH

Monitor

Live

History

Threat Scan

Audit Log

Shaping

Users

Dynamic

Host Rules

Forwarding Rules

16 Sessions

Traffic Selection

Forward, Local In, Local Out, IPv4, IPv6

Status Selection

Configured, Established, Failing, Pending

Src. VR Instance

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	nytimes.chartbeat.net		VRF-Classroom1-to-I...	0	254.0	0s
...	...	TCP	443	192.168.0.1	eth2	23.23.250.232	62.99.0.29.11...	eth3	VR01	VR01	sync.mathtag.com		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	messaging.notification		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	www.google.com		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	Google Services Base	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		VRF-Classroom1-to-I...	0	3.9 K	5s
...	...	TCP	443	192.168.0.1	eth2	172.217.23.196	62.99.0.29.58...	eth3	VR01	VR01	Google Services Base	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	Google Services Base	www.google.at	VRF-Classroom1-to-I...	0	6.2 K	6s
...	...	ICMP	62.99.0.29	eth3	62.99.0.254	eth0	10.17.94.1	eth0	VR01	VR01	OP-SRV-VPN		VRF-Classroom1-to-I...	0	240.0	6s
...	...	TCP	443	192.168.0.1	eth2	172.217.23.206	62.99.0.29.53...	eth3	VR01	VR01	Google Services Base	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	Google Services Base	et.static.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	static.nytimes.com		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	static.nytimes.com		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	activitystream-icons.s		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	activitystream-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		VRF-Classroom1-to-I...	0	660.8 K	22s

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_flowng_through_all_router_instances.png
13. traffic_flowng_only_through_VR01.png

© Barracuda Networks Inc., 2024 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.