

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

https://campus.barracuda.com/doc/96026379/

When configuring a virtual router instance for an HA pair, the configuration is transparently transferred to the secondary firewall after being completed on 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, see <u>How to Set</u> <u>Up a High Availability Cluster</u>.

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 <u>Virtual Routing and Forwarding (VRF)</u>.





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

When creating a router instance on the primary firewall, the configuration will be mirrored to the secondary 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.
- 9. Click **OK**.
- 10. Click Send Changes.
- 11. The Activate Changes window opens.
- 12. Click **Activate**.



VR Node on Primary Stand-alone Firewall	VR Node on Secondary Stand-alone Firewall (Configured via Primary)
🖃 📑 HA Cluster (Primary)	□····· 📑 HA Cluster (Secondary)
🛃 Box Properties	Secondary Properties
🔏 Administrative Settings	Administrative Settings
····· 😣 Identity	😣 Identity
🚊 🖧 Network	🚊 🚓 Secondary Network
······ 📇 VR Instance [VR01]	🖧 VR Instance [VR01.]
Traffic Shaping	📲 Traffic Shaping
	Administrators
Box Licenses	👰 Box Licenses
Advanced Configuration	🛓 🔚 Advanced Configuration
🛓 🔚 Infrastructure Services	🗄 Infrastructure Services
🗄 🔓 Assigned Services	🛓 📷 Assigned Services

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 primary firewall, double-click **CONFIGURATION > Configuration Tree > Box > 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	Ethemet	

Step 3. 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 4. Assign IP Addresses to the Interfaces of the VR Instance

- 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., eth 2 = 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-CLASSR00M1.
- 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 🗸	Other	∎-
IP Address	192.168.0.254		.
Associated Netmask	24-Bit	\sim	∎-
Responds to Ping	yes	\sim	∎-
Default Gateway			ī,
Route Metric	1		.
MTU	1500		۰.
Active	yes	\sim	ī,

- 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 Connydradon			
Interface Name	eth3	Other	•
IP Address	62.99.0.33		∎•
Associated Netmask	24-Bit	\sim	∎.
Responds to Ping	yes	\sim	∎-
Default Gateway	62.99.0.254		٦.
Route Metric	1		1
I MTU	1500		1
Active	yes	\sim	•

- 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**. Because the primary firewall is the active one, the interfaces with its IP addresses are displayed as configured.

Barracuda CloudGen Firewall



DASHBOARD	CONFIGURATION	CONTROL FIREWALL LOGS	S STATISTICS	EVENTS	SSH		Ċ
Server	Network	Resources 👰 Licenses	Box 🤱	Sessions		Refresh active	if C Refresh Not Disconnect
VR Instances		Interfaces/IPs IPs Interfaces I	Proxy ARPs ARPs	Statistics OSPF	RIP BGP Swit	ch Info IPv6 ND	Cache
🗸 VR01		Interface/IP	Label P	ng MAC of duplic	ate IP	Info	
🕑 default							
		2 127.0.0.1/8	loop c	k -			
		eth2, Speed=10000M	lb/s, Duplex=Full				
		192.168.0.254/32	c	k -			
		🛓 📥 eth3, Speed=10000M	lb/s, Duplex=Full				
		62.99.0.33/32	c	k -			
		1					
		TABLES ALL	\sim				
		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
		_					
		<					>
1		1					/

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.

DASHBUARD	CONFIGURATION	CONTROL FIREWALL	LOGS STATISTICS	EVENTS SSH		0
Server	Network	E Resources 🛛 👷 Lice	enses 📻 Box ₰	Sessions	Refresh if active	(F5) Refresh Disconnect
VR Instances		Interfaces/IPs IPs Ir	terfaces Proxy ARPs ARPs	Statistics OSPF RIP BGP	Switch Info IPv6 ND Cache	
VR01		Interface/IP	Label F	ing MAC of duplicate IP	Info	
🕑 defauit		-0≎ ⁰				
		0 📩 eth2				
		eth3				
		TABLES ALL	~			
		Table / Src Filter	State Type	Interface Src IP	Pref Gateway	Name
		Table main, From a	1			
		Table default, From	al			
		<				>

To activate the reverse HA constellation, perform an HA failover. For more information, see <u>How to</u> <u>Perform a Manual High Availability Failover</u>. 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. Go to CONFIGURATION > Configuration Tree > 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**.

Pass	VRF-Classroom1-to-INTER	NET
ed	nal 💍 🗌 Dynamic Ru	le 🕘 🗌 Deactivate Rule
Source VR Insta	nce VR01 VC	Destination VR Instance VR01
t Viewer 🔕 Source	Service	Destination
ect Viewer <a>	~ Any	V Internet
192.168.0.0/24	Ref: Any-TCP	Ref: Any
	Ref: Any-UDP	NOT 10.0.0.0/8
	Ref: ICMP	NOT 172.16.0.0/12
	ALLIP	NOT 192.168.0.0/16
Authenticated U	ser Policies	Connection Method
Any	V IPS Policy	Dynamic NAT
	Default Policy	Dynamic NAT
	Application Policy	
	SSL Inspection Policy	<i>v</i>
	N.A.	
	Schedule	
	Always	~
	QoS Band (Fwd)	
	No-Shaping	\checkmark
	No bridping	
	QoS Band (Reply)	

Step 7. 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**.



	Find Select All	<ctrl f=""> <ctrl a=""></ctrl></ctrl>	Default Columns Optimize All Columns Adjust All Columns	<ctrl *=""> <ctrl +=""> <ctrl -=""></ctrl></ctrl></ctrl>	
	Copy List to Clipboard		✓ Src. VR Instance		
	Export to File		Туре		
	Print List		Src.Port		
	Group by Src. VR Instance		User		
	Columns	>	ln Out		
'R01	VR01		Start		
'R01	VR01	🏈 Twitter Base	DNAT		
'R01	VR01	Bing Search	Status		

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., <u>www.nytimes.com</u>
- 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.

D	ASHBOARD	CONFIGU	JRATION	CONTRO	L FIR	EWALL LOC	SS STATIS	TICS E	VENTS SSH							C
۶	Monitor	(Å) Live	0	listory 🔽	Threat Scan	Audit Log	Shaping	1	lsers 💍 Dy	namic 🐪	Rules Porwarding		18 😪 18 Sess	iions	\$ ()	~
Traff	ic Selection	n Forward, I	Local In, Lo	ocal Out, IPv4, IF	Pv6 ♥ S	tatus Selection	Closing, Es	tablished, Faili	ng, Pending 🛛 💎	•						
ID	State	IP Protocol	Port	Source	Interface	Destination	SNAT	Output-IF	Src. VR Instance	Dst VR Instance	Application	Application Context	Rule	bit/s	Total	ldle ^
I	🚓 🐥	TCP	443	192.168.0.1	eth2	34.238.209.130	62.99.0.29:63	eth3	VR01	VR01		et nytimes.com	VRF-Classroom1 to-I	744	42.3 K	0s
I	🚓 🐥	TCP	443	192.168.0.1	eth2	74.121.136.139	62.99.0.29:38	eth3	VR01	VR01		sync.mathtag.com	VRF-Classroom1-to-I	744	10.0 K	Os
III	🚓 🐥	TCP	443	192.168.0.1	eth2	54.83.166.11	62.99.0.29:35	eth3	VR01	VR01		messaging-notification.	VRF-Classroom1-to-I	10.7 K	37.8 K	0s
I	🚓 🐥 —	TCP	807	10.17.4.136	eth0	10.17.94.120		eth0	default	default			MGMT-ACCESS	7.9 K	93.7 K	0s
I	🚓 🔶	ICMP .		62.99.0.29	eth3	62.99.0.254		eth3	VR01	VR01			QP-SRV-VPN	0	400.0	28
I	🚓 🐥 –	ICMP .		10.17.94.120	eth0	10.17.94.1		eth0	default	default			SOX-GW-TEST	0	390.0	7s
I	🚓 🔶 🚽	ICMP		62.99.0.28	eth1	62.99.0.254		eth1	default	default			QD-SRV-VPN	0	400.0	7s
I	🚓 🔶 –	TCP	443	192.168.0.1	eth2	54.197.225.116	62.99.0.29.22	eth3	VR01	VR01		prytimes.chartbeat.net	VRF-Classroom1-to-I	0	11.9 K	86
	🚓 🔶 🚽	TCP	443	192.168.0.1	eth2	172.217.23.196	62.99.0.29.22	eth3	VR01	VR01	G Google Services Base	www.google.com	VRF-Classroom1 to -I	0	364.4 K	37s
	- 4 * 4	TCP	443	192.168.0.1	eth2	172.217.23.196	62.99.0.29:58	eth3	VR01	VR01	G Google Services Base	www.google.com	VRF-Classroom1-to-I	0	8.2 K	38s
	🚓 🔶 –	TCP	443	192.168.0.1	eth2	172.217.19.67	62.99.0.29:48	eth3	VR01	VR01	G Google Services Base	www.google.at	VRF-Classroom 1-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	G Google Services Base	consent.google.com	VRF-Classroom1 to-I	0	58.4 K	39s
	- 4 * 4	TCP	443	192.168.0.1	eth2	172.217.23.195	62.99.0.29:38.	eth3	VR01	VR01	G Google Services Base	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 rytimes.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-stream-icons.s	VRF-Classroom1+to-I	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.nyt.com	VRF-Classroom1-to-I	0	659.7 K	56s
	🚓 🔶 👘	TCP	807	10.17.4.136	eth0	10.17.94.120		eth0	default	default			MGMT-ACCESS	0	84.2 K	14m 37s
	🚓 🔶	TCP	807	10.17.4.136	eth0	10.17.94.120		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.

D	ASHBOARD	CONFIGU	JRATION	CONTRO	L FIR	EWALL LOG	SS STATIS	TICS E	VENTS SSH							C
\$	Monitor	(Å) Live	1	History 🔽	Threat Scan	Audit Log	Shaping	1	sers 💍 Dy	namic 🐪	Host Forwarding Rules Rules		16 💏 Sess	ions	\$ (~
Traff	ic Selection	Forward, I	Local In, L	ocal Out, IPv4, IF	Pv6 🖤 S	tatus Selection	Closing, Est	tablished, Faili	ng, Pending 🛛 🛡	Src. VR Instar	nce 🗹 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	ldle ^
L	🚓 🐥	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	Os
I	🚓 🐥	TCP	443	192.168.0.1	eth2	23.23.250.232	62.99.0.29.11	eth3	VR01	VR01		pnytimes.chartbeat.net	VRF-Classroom1to-I	0	4.9 K	0s
I	🚓 🐥	TCP	443	192.168.0.1	eth2	74.121.136.139	62.99.0.29:38	eth3	VR01	VR01		sync.mathtag.com	VRF-Classroom1-to-I	0	10.7 K	36
I	🚓 🔶	TCP	443	192.168.0.1	eth2	54.83.166.11	62.99.0.29:35	eth3	VR01	VR01		messaging-notification	VRF-Classroom 1-to-I	0	48.5 K	48
I	🚓 🐥	TCP	443	192.168.0.1	eth2	172.217.23.196	62.99.0.29.22	eth3	VR01	VR01	G Google Services Base	www.google.com	VRF-Classroom1+to-I	0	364.9 K	5s
I	🚓 🔶	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	58
I	🚓 🐥 —	TCP	443	192.168.0.1	eth2	172.217.23.196	62.99.0.29.58	eth3	VR01	VR01	G Google Services Base	www.google.com	VRF-Classroom 1-to-I	0	8.7 K	6s
I	🚓 🐥 👘	TCP	443	192.168.0.1	eth2	172.217.19.67	62.99.0.29:48	eth3	VR01	VR01	G Google Services Base	www.google.at	VRF-Classroom1 to -1	0	6.2 K	68
I	🚓 🐣	ICMP		62.99.0.29	eth3	62.99.0.254		eth3	VR01	VR01			QP-SRV-VPN	0	240.0	6s
I	🚓 🐥	TCP	443	192.168.0.1	eth2	172.217.23.206	62.99.0.29.53	eth3	VR01	VR01	G Google Services Base	consent.google.com	VRF-Classroom 1 to -1	0	58.8 K	85
I	🚓 🐣	TCP	443	192.168.0.1	eth2	172.217.23.195	62.99.0.29:38	eth3	VR01	VR01	G Google Services Base	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-Classroom 1-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	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-stream-icons.s	VRF-Classroom 1-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.nyt.com	VRF-Classroom1-to-I	0	660.8 K	22s



Figures

- 1. vr_ha_standalone_80.png
- 2. ha_VR_node_created_on_primary.png
- 3. ha_VR_node_created_on_secondary.png
- 4. vrf_standalone_HA_primary_network_node_configured.png
- 5. vrf_standalone_HA_configure_primary_interface.png
- 6. vrf_standalone_HA_configure_second_interface.png
- 7. vrf standalone HA configuration complete HA1.png
- 8. vrf_standalone_HA_configuration_complete_HA2.png
- 9. vrf_enter_access_rule_for_vr01.png
- 10. vrf_select_vr_column_to_display.png
- 11. vrf_traffic_flowing_through_all_router_instances.png
- 12. traffic flowing 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.