

# How to Perform a Manual High Availability Failover

#### https://campus.barracuda.com/doc/96026368/

In an HA setup, the primary CloudGen Firewall stays active until a serious problem occurs. If services must be shut down (for example, for system maintenance), you can do a manual failover. When you do so, the primary firewall sends a signal to the secondary unit which, in turn, immediately activates the services followed by an immediate shutdown of all services running on the primary unit. This mechanism works identically for an HA pair that is managed by a Barracuda Firewall Control Center and a stand-alone HA pair.

### Step 1. Perform a High Availability Failover

This case assumes that the primary firewall is the active one while the secondary firewall is on standby (although the example also applies if the primary unit is on standby and the secondary unit is the active one). This is the setup that applies to the default state of two firewalls running in an HA configuration. When the failover is completed, the new status of both firewalls is locked so that it cannot be reverted accidentally.

In case a failover has already been initiated, continue with Step 2.

DASHBOARD       CONFIGURATION       CONTROL       FIREWALL       VPN       LOGS       STATISTICS       EVENTS       SSH         Services	C Disconnect
Services Services     Services </th <th>Disconnect</th>	Disconnect
Primary (connected to)     Secondary @       @Restart Shared Services     Creater Allower	•
PRIMARY (CONNECTED TO)	0
PRIMARY (CONNECTED TO)	•
Sestart Shared Services & Restart Network Restart Firmware C Restart Box	
Active	
Model VF1000 Model VF1000	
Firmware Version 8.3.1-0077 Firmware Version 8.3.1-0077	
Uptime 33d 17h 28m 51s Uptime 33d 17h 29m 13s	
System Time Tues System Time Tues	
Management IP 🥥 10.17.37.211/24 💮 Management IP 🔮 10.17.37.212/24	
Shared IP         Interview         Interview <t< th=""><th></th></t<>	
Services       Retwork       Centres       Admin       Centres       Admin       Centres         Hardware       Services       Network       Licenses       Admin       Hardware	
V INTERFACES on Primary	ø
eth0 eth1 eth2 eth3	
V SERVICES on Primary 🔅 V 🕕 SERVICES on Secondary HA Partner: Naath-HA	0
b 🚍 Box Services	
1 Distributed-Firewall OutlerFW 🕘	$\overline{\mathbf{\Theta}}$
Re Secure Access Controller 📀 NaathSACK 🥑 Recure Access Controller 🕕 NaathSACK	

1. Go to CONTROL > Services

- 2. Click the **Failover** button in the status area below the ribbon bar.
- 3. The firewall performs the failover.
- The High Availability Status bar now displays HA Takeover Blocked.



- 5. The **Failover** button is displayed grayed indicating that another HA failover is currently not possible.
- 6. In the HA status bar, the current state now reports: "High Availability Status: Backup Appliance has taken over".
- 7. The new firewall service status displays the status of the services on the **PRIMARY** firewall as **Blocked** and the services on the **SECONDARY** as **Active**.

ASHBOARD CONFIGURATION CO	NTROL FIREWALL VPN LOG	S STATISTICS EVENTS	S SSH		
Services Network	Resources 🖗 Licenses 🕞	Box NR Sessions		Refresh if active	C (F5) C Disconne
High Availability Status: HA Failover Blo	cked			Failover	Unlock Failover
PRIMARY (CONNECTED TO)		ö			ö
Restart Shared Services	Network 🖳 Restart Firmware 🔗 Restart I	Box	Restart Shared Services	lestart Network 🔊 Restart Firmware 🔿 Resta	art Box
Blocke	d		Activ	e	
Model	VF1000		Model	VF1000	
Firmware Version	8.3.1-0077		Firmware Version	8.3.1-0077	
Uptime	33d 18h 31m 59s		Uptime	33d 18h 32m 22s	
System Time	Tue		System Time	Tue	
Management IP	✓ 10.17.37.211/24	$\overline{\mathbf{\Theta}}$	Management IP	✓ 10.17.37.212/24	
Shared IP	0	$\overline{\Theta}$	Shared IP	✓ 127.0.0.9/32	
Services Network Licenses	Admin Hardware		Services Network Licenses	Admin Hardware	
V INTERFACES on Primary		0	V INTERFACES on Secondar	y HA Partner: Naath-HA	0
eth0 eth1 eth2 eth3			eth0 eth1 eth2 eth3		
SERVICES on Primary		0	✓ SERVICES on Secondary H	IA Partner: Naath-HA	0
Box Services	0		Box Services	0	
↑ Distributed-Firewall	ClusterFW	$\overline{\mathbf{\Theta}}$	1 Distributed-Firewall	📀 ClusterFW	Э
Secure Access Controller	NaathSACK	9	Secure Access Controller	North SACK	9

8. The Services icon is displayed in red color, indicating that all services are currently blocked. In the image above, the element for the services still shows all services with a leading green bullet because the services are still running on the primary unit and because the services on the secondary unit have still not taken over.

### (optional) Step 2. Release the HA-Failover Lockdown

To revert the failover to the standard status where the **PRIMARY** is **Active** and the **SECONDARY** is **Blocked**, you must first release the HA-failover lock. This will reactivate all services and keep them in a wait state in case the failover must be subsequently reverted.

- 1. Go to **CONTROL > Services**.
- 2. Click **Unlock Failover** in the status bar below the ribbon bar.
- 3. The status of the **PRIMARY** firewall is now displayed to be on **Standby** while the **SECONDARY** is **Active**.

### Barracuda CloudGen Firewall



	Resources & Licenses E Box > 96	Sessions		1 active	
High Availability Status: Backup Applia	nce has taken Over			Failover Lock Fa	ilover
PRIMARY (CONNECTED TO)		0	SECONDARY 🕘		
Restart Shared Services	t Network 💭 Restart Firmware 🔿 Restart Box		Restart Shared Services	twork 📮 Restart Firmware 🔿 Restart Box	
Standt	у		Active		
Model	VF1000		Model	VF1000	
Firmware Version	8.3.1-0077		Firmware Version	8.3.1-0077	
Uptime	33d 17h 32m 20s		Uptime	33d 17h 32m 43s	
System Time	Tue		System Time	Tue	
Management IP	10.17.37.211/24	$\overline{\mathbf{O}}$	Management IP	10.17.37.212/24	
Shared IP	0	$\overline{\mathbf{\Theta}}$	Shared IP	✓ 127.0.0.9/32	
Services Network Licenses	Admin Hardware		Services Network Licenses	R =∰ Hardware	
V INTERFACES on Primary		0	V INTERFACES on Secondary HA Pa	irtner: Naath-HA	
eth0 eth1 eth2 eth3			eth0 eth1 eth2 eth3		
V SERVICES on Primary		0	✓ SERVICES on Secondary HA Partney	er: Naath-HA	
Box Services	Ø		Box Services	0	

4. The **Services** icon is no longer displayed in red color, indicating that all services are ready to be reactivated.

### (optional) Step 3. Revert the HA-Failover to its Standard Configuration

- 1. Go to **CONTROL > Services**.
- 2. Click the **Failover** button in the status area below the ribbon bar.
- 3. The firewall performs the failover.

## Barracuda CloudGen Firewall



Services $\swarrow$ Network =	Resources 🚱 Licenses д Box 🔗	R Sessions		Refresh if Refresh	📈 Dis
00 111		1			
High Availability Status: HA Fallover Blo	cked			Failover Unlock Fai	lover
PRIMARY (CONNECTED TO)		ø	SECONDARY ()		
Restart Shared Services Restart I	Network Restart Firmware CRestart Box		Restart Shared Services	rt Network 🖳 Restart Firmware 🥂 Restart Box	
Active			Blocke	b	
Model	VF1000		Model	VF1000	
Firmware Version	8.3.1-0077		Firmware Version	8.3.1-0077	
Uptime	33d 17h 26m 28s		Uptime	33d 17h 26m 51s	
System Time	Tue		System Time	Tue	
Management IP	10.17.37.211/24	$\overline{\mathbf{O}}$	Management IP	2 10.17.37.212/24	
Shared IP	127.0.0.9/32	$\overline{\mathbf{\Theta}}$	Shared IP	0	
Services Network Licenses	Admin E		Services Network Licenses	Admin Hardware	
V INTERFACES on Primary		0	✓ INTERFACES on Secondary H/	A Partner: Naath-HA	
eth0 eth1 eth2 eth3			eth0 eth1 eth2 eth3		
✓ SERVICES on Primary		¢	V SERVICES on Secondary I	HA Partner: Naath-HA	
Box Services	Ø		Box Services	0	
↑ Distributed-Firewall	📀 ClusterFW	$\overline{\mathbf{\Theta}}$	1 Distributed-Firewall	ClusterFW	
0		0	0	0	

- 4. The **Services** icon is displayed in red color, indicating that all services are currently blocked.
- 5. Click Unlock Failover to switch the HA partners to their default state and prepare them for a future failover. All services on the secondary unit are displayed with a gray status bullet, indicating that they are prepared for the next HA failover. EVENTS SSH

ASHBOARD CONFIGURATION	CONTROL FIREWALL VPM	LOGS	STATISTICS EVENTS	SSH	
Services Network	E	Bo:	x AR Sessions	Refresh if active	N Disconnect
High Availability Status: OK			Failover	Lock Failov	er
PRIMARY		0	SECONDARY 🔿		0
Restart Shared Services Restart Net	work Restart Firmware Restart Box		Restart Shared Services Resta	art Network Restart Firmware Restart Box	(
Active			Standby	,	
Model	VF1000		Model	VF1000	
Uptime	14d 18h 14m 36s		Uptime	14d 18h 14m 31s	
System Time	Wed 2019		System Time	Wed 2019	
Management IP	/24	€	Management IP	24	
Shared IP	2 127.0.0.9/32	€	Shared IP	0	
Services Network Licenses	Admin Hardware		Services Network Lic	Admin     Image: Constraint of the second seco	
V INTERFACES on Primary		0	V INTERFACES on Seco	ondary HA Partner	0
eth0 eth1 eth2 eth3			eth0 eth1 eth2 eth	h3	
✓ SERVICES on Primary		0	✓ ● SERVICES on Set	condary HA Partner	ø
Box Services	0		Box Services	0	
Firewall	📀 NGFW	$\overline{\mathbf{O}}$	Firewall	NGFW	$\overline{\mathbf{\Theta}}$
VPN-Service	📀 vpn	$\overline{\mathbf{\Theta}}$	VPN-Service	O vpn	$\overline{\mathbf{\Theta}}$



6. In the HA status bar, the current state now reports: "High Availability Status: OK".

### Barracuda CloudGen Firewall



#### Figures

- 1. HA\_before\_failover.png
- 2. HA\_failover\_performed.png
- 3. HA\_failover\_unlocked.png
- 4. HA\_failover\_after\_reversion.png
- 5. HA\_in\_default\_state.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.