

How to Update Managed High Availability Clusters with Automatic Failover

<https://campus.barracuda.com/doc/70584915/>

To update the high availability cluster using automatic failover, both firewalls must be enabled. The passive firewall must be updated first while the active firewall keeps operating. After the passive firewall update is complete, the active firewall will automatically transfer control to the passive firewall and make it the active one. After the update of the primary firewall is complete, control will be transferred from the active secondary firewall back to the primary firewall. The secondary firewall will fall back to stay in passive mode.

If required, update your Control Center before updating your managed firewalls to a newer firmware version. After major version updates, the cluster version on the Control Center must be migrated to match the new firmware version.

The Control Center checks every hour for updates relevant to the configured cluster versions. It can take up to one hour for the updates, hotfixes, and patches to be displayed when a new cluster with a previously unused cluster version is created.

Before You Begin

If you are using SSL Interception on your border firewall, you must add **dlportal.barracudanetworks.com** and **d.barracudanetworks.com** to the SSL Interception **Domain Exceptions** on the **your F-Series Firewall > Virtual Servers > Assigned Services > Firewall > Security Policy** page.

Exception Handling

Domain Exceptions



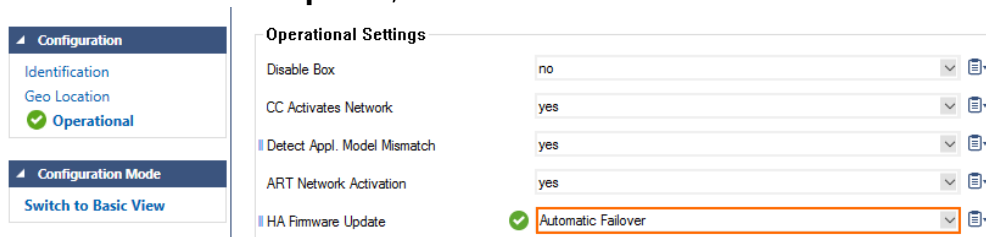
Step 1: Verify the Compatibility of the Control Center Firmware with the Managed Firewalls

Before updating a managed firewall to a higher firmware version, verify that the Control Center is running a firmware version that is equal to or higher than the highest firmware version used by a managed firewall after the update.

For more information, see [Updating F-Series Firewalls and Control Centers](#).

Step 2. Enable Automatic Failover

1. Go to **CONFIGURATION > Configuration Tree > Box > Box Properties**.
2. In the left menu, click **Operational**.
3. Expand the **Configuration Mode** menu and select **Switch to Advanced View**.
4. Click **Lock**.
5. From **HA Firmware Update**, select **Automatic Failover**.



Operational Settings	
Disable Box	no
CC Activates Network	yes
Detect Appl. Model Mismatch	yes
ART Network Activation	yes
HA Firmware Update	Automatic Failover

6. Click **Send Changes** and **Activate**.

Step 3. Download the Update Package to the Control Center

Download the update package to the Control Center.

1. Log into the Control Center.
2. Go to **CONTROL > Firmware Update**.
3. In the lower half of the screen, click the **Download Portal** tab.
4. Hover the mouse over the desired update package to display the download icon.

Download Portal					Files on Control Center
Filter	Filter	Filter	Filter	Filter	
Scope	Type	Release Date	For Versions	Name	
Maintenance	Package	24.08.2016	7.0	Hotfix 789 - Cumulative Hotfix	
Maintenance	Package	03.08.2016	7.0	Hotfix 793 - Virscan Service	
Maintenance	Package	03.08.2016	6.1	Hotfix 795 - Virscan Service	
Maintenance	Package	11.07.2016	6.0, 6.1, 6.2	Update package for NextGen F-Series from 6.X to 6.2.2	
Maintenance	Package	03.06.2016	6.0, 6.1, 6.2, 7.0	Update package for NextGen F-Series from 6.X to 7.0.0	
Maintenance	Package	05.05.2016	6.1	Hotfix 776 - SSLv2	
Maintenance	Package	23.03.2016	6.1	Hotfix 766 - DNS Server	
Security	Package	23.02.2016	6.1	Hotfix 749: glibc (CVE-2015-7547)	
Maintenance	Package	15.02.2016	6.0, 6.1, 6.2	Barracuda NG Firewall and NG Control Center 6.2.1 Update Package to update from 6.0.x and 6.1.x	
	App				

5. Click the download icon, and select **Download**.

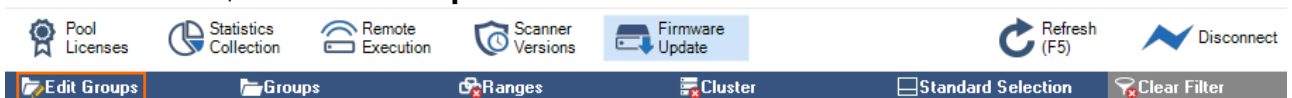
Download Portal					Files on Control Center
Filter	Filter	Filter	Filter	Filter	
Scope	Type	Release Date	For Versions	Name	
Maintenance	Package	24.08.2016	7.0	Hotfix 789 - Cumulative Hotfix	
Maintenance	Package	03.08.2016	7.0	Hotfix 793 - Virscan Service	
Maintenance	Package	03.08.2016	6.1	Hotfix 795 - Virscan Service	
Maintenance	Package	11.07.2016	6.0, 6.1, 6.2	Update package for NextGen F-Series from 6.X to 6.2.2	
Maintenance	Package	03.06.2016	6.0, 6.1, 6.2, 7.0	Update package for NextGen F-Series from 6.X to 7.0.0	
Maintenance	Package	05.05.2016	6.1		
Maintenance	Package	23.03.2016	6.1		
Security	Package	23.02.2016	6.1		
Maintenance	Package	15.02.2016	6.0, 6.1, 6.2		
	App				

After the download finishes, the update package is available in the **Files on Control Center** tab.

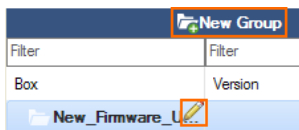
Download Portal					Files on Control Center
					<input type="button" value="Schedule File Transfer"/> <input type="button" value="Import local File"/>
Scope	Type	Release Date	For Versions	Name	
Maintenance	Package	16.03.2017	6.0, 6.1, 6.2, 7.0	Update package for NextGen F-Series from 6.X and 7.0.X to 7.0.2	

Step 4. (optional) Create Update Groups

- Go to **CONTROL > Firmware Update**.
- In the ribbon bar, click **Edit Groups**.



- Click **New Group**. A new update group is created in the list.
- Hover the mouse over the new group and click the edit icon.



- Enter a name for the update group.
- (optional) Use the Filter options to display the firewalls you want to add to this group.

New Group							
Filter		Filter		Filter		Filter	
Box	Version	Hotfixes	IP	Unit Description	Primary Server	Secondary Server	Last Status
Default Group							
HQ-NG1	7.1.0-290.ni...		10.0.10.33	Headquarters	VIRT1_HQ_1		05.04.2017 08:50:56
HQ-NG2	7.1.0-290.ni...		10.0.10.34	Headquarters HA		VIRT1_HQ_1	05.04.2017 08:50:04
HQFirewalls							

- Select, then drag and drop firewalls to the new user group.
- Click **Save Changes**.

New Group	Remove Group	Save Changes	Discard Changes	Edit Groups	Groups
HQ-NG	Filter	Filter	Filter	Filter	Filter
Box	Version	Hotfixes	IP	Unit Description	Primary Server
Default Group					Secondary Server
HQFirewalls					Last Status
HQ-NG1	7.1.0-290.ni...		10.0.10.33	Headquarters	VIRT1_HQ_1
HQ-NG2	7.1.0-290.ni...		10.0.10.34	Headquarters HA	VIRT1_HQ_1

Step 5. Select Firewalls and Schedule File Transfer

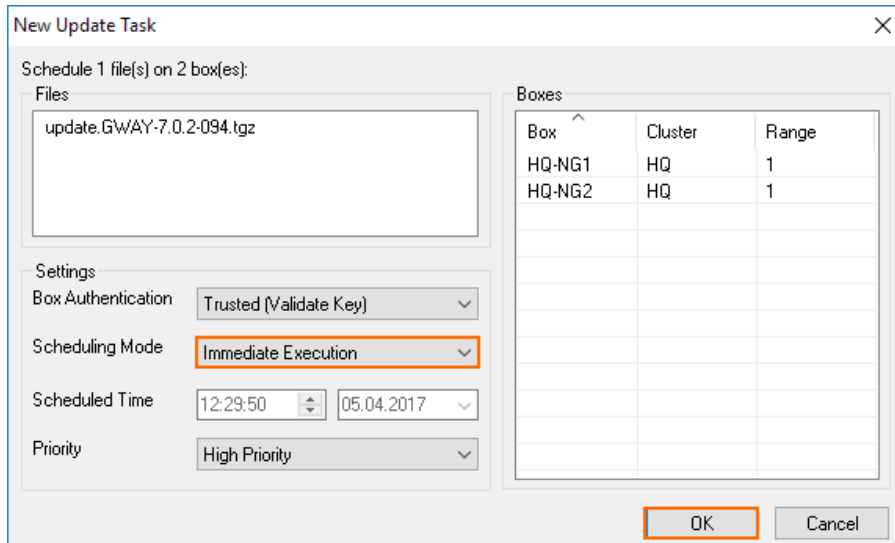
1. Go to **CONTROL > Firmware Update**.
2. Double-click on both firewalls on the HA cluster to add them to the **Selected Firewall Update List**.

CONTROL	CONFIGURATION	DATABASE	ADMINS	STATISTICS	EVENTS	NETWORK ACCESS CLIENT
Status Map	Zero Touch Deployment	Geo Maps	Configuration Updates	File Updates	Sessions	Barracuda Activation
Filter	Filter	Filter	Filter	Filter	Filter	Filter
Box	Version	Hotfixes	IP	Unit Description	Primary Server	Secondary Server
Default Group						
HQFirewalls						
Selected Units for new Update Task						
HQ-NGF1	7.1.0-338.ni...		10.0.10.33	Unit Description	Primary Server	Secondary Server
HQ-NGF2	7.1.0-338.ni...		10.0.10.34		VIRT1_HQ_1	

3. In the **Files on Control Center** tab, select the update package.
4. Click **Schedule File Transfer**. The **New Update Task** window opens.

Download Portal				Files on Control Center	
				Schedule File Transfer	Import local File
Scope	Type	Release Date	For Versions	Name	
Maintenance	Package	16.03.2017	6.0, 6.1, 6.2, 7.0	Update package for NextGen F-Series from 6.X and 7.0.X to 7.0.2	
Maintenance	Package	22.11.2016	7.0	Hotfix 812 - DNS Server	
Maintenance	Package	17.11.2016	7.0	Hotfix 811 - SSL VPN	
Maintenance	Package	10.11.2016	7.0	Hotfix 809 - Public Cloud VPN Service	

5. (optional) Select the **Scheduling Mode** and **Schedule Time** to schedule a time for the file transfer.



New Update Task

Schedule 1 file(s) on 2 box(es):

Files
update.GWAY-7.0.2-094.tgz

Boxes

Box	Cluster	Range
HQ-NG1	HQ	1
HQ-NG2	HQ	1

Settings

Box Authentication: Trusted (Validate Key)

Scheduling Mode: **Immediate Execution**

Scheduled Time: 12:29:50 05.04.2017

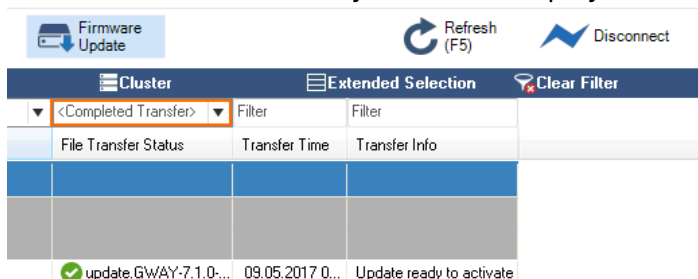
Priority: High Priority

OK Cancel

6. Click **OK**.

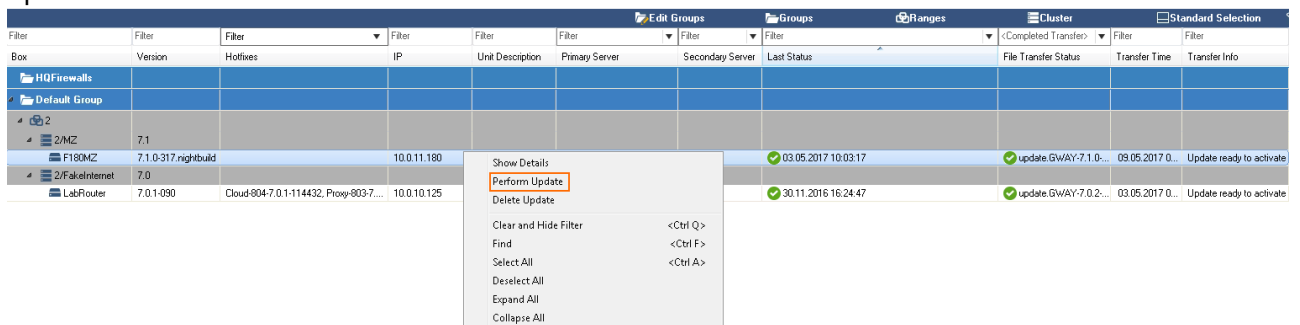
Step 6. Schedule Update for the Secondary Firewall

- Go to **CONTROL > Firmware Update**.
- In the **File Transfer Status** column, filter for **Completed Transfer**. The list of completed transfers for the secondary firewall is displayed.



File Transfer Status	Transfer Time	Transfer Info
update.GWAY-7.1.0-...	09.05.2017 0...	Update ready to activate

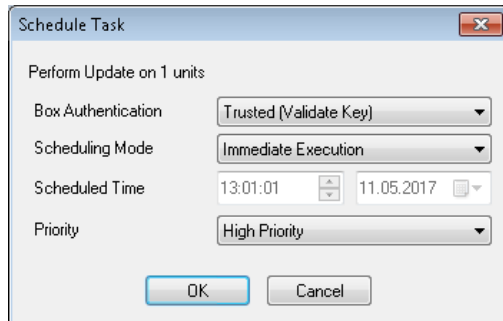
- Select the secondary firewall to perform the update.
- Right-click the secondary firewall and click **Perform Update**. The **Schedule Task** window opens.



Box	Version	Hotfixes	IP	Unit Description	Primary Server	Secondary Server	Last Status	File Transfer Status	Transfer Time	Transfer Info
HQFirewalls										
Default Group										
2										
F180M2	7.1	0-317 nightbuild	10.0.11.180				03.05.2017 10:03:17	update.GWAY-7.1.0-...	09.05.2017 0...	Update ready to activate
2/FakeInternet	7.0									
LabRouter	7.0.1-090	Cloud-804-7.0.1-114432, Proxy-803-7...	10.0.10.125				30.11.2016 16:24:47	update.GWAY-7.0.2-...	03.05.2017 0...	Update ready to activate

- (optional) Configure the time and authentication settings for the update:
 - Box Authentication** – Select **Trusted (Validate Key)**.
 - Scheduling Mode** – Select **Immediate Execution** to update immediately, or **Delayed Execution** to set the time the update is triggered.

- **Priority** – When multiple tasks are configured for execution, the priority setting determines the execution order.



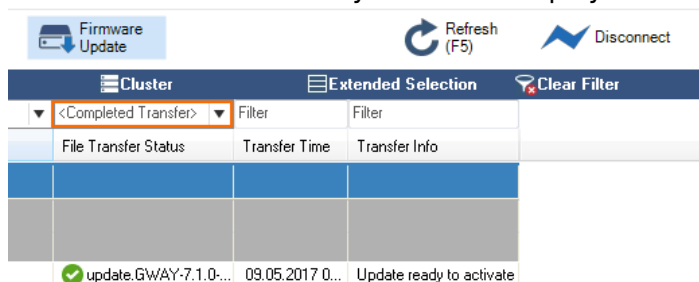
6. Click **OK**.

Wait for the update to finish. Depending on the system hardware, the process can last anywhere from 15 minutes (for a fast system) to 60 minutes (for flash appliances).

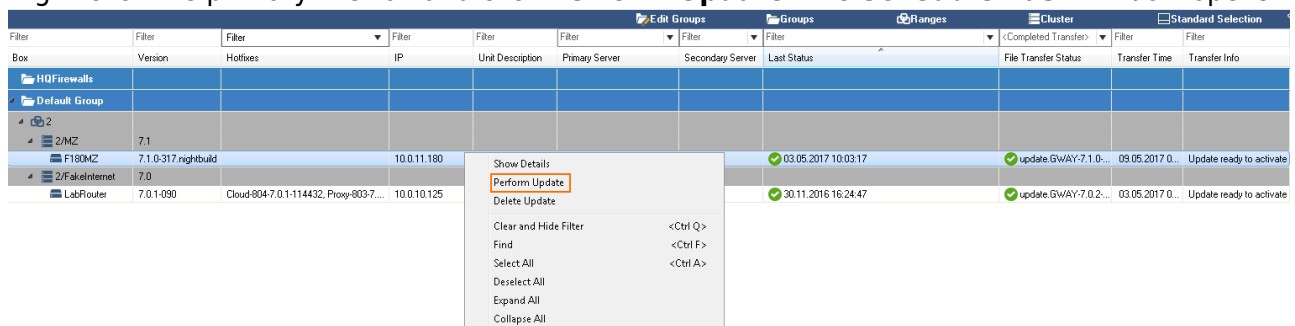
Unless otherwise noted, the firewall will reboot after the update.

Step 7. Schedule Update for the Primary Firewall

1. Go to **CONTROL > Firmware Update**.
2. In the **File Transfer Status** column, filter for **Completed Transfer**. The list of completed transfers for the secondary firewall is displayed.

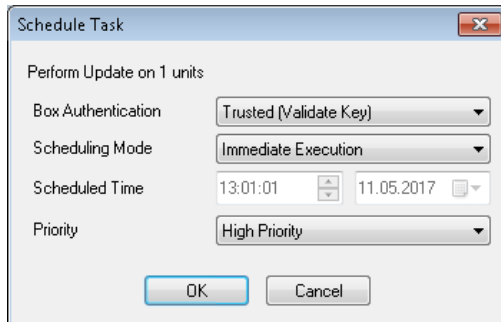


3. Select the primary firewall to perform the update.
4. Right-click the primary firewall and click **Perform Update**. The **Schedule Task** window opens.



5. (optional) Configure the time and authentication settings for the update:
 - **Box Authentication** – Select **Trusted (Validate Key)**.

- **Scheduling Mode** – Select **Immediate Execution** to update immediately, or **Delayed Execution** to set the time the update is triggered
- **Priority** – When multiple tasks are configured for execution, the priority setting determines the execution order.



6. Click **OK**.

When the firmware update starts at the scheduled time, the primary firewall will automatically transfer control over to the secondary firewall. The update packages will be copied to the primary firewall. After the update, server control will be completely transferred back from the secondary firewall to the primary firewall.

Wait for the update to finish. Depending on the system hardware, the process can last anywhere from 15 minutes (for a fast system) to 60 minutes (for flash appliances).

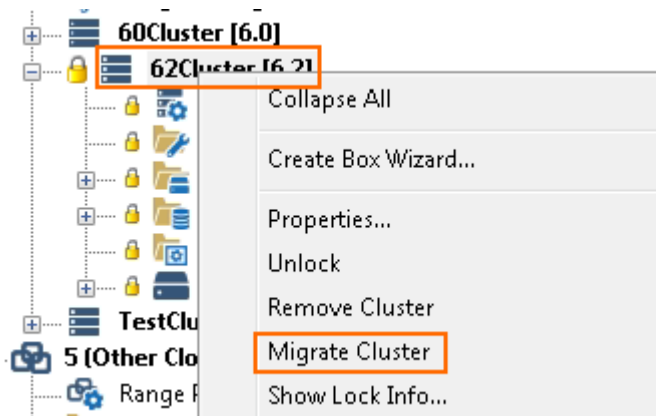
Unless otherwise noted, the firewall will reboot after the update.

Step 8. Migrate the Configuration Version of the Cluster

If you are updating to a new major version (e.g., 6.0 to 6.2, or 6.2 to 7.1), migrate the cluster version to the new major version after the update has completed. Multiple migrations may be required to reach the cluster version matching the firmware version.

Update the Clusters Individually

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > your range > your cluster**.
2. Right-click the cluster and select **Lock**.
3. Right-click the cluster and select **Migrate Cluster**.

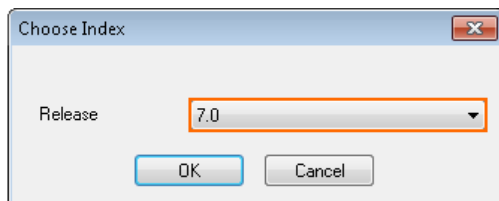


4. Select the new **Release** version.
5. Click **OK**.
6. Click **Activate**.

Update All Clusters in a Range

If all clusters in the range are on the same firmware version, you can migrate all clusters simultaneously.

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > your range**.
2. Right-click the range and select **Lock**.
3. Right-click the range and select **Migrate Range**.
4. Select the new **Release** version.
5. Click **OK**.



6. Click **Activate**.

Migrating the cluster version may have to be done multiple times if the firmware update skipped major firmware versions. E.g., when updating from 6.0 to 7.0.

Troubleshooting / Logs

After the update process, review the **Box\Release\update** or **Box\Release\update_hotfix** log for each system to verify that it was successfully updated. To view a system log, you must connect directly to the firewall and go to the **Logs** tab.

Figures

1. fw_update00.png
2. activate_ha_automatic_failover_00.png
3. cc_update_element_01.png
4. cc_update_element_02.png
5. cc_update_element_03.png
6. fwupdate_groups_01.png
7. fwupdate_groups_02.png
8. fwupdate_groups_03.png
9. fwupdate_groups_04.png
10. HA_firewalls_selected_for_update.png
11. managed_updates_02.png
12. managed_updates_03.png
13. managed_updates_04.png
14. managed_updates_05.png
15. managed_updates_06.png
16. managed_updates_04.png
17. managed_updates_05.png
18. managed_updates_06.png
19. managed_updates_07.png
20. managed_updates_08.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.