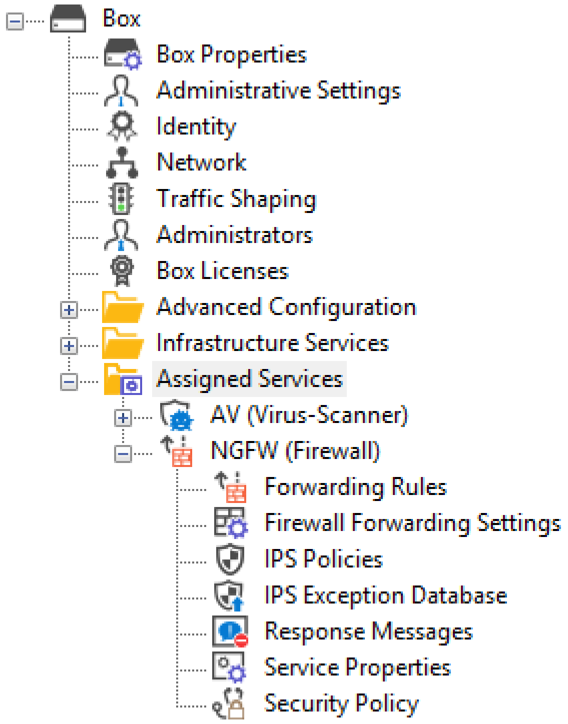
Transforming the Server Node to the Assigned Services Node (optional)

https://campus.barracuda.com/doc/93200135/

This article applies only to firewalls that are operating firmware 8.0.1, 8.0.2, 8.0.3, 8.0.4 or 8.0.5 and still display the old 3-layer architecture for server-service nodes in the configuration tree.

With the release of firmware version 8.0.2, you can now choose to transform the old 3-layer architecture to the new 2-layer architecture that was introduced with firmware version 8.0.1.



Choosing to do so is optional for firmware release 8.0.4 and will be enforced in the upcoming firmware versions.

The following table shows the different versions of how to migrate the server node to the new **Assigned Services** node:

Type of Firewall	Follow Migration Instructions
Stand-alone firewalls and CC (box-level only)	How to Migrate the Server Node to the Assigned Services Node for Stand-Alone Firewall and Control Centers (Box-Level only)
CC-managed firewalls	How to Migrate the Server Node to the Assigned Services Node for CC-Managed Firewalls

Stand-alone HA pairs	How to Migrate the Server Node to the Assigned Services Node for Stand-Alone HA Pairs
CC-managed HA pairs	How to Migrate the Server Node to the Assigned Services Node for CC-Managed HA Pairs

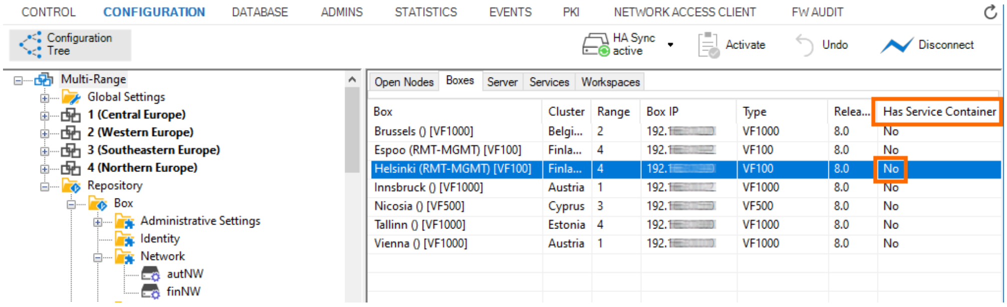
It is not possible to migrate boxes that have repositories linked to

- BOX/ Properties
- BOX/Network
- BOX/Infrastructure/Control

These nodes must be unlinked before starting the Assigned-Service-Migration process!

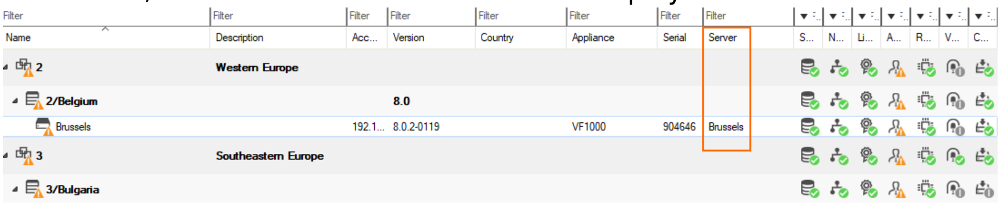
Known Issue after Box-Server Migration

After migrating the server node for CC-managed boxes, the status of the affected box will display the incorrect status **No** in the column **Has Service Container** in **CC > CONFIGURATION**:



Box	Cluster	Range	Box IP	Type	Relea...	Has Service Container
Brussels () [VF1000]	Belgi...	2	192.1[redacted]	VF1000	8.0	No
Espoo (RMT-MGMT) [VF100]	Finla...	4	192.1[redacted]	VF100	8.0	No
Helsinki (RMT-MGMT) [VF100]	Finla...	4	192.1[redacted]	VF100	8.0	No
Innsbruck () [VF1000]	Austria	1	192.1[redacted]	VF1000	8.0	No
Nicosia () [VF500]	Cyprus	3	192.1[redacted]	VF500	8.0	No
Tallinn () [VF1000]	Estonia	4	192.1[redacted]	VF1000	8.0	No
Vienna () [VF1000]	Austria	1	192.1[redacted]	VF1000	8.0	No

In addition, an incorrect status of the box is displayed in **CC > CONTROL**:



Name	Description	Acc...	Version	Country	Appliance	Serial	Server	S...	N...	Li...	A...	R...	V...	C...
2	Western Europe													
2/Belgium			8.0											
Brussels		192.1...	8.0.2-0119		VF1000	904646	Brussels							
3	Southeastern Europe													
3/Bulgaria														

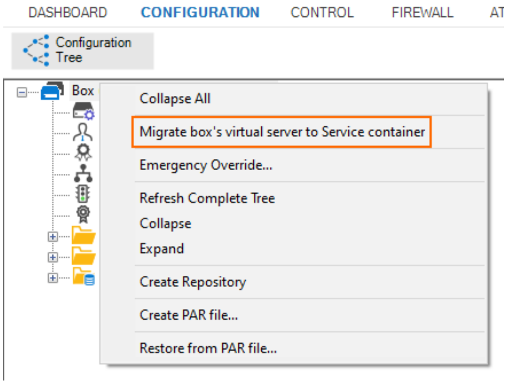
As a workaround, you can execute the command-line tool `conftool r - rebuild_db` which will update the database. As a result, the status of the migrated box will be displayed correctly.

Before You Begin

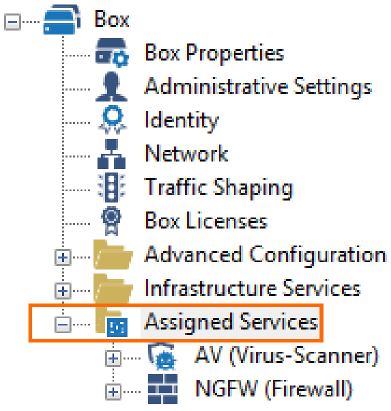
- Make sure you are familiar with the difference between the old 3-layer and the new 2-layer structure. For more information, see Understanding Assigned Services.
- The firewall/CC must have been upgraded from firmware version 7.x to 8.0.1 or 8.0.2, 8.0.3 or 8.0.4.
- On a Control Center, the feature level for clusters must set to 8.0.
- The configuration tree must display the old 3-layer structure with a virtual server node.

How to Migrate the Server Node to the Assigned Services Node for Stand-Alone Firewalls and Control Centers (Box-Level Only)

1. Log into the firewall or Control Center on box level.
2. Right-click **Box**.
3. The window with the menu is displayed.



4. In the list, click **Migrate box's virtual server to Service container**.
5. The old 3-layer server-service node with the name **Virtual Servers** will be transformed into the new 2-layer service node with the name **Assigned Services**.
6. When the conversion is completed, the configuration tree will contain the node **Assigned Services**.



How to Migrate the Server Node to the Assigned Services Node for CC-Managed

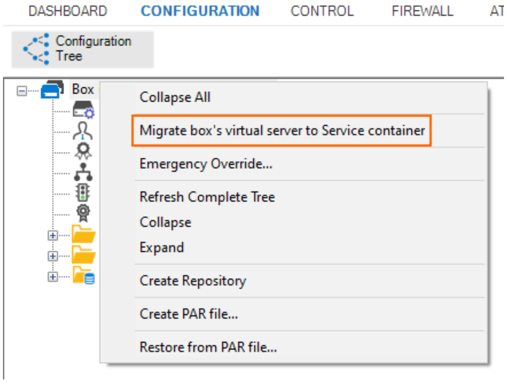
Firewalls

Before You Begin

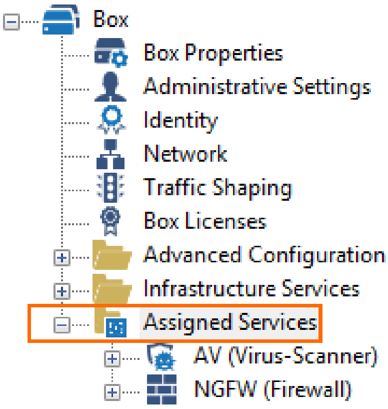
- On a Control Center, the feature level for the cluster the firewall lives in must be set to 8.0. For more information, see How to Manage Ranges and Clusters.
- If you are operating a GTI tunnel, you must lock the GTI Editor after the assigned-service migration to clean up the nonexisting VPN Services and VPN tunnels after the migration process!

Migrating the Server Node

1. Log into the Control Center that manages the target firewall.
2. Go to **CONFIGURATION** > **Configuration Tree** > **Multi Range** > ***your range*** > ***your cluster*** > **Boxes** > ***your box***.
3. Right-click **Box**.
4. The window with the menu is displayed.



5. In the list, click **Migrate box's virtual server to Service container**.
6. When the conversion is completed, the configuration tree will contain the node **Assigned Services**.



How to Migrate the Server Node to the Assigned Services Node for Stand-Alone HA Pairs

Before You Begin

- This example assumes that you have an unmanaged/stand-alone pair of HA firewalls running.

Migrating the Server Node

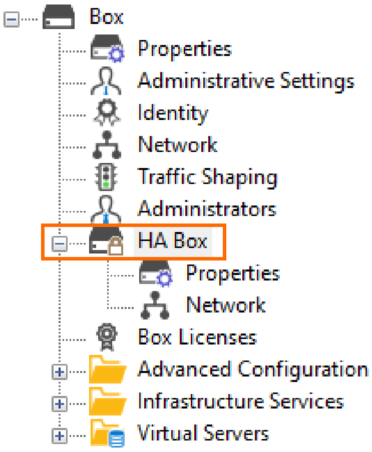
Step 1. Block the Server on the Secondary Firewall.

1. Log into the secondary firewall.
2. Go to **CONTROL**.
3. Click **Block server**.

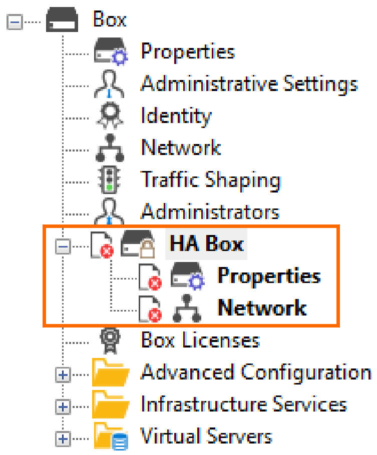
(optional) Step 2. Remove the HA Box Node for the Secondary on the Primary Firewall.

Perform the following steps only in case you experience issues during the migration.

1. Log into the primary firewall.
2. Go to **CONFIGURATION > Box > HA Box**.
3. Right-click **HA Box**.
4. In the list, click **Lock**.



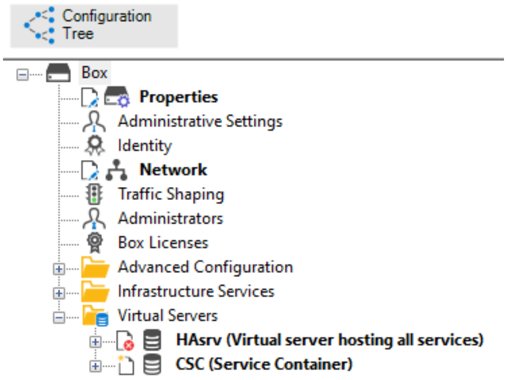
5. Right-click **HA Box**.
6. In the list, click **Remove**.
7. The node for HA box will be marked for deletion.



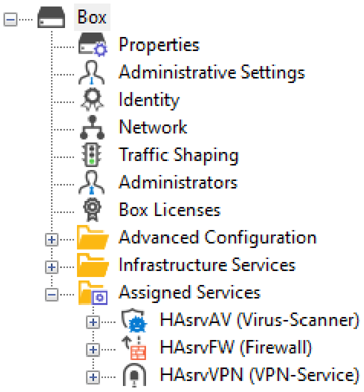
8. Click **Send Changes**.
9. Click **Activate**.

Step 3. Migrate the Virtual Server on the Primary Box.

1. Right-click **Box**.
2. In the list, click **Migrate box's virtual server to Service container**.
3. The window for **Migrating Box's Server to Container Server** is displayed.
4. Click **OK**.
5. The configuration tree will display the following:
    1. A new **Network** node.
    2. A new container for the services **CSC(Service Container)**.
    3. A red deletion symbol on the old server node.



6. Click **Activate**.
7. After the server node has been migrated, the configuration tree will display the new **Assigned Services** node.

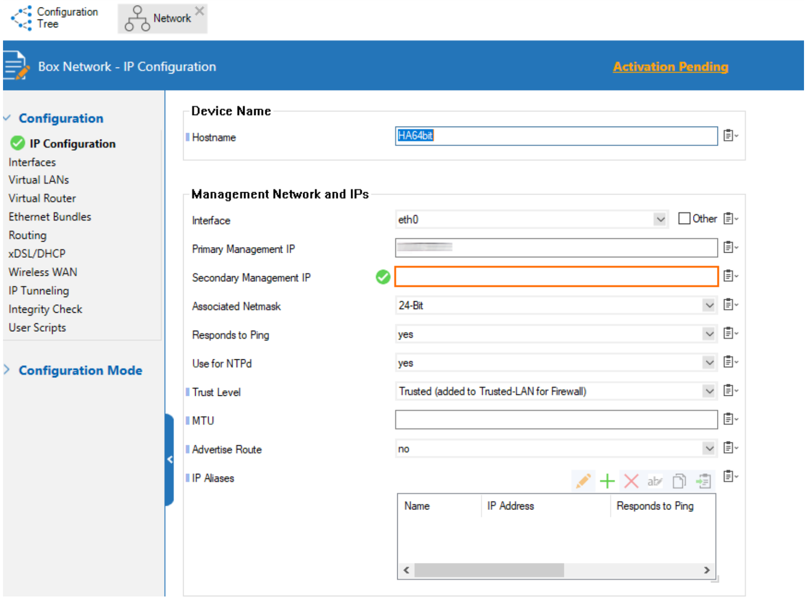


- Box
  - Properties
  - Administrative Settings
  - Identity
  - Network
  - Traffic Shaping
  - Administrators
  - Box Licenses
  - Advanced Configuration
  - Infrastructure Services
  - Assigned Services
    - HAsrvAV (Virus-Scanner)
    - HAsrvFW (Firewall)
    - HAsrvVPN (VPN-Service)

8. The names of the services will now consist of 'HAsrv' appended with the name of the service, e.g., HAsrvAV, HAsrvFW, HAsrvVPN.

Step 4. Create the Secondary Box on the Primary Firewall.

1. Right-click **Box**.
2. In the list, click **Create Secondary Box**.
3. The **Network** window for entering the MIP for the secondary firewall is displayed.



Device Name

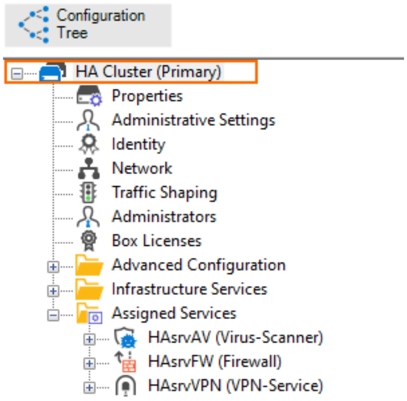
Hostname	HA64bit

Management Network and IPs

Interface	eth0 □ Other
Primary Management IP	[redacted]
Secondary Management IP	
Associated Netmask	24-Bit
Responds to Ping	yes
Use for NTPd	yes
Trust Level	Trusted (added to Trusted-LAN for Firewall)
MTU	
Advertise Route	no
IP Aliases	

Name	IP Address	Responds to Ping

4. For **Secondary Management IP**, enter the IP address.
5. Click **Send Changes**.
6. Click **Activate**.
7. After the creation of the secondary box, the configuration tree on the primary firewall will display the name **HA Cluster (Primary)**.



Step 5. Reactivate the Network Configuration

1. Go to **CONTROL > Box**.
2. In the left navigation bar, click **Network**.
3. In the left navigation bar, click **Activate new network configuration**.

Step 6. Create the PAR File for the Secondary Firewall

The new configuration must be propagated to the primary firewall.

1. Go to **CONFIGURATION > Configuration > Box**.
2. Right-click **Box** and select **Create PAR file for secondary box...**
3. Save the PAR file for the secondary firewall.
4. Reconnect to the primary firewall to see the new **CONTROL** window.

Step 7. Import the PAR file into the Secondary Firewall

1. Log into the secondary firewall.
2. Go to **CONFIGURATION > Configuration Tree > Box**.
3. Right-click **Box** and select **Emergency Override**.
4. Right-click **Box** and select **Restore from PAR file**.
5. Click **OK**.
6. Click **Activate**.

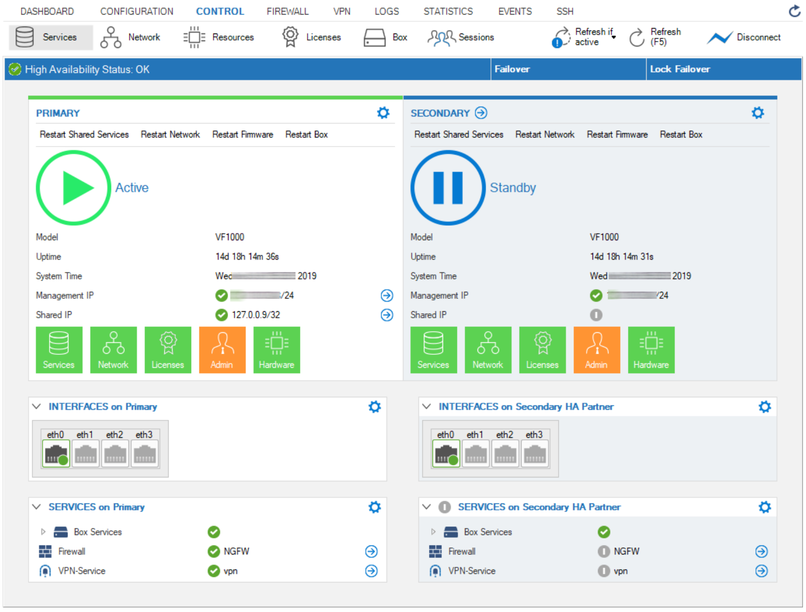
Step 8. Reactivate the Network Configuration

1. Go to **CONTROL > Box**.
2. In the left navigation bar, click **Network**.
3. In the left navigation bar, click **Activate new network configuration**.

Step 9. Reconnect to Both Firewalls to See the New CONTROL Window

Do the following steps on both the primary and secondary firewall:

1. Go to **CONFIGURATION**.
2. Click **Disconnect** on the right side of the ribbon bar.
3. The session to the firewall will be terminated.
4. Click **Connect** on the right side of the ribbon bar to reconnect to the firewall.
5. Go to **CONFIGURATION > CONTROL**.
6. The window now displays the new controls.



High Availability Status: OK

	PRIMARY	SECONDARY
	Active	Standby
Model	VF1000	VF1000
Uptime	14d 18h 14m 36s	14d 18h 14m 31s
System Time	Wed [redacted] 2019	Wed [redacted] 2019
Management IP	✓ [redacted]/24	✓ [redacted]/24
Shared IP	✓ 127.0.0.9/32	

SERVICES on Primary		SERVICES on Secondary HA Partner	
Box Services	✓	Box Services	✓
Firewall	✓ NGFW	Firewall	NGFW
VPN-Service	✓ vpn	VPN-Service	vpn

How to Migrate the Server Node to the Assigned Services Node for CC-Managed HA Pairs

Before You Begin

- All repository links that refer to the Network node must be unlinked.

Step 1. Migrate the Primary Firewall

1. Right-click **Box**.
2. In the list, click **Migrate box's virtual server to Service container**.
3. A window is displayed that asks you if you want to keep the server or remove it.
4. Confirm which option is more important to you. In case you keep the server, it will stay in the configuration tree but will no longer have any function.
5. The window for **Migrating Box's Server to Container Server** is displayed.
6. Click **OK**.

Step 2. Delete the Secondary Firewall

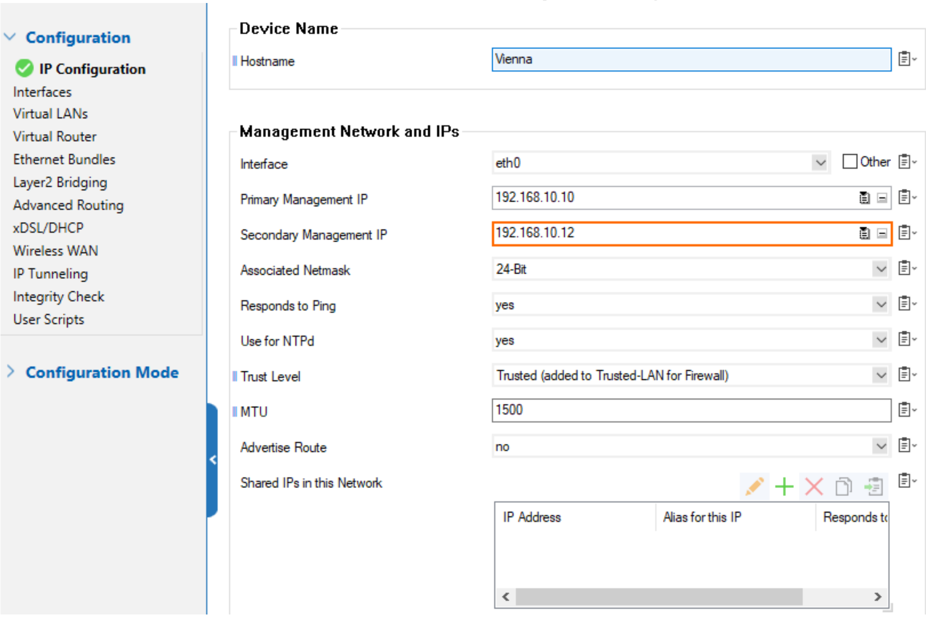
The secondary firewall must be deleted in the configuration tree because it will be managed via the primary firewall.

1. Right-click **Box** of your secondary firewall.
2. In the list, click **Lock**.
3. Right-click **Box** of your secondary firewall.
4. In the list, click **Remove**.
5. Click **Activate**.

Step 3. Create the PAR File for the Secondary Firewall

On the primary firewall, right-click **Box**.

1. In the list, select **Create Secondary box**.
2. In the file selection window, provide a file name for the PAR file.
3. Go to **Network**.
4. Provide the IP address for the **Secondary Management IP**.



Device Name

Hostname: Vienna

Management Network and IPs

Interface: eth0 □ Other

Primary Management IP: 192.168.10.10

Secondary Management IP: 192.168.10.12

Associated Netmask: 24-Bit

Responds to Ping: yes

Use for NTPd: yes

Trust Level: Trusted (added to Trusted-LAN for Firewall)

MTU: 1500

Advertise Route: no

Shared IPs in this Network

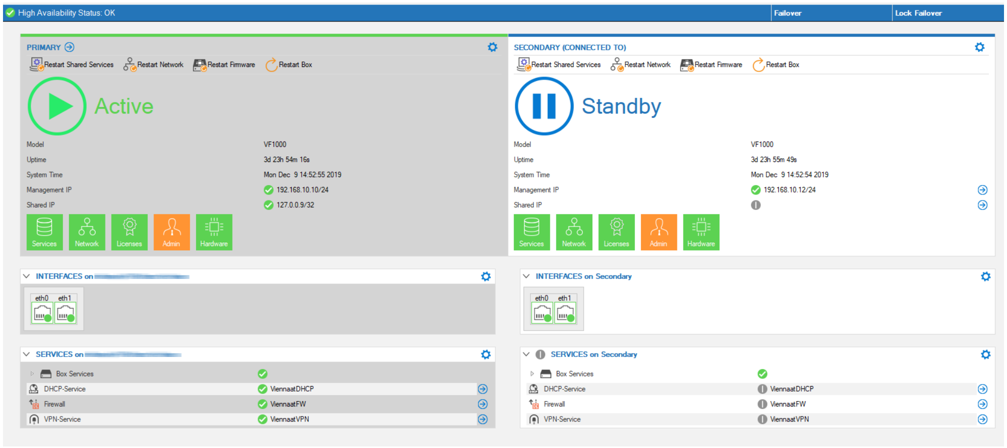
IP Address	Alias for this IP	Responds t

5. Click **Send Changes / Activate**.
6. The node for the secondary firewall will disappear from the configuration tree. From now on, the secondary firewall will be configured via the primary firewall. Therefore, only the node for the primary firewall will be visible in the configuration tree.
7. Right-click **Box** for the primary firewall.
8. In the list, click **Create PAR file for secondary**.

Step 4. Import the PAR File on the Secondary Firewall

1. In the CC, click **Status Map**.
2. Locate the secondary firewall in the list of managed firewalls. The name of the new secondary firewall will now have the name of the box trailed by the appendix "-HA", e.g., MyBox-HA.
3. In the **Status Map**, double-click the entry of the secondary firewall.

4. On the secondary firewall, go to **CONFIGURATION**.
5. Right-click **Box**.
6. Click **Emergency Override**.
7. Right-click **Box**.
8. Click **Restore from PAR File**.
9. In the file selection window, select the PAR file to restore.
10. Click **Activate**.
11. Go to **CONTROL > Box**.
12. In the left navigation bar, click **Network** to expand the list.
13. In the list, click **Activate new network configuration**.
14. In the ribbon bar, click **Disconnect** to close the session to the secondary firewall.
15. In the ribbon bar, click **Connect** to re-establish a new session to the secondary firewall.
16. Go to **CONTROL** to see the new window contents.



High Availability Status: OK

PRIMARY

Active

Model	VF1000
Uptime	3d 23h 54m 16s
System Time	Mon Dec 9 14:52:55 2019
Management IP	✓ 192.168.10.10/24
Shared IP	✓ 127.0.0.9/32

SECONDARY (CONNECTED TO)

Standby

Model	VF1000
Uptime	3d 23h 55m 49s
System Time	Mon Dec 9 14:52:54 2019
Management IP	✓ 192.168.10.12/24
Shared IP	

INTERFACES on [redacted]

INTERFACES on Secondary

SERVICES on [redacted]

Box Services	✓
DHCP-Service	✓ ViennaatDHCP
Firewall	✓ ViennaatFW
VPN-Service	✓ ViennaatVPN

SERVICES on Secondary

Box Services	✓
DHCP-Service	ViennaatDHCP
Firewall	ViennaatFW
VPN-Service	ViennaatVPN

Figures