

8.2.2 Migration Notes

<https://campus.barracuda.com/doc/96773479/>

Important Note for Users Operating Firmware 7.2.5 or 7.2.6

IMPORTANT NOTE

Ensure that the partition layout of your firewall/Control Center applies to the values in the table of paragraph **Disk Space Requirements** below.

1. If you operate a firewall that was shipped from the factory with firmware 7.2.6, or if you have already repartitioned the hard disk and performed a fresh install of firmware 7.2.6, then the hard disk already has a partition layout that is suitable for firmware 8.x. In this case, you can upgrade directly to firmware 8.x without repartitioning the hard disk.
2. If you operate a firewall with firmware version 7.2.5 or earlier, you must repartition the hard disk with the layout listed below and fresh install firmware 7.2.6. After that, you can update to 8.x without repartitioning.

Important Note for Users Wanting to Upgrade to Firmware Release 8.3.x at a Later Date

If your firewall is currently running firmware 8.2.1, and you plan to upgrade to release 8.3.x at a later date, you should consider switching to firmware 8.3.x now!

Because firmware 8.3.1 has been released after firmware 8.2.2, 8.3.1 does not include fixes contained in 8.2.2.

If you must switch to firmware 8.2.2, you can only upgrade to the upcoming releases 8.3.2 and 9.0.0 respectively.

Before You Begin

- The information contained in this article applies insofar as it was not already taken into account in the previous migration note 8.2.1.
- The following instructions apply both to firewalls and Control Centers.

Barracuda Firewall Admin

After updating a system, you must also download Firewall Admin with the same version. Firewall Admin is backward-compatible. That means you can manage 7.x and 8.x F-Series Firewalls and Control Centers with Firewall Admin 8.x.

Always use the latest version of Barracuda Firewall Admin.

Important Note Before Migrating

With firmware release 8.0.2, Barracuda introduced a new 2-layer service architecture that makes the former server node in the configuration tree obsolete. As already announced in previous migration notes, converting the former 3-layer server-service architecture to the new 2-layer service architecture was optional within the period of firmware version 8.0.2 to 8.0.4

If you have not yet done so, you must now transform the former 3-layer architecture to the new 2-layer service architecture on the box level before upgrading to firmware version 8.2.2.

This applies both to firewalls and Control Centers.

Supported Models for Firmware Version 8.2.2

The following models are capable of running firmware version 8.2.2:

| Barracuda CloudGen F-Series and Control Center Models | |
|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hardware Systems | F12 Rev A, F18 Rev A/B, F80 Rev A/B, F82 Rev A, F93 Rev A, F180 Rev A/B, F183 Rev A, F183R Rev A, F193 Rev A, F280 Rev B/C, F380 Rev A/B, F400 Rev B/C (8/12 ports), F600 Rev C/D, F800 Rev B/C, F900 Rev A (only fresh install), F900 Rev B, F1000 Rev A, F1000 Rev B |
| Virtual Systems | VF10, VF25, VF50, VF100, VF250, VF500, VF1000, VF2000, VF4000, VF8000, VC400, VC610, VC820, Proxmox running with KVM images |
| Public Cloud | AWS, Azure, Google Cloud |
| Standard Hardware Systems | |
| Standard Hardware | A standard hardware system is a Barracuda CloudGen Firewall F-Series running on 3rd-party server hardware using an SF license. Consult the Barracuda Networks Technical Support to find out if your specific standard hardware is supported. |

Disk Space Requirements

Upgrading to version 8.2.2 requires your disk partitions to have enough free disk space. Firmware 8.2.2 requires the following partition spaces:

Disk Space Requirements **FIREWALL**:

| Hard Drive Partition | Disk Space Required |
|----------------------|---------------------|
| Swap | 2 GB |
| Boot | 1 GB |
| / | 8 GB |
| /phion0 | 4 GB |
| /art | 3 GB |

Disk Space Requirements **CONTROL CENTER**:

| Hard Drive Partition | Disk Space Required |
|----------------------|---------------------|
| Swap | 2 GB |
| Boot | 1 GB |
| / | 10 GB |
| /phion0 | 4 GB |
| /art | 10 GB |

Migration Path

If you have already performed the 3-layer to 2-layer architecture transformation, you can skip Steps 1-3 and continue with "Migration Instructions for 8.2.2".

All users who have not yet performed the 3-layer to 2-layer architecture transformation must do the following:

- First, upgrade to firmware 8.0.6.
- Perform the 3-layer to 2-layer architecture transformation (also for clusters!).
- Then install firmware release 8.2.2 on top of 8.0.6.

Depending on the firmware release your firewall is currently operating, this migration requires 3 steps:

Step 1. Upgrade Your Firewall to Firmware Release 8.0.6

| Current Version | Via | Follow Migration Instructions |
|-----------------------------------------------------------------------------------------------------------------------------------------|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none">• 7.0.0 - 7.0.4• 7.1.0 EA - 7.1.5• 7.2.0 - 7.2.6 | 8.0.6 | For more information on how to migrate from your current version 7.0.0 - 7.2.6 to 8.0.5, see Migration from 7.x - 8.0.0 to 8.0.6 . |
| <ul style="list-style-type: none">• 8.0.1 - 8.0.5 | 8.0.6 | For more information on how to migrate from your current version 8.0.1 - 8.0.3 to 8.0.5, see Migration from 8.0.1/8.0.2/8.0.3/8.0.4/8.0.5 to 8.0.6 . |

Step 2. Transform the Former 3-Layer Server-Service Architecture to the New 2-Layer Assigned-Services Architecture

If you have not already done so in previous firmware upgrades, follow the steps in the article [Server Node to Assigned Services Node Migration](#).

Your firewall is now prepared to upgrade to firmware version 8.2.2.

Migration Instructions for 8.2.2

Before upgrading to firmware version 8.2.2, you may first need to complete a few additional steps. Check the following topic(s) and, if applicable, complete the migration steps listed below:

1. Upgrade of Virtual Machines for Forward Error Correction (FEC)

As of firmware version 8.2.1, release 8.2.2 also contains the new VPN feature Forward Error Correction (FEC). In order for this feature to work as expected on virtual deployments, the virtual hardware must be upgraded to the newest version to work on the ESXi hypervisor directly after the deployment of the virtual machine. For using FEC, the supported version of your hypervisor must be greater than or equal to version 6.5.

For more information, see Step 2 in [How to Deploy a CloudGen Firewall Vx OVA on VMware Hypervisors](#).

2. VPN, Usage of VPN Next Hop IPs

The following instructions apply only if you just have transformed your firewall from the former 3-layer server-service architecture to the new 2-layer assigned services architecture.

Before firmware version 8.2.1, certain VPN scenarios required you to configure next-hop interface IP addresses for the shared networks. Due to the new 2-layer service architecture, which is represented

through the **Assigned Services** node in the configuration tree, it is no longer necessary to explicitly configure these IP addresses.

However, in this special case, it is necessary to apply some additions to the host firewall ruleset.

If you have made changes/additions manually to your host firewall ruleset, you must back up these host firewall rules to restore them later.

For updating the host firewall ruleset, you have two options:

1. Add the missing rules manually
2. Update the host firewall ruleset with Copy from Default.

How to Update the Host Firewall Ruleset




Step 1. (optional) In case you have made additions/changes to the host firewall ruleset manually:

Create a copy of all these firewall rules.

Option 2.1 (recommended): Add the missing rules to the host firewall ruleset manually.

For more information on how to create a pass rule, see [How to Create a Pass Access Rule](#).

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Service > Host Firewall Rules**.
2. Ensure that **Inbound** is selected in the top-left corner of the rule list display area.
3. Click **Lock**.
4. Add each of the rules in the list to the **Inbound Host Firewall Ruleset**.

| Action | Name | Features | Service | Source | Destination |
|------------------------------------------|-------------|-------------------------------------------------------------------------------------|----------------------------------|------------------|---------------------------------------------------------------------------------|
| → Pass Original Source IP (same port) | OP-SRV-OSPF |  | OSPF OSPFv2 | Any 0.0.0.0/0 | Ref: OSPF-Nets , Ref: ServerIPs , Ref: VPN Next Hop IPs 224.0.0.5, 224.0.0.6 |
| → Pass Original Source IP (same port) | OP-SRV-RIP |  | RIP UDP 520 | Any 0.0.0.0/0 | Ref: ServerIPs , 224.0.0.9 , Ref: VPN Next Hop IPs 224.0.0.9 |
| → Pass Original Source IP (same port) | OP-SRV-BGP | | BGP TCP 179 | Any 0.0.0.0/0 | Ref: ServerIPs , Ref: VPN Next Hop IPs |
| → Pass Original Source IP (same port) | OP-SRV-BFD | | BFD UDP 3784, UDP 3785, UD... | Any 0.0.0.0/0 | Ref: ServerIPs , Ref: VPN Next Hop IPs |
| → Pass Original Source IP (same port) | OP-SRV-ICMP |  | ICMP ECHO | Any 0.0.0.0/0 | Ref: ServerIPs , Ref: VPN Next Hop IPs |

5. Click **Outbound** in the top-left corner of the rule list display area.
6. Add each of the rules in the list to the **Outbound Host Firewall Ruleset**.

| Action | Name | Features | Service | Source | Destination |
|------------------------------------------|-------------|----------|----------------------------------|-------------------------------------------|------------------|
| → Pass Original Source IP (same port) | OP-SRV-OSPF | | OSPF OSPFv2 | Ref: ServerIPs , Ref: VPN Next Hop IPs | Any 0.0.0.0/0 |
| → Pass Original Source IP (same port) | OP-SRV-RIP | | RIP UDP 520 | Ref: ServerIPs , Ref: VPN Next Hop IPs | Any 0.0.0.0/0 |
| → Pass Original Source IP (same port) | OP-SRV-BGP | | BGP TCP 179 | Ref: ServerIPs , Ref: VPN Next Hop IPs | Any 0.0.0.0/0 |
| → Pass Original Source IP (same port) | OP-SRV-BFD | | BFD UDP 3784, UDP 3785, UD... | Ref: ServerIPs , Ref: VPN Next Hop IPs | Any 0.0.0.0/0 |

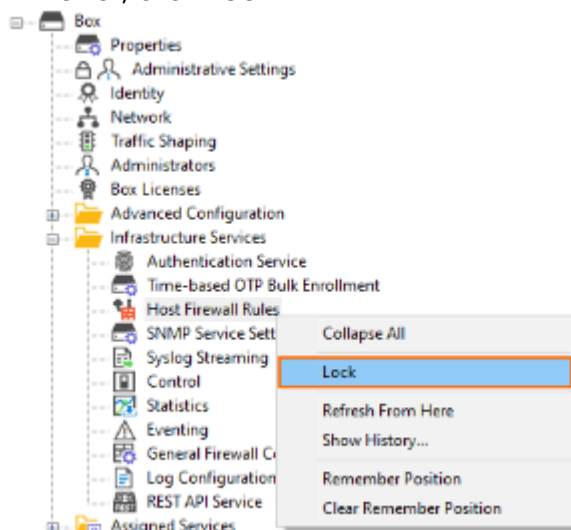
7. Click **Send Changes**.

Option 2.2: (Only if you did not complete Option 2.1) Update the host firewall ruleset with Copy from Default.

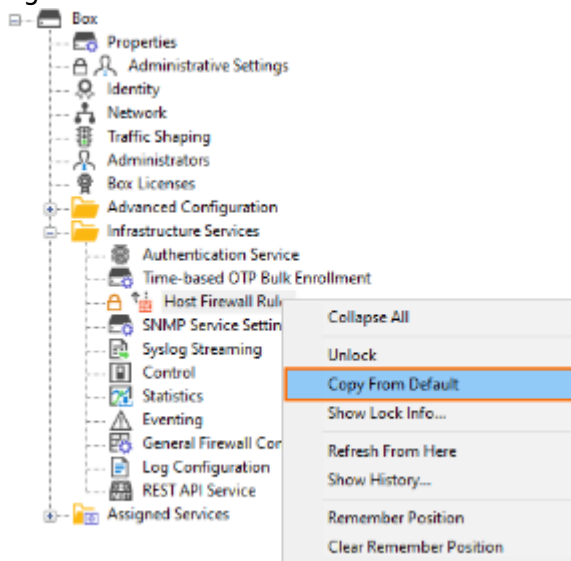
After the transformation to the new 2-layer service architecture, the host firewall ruleset can be rebuilt by copying it from the default.

Copy from Default will overwrite your existing host firewall ruleset. Any previously added custom rules will be lost!

1. Log into the firewall.
2. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services**.
3. Right-click **Host Firewall Rules**.
4. In the list, click **Lock**.



5. Right-click **Host Firewall Rules**.



6. In the list, click **Copy from Default**.
7. Click **Activate** in the top-right corner of the window.

Step 3. (optional) In case you have made a copy of individual firewall rules, you must restore them now.

Add your individual firewall rules that you copied before to the host firewall ruleset.

How to Migrate to Version 8.2.2

Download the appropriate download file.

To migrate to version 8.2.2

If You Migrate from Version 8.2.0 to 8.2.2

1. Go to the download portal
<https://dlportal.barracudanetworks.com/#/packages/5508/patch.GWAY-8.2.2-0225.tgz>.
2. Download the **patch** package.

If You Migrate from Versions 8.0.0 - 8.2.0 to 8.2.2

1. Go to the download portal
<https://dlportal.barracudanetworks.com/#/packages/5507/update.GWAY-8.2.2-0225.tgz>.
2. Download the **update** package.

Start the Update

You can now update the CloudGen Firewall or Control Center.

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

Figures

1. vpn_routed_hfw_inbound_rules_to_add.png
2. vpn_routed_hfw_outbound_rules_to_add.png
3. lock_host_firewall_rules.png
4. host_firewall_ruleset_copy_from_default.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.