

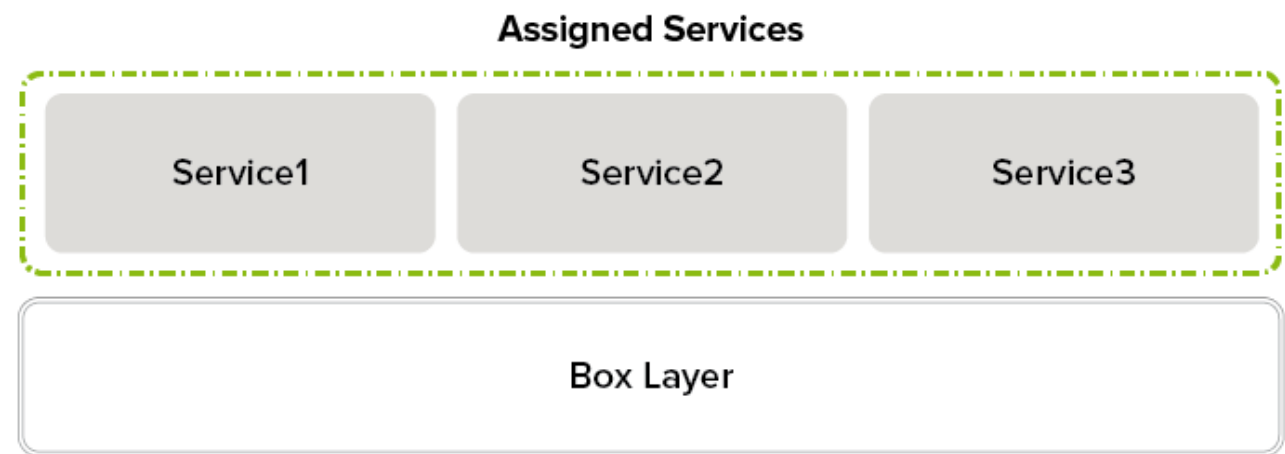
Understanding Assigned Services

<https://campus.barracuda.com/doc/96026736/>

Starting with firmware release 8.0.1, the concept of virtual servers and services has been replaced by a new 2-layer architecture.

The two layers are comprised of the following:

- **Box Layer** – The box layer runs infrastructure services, and is responsible for logging, event, configuration, and control. The network subsystem is also part of the box layer, which creates some peculiarities with network configuration. Only the management IP address and additional static box layer IP addresses of the CloudGen Firewall are allocated in the box layer. The box layer is always active.
- **Assigned Service** – Selected services can be activated by the user if required. After configuring these services, they run on top of the box layer in the service layer and are bound to the firewall they were created on.

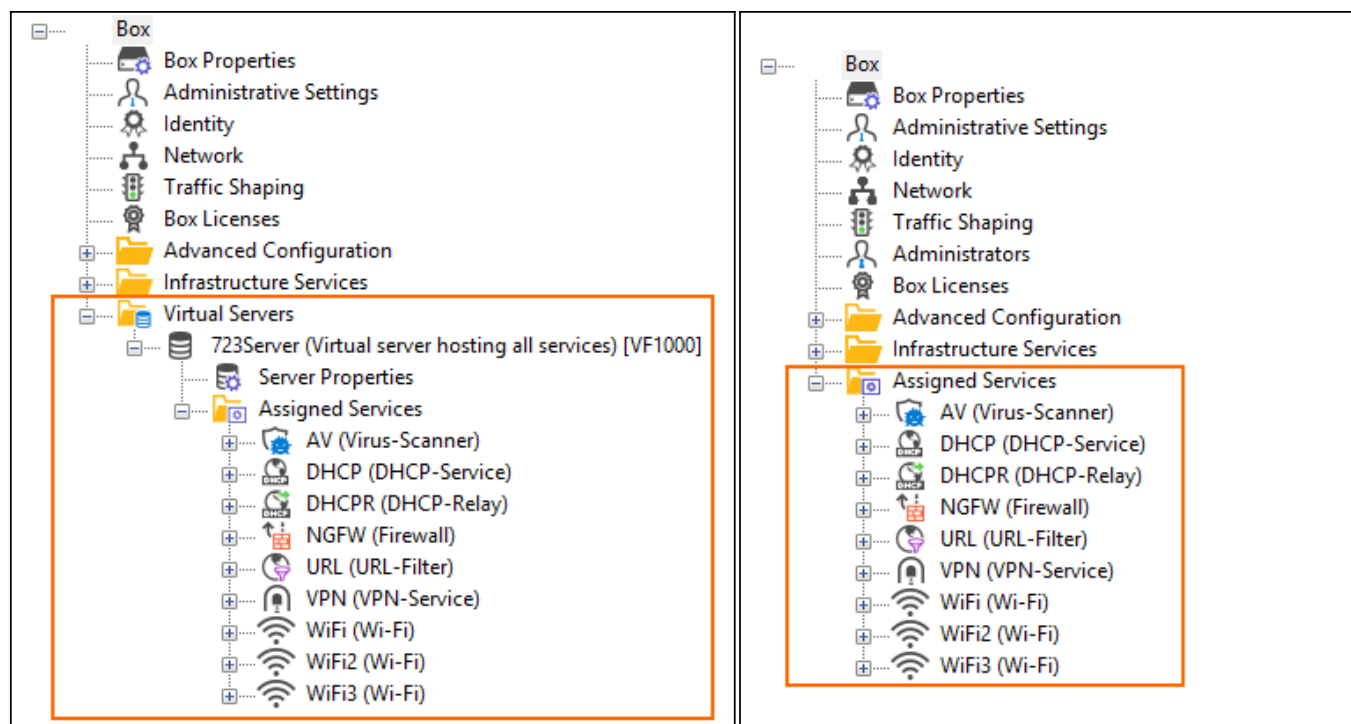


Visual Representation of New 2-Layer Architecture

To get the configuration tree displayed correctly, you must use the newest release of Firewall Admin that is released with firmware 8.0.1.

The newest Firewall Admin version that is released with firmware version 8.0.1 can display both the former 3-layer and the new 2-layer architecture.

3-Layer Architecture	2-Layer Architecture
----------------------	----------------------



Which architecture is effectively displayed depends on the following preconditions:

- The new 2-layer architecture applies to all firewalls that are delivered with firmware 8.0.1 or to firewalls that receive a completely fresh install of firmware 8.0.1.
- Firewalls that are being upgraded to firmware 8.0.1 from any lower release will continue to show the older server/service structure in the configuration tree.
- Firewalls running with firmware 8.0.1 and a restored PAR file from a firmware release < 8.0.1 will also show the older Virtual Servers/Service structure in the configuration tree. This also applies for CC-managed boxes with a firmware < 8.0.1 and the Control Center running with firmware 8.0.1.
- If a cluster with a version 7.x is migrated to version 8.x, the config tree will display the older Virtual Servers/Services structure. If a new firewall is created within that migrated cluster, the new 2-layer architecture will be applied.

When using the most recent version released with firmware 8.0.1, Firewall Admin will display server and service nodes according to the following table.

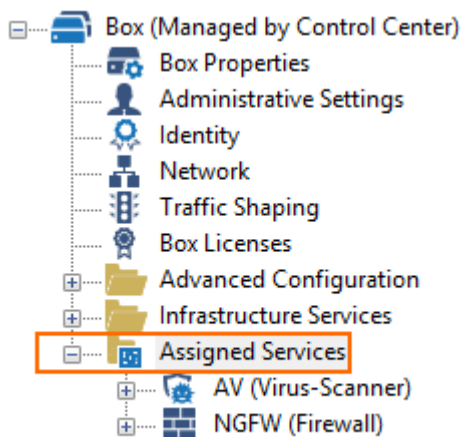
Box Type	Migrated from < 8.0.1 to 8.0.1	Fresh Install 8.0.1
Stand-alone Box	Virtual Server + services	Assigned services
HA Box Pair	Virtual Server + services	Assigned services
	Standard HA config (see below)	New HA structure (see below)
CC Mgd. Box	Virtual Server + services	Assigned services
CC Mgd. HA Box Pair	Virtual Server + services	Assigned services
	Standard HA config (see below)	New HA structure (see below)

CC Box Level	Virtual Server + services	Assigned services
CC CC Level	Virtual Server + services	Assigned services

Services, Service IP Addresses, and Service Names

In case you are operating multiple firewalls, it is strongly recommended that you configure unique names for all services. This is important especially before turning a stand-alone firewall into a managed one because in a cluster all service names must be unique. Otherwise, the import of a PAR file from a stand-alone box into the Control Center will fail.

The **Assigned Services** node in the configuration tree groups multiple services into one clear folder icon and contains all configured services, e.g., Firewall, VPN, DHCP, HTTP Proxy and many more.



For a service to handle incoming traffic on a respective interface, a network address must first be assigned to the interface (attached network), e.g., 10.0.10.0/24. Next, all required IP addresses within this network must be configured in order that they can be later used by a dedicated service, e.g., 10.0.10.1. A new virtual IP address is automatically tagged with the label 'None' but can also be tagged with the the label 'First' or 'Second' by the user.

For more information, see [Network](#).

Later, after a service is created, one or multiple service addresses can be selected from the pool of already configured IP addresses. Selecting the label 'First', 'Second' or 'First+Second' picks the related IP address(es). Alternatively, the label 'Explicit' allows you to select any IP address from the pool.

For more information, see [How to Assign Services](#).

Creation of New Services

- On firewalls upgraded to firmware 8.0.1, new services can be created only inside of a server node.
- On firewalls with a fresh install of 8.0.1, services will be created inside of the service container.

Moving Servers and Services of Boxes in a CC

- On firewalls upgraded to firmware 8.0.1, moving server nodes is not possible.
- moving services between server nodes is possible.
- On firewalls with a fresh install of 8.0.1, moving service containers is not possible.
- On firewalls with a fresh install of 8.0.1, services are directly bound to the Assigned Services container.

Cloning Boxes in a CC Using the Clone and Create Box Wizard

- On firewalls upgraded to firmware 8.0.1, cloning an existing box in a Control Center creates the new Assigned Services container structure for the new box.
- On firewalls upgraded to firmware 8.0.1, creating an new box in a Control Center creates the new Assigned Services container structure.

High Availability and Virtual IP Addresses

In an optional High Availability setup, two firewalls can be configured to run in parallel. With the exception of the Management-IP, all configured service IP addresses are mirrored to the secondary firewall that runs as a backup. In case the primary firewall goes down, the secondary unit immediately takes over and activates all services with the same service IP addresses as configured on the primary firewall. Service IP addresses are also called **Shared IP Addresses** to indicate that they will be shared between the primary and the secondary firewall for fallback purposes.

The configuration tree displays a different HA pair depending on what firmware version the firewall runs:

Migrated from < 8.0.1 to 8.0.1		Fresh Install 8.0.1	
Stand-alone Primary	Stand-alone Secondary	Stand-alone Primary	Stand-alone Secondary
<ul style="list-style-type: none"> Box <ul style="list-style-type: none"> Box Properties Administrative Settings Identity Network Traffic Shaping Administrators HA Box Box Licenses Advanced Configuration Infrastructure Services Virtual Servers 	<ul style="list-style-type: none"> HA Cluster (Secondary) <ul style="list-style-type: none"> HA Box Properties Administrative Settings Identity HA Network Traffic Shaping Administrators HA Box Box Licenses Advanced Configuration Infrastructure Services Virtual Servers 	<ul style="list-style-type: none"> HA Cluster (Primary) <ul style="list-style-type: none"> Box Properties Administrative Settings Identity Network Traffic Shaping Administrators Box Licenses Advanced Configuration Infrastructure Services Assigned Services 	<ul style="list-style-type: none"> HA Cluster (Secondary) <ul style="list-style-type: none"> Secondary Properties Administrative Settings Identity Secondary Network Traffic Shaping Administrators Box Licenses Advanced Configuration Infrastructure Services Assigned Services

All options for an HA pair can be configured in windows that are displayed in Firewall Admin when the

respective node is double-clicked.

HA Monitoring and Transparent Failover

In case of an HA configuration, services are initiated on both boxes. While the primary box activates the services, the secondary box keeps the services deactivated until a failover is initiated. In case of a failover, all services on the secondary box are immediately activated.

For HA failover, the management IP address and the first service IP address are monitored by default. To configure transparent monitoring for HA clusters, create monitoring policies for interfaces and IP addresses. The services stay up as long as these health check targets are reachable.

For more information, see [HA-Monitoring](#) and [High Availability](#).

Service Limitations

Some services can be introduced only once on a CloudGen Firewall:

- **Forwarding Firewall** – Because the Firewall module is based on the kernel, you can only have one firewall service per firewall.
- **VPN** – Because the VPN service is based on the kernel, it can be introduced only once on a firewall. The Forwarding Firewall and the VPN service must be in the same virtual server.
- **Access Control** – These services provide a user interface that is always bound to the first-introduced service of their type.
- **HTTP Proxy** – The HTTP Proxy service can be introduced multiple times, but the HTTP Proxy fail cache interface can be used by only one service.
- **HTTP Proxy** and **Web Filter** – You must also configure the HTTP Proxy service and the Web Filter service on the same system.

For more information, see [Services](#), [Shared Services](#) and [How to Assign Services](#).

Figures

1. 2_layer_service_container.png
2. 3_layer_arch.png
3. 2_layer_arch.png
4. assigned_services.png
5. HA_config_tree_primary_standalone_old.png
6. HA_config_tree_secondary_standalone_old.png
7. HA_config_tree_primary.png
8. HA_config_tree_secondary.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.