

How to Assign Services

<https://campus.barracuda.com/doc/98210747/>

The Barracuda CloudGen Firewall has two types of services. Box services provide functionality required to run the Barracuda CloudGen Firewall system. They are factory defined and cannot be created or removed by the user. User-related services can be created and are assigned to the configuration node Assigned Services.

Barracuda CloudGen Firewall Services

Depending on your model, some services may not be available. Consult the datasheet for your appliance for more information on which services are available for your model.

The following services are available for individual configuration on the Barracuda CloudGen Firewall:

- Access Control Service
- DHCP Service
- DHCP Relay
- DNS
- Firewall
- HTTP Proxy
- OSPF/RIP/BGP Service
- SNMP Service
- URL Filter
- VPN Service
- Virus Scanner
- CloudGen Access Proxy

Barracuda Firewall Control Center Service

The following services are available on a Barracuda Firewall Control Center:

- CC DNS
- CC Firewall
- CC Configuration Service
- CC Event Service
- CC Syslog Service
- CC FW Audit Log Service
- CC Reporter
- CC Statistics Collector
- CC VPN Service
- CC Access Control Service

Create a Service

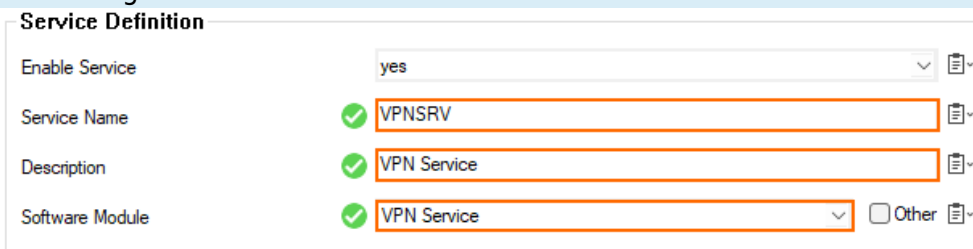
When creating a service is completed, the service will be subordinated to the Assigned Services node and bound to the firewall.

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.

Step 1. Add a Service

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services**.
2. Right-click **Assigned Services** and select **Create Service**.
3. Enter a **Service Name**. The name must be unique and no longer than 30 characters. The service name cannot be changed later.
4. In the **Software Module** field, select the type of service that you are creating, e.g., VPN service. You cannot change the service type after the service is created.

The types of services that you can create are dependent on your license and system model. Verify the product type and appliance model in the **Box Properties** if services are missing.

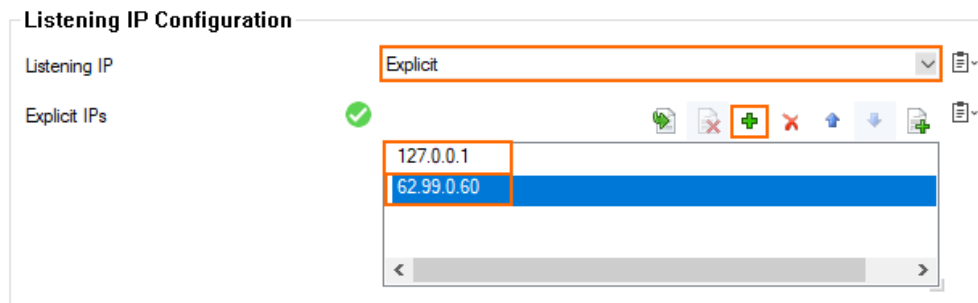


Service Definition	
Enable Service	yes
Service Name	VPNSRV
Description	VPN Service
Software Module	VPN Service

Step 2. Service IPs and Type of Service

Assign the IP addresses the service listens on.

1. In the **Listening IP Configuration** section, enter the IP addresses for the service.
2. Select the IP addresses the service listens on from the **Listening IP** list.
 - **All IPs** - Some services (e.g., Firewall) will automatically listen on all available shared IP addresses.
 - **First + Second-IP** - Listen on the first and second shared IP address.
 - **First-IP** - Listen on the first service IP address.
 - **Second-IP** - Listen on the second shared IP address.
 - **Explicit** - Add the IP addresses you want to use to the **Explicit Service IPs** table.



3. Click **Next**.

Step 3. Statistics (optional)

Enable statistics settings for the service. By default, all settings are enabled for the service:

1. In the **Statistics Settings** section, set **Generate Statistics** to **yes**.
2. Edit the following settings according to your requirements:
 - **Src Statistics** – Generates IP source-based statistical data for the service. Only the number of connections from IP addresses is recorded. The times at which the connections were made are not recorded.
 - **Src Time-Statistics** – Generates IP source-based statistical data for the service. Both the number of connections made from IP addresses and the times at which the connections were made are recorded.
 - **Dst Statistics** – Generates IP destination-based statistical data for the service. Only the number of connections to IP addresses is recorded. The times at which the connections were made are not recorded.
 - **Dst Time-Statistics** – Generates IP destination-based statistical data for the service. Both the number of connections made to IP addresses and the times at which the connections were made are recorded.
 - **Src-Dst Statistics** – Generates IP source/destination pair-based statistical data for the service. Only the number of connections to and from IP addresses is recorded. The times at which the connections were made are not recorded.
3. Click **Next**.

Step 4. Access Notification (optional)

Configure which events are created for successful and unsuccessful logins. On stand-alone firewalls and on the box level of the Control Center, this setting can be configured only for all administrators. On the Control Center, each type of administrator (**Multi-Range > Global Settings > CC Access Notification**) can be handled separately. Access notifications are available only for the DHCP Server, Firewall, VPN, and the Mail Gateway service.

The following events are used for login attempts:

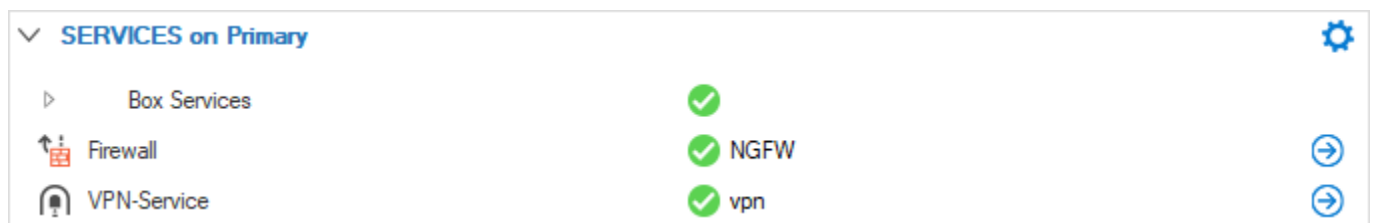
- The **User Unknown** event is generated when the admin ID is unknown to the underlying Barracuda Networks authentication module.

- The **Authentication Failure** event is used when the password or key does not match or when the admin is not authorized to access the service (multi-admin environment, only in conjunction with a Barracuda Firewall Control Center).

To configure which events are created, complete the following steps:

1. In the **Notification** section, edit the following settings according to your requirements:
 1. **Success** – Select the notification level for a successful login:
 - **Silent** – No event.
 - **Notice** – CGF Subsystem Login Notice [2420].
 - **Warning** – CGF Subsystem Login Warning [2421].
 - **Alert** – CGF Subsystem Login Alert [2422].
 2. **Failure** – Select the notification level for an unsuccessful login:
 - **Silent** – No event.
 - **Notice** – Authentication Notice [4110] or [4100].
 - **Warning** – Authentication Warning [4111] or [4100].
 - **Alert** – Authentication Failure [4111] or [4100].
2. Click **Finish**.
3. Click **Activate** to create the service.

The service is now displayed as active on the **CONTROL > Service** page.



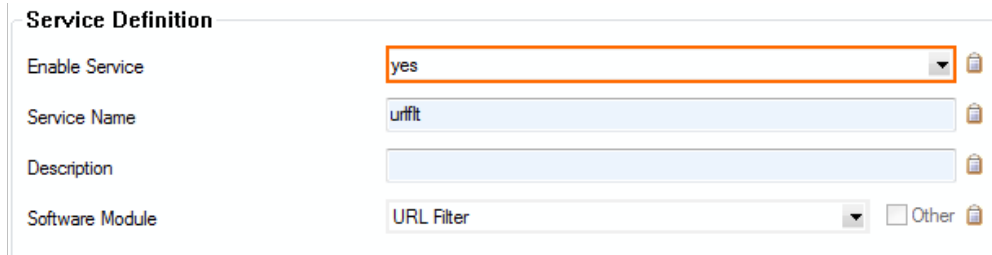
Remove a Service

Removing a service is permanent and cannot be undone.

1. Expand the **Assigned Services** node (**Configuration > Configuration Tree > Box**).
2. Right-click **the service you want to delete** and click **Lock**.
3. Right-click **the service you want to delete** and click **Remove Service**. A verification popup opens.
4. Click **Yes**.
5. Click **Activate**.

Enable or Disable a Service

1. Go to the **Service Properties** node (**CONFIGURATION > Configuration Tree > Box > Assigned Services > your service**).
2. Click **Lock**.
3. To disable the service set **Enable Service** to **No**.



4. To enable the service set **Enable Service** to **Yes**.
5. Click **Send Changes** and **Activate**.

After assigning a service, you can now configure its specific properties. For more information, see [Services](#).

Figures

1. create_service_01.png
2. create service_02.png
3. create service_99.png
4. create service_03.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.