

How to Configure Services

<https://campus.barracuda.com/doc/46208997/>

The Barracuda NextGen Firewall F-Series has two types of services. Box services provide functionality required to run the Barracuda NextGen Firewall F-Series system. They are factory-defined and cannot be created or removed by the user. Server services are created and run in a virtual server. Services relying on other services for certain functionality (i.e., firewall and virus scanner service) must be created on the same virtual server. Although possible, it is recommended to only create one service type per virtual server. You can create the following services:

Barracuda NextGen Firewall F-Series 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.

- DHCP Service
- DHCP Relay
- DNS
- Firewall
- FTP Gateway
- HTTP Proxy
- URL Filter
- Mail Gateway
- OSPF/RIP/BGP Service
- SNMP Service (Server Layer)
- SPAM Filter
- SSH Proxy
- Virus Scanner
- VPN Service
- Access Control Service

Barracuda NextGen Control Center Services

- 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
- CC PKI Service

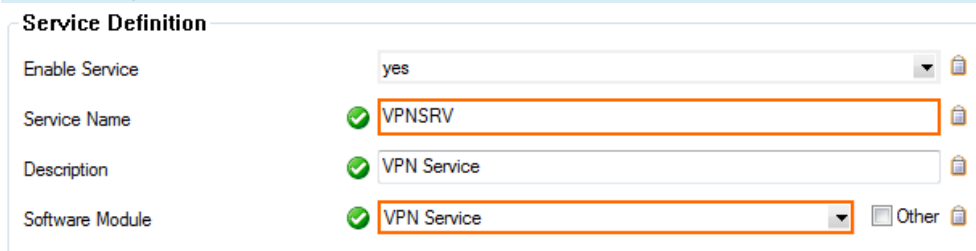
In this article:

Create a Service

Step 1. Add a Service to a Virtual Server

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > 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 six characters. The service name cannot be changed later.
4. In the **Software Module** field, select the type of service that you are creating. 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.



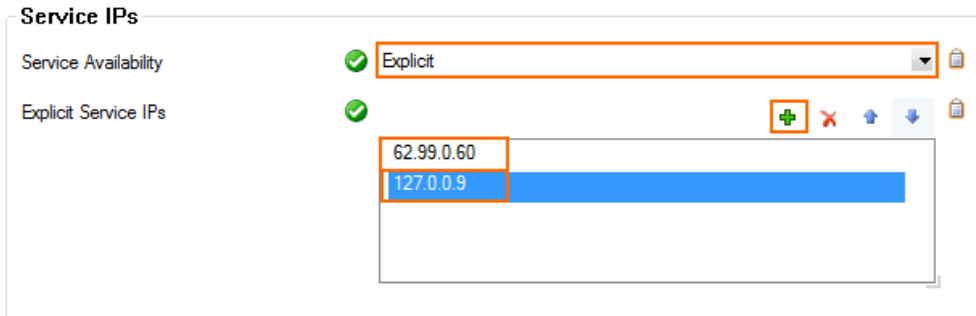
| Service Definition | |
|--------------------|-------------|
| Enable Service | yes |
| Service Name | VPNSRV |
| Description | VPN Service |
| Software Module | VPN Service |

Step 2. Service IPs and Type of Service

Assign the IP addresses the service listens on.






1. In the **Service IPs** section, enter the IP addresses for the service.
2. Select the IP addresses the service listens on from the **Service Availability** list.
 - **All IPs** – Some services (i.e., firewall) will automatically listen on all available Server IP addresses.
 - **First + Second-IP** – Listen on the first and second virtual server IP address.
 - **First-IP** – Listen on the first virtual server IP address.
 - **Second-IP** – Listen on the second virtual server IP address.
 - **Explicit** – Add the IP addresses you want to use to the **Explicit Service IPs** table. Explicit IP addresses must also be added to the **Additional IP** table in the **Server Properties** of the virtual server. For more information, see [How to Configure Virtual](#)

[Servers.](#)



Service IPs

Service Availability Explicit

Explicit Service IPs     

| |
|------------|
| 62.99.0.60 |
| 127.0.0.9 |

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 only be configured 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 only available for DHCP Server, Firewall, VPN Service 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 type is used when the password or key do not match or the admin is not authorized to access the service (multi-admin environment, only in conjunction with a Barracuda NextGen 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** - NGFW Subsystem Login Notice [2420].
 - **Warning** - NGFW Subsystem Login Warning [2421].
 - **Alert** - NGFW Subsystem Login Alert [2422].
 2. **Failure** - Select the notification level for an unsuccessful login:
 - **Silent** - No event.
 - **Notice** - NGFW Subsystem Login Notice [2420].
 - **Warning** - NGFW Subsystem Login Warning [2421].
 - **Alert** - NGFW Subsystem Login Alert [2422].
2. Click **Finish**.
3. Click **Activate** to create the service.

The service is now displayed as active (■) on the [Server Page](#).

| Server Status | | | | |
|---|---------|-------------------|--------------|--|
| Server | Status | Status HA Partner | IP Addresses | |
| [-] ■ AzureVS1 | primary | standby | 127.0.0.9 | |
| [-] ■ Status | primary | | | |
| [-] ■ HA | standby | | | |
| [-] ■ IP | | | | |
| [-] ■ 1 | | | 127.0.0.9 | |

Block Server Start Server Stop Server Restart Server

| Service Status | | | | | | |
|---|----------|--------|---------|---|-------------|------|
| Server / Service | Num Proc | Num FD | Mem KB | Module | | Info |
| [+] ■ box | | | | | | |
| [-] ■ AzureVS1 | | | | | | |
| [-] ■ AZFW1 | 1 | 3 | 7380 |  | Firewall | |
| [-] ■ AZVPN1 | 8 | 81 | 1801732 |  | VPN-Service | |

Block Service Start Service Stop Service Restart Service

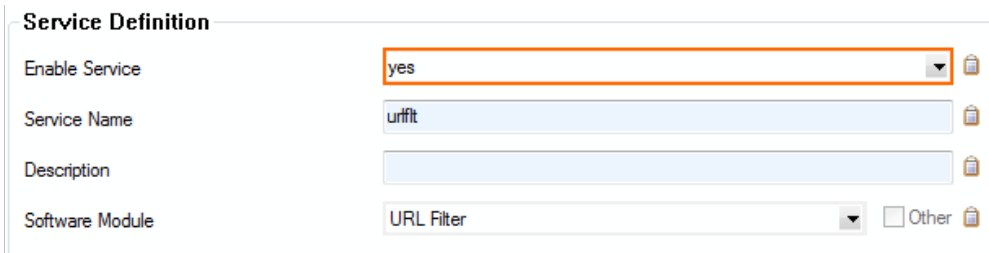
Remove a Service

Removing a service is permanent and cannot be undone.

1. Expand the **Assigned Services** node (**Configuration > Configuration Tree > Box > Virtual Servers > your virtual server**).
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 > Virtual Servers > your virtual server > Assigned Services > your service**).
2. Click **Lock**.
3. To disable the service set **Enable Service** to **No**.



| Service Definition | |
|--------------------|------------|
| Enable Service | yes |
| Service Name | urlfit |
| Description | |
| Software Module | URL Filter |

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

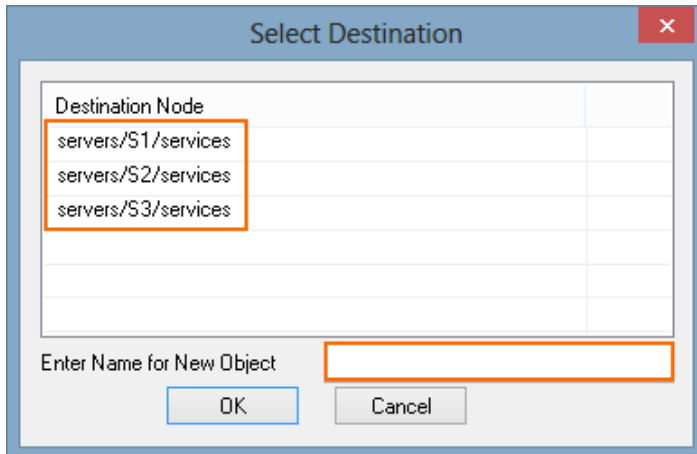
Move a Service

You can move services between virtual servers. If you are moving a service on a Barracuda NextGen Control Center, verify that the name of the service is unique in the cluster.

1. Expand the **Assigned Services** node (**CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server**).
2. Right-click **the service you want to move** and click **Lock**.
3. Right-click **the service you want to move** and click **Move Service**. The **Select Destination** window opens.
4. Select the destination virtual server.

5. Enter the **Name for the New Object**.

6. Click **OK**



7. Click **Activate**.

Figures

1. create_service_01.png
2. create_service_02.png
3. route_active.png
4. create_service_99.png
5. create_service_03.png
6. move_service_01.png

© Barracuda Networks Inc., 2019 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.