

How to Create Port Forwarding Rules

<https://campus.barracuda.com/doc/39818582/>

Port forwarding rules are executed only if the Barracuda Link Balancer firewall is enabled or if a WAN link has **Port Forwarding** enabled (see: [When the Firewall is Disabled](#)).

Create port forwarding rules to direct traffic on an external port to a port on a private IP address. The return path is handled automatically. The listen IP address on a specific WAN interface could be either the WAN IP address or one of the **Additional IP Addresses** on the same WAN interface. If an internal server needs to receive traffic from more than one WAN link, create a 1:1 NAT or port forwarding rule for each WAN link. If you then create a DNS domain, the Barracuda Link Balancer will automatically generate A records based on the Port Forwarding and 1:1 NAT rules.

Before you Begin:

The WAN IP address is the IP address used for general purpose NAT. If necessary, add the publicly accessible IP addresses to the configuration.

1. Log into the Barracuda Link Balancer web interface.
2. Go to the **Basic > Links** page.
3. Click the + sign to expand and edit the WAN link.
4. Add **Additional IP Addresses**, the external IP addresses that are eligible to be used.

An **Additional IP Address** used for port forwarding rules can NOT be used for 1:1 NAT rules.

5. Click **Save Changes**.

Create an Inbound Port Forwarding Rule

1. Log into the Barracuda Link Balancer web interface.
2. Go to the **FIREWALL > NAT** page.
3. In the **Port Forwarding Rules** table, enter a descriptive name in the **Rule Name** field.
4. From the **Listen Link** field, select the WAN link to use to listen for incoming packets on the port.
5. If desired, enter the hostname or the fully qualified domain name associated with the IP addresses in the **Hostname** field.

If you create a domain on the **Services > Authoritative DNS** page the Barracuda Link Balancer searches for matching domain names in the Port Forwarding and 1:1 NAT rules. For every match, a DNS A record is created linking this hostname to its external and internal IP addresses. You can enter a fully qualified domain name

(e.g. *www.example.com*. with or without the ending dot) or a hostname (e.g. *www*). If a hostname is entered, it is considered to be part of the default domain specified on the **Basic > IP Configuration** page.

6. In the **Listen IP** field, type the WAN IP address of this link and all of the Additional IP Addresses on the same WAN interface from the **Basic > Links** page. Select the address to use.
7. Select either an application or a port for the rule:
 1. When choosing the application option, select whether this rule should apply to any (*) application or only one from the **Application** list,

Applications let you define rules that apply to more than one port. You can define an application using the **Policy > Applications** page (see [How to Create Custom Applications](#)).
 2. When choosing the port option, enter one port, a list of comma-separated ports, or a hyphenated range in the **Port** field.

If multiple ports are being forwarded, then each port listed in the Listen IP Ports corresponds one-to-one with the entries in the Forward IP Ports list. If there are no Forward IP Ports, traffic is forwarded to the same port from which it was received.
8. Specify one or any protocol from the **Protocol** list.
9. In the **Forward IP** field, enter the private static IP address of the server which must be reachable from the LAN of the Barracuda Link Balancer. Or, if creating a DNAT rule for a link, type a static IP address reachable through a WAN link (usually, the firewall IP address reachable through WAN1).
10. In the **Ports** field, enter one port, a list of comma-separated ports, or a hyphenated range. If multiple ports are being forwarded, then each port in the **Listen IP Ports** list corresponds one-to-one with the the **Forward IP Ports** list. If there are no Forward IP Ports, traffic is forwarded to the same port from which it was received.
11. Make sure that you deselect **Disable** to enable the rule.
12. Select **Log** to write an entry in the Firewall Log whenever this rule is executed.
13. Select **Auto-create firewall rule** to enable auto-creating an accompanying inbound Access Firewall Rule to accept traffic on the listen link and port for the private IP address of the server.
14. Click **Add**.

When the Firewall is Disabled

If the Barracuda Link Balancer firewall is disabled, you can create a NAT rule to map the destination IP address of the inbound traffic on one WAN link to an IP address on another WAN link.

This option is also known as WAN IP impersonation. It is not available for WAN1.

The **NAT/Port Forwarding** feature allows you to add a new link without requiring an update to rules on your network firewall.

1. Go to the **Basic > Links** page.
2. Click the WAN link to open the configuration.
3. Select Yes to enable the **NAT/Port Forwarding** setting.
4. Click **Save Changes**.

After saving your changes here, create a Port Forwarding rule using the **Firewall > NAT** page.

© Barracuda Networks Inc., 2021 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.