
Step 2: Configure Networking Settings

<https://campus.barracuda.com/doc/5799947/>

This article describes the main networking settings that you can configure using the Barracuda Link Balancer web interface.

Viewing and Updating the WAN Link Configuration

Every WAN link that connects to the Barracuda Link Balancer must be manually identified. The information is provided by your internet service provider.

1. Log into the Barracuda Link Balancer Web Interface.
2. Go to the **BASIC > Links** page.
3. To identify links, move the mouse over the corresponding WAN port displayed in the upper section of the page. To change or add configuration information, click on the port or expand the link in the **Configure** column under the **Links Configuration** section.

Adding a New WAN Link

Remember, if you are adding one or more new WAN links to an already configured Barracuda Link Balancer, all links must be configured on the **BASIC > Links** page. Correctly configured WAN links are automatically used for outbound link balancing. For inbound traffic, if the Barracuda Link Balancer firewall is enabled, you can add a NAT rule on the **FIREWALL > NAT** page to map the destination IP address of traffic on the new link to an internal service.

WAN IP Impersonation

If the Barracuda Link Balancer firewall is disabled, you can avoid the need to update rules on your network firewall with the new WAN link by mapping the destination IP address of traffic on the new link to an existing WAN IP address (usually, an address on WAN1). To do this:

1. Select the **NAT/Port Forwarding** option on the **BASIC > Links** page.
2. Click **Save Changes**. The Barracuda Link Balancer will automatically perform a system Reload.
3. After the reload is complete, log back into the Barracuda Link Balancer.
4. Make sure to enter all IP addresses you own under their respective WAN links in the **Additional IPs** section of the **BASIC > Links** page. These IP addresses will be used to create NAT or Port Forward rules for WAN IP impersonation.

5. Create a NAT or Port Forward rule on the **Firewall > NAT** page to map the destination IP address of traffic on the new link to an external IP address on an existing link.

Authoritative DNS

The Barracuda Link Balancer can act as an authoritative DNS server, returning definitive answers to DNS queries about domain names in its configuration. This allows you to define one or more domains that are accessible via more than one WAN link. When asked to resolve a host, the Barracuda Link Balancer will return an IP address of one of the available WAN links.

However, before your servers can be accessed from the Internet by name, you must:

- Register your domains with a domain name registrar. Without this, the domain names will fail to resolve when accessed from the Internet.
- Once your domains are registered, you can configure authoritative DNS on the **SERVICES > Authoritative DNS** page.

Also, see [If You Add a WAN Link After the Domains are Created](#) for more information.

Adding Static Routes

If a separate subnet needs to use the Internet links accessible only through the Barracuda Link Balancer, add a static route to specify a gateway for that subnet so that return traffic takes the correct path. If you have disabled the Barracuda Link Balancer firewall, then static routes can be added to your network firewall. Otherwise, follow these instructions to add static routes to the Barracuda Link Balancer:

1. On the Barracuda Link Balancer web interface, go to **ADVANCED > Advanced Networking**.
2. Add the static routes.
3. Test connectivity from each internal network by changing the gateway IP address of a computer on each subnet to the LAN IP address of the Barracuda Link Balancer. Verify you can access the internet from each subnet.
4. Once verified, update the configuration of the DHCP server for clients to be the LAN IP address of the Barracuda Link Balancer as the default gateway. As leases are renewed, each client will gain access to the new Internet links.
5. Change the default gateway of any client with configured static IP addresses to the LAN IP address of the Barracuda Link Balancer.

Configuring VLANs

The Barracuda Link Balancer supports the IEEE 802.1Q standard for explicitly tagging Ethernet frames with VLAN information. Do the following to configure VLANs:

1. On the **ADVANCED > Advanced Networking** page, identify your VLANs.
2. Create a virtual interface associating an IP address and netmask with each VLAN.

Traffic sent to a virtual interface associated with a VLAN will be tagged with the VLAN ID and delivered correctly. VLANs cannot be on the same subnet.

Starting from firmware version 2.5, you can configure VLAN ID tagging for each link on the **BASIC > Links** page.

Creating IP Aliases

You can create virtual interfaces or IP address aliases by associating an IP address or subnet with a WAN, LAN or VLAN. Each IP address and netmask associate with only one WAN, LAN or VLAN. Virtual interfaces are used:

- To associate an IP address range with a VLAN
- To associate an externally accessible IP address on a subnet with no WAN link with a WAN link.

Create IP aliases on the **ADVANCED > Advanced Networking** page.

Configuring DNS Servers

On the **BASIC > Links** page, set the primary and secondary DNS servers for each WAN link. Your ISP provides you with these settings.

Configuring Per Interface Health Checks

On the **BASIC > Links** page, configure health checks for each link. Multiple methods are supported. You can enter more than one test target (e.g. resolve the DNS domain names of multiple websites) to

be sure that the link is actually down. Link failure is shown on the **BASIC > Links** and on the **BASIC > Status** page. Also, if a link fails, an SNMP trap is generated, an email is sent, and an event is logged.

Configuring the DHCP Server

The Barracuda Link Balancer can act as a DHCP server. On the **SERVICES > DHCP Server** page, enable and configure the DHCP server.

© 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.