Routing Outbound Traffic

https://campus.barracuda.com/doc/5799961/

By default, all outgoing traffic is link balanced and NAT'd. Also, the source IP address of outgoing traffic is the WAN link used by the traffic. You can create outbound routing rules to modify these defaults.

Specifying the Link Used by Outgoing Traffic

To exempt outgoing traffic from link balancing and/or NAT'ing, create IP/application rules on the **Policy > Outbound Routing** page. IP/application routing rules are based on the source IP address, application, and/or destination IP address. The IP/application routing rules are executed before the link load balancing algorithm. Traffic that matches no rule is both link balanced and NAT'd. These rules are executed regardless of the firewall operating mode.

Examples where IP/application routing rules may be useful include:

- If you are an ISP with externally accessible IP addresses (ARIN networks) behind the Barracuda Link Balancer that are not on the same subnet as your WAN interfaces.
- If you have subnets that you want to exempt from link balancing.
- If you have systems such as mail servers or VPN endpoints that send traffic that must maintain the original source IP address.
- If you have applications that you want to exclude from outgoing link balancing and NAT'ing.

Ping Traffic

To direct ping (ICMP) traffic that originates from behind the Barracuda Link Balancer to use a specific WAN link:

- Create a ping application on the **POLICY > Applications** page (select ICMP as the protocol, no port range).
- Create one or more IP/application routing rules for the ping application.

For example, if WAN1 is a private link to an office and WAN2 is a primary link used for other Internet traffic, make two rules: one that directs ping traffic to the office to use WAN1 and one that allows all other ping traffic to use WAN2. (Remember that private links are only used if the link is explicitly referenced.)

VPN and Email Rules

During installation, sample disabled IP/application routing rules are automatically created for outgoing VPN and email traffic to prevent it from being link balanced or NAT'd. To enable those rules, select the WAN link to be used for that traffic. If you would like to link balance outgoing email or VPN traffic because that is acceptable to the receiver, you can leave the rules in their disabled state or delete them. (For example, you may have created multiple SPF or DNS records for the WAN IP addresses).

Externally Accessible IP Addresses

If you would like to direct traffic from externally accessible IP addresses behind the Barracuda Link Balancer to the WAN link on the same subnet, create one or more rules where those addresses are the source IP addresses, link balancing and NAT are turned off, and **Primary Link** is set to **Auto**.
If you have a network where the externally accessible IP addresses (ARIN networks that are not in any WAN subnets) can send traffic on any WAN link, you can create rules so that traffic originating from those addresses goes out without being NAT'ed. Depending on how the ISP routers are set up, traffic from these networks may be link balanced or may be bound to one WAN link. For the latter case, select specific primary and backup links.

Changing the Source IP Address of Outgoing Traffic

To set the source IP address of outgoing traffic to a masquerade IP address other than the IP address of the WAN link, create outbound source NAT rules on the **POLICY > Outbound Routing** page. Outbound source NAT rules consider source IP address (or range) and, optionally, application and WAN link. If a rule match occurs, the specified external IP address is used as the source IP address of the traffic. The outbound source NAT rules are executed after the WAN link has been determined by the link load balancing algorithm. They are executed regardless of the firewall operating mode. The rules are arranged in a table on the **POLICY > Outbound Routing** page in order of precedence from top to bottom. Only the first matching rule to the profile of the traffic is executed. If the traffic matches a 1:1 NAT rule, the outbound source NAT rules are ignored.