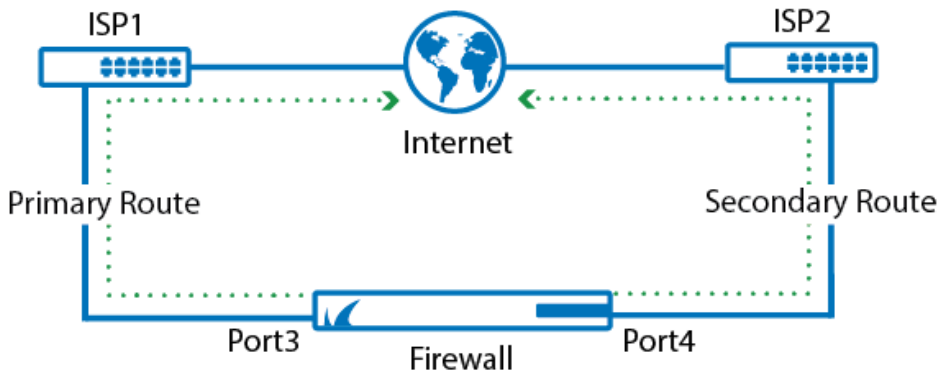
How to Configure Link Balancing and Failover for Multiple WAN Connections

https://campus.barracuda.com/doc/72516354/

If you are using two or more WAN connections, you can use outbound link balancing and load balancing to balance the traffic between the different Internet connections. If one link goes down, the traffic will be routed over the remaining connection. Basic link failover functionality can be achieved by using different route metrics. A better solution is to use custom connection objects to distribute the load and/or configure failover for different links. Using custom connection objects allows you to decide on link balancing on a per-access-rule basis.

To balance traffic among multiple links, create a firewall rule that uses a connection object that you configure. This connection object references all of the links and configures how to balance the traffic among them. You can also specify one link that is used for all the traffic matching the firewall rule, as long as it is available. If that link fails, the next link is used in its place.



Step 1. Failover - Dual Link Routing

In case one link connection fails, the firewall will automatically use the remaining Internet connection. Configure the routing metric for both connections:

1. Go to **NETWORK > IP Configuration**.
2. In the configurations for the primary and secondary interfaces, edit the **Metric** setting to specify the route priority. In a multi-provider configuration, the firewall selects the interface with the lowest metric value for outgoing traffic, assuming that it is available. Specify a higher metric value for the secondary or backup uplink. For example, use the following values for your primary and secondary interfaces:
   - **Primary Route Metric**: `100`
   - **Secondary Route Metric**: `200`

3. Click **Save** to save the new configuration.

Step 2. Link Balancing and Load Balacing

Create and use a custom connection object:

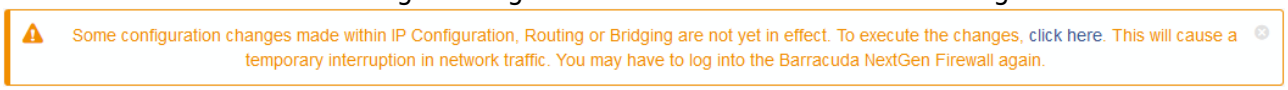
1. Go to **FIREWALL > Connection Objects**.
2. In the **Connection Objects** section, click **Add Connection Object**.
3. The **Add Connection Object** window opens.
4. From the **Translated Source IP** list, select either **Explicit** (to use the IP address that you specify) or **Network Interface** (to use the IP address of the link).
5. In the **Failover and Load Balancing** section, configure the following settings:
   - **Multilink Policy** – Defines what happens if multiple links are configured. Available policies are:
     - **None** – No fallback or source address cycling. This is not what you want for this object.
     - **Failover** – Falls back to the first alternate addresses and interface, called Alternate 1. If Alternate 1 fails, fail over to Alternate 2 and so on. When the original link (the one configured in the top section) becomes available, the firewall automatically resumes directing traffic to that interface.
     - **Weighted Round Robin** – Uses the IP addresses and interfaces configured as Alternate 1, 2, and 3, along with this interface, in weighted round robin fashion.
     - **Weighted Random** – Randomly uses one of the available IP addresses and interfaces specified in this object.
   - Specify the following for each of the alternate links:
     - **Translated Source IP** – Select one of these options:
       - **Network Interface** – Dynamic NAT using the first IP address on the interface selected from the **Interface** list.
       - **Explicit** – Uses the IP address in the **IP** address field.
     - **Weight** – Only used for the weighted round robin policy. The weight numbers represent the traffic balancing ratio of the available links. The higher the relative number, the more the link is used. For example, if four links are configured in this object, weight values of 6, 2, 1, and 1 mean that traffic is balanced over the configured interfaces in a ratio of 6:2:1:1. As a result, 60% percent of the traffic passes over Link #1, 20% of the traffic passes over Alternate 1, 10% of the traffic is directed to Alternate 2, and 10% to Alternate 3.
6. Click **Save** to save the new configuration or **Cancel** to discard it.

Step 3. Perform a Network Activation

After you create or change basic network configurations such as routing, you must activate your new

network configurations.

1. Scroll to the top of the page.
2. Click on the link in the warning message to activate the new network configuration.



After you have successfully created this connection object, you can go to **FIREWALL > Access Rules** and apply it to a rule that directs outgoing traffic.

Figures

1. lb_multiple_wan-01.png
2. network_activation_ip_configuration.png