How to Configure Failover and Load Balancing in Custom Connection Objects

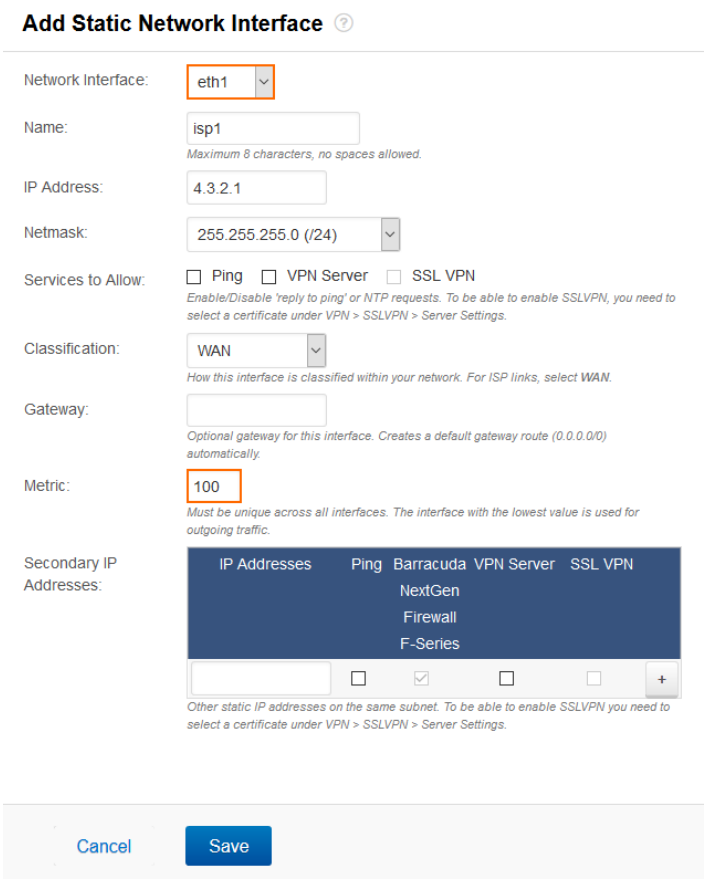
https://campus.barracuda.com/doc/72516036/

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, then the next link is used in its place.

Failover - Dual ISP Routing

In case one ISP 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 ISP uplink. For example, use the following values for your primary and secondary interfaces:
   - **Primary ISP Metric**: `100`
   - **Secondary ISP Metric** :`200`



3. Click **Save Changes**.
4. At the top of the page, click on the warning message to execute the new network configuration.

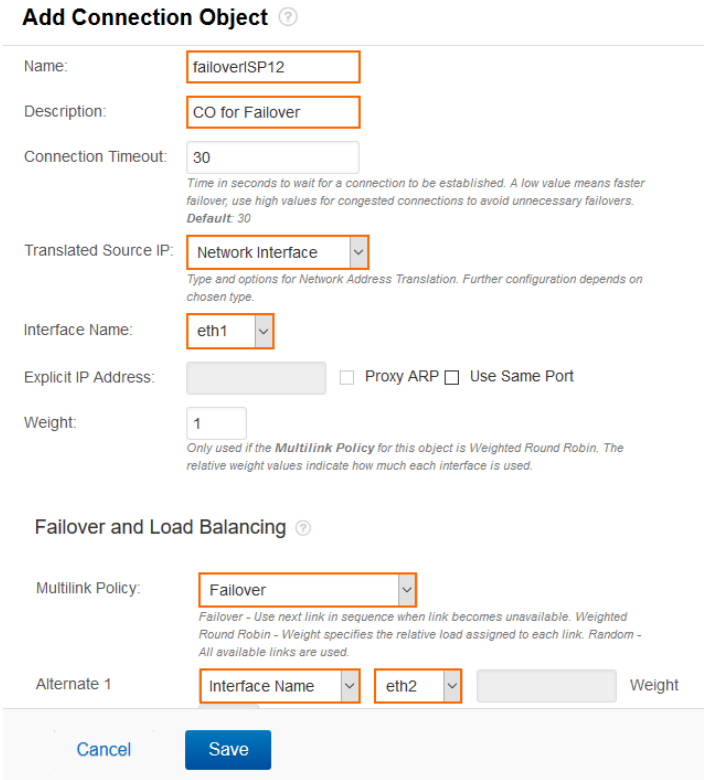
Link Balancing and Load Balancing

To use both your Internet connections to send outgoing traffic, create and use a custom connection object.

1. Go to **FIREWALL > Connection Objects**.
2. In the **Connection Object** section, click **Add Connection Object**.
3. From the **Translated Source IP** list in the **Add Connection Object** window, select either **Explicit IP** (to use the IP address that you specify) or **Network Interface** (to use the IP address of the link).
4. 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** – The firewall uses the IP addresses and interfaces configured as Alternate 1, 2, and 3, along with this interface, in weighted-round robin fashion.
- **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** – Source NAT using the first IP address on the interface selected from the **Interface** list.
    - **Explicit IP** – The firewall 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.



5. Click **Add**.

After creating this connection object, go to the **FIREWALL > Access Rules** page and apply it to a rule that directs outgoing traffic.

Figures

1. configure_metric_for_static_interface.png
2. configure_failover_interface.png