

How to Configure Automatic Failover Dynamic WAN Connections in Standby Mode

<https://campus.barracuda.com/doc/73719016/>

Only use this setup if you are using two WAN connections where the secondary connection is in Standby mode. For all other setups, see [How to Configure Link Balancing and Failover for Multiple WAN Connections](#) or [How to Configure Failover with Multiple xDSL or DHCP WAN Connections](#).

When using two Internet connections from the same ISP, both links cannot be active at the same time if they are connecting to the same remote network and using the same remote gateway IP address. Since it is not possible to have two default routes each using the same remote gateway, the backup uplink must be used in standby mode only and used if the primary connection goes down. A second virtual server is used to monitor the primary uplink. When the primary uplink becomes unavailable, a script is executed to activate the secondary uplink. Lowering the route metric of the secondary uplink ensures that the backup uplink is used. When the primary uplink becomes available again (probing is successful), a script will place the secondary uplink into standby again.

Step 1. Configure Two DHCP Connections

Configure two DHCP WAN connections. For more information, see [How to Configure an ISP with Dynamic IP Addresses \(DHCP\)](#).

For the primary and secondary DHCP uplink, use the following settings:

Setting	Primary DHCP Connection	Secondary DHCP Connection
Link Active	yes	yes
Standby Mode	no	yes
Route Metric	100	99

Step 2. Create an Additional Virtual Server

Create an additional virtual server and configure a monitoring policy of the virtual server to execute a custom script in case of failure / success.

1. Go to **CONFIGURATION > Configuration Tree > your box**.
2. Right-click **Virtual Servers** and select **Create Server**.

3. Enter a **Server Name**.
4. In the **First-IP [IP1]** field, enter 127.0.0.10
5. Click **Next**.
6. From the **IP Monitoring Policy** list, select **all-OR-all-present**.
7. In the **Monitored IPs I** table, add the IP address to be monitored. This is typically an IP address in the Internet or from your ISP that indicates that a connection to the Internet is available.
8. Click **Next**.
9. In the **Start Script** field, add the following script for the secondary DHCP uplink:
/epb/openxdhcp stop <secondary DHCP uplink name>
10. In the **Stop Script** field, add the following script for the secondary DHCP uplink:
/epb/openxdhcp start <secondary DHCP uplink name>
By default, DHCP02 is the name for the uplink. In the following scripts, replace <secondary DHCP uplink name> with the name that you specified for your secondary DHCP uplink.
11. Click **Finish**.

If the monitoring IP address is unreachable, the virtual server stops and enables the secondary DHCP uplink by executing the stop script. If the monitoring IP address is available again, the virtual server starts and disables the secondary DHCP uplink by executing the the start script.

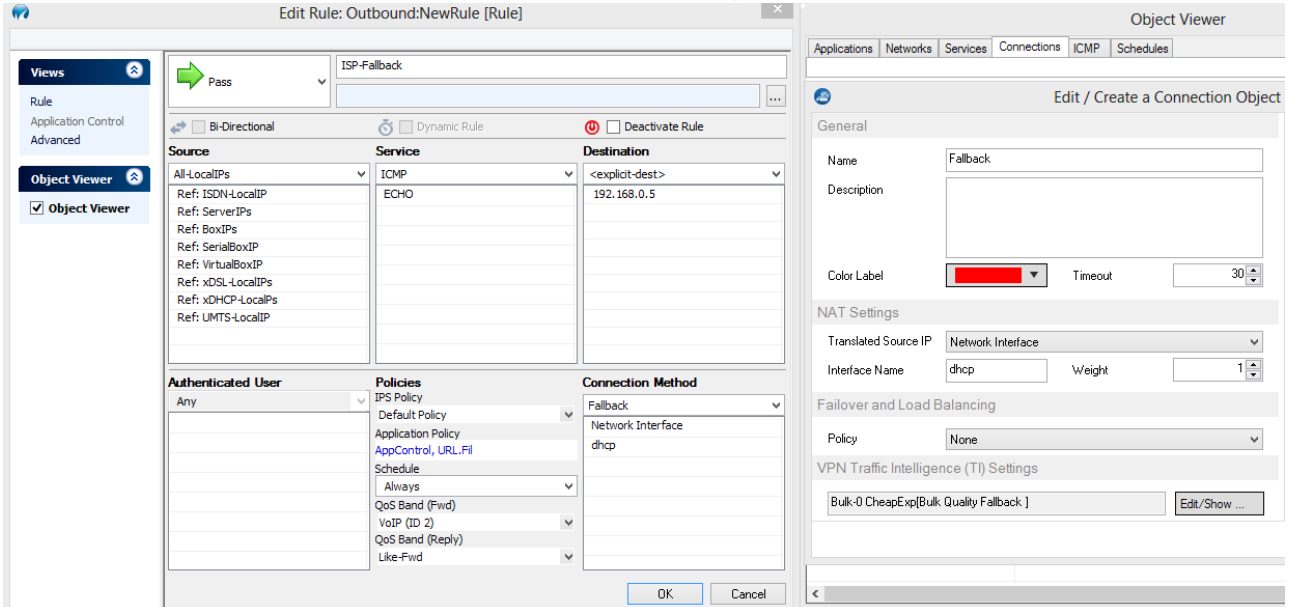
Step 3. Create a Host Firewall Rule

Create a Host Firewall rule to make sure that IP address probing is always done through the primary DHCP uplink (using the DHCP interface).

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Host Firewall Rules**.
2. Click **Lock**.
3. Select the **Outbound** rule set on top of the rule list.
4. Right-click in the rule list and select **New > Rule**.
5. Select **Pass** as the action.
6. Enter a name for the rule. For example, ISP-Fallback.
7. Specify the following settings that must be matched by the traffic handled by the access rule:
 - **Source** – Select **All-LocalIPs**
 - **Destination** – Enter the IP address to be monitored.
 - **Service** – Select **ICMP**
8. In the left pane, select the **Object Viewer** check box. The **Object Viewer** window opens.
9. Open the **Connections** tab and create the connection object:
 1. Right-click the table and select **New Connection**. The **Edit/Create a Connection Object** window opens.
 2. Enter a **Name** for the connection object. E.g., Fallback
 3. From the **NAT Address** list, select **Network Interface**.
 4. In the **Interface Name** field, enter dhcp

5. Click **OK**.

10. In the **Edit Rule** window, select the new connection object in the **Connection Method** section.



11. Click **OK**.

12. Drag and drop the new access rule in the rule set so no rule above it matches the traffic you want to forward.

13. Click **Send Changes** and **Activate**.

You can now see the active routes of the primary uplink and the pending route of the secondary uplink. If the primary uplink goes down, the virtual server is stopped and the stop script is executed - activating the secondary uplink. When the primary connection is available again, the virtual server executes the start script, which places the secondary link into standby mode again.

Figures

1. fb_rule_outbound.png

© Barracuda Networks Inc., 2020 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.