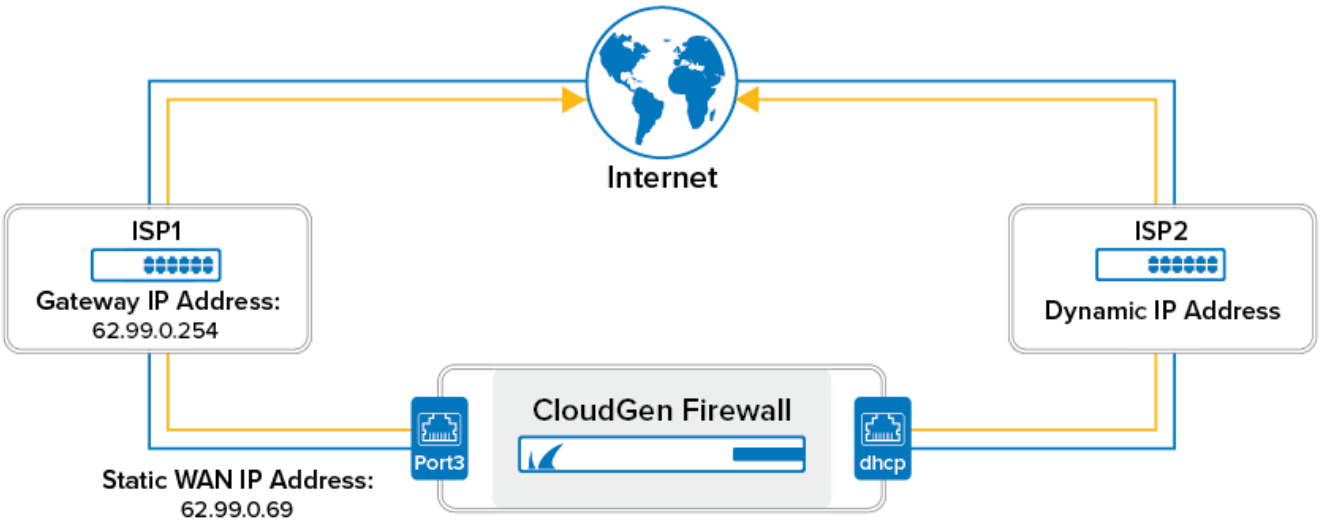
How to Configure Link Balancing and Failover for Multiple WAN Connections

https://campus.barracuda.com/doc/95258644/

If you are using multiple dynamic Internet connections (xDSL or DHCP), see How to Configure Failover with Multiple xDSL or DHCP WAN Connections.

If you are using two or more ISP connections, you can use outbound link and load balancing to balance the traffic between the different Internet connections. If one ISP 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. For this example we are using one static and one dynamic Internet connection.



Step 1. Configure the WAN Connections

Configure your WAN connections:

- For information on setting up an ISP with static IP address assignment, see How to Configure an ISP with Static IP Addresses.
- For information on setting up an ISP with dynamic DHCP IP address assignment, see How to Configure an ISP with Dynamic IP Addresses (DHCP).

This configuration uses the following example settings for both WAN connections:

ISP	IP Address	Gateway	Network Interface
ISP 1	62.99.0.69	62.99.0.254	port 3
ISP 2	dynamically assigned	dynamically assigned	dhcp

For WAN connections with dynamic address assignment (e.g. ,DHCP), verify that you enable the settings **Own Routing Table**, **Use Assigned IP**, and **Clone Routes** in the configuration. Disable **Create Default Route**.

Step 2. Add a Source Based Route

Configure the source routes for both connections to avoid IP packets from being sent via the wrong ISP line. For DHCP connections, the routes are already introduced automatically by the DHCP client. For ISP connections with static IP addresses, configure a source-based route.

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. In the left menu, select **Routing**.
3. Click **Lock**.
4. In the **Source Based Routing** section, click **+** to add a new route.
5. Enter a **Name** for the route and click **OK**.
6. In the **Source Networks** table, add the network for which the routing table is consulted., e.g., `62.99.0.0/24`
7. In the **Routing Table Contents** section, click **+** to configure the route.
8. In the **Target Network Address** field, enter `0.0.0.0/0.`
9. Select **unicast** as the **Route Type**.
10. Enter the **Gateway** IP address, e.g., `62.99.0.254`
11. Click **OK**.
12. Select **postmain** as the **Table Placement** option.
13. Click **OK**.
14. Click **Send Changes** and **Activate**.

Step 3. Configure Link Monitoring

Configure link monitoring for the static Internet connection. This is important for cases where e.g., the ISP router in front of the firewall does not go down but the uplink beyond does.

> To ensure proper functionality of monitoring via ICMP, it is strongly recommended to use a hosted, secured IP address or an address provided by your ISP. Do not use a common public address such as google.com, etc.

1. Go to **CONFIGURATION > Configuration Tree > Network > IP Configuration**.
2. Scroll down to the section **Shared Networks and IPs**.
3. In the **Configuration Mode** menu, select **Switch to Advanced View**.
4. Click **Lock**.
5. Edit the entry for the ISP in the **Shared Network and IPs** section.
6. In the **Reachable IPs** table, add one or more target IP addresses of hosts that should be reachable for probing.
7. Enter commands to be run when gateway or none of the reachable IP addresses is reachable.
8. Click **OK**.
9. Click **Send Changes** and **Activate**.

For the dynamic Internet connection, configure link monitoring for both routes (**default** and **source based**) to monitor IP addresses beyond the ISP gateway.

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. In the left menu, select **xDSL/DHCP**.
3. In the **Configuration Mode** menu, select **Switch to Advanced View**.
4. Click **Lock**.
5. Edit the DHCP link.
6. In the **Connection Monitoring** section, select **ICMP** as the **Monitoring Method**. The Barracuda CloudGen Firewall probes the **Reachable IPs** and, if there is no response, the gateway.
7. Enter one or more target IP addresses to be used for monitoring into the **Reachable IPs** table. These addresses must be reachable only via the DHCP connection.
8. Click **OK**.
9. Click **Send Changes** and **Activate**.

After you configure your routes, you must activate your new network configurations.

1. Go to **CONTROL > Box**.
2. In the left menu, expand **Network** and click **Activate new network configuration**.
3. Select **Failsafe**. A *Network Configuration Reconfigured* message will appear.

Step 4. Create a Custom Connection Object for Link Balancing with Failover (Fallback)

Create a custom connection object for link balancing and failover. For more information, see Connection Objects and How to Configure Failover and Load Balancing in Custom Connection Objects.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. In the left menu, click on **Connections**.

4. Right-click and select **New**. The **Edit/Create a Connection Object** window opens.
5. Enter a **Name** for the connection object. E.g., `LBFailover`
6. Select **From Interface** as the **NAT Address**.
7. In the **Interface Name** field, enter the port the ISP 1 is connected to. E.g. , `port3` or `dhcp`
8. In the **Failover and Load Balancing** section, select one load balancing/failover **Policy**. For more information, see Connection Objects.
   - **Failover**
   - **Weighted Round Robin**
   - **Weighted Random**
   - **Source IP Hash**
   - **Provider Optimization**
9. Click **OK**.
10. Click **Send Changes** and **Activate**.

Step 5. Apply the Connection Object

Use the object for all access rules handling outgoing traffic.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. **Edit** an access rule handling outgoing traffic. E.g., **LAN-2-INTERNET**
4. Select the custom connection object created in Step 4 from the **Connection Method** list.
5. Click **OK**.
6. Click **Send Changes** and **Activate**.

Step 6. (optional) Configure Notifications

You can configure the Barracuda CloudGen Firewall to send SNMP traps or email notifications in case one of the ISP connections fails. Depending on what kind of notification you want to send, change the **notification ID** for:

- **62 (Route Changed)**
- **64 (Route Disabled)**

For more information, see Events.

You are now load balancing and/or using failover for all outgoing connections, which are handled by access rules using the custom connection object. If needed, you can define multiple custom connection objects and use them to control which ISP connections are used by a specific network or IP

address.

Figures

1. stat_dhcp_wan.png

© 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.