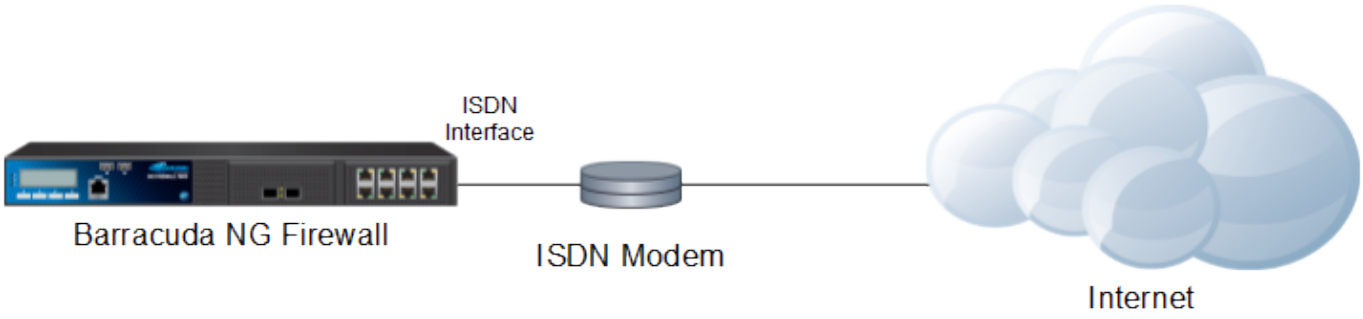
How to Configure an ISP with ISDN

https://campus.barracuda.com/doc/41116391/

The Barracuda NG Firewall supports up to four ISDN connections. The ISDN connection is initiated at startup or in **Dial-On-Demand** mode when used as a backup connection.



In this article:

Before you Begin

- Verify that you have the necessary configuration information provided to you by your ISP.
- Before configuring channel bonding (=mppp), verify that your provider supports this feature.

Step 1. Create and Configure the ISDN Connection

Enter the properties for the ISDN modem card and configure connection details.

1. Open the **Network** page (**Config > Full Config > Box**).
2. In the left menu, select **xDSL/DHCP/ISDN**.
3. Click **Lock**.
4. Set **ISDN Enabled** to **Yes**.
5. To use the ISDN modem as a backup connection, set **Standby Mode** to **Yes**.
   Standby connections must be started by a command line script. For more information, see Operating an ISDN Link in Standby Mode
6. Click **Set** next to **ISDN Settings**. The **ISDN Settings** window opens.
7. Select your card type from the **ISDN Modem Card** list.

8. Enter the **Provider Phone Number** that has been given to you by your provider.
9. Select the applicable **Encapsulation Mode**. The following modes are available:
   - **SyncPPP (default)** – Bit-oriented transfer protocol.
   - **RawIP** – No PPP; IP addresses must be specified manually. This mode can only be used with static IP addresses.
10. Select the **Dial Mode**. If set to **Dial-On-Demand**, specify **Idle Hangup Time** to automatically disable the link when it is not used anymore.
11. Enable **Use Channel Bonding** if applicable and supported by your ISP:
    1. Click **Set** next to **Channel Bonding Settings** and adjust the on-demand bandwidth allocation for the second channel.
    2. Enable **Use 2nd S0 Bus** if a 2nd S0 is required.
    3. Click **Set** next to **Parameters for 2nd S0 Bus** and configure the settings.
12. If you want to restrict the time when the ISDN connection can be established, set **Dial Allowed From / Until**.
13. If your ISP assigned your connection a static address, disable **Dynamic Address Assignment** and enter the **Static IP/Mask** and **Static Gateway IP** address.

Step 2. Configure Authentication

Select an authentication method and enter the credentials provided by your ISP.

1. In the **Authentication** section, select the **Authentication Method** that is used for the connection.
2. Enter the **User Access ID**, **Sub-ID,** and **Password** assigned by your provider. Do not enter the # sign.
3. If required, enter the **Provider Name**, which is appended to your User Access ID.
4. Select **Use ProviderDNS** to use the DNS servers assigned by your provider.
5. When using dynamic DNS, select **Use Dynamic DNS** and click **Set**. The **Dynamic DNS Params** window opens.
   1. Select a dynamic DNS **Service Type**. For information about available DynDNS service types, see http://www.dyndns.com/services/.
   2. Enter the **Dyn DNS Name** that was registered at dyndns.org.
   3. Enter the **User Access ID** and **Password** for accessing the server as defined during registration at dyndns.org.

Step 3. Configure Connection Monitoring

Configure connection monitoring by entering a list of health check targets that are only reachable through this connection. Should the ping to these health check targets fail, the Barracuda NG Firewall will terminate and reestablish the connection until the monitoring target IP addresses are reachable again.

1. In the **Connection Monitoring** section, select the Monitoring method:
   - **LCP** – If ping fails, the dial-in daemon is probed directly via LCP.
   - **ICMP** – The Barracuda NG Firewall probes the **Reachable IPs** and, if there is no response, the gateway.
   - **StrictLCP** – No ICMP probing occurs.
2. Enter one or more **Reachable IPs** to monitor the availability of the connection. The target IP addresses should only be accessible via this connection.
3. Select the **Unreachable Action** to be taken if the connection cannot be established. The following options are available:
   - **Restart** – Restarts the connection.
   - **Increase-Metric** – Changes the preference for ISDN routes until the probe succeeds.
4. Click **OK**.
5. Click **Send Changes** and **Activate**.

Step 4. Activate Network Changes

You must activate the network changes to bring up the xDSL connection.

1. Open the **Box** page (**Control > Box**).
2. In the left menu, expand the **Network** section and click **Activate new network configuration**.
3. Select **Failsafe**. The 'Failsafe Activation Succeeded' message is displayed after your new network configurations have been successfully activated.

Your ISDN connection is now active and the IP addresses assigned by your ISP are visible on the **CONTROL > Network** page. The status icons next to the ISDN interface are green, indicating an active connection. If the ISDN connection is your primary uplink, the default route pointing to the ISDN interface is also created. If more than one default route is present, the connection with the lowest route metric is used.

Operating an ISDN Link in Standby Mode

Enable **Standby Mode** in the ISDN configuration if you want to use the ISDN connection as a backup uplink. In standby mode, activation and subsequent monitoring of the connection must be triggered externally. Standby mode also lets you combine HA setups for HA ISDN connections.

1. The ISDN routes are set to **pending**, and the Barracuda NG Firewall does not check whether they are established.
2. The configuration is completely run through but the connection is not yet established.

Standby connection can only be started by a command line script. Example usage:

- connection start: `/etc/phion/dynconf/network/isdnrestart &`
- connection stop: `/etc/phion/dynconf/network/wipeisdn &`

Figures

1. isdn_wan.png