How to Configure a PPPoE xDSL WAN Connection with an External DSL Modem

https://campus.barracuda.com/doc/17250/

The firewall can dial in using PPPoE with an external modem and PPPoA on specific models with an internal DSL modem. The xDSL connection can be configured to be in Active or Standby mode. In Standby mode, the activation and subsequent monitoring of the link must be triggered externally. PPPoE/PPPoA requires no special configuration to the access network. Each PPP session learns the Ethernet address of the remote peer and creates a unique session identification (ID).

Before You Begin

- Connect the external xDSL modem supplied by your ISP to a port on the Barracuda CloudGen Firewall.
- Verify that you have all the necessary configuration information provided to you by your ISP.

Step 1. Configure Link Properties

Specify the properties for the DHCP link and define the transport protocol for PPP.

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. In the left menu, select **xDSL/DHCP**.
3. Click **Lock**.
4. Set **xDSL Enabled** to **Yes**.
5. In the **xDSL Links** table, click **+** to add an entry.
6. Enter a name for the xDSL link (no special characters) and click **OK**. The **xDSL Links** window opens.
7. Select the **Connection Type** to specify the transport protocol for PPP.
8. (optional) Enter the **Static Local** and **Gateway IP** address if your ISP does not assign it automatically.
9. Select the **Ethernet Interface** the xDSL modem is attached to.

Step 2. Configure Authentication

Most ISPs require authentication information to connect. These configuration settings are provided by your ISP. If no authentication is required, set **Authentication Method** to **NONE**.

If you use the PPPoE xDSL WAN connection for transmitting Web traffic, and if you also want to enable **PPPoE Acceleration**, you must set certain configuration parameters in the **Advanced Access Rule Settings** to the following values:

- **Maximum Segment Size** – 1400
- **Clear DF Bit** – Enable this option.

For more information, see [Advanced Access Rule Settings](#).

1. In the **Authentication** section, select the **Authentication Method**. Default: **PAP_or_CHAP**
2. In the **User Access ID** field, enter the principal account name (PPP username) assigned by your xDSL provider.
3. If your provider assigned a sub-ID to you, select **Add Sub-ID** and enter it in the **User Access Sub-ID** field. Do not enter the # sign.
4. Enter the **Access Password** assigned by your xDSL provider.
5. If a domain name is required as the user login, select **Add Provider** and enter the **Provider Name**.

   The user ID is generated automatically by combining **User Access ID**, **User Access Sub-ID** (if required), and **Provider Name** with # and @ symbols added between the parameters: [user_id]#[access_sub_id]@[provider_name]. E.g., 000xxxxxxxxx520069204717#0001@t-online.de
6. To use your ISP's DNS servers, select **Use ProviderDNS**.
7. To use dynamic DNS, select **Use Dynamic DNS** and click **Set**. The **Dynamic DNS Params** window opens.
   1. Select a dynamic DNS **Service Type**. For information on DynDNS service types, see http://www.dyndns.com/services/.
   2. Enter the **DynDNS Name** that was registered on dyndns.org.
   3. Enter the **User Access ID** and **Access Password** for accessing the dyndns.org service.
8. Click **OK**.

Step 3. Configure Routing Settings

Configure whether to create a default route, dynamic routing, and the route metric.

1. Set **Create Default Route** to **YES** to automatically create a default route via this xDSL connection.
2. If you are using dynamic routing protocols like [OSPF/RIP/BGP](#), enable **Advertise Route**.
3. Enter a **Route Metric** if multiple dynamic links are available. The link with the lowest route metric is automatically chosen if more than one default route is available.

Step 4. Configure Connection Monitoring

Configure log settings and define target IP addresses that will be regularly pinged to monitor the availability of the connection. Each target IP address is pinged every 20 seconds (2 ICMP packets each). If there is no response, the link is re-established.

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 CloudGen 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 be accessible only via the xDSL connection.
3. Select the **Unreachable Action** to be taken if the connection cannot be established. The following options are available:
   - **Restart** – Restarts the xDSL connection.
   - **Increase-Metric** – Changes the preference for xDSL routes until the probe succeeds.
4. Click **OK**.
5. Click **Send Changes** and **Activate**.

Step 5. Activate Network Changes

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

1. Go to **CONTROL > Box**.
2. In the left menu, expand the **Network** section and click **Activate new network configuration**.
3. Select **Failsafe**.

Your xDSL connection is now active, and the IP address assigned by your ISP is visible on the **CONTROL > Network** page. All status icons next to the ppp1 interface are green, indicating an active connection. If the xDSL connection is your primary Internet connection, the default route pointing to the ppp1 interface is also created. If more than one default route is present, the connection with the lowest route metric is used.

Operating an xDSL Link in Standby Mode

If required, e.g., for maintenance purposes, you can enable **Standby Mode** in the link configuration.

In Standby mode, the activation and subsequent monitoring of the link must be triggered externally. Standby mode also lets you combine HA setups for HA xDSL connections. In Standby mode:
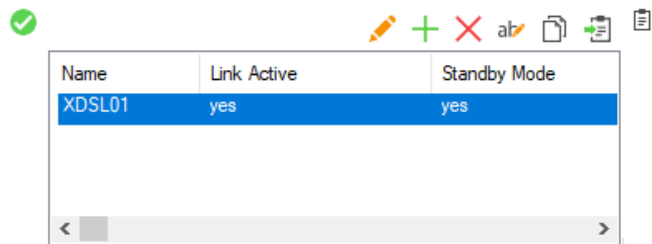
1. The involved routes are set to a pending state, and it is not checked whether they are established.
2. The configuration is completely run through, but the connection is not yet established.

Connecting is handled from the Command-Line Interface via a server-side script that is used for starting and stopping the connection with corresponding command lines:

- Start all xDSL connections – `/etc/phion/bin/openxdsl start &`
- Stop all xDSL connections – `/etc/phion/bin/openxdsl stop &`
- Start an explicit xDSL connection – `/etc/phion/bin/openxdsl start <linkname> &`
- Stop an explicit xDSL connections – `/etc/phion/bin/openxdsl stop <linkname> &`

<linkname> is the name of the configuration entry in the **xDSL Links** list:

Note: An external DSL modem is required to configure xDSL links.

Troubleshooting

In some cases, especially in combination with PPPoE acceleration, the segment size of the packets going into the tunnel might be too big. Set the **MSS (Maximum Segment Size)** to **1350** and **clear DF bit** to **yes** in the **Advanced Settings** tab for all access rules handling incoming and outgoing traffic for the PPPoE connection.

To review logs regarding DSL/PPPOE connection issues, see the **network.adsl.log** and **network-ppp.log** files respectively for connection and authentication issues.

Figures

1. xDSL_01.png