

---

## How to Configure Connection Fallback using Multiple VPN Gateways

<https://campus.barracuda.com/doc/46207305/>

Configure the Barracuda VPN Client for Windows to silently switch to fallback VPN gateways when a VPN gateway is not reachable, such as when the client is used in different corporate networks or geographic locations. A working VPN connection is always available and the appropriate gateway is automatically selected.

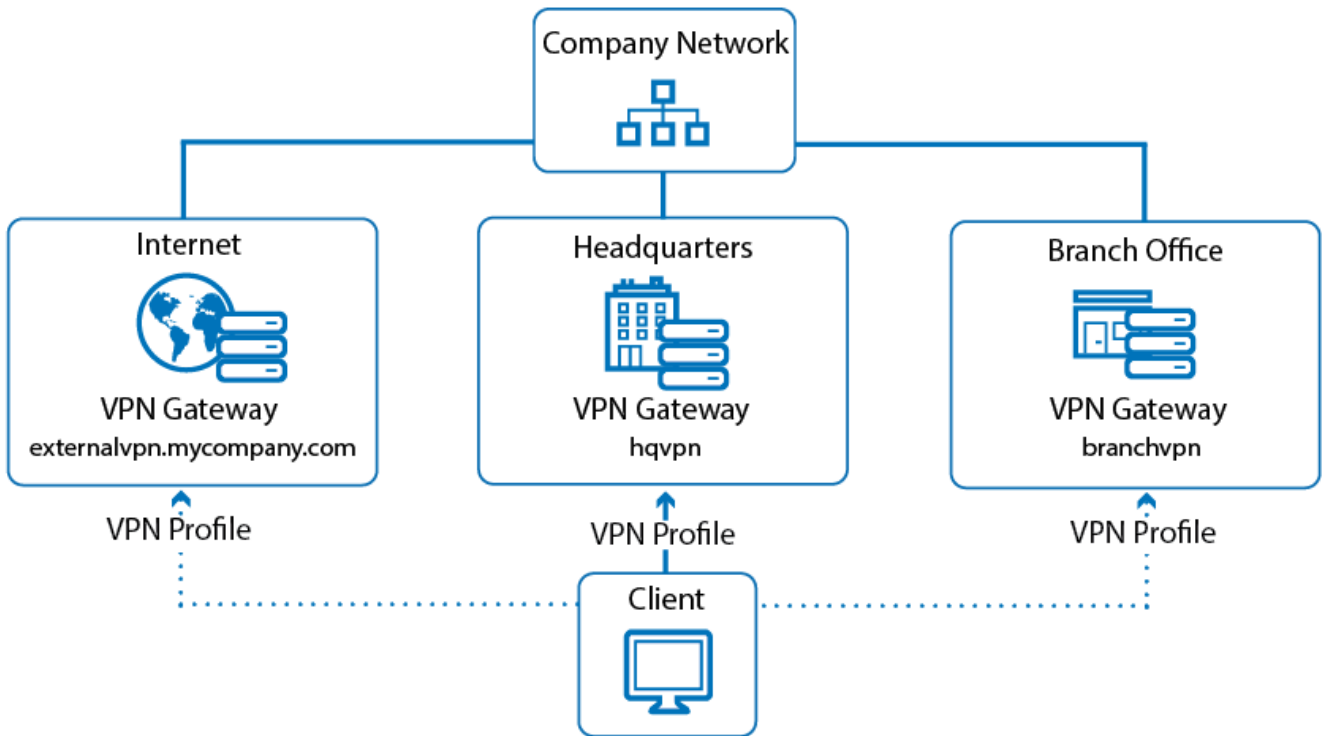
### Example Scenario

---

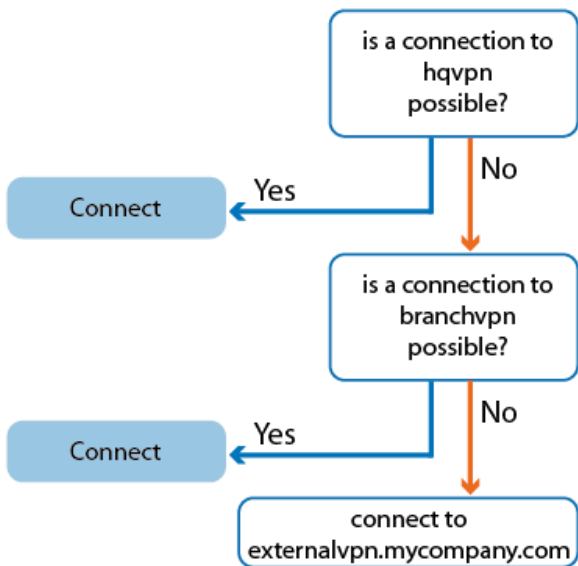
In this example, three VPN profiles are used to connect to a corresponding gateway into the company network:

- **externalvpn.mycompany.com** – The gateway to be used when the client is not connected to a corporate network.
- **hqvpn** – The gateway to be used within the company HQ network.
- **branchvpn** – The gateway to be used within a branch office network.

These VPN profiles are configured as part of a fallback chain that will be used by the VPN client to find the appropriate gateway. You can initiate a VPN connection using the **hqvpn** profile that is set as the default VPN profile. If necessary, the VPN client will try each configured VPN profile in the fallback chain until it can establish a connection.



**Fallback chain:**



**Configure the VPN Profiles**

Configure the VPN profiles for the three gateways as shown in the example scenario.

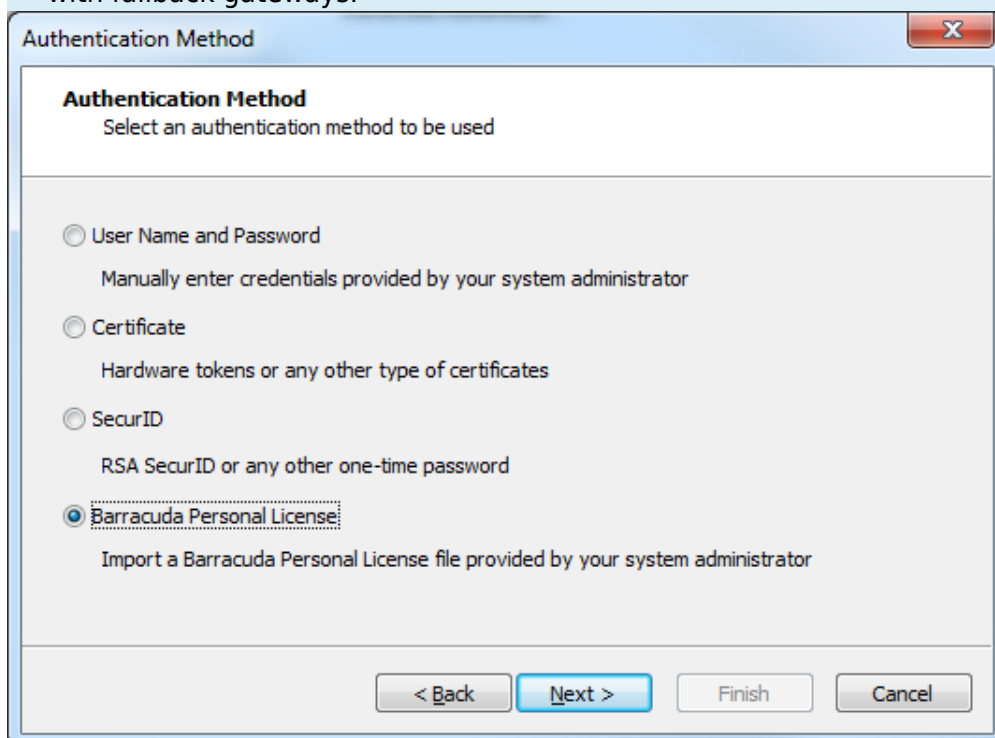
### Step 1. Set up the VPN Gateways

Create a VPN profile for each of the three VPN gateways.

1. In the **Barracuda VPN Client** window, click **Preferences**. The **Barracuda VPN Control** window opens.
2. Click **New** in the left navigation pane to launch the **Profile Wizard**. You can also right-click the window's main area and select **New (Wizard)** or **New**.
3. In the **Remote Server** field, enter the IP address or host name of the first gateway. E.g.:  
externalvpn.mycompany.com
4. Select the **Remember my user name** check box so that the client will reconnect to this server without prompting users for their username.
5. Click **Next**.
6. On the **Authentication Method** screen, select your authentication method:

- If you choose **User Name and Password**, you must configure additional settings to save the password locally if you do not want the client to constantly prompt users for a password when changing gateways.
- To automatically reconnect in the background, select **Certificate** or **Barracuda Personal License**.

Do not select **SecurID** because it uses one-time passwords, which are not suitable with fallback gateways.

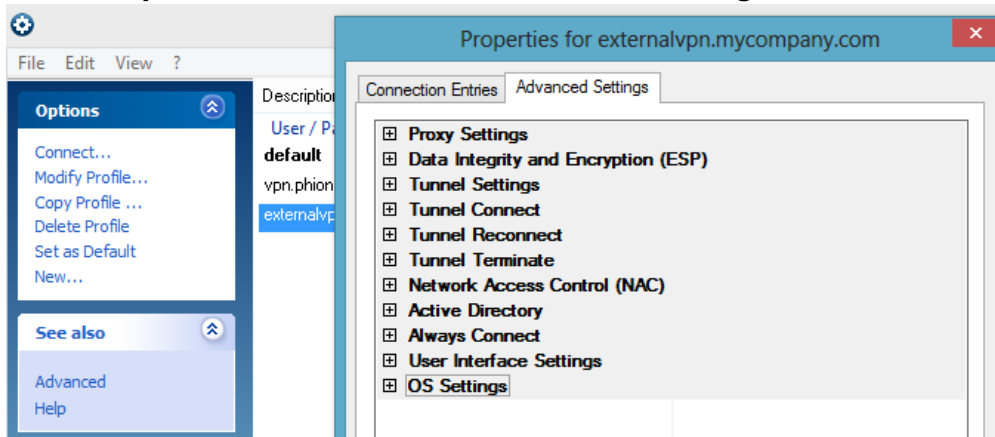


For more information on configuring a profile and choosing the correct authentication method, see [How to Create VPN Profiles](#).

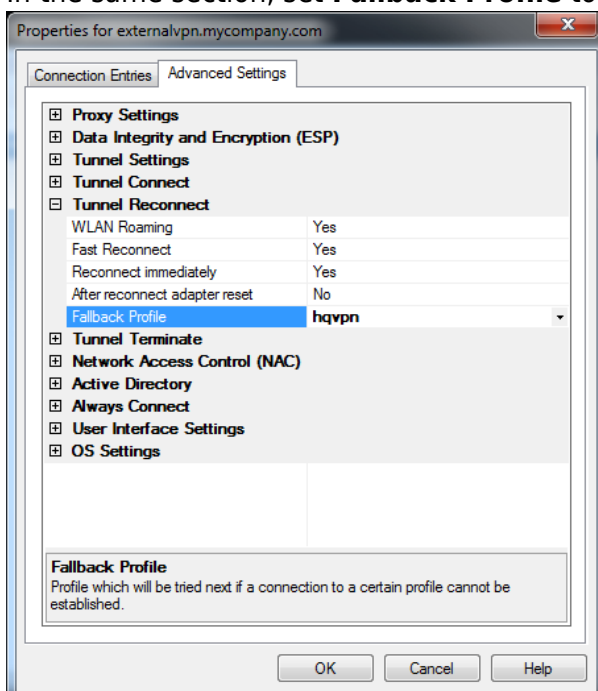
7. Configure the two remaining profiles with your respective parameters. The two remaining profiles used in the example scenario are named hqvpn and branchvpn, and they point to identically named VPN servers.

## Step 2. Configure externalvpn.mycompany.com

1. In the **Barracuda VPN Control** window, right-click the **externalvpn.mycompany.com** entry and select **Modify Profile**.
2. In the **Properties** window, click the **Advanced Settings** tab.



3. In the **Tunnel Connect** section, set **Enable VPN Tunnel Probing** to **Yes**. This setting ensures that the client will always use the fastest available gateway.
4. In the **Tunnel Reconnect** section, set **WLAN Roaming**, **Fast Reconnect**, and **Reconnect immediately** to **Yes**.
5. In the same section, set **Fallback Profile** to **hqvpn**.



With this option set, the next gateway in the chain will be tried if the primary gateway is not reachable.

6. Because the externalvpn.mycompany.com gateway is used when the client is not connected to the company network, you should disable it in the company network.
7. Although the external URL of a company's VPN server should not be reachable from within a cleanly configured company network, you can accelerate the switch to the next fallback profile by enabling the client to detect the company's Active Directory (AD) service.

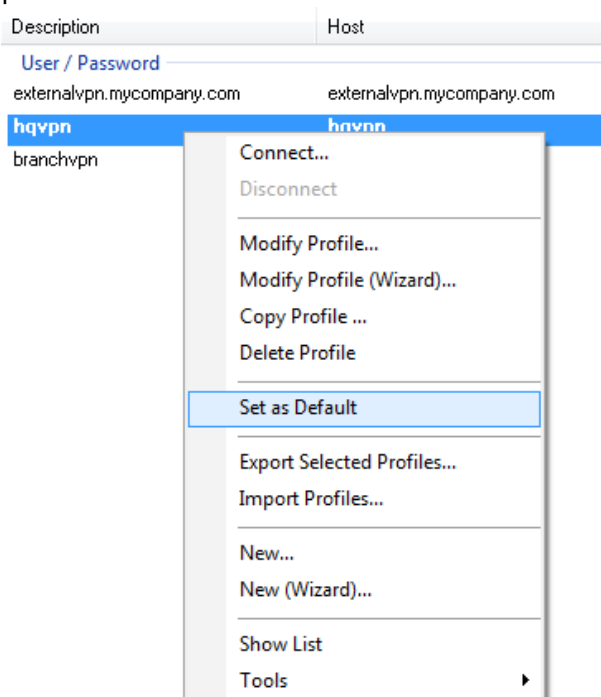
In the **Active Directory** section, configure the following settings:

- Set **Probe Active Directory** to **Yes**.
  - In the **Active Directory IP** field, you can enter one or more known IP addresses for the MSAD service to help the client quickly detect the AD service.
8. In the **User Interface Settings** section, configure the following settings:
- If you configured username and password authentication, set **Remember logon user name** to **Yes** to disable login prompts.
  - To store credentials after they are entered, set **Use MS Credential Manager** to **Local**.
  - To disable the informational pop-up window that displays connection status changes, set **Show Popup** to **No**.
9. Click **OK** to save the configuration.

### Step 3. Configure hqvpn

Configure the hqvpn profile with the same settings as the external profile, with these three exceptions:

1. In the **Tunnel Reconnect** section, set **Fallback Profile** to **branchvpn**. This way, the branch network's VPN gateway is defined to be the next gateway in the chain.
2. Disable Active Directory probing. In the **Active Directory** section, set **Probe Active Directory** to **No**.
3. Define hqvpn as the default profile by right-clicking its list entry in the **Barracuda VPN Control** window and selecting **Set as Default**. The client will automatically start with this profile in the fallback chain when it tries to establish a connection.



## Step 4. Configure branchvpn

Configure the branchvpn profile with the same settings as the hqvpn profile, with these two exceptions:

- In the **Tunnel Reconnect** section, set **Fallback Profile** to **externalvpn.mycompany.com**. This closes the fallback chain so that the external VPN gateway will be tried next if none of the company's internal VPN gateways is reachable.
- Do not select **branchvpn** as the default profile.

## Figures

1. vpn\_fallback.png
2. fallback\_chain.png
3. vpn\_auth.png
4. vpn\_adv.png
5. vpn\_adv\_fallback.png
6. vpn\_set\_default.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.