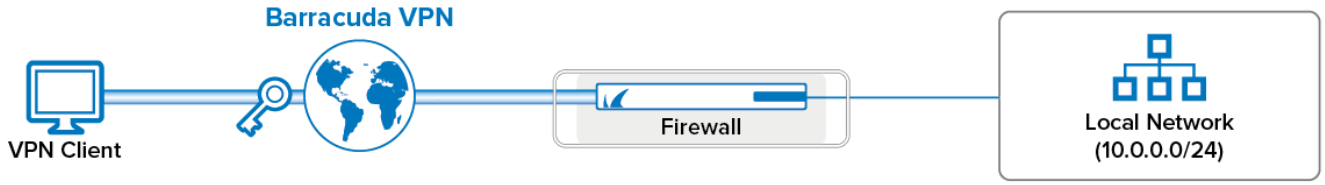
How to Configure a Client-to-Site TINA VPN with Personal Licenses

https://campus.barracuda.com/doc/96026129/

To let mobile workers securely connect to corporate resources, you can configure a client-to-site TINA VPN. Follow the steps in this article to configure a client-to-site VPN with the built-in Barracuda CA (lic files). To connect to this type of VPN, clients require the Barracuda VPN Client, an optionally password-protected certificate license file, and a server password. You can connect from any IPv4 or IPv6 address, as long as an external IPv4 and IPv6 address are configured as a service IP address for the VPN Service. Traffic passing through the client-to-site VPN is limited to IPv4. Only one simultaneous connection is possible for personal licenses. Use VPN Group policies and an Advanced Remote Access subscription to be able to have multiple concurrent connections by the same user.



Supported VPN Clients

The following VPN clients are compatible with this client-to-site configuration:

- Barracuda Network Access and VPN Client

Before You Begin

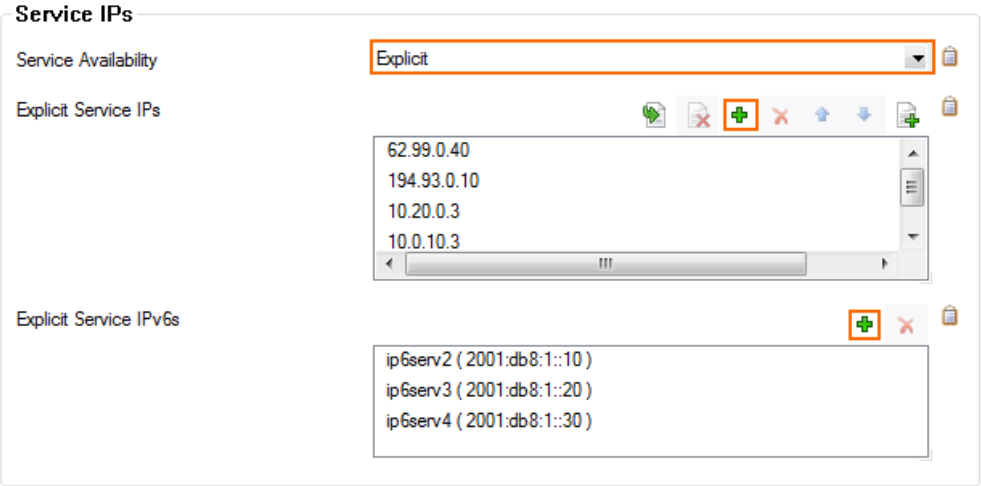
- Set up the VPN certificates using the Barracuda VPN CA. For more information, see How to Set Up Barracuda VPN CA VPN Certificates.
- Identify the subnet (static route) or a range in a local network (proxy ARP) to be used for the VPN clients.

Step 1. Configure the VPN Service Listeners

Configure the IPv4 and IPv6 listener addresses for the VPN service.

1. Go to **CONFIGURATION > Configuration Tree > Assigned Services > VPN > Service Properties**.
2. Click **Lock**.

3. From the **Service Availability** list, select the source for the IPv4 listeners of the VPN service.
   - When selecting **Explicit**, click **+** for each IP address and enter the IPv4 addresses in the **Explicit Service IPs** list.
4. Click **+** to add an entry to the **Explicit IPv6 Service IPs**.
5. Select an IPv6 listener from the list of configured explicit IPv6 service IP addresses.



6. Click **Send Changes** and **Activate**.

Step 2. Configure the Service and Default Server Certificates

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. Verify that the **Default Server Certificate** and **Default key** are both valid (green). If the **Default Server Certificate** and **Default key** are not valid, see How to Set Up Barracuda VPN CA VPN Certificates.
4. In the left menu, select **Service Keys**.
5. Right-click the table, and select **New Key**.
6. Enter the **Key Name**.
7. Select the **Key Length**.
8. Click **OK**.
9. Click **Send Changes** and **Activate**.

Step 3. Configure the VPN Client Network

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. In the left menu, select **Client Networks**.
4. Right-click the table, and select **New Client Network**.

5. In the **Client Network** window, configure the following settings:
    - **Name** – Enter a descriptive name for the network, e.g.: `Client to Site VPN Network`
    - **Network Address** – Enter the default network address, e.g.: `192.168.6.0`. All VPN clients will receive an IP address in this network.
    - **Gateway** – Enter the gateway network address, e.g.: `192.168.6.254`
    - **Type** – Select the type of network that is used for VPN clients:
        - **routed (Static Route)** – A separate subnet. A static route on the Barracuda CloudGen Firewall routes traffic between the VPN client subnet and the local network.
        - **local (proxy ARP)** – A subnet of a local network. For example, Local network: `10.0.0.0/24` , Local segment `10.0.0.128/28` . You must also specify the IP range for the network:
            - **IP Range Base** – Enter the first IP address in the IP range for the VPN client subnet, e.g.: `10.0.0.128`.
            - **IP Range Mask** – Specify the subnet mask of the VPN client subnet, e.g.: 28
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Step 4. Create a Barracuda VPN CA Template

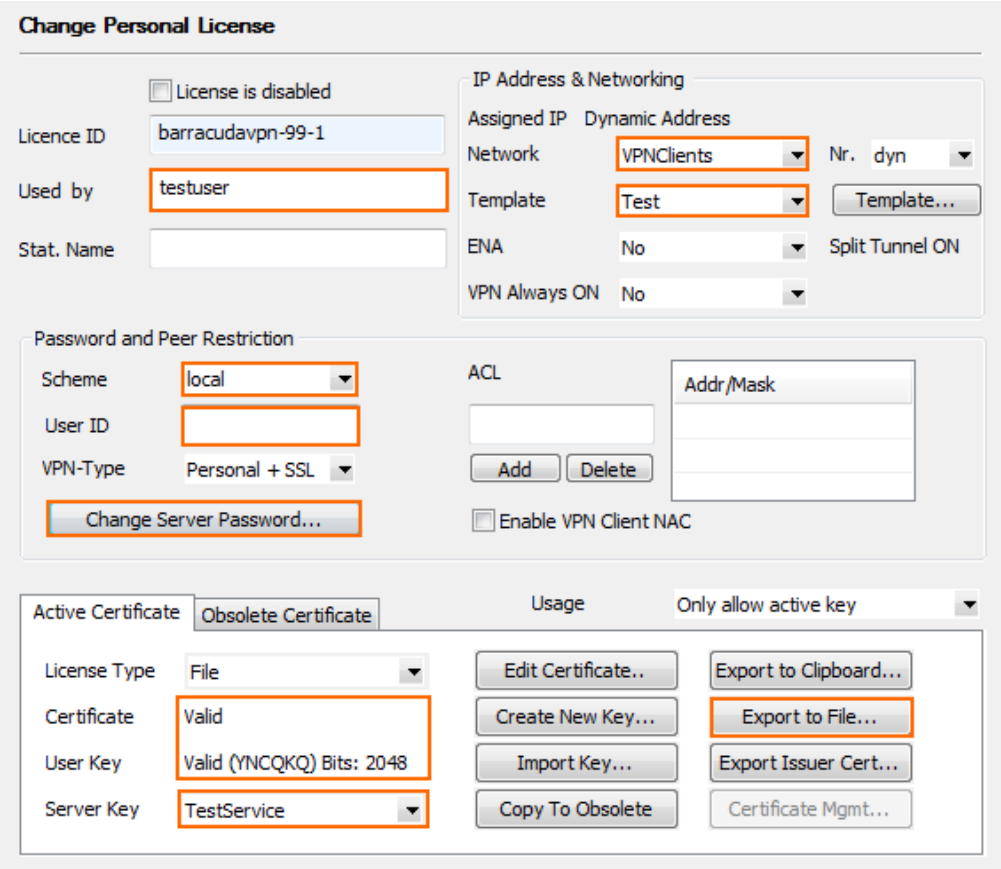
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Client to Site**.
2. Click **Lock**.
3. Click the **Barracuda VPN CA** tab, and then click the **Templates** tab under it.
4. Right-click the table, and select **New Template**.
5. In the **Barracuda Templates** window, configure the following settings:
    - **Name** – Enter a descriptive name for the template.
    - **(optional) DNS** – Enter the IP address of the DNS server.
    - **(optional) WINS** – Enter the IP address of the WINS server.
    - **Network Routes** – Add the routes to the local network. Enter the IP address, e.g.: `10.0.0.0/24` and click **Add** to add the entry.
    - **Accepted Ciphers** – Select the encryption algorithms that the VPN server will offer. Recommended settings:
        - **AES** for licensed systems.
        - **DES** for export restricted systems.
6. Click **OK** to save the template.
7. Click **Send Changes** and **Activate**.

Step 5. Add a Personal License

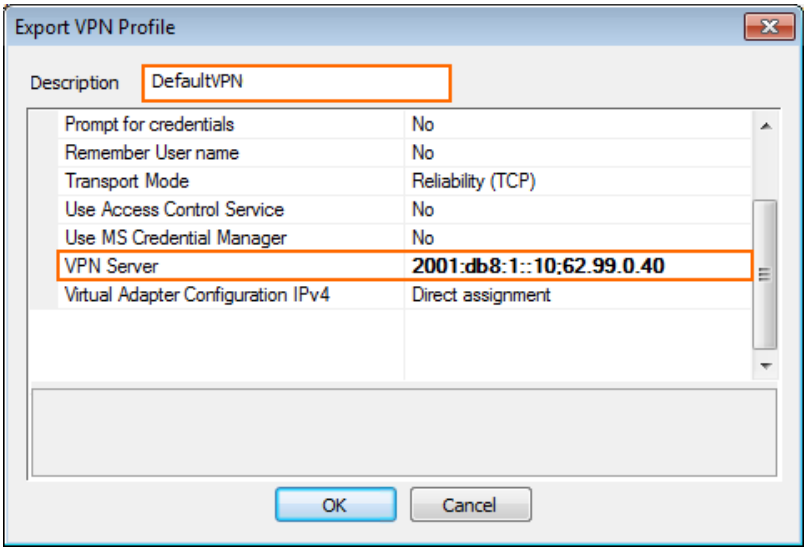
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service**

> Client to Site.

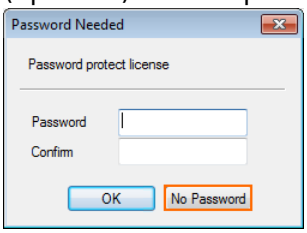
2. Click **Lock**.
3. Click the **Barracuda VPN CA** tab and then click the **Pool Licenses** tab under it.
4. In the upper table, select your **VPN Pool Licenses**.
5. Right-click the lower table, and select **New personal license**.
6. Select an index number for the new license, and then click **OK**. The **Personal License** window opens.
7. In the **Used by** field, enter the name of the user. E.g., `Test User`
8. Enter the **IP Address & Networking** settings:
   - **Network** – Select the VPN client network configured in step 3.
   - **(optional) Template** – Select a Barracuda VPN CA Template.
   - **(Windows NAC Client only) ENA** – Select to prevent clients from accessing any other than the published VPN network.
9. Configure the authentication service in the **Password and Peer Restriction** section:
   - Select **local** to use a server password to log in. Click **Change Server Password** to set a server password.
   - For external authentication servers, select the scheme, and enter the **User ID** user name. The user must enter the password associated with this user when logging in. For more information, see Authentication.
10. Click on the **Active Certificate** tab.
11. Select the server certificate from the **Certificate** list. E.g., **ServerCertificate**.
12. Verify that the **Certificate** and **User Key** are listed as **Valid**.
13. Click **Export to File** and **Export to *vpn file**. The **Export VPN Profile window opens**.



14. Enter a **Description**.
15. Enter the public IPv4 or IPv6 address the VPN service is listening on. Separate multiple IP addresses with a semicolon.



16. Click **OK**.
17. (optional) Enter a password to protect the file, and click **OK**, or click **No Password**.



18. Click **Send Changes** and **Activate**.

In the **Status** column next to the new personal license, a green check mark indicates that the license file can now be used on a client to connect to the VPN.

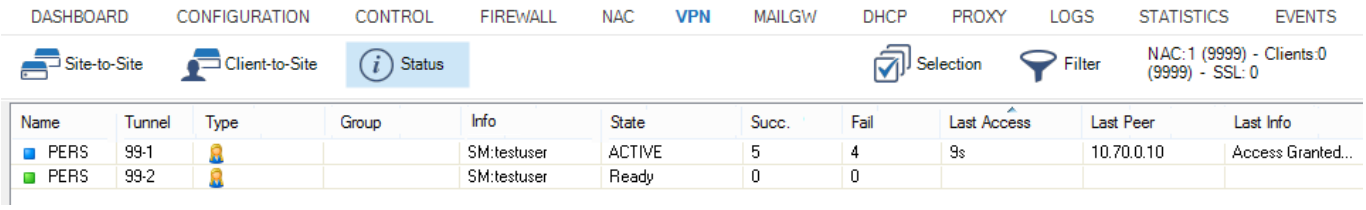
Status	Idx	Type	Person	IP	ENA	VPNNet	ServerKey	Template	Key Hash	License
Active	001		testuser	192.168.3.1+dyn	No	VPNClients	TestService	Test	YNCQKQ	barracudavpn-99-1

Step 6. Add Access Rules

Add two access rules to connect your client-to-site VPN to your network. For instructions, see How to Configure an Access Rule for a Client-to-Site VPN.

Monitoring VPN Connections

On the **VPN > Client-to-Site** page, you can monitor VPN connections.



The page lists all available client-to-site VPN tunnels. In the **Tunnel** column, the color of the square indicates the status of the VPN:

- **Blue** – The client is currently connected.
- **Green** – The VPN tunnel is available, but currently not in use.
- **Grey** – The VPN tunnel is currently disabled. To enable the tunnel, right-click it and select **Enable Tunnel**.

For more information about the **VPN > Client-to-Site** page, see VPN Tab.

VPN Log File

The VPN service uses the /VPN/VPN log file.

Figures