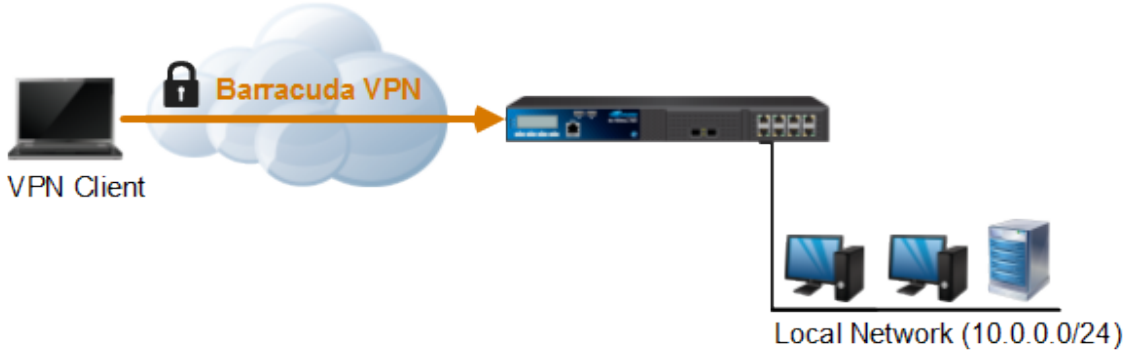
How to Configure a Client-to-Site Barracuda TINA VPN with Personal Licenses

https://campus.barracuda.com/doc/43847267/

To let mobile workers securely connect to corporate information 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. To enable multiple concurrent client-to-site sessions per user, a premium remote access subscription is required.



In this article:

Before You Begin

- Verify that the VPN service has been properly configured and that all necessary certificates are installed. For more information on how to create a service, see How to Configure Services.
- If you are deploying a routed (static route) client-to-site VPN, identify the subnet and gateway for the VPN clients in your network.
- If you are deploying a local (proxy ARP) client-to-site VPN, identify the subnet of the home network to be used for the VPN clients.
- To enable multiple simultaneous client-to-site connections by the same user, a premium remote access subscription is required. For more information, see Licensing

Step 1. Configure the Service and Default Server Certificates

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > VPN Settings** .
2. Click **Lock**.

3. Click **Click here for Server Settings**.
4. 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 VPN Certificates.
5. Click **OK**.
6. Click on the **Service Certificates/Keys** tab.
7. Right-click the table, and select **New Key**.
8. Enter the **Key Name**.
9. Select the **Key Length**.
10. Click **OK**.
11. Click **Send Changes** and **Activate**.

Step 2. Configure the VPN Client Network

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > VPN Settings** .
2. Click **Lock**.
3. Click the **Client Networks** tab.
4. Right-click the table, and select **New Client Network**.
5. In the **Client Network** window, configure the following settings:
    1. **Name** – Enter a descriptive name for the network, e.g.: `Client to Site VPN Network`
    2. **Network Address** – Enter the default network address, e.g.: `192.168.6.0`. All VPN clients will receive an IP address in this network.
    3. **Network Mask** – Specify the appropriate subnet mask, e.g.: 24
    4. **Gateway** – Enter the gateway network address, e.g.: `192.168.6.254`
    5. **Type –** Select the type of network that is used for VPN clients:
        - **routed (Static Route)** – A separate subnet. A static route on the Barracuda NG 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**.

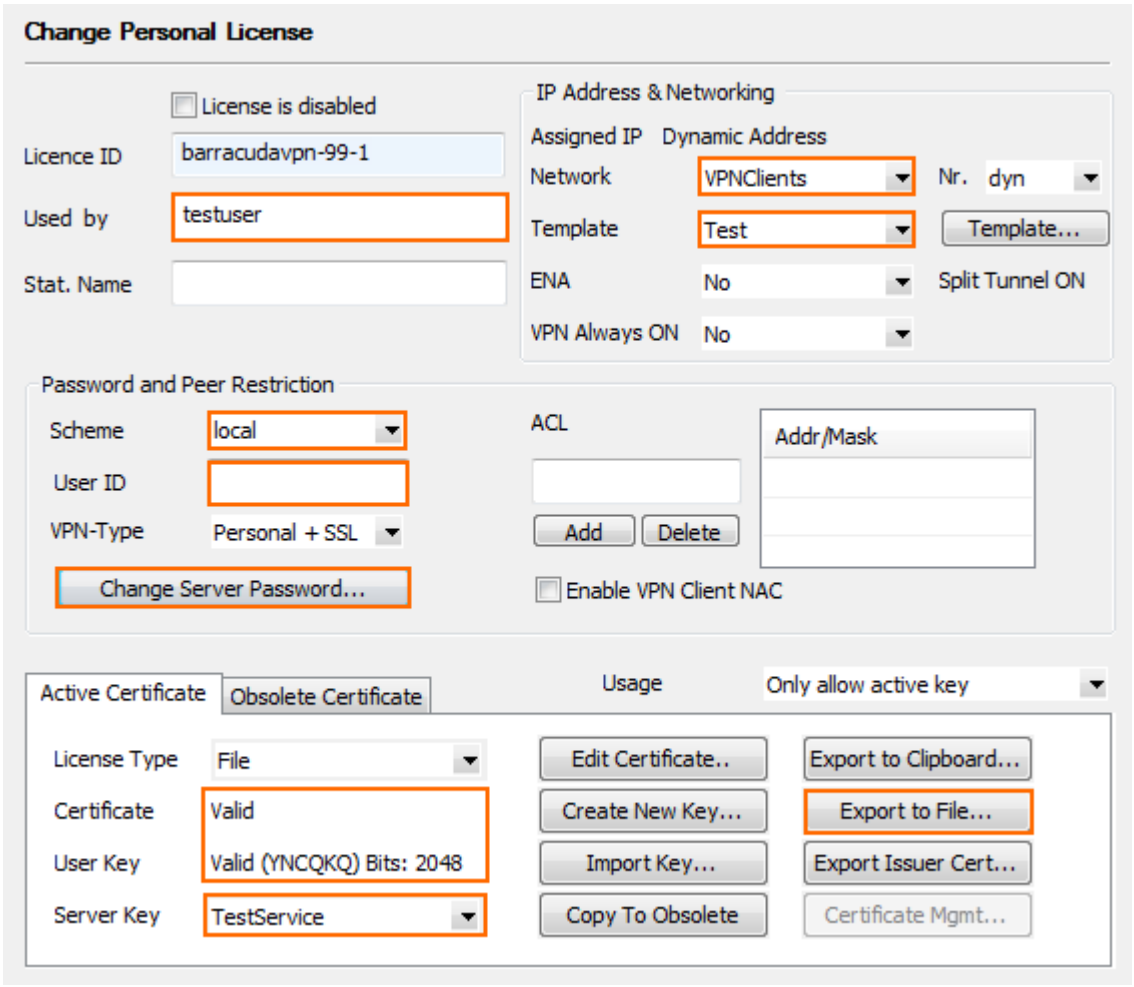
Step 3. Create a Barracuda VPN CA Template

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > Client to Site** .

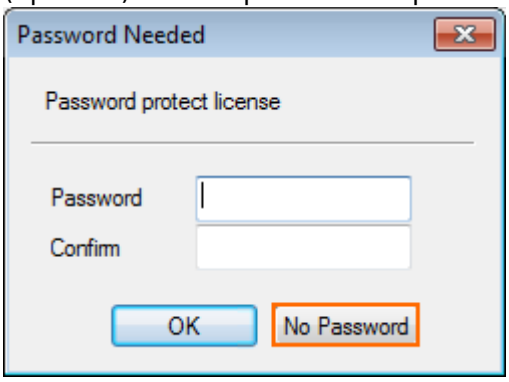
2. Click **Lock**.
3. Click the **Barracuda VPN CA** tab, and then click the **Templates** tab under it.
4. Right-click the table, and select **New Template**.
5. In the **Barracuda Templates** window, configure the following settings:
   - **Name** – Enter a descriptive name for the template, e.g.: `VPNTemplate`
   - **DNS –** (Optional) Enter the IP address of the DNS server.
   - **WINS –** (Optional) 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 4. Add a Personal License

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > 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 1.
   - **(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 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** to export the license file. This file will be distributed to clients to authenticate when connecting to the VPN.

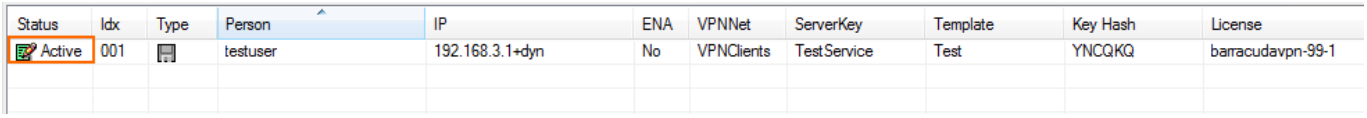


14. (optional) Enter a password to protect the file, and click **OK**, or click **No Password**.



15. 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.



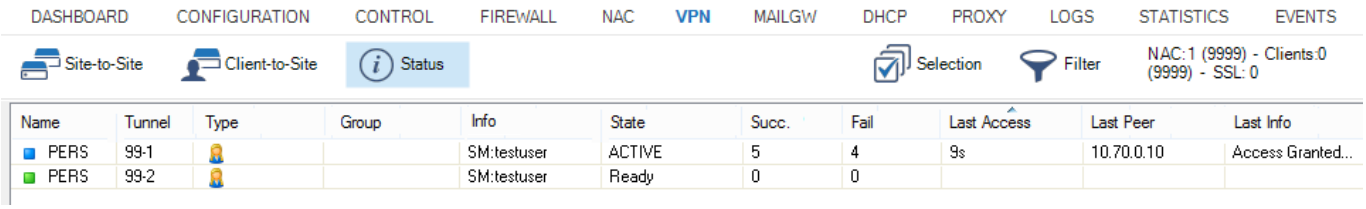
Status	Idx	Type	Person	IP	ENA	VPNNet	ServerKey	Template	Key Hash	License
Active	001		testuser	192.168.3.1+dyn	No	VPNClients	TestService	Test	YNCQKQ	barracudavpn-99-1

Step 5. 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 `/yourVirtualServer/VPN/VPN` log file.

Figures

1. Client2SiteVPN.png
2. c2s_lics01.png
3. c2s_lics02.png
4. c2s_lics03.png
5. ngadmin_vpn_status_client_to_site.PNG