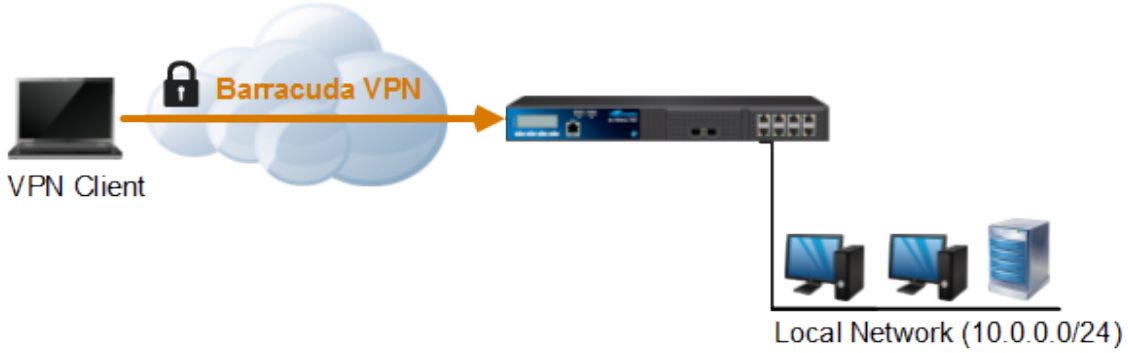
How to Configure a Client-to-Site Barracuda VPN (TINA)

https://campus.barracuda.com/doc/41116192/

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. To connect to this type of VPN, clients require the Barracuda VPN Client, an optionally password-protected certificate license file, and a server password.



In this article:

Before You Begin

Before configuring a client-to-site VPN connection:

- 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 (e.g., *192.168.6.0/24* and *192.168.6.254).*
- 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 (e.g., *10.0.0.50/28*).

Configure the Client-to-Site VPN

To configure the client-to-site VPN service, complete the following steps.

Step 1. Configure the Client Network and Gateway

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. Verify that the default server certificate and key are valid.
    1. Right-click the **Settings** table and select **Edit Server Settings**.
    2. 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.
    3. Close the **Server Settings** window.
4. Create a service certificate/key:
    1. Click on the **Service Certificates/Keys** tab.
    2. Right-click the table and select **New Key**.
    3. Enter the **Key Name**.
    4. Select the **Key Length**.
    5. Click **OK**.
5. Configure the client network.
    1. Click the **Client Networks** tab.
    2. Right-click the table and select **New Client Network**.
    3. 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.
        - **Network Mask** – Specify the appropriate subnet mask, e.g.: 24
        - **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 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 2. Create a Barracuda VPN CA Template

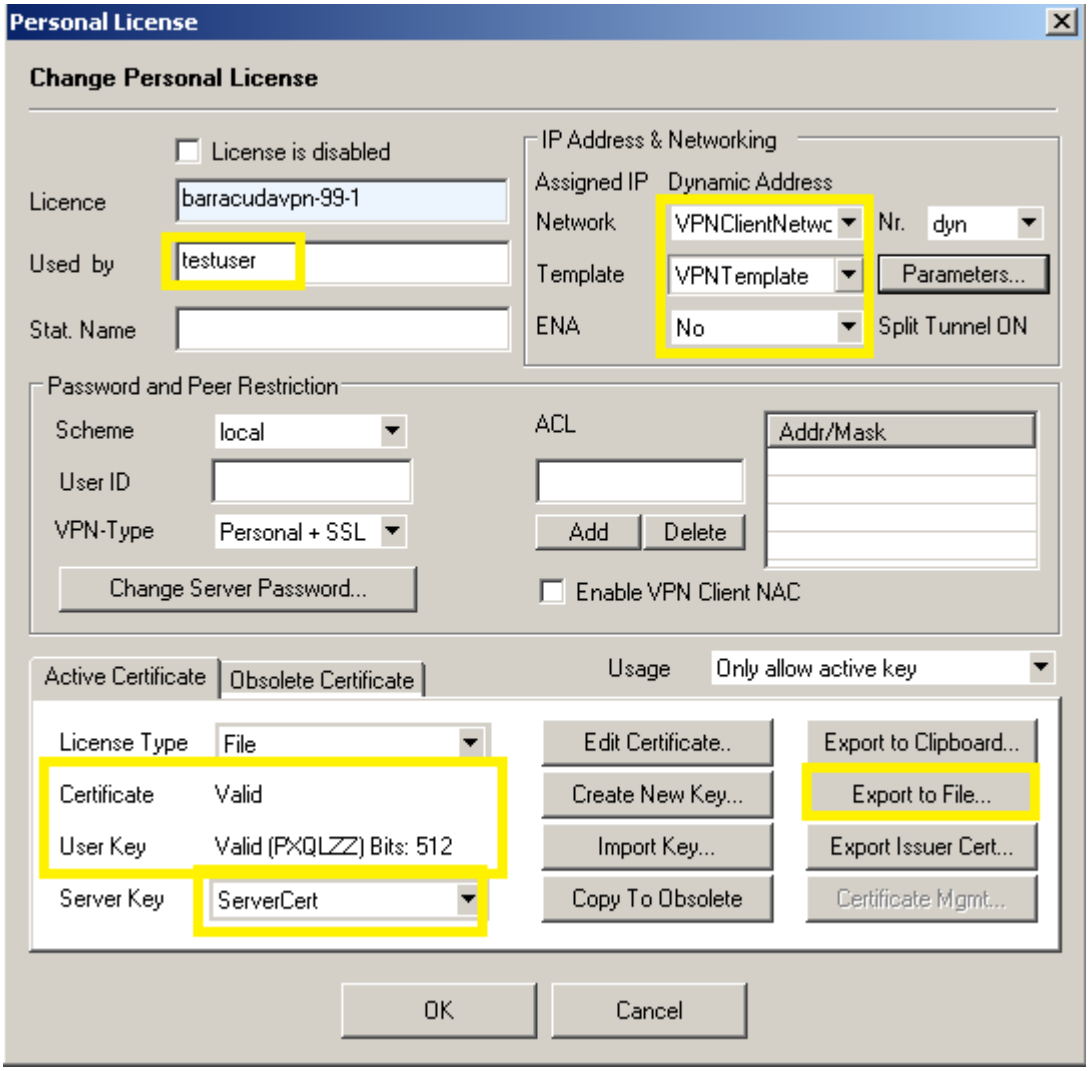
1. Open the **Client to Site** page (**Config > Full Config > Box > Virtual Server > *your virtual server* > Assigned Services > VPN Service > Client to Site**).
2. Click **Lock**.

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 3. Add a Personal License

1. Open the **Client to Site** page (**Config > Full Config > Box > Virtual Server > *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**.
7. In the **Personal License** window, configure the license.
   1. In the **Used by** field, enter the name of the user (e.g., *Test User*).
   2. In the **IP Address & Networking** section, specify these settings:
      - **Network** – The client network.
      - **Template** – The template CA template (e.g., *VPNTemplate*).
      - **ENA** – Active ENA (Exclusive Network Access) prevents access to networks the client is not directly connected to.

        VPN connections with enabled ENA setting, can only be established with VPN clients running the Barracuda Personal Firewall.
   3. In the **Password and Peer Restriction** section, click **Change Server Password** to set a server password.
   4. From the the **Active Certificate** tab:
      1. Select the server certificate from the **Certificate** list (e.g., *ServerCertificate*).
      2. Verify that the **Certificate** and **User Key** are listed as *Valid*.
      3. Click **Export to File** to export the license file. This file will be distributed to clients to authenticate when connecting to the VPN (e.g., *personal_license1.lic*).
         You can choose to enter a password to protect the file.



8. Click **OK** to save the personal license.
9. Click **Send Changes** and **Activate**.

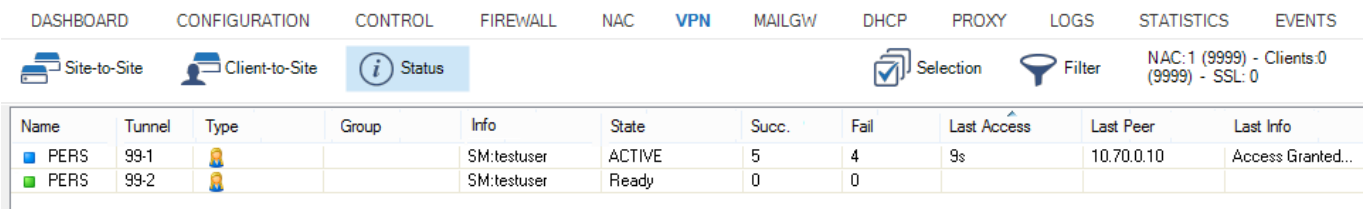
In the **Status** column next to the new personal license, a green check mark indicates that the license file can now be used on a client to connect to the VPN.

Step 4. Add Access Rules

Add two access rules to connect your client-to-site VPN to your network. For instructions, see How to Configure a Forwarding Firewall 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.

Troubleshooting

To troubleshoot VPN connections, see the `/yourVirtualServer/VPN/VPN` and `/yourVirtualServer/VPN/ike` log files. For more information on how to view log files, see Logs Tab.

Figures

1. Client2SiteVPN.png
2. ngadmin_personal_license_client_to_site.PNG
3. ngadmin_vpn_status_client_to_site.PNG