Example - Client-to-Site TINA VPN with Client Certificate Authentication

https://campus.barracuda.com/doc/96026127/

Use a client-to-site VPN to let mobile workers connect securely to your CloudGen Firewall. Each client must have a valid client certificate as well as the username and password to authenticate. The client must use the Barracuda VPN Client or CudaLaunch on Android to connect to the firewall via the TINA VPN protocol. By default, each user can have only one concurrent client-to-site VPN connection. An Advanced Remote Access subscription is required to enable concurrent client-to-site VPN sessions by the same user. 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.
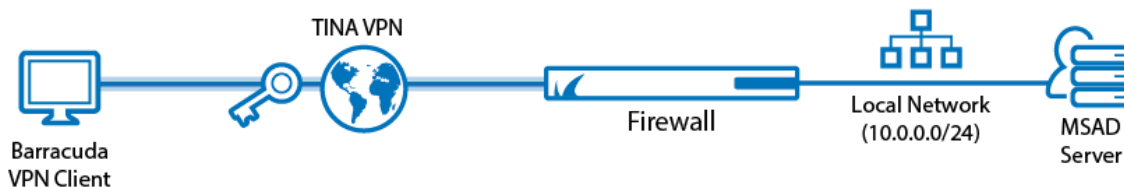
Supported VPN Clients

The following clients are supported for this client-to-site configuration:

- CudaLaunch for Android via VPN templates in SSL VPN. For more information, see How to Configure VPN Group Policies in the SSL VPN.
- VPN Client & Network Access Client

## Before You Begin

- Set up the VPN certificates for External CA. For more information, see How to Set Up External CA VPN Certificates.
- Configure an external or local authentication service. For more information, see Authentication.
- Identify the subnet and gateway address to use for the VPN service in your network (e.g., `192.168.6.0/24` and `192.168.6.254`).
- Identify the IPv4 and IPv6 addresses the VPN service is listening on. If you are using a dynamic WAN IP, see How to Configure VPN Access via a Dynamic WAN IP Address.

Step 1. Configure the VPN Service Listeners

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

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Service Properties**.
2. Click **Lock**.
3. From the **Listening IP** list, select the source for the IPv4 listeners for 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 IPs**.
5. Select an IPv6 listener from the list of configured explicit IPv6 service IP addresses.
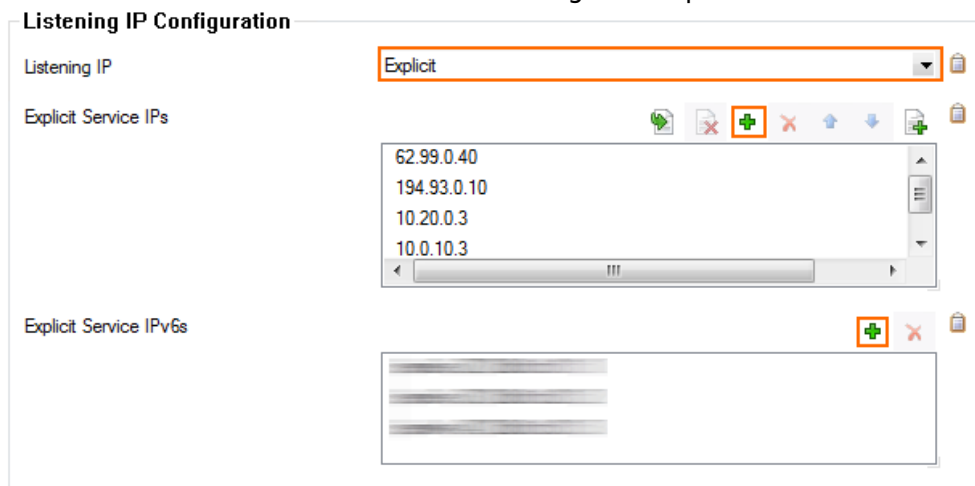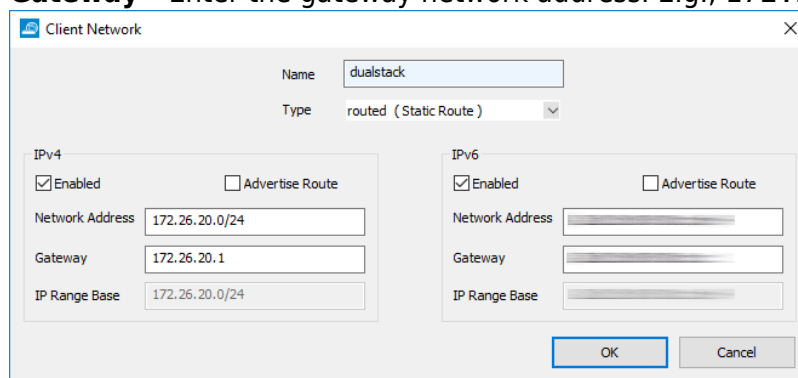

6. Click **Send Changes** and **Activate**.

Step 2. Create the VPN Client Network

All VPN clients will receive an IP address from the VPN client network with a static gateway. You can choose the gateway IP address freely from the subnet.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. Verify that the **Default Server Certificate** and **Private key** are both valid (green). If the **Default Server Certificate** and **Private key** are not valid, see How to Set Up Barracuda VPN CA VPN Certificates.
4. Configure the client network.
   1. In the left menu, select **Client Networks**.
   2. Right-click the table and select **New Client Network**. The **Client Network** window

opens.

3. In the **Client Network** window, configure the following settings either for IPv4 and/or IPv6. If IPv6 is globally disabled, the section for IPv6 is displayed in ghosted colors and cannot be enabled:
    - **Name** – Enter a descriptive name for the network.
    - **Type** – Select **routed (Static Route)**. VPN clients are assigned an address via DHCP (fixed or dynamic) in a separate network reserved for the VPN. A static route on the firewall leads to the local network.
    - **Network Address** – Enter the base network address for the VPN clients. E.g., `172.26.20.0/24`
    - **Gateway** – Enter the gateway network address. E.g., `172.26.20.1`

5. Click **OK**.
6. Upload the root certificate:
    1. In the left menu, select **Root Certificates**.
    2. Right-click the table and select **Import CER from File** or **Import PEM from File**. The **Root Certificate** window opens.
    3. Enter the **Name** for the root certificate.
    4. In the **Usage** section, select **Barracuda Personal**.
    5. (optional) Click the **Certificate revocation** tab to configure a CRL host.
    6. (optional) Click the **OCSP** tab to configure an OCSP server. For more information, see [How to Configure OCSP Validation](#).
    7. Click **OK**.
7. Upload the service key:
    1. In the left menu, select **Service Keys**.
    2. Right-click the table and select **Import from File**.
    3. Enter a **Name**.
    4. Click **OK**.
8. Click **Send Changes** and **Activate**.

Step 3. Configure VPN Group Match Settings

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Client to Site**.
2. Click **Lock**.

3. Click the **External CA** tab.
4. Click the **Click here for options** link. The **Group VPN Settings** window opens.
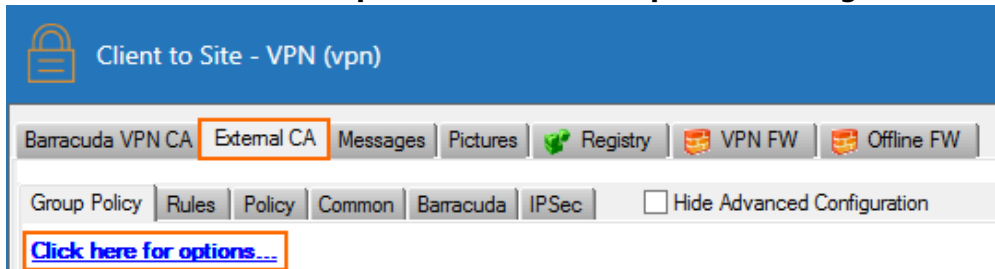
5. In the **Group VPN Settings** window, configure the following settings:
    1. In the **X509 Client Security** section, select **X509 Certificate**. This will force all users connecting to this firewall, regardless of the group policy, to use client certificate authentication.

        Selecting mandatory client credentials forces all group policies configured on the firewall to comply to these client security settings. If in doubt, leave these settings unchecked.
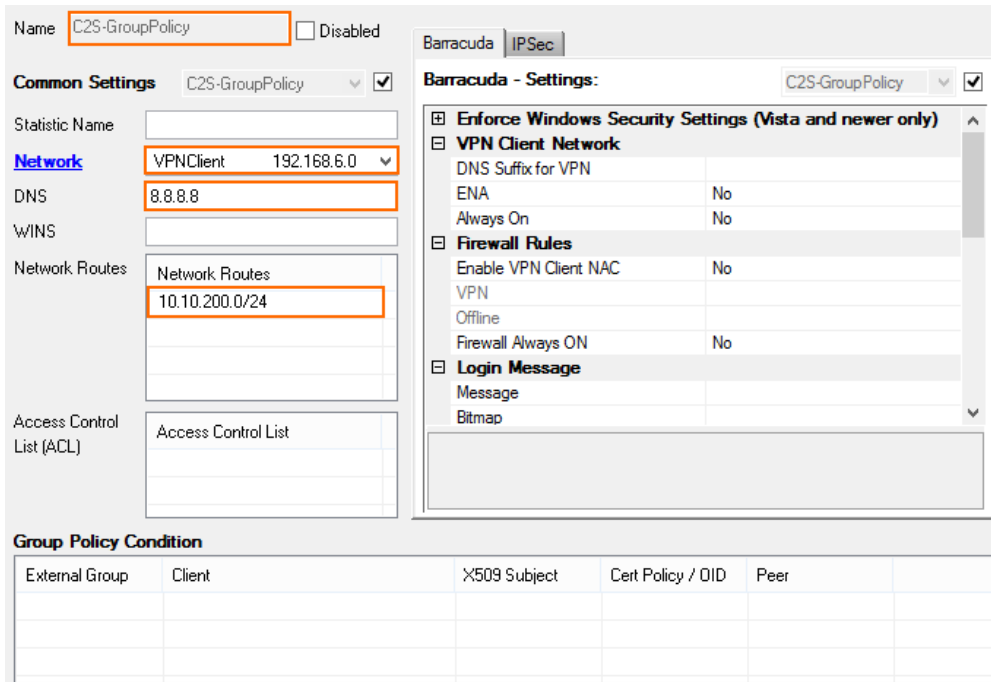
    2. In the **Server** section, select the **Authentication Scheme**:
        - **Default Authentication Scheme** – The default authentication scheme is used for all VPN group policies.
        - **Extract from username** – The authentication scheme is appended to the username. The authentication scheme with the appended name is used with the default authentication scheme acting as a fallback if the authentication scheme name is not present on the firewall. E.g., `user1@msad1` or `user2@domain.com@HQldap`.
    3. (optional) To allow only one root certificate to be used for all group policies on this firewall, select the certificate from the **Used Root Certificates** list.
    4. Select which X.509 certificate field is to be verified by the **Authentication Scheme** selected above. Typically, this is the **emailAddress**, or username in the **Subject**.

6. Click **OK**.
7. Click **Send Changes** and **Activate**.
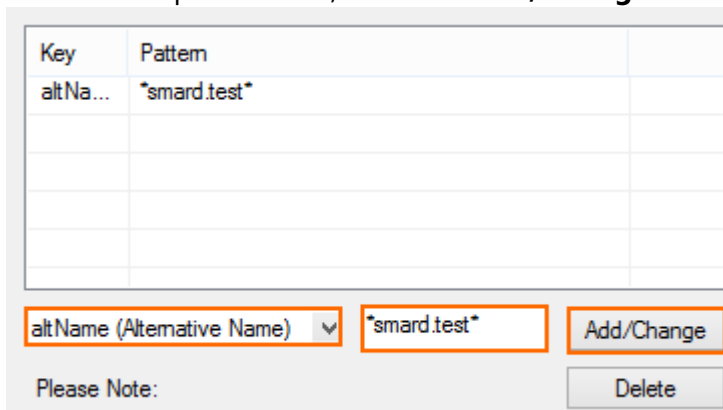
Step 4. Create a VPN Group Policy

The VPN group policy specifies the network IPsec settings and defines the conditions to be met by the client certificate.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Client to Site**.
2. Click **Lock**.
3. Click the **External CA** tab and then click the **Group Policy** tab.
4. Right-click the table and select **New Group Policy**. The **Edit Group Policy** window opens.
5. Enter a name for the **Group Policy**.
6. From the **Network** list, select the VPN client network.
7. In the **Network Routes** table, enter the network that must be reachable through the VPN connection. For example, `10.10.200.0/24`

   To route all traffic through the client-to-site VPN tunnel, add a `0.0.0.0/0` network route.

8. Configure the group policy conditions. Only clients matching these conditions are allowed to connect through this group policy.
    1. Right-click the **Group Policy Condition** table and select **New Rule**. The **Group Policy Condition** window opens.
    2. (optional) In the **Group Pattern** field, define the groups on the authentication server that will be assigned the policy. E.g.: CN=vpnusers*
    3. In the **X509 Certificate Conditions** section, click **Edit/Show**. The **Certificate Condition** window opens.
        1. For each certificate condition, select the certificate field from the drop-down list, enter the required value, and click **Add/Change**.

        2. Click **OK**.
    4. (optional) Enter an OID in the **Certificate Policy** to allow only certificates with a specific **Key Usage**. E.g., Client Authentication (1.3.6.1.5.5.7.3.2)
    5. In the **Peer Condition** section, verify that **Barracuda Client** check box is selected.
    6. In the **X509 Certificate Conditions** section, enter matching conditions for the X.509 client certificates.
9. Click **OK**.

10. Click **OK**.
11. Click **Send Changes** and **Activate**.

Step 5. Add Access Rules

Add an access rule to allow traffic from your client-to-site VPN to your network. For more information, 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. Clients authenticated via client certificate use a **Name** in the following format: *<GroupPolicy name>-<certificate serial number>-<username>*.

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 /VPN/VPN and /Box/Control/AuthService log files. For more information, see LOGS Tab.

Next Step

Configure the VPN client to connect to this VPN profile. For more information, see Remote Access Clients.

Figures

1. Client2SiteTINA_CertsVPN.png
2. vpn_service_listeners.png
3. client_network_config.png
4. PSK04.png
5. X509_1.png
6. PSK06.png
7. X509_03.png
8. X509_02.png
9. X509_04.png