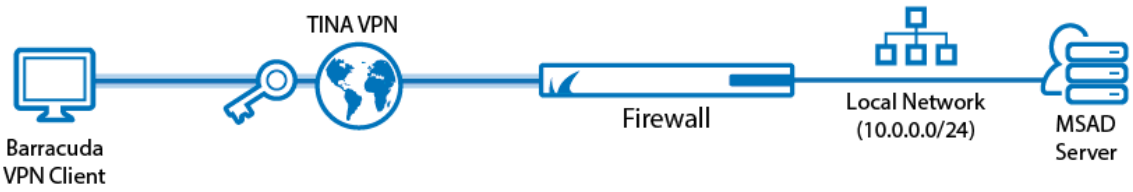
Example - Client-to-Site TINA VPN with MSAD Authentication

https://campus.barracuda.com/doc/91984714/

Use a client-to-site VPN to let mobile workers connect securely to your CloudGen Firewall. Each client must have a valid username and password to authenticate. The client must use the Barracuda VPN Client 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.

For a video description, see also https://campus.barracuda.com/video/play/13KM/client-to-site-tina-vpn-with-msad-hands-on-demo/.



Supported VPN Clients

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

- VPN Client & Network Access Client

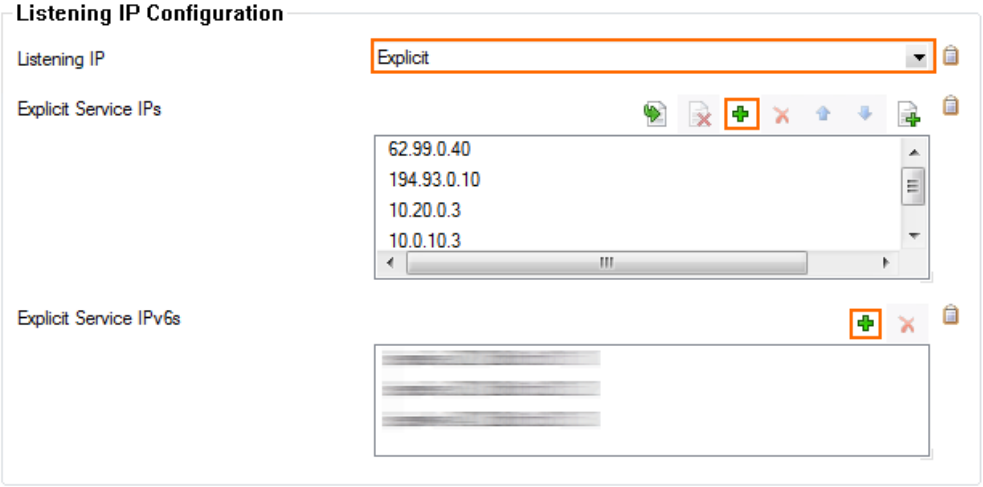
Before You Begin

- Configure MSAD authentication. For more information, see How to Configure MSAD 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.

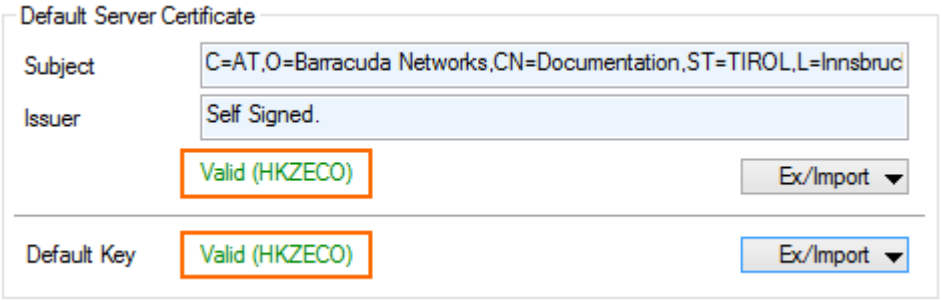


6. Click **Send Changes** and **Activate**.

Step 2. Create the VPN Client Network

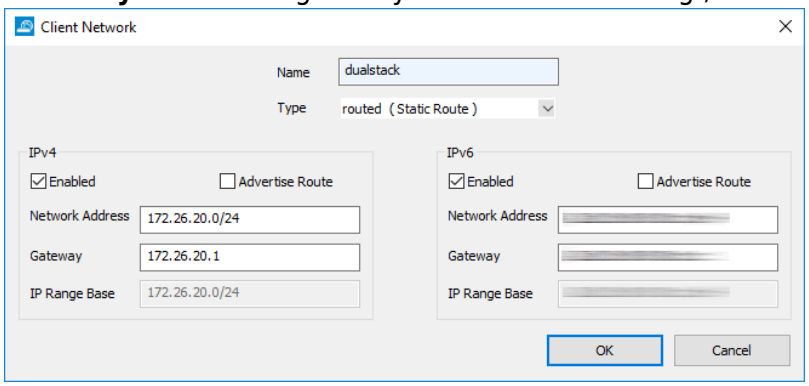
All VPN clients will receive an IP address from the VPN client network with a static gateway. You can choose the gateway IP address freely from the subnet.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. Verify that the default server certificate and 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 Barracuda VPN CA VPN Certificates.



3. Click **OK** to close the **Server Settings** window.

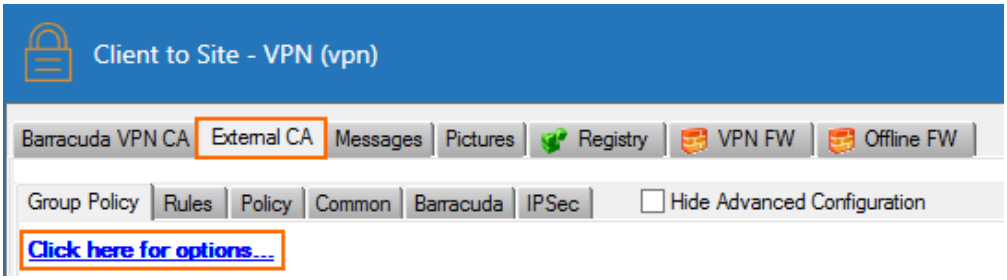
4. Configure the client network.
   1. Click the **Client Networks** tab.
   2. Right-click the table and select **New Client Network**. The **Client Network** window opens.
   3. In the **Client Network** window, configure the following settings either for IPv4 and/or IPv6. If IPv6 is globally disabled, 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`



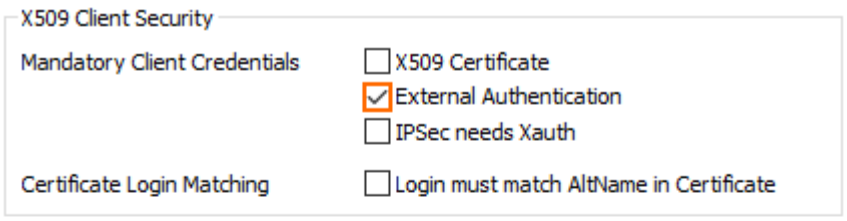
5. Click **OK**.
6. Click **Send Changes** and **Activate**.

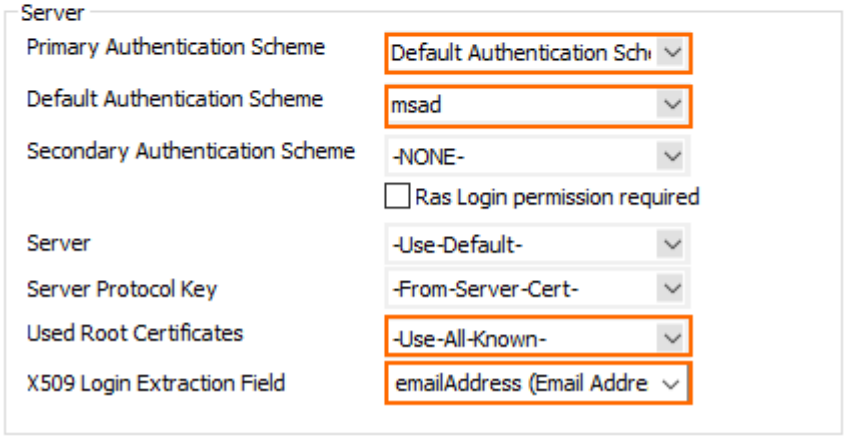
Step 3. Configure VPN Group Match Settings

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 **External Authentication**.
   2. For **Default Authentication Scheme**, select **msad**.





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

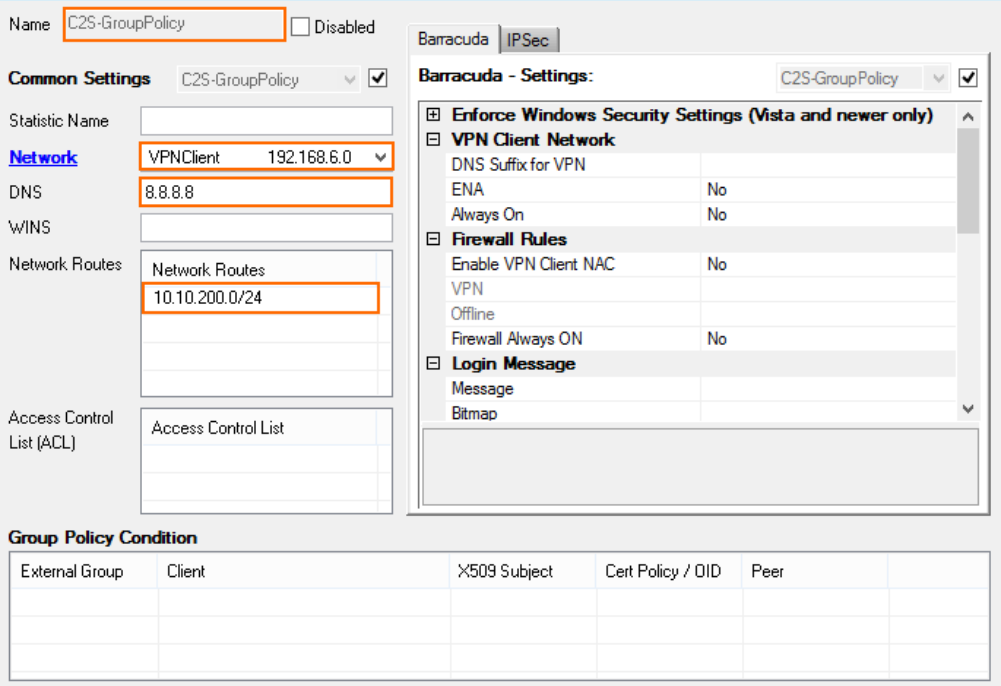
Step 4. Create a VPN Group Policy

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

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

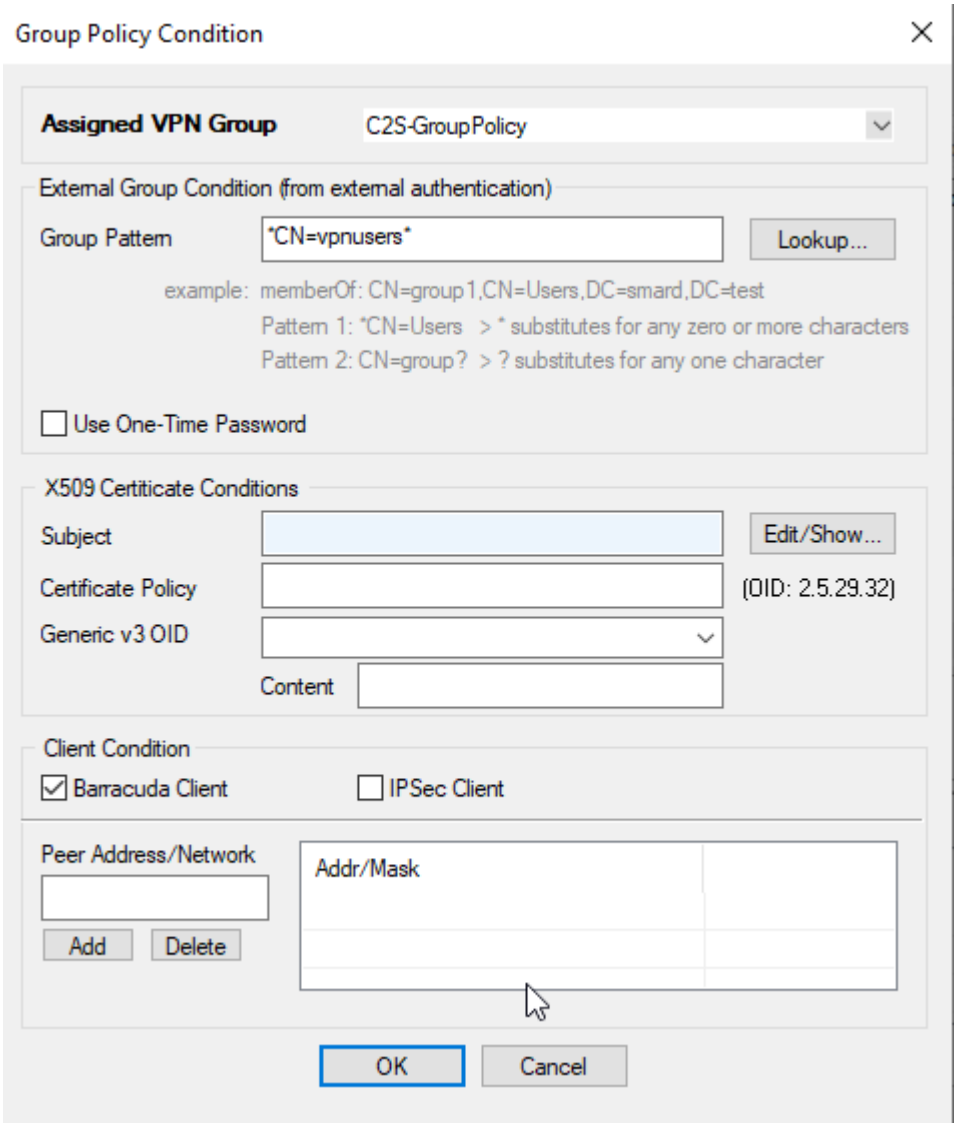
3. Click the **External CA** tab and then click the **Group Policy** tab.
4. Right-click the table and select **New Group Policy**. The **Edit Group Policy** window opens.
5. Enter a name for the **Group Policy**.
6. From the **Network** list, select the VPN client network.
7. In the **Network Routes** 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. In the **Group Pattern** field, define the groups on the authentication server that will be assigned the policy. E.g.: `CN=vpnusers*`

      Use the * as a wildcard if you want the user to be part of all groups and to have access to all resources.
9. Click **OK**.



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

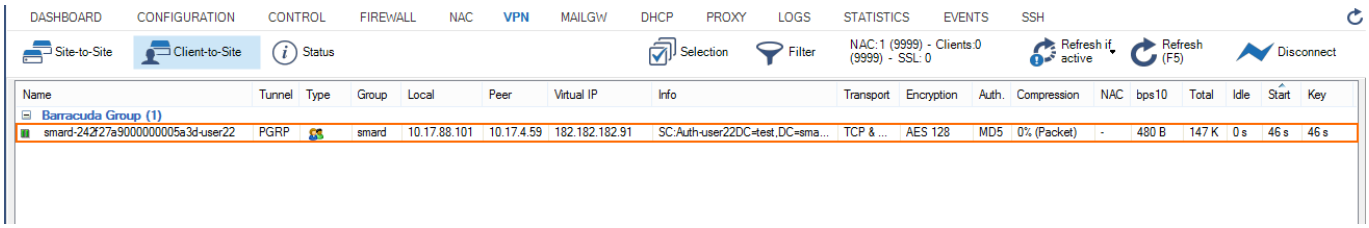
Step 5. Add Access Rules

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: *<root certificate name>-<certificate serial*

number>-<*username*>. Depending on the length of individual values (e.g., long certificate serial numbers or usernames), the displayed **Name** might also get truncated.



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.
- **Gray** – 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