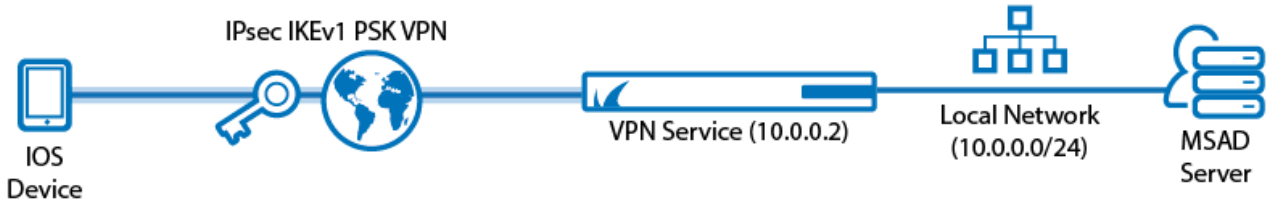
Example - Client-to-Site IKEv1 IPsec VPN with PSK

https://campus.barracuda.com/doc/17373/

To let users access a client-to-site IPsec VPN without having to install X.509 certificates on their client devices, you can create an IPsec client-to-site VPN group policy using a pre-shared key (PSK). For users with mobile devices that are not managed by a mobile device management platform (MDM), using a PSK is more convenient than having to install client certificates for authentication. To allow multiple concurrent client-to-site connections for a single user, an Advanced Remote Access subscription is required. 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.



Supported VPN Clients

Although any standard-compliant IPsec client should be able to connect via IPsec, Barracuda Networks recommends using to the following clients:

- CudaLaunch via VPN templates in SSL VPN. For more information, see How to Configure VPN Group Policies in the SSL VPN.
- Native iOS IPsec VPN Client

Starting with version 12, Android no longer supports IKEv1. For installation using IKEv2, see Native Android IPsec VPN Client.

Before You Begin

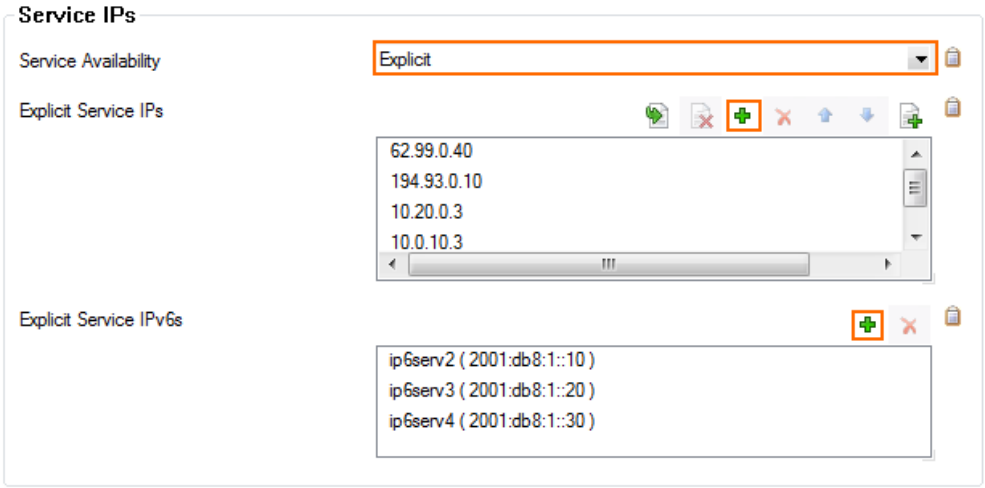
- Set up the VPN certificates for External CA. For more information, see How to Set Up External CA VPN Certificates.
- Configure an external or local authentication service. For more information, see Authentication.
- Identify the subnet (static route) or a range in a local network (proxy ARP) to be used for the VPN clients.
- Identify the IPv4 and IPv6 addresses the VPN service is listening on. If you are using a dynamic

IPv4 WAN, 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.

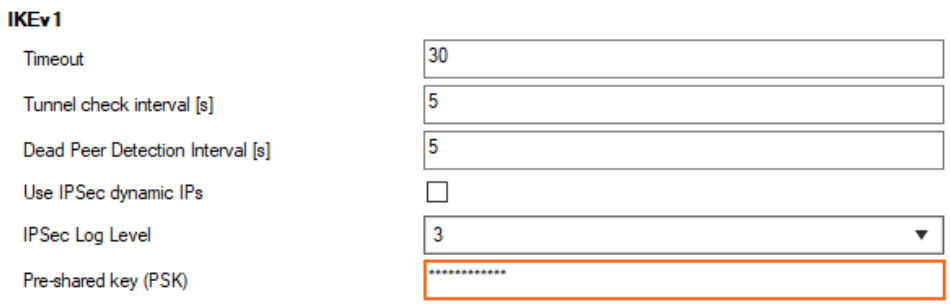
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Service Properties**.
2. Click **Lock**.
3. From the **Service Availability** list, select the source for the IPv4 listeners of the VPN service.
   - When selecting **Explicit**, click **+** for each IP address and 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.



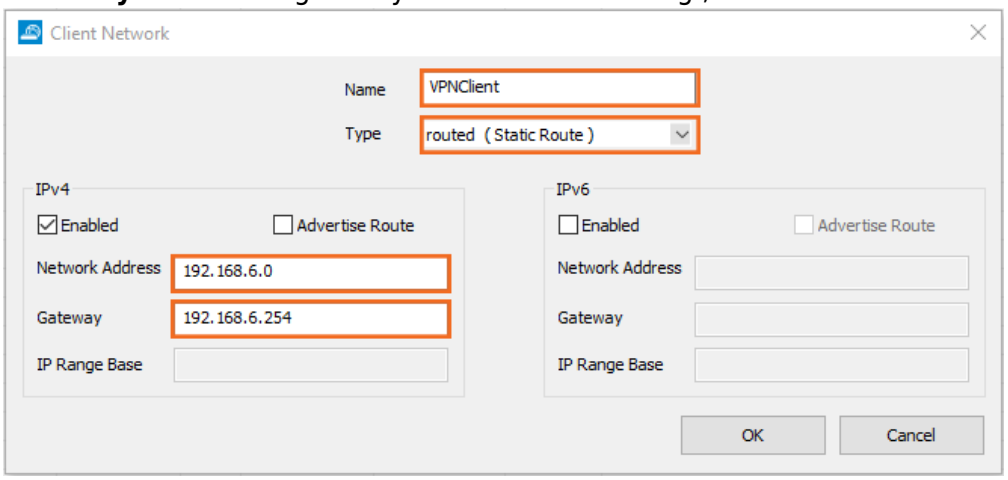
6. Click **Send Changes** and **Activate**.

Step 2. Configure the Client Network, Gateway, and PSK Key

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > 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. In the left menu, select **IPSec**.
5. In the **IKEv1** section, enter the **Pre-shared key**. E.g., `pre$haredKey`



6. 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:
      - **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., `192.168.6.0`
      - **Gateway** – Enter the gateway network address. E.g., `192.168.6.254`



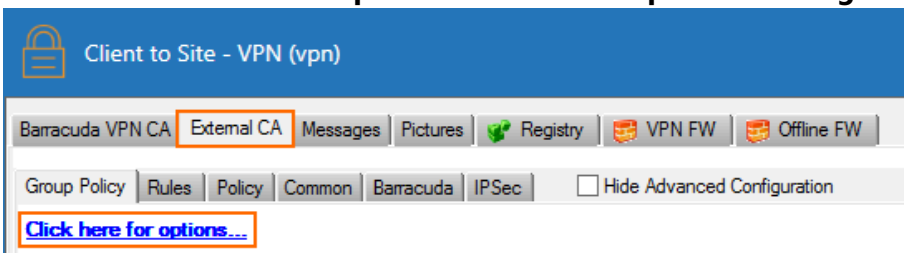
7. Click **OK**.
8. Click **Send Changes** and **Activate**.

Step 3. Configure VPN Group Match Settings

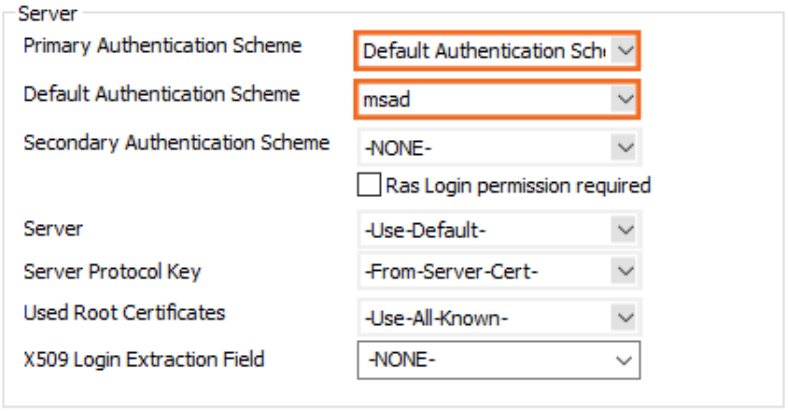
Configure the global authentication settings for VPN tunnels using an external X.509 certificate and group configurations.

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. 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`.
6. Select the **Default Authentication Scheme** from the drop-down list. This authentication scheme must be configured on box level of the firewall.



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

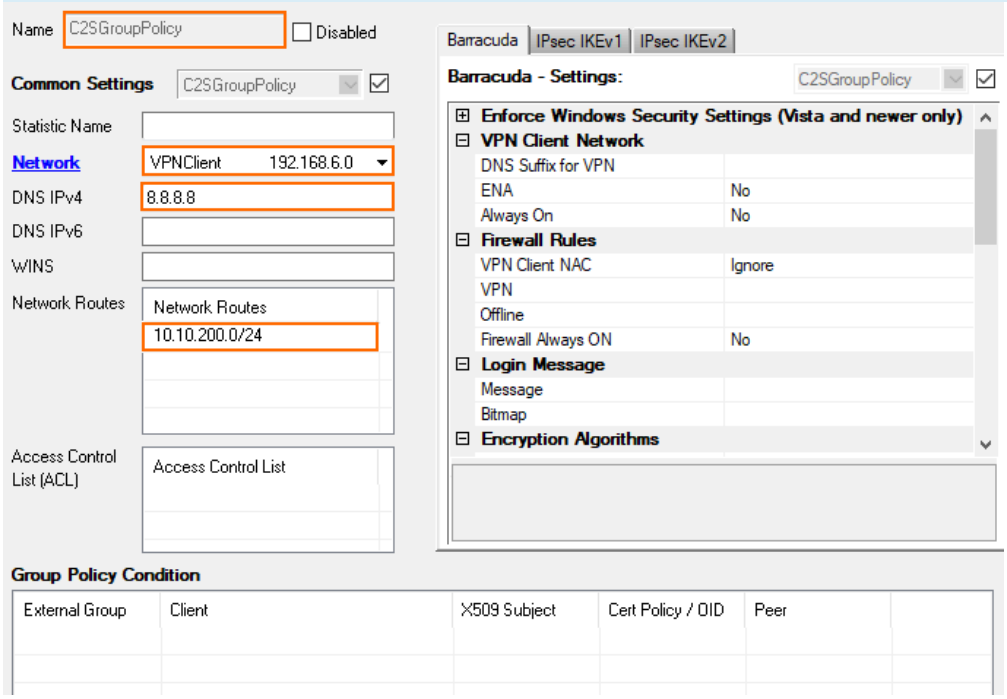
Step 4. Create a VPN Group Policy

The **VPN Group Policy** specifies the network IPsec settings. You can create group patterns to require users to meet certain criteria, as provided by the group membership of the external authentication server (e.g., `CN=vpnusers*`). You can also define conditions to be met by the certificate (e.g., `O(Organization)` must be the company name).

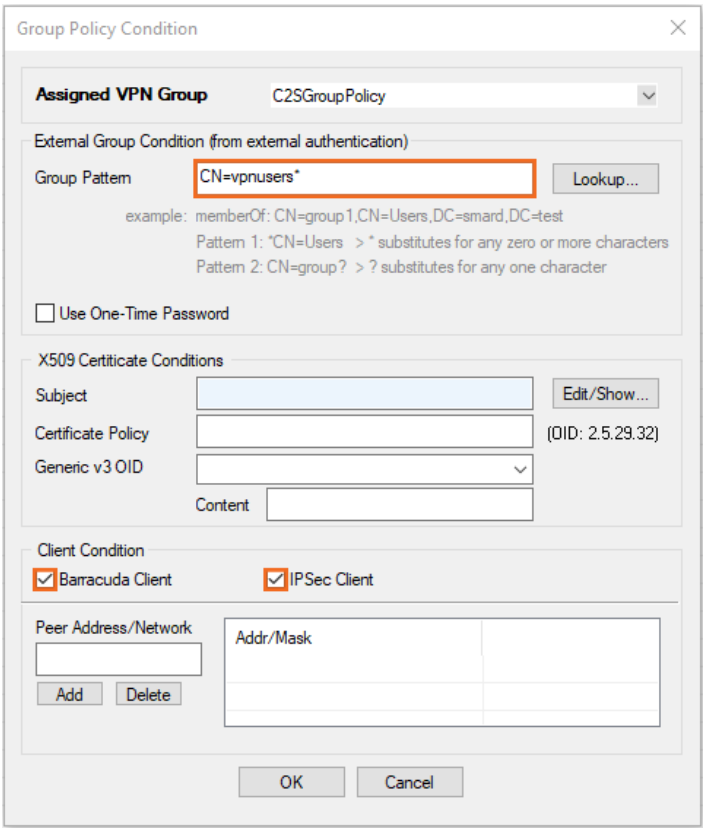
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Client to Site**.
2. Click **Lock**.
3. Click the **External CA** tab, and then click the **Group Policy** tab.

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`

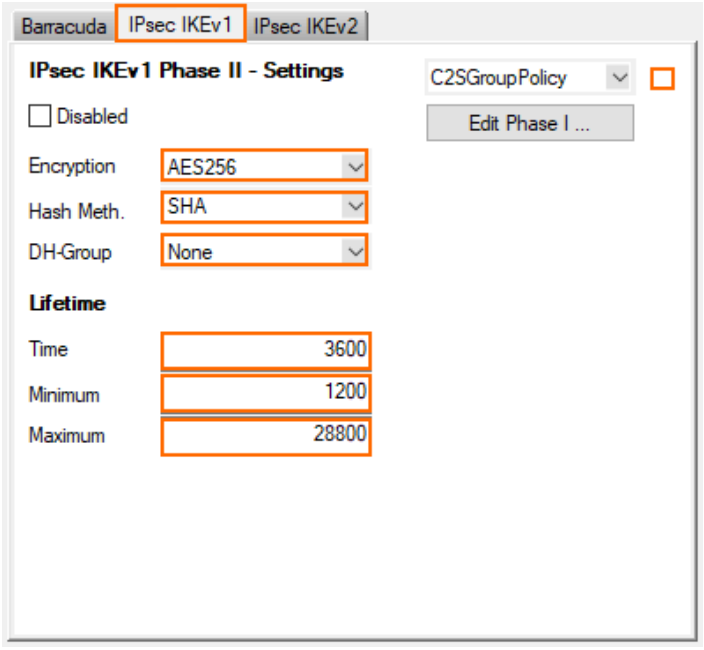
   To route all traffic through the client-to-site VPN tunnel, add a `0.0.0.0/0` network route.



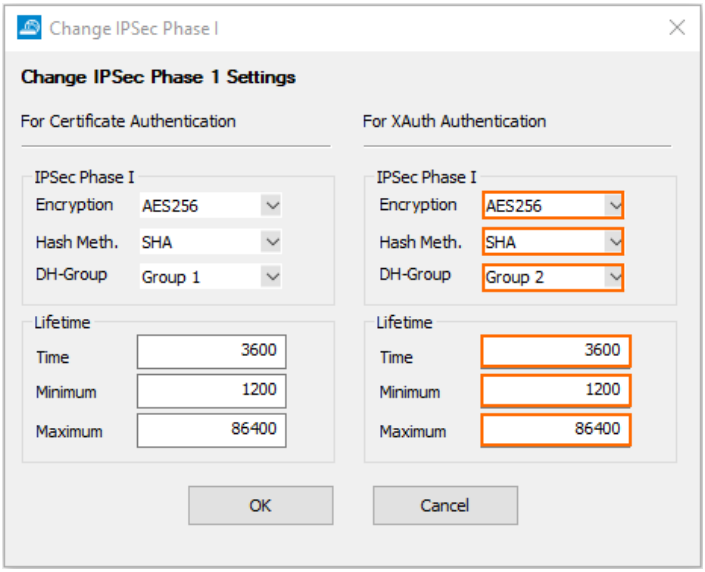
8. Configure the group policy.
   1. Right-click the **Group Policy Condition** table and select **New Rule**. The **Group Policy Condition** window opens.
   2. In the **Group Pattern** field, define the groups that will be assigned the policy. E.g., `CN=vpnusers*`
   3. In the **Peer Condition** section, verify that **IPsec Client** check box is selected.
   4. To use this group policy for SSL-VPN VPN template resources and CudaLaunch, enable **Barracuda Client**.
   5. Click **OK**.



9. Configure the encryption and hashing settings:
    1. Click the **IPSec** tab.
    2. Clear the check box in the top-right corner.
    3. From the **IPsec Phase II - Settings** list, select the entry that includes **(Create New)** in its name. For example, if you choose *Group Policy* as a name, the entry name is *Group Policy (Create new).*
    4. Set the following encryption algorithm settings for Phase II:
        - **Encryption** – Select **AES256**.
        - **Hash Meth.** – Select **SHA**.
        - **DH-Group** – Select **None**.
        - **Time** – Enter `3600`
        - **Minimum** – Enter `1200`
        - **Maximum** – Enter `28800`



5. Click **Edit IPsec Phase I** and select the encryption algorithm in the **For XAuth Authentication** section:
   - **Encryption** – Select **AES256**.
   - **Hash Meth.** – Select **SHA**.
   - **DH-Group** – Select **Group2**.
   - **Time** – Enter `3600`
   - **Minimum** – Enter `1200`
   - **Maximum** – Enter `86400`



6. Click **OK**.

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

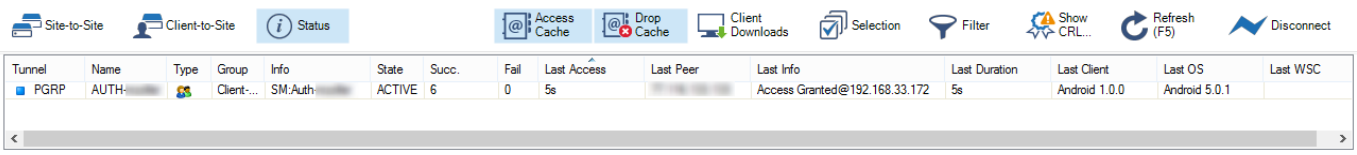
Step 5. Add Access Rules

Add two access rules to connect 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.



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 not in use.
- **Grey** – The VPN tunnel is 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 `/VPN/ike` log files. For more information, see LOGS Tab.

Next Steps

Configure the remote access clients to connect to the client-to-site VPN.

For more information, see Remote Access Clients.

Figures

1. Client2SiteIPsecXAUTHPSKVPN-01.png
2. vpn_service_listeners.png
3. PSK02.png
4. PSK03a.png
5. PSK04.png
6. PSK05v2.png
7. PSK06.png
8. PSK07.png
9. C2S_00.png
10. C2S_01.png
11. C2S_status_connected.png