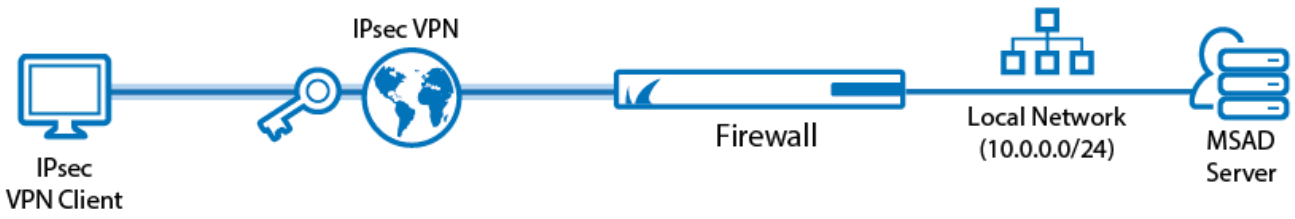
Example - Client-to-Site IKEv1 IPsec VPN with Client Certificate Authentication

https://campus.barracuda.com/doc/73719146/

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. Use CudaLaunch on iOS and Android to fully manage the VPN configuration remotely through the SSL VPN templates. To manually configure the native IPsec clients on iOS and Android, verify that you are using encryption settings compatible with the the version of your mobile operating system. By default, each user can have only one concurrent client-to-site VPN connection. An Advanced Remote Access subscription is required to enable multiple 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

Although any standard-compliant IPsec client should be able to connect via IPsec, Barracuda Networks recommends using 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
- Native Android IPsec VPN Client

Before You Begin

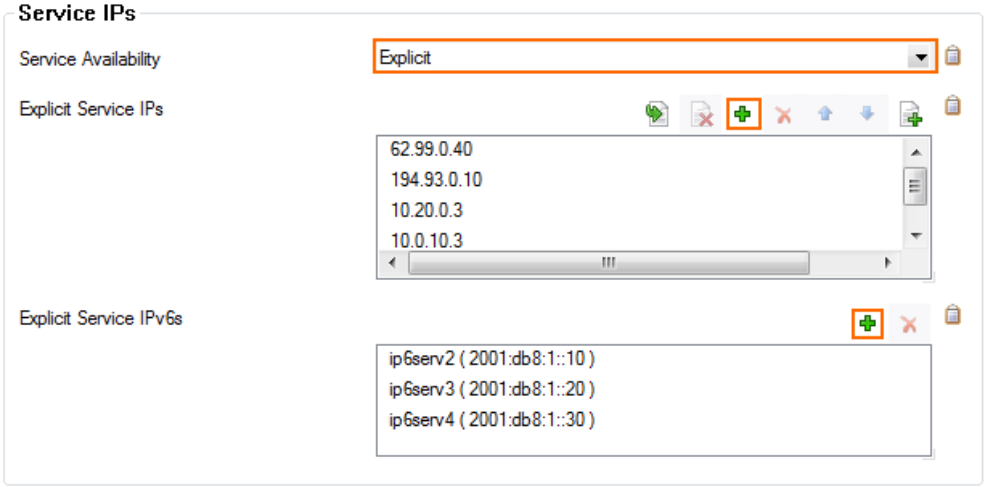
- Verify that the **server** and **default certificates** are installed and use DNS: *FQDN (e.g., DNS:vpn.mydomain.com*) as the **SubAltName**. This is necessary for iOS and Android devices to able to connect. The FQDN must resolve to the IP address the VPN service is listening on. For more information, 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 IP address 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 > Virtual Server > your virtual server > Assigned Services > VPN > Service Properties**.
2. Click **Lock**.
3. From the **Service Availability** list, select the source for the IPv4 listeners:
   - **First+Second-IP** – The VPN service listens on the first and second virtual server IPv4 address.
   - **First-IP** – The VPN service listens on the first virtual server IPv4 address.
   - **Second-IP** – The VPN service listens on the second virtual server IPv4 address.
   - **Explicit** – For each IP address, click **+** 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 virtual server IP addresses.

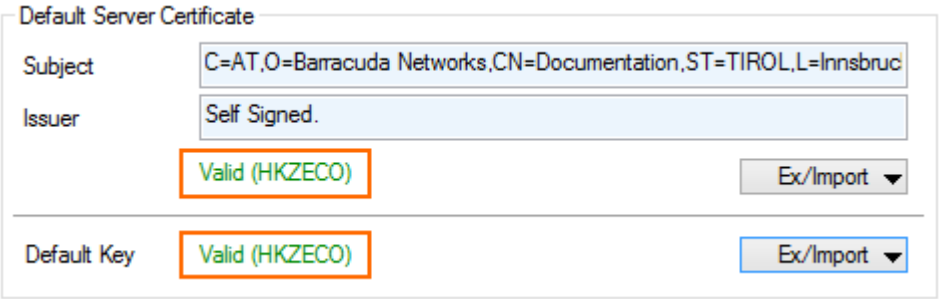


6. Click **Send Changes** and **Activate**.

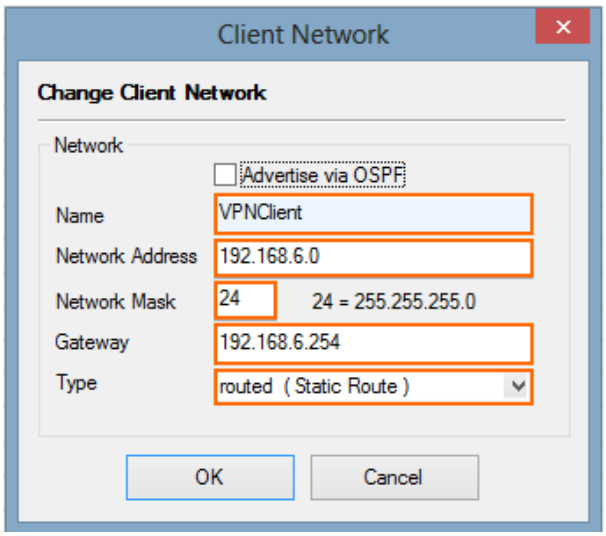
Step 2. Create the VPN Client Network

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 > 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 .



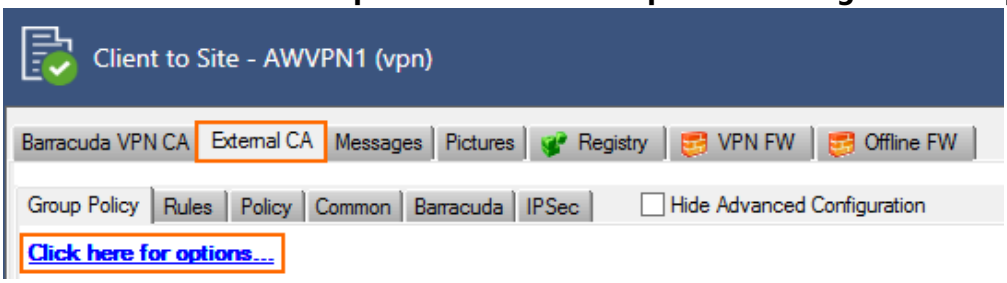
   3. Click **OK** to close the **Server Settings** window.
4. Configure the client network.
   1. Click the **Client Networks** tab.
   2. Right-click the table and select **New Client Network**. The **Client Network** window opens.
   3. In the **Client Network** window, configure the following settings:
      - **Name** – Enter a descriptive name for the network.
      - **Network Address** – Enter the base network address for the VPN clients.
      - **Network Mask** – Enter the subnet mask for the VPN client network.
      - **Gateway** – Enter the gateway network address.
      - **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.



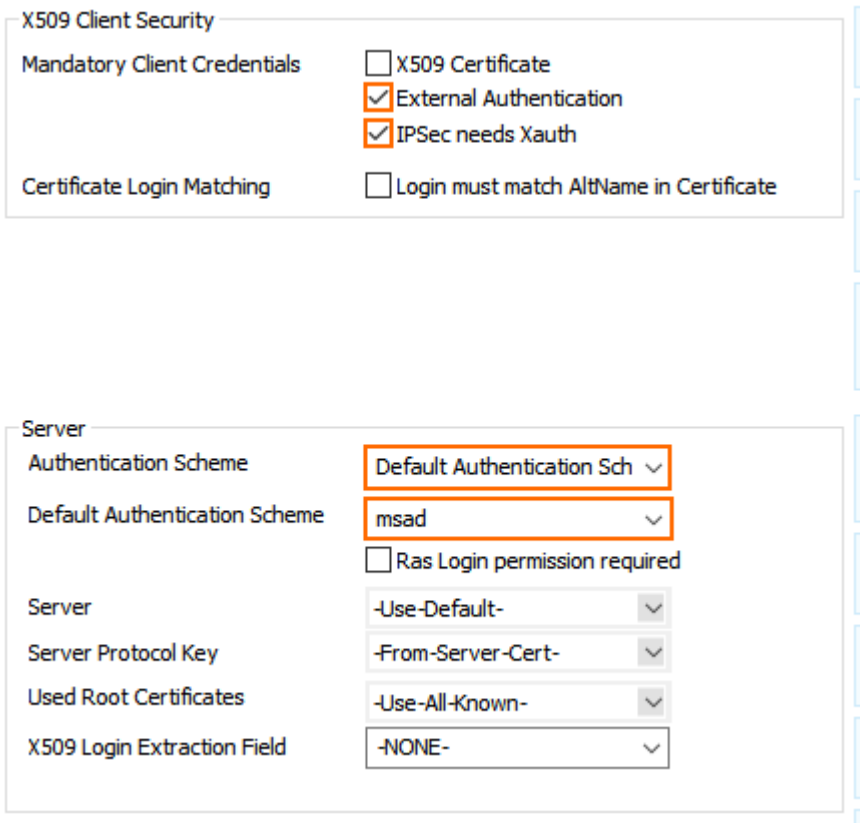
5. Click **OK**.
6. Click **Send Changes** and then click **Activate**.

Step 3. Configure VPN Group Match Settings

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



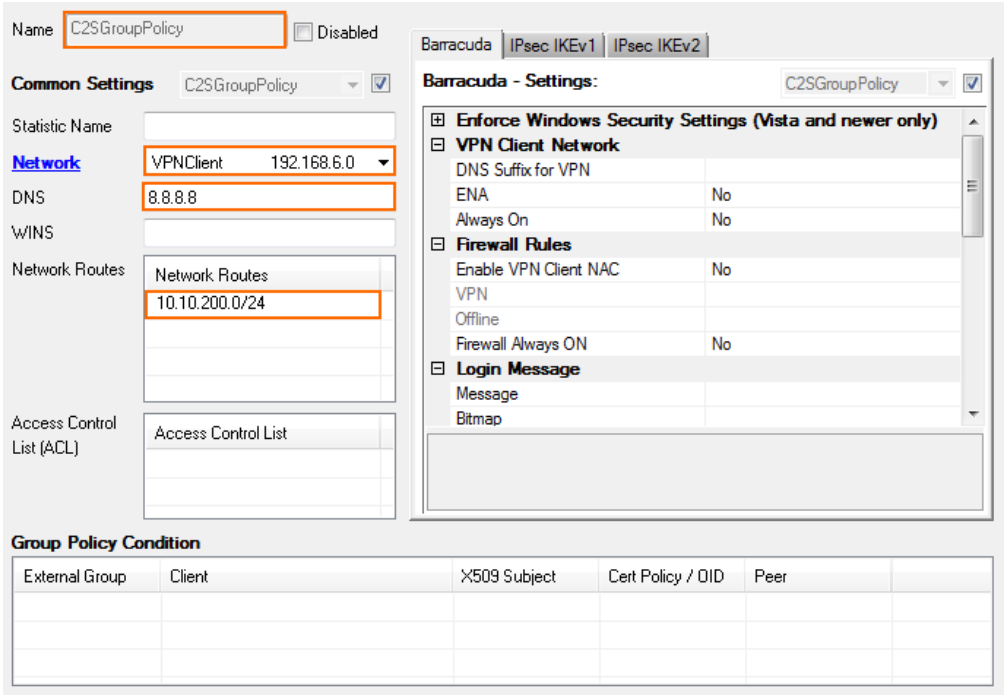
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Step 4. Create a VPN Group Policy

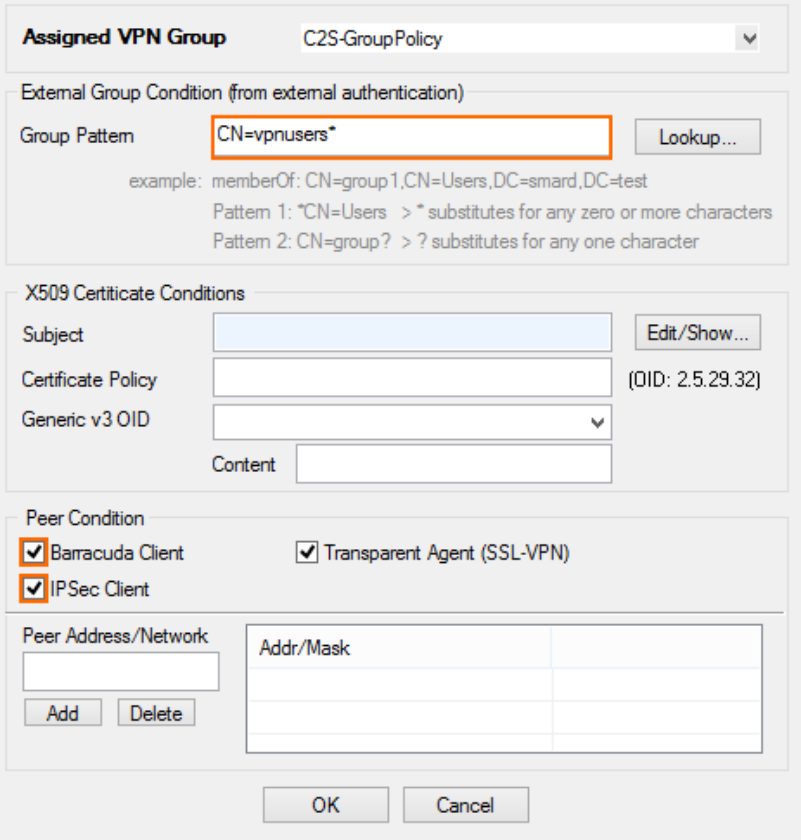
The VPN group policy specifies the network IPsec settings. You can group patterns to require users to meet certain criteria, as provided by the group membership of the external authentication server (e.g., `CN=vpnusers*`). You can also define conditions to be met by the certificate (e.g., `O(Organization)`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

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > 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`

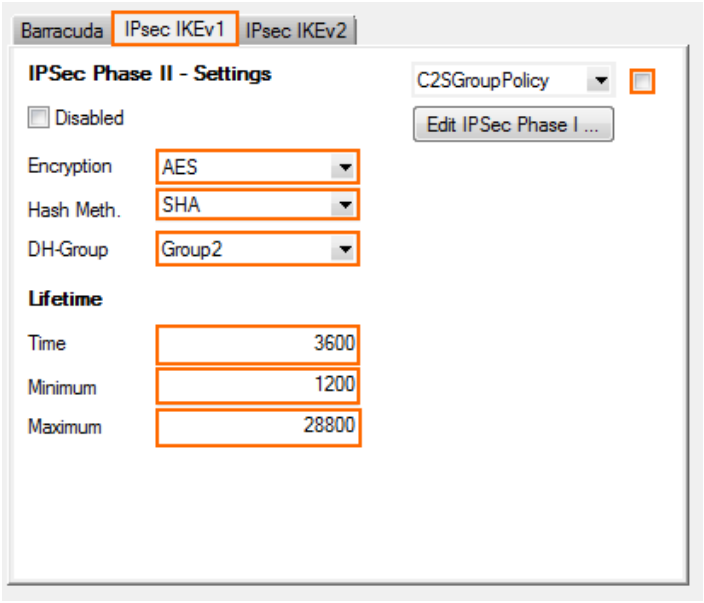
   To route all traffic through the client-to-site VPN tunnel, add a `0.0.0.0/0` network route.



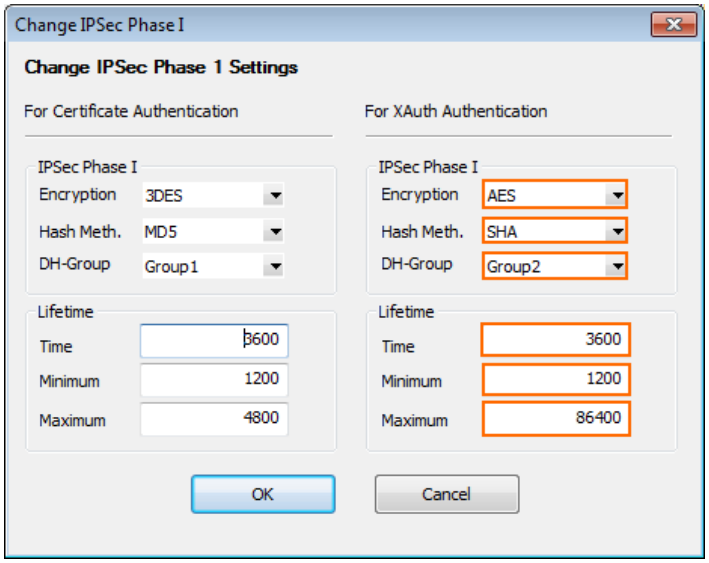
8. Configure the group policy.
    1. Right-click the **Group Policy Condition** table and select **New Rule**. The **Group Policy Condition** window opens.
    2. In the **Group Pattern** field, define the groups that will be assigned the policy. E.g., `CN=vpnusers*`
    3. In the **Peer Condition** section, verify that **IPsec Client** check box is selected.
    4. In the **X509 Certificate Conditions** section, enter matching conditions for the X.509 client certificates.
9. Click **OK**.



10. Configure the encryption and hashing settings:
    1. Click the **IPSec IKEv1** 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 **AES** .
        - **Hash Meth.** – Select **SHA** .
        - **DH-Group** – Select **Group2**.
        - **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 **AES.**
   - **Hash Meth.** – Select **SHA** .
   - **DH-Group** – Select **Group2**.
   - **Time** – Enter 3600
   - **Minimum** – Enter 1200
   - **Maximum** – Enter 86400



6. Click **OK** .

11. Click **Send Changes** and then click **Activate**.

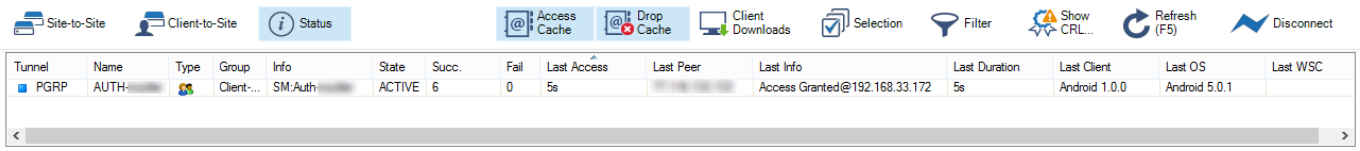
Step 5. Add Access Rules

Add an access rule 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 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, 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. Client2SiteIPsec_VPN.png
2. vpn_service_listeners.png
3. PSK01.png
4. PSK03.png
5. PSK04.png
6. PSK05.png
7. PSK06.png
8. PSK07.png
9. C2S_00.png
10. C2S_01.png
11. C2S_status_connected.png