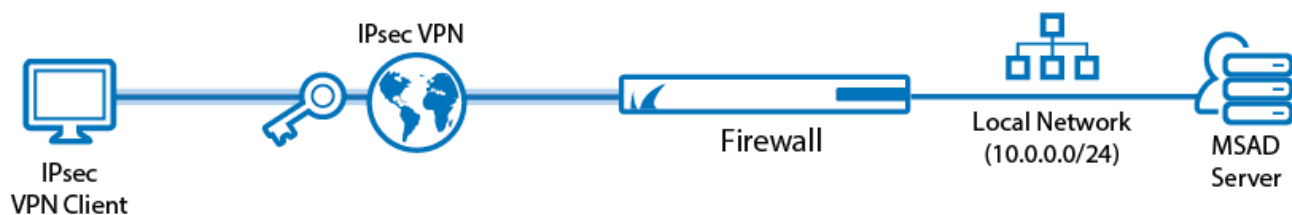


## Example - Client-to-Site IKEv1 IPsec VPN with Client Certificate Authentication

<https://campus.barracuda.com/doc/96026124/>

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 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

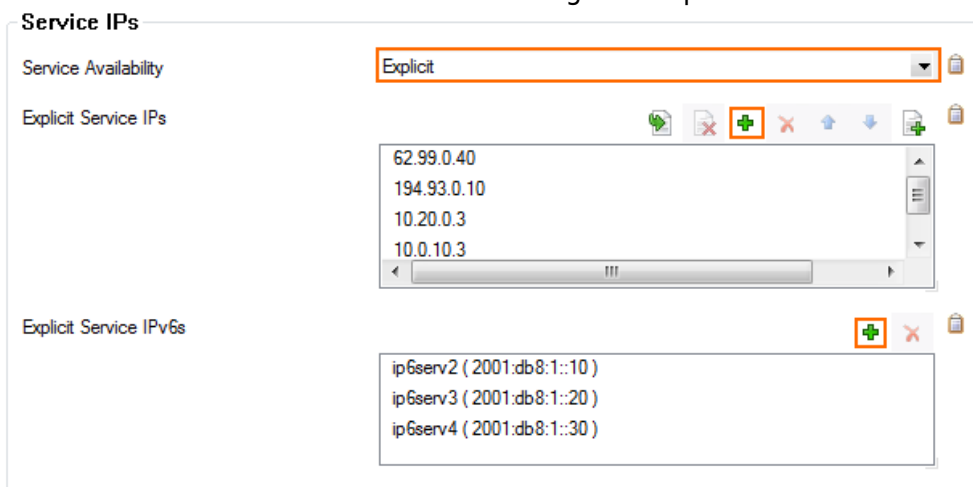
- Verify that the **server** and **default certificates** are installed and use DNS: *FQDN* (e.g., *DNS:vpn.mydomain.com*) as the **SubAltName**. This is necessary for iOS and Android devices to be able to connect. The FQDN must resolve to the IP address the VPN service is listening on. For more information, 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 > 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.



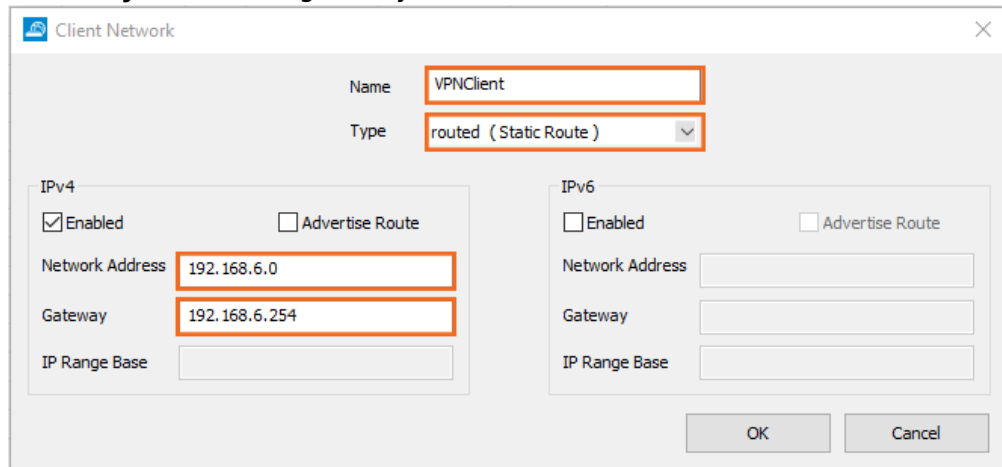
6. Click **Send Changes** and **Activate**.

## Step 2. 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**.

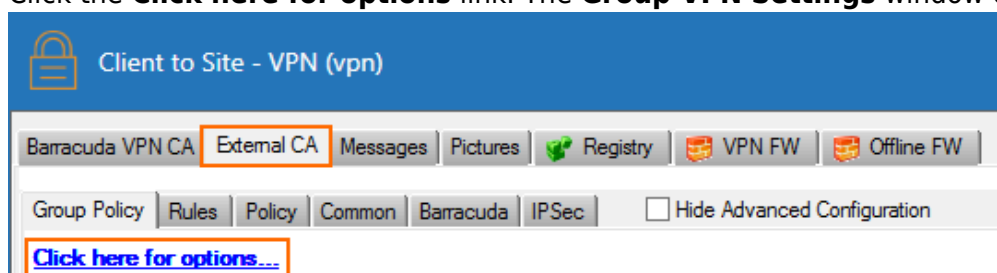
3. Verify that the **Default Server Certificate** and **Private key** are both valid (green). If the **Default Server Certificate** and **Private key** are not valid, see [How to Set Up Barracuda VPN CA VPN Certificates](#).
4. Configure the client network.
  1. In the left menu, select **Client Networks**.
  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:
    - **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.
    - **Gateway** – Enter the gateway network address.



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

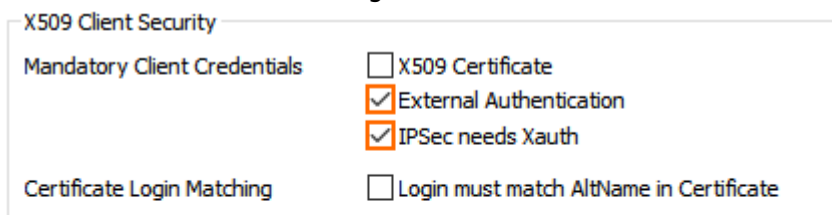
### Step 3. Configure VPN Group Match Settings

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.



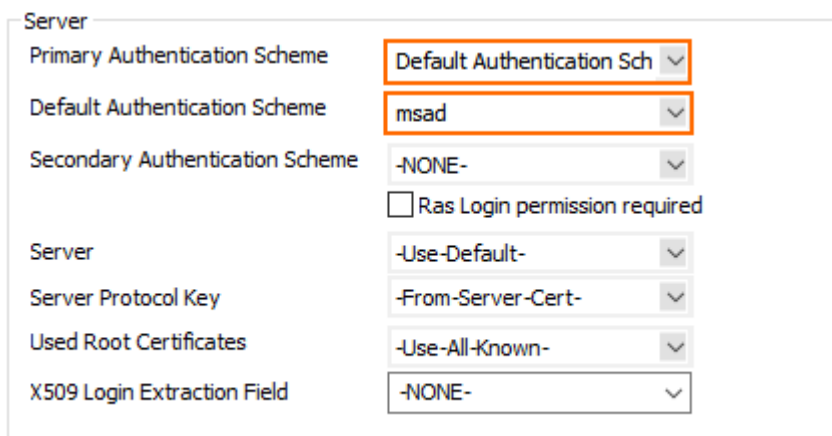
5. In the **Group VPN Settings** window, configure the following settings:

1. In the **X509 Client Security** section, select 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@HQ1dap.
3. Select the **Default Authentication Scheme** from the drop-down list. This authentication scheme must be configured on box level of the firewall.



X509 Client Security

Mandatory Client Credentials	<input type="checkbox"/> X509 Certificate
	<input checked="" type="checkbox"/> External Authentication
	<input checked="" type="checkbox"/> IPsec needs Xauth
Certificate Login Matching	<input type="checkbox"/> Login must match AltName in Certificate



Server

Primary Authentication Scheme	Default Authentication Sch
Default Authentication Scheme	msad
Secondary Authentication Scheme	-NONE-
	<input type="checkbox"/> Ras Login permission required
Server	-Use-Default-
Server Protocol Key	-From-Server-Cert-
Used Root Certificates	-Use-All-Known-
X509 Login Extraction Field	-NONE-

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

## Step 4. Create a VPN Group Policy

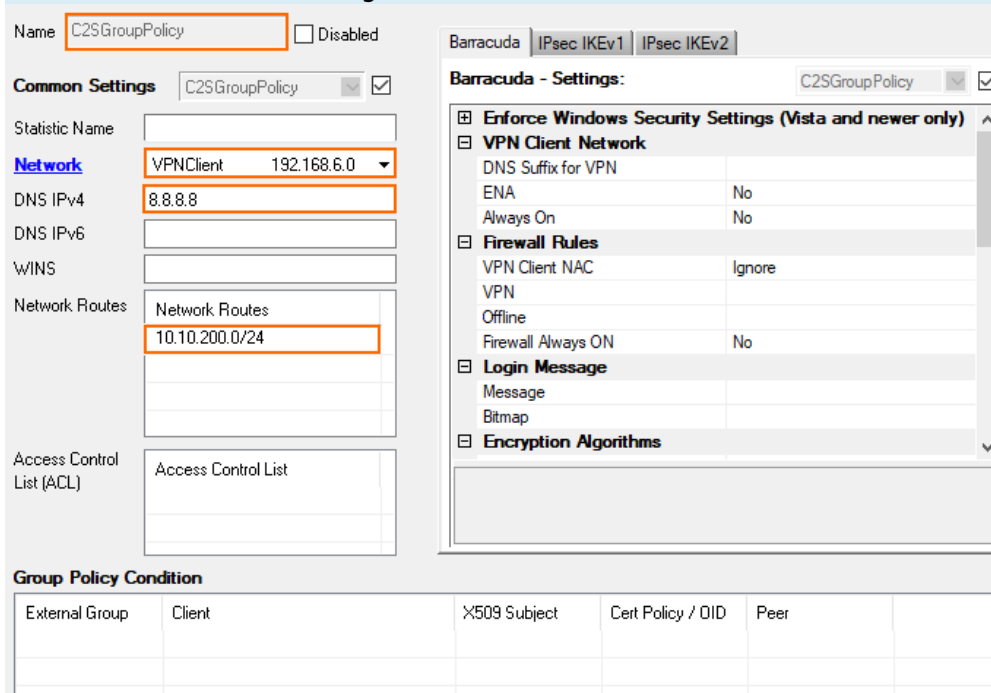
The VPN group policy specifies the network IPsec settings. You can group patterns to require users to meet certain criteria, as provided by the group membership of the external authentication server (e.g., CN=vpnusers\*). You can also define conditions to be met by the certificate (e.g., O(Organization)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

1. Go to **CONFIGURATION > Configuration Tree > Box > 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.



Name: **C2SGroupPolicy** ☐ Disabled

**Common Settings** **C2SGroupPolicy** ☒

Statistic Name:

**Network** **VPNClient** 192.168.6.0

DNS IPv4: **8.8.8.8**

DNS IPv6:

WINS:

Network Routes: 

Network Routes
10.10.200.0/24

Access Control List (ACL): 

Access Control List
---------------------

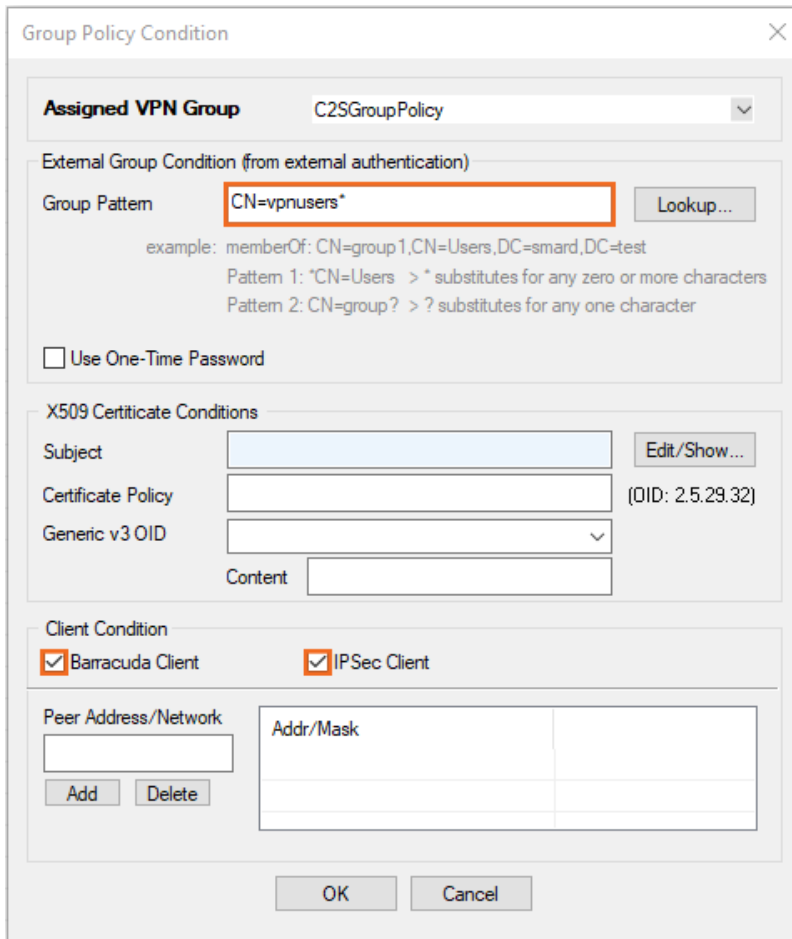
**Group Policy Condition**

External Group	Client	X509 Subject	Cert Policy / OID	Peer

**Barracuda - Settings:** **C2SGroupPolicy** ☒

- ☒ **Enforce Windows Security Settings (Vista and newer only)**
- ☒ **VPN Client Network**
  - DNS Suffix for VPN:
  - ENA:  No
  - Always On:  No
- ☒ **Firewall Rules**
  - VPN Client NAC:  Ignore
  - VPN:
  - Offline:
  - Firewall Always ON:  No
- ☒ **Login Message**
  - Message:
  - Bitmap:
- ☒ **Encryption Algorithms**

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**.



The image shows a 'Group Policy Condition' dialog box. At the top, 'Assigned VPN Group' is set to 'C2SGroupPolicy'. Under 'External Group Condition (from external authentication)', the 'Group Pattern' is 'CN=vpusers\*' and is highlighted with a red box. Below this, there are examples of LDAP patterns and a 'Lookup...' button. A checkbox for 'Use One-Time Password' is present. The 'X509 Certificate Conditions' section has fields for 'Subject', 'Certificate Policy', and 'Generic v3 OID', with an 'Edit/Show...' button. The 'Client Condition' section has checkboxes for 'Barracuda Client' and 'IPSec Client', both of which are checked. At the bottom, there is a 'Peer Address/Network' section with an 'Add' button and a table with columns 'Addr/Mask' and an empty row.

Group Policy Condition

Assigned VPN Group: C2SGroupPolicy

External Group Condition (from external authentication)

Group Pattern: CN=vpusers\* Lookup...

example: memberOf: CN=group1,CN=Users,DC=smard,DC=test  
Pattern 1: \*CN=Users > \* substitutes for any zero or more characters  
Pattern 2: CN=group? > ? substitutes for any one character

☐ Use One-Time Password

X509 Certificate Conditions

Subject:  Edit/Show...

Certificate Policy:  (OID: 2.5.29.32)

Generic v3 OID:

Content:

Client Condition

☒ Barracuda Client ☒ IPSec Client

Peer Address/Network

Add Delete

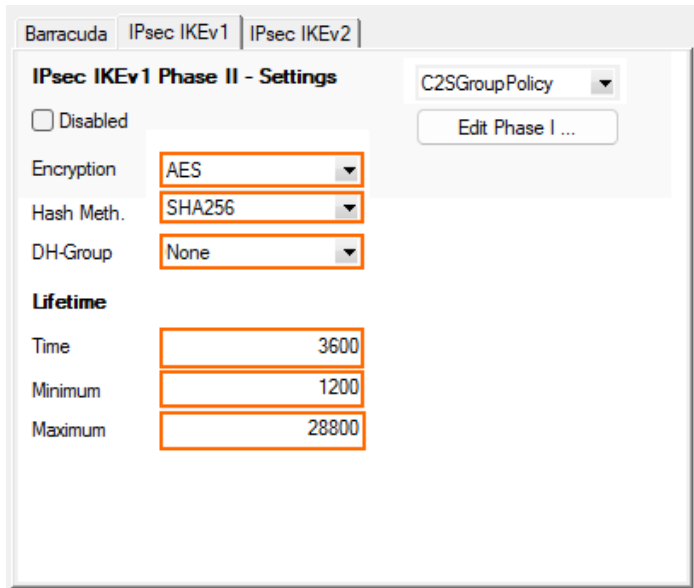
Addr/Mask

--	--

OK Cancel

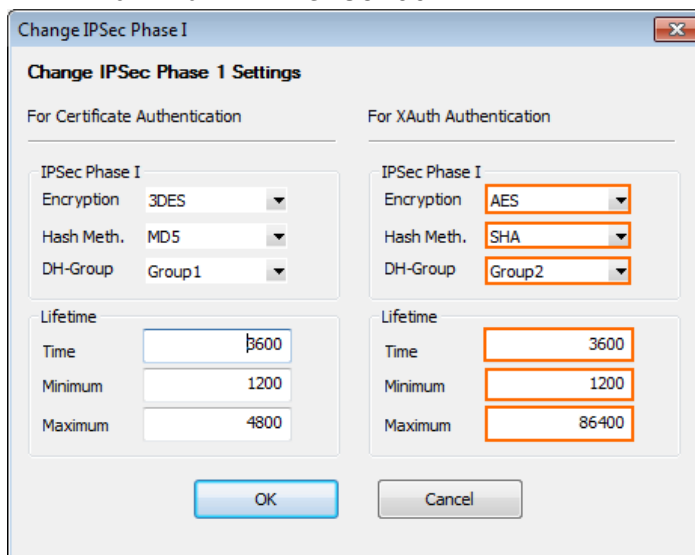
10. Configure the encryption and hashing settings:

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 **SHA256**.
  - **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 **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**.

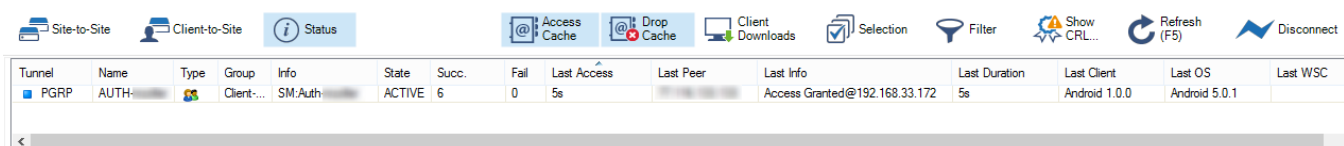
## Step 5. Add Access Rules



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.



Tunnel	Name	Type	Group	Info	State	Succ.	Fail	Last Access	Last Peer	Last Info	Last Duration	Last Client	Last OS	Last WSC
 PGRP	AUTH		Client...	SM:Auth	ACTIVE	6	0	5s		Access Granted@192.168.33.172	5s	Android 1.0.0	Android 5.0.1	

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 `/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. PSK03a.png
4. PSK04.png
5. PSK05.png
6. PSK06.png
7. PSK07.png
8. C2S\_00\_90.png
9. C2S\_01.png
10. C2S\_status\_connected.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.