

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

<https://campus.barracuda.com/doc/50660187/>

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 preshared 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, a premium remote connectivity license 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. 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

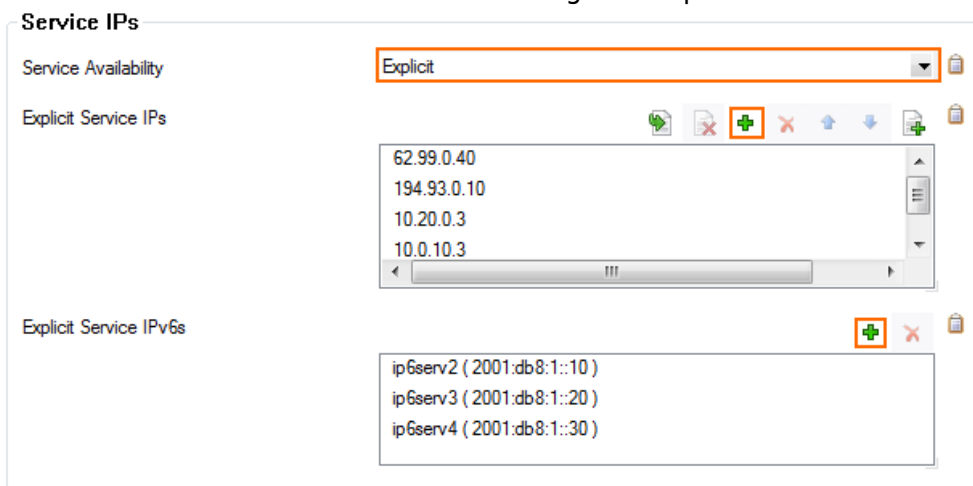
- Set up the VPN certificates for External CA. For more information, see [How to Set Up External CA VPN Certificates](#).
- Configure an external or local authentication service. For more information, see [Authentication](#).
- Identify the subnet (static route) or a range in a local network (proxy ARP) 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 > 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.

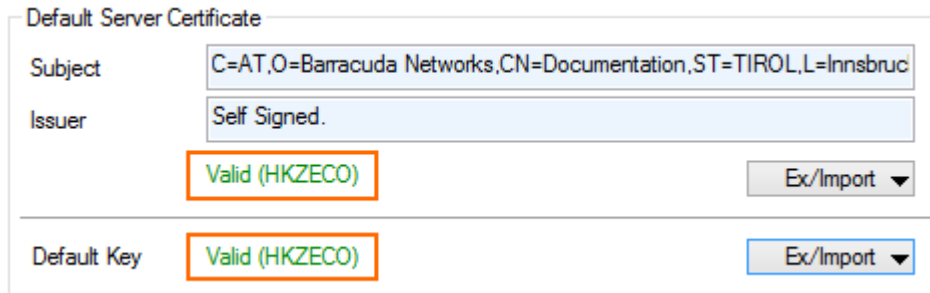


6. Click **Send Changes** and **Activate**.

Step 2. Configure the client network, gateway, and PSK key

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN > 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](#).



Default Server Certificate

Subject: C=AT,O=Barracuda Networks,CN=Documentation,ST=TIROL,L=Innsbruck

Issuer: Self Signed.

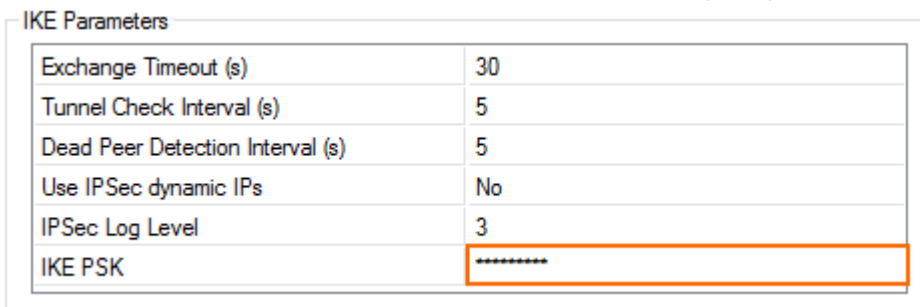
Valid (HKZECO)

Ex/Import ▼

Default Key: Valid (HKZECO)

Ex/Import ▼

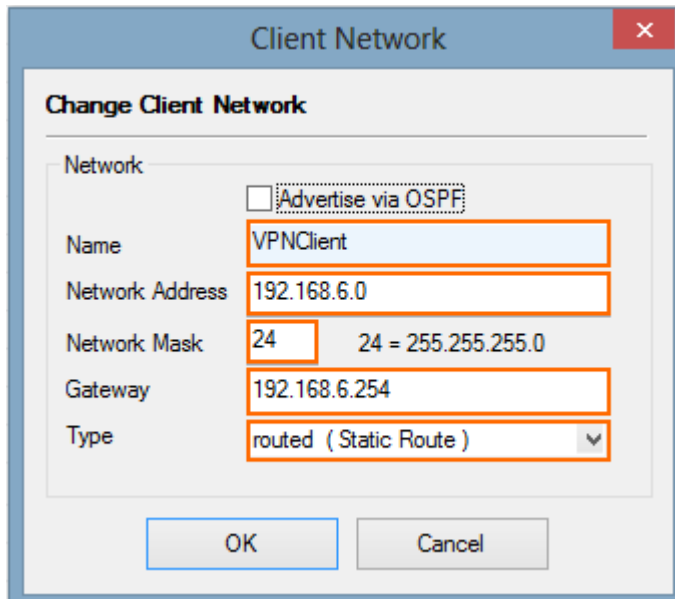
4. In the **Server Settings** window, click on the **Advanced** tab.
5. In the **IKE Parameter** section, enter the **IKE PSK** key. E.g., pre\$hareKey



IKE Parameters

Exchange Timeout (s)	30
Tunnel Check Interval (s)	5
Dead Peer Detection Interval (s)	5
Use IPSec dynamic IPs	No
IPSec Log Level	3
IKE PSK	*****

6. 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. E.g., 192.168.6.0
 - **Network Mask** – Enter the subnet mask for the VPN client network. E.g., 24
 - **Gateway** – Enter the gateway network address. E.g., 192.168.6.254
 - **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 Barracuda NextGen Firewall F-Series leads to the local network.

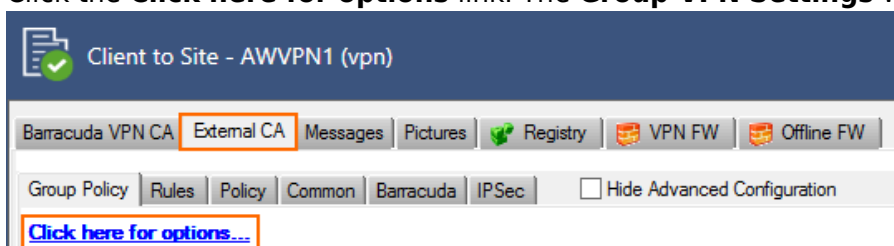


7. Click **OK**.
8. Click **Send Changes** and **Activate**.

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 > 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, select your previously configured authentication service from the **Authentication Scheme** list. For more information, see [Authentication](#).

Change Group VPN Settings

X509 Client Security

Mandatory Client Credentials
☐ X509 Certificate
☐ External Authentication
☐ IPsec needs Xauth

Certificate Login Matching
☐ Login must match AltName in Certificate

Server

Authentication Scheme
msad
☐ 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 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 > Virtual Servers > your virtual server > Assigned Services > VPN-Service > Client to Site**.
2. Click **Lock**.
3. Click on 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: 8.8.8.8

WINS:

Network Routes: Network Routes
10.10.200.0/24

Access Control List (ACL): Access Control List

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**

Enable VPN Client NAC	No
VPN	
Offline	
Firewall Always ON	No

☒ **Login Message**

Message	
Bitmap	

Group Policy Condition

External Group	Client	X509 Subject	Cert Policy / OID	Peer

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**.

Assigned VPN Group C2S-GroupPolicy

External Group Condition (from external authentication)

Group Pattern: **CN=vpnusers***

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

X509 Certificate Conditions

Subject:

Certificate Policy: (OID: 2.5.29.32)

Generic v3 OID:

Content:

Peer Condition

☒ Barracuda Client ☒ Transparent Agent (SSL-VPN)

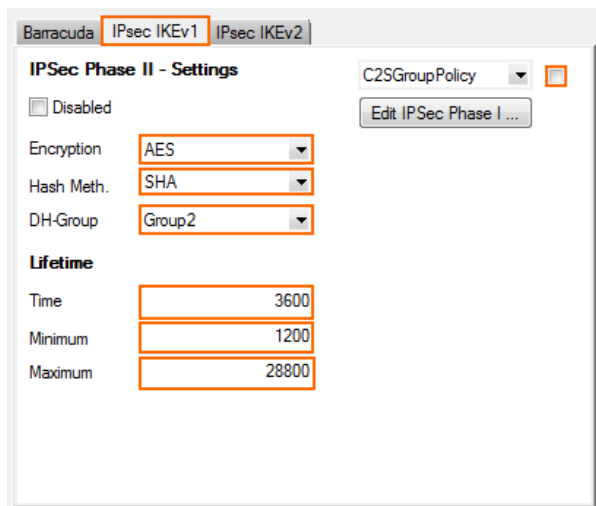
☒ IPsec Client

Peer Address/Network:

Addr/Mask:

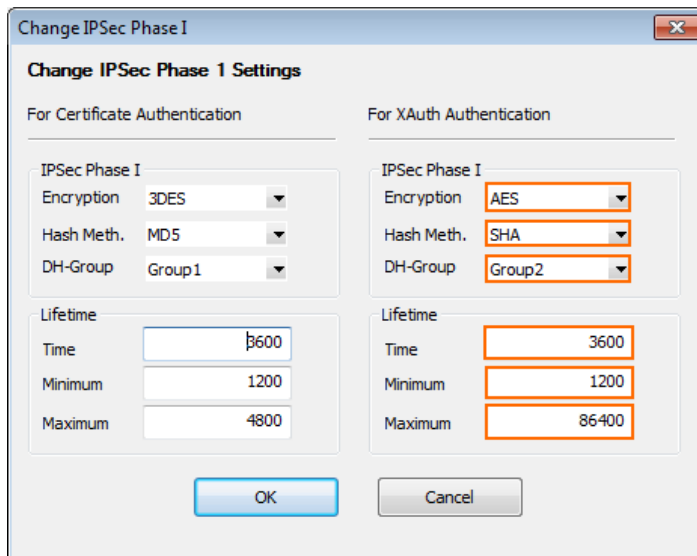
9. Configure the encryption and hashing settings:

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 **AES**.
 - **Hash Meth.** - Select SHA for iOS and Android 5.2 or lower. Select **SHA256** for Android 6.0 to 7.1.2, and **SHA512** for Android 7.1.2 and higher.
 - **DH-Group** - Select **Group2**.
 - **Time** - Enter 3600.
 - **Minimum** - Enter 1200.
 - **Maximum** - Enter 28800.



The screenshot shows the 'IPsec Phase II - Settings' configuration window. The 'Disabled' checkbox is unchecked. The 'Encryption' dropdown is set to 'AES', 'Hash Meth.' is set to 'SHA', and 'DH-Group' is set to 'Group2'. Under the 'Lifetime' section, 'Time' is 3600, 'Minimum' is 1200, and 'Maximum' is 28800. The 'C2SGroupPolicy' dropdown is visible at the top right, and an 'Edit IPsec Phase I ...' button is located below it.

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.



Change IPsec Phase I Settings

For Certificate Authentication

IPsec Phase I

Encryption: 3DES

Hash Meth.: MD5

DH-Group: Group1

Lifetime

Time: 3600

Minimum: 1200

Maximum: 4800

For XAuth Authentication

IPsec Phase I

Encryption: AES

Hash Meth.: SHA

DH-Group: Group2

Lifetime

Time: 3600

Minimum: 1200

Maximum: 86400

OK Cancel

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.

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 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 `/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.

Fore more information, see [Remote Access Clients](#).

Figures

1. Client2SiteIPsecXAUTHPSKVPN.png
2. vpn_service_listeners.png
3. PSK01.png
4. PSK02.png
5. PSK03.png
6. PSK04.png
7. PSK05v2.png
8. PSK06.png
9. PSK07.png
10. C2S_00.png
11. C2S_01.png
12. 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.