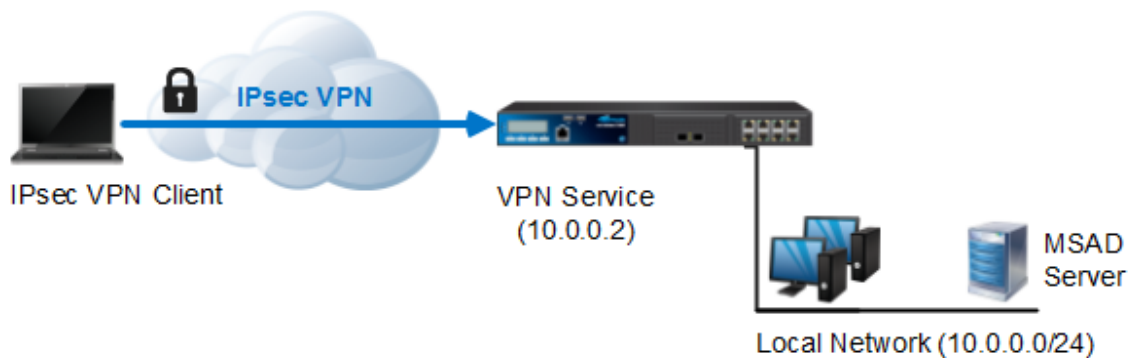


How to Configure a Client-to-Site IPsec VPN with Client Certificate Authentication

<https://campus.barracuda.com/doc/43847266/>

Use a Client-to-Site VPN to let mobile workers connect securely to your Barracuda NG Firewall. Each client must have a valid client certificate as well as the username and password to authenticate. By default, each user can have only one concurrent Client-to-Site VPN connection. A Remote Access Premium subscription is required to enable multiple concurrent Client-to-Site VPN sessions by the same user.



In this article:

Supported VPN Clients

You can use any standard-based IPsec VPN client. However, only the following clients are supported with the Barracuda NG Firewall:

- [The Barracuda VPN Client](#)
- [Apple iOS Devices](#)
- Android

Before You Begin

- Verify that the **server** and **default certificates** are installed and use DNS : *FQDN* (e.g.,

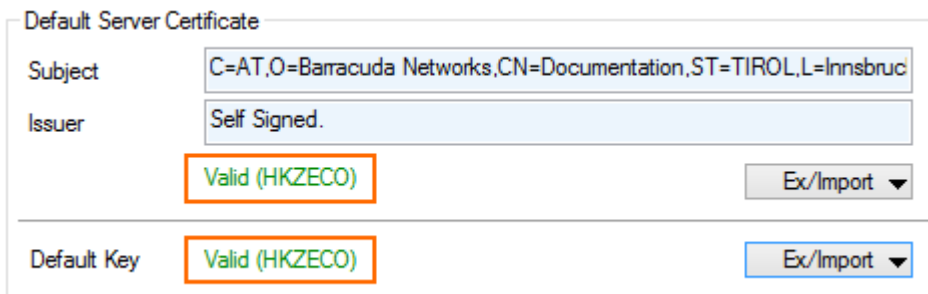
DNS:vpn.mydomain.com) as the **SubAltName**. This is necessary for iOS and Android devices to be able to connect. The FQDN must resolve to the IP address the VPN service is listening on. For more information, see [How to Set Up VPN Certificates](#).

- Configure an external or local authentication service. For more information, see [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 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. Create the VPN Client Network

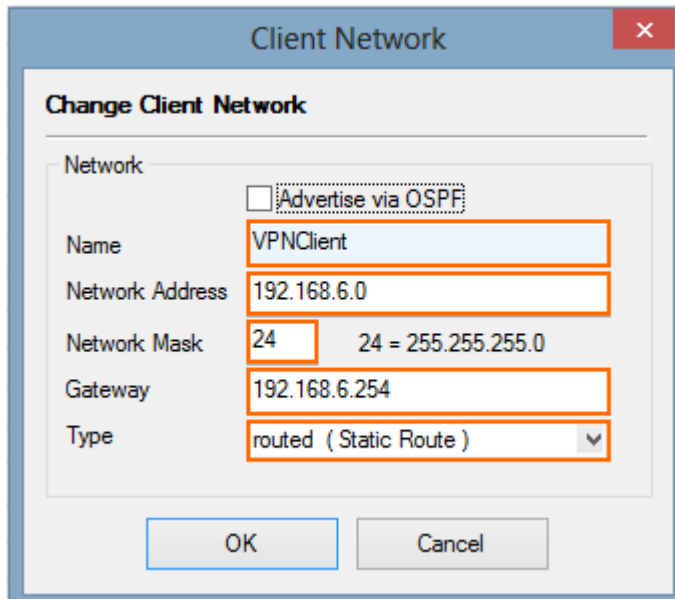
All VPN clients will receive an IP address from the VPN client network with a static gateway. You can choose the gateway IP address freely from the subnet.

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](#).



Default Server Certificate	
Subject	C=AT,O=Barracuda Networks,CN=Documentation,ST=TIROL,L=Innsbruck
Issuer	Self Signed.
	Valid (HKZECO) Ex/Import ▼
<hr/>	
Default Key	Valid (HKZECO) Ex/Import ▼

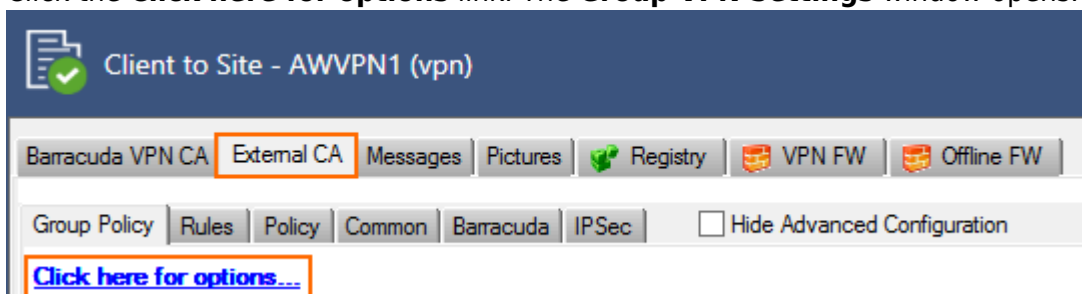
3. Click **OK** to close the **Server Settings** window.
4. Configure the client network.
 1. Click the **Client Networks** tab.
 2. Right-click the table and select **New Client Network**. The **Client Network** window opens.
 3. In the **Client Network** window, configure the following settings:
 -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



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

Step 2. 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** checkbox.
 2. In the **Server** section, 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 Ras Login permission required

Server

Server Protocol Key

Used Root Certificates

X509 Login Extraction Field

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

Step 3. 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 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 Disabled

Common Settings C2S-GroupPolicy

Statistic Name

Network 192.168.6.0

DNS

WINS

Network Routes

Network Routes
<input type="text" value="10.10.200.0/24"/>
<input type="text"/>
<input type="text"/>

Access Control List (ACL)

Access Control List
<input type="text"/>
<input type="text"/>
<input type="text"/>

Barracuda - Settings: C2S-GroupPolicy

Enforce Windows Security Settings (Vista and newer only)

VPN Client Network

DNS Suffix for VPN	ENA	Always On
<input type="text"/>	<input type="text" value="No"/>	<input type="text" value="No"/>

Firewall Rules

Enable VPN Client NAC	VPN	Offline	Firewall Always ON
<input type="text" value="No"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="No"/>

Login Message

Message	Bitmap
<input type="text"/>	<input type="text"/>

Group Policy Condition

External Group	Client	X509 Subject	Cert Policy / OID	Peer
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

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** checkbox is selected.
 4. In the **X509 Certificate Conditions** section enter matching conditions for the X509 client certificates.
9. Click **OK**.

Assigned VPN Group C2S-GroupPolicy

External Group Condition (from external authentication)

Group Pattern

example: memberOf: CN=group 1,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	

10. Configure the encryption and hashing settings:
1. Click the **IPsec** tab.
 2. Clear the checkbox 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.

- 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.

- Click **OK**.

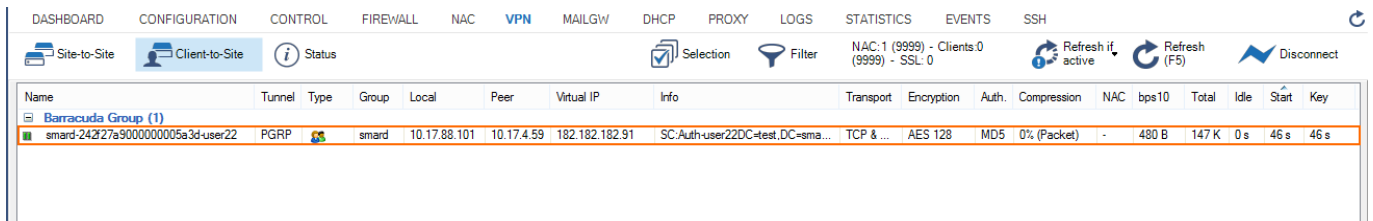
11. Click **Send Changes** and then click **Activate**.


Step 4. 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. Clients authenticated via client certificate use a name in the following format: --.



Name	Tunnel	Type	Group	Local	Peer	Virtual IP	Info	Transport	Encryption	Auth	Compression	NAC	bps10	Total	Idle	Start	Key
Barracuda Group (1)																	
smart-242f27a9000000005a3d-user22	PGRP		smard	10.17.88.101	10.17.4.59	182.182.182.91	SC:Auth-user22DC=rest.DC=sma...	TCP & ...	AES 128	MD5	0% (Packet)	-	480 B	147 K	0 s	46 s	46 s

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`, `/yourVirtualServer/VPN/ike` and `BOX/Control/AuthService` log files. For more information, see [LOGS Tab](#).

Figures

1. Client2SiteIPsecVPN.png
2. PSK01.png
3. PSK03.png
4. PSK04.png
5. PSK05.png
6. PSK06.png
7. PSK07.png
8. C2S_00.png
9. C2S_01.png
10. X509_04.png

© Barracuda Networks Inc., 2019 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.