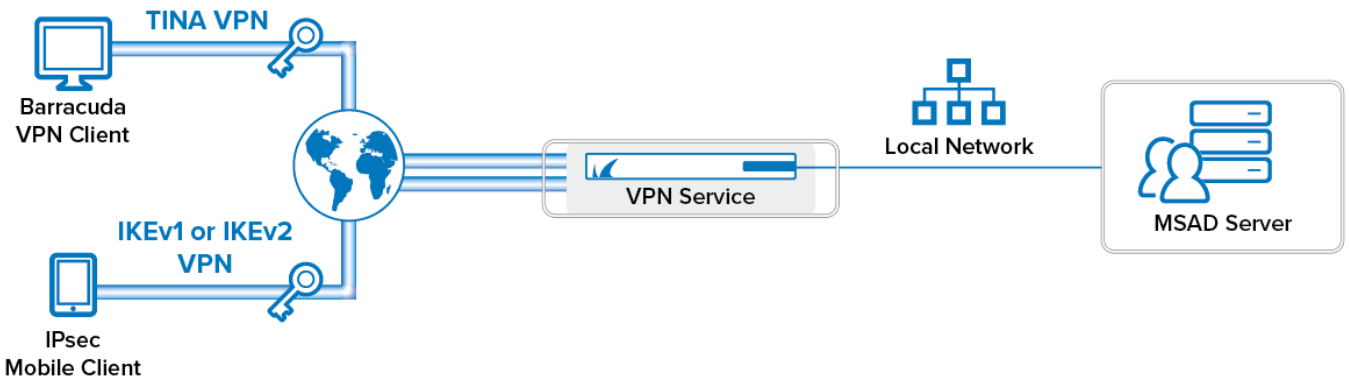
How to Configure a Client-to-Site VPN Group Policy

https://campus.barracuda.com/doc/96026130/

To let mobile workers securely connect to corporate information resources, create a client-to-site VPN group policy. This allows you to use one client-to-site configuration that enables CudaLaunch, Barracuda VPN clients, and native IKEv1 and IKEv2 IPsec clients to connect. 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. VPN clients can be authenticated either through external authentication schemes, client certificates, or a combination thereof.

Please note that the most recent Android versions no longer support IKEv1 tunnels and therefore do not work with pre-shared key.



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.
- VPN Client & Network Access Client
- Native iOS IPsec VPN Client
- Native Android IPsec VPN Client
- Windows 8/10 native IKEv2 IPsec VPN client

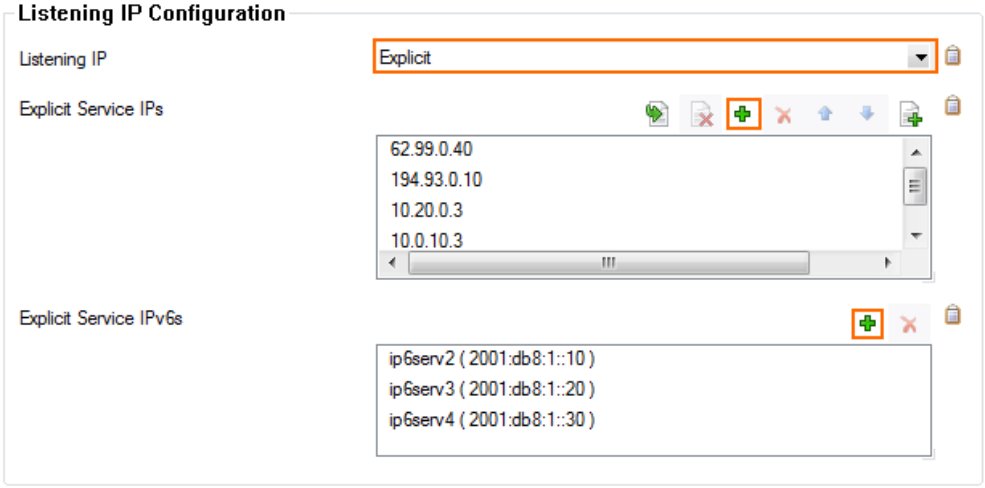
Before You Begin

- Set up the VPN certificates for External CA or Barracuda VPN CA. For more information, see How to Set Up External CA VPN Certificates, or How to Set Up Barracuda VPN CA VPN Certificates.
- Configure an external authentication scheme. 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.

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.
4. When selecting **Explicit**, click **+** for each IP address and enter the IPv4 addresses in the **Explicit Service IPs** list.
5. Click **+** to add an entry to the **Explicit IPv6 Service IPs**.
6. Select an IPv6 listener from the list of configured explicit IPv6 IP addresses.



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

Step 2. Configure the VPN Client Network

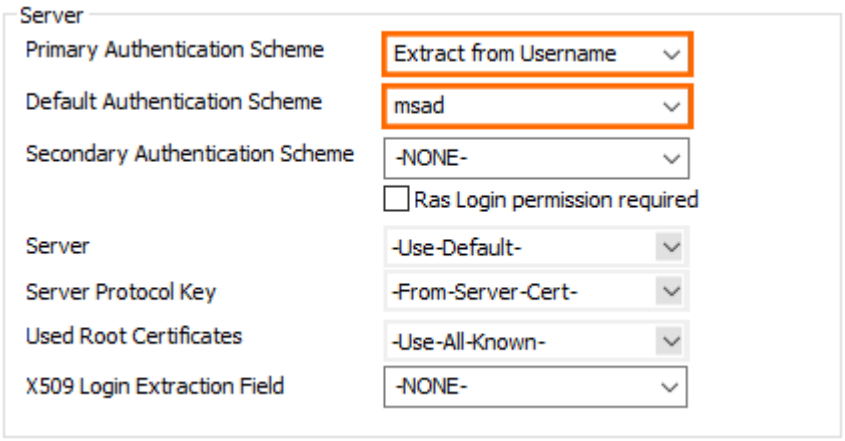
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.

3. In the left menu, select **Client Networks**.
4. Right-click the table, and select **New Client Network**.
5. In the **Client Network** window, configure the following settings:
   - **Name** – Enter a descriptive name for the network, e.g.: `Client to Site VPN Network`
   - **Network Address** – Enter the default network address, e.g.: `192.168.6.0`. All VPN clients will receive an IP address in this network.
   - **Network Mask** – Specify the appropriate subnet mask, e.g.: 24
   - **Gateway** – Enter the gateway network address, e.g.: `192.168.6.254`
   - **Type** – Select the type of network that is used for VPN clients:
     - **routed (Static Route)** – A separate subnet. A static route on the firewall routes traffic between the VPN client subnet and the local network.
     - **local (proxy ARP)** – A subnet of a local network. For example, Local network: `10.0.0.0/24` , Local segment `10.0.0.128/28` . You must also specify the IP range for the network:
       - **IP Range Base** – Enter the first IP address in the IP range for the VPN client subnet, e.g.: `10.0.0.128`.
       - **IP Range Mask** – Specify the subnet mask of the VPN client subnet, e.g.: 28
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Step 3. Configure Group Policy Settings

Configure the default **Group Policy** settings.

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 the **Group Policy** tab.
4. Click the **Click here for options** link. The **Group VPN Settings** window opens.
5. Select the **Authentication Scheme**:
   - **Primary Authentication Scheme** – The default authentication scheme used for all VPN group policies.
   - **Extract from username** – The authentication scheme is appended to the username, e.g., @msad. The authentication scheme (e.g., @msad) with the prepended username (e.g., user1@domain.com) 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@msad.
     > This scheme does not work for SAML authentication as SAML will instead cause a web browser to open and a token will be sent.
6. Select the **Default Authentication Scheme** from the drop-down list. This authentication scheme must be configured on box level of the firewall.



7. When using multi-factor authentication, select the **Secondary Authentication Scheme**.
8. Configure which certificates are used. By selecting a specific certificate, all VPN group policies must use this certificate:
   - **(optional) Server** – Select a server certificate, or use the default server certificate configured in the VPN settings.
   - **Server Protocol Key** – Select the service certificate.
   - **(optional) Used Root Certificates** – Select a root certificate, or use the default server certificate configured in the VPN settings.
   - **(optional) X509 Login Extraction Field** – Select the X.509 field containing the user name.
9. (optional) If needed, select the **Preauthentication Scheme**. A **Preauthentication Scheme** can be configured that allows users to determine the default authentication scheme based on attribute values from MSAD/LDAP/TACACS+. More details regarding preauthentication and a full overview of all available group policy settings can be found here: Client-to-Site Group Policy Settings.
10. Click **OK**.

When using X.509 certificate authentication, only X.509 certificate conditions can be assigned. Authentication will not work if group patterns are defined in the **External Group Condition** section. For IPsec XAUTH authentication, group patterns must be assigned.

Step 4. Create a VPN Group Policy

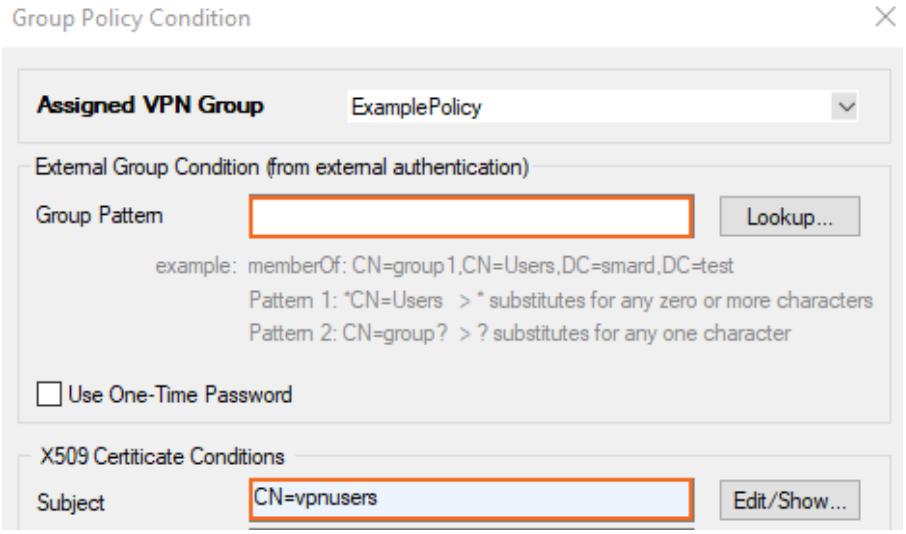
Create a group policy and configure the network settings for the client-to-site connections. If you want the client to send all traffic through the VPN tunnel, enter `0.0.0.0/0` as the network.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Client-to-Site**.
2. Click the **External CA** tab and then click the **Group Policy** tab.
3. Click **Lock**.
4. Right-click the table and select **New Group Policy**.
5. In the **Edit Group Policy** window, edit the following settings:

- **Name** – Enter a name for this policy.
- **Common Settings** – Select the check box.
- **Statistics Name** – To better allocate statistics entries, enter a name.
- **Network** – Select the required client network.
- **DNS** – Enter a DNS server for the clients.
- **Network Routes** – Add the IP address(es) and/or hostname(s) of all networks that should be reachable by the VPN clients.
  You can enter the network route also as an FQDN (domain name). If a public network address that is associated with a domain name changes, then the administrator does not need to change the network address manually, but instead the domain name will be resolved to the newest associated network address at runtime.
  Enter `0.0.0.0/0` for all traffic to be sent through the client-to-site VPN.

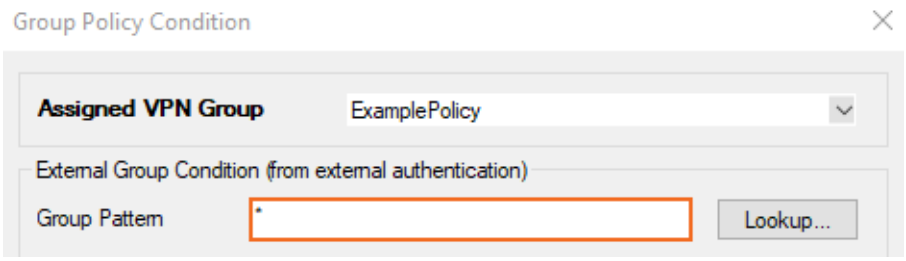
6. Right-click the **Group Policy Condition** field and select **New Rule**. The **Group Policy Condition** window opens.
   When using X.509 certificate authentication, set filters for the certificate in the **X.509 Certificate Conditions** section.
   - To let everyone with a valid certificate log on, click **Edit/Show** and add the following condition to the **Subject** field: CN=*.
   - To limit the condition to a specific group, add the following condition: *CN=groupname*. Certificate condition entries are case insensitive and can contain the quantification patterns **?** (zero or one) and ***** (zero or more).

     When using X.509 certificate authentication, the **Group Pattern** field must be blank!



   When using IPsec XAUTH authentication, set filters for the policy in the **Group Pattern** field:
   - To let everyone with a valid certificate log on, add the following condition: CN=*
   - To limit the condition to a specific group, add the following condition: *CN=groupname*. You can also hit **Lookup** to search for a group. Inside the AD lookup, put in your object filter or hit **Search**. From the list, select the desired group. You must be logged on to Firewall Admin from the domain controller to use this search query feature.

   For local authentication, add the following condition in the **Group Pattern** field to allow all users or groups: *. To limit, add the group name of your local users.



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

Step 5. (optional) Adjust Barracuda (TINA) Settings

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. Double-click the VPN group policy created in Step 2.
5. In the **Barracuda** tab configure:
   - **Windows Security Settings**
   - **VPN Client Network**
   - **Firewall Rules**
   - **Login Message**
   - **Ciphers**
6. Click **OK**.

Step 6. (optional) Adjust the IKEv1 IPsec Phase I and II Settings

To connect to the firewall using iOS and Android clients, you must use the following IKEv1 IPsec Phase I and II settings.

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. Double-click the VPN group policy created in Step 3.
5. Click the **IPSec IKEv1** tab and configure the following settings:
   - **IPSec IKEv1 Phase II - Settings** – Clear the check box and then select ***Group Policy Name*** **(Create New)**.
   - **Encryption** – Select **AES**.
   - **Hash Meth** – Select **SHA** for iOS and Android VPN 5.2 or lower. For Android 6.X use **SHA256**, for Android 7.0 or higher **SHA512**.

- **DH-Group** – Select **Group2**.
- **Time** – Enter `3600`
- **Minimum** – Enter `1200`
- **Maximum** – Enter `4800`

6. Configure the same settings for IPsec Phase I that you selected for IPsec Phase II.
   1. Click **Edit Phase I**.
   2. In the **Change IPSec Phase I** window, specify the same settings that you selected for the **IPSec Phase II - Settings**:
      - **Encryption** – Select **AES**.
      - **Hash Meth** – Select **SHA**.
      - **DH-Group** – Select **Group2**.
      - **Time** – Enter `3600`
      - **Minimum** – Enter `1200`
      - **Maximum** – Enter `4800`
   3. Click **OK**.
7. In the **Edit Group Policy** window, click **OK**.
8. Click **Send Changes** and **Activate**.

Step 7. (optional) Adjust the IKEv2 IPsec Phase I and II Settings

To allow IKEv2 IPsec clients to connect to the firewall using this group policy, create and configure the IKEv2 group policy settings.

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. Double-click the VPN group policy created in Step 3.
5. Click the **IPSec IKEv2** tab and configure the following settings:
   - **IPSec IKEv2 Phase II - Settings** – Clear the check box and then select ***Group Policy Name*** **(Create New)**.
   - **Encryption**
   - **Hash Meth**
   - **DH-Group**
   - **Lifetime**
6. Configure the same settings for IPsec Phase I that you selected for IPsec Phase II.
   1. Click **Edit Phase I**.
   2. In the **Change IPSec Phase I** window, specify the same settings that you selected for the **IPSec Phase II - Settings**:
      - **Encryption**
      - **Hash Meth**
      - **DH-Group**
      - **Lifetime**

3. Click **OK**.

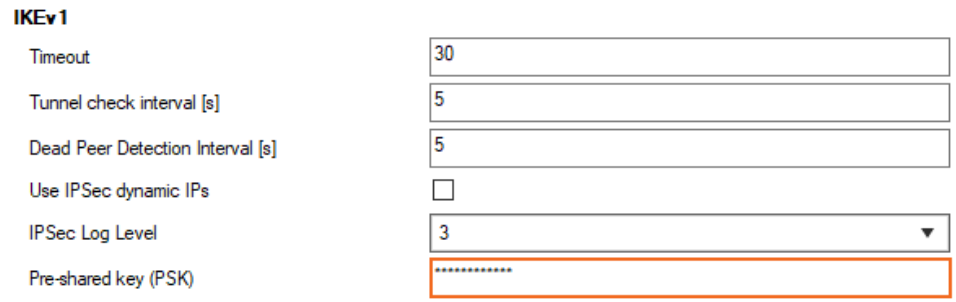
7. In the **Edit Group Policy** window, click **OK**.
8. Click **Send Changes** and **Activate**.

Step 8. (optional) Configure a Pre-Shared Key

If you want to authenticate using pre-shared keys for a IPsec IKEv1, client you must configure the shared secret in the VPN settings.

> The shared secret can consist of small and capital characters, numbers, and non-alphanumeric symbols, except the hash sign (#).

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. In the left menu, select **IPSec**.
4. In the **IKEv1** section, enter the **Pre-shared key (PSK)**. E.g., `pre$haredKey`



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

Step 9. Add Access Rules

Add an access rule to allow the VPN clients to connect 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:

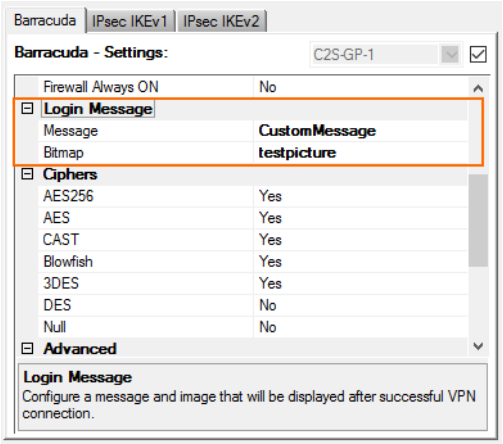
- **Blue** – The client is currently connected.
- **Green** – The VPN tunnel is available, but currently not in use.
- **Grey** – The VPN tunnel is currently disabled. To enable the tunnel, right-click it and select **Enable Tunnel**.

For more information about the **VPN > Client-to-Site** page, see VPN Tab.

Configure Custom Login Message

When using a Barracuda VPN client, you can define a custom welcome message as well as upload your company's logo as a custom **Picture**. Custom message and pictures can be selected in the **Barracuda - Settings** of the VPN group policy.

- **Messages** – Create a custom message in the **Message** tab of the **Client-to-Site** page, and then select the customized welcome messages in the **Barracuda Settings** tab of the VPN group policies.
- **Bitmap/Pictures** – Upload a 150x80 pixel, 256 color BMP bitmap in the **Pictures** tab of the **Client-to-Site** page, and then select the custom bitmap in the **Barracuda Settings** tab of the VPN group policies.



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. c2s_advanced_vpn.png
2. vpn_service_listeners.png
3. extract_from_msad.png
4. vpn_gpc.png
5. vpn_gp.png
6. PSK02.png
7. custom_login_message.png