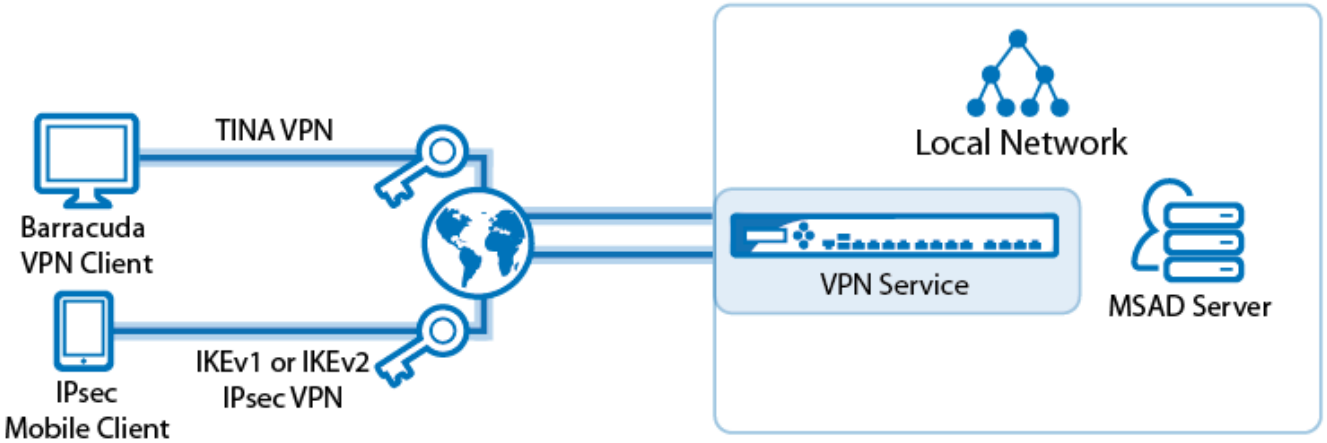
How to Configure a Client-to-Site VPN Group Policy

https://campus.barracuda.com/doc/46209144/

Use this client-to-site configuration to easily manage and connect your devices with CudaLaunch.

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 both Barracuda VPN Clients and IKEv1 and IKEv2 IPsec clients to connect. To allow Android and iOS devices to connect, you must use compatible IPSec IKEv1 settings. The client can be authenticated either through external authentication schemes, client certificates, or a combination thereof.



Supported VPN Clients

Depending on the group policy profile, you can use the Barracuda VPN Client or any standard IPsec IKEv1 or IKEv2 VPN client. However, only the following clients are supported:

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

Before You Begin

- Set up the VPN certificates. For more information, see How to Set Up VPN Certificates.
- Configure an external authentication scheme. For more information, see Authentication.

Step 1. Configure Group Policy Settings

Configure the default **Group Policy** 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 and then the **Group Policy** tab.
4. Click the **Click here for options** link.
5. In the **Server** section of the **Group VPN Settings** window, select the **Authentication Scheme**. E.g., **msad**
6. 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 X509 field containing the user name.
7. (optional) If needed, select the **Preauthentication Scheme**.
8. Click **OK**.

   Only X.509 certificate conditions can be assigned because IPsec XAUTH authentication will not work if group patterns are defined in the **External Group Condition** section.

Step 2. 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 > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > Client-to-Site**.
2. Click the **External CA** tab and then click the **Group Policy** tab.
3. Right-click the table and select **New Group Policy**.
4. 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 all networks that should be reachable by the VPN clients. Enter

0.0.0.0/0 for all traffic to be sent through the client-to-site VPN.

5. Right click the **Group Policy Condition** field and select **New Rule**.
6. In the **X509 Certificate Conditions** section of the **Group Policy Condition** window, set filters for the certificate. Click **Edit/Show** and specify the conditions:
   - To let everyone with a valid certificate log on,
     - Add the following condition to the **Subject** field: `CN=*`
   - To limit the condition to a specific group,
     - Add the following condition to the **Subject** field: `*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 NextGen Admin from the domain controller to use this search query feature.
   - For local authentication,
     - Add the following condition to the **Subject** field to allow all users or groups: *
     - To limit, add the group name of your local users.

   Certificate condition entries are case insensitive and can contain the quantification patterns **?** (zero or one) and ***** (zero or more).
7. Click **OK**.
8. Click **OK**.
9. Click **Send Changes** and **Activate**.

Step 3. (optional) Adjust Barracuda Network Access and VPN Client 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 and then click the **Group Policy** tab.
4. Double-click on 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 4. (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 > 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. Double-click on 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**: **AES**
   - **Hash Meth**: **SHA**
   - **DH-Group**: **Group2**
   - **Time**: 3600
   - **Minimum**: 1200
   - **Maximum**: 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**: **AES**
      - **Hash Meth**: **SHA**
      - **DH-Group**: **Group2**
      - **Time**: 3600
      - **Minimum**: 1200
      - **Maximum**: 4800
   3. Click **OK**.
7. In the **Edit Group Policy** window, click **OK**.
8. Click **Send Changes** and **Activate**.

Step 5. (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 > 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. Double-click on 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 6. 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.

Troubleshooting

To troubleshoot VPN connections, see the `/yourVirtualServer/VPN/VPN` and `/yourVirtualServer/VPN/ike` log files. For more information, see LOGS Tab.

Figures

1. Client2SiteIPsecAdvancedVPN.png