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

https://campus.barracuda.com/doc/53248505/

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 the version of your mobile operating system. VPN clients can be authenticated either through external authentication schemes, client certificates, or a combination thereof.

Supported VPN Clients

While 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
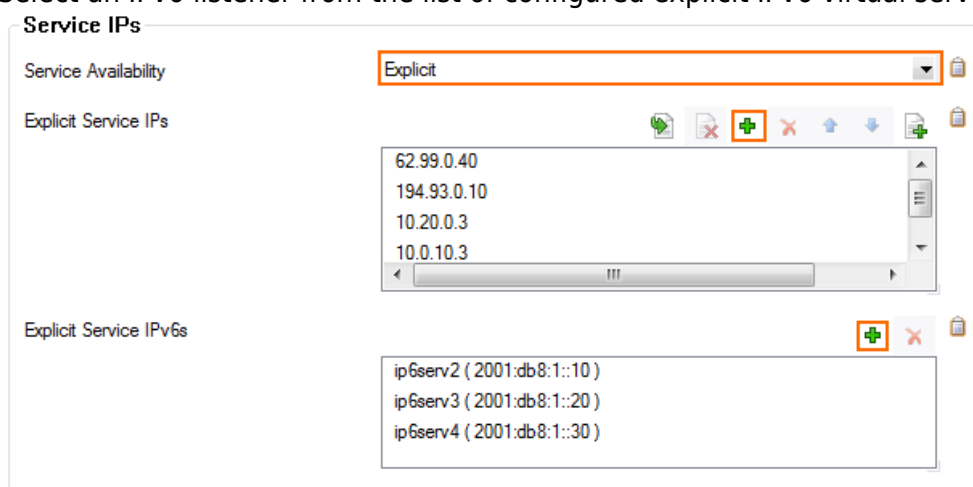- Windows 8/10 native IKEv2 IPsec VPN client

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 > 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 VPN Client Network

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service > VPN Settings** .
2. Click **Lock**.
3. Click the **Client Networks** tab.
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 Barracuda NextGen Firewall F-Series 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 > 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 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 > 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 5. (optional) Adjust Barracuda (TINA) 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 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 > 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** – 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 > 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 **SendChanges** and **Activate**.

Step 8. (optional) Configure a Preshared 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 alpha-numeric symbols, except the hash sign (#).

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN > VPN Settings**.

2. Click **Lock**.
3. In the **Server Settings** window, click on the **Advanced** tab.
4. In the **IKE Parameter** section, enter the **IKE PSK** key. E.g., `pre$haredKey`

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	********

5. Click **OK**.
6. 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:
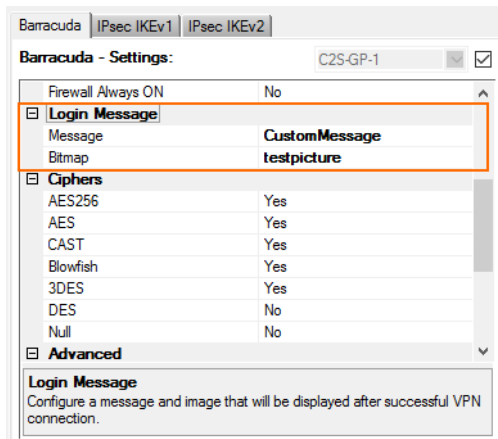
- **Blue** – The client is currently connected.
- **Green** – The VPN tunnel is available, but currently not in use.
- **Grey** – The VPN tunnel is currently disabled. To enable the tunnel, right-click it and select **Enable Tunnel**.

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 messages as well as upload your companies 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 `/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. Client2SiteIPsecAdvancedVPN.png
2. vpn_service_listeners.png
3. PSK02.png
4. custom_login_message.png