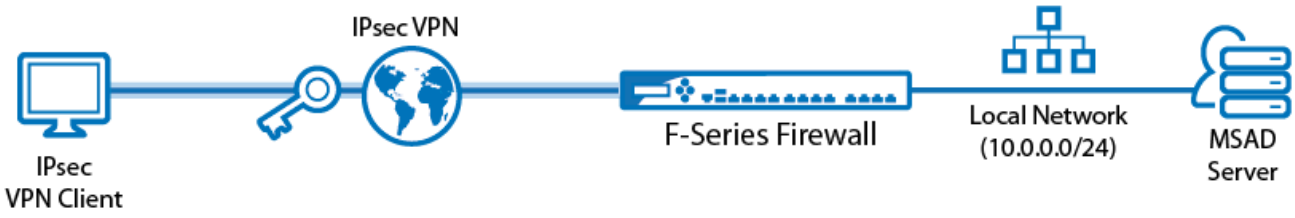
Example - Client-to-Site IKEv2 IPsec VPN

https://campus.barracuda.com/doc/50660242/

Use an IPsec IKEv2 client-to-site VPN to let mobile workers connect securely to your Barracuda NextGen F-Series Firewall with a standard compliant IKEv2 VPN client.



Supported VPN clients

Although any standard-compliant IPsec IKEv2 client should be able to connect via IPsec, Barracuda Networks recommends using the following clients:

- Windows 8/10 native IKEv2 IPsec VPN client
- Windows 10 Mobile 10.0.14393

Android and iOS devices are currently not supported.

Before you begin

- Set up the VPN certificates for external CA. For more information, see How to Set Up External CA VPN Certificates.
- Configure MS-Chapv2 authentication. For more information, see How to Configure MS-CHAP 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 IPv4 and IPv6 addresses 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.
- If you are using a Windows phone, you must install the root certificates on the phones certificate store.

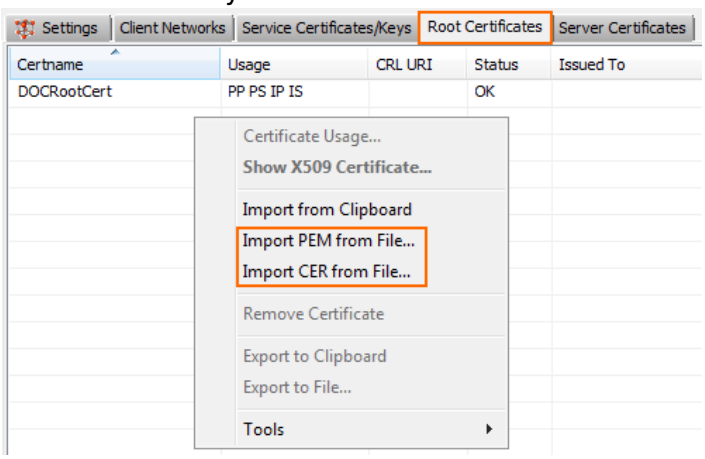
Step 1. Create VPN certificates

1. Create a root and VPN certificates with the following requirements for the VPN server certificate:
   - CN – Set to the FQDN or your VPN service. The FQDN must resolve to the IP address the VPN service is listening on.
   - SubAltName (SAN) – Must be the same as the the CN.
   - keyUsage = nonRepudiation, digitalSignature, keyEncipherment,
   - extendedKeyUsage = 1.3.6.1.5.5.8.2.2,serverAuth

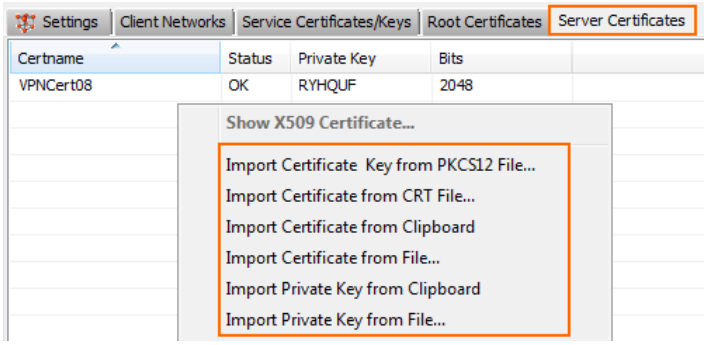
   You should now have a root certificate in CER or PEM format and a VPN certificate in PKCS12, CRT, or PEM format.

Step 2. Add certificates to VPN settings

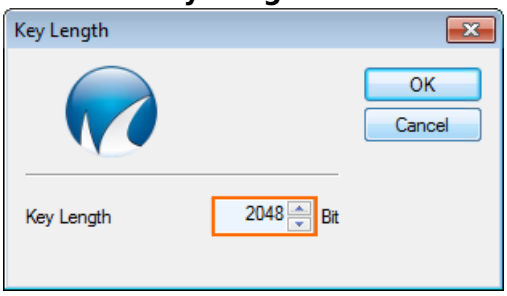
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > VPN Settings** .
2. Click **Lock**.
3. Click on the **Root Certificates** tab.
4. Right-click the table and click on **Import CER from File** or **Import PEM from File**, depending on the format of your root certificate.



5. Select and upload the root certificate created in step 1.
6. Click on the **Sever Certificates** tab.
7. Right-click the table and click on the **Import Certificate** menu item matching your VPN server certificate.



8. Select and upload the VPN certificate created in step 1.
9. Click on the **Service Certificates/Keys** tab.
10. Right-click the table and select **New Key**.
11. Enter a **Key Name**.
12. Select the **Key Length**.



13. Click **OK**.
14. Click **Send Changes** and **Activate**.

Step 3. 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.

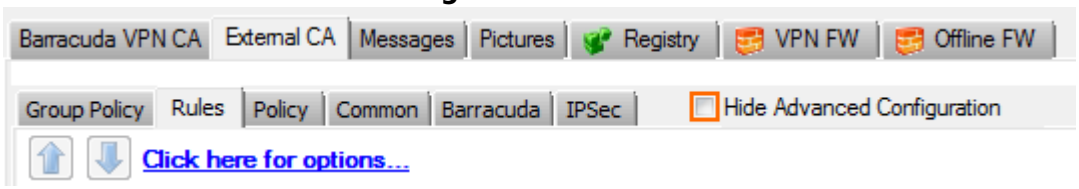
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > VPN Settings** .
2. Click **Lock**
3. Click the **Client Networks** tab.
4. Right-click the table and select **New Client Network**. The **Client Network** window opens.
5. In the **Client Network** window, configure the following settings:
   - **Advertise Route** – Enable check box to include the VPN network in the OSPF or BGP network
   - **Name** – Enter a descriptive name for the network.
   - **Network Address** – Enter the base network address for the VPN clients.
   - **Network Mask** – Enter the subnet mask for the VPN client network.
   - **Gateway** – Enter the gateway network address.
   - **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

firewall leads to the local network.

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

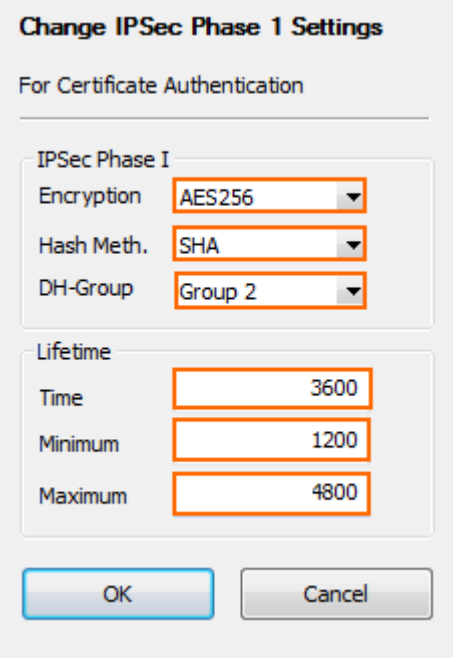
Step 4. Configure IKEv2 phase 1 and 2

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. Clear the **Hide Advanced Configuration** check box.

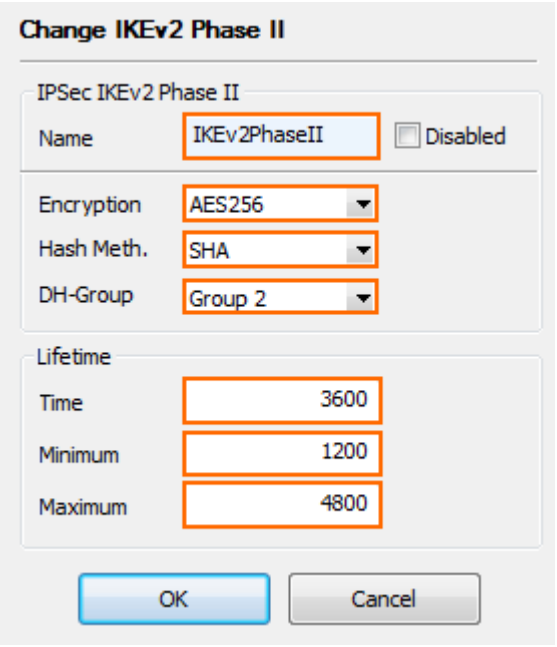


5. Click the **IPsec** sub-tab.

6. In the **IKEv2 Phase 1 (default)** section, double-click on the Phase 1 encryption settings. The **Change IPsec Phase 1** window opens.
7. Configure the **IPsec Phase I** encryption settings:
   - **Encryption** – Select **AES256**.
   - **Hash Meth** – Select **SHA**.
   - **DH-Group** – Select **Group 2**.
8. (optional) Set the IPsec Phase 1 **Lifetime** settings:
   - **Time** – Enter `3600`.
   - **Minimum** – Enter `1200`.
   - **Maximum** – Enter `4800`.
9. Click **OK.**



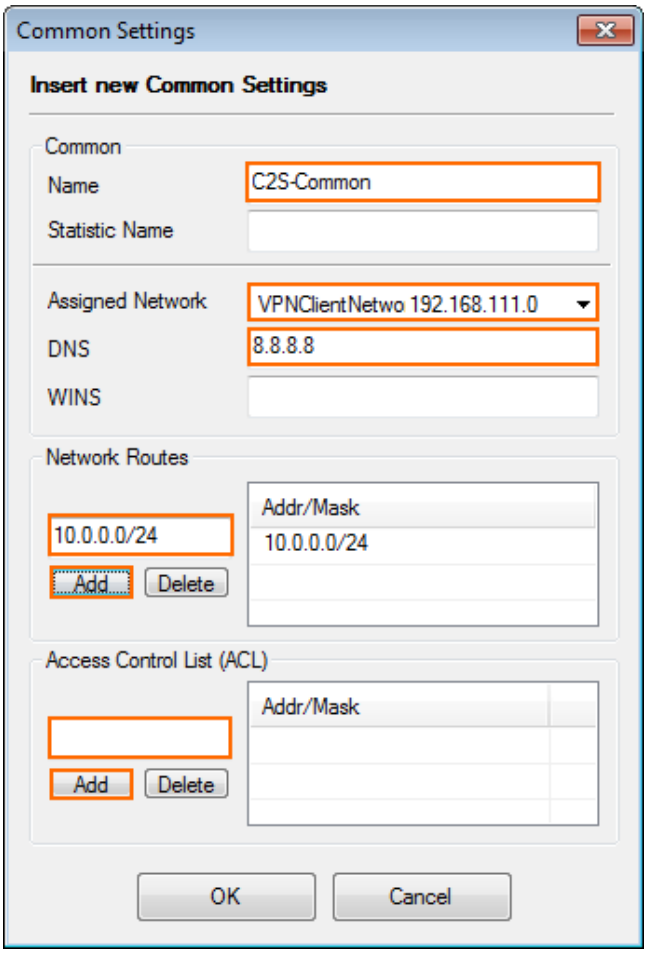
10. Right-click in the **IKEv2 Phase 2** table and select **New IKEv2 Phase II**. The **IPsec IKEv2 Phase II** windows opens.
11. Enter a **Name**.
12. Configure the IPsec phase 2 encryption settings:
    - **Encryption** – Select **AES256**.
    - **Hash Meth** – Select **SHA**.
    - **DH-Group** – Select **Group 2**.
13. (optional) Set the IPsec Phase 2 **Lifetime** settings:
    - **Time** – Enter `3600`.
    - **Minimum** – Enter `1200`.
    - **Maximum** – Enter `4800`.
14. Click **OK**.



15. Click **Send Changes** and **Activate**.

Step 5. Configure VPN common settings

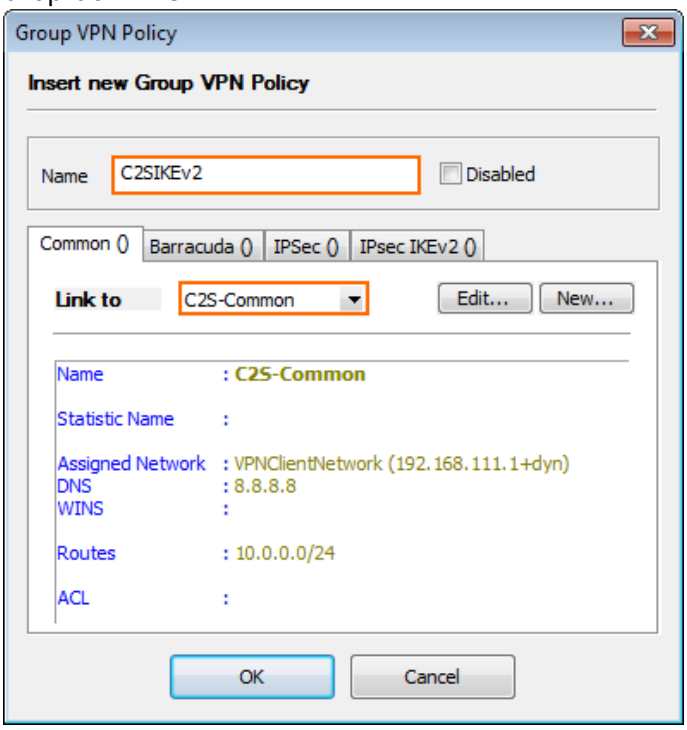
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > Client to Site** .
2. Click **Lock**.
3. Click on the **External CA** tab.
4. Click on the **Common** sub-tab.
5. Right-click the table and select **New Common**. The **Common Settings** window opens.
6. Enter a **Name**.
7. (optional) Enter a **Statistic Name**. For more information, see Statistics.
8. From the **Assigned Network** drop-down list, select the VPN network created in step 3.
9. (optional) Enter the **DNS** server IP address.
10. (optional) Enter the **WINS** server IP address.
11. Enter the **Network Routes** that should be sent through the VPN tunnel and click **Add**. To send all traffic through the VPN tunnel, enter `0.0.0.0/0`.
12. (optional) To limit the source from which VPN connections are accepted, add the IP addresses or subnets to the **Access Control List (ACL)**.



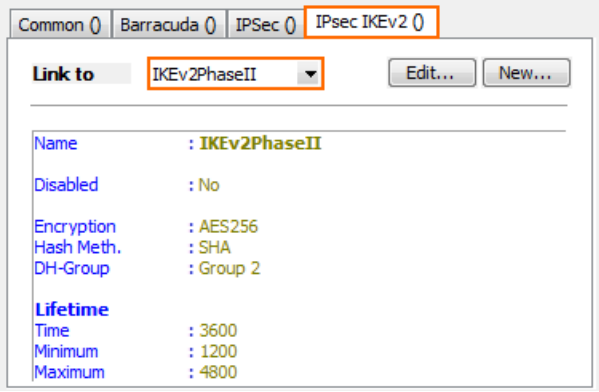
13. Click **OK**.
14. Click **Send Changes** and **Activate**.

Step 6. Configure a VPN group policy

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.
4. Click on the **Policy** sub-tab.
5. Right-click in the table and select **New Policy**. The **Group VPN Policy** window opens.
6. Enter a **Name**.
7. In the **Common** tab, select the VPN common settings you created in step 5 from the **Link to** drop-down list.



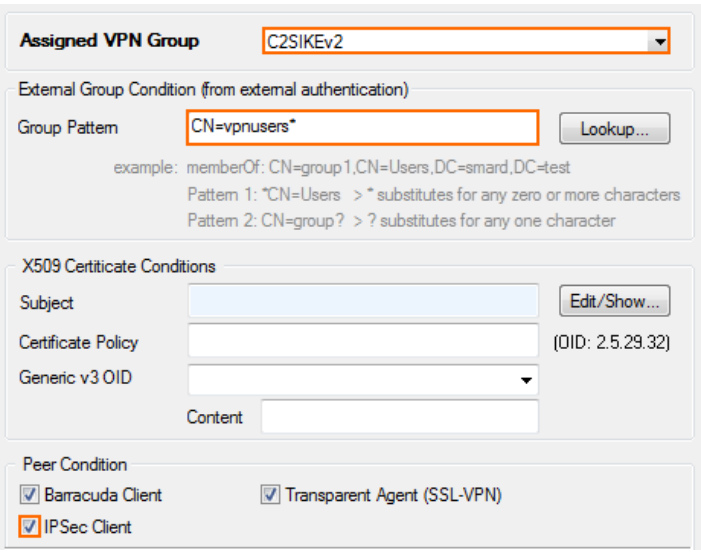
8. Click the **IPsecIKEv2** tab.
9. Select the IPsec IKEv2 Phase 2 settings from the **Link to** drop-down list.



10. Click **OK**.
11. Click **Send Changes** and **Activate**.

Step 7. Configure VPN rules

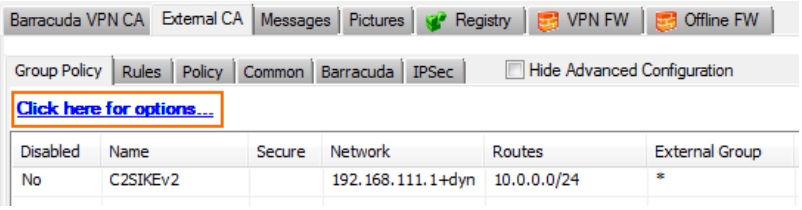
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > Client to Site** .
2. Click **Lock**.
3. Click on the **External CA** tab.
4. Click on the **Rules** sub-tab.
5. Right-click in the table and select **New Rule**. The **Group Policy Condition** window opens.
6. From the **Assigned VPN Group** list, select the group VPN policy created in step 6.
7. (external authentication only) Enter a **Group Pattern** to define the groups that will be assigned the policy. E.g.: `CN=vpnusers*`
8. In the **Peer Condition** section, verify that **IPsec Client** check box is selected.
9. (optional) In the **X509 Certificate Conditions** section, enter matching conditions for the X509 client certificates.



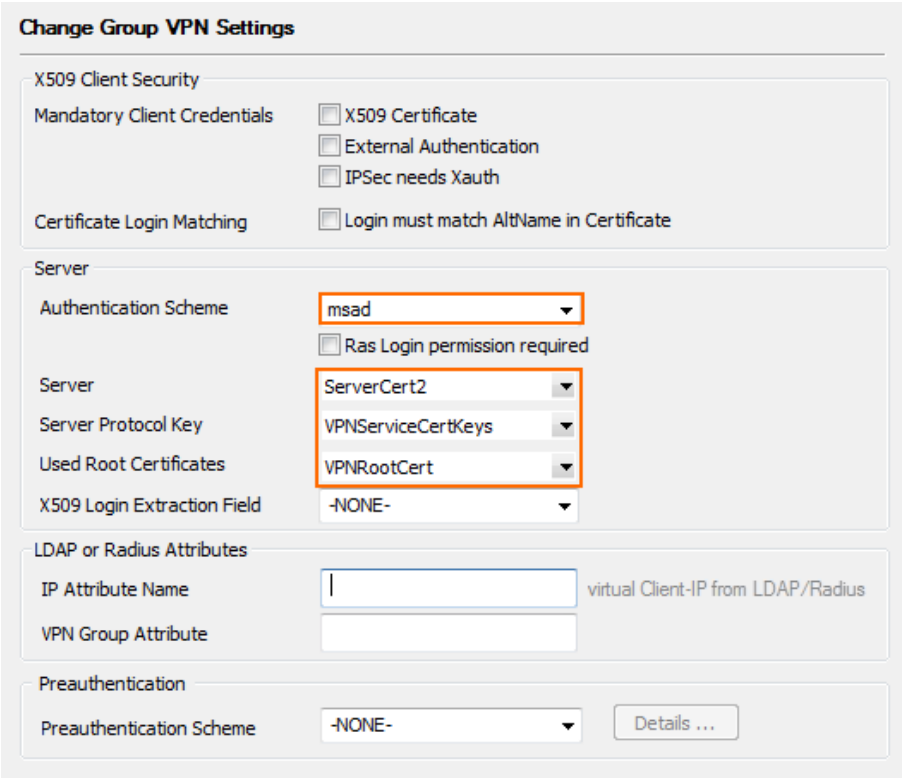
10. Click **OK**.
11. Click **Send Changes** and **Activate**.

Step 8. Configure group VPN 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 on the **External CA** tab.
4. Click the **Click here for options** link.



5. From the **Authentication Scheme** drop-down list, select **msad**.
6. From the **Server** drop-down list, select the VPN server certificate uploaded in step 2.
7. From the **Server Protocol Key** drop-down list, select the service certificate created in step 2.
8. From the **Used Root Certificates** drop-down list, select the root certificate uploaded in step 2.



9. Click **OK**.
10. Click **Send Changes** and **Activate**.

Step 9. 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. 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/IKEv2` log file. For more information, see LOGS Tab.

Next step

Configure the remote access clients to connect to the client-to-site VPN.

For more information, see Remote Access Clients.

Figures

1. Client2SiteIPsecVPN.png
2. C2S_IKEv2_01.png
3. C2S_IKEv2_02.png
4. C2S_IKEv2_02a.png
5. C2S_IKEv2_02b.png
6. C2S_IKEv2_03.png
7. C2S_IKEv2_04.png
8. C2S_IKEv2_05.png
9. C2S_IKEv2_06.png
10. C2S_IKEv2_07.png
11. C2S_IKEv2_08.png
12. C2S_IKEv2_09.png
13. C2S_IKEv2_11.png
14. C2S_IKEv2_10.png