Example - Client-to-Site IKEv1 IPsec VPN with Client Certificate Authentication

https://campus.barracuda.com/doc/50660162/

Use a client-to-site VPN to let mobile workers connect securely to your Barracuda NextGen Firewall F-Series. Each client must have a valid client certificate as well as the username and password to authenticate. 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. 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. You can connect from any IPv4 or IPv6 address, as long as an external IPv4 and IPv6 address are configured as a service IP address for the VPN service. Traffic passing through the client-to-site VPN is limited to IPv4.

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.
- Native iOS IPsec VPN Client
- Native Android IPsec VPN Client

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 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 External CA VPN Certificates.
- Configure an external or local authentication service. 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.
- 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. 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. 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](#).

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.
      - **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 Barracuda NextGen Firewall F-Series leads to the local network.

5. Click **OK**.

6. Click **Send Changes** and then click **Activate**.
Step 3. 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 check box.
   2. In the Server section, select your previously configured authentication service from the Authentication Scheme list. For more information, see Authentication.
6. Click OK.
7. Click Send Changes and Activate.

Step 4. 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.,
0(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.
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.

8. Configure the group policy.
   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 check box is selected.
   4. In the X509 Certificate Conditions section, enter matching conditions for the X.509 client certificates.
9. Click OK.
10. Configure the encryption and hashing settings:
   1. Click the **IPSec IKEv1** tab.
   2. Clear the check box 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** for iOS and Android 5.2 or lower. Select **SHA256** for Android 6.0.
      - **DH-Group** – Select **Group2**.
      - **Time** – Enter 3600.
      - **Minimum** – Enter 1200.
      - **Maximum** – Enter 28800.
5. 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.

6. Click **OK**.

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

**Step 5. 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.

![VPN Connections](image)

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**.

Next Steps

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. vpn_service_listeners.png
3. PSK01.png
4. PSK03.png
5. PSK04.png
6. PSK05.png
7. PSK06.png
8. PSK07.png
9. C2S_00.png
10. C2S_01.png
11. C2S_status_connected.png

© Barracuda Networks Inc., 2023 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.