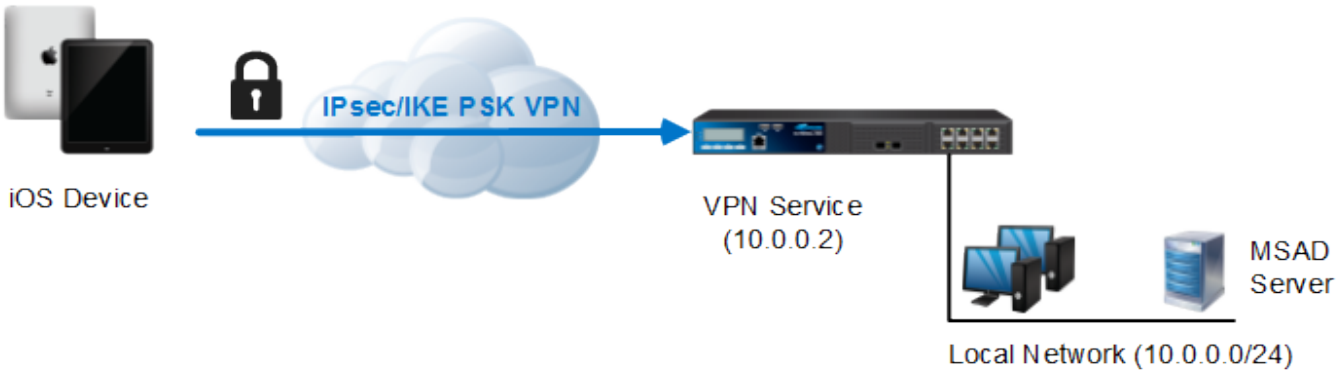
How to Configure a Client-to-Site IPsec VPN with PSK

https://campus.barracuda.com/doc/41116187/

To let users access a client-to-site IPsec VPN without having to install X.509 certificates on their client devices, you can configure a preshared key (PSK). For users with mobile devices that are not managed by a mobile device management platform (MDM), using a PSK is more convenient than having to install certificates for authentication.

The connection is set up in two phases by the Internet Key Exchange (IKE). In phase I, the PSK is used to create a secure channel over which phase II negotiates the security associations for the IPsec service.

Follow the instructions in this article to configure a client-to-site IPsec VPN with PSK. You must also configure MSAD to authenticate users.



In this article:

Supported VPN Clients

Currently, only Apple iOS and Android devices are supported with IPsec VPNs with PSK.

- For instructions on how to configure Apple iOS for IPsec PSK, see How to Configure Apple iOS Devices for Client-to-Site IPsec VPNs with PSK.
- For instructions on how to configure Android devices for IPsec PSK, see How to Configure Android Devices for Client-to-Site IPsec VPNs with PSK.

Before You Begin

Before you implement a client-to-site VPN with IPsec PSK with external authentication using MSAD:

- Verify that the VPN service has been properly configured and that the **server** and **default certificates** are installed. The certificate must use DNS:*FQDN (e.g., DNS:vpn.mydomain.com*) as the **SubAltName** 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 VPN Certificates.
- Verify that MSAD is configured. For more information, see How to Configure MSAD Authentication.
- Identify the subnet and gateway address for the VPN service in your network (e.g., `192.168.6.0/24` *and* `192.168.6.254`).
- Identify the IP address on which the VPN service will listen (e.g., `10.0.0.2`).

Configure the Client-to-Site VPN Service

To implement a client-to-site VPN with IPsec PSK and external username and password authentication using MSAD, complete the following steps.

Step 1. Configure the Client Network and Gateway and PSK Key

1. Open the **VPN Settings** page (**Config > Full Config > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN Service**).
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, seeHow to Set Up VPN Certificates.
4. In the **Server Settings** window click on the **Advanced** tab.
5. In the **IKE Parameter** section enter the **IKE PSK** key. E.g., `pre$haredKey`
   If you are using firmware version 5.4.2 with hotfix 559, the PSK has to be configured in the **L2TP/PPTP Settings** in the **IPsec Settings** section.
6. Configure the client network.
    1. Click the **Client Networks** tab.
    2. Right-click the table and select **New Client Network**.
    3. In the **Client Network** window, configure the following settings:

Setting	Description

Name	A descriptive name for the network (e.g., `Client to Site VPN Network`).
Network Address	The default network address. All VPN clients will receive an IP address in this network (e.g., `192.168.6.0`).
Network Mask	The appropriate subnet mask (e.g., `24`).
Gateway	The gateway network address (e.g., `192.168.6.254`).
Type	The type of network that is used for VPN clients. From this list, 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 NG Firewall leads to the local network.

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

Step 2. Configure VPN Group Match Settings

Configure the global authentication settings for VPN tunnels using an external X.509 certificate and group configurations.

1. Open the **Client to Site** page (**Config > Full Config > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN Service**).
2. Click **Lock**.
3. Click the **External CA** tab.
4. Click the **Click here for options** link.
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 **msad** from the **Authentication Scheme** list.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Step 3. Create a VPN Group Policy

The **VPN Group Policy** specifies the network IPsec settings. You can create 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., `O(Organization)` must be the company name).

1. Open the **Client to Site** page (**Config > Full Config > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN Service**).
2. Click **Lock**.
3. Click on the **External CA** tab and then click the **Group Policy** tab.
4. Right-click the table and select **New Group Policy**. The **Edit Group Policy** window opens.
5. Enter a name for the **Group Policy**. For example, `IPsecPSKGroupPolicyName`.

    The name of the group policy is used to associate VPN clients with the correct group policy. Most VPN clients call it **group name** or **IPsec identifier**.

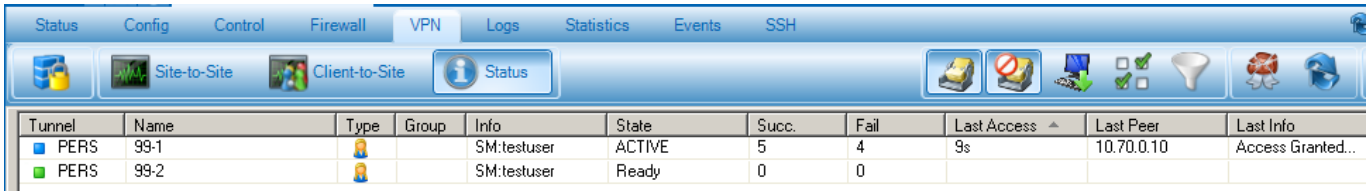
6. From the **Network** list, select the VPN client network.
7. In the **Network Routes** table, enter the network that must be reachable through the VPN connection. For example, `10.0.0.0/24.`
8. Configure the group policy.
    1. Right-click the **Group Policy Condition** table and select **New Rule**.
    2. In the **Group Pattern** field, define the groups that will be assigned the policy. For example: `CN=vpnusers*`
    3. Click **OK**.
9. To change the encryption algorithm:
    1. Click the **IPSec** tab.
    2. Clear the check box in the right top 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:
        - **Encryption:** AES
        - **Hash Meth.:** SHA
        - **DH-Group:** *Group2*
        - **Time**: 3600
        - **Minimum**: 1200
        - **Maximum**: 28800
    5. Click **Edit IPsec Phase I** and select the encryption algorithm in the **For XAuth Authentication** section:
        - **Encryption:** AES
        - **Hash Meth.:** SHA
        - **DH-Group:** Group2
        - **Time**: 3600
        - **Minimum**: 1200
        - **Maximum**: 86400
    6. Click **OK** to close the **Change IPSec Phase I** window.
10. Click **OK**.
11. Click **Send Changes** and **Activate**.

Step 4. Add Firewall Rules

Add two forwarding firewall rules to connect your client-to-site VPN to your network. For instructions, see How to Configure a Forwarding Firewall 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 not in use.
- **Grey –** The VPN tunnel is 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. Client2SiteIPsecXAUTHPSKVPN.png
2. ngadmin_vpn_status_client_to_site.PNG