How to configure a Roadwarrior OpenVPN connection with X.509 and PSK authentication in Panda GateDefender eSeries

'How-to' guides for configuring VPNs in Panda GateDefender eSeries

Panda Security wants to ensure you get the most out of Panda GateDefender eSeries. For this reason, we offer you all the information you need about the characteristics and configuration of the product. Refer to http://www.pandasecurity.com and http://www.pandasecurity.com/enterprise/support/gatedefender-performa-eseries.htm for more information.

'How-to' guides for Panda GateDefender eSeries

The software described in this document is delivered under the terms and conditions of the end user license agreement and can only be used after accepting the terms and conditions of said agreement.

Bothe the anti-spam and web filtering technologies in this product are provided by CYREN.

CONTENTS

LIST OF FIGURES

Introduction

This document details the steps to take to configure a Roadwarrior OpenVPN connection with X.509 and PSK authentication in Panda GateDefender eSeries.

> **IMPORTANT**: Even though in Panda GateDefender eSeries by default when an OpenVPN Server is enabled both a server instance and a CA certificate are already created, the present document will explain the entire process step by step from the start.

Therefore, the starting point will be a server without instances configured or CA certificates created.

How to configure a Roadwarrior OpenVPN connection with X.509 and PSK authentication

1. Create a ROOT (CA) certificate

Note:If, when accessing your Panda GateDefender eSeries unit, you see a screen similar to Figure 3, go to step 2: Create an OpenVPN.

This certificate will be used to sign the other certificates (client/server).

I. Go to the Panda GateDefender eSeries administration console.

II. Go to **VPN→ Certificates**. In the tab **Certificate Authority**, click **Generate new root/host certificates**.

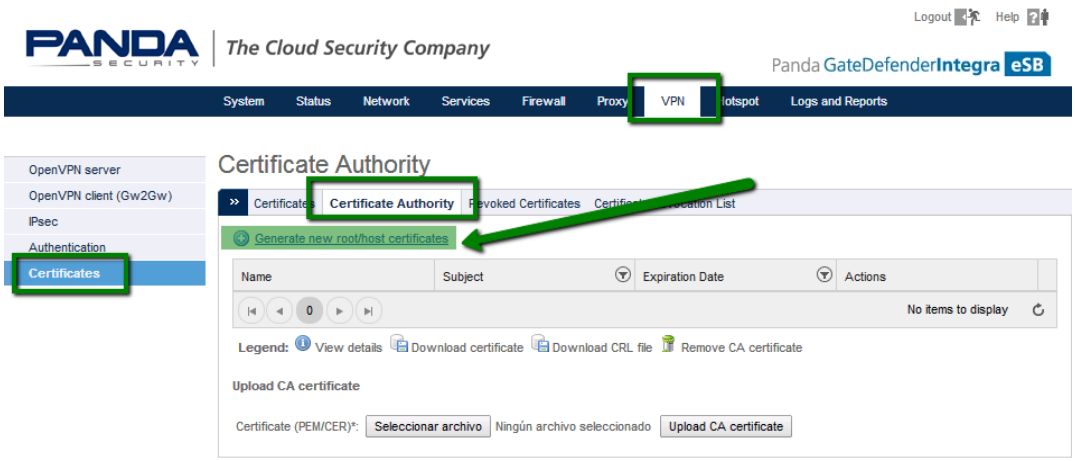

Figure 1 - Generate new root/host certificates

III. Fill in the data required.

Fields **System hostname** and **Organization name** are mandatory.

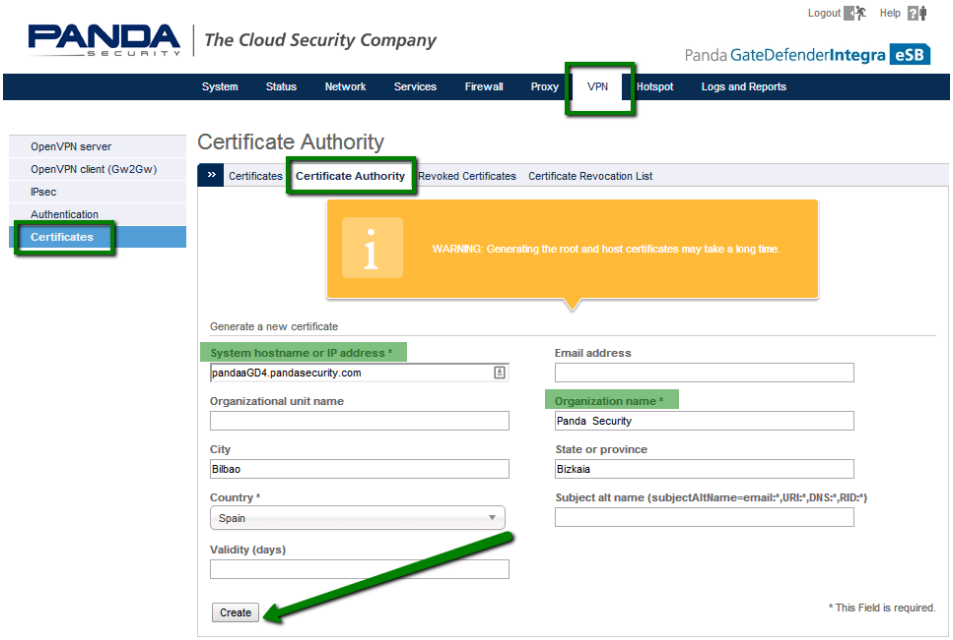

Figure 2 - Fill in the data required

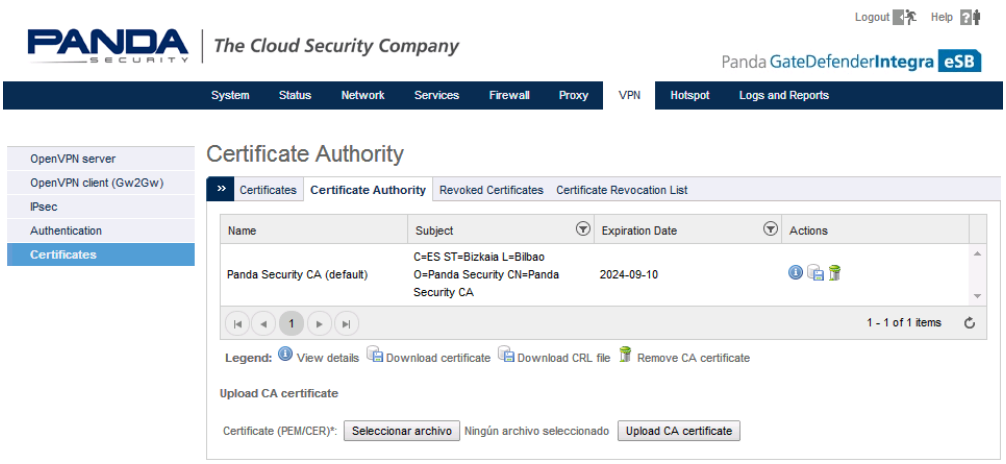

Figure 3 - Root certificate created

IV. After the ROOT (CA) certificate has been created, the server certificate will be automatically generated.

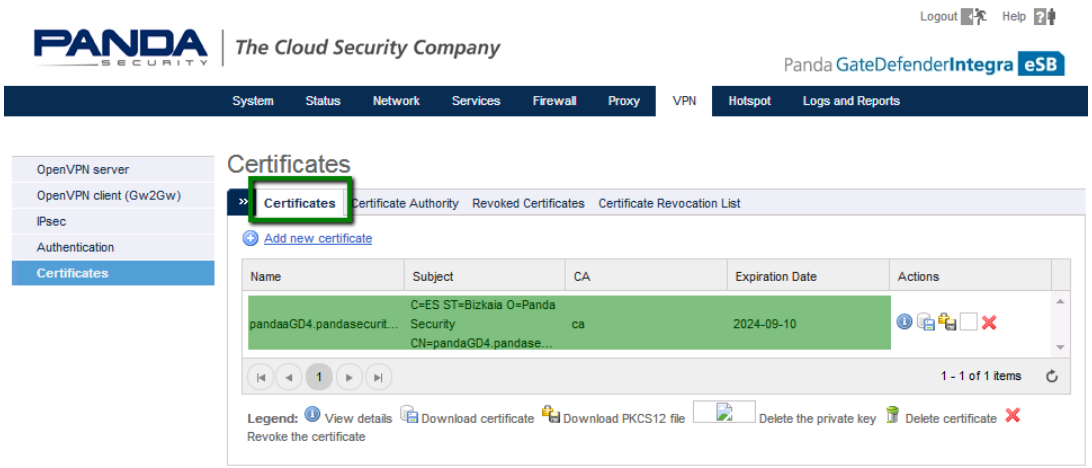

Figure 4 - Server certificate created

2. Create an OpenVPN server instance

Note: If, when accessing this section, you see a screen similar to Figure 5, go to step 3- Create the client certificate for the Roadwarrior.

I. Go to **VPN→ OpenVPN server**.

II. Enter a name and the port that the OpenVPN server instance will listen on.

III. Select a device type:

- TAP: Recommended for PCs, laptops, etc.
- TUN: Recommended when the Roadwarriors are mobile devices (iOS, Android).

Important: Bear in mind that both ends of the VPN connection must have the same type of interface configured.

In our example, we have selected **TAP** and assigned an IP address range that was available in the remote environment.

IV. Select **Enabled** and click **Add** to apply the changes.

V. After the Server instance has been created, select the server certificate to use and the authentication type.

In our example, we have selected ***X.509 Certificate & PSK (two factor)***, and ***Use an existing certificate*** as the authentication type.

VI. The system will display the certificate that was automatically created when the ROOT certificate was generated (see Figure 4 - Server certificate created).

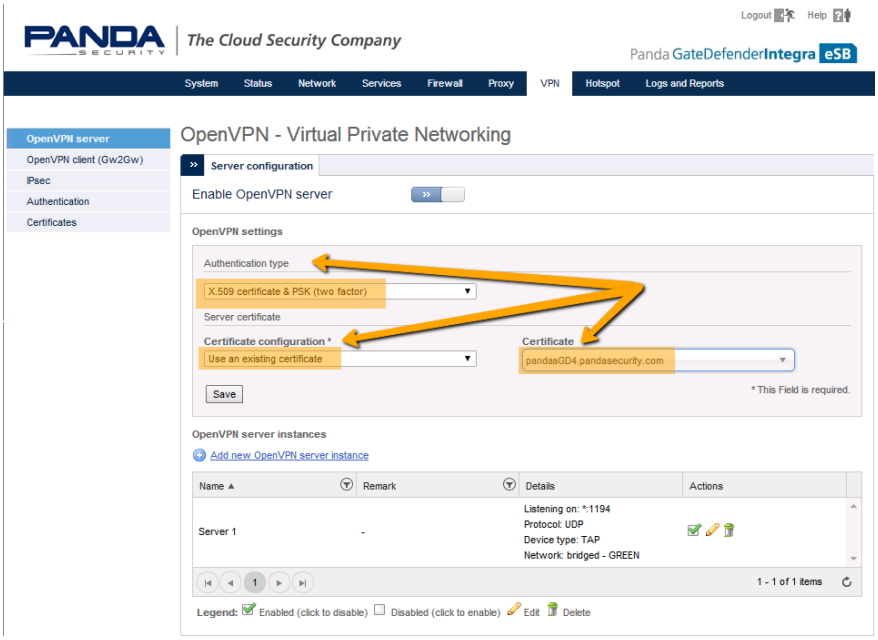

Figure 5 - Configure the certificate

VII. Click **Save** to save the information. The end result should be similar to this.

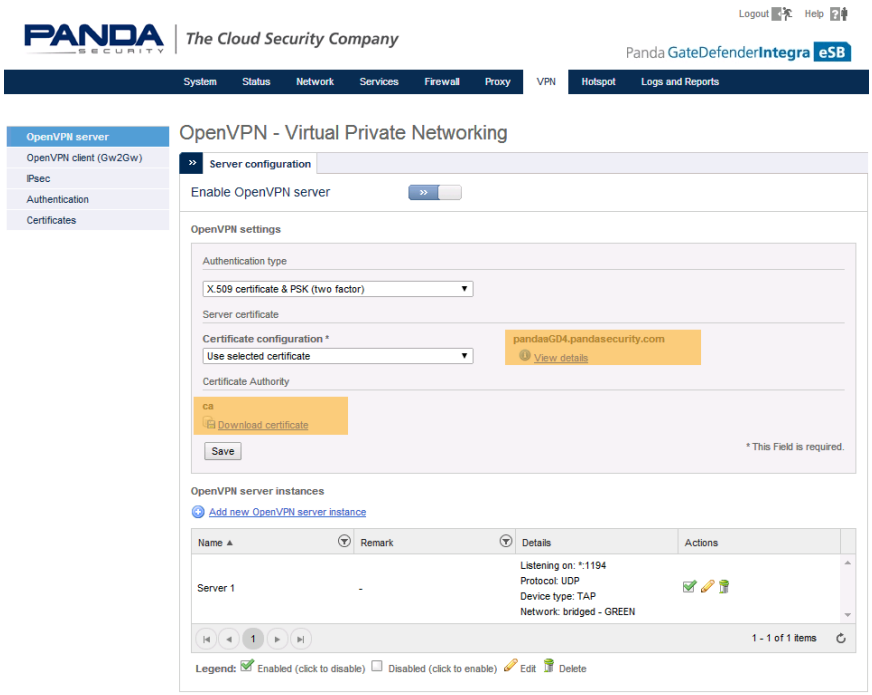

Figure 6 - Certificate created

3. Create the client certificate for the Roadwarrior user(s)

Next, it will be necessary to create the Client certificate to be used by the Roadwarrior (remote user) that will establish the connection.

You can create certificates for each individual Roadwarrior user or for user groups. That is, each Roadwarrior user can use their own certificate or share a certificate with other users.

I. Go to ***Certificates*** and click the ***Add new certificate*** link.

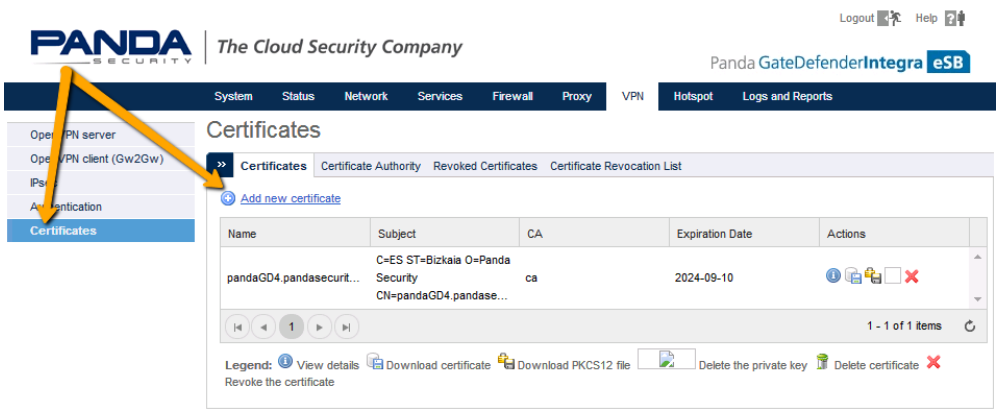

Figure 7 - Add a new certificate

II. Fill in the different fields:

- Certificate name
- Certificate type
  IMPORTANT: Select **CLIENT**.
- **PKCS12 file password.**
  Note: This password must be sent to the Roadwarrior user(s).

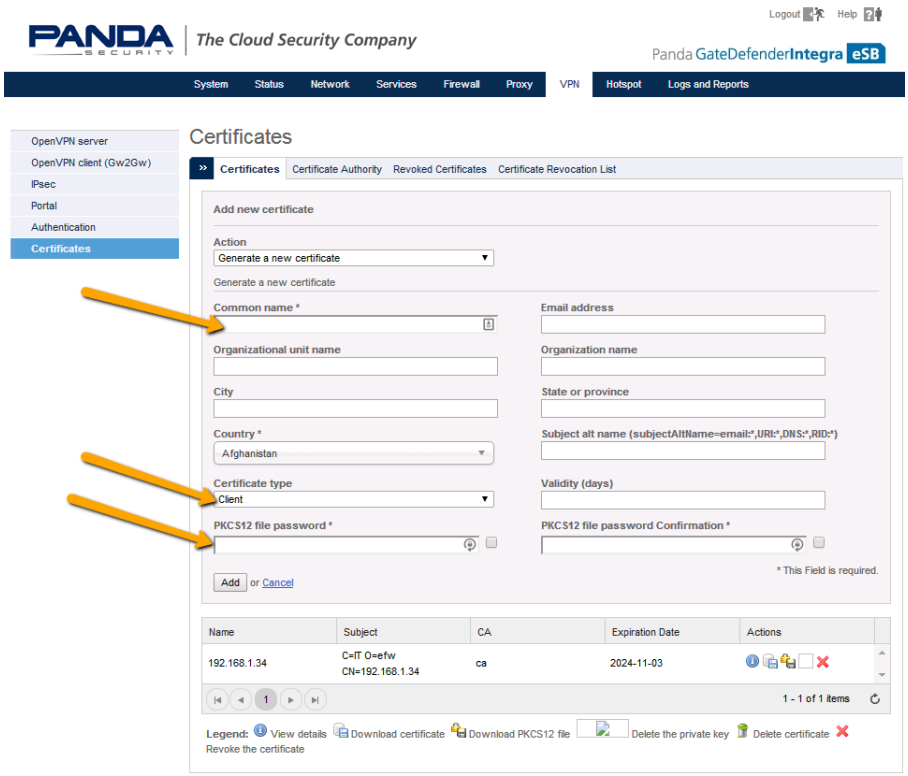

Figure 8 - Fill in the certificate data

III. Click **Add** to generate the certificate.

IV. Next, click the padlock icon to download the PKCS12 key.

Send this file and its password to the Roadwarrior user.

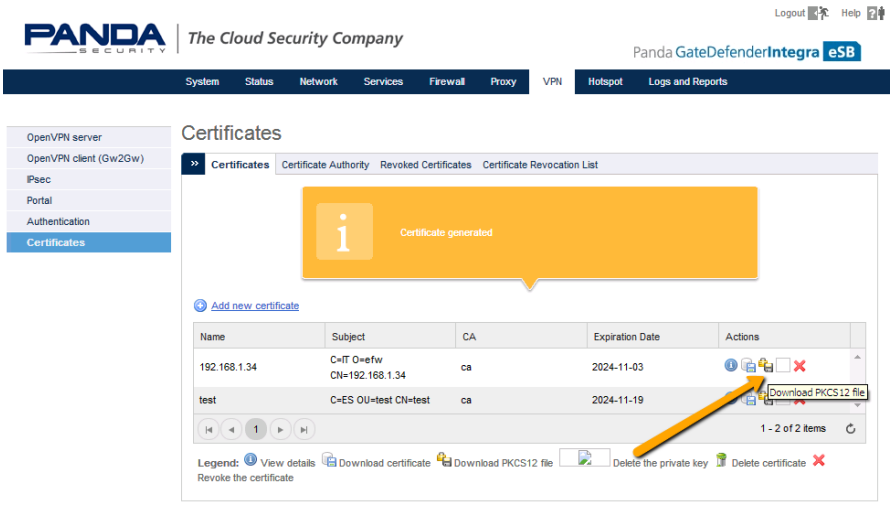

Figure 9 - Certificate generated

4. Create the Roadwarrior user that will establish the connection from a remote PC

I. Go to **VPN→ Authentication**.

II. Click the **Add new local user** link to create a new user.

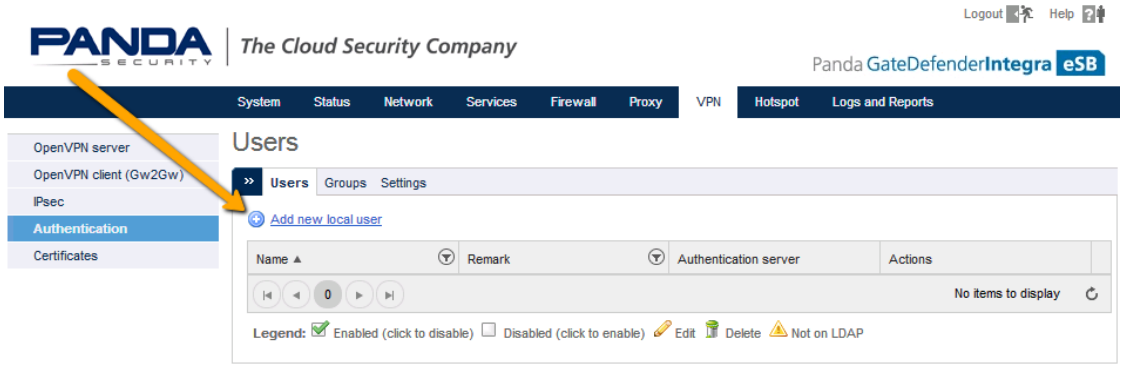

Figure 10 - Add a new local user

III. Enter a username and a password.

IV. As the Client certificate has been previously generated, select ***Don't change*** in the **Certificate Configuration** field.

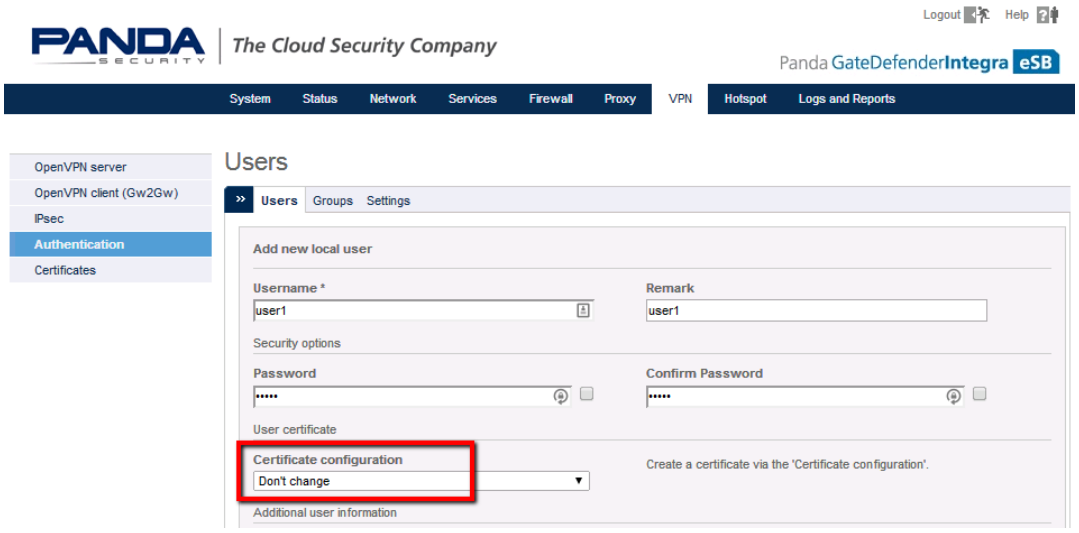

Figure 11 - Configure the certificate

In our example, all other fields will be left with the default options.

V. Apply the changes.

VI. The user created should look like this:

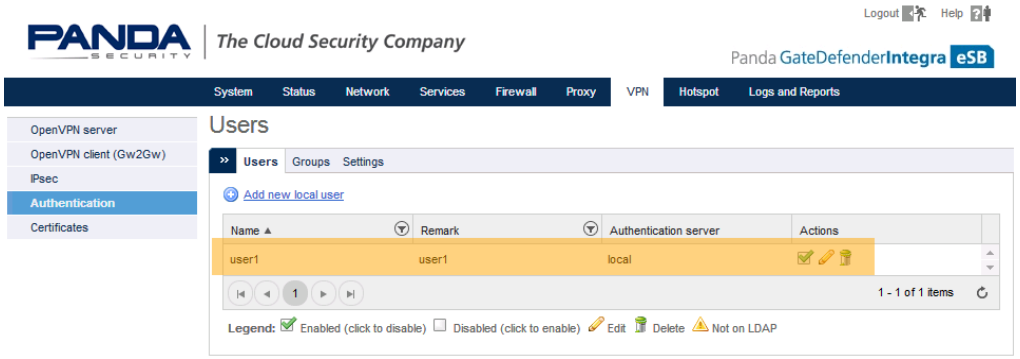

Figure 12 - User created

5. Install and configure the OpenVPN Client

I. Access the Panda Perimetral Management Console.
https://managedperimeter.pandasecurity.com

II. Download and install the OpenVPN client that is appropriate for the system.

Figure 13 - Download the VPN Client

III. Create a VPN profile.

The following data will be required:

i. The PKCS12 file. In our example, **user1cert.p12**

ii. The PKCS12 file password

iii. Public IP address and connection port

iv. Roadwarrior username and password

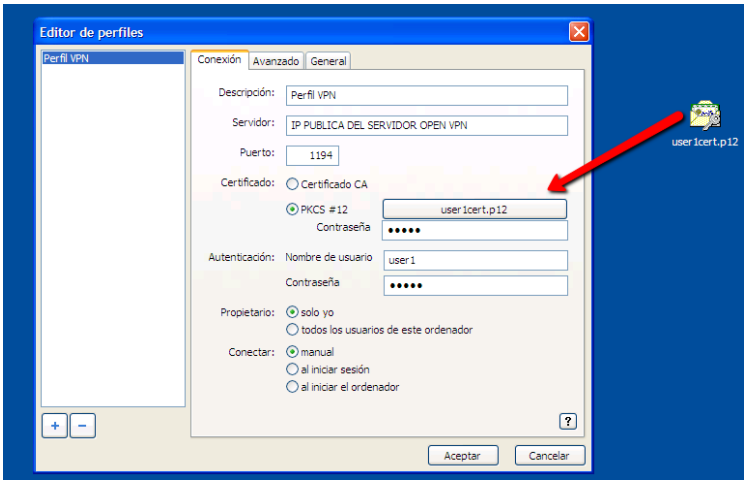

Figure 14 - Create the VPN profile

IV. Click ***OK*** to save the changes.

After these steps have been completed, the new profile will be created and it will be possible to establish the connection.