

Cómo configurar Open VPN Roadwarrior con autenticación X.509 y PSK en Panda GateDefender eSeries

Casos de uso para configurar VPNs con Panda GateDefender eSeries

Panda Security desea que obtenga el máximo beneficio de sus unidades GateDefender eSeries. Para ello, le ofrece la información que necesite sobre las características y configuración del producto. Consulte <http://www.pandasecurity.com/> y <http://www.pandasecurity.com/spain/enterprise/support/gatedefender-performa-eseries.htm> para más información.

El software descrito en este documento se entrega bajo un Acuerdo de Licencia y únicamente puede ser utilizado una vez aceptados los términos del citado Acuerdo.

La tecnología anti-spam y de filtrado web incluidas en este producto pertenecen a CYREN.

Aviso de Copyright

© Panda 2015. Todos los derechos reservados. Ni la documentación, ni los programas a los que en su caso acceda, pueden copiarse, reproducirse, traducirse o reducirse a cualquier medio o soporte electrónico o legible sin el permiso previo por escrito de Panda, C/ Gran Vía, 4 48001 Bilbao (Vizcaya) ESPAÑA.

Marca Registrada

Panda Security™. TruPrevent es una marca registrada en la Oficina de Patentes y Marcas de EEUU. Windows Vista y el logo de Windows son marcas o marcas registradas de Microsoft Corporation en los EEUU y/o otros países. Otros nombres de productos son marcas registradas de sus respectivos propietarios.

© Panda 2015. Todos los derechos reservados.

TABLA DE CONTENIDOS

Introducción	3
Pasos para configurar una conexión Open VPN Roadwarrior con autenticación X.509 y PSK	3
1. Crear el certificado ROOT o CA	3
2. Crear una instancia de servidor Open VPN	5
3. Crear el Certificado cliente para el usuario/s Roadwarrior/s	7
4. Crear el usuario RoadWarrior que conectará desde un PC remoto	9
5. Instalar y configurar el Cliente Open VPN	11

TABLA DE FIGURAS

Figura 1 - Generar nuevos certificados root/host	4
Figura 2 - Completar los campos requeridos	4
Figura 3 - Certificado Root creado	5
Figura 4 - Certificado servidor creado	5
Figura 5 - Configuración del certificado	6
Figura 6 - Certificado creado	7
Figura 7 - Añadir nuevo certificado	7
Figura 8 - Completar datos del certificado	8
Figura 9 - Certificado generado	9
Figura 10 - Añadir nuevo usuario local	9
Figura 11 - Configuración del certificado	10
Figura 12 - Usuario creado	10
Figura 13 - Descargar Cliente VPN	11
Figura 14 - Crear Perfil VPN	12

Introducción

En este documento se indican los pasos a seguir para configurar una conexión Open VPN Roadwarrior con autenticación X.509 y PSK en Panda GateDefender eSeries.

IMPORTANTE: Aunque en Panda GateDefender eSeries por defecto cuando se activa el servidor OpenVPN ya están creadas tanto una instancia de servidor como un certificado CA, en este documento se va a explicar el proceso desde el inicio, paso a paso.

Por lo tanto, el punto de partida es un servidor sin instancias configuradas y sin un certificado CA (autoridad certificadora) creado.

Pasos para configurar una conexión Open VPN Roadwarrior con autenticación X.509 y PSK

1. Crear el certificado ROOT o CA

Nota: Si al acceder a su dispositivo Panda GateDefender eSeries ve una imagen similar a Figura 3, vaya al paso 2: Crear una instancia de servidor Open VPN.

Este certificado se utilizará para firmar el resto de certificados (cliente/servidor).

- I. Acceder a la consola de administración de Panda GateDefender eSeries.
- II. Ir a **VPN** → **Certificados**, y en la pestaña **Certificate Authority**, pulsar **Generate new root/host certificates**.

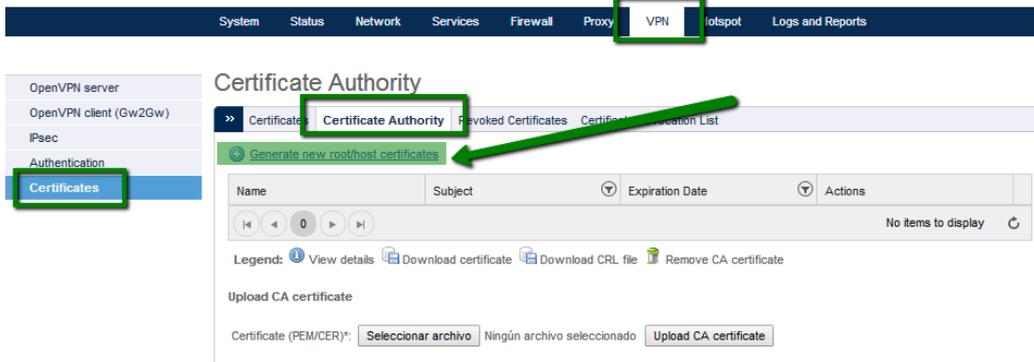


Figura 1 - Generar nuevos certificados root/host

III. Introducir los datos solicitados.

Los campos **Nombre del sistema** y **Nombre de la organización** son obligatorios.

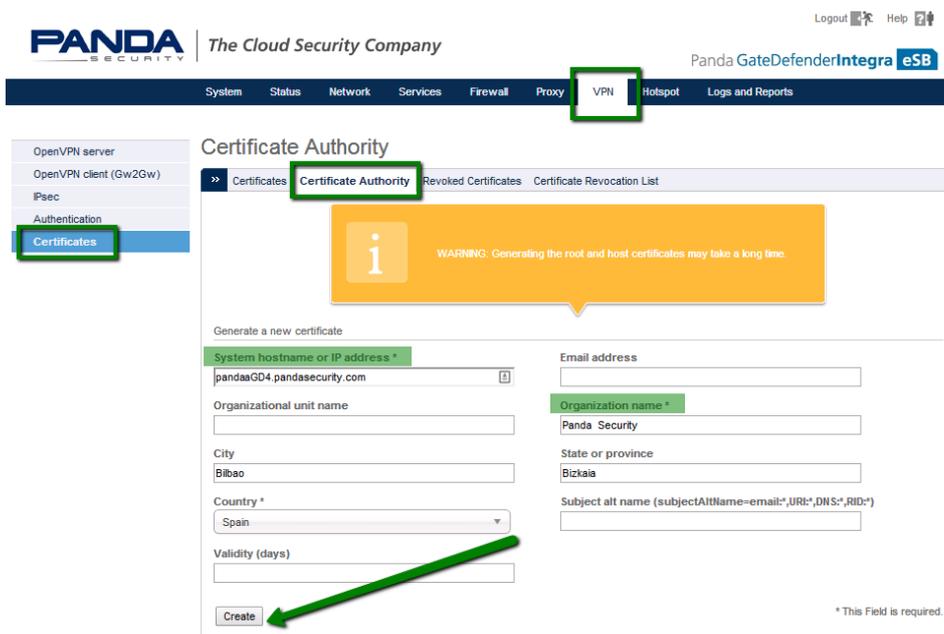


Figura 2 - Completar los campos requeridos

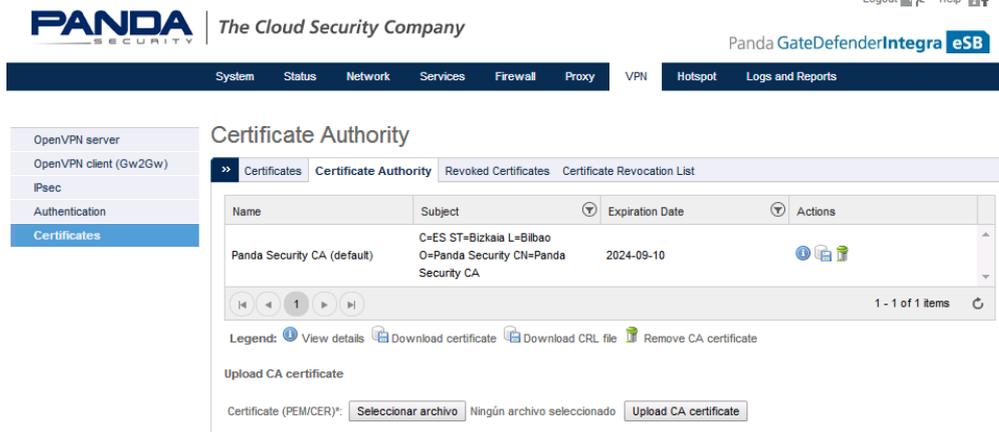


Figura 3 - Certificado Root creado

IV. Una vez creado el certificado ROOT (CA), se generará automáticamente el certificado servidor.

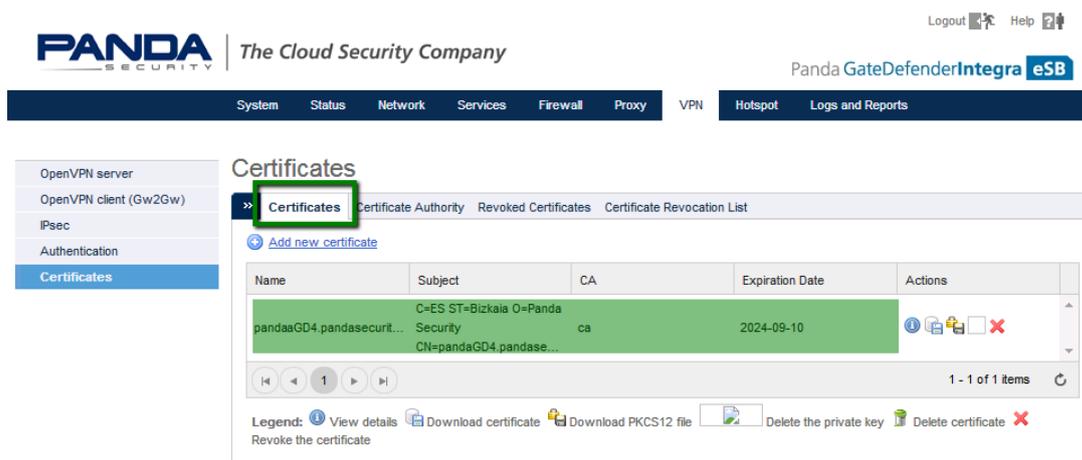


Figura 4 - Certificado servidor creado

2. Crear una instancia de servidor Open VPN

Nota: Si al acceder a esta sección ve una imagen similar a la Figura 5, vaya al paso 3- Crear el Certificado cliente para el usuario/s Roadwarrior/s.

- I. Ir a **VPN** → **OpenVPN server**.
- II. Añadir el nombre y el puerto por el cual estará escuchando esta instancia de servidor OpenVPN.

III. Seleccionar tipo de dispositivo:

- TAP: Recomendado para PC's, portátiles, etc.
- TUN: Recomendado cuando los RoadWarriors son dispositivos móviles, tipo iOS o Android.

Importante: Tenga en cuenta que ambos extremos de la VPN deben tener configurado el mismo tipo de interfaz.

En este ejemplo se ha elegido **TAP** y se ha asignado un rango de IPs disponibles en el entorno remoto.

- IV. Marcar la casilla **Activado** y hacer clic en el botón **Save** para aplicar los cambios.
- V. Una vez creada la instancia Servidor, seleccionar el certificado servidor que se va a utilizar y el tipo de autenticación.

En este ejemplo, se selecciona **X.509 Certificate & PSK (two factor)** y en tipo de autenticación, **Use an existing certificate**.

- VI. En este momento, se mostrará el certificado que fue creado automáticamente al generar el certificado ROOT (ver Figura 4 - Certificado servidor creado).

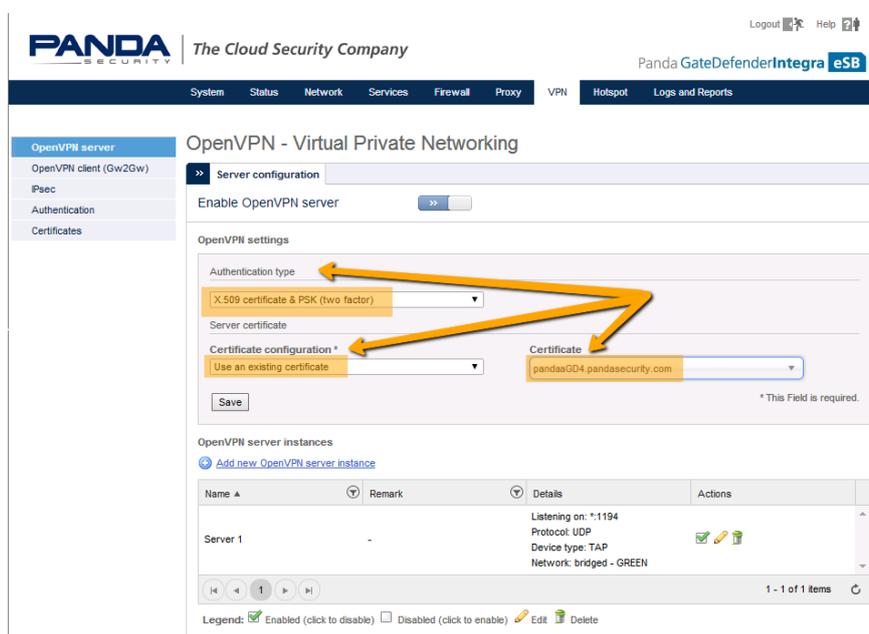


Figura 5 - Configuración del certificado

- VII. Pulsar **Save** para guardar la información. El resultado final será similar a la siguiente imagen.

System Status Network Services Firewall Proxy VPN Hotspot Logs and Reports

OpenVPN server
OpenVPN client (Gw2Gw)
IPsec
Authentication
Certificates

OpenVPN - Virtual Private Networking

Server configuration

Enable OpenVPN server

OpenVPN settings

Authentication type
X.509 certificate & PSK (two factor)

Server certificate
Certificate configuration *
Use selected certificate pandasGD4.pandasecurity.com [View details](#)

Certificate Authority
ca [Download certificate](#)

Save * This Field is required.

OpenVPN server instances

[Add new OpenVPN server instance](#)

Name	Remark	Details	Actions
Server 1	-	Listening on: *1194 Protocol: UDP Device type: TAP Network: bridged - GREEN	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Legend: Enabled (click to disable) Disabled (click to enable) Edit Delete

Figura 6 - Certificado creado

3. Crear el Certificado cliente para el usuario/s Roadwarrior/s

A continuación es necesario crear el certificado Cliente que utilizará el usuario Roadwarrior remoto que se va a conectar.

Se pueden generar certificados diferentes para cada usuario Roadwarrior o para grupos de usuarios. Es decir, cada usuario Roadwarrior puede emplear un certificado independiente o puede compartir el mismo certificado para diferentes usuarios.

- I. Ir a **Certificates** y pulsar el enlace **Add new certificate**.

System Status Network Services Firewall Proxy VPN Hotspot Logs and Reports

Panda GateDefenderIntegra eSB

Certificates

Certificate Authority Revoked Certificates Certificate Revocation List

[Add new certificate](#)

Name	Subject	CA	Expiration Date	Actions
pandaGD4.pandasecurit...	C=ES ST=Bizkaia O=Panda Security CN=pandaGD4.pandase...	ca	2024-09-10	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Legend: View details Download certificate Download PKCS12 file Delete the private key Delete certificate Revoke the certificate

Figura 7 - Añadir nuevo certificado

II. Completar los diferentes campos:

- Nombre para el certificado
- Tipo de certificado
IMPORTANTE: Hay que seleccionar el tipo de certificado **CLIENT**.
- Contraseña en el campo **PKCS12 file password**.
Nota: Esta contraseña debe ser remitida al usuario/s RoadWarrior.

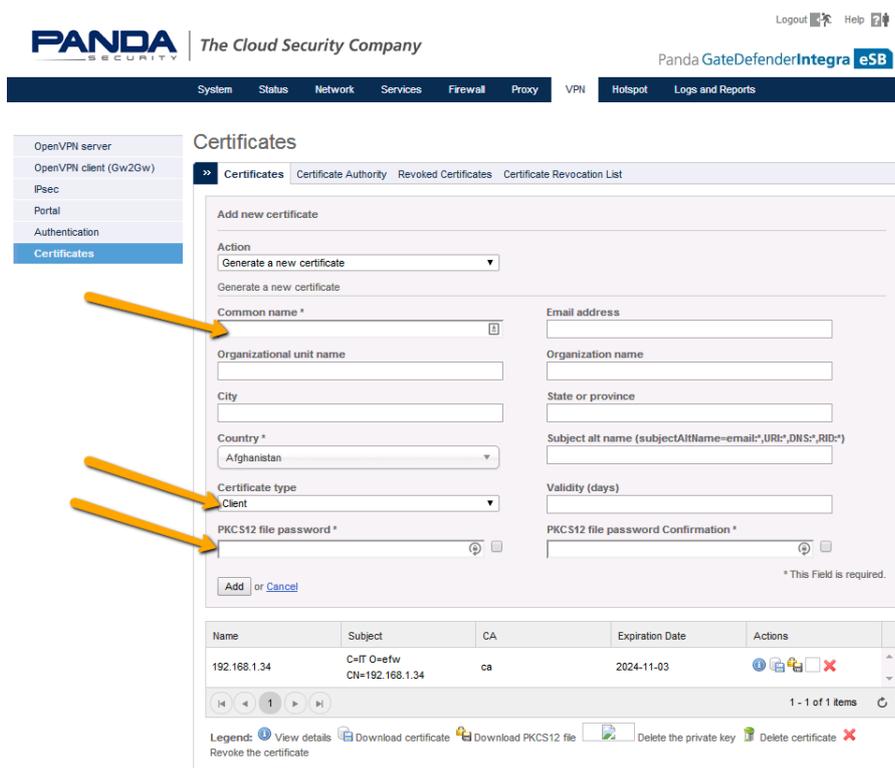


Figura 8 - Completar datos del certificado

- III. Pulsar **Add** para generar el certificado.
- IV. A continuación, pulsar el icono del candado para descargar la clave PKCS12.
- Se deberá remitir este archivo y su contraseña al usuario Roadwarrior.

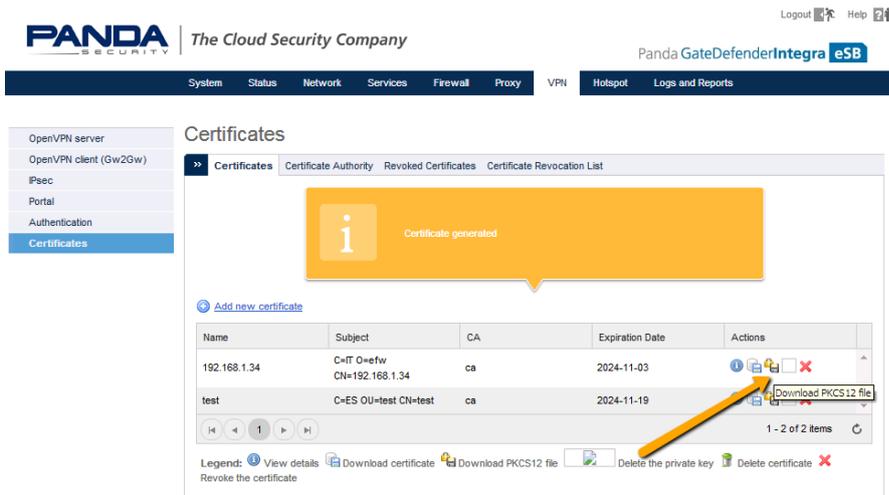


Figura 9 - Certificado generado

4. Crear el usuario RoadWarrior que conectará desde un PC remoto

- I. Ir a **VPN** → **Authentication**.
- II. Pulsar el enlace **Add new local user** para crear un nuevo usuario.

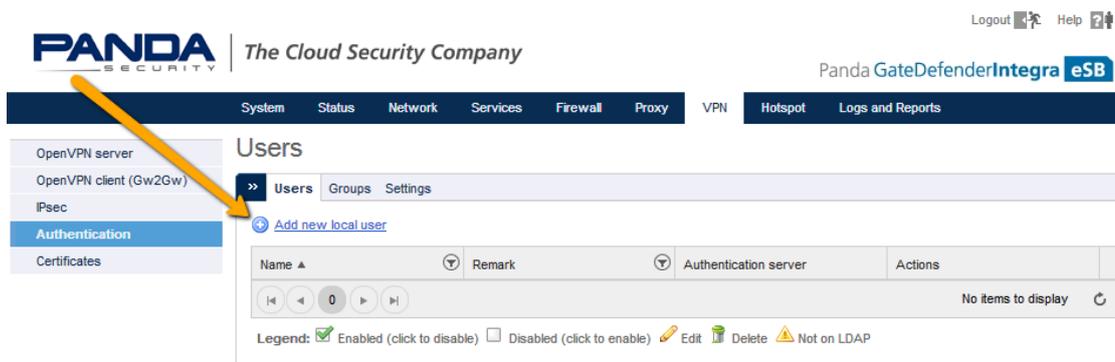


Figura 10 - Añadir nuevo usuario local

- III. Introducir un nombre único y una contraseña.
- IV. Como se ha generado el certificado Cliente previamente, en el campo **Certificate Configuration** se debe seleccionar **Don't change**.

System Status Network Services Firewall Proxy VPN Hotspot Logs and Reports

OpenVPN server
OpenVPN client (Gw2Gw)
IPsec
Authentication
Certificates

Users

>> Users Groups Settings

Add new local user

Username * Remark

Security options

Password Confirm Password

User certificate

Certificate configuration Create a certificate via the 'Certificate configuration'.

Additional user information

Figura 11 - Configuración del certificado

En este ejemplo, los campos restantes se dejan por defecto.

- V. Aplicar los cambios.
- VI. El usuario creado se verá como en la siguiente imagen:

System Status Network Services Firewall Proxy VPN Hotspot Logs and Reports

OpenVPN server
OpenVPN client (Gw2Gw)
IPsec
Authentication
Certificates

Users

>> Users Groups Settings

[Add new local user](#)

Name	Remark	Authentication server	Actions
user1	user1	local	<input checked="" type="checkbox"/> <input type="checkbox"/>

1 - 1 of 1 items

Legend: Enabled (click to disable) Disabled (click to enable) Edit Delete Not on LDAP

Figura 12 - Usuario creado

5. Instalar y configurar el Cliente Open VPN

- I. Acceder a la consola de gestión perimetral Panda Perimetral Management Console.
<https://managedperimeter.pandasecurity.com>
- II. Descargar e instalar el cliente Open VPN adecuado para el sistema.

Panda Perimetral Management Console

Log out PANDA SECURITY

My Account Systems Activationcodes Actions Account Downloads

GateDefender VPN Client

GateDefender Installation Images

438 Firewalls total!
281 are online
155 need to be updated
283 are up to date
77 are expired

Service Status
All services are online
More information
Service status updates

Panda GateDefender VPN Client

The Panda GateDefender VPN Client is an all-in-one solution to communicate with your OpenVPN servers. The VPN software features an easy to use graphical user interface which deals with all the hurdles coming with the setup of an OpenVPN connection.

Windows

Windows Installer (msi)
MD5 checksum: f42c8c929e3af95d62d21d713c3888c8

Mac OS X

Mac OS X (dmg)
MD5 checksum: eea94939ee2af906b179ccc0c14f08ac

Linux

The previously maintained Ubuntu package has been discontinued as Ubuntu already supports OpenVPN connections in its network manager. It is necessary to install the network-manager-openvpn package by running this command:
`sudo apt-get install network-manager-openvpn`
Additional information can be found at the [Ubuntu help page](#).

Figura 13 - Descargar Cliente VPN

- III. Crear un perfil VPN.

Para ello se necesitarán los siguientes datos:

- i. El archivo PKCS12. En este ejemplo, **user1cert.p12**
- ii. La contraseña del archivo PKCS12
- iii. IP pública y puerto de la conexión
- iv. Usuario y contraseña del Roadwarrior

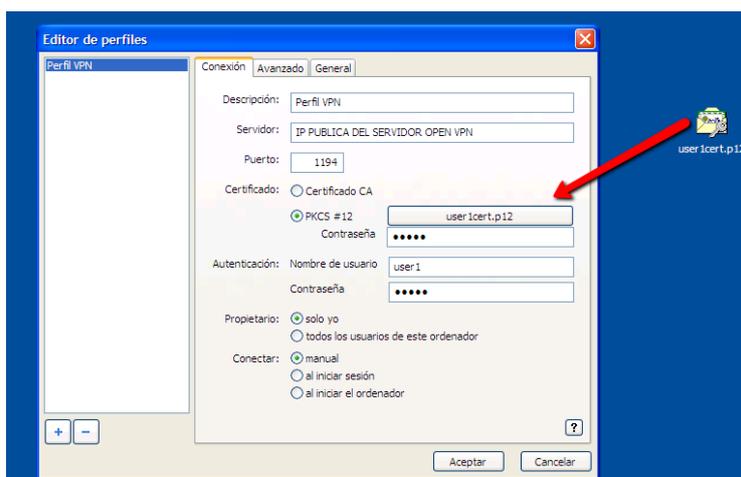


Figura 14 - Crear Perfil VPN

IV. Pulsar **Aceptar** para guardar los cambios.

El nuevo perfil será creado y podrá realizar la conexión.