

vpn,, ipsec,, certificados

## VPN ipsec con certificados

Vamos a realizar todo el proceso necesario para realizar conexiones a nuestro fortigate mediante certificados. Para ello necesitamos un crear una entidad certificadora, ya sea con un servidor Windows con el rol de AD CS(mirar las páginas de referencia), mediante openssl, o como en nuestro caso usando una aplicación para windows llamada XCA <http://xca.sourceforge.net/>.

Los pasos que vamos a seguir son:

1. Crear una entidad certificadora
2. Generar un certificado raíz
3. Generar certificados para los clientes de la vpn
  1. Generar un petición para los clienes desde el XCA
  2. Firmar la petición
  3. exportar el certificado firmado de cliente
  4. exportar desde el fortigate el certificado raíz CA\_Cert
  5. importar los certificados clientes y raíz al Forticlient
4. Crear vpn, políticas y usuarios en el fortigate

Una VPN con certificados nos garantiza una mayor seguridad, ya que por un lado usamos una clave de encriptación de mayor tamaño y por otro lado implica un segundo factor de autenticación ya que además del usuario/contraseña es necesario tener instalado un segundo elemento como es el certificado

### Crear una entidad certificadora

Nos bajamos el XCA y lo instalamos en nuestro equipo con permisos de administrador

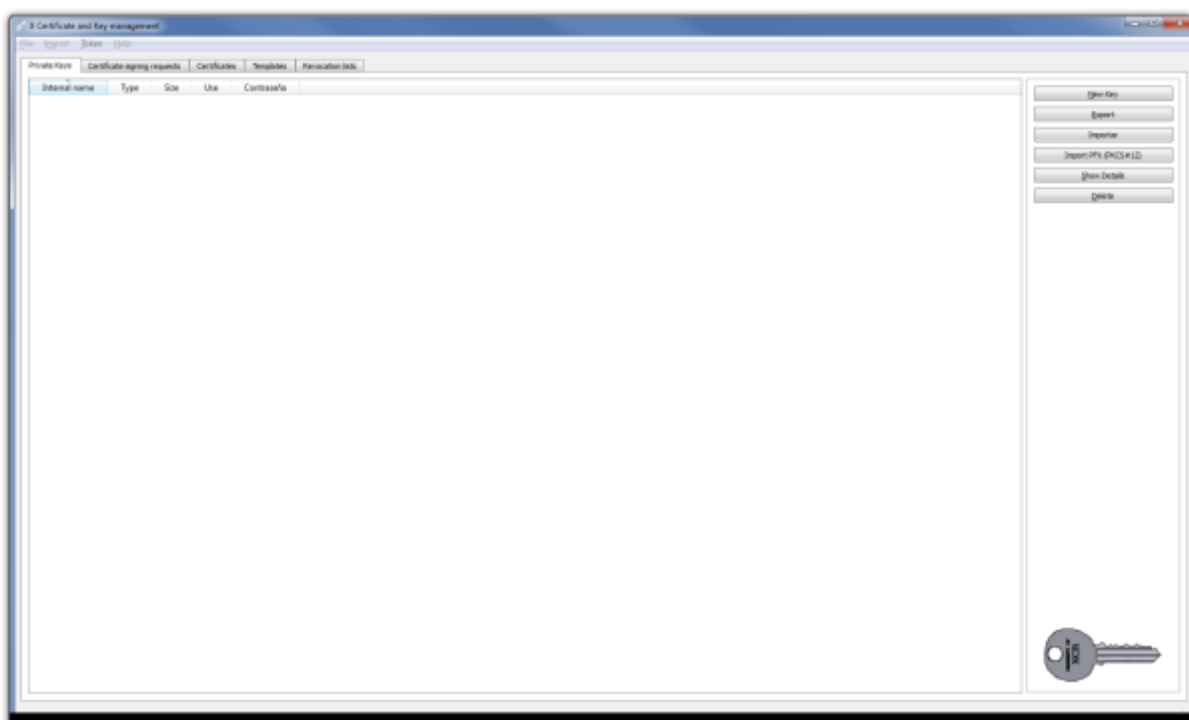
En XCA cada CA (Autoridad Certificadora)se almacena en un fichero con extensión \*.xdb. Se recomienda usar distintas bases de datos para cada PKI (Infraestructura de clave pública) que creemos.

Ejecutamos el programa Click File > New Database.

- En la ventana que se abre especificar el nombre y la ubicación donde se almacena el fichero con la base de datos XCA y pulsar guardar.
- Nos aparece una ventana donde debemos poner una contraseña para encriptar el fichero de la base de datos. Esa contraseña es necesaria para cada vez que vayamos a abrir esa base de datos.

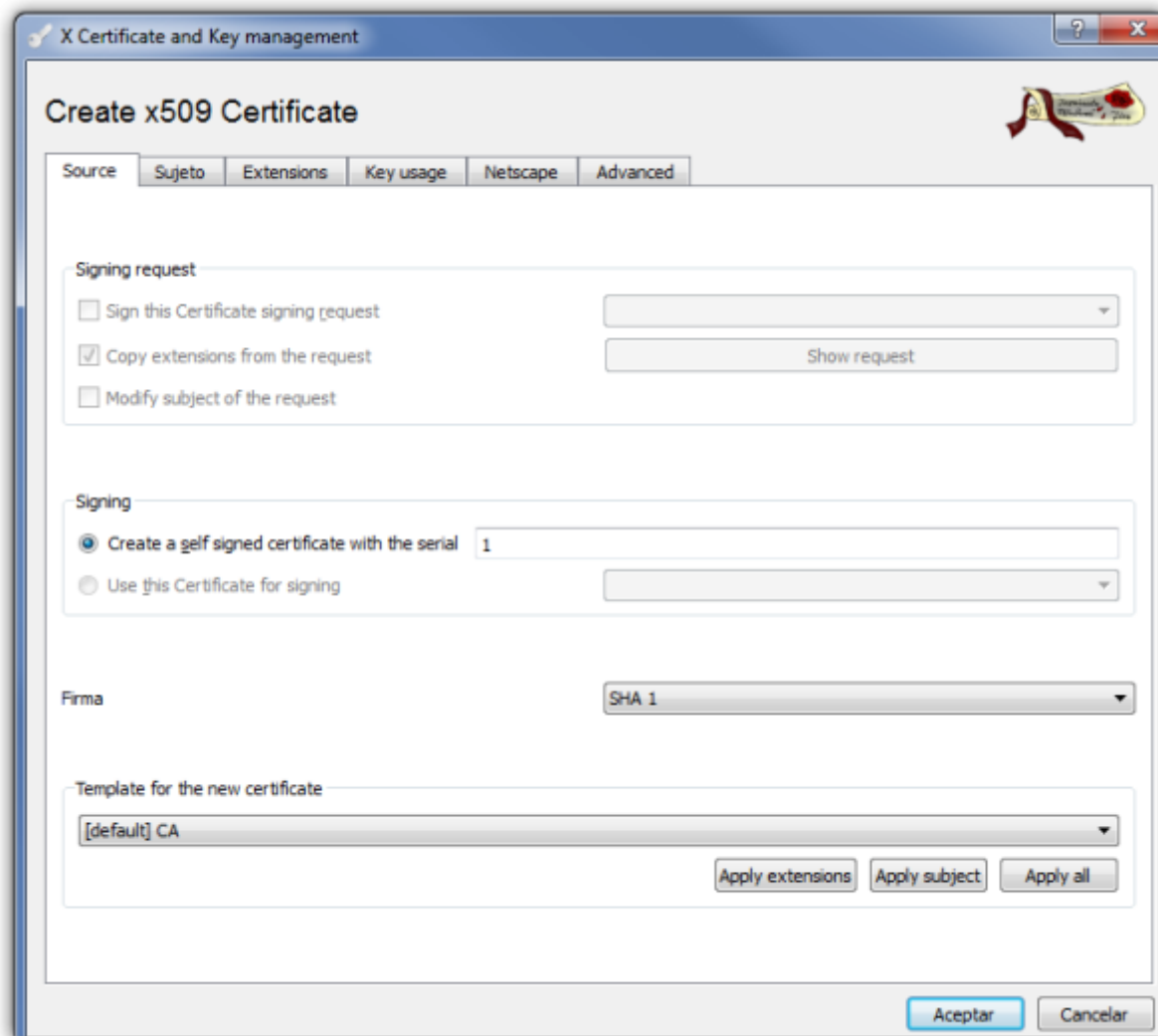


Nos aparece la siguiente ventana



## Generar el certificado Raíz

Pulsamos sobre la pestaña **Certificates** y entonces pulsamos en el botón **New Certificate**.



Configuramos los parámetros del certificado.

## Pestaña Sujeto

Configuramos la información de identificación.

Rellenamos los campos de Distinguished name y pulsamos sobre el botón inferior **Generate a new key**

X Certificate and Key management

### Create x509 Certificate

Source Subject Extensions Key usage Netscape Advanced

Distinguished name

Internal name	Certificado Raiz	organizationName	nombre empresa
countryName	es	organizationalUnitName	mi organización
stateOrProvinceName	Gran Canaria	commonName	empresa
localityName	Gran Canaria	emailAddress	tic@miempresa.es

Type	Content
------	---------

Add  
Delete

Exponente secreto

Used keys too Generate a new key

Aceptar Cancelar

Seleccionamos el tamaño de la clave y pulsamos el botón **Create**

X Certificate and Key management

### New key

Please give a name to the new key and select the desired keysize

Key properties

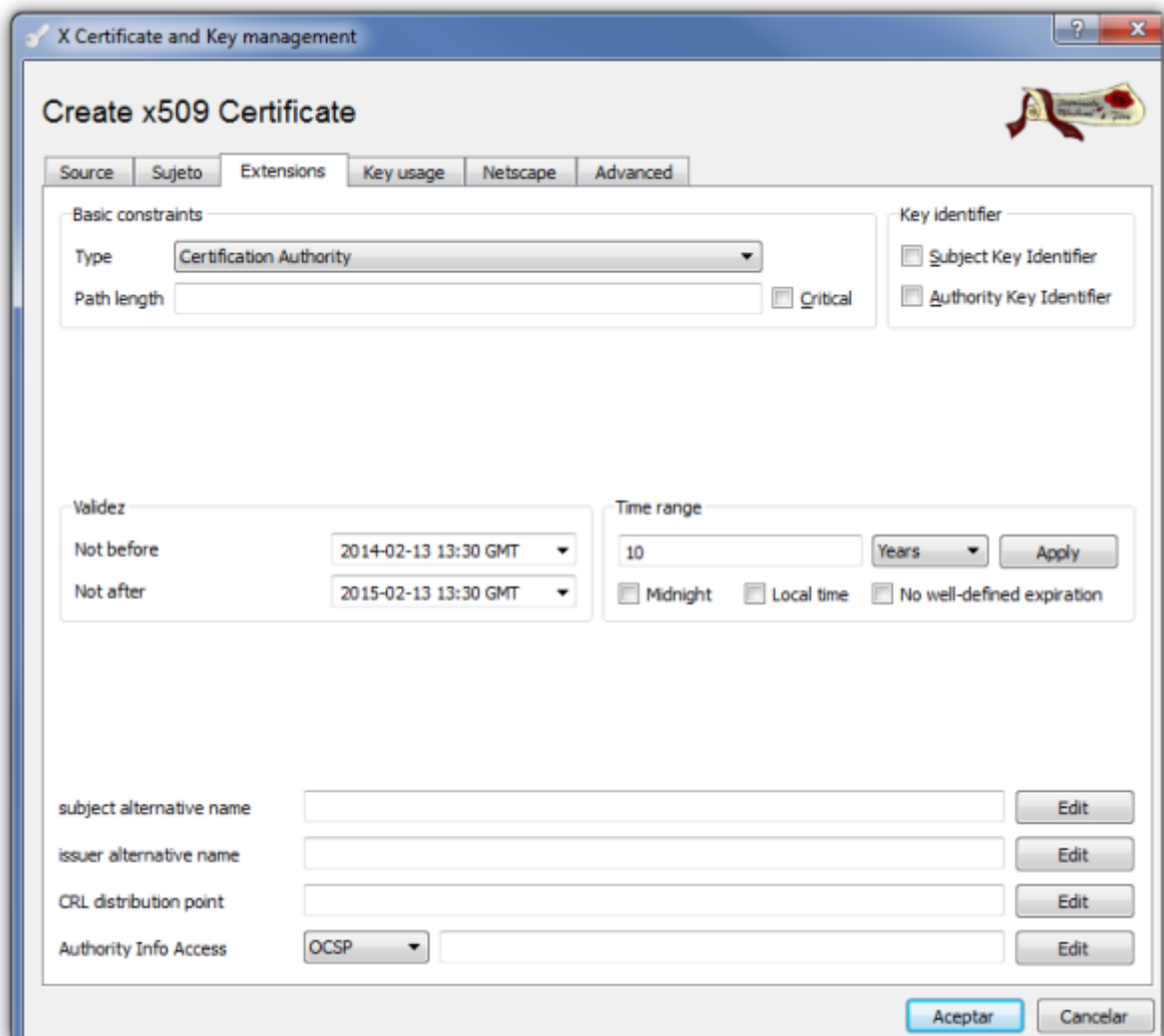
Nombre	Certificado Raiz
Keytype	RSA
Tamaño de clave	2048 bit

Create Cancelar

## Pestaña Extensions

modificamos los siguientes parámetros:

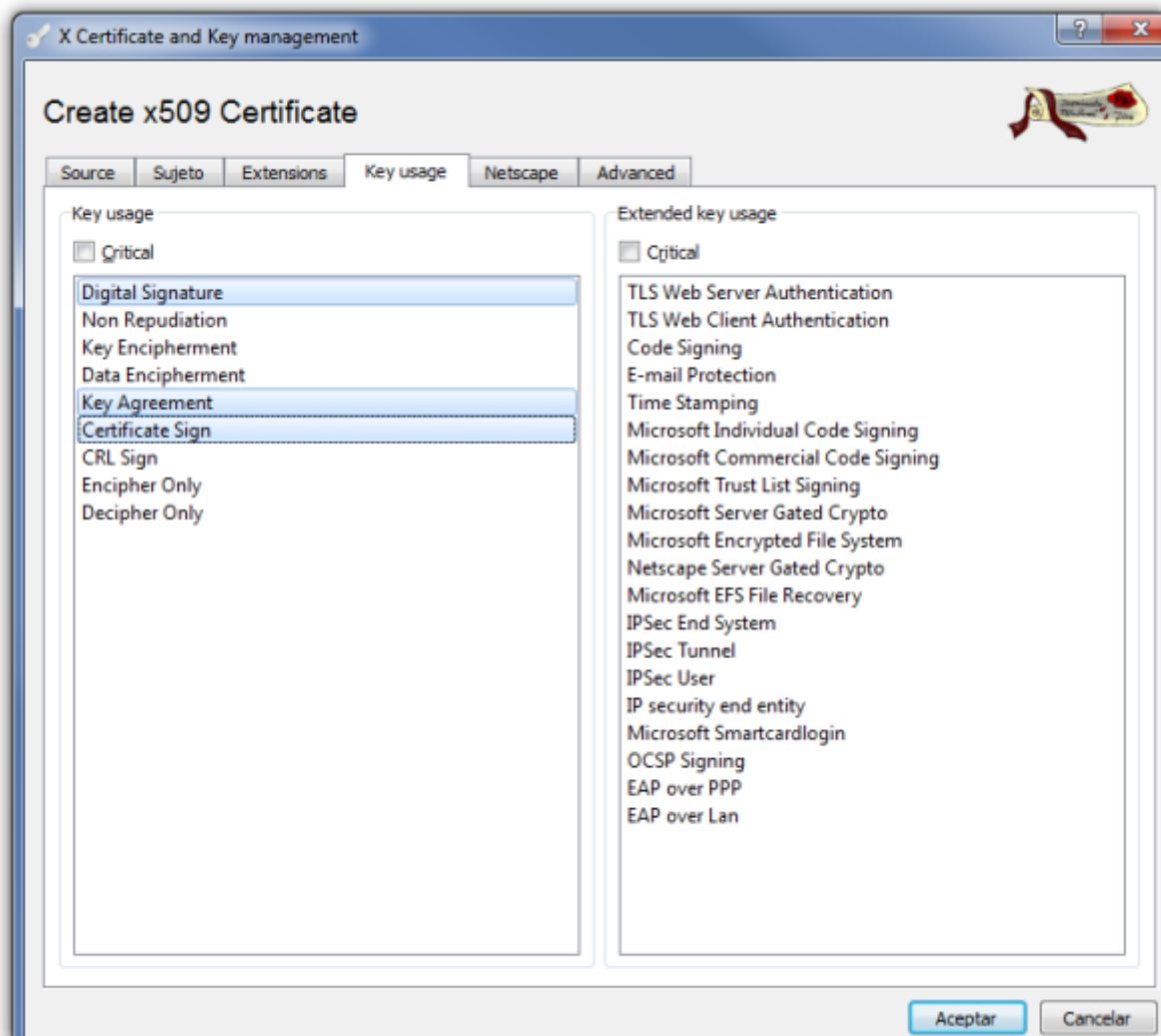
- en la lista desplegable **Type** elegimos **Certification Authority**
- En la casilla **Time range** ponemos 10 para que el certificado raíz tenga una validez de 10 años



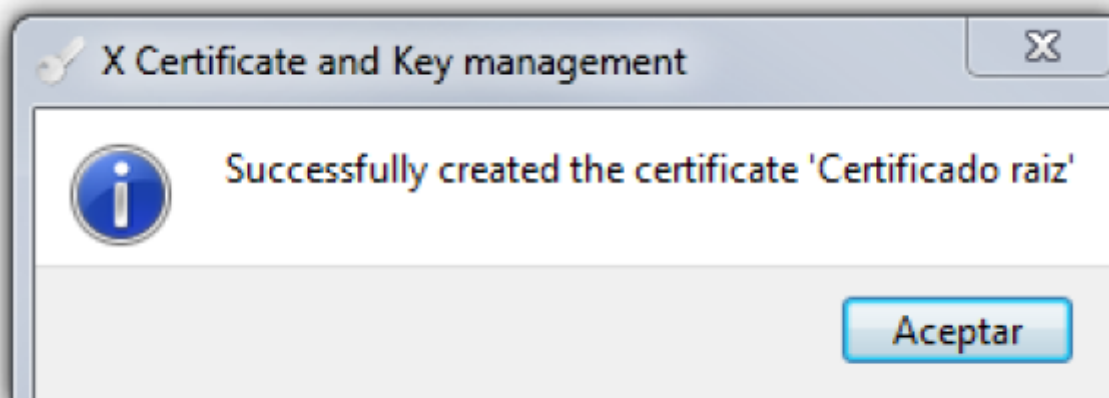
## Pestaña Key usage

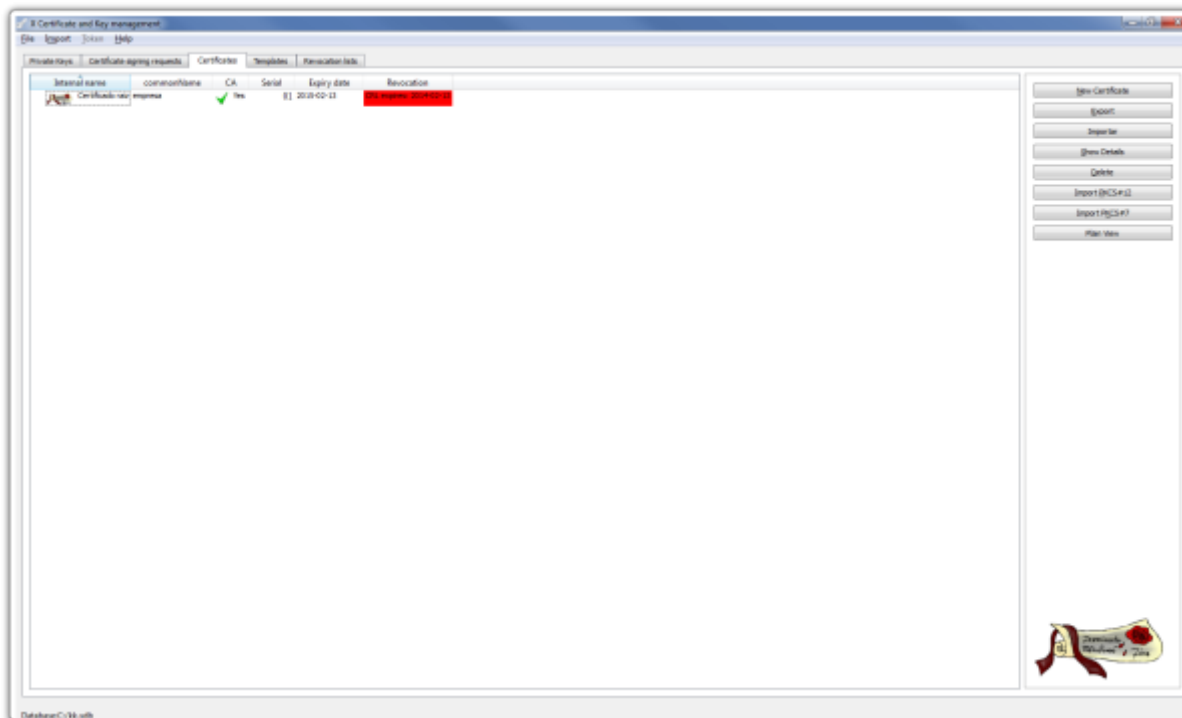
En el panel de la izquierda comprobamos que tenemos las opciones:

- Digital Signature
- Key Agreement
- Certificate Sign



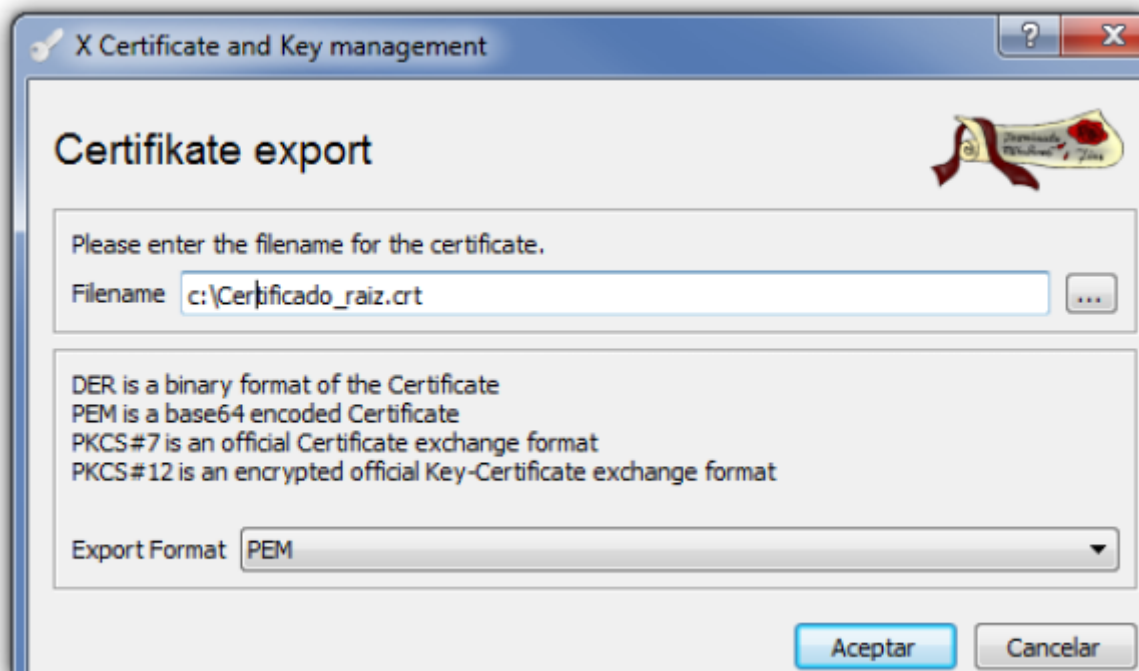
Pulsamos Aceptar y nos debe aparecer una ventana indicandonos que el certificado ha sido creado





Lo siguiente es exportar el certificado raíz para tener una copia de seguridad. Para ello hacemos lo siguiente:

- Pestaña certificados → Seleccionamos el certificado de la CZ → Botón exportar → ponemos la ubicación y el nombre de donde guardamos el certificado y pulsamos sobre el botón Aceptar



## Crear certificados para los clientes

Abrimos el XCA → Pestaña Solicitudes de Certificado (Certificate signing requests )→ Nueva solicitud (New Request)

X Certificate and Key management

### Create Certificate signing request

Source | **Sujeto** | Extensions | Key usage | Netscape | Advanced

Signing request

unstructuredName

challengePassword

Signing

☒ Create a self signed certificate with the serial

☐ Use this Certificate for signing Certificado Raiz

Firma SHA 1

Template for the new certificate

[default] CA

Apply extensions Apply subject Apply all

Aceptar Cancelar

Seleccionamos nuestra plantilla de CA para generar el nuevo certificado

En la ventana que se abre → Pestaña Subject → Rellenamos los campos y pulsamos sobre el botón generar una nueva clave (generate a new key)



X Certificate and Key management

### Create Certificate signing request

Source | **Sujeto** | Extensions | Key usage | Netscape | Advanced

Distinguished name

Internal name	usuario1	organizationName	mi empresa
countryName	es	organizationalUnitName	mi organizacion
stateOrProvinceName	Gran Canaria	commonName	empresa
localityName	Gran Canaria	emailAddress	tic@empresa.es

Type	Content
------	---------

Add  
Delete

Exponente secreto

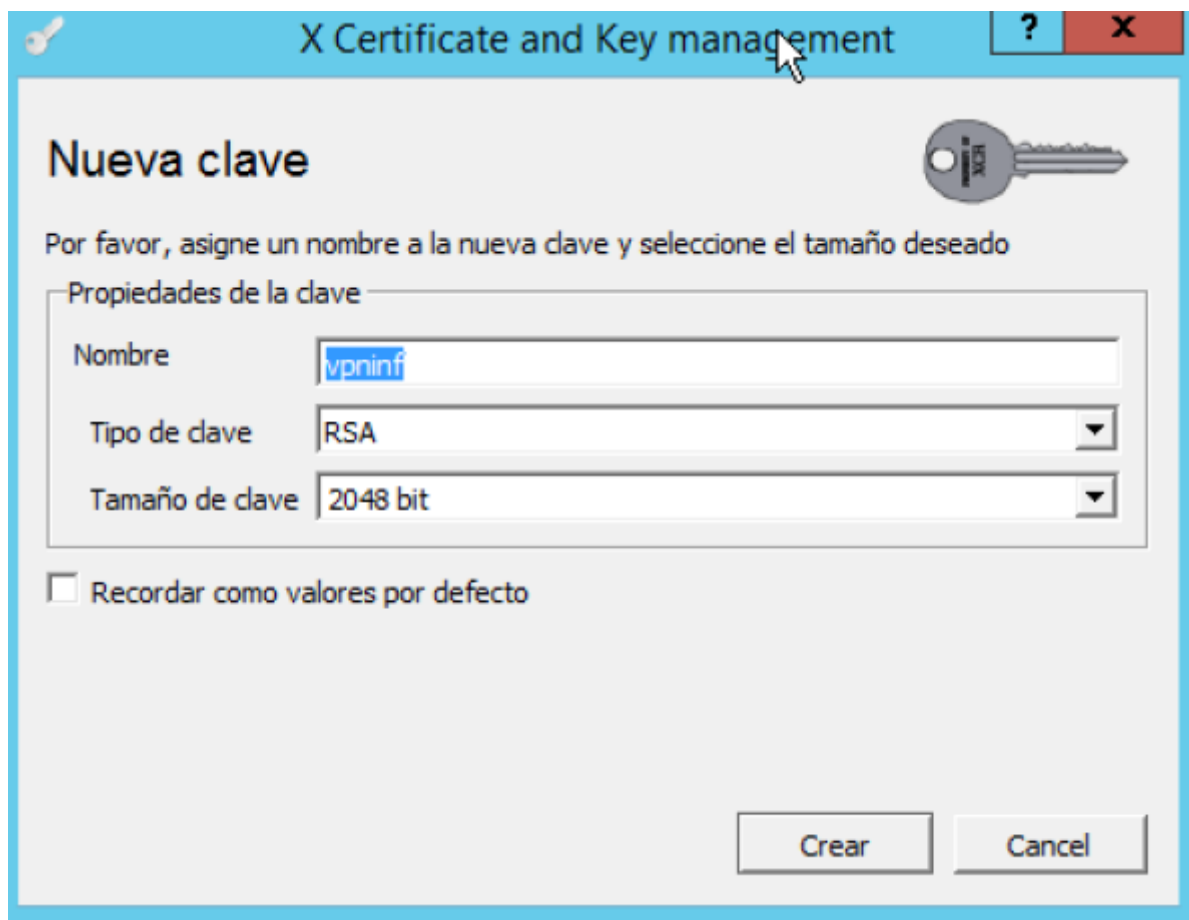
usuario1 (RSA) ☐ Used keys too [Generate a new key](#)

Aceptar Cancelar



el commonname tiene que coincidir con el del usuario pki que creamos en el fortinet

Seleccionamos el tamaño de la clave y pulsamos sobre create.



**X Certificate and Key management**

## Nueva clave

Por favor, asigne un nombre a la nueva clave y seleccione el tamaño deseado

Propiedades de la clave

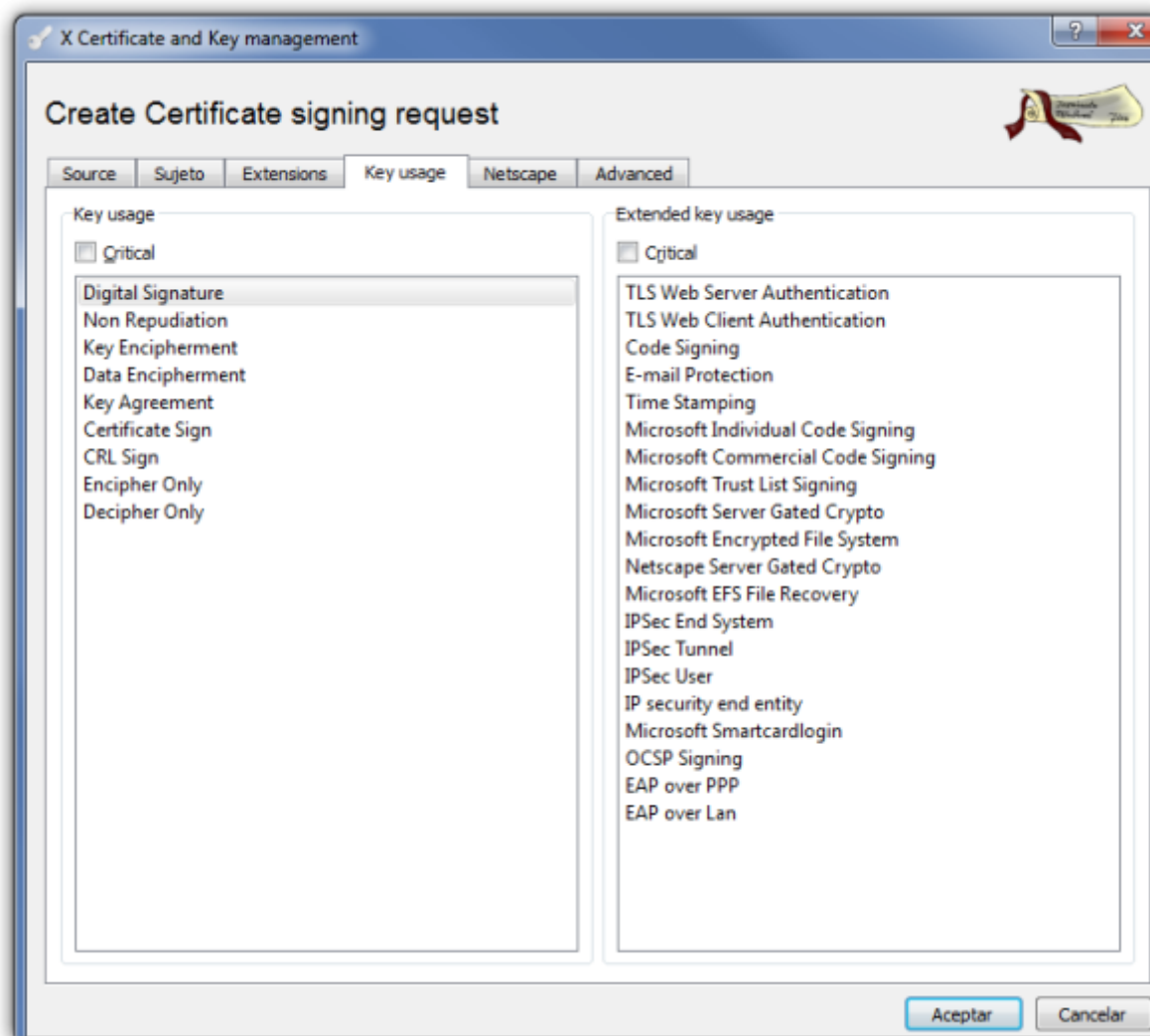
Nombre:

Tipo de clave:

Tamaño de clave:

☐ Recordar como valores por defecto

Una vez creada la clave vamos a la pestaña **key usage** y seleccionamos del panel de la izquierda → Digital signature

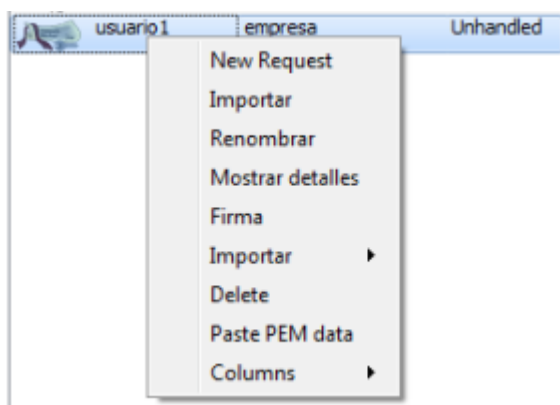


Pulsamos el botón de aceptar

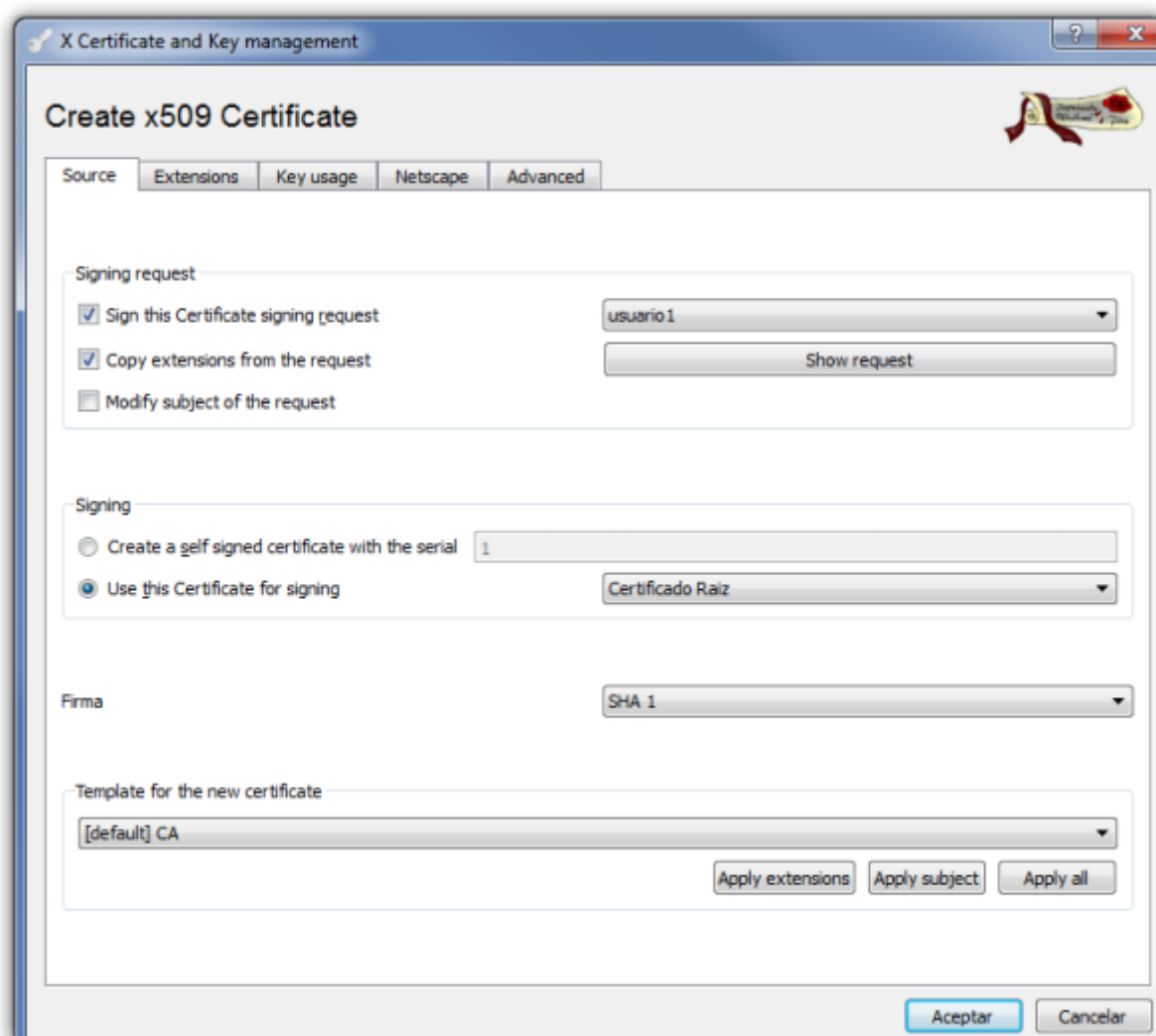
## Firma del certificado cliente

El siguiente paso sería firmar la petición de certificado que hemos generado. Vamos a la pestaña **Solicitudes de Certificado (Certificate signing requests)** aparece la petición que acabamos de crear con el estado de la columna firma como No Manejado (Unhandled).

Pulsamos con el botón derecho del ratón y en el menu contextual que aparece seleccionamos Firma



En la ventana que se abre en la parte de signing elegimos la opción **use this Certificate for signing** y seleccionamos el certificado raíz



Verificamos que en la pestaña **Extensions** la validez que queremos darle al certificado y pulsamos sobre aceptar

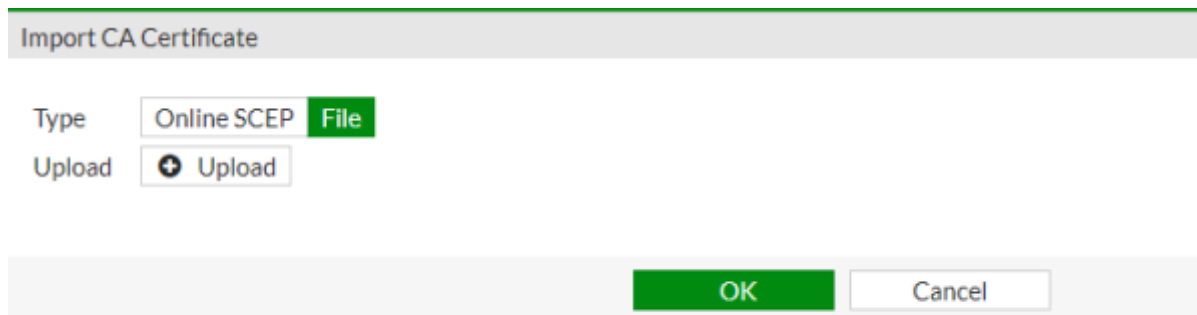
Ahora nos aparecerá el certificado firmado. Ya sólo falta exportar este certificado y el certificado raíz XCA→ Pestaña Certificate→ elegimos el certificado y le damos a exportar →PKCS#12

## Importar Certificados al Fortigate

Depués debemos de exportar los certificados de la CA y del cliente hay que importarlos al Fortigate.

### Importar Certificado Raiz

System →Certificates →Import→CA Certificates →Seleccionamos el fichero CA Raiz que previamente hemos exportado de nuestra entidad Certificadora



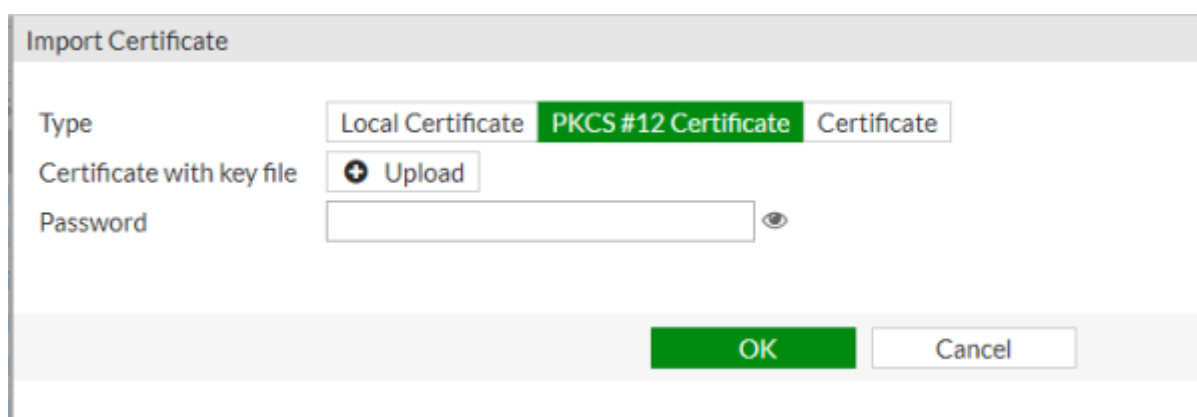
Import CA Certificate

Type:

Upload:

## Importar certificado cliente

Vamos al interfaz web del cortafuegos → System → Certificates → Local Certificate → Import →  
Seleccionamos el certificado cliente del paso anterior



Import Certificate

Type:

Certificate with key file:

Password:

## Forticlient

### Importar certificados al Forticlient

Para usar el certificado de cliente que hemos generado en el equipo del usuario debemos de enviárselo por algún medio y el usuario debe proceder a su instalación. En equipos con Windows 10 basta con pulsar dos veces sobre el certificado para que se inicie el asistente de instalación



## Asistente para importar certificados

### Este es el Asistente para importar certificados

Este asistente lo ayuda a copiar certificados, listas de certificados de confianza y listas de revocación de certificados desde su disco a un almacén de certificados.

Un certificado, que lo emite una entidad de certificación, es una confirmación de su identidad y contiene información que se usa para proteger datos o para establecer conexiones de red seguras. Un almacén de certificados es el área del sistema donde se guardan los certificados.

Ubicación del almacén

☒ Usuario actual

☐ Equipo local



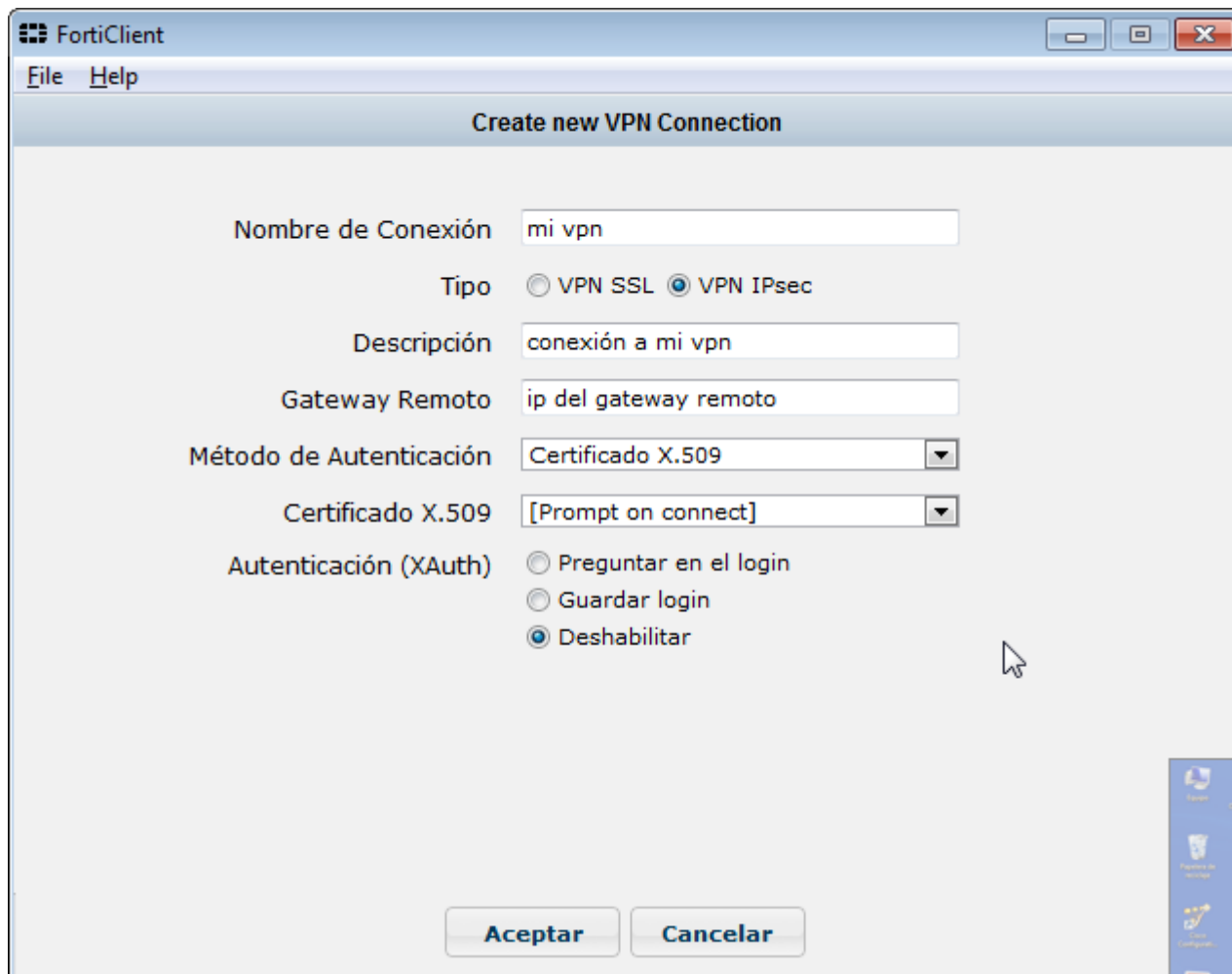
Haga clic en Siguiente para continuar.

Siguiente

Cancelar

### Crear la conexión

Añadimos una nueva conexión con los siguientes parámetros



La autenticación XAuth la he deshabilitado para simplificar, pero sería recomendable activarla tanto en el fortigate como en el cliente

## Crear conexión y usuarios en el Fortigate

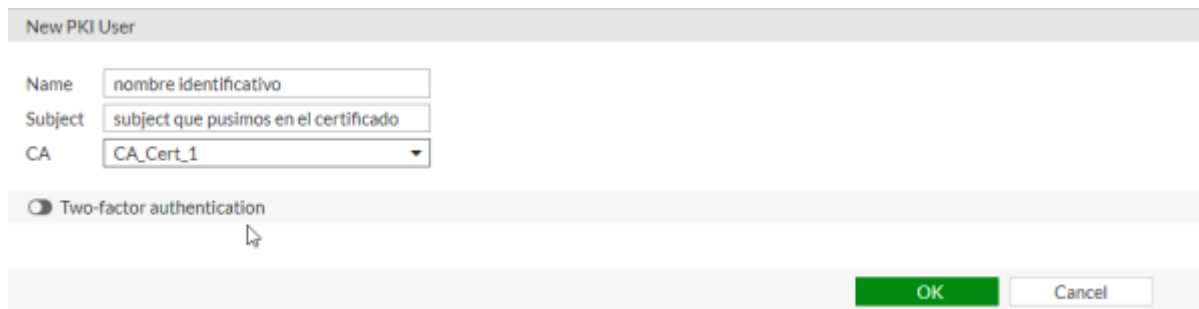
Aparte de los pasos anteriores se supone que en el fortigate hemos creado las políticas y los usuarios necesarios. En caso contrario los pasos a seguir son:

1. Crear los usuarios de validación PKI
2. Crear la VPN
3. Añadir políticas de acceso

### Creamos los usuarios de validación

#### Validación por certificados

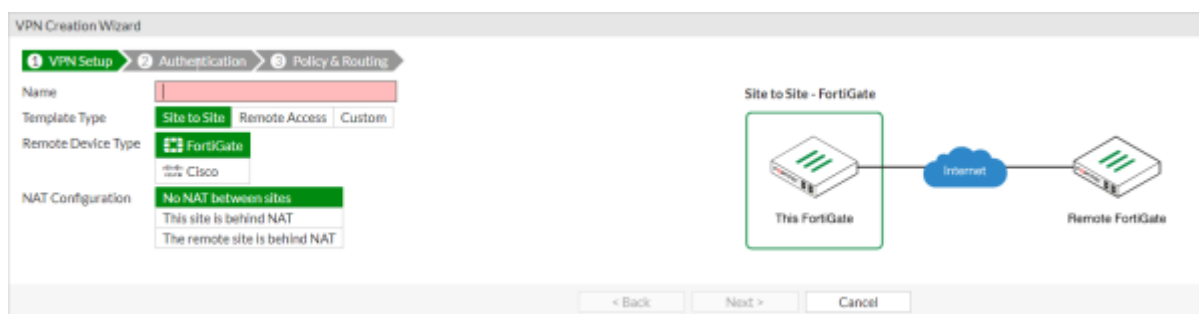
Para la validación por certificados hay que crear usuarios PKI. Fortigate → User & Device → PKI



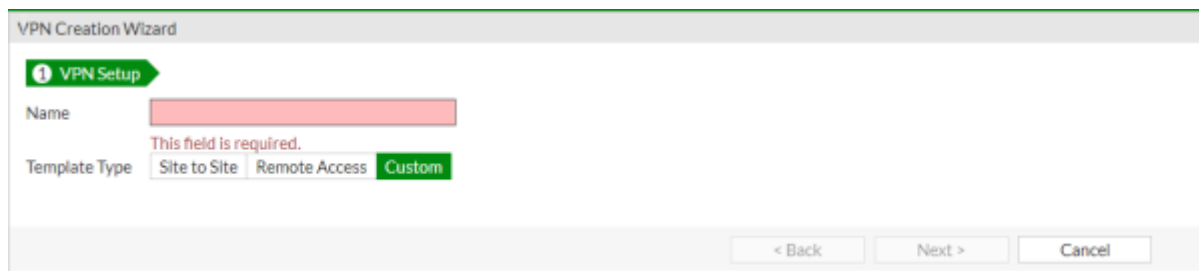
Creamos un nuevo usuario PKI teniendo en cuenta que el Subject tiene que ser el mismo que el del certificado y en CA el certificado de nuestra CA . Si sólo tienes añadida una, se llamara CA\_Cert1

## Creamos la VPN

En mi caso voy a generar una vpn por ipsec. Fortigate→VPN → Ipsec Tunnels → Create New



En mi caso voy a generarla utilizando el boton **Custom**





## New VPN Tunnel

Name

vpninf

Comments

Comments

0/255

Enable IPsec Interface Mode ☒

## Network

IP Version

IPv4 IPv6

Remote Gateway

Static IP Address

IP Address

0.0.0.0

Invalid IPv4 Address

Interface

Internet Idecnet (wan2)

Local Gateway



Mode Config



NAT Traversal

Enable Disable Forced

Keepalive Frequency

10

Dead Peer Detection

Disable On Idle On Demand

## Authentication

Method

Signature

Certificate Name



## IKE

Version

1 2

Mode

Aggressive Main (ID protection)

## Peer Options

Accept Types

Peer certificate

Peer certificate

Cambiamos Remote Gateway por **Dial up user**, la interface que vamos a usar, el método de autenticación a **signature** y seleccionamos el certificado que previamente habíamos importado. En mi caso lo he llamado igual que la vpn

En el campo **Acces Type** he seleccionado **Peer Certificate** y en el campo **Peer Certificate** he seleccionado el usuario pki creado anteriormente

<b>Authentication</b>	
Method	Signature ▼
Certificate Name	vpninf + ✕
<b>IKE</b>	
Version	1 2
Mode	Aggressive Main (ID protection)
<b>Peer Options</b>	
Accept Types	Peer certificate ▼
Peer certificate	👤 pki_vpninf ▼

El resto de parámetros los pondremos según nuestras necesidades, un ejemplo completo sería el siguiente

### Edit VPN Tunnel

**Name**

vpninf

**Comments**

Comments

**Network**

☒ ☐


IP Version

IPv4

Remote Gateway

Dialup User

Interface

 Internet Idecnet (wan2)

Local Gateway

☐

Mode Config

☒

Use system DNS in mode config

☒

Assign IP From

☒ Address/Address Group

**IPv4 mode config**

Client Address Range

☒ Rango VPN Informatica


Subnet Mask

255.255.255.255

Enable IPv4 Split Tunnel

☒

Accessible Networks

 GRP de redes para VPNInfTribut

**IPv6 mode config**

Client Address Range

☐

Prefix Length

128

Enable IPv6 Split Tunnel

☐

NAT Traversal

Enable

Disable

Forced

Dead Peer Detection

Disable

On Idle

On Demand

**Authentication**

☒ ☐

Method

Signature

Certificate Name

vpninf

+

**IKE**

Version

1

2

Mode

Aggressive


Main (ID protection)

**Peer Options**

Accept Types

Peer certificate

Peer certificate

 pki\_vpninf

Phase 1 Proposal

Add

Encryption

AES256

Authentication

SHA512

X

Encryption

AES256

Authentication

SHA256

X

Encryption

AES256

Authentication

SHA1

X

Diffie-Hellman Groups

☐

30

☐

29

☐

28

☐

27

☐

21☐☐☐☐☐☐☒☒☐☐

Key Lifetime (seconds)

86400

Local ID

C = ES, ST = GC, L = GC, O = CASA, OU

XAUTH

Type

Auto Server

User Group

Inherit from policy

Choose

usuariosvpn

**Phase 2 Selectors**

Name	Local Address	Remote Address
vpninf	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

**Edit Phase 2**

Name

vpninf

Comments

Comments

Local Address

Subnet

0.0.0.0/0.0.0.0

Remote Address

Subnet

0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal

Add

Encryption

AES256

Authentication

SHA512

X

Encryption

AES256

Authentication

SHA256

X

Encryption

AES256

Authentication

SHA1

X

Enable Replay Detection

☒

Enable Perfect Forward Secrecy (PFS)

☒

Diffie-Hellman Group

☐ 30 ☐ 29 ☐ 28 ☐ 27 ☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16 ☐ 15 ☒ 14 ☒ 5 ☐ 2 ☐ 1

Local Port

All

☒

Remote Port

All

☒

Protocol

All

☒

Autokey Keep Alive

☐

Key Lifetime

Seconds

Seconds

43200



Por supuesto hay que dar de alta en el Fortigate todos los rangos de las direcciones que vayamos a utilizar y las reglas de acceso que van a necesitar esas redes

From:

<http://wiki.intrusos.info/> - LCWIKI

Permanent link:

<http://wiki.intrusos.info/doku.php?id=hardware:fortigate:vpn:ipseccertificados>

Last update: **2023/01/18 14:45**

