

vpn,, ipsec,, certificados



Esta página está obsoleta. La nueva la puedes encontrar en [VPN ipsec con 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 un certificado para el Fortigate.
  1. Generar un petición en el fortigate
  2. Importar la petición del fortigate al XCA.
  3. firmarlo
  4. exportar el certificado firmado e importarlo al Fortigate
4. 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
5. Crear vpn, políticas y usuarios en el fortigate

Una VPN con certificados nos garantiza tanto la identidad del usuario que se conecta como la del sitio al que se coneca.

### Crear una entidad certificadora

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

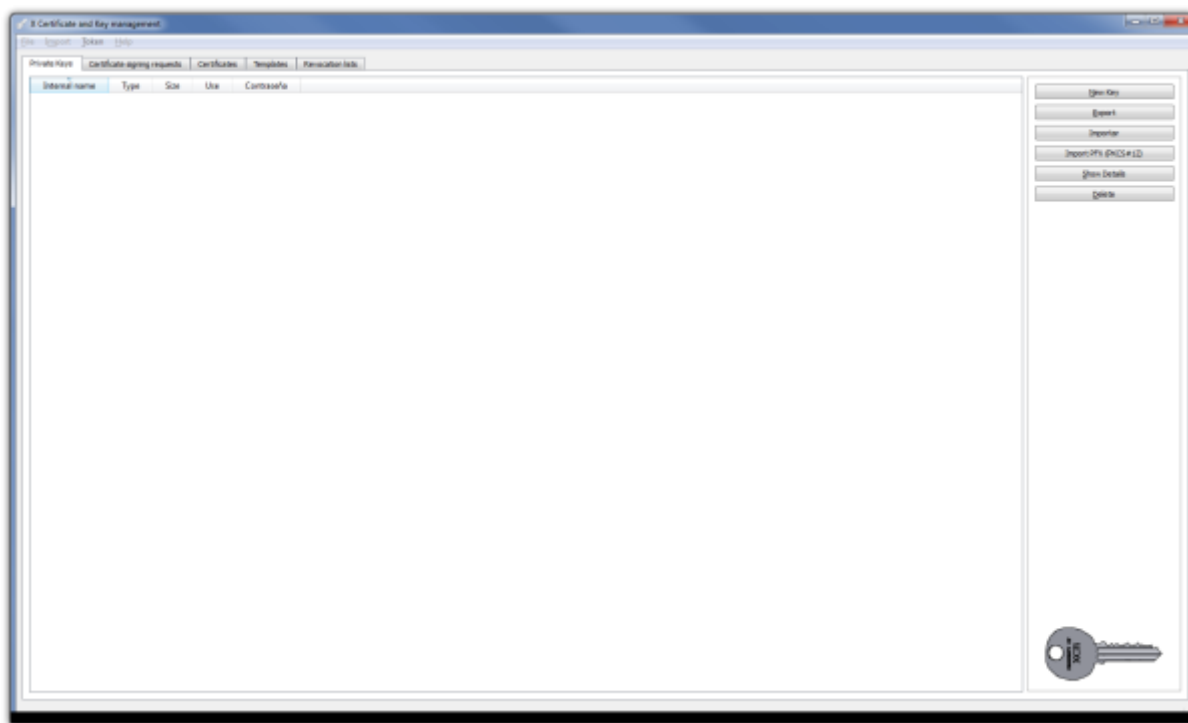
En XCA cada CA (Autoridad Certificadora)se almacena en un fichero con extensión \*.xdb. Se recomienda usar distintas bases de datos para cada PKI (Infraestructura de clave pública) que creemos.

Ejecutamos el programa Click File > New Database.

- En la ventana que se abre especificar el nombre y la ubicación donse 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.

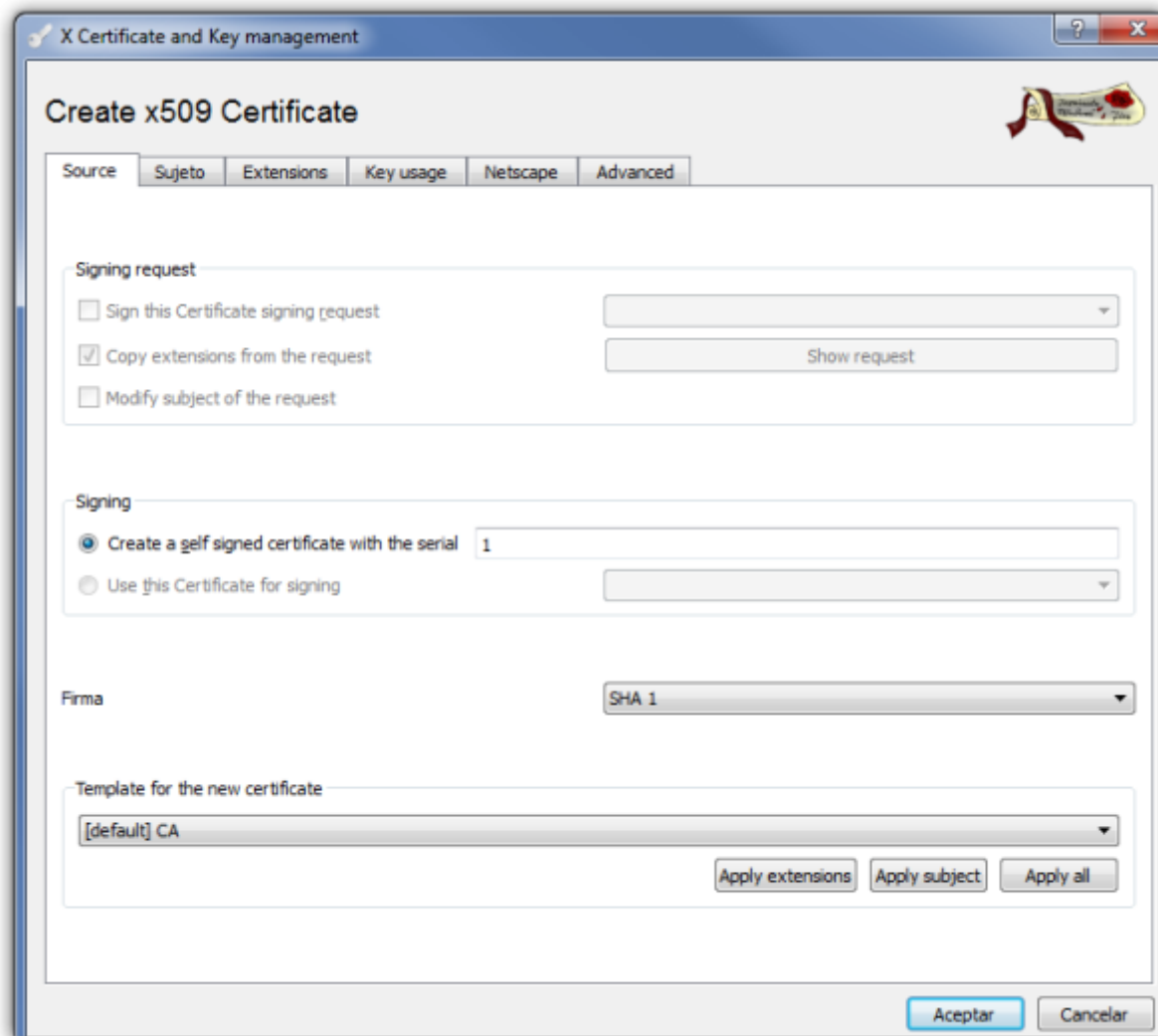


Nos aparece la siguiente ventana



## 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**

The screenshot shows the 'Create x509 Certificate' dialog box with the 'Sujeto' (Subject) tab selected. The 'Distinguished name' section contains the following fields:

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

Below the fields is a table with columns 'Type' and 'Content'. To the right of the table are 'Add' and 'Delete' buttons. At the bottom, there is a section for 'Exponente secreto' (Secret exponent) with a dropdown menu, a checkbox for 'Used keys too', and a 'Generate a new key' button. The 'Aceptar' (Accept) and 'Cancelar' (Cancel) buttons are at the bottom right.

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

The screenshot shows the 'New key' dialog box. It prompts the user to 'Please give a name to the new key and select the desired keysize'. The 'Key properties' section contains the following fields:

Field	Value
Nombre	Certificado Raiz
Keytype	RSA
Tamaño de clave	2048 bit

At the bottom are 'Create' and 'Cancelar' (Cancel) buttons.

## 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

X Certificate and Key management

### Create x509 Certificate

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

Basic constraints

Type: Certification Authority

Path length: 10 ☐ Critical

Key identifier

☐ Subject Key Identifier

☐ Authority Key Identifier

Validz

Not before: 2014-02-13 13:30 GMT

Not after: 2015-02-13 13:30 GMT

Time range

10 Years

☐ Midnight ☐ Local time ☐ No well-defined expiration

subject alternative name

issuer alternative name

CRL distribution point

Authority Info Access: OCSP

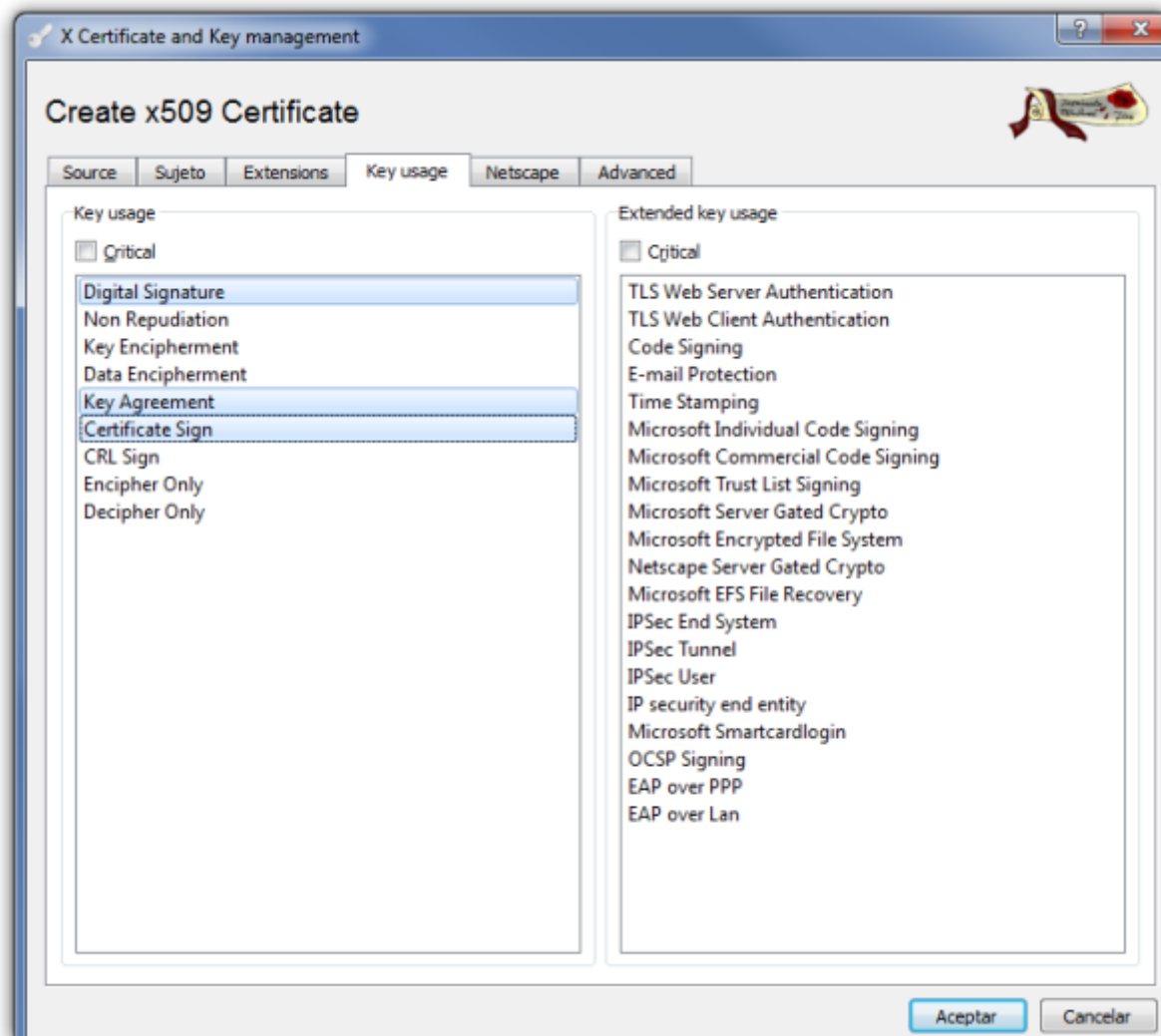
## Pestaña Key usage

En el panel de la izquierda seleccionamos:

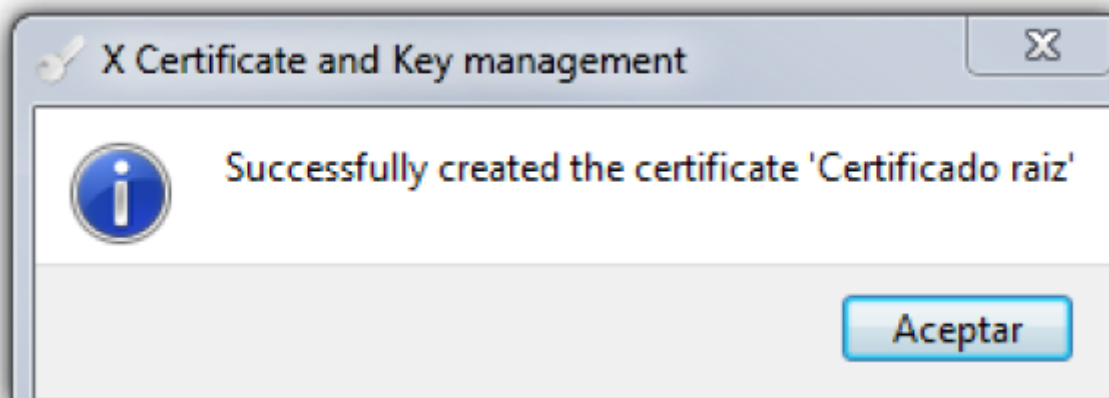
- Digital Signature
- Key Agreement
- Certificate Sign

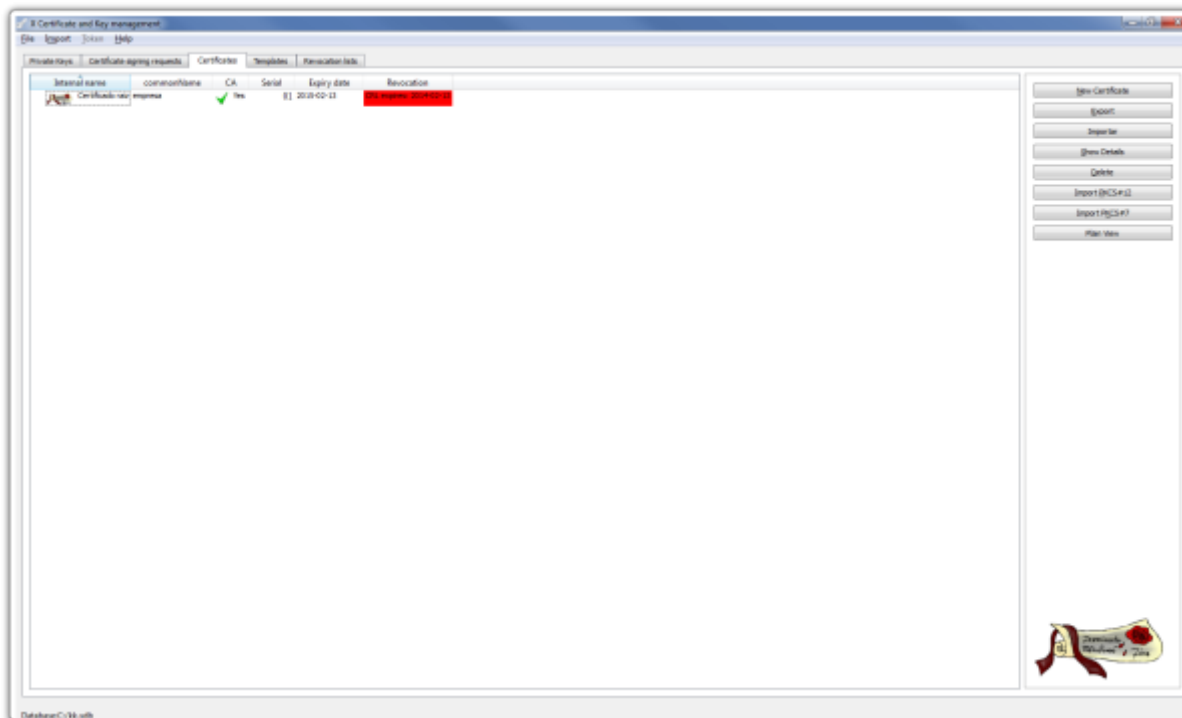


si seleccionamos otras opciones el certificado puede no ser reconocido/aceptado por ciertos equipos o sistemas operativos



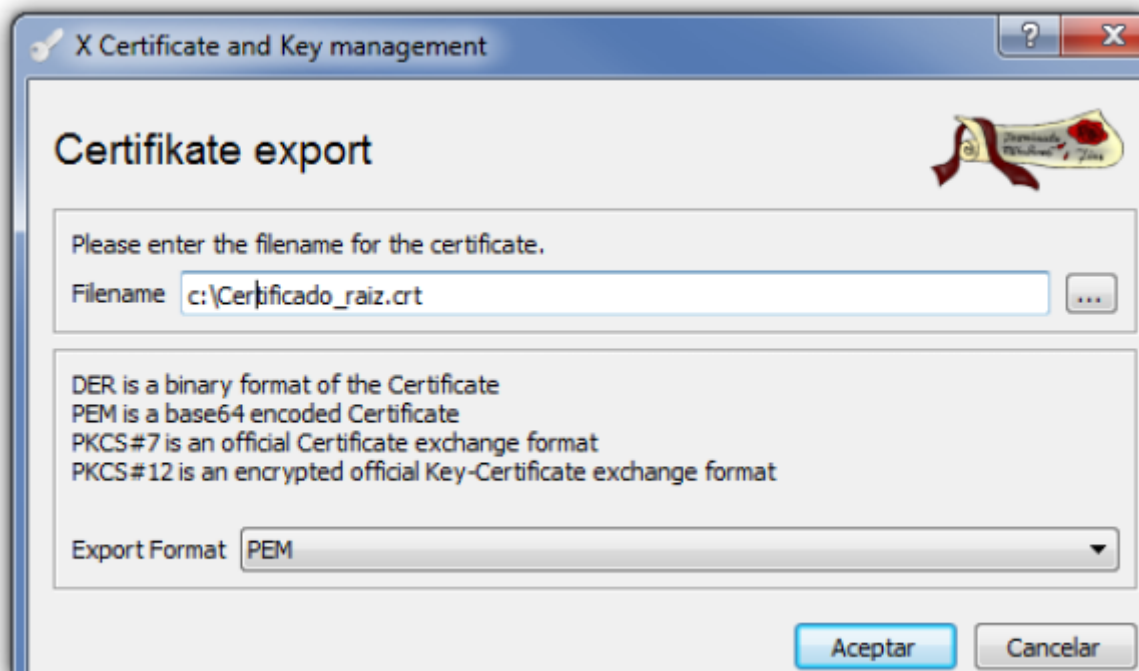
Pulsamos Aceptar y nos debe aparecer una ventana indicandonos que el certificado ha sido creado





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

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



## Generar certificado para el Fortigate

Abrimos la interfaz web de nuestro cortafuegos → System → Certificates → Local Certificates.

En la parte superior pulsamos sobre Generate y se abrirá la siguiente ventana

The screenshot shows the FortiGate 1000C web interface. The left sidebar contains a menu with options like Dashboard, Status, Top Sources, Top Destinations, Top Applications, Traffic History, Network, Config, Admin, Certificates, Local Certificates, External, CA Certificates, and CRL. The main content area is titled 'Generate Certificate Signing Request'. It contains several sections: 'Certificate Name' with a text input field; 'Subject Information' with a dropdown for 'ID Type' (set to 'Host IP') and a text input for 'IP' (set to '5.5.5.5'); 'Optional Information' with fields for 'Organization Unit', 'Organization', 'Locality/City', 'State/Province', 'Country/Region' (set to 'ES'), 'Email', and 'Subject Alternative Name'; 'Key Type' with a dropdown for 'Key Type' (set to 'RSA') and a text input for 'Key Size' (set to '2048 bits'); and 'Download Method' with radio buttons for 'File Based' (selected) and 'Online SCEP'. At the bottom right are 'OK' and 'Cancel' buttons.

Rellenamos los campos

This screenshot shows the same 'Generate Certificate Signing Request' form, but now with fields filled out. The 'Certificate Name' field contains 'breussl'. The 'ID Type' dropdown is still 'Host IP', but the 'IP' field now contains 'ip del interfaz wan'. In the 'Optional Information' section, 'Organization Unit' is 'mi empresa', 'Organization' is 'mi organización', 'Locality/City' is 'gran canaria', 'State/Province' is 'gran canaria', 'Country/Region' is 'SPAIN (ES)', 'Email' is 'info@empresa.es', and 'Subject Alternative Name' is empty. The 'Key Type' dropdown is 'RSA' and 'Key Size' is '2048 bits'. The 'Download Method' radio buttons remain the same. The 'OK' and 'Cancel' buttons are still at the bottom right.

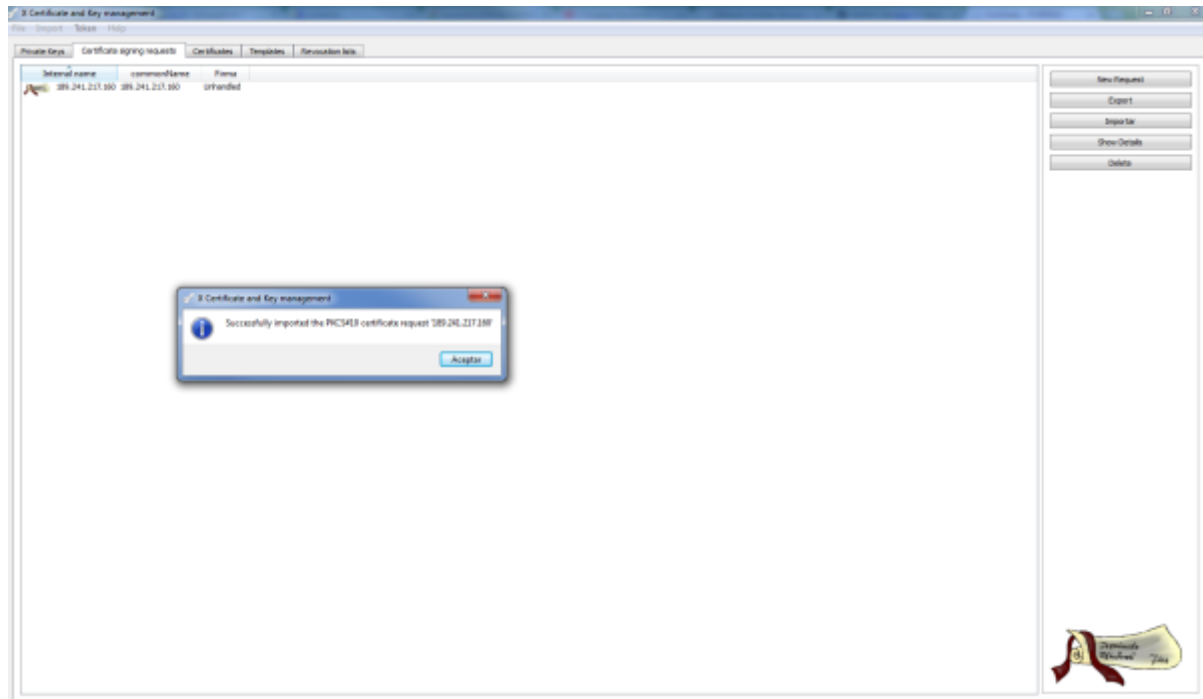
Al pulsar sobre ok volvemos a la página de Local Certificates. seleccionamos el certificado que hemos creado y pulsamos sobre el botón **download** de la barra.

Nos generará un fichero con la extensión **csr** que deberemos de importar en el XCA para firmar

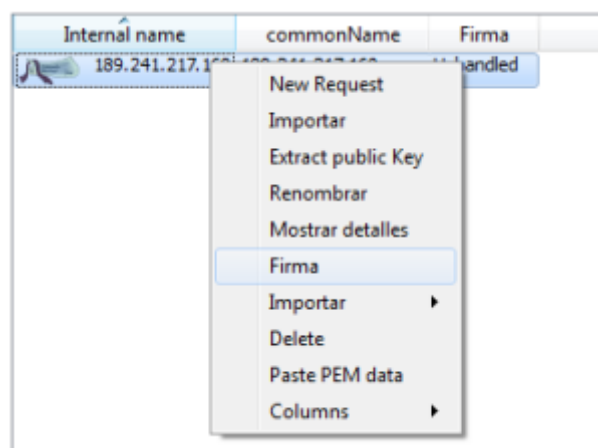
## Firma del Certificado generado

Abrimos el XCA y nos vamos a la pestaña **Certificate Signing requests** y pulsamos sobre el botón **Importar** y seleccionamos el fichero que descargamos en el paso anterior.





Botón derecho del ratón sobre el certificado que acabamos de importar → Firma



Editamos los parámetros antes de firmar de acuerdo a lo siguiente:

- En source verificar está marcada la opción de usar el certificado raíz que habíamos generado

X Certificate and Key management

## Create x509 Certificate

Source Extensions Key usage Netscape Advanced

**Signing request**

☒ Sign this Certificate signing request 189.241.217.160

☒ Copy extensions from the request Show request

☐ Modify subject of the request

**Signing**

☐ Create a self signed certificate with the serial 1

☒ 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

- En la pestaña de extensions, casilla Time range poner 1 año

**X Certificate and Key management**

### Create x509 Certificate

Source Extensions **Key usage** Netscape Advanced

**Basic constraints**

Type: Not defined

Path length:  ☐ Critical

**Key identifier**

☐ Subject Key Identifier

☐ Authority Key Identifier

**Validez**

Not before: 2014-02-14 12:48 GMT

Not after: 2015-02-13 13:30 GMT

**Time range**

1 Years

☐ Midnight ☐ Local time ☐ No well-defined expiration

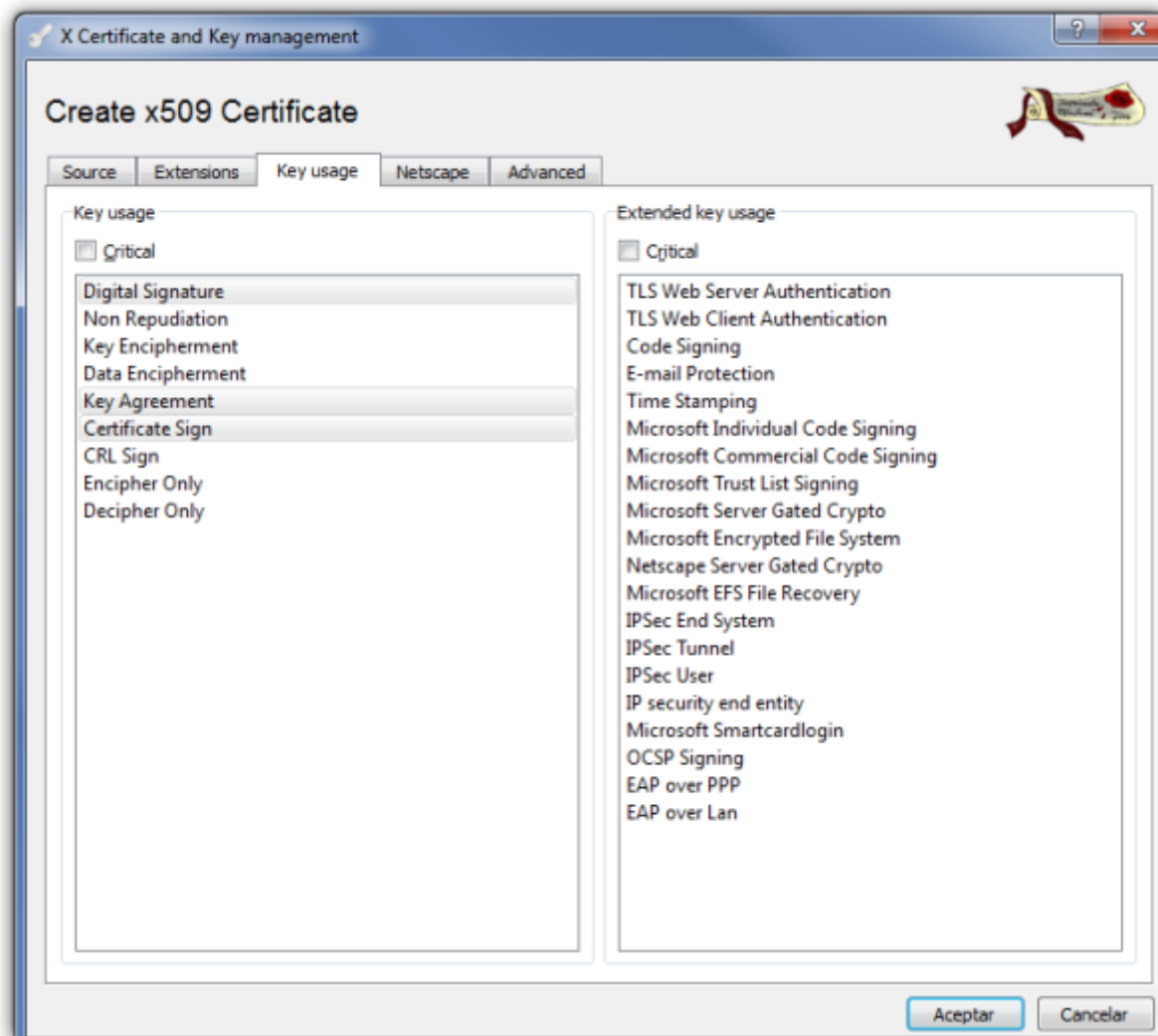
subject alternative name

issuer alternative name

CRL distribution point

Authority Info Access: OCSP

- En la pestaña Key Usage marcar
  - Digital Signature
  - Key Agreement
  - Certificate Sign



Pulsamos aceptar para que nos firme el certificado.

Después debemos de exportar el certificado y volverlo a importar al Fortigate. Para eso vamos a la pestaña certificates del XCA →seleccionamos el certificado y pulsamos el botón de exportar

## Importar certificado firmado

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

## Importar Certificado Raiz

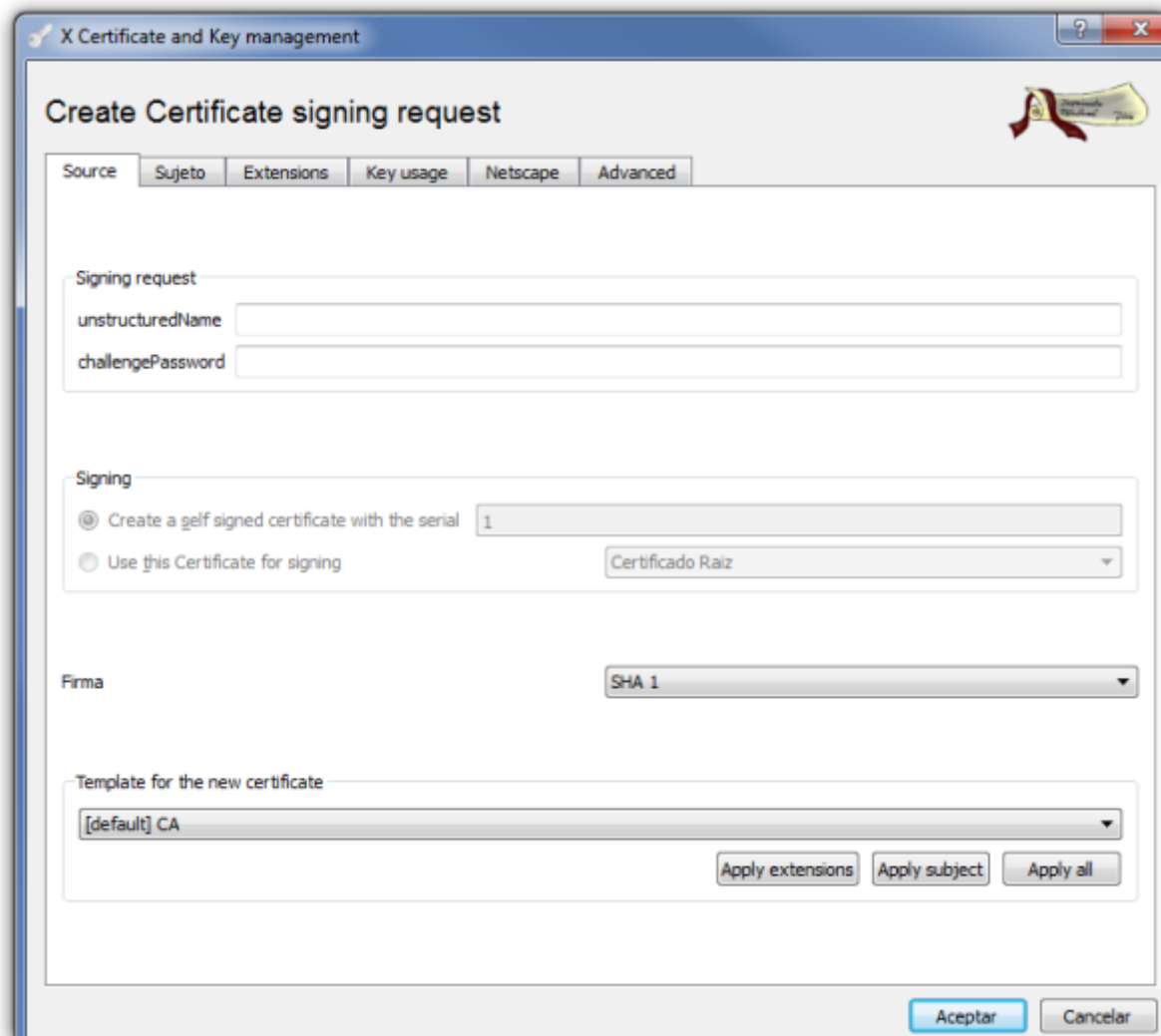
System →Certificates →CA Certificates →Import →Marcamos la casilla Local Pc y seleccionamos el fichero CA Raiz que previamente hemos exportado de nuestra entidad Certificadora



El certificado raíz es necesario importarlo tanto al cortafuegos, como a los clientes

## Crear certificados para los clientes

Abrimos el XCA → Pestaña Certificate signing requests → New Request



The screenshot shows the 'X Certificate and Key management' window with the 'Create Certificate signing request' dialog open. The 'Source' tab is selected. The dialog contains the following fields and options:

- Signing request:** Fields for 'unstructuredName' and 'challengePassword'.
- Signing:** Radio buttons for 'Create a self signed certificate with the serial' (selected, with a value of '1') and 'Use this Certificate for signing' (with a dropdown menu showing 'Certificado Raiz').
- Firma:** A dropdown menu showing 'SHA 1'.
- Template for the new certificate:** A dropdown menu showing '[default] CA'.
- Buttons:** 'Apply extensions', 'Apply subject', 'Apply all', 'Aceptar', and 'Cancelar'.

En la ventana que se abre → Pestaña Subject → Rellenamos los campos y pulsamos sobre el botón generate a new key

The screenshot shows the 'Create Certificate signing request' window in the Fortinet X Certificate and Key management interface. The window has a title bar with a question mark and a close button. The main title is 'Create Certificate signing request'. Below the title, there are tabs: 'Source', 'Sujeto', 'Extensions', 'Key usage', 'Netscape', and 'Advanced'. The 'Sujeto' tab is selected. The 'Distinguished name' section contains the following fields:

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

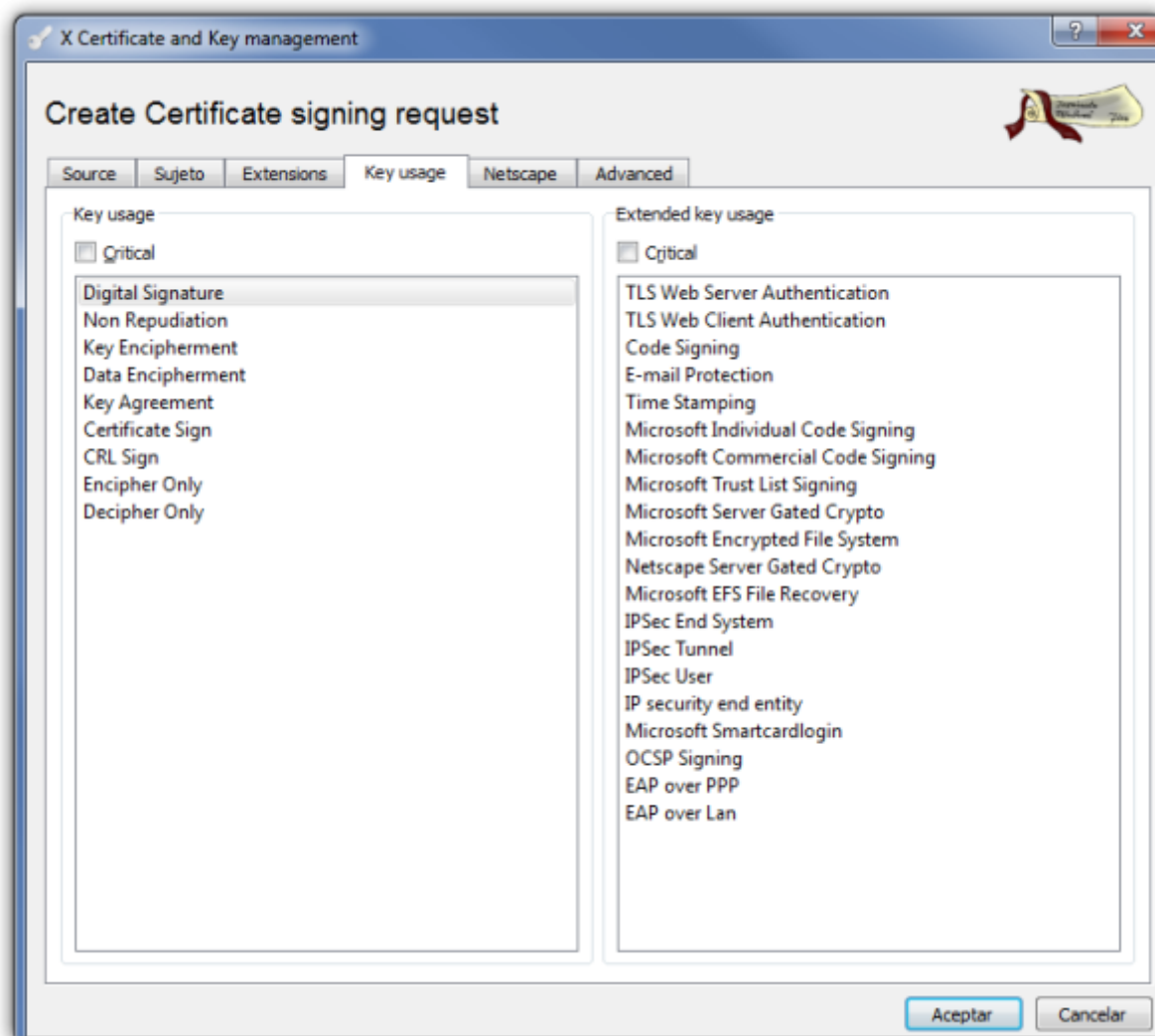
Below the distinguished name fields, there is a table with two columns: 'Type' and 'Content'. The table is currently empty. To the right of the table are two buttons: 'Add' and 'Delete'. At the bottom of the window, there is a section for 'Exponente secreto' with a dropdown menu showing 'usuario1 (RSA)' and a checkbox labeled 'Used keys too'. A 'Generate a new key' button is also present. At the very bottom, there are 'Aceptar' and 'Cancelar' buttons.



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.

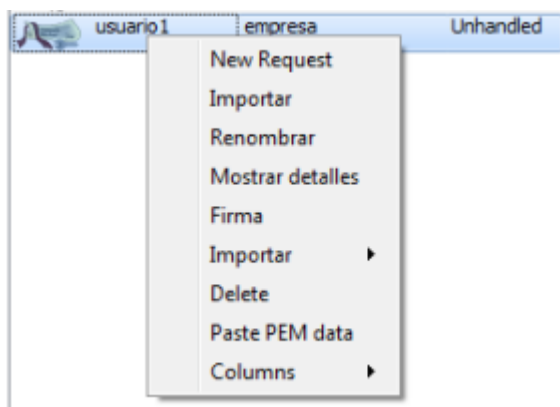
Pestaña **key usage** y seleccionamos del panel de la izquierda → Digital signature



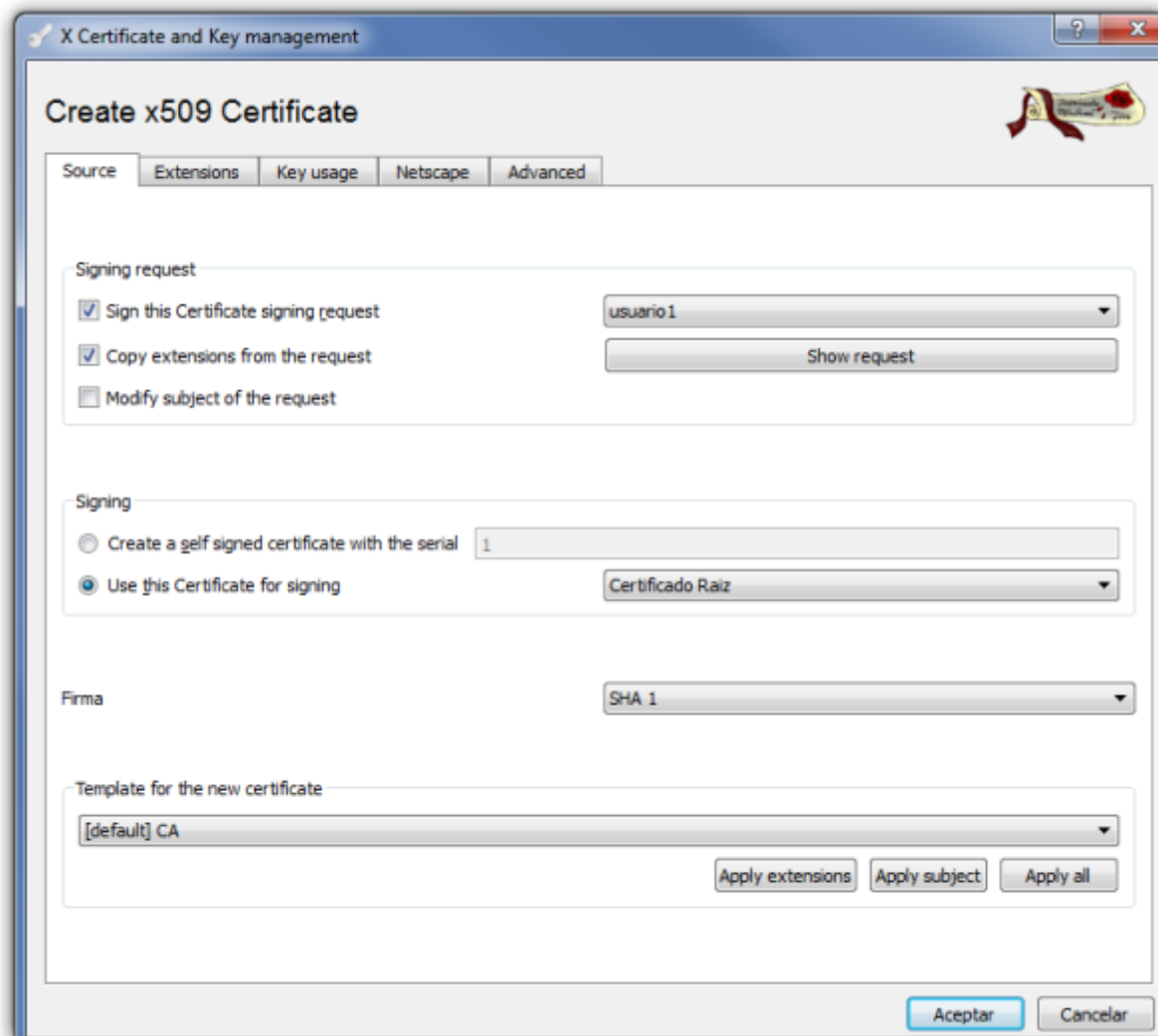
Pulsamos el botón de aceptar y bajo la pestaña **Certificate signing requests** aparece la petición que acabamos de crear con el estado de la columna firma como Unhandled.

### Firma del certificado cliente

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



En la pestaña **Key usage** no hace falta ahora seleccionar nada

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

## Forticlient

### Importar certificados al Forticlient

Desde el Fortigate descargamos la CA que hemos creado y que si es la primera seguramente se llamara el CA\_Cert\_1.

A su vez desde el XCA → pestaña Certificates →exportamos el certificado cliente en formato pkcs#12 e importamos ambos certificados al forticlient→Menu File→opciones→Gestión de Certificados→botón importar





Es necesario importar los dos certificados CA\_Cert1 y el del cliente

## Crear la conexión

Añadimos una nueva conexión con los siguientes parámetros

FortiClient

File Help

Create new VPN Connection

Nombre de Conexión: mi vpn

Tipo: ☐ VPN SSL ☒ VPN IPsec

Descripción: conexión a mi vpn

Gateway Remoto: ip del gateway remoto

Método de Autenticación: Certificado X.509

Certificado X.509: [Prompt on connect]

Autenticación (XAuth): ☐ Preguntar en el login ☐ Guardar login ☒ Deshabilitar

Aceptar Cancelar



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

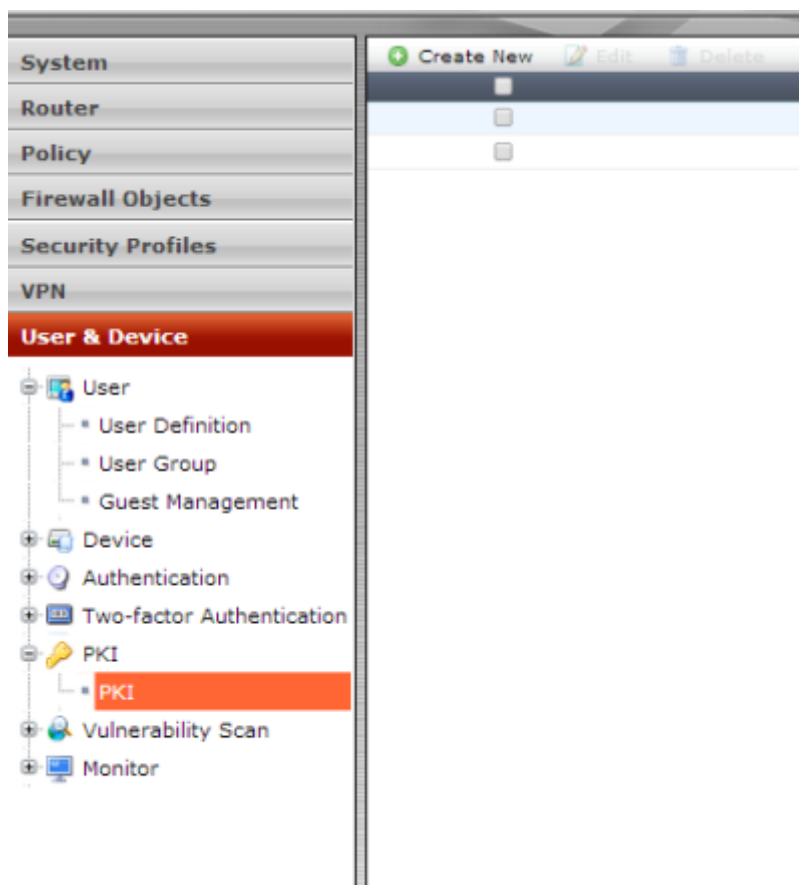
## Crear conexión y usuarios en el Fortigate

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. Nos validamos en el Fortigate y vamos a la pestaña VPN
2. Creamos los usuarios de validación
3. Pinchamos sobre el icono **Create FortiClient VPN**
4. Ponemos los siguientes parámetros

## Creamos los usuarios de validación

para PKI



Creamos uno nuevo teniendo en cuenta que el Subject tiene que ser el mismo que el del certificado y en CA el certificado de nuestra CA normalmente CA\_Cert1

## Referencias

- [https://stuff.purdon.ca/?page\\_id=21](https://stuff.purdon.ca/?page_id=21)
- [https://stuff.purdon.ca/?page\\_id=30](https://stuff.purdon.ca/?page_id=30)
- <http://jbouzada.wordpress.com/2009/03/03/trabajando-con-certificados-en-windows-server-2008-1/>
- <http://jbouzada.wordpress.com/2009/03/12/trabajando-con-certificados-en-windows-server-2008-2/>
- <http://jbouzada.wordpress.com/2009/03/16/trabajando-con-certificados-en-windows-server-2008-3/>
- <http://jbouzada.wordpress.com/2009/03/18/trabajando-con-certificados-en-windows-server-2008-4/>
- <http://jbouzada.wordpress.com/2009/03/25/trabajando-con-certificados-en-windows-server-2008-5/>
- <http://jbouzada.wordpress.com/2009/03/30/trabajando-con-certificados-en-windows-server-2008-%E2%80%A6-6/>
- <http://techlib.barracuda.com/display/CP/How%2Bto%2BCreate%2BCertificates%2Bwith%2BXCA>

- <https://campus.barracuda.com/product/campus/article/REF/CreateCertificatesXCA/>
- <http://firewallguru.blogspot.com.es/2009/05/creating-self-signed-certificates-for.html>

From:

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

Permanent link:

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

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

