1/19

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.

| Vew Password | ? 💌 |
|--------------------------------------|--|
| Contraseña | |
| Please enter a password C:/kk.xdb | that will be used to encrypt your private keys in the database file: |
| Contraseña Repeat Contraseña | |
| E <u>x</u> it | Aceptar Cancelar |

Nos aparece la siguiente ventana

| A E-Centricate and Eavy management | - 10 - 1 |
|--|----------------------|
| Bin layor John Help | |
| Printe Name Cambolan ageing inquests. Cambolanas. Seeplates Re-accutant lass | |
| Determinante Type Sox Uta Cantasarle | (jau Gay |
| | Expert |
| | Inpurior |
| | Inport PTI (PAIS#12) |
| | Share Datalite |
| | Department |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

Generar el certificado Raíz

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

| Advanced |
|--|
| |
| |
| Ť |
| Show request |
| on torr incipation |
| |
| Ţ |
| SHA 1 |
| |
| |
| • |
| Apply extensions Apply subject Apply all |
| |
| |
| |
| |

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 n | X Certificate and Key management | | | | | | | |
|-------------------------|----------------------------------|----------------|------------------------|------------------|--------------------|--|--|--|
| Create x509 Ce | Create x509 Certificate | | | | | | | |
| Source Sujeto E | xtensions Key u | 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 | | | | |
| Туре | e | | Content | | Add | | | |
| | | | | | Delete | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| Exponente secreto | | | | _ | | | | |
| | | | • | Used keys too | Generate a new key | | | |
| | | | | A | ceptar Cancelar | | | |

Seleccionamos el tamaño de la clave y pulsamos el botón Create

| of X Certificate and | X Certificate and Key management | | | | |
|---|--|----------|--|--|--|
| New key | | | | | |
| Please give a name to Key properties | o the new key and select the desired keysize | - | | | |
| Nombre | Certificado Raiz | | | | |
| Keytype | RSA | • | | | |
| Tamaño de dave | 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

| X Certificate and Key man | agement | | | 2 - |
|---|---|------------------------------|------------|---|
| Source Sujeto Exter | nsions Key usage Netscape | Advanced | | () Barnet () () |
| Basic constraints | | | | Key identifier |
| Type Certification | Authority | | • | Subject Key Identifier |
| Path length | | | Critical | Authority Key Identifier |
| | | | | |
| Validez Not before Not after | 2014-02-13 13:30 GMT 2015-02-13 13:30 GMT ▼ | Time range 10 Midnight | Local time | Years Apply No well-defined expiration |
| Validez Not before Not after subject alternative name | 2014-02-13 13:30 GMT ▼ 2015-02-13 13:30 GMT ▼ | Time range 10 Midnight | Local time | Years Apply No well-defined expiration Edit |
| Validez Not before Not after subject alternative name issuer alternative name | 2014-02-13 13:30 GMT ▼ 2015-02-13 13:30 GMT ▼ | Time range 10 Midnight | Local time | Years Apply No well-defined expiration Edit Edit Edit |
| Validez Not before Not after subject alternative name issuer alternative name CRL distribution point | 2014-02-13 13:30 GMT 2015-02-13 13:30 GMT | Time range 10 Midnight | Local time | Years Apply No well-defined expiration Edit Edit Edit Edit |

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

| 🗹 X Cer | 🗸 X Certificate and Key management | | | | | |
|---------|---|--|--|--|--|--|
| 1 | Successfully created the certificate 'Certificado raiz' | | | | | |
| | Aceptar | | | | | |



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

| 🖉 X Certific | ate and Key management | ? × |
|--|---|------------------|
| Certifik | ate export | A Comment |
| Please en | ter the filename for the certificate. | |
| Filename | c:\Cerbificado_raiz.crt | |
| DER is a b PEM is a b PKCS#7 is PKCS#12 | inary format of the Certificate ase64 encoded Certificate an official Certificate exchange format is an encrypted official Key-Certificate exchange format | |
| Export Fo | rmat (PEM | • |
| | | Aceptar Cancelar |

Generar certificado para el Fortigate

Abrimos la interfaz web de nuestro cortafuegos \rightarrow System \rightarrow Certificates \rightarrow Local Certificates.

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

| Last update: 2023/01/18 14:45 | hardware:fortigate:vpn:// | certificados https://intru | sos.info/doku.php?id=hai | rdware:fortigate:vpn:certificados |
|-------------------------------|---------------------------|----------------------------|--------------------------|-----------------------------------|
| • | J 1 | | | |

| | GLFI-Prosedure x | 😋 Carriesta 🛛 🛪 | 🖉 inisis and [MR22578MR2] × 🖣 | 🛚 vranjeti fazitaria | X 🏹 🗋 Maare of enter larger 1, X | N MARINO BARNAP & Replic | x 🚺 🗋 Facéliera - Finitestat | x |
|---|--|--|-------------------------------|----------------------|----------------------------------|--------------------------|------------------------------|----------|
| FortiGate 1000C | Torrust 🦲 Grecoux 🦲 Sider | | | | | | ee Waard Legend | FURTINET |
| System | Certificate Name | | | Generale Certi | licele Signing Request | | | |
| Batus Top Sources Top Destinations Top Destinations | Subject Information ID Type IP | Heat 3P | | | | | | |
| - Traffic Fatory - Traffic Fatory - Trister Hanny - Trister Hanny - Config - Stands - Stands - Config Centrolese - Config Centrolese - Remain - C.A. Config tes - C.A E.A | Optional Information Organization Construction Locality/City/ Bate/Thiv/site Establishic/City/ Bate/Thiv/site Establishic/City/ Bate/Thiv/site Establishic Subject Alternative Name Key Name Establishic | 654 20 2048 B (g) # File Basel © Online BC2P | | 1 | | | | |
| Bauter Følice Fremøl Objects Secarky Profiles 1978 Dere B. Brenn NAN Dyl. B. Cacho | | | | | | | | |

Rellenamos los campos

| W IT in an visition | 🔆 GLPI - Proceederes 💦 🛪 | Contests R | 🏹 inicia de [ABERITIANEL] 🛪 🏹 🗰 | vmangets Escoltaria | N Content of Sector Larger I.; N | N MARVO Backup & Replic | × 🚺 Ferliker - FWRIDD | |
|--|--|---|---------------------------------|---------------------|----------------------------------|-------------------------|-----------------------|----------------|
| ← → C (kberl//10.14) | 1.117.1/index | | | | | | | 이 슈 🔳 |
| 🗄 Aplicaciones 🛄 Gobierno 🦳 | Torncat 🦲 Grecasa 🦳 Sider | n.ei | | | | | | Otos mesadores |
| FortiGate 1000C | 3 | | | | | | Help Witzerd Legend | FORTIDET |
| System | | | | Generale Certi | ficate Signing Request | | | |
| O Danhoard - * Bana - * Status - * Too Sources - * Too PatriceSou - * Too PatriceSou - * Too PatriceSou - * Too PatriceSou - * Too PatriceSource * * Too Patrice * * * * * * * * * * * * * * * * * | Certificate Name Subject Information Ito Type 27 Organization Loanity(Ctry) Balat/Twome Control/Sagan Ernal Subject Xternative Name | Freezel Freezel g del interface war int angentación gran catación gran catación glana (165) boliemprese an | | | | | | |
| - CA Certificates - CRL R Reniter | Key Type Key Roe Devoluted Hellard | RSA = 2048 BA # 8 File Based © Online SCRP | | | Cancel | | | |
| | | | | | | | | |
| takir . | | | | | | | | |
| Firemall Objects | | | | | | | | |
| Security Prolites | | | | | | | | |
| 175 | | | | | | | | |
| User & Deuton | | | | | | | | |
| WMI Dpt. & Cache | | | | | | | | |
| Log & Report | | | | | | | | |

Al pulsar sobre ok volvemos a la página de Lcal 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 \rightarrow Firma



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

• En source verificar está marcada la opción de usar el certificado raiz que habiamos generado

| 🗸 X Certificate and Key management | ? × |
|---|--|
| Create x509 Certificate | |
| 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 gelf 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 a | and Key mana | gement | | | | ? 🗙 |
|-----------------------|--------------|---------------|---------------|------------|----------|--------------------------|
| Create x5 | 09 Certi | ficate | | | | A ANDRESS STR |
| Source Ex | tensions K | ey usage Nets | cape Advanced | đ | | |
| Basic constra | ints | | | | | Key identifier |
| Туре | Not defined | | | | • | Subject Key Identifier |
| Path length | | | | | Critical | Authority Key Identifier |
| Validez Not before | | 2014-02-14 | 12:48 GMT 👻 | Time range | | Years Apply |
| | | | | | | |
| subject alterna | tive name | | | | | Edit |
| issuer alternati | ve name | | | | | Edit |
| CRL distribution | n point | | | | | Edit |
| Authority Info | Access | OCSP 🔹 | | | | Edit |
| | | | | | | Aceptar Cancelar |

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

| ♂ X Certificate and Key management | ? × |
|--|---|
| Create x509 Certificate | |
| Source Extensions Key usage Netscape Advanced | |
| Key usage | Extended key usage |
| Critical | Critical |
| Digital Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement Certificate Sign CRL Sign Encipher Only Decipher Only | TLS Web Server Authentication TLS Web Client Authentication Code Signing E-mail Protection Time Stamping Microsoft Individual Code Signing Microsoft Commercial Code Signing Microsoft Trust List Signing Microsoft Server Gated Crypto Microsoft Encrypted File System Netscape Server Gated Crypto Microsoft EFS File Recovery IPSec End System IPSec Tunnel IPSec User IP security end entity Microsoft Smartcardlogin OCSP Signing EAP over PPP EAP over Lan |
| | Aceptar Cancelar |

Pulsamos aceptar para que nos firme el certificado.

Depués 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 \rightarrow System \rightarrow Certificates \rightarrow Local Certificate \rightarrow Import \rightarrow Seleccionamos el certificado firmado del paso anterior

Importar Certificado Raiz

System \rightarrow Certificates \rightarrow CA Certificates \rightarrow Import \rightarrow 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

note

Crear certificados para los clientes

Abrimos el XCA \rightarrow Pestaña Certificate signing requests \rightarrow New Request

| 🗸 X Certificate and Key management | ? 💌 |
|--|--|
| Create Certificate signing request | a menut |
| Source Sujeto Extensions Key usage Netscap | e Advanced |
| | |
| Signing request | |
| unstructuredName | |
| challengePassword | |
| | |
| Signing | |
| Create a gelf 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 |

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

| Source Sujeto E | xtensions Key | usage Netscap | pe Advanced | | |
|---------------------|--------------------|---------------|------------------------|----------------|--------|
| Internal name | usuario 1 | | organizationName | miemoreca | |
| countryName | usuario 1 | | organizationalUnitName | mi empresa | |
| stateOrProvinceName | es Rean Canaria | | commonName | emoresa | |
| localityName | Gran Canaria | | emailAddress | tic@empresa.es | |
| Тур | e | | Content | | Add |
| | | | | | Delete |
| | | | | | Delete |

el commonname tiene que coincider 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 \rightarrow 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 signning** y seleccionamos el certificado raíz

| X Certificate and Key management | ? 🗙 |
|---|--|
| Create x509 Certificate | |
| Source Extensions Key usage Netscape Advanced | |
| | |
| Signing request | |
| Sign this Certificate signing request | usuario1 🔹 |
| Copy extensions from the request | Show request |
| Modify subject of the request | |
| Create a gelf 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 |

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 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 not8

Es necesario importar los dos certificados CA_Cert1 y el del cliente

Crear la conexión

Añadimos una nueva conexión con los siguientes parámetros

| E FortiClient | | - • 💌 | | | | |
|---|--|-------|--|--|--|--|
| <u>F</u> ile <u>H</u> elp | | | | | | |
| Create new VPN Connection | | | | | | |
| Nombre de Conexión Tipo Descripción Gateway Remoto Método de Autenticación Certificado X.509 | mi vpn VPN SSL VPN IPsec conexión a mi vpn ip del gateway remoto Certificado X.509 [Prompt on connect] | | | | | |
| Autenticación (XAuth) | Preguntar en el login Guardar login Deshabilitar | G. | | | | |
| A | ceptar Cancelar | | | | | |

La autenticación XAuth la he deshabilitado para simplificar, pero sería recomendable activarla tanto 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

note

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=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%A6y-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: https://intrusos.info/ - **LCWIKI**

Permanent link: https://intrusos.info/doku.php?id=hardware:fortigate:vpn:certificados



Last update: 2023/01/18 14:45