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 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.

Last update: 2023/01/18 14:38

🗹 New Password	? 💌
Contraseña	
Please enter a passv C:/kk.xdb	ord, that will be used to encrypt your private keys in the database file:
Contraseña	
Repeat Contraseña	
Exit	Aceptar Cancelar

Nos aparece la siguiente ventana

Contribute and fay management	- 15 - 1
in the set of the set	
Private Kryes Castiliaate ageng requests Cartiliaate Straphote Revealed into	
Produktivers Confluence Investor lan.	ljen Gy Brent Injenire Joner Ph (AKS+12) Jone Denh Dens

Generar el certificado Raíz

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

X Certificate and Key management	2 x
Create x509 Certificate	
Source Sujeto Extensions Key usage Netscape	Advanced
Similar request	
Signing request	
Sign this Certificate signing request	+
Copy extensions from the request	Show request
Modify subject of the request	
Use this Certificate for signing	
Firma	SHA 1
Template for the new certificate	
[default] CA	•
[bending ex	Andrew Andrew Andrew Andrew
	Appry extensions Appry subject Appry all
	Aceptar Cancelar

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

reate	x509 C	ennicati	-				
Source	Sujeto	Extensions	Key usage	Netscape	Advanced		
Distingu	uished name				_		
Interna	Internal name Certificado Raiz countryName es		organizationName	nombre empresa mi organización			
country			organizationalUnitName				
stateOr	ProvinceName	e Gran Cana	ria		commonName	empresa	
locality/	Name	Gran Cana	ria		emailAddress	tic@miempresa.es	
	Tv	pe			Content		Add
							Delete
							Delete

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

of X Certificate and	Key management	? 🗙
New key		
Please give a name to	o the new key and select the desired keysize	
Key properties		
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 ma	anagement		? ×
Create x509 Cer	tificate		
Source Sujeto Ext	tensions Key usage Netscape	Advanced	
Basic constraints			Key identifier
Type Certificatio	n Authority	•	Subject Key Identifier
Path length		Critical	Authority Key Identifier
Validez		Time range	
Not before	2014-02-13 13:30 GMT 🔹	10	Years Apply
Not after	2015-02-13 13:30 GMT 🔹	Midnight Local time	No well-defined expiration
subject alternative name			Edit
CRL distribution point			Edit
CAL distribution point			
Authority Info Access	UCSP V		Edit
			Aceptar Cancelar

Pestaña Key usage

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

- Digital Signature
- Key Agreement
- Certificate Sign

Source Sujeto Extensions Key usage Gritical Digital Signature Non Repudiation Key Encipherment Data Encipherment Certificate Sign CRL Sign Encipher Only Decipher Only Decipher Only Decipher Only Microsoft Encrypted File System Netscape Server Gated Crypto Microsoft Encrypted File Recovery IPSec Tunnel IPSec Vision IPSecVision <	Create x509 Certificate	
	Source Sujeto Extensions Key usage Add Key usage	vanced Extended key usage Cgitical TLS Web Server Authentication TLS Web Client Authentication Code Signing E-mail Protection Time Stamping Microsoft Individual Code Signing Microsoft Commercial Code Signing Microsoft Commercial Code Signing Microsoft Server Gated Crypto Microsoft Server Gated Crypto Microsoft Ercs File Recovery IPSec End System IPSec Tunnel IPSec User IP security end entity Microsoft Smartcardlogin OCSP Signing EAP over Lan

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

🗹 X Cer	tificate 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 →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

🖉 X Certific	ate and Key management	? ×
Certifik	ate export	A Comment
Please en	ter the filename for the certificate.	
Filename	c:\Cerlificado_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

Crear certificados para los clientes

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

	Sujeto	Extensions	Key usage	Netscape	Advanced		
Signing	request						
unstruc	turedName						
challeng	ePassword						
 Cre Use 	ate a gelf sig this Certific	gned certificate cate for signing	with the serial	1	Certificado	Raiz	Ŧ
O Cre Use	ate a gelf sig this Certific	gned certificate	with the serial	1	Certificado	Raiz	Ţ
 Cre Use Irma Templat 	ate a gelf sig this Certific e for the ne	gned certificate cate for signing w certificate	with the serial	1	Certificado	Raiz	

Seleccionamos nuestra plantilla de CA para generar el nuevo certificado

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

Source Sujeto E	xtensions 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	
-					
lyp	2		Content		Add Delete
Тур	8		Content		Add 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.

Last update: 2023/01/18 14:38

<i>\$</i>	X Certificate and Key management
Nueva clave	
Por favor, asigne un Propiedades de la c	nombre a la nueva clave y seleccione el tamaño deseado lave
Nombre	vpninf
Tipo de dave	RSA
Tamaño de clave	2048 bit 💌
Recordar como v	alores por defecto
	Crear Cancel

Una vez creada la clave vamos a la pestaña **key usage** y seleccionamos del panel de la izquierda \rightarrow 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 signning** y seleccionamos el certificado raíz

Y 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	
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

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

Type Online SCEP File Upload O Upload	Import CA	Certificate				
Upload Opload	Туре	Online SCEP	File			
	Upload	O Upload				
				_		

Importar certificado cliente

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

mport Certificate			
Туре	Local Certificate	PKCS #12 Certificate	Certificate
Certificate with key file	O Upload		
Password		۲	
		ОК	Cancel

Forticlient

Importar certificados al Forticlient

Para usar el certificado de cliente que hemos generado en el equipo del usuario debemos de enviarselo por algún medio y el usario 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

×

Este es el Asistente para im	portar certificados
Este asistente lo ayuda a copiar certificado de revocación de certificados desde su dis	os, listas de certificados de confianza y listas co a un almacén de certificados.
Un certificado, que lo emite una entidad de identidad y contiene información que se us conexiones de red seguras. Un almacén de guardan los certificados.	e certificación, es una confirmación de su sa para proteger datos o para establecer e certificados es el área del sistema donde s
Ubicación del almacén	
 Usuario actual 	
C Equipo local	N
	43

Siguiente	Cancelar

Crear la conexión

Añadimos una nueva conexión con los siguientes parámetros

E FortiClient		- • •
<u>F</u> ile <u>H</u> elp		
Nombre de Conexió Tip Descripció Gateway Remo Método de Autenticació Certificado X.50 Autenticación (XAut	n mi vpn VPN SSL VPN IPsec conexión a mi vpn ip del gateway remoto Certificado X.509 [Prompt on connect] Preguntar en el login Guardar login Deshabilitar	
	Aceptar 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. 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

Last update: 2023/01/18 hardware:fortigate:vpn:ipseccertificados http://wiki.intrusos.info/doku.php?id=hardware:fortigate:vpn:ipseccertificados&rev=1587748939 14:38

Name	nombre identificativo
Subject	subject que pusimos en el certificado
CA	CA_Cert_1

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

VPN Creation Wizard	đ	
1 VPN Setup	Authentication S Policy & Routing	
Name		Site to Site - FortiGate
Template Type	Site to Site Remote Access Custom	
Remote Device Type	e 📰 FortiGate	
	the Cisco	Internet
NAT Configuration	No NAT between sites	
	This site is behind NAT	This FortiGate Remote FortiGate
	The remote site is behind NAT	
	< Back	Next > Cancel

En mi caso voy a generarla utilizando el boton Custom

VPN Creation Wizard	
1 VPN Setup	
Name	
This field is required. Template Type Site to Site Remote Access Custom	
	< Back Next > Cancel

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		▼			

Ponemos la ip de nuestro gateway, el interface, el método de autentificación 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

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	•			

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

E	dit VPN Tunnel							
	Name	vpnin	f					
Comments		Comr	Comments					
	Comments							
	Network			00				
	IP Version		IPv4					
	Remote Gateway		Dialup User 🔹]				
	Interface		Internet Idecnet (wan2)					
	Local Gateway							
	Mode Config							
	Use system DNS in mode con	nfig						
	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		写 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			0 D				
	Method		Signature 🔹					
	Certificate Name		vpninf 🗙 🕇					
	IKE							
	Version		1 2					
	Mode		Aggressive Main (ID protection)					
	Peer Options							
	Accept Types		Peer certificate 🔹					
	Peer certificate		🎝 pki_vpninf 🔹 🔻					

Last update: 2023/01/18 14:38

Phase 1 Propo	sal O Add	C ()
Encryption	AES256 🔻	Authentication SHA512 🔻 🗙
Encryption	AES256 🔻	Authentication SHA256 🕶 🗙
Encryption	AES256 🔻	Authentication SHA1 🔻 🗙
Diffie-Hellmar	Groups	 30 29 28 27 21 20 19 18 17 16 15 14 ✓ 5 2 1
Key Lifetime (s	econds)	86400
Local ID		$\underline{C} = ES, \underline{ST} = \underline{GC}, \underline{L} = \underline{GC}, O = CASA, \underline{OU}$
XAUTH		0 0
Туре		Auto Server 🔹
User Group		Inherit from policy Choose
		🖬 usuariosvpn 🔻

Name Local Addres		ress Remote Address
vpninf	0.0.0.0/0.0	0.0.0 0.0.0.0/0.0.0 🖋
Edit Phase 2		0
Name		vpninf
Comments		Comments
ocal Address		Subnet 0.0.0/0.0.00
lemote Addres	s	Subnet O.0.0/0.0.0
Advanced.		
hase 2 Propos	al O Add	
Incryption	AES256 💌	Authentication SHA512 🕶 🗙
ncryption	AES256 💌	Authentication SHA256 🕶 🗶
ncryption	AES256 💌	Authentication SHA1 🔻 🗙
nable Replay [Detection 🕢	
nable Perfect	Forward Secree	cy (PFS) 💌
Diffie-Hellman	Group	30 29 28 27 21 20 19 18 17 16 15 14 5 2 1
ocal Port		All 💌
Remote Pgrt		All 💌
Protocol		
Autokey Keep A	Alive	
(ey Lifetime		Seconds 🔹
Seconds		43200

Permanent link: http://wiki.intrusos.info/doku.php?id=hardware:fortigate:vpn:ipseccertificados&rev=1587748939	From: http://wiki.intrusos.info/ - LCWIKI	
Last update: 2023/01/18 14:38	Permanent link: http://wiki.intrusos.info/doku.php?id=hardware:fortigate:vpn:ipseccertificados&rev=1587748939	
	Last update: 2023/01/18 14:38	