

Guía de Seguridad de las TIC CCN-STIC 1507

Procedimiento de empleo seguro Forcepoint On-Premise Security 8.5 Anexo IV - Refuerzo de la seguridad en la operación



Noviembre 2021







Catálogo de Publicaciones de la Administración General del Estado https://cpage.mpr.gob.es



NIPO: 083-21-211-1 Fecha de Edición: noviembre de 2021.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

<u>ÍNDICE</u>

1. INTRODUCCIÓN	3
2. HABILITAR EL MODO FIPS EN EL APPLIANCE	4
3. ALMACENAMIENTO DE CLAVES PRIVADAS DE WEB SECURITY APPLIANCE	5
4. CERTIFICADOS PARA INTERCEPCIÓN DE TRÁFICO CIFRADO	6
4.1 CREACIÓN DE UNA SOLICITUD DE FIRMA DE CERTIFICADO (CSR)	7
4.2 FIRMA DE LA SOLICITUD	7
4.2.1 IMPORTAR LA CA RAÍZ SUBORDINADA EN APPLIANCES WEB CONTENT	
GATEWAY	9
4.3 CUSTOM CERTIFICATE KEY	11

1. INTRODUCCIÓN

- 1. Este anexo incluye ajustes de configuración de la solución *Forcepoint Security On-Prem v8.5.x Web* que permiten el funcionamiento de la plataforma de una forma más robusta. Entre estos cambios se incluye:
 - Habilitar el modo de funcionamiento FIPS en los *appliances*.
 - Proteger el almacenamiento de las claves privadas en el *appliance*.
 - Utilizar certificados de alta protección en caso de realizar intercepción sobre el tráfico cifrado en navegación.

2. HABILITAR EL MODO FIPS EN EL APPLIANCE

- 2. Para habilitar el funcionamiento en modo FIPS 140-2 sobre el *appliance* se deben seguir los siguientes pasos:
 - a) En el Content Gateway Manager, acceder a Configure>Security>FIPS Security.

Monitor Configure	
My Proxy	~
Protocols	~
🌌 Content Routing	~
🛉 Security	^
Connection Control	
FIPS Security	
Access Control	
🙀 Subsystems	~
📩 Networking	~
🔒 SSL	*
Figura 1 - Menú FIPS Secu	urity

ligura 1 - Mena III 5 Security

b) Seleccionar *Enabled*. Revisar el aviso que indica que una vez habilitado el modo FIPS no es posible deshabilitarlo sin una reinstalación completa del *appliance*. Pulsar OK y seleccionar *Apply*.

ontent Gateway	192.168.122.15:8081 indique	
FIPS Security	Warning: Once enabled, FIPS enforcement cannot be disabled without a full reinstallation of Content Gateway. For appliances, this requires reimaging the system. To proceed, click on OK and then click Apply to enable FIPS enforcement.	
FIPS (Federal Information Processing Standa only HTTPS connections that use TLSv1 and protocols, and a wide variety of ciphers are s	OK Annuler	ateway can enforce FIPS 140-4 hon-approved algorithms are b
FIPS		
EnabledDisabled	 Enables FIPS 140-2 enforcement on HTTPS connections. Content Gateway. For appliance installations, this requires 	Warning: If enabled, FIPS enforcem : reimaging the system.

Figura 2 - Aviso de habilitación de modo FIPS en Content Gateway Management

c) Reiniciar el Content Gateway Appliance.

3. ALMACENAMIENTO DE CLAVES PRIVADAS DE *WEB SECURITY APPLIANCE*

- 3. *Content Gateway* requiere actuar para la intercepción de tráfico cifrado como una Entidad Certificadora (CA). Para ello es necesario importar el certificado y clave privada correspondiente a dicha CA en el *Content Gateway*. La generación e importación de estas claves se muestran paso a paso en los puntos 4.1 y 4.2.
- 4. Cuando el modo FIPS 140-2 está habilitado (configuración recomendada de acuerdo al punto anterior), el certificado de esta Entidad Certificadora (CA Raíz a partir de ahora) a importar se requiere que tenga formato PKCS # 8 firmado con SHA-256.Para información relativa a los diferentes estándares de intercambio de claves puede consultarse <u>https://es.wikipedia.org/wiki/PKCS</u>.
- Cuando FIPS 140-2 no está habilitado (opción no recomendada), *Content Gateway* puede usar un tipo de clave PKCS # 8 o RSA. Se debe utilizar, en este caso, PKCS # 8, al igual que lo exigido por FIPS 140-2.
- 6. Si la clave privada de la CA raíz no está cifrada con el algoritmo SHA-256, se debe crear una nueva clave privada con formato PKCS # 8 y cifrado SHA-256.
- 7. Si la clave privada de la CA raíz no tiene formato PKCS # 8 pero está cifrada con el algoritmo SHA-256, se puede convertir esa clave a formato PKCS # 8.
- 8. Se puede utilizar el kit de herramientas de OpenSSL para crear o cambiar un certificado. Se recomienda emplear la versión más actualizada disponible. Puede consultarse información relativa a las diferentes versiones y las descargas de cada versión en <u>https://www.openssl.org/</u> desde donde hay enlaces a diferentes servidores con los archivos de instalación.
- 9. Para convertir la clave privada a una clave de formato PKCS # 8, se puede usar:

openssl pkcs8 -in wcg.key -topk8 -v2 aes-256-cbc -v2prf hmacWithSHA256 -out wcgkey_en.pem

donde *wcg.key* es el fichero original de la clave privada y *wcgkey_en.pem* es el fichero resultante de clave privada cifrado.

4. CERTIFICADOS PARA INTERCEPCIÓN DE TRÁFICO CIFRADO

- 10. La plataforma *Forcepoint Content Gateway* permite realizar tareas de intercepción de tráfico cifrado de modo que sea posible inspeccionar y proteger el tráfico de usuarios transmitido a través de protocolo HTTPS.
- 11. Cuando la plataforma inspecciona el tráfico cifrado actúa como proxy de protocolo SSL, descifra contenido y realiza análisis de seguridad y contenido en tiempo real, y vuelve a cifrar el contenido para entregarlo al cliente o al servidor de origen. De este modo, cada petición HTTPS consta de dos (2) sesiones separadas:
 - Uno desde el navegador del cliente a *Content Gateway*. Esta es la conexión entrante.
 - Otro de *Content Gateway* al servidor de origen que recibirá los datos seguros.
 Esta es la conexión saliente.
- 12. En la conexión saliente, el certificado del servidor puede ser validado según diferentes criterios, tales como la fecha de expiración, la confianza en la entidad certificadora, la coincidencia del nombre del sitio y el identificador del certificado, entre otros.
- 13. En la conexión entrante, la establecida entre el navegador del usuario y *Forcepoint Content Gateway*, el *appliance* emite en tiempo real un certificado para esa conexión. Este certificado emitido en el momento es firmado por la entidad certificadora raíz propia del *Content Gateway* o *Internal Root CA*.
- 14. La CA raíz interna predeterminada que se incluye con *Content Gateway* no es única y no debe utilizarse en un entorno de producción.
- 15. Se recomienda reemplazar la CA raíz interna predeterminada por la CA raíz de la organización o crear una nueva.
- 16. Existen tres (3) opciones para crear una CA raíz interna:
 - Aprovechar la CA existente en la organización e importarla a Content Gateway.
 - Crear una nueva CA raíz y ponerla a disposición de los navegadores.
 - Crear una CA subordinada que aproveche una CA existente, pero que también pueda ser revocada por esa CA. Esta es la opción recomendada, de modo que la CA raíz de la organización sea gestionada independientemente de los appliances, y permita generar claves con un tamaño mayor, de tal manera que se pueda gestionar la CA Subordinada y revocarla o cambiarla sin necesidad de desplegar de nuevo los certificados de CA Raíz en los dispositivos de usuario.

4.1 CREACIÓN DE UNA SOLICITUD DE FIRMA DE CERTIFICADO (CSR)

- 17. A continuación, se indican los pasos necesarios para llevar a cabo la creación de una solicitud de firma de certificado (CSR).
 - Iniciar sesión en las máquinas con Windows o Linux con permisos de administrador o root.
 - Abrir un símbolo del sistema o un Shell de comandos.
 - Ingresar el siguiente comando OpenSSL (requiere la instalación previa de OpenSSL toolkit (<u>www.openssl.org</u>):

openssl req - sha256 -new -newkey rsa:3072 -keyout wcg.key -out wcg.csr

Nota: se ha definido un tamaño de clave de 3072 por coherencia con el resto del documento, pero podría emplearse otro tamaño si se deseara (igual o superior a 4096 bits).

- En este paso, se solicitará incluir los datos del certificado tales como país, estado/región, ciudad, dirección de correo electrónico, nombre de organización y unidad y *Common Name* del certificado:
- El comando generará dos (2) ficheros:
 - *wcg.csr*: es la solicitud de certificado (CSR) que será firmada por la CA Raíz de la organización.
 - *wcg.key*: es la clave privada.

4.2 FIRMA DE LA SOLICITUD

- 18. Para utilizar los servicios de certificados de Microsoft para firmar la solicitud:
 - Abrir wcg.csr con un editor de texto que conserve el formato (como Wordpad) y copiar el contenido en el portapapeles (Editar> Seleccionar todo; Editar> Copiar).



Figura 3 - Ejemplo de contenido del fichero *wcg.csr* abierto en *Wordpad*

2) En un navegador, acceder a la entidad certificadora de Microsoft corporativa:

http://<CA_server_IP_address>/certsrv/

Θ	Ittp://192.168.1.254/certsrv/
File Edit	View Favorites Tools Help
🔶 Favorit	is 🛛 👍 🙋 Help Desk 🙋 My Telephone 🙋 Web Slice Gallery 👻 🙋 Webmail
🏉 Microso	ft Certificate Services
Micros	ft Certificate Services – NewsomeCA
Welco	ne
Use thi over the	Web site to request a certificate for your Web browser, e-mail client, or other program Web, sign and encrypt messages, and, depending upon the type of certificate you rec
You ca	also use this Web site to download a certificate authority (CA) certificate, certificate c
	r also ase and web site to download a certificate admonty (or t) certificate, certificate e
For mo	re information about Certificate Services, see <u>Certificate Services Documentation</u> .
For mo	re information about Certificate Services, see <u>Certificate Services Documentation</u> .
For mo Select Req	re information about Certificate Services, see <u>Certificate Services Documentation</u> . a task: <u>Jest a certificate</u>
For mo Select Req Viev	re information about Certificate Services, see <u>Certificate Services Documentation</u> . a task: <u>lest a certificate</u> <u>the status of a pending certificate request</u>

Figura 4 - Acceso a la entidad certificadora de Microsoft mediante interfaz web

- 3) Seleccionar la tarea *Request a certificate*.
- *4)* En la página de solicitud de certificado, seleccionar el enlace *submit a certificate request*.



Figura 5 - Petición de certificado cliente a través de entidad certificadora de Microsoft

5) En la página de solicitud de certificado, seleccionar la opción *Submit a certificate request by using a base-64-encoded CMC*.





6) Pegar el contenido del fichero *wcg.csr* (previamente copiado en el portapapeles) en el campo destinado a tal fin y hacer *click* en *Submit*.

To submit a sav renewal reques	red request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #1 it generated by an external source (such as a Web server) in the Saved Request box.
Saved Request:	
Base-64-encoded certificate request CMC or PKCS #10 or PKCS #7):	bd13ge2X/EQ9zFHKqeFKRU153bs3ZH3vOUJwVe2N yOlpvWAsVzBYn2DchYwvLnRRF7aja6C0fVE1W712Z isdfdfhEQ1HxhEpydnoO3CvmMNJRgjy7d8ez2r6 9eILRYus13zXqeWg3kU= END CERTIFICATE REQUEST
Certificate Temp	late:
	Subordinate Certification Authority 💌
Additional Attrib	utes:
Attributes:	< >

Figura 7 - Petición de firma de certificado a partir del contenido del fichero wcg.csr

7) A continuación, el certificado es emitido y aparece la pantalla Certificado emitido. Si en cambio aparece la pantalla Certificado pendiente, no se disponen de suficientes privilegios para crear una CA subordinada. Se recomienda ponerse en contacto con su administrador de dominio empresarial para completar el proceso de creación del certificado antes de continuar.

	•
ertificate issued	-
he certificate you requested was issued to you.	•
DER encoded or OBase 64 encoded Download certificate Download certificate	
Download certificate chain	

Figura 8 - Descarga de certificado desde la entidad certificadora

- 8) Seleccionar la opción Base 64 encoded y descarcar el nuevo certificado.
- 9) Guardar el certificado para poder importarlo posteriormente en *Forcepoint Content Gateway Appliance* junto con la clave privada generada anteriormente, así como con la CA Raíz de la corporación.

4.2.1 IMPORTAR LA CA RAÍZ SUBORDINADA EN APPLIANCES WEB CONTENT GATEWAY

- 19. Para importar la CA raíz es necesario seguir los siguientes pasos:
 - En el administrador del Content Gateway, ir a la pestaña Configure > SSL >

Internal Root CA > Import Root CA:

FORCEPOINT Web Securit	y Content Gateway		User: admin	Log OH
Monitor Configure				P Help!
Mu Drown	Import Post Cé Conste Dast Cé Dastus Dast Cé			
in Proxy -	Import Root CA Create Root CA Backup Root CA			
Protocols	Internal Root CA			
🔀 Content Routing 🗸 🗸				
🚖 Security 🗸 🗸				
🙀 Subsystems 🗸 🗸	Import Root CA			
Networking ~	Certificate	Choisir un fichier Aucun fichier choisi		
🔒 SSL 🔹 🔺	Cerundate	Please use only base64-encoded certificates.		
Certificates	Private key	Choisir un fichier Aucun fichier choisi		
Decryption / Encryption		Please use only base84-encoded certificates.		
Validation	Passphrase			
Incidents				
Client Certificates	Confirm passphrase			
Customization				
Internal Root CA				
Custom Certificate Key		Import Root CA		

Figura 9 - Menú de importación de certificado raíz en Content Gateway management

- Hacer clic en *Choose File* y buscar para seleccionar el certificado. El certificado debe estar en formato X.509 y codificado en base64.
- Hacer clic en *Choose File* y buscar para seleccionar la clave privada. Debe corresponder al certificado que seleccionó en el Paso 2.
- Ingresar y confirmar la contraseña.
- Haga clic en Import Root CA. La CA importada se almacena en la base de datos de configuración de SSL.

My Proxy	~ I	mport Root CA Create Root CA Backu	p Root CA
🔖 Protocols	~	atomal Doot CA	
🔀 Content Routing	~		
😽 Security	~		
🌍 Subsystems	~	Import Root CA	
Networking	~	Certificate	Choisir un fichier SubCA.cer
🔒 SSL	^		Please use only base64-encoded certificates.
Certificates		Private key	Choisir un fichier SubCA.key.pem
Decryption / Encryption			Please use only base64-encoded certificates.
Validation		Passphrase	•••••
Incidents			
Client Certificates		Confirm passphrase	•••••
Customization			
Internal Root CA			
Custom Certificate Key			Import Root CA

Figura 10 - Menú de importación de certificado raíz con ficheros importados

- Reiniciar el Content Gateway.
- 20. Este procedimiento aquí definido entiende que ya existe una entidad de certificación en la organización. Si no fuera el caso, es posible crear una entidad raíz a través del uso de OpenSSL mediante el comando:

openssl genrsa -out private/ca.key.pem 3072

21. Para generar la clave privada, se ha utilizado un tamaño de clave de 3072 por coherencia con el resto del documento, aunque podría utilizarse una mayor.

22. Y así se obtiene el certificado de CA Raíz. Utilizando esta entidad Certificadora Raíz, es posible generar el certificado de entidad intermedia que posteriormente se utilizará en *Forcepoint Content Gateway Appliance* para la intercepción SSL.

4.3 CUSTOM CERTIFICATE KEY

23. Es posible emplear la opción *Configure > SSL > Custom Certificate Key* para especificar una clave propia codificada en Base-64 que se utiliza en lugar de un par de claves predefinido para generar dinámicamente los certificados de servidor enviados a los clientes.

FORCEPOINT Web Sec	urity	y Content Gateway
Monitor Configure		
My Proxy	~	Import Custom Certificate Key Create Custom Certificate Key Back Up Custom Certificate Key
Protocols	~	Cuctom Partificato Kau
🍂 Content Routing	~	Custom der direkte key
🔗 Security	~	
🔯 Subsystems	~	Import Custom Certificate Key
Networking	~	All fields marked with a * are required.
🔒 SSL	^	Choicir un fichier ductoment nem *
Certificates		Custom Certificate Key Please use a 2048 or 4008 bit RSAkey.
Decryption / Encryption		*
Validation		Passphrase Please use a 440 character passphrase.
Incidents		Confirm passabrase
Client Certificates		
Customization		
Internal Root CA		Impart Custam Catificate Vou
Custom Certificate Key		This may take several seconds. Do not click this button again.

Figura 11 – Importar una clave de certificado personalizada

- 24. Esta clave propia puede ser de longitud 2048 ó 4096. Por motivos de seguridad, se deben usar claves de 4096 bits, de modo que los certificados enviados a los clientes tendrán esa misma longitud.
- 25. Para generar esta clave, es posible hacerlo desde el propio interfaz de *Content Gateway* en el menú *Configure > SSL > Custom Certificate* en la pestaña *Create Custom Certificate Key* y seleccionar el tamaño de clave 4096.
- 26. También es posible importar una clave externa generada por ejemplo a través de OpenSSL mediante el comando:

Openssl genrsa -aes256 -out NewCustomkey.key 4096



27. El fichero de clave obtenido "*NewCustomKey.key*" se importa en el menú *Configure > SSL > Custom Certificate Key* en la pestaña *Import Custom Certificate Key* introduciendo el *passphrase* definido en el momento de su creación, y tras un reinicio del equipo los nuevos certificados creados al vuelo y entregados a los usuarios tendrán una longitud de 4096 bits.







MINISTERIO DE DEFENSA

SUBSECRETARÍA DE DEFENSA SECRETARÍA GENERAL TÉCNICA SUBDIRECCIÓN GENERAL DE PUBLICACIONIES Y PATRIMONIO CULTURAL