centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1507

Procedimiento de empleo seguro
Forcepoint On-Premise Security 8.5
Anexo II - Empleo de mecanismos de cifrado robusto

Noviembre 2021

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN
centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.01.27 13:13:21 +01'00'

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

ÍNDICE

1. INTRODUCCIÓN

1. De cara a reforzar la seguridad en todas las comunicaciones, se procede a configurar los distintos elementos de la solución para que únicamente soporte cifrado basado en TLS v1.2 con los algoritmos de cifrado y fortaleza aprobados.

2. PROTOCOLOS SEGUROS EN SOLUCIÓN *FORCEPOINT WEB SECURITY*

2.1 FORZAR USO DE TLS V1.2 CON ALGORITMOS ACEPTADOS

2. Mediante los siguientes pasos de configuración, se va a forzar el uso exclusivo de TLS v1.2, en la conexión entre los diferentes elementos de la solución, y de los algoritmos de cifrado aprobados.

FSM - *Management UI* (port 9443):

a) Hacer un *backup* del fichero *httpd-ssl.conf* existente en *[...]\Websense\EIP Infra\apache\conf\extra* y abrir a continuación el fichero de configuración (la ruta por defecto de instalación es *C:\Program Files (64)* si bien puede modificarse en el momento de instalación. En el documento se señala [...] como ruta relativa al directorio de instalación, que en caso de haber optado por la instalación por defecto será *C:\Program Files (64)).*

b) Buscar la línea "*SSLProtocol all -SSLv2 -SSLv3*"

c) Reemplazar esa línea con el siguiente contenido: "*SSLProtocol -all +TLSv1.2*"

d) Reiniciar los siguientes servicios:

a. Acceder a la herramienta de gestión de servicios de Windows (ejecutar *services.msc* o acceder mediante las herramientas administrativas de Windows) y detener los siguientes servicios:
Websense TRITON Unified Security Center
Websense TRITON Web Server

b. A continuación, empleando la misma herramienta, arrancar:
Websense TRITON Web Server
Websense TRITON Unified Security Center

FSM - *Web Security Reporting Tools* (port 18443):

a) Hacer un *backup* del fichero *httpd.conf* existente en *[...]\Websense\Web Security\apache\conf\extra* y abrir a continuación el fichero de configuración.

b) Buscar la línea "*Listen 18443*"

c) Reemplazar esa línea con el siguiente contenido: "*Listen 127.0.0.1:18443"*

d) Hacer un *backup* del fichero *httpd.conf* existente en *[...]\Websense\Web Security\apache\conf* y abrir a continuación el fichero de configuración.

e) Buscar la línea *"SSLProtocol all -SSLv2 -SSLv3"*

f) Reemplazar esa línea con el siguiente contenido: "*SSLProtocol -all +TLSv1.2"*

g) Acceder a la herramienta de gestión de servicios de Windows (ejecutar *services.msc* o acceder mediante las herramientas administrativas de Windows) y Reiniciar el servicio "*Websense Web Reporting Tools"*

FSM - Web Security Module (ports 18445 and 18446):

a) Hacer un *backup* del fichero *server.xml* existente en *[...]\Websense\Web Security\tomcat\conf*, y abrir a continuación el fichero de configuración.

b) Buscar la línea que contiene "*sslEnabledProtocols*". Existen 3 pero solo las dos últimas necesitan ser modificadas.

```
[...]
    <!-- Define a forensics repo Connector on port 18444 -->
    <Connector port="${forensics_repo.port}" SSLEnabled="true" server="Websense Apps
Container/7.x"
    maxThreads="150" scheme="https"
protocol="org.apache.coyote.http11.Http11NioProtocol"
    ciphers="TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA"
    secure="true" clientAuth="want" sslProtocol="TLS"
sslEnabledProtocols="TLSv1.2,~~TLSv1.1,TLSv1~~"
    keystoreFile="${https.keystoreFile}"
[...]
    <!-- Define a reporting service Connector on port 18446 -->
    <Connector port="${reporting_service.port}" SSLEnabled="true" server="Websense
Apps Container/7.x"
    maxThreads="150" scheme="https"
protocol="org.apache.coyote.http11.Http11NioProtocol"
    ciphers="TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA"
    secure="true" clientAuth="want" sslProtocol="TLS"
sslEnabledProtocols="TLSv1.2,~~TLSv1.1,TLSv1~~"
    keystoreFile="${https.keystoreFile}"
[...]
```

c) Eliminar "*TLSv1*" y/o "*TLSv1*.1" de esas líneas si existieran.

d) Reiniciar el servicio "*Websense TRITON - Web Security service*".

FSM - Real-Time Monitor (port 9445):

a) Hacer un *backup* del fichero *server.xml* existente en *[...]\Web Security\rtm\tomcat\conf*, y abrir a continuación el fichero de configuración.

b) Buscar la etiqueta que comienza por *<Connector port="${https.port}"*

c) Fijar la variable *sslEnabledProtocols* a *sslEnabledProtocols="TLSv1.2".*

d) Reemplazar la lista de cifrados con los siguientes valores:
ciphers="TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384".

e) Guardar y reiniciar el servicio "*Websense RTM Client service*".

Forcepoint Web Content Gateway appliances – Management UI (port 8081):

NOTA: Los siguientes cambios harán que los *appliances Forcepoint Content Gateway* no puedan ser gestionados mediante el navegador Firefox, ya que Firefox no admite ninguno de los cifrados utilizados.

a) Acceder a la línea de comandos del *appliance* mediante conexión SSH y entrar en modo configuración ejecutando el comando *config* (solicitará las credenciales de administración nuevamente).

b) Ejecutar el siguiente comando:

set proxy content_line --entry proxy.config.admin.supported_cipher_list --value AES256-GCM-SHA384,AES256-SHA256,AES128-GCM-SHA256,AES128-SHA256 --type set

2.2 USO DE CURVAS ELÍPTICAS 256 BITS EN EL SERVIDOR DE GESTIÓN

3. En el servidor de administración Windows, se debe editar el archivo *C:\Archivos de programa (x86)\Websense\EIP Infra\apache\conf\extra\httpd-ssl.conf* para agregar las siguientes dos (2) directivas. Se pueden colocar en cualquier lugar del fichero, pero tiene sentido colocarlos inmediatamente después de la directiva *SSLCipherSuite*.
    - *SSLOpenSSLConfCmd Curves prime256v1:secp384r1:secp521r1*
    - *SSLOpenSSLConfCmd ECDHParameters Automatic*
4. Tras modificar el fichero, reiniciar el servicio "*Websense TRITON Web Server*".

2.3 CAMBIO DEL CERTIFICADO DEL INTERFAZ DE GESTIÓN

5. Con objeto de mejorar la seguridad en la conexión entre los administradores y el interfaz de gestión, se recomienda cambiar el certificado de la interfaz de gestión para garantizar que el **tamaño mínimo de clave privada es de 3072 bits**. Este cambio se realizará en el servidor FSM y en los *appliances Web Content Gateway* tal y como se describe a continuación.

2.3.1 FORCEPOINT SECURITY MANAGER

6. A continuación, se definen los pasos a realizar en el FSM:
    a) **Creación de un nuevo certificado:** Se creará un nuevo certificado de 3072 bits en sustitución del certificado por defecto de 2048 bits. Para ello, se siguen los siguientes pasos:
        i. Será necesario actualizar dos ficheros de configuración incluidos en el directorio de instalación K/SSL/Automation (por defecto *C:\Program Files (x86)\Websense\Web Security\apache\conf\ssl\automation\):*

        * **s1_newreq.bat** – se edita el fichero de la siguiente manera con objeto de que el nuevo certificado sea cifrado con sha256:
        fichero original: *"C:\Program Files (x86)\Websense\Web Security\apache\bin\openssl.exe" req -new > "C:\Program Files (x86)\Websense\Web*

Security\apache\conf\ssl\output\new.cert.csr" -keyout "C:\Program Files (x86)\Websense\Web Security\apache\conf\ssl\output\cakey.pem" -config "C:\Program Files (x86)\Websense\Web Security\apache\conf\ssl\openssl.cnf" -passin pass:spring_forward -passout pass:spring_forward < "C:\Program Files (x86)\Websense\Web Security\apache\conf\ssl\openssl.txt"

Insertar **"-sha256"** para que el archivo quede del siguiente modo:
[...]apache\bin\openssl.exe" req -sha256 -new > "C:\Program Files (x86)\[...]

Insertar **"-newkey *rsa*:3072"** para que el archivo quede del siguiente modo:
[...]output\new.cert.csr" -newkey rsa: 3072 -keyout "C:\Program Files (x86)\[...]

* **s3_server.crt** – se edita el fichero de la siguiente manera:
fichero original: *"C:\Program Files (x86)\Websense\Web Security\apache\bin\openssl.exe" x509 -in "C:\Program Files (x86)\Websense\Web Security\apache\conf\ssl\output\new.cert.csr" -out "C:\Program Files (x86)\Websense\Web Security\apache\conf\ssl\output\server.crt" -req -signkey "C:\Program Files (x86)\Websense\Web Security\apache\conf\ssl\output\server.key" -days 1095*

Insertar ***-sha256*** y ***-extfile*** *..\opensslv3.txt* entre *x509* y *-in* para que el archivo quede del siguiente modo*:*
[...]bin\openssl.exe" x509 -sha256 -extfile "C:\Program Files (x86)\Websense\Web Security\apache\conf\ssl\opensslv3.txt" -in "C:\Program[...]

ii. Crear un nuevo fichero (o editar, si ya existe) llamado opensslv3.txt en el directorio:

C:\Program Files (x86)\Websense\Web Security\apache\conf\ssl

e incluir en él el siguiente contenido (al final de cada línea debe incluirse un salto de línea):

```
basicConstraints = CA:FALSE
nsComment = "Triton Certificate"
subjectKeyIdentifier=hash
subjectAltName = @alt_names
[alt_names]
DNS.1   = <IPv4 Address>
DNS.2   = <FQDN >
IP.1    = <IPv4 Address>
```

iii. Crear un nuevo fichero (o editar si ya existiera) llamado *openssl.txt*, en el directorio:

C:\Program Files (x86)\Websense\Web Security\apache\conf\ssl

e incluir en él el siguiente contenido (al final de cada línea debe incluirse un salto de línea):

```
US
CA
SanDiego
Websense
Websense
<IPv4 Address>
<FQDN>
```

`spring_forward`

Nota: *IPv4 Address*= Dirección IP del servidor FSM para el que se genera el certificado

Nota: *FQDN= Fully qualified domain name* del servidor FSM para el que se genera el certificado

iv. Una vez modificados los ficheros, han de ejecutarse los siguientes scripts contenidos en el directorio:

C:\Program Files (x86)\Websense\Web Security\apache\conf\ssl\automation

en el siguiente orden y con permisos de administrador:

s1_newreq.bat
s2_server_key.bat
s3_server_crt.bat

v. Una vez ejecutados, se habrán generado los siguientes ficheros:

cakey.pem
new.cert.csr
server.crt
server.key
manager.p12

En el directorio:

C:\Program Files (x86)\Websense\Web Security\apache\conf\ssl\output

Donde *Server.crt* y *Server.key* se corresponden con la clave pública y la clave privada del nuevo certificado generado.

b) Instalación del nuevo certificado:

i. Detener los servicios *Websense TRITON Web Security* y *Websense TRITON Web Server* en el servidor FSM.

ii. Copiar el nuevo fichero *server.crt* en el directorio *C:\Program Files (x86)\Websense\Web Security\apache\conf\ssl\ssl.crt*

iii. Copiar el nuevo fichero *server.crt* en el directorio *C:\Program Files (x86)\Websense\EIP Infra\apache\conf\keystore\httpd* y renombrarlo como *httpd-server.cer.*

iv. Copiar el nuevo fichero *server.key* en el directorio *C:\Program Files (x86)\Websense\Web Security\apache\conf\ssl\ssl.key*

v. Copiar el nuevo fichero *server.key* en el directorio *C:\Program Files (x86)\Websense\EIP Infra\apache\conf\keystore\httpd* y renombrarlo como *httpd-server.key.pk8* (la opción de ocultar la extensión de los ficheros en la carpeta debe estar deshabilitada).

vi. Editar el archivo *extra\httpd-ssl.conf* contenido en el directorio *C:\Program Files (x86)\Websense\EIP Infra\apache\conf* añadiendo el

carácter "#" al inicio de la siguiente frase: *SSLCertificateChainFile conf/keystore/httpd/httpd-ca.cer*. De este modo queda comentado y no tiene efecto.

vii. Arrancar de nuevo los servicios *Websense TRITON Web Security* y *Websense TRITON Web Server* en el servidor FSM.

***Nota**: Puede encontrar información detallada del procedimiento en la siguiente nota técnica: https://support.forcepoint.com/KBArticle?id=creating-stronger-certificates.*

2.3.2 CONTENT GATEWAY APPLIANCE

7. Los pasos a realizar en el *Content Gateway Appliance* son los siguientes:

   a) Crear un nuevo certificado siguiendo los mismos pasos explicados en el punto anterior "2.3.1 FORCEPOINT SECURITY MANAGER" apartado *a) "Creación de un nuevo Certificado"*. Se deben repetir los pasos indicados en los subapartados i), ii), iii) y iv).

   b) Importar el certificado en el *Content Gateway appliance*.

Nota: Contactar con el servicio de soporte técnico de Forcepoint para poder actualizar el certificado en el *Forcepoint Content Gateway Appliance*. Para ello, es necesario habilitar el acceso de soporte técnico. El proceso para otorgar acceso al *appliance* a personal de soporte técnico se detalla en el *"Anexo I – Configuración de Administración Segura"*, apartado *"2.2- Acceso Restringido a los appliances a través de FSM"*. Los pasos que realizará el soporte técnico serán:

   a) Guardar una copia del archivo */opt/WCG/config/server.pem.*

   b) Copiar los ficheros *server.key* y *server.crt* en el directorio */opt/WCG/config.*

   c) Combinar los ficheros *server.key* y *server.crt* en un único fichero. Desde línea de comandos se ejecutará:

      cat server.key > server.pem
      cat server.crt >> server.pem

   d) Reiniciar el *appliance Content Gateway* mediante ejecución del comando:

      /opt/WCG/WCGAdmin restart

3. USO DE PROTOCOLOS SEGUROS EN FORCEPOINT DLP

8. Las comunicaciones entre el servidor DLP y los *endpoint* DLP están protegidas por TLS para protegerlas de la divulgación y modificación. Como recomendación, **se debe configurar que la versión TLS a utilizar sea TLSv1.2.**

9. Esto protege las políticas que se implementan en los dispositivos del cliente, así como las acciones tomadas por clientes como resultado de las políticas aplicadas. La protección lógica de estas comunicaciones es necesaria ya que los *endpoints* DLP no se ubican junto con el resto del entorno y, como tales, no se benefician de la protección física de una instalación segura.

10. Para forzar la utilización de TLSv1.2, es necesario realizar los siguientes cambios sobre cada uno de los siguientes procesos:

    a. ***Endpoint Server*** **(puerto 443, 17509)**. Este proceso escucha los estados e incidentes del Agente *Endpoint* de Forcepoint. Como se trata de un servidor Apache, se puede configurar en la configuración del servidor Apache. Para configurar *Endpoint Server* con TLSv1.2 para que utilice únicamente cifrado fuerte, será necesario seguir las siguientes acciones:

    - En la máquina donde resida el *Endpoint Server*, abrir el archivo *%DSS_HOME%\apache\conf\extra\httpd-ssl.conf*
    - Buscar la línea que contenga el atributo: *SSLProtocol*
    - En las líneas identificadas, redefinir el atributo con: *SSLProtocol -all +TLSv1.2*
    - Bajo todas las líneas identificadas, añadir el atributo: *SSLCompression Off*
    - Bajo todas las líneas identificadas, añadir el atributo: SSLHonorCipherOrder on
    - Bajo todas las líneas identificadas, añadir el atributo: *SSLOptions +StrictRequire* (si el atributo *SSLOptions* ya existía, añadir *"+StrictRequire"* al valor)
    - Buscar todas las líneas que contengan el atributo *SSLCipherSuite*
    - En todas las líneas localizadas redefinir el atributo con el siguiente valor: *SSLCipherSuite EECDH+AES128:RSA+AES128:EECDH+AES256:RSA+AES256*
    - Buscar todas las líneas que contengan el atributo *SSLOptions*. Si en alguna de las líneas no existe el valor *'+StrictRequire',* añadirlo.
    - Reiniciar el servicio *"Websense Data Security Web Server"*. Se reiniciará el Endpoint Server.

    b. ***JAVA Manager*** **(puerto 17443)**. Este servicio monitoriza los estados del *Endpoint Server* y los incidentes de *Policy Engine*. Como se trata de un

servidor *Tomcat*, se puede configurar en la configuración del servidor *Tomcat*. Para configurar el Management Server con TLSv1.2 para que utilice únicamente cifrado fuerte, será necesario seguir las siguientes acciones:

- En el servidor de gestión abrir el archivo:

  %DSS_HOME%\tomcat\conf\server.xml

- Buscar la etiqueta "*Connector*" con *attribute port="17443"*
- En esta etiqueta de conector buscar el atributo "*sslEnabledProtocols*" y borrar de todos sus valores todos los protocolos excepto TLSv1.2
- Todos los cifrados en este archivo son considerados seguros y no necesitan ser cambiados.
- Reiniciar el servicio "*Websense Data Security Manager*". Se reiniciará el *DSS Manager*.

c. ***Management Daemon*** **(Puertos 17500, 17090, 17000)** – Monitoriza los despliegues de gestión.

- Existe un ítem de configuración en *mgmtd.config.xml,* en el directorio *%DSS_HOME%* para *routing soap* (iniciado por Manager y *Forcepoint Crawlers*): *SoapRouterSslFlagsHexdecimal*. Su valor por defecto es *0x0000*, y su valor hace referencia a aceptar todas las versiones de TLS 1.x. Para recibir sólo versiones TLSv1.2, cambiar el valor de este ítem a *0x0400*.
- Existe otro ítem de configuración en el fichero *mgmtd.config.xml* que permite la reconfiguración remota indicando el *Policy Engine ID (PEI)* de los elementos (puerto 17090): *LocalOpenSSLFlagsHexDecimal*. Su valor por defecto es *0x03000000*, y su valor hace referencia a aceptar todas las versiones de TLS 1.x. Para recibir sólo versiones TLSv1.2, se debe cambiar el valor de este ítem a *0x17000000*.
- Deshabilitar la tarea programada *Forcepoint DLP Watchdog* existente en las tareas programadas (*Scheduled tasks*) de Windows. *Forcepoint DLP Watchdog* es un servicio de la solución que se encarga de verificar que todos los componentes de la solución están funcionando correctamente, y de mantener habilitados los servicios correspondientes. Es necesario detener esta tarea para poder reiniciar el servicio *"Websense Management Server".*
- Reiniciar el servicio "*Websense Management Server*".
- Habilitar de nuevo la tarea programada *Forcepoint DLP Watchdog* existente en las tareas programadas (*Scheduled tasks*) de Windows.

d. ***Fingerprint Repository*** **(puerto 17506)**. Monitoriza el componente *Crawler*. El componente *Crawler* son las tareas encargadas de llevar a cabo la recolección de información (*Fingerprinting*) y el descubrimiento de información en unidades de almacenamiento compartido (*Discovery / Data at Rest*). Estas

tareas de descubrimiento consisten en localizar información sensible que se encuentre almacenada en unidades de almacenamiento compartido, de modo que permiten detectar si la información sensible está en ubicaciones donde no debe estar, y tomar acciones para corregir esa posible fuga de información.

- Existe un ítem de configuración en *%DSS_HOME%\FPR.config.xml:*

  SSLFlagsHexDecimal (Full XML path: FingerprintRepository/OpenSSL/SSLFlagsHexDecimal).

  Su valor por defecto es *0x03000000*, y su valor hace referencia a aceptar todas las versiones de TLS 1.x. Para recibir sólo versiones TLSv1.2, se debe cambiar el valor de este ítem a *0x17000000*.

  <OpenSSL>
  <SSLKeyfile>C:\Program Files (x86)\Websense\Data Security\HostCert.key</SSLKeyfile>
  <SSLFlagsHexDecimal>0x17000000</SSLFlagsHexDecimal>
  <SSLCertFile>C:\Program Files (x86)\Websense\Data Security\allcerts.cer</SSLCertFile>
  <SSLCertPasswd/>
  </OpenSSL>

- Reiniciar el servicio "*Websense Data Fingerprint Database*". Esto reiniciará el servicio *Fingerprint Repository*.

e. **Policy Engine (puerto 17503)**. Monitoriza las transacciones de los agentes.

- Existe un ítem de configuración en *PolicyEngine.config.xml*: *OpenSSLFlagsHexDecimal*. Su valor por defecto es *0x03000000*, y su valor hace referencia a aceptar todas las versiones de TLS 1.x. Para recibir solo versiones TLSv1.2, se debe cambiar el valor de este ítem a *0x17000000*.
- Reiniciar el servicio "*Websense Data Policy Engine*". Se reiniciará el servicio *Policy Engine*.

f. **OCR Server (puerto 17512)**. Monitoriza peticiones OCR del *Policy Engine*.

- Existe un ítem de configuración en *%DSS_HOME%\OCR.config.xml: OCRSslFlagsHexDecimal*. Su valor por defecto es 0x03000000, y su valor hace referencia a aceptar todas las versiones de TLS 1.x. Para recibir sólo versiones TLSv1.2, se debe cambiar el valor de este ítem a *0x17000000.*
- Reiniciar el servicio "*Websense OCR*".

g. **Management Server – Puerto de gestión 9443**

- Localizar y editar el archivo: *\EIP Infra\apache\conf\extra\httpd-ssl.conf.*
- En todas las líneas coincidentes redefinir el siguiente atributo: *SSLProtocol -all +TLSv1.2*
- Localizar y editar el archivo: *\EIP Infra\tomcat\conf\server.xml*

- Añadir la siguiente entrada:

```
<!-- Define an AJP 1.3 Connector on port 19442 -->
<Connector port="19442" protocol="AJP/1.3" redirectPort="9443"
maxThreads="500" address="127.0.0.1" sslEnabledProtocols="TLSv1.2"/>
```

h. **Management Server – Puertos del gestor de la mensajería 17513 y 17514**

- Localizar y editar el archivo: *\MessageBroker\conf\activemq.xml*
- Buscar la cadena *"stop+ssl"*
- Al final de la línea añadir: *"&transport.enabledProtocols=TLSv1.2"*

```
<transportConnector name="stomp+ssl"
uri="stomp+ssl://0.0.0.0:17513?maximumConnections=10&amp;amp;wireFormat.maxFra
meSize=104857600&amp;amp;needClientAuth=true&amp;amp;transport.enabledCipherSuites=T
LS_RSA_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WIT
H_AES_256_CBC_SHA&amp;amp;transport.enabledProtocols=TLSv1.2"/>
```

- Reiniciar el Servicio "*DSSMessageBroker*" ("*Websense Data Security Message Broker*").
- Localizar y editar el archivo: *MessageBroker\conf\Jetty.xml*
- Buscar "*org.eclipse.jetty.util.ssl.SslContextFactory*"
- Añadir la etiqueta:

```
<property name="excludeProtocols" value="SSLv3,TLSv1, TLSv1.1" />
```

- Reiniciar el servicio "*DSSMessageBroker*".

11. Todas las comunicaciones entre los *endpoints* y los servidores se cifran en su comunicación con el *Endpoint Serv*er de Forcepoint DLP. Cuando el *endpoint* se comunica con el *Endpoint Server*, negocia la conexión segura utilizando un algoritmo aprobado por FIPS 140-2 según lo dictado por el servidor. El uso de TLSv1.2 se aplica en la comunicación de *endpoint* a servidor.

12. Por lo general, el algoritmo de elección para la comunicación *Endpoint-Servidor* es **AES-256**. Sin embargo, el *Endpoint Server* con el que el *endpoint* se comunica a través de HTTPS está configurado con la siguiente cadena de cifrado: *"TLSv1.2+FIPS:kRSA+FIPS:!eNULL:!*aNULL". La cadena indica la selección de versión TLSv1.2 en modo FIPS *compliant* y los métodos de cifrado correspondientes al uso del *appliance* en modo FIPS *compliant*; deshabilitando el resto de protocolos. Lo que significa es que el *endpoint* puede usar cualquiera de estos protocolos de cifrado para cifrar la comunicación con el servidor (dependiendo de cómo el *Endpoint Server* responda a la comunicación inicial del *endpoint*).

PUBLICACIONES DE DEFENSA
GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL