centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1507

Procedimiento de empleo seguro
Forcepoint On-Premise Security 8.5
Anexo III - Comunicación Segura entre FSM y Web Content

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 13:14:02 +01'00'

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

ÍNDICE

1. INTRODUCCIÓN

1. La comunicación entre los diferentes servicios de la solución está filtrada al centralizarse a través del *Policy Server*. Cada servicio tiene su propia clave de filtrado que se genera en la instalación y permite la identificación de los servicios entre sí en el establecimiento de la comunicación. Sin embargo, existe una excepción en este sentido: la comunicación entre los servicios *Filtering Service* de los *appliances* y *Log Service* del FSM no está cifrada.
2. Esta comunicación se produce desde los *appliances* hacia el servidor en el que se ubica el *Log Server*, tradicionamente el FSM, a través del puerto 55805. Se trata de un protocolo de comunicación propietario, que no se encuentra cifrado.
3. De cara a evitar la transmisión de datos sin cifrar, se configura como parte del proceso de empleo seguro de la solución el **establecimiento de un canal de comunicación cifrado entre los *appliances* y el servidor FSM, de modo que la comunicación entre *Filtering Service* y *Logs Server* se realice a través de este canal cifrado.**

2. COMUNICACIÓN ENTRE APPLIANCES Y SERVIDOR FSM A TRAVÉS DEL INTERFAZ C

4. La comunicación entre los *appliances Web Content Gateway* y la estación de gestión FSM se realizará siempre a través del interfaz C del *appliance* (interfaz empleado por el servicio *Web Security*, a través del que se realiza la gestión del *appliance*). Para que ello funcione correctamente, es necesario redirigir las peticiones hacia la estación de gestión que habitualmente utilizarían otros interfaces del *appliance* para que empleen el interfaz de gestión (C). Esta configuración requiere seguir los siguientes pasos en los *appliances Web Content Gateway* mediante conexión SSH:

```
login as: admin                    [acceso al appliance]
web.demo.com(view)# config         [acceso a modo configuración]
Password:  ************
web.demo.com(config)# set component_route --dest 192.168.122.21 --mask
255.255.255.255 --module proxy
[establecimiento de ruta interna del appliance para que todos los servicios se
comuniquen con el servidor de gestión FSM a través del módulo proxy]
web.demo.com(config)# show component_route
+---------------+----------------+-------------+--------+
|  Destination  |    Netmask     | Module Name | Active |
+---------------+----------------+-------------+--------+
| 192.168.122.21 | 255.255.255.255 |   proxy   |  Y   |
+---------------+----------------+-------------+--------+
web.demo.com(config)#
```

2.1 INSTALACIÓN DE *OPENSSH SERVER* EN FSM

5. Se habilita un servicio de servidor SSH en el FSM. En función de la versión de sistema operativo empleado se realiza de diferente forma.

2.1.1 SISTEMA OPERATIVO WINDOWS 2019

Para el sistema operativo Windows 2019, los pasos a seguir son:

a) Ejecutar *PowerShell* como administrador en el servidor. Para verificar la disponibilidad de *OpenSSH.Server* ejecutar el siguiente comando:

```
>Get-WindowsCapability -Online | ? Name -like 'OpenSSH.Server*'
```

El comando devolverá una salida similar a esta:

```
Name  : OpenSSH.Server    0.0.1.0

State : NotPresent
```

b) Con el siguiente comando, se instalará *OpenSSH.Server*:

```
>Add-WindowsCapability -Online -Name OpenSSH.Server    0.0.1.0
```

Devolverá la siguiente salida:

Path :

Online : True

RestartNeeded : False

2.1.2 SISTEMA OPERATIVO WINDOWS 2016 (O ANTERIOR)

6. Windows Server 2016 no incluye OpenSSH como parte del sistema operativo, por lo que sería necesaria su instalación como aplicativo externo.

2.2 PROTECCIÓN DEL SERVIDOR SSH

2.2.1 CREACIÓN DE USUARIO LOCAL PARA SU USO EXCLUSIVO DE ACCESO SSH

7. Se debe crear un usuario en el servidor FSM con permisos únicamente de usuario local que se utilizará para el acceso SSH. Ningún otro usuario tendrá acceso SSH al servidor. Para ello:

   a) Ejecutar *PowerShell* como administrador en el servidor. Se crea un *password* para el usuario en modo seguro:

   >$Password = Read-Host -AsSecureString

   b) Utilizar la mencionada variable *password* para asignársela al usuario

   >New-LocalUser "ssh" -Password $Password -FullName "sshuser" -Description "usuario para acceso SSH"

   El comando crea un nuevo usuario de nombre "*ssh*" asignándole el *password* creado en el paso anterior, al que se le otorga un nombre completo de usuario "*sshuser*" y una descripción del mismo donde se señala que será el usuario utilizado para acceso SSH.

2.2.2 MODIFICACIÓN DE LA CONFIGURACIÓN DE OPENSSH SERVER

8. Se modifica el puerto de escucha para utilizar un puerto no estándar como medida adicional de seguridad (por ejemplo, puerto TCP 55822) para:

   a) Permitir únicamente el acceso al nuevo usuario creado.

   b) Aceptar únicamente conexiones desde las direcciones IP de los *appliances*.

   c) Aceptar únicamente conexiones autenticadas con certificado cliente, y se deshabilita la autenticación por contraseña. De este modo solo teniendo la clave privada correspondiente a la clave pública configurada en el servidor podrá establecerse una comunicación SSH con el servidor FSM. Este último punto se realizará una vez configurado el par de claves a utilizar en el *appliance*.

d) Utilizar únicamente métodos de cifrado robustos incluidos en la guía CCN-STIC-807. En este caso como se tiene control de servidor y cliente, se especifican únicamente los métodos de cifrado más robustos soportados por ambos extremos.

e) Configurar un volumen (1G) y un tiempo (1hora) definidos para la renegociación de claves en la conexión cifrada.

9. Para realizar estas acciones **es necesario modificar el fichero de configuración *sshd_config***, que reside en el caso de la instalación sobre Windows Server 2019 en el directorio *%programdata%\ssh*, y en el caso de la instalación sobre Windows Server 2016 en el directorio definido durante la instalación (por defecto *C:\Program Data\ssh* con nombre *ssh_config*). Las modificaciones son:

   a) Modificación de puerto de escucha:

      Buscar la línea

      #port 22

      y sustituir por (nótese que la regla original estaba comentada, la modificada no)

      port 55822

   b) Restringir la escucha a la dirección IP del servidor que se comunique con los appliances:

      Buscar la línea

      #ListenAddress 0.0.0.0

      y sustituir por (nótese que la regla original estaba comentada, la modificada no)

      ListenAddress <ip_address_FSMServer>

   c) Limitación de acceso a usuario definido:

      Añadir al fichero de configuración la siguiente línea:

      AllowUsers <nombre_del_usuario>

   d) Limitación de acceso desde la dirección IP de el/los appliances:

      Sobre la línea anterior, donde se define el usuario permitido, añadir la dirección IP de los appliances desde los que se permitirá la conexión.

      AllowUsers ssh@<dir_ip_appliance1> ssh@<dir_ip_appliance2>

      Como recomendaciones adicionales, aunque no estrictamente necesarias, se pueden añadir los siguientes parámetros de configuración:

   e) Deshabilitar acceso a usuario con password vacia

      PermitEmptyPasswords no

f) Definir un tiempo máximo de sesión (deberá ser mayor que el intervalo de mensajes keepalive definido posteriormente):

ClientAliveInterval 300

g) No permitir la autenticación basada en hosts:

Buscar la línea

 # HostbasedAuthentication no

y sustituir por (nótese que la regla original estaba comentada, la modificada no)

HostbasedAuthentication no

h) Configurar un volumen y un tiempo definidos para la renegociación de claves

Buscar la línea

RekeyLimit default none

y sustituir por:

RekeyLimit 1G 1h

i) Debido a que en esta comunicación se tiene control tanto del servidor como del cliente, es posible establecer una configuración de métodos de cifrado soportados muy restringida, sin necesidad de que el servidor deba soportar un amplio número de algoritmos criptográficos. Por este motivo, en la sección de configuración de métodos cifrado se configura de la siguiente manera:

   i. Limitar el tipo de clave pública aceptada a ecdsa-sha2-521, dado que es el configurado en los *appliances* y no es necesario soportar ningún otro:

      PubkeyAcceptedKeyTypes ecdsa-sha2-nistp521

   ii. Restringir el KEX (Key Exchange) algorithm al utilizado por el cliente:

      KexAlgorithms ecdh-sha2-nistp521

   iii. Especificar el método de cifrado permitido haciéndolo estricto para su uso con los *appliances*, de modo que únicamente se utiliza este método:

      Ciphers aes256-ctr

   iv. Especificar el MAC (*Message Authentication Code*) algorithm permitido haciéndolo estricto para su uso con los *appliances*:

      MACs hmac-sha2-512-etm@openssh.com

2.2.3 INICIO DEL SERVICIO

10. Una vez establecida la configuración de seguridad del servidor es posible arrancar el servicio:

a) Iniciar el servicio sshd:

>Start Service sshd

b) Configurar el servicio para su inicio automático:

>Set-Service -Name sshd -StartupType 'Automatic'

c) Automáticamente se crea una regla de Firewall en el servidor. Puede confirmarse con el siguiente comando:

*>Get-NetFirewallRule -Name *ssh**

d) La nueva regla debe llamarse "OpenSSH-Server-In-TCP", habilitada con las opciones por defecto. Es necesario modificar el puerto de escucha en la regla del Firewall mediante el siguiente comando:

>Set-NetFirewallRule -Name OpenSSH-Server-In-TCP -LocalPort 55822

e) Es posible confirmar la configuración del nuevo puerto de la regla con el siguiente comando:

>Get-NetFirewallRule -Name OpenSSH-Server-In-TCP | Get-NetFirewallPortFilter

f) En caso de que dicha regla no fuera creada automáticamente (esto puede ocurrir en Windows 2016) es posible crearla con el siguiente comando:

>New-NetFirewallRule -Name OpenSSH-Server-in-TCP -DisplayName OpenSSH-Server -Direction Inbound -Protocol TCP -LocalPort 55822 -Action Allow

2.3 CONFIGURACIÓN DEL APPLIANCE

11. Para realizar esta tarea es necesario acceder al *appliance* con permisos de administrador, para lo que se requiere la participación de Servicios Profesionales o Soporte Técnico de Forcepoint, al tratarse de un acceso restringido.
12. Los pasos que se seguirán para la configuración serán los siguientes:
    a) Establecimiento del par de claves que serán utilizadas para la autenticación en la conexión SSH con el servidor FSM asociadas únicamente al usuario "*ssh*" creado para este fin.
    b) Definición de permisos en *firewall* interno del *appliance* para permitir la comunicación con el servidor FSM a través del puerto del servicio Log Server.
    c) Configuración de parámetros a utilizar para el establecimiento de la conexión.
    d) Configuración de mantenimiento de la conexión e inicio y reinicio automático.
13. Las actividades realizadas por parte de Servicios Profesionales o Tech Support de Forcepoint, con permisos de Administración, serán:
    a) Generación de par de claves para autenticación de usuario basada en

ECDSA 521. Estas claves se asociarán al usuario creado en el servidor FSM para permitir la conexión segura.

> ssh-keygen -t ecdsa -b 521

> ls ~/.ssh

Se obtienen así los archivos *id_ecdsa* e *id_ecdsa.pub.*

Mediante el siguiente comando se restringen los permisos de acceso a la clave privada:

> chmod 400 ~/.ssh/id_ecdsa

b) Definición de permisos en *firewall* Interno del *appliance*. Internamente el *appliance* dispone de un servicio de firewall que controla la comunicación de los diferentes servicios y las comunicaciones con el exterior. Es necesario por tanto permitir la comunicación del servicio *Log Server* con el servidor FSM a través del puerto definido anteriormente de escucha del SSH.

> iptables -I INPUT 10 -i br-mgmt -p tcp -s 169.254.254.3/32 --dport 55805 -j ACCEPT

> iptables-save>/tmp/iptable

> mv -f /tmp/iptable /etc/sysconfig/iptables

> service iptables restart (reinicia el servicio iptables para hacer efectivos los cambios)

c) Definición de parámetros de conexión para el establecimiento del túnel SSH

Se crea/edita el fichero *~/.ssh/config*, incluyendo la creación de un host que facilite la conexión con el servidor FSM con la siguiente información:

> vi ~/.ssh/config

Host FSM

HostName <FSM Server IP Address>

Port *<ssh listening port>*

User *<ssh created user in FSM Server>*

IdentityFile ~/.ssh/id_ecdsa

ServerAliveInterval 240

ServerAliveCountMax 2

d) Establecimiento del túnel para envío de logs

> ssh -f -N -L <C_Interface_Ipaddress>:55805: <FSM Server IP Address>:55805 FSM

Nota: no funcionará hasta no estar completada la configuración de los puntos siguientes.

14. Con objeto de establecer esta conexión de forma automática en el arranque del *appliance*, y reestablecerlo en caso de fallo del mismo, se crea un servicio en el propio *appliance*.
15. Para realizar esta tarea es necesario acceder al *appliance* con permisos de administrador, para lo que se requiere la participación de Servicios Profesionales o Soporte Técnico de Forcepoint, al tratarse de un acceso restringido.
16. Los pasos que seguirá Soporte Técnico para la configuración de este servicio serán los siguientes:
    a) Creación de un nuevo servicio (denominado por ejemplo *secure-tunnel.service*).
    b) Habilitar el servicio para que se asocie al arranque del *appliance*:
        i. Crear el fichero: */etc/systemd/system/secure-tunnel.service*
        ii. Incluir la siguiente configuración en el servicio:

```
[Unit]
Description=Setup a secure tunnel with FSM
After=network.target
[Service]
ExecStart=/usr/bin/ssh FSM -N -L
<C_Interface_Ipaddress>:55805:   <FSM Server IP
Address>:55805
# Restart every >2 seconds to avoid StartLimitInterval
failure
RestartSec=5
Restart=always
[Install]
WantedBy=multi-user.target
```

    Este fichero indica la creación de un servicio en el sistema del *appliance* que se ejecuta una vez que el *appliance* tiene operativa la conexión de red, y ejecuta el comando *ssh* haciendo uso del fichero de configuración indicado anteriormente, que incluye los parámetros de conexión necesarios para la autenticación, y se indica la creación de un túnel SSH a través de la dirección IP del interfaz C del *appliance* con el servidor FSM. De este modo, cuando el servicio "*Log Server*" comunique con la IP del interfaz C del *appliance* a través del puerto indicado, realmente lo hará con el servidor FSM al que enviará los logs de forma segura.
    c) Incluir el servicio en el arranque del equipo automáticamente y arrancar una vez creado:

Systemctl daemon-reload
Systemsctl enable secure-tunnel
Systemcto start secure-tunnel

2.4 CONFIGURACIÓN DE SERVIDOR SSH PARA AUTENTICACIÓN CON CERTIFICADO

17. En el servidor FSM es necesario modificar la configuración una vez creado el par de claves de usuario para que se permita únicamente el establecimiento de la conexión SSH basada en la utilización de claves definidas como confiables y deshabilitar así el acceso mediante usuario y contraseña. Para ello, se realizarán en el FSM los siguientes pasos:

    a) En el servidor FSM (OpenSSH Server) se crea el documento *authorized_keys* en el directorio *C:\Users\<nombre_de_usuario>\.ssh* (bajo el directorio del usuario que se vaya a utilizar para el acceso, ssh en el caso ejemplo)

    Nota: el directorio .ssh no está creado por defecto. Para crearlo es necesario hacerlo por línea de comandos ya que el explorador gráfico de los sistemas Windows no permite crear un directorio cuyo nombre comience por ".".

    Nota: verificar que el fichero *authorized_keys* no tiene extensión.

    b) Se copia en ese archivo el valor de la clave pública creada en el punto anterior ubicada en *~/.ssh/id_ecdsa.pub*

    c) Se modifican los permisos de dicho fichero para que únicamente los usuarios/grupos con permisos sobre el fichero sean *SYSTEM* y el propio usuario *ssh*. Es necesario quitar los permisos al grupo de administradores:

    - Acceder a las propiedades del fichero, y vaya a la pestaña de seguridad
    - Pulsar en "*Advanced*" (For Special permission or advanced setting, click Advanced)
    - Una vez abierta esa opción, hacer click en "*Disable Inheritance*" y seleccione la opción "*Convert inherited permissions into explicit permissions on this object*")
    - Pulsar "*Apply*" y después "*OK*"
    - De nuevo en la ventana de *Properties -> Security Pulse* en "*Edit*" (*to change permissions*, *click Edit*)

- Sobre la nueva ventana, seleccionar el grupo de administradores y pulsar en "*Remove*". Pulsar "*Apply*" y "OK", y otra vez "*OK*" para cerrar la ventana de propiedades.
- Se modifican los permisos de dicho fichero para que únicamente los usuarios/grupos

d) Realizar modificaciones sobre el fichero de configuración sshd_config:

- Buscar las líneas:

  #PasswordAuthentication yes

- Y sustituir por (nótese que las reglas originales estaban comentadas, las modificadas no):

  PubkeyAuthentication yes
  PasswordAuthentication no

- Con este cambio, se impide el acceso al servicio SSH mediante nombre de usuario y contraseña y se fuerza a hacerlo mediante certificado de usuario. Al final de este fichero, se deben comentar las siguientes líneas:

  Match Group administrators
  authorizedKeysFile__PROGRAMDATA__/ssh/administrators_authorized_keys

- Quedando de la siguiente forma:

  #Match Group administrators
  #authorizedKeysFile__PROGRAMDATA__/ssh/administrators_authorized_keys

- Por último, es necesario reiniciar el servicio 'OpenSSH SSH Server'

2.5 CONFIGURACIÓN DE LOG SERVER

18. Cuando el sistema está configurado y listo para el envío de los *logs* a través del túnel SSH establecido entre el *appliance* y el FSM, se configura la realización de dicho envío a través de ese túnel.
19. Para ello, sobre el interfaz de gestión del FMS, ir al menú *Settings* > *General* > *Logging* e introducir en él la dirección del interfaz C del *appliance*, utilizando el puerto configurado para el establecimiento de la conexión segura entre *appliances* y servidor FSM (en la configuración mostrada a lo largo del documento se trata del puerto 55805).
20. Con estos pasos, la transferencia de *logs* entre los distintos *appliances* y el servidor FSM se realiza de forma cifrada y segura. Por tanto, todas las comunicaciones entre los distintos componentes de la solución quedan cifradas.

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