

Procedimiento de empleo seguro

Forcepoint On-Premise Security 8.5

Anexo I - Configuración de Administración Segura





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

Edita:



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.

ÍNDICE

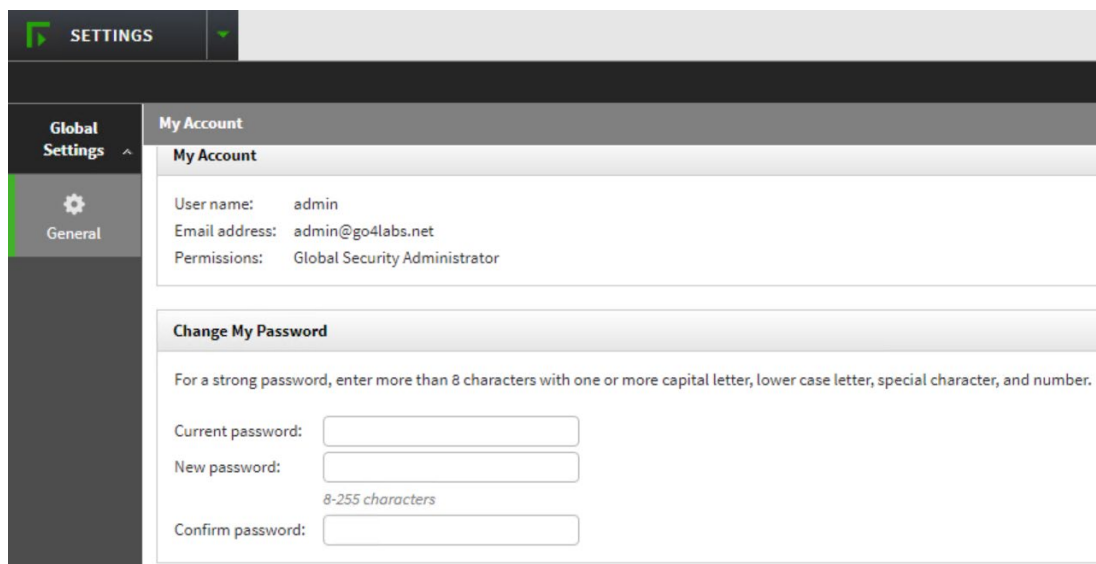
1. INTRODUCCIÓN	3
2. LONGITUD MÍNIMA DE CONTRASEÑA PARA ADMINISTRACIÓN	4
3. AUTENTICACIÓN DE DOBLE FACTOR PARA ADMINISTRACIÓN.....	5
3.1 AUTENTICACIÓN DE DOBLE FACTOR UTILIZANDO RSA SECURID	5
3.2 AUTENTICACIÓN DE DOBLE FACTOR UTILIZANDO CERTIFICADO CLIENTE	8
4. ACCESO RESTRINGIDO A LOS <i>APPLIANCES</i> A TRAVÉS DE FSM.....	11
4.1 HABILITAR EL ACCESO A LA GESTIÓN DE <i>APPLIANCES</i> DESDE FSM	13
4.2 DESHABILITAR CONEXIONES SSH EN <i>WEB SECURITY APPLIANCE</i>	14
4.3 LIMITACIÓN DE CONEXIÓN AL INTERFAZ DE <i>WEB CONTENT GATEWAY</i>	15

1. INTRODUCCIÓN

1. Aunque la administración de la plataforma Forcepoint Security On-Prem v8.5.x se realiza siempre a través de canales cifrados como HTTPS o SSH, con objeto de reforzar esta administración y proteger a la solución de posibles ataques que buscan el acceso a la gestión de la plataforma se proponen las siguientes mejoras en la configuración:
 - El acceso de administración a la plataforma de gestión FSM se configura para requerir una longitud mínima de contraseña y, además, un doble factor de autenticación, que podrá ser un dispositivo RSA o un certificado de usuario.
 - El acceso a la administración se centraliza en un único punto, que será el servidor FSM. La gestión de los *appliances* solo podrá llevarse a cabo a través del FSM, ya que el acceso directo a los mismos debe ser deshabilitado. A tal fin, la administración vía web (HTTPS) estará restringida para su acceso desde el FSM y el acceso a la administración de los *appliances* vía SSH será deshabilitado.

2. LONGITUD MÍNIMA DE CONTRASEÑA PARA ADMINISTRACIÓN

2. Para el acceso de administración a la plataforma FSM, todas las contraseñas de gestión serán de al **menos 12 caracteres**, incluyendo números, letras, caracteres especiales, etc. Además, **es muy recomendable el doble factor de autenticación**, como se indica más adelante.



The screenshot displays the 'SETTINGS' interface of the Forcepoint FSM. On the left, a sidebar contains 'Global Settings' and 'General'. The main content area is titled 'My Account' and includes a 'My Account' section with the following details:

User name:	admin
Email address:	admin@go4labs.net
Permissions:	Global Security Administrator

Below this is the 'Change My Password' section, which includes the instruction: 'For a strong password, enter more than 8 characters with one or more capital letter, lower case letter, special character, and number.' It features three input fields: 'Current password:', 'New password:' (with a note '8-255 characters' below it), and 'Confirm password:'.

Figura 1 - Definición de nueva contraseña en FSM

3. AUTENTICACIÓN DE DOBLE FACTOR PARA ADMINISTRACIÓN

3. La autenticación de doble factor para los usuarios de administración FSM es un requerimiento de seguridad necesario. Esta autenticación de doble factor puede realizarse utilizando RSA SecurID o autenticación vía certificado de usuario.

3.1 AUTENTICACIÓN DE DOBLE FACTOR UTILIZANDO RSA SECURID

4. Cuando se habilita la autenticación RSA SecurID en el menú de configuración de doble factor de autenticación, el proceso de inicio de sesión para un administrador que accede a la URL del administrador de seguridad es el siguiente:
- a) FSM detecta que la autenticación RSA SecurID está habilitada y disponible, y muestra la versión RSA de la pantalla de inicio de sesión. (El enlace "Olvidé mi contraseña" en esta pantalla no se aplica a las contraseñas de SecurID).

The image shows the login interface of Forcepoint Security Manager, version 8.4. At the top, the logo 'FORCEPOINT Security Manager' is displayed in green and black. Below it, the version 'Version 8.4' is shown. A light blue box contains the instruction 'To log on, enter your RSA SecurID credentials.' with a link for 'More information'. Below this are two input fields: 'User name' with a person icon and 'Passcode' with a lock icon. At the bottom, there is a link 'Forgot my password' and a green 'Log On' button.

Figura 2 - Inicio de sesión con *RSA authentication* activado

- b) Los administradores proporcionan sus credenciales de autenticación de dos factores según lo definido por su organización. Por ejemplo:
- El nombre de usuario de SecurID puede ser la dirección de correo electrónico del administrador o el nombre de inicio de sesión en la red.
 - El código de acceso suele ser un PIN combinado con un código de token proporcionado por un *token hardware* o *software* independiente; el formato depende de la configuración de cada organización.

- c) El mecanismo de autenticación busca en el repositorio local un perfil de usuario que coincida con el nombre de usuario proporcionado. Si no hay coincidencia, la búsqueda se repite en el servicio de directorio. Si se encuentra un usuario de la red, FSM busca grupos a los que se les hayan asignado permisos en el sistema y el inicio de sesión RSA continúa si se encuentra una intersección entre los grupos.
 - d) El agente personalizado (véase más adelante la información relativa al agente personalizado de autenticación RSA) de FSM verifica el nombre de usuario de SecurID y el código de acceso con *RSA Authentication Manager* (componente de autenticación de arquitectura RSA integrada). Si la autenticación falla, el administrador no puede iniciar sesión.
5. El agente personalizado admite la creación de un nuevo PIN, si es necesario, como parte del proceso de autenticación. Esto puede ser gestionado por el administrador de la solución *RSA Authentication Manager*, que configura la autenticación basada en integración con RSA o generado por el sistema. Si es aplicable, los criterios de seguridad para el PIN se muestran en la pantalla.
6. Para habilitar y usar la autenticación de doble factor basada en la solución RSA SecurID, en primer lugar, debe crearse un agente personalizado para FSM mediante *RSA Authentication Manager*. Este agente se utiliza para comunicarse con el servidor de *RSA Authentication Manager* cuando prueba la conexión en la página *General > Two-factor Auth* y durante el proceso de inicio de sesión.
7. A continuación, se enumeran los pasos necesarios para crear un agente personalizado:
- a) **En *RSA Authentication Manager***, agregar un *host* de agente con la siguiente configuración mínima:



Figura 3 - Añadir nuevo agente de *host* en *RSA Authentication Manager*

- a. Nombre: nombre de host del servidor de administración FSM. Debe resolverse en una dirección IP válida en la red local.
- b. Dirección de red: dirección IP del servidor de administración de FSM.
- c. Tipo de agente: seleccionar agente estándar.

- d. Tipo de cifrado: seleccionar el algoritmo de cifrado.

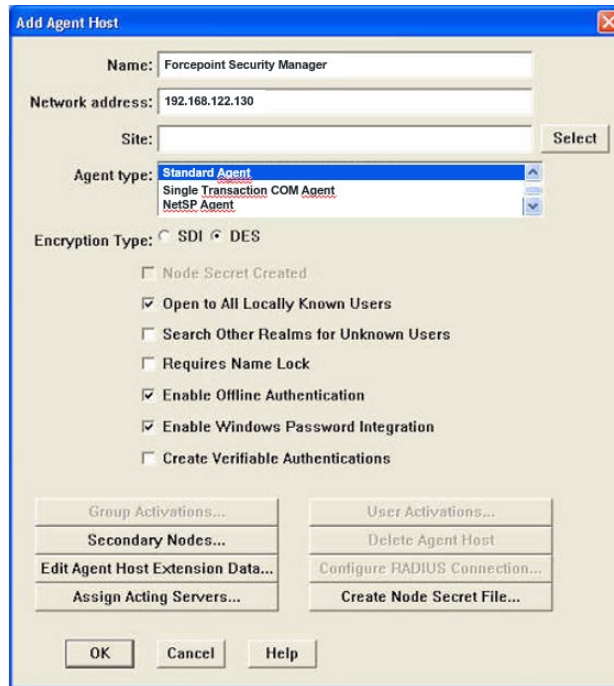


Figura 4 - Configuración nuevo agente de host

Nota: Para garantizar una configuración segura, *RSA Authentication Manager* debe permitir el uso del algoritmo de cifrado AES, con una fortaleza suficiente, según la guía CCN-STIC-807. En caso de que el uso de este algoritmo no pueda ser garantizado, se aconseja hacer uso únicamente de autenticación basada en certificado cliente.

- b) Hacer clic en *Generar archivos de configuración*.
- c) Copiar el archivo de configuración de *RSA Authentication Manager* (*sdconf.rec*) en el siguiente directorio en el servidor de administración de Forcepoint:

*C:\Archivos de programa (x86)\ Websense \ EIP \ tomcat \ wbsnData \ rsaSecurID *

Nota: De forma predeterminada, el archivo *sdconf.rec* se encuentra en la carpeta *\ACE \Data* en el servidor *RSA Authentication Manager*.

- d) Si existe un archivo secreto de nodo ("node secret file", *securid*), copiar este archivo también en el directorio anterior. Para los agentes que se basan en el protocolo TCP/IP como es el caso, el uso de archivo secreto de nodo es opcional y la ubicación del mismo se especifica en el fichero *rsa_api.properties* de *RSA Authentication Manager*. Se recomienda contactar con el administrador de *RSA Authentication Manager* para confirmar si se usa este archivo y conocer su ubicación.
- e) Asegurarse de que ningún administrador haya iniciado sesión en FSM.

- f) En el servidor de administración de Forcepoint, abrir la herramienta *Servicios de Windows*.
- g) Hacer clic con el botón derecho en el servicio *Websense TRITON Unified Security Center* y seleccione *Reiniciar*.
- h) A continuación, se enumeran los pasos necesarios para configurar la autenticación mediante RSA SecurID sobre la consola FSM:
 - Seleccionar la opción de autenticar a los administradores mediante la autenticación RSA SecurID.
 - Introducir un nombre de usuario y un código de acceso válidos para el inicio de sesión de *RSA SecurID*. El usuario debe poder autenticarse con *RSA Authentication Manager*, pero no tiene que ser un administrador de FSM.
 - Hacer clic en *Probar conexión a RSA Authentication Manager*.

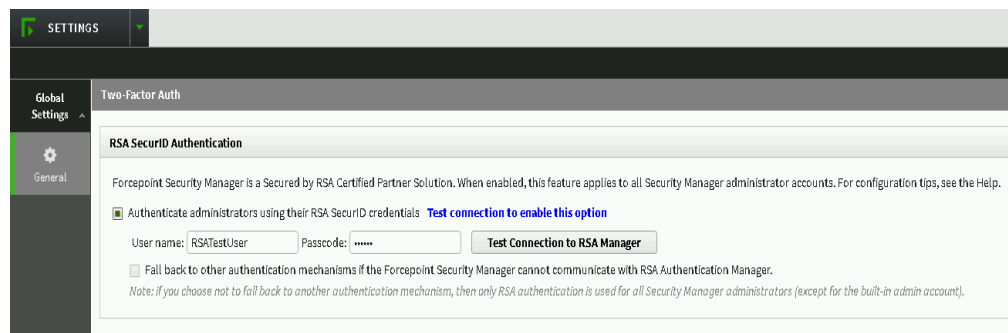


Figura 5 - Activación autenticación RSA en FSM

- La prueba de conexión debe ser exitosa antes de que FSM permita que los cambios se guarden en esta página. Los resultados de la prueba se muestran junto al botón *Probar conexión (Test Connection)*.

3.2 AUTENTICACIÓN DE DOBLE FACTOR UTILIZANDO CERTIFICADO CLIENTE

8. Cuando se habilita la autenticación mediante certificado en la página *Autenticación de dos factores*, el proceso de inicio de sesión para un administrador que accede a la URL de FSM es el siguiente:
 - a) FSM detecta si hay un certificado de cliente instalado. Si hay más de un certificado disponible, se le pide al administrador que seleccione el certificado que permite el acceso.
 - b) El administrador proporciona sus credenciales de autenticación de dos factores según lo definido por su organización. Por ejemplo, esto podría ser mediante el uso de la tarjeta de acceso común (CAC) y un lector de tarjetas.
 - c) Después de una autenticación exitosa, FSM recibe el certificado del cliente

y verifica que coincide con la firma en los certificados de CA raíz cargados. Si la firma coincide, FSM busca una coincidencia completa con los certificados que se cargaron en FSM o se importaron del directorio de usuarios. Si se encuentra una coincidencia, el administrador asociado con las credenciales de autenticación de dos factores inicia sesión.

- d) Si no se encuentra ninguna coincidencia de certificado y la coincidencia de atributos está configurada como una opción alternativa, se realiza una verificación para ver si el certificado de cliente contiene una propiedad que coincida con un atributo LDAP específico en su directorio de usuarios. Si se encuentra una coincidencia, el administrador asociado con las credenciales de autenticación de dos factores inicia sesión en FSM.
9. La autenticación por contraseña debe estar deshabilitada, por lo que los administradores sin certificados coincidentes no pueden iniciar sesión.
 10. A continuación, se enumeran los pasos necesarios para configurar la autenticación mediante certificado cliente de FSM:
 - a) En el menú *Settings>Global Settings>General>Two Factor Authentication* de FSM, seleccionar *Autenticar administradores mediante autenticación de certificado de cliente*.

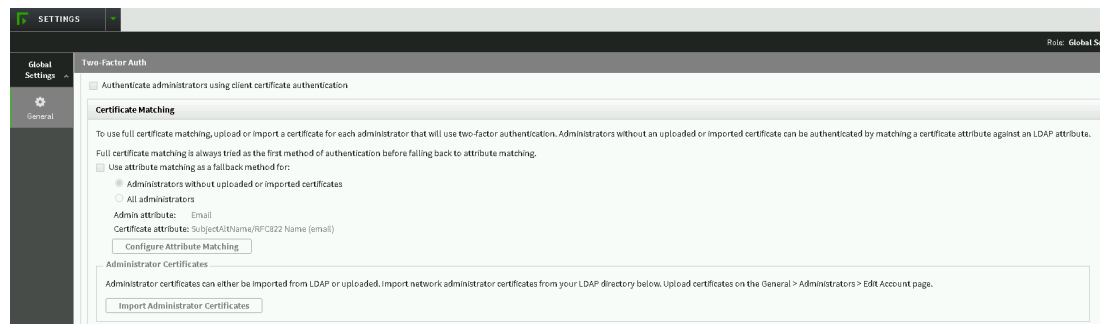


Figura 6 - Configuración de autenticación basada en Certificado Cliente

- b) Para habilitar la coincidencia de atributos, en la marca de coincidencia de certificados, se debe utilizar la coincidencia de atributos como método alternativo y seleccionar si se aplica a todos los administradores o solo a los administradores sin certificados. Para configurar los atributos utilizados para la coincidencia, hacer clic en *Configurar coincidencia de atributos* y, a continuación, consultar *Configuración de la coincidencia de atributos*.
- a) Los certificados de administrador pueden importarse desde LDAP o cargarse. Para importar certificados de administrador de red desde el directorio LDAP, hacer clic en *Importar certificados de administrador* (*Import Administrator Certificates*, ver Figura 6).
 - b) Cuando los certificados se importan correctamente, se muestra un mensaje de éxito en la parte superior de la página. Si alguno de los certificados no se

importa correctamente o no está presente en el servidor LDAP, se puede cargar un certificado para cada administrador de red en la página *General > Administrators > Edit Network Account page*.

- c) Haga clic en *Agregar en Certificados raíz* para agregar un certificado raíz para la verificación de la firma. Debe haber al menos un certificado raíz en FSM para que funcione la autenticación de dos factores.
- d) Buscar la ubicación del archivo del certificado raíz y haga clic en *Cargar certificado*.
- e) Siempre que se agregue o cambie un certificado raíz, crear un nuevo archivo de certificado maestro y copiar en el servicio "*Websense TRITON Web Server*". Hacer clic en "*Crear archivo de certificado maestro*" para crear el nuevo archivo, luego consultar "*Implementar el archivo de certificado maestro*" para obtener más información. Este certificado es utilizado por el servicio "*Websense Triton Web Server*" para permitir la autenticación basada en certificado cliente e incluir los nuevos certificados raíz en la negociación de autenticación basada en certificado cliente.
- f) Deshabilitar la autenticación de contraseña como método alternativo. Para ello, se debe desmarcar "*Permitir la autenticación de contraseña para iniciar sesión en el Administrador de seguridad para:*"
- g) Haga clic en "*Aceptar*" para guardar la configuración.

4. ACCESO RESTRINGIDO A LOS *APPLIANCES* A TRAVÉS DE FSM

11. El acceso a la administración de los *appliances Content Gateway* se permitirá únicamente a través de FSM. De este modo la configuración aplicada anteriormente para requisitos de tamaño mínimo de clave y autenticación de doble factor se aplica también a los métodos de acceso a los *appliances* que forman parte de la solución, y se deshabilita la posibilidad de acceso directo a la gestión de los *appliances Content Gateway*. Esto da lugar a:
 - Acceso a la interfaz de gestión de los *appliances Content Gateway* únicamente a través de FSM.
 - Acceso deshabilitado mediante SSH a los *appliances Content Gateway*.
 - Aunque realmente el intento de acceso al portal estaría inhabilitado si no es a través de FSM, el acceso directo a la gestión HTTPS de *Content Gateway* también debe estar deshabilitado.
12. Con los siguientes pasos se restringe el inicio de sesión único (*Single Sign-On*) para que los administradores tengan acceso al portal de gestión de los *appliances Web Content Gateway* únicamente a través de FSM. Para ello, se deshabilita la capacidad de inicio de sesión con contraseña en los *appliances Web Content Gateway*:
 - 1) Asegurarse de que los miembros del grupo de superadministradores en FSM tienen permisos de acceso directo a *Content Gateway* (inicio de sesión único o *Single Sign-on*, ver más adelante).
 - 2) Iniciar sesión en el *Content Gateway*:
 - i. Acceder por consola SSH al *appliance* y habilitar el acceso al mismo mediante el uso del usuario *tech-support* (usuario utilizado por *Forcepoint Technical Support* para realizar este cambio de configuración en los *appliances*).
 - ii. Acceder con las credenciales *Admin* (usuario por defecto existente en el *appliance* cuya contraseña se configura durante la configuración inicial del *appliance*).
 - iii. Una vez se acceda al interfaz de consola del *appliance*, escribir *config*.
 - iv. Introducir la contraseña del usuario *Admin* de nuevo.
 - 3) Una vez establecida la conexión en modo *config* siguiendo los pasos anteriores, se procede ahora a habilitar el acceso de asistencia remota y diagnóstico:
 - i. Escribir *set diagnostic_ports --status enabled*

ii. Escribir set account tech-support --status enabled

- 4) Esto devolverá un *passcode* que podrá ser descifrado por soporte técnico para acceder con el usuario *"tech-support"*. A partir de este paso se requerirá la asistencia de *Soporte Técnico de Forcepoint* en caso de tratarse de un *appliance* físico o virtual. Los pasos que realizará soporte técnico de Forcepoint son los siguientes:
 - a. Mediante el acceso proporcionado, y de forma coordinada con el administrador (mediante sesión remota, por ejemplo), soporte técnico accederá al *appliance* vía consola y obtendrá acceso de *root* ("su -", e introducirá una contraseña dinámicamente generada para este acceso).
 - b. Una vez adquirido el acceso privilegiado, Soporte Técnico de Forcepoint accederá al entorno de *Content Gateway* dentro del *appliance* mediante el comando *"ssh wcg"*.
 - c. Soporte Técnico de Forcepoint accederá al directorio *"/etc"* y comprobará la existencia de un subdirectorio *"/websense"*. Si no es así, se procederá a su creación mediante el comando *"mkdir websense"*.
 - d. Soporte Técnico de Forcepoint accederá al directorio *"/websense"* (la ruta ahora es *"/ etc / websense"*) y verificará si existe el archivo *"password-logon.conf"*. En caso contrario se procederá a su creación mediante el comando *"touch password-logon.conf"*.
 - e. Soporte Técnico de Forcepoint editará el fichero *"password-logon.conf"*.
 - f. Soporte Técnico de Forcepoint agregará o modificará la línea existente con el siguiente contenido:
 - i. password-logon = disabled*
 - g. Soporte Técnico de Forcepoint guardará el archivo y procederá a cerrarlo.
13. El cambio hace efecto inmediatamente. No es necesario reiniciar el *Content Gateway*. Con la configuración realizada, el acceso directo a través de la dirección IP de la interfaz de gestión del *appliance* queda deshabilitado.
14. Para volver a habilitar el inicio de sesión con contraseña para todos los administradores, se deberán realizar los siguientes pasos:
 - 1) Los primeros pasos para permitir el acceso con el usuario *"tech support"* son los mismos que los descritos anteriormente. A partir de ese momento se requerirá la asistencia de Soporte Técnico de Forcepoint en caso de tratarse de un *appliance* físico o virtual. Los pasos realizados por soporte técnico para volver a habilitar el inicio de sesión con contraseña serán:
 - a. Inicio de sesión en el sistema host de Content Gateway y adquisición de

privilegios de *root*.

- b. Acceso al directorio */etc/websense*.
- c. Edición del fichero *password-logon.conf* modificando la siguiente línea:
 - *password-logon = disabled*. Dicho parámetro deberá ser modificado a *“enabled”*.
- d. Guardado y cierre del archivo.

15. El cambio hace efecto inmediatamente. No es necesario reiniciar el *Content Gateway*. Una vez finalizada la configuración es posible deshabilitar el acceso de soporte técnico.

4.1 HABILITAR EL ACCESO A LA GESTIÓN DE APPLIANCES DESDE FSM

16. Con la configuración realizada, el acceso directo a través de la dirección IP de la interfaz C queda deshabilitado. Para poder acceder se debe habilitar el inicio de sesión único (*Single Sign-On*) del *appliance* para permitir el acceso con privilegios de administración de *Content Gateway* desde la consola de FSM.
17. Para usar autenticación de dos factores (mediante certificado) a través del FSM, se deberán realizar los siguientes pasos:
 - 1) Iniciar sesión en FSM. Para ello, introduzca en el navegador web la URL *https://<fsm_ipaddress>:9443*.
 - 2) Ir a la página *“Appliances > Manage Appliances”* en FSM.
 - 3) Registrar el dispositivo:

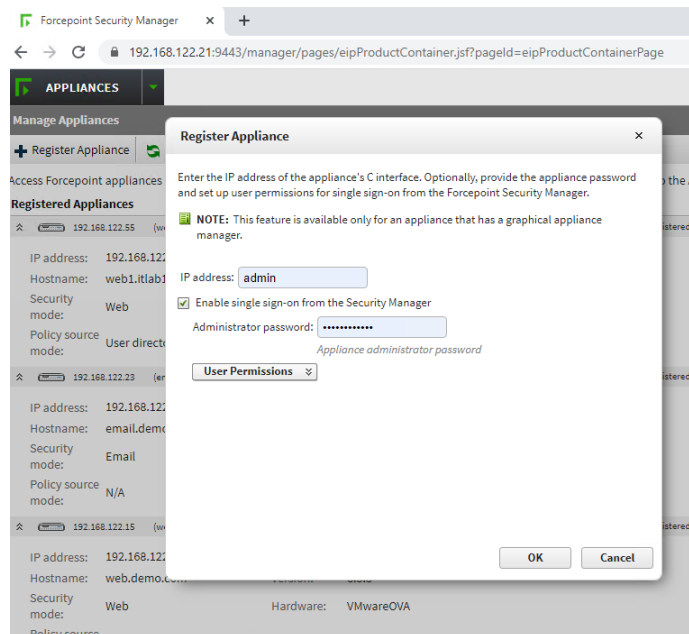


Figura 7 - Registro de *Appliances* en FSM

- 4) Salir e iniciar sesión nuevamente en la consola FSM.

- 5) Haciendo uso del botón “Switch Policy Server” ubicado en la parte superior, seleccionar el *appliance* a gestionar.

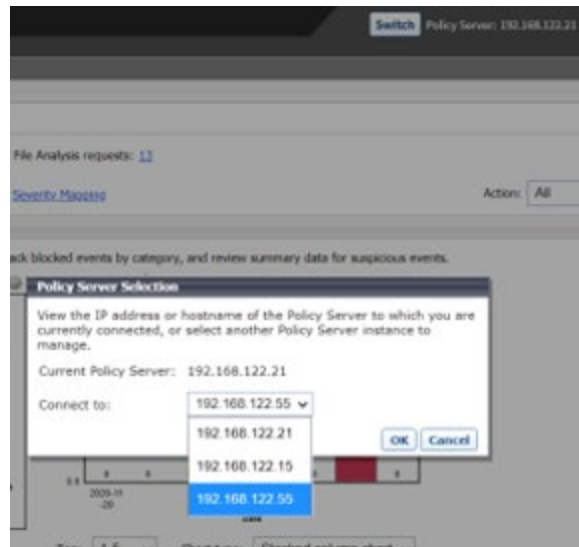


Figura 8 - Selección de Policy Server en FSM

- 6) Ir al menú *Settings > General > Content Gateway Access*

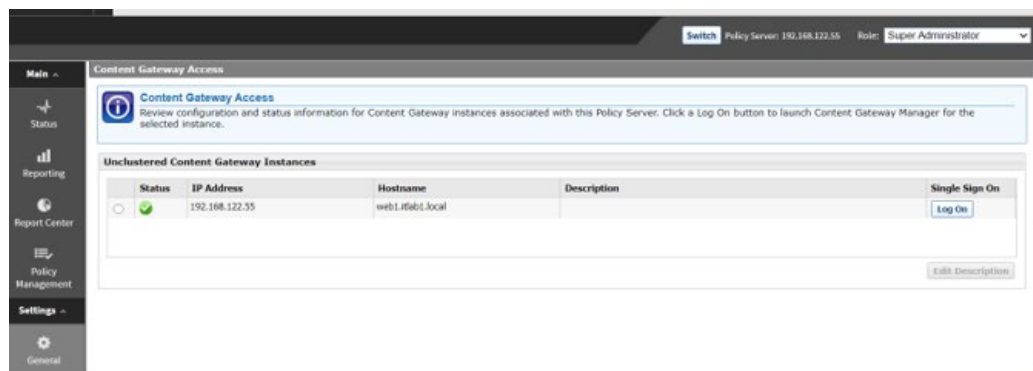


Figura 9 - Menú Content Gateway Access en FSM

4.2 DESHABILITAR CONEXIONES SSH EN WEB SECURITY APPLIANCE

18. Para restringir el acceso a la gestión de los *appliances*, una vez centralizado el acceso vía HTTPS a través de la plataforma FSM, se debe deshabilitar la administración de los *appliances* *Web Content Gateway* vía SSH, para evitar el acceso directo a los equipos. El acceso SSH está habilitado por defecto y puede ser deshabilitado a través del interfaz de línea de comandos mediante el siguiente procedimiento:

- 1) Conectarse al *appliance* mediante SSH utilizando la cuenta de administrador.
- 2) Ejecutar el comando “*config*” e introducir la contraseña de administrador para poder modificar la configuración.
- 3) Ejecutar el comando “*set access ssh –status disabled*” para deshabilitar el

acceso SSH.

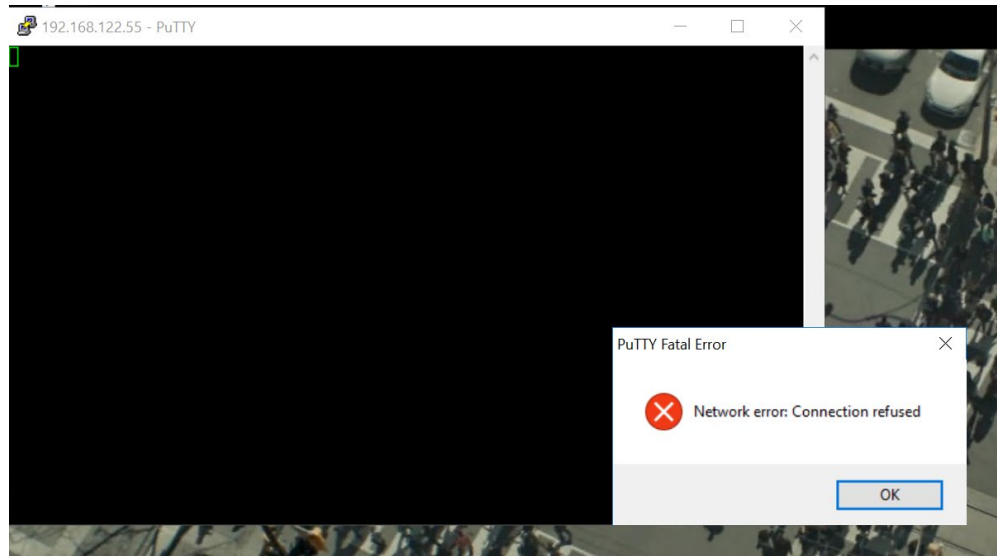


Figura 10 - Acceso SSH deshabilitado en los *appliances Content Gateway*

Nota: La configuración descrita en este documento requiere en varios pasos el acceso a gestión vía SSH a los *appliances*, por lo que se recomienda realizar este paso al final de la configuración de protección del *appliance*. En cualquier caso, si necesita acceso SSH, es posible habilitarlo desde la consola web. El acceso SSH de los *appliances Forcepoint Content Gateway* únicamente da acceso a entorno de línea de comandos (CLI), limitado sin acceso al sistema de archivos. El CLI permite realizar ciertas acciones de configuración en el *appliance*, de forma restringida, y asimismo permite dar acceso al perfil de soporte técnico de Forcepoint cuando es necesario realizar labores avanzadas de configuración.

4.3 LIMITACIÓN DE CONEXIÓN AL INTERFAZ DE WEB CONTENT GATEWAY

19. Por defecto, si un usuario accediera a la dirección IP del *appliance Web Content Gateway* sobre el puerto 8081, le aparecería el portal de acceso a la gestión del *appliance*, aunque con la configuración anterior aplicada le aparecería un mensaje de error indicando que el acceso basado en contraseña está deshabilitado. Con objeto de evitar que ni tan si quiera se permita la conexión con el interfaz de gestión de los *appliances Web Content Gateway*, es posible limitar el establecimiento de la conexión únicamente cuando la petición venga de la dirección IP del servidor FSM. De esta forma, un intento de conexión desde cualquier otra IP daría como resultado un error de conexión.
20. Para ello, se modifica el archivo de configuración interno del *appliance* (no accesible de forma directa) "*mgmt_allow.config*" a través del menú *Configure> My Proxy > UI Setup > Access*, y en él se debe permitir el acceso únicamente desde la IP del FSM y se bloquea el acceso desde cualquier otra IP.

