Guía de Seguridad de las TIC
CCN-STIC 651B

Procedimiento de Empleo Seguro
Cortafuegos Cisco Secure Firewall



Noviembre 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.11.04 14:07:01 +01:00

Fecha de Edición: Noviembre de 2026

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.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

1 INTRODUCCIÓN 4
2 OBJETO Y ALCANCE 5
3 ORGANIZACIÓN DEL DOCUMENTO 6
4 FASE PREVIA A LA INSTALACIÓN 7
4.1 ENTREGA SEGURA DEL PRODUCTO 7
4.2 ENTORNO DE INSTALACIÓN SEGURO 7
4.3 REGISTRO Y LICENCIAS 7
4.4 CONSIDERACIONES PREVIAS 8
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 8
5 FASE DE INSTALACIÓN 9
6 FASE DE CONFIGURACIÓN 10
6.1 MODO DE OPERACIÓN SEGURO 10
6.2 AUTENTICACIÓN 12
6.2.1 AUTENTICACIÓN FXOS 12
6.2.2 AUTENTICACIÓN FMC 13
6.3 ADMINISTRACIÓN DEL PRODUCTO 16
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 16
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES 19
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 20
6.4.1 ZONAS DE SEGURIDAD 21
6.4.2 ASIGNACIÓN DE DIRECCIONAMIENTO IP 21
6.4.3 ANTI-SPOOFING 23
6.4.4 ARP ESTÁTICO 23
6.4.5 CONSIDERACIONES FÍSICAS Y LÓGICAS 24
6.5 GESTIÓN DE CERTIFICADOS 24
6.6 SINCRONIZACIÓN 24
6.7 ACTUALIZACIONES 27
6.8 AUTO-CHEQUEOS 27
6.9 ALTA DISPONIBILIDAD 27
6.10 AUDITORÍA 27
6.10.1 REGISTRO DE EVENTOS 27
6.10.2 ALMACENAMIENTO LOCAL 28
6.10.3 ALMACENAMIENTO REMOTO 29
6.11 BACKUP 29
7 REFERENCIAS 31
8 ABREVIATURAS 33

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Enable CC compliance (system) 10
Ilustración 2. Enable CC compliance (Devices) 11
Ilustración 3: Configurar modo CC en FXOS para FPR4100/9300 12
Ilustración 4. Configuración de login en RADIUS 13
Ilustración 5. Uso de RADIUS tanto en Default como en Console Authentication 13
Ilustración 6. Configuración de RADIUS con FMC 14
Ilustración 7. Estableciendo el Timeout y número de reintentos 15
Ilustración 8. Habilitando Enabled para RADIUS 15
Ilustración 9. Desplegable "Shell Authentication" 16
Ilustración 10. Configuración del certificado HTTPS 16
Ilustración 11. Generando la solicitud de certificado 17
Ilustración 12. Solicitud de certificado 17
Ilustración 13. Importando certificado 18
Ilustración 14. Verificando el certificado en el navegador 18
Ilustración 15. Asignando zona de seguridad 22
Ilustración 16. Dando dirección IP 22
Ilustración 17. Asignación de IPs a zona de seguridad 22
Ilustración 18. Habilitando Anti Spoofing 23
Ilustración 19. Habilitando ARP estático 23
Ilustración 20. Configurando la zona horaria 25
Ilustración 21. Configuración del servidor NTP 25
Ilustración 22. Configurando servidor NTP desde la interfaz web 26
Ilustración 23. Especificación de zona horaria 26
Ilustración 24. Filtrado de Logs 28
Ilustración 25. Activando los logs de auditoría 29

1 INTRODUCCIÓN

Cisco Secure Firewall es una plataforma de seguridad unificada que integra firewall de próxima generación, prevención de intrusiones (IPS), protección avanzada contra malware (AMP) y filtrado de URL. Ofrece una defensa integral contra ciberamenazas, empleando inteligencia de amenazas de Cisco Talos para detectar y bloquear ataques conocidos y emergentes. Proporciona visibilidad profunda y control granular del tráfico, con gestión centralizada y despliegue flexible en entornos físicos y de nube.

2 OBJETO Y ALCANCE

El objeto de la presente guía es poner en conocimiento del administrador de la unidad los mecanismos de seguridad necesarios para proteger los sistemas de información y comunicaciones en cuyas instalaciones se emplee la solución de Cisco Secure Firewall. Con este conocimiento, es posible establecer un marco de referencia que contemple las recomendaciones STIC en el despliegue y utilización de esta familia de cortafuegos.

Las recomendaciones explicadas en este documento aplican principalmente a entornos de red que operen en modo centralizado (mediante Firewall Management Center - FMC), aunque algunos conceptos y prácticas pueden hacerse extensibles a entornos que operen con dispositivos Firepower en modo autónomo (Firewall Device Manager - FDM).

- Los dispositivos a los que aplica este procedimiento son los siguientes: Cisco Firepower Serie 1000 (1010, 1120, 1140 y 1150), Cisco Firepower 2100 (2110, 2120, 2130 y 2140), Cisco Secure Firewall Serie 3100 (3105, 3110, 3120, 3130 y 3140), Cisco Firepower Serie 4100 (4112, 4115, 4125 y 4145), Cisco Secure Firewall Serie 4200 (4215, 4225 y 4245), Cisco Firepower 9300, ISA 3000 y Firewall Management Center (FMC) (FMC1600, FMC2600, FMC4600, FMC1700, FMC2700, FMC4700 y FMCv).
- El software se compone de la imagen FTD 7.4 (o FTDv) y de la versión 7.4 de FMC (o FMCv).

El producto Cisco Secure Firewall ha sido incluido en el catálogo CPSTIC, para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF18].

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar antes de proceder a la instalación del producto.

b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto para lograr una configuración segura.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

La recepción segura de un dispositivo físico Cisco Secure Firewall se basa en una combinación de inspección física y validación tecnológica.

Al recibir el equipo, se deben seguir los siguientes pasos:

a) Inspeccionar el embalaje externo: Buscar signos de manipulación, roturas o cintas adhesivas no originales.

b) Números de Serie: Verificar que el número de serie coincida en:

- La caja del embalaje.
- La tarjeta extraíble ("asset card") en el frontal del chasis.
- La etiqueta de cumplimiento en la parte inferior del chasis.
- La documentación de compra y garantía.

c) Herramienta de Verificación de Cisco: Utilizar la herramienta en línea "Serial Number Checker" [REF14] de Cisco (requiere credenciales de Cisco.com) para validar la autenticidad y la cobertura de la garantía del equipo.

La integridad del software virtualizado (FTDv) se asegura mediante la verificación criptográfica de los archivos de imagen. Las imágenes de software deben obtenerse exclusivamente desde el Cisco Software Download Center [REF15], utilizando credenciales válidas y una conexión segura (HTTPS/TLS). Junto a cada enlace de descarga, Cisco publica el valor del hash de integridad, típicamente SHA-512 o SHA-256.

4.2 ENTORNO DE INSTALACIÓN SEGURO

Dada la variedad de equipos que conforman la familia de cortafuegos Cisco Secure Firewall, algunos de estos modelos están diseñados para ser instalados en Centros de Proceso de Datos (CDP). Para estos entornos, es importante seguir las mejores prácticas de restricción de acceso a los mismos siguiendo las normas indicadas por el ENS.

4.3 REGISTRO Y LICENCIAS

El modelo de licenciamiento para Firewall Threat Defense (FTD) utiliza Cisco Smart Licensing, que permite comprar y gestionar un conjunto centralizado de licencias sin que estas estén atadas a un número de serie o clave específica. Este modelo facilita la evaluación del uso y de las necesidades de licencias en tiempo real. Además, Smart Licensing permite comenzar a usar una función inmediatamente, incluso antes de comprar la licencia, siempre que el dispositivo esté registrado en el Cisco Smart Software Manager, lo que evita retrasos por aprobaciones de compra.

Las licencias se administran a través de una cuenta inteligente (Smart Account) que puede contener múltiples cuentas virtuales para organizar licencias y dispositivos según regiones, departamentos o subsidiarias. Cada cuenta virtual tiene sus propias licencias y dispositivos asociados, y es posible transferir licencias o dispositivos entre estas cuentas. Para registrar un Firepower Management Center (FMC) o un dispositivo FTD, se utiliza un token de registro generado por la cuenta virtual.

Los tipos de licencias, el impacto en el sistema en caso de falta de las mismas y sus funcionalidades se pueden encontrar en la referencia [REF2].

4.4 CONSIDERACIONES PREVIAS

No existe ninguna consideración previa a la instalación de los equipos.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

De cara al despliegue de la solución, y en cumplimiento de los requisitos de seguridad, además de la solución propiamente dicha (cortafuegos y gestora FMC) se incluirán sistemas Security Information and Event Management (SIEM) para el registro de eventos del sistema y servidores de autenticación.

5 FASE DE INSTALACIÓN

Durante el despliegue inicial de un Cisco Secure Firewall se deben configurar las direcciones IP de gestión del equipo, credenciales del usuario de administración (admin), resolutores de DNS y, en el caso de los firewalls, su modo de despliegue. En la referencia [REF1] se incluyen las guías de despliegue inicial para los distintos modelos de los equipos.

Es importante recordar que la versión de software 7.4 y sus correspondientes parches se pueden encontrar en la página web de Cisco [REF15].

Toda la información sobre el despliegue inicial de los firewalls se puede encontrar en la guía de Getting Started para cada modelo. En la sección de referencias se encuentran los distintos enlaces por plataforma, ya sea hardware físico o virtual ver [REF1] para la guía de instalación de los distintos modelos.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

Los equipos Cisco Secure Firewall soportan dos modos de despliegue que garantizan distintos estándares de seguridad:

- Common Criteria (CC).
- Unified Capabilities Approved Products List (UCAPL). El Departamento de Defensa de EE.UU. ha cambiado el nombre de UCAPL por Department of Defense Information Network Approved Products List (DoDIN APL). Las referencias a UCAPL en esta guía o en el producto pueden interpretarse como referencias a DoDIN APL.

En el caso de la versión cualificada en ENS, los equipos deben desplegarse en modo CC.

Dependiendo de si estamos hablando de un FMC o un firewall gestionado, la configuración para activar el modo CC es ligeramente diferente:

a) FMC**: System** (⚙) > **Configuration > UCAPL/CC Compliance.** Seleccionar CC y salvar la configuración.

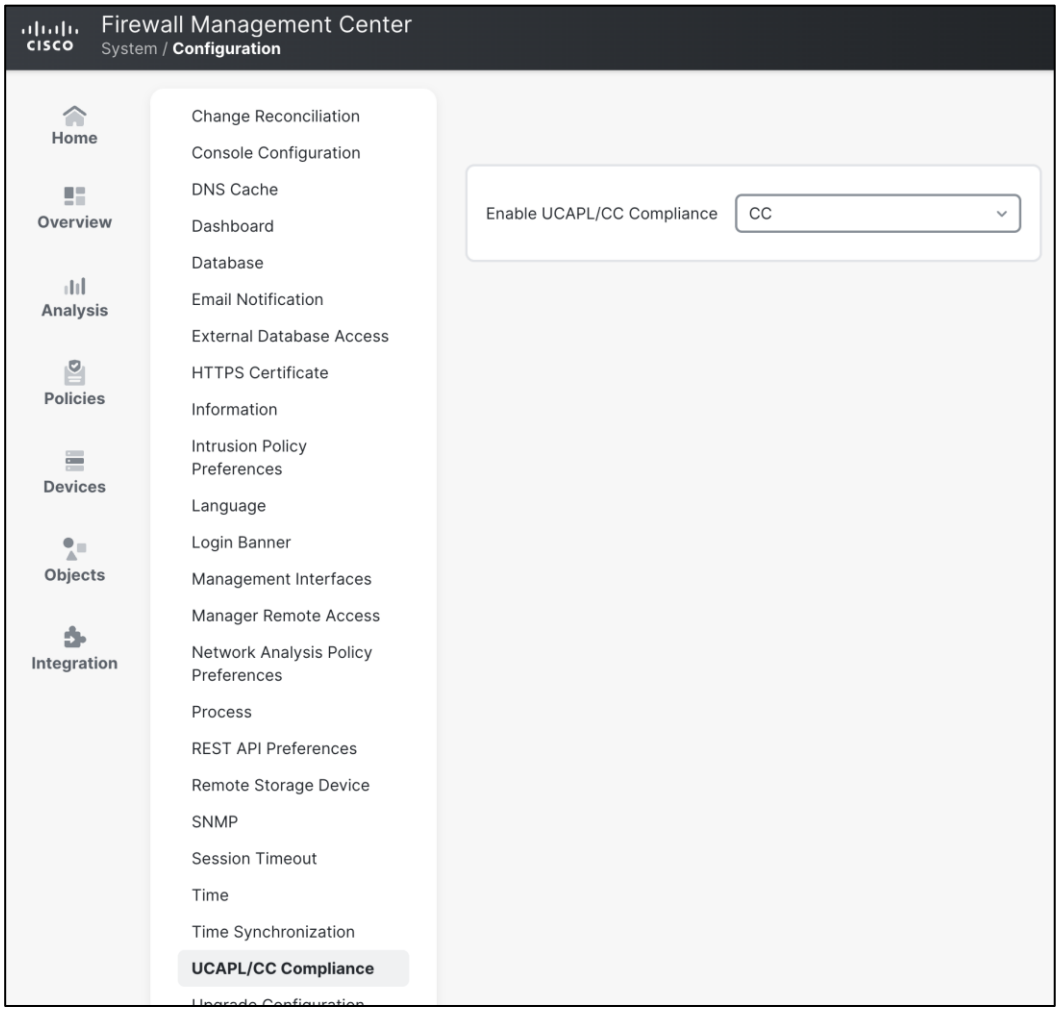


Ilustración 1. Enable CC compliance (system)

b) Cortafuegos: Devices > Platform Settings > UCAPL/CC Compliance. Seleccionar CC, guardar la configuración y realizar el despliegue de la misma.

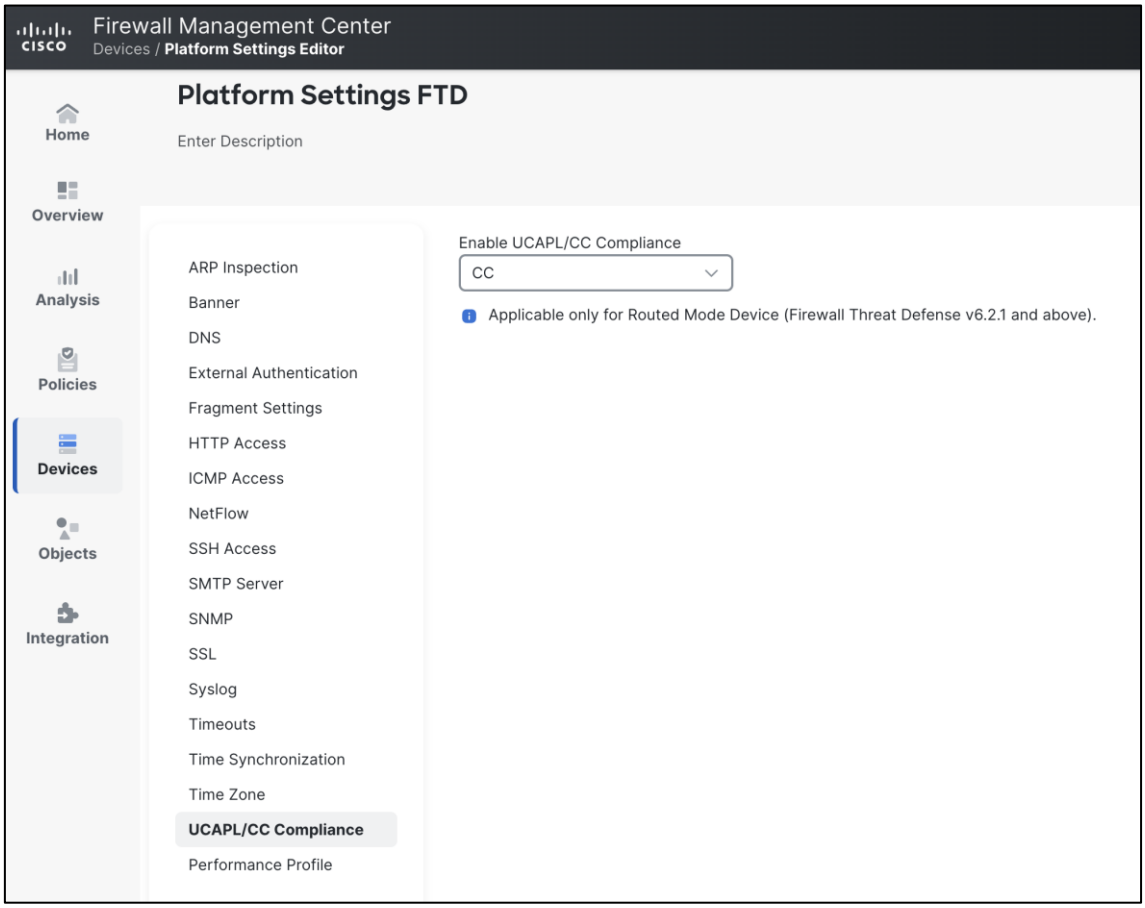


Ilustración 2. Enable CC compliance (Devices)

c) En el caso de los equipos FPR4100 y FPR9300, donde el software de gestión del chasis FXOS es independiente, también deberemos configurar el modo CC en él. Para ello, en FXOS seleccionar `Platform Settings > FIPS and Common Criteria`, marcar la casilla de CC y guardar la configuración.

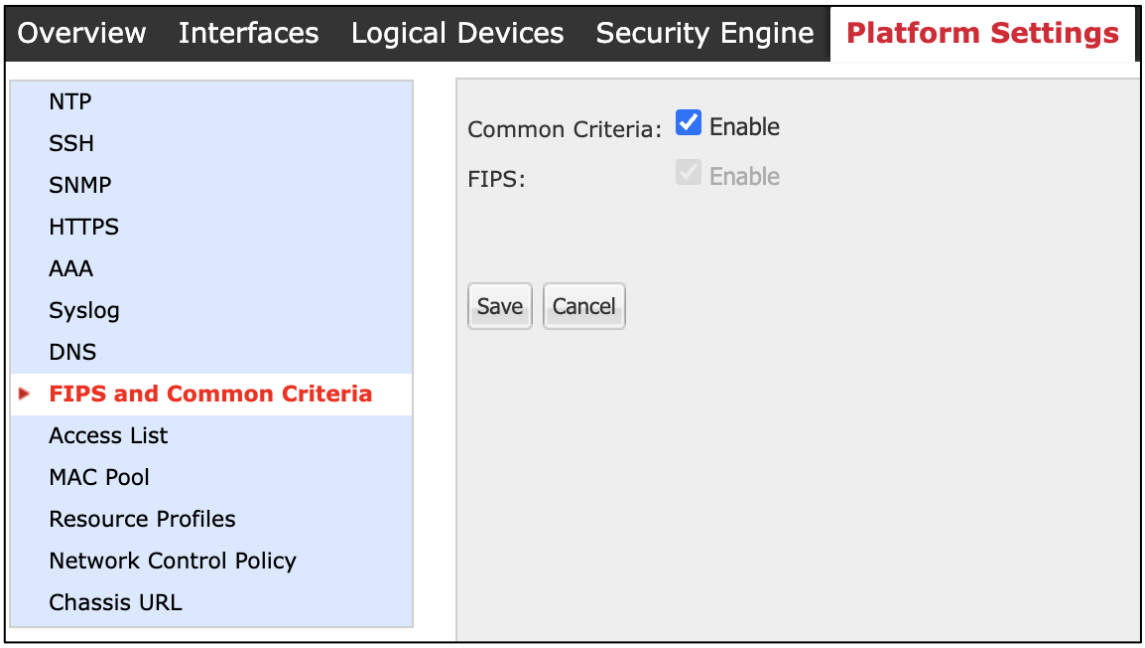


Ilustración 3: Configurar modo CC en FXOS para FPR4100/9300

6.2 AUTENTICACIÓN

Todos los equipos Cisco traen por defecto un usuario local admin cuyas credenciales están descritas en la guía de despliegue del producto [REF12]. Es importante cambiar la contraseña inicial en el primer acceso. Sin embargo, el equipo soporta la integración para la autenticación externa ya sea a través de LDAP, RADIUS, TACACS+ o SAML dependiendo del tipo de acceso.

6.2.1 AUTENTICACIÓN FXOS

El sistema FXOS permite autenticación mediante LDAP, RADIUS y TACACS. En esta guía se utilizará RADIUS por ser el sistema más ampliamente utilizado y por su capacidad de registro. Cualquier servidor RADIUS puede utilizarse; los más comunes son Cisco ISE, FreeRADIUS y Windows NPS.

Es posible integrar el RADIUS con un directorio activo que imponga una política de contraseñas (caducidad, bloqueo de reintentos, etc.). En ese caso, se recomienda crear un grupo separado (por ejemplo, “administradores”) y permitir el acceso únicamente a los usuarios del dominio que pertenezcan a ese grupo.

a) El primer paso es configurar el servidor o servidores RADIUS a utilizar. La configuración de timeout (seconds) y retries al configurar el servidor de RADIUS hace referencia al tiempo de espera y número de reintentos de conexión que hará el FMC antes de considerar que el servidor esté inoperativo. Se recomienda aumentar los reintentos a 3 y bajar el tiempo de timeout a 3 segundos. Se recomienda especificar el RADIUS por IP, ya que en caso de fallo de resolución DNS provocaría timeouts y problemas de entrada al dispositivo. La clave (key) es el secreto (contraseña) compartida con el servidor RADIUS.

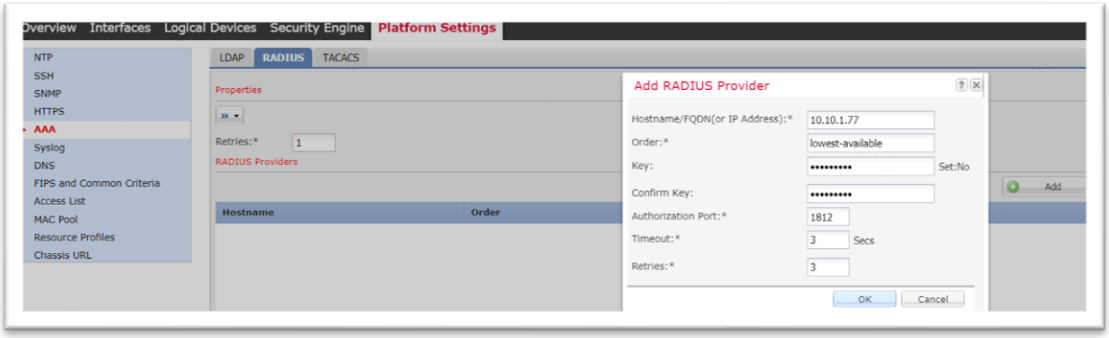


Ilustración 4. Configuración de login en RADIUS

b) El servidor RADIUS debe ser configurado para devolver al dispositivo un atributo que informe del rol o roles que deben asignarse al usuario autenticado con éxito. Esto se realiza con el atributo vendor Cisco-AV-Pair "shell:roles". Por ejemplo: shell:roles="admin". En el caso de que el servidor RADIUS no disponga por defecto de la configuración de atributos para Cisco, el valor de vendor ID para Cisco es 009 y el valor de vendor ID para el atributo es 001.

c) El siguiente paso es indicarle al sistema que debe usar el RADIUS para autenticar a los usuarios. Una vez asignado el RADIUS, los usuarios locales, como "admin", no estarán disponibles. Solo podrán usarse en caso de fallo del servidor RADIUS; es decir, como "fallback".

d) Por seguridad se debe usar RADIUS tanto en Default como en Console.

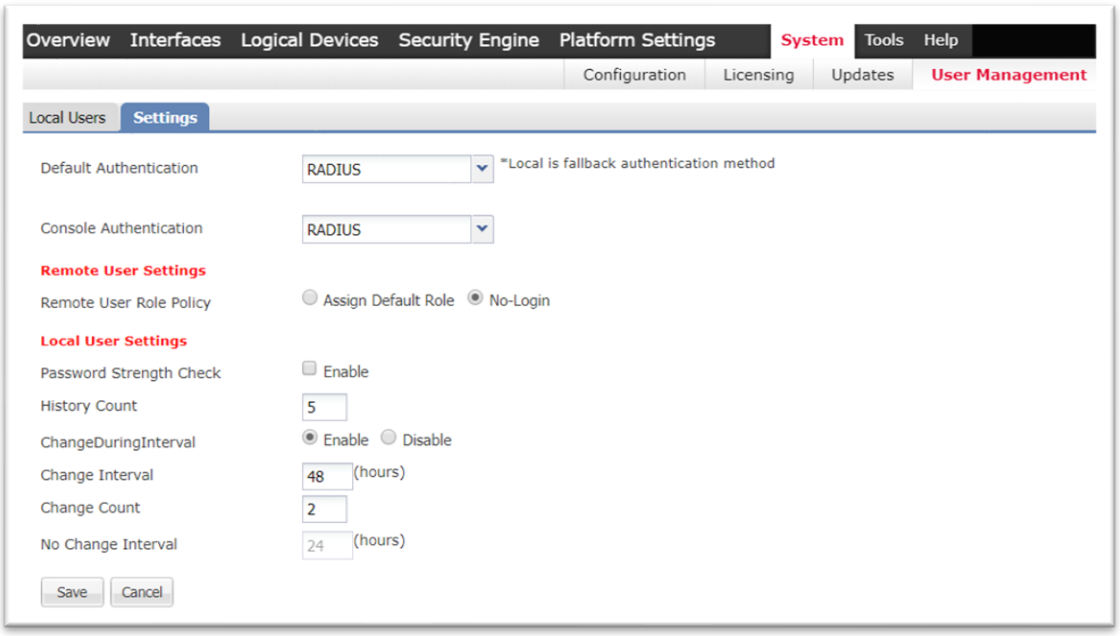


Ilustración 5. Uso de RADIUS tanto en Default como en Console Authentication

6.2.2 AUTENTICACIÓN FMC

Aunque es posible realizar una gestión de usuarios locales, se recomienda el uso de un sistema externo que provea de una política de gestión de contraseñas de acuerdo con las

especificaciones en la guía CCN-STIC-301 y otras que sean de aplicación. Ver referencia [REF16] con todas las guías del CCN.

El sistema FMC permite autenticación mediante LDAP y RADIUS. En esta guía utilizaremos RADIUS por ser el sistema más ampliamente utilizado y por su capacidad de registro. Para más información sobre como configurar la autenticación con LDAP ver la referencia [REF13].

Cualquier servidor RADIUS puede ser utilizado; entre los más comunes se encuentran Cisco ISE, FreeRADIUS y NPS.

Es posible integrar el RADIUS con un directorio activo que imponga una política de contraseñas (caducidad, bloqueo de reintentos, etc.). En ese caso, se recomienda crear un grupo separado (por ejemplo “administradores”) y permitir el acceso solo a los miembros del dominio que pertenezcan a ese grupo.

Se debe configurar el servidor o servidores Radius a utilizar. La configuración de timeout (seconds) y retries al configurar el servidor de RADIUS hace referencia al tiempo de espera y número de reintentos de conexión que hará el FMC antes de considerar que el servidor esté inoperativo. Se recomienda establecer los reintentos a 3 y el tiempo de timeout a 3 segundos. Se recomienda especificar el Radius por IP, ya que en caso de fallo de resolución DNS provocaría timeouts y problemas de entrada al dispositivo. La clave (key) es el secreto compartido con el Radius.

La configuración se realiza `en System->Users->External Authentication`.

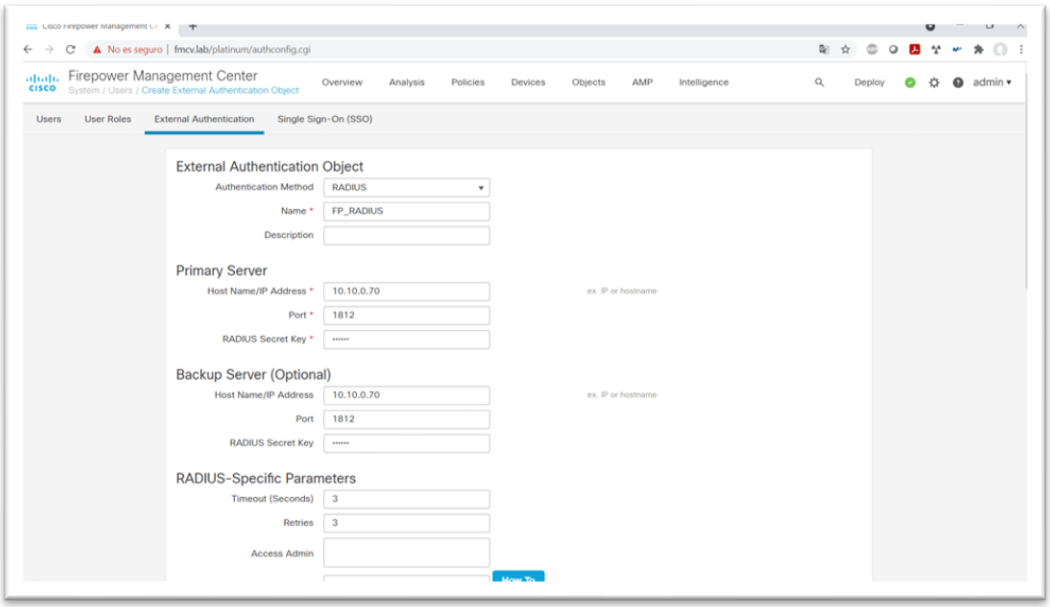


Ilustración 6. Configuración de RADIUS con FMC

Para la asignación de roles a los usuarios se recomienda realizarla a través de RADIUS. El gestor FMC permite la asignación usando cualquier atributo. Se recomienda usar el atributo RADIUS “Class” (25). En este ejemplo, se asigna el rol “Administrator” al atributo Class con valor “Administrator”.

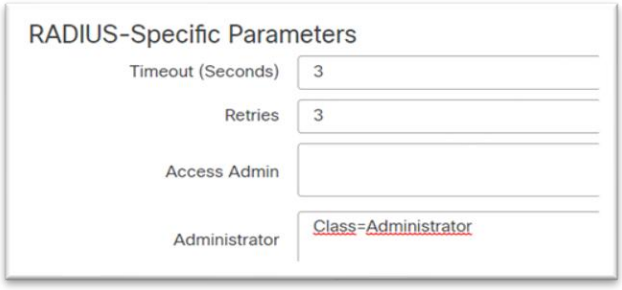


Ilustración 7. Estableciendo el Timeout y número de reintentos

El siguiente paso es indicarle al sistema que debe usar RADIUS para autenticar a los usuarios. Para ello, habilite “Enabled”.

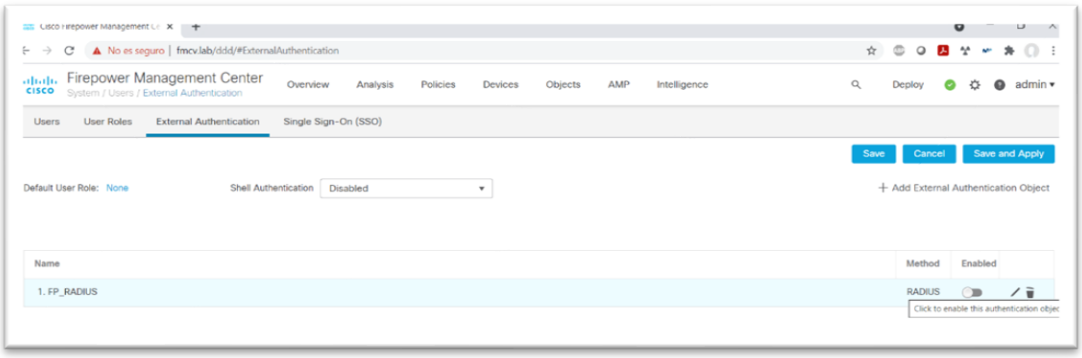


Ilustración 8. Habilitando Enabled para RADIUS

Importante. Una vez asignado el Radius, los usuarios locales, como “admin”, seguirán pudiendo ser utilizados. Se recomienda, dejar solo el usuario “admin” como local y ponerle una contraseña muy compleja que solo se use en caso de problemas de acceso.

Adicionalmente, se puede establecer el número de fallos de contraseña para bloqueo a 3 para el usuario “admin” y provocar los fallos para que se bloquee la cuenta. De esta manera, no habrá forma de que un usuario utilice un usuario de administración local y sólo los usuarios definidos como administradores en el servidor de autenticación externo podrán tener plenos poderes en el sistema.

Para poder acceder con los usuarios de Radius al CLI/SSH del gestor FMC, se debe seleccionar en el campo “Shell Authentication” el Radius correspondiente.

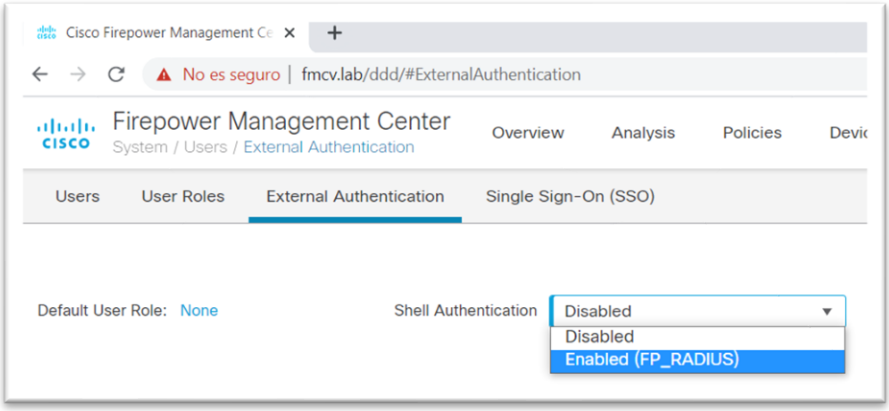


Ilustración 9. Desplegable "Shell Authentication"

Recuerde guardar con “Save and Apply”.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

La administración de la solución de Cisco Secure Firewall se realiza principalmente a través de la interfaz gráfica (GUI). Sin embargo, durante la configuración inicial de los equipos, para ciertas operaciones y para la resolución de problemas es posible acceder a los equipos mediante la línea de comandos (CLI).

6.3.1.1 ADMINISTRACIÓN DEL FMC

En la configuración inicial del dispositivo se genera un certificado autofirmado para la conexión segura mediante el protocolo HTTPS. Este certificado debe ser sustituido por otro de confianza (trusted) emitido por una entidad de certificación (CA).

Para generar la nueva llave privada y la petición de certificado es necesario conectarse al gestor por HTTPS y acceder al menú `System->Configuration->HTTPS Certificate`.

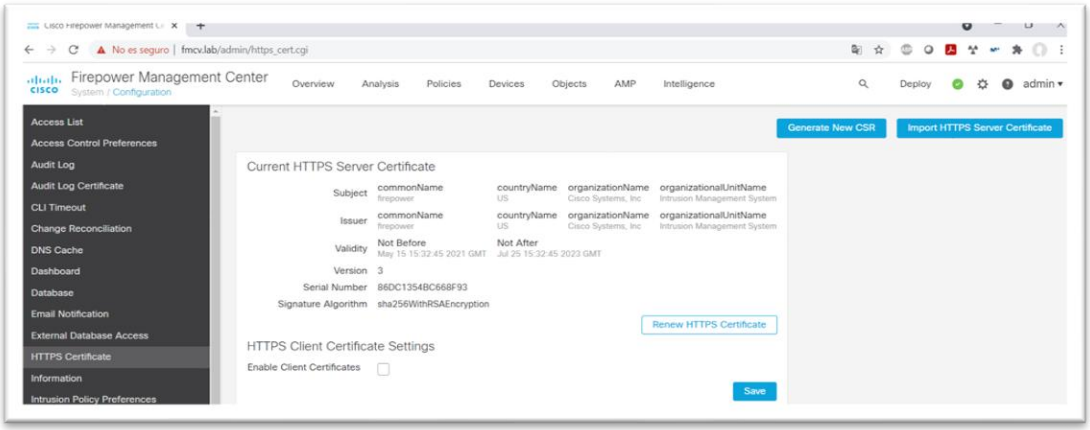


Ilustración 10. Configuración del certificado HTTPS

Pulse “Generate New CSR” y rellene los campos.

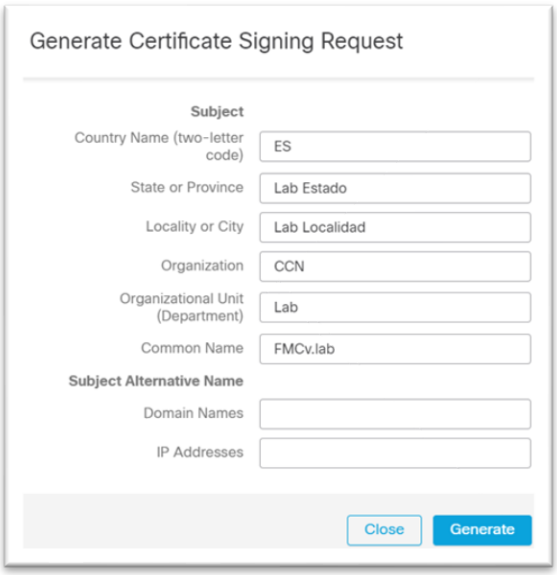


Ilustración 11. Generando la solicitud de certificado

Se obtendrá una solicitud de certificado en formato PEM que deberá llevar a la autoridad certificadora para la obtención del certificado.

Se recomienda que la autoridad certificadora añada los campos SAN (Subject Alternative Name) para ambos, el nombre DNS y la IP.

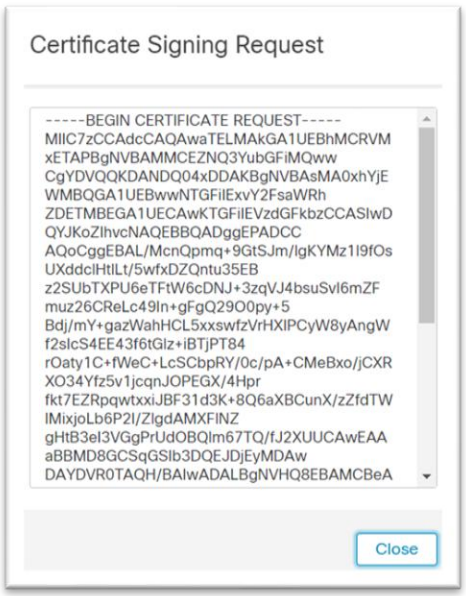


Ilustración 12. Solicitud de certificado

Una vez obtenido el certificado deberemos importarlo pinchando sobre “Import HTTPS Server Certificate”. En el desplegable deberemos pegar el certificado en formato PEM y,

adicionalmente, la cadena de certificación, certificado de la CA root e intermedia.

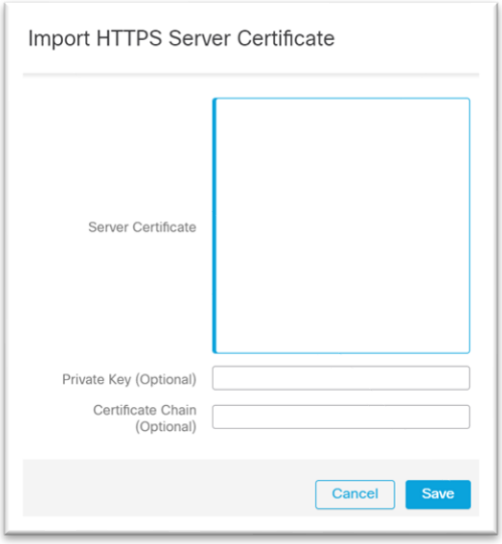


Ilustración 13. Importando certificado

Si al importar el certificado el equipo devuelve el error “Basic constraints are not critical or not defined”, es porque el FMC es estricto en cuanto a que el certificado generado debe contener la restricción “critical”: X509v3 Basic Constraints: critical.

Se deberá generar un certificado con esa extensión.

En las versiones recientes de FMC este atributo ya no es requerido.

Una vez importado con éxito el certificado, pulse SAVE para que el servicio se reinicie con el nuevo certificado.

Se vuelve a acceder a la pantalla de login HTTPS y se verifica que el certificado es ahora correcto.



Ilustración 14. Verificando el certificado en el navegador

El acceso al FMC por CLI está restringido a SSH versión 2. Por defecto, los cifrados permitidos son aes128-gcm@openssh.com, aes256-gcm@openssh.com, chacha20-poly1305@openssh.com, aes256-ctr, aes128-ctr y aes192-ctr. Estos cifrados están en línea con los requisitos del CCN definidos en la guía CCN-STIC 807 - Criptología de empleo en el Esquema Nacional de Seguridad (ver referencia [REF16]. Los cifrados soportados no son configurables de manera directa y en caso de tener que modificarse se recomienda abrir un caso con el soporte técnico de Cisco [REF17].

Para equipos FMC físicos, el acceso por consola es a través de un puerto VGA (el puerto por defecto), un cable serie o Light-Out Management (LOM) para los equipos que lo soportan.

6.3.1.2 ADMINISTRACIÓN DEL FTD

Los cortafuegos gestionados por FMC no tienen gestión por GUI. El acceso HTTPS puede habilitarse solo como mecanismo para monitorizar la salud en entornos de nube pública con balanceador. Por defecto este acceso está deshabilitado y no se recomienda habilitarlo salvo por el motivo descrito anteriormente.

El acceso por SSH se permite por defecto en la interfaz de gestión del equipo; cualquier otra interfaz debe configurarse manualmente, y solo se permite el acceso con SSH versión 2 y los mismos cifrados que los descritos para el FMC.

Los equipos físicos tienen un puerto de consola que permite el acceso local.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

La gestión de usuarios y permisos en FMC está basada en roles. A cada usuario se le asigna uno o más roles dentro de los roles definidos, que determinan lo que este puede hacer. Estos deben ser adaptados y asignados a la organización siguiendo los principios de mínimo privilegio y separación de funciones.

Existen una serie de roles predefinidos, se pueden crear nuevos con mezcla de permisos.

Los diferentes roles por defecto son:

- Administrator: Es el rol de mayor privilegio. Permisos de lectura y escritura en todo el sistema. El usuario “admin” por defecto pertenece a este grupo.
- Access Admin: Da acceso a las ACP (Access Control Policies) y características asociadas en el menú de políticas. No puede realizar Deploys.
- Discovery Admin: Permite acceso a Network Discovery, Application Detection y características de Correlación en el menú de políticas. No puede realizar Deploys.
- External Database User: Provee de acceso solo-lectura a la base de datos del sistema Firepower, que soporta conexiones JDBC SSL. Para permitir a aplicaciones de terceros interactuar con la base de datos se debe habilitar primero el acceso en el menú de configuración del FMC en la sección de “External Database Access”.
- Intrusion Admin: Permite acceso a las políticas de intrusión (IPS), reglas de intrusión y network analysis. No puede realizar Deploys.
- Maintenance User: Provee de acceso a características de monitorización y mantenimiento. Principalmente en el menú Health.
- Network Admin: Permite la administración de política de acceso ACP, inspección SSL, políticas DNS, políticas de identidad, así como la configuración de características de dispositivos en el menú Devices. Puede realizar Deploys.
- Security Analyst: Provee acceso a las características de análisis de eventos de seguridad y acceso de solo lectura a eventos de Health, Overview, Análisis y menú System.

- Security Analyst (Read Only): Provee acceso de solo-lectura a las características de análisis de eventos de seguridad además de a eventos de Health, Overview, Análisis y menú System.
- Security Approver: Permite acceso limitado a las políticas de acceso ACP y network Discovery. Puede visualizar y hacer Deploy de estas políticas, pero no hacer cambios.
- Threat Intelligence Director (TID) User: Provee de acceso al Threat Intelligence Director (si se encuentra activado).

Estos usuarios pueden ver y configurar el TID. Además de estos roles, se pueden crear nuevos roles customizados desde "Create User Role" donde dar acceso a los distintos menús del FMC de manera granular. Al contrario que los roles por defecto, estos roles customizados sí pueden modificarse seleccionando el icono del lápiz a la derecha del nombre del rol.

A la derecha de cada rol hay un botón deslizante de "Enabled" para deshabilitar un rol para todos los usuarios o volver a habilitarlo.

En la configuración de cada usuario local se pueden también definir las condiciones relacionadas con la contraseña del usuario tal y como indica la guía de referencia CCN-STIC 807:

- Máximo número de intentos de login fallidos. Debe ser 3 intentos.
- Longitud mínima de la contraseña. Debe ser 12 caracteres.
- Días hasta la expiración de la contraseña. La contraseña deberá cambiarse en un máximo de 60 días.
- Composición de la contraseña segura. Al activar esta opción se exigirán los siguientes requisitos para la contraseña:
  - Al menos una mayúscula.
  - Al menos una minúscula.
  - Al menos un dígito.
  - Al menos un carácter especial.
  - No puede tener más de dos caracteres repetidos consecutivos.
  - La contraseña se valida contra un diccionario de contraseñas comunes con el que no puede coincidir.

Los criterios de credenciales para usuarios definidos con autenticación externa quedarán sujetos a las condiciones definidas en el directorio de usuarios.

Desde la sección de "User Configuration" de la configuración del FMC se deberá definir el número de intentos fallidos de login a 3 y el tiempo de bloqueo de la cuenta en caso de varios intentos fallidos a 3 minutos.

También se define en la sección de configuración global la cantidad de sesiones simultáneas permitidas para un mismo usuario o dirección IP, así como el tiempo de inactividad antes de la desconexión automática de la sesión, que debe ser de 5 minutos.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

Una de las tareas más importantes de una integración es la correcta configuración de las interfaces y zonas de seguridad.

6.4.1 ZONAS DE SEGURIDAD

El concepto de zonas de seguridad se basa en la compartimentación, agrupando equipos de funcionamiento similar en cuanto a la red dentro de la misma zona.

Las definiciones de las zonas de seguridad también están sujetas a valoraciones subjetivas. Por ejemplo, una zona de seguridad "Servidores" la podemos definir como equipos a los que acceden los usuarios para sus peticiones y trabajo. Pero unos equipos, por ejemplo, bases de datos, a los que acceden otros servidores, podrían tratarse de la misma zona de seguridad, porque son servidores, o podría crearse otra zona nueva distinta "BackEnd" que se defina como de acceso solo desde "Servidores".

Es por ello importante que las zonas de seguridad se creen con definiciones formales que ayuden a entender por qué han sido creadas y la lógica de compartimentación.

En Secure Firewall, una interfaz de red puede ser asignada solo a 1 zona de seguridad. Pero 1 zona de seguridad puede contener varias interfaces. O, lo que es lo mismo, varias interfaces pueden ser asignadas a la misma zona de seguridad.

La zona de seguridad es importante porque se puede hacer referencia a ella en la política de seguridad ACP (Access Control Policy) y crear reglas sobre la misma.

Las zonas de seguridad pueden crearse en la sección de objetos `Objects->Object Management` o bien al editar una interfaz. En la creación y gestión de interfaces suele ser más conveniente.

6.4.2 ASIGNACIÓN DE DIRECCIONAMIENTO IP

Las direcciones IP son asignadas a las interfaces, que pueden ser interfaces físicas, EtherChannels (agregación de puertos), Subinterfaces (VLAN), o incluso Bridging (BVI).

En la sección de "Device Management," seleccionando un cortafuegos, podemos acceder a su sección de "Interfaces" y editar una interfaz para asignarle direccionamiento.

La interfaz debe asignarse a una zona de seguridad y tener un nombre (Name). Si la zona de seguridad no existe, la podemos crear desde el menú.

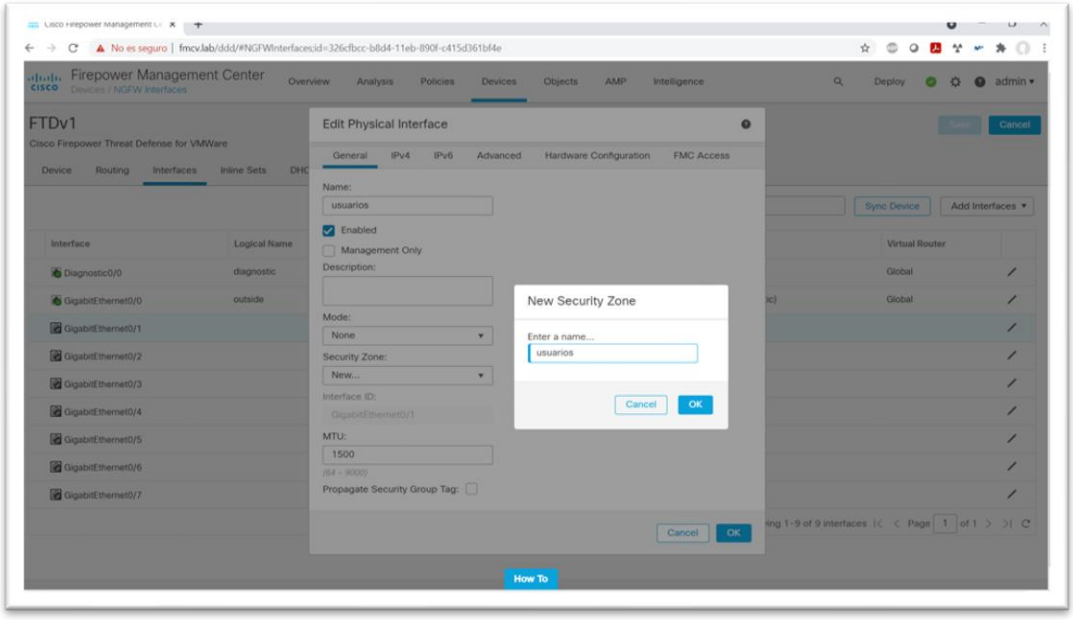


Ilustración 15. Asignando zona de seguridad

El direccionamiento se especifica en la pestaña de IPv4 (o IPv6). La notación puede ser con máscara en barra diagonal o clásica.

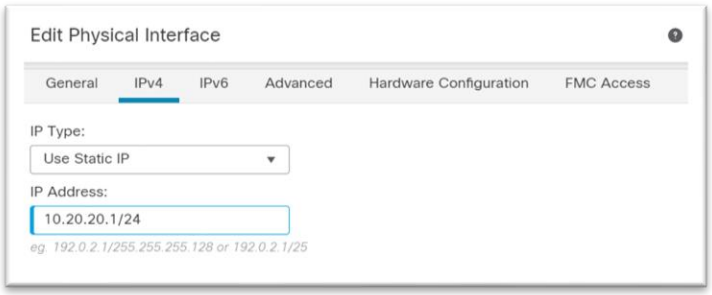


Ilustración 16. Dando dirección IP

Varias interfaces pueden ser asignadas a las mismas zonas de seguridad.

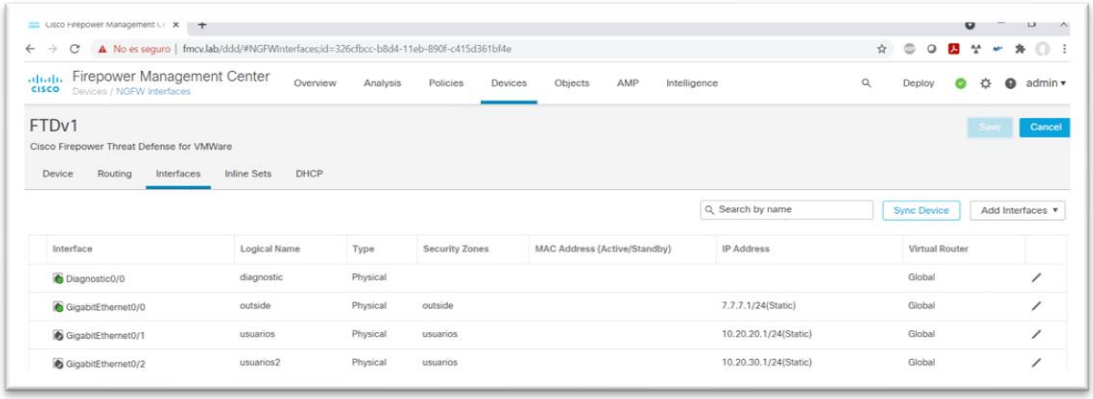


Ilustración 17. Asignación de IPs a zona de seguridad

Hay que recordar que para que los cambios sean efectivos, se requiere un Deploy al dispositivo cortafuegos.

6.4.3 ANTI-SPOOFING

Por norma general se debe habilitar la característica anti-spoofing.

Esta funcionalidad prohíbe que lleguen paquetes con IP de origen desde interfaces que, desde el punto de vista del cortafuegos, no están en ese rango. Es decir, que ni la IP del firewall está en ese rango, ni existe ruta hacia esa IP por esa interfaz.

Para activarlo, se realiza en la parte Advanced de la edición de la interfaz, que debe tener direccionamiento IP asignado.

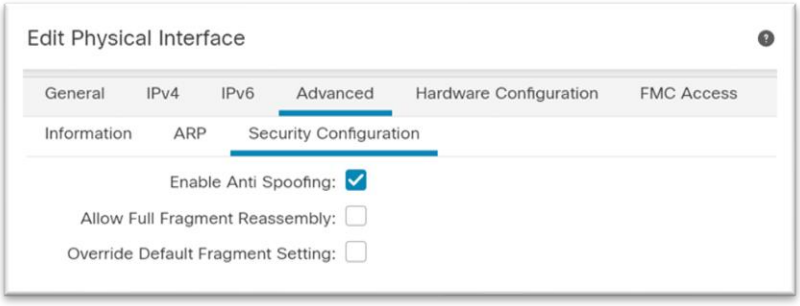


Ilustración 18. Habilitando Anti Spoofing

6.4.4 ARP ESTÁTICO

En ocasiones se debe asignar un ARP estático a una IP determinada. Por ejemplo, para intentar prevenir ataques del tipo Man-in-the-Middle (ARP spoofing).

Un caso de uso típico para esto es una red de interconexión WAN compartida donde se quiere asegurar que los paquetes siempre irán directamente al peer de conexión, evitando cualquier spoofing sencillo.

La configuración se realiza en el apartado Advanced de la interfaz, que debe tener direccionamiento IP asignado. El “Enable Alias” no se debe habilitar.

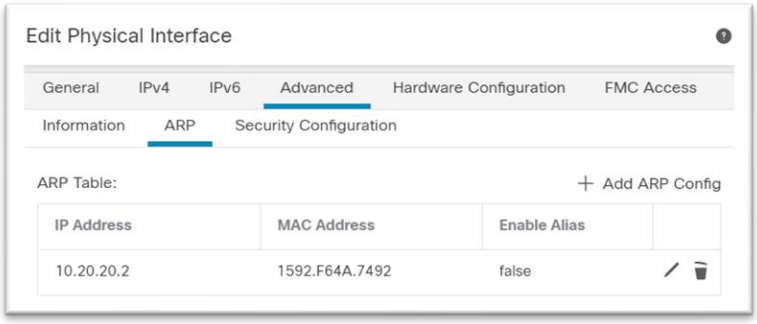


Ilustración 19. Habilitando ARP estático

6.4.5 CONSIDERACIONES FÍSICAS Y LÓGICAS

Es importante que todos los puertos que no estén en uso en el equipo se encuentren en "shutdown". Por defecto, una interfaz sin configuración no procesará tráfico ni permitirá el acceso al equipo. Sin embargo, es buena práctica confirmar que, a nivel lógico, la interfaz esté en "shutdown" y no permita ningún intento de conexión al puerto.

También es importante que aquellos puertos que sí cuenten con cableado y estén en uso se marquen mediante etiquetas físicas y, en la descripción de la interfaz en el software, se indique a qué equipo conecta cada puerto.

6.5 GESTIÓN DE CERTIFICADOS

Cisco Secure Firewall soporta y recomienda la utilización de algoritmos y funciones criptográficas en conformidad con las especificaciones establecidas en la guía **CCN-STIC-807 [**REF16**]**. Los parámetros soportados y recomendados son:

- **RSA**: Claves de al menos 3072 bits de longitud.
- **ECDSA**: Curvas P-256 o superiores.
- **DSA**: Claves de al menos 3072 bits de longitud.
- **Funciones Hash**: SHA-256 o superiores.

Estos algoritmos se pueden configurar durante la generación de solicitudes de certificados (CSR) y la importación de certificados en el FMC.

La gestión de los certificados se hace como objetos en la configuración del FMC. En la referencia [REF3] se encuentran todos los detalles al respecto.

6.6 SINCRONIZACIÓN

En un cortafuegos es de vital importancia que la fecha y la hora sean las correctas, tanto por cuestiones de funcionalidad como de visualización de conexiones en los logs, eventos ocurridos en un momento determinado, etc.

Para los equipos FPR4100 y FPR9300, la sincronización se realiza a través del protocolo NTP (Network Time Protocol), desde el Firepower Chassis Manager en la sección de “Platform Settings”.

a) Primero se debe configurar correctamente la zona horaria (Time Zone) y posteriormente el servidor o servidores NTP a utilizar. En Platform Settings > NTP, seleccionar la zona horaria correcta en el desplegable Time Zone y pulsar Save.

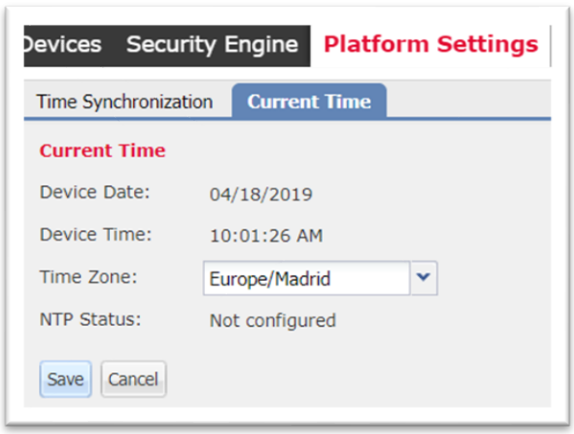


Ilustración 20. Configurando la zona horaria

b) En el mismo panel, dentro de Set Time Source, marcar Use NTP Server. Marcar NTP Server Authentication: Enable y confirmar con Yes. En FXOS la autenticación NTP es global (se aplica a todos los servidores configurados) y admite únicamente claves SHA1; el valor de la clave (Authentication Value) debe introducirse en formato hexadecimal. Nota: a diferencia de la vía FMC descrita anteriormente, FXOS no admite AES-128 CMAC para la autenticación NTP. Pulsar Add e identificar cada servidor por su dirección IP (recomendado). Si se emplea un nombre de host/FQDN, es imprescindible haber configurado previamente un servidor DNS en el chasis, ya que de lo contrario fallará la resolución. Se pueden configurar hasta 4 servidores NTP.

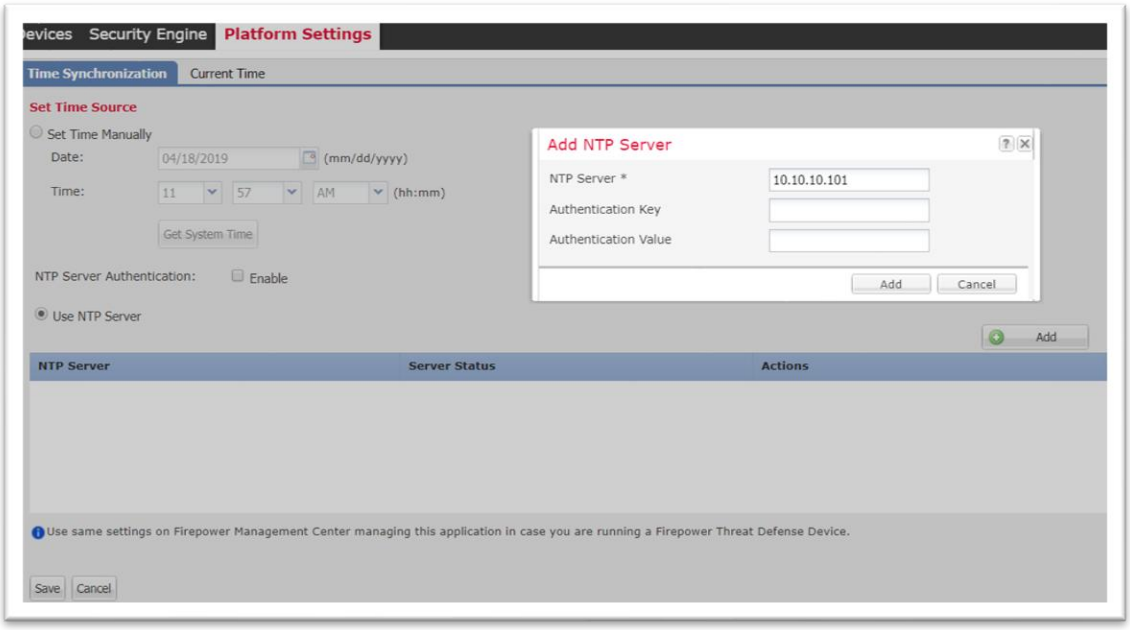


Ilustración 21. Configuración del servidor NTP

c) Se pueden configurar hasta 4 servidores NTP. Introducir el Authentication Key ID y el Authentication Value (clave SHA1 en hexadecimal) de cada servidor.

d) Una vez añadidos todos los servidores, pulsar Save.

Para el resto de los modelos la sincronización de tiempo se hace a través del FMC. Por defecto, el sistema FMC usa los servidores de NTP de Sourcefire para la sincronización de la hora. Sin embargo, estos requieren que el equipo tenga acceso a Internet.

Se pueden configurar otros servidores NTP libremente. El menú se encuentra en `System -> Configuration-> Time Synchronization`. Se pueden especificar varios servidores.

Al configurar un servidor NTP, se recomienda usar autenticación y que esta utilice un tipo de clave segura, a ser posible AES-128 CMAC.

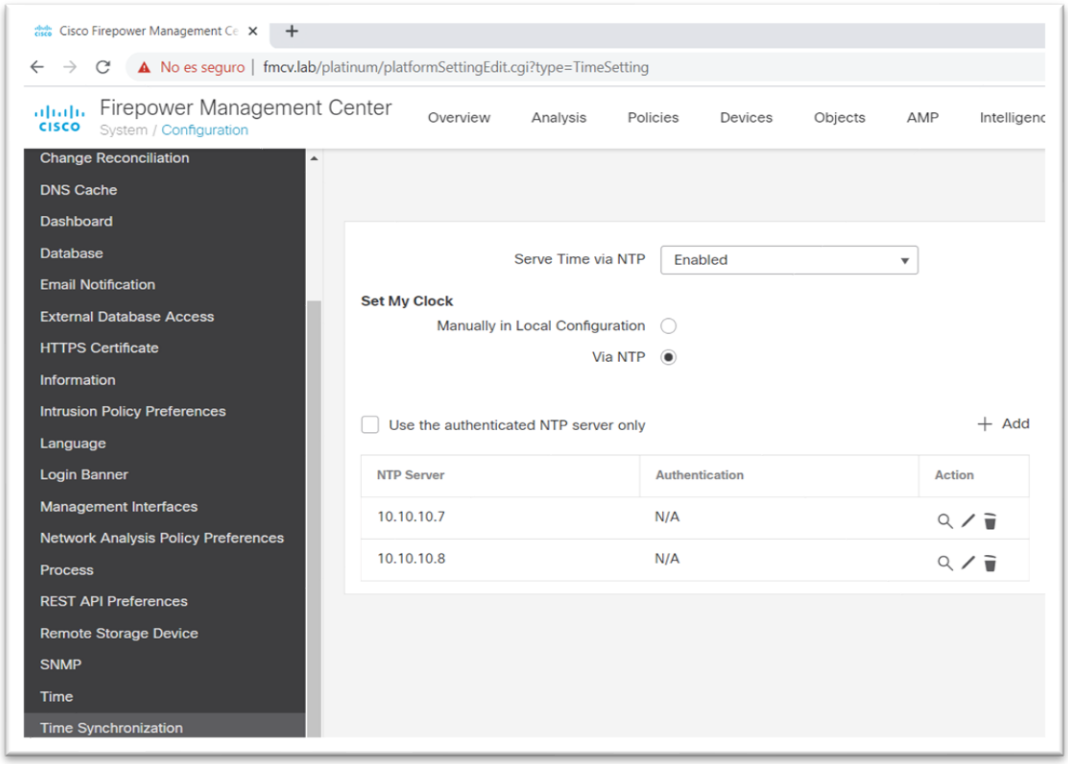


Ilustración 22. Configurando servidor NTP desde la interfaz web

La hora se muestra en UTC, pero puede ser más conveniente que la información que consultemos y usemos en el gestor sea la hora local correcta. Para ello, hay que especificarlo por usuario. En `USUARIO->User Preferences->Time Zone Preference` podemos especificar nuestra zona horaria.

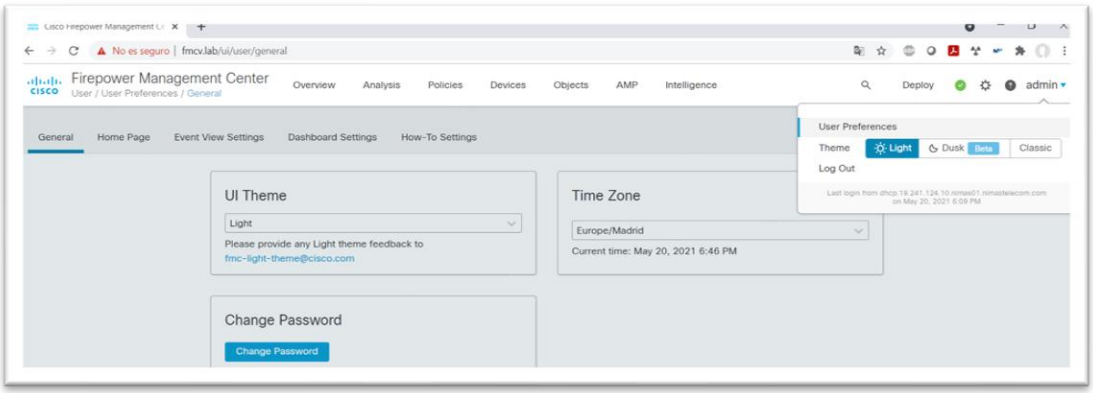


Ilustración 23. Especificación de zona horaria

Esta configuración es local y para el propio usuario y no afecta a los relojes del sistema.

6.7 ACTUALIZACIONES

Se recomienda tener actualizado el sistema a las últimas versiones recomendadas por el fabricante dentro de la versión mayor estable.

Para actualizar el sistema FMC se deberá descargar la imagen desde la web de Cisco, ya sea de manera manual o desde el propio FMC. El fichero es un ".tar" que no se debe descomprimir.

El FMC también se encarga de copiar los ficheros de actualización a los cortafuegos a través del canal de comunicación seguro de gestión entre el FMC y los cortafuegos.

El proceso de actualización de los equipos se puede encontrar en la referencia [REF4].

Además del software de los equipos, es importante mantener los paquetes de contenido actualizados con la última información sobre aplicaciones, vulnerabilidades, reglas de IPS y la base de datos de direcciones IP. La gestión de estos paquetes se hace desde la sección de "Content Updates".

6.8 AUTO-CHEQUEOS

Cisco Firepower ejecuta autochequeos de integridad y verificación del software automáticamente al inicio del sistema.

En caso de fallo en la validación del software, el equipo entrará en modo ROM Monitor a la espera de que se restaure el sistema al completo mediante un restablecimiento de fábrica (factory reset) o arrancando manualmente una imagen que supere las validaciones de integridad.

6.9 ALTA DISPONIBILIDAD

Todos los equipos Secure Firewall de Cisco soportan la configuración de alta disponibilidad.

La alta disponibilidad es una característica de vital importancia en cortafuegos de centro de datos, no solo por la mitigación de problemas de hardware, sino también para realizar las actualizaciones de los equipos con un corte mínimo o inapreciable. Ver referencia [REF5] para más detalles sobre la alta disponibilidad.

Además, la alta disponibilidad puede aumentar las capacidades de los cortafuegos si su funcionamiento es en clúster. Ver referencia [REF6] para más información sobre cómo configurar un clúster y las consideraciones de este despliegue.

6.10 AUDITORÍA

6.10.1 REGISTRO DE EVENTOS

En Cisco Secure Firewall, el registro de eventos incluye logs de configuración, sistema, seguridad y auditoría, siguiendo el ENS. Se registran cambios de configuración, autenticaciones, accesos, actualizaciones de políticas y alertas de seguridad. Los logs, en texto plano estructurado compatible con syslog, contienen campos como fecha/hora, tipo de evento, usuario, IP y descripción. La configuración se realiza desde el Firewall Management Center, habilitando los

eventos necesarios y definiendo formato y destino según las mejores prácticas de Cisco y requisitos del Centro Criptológico Nacional.

Los distintos tipos de eventos están descritos en la sección de Events and Assets que se encuentra en la referencia [REF7].

Los cortafuegos también son capaces de generar eventos relacionados con la plataforma en formato Syslog, que reporten datos sobre el estado del equipo, comportamientos anómalos o información del uso de la plataforma. Estos syslog tienen un sistema de códigos asociados que definen tanto la severidad del mismo como su categoría. La lista completa de syslog de plataforma se puede encontrar en la referencia [REF8].

6.10.2 ALMACENAMIENTO LOCAL

Los logs internos generados por los cortafuegos pueden ser necesarios para depurar problemas y/o ser usados para almacenar toda la información de las conexiones realizadas a través de estos.

Estos logs se generan como Syslog y pueden tanto enviarse a un servidor externo como almacenarse localmente.

A nivel local, los syslog rotarán en función de la configuración.

Un ajuste que suele servir para depurar problemas es loggear todos los eventos de nivel informational o inferior. Configure de esta manera pulsando OK, no ADD.

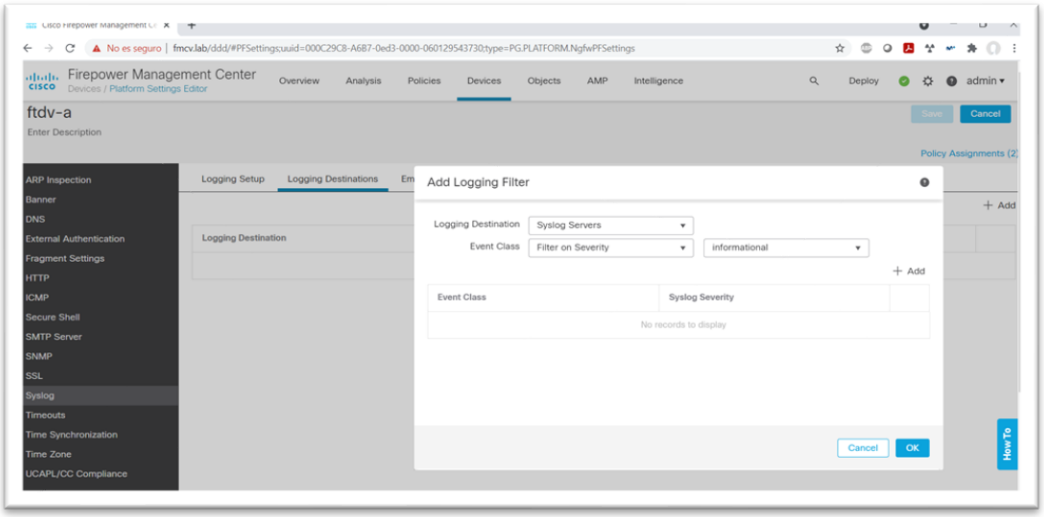


Ilustración 24. Filtrado de Logs

Seleccionar la casilla de “Enable Logging” y guardar la configuración con el botón de “Save”.

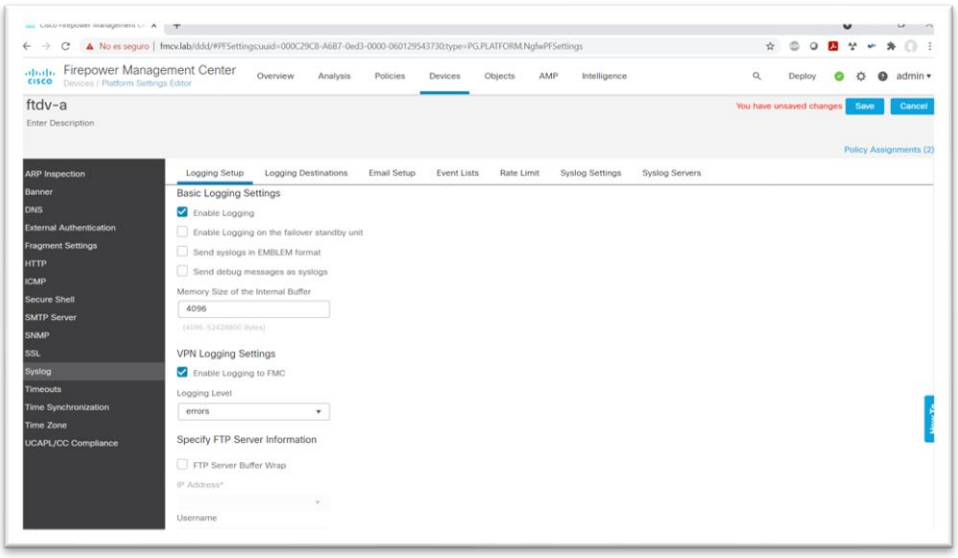


Ilustración 25. Activando los logs de auditoría

Tras aplicar la configuración, los logs se pueden ver por CLI con el comando “show logging”.

6.10.3 ALMACENAMIENTO REMOTO

En la sección anterior se describió el proceso para definir el logging de eventos de la plataforma. Los cortafuegos Cisco también permiten definir servidores externos a los que enviar los mensajes Syslog. Esta conexión puede ser vía TCP o UDP. Los detalles sobre la configuración de un servidor Syslog externo se encuentra en la [REF9].

6.11 BACKUP

Las copias de seguridad forman parte de la seguridad ya que proveen de respaldo para la restauración del servicio y, también, una imagen en el tiempo de los cambios que puedan haberse realizado inadvertidamente en los sistemas.

Existen dos tipos de copia de seguridad: copia de seguridad del gestor, Firepower Management Center, y copia de seguridad de los dispositivos.

Se deben realizar también copias de seguridad periódicas de los dispositivos, especialmente cuando se vaya a realizar una actualización a una versión mayor del dispositivo o se requiera tener una copia de respaldo por algún motivo específico. Una copia puede ser restaurada en un equipo de sustitución para facilitar su reemplazo en una arquitectura de alta disponibilidad.

Las copias de seguridad pueden realizarse directamente en el almacenamiento local del gestor o en un almacenamiento remoto. Se recomienda el almacenamiento remoto.

- Las copias de seguridad del FMC pueden ser de la configuración, de la información recibida por Threat Intelligence Director (TID) y de los eventos.

El proceso de cómo realizar una copia de seguridad se puede encontrar en la referencia [REF10].

También es posible programar los backups de manera recurrente como está explicado en la [REF11]. Se recomienda realizar las copias de seguridad de configuración al menos una vez por semana.

7 REFERENCIAS

[REF1] Install and Upgrade Guides
https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html

[REF2] Chapter: Licenses
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/740/management-center-admin-74/system-licenses.html

[REF3] Chapter: Certificates
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/740/management-center-device-config-74/objects-certs.html

[REF4] Upgrades and Updates
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/740/management-center-admin-74/system-updates.html

[REF5] Chapter: High Availability
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/740/management-center-device-config-74/high-availability.html

[REF6] Chapter: Clustering
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/740/management-center-device-config-74/device-ops-cluster-sec-fw-3100.html

[REF7] Events and Assets
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/740/management-center-admin-74/events-connection-logging.html

[REF8] Syslog Messages Guide
https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/fptd_syslog_guide.html

[REF9] Syslog Server Configuration
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/740/management-center-device-config-74/interfaces-settings-platform.html#concept_8637BBD154854CA498A2DA66D55A115E

[REF10] Chapter: Backup/Restore
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/740/management-center-admin-74/tools-backup.html

[REF11] Chapter: Scheduling
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/740/management-center-admin-74/tools-scheduling.html

[REF12] Chapter: Device Management
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/740/management-center-device-config-74/get-started-device-management.html

[REF13] Add an LDAP External Authentication Object for the Firewall Management Center
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/740/management-center-admin-74/system-users.html#id_63679

[REF14] Device Coverage Checker https://cway.cisco.com/sncheck/

[REF15] Cisco Software Central https://software.cisco.com/

[REF16] Guías CCN-STIC https://www.ccn-cert.cni.es/es/guias.html

[REF17] Cisco Support https://support.cisco.com/

[REF18] CPSTIC
https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

8 ABREVIATURAS

ACP	Access Control Policy
AES-128 CMAC	Advanced Encryption Standard 128-bit Cipher-based Message Authentication Code
AMP	Advanced Malware Protection
AntiDDoS	Anti-Distributed Denial of Service
ARP	Address Resolution Protocol
BVI	Bridge-Group Virtual Interface
CA	Certificate Authority
CC	Common Criteria
CDP	Centros de Proceso de Datos
CLI	Command Line Interface
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación
CSR	Certificate Signing Request
DNS	Domain Name System
DoDIN APL	Department of Defense Information Network Approved Products List
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad
FDM	Firewall Device Manager
FMC	Firewall Management Center
FMCv	Firewall Management Center virtual
FTD	Firewall Threat Defense
FTDv	Firewall Threat Defense virtual
FXOS	Firepower eXtensible Operating System
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
JDBC	Java Database Connectivity
LDAP	Lightweight Directory Access Protocol
LOM	Lights-Out Management

NPS	Network Policy Server
NTP	Network Time Protocol
PEM	Privacy-Enhanced Mail
RSA	Rivest-Shamir-Adleman
SAML	Security Assertion Markup Language
SAN	Subject Alternative Name
SHA-256	Secure Hash Algorithm 256
SHA-512	Secure Hash Algorithm 512
SIEM	Security Information and Event Management
SSH	Secure Shell
SSL	Secure Sockets Layer
Syslog	System Logging Protocol
TACACS+	Terminal Access Controller Access-Control System Plus
TID	Threat Intelligence Director
TLS	Transport Layer Security
UCAPL	Unified Capabilities Approved Products List
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network
WAN	Wide Area Network
X509v3	X.509 version 3