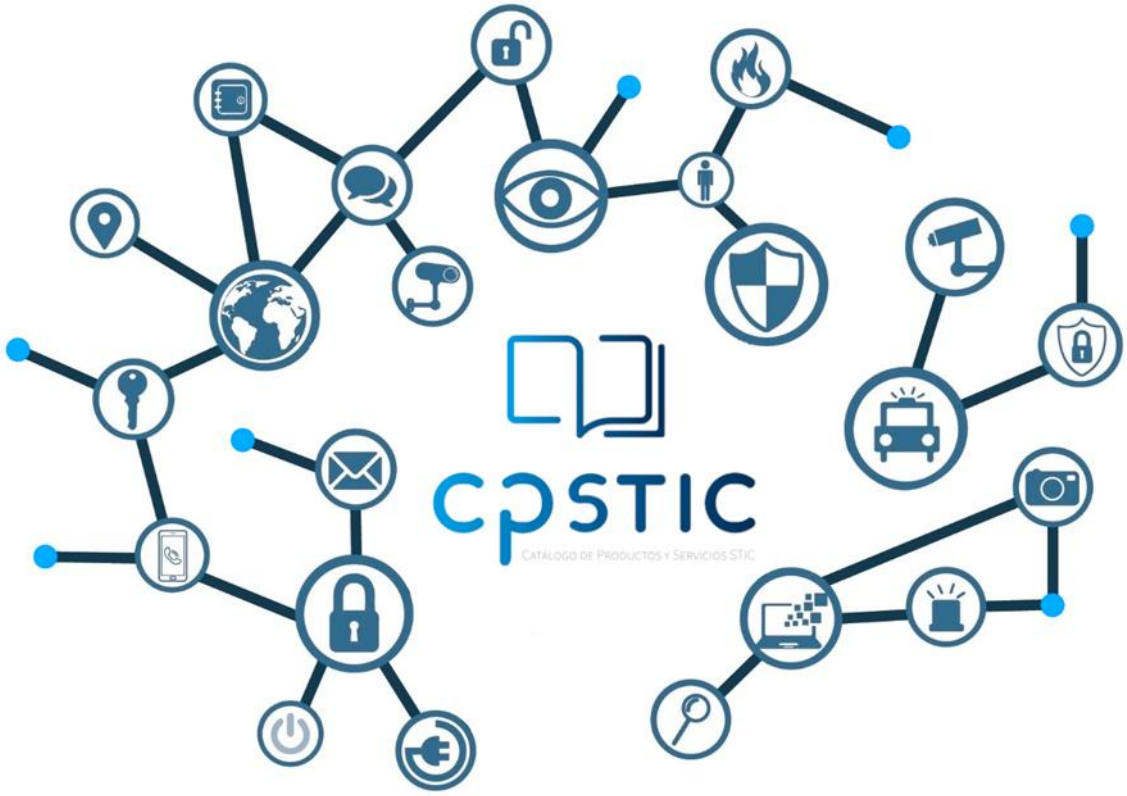
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1465

Procedimiento de empleo seguro
Cisco Catalyst 8200&8500 Series Edge Routers
(Cat8200. Cat8500). versión IOS-XE 17.6



Febrero 2025

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

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-25-201-8
Fecha de Edición: febrero de 2025.

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2026.01.16 07:49:46 +01'00'

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

ÍNDICE

1. INTRODUCCIÓN

1. El objetivo de este documento es proporcionar una guía o procedimiento de configuración y empleo seguro de las siguientes familias de enrutadores:
   a) Cisco Catalyst 8200 Series Edge Routers (Cat8200)
   b) Cisco Catalyst 8500 Series Edge Routers (Cat8500)
2. En todos los casos se va a usar el sistema operativo Cisco IOS-XE 17.6
3. Cisco Catalyst 8K Series Edge Routers es la nueva serie de enrutadores Cisco diseñada para ser escalable, segura y optimizada para un entorno multicloud. Gracias a sus características avanzadas, proveen un gran rendimiento y automatización para tecnologías tales como SD-WAN, 5G Wireless WAN y arquitecturas SASE.
4. La estructura del documento y sus contenidos no exigen una lectura lineal del mismo. Se recomienda al lector utilizar el índice de contenidos para localizar el capítulo que trate el aspecto concreto sobre el que se desee obtener información.

2. OBJETO Y ALCANCE

5. En la presente guía se recoge el procedimiento de empleo seguro para las familias de enrutadores Catalyst 8200 Series Edge Routers y Catalyst 8500 Series Edge Routers.

6. El objetivo es poner en conocimiento del administrador del enrutador los mecanismos de seguridad necesarios para proteger los sistemas de información y comunicaciones que empleen enrutadores de las familias de enrutadores cualificadas anteriormente mencionadas. Con este conocimiento, es posible establecer un marco de referencia que contemple las recomendaciones STIC en el despliegue y utilización de estas familias de enrutadores.

7. Este documento, salvo menciones especiales, no aporta ajustes de configuración para la operación del enrutador, fuera de las directamente relacionadas con su operación en modo seguro. Aspectos como las políticas de flujo de información y el control de acceso, deben ser implementadas de acuerdo con las políticas vigentes en la organización.

2.1 PRODUCTOS

8. En la siguiente tabla se muestran, en detalle, los diferentes modelos de cada serie que han sido cualificados dentro del catálogo de productos y servicios de seguridad TIC (CPSTIC) en la familia de “Enrutadores”.

2.1.1 CATALYST 8200

Familia	Modelo	Identificador
Familia Catalyst 8200	C8200-1N-4T	Cisco C8200-1N-4T
	C8200L-1N-4T	Cisco C8200L-1N-4T

Tabla 1. Modelos incluidos en la guía

2.1.2 CATALYST 8500

Familia	Modelo	Identificador
Familia Catalyst 8500	L-8S4X	Cisco C8500L-8S4X

Tabla 2. Modelos incluidos en la guía

2.2 SOFTWARE

9. Los routers llevan un Software Cisco IOS-XE cuyo nombre tiene la nomenclatura 17.6.Y.
   a) La *Major Release* (17) tiene varias *Minor Release*: 17.1, 17,2, ..., 17.6.
   b) Cada *Minor Release* tiene varias *Maintenance Release*: 17.6.1, 17.6.2, etc.

Ilustración 1. Versiones de Software.

10. Este documento se refiere a cualquier *Minor Release* de las versiones 17.6.
11. Más información sobre las imágenes IOS-XE se encuentra en la guía de Cisco: IOS-XE [1].

3. ORGANIZACIÓN DEL DOCUMENTO

12. El resto del documento se organiza y estructura de acuerdo con los apartados siguientes:

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

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.

d) Apartado **7.** En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto

e) Apartado **8.** Lista de comprobación de las configuraciones y recomendaciones planteadas en el procedimiento.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

13. Se deben seguir los siguientes pasos para verificar que el enrutador no ha sido manipulado durante la entrega:

    a) Antes de abrir el paquete, asegúrese de que tenga la serigrafía y logo de Cisco Systems. Si no lo tiene, contacte al proveedor (Cisco Systems o un distribuidor autorizado).

    b) Verifique que el paquete no ha sido abierto y vuelto a sellar, prestando atención a la cinta que lo cierra. Si parece haber sido manipulado, contacte con el proveedor, ya sea Cisco Systems o un distribuidor autorizado.

    c) Asegúrese de que la caja de cartón tenga la impresión resistente a manipulaciones de Cisco en la cara externa. Si no la tiene, contacte al proveedor. Esta impresión contiene información importante sobre el enrutador, tal como el número de producto de Cisco, su número de serie e información adicional sobre el contenido de la caja.

    d) Verifique que el número de serie del enrutador corresponde con el número de serie en la documentación del pedido y en la factura. Este número de serie debe aparecer en la etiqueta blanca de la caja enviada. Si no es así, se debe contactar con el proveedor del equipo (Cisco Systems o un distribuidor autorizado).

    e) En la recepción de la unidad, es necesario comprobar que el pedido fue enviado por el proveedor esperado (Cisco Systems o un distribuidor autorizado). Este proceso puede llevarse a cabo verificando el código de envío/paquete junto con la empresa de transporte. También es recomendable comprobar que los números de serie de los productos enviados concuerdan con los números de serie de los productos recibidos. Esta verificación debe ser llevada a cabo por algún mecanismo externo que no pertenezca al proceso de envío. Por ejemplo, teléfono, fax o un servicio online de rastreo de paquetes.

4.2 ENTORNO DE INSTALACIÓN SEGURO

14. Se debe instalar el enrutador dentro de un Centro de Proceso de Datos (CPD) que cuente con un sistema de control de acceso limitado únicamente a las personas autorizadas. Para asegurarse de que solo estas personas tengan acceso al enrutador (incluso fuera del horario laboral), la sala que alberga el CPD también debe contar con un sistema de control.

4.3 REGISTRO Y LICENCIAS

15. A partir de la versión 16.5.1 de IOS XE, se introduce el modo de licenciamiento “Cisco Smart Licensing”, el cual es opcional hasta la versión 16.9.8, pero se convierte en mandatorio a partir de la versión 16.10.1.

16. En el modelo Smart Licensing, los clientes pueden activar objetos con licencia sin el uso de una clave de software especial o un archivo de licencia de actualización. Los clientes simplemente activan la nueva funcionalidad usando los comandos y configuraciones apropiados para cada tipo de enrutador y la funcionalidad se activa. Es posible que en algunos casos se requiera de un reinicio del software según las capacidades y los requisitos del enrutador.

17. De manera similar, realizar un “downgrade” o eliminar una característica, rendimiento o funcionalidad avanzada requeriría simplemente de la eliminación de la configuración o el comando introducido anteriormente.
18. De los diferentes modos existentes para el licenciamiento Smart-licensing de plataformas de enrutadores, se contemplan los siguientes:
    - CSSM (Cisco Smart Software Manager): Mediante este procedimiento, el enrutador requiere de una configuración que le permita realizar consultas DNS y acceder a “tools.cisco.com” a través de los protocolos HTTP y HTTPS.
    - CSSM a través de CSLU (Cisco Smart License Utility): Este procedimiento emplea un software (CSLU) en una máquina de confianza, que será la que realice las consultas al portal de licencias de Cisco. El enrutador lanzará consultas a través de este software en lugar de realizarlo directamente.
    - CSSM a través de un Controlador: Si el enrutador está integrado en una plataforma de gestión como DNA-Center o vManage, será esta la encargada de gestionar las consultas y asignaciones de licencias entre la plataforma Smart Licensing y el enrutador.
    - *Sin conexión hacia el portal de Smart-Licensing:* Se asignan licencias a través de tokens, y se actualizan en la plataforma de Smart-Licensing a través de diferentes métodos
19. Para más información referente al licenciamiento de los enrutadores, revisar la referencia [6].

4.4 CONSIDERACIONES PREVIAS

20. El correcto funcionamiento del enrutador requiere de una serie de medidas en el entorno. Es responsabilidad del administrador autorizado garantizar que el entorno operacional proporciona las funciones necesarias y cumple los objetivos de seguridad siguientes:
    a) El enrutador no ofrece ninguna protección del tráfico que lo cruza. Se asume que la protección de dicho tráfico estará cubierta por otras medidas de seguridad y confianza en el entorno operativo.
    b) Las credenciales del administrador (clave privada) utilizadas para acceder al enrutador deben estar protegidas en cualquier otra plataforma en donde se encuentren.
    c) El administrador de seguridad garantiza que no hay ningún acceso no autorizado posible para la información residual confidencial (por ejemplo, claves criptográficas, material de claves, contraseñas, etc.) en el equipo de red, cuando el equipo se elimine o se retire de su entorno operativo.

5. FASE DE INSTALACIÓN

5.1 INSTALACIÓN FÍSICA

21. Para instalar correctamente el enrutador, es importante seguir las instrucciones detalladas en el "Manual de Instalación de Hardware de Cisco" [1]-[4] para cada uno de los enrutadores de la presente guía.

5.2 INSTALACIÓN SOFTWARE

22. El enrutador vendrá con una imagen del software Cisco IOS-XE cargada. Sin embargo, puede que el número de versión no sea la versión cualificada. En este caso, habrá que actualizar la versión:

    a) Descargar el archivo de la imagen de software cualificado en un ordenador de confianza. Las versiones cualificadas se pueden consultar en el CPSTIC.

    b) Las imágenes de software están disponibles en la siguiente URL:

    https://software.cisco.com/download/home

23. Después de descargar el archivo, es responsabilidad del administrador verificar que no haya sido alterado comprobando que SHA-512 del archivo descargado coincide con el hash de la imagen señalada en la Tabla 3. Si los hashes no coinciden, se deberá notificar al Centro de Asistencia Técnica (TAC) de Cisco.

    https://www.cisco.com/c/es_es/support/index.html

24. Una vez que el fichero ha sido copiado, se recomienda leer atentamente las diferentes guías [5]-[9], las cuales le ayudarán a tener una visión global del proceso de instalación y configuración.

25. Antes de la instalación, es importante verificar la firma digital del software utilizando el comando "**show software authenticity file**". Este comando permite mostrar información sobre la autenticación del software, incluyendo credenciales de la imagen, tipo de clave utilizada para la verificación, información de la cabecera y otros atributos de la firma, todo ello específicamente para cada imagen. Al ejecutar el comando, se extraerá la cabecera de la firma y sus campos a partir del archivo de la imagen, y se mostrará la información necesaria.

```
RT-IOS-XE17-CCN# show software authenticity file

RT-IOS-XE17-CCN# show software authenticity file flash:/sysboot/isr4400-mono-
universalk9.17.06.03a.SPA.pkg
File Name:   bootflash:/sysboot/isr4400-mono-universalk9.17.06.03a.SPA.pkg
Image type:  Production
             Signer Information
                    Common Name   :  CiscoSystems
Organization Unit   :  IOS-XE
Organization Name   :  CiscoSystems
Certificate Serial Number : 62502A52
Hash Algorithm            : SHA512
Signature Algorithm       : 2048-bit RSA
    Key Version                 : A
```

26. Para mostrar información relacionada con la autenticidad del monitor ROM actual (ROMMON), librería de monitorización (monlib), y la imagen de Cisco IOS usada para el proceso de arranque, deberá usarse el siguiente comando en modo EXEC privilegiado:

```
RT-IOS-XE17-CCN# show software authenticity running

RT-IOS-XE17-CCN# show software authenticity running
SYSTEM IMAGE
------------
Image type                        : Production
    Signer Information
        Common Name               : CiscoSystems
        Organization Unit         : IOS-XE
        Organization Name         : CiscoSystems
    Certificate Serial Number     : 62502A6D
    Hash Algorithm                : SHA512
    Signature Algorithm           : 2048-bit RSA
    Key Version                   : A

    Verifier Information
        Verifier Name             : ROMMON
        Verifier Version          : System Bootstrap, Version 17.6.1, RELEASE
SOFTWARE
Copyright (c)

ROMMON
------
Image type                        : Production
    Signer Information
        Common Name               : CiscoSystems
        Organization Unit         : IOS-XE
        Organization Name         : CiscoSystems
    Certificate Serial Number     : 60A59F44
    Hash Algorithm                : SHA512
    Signature Algorithm           : 2048-bit RSA
    Key Version                   : A

    Verifier Information
        Verifier Name              : Microloader
        Verifier Version          : MA0001R06.0404072015

Microloader
-----------
Image type                        : Release
    Signer Information
        Common Name               : CiscoSystems
        Organization Name         : CiscoSystems
    Certificate Serial Number     : 56ff20f4c0becb2824ec5fe6467b91ec
    Hash Algorithm                : HMAC-SHA256
    Verifier Information
        Verifier Name             : Hardware Anchor
        Verifier Version          : F01001R16.2187dab732018-06-28
```

27. Para instalar y configurar el enrutador, es necesario seguir las instrucciones descritas en cada una de las guías de configuración según la plataforma que se esté empleando [1]-[9].

28. Iniciar el enrutador y confirmar que carga la imagen correctamente, completa las autocomprobaciones internas, y muestra el aviso de exportación criptográfica en la consola.

29. Una vez que el enrutador haya sido iniciado, es importante verificar que se esté utilizando la versión cualificada del mismo. Para hacerlo, se puede utilizar el comando "show version",

el cual mostrará el nombre del archivo de la imagen del sistema en uso, así como la versión del software del sistema.

Plataforma	Nombre de imagen	Hash (SHA512 Cheksum)
C8200-1N-4T	c8000be-universalk9.17.06.06a.SPA.bin	8f5e5797de84795c7e9d67df2820ee2f8af9c61b5294a7de454edd21e03ea6ded10b063e1c225d62e29be023303ee8ecd92643e941f59707d23ec20b5c526968
C8200L-1N-4T	c8000be-universalk9.17.06.06a.SPA.bin	8f5e5797de84795c7e9d67df2820ee2f8af9c61b5294a7de454edd21e03ea6ded10b063e1c225d62e29be023303ee8ecd92643e941f59707d23ec20b5c526968
L-8S4X	c8000aes-universalk9.17.06.06a.SPA.bin	0d45daa77f2981e6fc63b5a18fea5b14962f0cc638eea8edcff1c8cd6d3b96d05e40417fed9bdd1f851fdc4f6821950b824af54a1f5997888fe8b3a997883818

Tabla 3. Imágenes IOS evaluadas

6. FASE DE CONFIGURACIÓN

6.1 MODOS DE OPERACIÓN

30. Un enrutador con sistema operativo IOS-XE tiene varios modos de funcionamiento:

    - **Booting** – durante el proceso de inicio, los enrutadores detienen todo el tráfico de red hasta que se cargue la imagen del enrutador y su configuración. Este modo avanza automáticamente hacia el modo normal de operación. Si el administrador pulsa la tecla de pausa en una conexión de consola durante los primeros 60 segundos del arranque, ingresará al modo ROM Monitor. Este modo se describe en la documentación de la IOS como "Inicialización de ROM Monitor". Además, si el enrutador no encuentra una imagen de sistema operativo válida, ingresará al modo ROM Monitor en lugar del modo normal, para proteger al enrutador de un arranque no seguro.
    - **Normal** – se carga la imagen de IOS del enrutador y su configuración, y el enrutador opera de acuerdo a dicha configuración. Todos los niveles de acceso administrativo ocurren en este modo y todas las funciones de seguridad basadas en el enrutador están en funcionamiento. Durante el funcionamiento, el enrutador tiene poca interacción con el administrador. Sin embargo, la configuración inadecuada del enrutador puede afectar negativamente la seguridad. Si se configura mal, la red no protegida puede tener acceso a la red interna/protegida.
    - **ROM Monitor** – Este modo es para tareas de mantenimiento, resolución de problemas y recuperación. Mientras el enrutador se encuentre en este modo, no se enruta ningún tráfico de red entre las interfaces de red. En este estado, se puede configurar el enrutador para cargar una nueva imagen de inicio desde un servidor TFTP específico, realizar tareas de configuración y ejecutar diversos comandos de resolución de problemas. Aunque no se requiere contraseña de administrador para acceder al modo ROM Monitor, se necesita acceso físico al enrutador. Por lo tanto, el enrutador debe mantenerse en un lugar seguro para evitar el acceso no autorizado, que puede provocar que el enrutador se encuentre en un estado no seguro.

31. Después de producirse un error de operación, el enrutador se reiniciará una vez se restaure la corriente eléctrica y automáticamente entrará en el modo *Booting*.

6.2 CONFIGURACIÓN INICIAL VÍA *DIRECT CONSOLE CONNECTION*

32. Todos los enrutadores y sus diferentes versiones incluidas en esta guía deben ser configurados, al menos con una configuración básica inicial, a través de una conexión de consola. Tras realizar esta configuración inicial, se puede conectar el enrutador a la red deseada.

6.2.1 CONFIGURACIÓN INICIAL DE LOS ROUTERS

33. La instalación se inicia automáticamente cuando el enrutador no tiene ningún archivo de configuración en su NVRAM. Al finalizar, presenta el Diálogo de Configuración del Sistema (Cisco Setup Command Facility). Dicho diálogo guía al administrador durante la configuración inicial, con indicaciones sobre la información básica del enrutador y la red. Posteriormente, toma todos estos datos y crea un archivo de configuración inicial. En las guías de los diferentes enrutadores [2]-[5] se puede consultar el método para establecer la

configuración básica inicial y realizar cambios en la misma. Durante la configuración inicial, es necesario tener en cuenta algunos puntos:

a) La cuenta creada durante la instalación inicial del enrutador se considera el administrador privilegiado y se otorga acceso a todos los comandos del enrutador.

b) El término "administrador autorizado" se refiere en el presente documento a cualquier administrador que se haya autenticado con éxito en el enrutador, y tenga acceso a los privilegios adecuados para realizar las funciones solicitadas.

c) La Guía de Referencia de Comandos IOS muestra un listado de los comandos disponibles para cada tipo de enrutador de esta guía [2]-[5]. De los comandos disponibles detallados en la Guía de Referencia se destacan los siguientes:

- ***Enable Secret*** – La contraseña debe ajustarse a los requisitos de complejidad descritos en la sección **6.5** CONTRASEÑAS del presente documento. Este comando garantiza que el *Enable Password* no se guarde en texto plano. Se configurará el *Enable Secret* tal como se indica en [7]-[10]:

  Si introducimos el comando "enable secret" seguido de la contraseña en texto plano, automáticamente la contraseña se encriptará. Se recomienda confirmar esta opción tras completar la configuración inicial. Para ello podemos ejecutar "show running configuration" y verificar que tengamos el texto "*enable secret 9*" dentro del archivo de configuración.

- ***Enable Password*** – La contraseña debe ajustarse a los requisitos de complejidad descritos en la sección **6.5** CONTRASEÑAS del presente documento. Este comando se utiliza para controlar el acceso a diversos niveles de privilegio. Esta contraseña deberá ser distinta a la de *Enable Secret* y se configurará siguiendo la siguiente guía [8]:

  El comando que permite realizar esta configuración es:

```
RT-IOS-XE17-CCN(config-line)# enable password 7 <hidden password>
```

- ***Virtual Terminal Password*** –Se recomienda proteger las líneas del terminal virtual (*vty*) con una contraseña que debe cumplir idénticos requisitos de complejidad que las anteriormente descritas. Esta contraseña permite el acceso al enrutador únicamente a través de la línea de comandos. En la sección 6.3.1 se indicarán los pasos a seguir para permitir *ssh* en las líneas *vty.* Se recomienda seguir las instrucciones facilitadas en la guía [9]:

- Verificar que **SNMP (Simple Network Management Protocol)** está deshabilitado (ya viene así por defecto). Para verificarlo, hay que revisar que en el archivo de configuración no aparezca ninguna entrada "snmp-server". Para garantizar que no hay ningún agente de servidor SNMP en funcionamiento, se utilizará el comando "no snmp-server". El comando quedaría como se muestra a continuación:

```
RT-IOS-XE17-CCN(config)# no snmp-server
```

6.2.2 GUARDAR LA CONFIGURACIÓN

34. IOS-XE utiliza una configuración de funcionamiento(running-config) y una configuración de inicio(startup-config). Cuando se realiza algún tipo de cambio sobre la configuración, este cambio se realiza sobre la configuración en funcionamiento. Para guardar dicha configuración, que se encuentra en la memoria, debe copiarse en la configuración de inicio. Esto se puede llevar a cabo utilizando el comando ***'write memory',*** el comando ***'copy system:running-config nvram:startup-config'*** ó el comando ***'copy running-config startup-config'***.

35. Estos comandos deben utilizarse con frecuencia cuando se realicen cambios en la configuración del enrutador. Si el enrutador se reinicia por cualquier motivo y hay cambios sin guardar, dichos cambios se perderán y este volverá a la última configuración guardada en la startup-config.

6.2.3 HABILITANDO MODO FIPS

36. El enrutador debe ejecutarse en el modo de operación seguro usando el parámetro FIPS. El uso del módulo criptográfico en cualquier otro modo no ha sido cualificado, y por lo tanto se debe emplear la configuración que se indica. Para habilitar el modo FIPS se deben ejecutar los siguientes comandos :

```
RT-IOS XE17-CCN#configure terminal
RT-IOS-XE17-CCN(config)# platform ipsec fips-mode
```

37. Se recomienda ajustar el valor del campo de arranque a 0x0102 con el objetivo de que se arranque automáticamente desde la imagen de IOS. Para ello, se debe ejecutar desde la línea de comandos ROMMON el comando "confreg 0x0102"

38. Durante el arranque del enrutador, como parte del POST, se realizarán las autocomprobaciones para las funciones criptográficas automáticamente. Si se desea realizar esta comprobación de manera manual, se puede emplear el siguiente comando:

```
RT-IOS-XE17-CCN# test crypto self-test
```

39. Para ejecutar dicho comando, es necesario estar registrado con un usuario de administrador.

40. En caso de fallo en el procedimiento de autocomprobaciones, el enrutador pasa a un estado de error, deteniéndose cualquier transmisión de datos segura. Si se da el caso, el propio enrutador nos muestra información referente a su estado e indicando el fallo.

6.2.4 CONFIGURACIÓN DE ADMINISTRADOR Y CREDENCIALES

41. Para garantizar la trazabilidad de todas las acciones realizadas sobre el enrutador, es necesario que se creen en el mismo un usuario nominal para cada uno de los administradores. Estos usuarios y contraseñas deberán ser únicos, debiendo también tener una contraseña para el comando "enable". Se debe garantizar que todas las contraseñas se almacenen de forma cifrada usando el siguiente comando:

```
RT-IOS-XE17-CCN# service password-encryption
```

42. Configurar la autenticación local AAA:

```
RT-IOS-XE17-CCN(config)# aaa new-model (necesario si no está habilitado)
RT-IOS-XE17-CCN(config)# aaa authentication login default local
RT-IOS-XE17-CCN(config)# aaa authorization exec default local
```

43. Al crear cuentas de administradores, se les debe otorgar un nivel de privilegio que es un número del 0 al 15, siendo el 1 el que se configura por defecto. El nivel de privilegio, siendo 15 el que otorga más privilegios, determina los comandos que puede ejecutar cada usuario en el enrutador y no son estrictamente jerárquicos. Para más información sobre los niveles de privilegio, se puede consultar el apartado 6.4.

44. Para crear un usuario, debemos ejecutar el siguiente comando:

```
RT-IOS-XE17-CCN#configure terminal
RT-IOS-XE17-CCN(config)#username <name> privilege [0-15] password <password>
```

45. Si se omite el parámetro "privilege" asignará por defecto el nivel 1.

6.2.5 FIN DE SESIÓN

46. Ha de establecerse un tiempo límite de inactividad para las sesiones de administración. Para establecer dicho límite se utilizan los siguientes comandos:

```
RT-IOS-XE17-CCN#configure terminal
RT-IOS-XE17-CCN(config)# line vty <first> <last>
RT-IOS-XE17-CCN(config-line)# exec-timeout <min> <sec>
RT-IOS-XE17-CCN(config-line)# line console
RT-IOS-XE17-CCN(config)# exec-timeout <min> <sec>
```

47. <first> y <last> son el rango de líneas vty a configurar (por ejemplo "1" y "15"), <min> y <sec> hacen referencia a los minutos y los segundos de inactividad que deben pasar para que la sesión finalice. Este tiempo de inactividad en ningún caso deberá ser superior a 15 minutos.

48. Esta configuración solo puede ser realizada desde un usuario administrador y no se aplica en la sesión actual desde la cual se realiza la configuración. Para que aplique dicha configuración, debe cerrarse sesión y volver a iniciar la sesión, en la cual ya estará vigente el tiempo de expiración configurado.

6.2.6 BLOQUEO DE USUARIO

49. Se recomienda configurar las cuentas de usuario para que queden bloqueadas después de un número máximo de intentos fallidos de autenticación. Esto deberá configurarse mediante el siguiente comando, donde el parámetro *"<x>"* indica el número de intentos fallidos requeridos antes del bloqueo.

```
RT-IOS-XE17-CCN(config)# aaa local authentication attempts max-fail <x>
```

50. Este bloqueo solo aplica a usuarios de privilegio 14 o inferior. Además, esto aplica a fallos consecutivos, y no se reinicia el contador por las desconexiones de la sesión SSH. Por ejemplo, si este comando de bloqueo está definido en 5 fallos, y SSH se desconecta después de 3 fallos, si el usuario intenta otra sesión SSH e introduce credenciales incorrectas dos veces más, la cuenta se bloqueará.
51. Las cuentas que han sido bloqueadas requieren desbloqueo por parte de un administrador privilegiado antes de que puedan ser utilizadas de nuevo.
52. Una cuenta de usuario bloqueada puede ser desbloqueada utilizando el siguiente comando, siendo *"<parámetros>"* el nombre de usuario concreto que se quiere desbloquear o "all" para especificar que se desbloqueen las cuentas de todos los usuarios bloqueados:

```
RT-IOS-XE17-CCN# clear aaa local user lockout <parámetros>
```

53. Los intentos fallidos de inicio de sesión se pueden borrar con el siguiente comando:

```
RT-IOS-XE17-CCN# clear aaa local user fail-attempts <username>.
```

54. Si un administrador privilegiado quiere listar los usuarios bloqueados puede usar el siguiente comando:

```
RT-IOS-XE17-CCN# show aaa local user lockout
```

6.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

6.3.1 PROTOCOLOS DE ADMINISTRACIÓN REMOTA

55. El servicio de Telnet se encuentra habilitado por defecto para propósitos de configuración y debe ser desactivado**.** Para la administración remota CLI solamente se utilizará el protocolo SSHv2.
56. Para asegurar que el administrador no utilice Telnet para la administración remota, se debe configurar el siguiente comando en las líneas vty, de manera que solamente se acepten conexiones SSH:

```
RT-IOS-XE17-CCN(config-line)# transport input ssh
```

57. Además, todos los algoritmos criptográficos utilizados por el protocolo SSH deberán cumplir los requisitos establecidos por la guía CCN-STIC-807 para nivel Alto del ENS.

6.3.1.1 PASOS PARA CONFIGURAR SSH EN EL ROUTER

58. El primer paso es configurar un nombre al enrutador:

```
RT-IOS-XE17-CCN(config)# hostname RT-IOS-XE17-CCN
```

59. Configurar un nombre de dominio con el siguiente comando:

```
RT-IOS-XE17-CCN(config)# ip domain name cisco.com
```

60. Para activar SSHv2, utilice el comando:

```
RT-IOS-XE17-CCN(config)# ip ssh version 2
```

61. Antes de configurar la sesión SSH, las claves RSA para el servidor SSH deben estar generadas. La longitud de la clave por defecto es de 1024 bits, siendo lo **exigible 3072 bits**, y se puede configurar hasta un máximo de 4096 bits. Para ello el usuario debe hacer uso del siguiente comando:

```
RT-IOS-XE17-CCN(config)# crypto key generate rsa modulus <size>
```

Solo una pareja de claves puede estar configurada, por lo que si se repite el comando sobrescribe las claves actuales [20].

62. Las claves RSA generadas por este comando se guardan en la memoria NVRAM (que nunca se muestra al usuario o se guarda en otro enrutador). Para ello, una vez las claves han sido generadas, se deben guardar con el siguiente comando, "**copy run start**". Si las claves no son guardadas, se pierden en el siguiente reinicio del enrutador.

63. SSH debe estar configurado para requerir al menos el uso de un grupo 15 para Diffie-Hellman. Para configurarlo se ha de especificar un tamaño mínimo de módulo de 3072 utilizando el siguiente comando [12]:

```
RT-IOS-XE17-CCN(config)# ip ssh dh min size 3072
```

64. Adicionalmente, tenemos que recordar que debemos configurar nuestro cliente SSH para el uso del grupo 15 de DH.

65. Otras configuraciones recomendadas para SSH son:

a) La utilización de AES-128-GCM y AES-256-GCM como algoritmos de cifrado. Para establecer esta configuración, utilice el siguiente comando [12]:

```
RT-IOS-XE17-CCN(config)# ip ssh server algorithm encryption aes128-gmc aes256-
gcm
```

b) La utilización de hmac-sha2 como algoritmo MAC. Para establecer esta configuración, utilice el siguiente comando [12]:

```
RT-IOS-XE17-CCN(config)# ip ssh server algorithm mac hmac-sha2-256 hmac-sha2-
512
```

c) Fijar el tiempo de inactividad de sesión y el número máximo fallos de autenticación. Para el tiempo de inactividad, el tiempo máximo, por defecto, y recomendado es de 120 segundos. Respecto al número de intentos de autenticación el valor por defecto es 3 y el máximo es 5. Se puede configurar con el uso de los siguientes comandos:

```
RT-IOS-XE17-CCN(config)# ip ssh timeout <segundos>
RT-IOS-XE17-CCN(config)# ip ssh authentication-retries <intentos>
```

d) Se recomienda configurar un tiempo máximo para que la sesión SSH vuelva a intercambiar claves (SSH rekey interval). Se recomienda no más de 60 minutos y no más de un gigabyte de intercambio de datos. Para ello se debe usar el siguiente comando:

```
RT-IOS-XE17-CCN(config)# ip ssh rekey {time <tiempo_minutos> | volume
<volumen_en_KB>}.
```

66. Para desconectar las sesiones SSH use el comando:

```
RT-IOS-XE17-CCN# disconnect ssh
```

67. Por último, se recomienda desactivar el resto de los protocolos: HTTP, HTTPS y SNMP. Para ello, ejecute los siguientes comandos respectivamente:

```
RT-IOS-XE17-CCN(config)# no ip http server
RT-IOS-XE17-CCN(config)# no ip http secure-server
RT-IOS-XE17-CCN(config)# no snmp-server
```

6.3.2 PROTOCOLOS DE AUTENTICACIÓN DE SERVIDOR

68. Un servidor RADIUS se puede utilizar para la autenticación remota de los administradores del enrutador. Está desactivado por defecto, pero el administrador puede habilitarlo. Se deben usar buenas prácticas para la selección y protección de la clave, asegurando que la clave no es fácilmente adivinable ni compartida con usuarios desautorizados. Consulte [11] para obtener más información acerca de la configuración.

69. Cuando se utilice RADIUS como protocolo de autenticación, se debe proteger la comunicación entre el enrutador y el servidor mediante un túnel IPSEC. En el punto 6.8 se detallan las diferentes configuraciones que se pueden aplicar para crear este túnel, dependiendo de en qué punto de la red se encuentre ubicado el servidor RADIUS.

6.3.3 USO DE EMBEDDED EVENT MANAGER

70. Para garantizar que todos los comandos ejecutados por un usuario administrador privilegiado (nivel 15) se guarden en un registro *syslog*, podemos utilizar el siguiente script haciendo uso de Embedded Event Manage. Para ello podemos introducir el siguiente script en el CLI:

```
RT-IOS-XE17-CCN (config)#event manager applet cli_log
RT-IOS-XE17-CCN (config-applet)#event cli pattern ".*" sync yes
RT-IOS-XE17-CCN (config-applet)#action 1.0 info type routername
RT-IOS-XE17-CCN (config-applet)#action 2.0 if $_cli_privilege gt "0"
RT-IOS-XE17-CCN (config-applet)#action 3.0 syslog msg "host[$_info_routername]
user[$_cli_username] port[$_cli_tty] exec_lvl[$_cli_privilege]
command[$_cli_msg] Executed"
RT-IOS-XE17-CCN (config-applet)#action 4.0 end
RT-IOS-XE17-CCN (config-applet)#action 5.0 set _exit_status "1"
RT-IOS-XE17-CCN (config-applet)#end
```

71. Para más información sobre el uso de EEM, consultar [16].

6.3.4 PROTECCIONES DEL REGISTRO DE AUDITORÍA REMOTO

72. En el caso de que un administrador autorizado quiera copiar los registros de actividad a un servidor *syslog*, es fundamental garantizar la seguridad de las comunicaciones con dicho servidor. Para ello, existen dos posibles métodos:

    a) Emplear un servidor *syslog* que actúe como un par IPsec. De este modo, la información se transmitiría a través de un túnel protegido por este protocolo. Para utilizar esta opción, el servidor *syslog* debe contar con la funcionalidad de IPsec.

    b) Utilizar un servidor *syslog* que no sea un par IPsec, pero que esté ubicado físicamente dentro de una instalación segura junto con un par IPsec del enrutador. De esta manera, se aprovecha el túnel creado por este par IPsec para establecer la conexión de forma segura.

73. Cuando se configura un servidor de eventos en un enrutador, los eventos que se auditan son enviados simultáneamente tanto al servidor externo como al buffer local del enrutador.

6.3.4.1 SYSLOG SERVER EJECUTÁNDOSE EN UN IPSEC ENDPOINT

74. Para implementaciones donde el servidor *syslog* puede operar como un extremo IPsec del enrutador, se protegerá mediante un túnel IPsec el envío de eventos al servidor.

75. A continuación, se muestra un ejemplo de configuración del enrutador para permitir un túnel IPsec con cifrado AES, con la dirección IP 10.10.10.101 asignada al puerto IPsec en el servidor syslog (en este caso este servidor actúa como par IPsec), con las direcciones IP 10.10.10.110 y 30.0.0.1 como locales y con el servidor syslog bajo la dirección IP 40.0.0.1 (una interfaz separada del servidor).

```
RT-IOS-XE17-CCN#configure terminal
RT-IOS-XE17-CCN(config)#crypto ikev2 keyring CCN-LLAVERO
RT-IOS-XE17-CCN(config-ikev2-keyring)#peer CCN-syslog
RT-IOS-XE17-CCN(config-ikev2-keyring-peer)#address 10.10.10.101
RT-IOS-XE17-CCN(config-ikev2-keyring-peer)#pre-shared-key CCN-syslog
RT-IOS-XE17-CCN(config-ikev2-keyring-peer)#exit
RT-IOS-XE17-CCN(config-ikev2-keyring)#exit
RT-IOS-XE17-CCN(config)#crypto ikev2 proposal CCN-proposal
       RT-IOS-XE17-CCN(config-ikev2-proposal)#encryption aes-cbc-256
       RT-IOS-XE17-CCN(config-ikev2-proposal)#integrity sha512
       RT-IOS-XE17-CCN(config-ikev2-proposal)#group 24
       RT-IOS-XE17-CCN(config-ikev2-proposal)#exit
       RT-IOS-XE17-CCN(config)#crypto ikev2 policy CCN-policy
       RT-IOS-XE17-CCN(config-ikev2-policy)#proposal CCN-proposal
       RT-IOS-XE17-CCN(config-ikev2-policy)#exit
       RT-IOS-XE17-CCN(config)#ip access-list extended CCN-acl
       RT-IOS-XE17-CCN(config-ext-nacl)#permit ip 30.0.0.0 0.0.0.255 40.0.0.0
0.0.0.255
       RT-IOS-XE17-CCN(config-ext-nacl)#exit
       RT-IOS-XE17-CCN(config)#crypto ipsec transform-set CCN-transform esp-aes
esp-sha512-hmac
       RT-IOS-XE17-CCN(cfg-crypto-trans)#mode tunnel
       RT-IOS-XE17-CCN(cfg-crypto-trans)#exit
       RT-IOS-XE17-CCN(config)#crypto ikev2 profile CCN-profile
       RT-IOS-XE17-CCN(config-ikev2-profile)#match identity remote address
10.10.10.101 255.255.255.255
             RT-IOS-XE17-CCN(config-ikev2-profile)#authentication local pre-
share
       RT-IOS-XE17-CCN(config-ikev2-profile)#authentication remote pre-share
       RT-IOS-XE17-CCN(config-ikev2-profile)#keyring local CCN-LLAVERO
```

```
      RT-IOS-XE17-CCN(config-ikev2-profile)#exit
            RT-IOS-XE17-CCN(config)#crypto map CCN-map 1 ipsec-isakmp
RT-IOS-XE17-CCN(config-crypto-map)#set peer 10.10.10.101
RT-IOS-XE17-CCN(config-crypto-map)#set pfs group24
RT-IOS-XE17-CCN(config-crypto-map)#set security-association lifetime seconds
28800
RT-IOS-XE17-CCN(config-crypto-map)#set transform-set CCN-transform
RT-IOS-XE17-CCN(config-crypto-map)#set ikev2-profile CCN-profile
RT-IOS-XE17-CCN(config-crypto-map)#match address CCN-acl
RT-IOS-XE17-CCN(config-crypto-map)#exit
RT-IOS-XE17-CCN (config)#interface Loopback1
RT-IOS-XE17-CCN (config-if)#ip address 30.0.0.1 255.255.255.0
RT-IOS-XE17-CCN (config-if)#exit
RT-IOS-XE17-CCN (config)#ip route 40.0.0.0 255.255.255.0 10.10.10.101
RT-IOS-XE17-CCN (config)#logging source-interface loopback 1
RT-IOS-XE17-CCN (config)#logging host 40.0.0.1
```

6.3.4.2 SYSLOG SERVER ADYACENTE A UN IPSEC PEER

76. Si el servidor *syslog* no está ubicado directamente junto al enrutador, el servidor *syslog* debe estar ubicado en una instalación con protección física, y debe conectarse a otro enrutador capaz de establecer un túnel IPsec con el enrutador. Esto protegerá los registros del *syslog* mientras pasen por la red pública.

77. A continuación, se muestra un ejemplo de configuración del enrutador para permitir un túnel IPsec con cifrado AES, con la dirección IP 11.1.1.4 asignada al par IPsec (en este caso se trata del par IPsec de entrada a la instalación segura), con las direcciones IP locales 10.1.1.7 y 11.1.1.6 y con el servidor syslog dentro de la subred 12.1.1.0/24. Para información sobre los siguientes comandos consulte el apartado 6.8 de la presente guía.

```
RT-IOS-XE17-CCN#configure terminal
RT-IOS-XE17-CCN(config)#crypto ikev2 keyring CCN-LLAVERO
RT-IOS-XE17-CCN(config-ikev2-keyring)#peer CCN-syslog
RT-IOS-XE17-CCN(config-ikev2-keyring-peer)#address 11.1.1.4
RT-IOS-XE17-CCN(config-ikev2-keyring-peer)#pre-shared-key CCN-syslog
RT-IOS-XE17-CCN(config-ikev2-keyring-peer)#exit
RT-IOS-XE17-CCN(config-ikev2-keyring)#exit
RT-IOS-XE17-CCN(config)#crypto ikev2 proposal CCN-proposal
RT-IOS-XE17-CCN(config-ikev2-proposal)#encryption aes-cbc-256
RT-IOS-XE17-CCN(config-ikev2-proposal)#integrity sha512
RT-IOS-XE17-CCN(config-ikev2-proposal)#group 24
RT-IOS-XE17-CCN(config-ikev2-proposal)#exit
RT-IOS-XE17-CCN(config)#crypto ikev2 policy CCN-policy
RT-IOS-XE17-CCN(config-ikev2-policy)#proposal CCN-proposal
RT-IOS-XE17-CCN(config-ikev2-policy)#exit
RT-IOS-XE17-CCN(config)#ip access-list extended CCN-acl
RT-IOS-XE17-CCN(config-ext-nacl)#permit ip 10.1.1.0 0.0.0.255 12.1.1.0
0.0.0.255
RT-IOS-XE17-CCN(config-ext-nacl)#exit
RT-IOS-XE17-CCN(config)#crypto ipsec transform-set CCN-transform esp-aes esp-
sha512-hmac
RT-IOS-XE17-CCN(cfg-crypto-trans)#mode tunnel
RT-IOS-XE17-CCN(cfg-crypto-trans)#exit
RT-IOS-XE17-CCN(config)#crypto ikev2 profile CCN-profile
RT-IOS-XE17-CCN(config-ikev2-profile)#match identity remote address 11.1.1.4
255.255.255.255
      RT-IOS-XE17-CCN(config-ikev2-profile)#authentication local pre-share
      RT-IOS-XE17-CCN(config-ikev2-profile)#authentication remote pre-share
      RT-IOS-XE17-CCN(config-ikev2-profile)#keyring local CCN-LLAVERO
      RT-IOS-XE17-CCN(config-ikev2-profile)#exit
            RT-IOS-XE17-CCN(config)#crypto map CCN-map 1 ipsec-isakmp
```

```
RT-IOS-XE17-CCN(config-crypto-map)#set peer 11.1.1.4
RT-IOS-XE17-CCN(config-crypto-map)#set pfs group24
RT-IOS-XE17-CCN(config-crypto-map)#set security-association lifetime seconds
28800
RT-IOS-XE17-CCN(config-crypto-map)#set transform-set CCN-transform
RT-IOS-XE17-CCN(config-crypto-map)#set ikev2-profile CCN-profile
RT-IOS-XE17-CCN(config-crypto-map)#match address CCN-acl
RT-IOS-XE17-CCN(config-crypto-map)#exit
RT-IOS-XE17-CCN (config)#interface gi1
RT-IOS-XE17-CCN (config-if)#ip address 11.1.1.4 255.255.255.0
 RT-IOS-XE17-CCN (config-if)#crypto map CCN-map
RT-IOS-XE17-CCN (config-if)#exit
RT-IOS-XE17-CCN (config)#ip route 12.1.1.0 255.255.255.0 11.1.1.4
RT-IOS-XE17-CCN (config)#logging host 12.1.1.1
```

6.3.5 CONFIGURACIÓN BASE DE FIREWALL RULE SET

78. Como se verá más adelante en el punto 6.8, para comunicar dos redes externas entre sí permitiendo el acceso confiable entre ambas redes se hará uso de VPNs. Este acceso entre redes debe filtrarse de manera que solamente las redes incluidas dentro de esta configuración se puedan ver entre sí. El objetivo de aplicar este filtrado de acceso no es otro que el evitar que desde el exterior de la red protegida se puedan acceder a recursos del interior de la red.

79. La guía CCN-STIC 140 detalla los requerimientos mínimos que deben cumplirse para realizar un filtrado de paquetes básico. Este filtrado será realizado sobre diferentes protocolos. Para este procedimiento de empleo seguro, vamos a tener en cuenta el filtrado de paquetes sobre los siguientes protocolos:

    - IPv4 (RFC791)
    - IPv6 (RFC 2460)
    - TCP (RFC 793)
    - UDP (RFC 768)

80. Un administrador privilegiado debe implementar este filtrado mediante ACLs. Para ello, puede hacer uso de los comandos ip inspect, access-list, crypto map y access-group.

81. El análisis de tráfico se realiza de arriba hacia abajo en la lista de acceso. La primera entrada que coincida con un paquete será la que se le aplique. Se requiere que las listas de control de acceso del enrutador se configuren para descartar todo el tráfico de manera predeterminada y que el tráfico que coincida con la ACL pueda registrarse. La regla predeterminada de descartar todo se puede lograr al incluir una regla de ACL para descartar todos los paquetes como la última regla en la configuración de ACL. El registro del tráfico coincidente se realiza agregando la palabra "log-input" al final de cada una de las sentencias de la ACL. A continuación, se muestran varios ejemplos de configuración de dichas ACLs.

82. Vamos a suponer que disponemos de 2 interfaces en nuestro enrutador. La interfaz GigabitEthernet1 será nuestra interfaz externa y tiene configurada la ip 192.168.10.1. La interfaz GigabitEthernet2 será nuestra interfaz interna y va a disponer de la ip 192.168.20.1

83. Si se requiere administración remota, debe permitirse explícitamente SSH, ya sea mediante la interfaz interna o la externa(En este caso se ha configurado la interfaz externa).

```
RT-IOS-XE17-CCN (config)# access-list 10 permit tcp host 192.168.10.1 host
192.168.10.1 eq 22 log-input
```

84. Para registrar las conexiones con la Autoridad de Certificación, deberá implementarse la siguiente ACL:

```
RT-IOS-XE17-CCN (config)# access-list 10 permit ip any host [IP CA] log-input
RT-IOS-XE17-CCN (config)# access-list 20 permit ip any host [IP CA] log-input
```

85. Todos aquellos puertos que no vayan a ser utilizados deberán cerrarse, dado que podrían introducir vulnerabilidades adicionales. Para ello, añadimos a la ACL las siguientes sentencias:

```
RT-IOS-XE17-CCN (config)# access-list 10 deny 132 any any log-input
RT-IOS-XE17-CCN (config)# access-list 20 deny 132 any any log-input
```

86. Deberá crearse de forma explícita la denegación por defecto de todos los paquetes que no cumplan ninguna de las sentencias de la ACL. Para ello vamos a configurar lo siguiente en cada una de las acls:

```
RT-IOS-XE17-CCN (config)# access-list 10 deny any any
RT-IOS-XE17-CCN (config)# access-list 20 deny any any
```

87. **Nota**: Se ha eliminado del final de cada sentencia el comando “log-input” para evitar que se registren un número elevado de registros.

88. Una vez creadas ambas listas de acceso, deberán aplicarse a las interfaces de la siguiente forma:

```
RT-IOS-XE17-CCN (config)# interface GigabitEthernet1
RT-IOS-XE17-CCN (config-if)# ip access-group 10 in
RT-IOS-XE17-CCN (config)# interface GigabitEthernet2
RT-IOS-XE17-CCN (config-if)# ip access-group 20 in
```

6.3.6 PROTOCOLOS DE ENRUTAMIENTO

89. Los protocolos de enrutamiento se usan para mantener las tablas de enrutamiento. Las tablas de enrutamiento se pueden configurar y mantener manualmente. Debido a la cantidad y complejidad de los diferentes protocolos de enrutamiento, queda fuera de la presente guía la configuración de estos. Se aconseja al lector que revise las guías de configuración específicas para cada protocolo.

90. En la referencia [13] se puede ver documentación oficial al respecto de cómo configurar diferentes protocolos de enrutamiento.

6.4 ROLES DE USUARIO

91. Como medida básica, se recomienda que los enrutadores se configuren siempre siguiendo los principios de mínima funcionalidad y mínimo privilegio. Estos principios implican que los usuarios administradores deberían ser los mínimos posibles y que el resto de los usuarios del enrutador no deberían tener más privilegios de los que necesiten.

92. En el conjunto de enrutadores que conforman este procedimiento de empleo seguro, se definen los siguientes roles de usuario:

    - Rol de administrador privilegiado y semi-privilegiado: El acceso privilegiado se define como cualquier usuario con cualquier nivel (de 0 a 15) que tras iniciar sesión en el enrutador, tiene la opción de entrar en el modo privilegiado del mismo. Esto es posible porque dentro de la configuración del enrutador, tiene asignado una clave del modo privilegiado asociado a su nivel de usuario (enable secret level <0-15> <0-9> password). Se recuerda que por defecto se asigna el nivel 1, y que el mayor es el 15, estando ambos preconfigurados por defecto. El resto de los niveles (0 y 2-14) se pueden personalizar para incluir comandos del nivel 15. Por ejemplo, si el comando "reload" pertenece al nivel 15, se puede añadir a un nivel 2 ("privilege exec level 2 reload").

93. Para encontrar los comandos disponibles, roles asociados y niveles de privilegio, se recomienda consultar la guía "IOS Command Reference Guide" (Guía de Referencia de Comandos IOS). [7]-[10]

6.5 CONTRASEÑAS

94. La complejidad de la contraseña no viene forzada por defecto en el enrutador, por lo que debe establecerse en la fase de configuración. Para evitar que los administradores establezcan contraseñas no seguras, se deberán seguir una serie de directrices y opciones de configuración:

95. Las contraseñas deben tener al menos **15 caracteres**. Para establecer este valor, usar el siguiente comando:

```
RT-IOS-XE17-CCN(config)#security passwords min-length 15
```

96. Una contraseña puede estar compuesta por cualquier combinación de caracteres incluyendo caracteres de al menos 3 de los siguientes conjuntos: letras en mayúscula, letras en minúscula, números y los siguientes caracteres especiales: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")".

    Esta complejidad en cuanto a contraseñas se configura habilitando el siguiente comando:

```
RT-IOS-XE17-CCN(config)# aaa password restriction
```

97. Se recomienda que las contraseñas cumplan las siguientes restricciones:

    a) La contraseña no puede contener más de tres caracteres consecutivos, tal como *abcd*.

    b) La contraseña no puede contener más de dos caracteres respetitos, tal como *aaabbb*.

    c) La contraseña no puede contener palabras de diccionario ni nombres propios.

    d) La contraseña no puede coincidir con el nombre de usuario asociado.

    e) La contraseña obtenida por la capitalización (mezcla de mayúsculas y/o minúsculas de cualquier tipo) del nombre de usuario o el mismo nombre de usuario al revés no será aceptada.

    f) La contraseña no podrá ser "cisco", "ocsic" o ninguna capitalización de las mismas. Tampoco es válido sustituir "1" por "|", "i" por "!", "o" por "0" o sustituir "s" por "$".

98. El comando anterior, solamente puede ser utilizado tras configurar el siguiente comando:

```
RT-IOS-XE17-CCN(config)# aaa new-model
```

99. Para guardar las contraseñas cifradas utilice el comando:

```
RT-IOS-XE17-CCN(config)# service password-encryption
```

100. Esté o no "**service password-encryption**" activado, se puede introducir una contraseña para un usuario en texto plano o como un valor hash SHA-256. Esta será almacenada como un valor hash SHA-256 en el fichero de configuración cuando se haga mediante el comando "**username** *name* **secret**" (más detalles en [14]). Este es un ejemplo para asignar a un usuario una contraseña utilizando el servicio *password encryption*:

    a) **username** nombre **secret** {**contraseña** | **0** | **5** contraseña cifrada |**8** contraseña cifrada | **9** contraseña cifrada }, donde:

    - "contraseña" es el valor que el usuario introduce en texto claro.
    - 0: Indica una contraseña en texto claro. Se convierte la contraseña en SHA256 y se almacena en el enrutador.
    - 5: Especifica un hash MD5. Se indica solo a modo de información, pero está totalmente desaconsejado el uso de MD5.
    - 8: Se debe introducir una contraseña con un hash en PBKDF2.
    - 9: Se debe introducir la contraseña con un hash creado por el propio enrutador mediante un script.

101. Para no guardar la contraseña *enable* en texto en claro, utilice el comando "enable secret" cuando establezca dicha contraseña. La contraseña *enable* puede ser introducida como texto en plano. Por ejemplo:

    a) **enable secret** [**level** nivel] { **contraseña** | **0** | **5** contraseña cifrada |**8** contraseña cifrada | **9** contraseña cifrada }

    - Nivel: (Opcional) Especifica el nivel al cual aplica la contraseña. Puede establecer hasta 15 niveles de privilegios, usando los números entre 1 y 15.
    - "contraseña" es el valor que el usuario introduce en texto claro.
    - 0: Indica una contraseña en texto claro. Se convierte la contraseña en SHA256 y se almacena en el enrutador.
    - 5: Especifica un hash MD5. Se indica solo a modo de información, pero está totalmente desaconsejado el uso de MD5.
    - 8: Se debe introducir una contraseña con un hash en PBKDF2.
    - 9: Se debe introducir la contraseña con un hash creado por el propio enrutador mediante un script.

6.6 CONFIGURACIÓN DEL RELOJ

102. La configuración del reloj solamente está permitida a través del administrador privilegiado. Para configurar el reloj, podemos usar los siguientes comandos que nos permitirán configurar la fecha y hora:

```
RT-IOS-XE17-CCN#configure terminal
RT-IOS-XE17-CCN(config)#clock timezone CET +1
RT-IOS-XE17-CCN(config)#clock summer-time CEST recurring last Sun Mar 2:00
last Sun Oct 3:00
```

```
RT-IOS-XE17-CCN (config)# exit

RT-IOS-XE17-CCN # clock set hh:mm:ss day month year
```

103. Otro de los métodos disponibles para configurar la fecha y hora es mediante el protocolo NTP. Para la configuración mediante este método podemos consultar en [14] e iremos navegando entre las secciones hasta llegar al apartado de configuración. Hay algunas consideraciones a tener en cuenta:

- El servidor NTP, si está configurado, es proporcionado por el entorno IT. Sin autenticación o control de acceso, NTP es inseguro y puede ser usado por un atacante para enviar paquetes NTP e intentar sobrecargar o bloquear el enrutador.
- La conexión al servidor NTP para la sincronización de tiempo debe ser protegida mediante un túnel IPsec.
- Si se va a usar NTP, configure la autenticación NTP usando **hmac-sha2-256** y el comando **ntp access-group**. Si NTP se habilita de forma global, debe ser desactivado en todas las interfaces en las cuales no sea necesario.

6.7 IDENTIFICACIÓN Y AUTENTICACIÓN

104. La configuración de identificación y autenticación está restringida al administrador privilegiado. Los enrutadores de la presente guía se pueden configurar para que utilicen alguno de los siguientes métodos de autenticación:

- Autentificación remota (RADIUS).

  Ver apartado 6.3.2 en este documento para más información.

- Autentificación local (contraseña o autentificación SSH de clave pública).

  Nota: Esta opción **solo** debe ser configurada como solución alternativa por defecto **si la autenticación remota del servidor no está disponible**.

- Certificados X.509v3.

  Ver apartado 6.8.4 de este documento para más información.

6.8 VIRTUAL PRIVATE NETWORKS(VPN)

6.8.1 IPSEC

105. El enrutador permite a los administradores privilegiados configurar políticas para IKE e IPsec.

106. IPsec proporciona los siguientes servicios de seguridad en la red:

a) **Confidencialidad**: El emisor IPsec puede cifrar paquetes antes de transmitirlos por la red.

b) **Integridad**: El receptor IPsec puede autenticar paquetes enviados por el emisor IPsec para asegurar que los datos no han sido alterados durante la transmisión.

c) **Autenticación de origen**: El receptor IPsec puede autenticar el origen de los paquetes IPsec recibidos. Este servicio depende del anterior.

d) **Anti-repetición**: El receptor IPsec puede detectar y rechazar paquetes repetidos.

107. IPsec facilita la creación de túneles seguros entre pares, como dos enrutadores. Los administradores pueden determinar qué paquetes son considerados sensibles y deben ser enviados a través de estos túneles, y especificar los parámetros y características de estos. Cuando un extremo IPsec reconoce un paquete sensible, se establece un túnel seguro y se envía el paquete a través de él.

108. Los túneles seguros son conjuntos de asociaciones de seguridad (SAs) que se establecen entre dos pares IPsec. Las SAs definen los protocolos y algoritmos que se aplican a los paquetes sensibles, así como su material criptográfico. Las SAs son unidireccionales y se establecen por cada protocolo de seguridad (AH o ESP).

109. Con IPsec, los administradores privilegiados pueden definir el tráfico que debe ser protegido entre dos pares IPsec mediante la configuración de listas de acceso y la aplicación de conjuntos de mapas criptográficos a las interfaces. El tráfico se selecciona en función de la dirección de origen y destino, y opcionalmente, del protocolo de capa 4 y el puerto. Las listas de acceso utilizadas por IPsec se usan únicamente para determinar el tráfico que necesita ser protegido por IPsec, no para bloquear o permitir el tráfico a través de la interfaz, para lo cual se usan otras listas de acceso.

110. Se introduce el termino **mapa criptográfico**, el cual hace referencia a un conjunto de:

    - listas de acceso criptográficas
    - uno o más pares IPsec
    - una o más transformaciones o conjunto de transformaciones.

111. Todo esto en conjunto, establece un mapa criptográfico, al cual se hará referencia de aquí en adelante.

112. Un conjunto de mapa criptográfico puede tener varias entradas, cada una con su lista de acceso asociada. El enrutador busca las entradas del mapa criptográfico en una secuencia determinada, intentando encontrar una lista de acceso que coincida con el paquete. Por ejemplo:

    a) La opción *discard* se implementa utilizando listas de acceso con entradas negadas. Estas se aplican a las interfaces dentro de los grupos de acceso.

    b) La opción de *bypass* se lleva a cabo utilizando listas de acceso con entradas denegadas. Estas se aplican a las interfaces dentro de los mapas criptográficos para IPsec.

    c) La opción de *Protecting* se lleva a cabo utilizando listas de acceso con entradas permitidas. Estas se aplican a las interfaces dentro de los mapas criptográficos para IPsec.

113. Cuando un paquete coincide con una entrada permitida en una lista de acceso criptográfica y esta lista de acceso esté asociada a un mapa criptográfico, se establecerán las conexiones. Si la entrada del mapa criptográfico está marcada como *ipsec-isakmp*, se activa IPsec. Si no existe una SA que IPsec pueda utilizar para proteger el tráfico entre los pares, IPsec utiliza IKE para negociar con el par remoto las SA necesarias. La negociación utiliza información específica en la entrada del mapa criptográfico, así como información del flujo de información de la entrada específica en la lista de acceso.

114. Después de establecer el conjunto de SAs, se aplican al paquete en cuestión y a todos los paquetes subsecuentes que salen del enrutador. Por ejemplo, todos los paquetes aplicables a esta configuración podrían ser encriptados antes de ser enviados al receptor remoto.

115. Las listas de acceso asociadas con las entradas del mapa criptográfico de IPsec identifican el tráfico que se debe proteger mediante IPsec. El tráfico entrante es procesado por entradas del mapa criptográfico. Si un paquete no protegido coincide con una entrada permitida en una lista de acceso particular asociada con una entrada del mapa criptográfico de IPsec, el paquete es descartado ya que no fue enviado como un paquete protegido por IPsec.

116. Las entradas del mapa criptográfico también incluyen conjuntos de transformaciones. Un conjunto de transformaciones es una combinación aceptable de protocolos de seguridad, algoritmos y otras configuraciones que pueden ser aplicados al tráfico protegido por IPsec. Durante la negociación de las SAs de IPsec, los pares acuerdan usar un conjunto de transformaciones específico para proteger un flujo de datos en particular.

6.8.2 CONFIGURACIÓN DE IPSEC

117. La configuración de túneles IPsec requiere la configuración de los siguientes elementos:

a) **Interfaces de la capa 3**: Interfaces IP activas que puedan actuar como endpoints de túneles locales.

b) **Listas de acceso criptográficas**: Cualquier lista de acceso aplicada a mapas criptográficos.

c) **Transformaciones de IKEv2:** Parámetros especificados administrativamente como permitidos durante la negociación de SAs de IKEv2. En esta guía no se tendrá en cuenta IKEv1 ya que no está recomendado su uso. La siguiente tabla muestra los parámetros permitidos en este caso.

PROPUESTA FASE 1(IKE)	
Protocolo IKE	IKEv2
Método de autenticación	ECDSA-SIGNATURES-256, ECDSA-SIGNATURES-384
Algoritmo de autenticación	SHA-256, SHA-384
Grupo DH	15, 16, 19, 20, 21 y 24
Algoritmo de cifrado	AES-128-CBC, AES-128-GCM, AES-192-CBC, AES-256-CBC, AES-256-GCM

Tabla 4. Algoritmos permitidos VPN IPSEC - Fase 1

d) **Conjuntos de transformaciones de IKEv2:** Conjuntos de transformaciones para IKEv2 especificados administrativamente y que pueden ser utilizados dentro de mapas criptográficos en lugar de asignar parámetros individualmente.

e) **Transformaciones de IPsec**: Parámetros especificados administrativamente que se acepten como permitidos durante la negociación de SAs de IPsec. La siguiente tabla muestra los parámetros permitidos en este caso.

PROPUESTA FASE 2(IPSEC)	
Protocolo IKE	IKEv2
Algoritmo de autenticación	HMAC-SHA1-96, HMAC-SHA-256-128
Grupo DH	15, 16, 19, 20, 21 y 24
Método de cifrado	ESP
Algoritmo de cifrado	AES-128-CBC, AES-128-GCM, AES-192-CBC, AES-256-CBC, AES-256-GCM

Tabla 5. Algoritmos permitidos VPN IPSEC - Fase 2

f) **Mapas criptográficos:** Como ya se explicó en el párrafo 113, representan una asociación de listas de accesos criptográficas, uno o más pares IPsec (accesibles desde una interfaz de capa 3 permitida), y con una o más transformaciones o conjunto de transformaciones.

118. A continuación, se detallan los pasos para llevar a cabo dichas configuraciones.

119. **Nota**: En el siguiente ejemplo se va a usar una preshared-key como método de autenticación entre extremos del túnel. Se va a optar por esta opción por evitar la complejidad de la solución en el ejemplo, pero siguiendo las directrices indicadas en el CCN-STIC 836, es recomendable el uso de certificados X.509 v3.

6.8.2.1 CONFIGURACIÓN IKEV2 KEYRING

120. El llavero consistirá en unas claves precompartidas, las cuales se van a asociar a un perfil. La autenticación entre extremos se realizará usando estas claves precompartidas, que a su vez estarán dentro del llavero.

```
RT-IOS-XE17-CCN#configure terminal
RT-IOS-XE17-CCN(config)#crypto ikev2 keyring LLAVERO1
RT-IOS-XE17-CCN(config-ikev2-keyring)#peer CCN-Peer-1
RT-IOS-XE17-CCN(config-ikev2-keyring-peer)#address 192.168.10.1
RT-IOS-XE17-CCN(config-ikev2-keyring-peer)#pre-shared-key GuiaCCNXE17
```

6.8.2.2 CONFIGURACIÓN IKEV2 PROPOSAL

121. Una propuesta IKEv2 va a consistir en una propuesta de transformación, la cual será usada en la negociación de los IKE SA. Para poder configurar esta propuesta vamos a necesitar configurar un algoritmo de encriptación, un algoritmo de integridad y un grupo Diffie-Hellman(DH).

```
RT-IOS-XE17-CCN#configure terminal
RT-IOS-XE17-CCN(config)#crypto ikev2 proposal CCN-Site1
RT-IOS-XE17-CCN(config-ikev2-proposal)#encryption aes-cbc-256
RT-IOS-XE17-CCN(config-ikev2-proposal)#integrity sha512
RT-IOS-XE17-CCN(config-ikev2-proposal)#group 24
```

6.8.2.3 CONFIGURACIÓN IKEV2 POLICIES

122. Una política IKEv2 va a contener las propuestas configuradas en el punto anterior, las cuales van a ser utilizadas para definir el algoritmo de encriptación, el algoritmo de integridad y el grupo Diffie-Hellman en el primer intercambio de paquetes(IKE_SA_INIT).

```
RT-IOS-XE17-CCN#configure terminal
RT-IOS-XE17-CCN(config)#crypto ikev2 policy CCN-Site1
RT-IOS-XE17-CCN(config-ikev2-policy)#proposal CCN-Site1
```

6.8.2.4 CONFIGURACIÓN LISTAS DE ACCESO CRIPTOGRÁFICAS

123. Una lista de acceso criptográfica será usada para indicar qué tráfico va a pasar a través del túnel IPSEC y por lo tanto será securizado, y qué tráfico no se enviará por el túnel viajando por tanto sin securizar. Para conseguir este funcionamiento simplemente usaremos las sentencias permit y deny. El tráfico que queramos pasar a través del túnel tendremos que marcarlo con permit, mientras que el tráfico que queramos dejarlo pasar sin securizar tendremos que aplicarle una regla deny.

```
RT-IOS-XE17-CCN#configure terminal
RT-IOS-XE17-CCN(config)#ip access-list extended CCN-Site1-ACL
RT-IOS-XE17-CCN(config-ext-nacl)#permit ip 192.168.100.0 0.0.0.255 192.168.200
0.0.0.255
```

6.8.2.5 CONFIGURACIÓN TRANSFORMACIONES IPSEC

124. En este apartado tenemos que definir de qué manera vamos a encriptar el tráfico que pasará a través del túnel IPsec. Para ello, usaremos los siguientes comandos:

```
RT-IOS-XE17-CCN#configure terminal
RT-IOS-XE17-CCN(config)#crypto ipsec transform-set CCN-Site1 esp-aes esp-
sha512-hmac
RT-IOS-XE17-CCN(cfg-crypto-trans)#mode tunnel
```

6.8.2.6 CONFIGURACIÓN IKEV2 PROFILES

125. Un perfil IKEv2 es un repositorio de los parámetros no negociables de IKE SA, como las identidades locales o remotas y los métodos de autenticación y los servicios que están disponibles para los pares autenticados que coinciden con el perfil. Un perfil IKEv2 debe adjuntarse al mapa criptográfico o Perfil IPSec tanto en el iniciador como en el respondedor IKEv2.

```
RT-IOS-XE17-CCN#configure terminal
RT-IOS-XE17-CCN(config)#crypto ikev2 profile CCN-Site1
```

126. El perfil IKEv2 DEBE tener:

    1. Un método de autenticación local y remoto.

    2. Una identidad de coincidencia o un certificado de coincidencia o cualquier declaración de coincidencia.

```
RT-IOS-XE17-CCN(config-ikev2-profile)#match identity remote address
192.168.10.2 255.255.255.255
RT-IOS-XE17-CCN(config-ikev2-profile)#authentication local pre-share
RT-IOS-XE17-CCN(config-ikev2-profile)#authentication remote pre-share
RT-IOS-XE17-CCN(config-ikev2-profile)#keyring local LLAVERO1
```

6.8.2.7 CONFIGURACIÓN MAPA CRIPTOGRÁFICO

127. El mapa criptográfico será utilizado para unir todos los apartados creados anteriormente. A continuación, se muestra un ejemplo:

```
RT-IOS-XE17-CCN#configure terminal
RT-IOS-XE17-CCN(config)#crypto map CCN-Site1 1 ipsec-isakmp
RT-IOS-XE17-CCN(config-crypto-map)#set peer 192.168.10.2
RT-IOS-XE17-CCN(config-crypto-map)#set pfs group24
RT-IOS-XE17-CCN(config-crypto-map)#set security-association lifetime seconds
28800
RT-IOS-XE17-CCN(config-crypto-map)#set transform-set CCN-Site1
RT-IOS-XE17-CCN(config-crypto-map)#set ikev2-profile CCN-Site1
RT-IOS-XE17-CCN(config-crypto-map)#match address CCN-Site1-ACL
```

128. El máximo tiempo de vida de una SA será de 86400 segundos, pero se recomienda establecerle en 8 horas (28800 segundos).

6.8.3 NAT TRAVERSAL

129. Los elementos con capacidad de traducción de direcciones o NAT (*Network Access Translation*) no son compatibles con los protocolos IPSec por defecto, ya que NAT realiza modificaciones en las cabeceras de los paquetes IP, y los protocolos IPSec protegen los paquetes IP (incluidas las cabeceras) frente a modificaciones.

130. NAT-T, conocido como NAT Transversal, es un estándar diseñado para solucionar la problemática existente entre IPSec y los entornos de NAT. NAT-T emplea por defecto el puerto 4500 para la encapsulación en paquetes UDP, algo que deberá tenerse en cuenta en la configuración de los cortafuegos.

131. En caso de requerir realizar NAT, deberá activarse NAT Traversal. Para realizar un NAT Traversal con éxito en un enrutador IOS-XE NAT, y obtener una conexión IPsec entre dos extremos se debe utilizar la siguiente configuración (Véase también el capítulo “IPsec NAT Transparency” de [15]).

En un enrutador IOS NAT (enrutador entre los extremos IPsec):

```
config terminal
ip nat service list <ACL-number> ESP spi-match
access-list <ACL-number> permit <protocol> <local-range> <remote-range>
end
```

En cada extremo IOS (extremos del enrutador IPsec):

```
config terminal
crypto ipsec nat-transparency spi-matching
end
```

6.8.4 CERTIFICADOS X.509

132. Los administradores privilegiados pueden configurar el enrutador para que utilice certificados X.509 v3 como método de autenticación entre los extremos del túnel IPsec. Para ello, puede utilizar certificados RSA ó ECDSA. La creación de dichos certificados y su carga en el enrutador está descrita en [15].

133. El administrador del enrutador debe verificar el tiempo de vida de estos certificados y mantener un método de revocación de certificados CRL o OCSP.

134. A continuación, se desglosa la configuración del enrutador para el uso de dichos certificados de autenticación. Hay que indicar, que en los siguientes sub-apartados no se incluye toda la configuración a realizar.

6.8.4.1 CREACIÓN DE CLAVES

135. Las claves para un certificado RSA o ECDSA son generadas por pares, una clave pública y otra clave privada. Para generar las claves podemos usar el comando ya comentado en el punto 6.3.1.

136. En el caso de usar RSA, usaremos el siguiente comando:

```
RT-IOS-XE17-CCN(config)#crypto key generate rsa modulus 3072
```

137. Si se desea utilizar ECDSA, tendremos que configurar lo siguiente:

```
RT-IOS-XE17-CCN(config)#crypto key generate ec keysize <256-521>
```

138. Las claves generadas a través de estos comandos serán almacenadas en la NVRAM cuando se ejecute algunos de los comandos usados para salvar la configuración del enrutador. En caso de no guardar los cambios, las claves generadas se perderán en el siguiente reinicio del enrutador.

139. Solamente se puede configurar un par de claves usando el comando “crypto key generate”. Esto implica que, cada vez que se ejecute dicho comando, las nuevas claves sobrescribirán a las anteriores.

140. Para la creación del par de claves, es estrictamente necesario que el enrutador tenga configurado un nombre de dominio. Para ello utilizar el comando “ip domain-name”.

6.8.4.2 CREACIÓN DE SOLICITUD DE FIRMA DE CERTIFICADO

141. La petición de firma de certificados para el enrutador se creará utilizando el par de claves RSA o ECDSA, y el nombre de dominio configurado en el punto anterior.

142. Para generar una petición de firma de certificados, el enrutador debe tener configurado un *hostname y* un *trustpoint.* La realización de estos pasos se hará de la siguiente forma:

- Configuración del hostname:

```
Router#configure terminal
Router(config)#hostname RT-IOS-XE17-CCN
```

- Para la configuración del trustpoint debemos establecer los siguientes puntos:
  - Darle un nombre al trustpoint con el cual lo identificaremos posteriormente.
  - Especificar que método de inscripción contra la CA se va a realizar
  - Indicarle el subject-name que irá en la petición del certificado contra la CA.
  - Especificar el método de revocación que vamos a utilizar.

- Y, por último, crear la petición que se pasará a la CA.

143. Estos serían los comandos a introducir en el enrutador para poder generar esta petición.

```
RT-IOS-XE17-CCN#configure terminal
RT-IOS-XE17-CCN(config)#crypto pki trustpoint CCN-Guia-trustpoint
RT-IOS-XE17-CCN(ca-trustpoint)#enrollment url http://192.168.10.100:80
RT-IOS-XE17-CCN(ca-trustpoint)#subject-name CN=CCN.Guia.IOS.XE17.com, OU=IT
RT-IOS-XE17-CCN(ca-trustpoint)#revocation-check crl
RT-IOS-XE17-CCN(config)#crypto pki enroll CCN-Guia-trustpoint
```

144. Si se desea ampliar la información sobre qué parámetros adicionales se puede configurar, ir a [13].

6.8.4.3 AUTENTICACIÓN DE LA AUTORIDAD DE CERTIFICACIÓN (CA)

145. El enrutador debe autenticar la CA reconociendo que sus atributos concuerdan con la huella pública. El administrador debe verificar que el resultado del comando mostrado a continuación coincide con la huella de la CA en su sitio público.

- Autentificar la CA: crypto pki authenticate trustpoint-name

```
RT-IOS-XE17-CCN#crypto pki authenticate CCN-Guia-trustpoint
El certificado tiene los siguientes atributos:
Huella: 0123 4567 89AB CDEF 0123
% Acepta este certificado? [sí/no]: sí
Certificado AC de trustpoint aceptado.
```

6.8.4.4 ALMACENAR CERTIFICADOS EN EL ALMACENAMIENTO LOCAL

146. Los certificados se almacenan en la NVRAM por defecto. Sin embargo, algunos enrutadores no tienen la capacidad de NVRAM necesaria para almacenar los certificados correctamente. Todas las plataformas Cisco soportan el almacenaje NVRAM y *flash* local. Según la plataforma, un administrador autorizado puede tener otras opciones de almacenaje local soportado, como *bootflash, slot*, disco, *flash USB*, o token USB. Durante el funcionamiento, un administrador autorizado puede especificar qué dispositivo de almacenaje local se utilizará para guardar certificados. Ver [16] para más información.

147. Los pasos resumidos para especificar una ubicación de almacenaje local para los certificados son los siguientes:

- Acceder al modo de configuración del terminal:

```
RT-IOS-XE17-CCN#configure terminal
```

- Especificar la ubicación de almacenaje local para certificados: crypto pki certificate storage location-name

```
RT-IOS-XE17-CCN(config)#crypto pki certificate storage flash:/certificados
```

- Salir:

```
RT-IOS-XE17-CCN(config)#exit
```

- Guardar los cambios realizados:

```
RT-IOS-XE17-CCN#copy system:running-config nvram:startup-config
```

- Mostrar los ajustes actuales para la ubicación de almacenaje de certificados PKI:

```
RT-IOS-XE17-CCN#show crypto pki certificates storage
```

6.8.4.5 CONFIGURACIÓN DEL MECANISMO DE REVOCACIÓN PARA LA VERIFICACIÓN DEL ESTADO DEL CERTIFICADO PKI

148. En la medida de lo posible, se aconseja siempre configurar y mantener un CRL. Para ello, deberá utilizarse el comando ***revocation-check*** que permite especificar al menos un método (OCSP, CRL, o saltar la comprobación de revocación) que debe utilizarse para garantizar que no se haya revocado el certificado de un extremo.

149. Si el enrutador no tiene un CRL aplicado y no pudiese obtenerlo, o si el servidor OCSP devuelve un error, deberá rechazar el certificado del extremo. El enrutador permite la configuración del comando "**crl cache none"**, evitando que se realice la comprobación de revocación de certificados.

```
RT-IOS-XE17-CCN(ca-trustpoint)#crl cache none
```

150. Sin embargo, esta opción no se recomienda y solo se permite su uso cuando dicha comprobación se realice por otros medios.

151. Cuando se utiliza OCSP, se envían *nonces* (identificadores únicos para peticiones de OCSP) por defecto durante comunicaciones de extremos con un servidor OCSP. El uso de *nonces* ofrece un canal de comunicación más seguro y fiable entre el peer y el servidor OCSP. Si el servidor OCSP no soporta *nonces*, un administrador autorizado podrá deshabilitar su envío. Para deshabilitarlo puede utilizar el comando **ocsp disable nonce.**

```
RT-IOS-XE17-CCN(ca-trustpoint)#ocsp disable-nonce
```

6.8.4.6 EDICIÓN MANUAL DE LA CONFIGURACIÓN DEL SERVIDOR OCSP EN UN CERTIFICADO

152. Los administradores pueden invalidar el ajuste del servidor OCSP especificado en el campo "*Authority Information Access (AIA*)" del certificado del cliente, o establecido al enviar el comando ***ocsp url***. Se pueden especificar manualmente uno o más servidores OCSP, ya sea por certificado de cliente o por grupo de certificados de cliente, mediante el comando ***match certificate override ocsp***. Dicho comando invalida el campo AIA del certificado del cliente, o el ajuste del comando ***ocsp url*** si un certificado de cliente coincide correctamente con un mapa de certificado durante la comprobación de revocación.

6.8.4.7 CONFIGURACIÓN DE LA VALIDACIÓN DE LA CADENA DE CERTIFICADOS

153. Para configurar el nivel de profundidad en la ruta de la cadena de certificados de extremos de la comunicación deberán tenerse en cuenta los siguientes prerrequisitos:

- El dispositivo debe estar inscrito en su jerarquía de PKI.

- El par de claves adecuado debe estar asociado con el certificado.

154. Y deberán seguirse los siguientes pasos:

- Acceder al modo de configuración del terminal:

```
RT-IOS-XE17-CCN# configure terminal
```

- Establecer el nombre del crypto pki trustpoint:

```
RT-IOS-XE17-CCN(config)# crypto pki trustpoint CCN-Guia-trustpoint
```

- Validar la cadena de certificados. Para configurar el nivel al que se procesa una cadena de certificados en todos los certificados, incluso los certificados CA subordinados, se utilizará el comando chain-validation [{stop | continue} [parenttrustpoint]]:

```
RT-IOS-XE17-CCN(ca-trustpoint)# chain-validation continue CCN-Guia-trustpoint
```

- Se utilizará la palabra clave *"stop"* para especificar que el certificado ya es de confianza. Este es el ajuste por defecto.
- Se utilizará la palabra clave "*continue*" para especificar que se debe validar el certificado CA subordinado asociado con el trustpoint.
- El argumento *"parent-trustpoint"* especifica el nombre del trustpoint principal contra el que se debe validar el certificado.

6.8.4.8 CONFIGURACIÓIN DE X.509 PARA IKE

155. La utilización de certificados se configurará para IKEv2 mediante los comandos:

```
RT-IOS-XE17-CCN(config)#crypto ikev2 profile CCN-Guia
RT-IOS-XE17-CCN(config-ikev2-profile)#authentication local ?
  ecdsa-sig  ECDSA Signature
  rsa-sig    Rivest-Shamir-Adleman Signature
```

156. y para el remoto:

```
RT-IOS-XE17-CCN(config)#crypto ikev2 profile CCN-Guia
RT-IOS-XE17-CCN(config-ikev2-profile)#authentication remote ?
  ecdsa-sig       ECDSA Signature
  rsa-sig         Rivest-Shamir-Adleman Signature
```

157. El uso de certificados para IKEv2 implica el hecho de que, en caso de que el certificado no sea válido, la autenticación no funcionará.

6.8.4.9 ELIMINAR CERTIFICADOS

158. En caso de necesidad, es posible la eliminación de los certificados que posea el enrutador.

159. Para borrar el certificado de la configuración del enrutador, se pueden utilizar los siguientes comandos en el modo de configuración global:

- Muestra los certificados guardados en el enrutador

```
RT-IOS-XE17-CCN#show crypto pki certificates
```

- Entra en el modo de configuración:

```
RT-IOS-XE17-CCN#configure terminal
```

- Borra el certificado que le pasemos como parámetro:

```
RT-IOS-XE17-CCN(config)#no crypto pki certificate chain  <nombre-certificado>
This will remove all certificates for trustpoint SLA-TrustPoint
Are you sure you want to do this? [yes/no]: y
```

6.8.5 POLÍTICAS DE FLUJO DE INFORMACIÓN

160. Para establecer las reglas de tráfico y las capacidades de VPN, los administradores autorizados pueden configurar listas de acceso y aplicarlas a interfaces que usen sets de acceso y mapas de cifrado. Dependiendo de los requisitos, se pueden usar diferentes opciones:

a) Para descartar el tráfico, se utilizan listas de acceso con entradas de rechazo que se aplican a las interfaces dentro de los grupos de acceso. Para obtener más información sobre la configuración de las políticas de flujo de la información en IOS, consulte la sección "Zone-based Policy Firewalls" o "Zone-Based Policy Firewall IPv6 Support" para IPv6 en [17].

b) Para omitir la protección, se utilizan listas de acceso con entradas de rechazo que se aplican a las interfaces dentro de los mapas de cifrado para IPsec y el comando "filter tunnel" para SSL VPN. Para obtener más información sobre la configuración de las entradas para IPsec, consulte [17].

c) Para omitir la protección, se utilizan listas de acceso con entradas de rechazo que se aplican a las interfaces dentro de los mapas de cifrado para IPsec y el comando "filter tunnel" para SSL VPN. Para obtener más información sobre la configuración de las entradas para IPsec, consulte [17].

161. Las listas de acceso se utilizan para filtrar el tráfico y se basan en la dirección de origen y destino, y, opcionalmente, en la capa 4 y el puerto.

162. Se recomienda registrar el mayor número de eventos posible para un análisis posterior y aplicar el principio de rechazo global en lugar del permiso global.

6.9 CONFIGURACIÓN DEL IDENTIFICADOR DE REFERENCIA

163. Cuando se emplean certificados para tareas de autenticación, se comprueba si el campo DN (distinguished name) es correcto y pertenece a una entidad válida. Los atributos del campo DN del certificado en el equipo son comparados con los atributos esperados y se consideran válidos si son del mismo tipo y valor.

164. El campo FQDN (fully qulified domain name) también puede ser usado para realizar esta comprobación, donde los atributos son comparados con los esperados en la forma CN: FQDN, CN: user FQDN y CN: IP Address.

165. Esta sección describe la configuración del identificador de referencia del extremo, que se consigue configurando los atributos de DN con un mapeo de certificado.

166. Los mapeos de certificado ofrecen la posibilidad de hacer comprobaciones en un certificado dados un conjunto concreto de criterios. Se puede especificar qué campos de un certificado se deben comprobar, y qué valores pueden o no tener dichos campos. Hay seis operadores lógicos para comparar el campo con el valor: igual, no igual, contiene, no contiene, menor que, y mayor o igual que. Los perfiles ISAKMP e IKEv2 pueden unirse a mapeos de certificados, y el enrutador determinará si son válidos durante la autentificación de IKE.

167. Para realizar la configuración de este mapeo, es necesario seguir los siguientes pasos:

- Desde el modo de configuración, acceder a la configuración de mapeo de certificado como se indica a continuación, indicando un nombre para el mapeo y una secuencia para el mismo que debe estar comprendida entre 1 y 65535.

```
RT-IOS-XE17-CCN(config)# crypto pki certifcate map <nombre_mapeo> <secuencia>
```

- Desde la configuración de mapeo, se especifican los campos, criterios y valores que se desean evaluar. Para el campo de fechas, es posible insertar formatos de día-mes-año-hora o mes-día-año, y siempre con el mismo formato para la hora que es de horas:minutos:segundos.

```
RT-IOS-XE17-CCN(ca-certificate-map)# {subject-name | issuer-name |
unstructured-subject-name | alt-subject-name | name | valid-start | expires-
on} {co | eq | nc | ne} <cadena_a_comparar>
RT-IOS-XE17-CCN(ca-certificate-map)# exit
```

- Asociar este mapeo con el perfil de IKEv2

```
RT-IOS-XE17-CCN(config)# crypto ikev2 profile <perfil_IKEv2> match certificate
<nombre_mapeo>
```

6.10 REGISTROS DE AUDITORÍA

168. Cuando ocurre un evento de auditoría, el enrutador puede generar registros de auditoría que se almacenan localmente y se descargan simultáneamente a un servidor syslog externo. La protección de la comunicación se describe en detalle en la Sección 6.3.4.

169. El administrador puede establecer el nivel de los registros de auditoría que se almacenan en un buffer local, se muestran en la consola, se envían al servidor syslog, o todas las opciones. Los detalles para la configuración de estos ajustes se encuentran en la Sección 6.10.1.

170. El buffer de registro local es circular, lo que significa que los mensajes más recientes sobrescriben a los más antiguos cuando el buffer está lleno. Los administradores deben

monitorear el buffer de registro con el comando **show logging privileged EXEC** para ver los registros de auditoría. El primer mensaje mostrado es el más antiguo en el buffer.

171. Cuando se configura la copia de seguridad del syslog, el enrutador descarga eventos de otro buffer al servidor syslog externo simultáneamente. Este buffer se utiliza para encolar eventos que se enviarán al servidor syslog si se pierde la conexión con el servidor. Es un buffer circular, lo que significa que los eventos más antiguos se sobrescriben cuando el espacio de almacenamiento está lleno.

172. La pista de auditoría local comprende los registros de auditoría individuales, un registro de auditoría para cada evento que ocurra. El registro de auditoría puede contener hasta 80 caracteres y un símbolo de porcentaje (%), que aparece tras la información de la marca de fecha.

173. Es importante capturar ciertos eventos de configuración, incluyendo cambios en datos clave secretos, cambios confirmados, inicio y cierre de sesión de usuarios, inicio del sistema, fallos al establecer una sesión de SSH, establecimiento o finalización de una sesión de SSH, cambios en la fecha y hora del sistema, finalización de una sesión remota utilizando el mecanismo de bloqueo de sesiones, finalización de una sesión interactiva y cambios en la configuración del sistema.

6.10.1 CONFIGURACIÓN DE AUDITORÍA

174. Para la configuración de las diferentes opciones de registros de eventos deberán seguirse los siguientes pasos:

175. Habilitar el registro de la ejecución de comandos:

```
RT-IOS-XE17-CCN (config)#archive
RT-IOS-XE17-CCN (config)#no logging console
RT-IOS-XE17-CCN (config-archive)#log config
RT-IOS-XE17-CCN (config-archive-log-cfg)#logging enable
RT-IOS-XE17-CCN (config-archive-log-cfg)#hidekeys
RT-IOS-XE17-CCN (config-archive-log-cfg)#notify syslog
RT-IOS-XE17-CCN (config-archive-log-cfg)#exit
RT-IOS-XE17-CCN (config-archive)#exit
```

176. Habilitar las marcas de tiempo, incluyendo el año:

```
RT-IOS-XE17-CCN (config)# service timestamps log datetime year
RT-IOS-XE17-CCN (config)# service timestamps debug datetime year
```

177. Para generar registros de eventos para inicios de sesión:

```
RT-IOS-XE17-CCN (config)# login on-failure log
RT-IOS-XE17-CCN (config)# login on-success log
```

178. Activar la depuración radius y ssh:

```
RT-IOS-XE17-CCN# debug radius authentication
RT-IOS-XE17-CCN# debug ip ssh
```

179. Los administradores deben tener cuidado al activar estas depuraciones debido a la carga que puede provocar en el enrutador. Activar la depuración relativa a IPsec:

```
RT-IOS-XE17-CCN# debug crypto ipsec
RT-IOS-XE17-CCN# debug crypto ikev2
```

180. Active la depuración de Network Time Protocol (NTP):

```
RT-IOS-XE17-CCN# debug ntp all
```

181. Establecer el tamaño del *buffer*. Es recomendable establecerlo en 150000000 como mínimo:

```
RT-IOS-XE17-CCN (config)# logging buffered <4096-2147483647>
```

182. Configurar que los logs se envíen al servidor syslog:

```
RT-IOS-XE17-CCN (config)# logging host {Hostname | IP address | fqdn | ipv4}
```

183. Para especificar el nivel de severidad de *logging* en el equipo *syslog*, deberá utilizarse el comando ***logging trap***. El nivel 7 enviará todos los logs generados por el enrutador, mientras que el nivel 0 sólo recopilará aquellos que sean de nivel de emergencia (el enrutador no se puede usar en condiciones normales). El comando es:

```
RT-IOS-XE17-CCN (config)# logging trap <0-7>
```

184. Esta opción puede generar un gran número de logs que puede afectar el rendimiento del enrutador, red, y equipo *syslog*, por lo que se debe tener precaución al seleccionar el nivel de syslog que se desea monitorizar.

185. Para configurar el histórico de *syslog*, deberá utilizarse el comando ***logging history*.** El nivel de severidad comprende los rangos del 0 al 7, donde 0 es el nivel más alto y 7 el más bajo. Cuando se especifica un valor, se registran los mensajes de ese valor de severidad y los de números menores en la tabla de histórico del enrutador.

```
RT-IOS-XE17-CCN (config)# logging history <level>
```

186. Para modificar el número de mensajes *syslog* almacenados en la tabla de histórico del enrutador, deberá utilizarse el comando de configuración ***logging history size global***. El rango de mensajes que se pueden almacenar es de 1-500. Cuando la tabla de histórico está llena (significa que se ha alcanzado el número de mensajes establecido por la variable <*number*>), se elimina el mensaje más antiguo de la tabla para registrar el nuevo mensaje.

```
RT-IOS-XE17-CCN (config)# logging history size <number>
```

6.10.2 ELIMINAR REGISTROS DE AUDITORÍA

187. El enrutador proporciona al administrador privilegiado la capacidad de suprimir los registros de auditoría almacenados mediante el comando *"**clear logging**"*.

```
RT-IOS-XE17-CCN#clear logging
Clear logging buffer [confirm]<ENTER>
```

6.11 SERVICIOS DE RED Y PROTOCOLOS

188. La siguiente tabla indica, para cada servicio o protocolo, si puede usarse en la configuración certificada:

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
AH	Authentication Header (part of IPsec)	Yes	Yes	Yes	Yes	No restrictions. ESP must be used in all IPsec connections. Use of AH in addition to ESP is optional. Protocol is not considered part of the evaluation.
DHCP	Dynamic Host Configuration Protocol	Yes	Yes	Yes	Yes	No restrictions. Protocol is not considered part of the evaluation.
DNS	Domain Name Service	Yes	Yes	No	n/a	No restrictions. Protocol is not considered part of the evaluation.
ESP	Encapsulating Security Payload (part of IPsec)	Yes	Yes	Yes	Yes	Configure ESP as described in Section 4.6.2 of this document.
FTP	File Transfer Protocol	Yes	No	No	n/a	Use SCP or HTTPS instead.
HTTP	Hypertext Transfer Protocol	Yes	For OCSP or copy	Yes	No	Used implicitly for OCSP. For other HTTP functions, such as "copy", recommend using HTTPS instead, or tunneling through IPsec. Protocol is not considered part of the evaluation.
HTTPS	Hypertext Transfer Protocol Secure	Yes	Yes	Yes	Yes	No restrictions. Protocol is not considered part of the evaluation.
ICMP	Internet Control Message Protocol	Yes	Yes	Yes	Yes	No restrictions. Protocol is not considered part of the evaluation.

Ilustración 2. Servicios y protocolos permitidos

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
IKE	Internet Key Exchange	Yes	Yes	Yes	Yes	As described in Section 4.6.1 of this document.
IMAP4S	Internet Message Access Protocol Secure version 4	Yes	Over TLS	No	n/a	No restrictions. Protocol is not considered part of the evaluation.
IPsec	Internet Protocol Security (suite of protocols including IKE, ESP and AH)	Yes	Yes	Yes	Yes	Used for securing both traffic that originates from or terminates at the TOE, as well as for "VPN Gateway" functionality to secure traffic through the TOE. See IKE and ESP for usage restrictions.
Kerberos	A ticket-based authentication protocol	Yes	Over IPsec	No	n/a	If used for authentication of TOE administrators, tunnel this authentication protocol secure with TLS or IPsec. Protocol is not considered part of the evaluation.
LDAP	Lightweight Directory Access Protocol	Yes	Over IPsec	No	n/a	Use LDAP-over-SSL instead. Protocol is not considered part of the evaluation.
LDAP-over-SSL	LDAP over Secure Sockets Layer	Yes	Over TLS	No	n/a	If used for authentication of TOE administrators, configure LDAP to be tunneled over IPsec. Protocol is not considered part of the evaluation.
NTP	Network Time Protocol	Yes	Yes	No	n/a	Any configuration. Use of key-based authentication is recommended.
RADIUS	Remote Authentication Dial In User Service	Yes	Yes	No	n/a	If used for authentication of TOE administrators, secure through IPsec.
SDI (RSA SecureID)	RSA SecurID authentication	Yes	Over IPsec	No	n/a	If used for authentication of TOE administrators, secure through IPsec. Protocol is not considered part of the evaluation.
SMTP	Simple Mail Transfer Protocol	Yes	Yes	No	n/a	Recommended to use SMTPS instead. Protocol is not considered part of the evaluation.
SNMP	Simple Network Management Protocol	Yes (snmp-trap)	Yes	Yes	No	Outbound (traps) only. Recommended to tunnel through IPsec. Protocol is not considered part of the evaluation.
SSH	Secure Shell	Yes	Yes	Yes	Yes	As described in the **Error! Reference source not ound.**section of this document.

Ilustración 3. Servicios y protocolos permitidos

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
SSL (not TLS)	Secure Sockets Layer	Yes	No	Yes	No	Use TLS instead. Protocol is not considered part of the evaluation.
Telnet	A protocol used for terminal emulation	Yes	No	Yes	No	Use SSH instead.
TFTP	Trivial File Transfer Protocol	Yes	Yes	No	n/a	Recommend using SCP instead, or tunneling through IPsec. Protocol is not considered part of the evaluation.

Ilustración 4. Servicios y protocolos permitidos

7. FASE DE OPERACIÓN Y MANTENIMIENTO

189. Durante la fase de operación y mantenimiento de los enrutadores, los administradores privilegiados deben llevar a cabo las siguientes tareas de mantenimiento:

    a) Mantenimiento del control de acceso al enrutador. De forma que el personal designado pueda acceder con el rol de usuario asignado.

    b) Comprobaciones periódicas del hardware y software para asegurar que no se ha introducido hardware o software no autorizado.

    c) Verificaciones periódicas del sistema operativo IOS-XE17 y su integridad, para comprobar que está libre de software malicioso. Tal como se especificaba en el epígrafe 5.2, se debe comprobar la integridad de la imagen con el comando ***"show software authenticity file"*** .

    d) Aplicación regular de parches de seguridad, con el objetivo de mantener una configuración segura. Cuando se publiquen actualizaciones, incluyendo PSIRTS (corrección de fallos) de la imagen software, el usuario recibirá un aviso indicando que dichas actualizaciones están disponibles (si ha adquirido la atención continuada), e información sobre cómo descargarlas y verificarlas.

    e) Mantenimiento de registros de auditoría. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos. La información de auditoría se guardará en las condiciones establecidas y por el periodo establecido en la normativa de seguridad. Para más información sobre los registros de auditoría, se recomienda revisar el punto 6.3.4 y 6.10 de la presente guía.

    f) Realización de copias de seguridad automáticas de forma periódica y, a poder ser, de forma centralizada.

7.1 ACTUALIZACIONES Y COMPROBACIONES DE FIRMWARE

190. Los dispositivos enrutadores deben estar protegidos de vulnerabilidades de su propio sistema operativo, para así subsanar posibles fallos de operación detectados tras el uso de dicho sistema operativo. Estas vulnerabilidades y fallos normalmente suelen corregirse a través de liberaciones de actualizaciones de la versión del firmware. El personal encargado y autorizado de la administración de los enrutadores, deberá revisar de forma periódica las actualizaciones que Cisco libere. Las versiones cualificadas se pueden consultar en el CPSTIC.

191. Cisco recomienda una serie de versiones de software en concreto, que se pueden consultar en las "Troubleshooting TechNotes", en la sección "Recommended Releases for Catalyst 8000 Edge, ASR100, ISR4000, CSR1000v and ISR1000 Platforms". Es posible que existan versiones más modernas que la recomendada, pero no significa que sean las más estables. De cualquier modo, es una tarea del personal administrador de los enrutadores el evaluar si es necesario actualizar a versiones superiores (por ejemplo, porque solucione un fallo de operación por el que se vea afectado de forma directa algunas de las características usadas en la configuración del enrutador).

192. Para consultar las versiones disponibles de los enrutadores, se debe realizar a través de la página oficial de Cisco, a través de un navegador Web seguro y consultando la URL "https://software.cisco.com/download/home". En esta página, deberá comprobar el

listado de los equipos, dirigiéndose a "Routers->*Wan Aggregation and internet Edge routers*" por ejemplo. Aparecerá el listado completo de enrutadores y se debe navegar en la familia deseada, seleccionando finalmente el modelo concreto.

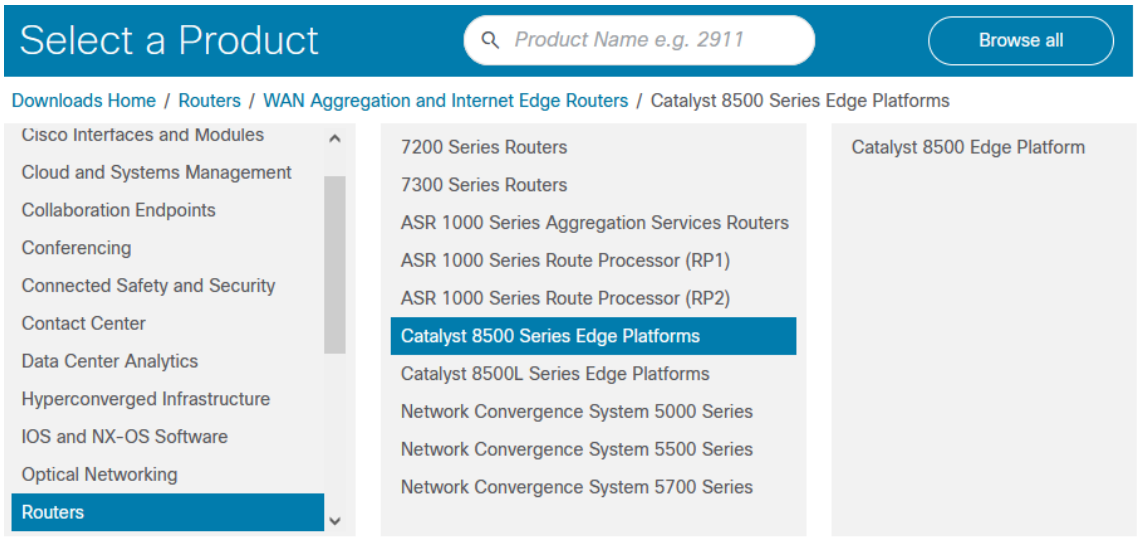


Ilustración 5. Navegación apartado de enrutadores de la web de Software de Cisco

193. También puede usar la herramienta "buscador" que ofrece la misma página web. De cualquier forma, una vez seleccionado el modelo se puede consultar toda la información disponible para el mismo. Se muestra en la siguiente imagen como ejemplo, el resultado de seleccionar el enrutador Catalyst 8500. Para consultar las versiones de firmware disponibles, se debe navegar a la sección "*IOS XE Software*".

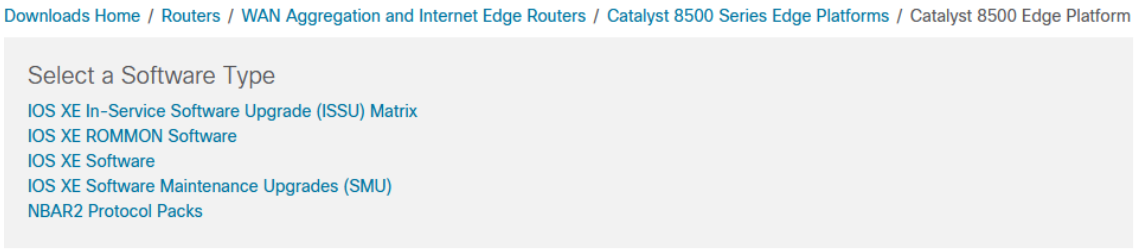


Ilustración 6. Selección de objeto de la descarga

194. El proceso de actualización debe comenzar por un trabajo previo, que consiste en determinar el correcto proceso de actualización, las implicaciones que tiene el mismo y los problemas que corrige la nueva versión de software. Para ello, hay que informarse a través del documento "*Releases Notes*" de la versión a la que se desea migrar. Estos documentos se pueden encontrar en la sección de descarga del software nombrada en el párrafo anterior. En la siguiente imagen, se muestra dónde puede encontrarse este documento para la imagen de software seleccionada, aunque esta ubicación es general para todas:

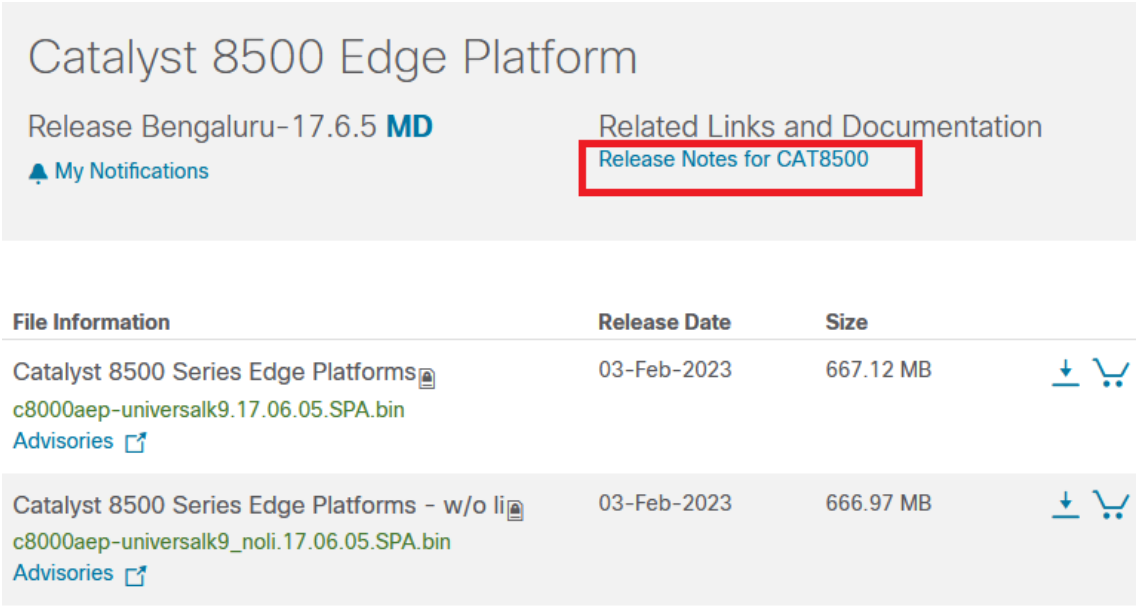


Ilustración 7. Descarga de las "Release notess" de la versión escogida

195. En cuanto al fichero de firmware, se recomienda tras su descarga, comprobar que es el fichero que indica la plataforma, y que no ha sufrido alteraciones. Para ello, se debe comprobar la firma SHA-512 en un equipo confiable de la organización. El valor a obtener debe comprobarse en los detalles del fichero disponible para descargar. Si no coinciden, el proceso de actualización debe detenerse.

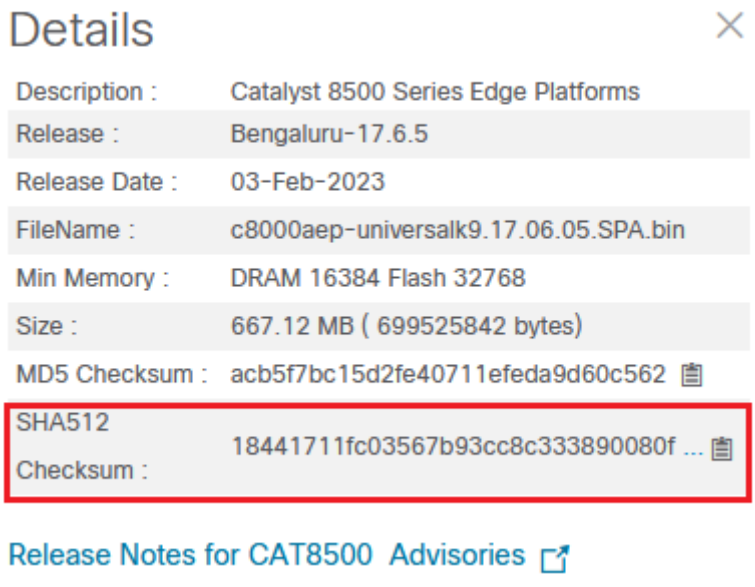


Ilustración 4. Comprobación del hash MD5/SHA512 de la versión de firmware seleccionada

196. Se deben consultar las referencias [5]-[9] para tener detalles precisos del proceso de actualización

8. LISTA DE COMPROBACIÓN

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del enrutador - Serigrafía y logo de Cisco en el embalaje. - Embalaje sellado, sin signos de haber sido manipulado. - Localización de la etiqueta resistente a manipulaciones. - Concordancia entre el número serie embalaje y el enrutador. - Elementos incluidos por defecto en el embalaje.	☐	☐	

Instalación segura
- Ubicación segura del enrutador (control de acceso y anclaje).
- Verificación del software
- Licenciamiento “Smart Licensing”
  ○ *CSSM*(Cisco Smart Software Manager)
  ○ *CSSM a través de CSLU(Cisco Smart License Utility)*
  ○ *CSSM a través de un controlador*
  ○ *Sin conexión hacia el portal de Smart-Licensing*
	☐	☐	

FASE DE CONFIGURACIÓN			
Modo FIPS habilitado	☐	☐	
Configuración de un usuario de administrador privilegiado	☐	☐	
Establecer limite de inactividad	☐	☐	
Bloqueo de usuarios	☐	☐	
Habilitar y configurar SSHv2 y desactivar Telnet	☐	☐	
Configuración de los registros de eventos	☐	☐	
Configurar ACLs necesarias para el filtrado de tráfico	☐	☐	
Configurar política de contraseñas(cifrado, longitud, etc)	☐	☐	
Establecer tiempos máximos de inactividad de sesiones.	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Configurar sincronización horaria.	☐	☐	
Crear perfiles IPSec (futuro uso para SNMP, RADIUS, etc.).	☐	☐	
Creación y administración de certificados	☐	☐	
Limitar usuarios y orígenes que alcanzan el enrutador.	☐	☐	
GUARDADO DE CONFIGURACIÓN Y ACTUALIZACIÓN SOFTWARE			
Guardado de configuración: - Guardar la configuración del enrutador internamente. - Exportar la configuración a un servidor externo, y usar clave de cifrado del fichero.	☐	☐	
Actualizar *software*: - Uso navegador web seguro para consultar periódicamente posibles actualizaciones del fabricante y usar la versión recomendada por el mismo - Prestar atención a la "*Release Note*" de la versión que se desea instalar, en especial al "*upgrade path*" y a compatibilidad con la infraestructura existente. - Descargar versión deseada y comprobar que la firma HASH SHA-512 indicada por el fabricante coincide con el fichero descargado a través de un equipo confiable. - Salvar y extraer configuración del enrutador de forma segura. - Subir el fichero de forma segura con la versión de *firmware* deseada. - Reinicio del enrutador. - Comprobación de la versión en ejecución tras reinicio.	☐	☐	

9. REFERENCIAS

CÓDIGO	REFERENCIA
[1]	*Hardware Installation Guide for Cisco Catalyst 8200 Series Edge Platforms* https://www.cisco.com/c/en/us/td/docs/routers/cloud_edge/c8200/hardware_install/b-cat-8200-series-edge-platforms-hig.html?dtid=osscdc000283
[2]	*Cisco Catalyst 8500 Series Edge Platforms Hardware Installation Guide* https://www.cisco.com/c/en/us/td/docs/routers/cloud_edge/c8500/hardware-installation-guide/b_C8500_HIG/m_Installation.html
[3]	*Configuration Fundamentals Configuration Guide* https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/xe-17/fundamentals-xe-17-book.html
[4]	*Cisco Catalyst 8200 Series Edge Platforms Software Configuration Guide* https://www.cisco.com/c/en/us/td/docs/routers/cloud_edge/c8300/software_config/cat8300swcfg-xe-17-book.html
[5]	*Cisco Catalyst 8500 Series Edge Platforms Software Configuration Guide* https://www.cisco.com/c/en/us/td/docs/routers/cloud_edge/c8500/software-configuration-guide/c8500-software-config-guide.html
[6]	*Smart Licensing Using Policy for Cisco Enterprise Routing Platforms* https://www.cisco.com/c/en/us/td/docs/routers/sl_using_policy/b-sl-using-policy.html
[7]	*Cisco IOS Security Command Reference: Commands A to C* https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-a1-cr-book_CLT_chapter.html
[8]	*Cisco IOS Security Command Reference: Commands D to L* https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/d1/sec-d1-cr-book/sec-d1-cr-book_CLT_chapter.html

CÓDIGO	REFERENCIA
[9]	*Cisco IOS Security Command Reference: Commands M to R* https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/m1/sec-m1-cr-book/sec-m1-cr-book_CLT_chapter.html
[10]	*Cisco IOS Security Command Reference: Commands S to Z* https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-cr-book/sec-s1-cr-book_CLT_chapter.html
[11]	*RADIUS Configuration Guide* https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_rad/configuration/xe-17/sec-usr-rad-xe-17-book.html
[12]	*Embedded Event Manager Configuration Guide, Cisco IOS XE 17* https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/xe-17/eem-xe-17-book/eem-overview.html
[13]	*IP Routing Configuration Guide, Cisco IOS XE 17.x* https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/ip-routing/b-ip-routing.html
[14]	*Basic System Management Configuration Guide, Cisco IOS XE 17* https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bsm/configuration/xe-17/bsm-xe-17-book.html
[15]	*IPsec Data Plane Configuration Guide, Cisco IOS XE 17* https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dplane/configuration/xe-17/sec-ipsec-data-plane-xe-17.html
[16]	*Public Key Infrastructure Configuration Guide* https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-17/sec-pki-xe-17-book.html
[17]	*Security Configuration Guide: Zone-Based Policy Firewall* https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_sec-zone-pol-fw-xe.html

10. ABREVIATURAS

ACL	*Access Control List*
AES	*Advanced Encryption Standard*
AH	*Authentication Header*
AIA	*Authority Information Access*
CA	*Certificate Authority*
CCN	*Centro Criptológico Nacional*
CLI	*Command Line Interface*
CN	*Common Name*
CPD	*Centro de Proceso de Datos*
CPSTIC	*Catálogo de Productos de Seguridad TIC*
CRL	*Certificate Revocation List*
CSLU	*Cisco Smart License Utility*
CSSM	*Cisco Smart Software Manager*
DH	*Diffie-Hellman*
DN	*Distinguished name*
DNA	*Digital Network Architecture*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
EEM	*Embedded Event Manager*
ESP	*Encapsulating Security Payload*
FIPS	*Federal Information Processing Standard*
FQDN	*Fully Qualified Domain Name*
HTTP/S	*Hypertext Transfer Protocol / Secure*
IKE	*Internet Key Exchange*
IP	*Internet Protocol*
IPsec	*Internet Protocol Security*
MACSec	*Media Access Control Security*
MD5	*Message Disgest Algorithm*
NAT	*Network Access Translation*
NAT-T	*Network Access Translation Transversal*
NTP	*Network Time Protocol*
NVRAM	*Non Volatile RAM*
OCSP	*Online Certificate Status Protocol*

PBKDF2	*Password-Based Key Derivation Function 2*
PKI	*Public Key Infrastructure*
PSIRTS	*Product Secruity Inciden Response Team*
RADIUS	*Remote Authentication Dial-In User Service*
RFC	*Request For Comments*
RSA	*Rivest Shamir Adleman*
SA	*Security Associations*
SASE	*Secure Access Service Edge*
SD-WAN	*Software Defined Wide Area Network*
SHA	*Secure Hash Algorithm*
SNMP	*Simple Network Management Protocol*
SSH	*Secure Shell*
TAC	*Technical Assistance Center*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
URL	*Uniform Resource Locator*
VPN	*Virtual Private Network*
VTY	*Virtual Teletype*
WAN	*Wide Area Network*

PUBLICACIONES DE DEFENSA

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