centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1414

Procedimiento de empleo seguro
Router Cisco Systems ISR/ASR

Mayo 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.05.28 16:18:38 +02'00'

NIPO: 083-20-128-9

Fecha de Edición: mayo de 2020

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

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Mayo de 2020

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1 INTRODUCCIÓN

1. Cisco ISR/ASR es una plataforma de enrutamiento que brinda conectividad y servicios de seguridad. Cisco ISR/ASR ejecuta el *software* modular Cisco IOS-XE.
2. En apoyo de las capacidades de enrutamiento, Cisco ISR/ASR proporciona capacidades de conexión IPsec para clientes habilitados para VPN.
3. Además, las familias más recientes de Cisco ISR4K ofrecen aceleración de cifrado y brindan conectividad y servicios de seguridad adicionales.

2 OBJETO Y ALCANCE

4. En la presente guía se recoge el procedimiento de empleo seguro para las familias ISR: 1100, 4000 y 4400 e ASR: 1000 Series.

5. Aunque las distintas familias pueden presentar diferentes opciones de configuración, el presente documento detalla los requisitos mínimos de configuración para el empleo seguro de los productos pertenecientes a las siguientes familias:

Familia	Número Modelo	Identificación externa
Familia ISR 1100	**C1111-8P**	C1111-8P, C1111-8PLTEEA, C1111-8PLTELA, C1111-8PWE, C1111-8PWB, C1111-8PWA, C1111-8PWZ, C1111-8PWN, C1111-8PWQ, C1111-8PWC, C1111-8PWR, C1111-8PWK, C1111-8PLTEEAWE, C1111- 8PLTEEAWB, C1111- 8PLTEEAWA, C1111- 8PLTEEAWR, C1111- 8PLTELAWZ, C1111- 8PLTELAWN, C1111- 8PLTELAWQ, C1111- 8PLTELAWC, C1111- 8PLTELAWK, C1111- 8PLTELAWD
	C1111-4P	C1111-4P, C1111-4PLTEEA, C1111-4PLTELA, C1111-4PWE, C1111-4PWB, C1111-4PWA, C1111-4PWZ, C1111-4PWN, C1111-4PWQ, C1111-4PWC, C1111-4PWR, C1111-4PWK, C1111-4PWD
	C1112-8P	C1112-8P, C1112-8PLTEEA
	C1113-8P	C1113-8P, C1113-8PM, C1113- 8PLTEEA, C1113-8PLTELA, C1113-8PMLTEEA, C1113- 8PWE, C1113-8PWA, C1113- 8PWZ, C1113-8PMWE, C1113- 8PLTEEAWE, C1113- 8PLTELAWE, C1113-8PLTELAWZ
	C1114-8P	C1114-8P, C1114-8PLTEEA
	C1115-8P	C1115-8P, C1115-8PLTEEA
	C1116-4P	C1116-4P, C1116-4PLTEEA, C1116-4PWE
	C1117-4P	C1117-4P, C1117-4PLTEEA, C1117-4PLTELA, C1117-4PWE, C1117-4PWA, C1117-4PWZ, C1117-4PM, C1117-4PMLTEEA, C1117-4PMWE
Familia ISR 4000	**4321**	ISR 4321
	4331	ISR 4331
	4351	ISR 4351
Familia ISR 4400	**4451-X**	CISCO 4451-X
	4431	CISCO 4431
Familia ASR Series	**1001X**	CISCO 1001X
	1001HX	CISCO 1001HX
	1002X	CISCO 1002X
	1002HX	CISCO 1002HX
	1004	CISCO 1004
	1006	CISCO 1006
	1006X	CISCO 1006X
	1009X	CISCO 1009X
	1013	CISCO 1013

Tabla 1- Familias CISCO

3 ORGANIZACIÓN DEL DOCUMENTO

6. El presente documento se divide en tres partes fundamentales, de acuerdo con distintas fases que componen el ciclo de vida del producto:

   a) **Apartado 4**. En este apartado se recogen los requisitos o recomendaciones asociadas a la fase de **despliegue e instalación física** del producto.

   b) **Apartado 5**. En este apartado se recogen requisitos o recomendaciones asociadas a la fase de **configuración** del producto.

   c) **Apartado 6**. En este apartado se recogen requisitos o recomendaciones asociadas a la fase de **operación y mantenimiento**.

4 FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

7. Durante el proceso de entrega deberán llevarse a cabo una serie tareas de comprobación, de cara a garantizar que el producto recibido no se ha manipulado indebidamente:

   a) Antes de desempaquetar el producto, será necesario realizar las siguientes comprobaciones:

   - Inspección del embalaje físico en el que fue entregado. Se verificará que el embalaje de cartón externo está impreso con el logotipo y los motivos de *Cisco Systems*.
   - Verificación que el paquete no ha sido abierto y reempaquetado, examinando la cinta que sella el paquete.
   - Verificación de que la caja tiene la etiqueta blanca a prueba de manipulación, con el código de barras de *Cisco Systems* en la parte externa de la caja de cartón. Dicha etiqueta debe incluir el número de producto de Cisco, número de serie, y otra información relativa al contenido de la caja.
   - Anotación del número de serie del producto indicado en la documentación de envío. El número de serie indicado en la etiqueta blanca adherida al embalaje externo corresponde al del dispositivo. Deberá verificarse que el número de serie de la documentación de envío concuerda con el número de serie en la factura del equipo, enviada por separado.
   - Verificación de que la caja fue enviada por el proveedor del equipo (*Cisco Systems* o un socio / distribuidor autorizado). Esto se puede hacer comprobando que el proveedor envió la caja con la empresa de mensajería que la entregó, y que el número del aviso de envío se corresponde con el indicado en la entrega. También se debe verificar que los números de serie de los artículos enviados corresponden a los de los artículos entregados. La verificación debería llevarse a cabo usando un mecanismo distinto al de entrega, por ejemplo, a través de teléfono, FAX o algún servicio online de seguimiento.
   - En caso de que alguna de las condiciones anteriores no se cumpla, deberá notificarse al proveedor del equipo (*Cisco Systems* o un socio / distribuidor autorizado).

- Una vez desempaquetado el producto, deberá verificarse que el número de serie mostrado en la unidad se corresponda con el número de serie del sello y de la factura y que la identificación externa es la indicada en la Tabla 1. En caso de que alguna de las condiciones anteriores no se cumpla, deberá notificarse al proveedor del equipo (Cisco *Systems* o un socio / distribuidor autorizado).

4.2 INSTALACIÓN SEGURA

8. El producto se envía con las imágenes de software cargadas. No obstante, puede que ésta no sea la versión evaluada, en cuyo caso deberá actualizarse utilizando alguno de los siguientes métodos aprobados:
   - Descargar el archivo de la imagen de software evaluado por *Common Criteria* desde Cisco.com, en un ordenador de confianza.
   - Las imágenes de software están disponibles en la siguiente URL: *http://www.cisco.com/cisco/software/navigator.html*.

9. Una vez descargado el fichero, el administrador deberá verificar que no ha sido modificado antes de instalarlo en el producto, realizando un hash del archivo descargado, y comparándolo con el hash de la imagen indicada en la Tabla 1. Si los hashes no concuerdan, deberá notificarse al CAT (Centro de Asistencia Técnica) de Cisco.

Plataforma	Nombre de imagen	*Hash*
4321	*isr4300-universalk9.16.03.02.SPA.bin*	SHA-256: ***14503889e9ebc7b6d869924d72c8062a1452688bd6e28008bb09f8ebcfd9ff071e9218f4ea1513d3ddb20ba78d4719fbf26714c3ead9393ad4c5566f9c25b929***
4331	*isr4300-universalk9.16.03.02.SPA.bin*	SHA-256: ***14503889e9ebc7b6d869924d72c8062a1452688bd6e28008bb09f8ebcfd9ff071e9218f4ea1513d3ddb20ba78d4719fbf26714c3ead9393ad4c5566f9c25b929***
4351	*isr4300-universalk9.16.03.02.SPA.bin*	SHA-256: ***14503889e9ebc7b6d869924d72c8062a1452688bd6e28008bb09f8ebcfd9ff071e9218f4ea1513d3ddb20ba78d4719fbf26714c3ead9393ad4c5566f9c25b929***
ISR 4451-X	*isr4400-universalk9.16.03.02.SPA.bin*	SHA512: ***1dc73626bb89df16849e35031f8a7eba491087fd533e123787ccf2efc70059aaa06b79f9c93ab7c5ff737d96b334e9efda68ec48022209d86c71edaad583464f***

Plataforma	Nombre de imagen	*Hash*
ISR 4431	*isr4400-universalk9.16.03.02.SPA.bin*	SHA512: ***1dc73626bb89df16849e35031f8a7eba491087fd533e123787ccf2efc70059aaa06b79f9c93ab7c5ff737d96b334e9efda68ec48022209d86c71edaad583464f***
ASR 1001X	*asr1001x-universalk9.16.03.02.SPA.bin*	SHA-512: ***247cdad2a7bc31940f30379999aab3c225748154ed0881273f3ec6dbef3cd5aa36501670022d6941b6525e44d94625a2a714f05a5c56b23b1e0417d935a20c43***
ASR 1001HX	*asr1000-universalk9.16.03.02.SPA.bin*	SHA-512: ***fe2c0c0d3899cfe743872050738fcf06cf17dbfc57dade19769a3f5974cf708f11240673d5f2bef8ef84de6ff59d4b51a9ff8c756758446f0938ae4f837240c2***
ASR 1002X	*asr1002x-universalk9.16.03.02.SPA.bin*	SHA-512: ***1fbd63a356bd7b43cb3f11877e97e882cff78c999b57688ba044fdf4d70ccc0140a5881dc7591dee0a4595e10120c7d10518f7040fbfeeff8ef2ee6167bcb20c***
ASR 1002HX	*asr1000-universalk9.16.03.02.SPA.bin*	SHA-512: ***fe2c0c0d3899cfe743872050738fcf06cf17dbfc57dade19769a3f5974cf708f11240673d5f2bef8ef84de6ff59d4b51a9ff8c756758446f0938ae4f837240c2***
ASR 1004	*asr1000rpx86-universalk9.16.03.02.SPA.bin*	SHA-512: ***69af51342e562cbd874ec65895c8d9082f514169806ef108f027eccd8f129b4c1dc265608bcb9dcbe7086eed123c9921e59866ecf38c5a33d801c11c59367093***
ASR 1006	*asr1000rpx86-universalk9.16.03.02.SPA.bin*	SHA-512: ***69af51342e562cbd874ec65895c8d9082f514169806ef108f027eccd8f129b4c1dc265608bcb9dcbe7086eed123c9921e59866ecf38c5a33d801c11c59367093***
ASR 1006X	*asr1000rpx86-universalk9.16.03.02.SPA.bin*	SHA-512: ***69af51342e562cbd874ec65895c8d9082f514169806ef108f027eccd8f129b4c1dc265608bcb9dcbe7086eed123c9921e59866ecf38c5a33d801c11c59367093***
ASR 1009X	*asr1000rpx86-universalk9.16.03.02.SPA.bin*	SHA-512: ***69af51342e562cbd874ec65895c8d9082f514169806ef108f027eccd8f129b4c1dc265608bcb9dcbe7086eed123c9921e59866ecf38c5a33d801c11c59367093***

Plataforma	Nombre de imagen	*Hash*
ASR 1013	*asr1000rpx86-universalk9.16.03.02.SPA.bin*	SHA-512: ***69af51342e562cbd874ec65895c8d9082f514169806ef108f027eccd8f129b4c1dc265608bcb9dcbe7086eed123c9921e59866ecf38c5a33d801c11c59367093***

Tabla 2 Imágenes binarias

10. El *software* ha sido firmado digitalmente, y la verificación de la imagen se hace con el hash SHA-256 o SHA-512. Una vez la imagen se haya cargado en la memoria *flash*, para mostrar la información relacionada con la autenticidad del software para cada imagen específica, deberá utilizarse el siguiente comando en modo privilegiado:

    Véase [1] -> en *Reference Guides -> Command References -> System Management -> Cisco IOS Configuration Fundamentals Command Reference ->* sección *"show protocols through showmon" ->* Haga clic en el comando *"**show software authenticity file**".*

    El comando "***show software authenticity file***" permite mostrar la información relacionada con la autenticación del *software*, que comprende información de credenciales de la imagen, tipo de clave usado para la verificación, información de la cabecera, y otros atributos de la firma, específicamente para cada imagen. El comando extraerá la cabecera de la firma y sus campos a partir del archivo de la imagen, y volcará la información necesaria.

    *Device# **show software authenticity file** {**bootflash0**:filename |*

    ***bootflash1**:filename | **bootflash**:filename | **nvram:**filename | **usbflash0**:filename |**usbflash1**:filename}*

    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:

    show software authenticity running

11. Para instalar y configurar el *router* de la Familia ISR, es necesario seguir las instrucciones descritas en [2] *Overview – Basic Configuration of a Cisco Networking Device-> Cisco IOS EX Setup Mode.* Según la organización y entorno de red actual, en la sección *"Where to go Next", seleccionar 'Using AutoInstall to Remotely Configure Cisco Networking Device'* o '*Using Setup Mode to Configure a Cisco Networking Device'.*

    Iniciar Router ISR/ASR tal como se describe en [3] [4], y ejecutar los comandos asociados en [5] y [1]. Confirmar que el producto carga la imagen correctamente,

completa las autocomprobaciones internas, y muestra el aviso de exportación criptográfica en la consola.

12. Cuando se haya iniciado el producto, se debe confirmar que está utilizando la versión evaluada. Para ello, es necesario utilizar el comando *"show version"* [5] para mostrar el nombre de archivo de la imagen de sistema en uso, y la versión de lanzamiento del software del sistema. También se recomienda que el nivel de licencia se verifique y active según lo indicado en [4]. Se asumirá que el usuario final ha adquirido una licencia permanente válida para la vida útil del sistema en el que está instalada.

13. Deberán seguirse las instrucciones detalladas en *"Cisco Hardware Installation Guide for the Cisco Integrated Services Routers (ISR)* [6] [7] [8]*"* para la instalación física del dispositivo. Además, el entorno operacional deberá proveer seguridad física, para lo cual deberán tenerse en cuenta los siguientes requisitos:

    a) Los dispositivos deberán instalarse dentro de un Centro de Proceso de Datos (CPD), cuyo acceso estará limitado a un conjunto de personas que posean una autorización expresa.

    b) Para ello, la sala en la que se ubica el CPD estará dotada de un sistema de control que asegure que únicamente dichas personas pueden acceder al dispositivo (incluido fuera del horario laboral).

5 FASE DE CONFIGURACIÓN

5.1 CONFIGURACIÓN INICIAL VÍA *DIRECT CONSOLE CONNECTION*

14. Los *Integrated Services Routers* (ISR) y *Aggregation Service Routers* (ASR) requieren una configuración básica a través de la consola antes de ser conectados a cualquier red.

5.1.1 CONFIGURACIÓN INICIAL DE LOS ROUTERS

15. La instalación se inicia automáticamente cuando un dispositivo no tiene ningún archivo de configuración en NVRAM. Al finalizar, presenta el Diálogo de Configuración del Sistema. Dicho diálogo guía al administrador durante la configuración inicial, con apuntes sobre información básica del producto y la red, y luego crea un archivo de configuración inicial. La *sección 'Performing Basic System Management'* en [9] describe cómo utilizar la Instalación para establecer una configuración básica y realizar cambios en la misma. Durante la instalación, es necesario tener en cuenta:

    a) La cuenta creada durante la instalación inicial del producto se considera el administrador privilegiado, y se le otorga acceso a todos sus comandos.

    b) El término "*administrador autorizado*" se refiere en el presente documento a cualquier administrador que se haya autenticado con éxito en el producto, 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, los roles asociados y los niveles de privilegio descritos en la sección 5.3, tal como se utiliza en el ejemplo anterior [2] [9] [5] [1]. 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 5.4, del presente documento. Este comando garantiza que el ***Enable Password*** no se guarde en texto sin formato. Se configurará el *Enable Secret 5* tal como se indica en:
            - *Cisco IOS Security Command Reference: Commands D to L -> E -> enable secret ->* [5].
            - Se recomienda confirmar esta opción tras completar la configuración inicial, examinando el archivo de configuración y buscando *"enable secret 5".*

- ***Enable Password*** – La contraseña debe ajustarse a los requisitos de complejidad descritos en la sección 5.4, 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 desde:
  - *Cisco IOS Security Command Reference: Commands D to L -> E -> enable password* [5].
- ***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 dispositivo únicamente a través del puerto de la consola. En la sección 5.2.1 se indicarán los pasos a seguir para permitir *ssh* en las líneas *vty (virtual teletype).* La configuración se realizará desde *Password (line configuration)* en *Cisco IOS Security Command Reference*: *Commands M to R -> pac key through port-misuse -> password (line configuration)* [5].
- Deberá configurarse ***SNMP Network Management*** – No (por defecto). Esta opción se puede confirmar tras completar la configuración, examinando el archivo de configuración para garantizar que no hay ninguna entrada *"snmp-server"*. Para garantizar que no hay ningún agente de servidor snmp en funcionamiento, se utilizará el comando 'no *snmpserver*' tal como se indica en *Configuring SNMP -> Disabling the SNMP Agent* [2]. Tenga en cuenta que, en la configuración evaluada, SNMP debería permanecer deshabilitado.

5.1.2 GUARDAR LA CONFIGURACIÓN

16. IOS utiliza una configuración de funcionamiento y una configuración de inicio. Los cambios en la configuración afectan a la configuración de 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'*** o el comando ***'copy system:running-config nvram:startup-config'***.

17. Estos comandos deben utilizarse con frecuencia cuando se realicen cambios en la configuración del *router*. Si el *router* se reinicia y reanuda el funcionamiento cuando hay cambios sin guardar, dichos cambios se perderán y este volverá a la última configuración guardada.

5.1.3 HABILITANDO MODO FIPS

18. El producto debe ejecutarse en modo FIPS. El uso del módulo criptográfico en cualquier otro modo no ha sido evaluado ni testeado durante la evaluación de *Common Criteria*. Para habilitar el modo FIPS se deben establecer los siguientes valores durante la configuración:

19. El valor del campo ***boot*** debe establecerse en 0x0102. Este ajuste deshabilita el comando ***break*** desde la consola al monitor ROM, y carga automáticamente la imagen de IOS. Desde la línea de comandos ROMMON, deberá introducirse el siguiente comando:

    confreg 0x0102

20. Las autocomprobaciones para las funciones criptográficas se realizan automáticamente durante el encendido, como parte de POST. El administrador privilegiado también puede ejecutar manualmente las mismas autocomprobaciones de POST para las operaciones criptográficas en cualquier momento, mediante el comando:

    test crypto self-test

21. Si falla alguna de estas autocomprobaciones, el producto pasa a un estado de error. En dicho estado, se detiene cualquier transmisión de datos segura, y el producto genera información de estado que indica el fallo.

5.1.4 CONFIGURACIÓN DE ADMINISTRADOR Y CREDENCIALES

22. El producto se debe configurar con un nombre de usuario y contraseña para cada administrador con el objeto de garantizar la trazabilidad de las acciones realizadas y controlar el acceso, y una contraseña para el comando "***enable***". Se debe garantizar que todas las contraseñas se almacenen de forma cifrada usando los siguientes comandos:

    Device(config)# ***service password-encryption***

23. Configurar la autenticación local AAA:

    *Device(config)****# aaa authentication login default local***

    *Device(config)****# aaa authorization exec default local***

24. Cuando se crea una cuenta de administrador, todas las cuentas individuales deben ser establecidas a 1 en el nivel de privilegio. El nivel de privilegio determina las funciones que puede realizar el usuario. Están numerados del 0 al 15 y no son necesariamente jerárquicos. El nivel de privilegio 15 tiene acceso a todos los comandos del producto. Para más información sobre los niveles de privilegio, se puede consultar el apartado 5.3.

25. Para realizar esta operación, deberán ejecutarse los siguientes comandos:

    *Device(config)****# username <name> password <password>***

para la creación de un nuevo nombre de Usuario y contraseña, y

*Device(config)****# username <name> privilege 1***

para establecer el nivel de privilegios de <*name*> a 1.

5.1.5 FIN DE SESIÓN

26. Las sesiones de administración deben configurarse para que expiren en caso de inactividad:

    *Device(config)****# line vty <first> <last>***

    *Device(config-line)****# exec-timeout <min> <sec>***

    *Device(config-line)****# line console***

    *Device(config)****# exec-timeout <min> <sec>***

    donde <first> y <last> son el rango de líneas vty (*virtual teletype*) en la caja (i.e. "0 4"), <min> son los minutos y <sec> los segundos de inactividad que deben pasar para que la sesión expire. Este tiempo de inactividad en ningún caso deberá ser superior a 15 minutos. La configuración de estos parámetros está limitada al administrador privilegiado (ver Sección 5.1).

27. Para guardar esta configuración y que se ejecute al iniciar:

    copy run start

28. Esta configuración no se activa inmediatamente para la sesión actual. Debe cerrarse la sesión de consola actual, y cuando se produzca un nuevo inicio de sesión, el tiempo de expiración se activará para la nueva sesión.

5.1.6 BLOQUEO DE USUARIO

29. Las cuentas de usuario se deben configurar para que queden bloqueadas después de un número definido de **intentos fallidos de inicio de sesión que en ningún caso deberá ser superior a 5**. Esto deberá configurarse mediante el siguiente comando.

    *Device(config)****# aaa local authentication attempts max-fail [number of failures]***

30. La configuración de estos parámetros está limitada al administrador privilegiado (ver Sección 5.3) y permite las siguientes funcionalidades adicionales:

Comandos relacionados	
clear aaa local user fail-attempts [username username | all]	Limpia el número de intentos de inicio de sesión de un usuario.
clear aaa local user lockout username [username]	Desbloquea a un usuario bloqueado.

show aaa local user lockout	Muestra una lista de todos los usuarios bloqueados.

Nota: Este bloqueo solo aplica a usuarios con nivel de privilegio 14 o inferior.

Nota: Este bloqueo aplica a intentos consecutivos, y no se ve afectado por desconexiones de sesión SSH después de sus intentos de autenticación. En otras palabras, si el valor está establecido en 5 intentos, y un usuario se desconecta después de 3 intentos fallidos, si el usuario intenta otro inicio de sesión mediante SSH e introduce una contraseña errónea dos veces, la cuenta se bloqueará.

5.2 PROTOCOLOS DE RED Y CONFIGURACIÓN CRIPTOGRÁFICA

5.2.1 PROTOCOLOS DE ADMINISTRACIÓN REMOTA

31. Para la administración remota podrán utilizarse dos protocolos: Telnet o SSH.

32. El servicio de Telnet se encuentra habilitado por defecto para propósitos de configuración y **deberá ser desactivado** para aplicar la configuración recomendada, en la cual solamente estará permitido el uso de SSHv2. Para deshabilitar telnet y permitir solo conexiones SSH para las sesiones remotas de administrador se utilizará el comando ***transport input ssh***.

33. Además, todos los algoritmos criptográficos utilizados por el protocolo SSH deberán cumplir los requisitos establecidos por la guía CCN-STIC-807 para Categoría ALTA, lo que implica una fortaleza criptológica de 128 bits o superior.

5.2.1.1 PASOS PARA CONFIGURAR SSH EN EL ROUTER

34. A continuación, se describen los pasos para configurar SSH en el *router*, para posibilitar la administración remota.

    a) Generación de claves RSA o ECDSA de una longitud de módulo que cumpla con los requisitos establecidos en la CCN-STIC-807 para Categoría ALTA (es decir, 3072 para RSA o superior). Para ello, se utilizarán los siguientes comandos: p. ej.:

    *Device****# crypto key generate ec keysize 256***

    Las claves RSA y ECDSA se generan en pares – una clave pública y otra privada. Este par de claves se guardan en la configuración privada en NVRAM (nunca se muestran al usuario, ni se hace copia de seguridad en otro dispositivo). En caso de que no se guarde la configuración en NVRAM con el comando "***copy run start***", las claves generadas se perderán cuando se vuelva a iniciar el *router*.

Si se desea borrar una clave manualmente, el administrador puede usar el comando ***crypto key zeroize <label>***.

b) Habilitar SSH:

Device ***# ip ssh authentication-retries 2***

c) Configurar – SSH *timeout*:

Device # ***ip ssh time-out 60***

d) Configurar la utilización de SSH v2:

Device # ***ip ssh version 2***

e) Garantizar que el producto está configurado para no soportar el intercambio de clave *diffie-hellman-group1-sha1* o *diffie-hellman-group14* mediante el comando '*ip ssh dh min size 3072'* o mayor:

Device ***# ip ssh dh min size 3072***

Además, es necesario configurar el cliente SSH para *dh-group-exchange.* De este modo, en lugar de usar un grupo fijo, el cliente pregunta al servidor el grupo a usar para el intercambio de claves. Para ello, en *Putty*, deberá configurarse el cliente SSH para soportar únicamente el intercambio de claves *diffie-hellman-group exchange*. Para configurar Putty:

- *Putty Configuration Select > Connection > SSH > Kex;*
- En la sección *Algorithm selection policy*, mover la opción *Diffie-Hellman group exchange* al principio de la lista;

Colocar la opción "*warn below here*" justo debajo de *DH group Exchange.*

f) Configurar las líneas *vty* para aceptar los servicios de acceso 'ssh'

*Device(config-line)****# transport input ssh***

g) Configurar un cliente SSH para que soporte únicamente los siguientes algoritmos de cifrado autorizados:

- *AES-CBC-128:*

  *peer****# ssh -l cisco -c aes128-cbc 1.1.1.1***

- *AES-CBC-256:*

  *peer****# ssh -l cisco -c aes256-cbc 1.1.1.1***

h) Configurar un cliente SSH para que soporte la autenticación de mensaje. Para ello, deberá seleccionarse uno de estos algoritmos MAC (*Message Authentication Code*):

- *hmac-sha1:*

*peer#**ssh -l cisco -m hmac-sha1-160 1.1.1.1***

- *hmac-sha1-96:*

  *peer#**ssh -l cisco -m hmac-sha1-96 1.1.1.1***

i) Para verificar que se utilizan los algoritmos de cifrado adecuados para conexiones establecidas, se utilizará el comando '*show ssh sessions*':

*Device **# show ssh sessions***

Nota: Para desconectar sesiones SSH, se utilizará el comando '*ssh disconnect*':

*Device **# ssh disconnect***

j) Los servidores HTTP y HTTPS no han sido evaluados y deben deshabilitarse:

*Device(config)**# no ip http server***

*Device(config)**# no ip http secure-server***

k) El servidor SNMP no ha sido evaluado y debe deshabilitarse:

*Device(config)**# no snmp-server***

35. Para recuperar la conexión en una situación en la que se haya roto de modo no intencionado, deberán seguirse los pasos mencionados anteriormente para establecer una conexión.

5.2.2 PROTOCOLOS DE AUTENTICACIÓN DE SERVIDOR

36. El uso de servidor RADIUS (salida) para la autenticación remota de los administradores se encuentra deshabilitado por defecto, pero el administrador deberá habilitarlo para cumplir con la configuración recomendada.

37. Para configurar RADIUS deberán utilizarse las mejores prácticas para la selección y protección de la clave descritas en [10], con objeto de garantizar que la clave no se pueda deducir fácilmente y no se comparta con usuarios no autorizados.

38. Cuando se utilicen estos protocolos, la comunicación deberán protegerse estableciendo un túnel IPSec. Las instrucciones para configurar este requisito son las mismas que para proteger las comunicaciones con el servidor *syslog*, detalladas en la sección 5.2.5.

5.2.3 CONFIGURACIÓN DE *LOGGING*

39. Para la configuración de las opciones de *logging* deberán seguirse los siguientes pasos:

40. Habilitar el logging:

*Device (config)**#archive***

*Device (config)**#no logging console***

*Device (config-archive)**#log config***

*Device (config-archive-log-cfg)**#logging enable***

*Device (config-archive-log-cfg)**#hidekeys***

*Device (config-archive-log-cfg)**#notify syslog***

*Device (config-archive-log-cfg)**#exit***

*Device (config-archive)**#exit***

41. Añadir un año al "*timestamp*":

    Device(config)# service timestamps log datetime year

42. Habilitar la depuración cuando se use RADIUS, IPsec, IKEv2, y NTP, para generar los eventos requeridos. Aun así, los administradores deben usarla con discreción cuando habiliten una gran cantidad de depuradores:

    *Device **# debug radius authentication***

    *Device **# debug crypto isakmp***

    AVISO: Aunque la utilización de *isakmp* no está recomendada, se aconseja activar la depuración para sus eventos como medida de seguridad y posible detección de malas configuraciones.

    *Device **# debug crypto ipsec***

    *Device **# debug crypto ikev2***

    *Device **# debug ntp all***

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

    *Device (config)**# logging buffer 150000000***

44. Configurar el equipo para que genere registros por cada intento erróneo o correcto de *login* mediante los siguientes comandos:

    *Device (config)**#login on-failure log***

    *Device (config)**#login on-success log***

45. Configurar que los logs se envíen al servidor *syslog*:

    *Device (config)**#logging host <ip address of syslog server>***

46. 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 requeridos en la evaluación hasta los logs a nivel de depuración (tal como se haya habilitado en el paso 3 más arriba) al servidor *syslog*:

    *Device (config)**# logging trap 7***

AVISO: Esta opción puede generar un gran número de logs que puede afectar el rendimiento del dispositivo, red, y equipo *syslog*.

47. 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 *router*.

    *Device (config)****# logging history <level>***

48. Para modificar el número de mensajes *syslog* almacenados en la tabla de histórico del *router*, 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.

    *Device (config)****# logging history size <number>***

5.2.4 USO DE *EMBEDDED EVENT MANAGER*

49. Para garantizar que todos los comandos ejecutados por un usuario de nivel 15 (ver apartado 5.3 para más información sobre los niveles de privilegio) se guarden en un registro *syslog*, podrá introducirse el siguiente script en el CLI:

    *Switch(config)****#event manager applet cli_log***

    *Switch(config-applet)****#event cli pattern ".*" sync yes***

    *Switch(config-applet)****#action 1.0 info type routername***

    *Switch(config-applet)****#action 2.0 if $_cli_privilege gt "0"***

    *Switch(config-applet)****#action 3.0 syslog msg "host[$_info_routername] user[$_cli_username] port[$_cli_tty] exec_lvl[$_cli_privilege] command[$_cli_msg] Executed"***

    *Switch(config-applet)****#action 4.0 end***

    *Switch(config-applet)****#action 5.0 set _exit_status "1"***

    *Switch(config-applet)****#end***

    Para más información sobre EEM scripting, consultar: *https://supportforums.cisco.com/community/netpro/network-infrastructure/eem*

5.2.5 PROTECCIONES DE *LOGGING*

50. Si un administrador autorizado desea realizar una copia de los logs al servidor *syslog*, se deben proteger las comunicaciones con el servidor *syslog*. Esta acción se puede realizar de dos (2) maneras:

    a) Con un servidor *syslog* que funcione como extremo IPsec del producto, y los registros se envíen a través de ese túnel sobre esa conexión,

    o

    b) Con un servidor *syslog* que no esté ubicado directamente junto al producto, pero sea adyacente a un *peer IPsec* dentro de una instalación de confianza, y los registros tunelados sobre la red pública.

5.2.5.1 *SYSLOG SERVER* EJECUTÁNDOSE EN UN *IPSEC ENDPOINT*

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

52. Puede verse un ejemplo de configuración del producto para soportar un túnel IPsec con cifrado AES de este modo en los documentos de configuración [3] [4] específicos para las familias ISR 1100/4000 sección 3.3.5.1.

5.2.5.2 SYSLOG SERVER ADYACENTE A UN *IPSEC PEER*

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

54. Puede verse un ejemplo de configuración del producto para soportar un túnel IPsec con cifrado AES de este modo en los documentos de configuración [3] [4] específicos para las familias ISR 1100/4000 sección 3.3.5.1.

5.2.6 CONFIGURACIÓN BASE DE *FIREWALL RULE SET*

55. Un administrador autorizado privilegiado podrá manipular los ACLs utilizando los comandos ***ip inspect***, ***access-list***, ***ctypto map***, y ***access-group***, tal como se describe en [5].

56. Las listas de acceso deben configurarse en el producto cumpliendo las siguientes directrices:

    Los dispositivos situados fuera de la red protegida pueden tratar de llevar a cabo servicios que están pensados para que se acceda solo desde la red protegida, o por entidades que utilicen una ruta de autenticación para entrar a dicha red protegida. Del mismo modo, los dispositivos situados fuera de la red protegida podrían ofrecer servicios a los que no es adecuado acceder desde la red protegida.

Desde una perspectiva de acceso, las pasarelas VPN se pueden configurar para que únicamente sean accesibles los servidores de red pensados para el consumo externo por parte de entidades que operan en una red fiable, y únicamente mediante unos puertos concretos.

Finalmente, desde una perspectiva de salida, las pasarelas VPN se pueden configurar para que, desde una red protegida, solo se pueda acceder a algunos servicios externos concretos, o incluso que se acceda a ellos mediante un canal cifrado.

Nota: dichas listas de acceso deben estar integradas en la política de seguridad definida para el *router*. Si se habilitan únicamente dichas listas de acceso sin permisos, se descartará el tráfico. Deberá asegurarse que las entradas de la lista de acceso se insertan sobre el '***deny acl***' por defecto.

57. Deberá tenerse en cuenta que la interfaz *GigabitEthernet0/0* es la interfaz externa, y se le asigna una dirección IP de 10.200.1.1. La interfaz *GigabitEthernet0/1* es la interfaz interna, y se le asigna una dirección IP de 10.100.1.1.

58. Si se requiere administración remota, debe permitirse explícitamente SSH, ya sea mediante la interfaz interna o la externa.

    Device ***# configure terminal***

    Introducir los comandos de configuración, uno por línea y terminar con CNTL/Z.

    *Device (config)****# access-list 199 permit tcp host 10.200.0.1 host 10.200.0.1 eq 22 log-input***

59. Para registrar conexiones en la Autoridad de Certificado, deberá implementarse el siguiente acl:

    *Device(config)****# access-list 100 permit ip any host [IP of CA] loginput***

    *Device(config)****# access-list 199 permit ip any host [IP of CA] loginput***

60. Todos aquellos puertos que no vayan a ser utilizados deberán cerrarse, dado que podrían introducir vulnerabilidades adicionales Para ello, se implementará el siguiente acl:

    *Device (config)****# access-list 100 deny 132 any any log-input***

    *Device (config)****# access-list 199 deny 132 any any log-input***

61. Deberá crearse de forma explícita el '*deny acl*' por defecto sin otras coincidencias, mediante los siguientes comandos:

    *Device (config)****# access-list 100 deny any any log-input***

    *Device (config)****# access-list 199 deny any any log-input***

Nota: detener todo el tráfico que llega al *'deny acl'* por defecto puede generar una gran cantidad de registros, y se debe determinar si es necesario antes de añadirlo al final de todas las listas de acceso.

62. Una vez creados los ACLs, deberán aplicarse a las interfaces:

*Device (config)****# interface GigabitEthernet0/0***

*Device (config-if)****# ip access-group 199 in***

*Device (config)****# interface GigabitEthernet0/1***

*Device (config-if)****# ip access-group 100 in***

Para más información sobre la creación del filtrado de paquetes, y políticas de flujo de información VPN, consultar la Sección 5.5.4.

5.2.7 PROTOCOLOS DE ENRUTAMIENTO

63. Los protocolos de enrutamiento se usan para mantener las tablas de enrutamiento. Las tablas de enrutamiento se pueden configurar y mantener manualmente. En la secciones que aplican de [2] *Configuration Fundamentals* se muestra la configuración de los protocolos de enrutamiento.

64. Adicionalmente, durante la configuración de protocolos de enrutamiento hay que considerar los puntos descritos en:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xe-16/macsec-xe-16-book/wan-macsec-mka-support-enhance.html#d74e990a1635

5.3 ROLES DE USUARIO

65. El equipo se configurará de acuerdo a los principios de mínima funcionalidad y mínimo privilegio. Es decir, los usuarios administradores deben ser los mínimos posibles y el conjunto de usuarios en general no debe disponer de más privilegios que los que necesita.

66. El acceso privilegiado se define como cualquier nivel de privilegio que introduzca un ***'enable secret 5'*** tras su conexión individual. El comando '*enable secret*' *es* un reemplazo del comando '*enable password*', ya que el '*enable secret*' crea la contraseña y la almacena cifrada.

67. Los niveles de privilegio de los usuarios están numerados del 0 al 15 y no son necesariamente jerárquicos. El nivel de privilegio 15 tiene acceso a todos los comandos del producto. Los niveles 0 y 1 están definidos por defecto, mientras que los niveles 2-14 no lo están. Los niveles 0-14 se pueden ajustar para que comprendan cualquiera de los comandos disponibles al administrador de nivel 15. El nivel de privilegio determina las funciones que puede realizar el usuario; por ello existe el administrador autorizado con los privilegios adecuados.

68. Para establecer un sistema de autenticación según el nombre de usuario, deberá utilizarse el comando '*username*' en el modo de configuración global.

    *Device (config)****# username name [privilege level]***

69. Cuando un usuario ya no necesite acceso al producto, deberá eliminarse su cuenta. Para eliminar una cuenta establecida con autentificación según el nombre de usuario, se utilizará la forma "no" del comando.

    *Device (config)****# no username name***

70. Para ver todos los comandos disponibles, así como los roles asociados y los niveles de privilegio puede consultarse la *Guía de Referencia de Comandos de IOS.*

5.4 CONTRASEÑAS

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

    a) Deberán ser fáciles de recordar, de modo que los usuarios no se sientan tentados a escribirlas. En caso de que sea necesario guardar una copia física de la contraseña, se hará en un contenedor seguro.

    b) Deberán ser privadas y no compartirse con nadie.

    c) Deberán cambiarse periódicamente, con un período establecido en los procedimientos operativos de seguridad del sistema.

    d) No deberá permitirse la repetición de al menos las 5 últimas contraseñas utilizadas.

    e) No deberá realizarse un nuevo cambio de contraseña en los 4 días posteriores al último cambio.

    f) Deberán ser de 12 caracteres como mínimo, aunque se recomienda utilizar 15 caracteres.

       *Device (config)****# security passwords min-length <length>***

    g) Deberán incluir al menos 3 variantes de estas 4: caracteres alfanuméricos y caracteres especiales como "!", "@", "#", "$", "%", "^", "&", "*", "(" y ")", mayúsculas, minúsculas y números. Podrá forzarse esta complejidad con el comando:

       *Device (config)****# aaa password restriction***

       Se recomienda habilitar el comando "***aaa password restriction***", para que las siguientes restricciones también sean vigentes:

- La nueva contraseña no puede tener ningún carácter repetido más de tres veces consecutivas.
- La nueva contraseña no puede tener el mismo valor que el nombre de usuario.
- No se aceptarán contraseñas que sean el nombre de usuario al revés o con mayúsculas.
- La nueva contraseña no puede ser "*cisco*", "*ocsic*", ni ninguna otra variante obtenida al sustituir alguna de estas letras por su versión en mayúscula, símbolos o números.

h) Nota: El comando "***aaa password restriction***" solo se puede usar después del comando "***aaa new-model***". El uso de caracteres de control en las contraseñas no está recomendado.

i) Además, son contraseñas poco recomendables:

- Cadenas que contengan 3 o más caracteres consecutivos.
- Las palabras que puedan estar en o que existan como forma permutada en un archivo de sistema, como */etc/passwd.*
- El nombre de host del sistema (siempre lo primero que se intenta).
- Cualquier palabra que aparezca en un diccionario, incluidos también diccionarios de otros idiomas distintos al inglés o al castellano, palabras que puedan aparecer en obras de autores famosos, palabras y frases habituales del mundo de los deportes, dichos, películas y series televisivas, nombres propios etc.
- Permutaciones de todo lo anterior. Por ejemplo, una palabra del diccionario cuyas vocales se hayan sustituido por números (por ejemplo, *f00t*) o a la que se añadan números al final.
- Palabras generadas por máquinas. Los algoritmos reducen el espacio de búsqueda de los programas de adivinación de contraseñas, por lo que no conviene usarlos.

72. Las contraseñas administrativas o cualquier contraseña "*enable*" que se establezca para cualquier nivel de privilegio, no deben guardarse en texto sin formato. Para guardar contraseñas en formato hash SHA-256, deberá utilizarse el comando "***service password-encryption***" en el modo de configuración.

*Device (config)****#service password-encryption***

73. Una vez habilitado este servicio, las contraseñas se podrán introducir en texto sin formato, o como valores de hash SHA-256, y se guardarán como valores de hash

SHA-256 en el archivo de configuración cuando se utilice el comando "***username***".

*Device (config)****#username name {password password | password encryptiontype encrypted-password}***

74. Esté o no habilitada la "***service password-encryption***", se puede introducir una contraseña para un nombre de usuario individual como texto sin formato o como valor hash SHA-256, y guardarla como valor hash SHA-256, mediante el siguiente comando:

    *Device (config)****#username name secret {0 password | 4 secret-string | 5 SHA256 secret-string}***

75. En vez de utilizar el comando '***enable password***', deberá utilizarse el comando '***enable secret***' ya que guarda un valor hash SHA-256 de la contraseña.

76. Para almacenar claves IKE pre-compartidas en modo cifrado, se utilizará el comando '***password encryption aes***' para permitir la funcionalidad, y el comando '***key config-key password-encrypt***' para establecer la contraseña maestra que se deberá utilizar para cifrar las claves pre-compartidas. Dichas claves se almacenarán cifradas con el cifrado simétrico *Advanced Encryption Standard [AES].*

    *Device (config)****# password encryption aes***

    *Device (config)****# key config-key password-encryption [text]***

5.5 CONFIGURACIÓN DEL RELOJ

77. La configuración del reloj está restringida al administrador privilegiado.

    Para configurar el reloj, se consultará [11] en *Configure -> hacer clic en Configuration Guides -> Network Management* -> hacer clic en *Network Management Configuration Guide Library* -> en la sección *"Basic System Management Configuration Guide"-> "Setting Time and Calendar Services".*

78. Esta sección contiene información para establecer el reloj local (*hardware*) o fuentes NTP. Cuando se configura NTP, el tiempo se sincroniza con un servidor NTP mediante NTPv3. NTP corre sobre UDP, que a su vez corre sobre el protocolo IP. Para más información sobre NTP Versión 3 (NTPv3), consulte el RFC 1305.

5.6 IDENTIFICACIÓN Y AUTENTICACIÓN

79. La configuración de identificación y autenticación está restringida al administrador privilegiado. Los *routers* ISR se pueden configurar para que utilicen alguno de los siguientes métodos de autentificación:

    a) Autentificación remota (RADIUS).

- Ver apartado 5.2.2 PROTOCOLOS DE AUTENTICACIÓN DE SERVIDOR este documento para más información.

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

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

c) Certificados X.509v3.

- Ver apartado 5.7.5 CERTIFICADOS X.509 de este documento para más información.

5.7 VIRTUAL PRIVATE NETWORKS (VPN)

80. El producto permite a los administradores privilegiados configurar el establecimiento de VPN IPsec, para proporcionar los siguientes servicios de seguridad de red:

a) Confidencialidad de los datos—IPsec puede cifrar los paquetes a enviar antes de transmitirlos a través de una red.

b) Integridad de los datos—IPsec puede autenticar paquetes enviados por el transmisor IPsec para garantizar que no se modifiquen los datos durante la transmisión.

c) Autenticación de los datos de origen—IPsec puede autenticar la fuente de origen de los paquetes de datos. Este servicio depende del servicio de integridad de los datos.

d) *Anti-replay*—El receptor IPsec puede detectar y descartar paquetes reenviados.

5.7.1 CONSIDERACIONES GENERALES PARA ESTABLECIMIENTO DE VPN IPSEC

1. Todas las VPN deberán configurarse de forma que se utilicen algoritmos de cifrado con una fortaleza criptológica de 128 bits o superior, de acuerdo con lo estipulado en la guía CCN-STIC-807 para el ENS Categoría ALTA.
2. Para ello, como regla general, deberán aplicarse las siguientes restricciones a las opciones de configuración que presenta el producto:

a) **Se seleccionará siempre IKEv2** en lugar de IKEv1 como protocolo de intercambio de claves. De hecho, el producto permite la utilización de IKEv1, que no se ha incluido en esta guía, dado que no es la configuración recomendada.

b) Para la autenticación extremo a extremo el producto permite utilizar certificados x509v3 o claves pre-compartidas (PSK) Por regla general, **no deberán utilizarse claves-precompartidas como método de autenticación,**

salvo que sea posible determinar *a priori* si la clave posee la fortaleza exigida.

c) No deberá utilizarse RSA-2048 como método de autenticación, dado que posee una fortaleza de 112 bits, por lo que incumple los requisitos mínimos establecidos. Solamente se permitirá el uso del RSA-2048 cuando la VPN se establezca dentro de la red local para ofrecer un canal seguro con el administrador remoto o el servidor de autenticación.

d) No deberá seleccionarse el grupo *Diffie Hellman* 14 (*DH group-14*) o inferiores para el establecimiento de secretos compartidos en la fase de intercambio de claves, dado que poseen una fortaleza menor de 128 bits.

e) No deberá seleccionarse *3des-cbc* como algoritmo de cifrado, dado que posee una fortaleza igual a 112 bits.

f) Deberá activarse la opción ***perfect-forward-secrecy*****,** ya que, **aunque supone incrementos en coste computacional,** impide que se descifre el contenido de la comunicación, aunque se comprometan las claves establecidas para las asociaciones de seguridad.

g) El tiempo de vida máximo recomendado para cada asociación e seguridad dependerá de las exigencias de cada aplicación y será inversamente proporcional al grado de clasificación o sensibilidad de la información que va a transmitir. A mayor frecuencia de renovación de claves mayor seguridad, aunque es necesario tener en cuenta posibles limitaciones impuestas por el tamaño de la red o el ancho de banda con el que se trabaja.

h) El tiempo de vida de las asociaciones de seguridad del protocolo ESP no deberá ser mayor que el de las de IKE y, en general, se recomiendan valores inferiores a 4 horas para las primeras e inferiores a 24 h para las segundas.

i) La siguiente tabla muestra una lista completa de los protocolos, modos, algoritmos y fortaleza de claves recomendados para una configuración segura de VPN:

PROPUESTA EN FASE 1 (P1, IKE)	
Protocolo IKE	IKEv2
Método de autenticación	ECDSA-SIGNATURES-256, ECDSA-SIGNATURES-384
Algortimo de autenticación	SHA-256, SHA-384
Grupo DH	19, 20, y 24

PROPUESTA EN FASE 1 (P1, IKE)	
Algortimo de cifrado	AES-128-CBC, AES-128-GCM, AES-192-CBC, AES-256-CBC, AES-256-GCM

Tabla 3 - Algoritmos permitidos para una VPN

PROPUESTA EN FASE 2 (P2, IPSEC)	
Protocolo IKE	IKEv2
Algortimo de autenticación	HMAC-SHA1-96, HMAC-SHA-256-128
Grupo DH	19, 20, y 24
Método de cifrado	ESP
Algortimo de cifrado	AES-128-CBC, AES-128-GCM, AES-192-CBC, AES-256-CBC, AES-256-GCM

Tabla 4 - Algoritmos permitidos para una VPN

5.7.2 CONFIGURACIÓN DE IPSEC

5.7.2.1 CONFIGURACIÓN DE IKEV2

81. IKEv2 es el protocolo utilizado por IPSec para el intercambio de claves entre extremos. Para configurar IKEv2, deberán seguirse los siguientes pasos:

82. Establecer IPsec para utilizar AES-CBC-256 para el cifrado del *payload.* Si es necesario por compatibilidad, podrá utilizarse AES 128, pero no otro de seguridad inferior. (Véase tabla Tabla 2 - Algoritmos permitidos para una VPN y Tabla 3 - Algoritmos permitidos para una VPN):

    Device ***# conf t***

    *Device (config)****#crypto ikev2 proposal sample***

    *Device (config-ikev2-proposal)****# integrity sha256***

    No deberá utilizarse *md5* ni *sha-1* para la configuración recomendada.

    *Device (config-ikev2-proposal)****# encryption aes-cbc-256***

83. El administrador autorizado deberá asegurarse de que el tamaño de clave para este parámetro es mayor o igual que el tamaño seleccionado para el ESP en la Sección 5.7.3.

84. Configurar el algoritmo de autenticación. El siguiente comando configura IPsec para que utilice criptográfica asimétrica en lugar de claves pre-compartidas, las cuales no se recomiendan. Los certificados X.509 v3 también están soportados para la autenticación de los extremos IPsec. Véase Sección 5.5.4 para más información.

*Device (config-ikev2-proposal)**# authentication ecdsa-sig***

85. Este comando selecciona DH Group 19 (*256-bit Random ECP*) para IKE, pero también se permiten, y están soportados: 20 (*384-bit Random ECP*), 15 (*3072 bit MODP*), y 16 (*4096-bit MODP*).

    *Device (config-ikev2-proposal)**# group 19***

86. Para establecer la frecuencia de renovación de claves:

    *Device (config-ikev2)**# lifetime[1] seconds 86400[2]***

87. Esta opción habilita los mensajes *syslog* IKEv2.

    La configuración presentada más arriba no es una configuración completa para IKEv2, y requiere parámetros adicionales, ver [12] *Configuring Internet Key Exchange Version* 2 (IKEv2) para terminar la configuración.

    *Device (config)**# crypto logging ikev2***

5.7.3 CONFIGURACIÓN DE ESP Y TIEMPOS DE VIDA DE LAS ASOCIACIONES DE SEGURIDAD IPSEC

88. A continuación, es necesario configurar los algoritmos de cifrado e integridad IPsec ESP, así como los parámetros de *IPsec lifetime*. Para ello, se seguirán los siguientes pasos:

    Establecer los algoritmos de autenticación de mensajes y cifrado de datos:
    *Device (config)**# crypto ipsec transform-set example esp-aes 128 espsha-hmac***

    Este ejemplo configura ESP para que utilice *HMAC-SHA-1* y *AES-CBC-128*. Para cambiar esta configuración a otros algoritmos permitidos, debe reemplazarse '*espaes128'* por: *esp-aes 256, esp-gcm 128, esp-gcm 256.*

    El tamaño de la clave seleccionada aquí debe ser menor o igual al de la clave seleccionada para la configuración de cifrado de IKE. Si en dichos puntos se ha seleccionado *AES-CBC-128* para utilizarlo con la encriptación de IKE, entonces en este punto solo se puede seleccionar *AES-CBC-128* o *AES-GMC-128*.

89. **Configurar explícitamente el modo túnel para IPsec**. Este modo está configurado por defecto, pero al configurarlo explícitamente, el *router* pedirá y únicamente aceptará dicho modo.

    *Device(config-crypto)**#mode tunnel***

90. Establecer los tiempos de vida de las asociaciones de seguridad. Estos tiempos se expresan en segundos o en kilobytes, de forma que el primero que se cumpla forzará una renovación de claves:

    *Device (config)**#crypto ipsec security-association lifetime seconds 14400[3]***

[1] El tiempo de vida de estas asociaciones de seguridad no deberá ser mayor de 24 horas (86.400 s.)
[2] El tiempo de vida de estas asociaciones de seguridad no deberá ser mayor de 24 horas (86.400 s.)

*Device(config)**#crypto ipsec security-association lifetime kilobytes 100000***

91. Ver [5] para más información sobre la configuración de IPsec. Los comandos IPSEC se encuentran repartidos dentro de las Referencias de Comandos de Seguridad. Esta funcionalidad junto con la configuración de ajustes de la VPN está disponible para el Administrador Privilegiado.

5.7.4 NAT TRAVERSAL

92. 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.

93. 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.

94. En caso de requerir realizar NAT, deberá activarse NAT Transversal. Para realizar un NAT Traversal con éxito en un dispositivo IOS-XE NAT, y obtener una conexión IPsec entre dos extremos se debe utilizar la siguiente configuración (Véase también el Capítulo 7 de [12]).

En un dispositivo IOS NAT (*router* 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 router IPsec):

config terminal

crypto ipsec nat-transparency spi-matching

end

5.7.5 CERTIFICADOS X.509

95. Los administradores privilegiados pueden configurar el producto para que utilice certificados X.509v3 para autenticar extremos IPsec. Tanto los certificados RSA como ECDSA están soportados. La creación de dichos certificados y su carga en el producto está descrita en [13]. A continuación, se muestra una parte de la configuración del producto para usar dichos certificados. Es importante que el

[3] El tiempo de vida de estas asociaciones de seguridad no deberá ser mayor de 4 horas (14.400 s.)

administrador considere el tiempo de vida de los certificados y se mantenga una lista de revocación de certificados (CRL).

5.7.5.1 CREACIÓN DE SOLICITUD DE FIRMA DE CERTIFICADO

96. La petición de firma de certificados para el producto se creará utilizando el par de claves RSA o ECDSA, y el nombre de dominio configurado en la sección 5.2.1.

97. Para generar una petición de firma de certificados, se debe configurar el producto con un *hostname* y un *trustpoint*, de la siguiente forma:

a) Acceder al modo de terminal de configuración:

Device ***# configure terminal***

b) Especificar el hostname: ***hostname name***

*Device(config)****# hostname asrTOE***

c) Configurar el trustpoint: ***crypto pki trustpoint trustpoint-name***

*Device (config)****#crypto pki trustpoint ciscotest***

d) Configurar un método de inscripción: ***enrollment [terminal, url url]***

*Device (ca-trustpoint)****#enrollment url http://192.168.2.137:80***

e) Configurar los ajustes de *subject-name* para el certificado: ***subject-name CN=hostname.domain.com,OU=OU-name***

*Device (ca-trustpoint)****#subject-name CN=asrTOE.cisco.com,OU=TAC***

f) Establecer el método de comprobación de revocación: ***revocation-check crl***

*Device (ca-trustpoint)****#revocation-check crl***

*Device (ca-trustpoint)****#exit***

g) Crear la petición de firma de certificado: ***crypto pki enroll trustpoint-name***

*Device (config)****#crypto pki enroll ciscotest***

5.7.5.2 CONECTARSE DE FORMA SEGURA A UNA AUTORIDAD DE CERTIFICACIÓN (AC) PARA LA FIRMA DE CERTIFICADOS

98. El producto debe comunicarse con la AC para la firma de certificados sobre IPSec.

99. A continuación, se muestra un ejemplo de como configurar el dispositivo para que soporte un túnel IPsec con cifrado AES, con 10.10.10.102 como IP del extremo IPsec en la AC, y 10.10.10.110 como IP local del dispositivo.

Device ***#configure terminal***

*Device (config)****#crypto ikev2 policy <policy-name>***

*Device (config-ikev2)**#encryption aes***

*Device (config-ikev2)**#authentication [local | remote] ecdsa-sig***

*Device (config-ikev2)**#group 19***

*Device (config-ikev2)**#lifetime seconds 86400***[4]

*Device (config)**#crypto ikev2 enable outside***

*Device (config)**#crypto ipsec ikev2 ipsec-proposal ikev2-proposal***

*Device (config)**#protocol esp encryption_aes***

*Device (config)**#protocol esp integrity sha256***

*Device (config)**# access-list ikev2-list extended permit ip 10.10.10.0 0.255.255.255 10.10.10.0 0.255.255.255***

*Device (config-tunnel-ipsec)**# tunnel-group 10.10.10.102 type ipsec-l2l***

*Device (config-tunnel-ipsec)**# tunnel-group 10.10.10.102 ipsec-attibutes***

*Device (config)**# ikev2 local-authentication certificate***

*Device (config)**# ikev2 remote-authentication certificate CA***

*Device (config)**#crypto map ikev2-map 1 match address ikev2-list***

*Device (config)**#crypto map ikev2-map 1 set peer 10.10.10.102***

*Device (config)**#crypto map ikev2-map 1 set ikev2 ipsec-proposal ikev2-proposal***

*Device (config)**#crypto map ikev2-map interface outside***

5.7.5.3 AUTENTICACIÓN DE LA AUTORIDAD DE CERTIFICACIÓN (AC)

100. El producto debe autenticar la AC 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 AC en su sitio público.

a) Autentificar la AC: **crypto ca authenticate *trustpoint-name***

*Device (config)**#crypto ca authenticate ciscotest***

El certificado tiene los siguientes atributos:

Huella: 0123 4567 89AB CDEF 0123

% Acepta este certificado? [sí/no]: sí

Certificado AC de trustpoint aceptado.

[4] El tiempo de vida de estas asociaciones de seguridad no deberá ser mejor de 24 h (86.400 s.)

5.7.5.4 ALMACENAR CERTIFICADOS EN EL ALMACENAMIENTO LOCAL

101. Los certificados se almacenan en NVRAM por defecto; sin embargo, algunos *routers* 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 [13] para más información.

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

    a) Acceder al modo de configuración del terminal:

    *Device****# configure terminal***

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

    *Device(config)****# crypto pki certificate storage flash:/certs***

    c) Salir:

    *Device(config)****# exit***

    d) Guardar los cambios realizados:

    *Device****# copy system:running-config nvram:startup-config***

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

    *Device****# show crypto pki certificates storage***

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

103. 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.

104. Si el producto no tiene el CRL aplicable y no puede obtenerlo, o si el servidor OCSP devuelve un error, deberá rechazar el certificado del extremo. – El producto permite que no se realice ninguna comprobación de revocación de certificados cuando el administrador incluya la palabra clave '*none*' en su configuración. El comando para aceptar siempre el certificado es ***crl cache none***. No obstante, esta opción no se recomienda y solo se permite su uso cuando dicha comprobación se realice por otros medios.

105. 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.

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

106. 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.

5.7.5.7 CONFIGURACIÓN DE LA VALIDACIÓN DE LA CADENA DE CERTIFICADOS

107. 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:

    a) El dispositivo debe estar inscrito en su jerarquía de PKI.

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

108. Y deberán seguirse los siguientes pasos:

    a) Acceder al modo de configuración del terminal:

    *Device****# configure terminal***

    b) Establecer el nombre del *crypto pki trustpoint:*

    *Device(config)****# crypto pki trustpoint ca-sub1***

    c) 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]]**:

    *Device(ca-trustpoint)****# chain-validation continue ca-sub1***

    - 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.

d) Salir:

*Device(ca-trustpoint)**# exit***

5.7.5.8 CONFIGURACIÓN DE X.509 PARA IKE

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

*Device (config)**#crypto ikev2 proposal sample***

*Device(config-ikev2-profile)**#authentication [remote | local] rsa-sig***

o

*Device(config-ikev2-profile)**#authentication [remote | local] ecdsa-sig***

Si se carga un certificado no válido, la autenticación no funcionará.

5.7.5.9 ELIMINAR CERTIFICADOS

110. Por motivos de caducidad, o por acciones específicas del plan de protección contra problemas de seguridad, si fuera necesario, se pueden eliminar los certificados guardados en el *router*. El *router* guarda sus propios certificados y el certificado de la AC.

Para borrar el certificado del *router* de su configuración, se pueden utilizar los siguientes comandos en el modo de configuración global:

*Router**# show crypto ca certificates*** [Muestra los certificados guardados en el router]

*Router(config)**# crypto ca certificate chain name*** [Entra en el modo de configuración de cadena de certificados]

*Router(config-cert-cha)**# no certificate certificate-serial-number*** [borra el certificado]

111. Para borrar el certificado de la AC, se debe eliminar la identidad de la AC por completo, lo que también elimina todos los certificados asociados con la AC, el certificado del *router* y el de la AC. Para eliminar la identidad de la AC, se puede utilizar el siguiente comando en el modo de configuración global:

*Router(config)**# no crypto ca identity name*** [Borra toda la información de identidad y los certificados asociados con la AC]

5.7.6 POLÍTICAS DE FLUJO DE INFORMACIÓN

112. Un administrador autorizado puede definir las normas de tráfico y capacidades VPN configurando listas de acceso (con acciones de permitir, rechazar y/o

registrar), y aplicando dichas listas de acceso a interfaces que utilicen sets de acceso y mapas de cifrado:

a) La opción de 'descarte' se consigue utilizando listas de acceso con entradas de rechazo, que se aplican a interfaces dentro de grupos de acceso. Ver [14] para más información sobre la configuración de las Políticas de Flujo de la Información en IOS, en las secciones "*Zone-based Policy Firewalls*" o "*Zone-Based Policy Firewall IPv6 Support*" para IPv6.

b) La opción de 'bypass' se consigue utilizando listas de acceso con entradas de rechazo, que se aplican a interfaces dentro de mapas de cifrado para IPsec y el comando '***filter tunnel***' para SSL VPN. Ver [15] para más información sobre la configuración de entradas para IPsec.

c) La opción de 'protección' se consigue utilizando listas de acceso con entradas de permiso, que se aplican a interfaces dentro de mapas de cifrado para IPsec y el comando '***filter tunnel***' para SSL VPN.

113. El criterio usado para filtrar el tráfico usando las listas de acceso contempla la dirección de origen y destino y opcionalmente la capa 4 y el puerto.

114. Se recomienda que el máximo número de eventos sea registrado para un posterior análisis si fuera necesario y aplicar el principio de rechazo global en contraposición del permiso global.

5.8 ACTUALIZACIÓN DEL PRODUCTO

115. La verificación de la autenticidad de una actualización de *software* se desarrolla verificando que el dispositivo está ejecutando una imagen valida. Véase sección 4.2, pasos 7, 8 y 9 anteriores para descargar y verificar una imagen antes de ejecutarla en el producto.

5.9 CONFIGURACIÓN DEL IDENTIFICADOR DE REFERENCIA

116. Esta sección describe la configuración del identificador de referencia del extremo, que se consigue mediante un mapa de certificado.

117. Los mapas de certificado ofrecen la posibilidad de hacer coincidir un certificado con 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 (6) tests 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 mapas de certificados, y el producto determinará si son válidos durante la autentificación de IKE.

Pasos	Comando	Descripción
Paso 1	(*config*)***# crypto pki certificate map*** *label*	*Inicia el modo certificate-map*

Pasos	Comando	Descripción
	sequence-number	
Paso 2	(*ca-certificate-map*)# *field-name matchcriteria match-value*	En el modo *ca-certificate-map*, se especifican uno o más campos de certificado, junto con sus criterios de coincidencia y el valor que debe coincidir. • *field-name*—Especifica uno de los siguientes *strings* de nombre no sensibles a mayúsculas, o una fecha: o *–subject-name* o *–issuer-name* o *–unstructured-subject-name* o *–alt-subject-name* o *–name* o *–valid-start* o *–expires-on* El formato de campo de Fecha es dd mm aaaa hh:mm:ss, o mm dd aaaa hh:mm:ss. • *match-criteria*—Especifica uno de los siguientes operadores lógicos: o –eq—Igual (válido para campos de nombre y fecha) o –ne—No igual (válido para campos de nombre y fecha) o –co—Contiene (válido únicamente para campos de nombre) o –nc—No contiene (válido únicamente para campos de nombre) o –lt —Menor que (válido únicamente para campos de fecha) o –ge —Mayor o igual que (válido únicamente para campos de fecha) • *match-value*—Especifica el nombre o fecha a testear con el operador lógico asignado por los criterios de

Pasos	Comando	Descripción
		coincidencia.
Paso 3	(*ca-certificate-map*)**# *exit***	Sale del modo *ca-certificate-map.*
Paso 4	Para IKEv2: *crypto ikev2 profile ikev2-profile1 match certificate label*	Asocia el ACL basado en certificado definido con el comando ***crypto pki certificate map*** al perfil.

Tabla 4 – Configuración de los mapas de certificados

5.10 REGISTOS DE AUDITORÍA

118. El producto es capaz de generar registros de auditoría que se almacenan localmente cuando ocurre un evento de auditoría, y se descargan simultáneamente a un servidor *syslog* externo. Los detalles para la protección de dicha comunicación se encuentran en la Sección 5.2.5.

119. 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 5.2.3.

120. El buffer de registro local es circular. Los mensajes más nuevos sobrescriben a los más antiguos cuando el buffer está lleno. Los administradores deben monitorizar el buffer de registro mediante el comando ***show logging privileged EXEC*** para visualizar los registros de auditoría. El primer mensaje mostrado es el mensaje más antiguo en el buffer.

121. Cuando se configure para una copia de seguridad del *syslog*, el producto descargará los eventos de otro buffer al servidor *syslog* externo de modo simultáneo. Este buffer se utiliza para poner en cola los eventos que se enviarán al servidor *syslog* si se pierde la conexión con el servidor. Es un servidor circular, así que cuando los eventos sobrepasan el espacio de almacenamiento, se sobrescriben los más antiguos.

122. 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.

123. Para ver ejemplos de eventos de seguridad que aplican al producto:

    a) Ver la Tabla 7 "*General Auditable Events*" de los documentos [16] [17] [18] donde se incluyen eventos generales.

b) Véase la Tabla 8 "*Auditable Administrative Events*" de los documentos [16] [17] [18] donde se incluyen eventos de acciones de administrador.

124. Los eventos de configuración que se deberían capturar como mínimo son:

a) Cambios en datos clave secretos dentro de la configuración.

b) Cambios confirmados.

c) Inicio y cierre de sesión por parte de los usuarios.

d) Inicio del sistema.

e) Fallos al establecer una sesión de SSH.

f) Establecimiento o finalización de una sesión de SSH.

g) Cambios en la fecha y hora del sistema.

h) Finalización de una sesión remota por medio del mecanismo de bloqueo de sesiones.

i) Finalización de una sesión interactiva.

j) Cambios en la configuración del sistema.

5.10.1 ELIMINAR REGISTROS DE AUDITORÍA

125. El producto proporciona al Administrador privilegiado la capacidad de suprimir los registros de auditoría almacenados mediante el comando *"**clear logging**"*.

*Device# **clear logging***

Clear logging buffer [confirm] <ENTER>

5.11 SERVICIOS DE RED Y PROTOCOLOS

126. 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.

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.

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.

5.12 MODOS DE OPERACIÓN

127. El *router* dispone de diversos modos de operación:

128. ***Booting*** – durante el arranque, los *routers* cesan cualquier tráfico de red hasta que se haya cargado la imagen del *router* y la configuración. Este modo de operación progresa automáticamente hacia el modo de operación Normal. Durante el arranque, el administrador puede pulsar la tecla de pausa en una conexión de consola durante los primeros 60 segundos del arranque para entrar en el modo de operación ROM Monitor. Este modo de *Booting* se menciona en los documentos de guía de la IOS como "Inicialización de ROM Monitor". Además, si el *router* no encuentra una imagen de sistema operativo válida, entrará en el modo ROM Monitor en vez del modo normal, protegiendo así el *router* para que no se inicie en un estado no seguro.

129. ***Normal*** – se cargan la imagen del *router* IOS y la configuración, y el *router* opera tal como se ha configurado. Debe tenerse en cuenta que todos los niveles de acceso administrativo suceden en este modo, y que todas las funciones de seguridad basadas en el *router* están operativas. Durante el funcionamiento, el router tiene poca interacción con el administrador. Sin embargo, la configuración del *router* puede tener efectos negativos en la seguridad. Si el router se configura mal, la red desprotegida puede tener acceso a la red interna/protegida.

130. ***ROM Monitor*** – Este modo de operación es un modo de mantenimiento, eliminación de fallos, y recuperación. Mientras el *router* se encuentre en este modo, no se enruta ningún tráfico de red entre las interfaces de red. En este estado, se puede configurar el *router* para que cargue una nueva imagen de arranque desde un servidor TFTP concreto, realice tareas de configuración, y ejecute diversos comandos de eliminación de fallos. Debe tenerse en cuenta que, aunque no se requiere ninguna contraseña de administrador para acceder al modo ROM Monitor, se requiere acceso físico al *router*; por lo tanto, el *router* debe almacenarse en una ubicación físicamente segura para evitar el acceso no autorizado, que puede provocar que el *router* se encuentre en estado no seguro.

131. Tras un error de operación, el *router* se reinicia (cuando se disponga de corriente) y entra en el modo *Booting*.

5.13 MEDIDAS DE SEGURIDAD PARA EL ENTORNO OPERACIONAL

132. El correcto funcionamiento del producto requiere de funcionalidades del entorno. Es responsabilidad del Administrador Autorizado garantizar que el entorno operacional proporciona las funciones necesarias y cumple los objetivos de seguridad siguientes:

a) El dispositivo 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 dispositivo 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 (p. ej., claves criptográficas, material de claves, PINs, contraseñas, etc.) en el equipo de red, cuando el equipo se elimine o se retire de su entorno operativo.

6 FASE DE OPERACIÓN Y MANTENIMIENTO

133. Durante la fase de operación de los dispositivos, los Administradores de Seguridad deben llevar a cabo las siguientes tareas de mantenimiento:

a) Comprobaciones periódicas del *hardware* y *software* para asegurar que no se ha introducido *hardware* o *software* no autorizado. El *firmware* activo y su integridad deberán verificarse periódicamente para comprobar que está libre de *software* malicioso.

b) Aplicación regular de parches de seguridad y actualizaciones del *firmware* del sistema, de cara a mantener su 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. Dicha información es la misma que la descrita anteriormente para la instalación de la imagen de *software*.

c) Mantenimiento de registros de auditoria. 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.

d) Auditoría de al menos los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.

e) Control de acceso a la información de auditoria de forma que únicamente el personal de seguridad designado pueda acceder a ella.

f) Realización de *backups* automáticos de forma periódica y, a poder ser, de forma centralizada.

7 REFERENCIAS

[1] Cisco, «Cisco IOS Configuration Fundamentals Command Reference,» [En línea]. Available: http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/Cisco_IOS_Configuration_Fundamentals_Command_Reference.html.

[2] Cisco, «Configuration Fundamentals Configuration Guide,» [En línea]. Available: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/xe-16/fundamentals-xe-16-book.html.

[3] Cisco, «Cisco 1100 Series Software Configuration Guide, Cisco IOS XE Everest 16.6.2,» [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/routers/access/1100/software/configuration/xe-16-6/cisco_1100_series_swcfg_xe_16_6_x.html.

[4] Cisco, «Cisco 4000 Series ISRs Software Configuration Guide,» [En línea]. Available: http://www.cisco.com/c/en/us/td/docs/routers/access/4400/software/configuration/guide/isr4400swcfg.pdf.

[5] Cisco, «Cisco IOS Security Command Reference,» [En línea]. Available: http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-a1-cr-book.html.

[6] Cisco, «Hardware Installation Guide for the Cisco 1100 Series Integrated Services Router,» [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/routers/access/1100/hardware/installation/guide/b-cisco-1100-series-hig.html.

[7] Cisco, «Hardware Installation Guide for the Cisco 4000 Series Integrated Services Router,» [En línea]. Available: http://www.cisco.com/c/en/us/td/docs/routers/access/4400/hardware/installation/guide4400-4300/C4400_isr.html.

[8] Cisco, «Hardware Installation Guide for the Cisco ISR 4400 and Cisco ISR 4300 Series Integrated Services Router,» [En línea]. Available: http://www.cisco.com/c/en/us/td/docs/routers/access/4400/hardware/installation/guide4400-4300/C4400_isr.html.

[9] Cisco, «Using Setup Mode to Configure a Cisco Networking Device,» [En línea]. Available: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/15-s/fundamentals-15-s-book.html.

[10] Cisco, «RADIUS Configuration Guide,» [En línea]. Available: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_rad/configuration/xe-16/sec-usr-rad-xe-16-book.html.

[11] Cisco, «Basic System Management Configuration Guide,» [En línea]. Available: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bsm/configuration/xe-16/bsm-xe-16-book.html.

[12] Cisco, «IP Addressing: NAT Configuration Guide,» [En línea]. Available: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-16/nat-xe-16-book.html.

[13] Cisco, «Public Key Infrastructure Configuration Guide,» [En línea]. Available: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-16/sec-pki-xe-16-book.html.

[14] Cisco, «IPsec Data Plane Configuration Guide,» [En línea]. Available: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dplane/configuration/xe-16/sec-ipsec-data-plane-xe-16-book.html.

[15] Cisco, «FlexVPN and Internet Key Exchange Version 2 Configuration Guide,» [En línea]. Available: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xe-16/sec-flex-vpn-xe-16-book.html.

[16] Cisco, «Integrated Services Routers (ISR) 1100 Family CC Configuration Guide,» 2018.

[17] Cisco, «Integrated Services Routers (ISR) 4000 Family CC Configuration Guide,» 2017.

[18] Cisco, «ISR-4400 CC Configuration Guide».

[19] Cisco, «MACSEC and MKA Configuration Guide,» [En línea]. Available: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xe-16/macsec-xe-16-book.html.

[20] Cisco, «Loading and Managing System Images Configuration Guide,» [En línea]. Available: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sys-image-mgmt/configuration/xe-16/sysimgmgmt-xe-16-book.html.

[21] Cisco, «Release Notes for the Cisco 1100 Series ISR 16.6.2,» [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/routers/access/1100/release/16-6-2/isr1k-rel-notes-xe-16-6.html.

[22] Cisco, «Release Notes for the Cisco 4000 Series ISRs,» [En línea]. Available: http://www.cisco.com/c/en/us/td/docs/routers/access/4400/release/xe-16-rn/isr4k-rel-notes-xe-16_3.html.

[23] CCN, «CCN-STIC-807 Criptología de empleo en el Esquema Nacional de Seguridad,» 2017.

8 ABREVIATURAS

CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de productos de Seguridad TIC
CRL	*Certificate Revocation List*
DH	*Diffie – Hellman Algorithm*
DHCP	*Dynamic Host Configuratio Protocol*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
ENS	Esquema Nacional de Seguridad
FIPS-CC	*Federal Information Processing Standard – Common Criteria*
FTP	*File Transport Protocol*
ICMP	*Internet Control Message Protocol*
IPsec	*Internet Protocol security*
RSA	Rivest, Shamir y Adleman *Algorithm*
SCP	*Secure Copy Protocol*
SHA	*Secure Hash Algorithm*
SSH	*Secure Shell Protocol*
SSL	*Secure Sockets Layer Protocol*
STIC	Seguridad de Tecnologías de Información y Comunciación
TCP	*Transmission Control Protocol*
TFTP	*Trivial File Transport Protocol*
TLS	*Transport Layer Security*
TLS	*Transport Layer Security Protocol*
UDP	*User Datagram Protocol*
VPN	*Virtual Private Network*