centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC-1459

Procedimiento de empleo seguro
Switches H3C

Enero 2024

MINISTERIO DE DEFENSA

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

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.02.01 12:35:29 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-024-7.
Fecha de Edición: enero de 2024.

ÍNDICE

1. INTRODUCCIÓN

1. El presente documento pretende servir de guía para establecer una configuración segura para los equipos pertenecientes a las series S10500, S7500, S6500, S5100, S5500, S12500, S9800, S6800 con sistema operativo H3C Comware Software, Versión 7.1.070.
2. Los switches anteriormente definidos de H3C son dispositivos de red diseñados para entornos empresariales, gubernamentales, educativos, financieros o industriales que ofrecen una variedad de funciones para garantizar conectividad eficiente y confiable. Los switches series de H3C proporcionan protocolos de seguridad estandarizados para la gestión de la configuración.
3. A lo largo de los diferentes capítulos, se ofrecen consejos y recomendaciones sobre:
    - Recepción del producto, entorno e instalación.
    - La activación o desactivación de servicios y funcionalidades del producto.
4. La finalidad es llevar el producto desde su configuración de fábrica hasta establecer una configuración segura que sea compatible con la configuración evaluada.
5. La estructura del documento y sus contenidos no exigen una lectura lineal del mismo. El lector puede utilizar el índice de contenidos para localizar y acceder al capítulo que trate el aspecto sobre el que desea mejorar la seguridad. Sin embargo, se recomienda realizar una lectura del documento completo para conocer de todas las funcionalidades descritas.
6. **Estos switches han sido cualificados para categoría ALTA e incluidos en el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC).** Se debe consultar el Catálogo para determinar la versión y modelos cualificados en cada momento.

2. OBJETO Y ALCANCE

7. El objeto de este documento es analizar los mecanismos de seguridad disponibles para proteger los entornos de sistemas de información y comunicaciones que emplean los equipos pertenecientes a las **series S10500, S7500, S6500, S5100, S5500, S12500, S9800, S6800 con sistema operativo H3C Comware Software, Versión 7.1**. Como consecuencia, se establece un marco de referencia que contempla las recomendaciones STIC en la implantación y utilización de los switches.
8. Las autoridades responsables de la aplicación de la política de seguridad de las TIC (STIC) determinarán el análisis y aplicación de este documento a los switches mencionados en el párrafo anterior bajo su responsabilidad.
9. Queda fuera del alcance de este documento la configuración de los mecanismos para garantizar la calidad de servicio necesaria para la explotación del dispositivo ya que se entiende que la calidad del servicio no afecta a la seguridad de este.
10. En el ámbito de este documento, se asume que existirá un usuario de nivel administrador que podrá configurar todas las funcionalidades requeridas.
11. Los dispositivos han sido cualificados e incluidos en el Catálogo de Productos y Servicios de seguridad (CPSTIC) del Centro Criptológico Nacional. Se debe comprobar el estado de cualificación (que este se mantiene) y que la versión de este documento es la más actualizada.

3. ORGANIZACIÓN DEL DOCUMENTO

12. El documento se organiza de la siguiente forma:

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

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

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

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

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

13. Para asegurarse que el producto no ha sido modificado durante su transporte, revisar el paquete que se entrega de la siguiente manera:
14. **Revisión Exterior:**
    - Comprobar que el embalaje exterior está en buenas condiciones.
    - Comprobar la cinta de embalar y etiquetas del embalaje de cartón exterior.
    - Comprobar el sellado de la bolsa plástica que se encuentra dentro del embalaje de cartón.
15. Si alguna de estas comprobaciones no es satisfactoria, el producto será considerado defectuoso.
16. **Comprobación de contenido:**
17. Revisar con la lista de elementos el contenido del paquete. Si hay alguna discrepancia en cuanto al tipo o número de elementos, el producto será considerado defectuoso.
18. **Inspección visual del contenido:**
19. Inspeccionar defectos en el chasis, conexiones dañadas, otro tipo de daños externos y etiquetas ilegibles. Si alguna superficie o material tiene daños, el producto será considerado defectuoso.
20. **Verificación de la integridad del software**
21. La imagen del software tiene una firma digital. Cuando el dispositivo arranca, la firma digital se verifica automáticamente, si falla, el producto no continuará con el arranque (principio de diseño *fail-safe*) y mostrará un mensaje de error.
22. Cada vez que se realice una actualización del software la firma digital de la nueva imagen será comprobada por el dispositivo. Para más información sobre el proceso de actualización ver la sección 6.9.
23. Si el producto se considera defectuoso, se debe para el proceso de desembalaje e instalación, guardar el paquete e informar a H3C para realizar la correspondiente investigación. Los bienes dañados serán reemplazados en caso de ser necesario.

4.2 ENTORNO DE INSTALACIÓN SEGURO

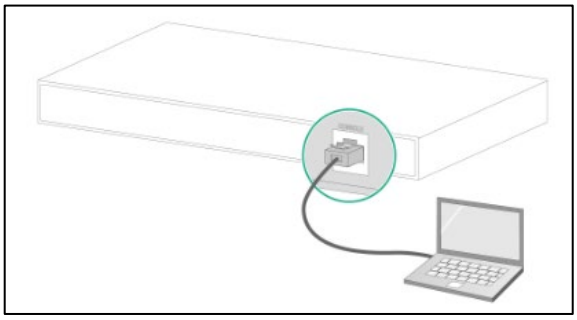
24. Se debe desplegar el producto en un entorno físico protegido, donde solo pueda acceder el personal expresamente autorizado por la organización y que disponga de las medidas de seguridad adecuadas.

4.3 REGISTRO Y LICENCIAS

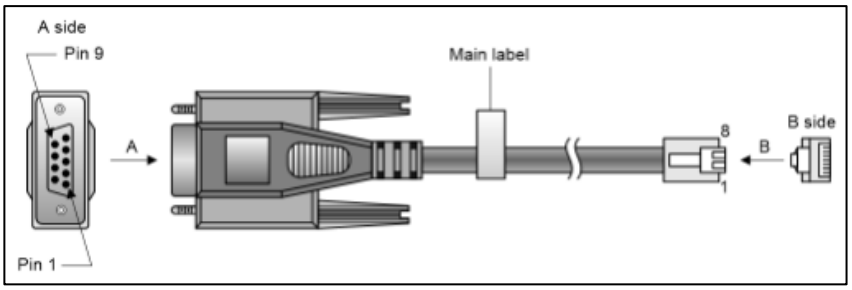
25. Los equipos pertenecientes a las series S10500, S7500, S6500, S5100, S5500, S12500, S9800, S6800 no tienen un sistema de registro y licenciamiento específico. El hecho de estar en posesión el producto da derecho a su uso.

4.4 CONSIDERACIONES PREVIAS

26. Para realizar la administración, la configuración de fábrica solo permite administrar el switch mediante consola conectando directamente un equipo al puerto serie de consola.



27. El puerto de consola del Switch es de tipo RJ45. Se necesitará un cable DB9-a-RJ45 o USB-a-RJ45 para conectar el equipo que realizará las tareas de administración del switch.
28. El mapeo de pines de un cable DB9-a-RJ45 depende del fabricante de este. Para evitar errores, se recomienda usar el cable proporcionado por H3C.



29. Para configurar y administrar el switch a través del puerto de consola, se debe utilizar un programa emulador de terminal. Configure los parámetros del terminal de la siguiente manera:
    - Bits por segundo: 9600.
    - Bits de datos: 8.
    - Paridad: Ninguna
    - Bits de parada: 1
    - Control de flujo: Ninguno.

30. Asimismo, antes de desplegar el equipo en la red es imprescindible realizar una actualización del mismo con las últimas versiones estables del sistema operativo, con el objeto de protegerlo de los problemas de seguridad detectados en versiones anteriores. Ver sección 6.9.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

31. Para administrar el equipo de forma local se requerirá de un equipo de gestión, tal y como se menciona en la sección 4.4 de este documento.
32. Debido a las limitaciones de almacenamiento de auditoría del dispositivo, se requiere de un servidor de auditoría externo (*syslog*), este debe ser accesible por el dispositivo y configurado según la sección 6.11.4.
33. El administrador también puede configurar el dispositivo para autenticar a los usuarios mediante un servidor de autenticación externo (compatibilidad con RADIUS y HWTACACS).

5. FASE DE INSTALACIÓN

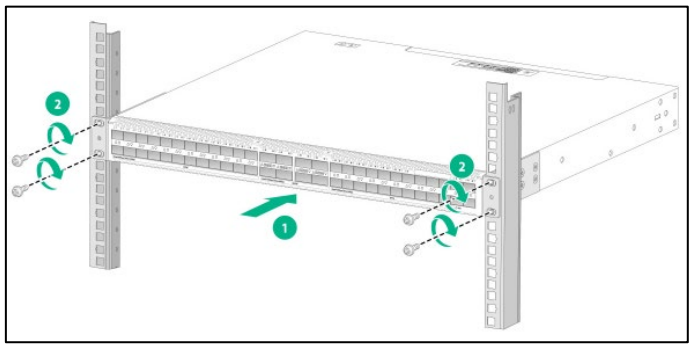
34. La instalación del producto se realizará en un bastidor (rack) de 19 pulgadas o sobre una superficie.

35. Los switches contemplados en este documento difieren en tamaño, por lo que **se aconseja revisar los manuales de instalación para cada switch en cuestión**.

36. Los pasos comunes para la instalación de los switches se muestran a continuación.

37. **Montaje del switch en el rack:**

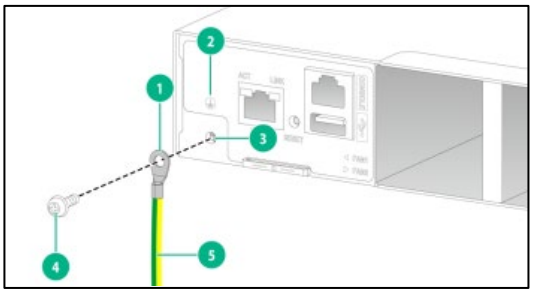
    1) Usar una muñequera electrostática para la protección contra las descargas.
    2) Verificar que los soportes de montaje estén firmemente sujetos al chasis del switch.
    3) Colocar las tuercas de la jaula en los soportes frontales del rack.
    4) Una persona soporta la parte inferior del switch y lo mueve a la posición adecuada en el rack.
    5) Otra persona utiliza tornillos M6 y tuercas de jaula para asegurar los soportes de montaje al rack, verificando que estén nivelados y seguros.



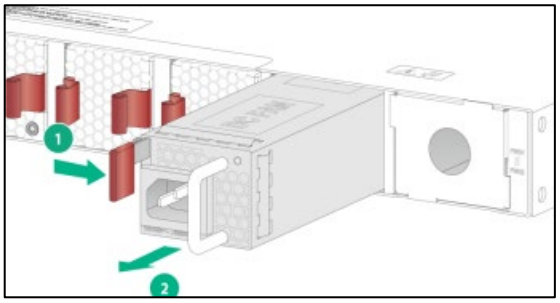
38. **Montaje del switch sobre una superficie:**

    1) Mantener un **espacio un mínimo de 10 centímetros alrededor del switch** para permitir la disipación de calor y verificar que la superficie sea resistente.
    2) Colocar el switch con la parte inferior hacia arriba, limpiar los agujeros de la parte de abajo del chasis donde irán sujetas las patas de goma y colocar las patas en los agujeros.
    3) Colocar el switch con la parte superior hacia arriba en la superficie.

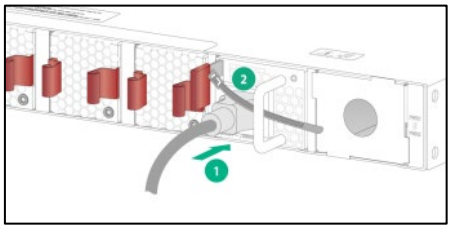
39. Conectar el switch a tierra, quitar el tornillo de conexión a tierra del chasis e introduciendo el anillo del cable de tierra en el tornillo, volver a atornillar al chasis.

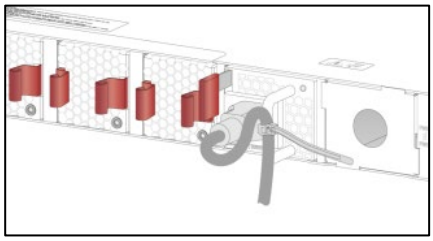


40. Instalar las fuentes de alimentación, en algunos modelos **es posible instalar más de una fuente de alimentación de forma que se garantice la disponibilidad** del servicio en caso de fallar una de las mismas.



41. Al poner el cable de alimentación asegurar el **cable con los elementos físicos que proporciona la fuente de alimentación** para tal efecto (enganches, abrazaderas), evitando desconexiones indeseadas del mismo.





42. Conectar un equipo de administración según lo indicado en la sección 4.4 CONSIDERACIONES PREVIAS.
43. Ejecutar un emulador de terminal en el equipo de administración, se puede realizar la conexión a través de Telnet y SSH.
44. En caso de contar con un servidor de auditoría, realizar la configuración definida en la sección 6.11.4.
45. En caso de contar con un servidor NTP para sincronizar el reloj del switch, realizar la configuración definida en la sección 6.8.

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

46. Los switches tienen un modo de operación FIPS. El nivel FIPS que cumplen estos dispositivos es “Level-2”.
47. En modo FIPS, los dispositivos verifican que el módulo criptográfico está operando correctamente.
48. Para que los dispositivos cumplan con la funcionalidad definida por CPSTIC, estos **deben tener el modo de operación FIPS activado, por defecto está desactivado**.
49. Para activar el modo FIPS, hay dos alternativas, hacerlo a través de un “reinicio automático” o un “reinicio manual”. Por simplicidad, en esta guía se explica el procedimiento a seguir mediante el método “reinicio automático” ya que es un proceso guiado por el propio dispositivo más simple y menos propenso a errores de administración. En caso de querer realizar el “reinicio manual” seguir los manuales del dispositivo.

6.1.1 ACTIVAR MODO FIPS

50. Prerrequisito: Poner la fecha/hora del dispositivo correctamente.
51. El procedimiento para activar el modo FIPS se muestra a continuación:
    1. Entrar la vista de sistema:

       ```
       <Sysname> system-view
       ```

    2. Activar el modo FIPS:

       ```
       [Sysname] fips mode enable
       ```

    3. El dispositivo pide al usuario que se elija el tipo de reinicio (manual o automático) que se quiere seguir para activar FIPS, elegir automático:

       ```
       FIPS mode change requires a device reboot. Continue? [Y/N]:y
       Reboot the device automatically? [Y/N]:y
       ```

    4. Introducir un nuevo nombre de usuario y contraseña, este será el usuario administrador del equipo. La contraseña debe contener un mínimo de 15 caracteres, mayúsculas y minúsculas, dígitos y caracteres especiales.

       ```
       Enter username(1-55 characters):root
       Enter password(15-63 characters):
       Confirm password:
       Waiting for reboot... After reboot, the device will enter FIPS
       mode.
       ```

52. El dispositivo hace las siguientes acciones de configuración:
    - Crea un usuario administrador con el nombre de usuario y contraseña dados.
    - Le asigna a dicho usuario el rol “network-admin” y acceso por consola.
    - Guarda la configuración actual y la asigna como configuración de arranque.

- Reinicia entrando en modo FIPS.

53. Para acceder al dispositivo, debes hacerlo con este usuario. Este usuario será identificado como “FIPS mode crypt officer”.

6.1.2 COMPROBAR MODO FIPS

54. En cualquier momento se puede comprobar si el dispositivo está ejecutando en modo FIPS con el siguiente comando:

```
<Sysname> display fips status
```

55. La salida del comando deberá ser:

```
FIPS mode is enabled.
```

6.2 AUTENTICACIÓN

6.2.1 AUTENTICACIÓN DE USUARIOS

56. El dispositivo permite los siguientes modos de autenticación de usuarios:
    - **Ninguno:** Desactiva la autenticación. Teste modo permite el acceso sin autenticación y es inseguro.
    - **Password:** Requiere autenticación por contraseña.
    - **Scheme:** Usa el módulo AAA para la autenticación local y remota. La autenticación se realiza por contraseña.
57. **En modo FIPS (el único permitido, ver sección 6.1), el dispositivo solo permite el modo “Scheme”.**
58. Al activar el modo FIPS el dispositivo utiliza el modo “Scheme”, no hace falta realizar ninguna otra acción.
59. El dispositivo admite la definición local de usuarios con contraseña y rol correspondientes. Las contraseñas pueden componerse de cualquier combinación de letras mayúsculas y minúsculas, números y caracteres especiales. La longitud mínima de la contraseña es configurable por el administrador de seguridad autorizado y admite contraseñas de entre 15 a 63 caracteres.
60. El administrador también puede configurar el dispositivo para delegar la autenticación de los usuarios a un servidor de autenticación externo. El dispositivo es compatible con servidores RADIUS y HWTACACS.
61. La autenticación remota se realiza mediante SSH (única opción posible y habilitada por defecto en modo FIPS).
62. En la activación de SSH solo se permitirán los siguientes algoritmos criptográficos: AEAD_AES_128_GCM, AEAD_AES_256_GCM, aes128-gcm@openssh.com, aes256-gcm@openssh.com

6.2.2 AUTENTICACIÓN DE SERVIDORES EXTERNOS

63. El dispositivo utiliza IPsec/IKEv2 para garantizar la autenticación de los servidores de auditoría y autenticación.
64. El dispositivo permite hacer la autenticación mediante dos mecanismos distintos:
    - **Clave previamente compartida (PSK):** Los dos extremos de comunicación usan una clave compartida preconfigurada para realizar la autenticación.
    - **Certificados digitales:** Los dos extremos utilizan certificados digitales emitidos por una CA para realizar la autenticación.
65. **Se recomienda utilizar certificados digitales, siempre que esta opción sea posible.**
66. Los protocolos criptográficos aceptados para la configuración segura de IPsec son:
    - Algoritmos criptográficos aceptados: AES-GCM-128 (RFC 4106), AES-GCM-192 (RFC 4106), AES-GCM-256 (RFC 4106).
    - Algoritmos hash aceptados: SHA256, SHA384, SHA512.
67. La configuración segura para IKEv2 será la siguiente:
    - Algoritmos criptográficos aceptados: AES-GCM-128 (RFC 4106), AES-GCM-192 (RFC 4106), AES-GCM-256 (RFC 4106).
    - Grupos DH aceptados: 19 (256-bit Random ECP), 20 (384-bit Random ECP), 24 (2048-bit MODP with 256-bit POS).
    - Tiempo de vida de IKE SA: El tiempo de vida podrá ser configurado en un periodo comprendido entre 1 y 8 horas.
    - Protocolo IPSec: El protocolo IPSec que se permite es ESP (ya que AH no proporciona confidencialidad de los datos transmitidos).
68. El par de claves utilizado en los certificados y utilizado para las negociaciones para establecer los canales seguros debe de cumplir con los siguientes requisitos criptográficos: RSA (3072 y 4096 bits) y ECDSA (P-256, P-384 y P-521).
69. El dispositivo puede usar un servidor NTP para sincronizar la hora del sistema. Las versiones del protocolo que se deben utilizar son NTPv3 (RFC 1305) y NTP V4 (RFC 5905).
70. La configuración criptográfica para este servicio se puede realizar a través de IPsec como para el resto de los servicios explicados en este punto o autenticación usando SHA256, SHA384, SHA512 como algoritmo hash.

6.3 ADMINISTRACIÓN DEL PRODUCTO

71. En esa sección se describe la configuración segura de los interfaces mediante los que los usuarios pueden interactuar directamente con los dispositivos. Los

dispositivos cuentan con otros interfaces para interactuar con otros equipos de red o servidores externos, dichos interfaces no están descritos en esta sección.

72. Los usuarios pueden interactuar mediante la línea de comandos (CLI) a través de una conexión física a través del puerto serie o mediante SSH a través de TCP/IP en el puerto 22.

6.3.1 ADMINISTRACIÓN LOCAL

73. El interfaz de administración local está habilitado por defecto, la configuración necesaria para acceder al mismo está definida en 4.4.
74. La administración local está protegida por usuario y contraseña, de cualquier modo, se recomienda limitar el acceso físico al dispositivo a los administradores del sistema.
75. Para configurar la consola de forma segura hay que seguir los pasos que se muestran a continuación:
    1. Configurar el mensaje inicial (banner o legal message).
    2. Configurar el interfaz de usuario Consola/AUX.
    3. Configurar la cuenta del usuario local.
76. **Configurar el mensaje inicial:** Se redacta el mensaje que recibirá un usuario cada vez que acceda al dispositivo. Para realizar esta configuración se utilizará el comando "`header legal`" en la terminal.
77. **Configurar el interfaz de usuario Consola/AUX:** Hay que definir la línea de consola que se está configurando con el comando `line` (ej. `Line aux 0`). A continuación, se utilizará el comando `iddle-timeout` para indicar el número de minutos para que se bloquee (lockout) la sesión.
78. **Configurar la cuenta del usuario local:** Se debe crear un usuario administrador y asignarle la contraseña correspondiente. A continuación, se muestra un ejemplo de cómo realizar esta configuración:

```
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1] service-type terminal
[Sysname-luser-manage-user1] authorization-attribute user-role
network-admin
[Sysname-luser-manage-user1] password
Password: ********************
Confirm : ********************
```

6.3.2 ADMINISTRACIÓN REMOTA

79. El dispositivo en modo FIPS limita la administración remota al protocolo SSH.
80. Para configurar SSH de forma segura se procederá de la siguiente manera:
    1. Configurar el mensaje inicial (banner o legal message).
    2. Activar el servidor SSH.

3. Configurar el interfaz de usuario para los clientes SSH.
4. Configurar las claves RSA o ECDSA del servidor.
5. Configurar un usuario SSH.

81. A continuación, se muestran los distintos pasos de forma detallada.
82. **Configurar el mensaje inicial:** Se redacta el mensaje que recibirá un usuario cada vez que acceda al dispositivo. Para realizar esta configuración se utilizará el comando "*header legal*" en la terminal desde la vista de sistema "system view".
83. **Activar el servidor SSH:** Para poder realizar conexiones SSH con el switch este debe tener el servicio activado. Para realizar esta configuración se utilizará el comando "*ssh server enable*".
84. **Configurar el interfaz de usuario para los clientes SSH:** Para que los usuarios puedan interactuar con el dispositivo, hay que habilitar una interfaz VTY (Virtual Teletype). En esta operación se especificará el tiempo que permanece sesión abierta si no se recibe actividad con el comando "idle-timeout", el valor que se propone son 10 minutos. Un ejemplo de configuración completa de este punto se muestra a continuación:

```
[Sysname] line class vty
[Sysname-line-class-vty] idle-timeout 10
[Sysname-line-class-vty] authentication-mode scheme
[Sysname-line-class-vty] protocol inbound ssh
```

85. **Configurar las claves RSA o ECDSA del servidor:** Para validar la autenticidad de un dispositivo desde un equipo remoto, el servidor tiene que generar un par de claves asimétricas y exportar su clave pública. Para crear las claves se utilizará el comando "*public-key local create {rsa | ecdsa}*" indicando el tipo de clave que se quiera generar.
86. Las claves que se generen tienen que cumplir con las siguientes características de complejidad: **RSA (3072 y 4096 bits)** y **ECDSA (P-256, P-384 y P-521).** Un ejemplo de creación de claves se muestra a continuación:

```
[Switch] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

87. Para exportar la clave pública se utiliza el comando *"public-key local export {rsa | ecdsa}"*.

6.3.2.1 USUARIO CON CONTRASEÑA

88. **Siempre que sea posible se recomienda utilizar, a parte de la contraseña un mecanismo de clave pública (sección 6.3.2.2). Esto permite que la autenticación sea de doble factor (lo que el usuario conoce y lo que posee).**
89. En esta sección se especifica como se crea un usuario con contraseña como credenciales de autenticación y acceso SSH. La creación del usuario es la misma

que la definida en la sección 6.3.1. Sin embargo, para esta operación se utiliza el comando "service-type ssh". Un ejemplo de su uso se puede ver a continuación:

```
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1] service-type ssh
 Sysname-luser-manage-user1] authorization-attribute user-role
network-admin
 [Sysname-luser-manage-user1] password
 Password: ********************
 Confirm : ********************
 [Sysname-luser-manage-user1] quit
```

6.3.2.2 USUARIO CON CONTRASEÑA Y CLAVE PÚBLICA

90. El primer paso es configurar un usuario con contraseña como se indica en el apartado 6.3.2.1.

91. Con el comando que se muestra a continuación importaremos la clave de un fichero definido por "filename" y le asignaremos un nombre en el dispositivo "keyname":

```
public-key peer keyname import sshkey filename
```

92. El último paso será vincular el usuario con la clave pública importada. Para esto especificaremos el nombre de usuario y el nombre de la clave (paso anterior) con el siguiente comando:

```
ssh user username service-type stelnet authentication-type
password-publickey assign publickey keyname
```

93. A partir de este momento la autenticación del usuario se realizará con contraseña y clave pública.

6.3.3 CONFIGURACIÓN DE ADMINISTRADORES

94. El TOE controla el acceso del usuario a comandos y recursos basado en el rol del usuario. A los usuarios se les otorga permiso para acceder a un conjunto de comandos y recursos basados en su rol de usuario. Para una información más detallada consulte la sección "Configuring RBAC" del documento [H3C-doc].

95. Para asignar permisos a un rol de usuario hay dos métodos distintos:

- Definir un conjunto de reglas en un rol de usuario para determinar los elementos accesibles o inaccesibles.
- Configurar en las políticas de acceso de los distintos recursos (interfaces, VLANs, instancias VPN) que usuarios tienen acceso al recurso y sus comandos.

6.3.3.1 USUARIOS PREDEFINIDOS

96. Por defecto, el dispositivo proporciona roles de usuario predefinidos. Estos roles de usuario tienen acceso a todos los recursos del sistema (interfaces, VLANs e

instancias de VPN). A continuación, se muestran los permisos de acceso de estos roles de usuario predefinidos.

Usuario	Permisos

network-admin	Accede a todas las características y recursos en el sistema, excepto a los comandos:
	`display security-logfile summary`
	`info-centersecurity-logfile directory`
	`security-logfile save`

network-operator	• Accede a los comandos de visualización (display) para todas las características y recursos en el sistema, excepto a comandos como:
	`display history-command all`
	`display security-logfile summary`
	• Permite que los usuarios que se autentican localmente puedan cambiar sus contraseñas.

security-audit	El rol tiene el siguiente acceso a los archivos de registro de seguridad:
	• Acceso a los comandos para visualizar y mantener archivos de registro de seguridad, por ejemplo, los comandos:
	`Dir`
	`display security-logfile summary`
	• Acceso a los comandos para gestionar archivos de registro de seguridad y el sistema de archivos de registro de seguridad, por ejemplo, los comandos:
	`info-center security-logfile directory`
	`mkdir`
	`security-logfile save`
	Solo el rol de usuario security-audit tiene acceso a los archivos de registro de seguridad.
	El rol security-audit y el registro de seguridad están desactivados por defecto y, cuando se activan, especifican una dirección de salida diferente para algunos tipos de eventos de auditoría, incluidos los eventos de inicio de sesión.

	Los registros de auditoría de seguridad del TOE se acceden a través del registro de auditoría local o mediante el servidor de auditoría syslog externo.
level-n	• **Level-0:** Tiene acceso a comandos de diagnóstico, incluyendo `ping`, `tracert`, `ssh2`, `telnet` y `super`. Los derechos de acceso de Level-0 son configurables. • **Level-1:** Tiene acceso a los comandos de visualización de todas las características y recursos en el sistema, excepto `display history-command all`. El rol de usuario level-1 también tiene todos los derechos de acceso del rol de usuario level-0. Los derechos de acceso de level-1 son configurables. • **Level-2 a Level-8 y Level-10 a Level-14:** No tienen derechos de acceso por defecto. Los derechos de acceso son configurables. • **Level-9:** Tiene acceso a la mayoría de las características y recursos en el sistema. Si ha iniciado sesión con una cuenta de usuario local que tiene un rol de usuario level-9, puede cambiar la contraseña en la cuenta de usuario local. A continuación, se presentan las principales características y comandos a los que el rol de usuario level-9 no puede acceder: – Usuarios locales. – Comandos RBAC. – Gestión de archivos. – Gestión del dispositivo. – El comando display history-command all. • **Level-15:** Tiene los mismos derechos que un network-admin.

6.3.3.2 CREACIÓN DE ROLES DE USUARIO

97. Además de los roles de usuario predefinidos, se pueden crear un máximo de 64 roles de usuario personalizados para un control de acceso más detallado.

98. Para crear un rol de usuario seguir los siguientes pasos:

    1. Crear un rol de usuario desde la vista de sistema:

       ```
       role name role-name
       ```

    2. (Opcional) Asignar una descripción al rol:

```
description text
```

6.3.3.3 CONFIGURACIÓN LAS REGLAS DE UN ROL DE USUARIO

99. Se pueden configurar reglas de roles de usuario para permitir o denegar el acceso de un rol de usuario a distintas funciones como comandos específicos o elementos XML.

100. Cualquier modificación, creación o eliminación de reglas para un rol de usuario solo tiene efecto en los usuarios que hayan iniciado sesión con ese rol de usuario después del cambio.

101. Las siguientes directrices se aplican a las reglas no-OID (no object identifier):

- Si dos reglas definidas por el usuario del mismo tipo entran en conflicto, la regla con el ID más alto tiene efecto. Por ejemplo, un rol de usuario puede usar el comando `tracert`, pero no el comando `ping` si el rol de usuario contiene reglas configuradas usando los siguientes comandos:

```
rule 1 permit command ping
rule 2 permit command tracert
rule 3 deny command ping
```

- Si una regla de rol de usuario predefinida (ver sección 6.3.3.1) y una regla de rol de usuario definida por el usuario entran en conflicto, la regla de rol de usuario definida por el usuario tiene efecto.

102. Las siguientes directrices se aplican a las reglas OID:

- El sistema compara un OID con los OID especificados en las reglas de roles de usuario, y utiliza el principio de coincidencia más larga para seleccionar una regla para el OID. Por ejemplo, un rol de usuario no puede acceder al nodo MIB con OID 1.3.6.1.4.1.25506.141.3.0.1 si el rol de usuario contiene reglas configuradas utilizando los siguientes comandos:

```
rule 1 permit read write oid 1.3.6
rule 2 deny read write oid 1.3.6.1.4.1
rule 3 permit read write oid 1.3.6.1.4
```

- Si el mismo OID está especificado en múltiples reglas, la regla con el ID más alto tiene efecto. Por ejemplo, un rol de usuario puede acceder al nodo MIB con OID 1.3.6.1.4.1.25506.141.3.0.1 si el rol de usuario contiene reglas configuradas utilizando los siguientes comandos:

```
rule 1 permit read write oid 1.3.6
rule 2 deny read write oid 1.3.6.1.4.1
rule 3 permit read write oid 1.3.6.1.4.1
```

103. Para configurar las reglas de un rol de usuario seguir los siguientes pasos:

1. Entrar en la vista del rol correspondiente:
2. Configurar las reglas para el rol, un rol creado por el administrador por defecto no tiene ninguna regla, se pueden añadir un máximo de 256 reglas utilizando uno de los siguientes comandos:

```
rule number { deny | permit } command command-string

rule number { deny | permit } { execute | read | write } *
feature [ feature-name ]

rule number { deny | permit } { execute | read | write } *
feature-group feature-group-name

rule number { deny | permit } { execute | read | write } * xml-
element [ xml-string ]

rule number { deny | permit } { execute | read | write } * oid
oid-string
```

6.3.3.4 CONFIGURACIÓN DE POLITICAS DE ACCESO A RECURSOS

104. Se pueden configurar las políticas de un rol de usuario definido por el usuario o de un rol de usuario predefinido de nivel-n para limitar su acceso a interfaces, VLANs e instancias de VPN.

105. La configuración de la política solo tiene efecto en los usuarios que hayan iniciado sesión con el rol de usuario después de la configuración.

106. Cada rol de usuario tiene una política de interfaz, una política de VLAN y una política de instancia de VPN. Por defecto, estas políticas permiten a los roles de usuario acceder a cualquier interfaz, VLAN e instancia de VPN. Para restringir los accesos de los usuarios a estos recursos hay que seguir los siguientes pasos:

    1. Denegar el acceso a los recursos correspondientes utilizando uno de los siguientes comandos:

    ```
    interface policy deny
    vlan policy deny
    vpn-instance policy deny
    ```

    2. Una vez eliminados los accesos a un tipo de recurso (intreface, vlan, vpn-instance) se dará acceso a los recursos que el rol necesite acceso con utilizando uno de los siguientes comandos:

    ```
    permit interface interface-list
    permit vlan vlan-id-list
    permit vpn-instance vpn-instance-name&<1-10>
    ```

6.3.3.5 ASIGNACIÓN DE ROLES A USUARIOS

107. Cada usuario local tiene un rol de usuario predeterminado. Si este rol de usuario predeterminado no es adecuado, elimine el rol de usuario predeterminado.

108. Si un usuario local es el único usuario con el rol de usuario *security-audit*, el usuario no puede ser eliminado. El rol de usuario *security-audit* es mutuamente excluyente con otros roles de usuario:

    - Cuando asigna el rol de usuario *security-audit* a un usuario local, el sistema solicita confirmación para eliminar todos los demás roles de usuario del usuario.

- Cuando asigna otros roles de usuario a un usuario local que tiene el rol de usuario *security-audit*, el sistema solicita confirmación para eliminar el rol de usuario *security-audit* del usuario.

109. Para asignar un rol de usuario a un usuario local, se debe acceder a la vista del usuario en cuestión y ejecutar el comando:

```
authorization-attribute user-role role-name.
```

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

6.4.1 DESACTIVACIÓN DE PUERTOS NO UTILIZADOS

110. Los puertos físicos del dispositivo están habilitados por defecto. Para evitar el uso de los puertos que no están siendo utilizados **se deben deshabilitar administrativamente los puertos que no vayan a ser utilizados**.

111. Para desactivar un puerto habrá que acceder a la vista del puerto en cuestión mediante el comando *interface interface-type interface-number* y posteriormente ejecutar el comando *shutdown*.

112. A continuación, se muestra un ejemplo de cómo realizar esta operación:

```
<Sysname> system-view
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] shutdown
[Sysname-FortyGigE1/1/1] undo shutdown
```

6.4.2 PROTOCOLOS DE DESCUBRIMIENTO DE RED (LLDP)

113. El protocolo LLDP (Link Layer Discovery Protocol) es un protocolo de capa de enlace estándar utilizado para la descubierta de dispositivos en redes locales. Diseñado para ser usado en dispositivos de red.

114. LLDP permite a un dispositivo anunciar su identidad y capacidades en la red local, así como recibir información similar de otros dispositivos.

115. LLDP transmite detalles sobre la configuración y la estructura de la red, lo que podría ser útil para un atacante que busca entender la topología de la red y encontrar posibles puntos vulnerables.

116. Se recomienda desactivar este protocolo que por defecto se encuentra activado ejecutando el comando:

```
undo lldp global enable
```

117. Para más información consulte la sección “Configuring LLDP” del documento [H3C-doc].

6.4.3 VLAN

118. Una red ethernet tradicional es una red plana, donde todos los hosts están en el mismo dominio de difusión y conectados entre sí a través de hubs o switches. Un

hub es un dispositivo de la capa física sin la función de conmutación, por lo que reenvía el paquete recibido a todos los puertos.

119. Un switch es un dispositivo de la capa de enlace que puede reenviar el paquete según la dirección MAC del paquete. Sin embargo, cuando el switch recibe un paquete de difusión o un paquete unicast desconocido cuya dirección MAC no está incluida en la tabla de direcciones MAC del switch, reenviará el paquete a todos los puertos excepto al puerto de entrada del paquete. Además, un atacante podría suplantar la MAC de un host legítimo y el switch no tendría forma de averiguarlo.

120. Para evitar esto el dispositivo permite aislar el tráfico en distintas VLANs, cada una con un dominio de difusión propio. Los hosts en la misma VLAN se comunican entre sí como si estuvieran en una LAN. Sin embargo, los hosts en diferentes VLANs no pueden comunicarse entre sí directamente.

121. El dispositivo permite la división en VLANs por dos métodos distintos:

- **Basado en puerto:** la forma más simple de clasificar VLANs. Puedes aislar los hosts y dividirlos en diferentes grupos de trabajo virtuales asignando los puertos en el dispositivo que se conecta a los hosts a diferentes VLANs. Este método es fácil de implementar y gestionar, es aplicable a hosts con posiciones relativamente fijas. Los puertos asignados a una VLAN pueden configurarse de las siguientes formas:
    - Access: El puerto solo puede pertenecer a una VLAN. Suele utilizarse para conectar un host.
    - Trunk: El puerto puede pertenecer a varias VLAN. Puede enviar y recibir paquetes a múltiples VLANs, generalmente se utiliza para conectar otro switch.
    - Hybrid: El puerto puede pertenecer a varias VLAN. Puede enviar y recibir paquetes a múltiples VLANs, generalmente se utiliza para conectar otro switch o un host.
- **Basado en protocolo:** El switch puede analizar los paquetes recibidos sin asignar a una VLAN en el puerto y según las reglas definidas la plantilla de protocolo definida por el usuario, asignar automáticamente la VLAN correspondiente, de acuerdo con diferentes formatos de encapsulación y los valores de campos específicos. Así, los datos del protocolo específico se asignan automáticamente a la VLAN correspondiente para su transmisión.

122. En la siguiente sección se muestra cómo crear una VLAN basada en puertos. Para realizar otra configuración consulte la sección “Configuring VLANs” del documento [H3C-doc].

6.4.3.1 VLAN BASADA EN PUERTOS

123. Para configurar un VLAN basada en puertos primero hay que crear la VLAN y entrar en la vista de esta:

```
vlan vlan-id
```

124. Dentro de la vista de la VLAN se le puede, de forma opcional, asignar un nombre y una descripción:

```
name string
description string
```

6.4.3.1.1 CONFIGURAR LOS PUERTOS EN MODO ACCESS

125. Desde la vista de sistema, entrar en la vista del puerto ethernet:

```
interface interface-type interface-number
```

126. Configurar el puerto como tipo Access:

```
port link-type access
```

127. Asignar el puerto a la VLAN correspondiente:

```
port access vlan vlan-id
```

6.4.3.1.2 Configurar los puertos en modo Trunk

128. Desde la vista de sistema, entrar en la vista del puerto ethernet:

```
interface interface-type interface-number
```

129. Configurar el puerto como tipo Trunk:

```
port link-type trunk
```

130. Indicar las VLANs permitidas en este puerto:

```
port trunk permit vlan { vlan-id-list | all }
```

131. Asignar la VLAN por defecto:

```
port access vlan vlan-id
```

6.4.3.1.3 Configurar los puertos en modo Hybrid

132. Desde la vista de sistema, entrar en la vista del puerto ethernet:

```
interface interface-type interface-number
```

133. Configurar el puerto como tipo Trunk:

```
port link-type hybrid
```

134. Indicar las VLANs permitidas en este puerto:

```
port hybrid vlan vlan-id-list { tagged | untagged }
```

135. Asignar la VLAN por defecto:

```
port hybrid pvid vlan vlan-id
```

6.5 CONFIGURTACIÓN IPSEC/IKE

136. El dispositivo, para su funcionamiento, puede delegar parte de su funcionalidad de seguridad en servidores externos. Estos servidores son:

- Network Time Server (NTP): Servidor que utiliza el dispositivo para actualizar su reloj de sistema. Esta información es fundamental para garantizar la correcta

asignación de hora y fecha a los eventos de seguridad generados por el dispositivo.

- Servidor de auditoría: Debido a la escasez de espacio de almacenamiento interno, el dispositivo debe hacer uso de un servidor de auditoría que almacene de forma definitiva los eventos de auditoría.
- Servidor de autenticación: El dispositivo puede delegar la autenticación a un servidor de autenticación.

137. **La comunicación entre estos servidores y el dispositivo se protegerá mediante IPsec/IKEv2.**

6.5.1 PROPIEDADES CRIPTOGRÁFICAS DEL INTERCAMBIO DE CLAVES (IKE PROPOSAL)

138. Una propuesta IKE (IKE proposal) define un conjunto de atributos que describen cómo debe tener lugar la negociación IKE. Esta negociación es el primer paso que se realiza durante la creación de un túnel IPSec entre dos extremos.
139. Puede crear varias propuestas IKE con diferentes prioridades. La prioridad de una propuesta IKE se representa por su número de secuencia. Cuanto menor sea el número de secuencia, mayor será la prioridad.
140. Dos pares deben tener al menos una propuesta IKE coincidente para una negociación IKE exitosa. Durante la negociación IKE:
    1. El iniciador envía sus propuestas IKE al otro extremo de la comunicación.
    2. El otro extremo busca en sus propias propuestas IKE una coincidencia.
    3. La búsqueda comienza desde la propuesta IKE con la prioridad más alta y procede en orden descendente de prioridad hasta que se encuentra una coincidencia. Las propuestas IKE coincidentes se utilizan para establecer la SA IKE.
    4. Dos propuestas IKE coincidentes tienen el mismo algoritmo de cifrado, método de autenticación, algoritmo de autenticación y grupo DH. El tiempo de vida de la SA toma el valor más pequeño de los ajustes de tiempo de vida de las dos propuestas.
141. Para realizar esta configuración, se utilizarán los siguientes comandos:
    - Creación de un “IKE proposal”:

```
ike proposal proposal-number
```

    - Establecer el algoritmo criptográfico:

```
encryption-algorithm { aes-gcm-128 | aes-gcm-192 | aes-gcm-256 }
```

    - Especificar el grupo Diffie-Hellman:

```
dh { group14 | group19 | group20 | group24 }
```

142. **Estas configuraciones deben cumplir con los requisitos definidos en la sección 6.2.2.**

6.5.2 PROPIEDADES CRIPTOGRÁFICAS DEL TUNEL IPSEC (TRANSFORM SET)

143. Tras la negociación IKE donde se produce el intercambio de claves entre los dos puntos de la conexión, el dispositivo y el otro extremo de la comunicación montan el túnel IPsec.

144. En este punto hay que definir los algoritmos utilizados para el cifrado, integridad y autenticación de la información en tránsito.

145. Estas propiedades se definen un "IPsec transform set". En el dispositivo puede existir distintos "IPsec transform set" creados por el usuario. Por defecto no hay ninguno creado.

146. Para realizar esta configuración se utilizan los siguientes comandos:

    1. Crear un "IPsec transform set" y asignarle un nombre:

```
ipsec transform-set transform-set-name
```

    2. Identificar el protocolo IPsec (el único permitido es ESP y es la configuración por defecto):

```
protocol { ah | ah-esp | esp }
```

147. Especificar el algoritmo de cifrado para ESP:

```
esp encryption-algorithm { gcm-128 | gcm-192 | gcm-256 }
```

148. Especificar el grupo Diffie-Hellman:

```
pfs { dh-group14 | dh-group19 | dh-group20 | dh-group24 }
```

149. **Estas configuraciones deben cumplir con los requisitos definidos en la sección 6.2.2.**

6.5.3 CONFIGURANDO UN PERFIL IKE (IKE PROFILE)

150. Por otro lado, un perfil IKE es un conjunto de parámetros de configuración que se utilizan para establecer una Asociación de Seguridad (SA) en la suite de protocolos IPsec.

151. Un perfil IKE puede contener uno o más IKE proposals (ver sección 6.5.1), así como otros parámetros de configuración, como la dirección IP del dispositivo remoto, el tiempo de vida de la SA y otros parámetros.

152. Para crear un perfil IKE se realizarán las siguientes acciones:

    1. Crear un perfil IKE (por defecto no hay ninguno creado):

```
ike profile profile-name
```

    2. Configurar la identificación del extremo remoto:

```
match remote { certificate policy-name | identity { address { {
ipv4-address [ mask | mask-length ] | range low-ipv4-address high-
```

```
ipv4-address } | ipv6 { ipv6-address [ prefix-length ] | range
low-ipv6-address high-ipv6-address } } [ vpn-instance vpn-name ] |
fqdn fqdn-name | user-fqdn user-fqdn-name } }
```

3. Establecer el tiempo de vida de SA:

```
sa duration { seconds }
```

4. Establecer el método de autenticación:

```
authentication-method { ecdsa-signature | pre-share | rsa-
signature }
```

5. Especificar si la negociación es mediante clave compartida (sección 6.5.5) o certificados (sección 6.5.6):

```
keychain keychain-name
certificate domain domain-name
```

6. Asignar los IKE proposals (sección 6.5.1) que estarán disponibles para la negociación:

```
proposal proposal-number&<1-6>
```

7. Configurar la identificación del dispositivo (por defecto se utilizará la configurada en *system-view* y si tampoco está configurará esta, se utiliza la IP del interfaz):

```
identity local { address { ipv4-address | ipv6 ipv6-address } | dn
| email email-string | fqdn fqdn-name | key-id key-id-string }
```

6.5.4 ESTABLECIMIENTO DE LOS TUNELES IPSEC (IPSEC POLICY)

153. Definidos en los pasos anteriores los requisitos criptográficos para el intercambio de claves y la generación del túnel IPsec, en este apartado definiremos los extremos de la comunicación. Esta configuración se hace mediante una "IPsec Policy".

154. La política se asignará a un Access Control List (ACL). Un ACL es un conjunto de reglas para identificar el tráfico basado en criterios como la dirección IP de origen, la dirección IP de destino y el número de puerto. De esta forma se define el otro extremo de la comunicación (ej. Servidor de auditoría).

155. Como crear el ACL está fuera del ámbito de este documento. Consultar la sección "Configuring ACLs" del documento [H3C-doc].

156. Los pasos a seguir serán los siguientes:

1. Crear la política con el comando:

```
ipsec { ipv6-policy | policy } policy-name seq-number isakmp
```

2. Asignar un ACL para la política:

```
security acl [ ipv6 ] { acl-number | name acl-name } [ aggregation
| per-host ]
```

3. Asignar el "transform set" (ver sección 6.5.2):

```
transform-set transform-set-name
```

4. Asignar el “IKE profile” (ver sección 6.5.3):

```
ikev2-profile profile-name
```

5. Configurar la IP origen y destino

```
local-address { ipv4-address | ipv6 ipv6-address }
remote-address { [ ipv6 ] host-name | ipv4-address | ipv6 ipv6-
address }
```

6. Establecer los criterios de refresco del material criptográfico (duración de la SA, 8 horas, a parte su tiempo de vida será limitado a un máximo de 100MB transmitidos):

```
ipsec sa global-duration { time-based seconds | traffic-based
kilobytes }
```

6.5.5 AUTENTICACIÓN MEDIANTE CLAVE PREVIAMENTE COMPARTIDA (PSK)

157. La configuración de IPsec se puede hacer mediante clave previamente compartida. De este modo se crea una contraseña que se introduce en los dos dispositivos sobre los que se quiere establecer la comunicación a través de IPsec.

158. Como el dispositivo puede conectarse múltiples servicios y cada uno de estos canales tendrá una IKEv2 keychain. Para crear una keychain se utilizará el comando:

```
ikev2 keychain “keychain-name”
```

159. Ahora hay que crear el extremo de la conexión que representa al servicio con el que se quiere conectar. Para esto se utiliza el comando:

```
peer “peer-name”
```

160. Una vez creado el extremo de la conexión del servicio, hay que configurar su direccionamiento utilizando el comando:

```
address { ipv4-address [ mask | mask-length ] | ipv6 ipv6-
address [ prefix-length ] }
```

161. Para identificar al servicio se le puede asignar una IP, DNS, correo electrónico, o identificador de contraseña:

```
identity { address { ipv4-address | ipv6 { ipv6-address } } |
fqdn fqdn-name | email email-string | key-id key-id-string }
```

162. Finalmente se especifica la clave previamente compartida, que deberá ser utilizada en el servicio correspondiente para generar el túnel IPsec:

```
pre-shared-key [ local | remote ] { ciphertext | plaintext }
string
```

6.5.6 AUTENTICACIÓN MEDIANTE CERTIFICADOS

163. Para realizar la autenticación con certificados, primero hay que crear y configurar un dominio PKI, para esto seguir los pasos indicados en la sección 6.6.

164. El dominio PKI creado será el utilizado en el paso 3 del párrafo 152 de la sección 6.5.3.

165. Las políticas del dominio PKI generadas mediante el procedimiento definido en la sección 6.6.10 serán las utilizadas a la hora de definir el túnel IPSEC en el paso 2 del párrafo 156 de la sección 6.5.4.

166. Tras esta configuración, las comunicaciones entre el dispositivo y los extremos configurados serán protegida mediante certificados. Seguir los procedimientos de gestión de certificados de la sección 6.6 para mantener los certificados actualizados.

6.6 GESTIÓN DE CERTIFICADOS

167. La gestión de certificados se realiza mediante los dominios PKI, la configuración de estos se encuentra en el manual “configuring PKI” del manual [H3C-doc].

168. En el manual se distinguen dos tipos de certificados, los certificados de las CAs (CA certificate o certificados de CA) y los certificados expedidos por estas (local certificate o certificados locales). En estos documentos mantendremos esta nomenclatura.

169. En esta sección se muestran los pasos relevantes a tener en cuenta para realizar la gestión de los certificados:

    1. Configuración del Entity Name Space del dispositivo (necesario).
    2. Creación del dominio PKI y configuración de sus parámetros (necesario).
    3. Petición de certificado PKI para el dispositivo (necesario).
    4. Obtener un certificado manualmente (opcional).
    5. Configurar la validación PKI (opcional).

170. También se explicará como destruir el par de claves del dispositivo (en caso de que se sospeche de la perdida de confidencialidad de la clave privada) y el borrado de un certificado de forma manual si ya no se confía en el mismo.

171. El dispositivo tiene una ruta de almacenamiento predeterminada para certificados y CRLs. Se puede cambiar la ruta de almacenamiento y especificar rutas diferentes para los certificados y CRLs. Después de cambiar la ruta de almacenamiento, los archivos de certificado (con la extensión .cer o .p12) y los archivos de CRL (con la extensión .crl) en la ruta original se mueven a la nueva ruta. Para hacer este cambio se utiliza el comando:

```
pki storage { certificates | crls } dir-path
```

6.6.1 CONFIGURACIÓN DEL ENTITY NAME SPACE DEL DISPOSITIVO

172. El *Entity Name Space* se refiere a una colección de atributos utilizados para identificar a una entidad. Una CA utiliza el *Distinguished-Name* (DN) para esta función.

173. En el dispositivo se pueden configurar hasta un máximo de dos DNs, ya que se pueden crear dos dominios PKI.

174. Los pasos a seguir son los siguientes:

1. Crear un *Entity Name Space* y entrar en su vista (para configurarlo):

```
pki entity name
```

2. Poner los distintos parámetros del *Distinguished-Name*:

```
common-name name
country country-code-str
fqdn name-str
ip ip-address
organization org-name
organization-unit org-unit-name
state state-name
```

6.6.2 CREACIÓN DEL DOMINIO PKI Y CONFIGURACIÓN DE SUS PARÁMETROS

175. El dispositivo solo permite crear dos dominios PKI, si ya hay dos dominios creados, habrá que eliminar uno. El comando para crear un dominio PKI y entrar en su vista es:

```
pki domain name
```

176. Una vez dentro de la vista del dominio PKI, el siguiente paso será configurar sus parámetros, antes de poder pedir la expedición de un certificado para el dispositivo. Para configurar los parámetros se seguirán los siguientes pasos:

1. Asignar un nombre a la CA. La CA es una entidad de confianza cuya función es expedir los certificados cuando se realiza un “certificate request”.

```
ca identifier name
```

2. Indicar la URL donde se debe enviar la orden de “certificate request”. Esta URL suele ser de la CA, aunque esta acción puede estar delegada a una RA (Registration Authority):

```
certificate request url url-string
```

3. Indicar el hash (fingerprint) del certificado raíz de la CA para comprobar la autenticidad del certificado. Se recomienda que el hash sha256 o superior, pero esto dependerá de la configuración de la CA:

```
root-certificate fingerprint hash-algorithm string
```

4. Especificar si la URL definida en el paso anterior pertenece a una CA o RA:

```
certificate request from { ca | ra }
```

5. Configuración del servidor LDAP, para tener actualizado el estado de revocación de los certificados:

```
ldap-server ip ip-address [ port port-number ] [ version
version-number ]
```

8. Definir los algoritmos criptográficos utilizados para generar el par de claves del dispositivo que será utilizado para que la CA genere el certificado correspondiente. **Estas configuraciones deben cumplir con los requisitos definidos en la sección 6.2.2:**

```
RSA
public-key rsa { { encryption name encryption-key-name [
length key-length ] | signature name signature-key-name [
length key-length ] } * | general name key-name [ length
key-length ] }

ECDSA
public-key ecdsa name key-name [ secp192r1 | secp256r1 |
secp384r1 | secp521r1 ]
```

6.6.3 SOLICITUD DE CERTIFICADO PKI PARA EL DISPOSITIVO

177. La solicitud de certificado es un proceso mediante el cual una entidad se presenta a una Autoridad de Certificación (CA). Una entidad proporciona a la CA su identidad y la correspondiente clave pública.

178. Una entidad puede presentar una solicitud de certificado a la CA de dos maneras: online y offline. En modo offline, una entidad puede enviar una solicitud a la CA por medios externos (por ejemplo, por teléfono, disco o correo electrónico).

179. La solicitud de certificado online se divide en dos categorías: manual y automática.

180. En la solicitud automática permite indicar la longitud de la clave, pero no los algoritmos empleados, ya que dependen de las suites de cifrado configuradas en la CA. Utilizar esta opción únicamente cuando las suites de cifrado son compatibles con los requisitos criptográficos definidos en la sección 6.2.2.

181. A continuación, se muestran la opción online automática y manual.

6.6.3.1 SOLICITUD DE CERTIFICADO PKI OFFLINE

182. Mediante este método, la solicitud de certificado se envía utilizando un canal offline, como teléfono, disco o correo electrónico. Puede utilizar este modo por motivos operacionales (ej. La CA no lo permite) o si no logra solicitar un certificado online. Los pasos a seguir serán los siguientes:

1. Imprimir la información de petición en la consola o guardarla en un fichero utilizando los comandos:

```
pki request-certificate domain pkcs10 (imprimir en consola)
pki request-certificate domain pkcs10 filename (volcar a
fichero)
```

2. Mandar la información en texto o en un fichero a la CA siguiendo los procedimientos indicados por esta.

6.6.3.2 SOLICITUD DE CERTIFICADO PKI ONLINE AUTOMATICAMENTE

183. En modo automático, una entidad solicitará automáticamente un certificado a través del protocolo SCEP en ausencia de un certificado local. Además, solicitará automáticamente un nuevo certificado cuando el existente esté a punto de caducar.

184. **Esta opción solo se puede utilizar cuando la ciphersuite de la CA cumpla con los requisitos definidos en la sección 6.2.2.**

185. Los pasos a seguir se definen a continuación:

1. Entrar en el dominio PKI correspondiente:

```
pki domain name
```

2. Ejecutar el comando para la solicitud automática del certificado, indicando la contraseña de revocación:

```
certificate request mode auto [ key-length key-length |
password { cipher | simple } password ] *
```

6.6.3.3 SOLICITUD DE CERTIFICADO PKI ONLINE MANUALMENTE

186. En modo manual, una entidad necesita obtener un certificado de CA, generar un par de claves local y solicitar el certificado manualmente. El objetivo de obtener un certificado de CA es verificar la autenticidad y validez del certificado a generar. **La fortaleza del par de claves del certificado será el definido en la sección 6.6.2**.

187. La generación de un par de claves es clave para la solicitud de certificado. La clave privada es mantenida por el dispositivo, mientras que la clave pública y otra información se transfieren a la CA para firmar un certificado. Siga estos pasos para configurar el envío de una solicitud de certificado manualmente:

1. Entrar en el dominio PKI correspondiente:

```
pki domain name
```

2. Indicar que se desea realizar esta operación de forma manual:

```
certificate request mode manual
```

3. Desde la vista de sistema obtener el certificado según se describe en la sección 6.6.4 de este documento.

4. Generar la petición de certificado de forma manual con el comando mostrado a continuación:

```
pki request-certificate domain domain-name [ password
password ] [ pkcs10 [ filename filename ] ]
```

6.6.4 OBTENER UN CERTIFICADO

188. Puede obtener el certificado de la CA, los certificados locales y los certificados de pares relacionados con un dominio PKI de una CA y guardarlos localmente para una mayor eficiencia de búsqueda. Para hacerlo, se puede utilizar el modo online y offline:

189. Modo offline: En este modo, se deben obtener los certificados por medios externos como FTP, disco o correo electrónico, y luego importarlos localmente. Utilice este modo cuando el repositorio de CRL no esté especificado o el servidor de la CA no admita SCEP. El comando utilizado para esta operación es:

```
pki retrieve-certificate domain domain-name { ca | local |
peer entity-name }
```

190. Modo online: En este modo, se obtiene el certificado de la CA a través de SCEP y los certificados locales o certificados de pares a través de LDAP. El comando utilizado para esta operación es:

```
pki import domain domain-name { der { ca | local | peer }
filename filename | p12 local filename filename | pem { ca
| local | peer } [ filename filename ] }
```

6.6.5 VERIFICACIÓN DE CERTIFICADOS

191. Un certificado se verifica automáticamente cuando es solicitado, obtenido o utilizado por una aplicación. Si el certificado expira, si no es emitido por una CA de confianza, o si ha sido revocado, el certificado no puede ser utilizado.

192. También puede verificar manualmente un certificado. Si ha sido revocado, no se puede solicitar ni obtener el certificado.

6.6.6 VERIFICACIÓN MEDIANTE CRL

193. Para utilizar la verificación mediante CRL (Lista de Revocación de Certificados), se debe obtener la información de revocación de un repositorio de CRL. El dispositivo selecciona el repositorio de CRL en el siguiente orden:

    1. Repositorio de CRL especificado en el dominio PKI.
    2. Repositorio de CRL en el certificado que está siendo verificado.
    3. Repositorio de CRL en el certificado de la CA o repositorio de CRL en el certificado de la CA de nivel superior si el certificado de la CA es el certificado que se está verificando.

194. Si no se encuentra ningún repositorio de CRL después del proceso de selección, el dispositivo obtiene el CRL a través de SCEP. En este escenario, el certificado de la CA y los certificados locales deben haber sido obtenidos.

195. Al verificar el certificado de la CA de un dominio PKI, el sistema necesita verificar todos los certificados en la cadena de certificados de la CA del dominio. Para asegurar un proceso exitoso de verificación de certificados, el dispositivo debe

contener todos los dominios PKI a los que pertenecen los certificados de la CA en la cadena de certificados.

196. Cada certificado de la CA contiene un campo de emisor que identifica a la CA padre que emitió el certificado. Después de identificar el certificado padre de un certificado, el sistema localiza los dominios PKI a los que pertenece el certificado padre. Si la verificación de CRL está habilitada para los dominios, el sistema verifica si el certificado de la CA ha sido revocado o no. El proceso continúa hasta que se alcanza el certificado de la CA raíz. El sistema verifica que cada certificado de la CA en la cadena de certificados sea emitido por la CA padre nombrada, comenzando desde la CA raíz.

197. Los pasos a seguir para realizar la verificación de certificados son los siguientes:

1. Desde la vista del sistema entrar en el dominio PKI correspondiente:

```
pki domain domain-name
```

2. Especificar la URL del repositorio CRL (en caso contrario se utilizará la configurada en la sección 6.6.2):

```
crl url url-string [ vpn-instance vpn-instance-name ]
```

3. Permitir la comprobación mediante CRL:

```
crl check enable
```

4. Salir de la vista del dominio pki a la vista del sistema y obtener el certificado de la CA como se indica en la sección 6.6.4.

5. Obtener la CRL y guardarla en el dispositivo:

```
pki retrieve-crl domain domain-name
```

6. Verificar la validez de los certificados:

```
pki validate-certificate domain domain-name { ca | local }
```

6.6.7 VERIFICACIÓN MANUAL

198. Para realizar verificación sin una CRL seguir los siguientes pasos:

1. Entrar en la vista de dominio PKI:

```
pki domain domain-name
```

2. Deshabilitar el chequeo por CRL:

```
undo crl check enable
```

3. Salir de la vista del dominio pki a la vista del sistema y obtener el certificado de la CA como se indica en la sección 6.6.4.

4. Verificar la validez de los certificados:

```
pki validate-certificate domain domain-name { ca | local }
```

6.6.8 EXPORTAR UN CERTIFICADO

199. Se pueden exportar el certificado de la CA y los certificados locales de un dominio PKI a archivos de certificado. Los archivos de certificado exportados se pueden importar de nuevo al dispositivo u otras aplicaciones PKI.

200. Al exportar un certificado local con el par de claves RSA, el nombre del archivo de destino puede ser diferente al nombre de archivo especificado con la palabra clave filename. Esto depende del propósito del par de claves del certificado.

201. Los certificados se pueden exportar en formatos DER, PKCS12 y PEM. **En los formatos en los que se incluye la clave privada utilizar una contraseña suficientemente compleja**. Los comandos para los distintos formatos son los siguientes:

```
pki export domain domain-name der { all | ca | local } filename
filename

pki export domain domain-name p12 { all | local } passphrase

pki export domain domain-name pem { { all | local } [ { aes-
128-cbc | aes-192-cbc | aes-256-cbc } pempasswordstring ] | ca
} [ filename filename ]
```

6.6.9 ELIMINAR UN CERTIFICADO

202. Se puede eliminar el certificado de la CA, el certificado local o los certificados de pares en un dominio PKI. Después de eliminar el certificado de la CA, el sistema elimina automáticamente los certificados locales, los certificados de pares y los CRLs en el dominio.

203. Se debe eliminar un certificado local y solicitar uno nuevo cuando **el certificado local esté a punto de caducar o la clave privada del certificado esté comprometida**. Para eliminar un certificado local y solicitar un nuevo certificado, se deben realizar las siguientes tareas:

    1. Eliminar el certificado local.
    2. Utilizar el comando `public-key local destroy` para destruir el par de claves local existente.
    3. Utilizar el comando `public-key local create` para generar un nuevo par de claves.
    4. Solicitar un nuevo certificado.

204. Para borrar un certificado se utilizará el comando:

```
pki delete-certificate domain domain-name { ca | local | peer [
serial serial-num ] }
```

6.6.10 POLITICA DE CONTROL DE ACCESO BASADA ENCERTIFICADOS

205. Las políticas de control de acceso basadas en certificados permiten autorizar el acceso a un dispositivo (por ejemplo, un servidor de autenticación a través de IPsec) basándose en los atributos del certificado de un cliente autenticado.

206. Una política de control de acceso basada en certificados es un conjunto de reglas de control de acceso (declaraciones de permitir o denegar), cada una asociada con un grupo de atributos de certificado. Un grupo de atributos de certificado contiene múltiples reglas de atributos, cada una definiendo un criterio de coincidencia para un atributo en el nombre del emisor del certificado, el nombre del sujeto o el campo de nombre alternativo del sujeto.

207. Si un certificado coincide con todas las reglas de atributos en un grupo de atributos de certificado asociado con una regla de control de acceso, el sistema determina que el certificado coincide con la regla de control de acceso. En este escenario, el proceso de coincidencia se detiene y el sistema realiza la acción de control de acceso definida en la regla de control de acceso.

208. Las siguientes condiciones describen cómo una política de control de acceso basada en certificados verifica la validez de un certificado:

    1. Si un certificado coincide con una regla de tipo permitir, el certificado pasa la verificación.
    2. Si un certificado coincide con una regla de tipo denegar o no coincide con ninguna declaración en la política, el certificado se considera inválido.
    3. Si una regla está asociada con un grupo de atributos inexistente, o el grupo de atributos no tiene reglas de atributos, el certificado coincide con la regla.
    4. Si la política de control de acceso basada en certificados referenciada por una aplicación de seguridad (por ejemplo, HTTPS) no existe, todos los certificados en la aplicación pasan la verificación.

209. Para configurar la política de control de acceso basada en certificados se procederá de la siguiente manera:

    1. Crear un grupo de atributos de certificado desde la vista de sistema:

    ```
    pki certificate attribute-group group-name
    ```

    2. Crear reglas para filtrar por atributos de los certificados:

    ```
    attribute id { alt-subject-name { fqdn | ip } | { issuer-name |
    subject-name } { dn | fqdn | ip } } { ctn | equ | nctn | nequ}
    attribute-value
    ```

    3. Volver a la vista de sistema y crear una política PKI basada en certificados:

    ```
    pki certificate access-control-policy policy-name
    ```

    4. Crear las distintas reglas para el grupo en cuestión:

    ```
    rule [ id ] { deny | permit } group-name
    ```

210. Para una configuración más avanzada puede consultar la sección “Configuring PKI” del documento [H3C-doc].

6.7 SERVIDORES DE AUTENTICACIÓN

211. **Las comunicaciones entre el dispositivo y el servidor de autenticación deben de ser protegidas utilizando el protocolo IPsec (ver sección 6.5).**

212. El dispositivo permite el uso de servidores de autenticación que utilicen los protocolos RADIUS (estándar o extendido) y HWTACACS.

213. En esta sección se muestran los pasos fundamentales para configurar el dispositivo para utilizar servidores de autenticación. Puede encontrar información más detallada en la sección “Configuring AAA” del documento [H3C-doc].

6.7.1 CREACIÓN DE UN DOMINIO ISP

214. Un Internet Service Provider (ISP) agrupa un conjunto de usuarios que pertenecen al mismo ISP. Para un nombre de usuario con formato “userid@isp-name”, isp-name es el nombre del dominio ISP.

215. El dispositivo de acceso utiliza userid como el nombre de usuario para la autenticación y isp-name como el nombre del dominio.

216. En un entorno multi-ISP, los usuarios conectados al mismo dispositivo pueden pertenecer a diferentes dominios. Debido a que los usuarios de diferentes ISPs pueden tener diferentes atributos (como diferentes nombres de usuario y contraseña, diferentes permisos), es necesario distinguir a los usuarios estableciendo dominios ISP.

217. Se puede configurar un conjunto de atributos de dominio ISP (por ejemplo, el esquema RADIUS o HWTACACS) para cada dominio ISP de forma independiente en la vista de dominio ISP.

218. En las secciones 6.7.2 y 6.7.3 se definirá en el proceso de configuración del servidor RADIUS o HWTACACS los pasos a tomar para asignar los esquemas a un ISP.

219. Para crear un dominio ISP se ejecutará el siguiente comando desde la vista de sistema:

```
domain { isp-name | default { disable | enable isp-name } }
```

6.7.2 UTILIZACIÓN DE UN SERVIDOR RADIUS

220. El protocolo RADIUS se configura mediante esquemas, puede haber varios esquemas RADIUS en un dispositivo. Para utilizar un servidor RADIUS seguir los siguientes pasos:

    1. Primero debe crear un esquema RADIUS y entrar en su vista antes de realizar otras configuraciones del protocolo RADIUS mediante el comando:

```
radius scheme radius-scheme-name
```

2. A continuación, se han de configurar la dirección de red y puerto del servidor RADIUS primario:

```
primary authentication ip-address [ port-number ]
```

3. De forma opcional, se puede configurar la dirección de red y puerto del servidor RADIUS secundario:

```
secondary authentication ip-address [ port-number ]
```

4. Ir a la vista del dominio ISP (ver sección 6.7.1) para configurar el esquema RADIUS al dominio:

```
domain domain-name
```

5. Configurar los servicios de autenticación y autorización del dominio al esquema RADIUS:

```
authentication login radius-scheme radius-scheme-name
authorization login radius-scheme radius-scheme-name
```

6.7.3 UTILIZACIÓN DE UN SERVIDOR HWTACACS

221. El protocolo HWTACACS se configura mediante esquemas, puede haber varios esquemas HWTACACS en un dispositivo.

222. El protocolo HWTACACS requiere de dos servidores de autenticación, uno primario y otro secundario (en RADIUS el servidor secundario es opcional). El dispositivo rechazará la configuración, si las direcciones IP de los servidores primario y secundario coinciden.

223. Para utilizar un servidor HWTACACS seguir los siguientes pasos:

1. Primero debe crear un esquema HWTACACS y entrar en su vista antes de realizar otras configuraciones del protocolo HWTACACS mediante el comando:

```
hwtacacs scheme hwtacacs-scheme-name
```

2. A continuación, se han de configurar la dirección de red y puerto del servidor HWTACACS de autenticación primario:

```
primary authentication ip-address [ port ]
```

3. Obligatoriamente se ha de configurar la dirección de red y puerto del servidor HWTACACS autenticación secundario:

```
secondary authentication ip-address [ port ]
```

4. Configurar la dirección de red y puerto del servidor HWTACACS autorización primario:

```
primary authorization ip-address [ port ]
```

5. Obligatoriamente se ha de configurar la dirección de red y puerto del servidor HWTACACS autorización secundario:

```
secondary authorization ip-address [ port ]
```

6. Ir a la vista del dominio ISP (ver sección 6.7.1) para configurar el esquema RADIUS al dominio:

```
domain domain-name
```

7. Configurar los servicios de autenticación y autorización del dominio al esquema HWTACACS:

```
authentication login hwtacacs-scheme hwtacacs-scheme-name
authorization login hwtacacs-scheme hwtacacs-scheme-name
```

6.8 SINCRONIZACIÓN

224. Para el correcto registro de los eventos de auditoría, la fecha y hora debe de ser precisa. Los dispositivos utilizan el reloj de sistema como fuente esta información.

225. Cuando el dispositivo está apagado, este mantiene la hora mediante relojes de tiempo real, los cuales son utilizados para actualizar el reloj de sistema en el arranque.

226. El administrador puede configurar manualmente la fecha y hora del dispositivo o configurar un servidor NTP para que proporcione esta información.

6.8.1 CONFIGURACIÓN DEL RELOJ INTERNO

227. Para configurar el reloj interno de forma manual y sin actualización mediante NTP utilizar los siguientes comandos:

```
[Sysname] clock protocol none
<Sysname> clock datetime HH:MM:SS MM/DD/YYYY
```

228. Para más información, ver la sección “Managing the device” del documento [H3C-doc].

6.8.2 SINCRONIZAR CON UN NTP

229. Si desea utilizar un NTP para mantener actualizado el reloj de sistema la configuración se realizará de la siguiente manera:

```
[Sysname] clock protocol ntp
[Sysname] ntp-service enable
[Sysname] ntp-service unicast-server X.X.X.X
```

230. Para más información ver la sección “Configuring NTP” del documento [H3C-doc].

6.9 ACTUALIZACIONES

231. El dispositivo está diseñado para admitir actualizaciones del programa de ROM de arranque y del archivo de arranque del sistema, así como para admitir hotfixes de software.

232. El dispositivo proporciona interfaces para que un administrador pueda consultar las versiones actuales del programa de ROM de arranque o del archivo de arranque del sistema, así como identificar cualquier parche instalado.

233. Tanto el programa de ROM de arranque como el archivo de arranque del sistema pueden actualizarse a través del menú de arranque o de la interfaz de línea de comandos, pero se requiere un reinicio en cada caso.

234. Los hotfixes solo pueden afectar al archivo de arranque del sistema, se pueden instalar a través de la interfaz de línea de comandos y no requieren un reinicio para ser efectivos.

6.9.1 VERIFICACIÓN DE LAS ACTUALIZACIONES

235. El dispositivo verifica las actualizaciones, previamente a hacer cualquier modificación en el mismo.

236. El dispositivo incluye una función de comprobación de validez que puede activarse al actualizar el programa de ROM de arranque, mientras que los archivos de arranque del sistema y los parches de software siempre se validan antes de la instalación.

237. Más específicamente, cada actualización incluye un encabezado y datos. El encabezado incluye un hash SHA-256 de los datos que está firmado por H3C. Para verificar los datos, el dispositivo genera su propio hash SHA-256 de los datos de actualización, lo compara con el hash firmado en el encabezado de la actualización para asegurarse de que coincidan y verifica la firma del hash utilizando su clave pública incluida de fábrica.

238. Existen distintos métodos para actualizar los dispositivos y estos pueden variar de un modelo a otro. Consulte el documento [H3C-fund].

6.10 AUTO-CHEQUEOS

239. Los auto-chequeos están disponibles en el modo FIPS (sección 6.1) que es requerido para el funcionamiento seguro del dispositivo.

240. Estos auto-chequeos son mecanismos de prueba diseñados para asegurar el correcto funcionamiento de los módulos criptográficos. Estos incluyen pruebas que se ejecutan automáticamente al encender el dispositivo (power-up self-test) y cuando una determinada funcionalidad es invocada (conditional self-test). Los *power-up self-test*, también se puede iniciar su ejecución de forma manual (ver sección 6.10.1).

241. Si los *power-up self-test* fallan, **el dispositivo se reinicia**. En caso de fallar un *conditional self-test* el sistema **muestra un mensaje de fallo**. En caso de que un self-test falle, contactar con el fabricante.

242. **Power-up Self-Tests**: Estas pruebas examinan la disponibilidad de algoritmos criptográficos permitidos por FIPS. Los tipos de pruebas de encendido que soporta el dispositivo son:

- Known-answer test (KAT): Un algoritmo criptográfico se ejecuta en datos para los cuales se conoce la salida correcta. Si la salida calculada no coincide con la respuesta conocida, la prueba KAT falla.
- Pairwise conditional test (PWCT): Se utiliza para probar algoritmos asimétricos. Se comprueba que las claves y el algoritmo de cifrado mantienen sus capacidades fundamentales
    - El sistema usa la clave privada para firmar datos específicos y luego la clave pública para autenticar los datos firmados.
    - El sistema utiliza la clave pública para encriptar un texto plano y luego la clave privada para desencriptar el texto encriptado.

243. **Conditional Self-Tests:** Estas pruebas se realizan cuando se invoca un módulo criptográfico asimétrico o un módulo generador de números aleatorios. Las pruebas que se realizan son las siguientes:

- Pairwise conditional test (PWCT): Mencionadas en el párrafo anterior. Se ejecutan al utilizar el módulo criptográfico asimétrico.
- Prueba de continuidad del generador de números aleatorios: El sistema compara el número generado con el número aleatorio generado previamente. Si ambos números son iguales, la prueba falla.

6.10.1 EJECUCIÓN MANUAL DE AUTO-CHEQUEOS

244. Para realizar manualmente los "self-tests", seguir estos pasos:

1. Entra en la vista del sistema: Debes estar en el modo de configuración del sistema. Para esto, utiliza el comando `system-view`.
2. Activa los self-tests: Ejecuta el comando `fips self-test` para iniciar las pruebas.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

245. Los logs de seguridad son importantes a la hora de localizar y solucionar problemas de seguridad. Generalmente, la auditoría de seguridad se muestra junto a la auditoría al resto de logs de auditoría. Se recomienda que el administrador guarde los logs de auditoría en un fichero aparte.

246. Por defecto, todos los puertos del producto generan logs de auditoría por cada evento de tipo “link up/down”. El administrador puede desactivar la generación de estos logs con el comando “`undo enable log updown`” si considera esta información irrelevante o si pueden generar un **problema de disponibilidad**.

247. **Por defecto la auditoría de seguridad está deshabilitada, es obligatorio que el administrador habilite esta funcionalidad (sección 6.11.2).**

6.11.2 CONFIGURANDO LA AUDITORÍA DE SEGURIDAD

248. La auditoría de seguridad es obligatoria y por defecto viene desactivada. Para activar esta funcionalidad hay que ejecutar el comando:

```
info-center security-logfile enable
```

249. Tras activar la auditoría de seguridad, estos eventos se guardan de la siguiente manera:

    1. El sistema manda los eventos al buffer de eventos de seguridad.
    2. El sistema vuelca los eventos del buffer de eventos de seguridad al fichero de eventos de seguridad a intervalos de tiempo (el administrador puede realizar esta operación de manera manual con el comando `security-logfile save`).
    3. Tras volcar los eventos en el paso anterior el buffer de eventos de seguridad se limpia inmediatamente.

250. El intervalo de tiempo en el que el buffer de eventos se define con el comando:

```
info-center security-logfile frequency freq-sec
```

251. El tamaño máximo del fichero de eventos de seguridad se define mediante el comando:

```
info-center security-logfile size-quota size
```

252. El dispositivo solo permite un fichero de eventos de seguridad. Para evitar la pérdida de eventos, se puede poner una alarma cuando dicho fichero alcance un umbral de uso utilizando el comando "`info-center security-logfile alarm-threshold`".

253. Cuando el umbral de uso se sobrepasa, el sistema muestra un mensaje para informar al administrador. El administrador debe con el perfil `security-audit` hacer una copia del log de seguridad para evitar la pérdida de datos de auditoría.

254. Para ver el estado en el que se encuentra la auditoría de seguridad (tamaño máximo, localización del fichero, umbral de la alarma, espacio ocupado y frecuencia de escritura) se puede utilizar el siguiente comando:

```
<Sysname> display security-logfile summary
  Security log file: Enabled
  Security log file size quota: 10 MB
  Security log file directory: flash:/seclog
  Alarm threshold: 80%
  Current usage: 30%
  Writing frequency: 24 hour 0 min 0 sec
```

255. Para mostrar el contenido del log de seguridad se utilizará el comando:

```
more seclog/seclog.log
```

6.11.3 ALMACENAMIENTO LOCAL

256. Para configurar el registro de auditoría de forma local se deben seguir los siguientes pasos:

- Info-center logfile overwrite-protection: Este comando se utiliza para configurar la protección de sobreescritura para el archivo de registro.
- Info-center logfile directory**:** Este comando se utiliza para configurar el directorio de almacenamiento para el archivo de registro. Por ejemplo, si desea configurar el directorio de almacenamiento como "flash:/log", puede utilizar el siguiente comando: `info-center logfile directory flash:/log`.
- Info-center logbuffer: Este comando se utiliza para configurar el número de entradas que puede contener como máximo el registro de auditoría.

257. Por defecto, todos los puertos del producto generan logs de auditoría por cada evento de tipo "link up/down". El administrador puede desactivar la generación de estos logs con el comando "`undo enable log updown`" si considera esta información irrelevante o si pueden generar un problema de disponibilidad.

6.11.4 ALMACENAMIENTO REMOTO

258. El dispositivo, debido a sus limitaciones de espacio interno, permite el envío de registros de auditoría a un servidor externo syslog.

259. El canal de comunicación entre el dispositivo y el servidor de auditoría **se debe de proteger con IPsec**. Ver la sección 6.5 para ver cómo realizar esta configuración.

260. Para indicar al dispositivo la dirección IP del servidor de auditoría se tiene que utilizar el comando "`info-center loghost host-ipv4-address`".

261. Se puede configurar el formato en el que se quiere enviar la fecha y hora de los eventos al servidor remoto con el comando "`info-center timestamp loghost`". Los únicos valores permitidos serán:

- Formato de Fecha (Date): Este formato presenta la marca de tiempo como "Mmm dd hh:mm:ss:ms aaaa", por ejemplo, "Dec 8 10:12:21:708 2012". Aquí, "Mmm" es la abreviatura de tres letras del mes, "dd" es el día del mes, "hh:mm:ss:ms" representa horas, minutos, segundos y milisegundos, y "aaaa" es el año con cuatro dígitos.
- Formato ISO: El formato ISO 8601 es ampliamente utilizado por su representación inequívoca de fechas y horas. Un ejemplo de este formato es "2012-09-21T15:32:55". En este formato, la fecha (año-mes-día) va seguida de una 'T' para indicar el comienzo de la parte de la hora (hora:minuto:segundo).

6.12 BACKUP

262. Para garantizar la disponibilidad del servicio, es importante realizar copias de seguridad de la configuración del dispositivo. De esta forma, en caso de que el

dispositivo falle, este se pueda recuperar o cambiar por otro en el menor tiempo posible.

263. En la documentación del producto se definen cuatro métodos para hacer copias de seguridad de la configuración, sin embargo, hay dos métodos que **no están permitidos:**

- Copiar la configuración en CLI: ya que requiere editar la información de forma manual por parte del usuario.
- Utilizar FTP: porque la información puede ser transmitida en claro.

264. Para más información consultar la sección "Managing configuration files" del documento [H3C-doc].

265. Para hacer una copia de seguridad del archivo de configuración de un dispositivo, puede utilizar uno de los siguientes métodos.

6.12.1 COPIA DE SEGURIDAD EN UN MEDIO DE ALMACENAMIENTO

266. Después de que el dispositivo se inicie, ejecute los siguientes comandos para hacer una copia de seguridad del archivo de configuración en el medio de almacenamiento predeterminado del dispositivo:

```
<sysname> save config.cfg
<sysname> copy config.cfg backup.cfg
```

267. Para almacenar el archivo de configuración en otro medio de almacenamiento, debe especificar la ruta absoluta del medio de almacenamiento. Por ejemplo, para hacer una copia de seguridad del archivo de configuración `config.cfg` en la carpeta test en la memoria USB en la carpeta `testbackup` en un disco USB y nombrar el archivo de configuración de copia de seguridad `backup.cfg`, ejecute los siguientes comandos:

```
<Sysname> copy flash:/test/config.cfg usba0:/testbackup/backup.cfg
```

6.12.2 COPIA DE SEGURIDAD A TRAVÉS DE TFTP

268. Configure el dispositivo como cliente TFTP. Inicie la aplicación del servidor TFTP en el PC, establezca la ruta de transmisión para descargar el archivo de configuración y especifique la dirección IP y el número de puerto del servidor TFTP. Ejecute el comando `tftp` en la vista de usuario para cargar el archivo de configuración en el servidor TFTP (192.168.0.1):

```
<sysname> tftp 192.168.0.1 put flash:/config.cfg backup.cfg
```

7. FASE DE OPERACIÓN

270. Durante la fase de operación del producto se recomienda llevar a cabo, al menos, las siguientes tareas para una gestión segura del producto:

- Los administradores deben estar correctamente formados en el uso y la correcta operación del producto, así como en las características del entorno seguro en que está presente. Al mismo tiempo, los administradores seguirán las guías y recomendaciones de seguridad.
- Los administradores se asegurarán de que el producto cuenta con las últimas actualizaciones de firmware y software para preservar al mismo de amenazas y vulnerabilidades conocidas.
- Los administradores mantendrán sus credenciales de acceso al producto seguras y protegidas.
- Se deberán realizar copias de seguridad periódicas para asegurar que no se pierde información.
- Se deberán revisar periódicamente los logs del dispositivo para verificar su correcto funcionamiento y uso.
- Gestionar los usuarios siguiendo el principio de mínimo privilegio, permitiendo el acceso solo a los usuarios necesarios en cada momento.

8. REFERENCIAS

[H3C docs] https://www.h3c.com/en/Support/

[H3C-doc] H3C S6805[S6825][S6850][S9850] Switch Series Configuration Guides, version 6W100, fecha 20221206

[H3C-fund] H3C S6805 & S6825 & S6850 & S9850 Switch Series Fundamentals Configuration Guide, version 6W103, fecha 20220420

9. ABREVIATURAS

AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
CA	Certificate Authority
CLI	Command Line Interface
CPSTIC	Catálogo de productos STIC
CRL	Certificate Revocation List
DB9	9-pin D-Subminiature
DER	Distinguished Encoding Rules
DH	Diffie-Hellman
DN	Distinguished Name
ENS	Esquema Nacional de Seguridad.
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standards
HTTPS	Hypertext Transfer Protocol Secure
HWTACACS	Huawei Terminal Access Controller Access-Control System
IKE	Internet Key Exchange
IPSec	Internet Protocol Security
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
NTP	Network Time Protocol
OID	Object Identifier
PEM	Privacy-Enhanced Mail
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PSK	pre-shared key
RA	Registration Authority
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role-Based Access Control
RJ45	Registered Jack 45
ROM	Read-Only Memory
SCEP	Simple Certificate Enrollment Protocol

SSH	Secure Shell
STIC	Seguridad de las Tecnologías de la Información y la Ccomunicación
TFTP	Trivial File Transfer Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VTY	Virtual Teletype
XML	eXtensible Markup Language

PUBLICACIONES DE DEFENSA

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