centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1418

Procedimiento de Empleo Seguro
Switches Huawei S Series

Enero de 2024

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

CCN 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 12:34:15 +01'00'

NIPO: 083-24-039-6.
Fecha de Edición: Enero de 2024.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

1. Los *Huawei S Series Ethernet Switches* son **conmutadores** GE (*Gigabit Ethernet*) de última generación diseñados para proporcionar acceso de ancho de banda y agregación multiservicio de *Ethernet*. Están basados en el *software* de la plataforma de enrutamiento versátil de Huawei y ofrecen una gran capacidad de conmutación, alta fiabilidad (ranuras de alimentación dobles y *AOM Ethernet* de *hardware*) y puertos GE con la capacidad de 10 Gbit/s de subida.
2. Los *Huawei S Series Ethernet Switches* pueden utilizarse en escenarios empresariales; pudiendo funcionar como conmutadores de acceso o agregación en una red de campus, como conmutadores de acceso *gigabit* en un centro de datos de Internet (*IDC*) o como conmutadores de escritorio para proporcionar acceso de 1000 Mbit/s a varios terminales.
3. El procesador de los *Huawei S Series Ethernet Switches* tiene una arquitectura programable, permitiendo definir modelos propios de reenvío de tramas y paquetes, además de poder definir su comportamiento y sus algoritmos de búsqueda. La programabilidad del microcódigo permite ofrecer nuevos servicios sin necesidad de sustituir el *hardware*.
4. Los *Huawei S Series Ethernet Switches* ofrecen una excelente calidad de servicio (*QoS*) y admiten algoritmos de programación de colas y control de la congestión.
5. Admiten la autenticación de direcciones MAC y 802.1X y pueden ofrecer de forma dinámica políticas para los usuarios (*VLAN, Qos, ACL*).
6. Proporcionan una serie de mecanismos de defensa contra:
    - Ataques DoS: incluyendo SYN *flood*, *Land*, *Smurf*, e ICMP *flood*.
    - Ataques dirigidos al usuario: incluyendo ataques a servidores DHCP falsos y suplantación de direcciones *IP*/*MAC*.
7. Estos enrutadores recopilan y registran información sobre los usuarios, direcciones IP y MAC, arrendamiento de direcciones IP, identificadores de VLANs e interfaces de acceso en una tabla de vinculación de DHCP *snooping*. Con esta información pueden defenderse de los ataques DHCP en la red. Además, permiten especificar interfaces de confianza y de no confianza para garantizar que los usuarios se conecten sólo al servidor de DHCP autorizado.
8. Los *Huawei S Series Ethernet Switches* soportan el aprendizaje de ARP, para evitar que los ataques de falsificación de ARP agoten los registros ARP, permitiendo que los usuarios puedan conectarse a la red con normalidad.
9. Disponen de tres (3) interfaces de administración:
    a) SSH: Interfaz de línea de comandos.
    b) *Serial*: Interfaz de línea de comandos.
    c) Web (HTTPS): Interfaz gráfica.

2. OBJETO Y ALCANCE

10. La configuración evaluada del producto y por lo tanto incluida en la presente guía de empleo seguro consiste en la combinación del

    a) *Software* **V600R022C10SPC500** en los siguientes modelos de *hardware* *Huawei S Series Ethernet Switches*:

Familia	Modelos
S3710	S3710-H24T4S-A S3710-H24P4S-A S3710-H48T4S-A S3710-H48LP4S-A
S5732	S5732-H24S4X6QZ-TV2 S5732-H24S4X6QZ-V2 S5732-H24UM4Y2CZ-TV2 S5732-H24UM4Y2CZ-V2 S5732-H44S4X6QZ-TV2 S5732-H44S4X6QZ-V2 S5732-H48UM4Y2CZ-TV2 S5732-H48UM4Y2CZ-V2
S5735	S5735-S24T4XE-V2 S5735-S24P4XE-V2 S5735-S48T4XE-V2 S5735-S48P4XE-V2 S5735-S24U4XE-V2 S5735-S48U4XE-V2 S5735I-S24T4XE-V2 S5735I-S24U4XE-V2 S5735I-S8T4SN-V2 S5735I-S8T4XN-V2 S5735I-S8U4XN-V2 S5735-L8T4X-QA-V2 S5735-L8T4S-A-V2 S5735-L10T4X-A-V2 S5735-L8P4X-QA-V2 S5735-L8P4S-A-V2 S5735-L8P2T4X-A-V2 S5735-L16T4X-QA-V2

Familia	Modelos
	S5735-L16T4S-A-V2 S5735-L24T4X-QA-V2 S5735-L24T4S-A-V2 S5735-L24T4XE-A-V2 S5735-L24T4XE-D-V2 S5735-L24P4S-A-V2 S5735-L24P4XE-A-V2 S5735-L48T4S-A-V2 S5735-L48T4XE-A-V2 S5735-L48T4XE-D-V2 S5735-L48LP4S-A-V2 S5735-L48LP4XE-A-V2 S5735-L48P4XE-A-V2 S5735I-L8P4X-A-V2 S5735I-L10T4X-A-V2
S6730	S6730-H24X6C-TV2 S6730-H24X6C-V2 S6730-H28X6CZ-TV2 S6730-H28X6CZ-V2 S6730-H48X6C-TV2 S6730-H48X6C-V2 S6730-H48X6CZ-TV2 S6730-H48X6CZ-V2 S6730-H48Y6C-TV2 S6730-H48Y6C-V2
S8700	S8700-6 S8700-10 S8700-4
S16700	S16700-4 S16700-8

b) Software ***V600R022C10SPC500*** en los siguientes modelos de hardware Huawei S Series Ethernet Switches:

Familia	Modelos
S5731	S5731-S24N4X2Q-A

Familia	Modelos
	S5731-S24UN4X2Q S5731-S8UM16UN2Q S5731-S24T4X S5731-S24P4X S5731-S48T4X S5731-S48P4X S5731-H24T4XC S5731-H24P4XC S5731-H48T4XC S5731-H48P4XC S5731-H48T4XC-B S5731-H24T4XC-K S5731-H24P4XC-K S5731-H48P4XC-K S5731S-H24T4XC-A S5731S-H48T4XC-A S5731S-H24T4S-A S5731S-H48T4S-A S5731S-H24T4X-A S5731S-H48T4X-A S5731S-H24HB4XZ-A S5731S-H48HB4XZ-A S5731-S24T4X-A S5731-S24T4X-D S5731-S48T4X-A S5731-S32ST4X S5731-S32ST4X-A S5731-S32ST4X-D S5731-S48S4X S5731-S48S4X-A S5731-H24HB4XZ S5731-H48HB4XZ
S5732	S5732-H24S6Q S5732-H48S6Q S5732-H24UM2CC S5732-H48UM2CC

Familia	Modelos
	S5732-H24S6Q-K
	S5732-H48S6Q-K
	S5732-H48XUM2CC
	S5732-H24UM2C-K
	S5732-H48UM2C-K
S5735	S5735-L12T4S-A
	S5735-L12P4S-A
	S5735-L24T4S-A
	S5735-L24P4S-A
	S5735-L24T4X-A
	S5735-L24T4X-D
	S5735-L24P4X-A
	S5735-L32ST4X-A
	S5735-L32ST4X-D
	S5735-L48T4S-A
	S5735-L48T4X-A
	S5735-L48P4X-A
	S5735S-L12T4S-A
	S5735S-L12P4S-A
	S5735S-L24FT4S-A
	S5735S-L24T4S-A
	S5735S-L24T4X-A
	S5735S-L24P4S-A
	S5735S-L24P4X-A
	S5735S-L32ST4X-A
	S5735S-L48FT4S-A
	S5735S-L48T4S-A
	S5735S-L48T4X-A
	S5735S-L48P4S-A
	S5735S-L48P4X-A
	S5735-L8T4S-A1
	S5735-L8P4S-A1
	S5735-L8T4X-A1
	S5735-L8P4X-A1
	S5735-L24T4S-A1
	S5735-L24P4S-A1

Familia	Modelos
	S5735-L24T4X-A1
	S5735-L24T4X-D1
	S5735-L24P4X-A1
	S5735-L32ST4X-A1
	S5735-L32ST4X-D1
	S5735-L48T4S-A1
	S5735-L48P4S-A1
	S5735-L48T4X-A1
	S5735-L48P4X-A1
	S5735-L8T4S-QA1
	S5735-L8P4S-QA1
	S5735-L24T4S-QA1
	S5735-L24T4X-QA1
	S5735S-L8T4S-A1
	S5735S-L8P4S-A1
	S5735S-L24T4S-A1
	S5735S-L24P4S-A1
	S5735S-L24T4X-A1
	S5735S-L24P4X-A1
	S5735S-L32ST4X-A1
	S5735S-L48T4S-A1
	S5735S-L48P4S-A1
	S5735S-L48T4X-A1
	S5735S-L48P4X-A1
	S5735S-L24T4S-MA
	S5735S-L24P4S-MA
	S5735S-L48T4S-MA
	S5735-L8T4X-IA1
	S5735-L8P4X-IA1
	S5735-S24T4X
	S5735-S24P4X
	S5735-S32ST4X
	S5735-S48T4X
	S5735-S48P4X
	S5735-S48S4X
	S5735-S24T4X-I

Familia	Modelos
	S5735S-S24T4S-A S5735S-S32ST4X-A S5735S-S48T4S-A S5735S-S24T4X-A S5735S-S24P4X-A S5735S-S48T4X-A S5735S-S48P4X-A S5735S-H24S4XC-A S5735-L24T4X-IA1
S5736	S5736-S24UM4XC S5736-S24T4XC S5736-S24U4XC S5736-S24S4XC S5736-S48T4XC S5736-S48U4XC S5736-S48S4XC S5736-S48S4X-A S5736-S48S4X-D
S6730	S6730-H24X4Y4C S6730-H24X6C S6730-H48X6C S6730-H28Y4C S6730-H24X6C-K S6730-H48X6C-K S6730-H28Y4C-K S6730-S24X6Q S6730S-S24X6Q-A S6730S-H24X6C-A
S6735	S6735-S24X6C S6735-S48X6C
S12700E	S12700E-4 S12700E-8 S12700E-12

Tabla 1 Familias y modelos incluidos

3. ORGANIZACIÓN DEL DOCUMENTO

11. El presente documento se estructura en las secciones indicadas a continuación:

    a) **Apartado 4.** . En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto.

    b) **Apartado 5.** . En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

    c) **Apartado 6.** . En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

    d) **Apartado 7.** . En este apartado se incluye una lista de tareas a revisar para verificar que se han llevado a cabo cada una de las recomendaciones y configuraciones descritas en la presente guía de empleo seguro.

    e) **Apartado 8.** . En este apartado se recogen las referencias utilizadas en la presente guía de empleo seguro.

    f) **Apartado 9.** . En este apartado se recogen las abreviaturas utilizadas en la presente guía de empleo seguro.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

12. Al tratarse de una combinación *hardware*/*software*, los *Huawei S Series Ethernet Switches* se entregan por correo ordinario. Por ello, es necesario realizar las siguientes acciones:

    - **Información de envío**. Se debe comprobar la documentación de envío para verificar que concuerda con la orden de compra original y que el envío ha sido realizado por Huawei.
    - **Embalaje externo**. Se debe inspeccionar el embalaje y la cinta de embalaje con la marca de Huawei. Se debe comprobar que la cinta esté intacta y que no haya sido cortada ni se haya deteriorado en ningún punto. Además, se debe inspeccionar que la caja no presente cortes ni daños que permitan acceder al dispositivo.
    - **Embalaje interno**. Se debe comprobar el embalaje interior de la misma manera que el embalaje exterior. Adicionalmente, se debe comprobar que la etiqueta presente en el embalaje exterior concuerda con el modelo de *switch* adquirido.

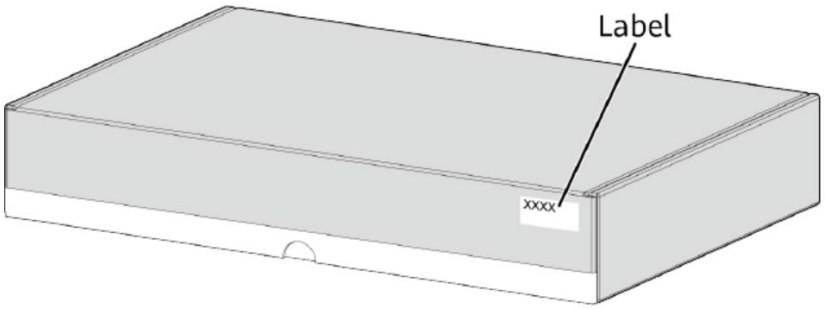


Ilustración 1. Embalaje interior

    - **Sello de garantía**. Se deberá verificar que el sello de garantía de la unidad esté intacto; este se encuentra en la parte inferior del producto y normalmente se coloca sobre un tornillo de acceso al chasis. El chasis no se puede abrir sin que este sello sea destruido.

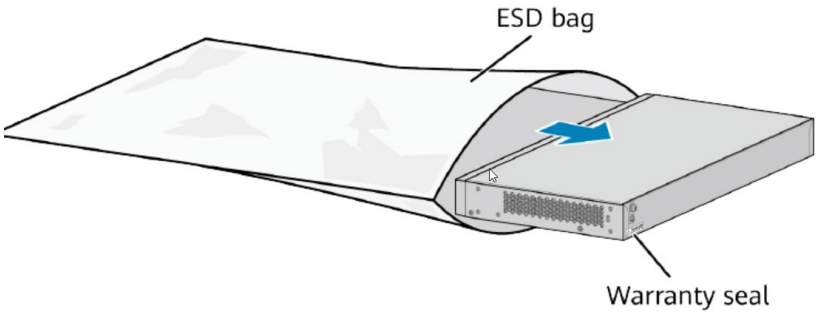


Ilustración 2. Switch y posición del sello de garantía

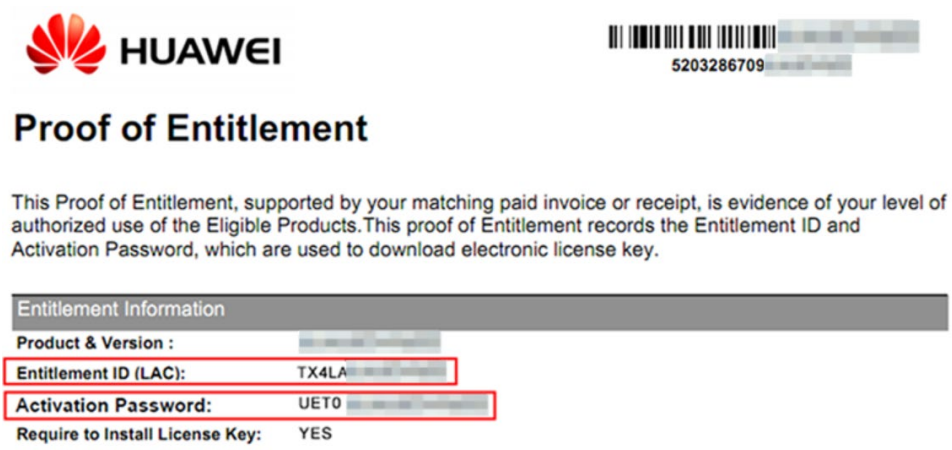
13. Si existe algún signo de daños, manipulación incorrecta o alteración, es necesario ponerse en contacto con el soporte de Huawei con carácter inmediato a fin de recibir instrucciones. Se recomienda dada esta situación, que no se realice la instalación del producto.

4.2 ENTORNO DE INSTALACIÓN SEGURO

14. Los componentes del producto deben instalarse en un entorno en el cual solo el personal técnico dispone de acceso y autorización para la configuración, despliegue y mantenimiento del producto.

4.3 REGISTRO Y LICENCIAS

15. Para los *Huawei S Series Ethernet Switches* existen dos (2) tipos de licencias:
    - **Licencia *COMM***: Normalmente, la mayoría de las licencias adquiridas por contrato tienen una validez permanente, aunque puede darse el caso de que algunas tienen un periodo de validez hasta una fecha determinada.
    - **Licencia temporal:** La licencia temporal también se conoce como licencia DEMO, que se utiliza para fines especiales como pruebas y ensayos.
16. Para realizar el registro de la licencia del producto es necesario realizar lo siguiente:
    a) Localizar el ID de derecho o la contraseña de activación de la licencia.


HUAWEI

5203286709

Proof of Entitlement

This Proof of Entitlement, supported by your matching paid invoice or receipt, is evidence of your level of authorized use of the Eligible Products.This proof of Entitlement records the Entitlement ID and Activation Password, which are used to download electronic license key.

Entitlement Information	
Product & Version :	
Entitlement ID (LAC):	TX4LA
Activation Password:	UET0
Require to Install License Key:	YES

Ilustración 3. Documento donde se encuentra la clave de activación

    b) Iniciar sesión en el producto a través de la interfaz de línea de comandos y ejecutar la instrucción *display license esn* en para obtener el ESN del dispositivo.

    c) Iniciar sesión en el sistema ESDP de Huawei a través de un PC: http://app.huawei.com/isdp

    d) Elegir "License *Activation" > "Password Activation*" en el menú izquierdo. Introduzca la contraseña en "*Password*", seleccione *"I have read the above carefully"* y pulse en "*Next*".

e) Introducir el ESN del dispositivo; pulsar en "*confirm activation*" y luego en "*Download*" para descargar un fichero que contiene la licencia.

f) Cargar el fichero en el producto mediante FTP (este protocolo se desactiva posteriormente debido a que es inseguro) en el directorio raíz; Usar el comando *license active <filename>* para activar la licencia en la interfaz de comandos del producto. Si la licencia se activa correctamente, el siguiente mensaje aparecerá en la interfaz:

```
<HUAWEI> license active license-test.dat
Info: The license is being activated. Please wait for a moment.
Info: Succeeded in activating the license file on the master board.
```

Ilustración 4. Activación correcta

4.4 INSTALACIÓN

17. La instalación física del producto —ya sea en un rack, en un escritorio o en una pared—, así como las medidas de precaución a tomar para cada uno de los diferentes casos se puede encontrar en la [GUÍA_PRODUCTO] en los módulos bajo *"Installation"* → *"Hardware Installation and Component Replacement"* → *"Installing a Switch"*. No obstante, se puntualiza que el lugar de instalación debe consistir en un lugar aislado y con buena ventilación, al que solo tenga acceso el personal autorizado.

18. Una vez el producto se ha instalado en una ubicación apropiada y se encuentra conectado a corriente, se procederá a su instalación. Para ello, se conectará el producto a un PC por su interfaz SERIAL en el puerto "*console*".

Ilustración 5. Diagrama de conexión al puerto consola

19. Para conectarse al producto por el puerto "*console*" es necesario iniciar un *software* emulador de terminal como *PuTTy*; con este *software* hay que crear una conexión con los siguientes parámetros:

Parámetro	Configuración
Velocidad en baudios	9600 bit/s
Control de flujo	Sin control de flujo
Paridad	Sin control de paridad
Stop bits	1
Data bits	8

Tabla 2. Configuración para conectarse al producto por el puerto consola

20. Al conectarse por primera vez a la interfaz *serial*, el producto requerirá una contraseña para el usuario *root* entre 8 y 16 caracteres. **Se recomienda usar una contraseña de 16 caracteres que cumpla con los siguientes requisitos de complejidad**: al menos 1 carácter en mayúscula, 1 carácter numérico y un símbolo; ya que en la sección *5.1 MODO DE OPERACIÓN SEGURO* se configura la longitud mínima de la contraseña como 16 caracteres.

```
An initial password is required for the first login via the console.
Set a password and keep it safe. Otherwise you will not be able to login via the console.

Please configure the login password (8-16)
Enter Password:
Confirm Password:
```

Ilustración 6. Cuadro donde se muestra el ingreso de la contraseña

21. De esta forma, ya estaría operativa la interfaz de comandos a través de la conexión *serial*. Para configurar el acceso por SSH, se conectará el extremo de un cable Ethernet al puerto ETH del producto, y el otro extremo a un PC. Luego, desde un navegador se debe acceder a la dirección 192.168.1.253/24.

22. Al acceder por primera vez a la interfaz *web*, el producto requerirá un usuario y contraseña para el usuario administrador; se debe usar un nombre de usuario diferente a *admin*/*root*/administrador/… y una contraseña de 16 caracteres o más, cumpliendo con los requisitos de complejidad definidos en el párrafo *24*. Tras crear el usuario y autenticarse en la interfaz WEB, se debe acceder en el menú superior a "*Maintenance*"→"*Administrator*"→"Usuario creado". En este menú se debe incluir SSH como método de acceso, definir el modo de autenticación como "*Password Authentication*", el tipo de servicio como "*Stelnet*", y el directorio autorizado como "*flash*:" (directorio raíz). Finalmente, se pulsará sobre OK y en el menú superior se guardarán los cambios. Tras esta configuración, ya se podrá acceder al producto por SSH a través de la conexión física en el puerto ETH.

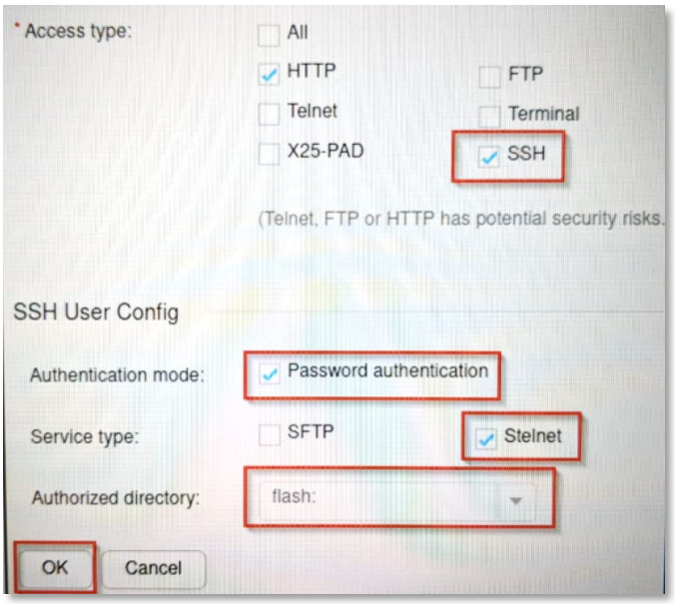


Ilustración 7. Menú de la interfaz web

23. Se recomienda cambiar la interfaz e IP por la cual se accede al producto por SSH. En el siguiente ejemplo se configura una IP en una interfaz MultiGE 0/0/x y luego se permite el acceso por SSH:

    system-view

    interface MultiGE 0/0/<numero_interfaz>

    ip address <ip_deseada> <máscara>

    quit

    ssh server-source -i MultiGE 0/0/<numero_interfaz_dada>

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

24. La configuración necesaria para que el producto opere de forma segura consiste en aplicar una configuración segura de varias políticas a través de la interfaz de línea de comandos. Esta interfaz es accesible a través del puerto SERIAL o a través de SSH por el puerto ETH.
25. Al acceder a la interfaz de línea de comandos y autenticarse, se accede al modo de *system-view*:

    system-view
26. Se debe configurar 16 caracteres como longitud mínima de contraseña:

    set password min-length 16
27. Se accede al modo *aaa*:

    aaa
28. Se debe configurar en 5 minutos el intervalo de reintento de autenticación, en 3 minutos el tiempo de reintento, y en 5 minutos el tiempo de bloqueo para evitar ataques de fuerza bruta:

    local-aaa-user wrong-password retry-interval 5 retry-time 3 block-time 5
29. Se vuelve al modo *system-view*:

    quit
30. Se debe implementar una política segura para acceder al sistema de ficheros:

    command-privilege level 3 view system execute
31. Se deben deshabilitar todas las interfaces que no se usarán:

    interface MultiGE 0/0/1

    shutdown

    display this

    #

    interface MultiGE 0/0/2

    shutdown

    display this

    #

    …
32. Se debe deshabilitar el servidor inseguro de TELNET:

    undo telnet server enable

undo telnet ipv6 server enable

33. Se deshabilita el servidor inseguro de FTP:

    undo ftp server

34. Se define como 4096 bits la longitud de las claves RSA:

    rsa local-key-pair-create

    y

    4096

35. Se define la ***suite* de cifrado segura** para el cifrado en SSH:

    ssh server cipher aes256_gcm aes128_gcm

36. Se define una ***suite* de cifrado** para el intercambio de claves en SSH y el método de curva elíptica como clave pública:

    ssh server key-exchange dh_group_exchange_sha256 dh_group16_sha512 curve 25519_sha256

    ssh server publickey ecc

37. Se define la *suite* de cifrado para TLSv1.3:

    ssl cipher-suite-list <nombreParaLaCipherSuite>

    set cipher-suite tls13_aes_128_gcm_sha256

    set cipher-suite tls13_aes_256_gcm_sha384

    set cipher-suite tls13_chacha20_poly1305_sha256

    set cipher-suite tls13_aes_128_ccm_sha256

    quit

    ssl policy <nombrePolitica>

    binding cipher-suite-customization <nombreDadoACipherSuite>

38. Si los siguientes protocolos no se van a utilizar, se han de **deshabilitar**:

    undo ipv6

    undo snmp-agent

    undo http server enable

    undo dhcp enable

    http secure-server disable

39. Por defecto, el puerto 64443 está abierto (el cuál ese utilizado para la autenticación Portal o 802.1X). Si no se va a utilizar esta funcionalidad se debe deshabilitar por seguridad:

    undo authentication https-redirect enable

40. El umbral para la generación de una nueva clave en comunicaciones a través de SSH se puede configurar a valores no permitidos, por ello habrá que ajustarlo a valores que lo estén (menos de un gigabyte y menos de una hora):

    ssh server rekey time 60

    ssh server rekey data-limit 1000

41. Se han de ajustar todas las interfaces con el modo "*sticky*" para prevenir ataques del tipo *MAC flooding*:

    interface <interfaz>

    port-security enable

    port-security mac-address sticky

    quit

42. Se guardan los cambios:

    save all

    y

5.2 AUTENTICACIÓN

43. Los mecanismos de autenticación que utiliza el producto para autenticar a un usuario son los siguientes:

    - Credenciales locales, mediante un usuario y contraseña de acceso.
    - Autenticación mediante servidor externo RADIUS.
    - Clave ECC para autenticación SSH por certificado (puede usarse clave RSA de 2048 bits, aunque por motivos de seguridad no se recomienda).

44. Los mecanismos de autenticación que utiliza el producto para autenticar a otros sistemas o dispositivos son los siguientes:

    - Certificado TSL/SSL para comunicarse con un servidor *syslog* externo.
    - Clave pre-compartida con cifrado HMAC-SHA256 para las comunicaciones con un servidor NTP externo.
    - Clave pre-compartida para cifrar la comunicación entre un servidor RADIUS externo y el producto; la información sensible como contraseñas es protegida mediante MD5 durante la transmisión por la red.

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

45. La administración local del producto se realiza a través de la interfaz *serial*. Para ello, es necesario conectar un PC al producto con un cable de consola. Para acceder

a las funciones de administración de la línea de comandos es necesario autenticarse con la contraseña del usuario *root* definida en **4.4 INSTALACIÓN**.

46. La administración remota del producto se realiza a través de SSH, para ello es necesario conectar un PC al producto con un cable de Ethernet en una interfaz física habilitada para tal propósito. Para acceder a las funciones de administración de la línea de comandos es necesario autenticarse con las credenciales de un usuario autorizado para conectarse por SSH al producto.
47. La administración remota del producto también puede realizarse por HTTPS a través de un navegador web, obteniendo una interfaz gráfica. No obstante, se recomienda deshabilitar este método de administración.
48. En la sección **5.1 MODO DE OPERACIÓN SEGURO** se define como deshabilitar protocolos inseguros como telnet, HTTP o FTP.

5.3.2 CONFIGURACIÓN DE ADMINISTRADORES

49. El producto no define roles como tal, sino que asocia un *"user privilege"* a cada usuario. Por defecto, los usuarios que acceden al producto por la interfaz de comandos tienen un nivel 3 de "*user privilege*" (administradores), y los demás un "*user privilege*" de 0 (visitantes). En la siguiente tabla se muestran los niveles de "*user privilege*" y los permisos asociados:

"User Privilege"	Permisos	Descripción
0	Visitante	Comandos de diagnóstico, como los comandos ping y *tracert*.
1	Seguimiento	Comandos de mantenimiento del sistema, como los comandos de *display*. No obstante, los comandos de *display* respecto a la configuración actual o la configuración guardada solo están disponible en niveles de "*user privilege*" de 3 o más.
2	Configuración	Comandos de configuración de los servicios.
3	Administración	Comandos de operación básica del sistema que se utilizan para dar soporte a los servicios, incluyendo el sistema de archivos, SFTP, comandos de gestión de usuarios, comandos de configuración a nivel de comandos y comandos de depuración.

Tabla 3. Permisos por nivel de privilegio

50. Para asignar un nivel específico de "*user privilege*" a un usuario es necesario acceder a la interfaz de línea de comandos del producto con un usuario con "*user privilege*" 3 y acceder a la vista *aaa*:

    system-view

    aaa

51. Luego, se puede asignar a un usuario un nivel de 0 a 15 de privilegios:

    local-aaa-user <nombre_usuario> privilege level <nivel>

52. Todo usuario con "*privelege level*" 3 puede establecer políticas seguras de contraseñas tales como:

    - Longitud de la contraseña (se debe implementar un **mínimo de 16 caracteres**):

      system-view

      set password min-length 16

    - **Complejidad** (uno o más caracteres en minúscula, uno o más caracteres en mayúscula, uno o más números, uno o más caracteres especiales):

      system-view

      aaa

      user-password complexity-check three-of-kinds

    - **Historial de contraseñas** (se deben guardar hasta las 10 últimas contraseñas utilizadas, para evitar que se utilicen contraseñas antiguas o contraseñas parecidas):

      system-view

      aaa

      local-aaa-user password policy administrator

      password history record number 10

      local-aaa-user password policy access-user

      password history record number 10

    - **Cambio de contraseñas** (el producto debe de forzar a los usuarios a cambiar su contraseña cada cierto tiempo, se recomienda **cada 120 días**):

      system-view

      aaa

      local-aaa-user password policy administrator

      password expire 120

      local-aaa-user password policy access-user

      password expire 120

53. **Se deben configurar tiempos de cierre de sesión tras un tiempo mínimo de inactividad**. Se recomienda, siempre que sea posible, que no exceda de los 10 minutos. Para configurar los cierres de sesión, utilizar un usuario con "*privelege level*" 3 para establecer las políticas seguras de sesión:

    - *Timeout de inactividad* (tiempo que puede permanecer la sesión inactiva, trascurrido el cual, se producirá la desconexión automática) para SSH:

      system-view

      ssh server timeout <tiempo_segundos>

    - *Timeout* de inactividad para HTTPS:

      system-view

      http timeout <tiempo_minutos>

    - *Timeout* de inactividad para la interfaz SERIAL:

      system-view

      user-interface console 0

      idle-timeout <tiempo_minutos> <tiempo_segundos>

    - Número máximo de intentos fallidos de autenticación, y tiempo de espera tras superar un umbral. Se define en la sección **5.1 MODO DE OPERACIÓN SEGURO**.

54. **Se debe configurar un banner de inicio de sesión**. Para ello, con un usuario con "*privelege level*" 15:

    header login information <MENSAJE>

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

55. **Se deben deshabilitar las interfaces físicas** (conexiones con el switch) **que no se utilicen y los servicios inseguros** (TELNET, HTTP, FTP…) como ya se realiza en la sección **5.1 MODO DE OPERACIÓN SEGURO**.

5.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

56. El producto usa SSH para administración remota y HTTPS/TLS para administración remota por Web y la comunicación con un servidor *syslog* externo.

57. El producto usa por defecto suites de cifrado con TLS 1.2, aunque se recomienda utilizar TLS 1.3.

58. En la sección **5.1 MODO DE OPERACIÓN SEGURO** se deshabilitan todas las versiones anteriores a SSHv2.

59. En la sección **5.1 MODO DE OPERACIÓN SEGURO** se configuran las siguientes *suites* de cifrado para SSH y TLS —los cuales se encuentran incluidos en la guía CCN-STIC-221 con la fortaleza adecuada para categoría ALTA en el ámbito del Esquema Nacional de Seguridad:

Tipo	Descripción suite de cifrado
TLS	Suites de Cifrado v1.3: *TLS_AES_128_GCM_SHA256* *TLS_AES_256_GCM_SHA384* *TLS_AES_128_CCM_SHA256* *TLS_CHACHA20_POLY1305_SHA256* Suite de cifrado v1.2 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 Establecimiento de clave: ECDHE Grupos de *Diffie-Hellman*: *brainpoolP256r1tls13* *brainpoolP384r1tls13* *brainpoolP512r1tls13* *x25519* *x448* Firma criptográfica: RSA Algoritmo de cifrado: AES 256 GCM Autenticación de mensajes: HMAC_SHA384
SSH	Establecimiento de clave: *DH-exchange-SHA256* *DH-grupo16-SHA512* Firma criptográfica: *ecdsa-sha2-nistp521* Algoritmo de cifrado: *AEAD_AES_128_GCM* *AEAD_AES_256_GCM*

Tabla 4. *Suites* de cifrado usadas por el producto en su modo de operación seguro

5.6 GESTIÓN DE CERTIFICADOS

60. El producto permite el uso de certificados X.509 autoafirmados para comunicarse con un servidor *syslog* externo. Sin embargo, **se recomienda la importación de certificados que cumplan con la política de seguridad del organismo**. En el módulo "*Managing Files When the Device Functions as an SFTP Server*" de la [GUÍA_PRODUCTO] se detalla cómo activar el servidor de SFTP del producto; luego,

se accede a este con las mismas credenciales que para SSH, pudiendo descargar o subir ficheros.

61. Se puede importar también un certificado de las CA raíz mediante el siguiente comando —una vez el certificado ya se encuentra en la memoria del producto—:

    trusted-ca load pem-ca <CA_raiz>

62. **Se debe configurar el producto para que verifique la vigencia de los certificados.** Para ello, se puede subir al producto un archivo CRL para comprobar si los certificados siguen siendo válidos, o configurar una dirección de un servidor OSCP para que lo compruebe contra el mismo servidor.

5.7 SERVIDORES DE AUTENTICACIÓN

63. El producto puede utilizar un servidor RADIUS externo como servidor de autenticación; una vez el servidor RADIUS esté listo para configurar junto al producto, se deberán seguir los pasos descritos en la sección "*Procedure*" de la [GUÍA_PRODUCTO] en el módulo *CONFIGURATION → CONFIGURATION → SECURITY SERVICES → AAA → RADIUS*. Los pasos descritos en esta sección se realizan a través de la interfaz web (se recomienda habilitar la interfaz web para la configuración y luego deshabilitarla una vez terminada la configuración del producto con el servidor RADIUS).

5.8 SINCRONIZACIÓN HORARIA

64. La sincronización horaria del producto se hará por medio de un servidor NTP externo. Se deben ejecutar las siguientes instrucciones para que el producto sincronice la hora con el servidor NTP:

    system-view

    ntp-service unicast-server <IP_ServidorNTP>

65. Para securizar la conexión, es necesario configurar una clave predefinida tanto en el servidor NTP como en el *switch*. Una vez se haya configurado la clave en el servidor NTP, se deben ejecutar las siguientes instrucciones en el producto:

    System-view

    ntp-service authentication enable

    ntp-service authentication-keyid <numero_asignar_clave> authentication-mode hmac-sha256 cipher <clave>

    ntp-service reliable authentication-keyid <numero_asignado_a_clave>

66. Se puede comprobar la fecha y hora del producto mediante la instrucción:

    clock datetime

67. La configuración del producto, por defecto, utiliza la versión NTPv3. No se debe modificar dicha configuración para evitar la utilización de versiones menos seguras del protocolo NTP.

5.9 ACTUALIZACIONES

68. El producto contempla dos (2) tipos de actualizaciones:
    - Paquete de parches: Conjunto de parches que actúan sobre una versión del *software* del sistema. El producto comprueba la validez del conjunto de parches antes de cargarlos en el sistema. Su extensión es (.pat).
    - *Software/firmware* del sistema: Se puede definir como el sistema operativo del producto. Al igual que los paquetes de parches, el producto comprueba la validez e integridad del *software* del sistema. Su extensión es (.cc).
69. Ambos tipos de actualizaciones puede descargarse de la web oficial de Huawei (*https://support.huawei.com*) y deben de subirse al directorio raíz del producto mediante SFTP.
70. Para configurar un paquete de parches como el paquete de parches por defecto del sistema, debe ejecutarse la siguiente instrucción:

    patch load <nombre_Parche>.pat all run

71. Para configurar un *software* del sistema como el *software* por defecto del producto se deben ejecutar las siguientes instrucciones:

    startup system-software <nombre_System_Software>.cc

    startup saved-configuration vrpcfg.zip

    reboot fast

72. Para listar el *software* del sistema y el paquete de parches configurados en el producto se debe ejecutar la siguiente instrucción:

    display startup

5.10 AUTO-CHEQUEOS

73. Cuando el producto se enciende o se reinicia realiza los siguientes auto-chequeos:
    - Auto-chequeo de la integridad del *software* del sistema.
    - Auto-chequeo de los algoritmos de cifrado (AES, HMAC, DRBG, SHA256/512, firmado con RSA).

5.11 SNMP

74. El producto puede funcionar como agente de SNMP, enviando mensajes SNMP a un NMS. Para ello, es necesario configurar el *switch* como se explica en el módulo

"*Configuring Basic SNMPv3 Functions*" de la [GUÍA_PRODUCTO]. **Se debe usar SNMP v3.** Para ello, se utiliza el siguiente comando:

snmp-agent sys-info version v3

5.12 ALTA DISPONIBILIDAD

75. La solución HSB (*Hot Standby*) ofrece un modo de red activo/en espera.

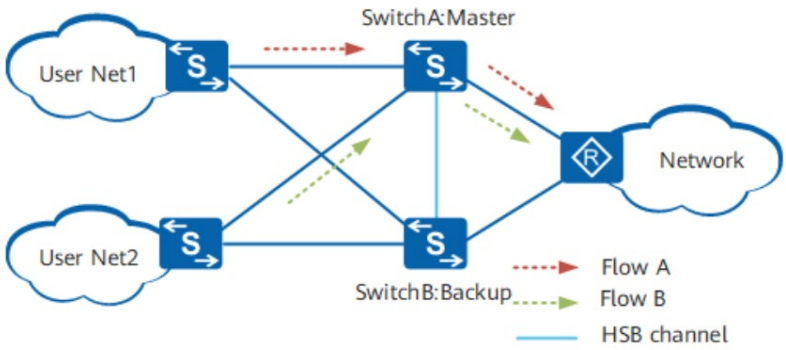


Ilustración 8. Solución HSB

76. Como se muestra en la figura superior, *SwitchA* y *SwitchB* forman un grupo VRRP (*Virtual Router Redundancy Protocol)*. El *SwitchA* es el dispositivo maestro y el *SwitchB* es el dispositivo de respaldo. Cuando el *SwitchA* funciona normalmente, procesa todos los servicios y transmite la información de sesión al *SwitchB* a través del canal HSB. *SwitchB* no procesa los servicios y sólo respalda la información de sesión.

77. Cuando el *SwitchA* falla, el *SwitchB* comienza a procesar los servicios, como se muestra en la imagen inferior. Como la información de la sesión está respaldada en el *SwitchB*, se pueden establecer nuevas sesiones sin interrumpir la sesión actual. Esto mejora la disponibilidad de la red.

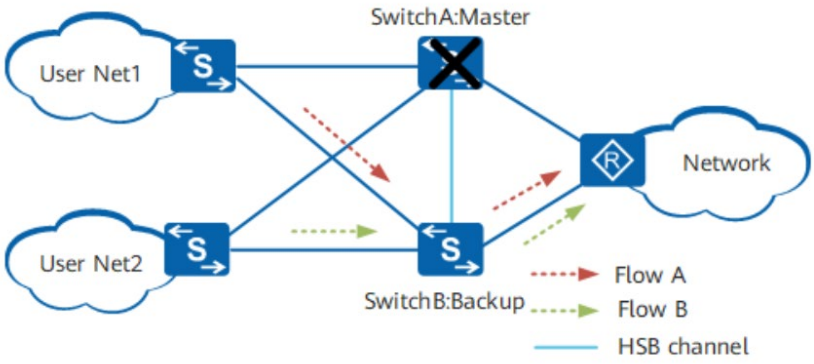


Ilustración 9. Solución HSB cuando falla el switch maestro

78. Cuando el dispositivo maestro original (*SwitchA*) se recupera, se convierte en el maestro en modo de preferencia. En el modo no preferente, se mantiene en el estado de reserva.

79. Para configurar HSB se recomienda seguir los pasos del módulo "HSB *Configuration*", así como de sus submódulos de la [GUÍA_PRODUCTO].

5.13 AUDITORÍA

5.13.1 REGISTRO DE EVENTOS

80. El producto almacena los siguientes eventos de seguridad en sus registros de auditoría:
    - *Login* y *logout* de los usuarios.
    - Inicio de las acciones de auditoría.
    - Cambio o generación de claves criptográficas.
    - Cambios en la configuración del producto.
    - Resetear o cambiar claves.
    - Intentos de *login* fallidos.
    - Configuración de un servidor NTP o eliminación del mismo.
    - Terminación de una sesión local o remota por el usuario o por inactividad.
    - Intentos de iniciar una actualización.
    - Fallos en establecer una sesión SSH.
81. El producto guarda la siguiente información de los eventos:

Campo	Descripción
Fecha y hora	Fecha y hora en la que se produce el evento.
Tipo de evento	Clase de evento que se produce (ej.: *login*, reseteo de clave…).
Sujeto que produce el evento	Usuario e IP (si corresponde).
Resultado	Resultado del evento, si aplica.

Tabla 5. Información que se guarda de los registros de auditoría

5.13.2 ALMACENAMIENTO LOCAL

82. El producto guarda en el directorio "*logfile*" —que se encuentra en el directorio raíz— un archivo llamado "*log.log*", que es donde se almacenan los registros de auditoría. Cuando el archivo "log.log" supera un tamaño determinado, se guarda automáticamente en un .zip llamado *<fechaDelLog>.log.zip*, vaciándose el archivo "*log.log*".

83. Para visualizar los registros de auditoría se debe de ejecutar el comando:

    display logfile <nombre_archivo_auditoria>

84. Si el producto alcanza el límite de almacenamiento sobrescribirá los registros más antiguos.

5.13.3 ALMACENAMIENTO REMOTO

85. El producto se puede configurar para enviar sus registros de auditoría a un servidor *syslog* externo. **Se debe configurar la comunicación con dicho servidor para usar TLS 1.2**, cifrando toda comunicación.

86. Para ello, una vez los certificados han sido creados y configurados en el servidor *syslog* externo, el certificado de CA debe subirse al producto mediante SFTP. Luego, se accede al producto por la interfaz de línea de comandos y se siguen los siguientes pasos:

    - Habilitar *info-center* (módulo del producto para enviar logs a un dispositivo externo):
      system-view

      info-center enable

      info-center channel 1 name loghost1
    - Especificar la dirección IP donde se encuentra el servidor *syslog* externo:
      info-center loghost <IP_servidor_syslog> channel loghost1
    - Especificar el nivel mínimo de *logs* a enviar:
      info-center source arp channel loghost1 log level notification
    - Crear una política de SSL para la comunicación segura:
      ssl policy <nombrar_politica_SSL>
    - Cargar el certificado de CA almacenado en el producto previamente:
      trusted-ca load pem-ca <fichero_certificado_CA>

      quit
    - Configurar que el producto use la política de SSL configurada para las comunicaciones con el servidor *syslog* externo:
      info-center loghost <IP_servidor_syslog> channel loghost1 transport tcp ssl-policy <nombre_dado_politica_SSL> verify-dns <syslog_DNS>

5.14 BACKUP

87. El producto almacena la configuración inicial (vacía) en el fichero "*vrpcfg.zip*", que se encuentra en el directorio raíz. Para guardar la configuración actual del producto (políticas implementadas, interfaces creadas, configuraciones de seguridad…) en el fichero "*vrpcfg.zip*" se debe de ejecutar el siguiente comando:

    save all vrpcfg.zip

88. No obstante, se debe guardar la configuración del producto de forma automática cada cierto periodo de tiempo. Esto se consigue mediante las siguiente instrucciones:

    system-view

    set save-configuration interval <rango_30_43200_minutos>

89. El archivo de configuración debe almacenarse en un dispositivo diferente del producto, ya sea descargándolo manualmente por medio de SFTP o a través de un servidor SFTP externo de forma automática mediante la siguiente instrucción:

    set save-configuration backup-to-server <IP_Servidor> transport-type sftp port <puerto> user <usuarioSFTP> password <passwordSFTP> path <directorio_servidor>

90. Por último, los registros de auditoría del sistema pueden enviarse a un servidor *syslog* externo, como se define en la sección **5.13 AUDITORÍA**.

5.15 SERVICIOS DE SEGURIDAD

91. **Se deben activar los mecanismos de protección de los que dispone el producto frente a ataques DoS** (denegación de servicio), incluyendo SYN *Flood*, *Land*, *Smurf* y ICMP *Flood*. Para ello, es necesario ejecutar los siguientes comandos en la interfaz de línea de comandos:

    system-view

    anti-attack tcp-syn enable

    anti-attack udp-flood enable

    anti-attack icmp-flood enable

    anti-attack abnormal enable

    anti-attack fragment enable

92. El producto permite evitar ataques ARP. Esto lo consigue mediante el aprendizaje de ARP, limitando el ratio de paquetes ARP relacionándolos con direcciones MAC o limitando el ratio de paquetes ARP por interfaz entre otros. **Se deben realizar las siguientes configuraciones frente a ataques ARP**. Para ello:

    system-view

    - Limitar el máximo de paquetes ARP que cualquier dirección MAC puede enviar por segundo. Lo mismo para IP.
      Arp speed-limit source-mac maximum <numero_paquetes_segundo>

      Arp speed-limit source-ip maximum <numero_paquetes_segundo>

    - Limitar el máximo de paquetes ARP de una dirección MAC en específico. Lo mismo para IP:
      arp speed-limit source-mac <dirección_MAC> maximum <numero_paquetes_segundo>

arp speed-limit source-mac <dirección_IP> maximum <numero_paquetes_segundo>

- Limitar el máximo de paquetes ARP en una interfaz o VLAN:
  interface <interfaz> <numero_interfaz | vlan <id_vlan>

  arp anti-attack rate-limit enable

  arp anti-attack rate-limit packet <numero_de_paquetes> interval <intervalo_segundos> block-timer <tiempo_bloqueo_cuando_sobrepasa>

- Configurar el aprendizaje de direcciones ARP:
  arp learning strict

93. **Se debe activar la funcionalidad contra DHCP *snooping*** que permite que los clientes de DHCP solo obtengan direcciones IP de servidores autorizados. Además, la funcionalidad registra un mapeo entre direcciones MAC y clientes DHCP, previniendo de ataques DHCP en la red. Para configurar la funcionalidad en el producto se deben efectuar las siguientes configuraciones:

    - Activar DHCP snooping para IPV4 (hacer lo mismo para IPV6 si se utiliza):
      system view

      dhcp snooping enable ipv4

    - Definir una interfaz y la VLAN a la que pertenece como interfaz de confianza para DHCP:
      interface <tipo_interfaz> <numero_interfaz>

      dhcp snooping trusted

      quit

      vlan <numero_vlan>

      dhcp snooping trusted interface <tipo_interfaz> <numero_interfaz>

    - Deshabilitar "*location transition*" para DHCP:
      undo dhcp snooping user-transfer enable

    - Configurar la asociación entre ARP y DHCP *Snooping*:
      arp dhcp-snooping-detect enable

    - Configurar el producto para limpiar el registro de direcciones MAC cuando un usuario se desconecta:
      dhcp snooping user-offline remove mac-address

94. Se recomienda seguir los pasos de configuración descritos en la [GUÍA_PRODUCTO] en la sección "*Typical Security Configuration*" si se desea implementar ACL, ARP, DHCP o IPSG de forma segura.

6. FASE DE OPERACIÓN

95. Durante la fase de operación del producto, lo administradores de seguridad deberán llevar a cabo, al menos, las siguientes tareas de mantenimiento.

- 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.
- Aplicación periódica de los parches de seguridad, con objeto de mantener una configuración segura.
- Realizar *back-ups* periódicos y la restauración de estos. Además de almacenarlos en localizaciones seguras y planificar el proceso de automatización.
- Mantenimiento de los 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 auditoria se guardará en las condiciones y por el periodo establecido en la normativa de seguridad.

7. CHECKLIST

96. A continuación, se recoge la lista de verificaciones que es necesario realizar para la garantizar la configuración segura del producto.

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
Registro de la licencia del producto	☐	☐	
Activación de la licencia del producto	☐	☐	
Instalación del producto	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Configuraciones del producto para llegar al modo de Operación seguro	☐	☐	
Elegir mecanismos de autenticación	☐	☐	
Configuración de administradores	☐	☐	
Configuración de interfaces puertos y servicios	☐	☐	
Configuración de protocolos seguros	☐	☐	
Gestión de certificados	☐	☐	
Asignar un servidor de autenticación (si fuera necesario)	☐	☐	
Sincronización horaria	☐	☐	
Configuración de las actualizaciones (si fuera necesario)	☐	☐	
Configuración de Alta disponibilidad (si fuera necesario)	☐	☐	
Auditoría (Almacenamiento remoto)	☐	☐	
Configuración de los back-ups	☐	☐	
Configuración de los servicios de seguridad	☐	☐	

Tabla 6. *Checklist*

8. REFERENCIAS

[GUÍA_PRODUCTO] *S300, S500, S2700CloudEngine S3700, S5700, and S6700 Series Ethernet SwitchesV600R022C10 Product Documentation, Version: V200R020C10, Issue: 0102, Date: 2021-05-102023-11-30*

S300, S500, S2700, S5700, and S6700 V200R022C00 Product Documentation, Issue: 02, Date: 2022-12-15

9. ABREVIATURAS

ACL	*Access Control List*
AOM	*Acousto-Optic Modulator*
ARP	*Address Resolution Protocol*
AES	*Advanced Encryption Standard*
AAA	*authentication, authorization, and accounting*
DEMO	*Demonstration*
DRBG	*Deterministic Random Bit Generator*
DHCP	*Dynamic Host Configuration Protocol*
ESDP	*Electronic Software Delivery Platform*
ESN	*Equipment Serial Number*
ETH	*Ethernet*
Gbit	*Gigabit*
GE	*Gigabit Ethernet*
HMAC	*Hash-based Message Authentication Code*
HSB	*Hot Standby*
HTTPS	*Hypertext Transfer Protocol Secure*
COMM	*Communication*
ID	*Identification*
ICMP	*Internet Control Message Protocl*
IDC	*Internet Data Center*
IP	*Internet Protocol*
MAC	*Media Access Control*
Mbit	*Megabit*
NMS	*Network Management System*
NTP	*Network Time Protocol*
PC	*Personal Computer*
QoS	*Quality of Service*
RADIUS	*Remote Authentication Dial-In User Service*
RSA	*Rivest, Shamir, & Adleman (public key encryption technology)*
SHA	*Secure Hash Algorithm*
SSH	*Secure Shell*
SSL	*Secure Sockets Layer*

SNMP	*Simple Network Management Protocol*
SYN	*Synchronization*
TLS	*Transport Layer Security*
VLAN	*Virtual Large Area Network*
VRRP	*Virtual Router Redundancy Protocol*

PUBLICACIONES DE DEFENSA

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