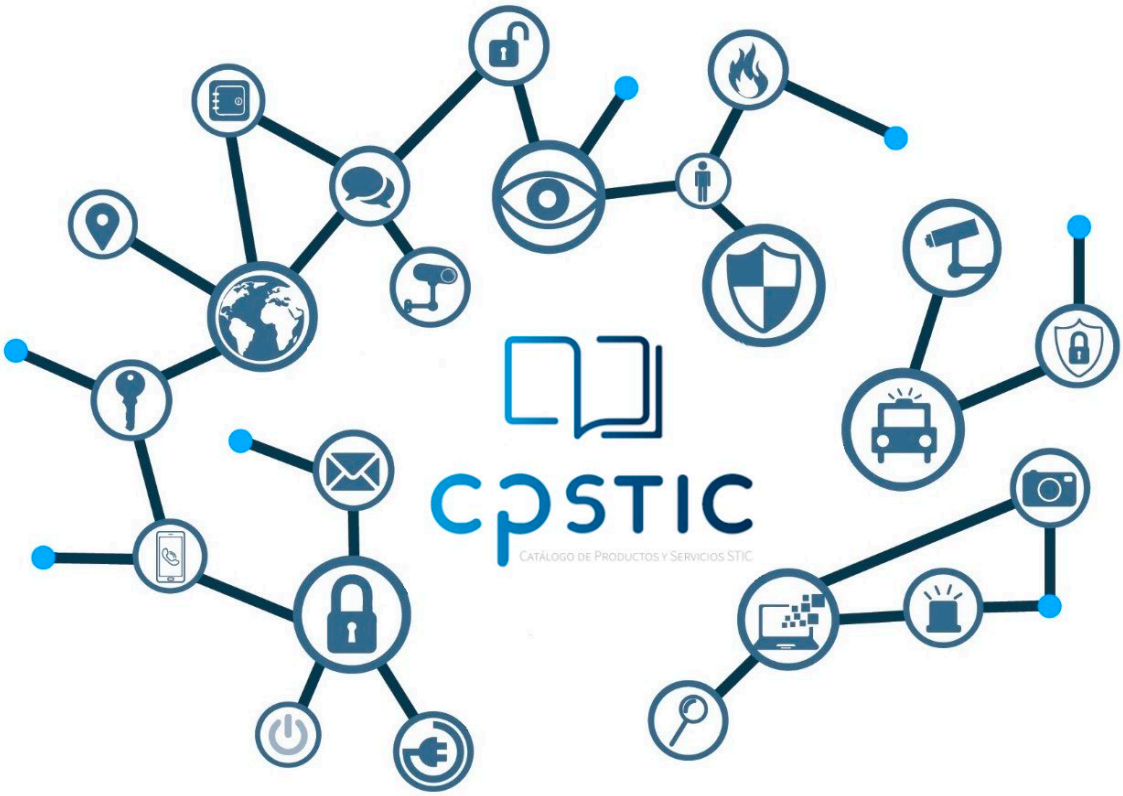
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1424

Procedimiento de Empleo Seguro
Huawei CE Series Switches



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

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 12:33:51 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-040-9.
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 conmutadores de la serie Huawei CloudEngine (CE) son **conmutadores** de alto rendimiento diseñados para centros de datos de próxima generación y redes de campus de alta gama. La serie incluye los conmutadores de núcleo CE16800 insignia de Huawei, el conmutador TOR de acceso 25GE CE8800, conmutadores de TOR de alto rendimiento CE680/ CE5800 para acceso 10GE / GE.
2. La serie CE utiliza la plataforma de *software* de próxima generación de Huawei y es compatible con amplias funciones de servicio de red de campus y centros de datos.
3. El procesador de los *Huawei CE Series 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 CE Series Switches* ofrecen una excelente calidad de servicio (QoS) y admiten algoritmos de programación de colas y control de la congestión. Admiten la autenticación de direcciones MAC y 802.1X y pueden ofrecer de forma dinámica políticas para los usuarios (VLAN, Qos, ACL).
5. Proporcionan 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*.
6. Los *Huawei CE Series Switches* recopilan y registran información sobre los usuarios, como direcciones IP, direcciones 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.
7. Soportan el aprendizaje de ARP. Esta funcionalidad evita que los ataques de falsificación de ARP agoten los registros ARP, permitiendo que los usuarios puedan conectarse a la red con normalidad.
8. Los *Huawei CE Series Switches* disponen de dos (2) interfaces de administración:
    - Serial: Interfaz de línea de comandos.
    - Mini-USB: Sólo algunos de los modelos de la serie permiten este acceso.

2. OBJETO Y ALCANCE

9. La configuración incluida en la presente guía de empleo seguro es la evaluada y cualificada en el Catálogo de Productos y Servicios de STIC (CPSTIC).

- *Software V300R022C00SPC200.* Modelos *hardware:*

Familia	Modelos
CE6800	CE6866-48S8CQ-P CE6860-HAM CE6860-SAN CE6881H-48S6CQ CE6881H-48T6CQ CE6820H-48S6CQ CE6863H-48S6CQ
CE8800	CE8851-32CQ8DQ-P CE8850-HAM CE8850-SAN
CE16800	CE16804 CE16808 CE16816

- *Software V200R022C00SPC500.* Modelos *hardware:*

Familia	Modelos
CE5800	CE5882-48T4S
CE6800	CE6870-48S6CQ-EI CE6870-48S6CQ-EI-A CE6881-48S6CQ CE6863E-48S6CQ CE6881-48T6CQ
CE8800	CE8850-64CQ-EI
CE9800	CE9860-4C-EI CE9860-4C-EI-A
CE16800	CE16804 CE16808 CE16816

3. ORGANIZACIÓN DEL DOCUMENTO

10. 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

11. Al tratarse de una combinación *hardware/software*, los Huawei CE Series Switches se entregan por correo ordinario. Por ello, se debe comprobar:

    - **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 de comprobar que la etiqueta presente en el embalaje exterior concuerda con el modelo de switch adquirido.

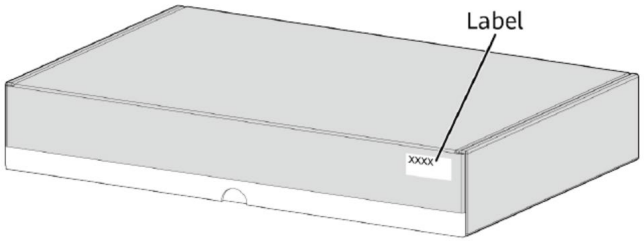


Ilustración 1. Embalaje interior

    - **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.

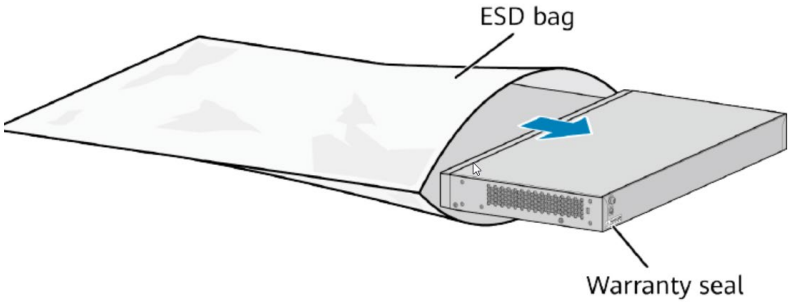


Ilustración 2. Switch y posición del sello de garantía

12. 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

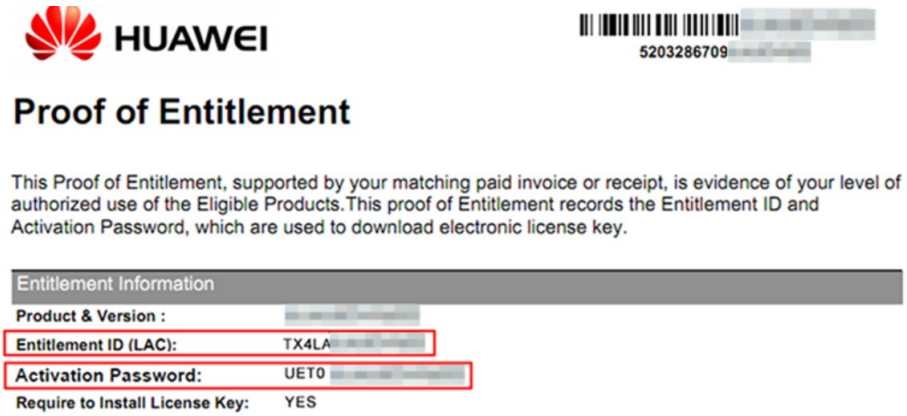
13. Los componentes del producto deben instalarse en un entorno en el cual solo el personal técnico dispone de autorización para la configuración, despliegue y mantenimiento del producto.

4.3 REGISTRO Y LICENCIAS

14. Para los *Huawei CE Series 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. En algunos casos, existen funcionalidades que necesitan de una licencia específica.
    - **Licencia temporal:** La licencia temporal también se conoce como licencia DEMO, que se utiliza para fines especiales como pruebas y ensayos.

15. Para realizar el registro de la licencia del producto es necesario 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

16. Se deben seguir los siguientes pasos:

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

    b) Iniciar sesión en el sistema ESDP de Huawei a través de un PC:

    http://app.huawei.com/isdp

    c) Elejir "*License Activation*" > "*Password Activation*" en el menú izquierdo. Introducir la contraseña en "*Password*", seleccionar "*I have read the above carefully*" y pulsar "*Next*".

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

e) 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. Cuadro donde se muestra que la licencia se ha activado correctamente.

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 las guías:

- **[GUÍA_PRODUCTO_16800]** en la sección "Installation" > "Hardware Installation and Manteinance Guide (Applicable to All Versions)" > "Installing a Switch".
- **[GUÍA_PRODUCTO_12800]** en la sección "Installation" > "Hardware Installation and Manteinance Guide (CE12800)" > "Installing a Switch".
- **[GUÍA_PRODUCTO_9800&8800&6800&5800]** en la sección "Installation" > "Hardware Installation and Manteinance Guide (Applicable to All Versions)" > "Installing a Switch".

18. 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**.

19. 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*"

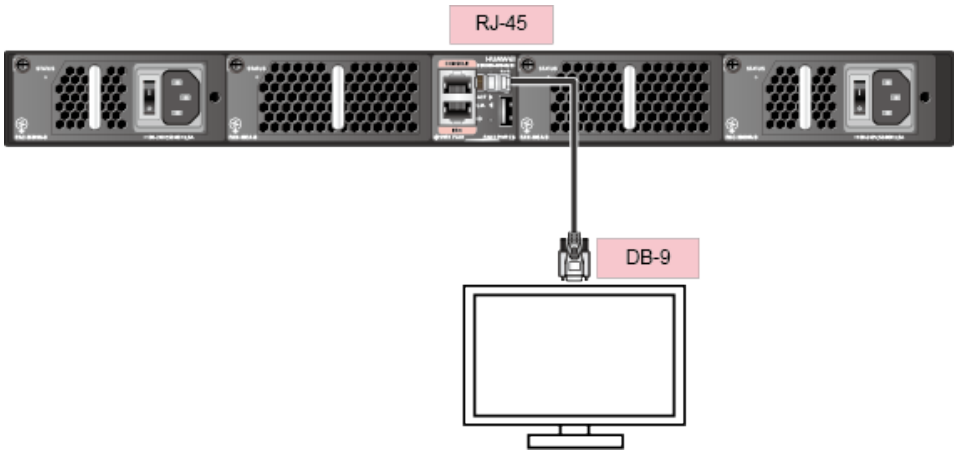


Ilustración 5. Diagrama de conexión al puerto consola

20. 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 1. Configuración para conectarse al producto por el puerto consola

21. 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.
Continue to set it? [Y/N]: y
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

22. De esta forma, ya estaría operativa la interfaz de comandos a través de la conexión *serial*.
23. Para conectarse al producto usando el puerto Mini-USB es necesario preparar:
    - Cable Mini-USB
    - El driver necesario compatible con el equipo de sobremesa.
    - Un emulador de terminal (*hyperterminal* o similar)
24. Se debe iniciar el *software* de emulación de terminal en la PC y crear una conexión. Para ello, seleccionar el puerto conectado y configurar los parámetros de comunicación. Una vez conectado, se verá el mismo mensaje que en la conexión a través de consola.
25. Una vez se ha accedido al equipo, se recomienda configurar el acceso a través de SSH.

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

26. 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.
27. Al acceder a la interfaz de línea de comandos y autenticarse, se accede al modo de *system-view*:

    system-view
28. Se accede al modo Authentication, Authorization, and Accounting (aaa):

    aaa
29. **Se debe de configurar 16 caracteres** como la longitud mínima de contraseña:

    local-user policy password min-len 16
30. 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-user authentication lock times 3 5
31. Se vuelve al modo *system-view*:

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

    command-privilege level 3 view system execute
33. Se deshabilitan todas las interfaces que no se usarán:

    interface 10gE 0/0/1

    shutdown

    display this

    #

    interface 10gE 0/0/2

    shutdown

    display this

    #

    …
34. Se deshabilita el servidor inseguro de TELNET:

    telnet server disable

    telnet ipv6 server disable

35. Se deshabilita el servidor inseguro de FTP:

    undo ftp server enable

36. Se **deshabilita** el soporte a la versión insegura de **SSHv1.x**:

    undo ssh server compatible-ssh1x enable

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

    rsa local-key-pair-create

    y

    4096

38. Se define las **suites de cifrado segura** para el encriptado en SSH:

    ssh server cipher aes256_gcm aes128_gcm

39. Se define las **suites de cifrado para el intercambio de claves en SSH** y el método de curva elíptica como clave pública:

    ssh server key-exchange dh_group16_sha512 ecdh_sha2_nistp256

    ssh server publickey ecc

40. Se definen las **suites de cifrado** para TLS 1.3:

    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>

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

    undo snmp-agent

    undo dhcp enable

42. 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

43. Se guardan los cambios:

commit

save

y

5.2 AUTENTICACIÓN

44. 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.
    - Clave ECC para autenticación SSH por certificado (puede usarse clave RSA de 2048 bits, aunque por motivos de seguridad no se recomienda).
45. 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.

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

46. 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*.
47. 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.
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 2. 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 3 de privilegios:

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

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

    a) La longitud de la contraseña (se debe implementar un mínimo de 16 caracteres):

    system-view

    aaa

    local-user policy password min-len 16

    b) La 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

    local-user policy password complexity-enhance

c) El historial de contraseñas (se deben guardar hasta las 10 últimas contraseñas utilizadas, para evitar que se utilicen contraseñas antiguas o contraseñas parecidas). Una vez utilizado el comando anterior se activa automáticamente el control para no repetir las últimas 10 contraseñas.

d) El cambio de contraseñas. El producto debe de forzar a los usuarios a cambiar su contraseña cada cierto tiempo. Se recomienda cada 60 días.

system-view

aaa

local-user policy password expire 60 prompt 7

El parámetro "*prompf*" especifica el número de días de anticipación que se notifica a los usuarios que sus contraseñas están a punto de caducar.

53. Todo usuario con "privilege level" 3 puede establecer políticas seguras de sesión como:

a) *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>

b) *Timeout* de inactividad para la interfaz SERIAL:

system-view

user-interface console 0

idle-timeout <tiempo_minutos> <tiempo_segundos>

c) 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**. Todo usuario con "*privilege level*" 3 puede definirlo a través del siguiente comando:

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, FTP…) como ya se especifica en la sección *5.1 MODO DE OPERACIÓN SEGURO.*

5.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

56. El producto puede usar SSH para administración remota 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. En dicha sección, también se configuran las siguientes suites de cifrado para SSH y TLS —los cuales se encuentran incluidos en la guía CCN-STIC-221 con fortaleza nivel ALTO—:

Tipo	Descripción suite de cifrado
TLS	Suites de Cifrado: ***TLS_AES_128_GCM_SHA256*** ***TLS_AES_256_GCM_SHA384*** ***TLS_AES_128_CCM_SHA256*** ***TLS_CHACHA20_POLY1305_SHA256*** Establecimiento de clave: ECDHE Grupos de *Diffie-Hellman*: ***brainpoolP256r1tls13*** ***brainpoolP384r1tls13*** ***brainpoolP512r1tls13*** ***x25519*** ***x448***
SSH	Establecimiento de clave: ***ECDH-SHA2-NISTP256*** ***DH-grupo16-SHA512*** Firma criptográfica: ***ecdsa-sha2-nistp521*** Algoritmo de cifrado: ***AEAD_AES_128_GCM*** ***AEAD_AES_256_GCM***

Tabla 3. Suites de cifrado usadas por el producto en su modo de operación seguro

5.6 GESTIÓN DE CERTIFICADOS

59. El producto usa certificados X.509 autoafirmados para comunicarse con un servidor *syslog* externo. **Sin embargo, se recomienda la importación de cetificados que cumplan con la política de seguridad del organismo.** En el módulo "*Files When the Device Functions as an SFTP Server*" de las guías incluidas en el apartado 8.REFERENCIAS se detalla como activar el servidor de SFTP del producto; luego, se accede a este con las mismas credenciales que para SSH, pudiendo descargar o subir ficheros.

60. Se puede importar 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>

61. **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 SINCRONIZACIÓN HORARIA

62. **El producto debe estar configurado de acuerdo a una fuente fiable de tiempo**. La sincronización horaria del producto se hará por medio de un servidor NTP externo. Se deben de ejecutar las siguientes instrucciones para que el producto sincronice la hora con un servidor NTP externo:

    system-view

    ntp unicast-peer ip-address <IP_ServidorNTP>

63. 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 authentication enable

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

    ntp trusted authentication-keyid <numero_asignar_clave>

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

    clock datetime

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

5.8 ACTUALIZACIONES

66. 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).
67. 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.
68. 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
69. 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
70. Para listar el *software* del sistema y el paquete de parches configurados en el producto se debe de ejecutar la siguiente instrucción:

    display startup

5.9 AUTO-CHEQUEOS

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

5.10 SNMP

72. 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 las guías indicadas en 8.REFERENCIAS.
73. **Se debe usar SNMPv3.** Para ello, se utiliza el siguiente comando:

    snmp-agent sys-info version v3

5.11 ALTA DISPONIBILIDAD

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

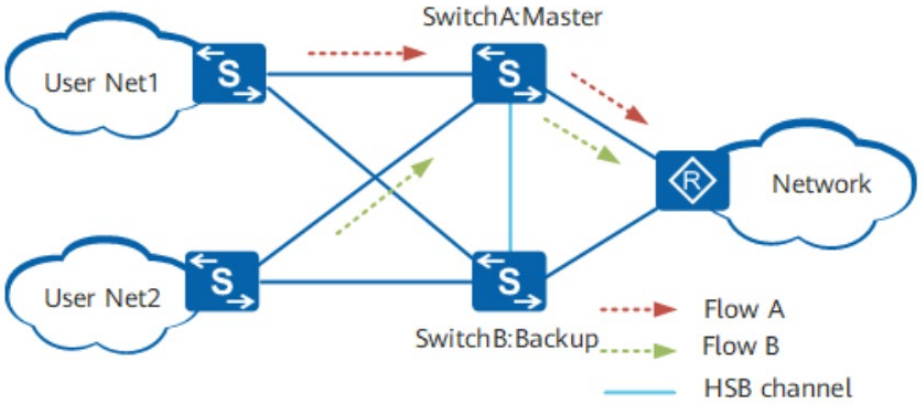


Ilustración 7. Solución HSB

75. Como se muestra en la figura superior, *SwitchA* y *SwitchB* forman un grupo VRRP. 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.

76. 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.

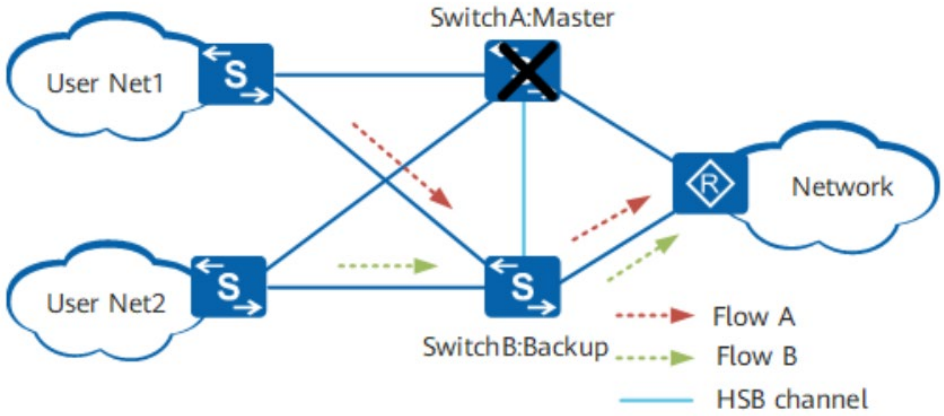


Ilustración 8. Solución HSB cuando falla el *switch* maestro

77. 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.

78. Para configurar HSB se recomienda seguir los pasos del módulo "HSB *Configuration*", así como de sus submódulos de las guías indicadas en 8.REFERENCIAS.

5.12 AUDITORÍA

5.12.1 REGISTRO DE EVENTOS

79. 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.

80. 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 4. Información que se guarda de los registros de auditoría

5.12.2 ALMACENAMIENTO LOCAL

81. 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 *log_5_<fechaDelLog>.log.zip*, vaciándose el archivo "*log.log*".

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

    display logfile <nombre_archivo_auditoria>

83. Si el producto alcanza el límite de almacenamiento sobrescribirá los registros más antiguos, por lo que **se recomienda su almacenamiento remoto**.

5.12.3 ALMACENAMIENTO REMOTO

84. 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.

85. Para ello, una vez los certificados autofirmados han sido creados (ej.: openSSL) 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>

5.13 *BACKUP*

86. 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

87. No obstante, se recomienda guardar la configuración del producto de forma automática cada cierto periodo de tiempo. Esto se consigue mediante las siguientes instrucciones:

    system-view

    set save-configuration interval <rango_30_43200_minutos>

88. 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>

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

5.14 SERVICIOS DE SEGURIDAD

90. **Se deben activar los mecanismos de protección de los que dispone el producto frente a ataques DoS.** El producto dispone de defensas contra ataques D), 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

91. 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:**

    system-view

- Se limita 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

92. **Se debe activar la funcionalidad contra DHCP *snooping*** 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>

    - Configurar la asociación entre ARP y DHCP *Snooping*:

      dhcp snooping user-bind arp-detect enable

- Configurar el producto para limpiar el registro de direcciones MAC cuando un usuario se desconecta:

  dhcp snooping user-offline remove mac-address

93. Se recomienda seguir los pasos de configuración descritos en las guías incluidas en el apartado 8.REFERENCIAS en la sección "*Security Configuration Guide*" si se desea implementar ACL, ARP o DHCP de forma segura.

6. FASE DE OPERACIÓN

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

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

    b) **Aplicación regular de los parches de seguridad**, con objeto de mantener una configuración segura.

    c) **Realizar *back-ups* periódicos y la restauración de estos**. Además de almacenarlos en localizaciones seguras y planificar el proceso de automatización.

    d) **Mantenimiento y análisis de los registros de auditoría**. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos. La información de auditoria se guardará en las condiciones y por el periodo establecido en la normativa de seguridad.

7. CHECKLIST

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 5. *Checklist*

8. REFERENCIAS

[GUÍA_PRODUCTO_8800&6800] *CloudEngine 8800, and 6800 Series Switches V300R022C00 Product Documentation, Issue: 01, Date: 2022-11-18.*

[GUÍA_PRODUCTO_16800] *CloudEngine 16800 Series Switches V300R022C00 Product Documentation Issue: 03, Date: 2023-10-31.*

[GUÍA_PRODUCTO_9800&8800 &6800& 5800] *CloudEngine 9800, 8800, 6800, and 5800 Series Switches V200R022C00 Product Documentation, Issue: 01, Date: 2022-11-18.*

[GUÍA_PRODUCTO_16800] *CloudEngine 16800 Series Switches V200R022C00 Product Documentation Issue: 03, Date: 2023-06-09.*

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