centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1437

Procedimiento de empleo seguro
Enrutadores Huawei AR6000&AR600

Septiembre de 2022

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
2022.09.28 14:07:06 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-245-3

Fecha de Edición: septiembre de 2022

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. **Huawei NetEngine AR6000** son routers empresariales de nueva generación que utilizan procesadores multinúcleo de alto rendimiento y una estructura de conmutación sin bloqueo. Los routers empresariales de la serie NetEngine AR6000 de Huawei pueden desplegarse en la sede central de la empresa o en las sucursales, según sea necesario, para proporcionar capacidades de salida de la red empresarial.
2. Huawei NetEngine AR600 son también routers empresariales de nueva generación que utilizan procesadores multinúcleo y una estructura de conmutación sin bloqueo, estando estos enfocados al despliegue en sucursales de PYMES y pequeñas empresas según sea necesario para proporcionar capacidades de salida de la red empresarial.
3. Los productos se componen de *hardware* y *software*, proporcionando la capacidad de procesamiento de tráfico de red. El software está compuesto por la plataforma de enrutamiento versátil (*Versatile Routing Platform o* VRP) y el sistema operativo (OS) subyacente. El tráfico de red es procesado y reenviado por el hardware subyacente según las decisiones de enrutamiento descargadas de la VRP.
4. El VRP ofrece amplias funciones de seguridad. Dichas funciones incluyen diferentes interfaces con niveles de acceso acordes para los administradores, la imposición de autenticaciones antes de establecer sesiones administrativas y la auditoría de las actividades de gestión relevantes para la seguridad.

2. OBJETO Y ALCANCE

5. El objeto del presente documento es facilitar la instalación y configuración segura del producto con la **versión *software* V300R019C11SPC200 con parche V300R019C11HP0095T**, en conjunción con los siguientes modelos *hardware*:

Serie *Hardware*	Modelo *Hardware*
NetEngine AR600	NetEngine AR651C
	NetEngine AR651
	NetEngine AR651W
	NetEngine AR657W
	NetEngine AR611W
	NetEngine AR617VW-LTE4EA
NetEngine AR6000	NetEngine AR6120
	NetEngine AR6121
	NetEngine AR6140-9G-2AC
	NetEngine AR6140-16G4XG
	NetEngine AR6280
	NetEngine AR6300

Tabla 1 – Modelos *hardware* a los que aplica este documento

6. **Este producto ha sido cualificado e incluido en el Catálogo de Productos y Servicios STIC (CPSTIC), en la categoría "Enrutadores".**

3. ORGANIZACIÓN DEL DOCUMENTO

7. El presente documento se estructurado en los siguientes apartados:
   a) **Apartado 4.** Fase de despliegue e instalación.
   b) **Apartado 5.** Recomendaciones en la fase de configuración y administración.
   c) **Apartado 6.** Recomendaciones en la fase de operación.
   d) **Apartado 7**. *Checklist* de las tareas a realizar y el estado de cada una de ellas.
   e) **Apartado 8.** Listado de documentación referenciada en este documento.
   f) **Apartado 9.** Listado de abreviaturas que aparecen en este documento.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

8. Los Huawei NetEngine AR Series Routers se entregan con una combinación *hardware/software,* siendo el dispositivo entregado por correo ordinario. Una vez recibido, 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 y exterior. Adicionalmente, se debe de comprobar que la etiqueta presente en el embalaje exterior concuerda con el modelo de *switch* NetEngine adquirido.

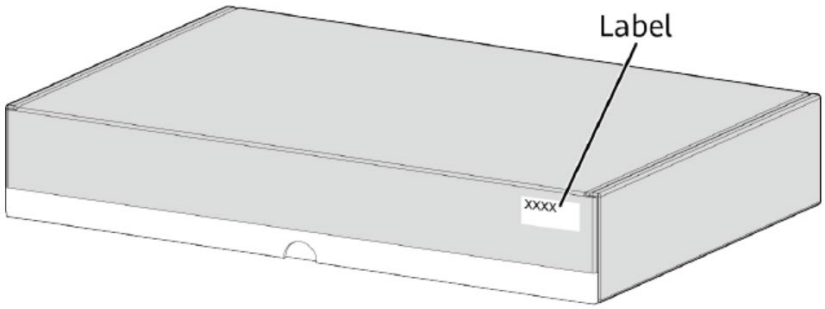


Ilustración 1 – Embalaje interno y localización del etiquetado

- **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.

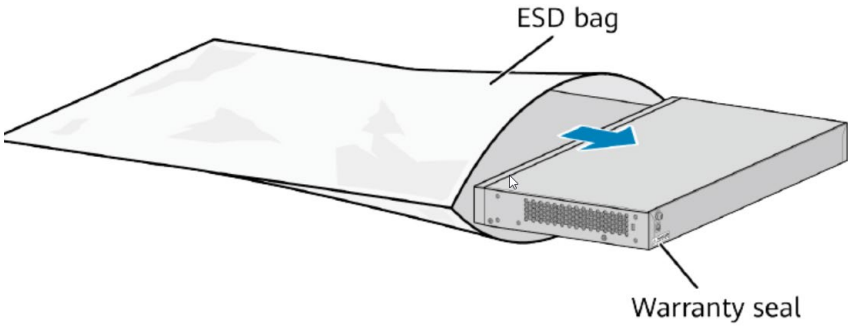


Ilustración 2 – Localización del sello de garantía en el enrutador

9. Si existe algún signo de daños, manipulación incorrecta o alteración del empaquetado o el producto, se deberá contactar con el soporte de Huawei inmediatamente. No se considera segura su operación en dicha situación.

4.2 ENTORNO DE INSTALACIÓN SEGURO

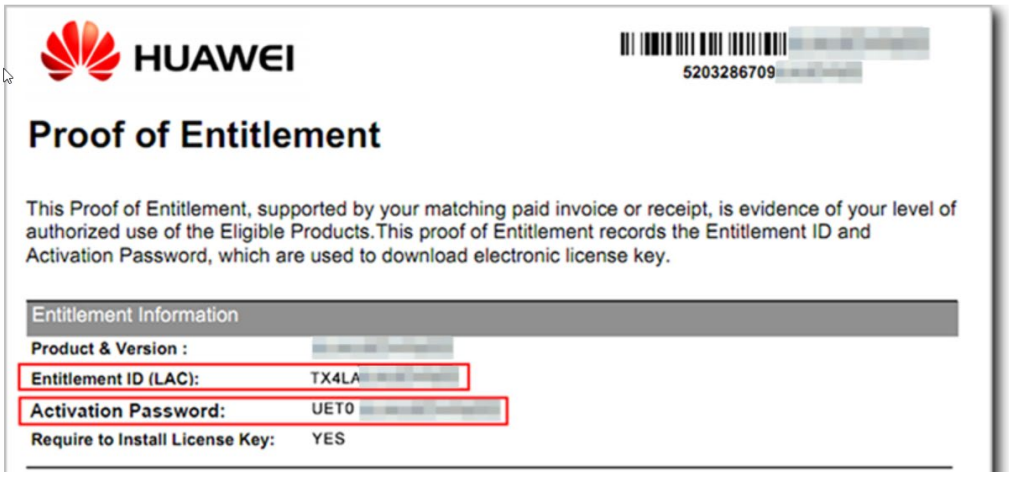
10. Los componentes del producto deben instalarse en un Centro de Proceso de Datos (CPD) o entorno seguro, al cual solo personal técnico limitado dispondrá de acceso y estará autorizado para realizar actividades de configuración, despliegue y mantenimiento del producto.

4.3 REGISTRO Y LICENCIAS

11. Para los *Huawei AR Series Routers* existen dos (2) tipos de licencias:

    - **Licencia COMM**: licencia comercial, adquirida por contrato. Tienen una validez permanente o, en algunos casos, un periodo de validez hasta una fecha determinada. Existen funcionalidades especiales que requieren una licencia específica.
    - **Licencia temporal:** La licencia temporal también se conoce como licencia DEMO, que se utiliza para fines especiales como pruebas y ensayos.

12. Para realizar el registro de la licencia del producto es necesario localizar el ID de derecho (*Entitlement ID*) o la contraseña de activación de la licencia. Este documento es enviado al usuario junto con el producto o por email.


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 – ID de derecho y clave de activación del producto

13. Para introducir la licencia, se debe acceder a la línea de comandos del producto e Iniciar sesión. Se debe ejecutar el comando '*display license esn'* para obtener el ESN del dispositivo. El registro de la licencia a través de la interfaz de comandos se ha de realizar una vez se ha instalado el producto según indica el apartado 5 INSTALACIÓN.

14. Seguir los pasos del apartado "*Obtaining COMM Licenses for New Site Projects*" de [REF1] para descargar la licencia mediante activación por contraseña (*Password Activation*) o activación por ID (*Entitlement Activation*).

15. A continuación, se debe cargar el fichero en el producto mediante SFTP en el directorio raíz. Para activar este servicio se debe seguir el apartado "*Managing Files When the Device Functions as an SFTP Server*" de la guía de documentación del producto [REF1] y ejecutar el siguiente comando:

    [Huawei] sftp server enable

16. Usar el comando '*license active* <nombre del archivo>' mediante 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 COMPONENTES DEL ENTORNO DE OPERACIÓN

17. El producto debe estar compuesto por los siguientes elementos *hardware* en su entorno de operación:

    - **Servidor de Administración de Red (*Network Management Server* o NMS):** sistema de administración que utiliza un cliente SSH instalado para conectarse al producto de forma segura.
    - **Consola Local:** sistema conectado al producto por puerto serie para la administración local de este.
    - **Servidor *Syslog*:** servidor externo donde se transmiten los de registros de auditoría. Para una comunicación segura con este servidor, se utiliza el protocolo TLS.
    - **Servidor NTP:** servidor para la sincronización de fecha y hora del producto.

5. INSTALACIÓN

18. La instalación física del producto, así como las medidas de precaución a tomar para cada uno de los diferentes casos se deben realizar siguiendo la guía [REF1] en el apartado "*Installation*" > "*Hardware Installation and Manteinance Guide"*

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 al sistema de administración local por puerto serie (puerto "*console*")

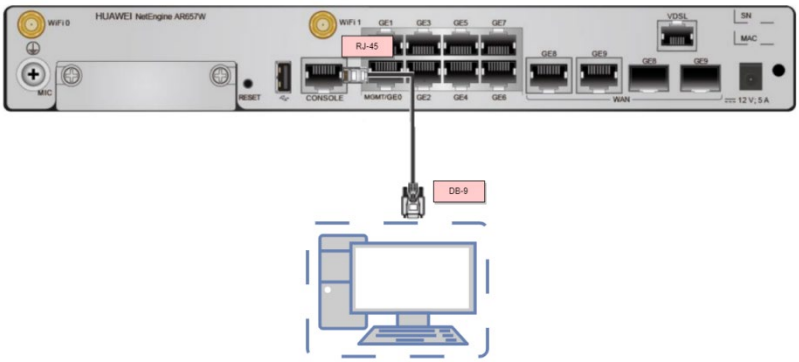


Ilustración 5 – Diagrama de conexión al puerto consola usando AR651W

20. Para conectarse al producto por al puerto "*console*" es necesario iniciar un *software* emulador de terminal como *PuTTy*. Consultar el apartado "*Logging In to a Device Through the Console Port"* de [REF1] para más información del procedimiento.

21. Al conectarse por primera vez a la interfaz serial, el producto requerirá una contraseña para el usuario '*root*' entre 8 y 16 caracteres. Para una configuración segura, **se debe seguir la política de contraseñas** indicada en el apartado 6.3.2 CONFIGURACIÓN DE ADMINISTRADORES.

```
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 queda operativa la interfaz de comandos a través del puerto serie para realizar la posterior configuración del dispositivo.

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

23. No es necesario ningún comando especial para activar el modo de operación seguro en el dispositivo. La configuración necesaria para que el producto opere de forma segura consistirá en aplicar una serie de configuraciones y políticas de seguridad a través de la interfaz de línea de comandos que se irán indicando en los siguientes apartados.

6.2 AUTENTICACIÓN

24. Los mecanismos de autenticación que utiliza el producto **para la autenticación de usuarios** son los siguientes:

    - **Credenciales**: mediante un usuario y contraseña de acceso. Utilizada tanto para autenticación tanto local como SSH.
    - **Clave pública:** uso de clave pública con algoritmos *ssh-rsa* para autenticación SSH.

25. Los mecanismos de autenticación que utiliza el producto **para la autenticación de otros sistemas** o dispositivos son los siguientes:

    - Certificado TLS para comunicarse con un servidor *Syslog* externo.
    - Clave pre-compartida con cifrado *HMAC-SHA256* para las comunicaciones con un servidor NTP externo. Este proceso se describe en "*Configuring NTP Operating Modes*" de la documentación del producto [REF1].

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

26. El producto puede ser administrado de forma local o remota:

    – **Administración local:** se realiza a través de la interfaz serial o puerto serie. Para ello es necesario conectar un equipo al producto con un cable de consola. Para acceder a las funciones de administración de la línea de comandos es necesario autenticarse como usuario administrador.

    – **Administración remota:** se realiza a través de SSH. Para acceder a las funciones de administración remota de la línea de comandos es necesario autenticarse con las credenciales de un usuario autorizado para conectarse por SSH al producto.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

27. En el producto se asignarán privilegios y permisos determinados a cada usuario, según un nivel definido por una escala numérica indicando el parámetro "Privilegio

de Usuario" (*User Privilege*). Por defecto, los usuarios que acceden al producto por la interfaz de comandos tienen un nivel del 3 al 15 (administradores), y los demás tendrán un nivel de 0 (visitantes). En la siguiente tabla se muestran los niveles de privilegio de usuario 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.
3-15	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

28. Para más información sobre los privilegios de usuario, consultar el apartado *"admin-user privilege level"* de [REF1]. **Se debe asignar a los usuarios los mínimos privilegios necesarios** para realizar sus labores de administración

29. Para la **creación de usuarios**, se debe consultar los apartados "*Configuring a Local User"* y *"Configuring an SSH User"* de [REF1] para el procedimiento en detalle sobre la configuración y creación de usuarios.

30. A continuación, se procederá a la configuración de la política de contraseñas, parámetros de sesión y establecimiento de privilegios de administrador.

31. Primeramente, se debe acceder a la interfaz de línea de comandos (indicada con la entrada *"<Huawei>"*) y autenticarse como usuario '*root*'. Posteriormente, se debe acceder al modo "*system-view".* Esta vista permite los comandos de configuración del dispositivo:

    <Huawei> system-view

32. Cuando se entra en este modo, la línea de comandos lo indicará mostrando la entrada "*[Huawei]".* Todas las configuraciones que se realicen en este modo se indicarán con dicha entrada en el presente documento.

33. A continuación, se debe acceder al modo "*Authentication, Authorization, and Accounting" (aaa)* con el siguiente comando:

    [Huawei] aaa

34. En este modo se configurarán los parámetros de política de seguridad de contraseñas y sesión.

35. Las contraseñas establecidas para los usuarios deberán cumplir con los siguientes requisitos mínimos:

    - **Longitud mínima de la contraseña: doce (12) caracteres**.

      [Huawei-aaa] set password min-length 12

    - **La contraseña debe incluir letras mayúsculas, letras minúsculas, números y símbolos especiales**. El comando '*complexity-check*' establece que tres (3) de los cuatro (4) tipos sean obligatorios a la hora de establecer una contraseña:

      [Huawei-aaa] user-password complexity-check

    - Para una configuración segura, **no se recomienda utilizar ninguna de las cinco (5) contraseñas anteriores:**

      [Huawei-aaa] local-aaa-user password policy access-user

      [Huawei-aaa-lupp-acc] password history record number 5

    - Para usuarios administradores se permite añadir un tiempo de validez en días a la política de las contraseñas tras el cual expiran, por defecto 90 días.

      [Huawei-aaa] local-aaa-user password policy administrator

      [Huawei-aaa-lupp-admin] local-user <usuario> *password expire 90*

36. Con respecto a los parámetros de sesión, **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:**

    [Huawei-aaa] access-user remote authen-fail retry-interval 5 retry-time 3 block-time 5

37. Se debe volver al modo '*system-view*' *(*volver a la vista de comandos anterior se realizará con el comando *'quit')* y **establecer un tiempo de inactividad para finalizar las sesiones remotas SSH**. Se recomienda cinco (5) minutos:

    [Huawei-aaa] quit

    [Huawei] ssh server timeout 300

38. Se debe establecer también un per**iodo de inactividad para finalizar las sesiones por puerto serie**:

    [Huawei] user-interface console 0

    [Huawei-ui-console0] idle-timeout 5

39. Para asignar un nivel específico de privilegios, "*User Privilege*" a un usuario es necesario acceder a la interfaz de línea de comandos del producto con un usuario con privilegios de nivel 3-15 y acceder a la vista "*aaa*":

    [Huawei] aaa

40. Posteriormente, se puede asignar a un usuario un nivel de 0 a 15 de privilegios:

    [Huawei-aaa] local-user <nombre_usuario> *privilege level* <nivel>

41. Finalmente, se **debe establecer un *banner* de inicio de sesión** con un mensaje de aviso y consentimiento:

    [Huawei] header login information <MENSAJE>

42. Guardar los cambios efectuados:

    [Huawei] save all

43. Se recomienda acceder a los apartados *"UI Configuration Commands"*, *"NAC Configuration Commands"*, *"CLI Overview Commands"*, *"User Login Configuration Commands"* y "*AAA Configuration Commands*" de [REF1] en caso de necesitar más información para utilizar los comandos mencionados.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

44. **Se deben deshabilitar todas las interfaces que no se encuentren en uso**. A continuación, se muestran los comandos a utilizar mediante un ejemplo:

    [Huawei] interface 10gE 0/0/1

    [Huawei-10gE0/0/1] shutdown

    [Huawei-10gE0/0/1] display this

45. Consultar el apartado *"Interface Management Commands"* y *"Basic Interface Configuration Commands"* de [REF1] para más información sobre los comandos de gestión de interfaces.

6.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

46. El protocolo SSHv2 es utilizado por el producto para la administración remota por los usuarios autorizados. El acceso a través de SSH deberá configurarse, primeramente, de forma que se **deshabilite el soporte a la versión insegura de *SSHv1.x***:

    [Huawei] undo ssh server compatible-ssh1x enable

47. A continuación, **se debe definir como 3072 bits la longitud de las claves RSA**:

    [Huawei] rsa local-key-pair create

    # Input the bits in the modulus [default = 2048]: ***3072***

48. Se define una ciphersuite de cifrado segura para el intercambio de claves en SSH y el método rsa como clave pública:

[Huawei] ssh server key-exchange ***dh_group15_sha512***

[Huawei] ssh server cipher ***aes256_ctr aes128_ctr***

[Huawei] ssh server ***hmac sha2_256***

49. Deshabilitar protocolos inseguros: **Telnet y FTP deben deshabilitarse**, tal y como se indica a continuación:

    [Huawei] undo telnet server enable

    [Huawei] undo telnet ipv6 server enable

    [Huawei] undo ftp server enable

    [Huawei] undo ftp ipv6 server enable

50. También **debe deshabilitarse el uso de HTTP**:

    [Huawei] set insecure-protocol disable

51. Para una configuración segura de privilegios, se debe **implementar una política segura para el acceso al sistema** (*system view*), ejecutando el siguiente comando:

    [Huawei] command-privilege level 3 view system execute

52. El protocolo TLS se debe utilizar estrictamente para la comunicación con el servidor de auditoría externo. Para su configuración segura, **se deben seguir los siguientes pasos**:

    [Huawei] system-view

    [Huawei] ssl policy <nombrePolitica> *type client*

    [Huawei] server verify enable

53. El producto usa por defecto TLS 1.2. Para la **configuración de ciphersuites seguras**, se deben ejecutar los siguientes comandos:

    [Huawei] ssl policy huawei

    [Huawei] prefer-ciphersuite ***ecdhe_rsa_aes256_gcm_sha384***

54. Se recomienda el uso de esta ciphersuite para una configuración segura. **No deben configurarse** las ciphersuites rsa_3des_cbc_sha ni rsa_aes_128_cbc_sha, ya que no se consideran seguras.

55. Para más información sobre las ciphersuites que se pueden configurar, consultar el apartado del comando '*prefer-ciphersuite*' de la documentación del producto [REF1].

Protocolo	Descripción de cifrados
TLS	Ciphersuite: *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384* Establecimiento de clave: *EC Diffie-Hellman Ephemeral* Firma criptográfica: RSA Algoritmo de cifrado: AES 256 GCM Autenticación de mensajes: HMAC_SHA384

Protocolo	Descripción de cifrados
SSH	Establecimiento de clave: dh_group15_sha512 Firma criptográfica: ecdsa-sha2-nistp521 Algoritmo de cifrado: AES256_CTR, AES128_CTR Autenticación de mensajes: HMAC-SHA2-256

Tabla 3 – Cifrado seguro recomendado para el producto en su modo de operación seguro.

56. Consultar los apartados *"User Login Configuration Commands" y "File Management Commands" y "SSL Configuration Commands*" de [REF1] para más información sobre los comandos utilizados.

57. Para más información sobre los mecanismos de cifra recomendamos, se recomienda consultar la **guía *CCN-STIC 807 Criptología de Empleo en el ENS*** [REF2].

6.6 GESTIÓN DE CERTIFICADOS

58. El producto usa certificados X.509v3 para autenticarse con el servidor *syslog* externo. Los certificados pueden ser generados con la herramienta OpenSSL y luego cargados en el producto mediante SFTP. En el apartado "*Managing Files When the Device Functions as an SFTP Server*" de [REF1] se detalla cómo activar el servidor de SFTP del producto y gestionar archivos mediante dicho protocolo.

59. Se debe acceder al servidor con las mismas credenciales que las utilizadas para la autenticación SSH de forma que el producto permita al administrador descargar o subir ficheros.

60. **Se debe importar un certificado de las CA raíz** mediante los siguientes comandos (una vez el certificado ya se encuentra cargado en la memoria del producto):

    [Huawei] pki realm <pkiname>

    [Huawei-pki-realm-<pkiname>] *quit*

    [Huawei] pki import-certificate ca realm <pkiname> pem filename <CA_raiz>

61. El producto verifica la vigencia de un certificado, comprobándolo contra su propia fecha y hora. Además, se puede subir al producto un archivo CRL para comprobar si los certificados siguen siendo válidos. Consultar la sección "*Manual CRL Update*" del apartado "*Configuring Local Certificate Check*" de la documentación del producto [REF1] para su configuración.

62. Para más información sobre certificados, consultar el apartado "*Installing a CA Certificate for a PKI Entity"* y obtener información sobre los comandos en el apartado *"PKI Configuration Commands*" de [REF1].

6.7 SERVIDORES DE AUTENTICACIÓN

63. Para una configuración segura del producto, **no se recomienda el uso de un servidor de autenticación externo RADIUS**. Únicamente se deben configurar los mecanismos de autenticación previamente indicados en el apartado 6.2 AUTENTICACIÓN.

6.8 SINCRONIZACIÓN

64. **Los dispositivos de la organización deben estar sincronizados para que las referencias de tiempo sean correctas y uniformes.**

65. La sincronización horaria del producto se puede realizar **por medio de un servidor NTP externo**. Para que el producto se conecte con el servidor NTP externo, se deben introducir los siguientes comandos en la consola CLI:

    [Huawei] ntp unicast-peer ip-address <IP_ServidorNTP>

66. Para una conexión segura, es necesario configurar una clave predefinida tanto en el servidor NTP como en el *switch*. Para la configuración de la clave en el producto, se deben ejecutar las siguientes instrucciones a través de la interfaz de comandos:

    [Huawei] ntp-service authentication enable

    [Huawei] ntp-service authentication-keyid <numero_identificador_asignar_clave> *authentication-mode hmac-sha256 cipher* <clave>

    [Huawei] ntp-service trusted authentication-keyid <numero_identificador_asignar_clave>

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

    [Huawei] clock datetime

68. Para más información de cómo configurar el servidor NTP, se recomienda consultar el ejemplo de la documentación [REF1] *"Example for Configuring Authenticated NTP Unicast Server/Client Mode"* en el apartado "*NTP Configuration*".

6.9 ACTUALIZACIONES

69. **El producto contempla dos (2) tipos de actualizaciones, que deben ser desplegadas lo antes posible**:

    - **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, comprobando que esté firmado con la firma legítima de Huawei. Su extensión es ".pat".
    - ***Software/firmware* del sistema:** 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".

70. Ambos tipos de actualizaciones pueden descargarse de la web oficial de Huawei (*https://support.huawei.com*) y deben de subirse al directorio raíz del producto mediante SFTP.

71. Para configurar un paquete de parches como el paquete de parches por defecto del sistema debe ejecutarse la siguiente instrucción:

    <Huawei> patch load <nombre_Parche>*.pat all run*

72. Para configurar un *software* del sistema como el software por defecto del producto se deben ejecutar los siguientes comandos:

    <Huawei> startup system-software <nombre_System_Software>.cc

    <Huawei> startup saved-configuration vrpcfg.zip

    <Huawei> reboot fast

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

    <Huawei> display startup

6.10 AUTO-CHEQUEOS

74. 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).

75. No es necesario realizar ninguna configuración para la ejecución de dichos autochequeos. Se realizan por defecto.

6.11 SNMP

76. Opcionalmente, el producto puede funcionar como agente SNMP, enviando mensajes SNMP a un NMS. Debe consultarse el apartado *"Configuring a Device to Communicate with an NMS Using SNMP"* de [REF1] para su configuración.

77. Para una configuración segura, **se debe asegurar el uso del protocolo SNMPv3**:

    [Huawei] snmp-agent sys-info version v3

78. Se debe definir también la **autenticación de usuario con SHA2-256** (*authentication-mode*) y el cifrado con AES-256 (*privacy-mode*).

79. Para información adicional sobre la configuración de SNMP, consultar el apartado "*Configuring Basic SNMPv3 Functions*" de [REF1].

6.12 AUDITORÍA

6.12.1 REGISTRO DE EVENTOS

80. El producto almacena, por defecto, 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 (ejemplo: *login*, reseteo de clave…).
Autor 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

6.12.2 ALMACENAMIENTO LOCAL

82. El producto guarda en el directorio "*logfile*" (que se encuentra en el directorio raíz) un archivo llamado "*log.log*", donde se almacenan los registros de auditoría.
83. Cuando el archivo "*log.log*" supera un tamaño determinado, se guarda automáticamente en un archivo con extensión ".zip" llamado log_5_<fechaDelLog>.log.zip, vaciándose el archivo "log.log".
84. Para visualizar los registros de auditoría se debe de ejecutar el comando:

    <Huawei> save logfile

<Huawei> more <nombre_archivo_auditoria> *all*

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

6.12.3 ALMACENAMIENTO REMOTO

86. **Se debe configurar un servidor *syslog* externo puede configurar para el almacenamiento externo de registros de auditoría**. La comunicación con dicho servidor se realizará de **forma cifrada mediante TLS 1.2.**

87. 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):

  [Huawei] info-center enable

  [Huawei] info-center channel 1 name loghost1

- Especificar la dirección IP donde se encuentra el servidor *syslog* externo:

  [Huawei] info-center loghost <IP_servidor_syslog> *channel loghost1*

- Especificar el nivel mínimo de *logs* a enviar:

  [Huawei] info-center source arp channel loghost1 log level notification

- Crear una política de SSL para la comunicación segura:

  [Huawei] ssl policy <nombrar_politica_SSL>

- Cargar el certificado de CA almacenado en el producto previamente:

  [Huawei] pki realm <pkiname>

  [Huawei-pki-realm-<pkiname>] *quit*

  [Huawei] pki import-certificate ca realm <pkiname> *pem filename* <CA_raiz>

- Configurar que el producto use la política de SSL configurada para las comunicaciones con el servidor syslog externo:

  [Huawei] info-center loghost <IP_servidor_syslog> *channel loghost1 transport tcp ssl-policy* <nombre_dado_politica_SSL> *verify-dns* <syslog_DNS>

6.13 COPIAS DE SEGURIDAD

88. El producto almacena su configuración (inicialmente vacía) en el fichero "*vrpcfg.zip*", que se encuentra en el directorio raíz. Para realizar un guardado de la configuración actual del producto (políticas implementadas, interfaces creadas, configuraciones de seguridad, etc.) en el fichero "vrpcfg.zip" se debe de ejecutar el siguiente comando:

<Huawei> save all vrpcfg.zip

89. No obstante, **se recomienda guardar la configuración del producto de forma automática cada cierto periodo de tiempo**. Esto se consigue mediante el siguiente comando:

    <Huawei> set save-configuration interval <rango_30_43200_minutos>

90. 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 el siguiente comando:

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

6.14 FUNCIONES DE SEGURIDAD

91. **El producto dispone de defensas contra ataques DoS que deben ser activadas**, incluyendo SYN *Flood*, *Land*, *Smurf* e ICMP *Flood*. Para ello, se deben ejecutar los siguientes comandos en la interfaz de línea de comandos:

    [Huawei] anti-attack tcp-syn enable

    [Huawei] anti-attack udp-flood enable

    [Huawei] anti-attack icmp-flood enable

    [Huawei] anti-attack abnormal enable

    [Huawei] anti-attack fragment enable

92. **El producto permite evitar ataques ARP**. Esto lo consigue mediante el aprendizaje de ARP, limitando la proporción de paquetes ARP relacionándolos con direcciones MAC o limitando la proporción de paquetes ARP por interfaz, entre otros. Se recomienda ejecutar las siguientes instrucciones:

    - Se limita el máximo de paquetes ARP que cualquier dirección MAC puede enviar por segundo. Lo mismo para IP:

      [Huawei] Arp speed-limit source-mac maximum <numero_paquetes_segundo>

      [Huawei] 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:

      [Huawei] arp speed-limit source-mac <dirección_MAC> maximum <numero_paquetes_segundo>

      [Huawei] arp speed-limit source-mac <dirección_IP> maximum <numero_paquetes_segundo>

- Limitar el máximo de paquetes ARP en una interfaz o VLAN:

  [Huawei] interface <interfaz> <numero_interfaz | vlan <id_vlan>

  [Huawei] arp anti-attack rate-limit enable

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

- Configurar el aprendizaje de direcciones ARP:

  [Huawei] 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):

      [Huawei] dhcp snooping enable ipv4

    - Definir una interfaz y la VLAN a la que pertenece como interfaz de confianza para DHCP:

      [Huawei] interface <tipo_interfaz> <numero_interfaz>

      [Huawei-<interfaz>] *dhcp snooping trusted*

      [Huawei-<interfaz>] *quit*

      [Huawei] vlan <numero_vlan>

      [Huawei] dhcp snooping trusted interface <tipo_interfaz> <numero_interfaz>

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

      [Huawei] dhcp snooping user-bind arp-detect enable

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

      [Huawei] dhcp snooping user-offline remove mac-address

94. Se recomienda seguir los pasos de configuración descritos en el apartado "*Security Configuration Guide*" de [REF1] si se desea implementar ACL, ARP o DHCP de forma segura, además de más información sobre los servicios de seguridad del producto.

7. 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 regular de los parches de seguridad**, con objeto de mantener una configuración segura.
- **Realización copias de seguridad periódicas y pruebas la restauración** de las mismas. Además de almacenarlos en localizaciones seguras y planificar el proceso de automatización.
- **Correcto mantenimiento y análisis 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.

8. *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			
Configuración de sistemas administradores	☐	☐	
Configuración de usuarios administradores	☐	☐	
Configuración de interfaces puertos y servicios	☐	☐	
Configuración de protocolos seguros	☐	☐	
Configuración de certificados	☐	☐	
Sincronización horaria (Configuración del servidor NTP)	☐	☐	
Configuración del servidor de auditoría	☐	☐	
Configuración de las copias de seguridad	☐	☐	
Configuración de las funciones de seguridad	☐	☐	
OPERACIÓN			
Comprobaciones periódicas del hardware y software.	☐	☐	
Aplicación regular de los parches de seguridad	☐	☐	
Realización copias de seguridad periódicas	☐	☐	
Almacenamiento protegido de los registros de auditoría	☐	☐	
Análisis de los registros de auditoría	☐	☐	

Tabla 5. *Checklist*

9. REFERENCIAS

[REF1] *NetEngine AR V300R019 Product Documentation*
https://support.huawei.com/enterprise/en/doc/EDOC1100087042

[REF2] CCN-STIC-807

10.ABREVIATURAS

ACL	*Access Control List*
ARP	*Address Resolution Protocol*
AES	*Advanced Encryption Standard*
AAA	*authentication, authorization, and accounting*
DEMO	*Demonstration License*
DRBG	*Deterministic Random Bit Generator*
DHCP	*Dynamic Host Configuration Protocol*
ESN	*Equipment Serial Number*
HMAC	*Hash-based Message Authentication Code*
COMM	*Commercial Licenses*
NMS	*Network Management System*
NTP	*Network Time Protocol*
RADIUS	*Remote Authentication Dial-In User Service*
SSH	*Secure Shell*
SSL	*Secure Sockets Layer*
SNMP	*Simple Network Management Protocol*
SYN	*Synchronization*
TLS	*Transport Layer Security*
VLAN	*Virtual Large Area Network*
VRP	*Versatile Routing Platform*

PUBLICACIONES DE DEFENSA

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