centro criptológico nacional

# Guía de Seguridad de las TIC
# CCN-STIC 1452

# Procedimiento de Empleo Seguro
# Huawei NetEngine AR6700 y AR8000


Abril 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


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
2024.04.29 10:21:32 +02'00'

NIPO: 083-24-160-0.
Fecha de Edición: abril 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. **Huawei NetEngine AR6700 y AR8000** son routers que proveen SD-WAN, enrutamiento, conmutación, VPN y funciones de seguridad.
2. Los productos se componen de *hardware* y *software*, proporcionando la capacidad de procesamiento de tráfico de red. El software está compuesto por la plataforma Yunshan 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 plataforma.
3. La plataforma 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

4. El objeto del presente documento es facilitar la instalación y configuración segura del producto con la versión software V600R021C10SPC100, en conjunción con los siguientes modelos hardware:

| Serie Hardware | Modelo Hardware |
|---|---|
| AR8000 | AR8140-12G10XG |
| | AR8140-T-12G10XG |
| AR6700 | AR6710-L26T2X4 |
| | AR6710-L26T2X4-T |
| | AR6710-L50T2X4 |
| | AR6710-L50T2X4-T |

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

5. Los enrutadores AR6700 y AR8000 han sido cualificados en el catálogo CPSTIC para la **familia "Enrutadores"**.

# 3 ORGANIZACIÓN DEL DOCUMENTO

6. Este documento recoge el uso del producto en sus distintas fases de su ciclo de vida, en los siguientes apartados:

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

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

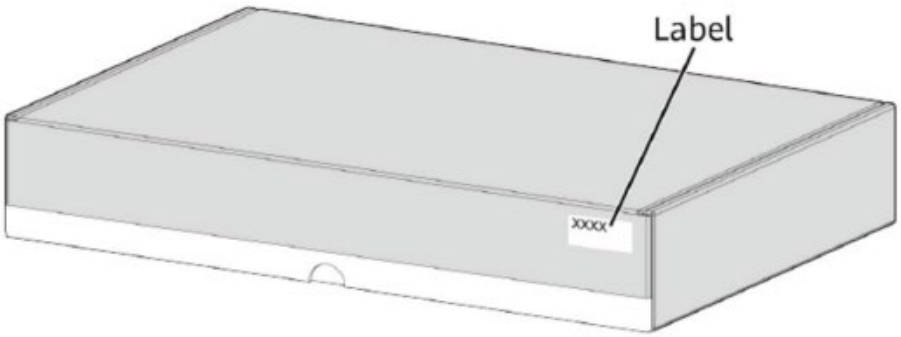
   c) Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

# 4 FASE PREVIA A LA INSTALACIÓN

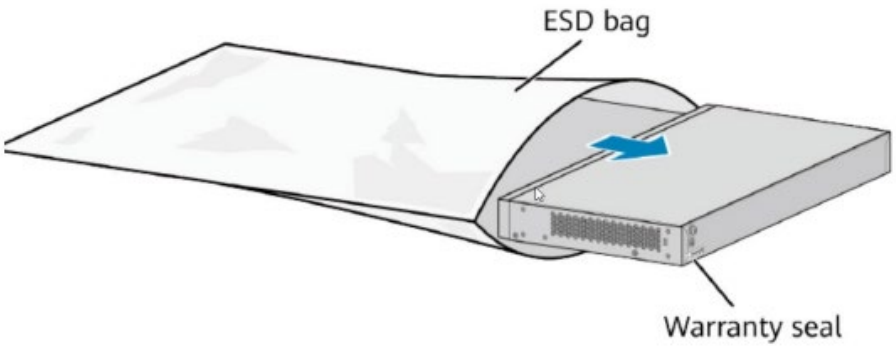
## 4.1 ENTREGA SEGURA DEL PRODUCTO

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




   - **Sello de garantía:** se debe 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.




8. 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

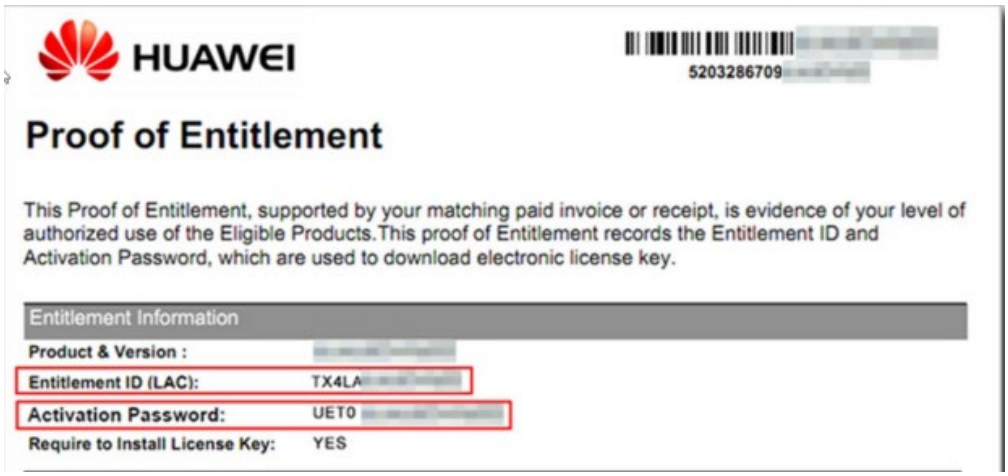
9. Los componentes del producto deben instalarse en un Centro de Proceso de Datos (CPD) o entorno seguro, al cual sólo personal técnico limitado dispondrá de acceso y estará autorizado para realizar actividades de configuración, despliegue y mantenimiento del producto.

## 4.3 REGISTRO Y LICENCIAS

10. 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.

11. 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 |

12. 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 FASE DE INSTALACIÓN.

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

14. 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 *"Configuring a Device as an SFTP Server"* de la guía de documentación del producto [REF1] y ejecutar el siguiente comando:

*[Huawei] sftp server enable*

15. User 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.
```

## 4.4 CONSIDERACIONES PREVIAS

16. Si fuese necesaria una configuración adicional **relativa a la seguridad, previa a iniciar la instalación y configuración** del producto, deben indicarse **paso a paso en este documento** aquellos aspectos que se deban tener en cuenta, puesto que influirán en la forma de configurarlo de forma segura.

17. Por ejemplo: preparación de otros componentes necesarios (token de entropía, almacén de claves criptográficas, plataformas hardware, etc.), decisión sobre aspectos de arquitectura física (por ejemplo, alta disponibilidad), o lógica (por ejemplo, métodos de autenticación).

## 4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

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

    - **Consola Local:** sistema conectado al producto por puerto serie para la administración local de este.
    - **Servidor Syslog:** servidor externo donde se transmiten los registros de auditoría. Para una comunicación segura con este servidor, se utiliza el protocolo TLS 1.2 o superior.

19. Si se requiere hacer uso de la funcionalidad de administración remota, el entorno además debe incluir el siguiente componente:

    - **Servidor de Administración de Red (*Network Management Server)*:** Sistema de administración que utiliza un cliente SSH instalado para conectarse al producto de forma segura.

# 5 FASE DE INSTALACIÓN

20. 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*".

21. 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 el puerto serie.

22. Como se describe en el apartado "*First Login Through the Console Port*" en [REF1], utilizar herramientas de terceros como PuTTY. Una vez conectado con los datos como se indican en la sección previamente mencionada, clicar **Enter** e introducir una contraseña como se muestra por la terminal.

```
Please Press ENTER.

Please configure the login password (8-16)
Enter Password:
Confirm Password: //Enter the password for logging in to the device through the console port.
Info: Save the password now. Please wait for a moment.
Info: The max number of VTY users is 21, the number of current VTY users online is 1, and total number of terminal users online i
s 2.
     The current login time is 2020-06-30 18:15:10+08:00
<HUAWEI>
```

23. 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

24. No es necesario ninguna configuración extra para activar el modo de operación seguro del dispositivo. La configuración necesaria para que el producto opere de forma segura está descrita en las siguientes secciones.

## 6.2 AUTENTICACIÓN

25. Los mecanismos empleados por el producto para la **autenticación de usuarios** son los siguientes:

    - **Credenciales:** mediante un usuario y contraseña de acceso. Utilizadas tanto para autenticación local como remota, a través de SSH.
    - **Clave pública:** uso de clave pública con algoritmos *ssh-ecc* para la autenticación remota mediante SSH como se describe en la sección *"Example for Configuring STelnet Login"* en [REF1].

26. Los mecanismos empleados por el producto para **autenticar otros sistemas** o dispositivos son los siguientes:

    - **Certificado TLS** para comunicarse con un servidor Syslog.

## 6.3 ADMINISTRACIÓN DEL PRODUCTO

### 6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

27. El producto puede ser administrado de forma local o remota de la siguiente forma:

    - **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 un 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. Para que el producto permita esta comunicación, se deberán ejecutar los siguientes comandos desde la consola de administración local:

      ```
      system-view
      ecc local-key-pair create
      stelnet server enable
      sftp server enable
      ssh server key-exchange ecdh_sha2_nistp256
      ```

28. De esta forma se ha activado el servicio SSH como se describe en [REF1], sección "Configuring *the SSH Server Function and Related Parameters*".

### 6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

29. El producto asigna privilegios y permisos a cada usuario. Estos privilegios y permisos dependen del nivel de dicho usuario, definido en una escala numérica. El privilegio por defecto es tres (3), el mayor valor, pero este puede variar entre cero (0) y tres (3). El nivel cero (0) se considera "*visit",* el nivel uno (1) se considera "*monitoring*", el nivel dos (2) se considera "*configurator*" y el nivel tres (3) "*management*". A niveles más altos se le otorgan los permisos de los niveles anteriores, el nivel (2) puede ejecutar funciones de "*configurator*" de igual manera que de "*monitoring*" y "*visit*".

30. Estos niveles se pueden consultar en la sección "*admin-user privilege level*" de [REF1].

31. Para crear un usuario, se ejecutará el comando "*local-user <nombre de usuario> password irreversible-cipher <contraseña>"*, si previamente se entró al submenú de configuración "*aaa"*.

32. Tener en cuenta los siguientes aspectos:

- **Configuración de la Política segura de contraseñas**. Deberá cumplir con los siguientes requisitos mínimos:
    - Longitud mínima de la contraseña: doce (12) caracteres. Ejecutando el comando "*set password min-length 12"* se ajusta la longitud mínima.
    - Composición de la contraseña: letras mayúsculas, letras minúsculas, números y símbolos especiales. Recomendar el uso de los cuatro (4) grupos si el producto lo permite, y al menos un mínimo de tres (3) grupos. Para configurar esto, ejecutar el comando "*user-password complexity-check"*.
    - Número de contraseñas anteriores que no se permite utilizar: al menos, cinco (5). Para configurar esta característica, ejecutar el comando "*local-aaa-user password policy access-user*" y tras este comando ejecutar "*password history record number 5*".
    - Tiempo de validez en días de las contraseñas tras el cual expiran para los administradores (por defecto 90 días). Ejecutar el comando "*local -aaa-user password policy administrator*", seguido por el comando "*local-user <usuario> password expire 90"*.
    - Número de días que deben transcurrir tras el cambio de una contraseña antes de poder modificarla de nuevo: diez (10) días.
- **Configuración de los parámetros de sesión**:
    - Tiempo de inactividad de las sesiones: cinco (5) minutos. Para ello, ejecutar el siguiente comando "*user-interface console 0"*, seguido del comando "*idle-timeout 5*"
    - Número de intentos fallidos de inicio de sesión: tres (3) intentos y tiempo de bloqueo tras los intentos fallidos: cinco (5) minutos. Ejecutando el comando "*accdess-user remote authen-fail retry-interval 5 retry-time 3 block-time 5*" se logra configurar el número de intentos fallidos a la vez que un bloqueo de cinco (5) minutos.
- Configuración del mensaje de aviso y consentimiento en el inicio de sesión (**login banner**). Ejecutar el comando "*header login information <mensaje>"*.

## 6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

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

```
interface <nombre de la interfaz>
shutdown
display this
```

34. Consultar el apartado "*Interface Management Commands*" de [REF1] para más información de los comandos de gestión de interfaces.

## 6.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

35. 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
```

36. A continuación, se **debe definir como 521 bits la longitud de las claves ECC**:

```
[Huawei] ecc local-key-pair create
# Input the bits in the modulus [default = 521]: 521
```

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

```
[Huawei] ssh server key-exchange ecdh_sha2_nistp521
[Huawei] ssh server cipher aes128_gcm aes256_gcm
[Huawei] ssh server publickey ecc
```

38. 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
```

39. Deshabilitar protocolos inseguros: Telnet, FTP y SNMP 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
[Huawei] undo snmp-agent protocol server disable
[Huawei] undo snmp-agent protocol server ipv4 disable
[Huawei] undo snmp-agent protocol server ipv6 disable
```

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

```
[Huawei] set insecure-protocol disable
```

41. 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
```

42. 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 type client
[Huawei] server verify enable
```

43. El producto usa por defecto TLS 1.2, aunque se recomienda TLS 1.3. Para la **configuración de ciphersuites seguras**, se deben ejecutar los siguientes comandos:

```
[Huawei] ssl cipher-suite-list <nombreParaLaCipherSuite>
[Huawei] set cipher-suite tls13_aes_256_gcm_sha384
[Huawei] quit
[Huawei] ssl policy <nombrePolitica>
[Huawei] binding cipher-suite-customization <nombreDadoACipherSuite>
```

44. 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.

45. Para más información sobre las ciphersuites que se pueden configurar, consultar el apartado del comando 'set cipher-suite' de la documentación del producto [REF1].

| Tipo | Descripción suite de cifrado |
|---|---|
| **TLS** | Suite de Cifrado:<br>TLS_AES_256_GCM_SHA384<br>Establecimiento de clave: ECDHE<br>Grupos de Diffie-Hellman:<br>brainpoolP256r1tls13<br>brainpoolP384r1tls13<br>brainpoolP512r1tls13 |
| **SSH** | Establecimiento de clave: ecdsa-sha2-nistp521<br>Método de clave pública: ECDSA-SHA2-*<br>Algoritmos de cifrado:<br>AEAD_AES_128_GCM<br>AEAD_AES_256_GCM |

**Tabla 2 – Cifrado seguro recomendado para el producto en su modo de operación seguro.**

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

## 6.6 GESTIÓN DE CERTIFICADOS

47. El producto usa certificados X509 para autenticarse con el servidor Syslog externo. Los certificados pueden generarse con la herramienta OpenSSL, para ser posteriormente

cargados al producto mediante SFTP. Para saber más acerca de este servicio, refiérase a la sección "*Managing Files When the Device Functions as an SFTP Server*" en [REF1].

48. Se debe acceder al servicio SFTP utilizando las mismas credenciales utilizadas para acceder por SSH a administrar el producto.

49. Se debe importar un certificado de las CA raíz mediante los siguientes comandos, tras haber cargado los ficheros en el producto.

```
pki realm <nombre dominio>
quit
pki import-certificate ca realm <nombre dominio> pem filename <fichero CA raíz>
```

50. El producto verifica la validez del certificado comparando la fecha de validez de este contra la fecha establecida en el producto.

51. Para más información acerca de los certificados, consultar el apartado "*Installing a CA certificate for a PKI Entity*" en [REF1].

## 6.7 SERVIDORES DE AUTENTICACIÓN

52. Para una configuración segura del producto, no se recomienda el uso de servidores de autenticación externos. Únicamente se deben configurar los mecanismos de autenticación previamente indicados en el aparado 6.2 AUTENTICACIÓN.

## 6.8 SINCRONIZACIÓN

53. Para que el producto esté sincronizado en fecha y hora, un administrador deberá ajustar la fecha de acuerdo a la sección "*System Time Configuration Commands*" de [REF1]. Esto se logrará ejecutando los siguientes comandos desde system-view:

```
[Huawei] clock datetime <HH:MM:SS AAAA-MM-DD>
[Huawei] clock timezone <ciudad> add/minus <número de horas a sumar/restar respecto a UTC>
```

## 6.9 ACTUALIZACIONES

54. 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".
- **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".

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

56. Para configurar un paquete de parches como el paquete por defecto del producto, se debe ejecutar el comando "*patch load <nombre del fichero>.pat all run*".
57. Para configurar un firmware del sistema se deben ejecutar los siguientes comandos:

```
startup system-software <nombre del fichero>.cc
startup saved-configuration vpcfg.zip
reboot fast
```

58. Verificar que la instalación de firmware/patch ejecutar el comando "*display startup*".

## 6.10 AUTO-CHEQUEOS

59. Cuando el producto se enciende o se reinicia realiza los siguientes autochequeos:
    - Autochequeo de integridad del software del sistema.
    - Autochequeo de los algoritmos de cifrado (AES, HMAC, DRBG, SHA256/512, firmado con RSA).
60. No es necesario realizar ninguna configuración para la ejecución de dichos autochequeos.

## 6.11 ALTA DISPONIBILIDAD

61. La configuración de **Alta Disponibilidad** puede consultarse en la sección "*High Availability Configuration*" en [REF1].

## 6.12 AUDITORÍA

### 6.12.1 REGISTRO DE EVENTOS

62. El producto almacena, por defecto, los siguientes eventos de seguridad en sus registros de auditoría:
    - Inicio y cierre de sesión de usuarios
    - Inicio de las acciones de auditoría
    - Cambio o generación de claves criptográficas
    - Resetear o cambiar claves
    - Intentos de inicio de sesión 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 inicio de actualización
    - Fallos al establecer una sesión SSH
63. El producto guarda la siguiente información de los eventos auditados.

| 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, etc.). |
| Autor que produce el evento | Usuario e IP (si corresponde). |
| Resultado | Resultado del evento, si aplica. |

### 6.12.2 ALMACENAMIENTO LOCAL

64. El producto almacena en el directorio "/logfile" un fichero llamado "log.log", donde se registran los logs de auditoría.
65. Cuando el archivo "log.log" supera un tamaño determiando, se guarda automáticamente en un archivo con extensión ".zip" llamado log_<fecha del log>.zip, vaciando el archivo "log.log" tras esto.
66. Para consultar los archivos de auditoría se deben ejecutar los siguientes comandos:

```
save logfile
more <nombre del fichero de auditoría> all
```

67. Si el producto alcanza el límite de almacenamiento, se sobrescribirán los registros más antiguos.

### 6.12.3 ALMACENAMIENTO REMOTO

68. **Se debe configurar un servidor Syslog externo para el almacenamiento remoto de registros de auditoría**. La comunicación con dicho servidor se realizará cifrada mediante **TLS 1.2**.
69. Una vez generados lo certificados y configurados en el servidor Syslog externo, el certificado de CA debe subirse al producto mediante SFTP. Luego, se accederá al producto por la interfaz de comandos y se seguirán los siguientes pasos:

- Habilitar el módulo de envío de logs a un dispositivo externo con los comandos:

```
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 <Nombre de la política SSL>
```

- Cargar el certificado de CA almacenado en el producto previamente

```
pki realm <nombre domino>
quit
pki import-certificate ca realm <nombre dominio> pem filename <fichero CA
    raíz>
```

- Configurar le producto para usar la política SSL configurada para las comunicaciones con el servidor Syslog externo:

```
Info-center loghost <IP servidor Syslog> channel loghost1 transport tcp ssl-
    policy <nombre dado a la política> verify-dns <Syslog DNS>
```

## 6.13 BACKUP

70. 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:

```
save all vrpcfg.zip
```

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

```
set save-configuration interval <rango 30-43200 minutos>
```

72. El archivo de configuración debe almacenarse en un dispositivo diferente al producto, ya sea descargándolo manualmente por medio de SFTP o a través de un servidor SFTP externo de forma automática mediante el siguiente comando:

```
set save-configuration backup-to-server <IP servidor> transport-type sftp
    port <puerto> user <usuario> password <contraseña> path <directorio
    servidor>
```

# 7 REFERENCIAS

[REF1] NetEngine AR V600R022C10 Product Documentation Library Version: 02 Date: 2022-05-13

# 8 ABREVIATURAS

| | |
|---|---|
| AES | Advanced Encryption Standard |
| COMM | Commercial |
| CPD | Centro de Proceso de Datos |
| CPSTIC | Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación |
| DEMO | Demonstration |
| DRBG | Deterministic Random Bit Generator |
| ECC | Elliptic Curve Cryptography |
| ECDHE | Elliptic Curve Diffie-Hellman Ephemeral |
| HMAC | Hash-Based Message Authentication Code |
| NTP | Network Time Protocol |
| RSA | Rivest–Shamir–Adleman |
| SD-WAN | Software-Defined Wide Area Network |
| SFTP | Secure File Transfer Protocol |
| SSH | Secure Shell |
| Syslog | System Logging |
| TLS | Transport Layer Security |
| VPN | Virtual Private Network |

PUBLICACIONES DE DEFENSA

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