centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1452

Procedimiento de Empleo Seguro
Huawei NetEngine AR5700, AR6700 y AR8000 Series Routers

Julio 2026

Edita:

Centro Criptológico Nacional, 2026

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.07.28 09:21:14 +02'00'

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1 INTRODUCCIÓN

Huawei NetEngine AR5700, AR6700 y AR8000 Series Routers son routers que proveen SD-WAN, enrutamiento, conmutación, VPN y funciones de seguridad. 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.

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.

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

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). La versión del *firmware* evaluada es: V600R023C00SPC100.

El producto Huawei NetEngine AR5700, AR6700 y AR8000 Series Routers ha sido incluido en el catálogo CPSTIC, para conocer el listado, la categoría o nivel y la familia consulte el sitio web del [CPSTIC].

3 ORGANIZACIÓN DEL DOCUMENTO

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 y operación del producto, para lograr una configuración segura.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

Los Huawei NetEngine AR5700, AR6700 y AR8000 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 comprobar que la etiqueta presente en el embalaje exterior concuerda con el modelo de enrutador NetEngine adquirido.

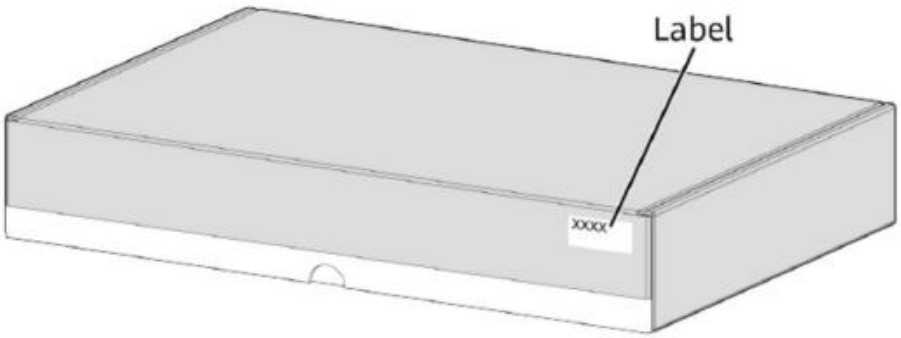

Ilustración 1 Embalaje exterior

- **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.

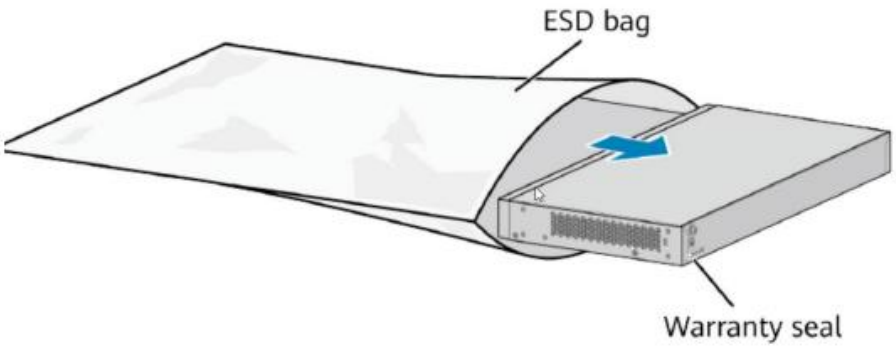

Ilustración 2 Router y posición del sello de garantía

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

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

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.

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 Obtención de licencias

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.

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

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 [GUÍA_PRODUCTO] y ejecutar el siguiente comando:

```
[Huawei] sftp server enable
```

Use el comando '*license active <nombre del archivo.dat>*' 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 Activación de la licencia

4.4 CONSIDERACIONES PREVIAS

No se requiere la realización de ninguna configuración adicional relativa a la seguridad previa al inicio de la instalación y configuración del producto. La instalación y configuración del producto puede realizarse directamente siguiendo los pasos descritos en las diversas secciones de este documento, los cuales ya contemplan todas las medidas necesarias para garantizar su empleo seguro conforme al entorno operativo previsto.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

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

- **Consola Local:** equipo de administración 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.

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

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

5 FASE DE INSTALACIÓN

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_PRODUCTO] en el apartado "*Installation > Hardware Installation and Maintenance Guide"*.

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 equipo de administración local por el puerto serie.

Como se describe en el apartado "*First Login Through the Console Port*" en [GUÍA_PRODUCTO], 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>
```

Ilustración 5 Configuración de contraseña de consola

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

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.

Al acceder a la interfaz de línea de comandos y autenticarse, se entra en el privilegiado con:

```
system-view
```

Se accede al modo AAA:

```
aaa
```

Se debe configurar 16 caracteres como la longitud mínima de contraseña:

```
local-user policy password min-len 16
```

Se debe configurar un intervalo de reintento de autenticación de 5 minutos, un máximo de 3 intentos de autenticación fallidos, y un tiempo de bloqueo de 5 minutos para prevenir ataques de fuerza bruta:

```
local-user authentication lock times 3 5
```

- Los parámetros utilizados son: `<failed-times>` y `<period>`, respectivamente.

```
local-user authentication lock duration 5
```

- El parámetro utilizado es `<duration-time>`.

Se vuelve al modo *system-view*:

```
quit
```

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

```
command-privilege level 3 view system execute
```

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
#
…
```

Se deshabilita el servidor inseguro de TELNET:

```
telnet server disable
telnet ipv6 server disable
```

Se deshabilita el servidor inseguro de FTP:

```
undo ftp server enable
```

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

```
undo ssh server compatible-ssh1x enable
```

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

```
rsa local-key-pair-create
y
4096
```

Se definen las suites de cifrado seguras para el cifrado en SSH:

```
ssh server cipher aes256_gcm aes128_gcm
```

Se definen 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
```

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>
```

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

```
undo snmp-agent
undo dhcp enable
```

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
```

Finalmente, para prevenir ataques del tipo *VLAN Hopping* se ha de ejecutar el siguiente comando:

```
drop ilegal-mac enable
```

Se guardan todos los cambios:

```
commit
save
y
```

6.2 AUTENTICACIÓN

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 [GUÍA_PRODUCTO].

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

La administración local del producto se realiza a través de la interfaz serial. Conecte un PC al producto con un cable de consola. Para acceder a las funciones de administración de la línea de comandos, autentíquese con la contraseña del usuario root definida en la sección 5 FASE DE INSTALACIÓN.

La administración remota del producto se realiza a través de SSH. Conecte un PC al producto con un cable Ethernet en una interfaz física habilitada para tal propósito. Para acceder a las funciones de administración de la línea de comandos, autentíquese con las credenciales de un usuario autorizado para conectarse por SSH al producto.

En la sección 6.1 MODO DE OPERACIÓN SEGURO se define cómo deshabilitar protocolos inseguros como telnet, HTTP o FTP.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

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 1 Permisos por nivel de privilegio

Para asignar un nivel específico de "user privilege" a un usuario, acceda a la interfaz de línea de comandos del producto con un usuario con "user privilege" 3 y acceda a la vista AAA:

```
system-view
aaa
```

Luego, asigne a un usuario un nivel de 0 a 3 de privilegios:

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

Todo usuario con "privilege level" 3 debe cumplir políticas seguras de contraseñas. Estas políticas se configuran para las cuentas de administrador y se aplican a los usuarios correspondientes.

Se debe establecer, al menos, los siguientes parámetros:

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

```
system-view
aaa
local-aaa-user password policy administrator
password min-length 16
```

- La complejidad (uno o más caracteres en minúscula, uno o más caracteres en mayúscula, uno o más números, uno o más caracteres especiales):

```
password complexity four-of-kinds
password history record number 10
```

- El historial de contraseñas (se deben guardar 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.
- El cambio de contraseñas. El producto debe forzar a los usuarios a cambiar su contraseña cada cierto tiempo. Se recomienda cada 60 días.

```
password expire 60
password alert before-expire 7
```

El parámetro "alert before-expire" especifica el número de días de anticipación con los que se notifica a los usuarios que sus contraseñas están a punto de caducar.

Todo usuario con "privilege level" 3 debe establecer políticas seguras de sesión como:

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

```
system-view
ssh server timeout <tiempo_segundos>
```

- *Timeout* de inactividad para la interfaz SERIAL:

```
system-view
user-interface console 0
```

```
idle-timeout <tiempo_minutos> <tiempo_segundos>
```

- Número máximo de intentos fallidos de autenticación, y tiempo de espera tras superar un umbral. Se define en la sección 6.1 MODO DE OPERACIÓN SEGURO.

2. Se debe configurar un banner de inicio de sesión. Todo usuario con "privilege level" 3 debe definirlo a través del siguiente comando:

```
header login information <MENSAJE>
```

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

3. Deben deshabilitarse las interfaces físicas que no se utilicen y los servicios inseguros (TELNET, FTP…) como ya se especifica en la sección 6.1 MODO DE OPERACIÓN SEGURO.
4. El producto puede usar SSH para la administración remota y la comunicación con un servidor Syslog externo.
5. El producto usa por defecto suites de cifrado con TLS 1.2, aunque se recomienda utilizar TLS 1.3.
6. En la sección 6.1 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 —las cuales se encuentran incluidas 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 2 Suites de cifrado usadas por el producto en su modo de operación seguro

6.5 GESTIÓN DE CERTIFICADOS

7. El producto usa certificados X.509 autoafirmados para comunicarse con un servidor Syslog externo. Sin embargo, se recomienda la importación de certificados de una infraestructura PKI que cumplan con la política de seguridad del organismo. En el módulo "Files When the Device Functions as an SFTP Server" de [GUÍA_PRODUCTO] se detalla cómo activar el servidor de SFTP del producto; luego, se accede a este con las mismas credenciales que para SSH, pudiendo descargar o subir ficheros.

8. 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>
```

9. Se debe configurar el producto para que verifique la vigencia de los certificados. Para ello, puede cargarse un fichero CRL en el sistema con el fin de validar los certificados localmente, o bien configurar la dirección de un servidor OCSP para que este consulte en línea el estado de revocación de los certificados frente a la autoridad emisora correspondiente.

6.6 SERVIDORES DE AUTENTICACIÓN

10. El producto soporta la integración con servidores de autenticación externos (por ejemplo, RADIUS). No obstante, para la configuración evaluada, no se recomienda su uso, priorizando el uso de mecanismos de autenticación locales en el TOE. Únicamente se deben configurar los mecanismos de autenticación previamente indicados en el aparado 6.2 AUTENTICACIÓN.

6.7 SINCRONIZACIÓN

11. El producto soporta la sincronización de fecha y hora mediante servidores NTP externos. No obstante, el uso de estos introduce una dependencia adicional del entorno de operación, por lo que deberá asegurarse su correcta configuración y protección. La configuración del servicio NTP deberá realizarse de acuerdo con la sección "NTP Configuration" de [GUÍA_PRODUCTO].

12. De forma alternativa, el administrador podrá configurar manualmente la fecha y hora del sistema mediante los siguientes comandos desde system-view (Para información adicional ver la sección "*System Time Configuration Commands*" de [GUÍA_PRODUCTO]):

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

6.8 ACTUALIZACIONES

13. El producto contempla dos (2) tipos de actualizaciones. Se recomienda que los administradores verifiquen periódicamente la disponibilidad de nuevas actualizaciones y avisos de seguridad publicados por el fabricante.
14. En particular, se recomienda realizar dicha comprobación con una periodicidad al menos semanal, tomando como referencia los canales oficiales del fabricante (por ejemplo [SA_PORTAL] https://securitybulletin.huawei.com/enterprise/en/security-advisory), donde se publican avisos de seguridad y actualizaciones relevantes.
15. La frecuencia de aplicación de las actualizaciones deberá ajustarse en función de la criticidad de las vulnerabilidades corregidas y del impacto en el entorno operativo.
    - **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".
16. Ambos tipos de actualizaciones pueden descargarse de la web oficial de Huawei [DESCARGA_SOFTWARE] (https://support.huawei.com/enterprise/en/software/index.html) y deben subirse al directorio raíz del producto mediante SFTP.
17. 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*".
18. 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
```

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

6.9 AUTO-CHEQUEOS

20. 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).
21. No es necesario realizar ninguna configuración para la ejecución de dichos autochequeos.

6.10 ALTA DISPONIBILIDAD

22. El producto soporta configuraciones de Alta Disponibilidad con el objetivo de mejorar la continuidad del servicio y la tolerancia a fallos. No obstante, la activación de mecanismos de Alta Disponibilidad no introduce requisitos adicionales desde el punto de vista del empleo seguro del producto.

23. En caso de que el administrador decida desplegar el producto en una arquitectura de Alta Disponibilidad, la configuración detallada de estos mecanismos puede consultarse en la sección “High Availability Configuration” de [GUÍA_PRODUCTO].

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

24. El producto almacena los siguientes eventos de seguridad en sus registros de auditoría:

- Inicio y cierre de sesión de los usuarios.
- Inicio de las acciones de auditoría.
- Cambio o generación de claves criptográficas.
- Cambios en la configuración del producto.
- Restablecer o cambiar claves.
- Intentos de inicio de sesión fallidos.
- Configuración o eliminación de un servidor NTP.
- Terminación de una sesión local o remota por el usuario o por inactividad.
- Intentos de iniciar una actualización.
- Fallos al establecer una sesión SSH.

25. 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 3 Información que se guarda en los registros de auditoría

6.11.2 ALMACENAMIENTO LOCAL

26. El producto almacena en el directorio “/logfile” un fichero llamado “log.log”, donde se registran los logs de auditoría.

27. Cuando el archivo “log.log” supera un tamaño determinado, se guarda automáticamente en un archivo con extensión “.zip” llamado log_<fecha del log>.zip, vaciando el archivo “log.log” tras esto.

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

```
display logfile <nombre_archivo_auditoria>
```

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

6.11.3 ALMACENAMIENTO REMOTO

30. 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.

31. 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 el 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>
```

32. Para más información consultar la sección “Information Management Configuration Commands” en [GUÍA_PRODUCTO].

6.12 BACKUP

33. 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
```

34. 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>
```

35. 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>
```

36. Por último, los registros de auditoría del sistema pueden enviarse a un servidor *syslog* externo, como se define en la sección 6.11 AUDITORÍA.

37. Para más información consultar la sección “Managing Configuration Files” en [GUÍA_PRODUCTO].

7 REFERENCIAS

[GUÍA_PRODUCTO]	NetEngine AR5700, AR6700, and AR8000 V600R023C00 Product Documentation (https://support.huawei.com/enterprise/en/doc/EDOC1100318335)
[DESCARGA_SOFTWARE]	https://support.huawei.com/enterprise/en/software/index.html
[SA_PORTAL]	https://securitybulletin.huawei.com/enterprise/en/security-advisory
[CPSTIC]	https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

8 ABREVIATURAS

AAA	Authentication, Authorization, and Accounting
AES	Advanced Encryption Standard
CA	Certificate Authority
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
DHCP	Dynamic Host Configuration Protocol
DRBG	Deterministic Random Bit Generator
ECC	Elliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ENS	Esquema Nacional de Seguridad.
FTP	File Transfer Protocol
HMAC	Hash-Based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
MAC	Media Access Control
NMS	Network Management System
NTP	Network Time Protocol
OS	Operating System
OCSP	Online Certificate Status Protocol
PYME	Pequeña y Mediana Empresa
RADIUS	Remote Authentication Dial-In User Service
RSA	Rivest–Shamir–Adleman
SD-WAN	Software-Defined Wide Area Network
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
Syslog	System Logging
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VPN	Virtual Private Network