centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1419

Procedimiento de Empleo Seguro
Routers Huawei NE40E Series

Septiembre de 2021

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.01.28 11:17:30 +01'00'

NIPO: 083-21-167-5

Fecha de Edición: septiembre de 2021

ÍNDICE

1. INTRODUCCIÓN

1. Los **enrutadores** de la serie HUAWEI NetEngine40E (NE40E) se despliegan en el borde de las redes troncales IP, en las redes IP de área metropolitana (MAN) y otras redes IP a gran escala. Funcionan en conjunto con enrutadores *core* para proporcionar una solución de red IP completa y jerárquica.
2. Disponen del sistema operativo *Versatile Routing Platform* (VRP) desarrollado por Huawei y utilizan la tecnología de reenvío basado en hardware y conmutación de datos sin bloqueo. Presentan las siguientes características:
   - Fiabilidad de clase *carrier*, capacidad de reenvío a velocidad de línea, excelente capacidad de expansión, mecanismo de calidad de servicio (QoS).
   - Capacidades de acceso y agregación de servicios, configuraciones flexibles con diversas funciones, como enrutamiento por segmentos sobre IPv6 (SRv6), *Ethernet* flexible (FlexE), telemetría de información de flujo in situ (iFIT), VPN *Ethernet* (EVPN), red privada virtual de capa 2 (L2VPN), red privada virtual de capa 3 (L3VPN), multidifusión, VPN multidifusión (MVPN), conmutación de etiquetas multiprotocolo (MPLS), ingeniería de tráfico (TE) y QoS, para garantizar la fiabilidad de la transmisión de servicios.
   - Compatibilidad con IPv6 y transición fluida de IPv4 a IPv6.
3. A continuación, se recogen sus principales características respecto a la seguridad:

Funcionalidad	Descripción
Administración de usuarios	▪ Gestión de la autorización de usuarios basada en AAA. ▪ Control del proceso de autorización de los usuarios, incluido el control basado en grupos de usuarios y el control basado en grupos de tareas. ▪ Gestión jerárquica de la autoridad de comandos, que impide que los usuarios no autorizados manejen los dispositivos. ▪ Autenticación y autorización HWTACACS.
Autenticación segura	▪ AAA. ▪ Autenticación HMAC-SHA256 para protocolos de enrutamiento (RIPv2, OSPF e IS-IS). ▪ Autenticación de conexión, GTSM y RPKI para BGP. ▪ Cifrado y autenticación para SNMPv3.
Dirección MAC	▪ Limitación de direcciones MAC ▪ Eliminación de direcciones MAC

Funcionalidad	Descripción
Supresión de tráfico desconocido	▪ Administración del tráfico de los usuarios ▪ Ancho de banda definido para cada usuario
Defensa contra ataques ARP	▪ Límite de entradas ARP basado en la interfaz. ▪ Supresión de la marca de tiempo basada en las direcciones IP de destino y origen de las entradas ARP. ▪ Comprobación de la dirección de destino de los paquetes ARP. ▪ Aislamiento bidireccional de ARP. ▪ Filtrado de paquetes ARP.
IGMP snooping	▪ El NE40E admite *IGMP snooping* en las interfaces de capa 2 y en los PW de VPLS.
DHCP snooping	▪ El NE40E admite *DHCP snooping* en las interfaces de capa 2 y en los PW de VPLS.
Keychain	▪ Autenticación de llaveros para aplicaciones no TCP. ▪ Autenticación de llavero para aplicaciones TCP.
Información de las cabeceras	▪ Obtención de las cabeceras de los paquetes enviados a las CPUs. ▪ Obtención de las cabeceras de los paquetes a reenviar.
Local anti-attack	▪ Listas blancas. ▪ Listas negras. ▪ Flujo definido por el usuario. ▪ Protección de enlace activo (ALP). ▪ Compensación del paquete más pequeño. ▪ Asociación de la capa de aplicación. ▪ Protección del plano de gestión y de servicio. ▪ Defensa contra ataques a paquetes TCP/IP. ▪ Rastreo del origen de los ataques. ▪ Descarte y límite de velocidad en función del rango TTL.

Funcionalidad	Descripción
SSHv2	▪ El NE40E puede actuar como cliente y servidor STelnet y cliente y servidor SFTP. Tanto el NE40E con STelnet como con SFTP son compatibles con SSH1 (SSH1.5) y SSH2 (SSH2.0).
IPsec	▪ Modo de transporte y modo de túnel. ▪ IKEv2. ▪ GRE sobre Ipsec. ▪ NAT trasversal. ▪ L3VPN. ▪ Fragmentación y reensamblaje de paquetes. ▪ *Keepalive* y DPD para la detección de pares. ▪ Acceso remoto dinámico a Ipsec. ▪ IPsec PKI. ▪ Clave precompartida. ▪ CMPv2, que gestiona los certificados en línea y simplifica la gestión y el mantenimiento de los mismos. ▪ Copia de seguridad de doble dispositivo Ipsec. ▪ VXLAN sobre Ipsec.

Tabla 1. Características de seguridad del producto

2. OBJETO Y ALCANCE

4. La configuración evaluada del producto y por lo tanto incluida en la presente guía de empleo seguro consiste en la combinación del ***software/firmware* V800R010C00SPC200 y el parche V800R010SPH220T** con los modelos de los enrutadores Huawei NE40E Series:

   - ***NE40E-X3A.***
   - ***NE40E-X16A.***

3. ORGANIZACIÓN DEL DOCUMENTO

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

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

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

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

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

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

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

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

6. Al tratarse de una combinación hardware/software, los enrutadores de la serie HUAWEI NetEngine40E se entregan por correo ordinario. Por ello, es necesario realizar las siguientes acciones:

   a) **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.

   b) **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.

   c) **Desembalaje de las partes del producto**. Después de desembalar los productos, se debe comprobar si el número total de productos coincide con el número indicado en la lista de empaque.

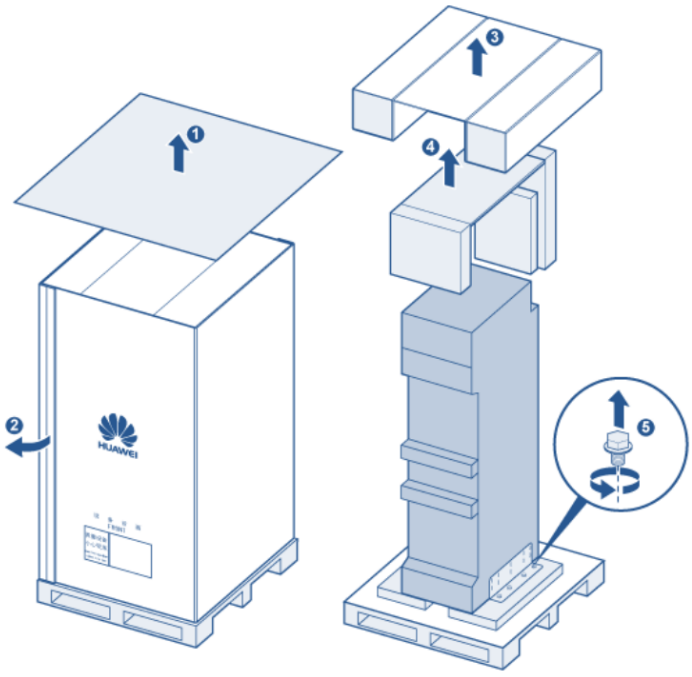


Ilustración 1. Desembalaje del producto

   d) **Sello de Garantía**. Se deberá verificar que el sello de garantía de la unidad esté intacto. El chasis no se puede abrir sin que este sello sea destruido.

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

4.2 ENTORNO DE INSTALACIÓN SEGURO

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

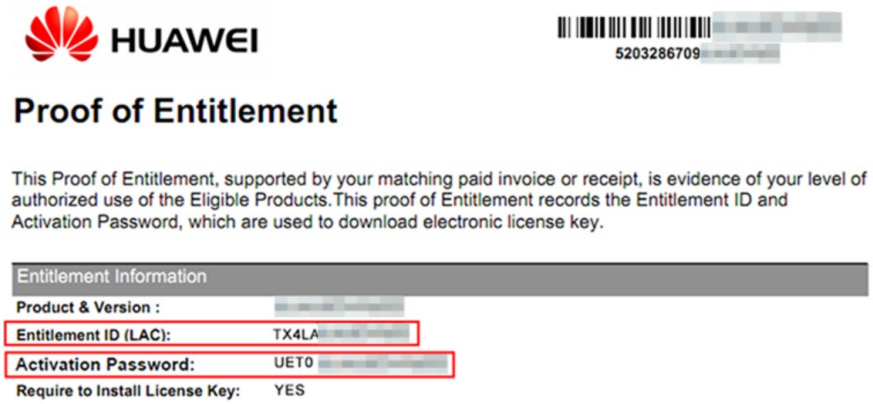
4.3 REGISTRO Y LICENCIAS

9. Para el producto existen varios tipos de licencias:

- **GTL**: El archivo de licencia se preinstala en un dispositivo antes de la entrega o puede descargarse del sitio *web* de ESDP, en función del contrato del proyecto y del ESN del dispositivo. Las licencias comerciales y las no comerciales (excluidas las de prueba) se presentan físicamente como archivos de licencia.
- **Licencia RTU de *Hardware***: Las licencias RTU de *hardware* controlan el permiso de uso de los puertos en las placas o en los dispositivos en forma de caja que se venden en el modelo de consumo (CM). Si las licencias RTU no están activadas para dichos puertos, el uso de los mismos está restringido.
- **Licencia de servicio**: Hay dos (2) tipos de licencias de servicio:
  - Licencia de servicio de control de funciones: este tipo de licencia tiene efecto en todo el dispositivo.
  - Licencia de servicio de control de recursos: este tipo de licencia tiene efecto en la tarjeta de una ranura específica o en un puerto específico.
- **Licencia de prueba**: Una licencia de prueba contiene todas las características soportadas por el dispositivo, incluyendo los recursos de licencia de RTU y de servicio. Cada vez que se habilita una licencia de prueba, puede utilizarse durante un máximo de 90 días. Cuando el periodo de prueba termina, las funciones controladas pierden su validez inmediatamente o después de reiniciar la tarjeta o el dispositivo.

10. Para realizar el registro de la licencia del producto, es necesario:

a) Localizar el ID de derecho o la contraseña de activación de la licencia.


HUAWEI

5203286709

Proof of Entitlement

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

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

Ilustración 2. Documento legal donde aparece la clave de activación

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

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

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

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

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

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

Ilustración 3. Activación de la licencia

4.4 INSTALACIÓN

11. La instalación física del producto, así como las medidas de precaución a tomar para cada uno de los diferentes casos se puede encontrar en la [GUÍA_PRODUCTO] en los módulos bajo "*Installation*" → "*Installation Guide*" → "*Installing NE40E-X16A*" y los módulos bajo "*Installation*" → "*Installation Guide*" → "*Installing NE40E-X3A*" dependiendo del modelo. No obstante, se puntualiza que el lugar de instalación debe consistir en un lugar aislado y con buena ventilación, al que solo tenga acceso el personal autorizado.

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

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

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

Parámetro	Configuración
Data bits	8

Tabla 2. Configuración de parámetros para conectarse al producto por consola

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

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

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

Ilustración 4. Configuración de la contraseña de inicio del usuario *root*

15. De esta forma, ya estaría operativa la interfaz de comandos a través de la conexión *serial*. Para configurar el acceso por SSH es necesario:
    - Iniciar sesión en el NE40E mediante la interfaz de consola y configurar una dirección IP para cada interfaz del NE40E.
    - Asegurarse de que hay una ruta directa o alcanzable entre el cliente SSH y el producto.
16. Para configurar el acceso y los usuarios SSH se deben seguir los pasos descritos en el módulo "*Logging In to the NE40E by Using SSH*" de la [GUÍA_PRODUCTO].
17. Se recomienda cambiar la interfaz e IP por la cual se accede al producto por SSH. En el siguiente ejemplo se configura una IP en una interfaz y luego se permite el acceso por SSH:

    system-view

    interface <tipo_interfaz> <numero_interfaz>

    ip address <ip_deseada> <máscara>

    quit

    ssh server-source -i <tipo_interfaz_declarada> <numero_interfaz_declarado>

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

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

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

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

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

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

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

    command-privilege level 3 view system execute
25. Se deshabilita el servidor inseguro de TELNET:

    undo telnet server enable

    undo telnet ipv6 server enable
26. Se deshabilita el servidor inseguro de FTP:

    undo ftp server enable
27. Se **deshabilita** el soporte a la versión insegura de **SSHv1.x**:

    undo ssh server compatible-ssh1x enable
28. Se define como **3072 bits la longitud de las claves RSA** (longitud por defecto del producto para claves RSA):

    rsa local-key-pair-create

    y
29. Se define una ***suite* de cifrado segura** para el intercambio de claves en SSH:

    ssh server key-exchange dh_group_exchange_sha256

30. Se define una ***suite* de cifrado seguras** para el encriptado en SSH:

    ssh server cipher aes256_gcm

31. Se define una ***suites* de cifrado segura** para HMAC en SSH:

    ssh server hmac sha2_256

32. Se define el método de RSA como algoritmo de clave pública:

    ssh server publickey rsa

33. Se define una *suite* de cifrado segura para TLSv1.2:

    ssl cipher-suite-list <nombreParaLaCipherSuite>

    set cipher-suite tls12_ck_rsa_with_aes_128_gcm_sha256 tls12_ck_rsa_with_aes_256_gcm_sha384

    quit

    ssl policy <nombrePolitica>

    binding cipher-suite-customization <nombreDadoACipherSuite>

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

    undo ipv6

    undo snmp-agent

    undo rip 100

    undo isis 100

    undo dhcp enable

35. Se guardan los cambios:

    save all

    y

5.2 AUTENTICACIÓN

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

    - Credenciales locales, mediante un usuario y contraseña de acceso.
    - Autenticación mediante servidor externo HWTACACS.

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

    - Certificado TSL/SSL para comunicarse con un servidor *syslog* externo.
    - Clave pre-compartida con cifrado HMAC-SHA256 para las comunicaciones con un servidor NTP externo.

- Clave pre-compartida para cifrar la comunicación entre un servidor RADIUS externo y el producto.

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

38. La administración local del producto se realiza a través de la interfaz *serial*. Para ello, es necesario conectar un PC al producto con un cable de consola. Para acceder a las funciones de administración de la línea de comandos es necesario autenticarse con la contraseña del usuario *root* definida en *4.4 INSTALACIÓN*.

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

40. En la sección 5.1 MODO DE OPERACIÓN SEGURO se define como deshabilitar protocolos inseguros como telnet o FTP.

5.3.2 CONFIGURACIÓN DE ADMINISTRADORES

41. 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 15 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.
3-15	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

"User Privilege"	Permisos	Descripción
		configuración a nivel de comandos y comandos de depuración.

Tabla 3. Nivel de privilegios y permisos asociados

42. Para asignar un nivel específico de "*user privilege*" a un usuario es necesario acceder a la interfaz de línea de comandos del producto con un usuario con "*user privilege*" 15 y acceder a la vista aaa:

    system-view

    aaa

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

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

44. Todo usuario con "*privelege level*" 15 puede establecer políticas seguras de contraseñas tales como:

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

      system-view

      set password min-length 16

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

      system-view

      aaa

      user-password complexity-check three-of-kinds

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

      system-view

      aaa

      local-aaa-user password policy administrator

      password history record number 10

      local-aaa-user password policy access-user

      password history record number 10

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

      system-view

aaa

local-aaa-user password policy administrator

password expire 120

local-aaa-user password policy access-user

password expire 120

45. **Se deben configurar tiempos de cierre de sesión tras un tiempo mínimo de inactividad**. Se recomienda, siempre que sea posible, que no exceda de los 10 minutos. Para configurar los cierres de sesión, utilizar un usuario con "*privelege level*" 15 para establecer las políticas seguras de sesión:

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

      system-view

      ssh server timeout <tiempo_segundos>

    - *Timeout* de inactividad para la interfaz SERIAL:

      system-view

      user-interface console 0

      idle-timeout <tiempo_minutos> <tiempo_segundos>

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

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

    header login information <MENSAJE>

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

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

5.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

48. El producto usa *SSH* para administración remota y TLS para la comunicación con un servidor *syslog* externo.

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

50. En la sección *5.1 MODO DE OPERACIÓN SEGURO* se configuran las siguientes suites de cifrado para SSH y TLS —los cuales se encuentran incluidos en la guía CCN-STIC-807 con la fortaleza adecuada para categoría ALTA en el ámbito del Esquema Nacional de Seguridad —, a excepción del grupo de establecimiento de

claves para SSH y TLS (grupo 14), por ello, **se deben limitar las conexiones del producto, solo permitiendo que las comunicaciones se realice de forma local en los canales internos de la organización**:

Tipo	Descripción suite de cifrado
TLS	Suites de Cifrado: *TLS_RSA_WITH_AES_128_GCM_SHA256 y TLS_RSA_WITH_AES_256_GCM_SHA384* Establecimiento de clave: *diffie-hellman-group14-sha1* Firma criptográfica: *RSA 3072 bits.* Algoritmos de cifrado: *AES 128 GCM* y *AES 256 GCM* Autenticación de mensajes: *HMAC_SHA256*
SSH	Establecimiento de clave: *diffie-hellman-group14-sha1* Firma criptográfica: *SSH-RSA 3072 bits* Algoritmos de cifrado: *AEAD_AES_128_GCM* y *AEAD_AES_256_GCM* Autenticación de mensajes: *HMAC-SHA1, HMAC-SHA1-96, HMAC-SHA2-256*

Tabla 4. Suites de cifrado configuradas en el producto

5.6 GESTIÓN DE CERTIFICADOS

51. El producto usa certificados X.509 autoafirmados para comunicarse con un servidor *syslog* externo. **Sin embargo, se recomienda la importación de certificados que cumplan con la política de seguridad del organismo**. En el módulo "*sftp server enable*" de la [GUÍA_PRODUCTO] se detalla como activar el servidor de SFTP del producto; luego, se accede a este con las mismas credenciales que para SSH, pudiendo descargar o subir ficheros.

52. 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>

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

5.7 SERVIDORES DE AUTENTICACIÓN

54. El producto puede utilizar un servidor HWTACACS externo como servidor de autenticación; una vez el servidor HWTACACS esté listo para configurar junto al producto, se deberán seguir los pasos descritos en la [GUÍA_PRODUCTO] en el

módulo "*Example for Configuring HWTACACS Authentication and Authorization for Administrators*".

5.8 SINCRONIZACIÓN HORARIA

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

    system-view

    ntp-service unicast-server <IP_ServidorNTP>

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

    System-view

    ntp-service authentication enable

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

    ntp-service reliable authentication-keyid <numero_asignado_a_clave>

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

    clock datetime

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

5.9 ACTUALIZACIONES

59. El producto contempla dos (2) tipos de actualizaciones:

    - Paquete de parches: Conjunto de parches que actúan sobre una versión del software del sistema. El producto comprueba la validez del conjunto de parches antes de cargarlos en el sistema. Su extensión es (.pat).
    - *Software/firmware* del sistema: Se puede definir como el sistema operativo del producto. Al igual que los paquetes de parches, el producto comprueba la validez e integridad del software del sistema. Su extensión es (.cc).

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

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

    patch load <nombre_Parche>.pat all run

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

startup system-software <nombre_System_Software>.cc

startup saved-configuration vrpcfg.zip

reboot fast

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

display startup

5.10 AUTO-CHEQUEOS

63. Cuando el producto se enciende o se reinicia realiza los siguientes auto-chequeos:

- Auto-chequeo de la integridad del *software* del sistema.
- Auto-chequeo de los algoritmos de cifrado (AES, HMAC, DRBG, SHA256/512, firmado con RSA).

5.11 SNMP

64. El producto puede funcionar como agente de SNMP, enviando mensajes SNMP a un NMS. Para ello es necesario configurar el enrutador como se explica en el módulo “Configuring Basic SNMPv3 Functions” de la [GUÍA_PRODUCTO]. **Se debe usar SNMP v3**. Para configurarlo:

snmp-agent sys-info version v3

5.12 AUDITORÍA

5.12.1 REGISTRO DE EVENTOS

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

- *Login* y *logout* de los usuarios.
- Inicio de las acciones de auditoría.
- Cambio o generación de claves criptográficas.
- Cambios en la configuración del producto.
- Resetear o cambiar claves.
- Intentos de *login* fallidos.
- Configuración de un servidor NTP o eliminación del mismo.
- Terminación de una sesión local o remota por el usuario o por inactividad.
- Intentos de iniciar una actualización.

- Fallos en establecer una sesión SSH.

66. El producto guarda la siguiente información de los eventos:

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

Tabla 5. Información que se registra de cada evento

5.12.2 ALMACENAMIENTO LOCAL

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

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

    display logfile <nombre_archivo_auditoria>

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

5.12.3 ALMACENAMIENTO REMOTO

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

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

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

      system-view

      info-center enable

      info-center channel 1 name loghost1

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

info-center loghost <IP_servidor_syslog> channel loghost1

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

  info-center source arp channel loghost1 log level notification

- Crear una política de SSL para la comunicación segura:

  ssl policy <nombrar_politica_SSL>

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

  trusted-ca load pem-ca <fichero_certificado_CA>

  quit

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

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

5.13 *BACKUP*

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

    save all vrpcfg.zip

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

    system-view

    set save-configuration interval <rango_30_43200_minutos>

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

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

75. Por último, los registros de auditoría del sistema pueden enviarse a un servidor syslog externo, como se define en la sección 5.12 AUDITORÍA.

5.14 SERVICIOS DE SEGURIDAD

76. **Se deben activar los mecanismos de protección de los que dispone el producto frente a ataques DoS** (Denegación de servicio), incluyendo SYN Flood, Land, Smurf

y ICMP Flood. Para ello, es necesario ejecutar los siguientes comandos en la interfaz de línea de comandos:

system-view

tcpsynflood enable

udp-packet-defend enable

car icmp cir 100 cbs 3000

abnormal-packet-defend enable

fragment-flood enable

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

    system-view

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

        arp speed-limit source-mac maximum <numero_paquetes_segundo>

        arp speed-limit source-ip maximum <numero_paquetes_segundo>

    - Limitar el máximo de paquetes ARP de una dirección MAC en específico. Lo mismo para IP:

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

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

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

        interface <interfaz> <numero_interfaz | vlan <id_vlan>

        arp anti-attack rate-limit enable

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

    - Configurar el aprendizaje de direcciones ARP:

        arp learning strict

78. **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 y IGMP snooping para IPV4 (hacer lo mismo para IPV6 si se utiliza):

  system view

  dhcp snooping enable ipv4

  igmp-snooping enable ipv4

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

  interface <tipo_interfaz> <numero_interfaz>

  dhcp snooping trusted

  quit

  vlan <numero_vlan>

  dhcp snooping trusted interface <tipo_interfaz> <numero_interfaz>

- Deshabilitar "*location transition*" para DHCP:

  undo dhcp snooping user-transfer enable

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

  arp dhcp-snooping-detect enable

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

  dhcp snooping user-offline remove mac-address

6. FASE DE OPERACIÓN

79. 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.
- Realizar *back-ups* periódicos y la restauración de estos. Además de almacenarlos en localizaciones seguras y planificar el proceso de automatización.
- Mantenimiento de los registros de auditoria. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos.
- La información de auditoria se guardará en las condiciones y por el periodo establecido en la normativa de seguridad.

7. *CHECKLIST*

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

Tabla 6. *Checklist*

8. REFERENCIAS

[GUIA_PRODUCTO] HUAWEI NE40E V800R012C10 *Product Documentation, Product Version*: V800R012C10, *Issue*: 05, *Date*: 2021-06-20

9. ABREVIATURAS

AAA	*Authentication, authorization, and accounting*
ALP	*Active Link Protection*
ARP	*Address Resolution Protocol*
BGP	*Border Gateway Protocol*
CA	*Certification Authority*
CM	*Consuming model*
CMPv2	*Certificate Management Protocol version 2*
CPU	*Central processing unit.*
DHCP	*Dynamic Host Configuration Protocol*
DPD	*Dead Peer Detection*
ENS	Esquema Nacional de Seguridad
ESDP	*Electronic Software Delivery Platform*
ESN	*Equipment Serial Number*
EVPN	*Ethernet VPN*
FLEXE	*Ethernet flexible*
FTP	*File Transfer Protocol*
GRE	*Generic Routing Encapsulation*
GTSM	*Generalized TTL*
HMAC	*Hash-based Message Authentication Code*
HWTACACS	*Huawei Terminal Access Controller Access-Control*
ID	*Identification*
iFIT	Telemetría de información de flujo in situ
IGMP	*Internet Group Management Protocol*
IGMP	*Internet Group Management Protocol*
IKEv2	*Internet Key Exchange version 2*
IP	*Internet Protocol*
IPSEC	*Internet Protocol Security*
IS-IS	*Intermediate System to Intermediate System*

L2VPN	*Layer 2 VPN*
L3VPN	*Layer 3 VPN*
LDP	*Label Distribution Protocol*
MAC	*Media Access Control*
MAN	*Metropolitan Area Network*
MVPN	*Multidiffussion VPN*
NAT	*Network Address Translation*
NMS	*Network Management Server*
NTP	*Network Time Protocol*
OSPF	*Open Shortest Path First*
PKI	*Public Key Infrastructure*
PW	*Power*
QoS	*Quality of Service*
RADIUS	*Remote Authentication Dial-In User Service*
RIP	*Routing Information Protocol*
RSVP	*Resource Reservation Protocol*
RTU	*Remote terminal unit*
SFTP	*Secure FTP*
SHA	*Secure Hash Algorithm*
SNMP	*Simple Network Management Protocol*
SSH	*Secure Shell*
Stelnet	*Secure Telnet*
TCP	*Transmission Control Protocol*
TE	*Traffic Engineering*
TTL	*Time To Live*
VPLS	*Virtual Private LAN Service*
VRP	*Versatile Routing Platform*
VXLAN	*Virtual Extensible Local Area Network*

PUBLICACIONES DE DEFENSA

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