centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1475

Procedimiento de Empleo Seguro
Huawei USG6000F & USG12000F Series Firewall

Octubre 2025

MINISTERIO DE DEFENSA

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

Edita:

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-26-130

Fecha de Edición: Octubre de 2025

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.05.05 10:37:42 +02'00'

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. El producto es una plataforma hardware que dispone de una imagen software integrada. Está diseñado para proporcionar funcionalidades de cortafuegos, IPv4/IPv6, VPN, Virtual Local Area Network (VLAN), protección antivirus, protección antispam y filtrado de contenido para proveer protecciones en redes TCP/IP.

2 OBJETO Y ALCANCE

2. El presente documento tiene como objetivo detallar las configuraciones de seguridad para *Huawei USG6000F & USG12000F Series Firewall* con el ***firmware V600R023C10SPC100*** *(con parche* ***V600R023SPH001_6****),* de forma que la protección y funcionamiento del producto se realice de acuerdo con unas garantías mínimas de seguridad.

3. Las configuraciones indicadas aplican a los siguientes modelos hardware:

Tipo	Modelos
USG6000F	USG6510F-D-AC USG6510F-DL-AC USG6510F-DPL-AC USG6525F-AC USG6525F-DC USG6530F-D-AC USG6530F-DL-AC USG6530F-DPL-AC USG6555F-AC USG6565F-AC USG6565F-DC USG6585F-AC USG6615F-AC USG6625F-AC USG6635F-AC USG6635F-DC USG6655F-AC USG6685F-AC USG6710F-AC USG6715F-AC USG6715F-DC USG6725F-AC
USG12000F	USG12004-AC USG12004-DC USG12008-AC USG12008-DC USG12004-F-AC USG12004-F-DC USG12008-F-AC USG12008-F-DC

Tabla 1. Modelos hardware

4. Dicha versión de firmware y los modelos de la tabla anterior son los **cualificados e incluidos en el Catálogo de Productos y Servicios STIC (CPSTIC)**, para categoría ALTA en la familia **'Cortafuegos'**.

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 del producto, para lograr una configuración segura.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

5. Al tratarse de una combinación *hardware/software*, los *Huawei USG6000F & USG12000F Series Firewall* se entregan por correo ordinario. Se debe comprobar:

   - **Información de envío.** Se debe comprobar la documentación de envío para verificar que concuerda con la orden de compra original y que el envío ha sido realizado por Huawei.
   - **Embalaje externo.** Se debe inspeccionar el embalaje y la cinta de embalaje con la marca de Huawei. Se debe comprobar que la cinta esté intacta y que no haya sido cortada ni se haya deteriorado en ningún punto. Además, se debe inspeccionar que la caja no presente cortes ni daños que permitan acceder al dispositivo.
   - **Embalaje interno.** Se debe comprobar el embalaje interior de la misma manera que el embalaje exterior. Adicionalmente, se debe comprobar que la etiqueta presente en el embalaje exterior concuerda con el modelo de dispositivo adquirido.
   - **Sello de garantía.** Se deberá verificar que la placa de identificación del producto, alojada en el chasis, es consistente con la etiqueta del embalaje del producto.

6. En caso de que exista algún desperfecto o alguna inconsistencia será necesario contactar con el soporte de Huawei de manera inmediata para recibir instrucciones. No se recomienda realizar la instalación en este caso.

4.2 ENTORNO DE INSTALACIÓN SEGURO

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

4.3 REGISTRO Y LICENCIAS

8. Existen dos tipos de licencias:

   - **Licencia COMM**: Normalmente, la mayoría de las licencias adquiridas por contrato tienen una validez permanente, aunque puede darse el caso de que algunas tienen un periodo de validez hasta una fecha determinada.
   - **Licencia DEMO**: Son licencias las cuales se usan para casos especiales como pruebas o evaluaciones.

9. Para registrar la licencia se necesita contar con el archivo de licencia. Para obtener el archivo de licencia, se debe obtener la contraseña de activación en el *"Proof of Entitlement"* que se recibe al adquirir el producto.

Ilustración 1. Obtención de licencias.

- Hacer login en el dispositivo y ejecutar el comando **display esn** para obtener el ESN del dispositivo.
- Hacer login en el ESDP de Huawei en http://app.huawei.com/isdp.
- Acceder a "License Activation" → "Password Activation"
- Introducir la contraseña de activación obtenida del "*Proof of Entitlement*", seleccionar "*I have read the above carefully*" y después pulsar "*Next*".
- Introducir el ESN obtenido anteriormente y hacer clic en "*Next*".
- Confirmar la activación haciendo clic en "*Activate License*".
- Finalmente, para descargar el archivo hacer clic en "*Download*".

10. Una vez obtenido el archivo de licencia, se debe iniciar sesión a través del portal Web UI:
    - Ir al menú "*System*" → "*License Management*".
    - Seleccionar "*Local Manual Activation*" en el apartado "*License Activation Mode*".
    - Hacer click en "*Browse*" y seleccionar el archivo de licencia previamente obtenido.
    - Hacer click en "*Activate*" para activar el archivo de licencia.
11. De forma alternativa, se puede realizar la activación de la licencia mediante la interfaz de línea de comandos.
    - Comprobar que hay espacio suficiente para almacenar el archivo de licencias con el comando `dir`.
12. Transferir el archivo de licencia al dispositivo mediante SFTP. Para poder realizar la transferencia de licencias al dispositivo, así como para futuras acciones, se debe activar el servidor SFTP, el cual está desactivado por defecto. Para ello utilizar el siguiente comando:

```
$ sftp server enable
```

13. Acceder a la vista de sistema `system-view`.
14. Activar el archivo de licencia transmitido con el comando `license active <nombre-de-archivo>`. Si la licencia se instala correctamente, se mostrará el siguiente mensaje:

```
Info: The license is being activated. Please wait for a moment.
Info: Succeeded in activating the license file on the master board.
```

Ilustración 2: Mensaje de éxito al activar la licencia.

4.4 CONSIDERACIONES PREVIAS

15. A la hora de instalar el producto, se debe asegurar que se tiene acceso físico al Firewall, aunque se deben situar en sitios seguros lo más restringidos posibles.
16. Se debe asegurar que se cuentan con las herramientas de conectividad necesarias, tales como conectores rj45 o cables serie necesarios para la administración del dispositivo.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

17. El entorno de operación consta de los siguientes componentes:
    - **Red.** Representa la red que el Firewall utiliza para gestionarla (puede incluir PCs de usuarios, otros dispositivos de red como switches, etc.)
    - **Ordenador de Administración.** Representa el dispositivo que el usuario administrador utiliza para conectarse al Firewall y gestionarlo.

5 FASE DE INSTALACIÓN

5.1 INSTALACIÓN DEL PRODUCTO

18. Para instalar el producto el usuario debe seguir los pasos que se detallan a continuación:

    a) Conectar al Firewall mediante cable serie.

    b) Una vez esté debidamente conectado, se procederá a iniciar sesión mediante el puerto serie. En el PC se hará uso del software PuTTY con los siguientes parámetros para iniciar sesión en el dispositivo. Es importante destacar que el parámetro *"Serial Line"* dependerá del número de puertos para cada PC.

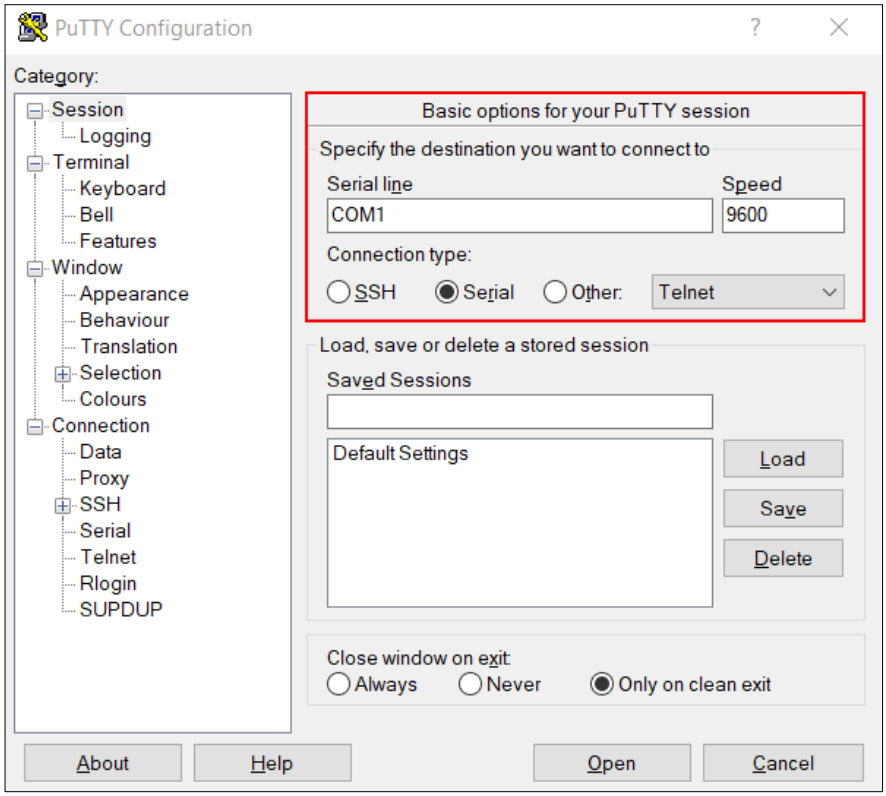
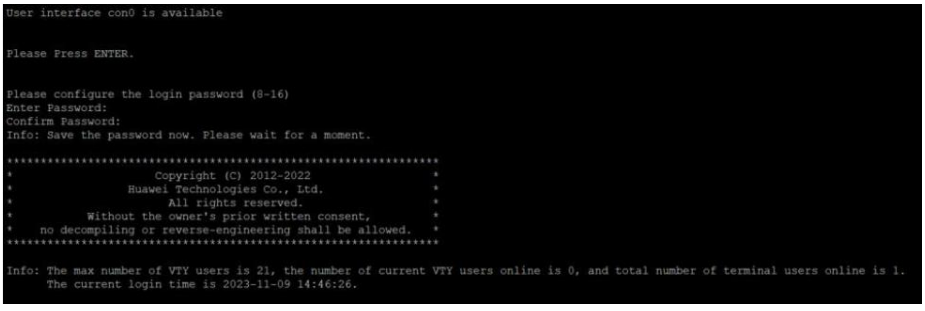


Ilustración 3: Conexión por puerto serie al firewall mediante PuTTY.

    c) Al conectarse por primera vez, el producto exige introducir una contraseña para la consola con una longitud de entre 8-16 caracteres. De esta forma, quedará operativa la interfaz de comandos a través de conexión serial.



d) Seguidamente se deberá configurar la hora y huso horario con los siguientes comandos:

```
$ clock timezone Madrid add 1
$ clock datetime <hh:mm:ss> <yyyy-mm-dd>
```

5.2 VERIFICACIÓN DEL FIRMWARE

19. Se debe verificar que el firewall disponga del ***firmware V600R023C10SPC100*** y el parche ***V600R023SPH001_6*** instalados. Para verificarlo, seguir los siguientes pasos:

    a) Para listar el *firmware* del sistema y el paquete de parches configurados en el producto se deben de ejecutar las siguientes instrucciones en la consola:

```
$ display version
$ display patch-information
```

20. En caso contrario, se deberá instalar dicho *firmware*. Para ello, se puede transferir al firewall mediante SFTP.
21. El detalle de actualización del *firmware* se puede consultar en el apartado 82 Para más detalle sobre los distintos comandos de NTP consultar la sección “NTP Configuration Commands” de [GUÍA_PRODUCTO].
22. ACTUALIZACIONES.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

23. El producto no dispone de un modo de operación seguro. Sin embargo, 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 el puerto ETH de gestión.
24. Para acceder a la interfaz de línea de comandos y autenticarse con el siguiente comando:

```
$ system-view
```

25. Se deben deshabilitar las interfaces que no se va a utilizar (ejemplo):

```
$ interface 100GE0/0/0
$ shutdown
$ interface 40GE0/0/2
$ shutdown
$ interface 10GE0/0/0
$ shutdown
```

26. Para más detalle sobre los comandos, consultar la sección “Interface Basic Configuration Commands” de [GUÍA_PRODUCTO].
27. Se deben deshabilitar los servicios inseguros de Telnet, FTP y SSHv1:

```
$ telnet server disable
$ telnet ipv6 server disable
$ undo ftp server enable
$ undo ftp ipv6 server enable
$ undo ssh server compatible ssh-1x enable
```

28. Para más detalle sobre los comandos, consultar la sección “CLI-based Device Login Configuration Commands” de [GUÍA_PRODUCTO]
29. Se debe deshabilitar el servicio SNMP si no se va a utilizar:

```
$ undo snmp-agent
```

30. Para más detalle sobre el comando, consultar la sección “SNMP Configuration Commands” de [GUÍA_PRODUCTO]
31. Se debe deshabilitar el tráfico IGMP en todas las interfaces que se usen (ejemplo):

```
$ interface 10GE0/0/8
$ undo igmp enable
$ interface 10GE0/0/9
$ undo igmp enable
```

32. Para más detalle sobre los comandos, consultar la sección “IGMP Configuration Commands” de [GUÍA_PRODUCTO]
33. Se debe deshabilitar el servicio BGP si no se va a utilizar:

```
$ undo bgp
```

34. Para más detalle sobre el comando, consultar la sección “BGP Configuration Commands” de [GUÍA_PRODUCTO]

35. Se debe deshabilitar el servicio snetconf (puerto 830) si no se va a utilizar:

```
$ undo snetconf server enable
$ netconf
$ undo protocol inbound ssh ipv4 port 830
```

36. Para más detalle sobre los comandos, consultar la sección “NETCONF Configuration Commands” de [GUÍA_PRODUCTO]

37. Se debe habilitar el anti-DDoS en todas las interfaces que se vayan a utilizar:

```
$ interface 10GE0/0/8
$ anti-ddos flow-statistic enable
$ quit
$ anti-ddos syn-flood source-detect
$ interface 10GE0/0/9
$ anti-ddos flow-statistic enable
$ quit
$ anti-ddos syn-flood source-detect
```

38. Para más detalle sobre los comandos, consultar la sección “Attack Defense Configuration Commands” de [GUÍA_PRODUCTO]

39. Para la protección de las comunicaciones de gestión remota, se deben establecer los algoritmos seguros de intercambio de claves del servidor y cliente SSH:

```
$ ssh server publickey ecc
$ ssh server hmac sha2_512 sha2_256
$ ssh server cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr
aes128_ctr
$ ssh server key-exchange ecdh_sha2_nistp384 ecdh_sha2_nistp256
dh_group16_sha512 dh_group_exchange_sha256 ecdh_sha2_nistp521
```

40. Para más detalle sobre los comandos, consultar la sección “SSH Configuration Commands” de [GUÍA_PRODUCTO]

41. Para TLS se debe crear una suite de cifrados y establecer los algoritmos seguros:

```
$ ssl cipher-suite-list <name-of-cipher-suite-list>
$ 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 syslog_ssl_policy
$ binding cipher-suite-customization <name-of-cipher-suite-list>
```

42. Para más detalle sobre los comandos, consultar la sección “SSL Configuration Commands” de [GUÍA_PRODUCTO]

6.2 AUTENTICACIÓN

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

    Credenciales locales, mediante usuario y contraseña de acceso. La gestión de usuarios locales se puede consultar en el apartado 0

44. Para más detalle sobre los distintos comandos de SSH, consultar la sección "SSH Configuration Commands" de [GUÍA_PRODUCTO].

    a) CONFIGURACIÓN DE ADMINISTRADORES.

Autenticación mediante servidor externo RADIUS, ver apartado 0

45. Para más detalle sobre los comandos, consultar la sección "Information Management Configuration Commands" de [GUÍA_PRODUCTO]

    a) SERVIDORES DE AUTENTICACIÓN.

    b) Clave RSA para autenticación del servicio SSH.

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

    a) Certificado TLS para comunicarse con el servidor syslog externo.

    b) Clave pre-compartida para las comunicaciones con un servidor NTP externo. Su configuración se indica en el apartado 6.7 SINCRONIZACIÓN.

Clave pre-compartida para cifrar la comunicación entre un servidor RADIUS externo y el producto. Su configuración se indica en el apartado 0

47. Para más detalle sobre los comandos, consultar la sección "Information Management Configuration Commands" de [GUÍA_PRODUCTO]

    a) SERVIDORES DE AUTENTICACIÓN.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

48. El producto dispone de los siguientes métodos de acceso para la administración:

Método		Descripción	Interfaz
Web (HTTPS)		El administrador realiza las operaciones de administración a través de una página web,	Cualquier puerto Ethernet accesible en el dispositivo. Es recomendable usar la interfaz de gestión.
CLI	Console	Método de acceso básico y local. Solo un administrador puede operar mediante este método al mismo tiempo.	Puerto consola.
	Telnet	Método para la administración y	

		mantenimiento remoto. Se debe evitar el uso de este método. **Deshabilitado en sección 6.1.**	Cualquier puerto Ethernet accesible en el dispositivo.
	STelnet	Método para la administración y mantenimiento remoto que permite autenticación y cifrado de la transmisión, más seguro que Telnet.	
API		El administrador hacer uso a la API northbound del FW a través de un cliente NETCONF o RESTCONF.	-

Tabla 2: Métodos de acceso para la administración

49. Para definir el tipo de acceso de cada usuario, se deben seguir los siguientes pasos:

    - Acceder a la interfaz de línea de comandos del producto con un usuario con "*user privilege*" 3 y acceder a la vista AAA:

```
$ system-view
$ aaa
```

    - Ejecutar el siguiente comando para definir el tipo de acceso:

```
$ local-user <usuario> service-type <ssh/terminal>
```

50. Para más detalle sobre los comandos, consultar la sección "AAA Configuration Commands" de [GUÍA_PRODUCTO]):

51. Aunque es posible la administración mediante protocolos como TELNET o FTP, su uso se debería evitar al ser estos considerados protocolos inseguros. Instrucciones para deshabilitar dichos protocolos son proporcionadas en la sección 6.1 MODO DE OPERACIÓN SEGURO.

52. En caso de usar el servicio SSH, **se recomienda el uso de clave pública/privada** para la autenticación en lugar de contraseña. Es posible crear las siguientes claves, pero se recomienda el uso de claves ECC:

    - **RSA** (se debe utilizar una longitud de **clave siempre igual o superior a 3072**):

```
$ system-view
$ ssh user <usuario> authentication-type <rsa>
$ rsa peer-public-key <nombre_clave> encoding-type { der | openssh | pem
}
$ public-key-code begin
$ <clave_pública>
$ public-key-code end
$ peer-public-key end
ECC (se debe utilizar una longitud de clave siempre igual o superior a
256):
$ system-view
$ ssh user <usuario> authentication-type <ecc>
```

```
$ ecc peer-public-key <nombre_clave> encoding-type {der | openssh | pem
}
$ public-key-code begin
$ <clave_pública>
$ public-key-code end
$ peer-public-key end
```

53. Es necesario enlazar la clave pública importada, bien sea ECC o RSA, al usuario en cuestión que vaya a usarla. Para ello se debe ejecutar:

```
$ ssh user <usuario> assign  { rsa-key | ecc-key } <nombre_clave>
```

54. Para más detalle sobre los distintos comandos de SSH, consultar la sección "SSH Configuration Commands" de [GUÍA_PRODUCTO].

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

55. El producto no define roles de administración, sino que asocia un número entero entre 1 y 3 a cada usuario, denominado *"user privilege"*, que corresponde al nivel de permisos de usuario. En la siguiente tabla se muestran los *user privileges* y los permisos que representan.

"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.
2	Configuración	Comandos de configuración de los servicios.
3	Administración	Comandos de operación básica del sistema que se utilizan para dar soporte a los servicios, incluyendo el sistema de archivos, SFTP, comandos de gestión de usuarios, comandos de configuración a nivel de comandos y comandos de depuración.

Tabla 2: Permisos de Usuario

56. No se recomienda modificar los niveles de acceso necesarios para acceder a los distintos comandos. Sin embargo, en caso de ser necesario, se pueden modificar los permisos necesarios para poder acceder a un comando mediante el comando *command-privilege level <nivel> view <vista> <comando>.*

57. Para crear un usuario se deben ejecutar los siguientes comandos:

```
$ local-user <nombre_usuario> password irreversible-cipher <contraseña>
```

58. Por defecto, un usuario recién creado tiene un privilegio de nivel 0. Para asignar un nivel específico de *"user privilege"* a un usuario:

- Acceder a la interfaz de línea de comandos del producto con un usuario con *"user privilege"* 3 y acceder a la vista con *AAA*:

```
$ system-view
$ aaa
```

- Luego, se puede asignar a un usuario un nivel 0 a 3 de privilegios:

```
$ local-user <nombre_usuario> privilege level <nivel>
```

59. Por defecto, la política de contraseñas consiste en un valor entre 8 y 128 caracteres que debe contener, al menos, una combinación de un número, un símbolo, una mayúscula o una minúscula. El usuario administrador puede modificar los siguientes parámetros:

- Longitud: La longitud de la contraseña mínima es 8, aunque se puede ampliar hasta 16. **Se recomienda un valor mínimo de 12 caracteres.**

```
$ system-view
$ set password min-length <longitud>
```

- Complejidad: Se puede ampliar la complejidad de la contraseña de forma que se exija la combinación de tres de los elementos mencionados anteriormente:

```
$ system-view
$ aaa
$ user-password complexity-check three-of-kinds
```

- Historial: Se puede ajustar el historial de contraseñas de forma que no se puedan establecer de nuevo contraseñas que ya se hubieran establecido antes. **Se recomienda un valor de, al menos, 5 contraseñas.**

```
$ system-view
$ aaa
$ local-aaa-user password policy administrator
$ password history record number 5
$ local-aaa-user password policy access-user
$ password history record number 5
```

60. El usuario administrador puede establecer las políticas seguras de sesión como:

- Tiempo de inactividad para SSH, **se recomienda un valor de 5 minutos** (300 segundos):

```
$ system-view
$ user-interface console 0
$ idle-timeout <tiempo_minutos> <tiempo_segundos>
```

- Tiempo de inactividad para la interfaz serie, **se recomienda un valor de 5 minutos**.

```
$ system-view
$ user-interface console 0
$ idle-timeout <minutos> <segundos>
```

- Número de intentos fallidos de autenticación (*retry-time*) y tiempo de espera al superar el umbral (*retry-interval*). **Se recomienda configurar un máximo de 3 intentos fallidos y un bloque de 5 minutos**.

```
$ system-view
```

```
$ local-aaa-user wrong-password retry-interval retry-time
```

61. Se debe también configurar un mensaje de aviso y consentimiento en el inicio de sesión.

```
$ system-view
$ header shell information <texto>
```

62. Para más detalle sobre los distintos comandos para configurar un usuario consultar las secciones “Configuring the Console User Interface” y “Configuring a Local Administrator” de [GUÍA_PRODUCTO].

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

63. Es posible mostrar el estado de todas las interfaces disponibles en el dispositivo.

```
$ display interface brief
```

64. Para deshabilitar una interfaz se hace uso del siguiente comando. Se debe reemplazar “GigabitEthernet 1/0/1” con el nombre de la interfaz deseada.

```
$ system-view
$ interface GigabitEthernet 1/0/1
$ shutdown
```

65. Para habilitar una interfaz que ha sido deshabilitada se hace uso del siguiente comando. Se debe reemplazar “GigabitEthernet 1/0/1 con el nombre de la interfaz deseada.

```
$ system-view
$ interface GigabitEthernet 1/0/1
$ undo shutdown
```

66. Para más detalle sobre los distintos comandos consultar la sección “Interface Basic Configuration Commands” de [GUÍA_PRODUCTO].

6.5 GESTIÓN DE CERTIFICADOS

67. El firewall permite importar la clave pública de la CA, lo cual es necesario para verificar la autenticidad de los certificados de otras entidades en las comunicaciones cifradas. Para ello es necesario crear un *realm* e importar la CA en dicho *realm*. Un *realm* es un identificador en el cual es posible inscribir certificados, tanto CA, como intermedios como finales. El fichero de la CA se deberá subir en formato PEM al producto mediante SFTP.

```
$ system-view
$ pki realm test
$ quit
$ pki import-certificate ca realm test pem filename cert.pem
```

68. Para más detalle sobre los comandos, consultar la sección “Digital Signature Management” de [GUÍA_PRODUCTO]

69. También es posible importar certificados intermediarios y certificados finales.

```
$ system-view
$ pki realm test
```

```
$ quit
$ pki import-certificate local realm test pem filename cert.pem
```

70. El producto verifica que los certificados son válidos comprobando sus *flags*, su vigencia o incluso su existencia en una CRL. Dicha CRL es subida al dispositivo mediante SFTP e importada en un *realm*:

```
$ system-view
$ pki realm test
$ quit
$ pki import-crl local realm test filename crl.file
```

71. Para más detalle sobre los comandos, consultar la sección "Configuring Certificate Revocation Status Check" de [GUÍA_PRODUCTO]

72. El *realm* creado anteriormente puede ser enlazado a una política SSL, de forma que el certificado CA importado sea usado posteriormente para autenticar el servidor *syslog* remoto. Para ello, se deben ejecutar los siguientes comandos:

```
$ system-view
$ ssl policy jtsec
$ trusted-ca load pem-ca <cert_ca>
$ quit
```

73. Para más detalle sobre los comandos, consultar la sección "Configuring an SSL Policy (Manually Loading a Certificate)" de [GUÍA_PRODUCTO]

74. Es posible verificar el *Common Name* (además de su firma y su vigencia) del certificado del servidor TLS al que se le envía auditoría:

```
$ system-view
$ info-center loghost <IP_Servidor> port <puerto_servidor> channel
<canal> transport tcp ssl-policy <politica_SSL> verify-dns-name
example.com
```

75. Para más detalle sobre los comandos, consultar la sección "Information Management Configuration Commands" de [GUÍA_PRODUCTO]

6.6 SERVIDORES DE AUTENTICACIÓN

76. El dispositivo permite la configuración de servidores externos de autenticación como RADIUS o LDAP entre otros.

77. Para llevar a cabo la configuración de RADIUS, se debe crear un *authorization-schema* y un *accounting-schema*. A continuación, se exponen los pasos necesarios:

```
$ system-view
$ aaa
$ authentication-scheme radius
$ authentication-mode radius
$ quit
$ accounting-scheme radius
```

78. A continuación, se debe configurar una RADIUS template para especificar los parámetros del servidor RADIUS. Para ello se deben ejecutar los siguientes comandos:

```
$ system-view
$ radius-server template <nombre>
$ radius-server authentication <direccion RADIUS> <puerto RADIUS>
$ radius-server accounting <direccion RADIUS> <puerto RADIUS>
$ radius-server shared-key cipher <contraseña>
```

79. Por último, se debe crear un perfil de autenticación y asociar los esquemas creados en los pasos previos:

```
$ system-view
$ authentication-profile name <nombre perfil>
$ authentication-scheme radius
$ accounting-scheme radius
$ radius-server <nombre template>
```

80. El detalle de configuración de RADIUS se puede consultar en el apartado Configuration Guide --> Object --> Authentication Server --> Configuring Authentication Servers Using the CLI --> Configuring a RADIUS Server, de la guía [GUÍA_PRODUCTO].

81. Para la configuración de un servidor de autenticación LDAP se deben seguir los siguientes pasos:

```
$ system-view
$ ldap-server template <nombre template>
$ ldap-server server-type { ad-ldap | ibm-tivoli | open-ldap | sun-one
}
$ ldap-server authentication <direccion LDAP>
$ ldap-server authentication base-dn <base-dn>
$ ldap-server authentication manager <usuario manager LDAP>
$ ldap-server authentication manager-password <password>
$ ldap-server ssl version tlsv1.2
$ ldap-server authorization bind-user enable
```

82. Adicionalmente, el detalle de configuración de LDAP se puede consultar en el apartado Configuration Guide --> Object --> Authentication Server --> Configuring Authentication Servers Using the CLI --> Configuring a LDAP Server Template, de la guía [GUÍA_PRODUCTO].

6.7 SINCRONIZACIÓN

83. El firewall permite el uso de NTP para la sincronización horaria. En lugar de establecer el tiempo manualmente, **se recomienda el uso de un servidor NTP para la sincronización horaria.** Se deben ejecutar las siguientes instrucciones para establecer un servidor externo NTP:

```
$ system-view
$ ntp-service unicast-server <IP_NTP> version <versión>
```

84. Por defecto, se utiliza la versión 3 del protocolo NTP, la cual es considerada segura. **Se debe hacer uso de la versión 3 o la 4**.

85. Es posible autenticar la conexión estableciendo una clave predefinida entre el servidor NTP y el firewall, se debe hacer uso de HMAC-SHA-256. Para ello, una vez configurada 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 <ID_Clave> authentication-mode hmac-
sha256 cipher <Clave>
$ ntp-service reliable authentication-keyid <ID_clave>
```

86. Para más detalle sobre los distintos comandos de NTP consultar la sección "NTP Configuration Commands" de [GUÍA_PRODUCTO].

6.8 ACTUALIZACIONES

87. El firewall permite dos (2) tipos de actualizaciones:

- **Parches:** Actúan sobre una versión del *software* del sistema. El producto comprueba la validez del parche antes de cargarlo 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).

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

89. Para realizar la descarga, seleccionar el firmware o parche deseado desde la página de descargas.

90. Desde dicha página, se puede obtener el fichero de firma del *software*, con la extensión *asc*, para verificar la autenticidad de la descarga. Esta firma se puede obtener haciendo clic sobre el icono  , el cual se muestra bajo el apartado *Download*.

91. Se debe verificar dicha firma haciendo uso de PGP. Se puede descargar *PGPVerify* desde la página de herramientas de Huawei (https://support.huawei.com/enterprise/en/tool). La clave pública se encuentra en el mismo paquete de instalación que la herramienta.

92. Para realizar la verificación se deben seguir los siguientes pasos:

- Ejecutar el siguiente comando:

```
$ "C:\PGPVerify.exe" -k "C:\KEYS" -f "C:\PGP\<software.zip.asc>
```

- Se mostrará el siguiente mensaje por pantalla:

```
[PASS]: Good Signature. File path: C:\PGP\, Public key fingerprint:
B1000AC3 8C41525A 19BDC087 99AD81DF 27A74824
[INFO]: Verify Complete.
```

- Se deberá obtener el resultado *"Good Signature"*.

93. Para establecer un parche en el firewall es necesario ejecutar la siguiente instrucción:

```
$ startup patch <parche> all
```

94. Para establecer un firmware en el firewall es necesario ejecutar la siguiente instrucción

```
$ startup system-software <firmware>
```

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

```
$ display version
```

6.9 AUTO-CHEQUEOS

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

    a) Auto chequeo de encendido: Comprueba principalmente el hardware, centrándose en la detección de fallos de hardware, fuente de alimentación, etc. Si el autochequeo falla, el dispositivo emitirá una alarma y el arranque fallará.

    b) Auto chequeo de integridad: Incluye principalmente la comprobación de la legalidad del certificado del dispositivo, la integridad del paquete de software, etc. Si la autocomprobación falla, el dispositivo intentará arrancar desde la partición de copia de seguridad. Si la partición de copia de seguridad tampoco supera la comprobación, el dispositivo emitirá una alarma y el arranque fallará.

97. Además, en el caso de establecer un nuevo parche o firmware, se verifica la integridad de la actualización. La verificación es automática y transparente al usuario. Solo en caso de error al intentar instalar el software se notifica al usuario.

6.10 ALTA DISPONIBILIDAD

98. El producto tiene la posibilidad de configurar la funcionalidad VRRP Hot Standby, que permite que un dispositivo secundario reemplace a otro activo que está fallando o que está fuera de servicio.

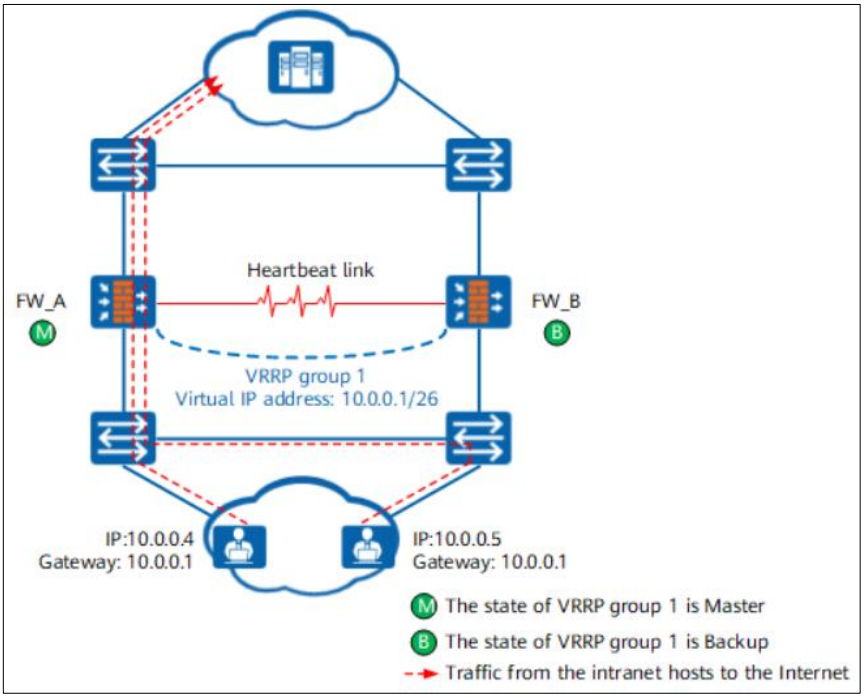


Ilustración 4. Configuración de Hot Standby.

99. En la anterior ilustración, se puede ver como FW_A está configurado como maestro y que FW_B es un dispositivo de respaldo. Dichos dispositivos comunican su estado a través del Heartbeat Link, en caso de que FW_A falle, FW_B tomaría el papel principal para seguir dando servicio.

100. El detalle de configuración para la funcionaldiad VRRP Hot Standby se puede consultar en [GUIA_PRODUCTO] en la sección "*Configuration*" → "*Configuration Guide*" → "*High Availability*" → "*Hot Standby*".

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

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

    a) Login y logout de usuarios tanto mediante la interfaz SSH, como la interfaz web, como el puerto serie.

    b) Inicio de las acciones de auditoría.

    c) Cambios en la configuración del producto.

    d) Comandos ejecutados vía CLI.

    e) Fallos al intentar establecer una sesión SSH

    f) Conexiones 802.1X y la identificación del dispositivo/usuario que realiza dicha conexión.

    g) Cambios en el tiempo del firewall.

    h) Inicio y terminación de las sesiones locales.

    i) Coincidencias de paquetes con las reglas establecidas en las políticas de seguridad

102. 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…).
Fuente del evento	Interfaz desde la que se produce el evento (ej.: SSH, Serial, Web…)
Sujeto que produce el evento	Usuario y/o IP (si corresponde).
Resultado	Resultado del evento, si aplica.

Tabla 3: Información que se guarda en los registros de auditoría.

103. Es posible configurar el mínimo nivel de gravedad de los logs, de manera que solo se registrarían aquellos que superen el valor mínimo. Hay 3 tipos de logs: *log, trap* y *debug*, los cuales a su vez tienen 8 niveles de gravedad:

- Emergencies
- Alert

- Critical
- Error
- Warning
- Notification
- Informational
- Debugging

Para configurar el nivel de gravedad mínimo de un canal y cada tipo de log es necesario ejecutar el siguiente comando:

```
$ info-center source channel <canal> log level <nivel_mínimo> trap level
<nivel_mínimo> debug level <nivel_mínimo>
```

Se puede consultar esta configuración que más detalle en [GUÍA_PRODUCTO] en la sección *Configuration → Configuration Guide → Monitoring and Troubleshooting → Configuring Information Center*.

6.11.2 ALMACENAMIENTO LOCAL

104. El producto almacena localmente los registros de auditoría bajo el directorio */logfile* (alojado en el directorio raíz). En dicho directorio se pueden encontrar los logs que el producto va generando.

105. En caso de que el archivo log.log o log.dblg sobrepasen un límite de tamaño establecido (8 MB por defecto), son comprimidos y almacenados como archivos con formato ZIP con nombre <Fecha>.<Hora>.log.zip o <Fecha>.<Hora>.dblg.zip, a la vez que los archivos *.log* y *.dblg* se quedan vacíos. El límite de tamaño establecido por defecto puede ser cambiado ejecutando los siguientes comandos.

```
$ system-view
$ info-center logfile size <tamaño 4, 8, 16 o 32 MB>
```

106. En caso de que se alcance el espacio de almacenamiento máximo, se borrarán archivos con formato ZIP antiguos. Es por esto que se recomienda realizar la configuración de un servidor de auditoría externo, tal como se indica a continuación.

6.11.3 ALMACENAMIENTO REMOTO

107. El firewall se puede configurar para enviar sus registros de auditoría a un servidor *syslog* externo. Es recomendable configurar la comunicación con dicho servidor bajo TLS 1.2, cifrando toda comunicación.

    Es recomendable asignar certificados a cada extremo de la comunicación firmados por una CA. De esta manera se puede importar la CA como se indica en el punto 0

108. Para más detalle sobre los distintos comandos consultar la sección “Interface Basic Configuration Commands” de [GUÍA_PRODUCTO].

109. GESTIÓN DE CERTIFICADOS y validar la firma del certificado TLS cuando se establezca la conexión. Para ello, se debe crear una política SSL en la cual se importe la CA que se haya subido al firewall.

```
$ system-view
$ ssl policy <nombre_policy>
$ trusted-ca load pem-ca ca.crt
```

110. Una vez creada la política, se debe crear un canal, el cual recoja todos los eventos posibles que se produzcan en el dispositivo, de cara a recoger toda la información de auditoría posible. Para ello, ejecutar los siguientes comandos:

```
$ system-view
$ info-center channel 6 name <nombre_canal>
$ info-center source default channel <nombre_canal> log level
debugging trap level debugging debug level debugging
```

111. Por último, se debe configurar el firewall para transmitir los logs al servidor Syslog mediante TLS.

```
$ info-center loghost <ip-servidor_syslog> channel <nombre_canal>
transport tcp ssl-policy <nombre_policy>
```

6.12 BACKUP

112. El producto almacena la configuración inicial en el fichero “vrpcfg.cfg”, 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.cfg*” se debe de ejecutar el siguiente comando:

```
$ save
```

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

```
$ system-view
$ set save-configuration interval <segundos>
```

114. El archivo de configuración debe almacenarse en un dispositivo diferente del producto, descargándolo manualmente por medio de SFTP. Para descargarlo se debe habilitar el servidor SFTP en el firewall y descargarlo desde el producto que almacenará la copia de la configuración. Una vez conectado mediante SFTP, para descargar el archivo de configuración, basta con ejecutar:

```
$ get vrpcfg.cfg
```

7 REFERENCIAS

[GUIA_PRODUCTO] HiSecEngine USG6000F V600R023C00 Product Documentation

8 ABREVIATURAS

ACL	*Access Control List*
AES	*Advanced Encryption Standard*
ARP	*Address Resolution Protocol*
CA	*Certificate Authority*
CRL	*Certificate Revocation List*
CSR	*Certificate Signing Request*
DHCP	*Dynamic Host Configuration Protocol*
DOS	*Denial of Service*
ENS	Esquema Nacional de Seguridad
ESN	*Equipment Serial Number*
GE	*Gigabit Ethernet*
HTTPS	*Hypertext Transfer Protocol Secure*
ICMP	*Internet Control Message Protocol*
IP	*Internet Protocol*
LDAP	*Lightweight Directory Access Protocol*
PEM	*Base64 encoded certificate*
PC	*Personal Computer*
RADIUS	*Remote Authentication Dial-In User Service*
RSA	*Rivest, Shamir, & Adleman (public key encryption technology)*
SFTP	*Secure File Transport Protocol*
SHA	*Secure Hash Algorithm*
SNMP	*Simple Network Management Protocol*
SSH	*Secure Shell*
SSL	*Secure Sockets Layer*
SYN	*Synchronization*
TLS	*Transport Layer Security*
VLAN	*Virtual Local Area Network*
VRRP	*Virtual Router Redundancy Protocol*

PUBLICACIONES DE DEFENSA

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