centro criptológico nacional

# Guía de Seguridad de las TIC
# CCN-STIC 1433

## Procedimiento de empleo seguro
## *Huawei USG 6000E Series Firewall*


**Abril de 2022**

MINISTERIO DE DEFENSA

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

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional
CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.04.22 11:45:20 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-130-6

Fecha de Edición: abril de 2022

**LIMITACIÓN DE RESPONSABILIDAD**

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

**AVISO LEGAL**

# ÍNDICE

# 1. INTRODUCCIÓN

1. Los cortafuegos USG 6000E están diseñados para proporcionar funcionalidades de cortafuegos, IPv6, VPN, Virtual Local Area Network (VLAN), protección antivirus, protección anti-spam y filtrado de contenido para proveer protecciones en redes TCP/.
2. Están formados por una plataforma hardware que dispone de una imagen software integrada.

## 2. OBJETO Y ALCANCE

3. El presente documento tiene como objetivo detallar las configuraciones de seguridad para los cortafuegos *Huawei USG 6000E*, de forma que la protección y funcionamiento del producto se realice de acuerdo a unas garantías mínimas de seguridad.
4. Las configuraciones indicadas aplican a los siguientes modelos *hardware*:
   - USG6510E
   - USG6530E
   - USG6525E
   - USG6555E
   - USG6565E
   - USG6585E
   - USG6575E-B
   - USG6610E
   - USG6620E
   - USG6650E
   - USG6680E
   - USG6605E-B
   - USG6712E
   - USG6716E

## 3. ORGANIZACIÓN DEL DOCUMENTO

5. El documento se divide en los siguientes apartados:

   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 Huawei USG 6000 Series 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 de comprobar que la etiqueta presente en el embalaje exterior concuerda con el modelo del 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.
7. 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 debe realizar la instalación en este caso.**

## 4.2 ENTORNO DE INSTALACIÓN SEGURO

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

## 4.3 REGISTRO Y LICENCIAS

9. Existen dos (2) tipos de licencias:
   - Licencia COMM: 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 que se usan para casos especiales como pruebas o evaluaciones.

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


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 |

The Eligible Products are listed below

**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*".

11. 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.
12. 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.*
    - 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:

*[sysname] sftp server enable*

- Acceder a la vista de sistema *system-view*.
- 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

13. A la hora de instalar el producto, se debe asegurar que se tiene acceso físico al cortafuegos.
14. 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 INSTALACIÓN

15. Para instalar el producto el usuario debe seguir los pasos que se detallan a continuación.
    - Insertar una tarjeta SD en el firewall. El puerto está situado en la parte trasera del firewall.


**Ilustración 3: Parte trasera del firewall, donde se debe insertar la tarjeta SD.**

    - Conectar al Firewall mediante cable serie.
    - Establecer la tarjeta SD.

*<sysname> system-view*

*[sysname] reset sd-card*

*[sysname] sd-card online*

- **Deshabilitar las interfaces que no se usarán**:

  *[sysname] interface GigabitEthernet 1/0/1*

  *[sysname-GigabitEthernet1/0/1] shutdown*

  *[sysname-GigabitEthernet1/0/1] quit*

  *...*

- **Deshabilitar el servicio telnet**:

  *[sysname] undo telnet server enable*

  *[sysname] undo telnet ipv6 server enable*

- **Deshabilitar el servicio FTP**:

  *[sysname] undo ftp server enable*

- **Deshabilitar el soporte para SSHv1.x:**

  *[sysname] undo ssh server compatible ssh-1x enable*

  *[sysname] undo web-manager enable*

- **Deshabilitar IPv6:**

  *[sysname] undo ipv6*

- **Deshabilitar el tráfico IGMP en todas las interfaces (se debe hacer en cada interfaz):**

  *[sysname] interface GigabitEthernet 1/0/1*

  *[sysname-GigabitEthernet1/0/1] undo igmp enable*

  *[sysname-GigabitEthernet1/0/1] quit*

  *...*

- **Deshabilitar BGP/OSPF:**

  *[sysname] undo ospf 1*

  *[sysname] undo bgp*

- **Deshabilitar SNMP:**

  *[sysname] undo snmp*

- **Denegar conexiones desde la zona *untrust* al *firewall*:**

  *[sysname] security-policy*

  *[sysname-policy-security] rule name untrust_local_1*

  *[sysname-policy-security-untrusut_local_1] source-zone untrust*

  *[sysname-policy-security-untrusut_local_1] destination-zone local*

*[sysname-policy-security-untrusut_local_1] source-address address-set test_1*

*[sysname-policy-security-untrusut_local_1] destination-address address-set test_1*

*[sysname-policy-security-untrusut_local_1] service http icmp ssh*

*[sysname-policy-security-untrusut_local_1] service protocol tcp destination-port 8443*

*[sysname-policy-security-untrusut_local_1] action deny*

*[sysname-policy-security-untrusut_local_1] quit*

*[sysname-policy-security] quit*

- **Deshabilitar escrituras no autorizadas a la tabla de enrutamiento mediante DHCP:**

  *[sysname] interface GigabitEthernet 1/0/1*

  *[sysname-GigabitEthernet1/0/1] undo dhcp client forbid apply gateway-option*

  *[sysname-GigabitEthernet1/0/1] undo dhcp client forbid apply static-route-option*

  *...*

  Nota: El administrador debe repetir los comandos previos para todas las interfaces ETH que no han sido deshabilitadas.

- **Crear una nueva cuenta de administrador** que será usada reemplazando al administrador original:

  *[sysname] aaa*

  *[sysname-aaa] manager-user newAdmin*

- Establecer la contraseña para el nuevo administrador (ver política de contraseñas del apartado 5.3.2 CONFIGURACIÓN DE ADMINISTRADORES):

  *[sysname-aaa-newAdmin] password cipher <password>*

- Habilitar el nuevo administrador para acceder por SSH y HTTPS al TOE.

  *[sysname-aaa-newAdmin] service-type web ssh*

- Establecer el rol del nuevo administrador.

  *[sysname] quit*

  *[sysname-aaa] bind manager user newAdmin role system-admin*

- **Cambiar la contraseña por defecto del usuario administrador original**.

  *[sysname] aaa*

*[sysname-aaa] manager-user admin*

*[sysname-aaa-admin] password cipher <password>*

*[sysname-aaa-admin] return*

Nota: Dado que el usuario administrador por defecto no es bloqueado con se exceden los intentos permitidos de autenticación fallidos, las contraseñas configuradas por el administrador deben tener un nivel de complejidad alto y ser suficientemente robustas para evitar un ataque directo.

- **Establecer el tiempo de *rekey* del servidor SSH a 1 hora**.

  *<system> system-view*

  *[sysname] ssh server rekey time 60*

- **Habilitar el registro de tráfico y políticas de seguridad.**

  *[sysname] log type traffic enable*

  *[sysname] log type policy enable*

- **Establecer los algoritmos seguros de intercambio de clave SSH.**

  *[sysname] ssh server key-exchange dh_group16_sha512*

- **Habilitar el registro de los paquetes descartados:**

  *[sysname] firewall log packet-discard enable*

  *[sysname] firewall log packet-discard others*

- En todas las interfaces, **habilitar la funcionalidad *anti-DDoS*:**

  *[sysname] interface GigabitEthernet 0/0/1*

  *[sysname-GigabitEthernet1/0/1] anti-ddos flow-statistic enable*

  *...*

  *[sysname-GigabitEthernet1/0/1] quit*

  *[sysname]anti-ddos syn-flood source-detect*

  *[sysname] anti-ddos syn-flood defend alert-rate 100*

  *[sysname] ddos-mode detect-clean*

# 5. FASE DE CONFIGURACIÓN

## 5.1 MODO DE OPERACIÓN SEGURO

16. 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.** Dicha configuración es la indicada en el apartado 4.5 INSTALACIÓN.

## 5.2 AUTENTICACIÓN

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

    a) Credenciales locales, mediante usuario y contraseña de acceso. La gestión de usuarios locales se puede consultar en el apartado 5.3.2 CONFIGURACIÓN DE ADMINISTRADORES.

    b) Autenticación mediante servidor externo RADIUS, ver apartado 5.7 SERVIDORES DE AUTENTICACIÓN.

    c) Clave RSA para autenticación del servicio SSH.

18. 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 5.8 SINCRONIZACIÓN HORARIA.

    c) Clave pre-compartida para cifrar la comunicación entre un servidor RADIUS externo y el producto. Su configuración se indica en el apartado 5.7 SERVIDORES DE AUTENTICACIÓN.

## 5.3 ADMINISTRACIÓN DEL PRODUCTO

### 5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

19. 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. | Puerto consola. |

| Método | | Descripción | Interfaz |
|---|---|---|---|
| | | Solo un administrador puede operar mediante este método al mismo tiempo. | |
| **API** | | El administrador hace uso a la API *northbound* del FW a través de un cliente NETCONF o RESTCONF. | - |

20. 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*" 15 y acceder a la vista *aaa*:

      *<sysname> system-view*

      *[sysname] aaa*

    – Configurar los métodos de *login* deseados para <Usuario>:

      *[sysname-aaa] manager-user <Usuario>*

      *[sysname-aaa-manager-user-<Usuario>] service-type {api|ssh|terminal|web}*

21. **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:

    - RSA:

      *<sysname> system-view*

      *[sysname] ssh user <Usuario> authentication-type <rsa>*

      *[sysname] rsa peer-public-key <nombre_clave> enconding-type { der | openssh | pem }*

      *[sysname-rsa-public-key] public-key-code begin*

      *[sysname-rsa-key-code] <pegar_clave_pública>*

      *[sysname-rsa-key-code] public-key-code end*

      *[sysname-rsa-public-key] peer-public-key end*

    - ECC:

      *<sysname> system-view*

      *[sysname] ssh user <usuario> authentication-type <ecc>*

      *[sysname] ecc peer-public-key <nombre_clave> enconding-type { der | openssh | pem }*

*[sysname-ecc-public-key] public-key-code begin*

*[sysname-ecc-key-code] <pegar_clave_pública>*

*[sysname-ecc-key-code] public-key-code end*

*[sysname-ecc-public-key] peer-public-key end*

22. 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:

*[sysname] ssh user <Usuario> assign {rsa-key|ecc-key} <Nombre_Clave>*

### 5.3.2 CONFIGURACIÓN DE ADMINISTRADORES

23. A continuación, se describen los roles de usuarios de administración que permite el producto.

| Nivel de administrador | Rol de administración por defecto | Nivel de ejecución |
|---|---|---|
| none | *none* | *none* |
| 0 | *none* | Permite acceso a comandos de invitado |
| 1 | *device-admin(monitor)* | Permite acceso a comandos de invitado y comandos de monitorización |
| 2 | *device-admin* | Permite acceso a comandos de invitado, comandos de monitorización y comandos de configuración |
| 3 | *system-admin* | Permite acceso a comandos de invitado, comandos de monitorización y comandos de configuración. No tiene acceso a funciones de auditoría |
| 4-15 | *system-admin* | Tiene los mismos permisos que el administrador de nivel 3. Los diferentes niveles de administrador disponibles (4-15) son usados para implementar una jerarquía entre cuentas de administración. Un administrador únicamente puede gestionar otras cuentas de administración cuyo nivel de administración es inferior o igual al nivel de administración propio. |
| 15 | *audit-admin* | Administrador dedicado para auditar políticas y revisar los registros de auditoría. |

24. El "*administrator level*" y los permisos asociados a cada rol proporcionado por defecto no debe modificarse.

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

*<sysname> system-view*

*[sysname] aaa*

*[sysname-aaa] manager-user <Usuario>*

26. Para asociar un rol a un usuario creado hay que hacer uso del siguiente comando:

    *<sysname> system-view*

    *[sysname] aaa*

    *[sysname-aaa] bind manager-user <Usuario> role {audit-admin|system-admin|device-admin|device-admin(monitor)}*

27. **Se debe definir una política de contraseñas**. Es el usuario administrador el que puede modificar los siguientes parámetros relacionados con la misma. Los parámetros que pueden ser configurados en el producto:

    - La longitud mínima por defecto definida en el dispositivo es de 8 caracteres. **Se debe configurar la política para que la longitud mínima sea de 12 caracteres.**

      *<sysname> system-view*

      *[sysname] aaa*

      *[sysname-aaa] manager-user password min-length <length>*

    - Las contraseñas tienen un periodo de validez por defecto de 90 días. **Se debe realizar la configuración para que el periodo de validez sea de 60 días.**

      *<sysname> system-view*

      *[sysname] aaa*

      *[sysname-aaa] manager-user password valid-days <dias>*

    - Número máximo de intentos fallidos de autenticación, y tiempo de espera tras superar un umbral. **Se deben configurar 3 intentos y 5 minutos de bloqueo.**

      *<sysname> system-view*

      *[sysname] aaa*

      *[sysname-aaa] lock-authentication enable*

      *[sysname-aaa] lock-authentication timeout <tiempo espera>*

      *[sysname-aaa] lock-authentication failed-count <numero intentos fallidos>*

    - Tiempo de inactividad para una sesión SSH. **El tiempo de inactividad máximo debe ser de 5 minutos.**

      *<sysname> system-view*

      *[sysname] ssh server timeout <segundos>*

- Tiempo de inactividad para la interfaz serie. **El tiempo de inactividad máximo debe ser de 5 minutos.**

  *<sysname> system-view*

  *[sysname] user-interface console 0*

  *[sysname-ui-console0] idle-timeout <Minutos> <Segundos>*

- **Se debe configuración un mensaje de aviso y consentimiento en el inicio de sesión.**

  *<sysname> system-view*

  *[sysname] header shell information %<Texto>%*

  *[sysname] quit*

## 5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

28. Para mostrar el estado de todas las interfaces disponibles en el dispositivo se puede utilizar el siguiente comando:

    <sysname> display interface brief

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

    *<sysname> system-view*

    *[sysname] interface GigabitEthernet 1/0/1*

    *[sysname-GigabitEthernet1/0/1] shutdown*

30. 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.

    *<sysname> system-view*

    *[sysname] interface GigabitEthernet 1/0/1*

    *[sysname-GigabitEthernet1/0/1] undo shutdown*

## 5.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

31. El firewall utiliza SSH para la administración remota, TLS como cliente para la transmisión de auditoría a un servidor externo y TLS como servidor para la interfaz web.

32. El producto usa suites de cifrado TLS 1.2 para el cifrado del cliente TLS a la hora de enviar auditoría. Se recomienda configurar la siguiente suite de cifrado:

    *<sysname> system-view*
    *[sysname] ssl cipher-suite-list <nombre listado suites cifrado>*
    *[sysname] set cipher-suite tls12_ck_rsa_aes_256_gcm_sha384*

*<sysname> system-view*
*[sysname] ssl policy <nombre politica>*
*[sysname-ssl-policy-politica] binding cipher-suite-customization <nombre listado suites cifrado>*

33. En el caso del protocolo SSH para la gestión del firewall, para que las suites criptográficas sean conformes a la guía [CCN-STIC-807], **se debe configurar para permitan únicamente algoritmos de intercambio de claves superiores al grupo 15.** Para ello:

    *<sysname> system-view*

    *[sysname] ssh server key-exchange dh_group16_sha512*

34. Las suites criptográficas recomendadas son:

| Tipo | Descripción suite de cifrado |
|---|---|
| **SSH (gestión)** | Establecimiento de clave: diffie-hellman-group16-sha512<br>Firma criptográfica: ecdsa-sha2-nistp521<br>Algoritmo de cifrado: AES256_CTR, AES128_CTR<br>Autenticación de mensajes: HMAC-SHA2-256 |
| **Servidor HTTPS (interfaz web)** | *ECDHE_RSA_AES256_GCM_SHA384*<br>*ECDHE_RSA_AES128_GCM_SHA256* |
| **Cliente TLS (auditoría externa)** | *TLS_DHE_RSA_WITH_AES_256_GCM_SHA384* |

## 5.6 GESTIÓN DE CERTIFICADOS

35. El cortafuegos permite importar certificados de CA (*Certificate Authority*) de confianza, lo cual es necesario para verificar el certificado del servidor TLS externo el cual es el encargado de recibir auditoría. 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.

    *<sysname> system-view*

    *[sysname] pki realm test*

    *[sysname-realm-test] quit*

    *[sysname] pki import-certificate ca realm test pem filename cert.pem*

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

    *<sysname> system-view*

*[sysname] pki realm test*

*[sysname-realm-test] quit*

*[sysname] pki import-certificate local realm test pem filename cert.pem*

37. 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*.

    *<sysname> system-view*

    *[sysname] pki realm test*

    *[sysname-realm-test] quit*

    *[sysname] pki import-crl local realm test filename crl.file*

38. 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:

    *<sysname> system-view*

    *[sysname] ssl policy jtsec*

    *[sysname-ssl-policy-test] trusted-ca load pem-ca <cert_ca>*

    *[sysname] quit*

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

    *<sysname> system-view*

    *[sysname] info-center loghost <IP_Servidor> port <puerto_servidor> channel <canal> transport tcp ssl-policy <politica_SSL> verify-dns-name example.com*

## 5.7 SERVIDORES DE AUTENTICACIÓN

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

### 5.7.1 RADIUS

41. 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:

    *<sysname> system-view*
    *[sysname] aaa*
    *[sysname-aaa] authentication-scheme radius*
    *[sysname-aaa-radius] authentication-mode radius*
    *[sysname] quit*
    *[sysname-aaa] accounting-scheme radius*

42. A continuación, se debe configurar una *RADIUS template* para especificar los parámetros del servidor. Para ello se deben ejecutar los siguientes comandos:
*<sysname> system-view*
*[sysname] radius-server template <nombre>*
*[sysname] radius-server authentication <direccion RADIUS> <puerto RADIUS>*
*[sysname] radius-server accounting <direccion RADIUS> <puerto RADIUS>*
*[sysname] radius-server shared-key cipher <contraseña>*

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

*<sysname> system-view*
*[sysname] authentication-profile name <nombre perfil>*
*[sysname] authentication-scheme radius*
*[sysname] accounting-scheme radius*
*[sysname] radius-server <nombre template>*

44. 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 [GUIA_PRODUCTO].

### 5.7.2 LDAP

45. Para llevar a cabo de un servidor de autenticación LDAP se deben seguir los siguientes pasos:

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

46. 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].

## 5.8 SINCRONIZACIÓN HORARIA

47. El dispositivo permite el uso de NTP para la sincronización horaria. En lugar de establecer el tiempo manualmente, **se recomiendo el uso de un servidor NTP para la sincronización horaria.** Para configurarlo:

*<sysname> system-view*

*[sysname] ntp-service unicast-server <IP_SERVIDOR_NTP> version <número_versión_NTP>*

48. Por defecto, se utiliza la versión 3 del protocolo NTP. **Se debe hacer uso de la versión 3 o la 4.**

49. Es posible autenticar la conexión estableciendo una clave predefinida entre el servidor NTP y el dispositivo. **Se debe hacer uso de HMAC-SHA-256**. Una vez configurada la clave en el servidor NTP, se deben seguir los siguientes pasos:

    *<sysname> system-view*

    *[sysname] ntp-service authentication enable*

    *[sysname] ntp-service authentication-keyid <ID_clave> authentication-mode hmac-sha256 cipher <Clave>*

    *[sysname] ntp-service reliable authentication-keyid <ID_clave>*

## 5.9 ACTUALIZACIONES

50. El firewall contempla dos (2) tipos de actualizaciones:

    a) 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).

    b) *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).

51. Se debe garantizar que el *firewall* dispone de los últimos parches de seguridad y de la última versión del *firmware*.

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

53. Para realizar la descarga, seleccionar el *firmware* o parche deseado desde la página de descargas, se mostrará la siguiente información:

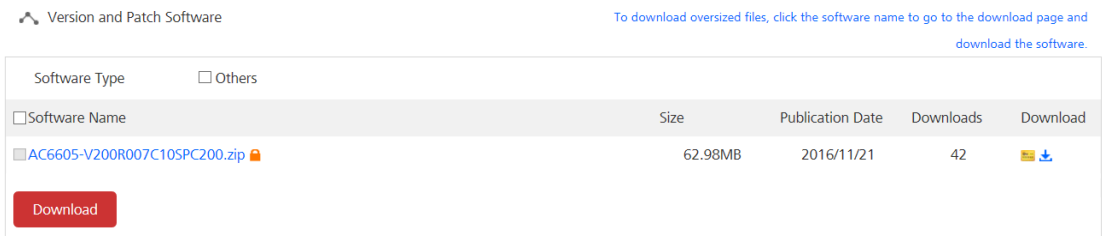



**Ilustración 4. Descarga de actualizaciones**

54. 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*.

55. **Se debe verificar dicha firma haciendo uso de PGP.** Se puede descargar *PGPVerify* desde la página de herramientas de Huawei. La clave pública se encuentra en el mismo paquete de instalación que la herramienta.
56. 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\<software.zip.asc>, Public key fingerprint: B1000AC3 8C41525A 19BDC087 99AD81DF 27A74824*

      *[INFO]: Verify Complete.*
    - Se deberá obtener el resultado "*Good Signature*".
57. Para establecer un parche en el *firewall* es necesario ejecutar la siguiente instrucción:

    *<sysname> startup patch <parche>*
58. Para establecer un *firmware* en el *firewall* es necesario ejecutar la siguiente instrucción

    *<sysname> startup system-software <firmware>*
59. Para listar el *firmware* del sistema y el paquete de parches configurados en el producto se debe de ejecutar la siguiente instrucción:

    *<sysname> display startup*

## 5.10 AUTO-CHEQUEOS

60. Cuando el producto se enciende o se reinicia realiza los siguientes autochequeos:
    a) Autochequeo de la integridad del *software* del sistema.
    b) Autochequeo de los algoritmos de cifrado.
61. 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.

## 5.11 SNMP

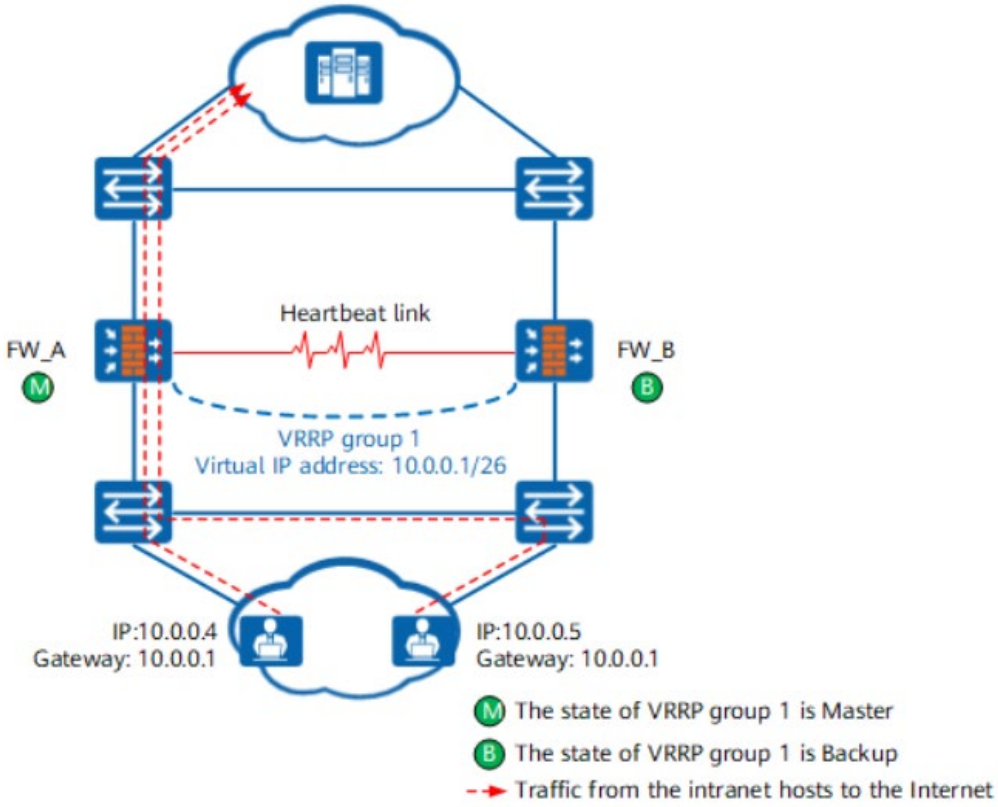
62. El producto puede hacer uso del protocolo SNMP para transmitir información a servidores NMS (*Network Management Station*), permitiendo al NMS la gestión de los dispositivos y recibir alarmas de los dispositivos. El detalle de la configuración del protocolo SNMP se puede consultar en la sección "*Configuration*" →

"*Configuration Guide*" → "*System Management*" → "*SNMP*" de la guía del producto [GUIA_PRODUCTO].

63. Se recomienda el uso exclusivo de SNMPv3, ya que las versiones anteriores del protocolo se consideran inseguras. Por defecto, el producto utiliza SNMPv3.

## 5.12 ALTA DISPONIBILIDAD

64. 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.




65. 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.

66. El detalle de configuración para la funcionalidad *VRRP Hot Standby* se puede consultar en la sección "*Configuration*" → "*Configuration Guide*" → "*High Availability*" → "*Hot Standby*".

## 5.13 AUDITORÍA

### 5.13.1 REGISTRO DE EVENTOS

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

    a) *Login* y *logout* de usuarios, mediante la interfaz SSH, la interfaz web y 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

68. 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 1: Información que se guarda en los registros de auditoría**

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

    - *Emergencies*
    - *Alert*
    - *Critical*
    - *Error*

- *Warning*
- *Notification*
- *Informational*
- *Debugging*

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

    *[sysname] info-center source channel <canal> log level <nivel_mínimo> trap level <nivel_mínimo> debug level <nivel_mínimo>*

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

### 5.13.2 ALMACENAMIENTO LOCAL

72. El producto almacena localmente los registros de auditoría en el directorio */loj* (alojado en el directorio raíz). En dicho directorio se puede encontrar el archivo *log.log*, el cual almacena los logs actuales en texto plano y el archivo *log.dblg*, el cual almacena los logs actuales en formato binario.

73. 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.

74. 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.

### 5.13.3 ALMACENAMIENTO REMOTO

75. El *firewall* se puede configurar para enviar sus registros de auditoría a un servidor b*syslog* externo. **Se debe configurar la comunicación con dicho servidor bajo TLS 1.2**.

76. **Es recomendable utilizar y cargar en el firewall certificados generados por una CA de confianza**. De esta manera, se puede importar la CA como se indica en el punto 5.6 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.

    *<sysname> system-view*

    *[sysname] ssl policy <nombre_policy>*

    *[sysname-ssl-policy-<nombre_policy>] trusted-ca load pem-ca ca.crt*

77. 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:

    *<sysname> system-view*

    *[sysname] info-center channel 6 name <nombre_canal>*

    *[sysname] info-center source default channel <nombre_canal> log level debugging trap level debugging debug level debugging*

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

    *[sysname] info-center loghost <ip-servidor_syslog> channel <nombre_canal> transport tcp ssl-policy <nombre_policy>*

## 5.14 *BACKUP*

79. Se recomienda la realización de *backups* de la configuración del *firewall*.

80. El producto almacena la configuración inicial 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 "*config.cfg*" se debe de ejecutar el siguiente comando:

    *<sysname> save all*

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

    *<sysname> system-view*

    *[sysname] set save-configuration interval <segundos>*

82. 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.zip*

## 5.15 SERVICIOS DE SEGURIDAD

83. Se deben activar los servicios de seguridad de los que dispone el producto: bloqueo de SYN flood, UDP flood, ICMP flood, HTTP flood, HTTPS flood, DNS Request Flood, DNS Reply Flood, SIP Flood y ARP flood.

84. Para **configurar la protección contra ataques *SYN flood***, se debe aplicar la siguiente configuración.

    *<sysname> system-view*

*[sysname] anti-ddos syn-flood source-detect*

*[sysname] anti-ddos syn-flood defend*

*[sysname] anti-ddos first-packet-check syn*

85. Para **configurar la protección contra ataques *UDP flood***, se debe aplicar la siguiente configuración.

    *<sysname> system-view*

    *[sysname] anti-ddos udp-flood dynamic-fingerprint-learn*

    *[sysname] anti-ddos udp-fingerprint-learn offset <offset> fingerprint-length <fingerprint-length>*

    *<offset>* es un entero entre 0 y 1500 *(bytes), <fingerprint-length>* es un entero entre 1 y 8.

    *[sysname] anti-ddos udp-fingerprint-learn packet-length enable*

    *[sysname] bandwidth-limit destination-ip type udp max-speed <max-speed>*

    *<max-speed> es un entero entre 1 y 2000000 (Mbytes).*

    *[sysname] firewall defend udp-flood base-session max-rate <max-rate-number>*

    *<max-rate-number>* es un entero entre 1 y 65535 (pps).

86. Para **configurar la protección contra ataques *ICMP flood***, se debe aplicar la siguiente configuración.

    *<sysname> system-view*

    *[sysname] interface <tipo_interfaz> <número_interfaz>*

    *[sysname] anti-ddos icmp-flood*

87. Para **configurar la protección contra ataques *HTTP flood***, se debe aplicar la siguiente configuración.

    *<sysname> system-view*

    *[sysname] anti-ddos http-flood source-detect [mode {basic|advanced|redirect}]*

    *[sysname] anti-ddos http-flood defend alert-rate <alert-rate>*

    *<alert-rate es un entero entre 1 y 80000000 (pps)*

88. Para configurar la protección contra ataques *HTTPS flood*, se debe aplicar la siguiente configuración.

    *<sysname> system-view*

    *[sysname] anti-ddos https-flood source-detect*

89. Para configurar la protección contra ataques *DNS Request flood*, se debe aplicar la siguiente configuración.

    *<sysname> system-view*

*[sysname] anti-ddos dns-request-flood source-detect mode {basic|auth-ns} [alert-rate <alert-rate>]*

*<alert-rate> es un entero entre 1 y 80000000 (pps)*

90. Para configurar la protección contra ataques *DNS Reply flood*, se debe aplicar la siguiente configuración.

    *<sysname> system-view*

    *[sysname] anti-ddos dns-reply-flood source-detect*

91. Para **configurar la protección contra ataques *SIP flood***, se debe aplicar la siguiente configuración.

    *<sysname> system-view*

    *[sysname] anti-ddos sip-flood source-detect*

92. Para **configurar la protección contra ataques *ARP flood***, se debe aplicar la siguiente configuración.

    *<sysname> system-view*

    [sysname] firewall defend arp-flood interface {<interface-type> <interface-number>|all} [max-rate <max-rate-number>]

    *<max-rate-number> es un entero entre 1 y 65535 (pps)*

## 6. FASE DE OPERACIÓN

93. Durante la fase de operación del producto, los administradores de seguridad deberán llevar a cabo, al menos, las siguientes tareas de mantenimiento.

    a) 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.

    b) **Aplicación regular de los parches de seguridad**, con objeto de mantener una configuración segura.

    c) **Realización de back-ups periódicos y la restauración de estos.** Además de almacenarlos en localizaciones seguras y planificar el proceso de automatización.

    d) **Mantenimiento de los registros de auditoría,** por el periodo establecido en la normativa de seguridad. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos.

## 7. CHECKLIST

| ACCIONES | SÍ | NO | OBSERVACIONES |
|---|---|---|---|
| **DESPLIEGUE E INSTALACIÓN** | | | |
| Verificación de la entrega segura del producto | ☐ | ☐ | |
| Instalación en un entorno seguro | ☐ | ☐ | |
| Registro de los equipos | ☐ | ☐ | |
| Registro de las licencias | ☐ | ☐ | |
| Actualización de *firmware* | ☐ | ☐ | |
| **CONFIGURACIÓN** | | | |
| Modo de Operación seguro activado (FIPS-CC) | ☐ | ☐ | |
| Autenticación | ☐ | ☐ | |
| Administración local | ☐ | ☐ | |
| Administración remota | ☐ | ☐ | |
| Configuración de interfaces, puertos y servicios | ☐ | ☐ | |
| Configuración de protocolos seguros | ☐ | ☐ | |
| Gestión de certificados | ☐ | ☐ | |
| Servidores de autenticación | ☐ | ☐ | |
| Sincronización horaria | ☐ | ☐ | |
| Autochequeos | ☐ | ☐ | |
| SNMPv3 | ☐ | ☐ | |
| Alta disponibilidad | ☐ | ☐ | |
| Registro de eventos | ☐ | ☐ | |
| Almacenamiento local | ☐ | ☐ | |
| Almacenamiento remoto con TLS | ☐ | ☐ | |

| ACCIONES | SÍ | NO | OBSERVACIONES |
|---|---|---|---|
| *Backup* de la configuración | ☐ | ☐ | |
| Activación de los servicios de seguridad | ☐ | ☐ | |
| **OPERACIÓN** | | | |
| Comprobaciones periódicas del hardware y software | ☐ | ☐ | |
| Aplicación regular de los parches de seguridad | ☐ | ☐ | |
| Realización de back-ups periódicos y la restauración de estos | ☐ | ☐ | |
| Mantenimiento de los registros de auditoría | ☐ | ☐ | |

## 8. REFERENCIAS

**[GUIA_PRODUCTO]** *USG6000E Firewall Product Documentation Version 04*

## 9. ABREVIATURAS

| | |
|---|---|
| **ACL** | *Access Control List* |
| **AES** | *Advanced Encryption Standard* |
| **ARP** | *Address Resolution Protocol* |
| **DHCP** | *Dynamic Host Configuration Protocol* |
| **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* |
| **PC** | *Personal Computer* |
| **RADIUS** | *Remote Authentication Dial-In User Service* |
| **RSA** | *Rivest, Shamir, & Adleman (public key encryption technology)* |
| **SHA** | *Secure Hash Algorithm* |
| **SNMP** | *Simple Network Management Protocol* |
| **SSH** | *Secure Shell* |
| **SSL** | *Secure Sockets Layer* |
| **SYN** | *Synchronization* |
| **TLS** | *Transport Layer Security* |
| **VLAN** | *Virtual Large 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