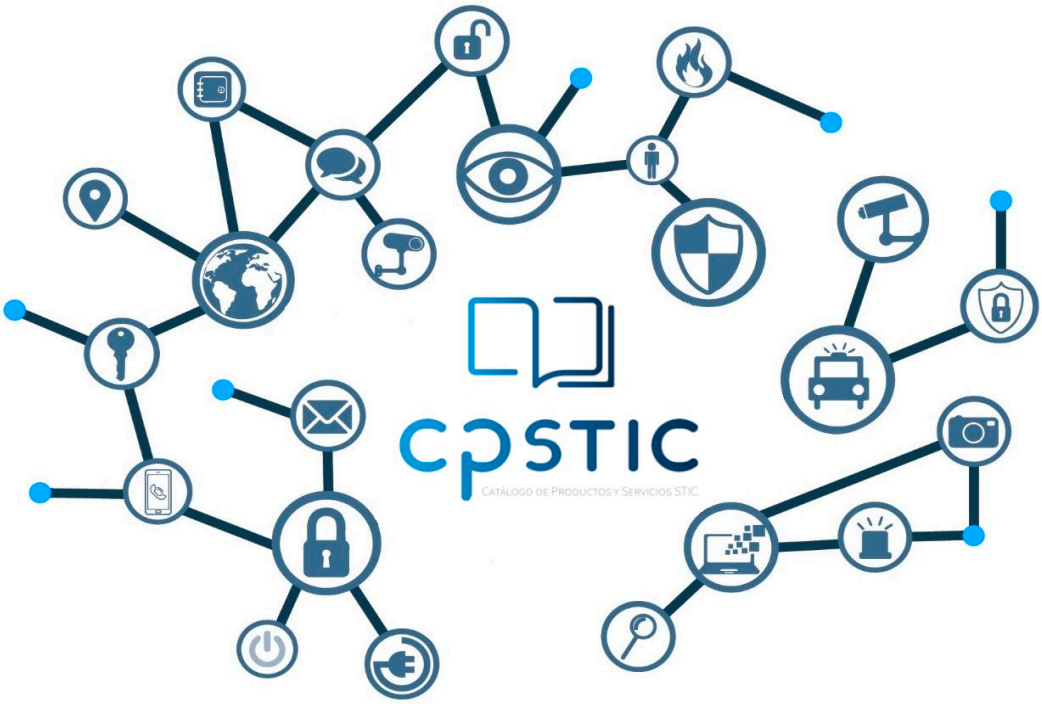
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1451

Procedimiento de empleo seguro
Extreme Networks Virtual Services Platform (VSP) Series Switches



Julio de 2023

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
2024.01.15 12:07:55 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-283-4.
Fecha de Edición: julio de 2023

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

ÍNDICE **2**
1. INTRODUCCIÓN **3**
2. OBJETO Y ALCANCE **4**
3. PROTECCIÓN FÍSICA DEL SWITCH **5**
4. ORGANIZACIÓN DEL DOCUMENTO **6**
5. FASE DE CONFIGURACIÓN **7**
5.1 MODO DE OPERACIÓN SEGURO 7
5.1.1 ACCESO AL SWITCH 7
5.1.2 PRIMER INICIO DE SESIÓN EN EL SISTEMA Y CAMBIO DE CREDENCIALES 8
5.1.3 CONFIGURAR LA DIRECCIÓN IP DE GESTIÓN 8
5.1.4 CONFIGURAR INDICADORES DE ARRANQUE 8
5.1.5 MODO SEGURO MEJORADO 9
5.1.6 HABILITAR UNA CUENTA DE USUARIO BLOQUEADA 12
5.1.7 CONFIGURACIÓN DE LA FECHA, HORA Y ZONA HORARIA DEL SISTEMA 12
5.1.8 CONFIGURAR EL SISTEMA DE NOMBRES DE DOMINIO 15
5.1.9 CONFIGURACIÓN DE SECURE SHELL 15
5.1.10 NEGOCIACIÓN TLS 20
5.1.11 GESTIÓN DE CERTIFICADOS 21
5.1.12 REGISTROS DE AUDITORÍA Y SYSLOG 28
5.2 TAREAS GENERALES DE CONFIGURACIÓN 31
5.2.1 DESHABILITAR SERVICIOS NO COMPATIBLES 31
5.2.2 CONFIGURACIÓN DEL MENSAJE DE *BANNER* 32
5.2.3 CONFIGURACIÓN DE UN UMBRAL DE TIEMPO DE ESPERA DE INACTIVIDAD DE SESIÓN 33
6. FASE DE OPERACIÓN **34**
6.1 ACTUALIZACIÓN DE *SOFTWARE* 34
6.2 VISUALIZACIÓN DEL INVENTARIO DE SOFTWARE 34
6.3 COPIA DE SEGURIDAD DE LA CONFIGURACIÓN 34
6.4 DESCARGA DE LA IMAGEN DE ACTUALIZACIÓN 35
6.5 PROCEDIMIENTO ACTUALIZACIÓN DE *SOFTWARE* 35
7. ABREVIATURAS **37**

1. INTRODUCCIÓN

1. El objeto de esta guía es establecer una referencia para la configuración segura de los switches de la familia Virtual Services Platform (VSP) de Extreme Networks. Incluye consejos y recomendaciones sobre la activación o desactivación de servicios y funcionalidades disponibles en el sistema operativo para mejorar la seguridad de la red.
2. Para conocer con más detalle las funcionalidades de los equipos *Virtual Services Platform (VSP)* de *Extreme Networks* se recomienda la consulta de las guías de configuración, guías del CLI, artículos y demás documentación disponible en:

   https://www.extremenetworks.com/support/documentation/vsp-operating-system-software-voss-8-0-0/.

2. OBJETO Y ALCANCE

3. Los switches *Extreme Networks Virtual Services Platform (VSP)* usan el sistema operativo VSP *Operating System Software (VOSS)* versión 8.3, que incluye las siguientes características:
   - El *hardware* del dispositivo
   - Puertos de gestión RJ-45/RS-232
   - Puerto USB
   - *Software/firmware* integrado instalado en el dispositivo
   - Interfaz de gestión de la CLI (*Command Line Interface*)
4. Estos switches son dispositivos de red independiente que facilitan la transferencia de datos de la capa de enlace entre los nodos de red conectados a sus puertos físicos, constan de un dispositivo de hardware con firmware integrado.
5. Para el desarrollo de esta guía se ha utilizado la versión de VOSS instalada en los siguientes switches:
   - *VSP4900*
   - *VSP7400*
   - *VSP8400*
   - *ExtremeAccess Platform (XA).*
6. **Estos modelos han sido cualificados e incluidos en el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC) en la familia "*Switches*". Se recomienda consular el CPSTIC para saber la versión del *firmware* cualificada.**

3. PROTECCIÓN FÍSICA DEL SWITCH

7. El emplazamiento físico del switch debe estar libre de interferencias magnéticas o electrostáticas y tener controles de temperatura y humedad. El switch debe estar alimentado por una fuente de alimentación ininterrumpida (UPS).
8. Deberá estar ubicado en un espacio controlado, accesible bajo llave solo por personal autorizado. Los mismos controles se deben aplicar tanto a los dispositivos que se usan para acceder al switch como a los conectores y al cableado que se emplea para efectuar la conexión física entre los dispositivos finales y el switch.

4. ORGANIZACIÓN DEL DOCUMENTO

9. Este documento se compone de los siguientes apartados:

   - 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.
   - Apartado **6**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.
   - Apartado **7**. En este apartado se incluye el listado de abreviaturas utilizadas a lo largo del documento.

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

10. En este apartado se describe cómo activar la configuración específica del producto para que este opere en el modo de operación de la cualificación del producto.

5.1.1 ACCESO AL SWITCH

11. Los administradores deberán utilizar uno de los siguientes métodos para acceder al switch y gestionarlo.

    - Conexión serie. Se deberá conectar un terminal a la interfaz de consola serie. Para ello, se proporcionarán las credenciales administrativas adecuadas para acceder al switch. Para cerrar una conexión se deberá ejecutar el comando *exit* o *logout*.
    - SSHv2. Se podrá acceder al switch desde un cliente remoto utilizando el comando *ssh* en una sesión CLI protegida por SSHv2, que emplea certificados, contraseñas y claves públicas para la autenticación. Se puede cerrar una sesión ejecutando el comando *exit* o *logout.*

5.1.1.1 ESTABLECIMIENTO DE UNA CONEXIÓN SERIE

12. Para conectar un terminal a la interfaz de consola serie para supervisar y configurar el sistema directamente, se debe disponer de:

    - Un terminal compatible con TeleTypewriter (TTY) o un ordenador portátil con puerto serie y software de emulación de terminal.
    - Un cable específico con un conector RJ-45 o USB para el puerto de consola del switch. El otro extremo del cable debe utilizar un conector apropiado para el puerto serie del ordenador o terminal.

      Nota: Para cumplir con las normativas y requisitos sobre emisiones, debe blindar el cable que se conecta al puerto de consola.

13. Para ello, se debe proceder de la siguiente forma:

    - Configurar el protocolo de la terminal de la siguiente manera
      - 9600 bd para el VSP8404C
      - 115200 bd para las series VSP 4900, VSP 7400 y XA 1400
      - 8 bits de datos
      - 1 bit de parada
      - Sin paridad
      - Sin control de flujo
    - Conectar el cable RJ-45 o USB al puerto de consola del switch.
    - Conectar el otro extremo del cable al terminal o al puerto serie del ordenador.
    - Encender el terminal.

- Proporcionar las credenciales administrativas adecuadas para acceder al switch.
- Cerrar una conexión serie, ejecute el comando *exit* o *logout*.

5.1.2 PRIMER INICIO DE SESIÓN EN EL SISTEMA Y CAMBIO DE CREDENCIALES

14. El administrador inicia sesión inicialmente en el switch utilizando el nombre de usuario predeterminado *admin* y la contraseña predeterminada *admin*.
15. A continuación, el switch solicita al administrador la creación de un nuevo nombre de usuario y una nueva contraseña.

5.1.3 CONFIGURAR LA DIRECCIÓN IP DE GESTIÓN

16. Se puede configurar la dirección IP para la interfaz de gestión de modo que se pueda acceder remotamente al switch utilizando el puerto de gestión fuera de banda.
17. La gestión segmentada es una forma de gestionar dispositivos en la que el plano de gestión (protocolos de gestión) está separado del plano de control (plano de enrutamiento) desde una perspectiva de proceso y ruta de datos. El método fuera de banda se utiliza para la configuración de Common Criteria (CC).
18. Para ello, se procede de la siguiente forma:
    - Acceder al modo de configuración fuera de banda.

      ```
      # enable
      # Configurar terminal
      # mgmt oob
      ```

    - Configurar la dirección IP y la máscara para el puerto de gestión.

      ```
      # ip addr <ip-addr/mask>
      ```

    - Configurar las rutas IP para la red de gestión.

      ```
      # ip route <ip-addr/mask> next-hop <ip-addr> weight 300
      ```

    - Habilitar la interfaz fuera de banda.

      ```
      # enable
      ```

    - Verificar la información de la interfaz IP de gestión.

      ```
      # show mgmt topology-ip
      ```

5.1.4 CONFIGURAR INDICADORES DE ARRANQUE

19. El sistema operativo VOSS tiene varios indicadores que controlan ciertos servicios durante el arranque del sistema. Para configurarlos, se procede de la siguiente forma:
    - Acceder al modo de configuración fuera de banda.

      ```
      # enable
      # Configurar terminal
      # mgmt oob
      ```

    - Mostrar las banderas de arranque actuales.

      ```
      # show boot config flags
      ```

El comando devuelve una lista de banderas y la configuración (*true o false*) para cada una.

- Comparar la configuración de cada bandera con la siguiente tabla.

Bandera	Descripción	Por defecto	Requisito CC	Comando
block-snmp	*Activar o desactivar SNMP*	*disabled*	*disabled*	*no boot config flags block-snmp*
ftpd	*Activar o desactivar el servidor FTP*	*disabled*	*disabled*	*no boot config flags ftpd*
hsecure	*Activar o desactivar el modo alta seguridad*	*disabled*	*disabled*	*no boot config flags hsecure*
sshd	*Activar o desactivar el servidor SSH*	*disabled*	*disabled*	*no boot config flags sshd*
tftpd	*Activar o desactivar el servidor TFTP*	*disabled*	*disabled*	*no boot config flags tftpd*
telnetd	*Activar o desactivar el servidor Telnet*	*disabled*	*disabled*	*no boot config flags telnetd*

20. Para cambiar la configuración de un indicador para cumplir el requisito de CC, se debe ejecutar el comando asociado con ese indicador.

5.1.5 MODO SEGURO MEJORADO

21. El modo seguro mejorado que debe ser configurado permite el control de acceso basado en roles (RBAC) y requiere una contraseña de alta complejidad de las contraseñas.
22. Después de activar el modo seguro mejorado, el switch admite RBAC y cinco niveles de acceso, cada uno con su propio conjunto de permisos.
23. Cada nombre de usuario está asociado a un determinado rol en el producto, con los derechos de autorización para ver y ejecutar comandos que están disponibles para ese rol. Con el modo seguro mejorado activado, la persona con el rol de administrador configura las credenciales de inicio de sesión para otros usuarios, basándose en sus roles.
24. En modo seguro mejorado, sólo puede haber un usuario por rol.

Rol	Descripción
Administrator	Tiene acceso a todas las configuraciones y comandos. Puede revisar el registro de archivos y los comandos de seguridad. El rol de administrador es el rol de usuario con mayor nivel. Los roles *privilege* y *administrator* no imponen un bloqueo en la consola, para evitar la pérdida de acceso administrativo al sistema. **Nota:** en el modo "*Enhanced Secure*" el nombre de usuario de CLI de *administrator* cambia a *admin.*
Privilege	Tiene el mismo conjunto de permisos que el *administrator*, pero sólo puede ser autenticado localmente dentro del switch. Este nivel también se conoce como administrador de emergencia. Un usuario con el rol *privilege* puede reactivar una cuenta bloqueada. Los roles *privilege* y *administrator* no imponen un bloqueo en la consola, para evitar la pérdida de acceso administrativo al sistema.
Operator	Tiene acceso a todas las configuraciones para el reenvío de paquetes en Capa 2 y 3. Tiene acceso a los comandos show para ver la configuración. No puede ver los registros de auditoría. No puede acceder a los comandos seguridad y contraseñas.
Auditor	Puede revisar los registros de auditoría y todas las configuraciones excepto la configuración de contraseñas.
Security	Tiene acceso a los parámetros de seguridad y puede ver las configuraciones.

25. Complejidad de la contraseña. Los requisitos de contraseña en el modo seguro mejorado son estrictos por defecto.
    - Las contraseñas requieren los siguientes caracteres: 2 mayúsculas, 2 minúsculas, 2 numéricos y 2 especiales (!, @, #, $, %, ^, *, (,) y &). **Se deben utilizar contraseñas robustas que exijan diferentes tipos de caracteres.**
    - La longitud mínima de la contraseña puede ser de 8 a 32 caracteres. El valor predeterminado es 15. **Se debe mantener este valor.**
    - El número mínimo de intentos fallidos consecutivos de inicio de sesión que pueden ocurrir antes de que un usuario sea bloqueado puede ser de 1 a 255 intentos. El valor predeterminado es 3. **Se debe mantener este valor.**

5.1.5.1 ACTIVAR EL MODO SEGURO MEJORADO

26. **Se debe activar el modo seguro mejorado** en el submodo non- JITC. Para ello, proceda de la siguiente forma:
    - Acceder al modo de configuración global.

```
# enable
# Configurar terminal
```

– Habilitar el modo seguro mejorado.

```
(config)# boot config flags enhancedsecure-mode non-jitc
```

– Guardar la configuración.

```
(config)# save config
```

– Reiniciar el switch.

```
(config)# exit
# boot
```

5.1.5.2 CREAR CUENTAS DE USUARIO

27. Con el modo seguro mejorado habilitado, la persona con el rol de administrador configura las cuentas de usuario para los otros usuarios y asigna el rol apropiado. Para ello:

– Acceder al modo de configuración global.

```
# enable
# Configurar terminal
```

– Crear una cuenta con el rol apropiado.

```
(config)# password create-user {auditor | operator | privilege |
security}
<username>
```

– Guardar la configuración.

```
(config)# save config
```

5.1.5.3 CONFIGURAR CONTRASEÑAS DE USUARIO

28. Con el modo seguro mejorado activado, la persona con el rol de administrador crea y cambia las contraseñas para los demás usuarios. Para ello:

– Acceder al modo de configuración global.

```
# enable
# Configurar terminal
```

– Crear o modificar una contraseña.

```
(config)# password set-password user-name <user-name>
```

– Introducir la contraseña.

– Guardar la configuración.

```
(config)# save config
```

5.1.5.4 CONFIGURACIÓN GLOBAL DE CONTRASEÑAS

29. Se puede configurar la longitud mínima de la contraseña y el número de intentos fallidos de contraseña antes del bloqueo. Estos ajustes afectan a todos los usuarios. Para ello:

– Acceder al modo de configuración global.

```
# enable
# Configurar terminal
```

– Establecer la longitud mínima de la contraseña para todos los usuarios.

```
config)# password min-passwd-len <value>
```

Los valores aceptables van de 8 a 32. El valor predeterminado es 15.

– Configurar el número de reintentos tras un intento fallido de inicio de sesión que pueden producirse antes de que se bloquee a un usuario.

```
(config)# password default-lockout-retries <value> (contraseña predeterminada de reintentos de bloqueo)
```

Los valores aceptables van de 1 a 255.

5.1.6 HABILITAR UNA CUENTA DE USUARIO BLOQUEADA

30. Solo el usuario con el rol Privilegio puede habilitar una cuenta de usuario bloqueada. Este rol solo tiene acceso al sistema a través de la consola serie. Para ello:

– Acceder al modo de configuración global.

```
# enable
# Configurar terminal
```

– Habilitar la cuenta bloqueada.

```
(config)# password enable-user user-name {admin | operator | security | auditor}
```

– Guardar la configuración.

```
(config)# save config
```

5.1.7 CONFIGURACIÓN DE LA FECHA, HORA Y ZONA HORARIA DEL SISTEMA

31. NTP proporciona un Reloj de Tiempo Universal (UTC) coordinado, el estándar de tiempo primario por el cual el mundo regula los relojes y el tiempo. UTC es utilizado por los dispositivos que dependen de tener una alta precisión, el tiempo universalmente aceptado, y puede sincronizar los tiempos de reloj de la computadora a una fracción de milisegundo.

32. NTP utiliza un sistema jerárquico, semi-capa de los niveles de las fuentes de reloj llamado un estrato. A cada estrato se le asigna un número de capa que empieza por 0 (cero), donde 0 significa el menor retraso. El número de estrato define la distancia, o número de saltos NTP, desde el reloj de referencia. Cuanto menor sea el número más cerca estará el dispositivo del reloj de referencia.

33. VOSS versión 8.3.100 utiliza NTPv4. La implementación de NTPv4 para VOSS 8.3.100 tiene las siguientes limitaciones y requerimientos:

– El administrador debe utilizar la autenticación NTP con autenticación SHA1.

– Los paquetes de multidifusión y difusión NTP no son compatibles con VOSS.

– El switch VOSS actúa como un cliente NTP. De acuerdo a CC, que el switch actúa como un servidor NTP no está permitido.

5.1.7.1 ESPECIFICAR Y ACTIVAR UN SERVIDOR NTP

34. **Se debe configurar el producto para que haga uso de una fuente fiable de tiempo**. Se debe especificar la dirección IPv4 o IPv6 del servidor NTP y luego verificarlo.
35. El switch VOSS, que actúa como cliente NTP, solicita información horaria al servidor NTP. Para NTPv4 puede configurar un máximo de 10 servidores NTP IPv4 y 10 servidores NTP IPv6. Para configurar dicho servidor NTP:
    - Acceder al modo de configuración global.

      ```
      # enable
      # Configurar terminal
      ```

    - Especificar y activar el servidor NTP.

      ```
      (config)# ntp server <ip-addr> enable
      ```

    - Verificar el servidor.

      ```
      (config) # show ntp server
      ```

5.1.7.2 ADMINISTRACIÓN DE LA AUTENTICACIÓN NTP

36. Se debe configurar el switch para obtener el tiempo solo de fuentes autenticadas y conocidas.
37. El switch utiliza un algoritmo *Secure Hash Algorithm* para la autenticación, haciendo coincidir la clave de autenticación en el servidor NTP con la clave de autenticación en el cliente NTP (el switch VOSS).
38. Se debe configurar una clave de autenticación para cada servidor NTP. Para ello:
    - Acceder al modo de configuración global.

      ```
      # enable
      # Configurar terminal
      ```

    - Crear un ID de clave SHA-1 y una clave secreta.

      ```
      (config)# ntp authentication-key <keyid> type sha1
      (Press Enter or Return)
      Clave <secret>
      Clave: <secret>
      ```

      Los valores válidos para el ID de la clave van de 1 a 65534 caracteres. Los valores válidos para el secreto van de 0 a 20 caracteres. **Se recomienda utilizar una cadena de caracteres lo más larga posible.**

    - Activar la autenticación en el servidor NTP.

      ```
      (config)# ntp server <ip-addr> auth-enable
      ```

      Utilizar la dirección IP IPv4 o IPv6 del servidor NTP.

    - Asignar una clave de autenticación al servidor NTP.

      ```
      (config)# ntp server <ip-addr> authentication-key <keyid>
      ```

      Utilizar la dirección IPv4 o IPv6 del servidor NTP y el ID de clave que creó en el paso 2.

    - Confirmar la clave de autenticación.

```
(config)# show ntp key
```

5.1.7.3 CONFIGURAR EL INTERVALO DE ACTUALIZACIÓN NTP

39. Los switches VOSS especifican el intervalo de tiempo entre actualizaciones NTP sucesivas como una potencia de 2 en segundos. El intervalo predeterminado es de 2 a 8 segundos.
40. Para configurar el intervalo:
    - Acceder al modo de configuración global.

      ```
      # enable
      # Configurar terminal
      ```

    - Especificar el intervalo.

      ```
      (config)# ntp interval <second>
      ```

      Los valores válidos van de 4 a 17.

5.1.7.4 RESTRINGIR EL TRÁFICO NTP

41. Con la función de restricción de NTP, se pueden identificar las direcciones IPv4 o IPv6 desde las que se permite el tráfico NTP. El tráfico procedente del resto de direcciones se ignora.
42. Para realizar esta restricción, se debe proceder de la siguiente forma:
    - Acceder al modo de configuración global.

      ```
      # enable
      # Configurar terminal
      ```

    - Restringir una dirección IP.

      ```
      (config)# ntp restrict <ip-addr>
      ```

    - Repetir el paso 2 tantas veces como sea necesario para un máximo de 128 direcciones IP.
    - Verificar las direcciones restringidas.

      ```
      (config)# show ntp restrict
      ```

5.1.7.5 MOSTRAR LA INFORMACIÓN DE ESTADO NTP

43. Se pueden usar varios comandos *show* para desplegar el estado global NTP y la información de las claves NTP:
    - Para revisar el estado global:

      ```
      # show ntp
      ```

    - Para revisar la información de la clave de autenticación de NTP:

      ```
      # show ntp key
      ```

    - Para desplegar la información de las direcciones IP restrictas:

      ```
      # show ntp restrict
      ```

    - Revisar la información del servidor NTP:

      ```
      # show ntp server
      ```

    - Para mostar las estadísticas NTP:

```
# show ntp statistics
```

5.1.8 CONFIGURAR EL SISTEMA DE NOMBRES DE DOMINIO

44. Para que el DNS cumpla con los requisitos de seguridad de la cualificación se debe configurar de la siguiente forma:

    – Acceder al modo de configuración global.

    ```
    # enable
    # Configurar terminal
    ```

    – Configurar el nombre del servidor para el switch.

    ```
    (config)# snmp-server name <sysName>
    ```

    El valor de la variable *sysName* es el indicador que ve un administrador cuando inicia sesión en el switch. El *sysName* se convierte en el nombre de host del switch.

    – Configurar el nombre de dominio.

    ```
    (config)# ip domain-name <domain-name>
    ```

    – Configurar el servidor DNS externo.

    ```
    (config)# ip name-server {primary|secondary|tertiary} <ip-addr>
    ```

    – Verificar la configuración DNS.

    ```
    (config)# show ip dns
    ```

    – Verificar la resolución DNS haciendo ping al servidor DNS.

    A continuación, se muestran dos ejemplos: uno para un nombre de host DNS y otro para una dirección IPv4.

    ```
    (config)# ping <host-name>
    (config)# ping <ipv4-addr>
    ```

5.1.9 CONFIGURACIÓN DE SECURE SHELL

45. Secure Shell (SSH) es un protocolo de cliente y servidor que especifica la forma de llevar a cabo comunicaciones seguras a través de una red.

46. SSH admite un esquema de cifrado de clave pública y privada. Utilizando la clave pública del servidor host, el cliente y el servidor (el switch VOSS) negocian para generar una clave de sesión que sólo conocen el cliente y el servidor. Esta clave única cifra todo el tráfico entre el cliente y el servidor. El switch sólo soporta SSH versión 2 (SSHv2).

47. La configuración evaluada tiene los siguientes requisitos SSH, que pueden ser gestionados por un administrador.

    – **Algoritmos de cifrado**. Sólo los siguientes algoritmos, que están activados por defecto, están aprobados para su uso en la configuración CC. Puede utilizar algunos o todos estos algoritmos.

        - *AES-128-CBC*
        - *AES-256-CBC*
        - *AES-128-CTR*
        - *AES-256-CTR*
        - *aes128-gcm@openssh.com o aes256-gcm@openssh.com*

Los algoritmos que no están aprobados para su uso en la configuración de CC también están habilitados por defecto y deben deshabilitarse.

- **Algoritmos MAC**. Sólo HMAC-SHA1 y HMAC-SHA2-256 están aprobados y ambos están habilitados por defecto. Los algoritmos que no se evaluaron, pero que están habilitados por defecto, deben deshabilitarse.
- **Método de intercambio de claves.** Sólo se aprueba el método Diffie-Hellman-Group14-SHA1, que está activado por defecto. No se necesita ni se permite ninguna configuración adicional.
- **Métodos de autenticación de usuario.** Se admiten los métodos de clave pública y contraseña, así como la autenticación mediante certificados digitales X.509. La autenticación por contraseña está activada por defecto.
- **Método de autenticación de host.** Se admite el método RSA, así como la autenticación mediante certificado digital X.509.
- **Limitaciones de la sesión.** Las mismas claves de sesión no pueden utilizarse durante más de 1 hora y con no más de 1 gigabyte de datos transmitidos. Si se supera cualquiera de estos umbrales, es necesario volver a introducir las claves.
- **Limitaciones de paquetes.** Los paquetes de más de 32.768 bytes se descartan. Los paquetes de 32.769 bytes o más se consideran sobredimensionados.

5.1.9.1 HABILITAR SSHV2

48. Se debe habilitar el servicio SSH en el switch antes de poder conectarse al switch desde un cliente SSHv2 externo. Este proceso no detiene ni inicia el servicio SSH, simplemente habilita el servicio en VOSS. Para ello:
    - Entrar en el modo de configuración global.

      ```
      # enable
      # Configurar terminal
      ```

    - Habilitar SSHv2 en el switch.

      ```
      (config)# boot config flags sshd
      ```

    - Guardar los cambios en el archivo de configuración.

      ```
      (config)# save config
      ```

5.1.9.2 DESHABILITAR MÉTODOS DE CIFRADO NO APROBADOS

49. Se deben deshabilitar los métodos que están habilitados por defecto pero que no están permitidos en la configuración recomendada. Los únicos métodos aprobados son aquellos mencionados en la sección ***5.1.9***. Para ello:
    - Acceder al modo de configuración global.

      ```
      # enable
      # Configurar terminal
      ```

    - Deshabilitar SSH.

      ```
      (config)# no ssh
      ```

    - Deshabilitar los métodos no aprobados.

```
(config)# no ssh encryption-type rijndae128-cbc
(config)# no ssh encryption-type rijndae256-cbc
(config)# no ssh encryption-type AES192-CTR
(config)# no ssh encryption-type AES192-CBC
(config)# no ssh encryption-type 3DES-CBC
(config)# no ssh encryption-type Blowfish-CBC
(config)# no ssh encryption-type aead-aes-192-gcm-ssh
```

- Activar SSH.

```
(config)# ssh
```

5.1.9.3 DESHABILITAR MÉTODOS DE AUTENTICACIÓN NO APROBADOS

50. Se deben desactivar 2 métodos no aprobados que están activados por defecto, pero no permitidos en la configuración recomendada. Los únicos métodos aprobados son aquellos mencionados en la sección ***5.1.9***. Para ello:

    - Acceder al modo de configuración global.

```
# enable
# Configurar terminal
```

    - Deshabilitar SSH.

```
(config)# no ssh
```

    - Deshabilitar los métodos no aprobados.

```
(config)# no ssh authentication-type aead-aes-128-gcm-ssh
(config)# no ssh authentication-type aead-aes-256-gcm-ssh
```

    - Activar SSH.

```
(config)# ssh
```

5.1.9.4 HABILITACIÓN DE LA AUTENTICACIÓN RSA Y GENERACIÓN DE LA CLAVE DE HOST

51. RSA es un sistema criptográfico que proporciona una transmisión de datos segura con una clave de cifrado pública y una clave de descifrado privada (la clave de host).

52. Se debe habilitar RSA y luego generar una clave de host antes de que el switch pueda aceptar conexiones SSH entrantes. La generación de una nueva clave sobrescribe la clave anterior. Para ello:

    - Acceder al modo de configuración global.

```
# enable
# Configurar terminal
```

    - Desactivar SSH.

```
(config)# no ssh
```

    - Activar la autenticación RSA.

```
(config)# ssh rsa-auth
```

    - Generar la clave de host.

```
(config)# ssh rsa-host-key <key-size>
```

    - Volver a habilitar SSH.

```
(config)# ssh
```

– Para eliminar manualmente una clave de host, seguir estos pasos. Aunque la generación de una nueva clave de host sobrescribe automáticamente la clave existente, puede eliminarla manualmente si es necesario.

  - *Desactivar SSH.*

    ```
    (config)# no ssh
    ```

  - *Elimine la clave de host.*

    ```
    (config)# no ssh rsa-host-key
    ```

  - *Vuelva a habilitar SSH.*

    ```
    (config)# ssh
    ```

5.1.9.5 HABILITAR LA AUTENTICACIÓN DE CLAVE PÚBLICA

53. Un par de claves SSH son dos claves criptográficamente seguras (una clave pública y una clave privada) que pueden utilizarse para autenticar a un cliente en un servidor SSH. Es importante asegurarse de que se puede acceder a la clave pública desde el sistema cliente.
54. La clave privada la conserva el cliente y debe mantenerse en absoluto secreto. Cualquier compromiso de la clave privada puede permitir a un atacante iniciar sesión en servidores configurados con la clave pública asociada sin autenticación adicional.
55. La clave pública asociada puede compartirse libremente sin consecuencias negativas. La clave pública puede utilizarse para cifrar mensajes que sólo la clave privada puede descifrar. Esta propiedad se emplea como forma de autenticación con el par de claves.
56. Para habilitar la autenticación de clave pública se debe proceder de la siguiente forma:

– Acceder al modo de configuración global.

```
# enable
# Configurar terminal
```

– Utilizar SCP para transferir la clave pública del sistema cliente al sistema VSP.

– Cambiar el nombre de la clave pública para que se corresponda con el rol de usuario para el que se utilizará.

```
Administrador: rsa_key_admin

Operador: rsa_key_operator

Auditor: rsa_key_auditor

Seguridad: rsa_key_security

Privilegio: rsa_key_priv

# copy /initflash/shared/id_rsa.pub /initflash/shared/rsa_key_admin

# copy /initflash/shared/id_rsa.pub /initflash/shared/rsa_key_operator

# copy /initflash/shared/id_rsa.pub /initflash/shared/rsa_key_auditor

# copy /initflash/shared/id_rsa.pub /initflash/shared/rsa_key_security

# copy /initflash/shared/id_rsa.pub /initflash/shared/rsa_key_priv
```

– Instalar la clave en la configuración SSH.

```
ssh install-user-key {admin, operator, auditor, security, priv} {public,
private} {rsa,dsa}.
```

- El tipo de clave debe ser RSA y el tipo de clave a instalar es pública, como se muestra en los siguientes ejemplos.

```
(config)# ssh install-user-key admin public rsa

(config)# ssh install-user-key operator public rsa

(config)# ssh install-user-key auditor public rsa

(config)# ssh install-user-key security public rsa

(config)# ssh install-user-key priv public rsa
```

5.1.9.6 HABILITAR LA AUTENTICACIÓN X.509

57. Se debe configurar la autenticación X.509 como parte del servicio SSH. Para ello:

- Acceder al modo de configuración global.

```
# enable

# Configurar terminal
```

- Desactivar SSH.

```
(config)# no ssh
```

- Eliminar todo lo que aparezca después del símbolo @ del nombre de usuario en el campo UPN.
- Realizar este paso sólo si hay una dirección de correo electrónico en el campo UPN del certificado. Por ejemplo, si el nombre de usuario es `admin@test.com`, ejecute este comando para eliminar `@test.com`, de forma que sólo aparezca admin en el sistema.

```
(config)# ssh x509-auth username strip-domain
```

- Habilitar la autenticación X.509.

```
(config)# ssh x509-auth enable
```

- Habilitar OCSP como método de comprobación de revocación.

```
(config)# ssh x509-auth revocation-check-method ocsp
```

  OCSP debe estar habilitado.

- Habilitar SSH.

```
(config)# ssh
```

  Se debe verificar que los certificados relacionados se añaden al sistema y están listos para ser utilizados para la autenticación.

5.1.9.7 CONFIGURAR LA RENOVACIÓN DE CLAVES SSH

58. Los servidores SSH se vuelven a establecer (o fuerzan) una conexión SSH entre el servidor y el cliente después de que se alcance el intervalo configurado o se Transferir la cantidad de datos configurada (lo que ocurra primero).
59. El administrador debe asegurarse de que el intervalo no sea superior a 1 hora y que el límite de datos no sea superior a 1 gigabyte.
60. SSH debe permanecer activado mientras se configura el cambio de clave. Para ello:

- Acceder al modo de configuración global.

```
# enable

# Configurar terminal
```

- Habilitar la renovación de clave SSH.

```
(config)# ssh rekey enable
```

- Configurar la cantidad de datos (en GB) que desencadena un cambio de clave.

```
(config)# ssh rekey data-limit 1
```

  Aunque los valores válidos van de 1 a 6 gigabytes, en la configuración evaluada sólo se admite 1 gigabyte.

- 4. Configurar el número de horas que desencadena una renovación de clave.

```
(config)# ssh rekey time-interval 1
```

  Aunque los valores válidos van de 1 a 6 horas, en la configuración evaluada sólo se admite 1 hora.

5.1.9.8 VER EL ESTADO Y LA CONFIGURACIÓN DE SSH

61. Se puede consultar información de SSH como el número de sesiones activas, la versión, el puerto de conexión y la información de autenticación. Para ello:

- Acceder al modo EXEC de usuario.

```
# enable
```

- Visualizar la información global de SSH.

```
# show ssh global
```

- Ver información SSH para la sesión activa.

```
# show ssh sesión
```

5.1.9.9 LIMITACIÓN CANAL SSH ADMINISTRACIÓN

62. El canal SSH de administración utiliza DH Grupo 14 para el establecimiento de claves y RSA 2048, lo que se considera que no es suficientemente robusto. Por lo tanto, **la administración ha de realizarse desde la red interna de la organización, es decir, desde una VLAN dedicada.**

5.1.10 NEGOCIACIÓN TLS

63. VOSS soporta el emparejamiento de identificadores de referencia, de acuerdo con RFC 6125. El identificador de referencia se especifica durante la configuración de la conexión TLS. Los identificadores de referencia soportados son nombres DNS para el *Subject Alternative Name (SAN)* y el *Common Name (CN).*

64. Como parte de la negociación de la conexión TLS, VOSS comprueba que el SAN o CN del certificado del cliente contiene el identificador de referencia esperado. El CN sólo se comprueba si el SAN está ausente. A continuación, sólo se establece una conexión si el

certificado del cliente es válido, de confianza, tiene un identificador de referencia coincidente y supera la comprobación de revocación.

65. A tener en cuenta:

    - Si la sesión TLS falla porque no se puede contactar con el servidor OCSP, se indicará que se debe verificar la ruta de red al servidor OCSP y el estado del servidor y, a continuación, que solucione cualquier problema. Cuando el servidor OCSP no está localizable, VSP acepta el certificado como 'no revocado' y continúa la conexión.
    - Si una sesión TLS exitosa se rompe inadvertidamente, puede restablecer la sesión como descrito en RECONECTAR UNA SESIÓN TLS.

5.1.10.1 RECONECTAR UNA SESIÓN TLS

66. Se puede volver a conectar manualmente una sesión TLS que se haya desconectado por error, pero no se haya restablecido automáticamente.
67. El sistema intenta automáticamente reconectar una sesión TLS. Sin embargo, si esos intentos fallan, por razones como la superación del umbral de intentos de reconexión, puede reconectar manualmente la sesión. Realice los siguientes pasos para desactivar y, a continuación, activar el servidor *syslog* en el *switch*, lo que provoca la reconexión de la sesión TLS.
68. Para ello, proceda de la siguiente forma:

    - Deshabilitar el servidor syslog.

      ```
      # disable syslog
      ```

    - Habilitar el servidor syslog.

      ```
      # enable syslog
      ```

5.1.11 GESTIÓN DE CERTIFICADOS

69. Un certificado digital es un documento electrónico que identifica al sujeto, demuestra la propiedad de una clave pública y está firmado digitalmente por una autoridad de certificación (CA) que certifica la validez de la información contenida en el certificado.
70. Un certificado digital es válido durante un periodo de tiempo determinado.
71. Los certificados digitales en el formato X.509 v3 proporcionan gestión de identidad. El *switch* utiliza el soporte PKI para obtener y utilizar certificados digitales para la comunicación segura en la red.
72. Una cadena de firmas de una CA y sus CA de certificados intermedias vincula una clave de firma pública determinada a una identidad digital determinada. VOSS puede autenticar usuarios SSH con certificados X.509 y puede autenticar un servicio de red que Utilizar TLS.
73. El sistema valida certificados X.509 v3 de acuerdo con RFC 5280 para los siguientes propósitos:

    - Como cliente TLS, el sistema valida el certificado presentado durante la negociación TLS con el servidor *syslog*.

- Como servidor SSH, el sistema valida el certificado presentado por un usuario administrativo durante el establecimiento de una sesión protegida por SSH que ofrece la CLI *admin*.
- Cuando se cargan certificados en el sistema, se validan los certificados importados.

74. En todos estos escenarios, el proceso de validación de certificados X.509 incluye lo siguiente:
    - Comprobación de la fecha de caducidad del certificado
    - Validación de la ruta del certificado (continuidad de la cadena del certificado) hasta la CA de confianza
    - Comprobación de la revocación del certificado
    - Comprobación de la clave pública, el algoritmo de clave y los parámetros
    - Comprobación del emisor del certificado
    - Procesamiento de extensiones de certificados
75. El sistema requiere que el certificado presentado por el servidor de *syslog* incluya el EKU *ServerAuth*, y requiere que los certificados de CA incluyan el indicador *BasicConstraints* como true. El sistema ignora todos los demás EKU de los certificados.
76. Los certificados presentados por un administrador al servidor SSH del sistema deben incluir la identidad del usuario (*username@domain.com*) como *PrincipalName* en la extensión *SubjectAltName* (SAN).
77. El proceso de configuración es descrito en los subapartados siguientes.

5.1.11.1 MÉTODOS DE APROVISIONAMIENTO DE CERTIFICADOS

78. Los *switches* VOSS admiten dos (2) métodos de aprovisionamiento de certificados, pero solo se admite el método fuera de línea para una configuración evaluada.

Gestión de certificados sin conexión

79. El método fuera de línea requiere que un administrador válido instale manualmente cada archivo de certificado en el subsistema de gestión de certificados de VOSS, incluidos los certificados raíz, CA y hoja de confianza. Este método es el único admitido en la configuración recomendada.
80. La gestión de certificados fuera de línea admite switches que no pueden comunicarse con la CA para obtener el certificado de identidad o certificados en línea mediante la operación de inscripción de certificados.
81. La CSR se utiliza para obtener el certificado de identidad fuera de línea. Se debe configurar el asunto y el par de claves RSA para obtener el certificado de identidad sin conexión. Se pueden generar y almacenar hasta 10 claves RSA identificadas por la etiqueta de nombre de clave. Para obtener varios certificados sin conexión, se debe especificar un nombre de asunto distinguido y un nombre de clave.
82. Se debe instalar el certificado de CA raíz y todos los certificados de CA intermedios de la cadena de certificados en el *switch* antes de instalar el certificado de identidad o de dispositivo sin conexión. Todos los certificados de CA raíz e intermedios se almacenan en el almacén de certificados y se utilizan para la validación de la cadena de certificados de CA.

83. La validación de la cadena de certificados de CA comienza desde el certificado de CA emisor hasta el certificado de CA raíz durante la instalación del certificado de identidad sin conexión. El certificado de identidad sin conexión sólo se instala si la validación de la cadena de certificados de CA, el asunto y la clave coinciden.

Gestión de certificados en línea

84. El método en línea sólo requiere la instalación manual del certificado de CA raíz de confianza. Este método de utiliza el protocolo simple de inscripción de certificados (SCEP) para obtener los certificados que necesita el sistema.

5.1.11.2 VALIDACIÓN DE CERTIFICADOS CON OCSP

85. El protocolo de estado de certificados en línea (OCSP) se utiliza para comprobar el estado de revocación de los certificados X.509 v3. El servidor OCSP, operado por la CA emisora, recibe una solicitud del *switch* para conocer el estado de un certificado. La solicitud incluye el número de serie del certificado para su validación. El servidor OCSP verifica el estado del certificado y envía una respuesta al *switch*. Basándose en la respuesta, el *switch* valida el certificado o lo rechaza si su estado es "revocado".

86. Cuando no se puede acceder al servidor OCSP, el VSP realiza las siguientes acciones:

    - Para TLS, el VSP acepta el certificado como *'no revocado'*.
    - Para SSH, el VSP rechaza el certificado.

5.1.11.3 CONFIGURACIÓN DE PARÁMETROS

87. Los parámetros serían, por ejemplo: el nombre, correo electrónico, compañía, departamento, ubicación, etc.

88. Los parámetros de asunto son los detalles necesarios para la solicitud de firma de certificado (CSR). El certificado resultante se utiliza como parte de la autenticación mutua TLS. En la tabla siguiente se definen todos los parámetros necesarios.

Parámetro	Valor
Common-name	Nombre del sujeto que envía la CSR a la autoridad de certificación (CA). Las entradas válidas van de 0 a 64 caracteres.
Country	El código de 2 caracteres del país del sujeto que envía la CSR a la CA.
E-mail	Dirección de correo electrónico del sujeto que envía la CSR a la CA. Las entradas válidas van de 0 a 254 caracteres.
Locality	Localidad del sujeto que envía la CSR a la CA. Las entradas válidas van de 0 a 128 caracteres.
Organization	Organización del sujeto que envía la CSR a la CA. Las entradas válidas van de 0 a 64 caracteres.
Province	Estado o provincia del sujeto que envía la CSR a la CA. Las entradas válidas van de 0 a 128 caracteres.

Parámetro	Valor
Subject-name	Aunque el sistema tiene asignado un asunto por defecto (Global), a efectos CC se asigna un valor único como identificador del asunto al que se asignan los parámetros del asunto. A efectos de los ejemplos del siguiente procedimiento, el nombre de asunto es VSPSubject. Las entradas válidas van de 1 a 45 caracteres.
Unit	La unidad organizativa del sujeto que envía la CSR a la CA. Las entradas válidas van de 0 a 64 caracteres.

89. Para realizar la configuración, se debe proceder de la siguiente forma:

    – Acceder al modo de configuración global.

```
# enable

# Configurar terminal
```

    – Configurar los parámetros

```
(config)# certificate subject subject-name VSPSubject common-name <name>

(config)# certificate subject subject-name VSPSubject country <2-letter-country-code>

(config)# certificate subject subject-name VSPSubject e-mail <email-addr>

(config)# certificate subject subject-name VSPSubject locality <locality>

(config)# certificate subject subject-name VSPSubject organization <organization>

(config)# certificate subject subject-name VSPSubject province <province>

(config)# certificate subject subject-name VSPSubject unit <organizational-unit>
```

    – Comprobar los detalles

```
(config)# show certificate subject subject-name VSPSubject
```

5.1.11.4 CONFIGURACIÓN DE NOMBRES ALTERNATIVOS

90. Utilizar nombres alternativos de asunto (SAN) para asociar valores como dirección de correo electrónico, dirección IP o FQDN a un certificado.

91. Para asociar SAN a un certificado, se debe utilizar el parámetro de nombre alternativo de asunto asociado a un certificado y CSR concretos. La siguiente tabla define los parámetros SAN. Todos ellos son opcionales.

Parámetro	Valor
DNS	El nombre de dominio completo del switch
e-mail	La dirección de correo electrónico del administrador del switch
IP	La dirección IPv4 del switch

92. Se debe:

- Acceder al modo de configuración global.

```
# enable

# Configurar terminal
```

- Configurar los SAN para el switch.

```
(config)# certificate subject-alternate-name subject-name VSPSubject dns <FQDN>

(config)# certificate subject-alternate-name subject-name VSPSubject e-mail <email-addr>

(config)# certificate subject-alternate-name subject-name VSPSubject ip <IPv4-addr>
```

- Visualizar las SAN configuradas.

```
(config)# show certificate subject-alternative-name
```

5.1.11.5 GENERAR EL PAR DE CLAVES

93. Para generar un par de claves RSA, se debe proceder de la siguiente forma:

- Acceder al modo de configuración global.

```
# enable

# Configurar terminal
```

- Generar el par de claves.

```
(config)# certificate generate-keypair type rsa size 2048 key-name VSPKey
```

- Mostrar la clave.

```
(config)# show certificate key-name VSPkey
```

5.1.11.6 INSTALAR UN CERTIFICADO RAÍZ DE CONFIANZA

94. Se debe instale un certificado raíz en el switch, que es el primer certificado de una cadena de confianza. VOSS sólo acepta certificados en formato DER (binario). Para instalarlo:

- Acceder al modo de configuración global.

```
# enable

# Configurar terminal
```

- Utilizar SCP para mover el archivo de certificado desde el sistema CA a la carpeta */initflash/shared/certs* del switch.
- Instalar el certificado raíz en el subsistema de certificados.

```
(config)# certificate install-file offline-root-ca-filename <cert-filename>.
```

El nombre del archivo no puede contener más de 80 caracteres y debe estar en formato *.der.

5.1.11.7 INSTALACIÓN DE UN CERTIFICADO CA

95. Una autoridad de certificación (CA) es una entidad de confianza que firma y emite certificados digitales. Los certificados de CA se firman con una clave privada que posee la CA. La clave privada corresponde a una clave pública en los certificados CA firmados.
96. VOSS sólo acepta certificados en formato DER (binario).
97. Para instalar los certificados CA:
    - Acceder al modo de configuración global.

      ```
      # enable

      # Configurar terminal
      ```

    - Utilizar SCP para mover el archivo de certificado desde el sistema CA a la carpeta `/initflash/shared/certs` del switch.
    - Instalar el certificado CA.

      ```
      (config)# certificate install-file offline-ca-filename <cert-filename>
      ```

    El nombre del archivo no puede contener más de 80 caracteres y debe estar en formato *.der.

5.1.11.8 GENERAR LA SOLICITUD DE FIRMA DE CERTIFICADO

98. Se genera una solicitud de firma de certificado (CSR) como parte del proceso de obtención del certificado SSL/TLS para el sistema VOSS. La CSR se genera utilizando un nombre de clave y un nombre de asunto previamente generados (que incluyen cualquier detalle SAN que se haya añadido). Para ello:
    - Acceder al modo de configuración global.

      ```
      # enable

      # Configurar terminal
      ```

    - Generar el CSR.

      ```
      (config)# certificate generate-csr subject-name VSPSubject key-name VSPKey
      ```

    - Confirmar que se ha generado la CSR.

      ```
      (config) # ls /initflash/shared/certs
      ```

    - Después de esto se deberá exportar la CSR y firmarla.

5.1.11.9 FIRMAR EL CERTIFICADO

99. Se pueden utilizar aplicaciones de terceros para exportar la CSR, firmar el certificado e importar el certificado firmado al sistema VOSS. SecureFX® de VanDyke Software es un cliente que admite varios métodos de transferencia de archivos, incluido SCP. Los certificados pueden firmarse en varias plataformas. OpenSSL es el *software* de código abierto más común para este fin.
100. Para firmar el certificado:
    - Utilizar SCP para exportar la CSR desde la carpeta */initflash/shared/certs* a la aplicación de firma de certificados.

- Seguir todos los pasos adecuados para que se firme el certificado.
- Utilizar SCP para importar el certificado firmado a la carpeta /initflash/shared/certs.
- Si es necesario, convertir el certificado firmado a formato DER (binario).

101. VOSS admite certificados en formato DER. No se puede instalar un certificado firmado que no esté en formato DER. A continuación, se muestra un ejemplo de conversión de un certificado en formato PEM a formato DER (en un sistema Linux).

```
$ openssl x509 -outform der -in <nombre-de-archivo-de-entrada.pem> -out <nombre-de-archivo-de-salida.der>
```

102. A continuación, se deberá instalar el certificado firmado.

5.1.11.10 INSTALAR UN CERTIFICADO FIRMADO

103. El certificado firmado se utiliza para la autenticación mutua con TLS y SSH X.509. Se debe:

- Verificar que se ha importado el certificado firmado a la carpeta:

```
/initflash/shared/certs
```

- Verificar que el cliente DNS está configurado y accesible si el respondedor OCSP del certificado contiene un nombre de host en lugar de una dirección IP.
- Acceder al modo de configuración global.

```
# enable

# Configurar terminal
```

- Verificar que el certificado se encuentra en la carpeta correcta.

```
(config) # ls /initflash/shared/certs
```

- Instalar el certificado.

```
(config)# certificate install-file offline-subject-file <cert-filename>.
```

- Comprobar que se ha instalado el certificado.

```
(config)# show certificate cert-type offline-subject-cert
```

5.1.11.11 VISUALIZACIÓN DE PARES DE CLAVES CONFIGURADOS

104. Para ver los nombres y las claves públicas de todos los pares de claves configurados:

- Acceder al modo de configuración global.

```
# enable

# Configurar terminal
```

- Mostrar los nombres y las claves públicas de todos los pares de claves.

```
(config)# show certificate key-name

Key Name: pki_key
```

5.1.11.12 ELIMINAR UNA CLAVE

105. Se puede eliminar una clave del almacén de certificados por varias razones como, por ejemplo, si una clave se ha visto comprometida o si una política requiere una nueva clave.

106. Para eliminar una clave, se debe proceder de la siguiente forma:

- Acceder al modo de configuración global.

```
# enable

# Configurar terminal
```

- Eliminar la clave especificada.

```
(config)# certificate remove key <key-label>
```

5.1.12 REGISTROS DE AUDITORÍA Y SYSLOG

107. La transmisión de registros de auditoría al servidor de auditoría externo se produce en tiempo real, transfiriéndose cada registro de auditoría a medida que se genera.

108. El *switch* VOSS puede comunicarse con cualquier servidor *syslog* que admita los protocolos *syslog* y TLSv1.2. Si se pierde la conexión con el servidor de auditoría externo, el *switch* VOSS sigue guardando los registros de auditoría locales para que no haya pérdida de auditoría.

109. Si se interrumpe la conexión *syslog*, los registros recibidos por el servicio de registro interno del *switch* no se reenvían al servidor *syslog* externo. Estos registros se omiten.

5.1.12.1 HABILITAR UNA CONEXIÓN TLS CON EL SERVIDOR *SYSLOG*

110. Como cliente *syslog*, el *switch* VOSS se comunica con un servidor *syslog* externo estableciendo un canal de confianza entre él y el servidor de auditoría. La implementación del canal de confianza emplea el reenvío de puertos utilizando TLS v1.2 (no permite TLS v1.0 ni TLS v1.1) con autenticación basada en certificados X.509 v3 entre un servidor *syslog* remoto y el *switch*.

111. El *switch* soporta las siguientes suites de cifrado para cumplir con los requisitos CC:

- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA*
- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA256*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA256*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256*

112. El switch realiza el intercambio de clave TLS con las siguientes curvas ECDHE:

- *secp256r1*
- *secp384r1*

- *secp521r1*

113. Si falla la conexión entre el servidor syslog y el switch, se intentará restablecer la conexión cada 2 minutos durante un máximo de 2 horas.

114. El VSP acepta certificados de un servidor syslog que identifique al servidor con su dirección IPv4 en la SAN o CN. El VSP también acepta certificados de un servidor syslog que identifique al servidor con su nombre DNS en la SAN o CN, siempre que ese nombre DNS pueda resolverse a la dirección IPv4 en la configuración del VSP.

115. Se deben realizar los siguientes pasos para configurar una conexión de reenvío de puerto remoto entre el switch y el servidor syslog que está instalado en un host que sirve como servidor TLS:

    - Acceder al modo de configuración global.

      ```
      # enable

      # Configurar terminal
      ```

    - Crear el host syslog y Especificar su dirección IPv4.

      ```
      (config)# syslog host <host-ID> address <ip-addr>
      ```

      Los valores válidos para el ID de host van de 1 a 10 caracteres. Las direcciones IPv4 válidas tienen el formato A.B.C.D.

    - Habilitar el host syslog.

      ```
      (config)# syslog host <host-ID> enable
      ```

    - Configurar el reenvío seguro en modo TLS.

      ```
      (config)# syslog host <host-ID> secure-forwarding mode tls server-cert-name <cert-name> (config)
      ```

      Los valores válidos para el nombre del certificado van de 1 a 64 caracteres y especifican el nombre del certificado X.509 v3.

    - Definir el puerto TCP para el reenvío seguro.

      ```
      (config)# syslog host <host-ID> secure-forwarding tcp-port <port-num>
      ```

      Los valores válidos para el número de puerto TCP van de 1025 a 49151. El valor predeterminado es 1025.

116. **Los certificados SSL/TLS utilizan RSA 2048 para la firma y autenticación del canal por lo que existe una limitación de uso en el servidor de syslog a la red interna de la organización donde se use el producto.**

5.1.12.2 ACTIVACIÓN DEL REGISTRO CLI

117. Para registrar todos los cambios de configuración realizados mediante la interfaz de línea de comandos (CLI) se debe:

    - Acceder al modo de configuración global.

      ```
      # enable

      # Configurar terminal
      ```

    - Habilitar el registro.

```
(config)# clilog enable
```

– Verificar la configuración.

```
(config)# show clilog
```

5.1.12.3 VER ARCHIVOS DE REGISTRO

118. Se pueden ver los archivos de registro en el búfer de memoria por parámetros como nombre de archivo, categoría y gravedad. Para ello:

– Acceder al modo EXEC de usuario.

```
# enable
```

– Ver una lista de registros desde el más antiguo al más

```
# show logging file
```

– Ver registros de entrada de alarma

```
# show logging file alarm
```

– Ver una lista de registros organizados por la CPU que los generó.

```
# show logging CPU <CPUs>
```

Los valores de CPU válidos van de 0 a 100 caracteres. Separe varias CPU con una barra vertical. Por ejemplo: CPU1|CPU2.

– Ver las entradas de registro de la CLI.

```
# show logging detail
```

– Ver los registros de un código de evento específico.

Los valores de código válidos van de 0 a 10 caracteres. Separe varios códigos con una barra vertical.

– Ver los registros de un módulo específico.

```
# Show logging module <module>
```

Los valores de módulo válidos van de 0 a 100 caracteres e incluyen las siguientes categorías de módulos: EAP, RMON, WEB, STG, IGMP, HW, MLT, FILTER, QOS, CLILOG, SW, CPU, IP, VLAN, IPMC, IP-RIP, OSPF, PIM, POLICY, RIP. Separe varios módulos con una barra vertical.

– Ver los registros de un archivo especificado.

```
# show logging name-of-file <string>
```

Las cadenas válidas de no más de 99 caracteres incluyen la ruta y el nombre del archivo, como /intflash/ logcopy.txt.

– Ver registros para uno o más niveles de gravedad.

```
# show logging severity <level>.
```

Los valores de nivel válidos van de 0 a 25 caracteres e incluyen los siguientes: INFO, ERROR, WARNING, FATAL. Separe varios niveles de gravedad con una barra vertical.

– Ver una lista de archivos de registro ordenados del más reciente al más antiguo.

```
# show logging tail
```

5.1.12.4 BORRAR MENSAJES Y ARCHIVOS DE REGISTRO

119. Para borrar los mensajes de registro de la memoria y eliminar los archivos de registro activos:

- Acceder al modo EXEC privilegiado.

```
# enable
```

- Borrar el archivo de memoria.

```
# clear logging
```

- Borrar los archivos de registro.
  - Determinar qué archivo es el archivo de registro activo.

```
# show logging info
```

  - Mostrar todos los archivos de registro almacenados en el sistema.

```
# ls
```

    Los archivos cuyos nombres empiezan por log se almacenan en el sistema.

  - Para eliminar un archivo de registro, ejecutar el siguiente comando e introduzca y en el indicador.

```
# del <filename>

Remove ./<filename> (y/n) ?
```

  - Para eliminar varios archivos de registro, ejecutar el siguiente comando.

```
# del log.* -y
```

    Se admiten caracteres * y -y responde al *prompt* con y.

5.2 TAREAS GENERALES DE CONFIGURACIÓN

120. Esta sección describe los procesos para deshabilitar servicios, crear mensajes de *banner*, establecer un umbral de inactividad y actualizar el *software*.

5.2.1 DESHABILITAR SERVICIOS NO COMPATIBLES

121. **Se deben deshabilitar los siguientes servicios: HTTP, HTTPS e *iqagent*.** Para ello, proceda de la siguiente forma:

- Acceder al modo de configuración global.

```
# enable

# Configurar terminal
```

- Deshabilitar el acceso web *HTTP*.

```
(config)# no web-server enable
```

- Desactivar el acceso web *HTTPS*.

```
(config)# no web-server secure-only
```

– Desactivar la aplicación *iqagent*.

```
(config)# application

(config-app)# no iqagent enable
```

5.2.2 CONFIGURACIÓN DEL MENSAJE DE *BANNER*

122. **Se debe configurar un banner de inicio de sesión que proporcione información a los usuarios que acceden a la interfaz de línea de comandos de VOSS a través de una conexión serie o una conexión SSHv2.**

123. Para configurar el mensaje que los usuarios ven antes de iniciar sesión (denominado banner personalizado) y el mensaje del día (MOTD), que ven después de iniciar sesión se debe:

– Acceder al modo de configuración global.

```
# enable

# Configurar terminal
```

– Habilitar el *switch* para utilizar un banner personalizado.

```
(config)# banner personalizado
```

– Crear el *banner* personalizado, que los usuarios verán antes de iniciar sesión.

```
(config)# banner <message-text>
```

124. Para crear un mensaje con múltiples líneas, se puede utilizar el comando `banner` antes de cada nueva línea del mensaje. Para crear una cadena de palabras separadas por espacios, se debe poner el texto entre comillas. Cada línea de texto del mensaje puede admitir hasta 80 caracteres. El número total de caracteres del mensaje no puede superar los 1896 caracteres.

```
config)# banner motd <message-text>
```

125. Para crear un MOTD con varias líneas, se debe utilizar el comando `banner motd` antes de cada nueva línea de del mensaje. Para crear una cadena de palabras separadas por espacios, ponga el texto entre comillas. Cada línea de texto del mensaje puede admitir hasta 80 caracteres. El número total de caracteres del MOTD no puede superar los 1516 caracteres.

– Habilitar el mensaje del día.

```
(config)# banner displaymotd
```

– Guardar los mensajes.

```
(config)# save config
```

– Verificar los mensajes.

```
(config)# show banner
```

– Detener e iniciar el servidor SSH interno.

126. Este paso permite mostrar el banner y el MOTD cuando los usuarios acceden al VOSS a través de una conexión SSHv2.

```
(config)# no ssh

(config)# ssh
```

5.2.3 CONFIGURACIÓN DE UN UMBRAL DE TIEMPO DE ESPERA DE INACTIVIDAD DE SESIÓN

127. **Se debe realizar la configuración de un umbral de tiempo de inactividad de sesión. Este umbral debe ser el menor tiempo posible que permita la operatividad del equipo.**

128. Se puede especificar el número máximo de segundos permitidos para que una sesión SSH o una conexión serie estén inactivas. Si la inactividad supera ese umbral, la sesión se desconecta y el usuario debe volver a conectarse. Para ello:

- Acceder al modo de configuración global.

```
# enable

# Configurar terminal
```

- Especificar el umbral de tiempo de espera.

```
(config)# cli timeout <seconds>
```

  Los valores válidos van de 30 a 655535. El valor predeterminado es 900.

6. FASE DE OPERACIÓN

6.1 ACTUALIZACIÓN DE *SOFTWARE*

129. **Se deben mantener los *switches* actualizados, sobre todo en lo que respecta a la aplicación de parches de seguridad que corrigen vulnerabilidad conocidas en los productos.**

130. El VSP realiza actualizaciones de *software* utilizando un método de "*activación retardada*". Es decir, el *software* se instala en el inventario de *software* antes de ser activado. Cuando se activa la imagen de actualización, el nuevo *software* se convierte en la imagen primaria. La imagen primaria actual se convierte en la imagen de copia de seguridad. La imagen de copia de seguridad actual se convierte en una imagen disponible en el inventario. El dispositivo solicitará el reinicio del *switch* para completar el proceso de activación.

131. El proceso de actualización de VOSS implica las siguientes tareas.

- Inventario de *software*. Puede verificar la versión en ejecución del *software* en cualquier momento utilizando el comando `show software`.
- Copia de seguridad de la configuración. Se realiza una copia de seguridad de la configuración para que el *switch* pueda volver a aplicar la configuración después de reiniciarse.
- Descarga de imagen. Descarga el archivo de imagen de actualización (*.tgz) a una ubicación a la que el switch pueda acceder.
- Actualización del *software*. Con el método de activación retardada, la versión actual del *software* continúa ejecutándose hasta que Reiniciar el switch para completar la activación.

6.2 VISUALIZACIÓN DEL INVENTARIO DE SOFTWARE

132. Como buena práctica, **se debe verificar la versión del software en ejecución antes de comenzar el proceso de actualización.** Para ello, se debe:

- Acceder al modo EXEC privilegiado.

```
# enable
```

- Verificar la versión en ejecución del software.

```
# show software
```

6.3 COPIA DE SEGURIDAD DE LA CONFIGURACIÓN

133. **Se deben realizar copias de seguridad de la configuración para facilitar su restauración en caso de ocurrir algún tipo de incidencia.** Cuando se realiza una copia de seguridad de la configuración, el *switch* puede volver a aplicar la configuración después de que se actualice el *software* y se Reiniciar el *switch*.

134. Para ello:

- Acceder al modo Privileged EXEC.

```
# enable
```

- Determinar el nombre del archivo de configuración.

```
# show boot config choice
```

- Guardar el archivo de configuración.

```
# save config file <file-name>
```

- Copiar el archivo de configuración en una ubicación accesible desde el switch.

```
# copy /intflash/config.cfg <direction ip>/dir/config_backup.cfg
```

6.4 DESCARGA DE LA IMAGEN DE ACTUALIZACIÓN

135. El archivo de imagen de actualización (*.tgz) contiene el código ejecutable que se ejecuta en el switch. Para su descarga, se deben realizar las siguientes acciones:

- Obtener la imagen de actualización del sitio de soporte de Extreme Networks: http://www.extremenetworks.com/support

  El acceso requiere un ID de usuario o sitio válido y una contraseña. Si no se dispone de una cuenta se puede solicitar una con el enlace "Solicitar inicio de sesión web".

- Utilizar SCP o un cliente SFTP para colocar los archivos de imagen en la siguiente ubicación en un servidor que su *switch* pueda localizar: `/initflash/shared`.

6.5 PROCEDIMIENTO ACTUALIZACIÓN DE *SOFTWARE*

136. Este procedimiento muestra cómo actualizar el *software* utilizando la memoria flash interna como ubicación de almacenamiento de archivos.

137. Durante la actualización, el sistema verifica las firmas digitales que están incrustadas en los archivos de actualización y rechaza la instalación de una imagen que tenga una firma no válida.

138. Para realizar la actualización del software, se debe proceder de la siguiente forma:

- Acceder al modo de configuración global.

```
# enable

# Configurar terminal
```

- Transferir los archivos de actualización al switch mediante SCP o a través del puerto USB.

- Extraer los archivos de actualización.

```
(config)# software add <version>
```

  Los archivos de imagen se añaden al subsistema de almacenamiento de imágenes de software y los archivos se extraen al directorio /intflash/release.

- Mostrar el inventario de software para confirmar que se han añadido los archivos de imagen.

```
(config)# show software
```

- Activar la imagen de actualización, que copia la versión especificada en el archivo flash de arranque.

```
(config)# software activar <version>
```

El *software* activado se convierte en la imagen primaria. La imagen primaria actual se convierte en la imagen de copia de seguridad. La imagen de copia de seguridad actual se convierte en una imagen disponible en el inventario. Se le pedirá que Reiniciar el switch para completar la activación.

- Cuando se le pida que Reiniciar el switch, introduzca y. Se completa el proceso de activación, se reinicia el sistema, se instala la nueva versión y se cargan los parámetros del sistema. Los parámetros provienen del archivo de configuración más reciente.
- Acceder al modo EXEC privilegiado.

  ```
  # enable
  ```

- Comprobar que la versión de software está instalada.

  ```
  # show software
  ```

  La salida del comando muestra el inventario de software en el sistema, incluidas las versiones primarias y de copia de seguridad.

- Confirmar el nuevo *software*, lo que garantiza que la versión del *software* es de confianza.

  ```
  # software commit
  ```

7. ABREVIATURAS

AES	*Advanced Encryption Standard*
CA	*Certificate Authority*
CC	*Common Criteria*
CLI	*Command Line Interface*
CN	*Common Name*
CSR	*Certificate Signing Request*
DNS	*Domain Name Server*
IP	*Internet Protocol*
NTP	*Network Time Protocol*
OCSP	*Online Certificate Status Protocol*
RBAC	*Role-Based Access Control*
SAN	*Subject Alternative Name*
SSH	*Secure Shell*
TLS	*Transport Layer Security*
TTY	*TeleTypewriter*
UPS	*Uninterruptible Power Supply*
USB	*Universal Serial Bus*
VOSS	*VSP Operative System Software*
VSP	*Virtual Services Platform*

PUBLICACIONES DE DEFENSA

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