centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1430

Procedimiento de empleo seguro
Switches Extreme Networks SLXOS

Marzo de 2022

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

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
2022.03.24 12:43:36 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-106-3

Fecha de Edición: marzo 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. Extreme Networks fabrica equipamiento de red y comunicaciones para entornos corporativos, administración pública y proveedores de servicios.
2. A menos que se indique lo contrario, la información de este documento es aplicable a todos los equipos mencionados en el apartado siguiente. En caso de haber alguna excepción, como palabras clave de comando asociadas con una versión de *software* específica, se indicará en el texto.
3. Cuando una característica, funcionalidad u operación es específica de un determinado *hardware*, se utiliza el nombre del equipo al que se refiere. Cuando las características, funcionalidades y operaciones son las mismas para toda una familia de productos, se hace referencia al equipo con el nombre genérico de *switch* o *router*.

2. OBJETO Y ALCANCE

4. El presente documento tiene como objetivo detallar las configuraciones de seguridad de los **switches de Extreme Networks basados en SLXOS, versiones 20.1.1aa y 20.2.1aa**, de forma que la protección y funcionamiento del producto se realice de acuerdo a unas garantías mínimas de seguridad
5. Los switches que ejecutan la versión 20.1.1aa de SLXOS son los siguientes:
    - ***SLX9150, SLX9250, SLX9640.***
6. Los switches que ejecutan la versión 20.2.1aa de SLXOS son los siguientes:
    - ***SLX9740, SLX 9540.***

3. ORGANIZACIÓN DEL DOCUMENTO

7. Se propone la siguiente estructura para este documento:

   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**. Se presenta un *checklist* de alto nivel para desplegar los dispositivos de forma segura.

   e) **Apartado 8**. Incluye el listado de documentos referenciados a lo largo del documento.

   f) **Apartado 9**. Incluye el listado de las abreviaturas empleadas a lo largo del documento.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

8. El producto se envía en formato *appliance* físico. Dichos *appliance* incluyen un sello que asegura que el producto no se ha manipulado tras abandonar las instalaciones del fabricante. Se debe verificar la integridad del sello.
9. Este *appliance* se entrega sin instalación de *firmware*, de tal forma que deberá descargarse e instalarse tras la recepción. La descarga del software se puede realizar desde la página de soporte de *Extreme Networks*.
10. Una vez descargada la versión correspondiente, **se debe verificar su integridad mediante el uso de firmas PGP**.
    - Descargar la clave PGP de *Extreme Networks* de la siguiente página.
    - Descargar el fichero ".tar.gz" correspondiente a la versión del software descargada. Este fichero contiene los hashes SHA256 y SH512 de la imagen firmados con la clave PGP.
    - Extraer el fichero y verificar que las firmas PGP de todos los ficheros son válidas.
    - Si las firmas son válidas, generar el hash SHA512 y SHA256 de la imagen y verificar que coincide con los indicados en dichos ficheros.
11. El detalle de verificación de las firmas PGP y los hashes de las imágenes software se puede consultar en el siguiente enlace.

4.2 ENTORNO DE INSTALACIÓN SEGURO

12. Los componentes del producto deben instalarse en un entorno en el cual solo el personal técnico dispone de autorización para la configuración, despliegue y mantenimiento del producto, por ejemplo, el Centro de Proceso de Datos de la organización.

4.3 INSTALACIÓN

13. Una vez obtenida la versión de *firmware* siguiendo los pasos indicados en el apartado 4.1 ENTREGA SEGURA DEL PRODUCTO, se debe instalar en el dispositivo.
14. Para ello, trasladar el fichero de *firmware* de forma segura al dispositivo y ejecutar el siguiente comando:

```
SLX# firmware download fullinstall scp host <ipaddress> user <username> password <password>
directory /<your_firmware_directory> coldboot
```

4.3.1 CONFIGURACIÓN BÁSICA

15. Utilizar el cable de serie incluido en la caja de accesorios que se entrega con el equipo y conectarlo al puerto de consola del dispositivo por un lado y por otro a un terminal o a un PC que ejecute una aplicación de emulación de terminal (por ejemplo, *HyperTerminal* o *TERM*).
16. La aplicación de terminal debe estar configurada para utilizar los parámetros estándar de puerto serie, todos los equipos de *Extreme* utilizan los mismos parámetros de puerto serie:
    - Bits por segundo: 115200.
    - Paridad: None.
    - Bits de Datos: 8.
    - Bits de Parada: 1.
    - El control de flujos tiene que estar deshabilitado.
17. Una vez que se ha conectado el cable y el terminal o la aplicación de terminal está en ejecución, pulsar la tecla "*Intro*" y aparecerá en pantalla el *prompt* predeterminado instando al usuario a entrar su nombre y contraseña (ver apartado 4.3.2 USUARIOS POR DEFECTO):

```
SLX#
```

18. Los ejemplos que vienen a continuación corresponden a un switch de distribución, aunque, a menos que se indique lo contrario, son aplicables a todos los dispositivos.
19. Para cambiar parámetros, introducir las sentencias de configuración una por una. Para dar valor negativo a un comando, simplemente anteponer la palabra "NO". A continuación, un ejemplo de configuración de un chasis y del *hostname* del dispositivo:
    - Para entrar en el modo de configuración global ejecutar:

```
SLX#configure terminal
SLX(config)#
```

    - Desde el modo de configuración global, para cambiar el nombre por defecto de *host* y del chasis. El *hostname* puede tener hasta 30 caracteres alfanuméricos:

```
SLX(config)# switch-attributes chassis-name <text-string>
SLX(config)# switch-attributes host-name <text-string>
```

    - El cifrado de las contraseñas debería estar activada por defecto, de tal forma que se almacenará el hash SHA-512 (su configuración se detalla en el apartado 5.4.4 POLÍTICA DE CONTRASEÑAS). Sin embargo, para asegurarse de ello, ejecutar el siguiente comando de configuración:

```
SLX(config)# service password-encryption
```

- La gestión fuera de banda se utiliza para poder disponer de un canal de comunicaciones ajeno al flujo de datos en la red. La gestión fuera de banda utiliza desde puertos serie a interfaces Ethernet. Desde el modo de configuración de la interfaz, configurar la interfaz de gestión "*Out of Band*" (OOBM).

```
SLX(config)# interface Management 0
SLX(config)# no shutdown
SLX(config)# vrf forwarding mgmt-vrf
SLX(config)# no ip address dhcp
SLX(config)# ip address <IPv4ADDRESS/Prefix>
SLX(config)# no ipv6 address autoconfig
```

20. Para asegurarse de que los cambios se guardan después de reinicios o apagado del equipo, se deben guardar los cambios en la configuración almacenada en memoria no volátil (VNRAM) con la siguiente sentencia:

```
SLX# copy running-config startup-config
```

4.3.2 USUARIOS POR DEFECTO

21. El producto inicialmente dispone de las siguientes cuentas por defecto:

    - *User*. Usuario local para el acceso a la gestión por consola. Puede ejecutar comandos de tipo "*show*", así como los siguientes comandos de operación: *cfm, execute-script, exit, mtrace, no, ping, rasman, ssh, sysmon, telnet, timestamp, trace-12* y *traceroute*. Su contraseña por defecto es "*password*".
    - *Admin*. Usuario local para el acceso a la gestión por consola. Puede ejecutar todos los comandos soportados en el dispositivo. La contraseña por defecto es "*password*".
    - *Root*. Usuario administrador para la gestión del sistema operativo Linux subyacente. Su contraseña por defecto es "*fibranne*".

22. **Se debe cambiar la contraseña por defecto de dichas cuentas una vez instalado el producto, tal como se indica a continuación.**

23. Para cambiar la contraseña de la cuenta *Root* seguir los siguientes pasos:

    - Iniciar sesión en el producto con la cuenta *Admin*.
    - Ejecutar "*start-shell*" para acceder a la interfaz de comandos del sistema operativo Linux.
    - El comando "*su-*" requiere una contraseña que, por defecto, es "*fibranne*". La primera vez que el usuario *admin* ejecuta "*su-*", se le pedirá que cambie la contraseña *root* por defecto.
    - Seguir la secuencia de configuración siguiente para cambiar la contraseña del usuario *root*:

```
SLX# start-shell
        2020/02/10-18:08:13, [SH-1001], 1500,, INFO, SLX, Event:
        SLXVM Linux shelln]. Login Time : Mon Feb 10 18:08:13 2020
        Entering Linux shell for the user: admin
[admin@SLX]# su -
        Password:
        set the default switch context
        Disclaimer for root account Usage!

        This SLX router is equipped with root account that is intended for
        diagnostics and debugging purposes solely by the equipment vendor's trained
        engineers. Improper use of the functionality made available through the root
        account could cause significant harm and disruption to the network
        operation.

        Please change passwords for router default accounts now.
        Use Control-C to exit or press 'Enter' key to proceed.

        Changing default password for "root"
        Warning: Access to the root account may be required for complete access of
        the router. Please ensure the root password is documented in a secure
        location. Recovery of a lost root password will result in downtime.

        Changing password for root
        Enter new password:
        Re-type new password:
        passwd: password updated successfully
```

24. Para cambiar la contraseña de las cuentas *Admin* y *User* seguir los siguientes pasos:

    - Iniciar sesión en el SLX con la cuenta *Admin* y la contraseña por defecto *password*.
    - Ejecutar los siguientes comandos de configuración:

```
SLX(config)# username admin role admin encryption-level 10 password
(<WORD:8-40>): ****************
2020/02/10-18:05:16, [SEC-1197], 1495,, INFO, SLX, Changed account admin.
Change User account password:
SLX(config)# username user role user encryption-level 10 password
(<WORD:8-40>): ****************
2020/02/10-18:05:16, [SEC-1197], 1495,, INFO, SLX, Changed account user.
```

25. Las cuentas *User* y *Admin* no pueden eliminarse del dispositivo. Por lo tanto, se deben deshabilitar utilizando el siguiente comando:

```
SLX(config)# username nombre_usuario enable false
```

4.4 LICENCIAS

26. El producto dispone de dos (2) tipos de licencias:

    - Licencias permanentes. Este tipo de licencia no tiene fecha de expiración y se vinculan a un único dispositivo de forma permanente.
    - Licencias SAU (*Self Authenticated Upgrade*). Este tipo de licencias no requieren de activación.

27. Para instalar una nueva licencia permanente en el dispositivo, se deben seguir los siguientes pasos:

- Primero, se debe generar la licencia. Para ello acceder al portal de soporte e ir a *Assets > Licenses Home*.
- Hacer clic en *Generate License* e introducir el *Voucher ID* recibido por correo electrónico durante la adquisición de la licencia.
- Hacer clic en *Next*, introducir el número de serie del dispositivo y hacer clic en *Submit*.
- Se mostrará una página con la información de la licencia, hacer clic en *Download* para obtener el fichero de licencia.
- Una vez obtenida la licencia, esta se debe instalar en el dispositivo. Para ello copiar el fichero de licencia en un servidor SCP local para transferirlo al dispositivo.
- Realizar la transferencia con el siguiente comando:

```
SLX(config)# license add SCP-URL scp://ubicación/fichero_licencia
```

- Verificar que se ha instalado correctamente con el comando *show license*.

28. En el caso de las licencias de tipo SAU, se deberá ejecutar el siguiente comando y seguir las instrucciones indicadas en pantalla:

```
SLX(config)# license eula accept
```

29. El detalle de instalación de licencias se puede consular en la guía *Extreme SLX-OS Software Licensing Guide, 20.1.1 – REF5.*

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

30. **El producto dispone de un modo de operación seguro que deberá activarse.**

31. Para habilitar el modo de empleo seguro del producto, se deben ejecutar los siguientes comandos:

```
SLX(config)# unhide fips
SLX(config)# fips cc-enable
```

32. Una vez habilitado el modo de operación segura, se activan las siguientes características:

    - Se eliminan y regeneran todas las contraseñas, secretos compartidos y claves privadas, así como la base de datos de configuración. Después se reinicia el dispositivo.
    - Se desactiva el servidor *Telnet* y se bloquea su configuración.
    - Se bloquea el acceso CLI mediante *Telnet*.
    - El servidor HTTP se desactiva.
    - No se permite el uso del cliente HTTP para descargas de firmware.
    - No se permite el uso de TFTP.

33. Adicionalmente, una vez activado el modo seguro, se recomienda:

    - No hacer uso de SNMP versiones uno, dos y tres.
    - No hacer uso de TACACS+.
    - No hacer uso de LDAP.

5.1.1 DESHABILITAR SERVICIOS

34. La desactivación de algoritmos, protocolos y servicios específicos es necesaria para el mantenimiento de un entorno seguro. **Se deben seguir los siguientes pasos para deshabilitar los protocolos inseguros:**

    - Desactivar el servidor *Telnet*:

```
SLX(config)# telnet server use-vrf default-vrf shutdown
SLX(config)# telnet server use-vrf mgmt-vrf shutdown
```

    - Desactivar el servidor HTTP:

```
SLX(config)# http server use-vrf default-vrf shutdown
SLX(config)# http server use-vrf mgmt-vrf shutdown
```

5.2 AUTENTICACIÓN

35. El acceso al producto requiere un mecanismo de autenticación basado en usuario y contraseña. Se dispone de una base de datos propia para almacenar los distintos usuarios y contraseñas y llevar a cabo una autenticación local. Consultar el apartado 5.4.1 CONFIGURACIÓN DE ADMINISTRADORES para el detalle de configuración de usuarios locales.

36. Adicionalmente, se permite la integración con servidores externos de autenticación. Se recomienda hacer uso sólo de RADIUS y en caso de ser necesario. El detalle de configuración se puede consultar en el apartado 5.3 SERVIDORES DE AUTENTICACIÓN.

37. La base de usuarios local admite hasta 64 usuarios. En caso de necesitar más, será necesario configurar un servidor de autenticación externo.

38. Para determinar el método de autenticación primario y secundario del producto, se debe utilizar el siguiente comando. Por ejemplo, para utilizar la base de datos local como método primario y el servidor RADIUS como secundario:

```
SLX(config)# aaa authentication login local radius
```

39. En caso de configurar un método primario y uno secundario, se consultará el método secundario en caso de no obtener respuesta del primario. Sin embargo, si el método primario deniega el acceso, no se consulta el método secundario.

40. En caso de utilizar solo la autenticación local, el comando sería:

```
SLX(config)# aaa authentication login local
```

5.3 SERVIDORES DE AUTENTICACIÓN

41. En caso de configurar autenticación mediante servidores externos, **se recomienda hacer uso únicamente de RADIUS sobre TLS**. Para ello, primero deberá importarse el certificado de CA del servidor RADIUS siguiendo los pasos indicados en el apartado 5.6.2 IMPORTAR CERTIFICADOS CA.

42. Una vez configurado el certificado, para llevar a cabo la configuración de un servidor RADIUS, se utiliza el siguiente comando:

```
SLX(config)# radius-server host { ip-address | host-name } [ use-vrf { mgmt-vrf | default-vrf | vrf-name } ][ auth-port portnum ] [ radsec ] [ timeout secs ] [ retries num ] [ key shared-secret ] [ protocol { chap | pap | peap} ] [ encryption-level value-level ]
```

43. Puede tener los siguientes parámetros:

    - *ip-address*: especifica la dirección IP del servidor RADIUS. Se soporta tanto IPv4 como IPv6.
    - *host-name*: especifica el *hostname* del servidor RADIUS. Soporta máximo 40 caracteres

- *use-vrf* (opcional). Fuerza la comunicación con el servidor RADIUS mediante un VRF específico.
- *auth-port*. Especifica el puerto para la autenticación. El puerto por defecto es UDP 1812. Para RADIUS sobre TLS el puerto TCP por defecto es 2083**. Se debe utilizar RADIUS sobre TLS**.
- *radsec*. Especifica que se utiliza RADIUS sobre TLS en lugar de RADIUS sobre UDP. **Debe indicarse este parámetro**.
- *encryption-level*. Designa el nivel de cifrado para la operación mediante claves secretas compartidas. Los valores válidos son de 0 a 7, siendo 0 texto claro y 7 el cifrado más alta. **El valor por defecto y recomendado es 7, correspondiente a AES 256**.
- *key*. Especifica la clave utilizada como secreto compartido entre el dispositivo y el servidor RADIUS para asegurar el intercambio de mensajes. La clave debe tener entre 1 y 40 caracteres. *En RADIUS sobre TLS la clave por defecto es radsec*.
- *protocol*. Especifica el protocolo de autenticación. Las opciones son CHAP, PEAP y PAP, siendo CHAP el habilitado por defecto. Se recomienda utilizar PAP.
- *retries*. Especifica el número de reintentos permitidos para conectarse a un servidor RADIUS. El valor por defecto es 5.

44. Ejemplo de pasos de configuración de un servidor RADIUS:

```
SLX(config)# radius-server host 192.168.0.10 use-vrf radsec
mgmt-vrf
SLX(config-host-ip_address/mgmt-vrf)# auth-port 2083
SLX(config-host-ip_address/mgmt-vrf)# protocol pap
SLX(config-host-ip_address/mgmt-vrf)# source-interface
management 0
SLX(config-host-ip_address/mgmt-vrf)# key <shared-secret>
SLX(config-host-ip_address/mgmt-vrf)# exit
SLX(config)#aaa authentication login radius local
SLX(config)#aaa accounting exec default start-stop none
SLX(config)#aaa accounting commands default start-stop none
SLX(config)#aaa authorization command none
SLX(config)# dot1x port-control auto
SLX(config)# no shutdown
```

45. **Por último, se debe especificar el uso de algoritmos de cifrado seguros en las comunicaciones RADIUS sobre TLS. Para esto se debe utilizar el comando *cipherset radius***. Dicho comando no permite configurar los algoritmos particulares, si no que forzará automáticamente el uso de:

- AES256-SHA256
- AES256-SHA
- AES128-SHA256
- AES128-SHA

5.4 ADMINISTRACIÓN DEL PRODUCTO

46. Los métodos para realizar la gestión del producto son:

    - Acceso CLI local accediendo al puerto serie.
    - Acceso CLI mediante SSHv2. Ver apartado 5.5.1 SSH para el detalle de configuración de SSH.
    - Acceso REST API mediante HTTPS. Ver apartado 5.6.1 CERTIFICADOS SSH para el detalle de configuración de HTTPS.

47. **Se recomienda hacer uso del acceso CLI mediante SSH para la gestión del producto**. Adicionalmente, todas las instrucciones de configuración indicadas en el presente documento harán uso de dicho método.

5.4.1 CONFIGURACIÓN DE ADMINISTRADORES

48. El producto utiliza el control de acceso basado en roles (RBAC) como mecanismo de autorización. Un rol es un contenedor de reglas, que especifican qué comandos se pueden ejecutar y con qué permisos. Cuando se crea una cuenta de usuario, se necesita especificar un rol para esa cuenta.

49. El *software* incluye por defecto dos cuentas predeterminadas (*Admin* y *User*) y sus dos roles predeterminados correspondientes:

    - *admin*: las cuentas con permisos de administrador pueden ejecutar todos los comandos admitidos en el dispositivo.
    - *user*: las cuentas con permisos de nivel de usuario pueden ejecutar todos los comandos *show* admitidos en el dispositivo. Las cuentas de nivel de usuario también pueden ejecutar los siguientes comandos operativos: *cfm, executecript, exit, mtrace, no, ping, rasman, ssh, sysmon, telnet, timestamp, trace-12* y *traceroute*.

50. Dichos roles predeterminados no pueden eliminarse ni modificarse. En el próximo apartado, se indica cómo configurar los roles y permisos del producto.

51. Los parámetros necesarios para crear una cuenta de usuario son el nombre de usuario, el rol que tendrá, y su contraseña. Para crear una cuenta, seguir los siguientes pasos:

    - En modo EXEC con privilegios, introducir el comando:

    ```
    SLX# configure terminal
    ```

    - Introducir el comando *username* con los parámetros correspondientes:

    ```
    SLX (config)# username username password password role role_name [ access-time
    HHMM to HHMM ] [ desc description ] [ enable { true | false } ] [ encryptionlevel
    { 0 | 7 | 10 } ] [ expire { never | YYYY-MM-DD } ]
    ```

52. Los parámetros de los que dispone son:

    - *Username.* Nombre de usuario.

- *Password.* Contraseña.
- *Role.* Rol asignado.
- *Access-time.* Parámetro opcional que determina en qué periodos en horas y minutos podrá acceder el usuario. En caso de no configurarlo tendrá acceso las 24h del día. **Se recomienda utilizar este parámetro para limitar lo máximo posible el tiempo de acceso.**
- *Desc.* Descripción opcional.
- *Enable*. Parámetro opcional que indica si el usuario está activado o no. Por defecto estará activado.
- *EncryptionLevel.* Indica cómo se almacenará la contraseña. Tal como se ha visto anteriormente, el comando *service password-encryption*, sobrescribe este valor para todo el producto.
- *Expire*. Indica cuando expirará la contraseña mediante fecha. Se recomienda configurar un valor que defina, como máximo, dos meses desde la creación de la contraseña.

53. En caso de querer modificar una cuenta de usuario existente, se utilizará el mismo comando. Se introducirá el nombre de usuario de la cuenta que desea modificarse y los valores nuevos que se desea asignar.
54. Con el parámetro *Enable* es posible deshabilitar una cuenta:

```
SLX (config)# username nombre_usuario enable false
```

5.4.2 CONFIGURACIÓN DE ROLES Y PERMISOS

55. Los roles "*admin*" y "*user*" están predefinidos en SLXOS. El rol "*admin*" puede ejecutar todos los comandos. El rol "*user*" no puede entrar en modo privilegiado para configurar el *switch*. Sin embargo, puede ejecutar todos los comandos *show*. Estos dos roles no pueden eliminarse ni modificarse.
56. El producto permite gestión de roles y permisos mediante el uso de reglas. Estas reglas determinarán los distintos permisos que tendrán los roles.
57. El comando *role*, permite la creación de roles. Este comando sólo define el nombre del rol, siendo necesaria la asignación de reglas para determinar los permisos.

```
SLX (config)# role name role_name [ desc description ]
```

58. El comando *rule*, permite la creación de reglas, que determinan los permisos de los distintos roles.

```
SLX (config)# rule index [ action { accept | reject } ] [ operation { read-only | readwrite } ] role role_name command command_name
```

- *Index.* Asigna un número identificativo a la regla.
- *Action*. Indica si el rol permite o deniega el uso del comando.

- *Operation*. Define el tipo de operación permitida (lectura o escritura).
- *Role*. Define el rol al que aplica la regla.
- *Command*. Especifica el comando sobre el que se define la regla.

59. El detalle de configuración de roles se puede consultar en el apartado *User defined roles* de la guía *Extreme SLX-OS Security Configuration Guide, 20.1.1 – REF3.*

60. Para asignar un rol a un usuario, se puede realizar durante la creación del mismo con el comando *username* (ver apartado 5.4.1 CONFIGURACIÓN DE ADMINISTRADORES). Adicionalmente se podrá modificar posteriormente con el mismo comando.

```
SLX(config)# username Admin password ""BwrsDbB+tABWGWpINOVKoQ==\n" encryption-level 7 role
LogAdmin desc "Log Configuration Administrator"
```

61. Una cuenta definida remotamente autenticada con RADIUS puede usar también RBAC. El servidor RADIUS puede ser configurado para incluir a un usuario en un grupo RBAC específico. El siguiente ejemplo es un ejemplo de fichero para un usuario en FreeRadius 3.0

```
#
alan   Cleartext-Password := "password"
       Brocade-Auth-Role: "Admin"
```

5.4.3 SEGURIDAD DE LA MAC DE PUERTO

62. **Se recomienda la configuración de Media Access Control (MAC)**, de tal forma que solo se pueda acceder a la gestión del producto haciendo uso de un dispositivo. Para ello utilizar los siguientes comandos:

    - Acceder a la interfaz deseada.

      ```
      SLX(config)# interface Ethernet <slot/port>
      ```

    - Activar las características de capa 2 de la interfaz, configurar modo acceso y se activa la seguridad de puertos.

      ```
      SLX(config)# switchport
      SLX(config)# switchport mode access
      SLX(config)# switchport port-security
      ```

    - Se configura la dirección MAC que tendrá acceso al dispositivo, se indica que el máximo direcciones MAC con acceso será 1.

      ```
      SLX(config)# switchport port-security mac-address address
      SLX(config)# switchport port-security max 1
      ```

5.4.4 POLÍTICA DE CONTRASEÑAS

63. Los usuarios han de contar con una contraseña segura para su acceso al producto. En el caso de utilizar autenticación con servidores externos, se utilizará la política de contraseñas definida en los mismos, por lo que **se debe configurar en los**

servidores de autenticación una política similar a la indicada en el presente apartado.

64. Las políticas de contraseñas definen y aplican un conjunto de reglas que hacen que las contraseñas sean más seguras, al someter todas las nuevas contraseñas a restricciones globales. Se pueden configurar políticas de seguridad para contraseñas, políticas de cifrado de contraseñas y políticas de bloqueo de cuentas.

65. Para configurar la política de contraseñas utilizar el siguiente comando:

```
SLX(config)# password-attributes {[max-retry maxretry] [min-length minlen] [maxlockout-duration duration] [admin-lockout | character-restriction { [lower numlower] [numeric numdigits] [special-char numsplchars] [upper numupper] } [history hisnum] [Login-notify-duration hours] [repeat repnum] [sequence seqnum]}
```

- *Min-lenght*: define la longitud mínima de la contraseña. **Se recomienda un valor de 12 caracteres al menos**. Las contraseñas tienen un máximo de 40 caracteres.
- *Character-restriction*: permite definir el número mínimo de caracteres de un tipo concreto. **Se recomienda configurar un valor de, al menos, uno (1) para cada tipo**:
  - *Lower*: define el mínimo de letras minúsculas que debe contener la contraseña.
  - *Upper*: define el mínimo de letras mayúsculas que debe tener la contraseña.
  - *Numeric*: define el mínimo de números que debe tener la contraseña.
  - *Special-char*: define el mínimo de caracteres especiales que debe tener la contraseña.
- *Admin-lockout*: habilita el bloqueo de cuentas con rol de administración. **Se recomienda utilizar este parámetro**.
- *Max-retry*: Define el número de fallos de inicio de sesión antes de bloquear una cuenta de usuario. **Se recomienda configurar un valor de tres (3) contraseñas fallidas**.
- *Max-lockout-duration*: define la duración del bloqueo en minutos. **Se recomienda un valor de, al menos, cinco (5) minutos**.
- *History*: define el número de contraseñas antiguas contra las que se comprueba una contraseña recién configurada. La nueva contraseña se descarta si coincide con una contraseña anterior. El rango es de 0 a 10. **Se recomienda configurar un valor de, al menos, cinco (5)**.
- *Login-notify-duration*: Especifica la cadencia en horas en la que se notifica al administrador el número de intentos exitosos ocurridos en ese lapso de tiempo. Los valores válidos van de 0 a 120 y el valor predeterminado es 0, que deshabilita la opción. **Se recomienda configurar un valor de 120**.

- *Repeat*: especifica el número mínimo de caracteres repetidos consecutivos en una nueva contraseña configurada. La nueva contraseña se descarta si tiene caracteres consecutivos repetidos (por ejemplo, aaa, xxx, 1111). Para deshabilitar este parámetro, configurar 1. El valor predeterminado es 1.
- *Sequence*: Especifica el número mínimo de caracteres secuenciales consecutivos tanto hacia delante como hacia atrás (por ejemplo, abc, cba) en una contraseña. La nueva contraseña se descarta si tiene caracteres secuenciales consecutivos (por ejemplo, abc, xyz, fedc). Para deshabilitar este parámetro, configurar 1. El valor predeterminado es 1.

66. El producto admite el cifrado de las contraseñas de todas las cuentas de usuario existentes, habilitando el cifrado de contraseñas a nivel de dispositivo, de tal forma que se almacenará únicamente su hash SHA-512. Por defecto, el servicio de cifrado está habilitado. En caso contrario, **se debe habilitar el cifrado** a nivel de producto con el siguiente comando:

```
SLX(config)# service password-encryption
```

67. Las siguientes reglas se aplican al cifrado de contraseñas:
    - Cuando se habilita el cifrado de contraseña a nivel de producto, todas las contraseñas de texto no cifradas existentes se cifrarán y posteriormente, las contraseñas que se agregan sin cifrar se almacenan en formato cifrado.
    - Hay tres (3) niveles de cifrado de contraseñas, definidos con el parámetro *encryption-level* del comando *username*:
        - Nivel 0: sin cifrado, texto claro.
        - Nivel 7: cifrado AES-256.
        - Nivel 10: formato HASH salted SHA-512. Este es el nivel de cifrado predeterminado.
    - Cuando se habilita el cifrado global se invalidan los parámetros a nivel de comando *username*. Por lo tanto, si se configurara una contraseña con *encryption-level 0*, esta se cifraría igualmente.
68. En caso de deshabilitar el servicio de cifrado de contraseñas, las nuevas contraseñas agregadas no cifradas serán almacenadas como texto claro en el dispositivo. Las contraseñas cifradas existentes permanecen cifradsa. **Se recomienda mantener el servicio activo siempre.**
69. Si existen contraseñas con nivel de cifrado 7 en el dispositivo, puede usar el comando ejecutable *password-encryption convert-enc-to-level-10* para actualizar las contraseñas al nivel de cifrado 10 (formato hash SHA-512). Una vez que este comando se ejecuta, todas las contraseñas de nivel 7 se convierten a nivel 10.

5.4.5 CONFIGURACIÓN DE LOS MENSAJES DE ACCESO AL SISTEMA

70. El producto permite la configuración de varios tipos de mensajes de tipo *banner*: "*INCOMING*", "*LOGIN*" y "*MESSAGE OF THE DAY (motd)*":

- El mensaje "*motd*" se presenta en el momento en que se introduce el username de la sesión remota. Para configurar un mensaje "motd" de varias líneas:
- El mensaje "*incoming*" se muestra cuando un usuario establece una sesión Telnet.
- El mensaje "*login*" se muestra cuando un usuario inicia sesión en el dispositivo.

71. **Se deberá configurar un mensaje de acceso al sistema**. Para configurar el *banner* del tipo deseado, se debe ejecutar el siguiente comando:

```
SLX(config)# banner [motd | incoming | login ] [ESC-m] [paste in banner] Cntl-D
```

5.4.6 CONFIGURACIÓN DE LA ACL DE GESTIÓN

72. La ACL de gestión de entrada está configurada para denegar de forma predeterminada y permitir como excepción. **Se recomienda configurar la ACL de gestión para denegar todo el tráfico no necesario en la interfaz de gestión del producto**. Para ello:

- Crear la ACL con el nombre deseado:

```
SLX(config)# ip access-list extended <ACL_Name>
```

- Permitir el acceso remoto SSH al puerto de gestión.

```
SLX(config)# seq 10 permit tcp <mgmt-network/prefix> host <mgmt_address> eq 22
count
```

- Permitir el protocolo NTP en el puerto de gestión.

```
SLX(config)# seq 20 permit tcp <mgmt-network/prefix> host <mgmt_address> eq 123
count
```

- Permitir SNMP en el puerto de gestión.

```
SLX(config)# seq 30 permit tcp <mgmt-network/prefix> host <mgmt_address> eq 161
count
```

- Denegar todo el tráfico no permitido explícitamente.

```
SLX(config)# seq 100 deny ip any any count
```

- Aplicar la ACL a la interfaz de gestión.

```
SLX(config)# Interface Management 0 Ip access-group <ACL_Name> in
```

5.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

5.5.1 SSH

73. El dispositivo hace uso de SSHv2 para la gestión remota por defecto. Hace uso de claves compartidas, autentica clientes o servidores y garantiza que los dispositivos

que acceden a la red son legítimos. También se hace uso de SSHv2 en la conexión con otros router o equipos SLX.

74. Los pasos para configurar SSHv2 son:
    - Configurar los algoritmos de cifrado del servidor y del cliente SSH.
    - Configurar los algoritmos de intercambio de claves de cliente y servidor SSH.
    - Configurar los algoritmos de autenticación de mensajes del servidor SSH y del cliente.
    - Configurar el número máximo de sesiones SSH.
75. Los algoritmos de cifrado, intercambio de claves y autenticación de mensajes no son mutuamente excluyentes. Se puede configurar en el dispositivo cualquier combinación de estos elementos
76. Se pueden configurar algoritmos de autenticación de mensajes tanto cuando el producto actúa como cliente como servidor SSH. Antes de comenzar el servidor SSH debe estar habilitado.
77. Para comprobar si el servidor SSH está habilitado ejecutar el comando:

```
SLX# show ssh server status
```

78. En caso de estar deshabilitado, se debe utilizar el comando *ssh server enable*.

```
SLX# no ssh server use-vrf vrf-name shutdown
```

79. Para configurar los algoritmos de autenticación de mensajes, seguir los siguientes pasos:
    - Entrar en el modo de configuración global.

      ```
      SLX# configure terminal
      ```

    - Configurar los algoritmos cuando actúa como servidor SSH. Se pueden especificar múltiples algoritmos separando los nombres de las cadenas con comas. **Se recomienda hacer uso de HMAC-SHA2-256 y HMAC-SHA2-512**.

      ```
      SLX(config)# ssh server mac hmac-sha2-256,hmac-sha2-512
      ```

    - Configurar los algoritmos cuando actúa como cliente SSH. Se pueden especificar múltiples algoritmos separando los nombres de las cadenas con comas. **Se recomienda hacer uso de HMAC-SHA2-256 y HMAC-SHA2-512**.

      ```
      SLX(config)# ssh client mac hmac-sha2-256,hmac-sha2-512
      ```

    - Reiniciar el servidor SSH para que la configuración surta efecto. Esta operación desconectará todas las sesiones SSH activas.

```
SLX(config)# do ssh-server restart
Warning: This operation will disconnect all active SSH sessions.
Are you sure you want to restart the SSH server [y/n]? y
SSH server is going down for restart NOW !!
SSH server restarted !!
```

- Confirmar la información de configuración de SSH con los siguientes comandos.

```
SLX(config)# do show running-config ssh server
SLX(config)# do show running-config ssh client
SLX(config)#  show ssh server status
SLX(config)# do show ssh client status
```

- El prefijo "no" en los comandos *ssh server mac* y *ssh client mac* se puede utilizar para eliminar los MAC deseados.

80. Se deberá también configurar los algoritmos de cifrado que utilizará el protocolo SSH. Para ello, seguir los siguientes pasos en la línea de comandos:

- Entrar en el modo de configuración de terminal.

```
SLX# configure terminal
```

- Configurar los algoritmos cuando actúa como servidor SSH. Se pueden utilizar múltiples cifrados separando los nombres de las cadenas con comas. **Se recomienda hacer uso de los siguientes cifrados**:

```
SLX(config)# ssh server cipher aes128-ctr, aes256-ctr, aes128-cbc, aes256-cbc
```

- Configurar los algoritmos cuando actúa como cliente SSH. Se pueden utilizar varios cifrados separando los nombres de las cadenas con comas. **Se recomienda hacer uso de los siguientes cifrados**:

```
SLX(config)# ssh client cipher aes128-ctr, aes256-ctr, aes128-cbc, aes256-cbc
```

- Reiniciar el servidor SSH para que la configuración surta efecto.

```
SLX(config)# do ssh-server restart
Warning: This operation will disconnect all active SSH sessions.
Are you sure you want to restart the SSH server [y/n]? y
SSH server is going down for restart NOW !!
SSH server restarted !!
```

- Se puede verificar la configuración con los comandos *do show running-config ssh server cipher* y *do show running-config ssh client cipher*.
- El prefijo "no" en los comandos *ssh server cipher* y *ssh client cipher* restablece los cifrados SSH a sus algoritmos predeterminados.

81. El producto permite también definir el intercambio de claves SSH, el cual especifica los algoritmos utilizados para generar claves de sesión de un solo uso para cifrado y autenticación con el servidor SSH.

82. Los siguientes algoritmos de intercambio de claves de servidor ssh y cliente ssh son compatibles con el modo seguro:

- *ecdh-sha2-nistp256.*

- *diffie-hellman-group-exchange-sha256.*
- *diffie-hellman-group14-sha1.*

83. Para configurar los algoritmos de intercambio de clave seguir los siguientes pasos:

    - Entrar en el modo de configuración de terminal.

      ```
      SLX# configure terminal
      ```

    - Utilizar el comando *ssh server key-exchange* para configurar el algoritmo de intercambio de claves cuando actúa como servidor. Se pueden utilizar múltiples algoritmos de intercambio de claves separando los nombres de las cadenas con comas. **Se recomienda hacer uso de *ecdh-sha2-nistp256 y, en cualquier caso, evitar diffie-hellman-group14-sha1, por no presentar la fortaleza suficiente***.

      ```
      SLX(config)# ssh server key-exchange ecdh-sha2-nistp521
      ```

    - Utilice el comando *ssh client key-exchange* para configurar el algoritmo de intercambio de claves cuando actúa como cliente. Se pueden utilizar múltiples algoritmos de intercambio de claves separando los nombres de las cadenas con comas. **Se recomienda hacer uso de *ecdh-sha2-nistp256 y, en cualquier caso, evitar diffie-hellman-group14-sha1, por no presentar la fortaleza suficiente***.

      ```
      SLX(config)# ssh client key-exchange ecdh-sha2-nistp521
      ```

    - Reiniciar el servidor SSH desde el modo EXEC utilizando el comando *ssh-server restart* para que la nueva configuración surta efecto.

      ```
      SLX(config)# exit
      SLX# ssh-server restart
      ```

    - El prefijo "no" en el comando *ssh server key-exchange* y *ssh client key-exchange* restablece los algoritmos de intercambio de claves SSH a sus valores predeterminados.

84. Se debe configurar a su vez la clave del dispositivo. Se admiten las siguientes claves SSH:

    - DSA.
    - RSA con longitudes de clave de 1024, 2048 y 4096 bits. **En caso de utilizar esta opción, se deberá utilizar claves de 4096 bits.**
    - ECDSA con longitud de clave de 256 bits.

85. DSA se utiliza de forma predeterminada. Cuando se utiliza RSA, el tamaño de clave RSA predeterminado es 2048. **Se debe realizar la configuración para hacer uso de ECDSA o RSA con longitudes de clave de 4096 bits**:

    ```
    SLX(config)# ssh server key ecdsa
    ```

86. Cuando se cambia la clave del servidor SSH, reiniciar el servidor SSH desde el modo *EXEC* utilizando el comando *ssh-server restart* para que la nueva configuración surta efecto.

5.5.1.1 PARÁMETROS DE SESIÓN EN SSH

87. Se deben configurar los parámetros de sesión para las conexiones SSH. Los siguientes comandos afectan tanto al protocolo SSH como a las conexiones seriales:

    - Tiempo máximo de inactividad, en segundos, **se debe configurar un valor de 5 minutos**:

      ```
      device(config)# ssh server max-idle-timeout 300
      ```

    - Tiempo máximo de conexión, en minutos, **se recomienda un valor bajo, por ejemplo 1h**:

      ```
      device(config)# line vty exec-timeout 60
      ```

    - Número máximo de intentos de autenticación, **se debe configurar un valor de 3. Una vez alcanzado el valor, se terminará la sesión**:

      ```
      device(config)# ssh server max-auth-tries 3
      ```

    - Tiempo máximo de autenticación, en segundos, si no se obtiene respuesta en ese periodo, se deniega el acceso. **Se recomienda un valor de 30 segundos**:

      ```
      device(config)# ssh server max-login-timeout 30
      ```

    - Tiempo y volumen de regeneración de claves:

      ```
      device(config)# ssh server rekey-volume <Megabytes: 512-4095 (default: 1024 MB)>
      device(config)# ssh server rekey-interval <Seconds: 900-3600 (default: 3600)>
      ```

5.5.1.2 CONFIGURACIÓN DE ACCESO MEDIANTE CLAVES PÚBLICAS

88. Se pueden importar claves públicas de cliente SSH para establecer el inicio de sesión de usuarios. También es posible eliminar la clave posteriormente para evitar que se siga utilizando. **Se debe hacer uso de claves ECDSA**.

89. Para importar una clave pública de cliente SSH al dispositivo mediante SCP, seguir los siguientes pasos. El parámetro *user* define el usuario local que utilizará dicha clave

    ```
    SLX# certutil import sshkey directory ssh_public_key_path file file-name protocol SCP host
    remote_ip_address login login_id password password user user_acct
    ```

90. Una vez que se añade una clave pública a un usuario de esta forma, se tratara de autenticar al usuario siempre primero con la clave pública. En caso de fallar esta autenticación, se solicitará la contraseña.

91. También se pueden añadir claves SSH a los usuarios copiando la clave pública directamente, **se recomienda hacer uso de este método**. Para ello utilizar el siguiente comando:

```
SLX# certutil sshkey user <user> pubkey <public key>
```

92. Una vez que la clave pública ha sido copiada mediante este comando, entonces la autenticación basada en contraseña se deshabilita para ese usuario en particular. El usuario no puede iniciar sesión con una contraseña válida, pero la autenticación basada en contraseña continúa funcionando para todos los demás usuarios que no tienen la clave pública configurada.

93. Se pueden eliminar claves mediante el siguiente comando:

```
SLX# no certutil sshkey user admin
```

94. Cuando se importa o elimina la clave pública, el servidor SSH se reinicia automáticamente y todas las conexiones SSH activas se finalizan

```
SLX# 2019/01/14-10:28:58, [SEC-3050], 75, INFO, SLX9540, Event: sshutil, Status: success,
Info: Imported SSH public key from 10.70.4.106 for
```

5.5.1.3 CONFIGURACIÓN DE ACCESO MEDIANTE CERTIFICADOS

95. Es posible también configurar el acceso SSH haciendo uso de certificados de tipo X.509v3. Para ello se deben seguir primero los pasos descritos en el apartado 5.6.1 CERTIFICADOS SSH, para configurar los certificados de servidor necesarios.

96. Una vez configurados dichos certificados, se deberá configurar también el DN de los usuarios que accederán mediante certificado, de tal forma que quede definida la forma de acceso:

```
device# certutil sshx509v3 user <> DN <>
```

5.5.2 TLS

97. El producto permite el uso de TLSv1.1 y TLSv1.2 en sus comunicaciones. Se pueden configurar los parámetros concretos de cada comunicación haciendo uso del comando *ssl-profile* dentro del modo de *management-security*. Las distintas conexiones en las que utiliza TLS son:

    - En el envío de registros de auditoría a un servidor externo mediante *syslog*, en este caso el producto actúa como cliente. Ver apartado 5.8.2 CONFIGURACIÓN DE SYSLOG.
    - Comunicación con el servidor RADIUS externo para la autenticación de usuarios, en este caso el producto actúa como cliente. Ver apartado 5.3 SERVIDORES DE AUTENTICACIÓN.
    - En la gestión remota mediante REST API. En este caso el producto actúa como servidor.

98. **Se debe hacer uso únicamente de TLSv1.2**. Para ello se debe configurar la versión de TLS mínima compatible con los modos de funcionamiento de servidor y cliente:

    - Entrar en el modo Terminal de Configuración.

```
SLX # config term
Entering configuration mode terminal
SLX (config)#
```

    - Entrar en el modo *management-security*.

```
SLX (config)# management-security
SLX (mgmt-security)#
```

    - El modo *management-security* permite configurar la versión mínima de TLS admitida para que el equipo SLX opere en los modos servidor y cliente. Este paso muestra cómo configurar el modo de funcionamiento C*lient:*

```
SLX (mgmt-security)#
SLX (mgmt-security)# ssl-profile ?
Possible completions:
client management security ssl profile client for tls configuration
server management security ssl profile server for tls configuration
SLX (mgmt-security)# ssl-profile client
SLX (mgmt-sec-ssl-profile-client)#
```

    - Utilizar el comando ***tls min-version*** para establecer la versión mínima para este modo de operación en TLSv1.2.

```
SLX (mgmt-sec-ssl-profile-client)# tls ?
Possible completions:
min-version min version to be supported by client
SLX(mgmt-sec-ssl-profile-client)# tls min-version ?
Possible completions:
<1.1|1.2> specify TLS version
SLX(mgmt-sec-ssl-profile-client)# tls min-version 1.2
```

    - Repetir los últimos pasos para la opción *ssl-profile server*.

99. Una vez configurado, el producto es capaz de controlar cómo se conecta a un servidor remoto (cuando funciona como cliente) y cómo los clientes remotos se conectan con él (cuando funciona como servidor). En caso de no cumplirse la versión mínima configurada, se deniega la conexión.

100. Por último, deberán configurarse los certificados necesarios para las comunicaciones TLS, para ello, ver el apartado 5.6 GESTION DE CERTIFICADOS.

5.6 GESTION DE CERTIFICADOS

5.6.1 CERTIFICADOS SSH

101. Para poder llevar a cabo la autenticación SSH mediante certificados, **se debe configurar el certificado de servidor del producto**. Para ello:

    - Configurar el par de claves y el *trustpoint*. **Se debe utilizar como *key type*, claves ECDSA**.

```
device# configure terminal
device(config)# crypto key label <key name> <key type> modulus <key size>
device(config)# crypto ca trustpoint <trustpoint name>
device(config-ca-<>)# keypair <key name>
device(config-ca-<>)# end
```

- Importar el certificado de CA utilizado para firmar el certificado de servidor.

```
device# crypto ca authenticate <trustpoint> cert-type [sshx509v3] protocol <>
directory <> file <> host <> user <> password <>
```

- Importar el certificado de servidor.

```
device# crypto ca [import] <trustpoint> cert-type [sshx509v3] protocol <>
directory <> file <> host <> user <> password <>
```

- Configurar el algoritmo aceptado por el servidor para negociar con los clientes. Las opciones son:

```
device(config)# [no] ssh server algorithm hostkey <x509v3-ssh-rsa |
x509v3rsa2048-sha256>
```

- Para la autenticación mutua, el servidor envía el certificado al cliente. Asociar el certificado de servidor al servicio SSH mediante la configuración de *trustpoint*.

```
device(config)# ssh server certificate profile server
device(ssh-server-cert-profile-server)# trustpoint sign <trustpoint name>
```

102. **Deberá importarse también la CA utilizada para firmar los certificados de usuario**:

```
device# crypto import sshx509v3ca protocol <> host <> directory <> file <> user <>
password <>
```

103. Configurar también el DN de los usuarios que accederán mediante certificado:

```
device# certutil sshx509v3 user <> DN <>
```

5.6.2 IMPORTAR CERTIFICADOS CA

104. Para las comunicaciones con los servidores *Syslog* y RADIUS, en las cuales el producto actúa como cliente, **se deberá importar la CA de los certificados de los servidores,** para poder realizar la verificación a la hora de comunicarse.

105. Para ello, utilizar los siguientes comandos:

```
device# crypto import syslogca host <hostip> user <username> password <password> directory
<dir name> file <ca file> protocol scp
device# crypto import radiusca host <hostip> user <username> password <password> directory
<dir name> file <ca file> protocol scp
```

5.6.3 CERTIFICADOS HTTPS

106. **Se deberán configurar los certificados necesarios para el acceso a la gestión mediante REST API**. Para ello se admiten claves de tipo DSA, RSA y ECDSA, se deberá hacer uso de estas últimas.

107. Se debe hacer uso únicamente de HTTPS. HTTP y HTTPS son mutuamente excluyentes:

- Si HTTP está habilitado (de forma predeterminada), ejecutar el comando *http server* para parar el servicio, seguido del comando *no http server* para habilitar HTTPS.
- Si HTTP está deshabilitado, ejecutar el comando *no http server* para habilitar HTTPS.
- Reiniciar el dispositivo.

108. Las etiquetas para el punto de confianza (*trustpoint*) y el par de claves deben ser coherentes durante todo este proceso. Para configurar los certificados HTTPS seguir los siguientes pasos:

- Entrar en el modo de configuración.

```
SLX#configure terminal
```

- Generar un par de claves para firmar y cifrar la información de seguridad durante los intercambios del protocolo de seguridad con el comando *crypto key*. Se debe hacer uso de ECDSA. El tamaño de clave con ECDSA puede ser 256, 384 o 521.

```
SLX(config)# crypto key label k1 ecdsa modulus [256/384/521] ecdsa modulus 521
```

- Configurar la autoridad certificadora (CA) de confianza que emitió el certificado de identidad importado, con el comando *crypto ca*.

```
SLX(config)# crypto ca trustpoint t1
SLX(config-ca-t1)#
```

- Asociar el par de claves al punto de confianza con el comando *keypair*. La asociación entre el punto de confianza, el par de claves y el certificado de identidad es válida hasta que se elimina explícitamente, cuando se eliminan el certificado, el par de claves o punto de confianza.

```
SLX(#config-ca-t1)# keypair k1
```

- Volver al modo EXEC con privilegios con el comando *end*.

```
SLX(#config-ca-t1)# end
```

- Autenticar el dispositivo ante la CA.

```
SLX# crypto ca authenticate t1 cert-type https protocol SCP host 10.70.12.102
user fvt directory /users/home/ crypto file cacert.pem
Password: **********
```

- Exportar el certificado de inscripción a la ubicación especificada para el host remoto con el comando *crypto ca enroll*

```
SLX# crypto ca enroll t1 cert-type https country US state CA locality SJ
organization BRC orgunit SFI common myhost.extreme.com protocol SCP host
10.70.12.102 user fvt directory /users/home/crypto password password
```

- Importar el certificado de servidor del producto:

```
SLX# crypto ca import t1 certificate cert-type https protocol SCP host
10.70.12.102 user fvt directory /users/home/crypto file swcert.pem password
```

109. El detalle de configuración de certificados HTTPS, incluyendo cómo deshabilitarlos en caso necesario, se puede consultar en el apartado *HTTPS Certificates* de la guía *Extreme SLX-OS Security Configuration Guide, 20.1.1 - REF3.*

110. Después de instalar los certificados HTTPS, el servidor web debe reiniciarse para configurar el servicio HTTPS. De forma predeterminada, el servicio web se ejecuta cuando se inicia el dispositivo.

- Reiniciar el servicio web con el comando *http server use-vrf <vrf-name> shutdown* en modo de configuración, seguido del comando *no http server use-vrf <vrf-name> shutdown.*
- Reiniciar completamente el dispositivo.

5.7 SINCRONIZACIÓN

111. **Se recomienda hacer uso de un servidor de tiempo NTP**. Para ello, seguir los siguientes pasos:

- Configurar la clave que se utilizará durante la autenticación NTP. Se puede hacer uso de MD5 o SHA1. Al no disponer de mecanismo de mayor fortaleza, **se recomienda el uso de SHA1**:

```
SLX(config)# ntp authentication-key 1 sha1 <key>
```

- Configurar dicha clave como clave de confianza para ser utilizada en las comunicaciones:

```
SLX(config)# ntp trusted-key 1
```

- Utilizar el siguiente comando para exigir la autenticación NTP a nivel global:

```
SLX(config)# ntp authenticate
```

- Configurar el servidor NTP, indicando la dirección IP del servidor, la clave que utilizará dicha comunicación y la versión de NTP que se utilizará (el dispositivo permite el uso de las versiones 3 y 4). **Se debe seleccionar la versión 4**.

```
SLX(config)# ntp server IP  key id-clave version 4
```

5.8 AUDITORÍA

5.8.1 REGISTRO DE EVENTOS

112. El producto permite almacenar hasta mil (1000) registros de auditoría. Una vez alcanzado el límite, los registros más antiguos se eliminan para permitir almacenar

los más recientes. **Es por esto que se recomienda realizar la configuración de un servidor de auditoría externo mediante *Syslog*, tal como se explica posteriormente**.

113. Los mensajes RAS (*Reliability, Availability* y *Serviceability*) fueron así denominados por IBM y se utilizan para almacenar eventos relativos a cambios de configuración o errores. Los mensajes se reportan con diferentes niveles de gravedad, desde informativo (INFO) hasta niveles crecientes de error (*WARNING, ERROR* y *CRITICAL*).

114. Los mensajes de auditoría se dividen en los siguientes tipos:

- Mensajes de sistema (LOG). Se reportan mensajes de eventos o información significativos a nivel de sistema y asimismo se usan para mostrar el estado de acciones de alto nivel iniciadas por el usuario. Se pueden enviar a un servidor *Syslog* externo. Un ejemplo de mensaje tipo LOG es:

  2017/09/14-23:26:44, [FW-1424], 620, M1 | Active, WARNING, SLX9850-8, Switch status changed from HEALTHY to MARGINAL

- Mensajes DCE RASLog: estos mensajes reportan eventos de errores e información sobre los módulos basados en protocolos, tales como *Network Service Module* (NSM), *System Services Manager* (SSM), etc. Se pueden enviar a un servidor *Syslog* externo. Un ejemplo de mensaje tipo DCE es:

  2017/09/14-23:26:25, [NSM-1004], 617, M1 | Active | DCE, INFO, SLX9850-8, Vlan 1 is created

- Mensajes *AUDIT* log. La auditoría de eventos está diseñada para soportar determinación de problemas basados en eventos de alta frecuencia de cierto tipo, como por ejemplo violaciones de seguridad, descargas de firmware y configuraciones. Se pueden enviar a un servidor *Syslog* externo. Un ejemplo de mensaje tipo DCE es:

  891 AUDIT, 2017/09/14-23:30:29 (GMT). [SEC-3024], INFO, SECURITY, NONE/root/NONE/None/CLI,, SLX9850-8, Event: passwd, Status: success, Info: User account [user], password changed

  Para cualquier evento de este tipo, se captura la siguiente información:

  - *User Name*: Nombre de usuario que ha disparado la acción.
  - *User Role*: El nivel de acceso del usuario, tal como *Root* o *Admin*.
  - *Event Name*: El nombre del evento que ha ocurrido.
  - *Status*: El estado del evento: *success* o *failure*.
  - *Event Info*: Información sobre el evento.

  La siguiente tabla describe las tres (3) clases de eventos que pueden ser auditadas:

Clase de Evento	Operando	Descripción
DCMCFG	*CONFIGURATION*	Pueden auditarse todos los cambios de configuración en el Sistema Operativo.
FIRMWARE	*FIRMWARE*	Pueden auditarse los eventos que hayan ocurrido durante el proceso de descarga de firmware.
SECURITY	*SECURITY*	Puede auditarse cualquier evento de seguridad iniciado por usuario para todos los interfaces de gestión. Para eventos que tengan impacto en la red entera, solamente se genera un mensaje de AUDIT para el switch desde el que se inició el evento.

- Mensajes FFDC. FFDC (*First Failure Data Capture*) se utiliza para capturar datos específicos sobre un fallo, cuando este aparece por primera vez y antes de que el switch se reinicie. Todas las iteraciones siguientes del mismo error se ignoran. Esta información crítica se salva en almacenamiento no volátil y puede recuperarse mediante el comando ***copy support***. Los mensajes de FFDC están diseñados para el uso por parte del soporte técnico de Extreme Networks, estando habilitados por defecto. Un ejemplo de mensaje de este tipo es:

  2017/09/14-23:28:18, [HASM 1200], 666, L1/0 | Active | FFDC, WARNING, SLX9850-8, Detected termination of process hslagtd:2915

- Mensajes CFFDC: CFFDC (*Chassis-wide FFDC*) se utiliza para capturar datos FFDC para cualquier módulo de gestión o tarjetas de línea en el chasis completo. Esta información se salva en memoria no volátil y puede ser recuperada mediante el comando ***copy support***. Estos mensajes solamente afectan a equipos basados en chasis.

115. El producto mantiene dos (2) repositorios de almacenamiento, *SYSTEM* y *DCE*:

- El repositorio *SYSTEM* se utiliza para mensajes de log críticos o importantes (así como para logs de seguridad). Puesto que almacena menos logs, los mensajes están almacenados durante mucho más tiempo.
- El repositorio *DCE* se utiliza para mensajes de log generales, y almacena los últimos eventos. (Habitualmente unos días, dependiendo del número de mensajes).

116. La siguiente tabla muestra los tipos de mensajes que se almacenan en cada repositorio.

Tipo de Mensaje	Repositorio DCE	Repositorio SYSTEM
LOG	No	Yes
DCE	Yes	No
CFFDC	Yes	Yes

Tipo de Mensaje	Repositorio DCE	Repositorio SYSTEM
FFDC	Yes	Yes
AUDIT	Yes	Yes

117. A su vez, los mensajes tienen cuatro (4) niveles de gravedad, desde *CRITICAL* hasta *INFO*. Por lo general, las definiciones abarcan un amplio espectro y deben utilizarse como una guía general para resolución de incidencias.

118. La tabla siguiente muestra los niveles de gravedad de los mensajes *RASLog*.

Nivel de Criticidad	Descripción
CRITICAL	Un mensaje *CRITICAL* indica que el software ha detectado serios problemas que causan un fallo parcial o total de un subsistema si no se corrige inmediatamente; por ejemplo, un fallo en una fuente de alimentación o una subida de temperatura deben recibir atención inmediata.
ERROR	Un mensaje de *ERROR* representa una condición de error que no afecta a de forma significativa a la funcionalidad completa del sistema. Por ejemplo un mensaje de ERROR puede indicar un *timeout* en una operación determinada, un fallo en una cierta operación después de un reintento, un parámetro no válido o un fallo al ejecutar una operación solicitada.
WARNING	Un mensaje de *WARNING* destaca una condición de operación que debe comprobarse o que puede producir un fallo en el futuro. Por ejemplo, el fallo de una fuente de alimentación en un sistema redundante proporciona un aviso que comunica que el sistema ya no está operando en modo redundante a no ser que la fuente que ha fallado sea reemplazada o arreglada.
INFO	Un mensaje de *INFO* reporta un estado no erróneo de los componentes del sistema. Por ejemplo, la detección de estado offline u online en un interface.

119. Los mensajes almacenados localmente pueden consultarse mediante el comando *show logging auditlog*.

120. Debido a las limitaciones de espacio en el almacenamiento local, **se recomienda configurar un servidor externo para la recepción de eventos de auditoría**. Para ello seguir los pasos indicados en el siguiente apartado.

5.8.2 CONFIGURACIÓN DE SYSLOG

121. Tal como se ha visto anteriormente, los mensajes de sistema, los mensajes *RASlog* y los de tipo *Auditlog*, pueden enviarse a un servidor de auditoría externo. Este envío utilizará *Syslog* sobre TLSv1.2. Para ello seguir los siguientes pasos:

- De forma previa se debe configurar la CA del certificado usado por el servidor de auditoría. Para ello seguir los pasos indicados en el apartado 5.6.2 IMPORTAR CERTIFICADOS CA.
- Configurar un servidor *Syslog* mediante el siguiente comando:

```
SLX(config)# logging syslog-server IP_Servidor use-vrf mgmt-vrf
```

5.9 ACTUALIZACIÓN DE *FIRMWARE*

122. Se deberán descargar las actualizaciones de *firmware* manualmente desde la página de soporte de *Extreme Networks*. El producto verifica de forma automática la integridad y la autenticidad del firmware previo a su instalación.

123. Asimismo, las imágenes están firmadas con GPG. Para verificar las firmas proceder de la siguiente forma:

- Descargar la clave de firma PGP de Extreme Networks (https://extremeportal.force.com/ExtrArticleDetail?an=000080173)
- Importar la clave en una instancia local de PGP o GPG.
- Descargar una imagen de *firmware* de *Extreme Networks*. Almacenar dicha imagen en un servidor local.
- Descargar el fichero *"<imagename>-digests.tar.gz".* Este fichero contiene los hashes SHA256 y SHA512 de la imagen de *firmware*.
- Extraer el fichero *"<imagename>-digests.tar.gz*" y verificar que las firmas PGP de todos los ficheros *"<file>-sha256.asc"* and *"<file>-sha512.asc*" son válidas.
- Si las firmas del paso anterior son válidas, entonces, y solo entonces, comprobar si los hashes calculados coinciden con los valores en los ficheros *"<file>-sha256"* y *"<file>-sha512*" respectivamente.

124. Actualizar el *firmware* del SLX-OS para asegurarse de que se aplican los parches de seguridad más recientes. El siguiente comando obtendrá el *firmware* desde el servidor local, lo reiniciará e instalará el nuevo *firmware*. Al hacer esta operación, tener cuidado si el *switch* está funcionando en producción.

```
SLX# firmware download fullinstall scp host <ipaddress> user <username> password
<password> directory /<your_firmware_directory> coldboot
```

125. Se admiten descargas mediante *ftp, scp, sftp* o usb. Se debe hacer uso únicamente de SCP o físicamente a través de un USB.

5.10 FUNCIONALIDADES DE SEGURIDAD IP

126. El producto incorpora varias funcionalidades de seguridad orientadas a mitigar, por ejemplo, los ataques de denegación de servicio (DoS). **Dichas funcionalidades deben ser activadas para este tipo de ataques. Para ello:**

- Configurar el dispositivo para denegar todos los paquetes ICMP fragmentados.

```
SLX(config)#  ip icmp-fragment enable
```

- Configurar el dispositivo para bloquear todos los paquetes con IP Options.

```
SLX(config)# ip option disable
```

- Configurar el dispositivo para no dar respuesta a mensajes ICMP *unreachable* o *Redirect*.

```
SLX(config)# no ip icmp unreachable
SLX(config)# no ip icmp redirect
SLX(config)# no ipv6 icmpv6 unreachable
SLX(config)# no ipv6 icmp redirect
```

5.11 POLÍTICAS DE PLANO DE CONTROL

127. Las políticas del plano de control están configuradas para limitar la tasa de un determinado tráfico o para deshabilitar tráfico configurado destinado al procesador del *switch*. El siguiente ejemplo es de una política de servicio que limita a 100 kbps los paquetes de sincronización TCP destinados al procesador del *switch*, el resto del tráfico a 8 Mbps sin deshabilitar ningún otro tráfico destinado al procesador del *switch*. Se pueden configurar políticas personalizadas específicas de esta manera. **Se deberán configurar políticas para limitar el tráfico solo al esperado.**

128. El comando *control-plane* permite acceder a la configuración del plano de control.

```
SLX# configure terminal
SLX(config)# policy-map policy1
SLX(config)# control-plane
```

129. El comando *police cir* permite configurar el *Committed Information Rate*, *Commmitted Burst Size*, *Exceeded Information Rate* y el *Exceeded Burst Size* para las clases de tráfico.

```
SLX(config)# policy-map
SLX(config-policymap-class)# police cir 100000
```

130. El comando *service-policy* asocia un *policy map* al tráfico del plano de control.

```
SLX(config)# control-plane
SLX(config-control-plane)# service policy in policy1
```

131. El comando *class* configura un *class map* para una política específica. Es obligatorio utilizar el comando *Police Cir*.

```
SLX(config-policymap)# class tcp-syn-cm
SLX(config-policymap-class)# police cir 100000
SLX(config)# class-map  everything-else-cm
```

132. Usamos el comando match para asociar un ACL a una *class map*.

```
SLX(config-classmap)# match access group everything-else
SLX(config))# class-map  tcp-syn-cm
SLX(config-classmap)# match access group tcp-syn
```

133.Definición del ACL.

```
SLX(config)# ip access-list extended tcp syn
SLX(config-ip-access-list-extended)# seq 10 permit tcp any any sync
SLX(config)# ip access-list extended tcp everything-else
SLX(config-ip-access-list-extended)# seq 10 permit ip any any
SLX(config-ip-access-list-extended)# seq20 permit icmp any any
SLX(config-ip-access-list-extended)# seq30 permit tcp any any
SLX(config-ip-access-list-extended)# seq40 permit ucp any any
```

6. FASE DE OPERACIÓN

134. El correcto funcionamiento del producto requiere de unas características que deben estar presentes en el entorno operacional:

- El producto debe contar con las **últimas actualizaciones de seguridad** para preservar al mismo de amenazas y vulnerabilidades conocidas.
- Se deben **mantener y analizar los registros de auditoría**. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos.
- Se deben **gestionar correctamente los certificados** utilizados, actualizándolos cuando sea necesario, por ejemplo, al expirar.
- Se deben realizar **copias de seguridad de manera periódica**, así como configurar el envío periódico de copias a un **servidor externo.**

7. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega del *appliance físico*	☐	☐	
Instalación en un entorno seguro	☐	☐	
Descarga del *firmware* y verificación de su integridad	☐	☐	
Instalación del *firmware* y registro de las licencias	☐	☐	
Cambio de contraseñas por defecto	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Configuración del modo seguro	☐	☐	
SERVIDORES DE AUTENTICACIÓN			
Configuración del servidor RADIUS	☐	☐	
ADMINISTRACIÓN DEL PRODUCTO			
Creación de usuarios y roles	☐	☐	
Configuración de las restricciones MAC	☐	☐	
Creación de la política de contraseñas	☐	☐	
Configuración del mensaje de acceso al sistema	☐	☐	
Creación de la ACL de gestión	☐	☐	
CONFIGURACIÓN DE PROTOCOLOS SEGUROS			
Configuración de los parámetros de SSH	☐	☐	
Configuración de los parámetros de TLS	☐	☐	
GESTIÓN DE CERTIFICADOS			
Creación de los certificados para SSH	☐	☐	
Importación de los certificados de las CA	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Creación de los certificados para HTTPS	☐	☐	
SINCRONIZACIÓN			
Configuración de un servidor de hora NTP	☐	☐	
AUDITORÍA			
Configuración de un servidor de auditoría externo	☐	☐	
FUNCIONALIDADES DE SEGURIDAD IP			
Activación de las protecciones	☐	☐	

8. REFERENCIAS

135. Las guías referenciadas a continuación se pueden consultar desde el siguiente enlace:

https://www.extremenetworks.com/support/documentation/slx-os-20-1-1/

REF1 *Extreme SLX-OS Management Configuration Guide, 20.1.1*

REF2 *Extreme SLX-OS Monitoring Configuration Guide, 20.1.1*

REF3 *Extreme SLX-OS Security Configuration Guide, 20.1.1*

REF4 *Extreme SLX-OS Command Reference, 20.1.1*

REF5 *Extreme SLX-OS Software Licensing Guide, 20.1.1*

REF6 *SLX-OS Release Notes:*

https://www.extremenetworks.com/support/release-notes/product/slx-c-series-software/

REF7 *SLX 9150:*

https://www.extremenetworks.com/support/documentation/slx9150/

REF8 *SLX9250:*

https://www.extremenetworks.com/support/documentation/slx9250/

REF9 *SLX9540:*

https://www.extremenetworks.com/support/documentation/slx9540/

REF10 *SLX9640:*

https://www.extremenetworks.com/support/documentation/slx9640/

REF11 *SLX9740:*

https://www.extremenetworks.com/support/documentation/slx9740/

REF12 *Extreme SLX-OS Message Guide:*

https://documentation.extremenetworks.com/slxos/sw/20xx/20.3.3/messages/GUID-88F1F989-1235-4FB8-BC9D-AEB238171EAF.shtml

REF13 *Extreme SLX-OS Security Configuration Guide, 20.2.1a*

https://documentation.extremenetworks.com/slxos/sw/20xx/20.2.1a/security/downloads/slx-20.2.1a-securityguide.pdf?_ga=2.157771002.1920589619.1637576382-124489780.1619420455

9. ABREVIATURAS

CIR	*Committed Information Rate*
CHAP	*Challenge Handshake Authentication Protocol*
ENS	*Esquema Nacional de Seguridad*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
GPG	*GNU Privacy Guard*
JITC	*Joint Interoperability Test Command*
OSPF	*Open Shortest Path First*
PAP	*Password Authentication Protocol*
PEAP	*Protected Extensible Authentication Protocol*
RADIUS	*Remote Authentication Dial-in Service*
RBAC	*Role Based Access Control*
SP	*Strict Priority*
SSL	*Secure Socket Layer*
TCP	*Transport Control Protocol*
TLS	*Transport Layer Security*
UDP	*User Datagram Protocol*
VRF	*Virtual Routing and Forwarding*
WFQ	*Weighted Fair Queuing*

PUBLICACIONES DE DEFENSA

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