centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1446

Procedimiento de empleo seguro
Switches EXOS de Extreme Networks

Junio de 2023

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.06.06 15:25:32 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-156-7.
Fecha de Edición: junio 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

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 objetivo de esta guía es establecer una referencia para la **configuración segura** de los **conmutadores o switches de la familia Summit 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.

5. Para conocer con más detalle las funcionalidades de los equipos Summit de Extreme Networks se recomienda la consulta de las guías de configuración, guías del CLI, artículos y demás documentación disponible en https://extremeportal.force.com

6. El sistema operativo de los *switches* Summit se llama **EXOS**. Está diseñado para proporcionar un alto rendimiento en los dispositivos, y tiene las capacidades necesarias para su despliegue en las redes de datos actuales (aplicaciones en la nube, Data Centers, proveedores de servicio, redes de pequeña y mediana empresa, etc).

7. Para el desarrollo de esta guía se ha utilizado la versión de EXOS 31.3.100 instalada en los siguientes switches*: ExtremeSwitching Series X435, X440-G2, X460-G2, X465, X695, 5520, 5320, 5420.* **Dichos switches han sido cualificados e incluidos en el Catálogo de Productos y Servicios de seguridad (CPSTIC) del Centro Criptólogico Nacional. Se debe consultar el CPSTIC para saber las versiones concretas que han sido cualificadas.**

8. EXOS está basado en un kernel de Linux versión 4.14.200 y tiene una estructura de configuración orientada a objetos. Un objeto puede ser un puerto, una Vlan, una ACL, una instancia de *routing* OSPF, etc.

9. La mayor parte de los comandos de configuración CLI tienen la siguiente estructura:

   create <objeto> / delete <objeto>
   configure <objeto> / unconfigure <objeto>
   configure <objeto> add / configure <objeto> delete
   enable <objeto> / disable <objeto>

10. Comandos de operación CLI útiles:

    show
    clear
    use
    reboot
    tftp put
    tftp get

11. Los cambios de configuración realizados en el *switch* no se guardan de forma automática en el fichero de configuración. Es necesario ejecutar el comando "*save*" para guardarlos de forma permanente. El *prompt* del CLI muestra un asterisco cuando hay cambios sin guardar:

    ** SW_EXOS.12 #*

3. ORGANIZACIÓN DEL DOCUMENTO

12. La estructura que sigue el documento es:

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

13. La descarga del *software* se puede realizar desde la página de soporte de *Extreme Networks.*
14. 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.
15. El detalle de verificación de las firmas PGP y los hashes de las imágenes software se puede consultar en el siguiente enlace:

    https://extremeportal.force.com/ExtrArticleDetail?an=000080173

4.2 PROTECCIÓN FÍSICA

16. 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).
17. 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*.

4.3 CONFIGURACIÓN DE PUERTOS

4.3.1 PUERTO DE CONSOLA

18. Los *switches* Summit disponen en el frontal de un puerto serie de consola que permite el acceso al *Command Line Interface* (CLI).
19. El puerto de Consola emplea RS-232 (9-pin), está cableado en RJ-45 y se utiliza normalmente para la configuración inicial del *switch*. A partir de entonces, se usa únicamente cuando el acceso remoto está desactivado o no está disponible.
20. El acceso al *switch* por el puerto de Consola requiere autenticación mediante usuario y contraseña, y presenta diversas vulnerabilidades:
    - El puerto de Consola no puede ser deshabilitado.
    - La desconexión del cable de Consola durante una sesión activa no finaliza la misma automáticamente.

21. El sistema operativo EXOS dispone de un temporizador de inactividad que, por defecto, termina las sesiones Telnet, SSH2 y de la consola cuando llevan 20 minutos inactivas. No obstante, **se deben cerrar siempre las sesiones con los comandos "*quit*" o "*logout*".**

    Nota: si una sesión telnet se pierde inadvertidamente el switch finaliza la sesión en un plazo de dos horas.

4.3.2 PUERTO ETHERNET DE GESTIÓN FUERA DE BANDA

22. Los *switches* Summit que usan el sistema operativo EXOS disponen en el frontal de un puerto Ethernet 10/100 Mbps o 10/100/1000 Mbps dedicado a la gestión fuera de banda. Este puerto:

    - No realiza conmutación de tráfico.
    - Pertenece a una VLAN especial llamada "*VLAN mgmt" (VID = 4095*), que está aislada dentro del *Virtual Router de gestión (VR-Mgmt).*
    - Permite el acceso a la gestión del switch siempre que la VLAN "Mgmt" tenga definida una dirección IP.

23. La gestión del *switch* mediante este puerto (fuera de banda) tiene notables ventajas respecto al empleo de interfaces de usuario (en banda). La gestión fuera de banda utiliza rutas físicas y lógicas dedicadas dentro del *switch*, garantizando que el tráfico de gestión esté totalmente aislado del tráfico de usuario.

24. A pesar de sus ventajas, se deben implementar las siguientes medidas de seguridad:

    - Se recomienda el uso de **políticas de seguridad** relativas a las cuentas de usuario y contraseñas descritas más adelante en esta guía.
    - **Configuración de un mensaje de advertencia** (*banner*) dirigido a los usuarios que deseen acceder al *switch*.
    - Se deben utilizar **protocolos de acceso y transferencia de ficheros seguros**: acceso al CLI mediante SSH y transferencia de archivos mediante SCP.
    - **Se recomienda el uso de un perfil de acceso o "*access-profile*" para cada tipo de acceso de gestión** al switch (Telnet, SSH, SNMP y Web). El *Access-Profile* permite restringir la conexión a las direcciones IPs específicas de los equipos de administración de red.

      configure telnet access-profile <policy_filename>
      configure snmp access-profile <policy_filename>
      configure ssh2 access-profile <policy_filename>
      configure web http access-profile add <ACL>

      El "*policy_filename*" es un fichero creado por el usuario en la memoria *flash* del switch donde se define la política de acceso. Su extensión es siempre ".pol". El formato de este fichero se describe en el apartado de ACLs.

25. Para más información y ejemplos se recomienda consultar la ***[User Guide].***

4.3.3 PUERTO USB

26. Los switches Summit que usan el sistema operativo EXOS disponen en el frontal de un puerto USB 2.0 que permite el intercambio de ficheros (logs, configuraciones, imágenes de firmware, etc) entre el switch y un dispositivo de memoria FAT32 conectado en el mismo.

27. Este puerto está habilitado por defecto, pero **se debe deshabilitar cuando no se utilice**. Es posible deshabilitar/habilitar este puerto mediante los comandos:

    disable switch usb

    enable switch usb

28. Para ver el estado del puerto USB, hay que utilizar el comando:

    show switch usb

29. El directorio donde se monta el contenido de una memoria conectada al puerto USB es:

    /usr/local/ext.

4.4 CONFIGURACIÓN POR DEFECTO O DE FÁBRICA

30. Los switches Summit que usan el sistema operativo EXOS arrancan por defecto (*default mode*) con una configuración simple de nivel 2:

    - Los puertos Telnet, STP (*Spanning Tree Protocol*) y SNMP desactivados
    - Todos los puertos habilitados y pertenecientes a una misma VLAN (la Default o 1).

31. Al conectarse por primera vez al puerto de Consola de un *switch* sin configuración, el sistema solicitará credenciales de acceso:

    login:admin

    password: (Enter)

32. Una vez iniciada una sesión por Consola, el switch ejecutará un script de interacción con el administrador (*safe-default-script*) con objetivo de configurar unos parámetros mínimos de seguridad sugeridos por Extreme Networks.

    This switch currently has some management methods enabled for convenience reasons. Please answer these questions about the security settings you would like to use. You may quit and accept the default settings by entering 'q' at any time.

    Would you like to activate VOSS? [y/N/q]

33. Para configurar el *switch* conforme a lo que establece esta guía**, no se ejecutará este script inicial**, sino que se realizará una configuración manual de todos los parámetros. Se debe seleccionar la opción "**q**", para **no ejecutar** el script de configuración inicial.

34. Si se desea devolver un *switch* ya configurado a un estado de fábrica (*factory defaults*) hay que ejecutar el siguiente comando:

    SW_EXOS.1 # unconfigure switch all

    Restore all factory defaults and reboot? (y/N)

4.5 CONFIGURACIÓN INICIAL BÁSICA

35. La identificación del switch es:

```
configure snmp sysName <Nombre>          /* Este es además el prompt del switch */
configure snmp sysLocation <Localización>
configure snmp sysContact <Contacto>
```

36. Virtual Routers y VLANs por defecto. Los switches Summit que usan el sistema operativo EXOS utilizan el concepto de Virtual Router (VR). Un VR es un contenedor de VLANs que permanece completamente aislado de otros Virtual Routers. Por defecto existen dos (2) Virtual *Routers*:

    - VR-Mgmt: Asociado a la VLAN "*Mgmt*" (VID = 4095). Esta VLAN sólo se utiliza para la gestión fuera de banda mediante el puerto *Mgmt* del frontal.
    - VR-Default: Asociado a la VLAN "*Default*" (VID=1), definida por defecto. Todas las nuevas VLANs que se creen pertenecerán por defecto a este VR.

37. Cada aplicación/comando de gestión que se ejecuta en el *switch* usa un VR por defecto para transmitir los paquetes. Si se desea que el tráfico salga por un VR diferente es necesario indicarlo en la ejecución.

38. Por defecto, estos son los VRs utilizados por las distintas aplicaciones:

```
Ping            -> vr-Default
telnet/ssh      -> vr-Mgmt
tftp get/put     -> VR donde se aloja la IP target
download        -> VR donde se aloja la IP target
upload           -> VR donde se aloja la IP target
syslog          -> vr-Mgmt
trap            -> depende de la configuración del servidor del NMS.
```

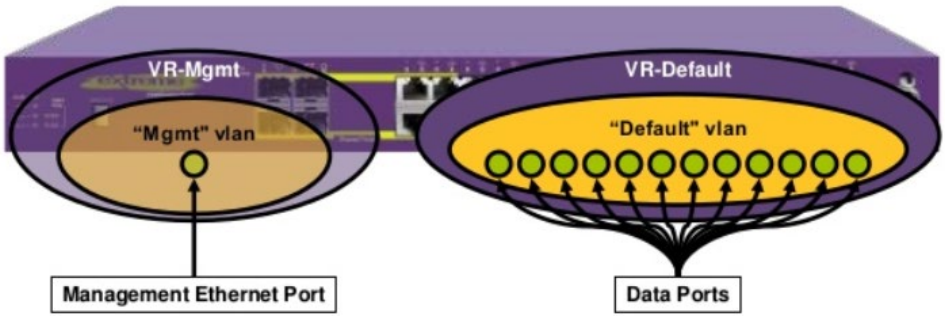
39. La gestión fuera de banda ess la mejor alternativa, aunque no siempre es posible.

```
configure vlan Mgmt ipaddress ip_address/subnet_mask
```

40. Un switch EXOS es gestionable a través de la interfaz de nivel 3 de cualquier VLAN. No existe el concepto de VLAN o dirección IP de gestión. **Es recomendable utilizar una VLAN exclusiva para la gestión del equipamiento de red**.

```
create vlan vlan_name tag tag
configure vlan vlan_name ipaddress ip_address/subnet_mask
```

41. En esta guía se ha considerado el despliegue más común realizado en las infraestructuras de red reales, donde los *switches* se gestionan en banda. En el resto del documento se utilizará por tanto el *VR-Default*.



42. Default Gateway:

    configure iproute add default gateway { metric } {multicast | multicast-only | unicast | unicast-only} {vr vrname}

43. Se deben borrar todos los puertos de la VLAN Default.

    configure vlan Default delete ports all

4.6 *SECURE SOCKET LAYER*

44. *Secure Socket Layer* (SSLv3) es una característica de *ExtremeXOS* que le permite autenticar y cifrar datos a través de una conexión SSL para proporcionar una comunicación segura.
45. El servidor web existente en ExtremeXOS permite a los clientes HTTP acceder a la página de inicio de sesión de red. Al utilizar HTTPS en el servidor web, los clientes acceden de forma segura a la página de inicio de sesión de red utilizando un navegador web habilitado para HTTPS.
46. Dado que SSL cifra los datos intercambiados entre el servidor y el cliente, estos están protegidos de una exposición no deseada.
47. El acceso HTTPS se proporciona a través de SSL y la Seguridad de la Capa de Transporte (TLS1.0). Estos protocolos permiten a los clientes verificar la autenticidad del servidor al que se conectan, garantizando así que los usuarios no se vean comprometidos por intrusos.
48. Se debe cargar o generar un certificado para el uso del servidor SSL. Antes de cargar un certificado, se debe obtener un certificado SSL de un proveedor de seguridad de Internet. Se admiten los siguientes algoritmos de seguridad:
    - RSA para criptografía de clave pública (generación de certificado y par de claves pública y privada, firma de certificados). Tamaño de clave RSA mayor a 3072 bits.
    - Cifrados simétricos (para cifrado de datos): AES-128-GCM and AES-256-GCM.
    - Algoritmos de código de autenticación de mensajes (MAC): HMAC-SHA-256.

4.6.1 ACTIVACIÓN Y DESACTIVACIÓN DE SSL

49. Para usar SSL con el inicio de sesión basado en web (acceso HTTP seguro, HTTPS) debe especificar el protocolo HTTPS al configurar la URL de redirección.
    - Para habilitar SSL y permitir el acceso seguro HTTP (HTTPS) en el puerto predeterminado (443), utilizar el siguiente comando:

      enable web https

- Para desactivar SSL y HTTPS, utilizar el siguiente comando:

  disable web https

4.6.2 CREACIÓN DE CERTIFICADOS AUTOFIRMADOS Y CLAVES PRIVADAS

50. Cuando se genera un certificado, éste se almacena en el archivo de configuración y la clave privada en la EEPROM. El certificado generado está en formato PEM. Por defecto, ExtremeXOS utiliza el algoritmo SHA-512 para crear el certificado. El algoritmo hash del certificado se puede configurar usando el comando

    configure ssl certificate hash-algorithm hash-algorithm.

51. ExtremeXOS admite SHA-256, SHA-384 y SHA-512. El algoritmo configurado se utiliza para crear certificados a partir de la próxima vez. Se puede utilizar el comando *show ssl* para comprobar el algoritmo hash de firma configurado actualmente.

52. Para crear un certificado autofirmado y una clave privada que puedan guardarse en la EEPROM, utilice el siguiente comando:

    configure ssl certificate privkeylen length country code organization org_name common-name name

53. Asegúrese de especificar lo siguiente:

    - Código de país (tamaño máximo de 2 caracteres).
    - Nombre de la organización (tamaño máximo de 64 caracteres)
    - Nombre común (tamaño máximo de 64 caracteres)

54. Cualquier certificado y clave privada existente se sobrescribe.

55. El tamaño del certificado depende de la longitud de la clave RSA (*privkeylen*) y de la longitud de los otros parámetros (país, nombre de la organización, etc.) suministrados por el usuario. Para una clave RSA de 4.096, la longitud del certificado es de aproximadamente 2 Kb, y la longitud de la clave privada es de aproximadamente 3 Kb.

4.6.3 DESCARGA DE UNA CLAVE DE CERTIFICADO DESDE UN SERVIDOR TFTP

56. Puede descargar una clave de certificado desde archivos almacenados en un servidor TFTP. Si la operación se realiza correctamente, cualquier certificado existente se sobrescribe. Tras una descarga correcta, el software intenta comparar la clave pública del certificado con la clave privada almacenada. Si las claves pública y privada no coinciden, el switch muestra un mensaje de advertencia.

57. Los certificados y claves descargados no se guardan al reiniciar el *switch,* a menos que guarde la configuración actual del *switch*. Después de utilizar el comando *save*, el certificado descargado se almacena en el archivo de configuración y la clave privada se almacena en la EEPROM.

    - Para descargar una clave de certificado de los archivos almacenados en un servidor TFTP, utilice el siguiente comando:

      download ssl ipaddress certificate {ssl-cert | trusted-ca | ocspsignature-ca | {csr-cert {ocsp [on | off]}} file_name

      NOTA: Por medidas de seguridad, sólo se puede descargar una clave de certificado en el *VR-Mgmt VR*.

- Para ver si la clave privada coincide con la clave pública almacenada en el certificado, utilice el siguiente comando:

  show ssl {detail}

58. Este comando también muestra:
    - Puerto HTTPS configurado. Este es el puerto en el que se conectarán los clientes.
    - Longitud de la clave RSA (el número de bits utilizados para generar la clave privada).
    - Información básica sobre el certificado almacenado.

4.6.4 DESCARGA DE UNA CLAVE PRIVADA DESDE UN SERVIDOR TFTP

59. Por razones de seguridad, al descargar claves privadas, se recomienda obtener una clave pre-generada en lugar de descargar una clave privada de un servidor TFTP.
60. Para descargar una clave privada de archivos almacenados en un servidor TFTP, utilice el siguiente comando:

    download ssl ipaddress privkey key_file

61. Si la operación se realiza correctamente, se sobrescribe la clave privada existente. Cuando la descarga se realiza correctamente se comprueba si la clave privada descargada coincide con la clave pública almacenada en el certificado. Si las claves privada y pública no coinciden, el switch muestra un mensaje de advertencia similar al siguiente:

    Warning: The Private Key does not match with the Public Key in the certificate.

    Nota: Esta advertencia actúa como recordatorio para descargar también el certificado correspondiente.
62. Los certificados y claves descargados no se guardan al reiniciar el *switch* a menos que se guarde la configuración del *switch*. Después de utilizar el comando guardar, el certificado descargado se almacena en el archivo de configuración y la clave privada se almacena en la EEPROM.

4.6.5 CONFIGURACIÓN DE CERTIFICADOS Y CLAVES PREGENERADOS

63. Para obtener el certificado pre-generado del usuario, utilice el siguiente comando:

    configure ssl certificate pregenerated

64. Puede copiar y pegar el certificado en la línea de comandos seguido de una línea en blanco para finalizar el comando.
65. Este comando también se utiliza al descargar o cargar la configuración. No se debe modificar el certificado almacenado en el archivo de configuración cargado porque el certificado está firmado con la clave privada del emisor.
66. El certificado y el archivo de clave privada deben estar en formato PEM y generarse utilizando RSA como algoritmo criptográfico.
67. Para obtener la clave privada pre-generada del usuario, utilice el siguiente comando:

    configure ssl privkey pregenerated

68. Se puede copiar y pegar la clave en la línea de comandos seguida de una línea en blanco para finalizar el comando.

69. Este comando también se utiliza al descargar o cargar la configuración. La clave privada se almacenada en la EEPROM.

70. El certificado y el archivo de clave privada deben estar en formato PEM y generarse utilizando RSA como algoritmo criptográfico.

4.6.6 CREACIÓN DE SOLICITUDES DE FIRMA DE CERTIFICADO Y CLAVES PRIVADAS

71. Secure Socket Layer (SSL) le permite:

    - Generar certificados autofirmados, que generan claves privadas y certificados X509 autofirmados.
    - Descargar la clave privada/certificado SSL utilizando *download ssl ipaddress certificate {sslcert| trusted-ca | ocsp-signature-ca | {csr-cert {ocsp [on | off]}} file_name* (generalmente utilizado para descargar certificados firmados por CA).
    - Puede obtener una clave privada/certificado SSL mediante el comando *configure ssl certificate pregenerated{{csr-cert} pregenerated {ocsp {on | off}}},* generalmente utilizado para obtener el certificado firmado por CA para copiar.

72. Además, puede crear solicitudes de firma de certificado (CSR)/pares de claves privadas. La CSR se puede a una Autoridad de Certificación (CA) para su firma. La CA proporciona entonces el certificado firmado, que puede descargarse en el *switch* utilizando cualquiera de los comandos enumerados anteriormente.

73. Para crear una CSR, utilice el siguiente comando:

    configure ssl csr privkeylen length country code organization org_name common-name

74. Para ver la CSR en cualquier momento después de crearla, utilice el siguiente comando:

    show ssl csr

75. Para mostrar una solicitud de firma de certificado (CSR), utilice el siguiente comando:

    show ssl csr

4.6.7 USO DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI) EN LA RED

76. La implementación de infraestructura de clave pública (PKI) de ExtremeXOS admite la autenticación segura del servidor Syslog y el cliente SSH en un dispositivo XOS de Extreme Networks mediante un certificado X.509. A continuación, se detallan los aspectos principales de una configuración PKI:

    NOTA Todos los certificados mencionados a continuación deben estar en formato PEM.

    - CA de confianza: los certificados X509v3 de la autoridad de certificación (CA) deben descargarse mediante la CLI: *download ssl ipaddress certificate {ssl-cert | trusted-ca | ocspsignature- ca | {csr-cert {ocsp [on | off]}} file_name* utilizando la opción *trusted-ca*. El certificado CA debe satisfacer los siguientes criterios para que se descargue correctamente:
        - Restricciones básicas: CA = *true*
        - El uso de la clave debe contener: *KeyCertSign*

- Peer Certificate-X509v3 certificado del peer, firmado por una de las CA de confianza anteriores. Los siguientes criterios deben cumplirse para una autenticación correcta:
    - Certificado del servidor Syslog: El uso de clave extendida debe contener "Autenticación de servidor
    - Certificado de cliente SSH:
        - Nombre común (CN) del sujeto del certificado debe ser el mismo que el nombre de usuario con el que se prueba la sesión SSH se prueba la sesión.
        - El uso de la clave extendida debe contener "Autenticación de cliente".
- OCSP-Protocolo de estado de certificado en línea utilizado para encontrar el estado de revocación del certificado de pares en el siguiente escenario:
    - El estado OCSP del certificado del servidor Syslog se identifica cuando se va a establecer una sesión TLS con el servidor Syslog. Sólo si el estado OCSP es GOOD se establece la sesión.
    - El estado OCSP del certificado del cliente SSH se identifica como parte de la autenticación. Sólo si el estado OCSP es GOOD se establece la sesión.

  NOTA: OCSP procesa los certificados de CA intermedios de forma iterativa, uno por uno.

  La dirección del servidor OCSP debe estar configurada en el Acceso a la Información de Autoridad (AIA) del certificado homólogo. De lo contrario, falla la autenticación PKI. Los modelos de respondedor OCSP soportados son: modelo de emisor común, modelo de respondedor de confianza delegado, modelo de respondedor de confianza.

- CA de firma OCSP: los certificados de los respondedores OCSP deben configurarse como CA de firma OCSP y CA de confianza. Para admitir el modelo de respondedor de confianza (TRM) de OCSP, el certificado X509v3 del respondedor OCSP debe descargarse mediante la CLI: *download ssl ipaddress certificado {ssl-cert | trusted-ca | ocsp-signature-ca | {csr-cert {ocsp [on | off]}} file_name* utilizando las opciones *ocsp-signature-ca* y *trusted-ca*.

77. La CA de firma OCSP sólo es necesaria para TRM; no se utiliza para DTM y emisor común. Este certificado debe contener una extensión de uso de confianza que permita la firma OCSP. Se puede añadir una "extensión de uso de confianza" a un certificado mediante OpenSSL.

4.6.8 CONFIGURACIÓN DE PKI

78. A continuación, se muestra el flujo de trabajo secuencial implicado en el establecimiento de sesión mediante PKI:

    - Generar los certificados X509v3 correspondientes: Certificados CA, certificado CA de firma OCSP, certificado Peer (por ejemplo: servidor Syslog o cliente SSH), certificado de dispositivo ExtremeXOS.

- Descargar los certificados CA y OCSP Signature CA al dispositivo ExtremeXOS.
- Descargar el certificado y la clave del dispositivo ExtremeXOS al dispositivo ExtremeXOS (necesarios para establecer la sesión TLS con el servidor Syslog).
- Configurar el peer (servidor Syslog o cliente SSH) para que utilice su propio certificado X509v3 en la solicitud de conexión.
- Inicie la solicitud de conexión desde el peer (servidor *Syslog* o cliente SSH) al dispositivo ExtremeXOS.
- El dispositivo ExtremeXOS realiza las siguientes tareas en el certificado del par recibido y acepta/rechaza la solicitud de conexión:
  - Verificación de la cadena de certificados.
  - Comprobación de las extensiones del certificado.
  - OCSP.

4.6.9 LIMITACIONES DE PKI

79. Todos los certificados deben estar en archivos con formato PEM.
80. No se admite la descarga de cadenas de certificados de CA.
81. Los certificados CA individuales de una cadena de certificados deben descargarse uno a uno mediante el siguiente comando:

    download ssl ipaddress certificate {ssl-cert | trusted-ca| ocsp-signature-ca | {csr-cert {ocsp [on | off]}} file_name

82. No se recomienda descargar certificados CA de tamaño superior a 7,5 KB.

- Listas de revocación de certificados (CRL): no compatible.
- No se admite el grapado OCSP.
- *Nonce* siempre está desactivado en la solicitud OCSP.
- OCSP no se realiza para el certificado de respuesta OCSP. Por lo tanto, el certificado de respuesta OCSP debe cumplir alguno de los siguientes criterios, de lo contrario se rechaza la respuesta OCSP:
  - El certificado del OCSP responder debe ser autofirmado, O
  - El certificado OCSP responder debe contener la extensión *id-pkix-ocsp-nocheck.*

4.7 PROTECCIÓN DE LAS SESIONES DE SEGURIDAD DE LA CAPA DE TRANSPORTE DE SYSLOG

83. Por defecto, los siguientes cifrados están habilitados para las sesiones *Syslog Transport Layer Security (TLS):*

    aes128-sha, aes128-sha256; aes256-sha256; dhe-rsa-aes128-sha256; dhe-rsa-aes256-sha256

Nota: la comunicación con Syslog usando TLS con AES_CBC se encuentra protegida con VPN o de forma local. Se establece de este modo una protección física para la comunicación.

84. Puede activar y desactivar selectivamente los cifrados mediante el siguiente comando:

    configure syslog tls cipher [[cipher | all] on | cipher off]

85. Para ver qué cifradores están habilitados o deshabilitados para las sesiones TLS de Syslog, utilice el siguiente comando:

    show log configuration

4.7.1 CÓMO EVITAR LA POSIBLE PÉRDIDA DEL REGISTRO TLS SYSLOG

86. En Linux, por defecto, el *kernel* tarda unos 15 minutos en finalizar una conexión TCP cuando los datos transmitidos permanecen sin confirmar. Esto resulta en una pérdida potencial de registros al servidor TLS Syslog durante la ventana de 15 minutos debido a la caída del enlace.

87. Para reducir esta ventana de tiempo, utilice el siguiente comando:

    configure syslog tls tcp-user-timeout [seconds | default]

88. Para ver el valor establecido para el tiempo de espera de usuario TLS TCP de Syslog, utilice el siguiente comando:

    show log configuration

4.7.2 DESACTIVACIÓN DE OCSP PARA CONEXIONES TLS A SERVIDORES SYSLOG REMOTOS

89. Para cumplir la norma RFC 6960 (Protocolo de estado de certificados en línea de infraestructura de clave pública de Internet X.509 - OCSP), puede desactivar OCSP para las conexiones TLS con servidores Syslog remotos mediante el siguiente comando:

    configure syslog tls ocsp [on | off]

90. Para ver el estado de la comprobación OCSP, utilice el siguiente comando:

    show log configuration

NOTA: Asegúrese de comprender las ramificaciones de desactivar OCSP si decide hacerlo.

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

91. El modo seguro de EXOS sólo funciona en SSH. Para este modo, sólo se permiten cifrados fuertes y códigos de autenticación de mensajes (MAC) en las conexiones de servidor SSH y cliente SSH.

92. Para activar el modo seguro realice los siguientes pasos:

    # configure ssh2 secure-mode on

    Note: All Secure mode Ciphers/MACs will be enabled

93. Para activar o desactivar cifrados y MACs utilice el siguiente comando:

    # configure ssh2 {enable | disable} {cipher | mac} <cipher | mac>

94. Después de activar el modo seguro:

    – Para la comunicación, el servidor SSH utiliza una nueva lista de modo seguro de ciphers y MAC.

    – En el caso del cliente SSH, se notifica a EPEM que cambie el bit dedicado al modo seguro SSH, que oculta las claves y MAC débiles de los comandos del CLI.

5.2 USUARIOS Y CONTRASEÑAS

95. Los switches Summit que usan el sistema operativo EXOS tienen dos (2) niveles de privilegio de acceso diferenciados: "*user*" con permisos de lectura y "*admin*" con permisos de escritura. Cada cuenta de usuario se asigna a uno de estos dos niveles a través del siguiente comando:

    Configure account {all | name} privilege {admin | user}

96. EXOS tiene por defecto dos (2) cuentas de usuario: una cuenta con privilegios "*admin*" llamada "*admin*" y otra con privilegios "*user*" llamada "*user*". Ninguna de ellas tiene contraseña por defecto.

97. Los nombres de todas las cuentas de usuario se pueden ver en texto claro en el fichero de configuración (comando "*show account*") en cambio las contraseñas se muestran siempre encriptadas.

98. Para poder mostrar las cuentas y las contraseñas se utiliza el siguiente comando:

    show account password-policy

5.2.1 NIVEL DE PRIVILEGIO "*USER*"

99. Una cuenta de usuario con nivel de privilegio "*user*" tiene visión (*Read Only)* de todos los parámetros administrables, a excepción de la base de datos de cuentas de usuarios de administración y las comunidades/usuarios SNMP.

100. Un usuario con una cuenta con nivel de privilegios "*user*" puede utilizar el comando ping para chequear conectividad con un equipo y cambiar su propia contraseña. Cuando el usuario accede al *switch* se muestra el *prompt* del CLI como ">".

101. Para más información y ejemplos se recomienda consultar la **[User Guide].**

5.2.2 NIVEL DE PRIVILEGIO "*ADMIN*"

102. Una cuenta de usuario con nivel de privilegio "*admin*" puede consultar y modificar (*Read-Write*) todos los parámetros del *switch*. Con este nivel, se pueden agregar y eliminar usuarios, así como modificar la contraseña de acceso de cualquier cuenta de usuario.

103. Un usuario "*admin*" puede desconectar una sesión iniciada por otro usuario en el *switch*. Si esto sucede, el usuario es notificado de que la sesión ha sido interrumpida.

104. Al acceder al *switch* con privilegios "*admin*", el *prompt* del CLI terminará en #:

SW_EXOS-1.2 #

5.2.3 CONFIGURACIÓN DE CUENTAS POR DEFECTO

105. **Se debe eliminar la cuenta de administrador predeterminada al realizar la configuración inicial del switch**. Será necesario crear previamente una nueva cuenta de administrador ya que el sistema siempre debe tener una. Los pasos son:

- Crear una nueva cuenta de administrador:

  SW_EXOS.9 # create account admin {admin | user | lawful-intercept} account-name {encrypted encrypted_password | password}

  password:

  Reenter password:

- Eliminar la cuenta de administrador predeterminada:

  delete account admin

106. Del mismo modo, **se debe eliminar la cuenta de usuario predeterminada y crear nuevas cuentas de usuario, según sea necesario**. Para ello:

- El comando general para eliminar cuentas es:

  delete account name

- Para crear nuevas cuentas con privilegios de usuario:

  create account user usename password

- Para visualizar la información de las cuentas de usuario:

```
* SW_EXOS.12 # show accounts
    User Name  Access LoginOK  Failed    State
--------------------------------  ------ -------
 administrador    R/W      2      0   Enabled
     manolo       RO       3      0   Enabled
      juan        R/W      1      1   Enabled
```

5.2.4 CUENTA *FAILSAFE*

107. Los switches Summit que usan el sistema operativo EXOS disponen de una cuenta "*failsafe*" o "*a prueba de fallos*" que garantiza el acceso a la gestión del dispositivo en cualquier circunstancia. Esta cuenta no está creada por defecto y tiene privilegios de administración. Los datos de usuario y contraseña de esta cuenta se guardan directamente en la NVRAM, por lo que no aparecen en el fichero de configuración.

108. Se recomienda habilitar esta cuenta para situaciones de emergencia*, password recovery,* etc.

109. Para realizar la configuración de la cuenta *failsafe*:

 # configure failsafe-account
enter failsafe user name: rescue
enter failsafe password:
enter password again:

110. Por defecto, la cuenta *failsafe* sólo tiene permitido el acceso al *switch* por el puerto de Consola. Se recomienda activar también su utilización con SSH.

configure failsafe-account permit ssh

111. Para mostrar los permisos de conectividad de la cuenta failsafe hay que ejecutar el comando:

show failsafe-account

5.2.5 POLÍTICA DE CONTRASEÑAS

112. La complejidad de la contraseña es la mejor medida contra los accesos no autorizados a los recursos de la red. EXOS dispone de varias opciones para mejorar la seguridad en las contraseñas. **Todas están deshabilitadas por defecto, pero deben ser configuradas para disponer de una política de contraseñas robustas.**

5.2.5.1 VALIDACIÓN DE CARACTERES

113. La validación de caracteres requiere que las contraseñas configuradas para las cuentas de acceso al *switch* tengan un mínimo de dos de los siguientes tipos de caracteres:

- Mayúsculas A-Z
- Minúsculas a-z
- 0-9
- !, @, #, $, %, ^, *, (,)

114. La exigencia de caracteres de validación mejora notablemente la seguridad del acceso al switch, haciendo que las credenciales de acceso sean difíciles de vulnerar.

115. Para configurar esta política de contraseñas:

configure account {all | name} password-policy char-validation [all-chargroups]

116. La opción "*all*" configura esta política para todas las cuentas. Se puede aplicar la política únicamente para ciertas cuentas.

117. Habilitar esta funcionalidad obliga a que cualquier contraseña tenga un mínimo de ocho caracteres.

5.2.5.2 TAMAÑO MÍNIMO DE LAS CONTRASEÑAS

118. El tamaño mínimo de una contraseña puede configurarse entre 1 y 32 caracteres. Cuantos más caracteres se utilicen en una contraseña, más difícil será de vulnerar.

configure account [all | <name>] password-policy min-length [num_characters]

119. La opción "*all*" configura esta política para todas las cuentas. Se puede aplicar la política únicamente para ciertas cuentas.

120. **Se recomienda un mínimo de 12 caracteres.**

5.2.5.3 BLOQUEO DE CUENTA POR FALLO EN LAS CREDENCIALES

121. **Se debe habilitar el bloqueo de una cuenta tras un fallo repetido al introducir sus credenciales de acceso**. Por defecto el sistema cierra la sesión tras tres intentos fallidos consecutivos, aunque el usuario no es bloqueado. Habilitando esta función se ayuda a proteger el switch contra un ataque iterativo mediante un generador de contraseñas.

122. El bloqueo de una cuenta se puede realizar de dos (2) formas distintas:

    – "Permanente". Deshabilita el acceso a la cuenta hasta que un usuario administrador vuelve a habilitarla:

      configure account [all | name] password-policy lockout-on-login-failures on

      Desbloquear acceso a una cuenta:

      clear account [all | name] lockout

    – "Temporal". Bloquea el acceso a la cuenta durante un tiempo configurable de entre 1 y 60 minutos.

      configure account [all | <name>] password-policy lockout-time-period <1-60 min>

123. En este caso, también se puede desbloquear la cuenta antes de que pase el tiempo configurado mediante el comando:

      clear account [all | name] lockout

124. La opción "*all*" configura esta política para todas las cuentas. Se puede aplicar la política únicamente para ciertas cuentas.

125. La cuenta "*failsafe*" no permite el uso de esta política de seguridad.

5.2.5.4 TIEMPO DE EXPIRACIÓN DE CONTRASEÑAS

126. Es posible configurar un período máximo de tiempo de validez de una contraseña de acceso al *switch*. El rango de validez puede variar entre 1 y 365 días. Habilitar esta función implica que los usuarios deban cambiar sus contraseñas de forma periódica.

127. Cuando un usuario intenta acceder al *switch* con una cuenta cuya contraseña está expirada el switch solicitará al usuario cambiar la contraseña de acceso.

      configure account [all | <name>] password-policy max-age <num_days>

128. La opción "*all*" configura esta política para todas las cuentas. Se puede aplicar esta política únicamente para ciertas cuentas.

5.2.5.5 HISTORIAL DE CONTRASEÑAS

129. El historial de contraseñas impide que un usuario utilice para su cuenta contraseñas ya empleadas anteriormente. Se puede configurar un histórico de entre 1 y 10 contraseñas. Utilizando este histórico se impide que un usuario alterne entre las mismas dos contraseñas cada vez que se le exige un cambio, haciendo más difícil para alguien no autorizado obtener una contraseña válida.

configure account [all | <name>] password-policy history <num_passwords>

130. La opción "*all*" configura esta política para todas las cuentas. Se puede aplicar la política únicamente para ciertas cuentas.

131. **Se recomienda un historial de al menos cinco contraseñas.**

5.2.6 AAA (AUTENTICACIÓN, AUTORIZACIÓN Y ACCOUNTING)

132. El sistema de gestión de cuentas local de EXOS (visto en los apartados anteriores) soporta muchas de las características de acceso requeridas en un entorno seguro.

133. Sin embargo, algunos entornos requieren funcionalidades adicionales que no pueden ser implementadas gestionando cuentas localmente en cada switch (bloqueo de cuentas por inactividad, gestión de cuentas basada en grupos, autorización por comando, administración y *accounting* centralizados, etc).

134. Aunque EXOS permite utilizar servidores de Autenticación, Autorización y *Accounting* (AAA) como RADIUS y TACACs+ para la autenticación centralizada de usuarios. Se recomienda la autenticación local, y en solo en caso de ser necesario se usará la autenticación en remoto por canales seguros y confiables de acuerdo a las siguientes secciones.

135. Estos servidores normalmente están enlazados con un Directorio Activo (LDAP) que es donde se guardan las credenciales de los usuarios.

Nota: No es posible utilizar RADIUS y TACACS+ a la vez para autenticar los accesos al switch.

5.2.6.1 RADIUS

136. *Remote Authentication Dial In User Service (RADIUS),* es un protocolo para la autenticación centralizada del acceso a los equipos de red. Extreme Networks recomienda que en cada switch se configure un servidor RADIUS primario y otro de backup.

137. Cuando un usuario intenta acceder a la administración del switch mediante SSH, HTTPS o CLI, las credenciales de acceso se reenvían hacia el servidor RADIUS principal y, si este no responde, al secundario. Si no hay respuesta de ninguno de ellos el switch utilizará su base de datos local de usuarios para realizar la autenticación.

138. En este apartado se verá cómo emplear un servidor RADIUS para autenticar el acceso a la gestión del switch. Los privilegios asignados al usuario en el servidor RADIUS son prioritarios frente a los configurados en la base de datos local del switch.

139. Cuando se configura un switch con autenticación RADIUS es recomendable limitar el número de cuentas locales. Idealmente sólo deberían existir una cuenta principal de administrador y la cuenta de failsafe.

140. Para configurar el servidor RADIUS hay que utilizar este comando:

configure radius mgmt-access primary server <ip_server> 1812 client-ip <ip_switch> vr vr-default

141. Para configurar el servidor RADIUS primario habrá que usar "primary". En caso del secundario, "secondary".

142. El campo "client-ip" indica la dirección IP del switch desde donde se enviarán los paquetes al servidor RADIUS.

143. Además de especificar la dirección IP del servidor RADIUS, éste debe ser confiable. Para verificar la comunicación entre el switch y el servidor se utiliza una clave compartida llamada “shared secred”.

configure radius mgmt-access [primary | secondary] shared-secret <string>

144. La clave será introducida en texto plano, aunque en el fichero de configuración aparecerá cifrada.

145. Para configurar un tiempo máximo de espera tras la petición de autenticación al servidor RADIUS (si este no responde) se puede configurar un timeout (Por defecto son 3 segundos):

configure radius mgmt-access timeout <seconds>

146. Si este período expira, se enviará otra petición de autenticación. Tras tres intentos fallidos (esto también es configurable), se consultará al servidor RADIUS secundario. Si este tampoco responde (tras un total por defecto de seis intentos), la petición se intentará autenticar contra la base de datos de usuarios local del switch.

147. Para habilitar/deshabilitar la funcionalidad RADIUS hay que usar los comandos:

enable radius mgmt-access

disable radius mgmt-access

148. Para ver las propiedades de RADIUS configuradas en el switch:

show radius

5.2.6.1.1 AUTORIZACIÓN DE LA EJECUCIÓN DE COMANDOS RADIUS

149. Es posible controlar qué comandos CLI puede ejecutar un usuario y cuales no empleando RADIUS. Para ello, es necesario que el servidor RADIUS envíe al switch los atributos VSA (Vendor Specific) Extreme-CLI-Authorization y Extreme-Security-Profile. Una vez los reciba, el switch consultará al servidor RADIUS antes de ejecutar cada comando.

150. A continuación, se incluye un ejemplo de usuario con autorización de comandos (FreeRADIUS):

Manolo *User-Password == “M@nol0”*
Service-Type = Administrative-Use
Extreme-CLI-Authorization = Enabled
Extreme-Security-Profile = Support_Profile

5.2.6.1.2 RADIUS ACCOUNTING

151. Los switches Summit que usan el sistema operativo EXOS pueden enviar al servidor RADIUS información de la actividad de los usuarios (*accounting*). Como con el caso de la autenticación, también es posible especificar dos servidores para el envío de esta información.

152. Para configurar los servidores de RADIUS accounting:

configure radius-accounting mgmt-access [primary | secondary] server <ipaddress> 1813 client-ip <ipaddress> vr vr-default

153. RADIUS accounting también utiliza una contraseña o clave compartida como mecanismo de validación de la comunicación entre el switch y los servidores.

configure radius-accounting mgmt-access [primary | secondary] sharedsecret <string>

154. Para habilitar o deshabilitar globalmente esta funcionalidad hay que ejecutar los comandos:

enable radius-accounting mgmt-access

disable radius-accounting mgmt-access

5.2.6.2 TACACS+

155. *Terminal Access Controller Access Control System Plus (TACACS+)* es un mecanismo alternativo a RADIUS para proporcionar Autenticación, Autorización y Accounting (AAA) desde un sistema centralizado.

156. Para configurar un servidor TACACS+ en EXOS:

configure tacacs [primary | secondary] server <ipaddress> 49 client-ip <ipaddress> vr vr-default

157. Al igual que en RADIUS, se recomienda el uso de dos (2) servidores: primario y secundario.

158. Para poder realizar consultas al servidor TACACS+, es necesario configurar también una clave secreta compartida:

configure tacacs [primary | secondary] shared-secret <string>

159. La clave se introduce en texto plano, aunque en el fichero de configuración aparecerá cifrada.

160. Para habilitar o deshabilitar globalmente TACACS+ hay que ejecutar los comandos:

enable tacacs

disble tacacs

161. Para ver las propiedades de TACACS+ configuradas en el switch:

show tacacs

5.2.6.2.1 AUTORIZACIÓN DE LA EJECUCIÓN DE COMANDOS CON TACACS+

162. Al igual que en RADIUS, es posible configurar en el servidor TACACS+ perfiles de ejecución de comandos y asociarlos a los usuarios del switch.

163. Para que el switch consulte al servidor TACACS+ si un usuario tiene permiso para ejecutar un comando es necesario configurar lo siguiente:

enable tacacs-authorization

5.2.6.2.2 TACACS+ ACCOUNTING

164. Al igual que en RADIUS, los *switches* Summit que usan el sistema operativo EXOS son capaces de enviar información de *accounting* a un servidor TACACS+.

configure tacacs-accounting [primary | secondary] server <ipaddress> 49 client-ip <ipaddress> vr vr-default

165. TACACS+ Accounting también utiliza una contraseña o clave compartida como mecanismo de validación de la comunicación entre el switch y los servidores.

configure tacacs-accounting [primary | secondary] shared-secret <string>

166. Para habilitar o deshabilitar globalmente TACACS+ hay que ejecutar los comandos:

enable tacacs-accounting

disable tacacs-accounting

5.3 BANNER O MENSAJE INFORMATIVO

167. **Se recomienda configurar un mensaje de aviso o advertencia de acceso al switch**. EXOS permite mostrar un aviso antes (*before-login*) o después (*after-login*) de solicitar las credenciales de acceso:

configure banner before-login

configure banner after-login

168. Al pulsar "*Enter*" se redacta el mensaje que se desee. Por ejemplo:

SW_EXOS1.7 # configure banner before-login

El uso de este dispositivo está restringido a los usuarios expresamente autorizados. Todos los accesos son monitorizados.

169. Para terminar de escribir el mensaje simplemente hay que pulsar dos veces "*Enter*".

170. El mensaje podrá contener un tamaño máximo de 24 filas con 79 columnas de texto

5.4 SNMP (*SIMPLE NETWORK MANAGEMENT PROTOCOL*)

171. Cualquier gestor de red (NMS) que utilice el protocolo SNMP puede administrar un switch EXOS siempre que disponga de las MIBs (*Management Information Base*) necesarias.

172. Extreme Management Center (XMC) es el gestor de red de Extreme Networks.

173. EXOS soporta concurrentemente SNMPv1/v2c y SNMPv3. Por defecto el acceso SNMP está deshabilitado en todas sus versiones.

174. SNMPv3 es la evolución del standard SNMP que mejora la seguridad y privacidad del acceso a los equipos gestionados y provee un control más sofisticado de acceso a las MIBs. **Se debe, por tanto, configurar SNMPv3 y no utilizar versiones anteriores.**

175. En SNMPv3 se utiliza el modelo de seguridad basada en usuarios (USM). USM trata todos los aspectos relacionados con la seguridad como la autenticación y encriptación de los mensajes SNMP y la definición de los usuarios y sus niveles de acceso. Este estándar también se encarga de la protección contra el retardo y la repetición de los mensajes y emplea los conceptos de usuario, grupo, modelo de seguridad y nivel de seguridad.

5.4.1 GRUPOS *SNMPV3*

176. Cada usuario SNMPv3 pertenece a un grupo. Los grupos definen el modelo de seguridad, el nivel de seguridad y la porción de la MIB que sus miembros pueden leer o escribir.

177. Para proporcionar compatibilidad entre versiones, SNMPv3 soporta tres (3) modelos de seguridad o "*sec-model*":

- snmpv1: Seguridad basada en comunidades.
- snmpv2c: Seguridad basada en comunidades.
- usm: Seguridad basada en usuarios.

178. En esta guía se utilizará el modelo usm.

179. Existen tres (3) niveles de seguridad "*sec-level*" soportados por el modelo USM:
    - noAuthnoPriv: Sin autenticación ni cifrado.
    - AuthnoPriv: Con autenticación y sin cifrado.
    - AuthPriv: Con autenticación y cifrado.
180. Por defecto hay definidas tres (3) vistas o porciones de la MIB que los miembros de un grupo podrán leer o escribir:
    - defaultUserView (Acceso Parcial. Hay zonas de la MIB excluidas)
    - defaultAdminView (Acceso total a la MIB)
    - defaultNotifyView (Cualquier parte de la MIB puede enviar notificaciones).
181. Para crear un grupo se utiliza el siguiente comando:

    SW_EXOS.2 # configure snmpv3 add access grupo1 sec-model usm sec-level priv write-view "defaultAdminView"

    SW_EXOS.3 # configure snmpv3 add access grupo2 sec-model usm sec-level priv read-view "defaultUserView"
182. Existen siete grupos de usuarios definidos por defecto:
    - admin (sec model usm, sec level priv)
    - initial (sec model usm, sec level noauth)
    - initial (sec model usm, sec level authnopriv)
    - v1v2c_ro (sec model snmpv1, sec level noauth)
    - v1v2c_ro (sec model snmpv2c, sec level noauth)
    - v1v2c_rw (sec model snmpv1, sec level noauth)
    - v1v2c_rw (sec model snmpv2c, sec level noauth)
183. Para mostrar información sobre la configuración de acceso de un grupo o de todos los grupos hay que utilizar el siguiente comando:

    show snmpv3 access <group_name>
184. Para eliminar un grupo hay que utilizar el siguiente comando:

    configure snmpv3 delete access <group_name>
185. Para más información y ejemplos se recomienda consultar la ***[User Guide].***

5.4.2 USUARIOS SNMPV3

186. Los usuarios SNMPv3 pueden utilizar autenticación y cifrado (opcional).
187. Para crear un usuario hay que utilizar el siguiente comando:

    SW_EXOS.18 # configure snmpv3 add user snmpuser authentication md5 snmpauthcred privacy des snmpprivcred
188. Por defecto en EXOS no hay creados usuarios SNMPv3. Sin embargo, están creados los usuarios v1v2c_ro y v1v2c_rw para acceso SNMPv1 y SNMPv2c

189. Para mostrar información sobre un usuario o todos los usuarios se utiliza el siguiente comando:

show snmpv3 user <user_name>

190. Para eliminar un usuario hay que usar el siguiente comando:

configure snmpv3 delete user <user_name>

191. Para más información y ejemplos se recomienda consultar la ***[User Guide].***

5.4.3 ASOCIACIÓN DE UN USUARIO A UN GRUPO SNMPV3

192. Para asociar un usuario a un grupo hay que utilizar el siguiente comando:

configure snmpv3 add group <group_name> user <user_name>

193. Para consultar los usuarios asociados a un grupo:

** SW_EXOS.9 # show snmpv3 group grupo1*
Group Name : grupo1
Security Name : usuario1
Security Model : USM
Storage Type : NonVolatile
Row Status : Active

194. Eliminar un usuario de un grupo:

configure snmpv3 delete group <group_name> user <user_name>

195. Para más información y ejemplos se recomienda consultar la ***[User Guide].***

5.5 ACTIVACIÓN DE SNMPV3

196. SNMP está desactivado por defecto en todas sus versiones. **Se debe activar sólo SNMPv3:**

enable snmp access snmpv3

197. Para más información y ejemplos se recomienda consultar la ***[User Guide].***

5.6 SERVICIOS DE ACCESO A LA GESTIÓN DEL *SWITCH*

198. **Limitar al puerto de consola el acceso a la gestión de un *switch* es la medida más efectiva para la securización de su gestión**. Lamentablemente este método no es nada práctico en las redes actuales. El acceso a la gestión del equipo se puede realizar sobre la red operacional (en banda) o bien mediante una red fuera de banda (fuera de banda).

199. **Los protocolos Telnet y HTTP son considerados inseguros puesto que la información viaja en claro por la red, por lo que deben ser deshabilitados**:

disable telnet
disable web http

200. Los switches Summit que usan el sistema operativo EXOS implementan varios servicios seguros y recomendados para la gestión remota del dispositivo como SSH y HTTPS.

201. Para visualizar la configuración de acceso a la gestión del switch hay que utilizar el comando:

show management

5.6.1 SSH

202. Para permitir la gestión del switch mediante SSH es necesario activarlo previamente:

**SW_EXOS # enable ssh2*
WARNING: Generating new server host key
This could take approximately 15 minutes and cannot be canceled. Continue? (y/N) Yes
Key Generated
Save the config to retain the key after reboot of the switch or restart of the process.

203. Se recomienda utilizar un perfil de acceso o "*Access-profile*" para restringir las conexiones a determinadas direcciones IPs (por ejemplo, a los equipos de administración de red).

204. Se puede aplicar un "access-profile" a cada protocolo de gestión remota.

205. Para permitir el acceso mediante SSH únicamente a las IPs de la red 192.168.0.0/24, denegando el acceso al resto:

configure ssh2 access-profile <policy_filename.pol>

Fichero policy: "allow192.pol"

```
configure ssh2 access-profile allow192.pol
entry allow192 {
   if {
            source-address 192.168.0.0/24;
   }
   then
   {
      permit;
   }
}
entry denyall {
   if {
   }
   then{
      deny;
   }
}
```

5.6.1.1 SCP (SECURE COPY)

206. SCP (*Secure Copy*) es un método seguro de transferencia de ficheros que utiliza SSH para la transferencia de datos y que incluye opciones de autenticación y encriptación disponibles en SSH. A diferencia de TFTP, SCP maneja el intercambio de información y de credenciales de usuario de forma segura.

207. EXOS únicamente permite SCP2 para la trasferencia de archivos de configuración (*.cfg) y ficheros de políticas (*.pol).

208. Si se quiere copiar desde un servidor Linux el fichero de configuración primary.cfg del switch 192.168.0.120, al que se accede con usuario "admin":

[user@linux-server]# scp2 admin@192.168.0.120:/config/primary.cfg primary.cfg

209. Para copiar un fichero de políticas “test.pol” desde el servidor Linux al switch:

[user@linux-server]# scp2 test.pol admin@192.168.0.120:/config/test.pol

5.6.2 HTTPS

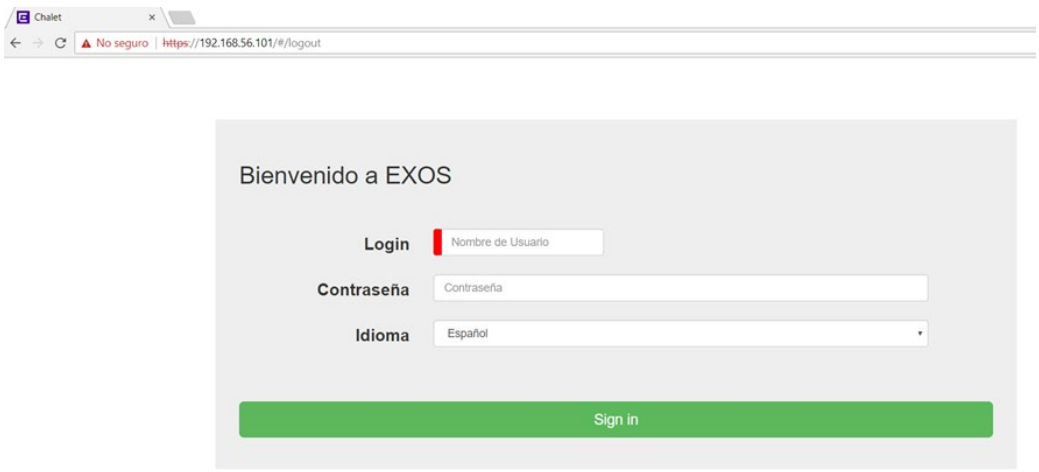
210. Los *switches* Summit que usan el sistema operativo EXOS disponen de una interfaz Web para la administración básica y la visualización de información del *switch*.

211. Para la utilización del servicio Web seguro (HTTPS) es necesario generar previamente un certificado SSL. EXOS permite generar un certificado SSL auto-firmado para la encriptación de los datos de la sesión.

configure ssl certificate privkeylen <lenght> country <code> organization <organizacion> *common-name <nombre>*

212. Una vez generado el certificado es posible habilitar la gestión HTTPS del switch:

enable web https



213. La administración de un switch mediante Web está fuera del alcance de esta guía. Para más información, consultar la documentación disponible en www.extremenetworks.com

214. Al igual que en SSH, también es posible aplicar un perfil de acceso o “*access-profile*” al servicio de gestión HTTPS:

configure web http access-profile add <ACL>

215. Para más información y ejemplos se recomienda consultar la ***[User Guide].***

5.7 ICMP

216. Para realizar comprobaciones de conectividad es posible utilizar herramientas basadas en ICMP como PING y *Traceroute*. Muchos de los ataques maliciosos utilizan ICMP como herramienta de reconocimiento de la red.

217. En EXOS no existe el concepto de “*Access-profile*” para el tráfico ICMP, por lo que es recomendable la utilización de una ACL para su filtrado. Esta ACL puede ser aplicada tanto a puertos específicos como a una Vlan.

5.8 MECANISMOS DE CONTROL DE BUCLES

218. EXOS ofrece diversos mecanismos de prevención de bucles de nivel 2 (ELRP, EAPS, ERPS, Redundant Port, etc). El utilizar uno u otro dependerá de las particularidades y necesidades de cada red. El mecanismo más comúnmente empleado es STP (*Spanning Tree Protocol*).

5.8.1 STP: SPANNING TREE PROTOCOL

219. EXOS tiene habilitado por defecto STP en su modo MSTP (*Multiple Spanning Tree Protocol* 802.1s). La instancia STP por defecto se llama "s0".

220. Es recomendable configurar el envío de traps SNMP al gestor de red ante un cambio de topología de STP, así como cuando se elige un nuevo Root bridge:

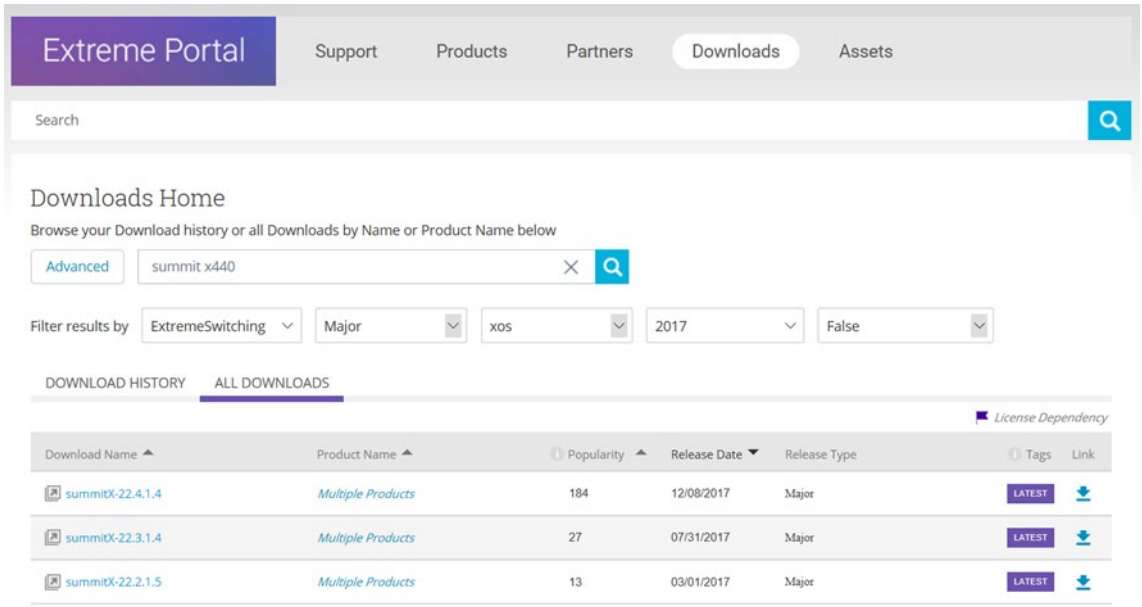
configure stpd s0 trap topology-change on

configure stpd s0 trap new-root on

5.8.2 OBTENCIÓN DE NUEVAS VERSIONES DE *FIRMWARE*

221. Extreme Networks pone a disposición de los usuarios de su equipamiento las actualizaciones de versiones de *firmware* a través del portal: https://extremeportal.force.com

222. En la sección "*Downloads*" se encuentran las imágenes del sistema operativo.



223. Es imprescindible leer la documentación de una versión antes de proceder al cambio de firmware: https://www.extremenetworks.com/support/release-notes

5.8.3 ACTUALIZACIÓN DEL *FIRMWARE*

224. Se recomienda seguir los siguientes pasos para instalar una nueva versión de *firmware* en un *switch*.

- Descargar la imagen en un servidor TFTP.

- Verificar conectividad entre el *switch* y el servidor TFTP.

  ping 172.16.0.199

- Guardar un fichero de configuración de *backup* en el propio *switch*, para tenerlo disponible en caso de ser necesaria una vuelta atrás.

  save configuration {primary | secondary | existing-config | new-config}

- Como medida adicional se recomienda salvar también la configuración en un servidor TFTP externo:

  tftp put 172.16.0.199 vr vr-default local_file {remote_filename} Los switches Summit que usan el sistema operativo EXOS disponen de dos (2) particiones en la memoria flash para guardar las imágenes de firmware: Primary y Secondary. El switch puede arrancar de cualquiera de ellas.

225. Se puede utilizar el comando "*show switch*" para ver el contenido de ambas particiones. La imagen "*Selected*" indica qué imagen se utilizará tras el siguiente reinicio del *switch*. La imagen "*Booted*" indica la imagen que se utilizó en el último reinicio del *switch*, es decir, la versión actual del SO.

    SW_EXOS # show switch
    …
    Image Selected: secondary
    Image Booted: secondary
    Primary ver: 21.1.1.4
    Secondary ver: 22.3.1.4
    patch1-8

226. La nueva imagen descargada en el *switch* se instalará por defecto en la partición que no está siendo utilizada (la no "*Selected*").

    download image 172.16.0.199 summitX-22.3.1.4.xos vr "VR-Default"

227. Para poner en marcha el nuevo *firmware* es necesario ejecutar el comando "*reboot*".

228. En caso de ocurrir algún problema durante la actualización del *firmware* se recuperará el sistema utilizando la partición no original.

5.8.3.1 COMPROBACIÓN DE LA INTEGRIDAD DE LA IMAGEN DE EXTREMEXOS

229. Si la función de comprobación de integridad de la imagen de ExtremeXOS está activada, durante el arranque, el sistema comprueba la integridad de la imagen de ExtremeXOS y notifica si ha sido comprometida o no (el error se notifica en el *Syslog*).

230. Para activar o desactivar la función de comprobación de integridad de la imagen de ExtremeXOS, utilice el siguiente comando:

    configure switch integridad-comprobar imagen [on | off]

231. Para ver el estado y la configuración de la función de comprobación de integridad de la imagen de ExtremeXOS, use el siguiente comando:

    show switch management

232. Este comando muestra uno de los siguientes valores:

- *On (Valid):* la función está activada y la comprobación se ha realizado correctamente.
- *On (Not Checked):* la función está activada, pero la imagen no se ha comprobado. Esto ocurre inmediatamente después de activar la función, pero antes de reiniciar, lo que iniciará la comprobación de integridad.
- *On (Invalid):* la función está activada y la comprobación ha fallado. La imagen de ExtremeXOS está dañada.
- *On (Failed):* la función está activada y la comprobación de integridad no se ha podido ejecutar debido a un fallo.
- *Off:* la función está desactivada.

5.9 SISTEMA DE GESTIÓN DE EVENTOS (EMS)/*LOGGING*

233. En EXOS se utiliza el término "evento" para nombrar cualquier situación del *switch* que pueda generar un mensaje de log o requerir una acción determinada.

234. Se consideran eventos de seguridad la pérdida de conectividad en un enlace, una autenticación correcta o incorrecta de un usuario, un comando ejecutado en la línea de comandos o la ejecución de un comando de *debugging*. Todos estos eventos pueden generar un mensaje de log.

235. Un evento en EXOS está compuesto por:

- Un componente (conjunto de eventos relacionados). Familia de eventos
- Un subcomponente (no siempre existe, es opcional). Subfamilia
- Una condición (disparador del evento)
- Un nivel de severidad (es fijo, no se puede modificar)
- Un mensaje de log

236. De esta forma, un evento se puede definir como:

- *Componente.Subcomponente.Condición* (el subcomponente no siempre existe).
- *Componente.Condición*
- *Componente.Subcomponente*

237. Para ver todos los componentes de los logs de EXOS se puede usar uno de estos dos comandos:

show log components

o

show log events all.

238. Cada evento tiene asociado un nivel de severidad por defecto que no es posible modificar. Los niveles de Severidad son los siguientes:

- *Critical (C)*
- *Error (E)*

- *Warning (W)*
- *Notice (N)*
- *Info (I)*
- *Debug-Summary (S)*
- *Debug-Verbose (V)*
- *Debug-Data (D)*

239. Los mensajes con alguna de las severidades de *debug* no se generarán a menos que se habilite el modo *debug* con el comando "*enable log debug-mode*". Por defecto, EXOS sólo genera eventos con severidades desde Info a Critical.

240. Es posible obtener un listado de todos los eventos de EXOS, así como los detalles de un evento en concreto:

```
SW-EXOS.40 # show log events all
Component   SubComponent Condition           Severity     Parameters
----------- ------------ ---------------------- ------------- ----------
AAA             accountLockedOut      Warning      1 Total
AAA             accountMod            Info         3 Total
AAA             authFail              Warning      2 Total
AAA             authPass              Info         2 Total
AAA             changePass            Info         2 Total
AAA             ChgAccntPrvlgFail     Notice       2 Total
AAA             ChgAccntPrvlgOK       Notice       2 Total
…
…
SW-EXOS.40 # show log events "FDB.MACTracking.MACMove" detail
Component   SubComponent Condition           Severity     Parameters
----------- ------------ ---------------------- ------------- ----------
FDB         MACTracking  MACMove              Notice       4 Total
                                                          0 - mac-address
                                                          1 - vlan
                                                          2 - ports
                                                          3 - ports
The MAC address %0% on VLAN "%1%" has moved from port %2% to port %3%
```

241. El subsistema que se encarga de mostrar, filtrar y guardar los eventos se llama EMS (*Event Management System*). EMS permite múltiples opciones sobre cómo generar mensajes de log, dónde mandarlos y con qué formato mostrarlos.

242. Es posible enviar los logs a los siguientes destinos:

- Consola: El envío de logs a la consola está deshabilitado por defecto. Se recomienda dejarlo así, y habilitarlo únicamente en caso de necesidad. Para habilitarlos:

```
enable log target console
```

- Sesión CLI activa: Telnet o SSH. Deshabilitado por defecto. Para habilitarlo utilizar el siguiente comando.

  enable log target session

243. También se puede modificar el nivel de severidad de los logs enviados. Por defecto es "Info".

     configure log target session severity <severidad>

     Nota: Este comando no se guarda en la configuración. Los logs se muestran únicamente en la sesión actual.

244. El buffer de memoria puede contener desde 200 hasta 20.000 mensajes de log. Por defecto está habilitado y almacena 1000 mensajes. Es un buffer circular, es decir, cuando llega al máximo de su capacidad comienza a sobrescribir, perdiéndose los mensajes de log más antiguos. Todos los mensajes de log se envían a este buffer de memoria sin importar su nivel de severidad. Los mensajes no se eliminan al reiniciarse el equipo. Los mensajes de log guardados en el buffer de memoria se muestran utilizando el comando:

     show log

245. O bien:

     show log messages memory-buffer

246. Para ver la configuración de *logging* en el buffer de memoria:

     show log configuration target memory-buffer

247. Es posible modificar la severidad de envío de logs al buffer:

     configure log target memory-buffer severity <severity>

248. Para modificar el número de mensajes de log en el buffer se puede utilizar este comando: (máximo 20.000)

     configure log target memory-buffer number-of-messages <num_mensajes>

249. NVRAM: Los mensajes de log enviados a este target también permanecen después de un reinicio del switch. Por defecto está habilitado y a él se sólo se envían los mensajes con severidad Warning, Error y Critical. Para ver los mensajes enviados a la NVRAM hay que utilizar el siguiente comando:

     show log messages nvram

250. Servidor Syslog externo: El almacenamiento de los eventos producidos es un factor clave a la hora de identificar una amenaza de seguridad. Los switches no están diseñados para realizar un tratamiento extenso de logs ya que disponen de una capacidad de memoria limitada, por lo que **se deben enviar a un servidor Syslog externo**. Se recomienda utilizar *Extreme Management Center (XMC)* como servidor de Syslog. Para configurar el envío de mensajes a un servidor Syslog externo hay que emplear los siguientes comandos:

     configure syslog <ipaddress> vr vr-default local0

     enable syslog

251. Es recomendable configurar el siguiente formato de los mensajes de log para su envío al XMC:

     configure log target syslog <IP Address> format timestamp seconds date mm/dd/yyyy event-name condition host-name tag-id tag-name

252. Para más información y ejemplos se recomienda consultar la ***[User Guide].***

5.9.1 FILTRADO DE EVENTOS ENVIADOS A RECEPTORES DE LOGS

253. No todos los mensajes son enviados a todos los receptores de log habilitados. Cada receptor o Target recibirá únicamente los mensajes para los que haya sido configurado.

254. Para especificar los mensajes de log a enviar a un receptor es posible configurar un nivel de severidad, un filtro, y una expresión de condición (match), que determinarán si el mensaje se envía o no. Además, es posible configurar el formato del mensaje a enviar.

255. Todos los receptores de logs tienen asociado por defecto un filtro llamado "*defaultFilter*", que sólo deja pasar los mensajes con una severidad igual o superior a la de la familia/componente del evento.

256. Para la familia de eventos "FDB" la severidad por defecto es "error". Si se quiere que el evento "*FDB.MACTracking.MACMove*", con severidad "notify" pase el filtro y sea enviada a un receptor hay que utilizar el siguiente comando:

```
configure log filter DefaultFilter add events FDB.MACTracking.MACMove
SW-EXOS.92 # show log configuration filter "DefaultFilter"
Log Filter Name: DefaultFilter
I/                                  Severity
E Component   SubComponent Condition           CEWNISVD
- ----------- ------------ ---------------------- --------
I FDB         MACTracking  MACMove              ---N----
I All                                  ********
```

257. Para ver la configuración de envío de *logs* hacia un receptor hay que utilizar el siguiente comando:

```
show log configuration target {console | memory-buffer | nvram | session | syslog }
```

258. Para más información y ejemplos se recomienda consultar la ***[User Guide].***

5.9.2 SERVICIO DE TIEMPO/HORA

259. Un factor importante a la hora de interpretar mensajes de log es conocer el momento en el que se ha producido un evento. **Se debe, por tanto, configurar el reloj interno del switch de forma manual (no recomendable) o mediante SNTP.**

   – Reloj local: Para configurar el reloj de manera local hay que utilizar el siguiente comando:

   ```
   configure time <mes> <día> <año> <hora> <minuto> <segundo>
   ```

   – SNTP: Para hacer consultas a un servidor SNTP y sincronizar el reloj interno del switch hay que utilizar los siguientes comandos:

   ```
   configure sntp-client primary <IP_NTP_server> vr "VR-Default"
   enable sntp-client
   ```

260. Es posible configurar un servidor SNTP de *backup* utilizando el argumento "*secondary*" en el comando anterior:

```
configure sntp-client secondary <IP_NTP_server_2> vr "VR-Default"
```

261. Tanto si se ha configurado SNTP o la hora local, es recomendable configurar la zona horaria del switch y el cambio de horario de verano:

configure timezone name CET 60 autodst name CEST 60 begins every last sunday march at 2 0 ends every last sunday october at 3 0

262. El comando "*show switch*" muestra la hora actual de dispositivo.

263. Para ver la configuración relacionada con la sincronización de reloj:

show configuration nettools

show configuration devmgr

5.9.3 CONFIGURACIÓN MÍNIMA RECOMENDADA PARA ENVÍO DE LOGS

264. La configuración mínima recomendada para el tratamiento de logs en los switches Summit que usan el sistema operativo EXOS es la siguiente:

- Habilitar el envío de logs a un servidor Syslog externo y dar el formato apropiado a los mensajes para el gestor XMC:

configure syslog <ipaddress> vr vr-default local0

enable syslog

configure log target syslog <ipaddress> vr VR-Default local0 format timestamp seconds date mm/dd/yyyy event-name condition host-name tag-id tag-name

- El logging a Consola está desactivado por defecto. No se debe modificar.
- Modificar el tamaño del buffer interno para que pueda contener más mensajes:

configure log target memory-buffer number-of-messages 20000

265. Se debe habilitar el registro de los cambios de configuración realizados sobre el *switch* (cada comando ejecutado en el CLI genera un mensaje de log):

enable cli-config-logging

266. Configurar el servicio de SNTP para sincronizar la hora:

configure sntp-client primary <IP_NTP_server> vr "VR-Default"

configure sntp-client secondary <IP_NTP_server_2> vr "VR-Default"

enable sntp-client

configure timezone name CET 60 autodst name CEST 60 begins every last sunday march at 2 0 ends every last sunday october at 3 0

5.10 PROTECCIÓN ANTE ATAQUES DoS

267. Se considera que está sucediendo un ataque de denegación de servicio (DoS) cuando ciertos recursos de computación o de red se sobrecargan de forma maliciosa impidiendo la prestación del servicio.

268. En su forma más simple, un ataque DoS no se puede distinguir de una gran cantidad de tráfico legítimo. Hay algunas operaciones en un switch que son más costosas que otras a efectos de CPU y, aunque el tráfico normal no es un problema ya que es conmutado en hardware, cierto tráfico especial debe ser enviado a la CPU del switch para su proceso.

269. Algunos de los paquetes que el switch procesa en CPU son:

- Tráfico proveniente de una nueva dirección MAC

- Protocolos de *routing* y control, incluidos ICMP, BGP, OSPF, STP, EAPS, ESRP, etc.
- Tráfico de gestión del *switch* como Telnet, SSH, SNMP, etc.

270. Si una de estas funciones se sobrecarga, la CPU puede llegar a estar muy ocupada para atender otras funciones y el rendimiento del switch se verá mermado. Incluso si se dispone de CPUs muy rápidas es posible llegar a sobrecargarlas con paquetes que requieran procesado software.
271. La funcionalidad de Protección DoS está diseñada para ayudar a prevenir la degradación del rendimiento intentando caracterizar el problema y filtrar el tráfico malicioso.
272. Cuando llega al switch una gran cantidad de paquetes destinados a la CPU, la protección DoS cuenta esos paquetes y hace lo siguiente:
273. Si el contador de paquetes se aproxima a un umbral de alerta, se guardan las cabeceras de los paquetes.
274. Si se alcanza el umbral de alerta las cabeceras son analizadas y a partir de esta información se crea una ACL hardware para limitar el flujo de esos paquetes hacia la CPU. Esta ACL permanecerá aplicada hasta que se libere la CPU.
275. **Nota**: Las ACLs creadas por el administrador tienen mayor prioridad que las ACLs aplicadas automáticamente para la protección DoS.
276. Durante un ataque, cuando se alcanza el umbral de alerta, la protección DoS generará una notificación (log).
277. **Se debe habilitar la funcionalidad de protección DoS,** para ello se debe utilizar el siguiente comando:

    enable dos-protect

278. Es posible configurar distintos parámetros de esta funcionalidad, aunque se recomienda comenzar con los parámetros por defecto.
279. Algunos puertos se pueden considerar como confiables, por lo que la protección DoS no aplicará sobre el tráfico entrante por estos puertos.

    configure dos-protect trusted-ports ports <port>

280. Para visualizar la información relativa a la protección DoS:

    show dos-protect

281. El modo simulado es útil para identificar y configurar los umbrales de tráfico normal en el switch. **Se recomienda comenzar la implantación de la protección DoS siempre en modo simulado.**
282. Para más información y ejemplos se recomienda consultar la ***[User Guide].***

5.11 PROTECCIÓN DE LA RED

283. Los puertos de conmutación de un switch pueden realizar diferentes funciones. Una primera clasificación suele distinguir entre puertos de acceso y puertos troncales:
    - **Puerto de acceso**: Destinado a la conexión de un usuario final como un PC. En estos puertos el tráfico suele ser untagged (una única VLAN)

- **Puerto troncal:** Puerto de conexión con otro switch o nodo de red por el que pasa el tráfico de varias VLANs. En este tipo de puertos se recomienda enviar todas las VLANs de usuario en modo tagged.

284. En los siguientes apartados se describirán las medidas de seguridad que se pueden aplicar a los puertos. Cuando sea necesario se hará la distinción entre puerto de acceso y troncal.

5.11.1 DESACTIVAR LOS PUERTOS NO UTILIZADOS.

285. Los puertos físicos están habilitados administrativamente por defecto. Se debe evitar la utilización de manera no autorizada de puertos, por lo que **se deben deshabilitar administrativamente aquellos puertos que no vayan a ser utilizados.**

286. Para activar o desactivar uno o más puertos de un switch hay que utilizar los siguientes comandos:

enable port [port_list | all]

disable port [port_list | all]

5.11.2 ELIMINAR LA VLAN *DEFAULT* EN TODOS LOS PUERTOS

287. Por defecto todos los puertos físicos en un switch EXOS están asignados a la VLAN "Default" (VLAN id=1) y están habilitados para conmutar tráfico. Es una configuración apropiada para el despliegue rápido de un switch, pero no es la mejor opción desde el punto de vista de la seguridad.

288. En términos generales de seguridad es recomendable que los puertos no utilizados no estén asignados a ninguna VLAN:

configure vlan Default delete ports all

5.11.3 PRIVATE VLANS

289. En EXOS una *Private VLAN (PVLAN)* está compuesta por los siguientes elementos:

- Una "*Network VLAN*", asignada al puerto promiscuo.
- Una o varias "*Subscriber Isolated VLAN*", las cuales tienen asociados los puertos aislados, que únicamente pueden comunicarse con el puerto promiscuo.
- Una o varias "*subscriber Non-Isolated VLAN*", cuyos puertos pueden comunicarse entre ellos y con el puerto promiscuo.

290. Para crear PVLANs es necesario llevar a cabo estos pasos:

- Crear una PVLAN.

  create private-vlan name {vr vr_name}

- Añadir una VLAN a la PVLAN como Network VLAN.

  configure private-vlan name add network vlan_name

- Añadir VLANS a las PVLAN como subscriber VLAN.

  configure private-vlan name add subscriber vlan_name {non-isolated} {loopback-port port}

291. Para más información y ejemplos se recomienda consultar la **[User Guide].**

5.11.4 SPANNING TREE PROTOCOL

292. La configuración de STP en cada puerto dependerá del tipo de puerto y su función en la red.

293. **Puertos de acceso**. La detección y prevención de bucles en un puerto de acceso configurado con STP se conoce en EXOS como *edge safeguard*. *Edge safeguard* permite prevenir bucles resultantes de la conexión entre dos puertos de acceso (de forma directa o mediante un hub). Un puerto configurado con *edge safeguard* entra inmediatamente en estado de *Forwarding*, pero sigue transmitiendo BPDUs. Si se detecta un bucle el puerto será bloqueado. Por otro lado, **es recomendable habilitar en los puertos de acceso la funcionalidad "*bpdu-restrict*"**, que deshabilita el puerto en cuanto se recibe una BPDU. De esta forma se evita la conexión incontrolada de otros switches STP.

configure stpd s0 port link-type edge <port> edge-safeguard enable bpdu-restrict

294. **Puertos troncales**. En los puertos troncales es necesario el intercambio normal de BPDUs para el mantenimiento de una red libre de bucles. En ciertas redes, algunos puertos troncales se conectan a equipos que no se consideran "fiables", por lo que la red se expone a notificaciones de STP que podrían comprometer su estabilidad. En estos casos es posible configurar restricciones a la recepción de mensajes STP TCN (Cambios de topología) y STP Root (cambios en la elección del Root Bridge)

configure stpd s0 ports restricted-tcn on <ports>

/ Impide que el switch procese tramas BPDUs TCN */*

configure stpd s0 ports restricted-role enable <port>

/ Impide que un puerto pueda ser Root Port */*

5.11.5 PROTOCOLOS DE DESCUBRIMIENTO DE RED

295. EXOS soporta diferentes protocolos de descubrimiento Layer 2 como EDP (*Extreme Discovery Protocol*), el estándar LLPD (802.1ab *Link Layer Discovery Protocol*) y CDP (*Cisco Discovery Protocol*).

296. La utilización de protocolos de descubrimiento implica el intercambio no seguro de información sensible (modelo y versión de *firmware*, por ejemplo) entre los equipos de la red, por lo que deben utilizarse con precaución. A tener en cuenta:

- EDP (*Extreme Discovery Protocol*): Está habilitado por defecto en todos los puertos. Se recomienda deshabilitarlo en los puertos de acceso.

  disable edp ports <ports>

- LLPD (*Link Layer Discovery Protocol*): Está habilitado por defecto en todos los puertos. Se recomienda deshabilitarlo en los puertos de acceso.

  disable lldp ports <ports>

- CDP (*Cisco Discovery Protocol*): Está deshabilitado por defecto. Activar sólo en caso necesario (puertos con teléfonos IP Cisco que no soporten LLDP, por ejemplo)

  enable cdp ports <ports>

5.11.6 NODEALIAS E IDENTITY MANAGER

297. En un *switch* funcionando a nivel 2 lo habitual es que la única información de los usuarios de la que se dispone sea la dirección MAC. *Nodealias* e *Identity Manager* son funcionalidades que permiten obtener mucha más información de los usuarios conectados

al *switch*, como su dirección IP, los protocolos que utilizan, el nombre de usuario Windows, etc

298. La configuración en un puerto de *nodealias* y la visualización de información puede realizarse a través de los siguientes comandos.

```
enable nodealias port 10
configure nodealias port 10 maxentries 20
show configuration nodealias
show nodealias
show nodealias protocol ip
show nodealias port 10
```

299. Identity Manager funciona de manera similar a Nodealias, pero usa *Kerberos Snooping* para capturar el nombre de los usuarios Windows que se autentican con un controlador de dominio.

300. La configuración de Identity Manager y la visualización de información puede realizarse a través de los siguientes comandos.

```
enable identity-management
configure identity-management kerberos snooping add server <DC>
configure identity-management add ports 10
show identity-management
show identity-management entries port 10
```

301. Identity Manager suele requerir que la VLAN a la que pertenece el puerto en el que se activa tenga definido una interfaz IP (SVI).

302. Para más información y ejemplos se recomienda consultar la ***[User Guide].***

5.11.7 MAC LOCKING

303. Por defecto un puerto aprende cualquier dirección MAC que se le conecte. La funcionalidad de *MAC Loc*king ayuda a prevenir el acceso no autorizado a la red limitando las direcciones MAC que un puerto puede aprender.

304. Un ataque de MAC Spoofing puede llenar la tabla de direcciones MAC del switch. Cuando esto ocurre el switch empieza a hacer flooding del tráfico entrante. Por esto es tan importante **activar *MAC Locking*.**

305. Hay dos (2) configuraciones posibles de MAC Locking:

- *MAC Locking First Arrival*: El puerto aprende las N primeras direcciones MAC (con N configurable). Las MACs siguientes ya no tendrán acceso a la red.
- Bloqueo estático de MACs: El puerto sólo permite la conexión de una o varias MAC predefinidas mediante configuración. Cualquier otra MAC no tiene acceso a la red.

306. Esta funcionalidad evita que un usuario mal intencionado genere tramas Ethernet con diferentes direcciones MAC origen o que conecte un Hub. También puede evitar la conexión de usuarios desconocidos.

307. Es posible convertir en estáticas las N direcciones MAC aprendidas de forma dinámica en un puerto mediante el siguiente comando:

```
configure mac-locking ports <port> first-arrival move-to-static
```

308. Este comando guarda en la configuración las direcciones MACs como estáticas (son preservadas tras un reinicio). Permite evitar tener que introducir manualmente las direcciones MAC confiables en cada puerto.

309. Para deshabilitar la funcionalidad MAC Locking de forma global hay que ejecutar el siguiente comando:

disable mac-locking

310. Para más información y ejemplos se recomienda consultar la ***[User Guide].***

5.11.8 MAC TRACKING

311. La funcionalidad de *MAC Tracking* permite detectar cuando una dirección MAC se mueve de un puerto a otro sin que en el puerto inicial haya pérdida de link. Esta situación puede indicar la existencia de un bucle.

312. MAC Tracking se habilita por puerto:

configure fdb mac-tracking add ports <port>

313. *MAC Tracking* genera un evento (log) que por defecto no pasa por el "Default Filter" del EMS. Es necesario añadir este evento al filtro para que sea visible.

configure log filter DefaultFilter add events FDB.MACTracking.MACMove

314. Para más información y ejemplos se recomienda consultar la ***[User Guide].***

5.11.9 LINK FLAPPING

315. Es posible configurar el envío de una notificación si un puerto está oscilando entre estados *Up/Down.*

316. Para más información y ejemplos se recomienda consultar la ***[User Guide].***

5.11.10 FLOOD CONTROL

317. Flood Control limita la aceptación de tramas Ethernet que se replican en salida a todos los puertos: *broadcast* y multicast con dirección MAC destino desconocida. Cuando se supera el umbral de entrada configurado en un puerto (paquetes por segundo) el tráfico es descartado y se envía una notificación.

318. Para mejorar los niveles de seguridad, se recomienda configurar *Flood Rate-Limit*:

configure ports <ports> rate-limit flood broadcast <pps> out-actions log trap

configure ports <ports> rate-limit flood multicast <pps> out-actions log trap

configure ports <ports> rate-limit flood unknown-destmac <pps> out-actions log trap

319. Para ver las estadísticas de *Flood Control*:

show ports <port_list> rate-limit flood

5.11.11 LISTAS DE CONTROL DE ACCESO (ACLS)

320. Las listas de control de acceso o ACLs son una de las herramientas principales para mejorar la seguridad en una red de datos. Controlan el flujo del tráfico permitiendo o denegando paquetes en función de una o varias condiciones. EXOS dispone de dos tipos de ACLs: Estáticas y Dinámicas.

321. Sobre un puerto pueden ser aplicadas al mismo tiempo ambos tipos de ACLs. En este caso las ACLs dinámicas tienen siempre preferencia.

5.11.11.1.1 ACLS ESTÁTICAS

322. Este tipo de ACL (o políticas en terminología EXOS) se definen en un fichero de texto con extensión ".pol" que se crea en la memoria flash del *switch*. Este fichero se puede crear directamente en el *switch* utilizando el editor "vi" o puede crearse en otro lugar (un PC, por ejemplo) y descargarse al *switch* mediante TFTP.

323. El fichero ".pol" puede contener varias reglas. Cada regla tiene condiciones de match, acciones y modificadores (if … then …).

324. Algunas condiciones de match:

ethernet-source-address
ethernet-destination-address
source-address
destination-address
source-port
destination-port
protocol
tcp-flags

325. Si hay varias condiciones se pueden utilizar los operadores lógicos "all" (AND, se efectúa la acción si cumplen todas las condiciones) o "any "(OR, se efectúa la acción si cumple una de las condiciones).

326. En una ACL, las condiciones pueden analizar parámetros de nivel 2, 3 y 4 del modelo OSI.

327. Algunas de las posibles acciones:

permit
deny
deny-cpu
copy-cpu-off
copy-cpu-and-drop
add-vlan-id
replace-dscp-value
do-ipfix
do-not-ipfix

328. Además de las acciones es posible utilizar modificadores.

329. Para consultar la lista completa de condiciones, acciones y modificadores disponibles para la creación de una ACL se pueden ejecutar los siguientes comandos:

```
check policy attribute
        /* Muestra todos los atributos */
check policy attribute ethernet-source-address
        /* Un atributo en concreto */
```

Nota: En EXOS las ACLs tienen al final una regla "permit" implícita, por lo que el tráfico que no haga match contra ninguna condición definidas será permitido.

330. Una vez creado el fichero de políticas o ACLs con extensión ".pol", es recomendable realizar un chequeo de la sintaxis mediante el comando:

```
SW_EXOS # check policy test
Policy file check successful
```

331. El fichero de ACL se lee únicamente cuando se aplica. Si se modifica con posterioridad es necesario indicar al switch que lo lea de nuevo para que tenga efecto:

```
SW_EXOS# refresh policy test
Policy test refresh done!
Para aplicar/borrar una ACL en un puerto:
configure access-list <name> ports 1 ingress|egress
unconfigure access-list port 1 ingress|egress
/* <name> es el nombre del fichero.pol sin la extension */
```

332. Para aplicar/borrar una ACL en una Vlan:

```
configure access-list <name> vlan "XYZ" ingress|egress
unconfigure access-list vlan "XYZ" ingress|egress
```

333. La configuración de ACLs en el switch puede obtenerse con el comando:

```
show configuration acl
```

334. Para más información y ejemplos se recomienda consultar la ***[User Guide].***

5.11.11.1.2 ACLS DINÁMICAS

335. Las ACLs dinámicas se crean desde el CLI. Utilizan una sintaxis muy similar a las estáticas (ficheros .pol) y pueden realizar las mismas acciones. Sin embargo, el modo de match de las condiciones es siempre ALL (no existe la opción ANY).

336. Cada ACL dinámica es una condición (con su acción y modificadores) en sí misma. Lo normal será aplicar varias ACLs dinámicas (varias condiciones) a un puerto o VLAN. Por defecto, las ACLs dinámicas se evalúan siguiendo el orden en el que se configuran.

337. Creación de una ACL Dinámica:

```
create access-list <acl_name> "condition_1; condition_2" "action"
```

338. ACL estática equivalente:

```
entry  icmp-echo {
   if{
      protocol  icmp;
      icmp-type echo-request;
   } then {
      deny;
   }
}
```

339. De hecho, es posible visualizar una ACL dinámica en formato estático (fichero.pol):

```
* SW-EXOS.18 # show access-list dynamic rule "icmp-echo"
entry icmp-echo {
if match all {
   protocol icmp ;
   icmp-type echo-request ;
} then {
   deny  ;
   }
}
```

340. Las ACL dinámicas se guardan en la configuración al ejecutar un "*save*" (se hacen permanentes). Si no se quieren guardar es necesario añadirles el parámetro *"non-permanent"*. De esta forma, tras un reinicio del *switch* son eliminadas.

341. Asignación de una ACL dinámica a un puerto: Se pueden aplicar varias ACLs al mismo puerto eligiendo el orden de las mismas.

```
configure access-list add rule1 first ports 3
configure access-list add rule2 after rule1 port 3
```

342. Además, es posible aplicar la ACL distinguiendo entre el tráfico entrante o saliente del puerto:

```
configure access-list add rule1 first ports 2 egress
 /* Aplica la ACL al tráfico saliente */
configure access-list add rule1 first ports 4 ingress
 /* Aplica la ACL al tráfico entrante */
```

343. Es posible consultar el valor de los contadores de las ACLs dinámicas mediante el siguiente comando:

```
* SW-EXOS.38 # show access-list dynamic counter
 Vlan Name       Port   Direction
   Counter Name              Packet Count       Byte Count
================================================================
 *           3     ingress
   kkk                    0              0
   ppp                    0              0
* SW-EXOS.39 # show access-list dynamic counter egress
 Vlan Name       Port   Direction
   Counter Name              Packet Count       Byte Count
================================================================
 *           2     egress
   kkk                    0              0
```

344. Para eliminar una ACL de un puerto hay que utilizar el siguiente comando:

```
configure access-list delete rule1 ports 3
```

345. Al igual que las ACLs estáticas, las ACLs dinámicas pueden ser aplicadas a una VLAN.

346. Para más información y ejemplos se recomienda consultar la ***[User Guide].***

5.12 *CLEAR-FLOW*

347. La funcionalidad *Clear-Flow* permite monitorizar el tráfico de entrada al *switch* para buscar anomalías. Utiliza para ello una extensión de las listas de acceso estáticas (ACL en fichero.pol).

348. Las reglas *Clear-Flow* se añaden al fichero de ACL para analizar y contar los paquetes de interés. El agente *Clear-Flow* monitoriza los contadores definidos y analiza su variación en un intervalo de muestreo o en una relación entre dos contadores. Por ejemplo, es posible monitorizar la proporción entre los paquetes *TCP SYN* y *TCP no SYN* entrantes. Una proporción anormalmente grande podría indicar un ataque *SYN Flood*.

349. Al igual que en las ACLs, si se cumple la condición de una regla *Clear-Flow* se pueden ejecutar determinadas acciones (bloqueo del puerto de entrada, aplicación de *QoS*, *mirror* a un *sniffer*, ejecución de un comando CLI, envío de un trap SNMP o mensaje de log EMS).

350. **Se debe habilitar la funcionalidad *Clear-Flow***. Para ello:

```
enable clear-flow
disable clear-flow
```

351. La sintaxis para la creación de reglas *Clear-Flow* es similar a la de las ACLs estáticas.

```
entry <CLFrulename> {    if <match-type> { <match-conditions>;    }
        then {           <actions>;
        } else {         <actions>;
        }
}
```

352. Es posible utilizar variables del sistema para la creación de reglas *Clear-Flow*. Algunas de ellas son:

$policyName	*Nombre de la politica.*
$ruleName	*Nombre de la regla CLEAR-Flow.*
$<counterName>	*Valor del contador que aparece en el nombre del parámetro.*
$ruleValue	*Valor actual de la regla.*
$ruleThreshold	*Umbral definido en la regla.*
$ruleInterval	*Intervalo de muestreo / evaluación de la regla.*
$vlanName	*Nombre de una VLAN.*
$port	*Puerto.*

353. Existen varias formas de analizar la evolución de los contadores *Clear-Flow*. Es posible utilizar más de uno a la vez:

- *Count*: contador > umbral
- *Delta*: (contador_ahora – contador_antes) > umbral.
- *Ratio*: (contador_ahora – contador_antes)/(tiempo_ahora – tiempo_antes) > umbral
- *Delta-Ratio*: combinación de las expresiones Delta y Ratio.
- *Rule-True-Count*: compara cuantas veces una regla es cierta con un valor umbral.

354. Para más información y ejemplos se recomienda consultar la **[User Guide].**

5.13 *ONE POLICY*

355. *One Policy* es la migración a EXOS del concepto de Política de *Enterasys*. Estas políticas permiten ser definidas de forma gráfica en un lugar centralizado (Extreme Management Center o XMC) y ser desplegadas en todos los *switches* de la red de forma sencilla. No es necesario acceder a todos los *switches* por el CLI para definir sus Políticas.

356. Por lo tanto, se debe activar estas políticas mediante el comando:

enable policy

357. La configuración de políticas puede obtenerse con el comando:

show configuration policy

Nota: En caso de conflicto, una Política Dinámica siempre tiene prioridad frente a una Estática.

5.14 IP SECURITY

358. IP Security es un conjunto de funcionalidades adicionales de seguridad de EXOS que se describen a continuación. Para ver la configuración de IP Security hay que utilizar el siguiente comando:

show configuration ip-security

5.14.1 *DHCP SNOOPING*

359. DHCP es un mecanismo de envío automático de información IP a un host en una red. Esta información incluye dirección IP, máscara de red, *default gateway*, servidores DNS y algunos atributos extras. La naturaleza abierta y automática del protocolo lo hace vulnerable ante el intento de hosts no autorizados a interferir en el proceso y asignar información incorrecta a los hosts legales que la solicitan en la red.

360. *DHCP Snooping* mejora la seguridad filtrando los mensajes DHCP no confiables y manteniendo una tabla de *bindings DHCP* por cada Vlan.

361. Es necesario definir los servidores DHCP conocidos, puesto que únicamente se confiará en el tráfico DHCP entre esos servidores y la red. En caso de recibir tráfico no confiable los paquetes DHCP son descartados.

362. *DHCP Snooping* esta deshabilitado por defecto en EXOS.

363. Para habilitar la funcionalidad:

enable ip-security dhcp-snooping vlan <vlan_name> ports <access_ports> violation-action drop-packet

364. Definición de los servidores DHCP confiables para cada Vlan:

configure trusted-server vlan <vlan> add server <dhcp_server> trust-for-dhcp-server

365. Visualización de la tabla de *bindings* construida por *DCHP snooping* para cada VLAN:

show ip-security dhcp-snooping entries vlan <vlan>

show ip-security dhcp-snooping vlan <vlan>

366. Para más información y ejemplos se recomienda consultar la ***[User Guide].***

5.14.2 *SOURCE IP LOCKDOWN*

367. Esta funcionalidad obliga a que en un puerto con *DHCP Snooping* habilitado el switch sólo admita el tráfico que provenga de una dirección IP asignada mediante DHCP.

368. Con *Source IP Lockdown* habilitado los hosts que tienen una dirección IP asignada por servidores DHCP confiables pueden acceder a la red. En cambio, el tráfico de otros hosts con dirección IP estática es descartado por el switch.

369. Esta funcionalidad de "*bloqueo de IP origen*" está ligada a *DHCP Snooping*. La misma tabla de *bindings* de *DHCP Snooping* se utiliza para crear ACLs dinámicas que sólo permiten el tráfico a los clientes seguros. Cualquier otro tráfico es descartado.

370. *Source IP Lockdown* se habilita por puerto, lo que implica que se aplica a todas las Vlans a las que el puerto pertenezca. Por tanto, **se recomienda utilizarlo sólo en los puertos de acceso de usuarios.**

371. Para más información y ejemplos se recomienda consultar la ***[User Guide].***

5.14.3 *ARP LEARNING / DHCP SECURED ARP*

372. *Address Resolution Protocol (ARP)* es el mecanismo de la suite TCP/IP que asocia dinámicamente la dirección física de un dispositivo (MAC) con su dirección lógica (IP).

373. El *switch* mantiene una tabla de ARP, también conocida como ARP Cache, donde se guarda cada dirección MAC y su correspondiente dirección IP. Por defecto, el *switch* construye su tabla de ARP a partir del seguimiento de las peticiones y respuestas ARP de los hosts. A este proceso se le llama *ARP Learning*.

374. Es posible deshabilitar el *ARP Learning*. De esta manera las únicas entradas en la tabla ARP del *switch* serán las añadidas de forma manual o las creadas a partir de "*DHCP Secured ARP"*, evitando la duplicidad de direcciones IP.

375. *DHCP Secured ARP* hace que las entradas de la tabla ARP del *switch* sean añadidas o eliminadas únicamente cuando un servidor DHCP asigna o reasigna una dirección IP a una estación. No analiza los mensajes *ARP Requests/Reply* de los equipos (ARP Learning).

376. Para deshabilitar el aprendizaje ARP en uno o más puertos de una *Vlan*:

    disable ip-security arp learning learn-from-arp {vlan} vlan_name ports [all | ports]

377. Para añadir una entrada permanente de forma manual a la tabla de ARP del switch:

    configure iparp add <ip_addr> vr vr-default <MAC_addr>

    Nota: Si se habilita *DHCP Secured ARP* en el switch sin deshabilitar previamente el aprendizaje de ARP se seguirán aprendiendo direcciones MACs y añadiendo entradas inseguras a la tabla de ARP.

378. Para habilitar *DHCP Secured ARP* hay que utilizar el siguiente comando:

    enable ip-security arp learning learn-from-dhcp {vlan} vlan_name ports [all | ports]

379. Para visualizar como el switch crea la tabla de ARP y de donde aprende las direcciones MAC:

    show ip-security arp learning {vlan} vlan_name

380. Para visualizar la tabla de ARP, incluyendo tanto las entradas permanentes como las estradas DHCP Secure ARP hay que utilizar el comando:

    show iparp

381. Para más información y ejemplos se recomienda consultar la ***[User Guide].***

5.14.4 ATAQUES ARP (GRATUITOUS ARP)

382. Cuando un *host* envía una solicitud ARP para resolver su propia dirección IP se denomina "*Gratuitous ARP*". Una petición *Gratuitous ARP* contiene los siguientes parámetros:

- Dirección MAC de Destino: Broadcast (FF:FF:FF:FF:FF:FF)
- Dirección MAC de Origen: Dirección MAC del emisor de la solicitud
- Dirección IP de Origen = Dirección IP destino: Dirección IP a resolver.

383. En un funcionamiento normal se utilizan *Gratuitous ARP* para:

- Detectar direcciones IP duplicadas.
- Anunciar que una dirección IP se ha movido o asociado a una nueva tarjeta de red (NIC).
- Notificar a un *switch* que un host se ha movido de un puerto a otro.

384. Sin embargo, un host también puede lanzar un ataque *man-in-the-middle* enviando por ejemplo solicitudes *Gratuitous ARP* hacia la dirección IP del *router*. Esto provoca que el resto de hosts de la red envíen el tráfico enrutado hacia al atacante y el atacante reenvíe esos datos al router, lo que permite interceptar contraseñas, claves y otra información. Este tipo de ataque basados en *Gratuitous ARP* también es conocido como *ARP Cache Poisoning*.

385. Si se habilitan las funcionalidades *DHCP Secure ARP* y *Gratuitous ARP* el switch protegerá su propia dirección IP de gestión y las direcciones IP de los hosts que aparecen en la tabla de ARP (añadidas como entradas seguras mediante *Secure ARP*).

386. La configuración de la funcionalidad de *Gratuitous ARP* se hace por Vlan. La validación se hace para todos los paquetes *Gratuitous ARP* recibidos en la Vlan sobre la que se habilita, independientemente del puerto por el que se reciben los paquetes.

387. Por lo tanto, se debe habilitar la protección ante ataques basados en *Gratuitous ARP* mediante el siguiente comando:

enable ip-security arp gratuitous-protection vlan <vlan_name>

388. **Nota**: La protección ante ataques *Gratuitous ARP* necesita las funcionalidades *de DHCP Snooping* y *DHCP Secured ARP*.

389. Para visualizar la información sobre este tipo de protección hay que utilizar el siguiente comando:

show ip-security arp gratuitous-protection

5.14.5 VALIDACIÓN DE ARP

390. La validación de ARP también es una función ligada a *DHCP Snooping*. La misma tabla de *bindings DHCP* creada al habilitar DHCP Snooping se utiliza para validar el tráfico ARP entre estaciones. En caso de que no pase la validación el tráfico es descartado**. Se debe habilitar esta funcionalidad.**

391. Para habilitar la validación de ARP en una Vlan hay que utilizar el comando:

enable ip-security arp validation vlan <vlan_name> ports all violation-action drop-packet

392. Para visualizar la información sobre la validación de ARP hay que emplear el comando:

show ip-security arp validation vlan vlan_name

6. FASE DE OPERACIÓN

393. 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. **Mantener actualizado el *firmware/software* es la clave para mantener seguro un sistema**. Según se van descubriendo nuevas vulnerabilidades, Extreme Networks hace las modificaciones necesarias en las nuevas versiones del Sistema Operativo EXOS. La información relativa a estos cambios se describe en la documentación que acompaña a cada nueva versión de código (*Release Notes*). La actualización implica el reemplazo del *firmware* en producción y a veces también del *bootrom* o sistema de arranque del equipo. La actualización requiere por regla general un reinicio del sistema, lo cual provocará un estado de "*off-line*" o desconexión del *switch*.
- 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			
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 de puertos	☐	☐	
CONFIGURACIÓN			
SERVIDORES DE AUTENTICACIÓN (si procede)			
Configuración del servidor RADIUS	☐	☐	
Configuración del servidor TACAS+	☐	☐	
ADMINISTRACIÓN DEL PRODUCTO			
Creación de usuarios y roles	☐	☐	
Creación de la política de contraseñas	☐	☐	
Configuración de bloqueo de cuentas	☐	☐	
Configuración del mensaje de acceso al sistema	☐	☐	
Creación de la ACL de gestión	☐	☐	
Configuración de las restricciones MAC	☐	☐	
CONFIGURACIÓN DE PROTOCOLOS SEGUROS			
Configuración de los parámetros de SSH	☐	☐	
Configuración de los parámetros de TLS	☐	☐	
Configuración de los parámetros de SNMPv3	☐	☐	
GESTIÓN DE CERTIFICADOS			
Creación de los certificados para SSH	☐	☐	
Creación de los certificados para HTTPS	☐	☐	

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

8. REFERENCIAS

[User Guide] ExtremeXOS® User Guide for Version 31.5 9037159-00 Rev AB January 2022

9. ABREVIATURAS

AAA	*Autentication, Autorization and Accounting*
ACL	*Access Control List*
AES	*Advanced Encryption Standard*
ARP	*Address Resolution Protocol*
BGP	*Border Gateway Protocol*
BPDUs	*Bridge Protocol Data Units*
CCN	*Centro Criptológico Nacional*
CDP	*Cisco Discovery Protocol*
CLI	*Command Line Interface*
CN	*Common Name*
CSR	*Certificate Signing Request*
DHCP	*Dinamic Host Configuration Protocol*
DNS	*Domain Name Server*
DOS	*Denial of Service*
EAPS	*Ethernet Automatic Protection Switching*
EDP	*Extreme Discovery Protocol*
EMS	*Event Management System*
ENS	*Esquema Nacional de Seguridad*
ESRP	*Extreme Standby Routing Protocol*
EXOS	*Extreme X Operative System*
HMAC	*Hash-based Message Authentication Code*
HTTPS	*Hyper Text Transfer Protocol Secure*
ICMP	*Internet Control Message Protocol*
IP	*Internet Protocol*
LLPD	*Link Layer Discovery Protocol*
MAC	*Media Access Control*
MIB	*Management Information Base*
NTP	*Network Time Protocol*
NVRAM	*Non-volatile random access memory*
OCSP	*Online Certificate Status Protocol*
OSPF	*Open Shortest Path First*

PGP	*Pretty Good Privacy*
RADIUS	*Remote Authentication Dial-In User Service*
RBAC	*Role-Based Access Control*
SAN	*Subject Alternative Name*
SCP	*Secure Copy Protocol*
SHA	*Secure Hash Algorithm*
SNMP	*Simple Network Management Protocol*
SNTP	*Simple Network Time Protocol*
SSH	*Secure Shell*
STP	*Spanning Tree Protocol*
TACACS	*Terminal Access Controller Access Control System*
TCP	*Transmission Control Protocol*
TFTP	*Trivial file transfer Protocol*
TLS	*Transport Layer Security*
TTY	*TeleTypewriter*
UPS	*Uninterruptible Power Supply*
USB	*Universal Serial Bus*
USM	*User-based Security Model*
VLAN	*Virtual Local Area Network*
XMC	*Extreme Management Center*

PUBLICACIONES DE DEFENSA

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