

Guía de Seguridad de las TIC CCN-STIC 1635

Procedimiento de empleo seguro *A10 Thunder*



Marzo de 2024





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

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2024

NIPO: 083-24-120-3.

Fecha de Edición: marzo 2024.

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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

ÍNDICE.....	2
1. INTRODUCCIÓN	4
2. OBJETO Y ALCANCE	5
3. ORGANIZACIÓN DEL DOCUMENTO	7
4. FASE PREVIA A LA INSTALACIÓN.....	8
4.1 ENTREGA SEGURA DEL PRODUCTO	8
4.2 ENTORNO DE INSTALACIÓN SEGURO	8
4.3 REGISTRO Y LICENCIAS	9
4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN.....	10
5. FASE DE INSTALACIÓN.....	12
5.1 ENTREGA DE <i>SOFTWARE</i> Y VERIFICACIÓN DE VERSIÓN	12
6. FASE DE CONFIGURACIÓN.....	13
6.1 MODO DE OPERACIÓN SEGURO	13
6.1.1 SOPORTE SSL/TLS EN MODO FIPS	13
6.1.2 IPSEC EN MODO FIPS.....	13
6.1.3 OTROS ASPECTOS A TENER EN CUENTA DEL MODO FIPS.....	14
6.1.4 CONFIGURACIÓN INICIAL A TRAVÉS DE LA CONSOLA LOCAL	14
6.1.5 CONEXIÓN INICIAL Y CONFIRMACIÓN DEL MODO FIPS.....	15
6.1.6 CONFIGURACIÓN DE PARÁMETROS BÁSICOS DEL SISTEMA.....	15
6.1.7 ESTABLECER UN TÚNEL IPSEC PARA CONEXIONES EN EL ENTORNO OPERATIVO	16
6.1.8 HABILITAR EL ACCESO A LA ADMINISTRACIÓN <i>SSH</i> REMOTA.....	18
6.2 AUTENTICACIÓN.....	18
6.3 ADMINISTRACIÓN DEL PRODUCTO.....	18
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA.....	18
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES	21
6.3.3 TERMINACIÓN DE LA SESIÓN	24
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS.....	25
6.4.1 CONFIGURACIÓN DE LA INTERFAZ DE ADMINISTRACIÓN	25
6.4.2 MANTENER LAS INTERFACES DE ADMINISTRACIÓN Y DE DATOS EN REDES SEPARADAS	26
6.4.3 OPCIONES DE ENRUTAMIENTO DE ADMINISTRACIÓN	26
6.5 GESTIÓN DE CERTIFICADOS.....	27
6.5.1 GENERAR CLAVE PRIVADA Y SOLICITUD DE FIRMA DE CERTIFICADO.....	27
6.5.2 GENERAR CERTIFICADOS FIRMADOS POR LA CA	28
6.5.3 IMPORTAR CERTIFICADOS FIRMADOS	28
6.5.4 IMPORTAR CERTIFICADOS DE CA RAÍZ.....	29
6.6 SERVIDORES DE AUTENTICACIÓN	29
6.6.1 CONFIGURACIÓN DE AUTENTICACIÓN, AUTORIZACIÓN Y CONTABILIDAD (AAA) PARA ACCESO DE ADMINISTRADOR	29
6.6.2 INTEGRACIÓN CON MFA	30
6.7 SINCRONIZACIÓN	30

6.7.1 CONFIGURACIÓN HORARIA DEL SISTEMA Y DE LA RED	30
6.8 ACTUALIZACIONES	31
6.9 AUTO-CHEQUEOS.....	31
6.10 ALTA DISPONIBILIDAD	32
6.11 AUDITORÍA	33
6.11.1 REGISTRO DE EVENTOS	33
6.11.2 ALMACENAMIENTO LOCAL	33
6.11.3 ALMACENAMIENTO REMOTO	34
6.11.4 ENTRADAS DE REGISTRO DE AUDITORÍA	35
6.12 BACKUP	35
6.12.1 DESCRIPCIÓN GENERAL DE LA COPIA DE SEGURIDAD DEL SISTEMA.....	36
6.12.2 USO DE LA GUI PARA REALIZAR UNA COPIA DE SEGURIDAD.....	36
6.12.3 RESTAURAR DESDE UNA COPIA DE SEGURIDAD	37
7. REFERENCIAS	39
8. ABREVIATURAS.....	41

1. INTRODUCCIÓN

1. Este documento ofrece una guía para configurar y utilizar de forma segura los dispositivos **A10 Thunder y vThunder Series Appliances** que ejecutan el sistema operativo ACOS versión 5.2.1-P3 de A10.
2. **Estos dispositivos han sido cualificados en categoría ALTA e incluidos en el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC), en la familia ‘Balanceadores de Carga’.** Se recomienda consultar el CPSTIC para conocer los modelos y versión cualificada en cada momento.

2. OBJETO Y ALCANCE

3. En la tabla a continuación se lista el *hardware* y el *software* del grupo de productos a los que aplica este procedimiento de empleo seguro:

MODELO	DESCRIPCION
TH-4435 A10 Networks Thunder	TH-4435 appliance (Plataforma hardware)
TH-5840-11 A10 Networks Thunder	TH-5840-11 appliance (Plataforma hardware)
TH-7445 A10 Networks Thunder	TH-7445 appliance (Plataforma hardware)
TH-7650-11 A10 Networks Thunder	TH-7650-11 appliance (Plataforma hardware)
TH-7655 A10 Networks Thunder	TH-7655 appliance (Plataforma hardware)
TH-940 A10 Networks Thunder	TH-940 appliance (Plataforma hardware)
TH-1040 A10 Networks Thunder	TH-1040 appliance (Plataforma hardware)
TH-3350E A10 Networks Thunder	TH-3350E appliance (Plataforma hardware)
TH-3350 A10 Networks Thunder	TH-3350 appliance (Plataforma hardware)
TH-3350S A10 Networks Thunder	TH-3350S appliance (Plataforma hardware)
TH-4440 A10 Networks Thunder	TH-4440 appliance (Plataforma hardware)
TH-5440 A10 Networks Thunder	TH-5440 appliance (Plataforma hardware)
TH-5840 A10 Networks Thunder	TH-5840 appliance (Plataforma hardware)
TH-5845 A10 Networks Thunder	TH-5845 appliance (Plataforma hardware)
TH-6440 A10 Networks Thunder	TH-6440 appliance (Plataforma hardware)
TH-6655S A10 Networks Thunder	TH-6655S appliance (Plataforma hardware)
TH-7440 A10 Networks Thunder	TH-7440 appliance (Plataforma hardware)
TH-7440 A10 Networks Thunder	TH-7440 appliance (Plataforma hardware)
TH-7650 A10 Networks Thunder	TH-7650 appliance (Plataforma hardware)
TH-14045 A10 Networks Thunder	TH-14045 appliance (Plataforma hardware)
vTH-200Mbps A10 Networks vThunder	vTH-200Mbps software license (Plataforma software)
vTH-1Gbps A10 Networks vThunder	vTH-1Gbps software license (Plataforma software)
vTH-4Gbps A10 Networks vThunder	vTH-4Gbps software license (Plataforma software)
vTH-8Gbps A10 Networks vThunder	vTH-8Gbps software license (Plataforma software)
vTH-10Gbps A10 Networks vThunder	vTH-10Gbps software license (Plataforma software)
vTH-20Gbps A10 Networks vThunder	vTH-20Gbps software license (Plataforma software)
vTH-40Gbps A10 Networks vThunder	vTH-40Gbps software license (Plataforma software)
vTH-100Gbps A10 Networks vThunder	vTH-100Gbps software license (Plataforma software)
vTH-Flexpool A10 Networks vThunder	vTH-Flexpool software license (Plataforma software)

Tabla 1 – Modelos incluidos en el procedimiento de empleo

4. En el siguiente enlace se pueden consultar las siguientes guías recomendadas para la instalación correcta y segura del producto:

<https://documentation.a10networks.com/#product> [REF16]

5. Entre las guías a revisar se incluyen:

- Guías de instalación de la serie A10 Thunder (para el modelo Thunder) Guías de configuración de ACOS
 - ACOS 5.2.1-P3 - Guía de configuración y administración del sistema
 - ACOS 5.2.1-P3 - Guía de seguridad y acceso a la gestión
 - ACOS 5.2.1-P3 - Referencia de interfaz de línea de comandos
 - ACOS 5.2.1-P3 - Guía de configuración de seguridad IP

6. Es necesario tener en cuenta que se requiere un ID de inicio de sesión y una contraseña de soporte de A10 Networks para acceder a la documentación en línea. Dicha cuenta se solicita y genera una vez recibido el producto (<https://glm.a10networks.com>) [REF6].

3. ORGANIZACIÓN DEL DOCUMENTO

7. Este documento se compone de los siguientes apartados:
 - a) Apartado **4**. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.
 - b) Apartado **5**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.
 - c) Apartado **6**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
 - d) Apartado **7**. En este apartado se incluye un listado de la documentación que ha sido referenciada a lo largo del documento
 - e) Apartado **8**. En este apartado se incluye el listado de las abreviaturas empleadas a lo largo del documento.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

8. El envío y seguimiento de los dispositivos *hardware* A10 es realizado directamente por el proveedor seleccionado.
9. El embalaje entregado deberá ir precintado y debe incluir los siguientes identificadores:
 - Identificación clara de los componentes incluidos en el interior.
 - Etiquetas indicativas con la nomenclatura del producto.
 - Número de serie del producto.
 - Información del número de albarán y del envío.
10. Los dispositivos ACOS tienen una o más etiquetas de evidencia de manipulación con un número de serie y una identificación de la empresa adheridos al chasis antes de entregarlos a los clientes.



Figura 1 – Etiqueta contra manipulación

11. El embalaje del dispositivo *A10 Thunder Series* debe ser inspeccionado cuidadosamente para detectar posibles alteraciones o irregularidades. Las etiquetas externas deben coincidir con el producto adquirido, así como los componentes deben coincidir con los de la documentación enviada con el producto. Igualmente, si la caja está dañada, será necesario ponerse en contacto inmediatamente con el proveedor.

4.2 ENTORNO DE INSTALACIÓN SEGURO

12. El dispositivo A10 Thunder o los servidores o entornos virtuales en los que se instalen las licencias vThunder deben instalarse en un Centro de Proceso de Datos (CPD). El CPD debe disponer de protección física para evitar ataques que puedan comprometer el producto y permitan la correcta operación de los sistemas IT instalados.
13. Los usuarios administradores del sistema A10 Thunder deberán estar autorizados, de acuerdo con las políticas de seguridad de la organización.
14. Las credenciales del administrador utilizadas para acceder al dispositivo de red estarán protegidas en la plataforma en la que residen.

4.3 REGISTRO Y LICENCIAS

15. Las licencias asociadas a los productos de A10 son gestionadas desde el portal *Global Licence Manager (GLM)*, <https://glm.a10networks.com/> [REF6].
16. El *Global License Manager (GLM)* es el sistema de licencias y facturación para A10 Networks. El GLM es administrado por A10 Networks y es el portal principal que se utiliza para obtener una licencia de clave de activación para dispositivos adquiridos.
17. Dicha URL también puede usarse para crear licencias de prueba, administrar activos existentes, rastrear el estado de la licencia, solicitar devolución Autorizaciones de mercancías (RMA) y acceso a recursos de instalación, como parches actualizados para varios aparatos A10.
18. Las Guías de alta de licencias y usuarios pueden encontrarse en el enlace [REF8]: <https://documentation.a10networks.com/#licensing-guide>
19. GLM funciona a través de los grupos *Organización* (nombre de la Empresa a la que se asocian las licencias) y *Usuarios*. Estos últimos pueden tener diferentes roles. Los roles asocian a los usuarios y a lo que le permiten hacer a cada usuario en una organización, incluidos los permisos de licencia.

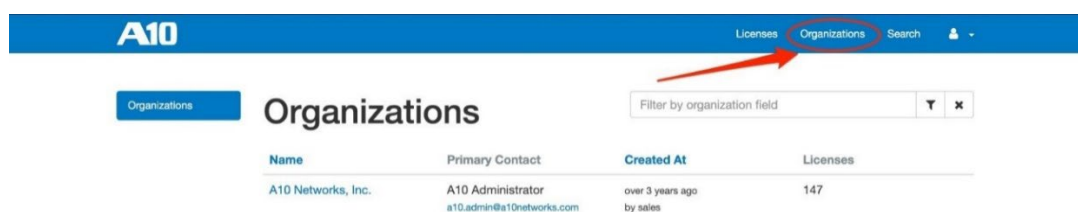


Figura 2 – Organización y licencias asociadas

20. Cada licencia puede restringir aún más el acceso de los usuarios a través de la página *Usuarios con Acceso*. Los usuarios agregados aquí se agregarán a la organización como miembros. Cualquier persona autorizada en la licencia y que disponga de los permisos adecuados (*owner* o *admin*), puede agregar más usuarios.

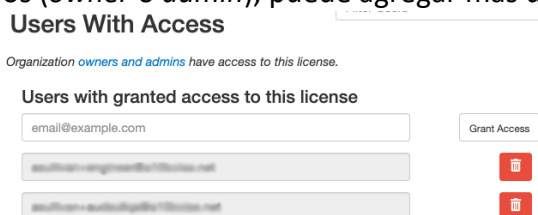


Figura 3 – Usuarios con acceso a la licencia

21. Toda la documentación asociada a cómo se dan de alta los usuarios y cómo se gestionan las licencias aparecen referenciados en el enlace [REF7]: <https://glm.a10networks.com/documentation>

4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN

22. El dispositivo de A10 interactúa con los siguientes sistemas:

- Interfaces administrativas locales y remotas.
- Interfaz de servidor *Syslog* para almacenamiento de registros de auditoría externa.
- Interfaz de servidor *Network Time Protocol* (NTP) para obtener información de tiempo confiable en los registros de auditoría.
- Interfaz de servidor de archivos para actualizaciones confiables y copias de seguridad de configuración.

23. El dispositivo A10 también interactúa con una Autoridad de Certificación (CA) para los certificados de servidor y la validación de certificados mediante listas de revocación de certificados (CRL) y el protocolo de estado de certificados en línea (OCSP).

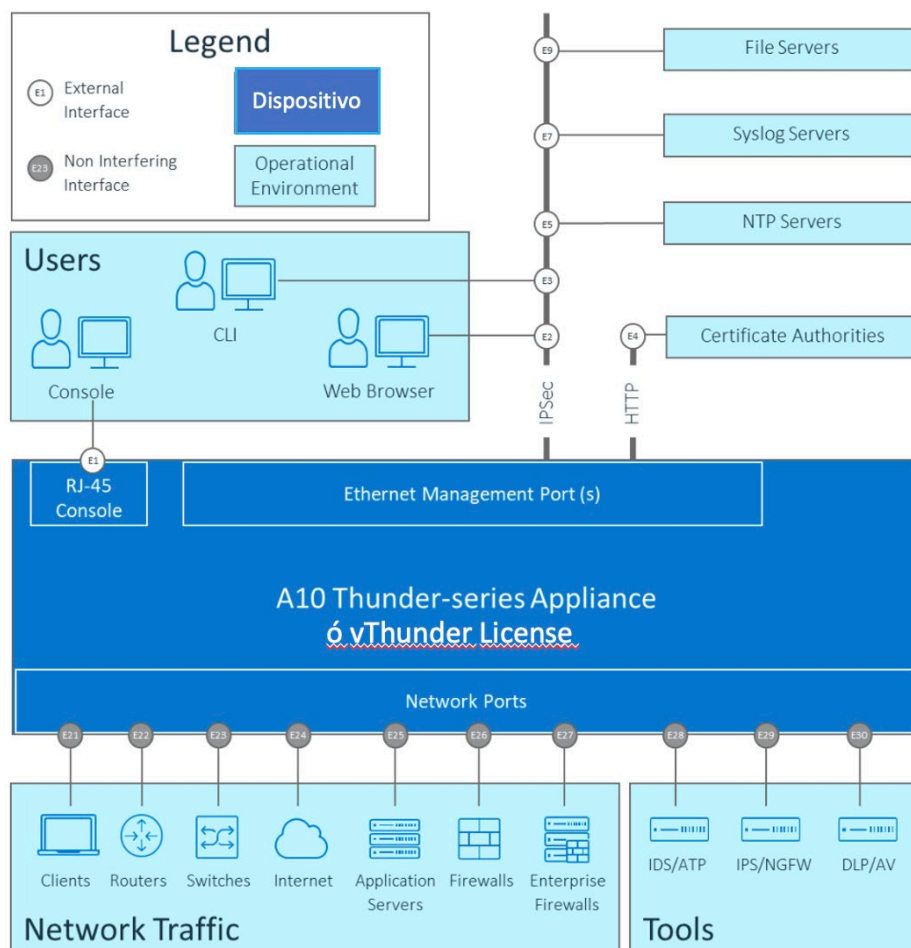


Figura 4 – Descripción de la arquitectura del dispositivo

24. El dispositivo utiliza el protocolo IPsec para proteger las comunicaciones con sistemas ubicados en su entorno operativo, con funcionalidad criptográfica proporcionada por OpenSSL y el proveedor *Linux Kernel Crypto*.

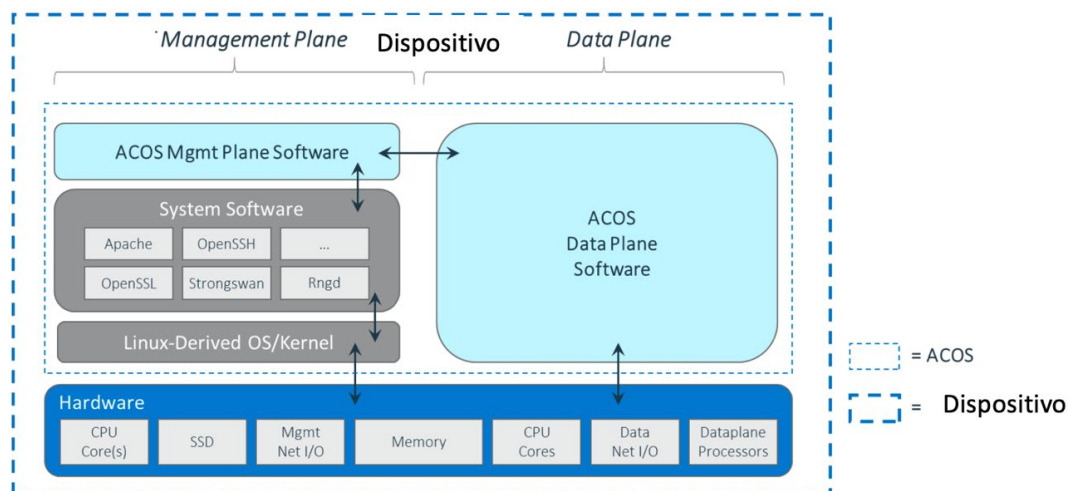


Figura 5 – Componentes dispositivo de la serie A10 Thunder

5. FASE DE INSTALACIÓN

25. Para llevar a cabo la instalación física del producto, es necesario preparar la localización e instalar el *hardware* A10 Thunder, desempaquetando el *hardware*, montándolo en un bastidor y conectando la administración Ethernet del dispositivo para una red local y el puerto de consola del dispositivo para acceder desde un servidor de terminal. Se debe tener en cuenta el punto 4.2 del presente documento.
26. A continuación, se indica la documentación concreta de instalación del modelo a instalar desde el enlace [REF9]:

<https://documentation.a10networks.com/#installation-guide>

5.1 ENTREGA DE SOFTWARE Y VERIFICACIÓN DE VERSIÓN

27. Los equipos físicos vienen con una versión instalada de fábrica. No obstante, se deberá verificar y asegurar que la versión del *software* sea compatible con **la versión del *software* de la que se hace uso está cualificada e incluida en el CPSTIC**
28. El comando "*show version*" CLI se puede utilizar para conocer las versiones de *software* instaladas en las imágenes de arranque principal y secundaria. El disco duro del equipo viene particionado de fábrica y contiene dos (2) imágenes totalmente independientes. Solo una de las imágenes puede estar siendo ejecutada en un determinado momento. De la misma forma, solo una de ellas puede ser configurada como imagen de arranque por defecto. Esta solución permite actualizar la imagen que no está en ejecución, sin interrupción del servicio, ya que la imagen en ejecución no se ve afectada.
29. Las imágenes de actualización o versiones software de vThunder se pueden descargar desde el sitio web de soporte de A10 Networks (<https://support.a10networks.com>) [REF5] a un servidor de confianza accesible a través de un túnel creado empleando el protocolo IPsec.
30. El comando CLI de actualización se puede utilizar para actualizar la imagen principal y secundaria del equipo mediante el uso de los protocolos SCP o SFTP para acceder a la imagen de actualización descargada.
31. Será necesario comprobar que las operaciones de actualización se realizan correctamente y confirmar que las imágenes primaria y secundaria de ACOS reflejan las versiones adecuadas mediante el comando "*show version*". A continuación, es necesario reiniciar el equipo con el comando "*reboot*", e iniciar sesión nuevamente en la consola del dispositivo como administrador raíz de ACOS "*admin*".

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

32. El modo de operación seguro se facilita utilizando la configuración creada para FIPS (en el punto 6.1.5 del presente documento se indica cómo activarla).
33. Se destaca que en dicho modo hay parámetros de configuración que aparecen por defecto deshabilitados.
34. **Este producto debe ser utilizado en modo de operación seguro.**

6.1.1 SOPORTE SSL/TLS EN MODO FIPS

35. Los siguientes cambios en el plano de datos SSL/TLS están configurados para el modo de operación FIPS:
- No se admiten las versiones de SSL/TLS: TLS 1.0 TLS 1.1.
 - Las familias de cifrado TLS no admitidas son las siguientes: TLS_RSA TLS_DHE, GMSSL y 3DES.
 - Los certificados RSA deben tener al menos 3072 bits. El procedimiento para cumplir la recomendación de que la clave RSA tenga una longitud como mínimo de 3072 bits, consistiría en crear o importar un certificado que use una clave RSA de longitud 4096 bits.
 - Solo se admiten certificados con autenticación SHA-2. En los intercambios cliente o servidor-TLS, el certificado o clave RSA que recibe el sistema ACOS debe tener al menos 4096 bits y autenticación SHA-2.
 - Para configuraciones RSA, solo se admiten claves configuradas de 3072 bits o superior.
 - Las claves solo se pueden exportar a través de protocolos seguros como HTTPS, SCP o SFTP.

6.1.2 IPSEC EN MODO FIPS

36. Los siguientes cambios de IPsec se aplican para los dispositivos ACOS FIPS:
- Los grupos *Diffie-Hellman* (DH) admitidos son 14 (predeterminado), 15, 16, 18, 19 y 20. Aunque el grupo *Diffie-Hellman* predeterminado para IPsec es el 14, como dicho grupo no se considera seguro, **se debe ejecutar el comando: “no dh-group 14”**, para que dicho grupo no sea aceptado.
 - Los grupos DH no admitidos son 0, 1, 2 y 5.
 - Solo se admite la versión 2 del protocolo de intercambio de claves de Internet (IKEv2).

- Los siguientes mecanismos de cifrado están deshabilitados y, por tanto, no están disponibles: DES, 3DES, MD5, Cifrado nulo y algoritmo hash nulo. Por considerarse inseguros, **no deben habilitarse**.
- Las opciones *eap-radius* y *eap-tls* para la autenticación IKE están deshabilitadas y no disponibles.
- **Se debe evitar el uso de claves precompartidas** y usar en su lugar claves de tipo RSA o ECDSA.

6.1.3 OTROS ASPECTOS A TENER EN CUENTA DEL MODO FIPS

37. Las siguientes son otras diferencias o limitaciones preconfiguradas para los dispositivos ACOS cuando funcionan en modo FIPS:

- Los servicios de Telnet no están disponibles, y no es posible habilitarlos mediante el comando de servicio *“enable-management”*.
- Los protocolos TFTP, FTP y HTTP, empleados para transferir los archivos desde y hacia el dispositivo ACOS no son compatibles con el modo FIPS, y por lo tanto son deshabilitados.
- Los tamaños de clave de intercambio de claves RSA deben ser de al menos 3072 bits.
- El servidor web ACOS para el acceso a la administración de GUI y aXAPI es compatible con FIPS. Los siguientes algoritmos criptográficos son compatibles con las configuraciones habilitadas para FIPS:
 - Estándar de cifrado avanzado (AES) y AES-GCM para el cifrado o descifrado.
 - *Secure Hash Algorithm 1 (SHA-1)* y *SHA-2* para hash y autenticación de mensajes hash. ECDSA y RSA para autenticación.
 - *Elliptic Curve Diffie Hellman Ephemeral (ECDHE)* para intercambio de llaves.
 - *NIST SP-800-90A* para DRBG.
 - Seguridad de la capa de transporte (TLS) mínimo 1.2.

38. Para los dispositivos ACOS FIPS configurados en modo no FIPS, RSA también es compatible con el intercambio de claves. La longitud de la clave RSA a utilizar en este caso debe de ser de al menos 3072 bits, aunque se recomienda el uso de claves de 4096 bits.

6.1.4 CONFIGURACIÓN INICIAL A TRAVÉS DE LA CONSOLA LOCAL

39. La configuración inicial del dispositivo debe realizarse a través de la consola local del dispositivo antes de conectarse a cualquier red. En cualquier momento durante este proceso, se puede emitir el comando CLI de escritura de memoria para escribir todos los cambios no guardados en la configuración de inicio de ACOS.

6.1.5 CONEXIÓN INICIAL Y CONFIRMACIÓN DEL MODO FIPS

40. Es necesario asegurarse de que el dispositivo esté funcionando en modo FIPS. Para ello, habrá que llevar a cabo el siguiente procedimiento.

1. Conectarse al dispositivo a través de la consola local utilizando una aplicación de terminal.
2. Autenticarse con las credenciales ACOS predeterminadas e ingresar al modo de configuración global.

login as: admin

Password: a10\$pass (for device configured in FIPS-mode)

a10 (for device configured in Non-FIPS-mode)

3. Confirmar que el modo de operación FIPS está configurado. Usando el comando "show versión". Si se indica "fips", el dispositivo está configurado para el modo FIPS. Si no se indica o la línea "Características de la plataforma" no se indica, entonces el dispositivo está configurado para el modo No FIPS.
4. Ingresar al modo de configuración EXEC privilegiado de ACOS.

ACOS> enable

ACOS# config

ACOS(config)#

6.1.6 CONFIGURACIÓN DE PARÁMETROS BÁSICOS DEL SISTEMA

41. A continuación, se detallan las acciones de configuración que deben ser aplicadas en el producto:

- **Cambiar la contraseña predeterminada** del dispositivo de la cuenta de administrador raíz de ACOS "admin" utilizando la contraseña de administrador. La nueva contraseña deberá tener una longitud de al menos 12 caracteres y cumplir con las características de complejidad de contraseñas.

ACOS(config)# admin password <nueva contraseña>

- **Establecer la fecha/hora del sistema y la zona horaria** mediante los comandos de consola clock y timezone; respectivamente. Por ejemplo:

ACOS(config)# timezone Europe/Madrid

ACOS(config)# clock set 10:31:00 July 21 2023

- **Establecer un nombre de host, servidores DNS y sufijo DNS** para el nombre de host del dispositivo, *ip dns [principal | secundario]* y los comandos CLI del sufijo *ip dns*; respectivamente.
- **Configurar el banner de inicio de sesión de CLI.** Este banner se muestra antes de solicitar las credenciales cuando se accede a la consola de ACOS localmente, o de forma remota a través de SSH sobre IPsec. El banner se puede ingresar en

un solo comando o en modo de varias líneas donde la consola solicita el contenido del banner a ingresar.

- **Establecer el tiempo de espera de inactividad** de la terminal en minutos mediante el comando *idle-timeout*, según la política de seguridad de la organización. Se recomienda establecer un tiempo de inactividad de **5 minutos**.
- Utilizar el comando CLI de administración de interfaz para **configurar la dirección IPv4 en la interfaz de administración** del dispositivo y habilitar la interfaz como predeterminada **para usar la función de control de administración** en el dispositivo.
- **Establecer una política de contraseñas estricta**. Habilitar un mínimo de 12 caracteres con 2 caracteres en minúsculas, 2 en mayúsculas, 2 numéricos y 1 especial como mínimo.
- **Establecer la política de bloqueo para el límite de 3 intentos fallidos** de autenticación, y la duración de los bloqueos mediante el comando de la CLI *admin-lockout*, según la política de seguridad de la organización. Cuando se alcanza el límite de 3 intentos fallidos de autenticación (definido por el comando "*admin-lockout threshold 3*"), el usuario es bloqueado y no puede hacer nuevos intentos de autenticación por un determinado periodo de tiempo, si se ha configurado el comando "*admin-lockout duration <minutes>*" con un valor distinto a 0 (valores disponibles entre 0-1440 minutos) o indefinidamente, si el valor es 0 (para desbloquear usuarios administradores bloqueados por esta política de seguridad, otro usuario con permisos de administrador tiene que ejecutar el siguiente comando "*admin <admin-username> unlock*").
- **Habilitar el registro de auditoría** para incluir el registro de comandos del modo de configuración, así como el registro de eventos. Seleccionar los niveles de gravedad del registro de eventos de acuerdo con la política de seguridad de la organización.

42. De manera predeterminada, ACOS mostrará las entradas del registro de eventos a la consola local. Para deshabilitar el informe (visualización) de estas entradas en la consola local, configurar lo siguiente:

```
ACOS(config)# logging console disable
```

6.1.7 ESTABLECER UN TÚNEL IPSEC PARA CONEXIONES EN EL ENTORNO OPERATIVO

43. Para admitir el acceso seguro a servidores externos y desde administradores de gestión remota en el entorno operativo del dispositivo, **es necesario configurar un túnel IPsec**.
44. Inicialmente, este túnel debe configurarse **con una clave RSA de 4096 bits** compatible con el par IPsec remoto del túnel.

45. Este túnel podría limitarse a un solo par de túnel o se podrían configurar túneles adicionales para admitir necesidades de conectividad más complejas. También se pueden elegir otros algoritmos según sea necesario para interoperar con pares IPsec.

46. A continuación, se enumera una serie de ajustes comunes necesarios para cumplir con la configuración recomendada:

- **Habilitar el registro de eventos de validación de certificados IPsec y X.509** en el registro de eventos ACOS con el siguiente comando CLI.

```
ACOS(config)# vpn ike-logging-enable
```

- **Habilitar la implementación de la clave IKE SA mayor o igual a ESP SA** en la negociación de establecimiento de túnel IPsec con el siguiente comando CLI.

```
ACOS(config)# vpn ipsec-cipher-check
```

- **Configurar el componente IKE del túnel** con el par VPN con los siguientes comandos CLI, donde *ike-psk-string* es una cadena de 1 a 127 caracteres. A continuación, se introduce un ejemplo de configuración:

```
vpn ike-gateway ipsec_mgmt_ike_1
ike-version v2
nat-traversal
auth-method rsa-signature sha256
interface-management
dh-group 15
encryption aes-256 hash sha256
local-id "10.1.1.38"
remote-id "10.1.1.164"
local-address ip 10.1.1.38
remote-address ip 10.1.1.164
lifetime 86400
```

- Por último, **configurar el componente ESP del túnel** con los siguientes comandos CLI para admitir intercambios con todas las direcciones IP en el segmento de red de confianza. A continuación, se introduce un ejemplo de configuración:

```
vpn ipsec ipsec_mgmt_esp_1
mode tunnel
proto esp
dh-group 15
encryption aes-256 hash sha256
lifetime 28800
lifebytes 10240
traffic-selector ipv4 local 10.1.1.38 255.255.255.255 remote 10.65.25.0
255.255.255.0 ike-gateway ipsec_mgmt_ike_1
```

- **Confirmar el estado del túnel como ACTIVO** usando los comandos ping o traceroute CLI a un sistema disponible en la subred remota confiable. Más

adelante en este documento, se proporciona orientación adicional y antecedentes para la administración de túneles IPsec en el dispositivo.

47. La guía de configuración de túneles IPsec está disponible en el enlace [REF 17]:

https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_IPSEC.pdf

6.1.8 HABILITAR EL ACCESO A LA ADMINISTRACIÓN SSH REMOTA

48. Para admitir un acceso CLI más conveniente, se puede habilitar el acceso desde clientes terminales SSH remotos a través del túnel IPsec.

49. Se debe confirmar que se puede acceder al dispositivo desde un cliente SSH en la subred admitida por el túnel IPsec utilizando la cuenta de administrador raíz de ACOS "admin" predeterminada. El acceso SSH no estará disponible a través del puerto de gestión del dispositivo, sino a través de la subred del túnel IPsec.

6.2 AUTENTICACIÓN

50. Los dispositivos ACOS proporcionan las siguientes interfaces de usuario:

- Interfaz de línea de comandos (CLI). Interfaz basada en texto en la que escribe comandos en una línea de comandos. Es posible acceder a la CLI directamente a través de la consola serie o a través de la red utilizando el protocolo Secure Shell (SSH) (versiones 1 y 2). **La versión 1 se considera no segura, por lo que se debe emplear SSHv2.**
- Interfaz gráfica de usuario (GUI). Interfaz basada en web desde la que es posible acceder a las páginas de configuración o administración y escribir o seleccionar valores para configurar o administrar el dispositivo. **Sólo se debe acceder a la GUI utilizando el protocolo seguro HTTPS.**

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

6.3.1.1 ACCESO VÍA CLI

51. Los dispositivos ACOS suministran funciones avanzadas para proteger el acceso de administración al dispositivo. En esta sección se da por supuesto que solo se han establecido las configuraciones de seguridad básicas.

52. Se debe iniciar la sesión en la CLI usando SSHv2.

53. El nivel *User EXEC* permite ingresar algunos comandos básicos, incluidos algunos comandos *show*, así como *ping* y *traceroute*. Para acceder al nivel *EXEC* privilegiado de la CLI y permitir el acceso a todos los niveles de configuración, ingresar el comando *enable*.

6.3.1.2 GESTIÓN REMOTA

54. El dispositivo admite la gestión remota a través de IPsec para:

- Clientes de terminal SSHv2 a ACOS CLI
- Clientes de navegador web para ACOS Web/GUI

55. Esta sección describe los procedimientos de administración segura para estas modalidades de administración remota.

6.3.1.2.1 CLIENTES SSH A TRAVÉS DE IPSEC

56. Los clientes SSH que accedan al dispositivo deberán configurarse para admitir las siguientes configuraciones clave para interoperar con el dispositivo.

- *SSH Protocol Version: 2*
- *Encryption Algorithms: aes128-ctr, aes256-ctr*
- *Integrity Algorithms: hmac-sha1, hmac-sha2-512, hmac-sha2-256*
- *Key Exchange: diffie-hellman-group15-3072-bit*
- *Public Key Authentication: RSA*

6.3.1.2.2 CLIENTES WEB/GUI A TRAVÉS DE IPSEC

57. Para admitir el acceso Web/GUI al dispositivo desde clientes de navegadores web remotos a través de los túneles IPsec configurados, se pueden configurar ACL (*listas de control de acceso*) adicionales para habilitar el acceso al dispositivo.

58. Confirmar que se puede acceder a dispositivo Web/GUI desde un cliente de navegador en la subred admitida por el túnel IPsec utilizando la cuenta de administrador raíz de ACOS "admin" u otra cuenta de administrador agregada. El acceso web/GUI no estará disponible para la subred conectada localmente del puerto de administración del dispositivo.

59. Los clientes del navegador que accedan al dispositivo deberán configurarse para admitir la Web/GUI del dispositivo con las siguientes opciones:

CIPHER SUITES	VERSIÓN
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_256_CCM	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_128_CCM	TLS 1.2
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	TLS 1.2

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2
TLS_DHE_RSA_WITH_AES_256_CCM	TLS 1.2
TLS_DHE_RSA_WITH_AES_128_CCM	TLS 1.2
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2
TLS_AES_128_GCM_SHA256	TLS 1.3
TLS_AES_256_GCM_SHA384	TLS 1.3
TLS_CHACHA20_POLY1305_SHA256	TLS 1.3
TLS_AES_128_CCM_SHA256	TLS 1.3
TLS_AES_128_CCM_8_SHA256	TLS 1.3

Tabla 2 – Ciphersuites empleados por clientes de navegador

6.3.1.2.3 GESTIÓN DE TÚNELES IPSEC

6.3.1.2.3.1 IPSEC COMPATIBLE CON EL DISPOSITIVO

60. IPsec admite las siguientes capacidades resumidas para la configuración recomendada:

- Solo compatible con IKEv2.
- Solo se admite el modo túnel. El modo de transporte no es compatible.
- Solo se admite ESP. AH no es compatible.
- Se admite NAT Traversal para IKEv2 para encapsular el tráfico ESP dentro de los paquetes UDP.
- IKEv2 admite los siguientes algoritmos y ciclos de vida de la Asociación de Seguridad (SA).
 - Encriptación: *AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256*
 - Integridad: *SHA-256, SHA-384*
 - PRF: *SHA-256, SHA-384*
 - Autenticación: *RSA, ECDSA*
 - *DH Groups: 15 (3072-bit MODP) ó superior*

- *SA Lifetimes: 300 seconds - 86400 seconds (24 hours)*
- ESP admite los siguientes algoritmos y ciclos de vida de la Asociación de seguridad (SA).
 - Cifrado: *AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256*
 - Integridad: *SHA-256, SHA-384*
 - Vida útil de SA: 300 segundos - 28800 segundos (8 horas) y/o 10 (o ilimitado) GBytes

6.3.1.2.3.2 CONFIGURAR UNA PUERTA DE ENLACE VPN IKE

61. Este punto se explica en el capítulo 3 de la guía de configuración de IPsec, que está disponible en el enlace [REF 17]:

https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_IPSEC.pdf

62. En la página 77 de la mencionada guía, también se encuentra un ejemplo de configuración.

6.3.1.2.3.3 CONFIGURAR UN TÚNEL VPN IPSEC

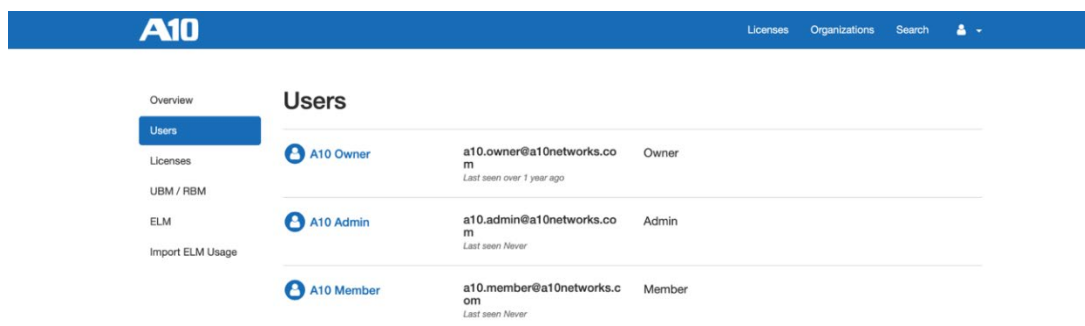
63. Este punto se explica en el capítulo 4 de la guía de configuración de IPsec, que está disponible en el enlace:

https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_IPSEC.pdf [REF 17].

64. En la página 119 de la mencionada guía, también se encuentra un ejemplo de configuración.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

65. En la página correspondiente a la organización hay una pestaña de "*Usuarios*". Esta pestaña lleva a la lista de usuarios y sus roles apropiados. Cuando un usuario pertenece a una organización, tiene uno de estos tres roles: propietario (*Owner*), administrador (*Admin*) o miembro (*Member*).






Users				
	A10 Owner	a10.owner@a10networks.com	Owner	Last seen over 1 year ago
	A10 Admin	a10.admin@a10networks.com	Admin	Last seen Never
	A10 Member	a10.member@a10networks.com	Member	Last seen Never

Figura 6 – Roles de usuario

66. Las organizaciones deben tener al menos un propietario (*OWNER*) de organización, pero pueden tener varios usuarios de cada rol.
67. El dispositivo admite dos (2) tipos de administradores (usuarios) en la configuración segura, con privilegios de solo lectura y privilegios de lectura y escritura.
- Los administradores de solo lectura solo pueden usar los servicios *User EXEC* de ACOS CLI o GUI para mostrar información y realizar tareas básicas como *pings* y *traceroutes*.
 - Los administradores de lectura y escritura pueden, además de los servicios *EXEC* de usuario, utilizar los servicios *EXEC* privilegiados de ACOS CLI o GUI para agregar, modificar y eliminar configuraciones del dispositivo.
68. La cuenta "*admin*" es una cuenta privilegiada permanente de lectura y escritura en el dispositivo. Los atributos asociados con las cuentas de administrador definidas localmente son:
- Nombre de inicio de sesión
 - Contraseña
 - Privilegio
 - Interfaces de acceso permitidas (a saber, CLI local/remota y Web/GUI remota).
69. Las credenciales de nombre de inicio de sesión y contraseña son para autenticarse en el dispositivo y determinar los privilegios que se permitirán para la sesión de administración.
70. Las cuentas definidas localmente en la administración del dispositivo se administran a través del comando *admin* CLI o la página web/GUI '*Sistema > Administrador > Usuarios*'. Por ejemplo, para agregar una cuenta de administrador de seguridad (por ejemplo, de lectura y escritura):

```
ACOS(config)# admin secadmin1
ACOS(config-admin:secadmin1)# password pw-string
ACOS(config-admin:secadmin1)# access cli web axapi
ACOS(config-admin:secadmin1)# privilege write
ACOS(config-admin:secadmin1)# enable
```

NOTA:

Los intentos de configurar valores para valores de cadena de contraseña que sean demasiado cortos o demasiado largos se considerarán errores de sintaxis de entrada por parte del comando *admin* y no se registrarán como registros de auditoría o eventos por parte del dispositivo.

71. De forma predeterminada, cuando se crea una nueva cuenta de usuario, ésta por defecto solo tiene permisos de lectura, a no ser que se configure expresamente el permiso de escritura para dicho usuario. Para distinguir un administrador de seguridad para el dispositivo, incluir el privilegio de escritura para la cuenta, tal y como se indica en el ejemplo anterior.

6.3.2.1 GESTIÓN DE CONTRASEÑAS

72. Las contraseñas mantenidas por el dispositivo se pueden componer usando cualquier combinación de letras mayúsculas y minúsculas, números y caracteres especiales, incluidos los siguientes. Los caracteres especiales de la contraseña son compatibles con las interfaces CLI y Web/GUI para autenticarse correctamente con el dispositivo:

" ", "!", "@", "#", "\$", "%", "^", "&", "*", "(", ")", " ", "'", " ", "+", " ", "-", " ", ".", " /", ":", " ", "<", "=", ">", "?", "[", "\", "]", "_", " ", "{", "|", "}", "~"

73. La política de contraseñas se puede configurar con opciones estrictas, medias y simples que incluyen varios mínimos para la cantidad de caracteres en minúsculas, mayúsculas, numéricos y especiales mediante el comando CLI de complejidad de la política de contraseñas del sistema. **Los parámetros que debería tener una contraseña para ser considerada segura son los siguientes:**

- Doce (12) caracteres.
- Composición de la contraseña: letras mayúsculas, letras minúsculas, números y símbolos especiales. Está recomendado el uso de los cuatro (4) grupos.
- Número de contraseñas anteriores que no se permite utilizar: al menos, cinco (5).
- Tiempo de validez en días de las contraseñas tras el cual expiran: aproximadamente dos meses (60 días).
- Número de días que deben transcurrir tras el cambio de una contraseña antes de poder modificarla de nuevo: diez (10) días.

ACOS(config)# system password-policy complexity ?

Strict Strict: Min length:12, Min Lower Case:2, Min Upper Case:2, Min Numbers:2, Min Special Character:1

74. La política de contraseñas es configurable por los administradores del dispositivo y admite una longitud mínima de contraseña de 8 caracteres y una longitud máxima de contraseña de 63 caracteres. Esta longitud mínima es configurable. Para cambiar la longitud mínima de las contraseñas configuradas en el dispositivo a 12 caracteres:

```
ACOS(config)# system password-policy complex Strict min-pswd-len 12
```

75. El parámetro de antigüedad de las contraseñas define el número de días definidos para las contraseñas de todos los usuarios con privilegios de administrador del dispositivo. **Se deberá marcar la opción *Strict (Estricto)***, en la que la validez máxima de las contraseñas se establece en **60 días**.
76. Para la **configuración del número de contraseñas anteriores admitidas**, se deberá marcar la opción *Strict (Estricto)* en el que el número de contraseñas anteriores almacenadas es 5.

6.3.3 TERMINACIÓN DE LA SESIÓN

6.3.3.1 TERMINACIÓN DE SESION POR INACTIVIDAD

77. Las sesiones autenticadas en el dispositivo se pueden configurar para tiempos de espera de inactividad de hasta 60 minutos mediante el comando CLI de terminal *idle-timeout*. **Se debe configurar un tiempo de terminación de la sesión por inactividad de 5 minutos.**
78. Este tiempo de espera afectará a las sesiones de administración del dispositivo CLI en la consola local o de forma remota mediante SSHv2 a través de IPsec. El valor predeterminado para este tiempo de inactividad es de 15 minutos. Para ajustarlo a 5 minutos el comando a emplear sería el siguiente:

```
ACOS(config)# terminal idle-timeout 5
```

79. Los valores de tiempo de espera del servicio web se pueden configurar de manera similar para controlar los tiempos de espera de inactividad para sesiones autenticadas en la GUI web del dispositivo a través de IPsec. Estos tiempos de espera se configuran mediante el comando CLI *web-service gui-timeout-policy*. El valor predeterminado para este tiempo de inactividad es de 10 minutos. Para ajustarlo a 5 minutos el comando a emplear sería el siguiente:

```
ACOS(config)# web-service gui-timeout-policy idle 5
```

6.3.3.2 BANNER DE LOGIN

80. Para todas las sesiones administrativas interactivas del dispositivo, no se puede realizar ninguna acción antes de autenticarse correctamente (iniciar sesión) en el dispositivo.
81. Antes de que se le soliciten las credenciales en estas sesiones, el dispositivo **deberá mostrar un aviso de aviso y mensajes de advertencia de consentimiento** según la

política de seguridad de la organización. Estos mensajes (*banners*) se pueden configurar para el dispositivo como se describe a continuación.

6.3.3.2.1 BANNER DE INICIO DE SESIÓN DE LA CLI

82. Antes de que se le soliciten las credenciales en las sesiones administrativas de la CLI del dispositivo utilizando la consola local o accediendo de forma remota a la CLI con SSHv2 a través de IPsec, se mostrará un banner. Este banner se configura para el dispositivo mediante el comando CLI de inicio de sesión de banner (*banner login <text>*).

6.3.3.2.2 BANNER DE INICIO DE SESIÓN WEB/GUI

83. Antes de que se soliciten las credenciales en las sesiones administrativas del dispositivo Web/GUI a través de IPsec, se mostrará un *banner*. Este banner está configurado para el dispositivo en la página Web/GUI '*Sistema > Configuración > Web*' para el parámetro '*Mensaje de inicio de sesión previo a la GUI*'. El *banner* se muestra en una ventana emergente que debe aceptarse haciendo clic en el botón "*Aceptar*" antes de que se muestre la página de inicio de sesión estándar del dispositivo, que solicita el ingreso del nombre de usuario y la contraseña.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

6.4.1 CONFIGURACIÓN DE LA INTERFAZ DE ADMINISTRACIÓN

84. La interfaz de administración (*MGMT*) es una interfaz Ethernet a la que puede asignar una sola dirección IPv4 y una sola dirección IPv6. La interfaz de gestión está separada de las interfaces de datos Ethernet.

85. La siguiente Figura muestra un ejemplo de la interfaz de administración en un dispositivo Thunder Series.

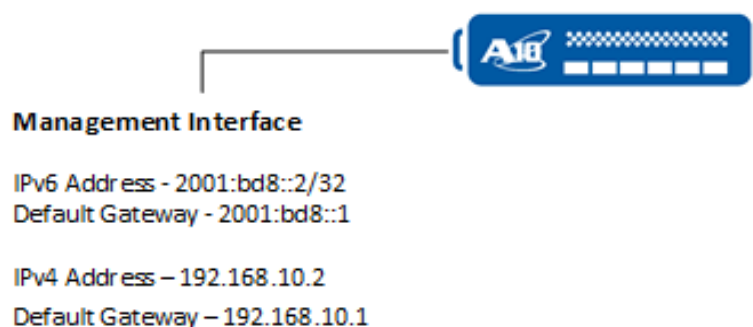


Figura 7 – Interfaz de administración

6.4.1.1 USO DE LA GUI PARA CONFIGURAR LA INTERFAZ DE ADMINISTRACIÓN

86. Esta sección describe cómo usar la GUI para configurar la interfaz de administración.

NOTA: a menos que ya haya configurado una interfaz IP, navegar hasta la dirección IP predeterminada: <http://172.31.31.31>.

- 1) ir a Network > Interfaces > Management
- 2) En la página de Gestión:
 - Configurar la “duplexity” de la interfaz de administración (Full, Half o auto)
 - Configurar la velocidad de la interfaz de gestión.
 - Configurar la IP de administración en IPv4 o IPv6.
 - Si se opta por configurar la IP de gestión en IPv4:
 - Seleccionar si la IP de gestión se va a obtener mediante DHCP o se va a configurar manualmente.
 - Si se opta por configurar la IP de administración de forma manual, indicar la IPv4, la máscara de subred y la puerta de enlace predeterminada.

6.4.1.2 USO DE LA CLI PARA CONFIGURAR LA INTERFAZ DE ADMINISTRACIÓN

87. Este punto se explica en la sección “Using the CLI to Configure the Management Interface” de la guía “ACOS 5.2.1-P3 System Configuration and Administration Guide”, más concretamente en la página 70. La guía está disponible en el enlace: https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_SAG.pdf [REF 18].

6.4.2 MANTENER LAS INTERFACES DE ADMINISTRACIÓN Y DE DATOS EN REDES SEPARADAS

88. **La interfaz de administración y las interfaces de datos deben estar en redes separadas.** Si ambas tablas tienen rutas a la misma subred de destino, algunas operaciones (por ejemplo, *ping*) pueden tener resultados inesperados. Una excepción es la ruta predeterminada (0.0.0.0/0), que puede estar en ambas tablas.
89. Para mostrar las rutas en la tabla de rutas de administración, usar el comando *show ip route mgmt*.
90. Para mostrar las rutas del plano de datos, utilizar los comandos *show ip route* o *show ip fib*.

6.4.3 OPCIONES DE ENRUTAMIENTO DE ADMINISTRACIÓN

91. Es posible configurar el dispositivo ACOS para usar la interfaz de administración como interfaz de origen para los siguientes protocolos de administración, utilizados para el tráfico de administración automatizado:
- SYSLOG

- SNMPD
- NTP
- RADIUS
- TACACS+
- SMTP

92. De manera predeterminada, el acceso Telnet está deshabilitado en todas las interfaces, incluida la interfaz de administración. El acceso SSH, HTTP, HTTPS y SNMP está habilitado de manera predeterminada solo en la interfaz de administración, y está deshabilitado de manera predeterminada en todas las interfaces de datos. A continuación, se indican **los comandos que se deben introducir para deshabilitar el protocolo HTTP, considerado inseguro**, en la interfaz de administración:

```
ACOS#config
```

```
ACOS(config)#disable-management service http
```

```
You may lose connection by disabling the http service.
```

```
Continue? [yes/no]: yes
```

```
ACOS(config-disable-management http)#management
```

6.5 GESTIÓN DE CERTIFICADOS

93. El dispositivo también admite el uso de certificados de clave pública X.509 y clave privada para la autenticación IPsec. Esta sección describe cómo configurar el dispositivo para certificados X.509 y claves privadas. En resumen, el proceso constará de los siguientes pasos.

- 1) Generar claves privadas y solicitudes de firma de certificados (CSR)
- 2) Exportar los CSR a un servidor de archivos confiable
- 3) Utilizar los CSR para generar certificados X.509 firmados por una autoridad de certificación (CA) raíz o una CA intermedia de la CA raíz
- 4) Importar los certificados X.509 firmados al dispositivo
- 5) Importar los certificados de CA raíz al dispositivo

94. El dispositivo admite los siguientes tamaños de clave para la configuración recomendada:

- RSA: 3072 bits o superior
- ECDSA: 256 bits o superior

6.5.1 GENERAR CLAVE PRIVADA Y SOLICITUD DE FIRMA DE CERTIFICADO

95. Utilizar el comando CLI *pki create* para generar una clave privada con la CSR correspondiente y exportar la CSR a un servidor de confianza. La opción de comando

use-mgmt-port debe usarse para la configuración recomendada de seguridad. Este comando sirve para indicar que se usará la interfaz de gestión (*management port*) para exportar el fichero CSR al servidor de confianza.

96. Este punto se explica en la sección “*Generating a Certificate Signing Request (CSR)*” de la guía “*ACOS 5.2.1-P3 Application Delivery Controller Guide*”, más concretamente en la página 503. La guía está disponible en el enlace:

https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_SLB.pdf [REF 19].

6.5.2 GENERAR CERTIFICADOS FIRMADOS POR LA CA

97. Usando los CSR exportados al servidor de confianza, es necesario generar certificados RSA y/o ECDSA, firmados por la CA raíz o una CA intermedia de la CA raíz.

98. Este punto se explica en la sección “*Creating Multiple CA Certificate in Server-SSL Templates*” de la guía “*ACOS 5.2.1-P3 Application Delivery Controller Guide*”, más concretamente en la página 515. La guía está disponible en el enlace:

https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_SLB.pdf [REF 19].

6.5.3 IMPORTAR CERTIFICADOS FIRMADOS

99. A continuación, es necesario utilizar el comando de la CLI *import cert* para importar los certificados firmados al dispositivo desde el servidor de confianza a través de IPsec. La opción de comando *use-mgmt-port* debe usarse para la configuración recomendada de seguridad.

100. A continuación, se incluye un ejemplo de los comandos a introducir para importar los certificados firmados desde el servidor SCP a través de túneles IPsec a la subred de confianza.

```
ACOS(config)#import cert rsa-cert1-signed use-mgmt-port \  
scp://adminusr@10.65.25.165/cert/rsa-cert1-signed
```

```
ACOS(config)#import cert ecdsa-cert1-signed use-mgmt-port \  
scp://adminusr@10.65.25.165/cert/ecdsa-cert1-signed
```

101. Este punto se explica en la sección “*Importing a Certificate and Key*” de la guía “*ACOS 5.2.1-P3 Application Delivery Controller Guide*”, más concretamente en la página 501. La guía está disponible en el enlace:

https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_SLB.pdf [REF 19].

6.5.4 IMPORTAR CERTIFICADOS DE CA RAÍZ

102. Por último, utilizar el comando *import ca-cert* de la CLI para importar los certificados raíz de CA al dispositivo desde el servidor de confianza a través de IPsec. La opción de comando *use-mgmt-port* debe usarse para la configuración recomendada.

103. Este punto se explica en la sección “*Importing a Certificate and Key*” de la guía “*ACOS 5.2.1-P3 Application Delivery Controller Guide*”, más concretamente en la página 502. La guía está disponible en el enlace:

https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_SLB.pdf [REF 19]

104. A continuación, se incluye un ejemplo para importar los certificados firmados desde el servidor SCP a través de túneles IPsec a la subred de confianza.

```
ACOS(config)#import ca-cert ca-cert1 use-mgmt-port  
scp://adminusr@10.65.25.165/cert/ca-cert1
```

6.6 SERVIDORES DE AUTENTICACIÓN

105. El usuario puede configurar distintos servicios de autenticación, dichos servicios vienen descritos en la guía *Management Access and Security Guide* disponible desde el enlace [REF10]:

<https://documentation.a10networks.com/docs/ACOS/521x/5-2-1-p7/>

106. De forma predeterminada, cuando alguien intenta iniciar sesión en el dispositivo ACOS, el dispositivo determina si el nombre de usuario y la contraseña existen en la base de datos administrativa local. Sin configuración adicional, el proceso de autenticación se detiene en este punto.

107. El usuario puede configurar el dispositivo ACOS para usar también servidores RADIUS, TACACS+ o LDAP externos para la autenticación. El detalle de cómo realizar dicha configuración se puede consultar en los capítulos 8 (LDAP) y 9 (TACACS+ y RADIUS) de la guía “*ACOS 5.2.1-P3 Management Access and Security Guide*”. La guía está disponible en el enlace:

https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_MAS.pdf [REF 21]

6.6.1 CONFIGURACIÓN DE AUTENTICACIÓN, AUTORIZACIÓN Y CONTABILIDAD (AAA) PARA ACCESO DE ADMINISTRADOR

108. Para configurar la autenticación, autorización y contabilidad (AAA):

- Si se utiliza el protocolo LDAP, para obtener más información, se recomienda consultar la guía [Lightweight Directory Access Protocol \[REF11\]](#).

- Para usar más de un protocolo AAA, se recomienda consultar el punto [Authentication and Modes](#) de la guía *Management Access and Security Guide*.

6.6.2 INTEGRACIÓN CON MFA

109. ACOS admite la autenticación de usuarios utilizando una base de datos local o servidores de autenticación (AS) como LDAP, TACACS y RADIUS. Este es el método de autenticación principal, además de que este usuario puede habilitar MFA.
110. Cuando se configura el MFA, se agrega otra capa de autenticación como segundo factor, que toma el certificado SSL del cliente como entrada y lo valida con el certificado raíz de CA que está configurado en ACOS.
111. Este punto se explica en el capítulo 10 “Configuring Multiple Factor Authentication (MFA) for Management Plane” de la guía “ACOS 5.2.1-P3 Management Access and Security Guide”, más concretamente en la página 160. La guía está disponible en el enlace: https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_MAS.pdf [REF 21]

6.7 SINCRONIZACIÓN

6.7.1 CONFIGURACIÓN HORARIA DEL SISTEMA Y DE LA RED

112. Una capacidad crítica para cualquier dispositivo de red seguro es mantener un sentido preciso del tiempo, como mínimo para garantizar sellos de tiempo confiables en el registro de auditoría, monitorear las sesiones del administrador para detectar inactividad y los períodos de bloqueo de la cuenta del administrador. Para ello, el dispositivo puede mantener la hora localmente como un dispositivo independiente cuando sea necesario, o en sincronía con la hora de la red cuando los servicios NTP estén disponibles.

6.7.1.1 CONFIGURACIÓN DE LA HORA DEL SISTEMA

113. El dispositivo mantiene la fecha/hora en función del reloj del sistema proporcionado por su hardware subyacente. Este sistema puede ser configurado (establecido) por el administrador usando los comandos CLI de reloj y zona horaria.

6.7.1.2 CONFIGURACIÓN DE TIEMPO DE RED (NTP)

114. El dispositivo admite hasta tres (3) servidores NTP para sincronizar el dispositivo con la fecha y la hora de la red con la comunicación protegida por el túnel IPsec en la configuración recomendada.
115. Los servidores NTP en la subred protegida IPsec se pueden configurar utilizando el comando `ntp server` CLI y extendiendo las ACL (*Access Control Lists*) para permitir el tráfico a través del túnel IPsec. La opción del comando `prefer` se puede usar para

designar uno de los servidores como una fuente NTP predeterminada con los servidores adicionales como fuentes NTP de tiempo de respaldo.

116. Confirmar la conectividad a los servidores NTP usando el comando *show ntp status* CLI que debería mostrar uno de los servidores con un estado "sincronizado" y los otros servidores como "sondeo". Si se pierde la conectividad con un servidor NTP sincronizado, el dispositivo intentará conectarse con los otros servidores configurados para mantener la sincronización con el dominio de tiempo de la red.
117. El dispositivo no es compatible con las actualizaciones de tiempo de *multicast* y *broadcast* NTP. El dispositivo solo se admite configuración de la versión 4 de NTP.
118. Las comunicaciones NTP están protegidas por túneles IPsec en la configuración recomendada.
119. Este punto se explica en la sección "*Setting the NTP Server*" de la guía "*ACOS 5.2.1-P3 System Configuration and Administration Guide*", más concretamente en la página 59. La guía está disponible en el enlace:

https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_SAG.pdf [REF 18]

6.8 ACTUALIZACIONES

120. La documentación referente a las actualizaciones está disponible en el sitio web de documentación de A10:
<https://documentation.a10networks.com/docs/ACOS/521x/5-2-1-p7/>
121. Adicionalmente, se recomienda consultar la sección "*Upgrading the Software Image Using aVCS*" del documento "*ACOS 5.2.1-P3 Release Notes*". El documento está disponible en el enlace [REF 20]:

6.9 AUTO-CHEQUEOS

122. Durante el arranque desde un encendido o un reinicio, el dispositivo realizará comprobaciones de integridad en el *software* del dispositivo y las capacidades criptográficas del dispositivo.
123. Se comprueba el correcto funcionamiento de los algoritmos de cifrado y las tarjetas criptográficas. Si alguna de estas pruebas falla, el dispositivo se pone en modo de fallo FIPS (estado específico A10 ACOS).
124. En este modo, el dispositivo operará con servicios de administración nominales disponibles solo desde la consola del dispositivo. La administración remota al dispositivo (rutas confiables), las conexiones a servidores externos (canales confiables) y los servicios del plano de datos del dispositivo tampoco estarán disponibles u operativos.
125. El modo de fallo de FIPS se indica por la falta general de disponibilidad del dispositivo en la infraestructura de la red y el siguiente aviso al iniciar sesión en la consola local del dispositivo:

ACOS(FIPS FAIL MODE)#

126. El chequeo de la verificación de integridad del software del dispositivo se puede confirmar observando los siguientes resultados.

ACOS(FIPS FAIL MODE)#show varlog | inc check failed

Sep 21 02:07:49 localhost a10mon: Image verification check failed

Sep 21 02:07:49 localhost a10mon: FIPS Power On Self Test failed. Enter FIPS fail mode

127. Alternativamente, el fallo de las capacidades criptográficas del dispositivo se puede confirmar observando los siguientes resultados.

ACOS(FIPS FAIL MODE)# show varlog | inc library power

Sep 21 20:53:36 localhost a10mon: FIPS library power on self test failed

Sep 21 20:53:36 localhost a10mon: FIPS Power On Self Test failed. Enter FIPS fail mode

128. Si ocurre esta condición, se deben tomar las siguientes acciones:

- Apagar y reiniciar el dispositivo para realizar estas pruebas nuevamente y determinar si se puede reanudar el funcionamiento normal.
- Si esta condición persiste, será necesario ponerse en contacto con el soporte de A10 Networks (<https://support.a10networks.com>) para solucionar el problema y coordinar el reemplazo del hardware, si es necesario.

6.10 ALTA DISPONIBILIDAD

129. VRRP-A es la implementación ACOS de alta disponibilidad. Permite que hasta ocho (8) dispositivos ACOS físicos o virtuales sirvan como copias de seguridad mutuas y permite proporcionar redundancia para los siguientes recursos IP:

- Direcciones IP del servidor virtual (VIP).
- Direcciones IP flotantes utilizadas como puertas de enlace predeterminadas por dispositivos descendentes.
- Grupos de NAT de IPv6.
- Grupos de NAT IPv4.
- Listas de rangos estáticos de IPv4 y asignaciones individuales para NAT de origen interno.

130. Es posible obtener información de la configuración de VRRP-A en el manual de implementación de VRRP-A disponible en el enlace de documentación: <https://documentation.a10networks.com/docs/ACOS/521x/5-2-1-p7/>

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

131. El registro de eventos de auditoría es compatible tanto localmente en el dispositivo como transmitido externamente a servidores Syslog remotos a través de IPsec.

6.11.2 ALMACENAMIENTO LOCAL

132. Las entradas de auditoría se generan y almacenan en dos (2) almacenes de registro en el dispositivo, uno para registros de categoría de auditoría ACOS y otro para registros de categoría de evento ACOS. Los registros de auditoría de ACOS son los que generan los administradores del sistema cuando realizan cambios en la configuración, ya sea a través de la GUI, la CLI o vía API (AXAPI). Sin embargo, los registros de tipo evento, son los que son generados por el propio sistema, como pueden ser los registros de tipo alerta, error, eventos del sistema operativo (ACOS), etc. Cada almacenamiento admite un registro circular con los registros más antiguos sobrescritos cuando el almacenamiento de registro está lleno.
133. La auditoría y el registro de eventos se habilitan a través del privilegio de habilitación de auditoría, y el registro de comandos CLI de nivel de registro almacenados en búfer, con el registro de eventos configurable para un rango seleccionado de gravedades de eventos. Los administradores del dispositivo deben habilitar estos servicios de registro.
134. Para habilitar el registro de auditoría de comandos y el registro de eventos para la notificación de eventos de emergencia se utilizan los siguientes comandos:
- ```
ACOS(config)# audit enable privilege
ACOS(config)# logging buffered notification
```
135. Estos registros almacenados localmente tienen un tamaño limitado y son circulares, de modo que los registros más antiguos se sobrescriben cuando sus respectivos almacenes están llenos. El tamaño de los almacenes de registro de eventos y auditoría se puede cambiar utilizando los comandos CLI *audit size* y *logging buffered max-messages*; respectivamente.
136. Las entradas del registro de auditoría se pueden ver con el comando *show audit* CLI. Las entradas del registro de eventos se pueden ver con el comando *show log* CLI.
137. Todos los administradores del dispositivo pueden ver estos registros. Solo los administradores de seguridad pueden habilitar/deshabilitar, borrar (eliminar) o modificar el tamaño de estos registros y ningún administrador puede modificar el contenido de los registros de ninguna manera. Si un administrador desactiva o borra un registro, se registra la auditoría de esta acción.
138. Los registros guardados localmente se pueden eliminar mediante los comandos de la CLI *clear audit* y *clear log*. El registro local para registros de categorías de

eventos y auditoría se puede desactivar mediante los comandos de la CLI *no audit enable* y *logging buffered disable*.

139. Este punto se explica en el capítulo 10 “*System Log Messages*” de la guía “*ACOS 5.2.1-P3 System Configuration and Administration Guide*”, más concretamente en la página 153. La guía está disponible en el enlace:

[https://documentation.a10networks.com/ACOS/521x/ACOS\\_5\\_2\\_1-P3/pdf/A10\\_5.2.1-P3\\_SAG.pdf](https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_SAG.pdf) [REF 18]

140. También se puede encontrar más información sobre los comandos descritos en este apartado en la guía “*ACOS 5.2.1-P3 Command Line Interface Reference*”. Para el comando “*audit*” en la página 155 y para “*logging buffered*” en la página 258. La guía está disponible en el enlace:

[https://documentation.a10networks.com/ACOS/521x/ACOS\\_5\\_2\\_1-P3/pdf/A10\\_5.2.1-P3\\_CLI.pdf](https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_CLI.pdf) [REF 15]

### 6.11.3 ALMACENAMIENTO REMOTO

141. Las entradas de categorías de eventos y auditoría se pueden registrar en servidores Syslog de confianza a través de IPsec en la configuración recomendada. Cuando se configura para iniciar sesión en uno o más servidores Syslog, los nuevos registros de auditoría y eventos se guardan en los almacenes locales de auditoría y registro de eventos, y se envían inmediatamente a los servidores Syslog a través del canal cifrado IPsec.
142. Se pueden configurar varios servidores Syslog en el dispositivo utilizando el comando CLI *logging host* una vez para cada servidor y extendiendo las ACL (*Access Control Lists*) para permitir el tráfico a través del túnel IPsec. Si usa el comando con la misma dirección IP que un servidor de registro existente, reemplaza cualquier configuración existente para ese servidor existente. Es decir, si existe un servidor configurado con la siguiente configuración “*logging host 10.10.10.1 port 514*”, que está enviando los mensajes de Syslog al servidor 10.10.10.1 al puerto 514 UDP y se ejecuta el siguiente comando “*logging host 10.10.10.1 port 4444*”, la configuración anterior para ese servidor existente será reemplazada y los mensajes de Syslog empezarán a ser enviados a ese mismo servidor (10.10.10.1), pero a través del puerto 4444 UDP. La opción de comando *use-mgmt-port* debe usarse para la configuración recomendada. Este comando sirve para indicar que se use la interfaz de gestión (*management port*) para establecer la conexión con el servidor Syslog remoto. La opción de comando de puerto permite configurar un servidor Syslog determinado para un puerto alternativo que no sea el 514 predeterminado.
143. Si las comunicaciones con un servidor Syslog se pierden y se restablecen, los nuevos registros se guardarán correctamente en el servidor. Los registros almacenados localmente mientras las comunicaciones con un servidor Syslog están inactivas se conservarán en los registros locales y no se registrarán (reenviarán) al servidor Syslog.

144. Este punto se explica en el capítulo 10 “*System Log Messages*” de la guía “ACOS 5.2.1-P3 *System Configuration and Administration Guide*”, más concretamente en la página 153. La guía está disponible en el enlace:

[https://documentation.a10networks.com/ACOS/521x/ACOS\\_5\\_2\\_1-P3/pdf/A10\\_5.2.1-P3\\_SAG.pdf](https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_SAG.pdf) [REF 18]

145. También se puede encontrar más información sobre los comandos descritos en este apartado en la guía “ACOS 5.2.1-P3 *Command Line Interface Reference*”. Para el comando “*audit*” en la página 155 y para “*logging host*” en la página 268. La guía está disponible en el enlace:

[https://documentation.a10networks.com/ACOS/521x/ACOS\\_5\\_2\\_1-P3/pdf/A10\\_5.2.1-P3\\_CLI.pdf](https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_CLI.pdf) [REF 15]

#### 6.11.4 ENTRADAS DE REGISTRO DE AUDITORÍA

146. Las entradas de auditoría se generan y almacenan en dos (2) almacenes de registro en el dispositivo, uno para registros de categoría de auditoría ACOS y otro para registros de categoría de evento ACOS.
147. La información en estos registros incluye la fecha y hora del evento, el tipo de evento, la identidad del sujeto del evento, la fuente del evento e información adicional relevante para el evento.

##### 6.11.4.1 REGISTROS DE EVENTOS

148. Los registros de categoría de eventos difieren ligeramente de los registros de categoría de auditoría, en particular porque incluyen un nivel de evento y un componente relacionado, al tiempo que incluyen el factor de éxito, fracaso e información, por la naturaleza de los mensajes registrados.

#### 6.12 BACKUP

149. De manera predeterminada, cuando se hace clic en el botón *Guardar* en la GUI o se ingresa el comando “*write memory*” en la CLI, todos los cambios de configuración no guardados se guardan en la configuración de inicio. La próxima vez que se reinicie el dispositivo ACOS, la configuración se volverá a cargar desde este archivo.
150. Además de estas sencillas opciones de gestión de la configuración, el dispositivo ACOS tiene opciones avanzadas de gestión de la configuración que le permiten guardar varios archivos de configuración. Es posible guardar archivos de configuración de forma remota en un servidor y localmente en el propio dispositivo ACOS.

**NOTA:**

Para obtener información sobre cómo administrar configuraciones para particiones separadas en un dispositivo ACOS, se recomienda consultar la Guía

de configuración de particiones de entrega de aplicaciones. Dicha guía se puede consultar en el siguiente enlace:

[https://documentation.a10networks.com/ACOS/521x/ACOS\\_5\\_2\\_1-P3/pdf/A10\\_5.2.1-P3\\_ADp.pdf](https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_ADp.pdf) [REF 22]

151. Para obtener información sobre cómo sincronizar la información de configuración entre varios dispositivos ACOS configurados para alta disponibilidad de VRRP-A, se recomienda consultar la Guía de configuración de alta disponibilidad de VRRP-A, en el siguiente enlace:

[https://documentation.a10networks.com/ACOS/521x/ACOS\\_5\\_2\\_1-P3/pdf/A10\\_5.2.1-P3\\_VRRP-A.pdf](https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_VRRP-A.pdf) [REF 23]

152. Para obtener instrucciones de actualización, se recomienda consultar las *Release Notes* de la versión de ACOS a la que planea actualizar.

### 6.12.1 DESCRIPCIÓN GENERAL DE LA COPIA DE SEGURIDAD DEL SISTEMA

153. El dispositivo ACOS permite realizar una copia de seguridad del sistema, los archivos de configuración individuales y las entradas de registro en servidores remotos. Es posible utilizar cualquiera de los siguientes protocolos de transferencia de archivos:

- Protocolo trivial de transferencia de archivos (TFTP)
- Protocolo de transferencia de archivos (FTP)
- Protocolo de copia segura (SCP)
- Protocolo de transferencia de archivos SSH (SFTP)

**NOTA:**

**No se recomienda el uso de los protocolos TFTP y FTP, al ser considerados inseguros.**

154. Se recomienda la configuración de la realización de *backups* periódicos del sistema.

**NOTA:**

No se admite la copia de seguridad del sistema desde una plataforma de hardware y su restauración a otra plataforma de hardware.

### 6.12.2 USO DE LA GUI PARA REALIZAR UNA COPIA DE SEGURIDAD

155. Para configurar la copia de seguridad mediante la GUI:

- 1) Ir a *System > Maintenance*.
- 2) En la barra de menú, hacer clic en *Backup*. En el menú desplegable que aparece, seleccionar uno de los siguientes:

- Sistema (*system*): esta opción realiza una copia de seguridad inmediata de los archivos de configuración, los scripts aFlex y los certificados y claves SSL.
  - Registro (*log*): esta opción realiza una copia de seguridad inmediata de las entradas de registro en el búfer Syslog del dispositivo ACOS (junto con cualquier archivo central en el sistema)
  - Copia de seguridad periódica (*Periodic Backup*): esta opción realiza una copia de seguridad programada del sistema o de los archivos de registro.
- 3) Completar la configuración de la copia de seguridad especificando la información necesaria (por ejemplo, el *host* y el puerto remotos, el protocolo de transferencia de archivos, la ubicación y el nombre del archivo de copia de seguridad y la información de acceso al sistema remoto).
156. Este punto se explica en el capítulo 8 “*Backing Up System Information*” de la guía “*ACOS 5.2.1-P3 System Configuration and Administration Guide*”, más concretamente en la página 83. La guía está disponible en el enlace:  
[https://documentation.a10networks.com/ACOS/521x/ACOS\\_5\\_2\\_1-P3/pdf/A10\\_5.2.1-P3\\_SAG.pdf](https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_SAG.pdf) [REF 18]

### 6.12.3 RESTAURAR DESDE UNA COPIA DE SEGURIDAD

157. Es posible usar una copia de seguridad guardada para restaurar el sistema actual; por ejemplo, si se está actualizando los dispositivos de la serie AX en la red a los dispositivos de la serie A10 Thunder más nuevos.
158. Esta sección contiene algunos aspectos importantes a tener en cuenta antes de realizar una operación de restauración:
- Memoria del sistema
    - Si el dispositivo actual tiene menos memoria que el dispositivo de respaldo (por ejemplo, 16 GB en el dispositivo actual, pero 32 GB en el dispositivo anterior), esto puede afectar negativamente el rendimiento del sistema.
  - FTA versus No FTA
    - Si se está restaurando desde un dispositivo FTA a un dispositivo no FTA, por ejemplo, es posible que algunos comandos no estén disponibles después de la operación de restauración.
  - Particiones L3V
    - Se restauran las particiones L3v y sus configuraciones; sin embargo, si se está restaurando a un dispositivo que admite una cantidad menor de particiones (por ejemplo, 32) que las que fueron configuradas desde el dispositivo de copia de seguridad (por ejemplo, 64), se

perderán todas las particiones y la configuración correspondiente más allá de 32.

- Asignación de puertos (*Port Mapping*)
  - Al restaurar desde un dispositivo que tiene una cantidad diferente de puertos, o incluso la misma cantidad de puertos, es posible asignar el número de puerto de la configuración anterior a un nuevo número de puerto (o el mismo número de puerto) en la nueva configuración.
  - En los casos en que la cantidad original de puertos sea mayor que la cantidad de puertos en el nuevo sistema, es posible que se pierda parte de la configuración.
  - Si se elige omitir la asignación de puertos, se conservan las configuraciones y los números de puerto originales. Si el dispositivo original tenía configurados los puertos del 1 al 10, y el nuevo dispositivo solo tiene los puertos del 1 al 8, y se omite la asignación de puertos, los puertos 9 y 10 se perderán. Si se elige la asignación de puertos, es posible decidir qué 8 de los 10 puertos originales se desea conservar durante el proceso de asignación de puertos.
- Los siguientes elementos no se restauran:
  - Configuraciones de VLAN.
  - Las configuraciones de VCS no son compatibles; para realizar una restauración y conservar las configuraciones de VCS, realizar la restauración mediante la GUI. Esta operación sobrescribe por completo la configuración en el sistema de destino y no proporciona las opciones disponibles en la CLI.

159. Para más información se recomienda consultar la página de documentación de A10: <https://glm.a10networks.com/documentation>

## 7. REFERENCIAS

- REF1** Datasheet licencia ADC  
<https://www.a10networks.com/wp-content/uploads/A10-DS-Thunder-ADC.pdf>
- REF2** Datasheet licencia CGN  
<https://www.a10networks.com/wp-content/uploads/A10-DS-Thunder-CGN.pdf>
- REF3** Datasheet licencia SSLi  
<https://www.a10networks.com/wp-content/uploads/A10-DS-Thunder-SSLi.pdf>
- REF4** Datasheet licencia cFW  
<https://www.a10networks.com/wp-content/uploads/A10-DS-Thunder-CFW.pdf>
- REF5** Sitio Web de soporte y descarga de versiones:  
<https://support.a10networks.com>
- REF6** Sitio Web de generación y control de licencias y registro de usuarios:  
<https://glm.a10networks.com>
- REF7** Documentación asociada al control de licencias y registro de usuarios:  
<https://glm.a10networks.com/documentation>
- REF8** Guías de alta de licencias y registro de usuarios:  
<https://documentation.a10networks.com/#licensing-guide>
- REF9** Documentación asociada a la instalación del dispositivo:  
<https://documentation.a10networks.com/#installation-guide>
- REF10** Documentación general de la solución, configuración e instalación.  
<https://documentation.a10networks.com/docs/ACOS/521x/5-2-1-p3/>
- REF11** Guía Lightweight Directory Access Protocol.  
[https://documentation.a10networks.com/ACOS/521x/ACOS\\_5\\_2\\_1-P7/html/mgmtsecurity\\_Responsive\\_HTML5/Content/mgmtsecurityTOC/mgmtsecurity-ldap.htm#mgmtsecurity-ldap\\_3582999530\\_1442657](https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P7/html/mgmtsecurity_Responsive_HTML5/Content/mgmtsecurityTOC/mgmtsecurity-ldap.htm#mgmtsecurity-ldap_3582999530_1442657)
- REF12** Guía de TAC (Technical Assistance Center)  
<https://www.a10networks.com/wp-content/uploads/A10-BR-Technical-Assistance-Center-Support-Guide.pdf>
- REF13** Página de política de ciclo de vida  
[https://support.a10networks.com/support/axseries/AX\\_Series\\_EOL\\_Policy](https://support.a10networks.com/support/axseries/AX_Series_EOL_Policy)
- REF14** Página de ciclo de vida  
<https://www.a10networks.com/support/end-of-sales/>



- REF15** Command Line Interface Reference Guide  
[https://documentation.a10networks.com/ACOS/521x/ACOS\\_5\\_2\\_1-P3/pdf/A10\\_5.2.1-P3\\_CLI.pdf](https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_CLI.pdf)
- REF16** Documentación de Productos  
<https://documentation.a10networks.com/#product>
- REF17** Guía de Configuración de IPSEC  
[https://documentation.a10networks.com/ACOS/521x/ACOS\\_5\\_2\\_1-P3/pdf/A10\\_5.2.1-P3\\_IPSEC.pdf](https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_IPSEC.pdf)
- REF18** Guía de Configuración y Administración del Sistema  
[https://documentation.a10networks.com/ACOS/521x/ACOS\\_5\\_2\\_1-P3/pdf/A10\\_5.2.1-P3\\_SAG.pdf](https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_SAG.pdf)
- REF19** Guía de balanceo de carga  
[https://documentation.a10networks.com/ACOS/521x/ACOS\\_5\\_2\\_1-P3/pdf/A10\\_5.2.1-P3\\_SLB.pdf](https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_SLB.pdf)
- REF20** Notas de versión  
[https://documentation.a10networks.com/ACOS/521x/ACOS\\_5\\_2\\_1-P3/html/relnotes\\_Responsive\\_HTML5/Default.htm#rel\\_original/relnotes\\_upgrade.htm](https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/html/relnotes_Responsive_HTML5/Default.htm#rel_original/relnotes_upgrade.htm)
- REF21** Guía de Gestión de Acceso y Seguridad  
[https://documentation.a10networks.com/ACOS/521x/ACOS\\_5\\_2\\_1-P3/pdf/A10\\_5.2.1-P3\\_MAS.pdf](https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_MAS.pdf)
- REF22** Guía de Configuración de Particiones  
[https://documentation.a10networks.com/ACOS/521x/ACOS\\_5\\_2\\_1-P3/pdf/A10\\_5.2.1-P3\\_ADG.pdf](https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_ADG.pdf)
- REF23** Guía de configuración de alta disponibilidad de VRRP-A  
[https://documentation.a10networks.com/ACOS/521x/ACOS\\_5\\_2\\_1-P3/pdf/A10\\_5.2.1-P3\\_VRRP-A.pdf](https://documentation.a10networks.com/ACOS/521x/ACOS_5_2_1-P3/pdf/A10_5.2.1-P3_VRRP-A.pdf)

## 8. ABREVIATURAS

|              |                                                                                    |
|--------------|------------------------------------------------------------------------------------|
| <b>ACL</b>   | <i>Access Control List</i>                                                         |
| <b>ACOS</b>  | <i>Advanced Core Operating System</i>                                              |
| <b>ADC</b>   | <i>Application Delivery Controller</i>                                             |
| <b>AES</b>   | <i>Advanced Encryption Standard</i>                                                |
| <b>AH</b>    | <i>Authentication Header</i>                                                       |
| <b>AXAPI</b> | <i>A10 AX Application Programming Interface CA Certificate Authority</i>           |
| <b>CBC</b>   | <i>Cipher Block Chaining</i>                                                       |
| <b>CC</b>    | <i>Common Criteria</i>                                                             |
| <b>CFW</b>   | <i>Convergent Firewall</i>                                                         |
| <b>CGN</b>   | <i>Carrier-Grade NAT</i>                                                           |
| <b>CLI</b>   | <i>Command-line interface</i>                                                      |
| <b>CMVP</b>  | <i>Cryptographic Module Validation Program CRL Certificate Revocation List</i>     |
| <b>CSR</b>   | <i>Certificate Signing Requests</i>                                                |
| <b>DES</b>   | <i>Data Encryption Standard</i>                                                    |
| <b>DH</b>    | <i>Diffie-Hellman</i>                                                              |
| <b>DNS</b>   | <i>Domain Name System</i>                                                          |
| <b>ECDSA</b> | <i>Elliptic Curve Digital Signature Algorithm</i>                                  |
| <b>ENS</b>   | <i>Esquema Nacional de Seguridad</i>                                               |
| <b>ESP</b>   | <i>Encapsulating Security Payload</i>                                              |
| <b>FIPS</b>  | <i>Federal Information Processing Standards GCM Galois Counter Mode</i>            |
| <b>GUI</b>   | <i>Graphical User Interface</i>                                                    |
| <b>HMAC</b>  | <i>Keyed-Hash Message Authentication Code HTTP HyperText Transfer Protocol</i>     |
| <b>HTTPS</b> | <i>HyperText Transfer Protocol Secure</i>                                          |
| <b>ICMP</b>  | <i>Internet Control Message Protocol</i>                                           |
| <b>IKE</b>   | <i>Internet Key Exchange</i>                                                       |
| <b>IP</b>    | <i>Internet Protocol</i>                                                           |
| <b>IPsec</b> | <i>Internet Protocol Security</i>                                                  |
| <b>LDAPS</b> | <i>Lightweight Directory Access Protocol Secure MD5 Message-Digest algorithm 5</i> |
| <b>NAT</b>   | <i>Network Address Translation</i>                                                 |

|               |                                                                                                                                      |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>NDcPP</b>  | <i>Network Device collaborative Protection Profile NIST National Institute of Standards and Technology NTP Network Time Protocol</i> |
| <b>OS</b>     | <i>Operating System</i>                                                                                                              |
| <b>OCSP</b>   | <i>Online Certificate Status Protocol PP Protection Profile</i>                                                                      |
| <b>PKI</b>    | <i>Public Key Infrastructure</i>                                                                                                     |
| <b>PRF</b>    | <i>Pseudo Random Function</i>                                                                                                        |
| <b>PSK</b>    | <i>Pre-Shared Key</i>                                                                                                                |
| <b>QSFP</b>   | <i>Quad (4-channel) Small Form-factor Pluggable</i>                                                                                  |
| <b>QSFP28</b> | <i>Quad (4-channel) Small Form-factor Pluggable 28 GB data RADIUS Remote Authentication Dial-In User Service</i>                     |
| <b>RSA</b>    | <i>Rivest Shamir Adleman Algorithm</i>                                                                                               |
| <b>SA</b>     | <i>Security Associations (IPSec)</i>                                                                                                 |
| <b>SCP</b>    | <i>Secure Copy Protocol</i>                                                                                                          |
| <b>SFP</b>    | <i>Small Form-factor Pluggable</i>                                                                                                   |
| <b>SFTP</b>   | <i>Secure File Transfer Protocol</i>                                                                                                 |
| <b>SHA</b>    | <i>Secure Hash Algorithm</i>                                                                                                         |
| <b>SSD</b>    | <i>Solid State Disk</i>                                                                                                              |
| <b>SSH</b>    | <i>Secure Shell</i>                                                                                                                  |
| <b>SSLi</b>   | <i>SSL Intercept</i>                                                                                                                 |
| <b>TACACS</b> | <i>Terminal Access Controller Access-Control System</i>                                                                              |
| <b>TCP</b>    | <i>Transmission Control Protocol</i>                                                                                                 |
| <b>TLS</b>    | <i>Transport Layer Security</i>                                                                                                      |
| <b>UDP</b>    | <i>User Datagram Protocol</i>                                                                                                        |
| <b>VPN</b>    | <i>Virtual Private Network</i>                                                                                                       |

