Guía de Seguridad de las TIC
CCN-STIC 1484

Procedimiento de Empleo Seguro
SDE-1x Series y SDE-2x Series

Julio 2026

Edita:

Centro Criptológico Nacional, 2026

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.07.28 09:31:07 +02'00'

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1 INTRODUCCIÓN

Los **dispositivos SDE** son una familia de *edge-routers* corporativos diseñada para ofrecer comunicaciones fiables y seguras, tanto en redes físicas como en la nube, incorporando según el modelo múltiples tecnologías de conexión (WAN, WWAN, LAN, WLAN) para adaptarse a cualquier escenario y garantizar los niveles de servicio que las empresas requieren. Estos equipos integran capacidades de firewalling avanzado, que protegen de forma inteligente y dinámica el tráfico corporativo. Combinados con las soluciones be.SDx (SD-WAN/SD-Branch), be.Safe Pro (SSE/SASE/ZTNA), be.Safe XDR (XDR/NTA) de Teldat, permiten optimizar y centralizar la gestión de la red, reforzar la seguridad perimetral y la protección frente a amenazas, y detectar y responder automáticamente a ciberataques, facilitando el despliegue de servicios digitales y mejorando el rendimiento, la integridad y la seguridad de las comunicaciones.

La configuración y gestión de sus funcionalidades se realiza de forma intuitiva mediante una consola de línea de comandos (CLI). Esta interfaz permite acceder y administrar los dispositivos tanto localmente como de manera remota, mediante protocolos seguros como SSHv2, garantizando así el cumplimiento de los estándares de seguridad establecidos por la normativa del ENS.

Estos dispositivos ofrecen distintas funcionalidades destacables en relación con la gestión de la red:

a) **Soporte de múltiples tipos de acceso WAN.**
   Gestión simultánea de diferentes accesos WAN para crear redes híbridas bajo control centralizado.
b) **Firewall integrado y políticas de seguridad.**
   Protección del tráfico de la red mediante cortafuegos de próxima generación y aplicación de políticas de seguridad centralizadas.
c) **Segmentación de red mediante VLAN.**
   Posibilidad de definir y gestionar VLANs para separar y controlar el tráfico dentro de la red, garantizando aislamiento y seguridad de datos.
d) **Asignación de prioridades del tráfico entrante (QoS).**
   Permite priorizar el tráfico según tipo de aplicación o servicio, garantizando rendimiento óptimo de aplicaciones críticas.
e) **Capacidad de crear banners.**
   Posibilidad de configurar mensajes de bienvenida, advertencia o información legal que se muestran al iniciar sesión en los dispositivos.
f) **Registro y trazabilidad de eventos (logging).**
   Generación de logs centralizados para monitorización de seguridad, auditorías, análisis de problemas y cumplimiento normativo.

2 OBJETO Y ALCANCE

El presente documento tiene como objeto detallar la integración y operación segura de los dispositivos SDE en la infraestructura del cliente. Asimismo, especifica las configuraciones necesarias para que los dispositivos cumplan con los estándares establecidos por las taxonomías bajo las cuales se han cualificado, que incluyen la familia de Enrutadores [REF1], familia de Switches [REF2] y familia de Cortafuegos [REF3].

El alcance de los dispositivos evaluados comprende:

a) La versión **v4.2.1.3** del *firmware.*
b) Los siguientes modelos de *hardware:*
    i) **SDE-1x Series**
    ii) **SDE-2x Series**
c) La interfaz utilizada para la configuración, gestión y diagnóstico de los dispositivos:
    i) **Interfaz de línea de comandos (CLI),** que permite el acceso tanto local —mediante la conexión de un teclado a través del puerto USB y un monitor mediante el puerto VGA— como remoto, a través del protocolo SSH.

Estos dispositivos han sido incluidos en el catálogo CPSTIC. Para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF11].

3 ORGANIZACIÓN DEL DOCUMENTO

El presente documento se estructura en las secciones indicadas a continuación:

a) **Apartado 4**. Este apartado recoge los aspectos y recomendaciones que deberán considerarse antes de proceder a la instalación del producto.
b) **Apartado 5**. Este apartado recoge las recomendaciones que deberán tenerse en cuenta durante la fase de instalación del producto.
c) **Apartado 6**. Este apartado recoge las recomendaciones que deberán considerarse durante la fase de configuración del dispositivo, con el objetivo de lograr una configuración segura.
d) **Apartado 7**. En este apartado se recogen las tareas recomendadas para la fase de operación y mantenimiento del producto.
e) **Apartado 8**. En este apartado se recogen las referencias utilizadas en la presente guía de empleo seguro.
f) **Apartado 9**. En este apartado se recogen las abreviaturas utilizadas en la presente guía de empleo seguro.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

Las organizaciones interesadas en los **dispositivos SDE** pueden adquirirlos a través de la página web de TELDAT (https://www.teldat.com/), acudiendo al apartado "CONTACT US". Aquí podrán expresar el interés de adquirir el modelo, donde se debe indicar que desean obtenerlo con los ajustes necesarios para cumplir con la evaluación LINCE y las medidas de seguridad del ENS.

Tras la gestión contractual entre la parte interesada y TELDAT, el equipo de TELDAT hará efectivo el envío del producto a la dirección especificada por la parte interesada, aportando el número de seguimiento correspondiente al envío.

En su recepción, la parte interesada deberá poner atención al empaquetado verificando que este no ha sido manipulado durante su transporte. El receptor deberá comprobar que el contenido del paquete se corresponde con lo indicado en la etiqueta de la caja. Si se observa que la etiqueta está rota o no está presente, contacte con el proveedor del producto.

Una vez el producto se ha desempaquetado, compruebe que el modelo, el número de serie y el identificador UUID (Universal Unique IDentifier) que aparece en el propio producto coincide con el modelo, número de serie e identificador UUID de la caja.

El producto que se entrega incluye el hardware y el firmware que compone el producto. Junto con el dispositivo, se incluye una tarjeta informativa en la que se indica la URL de acceso a la documentación técnica y a los manuales correspondientes.

Además, es posible acceder a los manuales y documentación técnica a través de la página web oficial de TELDAT [REF5].

TELDAT mantendrá la comunicación con las partes interesadas empleando direcciones de correo electrónico bajo el domino @teldat.com asegurando una comunicación directa y eficaz.

4.2 ENTORNO DE INSTALACIÓN SEGURO

El dispositivo debe instalarse en una ubicación física segura, cuyo acceso estará limitado a un conjunto de personas que posean una autorización expresa. Se espera que el producto se instale en un rack protegido, dentro de una sala de comunicaciones accesible solo a personal autorizado.

4.3 REGISTRO Y LICENCIAS

Las licencias para los dispositivos se proporcionan de dos formas distintas:

a) El cliente recibirá un correo electrónico con las licencias necesarias, estas se encuentran asignadas al identificador UUID del equipo en específico. Para dar de alta la licencia, el cliente debe cargar el archivo en la memoria flash del dispositivo. Una vez finalizada la carga, es necesario reiniciar el dispositivo para aplicar los cambios.
b) El cliente recibirá el producto con las licencias ya embebidas, siguiendo la orden del pedido, esta forma de entrega se denomina "*from-factory*".

4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN

A continuación, se detalla la arquitectura recomendada y los componentes esenciales que deben estar presentes en el entorno de operación de los dispositivos SDE:

a) **VLAN y WAN:** Una o más redes VLAN y WAN configuradas para la correcta segmentación y comunicación de la red.
b) **Servidor SYSLOG:** Es indispensable para el almacenamiento de los registros de auditoría, permitiendo el seguimiento y control de eventos.
c) **Servidor NTP:** Se recomienda que el entorno operativo incluya un servidor NTP autenticado para una sincronización precisa de la hora en tiempo real. Sin embargo, la ausencia de un servidor NTP en el entorno operativo no afecta a la funcionalidad de seguridad ya que los usuarios administradores tienen la opción de configurar manualmente el reloj del dispositivo.

El diagrama presentado proporciona un modelo orientativo del entorno operacional:

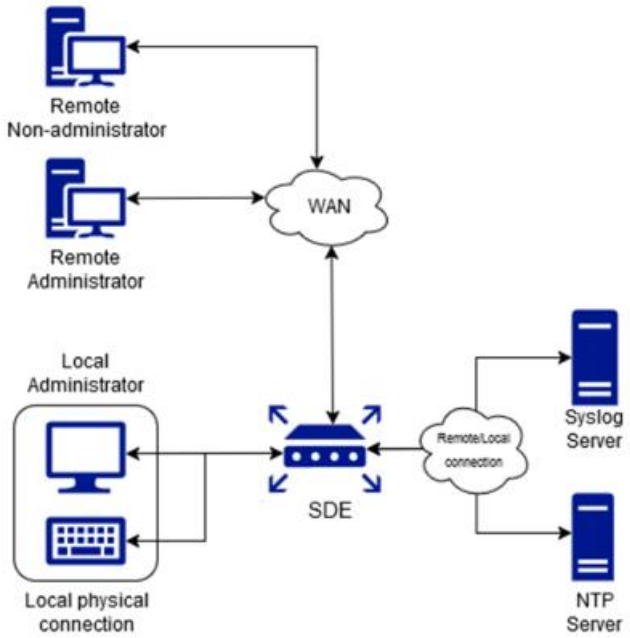

Ilustración 1. Infraestructura del cliente

La gestión del dispositivo será realizada exclusivamente por usuarios con privilegios administrativos, mediante acceso local o mediante acceso remoto de administración a través de las redes operacionales autorizadas, LAN/VLAN o WAN, según la arquitectura desplegada, utilizando una conexión Ethernet y protocolos seguros como SSHv2, IPsec o TLS."

Para ello, el administrador requiere un puesto de trabajo que cumpla, al menos, los siguientes requisitos mínimos:

a) Procesador compatible con la arquitectura x86-64.
b) Al menos 2 GB de memoria RAM.
c) Capacidad variable de almacenamiento persistente.
d) Adaptador de red con soporte para conexión Ethernet.

Adicionalmente, el dispositivo puede integrarse con un **servidor SYSLOG** y un **servidor NTP**. Dichos servidores pueden configurarse tanto de forma local como remota; habitualmente, se encuentran desplegados en la red local donde opera el dispositivo.

4.5 CONSIDERACIONES PREVIAS

Las credenciales por defecto son usuario **admin** y contraseña **admin**. Estas credenciales deben utilizarse únicamente para el acceso inicial al dispositivo y la contraseña debe modificarse de forma inmediata al activar el modo de operación seguro. El dispositivo obligará a realizar dicho cambio durante el proceso de activación.

Para que las configuraciones descritas en las siguientes secciones se apliquen correctamente, es necesario seguir los siguientes pasos:

a) Aplicar los cambios realizados mediante el comando:

```
commit
```

b) Guardar la configuración para que esta sea persistente entre reinicios del sistema mediante el comando:

```
save
```

5 FASE DE INSTALACIÓN

El dispositivo admite distintos modos de instalación. No obstante, se recomienda de manera preferente su instalación en un **rack** adecuado, con el objetivo de garantizar una correcta ventilación, una gestión ordenada del cableado y un acceso seguro para las tareas de operación y mantenimiento. En cualquier caso, el lugar de instalación deberá ser un entorno **aislado y controlado**, al que únicamente tenga acceso el **personal debidamente autorizado**.

Una vez instalado el dispositivo, es necesario realizar la configuración inicial:

a) Acceder al dispositivo. El acceso puede realizarse tanto por consola local como a través de SSH. Las credenciales predeterminadas son el usuario **admin** y la contraseña **admin**. Por motivos de seguridad, dichas credenciales deben utilizarse únicamente para el acceso inicial. Durante la activación del modo de operación seguro, el dispositivo requerirá obligatoriamente el cambio de la contraseña predeterminada.

   i) Para el acceso por consola local, es necesario disponer de un monitor y un teclado conectados directamente al dispositivo, mediante un cable VGA y un puerto USB, respectivamente.

   ii) Para el acceso remoto mediante SSH, basta con conectar el dispositivo a la red local a través de uno de los puertos SFP. El sistema intentará obtener automáticamente una dirección IP mediante el protocolo DHCP; en caso de no recibir una asignación, utilizará por defecto la dirección IP 192.168.1.1.

b) Acceder al modo de configuración con el comando:

```
configure
```

c) Eliminar la configuración asociada a la herramienta CNM *(Cloud Net Manager)* con el siguiente comando dado que dicha funcionalidad queda fuera del alcance de la evaluación:

```
delete service cnm
```

d) Configurar el nombre del dispositivo mediante el comando:

```
set system host-name <1-63 chars>
```

e) Configurar la puerta de enlace mediante el comando:

```
set protocols static route 0.0.0.0/0 next-hop <x.x.x.x>
```

f) Aplicar la configuración con el comando:

```
commit
```

g) Guardar la configuración de forma persistente con el comando:

```
save
```

Una vez finalizada la configuración inicial, es necesario comprobar que la versión del dispositivo es la esperada (en este caso v4.2.1.3). Para ello:

a) Salir del modo de configuración con el comando:

```
exit
```

b) Para verificar la versión instalada ejecutar el siguiente comando:

```
show version
```

c) Identificar en la salida del comando la versión de software instalada:

```
OS version:                    v4.2.1.3
```

Si la versión instalada no es la adecuada y fuera anterior a la versión cualificada, es necesario descargar dicha versión. Las distintas versiones se encuentran disponibles en el portal de soporte, previo registro del cliente.

Con la versión descargada, hacer la instalación en el dispositivo. Para ello existen varios mecanismos:

NOTA: Los métodos de instalación basados en descarga desde URL requieren que el dispositivo disponga previamente de conectividad de red operativa y configurada conforme a las directrices de seguridad establecidas; en caso de que el sistema se encuentre en una fase inicial de puesta en servicio o no se haya verificado dicha conectividad, deberá emplearse exclusivamente el método de instalación mediante transferencia manual.

a) Desde una URL preconfigurada. En este modo, el dispositivo descarga el firmware desde una URL configurada previamente en el sistema, que se utiliza como origen por defecto para los procesos de actualización. Los pasos son los siguientes:

i) Acceder al modo de configuración ejecutando el comando:

```
configure
```

ii) Configurar la URL donde se encuentre la versión con el comando:

```
set system image default-url <url>
```

iii) Ejecutar el siguiente comando para aplicar el cambio realizado:

```
commit
```

iv) De forma opcional, guardar la configuración mediante el siguiente comando con el fin de mantener esta URL configurada de manera persistente:

```
save
```

v) Salir del modo de configuración mediante la ejecución del comando:

```
exit
```

vi) Ejecutar el siguiente comando para instalar la versión:

```
image add default-url
```

vii) Reiniciar el dispositivo con el comando:

```
reboot
```

b) Desde una URL indicada en el momento de la actualización sin modificar la configuración del dispositivo. Para ello:

i) Ejecutar el comando:

```
image add <url>
```

ii) Reiniciar el dispositivo mediante la ejecución del comando:

```
reboot
```

c) Desde el propio dispositivo mediante transferencia manual. Los pasos son los siguientes:

i) Importar el firmware al dispositivo mediante la ejecución del siguiente comando o mediante el uso del protocolo SCP, actuando el dispositivo como servidor de la sesión:

```
file copy <url>
```

ii) Ejecutar el siguiente comando para instalar la nueva versión del firmware.

```
image add <filename>
```

iii) Reiniciar el dispositivo con el comando:

```
reboot
```

Al instalar la versión se realiza una verificación de la firma digital. Si la firma no es válida el dispositivo rechaza la actualización.

Una vez que el dispositivo se ha reiniciado, comprobar que la versión se ha instalado correctamente ejecutando nuevamente el comando:

```
show version
```

La **URL utilizada durante el proceso de actualización del firmware debe emplear obligatoriamente el protocolo HTTPS**, con el fin de garantizar la confidencialidad e integridad de los datos transmitidos. El uso de HTTPS permite asegurar la autenticidad del servidor de origen y protege el proceso de descarga frente a accesos no autorizados, manipulaciones o ataques de intermediario, contribuyendo así a la seguridad y fiabilidad del proceso de actualización del dispositivo.

Las actualizaciones solo pueden ser efectuadas por usuarios con **privilegios administrativos máximos (nivel 15)**. Cabe destacar que el dispositivo **no sobrescribe la versión anterior** del firmware, sino que la **mantiene y añade la nueva versión**. Es posible consultar todas las versiones de firmware instaladas en el dispositivo mediante la ejecución del comando:

```
image show
```

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

Antes de conectar el dispositivo a una red con acceso a internet, es imprescindible activar el **modo de operación seguro** para que el dispositivo funcione con la configuración acorde a unos requisitos de seguridad determinados y, por tanto, funcione de acuerdo con las garantías de seguridad requeridas.

Cuando el modo de operación seguro está habilitado, el dispositivo realiza las siguientes acciones:

a) Limita configuraciones consideradas inseguras en el dispositivo, como TELNET o SNMP, entre otras.

b) Aplica configuraciones predeterminadas relacionadas con la autenticación y el control de acceso al dispositivo.

c) Encripta las contraseñas para impedir su visibilidad a agentes externos.

d) Configura contraseñas seguras según las políticas de seguridad establecidas.

e) Restringe el uso de algoritmos criptográficos para garantizar el nivel de seguridad requerido.

f) Genera automáticamente un archivo en el que se registran diversos eventos del dispositivo.

Todas las funciones y algoritmos criptográficos proporcionados por el dispositivo se implementan mediante los siguientes módulos:

a) *Rsyslog:* Es una implementación multihilo de syslogd (una utilidad del sistema que proporciona soporte para el registro de mensajes).

b) *Openssl:* Contiene el binario de línea de comandos de uso general /usr/bin/openssl, útil para operaciones criptográficas.

c) *OpenSSH:* Una implementación “open-source” del protocolo Secure Shell.

d) *Strongswan:* Solución VPN basada en IPsec de código abierto, modular y portátil.

e) *Pycryptodome:* Es un paquete Python autocontenido de primitivas criptográficas de bajo nivel.

f) *Whois*: Contiene la utilidad *mkpasswd*, una interfaz con numerosas funciones para la encriptación de contraseñas.

g) *NTPSec*: Se utiliza para mantener la precisión de los relojes de los dispositivos sincronizándolos a través de Internet o de una red local.

En el **modo de operación seguro**, se deshabilitan los algoritmos criptográficos considerados débiles, permitiéndose únicamente el uso de **algoritmos y funciones criptográficas seguras de acuerdo con la normativa de seguridad criptográfica del CCN**. La siguiente tabla detalla los algoritmos criptográficos habilitados cuando el dispositivo opera en este modo:

Módulo criptográfico	Función	Algoritmos criptográficos
TLS	Cipher Suites TLS1.3	TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_AES_128_CCM_SHA256 TLS_CHACHA20_POLY1305_SHA256
	Cipher Suites TLS1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_CCM TLS_ECDHE_ECDSA_WITH_AES_256_CCM TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
SSH	Host key and Public Key Authentication algorithms	ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521
	MAC algorithms	hmac-sha2-256 hmac-sha2-512
	Key exchange algorithms	diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521
	Encryption algorithms	aes128-ctr aes192-ctr aes256-ctr
IPSEC	Key exchange algorithms	Diffie-Hellman group 15 (3072-bit MODP Group) Diffie-Hellman group 16 (4096-bit MODP Group) Diffie-Hellman group 17 (6144-bit MODP Group) Diffie-Hellman group 18 (8192-bit MODP Group) Diffie-Hellman group 19 (256-bit random ECP group) Diffie-Hellman group 20 (384-bit random ECP group) Diffie-Hellman group 21 (521-bit random ECP group)
	Encryption Algorithms	aes128gcm128 aes192gcm128 aes256gcm128 chacha20poly1305
	Hash functions	sha256 sha384 sha512
NTP	Authentication algorithms	sha256 sha384 sha512
	Cipher	AES-256-CBC

Claves privadas	Elliptic curves	P-256 P-384
Credenciales de usuario	Method type	sha512
Otras credenciales	Message digest	sha512
	Ciphers	AES-256-CBC

Tabla 1: Tabla algoritmos criptográficos habilitados

Los parámetros críticos de seguridad (CSPs) que maneja el dispositivo son los siguientes:

CSP	Descripción	Funciones y algoritmos criptográficos empleados
SSH Host Key Privada	Claves SSH utilizadas para identificar el dispositivo como servidor SSH. Se generan en la configuración inicial del dispositivo.	Ecdsa de 256 bits
SSH Session Key	Claves de sesión SSH usadas para el cifrado y el establecimiento de claves.	hmac-sha2-256 hmac-sha2-512 aes128-ctr aes192-ctr aes256-ctr diffie-hellman-group16-sha512 diffie-hellman-group18-sha512
SSH Authentication Algorithms	Algoritmos SSH usados para la autenticación.	ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521
Contraseñas de usuarios	Contraseñas de los usuarios para su autenticación.	sha512

Tabla 2: Tabla CSPs

A continuación, se muestran los pasos resumidos para **configurar el modo de operación seguro** desde la interfaz de comandos CLI:

a) Acceder al modo de configuración con el comando:

```
configure
```

b) A continuación, activar el modo de operación seguro ejecutando el siguiente comando:

```
set system security medium
```

c) Modificar la contraseña del usuario administrador por defecto **admin** por una contraseña segura basada en la siguiente política: Debe contener al menos 12 caracteres y debe incluir mayúsculas, minúsculas, números y al menos uno de los siguientes caracteres especiales (‘!’, ‘@’, ‘#’, ‘$’, ‘%’, ‘^’, ‘&’, ‘*’, ‘(‘, ‘)’). Para ello, usar el comando:

```
set system login admin authentication plaintext-password
<txt>
```

d) Aplicar los cambios con el comando:

```
commit
```

Esto provocará la finalización de la sesión actual, por lo que será necesario volver a iniciar sesión en el dispositivo utilizando las credenciales correspondientes.

e) Guardar los cambios mediante la ejecución del siguiente comando para que persistan después de un reinicio del dispositivo.

```
save
```

Una vez configurado el modo de operación seguro, el dispositivo realiza **automáticamente**, en cada reinicio, las **verificaciones** correspondientes **durante el arranque para garantizar la integridad de la versión del firmware**.

Para verificar que el dispositivo está en modo de operación seguro, salir del modo de configuración con el comando:

```
exit
```

Y ejecutar el comando:

```
Show running
```

```
set system security medium
```

Una vez activado el modo de operación seguro, el dispositivo estará preparado para su conexión a internet. A partir de este momento, puede continuarse con el resto del proceso de configuración, asegurando así una operación segura del dispositivo.

6.2 AUTENTICACIÓN

Los mecanismos de autenticación empleados por el dispositivo para verificar la identidad de los usuarios son los siguientes:

a) **Autenticación mediante nombre de usuario y contraseña:** Utilizada para el acceso al dispositivo a través de consola y mediante el protocolo SSH.

b) **Autenticación mediante nombre de usuario y clave pública:** Utilizada para el acceso al dispositivo a través del protocolo SSH.

Los mecanismos de autenticación empleados por el dispositivo para autenticarse frente a otros sistemas o dispositivos son los siguientes:

a) **Certificado TLS/SSL:** Utilizado para la comunicación con un servidor SYSLOG externo y para el establecimiento de túneles IPsec.

b) **Clave precompartida con cifrado SHA-256, SHA-384 o SHA-512:** Utilizada para las comunicaciones con un servidor NTP externo.

6.2.1 AUTENTICACIÓN DE USUARIOS

6.2.1.1 AUTENTICACIÓN CON NOMBRE DE USUARIO Y CONTRASEÑA

Para crear un nuevo usuario, es necesario acceder al modo configuración con el comando:

```
configure
```

Y, a continuación, ejecutar el siguiente comando donde se especifica la contraseña en plano:

```
set system login user <user> authentication plaintext-password
<txt>
```

Las **contraseñas de los usuarios** son almacenadas localmente en el dispositivo usando el algoritmo de hash **SHA512**.

En la autenticación mediante contraseña, el dispositivo incorpora mecanismos de seguridad que incluyen el bloqueo de usuarios tras varios intentos fallidos, retardos temporales entre intentos, límites de tiempo para el acceso correcto y períodos de inactividad, con el fin de prevenir ataques de fuerza bruta.

Política de contraseñas: Las contraseñas del dispositivo deben seguir el siguiente criterio cuando se habilita el modo de operación seguro: Debe incluir mayúsculas, minúsculas, números, al menos una longitud mínima de 12 caracteres y conteniendo al menos uno de los siguientes caracteres especiales (‘!’, ‘@’, ‘#’, ‘$’, ‘%’, ‘^’, ‘&’, ‘*’, ‘(‘, ‘)’).

6.2.1.2 AUTENTICACIÓN MEDIANTE CLAVE PÚBLICA SSH

En la autenticación mediante clave pública SSH, el usuario proporciona su nombre de usuario y demuestra la posesión de la clave privada correspondiente a la clave pública almacenada en el dispositivo para dicho usuario.

Cuando se habilita el **modo de operación seguro**, los algoritmos de clave pública permitidos son los siguientes: **ecdsa-sha2-nistp521**, **ecdsa-sha2-nistp384** y **ecdsa-sha2-nistp256**.

Para configurar la clave pública de un usuario, el dispositivo permite dos métodos distintos:

a) Importar la clave mediante el siguiente comando operacional o utilizando el protocolo SCP con el dispositivo actuando como servidor de la sesión:

```
file copy <url>
```

b) Se puede configurar generando un par de claves (pública y privada) directamente en el dispositivo mediante el comando operacional:

```
pki
```

Una vez configurada la clave en el dispositivo, se debe acceder al modo configuración mediante el comando:

```
configure
```

Y vincular el usuario con la clave correspondiente utilizando el comando:

```
set system login user <user> authentication public-key <filename>
```

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

La interfaz de línea de comandos (CLI) del dispositivo constituye la interfaz de software utilizada para acceder al dispositivo, supervisar su funcionamiento y modificar su configuración según sea necesario. El acceso a la CLI se realizará a través de los siguientes medios:

a) **Interfaces de gestión local**: mediante un monitor conectado por cable VGA para la visualización y un teclado para la interacción y operación.

b) **Protocolos de gestión remota**: mediante una conexión SSH. Se recomienda exclusivamente el uso de **SSHv2** como protocolo de gestión remota. El protocolo Telnet no está disponible cuando el dispositivo opera en modo de operación seguro.

A continuación, se presentan conceptos fundamentales que resultan necesarios para la comprensión de los apartados posteriores de este documento. Para obtener información detallada sobre la operativa de la CLI v4.2.1.3 CLI y sus comandos, se remite a la guía v4.2.1.3 [REF5].

La interfaz CLI tiene dos (2) modos:

a) **Modo Operacional**: Este modo permite la ejecución de acciones basadas en la configuración del dispositivo. Los comandos disponibles facilitan la visualización de información relevante del sistema, así como la realización de tareas de monitorización y comunicación con otros dispositivos. Entre los comandos más utilizados se encuentran los siguientes:

i) Muestra información resumida del dispositivo, incluyendo el sistema operativo, el hardware y el estado general del sistema.

```
show version
```

ii) Proporciona información básica sobre el estado de las interfaces.

```
interfaces show
```

iii) Permite apagar el dispositivo.

```
poweroff
```

iv) Permiten reiniciar el dispositivo.

```
reboot
```

v) Muestra la configuración que se encuentra actualmente activa en el dispositivo.

```
show running
```

Para obtener información adicional sobre estos y otros comandos, se recomienda consultar el correspondiente apartado de la guía de configuración y monitorización del producto [REF5].

La sintaxis del prompt en este modo es la siguiente: `<user>@<hostname>$`.

b) **Modo Configuración**: Este modo permite modificar la configuración del dispositivo con el fin de ajustar su comportamiento. Para ello, se emplean los comandos `set` y `delete`, seguidos del nodo de configuración correspondiente.

Los nodos de configuración se estructuran conforme a la finalidad que cumple cada uno en el dispositivo, a saber:

i) *interfaces*: Configuración de las interfaces de red.

ii) *protocols*: Configuración de los protocolos de enrutamiento.

iii) *service*: Configuración de los servicios que proporciona el dispositivo.

iv) *system*: Configuración de los parámetros del sistema del dispositivo.

v) *traffic*: Configuración de los elementos de clasificación y filtrado del tráfico entrante o saliente del dispositivo.

vi) *user-level:* Configuración de privilegios para la ejecución de comandos específicos (no disponible en modo seguro).

vii) *vpn*: Configuración de redes privadas virtuales.

Para obtener información detallada sobre la configuración activa, así como sobre aquella que ha sido añadida, eliminada o modificada, se emplean los siguientes comandos:

i) Muestra la configuración actualmente activa:

```
show running
```

ii) Muestra la configuración incluyendo los cambios no confirmados:

```
show working
```

iii) Muestra las diferencias existentes entre las configuraciones mostradas por los dos comandos anteriores:

```
show changes
```

Para consultar el conjunto completo de comandos disponibles en este modo, se recomienda consultar el correspondiente apartado de la guía de configuración y monitorización del producto [REF5].

La sintaxis del prompt en este modo es la siguiente: `<user>@<hostname>#`.

Al acceder al dispositivo, el sistema inicia por defecto en el modo operacional. Aunque existen diversos métodos para alternar entre ambos modos, la forma más sencilla de acceder al modo configuración desde el modo operacional es mediante la ejecución del comando:

```
configure
```

Para salir de este modo y regresar al modo operacional, se debe introducir el siguiente comando:

```
exit
```

Para que los cambios realizados en la configuración surtan efecto, es necesario confirmarlos mediante la ejecución del siguiente comando:

```
commit
```

Asimismo, es posible descartar en cualquier momento los cambios no confirmados con el comando:

```
discard
```

Cabe destacar que toda nueva configuración aplicada mediante el comando `commit` tiene efecto inmediato; no obstante, dicha configuración se perderá si el dispositivo se reinicia. Para garantizar la persistencia de la configuración entre reinicios, es necesario ejecutar el comando `save` después de realizar el `commit`.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

Las cuentas de usuario se configuran para permitir a los usuarios acceder al dispositivo. Para cada cuenta se define el nombre de usuario (<*login name*>), la contraseña y, de forma opcional, la clave pública asociada a dicho usuario.

Para cada cuenta de usuario, se pueden definir los siguientes parámetros:

a) Contraseña

b) Clave pública asociada

c) Rol (por defecto nivel 15)

6.3.2.1 PERMISOS Y ROLES DE USUARIO

Todos los usuarios que acceden al dispositivo deben tener un **rol de usuario** asignado. Existen tres roles predeterminados: ***monitor***, ***operator*** y ***admin***. Los roles se clasifican según niveles de acceso que van del **0 al 15**, donde el nivel 0 corresponde al menor privilegio y el nivel 15 al mayor. A medida que aumenta el nivel de acceso, también se incrementan los permisos del usuario para ejecutar acciones sobre el dispositivo.

Rol de usuario	Privilegios
Monitor **(Nivel cero)**	Comandos operacionales básicos
Operator **(Nivel cinco)**	Ejecuta gran parte de comandos operacionales

***Admin* (Nivel quince)**	Ejecuta todos los comandos operacionales y tiene acceso al menú de configuración

Tabla 3: Tabla Rol de usuario

Al crear un usuario, de forma predeterminada se le asigna el rol ***admin***, correspondiente al nivel de acceso más alto.

Es posible crear roles personalizados para definir distintas combinaciones de permisos mediante el comando:

```
set system login role <1-32 chars> level <0-15>
```

No obstante, cuando el dispositivo opera en modo de operación seguro, se debe restringir el uso de roles a uno de los tres roles predeterminados mencionados anteriormente, con el fin de evitar accesos no autorizados al menú de configuración, ya que los usuarios con un nivel de rol igual o superior a 10 disponen de acceso a dicho menú.

El comando que permite habilitar el **modo de operación seguro** está disponible exclusivamente para los usuarios que dispongan del **nivel máximo de acceso (nivel 15)**.

A continuación, se presenta una tabla que detalla los comandos operacionales a los que tienen acceso los usuarios con un rol igual o superior a 5 y aquellos con un rol igual o superior a 10. Cualquier otro comando operacional que no figure en dicha tabla se considera de nivel 0 y, por tanto, es accesible para cualquier usuario.

Rol de usuario	Comandos operacionales
***Operator* (Nivel cinco)**	arping interfaces clear interfaces <ifc_type> [<ifcN>] clear interfaces openvpn <ovpnN> reload monitor test nslookup ping poweroff protocols (bgp)/(vrf <txt> bgp) clear protocols (igmp)/(vrf <txt> igmp) clear protocols (ip)/(ipv6) clear protocols (ip)/(ipv6) prefix-list <txt> clear protocols (ip)/(vrf <txt> ip) clear multicast route protocols (ospf)/ospfv3) clear protocols (pim)/(vrf <txt> pim) clear protocols route-map <txt> clear protocols vrf <txt> (ospf)/(ospfv3) clear reboot service (dhcp-client)/(dhcpv6-client) renew service (dhcp-server)/(dhcpv6-server) clear service dns proxy service dns dynamic update service dns forwarding clear

	service firewall <txt> reload-rules service pppoe connect/disconnect/reconnect service ssh reload set date show changes/running/snapshot/tech-support ssh system advisor [<txt>] clear system alarm [<txt>] clear system conntrack clear system (ip)/(ipv6) neighbors clear system nftables clear system offload clear tech-support traceroute vpn ipsec clear/reload
Usuario de nivel diez	factory-reset file compress/copy/delete/move/uncompress image add/boot/comment/delete/install interfaces cellular <cellN> reconnect/open-at-terminal interfaces cellular <cellN> pdp <u32> reconnect interfaces openvpn <ovpnN> disconnect license load/read pki scep request-ca/enroll pki show/convert/generate/sign service cnm delete-certs/restart service firewall <txt> replay/restart service traffic-proxy restart service vrrp enable/disable system conntrack app-detect load-dictionary system coredump clear/cleanup/delete system journal clear

Tabla 4: Tabla Comando rol de usuario

6.4 PARÁMETROS DE SESIÓN

Los parámetros de intento de sesión que deben configurarse en estos dispositivos son los siguientes:

a) ***Intentos fallidos de autenticación***: Este parámetro permite establecer el número máximo de intentos fallidos permitidos para iniciar sesión antes de que se bloquee temporalmente el acceso. Se configura mediante el comando:

```
set system login max-auth-tries <1-65535>
```

Por defecto, el sistema permite 3 intentos fallidos de autenticación y no produce el bloqueo del usuario. Para que se produzca el bloqueo temporal del usuario es necesario configurar explícitamente este parámetro. Una vez habilitado, el tiempo de bloqueo es de 1 minuto por defecto, pudiéndose modificar mediante la opción *unlock-time*, descrita más adelante.

b) ***Intentos fallidos de autenticación vía SSH***: Para las conexiones remotas SSH se dispone del siguiente comando, que establece el número máximo de intentos de autenticación permitidos antes de que la conexión SSH sea rechazada:

```
set service ssh max-auth-tries <1-65535>
```

A diferencia del parámetro "*set system login max-auth-tries*", este mecanismo no bloquea la cuenta del usuario ni de forma temporal ni permanente, limitándose a finalizar la sesión SSH en curso una vez alcanzado el límite configurado. Asimismo, considera como intentos fallidos tanto las autenticaciones mediante contraseña como las realizadas mediante clave pública. Por su parte, el parámetro "*set system login max-auth-tries*" afecta también a las autenticaciones realizadas a través de SSH, pero únicamente teniendo en cuenta los intentos realizados mediante contraseña. El valor por defecto de este parámetro es 6.

Ambos mecanismos son independientes y su configuración conjunta debe realizarse de forma coherente para garantizar el comportamiento esperado de la política de autenticación.

c) ***Login banner***: Los dispositivos permiten configurar banners que se muestran a los usuarios antes o después de iniciar sesión. Estos banners tienen como finalidad mostrar avisos informativos de carácter general y no deben incluir, en ninguna circunstancia, información relativa al sistema, su configuración, versiones de software, arquitectura u otros datos técnicos que puedan ser utilizados por un atacante para identificar vulnerabilidades o facilitar accesos no autorizados. Los comandos de configuración son los siguientes:

```
set system login banner pre-login
set system login banner post-login
```

d) ***Restricción de acceso***: Establece el tiempo que debe pasar para desbloquear el acceso a un usuario cuando ha alcanzado el número máximo de intentos permitidos. Su comando de configuración es:

```
set system login unlock-time <0-65535>
```

Este campo tiene un valor por defecto de 60 segundos, pero para que entre en vigor se deberá configurar junto con el nodo "*set system login max-auth-tries*".

e) ***Tiempo de inactividad***: Corresponde al intervalo máximo durante el cual una sesión permanece activa sin registrar actividad por parte del usuario; una vez superado dicho período, la sesión se cierra automáticamente con el objetivo de reducir riesgos de acceso no autorizado, optimizar el uso de recursos del sistema y reforzar la seguridad del dispositivo. Por defecto, el tiempo es infinito, por lo que será responsabilidad del administrador configurar un valor mediante la ejecución del siguiente comando:

```
set system login idle-timeout <1-65535>
```

f) ***Tiempo de inactividad exclusivo del protocolo SSH***: Combinando los siguientes comandos, se establece el tiempo máximo que puede pasar una sesión SSH inactiva

antes de que el dispositivo la finalice abruptamente. El comportamiento es similar al parámetro "*system login idle-timeout*", pero solo afecta a SSH.

```
set service ssh keepalive-count-max
set service ssh keepalive-interval
```

g) ***Retardo de contraseñas***: Es un mecanismo de seguridad que establece un período de espera obligatorio cuando un usuario introduce credenciales incorrectas de forma consecutiva; dicha medida tiene como finalidad disuadir intentos de acceso no autorizado, limitar ataques de fuerza bruta y reforzar la protección del dispositivo y de la red. Se configura con el siguiente comando y aplica tanto a las conexiones por consola como por SSH. El tiempo por defecto cuando se activa el modo de operación seguro es de 10 segundos.

```
set system login password-prompt-delay <0-4294967295>
```

h) ***Deshabilitación de autenticación mediante contraseña en el protocolo SSH***: Este parámetro hace referencia a la posibilidad de restringir el acceso SSH única y exclusivamente mediante claves públicas. Su comando de configuración es:

```
set service ssh disable-password-authentication
```

i) ***Tiempo para acceder al dispositivo***: Con el siguiente comando se permite establecer el tiempo máximo para iniciar sesión a través de una sesión SSH antes de que el dispositivo la rechace (por defecto 2 minutos). Para el caso de un acceso por consola, el tiempo es de 60 segundos y no es configurable.

```
set service ssh login-grace-time <0-4294967295>
```

j) ***Máximo número de sesiones***: Define el límite de conexiones simultáneas que pueden establecerse con el dispositivo, con el propósito de controlar el uso de recursos, prevenir la saturación del sistema y reducir el riesgo de accesos indebidos mediante la restricción de sesiones concurrentes. Afecta tanto a consola como a SSH. El valor por defecto para el modo de operación seguro es de 5 sesiones. Se configura mediante el comando:

```
set system login max-sessions
```

6.5 CONFIGURACIÓN DE SSH

El dispositivo utiliza el protocolo **SSHv2 para la administración remota, la transferencia segura de ficheros y el establecimiento de conexiones remotas con otros dispositivos**. En estos escenarios, el dispositivo actúa tanto como **cliente SSH** y como **servidor SSH**, empleando las funciones y algoritmos criptográficos proporcionados por el módulo criptográfico *OpenSSH*.

La siguiente tabla muestra las funciones y los algoritmos que pueden configurarse para **SSHv2** cuando el producto opera en **modo de operación seguro**.

Establecimiento de claves (Key Exchange)	Autenticación (Authentication)	Cifrado (Cipher)	Autenticación de Mensajes (Message Auth)
diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521	ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521	aes128-ctr aes192-ctr aes256-ctr	hmac-sha2-256 hmac-sha2-512

Tabla 5: Tabla Configuración SSHv2

La configuración de SSH debe realizarse utilizando el usuario administrador, desde el modo de configuración, mediante la ejecución de los siguientes comandos:

a) Especificar los algoritmos de autenticación del servidor:

```
set service ssh host-key-algorithms
```

b) Especificar los algoritmos de autenticación de usuarios mediante clave pública:

```
set service ssh pubkey-accepted-algorithms
```

c) Especificar los algoritmos de intercambio de claves:

```
set service ssh key-exchange
```

d) Especificar los algoritmos de autenticación de mensajes:

```
set service ssh mac
```

e) Especificar los algoritmos de cifrado:

```
set service ssh cipher
```

6.6 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

Se recomienda desactivar las interfaces de red no utilizadas mediante la ejecución del siguiente comando de configuración:

```
set interfaces <type> <ifc-name> disable
```

Se deben deshabilitar aquellos servicios que no se utilicen con el correspondiente comando de configuración, ya que evita que queden puertos abiertos innecesarios que podrían ser explotados como vectores de ataque.

Para consultar el conjunto completo de comandos disponibles, se recomienda consultar el correspondiente apartado de la guía de configuración y monitorización del producto [REF5].

6.7 CONFIGURACIÓN VLAN

El dispositivo ofrece la posibilidad de crear **redes virtuales** (VLAN, *Virtual Local Area Network*), que permiten segmentar el tráfico de la red física en dominios lógicos independientes. Esta

funcionalidad facilita la organización de los recursos de la red, optimiza la gestión del tráfico y aísla diferentes grupos de usuarios o servicios.

En estos dispositivos, la configuración de una VLAN se realiza mediante la ejecución del siguiente comando:

```
set interfaces <type-ifc> <name-ifc> vif <vlan-id>
```

Este comando permite crear la VLAN y asignarla directamente a la interfaz física o subinterfaz correspondiente.

Adicionalmente, utilizando el mismo comando, es posible asignar una **dirección IP** a la VLAN, agregar una **descripción** y configurar **otros parámetros** asociados a la interfaz.

Para consultar el conjunto completo de opciones disponibles, se recomienda consultar el correspondiente apartado de la guía de configuración y monitorización del producto [REF5].

6.8 GESTIÓN DE CERTIFICADOS

Los dispositivos emplean **certificados X.509 v3** tanto para el establecimiento de **túneles IPsec** como para el envío de registros a un servidor externo mediante **SYSLOG sobre TLS**.

Para utilizar estos certificados, es necesario importarlos previamente en el dispositivo, ya sea mediante el siguiente comando a través de una conexión HTTPS, o bien utilizando el protocolo SCP desde el dispositivo en el que se encuentra almacenado el certificado:

```
file copy
```

En los **túneles IPsec**, se empleará el formato **PKCS#12** para los certificados, y su configuración se realizará de la siguiente manera:

```
set vpn ipsec auth-profile <auth-profile-name> local pkcs12 passphrase <passphrase>
set vpn ipsec auth-profile <auth-profile-name> local pkcs12 file <file>
```

En lo que respecta a **SYSLOG**, donde el dispositivo actúa exclusivamente como **cliente**, se deberá especificar la **Autoridad Certificadora (CA)** que ha emitido el certificado del servidor externo, así como el **Common Name (CN) del certificado**. Es importante destacar que dicho CN debe tener un formato FQDN (*Fully Qualified Domain Name*). Para ello, se deben utilizar los siguientes comandos de configuración:

```
set system syslog host <host> tls ca <ca-file>
set system syslog host <host> tls permitted-peer <FQDN>
```

6.9 GESTIÓN DE TÚNELES IPSEC

Los dispositivos permiten la creación de **túneles IPsec en modo túnel**, mediante los cuales se encapsulan y cifran de forma íntegra los paquetes IP originales durante su tránsito a través de redes públicas, garantizando la confidencialidad, integridad y autenticidad de la información.

Para el establecimiento seguro del túnel, deben emplearse los algoritmos, mecanismos criptográficos y modos de operación que se detallan a continuación:

Parámetros	Métodos y algoritmos autorizados
Protocolo IKE	IKEv2
Cifrado	aes128gcm128 aes192gcm128 aes256gcm128 chacha20poly1305
Integridad y autenticación	sha256 sha384 sha512
Intercambio de claves	Diffie-Hellman group 15 (3072-bit MODP Group) Diffie-Hellman group 16 (4096-bit MODP Group) Diffie-Hellman group 17 (6144-bit MODP Group) Diffie-Hellman group 18 (8192-bit MODP Group) Diffie-Hellman group 19 (256-bit random ECP group) Diffie-Hellman group 20 (384-bit random ECP group) Diffie-Hellman group 21 (521-bit random ECP group)

Tabla 6: Tabla Métodos y algoritmos autorizados

La autenticación de los dispositivos que participan en el túnel se realizará mediante **certificados digitales X.509** basados en **ECDSA**, garantizando la identidad de los extremos.

A continuación, se presentan los comandos necesarios para la configuración de un túnel IPSec:

```
set vpn ipsec auth-profile AUTH1 local id <id>
set vpn ipsec auth-profile AUTH1 local pkcs12 passphrase <passphrase>
set vpn ipsec auth-profile AUTH1 local pkcs12 file <file>
set vpn ipsec esp-group CHILD-SA mode tunnel
set vpn ipsec esp-group CHILD-SA proposal 1 encryption <alg_enc>
set vpn ipsec esp-group CHILD-SA proposal 1 pfs <dh-group>
set vpn ipsec esp-group CHILD-SA proposal 1 hash <alg_hash>
set vpn ipsec ike-group IKE-SA key-exchange ikev2
set vpn ipsec ike-group IKE-SA proposal 1 <dh-group>
set vpn ipsec ike-group IKE-SA proposal 1 encryption <alg_enc>
set vpn ipsec ike-group IKE-SA proposal 1 hash <alg_hash>
set vpn ipsec site-to-site peer PEER auth-profile AUTH1
set vpn ipsec site-to-site peer PEER default-esp-group CHILD-SA
set vpn ipsec site-to-site peer PEER ike-group IKE-SA

set vpn ipsec site-to-site peer PEER local-address <X.X.X.X>
set vpn ipsec site-to-site peer PEER remote-address <Y.Y.Y.Y>
set vpn ipsec site-to-site peer PEER tunnel 1 local-interface <ifc>
set vpn ipsec site-to-site peer PEER tunnel 1 local prefix <X.X.X.X/X>
set vpn ipsec site-to-site peer PEER tunnel 1 remote prefix <Y.Y.Y.Y/Y>
```

La autenticación de los extremos del túnel se llevará a cabo mediante un fichero en formato PKCS#12, el cual deberá incluir los siguientes elementos:

a) El certificado del dispositivo.

b) La clave privada asociada al certificado.

c) El certificado de la Autoridad de Certificación necesario para la validación del extremo opuesto del túnel.

El parámetro **id** hace referencia al **identificador del certificado** en uso, el cual habitualmente sigue la siguiente estructura:

"C=ES, ST=Madrid, L=Tres Cantos, O=Teldat, OU=OSDx, CN=Nombre Común del Certificado".

Para el establecimiento de la fase de negociación **IKE**, será necesario especificar las **direcciones IP de origen y destino** mediante los parámetros *local-address* y *remote-address*, correspondientes, respectivamente, al extremo local del dispositivo y al extremo remoto con el que se desea establecer el túnel.

Para el tráfico cifrado mediante **ESP**, deberá incluirse, al menos, el **prefijo local** (*local-prefix*) del extremo del dispositivo desde el cual se enviará la comunicación. Adicionalmente, se recomienda especificar el **prefijo remoto** (*remote-prefix*) y la **interfaz de salida asociada al prefijo local** (*local-interface*), la cual podrá ser tanto lógica como física, con el fin de optimizar el enrutamiento del tráfico a través del túnel.

Si se desea que el **dispositivo inicie la conexión** del túnel, se deberá configurar el siguiente comando:

```
set vpn ipsec site-to-site peer PEER connection-type initiate
```

En caso contrario, si se desea que el dispositivo **espere a que sea el extremo remoto quien inicie** la conexión, se deberá configurar lo siguiente:

```
set vpn ipsec site-to-site peer PEER connection-type respond
```

6.10 SINCRONIZACIÓN

Es fundamental que el dispositivo mantenga una hora precisa y correctamente sincronizada, ya que la correcta gestión temporal impacta directamente en funcionalidades críticas como auditoría, registro de eventos (*logging*) y trazabilidad de acciones. Además, la sincronización horaria correcta es imprescindible para la interoperabilidad con sistemas externos y servidores.

Los dispositivos disponen de **distintos mecanismos para establecer y sincronizar la hora del sistema**.

Para establecer de **forma manual** la fecha en el dispositivo, se puede utilizar el siguiente comando operacional, donde *<yyyy-MM-dd>* representa el año, mes y día en el formato indicado, y *<hh:mm:ss>* corresponde a la hora, los minutos y los segundos, respectivamente:

```
set date <yyyy-MM-dd> [ <hh:mm:ss>]
```

Como alternativa, es posible **sincronizar la hora del sistema con el reloj hardware** del dispositivo mediante el siguiente comando operacional, lo que garantiza que el sistema adopte la hora almacenada en el reloj interno del hardware:

```
set date hwclock to-system
```

Adicionalmente, los dispositivos permiten la sincronización temporal con un **servidor NTP autenticado**, como medida de seguridad para garantizar la integridad y autenticidad de la fuente de tiempo. La utilización de NTP autenticado se considera la configuración recomendada. Para el uso de un servidor NTP autenticado, será necesario configurar en el dispositivo tanto la **dirección del servidor NTP** como el **tipo de autenticación** que se empleará en la conexión. Dicha configuración se realiza mediante los siguientes comandos:

```
set system ntp authentication-key <keyID> key <txt>
set system ntp server address [<x.x.x.x> | <FQDN>] key <keyID>
set system ntp authentication-key <keyID> algorithm [sha256 |
sha384 | sha512]
```

6.11 ACTUALIZACIONES

Los dispositivos permiten consultar la versión del firmware a través de su interfaz de línea de comandos (CLI). La versión actualmente en ejecución puede verificarse mediante el siguiente comando atendiendo al campo *OS version*:

```
show version
```

Asimismo, es posible consultar el conjunto de versiones de software instaladas mediante el siguiente comando, lo que facilita la gestión y verificación del software del dispositivo.

```
image show
```

Todas las actualizaciones deben llevarse a cabo de forma manual.

El procedimiento de actualización es el mismo que el descrito en el apartado 5. Adicionalmente, se aclara que la configuración del sistema únicamente se conserva tras el proceso de actualización si ha sido previamente guardada de forma persistente. En caso de no haberse realizado dicho guardado, los cambios de configuración no persistidos se perderán durante el reinicio asociado a la actualización, siendo necesario su reconfiguración manual.

6.12 AUTO-CHEQUEOS

Los dispositivos realizan un **proceso de autochequeo durante el arranque con el fin de verificar su correcto funcionamiento**. Dicho proceso se ejecuta en todos los casos, incluso cuando el dispositivo no se encuentra en modo de operación seguro habilitado.

La verificación se realiza mediante la generación de un valor hash SHA-512 del fichero de firmware. Una vez calculado, dicho valor se compara con el hash previamente almacenado en el dispositivo durante el proceso de instalación del firmware. En caso de coincidencia entre ambos valores, el dispositivo inicia su funcionamiento con normalidad; en caso contrario, el dispositivo

se reinicia automáticamente utilizando un firmware alternativo que cumple con los requisitos de validación establecidos.

6.13 REGISTRO DE EVENTOS

A la hora de gestionar una red, resulta fundamental mantener un registro de los eventos que se producen en ella, de manera que el administrador pueda revisar dicha información y conocer con exactitud las acciones y sucesos acontecidos. Para ello, los registros de eventos deben configurarse de forma adecuada.

Se recomienda configurar el **sistema de auditoría** del dispositivo para que registre, al menos, los siguientes eventos:

a) Comandos introducidos por el usuario

b) Registros de inicio y fin del modo de operación seguro

c) Eventos asociados al protocolo NTP

d) Eventos relacionados con SSH

e) Eventos relativos a IPSEC

f) Eventos de SYSLOG

Los eventos del firewall solo se generan cuando se habilitan en las reglas de filtrado. Estos eventos no forman parte del conjunto de registros locales predefinidos del dispositivo, ya que este no es configurable. No obstante, pueden enviarse a un servidor SYSLOG si, además, se habilita la configuración correspondiente en SYSLOG para el envío de estos eventos.

La estructura de un mensaje de auditoría se detalla en la tabla siguiente. Para cada campo, se incluye, a modo de ejemplo, el valor correspondiente de un mensaje de auditoría:

Campo	Descripción	Ejemplo
Timestamp	Fecha del evento	2024-11-27 12:45:56.907336
Process	Proceso del evento	OSDxCLI
ProcessID	Identificador del proceso	10207
TAG	Nivel del evento	auth-notice
username	Usuario que produjo el evento	User 'admin'
message-text	Mensaje del evento	added a new cfg line: 'set system login user test authentication plaintext-password ******'

Tabla 7: Tabla estructura de un mensaje de auditoría

6.13.1 ALMACENAMIENTO LOCAL

Los registros de auditoría se almacenan localmente en **running://log/user/audit_file/audit_file**. Este fichero **se genera automáticamente** al iniciarse el modo de operación seguro y únicamente es accesible por el **usuario administrador**.

Cuando el fichero de registro **alcanza su tamaño máximo** permitido, el sistema **sobrescribe automáticamente los registros más antiguos**, garantizando la continuidad en el almacenamiento de nuevos eventos sin afectar al funcionamiento del sistema.

Los eventos registrados en este fichero corresponden a los descritos anteriormente.

6.13.2 ALMACENAMIENTO REMOTO

Se recomienda configurar el dispositivo para el envío de los registros de auditoría a un **servidor SYSLOG** remoto. La comunicación con dicho servidor deberá configurarse mediante **TLS**, asegurando el cifrado completo de la transmisión de información.

Una vez que los certificados hayan sido creados y configurados en el servidor SYSLOG externo, el certificado de la Autoridad de Certificación (CA) deberá cargarse en el dispositivo siguiendo las indicaciones descritas en el apartado 6.8. A continuación, se accederá al dispositivo a través de la interfaz de línea de comandos y se seguirán los pasos que se indican a continuación:

a) Definir el servidor remoto de destino y el puerto correspondiente al servicio:

```
set system syslog host <host> port <port>
```

b) Habilitar el uso de TLS como mecanismo de transporte, configurando la Autoridad de Certificación (CA) y el identificador del servidor reflejado en su certificado digital para verificar su identidad:

```
set system syslog host <host> protocol tcp
set system syslog host <host> tls ca <ca-file>
set system syslog host <host> tls permitted-peer <CN_FQDN>
```

c) Indicar los eventos que serán enviados al servidor SYSLOG mediante los siguientes comandos:

```
set system syslog host <host> filter <filter
name> app <process name>
set system syslog host <host> filter <filter name> level <log
level>
```

En estos comandos, el parámetro *app* hace referencia al nombre del proceso cuyos eventos se desean enviar, mientras que *level* indica el nivel mínimo de severidad de los registros a partir del cual se capturarán los eventos asociados a dicha aplicación. El parámetro *filter* representa la combinación de la aplicación y el nivel de severidad definidos. En consecuencia, cada servidor SYSLOG configurado contará con múltiples filtros, uno por cada conjunto “aplicación + nivel”. De manera análoga, en el almacenamiento local, cada tipo de evento registrado en el fichero corresponde igualmente a un filtro distinto.

A continuación, se presentan los comandos que deberán ejecutarse en el dispositivo para el envío al servidor SYSLOG externo de los eventos descritos anteriormente, incluidos los eventos del firewall:

```
set system syslog host <host> filter CLI app OSDxCLI
set system syslog host <host> filter CLI level info
set system syslog host <host> filter secure
regex '.*Secure mode.*'
set system syslog host <host> filter secure level info
set system syslog host <host> filter ntp app ntpd
set system syslog host <host> filter ntp level info
set system syslog host <host> filter ssh app sshd
set system syslog host <host> filter ssh level info
set system syslog host <host> filter ipsec app charon-
systemd

set system syslog host <host> filter ipsec level info
set system syslog host <host> filter syslog app rsyslogd
set system syslog host <host> filter syslog level info
set system syslog host <host> filter commit regex '^ Commit
'
set system syslog host <x.x.x.x> filter KERNEL app kernel
set system syslog host <x.x.x.x> filter KERNEL level debug
```

Una vez finalizada la configuración, se recomienda:

a) **Monitorizar el registro de eventos** generado en el dispositivo, por ejemplo, para las acciones de administración, y compararlo con los registros recibidos por el servidor SYSLOG, a fin de verificar su correspondencia.

b) **Examinar el tráfico entre el servidor SYSLOG y el dispositivo**, con el objetivo de comprobar que la información no es accesible durante la transmisión y que el servidor SYSLOG recibe correctamente los datos.

6.14 CONFIGURACIÓN DE REGLAS DE FILTRADO DE TRÁFICO

La configuración de un firewall mediante reglas de filtrado constituye un mecanismo fundamental para reforzar la seguridad de la red. Estas reglas permiten controlar y restringir el tráfico que entra, sale o atraviesa el dispositivo, en función de criterios como direcciones IP, puertos, protocolos o estados de las conexiones. De este modo, se autoriza únicamente el tráfico legítimo y necesario para la operación del sistema, al tiempo que se bloquean accesos no autorizados y posibles vectores de ataque.

En estos dispositivos la configuración del **firewall** se realiza mediante los siguientes comandos:

```
set traffic selector
set traffic policy
```

Los **selectores** se emplean para definir el tráfico que se desea filtrar, mientras que las **políticas** establecen la acción que debe aplicarse al tráfico seleccionado.

Es posible aplicar **reglas de filtrado** tanto al tráfico de **todo el sistema** como al tráfico asociado a una **interfaz específica**. A continuación, se incluye un ejemplo de ambos escenarios:

a) Tráfico de todo el sistema

```
set system traffic policy in POLICY
```

```
set traffic policy POLICY rule 1 action drop
set traffic policy POLICY rule 1 log
set traffic policy POLICY rule 1 selector ICMP
set traffic policy POLICY rule 2 action accept
set traffic policy POLICY rule 2 log
set traffic selector ICMP rule 1 icmp-code 0
set traffic selector ICMP rule 1 icmp-type 8
```

Todas las reglas definidas en esta política afectarán al tráfico que llega al dispositivo por todas sus interfaces.

Se bloquea solamente los paquetes de ping ICMPv4 entrantes.

Se registra un evento en los logs tanto para los paquetes bloqueados como para los permitidos.

b) Tráfico por interfaz específica

```
set interfaces ethernet eth0 traffic policy out POLICY
set traffic policy POLICY rule 1 action accept
set traffic policy POLICY rule 1 log
set traffic policy POLICY rule 1 selector UDP
set traffic policy POLICY rule 2 action drop
set traffic policy POLICY rule 2 log
set traffic selector UDP rule 1 destination port 1000
set traffic selector UDP rule 1 protocol udp
```

Todas las reglas definidas en esta política afectarán únicamente al tráfico que sale por eth0, no al tráfico entrante ni al tráfico de otras interfaces.

Cualquier tráfico saliente por eth0 que no sea UDP hacia el puerto 1000 es descartado.

Se registra un evento en los logs tanto para los paquetes bloqueados como para los permitidos.

El número asignado a cada regla dentro de una política de filtrado determina su **prioridad de aplicación**. A mayor valor numérico, menor será la prioridad de la regla, de manera que las reglas con números más bajos se evalúan primero y pueden prevalecer sobre las de mayor valor. Este mecanismo permite organizar jerárquicamente las reglas, asegurando que las acciones más críticas se apliquen antes que las de menor importancia.

En el dispositivo, la acción por defecto aplicada al tráfico es permitir, lo que implica que cualquier paquete que no coincida con una regla específica será aceptado automáticamente. Para reforzar la seguridad del sistema y garantizar un control estricto sobre las comunicaciones, es necesario definir una regla adicional que bloquee todo el tráfico entrante y saliente. De este modo, se asegura que únicamente el tráfico autorizado por reglas explícitas pueda ser transmitido o recibido, reduciendo significativamente la exposición a accesos no deseados o posibles ataques. Su configuración es la siguiente:

a) Tráfico de todo el sistema

```
set system traffic policy in POLICY
set system traffic policy out POLICY
set traffic policy POLICY rule 6000 action drop
set traffic policy POLICY rule 6000 log
```

b) Tráfico por interfaz específica

```
set interfaces ethernet eth0 traffic policy in POLICY
set interfaces ethernet eth0 traffic policy out POLICY
set traffic policy POLICY rule 6000 action drop
set traffic policy POLICY rule 6000 log
```

En ambas configuraciones el número asignado a la regla (6000) puede ser modificado según las necesidades de la política de filtrado. No obstante, es imprescindible seleccionar un valor relativamente alto, de modo que sea posible definir reglas adicionales con mayor prioridad, ya que los números más bajos corresponden a reglas de prioridad superior.

La información detallada relativa a la configuración de políticas y selectores puede consultarse el correspondiente apartado de la guía de configuración y monitorización del producto [REF5].

6.15 SERVICIOS INTERNOS

En el momento en que se activa el modo de operación seguro, no se permitirá el uso ni la configuración de servicios internos no autorizados, tales como SNMP, TELNET o la transferencia de ficheros mediante protocolos inseguros como FTP o HTTP, entre otros. En caso de que alguno de estos servicios se encuentre previamente configurado y se intente habilitar el modo de operación seguro, la interfaz de línea de comandos (CLI) mostrará un mensaje de error indicando que dichas configuraciones deberán eliminarse previamente.

Para la transferencia de ficheros o la descarga de versiones de software, deberá utilizarse el siguiente comando siendo obligatorio que la URL especificada emplee el protocolo HTTPS:

```
file copy <url>
```

Asimismo, es posible realizar transferencias de ficheros mediante el protocolo SCP, siempre que el dispositivo actúe como servidor de la sesión. A modo de ejemplo, se muestra la siguiente configuración para esta última opción:

```
scp -O /path/to/your/directory
<username>@<ipaddress>:/path/to/your/directory
```

Es importante señalar que la ruta de destino en el dispositivo se establece siempre a partir de *running://*. Por lo tanto, si se desea transferir un certificado a la ruta *running://auth/<certificate>*, será suficiente con especificar como destino *<username>@<ipaddress>:/auth/<certificate>*.

7 FASE DE OPERACIÓN Y MANTENIMIENTO

El correcto funcionamiento del producto requiere de características que deben estar presentes en el entorno. Es responsabilidad del administrador autorizado asegurar que el entorno operacional cumple con los requisitos enumerados a continuación:

a) El producto estará instalado y será mantenido en un entorno físico seguro. Esto incluye una sala con control de acceso o un entorno móvil controlado por el administrador.

b) El producto no contendrá ninguna aplicación de uso general como compiladores o aplicaciones de usuario.

c) Se realizarán comprobaciones periódicas del hardware del dispositivo para asegurar que no ha sido manipulado.

d) Los administradores deben estar correctamente entrenados en el uso y la correcta operación del producto, así como en las características del entorno seguro en que está presente. Al mismo tiempo, los administradores seguirán las guías e indicaciones presentes.

e) Los administradores se asegurarán de que el dispositivo cuenta con las últimas actualizaciones de software para preservar al mismo de amenazas y vulnerabilidades conocidas.

f) Los administradores mantendrán sus credenciales de acceso al dispositivo seguras y protegidas.

g) Los administradores deben eliminar toda la información residual sensible que pudiera quedar resultante de operar con el dispositivo después de terminar la vida útil de este.

h) Los auditores se encargarán de examinar de forma periódica los registros de auditoría buscando eventos específicos relacionados con los cambios de la configuración del sistema y que puedan indicar que éste ha sido comprometido.

8 REFERENCIAS

[REF1] Enrutadores (CCN-STIC-140-D1)

[REF2] Switches (CCN-STIC-140-D2)

[REF3] Cortafuegos (CCN-STIC-140-D3)

[REF4] Teldat Installation Manual

[REF5] Teldat Configuration and Monitoring

[REF6] https://support.teldat.com/osdx-doc/v4.2.1.3/

[REF7] Criptología de empleo en el Esquema Nacional de Seguridad (CCN-STIC-807)

[REF8] https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html

[REF9] LAN interfaces - Teldat Dm709-I

Syslog Client-Teldat-Dm 753-I

Software Updating Quick Guide – Teldat-Dm 835-I

[REF10] SSH Protocol – Teldat-Dm 787-I

[REF11] https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

9 ABREVIATURAS

CA	Certificate Authority
CCN	Centro Criptológico Nacional
CLI	Command-Line Interface
CN	Common Name
CNM	Cloud Net Manager
CPSTIC	*Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones*
CSP	Critical Security Parameter
DHCP	Dynamic Host Configuration Protocol
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad
ESP	Encapsulating Security Payload
FQDN	Fully Qualified Domain Name
GB	Gigabyte
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
LAN	Local Area Network
LINCE	Certificación Nacional Esencial de Seguridad (LINCE)
MAC	Message Authentication Code
NTA	Network Traffic Analysis
NTP	Network Time Protocol
PKCS12	Public Key Cryptography Standards #12
QoS	Quality of Service
RAM	Random Access Memory
SASE	Secure Access Service Edge
SCP	Secure Copy Protocol
SD-WAN	Software-Defined Wide Area Network
SFP	Small Form-factor Pluggable
SHA	*Secure Hash Algorithm*
SNMP	Simple Network Management Protocol
SSE	Security Service Edge

SSH	Secure Shell
TCP	Transmission Control Protocol
TELNET	Telecommunication Network
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
UUID	Universal Unique IDentifier
VGA	Video Graphics Array
VLAN	Virtual Local Area Networks
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WWAN	Wireless Wide Area Network
XDR	Extended Detection & Response
ZTNA	Zero Trust Network Access