Guía de Seguridad de las TIC
CCN-STIC 1470

Procedimiento de Empleo Seguro
Ekinops ONE2501



Noviembre 2026

Edita:





CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.11.04 14:07:00 +01:00

Fecha de Edición: Noviembre de 2026

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.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

1 INTRODUCCIÓN 3
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 COMPONENTES DEL ENTORNO DE OPERACIÓN 8
5 FASE DE INSTALACIÓN 10
6 FASE DE CONFIGURACIÓN 12
6.1 MODO DE OPERACIÓN SEGURO 12
6.2 AUTENTICACIÓN 13
6.3 ADMINISTRACIÓN DEL PRODUCTO 16
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 17
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES 17
6.4 CONFIGURACIÓN CRIPTOGRÁFICA 18
6.4.1 CONFIGURACIÓN DE CIPHERSUITES Y SERVICIOS 18
6.4.2 CONFIGURACIÓN DE IPSEC 19
6.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 25
6.6 CONFIGURACIÓN DEL SISTEMA DE COMUNICACIÓN INALÁMBRICA MÓVIL 25
6.7 GESTIÓN DE CERTIFICADOS 27
6.8 ACTUALIZACIONES 27
6.9 AUDITORÍA 28
6.9.1 REGISTRO DE EVENTOS 28
6.9.2 ALMACENAMIENTO LOCAL 29
6.9.3 ALMACENAMIENTO REMOTO 29
6.10 AUTO-CHEQUEOS 30
7 FASE DE OPERACIÓN 31
8 REFERENCIAS 32
9 ABREVIATURAS 33

ÍNDICE DE TABLAS

Tabla 1 Suites de Cifrado del dispositivo en el modo de operación seguro 13
Tabla 2. Roles y privilegios del dispositivo. 14
Tabla 3. Lista de comandos según el nivel de privilegio 15
Tabla 4. Nivel de severidad para la importancia de los eventos 28

ÍNDICE DE FIGURAS

Ilustración 1. Vista Esquemática del hardware de ONE2501 3
Ilustración 2. Límites del dispositivo ONE2501 5
Ilustración 3. Entorno operacional del dispositivo 9
Ilustración 4. Imagen del sistema operativo 10
Ilustración 5. Revisión de la integridad del software 30

1 INTRODUCCIÓN

El dispositivo ONE2501 es un router de acceso multiservicio (MSAR) para pequeñas y medianas empresas (PYME). Está pensado para su uso en las instalaciones del cliente.

Dispone de 4 puertos Ethernet Gigabit UTP, con la opción de agregar 4 puertos Ethernet Gigabit UTP adicionales y, opcionalmente, conectividad WiFi 11ac/b/g/n/a.

En el lado WAN, cuenta con 2 puertos Gigabit Ethernet combo (UTP y SFP), además de una opción para incluir una interfaz celular 4G/LTE.

En cuanto a rendimiento, ofrece un rendimiento de reenvío bidireccional para IPv4 e IPv6 de 600 o 1000 Mbps (ampliable a 1000 Mbps con licencia) utilizando paquetes IMIX409 con servicios IP; proporciona un rendimiento de reenvío bidireccional de 300 o 600 Mbps con paquetes IMIX409 y servicios IPsec.

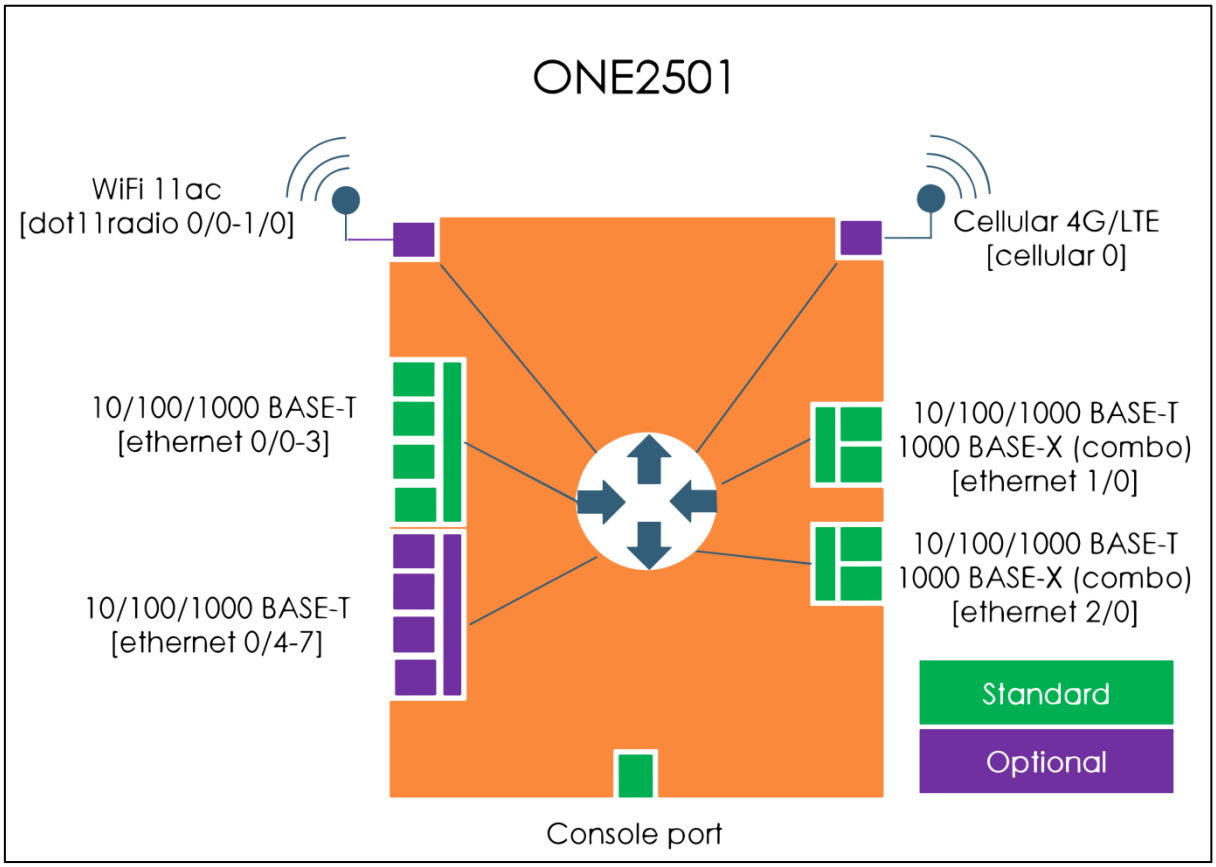


Ilustración 1. Vista Esquemática del hardware de ONE2501

Bajo **ONE2501** se ejecuta el sistema operativo OneOS versión **OneOS6.12x5patch01**. La versión de firmware **OneOS6.12.x5patch01** utiliza núcleos de procesador separados para los planos de control y gestión y para el plano de datos.

El plano de control y gestión ejecuta software basado en Linux. El plano de datos ejecuta código optimizado propietario de Ekinops para el reenvío de datos.

El dispositivo utiliza un procesador de 4 núcleos: 1 núcleo se utiliza para los planos de control y gestión, los otros 3 núcleos se utilizan para el plano de datos.

El dispositivo proporciona las siguientes funciones de seguridad:

- **Administración Confiable**: El TOE proporciona el rol de administración y la posibilidad de asociar usuarios a roles. El rol de administrador es el único que puede realizar las siguientes acciones: gestión del producto (tanto local como remotamente), configuración de los tiempos de finalización o bloqueo en caso de inactividad detectada, actualización del software del TOE, modificación de la configuración del TOE.
- **Identificación y Autenticación**: Todos los usuarios deben ser identificados y autenticados antes de que se les conceda el acceso. Para evitar ataques de autenticación por fuerza bruta, el TOE emplea una lista negra. Las contraseñas deben tener una longitud mínima de 12 caracteres e incluir una combinación de minúsculas, mayúsculas, números y caracteres especiales [«!», «@», «#», «$»,«%», «^», «&», «*», «(», «]. Además, el TOE permite la configuración de un temporizador de inactividad, cerrando automáticamente la sesión de los usuarios después de un período especificado de inactividad. Si un usuario intenta acceder al TOE utilizando credenciales por defecto o sin credenciales, el acceso es denegado.
- **Canales Confiables**: El TOE protege la información en tránsito estableciendo canales seguros al intercambiar datos sensibles con cualquier entidad autorizada, utilizando IPsec o SSHv2. Estos canales pueden ser iniciados por el propio TOE o por entidades autorizadas. Se emplean certificados digitales para la autenticación cuando se utiliza IPsec o SSHv2. Al intercambiar información con el administrador remoto, el TOE establecerá canales seguros utilizando IPsec o SSHv2.
- **Criptografía**: El TOE sólo permite el uso de los mecanismos criptográficos IPsec y SSH autorizados de acuerdo con lo establecido en la guía CCN-STIC-807.
- **Actualizaciones Confiables**: El TOE proporciona la opción de comprobar la versión de firmware/software actual y permite la iniciación manual de actualizaciones, no se admite ningún otro método de iniciación. El TOE utiliza firmas digitales autorizadas en CCN-STIC-807 para autenticar las actualizaciones de firmware/software antes de su instalación. Sólo los usuarios con rol de administración están autorizados a iniciar estas actualizaciones.
- **Auditoría**: El TOE genera registros de auditoría cuando ocurren ciertos eventos definidos. Estos registros de auditoría contienen como mínimo: la fecha y hora del evento, el tipo de evento identificado, el resultado del evento y el usuario que lo ha producido. El TOE incluye una política de acceso que determina las acciones permisibles relacionadas con el registro de auditoría para cada usuario. Los registros de auditoría pueden guardarse internamente y transmitirse a una entidad externa. Cuando el almacenamiento de auditoría dedicado está lleno, el TOE sobrescribe las entradas de auditoría anteriores.
- **Protección de credenciales y datos sensibles**: El TOE almacena las credenciales cifradas. Estas credenciales pueden guardarse utilizando hashing PBKDF2 o cifrado AES256-CBC con relleno.
- **Protección de fallos**: El TOE tiene la capacidad de realizar una prueba tanto durante el encendido del producto como a petición de un usuario autorizado para verificar la integridad del software/firmware.
- **Enrutamiento**: El TOE es capaz de gestionar puertos habilitándolos o deshabilitándolos y asignándoles prioridad. Reenvía el tráfico de red a través de sus puertos en el nivel de capa de red del modelo de Interconexión de Sistemas Abiertos, siguiendo una tabla de enrutamiento.

2 OBJETO Y ALCANCE

El objeto del presente documento es facilitar la instalación y configuración segura del router EKINOPS **ONE2501** el sistema operativo OneOS versión **OneOS6.12x5patch01**, junto con el aseguramiento del entorno en el que se despliega.

En la parte hardware (ONE2501) del TOE, existen tres tipos de puertos ethernet:

- 10/100/1000 BASE-T [Ethernet 0/0-3]
- 10/100/1000 BASE-T 1000 BASE-X (combo) [Ethernet 1/0]
- 10/100/1000 BASE-T 1000 BASE-X (combo) [Ethernet 2/0]

NOTA: Ambos tipos de interfaces Ethernet (BASE-T y BASE-T 1000 BASE-X combo) difieren en el esquema de codificación, ya que ambos se basan en la norma IEEE 802.3. Sin embargo, esta diferencia de estándares no se refleja en el TOE. Los usuarios pueden acceder al TOE de la misma manera independientemente de la interfaz física Ethernet utilizada.

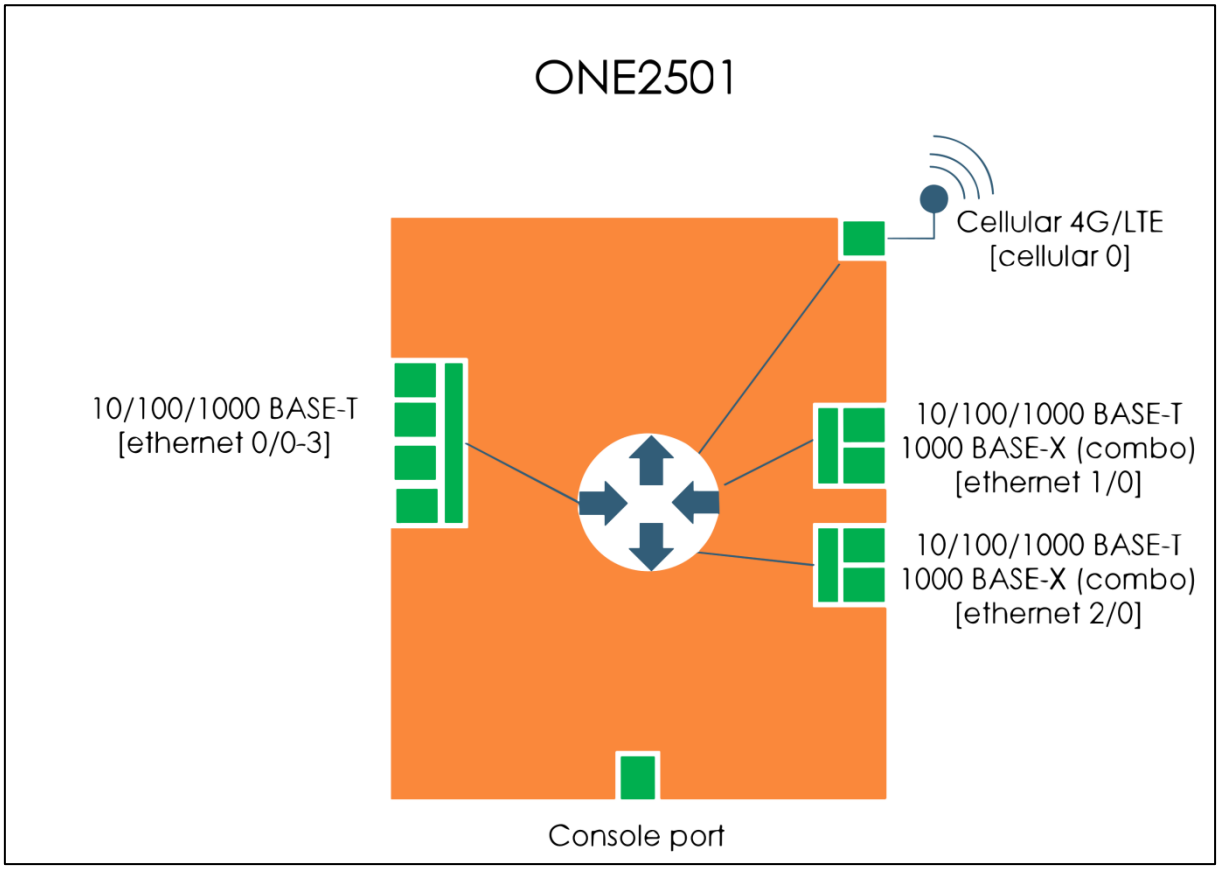


Ilustración 2. Límites del dispositivo ONE2501

El producto está diseñado para ser accesible **remotamente** a través de dos interfaces lógicas que implementan los protocolos de comunicaciones seguras (SSH o IPsec) y accesible **localmente** a través de un puerto de consola.

Además, el TOE es accesible para su administración a través del puerto de consola, LAN (Local Area Network) y WAN (Wide Area Network) como se muestra a continuación.

- **Puerto Consola**: Un usuario puede gestionar el TOE localmente a través del puerto de consola mediante un cable RS-232.
- **LAN**: El TOE establece su propia red LAN. Esta red es accesible a través de Ethernet utilizando SSH o túneles IPsec.
- **WAN**: El TOE es accesible a través de WAN mediante SSH o túneles IPsec. Por lo tanto, el TOE puede ser gestionado remotamente con características de seguridad mejoradas, proporcionando una solución flexible y robusta para una administración y control sin fisuras.
    - **Método Wired:** Un usuario puede administrar el TOE a través de una conexión ethernet utilizando SSH o túneles IPsec.
    - **Métodos Wireless:** El TOE es accesible a través de 4G/LTE utilizando protocolo SSH o túneles IPsec.

El producto Ekinops ONE2501 ha sido incluido en el CPSTIC. Para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF1].

3 ORGANIZACIÓN DEL DOCUMENTO

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 recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

Durante el proceso de entrega deberán llevarse a cabo una serie de tareas de comprobación para garantizar que el producto recibido no haya sido manipulado indebidamente:

a) **Etiqueta de envío**: deberá comprobarse que la etiqueta de envío identifica correctamente el nombre del cliente, su dirección y el dispositivo.

b) **Embalaje externo**: deberá inspeccionarse la caja de envío externa y la cinta adhesiva. Se comprobará que la cinta adhesiva no esté cortada ni se haya deteriorado en ningún punto. Así mismo, la caja no deberá presentar cortes ni daños que permitan acceder al dispositivo.

En caso de identificarse algún problema durante la inspección, el cliente deberá ponerse en contacto inmediatamente con EKINOPS S.A., al que se le indicará el número de pedido, el número de seguimiento y una descripción del problema.

Además, es necesario realizar una serie de comprobaciones para garantizar que la caja recibida la envió EKINOPS S.A. y no existe una suplantación de identidad. Para ello se aconseja al comprador verificar que efectivamente se ha realizado un pedido de compra al fabricante EKINOPS S.A. y el dispositivo recibido es exactamente el que se ha pedido al fabricante.

4.2 ENTORNO DE INSTALACIÓN SEGURO

Los dispositivos se deberán instalar dentro de un Centro de Procesamiento de Datos (CPD), cuyo acceso estará restringido a un grupo de personas con autorización explícita. Para garantizarlo, la sala que alberga el CPD contará con un sistema de control de acceso que asegure que solo el personal autorizado pueda ingresar al dispositivo, incluso fuera del horario laboral.

Será necesario que se sigan las recomendaciones indicadas en el presente documento, así como en las guías de instalación que se proporcionan junto al producto.

4.3 COMPONENTES DEL ENTORNO DE OPERACIÓN

El router EKINOPS **ONE2501** debe implementar el sistema operativo OneOS versión **OneOS6.12x5patch01.**

Para hacer realizar la configuración inicial del dispositivo será necesario un ordenador que permita al administrador realizar la administración de manera local o remota del dispositivo tal y cómo se indica en la Ilustración 3.

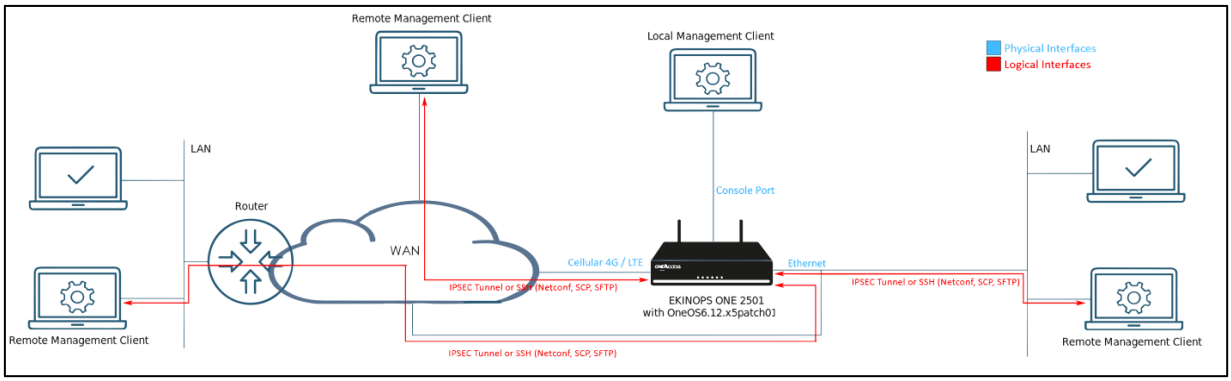


Ilustración 3. Entorno operacional del dispositivo

El ordenador utilizado por el administrador debe de disponer de un cliente SSH para realizar la comunicación con el dispositivo router.

5 FASE DE INSTALACIÓN

Una vez realizada la instalación física del producto, habrá que realizar una primera autenticación y comprobar la versión del firmware siguiendo los pasos indicados a continuación:

a) Conecte el puerto de consola (CON) a una computadora portátil o PC utilizando un cable RJ-45. Utilizar la velocidad de conexión serie por 9600 bps.

b) Inicie sesión como administrador haciendo uso de las credenciales por defecto:

- username: admin
- password: admin

NOTA: El dispositivo no requiere que el usuario `admin` (creado por defecto) cambie la contraseña durante el primer inicio de sesión. Por esta razón, más adelante, se configurará un único usuario con privilegios de administrador en el dispositivo, creando un nuevo usuario que cumpla con la política de cambio de contraseña. Este nuevo usuario administrador reemplazará al usuario predeterminado `admin`, asegurando el cumplimiento de las políticas de seguridad establecidas.

c) Compruebe que el dispositivo tiene instalado el firmware evaluado. Para ello será necesario ejecutar el siguiente comando:

```
CLI(config)> show software-image
```

d) El administrador se deberá de asegurar que el sistema operativo corriendo en el dispositivo es OneOS versión **OneOS6.12x5patch01,** identificado en el dispositivo como: "OneOS-pCPE-PPC_pi2-6.12.x5patch01". Para ello se utilizará el comando `show software-image` como se muestra en la siguiente imagen:

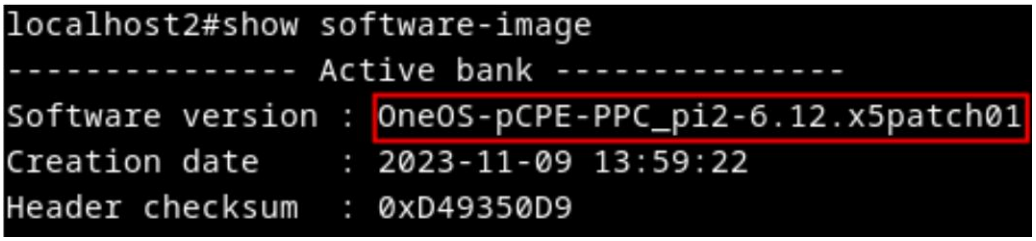


Ilustración 4. Imagen del sistema operativo

Si el administrador detecta que el sistema operativo que utiliza el dispositivo es diferente al mencionado anteriormente, deberá de ponerse en contacto inmediatamente con EKINOPS S.A. para solicitar el firmware evaluado y llevar a cabo la actualización del sistema. Para ello, los proveedores de servicios, operadores de telecomunicaciones y grandes empresas clientes de los productos de EKINOPS S.A., deberán de abrir una incidencia a través del sistema de tickets disponible en el Portal de Clientes (https://myconnect.ekinops.com/), para el cual es necesario disponer de registro previo. Otros usuarios que requieran soporte o deseen comunicar incidencias podrán hacerlo mediante el formulario web disponible en https://www.ekinops.com/contacts. Asimismo, las cuestiones relacionadas con la seguridad de los productos podrán notificarse a través de la dirección de correo electrónico product.security@ekinops.com.

e) Una vez obtenido dicho firmware (*OneOS-pCPE-PPC_pi2-6.12.x5patch01.ZZZ*) será necesario introducirlo en el dispositivo e instalarlo, para ello será necesario ejecutar el siguiente comando:

```
CLI> software-image install OneOS-pCPE-PPC_pi2-6.12.x5patch01.ZZZ
```

f) Ejecutar el siguiente comando para forzar que sólo haya un administrador en el dispositivo:

```
CLI(config)> user single-admin-user
```

6 FASE DE CONFIGURACIÓN

Una vez instalado el router es necesario configurarlo. A continuación, se muestran los pasos a seguir para configurar el producto. Para más información consultar la guía [REF2].

6.1 MODO DE OPERACIÓN SEGURO

Para activar el modo de operación seguro el usuario deberá de seguir los pasos descritos en el presente documento.

En concreto es obligatorio seguir las secciones indicadas a continuación, para que el dispositivo realice las siguientes funciones:

- Sección 6.4 CONFIGURACIÓN CRIPTOGRÁFICA: No permitirá el establecimiento de cualquier tipo de conexión que utilice suites de cifrado diferentes a las autorizadas durante la configuración.
- Sección 6.2 AUTENTICACIÓN: Las contraseñas se almacenarán protegidas con algoritmos sólidos (funciones hash). Así mismo, la política de contraseñas forzará a que las contraseñas de administrador estén compuestas por 12 caracteres como mínimo y contengan al menos una letra minúscula, una letra mayúscula, un número y un carácter especial.
- Sección 6.3.2 CONFIGURACIÓN DE ADMINISTRADORES: Implementará mecanismos de prevención de fuerza bruta por medio de blacklists.

El dispositivo hará uso de las siguientes suites de cifrado para los diferentes tipos de conexiones:

	Criptografía IKE (software)	Criptografía IPsec software	IPsec Aceleración Criptográfica por Hardware	Criptografía SSH (software)
Algoritmos de Encriptación				
AES-128-CBC	Sí	Sí	Sí	Sí
AES-192-CBC	Sí	Sí	Sí	Sí
AES-256-CBC	Sí	Sí	Sí	Sí
AES-128-GCM	No	No	Sí	Sí
AES-192-GCM	No	No	Sí	No
AES-256-GCM	No	No	Sí	Sí
AES-128-CTR	No	No	No	Sí
AES-192-CTR	No	No	No	Sí
AES-256-CTR	No	No	No	Sí
Algoritmos Hash				
HMAC SHA2-256	Sí	Sí	Sí	Sí
HMAC SHA2-256-etm@openssh.com	No	No	No	Sí
HMAC SHA2-384	Sí	Sí	Sí	No
HMAC SHA2-512	Sí	Sí	Sí	Sí

HMAC SHA2-512-etm@openssh.com	No	No	No	Sí
Intercambio de clave para IKE				
DH – 3072 (Group 15)	Sí	-	-	-
DH – 4096 (Group 16)	Sí	-	-	-
ECDH – 256 (Group 19)	Sí	-	-	-
ECDH – 384 (Group 20)	Sí	-	-	-
DH/DSA – 2048 (Group 24)	Sí	-	-	-
Intercambio de clave para SSH				
diffie-hellman-group16-sha512	-	-	-	Sí
diffie-hellman-group18-sha512	-	-	-	Sí
ecdh-sha2-nistp256	-	-	-	Sí
ecdh-sha2-nistp384	-	-	-	Sí
ecdh-sha2-nistp521	-	-	-	Sí

Tabla 1 Suites de Cifrado del dispositivo en el modo de operación seguro

6.2 AUTENTICACIÓN

Se utilizan contraseñas que contengan al menos una letra mayúscula, una letra minúscula, un número y un carácter especial con una longitud mínima de 12 caracteres como mecanismo de autenticación para los usuarios del TOE.

Por otra parte, en el primer inicio de sesión, el TOE forzará al usuario a cambiar la contraseña.

Esta autenticación será la que se utilice tanto para el inicio de sesión de manera local por el puerto serie como de manera remota haciendo uso de SSH.

Para que el mecanismo de autenticación funcione según los requisitos de cualificación del producto se deben realizar las siguientes acciones:

Configurar la política de contraseña correcta. Esto hará que se exija una contraseña de una longitud mínima de 12 caracteres y al menos una letra minúscula, una mayúscula, un carácter numérico y un carácter especial. Para ello habrá que ejecutar los siguientes comandos:

```
CLI(config)> aaa password-policy PWDPOLICY
CLI(conf-pwd-pol)> first-time-login password-change-enable
CLI(conf-pwd-pol)> exit
```

Crear un usuario administrador. En este caso se creará bajo el nombre de `user1`, sin embargo, el usuario puede utilizar otro nombre.

NOTA: Es recomendable que las cuentas con rol de administrador sean nominales y de uso exclusivo por una única persona, evitando el uso de cuentas compartidas.

Tras configurar este usuario como administrador y debido a la configuración realizada, el usuario `admin` (administrador por defecto) será eliminado automáticamente, quedando `user1` como el único usuario con privilegios de administrador.

CLI(config)> user-password-policy username user1 application cli password-policy PWDPOLICY

CLI(config)> user add user1 SecretP@ssword1 administrator clear-text type 3

NOTA: Existen tres tipos de roles predefinidos en el TOE que pueden ser utilizados para crear usuarios en el dispositivo estos son:

Rol predefinido	Privilegios	Nivel
User	Acceso a funciones elementales de visionado o funciones de diagnóstico como ping (configuración en modo sólo lectura), ningún acceso al sistema de archivos.	0
Manager	Acceso a todas las funciones de visionado, rastros y algunas funciones de configuración, puede ver y leer archivos, pero sin posibilidad de hacer cambios en el sistema de archivos.	7
Administrator	Acceso a toda la funcionalidad del dispositivo, incluyendo: - depuración avanzada - visionado avanzado - Comandos operacionales avanzados (escritura en el sistema de ficheros, instalación de nuevo firmware, reinicio del dispositivo, borrar sesiones de otros usuarios...) - Comandos de configuración avanzada (creación de usuarios de consola, cambio en los privilegios de los usuarios...)	15

Tabla 2. Roles y privilegios del dispositivo.

La siguiente tabla muestra la información de modo y privilegios para determinados comandos.

NOTA: Tenga en cuenta que los demás comandos que no se enumeran a continuación tienen asignado el nivel 7 de forma predeterminada

Comando	Modo	Nivel
clear expert	operational	15
clear vty-session	operational	15
copy	operational	15
debug expert	operational	15
disable	operational	0
display-level	operational	0
do	configure	15
enable	operational	0
erase	operational	15
exec	operational	15
exit	operational	0
expert scp	operational	15
help	operational	0
id	operational	0
idle-timeout	operational	0
ignore-leading-space	operational	0
logout	operational	0

logout session	operational	15
logout user	operational	15
mkdir	operational	15
mv	operational	15
nslookup	operational	0
paginate	operational	0
ping	operational	0
ping6	operational	0
pipe commands (save & append)	configure / operational	15
power	operational	15
privilege	configure	15
prompt1	operational	0
prompt2	operational	0
pwd	operational	0
quit	operational	0
reboot	operational	15
reboot_c	operational	15
restore	operational	15
rm	operational	15
rmtree	operational	15
save	operational	15
show boot version	operational	0
show expert	operational	15
show memory	operational	0
show privilege	operational	0
show software-image	operational	0
show system	operational	0
show version	operational	0
software-image	operational	15
ssh	operational	0
system	operational	0
telnet	operational	0
term	operational	0
terminal	operational	0
time	operational	0
timestamp	operational	0
traceroute	operational	0
traceroute6	operational	0
user	configure	15
username	configure	15
whoami	operational	0
write	operational	15
ztp bootstrap	operational	15

Tabla 3. Lista de comandos según el nivel de privilegio

Para crear cualquier tipo de usuario se utilizará el siguiente comando:

CLI(config)> user add <username> <password> { user | manager | administrator | <0-15> } [{ clear-text type {2|3} | encrypted type {2|3} <salt> }]

NOTA: El uso de la opción opcional `{ clear-text type {2|3} | encrypted type {2|3} <salt> }` define cómo se almacena la contraseña:

- Sin las palabras clave opcionales *encrypted* o *clear-text* con las palabras clave *clear-text type 2*, puedes ingresar la contraseña en texto claro y se almacenará en formato cifrado utilizando el tipo de cifrado heredado predeterminado tipo 2 (algoritmo PBKDF2).
- Con la opción c*lear-text type 3*, ingresas la contraseña en texto claro y se almacenará en formato cifrado utilizando el algoritmo de cifrado tipo 3, que es PBKDF2 basado en HMAC SHA256.
- Con la opción *encrypted type 2 <salt>*, puedes ingresar un usuario y contraseña previamente guardados, que fueron cifrados con el cifrado heredado predeterminado tipo 2 (algoritmo PBKDF2) y un valor de <salt>.
- Con la opción *encrypted type 3 <salt>*, puedes ingresar un usuario y contraseña previamente guardados, que fueron cifrados con el algoritmo de cifrado tipo 3 (PBKDF2 basado en HMAC SHA256) y un valor de <salt>.

Configurar el tiempo de inactividad máximo a 300 segundos:

CLI(config)> console timeout 300

6.3 ADMINISTRACIÓN DEL PRODUCTO

En el caso de que se desee realizar la administración de manera remota se deberán realizar las siguientes configuraciones:

Configurar una dirección IP donde quieras realizar las tareas de administración:

CLI(config)> interface gigabitethernet 0/0

CLI(config-if)> ip address 192.168.1.1 255.255.255.0

CLI(config-if)> exit

Los protocolos SSH/SCP/Netconf pueden vincularse a una lista de acceso. El ejemplo de lista de acceso ACL1 permite todo el tráfico IP, pero puede configurarse según las necesidades del cliente:

CLI(config)> ip access-list standard ACL1

CLI(config-std-nacl)> permit any

CLI(config-std-nacl)> exit

CLI(config)> exit

Crea la clave pública RSA de longitud 2048 para autenticarse contra un host remoto:

CLI> crypto key zeroize rsa

CLI> crypto key generate rsa 2048 no-confirm

CLI(config)> bind ssh acl ACL1

CLI(config)> bind ssh gigabitethernet 0/0

Por defecto SSH está desactivado, por tanto, para activarlo es necesario ejecutar los siguientes comandos:

```
CLI(config)> ip ssh enable
CLI(config)> ip ssh max-sessions 3
CLI(config)> ip ssh timeout 300
```

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

El TOE ofrece administración del dispositivo de manera local por medio del puerto de consola, haciendo uso de un cable RS-232 y administración remota por medio de los protocolos SSHv2 y túnel IPSEC.

El TOE presenta ciertos protocolos inseguros activos tales como:

- Telnet
- SNMP

Para desactivarlos será necesario ejecutar los siguientes comandos, tal y como se indica en el párrafo siguiente:

```
CLI (config) > ip telnet disable
CLI (config) > snmp agent-disable
```

Para la configuración de los protocolos seguros el administrador del dispositivo debe asegurarse que ha seguido correctamente los pasos descritos en la sección *5 FASE DE INSTALACIÓN* para SSH.

Por otro lado, el administrador del dispositivo debe configurar las suites de cifrado siguiendo la sección 6.4 CONFIGURACIÓN CRIPTOGRÁFICA que también servirá para configurar el protocolo IPSEC.

Para comprobar el estado final de la configuración de SSH e IPSEC, el administrador podrá ejecutar los siguientes comandos.

Para SSH:

```
CLI> show ip ssh client algorithms
CLI> show ip ssh server algorithms
```

Para IPSEC:

```
CLI> show crypto ipsec statistics
CLI> show crypto ikev2 stats
```

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

El fabricante detalla en sus guías los tres tipos diferentes de usuario que implementa el dispositivo. Estos son descritos en la Tabla 2. Roles y privilegios del dispositivo. del presente documento.

En el párrafo 0 de la sección 5, el administrador deberá **configurar una política de contraseña conforme a lo requerido en la cualificación**. Antes de crear un usuario, se debe

ejecutar el siguiente comando para garantizar que, cuando dicho usuario sea creado posteriormente, se le aplique la política de contraseñas configurada:

CLI(config)> user-password-policy username <username> application cli password-policy <password_policy>

Después de configurar la política de contraseñas, el administrador podrá crear un usuario utilizando el mismo nombre de usuario definido anteriormente. Es fundamental especificar el rol del usuario dentro del sistema mediante el indicador "role". Para ello, el administrador debe ejecutar el siguiente comando:

CLI(config)> user add <username> <password> <role> clear-text type 3

Como mecanismo para evitar ataques de autenticación por fuerza bruta, la siguiente configuración obligará a un usuario de la CLI a esperar <quarantine-delay> segundos (ejemplo: 30 segundos) después de <n> (ejemplo: 3) intentos de inicio de sesión fallidos consecutivos antes de poder intentar iniciar sesión de nuevo:

CLI(config)> blacklist attempts 3 quarantine-delay 30

6.4 CONFIGURACIÓN CRIPTOGRÁFICA

6.4.1 CONFIGURACIÓN DE CIPHERSUITES Y SERVICIOS

Ejecutar el siguiente comando para configurar que sólo las ciphersuites permitidas sean las disponibles en el dispositivo:

CLI(config)> ip ssh server algorithm encryption include aes128-ctr aes192-ctr aes256-ctr aes128-cbc aes192-cbc aes256-cbc

CLI(config)> ip ssh server algorithm mac include hmac-sha1 hmac-sha2-256 hmac-sha2-512

CLI(config)> ip ssh server algorithm key-exchange include diffie-hellman-group14-sha1 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521

CLI(config)> ip ssh client algorithm encryption include aes128-ctr aes192-ctr aes256-ctr aes128-cbc aes192-cbc aes256-cbc

CLI(config)> ip ssh client algorithm mac include hmac-sha1 hmac-sha2-256 hmac-sha2-512

CLI(config)> ip ssh client algorithm key-exchange include diffie-hellman-group14-sha1 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521

Deshabilitar servicios no incluidos en la cualificación:

CLI(config)> ip telnet disable

CLI(config)> snmp agent-disable

Habilitar la protección ante ataques fuerza bruta y de denegación de servicio:

CLI(config)> blacklist attempts 3 quarantine-delay 30

```
CLI(config)> ddos-protection
CLI(config)> ddos-protection local-policer default
CLI(ddos-local-policer)> exit
```

6.4.2 CONFIGURACIÓN DE IPSEC

Entra en el modo de propuesta IKEv2 con el nombre por defecto:

```
CLI(config)> crypto ikev2 proposal default
```

Configura los algoritmos de cifrado para esta propuesta IKEv2:

```
CLI(config-ikev2-proposal)> encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
```

Configura los algoritmos de integridad para esta propuesta IKEv2:

```
CLI(config-ikev2-proposal)> integrity sha256 sha384 sha512
```

Configura los algoritmos Diffie-Hellman para esta propuesta IKEv2:

```
CLI(config-ikev2-proposal)> group 14 15 16 19 20
```

Sal del modo de configuración de la propuesta IKEv2. Cualquier combinación de los algoritmos configurados será aceptada como una combinación válida de IKEv2:

```
CLI(config-ikev2-proposal)> exit
```

Puedes repetir los pasos anteriores para configurar múltiples propuestas IKEv2, sustituyendo *default* por el nombre que se desee asignar a cada propuesta:

```
CLI(config)> crypto ikev2 proposal <NOMBRE>
CLI(config-ikev2-proposal)> encryption <ENCRYPTION-ALGORITHMS>
CLI(config-ikev2-proposal)> integrity <INTEGRITY ALGORITHMS>
CLI(config-ikev2-proposal)> group <GROUPS>
CLI(config-ikev2-proposal)> exit
```

NOTA: Para que puedan aplicarse las nuevas propuestas personalizadas, es necesario deshabilitar la propuesta por defecto:

```
CLI(config)> crypto disable default ikev2 proposal
```

6.4.2.1 CONFIGURACIÓN DE POLÍTICA IKEV2

Entra en el modo de política IKEv2 y asígnale un nombre:

```
CLI(config)> crypto ikev2 policy <policy-name>
```

Asocia la propuesta IKEv2 configurada previamente a la política. Puedes repetir este paso varias veces para asociar varias propuestas IKEv2 a la misma política. Las diferentes propuestas se comparan con las propuestas del par para encontrar una coincidencia:

```
CLI(config-ikev2-policy)> proposal default
```

Opcionalmente, puedes asignar la política solo a los túneles IPsec terminados en la dirección IP dada:

```
CLI(config-ikev2-policy)> match address local <ip-address>
```

Opcionalmente, puedes asignar la política solo a los túneles IPsec terminados en el VRF de reenvío dado (fvrf). Por defecto, el túnel puede estar en cualquier VRF (any):

```
CLI(config-ikev2-policy)> match fvrf { any | <fvrf-name> }
```

Sal del modo de configuración de la política IKEv2:

```
CLI(config-ikev2-policy)> exit
```

Puedes repetir los pasos anteriores para configurar múltiples políticas IKEv2. Para cada túnel IPsec, se buscará una política que coincida.

6.4.2.2 CONFIGURACIÓN DEL KEYRING IKEV2

Entra en el modo de configuración del keyring IKEv2 y asígnale un nombre:

```
CLI(config)> crypto ikev2 keyring <keyring-name>
```

Con el comando peer, entra en el modo de configuración del peer:

```
CLI(config-ikev2-keyring)> peer <peer-name>
```

Cada sub-bloque de peer se identifica mediante una dirección IP o un grupo de direcciones IP (subred) (IPv4 o IPv6). Esto es obligatorio. Para coincidir con cualquier dirección de peer, puedes usar 0.0.0.0 0.0.0.0 (IPv4) o 0::0/0 (IPv6):

```
CLI(config-ikev2-keyring-peer)> address { <A.B.C.D> [<mask>] | <X:X:X:X::X/<0-128>> }
```

Define las pre-shared keys asociadas. Primero, especifica la clave de firma <key> con la palabra clave local. La clave se introduce inicialmente como una cadena de un máximo de 90 caracteres. Ingrésala en texto claro con el nivel 5; esto la almacenará con cifrado AES-256 y mostrará el resultado en la configuración con la clave cifrada y el nivel 6:

```
CLI(config-ikev2-keyring-peer)> pre-shared-key local <key> 5
```

Ahora haz lo mismo para la clave de verificación con la palabra clave remote:

```
CLI(config-ikev2-keyring-peer)> pre-shared-key remote <key> 5
```

Sal del modo de configuración del peer del keyring IKEv2:

```
CLI(config-ikev2-keyring-peer)> exit
```

Sal del modo de configuración del keyring IKEv2:

```
CLI(config-ikev2-keyring)> exit
```

6.4.2.3 CONFIGURACIÓN DE UN PERFIL IKEV2

Entra en el modo de configuración del perfil IKEv2 y asígnale un nombre:

```
CLI (config)> crypto ikev2 profile <profile-name>
```

Primero, define si la autenticación en el lado local usará claves precompartidas (pre-share) o un certificado X.509 (rsa-sig):

```
CLI(config-ikev2-profile)> authentication local {pre-share | rsa-sig}
```

Luego, define lo mismo para el lado del peer:

```
CLI(config-ikev2-profile)> authentication remote {pre-share | rsa-sig}
```

Configura al menos una coincidencia de identidad remota. La identidad del peer se usa para encontrar el perfil IKE válido. Si no se configura al menos una identidad remota, el perfil se considera incompleto y no se utilizará. Un perfil IKEv2 puede tener múltiples declaraciones de coincidencia de identidad. Estas son las opciones:

- **any:** No verifica la identidad presentada en la carga útil de IKEv2, típicamente usada con autenticación por certificado.
- **email:** Verifica la identidad del peer como una cadena de correo electrónico completamente calificada.
- **fqdn:** Verifica la identidad del peer como un nombre de dominio completamente calificado en la forma <name>.<domain>.<extension>. Opcionalmente, la parte <name> puede omitirse o reemplazarse por un * como comodín.
- **fqdn domain:** Verifica la identidad del peer como un nombre de dominio completamente calificado en la forma <domain>.<extension>:

```
CLI(config-ikev2-profile)> match identity remote {any | email <email> | fqdn <name>.<domain>.<extension> | fqdn <domain>.<extension>}
```

Usa esta configuración para hacer coincidir la solicitud entrante de IKEv2 con su dirección IP de destino:

```
CLI(config-ikev2-profile)> match address local <ip-address>
```

Usa el siguiente comando para hacer coincidir el perfil IKEv2 con un Front-Door VRF (FVRF). Solo se puede configurar una coincidencia de fvrf por perfil IKE. Al combinar coincidencias de diferentes tipos (identidad, local y fvrf), todos los tipos deben coincidir para que el perfil IKE coincida:

```
CLI(config-ikev2-profile)> match fvrf { any | <fvrf-name> }
```

Puedes definir la identidad IKE local para identificarte ante el peer. Estas son las opciones:

- **dn:** Usa esta opción con autenticación por certificado. Tomará el subjectAltName del certificado como la identidad presentada en la carga útil de autenticación.
- **email:** Usa esta opción para una cadena de correo electrónico completamente calificada.
- **fqdn:** Usa esta opción para un nombre de dominio completamente calificado:

```
CLI(config-ikev2-profile)> identity local {dn | email <email>| fqdn <fqdn-string> }
```

Si se ha elegido la autenticación local con claves precompartidas, hace referencia a un keyring local previamente definido para definir la información relacionada:

```
CLI(config-ikev2-profile)> keyring local <keyring-name>
```

En caso de autenticación con certificados, hace referencia a un trust-point previamente definido para definir la información relacionada:

```
CLI(config-ikev2-profile)> pki trustpoint <trustpoint>
```

La Detección de Peer Muerto (DPD) es una función de IKE para actualizar regularmente el estado de vida del peer. Si el peer no responde a tiempo, la conexión IKE se considera muerta y se cierran todas las SA de IPsec asociadas. El DPD puede configurarse globalmente para todos los perfiles IKEv2 o sobrescribirse por una configuración específica para cada perfil IKEv2. Estos son los parámetros:

- El primer parámetro es el tiempo de espera sin tráfico; cuando no se recibe tráfico del peer durante este período, se envía un mensaje de keepalive para verificar si sigue activo. Cualquier valor entre 2 y 3600 segundos puede configurarse.
- El segundo parámetro es el Intervalo de Reintento de DPD. Este es el número de segundos entre reintentos de keepalive si el mensaje anterior falla. Cualquier valor entre 1 y 60 segundos puede configurarse.
- periodic: Cuando se agrega esta palabra clave, se envían consultas DPD a intervalos regulares, incluso si se detectó tráfico en el túnel.
- on-demand: Cuando se agrega esta palabra clave, se envían consultas DPD solo cuando es necesario:

```
CLI(config-ikev2-profile)> dpd <2-3600> <1-60> {periodic | on-demand}
```

La vida útil de una Asociación de Seguridad IKEv2 está limitada para evitar cualquier hackeo. Un nuevo intercambio IKE tiene lugar antes del final de la vida útil actual para reemplazar las claves actuales por nuevas. Opcionalmente, se puede modificar el tiempo de vida predeterminado de IKEv2 de 1 hora o 3600 segundos a otro valor. <lifetime> se expresa en segundos:

```
CLI(config-ikev2-profile)> lifetime <lifetime>
```

Sal del modo de configuración del perfil IKEv2:

```
CLI(config-ikev2-profile)> exit
```

6.4.2.4 HABILITAR EL MOTOR CRIPTOGRÁFICO

```
CLI(config)> crypto engine enable
```

Configuración del perfil IPSEC:

Crea un conjunto de transformación IPsec y entra en el modo de configuración de transform-set IPsec. Dado que se pueden configurar múltiples transform-set, debes darle a cada uno un nombre único:

```
CLI(config)> crypto ipsec transform-set <name>
```

En el modo de transform-set, puedes configurar el algoritmo que se presentará al peer de terminación IPsec. Elige cualquiera de los comandos listados. Los algoritmos de cifrado ESP-GCM solo pueden usarse con el motor de cifrado habilitado:

CLI(crypto-trans)> esp-aes [esp-sha256-hmac | esp-sha384-hmac | esp-sha512-hmac]

CLI(crypto-trans)> esp-aes-192 [esp-sha256-hmac | esp-sha384-hmac | esp-sha512-hmac]

CLI(crypto-trans)> esp-aes-256 [esp-sha256-hmac | esp-sha384-hmac | esp-sha512-hmac]

CLI(crypto-trans)> esp-gcm

CLI(crypto-trans)> esp-gcm-192

CLI(crypto-trans)> esp-gcm-256

Opcionalmente, puedes cambiar el modo de túnel IPsec (por defecto) de túnel a transporte. En el modo túnel, el punto final del túnel IPsec agrega una nueva cabecera IP y una cabecera IPsec al paquete original. En el modo transporte, el punto final del túnel solo agrega una cabecera IPsec al paquete:

CLI(crypto-trans)> mode { transport | tunnel }

Sal del modo de configuración del transform-set:

CLI (crypto-trans)> exit

Define los parámetros de IPsec que se usarán para la protección IPsec entre dos peers y entra en el modo de configuración del perfil IPsec:

CLI(config)> crypto ipsec profile <profile-name>

Si deseas que OneOS6 solo responda a las solicitudes IPsec de sus peers, debes configurarlo:

CLI(ipsec-profile)> responder-only

Hace referencia a un transform-set previamente configurado para definir las combinaciones de algoritmos de cifrado que aceptas usar, en orden de prioridad. Puedes hacer referencia a múltiples transform-sets. Si no se configura, se utilizará un transform-set predeterminado (AES-128-CBC con SHA-1, a menos que el transform-set predeterminado haya sido reconfigurado):

CLI(ipsec-profile)> set transform-set <transform-set-name1> <transform-set-name2> ...

Perfect Forward Secrecy (PFS) es una opción recomendada donde el cálculo inicial y renovado de claves IPsec no se deriva de la negociación inicial de IKE para mejorar la seguridad. Para usar PFS, se debe configurar un grupo Diffie-Hellman (DH). DH es el algoritmo para calcular una nueva clave. Un número de grupo DH más alto proporciona un intercambio más seguro, pero toma más tiempo calcular la nueva clave. Por defecto, PFS no está habilitado:

CLI(ipsec-profile)> set pfs {group14 | group15 | group16 | group19 | group20 | group24}

Si deseas que la Asociación de Seguridad (SA) de IPsec se elimine si no pasa ningún dato durante un cierto tiempo, puedes configurar el tiempo de inactividad en segundos. Por defecto, el tiempo de inactividad está deshabilitado (valor 0):

```
CLI(ipsec-profile)> set security-association idle-time <0 | 60-86400>
```

Una SA de IPsec tiene un tiempo de vida. Antes de que expire la SA de IPsec, se configurará una nueva SA para reemplazar a la que está por expirar. Este tiempo de vida se puede configurar en segundos o en kilobytes de tráfico reenviado. Por defecto, una SA de IPsec expira después de 3600 segundos (1 hora) o cuando se han reenviado 4608000 KBytes (4,608 GBytes), lo que ocurra primero. Estos valores predeterminados se pueden modificar con los comandos mencionados:

```
CLI(ipsec-profile)> set security-association lifetime seconds <120-86400>
CLI(ipsec-profile)> set security-association lifetime kilobytes <2560-4294967295>
```

Opcionalmente, el tiempo de inactividad basado en volumen puede deshabilitarse con este comando. Ten en cuenta que el tiempo de vida basado en tiempo no puede deshabilitarse:

```
CLI(ipsec-profile)> set security-association lifetime kilobytes disable
```

Referencia a un perfil IKEv2 previamente definido:

```
CLI(ipsec-profile)> set ikev2-profile <ikev2-profile-name>
```

Sal del modo de configuración del perfil IPsec:

```
CLI(ipsec-profile)> exit
```

Configuración del túnel de IPSEC:

1) Crea una interfaz de túnel y entra en el modo de configuración de la interfaz de túnel:

```
CLI(config)> interface tunnel <unit>
```

Define el modo de túnel: usa IPSEC para encapsular la carga útil cifrada en un nuevo encabezado IP. Usa gre para encapsular la carga útil cifrada en un encabezado GRE. Puedes especificar que el encabezado exterior sea IPv4 (predeterminado) o IPv6:

```
CLI(config)> tunnel mode {ipsec | gre} [ipv4 | ipv6]
```

Aplica el perfil IPsec a este túnel. Esto implica que la carga útil del túnel será cifrada:

```
CLI(config-if)> tunnel protection ipsec profile <prof-name>
```

Una interfaz de túnel debe tener una dirección IP interna para todo el tráfico enviado o recibido por el router, como tráfico de enrutamiento y tráfico IKE. Sin esta dirección IP, la interfaz de túnel no es enrutable. Puedes configurar la dirección IP directamente como una dirección IPv4 o IPv6 con su subred, o la interfaz de túnel puede tomar prestada la dirección IP de otra interfaz (unnumbered interface). Usa uno de estos comandos:

```
CLI(config-if)> ip unnumbered <interface-type> <unit>
CLI(config-if)> ip address <ip-address> <netmask>
CLI(config-if)> ipv6 address <ipv6-address>/<0-128>
```

Una interfaz de túnel debe tener una dirección IP externa de origen. Todo el tráfico cifrado enviado utiliza esta dirección IP externa como dirección de origen, y todo el tráfico cifrado recibido tiene esta dirección IP externa como dirección de destino. Esta dirección puede ser una dirección IPv4 o IPv6 configurada, o puede ser tomada prestada de una interfaz:

CLI(config-if)> tunnel source { <X.X.X.X> | <X:X:X:X::X> |<type> <unit> }

Una interfaz de túnel debe tener una dirección IP externa de destino. Todo el tráfico cifrado enviado utiliza esta dirección IP externa como dirección de destino, y todo el tráfico cifrado recibido tiene esta dirección IP externa como dirección de origen. Esta dirección puede ser una dirección IPv4 o IPv6 configurada. Se pueden configurar múltiples direcciones IP; el túnel intentará establecer una conexión comenzando con la primera dirección IP. Si esto falla, intentará con la segunda dirección IP y así sucesivamente en un ciclo hasta que se pueda establecer una conexión. Alternativamente, se puede usar un nombre de host. El nombre de host se resolverá con DNS para encontrar la dirección IP correspondiente:

CLI(config-if)> tunnel destination { <X.X.X.X> [<Y.Y.Y.Y> <Z.Z.Z.Z> ...] | <X:X:X:X::X> [<Y:Y:Y::Y> <Z:Z:Z::Z> ...] | host <hostname>}

Sal del modo de configuración de la interfaz de túnel para aplicar la configuración del túnel:

CLI(config-if)> exit

Ejecuta el siguiente comando para configurar de manera correcta la auditoría:

CLI(config)> logging timestamp datetime msec

CLI(config)> login on-success log

CLI(config)> login on-failure log

6.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

El TOE presenta ciertos los protocolos inseguros activos tales como:

- Telnet
- SNMP

Para desactivarlos será necesario ejecutar los siguientes comandos (esta operación ya se describió en el párrafo 0):

CLI (config) > ip telnet disable

CLI (config) > snmp agent-disable

6.6 CONFIGURACIÓN DEL SISTEMA DE COMUNICACIÓN INALÁMBRICA MÓVIL

Si se desea hacer uso de la funcionalidad 4G del dispositivo se deberá realizar los pasos indicados a continuación.

Introducir la tarjeta SIM en la primera ranura SIM que se encuentra en la parte frontal del dispositivo.

En la terminal de configuración del dispositivo ejecuta el siguiente comando, reemplazando la palabra “pin-code” por el código pin de la tarjeta SIM introducida en el dispositivo:

CLI> cellular-radio pin-code install <pin-code> <confirm-pin-code> [sim-slot { 1 | 2 | both }] [encryption-type <enctypes>]

Ejecuta el siguiente comando. Es importante que este comando se ejecute sólo una vez:

CLI> cellular-radio pin-code install 1234 1234 sim-slot 1 encryption-type aes256-rfc5649

Crea un objeto de controlador celular:

CLI(config)> controller cellular 0

Establece el modo de funcionamiento del enlace de radio celular. El valor predeterminado es auto, que comenzará con la tecnología más alta: primero 5G, luego 4G, 3G, 2G. Para probar el TOE, selecciona 4G para asegurarte de que solo se utilice este modo de funcionamiento:

CLI(cellular)> mode <2g | 3g | 2g+3g | 4g | 2g+4g | 3g+4g | 3g+4g+5g | 4g+5g | 5g | auto>

En el objeto del controlador celular, crea un perfil celular que contenga los parámetros que la interfaz celular utilizará para establecer una conexión inicial con una red celular:

CLI(cellular)> profile <1-255>

En el perfil celular, ingresa el nombre del Punto de Acceso (APN) del proveedor de la red celular:

CLI(profile)> apn <apn-name>

Proporciona el nombre de usuario y la contraseña en caso de que el proveedor lo requiera. Elige el nivel 2 para la contraseña para que se encripte utilizando el algoritmo AES-256 (RFC-5649):

CLI(profile)> username <username>

CLI(profile)> password <password> [<level>]

Sal de la configuración del perfil:

CLI(profile)> exit

Indica a la interfaz celular qué parámetros del perfil utilizar para su conexión inicial:

CLI(cellular)> attach-profile <index>

Sal de la configuración del controlador celular:

CLI(cellular)> exit

Para llevar la interfaz celular al camino de reenvío, se necesita crear una interfaz ethernet virtual:

CLI(config)> interface virtual-ethernet <1-255>

Vincula la interfaz ethernet virtual al objeto del controlador celular y al perfil celular creados en los pasos anteriores:

```
CLI(config-if)> cellular 0 profile <1-255>
```

La interfaz ethernet virtual ejecuta DHCP por defecto, por lo que no es necesario configurarlo explícitamente. Aplica la traducción dinámica de direcciones de red (NAPT) para mapear los números de puerto y las direcciones IP privadas en la dirección IP pública recibida del proveedor de servicios celulares a través de DHCP:

```
CLI(config-if)> ip nat inside overload
```

Sal del modo de configuración de la interfaz ethernet virtual para aplicar la configuración:

```
CLI(config-if)> exit
```

6.7 GESTIÓN DE CERTIFICADOS

El producto utiliza certificados X.509 para la autenticación de IPsec. Para configurar un certificado X.509, se deben seguir los siguientes pasos:

a) Generar un CSR **(Certificate Signing Request)**: Cree una solicitud de firma de certificado para el cliente.

b) Utilice uno de los siguientes parámetros para la clave: Clave de tipo ECDSA, con un tamaño de 256 o 384 bits, y el algoritmo de firma SHA-384 o SHA-256. Clave de tipo RSA, con una longitud mínima de 3072 bits.

c) **Enviar el CSR a la Autoridad Certificadora (CA)**: Utilice la CA existente para firmar el CSR y emitir un certificado cliente. Este proceso asegura que el certificado sea válido y confiable.

d) **Almacenar los certificados en el almacenamiento local**: Una vez firmado, almacene tanto el certificado del cliente como el certificado de la CA en el sistema local para su uso posterior.

e) **Configurar la revocación de certificados**: Utilice listas de revocación de certificados (CRL) o el protocolo de estado de certificado en línea (OSCP), según las necesidades de seguridad.

f) **Configurar el certificado para su uso con IKE**: Configure los parámetros necesarios para que el certificado se utilice con IKE, asegurando una autenticación adecuada para las conexiones IPsec.

Es recomendable seguir cuidadosamente los pasos definidos en la sección 6.4 CONFIGURACIÓN CRIPTOGRÁFICA asegurar una configuración segura y conforme a las políticas establecidas.

6.8 ACTUALIZACIONES

La actualización del software debe realizarse siguiendo la guía [REF2]**.**

Se recomienda el uso de un ordenador adicional configurado con un servidor SFTP con el fin de realizar la instalación correcta del software.

El TOE no realiza comprobaciones automáticas para detectar nuevas actualizaciones de software o firmware. La identificación de nuevas versiones debe ser llevada a cabo manualmente por el administrador mediante la consulta del portal de clientes de Ekinops.

Para llevar a cabo la instalación, el administrador deberá ejecutar el siguiente comando:

```
CLI> software-image install sftp://login:password@192.168.1.2/OneOS-pCPE-PPC_pi2-6.12.x5patch01.ZZZ
```

Para verificar la versión del software instalada en el dispositivo se debe de ejecutar el siguiente comando:

```
CLI> show software-image
```

6.9 AUDITORÍA

6.9.1 REGISTRO DE EVENTOS

Los eventos se almacenan en un archivo en el directorio raíz, con un índice de extensión que comienza en 1. Cada archivo tiene un tamaño máximo (por defecto, 16 KBytes). Cuando un archivo se llena, se crea otro archivo nuevo hasta alcanzar un número máximo de archivos configurables (por defecto, 4). Luego, se inicia una rotación donde el archivo más antiguo se sobrescribe.

El proceso de rotación de registros funciona de la siguiente manera (ejemplo con el nombre del archivo de registro `events.txt`):

- Si `events.txt` alcanza su tamaño máximo, se copia a `events.txt.1` y se crea un nuevo `events.txt`.
- La próxima vez, `events.txt.1` se convierte en `events.txt.2` y `events.txt` pasa a ser `events.txt.1`.
- Si ya existen los 4 archivos, la próxima vez se elimina `events.txt.4`.
- Por tanto, los registros se encuentran en los archivos *events.txt*, *events.txt.1*, *events.txt.2*, *events.txt.3* y *events.txt.4*, del más reciente al más antiguo.

Cada evento tiene un nivel de severidad que indica la importancia del evento para el funcionamiento adecuado del dispositivo en la red. Los niveles de severidad posibles son:

<Nivel>	Descripción	Valor numérico de severidad
emergency	Mensajes de emergencia	0
alert	Acción inmediata necesaria	1
critical	Condiciones críticas	2
errors	Condiciones de error	3
warnings	Condiciones de advertencia	4
notifications	Condiciones normales pero significativas	5
Informational	Mensajes informativos	6
debug	Mensajes de depuración	7
debug-expert	Mensajes de depuración experta	8

Tabla 4. Nivel de severidad para la importancia de los eventos

Para almacenar todos los eventos en un búfer de RAM con un tamaño máximo de 100000 bytes (el valor predeterminado es 16384) para niveles de registro mayores o iguales a ***debug***:

```
CLI(config)> logging buffered debug
CLI(config)> logging buffered size 100000
CLI(config)> logging buffered filter all
```

Para poder ver los eventos almacenados se puede hacer uso de los siguientes comandos.

Si se encuentra en buffer:

```
CLI>show logging
```

Si se encuentra almacenado en un archivo:

```
CLI> cat logfile.txt
```

6.9.2 ALMACENAMIENTO LOCAL

Para almacenar todos los eventos en un archivo llamado `logfile.txt` en el sistema de archivos persistente para niveles de registro mayores o iguales a `debug`:

```
CLI(config)> logging file debug
CLI(config)> logging file name logfile.txt
CLI(config)> logging file filter all
```

6.9.3 ALMACENAMIENTO REMOTO

Para enviar todos los eventos a un servidor de auditoría (syslog) con el número de puerto 23 a través de UDP en la dirección IP <IP-address>, para niveles de registro mayores o iguales a **debug.**

```
CLI(config)> syslog server <IP-address> 23 udp
CLI(config)> logging syslog debug
CLI(config)> logging syslog filter all
```

Los mensajes de syslog en la configuración anterior se envían a través de UDP al servidor syslog, **lo cual no es un protocolo seguro por naturaleza**. Para cumplir con los requisitos de la cualificación, los mensajes de syslog **deben enviarse a través de un canal seguro**, como el **túnel IPsec** configurado en el capítulo 3.5 de Canales de Confianza de [REF2]. Para esto, se puede agregar una ruta estática a la configuración, por ejemplo:

```
CLI(config)> ip route 30.30.30.30 255.255.255.255 tunnel 1
```

Para que todos los mensajes de registro proporcionen la fecha y hora actual (con precisión de milisegundos), se utilizará el siguiente comando de configuración:

```
CLI(config)> logging timestamp datetime msec
```

6.10 AUTO-CHEQUEOS

El dispositivo realiza comprobaciones automáticas (auto-chequeos) de integridad del firmware durante los procesos de arranque y reinicio. Además, dichas verificaciones pueden ser realizadas bajo demanda cuando así lo solicite un usuario autorizado

Para iniciar el proceso de verificación bajo demanda, el usuario autorizado debe ejecutar los siguientes comandos en la interfaz de línea de comandos:

```
CLI(config)> software-image verify
```

Las verificaciones realizadas incluyen:

- Validación de la integridad del código binario almacenado en la memoria flash.
- Confirmación de que el código en la memoria RAM coincide exactamente con el código en la memoria flash, garantizando que el software no ha sido alterado (aplicable únicamente al firmware activo).

La ejecución de esta verificación se realiza con una prioridad relativamente baja, con el fin de no interferir con otras acciones de gestión del dispositivo. Durante el proceso, se muestran mensajes indicando el inicio y finalización exitosa de la operación. Ejemplo:

```
CLI> software-image verify

Starting code integrity check on active firmware. This operation can be time-consuming.

.....

Check operation succeeded.
```

Para verificar las comprobaciones automáticas realizadas durante el arranque o reinicio, el administrador debe conectarse al dispositivo mediante el puerto de consola y revisar la información generada por el sistema en dicho proceso.

La salida generada durante el arranque incluye información detallada similar a la siguiente:

```
Checking OneOs software ...
Signature verification passed.
Starting OneOs software ...

Welcome to OneOS-pCPE-PPC_pi2-6.12.x5patch01 (integci_r1_1pa422b2_dev_photo174)!
```

Ilustración 5. Revisión de la integridad del software

7 FASE DE OPERACIÓN

El funcionamiento adecuado del producto depende de ciertas condiciones que deben estar presentes en su entorno. Es responsabilidad del administrador autorizado asegurarse de que el entorno operativo cumpla con los requisitos mencionados a continuación:

a) El producto deberá instalarse y mantenerse en **un entorno físico seguro**, como una sala **con control de acceso** o un entorno móvil bajo la supervisión del administrador.

b) El producto **no deberá incluir aplicaciones de uso general** como compiladores o aplicaciones de usuario.

c) Los administradores deben estar **debidamente capacitados** en el uso y operación del producto, así como en las características del entorno seguro donde se utiliza. Además, deberán seguir las guías y recomendaciones proporcionadas por el fabricante.

d) Los administradores deben **garantizar** que el producto esté siempre con la **versión** del **firmware autorizada** bajo la cualificación para protegerlo contra amenazas y vulnerabilidades conocidas.

e) Los administradores deberán mantener sus **credenciales** de **acceso** al producto de **manera segura y protegida**.

f) Los administradores deberán de realizar un **seguimiento** y **mantenimiento** de los **registros de auditoría frecuentemente** con el fin de asegurar que no son borrados, modificados ni accedidos por agentes no autorizados.

g) Los administradores deberán realizar una **verificación** del **sistema operativo** de manera frecuente haciendo uso del comando:

```
CLI> software-image verify active
```

h) Los administradores deben **eliminar** cualquier **información residual sensible** que pudiera quedar después de que el producto haya llegado al final de su vida útil.

8 REFERENCIAS

[REF1]	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación del CCN.	https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic
[REF2]	ONE2501 Security Configuration Guide version 1.3	N/A
[REF3]	Guía de Seguridad de las TIC CCN-STIC 140 (Taxonomía de productos STIC -Anexo D.1-M: Enrutadores). Septiembre 2023.	https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3926-guia-140-anexo-d-1m-enrutadores/file?format=html
[REF4]	Security Target Description ONE2501 version 1.3, 24/01/2024	N/A
[REF5]	Definición de la Certificación Nacional Esencial de Seguridad (LINCE), versión 2.0. Marzo 2022. Centro Criptológico Nacional.	https://oc.ccn.cni.es/documentos/criterios-y-metodologias/79-ccn-stic-2001-definicion-de-la-certificacion-nacional-esencial-de-seguridad-lince/file
[REF6]	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE), versión 2.0. Marzo 2022. Centro Criptológico Nacional.	https://oc.ccn.cni.es/documentos/criterios-y-metodologias/80-ccn-stic-2002-metodologia-de-evaluacion-para-la-certificacion-nacional-esencial-de-seguridad-lince/file

9 ABREVIATURAS

4G/LTE	Fourth Generation/Long-Term Evolution
CPD	Centro de Procesamiento de Datos
DNS	Domain Name System
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad.
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
LAN	Red de Área Local
Mbps	Megabits per second
PYME	Pequeña y Mediana Empresa
RSA	Rivest-Shamir-Adleman
SA	Asociación de Seguridad
SFP	Small Form-factor Pluggable
SIM	Subscriber Identity Module
SSHv2	Secure Shell version 2
TLS	Transport Layer Security
TOE	Objetivo de la evaluación (Target of Evaluation)
UTP	Par Trenzado No Blindado (Unshielded Twisted Pair)
WAN	Red de Área Amplia