centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1014

Procedimiento de Empleo Seguro
Cisco Routers IOS-XE con SD-WAN



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 14:07:01 +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 4
2 OBJETO Y ALCANCE 4
3 ORGANIZACIÓN DEL DOCUMENTO 4
4 FASE PREVIA A LA INSTALACIÓN 5
4.1 ENTREGA SEGURA DEL PRODUCTO 5
4.2 ENTORNO DE INSTALACIÓN SEGURO 13
4.3 CONSIDERACIONES PREVIAS 13
4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN 13
5 FASE DE INSTALACIÓN 14
5.1 INSTALACIÓN DEL SERVIDOR UCS Y DEL HIPERVISOR ESXI 14
5.2 INSTALACIÓN DE CONTROLADORES SD-WAN VIRTUALES 15
5.3 INSTALACIÓN FÍSICA DEL HARDWARE (ROUTERS CEDGE FÍSICOS) 15
5.4 INSTALACIÓN DEL SOFTWARE (ENRUTADORES CEDGE VIRTUALES) 16
6 FASE DE CONFIGURACIÓN 17
6.1 CONFIGURACIÓN CONTROLADORES SD-WAN 17
6.1.1 CONFIGURACIÓN DE LA INFORMACIÓN DEL SISTEMA DEL CONTROLADOR 17
6.1.2 CONFIGURACIÓN DE LA VPN DE GESTIÓN DEL CONTROLADOR 17
6.1.3 CONFIGURACIÓN DE LA VPN DE TRANSPORTE DEL CONTROLADOR 18
6.1.4 CONFIGURACIÓN DEL CONTROLADOR PARA CERTIFICADOS EMPRESARIALES 19
6.2 CONFIGURACIÓN ROUTER CEDGE 21
6.2.1 CARGAR EL ARCHIVO SERIE DE CEDGE EN VMANAGE 21
6.3 MODO DE OPERACIÓN SEGURO 25
6.4 AUTENTICACIÓN 26
6.4.1 AUTENTICACIÓN LOCAL EN CONTROLADORES POR CLI 26
6.4.2 AUTENTICACIÓN LOCAL EN CEDGE POR CLI 26
6.4.3 BLOQUEO POR INTENTOS FALLIDOS 27
6.4.4 BLOQUEO EN CONTROLADORES 27
6.4.5 BLOQUEO EN CEDGE 27
6.5 ADMINISTRACIÓN DEL PRODUCTO 27
6.5.1 ADMINISTRACIÓN LOCAL Y REMOTA 27
6.5.2 CONFIGURACIÓN DE ADMINISTRADORES 29
6.6 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 30
6.7 GESTIÓN DE CERTIFICADOS 32
6.8 SERVIDORES DE AUTENTICACIÓN 32
6.9 SINCRONIZACIÓN 32
6.10 ACTUALIZACIONES 33
6.11 AUTO-CHEQUEOS 33
6.12 AUDITORÍA 33
6.12.1 REGISTRO DE EVENTOS 33
6.12.2 ALMACENAMIENTO LOCAL 34
6.12.3 ALMACENAMIENTO REMOTO 34
6.13 BACKUP 34
7 REFERENCIAS 35
8 ABREVIATURAS 36

ÍNDICE DE TABLAS

Tabla 1 Imágenes Software 9
Tabla 2 Imágenes Software Virtual 10
Tabla 3 Imágenes Software Controladores 12
Tabla 4 Componentes del entorno de operación 13
Tabla 5 Mecanismos criptográficos autorizados para SSH 28
Tabla 6 Roles de los diferentes componentes del producto 29
Tabla 7 Configuración de interfaces y puertos según las diferentes redes 31

ÍNDICE DE FIGURAS

Figura 1: Menú de configuración de administración 19
Figura 2: Configuración de autorización de certificados del controlador 19
Figura 3: Configuración de autorización de certificados en la nube perimetral de la WAN 20
Figura 4: Página de gestión de certificados del controlador 20
Figura 5: Instalación del certificado del controlador 21
Figura 6: Certificados del controlador 21
Figura 7: Plug and Play Connect web 22
Figura 8: Ventana de Plug and Play (PnP) donde introducir los detalles 22
Figura 9: Ventana de Plug and Play (PnP) con los detalles completados 23
Figura 10: Ventana de Plug and Play (PnP) con dispositivos añadidos 23
Figura 11: Ventana de Plug and Play (PnP) con dispositivos añadidos 24
Figura 12: Lista vManage WAN Edge 24
Figura 13: Subida de archivos de números de serie en vManage 24
Figura 14: Subida de archivos de números de serie en vManage 25

1 INTRODUCCIÓN

Cisco SD-WAN ofrece una solución de WAN definida por software que permite a las empresas y organizaciones conectar a los usuarios con sus aplicaciones de forma segura. Proporciona una superposición de software que se ejecuta sobre el transporte de red estándar.

Esta red virtualizada se ejecuta en los routers (físicos) de Cisco cEdge que corren el software IOS-XE que ofrecen capacidades de red, seguridad y cortafuegos. Actúan como puntos de conexión centrales para el tráfico WAN distribuido, como el tráfico hacia y desde trabajadores remotos o sucursales.

Los controladores centralizados de SD-WAN, que supervisan el plano de control de la estructura de Cisco SD-WAN, gestionan de forma eficiente y segura el aprovisionamiento, el mantenimiento y la seguridad de toda la red superpuesta.

El controlador vManage proporciona un panel de control que simplifica las operaciones de red. Ofrece configuración, gestión, funcionamiento y supervisión centralizados en toda la estructura SD-WAN.

2 OBJETO Y ALCANCE

Este procedimiento de empleo seguro aplica a los routers de Cisco cEdge que corren el software **IOS XE 17.12** y controladores ejecutando el software **IOS-XE 20.12**.

El producto ha sido incluido en el catálogo CPSTIC, para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF8].

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.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

El producto es distribuido y está compuesto tanto por software como por hardware e incluye routers cEdge y controladores SD-WAN. Uno de los routers Cisco cEdge, el C8000V, se implementa como máquina virtual.

Para garantizar que se recibe el producto correcto, deben examinarse los componentes físicos y virtuales del producto con el fin de asegurarse de que no se haya manipulado de forma indebida durante la entrega. Dado que varios de los componentes del producto son máquinas virtuales, se recomienda al administrador autorizado que compruebe también los componentes del sistema virtual (VS).

Compruebe que el software y el hardware del router físico cEdge no hayan sido manipulados durante el envío mediante las siguientes acciones:

Antes de desembalar el producto, revise el embalaje físico en el que se entregó el equipo. Compruebe que el embalaje exterior de cartón lleve impresos el logotipo y los motivos de Cisco Systems. Si no es así, póngase en contacto con el proveedor del equipo (Cisco Systems o un distribuidor o socio autorizado de Cisco).

Compruebe que el embalaje no haya sido abierto y vuelto a cerrar de forma evidente, examinando la cinta que sella el paquete. Si parece que el paquete ha sido vuelto a cerrar, póngase en contacto con el proveedor del equipo (Cisco Systems o un distribuidor o socio autorizado de Cisco).

Compruebe que la caja lleve una etiqueta blanca de Cisco Systems con código de barras, a prueba de manipulaciones y que indique si ha sido manipulada, pegada en la caja de cartón exterior. Si no es así, póngase en contacto con el proveedor del equipo (Cisco Systems o un distribuidor o socio autorizado de Cisco). Esta etiqueta incluirá el número de producto de Cisco, el número de serie, y otra información relativa al contenido de la caja.

Anote el número de serie del producto en la documentación de envío. El número de serie que aparece en la etiqueta blanca pegada en la caja exterior será el del dispositivo. Compruebe que el número de serie que figura en la documentación de envío coincide con el número de serie que aparece en la factura del equipo, enviada por separado. Si no es así, póngase en contacto con el proveedor del equipo (Cisco Systems o un distribuidor o socio autorizado de Cisco).

Compruebe que la caja haya sido enviada efectivamente por el proveedor previsto del equipo (Cisco Systems o un distribuidor o socio autorizado de Cisco). Para ello, puede confirmar con el proveedor que este haya enviado la caja a través de la empresa de mensajería que la entregó y que el número de albarán del envío coincida con el utilizado en la entrega. Compruebe también que los números de serie de los artículos enviados coinciden con los números de serie de los artículos entregados. Esta comprobación debe realizarse mediante algún mecanismo que no haya participado en la entrega real del equipo, por ejemplo, por teléfono/fax u otro servicio de seguimiento en línea.

Una vez desembalado el producto, inspeccione la unidad. Compruebe que el número de serie que figura en la propia unidad coincida con el número de serie que aparece en la documentación de envío y en la factura. Si no es así, póngase en contacto con el proveedor del equipo (Cisco Systems o un distribuidor o socio autorizado de Cisco).

Métodos aprobados para obtener imágenes de software evaluadas según Common Criteria:

a) Descargar el archivo de imagen del software evaluado según los Criterios Comunes desde Cisco.com a un sistema informático de confianza.

b) Las imágenes de software están disponibles en [REF4].

c) El producto se suministra con las imágenes de software correctas instaladas; sin embargo, es posible que no se trate de la versión de evaluación.

Una vez descargado el archivo, compruebe que no haya sido alterado utilizando una herramienta SHA-512 para calcular el hash SHA-512 del archivo descargado y compararlo con el hash SHA-512 de la imagen que figura en la Tabla 1 a continuación. Si los hashes SHA-512 no coinciden, póngase en contacto con el Centro de Asistencia Técnica de Cisco [REF5].

Para verificar la firma digital antes de la instalación, el siguiente comando:

```
show software authenticity file
```

permite mostrar información relacionada con la autenticación del software, que incluye datos de credenciales de la imagen, el tipo de clave utilizada para la verificación, información de la firma y otros atributos del sobre de firma, para un archivo de imagen específico. El controlador de comandos extraerá el sobre de firma y sus campos del archivo de imagen y mostrará la información requerida. Para mostrar las claves públicas del software que se encuentran en el almacenamiento junto con los tipos de clave, utilice el siguiente comando en modo EXEC privilegiado:

```
show software authenticity keys
```

Tras verificar la firma digital con el comando con los anteriores comandos, se debe configurar una actualización y un reinicio en el router. El router no se iniciará si la firma digital no es válida, y aparecerá un error en la consola: *autoboot: error de arranque, reiniciando...*

Una vez encendido el router, compruebe que el producto carga la imagen correctamente, completa las autocomprobaciones internas y muestra la advertencia de exportación criptográfica en la consola.

Una vez que el producto se haya iniciado, el usuario final debe confirmar que efectivamente está ejecutando la versión evaluada. Utilice el comando

```
show version
```

para mostrar el nombre del archivo de la imagen del sistema que se está ejecutando actualmente y la versión de lanzamiento del software del sistema. También se recomienda verificar y activar el nivel de licencia. Se da por supuesto que el usuario final ha adquirido una licencia permanente válida durante toda la vida útil del sistema en el que está instalada.

En caso de que se opte por la versión virtualizada preinstalada, se deben seguir los siguientes pasos:

a) Lance la versión virtualizada en su hipervisor.

b) El producto mostrará automáticamente la verificación del hash al arrancar o al ejecutar el comando:

```
reload
```

c) El mensaje de verificación correcta del hash aparecerá una vez que se haya verificado con éxito la imagen de arranque. Si la imagen ha sido alterada de alguna manera, aparecerá un error y la imagen no se iniciará. Compruebe que el C8000V carga la

imagen correctamente, completa las autocomprobaciones internas y muestra la advertencia de exportación criptográfica en la consola.

d) Una vez que la imagen se haya cargado en la memoria de arranque para mostrar información relacionada con la autenticidad del software de un archivo de imagen específico, desde la interfaz de línea de comandos (CLI), inicie sesión en el dispositivo y utilice el comando:

```
verify
```

e) Una vez que el producto se haya iniciado, el usuario final debe confirmar que efectivamente está ejecutando la versión evaluada. Utilice el comando

```
show version
```

f) para mostrar el nombre del archivo de la imagen del sistema que se está ejecutando actualmente y la versión de lanzamiento del software del sistema.

En caso de que se opte por la versión virtualizada, se deben seguir los siguientes pasos:

a) Vaya a la página de descargas de software de Cisco [REF6].

b) Escriba *Catalyst 8000V Edge Software* en el campo *Seleccionar un producto* y, a continuación, haga clic en el icono de búsqueda.

c) Haga clic en el enlace *Catalyst 8000V Edge Software* y, a continuación, seleccione el enlace *IOS XE Software*.

d) Seleccionar la versión *Dublin-17.12.2a(ED)* correspondiente a la versión incluida en la configuración evaluada. Antes de proceder a la instalación, el administrador deberá verificar en el portal oficial del fabricante que dicha versión continúa disponible, soportada y no afectada por vulnerabilidades críticas conocidas.

e) Elija el tipo de software que desea descargar.

f) Una vez descargada la imagen del software, el administrador debe calcular la suma de comprobación SHA512 de la copia local descargada del software. Si la suma de comprobación coincide con el valor publicado por Cisco, significa que el software se ha descargado correctamente y se puede proceder a la instalación o actualización.

g) Si los valores de la suma de comprobación no coinciden, es posible que el administrador desee volver a descargar el software. Si los valores siguen sin coincidir, el administrador deberá investigar el motivo de la discrepancia. Esto puede implicar ponerse en contacto con el Centro de Asistencia Técnica (TAC) de Cisco si fuera necesario.

h) Las Tabla 2 muestra la versión evaluada del software y sus hashes correspondientes.

MODELOS	VERSIÓN SOFTWARE	NOMBRE DE IMAGEN	VALORES DE HASH
ASR1001-HX ASR1002-HX	IOS XE 17.12	asr1000- universalk9.17.12.02.SPA.bin	06064503d790c414e56a9e78d53d71d010d70d9c06c4842a9dc90005983255d54b534478c638fad276277b5506c94ea3cddcc45ea46a8e631efbc9996ed1cf24
ISR4461		isr4400v2- universalk9.17.12.02.SPA.bin	aea237a7d1084bb505b1f6ca27408860211453cde51d11220a14a27c39e13e27e16b9096030a313d901fa3f3c22875269698dd64b24003cbd547059dbeb67724
C8300-1N1S-6T C8300-2N2S-6T		c8000be- universalk9.17.12.02.SPA.bin	7d7df2eed8a312f8872b6a847451b2cf64d1571a867be13615a0256cf1363250dbcc19f215b1c5b5f1312df9e9d880f35053982922aa92e2a810d7fa26f0acab

C8500-12X		c8000aep-universalk9.17.12.02.SPA.bin	3f7709b031e62ded4a0ee3a2da929a7f157d3a2cf1b7733212148ccfba5921d5ff720bf9df1cb32b21fbbe8eb38aa8171032e25a928b902be7c0e547d7fcb27b
C8000V		c8000v- universalk9.17.12.02.SPA.bin c8000V- universalk9.17.12.02.ova	894c489470ec2c4ca373f1096093f12b8b215e15180e9d3be0ff4853d4a2b478d1cdf33ad1e715a58e32eacf0f9f32224a000c460a98a416d77c0ef7af3d502a 3be618adcce6d97ecfd23c0d2248ff835eb6636a53290a6ce357d9eaeb087ef86459cce3520471dc5c1a1b58e7ac148364c54b2bcf35e4ec463b43160e4288dd

Tabla 1 Imágenes Software

MODELOS	VERSIÓN SOFTWARE	NOMBRE DE IMAGEN	VALORES DE HASH
C8000V	IOS XE 17.12	C800V-universalk9.17.12.02.ova	3be618adcce6d97ecfd23c0d2248ff835eb6636a53290a6ce357d9eaeb087ef86459cce3520471dc5c1a1b58e7ac148364c54b2bcf35e4ec463b43160e4288dd
		C8000Vuniversalk9.17.12.02.iso	62805becf756e6e59d72e1fa51bcb5b0eb9e09b71524364dc823b5da0f813ce0ba3326e8fc5c0e6cd63ef135a54b83476ce3456182e5ddcb20c9331ce81c7178
		C8000Vuniversalk9.17.12.02.SPA.bin	894c489470ec2c4ca373f1096093f12b8b215e15180e9d3be0ff4853d4a2b478d1cdf33ad1e715a58e32eacf0f9f32224a000c460a98a416d77c0ef7af3d502a

Tabla 2 Imágenes Software Virtual

Compruebe que los controladores preinstalados no hayan sido manipulados mediante las siguientes acciones:

a) Identifica la versión de software de cada dispositivo. Hay tres formas de identificar la versión de software.

   i. Introduce las credenciales necesarias para iniciar sesión en la interfaz de línea de comandos (CLI) de cada controlador, y, a continuación, escribe:

```
show version
```

ii. Establezca una sesión SSH remota con la interfaz de línea de comandos (CLI) de cada controlador, introduzca las credenciales necesarias para iniciar sesión en la CLI y, a continuación, escriba:

```
show version
```

iii. Establezca una sesión HTTPS remota con vManage e introduzca las credenciales correspondientes. Una vez que haya iniciado sesión correctamente, haga clic en el menú situado en la esquina superior izquierda, luego en `Mantenimiento` y, a continuación, en `Actualización de software`. En esa pantalla, seleccione `Controller`, que mostrará la versión actual del software en vSmart y vBond, o seleccione `vManage`, que mostrará la versión actual del software en vManage.

Compruebe que los controladores no hayan sido manipulados mediante las siguientes acciones:

a) Vaya a la página de descargas de software de Cisco [REF6].

b) Escriba *SD-WAN* en el campo *Seleccionar un producto* y, a continuación, haga clic en el icono de búsqueda.

c) Para descargar el software para una instalación nueva de una máquina virtual del controlador, hacer clic en el enlace *SD-WAN* y, a continuación, selecciona el enlace *vManage Software*, *vSmart Software* o *vEDGE Cloud*.

d) Seleccionar la versión 20.12.2(ED).

e) La Tabla 3 muestra la versión evaluada del software y sus hashes correspondientes.

MODELOS	VERSIÓN SOFTWARE	NOMBRE DE IMAGEN	VALORES DE HASH
vManage	SD-WAN 20.12	viptela-vmanage-20.12.2-genericx86 64.ova	ed9b10c3f077264edb 3915359fc69e56c707a 7f1d961cd8e2b3d57c 0d55de5f074e37a27c 45d923eaebdb0489f3 8b73e46fe21f48bad2d d7ef3bc400fca7c4e6
		vmanage-20.12.2- x86_64.tar.gz	f62edf184cf685570eb bf69e89b5c34843f6e3 327738957f4bde9a80 8fd7200f892146189cc 1f9d113605296d735a aa7fb4cae8f76ed34b6 34cd0220b856de03
vBond		viptela-edge-20.12.2-genericx86-64.ova	b4267f4767626b927e 41b61ccd39d4846f58 2c795ec20eb20bb0de 98c3014c7dad5f9fe38 9ba863ed5c3e1473f5 1ce26bc2beee88299cf c33d 9fc4fbd4d84428
		viptela-20.12.2-x86_64.tar.gz	b56c35cfac386142775 c0bb37f96caf9a9f54e 8dd6a0cb19415dd829 8515e2a825f2ae6a97f 5efc0eccd296e273570 9d90ab82a59924f793 693c83a790335f8f
vSmart		viptela-smart-20.12.2-genericx86-64.ova	4e161e5ac54c9921b3 25b381e229aa6c6462 df37968efb3c280fec8 11968296b699a1ade0 264cfa55e080bedcea0 77338c61919fb7b6e5 98ae c2686a63669106
		viptela-20.12.2-x86_64.tar.gz	b56c35cfac386142775 c0bb37f96caf9a9f54e 8dd6a0cb19415dd829 8515e2a825f2ae6a97f 5efc0eccd296e273570 9d90ab82a59924f793 693c83a790335f8f

Tabla 3 Imágenes Software Controladores

4.2 ENTORNO DE INSTALACIÓN SEGURO

Los componentes del producto deberán instalarse en un entorno seguro. Los controladores SD-WAN y los routers cEdge virtuales deberán desplegarse sobre una plataforma de virtualización segura y soportada. Los routers cEdge físicos deberán instalarse en ubicaciones con control de acceso físico, alimentación protegida, puesta a tierra adecuada y conexión únicamente a redes autorizadas, verificando previamente su integridad física y correspondencia con la documentación de entrega.

4.3 CONSIDERACIONES PREVIAS

No se contemplan consideraciones adicionales para la instalación y uso de este producto.

4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN

Para funcionar en la configuración evaluada, el producto requiere los componentes operativos que se enumeran en la siguiente tabla:

Componente	Uso
Cliente SSH	Utilizado por el administrador del producto para facilitar la administración del mismo a través de canales protegidos por SSH. Se puede utilizar cualquier cliente SSH que sea compatible con SSHv2.
Navegador Web	Utilizado por el administrador para gestionar el producto a través de HTTPS.
Consola Local	Utilizada por el administrador para realizar conexiones locales y gestionar el producto.
Servidor Syslog	Cualquier servidor syslog al que el producto envía los registros de auditoría.
VMWare ESXi 8.0	Hipervisor requerido para todas las máquinas virtuales.

Tabla 4 Componentes del entorno de operación

5 FASE DE INSTALACIÓN

En esta sección se describen las recomendaciones y pasos necesarios para instalar de forma segura los componentes que forman parte de la configuración evaluada de Cisco cEdge Routers con IOS XE 17.12 y SD-WAN 20.12.

La instalación debe realizarse exclusivamente por administradores autorizados, en un entorno controlado, utilizando imágenes obtenidas desde fuentes oficiales de Cisco y verificadas mediante los hashes publicados o incluidos en este Procedimiento de Empleo Seguro.

La instalación descrita aplica a los siguientes componentes del producto:

a) Controladores SD-WAN virtualizados:
   i. vManage.
   ii. vSmart.
   iii. vBond.
b) Routers cEdge físicos:
   i. ASR1001-HX, ASR1002-HX
   ii. ISR4461
   iii. C8300-1N1S-6T, C8300-2N2S-6T
   iv. C8500-12X
c) Router cEdge virtual:
   i. C8000V (Virtual Machine)

5.1 INSTALACIÓN DEL SERVIDOR UCS Y DEL HIPERVISOR ESXI

Los componentes virtuales del producto deben desplegarse sobre un entorno de virtualización seguro. La configuración evaluada contempla el uso de VMware ESXi 8.0 sobre servidores Cisco UCS C220/C240 M5.

La instalación física del servidor UCS debe realizarse siguiendo la documentación oficial de Cisco aplicable al modelo concreto. Como mínimo, el administrador autorizado debe:

a) Instalar el servidor en un rack ubicado en una sala con control de acceso físico.

b) Conectar el servidor a una toma eléctrica protegida y con puesta a tierra adecuada.

c) Conectar el puerto de gestión del servidor a la red de gestión definida por la organización.

d) Configurar el acceso de administración del servidor mediante Cisco Integrated Management Controller (CIMC).

e) Asignar direccionamiento IP estático o DHCP autorizado para la gestión del servidor.

f) Verificar que el firmware, BIOS y componentes de gestión del servidor están en versiones soportadas.

g) Documentar el número de serie, ubicación física y responsable del activo.

La instalación o actualización de VMware ESXi 8.0 debe realizarse conforme a la documentación oficial de VMware. El administrador debe verificar la versión instalada mediante la consola del hipervisor o mediante las interfaces de administración disponibles.

Las máquinas virtuales sobre las que corre el producto deben ser desplegadas sobre ESXi 8.0.

Para más información consultar la sección “3 Secure Installation and Configuration” de [REF2].

5.2 INSTALACIÓN DE CONTROLADORES SD-WAN VIRTUALES

Los controladores vManage, vSmart y vBond deben desplegarse como máquinas virtuales a partir de las imágenes OVA correspondientes a la versión evaluada.

Desde ESXi seguir los siguientes pasos:

a) Seleccionar “Create/Register VM”.

b) Seleccionar “Deploy a virtual machine from an OVF or OVA file”.

c) Introducir un nombre identificativo para la máquina virtual.

d) Seleccionar el fichero OVA correspondiente al controlador.

e) Seleccionar el datastore donde se almacenará la máquina virtual.

f) Asociar el adaptador de red inicial a la red de gestión.

g) Seleccionar aprovisionamiento de disco conforme a la política de la organización, preferiblemente “Thick Provisioning”.

h) Desmarcar el arranque automático inicial hasta revisar la configuración.

i) Finalizar el despliegue pulsando “Finish” para registrar la VM vManage.

j) Una vez completada la instalación de la máquina virtual, acceda a «Virtual Machines», y hacer clic con el botón derecho del ratón en la máquina virtual vManage y seleccionar “Edit settings”.

k) Asegurarse de que el adaptador de red 1 esté configurado para la red de gestión.

l) Hacer click en “Add Network Adapter” y seleccionar la red SD-WAN definida para el adaptador de red 2.

m) Actualizar el tamaño del disco duro 1 a 30 GB.

n) [Solo para vManage] Hacer click en “Add Hard Disk” y seleccionar “New Standard Hard Disk”; añadir el disco duro 2 y establecer el tamaño en 100 GB, de modo que vManage disponga de espacio suficiente para almacenar todos los registros del controlador.

o) Hacer click en “Save”.

p) Repetir los pasos anteriores para el vSmart y vBond.

Para más información consultar [REF3].

5.3 INSTALACIÓN FÍSICA DEL HARDWARE (ROUTERS CEDGE FÍSICOS)

Las siguientes instrucciones ofrecen una descripción general del proceso de instalación de un router cEdge basado en hardware, ya que se da por supuesto que el administrador autorizado está familiarizado con la instalación de hardware de red.

También se da por supuesto que ya se ha inspeccionado el chasis del hardware para detectar posibles manipulaciones o daños.

a) Si procede, instalar todos los NIMs antes de montar el dispositivo en el rack y conectarlo a la alimentación.

b) Fijar los soportes de montaje en rack adecuados al dispositivo y, a continuación, instalarlos en el rack.

c) Conectar el chasis a una toma de tierra fiable; el cable de tierra debe instalarse de acuerdo con las normas locales de seguridad eléctrica.

d) Conectar los cables de red a los puertos deseados para permitir el tráfico de gestión y SD-WAN.

e) Los routers ISR 4461, ASR 1001HX y ASR 1002HX disponen de puertos fuera de banda dedicados a la gestión de dispositivos. Internamente, estos se designan como interfaz Gigabit0. Los modelos Cat 8300 y 855 no disponen de una interfaz de gestión fuera de banda, por lo que la gestión utiliza una de las cuatro interfaces en banda denominadas Gigabit 0/0/0 a 0/0/3. Los VRF configurados en los routers de la serie Cat pueden utilizarse para reservar una interfaz exclusivamente para la gestión, de forma similar a la interfaz de gestión dedicada de los routers de las series ISR y ASR.

f) Finalmente, conectar los cables de alimentación al dispositivo.

5.4 INSTALACIÓN DEL SOFTWARE (ENRUTADORES CEDGE VIRTUALES)

Antes de instalar las máquinas virtuales, se da por hecho que el administrador autorizado ha descargado los archivos OVA correctos.

Las máquinas virtuales C8000v cEdge deben cumplir las especificaciones mínimas.

Además, debe haber al menos dos redes virtuales y conmutadores independientes en ESXi. Uno para la gestión de máquinas virtuales y otro para SD-WAN.

a) En ESXi, seleccione “Create/Register VM”.

b) En vManage, hacer click en “Deploy a virtual machine from an OVF or an OVA file”.

c) Introducir un nombre para la instancia del router Cat8000v cEdge y seleccione el archivo descargado del router Cat8000v cEdge.

d) Seleccionar el datastore donde se va a almacenar la máquina virtual.

e) Seleccionar la red de gestión de la máquina virtual para una de las tarjetas de red y seleccione “Thick Provisioning” en “Data Provisioning”. Desmarcar “Power on Automatically”.

f) Hacer clic en “Finish” para registrar la máquina virtual de vManage.

g) Una vez completada la instalación de la máquina virtual, ir a “Virtual Machines”, hacer clic con el botón derecho del ratón en la máquina virtual vManage y seleccionar "Edit Settings”.

h) Establecer el número de CPU de la máquina virtual en 4.

i) Añadir un cuarto adaptador de red. Configúralo para que utilice el conmutador de gestión y el grupo de puertos.

j) Finalmente, hacer click en “Save”.

6 FASE DE CONFIGURACIÓN

6.1 CONFIGURACIÓN CONTROLADORES SD-WAN

En esta sección se describen los pasos necesarios para configurar los controladores vManage, vSmart y vBond.

6.1.1 CONFIGURACIÓN DE LA INFORMACIÓN DEL SISTEMA DEL CONTROLADOR

Los pasos que se indican a continuación son similares para cada uno de los tres controladores, salvo que se indique lo contrario.

a) Comenzar la configuración con el dispositivo vManage.

b) Encender la máquina virtual.

c) Iniciar la consola local remota de ESXi.

d) Introducir los comandos que se indican a continuación en la CLI utilizando los parámetros adecuados para el dispositivo en cuestión (vManage, vSmart, vBond):

```
vmanage# config t
Entering configuration mode terminal
vmanage(config)# system
vmanage(config-system)# host-name vManage-1
vManage-1(config-system)# system-ip 10.255.255.10
vManage-1(config-system)# organization-name CC CLUS 2023
vManage-1(config-system)# site-id 1
vManage-1(config-system)# vbond 10.122.83.212
vManage-1(config-system)# commit
Commit complete.
```

e) Tener en cuenta que al configurar vBond, el comando «vbond» será: vBond-1(config-system)# vbond 10.122.83.212 local vbond.

f) Repetir los pasos anteriores para los dos controladores restantes.

6.1.2 CONFIGURACIÓN DE LA VPN DE GESTIÓN DEL CONTROLADOR

Los pasos que se indican a continuación son similares para cada uno de los tres controladores, salvo que se indique lo contrario

a) Comenzar la configuración con el dispositivo vManage.

b) Encender la máquina virtual.

c) Iniciar la consola local remota de ESXi.

d) Introducir los comandos que se indican a continuación en la CLI utilizando los parámetros adecuados para el dispositivo en cuestión (vManage, vSmart, vBond):

```
vManage-1#
vManage-1# config t
Entering configuration mode terminal
vManage-1(config)# vpn 512
vManage-1(config-vpn-512)# interface eth1
vManage-1(config-interface-eth1)# ip address 172.18.155.5/24
```

```
vManage-1(config-interface-eth1)# no shut
vManage-1(config-interface-eth1)# commit
Commit complete.
vManage-1(config-interface-eth1)# exit
vManage-1(config-vpn-512)# ip route 0.0.0.0/0 172.18.155.1
vManage-1(config-vpn-512)# commit
Commit complete.
```

e) Tener en cuenta que al configurar vBond, configure la interfaz 0 como interfaz de gestión mediante el comando: vBond-1(config-vpn-512)# interface eth 0.

f) Repetir los pasos anteriores para los dos controladores restantes.

6.1.3 CONFIGURACIÓN DE LA VPN DE TRANSPORTE DEL CONTROLADOR

Los pasos que se indican a continuación son similares para cada uno de los tres controladores, salvo que se indique lo contrario

a) Comenzar la configuración con el dispositivo vManage.

b) Encender la máquina virtual.

c) Iniciar la consola local remota de ESXi.

d) Introducir los comandos que se indican a continuación en la CLI utilizando los parámetros adecuados para el dispositivo en cuestión (vManage, vSmart, vBond):

```
vManage-1#
vManage-1# config t
Entering configuration mode terminal
vManage-1(config)# vpn 0
vManage-1(config-vpn-0)# interface eth0
vManage-1(config-interface-eth0)# ip address 10.122.83.211/24
vManage-1(config-interface-eth0)# no shut
vManage-1(config-interface-eth0)# tunnel-interface
vManage-1(config-tunnel-interface)# allow-service dhcp
vManage-1(config-tunnel-interface)# allow-service dns
vManage-1(config-tunnel-interface)# allow-service icmp
vManage-1(config-tunnel-interface)# allow-service https
vManage-1(config-tunnel-interface)# no allow-service sshd
vManage-1(config-tunnel-interface)# no allow-service netconf
vManage-1(config-tunnel-interface)# no allow-service ntp
vManage-1(config-tunnel-interface)# no allow-service stun
vManage-1(config-tunnel-interface)# commit
Commit complete.
vManage-1(config-tunnel-interface)# exit
vManage-1(config-interface-eth0)# exit
vManage-1(config-vpn-0)# ip route 0.0.0.0/0 10.122.83.1
vManage-1(config-vpn-0)# commit
Commit complete.
```

e) Tener en cuenta que al configurar vBond, configura la interfaz 0 como interfaz de gestión mediante el siguiente comando: vBond-1(config-vpn-0)# interface ge0/0.

f) Repetir los pasos anteriores para los dos controladores restantes.

6.1.4 CONFIGURACIÓN DEL CONTROLADOR PARA CERTIFICADOS EMPRESARIALES

En esta sección se describen los pasos necesarios para configurar los controladores vManage, vSmart y vBond.

De forma predeterminada, el producto está configurado para utilizar certificados autofirmados. Los pasos que se indican a continuación permitirán el uso de certificados firmados por una autoridad de certificación (CA).

a) Iniciar sesión en la consola web de vManage accediendo a «https://<dirección IP pública de vManage>:8443» en un navegador web.

b) Utilizar el menú de la esquina superior izquierda y acceda a “Administration” y, a continuación, en “Settings”. Desplazarse hacia abajo hasta los parámetros de “Controller Certificate Authorization” y “WAN Edge Cloud Certificate Authorization”.

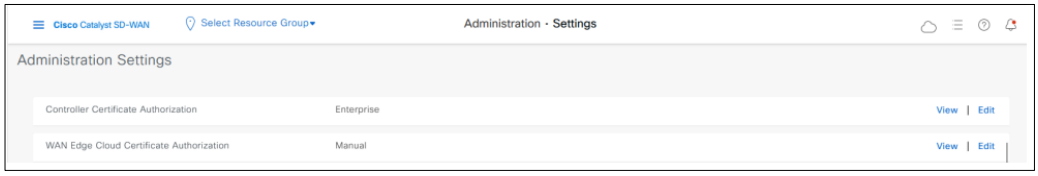


Figura 1: Menú de configuración de administración

c) Seleccionar “Edit” en “Controller Certificate Authorization” y marcar la casilla “Enterprise Root Certificate”; subir la CA mediante el enlace “Select a file link”; marca la casilla “Set CSR Properties” e introducir los valores que se utilizarán al generar las CSR.

d) Al cargar la cadena de confianza, cada certificado debe ir precedido de “-----BEGIN CERTIFICATE-----“y seguido de “-----END CERTIFICATE-----“.

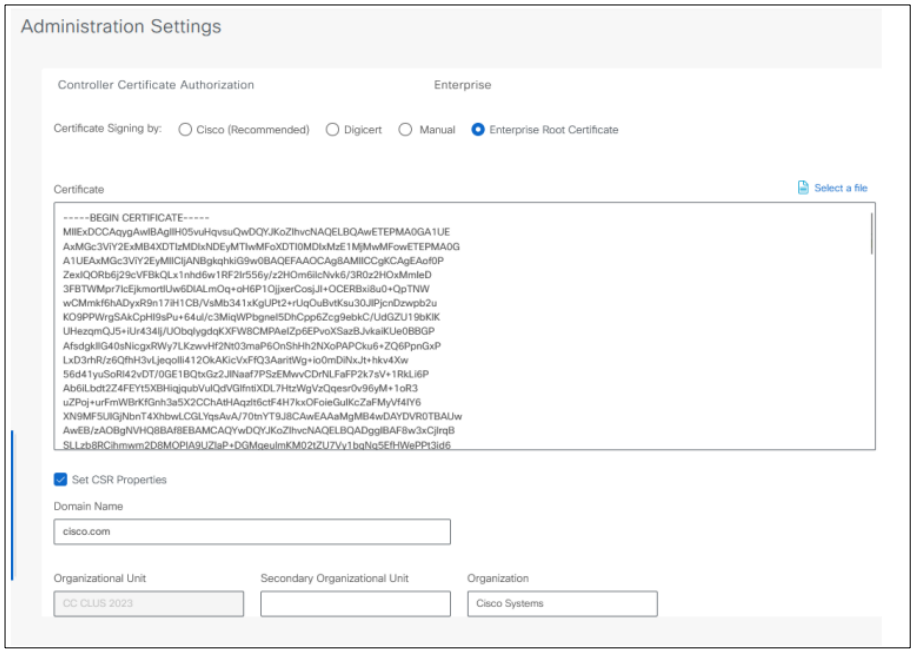


Figura 2: Configuración de autorización de certificados del controlador

e) La cadena de confianza debe aparecer de tal forma que el certificado raíz se encuentre al final del archivo. Asegurarse de que no haya ningún carácter adicional entre los certificados.

f) Tener en cuenta que al rellenar los datos en las propiedades de la CSR, el campo "Unidad organizativa" debe coincidir con el nombre de la organización del dispositivo. Sin embargo, el campo "Organización" puede contener cualquier valor.

g) Seleccionar "Import & Save" al finalizar.

h) Seleccionar "Editar" en "WAN Edge Cloud Certificate Authorization", marcar la opción "Manual (Enterprise CA – Recommended)" y seleccionar "Save" para guardar la configuración.



Figura 3: Configuración de autorización de certificados en la nube perimetral de la WAN

i) Utilizar el menú de la esquina superior izquierda e ir a "Configuration" luego a "Certificados" y, a continuación, seleccionar "Controllers".

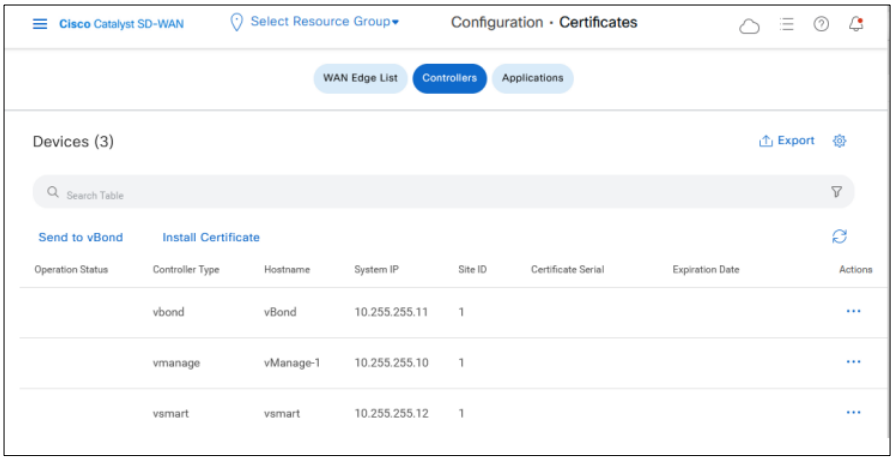


Figura 4: Página de gestión de certificados del controlador

j) En la parte derecha, en "Actions", seleccionar el icono "…" y, a continuación, selecciona "Generate CSR for vManage" y aparecerá una ventana emergente con la solicitud de firma de certificado. Descarga o copia la solicitud de firma de certificado para enviarla a firmar. Repite este proceso para vSmart y vBond.

k) Envíar las CSR a la CA para que firme las solicitudes.

l) Una vez firmadas, vuelve a vManage y ve a "Configuration", luego a "Certificates" y, a continuación, selecciona "Controllers". Esta vez, selecciona el enlace "Install Certificate". No es necesario seleccionar ningún controlador específico. vManage aplica los certificados al controlador adecuado.

m) Finalmente, en la ventana emergente que aparece, utiliza “Select a file” para buscar el certificado firmado de vManage. Una vez cargado, hacer clic en “Install”.

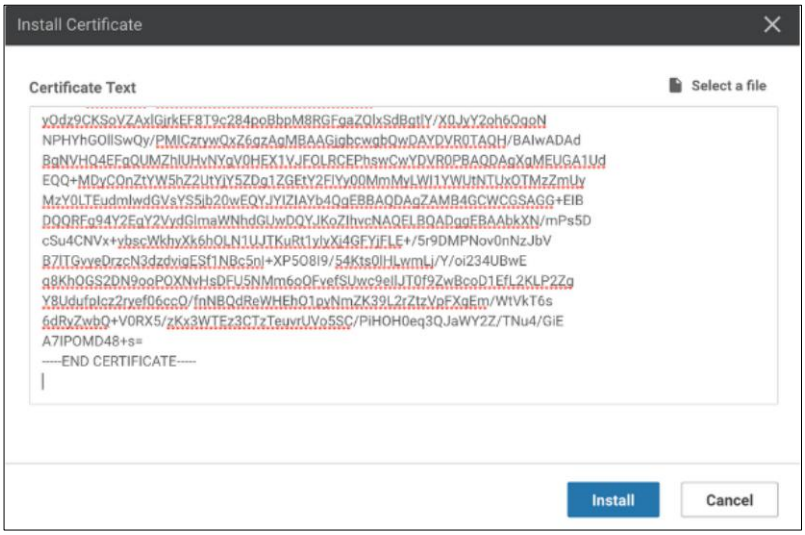


Figura 5: Instalación del certificado del controlador

n) Repetir los mismos pasos para vSmart y vBond.

o) Una vez instalados, los certificados deberían aparecer en la página “Certificate Management Page”.

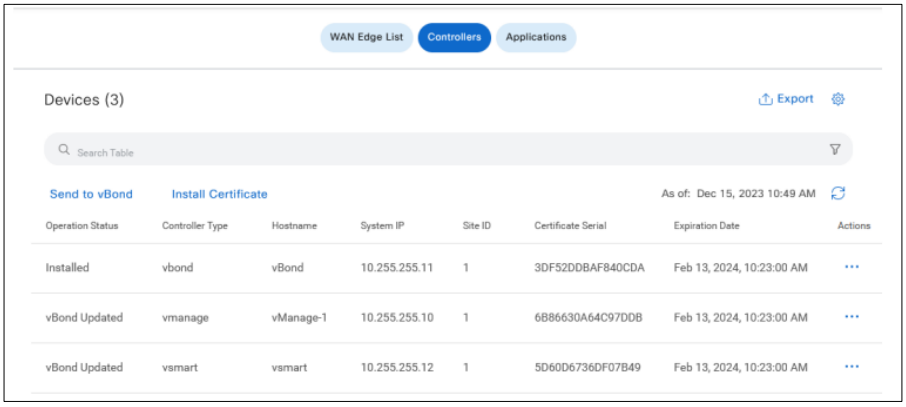


Figura 6: Certificados del controlador

Adicionalmente se puede comprobar la instalación del certificado en cada controlador introduciendo el comando desde la CLI con:

```
show certificate root-ca-cert | include Subject:
```

También se puede comprobar el despliegue de los controladores con el comando:

```
show control connections
```

6.2 CONFIGURACIÓN ROUTER CEDGE

6.2.1 CARGAR EL ARCHIVO SERIE DE CEDGE EN VMANAGE

Para que los dispositivos WAN Edge se pongan en marcha y estén activos en la red superpuesta, es necesario haber cargado en vManage un archivo de números de serie autorizados válido.

Este archivo de números de serie autorizados recoge los números de serie y de chasis de todos los routers WAN Edge permitidos en la red. vManage envía este archivo a los controladores, y solo los dispositivos cuyos números de serie coincidan con los de esta lista serán validados y autenticados correctamente por los controladores.

a) Acceder a Cisco Software Central a través del enlace [REF6].

b) A continuación, desplázate hacia abajo hasta la sección “Smart Licensing” y buscar “Network Plug and Play”.

c) En “Network Plug and Play” seleccionar “Manage Devices” para acceder a “Plug and Play Connect”.



Figura 7: Plug and Play Connect web

d) Si ya hay dispositivos cargados, pasar al paso correspondiente. De lo contrario, para añadir un dispositivo físico, selecciona “+ Add Device

e) En la siguiente pantalla, selecciona la pestaña “+ Identify Device”.

f) En la ventana que aparece, introduce el número de serie y el PID (identificador de producto) del dispositivo. Estos datos se pueden encontrar en la carcasa física del dispositivo o, desde la consola, utilizando el comando “show license udi” desde la CLI.

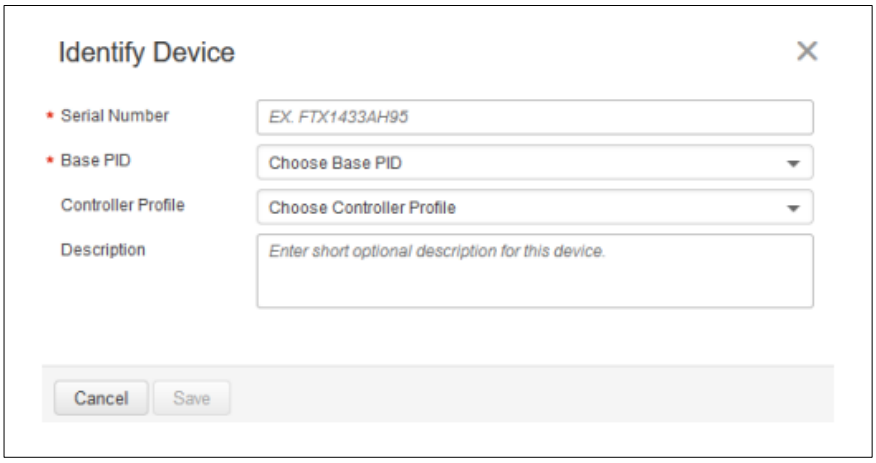


Figura 8: Ventana de Plug and Play (PnP) donde introducir los detalles

g) Una vez introducidos un número de serie y un PID válidos, aparecerán menús desplegables adicionales. Introduce el número de serie del certificado del dispositivo. El menú desplegable “Controller Profile” contendrá los controladores válidos para la cuenta. En ese momento, selecciona el controlador correcto, configura el “Device Mode” en “Controller”, marca la casilla “SD-WAN Capable” y, a continuación, seleccionar “Save” y luego “Next”.

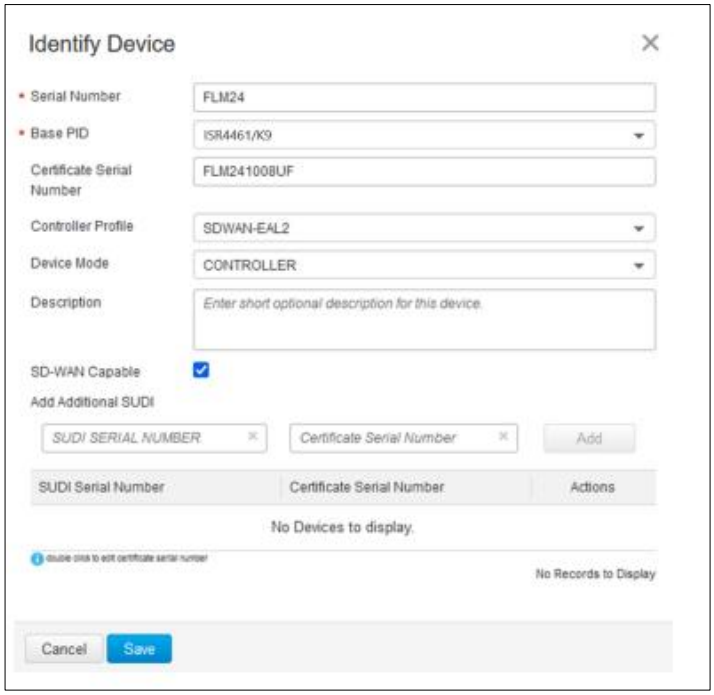


Figura 9: Ventana de Plug and Play (PnP) con los detalles completados

h) El dispositivo aparecerá ahora en la sección "Review & Submit". Hacer clic en "Submit" y, a continuación, en "Done", y el dispositivo se añadirá.

i) Si el dispositivo que se va a añadir es un dispositivo cEdge virtual Cat8000V, en la pestaña "Plug and Play Connect Devices" seleccionar "+ Add Software Devices" y, en la página siguiente, vuelve a hacer clic en "+ Add Software Devices".

j) El comando "show license udi" también funciona en routers virtuales. Rellenar los datos de la ventana emergente "Identity Device" y, a continuación, seleccionar "Save" y luego "Next".

k) El dispositivo aparecerá ahora en la sección "Review & Submit". Hacer clic en "Submit" y, a continuación, en "Done", y el dispositivo se añadirá.

l) Los dispositivos añadidos aparecerán en la página de resumen.

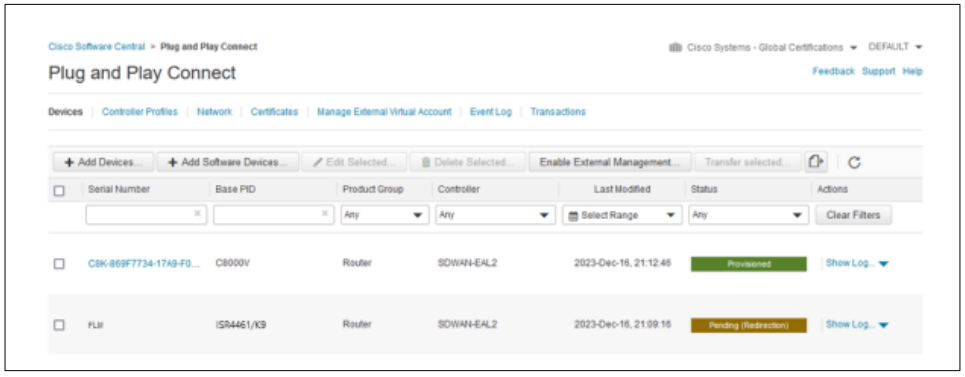


Figura 10: Ventana de Plug and Play (PnP) con dispositivos añadidos

m) Una vez añadido, seleccionar la pestaña "Controller Profiles".

n) En la pestaña “Controller Profiles”, buscar el controlador deseado y seleccionar el enlace “Provisioning file” asociado a dicho controlador.

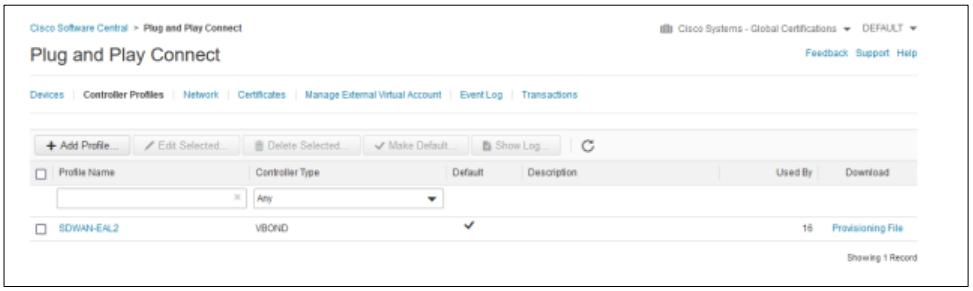


Figura 11: Ventana de Plug and Play (PnP) con dispositivos añadidos

o) En la ventana emergente que aparece, seleccionar en el menú desplegable “Controller Versions“ la opción “18.3 and newer” y hacer clic en “Download”. Se descargará un archivo llamado *serialFile.viptela*.

p) Iniciar sesión en la interfaz gráfica de usuario de vManage y ve a “Configuration”, luego a “Device” y, a continuación, a “WAN Edge List”. Desde ahí, selecciona el enlace “Upload WAN Edge List”.

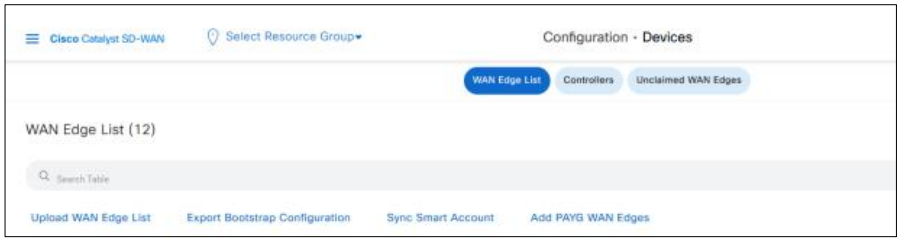


Figura 12: Lista vManage WAN Edge

q) En la ventana emergente que aparece, seleccionar el archivo *serialFile.viptela*, selecciona “Yes” en “Send to Controller” y, a continuación, hacer clic en “Upload”.



Figura 13: Subida de archivos de números de serie en vManage

r) Se mostrarán los controladores indicando el estado de la implementación. Una vez finalizada, el estado será de “Success”. En este momento, vuelve a la lista de WAN Edge para confirmar que se han añadido los dispositivos.

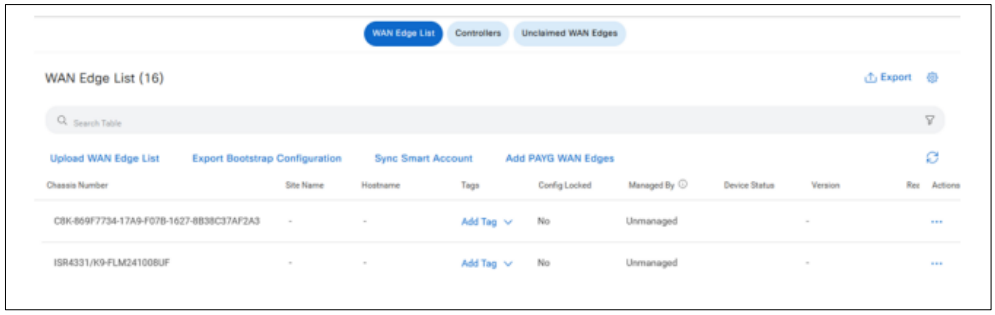


Figura 14: Subida de archivos de números de serie en vManage

6.3 MODO DE OPERACIÓN SEGURO

El administrador debe configurar los routers cEdge para que funcionen en modo FIPS. Esta configuración solo se aplica a los routers cEdge, ya que los controladores SD-WAN ya están en modo FIPS de forma predeterminada.

a) Se deberá comenzar con la configuración de la plantilla de funciones seleccionando "Cisco CLI Add-On Template".

> **NOTA**: Hay que tener en cuenta que la configuración del modo FIPS impedirá realizar más cambios de configuración a través de las plantillas de dispositivo. Al configurar el modo FIPS, aplica primero toda la configuración excepto el modo FIPS. A continuación, modificar la plantilla de complemento de CLI existente (si procede) o crear una plantilla de complemento de CLI independiente (si aún no existe ninguna) con el comando que figura a continuación, actualizar o aplicar la plantilla de complemento de CLI a la plantilla de dispositivo y, a continuación, asociar un dispositivo a la plantilla de dispositivo.

b) Introducir un nombre y una descripción para la plantilla; por ejemplo, "C8Kv-01-CLI-AddOn" (para ambos).

c) Posteriormente introducir el siguiente comando de texto en la ventana de texto:

```
platform ipsec fips-mode
```

d) Hacer clic en "Update" para guardar la plantilla del dispositivo.

e) Luego hacer clic en "Next" y espera a que aparezca la plantilla del dispositivo.

f) Seleccionar el dispositivo en la columna de la izquierda y hacer clic en "Configure Devices".

g) Comprobar que la plantilla se ha aplicado correctamente.

h) Luego ir al menú de la izquierda, selecciona "Maintenance" y, a continuación, "Device Reboot"

i) Seleccionar todos los dispositivos que hayan recibido las plantillas y hacer clic en "Reboot".

j) Finalmente confirmar en los routers cEdge que se ha activado el modo FIPS con el siguiente comando:

```
C8kV-1# show sdwan security-info
```

Deberá aparecer un mensaje de “security-info fips-mode Enabled”.

6.4 AUTENTICACIÓN

La configuración de identificación y autenticación está restringida a administradores privilegiados.

En la configuración evaluada, el producto utiliza autenticación local para los administradores. Aunque el producto puede soportar autenticación externa, por ejemplo, RADIUS, esta debe analizarse específicamente si se desea utilizar, ya que podría quedar fuera de la configuración evaluada.

Al utilizar la autenticación local, se debe configurar la funcionalidad AAA para la gestión local de los usuarios con los siguientes comandos:

```
Router(config)# aaa new-model
Router(config)# aaa authentication login default local
Router(config)# aaa authorization exec default local
```

Para más información de la configuración de AAA se puede consultar la guía [REF7].

6.4.1 AUTENTICACIÓN LOCAL EN CONTROLADORES POR CLI

Para configurar un controlador para que admita únicamente la autenticación local desde la CLI, introducir los siguientes comandos en la CLI:

```
vsmart# config t
vsmart(config)# system
vsmart(config-system)# aaa
vsmart(config-aaa)# auth-order local
vsmart(config-aaa)# commit
Commit complete
```

Para verificar que verificar que se ha hecho correctamente usar el siguiente comando en la CLI:

```
show run
```

Es posible también modificar la autenticación local en controladores mediante plantilla. Para más información consultar la sección “4.3.1.2 Controller Local Authentication Configuration via Template” de [REF2].

6.4.2 AUTENTICACIÓN LOCAL EN CEDGE POR CLI

Para configurar un router cEdge para que solo admita la autenticación local desde la CLI, introducir los siguientes comandos en la CLI:

```
C8kV-1# config-t
C8kV-1(config)# aaa authentication login default local
C8kV-1(config)# aaa authorization exec default local
C8kV-1(config)# commit
```

Para verificar que verificar que se ha hecho correctamente usar el siguiente comando en la CLI:

```
show run
```

Es posible también modificar la autenticación local en los routers cEdge mediante plantilla. Para más información consultar la sección "cEdge Local Authentication Configuration via Template" de [REF2].

6.4.3 BLOQUEO POR INTENTOS FALLIDOS

El producto permite configurar mecanismos de bloqueo por intentos fallidos de autenticación. Se deberá configurar un número máximo de intentos fallidos de 3 y un tiempo de bloqueo de 5 minutos.

> **NOTA**: Los usuarios con privilege level 15 pueden no quedar bloqueados por esta funcionalidad. Por ello, el número de cuentas con privilege level 15 debe mantenerse al mínimo imprescindible.

Los controladores son gestionados mediante plantillas, para configurar el tiempo de sesión GUI de vManage consultar la sección "vManage GUI Session Management" de [REF2]. Para configurar el tiempo de sesión de la CLI del controlador y del cEdge consultar la sección "Controller and cEdge GUI Session Timeout" [REF2].

6.4.4 BLOQUEO EN CONTROLADORES

Para configurar el bloqueo de la sesión SSH del controlador introducir los siguientes comandos desde la CLI (el siguiente es un ejemplo para vSmart):

```
vsmart# config t
vsmart(config)# system
vsmart(config-system)# aaa
vsmart(config-aaa)# lockout-policy
vsmart(config-lockout-policy)# fail-attempts 3
vsmart(config-lockout-policy)# fail-interval 300
vsmart(config-lockout-policy)# lockout-interval 300
vsmart(config-lockout-policy)# commit
```

6.4.5 BLOQUEO EN CEDGE

En routers cEdge se puede usar una plantilla Cisco CLI Add-On. Para más información consultar la sección "4.4.4 cEdge SSH Session Lockout" de [REF2].

6.5 ADMINISTRACIÓN DEL PRODUCTO

6.5.1 ADMINISTRACIÓN LOCAL Y REMOTA

La administración del producto debe realizarse únicamente por administradores autorizados y mediante canales protegidos. En la configuración evaluada, la administración remota del producto se realiza a través de:

a. HTTPS/TLS para el acceso a la interfaz gráfica de vManage.

b. SSHv2 para el acceso remoto a la CLI de los controladores y routers cEdge.

c. Consola local física para routers físicos, limitada a instalación inicial, mantenimiento o recuperación.

d. Consola remota local de ESXi para máquinas virtuales, limitada a instalación inicial, mantenimiento o recuperación.

Todas las comunicaciones administrativas remotas deben realizarse mediante una ruta de confianza, utilizando SSHv2 o HTTPS con TLSv1.2/TLSv1.3. No debe permitirse el uso de protocolos inseguros para la administración.

No deben utilizarse protocolos inseguros para administración:

a. Telnet debe permanecer deshabilitado.

b. HTTP no debe usarse; debe utilizarse HTTPS.

c. SSHv1 no debe usarse; debe utilizarse SSHv2.

d. FTP no debe usarse para transferencias sensibles; deben utilizarse SCP o SFTP.

e. TLS inferior a 1.2 no debe utilizarse.

Para limitar acceso VTY a tan solo SSH en los routers cEdge usar los siguientes comandos desde la CLI:

```
router# config-t
router(config)# line vty 0 4
router(config-line)# transport input ssh
router(config-line)# commit
```

También cuando el servicio HTTP esté disponible, debe deshabilitarse y mantenerse únicamente HTTPS si fuera necesario para funciones administrativas soportadas:

```
router# config-t
router(config)# no ip http server
router(config)# ip http secure-server
router(config)# commit
```

La administración CLI remota debe realizarse exclusivamente mediante SSHv2 con los siguientes mecanismos criptográficos:

Función criptográfica	Algoritmos recomendados
Cifrado	AES-128-GCM, AES-256-GCM, AES-128-CTR, AES-192-CTR, AES-256-CTR
Integridad/MAC	HMAC-SHA2-256, HMAC-SHA2-512
Intercambio de claves	ECDH P-256/P-384/P-521, DH grupo 16 cuando esté disponible
Clave de host	RSA SHA-2 con clave ≥ 3072 bits o ECDSA P-256 o superior si está soportado

Tabla 5 Mecanismos criptográficos autorizados para SSH

Cuando la versión evaluada lo soporte, el administrador podrá restringir los algoritmos SSH mediante CLI o mediante una plantilla Cisco CLI Add-On en vManage.

```
router# config-t
router(config)# ip ssh version 2
router(config)#  ip  ssh  server  algorithm  encryption  aes256-
gcm@openssh.com aes128-gcm@openssh.com aes256-ctr aes192-ctr aes128-
ctr
```

```
router(config)# ip ssh server algorithm mac hmac-sha2-512-etm@openssh.com hmac-sha2-256-etm@openssh.com
router(config)# ip ssh server algorithm kex ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group16-sha512
router(config)# line vty 0 4
router(config-line)# transport input ssh
router(config-line)# commit
```

Cuando se utilicen claves RSA para SSH, deben ser de al menos 3072 bits. Si la plataforma lo permite, se recomienda 4096 bits.

```
router# config-t
router(config)# crypto key generate rsa general-keys modulus 3072
router(config)# ip ssh version 2
router(config)# commit
```

6.5.2 CONFIGURACIÓN DE ADMINISTRADORES

Las credenciales configuradas durante la instalación inicial se consideran credenciales de sistema y no deben utilizarse para la administración diaria.

Se deben crear cuentas nominativas e individuales para cada administrador autorizado. No deben compartirse cuentas administrativas.

En la configuración evaluada se encuentran los siguientes usuarios/roles administrativos:

Componente	Rol administrativo
Controladores SD-WAN (vManage, vSmart, vBond)	Grupo netadmin.
Routers cEdge	Privilege level 15.

Tabla 6 Roles de los diferentes componentes del producto

NOTA: Aunque los diferentes componentes del producto permiten asignar a los usuarios múltiples roles con distintos o limitados niveles de acceso, en la configuración evaluada de operación segura solo debe utilizarse el rol de Security Administrator. En el caso de los componentes del controlador, esto implica la asignación de rol “netadmin” al usuario. En el caso de los dispositivos cEdge, esto implica proporcionar acceso de “privilege level 15”.

Los siguientes apartados detallan la creación de usuarios administradores para los diferentes componentes.

6.5.2.1 CREACIÓN DE ADMINISTRADORES EN CONTROLADORES POR CLI

Las cuentas administrativas deberán ser nominativas, individuales y asignadas únicamente a administradores autorizados. No deberán utilizarse cuentas genéricas, compartidas o asociadas exclusivamente a roles funcionales, con el fin de garantizar la trazabilidad de las acciones de administración realizadas sobre el producto.

Para crear un usuario administrador en los controladores (por ejemplo, un usuario llamado “admin2”) mediante CLI usar los siguientes comandos:

```
vsmart# config t
```

```
vsmart(config)# system
vsmart(config-system)# aaa
vsmart(config-aaa)# user admin2 group netadmin
vsmart(config-user-admin2)# password <password>
vsmart(config-user-admin2)# commit
```

6.5.2.2 CREACIÓN DE ADMINISTRADORES EN CEDGE POR CLI

Para crear un usuario administrador en los router cEdge (por ejemplo, un usuario llamado "admin2") mediante CLI usar los siguientes comandos:

```
router# config-t
router(config)# username admin2 privilege 15 secret <password>
router(config)# commit
```

6.5.2.3 POLÍTICA DE CONTRASEÑAS

La política de contraseñas asociadas a cuentas administrativas deberá cumplir, como mínimo, los siguientes requisitos:

a. Longitud mínima: 12 caracteres.
b. Composición: mayúsculas, minúsculas, números y caracteres especiales.
c. Uso recomendado de los cuatro grupos de caracteres.
d. Uso mínimo de tres grupos cuando el producto o la política no permitan exigir los cuatro.
e. No reutilizar, al menos, las últimas cinco contraseñas.
f. Validez máxima aproximada: 60 días.
g. Periodo mínimo antes de nuevo cambio: 10 días.
h. No usar palabras de diccionario, nombres de producto, nombres de usuario o contraseñas triviales.
i. Revocar o deshabilitar credenciales que ya no sean necesarias.

Se podrá configurar desde la CLI con los siguientes comandos:

```
Controller(config)#system
Controller(config)#aaa
Controller(config)#password-policy min-password-length 12
Controller(config)#password-policy num-lower-case-characters 1
Controller(config)#password-policy num-numeric-characters 1
Controller(config)#password-policy num-special-characters 1
Controller(config)#password-policy num-upper-case-characters 1
Controller(config)#password-policy password-expiry-age 60
Controller(config)# username <user-admin> password <password>
```

Para más información consultar la sección "4.2 Passwords" de [REF2].

6.6 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

La arquitectura debe separar, al menos tres capas:

a. Red de gestión.

b. Red de transporte SD-WAN.

c. Red de servicio o LAN.

La siguiente tabla muestra un ejemplo de asignación de interfaces:

Red	ASR/ISR/Catalyst 8300/8500	C8000V
Transporte	GigabitEthernet0/0/1	GigabitEthernet1
No utilizada	GigabitEthernet0/0/2	GigabitEthernet2
LAN / servicio	GigabitEthernet0/0/3	GigabitEthernet3
Gestión	GigabitEthernet0/0/0	GigabitEthernet4

Tabla 7 Configuración de interfaces y puertos según las diferentes redes

Para configurar la red de gestión en C8000V utilizar los siguientes comandos desde la CLI:

```
C8Kv-1# config-transaction
C8Kv-1(config)# hostname C8Kv-1
C8Kv-1(config)# vrf definition Mgmt-intf
C8Kv-1(config-vrf)# description Mgmt-intf VPN
C8Kv-1(config-vrf)# rd 1:512
C8Kv-1(config-vrf)# address-family ipv4
C8Kv-1(config-ipv4)# route-target export 1:512
C8Kv-1(config-ipv4)# route-target import 1:512
C8Kv-1(config-ipv4)# exit-address-family
C8Kv-1(config)# interface GigabitEthernet4
C8Kv-1(config-if)# description Mgmt-intf
C8Kv-1(config-if)# vrf forwarding Mgmt-intf
C8Kv-1(config-if)# ip address <IP_GESTION> <MASCARA>
C8Kv-1(config-if)# negotiation auto
C8Kv-1(config-if)# no shutdown
C8Kv-1(config)#    ip    route    vrf    Mgmt-intf    0.0.0.0    0.0.0.0
<GATEWAY_GESTION>
C8Kv-1(config)# commit
```

Posteriormente para configurar la red de transporte utilizar los siguientes comandos desde la CLI:

```
C8Kv-1(config)# interface GigabitEthernet1
C8Kv-1(config-if)# ip address <IP_TRANSPORTE> <MASCARA>
C8Kv-1(config-if)# no shutdown
C8Kv-1(config)# ip route 0.0.0.0 0.0.0.0 <GATEWAY_TRANSPORTE>
C8Kv-1(config)# commit

C8Kv-1(config)# interface Tunnel1
C8Kv-1(config-if)# no shutdown
C8Kv-1(config-if)# ip unnumbered GigabitEthernet1
C8Kv-1(config-if)# tunnel source GigabitEthernet1
C8Kv-1(config-if)# tunnel mode sdwan
C8Kv-1(config-if)# exit
C8Kv-1(config)# sdwan
C8Kv-1(config-sdwan)# interface GigabitEthernet1
C8Kv-1(config-interface-GigabitEthernet1)# tunnel-interface
C8Kv-1(config-tunnel-interface)# encapsulation ipsec
C8Kv-1(config-tunnel-interface)# color public-internet
C8Kv-1(config-tunnel-interface)# commit
```

La red de servicio debe configurarse en la VRF/VPN correspondiente. Si se utiliza OSPF u otro protocolo de routing, debe estar documentado y restringido a la red correspondiente:

```
C8Kv-1(config)# interface GigabitEthernet3
C8Kv-1(config-if)# description Service Side
C8Kv-1(config-if)# vrf forwarding 2
C8Kv-1(config-if)# ip address <IP_LAN> <MASCARA>
C8Kv-1(config-if)# no mop enabled
C8Kv-1(config-if)# no mop sysid
C8Kv-1(config-if)# no shutdown
C8Kv-1(config)# commit
```

Para más información consultar las secciones “3.7.4 Configure cEdge Management Interface”, “3.7.5 Configure cEdge Transport Interface” y “3.7.6 Configure cEdge LAN Side Interface” de [REF2].

6.7 GESTIÓN DE CERTIFICADOS

El producto utiliza certificados X.509 para la autenticación de los controladores y dispositivos cEdge dentro de la infraestructura SD-WAN. En la configuración evaluada, las comunicaciones entre controladores y dispositivos utilizan certificados emitidos por una Autoridad de Certificación (CA) de confianza. La gestión de certificados se realiza principalmente desde Cisco vManage. Se describe en detalle su configuración en el apartado *6.1.4 CONFIGURACIÓN DEL CONTROLADOR PARA CERTIFICADOS EMPRESARIALES.*

Los certificados empleados en el producto deberán cumplir los requisitos establecidos en la guía CCN-STIC-807:

a. RSA con longitud mínima de 3072 bits.

b. ECDSA utilizando curva P-256 o superior.

c. Funciones hash SHA-256 o superiores.

6.8 SERVIDORES DE AUTENTICACIÓN

La configuración evaluada utiliza autenticación local. Por lo tanto, no se deberá usar RADIUS/TACACS+ en la configuración evaluada de este Procedimiento de Empleo Seguro. No obstante el uso de servidores de autenticación depende del sistema y políticas de la organización.

6.9 SINCRONIZACIÓN

El producto permite gestionar internamente la fecha y la hora. Esta fecha y hora se utilizan como marca de tiempo que se aplica a los registros de auditoría generados por el producto.

Los administradores pueden actualizar el reloj del producto manualmente o utilizar un servidor NTP externo para la sincronización automática. Se recomienda el uso de NTP de forma segura.

Para la configuración del NTP de los controladores y de los router cEdge puede realizarse desde vManage mediante plantillas de dispositivo o desde la CLI.

En caso de usar NTP se deberá habilitar autenticación NTP para proteger la integridad de la sincronización horaria. Se podrá hacer usando los siguientes comandos desde la CLI:

```
cEdge# configure terminal
```

```
cEdge(config)# ntp authentication-key 1 hmac-sha2-256 <password>
```

6.10 ACTUALIZACIONES

Las actualizaciones deben realizarse únicamente por administradores autorizados y utilizando imágenes oficiales de Cisco. Pueden descargarse desde el portal del fabricante [REF6].

El producto permite actualización manual del firmware. Las imágenes de firmware son verificadas mediante firma digital antes de su instalación. Si la verificación de la imagen falla al intentar realizar una instalación o actualización, el producto desactiva de forma segura sus interfaces para impedir el flujo involuntario de cualquier información hacia o desde el mismo y se reinicia.

Una vez descargada la imagen de software, se debe transferir desde la ubicación de descarga al dispositivo Cisco empleando el protocolo SCP. No se deben emplear TFTP o FTP:

```
Puesto_de_gestion# scp <software image> admin@<IP de
GigabitEthernet0/0>:<software image>
```

Se deberán usar los siguientes comandos desde la CLI la nueva imagen:

```
Controller #request software sdwan software install bootflash:
<software image>
Controller#request software sdwan software activate <software image>
Controller#request software sdwan software set-default
```

Finalmente, para verificar la nueva versión de instalada se puede usar el comando siguiente:

```
Controller#Show version
```

6.11 AUTO-CHEQUEOS

El producto ejecuta una serie de autocomprobaciones durante el arranque inicial para verificar el correcto funcionamiento de los módulos criptográficos. Si algún componente indica un fallo en la prueba POST, el sistema se bloquea y se muestra la información correspondiente en la consola local. Durante la prueba POST, se impide que todos los puertos pasen al estado de reenvío.

Si todos los componentes de todos los módulos superan la prueba POST, el sistema pasa al estado «FIPS PASS» y se permite a los puertos reenviar el tráfico de datos. Si falla alguna de las pruebas, se muestra un mensaje en la consola local y el producto se reiniciará automáticamente. Si el administrador observa un fallo en la autocomprobación criptográfica, debe ponerse en contacto con el servicio de asistencia técnica de Cisco.

Si el administrador necesita ejecutar autocomprobaciones criptográficas en el router cEdge después de cargar la imagen, introducir el siguiente comando en la CLI:

```
test crypto self-test
```

6.12 AUDITORÍA

6.12.1 REGISTRO DE EVENTOS

El producto es capaz de generar registros de auditoría que se almacenan internamente en el propio producto cada vez que se produce un evento auditado, además de transferirse

simultáneamente a un servidor syslog externo. Para una lista todos los eventos que se auditan consultar la tabla 21 de [REF2].

El administrador puede configurar el nivel de los registros de auditoría para que se almacenen en un búfer local, se envíen al servidor syslog o ambas cosas. Además, el administrador puede consultar los archivos desde la CLI local o la interfaz gráfica de usuario de vManage.

6.12.2 ALMACENAMIENTO LOCAL

El búfer de registro local es circular. Los logs más recientes sobrescriben a los más antiguos una vez que el búfer se llena.

Cuando se configura para una copia de seguridad de Syslog, el producto descargará simultáneamente los eventos de un búfer independiente al servidor Syslog externo. Este búfer se utiliza para poner en cola los eventos que se enviarán al servidor Syslog en caso de que se pierda la conexión con el servidor.

Dado que el almacenamiento local de registros no es persistente y dispone de capacidad limitada, se deberá configurar el envío de eventos de auditoría a un servidor syslog externo protegido mediante TLS.

6.12.3 ALMACENAMIENTO REMOTO

El producto permite exportar registros mediante syslog protegido mediante TLS.

La configuración se realiza mediante la creación de una plantilla. Para más detalles sobre la creación y configuración de estos parámetros pueden consultarse en la sección “3.8.1.5 Create Cisco Logging Templates” de [REF2].

También es posible configurarlo desde la CLI con los siguientes comandos:

```
Controller(config)#system
Controller(config)#logging
Controller(config)#server <IP>
```

6.13 BACKUP

Tras la instalación, se deberá realizar una copia de seguridad de la configuración del producto. Asimismo, se recomienda la realización de forma periódica de copias de seguridad tras cualquier cambio relevante de configuración, actualización de firmware o modificación de parámetros de seguridad.

La restauración de una copia de seguridad únicamente deberá realizarse por administradores autorizados y verificando previamente que la copia corresponde a una configuración permitida dentro del alcance de la configuración evaluada.

Para realizar un backup del vManage a un servidor externo se puede usar el siguiente comando:

```
Controller#request nms configuration-db backup path
```

En el caso del vBond y vSmart se realizará con el siguiente comando:

```
Controller#sh run  (en un fichero texto)
```

7 REFERENCIAS

[REF1] Cisco cEdge Routers running IOS XE 17.12 with SD-WAN 20.12
Security Target Version: 1.2 Date: December 16 2024 (https://www.commoncriteriaportal.org/files/epfiles/654-LSS%20ST%20v1.2.pdf)

[REF2] Cisco cEdge Routers running IOS XE 17.12 with SD-WAN 20.12 Common Criteria Operational User Guidance and Preparative Procedures Version: 0.9
Date: 18 December 2024 (https://www.cisco.com/c/dam/en_us/solutions/industries/government/security_certification/pdfs/c-edge-routers-running-ios-xe-17-12-w.pdf)

[REF3] SD-WAN Controller Setup Guide (On-Prem, Non Cloud-Managed)
(https://community.cisco.com/t5/networking-knowledge-base/sd-wan-controller-setup-guide-on-prem-non-cloud-managed/ta-p/3921360)

[REF4] Portal de Software de Cisco (http://www.cisco.com/cisco/software/navigator.html)

[REF5] Centro de Asistencia Técnica de Cisco (TAC): (http://www.cisco.com/techsupport)

[REF6] Portal de descargas de Cisco (https://software.cisco.com/download/home)

[REF7] Cisco IOS XE Catalyst SD-WAN Qualified Command Reference Guide
(https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/iosxe/qualified-cli-command-reference-guide/m-aaa-commands.html)

[REF8] CPSTIC
https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

8 ABREVIATURAS

AES	Advanced Encryption Standard.
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol.
BIOS	Basic Input/Output System
CA	Certificate Authority
CC	Common Criteria.
CIMC	Cisco Integrated Management Controller
CLI	Command Line Interface.
CPD	Centro Procesamiento de Datos.
CPSTIC	Catálogo de Productos y Servicios de STIC.
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DHCP	Dynamic Host Configuration Protocol.
ECDSA	Elliptic Curve Digital Signature Algorithm.
ENS	Esquema Nacional de Seguridad.
FIPS	Federal Information Processing Standards.
FTP	File Transfer Protocol
GUI	Graphical User Interface.
HTTPS	HyperText Transfer Protocol Secure
LAN	Local Area Network
MitM	Man-in-the-Middle
NIM	Network Interface Module
NTP	Network Time Protocol.
OCSP	Online Certificate Status Protocol
OSPF	Open Shortest Path First
OVA	Open Virtual Appliance
OVF	Open Virtualization Format
POST	Power-On Self-Test
RADIUS	Remote Authentication Dial-In User Service
RSA	Rivest–Shamir–Adleman
SDN	Software-defined networking
SD-WAN	Software-Defined Wide Area Network
SHA	Secure Hash Algorithm
SSH	Secure Shell
STP	Spanning Tree Protocol
TACACS	Terminal Access Controller Access-Control System
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UCS	Unified Computing System
VLAN	Virtual Local Area Network
VRF	Virtual Routing and Forwarding