Guía de Cisco para reforzar los dispositivos empresariales de Cisco Unified Border Element (CUBE)

Contenido

Introducción

Este documento le ayudará a proteger y fortalecer sus dispositivos Cisco IOS e IOS-XE que actúan como controlador de borde de sesión (SBC) que ejecuta Cisco Unified Border Element (CUBE) Enterprise.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

- CUBE Enterprise con IOS-XE 17.10.1a.

Nota:

Que algunas características detalladas en este documento no estén disponibles en versiones anteriores de IOS-XE. Siempre que ha sido posible, se ha tenido cuidado de documentar cuándo se ha introducido o modificado un comando o función.

Este documento no es aplicable a CUBE Media Proxy, CUBE Service Provider, Gateways MGCP o SCCP, Gateways Cisco SRST o ESRST, Gateways H323 u otras Gateways de voz analógicas/TDM.

Antecedentes

Este documento sirve como una adición a lo que se puede encontrar en la Guía de Cisco para fortalecer los dispositivos Cisco IOS. Como tal, los elementos duplicados de ese documento no se duplicarán en este documento.

Criterios Comunes (CC) y Normas Federales de Información (FIPS)

Cisco virtual CUBE que utiliza IOS-XE 16.9+ en un CSR1000v o CAT8000v puede utilizar el comando **cc-mode** para habilitar la aplicación de Criterios comunes (CC) y de la certificación de los Estándares federales de información (FIPS) en varios módulos criptográficos, como los que se encuentran en Transport Layer Security (TLS) y . No existe un comando equivalente para CUBE que se ejecute en los routers de hardware, pero las secciones posteriores proporcionarán métodos para habilitar manualmente un endurecimiento similar.

Fuente: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_cc_fips_compliance.html

Seguridad de la capa de transporte (TLS) e infraestructura de clave pública (PKI)

En esta sección se analizarán los elementos relacionados con TLS y PKI que pueden mejorar la seguridad proporcionada por estos protocolos junto con las operaciones de protocolo de inicio de sesión seguro (SIP) y protocolo seguro en tiempo real (SRTP).

Utilizar TCP TLS y SRTP

De forma predeterminada, CUBE aceptará conexiones SIP entrantes a través de TCP, UDP o SIP TCP-TLS. Mientras que las conexiones TCP-TLS fallarán si no se configura nada, CUBE aceptará y procesará TCP y UDP. Para las conexiones salientes, SIP utilizará las conexiones UDP de forma predeterminada a menos que

haya un comando TCP o TCP-TLS presente. Del mismo modo, CUBE negociará sesiones de protocolo en tiempo real (RTP) no seguras. Ambos protocolos proporcionan una amplia oportunidad para que un atacante muestre brillo a los datos de una señalización de sesión SIP o un flujo de medios sin cifrar. Siempre que sea posible, se recomienda asegurar la señalización SIP con SIP TLS y la transmisión de medios con SRTP.

Consulte la guía de configuración de SIP TLS y SRTP:

- https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_sip_tls_support_cube.html
- https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_cc_fips_compliance.html?bookSearch=true#id_118373

Recuerde, la seguridad es tan fuerte como el enlace más débil y SIP-TLS y SRTP deben habilitarse en todos los tramos de llamada a través de CUBE.

Las secciones restantes se agregarán a estas configuraciones predeterminadas en un esfuerzo por proporcionar funciones de seguridad adicionales:

Desactivar puertos SIP no seguros

Recuerde la sección anterior detallada que CUBE aceptará TCP y UDP de entrada para CUBE de forma predeterminada. Una vez que se utiliza SIP TLS para todos los tramos de llamadas, puede ser deseable desactivar el puerto 5060 de escucha de SIP TCP y UDP no seguros.

Una vez inhabilitada, puede utilizar **show sip-ua status**, **show sip connections udp brief** o **show sip connections tcp brief** para confirmar que CUBE ya no escucha en 5060 conexiones SIP entrantes TCP o UDP.

<#root>

```
Router#
```

show sip-ua status

```
SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent for TLS over TCP : ENABLED

Router#
```

show sip connections udp brief | i 5060

```
0 [0.0.0.0]:5060: 0

Router#
```

show sip connections tcp brief | i 5060

```
0 [0.0.0.0]:5060: 0!



!
sip-ua
```

```
 no transport udp
 no transport tcp
!
```

<#root>

```
Router#
```

show sip-ua status

```
SIP User Agent Status
SIP User Agent for UDP :
```

DISABLED

```
SIP User Agent for TCP :
```

DISABLED

```
SIP User Agent for TLS over TCP : ENABLED
Router#
```

show sip connections tcp brief | i 5060

```
Router#
```

show sip connections udp brief | i 5060

CUBE también se puede configurar para funcionar junto con los VRF IOS-XE para proporcionar una mayor segmentación de la red.

Mediante la configuración de VRF y el enlace de una interfaz habilitada para VRF a un par de marcado/arrendatario; CUBE solo escuchará las conexiones entrantes para esa combinación de IP, puerto y VRF.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_voi-cube-multi-vrf.html

Aplicar TLS 1.2

En el momento de escribir este documento, TLS 1.2 es la versión más alta de TLS compatible con CUBE. TLS 1.0 está inhabilitado en IOS-XE 16.9 pero TLS 1.1 puede negociarse. Para limitar aún más las opciones durante un intercambio de señales TLS, un administrador puede forzar la única versión disponible para CUBE Enterprise a TLS 1.2

```
!
sip-ua
 transport tcp tls v1.2
!
```

Aplicar cifrados TLS

Puede ser deseable inhabilitar los cifrados TLS más débiles para que no se negocien en una sesión. A partir de IOS-XE 17.3.1, un administrador puede configurar un perfil TLS, lo que le permite al administrador la capacidad de definir exactamente qué cifrados TLS se ofrecerán durante una sesión TLS. En versiones anteriores de IOS-XE, esto se controlaba mediante el postfijo **strict-cipher** o **ecdsa-cipher** en el comando **crypto signaling** sip-ua.

Tenga en cuenta que los cifrados que seleccione deben ser compatibles con los dispositivos pares que negocian SIP TLS con CUBE. Consulte toda la documentación del proveedor correspondiente para determinar los mejores cifrados entre todos los dispositivos.

IOS-XE 17.3.1+

<#root>

```
Router(config)#
```

voice class tls-cipher 1

```
Router(config-class)#
```

cipher ?

```
<1-10> Set the preference order for the TLS cipher-suite (1 = Highest)
Router(config-class)#
```

cipher 1 ?

```
   DHE_RSA_AES128_GCM_SHA256      supported in TLS 1.2 & above
   DHE_RSA_AES256_GCM_SHA384      supported in TLS 1.2 & above
   DHE_RSA_WITH_AES_128_CBC_SHA   supported in TLS 1.0 & above
   DHE_RSA_WITH_AES_256_CBC_SHA   supported in TLS 1.0 & above
   ECDHE_ECDSA_AES128_GCM_SHA256  supported in TLS 1.2 & above
   ECDHE_ECDSA_AES256_GCM_SHA384  supported in TLS 1.2 & above
   ECDHE_RSA_AES128_GCM_SHA256    supported in TLS 1.2 & above
   ECDHE_RSA_AES256_GCM_SHA384    supported in TLS 1.2 & above
   RSA_WITH_AES_128_CBC_SHA       supported in TLS 1.0 & above
   RSA_WITH_AES_256_CBC_SHA       supported in TLS 1.0 & above
```

```
!
voice class tls-cipher 1
 cipher 1 ECDHE_RSA_AES128_GCM_SHA256
 cipher 2 ECDHE_RSA_AES256_GCM_SHA384
!
voice class tls-profile 1
 trustpoint TEST
 cipher 1
!
sip-ua
 crypto signaling default tls-profile 1
!
```

Todas las demás versiones

<#root>

```
! STRICT CIPHERS
sip-ua
 crypto signaling default trustpoint TEST
```

strict-cipher

```
 ! Only Enables:
 ! TLS_RSA_WITH_AES_128_CBC_SHA
 ! TLS_DHE_RSA_WITH_AES_128_CBC_SHA1
 ! TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 ! TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384



!
! ECDSA Ciphers
sip-ua
 crypto signaling default trustpoint TEST
```

ecdsa-cipher

```
 ! Only Enables:
 ! TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 ! TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
!
```

Utilizar claves criptográficas grandes

Se recomienda el uso de los estándares de criptografía de última generación de Cisco 2048 con las aplicaciones TLS 1.2. Los siguientes comandos se pueden utilizar para crear claves RSA para su uso con sesiones TLS.

El comando label permite a un administrador especificar fácilmente estas claves en un punto de confianza y el comando exportable garantiza que, si es necesario, el par de claves privada/pública se puede exportar con el comando como

crypto key export rsa CUBE-ENT pem terminal aes PASSWORD!123

<#root>

```
!
crypto key generate rsa general-keys modulus 2048 label CUBE-ENT exportable
!

Router#
```

show crypto key mypubkey rsa CUBE-ENT

```
% Key pair was generated at: 11:38:03 EST Mar 10 2023
Key name: CUBE-ENT
Key type: RSA KEYS
 Storage Device: private-config
 Usage: General Purpose Key
```

```
 Key is exportable. Redundancy enabled.
 Key Data:
  [..truncated..]
```

Utilizar certificados firmados por la autoridad certificadora (CA)

Los administradores deben utilizar certificados firmados por CA en lugar de certificados autofirmados al crear el certificado de punto de confianza e identidad (ID) para la empresa CUBE.

Los certificados de CA suelen proporcionar mecanismos de seguridad adicionales, como listas de revocación de certificados (CRL) o direcciones URL de protocolo de estado de certificados en línea (OCSP), que los dispositivos pueden utilizar para garantizar que el certificado no se ha revocado. El uso de cadenas de CA públicas de confianza facilita la configuración de la relación de confianza en los dispositivos del mismo nivel que pueden tener confianza incrustada para CA raíz conocidas o ya tienen confianza de CA raíz para su dominio de empresa.

Además, los certificados de CA deben incluir el indicador CA de True en las restricciones básicas y el certificado de identidad de CUBE debe incluir el parámetro de uso de clave extendida de autenticación de cliente habilitada.

A continuación, se muestran un ejemplo de certificado de CA raíz y un certificado de ID para CUBE mediante:

openssl x509 -in some-cert.cer -text -noout

<#root>

Root CA Cert

```
Certificate:
[..truncated..]
 X509v3 extensions:
```

X509v3 Basic Constraints

:

critical

CA:TRUE

```
, pathlen:0
[..truncated..]
   X509v3
```

Extended Key Usage

```
:
     TLS Web Server Authentication, TLS Web
```

Client Authentication

```
[..truncated..]
```

```
### ID Cert


Certificate:
 Data:
[..truncated..]
  Signature Algorithm:
sha256WithRSAEncryption


[..truncated..]
  Subject Public Key Info:
   Public Key Algorithm: rsaEncryption


RSA Public-Key: (2048 bit)


[..truncated..]
  X509v3 extensions:
   X509v3 Key Usage: critical
    Digital Signature, Key Encipherment
[..truncated..]
   X509v3
Extended Key Usage
:
    TLS Web Server Authentication,
TLS Web Client Authentication


[..truncated..]
```

Utilizar hashes potentes

Al configurar un punto de confianza para el Certificado de identidad de CUBE, se deben seleccionar algoritmos de hash seguros como SHA256, SHA384 o SHA512:

```
<#root>

Router(config)#
 crypto pki trustpoint CUBE-ENT


Router(ca-trustpoint)#
hash ?


 md5 use md5 hash algorithm
 sha1 use sha1 hash algorithm
 sha256 use sha256 hash algorithm


 sha384 use sha384 hash algorithm
```

```
sha512 use sha512 hash algorithm
```

Habilitar comprobaciones de la lista de revocación de certificados (CRL) o del protocolo de estado de certificados en línea (OCSP)

De forma predeterminada, los Trustpoints de IOS-XE intentarán verificar la CRL enumerada dentro de un certificado durante el comando **crypto pki auth**, más tarde durante los handshakes de TLS, IOS-XE también realizará otra captura de CRL basada en el certificado recibido para confirmar que el certificado sigue siendo válido. Los métodos para CRL pueden ser HTTP o LDAP y la conectividad con la CRL debe estar presente para que esto se realice correctamente. Es decir, la resolución DNS, el socket TCP y la descarga de archivos del servidor al router IOS-XE deben estar disponibles; de lo contrario, la comprobación de CRL fallará. De manera similar, un punto de confianza IOS-XE se puede configurar para utilizar el valor de OCSP de un encabezado AuthorityInfoAccess (AIA) dentro del certificado que realiza consultas a un Respondedor de OCSP a través de HTTP para verificar y realizar comprobaciones similares. Un administrador puede reemplazar el punto de distribución de CRL (CDP) o OCSP dentro de un certificado proporcionando una dirección URL estática en un certificado. Además, un administrador también puede configurar el orden en el que se comprueba CRL u OCSP suponiendo que ambos estén presentes.

Muchos simplemente inhabilitan las comprobaciones de revocación con **revocation-check none** para simplificar el proceso, pero al hacerlo un administrador debilita la seguridad y elimina el mecanismo de IOS-XE para verificar con estado si un certificado dado sigue siendo válido. Siempre que sea posible, los administradores deben aprovechar OCSP o CRL para realizar una comprobación de estado de los certificados recibidos. Para obtener más información sobre CRL u OCSP, revise el siguiente documento:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-17/sec-pki-xe-17-book/sec-cfg-auth-rev-cert.html

Comprobación de CRL

<#root>

```
! Sample A: CRL from the certificate


crypto pki trustpiont ROOT-CA
 revocation-check crl
!

! Sample B: CRL Override OCSP in certificate


crypto pki certificate map CRL-OVERRIDE 1
 issuer-name eq root-ca.cisco.com
 subject-name eq root-ca.cisco.com
 alt-subject-name co cisco.com
!
crypto pki trustpoint ROOT-CA
 revocation-check crl
 match certificate CRL-OVERRIDE override cdp url http://www.cisco.com/security/pki/crl/crca2048.crl
!
```

Comprobación de OCSP

<#root>

```
! Sample A: OCSP from the certificate


crypto pki trustpiont ROOT-CA
 revocation-check ocsp
!

! Sample B: Override OCSP in certificate


crypto pki certificate map OCSP-OVERRIDE 1
 issuer-name eq root-ca.cisco.com
 subject-name eq root-ca.cisco.com
 alt-subject-name co cisco.com
!
crypto pki trustpoint ROOT-CA
 revocation-check ocsp
 match certificate OCSP-OVERRIDE override ocsp 1 url http://ocsp-responder.cisco.com
!
```

Comprobación de OCSP y CRL solicitada

<#root>

```
! Check CRL if failure, check OCSP


crypto pki trustpoint ROOT-CA
 revocation-check crl ocsp
!
```

Habilitar la verificación de nombre común (CN) y nombre alternativo del sujeto (SAN)

CUBE se puede configurar para verificar que el CN o SAN del certificado coincide con el nombre de host del comando **session target dns:**. En IOS-XE 17.8+ se puede configurar un perfil TLS mediante el perfil TLS.

IOS-XE 17.8+

<#root>

```
Router(config)#

voice class tls-profile 1


Router(config-class)#

cn-san validate ?


  bidirectional Enable CN/SAN validation for both client and server certificate
  client Enable CN/SAN validation for client certificate
```

```
  server Enable CN/SAN validation for server certificate
```

Recuerde que la designación de cliente/servidor hace referencia al rol de dispositivos pares en el intercambio de señales TLS

Para ilustrar con más detalle:

- **servidor de validación cn-san:** CUBE realizará la validación del nombre de host de los certificados de *servidor de* peer recibidos para las conexiones TLS salientes, donde CUBE es la función de cliente.
- **cn-san validate client:** CUBE realizará la validación del nombre de host de los certificados de *cliente de* peer recibidos para las conexiones TLS entrantes donde CUBE es el rol de servidor.
- **cn-san validate bidirection**: habilita la validación del nombre de host para ambos roles de peer durante el intercambio de señales TLS.

Cuando utilice el comando **cn-san validate client** (o bidireccional), debe configurar una SAN para comprobarla, ya que el destino de sesión se comprueba sólo para las conexiones salientes y cn-san validate server.

Validación de nombre de host de cliente:

```
!
voice class tls-profile 1
 cn-san validate client
 cn-san 1 *.example.com
 cn-san 2 subdomain.example.com
!
```

Validación de nombre de host del servidor:

```
!
voice class tls-profile 1
 cn-san validate server
!
sip-ua
 crypto signaling default tls-profile 1
!
dail-peer voice 1 voip
 session target dns:subdomain.example.com
!
```

Anterior a 17.8.1

Nota: Sólo la validación del nombre de host del servidor está disponible mediante este método.

<#root>

```
!
sip-ua
 crypto signaling default trustpoint TEST
```

```
cn-san-validate server


!
dail-peer voice 1 voip
 session target dns:subdomain.example.com
!
```

CUBE también se puede configurar para enviar la extensión TLS 1.2 de indicación de nombre de servidor (SNI) con el nombre de host FQDN de CUBE dentro del protocolo de enlace TLS a dispositivos pares para facilitar sus esfuerzos de validación de nombres de host.

```
!
voice class tls-profile 1
 sni send
!
sip-ua
 crypto signaling default tls-profile 1
!
```

Una nota sobre el Mutual TLS de CUBE:

- De forma predeterminada, cuando CUBE actúa como servidor TLS (leer conexión TLS entrante), siempre solicitará un certificado de cliente. No hay ninguna configuración para deshabilitar este comportamiento.
- Cuando CUBE actúa como cliente TLS e inicia una conexión TLS saliente, la conexión mutua TLS depende del dispositivo par que actúa como servidor TLS. En esta situación, es posible que un dispositivo par no solicite un certificado de cliente de CUBE.
- En ambos escenarios, la cadena de certificados que CUBE enviaría está controlada por el **punto de confianza** definido en el perfil TLS o en el comando crypto signaling.

<#root>

```
!
sip-ua
 crypto signaling default
trustpoint CUBE-ENT


!
! OR
voice class tls-profile 1


trustpoint CUBE-ENT


!
sip-ua
 crypto signaling default tls-profile 1
!
```

Asignar conexiones TLS remotas a puntos de confianza específicos

Cuando se utiliza el comando **crypto signaling default** sip-ua **ALL** las conexiones TLS entrantes se mapean a esta configuración ya sea a través de los comandos tls-profile o los comandos individuales post-fix. Además, todos los puntos de confianza disponibles se comprueban al realizar la validación de certificados.

Puede ser deseable crear configuraciones de perfil TLS específicas para dispositivos pares específicos basados en la dirección IP para garantizar que exactamente los parámetros de seguridad que defina se aplican a esa sesión TLS. Para hacer esto, utilice el comando **crypto signaling remote-addr** para definir una subred IPv4 o IPv6 para mapear a un perfil tls o un conjunto de comandos postfix. También puede asignar directamente el punto de confianza de verificación a través de los comandos **client-vtp**) para bloquear exactamente qué puntos de confianza se utilizan para validar los certificados de peer.

El siguiente comando resume la mayoría de los elementos discutidos hasta este punto:

```
!
voice class tls-cipher 1
 cipher 1 ECDHE_RSA_AES128_GCM_SHA256
 cipher 2 ECDHE_RSA_AES256_GCM_SHA384
!
voice class tls-profile 1
 trustpoint CUBE-ENT
 cn-san validate bidirectional
 cn-san 1 *.example.com
 cipher 2
 client-vtp PEER-TRUSTPOINT
 sni send
!
sip-ua
 crypto signaling remote-addr 192.168.1.0 /24 tls-profile 1
!
```

Para las versiones más antiguas, esto se puede hacer de la siguiente manera:

```
!
sip-ua
 crypto signaling remote-addr 192.168.1.0 /24 trustpoint CUBE-ENT cn-san-validate server client-vtp PEER
!
```

A partir de la versión 17.8, también puede configurar los puertos de escucha por arrendatario y perfil de TLS por **arrendatario de clase de voz** para proporcionar opciones de segmentación adicionales en un puerto de escucha determinado.

```
!
voice class tenant 1
 tls-profile 1
 listen-port secure 5062
```

```
!
```

Aplicar SRTP estricto

Cuando se habilita SRTP en CUBE Enterprise, la operación predeterminada es no permitir el repliegue a RTP.

Siempre que sea posible, utilice SRTP en todos los tramos de llamada; sin embargo, de forma predeterminada, CUBE realizará RTP-SRTP según sea necesario.

Tenga en cuenta que CUBE no registra las claves SRTP en depuraciones que comienzan en 16.11+

```
!
voice service voip
 srtp
!
! or
!
dial-peer voice 1 voip
 srtp
!
```

Recortar cifrados SRTP no seguros

De forma predeterminada, CUBE envía todos los cifrados SRTP al crear una oferta. Un administrador puede reducir a cifrados más seguros como los conjuntos de cifrados AEAD de última generación mediante el comando voice class srtp-crypto en IOS-XE 16.5+.

Esta configuración también puede cambiar la preferencia predeterminada que se utiliza cuando CUBE selecciona un cifrado SRTP y crea una respuesta a alguna oferta con varias opciones disponibles.

Nota: es posible que algunos dispositivos de Cisco o dispositivos del mismo nivel antiguos no admitan cifrados AEAD. Consulte toda la documentación aplicable al recortar conjuntos cifrados.

<#root>

```
Router(config)#
```

voice class srtp-crypto 1

```
Router(config-class)#
```

crypto ?

```
  <1-4> Set the preference order for the cipher-suite (1 = Highest)
```

```
Router(config-class)#
```

crypto 1 ?

```
  AEAD_AES_128_GCM        Allow secure calls with SRTP AEAD_AES_128_GCM cipher-suite
  AEAD_AES_256_GCM        Allow secure calls with SRTP AEAD_AES_256_GCM cipher-suite
  AES_CM_128_HMAC_SHA1_32 Allow secure calls with SRTP AES_CM_128_HMAC_SHA1_32 cipher-suite
  AES_CM_128_HMAC_SHA1_80 Allow secure calls with SRTP AES_CM_128_HMAC_SHA1_80 cipher-suite
```

```
!
voice class srtp-crypto 1
 crypto 1 AEAD_AES_256_GCM
 crypto 2 AEAD_AES_128_GCM
!
voice service voip
 sip
  srtp-crypto 1
!
! or
!
voice class tenant 1
 srtp-crypto 1
!
! or
!
dial-peer voice 1 voip
 voice-class srtp-crypto 1
!
```

Desactivar otros protocolos VoIP no utilizados

Si H323, MGCP, SCCP, STCAPP, CME, SRST no se están utilizando en este gateway, vale la pena eliminar las configuraciones para fortalecer CUBE.

Desactivar H323 y permitir solo SIP para llamadas SIP

```
!
voice service voip
 allow-connections sip to sip
 h323
  call service stop
!
```

Inhabilite MGCP, SCCP, STCAPP, SIP y SCCP SRST.

Nota: Algunos de estos comandos eliminarán el resto de las configuraciones, asegúrese de que las funciones no se estén utilizando antes de eliminarlas completamente.

<#root>

```
Router(config)#
```

no mgcp

```
Router(config)#
no sccp

Router(config)#
no stcapp

Router(config)#
no voice register global

Router(config)#
no telephony-service

Router(config)#
no call-manager-fallback
```

Ruteo de llamadas y fraude de llamadas

Permitir conexiones desde IP fiables

De forma predeterminada, CUBE confiará en las conexiones entrantes de las direcciones IPv4 e IPv6 configuradas en las configuraciones de **destino de sesión de** dial-peer y de **grupo de servidores de clase de voz**.

Para agregar direcciones IP adicionales, utilice el comando **ip address trusted list** configurado a través del **servicio de voz voip.**

Cuando la validación del nombre de host cliente/servidor se configura junto con SIP TLS mediante la función de validación CN/SAN mencionada anteriormente, una validación CN/SAN satisfactoria omitirá las comprobaciones de la lista de direcciones IP fiables.

Evite utilizar **ninguna dirección IP autenticada de confianza** que permitirá a CUBE aceptar CUALQUIER conexión entrante.

```
!
voice service voip
 ip address trusted authenticate

 ip address trusted list
  ipv4 192.168.1.1
  ipv4 172.16.1.0 /24
!
```

Utilice **show ip address trusted list** para ver el estado de la verificación de la dirección IP y todas las definiciones de listas de confianza estáticas y dinámicas derivadas de otras configuraciones.

Tenga en cuenta que el valor dinámico derivado de un par de marcado/grupo de servidores se elimina de la

lista de confianza cuando un par de marcado se apaga o se establece en estado inactivo después de que se produzcan errores en las comprobaciones de keepalive.

De forma predeterminada, cuando una llamada entrante no pasa la verificación de la lista de confianza IP, se descarta silenciosamente, pero esto se puede anular usando el comando **no silent-discard untrusted** voice service voip > sip para enviar un error al remitente. Sin embargo, mediante el envío de una respuesta, un atacante puede utilizar esta función para indicar que el dispositivo está escuchando realmente el tráfico SIP y aumentar sus esfuerzos de ataque. Como tal, el descarte silencioso es el método preferido para manejar las caídas de la Lista de Confianza IP.

Evite el ruteo de dial-peer genérico

El uso de patrones de destino genéricos "catch all", como **destination-pattern .T**, puede aumentar la probabilidad de enrutar una llamada fraudulenta a través de CUBE.

Los administradores deben configurar CUBE para que enrute únicamente las llamadas de intervalos de números de teléfono conocidos o URI de SIP.

Consulte el siguiente documento para obtener una explicación más detallada de las funciones de enrutamiento de llamadas de CUBE:

https://www.cisco.com/c/en/us/support/docs/voice/ip-telephony-voice-over-ip-voip/211306-In-Depth-Explanation-of-Cisco-IOS-and-IO.html

Mitigación de amenazas CUBE

Manejo de paquetes mal formado

De forma predeterminada, CUBE inspeccionará los paquetes SIP y RTP para verificar si hay errores y descartará el paquete.

Paquetes RTP no fiables

De forma predeterminada, IOS-XE CUBE realiza la validación del puerto de origen para todos los flujos RTP/RTCP permitiendo solamente las conexiones negociadas a través de la señalización de oferta/respuesta SDP SIP y no se puede inhabilitar.

Éstos pueden ser monitoreados mediante la verificación del siguiente comando:

```
show platform hardware qfp active feature sbc global | s Total packets dropped|Dropped packets:
```

Para la interoperabilidad con CUCM, se recomienda habilitar la transmisión de medios dúplex a través del servicio Cisco CallManager para evitar que la música en espera se descarte cuando se origina en el puerto 4000.

RTP Port Range Hardening

De forma predeterminada, IOS-XE utiliza el intervalo de puertos de 8000 a 48198. Esto se puede configurar en un rango diferente como 16384 a 32768 a través del siguiente comando:

```
!
voice service voip
 rtp-port range 16384 32768
!
```

Un administrador también puede configurar intervalos de puertos RTP por intervalos de direcciones IPv4 e IPv6.

Esta configuración también permite que la aplicación VoIP de CUBE realice la gestión de paquetes fantasma de manera más eficiente al no puntear estos paquetes al proceso UDP en la CPU del router, ya que el rango de puertos e IP están definidos estáticamente. Esto puede ayudar a mitigar el uso elevado de la CPU al manejar un gran número de paquetes RTP legítimos o ilegítimos al eludir el comportamiento de punteo de la CPU.

```
voice service voip
 media-address range 192.168.1.1 192.168.1.1
  port-range 16384 32768
 media-address range 172.16.1.1 172.16.1.1
  port-range 8000 48198
```

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_phantom-packet-handling.html

Prevención de denegación de servicio (DOS)

Las funciones de control de admisión de llamadas se pueden habilitar para limitar las llamadas según el total de llamadas, la CPU, la memoria y el ancho de banda. Además, se pueden detectar picos de llamadas para rechazar las llamadas y evitar la denegación de servicio.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_voi-cube-call-admission-control.html

Ocultación de direcciones

De forma predeterminada, CUBE sustituirá las direcciones IP de los encabezados SIP como, entre otros, Via, Contact y From por su propia dirección IP.

Esto se puede ampliar a los encabezados Referir a, Referido por, 3xx contact header, History-Info y Diversion aplicando el comando **voice service voip address-hidden**.

Además, se crea un nuevo call-id para cada dirección IP de mitigación de tramo de llamada que se puede incrustar en este valor de encabezado.

Cuando se requiere un nombre de host en lugar de una dirección IP para ocultar la dirección, se puede configurar el comando **voice-class sip localhost dns:cube.cisco.com**.

Privacidad de identificación de llamada

CUBE se puede configurar para descartar los valores de Nombre de identificación de llamada de los encabezados SIP con el comando **clid-strip name** configurado en cualquier par de marcado.

Además, CUBE puede interactuar y comprender encabezados de privacidad SIP como P-Preferred Identity (PPID), P-Asserted Identity (PAID), Privacy, P-Called Party Identity (PCPID) e Remote-Party Identity (RPID). Para obtener más información, consulte el siguiente documento: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_voi-paid-ppid-priv.html

Autenticación implícita SIP

Durante el registro SIP por parte de CUBE a un proveedor de servicios o durante una señalización de llamada ascendente, los dispositivos UAS pueden devolver un código de estado 401 o 407 con un campo de encabezado WW-Authenticate/Proxy-Authenticate aplicable que desafía a CUBE a autenticarse. Durante este intercambio de señales, CUBE admite el algoritmo MD5 para calcular el valor del campo de encabezado de autorización en una solicitud posterior.

Encabezados SIP o SDP no compatibles

CUBE quitará los encabezados SIP o SDP no compatibles que no entienda. Se debe tener cuidado al utilizar comandos como **pass-thru content sdp**, **pass-thru content unsupp** o **pass-through header unsupp** para asegurarse de qué datos pasan a través de CUBE.

Eliminación o modificación de encabezados SIP o SDP

Donde se requiere control adicional, los perfiles SIP entrantes o salientes pueden ser configurados por un administrador para modificar o descartar de manera flexible un encabezado SIP o un atributo SDP.

Consulte los siguientes documentos sobre el uso del perfil SIP:

- https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_voi-sip-param-mod.html
- https://www.cisco.com/c/en/us/support/docs/voice/ip-telephony-voice-over-ip-voip/211306-In-Depth-Explanation-of-Cisco-IOS-and-IO.html#anc45

Otras Funciones de Seguridad

Contraseñas cifradas

CUBE requiere contraseñas cifradas para las versiones 16.11 y posteriores para cifrar el registro SIP y otras contraseñas IOS-XE en la configuración en ejecución.

```
password encryption aes
key config-key password-encrypt cisco123
```

Listas de acceso

La función de lista de confianza funciona en la capa 7 dentro de la aplicación CUBE. Cuando el paquete se descarta silenciosamente, el CUBE ya ha comenzado a procesar el paquete.

Puede ser conveniente bloquear las interfaces con las listas de acceso de capa 3 o 4 entrantes o salientes para descartar el paquete en el punto de entrada del router.

Esto garantiza que los ciclos de CPU de CUBE se gastan en tráfico legítimo. Las ACL junto con la lista de confianza IP y la validación de nombres de host proporcionan un enfoque por capas de la seguridad de CUBE.

Firewall basado en zonas (ZBFW)

Cisco CUBE se puede configurar junto con IOS-XE ZBFW para proporcionar inspección de aplicaciones y otras funciones de seguridad.

Consulte la Guía de CUBE y ZBFW para obtener más información sobre este tema:

https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-border-element/220378-configure-zone-based-firewall-zbfw-co.html

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).