Guide Cisco pour renforcer les périphériques d'entreprise Cisco Unified Border Element (CUBE)

Table des matières

Introduction

Ce document vous aidera à sécuriser et à renforcer vos périphériques Cisco IOS et IOS-XE agissant en tant que SBC (Session Border Controller) exécutant Cisco Unified Border Element (CUBE) Enterprise.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

- CUBE Enterprise exécutant IOS-XE 17.10.1a.

Remarque :

Il est possible que certaines fonctionnalités détaillées dans ce document ne soient pas disponibles dans les versions antérieures d'IOS-XE. Dans la mesure du possible, on a pris soin de documenter l'introduction ou la modification d'une commande ou d'une fonction.

Ce document ne s'applique pas aux passerelles CUBE Media Proxy, CUBE Service Provider, MGCP ou SCCP, aux passerelles Cisco SRST ou ESRST, aux passerelles H323 ou aux autres passerelles vocales analogiques/TDM.

Informations générales

Ce document vient s'ajouter à ce que l'on peut trouver dans le Guide Cisco pour renforcer les périphériques Cisco IOS. Par conséquent, les éléments en double de ce document ne seront pas dupliqués dans ce document.

Critères communs (CC) et Normes fédérales de l'information (NIPPF)

Le CUBE virtuel Cisco utilisant IOS-XE 16.9+ sur un routeur CSR1000v ou CAT8000v peut utiliser la commande cc-mode pour activer l'application d'une certification Common Criteria (CC) et FIPS (Federal Information Standards) sur divers modules cryptographiques tels que ceux trouvés dans Transport Layer Security (TLS) et . Il n'existe pas de commande équivalente pour CUBE s'exécutant sur des routeurs matériels, mais des sections ultérieures fourniront des méthodes permettant d'activer manuellement un durcissement similaire.

Source : 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

TLS (Transport Layer Security) et PKI (Public Key Infrastructure)

Cette section traite des éléments relatifs aux protocoles TLS et PKI qui peuvent améliorer la sécurité fournie par ces protocoles, parallèlement aux opérations SIP (Secure Session Initial Protocol) et SRTP (Secure Real Time Protocol).

Utiliser TCP TLS et SRTP

Par défaut, CUBE accepte les connexions SIP entrantes via TCP, UDP ou SIP TCP-TLS. Alors que les connexions TCP-TLS échoueront si rien n'est configuré, TCP et UDP seront acceptés et traités par CUBE. Pour les connexions sortantes, SIP utilise les connexions UDP par défaut, sauf si une commande TCP ou TCP-TLS est présente. De même, CUBE négociera les sessions RTP (Real Time Protocol) non sécurisées. Ces deux protocoles offrent à un pirate l'opportunité d'extraire des données d'un flux multimédia ou d'une signalisation de session SIP non chiffrée. Dans la mesure du possible, il est recommandé de sécuriser la signalisation SIP avec SIP TLS et le flux multimédia avec SRTP.

Reportez-vous au guide de configuration SIP TLS et 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

N'oubliez pas que la sécurité est aussi puissante que la liaison la plus faible. Les protocoles SIP-TLS et SRTP doivent être activés sur tous les tronçons d'appel via CUBE.

Les sections restantes seront ajoutées à ces configurations par défaut afin de fournir des fonctionnalités de sécurité supplémentaires :

Désactivation des ports SIP non sécurisés

Souvenez-vous de la section précédente, qui indique que CUBE accepte les protocoles TCP et UDP entrants pour CUBE par défaut. Une fois que le protocole SIP TLS est utilisé pour tous les tronçons d'appel, il peut être souhaitable de désactiver le port d'écoute SIP TCP et UDP non sécurisé 5060.

Une fois désactivé, vous pouvez utiliser show sip-ua status, show sip connections udp brief, ou show sip connections tcp brief pour confirmer que CUBE n'écoute plus sur 5060 les connexions SIP TCP ou UDP entrantes.

<#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 peut également être configuré pour fonctionner avec les VRF IOS-XE afin de permettre une segmentation réseau plus poussée.

En configurant des VRF et en liant une interface compatible VRF à un terminal de numérotation dial-peer/locataire, CUBE n'écoute que les connexions entrantes pour cette combinaison IP, Port, 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

Appliquer TLS 1.2

Au moment de la rédaction de ce document, TLS 1.2 est la version la plus élevée de TLS prise en charge par CUBE. TLS 1.0 est désactivé dans IOS-XE 16.9, mais TLS 1.1 peut être négocié. Pour limiter davantage les options lors d'une connexion TLS, un administrateur peut forcer la seule version disponible de CUBE Enterprise à utiliser TLS 1.2

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

Appliquer les chiffrements TLS

Il peut être souhaitable de désactiver la négociation des chiffrements TLS les plus faibles dans une session. À partir de la version 17.3.1 de la plate-forme logicielle IOS-XE, un administrateur peut configurer un profil TLS qui lui permet de définir exactement les chiffrements TLS qui seront proposés au cours d'une session TLS. Dans les versions plus anciennes d'IOS-XE, cela était contrôlé en utilisant le strict-cipher ou le suffixe ecdsa-cipher sur la commande crypto signaling sip-ua.

Notez que les chiffres que vous sélectionnez doivent être compatibles avec les périphériques homologues négociant SIP TLS avec CUBE. Reportez-vous à toute la documentation du fournisseur pour déterminer les meilleurs chiffrements entre tous les périphériques.

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
!
```

Toutes les autres versions

<#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
!
```

Utiliser de grandes clés cryptographiques

Les normes Cisco de cryptographie nouvelle génération recommandées pour 2048 sont destinées aux applications TLS 1.2. Les commandes ci-dessous peuvent être utilisées pour créer des clés RSA à utiliser avec des sessions TLS.

La commande label permet à un administrateur de spécifier facilement ces clés sur un point de confiance et la commande exportable garantit que, si nécessaire, la paire de clés privée/publique peut être exportée avec la commande telle que

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..]
```

Utiliser les certificats signés par une autorité de certification

Les administrateurs doivent utiliser des certificats signés par une autorité de certification au lieu de certificats auto-signés lors de la création d'un certificat de point de confiance et d'identité (ID) pour CUBE Enterprise.

Les certificats d’autorité de certification fournissent généralement des mécanismes de sécurité supplémentaires, tels que des URL de liste de révocation de certificats (CRL) ou de protocole OCSP (Online Certificate Status Protocol), qui peuvent être utilisés par les périphériques pour garantir que le certificat n’a pas été révoqué. L'utilisation de chaînes d'autorités de certification publiques approuvées facilite la configuration de la relation d'approbation sur les périphériques homologues qui peuvent avoir une approbation intégrée pour les autorités de certification racines connues ou qui ont déjà des approbations d'autorité de certification racine pour votre domaine

d'entreprise.

En outre, les certificats d'autorité de certification doivent inclure l'indicateur d'autorité de certification Vrai dans les contraintes de base et le certificat d'identité de CUBE doit inclure le paramètre d'utilisation de clé étendue de l'authentification client activée.

L'exemple de certificat CA racine et un certificat d'ID pour CUBE sont présentés ci-dessous à l'aide de :

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..]
```

Utiliser des hashs forts

Lors de la configuration d'un point de confiance pour le certificat d'identité de CUBE, vous devez sélectionner des algorithmes de hachage forts tels que SHA256, SHA384 ou 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
```

Activer les vérifications de la liste de révocation de certificats (CRL) ou du protocole OCSP (Online Certificate Status Protocol)

Par défaut, les points de confiance IOS-XE essaieront de vérifier la liste de révocation de certificats listée dans un certificat pendant la commande crypto pki auth, plus tard pendant les échanges TLS, IOS-XE effectuera également une autre récupération de liste de révocation de

certificats basée sur le certificat reçu pour confirmer que le certificat est toujours valide. Les méthodes de CRL peuvent être HTTP ou LDAP et la connectivité à la CRL doit être présente pour que cela fonctionne. Autrement dit, la résolution DNS, le socket TCP et le téléchargement de fichiers du serveur vers le routeur IOS-XE doivent être disponibles, sinon la vérification de la liste de révocation de certificats échouera. De même, un point de confiance IOS-XE peut être configuré pour utiliser la valeur OCSP d'un en-tête AuthorityInfoAccess (AIA) dans le certificat qui exécute des requêtes à un répondeur OCSP via HTTP pour vérifier et effectuer des vérifications similaires. Un administrateur peut remplacer OCSP ou CRL Distribution Point (CDP) dans un certificat en fournissant une URL statique sur un certificat. En outre, un administrateur peut également configurer l'ordre dans lequel les listes de révocation de certificats et les protocoles OCSP sont vérifiés, en supposant que les deux sont présents.

Beaucoup désactivent simplement les contrôles de révocation avec revocation-check none afin de simplifier le processus, mais ce faisant, un administrateur affaiblit la sécurité et supprime le mécanisme de l'IOS-XE pour vérifier de manière statique si un certificat donné est toujours valide. Dans la mesure du possible, les administrateurs doivent utiliser OCSP ou CRL pour effectuer une vérification avec état des certificats reçus. Pour plus d'informations sur les LCR ou le PCO, consultez le document suivant :

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

Vérification 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
!
```

Vérification 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
!
```

Vérification OCSP et CRL commandée

<#root>

```
! Check CRL if failure, check OCSP


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

Activer la vérification du nom commun (CN) et du nom alternatif de l'objet (SAN)

CUBE peut être configuré pour vérifier que le CN ou le SAN du certificat correspond au nom d'hôte de la commande session target dns: . Dans IOS-XE 17.8+, un profil TLS peut être configuré via le profil 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
```

Souvenez-vous que la désignation client/serveur fait référence au rôle des périphériques homologues dans la connexion TLS

Pour illustrer plus en détail :

- cn-san validate server : CUBE effectuera la validation du nom d'hôte des certificats de serveur homologue reçus pour les connexions TLS sortantes où CUBE est le rôle client.
- cn-san validate client : CUBE effectue la validation du nom d'hôte des certificats clients homologues reçus pour les connexions TLS entrantes où CUBE est le rôle serveur.
- cn-san validate bidirection : active la validation du nom d'hôte pour les deux rôles homologues lors de la connexion TLS.

Lors de l'utilisation de la commande cn-san validate client (ou bidirectionnelle), vous devez configurer un SAN à vérifier par rapport à, puisque la cible de session est check is only for outbound connections et cn-san validate server.

Validation du nom d'hôte client :

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

Validation du nom d'hôte du serveur :

```
!
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
!
```

Antérieure à 17.8.1

Remarque : seule la validation du nom d'hôte du serveur est disponible via cette méthode.

<#root>

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

```
cn-san-validate server
```

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

CUBE peut également être configuré pour envoyer l'extension SNI (Server Name Indication) TLS 1.2 avec le nom d'hôte FQDN de CUBE dans la connexion TLS aux périphériques homologues afin de faciliter leurs efforts de validation de nom d'hôte.

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

Remarque sur le TLS mutuel de CUBE :

- Par défaut, lorsque CUBE agit en tant que serveur TLS (lecture de la connexion TLS entrante), il demande toujours un certificat client. Aucune configuration ne permet de désactiver ce comportement.
- Lorsque CUBE agit en tant que client TLS et initie une connexion TLS sortante, TLS mutuel appartient au périphérique homologue agissant en tant que serveur TLS. Dans ce scénario, un périphérique homologue peut ne pas demander de certificat client à CUBE.
- Dans ces deux scénarios, la chaîne de certificats que CUBE enverrait est contrôlée par le trustpoint défini dans le profil TLS ou sur la commande de signalisation crypto.

<#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
!
```

Mapper les connexions TLS distantes à des points de confiance spécifiques

Lors de l'utilisation de la commande crypto signaling default sip-ua, TOUTES les connexions TLS entrantes sont mappées à ces configurations soit via tls-profile, soit via des commandes post-fix individuelles. En outre, tous les points de confiance disponibles sont vérifiés lors de la validation du certificat.

Il peut être souhaitable de créer des configurations de profil TLS spécifiques pour un périphérique homologue spécifique en fonction de l'adresse IP afin de garantir que les paramètres de sécurité que vous définissez sont appliqués exactement à cette session TLS. Pour ce faire, utilisez la commande crypto signaling remote-addr pour définir un sous-réseau IPv4 ou IPv6 à mapper à un tls-profile ou un ensemble de commandes postfix. Vous pouvez également mapper directement le point de confiance de vérification via les commandes client-vtp) pour verrouiller exactement quels points de confiance sont utilisés pour valider les certificats homologues.

La commande ci-dessous récapitule la plupart des éléments abordés jusqu'à ce point :

```
!
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
!
```

Pour les versions plus anciennes, cela peut être fait de la façon suivante :

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

À partir de la version 17.8, vous pouvez également configurer des ports d'écoute tls-profile et par locataire par locataire de classe vocale pour fournir d'autres options de segmentation sur un port d'écoute donné.

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

Appliquer SRTP strict

Lors de l'activation de SRTP sur CUBE Enterprise, l'opération par défaut consiste à interdire le retour à RTP.

Dans la mesure du possible, utilisez SRTP sur toutes les branches d'appel, mais par défaut, CUBE exécutera RTP-SRTP si nécessaire.

Notez que CUBE ne consigne pas les clés SRTP dans les débogages commençant dans 16.11+

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

Suppression des chiffrements SRTP non sécurisés

Par défaut, tous les chiffrements SRTP sont envoyés par CUBE lors de la création d'une offre. Un administrateur peut réduire le nombre de chiffrements plus sécurisés, tels que les suites de chiffrement AEAD de nouvelle génération, à l'aide de la commande voice class srtp-crypto dans IOS-XE 16.5+.

Cette configuration peut également modifier la préférence par défaut utilisée lorsque CUBE sélectionne un chiffrement SRTP et crée une réponse à une offre avec plusieurs options disponibles.

Remarque : certains périphériques Cisco ou homologues plus anciens peuvent ne pas prendre en charge les chiffrements AEAD. Reportez-vous à toute la documentation applicable lors de l'ajustement des suites de chiffrement.

<#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
!
```

Désactiver les autres protocoles VoIP inutilisés

Si H323, MGCP, SCCP, STCAPP, CME, SRST ne sont pas utilisés sur cette passerelle, il est utile de supprimer les configurations pour renforcer CUBE.

Désactivez H323 et autorisez uniquement les appels SIP à SIP

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

Désactivez MGCP, SCCP, STCAPP, SIP et SCCP SRST.

Remarque : certaines de ces commandes supprimeront toutes les autres configurations, assurez-vous que les fonctionnalités ne sont pas utilisées avant de les supprimer complètement.

```
<#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
```

Routage des appels et fraude interurbaine

Autoriser les connexions à partir d'IP approuvées

Par défaut, CUBE approuve les connexions entrantes provenant des adresses IPv4 et IPv6 configurées sur les configurations de cible de session de terminal de numérotation dial-peer et de groupe de serveurs de classe vocale.

Pour ajouter des adresses IP supplémentaires, utilisez la commande ip address trusted list configurée via voice service voip.

Lorsque la validation du nom d'hôte client/serveur est configurée avec SIP TLS par le biais de la fonctionnalité de validation CN/SAN décrite précédemment, une validation CN/SAN réussie contournera les vérifications de la liste de confiance des adresses IP.

Évitez d'utiliser no ip address trusted authenticate qui permettra à CUBE d'accepter TOUTE connexion entrante.

```
!
voice service voip
 ip address trusted authenticate

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

Utilisez show ip address trusted list pour afficher l'état de la vérification des adresses IP et toutes les définitions de listes de confiance statiques et dynamiques dérivées d'autres configurations.

Notez que la valeur dynamique dérivée d'un terminal de numérotation dial-peer/groupe de serveurs est supprimée de la liste de confiance lorsqu'un terminal de numérotation dial-peer est arrêté ou défini à l'état down après échec des vérifications keepalive.

Par défaut, lorsqu'un appel entrant ne passe pas la vérification de la liste de confiance IP, il est ignoré silencieusement, mais il peut être remplacé à l'aide de la commande no silent-discard untrusted service voip > sip pour renvoyer une erreur à l'expéditeur. Cependant, en envoyant une réponse, un pirate peut utiliser cette information pour indiquer que le périphérique écoute en fait le trafic SIP et intensifier ses efforts d'attaque. En tant que telle, la suppression silencieuse est la méthode préférée de gestion des abandons de listes de confiance IP.

Éviter le routage de terminal de numérotation dial-peer générique

L'utilisation de modèles de destination génériques « catch all » tels que destination-pattern .T peut augmenter la probabilité de routage d'un appel frauduleux via CUBE.

Les administrateurs doivent configurer CUBE pour acheminer uniquement les appels pour des plages de numéros de téléphone ou des URI SIP connues.

Reportez-vous au document suivant pour une explication plus détaillée des fonctions de routage d'appels 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

Atténuation des menaces CUBE

Gestion des paquets incorrecte

Par défaut, CUBE inspecte les paquets SIP et RTP afin de détecter les erreurs et d'abandonner le paquet.

Paquets RTP indésirables

Par défaut, IOS-XE CUBE effectue la validation du port source pour tous les flux RTP/RTCP en autorisant uniquement les connexions négociées via la signalisation offre/réponse SIP SDP et ne

peut pas être désactivée.

Vous pouvez les surveiller en vérifiant la commande suivante :

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

Pour l'interopérabilité avec CUCM, il est recommandé d'activer la diffusion multimédia bidirectionnelle via le service Cisco CallManager pour éviter que la musique d'attente ne soit abandonnée lorsqu'elle provient du port 4000.

Renforcement de la plage de ports RTP

Par défaut, IOS-XE utilise la plage de ports comprise entre 8000 et 48198. Cette plage peut être configurée sur une plage différente, par exemple de 16384 à 32768, à l'aide de la commande suivante :

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

Un administrateur peut également configurer des plages de ports RTP par plages d'adresses IPv4 et IPv6.

Cette configuration permet également à l'application VoIP de CUBE d'effectuer une gestion des paquets fantômes plus efficacement en ne dirigeant pas ces paquets vers le processus UDP au niveau du processeur du routeur, puisque les plages IP et de ports sont définies de manière statique. Cela peut aider à réduire le CPU élevé lors de la gestion d'un grand nombre de paquets RTP légitimes ou illégitimes en contournant le comportement de pointage du 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

Prévention des dénis de service (DOS)

Les fonctions de contrôle d'admission des appels peuvent être activées pour limiter les appels en fonction du nombre total d'appels, du processeur, de la mémoire et de la bande passante. En outre, des pics d'appels peuvent être détectés pour rejeter les appels et empêcher le déni de service.

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

Masquage d'adresse

Par défaut, CUBE remplace les adresses IP dans les en-têtes SIP tels que, mais sans s'y limiter, Via, Contact et From par sa propre adresse IP.

Il est possible de l'étendre aux en-têtes Refer-To, Referred-By, 3xx contact header, History-Info et Diversion en appliquant la commande voice service voip address-hide.

En outre, un nouvel ID d'appel est créé pour chaque adresse IP de limitation de branche d'appel qui peut être intégrée dans cette valeur d'en-tête.

Lorsqu'un nom d'hôte est requis à la place d'une adresse IP pour masquer l'adresse, la commande voice-class sip localhost dns : cube.cisco.com peut être configurée.

Confidentialité ID appelant

CUBE peut être configuré pour supprimer les valeurs Caller ID Name des en-têtes SIP avec la commande clid-strip name configurée sur n'importe quel terminal de numérotation dial-peer.

En outre, CUBE peut interagir et comprendre les en-têtes SIP Privacy tels que P-Preferred Identity (PPID), P-Asserted Identity (PAID), Privacy, P-Called Party Identity (PCPID), Remote-Party Identity (RPID). Pour plus d'informations, consultez le document suivant : 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

Authentification SIP Digest

Lors de l'enregistrement SIP par CUBE auprès d'un fournisseur de services ou lors d'un appel signalant des périphériques UAS en amont, il est possible de renvoyer un code d'état 401 ou 407 avec un champ d'en-tête WWW-Authenticate/Proxy-Authenticate applicable demandant à CUBE de s'authentifier. Au cours de cette connexion, CUBE prend en charge l'algorithme MD5 pour calculer la valeur du champ d'en-tête d'autorisation dans une requête suivante.

En-têtes SIP ou SDP non pris en charge

CUBE supprime les en-têtes SIP ou SDP non pris en charge qu'il ne comprend pas. Veillez à utiliser des commandes telles que pass-thru content sdp, pass-thru content unsupp ou pass-through headers unsupp pour vérifier les données qui transitent par CUBE.

Suppression ou modification des en-têtes SIP ou SDP

Lorsqu'un contrôle supplémentaire est requis, les profils SIP entrants ou sortants peuvent être configurés par un administrateur pour modifier ou supprimer de manière flexible un en-tête SIP ou un attribut SDP.

Reportez-vous aux documents suivants sur l'utilisation du profil 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

Autres fonctions de sécurité

Mots de passe chiffrés

CUBE requiert des mots de passe chiffrés pour la version 16.11 et les versions ultérieures pour chiffrer l'enregistrement SIP et les autres mots de passe IOS-XE dans la configuration en cours.

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

Listes d'accès

La fonctionnalité de liste de confiance fonctionne au niveau de la couche 7 dans l'application CUBE. Au moment où le paquet est abandonné en silence, le CUBE a déjà commencé à traiter le paquet.

Il peut être souhaitable de verrouiller les interfaces avec des listes d’accès de couche 3 ou 4 entrantes ou sortantes pour abandonner le paquet au point d’entrée du routeur.

Cela garantit que les cycles CPU de CUBE sont dépensés sur le trafic légitime. Les listes de contrôle d'accès, la liste de confiance IP et la validation du nom d'hôte fournissent une approche multicouche de la sécurité CUBE.

ZBFW (Zone-Based Firewall)

Cisco CUBE peut être configuré avec IOS-XE ZBFW pour fournir une inspection des applications et d'autres fonctions de sécurité.

Reportez-vous au Guide CUBE et ZBFW pour plus d'informations sur ce sujet :

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.