# 用來強化Cisco Unified Border Element(CUBE)企業裝置的思科指南

## 目錄

區域型防火牆(ZBFW)

# 簡介

本檔案將協助您保護和加固執行Cisco Unified Border Element(CUBE)Enterprise的Cisco IOS和IOS-XE裝置作用作業階段邊界控制器(SBC)。

# 必要條件

## 需求

本文件沒有特定需求。

## 採用元件

— 運行IOS-XE 17.10.1a的CUBE企業版。

附註：

並非本檔案所詳述的某些功能可能在舊版IOS-XE中無法使用。在可能的情況下，注意記錄何時引入或修改了命令或功能。

本檔案不適用於CUBE媒體代理、CUBE服務提供商、MGCP或SCCP閘道、Cisco SRST或ESRST閘道、H323閘道或其他類比/TDM語音閘道。

# 背景資訊

本檔案是Cisco IOS裝置加固指南新增內容。 因此，此文檔中的任何重複專案都不會在此文檔中重複。

# 通用標準(CC)和聯邦資訊標準(FIPS)

在CSR1000v或CAT8000v上使用IOS-XE 16.9+的Cisco virtual CUBE可以使用命令cc-mode命令在各種加密模組(例如傳輸層安全(TLS)和中的模組)上啟用通用標準(CC)和聯邦資訊標準(FIPS)認證實施。對於在硬體路由器上運行的CUBE，沒有相應的命令，但後續部分將提供手動啟用類似強化的方法。

來源： 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

# 傳輸層安全(TLS)和公鑰基礎架構(PKI)

本節將討論有關TLS和PKI的專案，這些專案可以增強這些協定以及安全會話初始協定(SIP)和安全即時協定(SRTP)操作提供的安全性。

## 使用TCP TLS和SRTP

預設情況下，CUBE將接受通過TCP、UDP或SIP TCP-TLS的入站SIP連線。如果未配置任何內容，TCP-TLS連線將失敗，而CUBE將接受並處理TCP和UDP。 對於出站連線，SIP將預設使用UDP連線，除非存在TCP或TCP-TLS命令。 同樣，CUBE將協商不安全的即時協定(RTP)會話。這兩種協定都為攻擊者提供了大量從未加密的SIP會話信令或媒體流中收集資料的機會。如果可能，建議使用SIP TLS保護SIP信令，使用SRTP保護媒體流。

請參閱SIP TLS配置和SRTP配置指南：

- 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

請記住，安全性的強弱取決於它是最薄弱的鏈路，並且應該通過CUBE在所有呼叫段上啟用SIP-TLS和SRTP。

其餘部分將新增到這些預設配置中，以提供其他安全功能：

## 禁用非安全SIP埠

回想上一節，其中詳細介紹了CUBE預設情況下將接受CUBE的入站TCP和UDP。一旦為所有呼叫段使用SIP TLS，可能需要禁用不安全的UDP和TCP SIP偵聽埠5060。

禁用後，可以使用show sip-ua status、show sip connections udp brief或show sip connections tcp brief確認CUBE不再在5060上偵聽入站TCP或UDP SIP連線。

<#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還可以配置為與IOS-XE VRF配合使用，以提供進一步的網路分段。

通過配置VRF並將啟用VRF的介面繫結到撥號對等體/租戶；CUBE將僅偵聽該IP、埠和VRF組合的入站連線。

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

## 實施TLS 1.2

在撰寫本文時，TLS 1.2是CUBE支援的TLS的最高版本。IOS-XE 16.9中禁用了TLS 1.0，但可以協商TLS 1.1。要進一步限制TLS握手期間的選項，管理員可以將CUBE Enterprise的唯一可用版本強製為TLS 1.2

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

## 實施TLS密碼

最好禁用會話中協商較弱的TLS密碼。從IOS-XE 17.3.1開始，管理員可以配置TLS配置檔案，使管理員能夠精確地定義TLS會話期間將提供的TLS密碼。在較舊版本的IOS-XE中，這是使用crypto signaling sip-ua命令上的strict-cipher或ecdsa-cipher postfix控制的。

請注意，您選擇的密碼應與協商採用CUBE的SIP TLS的對等裝置相容。請參閱所有適用的供應商文檔以確定所有裝置之間的最佳密碼。

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
!
```

所有其他版本

<#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
!
```

## 利用大型加密金鑰

建議將Cisco下一代加密標準用於TLS 1.2應用程式，編號為2048。以下命令可用於建立RSA金鑰以用於TLS會話。

label命令允許管理員在信任點上輕鬆指定這些金鑰，可匯出命令可確保必要時可使用以下命令匯出私有/公共金鑰對

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..]
```

## 利用證書頒發機構(CA)簽名的證書

為CUBE企業建立信任點和身份(ID)證書時，管理員應使用CA簽名證書代替自簽名證書。

CA憑證通常提供額外的安全機制，例如憑證撤銷清單(CRL)或線上憑證狀態通訊協定(OCSP)URL，可由裝置使用以確保憑證尚未撤銷。使用受信任的公共CA鏈可以簡化對等裝置上的信任關係配置，這些對等裝置可能具有對已知根CA的嵌入式信任或已經具有企業域的根CA信任。

此外，CA證書在基本約束中應包含CA標誌True，CUBE的身份證書應包含已啟用客戶端身份驗證的擴展金鑰使用引數。

下面顯示了使用下列方法的CUBE的根CA證書和ID證書示例：

**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..]
```

## 利用強雜湊

為CUBE的身份證書配置信任時，應選擇強雜湊演算法，如SHA256、SHA384或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
```

## 啟用證書吊銷清單(CRL)或聯機證書狀態協定(OCSP)檢查

預設情況下，IOS-XE信任將在crypto pki auth命令期間嘗試檢查證書中列出的CRL，稍後在TLS握手期間，IOS-XE還將基於收到的證書執行另一個CRL提取以確認證書仍然有效。CRL的方法可以是HTTP或LDAP，並且需要存在到CRL的連線才能成功。也就是說，需要提供DNS解析、從伺服器到IOS-XE路由器的TCP套接字和檔案下載，否則CRL檢查將失敗。同樣，可以將IOS-XE信任點配置為利用證書中AuthorityInfoAccess(AIA)標頭的OCSP值，該標頭通過HTTP對OCSP響應程式執行查詢，以檢查並執行類似的檢查。管理員可以通過在證書上提供靜態URL來覆蓋證書中的OCSP或CRL分發點(CDP)。此外，管理員還可以配置檢查CRL或OCSP的順序（假設兩者都存在）。

許多方法只是使用revocation-check none禁用撤銷檢查以簡化流程，但管理員這樣做會削弱安全性，並刪除IOS-XE的狀態檢查機制來檢查給定證書是否仍然有效。如果可能，管理員應利用OCSP或CRL對收到的證書執行狀態檢查。有關CRL或OCSP的詳細資訊，請檢視以下文檔：

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

CRL檢查

<#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
!
```

OCSP檢查

<#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
!
```

已訂購OCSP和CRL檢查

<#root>

```
! Check CRL if failure, check OCSP


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

## 啟用公用名(CN)和主體備用名(SAN)驗證

可以將CUBE配置為驗證證書的CN或SAN與session target dns: 命令中的主機名匹配。在IOS-XE 17.8+中，可以通過tls配置檔案配置TLS配置檔案。

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
```

請記住，客戶端/伺服器指定是指TLS握手中的對等裝置角色

進一步說明：

- cn-san validate server: CUBE將對收到的出站TLS連線對等服務器證書執行主機名驗證，其中

CUBE是客戶端角色。

- cn-san validate client: CUBE將對接收的對等客戶端證書執行主機名驗證，以入站TLS連線，其中CUBE是伺服器角色。
- cn-san validate bidirection：在TLS握手期間為兩個對等角色啟用主機名驗證。

使用cn-san validate client命令（或雙向）時，必須配置要檢查的SAN，因為會話目標只檢查出站連線和cn-san validate server。

客戶端主機名驗證：

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

伺服器主機名驗證：

```
!
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
!
```

17.8.1之前的版本

注意：通過此方法只能進行伺服器主機名驗證。

<#root>

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

**cn-san-validate server**

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

還可以將CUBE配置為使用TLS握手中的CUBE的FQDN主機名向對等裝置傳送伺服器名稱指示(SNI)TLS 1.2擴展，以方便其主機名驗證工作。

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

有關CUBE的相互TLS的說明：

- 預設情況下，當CUBE充當TLS伺服器（讀取入站TLS連線）時，它將始終請求客戶端證書。沒有禁用此行為的配置。
- 當CUBE充當TLS客戶端並啟動出站TLS連線時，相互TLS取決於充當TLS伺服器的對等裝置。在這種情況下，對等裝置可能無法從CUBE請求客戶端證書。
- 在這兩種情況下，證書鏈CUBE將傳送的證書由TLS配置檔案或crypto signaling命令中定義的信任點控制。

<#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
!
```

## 將遠端TLS連線對映到特定信任點

使用crypto signaling default sip-ua命令ALL 入站TLS連線通過tls-profile或單個後修復命令對映到這些配置。此外，在執行證書驗證時，還會檢查所有可用的信任點。

可能需要為基於IP地址的特定對等裝置建立特定TLS配置檔案配置，以確保將您定義的安全引數準確地應用於該TLS會話。為此，請使用crypto signaling remote-addr命令定義IPv4或IPv6子網以對映

到tls-profile或postfix命令集。 您還可以通過client-vtp)命令直接對映驗證信任點，以明確鎖定哪些信任點用於驗證對等證書。

以下命令彙總了迄今為止討論的大多數專案：

```
!
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
!
```

對於較舊版本，可以按如下方式完成：

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

從17.8開始，您還可以針對每個語音類租戶配置tls配置檔案和每租戶偵聽埠，以在給定的偵聽埠上提供進一步分段選項。

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

## 實施嚴格SRTP

在CUBE Enterprise上啟用SRTP時，預設操作是禁止回退到RTP。

如果可能，在所有呼叫段上使用SRTP，但預設情況下，CUBE將根據需要執行RTP-SRTP。

請注意，從16.11+開始，CUBE不會在調試中記錄SRTP金鑰

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

## Trim不安全SRTP密碼

預設情況下，建立服務時，所有SRTP密碼均由CUBE傳送。管理員可以使用IOS-XE 16.5+中的語音類srtp-crypto命令，將密碼縮減為更安全的密碼，例如下一代AEAD密碼套件。

此配置還可以更改當CUBE選擇SRTP密碼並建立多個可用選項的某個服務的響應時使用的預設首選項。

注意：某些舊思科裝置或對等裝置可能不支援AEAD密碼。在測試密碼套件時，請參閱所有適用的文檔。

```
<#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
!
```

# 禁用其他未使用的VoIP協定

如果H323、MGCP、SCCP、STCAPP、CME和SRST未在此網關上使用，則值得移除配置以強化CUBE。

禁用H323並僅允許SIP到SIP呼叫

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

禁用MGCP、SCCP、STCAPP、SIP和SCCP SRST。

注意：其中某些命令將刪除所有其他配置，確保在完全刪除這些配置之前未使用功能。

<#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
```

# 呼叫路由和話費欺詐

## 允許來自受信任IP的連線

預設情況下，CUBE將信任從撥號對等會話目標和語音類伺服器組配置上配置的IPv4和IPv6地址中配置的IPv6入站連線。

要新增其他IP地址，請使用通過語音服務voip配置的ip address trusted list命令。

通過前面討論的CN/SAN驗證功能在SIP TLS旁配置客戶端/伺服器主機名驗證時，成功的CN/SAN驗證將繞過IP地址可信清單檢查。

避免使用no ip address trusted authenticate，這將使CUBE接受ANY入站連線。

```
!
voice service voip
 ip address trusted authenticate

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

使用show ip address trusted list檢視IP地址檢查的狀態以及源自其他配置的所有靜態和動態信任清單定義。

請注意，當撥號對等體關閉或保持連線檢查失敗後設定為關閉狀態時，從撥號對等體/伺服器組派生的動態值將從信任清單中刪除。

預設情況下，當入站呼叫未通過IP受信任清單檢查時，會以靜默方式丟棄該呼叫，但可以使用no silent-discard untrusted voice service voip > sip命令覆蓋該呼叫，以將錯誤傳送回發件人。但是，通過傳送響應，攻擊者可以利用此資訊指示裝置實際上正在偵聽SIP流量並加大攻擊力度。因此，靜默丟棄是處理IP受信任清單丟棄的首選方法。

## 避免通用撥號對等路由

使用destination-pattern等通用「捕獲所有」目標模式，可以增加通過CUBE路由欺詐呼叫的可能性。

管理員應將CUBE配置為僅路由已知電話號碼範圍或SIP URI的呼叫。

有關CUBE呼叫路由功能的詳細說明，請參閱以下文檔：

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

# CUBE威脅緩解

## 錯誤資料包處理

預設情況下，CUBE將檢查SIP和RTP資料包以檢查是否存在錯誤並丟棄該資料包。

## 欺詐RTP資料包

預設情況下，IOS-XE CUBE僅允許通過SIP SDP提供/應答信令協商的連線，從而對所有RTP/RTCP流執行源埠驗證，並且不能禁用。

可通過檢查以下命令監控這些情況：

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

對於與CUCM的互操作，建議通過Cisco CallManager服務啟用雙工媒體流，以避免源自埠4000的保留音樂被丟棄。

## RTP連線埠範圍強化

預設情況下，IOS-XE使用的埠範圍是8000到48198。可通過以下命令將此範圍配置到不同的範圍，例如16384到32768:

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

管理員還可以根據IPv4和IPv6地址範圍配置RTP埠範圍。

此配置還使CUBE的VoIP應用能夠更有效地執行虛擬資料包處理，因為靜態定義了IP和埠範圍，所以不會將這些資料包傳送到路由器CPU的UDP進程。通過繞過CPU分流行為，這有助於在處理大量合法或非法的RTP資料包時降低高CPU使用率。

```
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

## 拒絕服務(DOS)預防

可以啟用呼叫准入控制功能，以根據呼叫總數、CPU、記憶體和頻寬限制呼叫。此外，還可以檢測呼叫峰值，以拒絕呼叫並防止拒絕服務。

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

## 地址隱藏

預設情況下，CUBE將用自己的IP地址替換SIP報頭中的IP地址，例如，但不限於Via、Contact和From。

這可以通過應用voice service voip命令address-hiding擴展到Refer-To、Referred-By、3xx contact header、History-Info和Distribution header。

此外，會為每個可嵌入在此報頭值中的呼叫段緩解IP地址建立新的呼叫ID。

如果為了地址隱藏需要主機名來代替IP地址，則可以配置命令voice-class sip localhost dns:cube.cisco.com。

## 來電者ID隱私

可以將CUBE配置為使用在任何撥號對等體上配置的clid-strip name 命令從SIP報頭中刪除呼叫者ID名稱值。

此外，CUBE可以互通和理解SIP隱私標頭，例如P-Preferred Identity(PPID)、P-Asserted Identity(PAID)、Privacy、P-Called Party Identity(PCPID)、Remote-Party Identity(RPID)。有關詳細資訊，請參閱以下文檔：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

## SIP摘要式驗證

在由CUBE向服務提供商進行SIP註冊期間，或在呼叫信令期間，上游UAS裝置可返回401或407狀態代碼，該狀態代碼帶有可應用的WWW-Authenticate/Proxy-Authenticate標頭欄位，以挑戰CUBE進行身份驗證。在此握手期間，CUBE支援MD5演算法，用於計運算元級請求中的授權報頭欄位值。

### 不支援的SIP報頭或SDP

CUBE將剝離其無法理解的不受支援的SIP報頭或SDP。當使用諸如傳遞內容sdp、傳遞內容unsupp或傳遞標頭unsupp之類的命令時，應確保哪些資料通過CUBE。

### 刪除或修改SIP報頭或SDP

需要額外控制時，管理員可以配置入站或出站SIP配置檔案來靈活修改或完全丟棄SIP報頭或SDP屬性。

請參閱以下有關SIP配置檔案用法的文檔：

- 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

## 其他安全功能

### 加密密碼

CUBE需要16.11及更高版本的加密密碼，才能加密運行配置中的SIP註冊和其他IOS-XE密碼。

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

### 存取清單

可信清單功能在CUBE應用程式的第7層運行。在資料包被靜默丟棄時，CUBE已開始處理資料包。

最好使用入站或出站第3層或第4層訪問清單來鎖定介面，以便在路由器的入口點丟棄資料包。

這可確保來自CUBE的CPU週期用於合法流量。ACL以及IP可信清單和主機名驗證為CUBE安全提供了一種分層方法。

### 區域型防火牆(ZBFW)

Cisco CUBE可與IOS-XE ZBFW一起配置，以提供應用檢查和其他安全功能。

有關此主題的詳細資訊，請參閱CUBE和ZBFW指南：

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。