思科加强思科统一边界要素(CUBE)企业设备指南

目录

简介

本文档将帮助您保护和加固运行Cisco Unified Border Element(CUBE)Enterprise的Cisco IOS和IOS-XE设备充当会话边界控制器(SBC)。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

— 运行IOS-XE 17.10.1a的CUBE企业版。

注意：

并非本文档中详述的某些功能在较旧的IOS-XE版本中可能不可用。尽可能注意记录何时引入或修改了命令或功能。

本文档不适用于CUBE媒体代理、CUBE服务提供商、MGCP或SCCP网关、Cisco SRST或ESRST网关、H323网关或其他模拟/TDM语音网关。

背景信息

本文档是对Cisco IOS设备加固指南的补充。 因此，本文档中不会重复该文档中的任何重复项目。

通用标准(CC)和联邦信息标准(FIPS)

在CSR1000v或CAT8000v上使用IOS-XE 16.9+的Cisco virtual CUBE可以使用命令cc-mode命令在各种加密模块(如传输层安全(TLS)和中的模块)上启用通用标准(CC)和联邦信息标准(FIPS)认证实施。硬件路由器上运行的CUBE没有等效命令，但后续部分将提供手动启用类似强化的方法。

来源：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

传输层安全(TLS)和公共密钥基础设施(PKI)

本节将讨论TLS和PKI的相关项目，它们可以增强这些协议提供的安全性，同时还可以增强安全会话初始协议(SIP)和安全实时协议(SRTP)操作。

使用TCP TLS和SRTP

默认情况下，CUBE将接受通过TCP、UDP或SIP TCP-TLS的入站SIP连接。当未配置任何内容时，TCP-TLS连接将失败，CUBE将接受并处理TCP和UDP。 对于出站连接，SIP将默认使用UDP连

接，除非存在TCP或TCP-TLS命令。 同样，CUBE将协商不安全的实时协议(RTP)会话。这两种协议都为攻击者提供了从未加密的SIP会话信令或媒体流中收集数据的充足机会。如果可能，建议使用SIP TLS保护SIP信令，使用SRTP保护媒体流。

请参阅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

请记住，安全功能仅与其最薄弱的链路一样强大，并且应通过CUBE在所有呼叫段上启用SIP-TLS和SRTP。

其余部分将添加到这些默认配置中，以提供其他安全功能：

禁用非安全SIP端口

请回忆上一节，该节详细说明了CUBE默认情况下将接受CUBE的入站TCP和UDP。将SIP TLS用于所有呼叫段后，可能需要禁用不安全的UDP和TCP SIP侦听端口5060。

禁用后，您可以使用show sip-ua status、show sip connections udp brief或show sip connections tcp brief确认CUBE在5060上不再侦听入站TCP或UDP SIP连接。

<#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还可以配置为与IOS-XE VRF配合使用，以提供进一步的网络分段。

通过配置VRF并将启用VRF的接口绑定到拨号对等体/租户；CUBE将仅侦听该IP、端口、VRF组合的入站连接。

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

实施TLS 1.2

在撰写本文档时，TLS 1.2是CUBE支持的TLS的最高版本。IOS-XE 16.9中禁用了TLS 1.0，但可以协商TLS 1.1。为了在TLS握手期间进一步限制选项，管理员可以强制将CUBE企业版的唯一可用版本设置为TLS 1.2

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

实施TLS密码

最好禁用会话中协商较弱的TLS密码。从IOS-XE 17.3.1开始，管理员可以配置TLS配置文件，使管理员能够精确定义在TLS会话期间将提供哪些TLS密码。在IOS-XE的早期版本中，使用crypto signaling sip-ua命令上的strict-cipher或ecdsa-cipher postfix控制此功能。

请注意，您选择的密码应与协商采用CUBE的SIP TLS的对等设备兼容。请参阅所有适用的供应商文档，确定所有设备之间的最佳密码。

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
!
```

使用大型加密密钥

建议将Cisco下一代加密标准用于TLS 1.2应用程序，编号为2048。以下命令可用于创建RSA密钥以用于TLS会话。

label命令允许管理员在信任点上轻松指定这些密钥，可导出命令可确保必要时可使用以下命令导出专用/公共密钥对：

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..]
```

使用证书颁发机构(CA)签名证书

为CUBE企业创建信任点和身份(ID)证书时，管理员应使用CA签名证书代替自签名证书。

CA证书通常提供其他安全机制，例如证书撤销列表(CRL)或在线证书状态协议(OCSP)URL，设备可使用这些URL来确保证书未被撤销。使用受信任的公共CA链可以简化对等设备上的信任关系配置，这些对等设备可能具有已知根CA的嵌入式信任或已经具有企业域的根CA信任。

此外，CA证书应在基本约束中包含CA标志True，并且CUBE的身份证书应包含已启用客户端身份验证的扩展密钥使用参数。

CUBE的样本根CA证书和ID证书如下所示：

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..]
```

利用强散列

为CUBE的身份证书配置信任时，应选择强散列算法，例如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
```

启用证书撤销列表(CRL)或在线证书状态协议(OCSP)检查

默认情况下，IOS-XE信任点将在crypto pki auth命令期间尝试检查证书中列出的CRL，稍后在TLS握手期间，IOS-XE还将基于收到的证书执行另一个CRL获取，以确认证书仍然有效。CRL的方法可以是HTTP或LDAP，并且需要存在与CRL的连接才能成功。也就是说，DNS解析、TCP套接字和文件从服务器下载到IOS-XE路由器需要可用，否则CRL检查将失败。同样，可以将IOS-XE信任点配置为使用证书中AuthorityInfoAccess(AIA)信头的OCSP值，该信头通过HTTP对OCSP响应器执行查询，以检查并执行类似检查。管理员可以通过在证书上提供静态URL来覆盖证书中的OCSP或CRL分发点(CDP)。此外，管理员还可以配置检查CRL或OCSP的顺序（假设两者都存在）。

许多方法只是使用revocation-check none禁用撤销检查以简化流程，但管理员这样做会削弱安全性，并删除IOS-XE的状态检查机制，以检查给定证书是否仍然有效。如果可能，管理员应利用OCSP或CRL对收到的证书执行状态检查。有关CRL或OCSP的详细信息，请查看以下文档：

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检查

<#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检查

<#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
!
```

已订购的OCSP和CRL检查

<#root>

```
! Check CRL if failure, check OCSP
```

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

启用公用名(CN)和主题备用名(SAN)验证

可以配置CUBE以验证证书的CN或SAN与session target dns:命令中的主机名匹配。在IOS-XE 17.8+中，可以通过tls配置文件配置TLS配置文件。

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
```

请记住，客户端/服务器指定是指TLS握手中的对等设备角色

进一步说明：

- cn-san validate server:CUBE将对接收的对等服务器证书执行主机名验证，其中CUBE是客户

端角色。

- cn-san validate client:CUBE将对接入的TLS连接（其中CUBE是服务器角色）的已收到的对等客户端证书执行主机名验证。
- cn-san validate bidirection:在TLS握手期间为两个对等角色启用主机名验证。

使用cn-san validate client命令（或双向）时，必须配置要检查的SAN，因为会话目标只检查出站连接和cn-san validate server。

客户端主机名验证：

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

服务器主机名验证：

```
!
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：通过此方法只能进行服务器主机名验证。

<#root>

```
!
sip-ua
 crypto signaling default trustpoint TEST
cn-san-validate server

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

还可以配置CUBE以将服务器名称指示(SNI)TLS 1.2扩展以及TLS握手中的CUBE FQDN主机名发送到对等设备，以便进行主机名验证工作。

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

关于CUBE的相互TLS的说明：

- 默认情况下，当CUBE充当TLS服务器（读取入站TLS连接）时，它将始终请求客户端证书。没有禁用此行为的配置。
- 当CUBE充当TLS客户端并启动出站TLS连接时，相互TLS取决于充当TLS服务器的对等设备。在这种情况下，对等设备可能无法从CUBE请求客户端证书。
- 在这两种情况下，证书链CUBE将发送由TLS配置文件或crypto signaling命令中定义的信任点控制。

<#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
!
```

将远程TLS连接映射到特定信任点

使用crypto signaling default sip-ua命令时，所有入站TLS连接通过tls-profile或单个后修复命令映射到这些配置。此外，在执行证书验证时，还会检查所有可用的信任点。

可能需要基于IP地址为特定对等设备创建特定TLS配置文件配置，以确保您定义的安全参数完全应用于该TLS会话。为此，请使用crypto signaling remote-addr命令定义IPv4或IPv6子网以映射到tls-

profile或postfix命令集。 您还可以通过client-vtp)命令直接映射验证信任点，以准确锁定用于验证对等证书的信任点。

以下命令汇总了到目前为止讨论的大多数项目：

```
!
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
!
```

对于较旧版本，可以按如下方式完成此操作：

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

从17.8开始，您还可以按语音类租户配置tls配置文件和每租户侦听端口，以在给定侦听端口上提供进一步分段选项。

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

实施严格SRTP

在CUBE Enterprise上启用SRTP时，默认操作是禁止回退到RTP。

如果可能，在所有呼叫段上使用SRTP，但默认情况下，CUBE将根据需要执行RTP-SRTP。

请注意，从16.11+开始，CUBE不会在调试中记录SRTP密钥

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

修剪不安全的SRTP密码

默认情况下，创建服务时，所有SRTP密码均由CUBE发送。管理员可以在IOS-XE 16.5+中使用voice class srtp-crypto命令，将密码缩减为更安全的密码，例如下一代AEAD密码套件。

此配置还可以更改当CUBE选择SRTP密码并创建具有多个可用选项的某个服务的应答时使用的默认首选项。

注意：某些较早的思科设备或对等设备可能不支持AEAD密码。触发密码套件时，请参阅所有适用的文档。

```
<#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协议

如果H323、MGCP、SCCP、STCAPP、CME和SRST未在此网关上使用，则有必要删除配置，以强化CUBE。

禁用H323并仅允许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：其中一些命令将删除所有其他配置，确保在完全删除功能之前没有使用功能。

<#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
```

呼叫路由和话费欺诈

允许来自受信任IP的连接

默认情况下，CUBE将信任从拨号对等体会话目标和语音类服务器组配置上配置的IPv4和IPv6地址进行入站连接。

要添加其他IP地址，请使用通过语音服务voip配置的ip address trusted list命令。

通过前面讨论的CN/SAN验证功能在SIP TLS旁配置客户端/服务器主机名验证时，成功的CN/SAN验证将绕过IP地址受信任列表检查。

避免使用no ip address trusted authenticate，这将使CUBE能够接受ANY入站连接。

```
!
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查看IP地址检查的状态以及从其他配置派生的所有静态和动态信任列表定义。

请注意，当拨号对等体关闭或保持连接检查失败后设置为关闭状态时，从拨号对等体/服务器组派生的动态值会从受信任列表中删除。

默认情况下，当入站呼叫未通过IP受信任列表时，会将其以静默方式丢弃，但可以使用no silent-discard untrusted voice service voip > sip命令覆盖此情况，以便将错误发送回发件人。但是，通过发送响应，攻击者可能会使用此信息来表示设备实际上正在侦听SIP流量并加大攻击力度。因此，静默丢弃是处理IP受信任列表丢弃的首选方法。

避免通用拨号对等体路由

使用destination-pattern等通用“捕获所有”目标模式，可以增加通过CUBE路由欺诈呼叫的可能性。

管理员应将CUBE配置为仅路由已知电话号码范围或SIP URI的呼叫。

有关CUBE呼叫路由功能的详细说明，请参阅以下文档：

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威胁缓解

格式错误的数据包处理

默认情况下，CUBE将检查SIP和RTP数据包以检查错误并丢弃数据包。

非法RTP数据包

默认情况下，IOS-XE CUBE仅允许通过SIP SDP提供/应答信令协商的连接，从而对所有RTP/RTCP流执行源端口验证，且不能禁用。

可以通过检查以下命令监控这些设备：

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

对于与CUCM的互操作，建议通过Cisco CallManager服务启用双工媒体流，以避免从端口4000发出呼叫时丢弃保留音乐。

RTP端口范围强化

默认情况下，IOS-XE使用8000到48198的端口范围。可通过以下命令将此范围配置为不同的范围，例如16384到32768:

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

管理员还可以根据IPv4和IPv6地址范围配置RTP端口范围。

此配置还使CUBE的VoIP应用能够更高效地执行虚拟数据包处理，因为静态定义了IP和端口范围，所以不会将这些数据包传送到路由器CPU上的UDP进程。当处理大量合法或非法的RTP数据包时，通过绕过CPU传送行为，这有助于降低高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

拒绝服务(DOS)预防

可以启用呼叫准入控制功能，以根据呼叫总数、CPU、内存和带宽限制呼叫。此外，还可以检测呼叫尖峰，以拒绝呼叫并防止拒绝服务。

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

地址隐藏

默认情况下，CUBE将使用自己的IP地址替换SIP报头中的IP地址，例如，但不限于Via、Contact和From。

通过应用voice service voip命令address-hiding，可以将此扩展到Refer-To、Referred-By、3xx contact header、History-Info和Distribution header。

此外，会为每个可嵌入在此报头值中的呼叫段缓解IP地址创建新的呼叫ID。

如果需要主机名来代替IP地址才能隐藏地址，可以配置命令voice-class sip localhost dns:cube.cisco.com。

呼叫方ID隐私

CUBE可以配置为使用在任何拨号对等体上配置的clid-strip name命令从SIP报头中删除呼叫方ID名称值。

此外，CUBE可以交互和理解SIP隐私头，例如P-Preferred Identity(PPID)、P-Asserted Identity(PAID)、Privacy、P-Called Party Identity(PCPID)、Remote-Party Identity(RPID)。有关详细信息，请参阅以下文档：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摘要身份验证

在由CUBE向服务提供商进行SIP注册期间，或在呼叫信令期间，上游UAS设备可返回401或407状态代码，该状态代码带有用于挑战CUBE进行身份验证的适用的WWW-Authenticate/Proxy-Authenticate报头字段。在此握手期间，CUBE支持MD5算法，用于计算子请求中的授权报头字段值。

不支持的SIP报头或SDP

CUBE将删除不支持的SIP报头或它无法理解的SDP。当使用诸如传递内容sdp、传递内容unsupp或传递标头unsupp之类的命令时，应小心谨慎，以确保哪些数据通过CUBE。

删除或修改SIP报头或SDP

需要额外控制时，入站或出站SIP配置文件可由管理员配置，以灵活修改或完全丢弃SIP报头或SDP属性。

请参阅以下有关SIP配置文件用法的文档：

- 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

加密密码

CUBE需要16.11及更高版本的加密密码，才能在运行配置中加密SIP注册和其他IOS-XE密码。

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

访问列表

可信列表功能在CUBE应用中的第7层运行。当以静默方式丢弃数据包时，CUBE已开始处理数据包。

可能需要锁定具有入站或出站第3层或第4层访问列表的接口，以便在路由器的入口点丢弃数据包。

这样可以确保来自CUBE的CPU周期花费在合法流量上。ACL以及IP可信列表和主机名验证为CUBE安全提供了一种分层方法。

基于区域的防火墙(ZBFW)

Cisco CUBE可与IOS-XE ZBFW一起配置，以提供应用检测和其他安全功能。

有关此主题的详细信息，请参阅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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。