Cisco Unified Border Element(CUBE)エンタープライズデバイスの強化に関するシスコガイド

内容

概要

このドキュメントでは、Cisco Unified Border Element(CUBE)Enterpriseを実行するセッションボーダーコントローラ(SBC)を実行するCisco IOSおよびIOS XEデバイスのセキュリティ保護とセキュリティ強化について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

- IOS-XE 17.10.1aを実行するCUBE Enterprise

注：

このドキュメントで説明する一部の機能は、古いIOS-XEバージョンでは使用できない可能性があります。可能であれば、コマンドや機能が導入または変更された際に注意を払って文書化してください。

このドキュメントは、CUBEメディアプロキシ、CUBEサービスプロバイダー、MGCPまたはSCCPゲートウェイ、Cisco SRSTまたはESRSTゲートウェイ、H323ゲートウェイ、またはその他のアナログ/TDM音声ゲートウェイには適用されません。

背景説明

このドキュメントは、『Cisco IOSデバイスのセキュリティ強化に関するガイド』に記載されている内容の補足として役立ちます。 したがって、そのドキュメントから重複するアイテムは、このドキュメントでは複製されません。

共通基準(CC)および連邦情報標準(FIPS)

CSR1000vまたはCAT8000v上のIOS-XE 16.9+を使用するCisco仮想CUBEでは、コマンドcc-modeを使用して、Transport Layer Security(TLS)やなどのさまざまな暗号化モジュールでCommon Criteria(CC)およびFederal Information Standards(FIPS)認証適用を有効にできます。ハードウェアルータで実行するCUBEに対応するコマンドはありませんが、以降のセクションでは、同様の強化を手動で有効にする方法について説明します。

出典：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

Transport Layer Security(TLS)およびPublic Key

Infrastructure(PKI)

このセクションでは、Secure Session Initial Protocol(SIP)およびSecure Real Time Protocol(SRTP)の動作に加えて、これらのプロトコルによって提供されるセキュリティを強化できるTLSおよびPKIに関する項目について説明します。

TCP TLSおよびSRTPの使用

デフォルトでは、CUBEはTCP、UDP、またはSIP TCP-TLS経由の着信SIP接続を受け入れます。何も設定されていない場合はTCP-TLS接続が失敗しますが、TCPとUDPはCUBEによって受け入れられ、処理されます。 発信接続では、TCPまたはTCP-TLSコマンドが存在しない限り、SIPはデフォルトでUDP接続を使用します。 同様に、CUBEはセキュアでないReal Time Protocol(RTP)セッションをネゴシエートします。これらのプロトコルはどちらも、攻撃者が暗号化されていないSIPセッションシグナリングまたはメディアストリームからデータを収集する機会を十分に提供します。可能な場合は、SIP TLSでSIPシグナリングを保護し、SRTPでメディアストリームを保護することをお勧めします。

詳細については、『SIP TLS設定およびSRTP設定ガイド：

- 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

セキュリティは最も弱いリンクと同程度に強力であり、SIP-TLSとSRTPはCUBEを介してすべてのコールレッグで有効にする必要があることに注意してください。

その他のセクションは、追加のセキュリティ機能を提供するために、次のデフォルト設定に追加されます。

非セキュアSIPポートの無効化

前の項で、CUBEがデフォルトでCUBEの着信TCPおよびUDPを受け入れることを説明しました。すべてのコールレッグでSIP TLSが使用されている場合は、セキュアでないUDPとTCPのSIPリスニングポート5060を無効にすることが望ましい場合があります。

ディセーブルにした後は、show sip-ua status、show sip connections udp brief、またはshow sip connections tcp briefを使用して、CUBEが5060で着信TCPまたはUDP SIP接続をリッスンしていないことを確認します。

<#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は、IOS-XE VRFと連携して動作するように設定して、さらにネットワークをセグメント化することもできます。

VRFを設定し、VRF対応インターフェイスをダイヤルピア/テナントにバインドすることで、

CUBEはそのIP、ポート、VRFの組み合わせの着信接続のみをリッスンします。

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

TLS 1.2の適用

このドキュメントの作成時点では、TLS 1.2がCUBEでサポートされているTLSの最新バージョンです。IOS-XE 16.9ではTLS 1.0が無効になっていますが、TLS 1.1がネゴシエートされる場合があります。TLSハンドシェイク中にオプションをさらに制限するために、管理者はCUBE Enterpriseで使用可能な唯一のバージョンをTLS 1.2に強制できます

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

TLS暗号の適用

弱いTLS暗号がセッションでネゴシエートされないようにすることが望ましい場合があります。IOS-XE 17.3.1以降、管理者はTLSプロファイルを設定できます。これにより、管理者はTLSセッション中にどのTLS暗号を提供するかを正確に定義できます。古いバージョンのIOS XEでは、crypto signaling sip-uaコマンドのstrict-cipherまたはecdsa-cipherポストフィックスを使用してこれを制御していました。

選択する暗号は、CUBEでSIP TLSをネゴシエートするピアデバイスと互換性がある必要があります。すべてのデバイス間で最適な暗号を決定するには、該当するすべてのベンダーのマニュアルを参照してください。

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
!
```

その他すべてのバージョン

<#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
!
```

サイズの大きい暗号キーを使用する

Cisco Next Generation Cryptography standards(NGC)では、TLS 1.2アプリケーションでの使用を2048年に推奨しています。次のコマンドを使用して、TLSセッションで使用するRSAキーを作成できます。

labelコマンドを使用すると、管理者はトラストポイントでこれらのキーを簡単に指定できます。exportableコマンドを使用すると、必要に応じて、次のようなコマンドを使用してプライベート/パブリックキーペアをエクスポートできます

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..]
```

認証局(CA)署名付き証明書の使用

管理者は、CUBEエンタープライズのトラストポイントおよびID(ID)証明書を作成する際に、自己署名証明書の代わりにCA署名証明書を使用する必要があります。

CA証明書には通常、証明書失効リスト(CRL)やオンライン証明書ステータスプロトコル(OCSP)URLなどの追加のセキュリティメカニズムが備わっており、デバイスはこれを使用して証明書が失効していないことを確認できます。信頼されたパブリックCAチェーンを使用すると、既知のルートCAに対する信頼が埋め込まれているか、エンタープライズドメインに対するルートCAの信頼が既にあるピアデバイス上の信頼関係の構成が容易になります。

さらに、CA証明書にはBasic ConstraintsでCA Flag of Trueが含まれている必要があり、CUBEのID証明書にはClient Auth enabledのExtended Key Usageパラメータが含まれている必要があります。

次に、CUBEのルートCA証明書とID証明書の例を示します。

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..]
```

強力なハッシュを利用する

CUBEのID証明書のトラストポイントを設定する場合は、SHA256、SHA384、SHA512などの強力なハッシュアルゴリズムを選択する必要があります。

```
<#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
```

証明書失効リスト(CRL)またはオンライン証明書ステータスプロトコル(OCSP)チェックを有効にする

デフォルトでは、IOS-XEトラストポイントはcrypto pki authコマンド中に証明書内にリストされているCRLをチェックしようとします。その後のTLSハンドシェイク中に、IOS-XEは受信した証明書に基づいて別のCRLフェッチを実行し、証明書がまだ有効であることを確認します。CRLの方式はHTTPまたはLDAPのいずれかであり、これが成功するにはCRLへの接続が存在する必要があります。つまり、サーバからIOS-XEルータへのDNS解決、TCPソケット、およびファイルのダウンロードが可能である必要があります。そうしないと、CRLチェックが失敗します。同様に、IOS-XEトラストポイントは、証明書内のAuthorityInfoAccess(AIA)ヘッダーからのOCSP値を利用するように設定できます。このヘッダーは、HTTP経由でOCSPレスポンダにクエリを実行して、同様のチェックを実行します。管理者は、証明書に静的URLを指定することで、証明書内のOCSPまたはCRL配布ポイント(CDP)を上書きできます。さらに、CRLとOCSPの両方が存在することを前提に、CRLとOCSPのチェック順序を設定することもできます。

多くの場合、プロセスを簡素化するためにrevocation-check noneを使用して失効チェックを無効にしますが、その際に管理者はセキュリティを弱め、特定の証明書がまだ有効であるかどうかをステートフルチェックするIOS-XEのメカニズムを削除します。可能であれば、管理者はOCSPま

たはCRLを利用して、受信した証明書のステートフルチェックを実行する必要があります。
CRLまたはOCSPの詳細については、次の文書を参照してください。

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チェック

<#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チェック

<#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
!
```

順序付けされたOCSPとCRLのチェック

<#root>

```
! Check CRL if failure, check OCSP


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

共通名(CN)とサブジェクトの別名(SAN)の確認を有効にする

CUBEは、証明書のCNまたはSANがsession target dns:コマンドからのホスト名と一致することを確認するように設定できます。IOS-XE 17.8+では、TLSプロファイルはtlsプロファイルを使用して設定できます。

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
```

クライアント/サーバの指定は、TLSハンドシェイクのピアデバイスのロールを参照することに注意してください

さらに詳しく説明するには、次のようにします。

- cn-san validate server:CUBEは、CUBEがクライアントロールである発信TLS接続に対して、受信したピアサーバ証明書のホスト名検証を実行します。
- cn-san validate client:CUBEは、受信したピアクライアント証明書のホスト名検証をインバウンドTLS接続に対して実行します。ここで、CUBEはサーバロールです。
- cn-san validate bidirection:TLSハンドシェイク中に両方のピアロールのホスト名の検証を有効にします。

cn-san validate clientコマンド（または双方向）を使用する場合、チェック対象のSANを設定する必要があります。これは、セッションターゲットが発信接続とcn-san validateサーバに対しての

みチェックされるためです。

クライアントホスト名の検証：

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

サーバホスト名の検証：

```
!
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 よりも前

注：この方法では、サーバホスト名の検証のみが可能です。

<#root>

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

cn-san-validate server

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

CUBEは、TLSハンドシェイク内でCUBEのFQDNホスト名を含むサーバ名表示(SNI)TLS 1.2拡張をピアデバイスに送信するように設定して、ホスト名の検証作業を容易にすることもできます。

```
!
```

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

CUBEの相互TLSに関する注記：

- デフォルトでは、CUBEがTLSサーバとして機能している場合（着信TLS接続の読み取り）、常にクライアント証明書を要求します。この動作を無効にする設定はありません。
- CUBEがTLSクライアントとして機能し、アウトバウンドTLS接続を開始する場合、相互TLSはTLSサーバとして機能するピアデバイスに依存します。このシナリオでは、ピアデバイスはCUBEからクライアント証明書を要求しない場合があります。
- どちらのシナリオでも、証明書チェーンCUBEが送信する証明書チェーンは、TLSプロファイルまたはcrypto signalingコマンドで定義されたトラストポイントによって制御されます。

<#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
!
```

特定のトラストポイントへのリモートTLS接続のマッピング

crypto signaling default sip-uaコマンドを使用すると、すべての着信TLS接続がtls-profileまたは個々の事後修正コマンドによって、これらの設定にマッピングされます。さらに、証明書の検証を実行するときに、使用可能なすべてのトラストポイントがチェックされます。

IPアドレスに基づいて特定のピアデバイス用の特定のTLSプロファイル設定を作成し、定義したセキュリティパラメータがそのTLSセッションに正確に適用されるようにすることが望ましい場合があります。これを行うには、crypto signaling remote-addrコマンドを使用して、tls-profileまたはpostfixコマンドのセットにマッピングするIPv4またはIPv6サブネットを定義します。 client-vtp)コマンドを使用して検証トラストポイントを直接マッピングし、ピア証明書の検証に使用するトラストポイントを正確にロックダウンすることもできます。

次のコマンドは、これまでに説明したほとんどの項目をまとめたものです。

```
!
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
!
```

古いバージョンの場合は、次のように実行できます。

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

17.8以降では、音声クラステナントごとにTLSプロファイルおよびテナントごとのリスニングポートを設定して、特定のリスニングポート上でさらにセグメンテーションオプションを提供することもできます。

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

厳密なSRTPの適用

CUBE EnterpriseでSRTPを有効にすると、デフォルトの操作ではRTPへのフォールバックが許可されません。

可能な場合は、すべてのコールレッグでSRTPを使用しますが、デフォルトではCUBEが必要に応じてRTP-SRTPを実行します。

16.11+以降では、CUBEはデバッグにSRTPキーを記録しません

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

セキュアでないSRTP暗号の削除

デフォルトでは、オファーの作成時にすべてのSRTP暗号がCUBEによって送信されます。管理者は、IOS-XE 16.5+でvoice class srtp-cryptoコマンドを使用して、次世代のAEAD暗号スイートなどのよりセキュアな暗号に切り詰めることができます。

この設定では、CUBEがSRTP暗号を選択し、複数のオプションを使用してオファーに対する応答を作成する際に使用されるデフォルト設定を変更することもできます。

注：一部の古いシスコデバイスまたはピアデバイスは、AEAD暗号をサポートしていない可能性があります。暗号スイートをトリミングする際は、該当するすべてのドキュメントを参照してください。

```
<#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
!
```

その他の未使用VoIPプロトコルのディセーブル化

H323、MGCP、SCCP、STCAPP、CME、SRSTがこのゲートウェイで使用されていない場合は、CUBEを強化するための設定を削除する価値があります。

H323を無効にし、SIPからSIPへのコールのみを許可する

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

MGCP、SCCP、STCAPP、SIP、およびSCCP SRSTを無効にします。

注：これらのコマンドの中には、他のすべての設定を削除するものもあります。機能が使用されていないことを確認してから完全に削除してください。

<#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
```

コールルーティングと通話料金の不正

信頼できるIPからの接続を許可する

デフォルトでは、CUBEはダイヤルピアのsession targetおよびvoice class server-group設定で設定されたIPv4およびIPv6アドレスからの着信接続を信頼します。

IPアドレスを追加するには、voice service voipで設定されたip address trusted listコマンドを使用します。

前述したCN/SAN検証機能を使用してクライアント/サーバのホスト名検証がSIP TLSとともに設定されると、CN/SAN検証が成功すると、IPアドレスの信頼リストのチェックがバイパスされます。

CUBEでANY着信接続を受け入れるようにするno ip address trusted authenticateの使用は避けてください。

```
!
voice service voip
 ip address trusted authenticate

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

show ip address trusted listを使用して、IPアドレスチェックのステータスと、他の設定から取得されたすべてのスタティックおよびダイナミックな信頼リストの定義を表示します。

ダイヤルピア/サーバグループから取得されたダイナミック値は、ダイヤルピアがシャットダウンされた場合、またはキープアライブチェックに失敗した後でdown状態に設定された場合に、信頼リストから削除されます。

デフォルトでは、着信コールがIP信頼リストのチェックを通過しない場合、サイレントに廃棄されますが、これはno silent-discard untrusted voice service voip > sipコマンドを使用して上書きされ、エラーを送信者に返信できます。ただし、応答を送信することで、攻撃者はこれを使用して、デバイスが実際にSIPトラフィックをリッスンしていることを示し、攻撃の取り組みを強化する可能性があります。そのため、サイレント廃棄はIP信頼リスト(IP TIL)の廃棄を処理する推奨方式です。

一般的なダイヤルピアルーティングの回避

destination-pattern .T などの一般的な「catch all」宛先パターンを使用すると、CUBE経由で不正なコールをルーティングする可能性が高くなります。

管理者は、既知の電話番号範囲またはSIP URIのコールのみをルーティングするようにCUBEを設定する必要があります。

CUBEコールルーティング機能の詳細については、次のドキュメントを参照してください。

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脅威の軽減

不正なパケット処理

デフォルトでは、CUBEはSIPおよびRTPパケットを検査して、エラーをチェックし、パケットをドロップします。

不正なRTPパケット

デフォルトでは、IOS-XE CUBEは、SIP SDPオファー/アンサーシグナリング経由でネゴシエートされた接続のみを許可し、無効にできないため、すべてのRTP/RTCPストリームの送信元ポート検証を実行します。

これらは、次のコマンドをチェックすることで監視できます。

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

CUCMとの相互運用では、ポート4000から発信された保留音が廃棄されないように、Cisco CallManagerサービス経由のデュプレックスメディアストリーミングを有効にすることを推奨します。

RTPポート範囲の強化

デフォルトでは、IOS-XEは8000 ~ 48198のポート範囲を使用します。これは、次のコマンドを

使用して、16384 ~ 32768などの異なる範囲に設定できます。

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

管理者は、IPv4およびIPv6アドレス範囲ごとにRTPポート範囲を設定することもできます。

また、この設定により、CUBEのVoIPアプリケーションは、IPとポート範囲が静的に定義されるため、これらのパケットをルータのCPUのUDPプロセスにパントしないことにより、ファントムパケット処理をより効率的に実行できます。これは、CPUのパント動作をバイパスすることで、多数の正規または不正なRTPパケットを処理する際に高いCPU使用率を軽減するのに役立ちます。

```
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

サービス拒否(DOS)の防止

コールアドミッション制御機能を有効にすると、コールの合計数、CPU、メモリ、帯域幅に基づいてコールを制限できます。さらに、コールスパイクを検出して、コールを拒否し、サービス拒否を防ぐことができます。

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

アドレス隠蔽

デフォルトでは、CUBEはSIPヘッダー内のIPアドレス（Via、Contact、Fromなど）を独自のIPアドレスに置き換えます。

これは、voice service voipコマンドのaddress-hidingを適用することで、Refer-To、Referred-By、3xx contact header、History-Info、およびDiversion headerに拡張できます。

さらに、このヘッダー値に埋め込まれる可能性があるIPアドレスを軽減するコールレッグごとに新しいコールIDが作成されます。

アドレス隠蔽のために、IPアドレスの代わりにホスト名が必要な場合は、コマンドvoice-class sip localhost dns:cube.cisco.comを設定できます。

発信者IDプライバシー

CUBEは、コマンドclid-strip nameを任意のダイヤルピアで設定することにより、SIPヘッダーから発信者ID名の値をドロップするように設定できます。

さらに、CUBEは、P-Preferred Identity(PPID)、P-Asserted Identity(PAID)、プライバシー、P-Called Party Identity(PCPID)、Remote-Party Identity(RPID)などのSIPプライバシーヘッダーを相互に連携して理解できます。詳細については、次のドキュメントを参照してください。
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ダイジェスト認証

サービスプロバイダーへのCUBEによるSIP登録中、またはアップストリームのUASデバイスへのコールシグナリング中に、適用できるWWW-Authenticate/Proxy-Authenticateヘッダーフィールドが設定された401または407ステータスコードが返され、CUBEによる認証が困難になる場合があります。このハンドシェイク中、CUBEは後続の要求で認証ヘッダーフィールド値を計算するためのMD5アルゴリズムをサポートします。

サポートされていないSIPヘッダーまたはSDP

CUBEは、サポートされていないSIPヘッダーまたはSDPを取り除きます。これらのヘッダーまたはSDPは認識されません。pass-thru content sdp、pass-thru content unsupp、またはpass-through headers unsuppなどのコマンドを使用する場合は、CUBEを介して送信されるデータを確認するように注意する必要があります。

SIPヘッダーまたはSDPの削除または変更

着信または発信SIPプロファイルに追加の制御が必要な場合、管理者はSIPヘッダーまたはSDP属性を柔軟に変更または完全にドロップするように設定できます。

SIPプロファイルの使用方法については、次のドキュメントを参照してください。

- 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

その他のセキュリティ機能

暗号化されたパスワード

CUBEでは、実行コンフィギュレーションでSIP登録およびその他のIOS-XEパスワードを暗号化するために、16.11以降のバージョンの暗号化されたパスワードが必要です。

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

アクセス リスト

信頼リスト機能は、CUBEアプリケーション内のレイヤ7で動作します。パケットが通知なしにドロップされる時点で、CUBEはパケットの処理をすでに開始しています。

ルータのエントリポイントでパケットをドロップするには、着信または発信レイヤ3または4アクセスリストを使用してインターフェイスをロックダウンすることが望ましい場合があります。

これにより、CUBEからのCPUサイクルが正当なトラフィックに費やされるようになります。ACLとIP信頼リストおよびホスト名検証により、CUBEセキュリティに対する階層型アプローチが提供されます。

ゾーンベース ファイアウォール（ZBFW）

Cisco CUBEは、IOS-XE ZBFWとともに設定して、アプリケーション検査およびその他のセキュリティ機能を提供できます。

このトピックの詳細については、『CUBEおよびZBFWガイド』を参照してください。

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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。