Cisco Leitfaden zur Absicherung von Cisco Unified Border Element (CUBE) Enterprise-Geräten

Inhalt

Einleitung

Dieses Dokument unterstützt Sie dabei, Ihre Cisco IOS- und IOS-XE-Geräte mit Session Border Controller (SBC) und Cisco Unified Border Element (CUBE) Enterprise zu sichern und zu schützen.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

- CUBE Enterprise mit IOS-XE 17.10.1a

Anmerkung:

Einige der in diesem Dokument beschriebenen Funktionen sind in älteren IOS-XE-Versionen möglicherweise nicht verfügbar. Wenn möglich wurde sorgfältig dokumentiert, wenn ein Befehl oder eine Funktion eingeführt oder geändert wurde.

Dieses Dokument gilt nicht für CUBE Media Proxy, CUBE Service Provider, MGCP- oder SCCP-Gateways, Cisco SRST- oder ESRST-Gateways, H323-Gateways oder andere Analog-/TDM-Voice-Gateways.

Hintergrundinformationen

Dieses Dokument ergänzt den Leitfaden von Cisco zur Verwendung robuster Cisco IOS-Geräte. Daher werden doppelte Einträge aus diesem Dokument nicht in diesem Dokument dupliziert.

Common Criteria (CC) und Federal Information Standards (FIPS)

Cisco Virtual CUBE mit IOS-XE 16.9+ auf einem CSR1000v oder CAT8000v kann den Befehl **cc-mode** verwenden, um eine Common Criteria (CC)- und FIPS-Zertifizierungsdurchsetzung auf verschiedenen kryptografischen Modulen zu aktivieren, wie z. B. in Transport Layer Security (TLS) und . Es gibt keinen gleichwertigen Befehl für CUBE, das auf Hardware-Routern ausgeführt wird. In den späteren Abschnitten werden jedoch Methoden zum manuellen Aktivieren einer ähnlichen Härtung bereitgestellt.

Quelle: 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) und Public Key Infrastructure (PKI)

In diesem Abschnitt werden Aspekte im Zusammenhang mit TLS und PKI behandelt, die die Sicherheit dieser Protokolle neben SIP- (Secure Session Initial Protocol) und SRTP-Vorgängen (Secure Real Time Protocol) verbessern können.

Verwendung von TCP, TLS und SRTP

CUBE akzeptiert standardmäßig eingehende SIP-Verbindungen über TCP, UDP oder SIP TCP-TLS. Während die TCP-TLS-Verbindungen fehlschlagen, wenn nichts konfiguriert ist, werden TCP und UDP von CUBE akzeptiert und verarbeitet. Für ausgehende Verbindungen verwendet SIP standardmäßig UDP-Verbindungen, es sei denn, ein TCP- oder TCP-TLS-Befehl ist vorhanden. Ebenso handelt CUBE unsichere Real Time Protocol (RTP)-Sitzungen aus. Beide Protokolle bieten einem Angreifer ausreichend

Gelegenheit, Daten aus einem unverschlüsselten SIP-Sitzungssignalisierungs- oder Medien-Stream zu entschlüsseln. Nach Möglichkeit wird empfohlen, die SIP-Signalisierung mit SIP TLS und den Medien-Stream mit SRTP zu sichern.

Weitere Informationen finden Sie im SIP-TLS-Konfigurations- und SRTP-Konfigurationsleitfaden:

- 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

Denken Sie daran, dass die Sicherheit nur so stark ist wie die schwächste Verbindung. SIP-TLS und SRTP sollten über CUBE auf allen Anrufabschnitten aktiviert werden.

Die übrigen Abschnitte werden den folgenden Standardkonfigurationen hinzugefügt, um zusätzliche Sicherheitsfunktionen bereitzustellen:

Deaktivierung nicht sicherer SIP-Ports

Erinnern Sie sich an den vorherigen Abschnitt, in dem erläutert wurde, dass CUBE eingehende TCP und UDP für CUBE standardmäßig akzeptiert. Wenn SIP-TLS für alle Anrufabschnitte verwendet wird, kann es wünschenswert sein, den unsicheren UDP- und TCP-SIP-Listen-Port 5060 zu deaktivieren.

Nach der Deaktivierung können Sie **show sip-ua status**, **show sip connections udp brief** oder **show sip connections tcp brief** verwenden, um zu bestätigen, dass CUBE auf 5060 nicht mehr auf eingehende TCP- oder UDP SIP-Verbindungen wartet.

<#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 kann auch für die Zusammenarbeit mit IOS-XE VRFs konfiguriert werden, um eine weitere Netzwerksegmentierung zu ermöglichen.

Durch die Konfiguration von VRFs und das Binden einer VRF-fähigen Schnittstelle an einen Dial-Peer/Tenant überwacht CUBE nur eingehende Verbindungen für diese Kombination aus IP, Port und 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

TLS 1.2 durchsetzen

Zum Zeitpunkt der Erstellung dieses Dokuments ist TLS 1.2 die höchste von CUBE unterstützte Version von TLS. TLS 1.0 ist in IOS-XE 16.9 deaktiviert, TLS 1.1 kann jedoch ausgehandelt werden. Um die Optionen während eines TLS-Handshakes weiter einzuschränken, kann ein Administrator die einzige verfügbare Version für CUBE Enterprise auf TLS 1.2 zwingen.

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

TLS-Chiffren durchsetzen

Es kann wünschenswert sein, die Aushandlung schwächerer TLS-Chiffren in einer Sitzung zu deaktivieren. Ab IOS-XE 17.3.1 kann ein Administrator ein TLS-Profil konfigurieren, mit dem ein Administrator genau definieren kann, welche TLS-Chiffren während einer TLS-Sitzung angeboten werden. In älteren Versionen von IOS-XE wurde dies mit dem Postfix **strict-cipher** oder **ecdsa-cipher** des Befehls **crypto signaling** sip-ua gesteuert.

Beachten Sie, dass die von Ihnen ausgewählten Chiffren mit Peer-Geräten kompatibel sein sollten, die SIP-TLS mit CUBE verhandeln. In der entsprechenden Herstellerdokumentation finden Sie die besten Chiffren für alle Geräte.

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
!
```

Alle anderen Versionen

<#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
!
```

Große kryptografische Schlüssel verwenden

Die für TLS 1.2-Anwendungen empfohlenen Cisco Verschlüsselungsstandards der nächsten Generation (2048). Die folgenden Befehle können verwendet werden, um RSA-Schlüssel für TLS-Sitzungen zu erstellen.

Mithilfe des Befehls label kann ein Administrator diese Schlüssel auf einfache Weise auf einem Vertrauenspunkt angeben. Der Befehl "exportfähig" stellt sicher, dass das private/öffentliche Tastenpaar bei Bedarf mit dem folgenden Befehl exportiert werden kann:

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..]
```

Verwendung von Zertifikaten, die von der Zertifizierungsstelle signiert wurden

Administratoren sollten CA-signierte Zertifikate anstelle selbstsignierter Zertifikate verwenden, wenn sie ein Trustpoint- und Identitäts-(ID-)Zertifikat für CUBE Enterprise erstellen.

CA-Zertifikate bieten in der Regel zusätzliche Sicherheitsmechanismen wie CRL (Certificate Revocation List) oder OCSP-URLs (Online Certificate Status Protocol), die von Geräten verwendet werden können, um sicherzustellen, dass das Zertifikat nicht widerrufen wurde. Die Verwendung von vertrauenswürdigen öffentlichen Zertifizierungsstellenketten vereinfacht die Konfiguration der Vertrauensstellung auf Peer-Geräten, die möglicherweise über eingebettete Vertrauensstellung für bekannte Stammzertifizierungsstellen verfügen oder bereits über Stammzertifizierungsstellen für Ihre Unternehmensdomäne verfügen.

Darüber hinaus sollten die Zertifizierungsstellenzertifikate das CA-Flag "True" in grundlegenden Einschränkungen enthalten, und das Identitätszertifikat von CUBE sollte den Parameter "Extended Key Usage" (Erweiterte Schlüsselverwendung) enthalten, bei dem die Clientauthentifizierung aktiviert ist.

Im Folgenden wird ein Beispiel für ein Root-Zertifizierungsstellenzertifikat und ein ID-Zertifikat für CUBE dargestellt:

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..]
```

Starke Hashes verwenden

Wenn Sie einen Trustpoint für das Identitätszertifikat von CUBE konfigurieren, sollten Sie starke Hashing-Algorithmen wie SHA256, SHA384 oder SHA512 auswählen:

<#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

Aktivieren Sie die Überprüfung der Zertifikatsperrliste (Certificate Revocation List, CRL) oder des Online Certificate Status Protocol (OCSP).

IOS-XE-Vertrauenspunkte versuchen standardmäßig, die in einem Zertifikat aufgeführte Zertifikatsperrliste während des Befehls **crypto pki auth** zu überprüfen. Später, während der TLS-Handshakes, führt IOS-XE einen weiteren Zertifikatsperrlisten-Abruf auf Basis des empfangenen Zertifikats aus, um zu bestätigen, dass das Zertifikat noch gültig ist. Die Methoden für die Zertifikatsperrliste können HTTP oder LDAP sein, und es muss eine Verbindung zur Zertifikatsperrliste vorhanden sein, damit dies erfolgreich ist. Das heißt, DNS-Auflösung, TCP-Socket und Datei-Download vom Server auf den IOS-XE-Router müssen verfügbar sein, andernfalls schlägt die CRL-Prüfung fehl. Ebenso kann ein IOS-XE-Vertrauenspunkt so konfiguriert werden, dass er den OCSP-Wert aus einem AuthorityInfoAccess (AIA)-Header innerhalb des Zertifikats verwendet, der Abfragen an einen OCSP-Responder über HTTP durchführt, um ähnliche Prüfungen durchzuführen. Ein Administrator kann den OCSP- oder CRL Distribution Point (CDP) innerhalb eines Zertifikats überschreiben, indem er eine statische URL für ein Zertifikat bereitstellt. Außerdem kann der Administrator die Reihenfolge festlegen, in der die Sperrlisten oder OCSP überprüft werden, vorausgesetzt, beide sind vorhanden.

Viele deaktivieren einfach die Widerrufsprüfung mit **der Widerrufsprüfung none,** um den Prozess zu vereinfachen, aber dadurch schwächt ein Administrator die Sicherheit und entfernt den Mechanismus von IOS-XE, um zustandsfähig zu prüfen, ob ein bestimmtes Zertifikat noch gültig ist. Administratoren sollten, wenn möglich, OCSP oder CRL verwenden, um empfangene Zertifikate zustandsgesteuert zu überprüfen. Weitere Informationen zu CRL oder OCSP finden Sie im folgenden Dokument:

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

Sperrlisten-Überprüfung

<#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-Überprüfung

<#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
!
```

Bestellte OCSP- und CRL-Prüfung

<#root>

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

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

Überprüfung von Common Name (CN) und Subject Alternate Name (SAN) aktivieren

CUBE kann so konfiguriert werden, dass überprüft wird, ob die CN oder das SAN des Zertifikats mit dem Hostnamen aus dem Befehl **session target dns: übereinstimmt**. In IOS-XE 17.8+ kann ein TLS-Profil über das TLS-Profil konfiguriert werden.

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
```

Denken Sie daran, dass die Client-/Server-Bezeichnung in Bezug auf die Peer-Device-Rolle im TLS-

Handshake steht.

Weitere Erläuterungen:

- **cn-san validate server:** CUBE führt eine Hostnamenüberprüfung der empfangenen Peer-*Server*-Zertifikate für ausgehende TLS-Verbindungen durch, wobei CUBE die Client-Rolle ist.
- **cn-san validate client:** CUBE führt eine Hostnamenüberprüfung der empfangenen Peer-*Client*-Zertifikate für eingehende TLS-Verbindungen durch, wobei CUBE die Serverrolle ist.
- **cn-san validate bidirection**: Ermöglicht die Überprüfung des Hostnamens für beide Peer-Rollen während des TLS-Handshakes.

Wenn Sie den **Client**-Befehl **cn-san validate (**oder bidirektional) verwenden, müssen Sie ein SAN für die Prüfung konfigurieren, da das Sitzungsziel check nur für ausgehende Verbindungen und cn-san validate-Server verwendet wird.

Überprüfung des Client-Hostnamens:

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

Validierung des Serverhostnamens:

```
!
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
!
```

vor 17.8.1

Hinweis: Über diese Methode ist nur die Überprüfung des Server-Hostnamens verfügbar.

<#root>

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

cn-san-validate server

```
!
```

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

CUBE kann auch so konfiguriert werden, dass die TLS 1.2-Erweiterung (Server Name Indication, SNI) mit dem FQDN-Hostnamen von CUBE im TLS-Handshake an Peer-Geräte gesendet wird, um die Überprüfung des Hostnamens zu erleichtern.

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

Hinweis zum gegenseitigen TLS von CUBE:

- Wenn CUBE als TLS-Server fungiert (eingehende TLS-Verbindung lesen), wird standardmäßig immer ein Client-Zertifikat angefordert. Es gibt keine Konfiguration zum Deaktivieren dieses Verhaltens.
- Wenn CUBE als TLS-Client agiert und eine ausgehende TLS-Verbindung initiiert, ist die gegenseitige TLS dem Peer-Gerät überlassen, das als TLS-Server agiert. In diesem Szenario fordert ein Peer-Gerät möglicherweise kein Client-Zertifikat von CUBE an.
- In beiden Szenarien wird die Zertifikatkette, die von CUBE gesendet wird, durch den im TLS-Profil oder im Crypto-Signalisierungsbefehl definierten **Vertrauenspunkt** gesteuert.

<#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
!
```

Zuordnung von Remote-TLS-Verbindungen zu bestimmten Vertrauenspunkten

Bei Verwendung des **Crypto-Signalisierungs-Standardbefehls** sip-ua werden **ALLE** eingehenden TLS-

Verbindungen dieser Konfiguration entweder über tls-profile oder einzelne Befehle nach der Fehlerbehebung zugeordnet. Darüber hinaus werden bei der Zertifikatsvalidierung alle verfügbaren Vertrauenspunkte überprüft.

Möglicherweise ist es wünschenswert, für bestimmte Peer-Geräte auf Basis der IP-Adresse bestimmte TLS-Profilkonfigurationen zu erstellen, um sicherzustellen, dass die von Ihnen definierten Sicherheitsparameter auf die jeweilige TLS-Sitzung angewendet werden. Verwenden Sie dazu den Befehl **crypto signaling remote-addr,** um ein IPv4- oder IPv6-Subnetz zu definieren, das einem TLS-Profil oder einem Satz von Postfix-Befehlen zugeordnet wird. Sie können den Verifizierungs-Trustpoint auch direkt über **client-vtp-**Befehle zuordnen, um genau festzulegen, welche Trustpoints zur Validierung von Peer-Zertifikaten verwendet werden.

Mit dem folgenden Befehl werden die meisten bisher behandelten Themen zusammengefasst:

```
!
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
!
```

Bei älteren Versionen kann dies folgendermaßen durchgeführt werden:

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

Ab Version 17.8 können Sie auch TLS-Profil- und Per-Tenant-Listen-Ports pro **Tenant der Sprachklasse** konfigurieren, um weitere Segmentierungsoptionen für einen bestimmten Listen-Port bereitzustellen.

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

Durchsetzen von striktem SRTP

Bei der Aktivierung von SRTP auf CUBE Enterprise wird als Standardvorgang die Deaktivierung des Fallbacks auf RTP verwendet.

Verwenden Sie, sofern möglich, SRTP auf allen Anrufabschnitten. Standardmäßig führt CUBE jedoch RTP-SRTP bei Bedarf aus.

Beachten Sie, dass CUBE die SRTP-Schlüssel nicht in Debugs protokolliert, die in Version 16.11+ beginnen.

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

Unsichere SRTP-Chiffren trimmen

Standardmäßig werden alle SRTP-Chiffren von CUBE gesendet, wenn ein Angebot erstellt wird. Ein Administrator kann mit dem Befehl voice class srtp-crypto in IOS-XE 16.5+ auf sicherere Chiffren wie die AEAD-Chiffriersuiten der nächsten Generation zurückgreifen.

Mit dieser Konfiguration kann auch die Standardeinstellung geändert werden, wenn CUBE einen SRTP-Cipher auswählt und eine Antwort auf ein Angebot mit mehreren verfügbaren Optionen erstellt.

Hinweis: Einige ältere Cisco Geräte oder Peer-Geräte unterstützen möglicherweise keine AEAD-Verschlüsselung. Weitere Informationen zum Trimmen von Verschlüsselungsreihen finden Sie in der entsprechenden Dokumentation.

<#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
!
```

Deaktivieren anderer nicht verwendeter VoIP-Protokolle

Wenn H323, MGCP, SCCP, STCAPP, CME, SRST auf diesem Gateway nicht verwendet werden, sollten Sie die Konfigurationen entfernen, um CUBE zu härten.

Deaktivieren von H323 und ausschließlich SIP-SIP-Anrufe zulassen

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

Deaktivieren Sie MGCP, SCCP, STCAPP, SIP und SCCP SRST.

Hinweis: Einige dieser Befehle löschen alle anderen Konfigurationen. Stellen Sie vor dem vollständigen Entfernen sicher, dass keine Funktionen verwendet werden.

<#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
```

Anrufweiterleitung und Gebührenbetrug

Verbindungen von vertrauenswürdigen IPs zulassen

CUBE vertraut standardmäßig eingehenden Verbindungen von IPv4- und IPv6-Adressen, die für Dial-Peer-**Sitzungsziele** und **Servergruppenkonfigurationen der Sprachklasse** konfiguriert wurden.

Um weitere IP-Adressen hinzuzufügen, verwenden Sie den Befehl **ip address trusted list**, der über **Sprachservice-VoIP** konfiguriert wurde**.**

Wenn die Validierung des Client-/Server-Hostnamens zusammen mit SIP TLS mithilfe der zuvor erläuterten CN/SAN-Validierungsfunktion konfiguriert wird, umgeht eine erfolgreiche CN/SAN-Validierung die Prüfung der vertrauenswürdigen Liste der IP-Adressen.

Vermeiden Sie die Verwendung von **no ip address trusted authate**, wodurch CUBE ALLE eingehenden Verbindungen akzeptieren kann.

```
!
voice service voip
 ip address trusted authenticate

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

Verwenden Sie **show ip address trusted list**, um den Status der IP-Adressprüfung und alle statischen und dynamischen Definitionen vertrauenswürdiger Listen anzuzeigen, die von anderen Konfigurationen abgeleitet wurden.

Beachten Sie, dass der von einem Dial-Peer/einer Server-Gruppe abgeleitete dynamische Wert aus der vertrauenswürdigen Liste entfernt wird, wenn ein Dial-Peer nach fehlgeschlagenen Keepalive-Prüfungen heruntergefahren oder auf den Zustand "nicht verfügbar" gesetzt wird.

Wenn ein eingehender Anruf die Prüfung der vertrauenswürdigen IP-Liste nicht besteht, wird er standardmäßig verworfen. Dies kann jedoch mit dem Befehl **no silent-discard untrusted** voice service voip > sip überschrieben werden, um einen Fehler zurück an den Absender zu senden. Wenn ein Angreifer jedoch eine Antwort sendet, kann dies darauf hinweisen, dass das Gerät tatsächlich auf SIP-Datenverkehr wartet und so seine Angriffsbemühungen verstärken. Daher ist der automatische Abwurf die bevorzugte Methode zur Behandlung von IP Trusted List-Drops.

Generisches Dial-Peer-Routing vermeiden

Die Verwendung generischer "catch all"-Zielmuster wie **destination-pattern .T** kann die Wahrscheinlichkeit erhöhen, dass ein betrügerischer Anruf über CUBE weitergeleitet wird.

Administratoren sollten CUBE so konfigurieren, dass nur Anrufe für bekannte Rufnummernbereiche oder SIP-URIs weitergeleitet werden.

Im folgenden Dokument finden Sie eine ausführlichere Erläuterung der CUBE-Anrufweiterleitungsfunktionen:

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-Bedrohungsschutz

Ungültige Paketbehandlung

CUBE überprüft SIP- und RTP-Pakete standardmäßig auf Fehler und verwirft das Paket.

Nicht autorisierte RTP-Pakete

Standardmäßig führt das IOS-XE CUBE eine Quell-Port-Validierung für alle RTP-/RTCP-Streams durch, indem es nur über SIP-SDP-Offer/Answer-Signalisierung ausgehandelte Verbindungen zulässt und nicht deaktiviert werden kann.

Diese können durch Überprüfen des folgenden Befehls überwacht werden:

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

Für die Interoperabilität mit CUCM wird empfohlen, das Duplex Media-Streaming über den Cisco CallManager-Service zu aktivieren, um zu vermeiden, dass Warteschleifenmusik beim Erwerb von Port 4000 verloren geht.

RTP-Port-Bereich-Härtung

IOS-XE verwendet standardmäßig den Port-Bereich von 8000 bis 48198. Dies kann mithilfe des folgenden Befehls für einen anderen Bereich konfiguriert werden, z. B. 16384 bis 32768:

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

!

Ein Administrator kann auch RTP-Port-Bereiche pro IPv4- und IPv6-Adressbereich konfigurieren.

Durch diese Konfiguration kann die VoIP-Anwendung von CUBE eine effizientere Verarbeitung von Phantom-Paketen durchführen, indem diese Pakete nicht an den UDP-Prozess der Router-CPU gesendet werden, da die IP- und Port-Bereiche statisch definiert sind. Dies kann dazu beitragen, eine hohe CPU-Auslastung zu minimieren, wenn eine große Anzahl legitimer oder unzulässiger RTP-Pakete verarbeitet wird, indem das CPU-Punt-Verhalten umgangen wird.

```
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

Schutz vor Denial of Service (DOS)

Die Anrufzugangskontrolle kann aktiviert werden, um Anrufe basierend auf Gesamtanrufe, CPU, Arbeitsspeicher und Bandbreite zu begrenzen. Darüber hinaus können Anrufspitzen erkannt werden, um Anrufe abzulehnen und eine Diensteverweigerung zu verhindern.

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

Adressverbergen

Standardmäßig ersetzt CUBE IP-Adressen in SIP-Headern wie, aber nicht beschränkt auf Via, Contact und From durch eine eigene IP-Adresse.

Sie können diese Funktion auf die Header "Refer-To", "Referred-By", "3xx Contact", "History-Info" und "Diversion" erweitern, indem Sie den **Voice Service**-Befehl "**voip" zum Ausblenden** der **Adresse** anwenden.

Darüber hinaus wird für jede IP-Adresse, die zur Reduzierung von Anrufzweigen verwendet wird und in diesen Header-Wert eingebettet sein kann, eine neue Anruf-ID erstellt.

Wenn anstelle einer IP-Adresse ein Hostname zum Ausblenden von Adressen benötigt wird, kann der Befehl **voice-class sip localhost dns:cube.cisco.com** konfiguriert werden.

Anrufer-ID-Datenschutz

CUBE kann so konfiguriert werden, dass Anrufer-ID-Namenswerte aus SIP-Headern mit dem Befehl **clid-strip name** auf jedem Dial-Peer konfiguriert werden.

Darüber hinaus kann CUBE SIP-Datenschutz-Header wie P-Preferred Identity (PPID), P-Asserted Identity (PAID), Privacy, P-Called Party Identity (PCPID), Remote-Party Identity (RPID) miteinander verarbeiten

und verstehen. Weitere Informationen finden Sie in folgendem Dokument: 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-Digest-Authentifizierung

Während der SIP-Registrierung durch CUBE an einen Service Provider oder während eines Anrufsignalisierungsvorgangs können Upstream-UAS-Geräte einen 401- oder 407-Statuscode mit einem anwendbaren WWW-Authenticate/Proxy-Authenticate-Headerfeld zurückgeben, der die CUBE-Authentifizierung herausfordert. Während dieses Handshakes unterstützt CUBE den MD5-Algorithmus zur Berechnung des Authorization-Header-Feldwerts in einer nachfolgenden Anforderung.

Nicht unterstützte SIP-Header oder SDP

CUBE entfernt nicht unterstützte SIP-Header oder SDP, die es nicht versteht. Bei der Verwendung von Befehlen wie **pass-thru content sdp, pass-thru content unsupp** oder **pass-through headers unsupp** sollte sorgfältig darauf geachtet werden, welche Daten durch CUBE übertragen werden.

Entfernen oder Ändern von SIP-Headern oder SDP

Wenn zusätzliche Kontrolle erforderlich ist, können eingehende oder ausgehende SIP-Profile von einem Administrator so konfiguriert werden, dass ein SIP-Header oder ein SDP-Attribut flexibel geändert oder endgültig gelöscht werden kann.

Weitere Informationen zur Nutzung des SIP-Profils finden Sie in den folgenden Dokumenten:

- 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

Weitere Sicherheitsfunktionen

Verschlüsselte Passwörter

CUBE erfordert verschlüsselte Kennwörter für Version 16.11 und höher, um die SIP-Registrierung und andere IOS-XE-Kennwörter in der aktuellen Konfiguration zu verschlüsseln.

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

Zugriffslisten

Die Funktion der vertrauenswürdigen Liste wird auf Layer 7 der CUBE-Anwendung ausgeführt. Wenn das Paket unbeaufsichtigt verworfen wird, hat CUBE bereits mit der Verarbeitung des Pakets begonnen.

Es kann wünschenswert sein, Schnittstellen mit Layer-3- oder Layer-4-Zugriffslisten für ein- oder ausgehenden Datenverkehr zu sperren, um das Paket am Eingangspunkt des Routers zu verwerfen.

So wird sichergestellt, dass CPU-Zyklen von CUBE für legitimen Datenverkehr verwendet werden. ACLs

bieten zusammen mit der IP Trusted List- und Hostnamen-Validierung einen mehrschichtigen Ansatz für die CUBE-Sicherheit.

Zonenbasierte Firewall (ZBFW)

Cisco CUBE kann zusammen mit IOS-XE ZBFW konfiguriert werden, um Anwendungsinspektion und andere Sicherheitsfunktionen bereitzustellen.

Weitere Informationen zu diesem Thema finden Sie im CUBE- und ZBFW-Leitfaden:

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.