Cisco-gids voor Harden Cisco Unified Border Element (CUBE) Enterprise-apparaten

Inhoud

Inleiding

Dit document zal u helpen uw Cisco IOS- en IOS-XE-apparaten te beveiligen en te verharden die werken met Session border-controller (SBC) en Cisco Unified Border Element (CUBE) Enterprise uitvoeren.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

- CUBE Enterprise met IOS-XE 17.10.1a.

Opmerking:

Het is mogelijk dat niet alle functies die in dit document zijn beschreven, beschikbaar zijn in oudere IOS-XE-versies. Waar mogelijk is het document gedocumenteerd wanneer een opdracht of een functie is ingevoerd of gewijzigd.

Dit document is niet van toepassing op CUBE Media Proxy, CUBE Service Provider, MGCP of SCCP-gateways, Cisco SRST of ESR-gateways, H323-gateways of andere analoge/TDM-spraakgateways.

Achtergrondinformatie

Dit document dient als een aanvulling op wat u kunt vinden in de Cisco Guide to Harden Cisco IOS Devices. Zo worden eventuele dubbele items uit dat document niet gedupliceerd in dit document.

Gemeenschappelijke criteria (CC) en de Federal Information Standards (FIPS)

Cisco Virtual CUBE die IOS-XE 16.9+ op een CSR1000v of CAT8000v gebruikt, kan de opdracht **cc-mode** gebruiken om een Common Criteria (CC) en de Federal Information Standards (FIPS) Certificatie-handhaving mogelijk te maken op verschillende cryptografische modules zoals die gevonden in Transport Layer Security (TLS) en . Er is geen equivilant opdracht voor CUBE die op Hardware Routers loopt maar de recentere secties zullen methodes verstrekken om het gelijkaardige verharden manueel toe te laten.

Bron: 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) en Public Key Infrastructure (PKI)

In deze sectie worden items besproken rond TLS en PKI die de beveiliging kunnen verbeteren die door die protocollen wordt geboden naast Secure Session Initial Protocol (SIP) en Secure Real Time Protocol (SRTP)-bewerkingen.

Gebruik TCP/TLS en SRTP

Standaard accepteert CUBE inkomende SIP-verbindingen via TCP, UDP of SIP TCP-TLS. Terwijl de TCP-TLS-verbindingen zullen mislukken als er niets is geconfigureerd, zullen TCP en UDP worden geaccepteerd en verwerkt door CUBE. Voor uitgaande verbindingen zal SIP standaard UDP-verbindingen gebruiken tenzij er een TCP- of TCP-TLS-opdracht aanwezig is. Op dezelfde manier zal CUBE onveilige Real Time Protocol (RTP)-sessies onderhandelen. Beide protocollen bieden ruime mogelijkheden voor een aanvaller om gegevens te gamen van een niet-versleutelde SIP-sessiesignalering of mediastroom. Waar mogelijk wordt aanbevolen de SIP-signalering te beveiligen met SIP TLS en de mediastroom met SRTP.

Raadpleeg de SIP TLS-configuratie en de SRTP-configuratiehandleiding:

- 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

Vergeet niet dat de beveiliging zo sterk is als de zwakste link en dat SIP-TLS en SRTP op alle call-benen via CUBE ingeschakeld moeten worden.

De resterende secties worden aan deze standaardconfiguraties toegevoegd in een poging om extra beveiligingsfuncties te bieden:

Niet-beveiligde SIP-poorten uitschakelen

Herinner de vorige sectie gedetailleerd dat CUBE binnenkomende TCP en UDP voor CUBE door gebrek zal goedkeuren. Zodra SIP TLS wordt gebruikt voor alle aanroepbenen, kan het wenselijk zijn om de onbeveiligde UDP en TCP SIP Listen poort 5060 uit te schakelen.

Als deze optie is uitgeschakeld, kunt u de **show sip-ua status** gebruiken, **tonen sip connecties udp korte** of **tonen sip connecties tcp korte** om te bevestigen dat CUBE niet meer luistert op 5060 voor inkomende TCP- of UDP SIP-verbindingen.

<#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 kan ook worden geconfigureerd om naast IOS-XE VRF's te werken voor verdere netwerksegmentatie.

Door VRF's te configureren en een VRF-enabled interface te binden aan een dial-peer/huurder; CUBE zal alleen luisteren naar inkomende verbindingen voor die IP, poort, VRF-combinatie.

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 afdwingen

Op het moment van schrijven van dit document is TLS 1.2 de hoogste versie van TLS die door CUBE wordt ondersteund. TLS 1.0 is uitgeschakeld in IOS-XE 16.9, maar er kan over TLS 1.1 worden onderhandeld. Om de opties tijdens een TLS-handdruk verder te beperken, kan een beheerder de enige beschikbare versie voor CUBE Enterprise dwingen om TLS 1.2 in te voeren

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

TLS-algoritmen afdwingen

Het kan wenselijk zijn om zwakkere TLS-algoritmen uit te schakelen van onderhandelingen in een sessie. Vanaf IOS-XE 17.3.1 kan een beheerder een TLS-profiel configureren waarmee een beheerder precies kan definiëren welke TLS-algoritmen tijdens een TLS-sessie zullen worden aangeboden. In oudere versies van IOS-XE werd dit gecontroleerd met behulp van de **strikte algoritme** of **ecdsa-algoritme** postfix op de

crypto signalering sip-ua opdracht.

Merk op dat de algoritmen die u selecteert compatibel zouden moeten zijn met peer apparaten die SIP TLS met CUBE onderhandelen. Raadpleeg alle relevante documentatie van leveranciers om de beste algoritmen tussen alle apparaten te bepalen.

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 andere versies

<#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
!
```

Gebruik grote cryptografische toetsen

Cisco Next Generation-normen voor cryptografie aanbevolen 2048 voor gebruik met TLS 1.2-toepassingen. Met onderstaande opdrachten kunt u RSA-toetsen maken die u met TLS-sessies kunt gebruiken.

Met de labelopdracht kan een beheerder deze sleutels eenvoudig op een trustpoint specificeren en met de exporteerbare opdracht wordt ervoor gezorgd dat, indien nodig, het private/publieke sleutelpaar kan worden geëxporteerd met de opdracht zoals

crypto key export rsa CUBE-ENT pem terminal aes WACHTWOORD!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..]
```

Gebruikt door de certificeringsinstantie (CA) ondertekende certificaten

Beheerders moeten CA-ondertekende certificaten gebruiken in plaats van zelf-ondertekende certificaten bij het creëren van vertrouwens- en identiteitsbewijs (ID) voor CUBE-bedrijf.

CA-certificaten bieden doorgaans aanvullende beveiligingsmechanismen zoals de URLâ€™s van de certificaatintrekkingslijst (CRL) of het Online Certificate Status Protocol (OCSP) die door apparaten kunnen worden gebruikt om er zeker van te zijn dat het certificaat niet is ingetrokken. Het gebruik van vertrouwde openbare CA-ketens vergemakkelijkt de vertrouwensrelatie configuratie op peer-apparaten die vertrouwen ingebed kunnen hebben voor bekende wortel CA's of reeds hebben Root CA-trusts voor uw ondernemingsdomein.

Bovendien moeten de CA-certificaten de CA-vlag van True in Basic Constraints bevatten en moet het CUBE-identiteitscertificaat de uitgebreide Key Usage-parameter van de aan client toegewezen autorisatie bevatten.

Het certificaat van de Root CA van de steekproef en een Cert van ID voor CUBE worden hieronder getoond gebruiken:

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..]
```

Gebruik sterke hashes

Bij het configureren van een trustpoint voor het Identity Certificate van CUBE moet u sterke hashingalgoritmen selecteren zoals SHA256, SHA384 of 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
```

Controles van Certificaatherroepingslijst (CRL) of Online Certificate Status Protocol

(OCSP) inschakelen

Standaard zal IOS-XE Trustpionts proberen om het CRL te controleren dat in een certificaat wordt vermeld tijdens de opdracht **crypto pki auth**, later tijdens de TLS handshakes IOS-XE zal ook een andere CRL-haal uitvoeren gebaseerd op de ontvangen cert om te bevestigen dat het certificaat nog steeds geldig is. De methodes voor CRL kunnen of HTTP of LDAP zijn en de connectiviteit aan CRL moet aanwezig zijn voor dit om te slagen. Dat wil zeggen, DNS resolutie, TCP socket en bestand downloaden van de server naar de IOS-XE router moet beschikbaar zijn anders de CRL-controle zal falen. Op dezelfde manier kan een IOS-XE Trustpoint worden geconfigureerd om OCSP-waarde te gebruiken van een AuthorityInfoAccess (AIA)-header binnen het certificaat die vragen uitvoert en een OCSP-Responder via HTTP om soortgelijke controles uit te voeren. Een beheerder kan OCSP- of CRL-distributiepunt (CDP) binnen een certificaat negeren door een statische URL op een certificaat op te geven. Verder kan een beheerder ook de volgorde configureren waarin CRL of OCSP zijn gecontroleerd, ervan uitgaande dat beide aanwezig zijn.

Velen maken herroepingscontroles met **herroeping-controle niets** onbruikbaar om het proces te vereenvoudigen maar in het doen verzwakt een beheerder veiligheid en verwijdert IOS-XE's mechanisme om stateful te controleren als een bepaald certificaat nog geldig is. Waar mogelijk moeten beheerders OCSP of CRL gebruiken om stateful inspection van ontvangen certificaten uit te voeren. Bekijk het volgende document voor meer informatie over CRL of OCSP:

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-controle

<#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-controle

<#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
!
```

Bestelde OCSP- en CRL-controle

<#root>

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

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

De verificatie van de algemene naam (CN) en de alternatieve naam (SAN) van het onderwerp inschakelen

CUBE kan worden geconfigureerd om te controleren of de CN of SAN van het certificaat overeenkomen met de hostnaam van het **sessiedoel dns:** commando. In IOS-XE 17.8+ kan een TLS-profiel worden geconfigureerd via het tls-profiel.

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
```

Vergeet niet dat de client/server-aanduiding verwijst naar de rol van peer-apparaten in de TLS-handdruk

Ter nadere illustratie:

- **cn-san validate server:** CUBE zal hostname validatie uitvoeren van ontvangen peer *server* certificaten voor uitgaande TLS verbindingen waar CUBE de client rol is.
- **cn-san validate client:** CUBE zal hostname validatie van ontvangen peer *client* certificaten uitvoeren voor inkomende TLS-verbindingen waar CUBE de serverrol is.
- **cn-san valideren bidirectie**: maakt hostname validatie mogelijk voor beide peer rollen tijdens de TLS handshake.

Bij gebruik van de **cn-san validate client** commando (of tweerichtingsverkeer) moet u een SAN configureren om te controleren, aangezien het sessiedoel is te controleren of het alleen gaat om uitgaande verbindingen en cn-san validate server.

Validatie van clienthostnaam:

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

Server Hostname Validatie:

```
!
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
!
```

Vóór 17.8.1

Opmerking: alleen server hostname validatie is beschikbaar via deze methode.

<#root>

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

cn-san-validate server

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

CUBE kan ook worden geconfigureerd om de Server Name Indication (SNI) TLS 1.2-extensie met de FQDN-hostnaam van CUBE binnen de TLS-handdruk naar peer-apparaten te sturen om hun hostname-validatie-inspanningen te vergemakkelijken.

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

Een opmerking over de wederzijdse TLS van CUBE:

- Standaard zal CUBE als een TLS-server (lees inkomende TLS-verbinding) altijd een clientcertificaat aanvragen. Er is geen configuratie om dit gedrag uit te schakelen.
- Wanneer CUBE optreedt als een TLS-client en een uitgaande TLS-verbinding initieert, is wederzijdse TLS-verbinding ingesteld op het peer-apparaat dat fungeert als een TLS-server. In dit scenario kan een peer-apparaat geen clientcertificaat aanvragen bij CUBE.
- In beide scenario's wordt de certificaatketen CUBE verzonden door het **trustpoint** dat in het TLS-profiel is gedefinieerd of op de opdracht crypto signalering.

<#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
!
```

Toewijzing van externe TLS-verbindingen aan specifieke trustpoints

Bij gebruik van **crypto signalering standaard** sip-ua opdracht **ALLE** inkomende TLS-verbindingen worden aan deze configuratie toegewezen via tls-profiel of individuele post-fix commando's. Bovendien worden alle beschikbare betrouwbaarheidspunten gecontroleerd bij het valideren van certificaten.

Het kan wenselijk zijn om specifieke TLS-profielconfiguraties te maken voor een specifiek peer-apparaat op basis van IP-adres, om er zeker van te zijn dat de door u gedefinieerde beveiligingsparameters worden

toegepast op die TLS-sessie. Hiervoor gebruikt u de opdracht **crypto signalering op afstand** om een IPv4- of IPv6-subnetverbinding te definiëren voor toewijzing aan een TLS-profiel of een set postfixopdrachten. U kunt ook direct verificatie trustpoint toewijzen via **client-vtp**) opdrachten om precies vast te leggen welke trustpoints worden gebruikt om peer certificaten te valideren.

In de opdracht hieronder worden de meeste items die tot op dit punt zijn besproken, samengevat:

```
!
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
!
```

Voor oudere versies kan dit als volgt worden gedaan:

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

Beginnend in 17.8 kunt u ook tls-profiel en per-tenant luisterpoorten per **spraakklassehuurder** configureren om verdere segmentatieopties op een bepaalde luisterpoort te bieden.

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

Strict SRTP afdwingen

Wanneer u SRTP op CUBE Enterprise inschakelt, wordt de standaardhandeling gebruikt om terugbellen naar RTP te verbieden.

Waar mogelijk zal het gebruik SRTP op alle vraag-benen echter door gebrek CUBE RTP-SRTP uitvoeren zoals nodig.

Merk op dat CUBE de SRTP-toetsen niet vastlegt in debugs vanaf 16.11+

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

Trim onveilige SRTP-algoritmen

Standaard worden alle SRTP-algoritmen door CUBE verzonden bij het maken van een aanbieding. Een beheerder kan omlaag trimmen naar veiliger algoritmen zoals de next-generation AEAD algoritme suites door de Voice class srtp-crypto opdracht in IOS-XE 16.5+ te gebruiken.

Deze configuratie kan ook de standaardvoorkeur veranderen die wordt gebruikt wanneer CUBE een SRTP-algoritme selecteert en een antwoord op sommige aanbiedingen maakt met meerdere opties beschikbaar.

N.B.: Sommige oudere Cisco-apparaten of peer-apparaten ondersteunen mogelijk geen AEAD-algoritmen. Raadpleeg alle toepasselijke documentatie bij het trimmen van de cijfersuites.

<#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
!
```

Andere ongebruikte VoIP-protocollen uitschakelen

Als H323, MGCP, SCCP, STCAPP, CME, SRST niet op deze gateway worden gebruikt, is het de moeite waard om de configuraties te verwijderen om CUBE te verharden.

Schakel H323 uit en laat alleen SIP-oproepen toe

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

MGCP, SCCP, STCAPP, SIP en SCCP SRST uitschakelen.

N.B.: Sommige van deze opdrachten verwijderen alle andere configuraties, zorgen ervoor dat er geen functies worden gebruikt voordat ze volledig worden verwijderd.

<#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
```

Oproeproutering en tolfraude

Verbindingen toestaan vanaf vertrouwde IPâ€™s

Standaard vertrouwt CUBE op inkomende verbindingen van IPv4- en IPv6-adressen die zijn geconfigureerd op **doelen voor** dial-peers-**sessies** en configuraties van **servergroepen met spraakklassen**.

Om extra IP-adressen toe te voegen, gebruikt u de opdracht **IP-adres vertrouwde lijst** die via **voip voor spraakservice is** geconfigureerd**.**

Wanneer client/server hostname validatie is geconfigureerd naast SIP TLS via de eerder besproken CN/SAN validate functie, zal een succesvolle CN/SAN validatie IP-adres vertrouwde lijstcontroles omzeilen.

Vermijd het gebruik van **geen ip adres vertrouwde authenticate** wat zal toelaten CUBE om elke inkomende verbinding te accepteren.

```
!
voice service voip
 ip address trusted authenticate

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

Gebruik **tonen IP adres vertrouwde lijst** om de status van IP adres controle en alle statische en dynamische vertrouwde lijst definities afgeleid uit andere configuraties te bekijken.

Merk op dat de dynamische waarde die uit een wijzerplaat-peer/server-groep wordt afgeleid uit de vertrouwde op lijst wordt verwijderd wanneer een wijzerplaat-peer sluiting of reeks aan benedenstaat na het ontbreken keepalive controles is.

Standaard wordt een inkomende oproep niet doorgegeven aan de IP Trusted List controle, maar deze wordt stilzwijgend genegeerd, maar dit kan worden genegeerd met de opdracht **no silent-discard unusted** voice service voip > SIP om een fout terug te sturen naar de afzender. Door een reactie te verzenden kan een aanvaller dit echter gebruiken om aan te geven dat het apparaat in feite luistert naar SIP-verkeer en hun aanvalsinspanningen opvoert. Als zodanig stille verwerping is de geprefereerde methode om IP Trusted List druppels te behandelen.

Vermijd generieke dial-peer routing

Het gebruiken van generische "vangst alle" bestemming-patronen zoals **bestemming-patroon .T** kan de

waarschijnlijkheid verhogen om een frauduleuze vraag door CUBE te leiden.

De beheerders zouden CUBE moeten vormen om slechts routevraag naar bekende telefoonnummerreeksen of SIP URIs te vormen.

Zie het volgende document voor een grotere uitleg van de functies voor gespreksrouting van 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

Beperken van CUBE-bedreigingen

Misvormde pakketverwerking

Standaard zal CUBE SIP- en RTP-pakketten inspecteren om op fouten te controleren en het pakket te laten vallen.

Rogue RTP-pakketten

Door gebrek voert IOS-XE CUBE bron-poorts validatie uit voor alle RTP/RTCP-stromen door alleen verbindingen toe te staan die worden onderhandeld via SIP SDP-aanbieding/antwoordsignalering en kan niet worden uitgeschakeld.

Deze kunnen worden bewaakt door de volgende opdracht te controleren:

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

Voor interop met CUCM wordt aanbevolen om het streamen van duplexmedia via de Cisco CallManager-service mogelijk te maken om te voorkomen dat muziek bij stilstand wordt gedropt wanneer ze wordt betrokken vanaf poort 4000.

RTP-verharding van poortbereik

Standaard gebruikt IOS-XE het poortbereik van 8000 tot 48198. Dit kan op een ander bereik worden ingesteld, zoals 16384 via 32768 via de volgende opdracht:

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

Een beheerder kan ook RTP-poortbereiken per IPv4- en IPv6-adresbereiken configureren.

Deze configuratie maakt het ook mogelijk dat de VoIP-toepassing van CUBE spookpakketverwerking efficiënter uitvoert door deze pakketten niet in het UDP-proces bij de CPU van de router te storten, aangezien het IP- en poortbereik statisch zijn gedefinieerd. Dit kan helpen hoge CPU verlichten bij het verwerken van een groot aantal legitieme of illegale RTP-pakketten door het CPU-puntinggedrag te omzeilen.

```
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

DOS-preventie (Denial of Service)

De functies van Call Admission Control kunnen worden ingeschakeld om oproepen te beperken op basis van Totale oproepen, CPU, geheugen, bandbreedte. Daarnaast kunnen Call Spikes worden gedetecteerd om oproepen te weigeren en ontkenning van de service te voorkomen.

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

Adresverberging

Standaard zal CUBE IP-adressen in SIP-headers zoals, maar niet beperkt tot Via, Contact en From vervangen met zijn eigen IP-adres.

Dit kan worden uitgebreid naar Refer-To, Referred-By, 3xx contact header, History-Info en Diversion headers door het **verstoppen van** de **voip**-opdracht van de **spraakdienst toe te** passen.

Bovendien wordt een nieuwe call-id aangemaakt voor elk call-leg verzachtend IP-adres dat in deze headerwaarde kan worden ingesloten.

Waar een hostname vereist is in plaats van een IP-adres voor adrestoepassingen, de commando **spraakklasse sip localhost dns:cube.cisco.com** kan worden geconfigureerd.

Privacy van nummerherkenning

CUBE kan worden geconfigureerd om de waarden voor de naam van de nummerherkenning uit SIP-koppen te laten vallen terwijl de **naam van de** opdrachtregel op elke dial-peer is geconfigureerd.

Bovendien kan CUBE interageren en de kopregels van de SIP-privacy begrijpen zoals P-Preferred Identity (PPID), P-Asserted Identity (PAID), Privacy, P-Calling Party Identity (PCPID), Remote-Party Identity (RPID). Zie voor meer informatie het volgende document: 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-digestieverificatie

Tijdens SIP-registratie door CUBE aan een serviceprovider of tijdens een oproep die upstream UAS-apparaten signaleert, kunnen deze een 401- of 407-statuscode retourneren met een toepasbaar WW-Authenticate/Proxy-Authenticate-headerveld dat de CUBE uitdaagt om te authenticeren. Tijdens deze handdruk ondersteunt CUBE het MD5-algoritme voor het berekenen van de veldwaarde van de autorisatieheader in een volgaanvraag.

Niet-ondersteunde SIP-koppen of SDP

CUBE zal niet-ondersteunde SIP-koppen of SDP verwijderen die niet worden begrepen. Voorzichtigheid moet worden betracht bij het gebruik van opdrachten zoals **pass-thru content sdp**, **pass-thru content unsupp**, of **pass-through headers unsupp** om te verzekeren welke gegevens het maken door CUBE.

SIP-koppen of SDP verwijderen of wijzigen

Waar extra controle vereist is, kunnen inkomende of uitgaande SIP-profielen door een beheerder worden geconfigureerd om een SIP-header of SDP-kenmerk flexibel aan te passen of rechtstreeks te laten vallen.

Raadpleeg de volgende documenten over gebruik van SIP-profiel:

- 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

Overige beveiligingsfuncties

Versleuteld wachtwoord

CUBE vereist versleutelde wachtwoorden voor 16.11 en latere versies om SIP-registratie en andere IOS-XE wachtwoorden in de actieve configuratie te versleutelen.

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

Toegangslijsten

De vertrouwde lijstfunctie werkt op Layer 7 binnen de CUBE-toepassing. Tegen de tijd dat het pakket stilletjes wordt losgelaten is de CUBE al begonnen met de verwerking van het pakket.

Het kan wenselijk zijn om interfaces met inkomende of uitgaande Layer 3 of 4 toegangslijsten te vergrendelen om het pakket op het ingangspunt van de router te laten vallen.

Dit garandeert dat CPU-cycli van CUBE worden besteed aan legitiem verkeer. ACLâ€™s naast IP Trusted List en Hostname-validatie bieden een gelaagde aanpak van CUBE-beveiliging.

Op zone gebaseerde firewall (ZBFW)

Cisco CUBE kan naast IOS-XE ZBFW worden geconfigureerd om toepassingsinspectie en andere beveiligingsfuncties te bieden.

Raadpleeg de CUBE- en ZBFW-gids voor meer informatie over dit onderwerp:

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.