Guida Cisco per fortificare i dispositivi Enterprise Cisco Unified Border Element (CUBE)

Sommario

Introduzione

Questo documento aiuta a proteggere e rafforzare i dispositivi Cisco IOS e IOS-XE che operano con Session Border Controller (SBC) con Cisco Unified Border Element (CUBE) Enterprise.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

- CUBE Enterprise con IOS-XE 17.10.1a.

Nota:

Il fatto che alcune funzionalità descritte in questo documento potrebbero non essere disponibili nelle versioni precedenti di IOS-XE. Nei casi in cui è possibile, è stata prestata attenzione nel documentare quando un comando o una funzionalità è stata introdotta o modificata.

Il presente documento non è applicabile a CUBE Media Proxy, CUBE Service Provider, MGCP o SCCP Gateway, Cisco SRST o ESRST Gateway, H323 Gateway o altri gateway voce analogici/TDM.

Premesse

Questo documento offre un'aggiunta a quanto contenuto nella Guida Cisco per fortificare i dispositivi Cisco IOS. Di conseguenza, gli elementi duplicati di tale documento non verranno duplicati nel documento.

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

Cisco virtual CUBE che utilizza IOS-XE 16.9+ su un CSR1000v o CAT8000v può utilizzare il comando **cc-mode** per abilitare l'applicazione di un Common Criteria (CC) e della Certificazione Federal Information Standards (FIPS) su vari moduli di crittografia, come quelli trovati in Transport Layer Security (TLS) e . Non esiste un comando equivalente per CUBE in esecuzione sui router hardware, ma nelle sezioni successive verranno illustrati i metodi per abilitare manualmente una protezione avanzata simile.

Fonte: 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

TLS (Transport Layer Security) e PKI (Public Key Infrastructure)

In questa sezione verranno illustrati gli elementi relativi a TLS e PKI che possono migliorare la protezione fornita da tali protocolli insieme alle operazioni SIP (Secure Session Initial Protocol) e SRTP (Secure Real Time Protocol).

Usa TCP TLS e SRTP

Per impostazione predefinita, il CUBE accetta connessioni SIP in entrata tramite TCP, UDP o SIP TCP-TLS. Le connessioni TCP-TLS avranno esito negativo se non viene configurato alcun valore, mentre TCP e UDP verranno accettati ed elaborati da CUBE. Per le connessioni in uscita, il SIP utilizzerà le connessioni UDP per impostazione predefinita, a meno che non sia presente un comando TCP o TCP-TLS. Analogamente, CUBE negozierà le sessioni RTP (Real Time Protocol) non sicure. Entrambi i protocolli offrono agli utenti non autorizzati ampie opportunità di visualizzare i dati da un flusso multimediale o da una segnalazione di sessione SIP non crittografata. Ove possibile, si consiglia di proteggere la segnalazione SIP con SIP TLS e il flusso multimediale con SRTP.

Fare riferimento alla guida alla configurazione del protocollo SIP TLS e del protocollo SRTP:

- 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

Tenere presente che la sicurezza è tanto forte quanto il suo collegamento più debole e che SIP-TLS e SRTP devono essere abilitati su tutte le tappe della chiamata tramite CUBE.

Le sezioni rimanenti verranno aggiunte a queste configurazioni predefinite allo scopo di fornire funzionalità di sicurezza aggiuntive:

Disabilita porte SIP non protette

Richiamare la sezione precedente specificando che CUBE accetterà per impostazione predefinita TCP e UDP in entrata per CUBE. Una volta che SIP TLS è in uso per tutti i terminali di chiamata, potrebbe essere opportuno disabilitare la porta di ascolto UDP e TCP SIP non sicura 5060.

Una volta disabilitato, è possibile usare **show sip-ua status**, **show sip connections udp brief** o **show sip connections tcp brief** per confermare che CUBE non è più in ascolto sulla 5060 per le connessioni TCP o SIP UDP in entrata.

<#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 può anche essere configurato per funzionare insieme ai VRF IOS-XE per fornire un'ulteriore segmentazione della rete.

Configurando VRF e associando un'interfaccia abilitata VRF a un dial-peer/tenant, CUBE ascolterà solo le connessioni in entrata per quella combinazione di IP, porta e 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

Applica TLS 1.2

Al momento della scrittura di questo documento, TLS 1.2 è la versione più recente di TLS supportata da CUBE. TLS 1.0 è disabilitato in IOS-XE 16.9 ma TLS 1.1 può essere negoziato. Per limitare ulteriormente le opzioni durante un handshake TLS, un amministratore può forzare l'unica versione disponibile per CUBE Enterprise a TLS 1.2

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

Applica crittografia TLS

Può essere opportuno disattivare la negoziazione in una sessione di cifrature TLS più deboli. A partire da IOS-XE 17.3.1, un amministratore può configurare un profilo TLS che consente all'amministratore di definire esattamente le cifrature TLS da offrire durante una sessione TLS. Nelle versioni precedenti di IOS-XE, il controllo veniva effettuato usando il suffisso **strict-cipher** o **ecdsa-cipher** sul comando **crypto signaling** sip-ua.

Si noti che le cifrature selezionate devono essere compatibili con i dispositivi peer che negoziano SIP TLS con CUBE. Per determinare la migliore crittografia tra tutti i dispositivi, consultare la documentazione del fornitore.

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
!
```

Tutte le altre versioni

<#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
!
```

Utilizzo di chiavi crittografiche di grandi dimensioni

Gli standard di crittografia Cisco di nuova generazione consigliati per il 2048 possono essere utilizzati con le applicazioni TLS 1.2. I comandi seguenti possono essere usati per creare chiavi RSA da usare con le sessioni TLS.

Il comando label consente all'amministratore di specificare facilmente queste chiavi in un trust point e il comando esportabile garantisce che, se necessario, la coppia di chiavi privata/pubblica possa essere esportata con il comando

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..]
```

Utilizza certificati firmati da CA (Certification Authority)

Durante la creazione di certificati di trust e di identità (ID) per l'organizzazione CUBE, gli amministratori devono utilizzare certificati firmati dall'autorità di certificazione anziché certificati autofirmati.

I certificati CA in genere forniscono meccanismi di protezione aggiuntivi, ad esempio CRL (Certificate Revocation List) o URL OCSP (Online Certificate Status Protocol), che possono essere utilizzati dai dispositivi per verificare che il certificato non sia stato revocato. L'utilizzo di catene di CA pubbliche attendibili interrompe la configurazione della relazione di trust sui dispositivi peer che possono avere trust incorporati per CA radice conosciute o già avere trust CA radice per il dominio enterprise.

Inoltre, i certificati CA devono includere il flag CA True in Basic Constraints e il certificato di identità CUBE deve includere il parametro Extended Key Usage di Client Auth abilitato.

Di seguito sono riportati un esempio di certificato CA radice e un certificato ID per CUBE utilizzando:

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..]
```

Utilizza hash avanzati

Quando si configura un trust point per il certificato di identità CUBE, è necessario selezionare algoritmi di hashing avanzati come SHA256, SHA384 o 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
```

Abilita controlli CRL (Certificate Revocation List) o OCSP (Online Certificate Status Protocol)

Per impostazione predefinita, i trust IOS-XE tentano di controllare il CRL elencato all'interno di un certificato durante il comando **crypto pki auth**. Successivamente, durante gli handshake TLS, IOS-XE

esegue anche un altro recupero del CRL basato sul certificato ricevuto per confermare che il certificato è ancora valido. I metodi per la CRL possono essere HTTP o LDAP e la connettività alla CRL deve essere presente affinché questa operazione abbia esito positivo. In altre parole, la risoluzione DNS, il socket TCP e il download di file dal server al router IOS-XE devono essere disponibili, altrimenti il controllo CRL non riuscirà. Analogamente, un trust point IOS-XE può essere configurato per utilizzare il valore OCSP da un'intestazione AuthorityInfoAccess (AIA) all'interno del certificato che esegue query su un risponditore OCSP tramite HTTP per verificare ed eseguire controlli simili. Un amministratore può ignorare il punto di distribuzione OCSP o CRL (CDP) all'interno di un certificato specificando un URL statico in un certificato. L'amministratore può inoltre configurare l'ordine in cui vengono controllati CRL o OCSP presupponendo che entrambi siano presenti.

Molti si limitano a disabilitare i controlli di revoca con **revocation-check none** per semplificare il processo, ma in questo modo un amministratore indebolisce la sicurezza e rimuove il meccanismo di IOS-XE per controllare in modo stateful se un determinato certificato è ancora valido. Ove possibile, gli amministratori devono utilizzare OCSP o CRL per eseguire il controllo dello stato dei certificati ricevuti. Per ulteriori informazioni su CRL o OCSP, vedere il documento seguente:

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

Controllo CRL

<#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
!
```

Controllo OCSP

<#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
!
```

Controllo OCSP e CRL ordinato

<#root>

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

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

Abilita verifica nome comune (CN) e nome alternativo soggetto (SAN)

CUBE può essere configurato in modo da verificare che il CN del certificato o la SAN corrispondano al nome host specificato nel comando **dns: di destinazione della sessione**. In IOS-XE 17.8+ è possibile configurare un profilo TLS tramite profilo tls.

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
```

Tenere presente che la designazione client/server fa riferimento al ruolo dei dispositivi peer nell'handshake TLS

Per illustrare meglio:

- **server di convalida cn-san:** CUBE eseguirà la convalida del nome host dei certificati del *server* peer ricevuti per le connessioni TLS in uscita in cui CUBE è il ruolo del client.

- **client di convalida cn-san:** CUBE eseguirà la convalida del nome host dei certificati *client* peer ricevuti per le connessioni TLS in ingresso in cui CUBE è il ruolo del server.
- **cn-san validate bidirection**: abilita la convalida del nome host per entrambi i ruoli peer durante l'handshake TLS.

Quando si utilizza il comando **cn-san validate client** (o bidirezionale), è necessario configurare una rete SAN in base alla quale eseguire il controllo, poiché la destinazione della sessione è check is only for outbound connections and cn-san validate server.

Convalida nome host client:

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

Convalida nome host server:

```
!
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
!
```

Prima della 17.8.1

Nota: tramite questo metodo è disponibile solo la convalida del nome host del server.

<#root>

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

cn-san-validate server

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

CUBE può anche essere configurato per inviare l'estensione TLS 1.2 SNI (Server Name Indication) con il

nome host FQDN di CUBE all'interno dell'handshake TLS ai dispositivi peer per facilitare le operazioni di convalida del nome host.

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

Nota sulla Mutual TLS di CUBE:

- Per impostazione predefinita, quando CUBE agisce come server TLS (lettura della connessione TLS in ingresso) richiede sempre un certificato client. Non è disponibile alcuna configurazione per disattivare questo comportamento.
- Quando CUBE agisce come client TLS e l'avvio di una connessione TLS in uscita, TLS reciproco dipende dal dispositivo peer che agisce come server TLS. In questo scenario un dispositivo peer potrebbe non richiedere un certificato client da CUBE.
- In entrambi gli scenari, la catena di certificati che CUBE invierebbe è controllata dal **trust point** definito nel profilo TLS o nel comando di segnalazione crittografica.

<#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
!
```

Mapping delle connessioni TLS remote a trust point specifici

Quando si usa il comando **crypto signaling default** sip-ua, **TUTTE** le connessioni TLS in entrata vengono mappate a questa configurazione tramite il profilo tls o i singoli comandi post-fix. Quando si esegue la convalida dei certificati, vengono inoltre controllati tutti i trust point disponibili.

Può essere utile creare configurazioni di profilo TLS specifiche per dispositivi peer specifici basate sull'indirizzo IP per garantire che i parametri di sicurezza definiti vengano applicati esattamente alla sessione TLS. A tale scopo, utilizzare il comando **crypto signaling remote-addr** per definire una subnet

IPv4 o IPv6 da mappare a un profilo tls o a un insieme di comandi di suffisso. È inoltre possibile mappare direttamente i trust point di verifica tramite i comandi **client-vtp**) per bloccare esattamente i trust utilizzati per convalidare i certificati peer.

Il comando seguente riepiloga la maggior parte degli elementi discussi fino a questo punto:

```
!
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
!
```

Per le versioni precedenti questa operazione può essere eseguita nel modo seguente:

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

A partire dalla versione 17.8, è inoltre possibile configurare le porte di ascolto tls-profile e per tenant per **tenant voice class** per fornire ulteriori opzioni di segmentazione su una determinata porta di ascolto.

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

Imponi Strict SRTP

Quando si abilita SRTP su CUBE Enterprise, l'operazione predefinita prevede di non consentire il fallback su RTP.

Ove possibile, utilizzare il protocollo SRTP su tutti gli elementi di chiamata, ma per impostazione predefinita il CUBE eseguirà il protocollo RTP-SRTP in base alle esigenze.

Si noti che CUBE non registra le chiavi SRTP nei debug a partire dalla versione 16.11+

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

Tagliare le cifrature SRTP non protette

Per impostazione predefinita, tutte le cifrature SRTP vengono inviate da CUBE durante la creazione di un'offerta. Un amministratore può ridurre il livello di sicurezza dei cifrari, ad esempio le suite di cifratura AEAD di nuova generazione, utilizzando il comando voice class srtp-crypto in IOS-XE 16.5+.

Questa configurazione può inoltre modificare la preferenza predefinita utilizzata quando CUBE seleziona una cifratura SRTP e crea una risposta a un'offerta con più opzioni disponibili.

Nota: alcuni dispositivi Cisco o peer meno recenti potrebbero non supportare le cifrature AEAD. Per il trim delle suite di cifratura, consultare tutta la documentazione pertinente.

<#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
!
```

Disabilita altri protocolli VoIP inutilizzati

Se H323, MGCP, SCCP, STCAPP, CME, SRST non vengono utilizzati su questo gateway, è opportuno rimuovere le configurazioni per fortificare CUBE.

Disabilita H323 e consenti solo chiamate SIP a SIP

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

Disabilitare MGCP, SCCP, STCAPP, SIP e SCCP SRST.

Nota: alcuni di questi comandi eliminano tutte le altre configurazioni e garantiscono che le funzionalità non vengano utilizzate prima di rimuoverle completamente.

<#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
```

Routing delle chiamate e frodi

Consenti connessioni da indirizzi IP attendibili

Per impostazione predefinita, il CUBE considererà attendibili le connessioni in entrata dagli indirizzi IPv4 e IPv6 configurati nelle configurazioni **server-gruppo di sessioni** dial-peer e **server-**group.

Per aggiungere altri indirizzi IP, usare il comando **ip address trusted list** configurato tramite il **servizio vocale voip.**

Quando la convalida del nome host del client/server viene configurata insieme al SIP TLS mediante la funzione di convalida CN/SAN descritta in precedenza, una convalida CN/SAN riuscita ignorerà i controlli dell'elenco indirizzi attendibili.

Evitare di utilizzare l'autenticazione **attendibile senza indirizzo IP** che consentirà al CUBE di accettare QUALSIASI connessione in ingresso.

```
!
voice service voip
 ip address trusted authenticate

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

Utilizzare **show ip address trusted list** per visualizzare lo stato della verifica degli indirizzi IP e tutte le definizioni di elenchi attendibili statici e dinamici derivate da altre configurazioni.

Si noti che il valore dinamico derivato da un dial-peer/server-group viene rimosso dall'elenco di fiducia quando un dial-peer viene arrestato o impostato sullo stato inattivo dopo controlli keepalive non riusciti.

Per impostazione predefinita, quando una chiamata in entrata non supera il controllo dell'elenco di indirizzi attendibili IP, viene scartata automaticamente, ma è possibile ignorare questa impostazione utilizzando il comando **no silent-scard untrusted** voice service voip > sip per inviare un errore al mittente. Tuttavia, inviando una risposta, un utente non autorizzato può usare questa indicazione per indicare che il dispositivo è in realtà in ascolto del traffico SIP e aumentare i propri sforzi di attacco. Di conseguenza, l'eliminazione invisibile all'utente è il metodo preferibile per la gestione delle eliminazioni dall'elenco di indirizzi attendibili IP.

Evitare il routing dial-peer generico

L'utilizzo di modelli di destinazione generici "catch all", ad esempio **destination-pattern .T**, può aumentare la probabilità di instradare una chiamata fraudolenta tramite CUBE.

Gli amministratori devono configurare CUBE in modo da instradare le chiamate solo per intervalli di numeri di telefono noti o URI SIP.

Per ulteriori informazioni sulle funzioni di instradamento delle chiamate CUBE, vedere il documento seguente:

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

Riduzione delle minacce CUBE

Gestione pacchetti in formato non valido

Per impostazione predefinita, il CUBE ispeziona i pacchetti SIP e RTP per verificare la presenza di errori e li scarta.

Pacchetti RTP non autorizzati

Per impostazione predefinita, IOS-XE CUBE esegue la convalida della porta di origine per tutti i flussi RTP/RTCP consentendo solo le connessioni negoziate tramite segnalazione offerta/risposta SDP SIP e non può essere disabilitato.

È possibile monitorare queste impostazioni eseguendo il seguente comando:

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

Per l'interoperabilità con CUCM, si consiglia di abilitare lo streaming multimediale duplex tramite il servizio Cisco CallManager per evitare che la musica in attesa venga eliminata quando originata dalla porta 4000.

Protezione avanzata intervallo porte RTP

Per impostazione predefinita, IOS-XE utilizza l'intervallo di porte da 8000 a 48198. È possibile configurare questa opzione su un intervallo diverso, ad esempio da 16384 a 32768, tramite il seguente comando:

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

Gli amministratori possono inoltre configurare intervalli di porte RTP per intervalli di indirizzi IPv4 e IPv6.

Questa configurazione consente anche all'applicazione VoIP di CUBE di eseguire la gestione dei pacchetti fantasma in modo più efficiente evitando di reindirizzare questi pacchetti al processo UDP sulla CPU del router, poiché l'intervallo di porte e IP sono definiti in modo statico. In questo modo è possibile ridurre il

numero elevato di CPU quando si gestiscono un numero elevato di pacchetti RTP legittimi o non legittimi ignorando il comportamento di punzonatura della CPU.

```
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

Prevenzione di Denial of Service (DOS)

Le funzioni di controllo dell'ammissione di chiamata possono essere attivate per limitare le chiamate in base a chiamate totali, CPU, memoria, larghezza di banda. È inoltre possibile rilevare picchi di chiamate per rifiutare le chiamate e impedire la negazione del servizio.

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

Nascondi indirizzo

Per impostazione predefinita, il cubo sostituirà gli indirizzi IP nelle intestazioni SIP, ad esempio Via, Contatto e Da, con il proprio indirizzo IP.

Questa opzione può essere estesa alle intestazioni Referred-To, Referred-By, 3xx contact header, History-Info e Diversion applicando il comando **voip** command **address-hiding**.

Inoltre, viene creato un nuovo ID chiamata per ogni indirizzo IP di mitigazione call-leg che può essere incorporato in questo valore di intestazione.

Se è necessario un nome host al posto di un indirizzo IP per nascondere gli indirizzi, è possibile configurare il comando **voice-class sip localhost dns:cube.cisco.com**.

Privacy ID chiamante

CUBE può essere configurato per eliminare i valori del nome ID chiamante dalle intestazioni SIP con il comando **clid-strip name** configurato su qualsiasi dial-peer.

CUBE può inoltre interagire e comprendere le intestazioni di privacy SIP, quali P-Preferred Identity (PPID), P-Asserted Identity (PAY), Privacy, P-Called Party Identity (PCPID), Remote-Party Identity (RPID). Per ulteriori informazioni, consultare il documento seguente: 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

Autenticazione digest SIP

Durante la registrazione SIP da parte di CUBE a un provider di servizi o durante una segnalazione di chiamata i dispositivi UAS a monte possono restituire un codice di stato 401 o 407 con un campo di intestazione WWW-Authenticate/Proxy-Authenticate applicabile che richiede l'autenticazione di CUBE. Durante questo handshake CUBE supporta l'algoritmo MD5 per il calcolo del valore del campo

dell'intestazione Authorization in una richiesta successiva.

Intestazioni SIP o SDP non supportati

CUBE eliminerà le intestazioni SIP o SDP non supportate che non è in grado di comprendere. È necessario prestare attenzione quando si utilizzano comandi quali **pass-thru content sdp**, **pass-thru content unsupp** o **pass-through headers unsupp** per garantire quali dati passano attraverso CUBE.

Rimozione o modifica delle intestazioni SIP o SDP

Laddove è richiesto un controllo aggiuntivo, i profili SIP in entrata o in uscita possono essere configurati da un amministratore per modificare in modo flessibile o eliminare completamente un'intestazione SIP o un attributo SDP.

Consultare i seguenti documenti sull'utilizzo del profilo SIP:

- 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

Altre funzioni di sicurezza

Password crittografate

CUBE richiede password crittografate per la versione 16.11 e successive per crittografare la registrazione SIP e altre password IOS-XE nella configurazione corrente.

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

Elenchi di accesso

La funzionalità Elenco attendibile funziona al livello 7 all'interno dell'applicazione CUBE. Quando il pacchetto viene scartato in modo invisibile all'utente, il CUBE ha già iniziato l'elaborazione del pacchetto.

Può essere opportuno bloccare le interfacce con elenchi degli accessi di layer 3 o 4 in entrata o in uscita per rilasciare il pacchetto sul punto di ingresso del router.

In questo modo i cicli della CPU da CUBE vengono utilizzati per il traffico legittimo. Gli ACL, insieme all'elenco di attendibilità IP e alla convalida del nome host, forniscono un approccio su più livelli alla sicurezza CUBE.

Zone-Based Firewall (ZBFW)

Cisco CUBE può essere configurato insieme a IOS-XE ZBFW per fornire l'ispezione delle applicazioni e altre funzioni di sicurezza.

Per ulteriori informazioni su questo argomento, consultare la guida CUBE and ZBFW Guide:

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).