Guia da Cisco para fortalecer os dispositivos corporativos do Cisco Unified Border Element (CUBE)

Contents

Introduction

Este documento o ajudará a proteger e fortalecer os dispositivos Cisco IOS e IOS-XE que atuam como

Session Border Controller (SBC) executando o Cisco Unified Border Element (CUBE) Enterprise.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

- CUBE Enterprise executando IOS-XE 17.10.1a.

Note:

Que alguns recursos detalhados neste documento podem não estar disponíveis em versões mais antigas do IOS-XE. Onde possível, foi tomado cuidado para documentar quando um comando ou recurso foi introduzido ou modificado.

Este documento não se aplica ao CUBE Media Proxy, ao CUBE Service Provider, aos gateways MGCP ou SCCP, aos gateways Cisco SRST ou ESRST, aos gateways H323 ou a outros gateways de voz analógicos/TDM.

Informações de Apoio

Este documento serve como uma adição ao que pode ser encontrado no Guia da Cisco para Fortalecer os Dispositivos IOS Cisco. Como tal, quaisquer itens duplicados desse documento não serão duplicados neste documento.

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

O Cisco Virtual CUBE que utiliza IOS-XE 16.9+ em um CSR1000v ou CAT8000v pode utilizar o comando **cc-mode** para ativar uma aplicação de certificação Common Criteria (CC) e The Federal Information Standards (FIPS) em vários módulos criptográficos, como aqueles encontrados em Transport Layer Security (TLS) e . Não há nenhum comando equivalente para o CUBE em execução nos roteadores de hardware, mas as seções posteriores fornecerão métodos para ativar o endurecimento semelhante manualmente.

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, infraestrutura de chave pública)

Esta seção discutirá os itens sobre TLS e PKI que podem aprimorar a segurança fornecida por esses protocolos junto com as operações do protocolo SIP e do protocolo SRTP.

Usar TCP TLS e SRTP

Por padrão, o CUBE aceitará conexões SIP de entrada via TCP, UDP ou SIP TCP-TLS. Enquanto as conexões TCP-TLS falharão se nada for configurado, o TCP e o UDP serão aceitos e processados pelo

CUBE. Para conexões de saída, o SIP utilizará conexões UDP por padrão, a menos que um comando TCP ou TCP-TLS esteja presente. Da mesma forma, o CUBE negociará sessões não seguras do Protocolo de Tempo Real (RTP). Esses dois protocolos fornecem ampla oportunidade para que um invasor obtenha dados de uma sinalização de sessão SIP não criptografada ou de um fluxo de mídia. Sempre que possível, recomenda-se proteger a Sinalização SIP com SIP TLS e o fluxo de mídia com SRTP.

Consulte a configuração SIP TLS e o guia de configuração do 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

Lembre-se de que a segurança é tão forte quanto o link mais fraco, e o SIP-TLS e o SRTP devem ser ativados em todos os trechos de chamada através do CUBE.

As seções restantes serão adicionadas a essas configurações padrão em um esforço para fornecer recursos de segurança adicionais:

Desative portas SIP não seguras

Lembre-se da seção anterior detalhada que o CUBE aceitará TCP e UDP de entrada para CUBE por padrão. Uma vez que o SIP TLS esteja sendo usado para todos os trechos de chamada, talvez seja conveniente desativar a porta UDP e TCP SIP Listen não segura 5060.

Uma vez desativado, você pode usar **show sip-ua status**, **show sip connections udp brief** ou **show sip connections tcp brief** para confirmar se o CUBE não está mais escutando no 5060 para conexões SIP de entrada TCP ou UDP.

<#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

O CUBE também pode ser configurado para funcionar junto com VRFs IOS-XE para fornecer segmentação de rede adicional.

Ao configurar VRFs e vincular uma interface habilitada para VRF a um peer de discagem/locatário, o CUBE somente ouvirá as conexões de entrada para essa combinação de 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

Aplicar TLS 1.2

No momento em que este documento foi escrito, o TLS 1.2 era a versão mais recente do TLS suportada pelo CUBE. O TLS 1.0 está desabilitado no IOS-XE 16.9, mas o TLS 1.1 pode ser negociado. Para limitar ainda mais as opções durante um handshake TLS, um administrador pode forçar a única versão disponível do CUBE Enterprise para TLS 1.2

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

Aplicar cifras TLS

Pode ser desejável desativar as cifras TLS mais fracas para que não sejam negociadas em uma sessão. A partir do IOS-XE 17.3.1, um administrador pode configurar um perfil TLS que permita a um administrador definir exatamente quais cifras TLS serão oferecidas durante uma sessão TLS. Em versões mais antigas do IOS-XE, isso era controlado usando o **sufixo strict-cipher** ou **ecdsa-cipher** no comando **crypto signaling** sip-ua.

Observe que as cifras selecionadas devem ser compatíveis com dispositivos pares que negoceiam SIP TLS com CUBE. Consulte toda a documentação aplicável do fornecedor para determinar as melhores cifras entre todos os dispositivos.

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
!
```

Todas as outras versões

<#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
!
```

Utilizar chaves criptográficas grandes

Padrões Cisco Next Generation Cryptography recomendados 2048 para uso com aplicações TLS 1.2. Os comandos abaixo podem ser usados para criar chaves RSA para uso com sessões TLS.

O comando label permite que um administrador especifique facilmente essas chaves em um ponto confiável e o comando exportável garante que, se necessário, o par de chaves privado/público possa ser exportado com o comando, como

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..]
```

Utilizar Certificados Assinados pela Autoridade de Certificação (CA)

Os administradores devem utilizar certificados assinados pela CA em vez de certificados autoassinados ao criar certificados de ponto de confiança e identidade (ID) para o CUBE Enterprise.

Os certificados CA geralmente fornecem mecanismos de segurança adicionais, como CRL (Certificate Revocation List) ou URLs do protocolo de status de certificados online (OCSP), que podem ser usados por dispositivos para garantir que o certificado não foi revogado. O uso de cadeias CA públicas confiáveis facilita a configuração da relação de confiança em dispositivos pares que podem ter confiança incorporada para CAs raiz bem conhecidas ou que já têm relações de confiança de CA raiz para o seu domínio corporativo.

Além disso, os certificados de CA devem incluir o indicador de CA verdadeiro em restrições básicas e o certificado de identidade do CUBE deve incluir o parâmetro de uso de chave estendida de autenticação de cliente habilitada.

Um exemplo de certificado de CA raiz e um certificado de ID para CUBE são mostrados abaixo usando:

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..]
```

Utilizar hashes fortes

Ao configurar um ponto de confiança para o Certificado de identidade do CUBE, selecione algoritmos de hash fortes, como SHA256, SHA384 ou 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

Habilitar Verificações de Lista de Certificados Revogados (CRL) ou Protocolo de Status de Certificados Online (OCSP)

Por padrão, os pontos de confiança IOS-XE tentarão verificar a CRL listada em um certificado durante o comando **crypto pki auth**, mais tarde durante os handshakes TLS, o IOS-XE também executará outra busca de CRL com base no certificado recebido para confirmar se o certificado ainda é válido. Os métodos para CRL podem ser HTTP ou LDAP e a conectividade com a CRL precisa estar presente para que isso tenha êxito. Ou seja, a resolução DNS, o soquete TCP e o download de arquivos do servidor para o roteador IOS-XE precisam estar disponíveis, caso contrário, a verificação de CRL falhará. Da mesma forma, um ponto confiável IOS-XE pode ser configurado para utilizar o valor OCSP de um cabeçalho AuthorityInfoAccess (AIA) dentro do certificado que executa consultas de um Respondente OCSP via HTTP para verificar e executar verificações semelhantes. Um administrador pode substituir o OCSP ou o CRL Distribution Point (CDP) em um certificado, fornecendo uma URL estática em um certificado. Além disso, um administrador também pode configurar a ordem na qual a CRL ou o OCSP são verificados, supondo que ambos estejam presentes.

Muitos simplesmente desabilitam verificações de revogação com **revocation-check none** para simplificar o processo, mas ao fazê-lo um administrador enfraquece a segurança e remove o mecanismo do IOS-XE para verificar de forma stateful se um determinado certificado ainda é válido. Sempre que possível, os administradores devem utilizar o OCSP ou a CRL para executar a verificação stateful dos certificados recebidos. Para obter mais informações sobre CRL ou OCSP, consulte o seguinte documento:

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

Verificação de 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
!
```

Verificação 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
!
```

Verificação de OCSP e CRL Solicitada

<#root>

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

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

Habilitar verificação de CN (Common Name, nome comum) e SAN (Subject Alternate Name, nome alternativo do assunto)

O CUBE pode ser configurado para verificar se o CN ou SAN do certificado corresponde ao nome de host do comando **session target dns:** . No IOS-XE 17.8+, um perfil TLS pode ser configurado através do perfil 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
```

Lembre-se de que a designação de cliente/servidor é uma referência à função de dispositivos pares no handshake TLS

Para ilustrar melhor:

- **cn-san validate server: o** CUBE executará a validação do nome de host dos *certificados de* servidor *de* mesmo nível recebidos para conexões TLS de saída, em que CUBE é a função do cliente.
- **cn-san validate client: o** CUBE executará a validação do nome de host dos *certificados de cliente de* mesmo nível recebidos para conexões TLS de entrada, em que CUBE é a função do servidor.
- **cn-san validate bidirection**: habilita a validação do nome de host para ambas as funções de peer durante o handshake TLS.

Ao usar o comando **cn-san validate client** (ou bidirectional), você deve configurar uma SAN para verificação, já que o destino da sessão é verificado somente para conexões de saída e servidor cn-san validate.

Validação do nome de host do cliente:

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

Validação do nome de host do servidor:

```
!
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
!
```

Anterior a 17.8.1

Observação: somente a validação do nome de host do servidor está disponível por meio desse método.

<#root>

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

cn-san-validate server

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

O CUBE também pode ser configurado para enviar a extensão Server Name Indication (SNI) TLS 1.2 com o nome de host FQDN do CUBE dentro do handshake TLS para dispositivos pares, a fim de facilitar seus esforços de validação de nome de host.

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

Uma observação sobre o TLS mútuo do CUBE:

- Por padrão, quando o CUBE estiver atuando como um servidor TLS (leia a conexão TLS de entrada), ele sempre solicitará um certificado de cliente. Não há configuração para desativar esse comportamento.
- Quando o CUBE está atuando como um cliente TLS e iniciando uma conexão TLS de saída, o TLS mútuo depende do dispositivo par que está atuando como um servidor TLS. Neste cenário, um dispositivo de mesmo nível não pode solicitar um certificado de cliente do CUBE.
- Em ambos os cenários, a cadeia de certificados que o CUBE enviaria é controlada pelo **ponto confiável** definido no perfil TLS ou no comando crypto signaling.

<#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
!
```

Mapear conexões TLS remotas para pontos de confiança específicos

Ao usar o comando **crypto signaling default** sip-ua **ALL** as conexões TLS de entrada são mapeadas para essas configurações por meio de comandos tls-profile ou post-fix individuais. Além disso, todos os pontos de confiança disponíveis são verificados durante a validação do certificado.

Pode ser desejável criar configurações de perfil TLS específicas para um dispositivo de peer específico com base no endereço IP para garantir que exatamente os parâmetros de segurança definidos sejam aplicados a essa sessão TLS. Para fazer isso, use o comando **crypto signaling remote-addr** para definir uma sub-rede IPv4 ou IPv6 para mapear para um perfil tls ou um conjunto de comandos postfix. Você também pode mapear diretamente o ponto de confiança de verificação através de **comandos client-vtp**) para bloquear exatamente quais pontos de confiança são usados para validar certificados de pares.

O comando abaixo resume a maioria dos itens discutidos até este ponto:

```
!
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
!
```

Para versões mais antigas, isso pode ser feito da seguinte forma:

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

A partir da versão 17.8, você também pode configurar as portas de escuta por usuário e por perfil de tls por **locatário de classe de voz** para fornecer mais opções de segmentação em uma determinada porta de escuta.

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

Aplicar SRTP estrito

Ao ativar o SRTP no CUBE Enterprise, a operação padrão é não permitir fallback para RTP.

Quando possível, use o SRTP em todos os trechos de chamada; no entanto, por padrão, o CUBE executará o RTP-SRTP conforme necessário.

Observe que o CUBE não registra as chaves SRTP nas depurações iniciadas em 16.11+

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

Aparar cifras de SRTP não seguras

Por padrão, todas as cifras SRTP são enviadas pelo CUBE durante a criação de uma oferta. Um administrador pode reduzir para cifras mais seguras, como os conjuntos de cifras AEAD de próxima geração, usando o comando voice class srtp-crypto no IOS-XE 16.5+.

Essa configuração também pode alterar a preferência padrão usada quando o CUBE seleciona uma cifra SRTP e cria uma resposta para alguma oferta com várias opções disponíveis.

Observação: alguns dispositivos Cisco mais antigos ou dispositivos pares podem não suportar cifras AEAD. Consulte toda a documentação aplicável ao aparar conjuntos de cifras.

<#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
!
```

Desative outros protocolos VoIP não utilizados

Se H323, MGCP, SCCP, STCAPP, CME, SRST não estiverem sendo usados nesse gateway, vale a pena remover as configurações para fortalecer o CUBE.

Desabilite o H323 e permita apenas chamadas SIP para SIP

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

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

Observação: alguns desses comandos excluirão todas as outras configurações, verifique se os recursos não estão sendo usados antes de removê-los 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
```

Roteamento de chamadas e fraude de tarifas

Permitir conexões de IPs confiáveis

Por padrão, o CUBE confiará em conexões de entrada de endereços IPv4 e IPv6 configurados em **configurações de destino de sessão de** peer de discagem e **grupo de servidores de classe de voz**.

Para adicionar endereços IP adicionais, utilize o **comando ip address trusted list** configurado via **voice service voip.**

Quando a validação de nome de host cliente/servidor é configurada junto com o SIP TLS por meio do recurso de validação CN/SAN discutido anteriormente, uma validação CN/SAN bem-sucedida ignorará as verificações de lista confiável de endereços IP.

Evite usar **no ip address trusted authenticate** que permitirá que o CUBE aceite QUALQUER conexão de entrada.

```
!
voice service voip
 ip address trusted authenticate

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

Use **show ip address trusted list** para exibir o status da verificação de Endereço IP e todas as definições de lista confiável estática e dinâmica derivadas de outras configurações.

Observe que o valor dinâmico derivado de um peer de discagem/grupo de servidores é removido da lista confiável quando um peer de discagem é desligado ou definido para o estado inativo após falhar nas verificações de keepalive.

Por padrão, quando uma chamada de entrada não passa pela verificação da lista IP confiável, ela é descartada silenciosamente, mas pode ser substituída usando o comando **no silent-discard untrusted** voice service voip > sip para enviar um erro de volta ao remetente. No entanto, ao enviar uma resposta, um invasor pode usar isso para indicar que o dispositivo está realmente ouvindo o tráfego SIP e intensificar seus esforços de ataque. Como tal, o descarte silencioso é o método preferencial de tratamento de descartes de

Lista Confiável IP.

Evite o roteamento de peer de discagem genérico

O uso de padrões de destino genéricos "catch all", como **destination-pattern .T** , pode aumentar a probabilidade de roteamento de uma chamada fraudulenta por meio do CUBE.

Os administradores devem configurar o CUBE para rotear apenas chamadas para intervalos de números de telefone conhecidos ou URIs SIP.

Consulte o seguinte documento para obter uma explicação maior sobre os recursos de roteamento de chamadas do 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

Atenuação de ameaças do CUBE

Manipulação de pacotes malformados

Por padrão, o CUBE inspecionará os pacotes SIP e RTP para verificar se há erros e descartar o pacote.

Pacotes RTP invasores

Por padrão, o IOS-XE CUBE executa a validação da porta de origem para todos os fluxos de RTP/RTCP permitindo apenas conexões negociadas via sinalização de oferta/resposta SIP SDP e não pode ser desabilitado.

Eles podem ser monitorados verificando o seguinte comando:

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

Para a interoperabilidade com o CUCM, é recomendável habilitar o fluxo de mídia duplex através do Cisco CallManager Service para evitar que o Music on Hold seja descartado quando for originado da porta 4000.

Fortalecimento do Intervalo de Portas RTP

Por padrão, o IOS-XE usa o intervalo de portas de 8000 a 48198. Isso pode ser configurado para um intervalo diferente, como 16384 por 32768, por meio do seguinte comando:

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

Um administrador também pode configurar intervalos de portas RTP por Intervalos de Endereços IPv4 e IPv6.

Essa configuração também permite que o aplicativo VoIP do CUBE execute o tratamento de pacotes fantasmas com mais eficiência, não direcionando esses pacotes para o processo UDP na CPU do Roteador, já que o IP e o intervalo de portas estão definidos estaticamente. Isso pode ajudar a reduzir a utilização elevada de CPU ao manipular um grande número de pacotes RTP legítimos ou ilegítimos, ignorando o comportamento de punting da 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

Prevenção contra negação de serviço (DOS)

Os recursos de controle de admissão de chamadas podem ser ativados para limitar chamadas com base no total de chamadas, CPU, memória, largura de banda. Além disso, os picos de chamada podem ser detectados para rejeitar chamadas e impedir a negação de serviço.

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

Ocultação de endereço

Por padrão, o CUBE substituirá os endereços IP em cabeçalhos SIP como, mas não limitado a Via, Contact e From, por seu próprio endereço IP.

Isso pode ser estendido para os cabeçalhos Refer-To, Referred-By, 3xx contact header, History-Info e Diversion aplicando o comando **voice service voip address-hide**.

Além disso, uma nova ID de chamada é criada para cada endereço IP de mitigação do leg da chamada que pode ser incorporado nesse valor de cabeçalho.

Quando um nome de host é exigido no lugar de um endereço IP para fins de ocultação de endereço, o comando **voice-class sip localhost dns:cube.cisco.com** pode ser configurado.

Privacidade de identificador de chamada

O CUBE pode ser configurado para descartar valores de Nome de ID de chamador de Cabeçalhos SIP com o comando **clid-strip name** configurado em qualquer peer de discagem.

Além disso, o CUBE pode interagir e entender cabeçalhos de privacidade do SIP, como PPID (P-Preferred Identity, Identidade Preferencial), PAID (P-Asserted Identity, Identidade de quem recebeu a chamada), PCPID (Remote-Party Identity, Identidade de quem recebeu a chamada). Para obter mais informações, consulte o seguinte documento: 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

Autenticação Digest do SIP

Durante o registro do SIP pelo CUBE para um provedor de serviços ou durante uma chamada, os dispositivos de UAS upstream de sinalização podem retornar um código de status 401 ou 407 com um campo de cabeçalho WWW-Authenticate/Proxy-Authenticate aplicável desafiando o CUBE a autenticar. Durante esse handshake, o CUBE suporta o algoritmo MD5 para calcular o valor do campo do cabeçalho de autorização em uma solicitação substituta.

Cabeçalhos SIP ou SDP sem suporte

O CUBE removerá cabeçalhos SIP ou SDP sem suporte que não entenda. Deve-se tomar cuidado ao usar comandos como **pass-thru content sdp**, **pass-thru content unsupp** ou **pass-through headers unsupp** para garantir que os dados estão passando pelo CUBE.

Remoção ou modificação de cabeçalhos SIP ou SDP

Onde o controle adicional é necessário, os perfis SIP de entrada ou saída podem ser configurados por um administrador para modificar com flexibilidade ou descartar diretamente um cabeçalho SIP ou atributo SDP.

Consulte os seguintes documentos sobre o uso do Perfil 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

Outros recursos de segurança

Senhas criptografadas

O CUBE requer senhas criptografadas para 16.11 e versões posteriores para criptografar o Registro SIP e outras senhas do IOS-XE na configuração em execução.

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

Listas de acesso

O recurso de lista confiável opera na camada 7 dentro do aplicativo CUBE. Quando o pacote é descartado silenciosamente, o CUBE já começou a processá-lo.

Pode ser desejável bloquear interfaces com listas de acesso de entrada ou saída das camadas 3 ou 4 para descartar o pacote no ponto de entrada do roteador.

Isso garante que os ciclos de CPU do CUBE sejam gastos em tráfego legítimo. As ACLs, juntamente com a lista confiável de IP e a validação de nome de host, fornecem uma abordagem em camadas para a segurança do CUBE.

Firewall baseado em zona (ZBFW)

O Cisco CUBE pode ser configurado juntamente com o IOS-XE ZBFW para fornecer inspeção de aplicativos e outros recursos de segurança.

Consulte o Guia CUBE e ZBFW para obter mais informações sobre este tópico:

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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.