Unified Communications Manager Express voor fraudepreventie

Inhoud

Inleiding

Dit document biedt een configuratiehandleiding die kan worden gebruikt om te helpen een Cisco Communications Manager Express (CME)-systeem te beveiligen en de dreiging van tolfraude te beperken. CME is de op de router gebaseerde Call Control-oplossing van Cisco die een slimme, eenvoudige en veilige oplossing biedt voor organisaties die Unified Communications willen implementeren. Het is zeer bemoedigend dat u de in dit document beschreven beveiligingsmaatregelen doorvoert om extra beveiligingsniveaus te waarborgen en de mogelijkheid van tolfraude te beperken.

Het doel van dit document is u te informeren over de verschillende beveiligingsgereedschappen

die beschikbaar zijn op Cisco Voice Gateways en CME. Deze instrumenten kunnen in een CME-systeem worden geïmplementeerd om de dreiging van tolfraude door zowel interne als externe partijen te helpen verminderen.

Dit document bevat instructies over de manier waarop u een CME-systeem kunt configureren met verschillende gereedschappen voor tolbeveiliging en functiebeperking. Het document schetst ook waarom bepaalde beveiligingsgereedschappen in bepaalde implementaties worden gebruikt.

De algemene inherente flexibiliteit van Cisco ISR platforms staat u toe om CME in vele verschillende types van implementaties in te zetten. U moet dus een combinatie gebruiken van de functies die in het document worden beschreven, om het CME-programma te helpen sluiten. Dit document dient als richtsnoer voor de toepassing van beveiligingsinstrumenten op CME en garandeert op geen enkele manier dat er geen sprake zal zijn van fraude met tolgelden of misbruik door zowel interne als externe partijen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unified Communications Manager Express

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Unified Communications Manager Express 4.3 en CME 7.0.

Opmerking: Cisco Unified CME 7.0 heeft dezelfde functies als Cisco Unified CME 4.3 en is hernummerd tot 7.0 om deze uit te lijnen met Cisco Unified Communications-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Overzicht

Dit document bestrijkt de meest gebruikelijke beveiligingsinstrumenten die op een CME-systeem kunnen worden gebruikt om de dreiging van tolfraude te verminderen. De in dit document genoemde CME-beveiligingstools omvatten tolbeperkingsgereedschappen en gereedschappen voor functiebeperkingen.

Tools voor tolbeperking

- Direct-inward-dial
- Beperking van het aantal nauren
- Beperkingsklasse
- Toegangslijst om de toegang tot H323/SIP-romp te beperken

Tools voor functiebeperking

- overdrachtspatroon
- Verschuivingspatroon geblokkeerd
- Overschrijving max. lengte
- Bel een voorwaartse max-lengte
- Geen vervroegde lokale oproepen
- Geen autoreg-telefoon

Cisco Unity Express restrictietools

- Secure Cisco Unity Express PSTN-toegang
- Beperking van berichtgeving

Vastlegging gesprekken

- Vastlegging oproepen om records voor gespreksdetails (CDR's) op te nemen

Interne vs. externe bedreigingen

In dit document wordt ingegaan op bedreigingen van zowel interne als externe partijen. De interne partijen omvatten IP telefoongebruikers die op een CME systeem wonen. Externe partijen omvatten gebruikers op buitenlandse systemen die kunnen proberen het host CME te gebruiken om frauduleuze oproepen te doen en de gesprekken aan uw CME-systeem terug te laten betalen.

Tools voor tolbeperking

Direct-inward-dial

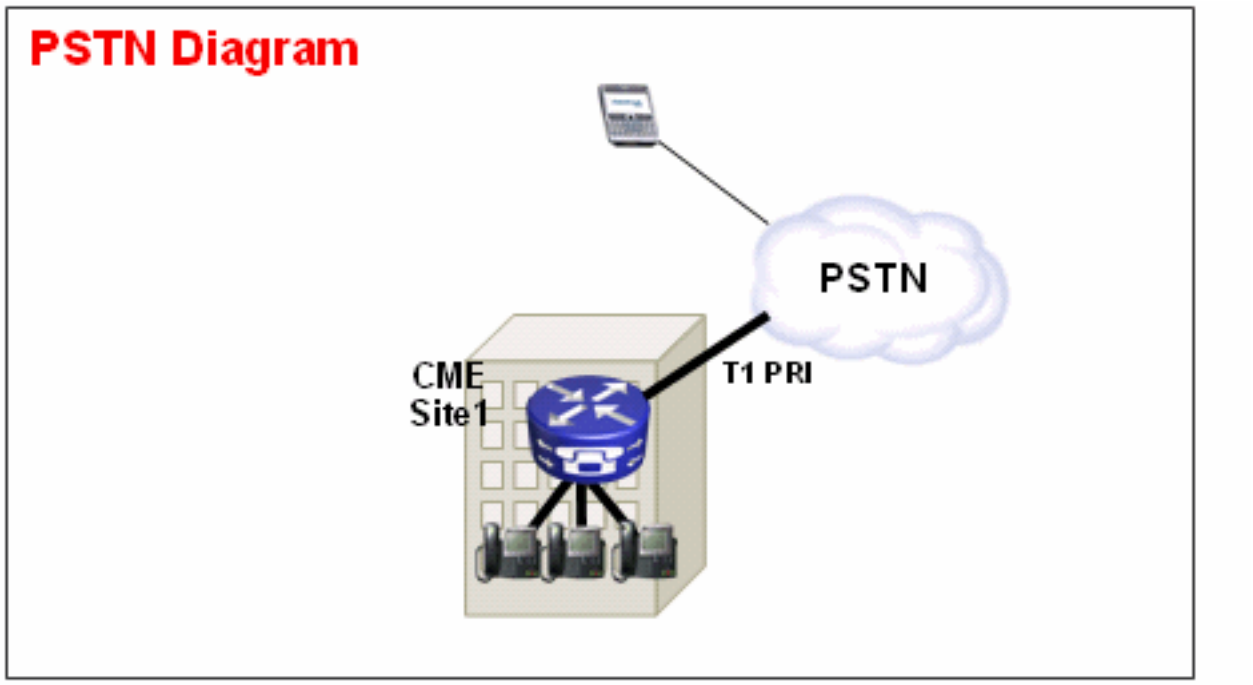
Abstract

Direct-Inward-dial (DID) wordt gebruikt op de spraakgateways van Cisco om de gateway toe te staan om een inkomende vraag te verwerken nadat het cijfers van de PBX of de CO switch ontvangt. Als DID is ingeschakeld, geeft de Cisco-gateway geen secundaire kiestoon voor de beller weer en wacht u niet op het verzamelen van extra cijfers bij de beller. Het zendt de oproep rechtstreeks naar de bestemming die overeenkomt met de inkomende Dited Nummeridentificatieservice (DNIS). Dit heet eenfasig draaien.

Opmerking: dit is een **externe dreiging**.

Probleemverklaring

Als Direct-Inward-dial NIET op een gateway van Cisco of CME wordt gevormd, wanneer een vraag van de CO of PBX aan de gateway van Cisco komt, hoort de caller een secundaire kiestoon. Dit heet tweefasendraaien. Zodra de PSTN-bellers de secundaire kiestoon horen, kunnen ze cijfers invoeren om een interne extensie te bereiken of als ze de PSTN-toegangscode kennen, kunnen ze lange afstand of internationale nummers bellen. Dit leidt tot een probleem omdat de PSTN-beller het CME-systeem kan gebruiken om uitgaande langeafstandsgesprekken of internationale gesprekken te plaatsen en het bedrijf wordt belast met de gesprekken.



[Voorbeeld 1]

Op site 1 is het CME verbonden met het PSTN via een T1 PRI romp. De PSTN-provider levert de **40855512.** DID-bereik voor CME Site 1. Alle PSTN-oproepen die bestemd zijn voor 4085551200 - 4085551299 worden naar de CME gestuurd. Als u geen **direct-naar-binnen-wijzerplaat** vormt op het systeem, hoort een inkomende PSTN beller een secundaire kiestoon en moet de interne extensie handmatig bellen. Het grotere probleem is dat als de beller een misbruiker is en de PSTN-toegangscode op het systeem kent, algemeen **9**, ze **9** dan elk doelnummer kunnen bellen dat ze willen bereiken.

Oplossing 1

Om deze dreiging te verzachten moet u de **knop direct naar binnen** configureren. Dit veroorzaakt de gateway van Cisco om de inkomende vraag rechtstreeks naar de bestemming door te sturen die de inkomende DNIS aanpast.

Monsterconfiguratie

```
dial-peer voice 1 pots
port 1/0:23
incoming called-number .
direct-inward-dial
```

Zorg ervoor dat DID correct werkt, dat de inkomende aanroep overeenkomt met de juiste POTS dial-peer waar de **direct-inward-dial** opdracht is geconfigureerd. In dit voorbeeld, wordt T1 PRI aangesloten op poort 1/0:23. Om de juiste binnenkomende wijzerplaat te passen geef het

inkomende vraag de **vraag** terug **het** peer bevel van **het** aantal bellen onder de DID POTS kiespeer uit.

Voorbeeld 2

Op site 1 is het CME verbonden met het PSTN via een T1 PRI romp. De PSTN-aanbieder geeft de **40855512..** en **40855513..** DID-bereik voor CME Site 1. Dus alle PSTN-oproepen die bestemd zijn voor 4085551200 - 4085551299 en 40855551300 - 408551399 worden ingestuurd. gebonden aan het CME.

Onjuiste configuratie:

Als u een inkomende wijzerplaat-peer vormt, zoals in de steekproefconfiguratie in deze sectie, treedt de mogelijkheid voor tolfraude nog steeds op. Het probleem met deze inkomende kies-peer is dat het slechts inkomende vraag aan **40852512** aansluit en dan de DID dienst toepast. Als een PSTN-gesprek in **40852513** komt.. komt de inkomende post-dial-peers niet overeen en wordt de DID-service niet toegepast. Als een inkomende dial-peer met DID niet wordt aangepast, dan wordt de standaard wijzerplaat-peer 0 gebruikt. DID is standaard uitgeschakeld aan dial-peers 0.

Monsterconfiguratie

```
dial-peer voice 1 pots
incoming called-number 40855512..
direct-inward-dial
```

Configuratie corrigeren

De juiste manier om de dienst DID op een inkomende wijzerplaat-peer te vormen wordt in dit voorbeeld getoond:

Monsterconfiguratie

```
dial-peer voice 1 pots
port 1/0:23
incoming called-number .
direct-inward-dial
```

Raadpleeg DID Configuration voor POTS Dial Peers voor meer informatie over DID voor digitale T1/E1-spraakpoorten.

Opmerking: het gebruik van DID is **niet** nodig wanneer Automatic Ringdown (PLAR) van de privélijn wordt gebruikt op een spraak-poort of wanneer een serviceteken zoals Auto-Attendant (AA) wordt gebruikt op de inkomende dial-peer.

Configuratie-PLAR van monster

```
voice-port 1/0
connection-plar 1001
```

Steekproef configuratie—servicesscripts

```
dial-peer voice 1 pots
service AA
```

```
port 1/0:23
```

Beperkingen na uren

Abstract

Na-urenlang is de Tolheffing een nieuw veiligheidsmiddel beschikbaar in CME 4.3/7.0 dat u in staat stelt om beleid van de tolbeperking te vormen op basis van tijd en datum. U kunt beleid configureren zodat gebruikers niet toestemming krijgen om oproepen naar vooraf gedefinieerde getallen te maken gedurende bepaalde uren van de dag of de hele tijd. Als het 7x24-aanroep blokkeringsbeleid wordt ingesteld, beperkt het ook de reeks getallen die door een binnengebruiker kunnen worden ingevoerd om **Call-forward** in te stellen.

Opmerking: dit is een **interne bedreiging**.

Voorbeeld 1

Dit voorbeeld definieert verschillende patronen van cijfers waarvoor uitgaande oproepen worden geblokkeerd. De patronen 1 en 2, die oproepen naar externe getallen blokkeren die beginnen met "1" en "011", zijn geblokkeerd op maandag tot en met vrijdag vóór 7 uur 's morgens en na 19:00 uur, op zaterdag vóór 7 uur 's avonds en na 13 uur 's avonds en op de hele dag. Patroon 3 blokken aanroepen naar 900 nummers 7 dagen per week, 24 uur per dag.

Monsterconfiguratie

```
telephony-service
after-hours block pattern 1 91
after-hours block pattern 2 9011
after-hours block pattern 3 91900 7-24
after-hours day mon 19:00 07:00
after-hours day tue 19:00 07:00
after-hours day wed 19:00 07:00
after-hours day thu 19:00 07:00
after-hours day fri 19:00 07:00
after-hours day sat 13:00 07:00
after-hours day sun 12:00 12:00
```

Raadpleeg het gedeelte Gespreksblokkering configureren voor meer informatie over tolbeperkingen.

Beperkingsklasse

Abstract

Als u korrelige bediening wilt bij het configureren van tolbeperkingen, moet u klasse van Beperking (COR) gebruiken. Verwijs naar klasse van beperkingen: Voorbeeld voor meer informatie.

Beperkingen van tol door H.323/SIP-trunks

Abstract

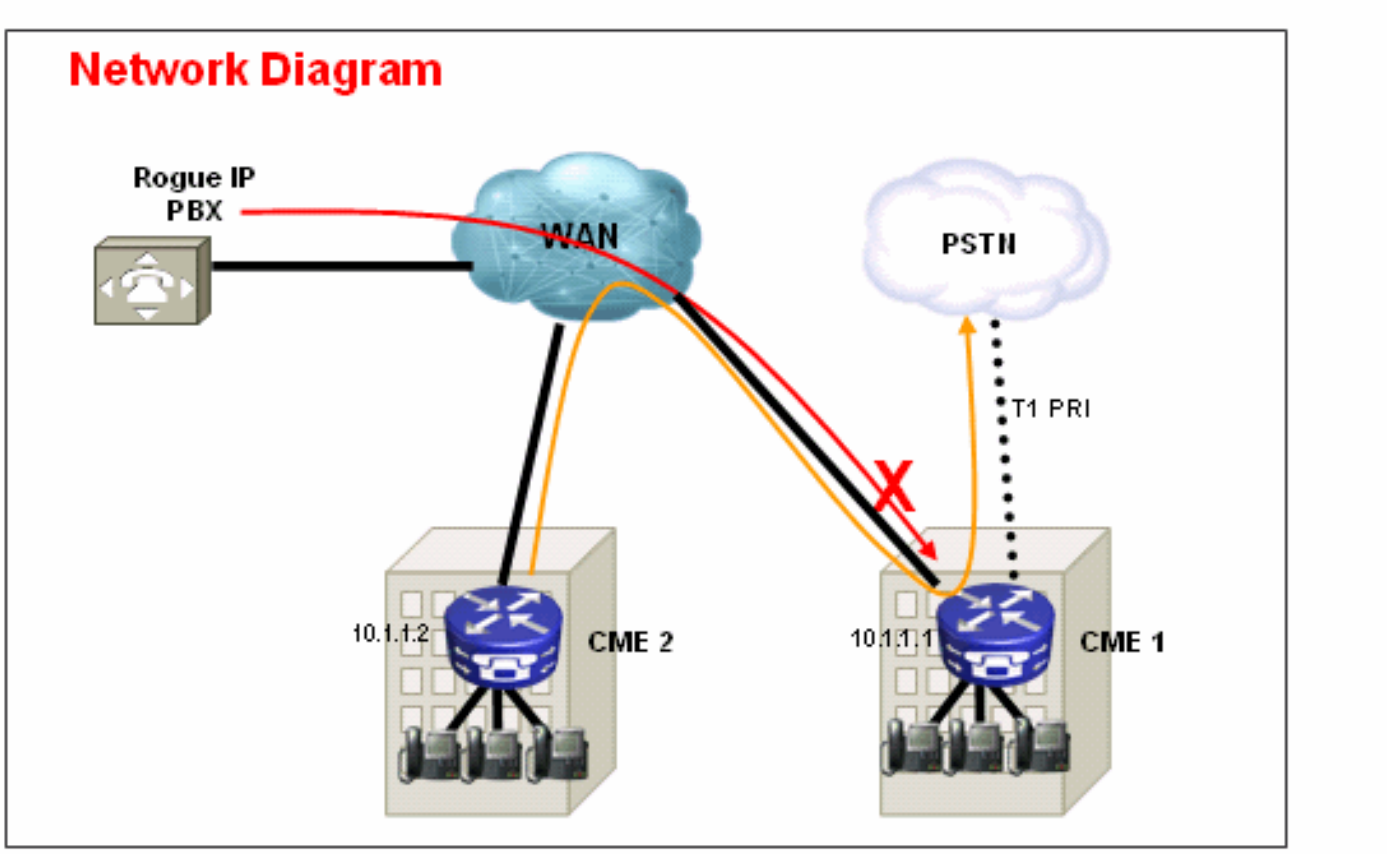
In gevallen waarin een CME-systeem via een WAN is verbonden met andere CME-apparaten via

een SIP- of H.323-stam, kunt u SIP/H.323-toegang tot de CME beperken om te voorkomen dat gebruikers uw systeem gebruiken om oproepen naar het PSTN illegaal door te geven.

Opmerking: dit is een **externe dreiging**.

Voorbeeld 1

In dit voorbeeld heeft CME 1 PSTN-connectiviteit. CME 2 wordt via WAN met CME 1 verbonden via een H.323-stam. Om CME 1 te beveiligen, kunt u een toegangslijst configureren en deze op de WAN-interface toepassen en dus alleen IP-verkeer van CME 2 toestaan. Dit voorkomt dat de Ruwe IP PBX-verbinding VOIP-oproepen door CME 1 naar het PSTN stuurt.



Oplossing

Laat de WAN-interface op CME 1 niet toe om verkeer te aanvaarden van schurkenapparaten die het niet herkent. Merk op dat er een impliciete DENY is aan het eind van een toegangslijst. Als er meer apparaten zijn waarvan u inkomende IP verkeer wilt toestaan, zorg er dan voor dat u het IP-adres van het apparaat aan de toegangslijst wilt toevoegen.

Configuratie—CME 1

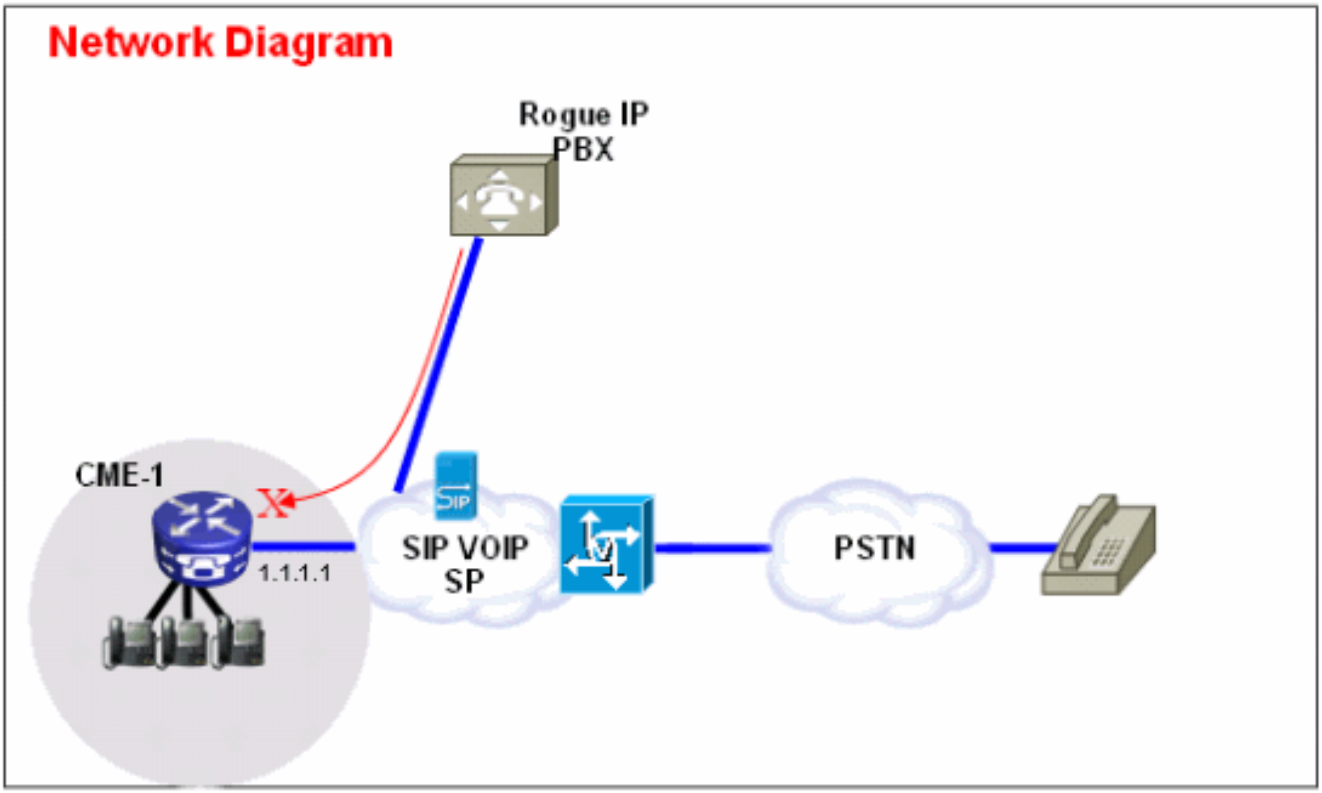
```
interface serial 0/0
  ip access-group 100 in
!
access-list 100 permit ip 10.1.1.2 255.255.255.255 any
```

Voorbeeld 2

In dit voorbeeld wordt CME 1 aangesloten op de SIP provider voor PSTN-connectiviteit met de

voorbeeldconfiguratie die wordt geboden in het voorbeeld SIP Trunking Configuration, CME Express (CME).

Aangezien CME 1 op het openbare internet is, is het mogelijk dat *tolfraude* kan optreden als een frauduleuze gebruiker openbare IP-adressen scant voor bekende poorten voor H.323 (TCP 1720) of SIP (UDP of TCP 5060) signalering en SIP of H.323 berichten doorstuurt die route uit SIP naar PIP belt STN. Het meest voorkomende misbruik in dit geval is dat de frauduleuze gebruiker meerdere internationale gesprekken voert via de SIP- of H.323-stam en de eigenaar van CME 1 ertoe aanzet voor deze tolfraudegesprekken te betalen - in sommige gevallen duizenden dollars.



Oplossing

Om deze dreiging te verzachten kunt u meerdere oplossingen gebruiken. Als een VOIP-signalering (SIP of H.323) niet via de WAN-link(s) in CME 1 wordt gebruikt, moet dit zoveel mogelijk worden geblokkeerd met de firewalltechnieken op CME 1 (toegangslijsten of ACL's).

1. Bevestig de WAN-interface met de Cisco IOS® firewall op CME 1:Dit impliceert dat u alleen bekend SIP- of H.323-verkeer op de WAN-interface toestaat. Alle andere SIP- of H.323-verkeer is geblokkeerd. Dit vereist ook dat u de IP adressen kent die SIP VOIP SP voor het signaleren op de SIP Trunk gebruikt. Deze oplossing veronderstelt dat SP bereid is om alle IP adressen of DNS namen te verstrekken die zij in hun netwerk gebruiken. Als DNS-namen worden gebruikt, vereist de configuratie ook dat een DNS-server die deze namen kan oplossen bereikbaar is. Als SP op hun end om het even welke adressen verandert, moet de configuratie op CME 1 worden bijgewerkt. Let op dat deze lijnen naast om het even welke ACL ingangen die reeds op de WAN interface aanwezig zijn moeten worden toegevoegd.Configuratie—CME 1

```
interface serial 0/0
  ip access-group 100 in
!
access-list 100 permit udp host 1.1.1.254 eq 5060 any
```

```
!--- 1.1.1.254 is SP SIP proxy access-list 100 permit udp host 1.1.1.254 any eq 5060
access-list 100 permit udp any any range 16384 32767
```

2. Zorg ervoor dat aanroepen die op de SIP-romp komen **NIET** opnieuw haarspelden:Dit impliceert dat de configuratie van CME 1 slechts SIP - SIP haarspelden van oproepen naar een specifiek bekend PSTN - cijferbereik toestaat, worden alle andere oproepen geblokkeerd. U moet specifieke inkomende kiespeers configureren voor de PSTN-getallen die in de SIP-stam komen die in kaart zijn gebracht met uitbreidingen of auto-verzorger(s) of voicemail op CME 1. Alle andere oproepen naar getallen die geen deel uitmaken van het CME 1 PSTN-nummerbereik zijn geblokkeerd. Dit heeft geen invloed op de doorsturen / overboekingen naar voicemail (Cisco Unity Express) en Bel alle naar PSTN-nummers vanuit IP-telefoons op CME 1, omdat de eerste oproep nog steeds gericht is op een extensie op CME 1.Configuratie—CME 1

```
dial-peer voice 1000 voip
  description ** Incoming call to 4085551000 from SIP trunk **
  voice-class codec 1
  voice-class sip dtmf-relay force rtp-nte
  session protocol sipv2
  incoming called-number 4085551000
  dtmf-relay rtp-nte
  no vad
!
dial-peer voice 1001 voip
  permission term
!--- Prevent hairpinning calls back over SIP Trunk. description ** Incoming call from SIP
trunk ** voice-class codec 1 voice-class sip dtmf-relay force rtp-nte session protocol
sipv2 incoming called-number .T
!--- Applies to all other inbound calls. dtmf-relay rtp-nte no vad
```

3. Gebruik vertaalregels om specifieke kiesregels te blokkeren:De meeste tolgevallen omvatten internationale telefoongesprekken. Dientengevolge, kunt u een specifiek binnenkomend wijzerplaat-peer creëren die specifieke gedraaid koorden en blokkeert roepen aan hen aanpast. De meeste CME's gebruiken een specifieke toegangscode, zoals 9, om uit te bellen en de internationale kiescode in de VS is 1011. Daarom is de meest gebruikelijke kiestoon om in de VS te blokkeren 9011 + elke cijfers nadat die op de SIP-stam zijn ingekomen.Configuratie—CME 1

```
voice translation-rule 1000
 rule 1 reject /^9011/
 rule 2 reject /^91900…….$/
 rule 3 reject /^91976…….$/
!
voice translation-profile BLOCK
translate called 1000
!
dial-peer voice 1000 voip
description ** Incoming call from SIP trunk **
incoming called-number 9011T
call-block translation-profile incoming BLOCK
```

Tools voor functiebeperking

Overdrachtspatroon

Abstract

Overdrachten naar alle getallen behalve die op de lokale SCCP IP-telefoons worden automatisch geblokkeerd. Tijdens de configuratie kunt u overboekingen naar niet-lokale nummers toestaan. De opdracht **overdrachtspatroon** wordt gebruikt om de overdracht van telefonieoproepen van Cisco SCCP IP-telefoons naar telefoons anders dan Cisco IP-telefoons toe te staan, zoals externe PSTN-oproepen of telefoons op een ander CME-systeem. U kunt het **overdrachtspatroon** gebruiken om de oproepen tot alleen interne extensies te beperken of misschien de oproepen tot PSTN-getallen in een bepaalde gebiedscode alleen te beperken. Deze voorbeelden tonen hoe het **overdracht-patroon** bevel kan worden gebruikt om vraag tot verschillende getallen te beperken.

Opmerking: dit is een **interne bedreiging**.

Voorbeeld 1

Laat gebruikers alleen oproepen naar de 408 gebiedscode overdragen. In dit voorbeeld, is de veronderstelling dat CME met een wijzerplaat-peer wordt gevormd die een bestemming-patroon van 9T heeft.

Monsterconfiguratie

```
telephony-service
transfer-pattern 91408
```

Transactieplatform geblokkeerd

Abstract

In Cisco Unified CME 4.0 en latere versies kunt u individuele telefoons verhinderen om telefoontjes naar getallen over te brengen die wereldwijd voor overdracht zijn ingeschakeld. De **overhevelingspatroon geblokkeerde** opdracht voert de **overdracht-patroon** opdracht uit en schakelt de gespreksoverdracht naar een bestemming uit die bereikt moet worden door een POTS of VoIP-dial-peer. Dit omvat PSTN-getallen, andere spraakgateways en Cisco Unity Express. Dit waarborgt dat individuele telefoons geen tol kosten wanneer de vraag buiten het Cisco Unified CME systeem wordt overgebracht. De verbinding van de vraag kan blokkeren voor individuele telefoons of als deel van een sjabloon worden gevormd dat op een reeks telefoons van toepassing is.

Opmerking: dit is een **interne bedreiging**.

Voorbeeld 1

In deze voorbeeldconfiguratie is telefoon 1 niet toegestaan om overdrachtspatroon (wereldwijd gedefinieerd) te gebruiken om gesprekken over te brengen, terwijl telefoon 2 het overdrachtspatroon kan gebruiken dat is gedefinieerd onder telefonie-service om gesprekken over te brengen.

Monsterconfiguratie

```
ephone-template 1
transfer-pattern blocked
!
ephone 1
```

```
ephone-template 1
!
ephone 2
!
```

Overschrijving max. lengte

Abstract

De opdracht **max-lengte overbrengen** bepaalt het maximale aantal cijfers dat de gebruiker kan bellen wanneer een oproep wordt overgebracht. De **overdracht-patroon max-length** passeert de **overdracht-patroonopdracht** en dwingt de maximaal toegestane cijfers voor overdrachtbestemming af. Het argument specificeert het aantal toegestane cijfers in een aantal waar een vraag wordt overgebracht. Bereik: 3 t/m 16. Standaard: 16.

Opmerking: dit is een **interne bedreiging**.

Voorbeeld 1

Deze configuratie staat alleen telefoons toe die deze telefoonsjabloon hebben toegepast op overdracht naar bestemmingen die maximaal vier cijfers lang zijn.

Monsterconfiguratie

```
ephone-template 1
transfer max-length 4
```

Doorsturen max. lengte

Abstract

Om het aantal cijfers te beperken dat met de zachte sleutel van CfwdALL op een IP-telefoon kan worden ingevoerd, gebruikt u de opdracht **call-forward max-length** opdracht in de **configuratie** van het telefoon-dn of het telefoon-dn-sjabloon. Om een beperking op het aantal cijfers te verwijderen dat kan worden ingevoerd, gebruik de **geen** vorm van deze opdracht.

Opmerking: dit is een **interne bedreiging**.

Voorbeeld 1

In dit voorbeeld, is de folder extensie 101 toegestaan om een oproep-door te sturen naar elke extensie die één tot vier cijfers lang is. Alle gesprekken naar bestemmingen langer dan vier cijfers ontbreken.

Monsterconfiguratie

```
ephone-dn  1  dual-line
number 101
call-forward max-length 4
```

of

```
ephone-dn-template  1
call-forward max-length 4
```

Geen lokaal gesprek doorsturen

Abstract

Wanneer de opdracht **geen voorwaartse lokale oproepen** wordt gebruikt in de configuratie van het telefoon-dn, worden interne oproepen naar een bepaalde telefoon-dn met **geen** lokaal-**geannuleerde oproepen** niet doorgestuurd als de telefoon-dn bezig is of geen antwoord geeft. Als een interne beller deze telefoon-dn belt en de telefoon-dn bezig is, hoort de beller een druk signaal. Als een interne beller dit telefoon-dn belt en het antwoord niet, hoort de beller een ringsignaal. De interne verbinding wordt niet doorgestuurd zelfs als het aanroepen van de telefoon voor de telefoon-dn wordt ingeschakeld.

Opmerking: dit is een **interne bedreiging**.

Voorbeeld 1

In dit voorbeeld, verlengde 2222 vraag verlenging 3675 en hoort een ringrug of een druk signaal. Als een externe beller verlenging 3675 bereikt en er geen antwoord is, wordt de oproep doorgestuurd naar verlenging 4000.

Monsterconfiguratie

```
ephone-dn  25
number 3675
no forward local-calls
call-forward noan 4000 timeout 30
```

Auto-registratie in CME-systeem uitschakelen

Abstract

Wanneer **auto-reg-telefoon** onder telefonieservice op een SCCP CME-systeem is ingeschakeld, worden nieuwe IP-telefoons die in het systeem zijn aangesloten automatisch geregistreerd en als **autoToewijzen** is ingesteld om automatisch verlengingsnummers toe te wijzen, kan een nieuwe IP-telefoon direct oproepen.

Opmerking: dit is een **interne bedreiging**.

Voorbeeld 1

In deze configuratie is een nieuw CME-systeem ingesteld, zodat u handmatig een telefoon moet toevoegen zodat het nummer zich aan het CME-systeem kan registreren en het kan gebruiken om IP-telefonie te bellen.

Oplossing

U kunt **autoreg-telefoon** uitschakelen onder de telefonieservice, zodat nieuwe IP-telefoons die aangesloten zijn op een CME-systeem niet automatisch worden geregistreerd op het CME-

systeem.

Monsterconfiguratie

```
telephony-service
no auto-reg-ephone
```

Voorbeeld 2

Als u SCCP CME gebruikt en van plan bent om Cisco SIP-telefoons aan het systeem te registreren, moet u het systeem configureren zodat de SIP-endpoints voor authentiek moeten zijn met een gebruikersnaam en wachtwoord. U kunt dit vervolgens eenvoudig configureren:

```
voice register global
 mode cme
 source-address 192.168.10.1 port 5060
 authenticate register
```

Raadpleeg SIP: Installatie van Cisco Unified CME voor een gedetailleerdere configuratiehandleiding voor SIP CME.

Cisco Unity Express restrictietools

Secure Cisco Unity Express: AA PSTN-toegang

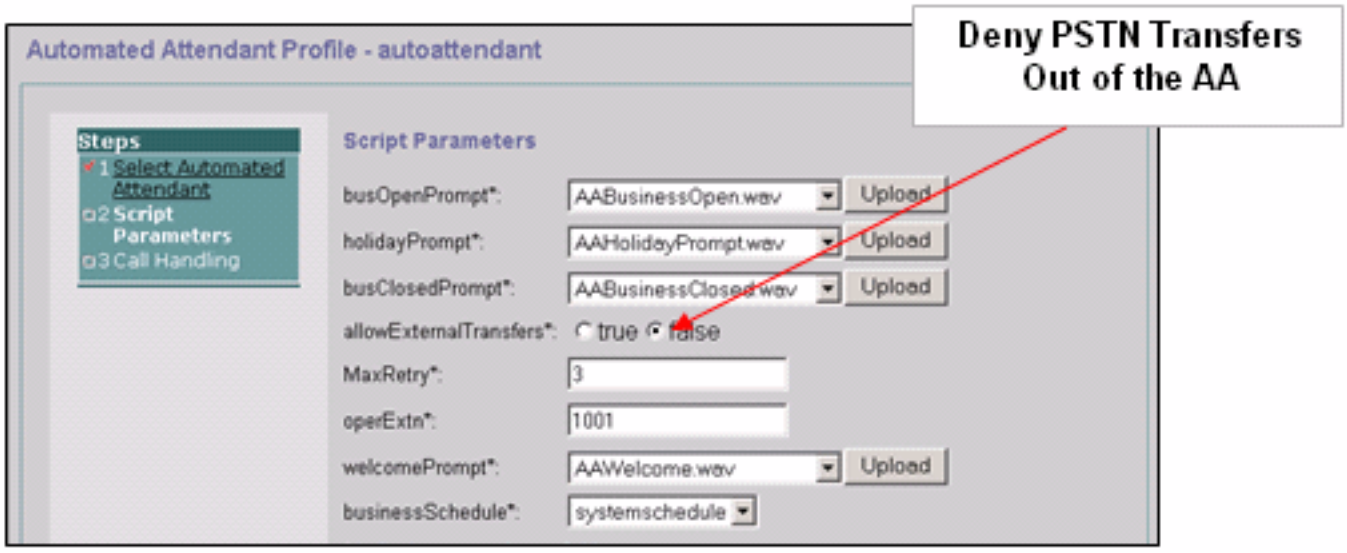
Abstract

Wanneer uw systeem zo is geconfigureerd dat inkomende oproepen naar automatische-verzorger (AA) worden doorgestuurd op Cisco Unity Express, kan het nodig zijn om externe overdracht naar het PSTN uit te schakelen van Cisco Unity Express AA. Dit staat externe gebruikers niet toe om uit te bellen naar externe getallen nadat ze Cisco Unity Express AA hebben bereikt.

Opmerking: dit is een **externe dreiging**.

Opmerking: Oplossing

N.B.: Schakel de optie **allowExterne overdrachten** uit op de Cisco Unity Express GUI.



Opmerking: Als PSTN-toegang van de AA vereist is, beperkt u de getallen of het bereik van de getallen die geldig worden geacht door het script.

Cisco Unity Express restrictietabellen

Abstract

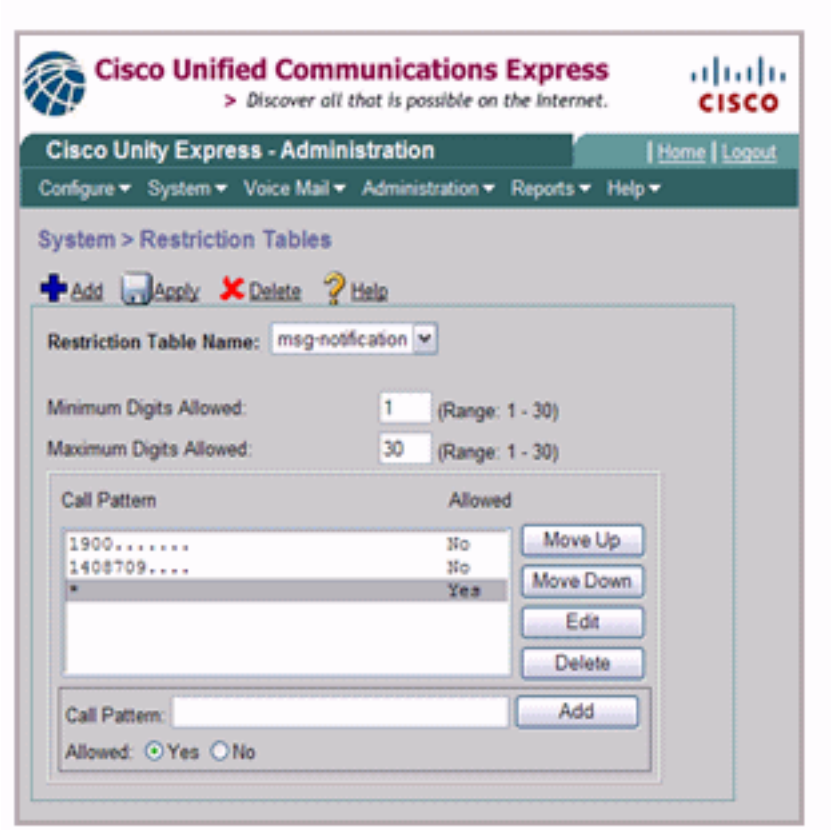
U kunt de Cisco Unity Express restrictietabellen gebruiken om de bestemmingen te beperken die tijdens een oproep vanuit Cisco Unity Express kunnen worden bereikt. De Cisco Unity Express restrictietabel kan worden gebruikt om tolfraude en kwaadaardig gebruik van het Cisco Unity Express-systeem te voorkomen voor uitgaande gesprekken. Als u de Cisco Unity Express restrictietabel gebruikt, kunt u aanroep patronen op een wilde kaart specificeren. Toepassingen die de Cisco Unity Express restrictietabel gebruiken zijn:

- Fax
- Cisco Unity Express Live Replay
- Bericht
- Geen Subscriber-berichtlevering

Opmerking: dit is een **interne bedreiging**.

Oplossing

Om de bestemmingspatronen te beperken die door Cisco Unity Express op een uitgaande externe oproep kunnen worden bereikt, dient u het **Call Pattern** te configureren in het **Systeem > Beperkingstabellen** van de Cisco Unity Express GUI.



Vastlegging gesprekken

Uitgebreide CDR.

U kunt het CME-systeem configureren om een verbeterde CDR op te nemen en de CDR te loggen naar de routerflitser of een externe FTP-server. Deze gegevens kunnen dan worden gebruikt om oproepen te retraceren om te zien of misbruik door interne of externe partijen is opgetreden.

De bestands accounting optie die met CME 4.3/7.0 in Cisco IOS release 12.4(15)XY geïntroduceerd is, biedt een methode om accounting records in een komma gescheiden waarde (1.csv)-formaat op te nemen en de records in een interne flitser of een externe FTP-server op te slaan. Het breidt de ondersteuning van poortboekhoudingen uit, die ook de AAA- en syslogmechanismen van houtkapinformatie omvat.

Het boekhoudproces verzamelt boekhoudgegevens voor elk telefoonbeen dat op een Cisco spraakgateway wordt gemaakt. U kunt deze informatie gebruiken voor post-verwerkingsactiviteiten zoals het genereren van factureringsrecords en voor netwerkanalyse. Cisco spraak gateways vangen boekhoudkundige gegevens in de vorm van Call detailrecords (CDR's) die eigenschappen bevatten die door Cisco worden gedefinieerd. De gateway kan CDR's naar een RADIUS-server, syslogserver en met de nieuwe bestandmethode naar flitser of een FTP-server in .csv-formaat verzenden.

Raadpleeg CDR-voorbeelden voor meer informatie over de uitgebreide CDR-functies.

Gerelateerde informatie

- Cisco Unified Communications Manager Express security beste praktijken
- Cisco Communications Manager Express-beheerdershandleiding

- Cisco Communications Manager Express-beheerdershandleiding - gespreksblokkering
- De betekenis van dial-peers op IOS-platforms
- Nummeromzetting met spraakvertaalprofielen
- Referentie-netwerkontwerp voor CME-oplossing
- Technische ondersteuning en documentatie – Cisco Systems