Unified Communications Manager Express Edition - Prévention de la fraude touchant les appels

Contenu

Introduction

Ce document est un guide de configuration qui peut être utilisé pour sécuriser un système Cisco Communications Manager Express (CME) et atténuer les risques de fraude touchant les appels interurbains. CME est une solution basée sur routeur du Contrôle d'appel de Cisco qui fournit une solution intelligente, simple et sécurisée pour les organismes qui veulent implémenter des transmissions unifiées. Il est recommandent fortement que vous implémentiez les mesures de sécurité décrites dans ce document afin de fournir le contrôle de niveaux de sécurité supplémentaire et réduire la possibilité de fraude de contournement.

L'objectif de ce document est de vous instruire sur les divers outils de Sécurité disponibles sur des Passerelles voix et CME de Cisco. Ces outils peuvent être mis en application sur un système de CME afin d'aider à atténuer la menace de la fraude de contournement par les interlocuteurs internes et externes.

Ce document fournit des instructions sur la façon dont configurer un système de CME avec de divers outils de Sécurité de contournement et de restriction de caractéristique. De document les contours également pourquoi certains outils de Sécurité sont utilisés dans certains déploiements.

La flexibilité inhérente globale des Plateformes ISR de Cisco te permet pour déployer CME dans beaucoup de différents types de déploiements. Ainsi il peut exiger pour utiliser une combinaison des caractéristiques décrites dans ce document pour aider à verrouiller en bas de CME. Ce document sert d'instruction à la façon appliquer des outils de Sécurité sur CME et nullement des garanties que la contournement-fraude ou l'abus par les interlocuteurs internes et externes ne se produira pas.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Communications Manager Express

Composants utilisés

Les informations dans ce document sont basées sur le Cisco Unified Communications Manager Express 4.3 et CME 7.0.

Remarque: Le Cisco Unified CME 7.0 inclut les mêmes caractéristiques que le Cisco Unified CME 4.3, qui est renuméroté à 7.0 pour aligner avec des versions de Cisco Unified Communications.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Aperçu

Ce document couvre les outils de la Sécurité la plus commune qui peuvent être utilisés sur un système de CME pour aider à atténuer la menace de la fraude de contournement. Les outils de Sécurité de CME référencés dans ce document incluent des outils de restriction de contournement et des outils de restriction de caractéristique.

Outils de restriction de contournement

- Sélection directe à l'arrivée
- Après la restriction de contournement d'heures
- Classe de la restriction
- Liste d'accès pour limiter l'accès de joncteur réseau H323/SIP

Outils de restriction de caractéristique

- Transfert-modèle
- Transfert-modèle bloqué
- Maximum-longueur de transfert
- maximum-longueur Appel-en avant
- Aucun appels locaux en avant
- Aucun automatique-Reg-ephone

Outils de restriction de Cisco Unity Express

- Accès sécurisé PSTN de Cisco Unity Express
- Restriction de notification de message

Se connecter d'appel

- Appelez se connecter pour saisir les articles mouvement d'appel (les CDR)

Interne contre des menaces extérieures

Ce document discute des menaces des interlocuteurs internes et externes. Les interlocuteurs internes incluent les utilisateurs de téléphone IP qui résident sur un système de CME. Les interlocuteurs externes incluent des utilisateurs sur les systèmes étrangers qui peuvent essayer d'utiliser l'hôte CME pour faire des appels frauduleux et pour avoir les appels chargés de nouveau à votre système de CME.

Outils de restriction de contournement

Sélection directe à l'arrivée

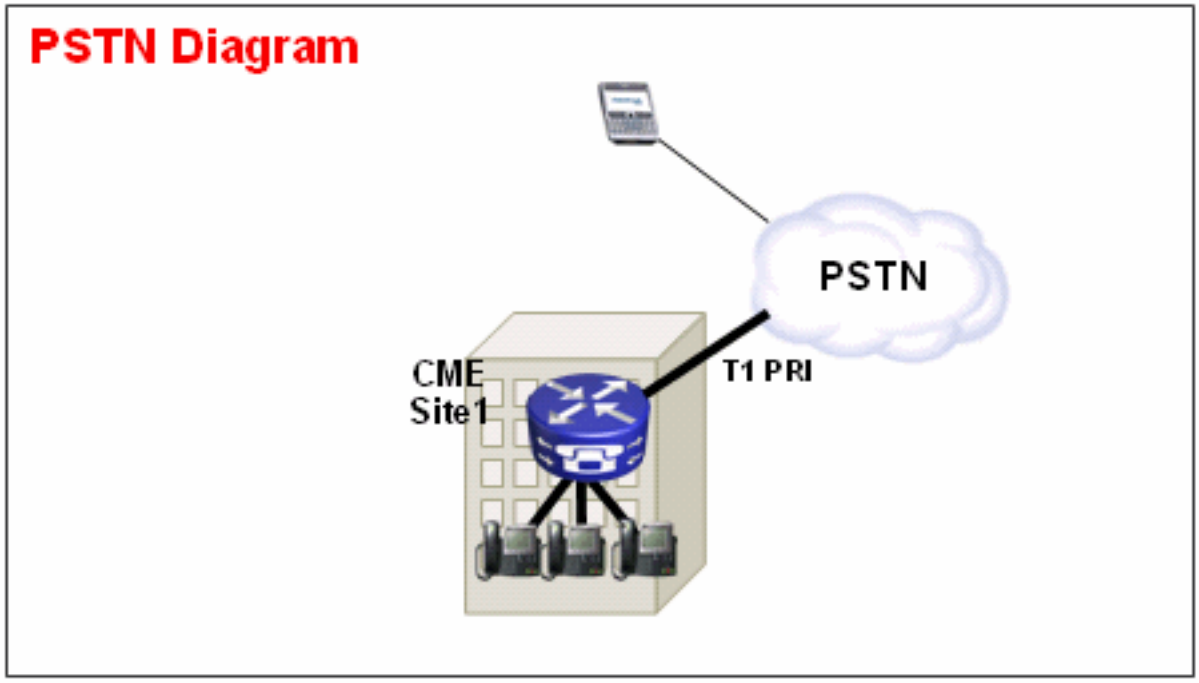
Abstrait

Le direct-inward-dial (A FAIT) est utilisé sur des Passerelles voix de Cisco afin de permettre à la passerelle pour traiter un appel d'arrivée après qu'il reçoive des chiffres du PBX ou commutateur CO. Quand A FAIT est activé, la passerelle Cisco ne présente pas une tonalité secondaire à l'appelant et n'attend pas de collecter les chiffres supplémentaires de l'appelant. Il en avant l'appel directement à la destination qui apparie le Service d'identification du numéro composé réacheminé (RDNIS) d'arrivée. Ceci s'appelle la composition en une étape.

Remarque: C'est une **menace extérieure**.

Déclaration de problème

Si le direct-inward-dial n'est pas configuré sur une passerelle Cisco ou CME, toutes les fois qu'un appel entre de la Co ou du PBX à la passerelle Cisco, l'appelant entend une tonalité secondaire. Ceci s'appelle composition à deux étages. Une fois que les appelants PSTN entend la tonalité secondaire, ils peuvent écrire des chiffres pour atteindre n'importe quelle extension interne ou s'ils connaissent le code d'accès PSTN, ils peuvent composer la longue distance ou les numéros internationaux. Ceci présente un problème parce que l'appelant PSTN peut employer le système de CME pour placer la longue distance sortante ou les appels internationaux et la société obtient facturé les appels.



Exemple 1

Au site 1, CME est connecté au PSTN par un joncteur réseau de T1 PRI. Le fournisseur PSTN fournit les **40855512.** Soyez-vous étendu pour le site 1. de CME. Ainsi tous les appels PSTN destinés pour 4085551200 – 4085551299 sont d'arrivée conduit à CME. Si vous ne configurez pas le **direct-inward-dial** sur le système, un appelant d'arrivée PSTN entend un secondaire une tonalité et doit manuellement composer l'extension interne. Le problème plus grand est que si l'appelant est un trompeur et connaît le code d'accès PSTN sur le système, généralement **9**, ils peuvent composent **9** puis n'importe quels numéros de destination qu'ils veulent atteindre.

Solution 1

Afin d'atténuer cette menace, vous devez configurer le **direct-inward-dial**. Ceci fait expédier la passerelle Cisco l'appel d'arrivée directement à la destination qui apparie le DNIS d'arrivée.

Exemple de configuration

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

Pour avez fonctionné correctement, s'assurent que l'appel d'arrivée apparie l'homologue de numérotation POTS correct où la commande de **direct-inward-dial** est configurée. Dans cet

exemple, le T1 PRI est connecté au port 1/0:23. Afin d'apparier l'homologue de numérotation en entrée correct, émettez le pair de cadran **entrant de numéro appelé que la** commande sous A FAIT l'homologue de numérotation POTS.

Exemple 2

Au site 1, CME est connecté au PSTN par un joncteur réseau de T1 PRI. Le fournisseur PSTN donne les **40855512.** et **40855513.** A FAIT des plages pour le site 1. de CME. Ainsi tous les appels PSTN destinés pour 4085551200 – 4085551299 et 4085551300 - 4085551399 sont d'arrivée conduit à CME.

Configuration incorrecte :

Si vous configurez un homologue de numérotation en entrée, comme dans la configuration d'échantillon dans cette section, la possibilité pour la fraude de contournement se produit toujours. Le problème avec cet homologue de numérotation en entrée est qu'il apparie seulement des appels d'arrivée à **40852512.** et applique alors a entretenu. Si un appel PSTN entre dans **40852513.** , le cadran-pair d'arrivée de pots n'est pas assorti et avez entretenu ainsi n'est pas appliqué. Si un homologue de numérotation en entrée avec FAISAIT n'est pas apparié, alors l'homologue de numérotation par défaut 0 est utilisé. A FAIT est désactivé par défaut sur le dial-peer 0.

Exemple de configuration

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

Configuration correcte

La manière correcte de configurer a entretenu sur un homologue de numérotation en entrée est affichée dans cet exemple :

Exemple de configuration

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

Refer to A FAIT la configuration pour des homologues de numérotation POTS pour plus d'informations sur A FAIT pour les ports vocaux T1/E1 numériques.

Remarque: L'utilisation de A FAIT n'est pas nécessaire quand le Privé-Line Ringdown qu'automatique (PLAR) est utilisé sur un port vocal ou un script de service tel que la réception automatique (aa) est utilisé sur l'homologue de numérotation en entrée.

Configuration d'échantillon — PLAR

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

Configuration d'échantillon — Entretenez le script

```
dial-peer voice 1 pots
service AA
port 1/0:23
```

Après des restrictions de contournement d'heures

Abstrait

Après des heures la restriction de contournement est un nouvel outil de Sécurité disponible dans CME 4.3/7.0 qui te permet pour configurer des stratégies de restriction de contournement basées sur la date et heure. Vous pouvez configurer des stratégies de sorte qu'on ne permette pas à des des utilisateurs pour faire des appels aux nombres de prédéfinis pendant certaines heures du jour ou tout le temps. Si le 7x24 après stratégie de blocage d'appel d'heures est configuré, il limite également l'ensemble de nombres qui peut être écrit par un utilisateur intérieur pour placer **call forward all**.

Remarque: C'est une **menace interne**.

Exemple 1

Cet exemple définit plusieurs configurations de chiffres pour lesquels des appels sortants sont bloqués. Modèles 1 et 2, qui bloquent des appels aux nombres externes qui commencent par "1" et "011," sont bloqués le lundi à vendredi avant 7h du matin et après 19h, le samedi avant 7h du matin et après 13h, et toute la journée dimanche. Le modèle 3 bloque des appels à 900 nombres 7 jours par semaine, 24 heures sur 24.

Exemple de configuration

```
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
```

Référez-vous à configurer le blocage d'appel pour plus d'informations sur la restriction de contournement.

Classe de la restriction

Abstrait

Si vous voulez le contrôle granulaire quand vous configurez la restriction de contournement, vous devez utiliser la classe de la restriction (COR). Référez-vous à la classe de la restriction : Pour en savoir plus d'exemple.

H.323/SIP de joncteurs réseau de contournement de restrictions de fraude

Abstrait

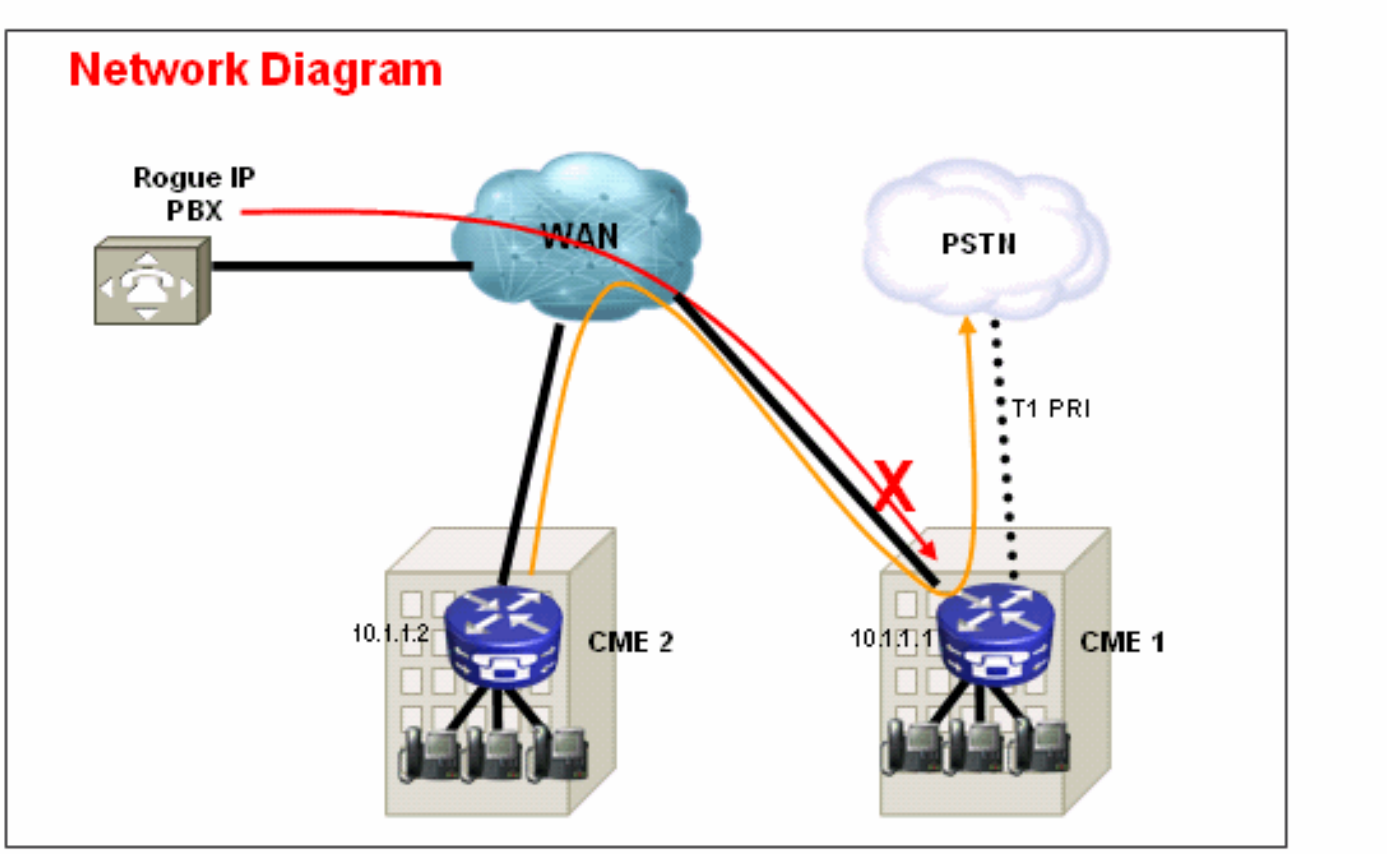
Dans les cas où un système de CME est connecté au-dessus d'un WAN à d'autres périphériques de CME par un SIP ou H.323 un joncteur réseau, vous pouvez limiter l'accès du joncteur réseau

SIP/H.323 à CME afin d'empêcher des trompeurs d'employer votre système pour transmettre par relais illégalement des appels au PSTN.

Remarque: C'est une **menace extérieure**.

Exemple 1

Dans cet exemple, CME 1 a la connectivité RTPC. CME 2 est connecté au-dessus du WAN à CME 1 par H.323 un joncteur réseau. Afin de sécuriser CME 1, vous pouvez configurer une liste d'accès et l'appliquer d'arrivée sur l'interface WAN et seulement permettre ainsi le trafic IP de CME 2. Ceci empêche l'IP PBX d'escroc d'envoyer des appels de VOIP par CME 1 au PSTN.



Solution

Ne permettez pas à l'interface WAN sur CME 1 pour recevoir le trafic des périphériques escrocs qu'ils n'identifient pas. Notez qu'il y a un implicite REFUSENT tous à la fin d'une liste d'accès. S'il y a plus de périphériques dont vous voulez permettre le trafic IP d'arrivée, soyez sûr d'ajouter l'adresse IP du périphérique à la liste d'accès.

Configuration d'échantillon — CME 1

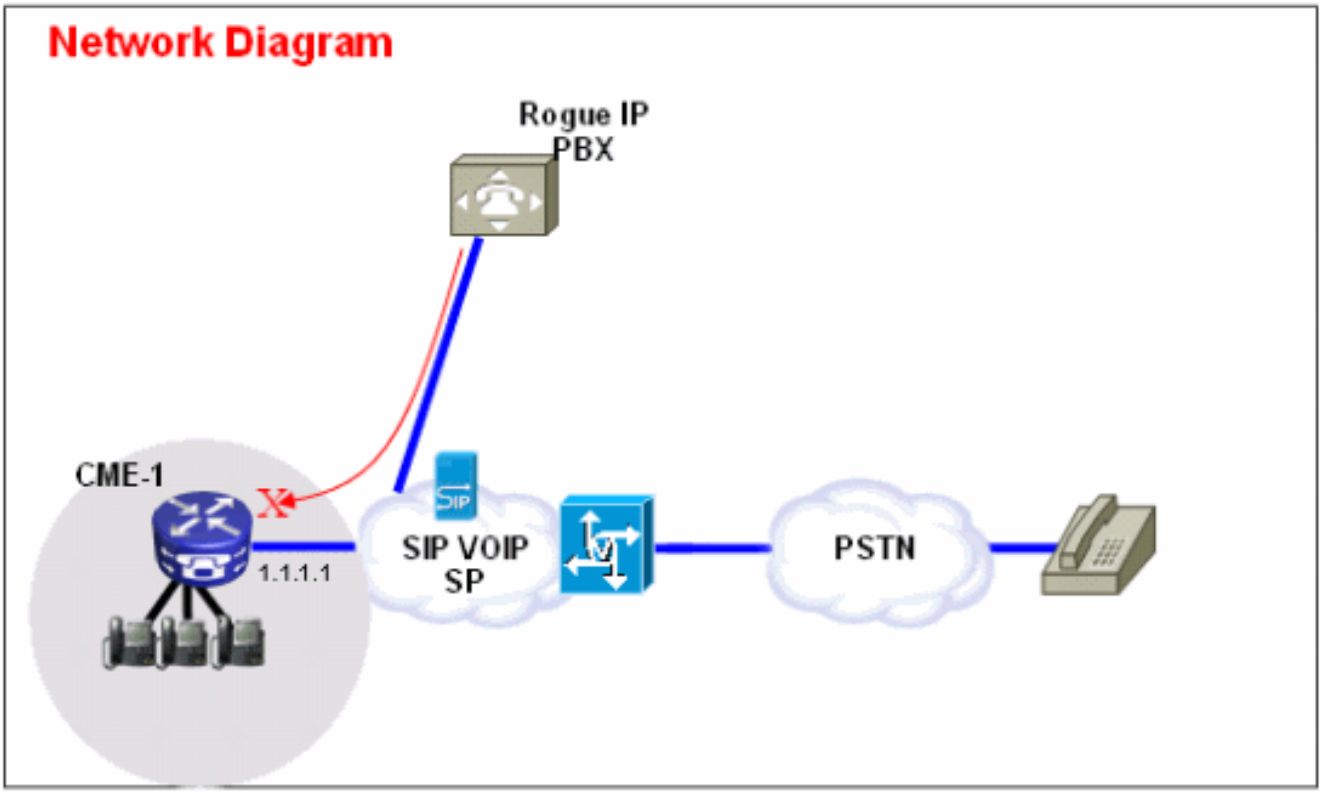
```
interface serial 0/0
  ip access-group 100 in
!
access-list 100 permit ip 10.1.1.2 255.255.255.255 any
```

Exemple 2

Dans cet exemple, CME 1 est connecté au fournisseur de SIP pour la connectivité RTPC à la configuration d'échantillon fournie à l'exemple de configuration de jonction SIP de Cisco

CallManager Express (CME).

Puisque CME 1 est sur l'Internet public, il est possible que la *fraude de contournement* puisse se produire si un utilisateur escroc balaye des adresses IP publique pour des ports connus pour H.323 (TCP 1720) ou signalisation de SIP (UDP ou TCP 5060) et envoie le SIP ou H.323 les messages qui conduisent des appels soutiennent du joncteur réseau de SIP au PSTN. La plupart des abus communs sont dans ce cas l'utilisateur escroc fait de plusieurs appels internationaux par le SIP ou H.323 le joncteur réseau et fait payer le propriétaire de CME 1 ces appels de fraude de contournement - dans certains cas des milliers de dollars.



Solution

Afin d'atténuer cette menace, vous pouvez utiliser de plusieurs solutions. Si aucun VOIP signalant (SIP ou H.323) n'est utilisé au-dessus du lien WAN dans CME 1, ceci doit être bloqué avec les techniques de Pare-feu sur CME 1 (des Listes d'accès ou ACLs) autant que possible.

1. Sécurisez l'interface WAN avec le Pare-feu de Cisco IOS® sur CME 1 :Ceci implique que vous laissez seulement le SIP connu ou trafiquez H.323 pour entrer sur l'interface WAN. Tout l'autre SIP ou H.323 le trafic est bloqué. Ceci exige également que vous connaissez les adresses IP que le fournisseur de services de VOIP de SIP utilise pour signaler sur le joncteur réseau de SIP. Cette solution suppose que le fournisseur de services est disposé à fournir tous les adresses IP ou noms DNS qu'ils les utilisent dans leur réseau. En outre, si des noms DNS sont utilisés, la configuration exige qu'un serveur DNS qui peut résoudre ces noms est accessible. En outre, si le fournisseur de services change n'importe quelles adresses sur leur extrémité, la configuration doit être mise à jour sur CME 1. Notez que ces lignes doivent être ajoutées en plus de tous les rubriques de liste ACL déjà actuels sur l'interface WAN.Configuration d'échantillon — 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. Assurez qu'appels qui entrent sur le joncteur réseau de SIP l'épingle à cheveux ne soutiennent pas :Ceci implique que CME 1 configuration laisse seulement le SIP – SIROTEZ l'épingle à cheveux des appels à une plage numérique PSTN connue par particularité, tous autres appels sont bloqués. Vous devez configurer les homologues de numérotation en entrée spécifiques pour les nombres PSTN qui entrent sur le joncteur réseau de SIP qui sont tracés aux extensions ou la réception automatique ou la messagerie vocale sur CME 1. Tout l'autre appelle aux nombres qui ne sont pas une partie de CME que 1 plage numérique PSTN sont bloquées. La note, ceci n'affecte pas l'appel en avant/transferts à la messagerie vocale (Cisco Unity Express) et call forward all aux nombres PSTN des Téléphones IP sur CME 1, parce que l'appel initial est encore visé vers une extension sur CME 1.Configuration d'échantillon — 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. Règles de traduction d'utilisation afin de bloquer les chaînes spécifiques de cadran :La plupart des fraudes de contournement comportent la composition d'appel international. En conséquence, vous pouvez créer un homologue de numérotation en entrée spécifique qui apparie les numéros composés spécifiques et les blocs appelle à eux. La plupart d'utilisation de CMEs un code d'accès spécifique, tel que 9, de composer pour sortir et code téléphonique international aux USA est 011. Par conséquent, la chaîne de cadran la plus commune à bloquer aux USA est 9011 + tout ce de chiffres ensuite entré sur le joncteur réseau de SIP.Configuration d'échantillon — 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
```

Outils de restriction de caractéristique

Modèle de transfert

Abstrait

Des transferts à tous les nombres excepté ceux sur les Téléphones IP locaux de SCCP sont automatiquement bloqués par défaut. Pendant la configuration, vous pouvez permettre des transferts non aux numéros locaux. La commande de transfert-**modèle** est utilisée afin de permettre le transfert des appels de téléphonie à partir des Téléphones IP de SCCP de Cisco aux téléphones autres que des Téléphones IP de Cisco, tels que des appels PSTN externes ou des téléphones à un autre système de CME. Vous pouvez employer le transfert-**modèle** afin de limiter les appels aux extensions internes seulement ou peut-être la limite appelle aux nombres PSTN dans certain code postal seulement. Ces exemples affichent comment la commande de transfert-**modèle** peut être utilisée pour limiter des appels aux numéros différents.

Remarque: C'est une **menace interne**.

Exemple 1

Permettez aux utilisateurs pour transférer exige seulement à code postal 408. Dans cet exemple, la supposition est que CME est configuré avec un cadran-pair qui a une destination-pattern de 9T.

Exemple de configuration

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

Transfert-modèle bloqué

Abstrait

Dans le Cisco Unified CME 4.0 et les versions ultérieures, vous pouvez empêcher différents téléphones des transferts d'appels aux nombres qui sont globalement activés pour le transfert. La commande **bloquée parmodèle** ignore la commande de transfert-**modèle** et les débronchements appellent le transfert à n'importe quelle destination qui doit être atteinte par les POTS ou l'homologue de numérotation VoIP. Ceci inclut des nombres PSTN, d'autres Passerelles voix et Cisco Unity Express. Ceci s'assure que les différents téléphones n'occasionnent pas des taxations quand des appels sont transférés en dehors du système de Cisco Unified CME. Le blocage de transfert d'appel peut être configuré pour différents téléphones ou être configuré en tant qu'élément d'un modèle qui est appliqué à un ensemble de téléphones.

Remarque: C'est une **menace interne**.

Exemple 1

Dans cette configuration d'échantillon, on ne permet pas à l'l'ephone 1 pour employer le transfert-modèle (défini globalement) pour transférer des appels, alors que l'ephone 2 peut utiliser le transfert-modèle défini sous le service téléphonique pour transférer des appels.

Exemple de configuration

```
ephone-template 1
transfer-pattern blocked
!
ephone 1
ephone-template 1
!
ephone 2
!
```

Maximum-longueur de transfert

Abstrait

La commande de maximum-**longueur de transfert** spécifie le nombre maximal de chiffres que l'utilisateur peut composer quand un appel est transféré. **La maximum-longueur de transfert-modèle** ignore la commande de transfert-**modèle** et impose les chiffres maximum permis pour la destination de transfert. L'argument spécifie le nombre de chiffres permis dans un nombre vers lequel un appel est transféré. Plage : 3 à 16. Par défaut : 16.

Remarque: C'est une **menace interne**.

Exemple 1

Cette configuration permet seulement les téléphones qui ont ce ephone-modèle appliqué pour transférer vers les destinations qui sont un maximum de quatre chiffres longs.

Exemple de configuration

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

L'appel expédient la maximum-longueur

Abstrait

Afin de limiter le nombre de chiffres qui peuvent être écrits avec la clé douce de CfwdALL sur un téléphone IP, utilisez la commande appel-**en avant de maximum-longueur** dans le mode de configuration d'ephone-dn ou d'ephone-dn-modèle. Afin de retirer une restriction sur le nombre de chiffres qui peuvent être écrits, utilisez le **forme no de** cette commande.

Remarque: C'est une **menace interne**.

Exemple 1

Dans cet exemple, on permet à l'l'extension 101 de répertoire pour exécuter un appel-en avant à n'importe quelle extension qui est un à quatre chiffres de longueur. N'importe quel appel-en avant à de plus longs que quatre chiffres de destinations échouent.

Exemple de configuration

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

ou

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

Aucun appel local en avant

Abstrait

Quand l'**aucune** commande **en avant d'appels locaux** n'est utilisée dans le mode de configuration d'ephone-dn, des appels internes à un ephone-dn particulier sans des **appels locaux en avant** appliqués ne sont pas expédiés si l'ephone-dn est occupé ou ne répond pas. Si un appelant interne sonne cet ephone-dn et l'ephone-dn est occupé, l'appelant entend un signal d'occupation. Si un appelant interne sonne cet ephone-dn et il ne répond pas, l'appelant entend un signal de rappel. L'appel interne n'est pas expédié même si le transfert d'appel est activé pour l'ephone-dn.

Remarque: C'est une **menace interne**.

Exemple 1

Dans cet exemple, l'extension 2222 appelle l'extension 3675 et entend un rappel ou un signal

d'occupation. Si un appelant externe atteint l'extension 3675 et il y a pas de réponse, l'appel est expédié à l'extension 4000.

Exemple de configuration

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

Enregistrement automatique de débronchement sur le système de CME

Abstrait

Quand automatique-**Reg-ephone** est activé sous le service téléphonique sur un système de CME de SCCP, les nouveaux Téléphones IP qui sont branchés au système sont automatique enregistré et si **automatiquement désigné** sont configurés pour assigner automatiquement des numéros de poste, alors un nouveau téléphone IP peut faire des appels immédiatement.

Remarque: C'est une **menace interne**.

Exemple 1

Dans cette configuration, un nouveau système de CME est configuré de sorte que vous deviez manuellement ajouter un ephone pour que l'ephone enregistre à CME le système et pour l'emploie pour faire des appels de Téléphonie sur IP.

Solution

Vous pouvez désactiver automatique-**Reg-ephone** sous le service téléphonique de sorte que les nouveaux Téléphones IP connectés à un système de CME fassent pas registre automatique au système de CME.

Exemple de configuration

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

Exemple 2

Si vous utilisez le SCCP CME et prévoyez d'enregistrer des téléphones SIP de Cisco au système, vous devez configurer le système de sorte que les points finaux de SIP doivent authentifier avec un nom d'utilisateur et mot de passe. Afin de faire ainsi, configurez simplement ceci :

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

Référez-vous au SIP : Installation du Cisco Unified CME pour un guide de configuration plus complet pour le SIP CME.

Outils de restriction de Cisco Unity Express

Cisco Unity Express sécurisé : Accès PSTN aa

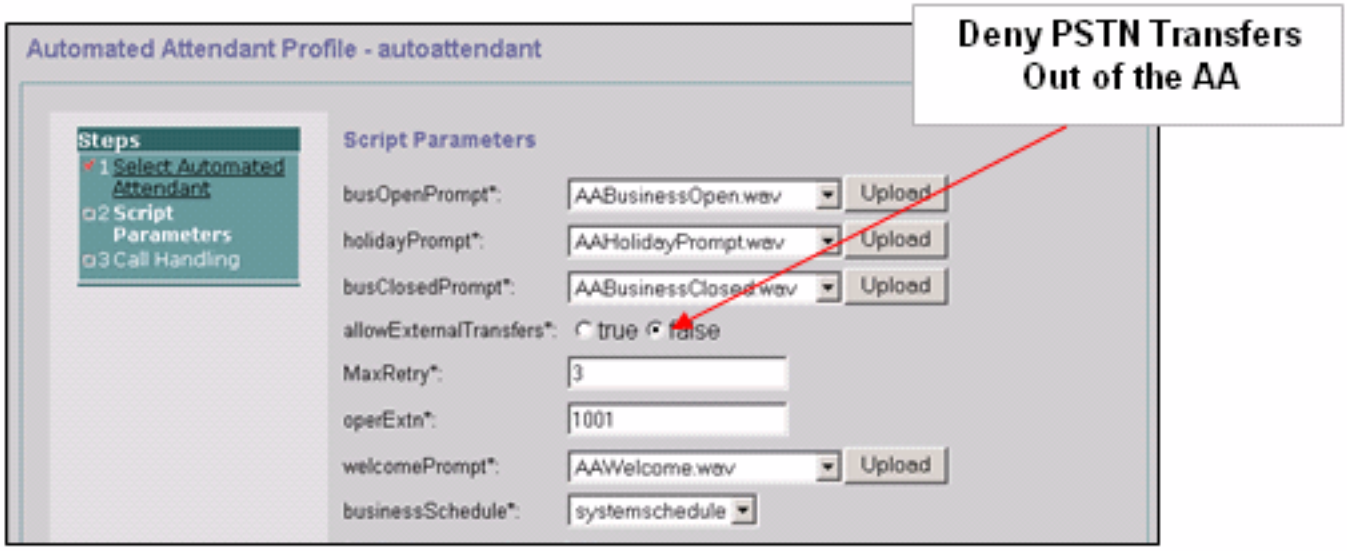
Abstrait

Quand votre système est configuré de sorte que des appels d'arrivée soient expédiés à la réception automatique (aa) sur le Cisco Unity Express, il peut être nécessaire de désactiver le transfert externe au PSTN à partir du Cisco Unity Express aa. Ceci ne permet pas à des utilisateurs externes pour composer sortant aux nombres externes après qu'ils atteignent le Cisco Unity Express aa.

Remarque: C'est une **menace extérieure**.

Remarque: Solution

Remarque: Désactivez l'option d'**allowExternalTransfers** sur le GUI de Cisco Unity Express.



Remarque: Si l'accès PSTN de l'aa est exigé, limitez les nombres ou la plage de nombres qui sont considérés valides par le script.

Tableaux de restriction de Cisco Unity Express

Abstrait

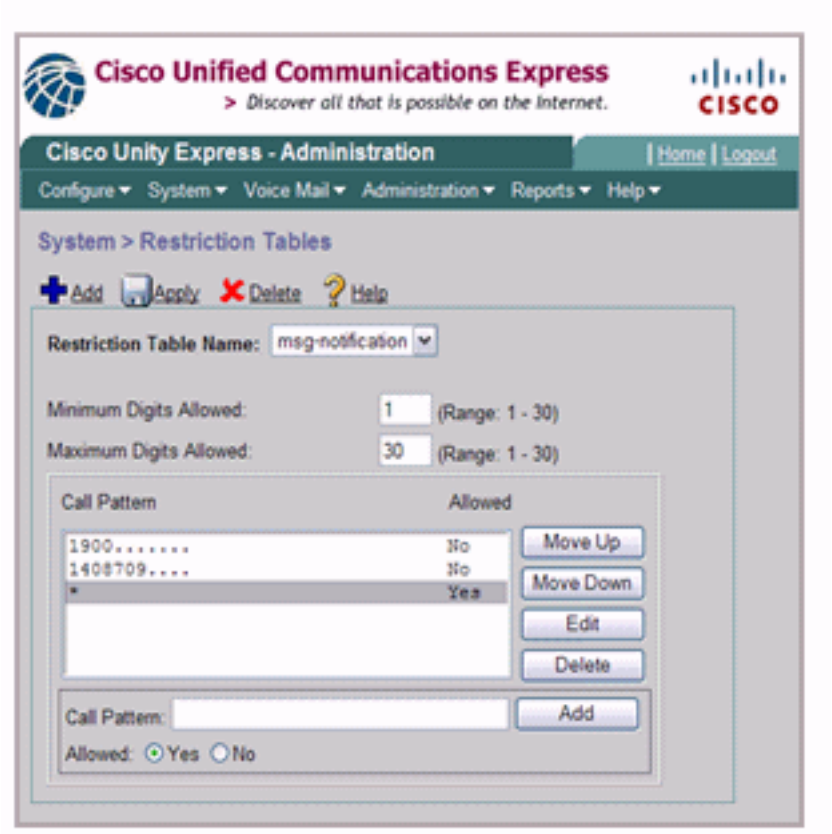
Vous pouvez employer les tables de restriction de Cisco Unity Express afin de limiter les destinations qui peuvent être atteintes pendant un outcall de Cisco Unity Express. La table de restriction de Cisco Unity Express peut être utilisée afin d'empêcher la fraude de contournement et l'utilisation malveillante du système de Cisco Unity Express de faire des appels sortants. Si vous utilisez la table de restriction de Cisco Unity Express, vous pouvez spécifier des modèles d'appel à la correspondance de caractère générique. Les applications qui utilisent la table de restriction de Cisco Unity Express incluent :

- Télécopie
- Rediffusion vivante de Cisco Unity Express
- Notification de message
- La livraison non abonnée de message

Remarque: C'est une **menace interne**.

Solution

Afin de limiter les modèles de destination qui peuvent être atteints par Cisco Unity Express sur un appel externe sortant, configurez le **modèle d'appel** dans le **système > les Tableaux de restrictions du** GUI de Cisco Unity Express.



Se connecter d'appel

CDR amélioré

Vous pouvez configurer le système de CME pour capturer le CDR amélioré et pour se connecter le CDR au flash du routeur ou à un ftp server externe. Ces enregistrements peuvent alors être utilisés pour retracer des appels pour voir si l'abus par les interlocuteurs internes ou externes s'est produit.

La fonctionnalité de comptabilisation de fichier introduite avec CME 4.3/7.0 dans la Cisco IOS version 12.4(15)XY fournit une méthode pour saisir des enregistrements des comptes dans le format de la valeur séparé par virgule (.csv) et pour enregistrer les enregistrements à un fichier dans l'éclair interne ou à un ftp server externe. Il développe le support de comptabilité de passerelle, qui inclut également l'AAA et les mécanismes de Syslog de se connecter l'information de comptabilité.

Le processus de comptabilité collecte des données de comptabilité pour chaque tronçon d'appel créé sur une passerelle de Voix de Cisco. Vous pouvez utiliser ces informations pour le courrier traitant des activités comme pour générer des enregistrements de facturation et pour l'analyse réseau. Les Passerelles voix de Cisco capturent des données de comptabilité sous forme d'articles mouvement d'appel (CDR) qui contiennent des attributs définis par Cisco. La passerelle

peut envoyer des CDR à un serveur de RAYON, serveur de Syslog, et avec la méthode de nouveau fichier, pour flasher ou un ftp server dans le format .csv.

Référez-vous aux exemples CDR pour plus d'informations sur les capacités améliorées CDR.

Informations connexes

- Pratiques recommandées de Sécurité de Cisco Unified Communications Manager Express
- Guide d'administrateurs exprès de Cisco Communications Manager
- Guide d'administrateurs exprès de Cisco Communications Manager – Blocage d'appel
- Compréhension de la mise en correspondance du homologue de numérotation sur des plates-formes IOS
- Conversion de numéros à l'aide de profils de conversion de voix
- Guide de conception de réseaux de référence de solution de CME
- Support et documentation techniques - Cisco Systems