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 la solution de contrôle des appels basée sur les routeurs de Cisco qui fournit une solution intelligente, simple et sécurisée pour les entreprises qui souhaitent mettre en oeuvre les communications unifiées. Il est fortement recommandé de mettre en oeuvre les mesures de sécurité décrites dans ce document afin de fournir des niveaux supplémentaires de contrôle de sécurité et de réduire les risques de fraude par téléphone.

L'objectif de ce document est de vous renseigner sur les différents outils de sécurité disponibles sur les passerelles vocales Cisco et CME. Ces outils peuvent être mis en oeuvre sur un système CME afin d'aider à atténuer la menace de fraude au péage par les parties internes et externes.

Ce document fournit des instructions sur la façon de configurer un système CME avec différents outils de sécurité des interurbains et de restriction des fonctionnalités. Le document explique également pourquoi certains outils de sécurité sont utilisés dans certains déploiements.

La flexibilité générale inhérente aux plates-formes ISR de Cisco vous permet de déployer CME dans de nombreux types de déploiements différents. Il peut donc être nécessaire d'utiliser une combinaison des fonctionnalités décrites dans ce document pour verrouiller le CME. Ce document sert de ligne directrice sur la façon d'appliquer les outils de sécurité à CME et ne garantit en aucune façon que des fraudes ou des abus par des parties internes et externes ne se produiront pas.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Communications Manager Express

Components Used

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

Remarque : Cisco Unified CME 7.0 inclut les mêmes fonctionnalités que Cisco Unified CME 4.3, qui est renuméroté 7.0 pour s'aligner sur les versions de Cisco Unified Communications.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

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 sécurité les plus courants qui peuvent être utilisés sur un système CME pour aider à atténuer la menace de fraude par télépéage. Les outils de sécurité CME référencés dans ce document incluent des outils de restriction de péage et des outils de restriction de fonctionnalité.

Outils de restriction de péage

- Sélection directe à l'arrivée
- Restriction de péage après les heures de bureau
- Classe de restriction
- Liste d'accès pour restreindre l'accès à la liaison H323/SIP

Outils de restriction de fonctionnalité

- Modèle de transfert
- Modèle de transfert bloqué
- Transfert max-length
- Longueur max. de renvoi d'appel
- Aucun renvoi d'appels locaux
- Pas d'ephone-rég automatique

Outils de restriction Cisco Unity Express

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

Enregistrement des appels

- Journalisation des appels pour capturer les enregistrements de détails des appels (CDR)

Menaces internes ou externes

Ce document traite des menaces provenant de parties internes et externes. Les parties internes incluent les utilisateurs de téléphones IP qui résident sur un système CME. Les parties externes incluent les utilisateurs de systèmes étrangers qui peuvent essayer d'utiliser le CME hôte pour passer des appels frauduleux et faire recharger les appels sur votre système CME.

Outils de restriction de péage

Sélection directe à l'arrivée

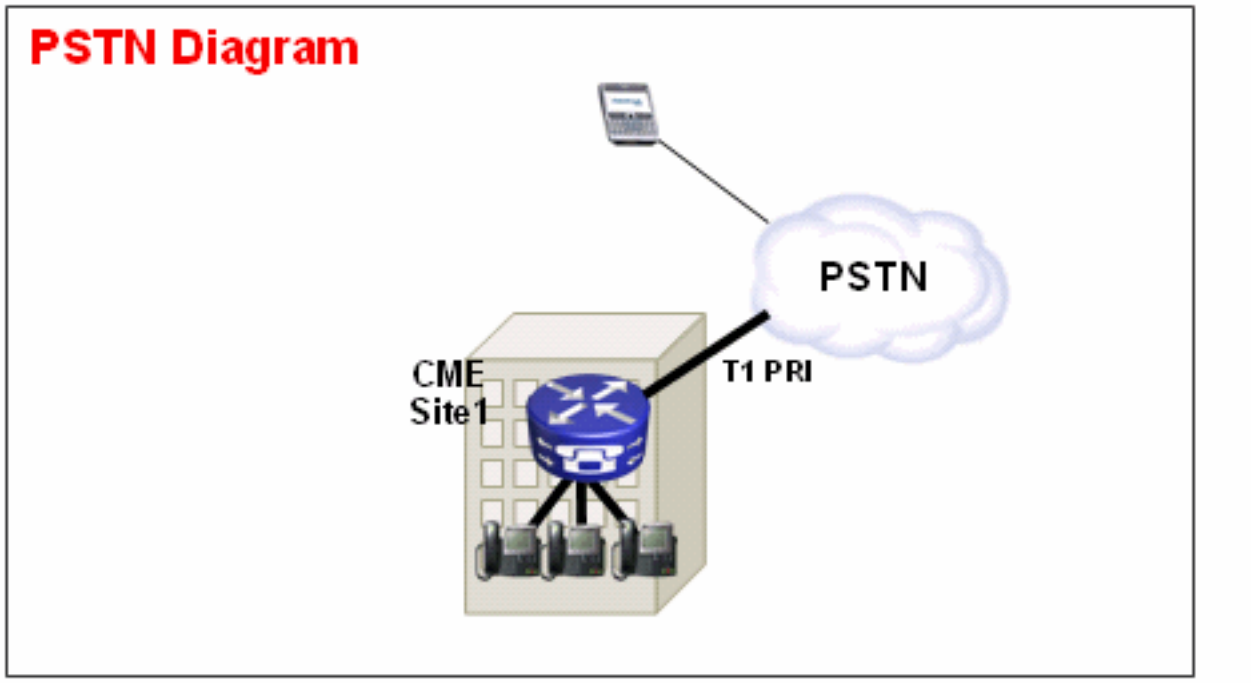
Résumé

La fonction DID (Direct-Inward-dial) est utilisée sur les passerelles vocales Cisco afin de permettre à la passerelle de traiter un appel entrant après avoir reçu des chiffres du commutateur PBX ou CO. Lorsque DID est activé, la passerelle Cisco ne présente pas de tonalité secondaire à l'appelant et n'attend pas de recueillir des chiffres supplémentaires auprès de l'appelant. Il transfère l'appel directement à la destination qui correspond au service d'identification du numéro composé entrant (DNIS). C'est ce qu'on appelle la numérotation en une étape.

Note : Il s'agit d'une **menace externe**.

Énoncé du problème

Si la numérotation directe vers l'intérieur n'est PAS configurée sur un modem routeur Cisco ou un CME, chaque fois qu'un appel arrive du central téléphonique ou du PBX vers le modem routeur Cisco, l'appelant entend une tonalité secondaire. C'est ce qu'on appelle la numérotation en deux étapes. Une fois que les appelants RTPC entendent la tonalité secondaire, ils peuvent saisir des chiffres pour accéder à n'importe quel poste interne ou, s'ils connaissent le code d'accès RTPC, ils peuvent composer des numéros longue distance ou internationaux. Cela pose un problème car l'appelant RTPC peut utiliser le système CME pour passer des appels interurbains ou internationaux sortants et la société est facturée pour les appels.



Exemple 1

Sur le site 1, le CME est connecté au RTPC via une liaison T1 PRI. Le fournisseur RTPC fournit le **40855512.** Plage DID pour le site CME 1. Ainsi, tous les appels RTPC destinés à 4085551200 - 4085551299 sont routés en entrée vers le CME. Si vous ne configurez pas la **numérotation directe entrante** sur le système, un appelant RTPC entrant entend une tonalité secondaire et doit composer manuellement le numéro de poste interne. Le plus gros problème est que si l'appelant est un abuseur et connaît le code d'accès PSTN sur le système, généralement **9**, il peut composer **9** puis n'importe quel numéro de destination qu'il veut atteindre.

Solution 1

Afin d'atténuer cette menace, vous devez configurer la **numérotation directe entrante**. La passerelle Cisco transfère ainsi l'appel entrant directement à la destination correspondant au DNIS entrant.

Exemple de configuration

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

Pour que DID fonctionne correctement, assurez-vous que l'appel entrant correspond au terminal de numérotation dial-peer POTS correct où la commande **direct-inward-dial** est configurée. Dans

cet exemple, le T1 PRI est connecté au port 1/0:23. Afin de faire correspondre le terminal de numérotation dial-peer entrant correct, émettez la commande **entrant call-number** dial peer sous le terminal de numérotation dial-peer DID POTS.

Exemple 2

Sur le site 1, le CME est connecté au RTPC via une liaison T1 PRI. Le fournisseur RTPC donne le **40855512.** et **40855513.** Plages DID pour le site CME 1. Ainsi, tous les appels RTPC destinés à 4085551200 - 4085551299 et 4085551300 - 4085551399 sont acheminés vers le CME.

Configuration incorrecte :

Si vous configurez un terminal de numérotation dial-peer entrant, comme dans l'exemple de configuration de cette section, la possibilité de fraude à l'interurbain persiste. Le problème avec ce terminal de numérotation dial-peer entrant est qu'il ne fait correspondre que les appels entrants à **40852512.** puis applique le service DID. Si un appel RTPC arrive dans **40852513..**, le terminal de numérotation dial-peer pots entrant ne correspond pas et le service DID n'est donc pas appliqué. Si un terminal de numérotation dial-peer entrant avec DID n'est pas mis en correspondance, le terminal de numérotation dial-peer par défaut 0 est utilisé. DID est désactivé par défaut sur le terminal de numérotation 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 le service DID sur un terminal de numérotation dial-peer entrant est présentée dans cet exemple :

Exemple de configuration

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

Référez-vous à Configuration DID pour les homologues de numérotation POTS pour plus d'informations sur DID pour les ports vocaux T1/E1 numériques.

Remarque : L'utilisation de DID **n**'est **pas** nécessaire lorsque la fonction de sonnerie automatique de ligne privée (PLAR) est utilisée sur un port vocal ou lorsqu'un script de service tel que la réception automatique (AA) est utilisé sur le terminal de numérotation dial-peer entrant.

Exemple de configuration : PLAR

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

Exemple de configuration - Script de service

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

Restrictions de péage en dehors des heures de bureau

Résumé

La restriction de péage après les heures de bureau est un nouvel outil de sécurité disponible dans CME 4.3/7.0 qui vous permet de configurer des stratégies de restriction de péage en fonction de l'heure et de la date. Vous pouvez configurer des stratégies de sorte que les utilisateurs ne soient pas autorisés à passer des appels vers des numéros prédéfinis pendant certaines heures de la journée ou tout le temps. Si la stratégie de blocage des appels 7x24 en dehors des heures de bureau est configurée, elle limite également l'ensemble de numéros qui peuvent être entrés par un utilisateur interne pour définir le **renvoi de tous les appels**.

Note : Il s'agit d'une **menace interne**.

Exemple 1

Cet exemple définit plusieurs modèles de chiffres pour lesquels les appels sortants sont bloqués. Les modèles 1 et 2, qui bloquent les appels vers des numéros externes commençant par « 1 » et « 011 », sont bloqués du lundi au vendredi avant 7 h et après 19 h, le samedi avant 7 h et après 13 h, et toute la journée le dimanche. Le modèle 3 bloque les appels vers 900 numéros 7 jours sur 7, 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 Configuration du blocage des appels pour plus d'informations sur la restriction de péage.

Classe de restriction

Résumé

Si vous voulez un contrôle granulaire lorsque vous configurez la restriction de péage, vous devez utiliser la classe de restriction (COR). Reportez-vous à Classe de restriction : Exemple pour plus d'informations.

Restrictions relatives aux fraudes aux numéros de téléphone des liaisons H.323/SIP

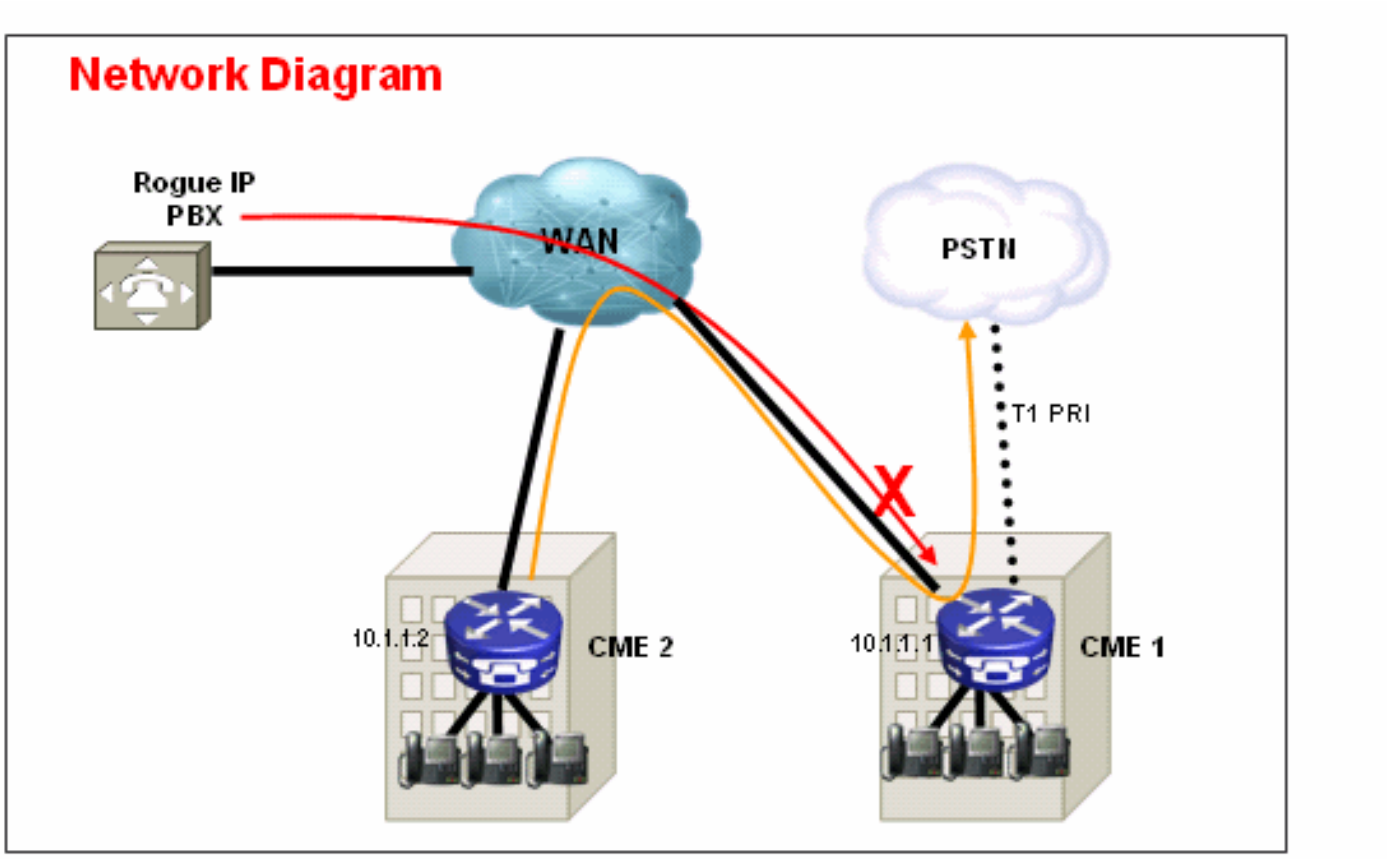
Résumé

Dans les cas où un système CME est connecté sur un WAN à d'autres périphériques CME via une liaison SIP ou H.323, vous pouvez restreindre l'accès de liaison SIP/H.323 au CME afin d'empêcher les utilisateurs malveillants d'utiliser votre système pour relayer illégalement des appels vers le RTPC.

Note : Il s'agit d'une **menace externe**.

Exemple 1

Dans cet exemple, CME 1 dispose d'une connectivité RTPC. CME 2 est connecté sur le WAN à CME 1 via une liaison H.323. Afin de sécuriser le CME 1, vous pouvez configurer une liste d'accès et l'appliquer en entrée sur l'interface WAN et ainsi autoriser uniquement le trafic IP en provenance de CME 2. Cela empêche le PBX IP non autorisé d'envoyer des appels VOIP via CME 1 au RTPC.



Solution

Ne laissez pas l'interface WAN sur CME 1 accepter le trafic provenant de périphériques non autorisés qu'elle ne reconnaît pas. Notez qu'il existe un REFUS implicite à la fin d'une liste d'accès. Si vous souhaitez autoriser le trafic IP entrant sur d'autres périphériques, veillez à ajouter l'adresse IP du périphérique à la liste d'accès.

Exemple de configuration : CME 1

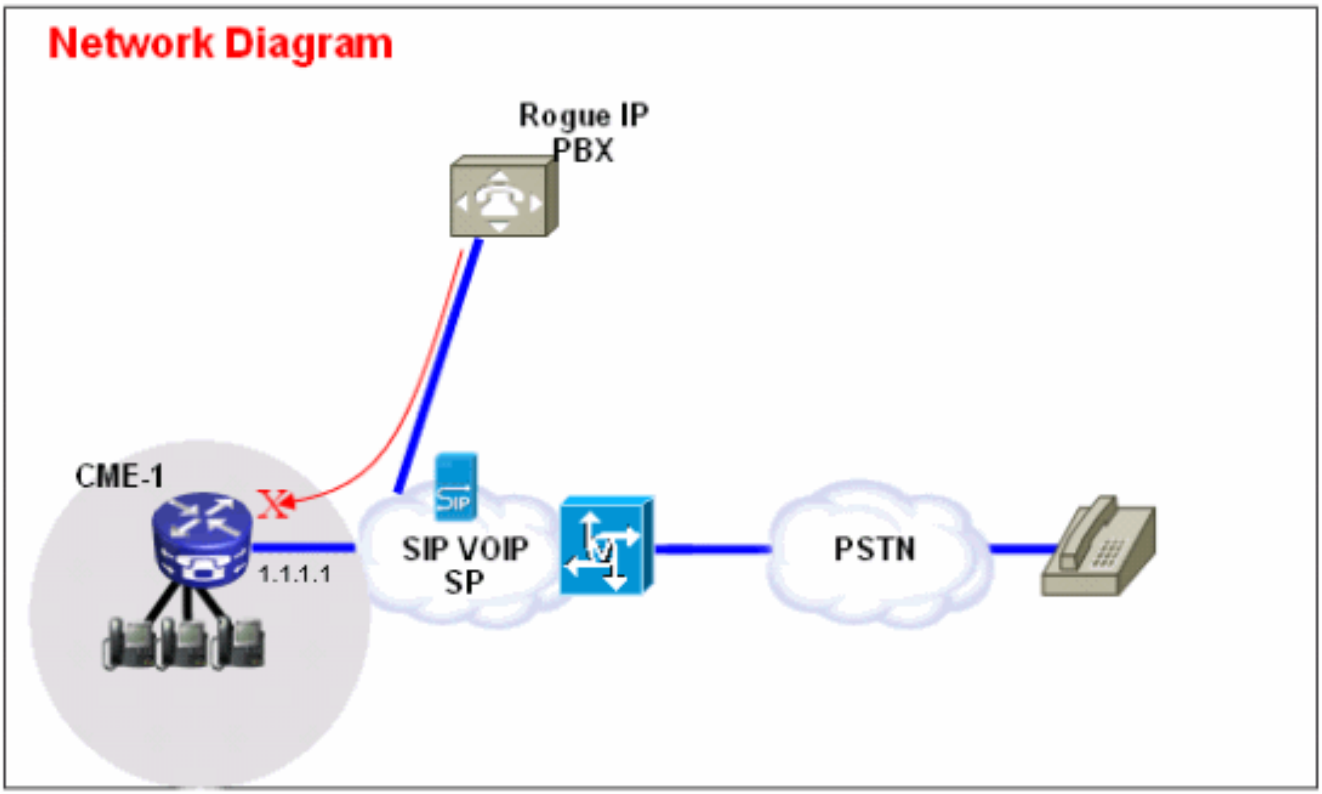
```
interface serial 0/0
  ip access-group 100 in
```

```
!
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 SIP pour la connectivité RTPC avec l'exemple de configuration fourni à l'exemple de configuration de liaison SIP de Cisco CallManager Express (CME).

Étant donné que CME 1 se trouve sur l'Internet public, il est possible qu'une *fraude* à *péage* se produise si un utilisateur non autorisé analyse les adresses IP publiques des ports connus pour détecter la signalisation H.323 (TCP 1720) ou SIP (UDP ou TCP 5060) et envoie des messages SIP ou H.323 qui acheminent les appels en provenance de la liaison SIP. RTPC. Les abus les plus courants dans ce cas sont que l'utilisateur non autorisé effectue plusieurs appels internationaux via la liaison SIP ou H.323 et que le propriétaire du CME 1 paie ces appels de fraude à péage - dans certains cas des milliers de dollars.



Solution

Afin d'atténuer cette menace, vous pouvez utiliser plusieurs solutions. Si aucune signalisation VOIP (SIP ou H.323) n'est utilisée sur les liaisons WAN dans CME 1, elle doit être bloquée autant que possible par les techniques de pare-feu sur CME 1 (listes d'accès ou listes de contrôle d'accès).

1. Sécurisez l'interface WAN avec le pare-feu Cisco IOS® sur CME 1 :Cela implique que vous autorisez uniquement le trafic SIP ou H.323 connu à entrer sur l'interface WAN. Tout autre trafic SIP ou H.323 est bloqué. Cela nécessite également que vous connaissiez les adresses IP utilisées par le fournisseur de services SIP VOIP pour la signalisation sur la ligne principale SIP. Cette solution suppose que le fournisseur de services est prêt à fournir toutes les adresses IP ou tous les noms DNS qu'il utilise sur son réseau. En outre, si des noms

DNS sont utilisés, la configuration nécessite qu'un serveur DNS capable de résoudre ces noms soit accessible. En outre, si le SP modifie des adresses à leur extrémité, la configuration doit être mise à jour sur CME 1. Notez que ces lignes doivent être ajoutées en plus des entrées de liste de contrôle d'accès déjà présentes sur l'interface WAN.Exemple de configuration : 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-vous que les appels entrants sur la ligne principale SIP ne sortent **PAS** en épingle à oreilles :Cela signifie que la configuration CME 1 autorise uniquement la coiffure SIP - SIP des appels vers une plage de numéros RTPC connue spécifique, tous les autres appels étant bloqués. Vous devez configurer des terminaux de numérotation dial-peer entrants spécifiques pour les numéros RTPC qui arrivent sur la ligne principale SIP et qui sont mappés à des postes ou à un ou plusieurs standard(s) automatique(s) ou à la messagerie vocale sur CME 1. Tous les autres appels vers des numéros qui ne font pas partie de la plage de numéros RTPC CME 1 sont bloqués. Remarque : cela n'affecte pas le renvoi/transfert d'appels vers la messagerie vocale (Cisco Unity Express) et le renvoi de tous les appels vers les numéros RTPC à partir des téléphones IP sur CME 1, car l'appel initial est toujours ciblé sur un poste sur CME 1.Exemple de configuration : 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. Utilisez des règles de traduction afin de bloquer des chaînes de numérotation spécifiques :La plupart des fraudes à l'interurbain impliquent la numérotation internationale. Par conséquent, vous pouvez créer un terminal de numérotation dial-peer entrant spécifique qui correspond à des chaînes composées spécifiques et bloque les appels vers eux. La plupart des CME utilisent un code d'accès spécifique, tel que 9, pour composer un numéro sortant et le code de numérotation international aux États-Unis est 011. Par conséquent, la chaîne de numérotation la plus courante à bloquer aux États-Unis est 9011 + n'importe quel chiffre après celui qui arrive sur la ligne principale SIP.Exemple de configuration : 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 fonctionnalité

Modèle de transfert

Résumé

Les transferts vers tous les numéros sauf ceux des téléphones IP SCCP locaux sont automatiquement bloqués par défaut. Lors de la configuration, vous pouvez autoriser les transferts vers des numéros non locaux. La commande **transfer-pattern** est utilisée afin de permettre le transfert d'appels téléphoniques des téléphones IP Cisco SCCP vers des téléphones autres que les téléphones IP Cisco, tels que les appels RTPC externes ou les téléphones d'un autre système CME. Vous pouvez utiliser le **modèle de transfert** afin de limiter les appels aux postes internes uniquement ou peut-être limiter les appels aux numéros RTPC dans un code régional spécifique uniquement. Ces exemples montrent comment la commande **transfer-pattern** peut être utilisée pour limiter les appels à différents numéros.

Note : Il s'agit d'une **menace interne**.

Exemple 1

Autoriser les utilisateurs à transférer des appels vers l'indicatif régional 408 uniquement. Dans cet exemple, l'hypothèse est que le CME est configuré avec un terminal de numérotation dial-peer qui a un modèle de destination de 9T.

Exemple de configuration

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

Modèle de transfert bloqué

Résumé

Dans Cisco Unified CME 4.0 et les versions ultérieures, vous pouvez empêcher des téléphones individuels de transférer des appels vers des numéros qui sont globalement activés pour le transfert. La commande **transfer-pattern block** remplace la commande **transfer-pattern** et désactive le transfert d'appel vers n'importe quelle destination qui doit être atteinte par un terminal de terminal de téléphonie sur POTS ou un terminal de numérotation dial-peer VoIP. Cela inclut les numéros RTPC, les autres passerelles vocales et Cisco Unity Express. Cela permet de s'assurer que les téléphones individuels ne sont pas facturés lorsque les appels sont transférés en dehors du système Cisco Unified CME. Le blocage du transfert d'appels peut être configuré pour des téléphones individuels ou dans le cadre d'un modèle appliqué à un ensemble de téléphones.

Note : Il s'agit d'une **menace interne**.

Exemple 1

Dans cet exemple de configuration, l'ephone 1 n'est pas autorisé à utiliser le modèle de transfert (défini globalement) pour transférer des appels, tandis que l'ephone 2 peut utiliser le modèle de transfert défini sous telephony-service pour transférer des appels.

Exemple de configuration

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

Transfert max-length

Résumé

La commande **transfer max-length** spécifie le nombre maximal de chiffres que l'utilisateur peut composer lorsqu'un appel est transféré. La **longueur maximale du modèle de transfert** dépasse la commande **transfer-pattern** et applique les chiffres maximaux autorisés pour la destination de transfert. L'argument spécifie le nombre de chiffres autorisés dans un numéro vers lequel un appel est transféré. Plage : 3 à 16. Par défaut : 16.

Note : Il s'agit d'une **menace interne**.

Exemple 1

Cette configuration autorise uniquement les téléphones auxquels ce modèle ephone est appliqué à transférer vers des destinations d'une longueur maximale de quatre chiffres.

Exemple de configuration

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

Longueur max. du renvoi d'appels

Résumé

Afin de limiter le nombre de chiffres pouvant être entrés avec la touche de fonction CfwdALL sur un téléphone IP, utilisez la commande **call-forward max-length** en mode de configuration ephone-dn ou ephone-dn-template. Afin de supprimer une restriction sur le nombre de chiffres pouvant être entrés, utilisez la forme **no** de cette commande.

Note : Il s'agit d'une **menace interne**.

Exemple 1

Dans cet exemple, le poste d'annuaire 101 est autorisé à effectuer un renvoi d'appel vers

n'importe quel poste d'une à quatre chiffres. Tout renvoi d'appels vers des destinations de plus de quatre chiffres échoue.

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 de transfert

Résumé

Lorsque la commande **no forward local-appels** est utilisée en mode de configuration ephone-dn, les appels internes vers un ephone-dn particulier sans **renvoi d'appels locaux** appliqués ne sont pas transférés si l'ephone-dn est occupé ou ne répond pas. Si un appelant interne sonne cet ephone-dn et que l'ephone-dn est occupé, l'appelant entend un signal occupé. Si un appelant interne sonne cet ephone-dn et ne répond pas, il entend un signal de retour. L'appel interne n'est pas transféré même si le renvoi d'appels est activé pour l'ephone-dn.

Note : Il s'agit d'une **menace interne**.

Exemple 1

Dans cet exemple, le poste 222 appelle le poste 3675 et entend une sonnerie ou un signal occupé. Si un appelant externe atteint le poste 3675 et qu'il n'y a pas de réponse, l'appel est transféré au poste 4000.

Exemple de configuration

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

Désactiver l'enregistrement automatique sur le système CME

Résumé

Lorsque **auto-reg-ephone** est activé sous telephony-service sur un système CME SCCP, les nouveaux téléphones IP connectés au système sont enregistrés automatiquement et si **auto assignation** est configurée pour attribuer automatiquement des numéros de poste, alors un nouveau téléphone IP peut passer des appels immédiatement.

Note : Il s'agit d'une **menace interne**.

Exemple 1

Dans cette configuration, un nouveau système CME est configuré de sorte que vous devez ajouter manuellement un ephone pour que l'ephone s'enregistre sur le système CME et l'utilise pour passer des appels de téléphonie IP.

Solution

Vous pouvez désactiver **auto-reg-ephone** sous telephony-service afin que les nouveaux téléphones IP connectés à un système CME ne s'enregistrent pas automatiquement sur le système CME.

Exemple de configuration

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

Exemple 2

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

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

Reportez-vous à SIP : Configuration de Cisco Unified CME pour un guide de configuration plus complet pour SIP CME.

Outils de restriction Cisco Unity Express

Cisco Unity Express sécurisé : Accès RTPC AA

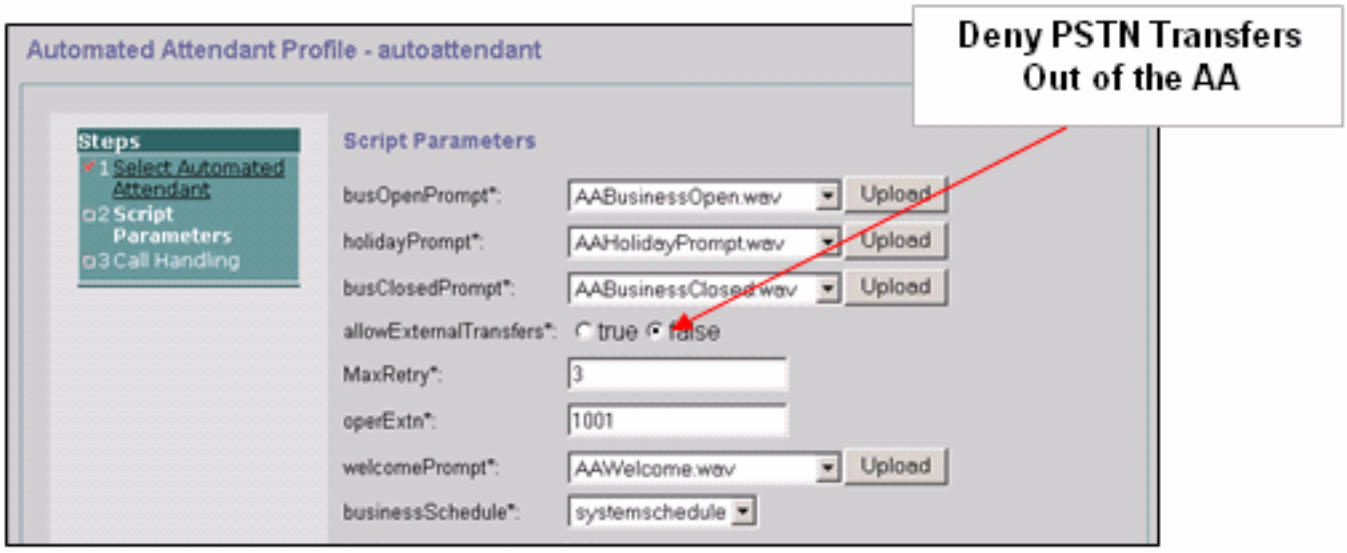
Résumé

Lorsque votre système est configuré de sorte que les appels entrants soient transférés à la réception automatique (AA) sur Cisco Unity Express, il peut être nécessaire de désactiver le transfert externe vers le RTPC à partir de Cisco Unity Express AA. Cela ne permet pas aux utilisateurs externes de composer des numéros sortants vers des numéros externes après qu'ils aient atteint Cisco Unity Express AA.

Note : Il s'agit d'une **menace externe**.

Note: Solution

Remarque : désactivez l'option **allowExternalTransfers** sur l'interface utilisateur graphique de Cisco Unity Express.



Remarque : Si un accès RTPC à partir de l'AA est requis, limitez les nombres ou la plage de nombres considérés valides par le script.

Tables de restrictions Cisco Unity Express

Résumé

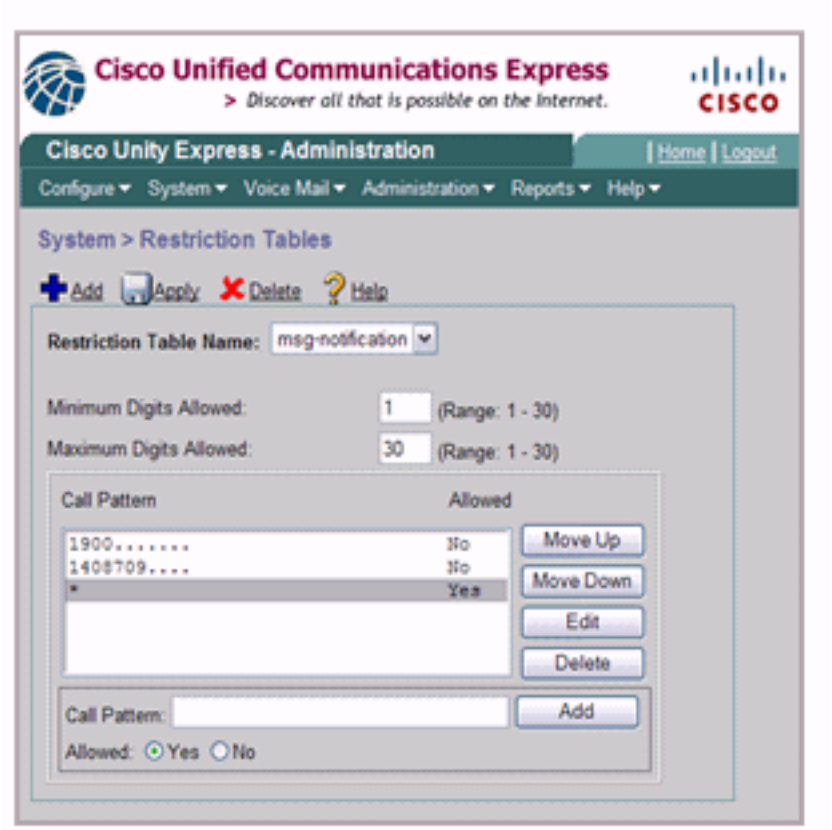
Vous pouvez utiliser les tables de restrictions de Cisco Unity Express afin de restreindre les destinations qui peuvent être atteintes lors d'un appel sortant de Cisco Unity Express. La table de restrictions de Cisco Unity Express peut être utilisée afin d'empêcher les fraudes et l'utilisation malveillante du système Cisco Unity Express pour passer des appels sortants. Si vous utilisez la table de restrictions de Cisco Unity Express, vous pouvez spécifier des modèles d'appel pour une correspondance de caractères génériques. Les applications qui utilisent la table de restrictions Cisco Unity Express sont les suivantes :

- Télécopie
- Rediffusion en direct de Cisco Unity Express
- Notification de message
- Remise de messages non abonnés

Note : Il s'agit d'une **menace interne**.

Solution

Afin de restreindre les modèles de destination qui peuvent être atteints par Cisco Unity Express sur un appel externe sortant, configurez le **modèle d'appel** dans **System > Restrictions Tables** de l'interface utilisateur graphique de Cisco Unity Express.



Enregistrement des appels

CDR amélioré

Vous pouvez configurer le système CME pour capturer le CDR amélioré et enregistrer le CDR sur la mémoire flash du routeur ou sur un serveur FTP externe. Ces enregistrements peuvent ensuite être utilisés pour retracer les appels afin de voir si des tiers internes ou externes ont abusé.

La fonctionnalité de gestion des fichiers introduite avec CME 4.3/7.0 dans Cisco IOS version 12.4(15)XY fournit une méthode pour capturer les enregistrements comptables au format .csv (valeur séparée par des virgules) et stocker les enregistrements dans un fichier dans la mémoire flash interne ou sur un serveur FTP externe. Il étend la prise en charge de la comptabilité de passerelle, qui inclut également les mécanismes AAA et syslog de journalisation des informations de comptabilité.

Le processus de comptabilisation collecte des données de comptabilisation pour chaque segment d'appel créé sur une passerelle vocale Cisco. Vous pouvez utiliser ces informations pour des activités de post-traitement telles que la génération d'enregistrements de facturation et l'analyse du réseau. Les passerelles vocales Cisco capturent les données comptables sous la forme d'enregistrements de détails d'appels (CDR) contenant des attributs définis par Cisco. La passerelle peut envoyer des CDR à un serveur RADIUS, à un serveur syslog et avec la nouvelle méthode de fichier, à la mémoire Flash ou à un serveur FTP au format .csv.

Référez-vous à Exemples de CDR pour plus d'informations sur les fonctionnalités Enhanced CDR.

Informations connexes

- Meilleures pratiques de sécurité de Cisco Unified Communications Manager Express

- Guide des administrateurs de Cisco Communications Manager Express
- Guide des administrateurs de Cisco Communications Manager Express - Blocage des appels
- Présentation de la correspondance des homologues de numérotation sur les plates-formes IOS
- Conversion de numéros à l'aide de profils de conversion de voix
- Guide de conception du réseau de référence de la solution CME
- Support et documentation techniques - Cisco Systems