مدير الاتصالات الموحدة Express منع الاحتيال بالمكالمات غير المجانية

المحتويات

المقدمة

يقدم هذا المستند دليل تكوين يمكن إستخدامه للمساعدة في تأمين نظام Cisco Communications Manager Express (CME) والتخفيف من تهديد الاحتيال في المكالمات. CME هو حل التحكم في المكالمات المستند إلى موجه Cisco الذي يوفر حلا ذكيا وبسيطا وآمنا للمؤسسات التي تريد تنفيذ الاتصالات الموحدة. يوصى بشدة بتنفيذ التدابير الأمنية الموضحة في هذا المستند من أجل توفير مستويات إضافية من التحكم في الأمان والحد من إمكانية حدوث حالات غش بسبب المكالمات الهاتفية.

الهدف من هذا المستند هو تعليمك حول أدوات الأمان المختلفة المتوفرة على بوابات الصوت من Cisco و CME. يمكن تطبيق هذه الأدوات على نظام CME للمساعدة في الحد من خطر الاحتيال في الرسوم من قبل الأطراف الداخلية والخارجية على حد سواء.

يزود هذا وثيقة تعليم على كيف أن يشكل نظام CME مع مختلف رسوم التأمين وأداة تقييد سمة. كما تحدد الوثيقة لماذا يتم إستخدام أدوات أمان معينة في عمليات نشر معينة.

تتيح لك المرونة الكلية الكامنة في أنظمة ISR الأساسية من Cisco نشر إدارة البنية الأساسية (CME) في العديد من أنواع النشر المختلفة. وبالتالي، يمكن مطالبته باستخدام مجموعة من الميزات الموضحة في هذا المستند للمساعدة في تأمين بنية إدارة البنية الأساسية (CME). تستخدم هذه الوثيقة كدليل إرشادي لكيفية تطبيق الأدوات الأمنية على "البنية التحتية البحرية" ولا تضمن بأي شكل من الأشكال عدم حدوث غش أو إساءة إستخدام من قبل كل من الأطراف الداخلية والخارجية.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- مدير الاتصالات الموحدة الفائق من Cisco

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى Cisco Unified Communications Manager Express 4.3 و CME 7.0.

ملاحظة: يتضمن Cisco Unified CME 7.0 نفس الميزات مثل Cisco Unified CME 4.3، التي يتم ترقيمها إلى 7.0 للمحاذاة مع إصدارات الاتصالات الموحدة من Cisco.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

نظرة عامة

يغطي هذا المستند أكثر أدوات الأمان شيوعا التي يمكن إستخدامها على نظام الحماية المادية (CME) للمساعدة في الحد من تهديد الاحتيال في المكالمات الهاتفية. تتضمن أدوات أمان CME المشار إليها في هذا المستند أدوات تقييد رسوم المرور وأدوات تقييد الميزات.

أدوات تقييد رسوم المكالمات

- الطلب الداخلي المباشر
- تقييد عدد المكالمات بعد ساعات العمل
- فئة التقييد
- قائمة الوصول لتقييد الوصول إلى خط اتصال H323/SIP

أدوات تقييد الميزة

- نمط النقل
- تم حظر نمط النقل
- الحد الأقصى لطول التحويل
- الحد الأقصى لطول المكالمة الأمامية
- عدم إعادة توجيه المكالمات المحلية
- لا يوجد هاتف Auto-reg-ephone

أدوات التقييد Cisco Unity Express

- الوصول الآمن إلى PSTN Unity Express من Cisco
- تقييد إخطار الرسالة

تسجيل المكالمات

- تسجيل المكالمات لالتقاط سجلات تفاصيل المكالمة (CDRs)

التهديدات الداخلية مقابل التهديدات الخارجية

وتناقش هذه الوثيقة التهديدات من كل من الأطراف الداخلية والخارجية. تتضمن الأطراف الداخلية مستخدمي هاتف بروتوكول الإنترنت الموجودين على نظام CME. تتضمن الأطراف الخارجية المستخدمين على الأنظمة الأجنبية التي يمكنها محاولة إستخدام CME المضيف لإجراء مكالمات احتيالية وإرسال المكالمات إلى نظام CME الخاص بك.

أدوات تقييد رسوم المكالمات

الطلب الداخلي المباشر

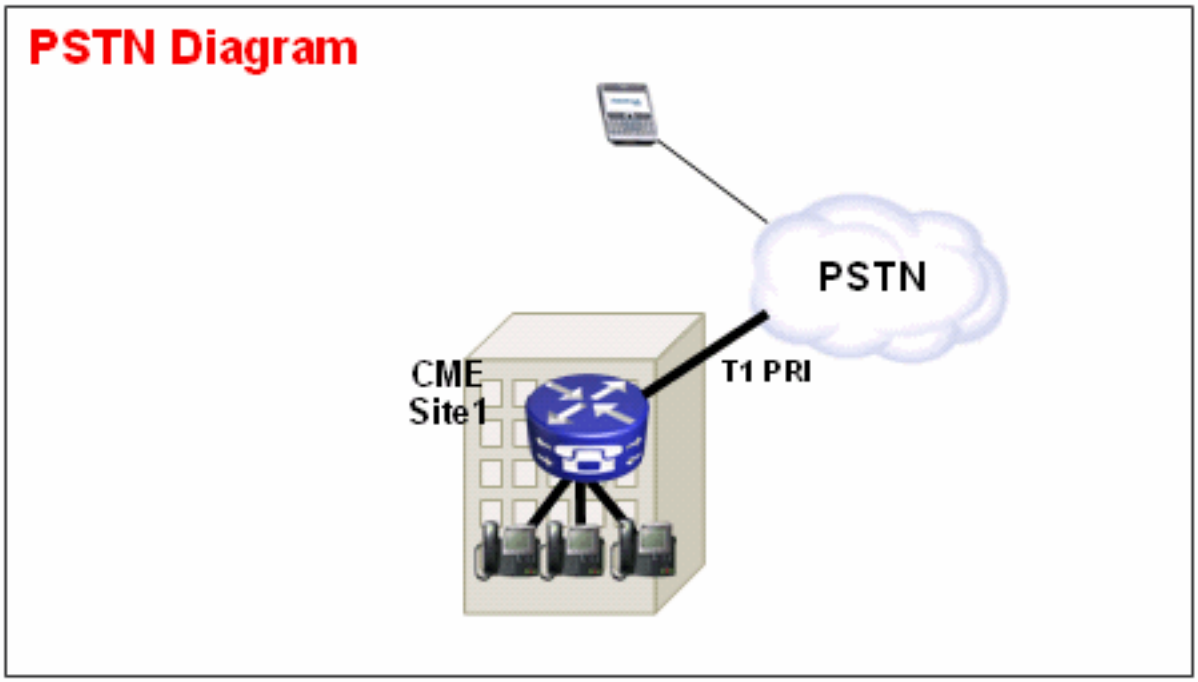
مجرد

يتم إستخدام الطلب الداخلي المباشر (DID) على بوابات الصوت من Cisco للسماح للعبارة بمعالجة مكالمة واردة بعد أن تستلم أرقام من محول PBX أو CO. عند تمكين DID، لا تقدم بوابة Cisco نغمة طلب ثانوية للمتصل ولا تنتظر لجمع أرقام إضافية من المتصل. إنه يعيد توجيه المكالمة مباشرة إلى الوجهة التي تطابق خدمة التعرف على الرقم المطلوب الوارد (DNIS). يسمى هذا الاتصال من مرحلة واحدة.

ملاحظة: هذا **تهديد خارجي**.

بيان المشكلة

إذا لم يتم تكوين الطلب الداخلي المباشر على بوابة Cisco أو CME، كلما ظهرت مكالمة من CO أو PBX إلى بوابة Cisco، يسمع المتصل نغمة طلب ثانوية. يسمى هذا الاتصال على مرحلتين. بمجرد أن يسمع متصلون PSTN نغمة الطلب الثانوية، يمكنهم إدخال أرقام للوصول إلى أي امتداد داخلي أو إذا كانوا يعرفون رمز الوصول إلى PSTN، يمكنهم الطلب لمسافات طويلة أو أرقام دولية. وهذا يمثل مشكلة لأن المتصل بشبكة PSTN يمكنه إستخدام نظام CME لإجراء المكالمات الخارجية البعيدة أو الدولية ويتم تحميل الشركة تكلفة المكالمات.



مثال 1

في الموقع 1، يتم توصيل CME ببروتوكول PSTN من خلال خط اتصال T1 PRI. يوفر مزود **4085512** PSTN. نطاق DID لموقع CME 1. لذلك يتم توجيه جميع مكالمات PSTN الموجهة ل 4085551200 - 408551299 إلى CME. إذا لم تقم بتكوين **الطلب الداخلي المباشر** على النظام، فسيقوم متصل PSTN الوارد بسماع نغمة طلب ثانوية ويجب عليه طلب الملحق الداخلي يدويا. المشكلة الأكبر هي أنه إذا كان المتصل مسيئا ويعرف رمز الوصول إلى PSTN على النظام، وبشكل عام **9**، فيمكنهم الاتصال **9** ثم أي رقم الوجهة الذي يرغبون في الوصول إليه.

الحل 1

للحد من هذا التهديد، يجب تكوين **الطلب الداخلي المباشر**. وهذا يتسبب في قيام بوابة Cisco بإعادة توجيه المكالمة الواردة مباشرة إلى الوجهة التي تطابق DNIS الوارد.

عينة من التكوين

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

لعمل DID بشكل صحيح، تأكد من تطابق المكالمة الواردة مع نظير POTS الصحيح حيث تم تكوين الأمر **direct-inward-dial**. في هذا المثال، يتم توصيل T1 PRI بالمنفذ 0:23/1. لمطابقة نظير الطلب الوارد الصحيح، قم بإصدار أمر نظير الطلب **الوارد** باسم **الرقم** أسفل نظير الطلب DID POTS.

مثال 2

في الموقع 1، يتم توصيل CME ببروتوكول PSTN من خلال خط اتصال T1 PRI. يعطي موفر **40855512** PSTN. و**40855513..** نطاقات DID لموقع CME 1. لذلك يتم توجيه جميع مكالمات PSTN الموجهة ل 408551200 - 408551299 و 408551300 - 408551399 إلى CME.

تكوين غير صحيح:

إذا قمت بتكوين نظير اتصال داخلي، كما هو الحال في تكوين العينة في هذا القسم، فإن إمكانية حدوث غش في رسوم المكالمات ما تزال موجودة. المشكلة مع نظير الطلب الوارد هذا هي أنه يطابق المكالمات الواردة فقط إلى

40852512.. ثم يطبق خدمة DID. إذا تم إستدعاء PSTN في **40852513..**، فإن نظير الطلب الداخلي لا يتطابق وبالتالي لا يتم تطبيق خدمة DID. إذا لم تتم مطابقة نظير اتصال داخلي مع DID، فيتم إستخدام نظير الطلب الافتراضي 0. DID معطل بشكل افتراضي على نظير الطلب 0.

عينة من التكوين

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

التكوين الصحيح

يتم عرض الطريقة الصحيحة لتكوين خدمة DID على نظير الطلب الوارد في هذا المثال:

عينة من التكوين

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

أحلت DID تشكيل ل POTS طلب نظير ل كثير معلومة على DID ل رقمي T1/E1 صوت ميناء.

ملاحظة: لا يلزم إستخدام DID عندما يتم إستخدام PLAR) Private-Line Automatic RingDown) على منفذ صوت أو يتم إستخدام برنامج نصي للخدمة مثل AA) Auto-Attendant) على نظير الطلب الوارد.

نموذج التكوين—PLAR

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

نموذج التكوين—برنامج نصي للخدمة

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

قيود رسوم ما بعد ساعات العمل

مجرد

After-Hours Toll Restriction هو أداة أمان جديدة متوفرة في CME 4.3/7.0 تسمح لك بتكوين سياسات تقييد رسوم المكالمات بناء على الوقت والتاريخ. يمكنك تكوين السياسات بحيث لا يسمح للمستخدمين بإجراء مكالمات إلى أرقام محددة مسبقا خلال ساعات معينة من اليوم أو طوال الوقت. في حالة تكوين نهج حظر المكالمات على مدار 24 ساعة طوال ساعات العمل، فإنه يقيد أيضا مجموعة الأرقام التي يمكن إدخالها بواسطة مستخدم داخلي لتعيين **إعادة توجيه المكالمات الكل**.

ملاحظة هذا **تهديد داخلي**.

مثال 1

يحدد هذا المثال عدة أنماط من الأرقام التي يتم حظر المكالمات الصادرة لها. تم حظر الرقمين 1 و 2، اللذين يحجبان إستدعاءات الأرقام الخارجية التي تبدأ ب "1" و "011"، من الاثنين إلى الجمعة قبل السابعة صباحا وبعد السابعة

مساء، السبت قبل السابعة صباحا وبعد الواحدة ظهرا، ويوم الأحد طوال اليوم. يقوم النمط 3 بحظر المكالمات إلى 900 رقم 7 أيام في الأسبوع، 24 ساعة في اليوم.

عينة من التكوين

```
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
```

ارجع إلى تكوين حظر المكالمات للحصول على مزيد من المعلومات حول تقييد رسوم المكالمات.

فئة التقييد

مجرد

إذا كنت ترغب في التحكم متعدد المستويات عند تكوين تقييد الرسوم، يجب إستخدام فئة التقييد (COR). راجع فئة التقييد: مثال للحصول على مزيد من المعلومات.

H.323 / قيود الاحتيال في شبكات SIP

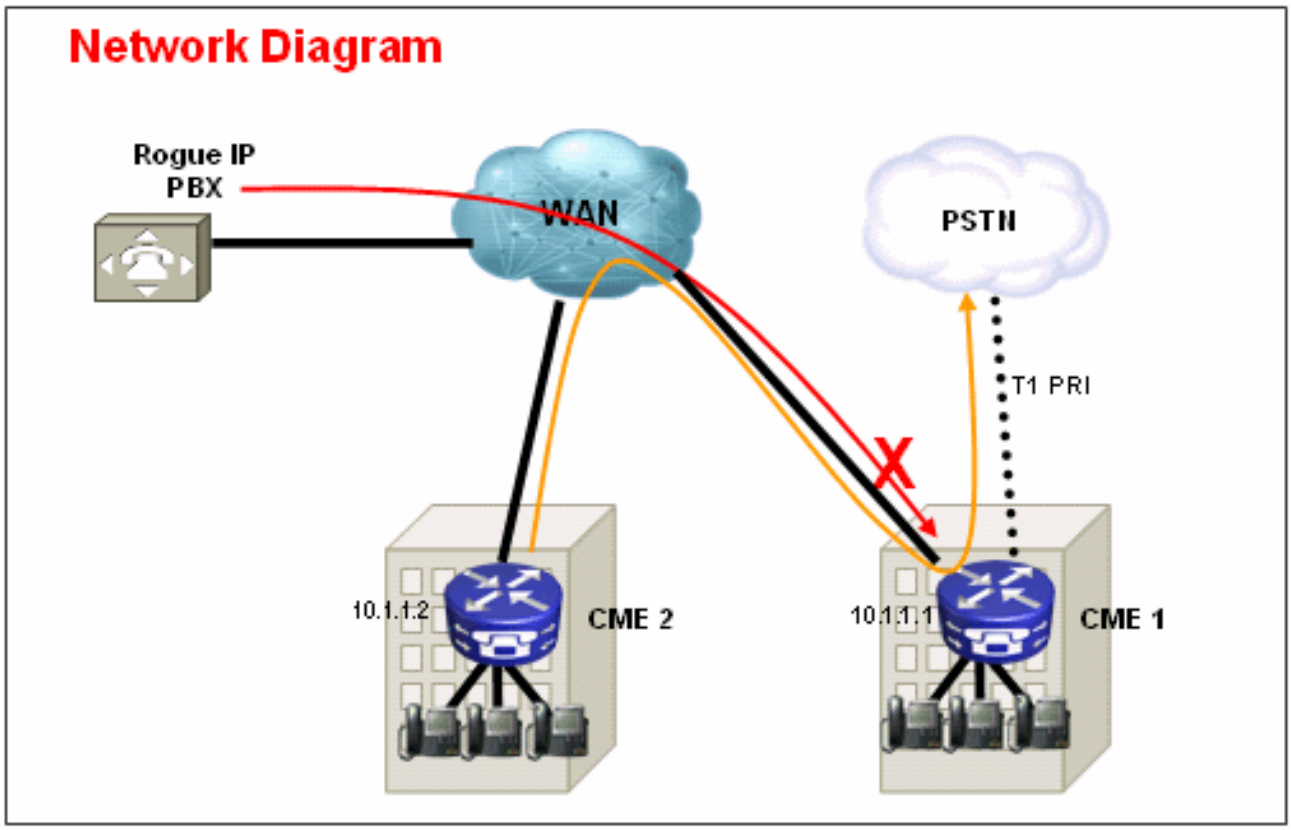
مجرد

في الحالات التي يتم فيها توصيل نظام CME عبر شبكة WAN بأجهزة CME الأخرى من خلال SIP أو خط اتصال H.323، يمكنك تقييد وصول خط اتصال SIP/H.323 إلى CME لمنع المسيئين من إستخدام نظامك لترحيل المكالمات إلى PSTN بشكل غير قانوني.

ملاحظة: هذا **تهديد خارجي**.

مثال 1

في هذا المثال، يحتوي CME 1 على اتصال PSTN. يتم توصيل CME 2 عبر شبكة WAN ب CME 1 من خلال خط اتصال H.323. لتأمين CME 1، يمكنك تكوين قائمة وصول وتطبيقها على واجهة WAN وبالتالي السماح بحركة مرور IP من CME 2 فقط. وهذا يؤدي إلى منع IP PBX المخادع من إرسال مكالمات VoIP من خلال CME 1 إلى PSTN.



الحل

لا تسمح لواجهة WAN على CME 1 بقبول حركة مرور البيانات من الأجهزة المخادعة التي لا تتعرف عليها. لاحظ وجود رفض ضمني للكل في نهاية قائمة الوصول. إذا كان هناك المزيد من الأجهزة التي تريد السماح بحركة مرور IP الواردة منها، فتأكد من إضافة عنوان IP الخاص بالجهاز إلى قائمة الوصول.

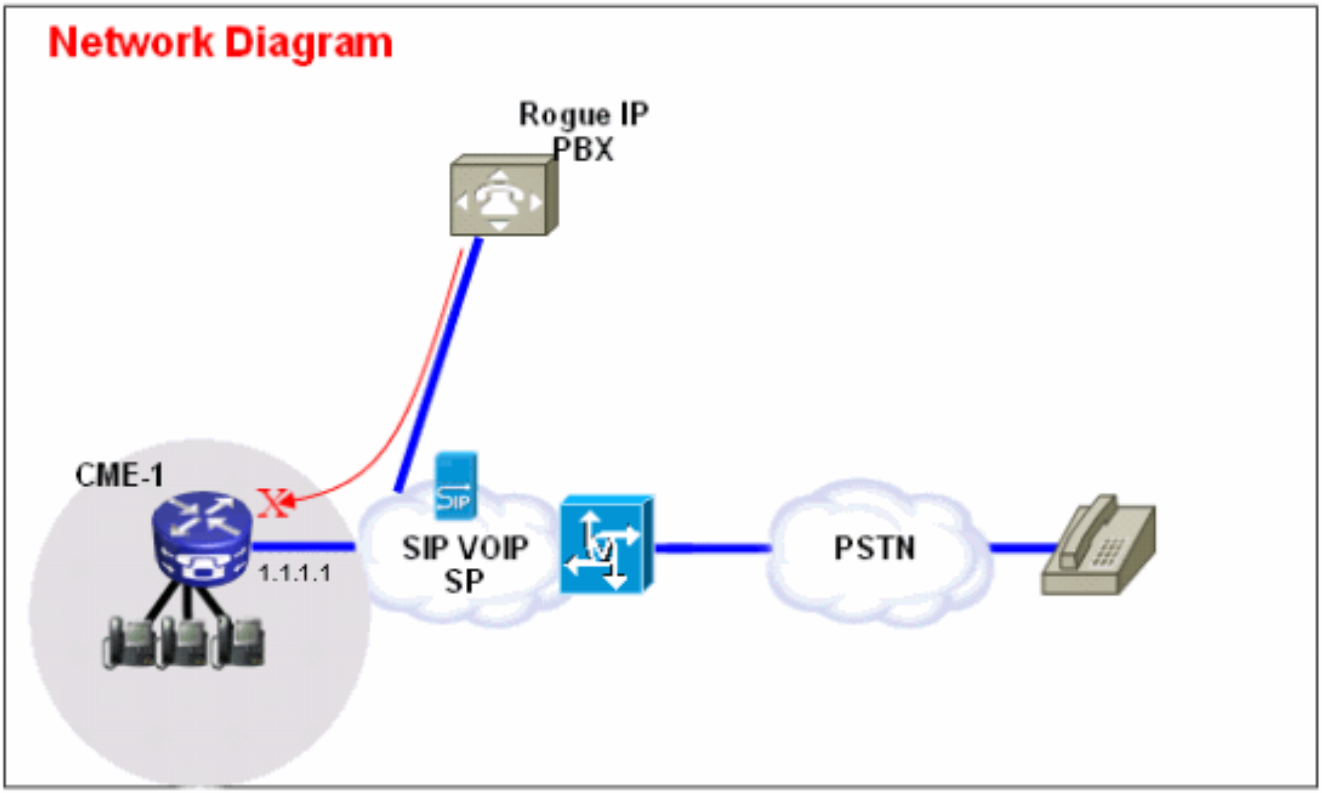
نموذج التكوين—CME 1

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

مثال 2

في هذا المثال، يتم توصيل CME 1 بموفر SIP لاتصال PSTN باستخدام نموذج التكوين المتوفر في مثال تكوين توصيل SIP (CME) Cisco CallManager Express.

بما أن CME 1 يكون على الإنترنت العام، من الممكن أن *إحتيال الرسوم* يمكن أن يحدث إذا قام مستخدم مارق بفحص عناوين IP العامة للمنافذ المعروفة ل H.323 (TCP 1720) أو SIP (UDP أو TCP 5060) يرسل رسائل SIP أو H.323 التي توجه المكالمات من خط اتصال SIP إلى PSTN. معظم الإساءات الشائعة في هذه الحالة هي أن المستخدم المارق يجري العديد من المكالمات الدولية من خلال SIP أو شنطة H.323 ويدفع مالك CME 1 لدفع رسوم المكالمات الخاصة بالغش - وفي بعض الحالات آلاف الدولارات.



الحل

من أجل تخفيف هذا التهديد، يمكنك إستخدام حلول متعددة. إذا لم يتم إستخدام أي إرسال إشارات VoIP (SIP أو H.323) عبر إرتباط (إرتباطات) WAN في CME 1، فيجب حظر ذلك باستخدام تقنيات جدار الحماية على CME 1 (قوائم الوصول أو قوائم التحكم في الوصول) قدر الإمكان.

1. تأمين واجهة WAN باستخدام جدار حماية Cisco IOS® على CME 1:هذا يعني أن أنت تسمح فقط معروف SIP أو H.323 حركة مرور أن يأتي على ال WAN قارن. تم حظر جميع حركة مرور SIP أو H.323 الأخرى. وهذا يتطلب أيضا أن تعرف عناوين IP التي يستخدمها SIP VoIP SP لإرسال الإشارات على خط اتصال SIP. يفترض هذا الحل أن SP على إستعداد لتوفير جميع عناوين IP أو أسماء DNS التي تستخدمها في شبكتهم. أيضا، في حالة إستخدام أسماء DNS، يتطلب التكوين إمكانية الوصول إلى خادم DNS الذي يمكنه حل هذه الأسماء. أيضا، إذا قام sp بتغيير أي عناوين على نهايتها، فسيلزم تحديث التكوين على CME 1. لاحظ أنه يلزم إضافة هذه البنود بالإضافة إلى أي إدخالات لقوائم التحكم في الوصول (ACL) موجودة بالفعل على واجهة شبكة WAN.نموذج التكوين—CME 1

```
interface serial 0/0
 ip access-group 100 in
!
access-list 100 permit udp host 1.1.1.254 eq 5060 any
is SP SIP proxy access-list 100 permit udp host 1.1.1.254 any eq 5060 1.1.1.254 ---!
access-list 100 permit udp any any range 16384 32767
```

2. تأكد من أن المكالمات التي تأتي على خط اتصال SIP **لا** ترجع تسريحة:وهذا يعني ضمنا أن تكوين CME 1 يسمح فقط ب SIP - SIP مهدئ المكالمات لنطاق رقم PSTN محدد معروف، ويتم حظر جميع المكالمات الأخرى. يجب تكوين أقران طلب داخليين محددين لأرقام PSTN التي تأتي على خط اتصال SIP التي تم تعيينها على الملحقات أو الرد التلقائي أو البريد الصوتي على CME 1. يتم حظر جميع الاستدعاءات الأخرى للأرقام التي ليست جزءا من نطاق رقم PSTN CME 1. لاحظ، أن هذا لا يؤثر على عمليات توجيه المكالمات / النقل إلى البريد الصوتي (Cisco Unity Express) وإعادة توجيه كل الأرقام إلى PSTN من هواتف IP على CME 1، لأن المكالمة الأولية لا تزال موجهة نحو ملحق على CME 1.نموذج التكوين—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. أستخدم قواعد الترجمة لحظر سلاسل طلب محددة:تتضمن معظم حالات الاحتيال بسبب المكالمات الدولية. ونتيجة لذلك، يمكنك إنشاء نظير اتصال داخلي محدد يطابق سلاسل طلب محددة ويحظر المكالمات إليهم. تستخدم معظم أنظمة CME رمز وصول محدد، مثل 9، للطلب ورمز الطلب الدولي في الولايات المتحدة هو 011. لذلك، فإن سلسلة الطلب الأكثر شيوعا التي يتم حظرها في الولايات المتحدة هي 9011 + أي أرقام بعد أن تأتي على خط اتصال SIP.نموذج التكوين—1 CME

```
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
```

أدوات تقييد الميزة

نمط النقل

مجرد

يتم حظر عمليات النقل إلى جميع الأرقام باستثناء تلك الموجودة على هواتف IP المحلية ل SCCP تلقائيا بشكل افتراضي. أثناء التكوين، يمكنك السماح بعمليات النقل إلى أرقام غير محلية. يتم إستخدام الأمر **transfer-style** للسماح بنقل المكالمات الهاتفية من هواتف بروتوكول الإنترنت (IP) من Cisco SCCP إلى هواتف أخرى غير هواتف بروتوكول الإنترنت (IP) من Cisco، مثل مكالمات PSTN الخارجية أو الهواتف على نظام CME آخر. يمكنك إستخدام **نمط النقل** لتحديد الاستدعاءات إلى الملحقات الداخلية فقط أو ربما الحد من الاستدعاءات إلى أرقام PSTN في رمز منطقة معين فقط. توضح هذه الأمثلة كيف يمكن إستخدام الأمر **transfer-pattern** لتحديد المكالمات بأرقام مختلفة.

ملاحظة هذا **تهديد داخلي**.

مثال 1

السماح للمستخدمين بنقل المكالمات إلى كود المنطقة 408 فقط. في هذا المثال، يفترض أن يتم تكوين CME باستخدام نظير طلب لديه نمط وجهة من 9T.

عينة من التكوين

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

تم حظر نمط التحويل

مجرد

في إصدارات Cisco Unified CME 4.0 والإصدارات الأحدث، يمكنك منع الهواتف الفردية من نقل المكالمات إلى أرقام تم تمكينها بشكل عام للنقل. يقوم الأمر **transfer-pattern blocked** بالتجاوز على الأمر **transfer-style** وتعطيل نقل المكالمات إلى أي وجهة يلزم الوصول إليها بواسطة POTS أو VoIP dial-peer. ويتضمن ذلك أرقام PSTN وبوابات الصوت الأخرى و Cisco Unity Express. وهذا يضمن أن الهواتف الفردية لا تتحمل رسوم رسوم المكالمات عند نقل المكالمات خارج نظام CME الموحد من Cisco. يمكن تكوين حظر نقل المكالمات للهواتف الفردية أو تكوينه كجزء من قالب يتم تطبيقه على مجموعة من الهواتف.

ملاحظة هذا **تهديد داخلي**.

مثال 1

في نموذج التكوين هذا، لا يسمح ل ephone 1 باستخدام نمط النقل (المحدد بشكل عام) لنقل المكالمات، بينما يمكن ل ephone 2 إستخدام نمط النقل المحدد ضمن خدمة الهاتف لنقل المكالمات.

عينة من التكوين

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

الحد الأقصى لطول التحويل

مجرد

يحدد الأمر **transfer max-length** الحد الأقصى لعدد الأرقام التي يمكن للمستخدم طلبها عند نقل مكالمة. يتجاوز **الحد الأقصى للطول** لنمط النقل الأمر **transfer-style** ويفرض الحد الأقصى للأرقام المسموح بها لوجهة النقل. تحدد الوسيطة عدد الأرقام المسموح بها في رقم يتم تحويل الاستدعاء إليه. النطاق: من 3 إلى 16. الافتراضي: 16.

ملاحظة هذا **تهديد داخلي**.

مثال 1

يسمح هذا التكوين فقط للهواتف التي تم تطبيق قالب الهاتف الإلكتروني هذا عليها لنقلها إلى الوجهات التي يصل طولها إلى أربعة أرقام كحد أقصى.

عينة من التكوين

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

الحد الأقصى لطول المكالمة الأمامية

مجرد

لتقييد عدد الأرقام التي يمكن إدخالها باستخدام المفتاح CfwdALL السهل على هاتف IP، أستخدم الأمر **call-forward max-length** في وضع تكوين ePhone-dn أو ephone-dn-template. لإزالة قيد على عدد الأرقام التي يمكن إدخالها، أستخدم الصيغة **no** من هذا الأمر.

ملاحظة هذا **تهديد داخلي**.

مثال 1

في هذا المثال، يسمح لملحق الدليل 101 بإجراء إستدعاء إعادة توجيه إلى أي ملحق يتراوح طوله من واحد إلى أربعة أرقام. أي إستدعاء إلى وجهات أطول من أربع أرقام يفشل.

عينة من التكوين

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

أو

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

لا توجد مكالمة محلية إعادة توجيه

مجرد

عند إستخدام الأمر **no forward local-calls** في وضع تكوين ephone-dn، لا تتم إعادة توجيه المكالمات الداخلية إلى ephone-dn معين **مع عدم** تطبيق **مكالمات محلية** مسبقة إذا كان ephone-dn مشغولا أو لا يستجيب. إذا قام متصل داخلي باتصال EPHONE-dn هذا وكان EPHONE-DN مشغولا، فسيسمع المتصل إشارة مشغولة. إذا قام متصل داخلي باتصال شبكة EPHONE DN هذه ولم ترد عليه، فسيسمع المتصل إشارة إعادة اتصال. لا تتم إعادة توجيه المكالمة الداخلية حتى إذا تم تمكين إعادة توجيه المكالمات ل ephone-dn.

ملاحظة هذا **تهديد داخلي**.

مثال 1

في هذا المثال، يدعو الملحق 2222 الملحق 3675 ويسمع إشارة مشغل أو إعادة اتصال. إذا وصل المتصل الخارجي إلى الملحق 3675 ولم يتم الرد، تتم إعادة توجيه المكالمة إلى الملحق 4000.

عينة من التكوين

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

تعطيل التسجيل التلقائي على نظام CME

مجرد

عند تمكين **هاتف reg-ephone** أسفل الخدمة الهاتفية على نظام SCCP CME، يتم تسجيل هواتف IP الجديدة المتصلة بالنظام تلقائيا وإذا تم تكوين **التعيين التلقائي** لتعيين أرقام الملحقات تلقائيا، يمكن لهاتف IP جديد إجراء المكالمات على الفور.

ملاحظة هذا **تهديد داخلي**.

مثال 1

في هذا التكوين، يتم تكوين نظام CME جديد بحيث يجب عليك إضافة هاتف إلكتروني يدويا لتسجيل الهاتف الإلكتروني إلى نظام CME واستخدامه لإجراء مكالمات IP الهاتفية.

الحل

يمكنك تعطيل **Auto-reg-ephone** أسفل الخدمة الهاتفية بحيث لا يتم تسجيل هواتف IP الجديدة المتصلة بنظام CME تلقائيا إلى نظام CME.

عينة من التكوين

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

مثال 2

إذا كنت تستخدم بروتوكول SCCP CME وتخطط لتسجيل هواتف بروتوكول SIP من Cisco إلى النظام، فيجب عليك تكوين النظام حتى يكون على نقاط نهاية SIP المصادقة باستخدام اسم مستخدم وكلمة مرور. للقيام بذلك، ما عليك سوى تكوين ما يلي:

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

ارجع إلى SIP: إعداد Cisco Unified CME للحصول على دليل تكوين أكثر شمولا ل SIP CME.

أدوات التقييد Cisco Unity Express

Cisco Unity Express الآمن: الوصول AA PSTN

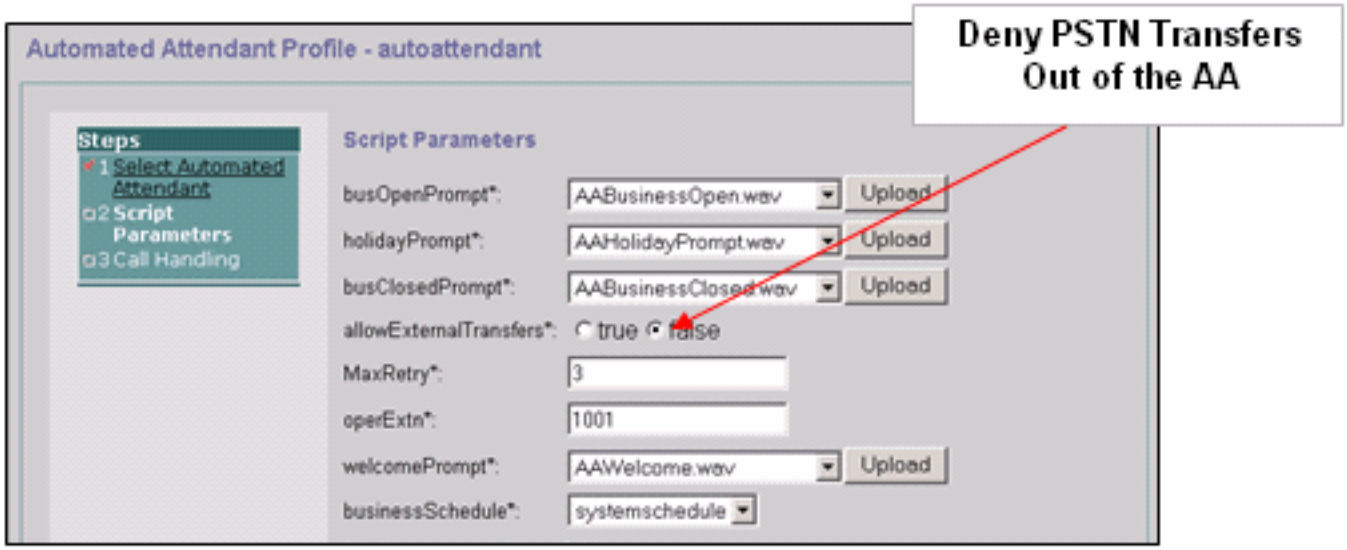
مجرد

عندما يتم تكوين نظامك بحيث يتم إعادة توجيه المكالمات الواردة إلى الرد التلقائي (AA) على Cisco Unity Express، قد يكون من الضروري تعطيل النقل الخارجي إلى PSTN من Cisco Unity Express AA. لا يسمح هذا للمستخدمين الخارجيين بالاتصال الصادر بالأرقام الخارجية بعد الوصول إلى Cisco Unity Express AA.

ملاحظة: هذا **تهديد خارجي**.

ملاحظة: الحل

ملاحظة: قم بتعطيل خيار **السماح بعمليات النقل الخارجية** على واجهة المستخدم الرسومية Cisco Unity Express.



ملاحظة: إذا كان وصول PSTN من المصادقة والتفويض والمحاسبة (AA) مطلوبا، فحدد الأرقام أو نطاق الأرقام التي يعتبرها البرنامج النصي صحيحة.

جداول التقييد Cisco Unity Express

مجرد

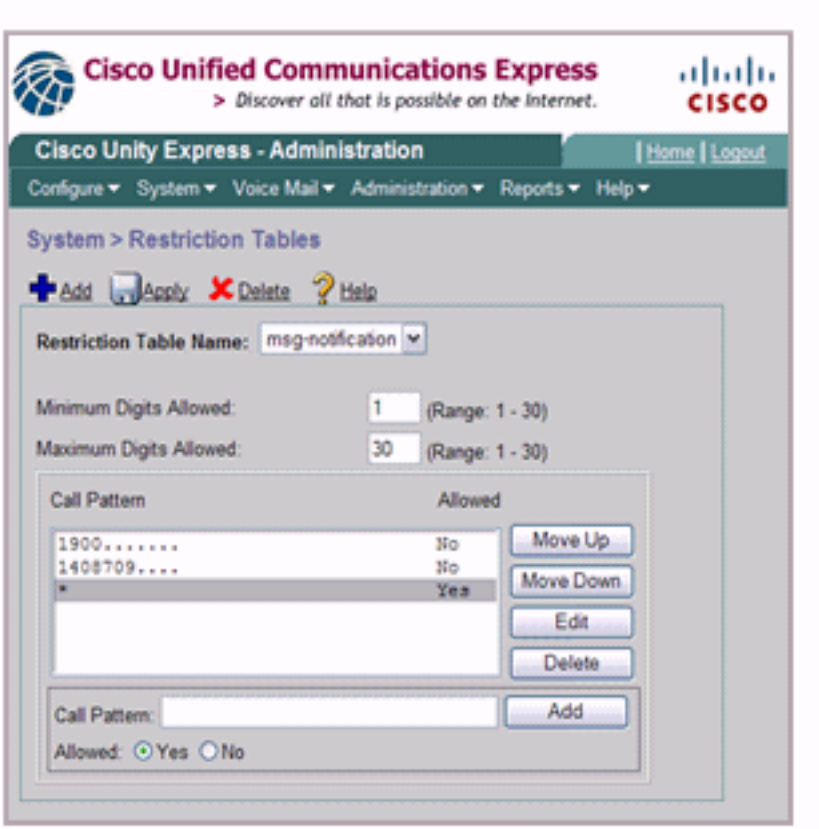
أنت يستطيع استعملت ال cisco Unity Express قيد طاولة in order to قيدت الوجهات أن يستطيع كنت بلغت أثناء إستدعاء من cisco Unity Express. يمكن إستخدام جدول التقييد Cisco Unity Express لمنع الاحتيال في الرسوم الجمركية والاستخدام الضار لنظام Cisco Unity Express لإجراء المكالمات الصادرة. إذا كنت تستخدم جدول التقييد Cisco Unity Express، فيمكنك تحديد أنماط الاستدعاء إلى تطابق البطاقة المفرغة. تتضمن التطبيقات التي تستخدم جدول تقييد Cisco Unity Express:

- فاكس
- Cisco Unity Express Live Replay
- إعلام الرسائل
- تسليم الرسائل لغير المشترك

ملاحظة هذا **تهديد داخلي**.

الحل

لتقييد أنماط الوجهة التي يمكن الوصول إليها بواسطة Cisco Unity Express على مكالمة خارجية صادرة، قم بتكوين **نمط الاستدعاء** في **النظام > جداول القيود** من واجهة المستخدم الرسومية Cisco Unity Express.



تسجيل المكالمات

وحدات ذاكرة CDR محسنة

يمكنك تكوين نظام CME لالتقاط CDR المحسن وتسجيل CDR إلى الذاكرة المؤقتة للموجه أو خادم FTP خارجي. ويمكن بعد ذلك إستخدام هذه السجلات لتعقب المكالمات لمعرفة ما إذا كان قد حدث إساءة إستخدام من قبل أطراف داخلية أو خارجية.

توفر ميزة محاسبة الملفات التي تم تقديمها مع CME 4.3/7.0 في الإصدار XY(15)12.4 من Cisco IOS طريقة لالتقاط سجلات المحاسبة بتنسيق قيمة مفصولة بفاصلة (.csv) وتخزين السجلات إلى ملف في ذاكرة الفلاش الداخلية أو إلى خادم FTP خارجي. وهو يوسع دعم محاسبة العبارة، والذي يتضمن أيضا آليات AAA و syslog لمعلومات محاسبة التسجيل.

تقوم عملية المحاسبة بتجميع بيانات المحاسبة لكل نقطة اتصال يتم إنشاؤها على بوابة الصوت من Cisco. يمكنك إستخدام هذه المعلومات لأنشطة معالجة ما بعد النشر مثل إنشاء سجلات الفوترة ولتحليل الشبكة. تلتقط بوابات الصوت من Cisco بيانات المحاسبة في شكل سجلات تفاصيل المكالمة (CDRs) التي تحتوي على سمات معرفة بواسطة Cisco. يمكن أن ترسل البوابة وحدات CDR إلى خادم RADIUS وخادم syslog، وبطريقة الملف الجديدة، إلى flash أو خادم FTP بتنسيق .csv.

راجع أمثلة CDR للحصول على مزيد من المعلومات حول إمكانيات CDR المحسنة.

معلومات ذات صلة

- مدير الاتصالات الموحدة الفائق من Cisco
- دليل مسئولي Cisco Communications Manager Express
- دليل مسؤولي Cisco Communications Manager Express - حظر المكالمات
- فهم تطابق نظير الطلب على الأنظمة الأساسية IOS

- ترجمة الرقم باستخدام ملفات تعريف الترجمة الصوتية
- دليل تصميم الشبكة المرجعية لحل CME
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).