Prevención de Fraude de Llamadas de Larga Distancia de Unified Communications Manager Express

Contenido

Introducción

Este documento proporciona una guía de configuración que se pueda utilizar para ayudar a asegurar un sistema CME (Cisco Communications Manager Express) y atenuar la amenaza del fraude de cargos de llamada. CME es la solución de control de llamadas basada en router de Cisco que proporciona una solución inteligente, sencilla y segura para las organizaciones que desean implementar Unified Communications. Se recomienda encarecidamente implementar las medidas de seguridad descritas en este documento para proporcionar niveles adicionales de control de seguridad y reducir la posibilidad de fraude de peaje.

El objetivo de este documento es informarle sobre las diversas herramientas de seguridad disponibles en Cisco Voice Gateways y CME. Estas herramientas se pueden implementar en un sistema CME para ayudar a mitigar la amenaza de fraude de peaje tanto por parte de las partes internas como externas.

Este documento proporciona instrucciones sobre cómo configurar un sistema CME con varias herramientas de seguridad de llamadas y de restricción de funciones. El documento también describe por qué ciertas herramientas de seguridad se utilizan en ciertas implementaciones.

La flexibilidad inherente general de las plataformas ISR de Cisco le permite implementar CME en muchos tipos diferentes de implementaciones. Por lo tanto, puede ser necesario utilizar una combinación de las funciones descritas en este documento para ayudar a bloquear el CME. Este documento sirve como guía para aplicar las herramientas de seguridad en CME y no garantiza de ninguna manera que no se produzcan fraudes o abusos por parte de partes internas y externas.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Communications Manager Express

Componentes Utilizados

La información de este documento se basa en Cisco Unified Communications Manager Express 4.3 y CME 7.0.

Nota: Cisco Unified CME 7.0 incluye las mismas funciones que Cisco Unified CME 4.3, que se renumera como 7.0 para ajustarse a las versiones 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.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Overview

Este documento cubre las herramientas de seguridad más comunes que se pueden utilizar en un sistema CME para ayudar a mitigar la amenaza de fraude de llamadas. Las herramientas de seguridad CME a las que se hace referencia en este documento incluyen herramientas de restricción de tarifas y herramientas de restricción de funciones.

Herramientas de restricción de llamadas

- Direct-inward-dial
- Restricción de llamadas fuera de horario
- Clase de restricción
- Lista de acceso para restringir el acceso troncal H323/SIP

Herramientas de restricción de funciones

- Patrón de transferencia
- Patrón de transferencia bloqueado
- Transfer max-length
- Call-Forward max-length
- No reenviar llamadas locales
- No auto-reg-ephone

Herramientas de restricción de Cisco Unity Express

- Acceso PSTN Cisco Unity Express seguro
- Restricción de notificación de mensajes

Registro de llamadas

- Registro de llamadas para capturar registros de detalles de llamadas (CDR)

Amenazas internas frente a externas

Este documento trata las amenazas tanto de partes internas como externas. Entre los usuarios internos se incluyen los usuarios de teléfonos IP que residen en un sistema CME. Los usuarios externos incluyen usuarios de sistemas extranjeros que pueden intentar utilizar el CME host para realizar llamadas fraudulentas y hacer que las llamadas se vuelvan a cargar en el sistema CME.

Herramientas de restricción de llamadas

Direct-inward-dial

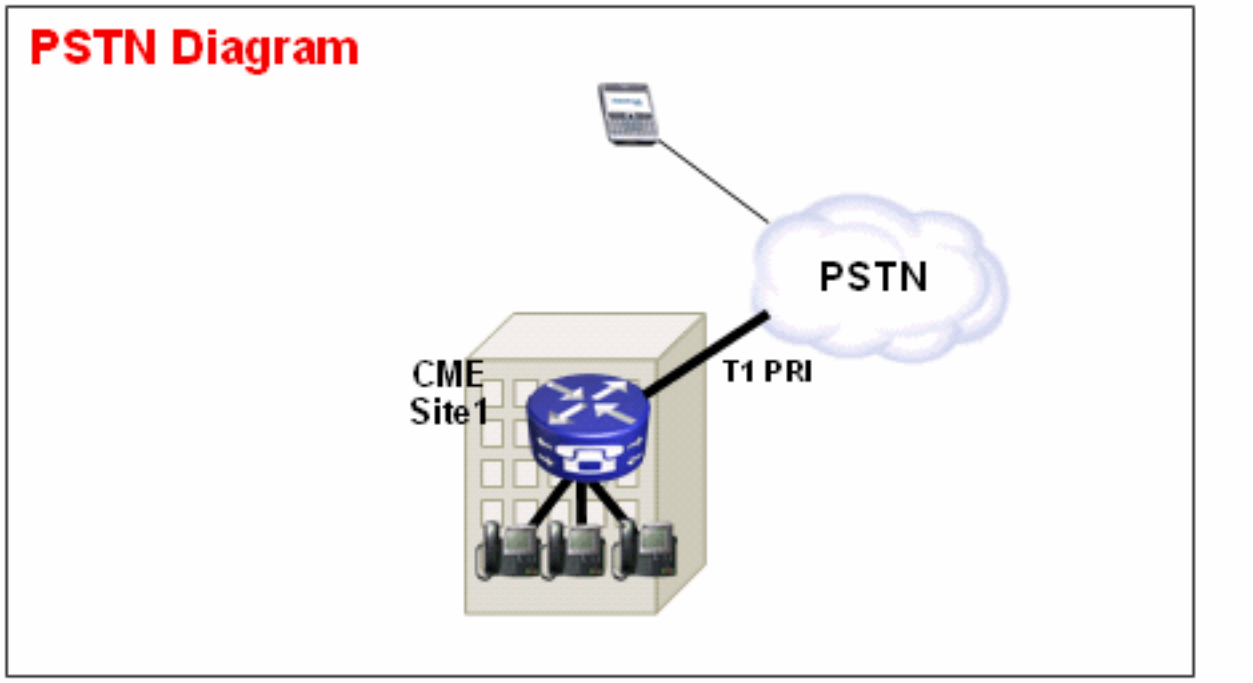
Abstracto

La marcación directa entrante (DID) se utiliza en los gateways de voz de Cisco para permitir que el gateway procese una llamada entrante después de recibir dígitos del switch PBX o CO. Cuando se habilita DID, la gateway de Cisco no presenta un tono de marcado secundario para la persona que llama y no espera a recopilar dígitos adicionales de la persona que llama. Reenvía la llamada directamente al destino que coincida con el servicio de identificación de número marcado (DNIS) entrante. Esto se denomina marcado en una etapa.

Nota: Esta es una **amenaza externa**.

Declaración de problema

Si la marcación entrante directa NO está configurada en un gateway de Cisco o CME, siempre que una llamada entre el CO o el PBX en el gateway de Cisco, la persona que llama oye un tono de marcado secundario. Esto se denomina marcación en dos etapas. Una vez que las personas que llaman PSTN escuchan el tono de marcado secundario, pueden introducir dígitos para alcanzar cualquier extensión interna o si conocen el código de acceso PSTN, pueden marcar números de larga distancia o internacionales. Esto presenta un problema porque la persona que llama a PSTN puede utilizar el sistema CME para realizar llamadas salientes de larga distancia o internacionales y la empresa recibe cargos por las llamadas.



Ejemplo 1

En el Sitio 1, el CME se conecta al PSTN a través de un tronco T1 PRI. El proveedor de PSTN proporciona el **4085512.** Intervalo DID para el sitio CME 1. Por lo tanto, todas las llamadas PSTN destinadas al 4085551200 - 4085551299 se enrutan de forma entrante al CME. Si no configura **direct-inward-dial** en el sistema, un llamante PSTN entrante escucha un tono de marcado secundario y debe marcar manualmente la extensión interna. El problema más grande es que si la persona que llama es un agresor y conoce el código de acceso PSTN en el sistema, normalmente **9**, pueden marcar **9** y luego cualquier número de destino al que deseen llegar.

Solución 1

Para mitigar esta amenaza, debe configurar **direct-inward-dial**. Esto hace que el gateway de Cisco reenvíe la llamada entrante directamente al destino que coincida con el DNIS entrante.

Configuración de muestra:

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

Para que DID funcione correctamente, asegúrese de que la llamada entrante coincida con el dial-peer POTS correcto en el que está configurado el comando **direct-inward-dial**. En este ejemplo, el T1 PRI está conectado al puerto 1/0:23. Para hacer coincidir el dial peer entrante correcto, ejecute

el comando dial peer **incoming called-number** bajo el dial peer DID POTS.

Ejemplo 2

En el Sitio 1, el CME se conecta al PSTN a través de un tronco T1 PRI. El proveedor de PSTN proporciona el **4085512.** y **40855513.** Rangos DID para el sitio CME 1. Por lo tanto, todas las llamadas PSTN destinadas a 4085551200 - 408551299 y 4085551300 - 4085551399 se enrutan hacia el CME.

Configuración incorrecta:

Si configura un dial-peer entrante, como en la configuración de ejemplo de esta sección, la posibilidad de fraude de llamadas todavía ocurre. El problema con este par de marcado entrante es que sólo coincide con las llamadas entrantes a **40852512.** y luego aplica el servicio DID. Si una llamada PSTN entra en **40852513.**., el dial-peer pots entrante no coincide y por lo tanto el servicio DID no se aplica. Si un dial-peer entrante con DID no coincide, se utiliza el dial-peer predeterminado 0. DID se encuentra inhabilitado en forma predeterminada en el par de marcado 0.

Configuración de muestra:

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

Configuración correcta

En este ejemplo se muestra la forma correcta de configurar el servicio DID en un dial-peer entrante:

Configuración de muestra:

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

Consulte Configuración de DID para Peers de Marcación POTS para obtener más información sobre DID para puertos de voz T1/E1 digitales.

Nota: El uso de DID **no** es necesario cuando se utiliza el timbre automático de línea privada (PLAR) en un puerto de voz o una secuencia de comandos de servicio como Auto-Attendant (AA) en el dial-peer entrante.

Ejemplo de configuración: PLAR

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

Ejemplo de configuración: secuencia de comandos de servicio

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

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

Restricciones de llamadas fuera de horario

Abstracto

La restricción de llamadas fuera de horario es una nueva herramienta de seguridad disponible en CME 4.3/7.0 que le permite configurar políticas de restricción de llamadas en función de la hora y la fecha. Puede configurar políticas para que los usuarios no puedan realizar llamadas a números predefinidos durante determinadas horas del día o en todo momento. Si se configura la política de bloqueo de llamadas 7 horas después de las 24 horas, también restringe el conjunto de números que puede ingresar un usuario interno para establecer **el reenvío de todas las llamadas**.

Nota: Esta es una **amenaza interna**.

Ejemplo 1

Este ejemplo define varios patrones de dígitos para los que se bloquean las llamadas salientes. Los patrones 1 y 2, que bloquean las llamadas a números externos que comienzan por "1" y "011", se bloquean de lunes a viernes antes de las 7 de la mañana y después de las 7 de la tarde, el sábado antes de las 7 de la mañana y después de las 1 de la tarde y todo el domingo. El patrón 3 bloquea las llamadas a 900 números 7 días a la semana, 24 horas al día.

Configuración de muestra:

```
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
```

Consulte Configuración del Bloqueo de Llamadas para obtener más información sobre la restricción de tarifas.

Clase de restricción

Abstracto

Si desea un control granular al configurar la restricción de tarifas, debe utilizar la clase de restricción (COR). Consulte Clase de Restricción: Ejemplo para obtener más información.

Restricciones de fraude de llamadas H.323/SIP Trunks

Abstracto

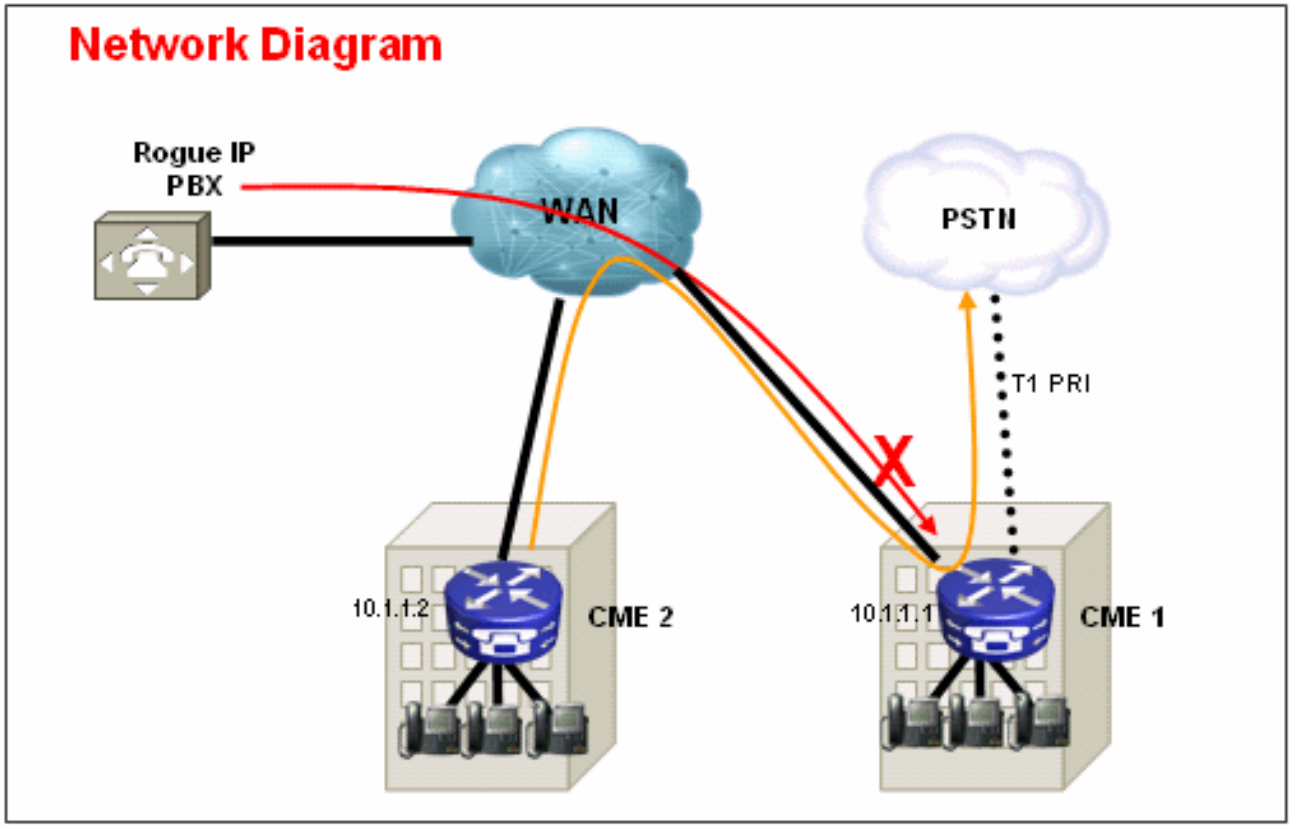
En los casos en los que un sistema CME se conecta a través de una WAN a otros dispositivos

CME a través de un troncal SIP o H.323, puede restringir el acceso troncal SIP/H.323 al CME para evitar que los abusadores utilicen su sistema para retransmitir llamadas ilegalmente a la PSTN.

Nota: Esta es una **amenaza externa**.

Ejemplo 1

En este ejemplo, el CME 1 tiene conectividad PSTN. El CME 2 se conecta a través de la WAN al CME 1 a través de un tronco H.323. Para asegurar el CME 1, puede configurar una lista de acceso y aplicarla de entrada en la interfaz WAN y, por lo tanto, permitir solamente el tráfico IP de CME 2. Esto evita que la PBX IP no autorizada envíe llamadas VOIP a través de CME 1 a la PSTN.



Solución

No permita que la interfaz WAN en CME 1 acepte el tráfico de dispositivos no autorizados que no reconoce. Observe que hay una DENY all implícita al final de una lista de acceso. Si hay más dispositivos desde los que desea permitir el tráfico IP entrante, asegúrese de agregar la dirección IP del dispositivo a la lista de acceso.

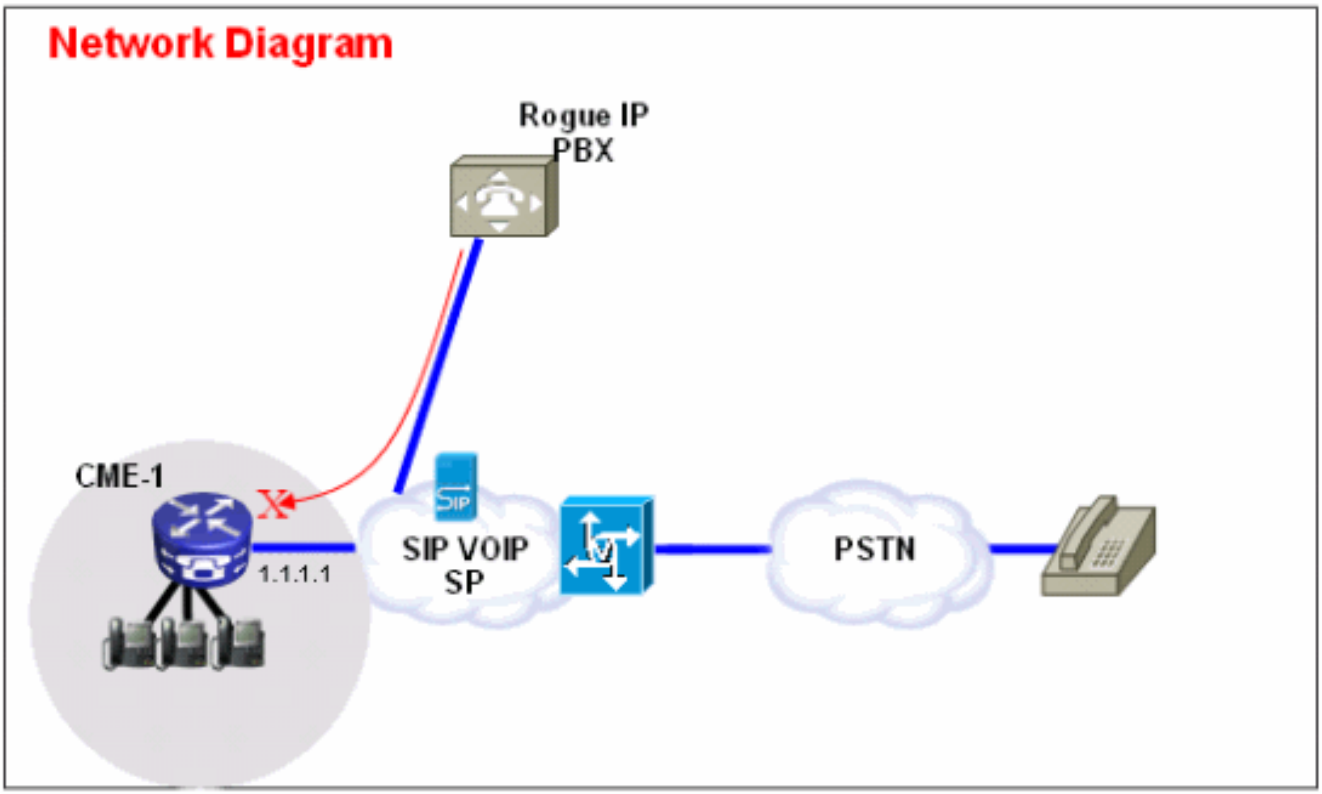
Ejemplo de configuración: CME 1

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

Ejemplo 2

En este ejemplo, el CME 1 se conecta al proveedor SIP para la conectividad PSTN con la configuración de ejemplo proporcionada en el ejemplo de configuración de enlace troncal SIP de Cisco CallManager Express (CME).

Dado que CME 1 se encuentra en la Internet pública, es posible que se produzca un *fraude de llamadas* si un usuario no autorizado explora las direcciones IP públicas en busca de puertos conocidos para la señalización H.323 (TCP 1720) o SIP (UDP o TCP 5060) y envía mensajes SIP o H.323 que enrutan las llamadas de retorno desde el troncal SIP al PSTN. La mayoría de los abusos comunes en este caso son los usuarios desconocidos que realizan múltiples llamadas internacionales a través del tronco SIP o H.323 y hacen que el propietario del CME 1 pague por estas llamadas de fraude de peaje - en algunos casos miles de dólares.



Solución

Para mitigar esta amenaza, puede utilizar varias soluciones. Si no se utiliza ninguna señalización VoIP (SIP o H.323) a través de los enlaces WAN en CME 1, ésta debe bloquearse con las técnicas de firewall de CME 1 (listas de acceso o ACL) tanto como sea posible.

1. Proteja la interfaz WAN con el firewall Cisco IOS® en CME 1:Esto implica que sólo se permite el ingreso de tráfico SIP o H.323 conocido en la interfaz WAN. El resto del tráfico SIP o H.323 está bloqueado. Esto también requiere que conozca las direcciones IP que el SIP VOIP SP utiliza para la señalización en el troncal SIP. Esta solución asume que el SP está dispuesto a proporcionar todas las direcciones IP o los nombres DNS que utilizan en su red. Además, si se utilizan nombres DNS, la configuración requiere que se pueda acceder a un servidor DNS que pueda resolver estos nombres. Además, si el SP cambia alguna dirección en su extremo, la configuración debe actualizarse en CME 1. Tenga en cuenta que estas líneas deben agregarse además de cualquier entrada ACL ya presente en la interfaz WAN.Ejemplo de configuración: 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. Asegúrese de que las llamadas que entran en el troncal SIP **NO** se desvían:Esto implica que la configuración de CME 1 sólo permite que SIP - SIP de las llamadas a un rango de números PSTN conocido específico, todas las demás llamadas se bloquean. Debe configurar pares de marcado entrantes específicos para los números PSTN que entran en el troncal SIP y que están asignados a extensiones o contestadores automáticos o correo de voz en CME 1. El resto de llamadas a números que no forman parte del intervalo de números PSTN CME 1 se bloquean. Tenga en cuenta que esto no afecta a los reenvíos o transferencias de llamadas al correo de voz (Cisco Unity Express) y a los números PSTN de los teléfonos IP en CME 1, ya que la llamada inicial todavía está dirigida a una extensión en CME 1.Ejemplo de configuración: 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. Utilice reglas de traducción para bloquear cadenas de marcado específicas:La mayoría de los fraudes de llamadas implican marcación internacional. Como resultado, puede crear un par de marcado entrante específico que coincida con cadenas marcadas específicas y bloquee llamadas a ellas. La mayoría de los CME utilizan un código de acceso específico, como 9, para marcar y el código de marcación internacional en EE. UU. es 011. Por lo tanto, la cadena de marcado más común para bloquear en EE. UU. es 9011 + cualquier dígito después de que se introduzca en el troncal SIP.Ejemplo de configuración: 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
```

Herramientas de restricción de funciones

Patrón de transferencia

Abstracto

Las transferencias a todos los números excepto a los de los teléfonos IP SCCP locales se bloquean automáticamente de forma predeterminada. Durante la configuración, puede permitir transferencias a números no locales. El comando **transfer-pattern** se utiliza para permitir la transferencia de llamadas telefónicas desde teléfonos IP Cisco SCCP a teléfonos que no sean Cisco IP Phones, como llamadas PSTN externas o teléfonos en otro sistema CME. Puede utilizar el **patrón de transferencia** para limitar las llamadas sólo a extensiones internas o tal vez limitar las llamadas a números PSTN sólo en un código de área determinado. Estos ejemplos muestran cómo el comando **transfer-pattern** se puede utilizar para limitar las llamadas a números diferentes.

Nota: Esta es una **amenaza interna**.

Ejemplo 1

Permitir a los usuarios transferir llamadas sólo al código de área 408. En este ejemplo, la suposición es que el CME se configura con un par de marcado que tiene un patrón de destino de 9T.

Configuración de muestra:

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

Trama de transferencia bloqueada

Abstracto

En las versiones 4.0 y posteriores de Cisco Unified CME, puede evitar que los teléfonos individuales transfieran llamadas a números que están globalmente habilitados para la transferencia. El comando **transfer-pattern locked** reemplaza el comando **transfer-pattern** e inhabilita la transferencia de llamadas a cualquier destino al que deba alcanzar un dial-peer POTS o VoIP. Esto incluye números PSTN, otros gateways de voz y Cisco Unity Express. Esto garantiza que los teléfonos individuales no incurren en cargos por llamadas cuando se transfieren fuera del sistema Cisco Unified CME. El bloqueo de transferencia de llamadas se puede configurar para teléfonos individuales o como parte de una plantilla que se aplica a un conjunto de teléfonos.

Nota: Esta es una **amenaza interna**.

Ejemplo 1

En esta configuración de ejemplo, el ephone 1 no puede utilizar el patrón de transferencia (definido globalmente) para transferir llamadas, mientras que el ephone 2 puede utilizar el patrón de transferencia definido en telephony-service para transferir llamadas.

Configuración de muestra:

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

```
ephone 2
!
```

Transfer max-length

Abstracto

El comando **transfer max-length** especifica el número máximo de dígitos que el usuario puede marcar cuando se transfiere una llamada. El **patrón de transferencia max-length** reemplaza el comando **transfer-pattern** y aplica los dígitos máximos permitidos para el destino de la transferencia. El argumento especifica el número de dígitos permitidos en un número al que se transfiere una llamada. Rango: 3 a 16. Predeterminado: 16.

Nota: Esta es una **amenaza interna**.

Ejemplo 1

Esta configuración sólo permite a los teléfonos que tienen esta plantilla de teléfono aplicada para transferir a destinos con un máximo de cuatro dígitos.

Configuración de muestra:

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

Call Forward max-length

Abstracto

Para restringir el número de dígitos que se pueden ingresar con la tecla programable CfwdALL en un teléfono IP, utilice el comando **call-forward max-length** en el modo de configuración ephone-dn o ephone-dn-template. Para eliminar una restricción en el número de dígitos que se pueden ingresar, utilice la forma **no** de este comando.

Nota: Esta es una **amenaza interna**.

Ejemplo 1

En este ejemplo, se permite a la extensión de directorio 101 realizar un reenvío de llamada a cualquier extensión con una longitud de uno a cuatro dígitos. Cualquier desvío de llamadas a destinos con más de cuatro dígitos fallará.

Configuración de muestra:

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

or

```
ephone-dn-template  1
```

```
call-forward max-length 4
```

No reenviar llamada local

Abstracto

Cuando el comando **no forward local-calls** se utiliza en el modo de configuración ephone-dn, las llamadas internas a un ephone-dn particular sin **reenviar llamadas locales** aplicadas no se reenvían si el ephone-dn está ocupado o no responde. Si una persona que llama interna llama a este ephone-dn y el ephone-dn está ocupado, la persona que llama oye una señal de ocupado. Si una persona que llama interna llama a este ephone-dn y no responde, la persona que llama oye una señal de recepción de llamada. La llamada interna no se reenvía aunque el desvío de llamadas esté habilitado para el ephone-dn.

Nota: Esta es una **amenaza interna**.

Ejemplo 1

En este ejemplo, la extensión 2222 llama a la extensión 3675 y oye una señal de recepción de llamada o una señal de ocupado. Si una persona que llama externa alcanza la extensión 3675 y no hay respuesta, la llamada se reenvía a la extensión 4000.

Configuración de muestra:

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

Desactivar registro automático en el sistema CME

Abstracto

Cuando se habilita **auto-reg-ephone** bajo el servicio de telefonía en un sistema CME SCCP, los nuevos teléfonos IP que se conectan al sistema se registran automáticamente y si la **asignación automática** se configura para asignar automáticamente números de extensión, entonces un nuevo teléfono IP puede realizar llamadas inmediatamente.

Nota: Esta es una **amenaza interna**.

Ejemplo 1

En esta configuración, se configura un nuevo sistema CME de modo que debe agregar manualmente un ephone para que el ephone se registre en el sistema CME y utilizarlo para realizar llamadas de telefonía IP.

Solución

Puede inhabilitar **auto-reg-ephone** debajo del servicio de telefonía para que los nuevos teléfonos IP conectados a un sistema CME no se registren automáticamente en el sistema CME.

Configuración de muestra:

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

Ejemplo 2

Si utiliza SCCP CME y planea registrar los teléfonos SIP de Cisco en el sistema, debe configurar el sistema para que los terminales SIP tengan que autenticarse con un nombre de usuario y una contraseña. Para hacerlo, simplemente configure esto:

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

Consulte SIP: Configuración de Cisco Unified CME para obtener una guía de configuración más completa para SIP CME.

Herramientas de restricción de Cisco Unity Express

Cisco Unity Express seguro: Acceso PSTN AA

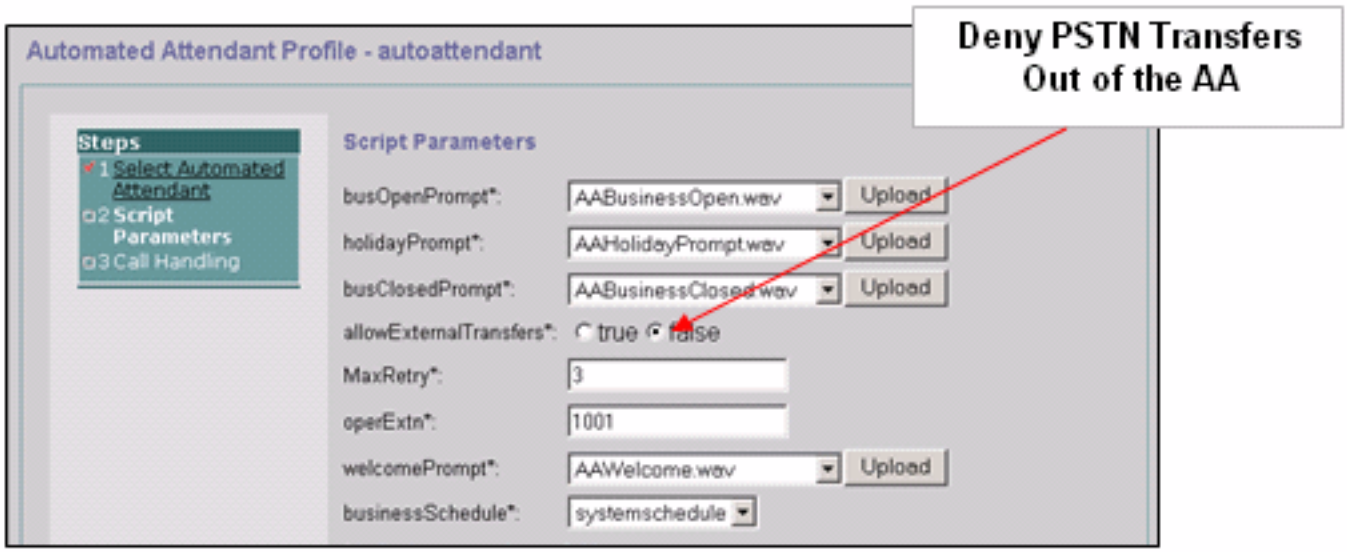
Abstracto

Cuando su sistema se configura de modo que las llamadas entrantes se reenvíen al contestador automático (AA) en Cisco Unity Express, es posible que sea necesario desactivar la transferencia externa a PSTN desde Cisco Unity Express AA. Esto no permite a los usuarios externos marcar de salida a números externos después de que alcancen Cisco Unity Express AA.

Nota: Esta es una **amenaza externa**.

Nota: **Solución**

Nota: Inhabilite la opción **allowExternalTransfers** en la GUI de Cisco Unity Express.



Nota: Si se requiere acceso PSTN desde el AA, limite los números o el rango de números que el script considera válidos.

Tablas de Restricción de Cisco Unity Express

Abstracto

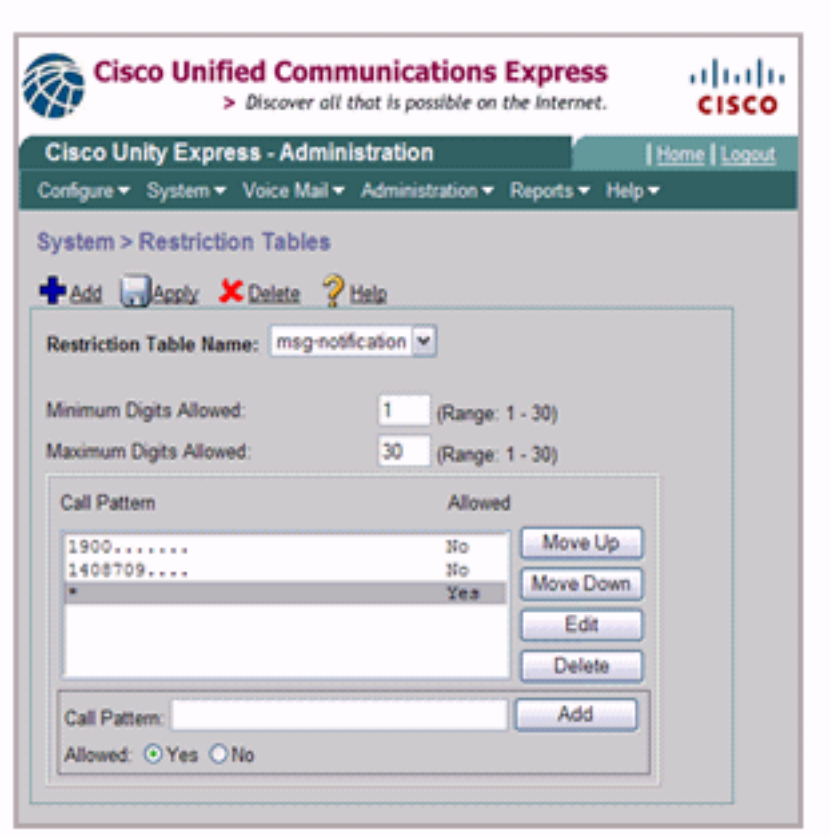
Puede utilizar las tablas de restricción de Cisco Unity Express para restringir los destinos a los que se puede llegar durante una llamada saliente de Cisco Unity Express. La tabla de restricción de Cisco Unity Express se puede utilizar para evitar el fraude de cargos y el uso malintencionado del sistema Cisco Unity Express para realizar llamadas salientes. Si utiliza la tabla de restricción de Cisco Unity Express, puede especificar patrones de llamada para la coincidencia con comodín. Las aplicaciones que utilizan la tabla de restricción de Cisco Unity Express incluyen:

- Fax
- Reproducción en directo de Cisco Unity Express
- Notificación de mensaje
- Entrega de mensajes no suscriptores

Nota: Esta es una **amenaza interna**.

Solución

Para restringir los patrones de destino a los que puede llegar Cisco Unity Express en una llamada externa saliente, configure el **patrón de llamada** en el **sistema > tablas de restricciones** desde la GUI de Cisco Unity Express.



Registro de llamadas

CDR mejorado

Puede configurar el sistema CME para capturar CDR mejorado y registrar el CDR en la memoria flash del router o en un servidor FTP externo. Estos registros se pueden utilizar entonces para volver a rastrear las llamadas para ver si se ha producido un abuso por parte de partes internas o externas.

La función de contabilidad de archivos introducida con CME 4.3/7.0 en Cisco IOS Release 12.4(15)XY proporciona un método para capturar registros contables en formato de valor separado por comas (.csv) y almacenar los registros en un archivo en la memoria flash interna o en un servidor FTP externo. Amplía el soporte de contabilidad de gateway, que también incluye los mecanismos AAA y syslog de registro de información de contabilidad.

El proceso de contabilidad recopila los datos de contabilidad para cada tramo de llamada creado en un gateway de voz de Cisco. Puede utilizar esta información para actividades de procesamiento de publicaciones, como generar registros de facturación y para el análisis de red. Los gateways de voz de Cisco capturan los datos de contabilidad en forma de registros de detalles de llamadas (CDR) que contienen atributos definidos por Cisco. El gateway puede enviar CDR a un servidor RADIUS, servidor syslog y con el nuevo método de archivo, a flash o a un servidor FTP en formato .csv.

Consulte Ejemplos de CDR para obtener más información sobre las capacidades de CDR mejoradas.

Información Relacionada

- Prácticas recomendadas de seguridad de Cisco Unified Communications Manager Express
- Guía del administrador de Cisco Communications Manager Express
- Guía del administrador de Cisco Communications Manager Express - Bloqueo de llamadas
- Introducción a la coincidencia de pares de marcado en las plataformas IOS
- Traducción de número mediante perfiles de traducción de voz
- Guía de diseño de red de referencia de solución CME
- Soporte Técnico y Documentación - Cisco Systems