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. El CME es la solución del Control de llamadas basada en el router de Cisco que proporciona una solución elegante, simple y segura para las organizaciones que quieren implementar las Comunicaciones unificadas. Es recomienda altamente que usted implementa las medidas de seguridad descritas en este documento para proporcionar el control de niveles de seguridad adicional y reducir la posibilidad del fraude de cargos de llamada.

El objetivo de este documento es educarle en las diversas herramientas de seguridad disponibles en los gateways de voz de Cisco y el CME. Estas herramientas se pueden implementar en un sistema CME para ayudar a atenuar la amenaza del fraude de cargos de llamada por los partidos internos y externos.

Este documento proporciona las instrucciones en cómo configurar un sistema CME con las diversas herramientas de la Seguridad del peaje y de la restricción de la característica. El documento también delinea porqué ciertas herramientas de seguridad se utilizan en ciertas implementaciones.

La flexibilidad inherente total de las Plataformas ISR de Cisco permite que usted despliegue el CME en muchos diversos tipos de implementaciones. Así puede ser requerido para utilizar una combinación de las características descritas en este documento para ayudar a bloquear abajo del CME. Este documento sirve como guía de consulta para que cómo aplique las herramientas de seguridad en el CME y de ninguna manera las garantías que no ocurrirá el fraude de cargos de llamada o el abuso por los partidos internos y externos.

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Communications Manager Express

Componentes Utilizados

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

Nota: Cisco unificó CME 7.0 incluye las mismas características que el CME unificado Cisco 4.3, que se renumera a 7.0 para alinear con las versiones de las Comunicaciones unificadas de Cisco.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

Información general

Este documentos abarca la mayoría de las herramientas de la seguridad común que se pueden utilizar en un sistema CME para ayudar a atenuar la amenaza del fraude de cargos de llamada. Las herramientas de seguridad CME referidas a este documento incluyen las herramientas de la restricción del peaje y las herramientas de la restricción de la característica.

Herramientas de la restricción del peaje

- Direct-inward-dial
- Después de la restricción del peaje de las horas
- Clase de restricción
- Lista de acceso para restringir el acceso del trunk H323/SIP

Herramientas de la restricción de la característica

- Transferencia-modelo
- Transferencia-modelo bloqueado
- MAX-longitud de la transferencia
- MAX-longitud Llamada-delantera
- Ningunas Llamadas locales delanteras
- Ningún auto-REG-ephone

Herramientas de la restricción del Cisco Unity Express

- Acceso seguro del Cisco Unity Express PSTN
- Restricción de la notificación del mensaje

Registro de la llamada

- Registro de la llamada para capturar los registros de detalles de la llamada (CDR)

Interno contra las amenazas exteriores

Este documento discute las amenazas de los partidos internos y del externo. Los partidos internos incluyen a los usuarios del teléfono del IP que residen en un sistema CME. Los partidos externos incluyen a los usuarios en los sistemas no nativos que pueden intentar utilizar el host CME para hacer las llamadas fraudulentas y para tener las llamadas cargadas de nuevo a su sistema CME.

Herramientas de la restricción del peaje

Direct-inward-dial

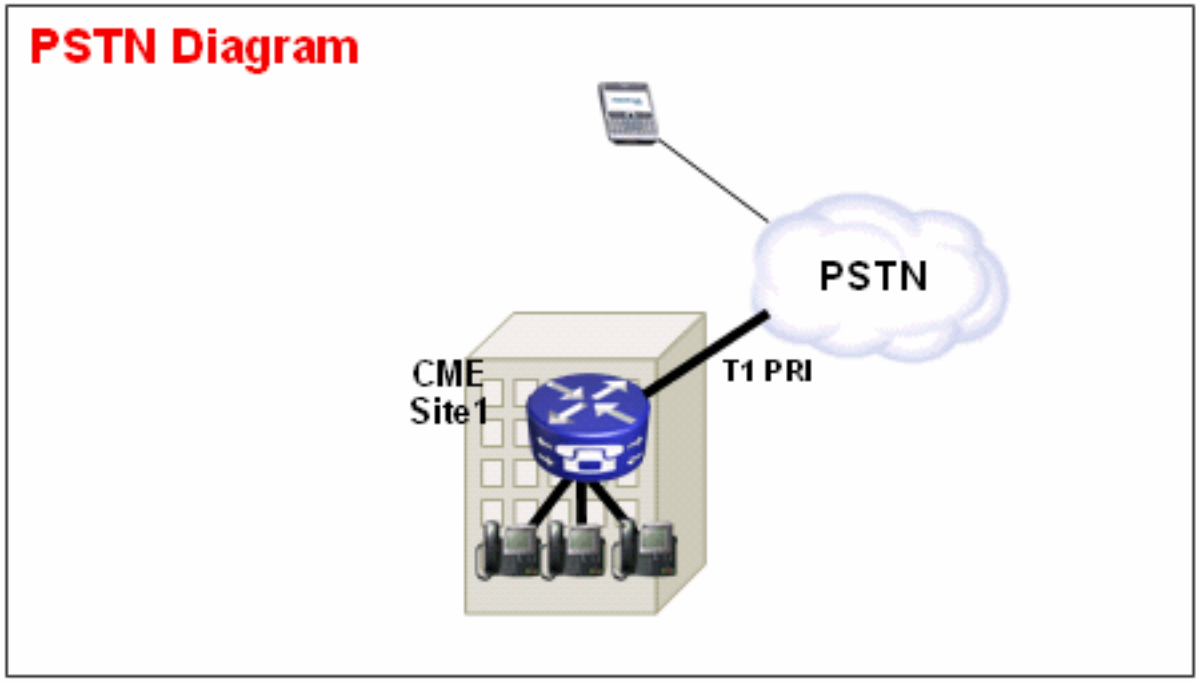
Abstracto

el Directo-hacia adentro-dial (HIZO) se utiliza en los gatewayes de voz de Cisco para permitir que el gateway procese una llamada entrante después de que reciba los dígitos del switch PBX o CO. Cuando LO HIZO se habilita, el gateway de Cisco no presenta un tono de marcación secundario al llamador y no espera para recoger los dígitos adicionales del llamador. Él adelante la llamada directamente al destino que hace juego el Dialed Number Identification Service (DNIS). entrante Esto se denomina marcado en una etapa.

Nota: Esto es una **amenaza exterior**.

Declaración de problema

Si el directo-hacia adentro-dial no se configura en un gateway de Cisco o un CME, siempre que una llamada venga adentro del CO o del PBX al gateway de Cisco, el llamador oye un tono de marcado secundario. Esto se llama discado en dos etapas. Una vez que los llamadores PSTN oyen el tono de marcado secundario, pueden ingresar los dígitos para alcanzar cualquier extensión interna o si conocen el código de acceso PSTN, pueden marcar la distancia o los números internacionales. Esto presenta un problema porque el llamador PSTN puede utilizar el sistema CME para poner la distancia saliente o las llamadas internacionales y la compañía consigue cargadas para las llamadas.



Ejemplo 1

En el sitio 1, el CME está conectado con el PSTN a través de un trunk del T1 PRI. El proveedor PSTN proporciona los **40855512.** Extiéndase para el sitio 1. CME. Así todas las llamadas PSTN destinadas para 4085551200 – 4085551299 son entrantes ruteado al CME. Si usted no configura el directo-hacia adentro-**dial** en el sistema, un llamador PSTN entrante oye un secundario una señal y debe marcar manualmente la extensión interna. El problema más grande es que si el llamador es un adicto y conoce el código de acceso PSTN en el sistema, pueden comúnmente **9**, ellos marcan **9** entonces cualesquiera números de destino que quieran alcanzar.

Solución 1

Para atenuar esta amenaza, usted debe configurar el directo-hacia adentro-**dial**. Esto hace el gateway de Cisco remitir la llamada entrante directamente al destino que hace juego el DNIS entrante.

Configuración de muestra:

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

Para trabaje correctamente, se aseeguran la llamada entrante hace juego al POTS dial peer

correcto donde configuran al **comando direct-inward-dial**. En este ejemplo, el T1 PRI está conectado con el puerto 1/0:23. Para hacer juego al dial peer de entrada correcto, publique el comando dial peer **entrante del llamar-número** bajo HIZO al POTS dial peer.

'Ejemplo 2'

En el sitio 1, el CME está conectado con el PSTN a través de un trunk del T1 PRI. El proveedor PSTN da los **40855512.** y **40855513.** HIZO los rangos para el sitio 1. CME. Así todas las llamadas PSTN destinadas para 4085551200 – 4085551299 y 4085551300 - 4085551399 son entrantes ruteado al CME.

Configuración incorrecta:

Si usted configura a un dial peer de entrada, como en la configuración de muestra en esta sección, la posibilidad del fraude de cargos de llamada todavía ocurre. El problema con este dial peer de entrada es que hace juego solamente las llamadas entrantes a **40852512.** y entonces aplica mantuvo. Si una llamada PSTN entra en **40852513.** , el dial-peer de los POT entrantes no hace juego y mantenga así no es aplicado. Si LO HIZO un dial peer de entrada con no se corresponde con, después utilizan al dial-peer por default 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

La manera correcta de configurar mantuvo en un dial peer de entrada se muestra en este ejemplo:

Configuración de muestra:

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

Refiera a la Configuración DID para los POTS dial peer para más información encendido HIZO para los puertos de voz digitales T1/E1.

Nota: El uso de HIZO no es necesario cuando la generación de llamada automática de la Línea privada (PLAR) se utiliza en un puerto de voz o un script del servicio tal como Auto Attendant (AA) se utiliza en el dial peer de entrada.

Configuración de muestra — PLAR

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

Configuración de muestra — Mantenga el script

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

Después de las horas toque las restricciones

Abstracto

Después de las horas la restricción del peaje es una nueva herramienta de seguridad disponible en el CME 4.3/7.0 que permite que usted configure las directivas de la restricción del peaje basadas el la Fecha y hora. Usted puede configurar las directivas para no permitir los usuarios que hagan las llamadas a los números predefinidos durante ciertas horas del día o todo el tiempo. Si el 7x24 después de la directiva del Bloqueo de llamada de las horas se configura, también restringe el conjunto de números que se puede ingresar por un usuario interior para fijar el **call forward all**.

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

Ejemplo 1

Este ejemplo define varios modelos de los dígitos para los cuales se bloquean las llamadas de salida. Modelos 1 y 2, que bloquean las llamadas a los Números externos que comienzan con el "1" y el "011," se bloquean el de lunes a viernes antes de 7 mañanas y después de 7 P.M., el sábado antes de 7 mañanas y después de 1 P.M., y todo el día domingo. El modelo 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
```

Refiera a configurar el Bloqueo de llamada para más información sobre la restricción del peaje.

Clase de restricción

Abstracto

Si usted quiere el control granular cuando usted configura la restricción del peaje, usted debe utilizar la clase de la restricción (COR). Refiera a la clase de restricción: Ejemplo para más información.

Restricciones del fraude de cargos de llamada de los links troncales H.323/SIP

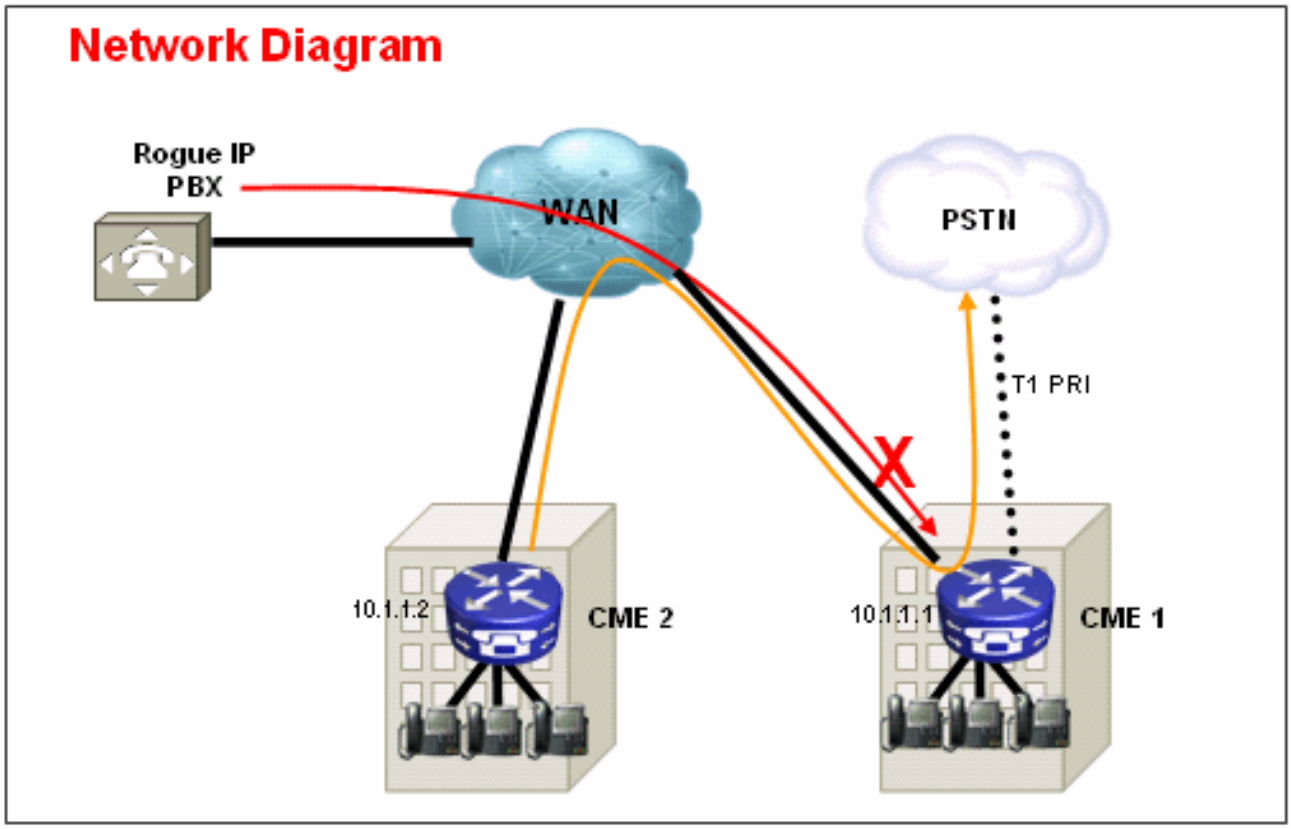
Abstracto

En caso de que un sistema CME esté conectado sobre WAN con otros dispositivos CME a través de un SORBO o de un trunk de H.323, usted puede restringir el acceso del trunk SIP/H.323 al CME para evitar que los adictos usen su sistema para retransmitir ilegal las llamadas al PSTN.

Nota: Esto es una **amenaza exterior**.

Ejemplo 1

En este ejemplo, el CME 1 tiene conectividad PSTN. El CME 2 está conectado sobre WAN con CME 1 a través de un trunk de H.323. Para asegurar el CME 1, usted puede configurar una lista de acceso y aplicarla entrante en la interfaz de WAN y permitir así solamente el tráfico IP de CME 2. Esto evita que el IP PBX del granuja envíe las llamadas VoIP con CME 1 al PSTN.



Solución

No permita que la interfaz de WAN en CME 1 valide el tráfico de los dispositivos ficticios que no reconocen. Observe que hay un implícito NIEGA todos en el extremo de una lista de acceso. Si hay más dispositivos de los cuales usted quiere permitir el tráfico IP entrante, esté seguro de agregar la dirección IP del dispositivo a la lista de acceso.

Configuración de muestra — CME 1

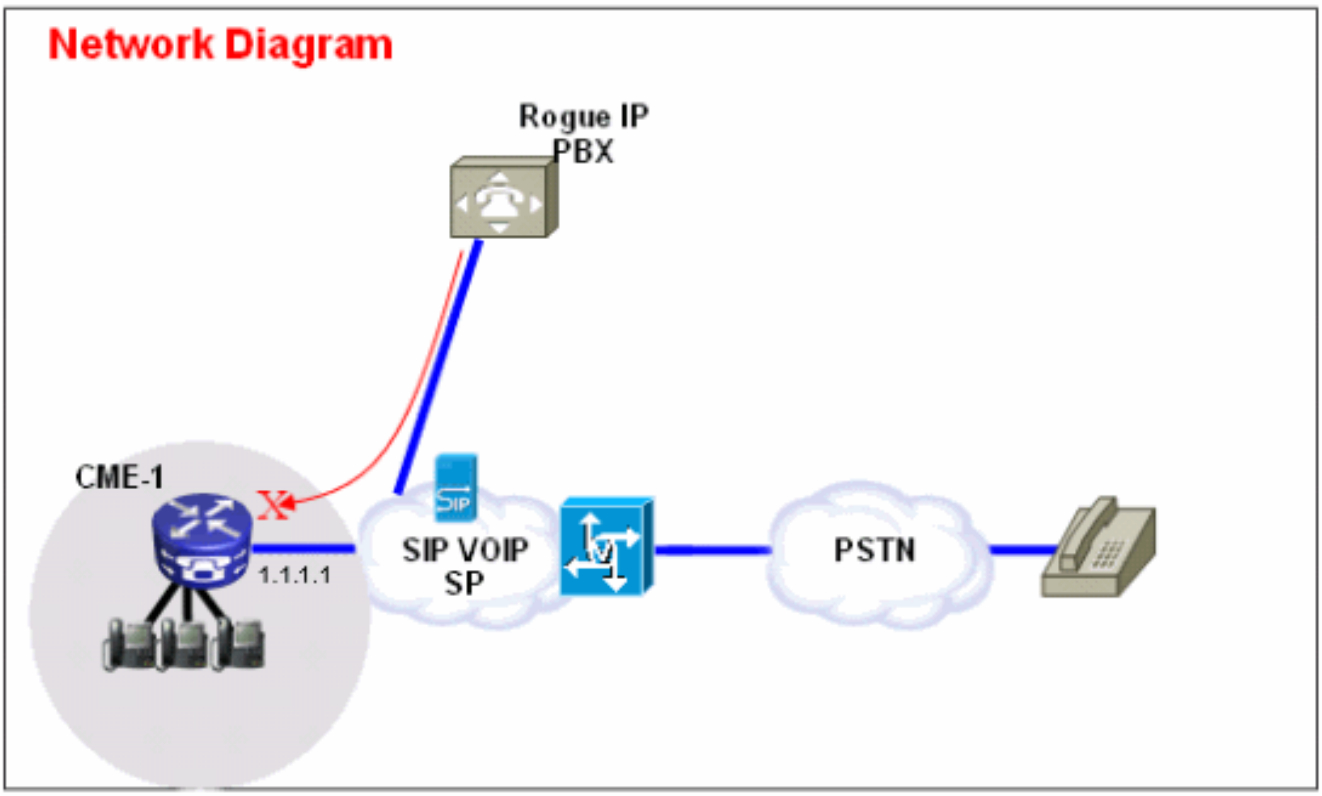
```
interface serial 0/0
  ip access-group 100 in
!
access-list 100 permit ip 10.1.1.2 255.255.255.255 any
```

'Ejemplo 2'

En este ejemplo, el CME 1 está conectado con el proveedor del SORBO para la conectividad PSTN con la configuración de muestra proporcionada en el ejemplo expreso de la configuración de conexión de troncal del SORBO del Cisco CallManager (CME).

Puesto que el CME 1 está en Internet público, es posible que el *fraude de cargos de llamada* puede ocurrir si un usuario rogue analiza a los IP Address públicos para los puertos conocidos para H.323 (TCP 1720) o la señalización del SORBO (UDP o TCP 5060) y envía el SORBO o los

mensajes de H.323 que rutean las llamadas se retira del trunk del SORBO al PSTN. La mayoría de los abusos comunes en este caso son el usuario rogue hacen las llamadas internacionales múltiples a través del SORBO o del trunk de H.323 y hacen al propietario del CME 1 pagar estas llamadas del fraude de cargos de llamada - en algunos casos los millares de dólares.



Solución

Para atenuar esta amenaza, usted puede utilizar las soluciones múltiples. Si ninguna señalización VoIP (SORBO o H.323) no se utiliza sobre los links PÁLIDOS en CME 1, esto se debe bloquear con las técnicas del Firewall en CME 1 (las listas de acceso o los ACL) tanto cuanto sea posible.

1. Asegure la interfaz de WAN con el Firewall del ® del Cisco IOS en CME 1:Esto implica que usted permite que solamente el SORBO sabido o el tráfico de H.323 venga adentro en la interfaz de WAN. Se bloquea el resto de SORBO o del tráfico de H.323. Esto también requiere que usted conozca los IP Addresses que el SORBO VOIP SP utiliza para señalar en el trunk del SORBO. Esta solución asume que el SP está dispuesto a proporcionar todos los IP Addresses o nombres DNS que utilizan en su red. También, si se utilizan los nombres DNS, la configuración requiere que un servidor DNS que puede resolver estos nombres sea accesible. También, si el SP cambia cualesquiera direccionamientos en su extremo, la configuración necesita ser puesta al día en CME 1. Observe que estas líneas necesitan ser agregadas además de cualquier entrada ACL ya presente en la interfaz de WAN.Configuración de muestra — 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 que llamadas que vienen adentro en el trunk del SORBO no se retira la horquilla:Esto implica que la configuración CME 1 permite solamente el SORBO – SORBA la horquilla de las llamadas a un rango de números sabido específico PSTN, el resto de las

llamadas se bloquean. Usted debe configurar a los dial peer de entrada específicos para los números PSTN que vienen adentro en el trunk del SORBO que se asocia a las Extensiones o Auto Attendant o voicemail en CME 1. Todo el otro llama a los números que no son parte de que se bloquea el rango de números CME 1 PSTN. Observe, esto no afecta a la llamada adelante/las transferencias al voicemail (Cisco Unity Express) y call forward all a los números PSTN de los Teléfonos IP en CME 1, porque la llamada inicial todavía se apunta hacia una extensión en CME 1.Configuración de muestra — 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 las Reglas de traducción para bloquear las cadenas de marcado específicas:La mayoría de los fraudes de cargos de llamada implican la marca de la llamada internacional. Como consecuencia, usted puede crear a un dial peer de entrada específico que las cadenas marcadas específicas de las coincidencias y bloqueen las llamadas a ellos. La mayoría de los CME utilizan un código de acceso específico, tal como 9, para marcar hacia fuera y el código de marcación internacional en los E.E.U.U. es 011. Por lo tanto, la cadena de marcado más común a bloquear en los E.E.U.U. es 9011 + cualquier dígito después que venga adentro en el trunk del SORBO.Configuración de muestra — 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 la restricción de la característica

Modelo de la transferencia

Abstracto

Transferencias a todos los números a menos que ésos en los Teléfonos IP locales del SCCP se bloqueen automáticamente por abandono. Durante la configuración, usted puede permitir las transferencias no a los números locales. El comando del transferencia-**modelo** se utiliza para permitir la transferencia de las llamadas de telefonía de los Teléfonos IP del SCCP de Cisco a los teléfonos con excepción de los Teléfonos IP de Cisco, tales como llamadas del externo PSTN o teléfonos en otro sistema CME. Usted puede utilizar el transferencia-**modelo** para limitar las llamadas a las extensiones internas solamente o quizás el límite llama a los números PSTN en cierto código de área solamente. Estos ejemplos muestran cómo el comando del transferencia-**modelo** se puede utilizar para limitar las llamadas a diversos números.

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

Ejemplo 1

Permita que los usuarios transfieran dice en voz alta solamente al código de área 408. En este

ejemplo, la suposición es que el CME está configurado con un dial-peer que tiene un destino-modelo de 9T.

Configuración de muestra:

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

Transferencia-modelo bloqueado

Abstracto

En Cisco unificó las versiones CME 4.0 y posterior, usted puede prevenir los teléfonos individuales de las transferencias de llamada a los números que global se habilitan para la transferencia. El comando **bloqueado transferencia-modelo** reemplaza el comando del transferencia-**modelo** y inhabilita la transferencia de llamada a cualquier destino que necesite ser alcanzado por los CRISOLES o VoIP dial-peer. Esto incluye los números PSTN, el otro Gateways de voz y el Cisco Unity Express. Esto se asegura de que los teléfonos individuales no incurran en a los cargos por larga distancia cuando las llamadas se transfieren fuera del sistema unificado Cisco CME. El bloqueo de la transferencia de llamada se puede configurar para los teléfonos individuales o configurar como parte de una plantilla que se aplique a un conjunto de los teléfonos.

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

Ejemplo 1

En esta configuración de muestra, el ephone 1 no se permite utilizar el transferencia-modelo (definido global) para transferir las llamadas, mientras que el ephone 2 puede utilizar el transferencia-modelo definido bajo telefonía-servicio para transferir las llamadas.

Configuración de muestra:

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

MAX-longitud de la transferencia

Abstracto

El comando de la MAX-**longitud de la transferencia** especifica el número máximo de dígitos que el usuario puede marcar cuando se transfiere una llamada. **La max-longitud del transferencia-modelo** reemplaza el comando del transferencia-**modelo** y aplica los Dígitos máximos permitidos para el destino de la transferencia. El argumento especifica el número de dígitos permitidos en un número al cual se transfiera una llamada. Rango: 3 a 16. Predeterminado: 16.

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

Ejemplo 1

Esta configuración permite solamente los teléfonos que tienen esta ephone-plantilla aplicada para transferir a los destinos que son un máximo de cuatro dígitos de largo.

Configuración de muestra:

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

La llamada remite la MAX-longitud

Abstracto

Para restringir el número de dígitos que se puedan ingresar con la clave suave de CfwdALL en un teléfono del IP, utilice el comando llamada-**delantero de la MAX-longitud** en el ephone abajo o el modo de configuración de la ephone-dn-plantilla. Para quitar una restricción en el número de dígitos que puedan ser ingresados, no utilice la **ninguna** forma de este comando.

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

Ejemplo 1

En este ejemplo, la extensión 101 del directorio se permite realizar un llamada-delantero a cualquier extensión que sea un a cuatro dígitos de largo. Cualquier llamada-adelante a los destinos de cuatro dígitos falla más de largo.

Configuración de muestra:

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

o

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

Ninguna Llamada local delantera

Abstracto

Cuando no se utiliza el **ningún** comando **delantero de las Llamadas locales** en el modo de configuración del ephone abajo, las llamadas internas a un ephone abajo determinado sin las **Llamadas locales delanteras** aplicadas no se remiten si el ephone abajo está ocupado o no contesta. Si un llamador interno suena este ephone abajo y el ephone abajo está ocupado, el llamador oye una señal de ocupado. Si un llamador interno suena este ephone abajo y no contesta, el llamador oye una señal de señal de llamada. La llamada interna no se remite incluso si el reenvío de llamada se habilita para el ephone abajo.

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

Ejemplo 1

En este ejemplo, la extensión 2222 llama la extensión 3675 y oye una señal de llamada o una señal de ocupado. Si una parte llamadora externa alcanza la extensión 3675 y no hay respuesta, la llamada se remite a la extensión 4000.

Configuración de muestra:

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

Autoregistro de la neutralización en el sistema CME

Abstracto

Cuando el auto-REG-**ephone** se habilita por debajo el telefonía-servicio en un sistema del SCCP CME, los nuevos Teléfonos IP que está conectado en el sistema son auto registrado y si el **auto asigna** se configuran para asignar automáticamente los números de interno, después un nuevo teléfono del IP pueden hacer las llamadas inmediatamente.

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

Ejemplo 1

En esta configuración, se configura un nuevo sistema CME de modo que usted deba agregar manualmente un ephone para que el ephone se registre al sistema CME y lo utilice para hacer las llamadas de la Telefonía IP.

Solución

Usted puede inhabilitar el auto-REG-**ephone** por debajo el telefonía-servicio de modo que los nuevos Teléfonos IP conectados con un sistema CME lo hagan no registro auto al sistema CME.

Configuración de muestra:

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

'Ejemplo 2'

Si usted utiliza el SCCP CME y planea registrar los teléfonos del SIP de Cisco al sistema, usted debe configurar el sistema de modo que los puntos finales del SORBO tengan que autenticar con un nombre de usuario y contraseña. Para hacer así pues, configure simplemente esto:

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

Refiera al SORBO: Configurando Cisco unificó el CME para una más guía de configuración general para el SORBO CME.

Herramientas de la restricción del Cisco Unity Express

Asegure el Cisco Unity Express: Acceso AA PSTN

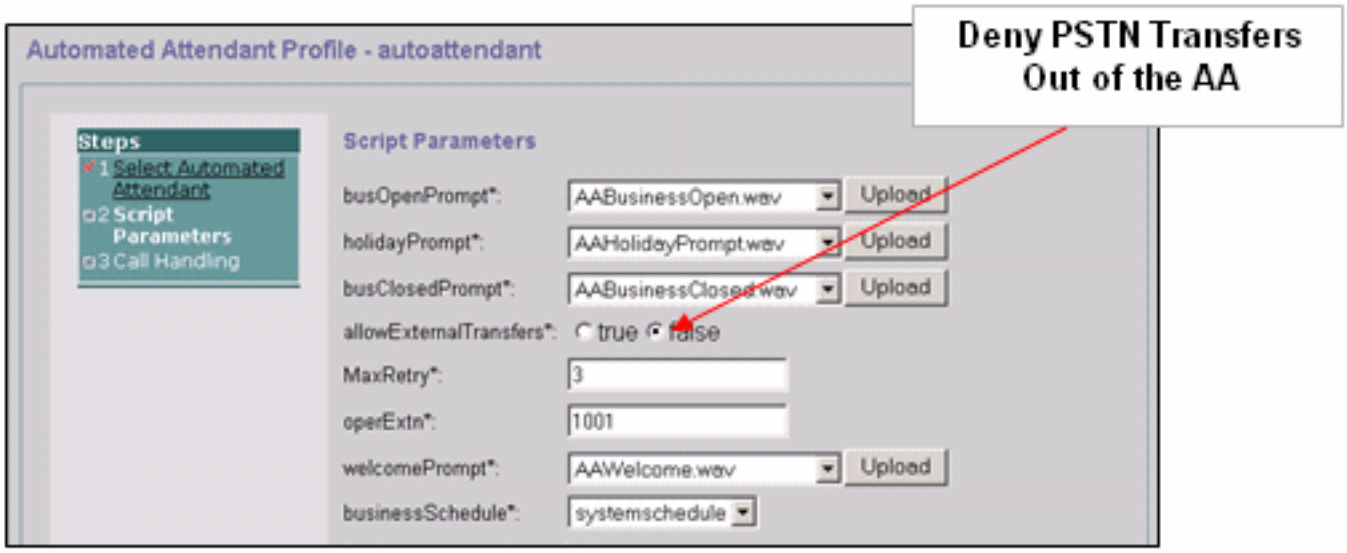
Abstracto

Cuando se configura su sistema para remitir las llamadas entrantes al Auto Attendant (AA) en el Cisco Unity Express, puede ser necesario inhabilitar la transferencia del externo al PSTN del Cisco Unity Express AA. Esto no permite que los usuarios externos marquen saliente a los Números externos después de que alcancen el Cisco Unity Express AA.

Nota: Esto es una **amenaza exterior**.

Nota: **Solución**

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



Nota: Si el acceso PSTN del AA se requiere, limite los números o el rango de los números que son considerados válidos por el script.

Tablas de restricción del Cisco Unity Express

Abstracto

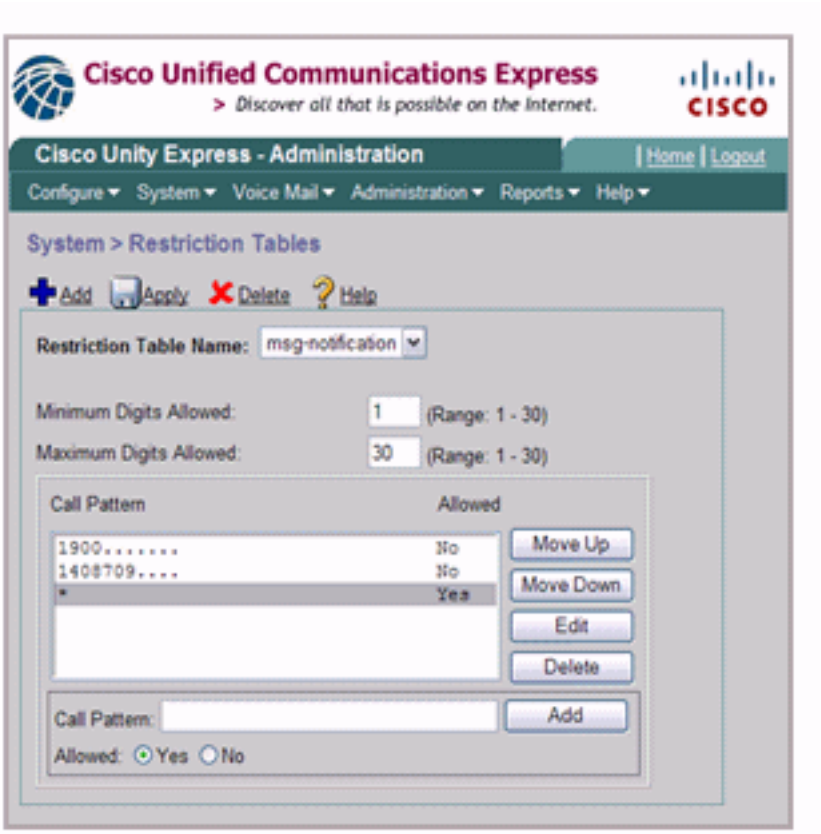
Usted puede utilizar las tablas de restricción del Cisco Unity Express para restringir los destinos que se pueden alcanzar durante un outcall del Cisco Unity Express. La tabla de restricción del Cisco Unity Express se puede utilizar para prevenir el fraude de cargos de llamada y el uso malévolo del sistema del Cisco Unity Express de hacer las llamadas de salida. Si usted utiliza la tabla de restricción del Cisco Unity Express, usted puede especificar los modelos de la llamada a la coincidencia de la placa comodín. Las aplicaciones que utilizan la tabla de restricción del Cisco Unity Express incluyen:

- Fax
- Respuesta viva del Cisco Unity Express
- Notificación del mensaje
- Entrega de mensajes del NON-suscriptor

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

Solución

Para restringir los diagramas de destinos que se pueden alcanzar por el Cisco Unity Express en una llamada externa saliente, configure el **modelo de la llamada** en el **sistema > las tablas de las restricciones del** Cisco Unity Express GUI.



Llame el registro

CDR aumentado

Usted puede configurar el sistema CME para capturar el CDR aumentado y para registrar el CDR a memoria Flash del router o a un servidor FTP externo. Estos expedientes se pueden entonces utilizar para retrazar las llamadas para considerar si ha ocurrido el abuso por los partidos internos o externos.

La característica de contabilidad del archivo introducida con CME 4.3/7.0 en el Cisco IOS Release 12.4(15)XY proporciona un método para capturar los registros de contabilidad en el formato del Comma Separated Value (.csv) y para salvar los expedientes a un archivo en el Flash interno o a un servidor FTP externo. Amplía el soporte de las estadísticas del gateway, que también incluye el AAA y los mecanismos del Syslog de la información de la cuenta del registro.

El proceso de las estadísticas recoge los datos de contabilidad para cada tramo de llamada creado en un gateway de voz de Cisco. Usted puede utilizar esta información para el poste que procesa las actividades por ejemplo para generar los registros de facturación y para la Análisis de red. Los gatewayes de voz de Cisco capturan los datos de contabilidad bajo la forma de registros de detalles de la llamada (CDR) que contengan los atributos definidos por Cisco. El gateway puede enviar los CDR a un servidor de RADIUS, servidor de Syslog, y con el método del nuevo archivo, para contellear o un servidor FTP en el formato del .csv.

Refiera a los ejemplos CDR para más información sobre las capacidades aumentadas CDR.

Información Relacionada

- Mejores prácticas de la Seguridad del Cisco Unified Communications Manager Express
- Guía de administradores expresa del administrador de comunicaciones de Cisco
- Guía de administradores expresa del administrador de comunicaciones de Cisco – Bloqueo de llamada
- Comprensión de la correspondencia de dial-peer en las plataformas IOS
- Traducción del número usando los perfiles de la traducción de la Voz
- Guía de diseño de red de la referencia de la solución CME
- Soporte Técnico y Documentación - Cisco Systems