Prevenção de fraude na tarifa de chamadas expressas do gerente de comunicações unificadas

Índice

Introdução

Este documento fornece um guia de configuração que pode ser usado para otimizar a segurança de um sistema Cisco Communications Manager Express (CME) e reduzir a ameaça de fraudes nas tarifas de ligações. O CME é a solução de Controle de chamadas roteador-baseada de Cisco que fornece uma solução esperta, simples e segura para as organizações que querem executar comunicações unificadas. É recomenda altamente que você executa as medidas de segurança descritas neste documento a fim fornecer o controle de níveis de segurança adicional e reduzir a possibilidade de fraude na tarifa de ligações.

O objetivo deste documento é educá-lo nas várias ferramentas de segurança disponíveis em ciscos voices gateways e em CME. Estas ferramentas podem ser executadas em um sistema CME a fim ajudar a abrandar a ameaça da fraude na tarifa de ligações por partidos internos e externos.

Este documento fornece instruções em como configurar um sistema CME com as várias ferramentas da Segurança do pedágio e da limitação da característica. Do documento os esboços igualmente porque determinadas ferramentas de segurança são usadas em determinadas disposições.

A flexibilidade inerente total das plataformas ISR de Cisco permite que você distribua o CME em muitos tipos diferentes de disposições. Assim pode-se exigir para usar uma combinação das características descritas neste documento para ajudar a travar abaixo do CME. Este documento serve como uma diretriz para que como aplique ferramentas de segurança no CME e de modo algum nas garantias que a fraude na tarifa de ligações ou o abuso por partidos internos e externos não ocorrerão.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Communications Manager Express

Componentes Utilizados

A informação neste documento é baseada no Cisco Unified Communications Manager Express 4.3 e em CME 7.0.

Nota: Cisco unificou CME 7.0 inclui as mesmas características que o CME unificado Cisco 4.3, que renumbered a 7.0 para alinhar com as versões das comunicações unificadas de Cisco.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Visão geral

Este capas de documento a maioria de ferramentas da segurança comum que podem ser usadas em um sistema CME para ajudar a abrandar a ameaça da fraude na tarifa de ligações. As ferramentas de segurança CME providas neste documento incluem ferramentas da limitação do pedágio e ferramentas da limitação da característica.

Ferramentas da limitação do pedágio

- Direct-inward-dial
- Após a limitação do pedágio das horas
- Classe de limitação
- Lista de acesso para restringir o acesso do tronco H323/SIP

Ferramentas da limitação da característica

- Transferência-teste padrão
- Transferência-teste padrão obstruído
- MAX-comprimento de transferência
- MAX-comprimento Atendimento-dianteiro
- Nenhumas chamadas local dianteiras
- Nenhum auto-REG-Ephone

Ferramentas da limitação do Cisco Unity Express

- Fixe o acesso do Cisco Unity Express PSTN
- Limitação da notificação de mensagem

Registro do atendimento

- Atendimento que registra para capturar os registros dos destalhes da chamada (CDR)

Interno contra ameaças externos

Este documento discute ameaças dos partidos internos e externos. Os partidos internos incluem os usuários de telefone IP que residem em um sistema CME. Os partidos externos incluem usuários nos sistemas estrangeiros que podem tentar usar o host CME para fazer atendimentos fraudulentos e para ter os atendimentos carregados de volta a seu sistema CME.

Ferramentas da limitação do pedágio

Direct-inward-dial

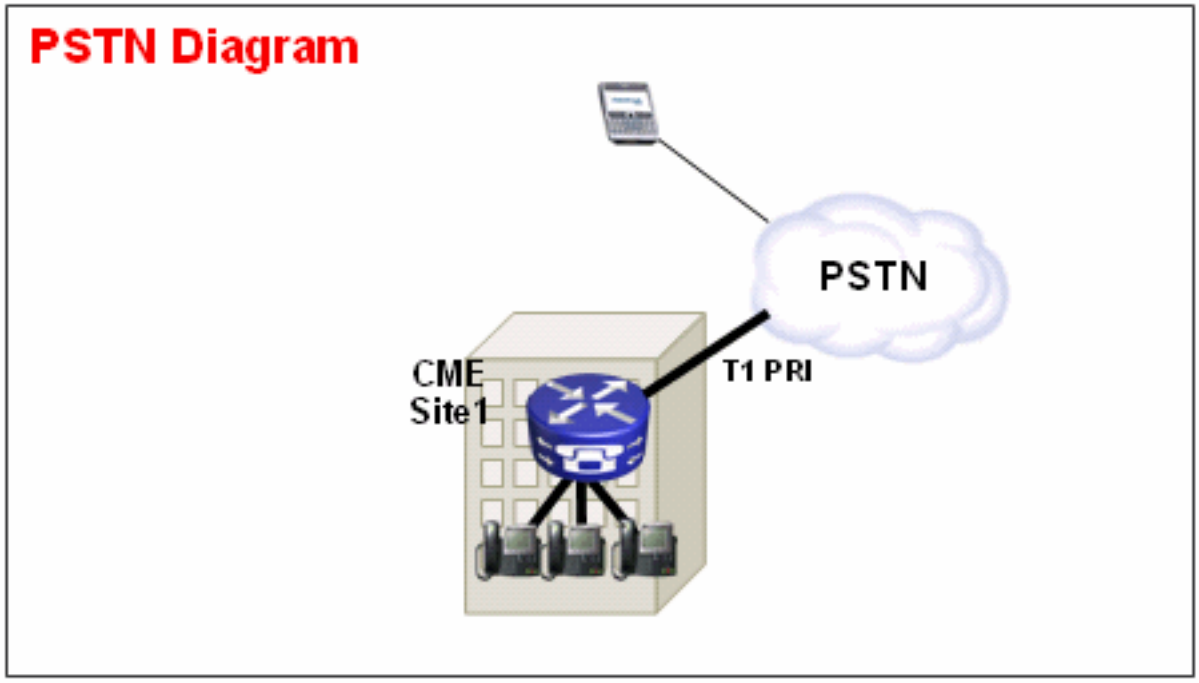
Resumo

o Direto-para dentro-seletor (FEZ) está usado em ciscos voices gateways a fim permitir que o gateway processe uma chamada recebida depois que recebe dígitos do Switch PBX ou CO. Quando FEZ é permitido, o Cisco gateway não apresenta um tom de discagem secundário ao chamador e não espera para recolher dígitos adicionais do chamador. Ele para a frente o atendimento diretamente ao destino que combina o Dialed Number Identification Service (DNIS). de entrada Isso é chamado de discagem de um estágio.

Nota: Esta é uma **ameaça externo**.

Instrução do problema

Se o direto-para dentro-seletor não é configurado em um Cisco gateway ou em um CME, sempre que um atendimento vem dentro do CO ou do PBX ao Cisco gateway, o chamador ouve um tom de discagem secundário. Isto é chamado discagem em dois estágios. Uma vez que os chamadores de PSTN ouvem o tom de discagem secundário, podem incorporar dígitos para alcançar toda a extensão interna ou se conhecem o código de acesso PSTN, podem discar a grande distância ou os números internacionais. Isto apresenta um problema porque o chamador de PSTN pode usar o sistema CME para colocar a grande distância de partida ou as chamadas internacionais e a empresa obtêm carregadas para os atendimentos.



Exemplo 1

No local 1, o CME é conectado ao PSTN através de um tronco do T1 PRI. O fornecedor PSTN fornece os **40855512.** Varie para o local 1. CME. Assim todos os atendimentos PSTN destinados para 4085551200 – 4085551299 são de entrada distribuído ao CME. Se você não configura o direto-para dentro-**seletor no** sistema, um chamador de PSTN de entrada ouve um secundário um tom de discagem e deve manualmente discar a extensão interna. O problema mais grande é que se o chamador é um abusador e conhece o código de acesso PSTN no sistema, geralmente **9**, eles pode discar **9** então todo o número de destino que quiserem alcançar.

Solução 1

A fim abrandar esta ameaça, você deve configurar o direto-para dentro-**seletor**. Isto faz com que o Cisco gateway envie a chamada recebida diretamente ao destino que combina o DNIS de entrada.

Configuração de exemplo

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

Para trabalhe corretamente, certificam-se que a chamada recebida combina o POTS dial peer

correto onde o **comando direct-inward-dial** é configurado. Neste exemplo, o T1 PRI é conectado à porta 1/0:23. A fim combinar o dial peer de entrada correto, emita o **novo** comando dial peer do chamar-**número** sob FEZ o POTS dial peer.

Exemplo 2

No local 1, o CME é conectado ao PSTN através de um tronco do T1 PRI. O fornecedor PSTN dá os **40855512.** e **40855513.** FEZ escalas para o local 1. CME. Assim todos os atendimentos PSTN destinados para 4085551200 – 4085551299 e 4085551300 - 4085551399 são de entrada distribuído ao CME.

Configuração incorreta:

Se você configura um dial peer de entrada, como na configuração de exemplo nesta seção, a possibilidade para a fraude na tarifa de ligações ainda ocorre. O problema com este dial peer de entrada é que combina somente chamadas recebidas a **40852512.** e aplica então prestou serviços de manutenção. Se um atendimento PSTN entra **40852513.** , o dial-peer do POTS de entrada não combina e assim preste serviços de manutenção não é aplicado. Se um dial peer de entrada com FEZ não está combinado, a seguir o dial peer padrão 0 é usado. Por padrão, O DID é desabilitado no peer de discagem 0.

Configuração de exemplo

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

Configuração correta

A maneira correta configurar prestou serviços de manutenção em um dial peer de entrada é mostrada neste exemplo:

Configuração de exemplo

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

Refira a configuração de DID para POTS dial peer para obter mais informações sobre de FEZ para as portas de voz T1/E1 digitais.

Nota: O uso de FEZ não é precisado quando a Linha privada que o ringdown automático (PLAR) está usado em uma porta de voz ou em um script do serviço tal como o atendimento automático (AA) é usado no dial peer de entrada.

Configuração de exemplo — PLAR

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

Configuração de exemplo — Preste serviços de manutenção ao script

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

Após horas anuncie limitações

Resumo

Após horas a limitação do pedágio é uma ferramenta de segurança nova disponível no CME 4.3/7.0 que permite que você configure as políticas da limitação do pedágio baseadas em horas e data. Você pode configurar políticas de modo que não sejam permitidos aos usuários fazer atendimentos aos números predefinidos durante determinadas horas do dia ou todo o tempo. Se o 7x24 após a política do bloqueio de chamada das horas é configurado, igualmente restringe o conjunto de número que pode ser incorporado por um usuário interno para ajustar o **call forward all**.

Nota: Esta é uma **ameaça interna**.

Exemplo 1

Este exemplo define diversos testes padrões de dígitos para que as chamadas externas são obstruídas. Testes padrões 1 e 2, que obstruem atendimentos aos números externos que começam com o "1" e o "011," são obstruídos em de segunda-feira a sexta-feira antes de 7 A M. e após 7 P.m., em sábado antes de 7 A M. e após 1 P.m., e o dia inteiro domingo. O teste padrão 3 obstrui atendimentos a 900 números 7 dias por semana, 24 horas um o dia.

Configuração de exemplo

```
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
```

Refira configurar o bloqueio de chamada para obter mais informações sobre da limitação do pedágio.

Classe de limitação

Resumo

Se você quer o controle granulado quando você configura a limitação do pedágio, você deve usar a classe da limitação (COR). Refira a classe de limitação: Exemplo para mais informação.

Limitações da fraude na tarifa de ligações dos troncos H.323/SIP

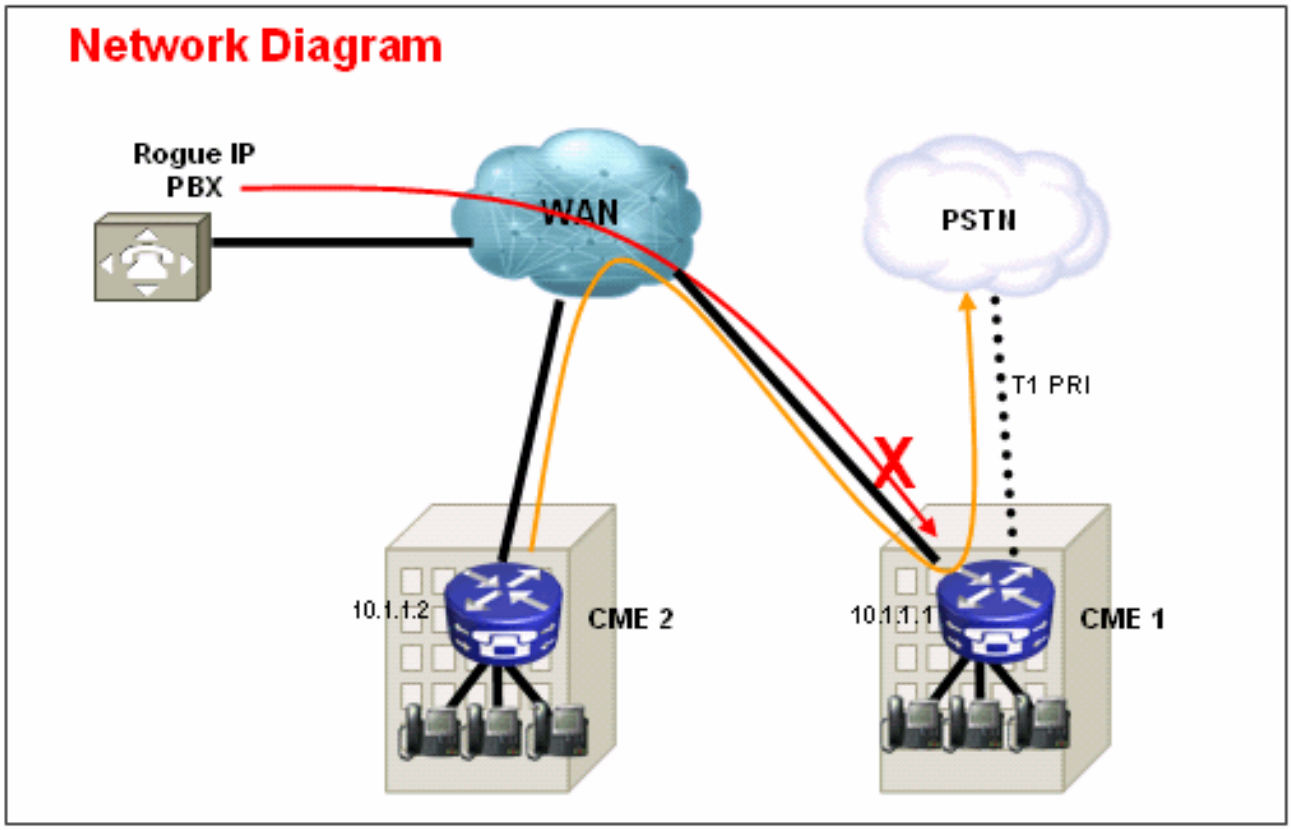
Resumo

Nos casos onde um sistema CME é conectado sobre WAN a outros dispositivos CME através de um SORVO ou de um tronco de H.323, você pode restringir o acesso do tronco SIP/H.323 ao CME a fim impedir que os abusadores usem seu sistema para retransmitir ilegalmente atendimentos ao PSTN.

Nota: Esta é uma **ameaça externo**.

[Exemplo 1]

Neste exemplo, o CME 1 tem a conectividade de PSTN. O CME 2 é conectado sobre WAN a CME 1 através de um tronco de H.323. A fim fixar o CME 1, você pode configurar uma lista de acesso e aplicá-la de entrada na interface WAN e assim somente permitir o tráfego IP de CME 2. Isto impede que o IP PBX do rogue envie chamadas VoIP com CME 1 ao PSTN.



Solução

Não permita que a interface WAN em CME 1 aceite o tráfego dos dispositivos de rogue que não reconhecem. Note que há um implícito NEGA tudo na extremidade de uma lista de acesso. Se há mais dispositivos de que você quer permitir o tráfego IP de entrada, seja certo adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT do dispositivo à lista de acesso.

Configuração de exemplo — CME 1

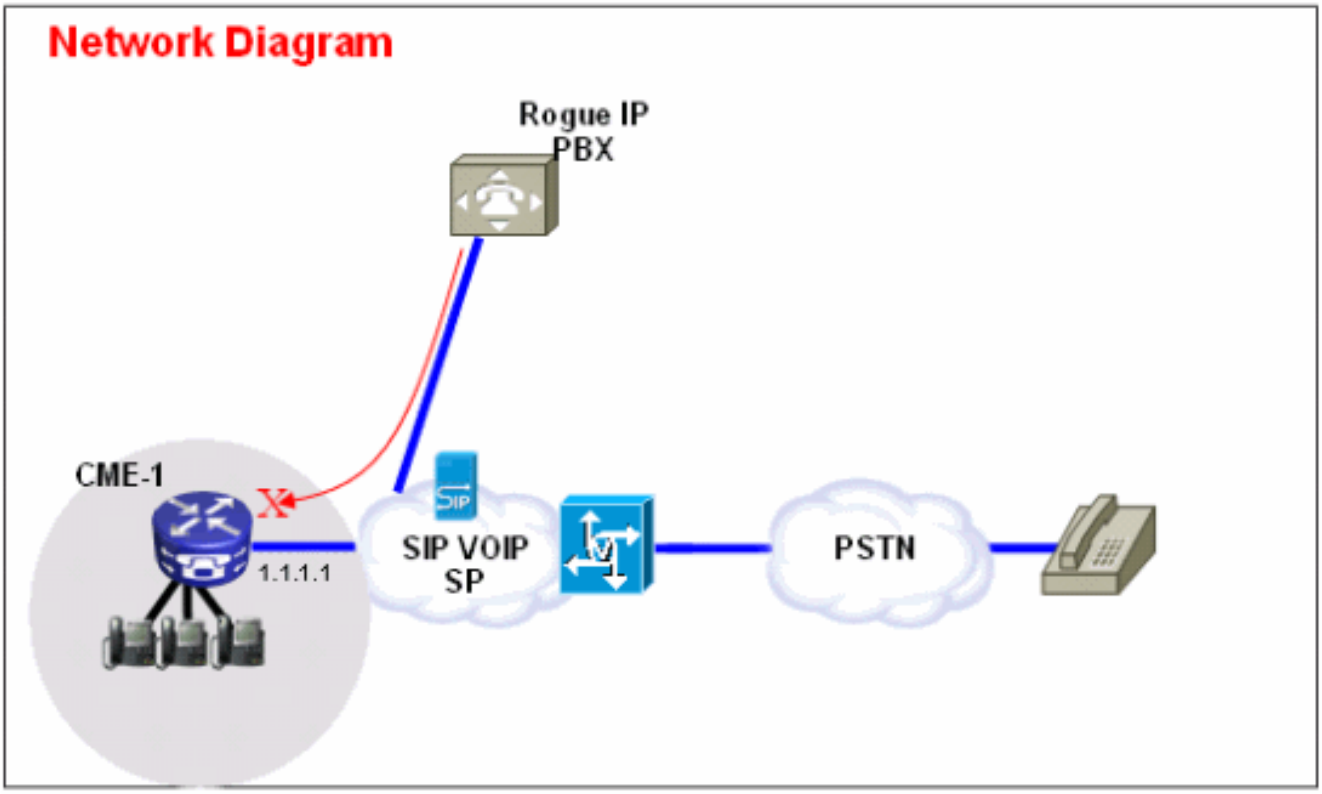
```
interface serial 0/0
  ip access-group 100 in
!
access-list 100 permit ip 10.1.1.2 255.255.255.255 any
```

[Exemplo 2]

Neste exemplo, o CME 1 é conectado ao fornecedor do SORVO para a conectividade de PSTN com a configuração de exemplo fornecida no exemplo expresso da configuração de entroncamento do SORVO do CallManager da Cisco (CME).

Desde que o CME 1 está no Internet público, é possível que a *fraude na tarifa de ligações* pode

ocorrer se um usuário desonesto faz a varredura de endereços IP públicos para portas bem conhecidas para H.323 (TCP 1720) ou a sinalização do SORVO (UDP ou TCP 5060) e envia o SORVO ou as mensagens de H.323 que distribuem atendimentos para trás fora do tronco do SORVO ao PSTN. A maioria de abusos comuns são neste caso o usuário desonesto fazem chamadas internacionais múltiplas através do SORVO ou do tronco de H.323 e fazem com que o proprietário do CME 1 pague por estes atendimentos da fraude na tarifa de ligações - em alguns casos milhares de dólares.



Solução

A fim abrandar esta ameaça, você pode usar soluções múltiplas. Se nenhuma sinalização voip (SORVO ou H.323) não é usada sobre os links MACILENTOS em CME 1, esta deve ser obstruída com as técnicas do Firewall em CME 1 (listas de acesso ou ACL) tanto quanto possível.

1. Fixe a interface WAN com o Firewall do ® do Cisco IOS em CME 1:Isto implica que você permite que somente o SORVO conhecido ou o tráfego de H.323 venham dentro na interface WAN. Todo SORVO ou tráfego restante de H.323 são obstruídos. Isto igualmente exige que você conhece os endereços IP de Um ou Mais Servidores Cisco ICM NT que o SORVO VOIP SP usa sinalizando no tronco do SORVO. Esta solução supõe que o SP é disposto fornecer todos os endereços IP de Um ou Mais Servidores Cisco ICM NT ou nomes de DNS que se usam em sua rede. Também, se os nomes de DNS são usados, a configuração exige que um servidor DNS que possa resolver estes nomes é alcançável. Também, se o SP muda quaisquer endereços em sua extremidade, a configuração precisa de ser atualizada em CME 1. Note que estas linhas precisam de ser adicionadas além do que todas as entradas ACL já atuais na interface WAN.Configuração de exemplo — 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. Assegure-se de que atendimentos que vêm dentro no tronco do SORVO não faz a parte traseira do gancho de cabelo para fora:Isto implica que a configuração CME 1 reserva somente o SORVO – SORVA o gancho de cabelo dos atendimentos a uma faixa de número conhecida específico PSTN, todos atendimentos restantes são obstruídos. Você deve configurar dial peer de entrada específicos para os números PSTN que vêm dentro no tronco do SORVO que é traçado aos Ramais ou o atendimento automático ou o correio de voz em CME 1. Todo o outro chama aos números que não são a faixa de número CME 1 PSTN são obstruídos parte de. Note, isto não afeta o atendimento para a frente/transferências ao correio de voz (Cisco Unity Express) e call forward all aos números PSTN dos Telefones IP em CME 1, porque a chamada inicial é visada ainda para uma extensão em CME 1.Configuração de exemplo — 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. Use Regras de tradução a fim obstruir séries de discagem específicas:A maioria de fraudes na tarifa de ligações envolvem discar da chamada internacional. Em consequência, você pode criar um dial peer de entrada específico que as séries discadas específicas dos fósforos e obstruam atendimentos a elas. A maioria de CME usam um código de acesso específico, tal como 9, para discar para fora e o código de discagem internacional nos E.U. é 011. Consequentemente, a série de discagem a mais comum a obstruir nos E.U. é 9011 + todos os dígitos em seguida que vierem dentro no tronco do SORVO.Configuração de exemplo — 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
```

Ferramentas da limitação da característica

Teste padrão de transferência

Resumo

Transferências a todos os números a não ser que aqueles em Telefones IP locais SCCP sejam obstruídos automaticamente à revelia. Durante a configuração, você pode permitir transferências não aos números locais. O comando do transferência-**teste padrão** é usado a fim permitir transferência das chamadas de telefonia dos Telefones IP de Cisco SCCP aos telefones diferentes dos Telefones IP de Cisco, tais como atendimentos externos PSTN ou telefones em um outro sistema CME. Você pode usar o transferência-**teste padrão** a fim limitar os atendimentos às extensões internas somente ou talvez o limite chama aos números PSTN em um determinado código de área somente. Estes exemplos mostram como o comando do transferência-**teste padrão** pode ser usado para limitar atendimentos aos números diferentes.

Nota: Esta é uma **ameaça interna**.

Exemplo 1

Permita que os usuários transfiram chama somente ao código de área 408. Neste exemplo, a suposição é que o CME está configurado com um dial-peer que tem um destino-teste padrão de 9T.

Configuração de exemplo

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

Transferência-teste padrão obstruído

Resumo

Em Cisco unificou CME 4.0 e umas versões mais atrasadas, você pode impedir telefones individuais das chamadas de transferência aos números que são permitidos globalmente para transferência. O comando **obstruído transferência-teste padrão** cancela o comando do transferência-**teste padrão** e desabilita transferência de chamada a todo o destino que precisar de ser alcançado pelo POTENCIÔMETROS ou VoIP dial-peer. Isto inclui números PSTN, o outro Gateways de voz e o Cisco Unity Express. Isto assegura-se de que os telefones individuais não incorram cobranças de tarifa quando os atendimentos são transferidos fora do sistema unificado Cisco CME. A obstrução de transferência de chamada pode ser configurada para telefones individuais ou ser configurada como parte de um molde que seja aplicado a um grupo de telefones.

Nota: Esta é uma **ameaça interna**.

Exemplo 1

Nesta configuração de exemplo, o ephone 1 não é permitido usar o transferência-teste padrão (definido globalmente) para transferir atendimentos, quando o ephone 2 puder usar o transferência-teste padrão definido sob o telefonia-serviço para transferir atendimentos.

Configuração de exemplo

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

MAX-comprimento de transferência

Resumo

O comando do MAX-**comprimento de transferência** especifica o número máximo de dígitos que o usuário pode discar quando um atendimento é transferido. **O max-comprimento do transferência-teste padrão** cancela o comando do transferência-**teste padrão** e reforça os dígitos máximos permitidos o destino de transferência. O argumento especifica o número de dígitos permitidos em um número a que um atendimento é transferido. Escala: 3 a 16. Padrão: 16.

Nota: Esta é uma **ameaça interna**.

Exemplo 1

Esta configuração permite somente os telefones que têm este Ephone-molde aplicado para transferir aos destinos que são um máximo de quatro dígitos por muito tempo.

Configuração de exemplo

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

O atendimento envia o MAX-comprimento

Resumo

A fim restringir o número de dígitos que podem ser incorporados com a chave macia de CfwdALL em um telefone IP, use o comando atendimento-**dianteiro do MAX-comprimento no** ephone-dn ou no modo de configuração do Ephone-dn-molde. A fim remover uma limitação no número de dígitos que podem ser incorporados, não use **nenhum** formulário deste comando.

Nota: Esta é uma **ameaça interna**.

Exemplo 1

Neste exemplo, a extensão 101 do diretório é permitida executar um atendimento-dianteiro a toda a extensão que for um a quatro dígitos de comprimento. Todo o atendimento-para a frente aos destinos mais por muito tempo de quatro dígitos falha.

Configuração de exemplo

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

ou

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

Nenhuma chamada local dianteira

Resumo

Quando **nenhum** comando **dianteiro das chamadas local** é usado no modo de configuração do ephone-dn, as chamadas internas a um ephone-dn particular sem as **chamadas local dianteiras** aplicadas não estão enviadas se o ephone-dn é ocupado ou não responde. Se um chamador interno soa este ephone-dn e o ephone-dn é ocupado, o chamador ouve um busy signal (sinal ocupado). Se um chamador interno soa este ephone-dn e não responde, o chamador ouve um sinal de ringback. A chamada interna não é enviada mesmo se o encaminhamento de chamada é permitido para o ephone-dn.

Nota: Esta é uma **ameaça interna**.

Exemplo 1

Neste exemplo, a extensão 2222 chama a extensão 3675 e ouve um ringback ou um busy signal (sinal ocupado). Se um caller externo alcança a extensão 3675 e há uma sem resposta, o atendimento está enviado à extensão 4000.

Configuração de exemplo

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

Registro automático do desabilitação no sistema CME

Resumo

Quando auto-REG-**Ephone** é permitido debaixo do telefonia-serviço em um sistema SCCP CME, os Telefones IP novos que é obstruído no sistema são automóvel registrado e se o **automóvel atribui** estão configurados para atribuir automaticamente números de extensão, a seguir um telefone IP novo podem fazer imediatamente atendimentos.

Nota: Esta é uma **ameaça interna**.

Exemplo 1

Nesta configuração, um sistema novo CME é configurado de modo que você deva manualmente adicionar um ephone para que o ephone se registre ao sistema CME e se use o para fazer atendimentos da Telefonia IP.

Solução

Você pode desabilitar auto-REG-**Ephone** debaixo do telefonia-serviço de modo que os Telefones IP novos conectados a um sistema CME façam não auto registro ao sistema CME.

Configuração de exemplo

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

Exemplo 2

Se você usa SCCP CME e o planeia registrar telefones do SIP Cisco ao sistema, você deve configurar o sistema de modo que os valores-limite do SORVO tenham que autenticar com um nome de usuário e senha. A fim fazer assim, configurar simplesmente isto:

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

Refira o SORVO: Estabelecendo Cisco unificou o CME para mais guia de configuração abrangente para o SORVO CME.

Ferramentas da limitação do Cisco Unity Express

Fixe o Cisco Unity Express: Acesso AA PSTN

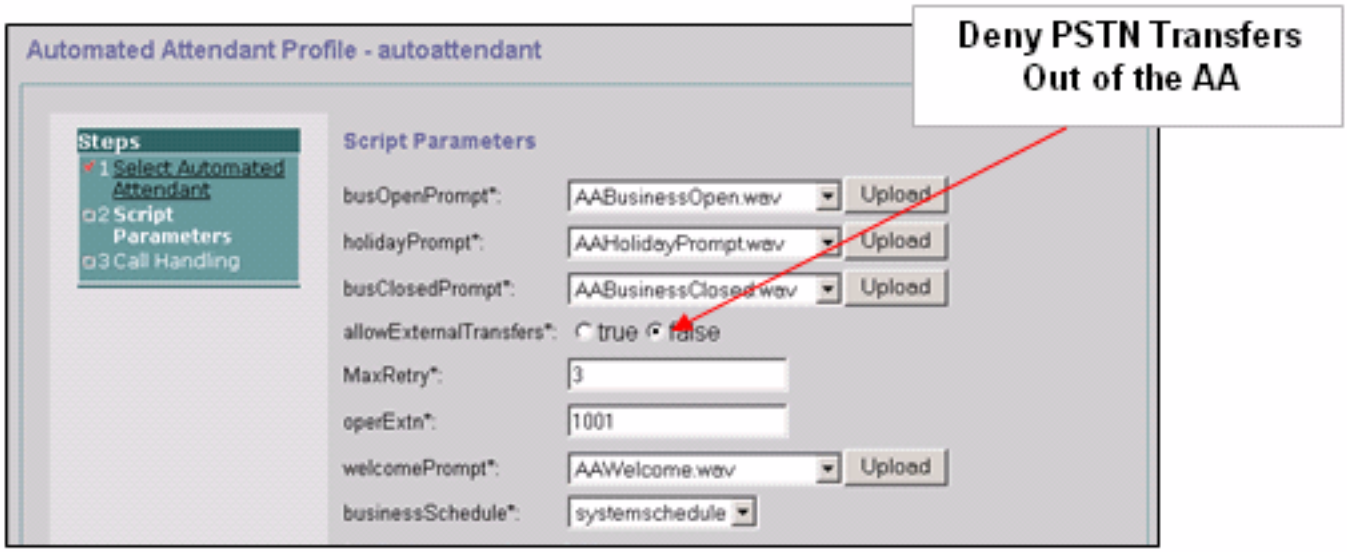
Resumo

Quando seu sistema é configurado de modo que as chamadas recebidas estejam enviadas ao atendimento automático (AA) no Cisco Unity Express, pode ser necessário desabilitar transferência externo ao PSTN do Cisco Unity Express AA. Isto não permite que os usuários externos disquem de partida aos números externos depois que alcança o Cisco Unity Express AA.

Nota: Esta é uma **ameaça externo**.

Nota: Solução

Nota: Desabilite a opção dos **allowExternalTransfers no** Cisco Unity Express GUI.



Nota: Se o acesso PSTN do AA é exigido, limite os números ou a escala dos números que são considerados válidos pelo script.

Tabelas de restrição do Cisco Unity Express

Resumo

Você pode usar as tabelas de restrição do Cisco Unity Express a fim restringir os destinos que podem ser alcançados durante uma chamada de saída do Cisco Unity Express. A tabela de restrição do Cisco Unity Express pode ser usada a fim impedir a fraude na tarifa de ligações e o uso malicioso do sistema do Cisco Unity Express fazer chamadas externas. Se você usa a tabela de restrição do Cisco Unity Express, você pode especificar testes padrões do atendimento ao fósforo da curinga. Os aplicativos que usam a tabela de restrição do Cisco Unity Express incluem:

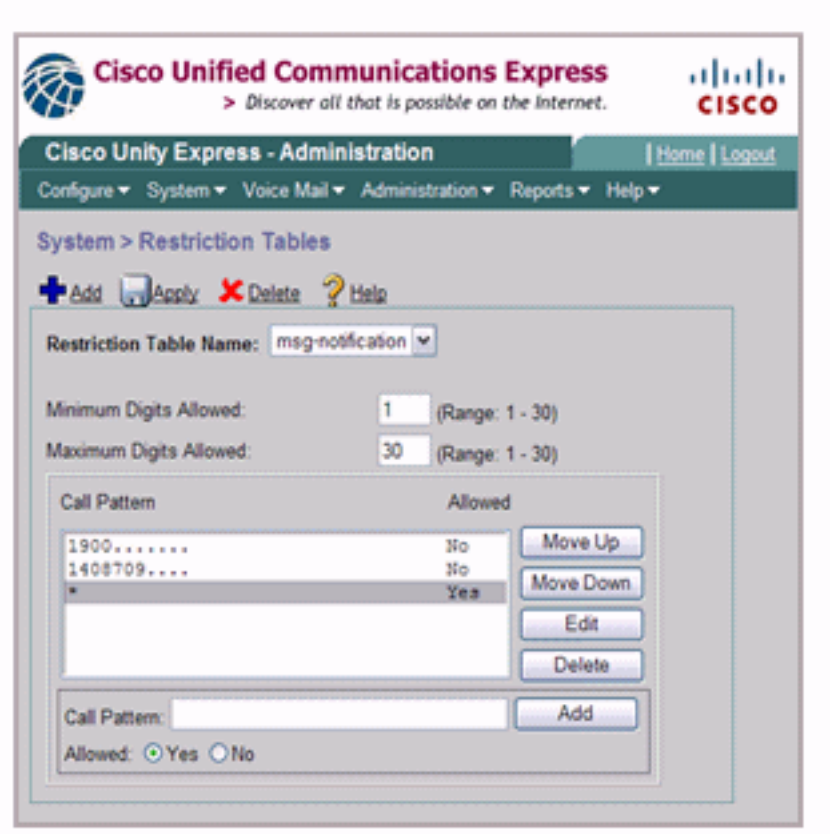
- Fax
- Repetição viva do Cisco Unity Express
- Notificação de mensagem

- Entrega de mensagem do NON-subscritor

Nota: Esta é uma **ameaça interna**.

Solução

A fim restringir os padrões de destino que podem ser alcançados pelo Cisco Unity Express em uma chamada externa de partida, configurar o **teste padrão do atendimento no sistema > tabelas das limitações do** Cisco Unity Express GUI.



Chame o registro

CDR aumentado

Você pode configurar o sistema CME para capturar o CDR aumentado e para registrar o CDR ao flash de roteador ou a um servidor FTP externo. Estes registros podem então ser usados para reconstituir atendimentos para considerar se o abuso por partidos internos ou externos ocorreu.

Os recursos de contabilidade do arquivo introduzidos com CME 4.3/7.0 no Cisco IOS Release 12.4(15)XY fornecem um método para capturar registros de contabilidade no formato do Comma Separated Value (.csv) e para armazenar os registros a um arquivo no flash interno ou a um servidor FTP externo. Expande o apoio da contabilidade do gateway, que igualmente inclui o AAA e os mecanismos do Syslog da informação de contabilidade de registro.

O processo da contabilidade recolhe dados de contabilidade para cada trecho de chamada criado em um cisco voice gateway. Você pode usar esta informação para o cargo que processa atividades como para gerar registros de faturamento e para a análise de rede. Os ciscos voices gateways capturam dados de contabilidade sob a forma dos registros dos destalhes da chamada (CDR) que contêm os atributos definidos por Cisco. O gateway pode enviar CDR a um servidor Radius, servidor de SYSLOG, e com o método do arquivo novo, para piscar ou um servidor FTP

no formato .csv.

Refira exemplos CDR para obter mais informações sobre das capacidades aumentadas CDR.

Informações Relacionadas

- Melhores prática da Segurança do Cisco Unified Communications Manager Express
- Guia de administradores expresso do Gerenciador de Comunicações de Cisco
- Guia de administradores expresso do Gerenciador de Comunicações de Cisco – Bloqueio de chamada
- Compreendendo a correspondência de dial peer em plataformas IOS
- Tradução do número usando perfis da tradução da Voz
- Guia de design de rede da referência da solução CME
- Suporte Técnico e Documentação - Cisco Systems