Unified Communications Manager Express长话欺骗预防

目录

简介

本文提供能使用为了帮助安全Cisco Communications Manager Express的一个配置指南(CME)系统和缓和长话欺骗威胁。CME是为组织提供一聪明，简单和安全解决方案要实现统一通信的思科的基于路由器的呼叫控制解决方案。它是强烈建议您实现在本文描述的安全措施为了提供另外的安全级别电平控制和减少长话欺骗的可能性。

本文目标将教育您在多种安全工具可用在Cisco语音网关和CME。这些工具在CME系统可以实现为了帮助缓和长话欺骗威胁由内部和外部当事人。

本文提供说明关于怎样配置一个CME系统以多种费用安全和显示功能限制工具。也本文概述某些安

全工具为什么用于某些部署。

思科的ISR平台的整体内在的灵活性允许您部署在许多不同种类的CME的部署。因而它在本文可以要求使用描述的功能的组合帮助锁定在CME下。本文起一个指南作用对于如何应用在CME和绝不保证的安全工具长话欺骗或滥用由内部和外部当事人不会发生。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Unified Communications Manager Express

使用的组件

本文档中的信息根据Cisco Unified Communications Manager Express 4.3和CME 7.0。

注意： Cisco Unified CME 7.0包括功能和Cisco Unified CME 4.3一样，被重数到7.0与Cisco Unified通信版本对齐。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

概述

本文包括在CME系统能使用帮助缓和长话欺骗威胁的多数普通的安全性工具。本文参考的CME安全工具包括费用限制工具并且显示功能限制工具。

费用限制工具

- Direct-inward-dial
- 在几小时费用限制以后
- 限制中集集团
- access-list限制H323/SIP中继访问

功能限制工具

- 转移模式
- 阻塞的转移模式
- 转移麦斯长度
- 呼叫转移麦斯长度
- 没有向前本地呼叫

- 没有自动REG ephone

Cisco Unity Express限制工具

- 安全Cisco Unity Express PSTN访问
- 留言通知限制

呼叫记录日志

- 捕获呼叫详细记录的呼叫记录日志(CDR)

内部与外部危机

本文讨论自内部和外部当事人的威胁。内部当事人包括在CME系统驻留的IP电话用户。外部当事人包括能设法使用主机CME做欺骗呼叫和有呼叫被充电回到您的CME系统的外国系统的用户。

费用限制工具

Direct-inward-dial

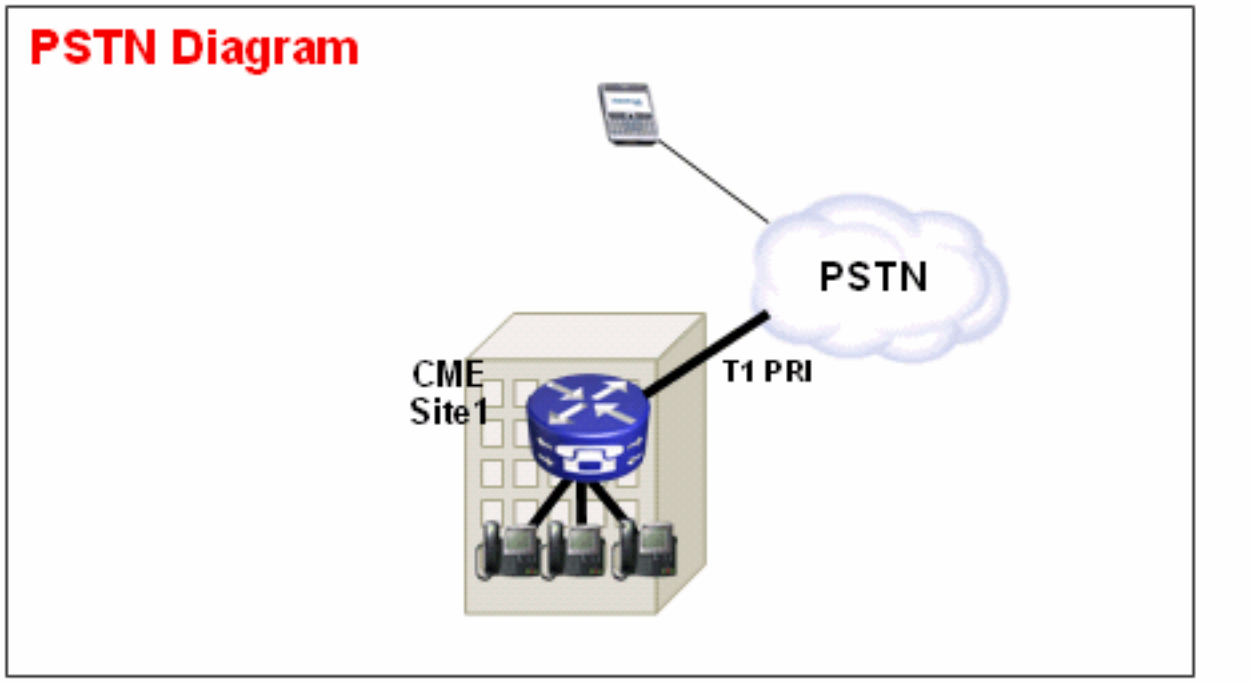
摘要

在收到从Pbx或CO交换机后的位直接拨入(DID)在Cisco语音网关用于为了允许网关处理呼入呼叫。当DID启用时， Cisco网关不提交一二次拨号音给呼叫方，并且不等待从呼叫方收集另外的位。它传送呼叫直接地对匹配入站拨号号码识别服务(DNIS)的目的地。这称为一次拨号。

注意： 这是一个**外部危机**。

问题陈述

如果直接拨入在Cisco网关或CME没有配置，每当呼叫自CO或PBX进来到Cisco网关，呼叫方听到辅助拨号音。这呼叫两阶段拨号。一旦PSTN呼叫方听到辅助拨号音，他们能进入位到达所有内部分机或，如果他们认识PSTN接入代码，他们能拨号长距离或国际号码。因为PSTN主叫方能使用CME系统放置出站长距离或国际呼叫和收的公司获得呼叫，这提出一问题。



示例 1

在站点1， CME连接对PSTN通过T1PRI中继。PSTN供应商提供**40855512。**CME站点的1. DID的范围。因而被注定的所有PSTN呼叫4085551200 – 4085551299的路由的入站对CME。如果不配置在系统的**直接拨入**，一入站PSTN主叫方听到第二播号音，并且必须手工拨号内部分机。更大的问题是，如果呼叫方是滥用者并且认识在系统的PSTN接入代码，他们要到达的通常**9**，他们能拨号**9**然后任何目标号码。

解决方案 1

为了缓和此威胁，您必须配置**直接拨入。**这造成Cisco网关传送呼入呼叫直接地到匹配入站DNIS的目的地。

配置示例

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

为了使DID正确地工作，请确保呼入呼叫匹配**direct-inward-dial命令**配置的正确POTS拨号对等。在本例中， T1PRI连接到端口1/0:23。为了匹配正确呼入拨号对端，请发出**incoming called-number** dial peer命令在DID的POTS拨号对端下。

示例 2

在站点1， CME连接对PSTN通过T1PRI中继。PSTN供应商给**40855512。**并且**40855513。**CME站点的1. DID的范围。因而被注定的所有PSTN呼叫4085551200 – 4085551299和4085551300 - 4085551399的路由的入站对CME。

不正确的配置：

如果配置呼入拨号对端，正如在此部分的配置示例，长话欺骗的可能性仍然发生。与此呼入拨号对端的问题是只匹配呼入呼叫到**40852512。**然后运用DID的服务。如果PSTN呼叫进入**40852513。**呼入POTS dial-peer不配比，并且DID的服务没有因而应用。如果有DID的一呼入拨号对端没有匹配

，则使用默认拨号对端0。默认情况下在拨号对等体 0 上禁用 DID。

配置示例

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

正确配置

正确方式配置在呼入拨号对端的DID的服务显示在本例中：

配置示例

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

POTS拨号对端的参考的DID配置关于数字T1/E1语音端口的DID的更多信息。

注意： 使用DID不是需要的，当私有线路自动回环(PLAR)时在语音端口或脚本例如自动总机的服务使用(AA)在呼入拨号对端使用。

配置示例— PLAR

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

配置示例—服务脚本

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

在几小时费用限制以后

摘要

在几小时之后允许您配置费用准时基于的限制策略和定日期的费用限制是在CME 4.3/7.0的一新的安全工具联机。您能配置策略，以便用户没有允许做呼叫到预定义的编号在天的一直某些小时或。如果在几小时呼叫阻塞策略以后的7x24配置，也限制可以由一个内部的用户输入设置**转发所有呼叫的**一组数字。

注意： 这是**内部威胁**。

示例 1

此示例定义了呼出阻塞的几种数字模式。模式1和2，阻塞呼叫到外线号码开始与"1"和"011,"星期一到星期五阻塞在上午7点前和在下午7点以后，在上午7点前的星期六和在下午1点以后和整天星期日。模式3阻塞呼叫到900号码每星期七天，一天24小时。

配置示例

```
 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
```

参考配置呼叫阻塞关于费用限制的更多信息。

限制中集集团

摘要

如果想要粒状控制，当您配置费用限制时，您必须使用中集集团限制(COR)。限制参考的中集集团：示例欲知更多信息。

H.323/SIP中继长话欺骗限制

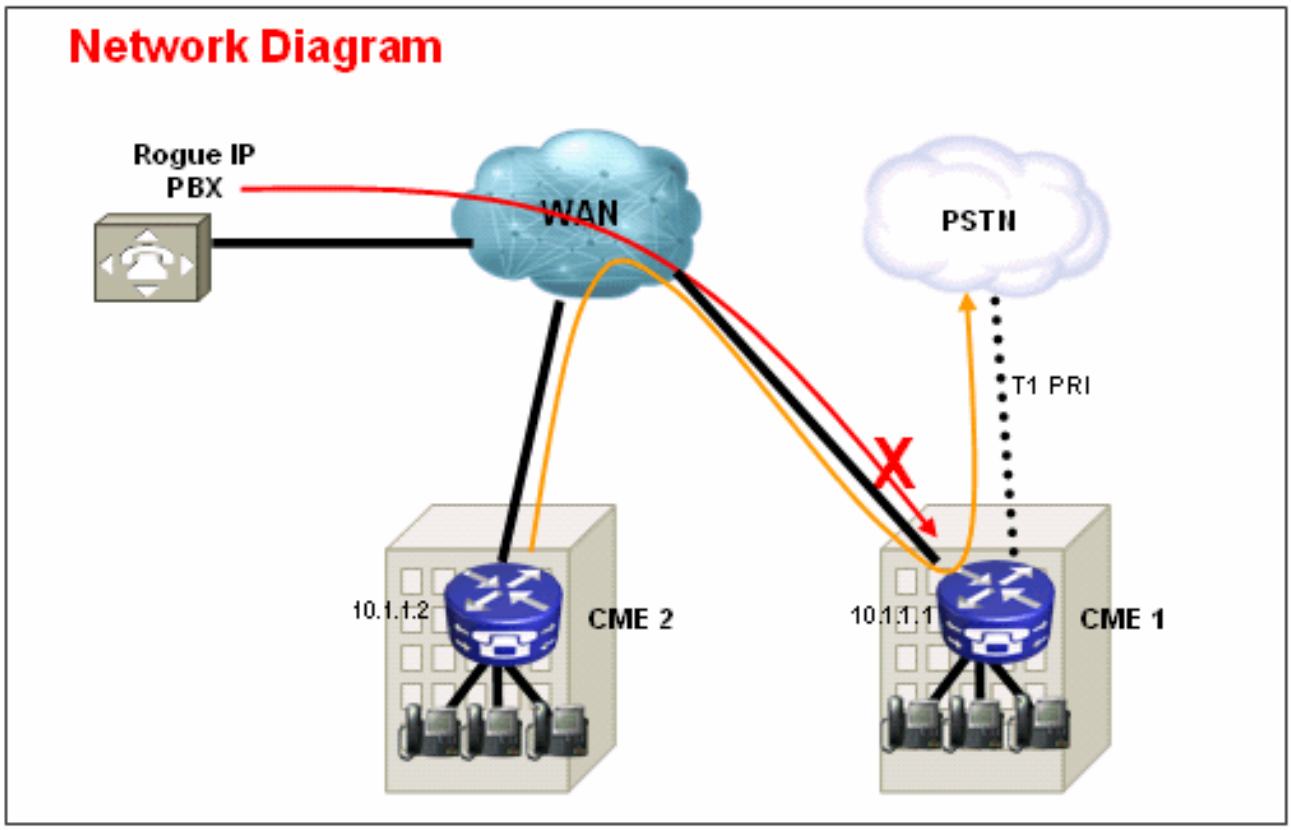
摘要

在CME系统在对其他CME设备的广域网连接到SIP或H.323中继处，您能限制SIP/H.323对CME的中继访问为了防止滥用者使用您的系统非法中继呼叫到PSTN。

注意： 这是一个**外部危机**。

示例 1

在本例中， CME 1有PSTN连接。CME 2在对CME 1的广域网连接通过H.323中继。为了获取CME 1，您能配置access-list和应用它入站在广域网接口和只因而允许从CME 2.的IP数据流。这防止恶意IP PBX发送VoIP呼叫通过CME 1对PSTN。



解决方案

请勿允许在CME 1的广域网接口接收从不识别的恶意设备的流量。注意隐式拒绝所有在结束时access-list。如果有您要允许入站IP数据流的更多设备，请务必添加设备的IP地址对access-list。

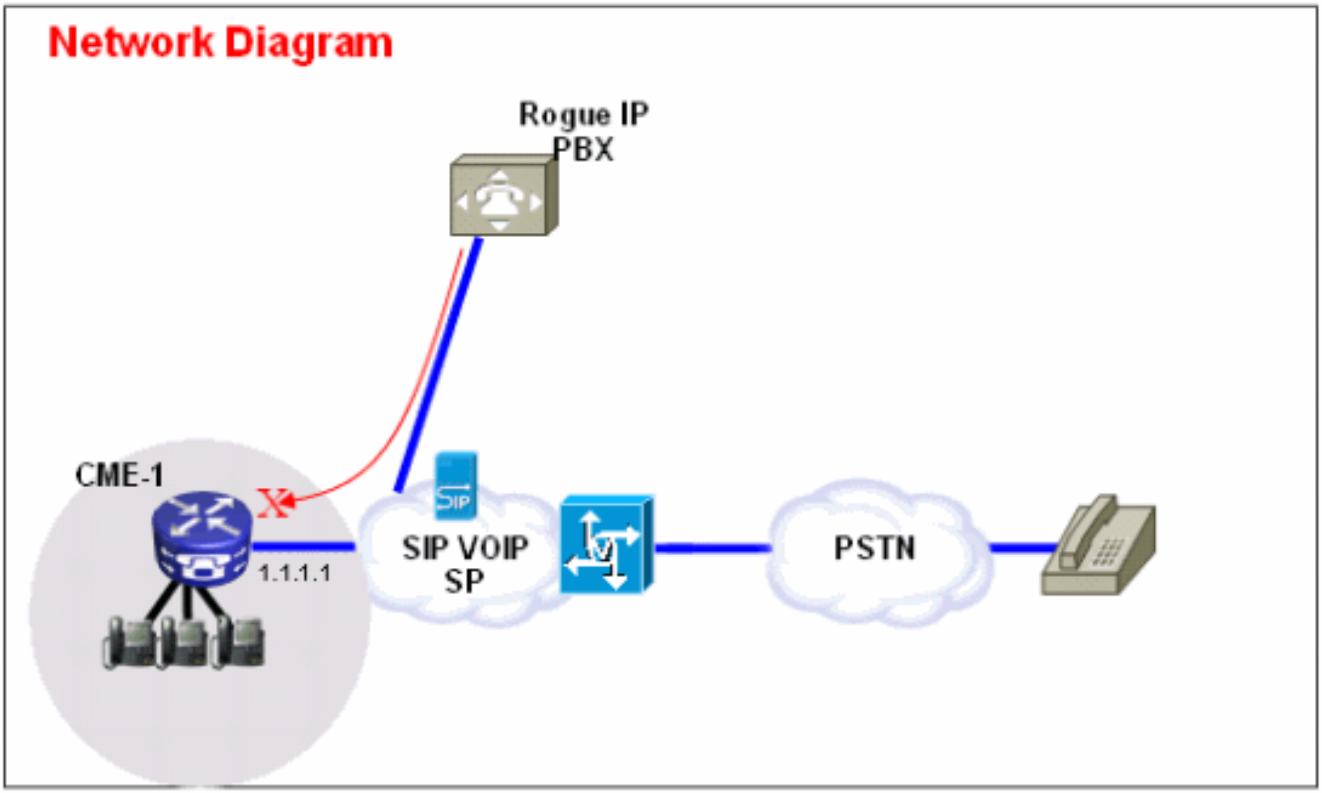
配置示例— CME 1

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

示例 2

在本例中， CME 1连接对PSTN连接的SIP供应商与配置示例提供在Cisco CallManager Express (CME) SIP中继配置示例。

因为CME 1在公共互联网，很可能，*长话欺骗*能发生，如果一个恶意用户扫描公认端口的公共IP地址H.323 (TCP 1720)或SIP (UDP或TCP 5060)信令的并且传送路由呼叫取消SIP中继对PSTN的SIP或H.323信息。最普通的滥用在这种情况下是恶意用户通过SIP或H.323中继做多次国际呼叫并且造成CME 1的所有者支付这些长话欺骗呼叫-在某些情况下千位美元。



解决方案

为了缓和此威胁，您能使用多种解决方案。如果任何VoIP信令(SIP或H.323)没有在广域网链路使用到CME 1，必须尽量阻塞这与在CME 1的防火墙技术(访问列表或ACL)。

1. 巩固与Cisco IOS防火墙的广域网接口在CME 1 ：这暗示您在广域网接口允许已知仅SIP或H.323流量进来。其他SIP或H.323流量阻塞。这也要求您认识发信号的SIP VOIP SP用途在SIP中继的IP地址。此解决方案假设， SP是愿意提供他们在他们的网络使用的所有IP地址或DNS名。并且，如果使用DNS名，配置要求能解析这些名称的DNS服务器可及的。并且，如果SP更改在他们的末端的任何地址，配置在CME 1.需要更新。注意这些线路需要被添加除所有ACL条目之外已经在广域网接口。配置示例— 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. 保证在SIP中继进来发夹不取消的呼叫：这暗示1配置只允许SIP –呼叫SIP发夹对特定已知PSTN号码范围的CME，其他呼叫阻塞。您必须配置在SIP中继进来被映射对扩展或Auto Attendant或者语音邮件在CME 1.的PSTN编号的特定呼入拨号对端。对不作为CME 1 PSTN号码范围的部分的编号的其他呼叫阻塞。注意，这不影响呼叫转发/对PSTN编号的转移到语音邮件(Cisco Unity Express)和转发所有呼叫从在CME 1的IP电话，因为初始呼叫仍然被瞄准往在CME 1.的一分机。配置示例— 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. 请使用翻译规则为了阻塞特定拨号字符串：多数长话欺骗介入国际呼叫正在拨号。结果，您能创建匹配特定被叫字符串，并且块呼叫对他们的一特定呼入拨号对端。多数CMEs使用一特定接入代码，例如9，拨出和国际电话代码在美国是011。所以，阻塞的最普通的拨号字符串在美国是9011 +在SIP中继进来的所有位以后。配置示例— 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`**

功能限制工具

转移模式

摘要

默认情况下转移到除了那些的所有编号在本地SCCP IP电话自动地阻塞。在配置时，您能允许转移到非本地号码。**转移模式**命令用于为了允许电话呼叫转移从思科SCCP IP电话到电话除思科IP电话之外，例如外部PSTN呼叫或电话在另一个CME系统。或许您能使用转移**模式**为了对仅内部分机限制呼叫或对在仅某一区域代码的PSTN编号限制呼叫。这些示例显示转移**模式**命令如何可以用于对不同的编号限制呼叫。

注意： 这是**内部威胁**。

示例 1

允许用户转接召集对仅408区域代码。在本例中，假定是CME配置与有9T目的地模式的dial-peer。

配置示例

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

阻塞的转移模式

摘要

在Cisco Unified CME 4.0及以上版本版本中，您可以从转接呼叫防止各自的电话到全局为转移启用的编号。**转移模式阻塞的**命令改写转移**模式**命令并且禁用对需要由POTS或VoIP拨号对等体到达的所有目的地的呼叫转移。这包括PSTN编号、其他语音网关和Cisco Unity Express。这保证各自的电话不导致长途话费，当呼叫Cisco Unified CME系统的外部时转接。呼叫转移阻塞可以为各自的电话配置或配置作为应用对一套电话的模板一部分。

注意： 这是**内部威胁**。

示例 1

在此配置示例中， ephone 1没有允许使用转移模式(定义全局)转移呼叫，而ephone 2能使用转移模式定义在telephony-service下转移呼叫。

配置示例

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

转移麦斯长度

摘要

转移麦斯长度命令指定用户能拨位的最大，当呼叫转接时。**转移模式麦斯长度**改写转移**模式**命令并且强制执行为转移目的地允许的最大位。参数指定在呼叫转接的编号允许的位数量。范围：3到16。默认：16.

注意： 这是**内部威胁**。

示例 1

此配置只允许有应用的此ephone模板转接到目的地是长最多四个的位的电话。

配置示例

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

呼叫向前麦斯长度

摘要

为了限制可以用在IP电话的CfwdALL软键进入位的数量，请使用**呼叫转移麦斯长度**in命令ephone-dn或ephone DN模板配置模式。为了删除在可以进入位的数量的一限制，请使用此命令**no表示**。

注意： 这是**内部威胁**。

示例 1

在本例中，目录分机101允许执行呼叫转移到是长度一个到四个位的所有分机。其中任一呼叫转发对长目的地比四个位发生故障。

配置示例

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

或

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

没有向前本地呼叫

摘要

当**向前本地呼叫**命令没有用于ephone-dn配置模式时，对一特定的ephone-dn的内部呼叫没有应用的**向前本地呼叫没有**转发，如果ephone-dn忙碌或不应答。如果一个内部呼叫方敲响此ephone-dn，并且ephone-dn忙碌，呼叫方听到占线信号。如果一个内部呼叫方敲响此ephone-dn，并且不回答，呼叫方听到回铃信号。内部呼叫没有转发，即使呼叫转接为ephone-dn启用。

注意： 这是**内部威胁**。

示例 1

在本例中，分机2222呼叫分机3675并且听到回铃或占线信号。如果外部呼叫者到达分机3675，并且没有答案，呼叫转发对分机4000。

配置示例

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

在CME系统的禁用自动注册

摘要

当自动REG **ephone**在SCCP CME系统时的telephony-service下启用，插入系统的新建的IP电话是注册的自动和，如果**自动分配**配置自动地分配分机号，然后一个新的IP电话能立即做呼叫。

注意： 这是**内部威胁**。

示例 1

在此配置中，一个新的CME系统配置，以便您必须手工添加ephone为了ephone能注册到CME系统和使用它做IP电话呼叫。

解决方案

您能禁用在telephony-service下的自动REG **ephone，**以便新的IP电话连接对CME系统没有自动寄存器到CME系统。

配置示例

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

示例 2

如果使用SCCP CME并且计划注册Cisco SIP电话到系统，您必须配置系统，以便SIP终端必须验证与用户名和密码。为了执行如此，请配置此：

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

```
authenticate register
```
参考SIP:设置更多全面配置指南的Cisco Unified CME SIP的CME。

Cisco Unity Express限制工具

安全Cisco Unity Express ：AA PSTN访问

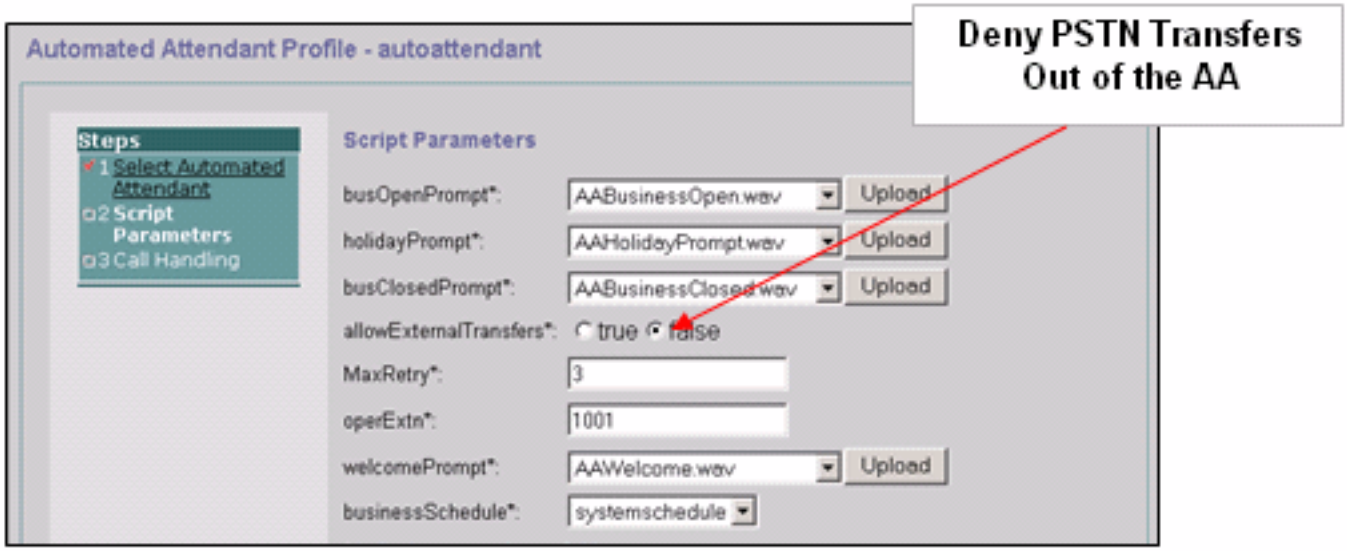
摘要

当您的系统配置时，以便呼入呼叫转发给自动总机(AA) Cisco Unity Express的，禁用外部转移到PSTN从Cisco Unity Express AA可能是必要的。在他们到达Cisco Unity Express AA后，这不允许外部用户拨号出站到外线号码。

注意： 这是一个**外部危机。**

注意： 解决方案

注意： 禁用在Cisco Unity Express GUI的**allowExternalTransfers**选项。



注意： 如果从AA的PSTN访问要求，请限制由脚本认为有效的数量或范围编号。

Cisco Unity Express限制表

摘要

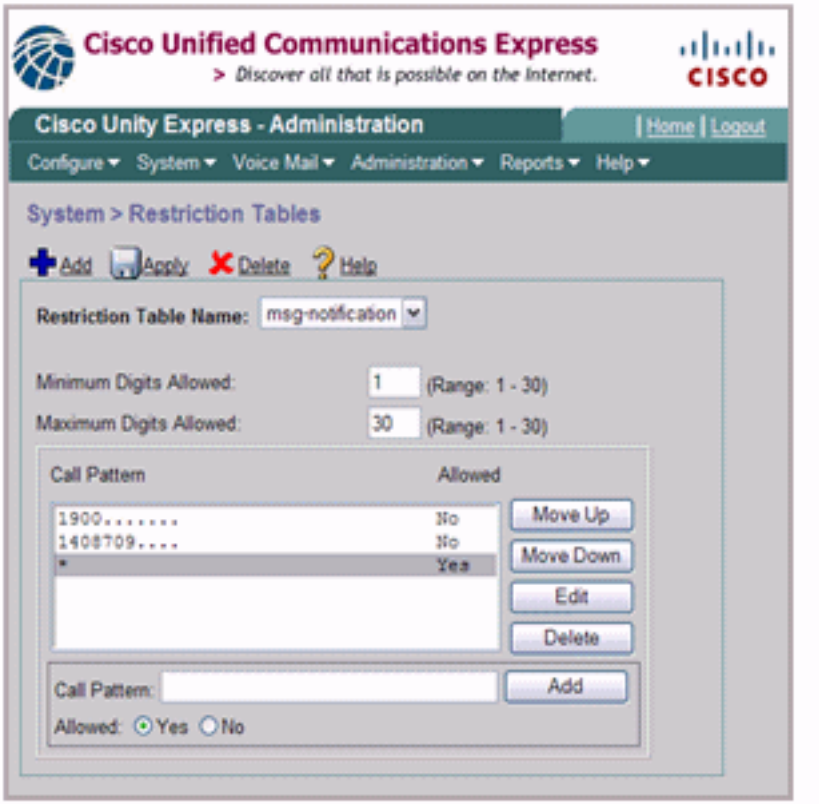
您能使用Cisco Unity Express限制表为了限制在从Cisco Unity Express的一叫牌期间可以到达的目的地。Cisco Unity Express限制表可以用于为了防止长话欺骗和恶意利用Cisco Unity Express系统做呼出。如果使用Cisco Unity Express限制表，您能指定呼叫模式到通配符匹配。使用Cisco Unity Express限制表的应用程序包括：

- 传真
- Cisco Unity Express Live重播
- 留言通知
- 非订户的消息发送

注意： 这是**内部威胁**。

解决方案

为了限制可以由在一次外部呼叫的Cisco Unity Express到达的目的地模式，请配置**呼叫模式**在**系统>**从Cisco Unity Express GUI的**限制表里**。



呼叫记录日志

增强版CDR

您能配置CME系统捕获增强版CDR和记录CDR到路由器闪存或一个外部FTP服务器。这些记录可能然后用于折回呼叫发现由内部或外部当事人的滥用是否发生。

文件记帐功能介绍与CME 4.3/7.0在Cisco IOS版本12.4(15)XY提供一个方法捕获在逗号分隔的值(.csv)格式的计费记录和存储记录到在内部闪存的一个文件或到一个外部FTP服务器。它展开网关核算支持，也包括记录日志记帐信息AAA和Syslog机制。

核算进程收集在Cisco语音网关创建的每个呼叫段的帐户数据。能使用此信息发表物处理活动例如的您生成计费记录和网络分析。Cisco语音网关包含思科定义的属性以呼叫详细记录(CDR)的形式的捕获帐户数据。网关能发送CDR到RADIUS服务器，系统日志服务器和与新的文件方法，闪烁或一个FTP服务器在.csv格式。

参考CDR示例关于增强版CDR功能的更多信息。

相关信息

- Cisco Unified Communications Manager Express安全最佳实践

- Cisco Communications Manager Express管理员指南
- Cisco Communications Manager Express管理员指南–呼叫阻塞
- 了解在IOS平台的拨号对端匹配
- 使用语音转换配置文件进行号码转换
- CME解决方案参考网络设计指南
- 技术支持和文档 - Cisco Systems