Предотвращение несанкционированного доступа к платным услугам связи Unified Communications Manager Express

Содержание

Введение

Этот документ служит руководством по конфигурации, которое призвано помочь защитить систему Cisco Communications Manager Express (CME) и свести к минимуму угрозу мошенничества в междугородных телефонных сетях. CME представляет собой систему управления вызовами на основе маршрутизатора Cisco, которая послужит интеллектуальным, простым и защищенным решением для организаций, заинтересованных во внедрении унифицированных коммуникаций. Это, настоятельно рекомендуют, чтобы вы внедрили измерения безопасности, описанные в этом документе для обеспечения

дополнительных уровней безопасности, управляют и уменьшают возможность мошенничества в междугородных телефонных сетях.

Цель этого документа состоит в том, чтобы рассказать вам о различных средствах безопасности, доступных на Голосовых шлюзах Cisco и CME. Эти программные средства могут быть внедрены в системе CME, чтобы помочь смягчать угрозу мошенничества в междугородных телефонных сетях и внутренними и третьими сторонами.

Этот документ предоставляет инструкции по тому, как настроить систему CME с различной междугородной безопасностью и программными средствами ограничения функции. Документ также выделяет, почему определенные средства безопасности используются в определенных развертываниях.

Полная свойственная гибкость платформ ISR Cisco позволяет вам развертывать CME во многих различные типы развертываний. Таким образом это может потребоваться, чтобы использовать комбинацию функций, описанных в этом документе, чтобы помочь блокировать вниз CME. Этот документ служит рекомендацией для того, как применить средства безопасности на CME и никоим образом не гарантирует, что не произойдут мошенничество в междугородных телефонных сетях или злоупотребление и внутренних и третьих сторон.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco Unified Communications Manager Express

Используемые компоненты

Сведения в этом документе основываются на Cisco Unified Communications Manager Express 4.3 и CME 7.0.

Примечание: Унифицированный CME 7.0 Cisco включает те же функции как Cisco Унифицированный CME 4.3, который перенумерован к 7.0 для выравнивания с версиями Унифицированной связи Cisco.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Обзор

Этот документ покрывает наиболее распространенные средства безопасности, которые могут использоваться в системе CME, чтобы помочь смягчать угрозу мошенничества в междугородных телефонных сетях. Средства безопасности CME, на которые ссылаются в этом документе, включают междугородные программные средства ограничения и программные средства ограничения функции.

Междугородные программные средства ограничения

- Direct-inward-dial
- Междугородное ограничение после закрытия
- Класс ограничения
- Access-list для ограничения доступа H323/МАГИСТРАЛИ SIP

Программные средства ограничения функции

- Transfer-pattern
- Transfer-pattern blocked
- Transfer max-length
- Call-forward max-length
- No forward local-calls
- No auto-reg-ephone

Программные средства ограничения Cisco Unity Express

- Безопасный доступ к тфоп Cisco Unity Express
- Ограничение уведомления о сообщении

Регистрация вызовов

- Регистрация вызовов для получения подробных записей о вызовах (CDRs)

Внутренний по сравнению с Внешние угрозы

Этот документ обсуждает угрозы и от внутренних и от третьих сторон. Внутренние стороны включают Пользователей IP-телефона, которые находятся в системе CME. Третьи стороны включают пользователей во внешних системах, которые могут попытаться использовать CME хоста, чтобы выполнить мошеннические вызовы и иметь вызовы, заряженные назад к вашей системе CME.

Междугородные программные средства ограничения

Direct-inward-dial

Краткое изложение

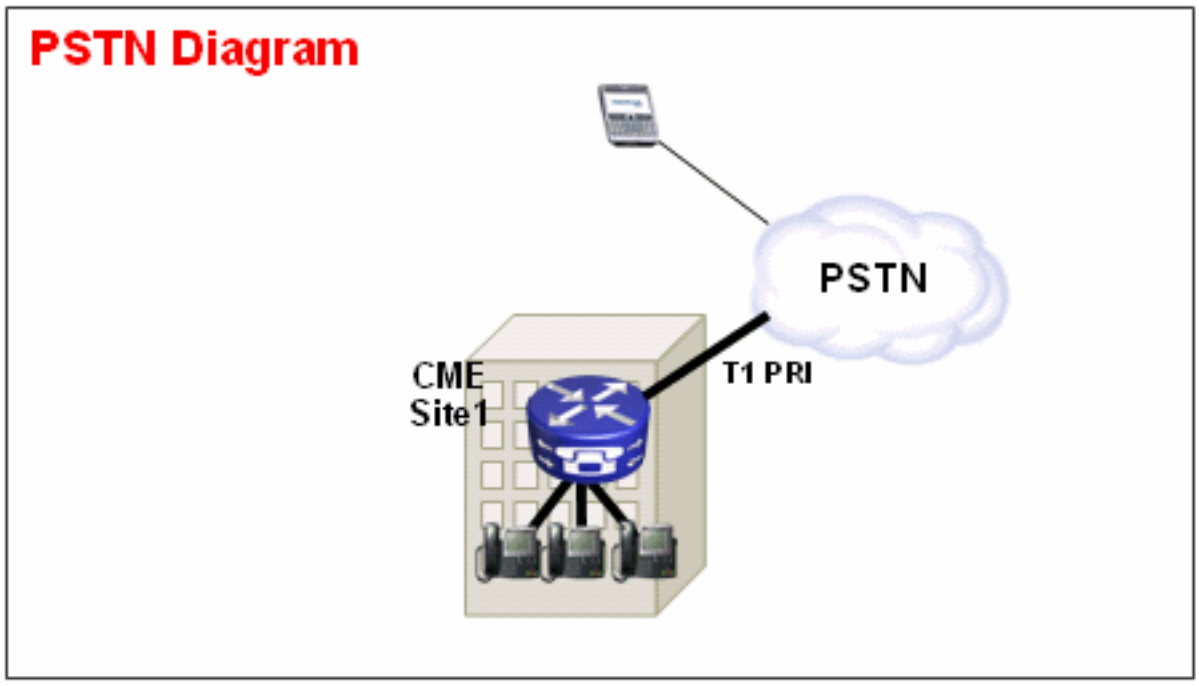
Direct-inward-dial (DID) используется на Голосовых шлюзах Cisco, чтобы позволить шлюзу обрабатывать входящий вызов после того, как это получает цифры от УАТС или

Коммутатора CO. Когда DID включен, шлюз Cisco не представляет дополнительный тональный сигнал абоненту и не ждет для сбора дополнительных цифр от абонента. Это переводит вызов непосредственно назначению, которое совпадает с входящим Dialed Number Identification Service (DNIS). Это называется одноступенчатым соединением.

Примечание: Это - **внешняя угроза**.

Постановка задачи

Если direct-inward-dial НЕ настроен на шлюзе Cisco или CME, каждый раз, когда вызов входит от CO или УАТС к шлюзу Cisco, абонент слышит дополнительный тональный сигнал. Это называют соединением в два этапа. Однажды Вызывающие абонент PSTN слышит дополнительный тональный сигнал, они в состоянии ввести цифры для достижения любого внутреннего добавочного номера или если они знают код доступа к тфоп, они могут набрать дальний или международные номера. Это представляет проблему, потому что Вызывающий абонент PSTN может использовать систему CME для размещения исходящих междугородних звонков или международных вызовов, и компания обвинена за вызовы.



Пример 1

На Узле 1, CME связан с PSTN через транк T1 PRI. Поставщик PSTN предоставляет **40855512..** Диапазон DID для Узла CME 1. Таким образом все вызовы PSTN, предназначенные для 4085551200 – 4085551299, маршрутизируются входящие к CME. Если вы не настраиваете **direct-inward-dial** в системе, входящий Вызывающий абонент PSTN слышит вторичное устройство тональный сигнал готовности линии и должен вручную набрать внутренний добавочный номер. Большая проблема состоит в том, что, если абонент является злоумышленником и знает код доступа к тфоп в системе, обычно **9**, они могут набрать **9** тогда любых назначенных номеров, которых они хотят достигнуть.

Решение 1

Для смягчения этой угрозы необходимо настроить **direct-inward-dial**. Это заставляет шлюз Cisco передавать входящий вызов непосредственно назначению, которое совпадает с

входящим DNIS.

Пример конфигурации

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

Для DID для работы правильно удостоверьтесь, что входящий вызов совпадает с верной адресуемой точкой вызова POTS, где настроена **команда direct-inward-dial**. В данном примере T1 PRI связан с портом 1/0:23. Для соответствия с корректным входящим одноранговым телефонным соединением выполните **входящую** команду точки вызова **вызванного номера** под узлом обычной телефонной сети DID.

Пример 2

На Узле 1, CME связан с PSTN через транк T1 PRI. Поставщик PSTN дает **40855512..** и **40855513..** DID располагается для Узла CME 1. Таким образом все вызовы PSTN, предназначенные для 4085551200 – 4085551299 и 4085551300 - 4085551399, маршрутизируются входящие к CME.

Некорректная конфигурация:

При настройке входящего однорангового телефонного соединения поскольку в примере конфигурации в этом разделе, все еще происходит возможность для мошенничества в междугородных телефонных сетях. Проблема с этим входящим одноранговым телефонным соединением состоит в том, что оно только совпадает с входящими вызовами к **40852512..** и затем применяет сервис DID. Если вызов PSTN входит **40852513..**, входящая точка вызова POTS не совпадает, и таким образом сервис DID не применен. Если с входящим одноранговым телефонным соединением с DID не совпадают, то одноранговое телефонное соединение по умолчанию 0 используется. DID по умолчанию отключен для адресуемой точки вызова 0.

Пример конфигурации

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

Корректная конфигурация

Правильно для настройки сервиса DID на входящем одноранговом телефонном соединении показан в данном примере:

Пример конфигурации

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

См. Конфигурацию DID для Узлов обычной телефонной сети для получения дополнительной информации о DID для цифровых голосовых портов T1/E1.

Примечание: Использование DID не необходимо, когда Автоматический вызов по звонку выделенной линии (PLAR) используется на голосовом порте, или сервисный сценарий,

такой как Автоответчик (AA) используется на входящем одноранговом телефонном соединении.

Пример конфигурации — PLAR

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

Пример конфигурации — сервисный сценарий

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

Междугородные ограничения после закрытия

Краткое изложение

Междугородное Ограничение после закрытия является новым средством безопасности, доступным в CME 4.3/7.0, который позволяет вам настраивать междугородную политику ограничения на основе времени и даты. Можно настроить политику так, чтобы пользователям не разрешали выполнить вызовы к предопределенным номерам в течение определенных часов дня или все время. Если политика блокирования вызовов после закрытия 7 дней в неделю, 24 часа в сутки настроена, она также ограничивает набор номеров, которые могут быть введены внутренним пользователем для установки **переадресации всех вызовов**.

Примечание: Это - **внутренняя угроза**.

Пример 1

Данный пример определяет несколько образцов цифр, для которых заблокированы исходящие вызовы. Образцы 1 и 2, которые блокируют вызовы к внешним номерам, которые начинаются "1" и "011", заблокированы в понедельник в течение пятницы до 7:00 и после 19:00, в субботу до 7:00 и после 13:00, и весь день в воскресенье. Образец 3 блока вызывает к 900 номерам 7 дней в неделю, 24 часа в день.

Пример конфигурации

```
 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
```

См. Блокирование вызовов Настройки для получения дополнительной информации о междугородном ограничении.

Класс ограничения

Краткое изложение

Если вы хотите гранулированный контроль при настройке междугородного ограничения необходимо использовать Класс ограничения (COR). См. Класс Ограничения: Пример для получения дополнительной информации.

H.323 / ограничения мошенничества в междугородных телефонных сетях магистралей SIP

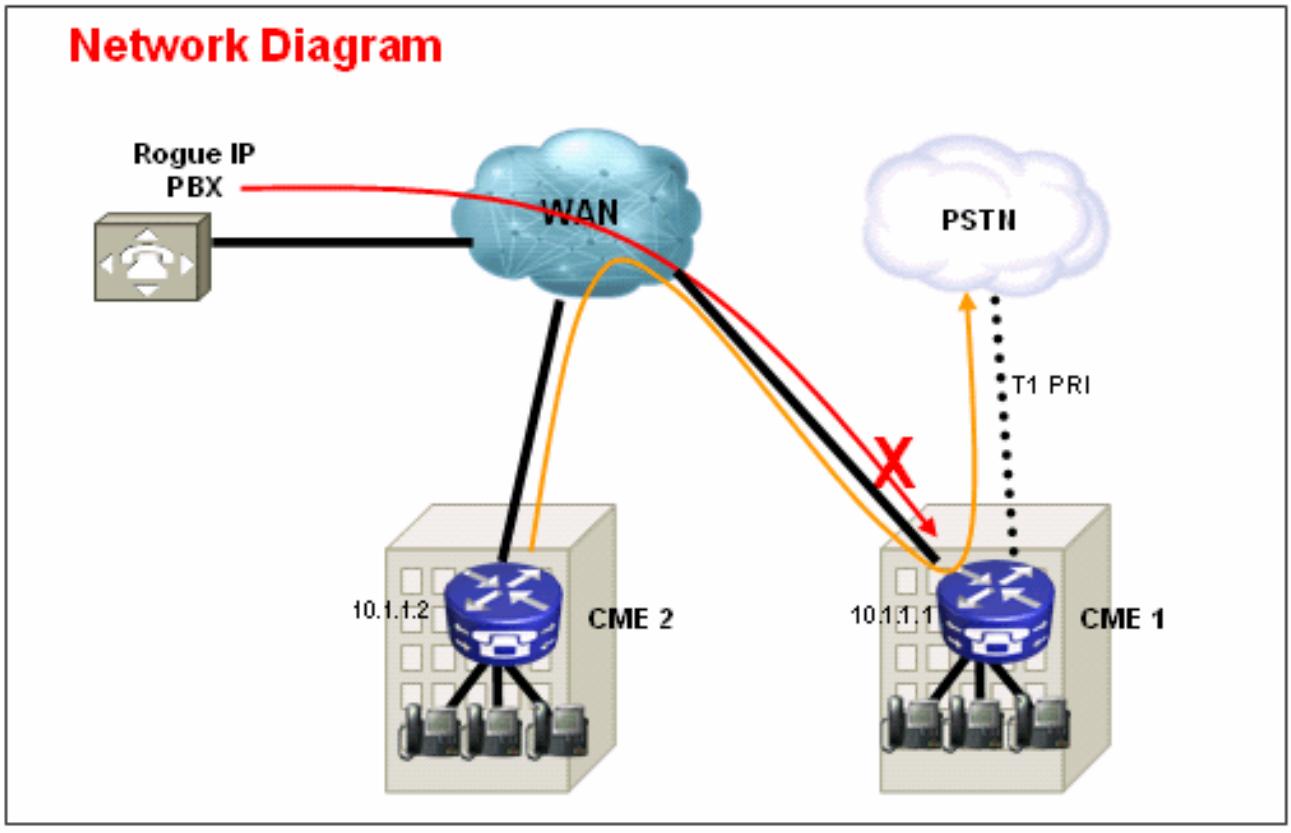
Краткое изложение

В случаях, где система CME связана по глобальной сети (WAN) с другими устройствами CME через SIP или транком H.323, можно ограничить доступ транка SIP/H.323 к CME, чтобы препятствовать тому, чтобы злоумышленники использовали систему для незаконно релейных вызовов к PSTN.

Примечание: Это - **внешняя угроза**.

Пример 1

В данном примере CME 1 имеет подключение PSTN. CME 2 связан по глобальной сети (WAN) с CME 1 через транк H.323. Для обеспечения CME 1 можно настроить access-list и применить его входящий на Интерфейс WAN и таким образом только позволить IP - трафик от CME 2. Это препятствует тому, чтобы Посторонняя УАТС IP передала вызовы VoIP через CME 1 к PSTN.



Решение

Не позволяйте Интерфейсу WAN на CME 1 принимать трафик от неконтролируемых устройств, которые это не распознает. Обратите внимание на то, что существует неявное, ЗАПРЕЩАЮТ все в конце access-list. Если существует больше устройств, от которых вы хотите позволить входящий IP - трафик, несомненно, добавят IP-адрес устройства к access-list.

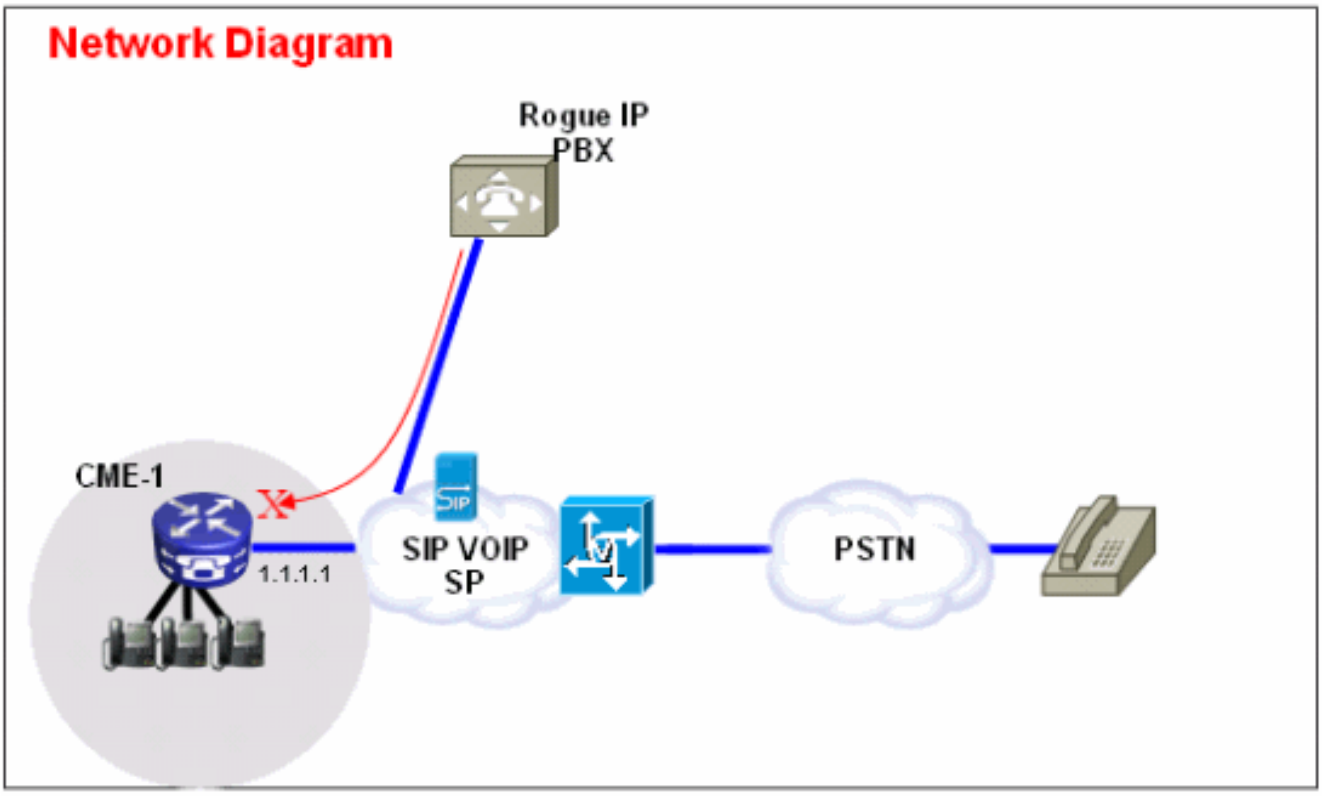
Пример конфигурации — CME 1

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

Пример 2

В данном примере CME 1 связан с поставщиком SIP для подключения PSTN с примером конфигурации, предоставленным в Cisco CallManager Express (CME) Пример Конфигурации магистрали SIP.

Так как CME 1 находится в общем Интернете, возможно, что *мошенничество в междугородных телефонных сетях* может произойти, если посторонний пользователь просматривает открытые IP - адреса для стандартных портов для H.323 (TCP 1720) или SIP (UDP или TCP 5060) сигнализация и передает SIP или сообщения H.323, что маршрут перезванивает из магистрали SIP к PSTN. Наиболее распространенные злоупотребления в этом случае являются посторонним пользователем, выполняет множественные международные вызовы через SIP или транк H.323 и заставляет владельца CME 1 платить за эти вызовы мошенничества в междугородных телефонных сетях - в некоторых случаях тысячи долларов.



Решение

Для смягчения этой угрозы можно использовать множественные решения. Если какой-либо VoIP передача сигналов (SIP или H.323) не используется по каналу (каналам) WAN в CME 1, это должно быть заблокировано со способами межсетевого экрана на CME 1 (Access-lists или ACL) так же как возможное.

1. Защитите Интерфейс WAN с межсетевым экраном Cisco IOS® на CME 1:Это подразумевает, что вы позволяете только известному SIP или трафику H.323 входить на Интерфейсе WAN. Весь другой трафик SIP или H.323 заблокирован. Это также требует, чтобы вы знали IP-адреса, которые SP VOIP SIP использует для сигнализации на магистрали SIP. Это решение предполагает, что SP готов предоставить все IP-адреса или имена DNS, которые они используют в их сети. Кроме того, если имена DNS используются, конфигурация требует, чтобы сервер DNS, который может решить эти названия, был достижим. Кроме того, если SP изменяет какие-либо адреса на их конце, конфигурация должна быть обновлена на CME 1. Обратите внимание на то, что эти линии должны быть добавлены в дополнение к любым записям ACL, уже представляют на Интерфейсе WAN.Пример конфигурации — 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. Гарантируйте вызовы, которые входят на магистрали SIP, убирают **НЕ** шпильку назад:Это подразумевает, что конфигурация CME 1 только позволяет SIP – шпилька SIP вызовов к определенному известному диапазону чисел PSTN, все другие вызовы заблокированы. Необходимо настроить определенные входящие одноранговые телефонные соединения для номеров PSTN, которые входят на магистрали SIP, которые сопоставлены с расширениями или автоответчиком (автоответчиками) или голосовой почтой на CME 1. Заблокированы все другие вызовы к номерам, которые не являются частью диапазона чисел CME 1 PSTN. Обратите внимание, это не влияет на вызов вперед / передает голосовой почте (Cisco Unity Express) и переадресация всех вызовов к номерам PSTN от IP-телефонов на CME 1, потому что первоначальный вызов все еще предназначен к расширению на CME 1.Пример конфигурации — 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. Используйте правила трансляции для блокирования определенных строк набора:Большая часть мошенничества в междугородных телефонных сетях включает набор номера международного вызова. В результате можно создать определенное входящее одноранговое телефонное соединение, которое совпадает с определенными строками набора и вызовами блоков им. Большинство CME использует определенный код доступа, такой как 9, для набора номера, и международный телефонный код в US равняется 011. Поэтому наиболее распространенная строка набора для блокирования в US 9011 +, любые цифры после этого входят на магистрали SIP.Пример конфигурации — 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
```

Программные средства ограничения функции

Образец передачи

Краткое изложение

Передачи во все номера кроме тех на локальных IP-телефонах SCCP автоматически заблокированы по умолчанию. Во время конфигурации можно позволить передачи в нелокальные номера. **Команда transfer-pattern** используется для разрешения передачи вызовов в телефонии с IP-телефонов SCCP Cisco на телефоны кроме Cisco IP Phone, таких как внешние вызовы PSTN или телефоны в другой системе CME. Можно использовать **образец передачи**, чтобы ограничить вызовы внутренними добавочными номерами только или возможно ограничить вызовы номерами PSTN в коде определенной области только. Эти примеры показывают, как **команда transfer-pattern** может использоваться для ограничения вызовов другими номерами.

Примечание: Это - **внутренняя угроза**.

Пример 1

Позвольте, что пользователи для передачи обращаются только к 408 кодам зоны. В данном примере предположение - то, что CME настроен с точкой вызова, которая имеет destination-pattern 9T.

Пример конфигурации

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

Transfer-Pattern Blocked

Краткое изложение

В Cisco Унифицированный CME 4.0 и более поздние версии, можно предотвратить индивидуальные телефоны от переводов вызова до номеров, которые глобально включены для передачи. **Команда transfer-pattern blocked** отвергает **команду transfer-pattern** и отключает передачу вызова любому назначению, которое должно быть достигнуто POTS или узлом коммутации VoIP. Это включает номера PSTN, другие голосовые шлюзы и Cisco Unity Express. Это гарантирует, что индивидуальные телефоны не подвергаются платам за телефонный вызов, когда вызовы переданы за пределами Cisco Унифицированная система CME. Блокирование передачи вызова может быть настроено для индивидуальных телефонов или настроено как часть шаблона, который применен к ряду телефонов.

Примечание: Это - **внутренняя угроза**.

Пример 1

В то время как ephone 2 может использовать образец передачи, определенный под telephony-service для передачи вызовов, в этом примере конфигурации ephone 1 не позволяют использовать образец передачи (определенный глобально) для передачи вызовов.

Пример конфигурации

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

Transfer max-length

Краткое изложение

Команда transfer max-length задает максимальное число цифр, которые может набрать пользователь, когда передан вызов. **Max. длина образца передачи** отвергает **команду transfer-pattern** и принуждает максимальные цифры, обеспечил адресата переадресации. Аргумент задает количество цифр, позволенных в номере, которому передан вызов. Диапазон: 3 - 16. По умолчанию: 16.

Примечание: Это - **внутренняя угроза**.

Пример 1

Эта конфигурация только позволяет телефоны, которым применили этот шаблон ephone, чтобы передать назначениям, которые являются максимумом четырех цифр долго.

Пример конфигурации

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

Max. длина Переадресации вызовов

Краткое изложение

Для ограничения количества цифр, которые могут быть введены с программируемой клавишей CfwdALL на IP-телефоне, использовать **команду call-forward max-length** в режиме конфигурации шаблона ephone-dn или ephone-dn. Для удаления ограничения на количество цифр, которые могут быть введены, использовать **эту команду с параметром no**.

Примечание: Это - **внутренняя угроза**.

Пример 1

В данном примере расширению каталога 101 позволяют выполнить переадресацию вызовов к любому расширению, которое является одной - четырьмя цифрами в длине. Любой вызов

вперед назначениям дольше, чем четыре сбоя цифр.

Пример конфигурации

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

или

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

Нет переведите локальный вызов

Краткое изложение

Когда **команда no forward local-calls** используется в режиме конфигурации ephone-dn, внутренние вызовы к определенному ephone-dn **без прямых** примененных **локальных вызовов** не переданы, если ephone-dn занят или не отвечает. Если внутренний вызывающий абонент звонит на этого ephone-dn, и ephone-dn занят, абонент слышит сигнал занято. Если внутренний вызывающий абонент звонит на этого ephone-dn, и он не отвечает, абонент слышит, что сигнализирует обратный вызов. Даже если переадресация вызовов включена для ephone-dn, внутренний вызов не передан.

Примечание: Это - **внутренняя угроза**.

Пример 1

В данном примере, расширение 2222 расширения вызовов 3675 и слышит обратный вызов или сигнал занято. Если внешняя вызывающая программа достигает расширения 3675 и никто не отвечает, вызов переведен к расширению 4000.

Пример конфигурации

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

Отключите авторегистрацию в системе CME

Краткое изложение

То, когда **auto-reg-ephone** включают нижний telephony-service в системе CME SCCP, новые IP-телефоны, которые включены, система автоматическая зарегистрированный и, если **автоматический назначает**, настроено для автоматического присвоения добавочных номеров, тогда новый IP-телефон в состоянии выполнить вызовы сразу.

Примечание: Это - **внутренняя угроза**.

Пример 1

В этой конфигурации настроена новая система CME так, чтобы вы вручную добавили

ephone для ephone, чтобы зарегистрироваться к системе CME и использовать его для совершения вызовов IP-телефонии.

Решение

Можно отключить **auto-reg-ephone** под telephony-service так, чтобы новые IP-телефоны, связанные с системой CME, не делали автоматического регистра к системе CME.

Пример конфигурации

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

Пример 2

При использовании CME SCCP и планируете зарегистрировать телефоны Cisco SIP к системе, необходимо настроить систему так, чтобы оконечные точки SIP аутентифицировались с именем пользователя и паролем. В заказе для этого просто настраивают это:

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

См. SIP: Устанавливание Cisco Унифицированный CME для большего количества руководства комплексной конфигурации для CME SIP.

Программные средства ограничения Cisco Unity Express

Безопасный Cisco Unity Express: доступ к тфоп AA

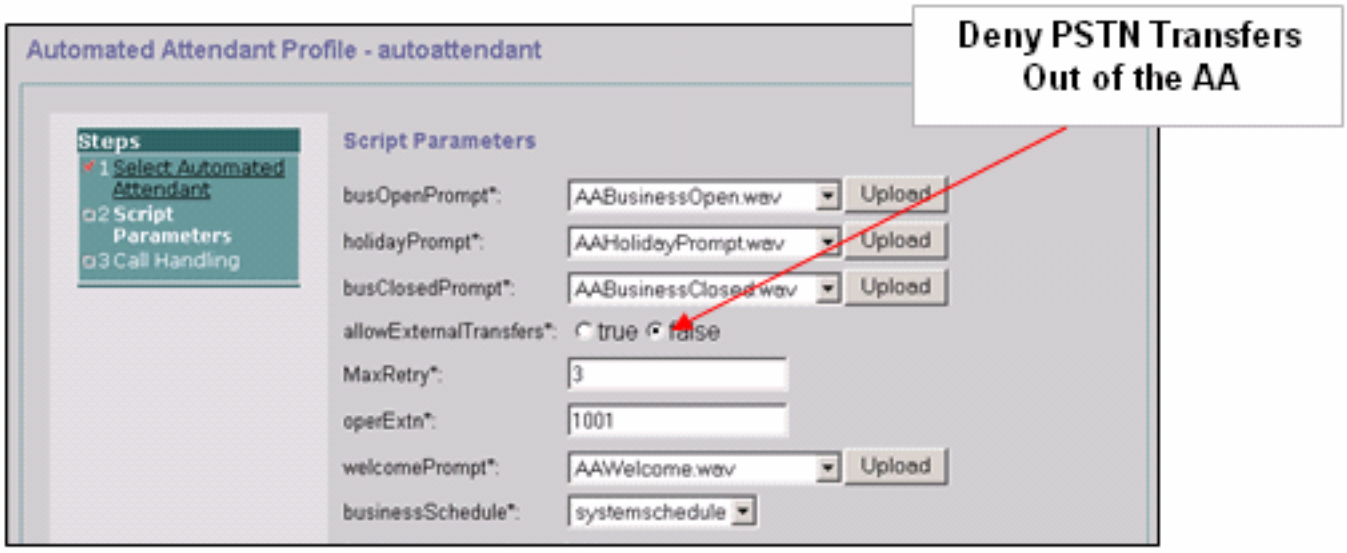
Краткое изложение

Когда ваша система настроена так, чтобы входящие вызовы были переданы автоответчику (AA) на Cisco Unity Express, может быть необходимо отключить внешнюю передачу в PSTN от AA Cisco Unity Express. Это не позволяет внешним пользователям набирать исходящий к внешним номерам после того, как они достигнут AA Cisco Unity Express.

Примечание: Это - **внешняя угроза**.

Примечание: Решение

Примечание: Отключите **allowExternalTransfers** опцию на GUI Cisco Unity Express.



Примечание: Если доступ к тфоп от AA требуется, ограничьте номера или диапазон номеров, которые считает допустимыми сценарий.

Таблицы ограничений Cisco Unity Express

Краткое изложение

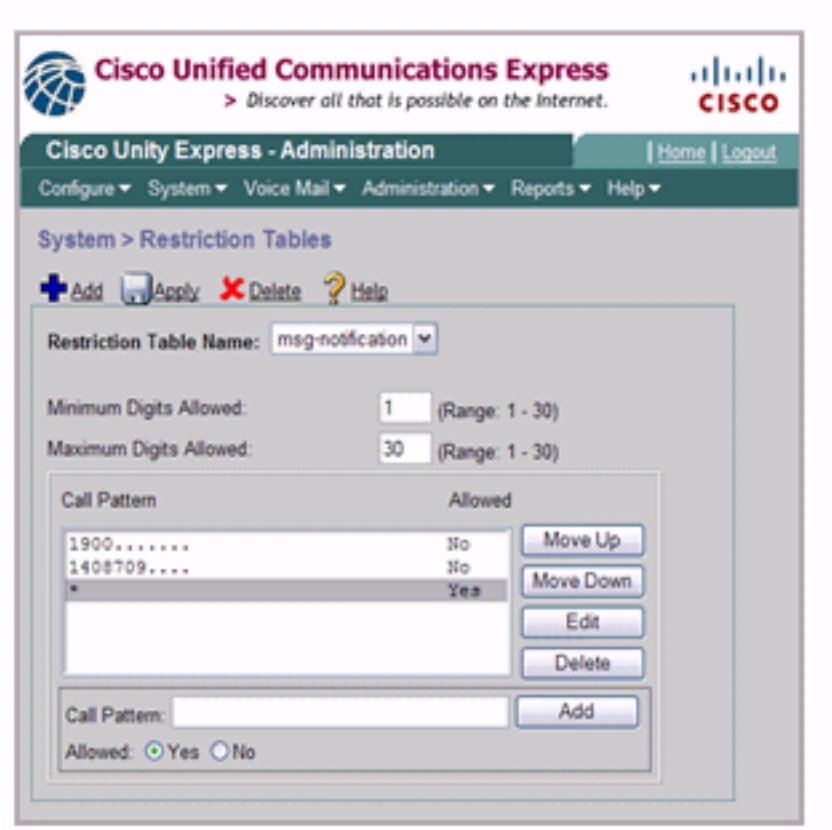
Можно использовать таблицы ограничений Cisco Unity Express для ограничения назначений, которые могут быть достигнуты во время вызова на дом от Cisco Unity Express. Таблица ограничений Cisco Unity Express может использоваться для предотвращения мошенничества в междугородных телефонных сетях и злонамеренного использования системы Cisco Unity Express для создания исходящих вызовов. При использовании таблицы ограничений Cisco Unity Express можно задать образцы вызова к соответствию подстановочного знака. Приложения, которые используют таблицу ограничений Cisco Unity Express, включают:

- Факс
- Cisco Unity Express оперативное воспроизведение
- Message Notification (Уведомление о сообщении)
- Доставка сообщения неабонента

Примечание: Это - **внутренняя угроза**.

Решение

Для ограничения шаблонов назначения, которые могут быть достигнуты Cisco Unity Express на исходящем внешнем вызове, настроить **Образец Вызова** в **Системе> Таблицы Ограничений** от GUI Cisco Unity Express.



Регистрация вызовов

Расширенный CDR

Можно настроить систему CME, чтобы перехватить улучшенный CDR и регистрировать CDR к флэшу - памяти маршрутизатора или внешнему серверу FTP. Эти записи могут тогда использоваться для восстановления вызовов видеть, произошло ли злоупотребление внутренних или третьих сторон.

Функция учета файла, начатая с CME 4.3/7.0 в Cisco IOS Release 12.4 (15) XY, предоставляет метод, чтобы перехватить учетные записи в отделенном запятой значении (.csv) формат и сохранить записи на файл во внутренней флэш - памяти или к внешнему серверу FTP. Это разворачивает поддержку учета шлюза, которая также включает AAA и механизмы системного журнала регистрации учетной информации.

Бухгалтерский процесс собирает учетные данные для каждой ветви вызовов, созданной на Голосовом шлюзе Cisco. Можно использовать эту информацию для действий обработки поста, например, для генерации записей информации для выставления счетов и для анализа сети. Голосовые шлюзы Cisco перехватывают учетные данные в форме подробных записей о вызовах (CDRs), который содержит атрибуты, определенные Cisco. Шлюз может передать CDRs к серверу RADIUS, серверу системного журнала, и с новым методом файла, для мигания или сервер FTP в формате .csv.

См. Примеры CDR для получения дополнительной информации о Расширенных возможностях CDR.

Дополнительные сведения

- Оптимальные методы безопасности Cisco Unified Communications Manager Express
- Руководство администратора Cisco Communications Manager Express
- Руководство администратора Cisco Communications Manager Express – блокирование вызовов
- Понимание Соответствия при одноранговом телефонном соединении на платформах IOS
- Преобразование номеров с использованием профилей преобразования голосовых данных
- Ссылочное руководство по организации сети решения для CME
- Cisco Systems – техническая поддержка и документация