Unified Communications Manager Express 요금 사기 방지

목차

소개

이 문서에서는 Cisco CME(Communications Manager Express) 시스템을 보호하고 유료 사기 위협을 완화하기 위해 사용할 수 있는 컨피그레이션 가이드를 제공합니다.CME는 Cisco의 라우터 기반 통화 제어 솔루션으로, Unified Communications를 구현하려는 조직에 스마트하고 간단하며 안전한 솔루션을 제공합니다.추가적인 보안 제어 수준을 제공하고 유료 사기 가능성을 줄이려면 이 문서에 설명된 보안 조치를 구현하는 것이 좋습니다.

이 문서의 목적은 Cisco Voice Gateways 및 CME에서 사용할 수 있는 다양한 보안 툴에 대해 설명하는 것입니다.이러한 툴을 CME 시스템에 구현하여 내부 및 외부 당사자의 요금 사기 위협을 완화할 수 있습니다.

이 문서에서는 다양한 유료 보안 및 기능 제한 툴을 사용하여 CME 시스템을 구성하는 방법에 대한 지침을 제공합니다.또한 특정 구축에서 특정 보안 툴을 사용하는 이유에 대해서도 설명합니다.

Cisco ISR 플랫폼의 전반적인 기본 유연성을 통해 다양한 구축 유형에 CME를 구축할 수 있습니다 .따라서 CME를 잠그기 위해 이 문서에 설명된 기능의 조합을 사용해야 할 수 있습니다.이 문서는 CME에 보안 툴을 적용하는 방법에 대한 지침으로 사용되며, 내부 및 외부 당사자에 의한 요금 사기 또는 남용이 발생하지 않도록 보증하지 않습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Unified Communications Manager Express

사용되는 구성 요소

이 문서의 정보는 Cisco Unified Communications Manager Express 4.3 및 CME 7.0을 기반으로 합니다.

참고: Cisco Unified CME 7.0에는 Cisco Unified CME 4.3과 동일한 기능이 포함되어 있으며, Cisco Unified Communications 버전에 맞게 7.0으로 번호가 다시 매겨집니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

개요

이 문서에서는 유료 사기 위협을 완화하기 위해 CME 시스템에서 사용할 수 있는 가장 일반적인 보안 툴을 다룹니다.이 문서에서 참조하는 CME 보안 툴에는 유료 제한 툴 및 기능 제한 툴이 포함되어 있습니다.

유료 제한 툴

- 직접 안쪽으로 다이얼
- 시간 후 유료 전화 제한
- 제한 등급
- H323/SIP 트렁크 액세스를 제한하는 액세스 목록

기능 제한 도구

- 전송 패턴

- 전송 패턴 차단됨
- 전송 최대 길이
- 통화 착신 전환 최대 길이
- 착신 전환 로컬 통화 없음
- 자동 등록 전화 없음

Cisco Unity Express 제한 툴

- Cisco Unity Express PSTN 액세스 보안
- 메시지 알림 제한

통화 로깅

- CDR(Call Detail Record)을 캡처하기 위한 통화 로깅

내부 및 외부 위협 비교

이 문서에서는 내부 및 외부 당사자의 위협에 대해 설명합니다.내부 대상에는 CME 시스템에 상주하는 IP 전화 사용자가 포함됩니다.외부 대상에는 호스트 CME를 사용하여 사기성 전화를 걸거나 CME 시스템에 다시 걸려온 통화를 받을 수 있는 외부 시스템의 사용자가 포함됩니다.

유료 제한 툴

직접 안쪽으로 다이얼

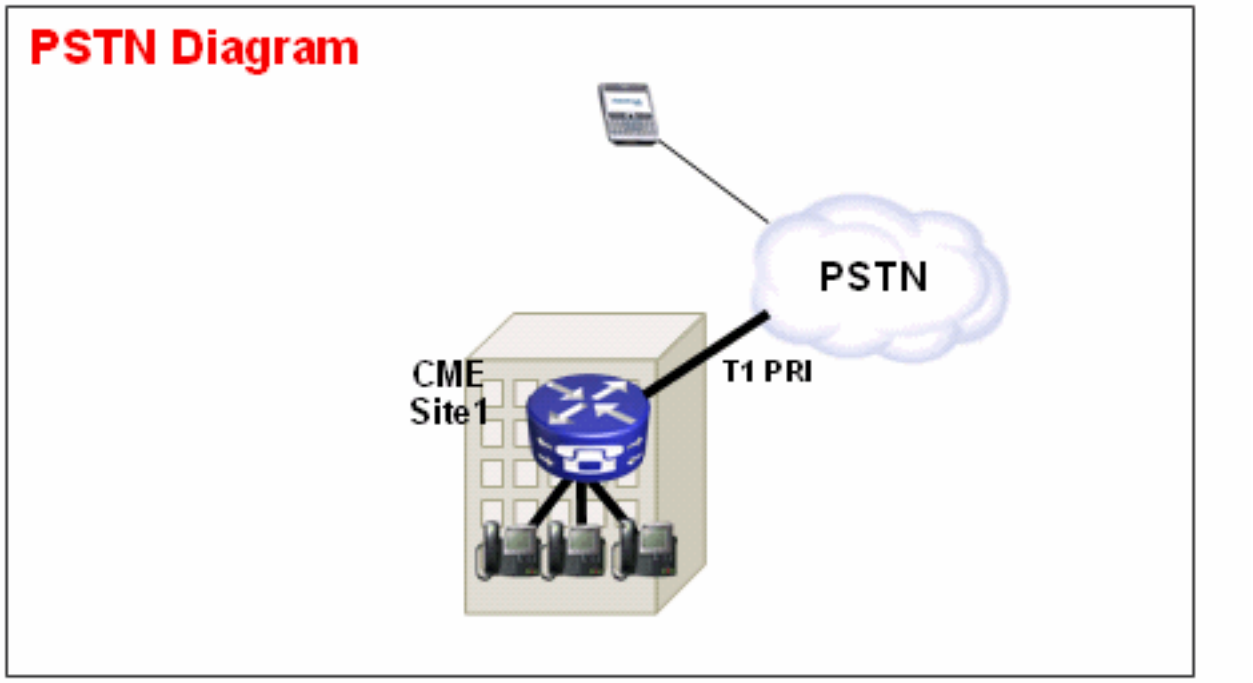
요약

PBX 또는 CO 스위치에서 번호를 수신한 후 게이트웨이가 인바운드 통화를 처리할 수 있도록 Cisco 음성 게이트웨이에서 DID(Direct-Inward-Dial)를 사용합니다.DID가 활성화된 경우 Cisco 게이트웨이는 발신자에게 보조 신호음을 표시하지 않으며 발신자로부터 추가 숫자를 수집할 때까지 기다리지 않습니다.수신 전화 건 번호 식별 서비스(DNIS)와 일치하는 대상에 통화를 직접 전달합니다. 이를 1단계 다이얼링이라고 합니다.

참고: 이는 **외부 위협**입니다.

문제 설명

Cisco 게이트웨이 또는 CME에 다이렉트-인사이드 다이얼이 구성되지 않은 경우, CO 또는 PBX에서 Cisco 게이트웨이로 통화가 수신될 때마다 발신자는 2차 다이얼톤을 듣습니다.이를 2단계 다이얼링이라고 합니다.PSTN 발신자가 2차 신호음을 듣고 나면 번호를 입력하여 내부 내선에 연결하거나 PSTN 액세스 코드를 알고 있으면 장거리 또는 국제 번호로 전화를 걸 수 있습니다.이는 PSTN 발신자가 CME 시스템을 사용하여 아웃바운드 장거리 또는 국제 전화를 걸 수 있으며 회사에서 통화에 대해 요금을 부과하기 때문에 문제가 됩니다.



예 1

사이트 1에서 CME는 T1 PRI 트렁크를 통해 PSTN에 연결됩니다.PSTN 공급자는 **40855512**를 제공합니다.CME 사이트 1의 DID 범위. 따라서 4085551200 - 4085551299로 향하는 모든 PSTN 통화는 CME로 인바운드됩니다.시스템에서 **직접** 내부 **다이얼을** 구성하지 않으면 인바운드 PSTN 호출자가 보조 다이얼톤을 듣고 내부 내선 번호를 수동으로 다이얼해야 합니다.더 큰 문제는 발신자가 abuser이고 시스템의 PSTN 액세스 코드(일반적으로 **9**)를 알고 있는 경우, **9**를 누른 다음 원하는 목적지 번호로 전화를 걸 수 있다는 것입니다.

솔루션 1

이 위협을 완화하려면 **직접** 내부 **다이얼을 구성해야** 합니다.그러면 Cisco 게이트웨이가 인바운드 통화를 인바운드 DNIS와 일치하는 대상으로 직접 착신 전환합니다.

샘플 컨피그레이션

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

DID가 올바르게 작동하려면 인바운드 통화가 **직접** 안쪽으로 다이얼 명령이 구성된 올바른 POTS 다이얼 피어와 일치하는지 확인합니다.이 예에서 T1 PRI는 포트 1/0:23에 연결됩니다. 올바른 인바운드 다이얼 피어와 일치시키려면 DID POTS 다이얼 피어 아래에서 **수신**의 **called-number** dial peer 명령을 실행합니다.

예 2

사이트 1에서 CME는 T1 PRI 트렁크를 통해 PSTN에 연결됩니다.PSTN 공급자는 **40855512.** 및 **40855513을 제공합니다.**CME 사이트 1에 대한 DID 범위. 따라서 4085551200 - 4085551299 및 408551300 - 408551399로 향하는 모든 PSTN 통화는 CME로 라우팅됩니다.

잘못된 구성:

이 섹션의 샘플 컨피그레이션과 같이 인바운드 다이얼 피어를 구성하는 경우 유료 사기 가능성은 계속 발생합니다.이 인바운드 다이얼 피어의 문제는 이 피어가 **40852512**로의 인바운드 통화만 **일치시킨** 다음 DID 서비스를 적용한다는 것입니다.PSTN 통화가 **40852513.**로 들어오는 경우 인바운드 포트 다이얼 피어가 일치하지 않으므로 DID 서비스가 적용되지 않습니다.DID를 사용하는 인바운드 다이얼 피어가 일치하지 않으면 기본 다이얼 피어 0이 사용됩니다.DID는 다이얼 피어 0에서 기본적으로 비활성화되어 있습니다.

샘플 컨피그레이션

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

올바른 구성

인바운드 다이얼 피어에서 DID 서비스를 구성하는 올바른 방법은 다음 예에 나와 있습니다.

샘플 컨피그레이션

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

디지털 T1/E1 음성 포트의 DID에 대한 자세한 내용은 POTS 다이얼 피어용 DID 컨피그레이션을 참조하십시오.

참고: PLAR(Private-Line Automatic Ringdown)이 음성 포트 또는 AA(Auto-Attendant)와 같은 서비스 스크립트를 인바운드 다이얼 피어에서 사용하는 경우에는 DID를 사용할 필요가 없습니다.

샘플 컨피그레이션 - PLAR

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

샘플 컨피그레이션 - 서비스 스크립트

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

근무 시간 후 요금 제한

요약

CME 4.3/7.0에서 사용할 수 있는 새로운 보안 툴인 After-hours Toll Restriction을 사용하면 시간과 날짜를 기준으로 요금 제한 정책을 구성할 수 있습니다.사용자가 하루 중 특정 시간 또는 하루 종일 미리 정의된 번호로 전화를 걸 수 없도록 정책을 구성할 수 있습니다.7x24 통화 후 차단 정책이 구성된 경우 내부 사용자가 입력할 수 있는 번호 집합을 **모두**로 **착신 전환**을 설정하도록 제한합니다.

참고: 이는 **내부 위협**입니다.

예 1

이 예에서는 아웃바운드 통화가 차단되는 몇 가지 숫자 패턴을 정의합니다."1"과 "011"으로 시작하는 외부 번호로 거는 전화를 차단하는 패턴 1과 2는 월요일부터 금요일, 오전 7시 전, 그리고 오후 7시 이후, 토요일 오전 7시 전, 오후 1시 이후, 일요일 낮에 모두 차단됩니다.패턴 3은 하루 24시간 주 7일 900 번호로 통화를 차단합니다.

샘플 컨피그레이션

```
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
```

요금 제한에 대한 자세한 내용은 통화 차단 구성을 참조하십시오.

제한 등급

요약

요금 제한을 구성할 때 세분화된 제어를 원하는 경우 COR(Class of Restriction)을 사용해야 합니다. 제한 클래스 참조:자세한 내용은 예를 참조하십시오.

H.323 / SIP 트렁크 요금 사기 제한

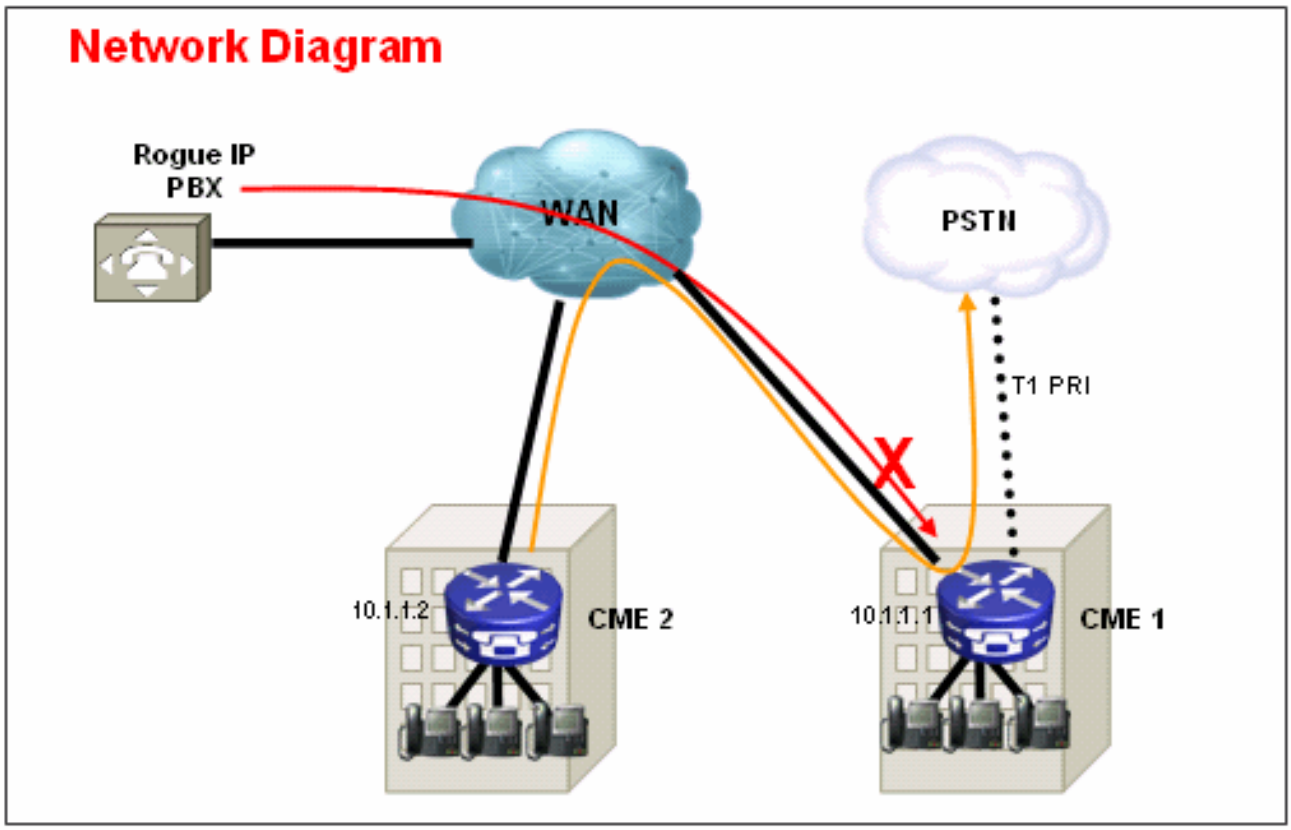
요약

CME 시스템이 SIP 또는 H.323 트렁크를 통해 WAN을 통해 다른 CME 디바이스로 연결되는 경우, CME에 대한 SIP/H.323 트렁크 액세스를 제한하여 사용자가 시스템을 사용하여 PSTN으로 통화를 불법으로 릴레이하지 못하도록 할 수 있습니다.

참고: 이는 **외부 위협**입니다.

예 1

이 예에서는 CME 1에 PSTN 연결이 있습니다.CME 2는 H.323 트렁크를 통해 WAN을 통해 CME 1에 연결됩니다.CME 1을 보호하기 위해 액세스 목록을 구성하고 WAN 인터페이스에 이를 적용하여 CME 2의 IP 트래픽만 허용할 수 있습니다. 이렇게 하면 비인가 IP PBX가 CME 1을 통해 PSTN으로 VOIP 통화를 보내지 않습니다.



솔루션

CME 1의 WAN 인터페이스에서 인식되지 않는 비인가 디바이스의 트래픽을 수락하도록 허용하지 마십시오.액세스 목록의 끝에 암시적 DENY all이 있습니다.인바운드 IP 트래픽을 허용할 디바이스가 더 많은 경우 디바이스의 IP 주소를 액세스 목록에 추가해야 합니다.

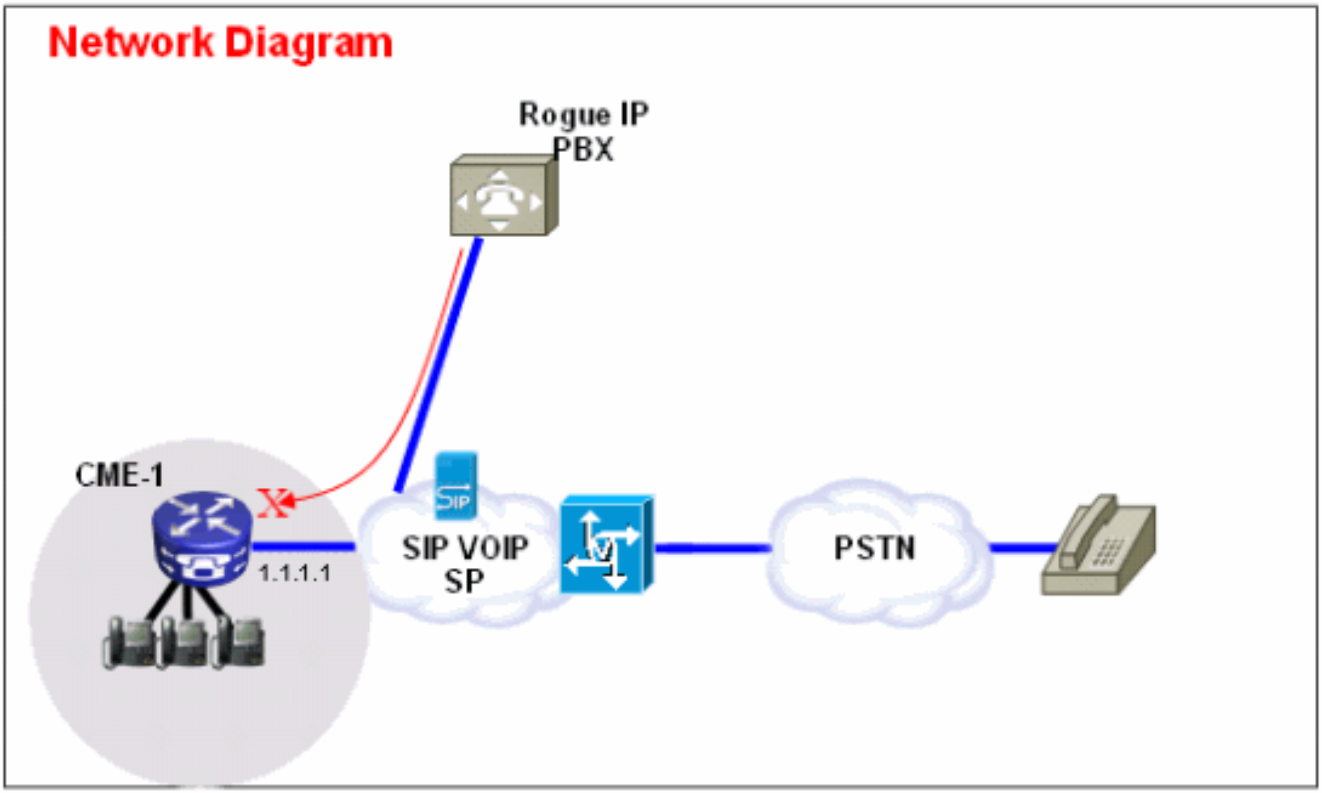
샘플 컨피그레이션 - CME 1

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

예 2

이 예에서 CME 1은 Cisco CME(CallManager Express) SIP 트렁킹 컨피그레이션 예에서 제공하는 샘플 컨피그레이션과 PSTN 연결을 위한 SIP 공급자에 연결됩니다.

CME 1은 공용 인터넷에 있으므로, 비인가 사용자가 H.323(TCP 1720) 또는 SIP(UDP 또는 TCP 5060) 신호 처리를 위해 공용 IP 주소를 스캔하고 SIP 트렁크에서 PSTN으로 다시 전화를 거는 SIP 또는 H.323 메시지를 보낼 경우 *요금 사기가* 발생할 수 있습니다.이 경우 가장 일반적인 악용 사례는 비인가 사용자가 SIP 또는 H.323 트렁크를 통해 여러 국제 전화를 걸며 CME 1의 소유주가 이러한 유료 사기 전화 비용을 지불하도록 하는 것입니다. 경우에 따라 수천 달러가 듭니다.



솔루션

이러한 위협을 완화하기 위해 여러 솔루션을 사용할 수 있습니다.CME 1에 대한 WAN 링크를 통해 VOIP 신호(SIP 또는 H.323)를 사용하지 않는 경우 CME 1(액세스 목록 또는 ACL)의 방화벽 기술로 최대한 차단해야 합니다.

1. CME 1의 Cisco IOS® 방화벽으로 WAN 인터페이스를 보호합니다.이는 알려진 SIP 또는 H.323 트래픽만 WAN 인터페이스에 들어오는 것을 허용함을 의미합니다.다른 모든 SIP 또는 H.323 트래픽은 차단됩니다.또한 SIP VOIP SP가 SIP 트렁크에서 신호를 보내는 데 사용하는 IP 주소를 알고 있어야 합니다.이 솔루션은 SP가 네트워크에서 사용하는 모든 IP 주소 또는 DNS 이름을 제공한다고 가정합니다.또한 DNS 이름을 사용하는 경우, 이러한 이름을 확인할 수 있는 DNS 서버에 연결할 수 있어야 합니다.또한 SP가 끝에 있는 주소를 변경할 경우 CME 1에서 구성을 업데이트해야 합니다. WAN 인터페이스에 이미 있는 ACL 항목 외에 이러한 행을 추가해야 합니다.샘플 컨피그레이션 - 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. SIP 트렁크에 걸려온 통화가 헤어핀을 해제하지 않는지 확인합니다.이는 CME 1 컨피그레이션에서 알려진 특정 PSTN 번호 범위에 대한 통화의 SIP - SIP 헤어핀만 허용하고 다른 모든 통화는 차단됨을 의미합니다.CME 1의 내선 번호나 자동 전화 교환이나 음성 메일에 매핑된 SIP 트렁크에 들어오는 PSTN 번호에 대해 특정 인바운드 다이얼 피어를 구성해야 합니다. CME 1 PSTN 번호 범위에 속하지 않는 다른 모든 번호 통화는 차단됩니다.초기 통화는 여전히 CME 1의 내선 번호로 지정되어 있으므로, 이는 통화 착신 전환/음성 메일로 전송(Cisco Unity Express) 및 CME 1의 IP 전화기에서 PSTN 번호로 모두 착신 전환에는 영향을 미치지 않습니다.샘플 컨피그레이션 - 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. 특정 다이얼 문자열을 차단하려면 변환 규칙을 사용합니다.대부분의 유료 전화기는 국제 전화 통화와 관련이 있습니다.따라서 특정 전화 건 문자열과 일치하는 특정 인바운드 다이얼 피어를 생성하고 그에 대한 통화를 차단할 수 있습니다.대부분의 CME는 9와 같은 특정 액세스 코드를 사용하여 전화를 걸며 미국의 국제 전화 번호는 011입니다. 따라서 미국에서 가장 일반적인 전화 걸기 문자열은 9011 + SIP 트렁크에 들어 오는 모든 숫자입니다.샘플 컨피그레이션 - 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
```

기능 제한 도구

전송 패턴

요약

로컬 SCCP IP 전화기의 번호를 제외한 모든 번호로 전송되는 것은 기본적으로 자동으로 차단됩니다.컨피그레이션 중에 비로컬 번호로 전송을 허용할 수 있습니다.transfer-**pattern** 명령은 Cisco SCCP IP 전화에서 Cisco IP Phone이 아닌 다른 CME 시스템의 외부 PSTN 통화나 전화기 등의 전화기로 텔레포니 통화를 전송할 수 있도록 하는 데 사용됩니다.**이전 패턴**을 사용하여 내부 내선 번호로만 통화를 제한하거나 특정 지역 번호에서만 통화를 PSTN 번호로 제한할 수 있습니다.다음 예에서는 **transfer-pattern** 명령을 사용하여 통화를 다른 번호로 제한하는 방법을 보여 줍니다.

참고: 이는 **내부 위협**입니다.

예 1

사용자가 408 지역 번호로만 통화를 전송할 수 있습니다.이 예에서 CME는 목적지 패턴이 9T인 다이얼 피어로 구성되었다고 가정합니다.

샘플 컨피그레이션

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

전송 패턴 차단됨

요약

Cisco Unified CME 4.0 이상 버전에서는 개별 전화기가 전송을 위해 전역으로 활성화된 번호로 통화를 전송하지 못하도록 할 수 있습니다.transfer-**pattern blocked** 명령은 **transfer-pattern** 명령을 오버라이드하고 POTS 또는 VoIP 다이얼 피어에 의해 도달해야 하는 대상으로의 통화 전송을 비활성화합니다.여기에는 PSTN 번호, 기타 음성 게이트웨이 및 Cisco Unity Express가 포함됩니다.이렇게 하면 Cisco Unified CME 시스템 외부로 통화가 전송될 때 개별 전화기에 유료 요금이 부과되지 않습니다.개별 전화기에 대해 통화 호전환 차단을 구성하거나 전화기 집합에 적용되는 템플릿의 일부로 구성할 수 있습니다.

참고: 이는 **내부 위협**입니다.

예 1

이 샘플 컨피그레이션에서는 전화 1이 통화를 호전환하는 데 호전환 패턴(전역적으로 정의됨)을 사용할 수 없으며, 전화기 2는 전화 통신 서비스 아래에 정의된 호전환 패턴을 사용하여 통화를 호전환할 수 있습니다.

샘플 컨피그레이션

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

전송 최대 길이

요약

transfer **max-length** 명령은 통화가 전송될 때 사용자가 전화를 걸 수 있는 최대 자릿수를 지정합니다.transfer-**pattern max-length** over-rides **transfer-pattern** 명령을 사용하고 전송 대상에 허용되는 최대 숫자를 적용합니다.인수는 통화가 전송되는 번호에 허용되는 자릿수를 지정합니다.범위:3~16. 기본값:16.

참고: 이는 **내부 위협**입니다.

예 1

이 컨피그레이션에서는 이 전화기 템플릿이 적용된 전화기만 최대 4자리 길이의 대상으로 전송할 수 있습니다.

샘플 컨피그레이션

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

통화 착신 전환 최대 길이

요약

IP 전화의 CfwdALL 소프트 키로 입력할 수 있는 자릿수를 제한하려면 ephone-dn 또는 ephone-dn-template 컨피그레이션 모드에서 **call-forward max-length** 명령을 사용합니다.입력할 수 있는 자릿수에 대한 제한을 제거하려면 이 명령의 **no** 형식을 사용합니다.

참고: 이는 **내부 위협**입니다.

예 1

이 예에서 디렉터리 내선 번호 101은 길이가 1에서 4자리인 내선 번호로 착신 전환을 수행할 수 있습니다.4자리 이상의 대상에 대한 모든 통화 착신 전환이 실패합니다.

샘플 컨피그레이션

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

또는

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

착신 전환 로컬 통화 없음

요약

no forward local-calls 명령을 ephone-dn 컨피그레이션 모드에서 사용할 경우 **착신 전환 로컬 통화**가 적용되지 않은 특정 phone-dn에 대한 내부 통화는 phone-dn이 사용 중이거나 응답하지 않을 경우 전달되지 않습니다.내부 발신자가 이 phone-dn에 전화를 걸며 ephone-dn이 사용 중인 경우 통화자는 통화 중 신호를 수신합니다.내부 발신자가 이 전화-dn에 전화를 걸어도 응답이 없으면 발신자는 벨소리 수신 신호를 수신합니다.ephone-dn에 대해 통화 착신 전환이 활성화된 경우에도 내부 통화가 전달되지 않습니다.

참고: 이는 **내부 위협**입니다.

예 1

이 예에서 내선 번호 2222는 내선 번호 3675를 호출하고 벨소리 재생이나 통화 중 신호를 수신합니다.외부 발신자가 내선 번호 3675에 도달했지만 응답이 없으면 통화가 내선 번호 4000으로 전달됩니다.

샘플 컨피그레이션

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

CME 시스템에서 자동 등록 비활성화

요약

SCCP **CME** 시스템의 텔레포니 서비스 아래에 auto-reg-phone이 활성화되면 시스템에 연결된 새 IP 전화기가 자동으로 등록되며, **자동 할당**이 내선 번호를 자동으로 할당하도록 구성된 경우 새 IP 전화가 즉시 전화를 걸 수 있습니다.

참고: 이는 **내부 위협**입니다.

예 1

이 컨피그레이션에서는 전화기가 CME 시스템에 등록되고 이를 사용하여 IP 텔레포니 통화를 하려면 전화기를 수동으로 추가해야 하도록 새 CME 시스템이 구성됩니다.

솔루션

CME 시스템에 연결된 새 IP 전화가 CME 시스템에 자동 등록되지 않도록 텔레포니 서비스 아래**에 자동 등록** 전화기를 비활성화할 수 있습니다.

샘플 컨피그레이션

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

예 2

SCCP CME를 사용하고 Cisco SIP 전화기를 시스템에 등록하려는 경우 SIP 엔드포인트가 사용자 이름 및 비밀번호로 인증하도록 시스템을 구성해야 합니다.이를 위해 다음을 구성하면 됩니다.

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

SIP 참조:SIP CME에 대한 보다 포괄적인 컨피그레이션 가이드를 위해 Cisco Unified CME 설정

Cisco Unity Express 제한 툴

보안 Cisco Unity Express:PSTN 액세스

요약

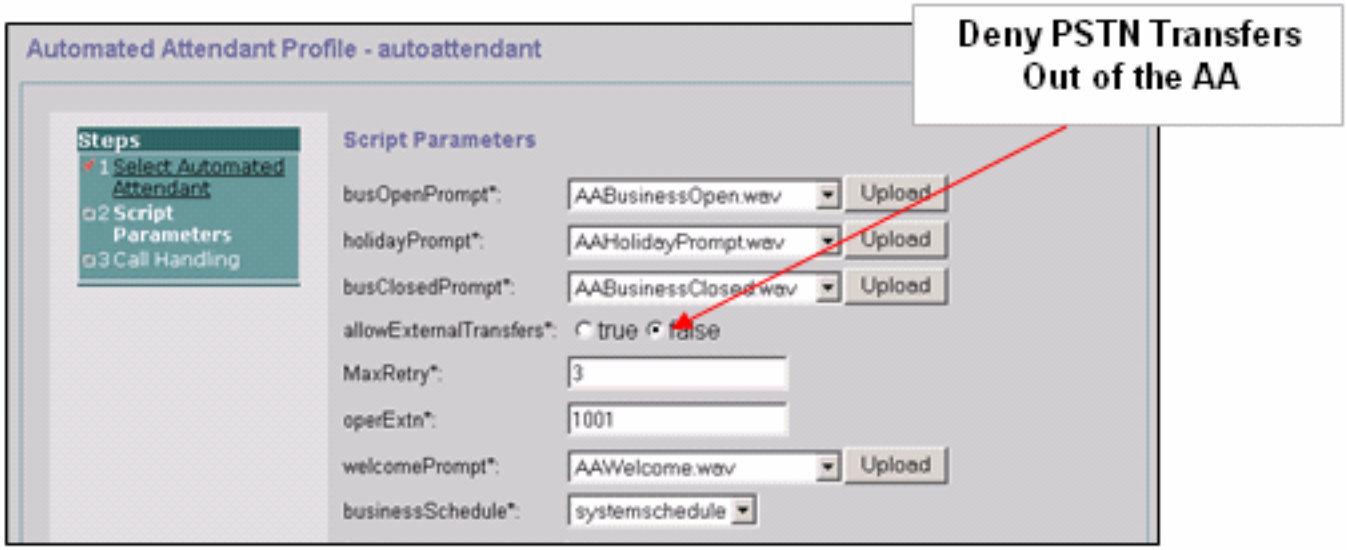
인바운드 통화가 Cisco Unity Express의 자동 전화 교환(AA)으로 전달되도록 시스템을 구성하는 경

우 Cisco Unity Express AA에서 PSTN으로의 외부 전송을 비활성화해야 할 수 있습니다.외부 사용자가 Cisco Unity Express AA에 연결한 후에는 외부로 전화를 걸 수 없습니다.

참고: 이는 **외부 위협**입니다.

참고: 솔루션

참고: Cisco Unity Express GUI에서 **allowExternalTransfers** 옵션을 비활성화합니다.



참고: AA에서 PSTN 액세스가 필요한 경우 스크립트에서 유효한 것으로 간주되는 번호의 숫자 또는 범위를 제한합니다.

Cisco Unity Express 제한 표

요약

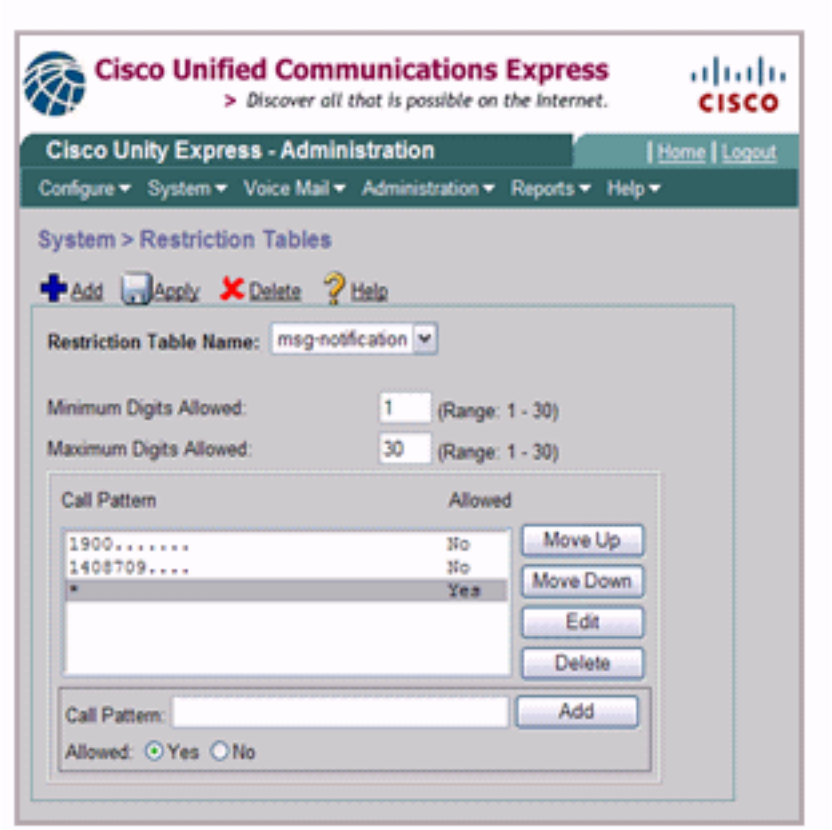
Cisco Unity Express 제한 테이블을 사용하여 Cisco Unity Express에서 발신 중에 도달할 수 있는 대상을 제한할 수 있습니다.Cisco Unity Express 제한 표를 사용하여 유료 사기 및 Cisco Unity Express 시스템의 악의적 사용을 방지하여 아웃바운드 통화를 할 수 있습니다.Cisco Unity Express 제한 테이블을 사용하는 경우 와일드카드 일치에 대한 통화 패턴을 지정할 수 있습니다.Cisco Unity Express 제한 테이블을 사용하는 애플리케이션은 다음과 같습니다.

- 팩스
- Cisco Unity Express 라이브 재생
- 메시지 알림
- 구독자가 아닌 메시지 전달

참고: 이는 **내부 위협**입니다.

솔루션

아웃바운드 외부 통화에서 Cisco Unity Express에서 연결할 수 있는 대상 패턴을 제한하려면 Cisco Unity Express GUI에서 **System(시스템) > Restrictions Tables(제한 테이블)**에서 **Call Pattern(통화 패턴)**을 구성합니다.



통화 로깅

향상된 CDR

향상된 CDR을 캡처하고 CDR을 라우터 플래시 또는 외부 FTP 서버에 기록하도록 CME 시스템을 구성할 수 있습니다.그런 다음 이 레코드를 사용하여 내부 또는 외부 당사자에 의한 악용 여부를 확인하기 위해 통화를 다시 추적할 수 있습니다.

Cisco IOS Release 12.4(15)XY에서 CME 4.3/7.0과 함께 도입된 파일 계정 기능은 쉼표로 구분된 값(.csv) 형식으로 계정 레코드를 캡처하고 내부 플래시에 있는 파일 또는 외부 FTP 서버에 레코드를 저장하는 방법을 제공합니다.또한 AAA 및 syslog 메커니즘을 포함하여 게이트웨이 어카운팅 지원을 확장합니다.

어카운팅 프로세스는 Cisco 음성 게이트웨이에서 생성된 각 통화 레그에 대한 어카운팅 데이터를 수집합니다.이 정보를 사용하여 청구 레코드를 생성하고 네트워크 분석에 사용할 수 있습니다 .Cisco 음성 게이트웨이는 Cisco에서 정의한 특성을 포함하는 CDR(Call Detail Records) 형식으로 계정 데이터를 캡처합니다.게이트웨이는 RADIUS 서버, syslog 서버 및 새 파일 방법으로 CDR을 플래시 또는 FTP 서버에 .csv 형식으로 전송할 수 있습니다.

향상된 CDR 기능에 대한 자세한 내용은 CDR 예를 참조하십시오.

관련 정보

- Cisco Unified Communications Manager Express 보안 모범 사례
- Cisco Communications Manager Express 관리자 가이드
- Cisco Communications Manager Express 관리자 가이드 - 통화 차단
- IOS 플랫폼에서 다이얼 피어 일치 이해

- 음성 변환 프로파일을 사용한 번호 변환
- CME 솔루션 참조 네트워크 설계 가이드
- 기술 지원 및 문서 – Cisco Systems