Unified Communications Manager Express - Verhinderung von Gebührenbetrug

Inhalt

Einführung

Dieses Dokument enthält einen Konfigurationsleitfaden, der zum Schutz eines Cisco Communications Manager Express (CME)-Systems und zur Eindämmung von Gebührenbetrug verwendet werden kann. CME ist die routerbasierte Anrufsteuerungslösung von Cisco, die eine intelligente, einfache und sichere Lösung für Unternehmen bietet, die Unified Communications implementieren möchten. Es wird dringend empfohlen, die in diesem Dokument beschriebenen Sicherheitsmaßnahmen zu implementieren, um zusätzliche Sicherheitskontrollen zu ermöglichen und das Risiko von Gebührenbetrug zu verringern.

Ziel dieses Dokuments ist es, Sie über die verschiedenen Sicherheitstools zu informieren, die auf

Cisco Voice Gateways und CME verfügbar sind. Diese Tools können in einem CME-System implementiert werden, um die Gefahr von Gebührenbetrug sowohl für interne als auch für externe Parteien zu mindern.

Dieses Dokument enthält Anweisungen zur Konfiguration eines CME-Systems mit verschiedenen Tools für die Sicherheit und die Einschränkung von Funktionen. In diesem Dokument wird auch erläutert, warum bestimmte Sicherheitstools in bestimmten Bereitstellungen verwendet werden.

Die umfassende Flexibilität der ISR-Plattformen von Cisco ermöglicht die Bereitstellung von CME in vielen verschiedenen Bereitstellungsarten. Daher kann es erforderlich sein, eine Kombination der in diesem Dokument beschriebenen Funktionen zu verwenden, um CME zu sperren. Dieses Dokument dient als Richtlinie für die Anwendung von Sicherheitstools auf CME und garantiert keinesfalls, dass Gebührenbetrug oder Missbrauch durch interne und externe Parteien nicht auftreten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Unified Communications Manager Express

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Unified Communications Manager Express 4.3 und CME 7.0.

Hinweis: Cisco Unified CME 7.0 bietet dieselben Funktionen wie Cisco Unified CME 4.3, das in Übereinstimmung mit den Cisco Unified Communications-Versionen in 7.0 umnummeriert wird.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Übersicht

In diesem Dokument werden die gängigsten Sicherheitstools erläutert, die in einem CME-System verwendet werden können, um die Gefahr von Gebührenbetrug zu mindern. Die in diesem Dokument erwähnten CME-Sicherheitstools umfassen Tools zur Gebührenbeschränkung und Tools zur Einschränkung von Funktionen.

Tools zur Gebührenbeschränkung

- Durchwahl
- Gebührenbeschränkung nach Geschäftsschluss
- Einschränkungsklasse
- Zugriffsliste zur Beschränkung des H323-/SIP-Trunk-Zugriffs

Funktionseinschränkungstools

- Übertragungsmuster
- Übertragungsmuster blockiert
- Maximale Übertragungslänge
- Anrufweiterleitung mit max. Länge
- Keine lokalen Rufumleitungen
- Kein Auto-Reg-ephone

Cisco Unity Express-Einschränkungstools

- Sicherer Zugriff auf das PSTN mit Cisco Unity Express
- Nachrichtenbenachrichtigungsbeschränkung

Anrufprotokollierung

- Anrufprotokollierung zum Erfassen von CDRs

Interne und externe Bedrohungen

Dieses Dokument behandelt Bedrohungen von internen und externen Parteien. Zu den internen Parteien gehören IP-Telefonbenutzer, die sich in einem CME-System befinden. Zu externen Parteien gehören Benutzer in ausländischen Systemen, die versuchen können, mithilfe des Host-CME betrügerische Anrufe zu tätigen, und die Anrufe an Ihr CME-System zurückgebucht haben.

Tools zur Gebührenbeschränkung

Durchwahl

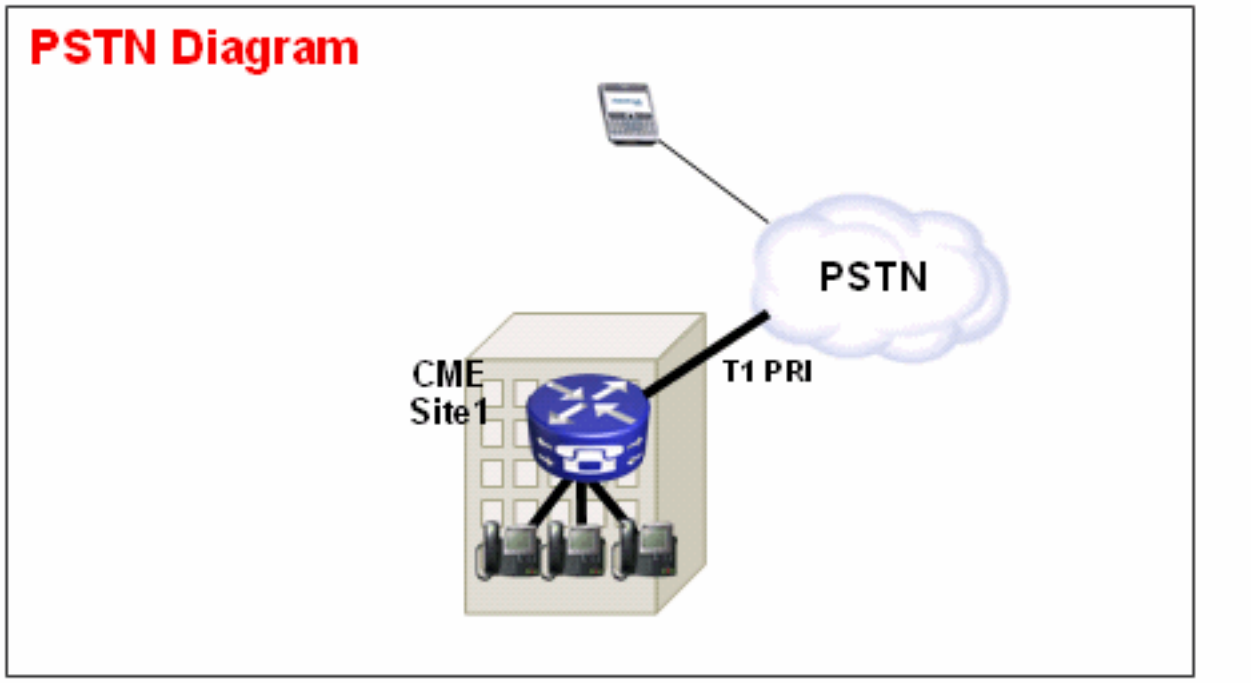
Zusammenfassung

Direct-Inward-Dial (DID) wird auf Cisco Sprach-Gateways verwendet, damit das Gateway einen eingehenden Anruf verarbeiten kann, nachdem es Nummern vom PBX- oder CO-Switch empfängt. Wenn die DID aktiviert ist, gibt das Cisco Gateway dem Anrufer keinen sekundären Wählton aus und wartet nicht darauf, zusätzliche Nummern vom Anrufer zu sammeln. Er leitet den Anruf direkt an das Ziel weiter, das mit dem DNIS (Inbound Dialed Number Identification Service) übereinstimmt. Dies wird als Einstufen-Wählen bezeichnet.

Hinweis: Dies ist eine **externe Bedrohung**.

Problem-Anweisung

Wenn Direct-Inward-Dial NICHT auf einem Cisco Gateway oder CME konfiguriert ist, hört der Anrufer bei jedem Anruf vom CO- oder PBX-System zum Cisco Gateway einen sekundären Wählton. Dies wird als zweistufiges Wählen bezeichnet. Wenn die Anrufer des PSTN den sekundären Wählton hören, können sie Ziffern eingeben, um eine interne Durchwahl zu erreichen. Wenn sie den Zugriffscode des PSTN kennen, können sie Ferngespräche führen oder internationale Nummern wählen. Dies stellt ein Problem dar, da der Anrufer im PSTN über das CME-System ausgehende Fern- oder Auslandsgespräche tätigen kann und das Unternehmen für die Anrufe in Rechnung gestellt wird.



Beispiel 1

An Standort 1 ist das CME über eine T1 PRI-Hauptleitung mit dem PSTN verbunden. Der PSTN-Provider stellt den **40855512 bereit.** DID-Bereich für CME-Standort 1. So werden alle PSTN-Anrufe, die für 4085551200 - 4085551299 bestimmt sind, eingehend an CME weitergeleitet. Wenn Sie die **Direktwahl** im System nicht konfigurieren, hört ein eingehender PSTN-Anrufer einen sekundären Wählton und muss die interne Durchwahl manuell wählen. Das größere Problem besteht darin, dass der Anrufer, wenn er ein Benutzer ist und den PSTN-Zugriffscode im System kennt (in der Regel **9**), eine **9** wählen kann und dann jede Zielnummer wählen kann, die er erreichen möchte.

Lösung 1

Um diese Bedrohung abzuwehren, müssen Sie **Direktwahlnummern** konfigurieren. Dadurch leitet das Cisco Gateway den eingehenden Anruf direkt an das Ziel weiter, das mit dem eingehenden DNIS übereinstimmt.

Beispielkonfiguration

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

Damit die DID ordnungsgemäß funktioniert, müssen Sie sicherstellen, dass der eingehende Anruf

mit dem richtigen POTS-DFÜ-Peer übereinstimmt, für den der Befehl **Direct-Inward-Dial** konfiguriert ist. In diesem Beispiel ist die T1 PRI mit Port 1/0:23 verbunden. Um dem richtigen DFÜ-Peer für eingehende Anrufe zu entsprechen, führen Sie den Befehl **incoming called-number-** dial peer (DFÜ-Peer für eingehende Anrufe) unter dem DID POTS-DFÜ-Peer aus.

Beispiel 2

An Standort 1 ist das CME über eine T1 PRI-Hauptleitung mit dem PSTN verbunden. Der PSTN-Provider gibt den **40855512.** und **40855513.** DID-Bereiche für CME-Standort 1. So werden alle PSTN-Anrufe, die für 4085551200 - 4085551299 und 408551300 - 4085551399 bestimmt sind, an die CME weitergeleitet.

Falsche Konfiguration:

Wenn Sie wie in der Beispielkonfiguration in diesem Abschnitt einen eingehenden DFÜ-Peer konfigurieren, besteht weiterhin die Möglichkeit eines Gebührenbetrugs. Das Problem bei diesem eingehenden DFÜ-Peer besteht darin, dass er nur eingehende Anrufe mit **40852512** vergleicht**.** und wendet dann den DID-Dienst an. Wenn ein PSTN-Anruf bei **40852513** eingeht**..**, stimmt der Dial-Peer der eingehenden Ports nicht überein, und der DID-Dienst wird daher nicht angewendet. Wenn kein eingehender Dial-Peer mit DID zugeordnet wird, wird der standardmäßige DFÜ-Peer 0 verwendet. DID ist auf Dial-Peer 0 standardmäßig deaktiviert.

Beispielkonfiguration

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

Richtige Konfiguration

In diesem Beispiel wird die richtige Methode zum Konfigurieren des DID-Dienstes auf einem eingehenden DFÜ-Peer gezeigt:

Beispielkonfiguration

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

Unter DID-Konfiguration für POTS-DFÜ-Peers finden Sie weitere Informationen zu DID für digitale T1/E1-Sprach-Ports.

Hinweis: Die Verwendung von DID ist **nicht** erforderlich, wenn Private Line Automatic Ringdown (PLAR) für einen Sprach-Port oder ein Service-Skript wie die automatische Anrufvermittlung (AA) für den eingehenden Dial-Peer verwendet wird.

Beispielkonfiguration - PLAR

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

Beispielkonfiguration - Service-Skript

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

Gebührenbeschränkungen nach Geschäftsschluss

Zusammenfassung

Die Gebührenbeschränkung nach Geschäftsschluss ist ein neues Sicherheitstool, das in CME 4.3/7.0 verfügbar ist und Ihnen die Konfiguration von Richtlinien zur Gebührenbeschränkung basierend auf Datum und Uhrzeit ermöglicht. Sie können Richtlinien so konfigurieren, dass Benutzer zu bestimmten Tageszeiten oder zu jeder Zeit keine Anrufe an vordefinierte Nummern tätigen dürfen. Wenn die Richtlinie zur Blockierung von Anrufen rund um die Uhr (7x24 After Hours) konfiguriert wird, wird auch der Nummernsatz eingeschränkt, der von einem internen Benutzer eingegeben werden kann, um die **Rufumleitung für alle Anrufe** festzulegen.

Hinweis: Dies ist eine **interne Bedrohung**.

Beispiel 1

In diesem Beispiel werden mehrere Ziffernmuster definiert, für die ausgehende Anrufe blockiert werden. Die Muster 1 und 2, die Anrufe an externe Nummern blockieren, die mit "1" und "011" beginnen, werden montags bis freitags vor 7 Uhr und nach 19 Uhr, am Samstag vor 7 Uhr und nach 13 Uhr sowie am Sonntag blockiert. Muster 3 blockiert Anrufe an 900 Nummern 7 Tage die Woche, 24 Stunden am Tag.

Beispielkonfiguration

```
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
```

Weitere Informationen zur Gebührenbeschränkung finden Sie unter Konfigurieren der Anrufblockierung.

Einschränkungsklasse

Zusammenfassung

Wenn Sie beim Konfigurieren der Gebührenbeschränkung eine präzise Kontrolle benötigen, müssen Sie Class of Restriction (COR) verwenden. Siehe Class of Restriction: Beispiel für weitere Informationen.

H.323/SIP-Trunks - Einschränkungen für Gebührenbetrug

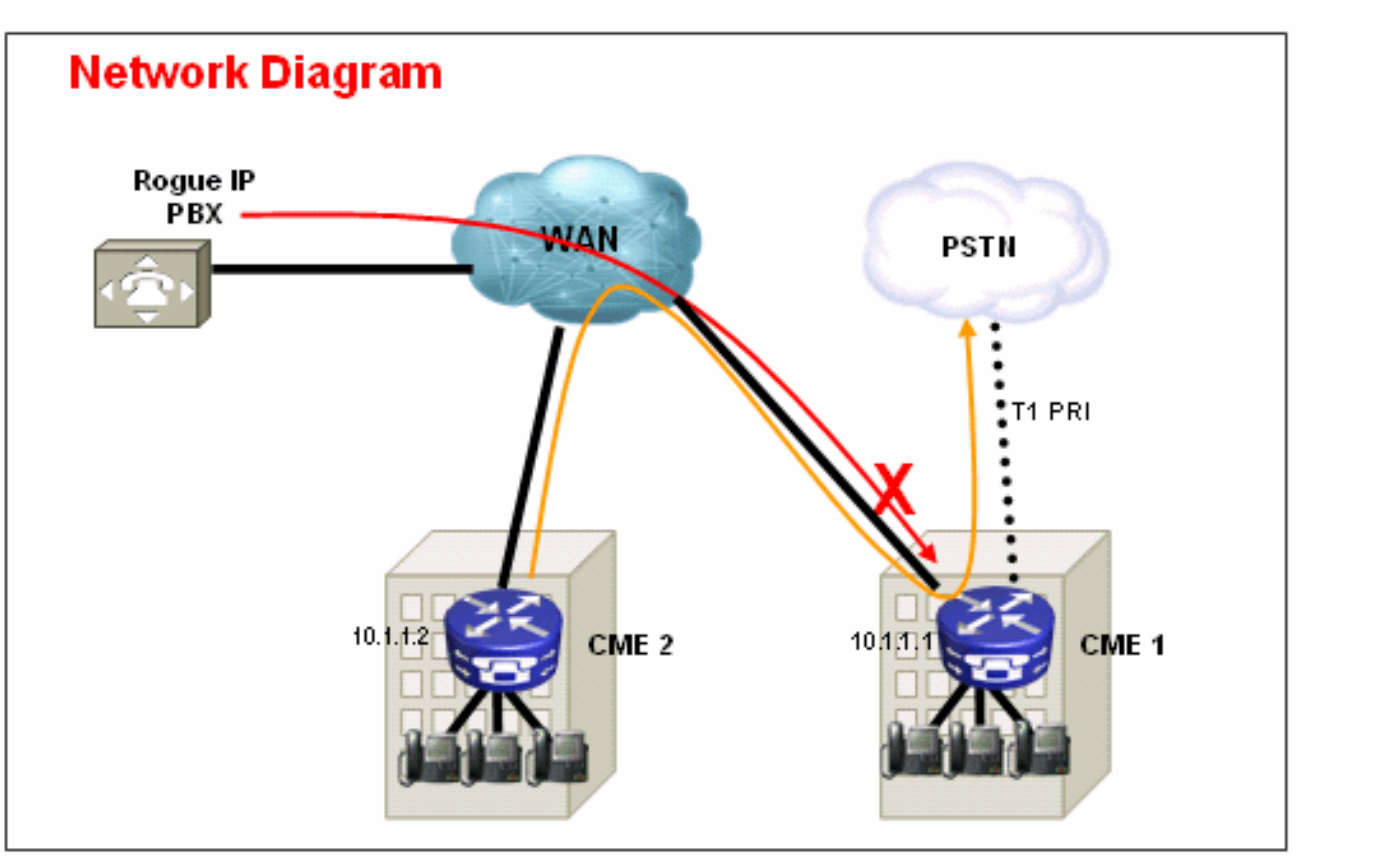
Zusammenfassung

In Fällen, in denen ein CME-System über ein WAN mit anderen CME-Geräten über einen SIP- oder H.323-Trunk verbunden ist, können Sie den SIP/H.323-Trunk-Zugriff auf das CME einschränken, um zu verhindern, dass Benutzer Ihr System zur illegalen Weiterleitung von Anrufen an das PSTN verwenden.

Hinweis: Dies ist eine **externe Bedrohung**.

Beispiel 1

In diesem Beispiel verfügt CME 1 über PSTN-Verbindungen. CME 2 ist über das WAN mit CME 1 über einen H.323-Trunk verbunden. Um CME 1 zu sichern, können Sie eine Zugriffsliste konfigurieren und diese an der WAN-Schnittstelle eingehend anwenden und somit nur IP-Datenverkehr von CME 2 zulassen. Dadurch wird verhindert, dass die nicht autorisierte IP-Telefonanlage VoIP-Anrufe über CME 1 an das PSTN sendet.



Lösung

Lassen Sie der WAN-Schnittstelle auf CME 1 nicht zu, Datenverkehr von nicht erkannten Geräten zu akzeptieren. Beachten Sie, dass am Ende einer Zugriffsliste eine implizite ABLEHNUNG vorhanden ist. Wenn es mehr Geräte gibt, von denen aus eingehender IP-Datenverkehr zugelassen werden soll, müssen Sie der Zugriffsliste unbedingt die IP-Adresse des Geräts hinzufügen.

Beispielkonfiguration - CME 1

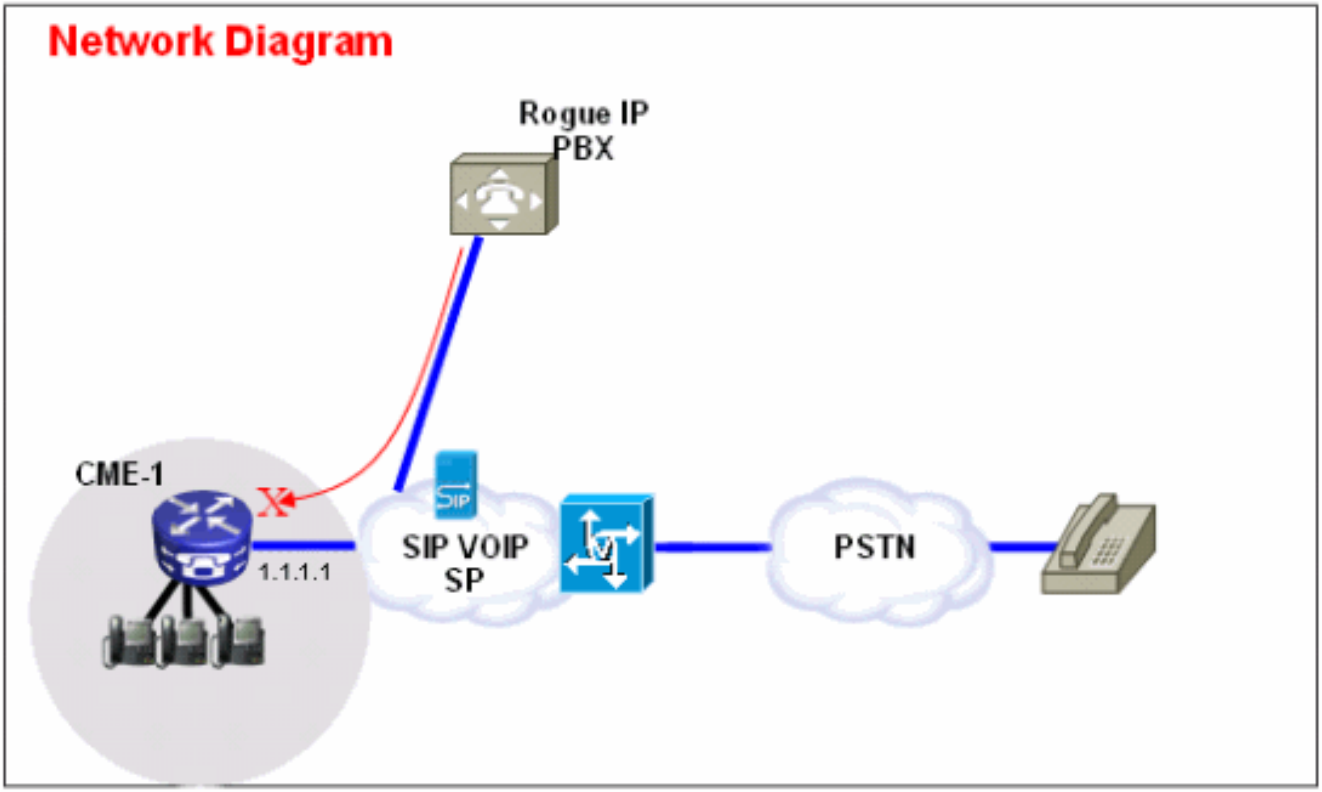
```
interface serial 0/0
```

```
  ip access-group 100 in
!
access-list 100 permit ip 10.1.1.2 255.255.255.255 any
```

Beispiel 2

In diesem Beispiel ist CME 1 mit dem SIP-Provider für die PSTN-Verbindung verbunden. Die Beispielkonfiguration wird unter Konfigurationsbeispiel für Cisco CallManager Express (CME) SIP-Trunking bereitgestellt.

Da sich CME 1 im öffentlichen Internet befindet, ist es möglich, dass *Gebührenbetrug* auftreten kann, wenn ein unberechtigter Benutzer öffentliche IP-Adressen für bekannte H.323- (TCP 1720)- oder SIP-Signalisierungen (UDP oder TCP 5060) prüft und SIP- oder H.323-Nachrichten sendet, die Anrufe aus dem SIP-Trunk zurückleiten PSTN. Die häufigsten Missbräuche in diesem Fall sind, dass der unberechtigte Benutzer mehrere internationale Anrufe über den SIP- oder H.323-Trunk durchführt und den Eigentümer der CME 1 veranlasst, diese Telefongebühren zu bezahlen - in einigen Fällen Tausende von Dollar.



Lösung

Zur Abwehr dieser Bedrohung können Sie mehrere Lösungen verwenden. Wenn über die WAN-Verbindung(en) in CME 1 keine VoIP-Signalisierung (SIP oder H.323) verwendet wird/werden, muss dies mit den Firewall-Techniken in CME 1 (Zugriffslisten oder ACLs) so weit wie möglich blockiert werden.

1. Sicherung der WAN-Schnittstelle mit der Cisco IOS® Firewall auf CME 1:Dies impliziert, dass Sie nur bekannten SIP- oder H.323-Datenverkehr auf der WAN-Schnittstelle zulassen. Alle anderen SIP- oder H.323-Datenverkehr werden blockiert. Dazu müssen Sie auch die IP-Adressen kennen, die der SIP VOIP SP für die Signalisierung auf dem SIP-Trunk verwendet. Diese Lösung setzt voraus, dass der SP bereit ist, alle IP-Adressen oder DNS-Namen bereitzustellen, die er in seinem Netzwerk verwendet. Wenn DNS-Namen verwendet werden,

muss für die Konfiguration ein DNS-Server verfügbar sein, der diese Namen auflösen kann. Wenn der Service Provider außerdem Adressen an seinem Ende ändert, muss die Konfiguration auf CME 1 aktualisiert werden. Beachten Sie, dass diese Zeilen zusätzlich zu den bereits auf der WAN-Schnittstelle vorhandenen ACL-Einträgen hinzugefügt werden müssen.Beispielkonfiguration - 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. Stellen Sie sicher, dass Anrufe, die auf dem SIP-Trunk eingehen, **KEINE** Fairpin-Rückmeldung erhalten:Dies bedeutet, dass die CME 1-Konfiguration nur SIP-SIP-Hairpin von Anrufen für einen bestimmten bekannten PSTN-Nummernbereich zulässt, alle anderen Anrufe blockiert werden. Sie müssen bestimmte eingehende DFÜ-Peers für die PSTN-Nummern konfigurieren, die auf dem SIP-Trunk eingehen und den Nebenstellen oder der automatischen Anrufvermittlung bzw. Voicemail auf CME 1 zugeordnet sind. Alle anderen Anrufe bei Nummern, die nicht Teil des PSTN-Nummernbereichs von CME 1 sind, werden blockiert. Beachten Sie, dass dies die Weiterleitung von Anrufen/Weiterleitungen an Voicemail (Cisco Unity Express) und die Weiterleitung aller Anrufe an PSTN-Nummern von IP-Telefonen auf CME 1 nicht betrifft, da der erste Anruf immer noch auf eine Durchwahl auf CME 1 ausgerichtet ist.Beispielkonfiguration - 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. Verwenden Sie Übersetzungsregeln, um bestimmte Wählzeichenfolgen zu blockieren:Bei den meisten Gebührenbetrügereien handelt es sich um internationale Anrufe. Als Ergebnis können Sie einen bestimmten eingehenden Dial-Peer erstellen, der bestimmten gewählten Zeichenfolgen entspricht und Anrufe blockiert. Die meisten CMEs verwenden einen bestimmten Zugriffscode (z. B. 9), um sich auszuwählen, und der internationale Wählcode in den USA lautet 011. Die gebräuchlichste Wählzeichenfolge in den USA lautet daher 9011 + alle Ziffern, die danach im SIP-Trunk eingegeben werden.Beispielkonfiguration - 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
```

Funktionseinschränkungstools

Übertragungsmuster

Zusammenfassung

Übertragungen zu allen Nummern, mit Ausnahme derjenigen auf lokalen SCCP-IP-Telefonen, werden standardmäßig gesperrt. Während der Konfiguration können Sie Transfers zu nicht lokalen Nummern zulassen. Der Befehl **transfer pattern** wird verwendet, um die Weiterleitung von Telefonanrufen von Cisco SCCP IP-Telefonen an andere Telefone als Cisco IP Phones zu ermöglichen, z. B. externe PSTN-Anrufe oder Telefone in einem anderen CME-System. Sie können das **Übertragungsmuster** verwenden, um die Anrufe nur auf interne Durchwahlen zu beschränken oder Anrufe möglicherweise auf PSTN-Nummern in einem bestimmten Bereichscode zu beschränken. In diesen Beispielen wird veranschaulicht, wie der Befehl **transfer pattern** verwendet werden kann, um Anrufe auf verschiedene Nummern zu beschränken.

Hinweis: Dies ist eine **interne Bedrohung**.

Beispiel 1

Benutzer dürfen Anrufe nur an den Ortsvorwahl 408 weiterleiten. In diesem Beispiel wird davon ausgegangen, dass CME mit einem Dial-Peer konfiguriert ist, der ein Zielmuster von 9T aufweist.

Beispielkonfiguration

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

Gesperrtes Übertragungsmuster

Zusammenfassung

In Cisco Unified CME 4.0 und höheren Versionen können Sie verhindern, dass einzelne Telefone Anrufe an Nummern weiterleiten, die global für die Weiterleitung aktiviert sind. Der Befehl **transfer pattern locking** überschreibt den Befehl **transfer pattern** und deaktiviert die Anrufweiterleitung an ein Ziel, das über einen POTS- oder VoIP-Dial-Peer erreicht werden muss. Dazu gehören PSTN-Nummern, andere Sprach-Gateways und Cisco Unity Express. So wird sichergestellt, dass für einzelne Telefone keine Gebühren anfallen, wenn Anrufe außerhalb des Cisco Unified CME-Systems weitergeleitet werden. Die Blockierung der Anrufweiterleitung kann für einzelne Telefone konfiguriert oder als Teil einer Vorlage konfiguriert werden, die auf eine Reihe von Telefonen angewendet wird.

Hinweis: Dies ist eine **interne Bedrohung**.

Beispiel 1

In dieser Beispielkonfiguration darf ephone 1 keine Übertragungsmuster (global definiert) für die

Weiterleitung von Anrufen verwenden, während ephone 2 das unter Telefoniedienst definierte Übertragungsmuster für die Weiterleitung von Anrufen verwenden kann.

Beispielkonfiguration

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

Maximale Übertragungslänge

Zusammenfassung

Der Befehl **transfer max-length** gibt die maximale Anzahl von Ziffern an, die der Benutzer bei der Weiterleitung eines Anrufs wählen kann. Das **Übertragungsmuster max-length** überschreibt den Befehl **Transfer Pattern** und erzwingt die maximal zulässigen Ziffern für das Transferziel. Das Argument gibt die Anzahl der zulässigen Ziffern in einer Nummer an, an die ein Anruf weitergeleitet wird. Bereich: 3 bis 16. Standard: 16.

Hinweis: Dies ist eine **interne Bedrohung**.

Beispiel 1

Mit dieser Konfiguration können Telefone, bei denen diese Telefonvorlage angewendet wurde, nur an Ziele weitergeleitet werden, die maximal vier Stellen lang sind.

Beispielkonfiguration

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

Anrufweiterleitung mit max. Länge

Zusammenfassung

Um die Anzahl der Ziffern einzuschränken, die mit der Softtaste CfwdALL auf einem IP-Telefon eingegeben werden können, verwenden Sie den Befehl **call-forward max-length** im Konfigurationsmodus ephone-dn oder ephone-dn-template. Um eine Beschränkung der Anzahl der eingegebenen Ziffern zu entfernen, verwenden Sie die **no-**Form dieses Befehls.

Hinweis: Dies ist eine **interne Bedrohung**.

Beispiel 1

In diesem Beispiel darf die Verzeichnisdurchwahl 101 eine Rufumleitung an eine beliebige Durchwahl durchführen, die eine bis vier Ziffern lang ist. Alle Anrufweiterleitungen an Ziele mit

einer Länge von mehr als vier Ziffern schlagen fehl.

Beispielkonfiguration

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

oder

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

Kein lokaler Anruf weiterleiten

Zusammenfassung

Wenn der Befehl **no forward local-calls** im ePhone-dn-Konfigurationsmodus verwendet wird, werden interne Anrufe an eine bestimmte ePhone-DN, bei der **keine lokalen Weiterleitungsanrufe** angewendet werden, nicht weitergeleitet, wenn die ePhone-DN besetzt ist oder nicht antwortet. Wenn ein interner Anrufer diese ephone-dn anruft und die ephone-dn besetzt ist, hört der Anrufer ein Besetztzeichen. Wenn ein interner Anrufer diese ephone-dn anruft und diese nicht antwortet, hört der Anrufer ein Rückrufsignal. Der interne Anruf wird nicht weitergeleitet, selbst wenn die Rufumleitung für die ephone-dn aktiviert ist.

Hinweis: Dies ist eine **interne Bedrohung**.

Beispiel 1

In diesem Beispiel wählt die Durchwahl 2222 die Durchwahl 3675 und hört einen Rückruf oder ein Besetztzeichen. Wenn ein externer Anrufer die Durchwahl 3675 erreicht hat und keine Antwort gefunden wurde, wird der Anruf an die Durchwahl 4000 weitergeleitet.

Beispielkonfiguration

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

Deaktivieren Sie die automatische Registrierung auf dem CME-System.

Zusammenfassung

Wenn **Auto-Reg-ephone** unter dem Telefoniedienst auf einem SCCP-CME-System aktiviert ist, werden neue IP-Telefone, die an das System angeschlossen sind, automatisch registriert. Wenn die **automatische Zuweisung** für die automatische Zuweisung von Durchwahlnummern konfiguriert ist, kann ein neues IP-Telefon sofort Anrufe tätigen.

Hinweis: Dies ist eine **interne Bedrohung**.

Beispiel 1

In dieser Konfiguration wird ein neues CME-System konfiguriert, sodass Sie manuell ein ephone hinzufügen müssen, damit sich das ephone beim CME-System registrieren und IP-Telefonieanrufe tätigen kann.

Lösung

Sie können **Auto-Reg-ephone** unter Telefoniedienst deaktivieren, sodass sich neue, mit einem CME-System verbundene IP-Telefone nicht automatisch beim CME-System registrieren.

Beispielkonfiguration

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

Beispiel 2

Wenn Sie SCCP CME verwenden und planen, Cisco SIP-Telefone im System zu registrieren, müssen Sie das System so konfigurieren, dass die SIP-Endpunkte sich mit einem Benutzernamen und Kennwort authentifizieren müssen. Konfigurieren Sie dazu einfach Folgendes:

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

Siehe SIP: Einrichten von Cisco Unified CME für einen umfassenderen Konfigurationsleitfaden für SIP CME.

Cisco Unity Express-Einschränkungstools

Secure Cisco Unity Express: AA-PSTN-Zugriff

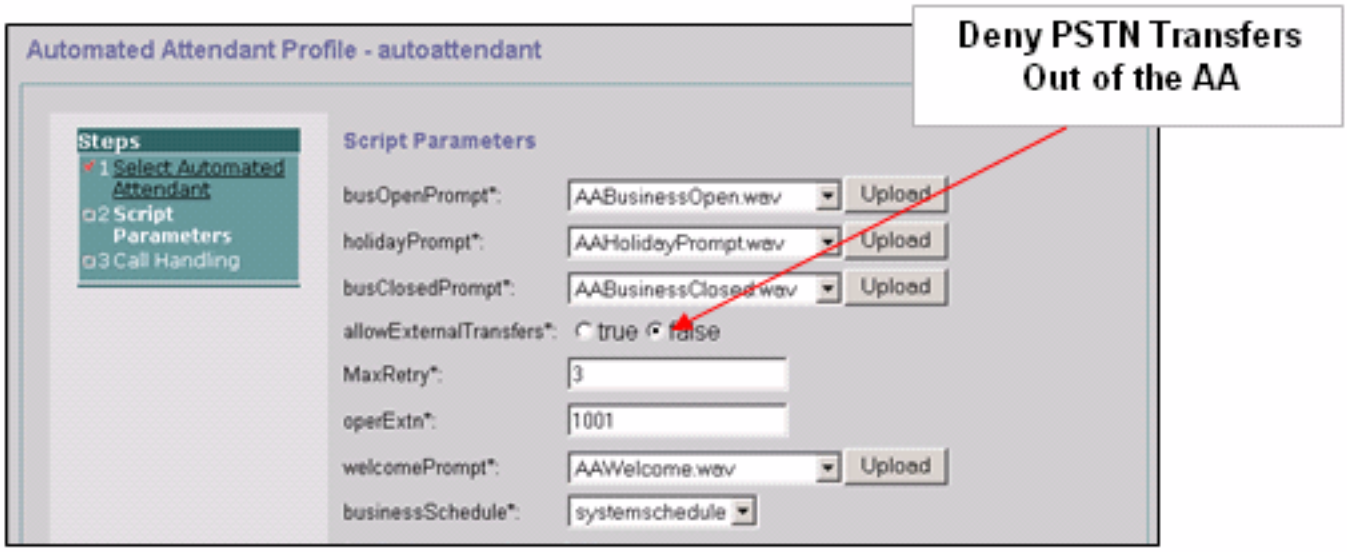
Zusammenfassung

Wenn Ihr System so konfiguriert ist, dass eingehende Anrufe an die automatische Anrufvermittlung (AA) in Cisco Unity Express weitergeleitet werden, kann es erforderlich sein, die externe Weiterleitung von Cisco Unity Express AA an das PSTN zu deaktivieren. Externe Benutzer können keine ausgehenden Nummern wählen, wenn sie Cisco Unity Express AA erreicht haben.

Hinweis: Dies ist eine **externe Bedrohung**.

Hinweis: Lösung

Hinweis: Deaktivieren Sie die Option **allowExternalTransfers** in der Benutzeroberfläche von Cisco Unity Express.



Hinweis: Wenn der PSTN-Zugriff von der AA erforderlich ist, begrenzen Sie die Nummern oder den Nummernbereich, die vom Skript als gültig angesehen werden.

Einschränkungstabellen für Cisco Unity Express

Zusammenfassung

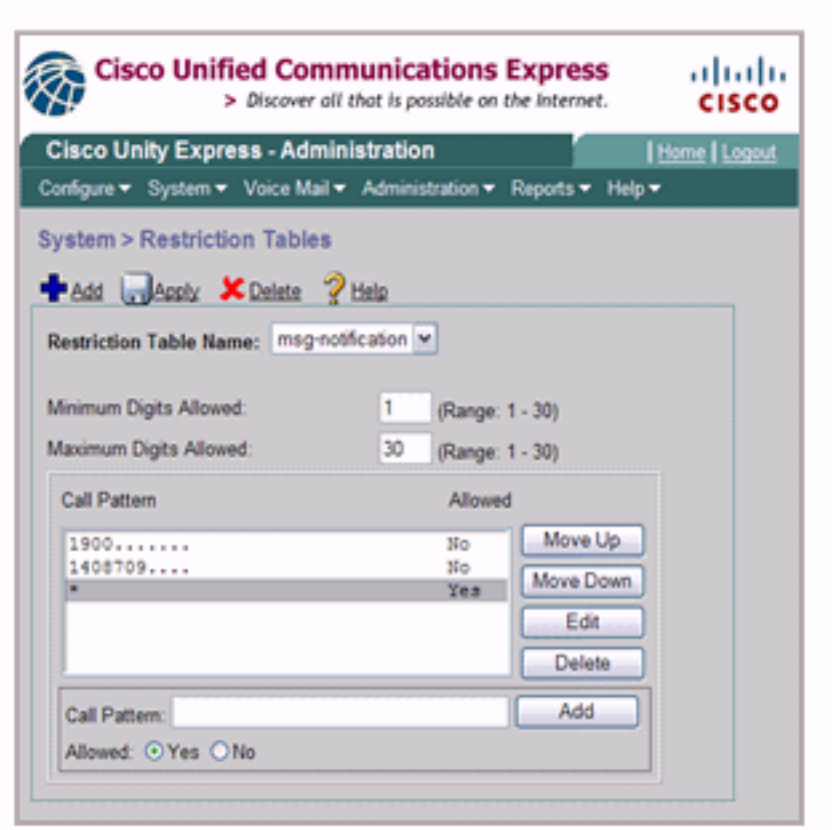
Sie können die Einschränkungstabellen von Cisco Unity Express verwenden, um die Ziele einzuschränken, die während eines ausgehenden Anrufs von Cisco Unity Express erreicht werden können. Die Cisco Unity Express-Einschränkungstabelle kann verwendet werden, um Gebührenbetrug und die böswillige Verwendung des Cisco Unity Express-Systems für ausgehende Anrufe zu verhindern. Wenn Sie die Einschränkungstabelle von Cisco Unity Express verwenden, können Sie Anrufmuster für die Übereinstimmung mit einer Wildcard angeben. Zu den Anwendungen, die die Einschränkungstabelle von Cisco Unity Express verwenden, gehören:

- Fax
- Live-Aufzeichnung von Cisco Unity Express
- Benachrichtigung
- Nachrichtenzustellung für Nicht-Abonnenten

Hinweis: Dies ist eine **interne Bedrohung**.

Lösung

Um die Zielmuster einzuschränken, die mit Cisco Unity Express bei einem ausgehenden externen Anruf erreicht werden können, konfigurieren Sie das **Anrufmuster** in der **Tabelle "System > Restrictions" (Systemeinschränkungen)** in der Benutzeroberfläche von Cisco Unity Express.



Anrufprotokollierung

Verbesserte CDRs

Sie können das CME-System so konfigurieren, dass erweiterte CDRs erfasst und die CDRs im Router-Flash oder auf einem externen FTP-Server protokolliert werden. Diese Datensätze können dann verwendet werden, um Anrufe zurückzuverfolgen, um festzustellen, ob es zu Missbrauch durch interne oder externe Parteien gekommen ist.

Die Dateiabrechnungsfunktion, die mit CME 4.3/7.0 in Cisco IOS Release 12.4(15)XY eingeführt wurde, bietet eine Methode zum Erfassen von Abrechnungsdatensätzen im CSV-Format (Comma Separate Value) und zum Speichern der Datensätze in einer Datei im internen Flash-Speicher oder auf einem externen FTP-Server. Es erweitert die Gateway-Accounting-Unterstützung, die auch die AAA- und Syslog-Mechanismen zur Protokollierung von Accounting-Informationen umfasst.

Beim Accounting werden für jede Anrufkomponente, die auf einem Cisco Voice Gateway erstellt wurde, Accounting-Daten erfasst. Sie können diese Informationen für Nachverarbeitungsaktivitäten wie das Generieren von Abrechnungsdatensätzen und für Netzwerkanalysen verwenden. Cisco Voice Gateways erfassen Abrechnungsdaten in Form von CDRs (Call Detail Records), die von Cisco definierte Attribute enthalten. Das Gateway kann CDRs an einen RADIUS-Server, einen Syslog-Server und mit der neuen Dateimethode an einen Flash- oder FTP-Server im CSV-Format senden.

Weitere Informationen zu den erweiterten CDR-Funktionen finden Sie in CDR-Beispielen.

Zugehörige Informationen

- Cisco Unified Communications Manager Express - Best Practices für die Sicherheit
- Administratorhandbuch für Cisco Communications Manager Express
- Cisco Communications Manager Express-Administratorhandbuch - Anrufblockierung
- Verständnis der DFÜ-Peer-Matching auf IOS-Plattformen
- Nummernübersetzung mithilfe von Sprachübersetzungsprofilen
- Designleitfaden für das Referenznetzwerk der CME-Lösung
- Technischer Support und Dokumentation - Cisco Systems