Prevenzione delle frodi con pedaggio di Unified Communications Manager Express

Sommario

Introduzione

Questo documento offre una guida alla configurazione che può essere utilizzata per proteggere un sistema Cisco Communications Manager Express (CME) e ridurre il rischio di frodi. CME è la soluzione di controllo delle chiamate basata su router di Cisco che fornisce una soluzione intelligente, semplice e sicura per le organizzazioni che desiderano implementare Unified Communications. Si consiglia vivamente di applicare le misure di sicurezza descritte in questo documento al fine di fornire ulteriori livelli di controllo della sicurezza e ridurre la possibilità di frodi relative ai pedaggi.

L'obiettivo di questo documento è quello di fornire informazioni sui vari strumenti di sicurezza

disponibili su Cisco Voice Gateway e CME. Questi strumenti possono essere implementati su un sistema CME al fine di contribuire a ridurre la minaccia di frode dei pedaggi da parte di parti sia interne che esterne.

In questo documento viene spiegato come configurare un sistema CME con diversi strumenti di sicurezza del pedaggio e di restrizione delle funzioni. Nel documento viene inoltre illustrato il motivo per cui alcuni strumenti di protezione vengono utilizzati in determinate distribuzioni.

La flessibilità complessiva delle piattaforme ISR di Cisco consente di implementare CME in molti tipi diversi di installazioni. Pertanto, può essere necessario utilizzare una combinazione delle funzionalità descritte in questo documento per bloccare il CME. Il presente documento funge da orientamento per l'applicazione degli strumenti di sicurezza alla CME e non garantisce in alcun modo che non si verifichino frodi o abusi da parte di soggetti interni ed esterni.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unified Communications Manager Express

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco Unified Communications Manager Express 4.3 e CME 7.0.

Nota: Cisco Unified CME 7.0 include le stesse funzionalità di Cisco Unified CME 4.3, che è stato rinumerato come 7.0 per essere allineato alle versioni di Cisco Unified Communications.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Panoramica

Questo documento descrive gli strumenti di sicurezza più comuni che possono essere utilizzati su un sistema CME per ridurre la minaccia di frodi. Gli strumenti di sicurezza CME a cui si fa riferimento in questo documento includono gli strumenti di limitazione del pedaggio e gli strumenti di restrizione delle funzionalità.

Strumenti di limitazione del numero a tariffa

- Direct-inward-dial
- Limitazione di pedaggio fuori orario
- Classe di restrizione
- Access-list per limitare l'accesso al trunk H323/SIP

Strumenti di limitazione delle feature

- Modello di trasferimento
- Modello di trasferimento bloccato
- Trasferisci lunghezza massima
- Lunghezza massima call-forward
- Non inoltrare chiamate locali
- No auto-reg-phone

Strumenti di restrizione Cisco Unity Express

- Accesso sicuro PSTN Cisco Unity Express
- Restrizione notifica messaggio

Registrazione chiamate

- Registrazione delle chiamate per acquisire i record dei dettagli delle chiamate (CDR)

Minacce interne ed esterne

In questo documento vengono discusse le minacce provenienti da parti interne ed esterne. Le parti interne comprendono gli utenti di telefoni IP che risiedono su un sistema CME. Le parti esterne includono utenti su sistemi esteri che possono provare a utilizzare l'host CME per effettuare chiamate fraudolente e avere le chiamate ricaricate al sistema CME.

Strumenti di limitazione del numero a tariffa

Direct-inward-dial

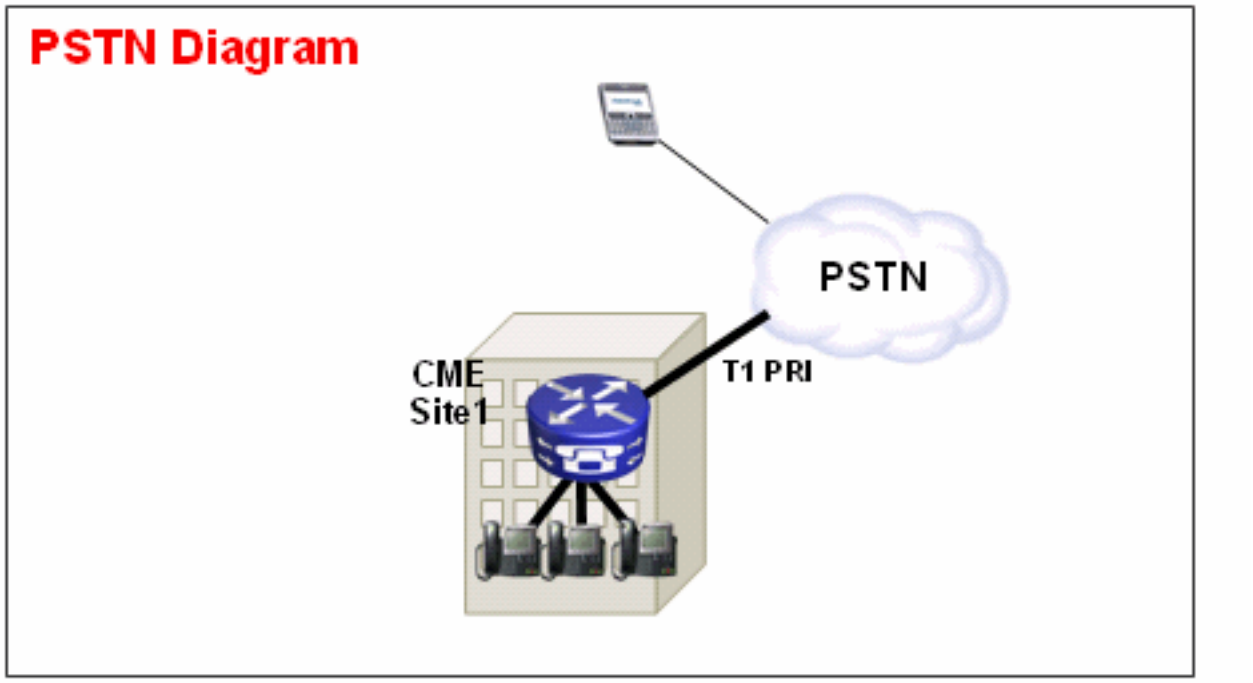
Riassunto

Il comando Direct-Inward-Dial (DID) viene usato sui gateway voce Cisco per consentire al gateway di elaborare una chiamata in entrata dopo aver ricevuto cifre dallo switch PBX o CO. Quando la funzione DID è abilitata, il gateway Cisco non emette un segnale di linea secondario al chiamante e non attende di raccogliere altre cifre dal chiamante. Inoltra la chiamata direttamente alla destinazione corrispondente al DNIS (Dialed Number Identification Service) in entrata. Questa modalità è denominata connessione a una fase.

Nota: si tratta di una **minaccia esterna**.

Dichiarazione di problema

Se la composizione diretta verso l'interno NON è configurata su un Cisco Gateway o CME, ogni volta che il CO o il PBX effettuano una chiamata al Cisco Gateway, il chiamante sente un segnale di composizione secondario. Questa composizione si chiama composizione in due fasi. Una volta che i chiamanti PSTN hanno sentito il segnale di linea secondario, possono immettere cifre per raggiungere qualsiasi estensione interna o, se conoscono il codice di accesso PSTN, possono comporre numeri internazionali o di lunga distanza. Questo rappresenta un problema perché il chiamante PSTN può utilizzare il sistema CME per effettuare chiamate in uscita interurbane o internazionali e alla società viene addebitato il costo delle chiamate.



[Esempio 1]

Nel sito 1, il CME è collegato alla PSTN tramite un T1 PRI trunk. Il provider PSTN fornisce **40855512.** Intervallo DID per il sito CME 1. Pertanto tutte le chiamate PSTN destinate a 4085551200 - 4085551299 vengono instradate in entrata verso CME. Se non si configura la **composizione diretta** sul sistema, un chiamante PSTN in ingresso sentirà un segnale di composizione secondario e dovrà comporre manualmente l'estensione interna. Il problema maggiore è che se il chiamante è un utente malintenzionato e conosce il codice di accesso PSTN sul sistema, in genere **9**, può comporre **9** quindi qualsiasi numero di destinazione che desidera raggiungere.

Soluzione 1

Per ridurre questo rischio, è necessario configurare la **connessione diretta verso l'interno**. In questo modo, il gateway Cisco inoltra la chiamata in entrata direttamente alla destinazione che corrisponde al DNIS in entrata.

Esempio di configurazione

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

Per il corretto funzionamento di DID, verificare che la chiamata in entrata corrisponda al dial-peer

POTS corretto in cui è configurato il comando **direct-inward-dial**. In questo esempio, il sistema T1 PRI è collegato alla porta 1/0:23. Per trovare la corrispondenza con il dial peer in entrata corretto, usare il comando **call-number** dial peer **in entrata** sotto il dial peer DID POTS.

Esempio 2

Nel sito 1, il CME è collegato alla PSTN tramite un T1 PRI trunk. Il provider PSTN fornisce **40855512.** e **40855513.** Intervalli DID per il sito CME 1. Pertanto tutte le chiamate PSTN destinate a 4085551200 - 4085551299 e 408551300 - 408551399 vengono instradate in entrata verso il CME.

Configurazione non corretta:

Se si configura un dial-peer in entrata, come nella configurazione di esempio illustrata in questa sezione, è ancora possibile che si verifichi una frode del pedaggio. Il problema di questo dial-peer in ingresso è che corrisponde solo alle chiamate in ingresso a **40852512.** e quindi applica il servizio DID. Se una chiamata PSTN arriva in **40852513.**, il dial-peer delle porte in ingresso non corrisponde e quindi il servizio DID non viene applicato. Se non viene trovata una corrispondenza tra un dial-peer in entrata e DID, viene utilizzato il dial-peer predefinito 0. DID è disabilitato per impostazione predefinita sul dial-peer 0.

Esempio di configurazione

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

Configurazione corretta

Nell'esempio seguente viene illustrato il modo corretto per configurare il servizio DID su un dial-peer in ingresso:

Esempio di configurazione

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

Per ulteriori informazioni su DID per le porte vocali digitali T1/E1, fare riferimento alla configurazione DID per i peer di composizione POTS.

Nota: l'uso di DID **non** è necessario quando si utilizza il PLAR (Private-Line Automatic Ringdown) su una porta voce o quando si utilizza uno script di servizio, ad esempio Auto-Attendant (AA), sul dial-peer in entrata.

Configurazione di esempio - PLAR

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

Configurazione di esempio: script di servizio

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

Restrizioni di accesso al servizio fuori orario

Riassunto

La limitazione dei pedaggi fuori orario è un nuovo strumento di sicurezza disponibile in CME 4.3/7.0 che consente di configurare i criteri di limitazione dei pedaggi in base alla data e all'ora. È possibile configurare i criteri in modo che agli utenti non sia consentito effettuare chiamate a numeri predefiniti durante determinate ore del giorno o in qualsiasi momento. Se è stato configurato il criterio di blocco delle chiamate 7x24 al di fuori dell'orario di ufficio, viene limitata anche la serie di numeri che possono essere immessi da un utente interno per impostare **call-forward all**.

Nota: si tratta di una **minaccia interna**.

Esempio 1

In questo esempio vengono definiti diversi modelli di cifre per le quali le chiamate in uscita vengono bloccate. I modelli 1 e 2, che bloccano le chiamate a numeri esterni che iniziano con "1" e "011", vengono bloccati dal lunedì al venerdì prima delle 7.00 e dopo le 19.00, il sabato prima delle 7.00 e dopo le 13.00 e tutta la domenica. Modello 3 blocca le chiamate a 900 numeri 7 giorni alla settimana, 24 ore al giorno.

Esempio di configurazione

```
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
```

Per ulteriori informazioni sulla limitazione del numero di telefono, fare riferimento a Configurazione del blocco delle chiamate.

Classe di restrizione

Riassunto

Se si desidera un controllo granulare quando si configura la limitazione di pedaggio, è necessario utilizzare la classe di limitazione (COR). Per ulteriori informazioni, fare riferimento al documento sulla classe di restrizione: Esempio per ulteriori informazioni.

Restrizioni alle frodi dovute ai pedaggi H.323 / SIP Trunks

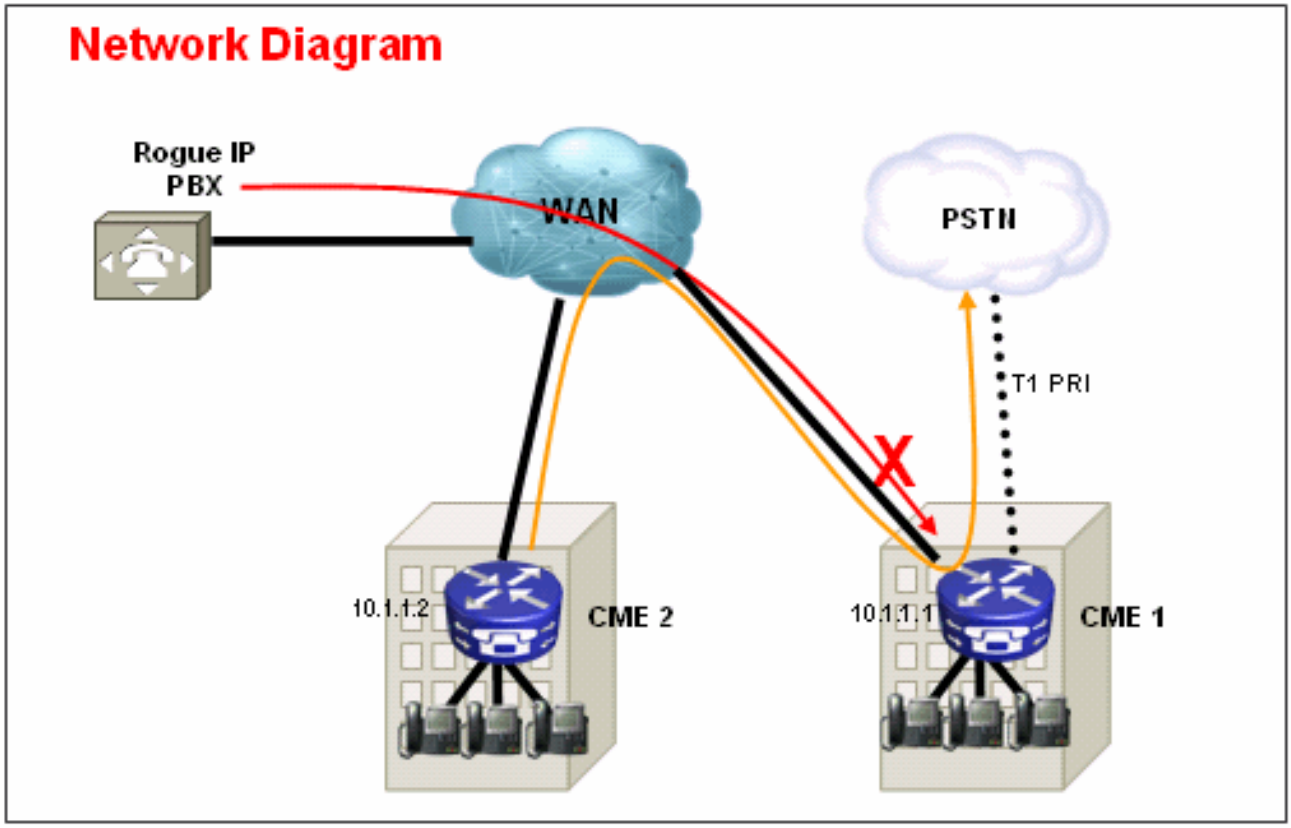
Riassunto

Nei casi in cui un sistema CME è connesso tramite WAN ad altri dispositivi CME tramite un SIP o un trunk H.323, è possibile limitare l'accesso trunk SIP/H.323 al CME in modo da impedire agli utenti abusivi di utilizzare il sistema per inoltrare illegalmente le chiamate alla PSTN.

Nota: si tratta di una **minaccia esterna**.

Esempio 1

In questo esempio, CME 1 dispone di connettività PSTN. CME 2 è collegato sulla WAN a CME 1 attraverso un trunk H.323. Per proteggere il CME 1, è possibile configurare un access-list e applicarlo in entrata sull'interfaccia WAN e quindi consentire solo il traffico IP da CME 2. In questo modo il Rogue IP PBX non può inviare chiamate VOIP attraverso CME 1 alla PSTN.



Soluzione

Non consentire all'interfaccia WAN su CME 1 di accettare traffico proveniente da dispositivi non autorizzati che non riconosce. Si noti che alla fine di un elenco degli accessi è presente un'istruzione implicita di RIFIUTO. Se vi sono più dispositivi da cui si desidera consentire il traffico IP in entrata, aggiungere l'indirizzo IP del dispositivo all'elenco degli accessi.

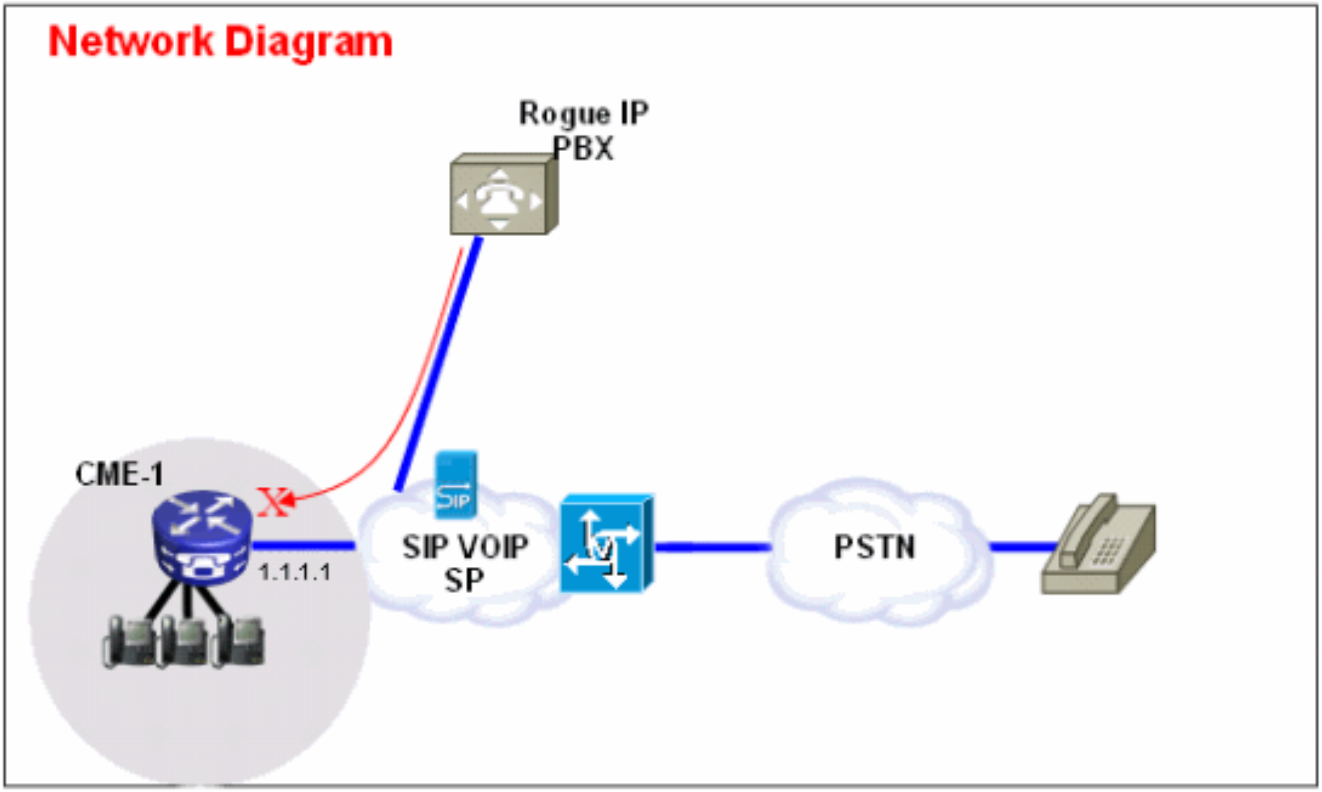
Configurazione di esempio: CME 1

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

Esempio 2

In questo esempio, CME 1 è connesso al provider SIP per la connettività PSTN con la configurazione di esempio fornita in Cisco CallManager Express (CME) SIP Trunking Configuration Example.

Poiché CME 1 è disponibile su Internet, è possibile che si verifichino *frodi* nel *pagamento del pedaggio* se un utente malintenzionato cerca negli indirizzi IP pubblici le porte conosciute per la segnalazione H.323 (TCP 1720) o SIP (UDP o TCP 5060) e invia messaggi SIP o H.323 che indirizzano le chiamate dal trunk SIP alla PSTN. Gli abusi più comuni in questo caso sono l'utente malintenzionato effettua più chiamate internazionali attraverso il SIP o H.323 trunk e induce il proprietario del CME 1 a pagare per queste chiamate di frode pedaggio - in alcuni casi migliaia di dollari.



Soluzione

Per ridurre questo rischio, è possibile utilizzare più soluzioni. Se non si usa alcuna segnalazione VOIP (SIP o H.323) sui collegamenti WAN nell'interfaccia CME 1, questa deve essere bloccata il più possibile usando le tecniche del firewall sull'interfaccia CME 1 (Access-lists o ACL).

1. Proteggere l'interfaccia WAN con il firewall Cisco IOS® su CME 1:Ciò significa che è consentito solo il traffico SIP o H.323 noto in arrivo sull'interfaccia WAN. Tutto il resto del traffico SIP o H.323 è bloccato. È quindi necessario conoscere gli indirizzi IP utilizzati dallo Storage Processor (SP) SIP VOIP per la segnalazione sul trunk SIP. Questa soluzione presuppone che l'SP sia disposto a fornire tutti gli indirizzi IP o i nomi DNS utilizzati nella rete. Inoltre, se si utilizzano i nomi DNS, la configurazione richiede che sia raggiungibile un server DNS in grado di risolverli. Inoltre, se l'SP modifica uno degli indirizzi all'estremità, la configurazione deve essere aggiornata su CME 1. Queste righe devono essere aggiunte in aggiunta alle voci ACL già presenti sull'interfaccia WAN.Configurazione di esempio: 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. Verificare che le chiamate in ingresso nel trunk SIP **NON** vengano reinserite:Ciò implica che la configurazione CME 1 consente solo il hairpin SIP - SIP delle chiamate a uno specifico intervallo di numeri PSTN noti, tutte le altre chiamate sono bloccate. È necessario configurare i dial-peer in entrata specifici per i numeri PSTN che entrano nel trunk SIP e che sono mappati alle estensioni o agli operatori automatici o alla segreteria telefonica su CME 1. Tutte le altre chiamate a numeri che non fanno parte dell'intervallo di numeri PSTN CME 1 sono bloccate. Nota, questa opzione non influisce sugli inoltri di chiamata/trasferimenti a messaggi vocali (Cisco Unity Express) e inoltrare tutti i numeri PSTN dai telefoni IP sul CME 1, poiché la chiamata iniziale è ancora indirizzata verso un'estensione sul CME 1.Configurazione di esempio: 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. Utilizzare le regole di conversione per bloccare stringhe di composizione specifiche:La maggior parte delle frodi a livello di pedaggio comporta chiamate internazionali. Di conseguenza, è possibile creare un dial-peer in ingresso specifico che corrisponda a specifiche stringhe composte e blocchi le chiamate a tali stringhe. La maggior parte dei CME utilizza un codice di accesso specifico, ad esempio 9, per le chiamate in uscita e il codice di composizione internazionale negli Stati Uniti è 011. Di conseguenza, la stringa di composizione più comune da bloccare negli Stati Uniti è 9011 + qualsiasi cifra successiva che venga inserita nel trunk SIP.Configurazione di esempio: 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
```

Strumenti di limitazione delle feature

Modello di trasferimento

Riassunto

I trasferimenti a tutti i numeri ad eccezione di quelli sui telefoni IP SCCP locali vengono bloccati automaticamente per impostazione predefinita. Durante la configurazione, è possibile consentire i trasferimenti a numeri non locali. Il comando **transfer-pattern** viene usato per consentire il trasferimento di chiamate di telefonia da telefoni IP SCCP di Cisco a telefoni diversi da telefoni IP Cisco, come chiamate PSTN esterne o telefoni su un altro sistema CME. È possibile utilizzare il modello **transfer-pattern** per limitare le chiamate solo alle estensioni interne o forse limitare le chiamate ai numeri PSTN solo in un determinato indicativo località. In questi esempi viene illustrato come utilizzare il comando **transfer-pattern** per limitare le chiamate a numeri diversi.

Nota: si tratta di una **minaccia interna**.

Esempio 1

Consenti agli utenti di trasferire le chiamate in uscita solo all'indicativo località 408. In questo esempio, si presume che il CME sia configurato con un dial-peer con un modello di destinazione di 9T.

Esempio di configurazione

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

Modello di trasferimento bloccato

Riassunto

In Cisco Unified CME 4.0 e versioni successive, è possibile impedire ai singoli telefoni di trasferire le chiamate a numeri abilitati globalmente per il trasferimento. Il comando **transfer-pattern locked** sostituisce il comando **transfer-pattern** e disabilita il trasferimento delle chiamate verso qualsiasi destinazione che deve essere raggiunta da un dial-peer POTS o VoIP. Sono inclusi i numeri PSTN, altri gateway voce e Cisco Unity Express. In questo modo, i singoli telefoni non verranno tassati quando le chiamate vengono trasferite all'esterno del sistema Cisco Unified CME. Il blocco del trasferimento di chiamata può essere configurato per singoli telefoni o come parte di un modello applicato a un insieme di telefoni.

Nota: si tratta di una **minaccia interna**.

Esempio 1

In questa configurazione di esempio, al numero 1 non è consentito utilizzare il modello di trasferimento (definito globalmente) per trasferire le chiamate, mentre al numero 2 è consentito utilizzare il modello di trasferimento definito in servizio di telefonia per trasferire le chiamate.

Esempio di configurazione

```
ephone-template 1
```

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

Trasferisci lunghezza massima

Riassunto

Il comando **transfer max-length** specifica il numero massimo di cifre che l'utente può comporre quando viene trasferita una chiamata. Il comando **transfer-pattern max-length** esegue il override del comando **transfer-pattern** e applica le cifre massime consentite per la destinazione del trasferimento. L'argomento specifica il numero di cifre consentite in un numero a cui viene trasferita una chiamata. Intervallo: da 3 a 16. Predefinito: 16.

Nota: si tratta di una **minaccia interna**.

Esempio 1

Questa configurazione permette solo ai telefoni a cui è applicato questo modello di telefono di essere trasferiti a destinazioni che hanno una lunghezza massima di quattro cifre.

Esempio di configurazione

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

Lunghezza massima inoltro di chiamata

Riassunto

Per limitare il numero di cifre che è possibile immettere con il tasto software CfwdALL su un telefono IP, usare il comando **call-forward max-length** in modalità di configurazione phone-dn o phone-dn-template. Per rimuovere le limitazioni sul numero di cifre che è possibile immettere, utilizzare la forma **no** di questo comando.

Nota: si tratta di una **minaccia interna**.

Esempio 1

In questo esempio, l'estensione di directory 101 può eseguire un inoltro a qualsiasi estensione di lunghezza compresa tra una e quattro cifre. Qualsiasi inoltro di chiamata a destinazioni con più di quattro cifre ha esito negativo.

Esempio di configurazione

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

o

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

Nessuna chiamata locale di inoltro

Riassunto

quando si usa il comando **no forward local-call** in modalità di configurazione phone-dn, le chiamate interne a una particolare phone-dn a cui si applica **no forward local-call** non vengono inoltrate se la phone-dn è occupata o non risponde. Se un chiamante interno suona questa linea telefonica e la linea telefonica è occupata, il chiamante sente un segnale occupato. Se un chiamante interno squilla questo telefono-dn e non risponde, il chiamante sente un segnale di ritorno. La chiamata interna non viene inoltrata anche se per il telefono-dn è abilitato il trasferimento delle chiamate.

Nota: si tratta di una **minaccia interna**.

Esempio 1

In questo esempio, l'estensione 222 chiama l'estensione 3675 e sente un segnale di ritorno o occupato. Se un chiamante esterno raggiunge l'interno 3675 e non c'è risposta, la chiamata viene inoltrata all'interno 4000.

Esempio di configurazione

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

Disattiva registrazione automatica sul sistema CME

Riassunto

Quando la funzione **auto-reg-phone** è abilitata in telephony-service su un sistema SCCP CME, i nuovi telefoni IP collegati al sistema vengono registrati automaticamente e se la funzione **auto assign** è configurata per assegnare automaticamente i numeri di interno, un nuovo telefono IP può effettuare chiamate immediatamente.

Nota: si tratta di una **minaccia interna**.

Esempio 1

In questa configurazione, viene configurato un nuovo sistema CME che richiede l'aggiunta manuale di un numero telefonico affinché il numero possa registrarsi sul sistema CME e utilizzarlo per effettuare chiamate di telefonia IP.

Soluzione

Èpossibile disattivare la funzione **auto-reg-phone** sotto il servizio di telefonia in modo che i nuovi telefoni IP collegati a un sistema CME non si registrino automaticamente nel sistema CME.

Esempio di configurazione

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

Esempio 2

Se si usa SCCP CME e si intende registrare i telefoni SIP Cisco sul sistema, è necessario configurare il sistema in modo che gli endpoint SIP debbano autenticarsi con un nome utente e una password. A tale scopo, è sufficiente configurare quanto segue:

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

Per ulteriori informazioni, fare riferimento al documento SIP: Configurazione di Cisco Unified CME per una guida alla configurazione più completa di SIP CME.

Strumenti di restrizione Cisco Unity Express

Secure Cisco Unity Express: Accesso PSTN AA

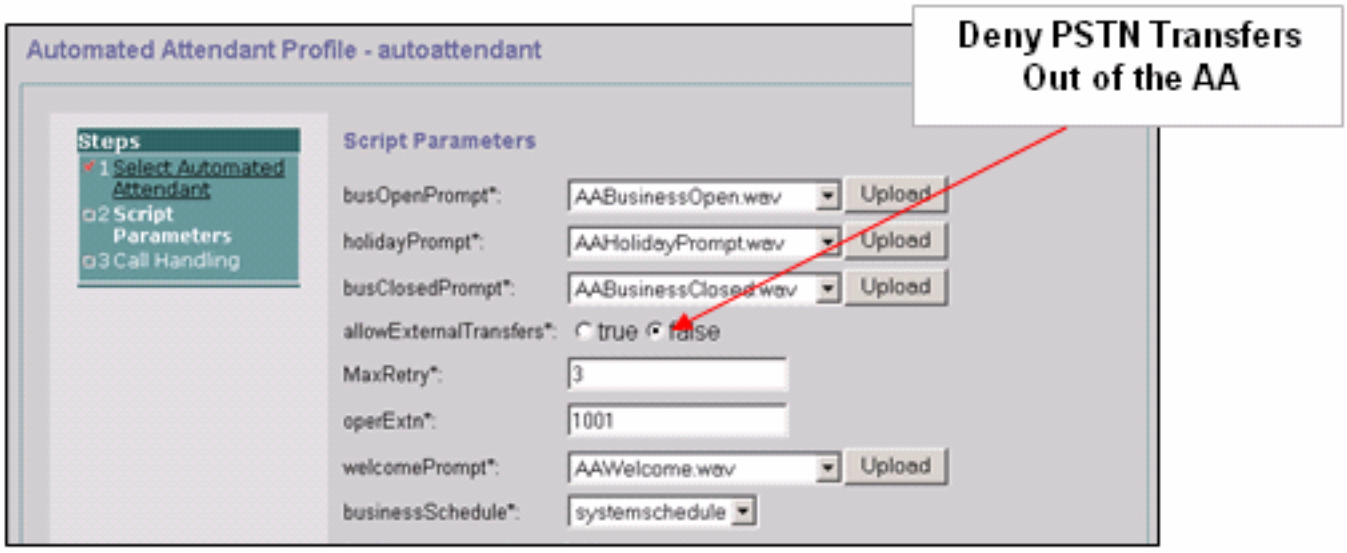
Riassunto

Quando il sistema è configurato in modo che le chiamate in entrata vengano inoltrate all'operatore automatico (AA) su Cisco Unity Express, potrebbe essere necessario disabilitare il trasferimento esterno alla rete PSTN da Cisco Unity Express ASA. Ciò non consente agli utenti esterni di comporre il numero in uscita su numeri esterni dopo aver raggiunto Cisco Unity Express ASA.

Nota: si tratta di una **minaccia esterna**.

Nota: Soluzione

Nota: disabilitare l'opzione **allowExternalTransfers** sull'interfaccia utente di Cisco Unity Express.



Nota: se è necessario l'accesso PSTN dall'ASA, limitare i numeri o l'intervallo di numeri considerati validi dallo script.

Tabelle di restrizione di Cisco Unity Express

Riassunto

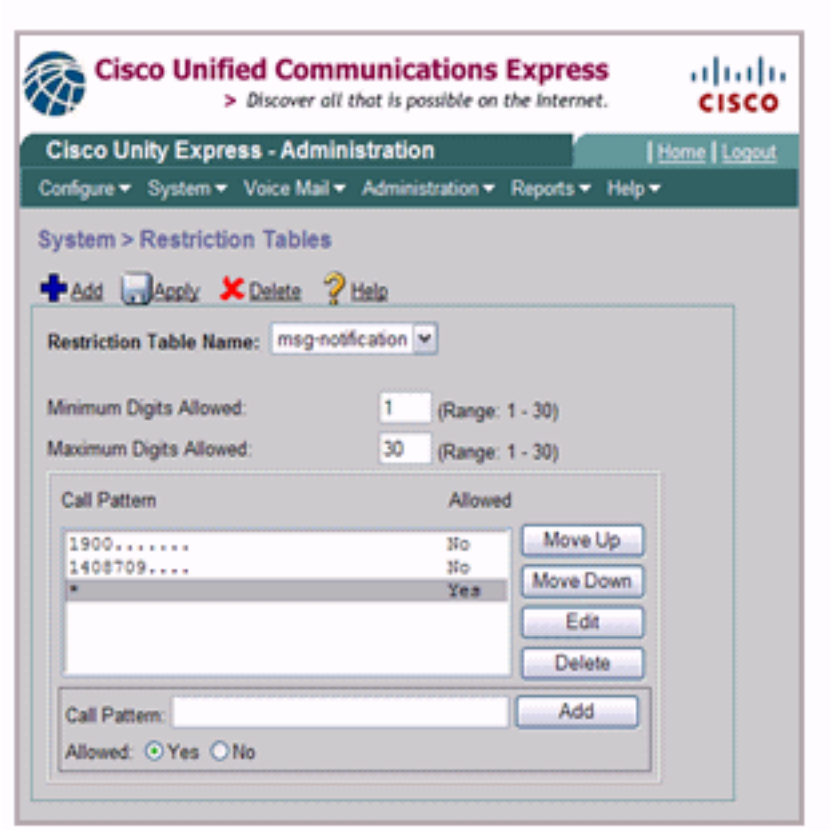
Èpossibile utilizzare le tabelle di restrizione di Cisco Unity Express per limitare le destinazioni che possono essere raggiunte durante una chiamata in uscita da Cisco Unity Express. La tabella di restrizione di Cisco Unity Express può essere utilizzata per prevenire frodi nel sistema di pedaggio e usi dannosi del sistema Cisco Unity Express per effettuare chiamate in uscita. Se si utilizza la tabella di restrizione di Cisco Unity Express, è possibile specificare i modelli di chiamata per la corrispondenza con caratteri jolly. Le applicazioni che utilizzano la tabella delle restrizioni di Cisco Unity Express includono:

- Fax
- Cisco Unity Express Live Replay
- Notifica messaggio
- Recapito messaggi non sottoscrittore

Nota: si tratta di una **minaccia interna**.

Soluzione

Per limitare i modelli di destinazione raggiungibili da Cisco Unity Express su una chiamata esterna in uscita, configurare il **modello di chiamata** in **Sistema > Tabelle delle restrizioni** dalla GUI di Cisco Unity Express.



Registrazione chiamate

CDR migliorato

Èpossibile configurare il sistema CME in modo da acquisire il CDR avanzato e registrare il CDR sul flash del router o su un server FTP esterno. Questi record possono quindi essere utilizzati per ripercorrere le chiamate per verificare se si sono verificati abusi da parte di parti interne o esterne.

La funzionalità di accounting dei file introdotta con CME 4.3/7.0 in Cisco IOS versione 12.4(15)XY offre un metodo per acquisire i record contabili in formato CSV (Comma Separated Value) e memorizzarli in un file flash interno o in un server FTP esterno. Espande il supporto dell'accounting gateway, che include anche i meccanismi AAA e syslog per la registrazione delle informazioni di accounting.

Il processo di accounting raccoglie dati di accounting per ogni tappa della chiamata creata su un gateway voce Cisco. È possibile utilizzare queste informazioni per le attività di post-elaborazione, ad esempio per generare record di fatturazione e per l'analisi della rete. I gateway voce Cisco acquisiscono i dati contabili sotto forma di Call Detail Records (CDR) contenenti gli attributi definiti da Cisco. Il gateway può inviare i dati CDR a un server RADIUS, a un server syslog e, con il nuovo metodo file, alla memoria flash o a un server FTP in formato .csv.

Per ulteriori informazioni sulle funzionalità avanzate di CDR, fare riferimento agli esempi di CDR.

Informazioni correlate

- Best practice per la sicurezza di Cisco Unified Communications Manager Express
- Guida per l'amministratore di Cisco Communications Manager Express
- Guida per l'amministratore di Cisco Communications Manager Express - Blocco delle

chiamate
- Informazioni sulla corrispondenza Dial-Peer sulle piattaforme IOS
- Traduzione del numero tramite profili di traduzione vocale
- Guida alla progettazione della rete di riferimento per la soluzione CME
- Documentazione e supporto tecnico – Cisco Systems