# Funzione Voice Source-Group

## Sommario



## Introduzione

Questo documento descrive la funzione Voice Source-Group (VSG) di Cisco IOS® che consente al gateway, o Cisco Unified Border Element (CUBE), di identificare l'origine e controllare il routing delle chiamate VoIP.

> **Nota:** In questo documento, i termini CUBE e IP-to-IP Gateway (IPIPGW) sono usati indifferentemente.

## Premesse

In una situazione in cui si desidera implementare una frode a livello di pedaggio bloccando la segnalazione di chiamata da indirizzi IP non autorizzati, è possibile usare la funzione di prevenzione delle frodi a livello di pedaggio, introdotta in Cisco IOS 15.1(2)T. Per ulteriori informazioni, fare riferimento all'articolo sulla funzionalità di prevenzione delle frodi a livello di pedaggio nella versione 15.1(2)T.

Tuttavia, se si dispone di una versione precedente di Cisco IOS o si necessita di questi controlli aggiuntivi, è consigliabile prendere in considerazione la funzione VSG:

- codice causa di rifiuto configurabile
- modificare i numeri da chiamare o da chiamare in base all'origine della chiamata
- controllare l'instradamento (ad esempio, il percorso verso un vettore specifico)

La funzione VSG consente di identificare l'origine della chiamata VoIP in modo che i servizi selezionati vengano forniti alla chiamata. Questi servizi includono la conversione dei numeri, la corrispondenza dial-peer in entrata e il controllo dell'accettazione/rifiuto delle chiamate. Inoltre, la funzione consente di controllare l'indirizzamento della chiamata (consentita) in modi diversi dall'applicazione di frode. Ad esempio, è possibile associare traduzioni vocali al VSG per modificare i numeri chiamanti/chiamati *PRIMA che* la chiamata raggiunga il dial-peer in entrata. Questa funzionalità è molto utile perché le chiamate con lo ***stesso*** numero composto possono essere instradate attraverso dial-peer in ingresso diversi.

Per effettuare l'identificazione, VSG usa l'Access Control List (ACL) di Cisco IOS.

# Attributi VSG

## Elenco accessi

Per specificare gli indirizzi IP delle origini da cui le chiamate vengono accettate ed elaborate, viene configurato un ACL IOS standard. All'ACL viene quindi fatto riferimento nel VSG associato.

Se l'indirizzo IP dell'origine (di una chiamata in arrivo) non ha una voce nell'ACL, il gateway NON associa il VSG alla chiamata. Ciò significa che la chiamata non è soggetta ad alcuna delle manipolazioni configurate in VSG.

Se le chiamate da un particolare indirizzo IP devono essere rifiutate, quell'indirizzo IP deve essere incluso in un'istruzione **deny** sotto l'ACL.

In alternativa, l'istruzione **deny any** è configurata per rifiutare le chiamate da qualsiasi indirizzo IP non esplicitamente consentito o negato.

## Causa disconnessione

Il codice causa con cui la chiamata in ingresso viene rifiutata è configurabile in VSG. Per impostazione predefinita, la causa della disconnessione è **no-service**. Il risultato è l'**errore interno del server 500** per le chiamate Session Initiation Protocol (SIP) e **ReleaseComplete** con codice causa 63 (servizio o opzione non disponibile, non specificato) per le chiamate H.323.

Motivi di disconnessione definiti dall'utente:

- Numero non valido
- Numero non assegnato
- Utente occupato
- Chiamata rifiutata

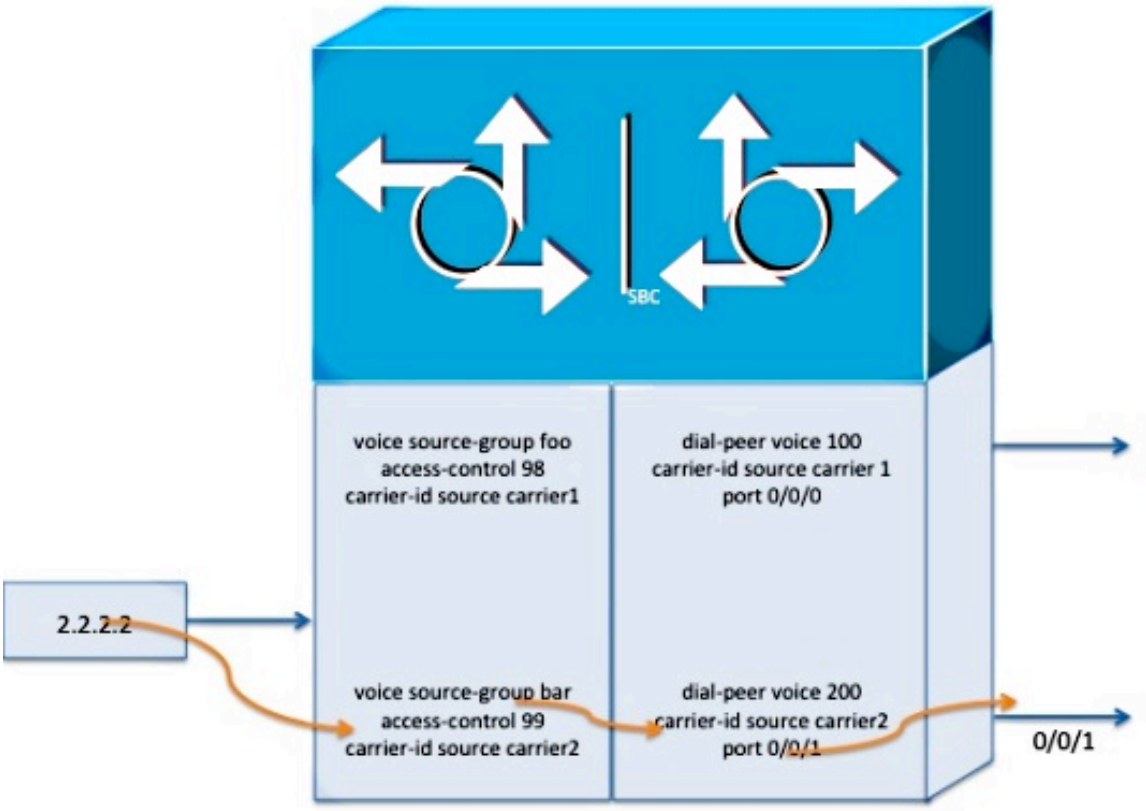
## ID vettore

L'attributo carrier-ID è configurato sul VSG in modo che le chiamate che corrispondono all'ACL associato siano contrassegnate con carrier-ID. In questo modo, le chiamate con *lo stesso* numero chiamato verranno instradate (sul lato in uscita) attraverso diversi vettori, in base all'indirizzo IP

dell'origine. Ad esempio, se si dispone di due gruppi di indirizzi IP, le chiamate da un gruppo di indirizzi possono passare attraverso un VSG e possono essere contrassegnate con un ID vettore e le chiamate (allo stesso numero chiamato) dall'altro gruppo possono essere contrassegnate con un ID vettore diverso. Di seguito è riportato un esempio:

```
voice source-group foo
access-control 98
carrier-id source carrier1

voice source-group bar
access-control 99
carrier-id source carrier2

dial-peer voice 100 pots
carrier-id source carrier1
...

dial-peer voice 200 pots
carrier-id source carrier2
...

ip access-control standard 98
permit 1.1.1.1

ip access-control standard 99
permit 2.2.2.2
deny any any
```

Con la configurazione precedente, le chiamate dalla versione 1.1.1.1 vengono instradate attraverso il dial-peer 100 e le chiamate dalla versione 2.2.2.2 vengono instradate attraverso il dial-peer 200.




### Trunk-Group-Label

L'etichetta trunk-group-label funziona in modo simile all'ID vettore. La chiamata VoIP in arrivo è contrassegnata con il gruppo trunk configurato, che viene quindi utilizzato per selezionare il dial-peer appropriato quando la chiamata viene instradata attraverso la gamba in uscita.

### ID zona H.323

Questa opzione è applicabile solo al protocollo H.323 e viene utilizzata per far corrispondere la zona di origine della chiamata H.323 in arrivo a un VSG. L'ID della zona di origine viene trasportato in una chiamata H.323 in arrivo che utilizza il protocollo di segnalazione H.323V4 e proviene da un gatekeeper H.323.

## Più gruppi di servizi voce

Èpossibile configurare più VSG su un IPIPGW in modo che ciascuno consenta o non consenta le chiamate da un set diverso di indirizzi IP.

Se si hanno più VSG, aggiungere **deny any** ONLY all'ACL dell'ultimo VSG. In caso contrario, se un ACL intermedio ha **negato** un indirizzo IP, le chiamate da qualsiasi indirizzo IP esplicitamente

autorizzato in un altro ACL verranno comunque rifiutate se tale ACL è DOPO quello specificato con il comando **deny any**. Di seguito sono riportati due VSG:

```
voice source-group foo
access-list 98

voice source-group bar
access-list 99
```

Di seguito sono riportati gli ACL dei VSG:

```
ip access-list standard 98
permit 1.1.1.1
deny any

ip access-list standard 99
permit 2.2.2.2
deny any
```

Nell'esempio, le chiamate alla versione 2.2.2.2 vengono rifiutate, perché l'ACL che autorizza l'indirizzo IP è AFTER the ACL (98) with **deny any**.

Èpossibile utilizzare questo comando per confermare che le chiamate vengono rifiutate.

```
Router#test source-group ip-address 2.2.2.2
A source-group is found with ip address=2.2.2.2
An ip address 2.2.2.2 is rejected with disc-cause="no-service"
```

Per autorizzare la chiamata, è necessario rimuovere il comando **deny any** dall'elenco degli accessi 98.

```
ip access-list standard 98
permit 1.1.1.1
```

Èpossibile utilizzare nuovamente il comando **test source-group ip 2.2.2.2** per verificare che le chiamate dall'indirizzo IP in questione non vengano più rifiutate.

```
Router#test  source-group ip-address 2.2.2.2
A source-group is found with ip address=2.2.2.2
```

# Verifica

Il comando **test source-group *<VSG>*** può essere usato per verificare se le chiamate da un determinato indirizzo IP verranno elaborate da un VSG.

# Risoluzione dei problemi

Come accennato nella sezione precedente, il comando **test source-group *<VSG>*** è utile per determinare se una determinata chiamata verrà autorizzata o rifiutata. Inoltre, se la chiamata sarà consentita, questo comando mostrerà anche quale VSG effettuerà il ?routing? la chiamata. Analogamente, se la chiamata verrà rifiutata, verrà indicata la causa del rifiuto. Con questo comando viene trovato il servizio VSG di routing in base ad altri attributi, oltre all'indirizzo IP.

L'altro aiuto alla risoluzione dei problemi è il comando **debug voice-group** debug. Ad esempio, quando una chiamata H.323 viene rifiutata (con il codice causa predefinito), il debug genera questo output:

```
092347: .Apr  7 10:53:46.132: SIPG:src_grp_check_config() src_grp or src_grp
acl is defined
092348: .Apr  7 10:53:46.136: %VOICE_IEC-3-GW: H323: Internal Error (H323
Interworking Error): IEC=1.1.127.5.21.0 on callID 264
```

# Avvertenze e avvertenze

Ecco alcune importanti avvertenze relative al VSG:

- VSG è molto meno flessibile rispetto all'applicazione di toll-truffa. Impedisce alle chiamate di raggiungere il livello di controllo delle chiamate e non registra alcun messaggio di errore. Ciò è valido indipendentemente dal fatto che una chiamata sia consentita o bloccata.
- In alcuni casi si è verificato un problema con il protocollo GLBP (Global Load Balancing Protocol) abilitato per il gateway. Sembra esserci una dipendenza oscura dall'ordine relativo in cui GLBP e VSG sono configurati. In caso di problemi di questo tipo, attenersi alla seguente procedura: Disabilitare **GLBP**.Riapplicare **VSG**.Riavviare il **gateway**.Verificare il funzionamento di VSG.Abilitare **GLBP**.

# Informazioni correlate

- Informazioni sui miglioramenti relativi alle frodi a pagamento in 15.1(2)T
- Metodi di sicurezza SIP dello strumento Cisco CCA
- Documentazione e supporto tecnico – Cisco Systems