Voice Source Group-Funktion

Inhalt

[Einführung](#)
[Hintergrundinformationen](#)
[VSG-Attribute](#)
[Zugriffsliste](#)
[Trennursache](#)
[Carrier-ID](#)
[Trunk-Group-Label](#)
[H.323-Zonen-ID](#)
[Mehrere Voice-Service-Gruppen](#)
[Überprüfen](#)
[Fehlerbehebung](#)
[Vorsichtsmaßnahmen und Hinweise](#)
[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird die Funktion der Voice Source Group (VSG) in Cisco IOS® beschrieben, mit der das Gateway oder Cisco Unified Border Element (CUBE) die Quelle und die Steuerung der Weiterleitung von VoIP-Anrufen identifizieren kann.

> **Hinweis**: Die Begriffe CUBE und IP-to-IP Gateway (IPGW) werden in diesem Dokument synonym verwendet.

Hintergrundinformationen

Wenn Sie eine Situation festgestellt haben, in der Sie Gebührenbetrug implementieren möchten, indem Sie die Anrufsignalisierung von nicht autorisierten IP-Adressen blockieren, können Sie die Funktion zur Verhinderung von Gebührenbetrug verwenden, die in Cisco IOS 15.1(2)T eingeführt wurde. Weitere Informationen finden Sie im Artikel [zur Verhinderung von Gebührenbetrug in IOS, Version 15.1(2)T](#).

Wenn Sie jedoch über eine ältere Version von Cisco IOS verfügen oder diese zusätzlichen Steuerelemente benötigen, sollten Sie die VSG-Funktion in Betracht ziehen:

- konfigurierbarer Ablehnungsursachencode
- Anrufer-/angerufene Nummern ändern, abhängig davon, von wem der Anruf stammt
- Steuerungs-Routing (z. B. Route zu einem bestimmten Carrier)

Mit der VSG-Funktion können Sie die Quelle des VoIP-Anrufs so identifizieren, dass ausgewählte Services für den Anruf bereitgestellt werden. Zu diesen Services gehören die Nummernübersetzung, die eingehende DFÜ-Peer-Abstimmung und die Anrufannahme-/Ablehnungskontrolle. Darüber hinaus können Sie mit dieser Funktion die Weiterleitung von (zulässigen) Anrufen so steuern, wie es die Anwendung zum Gebührenbetrug nicht kann. Beispielsweise können Sie dem VSG Sprachübersetzungen zuordnen, um die anrufenden/angerufenen Nummern zu bearbeiten, *BEVOR* der Anruf den eingehenden DFÜ-Peer erreicht. Dies ist besonders wichtig, da Anrufe mit ***derselben*** gewählten Nummer über verschiedene eingehende DFÜ-Peers weitergeleitet werden können.

VSG verwendet die Cisco IOS-Zugriffskontrollliste (ACL), um die Identifizierung zu ermöglichen.

VSG-Attribute

Zugriffsliste

Eine Standard-IOS-ACL wird konfiguriert, um die IP-Adressen der Quellen anzugeben, von denen Anrufe angenommen und verarbeitet werden. Auf die ACL wird dann im zugehörigen VSG verwiesen.

Wenn die IP-Adresse der Quelle (eines eingehenden Anrufs) keinen Eintrag in der ACL hat, ordnet das Gateway dem Anruf NICHT das VSG zu. Das bedeutet, dass der Anruf keiner der vom VSG konfigurierten Manipulationen unterliegt.

Wenn Anrufe von einer bestimmten IP-Adresse abgelehnt werden sollen, muss diese IP-Adresse in einer **deny-**Anweisung unter der ACL enthalten sein.

Alternativ dazu wird **die** Anweisung **"Ablehnen einer** Anweisung" konfiguriert, um Anrufe von einer IP-Adresse abzulehnen, die nicht explizit zugelassen oder abgelehnt wurde.

Trennursache

Der Ursachencode, mit dem der eingehende Anruf abgelehnt wird, ist unter dem VSG konfigurierbar. Standardmäßig ist die Disconnect-Ursache **kein Service**. Dies führt zu dem **500 internen Serverfehler** für SIP-Anrufe (Session Initiation Protocol) und **ReleaseComplete** mit Ursachencode 63 (Service oder Option nicht verfügbar, nicht angegeben) für H.323-Anrufe.

Die Gründe für eine vom Benutzer definierte Trennung sind:

- Ungültige Nummer
- Nicht zugewiesene Nummer
- Benutzer beschäftigt
- Anruf abgelehnt

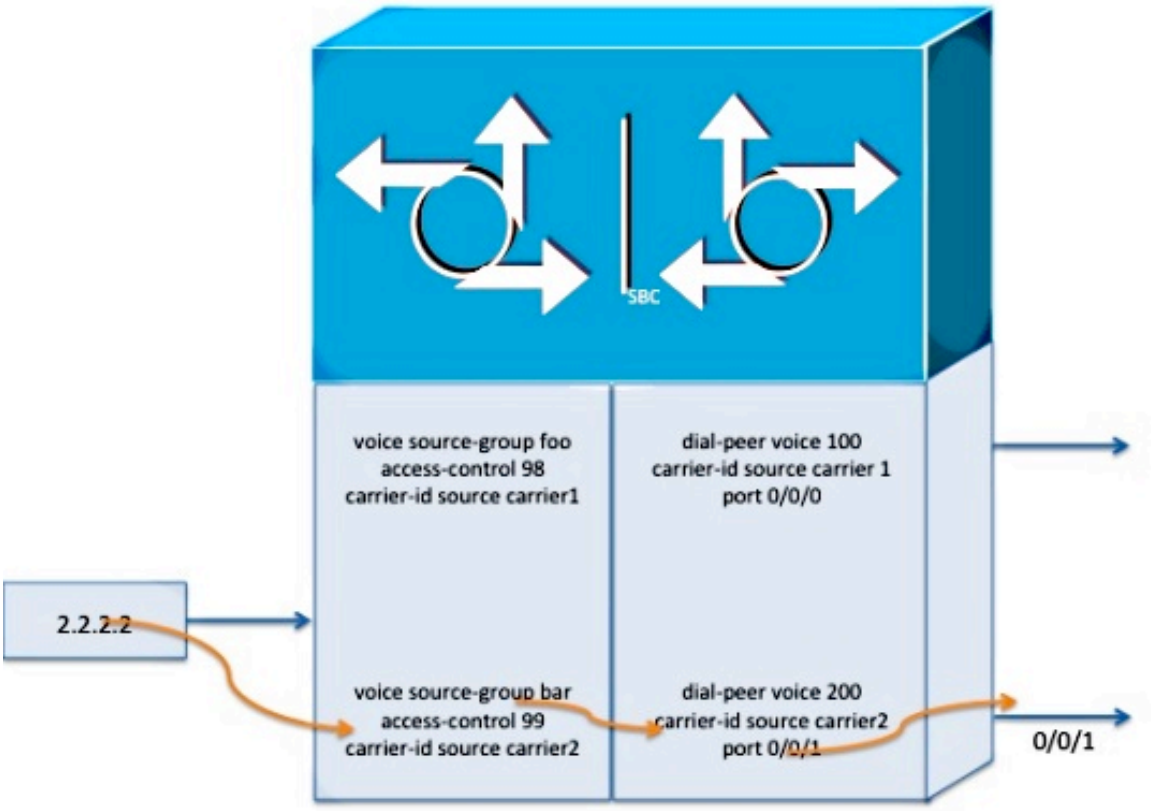
Carrier-ID

Das Carrier-ID-Attribut wird auf dem VSG so konfiguriert, dass Anrufe, die mit der zugehörigen

ACL übereinstimmen, mit der Carrier-ID versehen werden. Dadurch können Anrufe mit *derselben* angerufenen Nummer (auf der ausgehenden Seite) über verschiedene Carrier weitergeleitet werden, basierend auf der IP-Adresse der Quelle. Wenn Sie z. B. über zwei Gruppen von IP-Adressen verfügen, können Anrufe von einer Gruppe von Adressen über ein VSG weitergeleitet und mit einer Carrier-ID getaggt werden. Anrufe (zur gleichen angerufenen Nummer) von der anderen Gruppe können mit einer anderen Carrier-ID versehen werden. Hier ein Beispiel:

```
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
```

Bei der vorherigen Konfiguration werden Anrufe aus 1.1.1.1 über DFÜ-Peer 100 weitergeleitet, und Anrufe aus 2.2.2.2 werden über DFÜ-Peer 200 weitergeleitet.



Trunk-Group-Label

Das Trunk-Group-Label funktioniert ähnlich wie die Carrier-ID. Der eingehende VoIP-Anruf wird mit der konfigurierten Trunk-Gruppe gekennzeichnet, die dann verwendet wird, um den geeigneten DFÜ-Peer auszuwählen, wenn der Anruf über den ausgehenden Abschnitt weitergeleitet wird.

H.323-Zonen-ID

Dies gilt nur für das H.323-Protokoll und wird verwendet, um die Quellzone des eingehenden H.323-Anrufs an ein VSG abzugleichen. Die Quellzone-ID wird in einem eingehenden H.323-Anruf übertragen, der das H.323V4-Signalisierungsprotokoll verwendet und von einem H.323-Gatekeeper stammt.

Mehrere Voice-Service-Gruppen

Sie können mehrere VSGs auf einem IPGW konfigurieren, bei denen jedes einzelne Anrufe von einem anderen Satz von IP-Adressen zulässt oder untersagt.

Achten Sie darauf, **der** ACL des letzten VSG **jede** NUR **verweigern**, wenn Sie über mehrere VSGs

verfügen. Andernfalls werden Anrufe von einer IP-Adresse, die in einer anderen ACL explizit zulässig ist, **abgelehnt**, wenn diese ACL NACH der ACL mit der **Ablehnungsoption** lautet. Es gibt z. B. zwei VSGs:

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

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

Nachfolgend sind die ACLs für die VSGs aufgeführt:

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

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

In diesem Beispiel werden Anrufe aus 2.2.2.2 abgelehnt, da die Zugriffskontrollliste, die die IP-Adresse zulässt, "NACH" (AFTER) (98) lautet und **eine beliebige Zugriffskontrollliste verweigern**.

Mit diesem Befehl können Sie bestätigen, dass die Anrufe abgelehnt wurden.

```
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"
```

Um den Anruf zuzulassen, müssen Sie die **Option "Deny any"** aus der Zugriffsliste 98 entfernen.

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

Sie können den Befehl **test source-group ip 2.2.2.2** erneut verwenden, um zu überprüfen, ob Anrufe von der betreffenden IP-Adresse nicht mehr abgelehnt werden.

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

Überprüfen

Der Befehl **Test source-group *<VSG>*** kann für eine grundlegende Überprüfung verwendet werden - ob Anrufe von einer bestimmten IP-Adresse von einem VSG verarbeitet werden.

Fehlerbehebung

Wie im vorherigen Abschnitt erwähnt, ist der Befehl **für die Testquellengruppe *<VSG>*** hilfreich, um festzustellen, ob ein bestimmter Anruf zulässig oder abgelehnt wird. Wenn ein Anruf zulässig ist, zeigt dieser Befehl außerdem an, welches VSG die Route übernimmt. den Anruf. Wenn der Anruf abgelehnt wird, wird ebenfalls die Ablehnungsursache angezeigt. Mit diesem Befehl wird das Routing-VSG anhand anderer Attribute gefunden, zusätzlich zur IP-Adresse.

Die andere Hilfe zur Fehlerbehebung ist der Befehl **debug voice source-group** debug. Wenn z. B. ein H.323-Aufruf abgelehnt wird (mit dem Standard-Ursachencode), erzeugt der Debugger diese Ausgabe:

```
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
```

Vorsichtsmaßnahmen und Hinweise

Hier einige wichtige Vorbehalte zum VSG:

- VSG ist viel weniger flexibel als die Anwendung zum Gebührenbetrug. Sie verhindert, dass die Anrufe die Anrufsteuerungsebene erreichen, und protokolliert keine Fehlermeldungen. Dies gilt unabhängig davon, ob ein Anruf zulässig oder blockiert ist.
- Bei einigen ist ein Problem aufgetreten, wenn das Global Load Balancing Protocol (GLBP) für dieses Gateway aktiviert ist. Die Abhängigkeit von der relativen Reihenfolge, in der GLBP und VSG konfiguriert werden, scheint undurchsichtig zu sein. Gehen Sie wie folgt vor, wenn solche Probleme auftreten: Deaktivieren Sie **GLBP**.**VSG** erneut anwenden.Starten Sie das **Gateway neu**.Überprüfen/Überprüfen der Funktionsweise von VSGAktivieren Sie **GLBP**.

Zugehörige Informationen

- Informationen zu Neuerungen bei Gebührenbetrug in 15.1(2)T
- Cisco CCA Tool SIP-Sicherheitsmethoden
- Technischer Support und Dokumentation - Cisco Systems