Fonctionnalité Groupe de sources vocales

Contenu

[Introduction](#)
[Informations générales](#)
[Attributs VSG](#)
[Liste d'accès](#)
[Cause de déconnexion](#)
[ID du transporteur](#)
[Étiquette de groupe de faisceaux](#)
[ID de zone H.323](#)
[Plusieurs groupes de services vocaux](#)
[Vérification](#)
[Dépannage](#)
[Avertissements et cavernes](#)
[Informations connexes](#)

Introduction

Ce document décrit la fonctionnalité VSG (Voice Source-Group) de Cisco IOS® qui permet à la passerelle, ou Cisco Unified Border Element (CUBE), d'identifier la source et de contrôler le routage des appels VoIP.

> **Note**: Les termes CUBE et IPIPGW (IP-to-IP Gateway) sont utilisés de manière interchangeable dans tout ce document.

Informations générales

Si vous avez rencontré une situation dans laquelle vous souhaitez mettre en oeuvre une fraude à l'interurbain en bloquant la signalisation des appels à partir d'adresses IP non autorisées, vous pouvez utiliser la fonctionnalité de prévention des fraudes à l'interurbain, introduite dans Cisco IOS 15.1(2)T. Reportez-vous à l'article Toll-Fraud Prevention Feature in IOS Release 15.1(2)T pour plus d'informations.

Toutefois, si vous disposez d'une version antérieure de Cisco IOS ou si vous avez besoin de ces contrôles supplémentaires, vous devez considérer la fonctionnalité VSG :

- code cause-rejet configurable
- modifier les numéros d'appel/d'appel en fonction de l'origine de l'appel
- routage de contrôle (route vers un opérateur spécifique, par exemple)

La fonction VSG vous permet d'identifier la source de l'appel VoIP de sorte que les services sélectionnés soient fournis à l'appel. Ces services incluent la traduction de numéros, la mise en correspondance des homologues de numérotation entrante et le contrôle d'acceptation/rejet des appels. En outre, cette fonctionnalité vous permet de contrôler le routage de l'appel (autorisé) de manière que l'application de fraude à l'appel ne peut pas contrôler. Par exemple, vous pouvez associer des traductions vocales au VSG afin de manipuler les numéros d'appel/d'appel *AVANT* que l'appel n'atteigne le terminal de numérotation dial-peer entrant. Cette fonction est puissante car les appels avec le ***même*** numéro composé peuvent être acheminés via différents terminaux de numérotation dial-peer entrants.

VSG utilise la liste de contrôle d'accès (ACL) de Cisco IOS afin d'accomplir l'identification.

Attributs VSG

Liste d'accès

Une liste de contrôle d’accès IOS standard est configurée afin de spécifier les adresses IP des sources à partir desquelles les appels sont acceptés et traités. La liste de contrôle d’accès est ensuite référencée dans la passerelle VSG associée.

Si l'adresse IP de la source (d'un appel entrant) n'a pas d'entrée dans la liste de contrôle d'accès, la passerelle n'associe PAS la passerelle VSG à l'appel. Cela signifie que l'appel n'est soumis à aucune des manipulations configurées sous le VSG.

Si les appels d'une adresse IP particulière doivent être rejetés, cette adresse IP doit être incluse dans une instruction **deny** sous la liste de contrôle d'accès.

Sinon, l'instruction **deny any** est configurée afin de rejeter les appels de toute adresse IP qui n'est pas explicitement autorisée ou refusée.

Cause de déconnexion

Le code de cause avec lequel l'appel entrant est rejeté est configurable sous VSG. Par défaut, la cause de déconnexion est **sans service**. Cela se traduit par l'**erreur de serveur interne 500** pour les appels SIP (Session Initiation Protocol) et **ReleaseComplete** avec le code de cause 63 (Service ou option non disponible, non spécifié) pour les appels H.323.

Les raisons de déconnexion définies par l'utilisateur sont les suivantes :

- Nombre incorrect
- Numéro non affecté
- Utilisateur occupé
- Appel rejeté

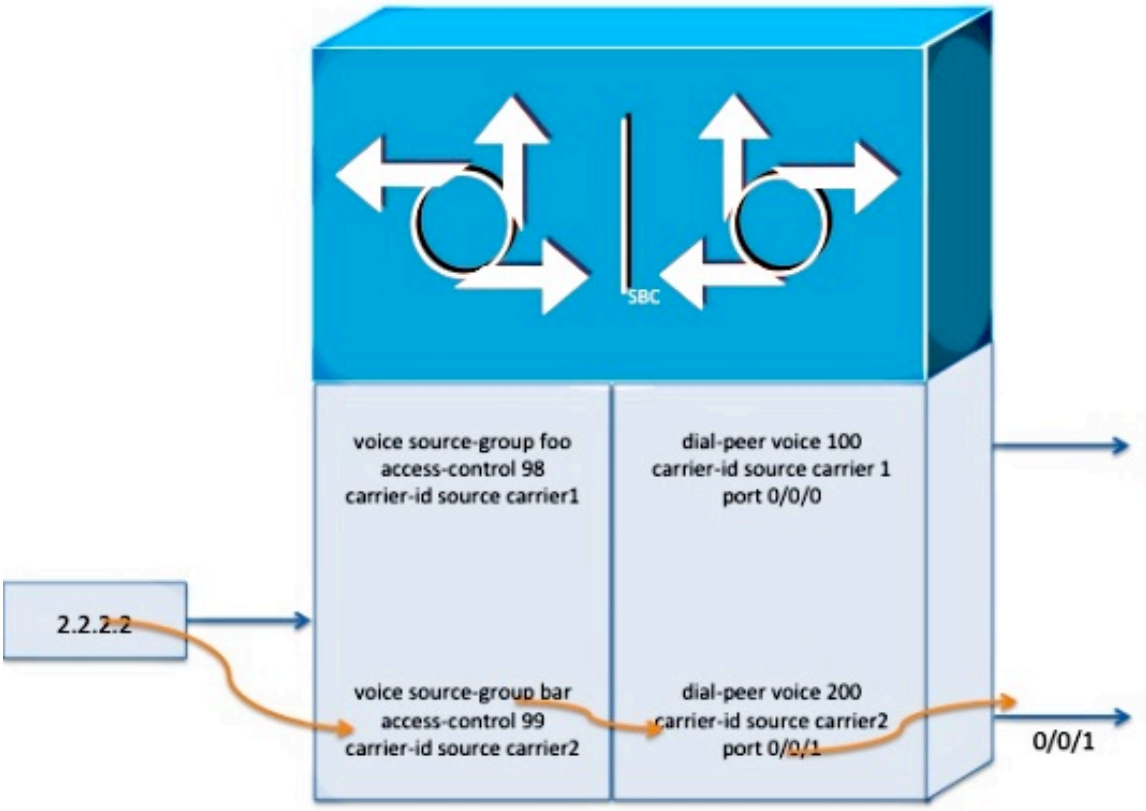
ID du transporteur

L'attribut carrier-ID est configuré sur le VSG de sorte que les appels qui correspondent à la liste de

contrôle d'accès associée soient marqués avec l'ID de transporteur. Cela permet de router les appels avec le *même* numéro appelé (côté sortant) via différents opérateurs, en fonction de l'adresse IP de la source. Par exemple, si vous avez deux groupes d'adresses IP, les appels d'un groupe d'adresses peuvent passer par un VSG et être marqués avec un ID d'opérateur, et les appels (au même numéro appelé) de l'autre groupe peuvent être marqués avec un ID d'opérateur différent. Voici un exemple :

```
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
```

Avec la configuration précédente, les appels de 1.1.1.1 sont acheminés via le terminal de numérotation dial-peer 100 et les appels de 2.2.2.2 sont acheminés via le terminal de numérotation dial-peer 200.



Étiquette de groupe de faisceaux

L'étiquette de groupe de faisceaux fonctionne de la même manière que l'ID de porteuse. L'appel VoIP entrant est étiqueté avec le groupe de faisceaux configuré, qui est ensuite utilisé afin de sélectionner le terminal de numérotation dial-peer approprié lorsque l'appel est acheminé via le tronçon sortant.

ID de zone H.323

Ceci s'applique uniquement au protocole H.323 et est utilisé afin de faire correspondre la zone source de l'appel H.323 entrant à un VSG. L'ID de zone source est transporté dans un appel H.323 entrant qui utilise le protocole de signalisation H.323V4 et provient d'un contrôleur d'accès H.323.

Plusieurs groupes de services vocaux

Vous pouvez configurer plusieurs VSG sur un IPIPGW où chacun autorise ou désautorise les appels d'un ensemble d'adresses IP différent.

Veillez à ajouter **deny any** UNIQUEMENT à la liste de contrôle d'accès du dernier VSG, lorsque

vous avez plusieurs VSG. Sinon, si une liste de contrôle d'accès intermédiaire a **refusé tout**, les appels de toute adresse IP explicitement autorisée dans une autre liste de contrôle d'accès seront toujours rejetés si cette liste est APRÈS la liste de contrôle d'accès avec le **refus any**. Par exemple, voici deux VSG :

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

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

Voici les listes de contrôle d'accès des 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
```

Dans cet exemple, les appels de 2.2.2.2 sont rejetés, car la liste de contrôle d'accès qui autorise l'adresse IP est AFTER (98) avec **deny any**.

Vous pouvez utiliser cette commande afin de confirmer que les appels sont rejetés.

```
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"
```

Pour autoriser l'appel, vous devez supprimer le **refus any** de la liste d'accès 98.

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

Vous pouvez utiliser à nouveau la commande **test source-group ip 2.2.2.2** afin de vérifier que les appels de l'adresse IP en question ne sont plus rejetés.

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

Vérification

La commande **test source-group *<VSG>*** peut être utilisée pour la vérification de base : si les appels d'une adresse IP donnée sont traités par un VSG.

Dépannage

Comme indiqué dans la section précédente, la commande **test source-group *<VSG>*** est utile pour déterminer si un appel donné est autorisé ou rejeté. En outre, si l'appel est autorisé, cette commande indique également quel VSG routera ? l'appel. De même, si l'appel est rejeté, il indique la cause du rejet. Cette commande recherche la passerelle VSG de routage en fonction d'autres

attributs, en plus de l'adresse IP.

L'autre aide au dépannage est la commande debug **debug voice source-group**. Par exemple, lorsqu'un appel H.323 est rejeté (avec le code de cause par défaut), le débogage produit ce résultat :

```
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
```

Avertissements et cavernes

Voici quelques mises en garde importantes concernant la passerelle VSG :

- VSG est beaucoup moins flexible que l'application de fraude à péage. Elle empêche les appels d'atteindre la couche de contrôle des appels et ne consigne aucun message d'erreur. Cela est vrai, qu'un appel soit autorisé ou bloqué.
- Certains ont rencontré un problème avec le protocole GLBP (Global Load Balancing Protocol) activé pour cette passerelle. Il semble y avoir une dépendance obscure sur l'ordre relatif dans lequel GLBP et VSG sont configurés. Si vous rencontrez de tels problèmes, procédez comme suit : Désactivez **GLBP**.Réappliquer **VSG**.Redémarrez la **passerelle**.Testez/vérifiez que VSG fonctionne.Activez **GLBP**.

Informations connexes

- Comprendre les améliorations apportées à la fraude par numéro dans 15.1(2)T
- Méthodes de sécurité SIP de l'outil Cisco CCA
- Support et documentation techniques - Cisco Systems