Caractéristique de voice source-group

Contenu

[Introduction](#)
[Informations générales](#)
[Attributs VSG](#)
[Liste d'accès](#)
[Cause de débranchement](#)
[TRANSPORTEUR-ID](#)
[Joncteur Réseau-Groupe-étiquette](#)
[H.323 ID de zone](#)
[Plusieurs groupes de service vocal](#)
[Vérifiez](#)
[Dépannez](#)
[Attentions et mises en garde](#)
[Informations connexes](#)

Introduction

Ce document décrit la caractéristique de la voice source-group (VSG) dans le Cisco IOS® qui permet la passerelle, ou le Logiciel Cisco Unified Border Element (CUBE), pour identifier la source et contrôler le routage du VoIP appelle.

> Remarque: Le CUBE en termes et la passerelle IP-à-IP (IPIPGW) sont utilisés l'un pour l'autre dans tout ce document.

Informations générales

Si vous avez rencontré une situation où vous voulez implémenter la contournement-fraude en bloquant la signalisation d'appel des adresses IP escrocs, alors vous pourriez utiliser la caractéristique de prévention de contournement-fraude, introduite dans le Cisco IOS 15.1(2)T. Référez-vous à la caractéristique de prévention de Contournement-fraude dans le pour en savoir plus d'article de la release 15.1(2)T IOS.

Cependant, si vous avez une version plus ancienne de Cisco IOS, ou ayez besoin de ces contrôles supplémentaires, puis vous devriez considérer la caractéristique VSG :

- cause-code configurable d'anomalie
- changez appeler/numéros appelés basés sur qui lance l'appel
- contrôlez le routage (l'artère au transporteur spécifique, par exemple)

La caractéristique VSG te permet pour identifier la source d'appel VoIP tels que des services sélectionnés sont fournis à l'appel. Ces services incluent la conversion de numéros, apparier d'homologue de numérotation en entrée, et l'acceptation d'appel/contrôle de rejet. En outre, la caractéristique te permet pour contrôler le routage de l'appel (permis) des manières que l'application de contournement-fraude ne peut pas. Par exemple, vous pouvez associer des traductions de Voix au VSG afin de manipuler appeler/numéros appelés *AVANT QUE l'*appel atteigne l'homologue de numérotation en entrée. C'est puissant parce que des appels avec le ***même*** numéro composé pourraient être conduits par différents homologues de numérotation en entrée.

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

Attributs VSG

Liste d'accès

Un ACL IOS standard est configuré afin de spécifier les adresses IP des sources desquelles des appels sont reçus et traités. L'ACL est alors mis en référence dans le VSG associé.

Si l'adresse IP de la source (d'appel entrant) n'a pas une entrée dans l'ACL, la passerelle n'associe pas le VSG à l'appel. Ceci signifie que l'appel n'est pas sujet à des manipulations l'unes des configurées sous le VSG.

Si des appels d'une adresse IP particulière doivent être rejetés, cette adresse IP doit être incluse dans une **instruction de refus** sous l'ACL.

Alternativement, le **refuser n'importe quelle** déclaration est configuré afin de rejeter des appels de n'importe quelle adresse IP qui n'est pas explicitement permise ou est refusée.

Cause de débranchement

Code de cause avec lequel l'appel entrant est rejeté est configureable sous le VSG. Par défaut, la débranchement-cause est NO--**service**. Ceci se traduit à l'**erreur interne du serveur 500** pour des appels et **ReleaseComplete de** Protocole SIP (Session Initiation Protocol) avec le cause-code 63 (service ou à l'option non disponible, non spécifiée) pour H.323 des appels.

Les raisons définies par l'utilisateur de débranchement sont :

- Nombre non valide
- Nombre non affecté
- Utilisateur occupé
- Appel rejeté

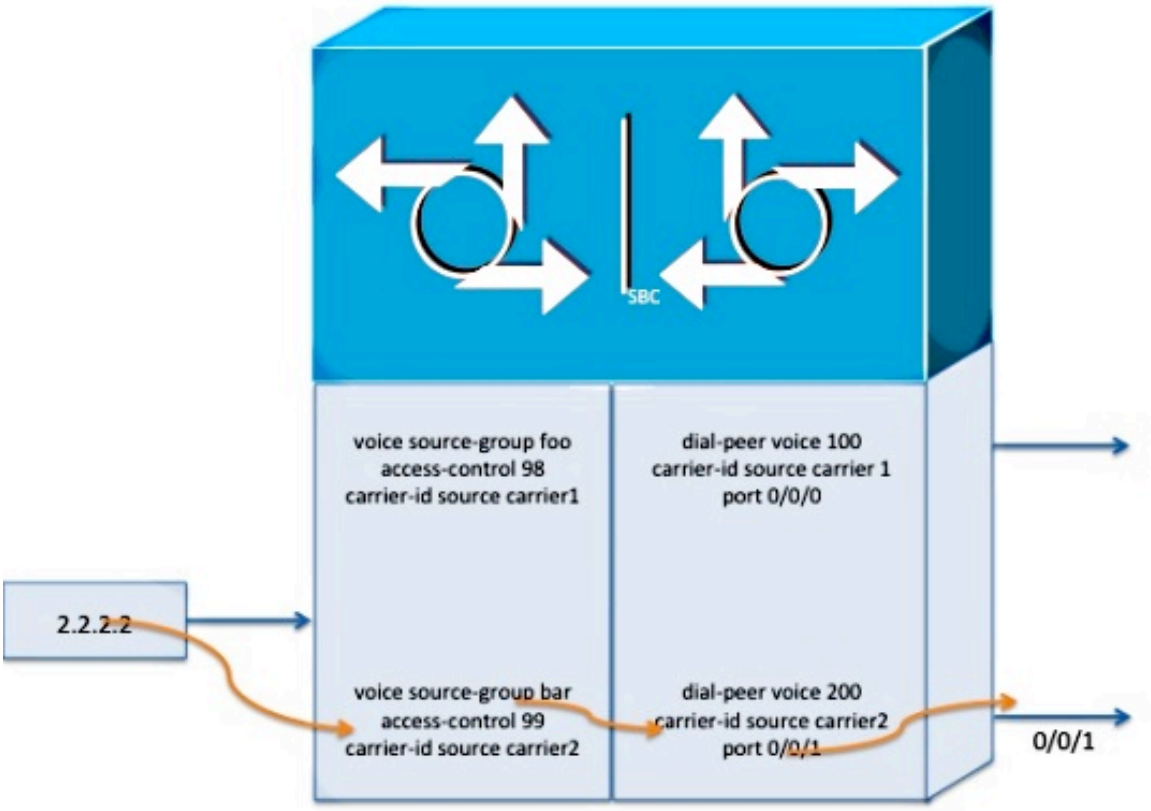
TRANSPORTEUR-ID

L'attribut de transporteur-ID est configuré sur le VSG de sorte que des appels qui apparient l'ACL associé soient étiquetés avec le transporteur-ID. Ceci permet à des appels avec le *même* numéro

appelé d'être conduits (du côté sortant) par différents transporteurs, basés sur l'adresse IP de la source. Par exemple, si vous avez deux groupes d'adresses IP, les appels d'un groupe d'adresses pourraient traverser un VSG et pourraient obtenir étiqueté avec un transporteur-ID, et des appels (au même numéro appelé) de l'autre groupe pourraient être étiquetés avec un transporteur-ID 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, des appels de 1.1.1.1 sont conduits par le cadran-pair 100, et des appels de 2.2.2.2 sont conduits par le cadran-pair 200.



Joncteur Réseau-Groupe-étiquette

Les travaux de joncteur réseau-groupe-étiquette pareillement au transporteur-ID. L'appel entrant VoIP est étiqueté avec le groupe de faisceaux configuré, qui est alors utilisé afin de sélectionner le cadran-pair approprié quand l'appel est conduit par le tronçon sortant.

H.323 ID de zone

Ce s'applique pour H.323 le protocole seulement et est utilisé afin d'apparier la zone de source H.323 de l'appel entrant à un VSG. L'ID de zone de source est porté dedans H.323 un appel entrant qui utilise le protocole de signalisation H.323V4 et provient d'un contrôleur d'accès H.323.

Plusieurs groupes de service vocal

Vous pouvez configurer plusieurs VSGs sur un IPIPGW où chacun permet ou rejette des appels d'un ensemble différent d'adresses IP.

Faites attention à ajouter **refusent** SEULEMENT à l'ACL du dernier VSG, quand vous avez plusieurs VSGs. Autrement, si un ACL intermédiaire en a **pour refuser**, puis appelle de n'importe quelle adresse IP qui est explicitement permise dans un autre ACL sera toujours rejetée si cet

ACL est APRÈS l'ACL avec le **refuser**. Par exemple, voici deux VSGs :

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

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

Voici l'ACLs pour le VSGs :

```
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, des appels de 2.2.2.2 sont rejetés, puisque l'ACL qui permet l'adresse IP en est APRÈS l'ACL (98) avec **refusent**.

Vous pouvez employer 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"
```

Afin de permettre l'appel, vous en devez enlever le **refuser de la** liste d'accès 98.

```
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"
```

Vous pouvez employer la commande de **2.2.2.2 d'IP de test source-group** afin de vérifier de nouveau que des 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
```

Vérifiez

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

Dépannez

Comme mentionné dans la section précédente, la commande du **test source-group *<VSG>*** est utile afin de la découvrir si un appel donné sera permis ou rejeté. En outre, si on permettra l'appel, expositions de cette commande également que VSG va le faire ? artère ? l'appel. De même, si l'appel sera rejeté, il affiche la cause de rejet. Cette commande trouve le VSG de acheminement basé sur d'autres attributs, en plus de l'adresse IP.

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

```
Router#test  source-group ip-address 2.2.2.2
```

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

Attentions et mises en garde

Voici quelques importantes mises en garde avec le VSG :

- VSG est beaucoup moins flexible que l'application de contournement-fraude. Il empêche les appels d'atteindre la couche de contrôle d'appel et ne se connecte aucun message d'erreur. C'est vrai indépendamment de si un appel est permis ou bloqué.
- Certains ont éprouvé une question avec l'Équilibrage de charge global Protocol (GLBP) activé pour cette passerelle. Il semble y a une dépendance obscure sur la commande relative dans laquelle le GLBP et les VSG sont configurés. Si vous rencontrez de telles questions, terminez-vous ces étapes : **GLBP de** débronchement.Réappliquez **VSG**.Redémarrez la **passerelle**.Testez/vérifiez que VSG fonctionne.**GLBP d'**enable.

Informations connexes

- Compréhension des améliorations de Contournement-fraude dans 15.1(2)T
- Méthodes de Sécurité de SIP d'outil de CCA de Cisco
- Support et documentation techniques - Cisco Systems