Kenmerken spraakbron-groep

Inhoud

Inleiding

Dit document beschrijft de Voice Source-Group (VSG) optie in Cisco IOS® die de gateway, of Cisco Unified Border Element (CUBE) toestaat om de bron te identificeren en de routing van VoIP-oproepen te controleren.

> **Opmerking:** De termen CUBE en IP-to-IP Gateway (IPGW) worden door dit document onderling verwisselbaar gebruikt.

Achtergrondinformatie

Als u een situatie hebt ervaren waarin u tolfraude wilt uitvoeren door het bellen vanaf schurken IP-adressen te blokkeren, dan kunt u de functie voor de preventie van tolfraude gebruiken, die in Cisco IOS 15.1(2)T is geïntroduceerd. Raadpleeg het [artikel](#) over [preventie van fraude in IOS release 15.1(2)T](#) voor meer informatie.

Als u echter een oudere versie van Cisco IOS hebt of deze extra controles nodig hebt, dan dient u rekening te houden met de VSG-functie:

- Configureerbare afwijzende oorzaakcode
- verandering het roepen/geroepen getallen gebaseerd op wie de vraag voortkomt
- controle routing (route naar specifieke drager, bijvoorbeeld)

Met de VSG-functie kunt u de bron van de VoIP-oproep identificeren, zodat er geselecteerde

services worden geleverd aan de oproep. Deze services omvatten nummervertaling, inkomende dial-peers matching en aanroep acceptatie/verwerping controle. Bovendien kunt u met deze functie de routing van de (geoorloofde) oproep controleren op manieren die niet in de toepassing van de tol-fraude kunnen worden gebruikt. Bijvoorbeeld, kunt u spraakvertalingen naar de VSG associëren om de aangeroepen/aangeroepen getallen te manipuleren *VOORDAT* de oproep de inkomende wijzerplaat-peer bereikt. Dit is krachtig omdat oproepen met ***hetzelfde*** gedialineerde nummer door verschillende inkomende kiespeers kunnen worden routeerd.

VSG gebruikt de Cisco IOS Access Control List (ACL) om de identificatie te realiseren.

VSG-kenmerken

Toegangslijst

Een standaard IOS ACL wordt ingesteld om de IP-adressen van de bronnen te specificeren waarvan oproepen worden geaccepteerd en verwerkt. ACL wordt dan verwezen in de geassocieerde VSG.

Als het IP-adres van de bron (van een inkomende vraag) geen ingang in ACL heeft, associeert de gateway VSG NIET aan de vraag. Dit betekent dat de oproep niet onderworpen is aan enige manipulatie die is ingesteld onder de VSG.

Als de vraag van een bepaald IP adres moet worden afgewezen, moet dat IP-adres in een **ontkende** verklaring onder ACL worden opgenomen.

In plaats hiervan **ontkent** u **elke** verklaring die is ingesteld om oproepen van een IP-adres af te wijzen dat niet expliciet is toegestaan of ontkend.

Oorzaak van verbroken verbinding

De oorzaakcode waarmee het inkomende gesprek wordt afgewezen, kan worden ingesteld onder de VSG. Standaard is de **oorzaak** van de **loskoppeling geen service**. Dit vertaalt zich naar de **500 interne serverfout** voor SIP-oproepen (Session Initiation Protocol) en **releaseComplete** met oorzaakcode 63 (Service of optie niet beschikbaar, niet gespecificeerd) voor H.323-oproepen.

Door de gebruiker gedefinieerde redenen om de verbinding te verbreken zijn:

- Ongeldig nummer
- Ontoegewezen nummer
- Gebruiker druk
- Aanvraag verworpen

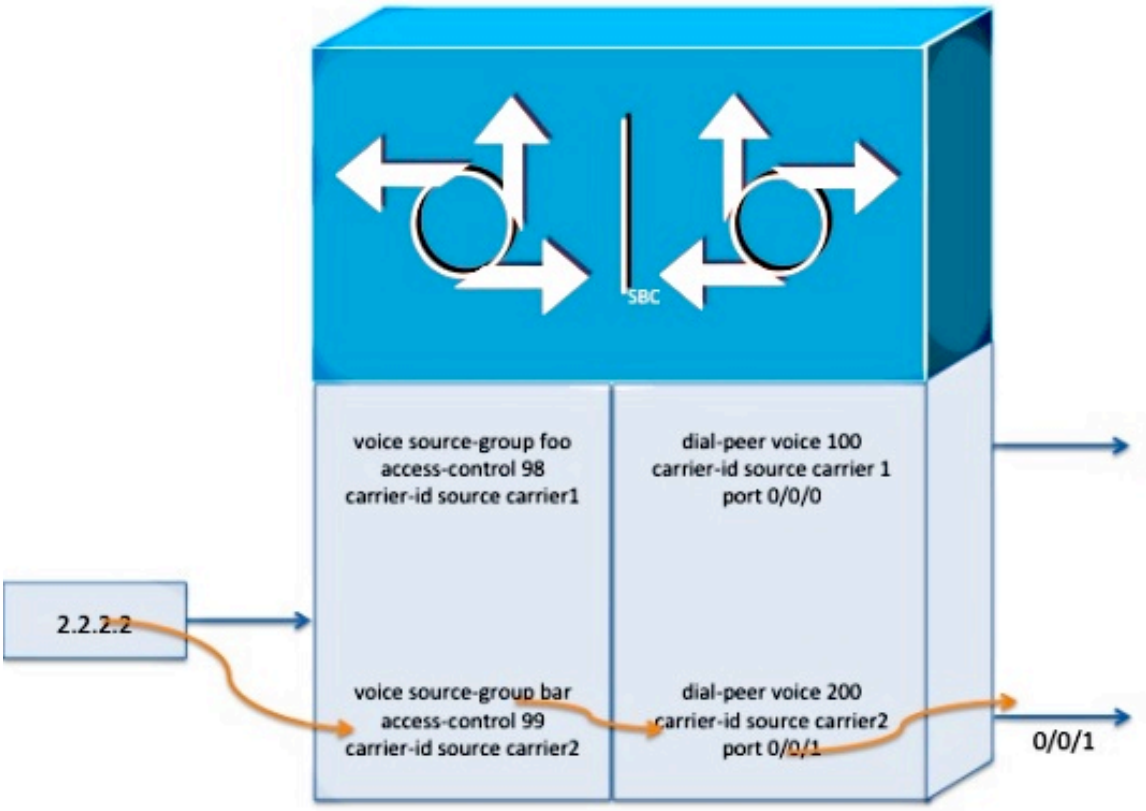
Carrier-ID

De drager-ID eigenschap wordt ingesteld op VSG zodat aanroepen die overeenkomen met de gekoppelde ACL worden getagd met de drager-ID. Dit maakt het mogelijk dat oproepen met *hetzelfde* aangeroepen nummer via verschillende dragers worden routeerd (aan de kant van de

uitgang), op basis van het IP-adres van de bron. Bijvoorbeeld, als u twee groepen IP adressen hebt, zou de vraag van één groep van adressen door één VSG kunnen stromen en door één drager-ID kunnen worden gelabeld, en de vraag (aan het zelfde geroepen aantal) van de andere groep zou met een andere drager-ID kunnen worden gelabeld. Hierna volgt een voorbeeld:

```
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
```

Bij de vorige configuratie worden oproepen van 1.1.1.1 door dial-peers 100 routeerd en worden oproepen van 2.2.2.2 door dial-peers 200 routeerd.



Trunk-groepslabel

Het label van de groep werkt vergelijkbaar met de drager-ID. De inkomende VoIP vraag is gelabeld met de geconfigureerde stam-groep, die dan wordt gebruikt om de juiste dial-peers te selecteren wanneer de oproep door het uitgaande been wordt routeerd.

ID H.323 zone

Dit is alleen van toepassing op H.323-protocol en wordt gebruikt om de bronzone van de inkomende H.323-oproep aan een VSG aan te passen. De bron zone-ID wordt vervoerd in een inkomende H.323-oproep die gebruik maakt van een H.323V4-signaalprotocol en afkomstig is van een H.323-poorts.

Meervoudige spraakservicegroepen

U kunt meerdere VSG's op een IPGW configureren, waarbij elk oproepen vanuit een andere set IP-adressen toestaat of afsluit.

Let op dat u ALLEEN **ontkent** dat u ACL's van de laatste VSG hebt, wanneer u meerdere VSG's hebt. Anders, als een intermediaire ACL **om het even welke** heeft **ontkend**, dan zal vraag van om

het even welk IP adres dat expliciet in een andere ACL wordt toegestaan worden verworpen als die ACL NA ACL met het **ontkennen** van **om het even welke is**. Hier zijn bijvoorbeeld twee VSG's:

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

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

Hier zijn de ACL's voor VSG's:

```
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 dit voorbeeld, wordt de vraag van 2.2.2 afgewezen, aangezien ACL die het IP adres toestaat na ACL (98) is met **ontkennen om het even welk**.

U kunt deze opdracht gebruiken om te bevestigen dat de oproepen zijn verworpen.

```
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"
```

Om de oproep toe te staan, moet u het **ontkennen van om het even welke** van toegangslijst 98 verwijderen.

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

U kunt de opdracht **ip 2.2.2.2** van de **testbron** gebruiken om te verifiëren dat de oproepen van het IP-adres in kwestie niet meer worden afgewezen.

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

Verifiëren

De opdracht **tebrongroep *<VSG>*** kan voor basiscontrole worden gebruikt - of oproepen van een bepaald IP-adres door een VSG worden verwerkt.

Problemen oplossen

Zoals in de vorige sectie vermeld, is de opdracht **testbron-groep *<VSG>***nuttig om te ontdekken of een bepaalde oproep geautoriseerd of verworpen zal worden. Bovendien, als de oproep wordt toegestaan, toont deze opdracht ook aan welke VSG de route zal volgen? de oproep . En als de oproep wordt verworpen, dan is er ook de reden van de afwijzing. Deze opdracht vindt de routing VSG op basis van andere eigenschappen, naast het IP-adres.

De andere hulp bij het oplossen van problemen is de **debug van spraakbron-groep** debug opdracht. Bijvoorbeeld, wanneer een vraag van H.323 wordt verworpen (met de standaard oorzaak-code), debug produceert deze uitvoer:

```
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
```

Veiligheidsinstructies en voorzorgsmaatregelen

Hier zijn een paar belangrijke uitzonderingen met de VSG:

- VSG is veel minder flexibel dan de tolfraudeapplicatie. Het voorkomt de vraag van het bereiken van de vraag-controle laag en logt geen foutmeldingen. Dit geldt ongeacht of een telefoontje is toegestaan of geblokkeerd.
- Sommigen hebben een probleem ervaren met de GLBP-technologie (Global taakverdeling Protocol) die voor die gateway is ingeschakeld. Er lijkt een obscure afhankelijkheid te zijn van de relatieve volgorde waarin GLBP en VSG zijn ingesteld. Als u dergelijke problemen ondervindt, voert u deze stappen uit: **GLBP** uitschakelen.Breng **VSG** opnieuw aan.Start de **poort opnieuw op**.Test/controleer of VSG werkt.GLBP inschakelen.

Gerelateerde informatie

- Verbeteringen in tolfraude in 15.1(2)T
- Cisco CCA Tool SIP-beveiligingsmethoden
- Technische ondersteuning en documentatie – Cisco Systems