Recurso de grupo de origem de voz

Contents

Introduction

Este documento descreve o recurso Voice Source-Group (VSG) no Cisco IOS® que permite que o gateway, ou Cisco Unified Border Element (CUBE), identifique a origem e controle o roteamento de chamadas VoIP.

> **Note**: Os termos CUBE e IP-to-IP Gateway (IPIPGW) são usados como sinônimos neste documento.

Informações de Apoio

Se você tiver encontrado uma situação em que deseja implementar fraudes de tarifas bloqueando a sinalização de chamadas de endereços IP não autorizados, poderá usar o recurso de prevenção de fraudes de tarifas, introduzido no Cisco IOS 15.1(2)T. Consulte o recurso de prevenção de fraude no IOS versão 15.1(2)T para obter mais informações.

No entanto, se você tiver uma versão mais antiga do Cisco IOS ou precisar desses controles adicionais, considere o recurso VSG:

- código de causa de rejeição configurável
- alterar números de chamada/chamada com base em quem originou a chamada
- roteamento de controle (rota para uma operadora específica, por exemplo)

O recurso VSG permite identificar a origem da chamada VoIP, de modo que os serviços

selecionados sejam fornecidos à chamada. Esses serviços incluem conversão de números, correspondência de peer de discagem de entrada e controle de aceitação/rejeição de chamadas. Além disso, o recurso permite que você controle o roteamento da chamada (permitida) de maneiras que o aplicativo de fraude de tarifas não pode. Por exemplo, você pode associar traduções de voz ao VSG para manipular os números de chamada/chamada *ANTES* que a chamada chegue ao peer de discagem de entrada. Isso é poderoso porque as chamadas com o ***mesmo*** número discado podem ser roteadas através de diferentes peers de discagem de entrada.

O VSG usa a ACL (Access Control List, lista de controle de acesso) do Cisco IOS para realizar a identificação.

Atributos do VSG

Lista de acesso

Uma ACL padrão do IOS é configurada para especificar os endereços IP das origens das quais as chamadas são aceitas e processadas. A ACL é referenciada no VSG associado.

Se o endereço IP da origem (de uma chamada recebida) não tiver uma entrada na ACL, o gateway NÃO associará o VSG à chamada. Isso significa que a chamada não está sujeita a nenhuma das manipulações configuradas no VSG.

Se as chamadas de um endereço IP específico forem rejeitadas, esse endereço IP deverá ser incluído em uma instrução **deny** na ACL.

Como alternativa, a instrução **deny any** é configurada para rejeitar chamadas de qualquer endereço IP que não seja explicitamente permitido ou negado.

Causa da desconexão

O código de causa com o qual a chamada recebida é rejeitada pode ser configurado no VSG. Por padrão, a causa da desconexão é **no-service**. Isso se traduz no **erro interno do servidor 500** para chamadas do Session Initiation Protocol (SIP) e **ReleaseComplete** com código de causa 63 (Serviço ou opção não disponível, não especificado) para chamadas H.323.

Os motivos de desconexão definidos pelo usuário são:

- Número inválido
- Número não atribuído
- Usuário ocupado
- Chamada rejeitada

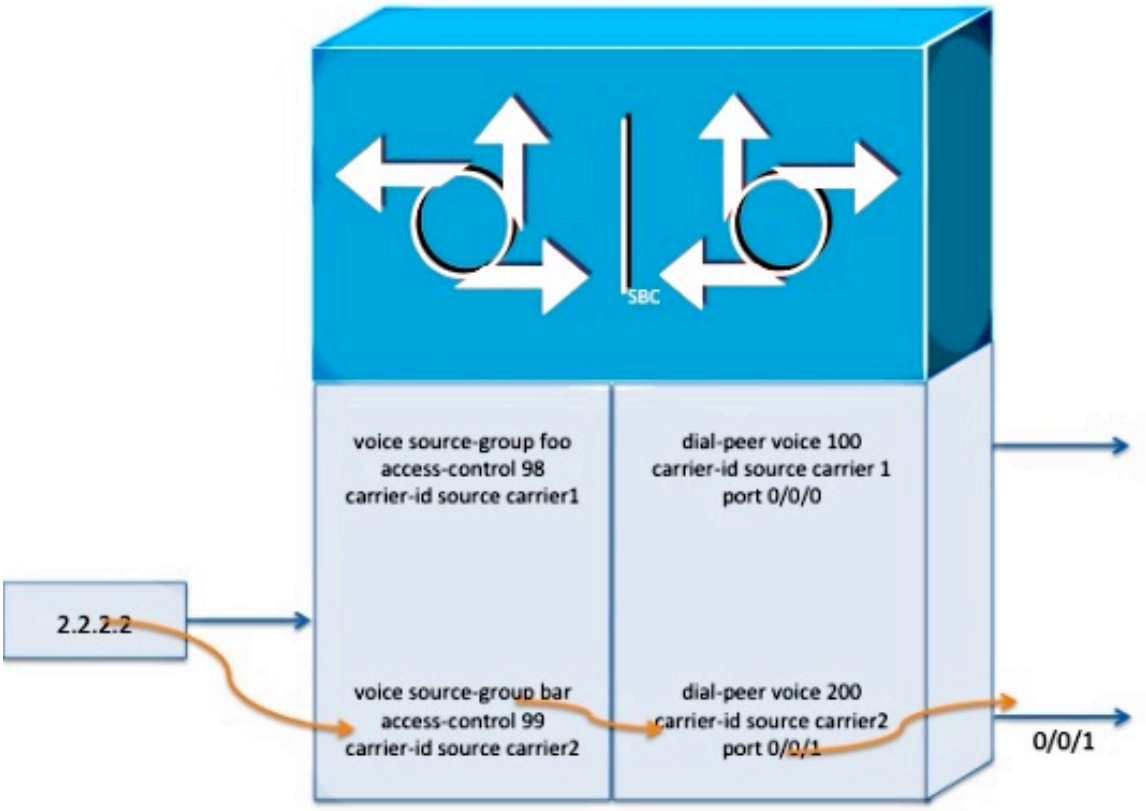
ID da portadora

O atributo ID da portadora é configurado no VSG para que as chamadas que correspondem à ACL associada sejam marcadas com o ID da portadora. Isso permite que as chamadas com o *mesmo* número chamado sejam roteadas (no lado de saída) por diferentes operadoras, com base

no endereço IP da origem. Por exemplo, se você tiver dois grupos de endereços IP, as chamadas de um grupo de endereços podem fluir por um VSG e podem ser marcadas com um ID de portadora, e as chamadas (para o mesmo número chamado) do outro grupo podem ser marcadas com um ID de portadora diferente. Aqui está um exemplo:

```
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
```

Com a configuração anterior, as chamadas de 1.1.1.1 são roteadas pelo peer de discagem 100 e as chamadas de 2.2.2.2 são roteadas pelo peer de discagem 200.



Trunk-Group-Label

O trunk-group-label funciona de forma semelhante ao ID da portadora. A chamada VoIP recebida é marcada com o grupo de troncos configurado, que é usado para selecionar o correspondente de discagem apropriado quando a chamada é roteada através do segmento de saída.

ID da zona H.323

Isso se aplica somente ao protocolo H.323 e é usado para corresponder a zona de origem da chamada H.323 recebida para um VSG. O ID da zona de origem é transportado em uma chamada de entrada H.323 que usa o protocolo de sinalização H.323V4 e se origina de um gatekeeper H.323.

Vários grupos de serviço de voz

Você pode configurar vários VSGs em um IPIPGW onde cada um permite ou despermite chamadas de um conjunto diferente de endereços IP.

Tome cuidado para adicionar **deny any** SOMENTE à ACL do último VSG, quando você tiver vários VSGs. Caso contrário, se uma ACL intermediária tiver **negado qualquer**, as chamadas de

qualquer endereço IP explicitamente permitido em outra ACL ainda serão rejeitadas se essa ACL for APÓS a ACL com a **negação de qualquer**. Por exemplo, aqui estão dois VSGs:

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

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

Aqui estão as ACLs para os 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
```

Neste exemplo, as chamadas de 2.2.2.2 são rejeitadas, já que a ACL que permite o endereço IP é APÓS a ACL (98) com **deny any**.

Você pode usar esse comando para confirmar se as chamadas foram rejeitadas.

```
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"
```

Para permitir a chamada, você deve remover o **deny any** da lista de acesso 98.

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

Você pode usar o **comando test source-group ip 2.2.2.2** novamente para verificar se as chamadas do endereço IP em questão não são mais rejeitadas.

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

Verificar

O comando **test source-group *<VSG>*** pode ser usado para verificação básica - se as chamadas de um determinado endereço IP serão processadas por um VSG.

Troubleshoot

Como mencionado na seção anterior, o comando **test source-group *<VSG>*** é útil para descobrir se uma determinada chamada será permitida ou rejeitada. Além disso, se a chamada for permitida, esse comando também mostrará qual VSG irá ?rotear? a chamada. Da mesma forma, se a chamada for rejeitada, ela mostrará a causa da rejeição. Esse comando localiza o VSG de roteamento com base em outros atributos, além do endereço IP.

A outra ajuda para solução de problemas é o comando debug **voice source-group** debug. Por exemplo, quando uma chamada H.323 é rejeitada (com o código de causa padrão), a depuração produz esta saída:

```
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
```

Precauções e avisos

Aqui estão algumas ressalvas importantes com o VSG:

- O VSG é muito menos flexível do que o aplicativo de fraude de tarifas. Evita que as chamadas cheguem à camada de controle de chamadas e não registra nenhuma mensagem de erro. Isso é verdadeiro independentemente de uma chamada ser permitida ou bloqueada.
- Alguns tiveram um problema com o Global Load Balancing Protocol (GLBP) ativado para esse gateway. Parece haver uma dependência obscura na ordem relativa em que o GLBP e o VSG estão configurados. Se você encontrar tais problemas, faça o seguinte: Desative o **GLBP**.Reaplique o **VSG**.Reinicialize o **gateway**.Teste/verifique se o VSG funciona.Ative o **GLBP**.

Informações Relacionadas

- Compreendendo melhorias na fraude de tarifas em 15.1(2)T
- Métodos de segurança SIP da ferramenta Cisco CCA
- Suporte Técnico e Documentação - Cisco Systems