Función Voice Source-Group

Contenido

Introducción

Este documento describe la función Voice Source-Group (VSG) en Cisco IOS® que permite al gateway, o Cisco Unified Border Element (CUBE), identificar el origen y controlar el enrutamiento de las llamadas VoIP.

> **Nota:** Los términos CUBE y IP-to-IP Gateway (IPIPGW) se utilizan indistintamente en este documento.

Antecedentes

Si ha encontrado una situación en la que desea implementar el fraude de llamadas bloqueando la señalización de llamadas desde direcciones IP no fiables, entonces podría utilizar la función de prevención del fraude de llamadas, introducida en Cisco IOS 15.1(2)T. Refiérase al artículo Función de Prevención de Fraude de Llamada de IOS Release 15.1(2)T para obtener más información.

Sin embargo, si tiene una versión anterior de Cisco IOS o necesita estos controles adicionales, debe considerar la función VSG:

- código de causa de rechazo configurable
- cambiar los números que llaman/a los que llaman en función de quién origina la llamada
- ruteo de control (ruta a una portadora específica, por ejemplo)

La función VSG le permite identificar el origen de la llamada VoIP de modo que los servicios seleccionados se proporcionen a la llamada. Estos servicios incluyen traducción de números, coincidencia de pares de marcado entrante y control de aceptación/rechazo de llamadas. Además, la función permite controlar el enrutamiento de la llamada (permitida) de formas que la aplicación de fraude de llamadas no puede realizar. Por ejemplo, puede asociar traducciones de voz al VSG para manipular los números de llamada/llamada *ANTES* de que la llamada llegue al par de marcado entrante. Esto es poderoso porque las llamadas con el ***mismo*** número marcado podrían enrutarse a través de diferentes pares de marcado entrantes.

VSG utiliza la lista de control de acceso (ACL) de Cisco IOS para lograr la identificación.

Atributos VSG

Lista de acceso

Se configura una ACL IOS estándar para especificar las direcciones IP de los orígenes desde los que se aceptan y procesan las llamadas. A continuación, se hace referencia a la ACL en el VSG asociado.

Si la dirección IP del origen (de una llamada entrante) no tiene una entrada en la ACL, la gateway NO asocia el VSG a la llamada. Esto significa que la llamada no está sujeta a ninguna de las manipulaciones configuradas bajo el VSG.

Si se rechazan las llamadas de una dirección IP determinada, esa dirección IP debe incluirse en una instrucción **deny** bajo la ACL.

Alternativamente, la instrucción **deny any** se configura para rechazar llamadas de cualquier dirección IP que no se permita o se niegue explícitamente.

Causa de desconexión

El código de causa con el que se rechaza la llamada entrante se puede configurar en el VSG. De forma predeterminada, la causa de desconexión es **no-service**. Esto se traduce en el **error 500 del servidor interno** para las llamadas del protocolo de inicio de sesión (SIP) y **ReleaseComplete** con código de causa 63 (Servicio u opción no disponible, no especificado) para las llamadas H.323.

Los motivos de desconexión definidos por el usuario son:

- Número no válido
- Número sin asignar
- Usuario ocupado
- Llamada rechazada

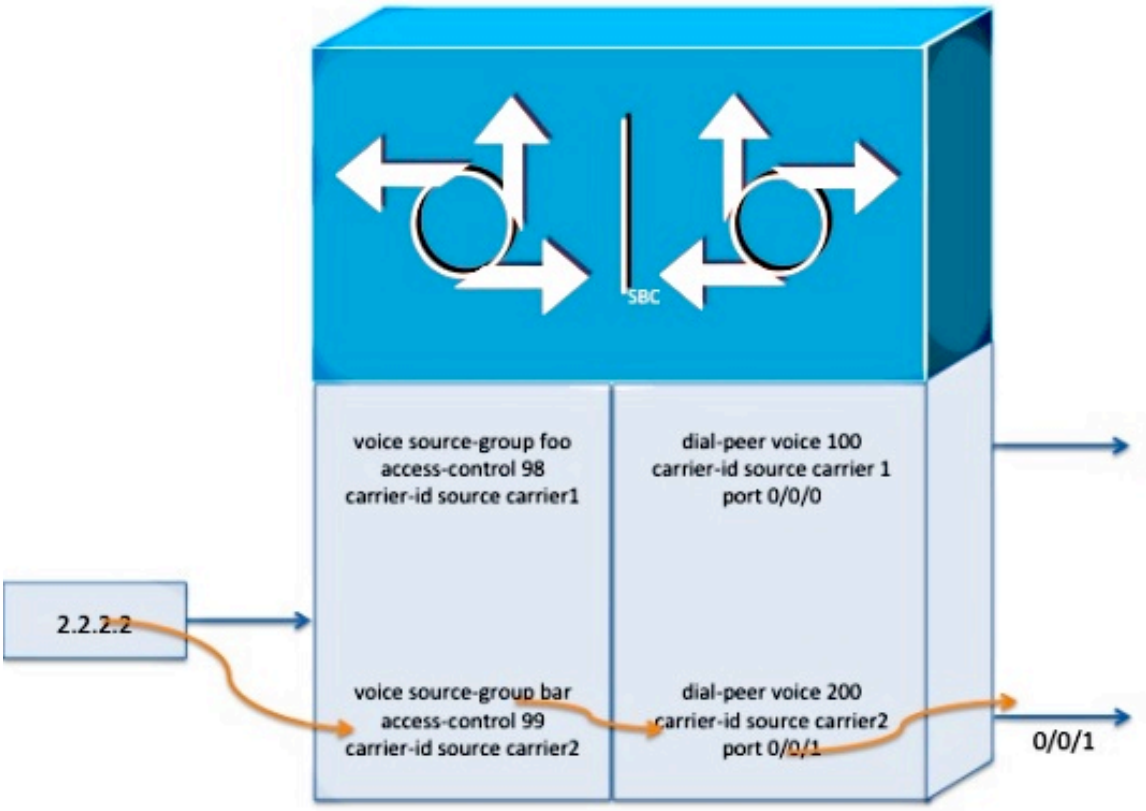
Carrier-ID

El atributo carrier-ID se configura en el VSG para que las llamadas que coincidan con la ACL asociada se etiqueten con la carrier-ID. Esto permite que las llamadas con el *mismo* número

llamado se enruten (en el lado saliente) a través de diferentes operadores, en función de la dirección IP del origen. Por ejemplo, si tiene dos grupos de direcciones IP, las llamadas de un grupo de direcciones podrían fluir a través de un VSG y se podrían etiquetar con un ID de operador, y las llamadas (al mismo número llamado) del otro grupo podrían etiquetarse con un ID de operador diferente. Aquí tiene un ejemplo:

```
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
```

Con la configuración anterior, las llamadas de 1.1.1.1 se enrutan a través del dial-peer 100, y las llamadas de 2.2.2.2 se enrutan a través del dial-peer 200.



Trunk-Group-Label

El trunk-group-label funciona de manera similar al carrier-ID. La llamada VoIP entrante se etiqueta con el grupo troncal configurado, que luego se utiliza para seleccionar el par de marcado adecuado cuando la llamada se enruta a través del tramo saliente.

ID de zona H.323

Esto es aplicable sólo para el protocolo H.323 y se utiliza para hacer coincidir la zona de origen de la llamada H.323 entrante con un VSG. El ID de la zona de origen se transporta en una llamada H.323 entrante que utiliza el protocolo de señalización H.323V4 y se origina desde un gatekeeper H.323.

Varios grupos de servicios de voz

Puede configurar varios VSG en un IPIPGW donde cada uno permite o rechaza llamadas de un conjunto diferente de direcciones IP.

Tenga cuidado de agregar **deny any** ONLY a la ACL de la última VSG, cuando tenga varios VSG. De lo contrario, si una ACL intermedia ha **denegado alguna**, las llamadas de cualquier dirección

IP que esté permitida explícitamente en otra ACL seguirán siendo rechazadas si esa ACL está DESPUÉS de la ACL con la **negación alguna**. Por ejemplo, aquí hay dos VSG:

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

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

Estas son las ACL para los 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
```

En este ejemplo, se rechazan las llamadas de 2.2.2.2, ya que la ACL que permite la dirección IP es DESPUÉS de la ACL (98) con **deny any**.

Puede utilizar este comando para confirmar que se rechazan las llamadas.

```
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 la llamada, debe quitar la **denegación any** de la lista de acceso 98.

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

Puede utilizar el comando **test source-group ip 2.2.2.2** de nuevo para verificar que las llamadas de la dirección IP en cuestión ya no se rechazan.

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

Verificación

El comando **test source-group *<VSG>*** se puede utilizar para la verificación básica: si las llamadas de una dirección IP determinada serán procesadas por un VSG.

Troubleshoot

Como se mencionó en la sección anterior, el comando **test source-group *<VSG>*** es útil para descubrir si una llamada dada será permitida o rechazada. Además, si se permite la llamada, este comando también muestra a qué VSG le enviará? la llamada. Asimismo, si se rechaza la llamada, se muestra la causa del rechazo. Este comando encuentra el VSG de ruteo basado en otros atributos, además de la dirección IP.

La otra ayuda para la resolución de problemas es el comando debug **debug voice source-group**. Por ejemplo, cuando se rechaza una llamada H.323 (con el código de causa predeterminado), la depuración produce este resultado:

```
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
```

Precauciones y advertencias

Estas son algunas de las importantes advertencias con el VSG:

- VSG es mucho menos flexible que la aplicación de fraude de tarifas. Evita que las llamadas lleguen a la capa de control de llamadas y no registra ningún mensaje de error. Esto es cierto independientemente de si una llamada está permitida o bloqueada.
- Algunos han experimentado un problema con el protocolo de equilibrio de carga global (GLBP) habilitado para ese gateway. Parece haber una oscura dependencia del orden relativo en el que se configuran GLBP y VSG. Si detecta estos problemas, complete estos pasos: Inhabilite **GLBP**.Vuelva a aplicar **VSG**.Reinicie el **gateway**.Pruebe/verifique que VSG funciona.Habilite **GLBP**.

Información Relacionada

- Introducción a las mejoras en el fraude telefónico en 15.1(2)T
- Métodos de seguridad SIP de la herramienta CCA de Cisco
- Soporte Técnico y Documentación - Cisco Systems