Característica de la prevención de fraude de cargos de llamada en la versión del IOS 15.1(2)T

ID del Documento: 112083

Actualizado: De julio el 29 de 2010

Productos Relacionados

- Servidor de facturación y medidas de Cisco
- Voz over Frame Relay (VoFR)
- Calidad de voz
- Cisco SC 2200 Signaling Controller
- Skinny Call Control Protocol (SCCP)
- Cisco Digital Gateway DE-30+
- H.323
- Protocolo de Control de Gateway de Medios (MGCP)
- Voz over ATM (VoATM)
- Signaling System 7 (SS7)
- + demostración más

Contenido

Introducción

Una nueva función se ha introducido en el Software Release 15.1(2)T de Cisco IOS® para

guardar contra la incidencia del fraude de cargos de llamada en el Gateways de voz (VGWs) instalado con el Cisco IOS. Comenzando con IOS 15.1(2)T y más nuevas versiones del IOS basados en esta versión, las configuraciones de la prevención de fraude de cargos de llamada son el comportamiento predeterminado de Cisco VGWs basado en IOS.

El propósito de este documento es aumentar la conciencia de esta nueva función, como el actualizar a esta versión requerirá la configuración adicional permitir que pongan a los tipos determinados de llamadas de voz y ruta a la realización. Es importante observar que el actualizar a 15.1(2)T bloqueará todos VoIP entrante las configuraciones de la llamada hasta que el VGW se configure correctamente para confiar en estas fuentes. Cualquier plan a actualizar a las versiones con esta característica debe incluir los pasos adicionales para configurar los host de confianza VoIP después de la actualización para que las llamadas ruteen con éxito. Además, el discado en dos etapas se habilita no más por abandono con esta versión.

prerrequisitos

Requisitos

Este documento asume que el lector tiene ya un conocimiento sobre el funcionamiento en la configuración de gateway de voz, así como Conocimiento fundamental en cómo hacer el debug de los errores de la llamada de voz.

Componentes Utilizados

El documento discute las configuraciones que se aplican a los gatewayes de la voz del Cisco IOS, que incluirían al Routers de los Servicios integrados (ISR).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Comportamiento antes de 15.1(2)T

Para todas las versiones del IOS antes de 15.1(2)T, el comportamiento predeterminado para los gatewayes de voz del IOS es validar las configuraciones de la llamada de todas las fuentes. Mientras los servicios de voz se estén ejecutando en el router, la configuración predeterminada tratará una configuración de la llamada de cualquier dirección IP de origen como un legítimo y fuente confiable para fijar un llamar para. También, los puertos FXO y las llamadas entrantes en los circuitos ISDN presentarán el tono de marcación secundario para las llamadas entrantes, permitiendo para el discado en dos etapas. Esto asume que están correspondiendo con a un dial peer de entrada apropiado.

Comportamiento con y posterior las versiones 15.1(2)T

Comenzando con 15.1(2)T, el comportamiento predeterminado del router es no confiar en una configuración de la llamada de una fuente VoIP. Esta característica agrega una aplicación interna nombrada TOLLFRAUD_APP al stack predeterminado del Control de llamadas, que marca el IP de la fuente de la configuración de la llamada antes de rutear la llamada. Si el IP de la fuente no hace juego una entrada explícita en la configuración como fuente de confianza VoIP, se rechaza la llamada.

Nota: Si usted tiene el dial-peers configurado con el destino de la sesión, las llamadas de esos IP serán validadas incluso si no hay lista de confianza configurada.

Al iniciar una versión del IOS con la aplicación de la prevención de fraude de cargos de llamada, esto se imprime a la consola del dispositivo durante la secuencia de arranque:

```
Following voice command is enabled:
   voice service voip
    ip address trusted authenticate

 The command enables the ip address authentication
 on incoming H.323 or SIP trunk calls for toll fraud
 prevention supports.

 Please use "show ip address trusted list" command
 to display a list of valid ip addresses for incoming
 H.323 or SIP trunk calls.

 Additional valid ip addresses can be added via the
 following command line:
   voice service voip
    ip address trusted list
     ipv4 <ipv4-address> [<ipv4 network-mask>]
```

El router agrega automáticamente cualquier destino que se defina como blanco ipv4 en un VoIP dial-peer a la lista de fuente confiable. Usted puede observar este comportamiento con la salida de este comando:

```
Router#show ip address trusted list IP Address Trusted Authentication Administration State: UP
Operation State: UP IP Address Trusted Call Block Cause: call-reject (21) VoIP Dial-peer IPv4
Session Targets: Peer Tag Oper State Session Target -------- ---------- -------------- 3000 UP
ipv4:203.0.113.100 1001 UP ipv4:192.0.2.100
```

Cómo identificar si TOLLFRAUD_APP está bloqueando su llamada

Si el TOLLFRAUD_APP está rechazando la llamada, genera un valor del Desconectar causa Q.850 de 21, que representa la “llamada rechazada”. **El comando debug voip ccapi inout** puede ser funcionado con para identificar el valor de causa.

Además, el **Syslog IEC de la Voz** se puede habilitar para verificar más lejos si la falla de llamada es un resultado de la prevención de fraude de cargos de llamada. Esta configuración, que es a menudo práctica resolver problemas el origen del error de una perspectiva del gateway, imprimirá que la llamada está siendo rechazado debido al fraude de la llamada de larga distancia. El CCAPI y la salida de la Voz IEC se demuestra en esta salida de los debugs:

```
%VOICE_IEC-3-GW: Application Framework Core: Internal Error (Toll fraud call rejected):
IEC=1.1.228.3.31.0 on callID 3 GUID=F146D6B0539C11DF800CA596C4C2D7EF 000183: *Apr 30
14:38:57.251: //3/F146D6B0800C/CCAPI/ccCallSetContext: Context=0x49EC9978 000184: *Apr 30
14:38:57.251: //3/F146D6B0800C/CCAPI/cc_process_call_setup_ind: >>>>CCAPI handed cid 3 with tag
1002 to app "_ManagedAppProcess_TOLLFRAUD_APP" 000185: *Apr 30 14:38:57.251:
//3/F146D6B0800C/CCAPI/ccCallDisconnect: Cause Value=21, Tag=0x0, Call Entry(Previous Disconnect
Cause=0, Disconnect Cause=0)
```

El valor de la desconexión Q.850 que se vuelve para las llamadas bloqueadas se puede también cambiar del valor por defecto de 21 con este comando:

```
voice service voip
 ip address trusted call-block cause <q850 cause-code>
```

Cómo volver al comportamiento Pre-15.1(2)T

Lista de la confianza de la dirección IP de origen

Hay tres maneras de volver al comportamiento previó del Gateways de voz antes de que esta característica de la prevención de fraude de cargos de llamada de la dirección confiable fuera implementada. Todas estas configuraciones requieren que usted esté ejecutando ya 15.1(2)T para que usted realice el cambio de configuración.

1. Habilite explícitamente esas dirección IP de origen de las cuales usted quisiera agregar a la lista de confianza para las llamadas VoIP legítimas. Hasta 100 entradas pueden ser definidas. Esta configuración abajo valida las llamadas de esos el host 203.0.113.100/32, así como de la red 192.0.2.0/24. Las configuraciones de la llamada del resto de los host se rechazan. Éste es el método recomendado de una perspectiva de la Seguridad de la Voz.
```
voice service voip
 ip address trusted list
  ipv4 203.0.113.100 255.255.255.255
  ipv4 192.0.2.0 255.255.255.0
```
2. Configure al router para validar las configuraciones de llamada entrante de todas las dirección IP de origen.
```
voice service voip
 ip address trusted list
  ipv4 0.0.0.0 0.0.0.0
```
3. Inhabilite la aplicación de la prevención de fraude de cargos de llamada totalmente.
```
voice service voip
 no ip address trusted authenticate
```

Discado en dos etapas

Si se requiere el discado en dos etapas, lo que sigue se puede configurar para volver el comportamiento para hacer juego las versiones anteriores.

Para las llamadas ISDN entrantes:

```
voice service pots
 no direct-inward-dial isdn
```

Para las llamadas entrantes FXO:

```
voice-port <fxo-port>
 secondary dialtone
```

Entre en contacto el Centro de Asistencia Técnica de Cisco

Si usted ha completado todos los pasos de Troubleshooting y requiere la asistencia adicional, o si usted tiene cualquier preguntas más otra con respecto a este documento técnico del troubleshooting, entre en contacto el Centro de Asistencia Técnica (TAC) de Cisco Systems por uno de estos métodos:

- Abrir una solicitud de servicio en Cisco.com
- Vía correo electrónico

- Por teléfono

Información Relacionada

- Soporte de tecnología de voz
- Soporte de Productos de Voice and Unified Communications
- Troubleshooting de Cisco IP Telephony
- Soporte Técnico y Documentación - Cisco Systems

¿Era este documento útil? Sí ningún

Gracias por su feedback.

Abra un caso de soporte (requiere un contrato de servicios con Cisco.)

Discusiones relacionadas de la comunidad del soporte de Cisco

La comunidad del soporte de Cisco es un foro para que usted haga y conteste a las preguntas, las sugerencias de la parte, y colabora con sus pares.

Refiera a los convenios de los consejos técnicos de Cisco para la información sobre los convenios usados en este documento.

Actualizado: De julio el 29 de 2010
ID del Documento: 112083