IOS Release 15.1(2)T の電話ハッカーの侵入阻止機能

Document ID: 112083

Updated: 2010 年 7 月 29 日

PDF のダウンロード
印刷
フィードバック

関連製品

- Cisco Billing and Measurements Server
- Voice over Frame Relay (VoFR)
- 音声品質
- Cisco SC 2200 シグナリング コントローラ
- Skinny Client Control Protocol (SCCP)
- Cisco Digital Gateway DE-30+
- H.323
- メディア ゲートウェイ コントロール プロトコル (MGCP)
- Voice over ATM (VoATM)
- Signaling System 7 (SS7)
- + 詳細情報

目次

概要

Cisco IOS® を搭載して設置された音声ゲートウェイ (VGW) を電話ハッカーから防御するため

に、Cisco IOS ソフトウェア リリース 15.1(2)T に新機能が導入されました。 IOS 15.1(2)T 以降およびこのバージョンに基づく新しい IOS リリースでは、電話ハッカーの侵入阻止設定は、Cisco IOS ベースの VGW のデフォルト動作になっています。

このドキュメントでは、このリリースにアップグレードする場合は、特定のタイプのボイスコールを発信してルートを完結できるようにする追加設定が必要になるため、この新機能に対する意識を高めることを目的としています。 これらの送信元を信頼するように VGW を適切に設定するまでは、15.1(2)T へのアップグレードによって、すべての着信 VoIP コール セットアップがブロックされることに注意してください。 この機能を持つリリースへのアップグレード プランでは、コールが正常にルーティングされるように、アップグレード後に、信頼できる VoIP ホストを設定する追加の手順を含む必要があります。 また、このリリースでは、2 段階ダイヤリングがデフォルトでイネーブルにされなくなりました。

前提条件

要件

このドキュメントでは、読者は、音声ゲートウェイの設定に関する実務知識およびボイスコールの障害をデバッグする方法に関する基礎知識をすでに持っていると想定しています。

使用するコンポーネント

このドキュメントでは、Cisco IOS 音声ゲートウェイに適用される設定について説明します。これには、サービス統合型ルータ（ISR）を含みます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

15.1(2)T 以前の動作

15.1(2)T よりも前のいずれの IOS リリースでも、IOS 音声ゲートウェイは、すべての送信元からのコール セットアップを受け入れる動作がデフォルトになっています。 音声サービスがルータ上で実行されている限り、デフォルト設定では、任意の送信元 IP アドレスからのコール セットアップを正規で信頼できる送信元であると扱ってコールをセットアップします。 また、FXO ポートと ISDN 回線の着信コールでは、着信コールに対して 2 次ダイヤル トーンが提示され、その結果 2 段階ダイヤリングが可能になります。 これは、正しい着信ダイヤルピアと組み合わさっていることを想定しています。

15.1(2)T 以降のリリースでの動作

15.1(2)T 以降では、VoIP の送信元からのコール セットアップを信頼しない動作がルータのデフォルト動作です。 この機能により、TOLLFRAUD_APP という内部アプリケーションがデフォルトのコール制御スタックに追加されます。このアプリケーションは、コールをルーティングする

前にコール セットアップの送信元 IP をチェックします。 送信元 IP が、信頼できる VoIP 送信元として設定に含まれている明示的なエントリと一致しない場合、コールは拒否されます。

注: session target を使用して設定されたダイヤルピアがある場合、その IP からのコールは、信頼できるリストが設定されていなくても受け入れられます。

電話ハッカーの侵入阻止アプリケーションを含むバージョンの IOS をブートすると、ブート シーケンスの際に次の情報がデバイスのコンソールに表示されます。

```
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>]
```

ルータでは、VoIP ダイヤルピアに ipv4 ターゲットとして定義されているすべての宛先を、信頼できる送信元リストに自動的に追加します。 この動作は、次のコマンドの出力によって確認できます。

```
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
```

TOLLFRAUD_APP がコールをブロックしているかどうかを識別する方法

TOLLFRAUD_APP では、コールを拒否する場合、Q.850 接続解除原因値 21 を生成します。これは、「コールの拒否」を表します。 **debug voip ccapi inout** コマンドを実行すると、原因値を識別できます。

また、**voice iec syslog** をイネーブルにすると、コール障害が電話ハッカーの侵入阻止の結果であるかどうかをさらに確認できます。 この設定は、ゲートウェイの視点から障害の原因をトラブルシューティングするために便利な場合が多く、有料通話詐欺が原因でコールを拒否する場合にメッセージを出力します。 CCAPI および音声 IEC 出力を次のデバッグ出力に示します。

```
%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)
```

返されたコールをブロックしたときに返す Q.850 接続解除値も、次のコマンドを使用してデフォルトの 21 から変更できます。

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

15.1(2)T 以前の動作に戻す方法

送信元 IP アドレス信頼リスト

この信頼できるアドレスによる電話ハッカーの侵入阻止機能を実装する前の以前の音声ゲートウェイの動作に戻す方法は 3 通りあります。 このいずれの設定でも、設定を変更するには、すでに 15.1(2)T を実行している必要があります。

1. 正規の VoIP コールの信頼できるリストに追加する送信元 IP アドレスを明示的にイネーブルにします。 100 エントリまで定義できます。 次の設定では、ホスト 203.0.113.100/32 からのコールおよびネットワーク 192.0.2.0/24 からのコールを受け入れます。 他のホストからのコール セットアップは拒否されます。 音声セキュリティの観点から、この方法をお薦めします。
```
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. すべての送信元 IP アドレスからの着信コール セットアップを受け入れるようにルータを設定します。
```
voice service voip
 ip address trusted list
  ipv4 0.0.0.0 0.0.0.0
```
3. 電話ハッカーの侵入阻止アプリケーションを完全にディセーブルにします。
```
voice service voip
 no ip address trusted authenticate
```

2 段階ダイヤリング

2 段階ダイヤリングが必要な場合は、次の設定によって、ずっと前のリリースの動作に戻すことができます。

着信 ISDN コールの場合：

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

着信 FXO コールの場合：

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

Cisco Technical Assistance Center へのお問い合わせ

すべてのトラブルシューティング手順を完了してさらに支援を必要とするか、このトラブルシューティング テクニカル ドキュメントに関してさらに質問がある場合は、次のいずれかの方法により、シスコの Technical Assistance Center (TAC) に問い合わせてください。

- サービスリクエストをオープン
- E メールで問い合わせる
- 電話で問い合わせる

関連情報

- **音声に関する技術サポート**
- **音声とユニファイド コミュニケーションに関する製品サポート**
- Cisco IP Telephony のトラブルシューティング

- テクニカルサポートとドキュメント - Cisco Systems

このドキュメントは有用でしたか。 はい いいえ

フィードバックいただき、ありがとうございました。

サポート ケースのオープン（シスコ サービス契約< ts generic='1' nval='P%1,2%%'が必要です）。

Cisco サポート コミュニティ - 特集対話

Cisco サポート コミュニティでは、フォーラムに参加して情報交換することができます。

このドキュメントで使用されている表記法の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

Updated: 2010 年 7 月 29 日
Document ID: 112083