Toll−Fraud Prevention Feature in IOS Release 15.1(2)T

Document ID: 112083

Contents

Introduction

A new feature has been introduced in Cisco IOS® Software Release 15.1(2)T to guard against the incidence of toll−fraud on Voice GateWays (VGWs) installed with Cisco IOS. Starting with IOS 15.1(2)T and newer releases of IOS based on this version, the toll−fraud prevention settings are the default behavior of Cisco IOS−based VGWs.

The purpose of this document is to raise awareness of this new feature, as upgrading to this release will require additional configuration to permit certain types of voice calls to be placed and route to completion. It is important to note that upgrading to 15.1(2)T will block all inbound VoIP call setups until the VGW is properly configured to trust these sources. Any plans to upgrade to releases with this feature must include extra steps to configure trusted VoIP hosts after the upgrade in order for calls to route successfully. Additionally, two−stage dialing is no longer enabled by default with this release.

Prerequisites

Requirements

This document assumes that the reader already has a working knowledge on voice gateway configuration, as well as fundamental knowledge on how to debug voice call failures.

Components Used

The document discusses configurations that apply to Cisco IOS Voice Gateways, which would include the Integrated Services Routers (ISRs).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Behavior Before 15.1(2)T

For all IOS releases before 15.1(2)T, the default behavior for IOS voice gateways is to accept call setups from all sources. As long as voice services are running on the router, the default configuration will treat a call setup from any source IP address as a legitimate and trusted source to set a call up for. Also, FXO ports and inbound calls on ISDN circuits will present secondary−dial tone for inbound calls, allowing for two−stage dialing. This assumes a proper inbound dial−peer is being matched.

Behavior with 15.1(2)T and Later Releases

Starting with 15.1(2)T, the router s default behavior is to not trust a call setup from a VoIP source. This feature adds an internal application named TOLLFRAUD_APP to the default call control stack, which checks the source IP of the call setup before routing the call. If the source IP does not match an explicit entry in the configuration as a trusted VoIP source, the call is rejected.

Note: If you have dial−peers configured with session target, calls from those IPs will be accepted even if there is no trusted list configured.

When booting a version of IOS with the toll−fraud prevention application, this is printed to the device s console during the boot sequence:

```
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>]
```

The router automatically adds any destinations that are defined as an ipv4 target in a VoIP dial−peer to the trusted source list. You can observe this behavior with the output of this command:

```
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
```

How to Identify if TOLLFRAUD_APP is Blocking Your Call

If the TOLLFRAUD_APP is rejecting the call, it generates a Q.850 disconnect cause value of 21, which represents Call Rejected . The **debug voip ccapi inout** command can be run to identify the cause value.

Additionally, **voice iec syslog** can be enabled to further verify if the call failure is a result of the toll−fraud prevention. This configuration, which is often handy to troubleshoot the origin of failure from a gateway perspective, will print out that the call is being rejected due to toll call fraud. The CCAPI and Voice IEC output is demonstrated in this debug output:

```
%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)
```

The Q.850 disconnect value that is returned for blocked calls can also be changed from the default of 21 with this command:

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

How to Return to Pre−15.1(2)T Behavior

Source IP Address Trust List

There are three ways to return to the previous behavior of voice gateways before this trusted address toll−fraud prevention feature was implemented. All of these configurations require that you are already running 15.1(2)T in order for you to make the configuration change.

1. Explicitly enable those source IP addresses from which you would like to add to the trusted list for legitimate VoIP calls. Up to 100 entries can be defined. This below configuration accepts calls from those host 203.0.113.100/32, as well as from the network 192.0.2.0/24. Call setups from all other hosts are rejected. This is the recommended method from a voice security perspective.

   ```
   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 the router to accept incoming call setups from all source IP addresses.

   ```
   voice service voip
    ip address trusted list
     ipv4 0.0.0.0 0.0.0.0
   ```
3. Disable the toll−fraud prevention application completely.

   ```
   voice service voip
    no ip address trusted authenticate
   ```

Two−Stage Dialing

If two−stage dialing is required, the following can be configured to return behavior to match previous releases.

For inbound ISDN calls:

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

For inbound FXO calls:

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

Contact the Cisco Technical Assistance Center

If you have completed all troubleshooting steps and require further assistance, or if you have any further questions regarding this troubleshooting technical document, contact the Cisco Systems Technical Assistance Center (TAC) by one of these methods:

- Open a service request on Cisco.com
- By email
- By telephone

Related Information

- **Voice Technology Support**
- **Voice and Unified Communications Product Support**
- **Troubleshooting Cisco IP Telephony**
- **Technical Support & Documentation − Cisco Systems**

Updated: Jul 29, 2010 Document ID: 112083
