关于防止语音网关被盗用的最佳实践

目录

技术领域

H323, SIP , TCL, COR

问题描述

尽管事实情况是没有任何内部用户拨打过国际或省际长途电话，但用户的电信账单依然出现了难以置信的高额费用。记录显示，用户曾经频繁、长时间联系国际和省际的长途用户，从而产生了非常高的长途费用。本文介绍如何发现并防止语音网关被盗用的实例。

最佳实践

防止来自IP网络的盗用

如果用户的语音网关有Internet/Intranet可达的IP地址，但没有配置足够的安全特性，任何voip的终端都有可能跳过管理员的耳目，实现越权拨打电话。针对此类风险，我们建议的最佳实践如下：

在网关上增加访问列表，除了允许信任的远端voip设备和所有telnet之外，其他所有的tcp连接一概拒绝。

```
access-list 100 permit ip host 192.168.1.1 host 10.0.0.87
!192.168.1.1
access-list 100 permit tcp any host 10.0.0.87 eq 23
! (telnet)
access-list 100 permit udp any any  range 16384 32768
!RTP
access-list  100 deny ip any any
!  (H323,SIP)
!
interface g0/0
ip address 10.0.0.87 255.255.255.0
ip access-group 100 in
!,IP
```

防止来自PSTN的盗用

当用户使用了基于TCL的自动话务员系统的时候，不安全的配置同样会给来自PSTN的非法用户以可乘之机。例如，当非法用户打到基于TCL的自动话务员的时候，系统提示输入分机号码，而他输入的是90019723451234，如果用户的网关正好使用的是出局加9（destination-

pattern 9T 打向出局的E1/FXO）的话，那么这个用户就会被连接到美国的号码为9723451234。

COR (class of restriction)是Cisco IOS 内置的用来实现呼叫权限管理的特性，它能够帮助我们用来防止面向PSTN的hairpin的呼叫的发生，配置案例如下。

```
dial-peer cor custom
name Voip
name PSTN
!
dial-peer cor list PSTN
member PSTN
!
dial-peer cor list All
member Voip
member PSTN
!
dial-peer voice 101 pots
 corlist incoming PSTN
 description "matched all Incoming calls"
 service AA
 incoming called-number .T
direct-inward-dial
 port 2/0:15
!
dial-peer voice 102 pots
 corlist outgoing All
 description "matched all Outgoing calls"
 destination-pattern 9T
 port 2/0:15
```

如果用户有多个E1， dial-peer voice 101和102的配置需要复制为201和202。根据上面的配置，如果用户打到AA上面，并输入90019723451234， dial-peer 102不会被match，所以阻止了对这条E1的国际长途盗用。