当Verizon是运营商时，排除IP源违规故障

目录

简介

本文档介绍如何对Verizon作为运营商时经常出现的IP源违规问题进行故障排除。

先决条件

要求

Cisco 建议您具有以下主题的基础知识：

- 5G蜂窝网络基础
- 思科蜂窝网网关522-E
- 思科P-5GS6-GL模块
- 思科IOS-XE
- 思科IOS-CG

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 蜂窝网关522-E，带IOS-CG版本17.9.5a。
- 插入P-5GS6-GL模块的IR1101，带IOS-XE版本17.9.5。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

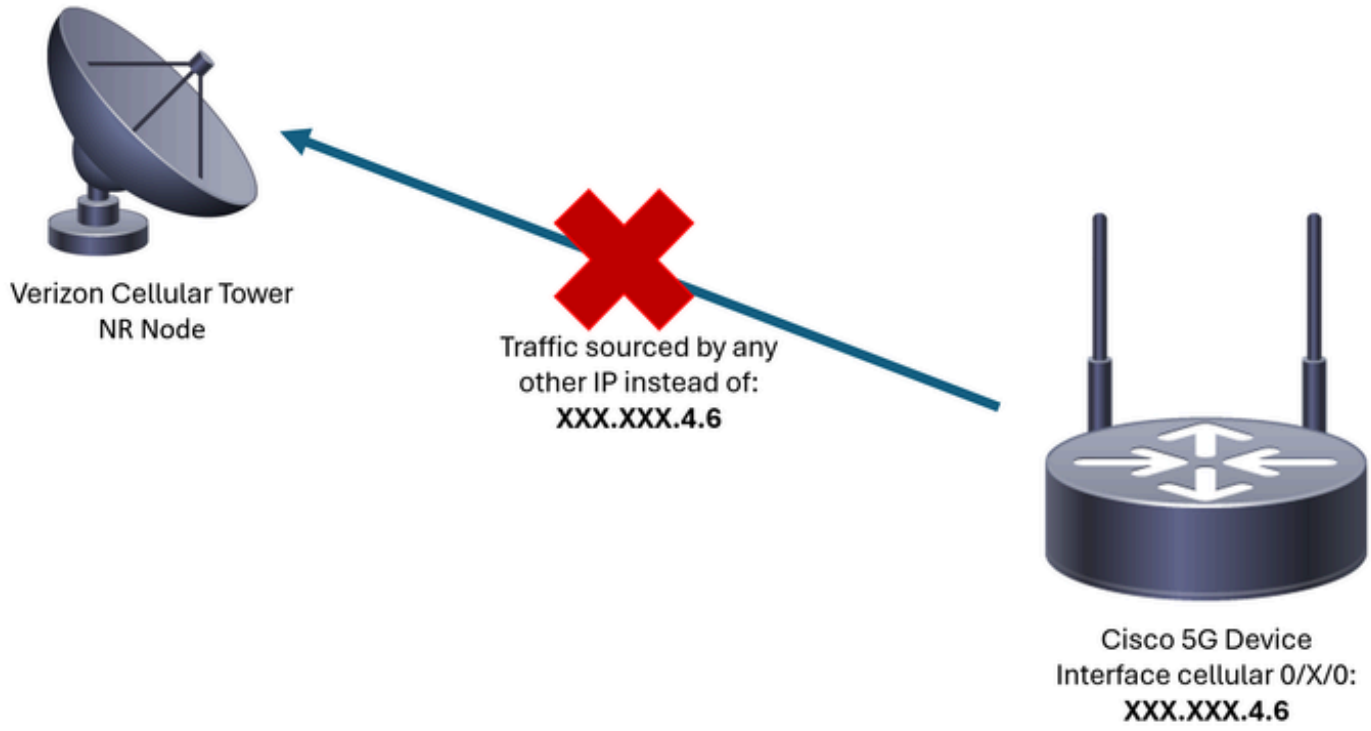
这适用于以单机模式连接到路由器的P-5GS6-GL模块，或以SD-WAN管理的单机或控制器模式连接到路由器的CG522-E。本文档不适用于连接到SD-WAN中路由器的P-5GS6-GL模块，因为命令语法不同。

问题

Verizon专门为每个客户端/SIM分配一个IP地址，并且他们始终期望接收仅来自该IP的流量。

当Verizon检测到从客户端发送的流量来自与之前分配的不同IP时，就会发生源违规。

例如，如果分配了IP地址XXX.XXX.4.6，并且Verizon收到来自IP地址XXX.XXX.8.9的流量，则问题存在：



每次Verizon收到来自具有不同IP地址的设备的10个以上数据包时，与蜂窝网络的连接就会抖动和停止。因此，从蜂窝设备发起新的连接，并且它可获取与以前相同的IP地址或新的IP地址。这取决于获得的服务。

检测连接到路由器的P-5GS6-GL模块中的问题

当命令的输出中存在图中所示的断开原因时，将置入源违规：

<#root>

isr#

show cellular 0/X/0 call-history

```
                              *
                              *
[Wed May    8  18:46:26   2024]   Session disconnect reason = Regular deactivation (36)

                              *
                              *
```

如果之前的输出未提供信息（由于缓冲区进程），则可以使用以下命令执行Netflow数据包捕获：

```
isr#conf t
isr(config)#flow record NETFLOW_MONITOR
isr(config-flow-record)#match ipv4 protocol
isr(config-flow-record)#match ipv4 source address
isr(config-flow-record)#match ipv4 destination address
isr(config-flow-record)#match transport source-port
isr(config-flow-record)#match transport destination-port
isr(config-flow-record)#collect ipv4 source prefix
isr(config-flow-record)#collect ipv4 source mask
isr(config-flow-record)#collect ipv4 destination prefix
isr(config-flow-record)#collect ipv4 destination mask
isr(config-flow-record)#collect interface output
isr(config-flow-record)#exit

isr(config)#flow monitor NETFLOW_MONITOR
isr(config-flow-monitor)#cache timeout active 60
isr(config-flow-monitor)#record NETFLOW_MONITOR
isr(config-flow-monitor)#exit

isr(config)#interface cellular 0/X/0
isr(config-if)#ip flow monitor NETFLOW_MONITOR output
isr(config-if)#exit
```

要查看捕获的输出，请执行以下操作：

<#root>

isr#

show flow monitor NETFLOW_MONITOR cache format table

可以使用以下命令查看Verizon为设备分配的IP地址：

<#root>

isr#

show ip interface brief

```
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES NVRAM  administratively down down
FastEthernet0/0/1      unassigned      YES unset  down                  down
FastEthernet0/0/2      unassigned      YES unset  down                  down
FastEthernet0/0/3      unassigned      YES unset  down                  down
FastEthernet0/0/4      unassigned      YES unset  down                  down

Cellular0/1/0          IP_address      YES IPCP   up                    up


Cellular0/1/1          unassigned      YES NVRAM  administratively down down
Async0/2/0             unassigned      YES unset  up                    down
Vlan1                  unassigned      YES unset  up                    down
```

如果在Netflow的日志中捕获任何流量，系统会报告其来源与蜂窝网接口中确认的不同IP地址。存在源违规。

连接到路由器的P-5GS6-GL模块的解决方案

目标是确保所有流量仅通过Verizon分配的IP发送。有多种方法可以实现此目标。其实施取决于部署和网络要求：

- 选项1：用于出站流量的ACL
- 通过访问控制列表，您可以确保从设备发送的流量仅来自Verizon IP地址：

```
isr#conf t
isr(config)#ip access-list extended 196
isr(config-ext-nacl)#permit ip host <IP_Assigned_by_Verizon> any
isr(config-ext-nacl)#deny ip any any
isr(config-ext-nacl)#exit

isr(config)#interface cellular 0/X/0
isr(config-if)#ip access-group 196 out
isr(config-if)#end
```

- 选项2：用于内部流量的NAT
- 必须满足以下要求：
    1. 蜂窝网接口配置为“ip nat outside”。
    2. 局域网接口配置为“ip nat inside”。
    3. 实施NAT过载(PAT)，因此也会转换所有端口。
    4. 使用ACL定义要进行NAT处理的流量。

配置示例：

<#root>

```
isr#conf t


isr(config)#interface cellular 0/X/0
isr(config-if)#ip nat outside
isr(config-if)#exit

isr(config)#interface vlan 6
isr(config-if)#ip nat inside
isr(config-if)#exit

isr(config)#access-list 20 permit <IPv4_subnet_to_be_NATed> <wildcard>
isr(config)#ip nat inside source list 20 interface cellular 0/1/0 overload
```

- 选项3：实施IPsec或任何其他隧道配置
- 此隧道使用Verizon分配的IP地址完成。当所有流量都流经内部时，外部IP地址始终不变。
- 选项4：实施路由映射
- 如果有路由器生成的流量，则可以实施路由映射，以便正确发出流量。例如，继续向DNS发出ping命令，确保存在“Internet连接”，而且可以实施路由映射，确保正确发出流量。

对连接到路由器的Cisco P-5GS6-GL模块中的源违规进行故障排除的过程到此结束。

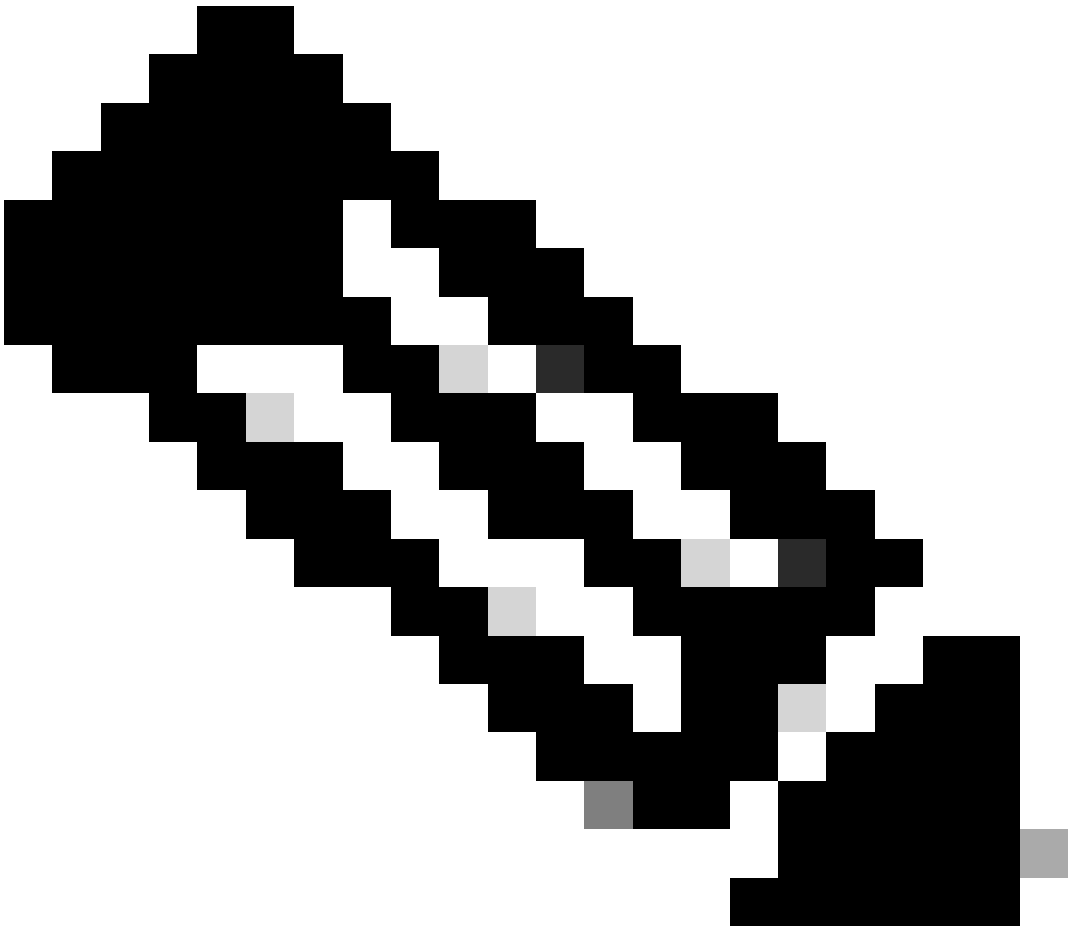
CG522-E中的IP源违规

默认情况下，在这些设备的代码中会激活用于消除此问题的功能。

证实设备显示以下输出：

```
<#root>
CellularGateway#
show cellular 1 drop-stats


Ip Source Violation details:


Ipv4 Action = Drop


  Ipv4 Packets Drop = 0
  Ipv4 Bytes Drop   = 0

  Ipv6 Action = Drop


  Ipv6 Packets Drop = 0
  Ipv6 Bytes Drop   = 0
```

Ipv4/Ipv6操作的状态必须为丢弃。 表示已启用该功能。



注意：如果输出显示Permit，则禁用该功能。

使用这些命令可重新激活功能：

```
CellularGateway#conf t
CellularGateway(config)# controller cellular 1
CellularGateway(config-cellular-1)# no ip-source-violation-action ipv4-permit
CellularGateway(config-cellular-1)# no ip-source-violation-action ipv6-permit
CellularGateway(config-cellular-1)# commit
Commit complete.
CellularGateway(config-cellular-1)# end
```

对Cisco CG522-E中的源违规进行故障排除的过程到此结束。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。