Solucionar problemas de violación de origen de IP cuando Verizon es el operador

Contenido

Introducción

Este documento describe cómo resolver problemas de violación de origen de IP, que es un problema frecuente cuando Verizon es el portador.

Prerequisites

Requirements

Cisco recomienda tener conocimientos básicos sobre estos temas:

- Fundamentos de la red móvil 5G
- Gateway Móvil 522-E De Cisco
- Módulo Cisco P-5GS6-GL
- Cisco IOS-XE
- Cisco IOS-CG

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Gateway móvil 522-E con IOS-CG versión 17.9.5a.

- IR1101 con IOS-XE versión 17.9.5 con un módulo P-5GS6-GL conectado.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

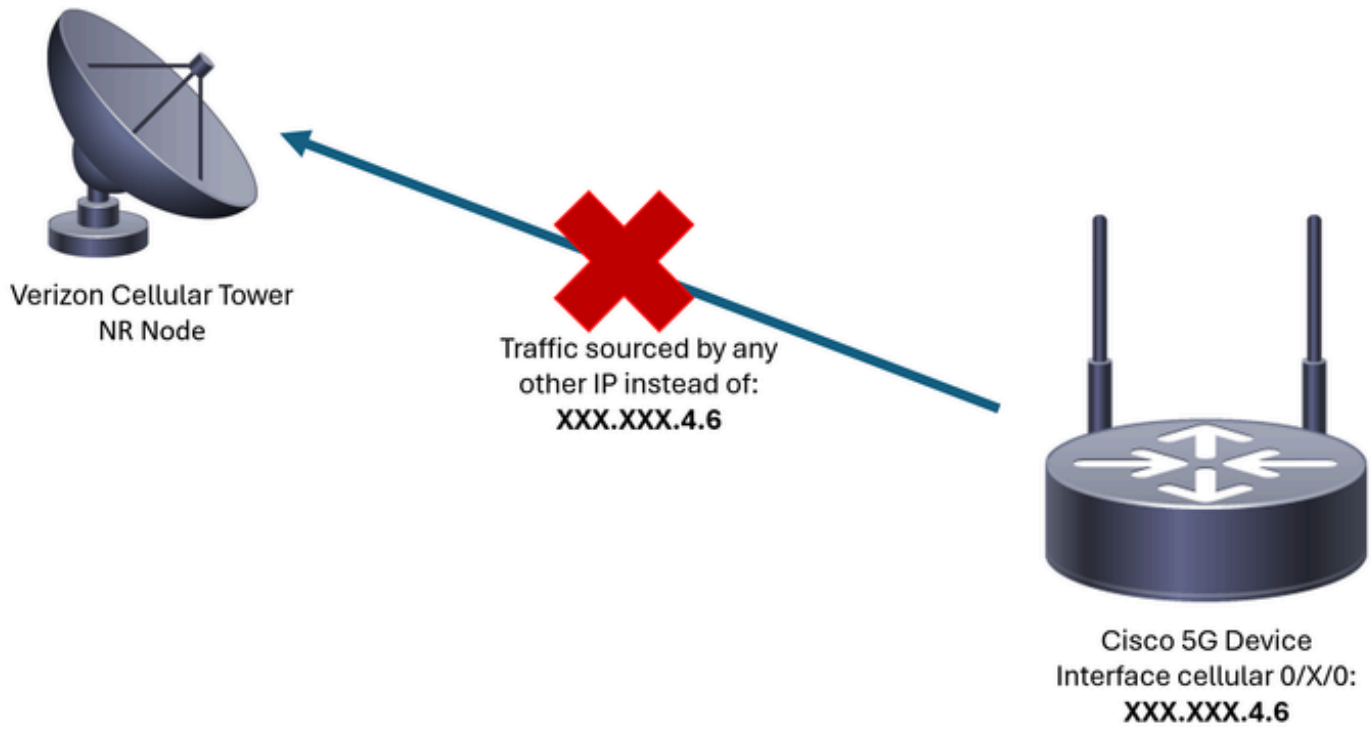
Esto se aplica a un módulo P-5GS6-GL conectado a un router en modo autónomo o a un CG522-E en modo independiente o controlador administrado por SD-WAN. Este documento no se aplica a un módulo P-5GS6-GL conectado a un router en SD-WAN ya que la sintaxis del comando es diferente.

Problema

Verizon asigna una dirección IP específicamente a cada cliente/SIM, y siempre esperan recibir tráfico originado solamente desde esa IP.

La violación de origen ocurre cuando Verizon detecta que el tráfico enviado desde el cliente es originado por una IP diferente de la que asignó previamente.

Por ejemplo, si se asignó la dirección IP XXX.XXX.4.6 y Verizon recibe tráfico de la dirección IP XXX.XXX.8.9, el problema está presente:



Cada vez que Verizon recibe más de 10 paquetes del dispositivo con una dirección IP diferente, la conexión a la red celular se inestabiliza y se detiene. Como resultado, se inicia una nueva

conexión desde el dispositivo móvil, y puede obtener la misma dirección IP que antes o una nueva. Depende del servicio adquirido.

Detecte el problema en un módulo P-5GS6-GL conectado a un router

Cuando la razón de desconexión mostrada está presente en la salida del comando, la violación de origen está en lugar:

<#root>

```
isr#
show cellular 0/X/0 call-history

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

                              *
                              *
```

Si la salida anterior no proporciona información (debido al proceso de buffer), se puede tomar una captura de paquetes de Netflow con estos comandos:

```
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
```

Para ver el resultado de la captura:

```
<#root>

isr#

show flow monitor NETFLOW_MONITOR cache format table
```

La dirección IP asignada por Verizon al dispositivo se puede ver con el comando:

```
<#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
```

Si en los registros de Netflow se captura cualquier tráfico, se informa que se originó con una dirección IP diferente de la confirmada en la interfaz celular. La violación de origen está presente.

Solución para un módulo P-5GS6-GL conectado a un router

El objetivo es garantizar que todo el tráfico se envíe únicamente con origen en la IP asignada por Verizon. Hay diferentes métodos que cumplen este objetivo. Su implementación depende de la implementación y de los requisitos de la red:

- Opción 1: ACL para tráfico saliente
- Con una Lista de control de acceso, puede asegurarse de que el tráfico enviado desde el dispositivo se origina solamente desde la Dirección IP de Verizon:

```
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
```

- Opción 2: NAT para tráfico interno

- Estos requisitos deben cumplirse:
    1. La interfaz móvil se configura como "ip nat outside".
    2. La interfaz LAN se configura como "ip nat inside".
    3. La sobrecarga NAT (PAT) se implementa para que todos los puertos también se traduzcan.
    4. El uso de una ACL para definir el tráfico que se NATed.

Ejemplo de configuración:

<#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
```

- Opción 3: Implemente una Configuración de Túnel IPsec o Cualquier Otra

- Este túnel se realiza con la dirección IP asignada por Verizon. Como todo el tráfico viaja dentro de él, la dirección IP externa nunca cambia.

- Opción 4: Implementar un mapa de ruta

- Si hay tráfico generado por el router, se puede implementar un mapa de ruta para que el tráfico se origine correctamente. Por ejemplo, un cliente continúa haciendo ping a un DNS para asegurarse de que hay "conectividad a Internet" y se puede implementar un mapa de rutas para que el tráfico se origine correctamente.

Esto finaliza el procedimiento para resolver problemas de violación de origen en un módulo Cisco P-5GS6-GL conectado a un router.

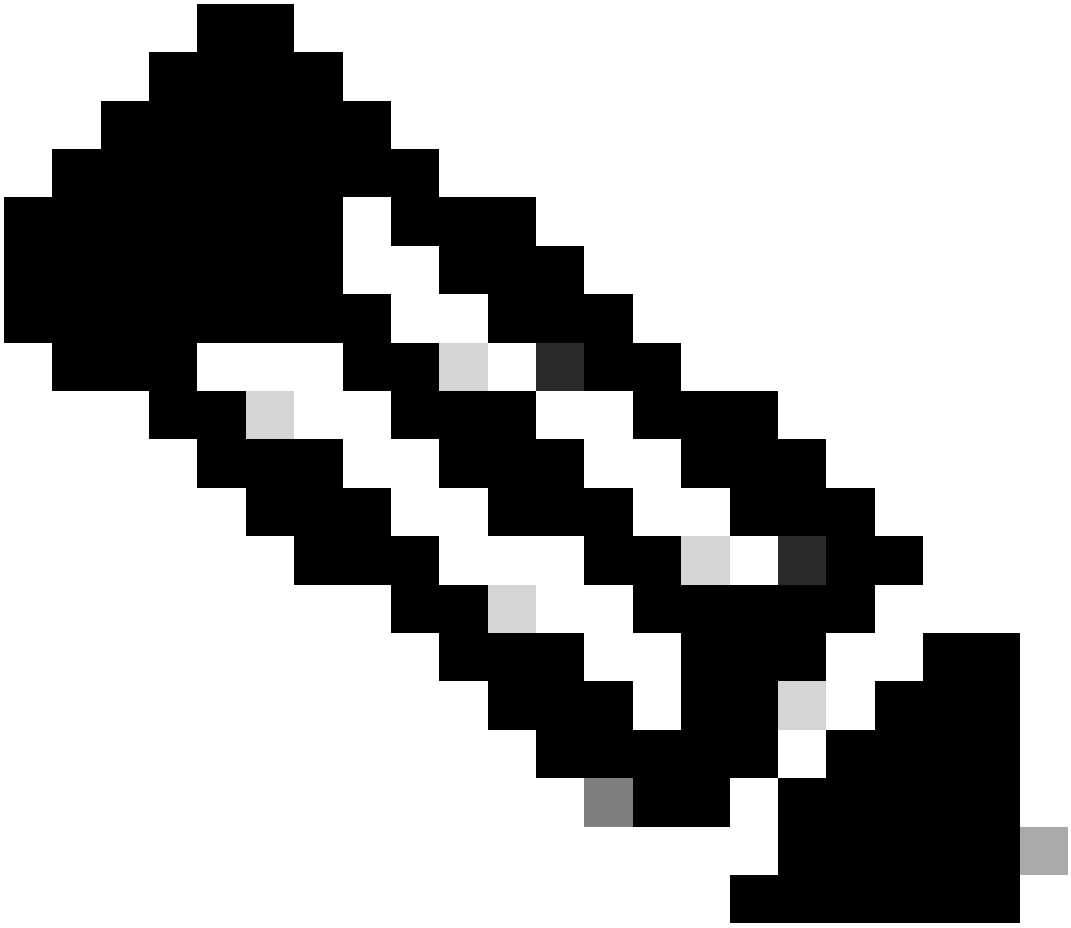
Violación de IP de Origen en un CG522-E

De forma predeterminada, se activa una función para eliminar este problema en el código de estos dispositivos.

Corroborar que el dispositivo muestra esta salida:

```
<#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
```

El estado de la acción Ipv4/Ipv6 debe ser Drop. Significa que la función está habilitada.



Nota: Si la salida indica Permitir, la función está desactivada.

Con estos comandos, la función se puede reactivar:

```
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
```

Esto finaliza el procedimiento para resolver problemas de violación de origen en un Cisco CG522-E.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).