

Solucionar problemas de violação de origem de IP quando a Verizon é a operadora

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Problema](#)

[Detecte o problema em um módulo P-5GS6-GL conectado a um roteador](#)

[Solução para um módulo P-5GS6-GL conectado a um roteador](#)

[Opção 1: ACL para tráfego de saída](#)

[Opção 2: NAT para tráfego interno](#)

[Opção 3: Implementar um IPsec ou qualquer outra configuração de túnel](#)

[Opção 4: Implementar um mapa de rotas](#)

[Violação de origem de IP em um CG522-E](#)

Introdução

Este documento descreve como solucionar problemas de violação de origem de IP, que é um problema frequente quando a Verizon é a operadora.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento básico destes tópicos:

- Conceitos Básicos de Redes Celulares 5G
- Gateway celular Cisco 522-E
- Módulo Cisco P-5GS6-GL
- Cisco IOS-XE
- Cisco IOS-CG

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Gateway celular 522-E com IOS-CG versão 17.9.5a.
- IR1101 com IOS-XE versão 17.9.5 com um módulo P-5GS6-GL conectado.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

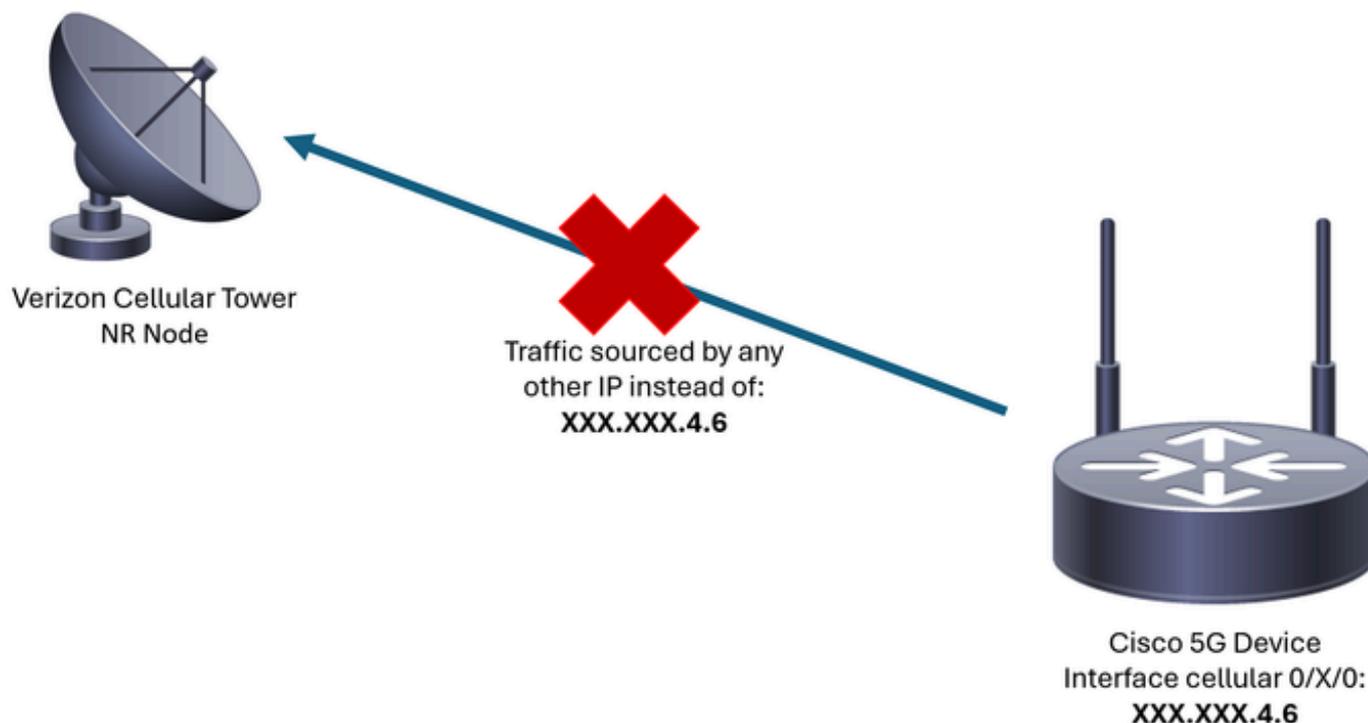
Isso se aplica a um módulo P-5GS6-GL conectado a um roteador no modo autônomo ou a um CG522-E no modo autônomo ou no modo de controlador gerenciado pelo SD-WAN. Este documento não se aplica a um módulo P-5GS6-GL conectado a um roteador em SD-WAN, já que a sintaxe do comando é diferente.

Problema

A Verizon atribui um endereço IP especificamente a cada cliente/SIM e eles sempre esperam receber o tráfego originado apenas desse IP.

A violação de origem ocorre quando a Verizon detecta que o tráfego enviado do cliente é originado por um IP diferente daquele atribuído anteriormente.

Por exemplo, se o endereço IP XXX.XXX.4.6 foi atribuído e a Verizon recebe tráfego do endereço IP XXX.XXX.8.9, o problema está presente:



Toda vez que a Verizon recebe mais de 10 pacotes do dispositivo com um endereço IP diferente, a conexão com a rede celular oscila e pára. Como resultado, uma nova conexão é iniciada do dispositivo celular e pode obter o mesmo endereço IP que antes ou um novo. Depende do serviço adquirido.

Detecte o problema em um módulo P-5GS6-GL conectado a um roteador

Quando o motivo de desconexão mostrado está presente na saída do comando, a violação de origem é colocada:

```
<#root>
```

```
isr#
```

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

```

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

Se a saída anterior não fornecer informações (devido ao processo de buffer), uma captura de pacote do Netflow poderá ser realizada com estes 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 a saída da captura:

```
<#root>
```

```
isr#
```

```
show flow monitor NETFLOW_MONITOR cache format table
```

O endereço IP atribuído pela Verizon ao dispositivo pode ser visto com o 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

Se nos registros do Netflow capturar qualquer tráfego, ele será informado originado com um endereço IP diferente daquele confirmado na interface do celular. A violação de origem está presente.

Solução para um módulo P-5GS6-GL conectado a um roteador

O objetivo é garantir que todo o tráfego seja enviado apenas com origem no IP atribuído pela Verizon. Há diferentes métodos para atingir essa meta. Sua implementação depende da implantação e dos requisitos de rede:

- Opção 1: ACL para tráfego de saída
- Com uma lista de controle de acesso, você pode garantir que o tráfego enviado do dispositivo seja apenas originado do endereço IP da 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
```

- Opção 2: NAT para tráfego interno
- Estes requisitos devem ser cumpridos:
 1. A interface do celular está configurada como "ip nat outside".
 2. A interface da LAN está configurada como "ip nat inside".
 3. A sobrecarga de NAT (PAT) é implementada para que todas as portas também sejam convertidas.
 4. O uso de uma ACL para definir o tráfego a ser NATed.

Exemplo de configuração:

```
<#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
```

- Opção 3: Implementar um IPsec ou qualquer outra configuração de túnel
- Esse túnel é feito com o endereço IP atribuído pela Verizon. Como todo o tráfego trafega dentro dele, o endereço IP externo nunca muda.
- Opção 4: Implementar um mapa de rotas
- Se houver tráfego gerado pelo roteador, um mapa de rotas pode ser implementado para que o tráfego seja originado corretamente. Por exemplo, a continua fazendo ping para um DNS, para garantir que haja "conectividade com a Internet", e um mapa de rotas pode ser implementado para que o tráfego seja originado corretamente.

Isso encerra o procedimento para solucionar problemas de violação de origem em um módulo Cisco P-5GS6-GL conectado a um roteador.

Violação de origem de IP em um CG522-E

Por padrão, um recurso para eliminar esse problema é ativado no código desses dispositivos.

Confirme se o dispositivo mostra esta saída:

```
<#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
```

O estado da Ação Ipv4/Ipv6 deve ser Drop. Isso significa que o recurso está ativado.

Observação: se a saída disser Permit, o recurso será desabilitado.

Com esses comandos, o recurso pode ser reativado:

```
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
```

Isso encerra o procedimento para solucionar problemas de violação de origem em um Cisco CG522-E.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.