# Verizon이 통신사인 경우 IP 소스 위반 문제 해결

## 목차



## 소개

이 문서에서는 Verizon이 통신사업자인 경우 자주 발생하는 IP 소스 위반 문제를 해결하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

Cisco에서는 다음 항목에 대한 기본 지식을 갖춘 것을 권장합니다.

- 5G 셀룰러 네트워크 기본 사항
- Cisco Cellular Gateway 522-E
- Cisco P-5GS6-GL 모듈
- Cisco IOS-XE
- Cisco IOS-CG

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cellular Gateway 522-E with IOS-CG version 17.9.5a.
- IOS-XE 버전 17.9.5의 IR1101(P-5GS6-GL 모듈 연결)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

이는 독립형 모드의 라우터에 연결된 P-5GS6-GL 모듈 또는 SD-WAN에서 관리하는 독립형 또는 컨트롤러 모드의 CG522-E에 적용됩니다. 이 문서는 명령 구문이 다르므로 SD-WAN의 라우터에 연결된 P-5GS6-GL 모듈에는 적용되지 않습니다.

## 문제

Verizon은 각 클라이언트/SIM에 특별히 IP 주소를 할당하며, 항상 해당 IP에서 제공된 트래픽만 수신하려고 합니다.

Verizon에서 클라이언트에서 전송된 트래픽이 이전에 할당한 IP와 다른 IP에 의해 소싱됨을 탐지하면 소스 위반이 발생합니다.

예를 들어, IP 주소 XXX.XXX.4.6이 할당되었고 Verizon이 IP 주소 XXX.XXX.8.9에서 트래픽을 수신하는 경우, 문제가 발생합니다.


Verizon이 디바이스에서 다른 IP 주소로 10개가 넘는 패킷을 수신할 때마다 셀룰러 네트워크에 대한 연결이 끊기고 중단됩니다. 그 결과 셀룰러 디바이스에서 새 연결이 시작되고 이전과 동일한 IP 주소 또는 새 IP 주소를 가져올 수 있습니다. 획득한 서비스에 따라 다릅니다.

### 라우터에 연결된 P-5GS6-GL 모듈에서 문제 감지

명령 출력에 표시된 연결 끊기 이유가 있는 경우 소스 위반이 적용됩니다.

<#root>

isr#

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

*
*

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

*
*

버퍼 프로세스로 인해 이전 출력에서 정보를 제공하지 않을 경우 다음 명령으로 Netflow 패킷 캡처를 수행할 수 있습니다.

```
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
```

캡처 출력을 보려면

<#root>

isr#

**show flow monitor NETFLOW_MONITOR cache format table**

Verizon이 디바이스에 할당한 IP 주소는 다음 명령을 사용하여 확인할 수 있습니다.

<#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 |

Netflow의 로그에서 트래픽을 캡처하는 경우 셀룰러 인터페이스에 확인된 것과 다른 IP 주소로 소스가 보고됩니다. 소스 위반이 있습니다.

# 라우터에 연결된 P-5GS6-GL 모듈용 솔루션

목표는 모든 트래픽이 Verizon에서 할당한 IP를 통해서만 전송되도록 하는 것입니다. 이 목표를 충족시키는 다른 방법들이 있습니다. 구축 및 네트워크 요구 사항에 따라 구현이 달라집니다.

- 옵션 1: 아웃바운드 트래픽용 ACL
- 액세스 제어 목록을 사용하면 디바이스에서 전송된 트래픽이 Verizon IP 주소에서만 제공되는지 확인할 수 있습니다.

```
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
```

- 옵션 2: 내부 트래픽용 NAT
- 다음 요건을 충족해야 합니다.
    1. 셀룰러 인터페이스는 "ip nat outside"로 구성됩니다.
    2. LAN 인터페이스는 "ip nat inside"로 구성됩니다.
    3. PAT(NAT overload)가 구현되어 모든 포트도 변환됩니다.

4. NAT할 트래픽을 정의하는 데 ACL을 사용합니다.

컨피그레이션 예시:

<#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
```

- 옵션 3: IPsec 또는 기타 터널 컨피그레이션 구현
- 이 터널은 Verizon이 할당한 IP 주소로 수행됩니다. 모든 트래픽이 내부에서 이동하므로 외부 IP 주소는 변경되지 않습니다.
- 옵션 4: 경로 맵 구현
- 라우터에서 생성한 트래픽이 있는 경우, 트래픽이 올바르게 소싱되도록 경로 맵을 구현할 수 있습니다. 예를 들어 는 DNS에 대해 ping을 계속 수행하여 "인터넷 연결"이 있는지 확인하고, 트래픽이 올바르게 소싱되도록 경로 맵을 구현할 수 있습니다.

라우터에 연결된 Cisco P-5GS6-GL 모듈에서 소스 위반 문제를 해결하는 절차를 종료합니다.

# CG522-E의 IP 소스 위반

기본적으로 이러한 장치의 코드에서 이 문제를 제거하는 기능이 활성화되어 있습니다.

장치에서 이 출력을 표시함을 입증합니다.

<#root>

```
CellularGateway#

show cellular 1 drop-stats


Ip Source Violation details:


Ipv4 Action = Drop
```

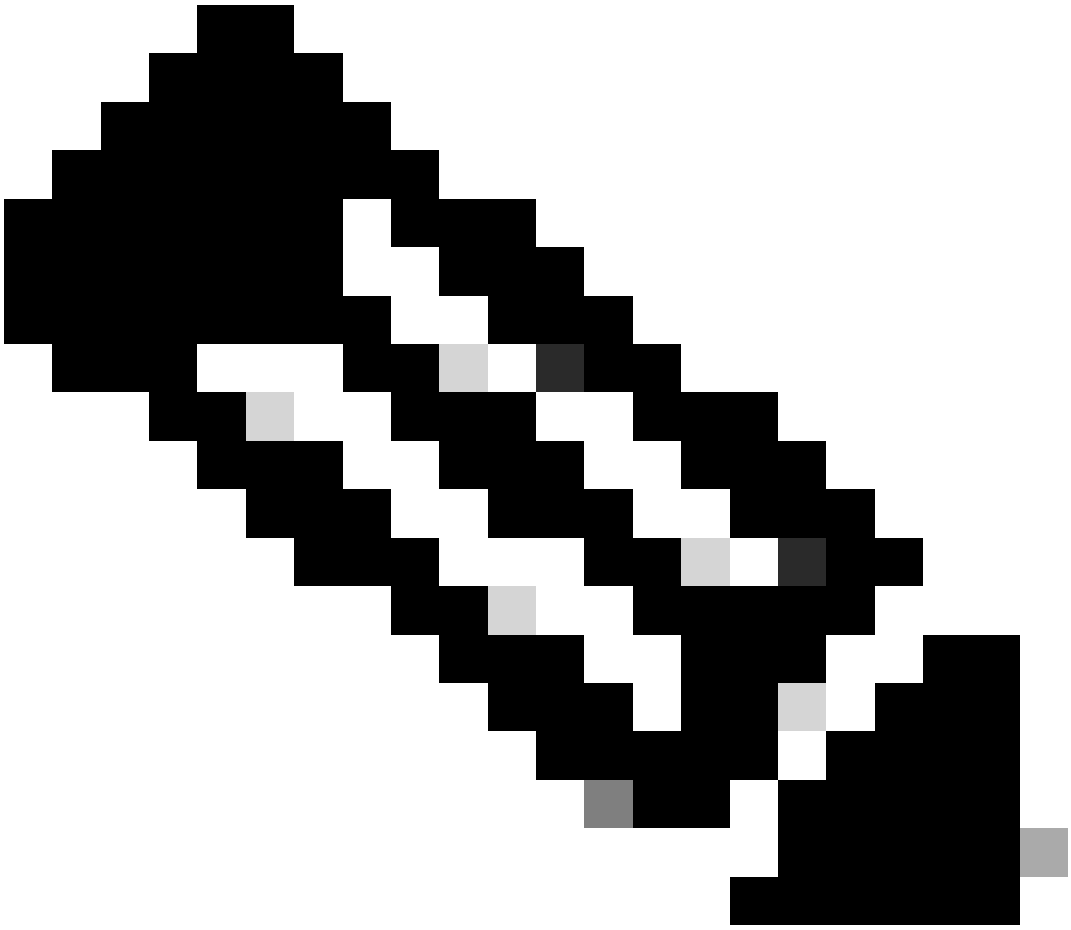
```
  Ipv4 Packets Drop = 0
  Ipv4 Bytes Drop   = 0

  Ipv6 Action = Drop


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

Ipv4/Ipv6 Action의 상태는 Drop이어야 합니다. 이는 해당 기능이 활성화되었음을 의미합니다.

---



참고: 출력에 Permit이 표시되면 이 기능은 비활성화됩니다.

---

다음 명령을 사용하여 기능을 다시 활성화할 수 있습니다.

```
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
```

이렇게 하면 Cisco CG522-E에서 소스 위반을 트러블슈팅하는 절차가 종료됩니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.