Risoluzione dei problemi relativi alla violazione dell'origine IP quando il vettore è Verizon

Sommario

Introduzione

Questo documento descrive come risolvere i problemi di violazione dell'origine IP che sono un problema frequente quando Verizon è il vettore.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Nozioni di base sulla rete cellulare 5G
- Cisco Cellular Gateway 522-E
- Modulo Cisco P-5GS6-GL
- Cisco IOS-XE
- Cisco IOS-CG

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cellular Gateway 522-E con IOS-CG versione 17.9.5a.

- IR1101 con IOS-XE versione 17.9.5 con un modulo P-5GS6-GL collegato.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

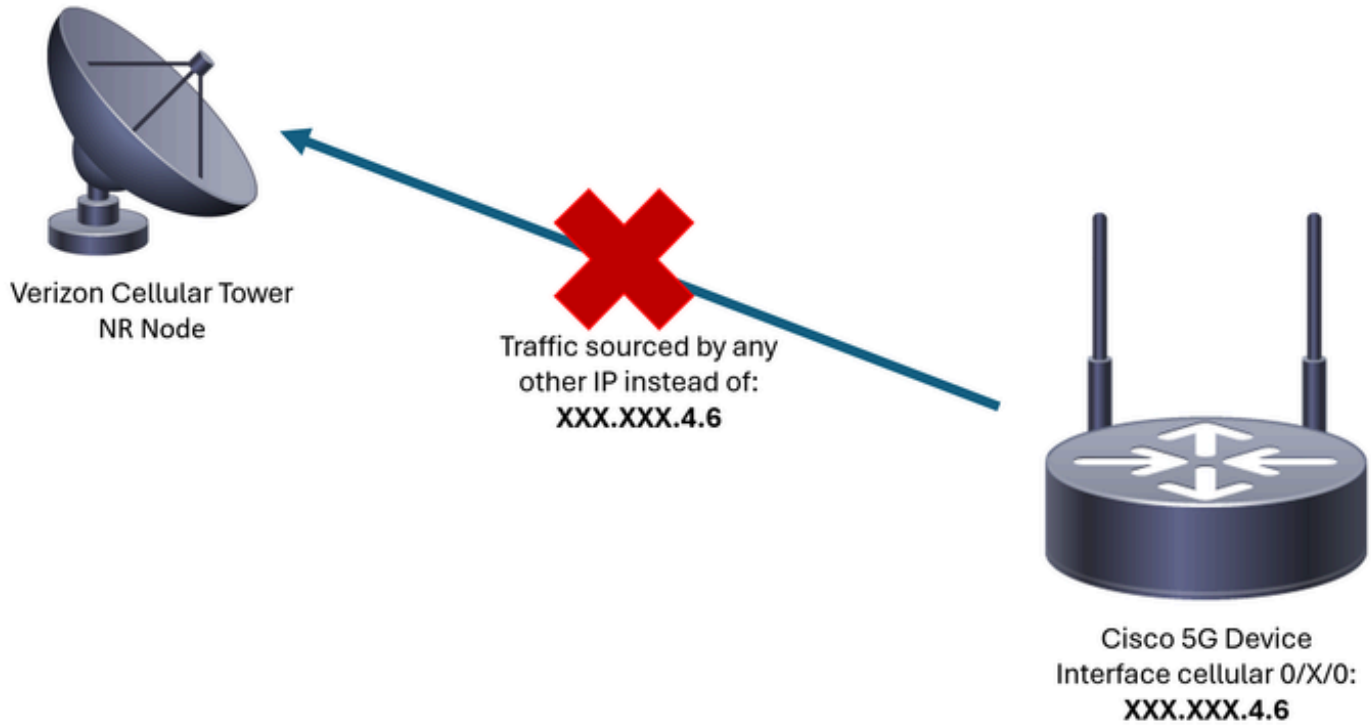
Ciò vale per un modulo P-5GS6-GL collegato a un router in modalità standalone o un CG522-E in modalità standalone o controller gestito da SD-WAN. Questo documento non si applica a un modulo P-5GS6-GL collegato a un router in SD-WAN poiché la sintassi del comando è diversa.

Problema

Verizon assegna un indirizzo IP specifico a ciascun client/SIM e si aspetta sempre di ricevere il traffico proveniente solo da tale IP.

La violazione del codice sorgente si verifica quando Verizon rileva che il traffico inviato dal client proviene da un IP diverso da quello precedentemente assegnato.

Ad esempio, se è stato assegnato l'indirizzo IP XXX.XXX.4.6 e Verizon riceve traffico dall'indirizzo IP XXX.XXX.8.9, il problema è presente:



Ogni volta che Verizon riceve più di 10 pacchetti dal dispositivo con un indirizzo IP diverso, la connessione alla rete cellulare si interrompe. Di conseguenza, una nuova connessione viene avviata dal dispositivo cellulare e può ottenere lo stesso indirizzo IP di prima o un nuovo indirizzo.

Dipende dal servizio acquisito.

Rilevare il problema in un modulo P-5GS6-GL collegato a un router

Quando il motivo di disconnessione indicato è presente nell'output del comando, la violazione dell'origine si trova nella posizione:

<#root>

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

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

                              *
                              *
```

Se l'output precedente non fornisce informazioni (a causa del processo del buffer), è possibile acquisire un pacchetto Netflow con questi comandi:

```
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
```

Per visualizzare l'output dell'acquisizione:

```
<#root>

isr#

show flow monitor NETFLOW_MONITOR cache format table
```

L'indirizzo IP assegnato da Verizon al dispositivo può essere visualizzato con il 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 nei log di Netflow è stato acquisito del traffico, questo viene segnalato come proveniente da un indirizzo IP diverso da quello confermato nell'interfaccia cellulare. Violazione di origine presente.

Soluzione per un modulo P-5GS6-GL collegato a un router

L'obiettivo è garantire che tutto il traffico venga inviato esclusivamente tramite l'indirizzo IP assegnato da Verizon. Ci sono diversi metodi che soddisfano questo obiettivo. La loro implementazione dipende dai requisiti di installazione e di rete:

- Opzione 1: ACL per il traffico in uscita
- Con un elenco di controllo di accesso, è possibile garantire che il traffico inviato dal dispositivo provenga solo dall'indirizzo IP di 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
```

- Opzione 2: NAT per il traffico interno

- Devono essere soddisfatti i seguenti requisiti:
    1. L'interfaccia cellulare è configurata come "ip nat outside".
    2. L'interfaccia LAN è configurata come "ip nat inside".
    3. Il sovraccarico NAT (PAT) viene implementato in modo da convertire anche tutte le porte.
    4. L'uso di un ACL per definire il traffico da NAT.

Esempio di configurazione:

<#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
```

- Opzione 3: Implementazione di una configurazione IPsec o di un altro tunnel

- Questo tunnel viene eseguito con l'indirizzo IP assegnato da Verizon. Man mano che il traffico si sposta all'interno, l'indirizzo IP esterno non cambia mai.

- Opzione 4: Implementazione di una mappa dei percorsi

- In caso di traffico generato dal router, è possibile implementare una mappa dei percorsi in modo che il traffico venga originato correttamente. Ad esempio, continua il ping verso un DNS per verificare la presenza di una "connettività Internet" e può essere implementata una mappa dei percorsi in modo che il traffico provenga correttamente.

In questo modo si termina la procedura per risolvere la violazione della fonte in un modulo Cisco P-5GS6-GL collegato a un router.

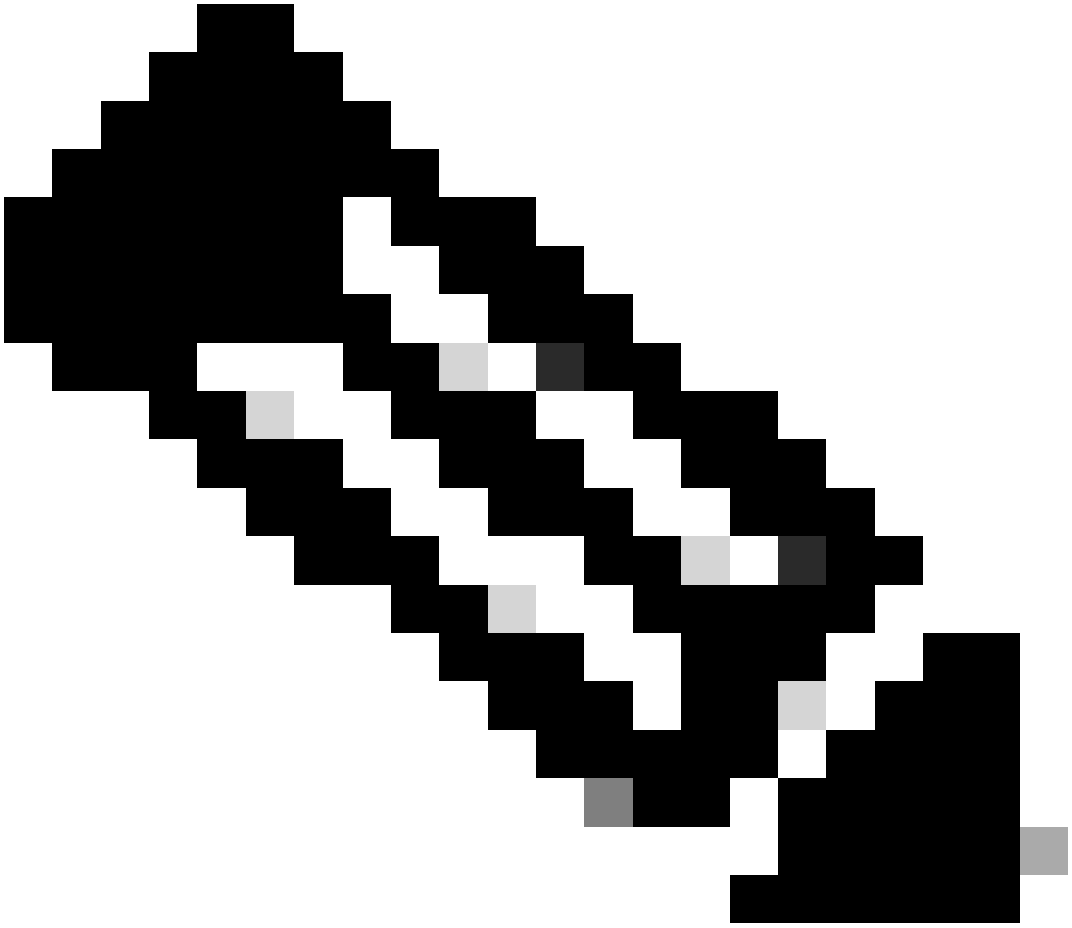
Violazione dell'origine IP in un CG522-E

Per impostazione predefinita, nel codice di queste periferiche viene attivata una funzione per eliminare questo problema.

Confermare che il dispositivo visualizza questo output:

```
<#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
```

Lo stato dell'azione Ipv4/Ipv6 deve essere Drop. Significa che la funzionalità è attivata.



Nota: se nell'output è indicato Permit, la funzione è disabilitata.

Con questi comandi, la feature può essere riattivata:

```
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
```

In questo modo si termina la procedura per la risoluzione dei problemi di violazione della sorgente in un Cisco CG522-E.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).