Dépannage de la violation de source IP lorsque Verizon est le transporteur

Table des matières

Introduction

Ce document décrit comment dépanner la violation de la source IP qui est un problème fréquent lorsque Verizon est l'opérateur.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Notions de base sur le réseau cellulaire 5G
- Passerelle cellulaire Cisco 522-E
- Module Cisco P-5GS6-GL
- Cisco IOS-XE
- Cisco IOS-CG

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Passerelle cellulaire 522-E avec IOS-CG version 17.9.5a.

- IR1101 avec IOS-XE version 17.9.5 avec un module P-5GS6-GL branché.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

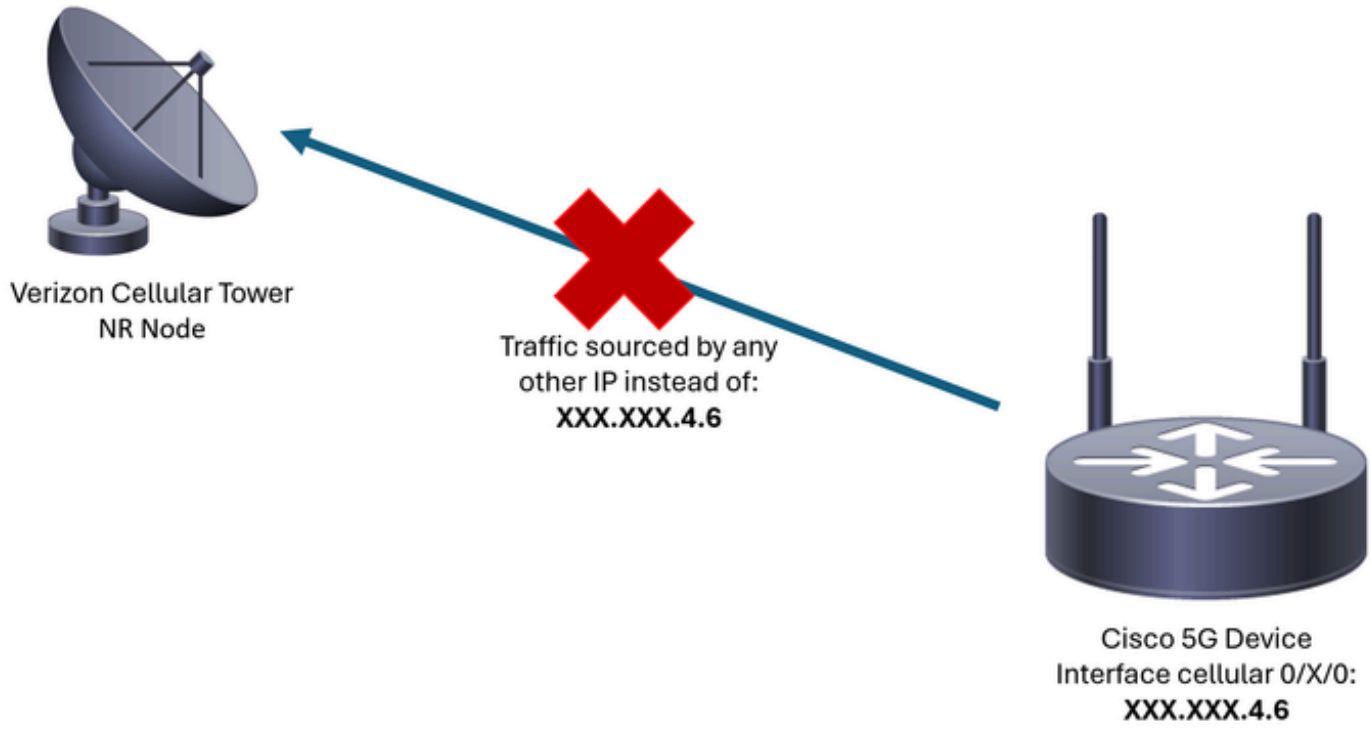
Ceci s'applique à un module P-5GS6-GL connecté à un routeur en mode autonome, ou à un CG522-E en mode autonome ou contrôleur géré par SD-WAN. Ce document ne s'applique pas à un module P-5GS6-GL connecté à un routeur dans SD-WAN car la syntaxe des commandes est différente.

Problème

Verizon attribue une adresse IP spécifique à chaque client/SIM et s'attend toujours à recevoir le trafic provenant uniquement de cette adresse IP.

Une violation de la source se produit lorsque Verizon détecte que le trafic envoyé par le client provient d'une adresse IP différente de celle qu'il avait précédemment attribuée.

Par exemple, si l'adresse IP XXX.XXX.4.6 a été attribuée et que Verizon reçoit le trafic de l'adresse IP XXX.XXX.8.9, le problème est présent :



Chaque fois que Verizon reçoit plus de 10 paquets du périphérique avec une adresse IP différente, la connexion au réseau cellulaire s'interrompt et s'interrompt. Par conséquent, une nouvelle connexion est établie à partir du périphérique cellulaire et il peut obtenir soit la même

adresse IP qu'avant, soit une nouvelle. Cela dépend du service acquis.

Détection du problème dans un module P-5GS6-GL connecté à un routeur

Lorsque la raison de déconnexion affichée est présente dans le résultat de la commande, la violation de source est placée :

<#root>

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

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

                              *
                              *
```

Si le résultat précédent ne donne pas d'informations (en raison du processus de mémoire tampon), une capture de paquets Netflow peut être effectuée avec ces commandes :

```
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
```

Pour afficher le résultat de la capture :

<#root>

isr#

show flow monitor NETFLOW_MONITOR cache format table

Verizon a attribué l'adresse IP au périphérique peut être vu avec la commande :

<#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, dans les journaux du NetFlow, le trafic est capturé, il est signalé comme provenant d'une adresse IP différente de celle confirmée dans l'interface cellulaire. La violation source est présente.

Solution pour un module P-5GS6-GL connecté à un routeur

L'objectif est de s'assurer que tout le trafic est envoyé uniquement à partir de l'adresse IP attribuée par Verizon. Différentes méthodes permettent d'atteindre cet objectif. Leur mise en oeuvre dépend du déploiement et des besoins du réseau :

- Option 1 : ACL pour le trafic sortant
- Avec une liste de contrôle d'accès, vous pouvez vous assurer que le trafic envoyé à partir du périphérique provient uniquement de l'adresse IP 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
```

- Option 2 : NAT pour le trafic interne

- Ces exigences doivent être satisfaites :
    1. L'interface cellulaire est configurée comme « ip nat outside ».
    2. L'interface LAN est configurée comme « ip nat inside ».
    3. La surcharge NAT (PAT) est implémentée de sorte que tous les ports sont également traduits.
    4. Utilisation d'une liste de contrôle d'accès pour définir le trafic à utiliser pour la traduction NAT.

Exemple de configuration :

<#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
```

- Option 3 : implémentation d'une configuration IPsec ou de tout autre tunnel

- Ce tunnel est effectué avec l'adresse IP attribuée à Verizon. Comme tout le trafic y circule, l'adresse IP externe ne change jamais.

- Option 4 : implémentation d'une carte de routage

- S'il y a du trafic généré par le routeur, une carte de route peut être implémentée afin que le trafic soit correctement généré. Par exemple, une requête ping continue vers un DNS, afin de s'assurer de la « connectivité Internet », et une carte de routage peut être implémentée afin que le trafic soit correctement approvisionné.

Ceci met fin à la procédure de dépannage de la violation de source dans un module Cisco P-5GS6-GL connecté à un routeur.

Violation de la source IP dans un CG522-E

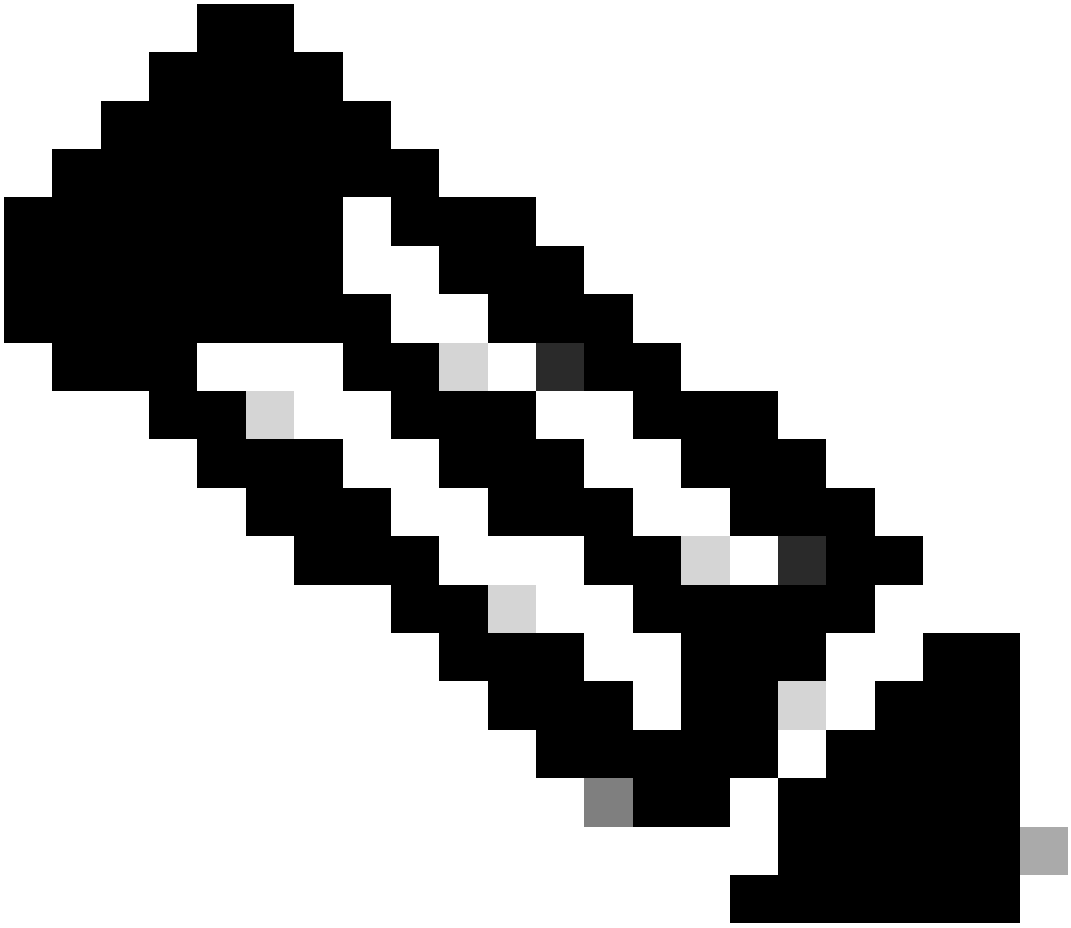
Par défaut, une fonctionnalité permettant d'éliminer ce problème est activée dans le code de ces périphériques.

Confirmez que le périphérique affiche ce résultat :

<#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
```

L'état de l'action Ipv4/Ipv6 doit être Drop. Cela signifie que la fonctionnalité est activée.



Remarque : si la sortie indique Permit, la fonction est désactivée.

Avec ces commandes, la fonctionnalité peut être réactivée :

```
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
```

Ceci met fin à la procédure de dépannage de la violation de source dans un Cisco CG522-E.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.