Fehlerbehebung bei Verletzungen der IP-Quelle, wenn Verizon als Betreiber fungiert

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung bei IP-Quellverletzungen beschrieben, die häufig auftreten, wenn Verizon als Netzbetreiber fungiert.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Grundkenntnisse in diesen Themen verfügen:

- Grundlagen des 5G-Mobilfunknetzes
- Cisco Cellular Gateway 522-E
- Cisco P-5GS6-GL-Modul
- Cisco IOS-XE
- Cisco IOS-CG

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cellular Gateway 522-E mit IOS-CG Version 17.9.5a.

- IR1101 mit IOS-XE Version 17.9.5 mit eingestecktem P-5GS6-GL Modul.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

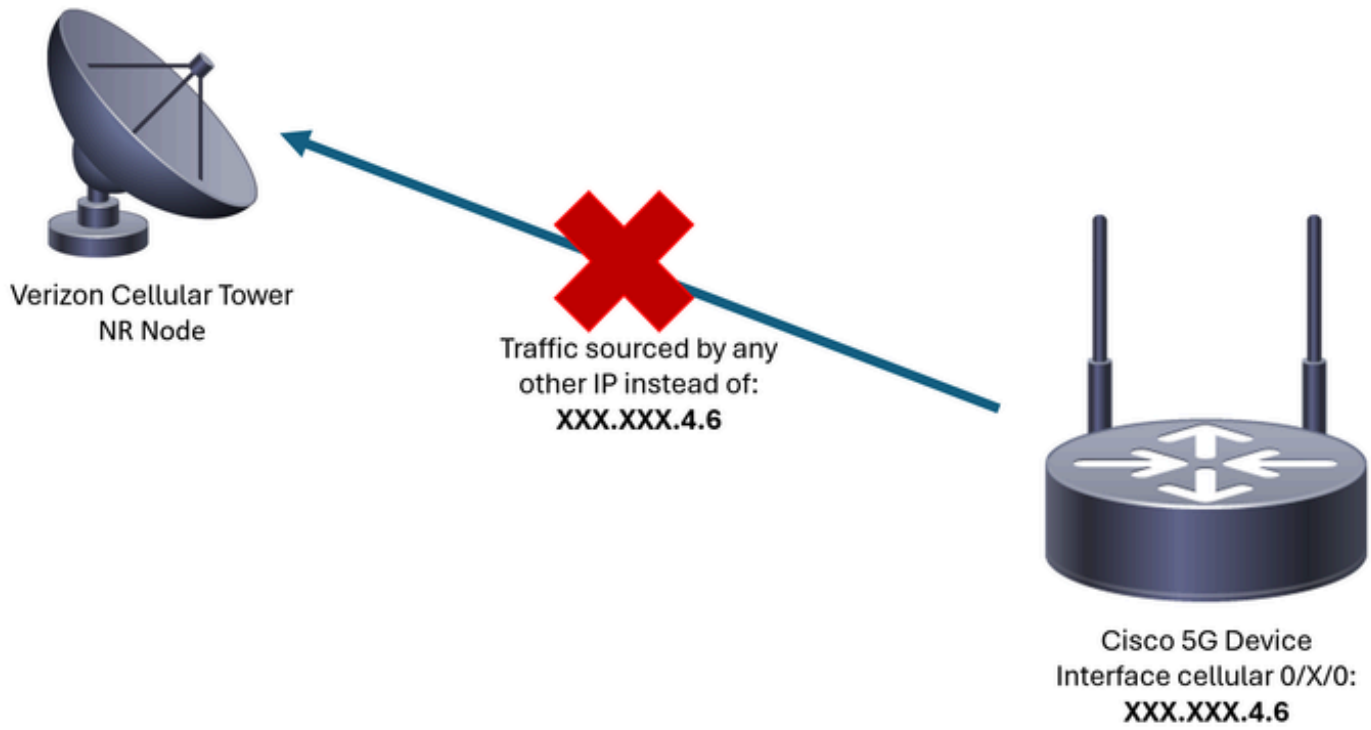
Dies gilt für ein P-5GS6-GL-Modul, das mit einem Router im Standalone-Modus verbunden ist, oder für ein CG522-E im Standalone-Modus oder im Controller-Modus, der vom SD-WAN verwaltet wird. Dieses Dokument gilt nicht für ein P-5GS6-GL-Modul, das mit einem Router im SD-WAN verbunden ist, da sich die Befehlssyntax unterscheidet.

Problem

Verizon weist jedem Client/SIM eine eigene IP-Adresse zu und erwartet immer, dass der Datenverkehr nur von dieser IP stammt.

Eine Quellenverletzung tritt auf, wenn Verizon feststellt, dass der vom Client gesendete Datenverkehr von einer anderen IP-Adresse stammt als der zuvor zugewiesenen.

Wenn beispielsweise die IP-Adresse XXX.XXX.4.6 zugewiesen wurde und Verizon Datenverkehr von der IP-Adresse XXX.XXX.8.9 empfängt, liegt das Problem vor:



Jedes Mal, wenn Verizon mehr als 10 Pakete von einem Gerät mit einer anderen IP-Adresse empfängt, flattert und stoppt die Verbindung zum Mobilfunknetz. Als Ergebnis wird eine neue

Verbindung vom Mobilgerät initiiert, und es kann entweder die gleiche IP-Adresse als zuvor oder eine neue erhalten. Das hängt vom erworbenen Service ab.

Erkennen des Problems in einem P-5GS6-GL-Modul, das mit einem Router verbunden ist

Wenn der angezeigte Grund für die Verbindungstrennung in der Ausgabe des Befehls vorhanden ist, wird die Quellenverletzung eingefügt:

<#root>

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

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

                              *
                              *
```

Wenn die vorherige Ausgabe keine Informationen liefert (aufgrund eines Pufferprozesses), kann eine NetFlow-Paketerfassung mit den folgenden Befehlen durchgeführt werden:

```
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
```

So zeigen Sie die Ausgabe der Erfassung an:

```
<#root>

isr#

show flow monitor NETFLOW_MONITOR cache format table
```

Die von Verizon dem Gerät zugewiesene IP-Adresse wird durch folgenden Befehl angezeigt:

```
<#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
```

Wenn in den Protokollen von NetFlow Datenverkehr erfasst wird, wird gemeldet, dass die Quelle eine andere IP-Adresse als die in der Mobilfunkschnittstelle bestätigte IP-Adresse aufweist. Die Quellverletzung ist vorhanden.

Lösung für ein P-5GS6-GL-Modul, das mit einem Router verbunden ist

Ziel ist es, sicherzustellen, dass der gesamte Datenverkehr nur über die von Verizon zugewiesene IP-Adresse gesendet wird. Es gibt verschiedene Methoden, um dieses Ziel zu erreichen. Ihre Implementierung hängt von den Bereitstellungs- und Netzwerkanforderungen ab:

- Option 1: ACL für ausgehenden Datenverkehr
- Mithilfe einer Zugriffskontrollliste können Sie sicherstellen, dass der vom Gerät gesendete Datenverkehr nur von der Verizon-IP-Adresse stammt:

```
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 für internen Datenverkehr

- Diese Anforderungen müssen erfüllt werden:
    1. Die Mobilfunkschnittstelle wird als "ip nat outside" konfiguriert.
    2. Die LAN-Schnittstelle wird als "ip nat inside" konfiguriert.
    3. NAT-Überlastung (PAT) wird implementiert, sodass alle Ports ebenfalls umgewandelt werden.
    4. Die Verwendung einer ACL zum Definieren des zu NAT führenden Datenverkehrs.

Konfigurationsbeispiel:

<#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: Implementieren einer IPsec- oder einer anderen Tunnelkonfiguration

- Dieser Tunnel wird mit der von Verizon zugewiesenen IP-Adresse erstellt. Da der gesamte Datenverkehr innerhalb des Netzwerks übertragen wird, ändert sich die externe IP-Adresse nie.

- Option 4: Implementieren einer Routenübersicht

- Bei von Routern generiertem Datenverkehr kann eine Routenübersicht implementiert werden, sodass der Datenverkehr von der richtigen Quelle stammt. So wird z. B. weiterhin ein Ping an einen DNS gesendet, um eine "Internetverbindung" sicherzustellen. Außerdem

kann eine Routenübersicht implementiert werden, sodass die korrekte Quelle des Datenverkehrs sichergestellt ist.

Damit ist das Verfahren zur Fehlerbehebung bei einem mit einem Router verbundenen Cisco P-5GS6-GL-Modul beendet.

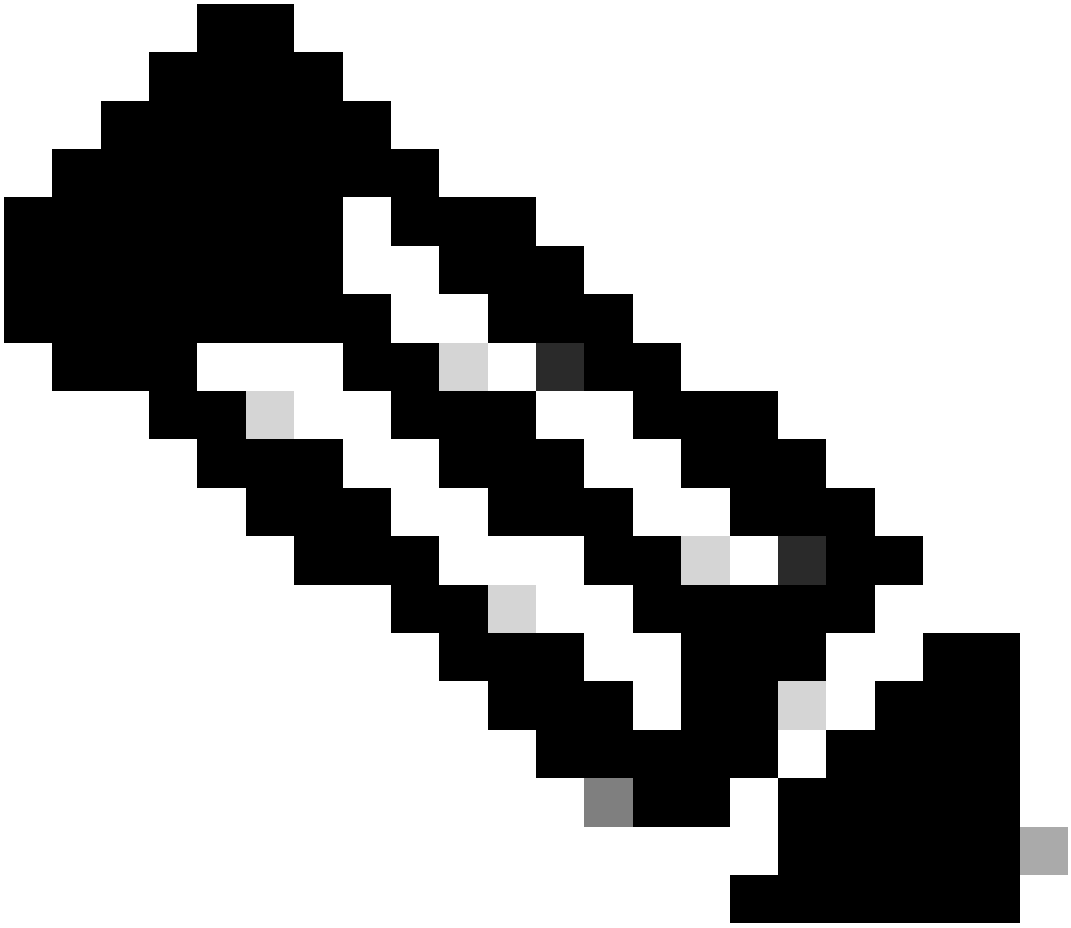
Verletzung der IP-Quelle in einem CG522-E

Standardmäßig wird eine Funktion zur Behebung dieses Problems im Code dieser Geräte aktiviert.

Stellen Sie sicher, dass das Gerät diese Ausgabe anzeigt:

```
<#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
```

Der Status von IPv4/IPv6-Aktion muss Drop sein. Das bedeutet, dass die Funktion aktiviert ist.



Hinweis: Wenn die Ausgabe "Zulassen" lautet, ist die Funktion deaktiviert.

Mit diesen Befehlen kann die Funktion erneut aktiviert werden:

```
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
```

Damit ist das Verfahren zur Fehlerbehebung bei einem Cisco CG522-E beendet.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.