Verizonがキャリアの場合のIPソース違反のトラブルシューティング

内容

はじめに

このドキュメントでは、Verizonがキャリアであるときに頻繁に発生するIPソースの違反をトラブルシューティングする方法について説明します。

前提条件

要件

次の項目に関する基本的な知識が推奨されます。

- 5Gセルラーネットワークの基本
- Ciscoセルラーゲートウェイ522-E
- Cisco P-5GS6-GLモジュール
- Cisco IOS XE
- Cisco IOS-CG

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- IOS-CGバージョン17.9.5aを搭載したセルラーゲートウェイ522-E。
- P-5GS6-GLモジュールが接続されたIOS-XEバージョン17.9.5を搭載したIR1101。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

これは、スタンドアロンモードのルータに接続されたP-5GS6-GLモジュール、またはSD-WANによって管理されるスタンドアロンモードまたはコントローラモードのCG522-Eに適用されます。このドキュメントは、コマンド構文が異なるため、SD-WANのルータに接続されているP-5GS6-GLモジュールには適用されません。

問題

Verizonは各クライアント/SIMに固有のIPアドレスを割り当て、常にそのIPを送信元とするトラフィックの受信を想定します。

Verizonが、クライアントから送信されたトラフィックが以前に割り当てられたIPとは異なるIPから送信されていることを検出すると、ソース違反が発生します。

たとえば、IPアドレスXXX.XXX.4.6が割り当てられており、VerizonがIPアドレスXXX.XXX.8.9からのトラフィックを受信する場合は、次の問題が存在します。

Verizonが異なるIPアドレスを持つデバイスから10を超えるパケットを受信するたびに、セルラーネットワークへの接続がフラップして停止します。その結果、セルラーデバイスから新しい接続が開始され、以前と同じIPアドレスまたは新しいIPアドレスを取得できます。取得したサービスによって異なります。

ルータに接続されたP-5GS6-GLモジュールでの問題の検出

コマンドの出力に表示された接続解除理由が存在する場合、送信元違反が発生しています。

```
<#root>

isr#

show cellular 0/X/0 call-history

                              *
                              *

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

                              *
                              *
```

上記の出力で情報が得られない場合（バッファプロセスが原因）、Netflowパケットキャプチャは次のコマンドで実行できます。

```
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
```

キャプチャの出力を表示するには、次の手順を実行します。

```
<#root>

isr#
```

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

デバイスに割り当てられたVerizonのIPアドレスは、次のコマンドで確認できます。

```
<#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
```

Netflowのログにトラフィックがキャプチャされている場合は、セルラーインターフェイスで確認されたものとは異なるIPアドレスが送信元として報告されます。ソース違反が存在します。

ルータに接続されたP-5GS6-GLモジュールのソリューション

目標は、すべてのトラフィックがVerizonによって割り当てられたIPからのみ送信されるようにすることです。この目標を達成するさまざまな方法があります。実装は、導入とネットワーク要件によって異なります。

- オプション1：アウトバウンドトラフィック用のACL
- アクセスコントロールリストを使用すると、デバイスから送信されたトラフィックがVerizon IPアドレスからのみ送信されるようにすることができます。

```
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
```

- オプション2：内部トラフィックのNAT

- 以下の要件を満たす必要があります。
    1. セルラーインターフェイスは「ip nat outside」として設定されます。
    2. LANインターフェイスは「ip nat inside」として設定されています。
    3. NATオーバーロード(PAT)が実装されているため、すべてのポートも変換されます。
    4. NATを適用するトラフィックを定義するACLの使用。

設定例：

<#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
```

- オプション3:IPsecまたはその他のトンネル設定の実装

- このトンネルは、Verizonによって割り当てられたIPアドレスを使用して実行されます。すべてのトラフィックがその内部を移動するため、外部IPアドレスは変更されません。

- オプション4：ルートマップの実装

- ルータで生成されたトラフィックが存在する場合は、トラフィックが正しく送信されるようにルートマップを実装できます。たとえば、が「インターネット接続」を確保するためにDNSへのpingを続行し、トラフィックが正しく送信されるようにルートマップを実装できます。

これで、ルータに接続されたCisco P-5GS6-GLモジュールでのソース違反のトラブルシューティング手順は終了です。

CG522-EにおけるIPソース違反

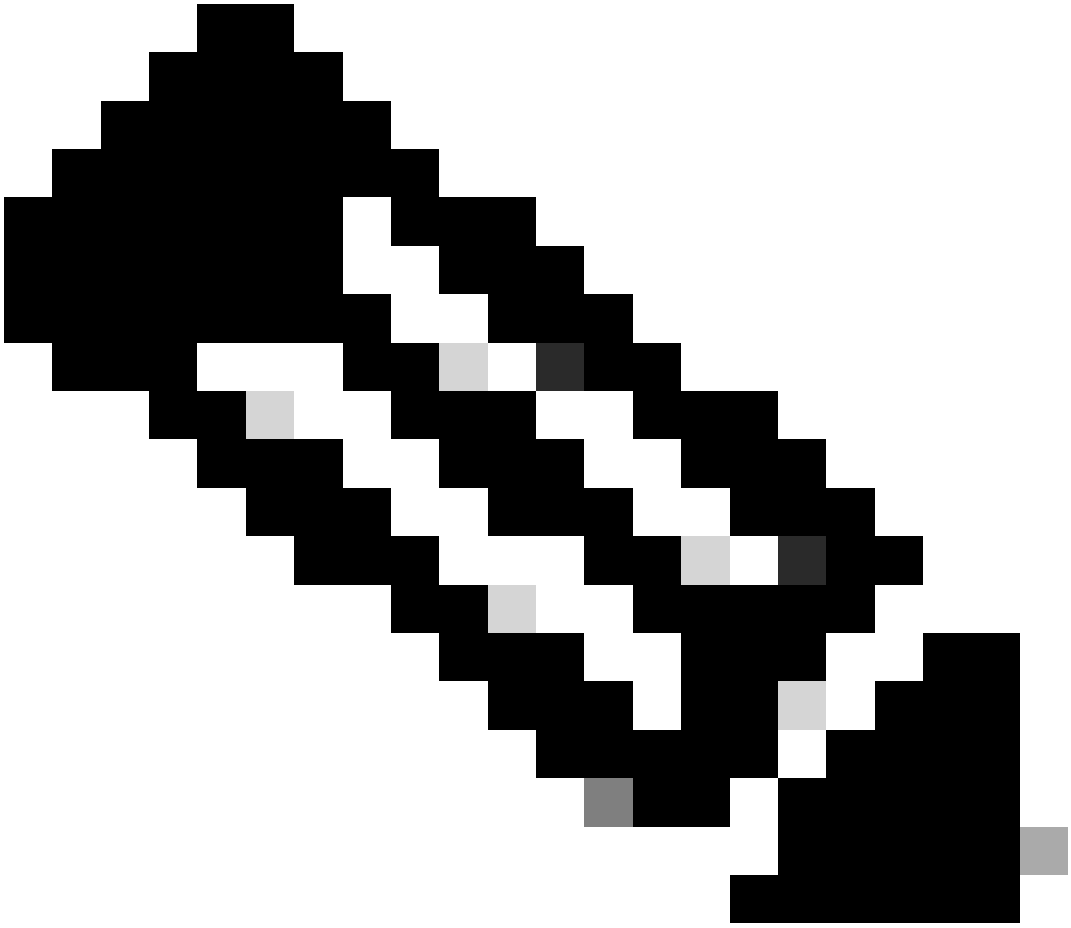
デフォルトでは、この問題を解消する機能が、これらのデバイスのコードで有効になっています。

デバイスに次の出力が表示されることを確認します。

<#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 Actionの状態はDropである必要があります。 これは、機能が有効であることを意味します。



注：出力にPermitと表示されている場合、この機能は無効です。

次のコマンドを使用して、機能を再アクティブ化できます。

```
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
```

これで、Cisco CG522-Eのソース違反のトラブルシューティング手順は終了です。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。