特定のWeb URLに関するユーザデータ参照の問題のトラブルシューティング

内容

はじめに

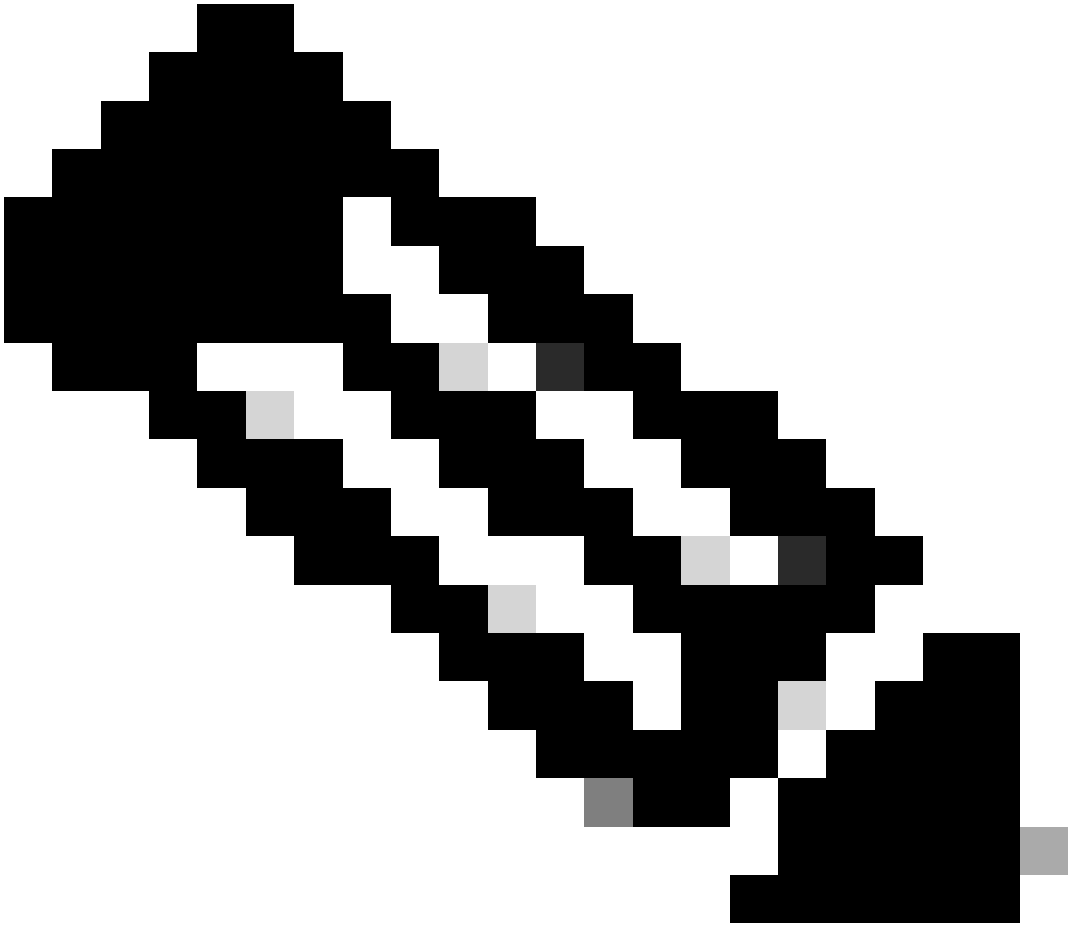
このドキュメントでは、すべてのUniform Resource Locator(URL)に対する4Gネットワークでのユーザデータブラウジングの問題について説明します。

前提条件

次のノードの機能に関する知識があることが推奨されます。

- Serving Packet Data Gateway(SPGW)
- コントロールプレーンとユーザプレーンの分離(CUPS)

症状の特定



注：テストと口グ収集を開始する前に、これらの詳細を確認する必要があります。

1. 問題となっているデータタイプを確認します：IPv4/IPv6/IPv4v6

2. 問題が特定のアクセスポイント名(APN)に関連している可能性があるため、問題が特定のAPNまたはすべてのAPNに関連しているかどうかを確認します。

3. 問題が特定のWeb URLまたは複数のURLにあるかどうかを確認します。

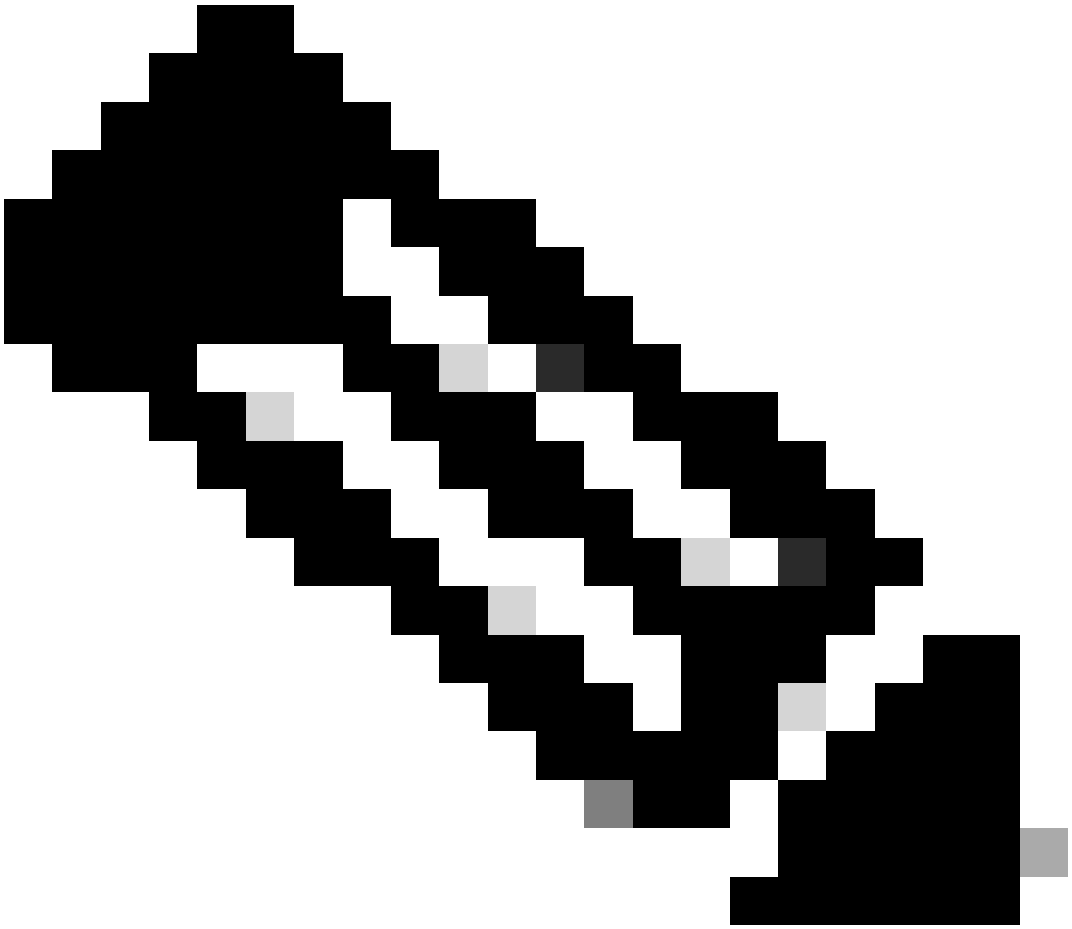
4. URLがエンタープライズURL/カスタマーアプリURLまたは通常のサービスURLであるかどうかを確認し、問題が特定のVPNにあるかどうかを確認します。

5. ブラウザから直接URLにアクセスする際、またはWebアプリ自体にアクセスする際に問題が発生するかどうかを確認します。

6. ハンドセットの再起動後に問題が断続的に発生するか、Web URLの更新が機能するか、またはハンドセットを再起動しても問題が継続して発生し機能しないかを確認します。

7. 発生した拒否の原因および評価グループを確認します。

ログ収集/テスト



> 注：この種の問題では、問題のあるユーザIMSIに対してリアルタイムのオンライントラブルシューティングを実行し、それに応じてログやトレースを収集する必要があります。

テストと口グ収集に進む前に、次の手順を実行します。

```
Flush the subscriber from the node and also clear browsing history/database from testing user handset s

clear subscriber imsi <IMSI number>  ------------------ to be executed in the node to clear the subscri
```

1. まず、問題が発生するIPv4のような1つのPDPタイプのテストから始めます。
2. 次のデバッグログを有効にして、puttyセッションをログに記録します。セッションが終了しないことを確認します（セッションが終了しないようにするには、tabキーを押すか、数分ごとに入力します）。

<#root>

On SPGW:

```
logging filter active facility sessmgr level debug
logging filter active facility acsmgr level debug
logging filter active facility npumgr-acl level debug
logging filter active facility firewall level debug
logging filter active facility vpn level debug
logging filter active facility vpnmgr level debug
logging active   ---------------- to enable the logging

after 5 mins
no logging active ---------------- to disable the logging
```

On CP:

```
logging filter active facility sessmgr level debug
logging filter active facility sxdemux level debug
logging filter active facility firewall level debug
logging filter active facility vpn level debug
logging filter active facility vpnmgr level debug
logging active ---------------- to enable the logging

after 5 mins
no logging active ---------------- to disable the logging
```

On UP:

```
logging filter active facility sessmgr level debug
logging filter active facility sxdemux level debug
logging filter active facility npumgr-acl level debug
logging filter active facility firewall level debug
logging filter active facility vpn level debug
logging filter active facility vpnmgr level debug
logging active ---------------- to enable the logging
no logging active ---------------- to disable the logging

Note :: These logging has to be enabled for short time depending on the CPU utilization because it
increase the utilization so while enabling logging need to keep a watch on CPU
```

3. コンフィギュレーションモードに移動し、サブスクライバのロギングモニタを有効にします。

```
config
logging monitor msid <imsi>
```

```
end
```

4. 別の端末を開き、puttyセッションをログに記録し、冗長性5を使用してサブスクライバの監視を開始し、次のオプションを有効にします。

<#root>

SPGW:

```
Press + for times then it collects the logs verbosity 5 logs then select next options
+++++
X, A, Y, 19, 33, 34, 35, 22, 26, 75
Once option 75 is pressed then select 3,4,8 then press esc
```

CUPS::

on CP:

```
monitor subscriber imsi <IMSI> +++++        S, X,A,Y,56,26,33,34,19,37,35,88,89
```

on UP:

```
monitor subscriber imsi <IMSI> +++++        S,X,A,Y,56,26,33,34,19,37,35,88,89
```

5. サブスクライバを接続し、URLを3 ~ 5分間連続してブラウズします。ブラウズ中に、これらのコマンドを複数回実行し、同じことをPuttyセッションに記録します。

<#root>

ON SPGW/SAEGW:

```
show subscriber full imsi <>
show active-charging session full imsi <>
show subscriber pgw-only full imsi <>
show subscriber sgw-only full imsi <>
show subscribers data-rate summary imsi <>
show ims-authorization sessions full imsi <>
show subscribers debug-info msid <>
```

On CP node:

```
Show subscriber full imsi <imsi>
Show active-charging session full imsi <imsi>
show subscribers pgw-only full imsi <>
```

```
show subscribers sgw-only full imsi <>
show session subsystem facility sessmgr instance <> verbose
show logs
```

On UP node:

```
show sub user-plane-only full callid  <>
show sub user-plane-only callid <> urr full all
show sub user-plane-only callid <> far full all
show sub user-plane-only callid <> pdr full all
show subscribers user-plane-only callid <> far all
show subscribers user-plane-only callid <> far
show subs data-rate call <callid>
show subscribers user-plane-only flows
show user-plane-service statistics all
show user-plane-service statistic rulebase name <rulebase_name>
```

6. 5分間参照した後、ステップ3で開いた他の端末でno logging activeを実行します。

7. サブスクライバのロギング・モニターを無効にします。

Config
no logging monitor msid <imsi>
end

8. mon subを停止して、numberトレースの収集が終了するまで実行させておき、CPUを監視してください。

9. 次のコマンドを実行して、サブスクライバの発信者IDを取得し、これに対するputtyセッションも口グに記録します。

Show subscriber full imsi <imsi>. -à get the call id
show logs callid <call_id>
show logs

発信者IDが存在する場合、サブスクライバセッションログが収集されたことは明らかです。収集されていない場合は、もう一度実行する必要があります。

実施したトラブルシューティング

- Web URLサーバのIPアドレスにpingを実行し、パケットドロップがないか確認します。

ping <URL IP address> ---------- from Gi context

--- ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 12160ms. >.>>>> There are packet drops, now we need to check were it is dropping

2. GIコンテキストからtracerouteを実行し、到達可能性の問題を確認します。

traceroute <peer ip address> src <local diameter origin host ip address>

Ex: traceroute 10.52.5.49 src 10.203.144.8

3. パケットドロップを確認するために、加入者の統計情報をチェックします。

<#root>

Show subscriber full imsi <imsi number>

```
input pkts: 455 output pkts: 474
input bytes: 75227 output bytes: 103267
input bytes dropped: 0 output bytes dropped: 0
input pkts dropped: 0 output pkts dropped: 0
input pkts dropped due to lorc : 0 output pkts dropped due to lorc : 0
input bytes dropped due to lorc : 0
in packet dropped suspended state: 0 out packet dropped suspended state: 0
in bytes dropped suspended state: 0 out bytes dropped suspended state: 0
in packet dropped sgw restoration state: 0 out packet dropped sgw restoration state: 0
in bytes dropped sgw restoration state: 0 out bytes dropped sgw restoration state: 0
pk rate from user(bps): 18547 pk rate to user(bps): 25330
ave rate from user(bps): 6182 ave rate to user(bps): 8443
sust rate from user(bps): 5687 sust rate to user(bps): 7768
pk rate from user(pps): 13 pk rate to user(pps): 14
ave rate from user(pps): 4 ave rate to user(pps): 4
sust rate from user(pps): 4 sust rate to user(pps): 4
link online/active percent: 92
ipv4 bad hdr: 0 ipv4 ttl exceeded: 0
ipv4 fragments sent: 0 ipv4 could not fragment: 0
ipv4 input acl drop: 0 ipv4 output acl drop: 0
ipv4 bad length trim: 0
ipv6 input acl drop: 0 ipv6 output acl drop: 0
ipv4 input css down drop: 0 ipv4 output css down drop: 0
ipv4 input css down drop: 0 ipv4 output css down drop: 0
ipv4 output xoff pkts drop: 0 ipv4 output xoff bytes drop: 0
ipv6 output xoff pkts drop: 0 ipv6 output xoff bytes drop: 0
ipv6 input ehrpd-access drop: 0 ipv6 output ehrpd-access drop: 0
input pkts dropped (0 mbr): 0 output pkts dropped (0 mbr): 0
ip source violations: 0 ipv4 output no-flow drop: 0
ipv6 egress filtered: 0
ipv4 proxy-dns redirect: 0 ipv4 proxy-dns pass-thru: 0
ipv4 proxy-dns drop: 0
ipv4 proxy-dns redirect tcp connection: 0
ipv6 bad hdr: 0 ipv6 bad length trim: 0
ip source violations no acct: 0
```

```
ip source violations ignored: 0
dormancy total: 0 handoff total: 0
ipv4 icmp packets dropped: 0
APN AMBR Input Pkts Drop: 0 APN AMBR Output Pkts Drop: 0
APN AMBR Input Bytes Drop: 0 APN AMBR Output Bytes Drop: 0
APN AMBR UE Overload Input Pkts Drop: 0 APN AMBR UE Overload Output Pkts Drop: 0
APN AMBR UE Overload Input Bytes Drop: 0 APN AMBR UE Overload Output Bytes Drop: 0
Access-flows:0
Num Auxiliary A10s:0
```

4. 加入者トラフィックに対する影響については、show active chargingの出力を確認します。

Show active-charging session full imsi <imsi num>

PP Dropped Packets: 0
CC Dropped Uplink Packets: 0 CC Dropped Uplink Bytes: 0
CC Dropped Downlink Packets: 0 CC Dropped Downlink Bytes: 0

5. show active chargingコマンド出力でECS/ACSレベルのパケットドロップを確認し、パケットドロップがないか確認します。次に、設定されているアクションを設定で確認します。

<#root>

Show active-charging session full imsi <imsi num> or show sub user-plane-only full callid <>

```
 Ruledef Name Pkts-Down Bytes-Down Pkts-Up Bytes-Up Hits Match-Bypassed
-------------------- ---------- ---------- ---------- ---------- ---------- --------------
dns_free_covid 4 428 4 340 8 0
icmpv6 0 0 5 1423 5 0
ip-pkts 479 103670 432 74488 764 429
```

6. DNS解決が成功したかどうかを確認します。成功した場合、DNSに関する問題はありません。

7. ユーザ機器(UE)とサーバ間でTCP接続が正常に確立されていることを確認します。

8. これらの手順のいずれかでドロップが観察されない場合、ノードに問題はありません。

パケットドロップ

1. 次に示すようなパケットドロップが発生しているかどうかを判別するには、サブスクライバのリリースの統計情報を確認します。

Total Dropped Packets : 132329995
Total Dropped Packet Bytes: 14250717212

Total PP Dropped Packets : 0
Total PP Dropped Packet Bytes: 0

R7Gx Rule-Matching Failure Stats:
Total Dropped Packets : 871921
Total Dropped Packet Bytes : 86859232

P2P random drop stats:
Total Dropped Packets : 0
Total Dropped Packet Bytes : 0

2. show subscriberの出力で観察された障害のパーセンテージをチェックします。パケットのドロップが1 %未満の場合は、ほとんどの場合は水疱で何も起こりません。

input pkts: 455 output pkts: 474
input bytes: 75227 output bytes: 103267
input bytes dropped: 0 output bytes dropped: 0
input pkts dropped: 0 output pkts dropped: 0

3. RX評価グループでのパケットドロップとITCパケットドロップが発生している場合、帯域幅問題が原因でサブスクライバパッケージの期限が切れている可能性が高いです。

ITC Packets Drop: 47235019

4. Enhanced Charging Service(ECS)レベルで、ルール/課金処理/ルールベースの定義方法とブロック要因があるかどうかをECS構成で確認する必要があります。ECSレベルにはさまざまなタイプの廃棄があり、廃棄の種類に基づいて次のアクションプランに進む必要があります。

5. 渡されていて処理されていないパケットサイズのMTUサイズ。

6. パケットがドロップされる中間パスの問題は、TCPダンプ/ユーザレベルトレースから特定できます。

問題のパターンによって異なるため、このタイプの問題に対する回復処理計画は同じではありません。

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。