특정 웹 URL에 대한 사용자 데이터 검색 문제 해결

목차

소개

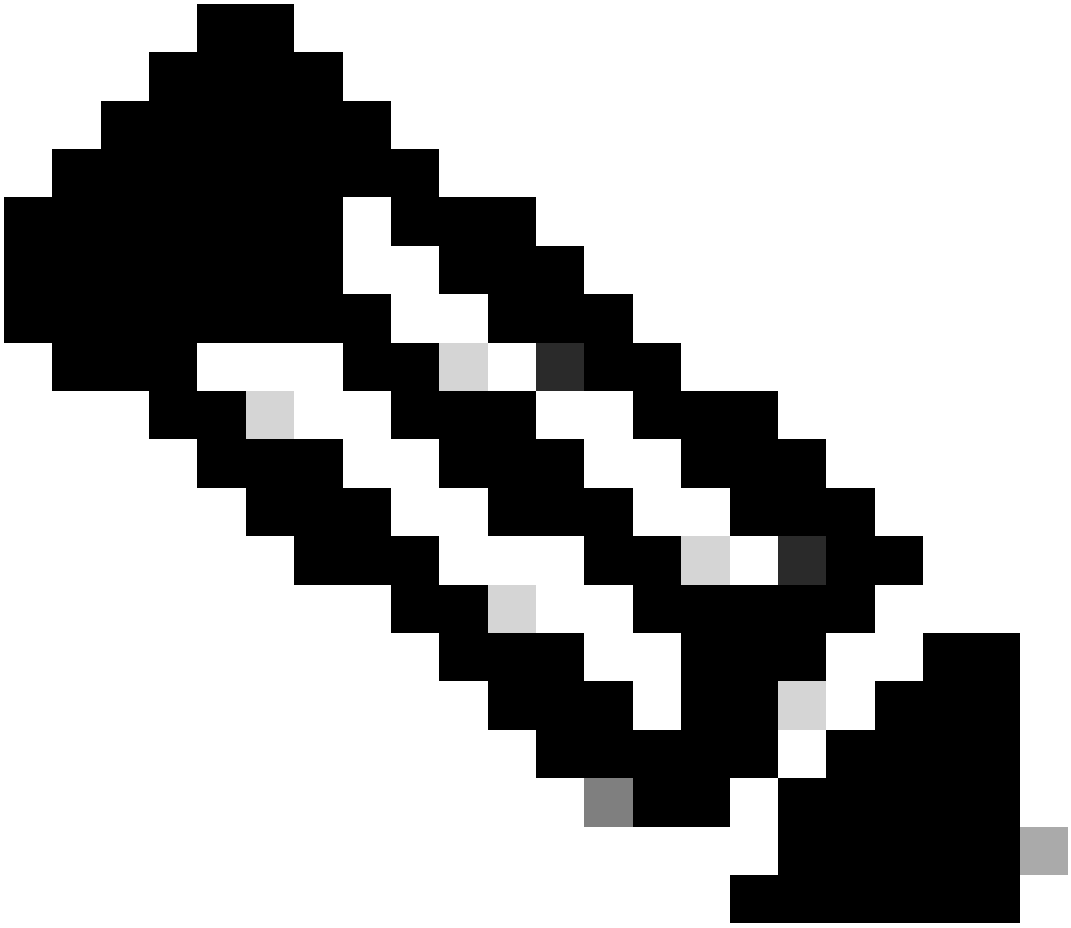
이 문서에서는 모든 URL(Uniform Resource Locator)에 대한 4G 네트워크의 사용자 데이터 브라우징 문제를 설명합니다.

사전 요구 사항

Cisco에서는 이러한 노드의 기능에 대해 알고 있는 것이 좋습니다.

- SPGW(Serving Packet Data Gateway)
- 제어 및 사용자 평면 분리(CUPS)

증상 확인



참고: 테스트 및 로그 수집을 시작하기 전에 이러한 세부 정보를 확인해야 합니다.

---

1. 문제가 되는 데이터 유형을 확인합니다. IPv4/IPv6/IPv4v6

2. 문제가 특정 APN(Access Point Name)과 관련된 문제인지 또는 특정 APN과 관련된 문제인지 확인합니다.

3. 특정 웹 URL에 대한 문제인지 또는 여러 URL에 대한 문제인지 확인합니다.

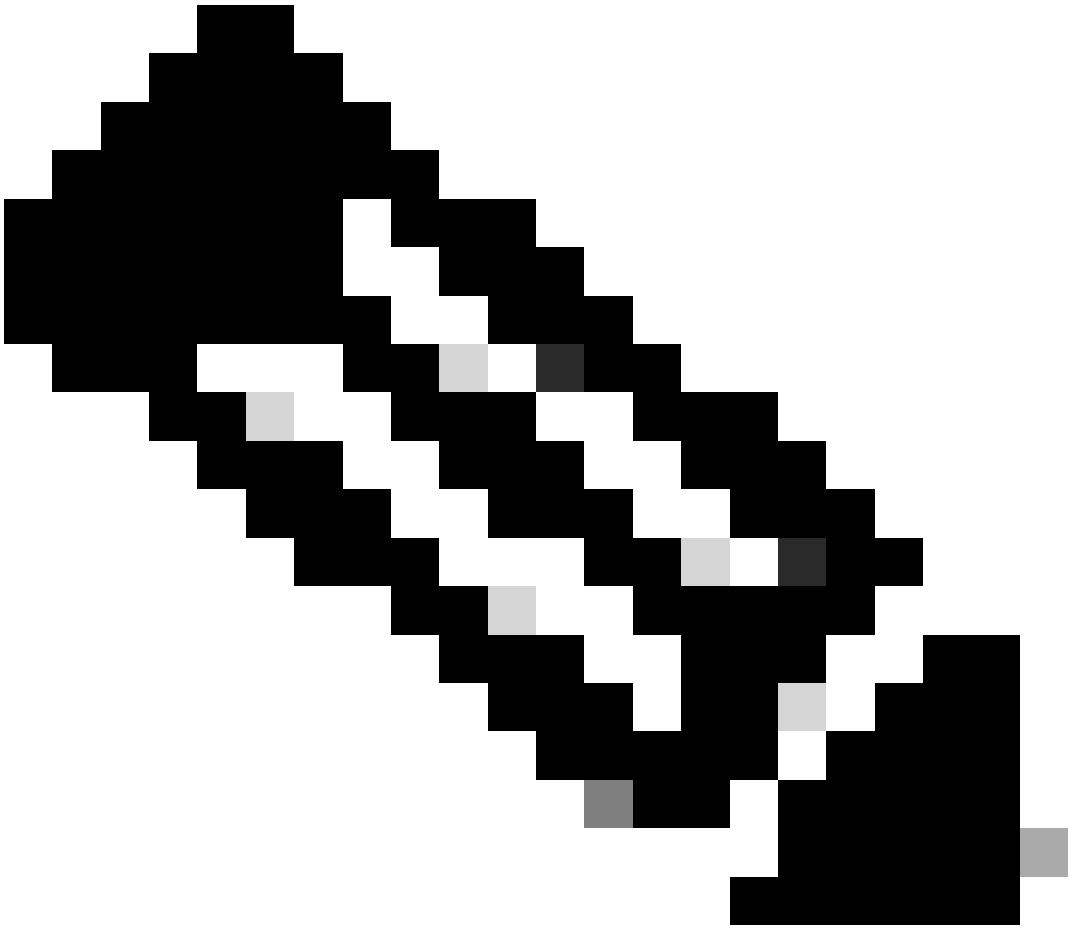
4. URL이 기업 URL/고객 앱 URL인지 아니면 일부 일반 서비스 URL인지 확인하고 특정 VPN에 문제가 있는지 확인합니다.

5. 브라우저에서 직접 URL에 액세스하거나 웹 앱 자체에 액세스하는 동안 문제가 발생하는지 확인합니다.

6. 핸드셋의 사후 재시작이나 새로 고침 웹 URL이 작동하기 시작하는 등 문제가 간헐적으로 발생하는지 또는 핸드셋 재시작 후에도 문제가 일관되고 작동하지 않는지 확인합니다.

7. 거부 사유가 관찰되었는지, 어떤 등급군에 해당하는지를 확인합니다.

로그 수집/테스트



> 참고: 이러한 종류의 문제에 대해서는 문제가 있는 사용자 IMSI를 사용하여 실시간 온라인 문제 해결을 수행해야 하며, 이에 따라 로그/추적을 수집해야 합니다.

테스트 및 로그 수집을 진행하기 전에 다음을 수행합니다.

```
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. 먼저 IPv4와 같은 PDP 유형 하나로 문제를 확인하는 테스트로 시작합니다.

2. 이러한 디버그 로그를 활성화하고 putty 세션을 기록합니다. 세션이 종료되지 않아야 합니다 (세션이 종료되지 않도록 Tab 키를 누르고 몇 분마다 Enter 키 누름).

<#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. 구성 모드로 이동한 다음 가입자에 대한 로깅 모니터를 활성화합니다.

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

4. 다른 터미널을 열고 putty 세션을 로깅한 다음 세부 정보 5로 가입자 모니터링을 시작하고 다음 옵션을 활성화합니다.

<#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. 가입자를 연결하여 URL을 3분에서 5분 동안 계속 검색하고, 검색하는 동안 이러한 명령을 여러 번 실행하고 putty 세션을 로깅합니다.

<#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. 5분 탐색 후 3단계에서no logging active 연 다른 단말기에서 를 실행합니다.

7. 가입자에 대한 로깅 모니터를 비활성화합니다.

Config
no logging monitor msid <imsi>
end

8. mon sub를 중지하지 말고 숫자 추적 수집이 끝날 때까지 실행하되 CPU를 계속 주시하십시오.

9. 가입자의 발신자 id를 가져오고 이에 대한 putty 세션도 로깅하려면 이 명령을 실행합니다.

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

발신자 ID가 있는 경우 가입자 세션 로그가 수집되었는지 분명하며, 그렇지 않은 경우 다시 실행해야 합니다.

수행된 트러블슈팅

- 웹 URL 서버 IP 주소를 Ping하고 패킷 손실이 있는지 확인합니다.

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 컨텍스트에서 traceroute를 수행하고 연결 문제가 있는지 확인합니다.

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

Ex: traceroute 10.52.5.49 src 10.203.144.8

3. 패킷 삭제를 확인하려면 가입자 통계를 확인합니다.

<#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. 가입자 트래픽에 영향을 주는 활성 충전 출력 표시를 확인합니다.

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. ECS/ACS 레벨 패킷 삭제에 대한 show active charging 명령 출력을 확인하고 패킷 삭제가 있는지 확인합니다. 그런 다음 어떤 작업이 구성되었는지 컨피그레이션을 확인합니다.

<#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 확인이 성공했는지 확인합니다. 성공하면 DNS에는 문제가 없습니다.

7. TCP 연결이 UE(User Equipment)와 서버 간에 성공적으로 설정되었는지 확인합니다.

8. 이러한 단계에서 누락이 관찰되지 않으면 노드에는 문제가 없습니다.

패킷 삭제

1. 여기에 표시된 것과 유사한 패킷 삭제를 경험하고 있는지 확인하려면 가입자 릴리스 통계를 확인합니다.

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 출력에 관찰된 실패 비율을 확인합니다. 패킷 드랍이 1% 미만이면 대부분 플러크일 가능성이 높으므로 효과가 없습니다.

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 등급 그룹의 패킷 삭제 및 ITC 패킷 삭제를 확인할 경우, 이는 대역폭 문제 및 가입자 패키지 만료 때문일 가능성이 높습니다.

ITC Packets Drop: 47235019

4. ECS(Enhanced Charging Service) 레벨에서 관리/과금 조치/룰베이스가 어떻게 정의되는지 그리고 차단 요인이 있는지 ECS 컨피그레이션을 확인/확인해야 합니다. ECS 레벨에는 다양한 유형의 드롭이 있으며, 드롭의 유형에 따라 다음 작업 계획을 진행해야 합니다.

5. 전달 중이고 처리되지 않은 패킷 크기의 MTU 크기입니다.

6. 패킷이 삭제되는 중간 경로 문제는 TCP 덤프/사용자 수준 추적에서 식별할 수 있습니다.

복구 작업 계획은 문제의 패턴에 따라 달라지므로 이 유형의 문제에 대해서는 동일하지 않습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.