WAAS - WCCP 트러블슈팅

장:WCCP 문제 해결

이 문서에서는 WCCP 문제를 해결하는 방법에 대해 설명합니다.

목차

다음과 같은 증상이 나타날 수 있는 WCCP 문제를 나타냅니다.

- WAE가 트래픽을 수신하지 않습니다(WCCP 컨피그레이션 오류 때문일 수 있음).
- 최종 사용자는 서버 애플리케이션에 연결할 수 없습니다(트래픽 블랙홀 때문일 수 있음).
- WCCP가 활성화된 경우 네트워크 속도 저하(라우터 패킷 삭제 또는 라우터 CPU 사용량이 높기 때문일 수 있음)
- 라우터 CPU 사용량이 너무 많음(하드웨어 대신 소프트웨어의 리디렉션으로 인해 발생할 수 있음)

WCCP 문제는 라우터(또는 디바이스 리디렉션)와 관련된 문제 또는 WAE 디바이스에서 발생할 수 있습니다.라우터와 WAE 디바이스 모두에서 WCCP 컨피그레이션을 확인해야 합니다.먼저 라우터의 WCCP 컨피그레이션을 살펴본 다음 WAE에서 WCCP 컨피그레이션을 확인합니다.

라우터에서 WCCP 문제 해결

이 섹션에서는 다음 디바이스의 트러블슈팅에 대해 설명합니다.

- Catalyst 6500 Series 스위치 및 ISR 및 3700 Series 라우터
- ASR 1000 Series 라우터

Catalyst 6500 Series 스위치 및 ISR 및 3700 Series 라우터에서 WCCP 문제 해결

다음과 같이 **show ip wccp** IOS 명령을 사용하여 스위치 또는 라우터에서 WCCPv2 가로채기를 확인하여 문제 해결을 시작합니다.

```
Router# show ip wccp
Global WCCP information:
   Router information:
       Router Identifier:                  10.88.81.242
       Protocol Version:                   2.0

   Service Identifier: 61
       Number of Service Group Clients:    1                   <-----Client = WAE
       Number of Service Group Routers:    1
       Total Packets s/w Redirected:       68755               <-----Increments for software-
based redirection
         Process:                          2                   <-----
         Fast:                             0                   <-----
         CEF:                              68753               <-----
       Service mode:                       Open
       Service access-list:                -none-
       Total Packets Dropped Closed:       0
       Redirect access-list:               -none-
       Total Packets Denied Redirect:      0                   <-----Match service group but not
redirect list
       Total Packets Unassigned:           0
       Group access-list:                  -none-
       Total Messages Denied to Group:     0
       Total Authentication failures:      0                   <-----Packets have incorrect
service group password
       Total Bypassed Packets Received:    0
--More--
```

소프트웨어 기반 리디렉션을 사용하는 플랫폼에서 위의 명령 출력에서 Total Packets s s/w Redirected 카운터가 증가하는지 확인합니다.하드웨어 기반 리디렉션을 사용하는 플랫폼에서 이러한 카운터가 많이 증가해서는 안 됩니다.하드웨어 기반 플랫폼에서 이러한 카운터가 크게 증가하면 라우터에서 WCCP가 잘못 구성되거나(WCCP GRE는 기본적으로 소프트웨어에서 처리됨), TCAM 리소스 부족 등의 하드웨어 리소스 문제로 인해 라우터가 소프트웨어 리디렉션으로 다시 전환될 수 있습니다.하드웨어 기반 플랫폼에서 이러한 카운터가 증가하여 CPU 사용량이 증가할 수 있는 경우 더 많은 조사가 필요합니다.

서비스 그룹과 일치하지만 리디렉션 목록과 일치하지 않는 패킷에 대한 Total Packets Denied Redirect 카운터 증분.

잘못된 서비스 그룹 비밀번호로 수신된 패킷에 대한 Total Authentication failures 카운터가 증가합니다.

소프트웨어에서 WCCP 리디렉션이 수행되는 라우터에서 **show ip wccp 61 detail** IOS 명령을 사용하여 라우터에서 WCCPv2 인터셉션을 다음과 같이 확인하여 계속합니다.

```
Router# show ip wccp 61 detail
WCCP Client information:
       WCCP Client ID:          10.88.81.4
       Protocol Version:        2.0
       State:                   Usable                                  <-----Should be Usable
       Initial Hash Info:       00000000000000000000000000000000
                                00000000000000000000000000000000
       Assigned Hash Info:      FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                                FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
       Hash Allotment:          256 (100.00%)                           <-----Buckets handled by
this WAE
       Packets s/w Redirected:  2452
       Connect Time:            01:19:46                                <-----Time WAE has been
in service group
       Bypassed Packets
         Process:               0
         Fast:                  0
         CEF:                   0
```

서비스 그룹 61의 WAE 상태가 사용 가능인지 확인합니다.해시 버킷이 Hash Spatch(해시 할당) 필드에서 WAE에 할당되었는지 확인합니다.백분율은 이 WAE에서 처리하는 총 해시 버킷 수를 나타냅니다.WAE가 서비스 그룹에 속한 시간이 연결 시간 필드에 보고됩니다.해시 할당 방법은 소프트웨어 기반 리디렉션과 함께 사용해야 합니다.

다음과 같이 라우터에서 **show ip wccp** *service* **hash** *dst-ip src-ip dst-port src-port hidden IOS 명령*을 사용하여 팜에서 어떤 WAE가 특정 요청을 처리할지 결정할 수 있습니다.

```
Router# show ip wccp 61 hash 0.0.0.0 10.88.81.10 0 0
WCCP hash information for:
   Primary Hash:   Src IP: 10.88.81.10
   Bucket:   9
   WCCP Client: 10.88.81.12                                  <-----Target WAE
```

하드웨어에서 WCCP 리디렉션이 수행되는 라우터에서 **show ip wccp 61 detail** IOS 명령을 사용하여 라우터에서 WCCPv2 인터셉션을 다음과 같이 확인하여 계속합니다.

```
Cat6k# sh ip wccp 61 detail
WCCP Client information:
   WCCP Client ID:          10.88.80.135
   Protocol Version:        2.0
   State:                   Usable
   Redirection:             L2
   Packet Return:           GRE                    <-----Use generic GRE for hardware-based
platforms
   Packets Redirected:    0
   Connect Time:          1d18h
   Assignment:            MASK                     <-----Use Mask for hardware-based
redirection

   Mask  SrcAddr    DstAddr    SrcPort DstPort
   ----  -------    -------    ------- -------
   0000: 0x00001741 0x00000000 0x0000  0x0000       <-----Default mask

   Value SrcAddr    DstAddr    SrcPort DstPort CE-IP
   ----- -------    -------    ------- ------- -----
   0000: 0x00000000 0x00000000 0x0000  0x0000  0x0A585087 (10.88.80.135)
   0001: 0x00000001 0x00000000 0x0000  0x0000  0x0A585087 (10.88.80.135)
```

```
0002: 0x00000040 0x00000000 0x0000  0x0000  0x0A585087 (10.88.80.135)
0003: 0x00000041 0x00000000 0x0000  0x0000  0x0A585087 (10.88.80.135)
```

하드웨어 리디렉션을 지원하는 라우터의 마스크 할당 방법을 확인하려고 합니다.

라우터에 TCAM 리소스를 저장하려면 네트워크 환경에 맞게 기본 WCCP 마스크를 변경하는 것이 좋습니다.다음 권장 사항을 고려하십시오.

- WCCP 리디렉션 ACL을 사용할 때 가능한 최소 마스크 비트 수를 사용합니다.리디렉션 ACL과 함께 사용할 경우 마스크 비트 수가 작을수록 TCAM 사용률이 낮아집니다.클러스터에 1-2개의 WCCP 클라이언트가 있는 경우 1비트를 사용합니다.3~4개의 WCCP 클라이언트가 있는 경우 2비트를 사용합니다.5-8개의 WCCP 클라이언트가 있는 경우 3비트 등을 사용합니다.
- WAAS 기본 마스크(0x1741)는 사용하지 않는 것이 좋습니다. 데이터 센터 구축의 경우, 클라이언트 또는 호스트가 아닌 데이터 센터에 브랜치 사이트를 로드 밸런싱하는 것이 목표입니다.오른쪽 마스크는 데이터 센터 WAE 피어링을 최소화하여 스토리지를 확장합니다.예를 들어, 지사 네트워크가 /24개인 소매 데이터 센터에 0x100~0x7F00을 사용합니다.비즈니스당 16이 /인 대기업의 경우 0x10000 ~ 0x7F0000을 사용하여 엔터프라이즈 데이터 센터로 비즈니스 로드 밸런싱을 수행합니다.지사의 목표는 DHCP를 통해 IP 주소를 얻는 클라이언트의 균형을 맞추는 것입니다.DHCP는 일반적으로 서브넷에서 가장 낮은 IP 주소에서 클라이언트 IP 주소를 증가시킵니다.DHCP에서 할당한 IP 주소의 균형을 마스크와 최대화하려면 0x1~0x7F를 사용하여 클라이언트 IP 주소의 가장 낮은 순서 비트만 고려하면 최상의 배포를 달성할 수 있습니다.

WCCP 리디렉션 액세스 목록에서 사용하는 TCAM 리소스는 구성된 WCCP 비트 마스크에 대해 해당 ACL의 내용을 곱한 결과입니다.따라서 마스크에 따라 생성되는 WCCP 버킷 수와 리디렉션 ACL의 항목 수 간에는 경합이 있습니다.예를 들어, 0xF(4비트) 마스크와 200 라인 리디렉션 허용 ACL은 3200(2^4 x 200) TCAM 항목을 생성할 수 있습니다.마스크를 0x7(3비트)로 줄이면 TCAM 사용량이 50% 감소합니다(2^3 x 200 = 1600).

Catalyst 6500 Series 및 Cisco 7600 Series 플랫폼은 소프트웨어와 하드웨어 모두에서 WCCP 리디렉션을 처리할 수 있습니다.패킷이 실수로 소프트웨어에서 리디렉션되는 경우 하드웨어 리디렉션을 예상하면 라우터 CPU 사용량이 지나치게 많을 수 있습니다.

TCAM 정보를 검사하여 소프트웨어 또는 하드웨어에서 리디렉션이 처리되는지 확인할 수 있습니다.show tcam IOS 명령을 다음과 같이 사용합니다.

```
Cat6k# show tcam interface vlan 900 acl in ip

* Global Defaults not shared


Entries from Bank 0


Entries from Bank 1

    permit       tcp host 10.88.80.135 any
    punt         ip any any (8 matches)              <-----Packets handled in software
```

"펀트" 일치 항목은 하드웨어에서 처리되지 않은 요청을 나타냅니다.이 상황은 다음 오류로 인해 발생할 수 있습니다.

- 마스크 대신 해시 할당
- 인바운드 대신 아웃바운드 리디렉션
- 다음에서 제외 리디렉션

- 알 수 없는 WAE MAC 주소
- 일반 GRE 터널 대상에 대한 루프백 주소 사용

다음 예에서 policy-route 항목은 라우터가 전체 하드웨어 리디렉션을 수행하고 있음을 보여줍니다.

```
Cat6k# show tcam interface vlan 900 acl in ip

* Global Defaults not shared


Entries from Bank 0


Entries from Bank 1

   permit       tcp host 10.88.80.135 any
   policy-route tcp any 0.0.0.0 255.255.232.190 (60 matches)         <-----These entries show
hardware redirection
   policy-route tcp any 0.0.0.1 255.255.232.190 (8 matches)
   policy-route tcp any 0.0.0.64 255.255.232.190 (16 matches)
   policy-route tcp any 0.0.0.65 255.255.232.190 (19 matches)
   policy-route tcp any 0.0.1.0 255.255.232.190
   policy-route tcp any 0.0.1.1 255.255.232.190
   policy-route tcp any 0.0.1.64 255.255.232.190
   policy-route tcp any 0.0.1.65 255.255.232.190
   policy-route tcp any 0.0.2.0 255.255.232.190
   policy-route tcp any 0.0.2.1 255.255.232.190
   policy-route tcp any 0.0.2.64 255.255.232.190
   policy-route tcp any 0.0.2.65 255.255.232.190 (75 matches)
   policy-route tcp any 0.0.3.0 255.255.232.190 (222195 matches)
```

WAE의 HIA(Here I Am)는 WAE MAC가 알려진 인터페이스와 동일한 인터페이스를 입력해야 합니다.WAE 라우터 목록에서 직접 연결된 인터페이스가 아닌 루프백 인터페이스를 사용하는 것이 좋습니다.

ASR 1000 Series 라우터의 WCCP 문제 해결

Cisco ASR 1000 Series 라우터의 WCCP 문제 해결 명령은 다른 라우터와 다릅니다.이 섹션에서는 ASR 1000에서 WCCP 정보를 가져오는 데 사용할 수 있는 명령을 보여줍니다.

경로 프로세서 WCCP 정보를 표시하려면 다음과 같이 **show platform software wccp rp active** 명령을 사용합니다.

```
ASR1000# sh platform software wccp rp active
Dynamic service 61
Priority: 34, Number of clients: 1                          <-----Number of WAE clients
Assign Method: Mask, Fwd Method: GRE, Ret Method: GRE       <-----Assignment, forwarding, and
return methods
L4 proto: 6, Use Source Port: No, Is closed: No
Dynamic service 62
Priority: 34, Number of clients: 1                          <-----
Assign Method: Mask, Fwd Method: GRE, Ret Method: GRE       <-----
L4 proto: 6, Use Source Port: No, Is closed: No
```

다음 예는 포워딩 프로세서 정보를 검사하는 데 사용할 수 있는 추가 명령을 보여줍니다.

```
ASR1000# sh platform software wccp fp active ?
  <0-255>     service ID
  cache-info  Show cache-engine info
  interface   Show interface info
  statistics  Show messaging statistics
  web-cache   Web-cache type
  |           Output modifiers
  <cr>
```

각 인터페이스에 대해 리디렉션된 패킷 통계를 표시하려면 다음과 같이 **show platform software wccp interface counters** 명령을 사용합니다.

```
ASR1000# sh platform software wccp interface counters
Interface GigabitEthernet0/1/2
       Input Redirect Packets  = 391
       Output Redirect Packets  = 0
Interface GigabitEthernet0/1/3
       Input Redirect Packets  = 1800
       Output Redirect Packets  = 0
```

다음과 같이 WCCP 캐시 정보를 표시하려면 **show platform software wccp web-cache counters** 명령을 사용합니다.

```
ASR1000# sh platform software wccp web-cache counters
Service Group (0, 0) counters
       unassigned_count = 0
       dropped_closed_count = 0
       bypass_count = 0
       bypass_failed_count = 0
       denied_count = 0
       redirect_count = 0
```

하위 수준 세부 정보를 표시하려면 다음 명령을 사용합니다.

- **show platform so interface F0 brief**
- **show platform software wccp f0 interface**
- **디버그 플랫폼 소프트웨어 wccp 구성**

자세한 내용은 백서 "Cisco ASR 1000 Series Aggregation Services Routers의 Web Cache Control Protocol 버전 2 구축 및 문제 해결"을 참조하십시오.

WAE에서 WCCP 문제 해결

show wccp services 명령을 사용하여 WAE의 문제 **해결을** 시작합니다.다음과 같이 구성된 서비스 61과 62를 모두 볼 수 있습니다.

```
WAE-612# show wccp services
Services configured on this File Engine
       TCP Promiscuous 61
       TCP Promiscuous 62
```

그런 다음 show wccp status 명령을 사용하여 WCCP 상태를 확인합니다.다음과 같이 WCCP 버전 2가 활성화되고 활성화되었음을 확인할 수 있습니다.

```
WAE-612# show wccp status
WCCP version 2 is enabled and currently active
```

show wccp wide-area-engine 명령을 사용하여 WCCP 팜 정보**를 확인합니다**.이 명령은 다음과 같이 팜에 있는 WAE 수, IP 주소, 리드 WAE, WAE를 볼 수 있는 라우터 및 기타 정보를 표시합니다.

```
WAE612# show wccp wide-area-engine
Wide Area Engine List for Service: TCP Promiscuous 61

Number of WAE's in the Cache farm: 3
Last Received Assignment Key IP address: 10.43.140.162     <-----All WAEs in farm should have
same Key IP
Last Received Assignment Key Change Number: 17
Last WAE Change Number: 16
Assignment Made Flag = FALSE

       IP address = 10.43.140.162       Lead WAE = YES  Weight = 0
       Routers seeing this Wide Area Engine(3)
               10.43.140.161
               10.43.140.166
               10.43.140.168

       IP address = 10.43.140.163       Lead WAE = NO  Weight = 0
       Routers seeing this Wide Area Engine(3)
               10.43.140.161
               10.43.140.166
               10.43.140.168

       IP address = 10.43.140.164       Lead WAE = NO  Weight = 0
       Routers seeing this Wide Area Engine(3)
               10.43.140.161
               10.43.140.166
               10.43.140.168
. . .
```

show wccp routers 명령을 사용하여 라우터 정보를 **확인합니다**.WCCP 지원 라우터와 양방향 통신이 있고 모든 라우터에 다음과 같이 동일한 KeyIP 및 KeyCN(변경 번호)이 표시되는지 확인합니다.

```
WAE-612# show wccp routers

Router Information for Service: TCP Promiscuous 61
       Routers Seeing this Wide Area Engine(1)
       Router Id       Sent To         Recv ID     KeyIP         KeyCN  MCN
       10.43.140.161   10.43.140.161   00203A21    10.43.140.162  17    52   <-----Verify
routers have same KeyIP and KeyCN
       10.43.140.166   10.43.140.166   00203A23    10.43.140.162  17    53
       10.43.140.168   10.43.140.165   00203A2D    10.43.140.162  17    25
       Routers not Seeing this Wide Area Engine
               -NONE-
       Routers Notified of from other WAE's
               -NONE-
       Multicast Addresses Configured
               -NONE-
. . .
```

WAE가 라우터에 인접한 레이어 2가 아니거나 루프백 주소를 사용하는 경우 WCCP를 지원하려면 고정 경로 또는 기본 게이트웨이가 필요합니다.

서비스 그룹에서 해시 버킷 배포를 검사하려면 다음과 같이 show wccp flows tcp-**promiscuous** 명령

을 사용합니다.

```
wae# sh wccp flows tcp-promiscuous
Flow counts for service: TCP Promiscuous 61
Bucket                                Flow Counts
  0- 11:     0     0     0     0     0     0     0     0     0     0     0     0
 12- 23:     0     0     0     0     0     0     0     0     0     0     0     0
 24- 35:     0     0     0     0     0     0     0     0     0     0     0     0
 36- 47:     0     0     0     0     0     0     0     0     0     0     0     0
 48- 59:     0     0     0     0     0     0     0     0     0     0     0     0
 60- 71:     0     0     0     0     0     0     0     0     0     0     0     0
 72- 83:     0     0     0     0     0     0     0     0     0     0     0     0
 84- 95:     0     0     0     0     0     0     0     0     0     0     0     0
 96-107:     0     0     0     0     0     0     0     0     0     0     0     0
108-119:     0     0     0     0     0     0     0     0     0     0     0     0
120-131:     0     0     0     0     0     0     0     0     0     0     0     0
132-143:     0     0     0     0     0     0     0     0     0     0     0     0
144-155:     0     0     0     0     0     0     0     0     0     0     0     0
156-167:     0     0     0     0     0     0     0     0     0     0     0     0
168-179:     0     0     0     0     0     0     0     0     0     0     0     0
180-191:     0     0     0     0     0     0     0     0     0     0     0     0
192-203:     0     0     0     0     0     0     0     0     0     0     0     0
204-215:     0     0     0     0     0     0     0     0     0     0     0     0
216-227:     0     0     0     0     0     0     0     0     0     0     0     0
228-239:     0     0     0     0     0     0     0     0     0     3     0     0
240-251:     0     0     0     0     0     0     0     0     0     0     0     0
252-255:     0     0     0     0
```

또는 명령의 요약 버전을 사용하여 흐름 정보를 우회하고 유사한 정보를 볼 수 있습니다.

```
wae# sh wccp flows tcp-promiscuous summary
Flow summary for service: TCP Promiscuous 61
Total Buckets
OURS = 256

  0- 59: OOOOOOOOOO OOOOOOOOOO OOOOOOOOOO OOOOOOOOOO OOOOOOOOOO OOOOOOOOOO
 60-119: OOOOOOOOOO OOOOOOOOOO OOOOOOOOOO OOOOOOOOOO OOOOOOOOOO OOOOOOOOOO
120-179: OOOOOOOOOO OOOOOOOOOO OOOOOOOOOO OOOOOOOOOO OOOOOOOOOO OOOOOOOOOO
180-239: OOOOOOOOOO OOOOOOOOOO OOOOOOOOOO OOOOOOOOOO OOOOOOOOOO OOOOOOOOOO
240-255: OOOOOOOOOO OOOOOO

BYP  = 0

  0- 59: .......... .......... .......... .......... .......... ..........
 60-119: .......... .......... .......... .......... .......... ..........
120-179: .......... .......... .......... .......... .......... ..........
180-239: .......... .......... .......... .......... .......... ..........
240-255: .......... ......

AWAY = 0

  0- 59: .......... .......... .......... .......... .......... ..........
 60-119: .......... .......... .......... .......... .......... ..........
120-179: .......... .......... .......... .......... .......... ..........
180-239: .......... .......... .......... .......... .......... ..........
240-255: .......... ......
. . .
```

다음과 같이 **show wccp gre** 명령을 사용하여 GRE 패킷 통계를 표시합니다.

```
WAE-612# show wccp gre
Transparent GRE packets received:              5531561         <-----Increments for WCCP GRE
redirection
Transparent non-GRE packets received:          0               <-----Increments for WCCP L2
redirection
Transparent non-GRE non-WCCP packets received: 0               <-----Increments for ACE or PBR
redirection
Total packets accepted:                        5051            <-----Accepted for optimization;
peer WAE found
Invalid packets received:                      0
Packets received with invalid service:         0
Packets received on a disabled service:        0
Packets received too small:                    0
Packets dropped due to zero TTL:               0
Packets dropped due to bad buckets:            0
Packets dropped due to no redirect address:    0
Packets dropped due to loopback redirect:      0
Pass-through pkts dropped on assignment update:0
Connections bypassed due to load:              0
Packets sent back to router:                   0
GRE packets sent to router (not bypass)        0               <-----Handled with WCCP
negotiated return egress
Packets sent to another WAE:                   0
GRE fragments redirected:                      0
GRE encapsulated fragments received:           0
Packets failed encapsulated reassembly:        0
Packets failed GRE encapsulation:              0
--More--
```

WCCP 리디렉션이 작동하는 경우 처음 두 카운터 중 하나가 증가해야 합니다.

WCCP Layer 2 리디렉션 전달 방법을 사용하여 리디렉션되는 패킷에 대해 Transparent non-GRE 패킷이 카운터 증분으로 수신되었습니다.

WCCP가 아닌 인터셉션 방법(예: ACE 또는 PBR)에 의해 리디렉션되는 패킷에 대해 수신된 Transparent non-GRE non-WCCP 패킷은 카운터 증분 값을 받습니다.

Total packets accepted 카운터는 자동 검색이 피어 WAE를 발견했기 때문에 최적화를 위해 수락된 패킷을 나타냅니다.

GRE packets sent to router (not bypass) 카운터는 WCCP 협상된 반환 이그레스 방법을 사용하여 처리된 패킷을 나타냅니다.

다른 WAE 카운터로 전송된 패킷은 다른 WAE가 서비스 그룹에 추가되고 다른 WAE에서 이전에 처리하던 버킷 할당을 처리하기 시작할 때 플로우 보호가 이루어지고 있음을 나타냅니다.

다음과 같이 **show egress-methods** 명령을 사용하여 사용 중인 이그레스(egress) 메서드가 예상된 메서드인지 확인합니다.

```
WAE674# show egress-methods

Intercept method : WCCP

 TCP Promiscuous 61 :
     WCCP negotiated return method : WCCP GRE

                       Egress Method      Egress Method
```

```
     Destination        Configured            Used
     -----------  ----------------------  -------------
     any          WCCP Negotiated Return  WCCP GRE               <-----Verify these are
expected

 TCP Promiscuous 62 :
     WCCP negotiated return method : WCCP GRE

                      Egress Method      Egress Method
     Destination        Configured            Used
     -----------  ----------------------  -------------
     any          WCCP Negotiated Return  WCCP GRE               <-----Verify these are
expected
```

이그레스(egress) 메서드 불일치(mismatch)는 다음 조건에서 발생할 수 있습니다.

- 협상된 반환 이그레스 방법이 구성되었지만 WCCP는 레이어 2 반환 방법을 협상하며 WAAS에서는 GRE 반환만 지원합니다.
- 일반 GRE 이그레스 방법이 구성되었지만 인터셉션 방법은 레이어 2이며 일반 GRE 이그레스(egress)가 구성된 경우 WCCP GRE만 인터셉션 방법으로 지원됩니다.

이러한 경우 이그레스 방법 또는 WCCP 컨피그레이션을 변경하여 불일치가 해결되면 경보의 발생 및 지워집니다.경보가 해제될 때까지 기본 IP 포워딩 이그레스(egress) 방법이 사용됩니다.

다음 예에서는 불일치가 있을 때 명령 출력을 보여 줍니다.

```
WAE612# show egress-methods
Intercept method : WCCP
 TCP Promiscuous 61 :
     WCCP negotiated return method : WCCP GRE

                      Egress Method      Egress Method
     Destination        Configured            Used
     -----------  ----------------------  -------------
     any          Generic GRE             IP Forwarding                    <-----Mismatch

     WARNING:  WCCP has negotiated WCCP L2 as the intercept method for    <-----Warning if
mismatch occurs
               which generic GRE is not supported as an egress method
               in this release. This device uses IP forwarding as the
               egress method instead of the configured generic GRE
               egress method.
 TCP Promiscuous 62 :

     WCCP negotiated return method : WCCP GRE
                      Egress Method      Egress Method
     Destination        Configured            Used
     -----------  ----------------------  -------------
     any          Generic GRE             IP Forwarding                    <-----Mismatch

     WARNING:  WCCP has negotiated WCCP L2 as the intercept method for    <-----Warning if
mismatch occurs
               which generic GRE is not supported as an egress method
               in this release. This device uses IP forwarding as the
               egress method instead of the configured generic GRE
               egress method.
```

Catalyst 6500 Sup720 또는 Sup32 라우터의 경우 하드웨어에서 처리되는 일반 GRE 이그레스 방법을 사용하는 것이 좋습니다.또한 각 WAE에 대해 하나의 포인트-투-포인트 터널이 아닌 손쉬운 구성을 위해 하나의 멀티포인트 터널을 사용하는 것이 좋습니다.터널 컨피그레이션에 대한 자세한 내

용은 *Cisco Wide Area Application Services 컨피그레이션 가이드*의 라우터에서 GRE 터널 인터페이스 구성 섹션을 참조하십시오.

각 가로채기 라우터에 대한 GRE 터널 통계를 보려면 다음과 같이 **show statistics generic-gre** 명령을 사용합니다.

```
WAE# sh stat generic
Tunnel Destination:                              10.10.14.16
Tunnel Peer Status:                              N/A
Tunnel Reference Count:                          2
Packets dropped due to failed encapsulation:     0
Packets dropped due to no route found:           0
Packets sent:                                    0
Packets sent to tunnel interface that is down:   0
Packets fragmented:                              0
```

WAE의 이그레스 패킷이 다시 차단되지 않도록 하는 데 실패하면 리디렉션 루프로 이어질 수 있습니다.WAE가 TCP 옵션 필드에 반환된 자체 ID를 탐지하면 리디렉션 루프가 발생하며 다음 syslog 메시지가 나타납니다.

```
%WAAS-SYS-3-900000: 137.34.79.11:1192 - 137.34.77.196:139 - opt_syn_rcv: Routing Loop detected -
Packet has our own devid. Packet dropped.
```

다음과 같이 **find** 명령을 사용하여 syslog.txt 파일에서 이 오류의 인스턴스를 검색할 수 있습니다.

```
WAE-612# find match “Routing Loop” syslog.txt
```

이 오류는 **show statistics filtering** 명령에서 사용할 수 있는 TFO 플로우 통계에도 다음과 같이 표시됩니다.

```
WAE-612# show statistics filtering
. . .
Syn packets dropped with our own id in the options:   8          <-----Indicates a redirection
loop
. . .
```

라우터에서 아웃바운드 리디렉션을 수행하는 경우 트래픽이 라우터를 떠날 때 WAE로 다시 리디렉션됩니다. 그러면 라우터에서 패킷을 다시 라우팅하여 라우팅 루프가 발생합니다.데이터 센터 WAE와 서버가 서로 다른 VLAN에 있고 브랜치 WAE와 클라이언트가 서로 다른 VLAN에 있는 경우 WAE VLAN에서 다음 라우터 컨피그레이션을 사용하여 라우팅 루프를 피할 수 있습니다.

```
ip wccp redirect exclude in
```

WAE가 인접한 클라이언트 또는 서버와 동일한 VLAN을 공유하는 경우 협상된 반환 방법을 사용하여 라우팅 루프를 방지하거나 하드웨어에서 WCCP 리디렉션이 수행되는 플랫폼에 대해 일반 GRE 리턴을 방지할 수 있습니다.일반 GRE 반환을 사용할 때 WAE는 GRE 터널을 사용하여 라우터로 트래픽을 반환합니다.

버전 4.4.1에서 구성 가능한 서비스 ID 및 변수 시간 초과 문제 해결

참고:WCCP 구성 가능 서비스 ID 및 변수 실패 감지 시간 초과 기능이 WAAS 버전 4.4.1에 도입되었습니다. 이 섹션은 이전 WAAS 버전에는 적용되지 않습니다.

WCCP 팜의 모든 WAE는 동일한 WCCP 서비스 ID 쌍(기본값은 61 및 62)을 사용해야 하며 이러한 ID는 팜을 지원하는 모든 라우터와 일치해야 합니다.WCCP 서비스 ID가 라우터에 구성된 WAE와 다른 WCCP 서비스 ID는 팜에 조인할 수 없으며 기존 "라우터 도달 불가" 경보가 발생합니다.마찬가지로, 팜의 모든 WAE는 오류 탐지 시간 제한에 동일한 값을 사용해야 합니다.일치하지 않는 값으로 WAE를 구성하면 경보가 발생합니다.

WAE가 WCCP 팜에 조인할 수 없다는 경보가 표시되면 WAE에 구성된 WCCP 서비스 ID와 팜의 라우터가 일치하는지 확인합니다.WAE에서 **show wccp wide-area-engine** 명령을 사용하여 구성된 서비스 ID를 확인합니다.라우터에서 **show ip wccp** IOS 명령을 사용할 수 있습니다.

WAE가 라우터에 연결되어 있는지 확인하려면 show wccp **services detail** 및 show wccp **router detail** 명령을 사용합니다.

또한 debug ip wccp **이벤트** 또는 debug ip wccp **packet** 명령을 사용하여 WAE에서 WCCP 디버그 출력을 활성화할 수 있습니다.

WAE에 대한 "Router Unavailable" 하위 경보가 표시되면 WAE에 설정된 변수 실패 탐지 시간 초과 값이 라우터에서 지원되지 않음을 의미할 수 있습니다.**show alarm minor detail** 명령을 사용하여 경보 사유가 "Timer interval mismatch with router"인지 확인합니다.

```
WAE# show alarm minor detail

Minor Alarms:
-------------
       Alarm ID                 Module/Submodule                Instance
  ---------------             --------------------          ---------------
  1 rtr_unusable              WCCP/svc051/rtr2.192.9.161

    Jan 11 23:18:41.885 UTC, Communication Alarm, #000005, 17000:17003
    WCCP router 2.192.9.161 unusable for service id: 51 reason: Timer interval       <-----Check
reason
mismatch with router                                                                 <-----
```

WAE에서 다음과 같이 구성된 실패 감지 시간 제한을 확인합니다.

```
WAE# show wccp services detail

Service Details for TCP Promiscuous 61 Service
       Service Enabled                    : Yes
       Service Priority                   : 34
       Service Protocol                   : 6
       Application                        : Unknown
       Service Flags (in Hex)             : 501
       Service Ports                      :      0     0     0     0
                                          :      0     0     0     0
       Security Enabled for Service       : No
       Multicast Enabled for Service      : No
       Weight for this Web-CE             : 1
       Negotiated forwarding method       : GRE
       Negotiated assignment method       : HASH
       Negotiated return method           : GRE
       Negotiated HIA interval            : 2 second(s)
       Negotiated failure-detection timeout  : 30 second(s)          <-----Failure detection
```

```
timeout configured
. . .
```

라우터에서 IOS 버전이 변수 실패 감지 시간 제한을 지원하는지 확인합니다.이 경우 **show ip wccp *xx* detail** 명령을 사용하여 구성된 설정을 확인할 수 있습니다. 여기서 *xx*는 WCCP 서비스 ID입니다 .세 가지 가능한 결과가 있습니다.

- WAE는 30초의 기본 실패 감지 시간 제한을 사용하며 라우터는 동일하게 구성되거나 변수 시간 제한을 지원하지 않습니다.라우터 출력에 시간 초과 설정에 대한 세부 정보가 표시되지 않습니다.이 컨피그레이션은 정상적으로 작동합니다.
- WAE는 기본이 아닌 오류 감지 시간 초과인 9 또는 15초를 사용하고 있으며 라우터는 변수 시간 제한을 지원하지 않습니다.State(상태) 필드에는 "NOT Usable(사용 불가)"이 표시되고 WAE는 라우터를 사용할 수 없습니다.wccp tcp failure-detection **30 전역** 컨피그레이션 명령을 사용하여 WAE 실패 감지 시간 제한을 기본값인 30초로 변경합니다.
- WAE는 9 또는 15초의 기본 오류 감지 시간 제한을 사용하며 라우터는 변수 시간 제한을 지원합니다.클라이언트 시간 초과 필드는 WAE와 일치하는 구성된 실패 감지 시간 제한을 표시합니다.이 컨피그레이션은 정상적으로 작동합니다.

링크 플래핑으로 인해 WCCP 팜이 불안정하면 WCCP 실패 감지 시간 제한이 너무 낮기 때문일 수 있습니다.