eBGP 인접성 설정 실패 문제 해결

목차

문제

방화벽과 피어 디바이스 간의 eBGP(external Border Gateway Protocol) 인접성이 실패합니다. 다음과 같은 증상이 관찰됩니다.

1. 방화벽의 피어 상태가 유휴 상태입니다.

<#root>

fw#

show bgp summary

BGP router identifier 192.0.2.2, local AS number 65001
BGP table version is 1, main routing table version 1

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd

198.51.100.2

4 65002 0 0 1 0 0 never

Idle

2. 피어 디바이스의 TCP SYN 패킷만 인터페이스 캡처에 표시됩니다.

<#root>

fw#

cap capo interface WAN-Telekom

fw#

```
show cap capo


26 packets captured

   1: 06:22:44.990595       198.51.100.2.31242 > 192.0.2.2.179: S 2838607371:2838607371(0) win 16384 <m
   2: 06:22:46.990152       198.51.100.2.31242 > 192.0.2.2.179: S 2838607371:2838607371(0) win 16384 <m
   3: 06:22:50.991007       198.51.100.2.31242 > 192.0.2.2.179: S 2838607371:2838607371(0) win 16384 <m
   4: 06:22:58.991281       198.51.100.2.31242 > 192.0.2.2.179: S 2838607371:2838607371(0) win 16384 <m
```

3. 피어 장치의 IP 주소에 대한 ICMP 연결이 성공적으로 설정되었습니다.

```
<#root>

fw#

ping 198.51.100.2


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.51.100.2, timeout is 2 seconds:

!!!!!


Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

이렇게 하면 방화벽과 피어 디바이스 간의 IP 네트워크 레벨 연결이 확인됩니다.

4. 디버깅 레벨 syslog 메시지는 피어 디바이스에서 취소된 TCP 요청을 나타냅니다.

```
<#root>

fw#

show logging

…

May 20 2026 06:32:58: %FTD-7-710005: TCP request discarded from 198.51.100.2/20217 to WAN-Telekom:192.0.


May 20 2026 06:33:00: %FTD-7-710005: TCP request discarded from 198.51.100.2/20217 to WAN-Telekom:192.0
May 20 2026 06:33:04: %FTD-7-710005: TCP request discarded from 198.51.100.2/20217 to WAN-Telekom:192.0
May 20 2026 06:33:12: %FTD-7-710005: TCP request discarded from 198.51.100.2/20217 to WAN-Telekom:192.0
```

5. BGP 디버그는 "no route to peer" 메시지를 표시합니다.

<#root>

fw#

debug ip bgp

BGP debugging is on
    for address family: IPv4 Unicast
Successfully set for module BGP at level 1

BGP: 198.51.100.2 Active open failed - no route to peer, open active delayed 21504ms (35000ms max, 60% j

환경

토폴로지

- FTD 7.4.4를 실행 중이며 FMC(Secure Firewall Management Center)에서 관리되는 firepower 2110. 다른 하드웨어 플랫폼 및 소프트웨어 버전도 영향을 받을 수 있습니다.
- 방화벽에는 ISP(인터넷 서비스 공급자)에 연결된 WAN-Telekom 인터페이스를 통해 피어 주소에 대한 고정 경로가 있습니다.

<#root>

fw#

show route 198.51.100.2

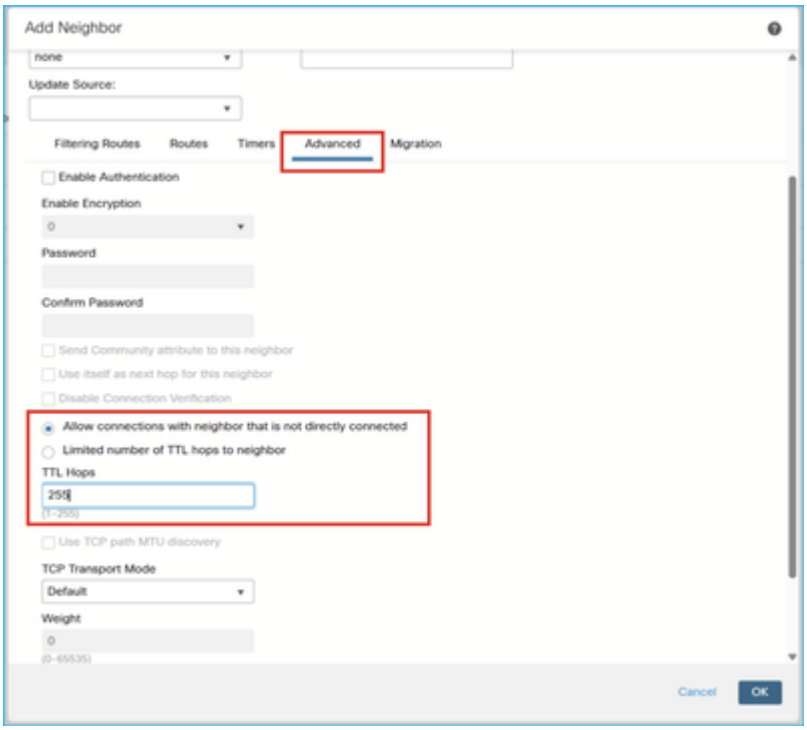
```
Routing entry for 198.51.100.2 255.255.255.255


  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:

  * 192.0.2.1, via WAN-Telekom


Route metric is 0, traffic share count is 1
```

- 방화벽에 BGP 컨피그레이션이 있습니다. 피어 198.51.100.2에는 다른 자동 시스템 번호가 있으므로 외부에 있습니다.

```
<#root>

fw#

show run router



router bgp 65001


 bgp log-neighbor-changes
 bgp graceful-restart
 address-family ipv4 unicast

  neighbor 198.51.100.2 remote-as 65002


  neighbor 198.51.100.2 transport path-mtu-discovery disable
  neighbor 198.51.100.2 update-source WAN-Telekom
  neighbor 198.51.100.2 activate
```

해결

인접성은 BGP 인접 디바이스 컨피그레이션의 Advanced(고급) 섹션에서 Allow connections with not directly connected(직접 연결되지 않은 인접 디바이스와의 연결 허용) 옵션을 활성화하고 TTL Hops를 255로 설정한 후 설정됩니다.



원인

기본적으로 방화벽은 직접 연결된 피어, 즉 동일한 서브넷에 있는 피어 간의 eBGP 인접성을 허용합니다. 직접 연결되지 않은 피어 간의 인접성을 허용하려면 직접 연결되지 않은 네이버와의 연결 허용 옵션을 활성화해야 합니다. 또한 사용자는 피어에 대한 TTL 홉 수를 제한하고 피어에서 수신한 TCP 패킷의 IP 헤더에 최소 예상 Time To Live 값을 설정할 수 있습니다. 기본값은 1입니다.

확인

1. 직접 연결되지 않은 인접 디바이스와의 연결 허용 옵션이 구성되지 않았습니다.

<#root>

fw#

show bgp neighbors 198.51.100.2 | i External

External BGP neighbor not directly connected.

2. 직접 연결되지 않은 네이버와의 연결 허용 옵션이 구성되고 TTL 홉이 1로 설정됩니다.

<#root>

```
fw#

show run router bgp | i 198.51.100.2


  neighbor 198.51.100.2 remote-as 65002

  neighbor 198.51.100.2 ebgp-multihop 1


  neighbor 198.51.100.2 transport path-mtu-discovery disable
  neighbor 198.51.100.2 update-source WAN-Telekom
  neighbor 198.51.100.2 activate


fw#

show bgp neighbors 198.51.100.2 | i External



  External BGP neighbor not directly connected.
```

3. 직접 연결되지 않은 네이버와의 연결 허용 옵션이 구성되고 TTL 홉이 255로 설정됩니다.

<#root>

```
fw#

show run router bgp | i 198.51.100.2


  neighbor 198.51.100.2 remote-as 65002

  neighbor 198.51.100.2 ebgp-multihop 255


  neighbor 198.51.100.2 transport path-mtu-discovery disable
  neighbor 198.51.100.2 update-source WAN-Telekom
  neighbor 198.51.100.2 activate


fw#

show bgp neighbors 198.51.100.2 | i External
```

```
External BGP neighbor may be up to 255 hops away.
```

관련 콘텐츠

- Cisco 기술 지원 및 다운로드

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.