Fehlerbehebung bei eBGP-Adjazenzbegründungsfehler

Inhalt

Problem

Die eBGP-Adjacency zwischen der Firewall und den Peer-Geräten schlägt fehl. Diese Symptome wurden beobachtet:

1. Der Peer-Status auf der Firewall ist inaktiv:

<#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. Nur TCP SYN-Pakete vom Peer-Gerät werden in der Schnittstelle erkannt, die Folgendes erfasst:

<#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. Eine ICMP-Verbindung zur IP-Adresse des Peer-Geräts wurde erfolgreich hergestellt:

```
<#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
```

Dies bestätigt die Erreichbarkeit auf IP-Netzwerkebene zwischen der Firewall und dem Peer-Gerät.

4. Die Syslog-Meldungen auf Debugging-Ebene weisen darauf hin, dass die TCP-Anforderung vom Peer-Gerät verworfen wurde:

```
<#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. Die BGP-Fehlerbehebungen zeigen die Meldung "no route to peer" an:

<#root>

```
fw#
```

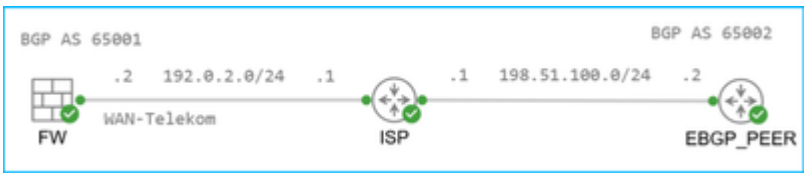
```
debug ip bgp
```

```
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
```

Umwelt

Topologie



- Firepower 2110 mit FTD 7.4.4 und verwaltet durch das Secure Firewall Management Center (FMC). Auch andere Hardwareplattformen und Softwareversionen können betroffen sein.
- Die Firewall hat eine statische Route zur Peer-Adresse über eine WAN-Telekom-Schnittstelle, die mit dem Internet Service Provider (ISP) verbunden ist:

<#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
```

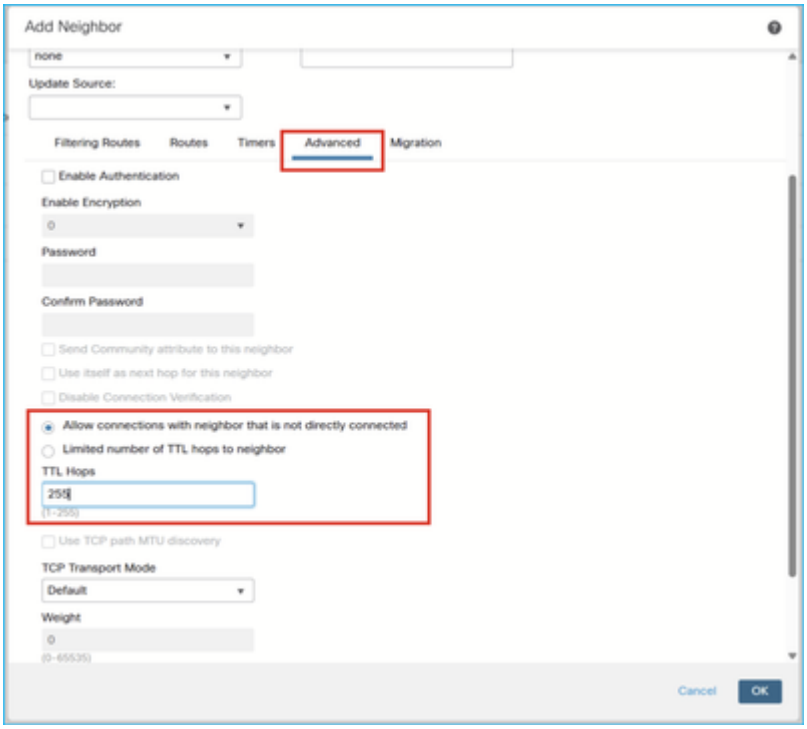
- Die Firewall hat die BGP-Konfiguration. Der Peer 198.51.100.2 hat eine andere autonome Systemnummer und ist daher extern:

<#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
```

Auflösung

Die Adjacency wird eingerichtet, nachdem die Option Verbindungen mit Nachbarn zulassen, die nicht direkt verbunden sind, im Abschnitt Erweitert der BGP-Nachbarkonfiguration aktiviert und die TTL-Hops auf 255 festgelegt wurden:



Ursache

Standardmäßig lässt die Firewall die eBGP-Adjacency zwischen den direkt verbundenen Peers zu, d. h. den Peers im gleichen Subnetz. Um die Adjacency zwischen nicht direkt verbundenen Peers zu ermöglichen, muss die Option Verbindungen mit Nachbarn zulassen, die nicht direkt verbunden sind, aktiviert sein. Darüber hinaus kann der Benutzer die Anzahl der TTL-Hops zum Peer begrenzen und den erwarteten Time To Live-Mindestwert im IP-Header des vom Peer empfangenen TCP-Pakets festlegen. Der Standardwert ist 1.

Verifizierung

1. Die Option Verbindungen mit Nachbarn zulassen, die nicht direkt verbunden sind, ist nicht konfiguriert:

<#root>

```
fw#
```

```
show bgp neighbors 198.51.100.2 | i External
```

```
External BGP neighbor not directly connected.
```

2. Die Option Verbindungen mit Nachbarn zulassen, die nicht direkt verbunden sind ist konfiguriert, und TTL-Hops ist auf 1 gesetzt:

<#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. Die Option Verbindungen mit Nachbarn zulassen, die nicht direkt verbunden sind ist konfiguriert, und TTL-Hops ist auf 255 festgelegt:

<#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.
```

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.