Problemen met eBGP-aangrenzende vestiging oplossen

Inhoud

uitgeven

Het eBGP-protocol (External Border Gateway Protocol) tussen de firewall en de peer-apparaten werkt niet. Deze symptomen worden waargenomen:

1. De peerstatus op de firewall is inactief:

<#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. Alleen TCP SYN-pakketten van het peer-apparaat worden weergegeven in de interfaceopnames:

<#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. Er is een ICMP-verbinding met het IP-adres van het peer-apparaat tot stand gebracht:

<#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

Dit bevestigt de bereikbaarheid op IP-netwerkniveau tussen de firewall en het peer-apparaat.

4. De syslog-berichten op foutopsporingsniveau geven aan dat het TCP-verzoek van het peer-apparaat is afgewezen:

<#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. De BGP-debugs tonen het bericht "geen route naar peer":

<#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

milieu

Topologie

- Firepower 2110 met FTD 7.4.4 en beheerd door het Secure Firewall Management Center (FMC). Ook andere hardwareplatforms en softwareversies kunnen worden beïnvloed.
- De firewall heeft een statische route naar het peer-adres via de WAN-Telekom-interface die is verbonden met de Internet Service Provider (ISP):

<#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
```

- De firewall heeft de BGP-configuratie. De peer 198.51.100.2 heeft een ander autonoom systeemnummer en is dus extern:

<#root>

```
fw#
```

```
show run router
```

```
router bgp 65001
```

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

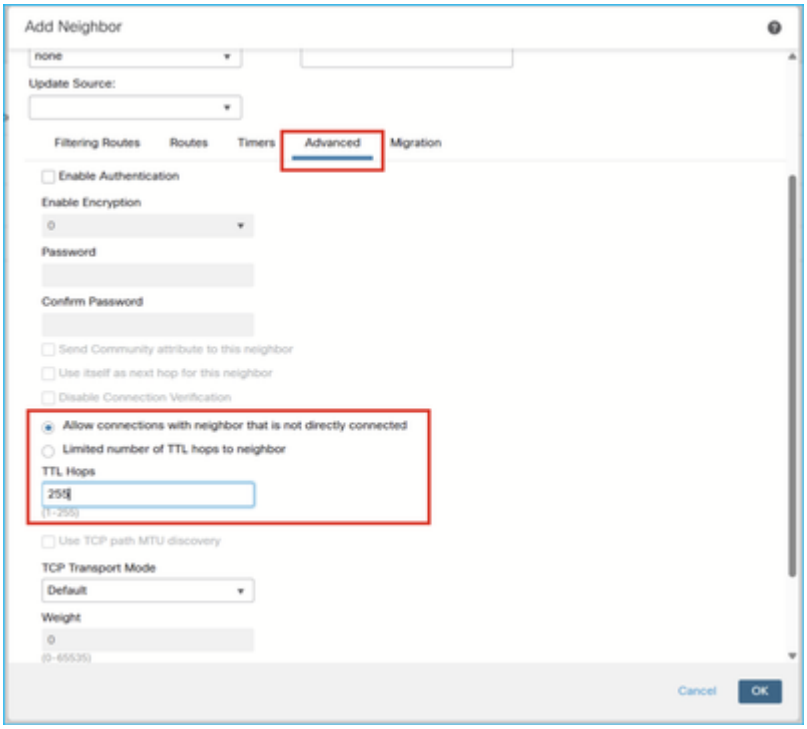
```
  neighbor 198.51.100.2 remote-as 65002
```

```
  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
```

resolutie

De nabijheid wordt vastgesteld nadat de optie Verbindingen toestaan met buren die niet

rechtstreeks zijn verbonden in het gedeelte Geavanceerd van de BGP-buurconfiguratie is ingeschakeld en de TTL-hop is ingesteld op 255:



Oorzaak

Standaard staat de firewall de eBGP-nabijheid toe tussen de direct verbonden peers, dat wil zeggen de peers in hetzelfde subnet. Om de nabijheid van niet-direct verbonden peers mogelijk te maken, moet de optie Verbindingen toestaan met buren die niet direct verbonden zijn, worden ingeschakeld. Bovendien kan de gebruiker het aantal TTL-hops beperken tot peer en de minimale verwachte Time To Live-waarde instellen in de IP-header van het TCP-pakket dat van de peer is ontvangen. De standaardwaarde is 1.

Verificatie

1. De optie Verbindingen toestaan met buren die niet rechtstreeks zijn verbonden, is niet geconfigureerd:

<#root>

fw#

show bgp neighbors 198.51.100.2 | i External

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

2. De optie Verbindingen toestaan met buren die niet rechtstreeks zijn verbonden, is geconfigureerd en TTL Hops is ingesteld op 1:

```
<#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. De optie Verbindingen toestaan met buren die niet rechtstreeks zijn verbonden, is geconfigureerd en TTL Hops is ingesteld op 255:

```
<#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.

Verwante inhoud

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.