排除eBGP邻接建立故障

目录

问题

防火墙和对等设备之间的外部边界网关协议(eBGP)邻接失败。观察到以下症状：

1.防火墙上的对等体状态为空闲：

<#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.在接口捕获中只能看到来自对等设备的TCP SYN数据包：

<#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.成功建立到对等设备的IP地址的ICMP连接：

```
<#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
```

这可以确认防火墙和对等设备之间的IP网络级别可达性。

4.调试级别的系统日志消息表示从对等设备丢弃的TCP请求：

```
<#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调试显示“no route to peer”消息：

<#root>

fw#

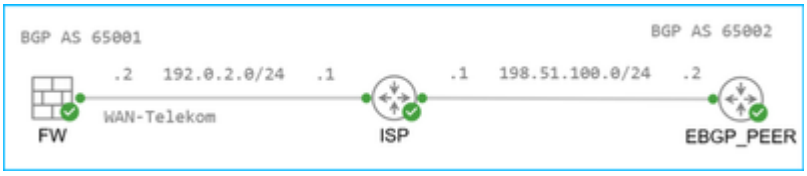
debug ip bgp

```
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

环境

拓扑



- 运行FTD 7.4.4并由安全防火墙管理中心(FMC)管理的Firepower 2110。 其他硬件平台和软件版本也可能受到影响。
- 防火墙通过连接到Internet服务提供商(ISP)的WAN-Telekom接口具有到对等地址的静态路由：

<#root>

fw#

show route 198.51.100.2

```
Routing entry for 198.51.100.2 255.255.255.255
```

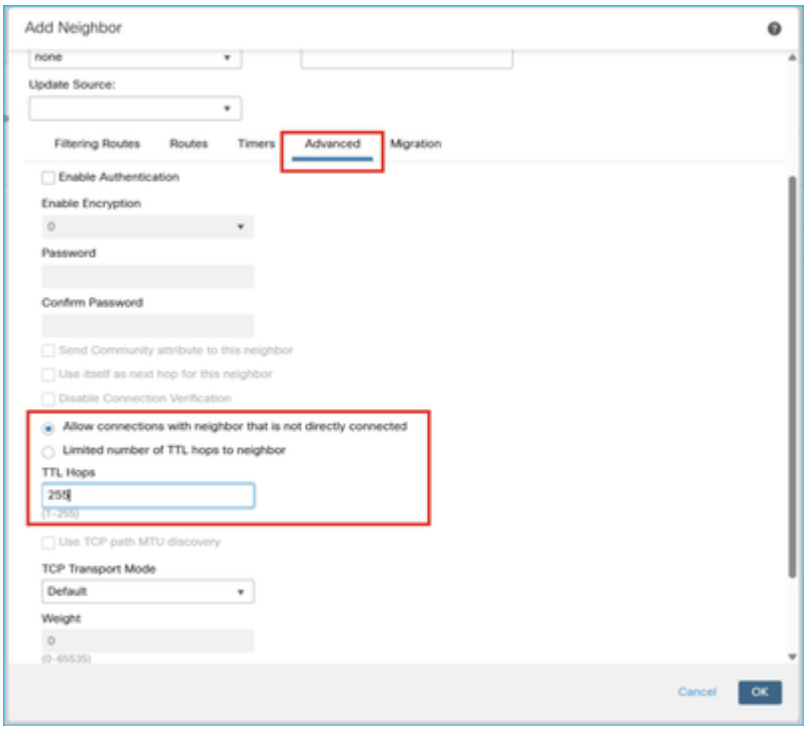
```
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:

  * 192.0.2.1, via WAN-Telekom


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

- 防火墙具有BGP配置。对等体198.51.100.2具有不同的自治系统编号，因此是外部的：

```
<#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
```

分辨率

启用BGP邻居配置的Advanced部分中的Allow connections with neighbor that is not directly connected选项并将TTL Hops设置为255后，邻接关系即建立：



原因

默认情况下，防火墙允许直连对等体（即同一子网中的对等体）之间的eBGP邻接。要允许非直连对等体之间的邻接，必须启用允许与未直连的邻居的连接选项。此外，用户可以限制对等体的TTL跳数，并在从对等体收到的TCP数据包的IP报头中设置最小预期生存时间值。默认值为 1。

确认

1.未配置Allow connections with neighbor that is not directly connected选项：

<#root>

fw#

show bgp neighbors 198.51.100.2 | i External

External BGP neighbor not directly connected.

2.配置了Allow connections with neighbor that is not directly connected选项，并且TTL Hops设置为

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.配置了Allow connections with neighbor that is not directly connected选项，并且TTL Hops设置为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.
```

相关内容

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。