eBGP隣接関係確立の障害のトラブルシューティング

内容

お問い合わせ内容

ファイアウォールとピアデバイスの間の外部ボーダーゲートウェイプロトコル(eBGP)隣接関係に障害が発生する。確認された症状は次のとおりです。

1. ファイアウォールのピア状態はidle:

<#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. ピアデバイスからのTCP SYNパケットだけがインターフェイスキャプチャに表示されます。

<#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. ピアデバイスのIPアドレスへのICMP接続が正常に確立されます。

```
<#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
```

これにより、ファイアウォールとピアデバイスの間のIPネットワークレベルの到達可能性が確認されます。

4. デバッグレベルのsyslogメッセージは、ピアデバイスから廃棄されたTCP要求を示しています。

```
<#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デバッグで「no route to peer」メッセージが表示されます。

<#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

環境

トポロジ

- FTD 7.4.4が稼働し、Secure Firewall Management Center(FMC)で管理されるFirepower 2110。 他のハードウェアプラットフォームやソフトウェアバージョンも影響を受ける可能性があります。
- ファイアウォールには、Internet Service Provider（ISP；インターネットサービスプロバイダー）に接続されたWAN-Telekomインターフェイスを介したピアアドレスへのスタティックルートがあります。

<#root>

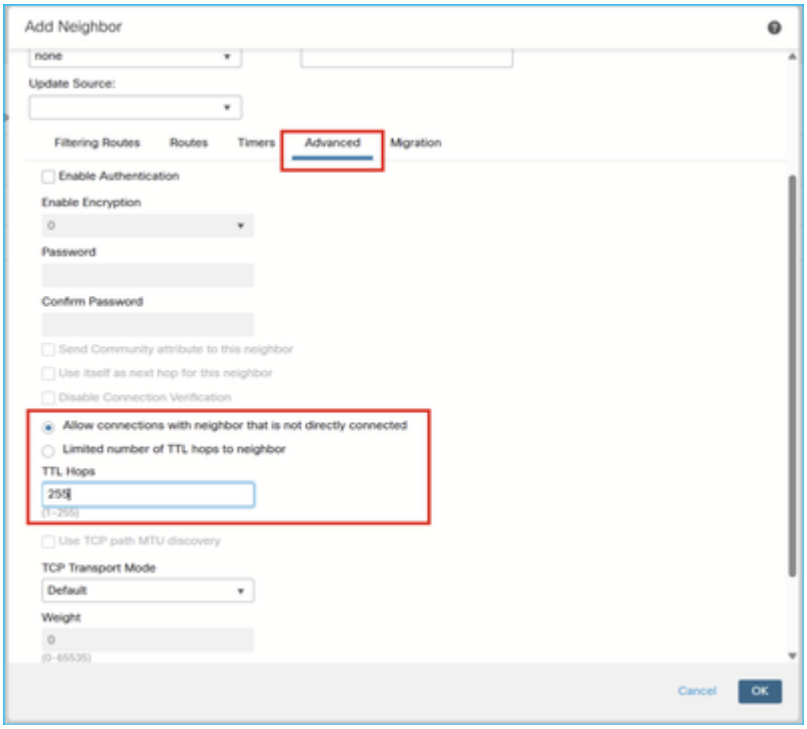
```
fw#

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
```

- ファイアウォールにはBGP設定があります。ピア198.51.100.2は異なる自律システム番号を持つため、外部です。

```
<#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
```

解決策

隣接関係が確立されるのは、BGPネイバー設定のAdvancedセクションでAllow connections with the neighbor that is not directly connectedオプションを有効にして、TTL Hopsを255に設定した後です。



原因

デフォルトでは、ファイアウォールは直接接続されたピア、つまり同じサブネット内のピア間のeBGP隣接関係を許可します。直接接続されていないピア間の隣接関係を許可するには、Allow connections with neighbor that is not directly connectedオプションを有効にする必要があります。また、ユーザはピアへのTTLホップ数を制限し、ピアから受信したTCPパケットのIPヘッダーで存続可能時間(TTL)の最小値を設定できます。デフォルト値は 1 です。

検証

1. Allow connections with neighbor that is not directly connectedオプションが設定されていない。

<#root>

fw#

show bgp neighbors 198.51.100.2 | i External

External BGP neighbor not directly connected.

2. Allow connections with neighbor that is not directly connectedオプションが設定されており、TTL Hopsが1に設定されている場合。

<#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. Allow connections with neighbor that is not directly connectedオプションが設定されており、TTL Hopsが255に設定されている場合。

<#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.

関連コンテンツ

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。