

Troubleshooting de Falha de Estabelecimento de Adjacência de eBGP

Contents

Problema

A adjacência do Border Gateway Protocol (eBGP) externo entre o firewall e os dispositivos pares falha. Estes sintomas são observados:

1. O estado par no firewall é ocioso:

```
<#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. Somente os pacotes TCP SYN do dispositivo par são vistos nas capturas de interface:

```
<#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. Uma conexão ICMP com o endereço IP do dispositivo par é estabelecida com êxito:

```
<#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
```

Isso confirma a acessibilidade do nível de rede IP entre o firewall e o dispositivo par.

4. As mensagens de syslog de nível de depuração indicam uma solicitação TCP descartada do dispositivo de mesmo nível:

```
<#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. As depurações de BGP mostram a mensagem "no route to peer" :

```
<#root>
```

```
fw#
```

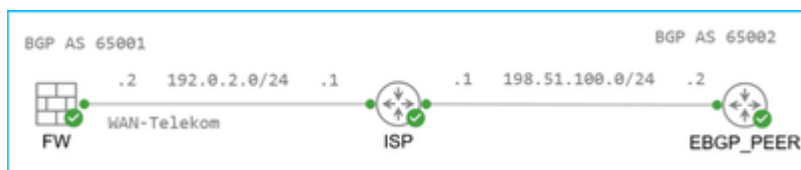
```
debug ip bgp
```

```
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%
```

Ambiente

Topologia



- Firepower 2110 executando o FTD 7.4.4 e gerenciado pelo Secure Firewall Management Center (FMC). Outras plataformas de hardware e versões de software também podem ser afetadas.
- O firewall tem uma rota estática para o endereço do peer através da interface WAN-Telekom conectada ao Provedor de Serviços de Internet (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
```

- O firewall tem a configuração de BGP. O peer 198.51.100.2 tem um número de sistema autônomo diferente, portanto é externo:

```
<#root>
```

```
fw#
```

```
show run router
```

```
router bgp 65001
```

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

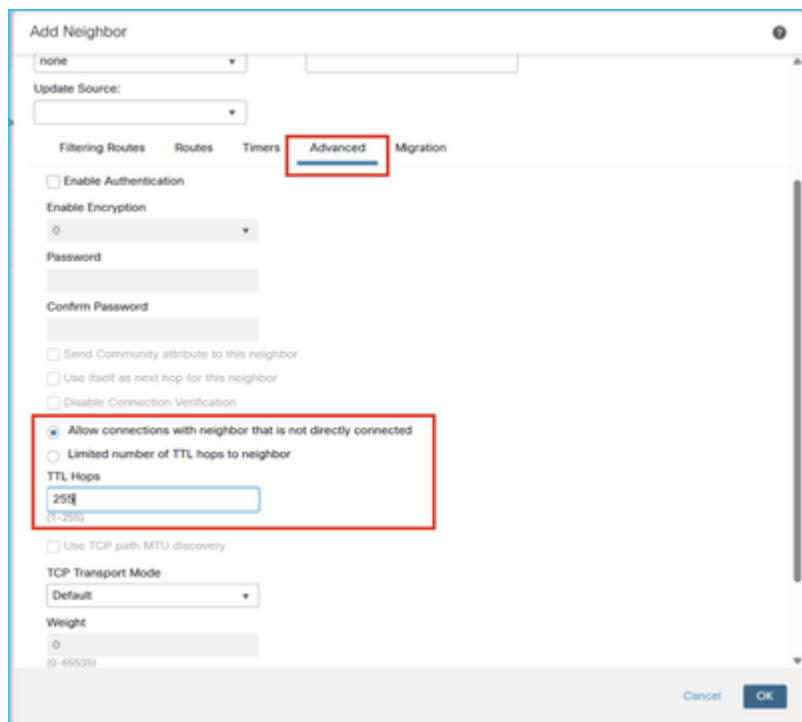
```
neighbor 198.51.100.2 remote-as 65002
```

```
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
```

Resolução

A adjacência é estabelecida após a habilitação da opção Permitir conexões com o vizinho que

não está diretamente conectado na seção Avançado da configuração do vizinho BGP e a definição de Saltos TTL como 255:



Causa

Por padrão, o firewall permite a adjacência de eBGP entre os peers diretamente conectados, ou seja, os peers na mesma sub-rede. Para permitir a adjacência entre peers não diretamente conectados, a opção Permitir conexões com vizinhos que não estejam diretamente conectados deve ser habilitada. Além disso, o usuário pode limitar o número de saltos TTL para peer e definir o valor mínimo esperado de Time To Live no cabeçalho IP do pacote TCP recebido do peer. O valor padrão é 1.

Verificação

1. A opção Permitir conexões com vizinhos que não estejam diretamente conectados não está configurada:

```
<#root>
```

```
fw#
```

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

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

2. A opção Permitir conexões com o vizinho que não está diretamente conectado está configurada e os Saltos TTL estão definidos como 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. A opção Permitir conexões com o vizinho que não está diretamente conectado está configurada e os Saltos TTL estão definidos como 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.

Conteúdo relacionado

- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.