

Risoluzione dei problemi relativi all'errore di determinazione dell'adiacenza eBGP

Sommario

Problema

Errore dell'adiacenza del protocollo eBGP (Border Gateway Protocol) esterno tra il firewall e i dispositivi peer. Questi sintomi sono osservati:

1. Lo stato peer sul firewall è inattivo:

```
<#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. Nelle acquisizioni dell'interfaccia vengono visualizzati solo i pacchetti TCP SYN dal dispositivo peer:

```
<#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. È stata stabilita una connessione ICMP all'indirizzo IP del dispositivo peer:

<#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

Ciò conferma che il firewall e il dispositivo peer sono raggiungibili a livello di rete IP.

4. I messaggi syslog del livello di debug indicano una richiesta TCP scartata dal dispositivo peer:

<#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. I debug BGP visualizzano il messaggio "no route to peer":

```
<#root>
```

```
fw#
```

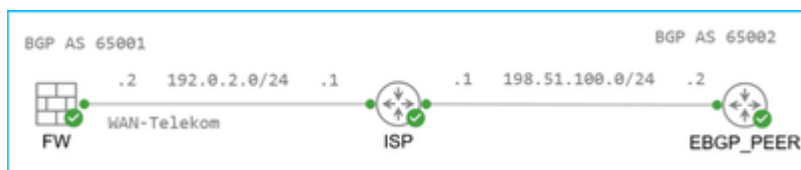
```
debug ip bgp
```

```
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 con FTD 7.4.4 e gestito da Secure Firewall Management Center (FMC). Possono essere interessate anche altre piattaforme hardware e versioni software.
- Il firewall dispone di un percorso statico all'indirizzo del peer tramite l'interfaccia WAN-Telekom connessa al provider di servizi 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
```

- Il firewall dispone della configurazione BGP. Il peer 198.51.100.2 ha un diverso numero di sistema autonomo, quindi è esterno:

```
<#root>
```

```
fw#
```

```
show run router
```

```
router bgp 65001
```

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

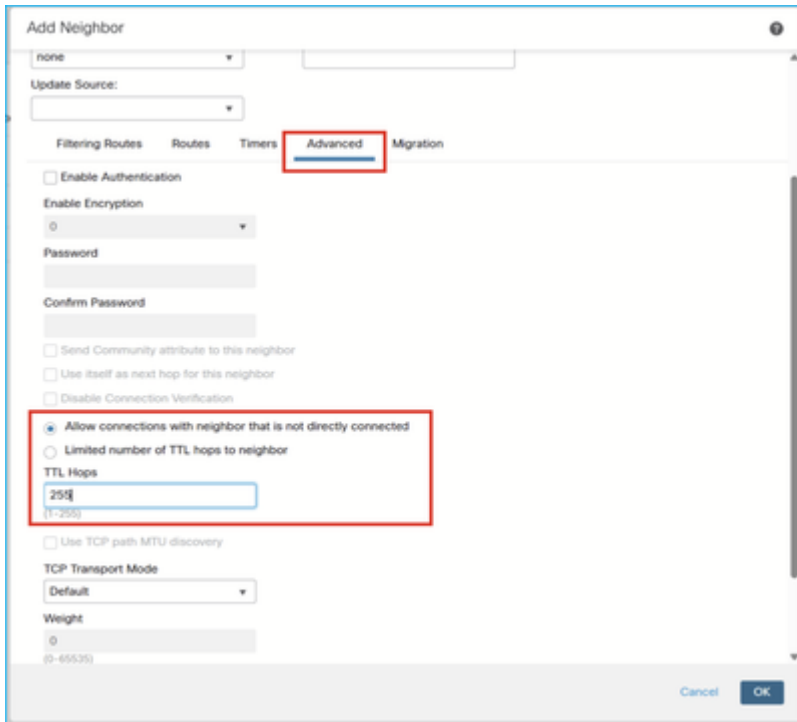
```
neighbor 198.51.100.2 remote-as 65002
```

```
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
```

Risoluzione

L'adiacenza viene stabilita dopo aver abilitato l'opzione Consenti connessioni con router adiacente

non connesso direttamente nella sezione Avanzate della configurazione dei router adiacenti BGP e aver impostato gli hop TTL su 255:



Causa

Per impostazione predefinita, il firewall consente l'adiacenza eBGP tra i peer connessi direttamente, ovvero i peer nella stessa subnet. Per consentire l'adiacenza tra peer non connessi direttamente, è necessario attivare l'opzione Consenti connessioni con router adiacente non connesso direttamente. Inoltre, l'utente può limitare il numero di hop TTL al peer e impostare il valore Time To Live minimo previsto nell'intestazione IP del pacchetto TCP ricevuto dal peer. Il valore predefinito è 1.

Verifica

1. L'opzione Consenti connessioni con router adiacente non connesso direttamente non è configurata:

```
<#root>
```

```
fw#
```

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

External BGP neighbor not directly connected.

2. L'opzione Consenti connessioni con router adiacente non connesso direttamente è configurata e TTL Hops è impostato su 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. L'opzione Consenti connessioni con router adiacente non connesso direttamente è configurata e TTL Hops è impostato su 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.

Contenuto correlato

- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).