

Configurazione di BGP Multipath in Secure Firewall Threat Defense

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Diagramma](#)

[Configurazione BGP](#)

[Configurazione BGP Multipath](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Domande e risposte](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare Border Gateway Protocol (BGP) Multipath in Cisco Secure Firewall Threat Defense.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione BGP su Cisco Secure Firewall Threat Defense (FTD)
- Generale BGP
- Cisco Secure Firewall Management Center (FMC)

Componenti usati

Le informazioni di questo documento si basano sulla seguente versione software e hardware:

- Cisco FTD versione 7.6
- Cisco FMC versione 7.6

Avvertenza: Le reti e gli indirizzi IP menzionati in questo documento non sono associati a singoli utenti, gruppi o organizzazioni. Questa configurazione è stata creata esclusivamente per l'uso in

ambienti lab.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In questo documento viene descritto come configurare la condivisione del carico BGP Multipath in Firepower Threat Defense quando si riceve un percorso alla stessa destinazione da router diversi nello stesso AS (ad esempio, lo stesso ISP).

BGP Multipath consente l'installazione nella tabella di routing IP di più percorsi BGP a costo uguale allo stesso prefisso di destinazione. Il traffico diretto al prefisso di destinazione viene quindi condiviso su tutti i percorsi installati.

Questi percorsi vengono aggiunti alla tabella di routing insieme al percorso migliore per la condivisione del carico. Il protocollo BGP Multipath non influenza il processo di selezione del percorso migliore. Ad esempio, un FTD seleziona ancora un percorso come il migliore in base all'algoritmo e annuncia questo miglior percorso ai suoi peer BGP.

Per essere qualificati come percorsi multipli, i percorsi alla stessa destinazione devono corrispondere al percorso migliore nelle seguenti caratteristiche:

- Peso
- Preferenza locale
- Lunghezza AS-PATH
- Codice origine
- Discriminatore Multi Exit (MED)

Effettuare una delle seguenti operazioni:

- AS o sub-AS adiacente (prima dell'aggiunta di BGP Multipath)
- AS-PATH (dopo l'aggiunta di BGP Multipath)

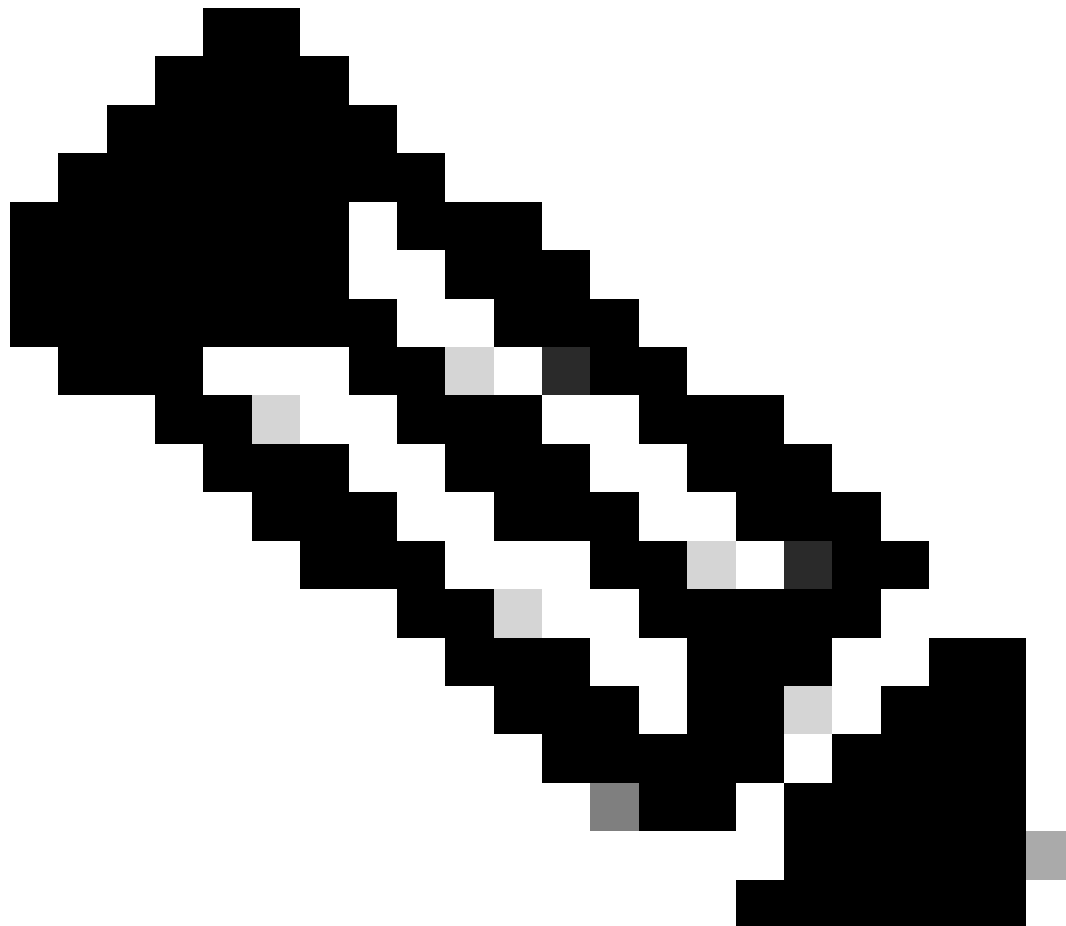
Alcune funzionalità BGP Multipath impongono ulteriori requisiti ai candidati a percorsi multipli:

- Il percorso deve avere origine da un router adiacente esterno o di confederazione (eBGP).
- La metrica IGP per l'hop successivo BGP deve corrispondere alla metrica IGP del percorso migliore.

Per i candidati interni a percorsi multipli BGP (iBGP), si applicano i seguenti requisiti aggiuntivi:

- Il percorso deve essere appreso da un sistema adiacente interno (iBGP).
- La metrica IGP per l'hop successivo BGP deve corrispondere alla metrica IGP dei percorsi migliori, a meno che il router non sia impostato per i percorsi multipli iBGP di costo diseguale.

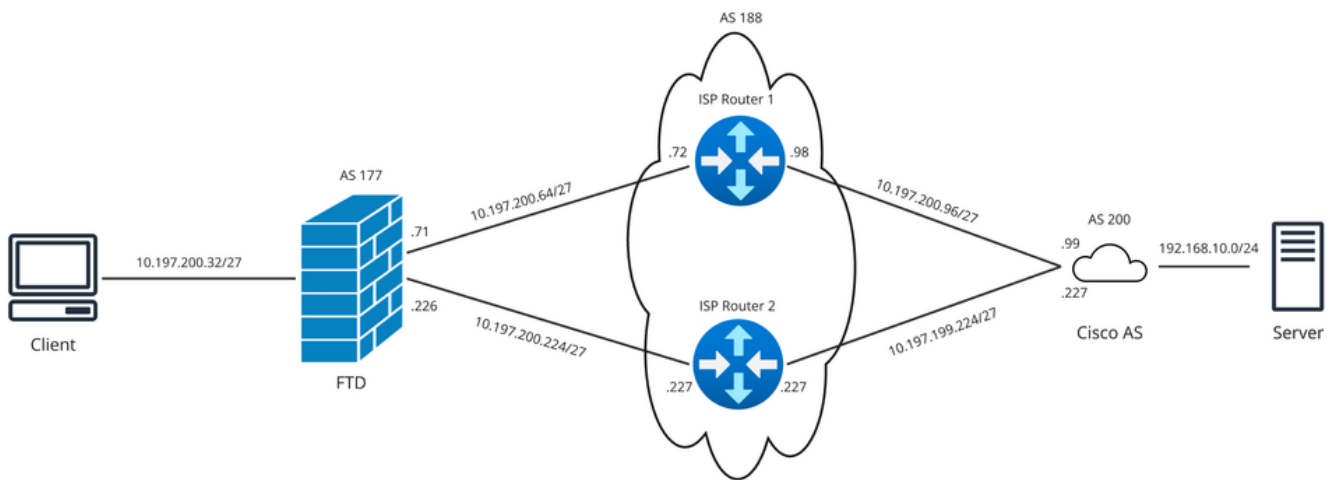
BGP inserisce nella tabella di routing IP n i percorsi ricevuti più di recente dai candidati a percorsi multipli, dove n è il numero di percorsi da installare nella tabella di routing, come specificato quando si configura BGP Multipath. L'intervallo di valori per n è compreso tra 1 e 8 per FTD. Il valore predefinito, quando il multipath è disabilitato, è 1.



Nota: il next-hop-self equivalente viene eseguito sul percorso migliore scelto tra i multipath eBGP prima di essere inoltrato ai peer interni.

Configurazione

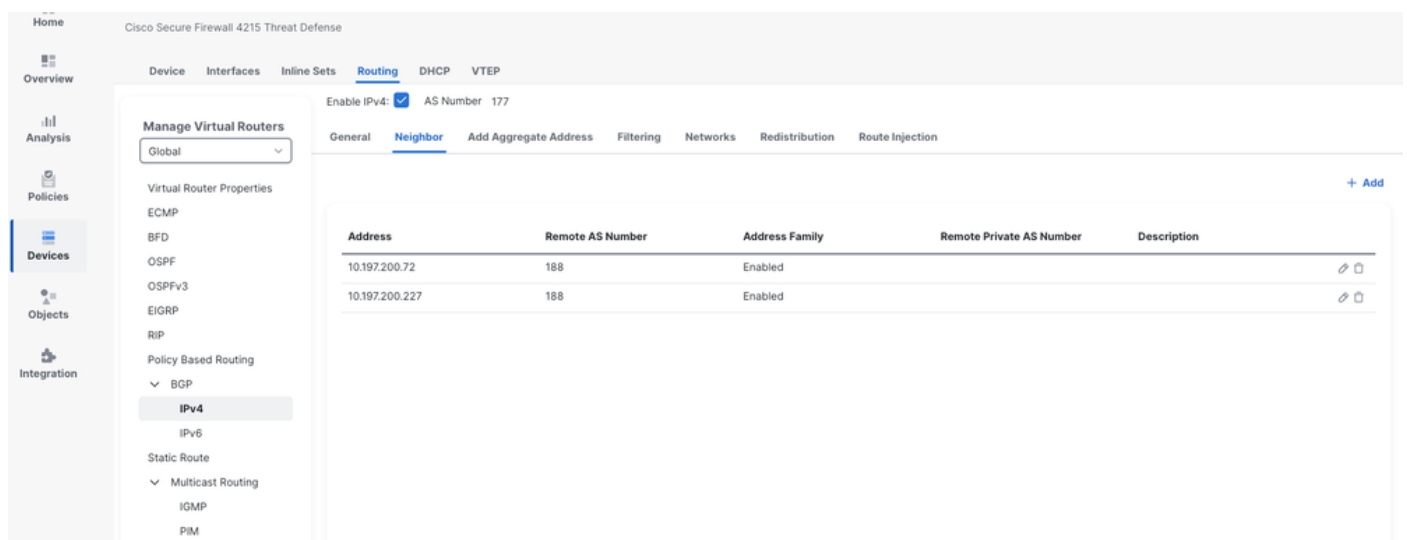
Diagramma



Esempio di rete

Configurazione BGP

Selezionare Dispositivi > Gestione dispositivi > Modifica dispositivo > Routing > BGP > IPv4 per configurare BGP dopo averlo abilitato.



Configurazione BGP

Configurazione BGP da LINA:

```

router bgp 177
  bgp log-neighbor-changes
  bgp router-id 1.1.x.x
  bgp router-id vrf auto-assign
  address-family ipv4 unicast
    neighbor 10.197.200.72 remote-as 188
    neighbor 10.197.200.72 transport path-mtu-discovery disable
    neighbor 10.197.200.72 activate
    neighbor 10.197.200.227 remote-as 188
    neighbor 10.197.200.227 transport path-mtu-discovery disable
    neighbor 10.197.200.227 activate
  no auto-summary
  
```

```
no synchronization
exit-address-family
!
```

Due router BGP adiacenti dallo stesso AS:

```
ftd1# show bgp summary
BGP router identifier 1.1.x.x, local AS number 177
BGP table version is 9, main routing table version 9
2 network entries using 400 bytes of memory
4 path entries using 320 bytes of memory
1/1 BGP path/bestpath attribute entries using 208 bytes of memory
1 BGP AS-PATH entries using 40 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 968 total bytes of memory
BGP activity 4/2 prefixes, 10/6 paths, scan interval 60 secs
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.197.200.72	4	188	67	66	9	0	0	01:10:15	1
10.197.200.227	4	188	60	60	9	0	0	01:00:56	1

Si noti che sono disponibili due route valide ricevute per la stessa rete di destinazione, una per ogni router adiacente.

```
ftd1# show bgp 192.168.10.0 255.255.255.0
BGP routing table entry for 192.168.10.0/24, version 9
Paths: (2 available, best #2, table default)
  Advertised to update-groups: 3
    188 200
      10.197.200.227 from 10.197.200.227 (3.3.x.x)
        Origin incomplete, localpref 100, valid, external
    188 200
      10.197.200.72 from 10.197.200.72 (2.2.x.x)
        Origin incomplete, localpref 100, valid, external, best
```

Il percorso migliore selezionato e installato nella tabella di routing è quello ricevuto dalla versione adiacente 10.197.200.72.

```
ftd1# show route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF
```

Gateway of last resort is not set

B 192.168.10.0 255.255.255.0 [20/0] via 10.197.200.72, 00:01:55

Configurazione BGP Multipath

Configurare BGP multi path in Devices > Device management > Edit Device > Routing > BGP > IPv4 > Edit Forward Packets over Multiple Paths.

The screenshot shows the Cisco Secure Firewall 4215 Threat Defense configuration interface. The left sidebar contains navigation options: Overview, Analysis, Policies, Devices, Objects, and Integration. The main panel is titled 'Cisco Secure Firewall 4215 Threat Defense' and has tabs for Device, Interfaces, Inline Sets, Routing, DHCP, and VTEP. The 'Routing' tab is selected, and the 'General' sub-tab is active. The 'Enable IPv4' checkbox is checked, and the 'AS Number' is 177. The 'Forward Packets Over Multiple Paths' section is highlighted with a red box. It contains two settings: 'Number of Paths' and 'IBGP number of paths', both set to 1.

Setting	Value
Number of Paths	1
IBGP number of paths	1

BGP Multipath in FMC

The screenshot shows the Cisco Secure Firewall 4215 Threat Defense configuration interface. The left sidebar contains navigation options: Overview, Analysis, Policies, Devices, Objects, and Integration. The main panel is titled 'Cisco Secure Firewall 4215 Threat Defense' and has tabs for Device, Interfaces, Inline Sets, Routing, DHCP, and VTEP. The 'Routing' tab is selected, and the 'General' sub-tab is active. The 'Forward Packets Over Multiple Paths' section is highlighted with a red box. A dialog box titled 'Edit Forward packets Over Multiple Paths' is open, showing the 'Number of Paths' field set to 2 and the 'IBGP Number of Paths' field set to 1. The 'OK' button is highlighted.

Setting	Value
Number of Paths	2
IBGP Number of Paths	1

BGP Multipath in FMC

Salvare le modifiche e distribuire.

Verifica

Configurazione BGP da LINA dopo l'abilitazione di multipath:

<#root>

```
ftd1# sh run router
router bgp 177
bgp log-neighbor-changes
bgp router-id 1.1.x.x
bgp router-id vrf auto-assign
address-family ipv4 unicast
neighbor 10.197.200.72 remote-as 188
neighbor 10.197.200.72 transport path-mtu-discovery disable
neighbor 10.197.200.72 activate
neighbor 10.197.200.227 remote-as 188
neighbor 10.197.200.227 transport path-mtu-discovery disable
neighbor 10.197.200.227 activate
```

maximum-paths 2

```
no auto-summary
no synchronization
exit-address-family
```

Si noti che la m precede una delle route che indicano percorsi multipli

<#root>

```
ftd1# show bgp
```

```
BGP table version is 11, local router ID is 1.1.x.x
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
Network Next Hop Metric LocPrf Weight Path
```

```
*m 192.168.10.0 10.197.200.227 0 188 200 ?
```

```
*> 10.197.200.72 0 188 200 ?
```

```
ftd1# show bgp 192.168.10.0 255.255.255.0
BGP routing table entry for 192.168.10.0/24, version 11
Paths: (2 available, best #2, table default)
Multipath: eBGP
Advertised to update-groups: 3
188 200
10.197.200.227 from 10.197.200.227 (3.3.x.x)
Origin incomplete, localpref 100, valid, external,
```

multipath

```
188 200
10.197.200.72 from 10.197.200.72 (2.2.x.x)
Origin incomplete, localpref 100, valid, external,
```

multipath

, best

Si noti che ora nella tabella di routing sono installate due route alla stessa destinazione dopo l'abilitazione del multipath BGP.

<#root>

```
ftd1# show route bgp
```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, + - replicated route

SI - Static InterVRF

Gateway of last resort is not set

```
B 192.168.10.0 255.255.255.0 [20/0] via 10.197.200.227, 00:01:17
```

```
[20/0] via 10.197.200.72, 00:01:17
```

Risoluzione dei problemi

1. Verificare la configurazione BGP:

Utilizzare il comando `show bgp` per controllare la tabella BGP e verificare che più percorsi siano contrassegnati come `multipat`.

Confermare che Numero di percorsi sia configurato per consentire più percorsi.

2. Controllare gli attributi del percorso:

Verificare che i percorsi dispongano degli stessi attributi BGP richiesti per i percorsi multipli; ad esempio spessore, preferenza locale, lunghezza percorso AS e così via.

3. Verifica della condivisione del carico:

Utilizzare il comando `show route` per verificare che i percorsi siano utilizzati per la condivisione del carico. L'output deve mostrare più percorsi per la stessa destinazione.

Domande e risposte

1. Il comando `bgp bestpath as-path multipath-relax` è supportato in FTD tramite Flex config per la condivisione del carico?

No, è già presente un miglioramento per il supporto di questa funzionalità in FTD/ASA. ID bug Cisco [CSCvw1654](#)

Informazioni correlate

[Risoluzione dei problemi comuni di BGP](#)

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).