Esempio di configurazione di FlexVPN Spoke in un hub ridondante con un approccio a doppio cloud

Sommario

Introduzione

Questo documento descrive come configurare un spoke in una rete FlexVPN con l'uso del blocco di configurazione client FlexVPN in uno scenario in cui sono disponibili più hub.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- FlexVPN
- Protocolli di routing Cisco

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie G2 Integrated Service Router (ISR)
- Cisco IOS® versione 15.2M

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.

Configurazione

Per motivi di ridondanza, un spoke potrebbe dover connettersi a più hub. La ridondanza sul lato spoke consente il funzionamento continuo senza un singolo punto di errore sul lato hub.

I due progetti di hub ridondanti FlexVPN più comuni che utilizzano la configurazione spoke sono:

- **Approccio basato su cloud doppio**, in cui un spoke dispone di due tunnel separati attivi a entrambi gli hub in qualsiasi momento.
- **Approccio di failover**, in cui un spoke ha un tunnel attivo con un hub in un determinato point in time.

Entrambi gli approcci hanno un insieme unico di pro e contro.

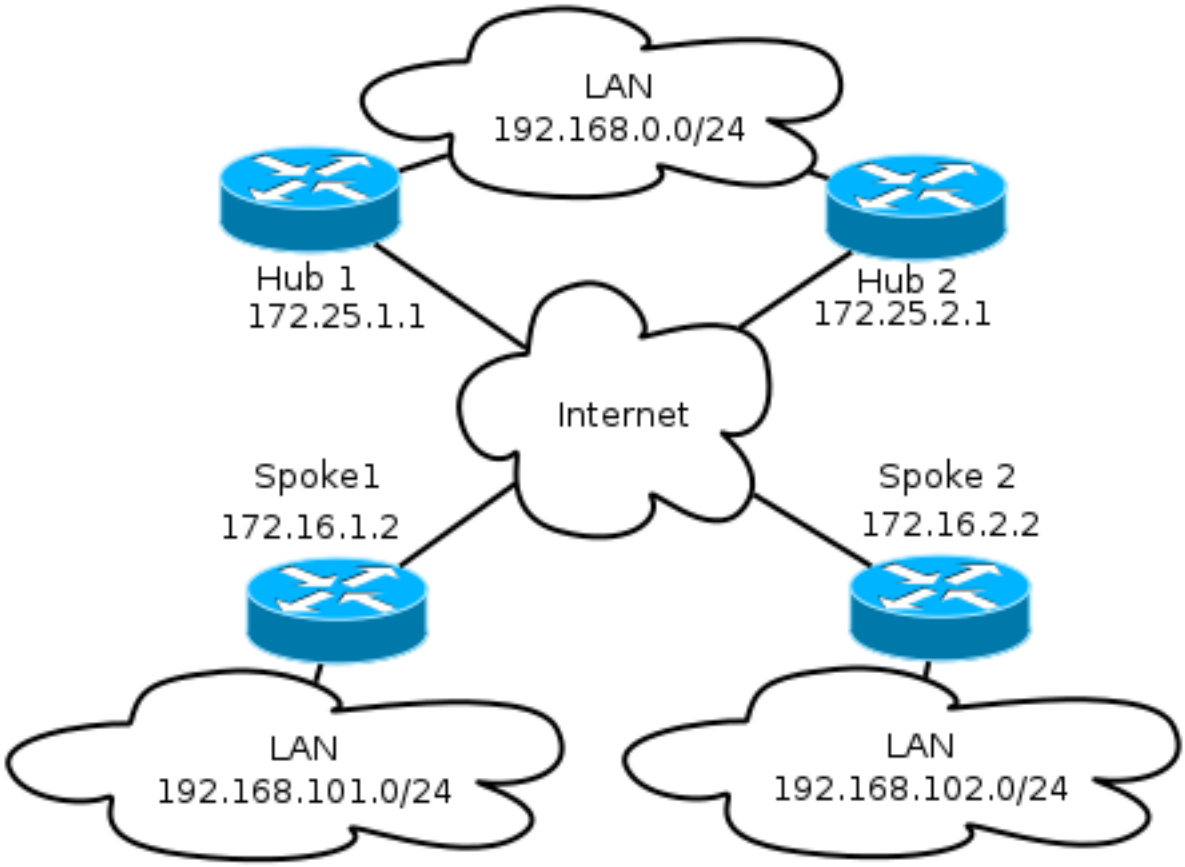
Approccio	Pro	Svantaggi
Cloud doppio	• Ripristino più rapido in caso di guasto, in base ai timer del protocollo di routing • Più possibilità di distribuire il traffico tra gli hub, poiché la connessione a entrambi gli hub è attiva	• Spoke mantiene la sessione su entrambi g hub contemporaneamente, consumando l risorse su entrambi gli hub
Failover	• Configurazione semplice - integrata in FlexVPN • Non si basa sul protocollo di routing in caso di errore	• Tempi di ripristino più lenti, basati su Deac Peer Detection (DPD) o (facoltativamente) Object Tracking • Tutto il traffico è costretto a viaggiare su u hub alla volta.

Questo documento descrive il primo approccio. L'approccio a questa configurazione è simile a quello della configurazione DMVPN (Dynamic Multipoint VPN) con doppio cloud. La configurazione di base di Hub and Spoke si basa sui documenti di migrazione da DMVPN a FlexVPN. Fare riferimento alla migrazione di FlexVPN: Articolo Hard Move from DMVPN to FlexVPN on Same Devices (Spostamento rapido da DMVPN a FlexVPN sugli stessi dispositivi) per una descrizione di questa configurazione.

Esempio di rete

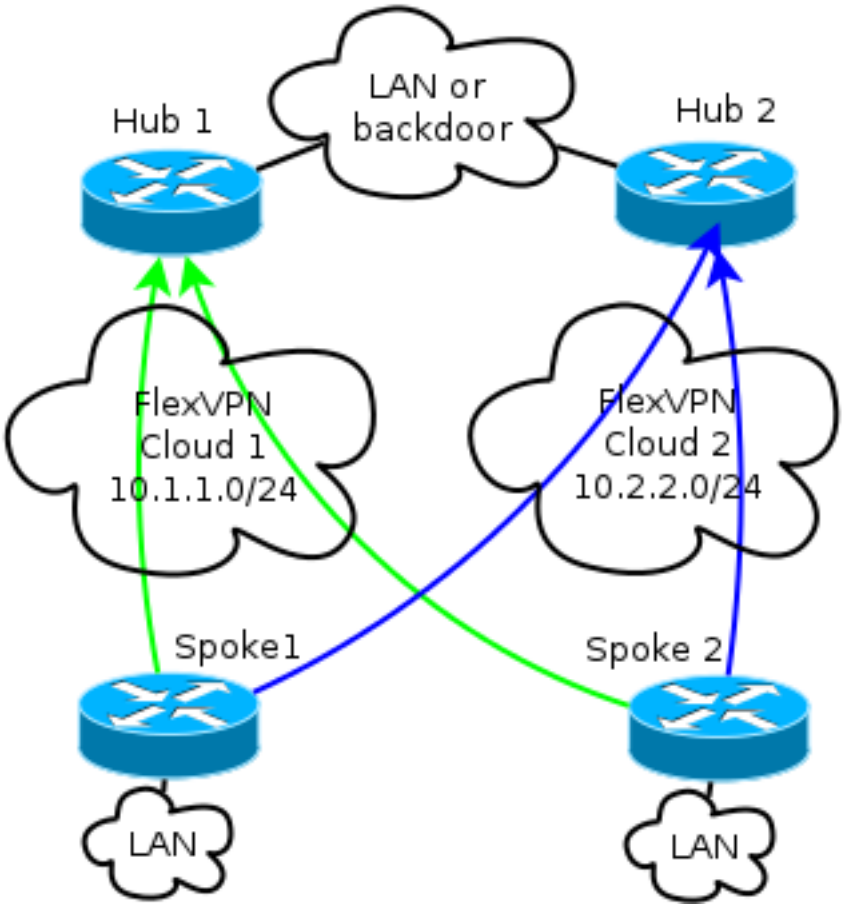
Transport Network

Il diagramma mostra la rete di trasporto di base generalmente utilizzata nelle reti FlexVPN.



Sovrapponi rete

Nel diagramma viene illustrata la rete sovrapposta con connettività logica che illustra il funzionamento del failover. Durante il normale funzionamento, il raggio 1 e il raggio 2 mantengono una relazione con entrambi gli hub. In caso di errore, il protocollo di routing passa da un hub all'altro.



Nota: Nel diagramma, le linee verdi indicano la connessione e la direzione delle sessioni di Internet Key Exchange versione 2 (IKEv2)/Flex all'hub 1, mentre le linee blu indicano la connessione all'hub 2.

Entrambi gli hub mantengono indirizzi IP separati in cloud sovrapposti. L'indirizzamento **/24** rappresenta il pool di indirizzi allocati per questo cloud, non l'indirizzamento effettivo dell'interfaccia. Infatti, in genere, l'hub FlexVPN alloca un indirizzo IP dinamico per l'interfaccia spoke e si basa sulle route inserite in modo dinamico tramite i comandi route nel blocco di autorizzazione FlexVPN.

Configurazioni spoke

Configurazione interfaccia tunnel spoke

La configurazione tipica utilizzata in questo esempio è semplicemente due interfacce tunnel con due indirizzi di destinazione separati.

```
interface Tunnel1
ip address negotiated
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
```

```
tunnel destination 172.25.1.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default

interface Tunnel2
ip address negotiated
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel destination 172.25.2.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

Per consentire la corretta formazione dei tunnel spoke, è necessario un modello virtuale (VT, Virtual Template).

```
interface Virtual-Template1 type tunnel
ip unnumbered ethernet1/0
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

Lo spoke utilizza un'interfaccia senza numero che indica l'interfaccia LAN nel VRF (Virtual Routing and Forwarding), che in questo caso è globale. Tuttavia, potrebbe essere preferibile fare riferimento a un'interfaccia di loopback. Questo perché le interfacce di loopback rimangono online in quasi tutte le condizioni.

Configurazione Spoke Border Gateway Protocol (BGP)

Poiché Cisco consiglia iBGP come protocollo di routing da utilizzare nella rete di overlay, questo documento menziona solo questa configurazione.

> **Nota:** Gli spoke devono mantenere la raggiungibilità BGP a entrambi gli hub.

```
router bgp 65001
bgp log-neighbor-changes
network 192.168.101.0
neighbor 10.1.1.1 remote-as 65001
neighbor 10.1.1.1 fall-over
neighbor 10.2.2.1 remote-as 65001
neighbor 10.2.2.1 fall-over
```

FlexVPN in questa configurazione non dispone di un concetto di hub primario o secondario. L'amministratore decide se il protocollo di routing preferisce un hub a un altro oppure, in alcuni scenari, esegue il bilanciamento del carico.

Considerazioni su failover e convergenza spoke

Per ridurre al minimo il tempo necessario affinché un spoke rilevi il guasto, utilizzate questi due metodi tipici.

- Abbreviare i timer BGP. Il tempo di attesa predefinito causa il failover.
- Configurare il failover BGP, descritto in questo articolo, Supporto BGP per la disattivazione rapida della sessione di peering.
- Non utilizzare il rilevamento inoltro bidirezionale (BFD), poiché non è consigliato nella maggior parte delle distribuzioni FlexVPN.

Tunnel e failover spoke-to-spoke

I tunnel spoke utilizzano la commutazione rapida NHRP (Next Hop Resolution Protocol). Cisco IOS indica che tali collegamenti sono route NHRP, ad esempio:

```
Spoke1#show ip route nhrp
(...)

192.168.102.0/24 is variably subnetted, 2 subnets, 2 masks
H 192.168.102.0/24 [250/1] via 10.2.2.105, 00:00:21, Virtual-Access1
```

Queste route non scadono quando scade la connessione BGP; al contrario, vengono trattenute per un periodo di sospensione NHRP, che per impostazione predefinita è di due ore. Ciò significa che i tunnel spoke attivi rimangono in funzione anche in caso di guasto.

Configurazioni hub

Pool locali

Come indicato nella sezione **Diagramma reticolare**, entrambi gli hub mantengono indirizzi IP separati.

Hub1

```
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

Hub2

```
ip local pool FlexSpokes 10.2.2.100 10.2.2.254
```

Configurazione BGP hub

La configurazione BGP dell'hub rimane simile agli esempi precedenti.

Questo output viene generato dall'hub 1 con indirizzo IP LAN **192.168.0.1**.

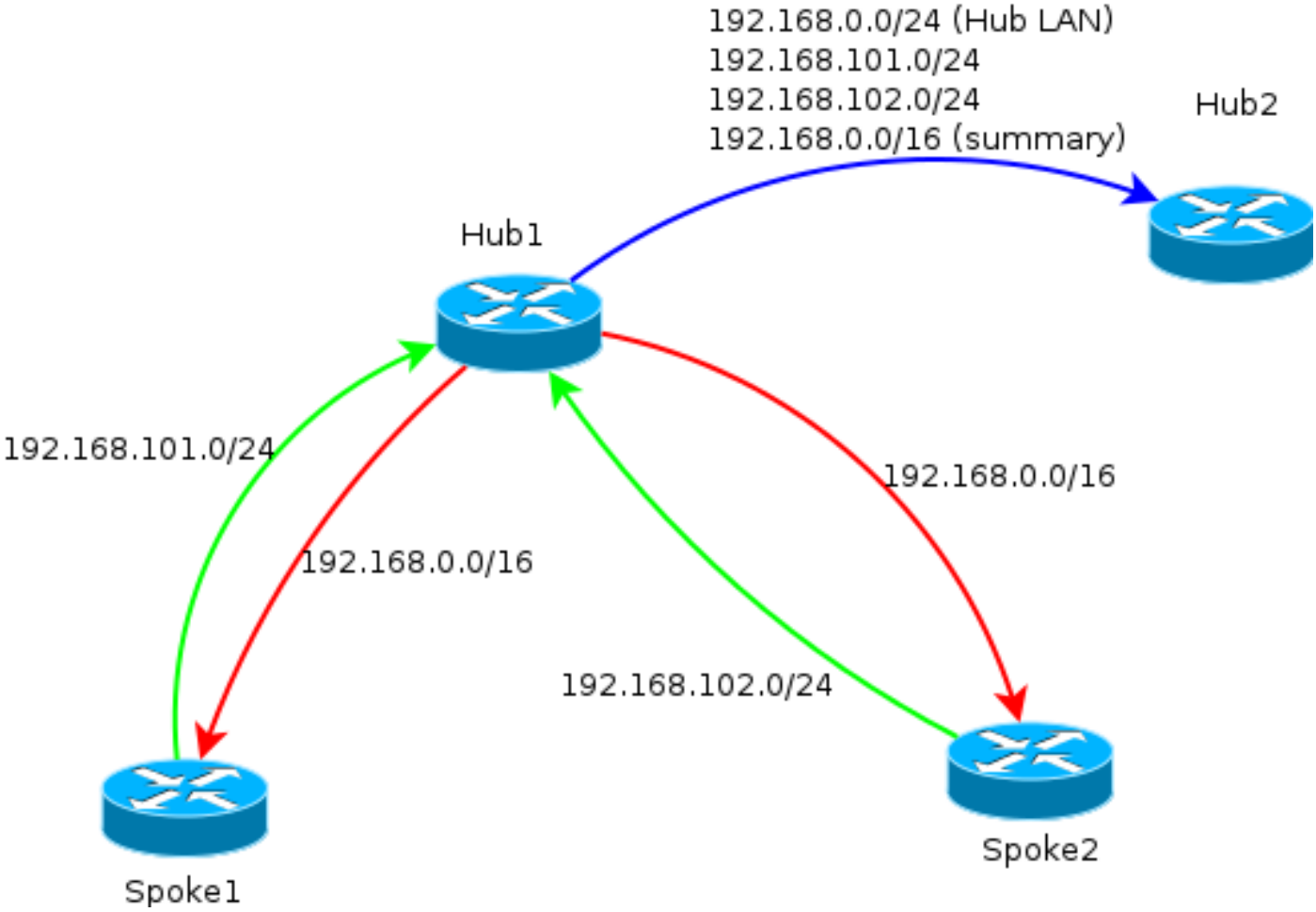
```
router bgp 65001
bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
network 192.168.0.0
aggregate-address 192.168.0.0 255.255.0.0 summary-only
neighbor Spokes peer-group
neighbor Spokes remote-as 65001
neighbor Spokes fall-over
```

```
neighbor 192.168.0.2 remote-as 65001
neighbor 192.168.0.2 route-reflector-client
neighbor 192.168.0.2 next-hop-self all
neighbor 192.168.0.2 unsuppress-map ALL

route-map ALL permit 10
match ip address 1

ip access-list standard 1
permit any
```

In sostanza, questo è ciò che viene fatto:

- Il pool di indirizzi FlexVPN locale è incluso nell'intervallo di ascolto BGP.
- La rete locale è 192.168.0.0/24.
- Un riepilogo viene pubblicizzato solo per i raggi. La configurazione dell'indirizzo di aggregazione crea una route statica per il prefisso tramite l'interfaccia null0, ovvero una route da ignorare utilizzata per impedire i loop di routing.
- Tutti i prefissi specifici vengono annunciati all'altro hub. Poiché è anche una connessione iBGP, richiede una configurazione del router-reflector.

Questo diagramma rappresenta lo scambio di prefissi BGP tra spoke e hub in un cloud FlexVPN.



Nota: Nel diagramma, la linea verde rappresenta le informazioni fornite dagli spoke all'hub, la linea rossa rappresenta le informazioni fornite da ciascun hub agli spoke (solo un riepilogo) e la linea blu rappresenta i prefissi scambiati tra gli hub.

Verifica

Poiché ogni spoke mantiene l'associazione con entrambi gli hub, con il comando **show crypto ikev2 sa** vengono visualizzate due sessioni IKEv2.

```
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
3 172.16.1.2/500 172.16.2.2/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3147 sec

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.1.2/500 172.25.2.1/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3256 sec
```

Per visualizzare le informazioni sul protocollo di routing, immettere questi comandi:

```
show bgp ipv4 unicast

show bgp summary
```

Sugli spoke, il prefisso di riepilogo viene ricevuto dagli hub e le connessioni a entrambi gli hub sono attive.

```
Spoke1#show bgp ipv4 unicast
BGP table version is 4, local router ID is 192.168.101.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
*>i 192.168.0.0/16 10.1.1.1 0 100 0 i
* i 10.2.2.1 0 100 0 i
*> 192.168.101.0 0.0.0.0 0 32768 i
Spoke1#show bgp summa
Spoke1#show bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
BGP table version is 4, main routing table version 4
2 network entries using 296 bytes of memory
3 path entries using 192 bytes of memory
3/2 BGP path/bestpath attribute entries using 408 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 896 total bytes of memory
BGP activity 2/0 prefixes, 3/0 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 7 7 4 0 0 00:00:17 1
10.2.2.1 4 65001 75 72 4 0 0 01:02:24 1
```

Risoluzione dei problemi

I principali blocchi da risolvere sono due:

- IKE (Internet Key Exchange)
- IPsec (Internet Protocol Security)

Di seguito sono riportati i comandi show rilevanti:

```
show crypto ipsec sa

show crypto ikev2 sa
```

Di seguito sono riportati i comandi di debug pertinenti:

```
debug crypto ikev2 [internal|packet]

debug crypto ipsec

debug vtemplate event
```

Di seguito è riportato il protocollo di routing desiderato:

```
show bgp ipv4 unicast (or show ip bgp)

show bgp summary
```