Esempio di configurazione del blocco client FlexVPN Spoke in un hub ridondante con FlexVPN

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.

Premesse

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 le connessioni a entrambi gli hub sono attive	• Spoke mantiene la sessione su entrambi hub contemporaneamente, consumando 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 Dea Peer Detection (DPD) o (facoltativamente Object Tracking • Tutto il traffico deve necessariamente passare a un hub alla volta

Questo documento descrive il secondo approccio.

Configurazione

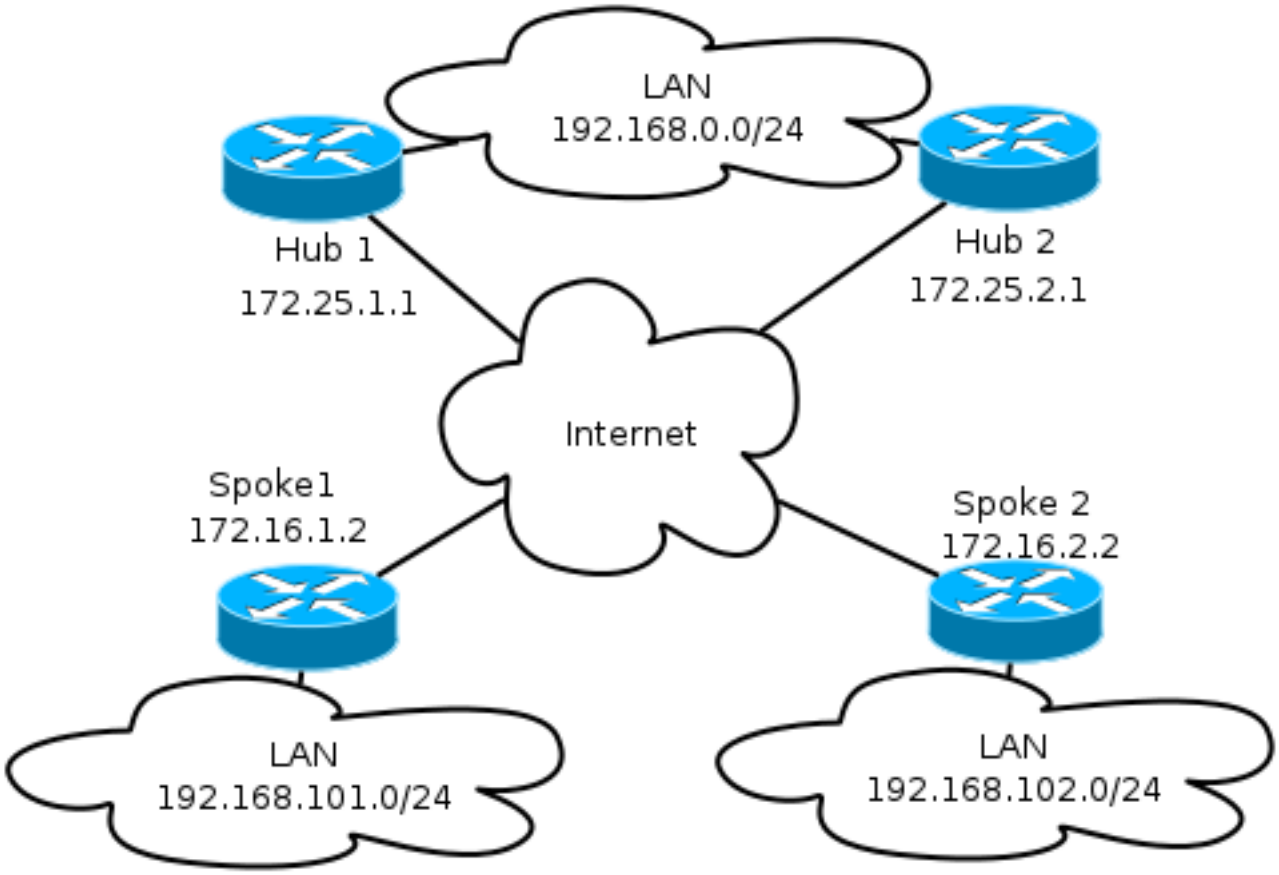
Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Diagrammi di rete

Questi diagrammi mostrano i diagrammi della topologia di trasporto e sovrapposizione.

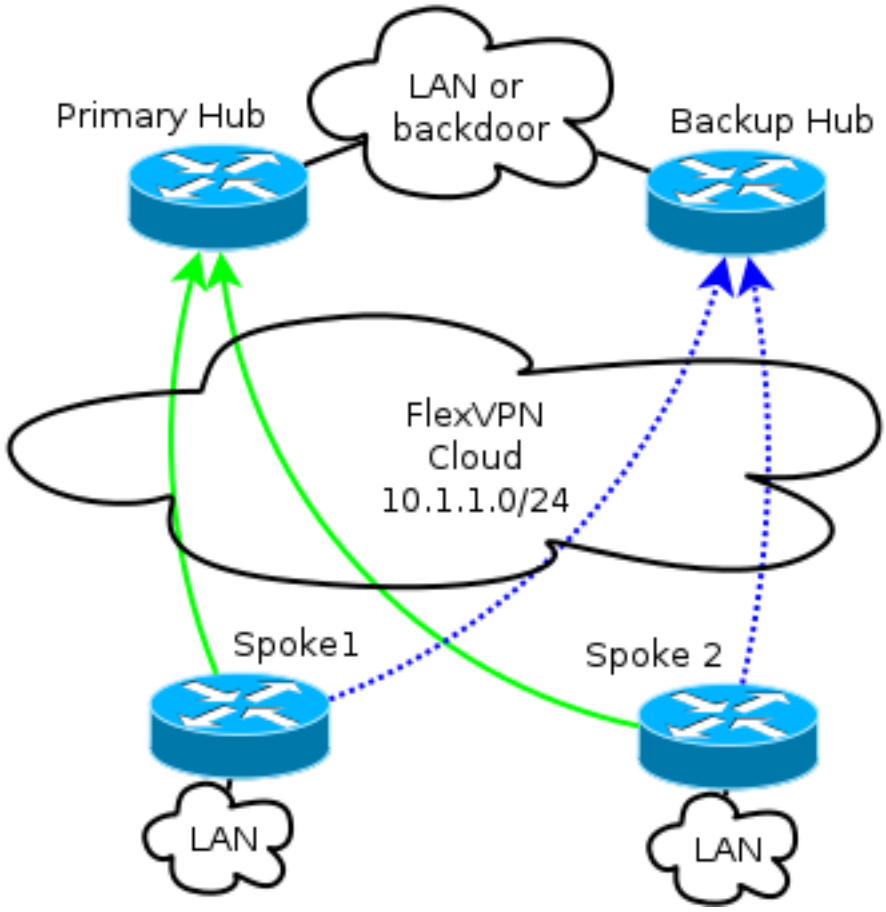
Transport Network

Il diagramma mostra la rete di trasporto di base che viene in genere utilizzata nelle reti FlexVPN.



Sovrapponi rete

In questo 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 un solo hub.



Nota: Nel diagramma, le linee verdi continue indicano la connessione e la direzione delle sessioni primarie IKEv2 (Internet Key Exchange versione 2)/Flex, mentre le linee blu tratteggiate indicano la connessione di backup in caso di errore della sessione IKE (Internet Key Exchange) all'hub primario.

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.

Configurazione di base di spoke e hub

La configurazione di base di Hub and Spoke si basa sui documenti di migrazione da DMVPN (Dynamic Multipoint VPN) a FlexVPN. Questa configurazione è descritta nella sezione Migrazione FlexVPN: Articolo Hard Move da DMVPN a FlexVPN sullo stesso dispositivo.

Regolazione configurazione spoke

Configurazione spoke - Blocco configurazione client

La configurazione spoke deve essere estesa dal blocco di configurazione client.

Nella configurazione di base vengono specificati più peer. Il peer con la preferenza più alta

(numero più basso) viene considerato prima degli altri.

```
crypto ikev2 client flexvpn Flex_Client
peer 1 172.25.1.1
peer 2 172.25.2.1
client connect Tunnel1
```

La configurazione del tunnel deve essere modificata per consentire la scelta dinamica della destinazione del tunnel, in base al blocco di configurazione del client FlexVPN.

```
interface Tunnel1
 tunnel destination dynamic
```

Èfondamentale ricordare che il blocco di configurazione del client FlexVPN è collegato a un'interfaccia e non a IKEv2 o al profilo IPsec (Internet Protocol Security).

Il blocco di configurazione del client fornisce diverse opzioni per regolare il tempo di failover e le operazioni, tra cui la registrazione dell'utilizzo degli oggetti, il dial backup e le funzionalità dei gruppi di backup.

Nella configurazione di base, lo spoke si basa sulle DPD per rilevare se un spoke non risponde, e attiva una modifica una volta che il peer è dichiarato morto. L'opzione di utilizzare DPD non è veloce, a causa di come funziona DPD. Un amministratore potrebbe voler migliorare la configurazione con il tracciamento degli oggetti o con miglioramenti simili.

Per ulteriori informazioni, fare riferimento al capitolo **FlexVPN Client Configuration** della guida alla configurazione di Cisco IOS, collegata alla sezione **Informazioni correlate** alla fine di questo documento.

Configurazione completa - Riferimento

```
crypto logging session

crypto ikev2 keyring Flex_key
 peer Spokes
 address 0.0.0.0 0.0.0.0
 pre-shared-key local cisco
 pre-shared-key remote cisco

crypto ikev2 profile Flex_IKEv2
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local Flex_key
 aaa authorization group psk list default default
 virtual-template 1

crypto ikev2 dpd 30 5 on-demand

crypto ikev2 client flexvpn Flex_Client
 peer 1 172.25.1.1
 peer 2 172.25.2.1
 client connect Tunnel1

crypto ipsec transform-set IKEv2 esp-gcm
 mode transport
```

```
crypto ipsec profile default
 set ikev2-profile Flex_IKEv2

interface Tunnel1
 description FlexVPN tunnel
 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
 delay 2000
 tunnel source Ethernet0/0
 tunnel destination dynamic
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
```

Configurazione hub

Anche se la maggior parte della configurazione dell'hub rimane invariata, è necessario considerare diversi aspetti. La maggior parte di essi riguarda una situazione in cui uno o più raggi sono collegati a un hub, mentre altri rimangono in relazione a un altro hub.

Indirizzi spoke

Poiché gli spoke ottengono indirizzi IP dagli hub, in genere si desidera che gli hub assegnino indirizzi da subnet diverse o da una parte diversa di una subnet.

Ad esempio:

Hub1

```
ip local pool FlexSpokes 10.1.1.100 10.1.1.175
```

Hub2

```
ip local pool FlexSpokes 10.1.1.176 10.1.1.254
```

Ciò impedisce la creazione di sovrapposizioni, anche se gli indirizzi non sono instradati all'esterno del cloud FlexVPN, il che potrebbe compromettere la risoluzione dei problemi.

Indirizzo sovrapposto hub

Entrambi gli hub possono mantenere lo stesso indirizzo IP su un'interfaccia basata su un modello virtuale. in alcuni casi, tuttavia, ciò può influire sulla risoluzione dei problemi. Questa scelta di progettazione semplifica l'installazione e la pianificazione, in quanto lo spoke deve avere un solo indirizzo peer per Border Gateway Protocol (BGP).

In alcuni casi, potrebbe non essere desiderato o necessario.

Routing

Ènecessario che gli hub scambino informazioni sui raggi collegati.

Gli hub devono essere in grado di scambiare i percorsi specifici dei dispositivi connessi e continuare a fornire un riepilogo agli spoke.

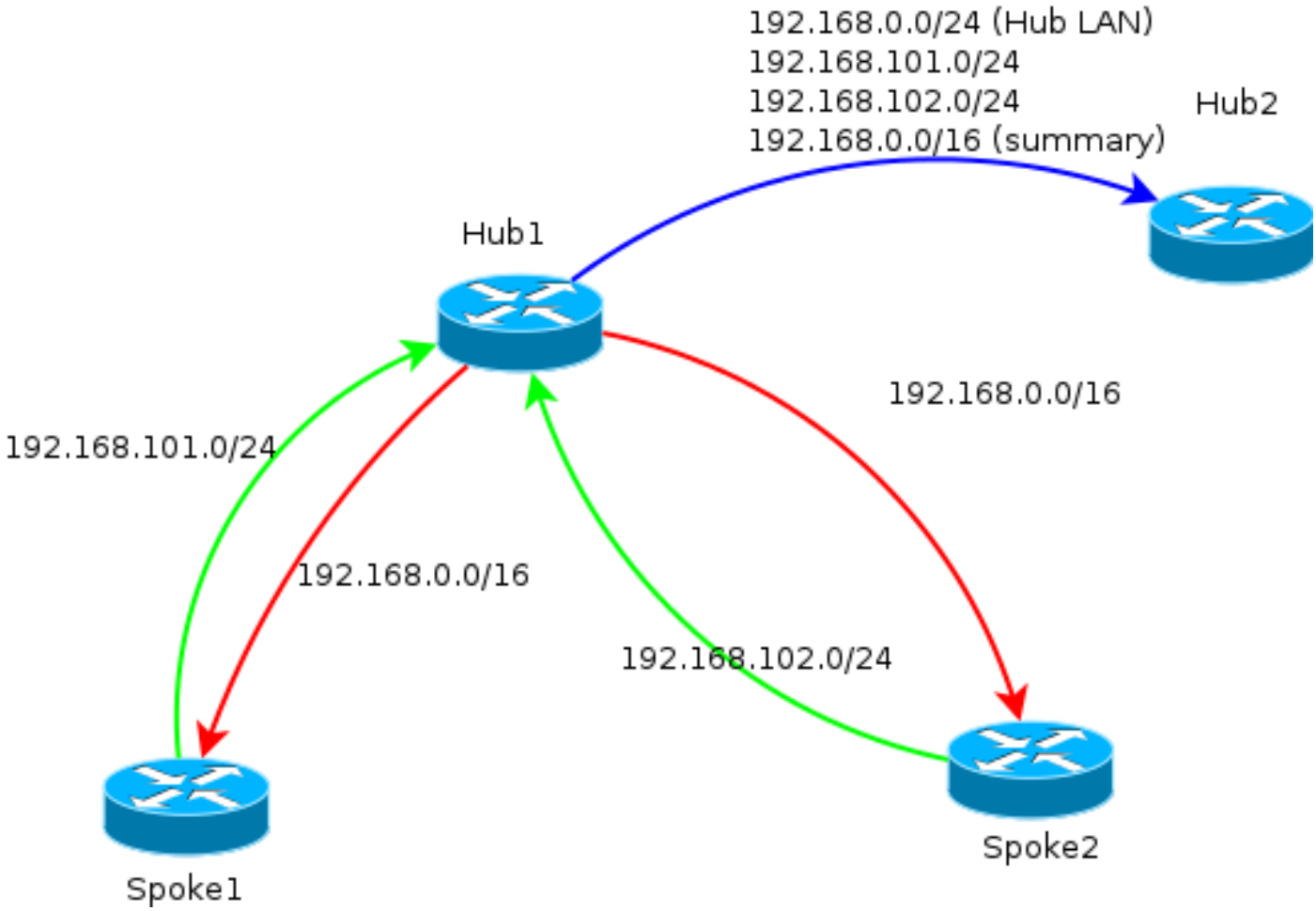
Poiché Cisco consiglia di utilizzare iBGP con FlexVPN e DMVPN, viene mostrato solo il protocollo di routing.

```
bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
network 192.168.0.0
neighbor Spokes peer-group
neighbor Spokes remote-as 65001
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

access-list 1 permit any

route-map ALL permit 10
match ip address 1
```

Questa configurazione consente:

- Listener dinamico dagli indirizzi assegnati agli spoke
- Rete pubblicitaria di 192.168.0.0/24
- Percorso di riepilogo pubblicità di 192.168.0.0/16 per tutti i raggi. La configurazione dell'indirizzo di aggregazione crea una route statica per il prefisso tramite l'interfaccia null0, ovvero una route di eliminazione utilizzata per impedire loop di routing.
- Inoltro di prefissi specifici all'altro hub
- Client di Route-reflector per garantire che gli hub si scambino le informazioni apprese dagli spoke

Questo diagramma rappresenta lo scambio di prefissi in BGP in questa configurazione, dal punto di vista di uno degli hub.



Nota: In questo 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.

Uso dei riepiloghi di rete

In alcuni scenari i riepiloghi potrebbero non essere applicabili o desiderati. Prestare attenzione quando si designa l'IP di destinazione nei prefissi, in quanto iBGP non sostituisce l'hop successivo per impostazione predefinita.

I riepiloghi sono consigliati nelle reti che cambiano spesso lo stato. Ad esempio, connessioni Internet instabili potrebbero richiedere riepiloghi per: evitare la rimozione e l'aggiunta di prefissi, limitare il numero di aggiornamenti e consentire la corretta scalabilità della maggior parte delle impostazioni.

Tunnel spoke-to-spoke

Nello scenario e nella configurazione menzionati nella sezione precedente, gli spoke su hub diversi non sono in grado di stabilire tunnel spoke diretti. Il traffico tra i raggi collegati a diversi hub passa attraverso i dispositivi centrali.

Per risolvere questo problema, è disponibile una soluzione semplice. Tuttavia, è necessario che tra gli hub sia abilitato il protocollo NHRP (Next Hop Resolution Protocol) con lo stesso ID di rete.

A tale scopo, ad esempio, è possibile creare un tunnel GRE (Generic Routing Encapsulation) point-to-point tra gli hub. IPsec non è richiesto.

Verifica

Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi show. Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

Il comando **show crypto ikev2 sa** informa l'utente sulla connessione corrente del raggio.

Il comando **show crypto ikev2 client flexvpn** consente a un amministratore di comprendere lo stato corrente dell'operazione del client FlexVPN.

```
Spoke2# show crypto ikev2 client flexvpn

Profile : Flex_Client
Current state:ACTIVE
Peer : 172.25.1.1
Source : Ethernet0/0
ivrf : IP DEFAULT
fvrf : IP DEFAULT
Backup group: Default
Tunnel interface : Tunnel1
Assigned IP address: 10.1.1.111
```

Se il failover con la configurazione **show logging** ha esito positivo, l'output viene registrato nel dispositivo spoke:

```
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is DOWN.  Peer 172.25.1.1:500
Id: 172.25.1.1
%FLEXVPN-6-FLEXVPN_CONNECTION_DOWN: FlexVPN(Flex_Client) Client_public_addr =
172.16.2.2 Server_public_addr = 172.25.1.1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is UP.  Peer 172.25.2.1:500
Id: 172.25.2.1
%FLEXVPN-6-FLEXVPN_CONNECTION_UP: FlexVPN(Flex_Client) Client_public_addr =
172.16.2.2 Server_public_addr = 172.25.2.1 Assigned_Tunnel_v4_addr = 10.1.1.177
```

In questo output, lo spoke si disconnette dall'**hub 172.25.1.1**, il blocco di configurazione del client Flex_Client rileva un errore e forza una connessione a **172.25.2.1** dove arriva un tunnel e a uno spoke viene assegnato un IP di **10.1.1.177**.

Risoluzione dei problemi

Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi show. Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

> **Nota:** consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug.**

Di seguito sono riportati i comandi di debug pertinenti:

- **debug crypto ikev2**
- **raggio di debug**

Informazioni correlate

- Guida alla configurazione di FlexVPN e Internet Key Exchange versione 2, Cisco IOS release 15 M e T
- Documentazione e supporto tecnico – Cisco Systems