Esempio di configurazione della migrazione soft da DMVPN a FlexVPN

Sommario

Introduzione

In questo documento viene descritto come eseguire una migrazione *soft* in cui sia DMVPN (Dynamic Multipoint VPN) che FlexVPN funzionano su un dispositivo contemporaneamente senza la necessità di una soluzione alternativa e viene fornito un esempio di configurazione.

> **Nota:** Questo documento approfondisce i concetti descritti in Migrazione FlexVPN: Spostamento rapido da DMVPN a FlexVPN sugli stessi dispositivi e migrazione FlexVPN: Spostamento rapido da DMVPN a FlexVPN su un hub diverso articoli di Cisco. Entrambi i documenti descrivono le migrazioni *complesse*, che causano alcune interruzioni al traffico durante la migrazione. Le limitazioni di questi articoli sono dovute a una carenza del

software Cisco IOS® che è stata ora corretta.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- DMVPN
- FlexVPN

Componenti usati

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

- Cisco Integrated Service Router (ISR) versione 15.3(3)M o successive
- Cisco serie 1000 Aggregated Service Router (ASR1K) release 3.10 o successive

Nota: Non tutti i componenti software e hardware supportano Internet Key Exchange versione 2 (IKEv2). Per informazioni, consultare Cisco Feature Navigator.

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

Uno dei vantaggi della nuova piattaforma e del nuovo software Cisco IOS è la capacità di utilizzare la crittografia di nuova generazione. Un esempio è l'uso di Advanced Encryption Standard (AES) in modalità Galois/Counter (GCM) per la crittografia in IPSec, come descritto nella RFC 4106. AES GCM consente velocità di crittografia molto più elevate su alcuni componenti hardware.

Nota: Per ulteriori informazioni sull'utilizzo della crittografia di nuova generazione e sulla migrazione a tale sistema, fare riferimento all'articolo di Cisco sulla crittografia di nuova generazione.

Configurazione

Questo esempio di configurazione è incentrato su una migrazione da una configurazione DMVPN fase 3 a una FlexVPN, poiché entrambe le progettazioni funzionano in modo simile.

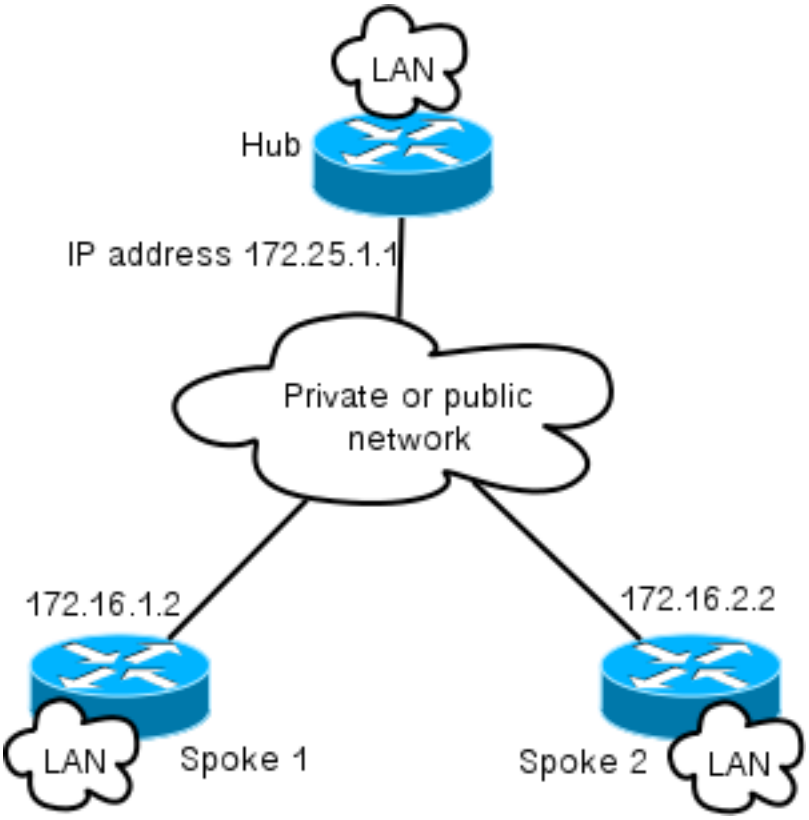
	DMVPN fase 2	DMVPN fase 3	FlexVPN
Trasporto	GRE over IPsec	GRE over IPsec	GRE over IPse
Utilizzo NHRP	Registrazione e risoluzione	Registrazione e risoluzione	Risoluzione
Hop successivo da spoke	Altri raggi o hub	Riepilogo da hub	Riepilogo da hu
NHRP Shortcut Switching	No	Sì	Sì (facoltativo)
Reindirizzamento NHRP	No	Sì	Sì
IKE e IPsec	IPsec Facoltativo, IKEv1 Tipico	IPsec Facoltativo, IKEv1 Tipico	IPsec, IKEv2

Diagrammi di rete

In questa sezione vengono forniti diagrammi di rete di trasporto e sovrapposizione.

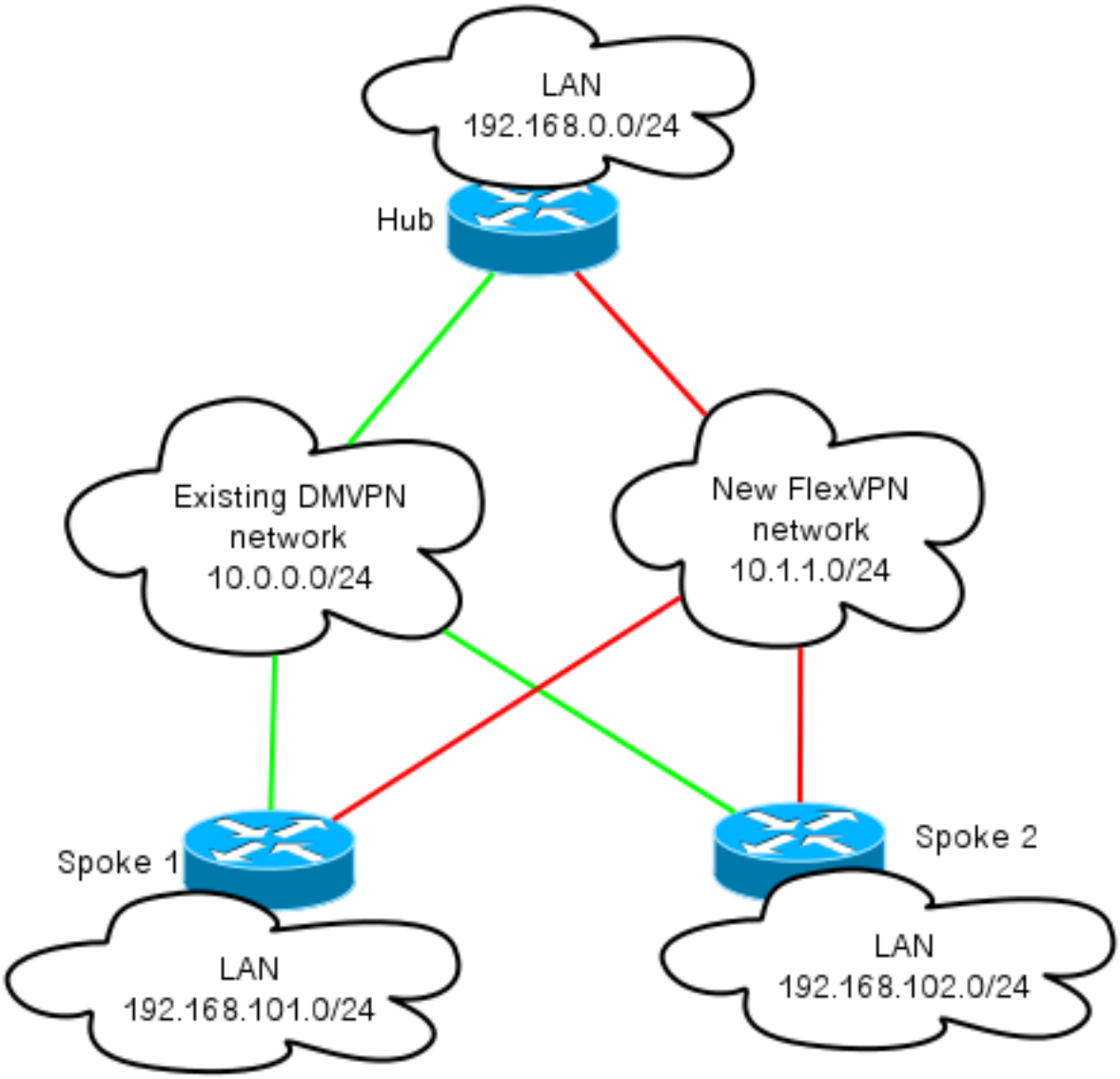
Esempio di rete di trasporto

La rete di trasporto utilizzata in questo esempio include un hub singolo con due spoke connessi. Tutti i dispositivi sono connessi tramite una rete che simula Internet.



Sovrapponi diagramma reticolare

La rete di overlay utilizzata in questo esempio include un unico hub con due spoke connessi. Tenere presente che sia DMVPN che FlexVPN sono attivi contemporaneamente, ma utilizzano spazi di indirizzi IP diversi.



Configurazioni

Questa configurazione esegue la migrazione della distribuzione più popolare di DMVPN fase 3 tramite il protocollo EIGRP (Enhanced Interior Gateway Routing Protocol) a FlexVPN con Border Gateway Protocol (BGP). Cisco consiglia di utilizzare BGP con FlexVPN, perché consente una migliore scalabilità delle installazioni.

> **Nota:** L'hub termina le sessioni IKEv1 (DMVPN) e IKEv2 (FlexVPN) sullo stesso indirizzo IP. Ciò è possibile solo con le versioni più recenti di Cisco IOS.

Configurazione spoke

Questa è una configurazione molto semplice, con due eccezioni degne di nota che consentono l'interoperabilità di IKEv1 e IKEv2, nonché due framework che usano GRE (Generic Routing Encapsulation) su IPsec per il trasporto e possono coesistere.

> **Nota:** Le modifiche apportate alla configurazione di ISAKMP (Internet Security Association and Key Management Protocol) e IKEv2 sono evidenziate in grassetto.

```
crypto keyring DMVPN_IKEv1
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco

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 isakmp policy 10
encr aes
authentication pre-share

crypto isakmp keepalive 30 5

crypto isakmp profile DMVPN_IKEv1
keyring DMVPN_IKEv1
match identity address 0.0.0.0

crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
mode transport

crypto ipsec profile DMVPN_IKEv1
set transform-set IKEv1
set isakmp-profile DMVPN_IKEv1

crypto ipsec profile default
set ikev2-profile Flex_IKEv2

interface Tunnel0
 desciption DMVPN tunnel
ip address 10.0.0.101 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp map 10.0.0.1 172.25.1.1
ip nhrp map multicast 172.25.1.1
ip nhrp network-id 1
ip nhrp holdtime 900
ip nhrp nhs 10.0.0.1
ip nhrp shortcut
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel mode gre multipoint
 tunnel key 0
tunnel protection ipsec profile DMVPN_IKEv1 isakmp-profile DMVPN_IKEv1

interface Tunnel1
description FlexVPN spoke-to-hub 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
tunnel source Ethernet0/0
tunnel destination 172.25.1.1
 tunnel protection ipsec profile default ikev2-profile Flex_IKEv2


interface Virtual-Template1 type tunnel
description FlexVPN spoke-to-spoke
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 protection ipsec profile default ikev2-profile Flex_IKEv2
```

Cisco IOS release 15.3 consente di collegare entrambi i profili IKEv2 e ISAKMP in una configurazione di *protezione tunnel*. Oltre ad alcune modifiche interne al codice, ciò consente a IKEv1 e IKEv2 di funzionare sullo stesso dispositivo contemporaneamente.

A causa del modo in cui Cisco IOS seleziona i profili (IKEv1 o IKEv2) nelle versioni precedenti alla 15.3, sono emerse alcune avvertenze, ad esempio situazioni in cui IKEv1 viene avviato a IKEv2 tramite il peer. La separazione di IKE si basa ora sul livello di profilo, non sul livello di interfaccia, e viene ottenuta tramite la nuova CLI.

Un altro aggiornamento della nuova versione di Cisco IOS è l'aggiunta della *chiave* del *tunnel*. Questa operazione è necessaria perché DMVPN e FlexVPN utilizzano la stessa interfaccia di origine e lo stesso indirizzo IP di destinazione. In questo modo, non è possibile per il tunnel GRE sapere quale interfaccia tunnel viene utilizzata per decapsulare il traffico. La chiave del tunnel consente di distinguere tunnel0 e tunnel1 con l'aggiunta di un piccolo sovraccarico (4 byte). È possibile configurare una chiave diversa su entrambe le interfacce, ma in genere è necessario differenziare solo un tunnel.

> Nota: L'opzione di protezione del tunnel condiviso non è richiesta quando DMVPN e FlexVPN condividono la stessa interfaccia.

Pertanto, la configurazione del protocollo di routing spoke è di base. EIGRP e BGP funzionano separatamente. EIGRP esegue la pubblicità solo sull'interfaccia del tunnel per evitare il peering sui tunnel spoke-to-spoke, che limita la scalabilità. BGP mantiene una relazione solo con il router hub (10.1.1.1) per pubblicizzare la rete locale (192.168.101.0/24).

```
router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.101.0
passive-interface default
no passive-interface Tunnel0

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

Configurazione hub

Ènecessario apportare modifiche simili alla configurazione hub-side descritta nella sezione **Configurazione spoke**.

> **Nota:** Le modifiche rilevanti alla configurazione di ISAKMP e IKEV2 sono evidenziate in grassetto.

```
crypto ikev2 authorization policy default
pool FlexSpokes
route set interface

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 isakmp policy 10
encr aes
authentication pre-share

crypto isakmp key cisco address 0.0.0.0


crypto ipsec profile DMVPN_IKEv1
set transform-set IKEv1

crypto ipsec profile default
set ikev2-profile Flex_IKEv2

interface Tunnel0
ip address 10.0.0.1 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp map multicast dynamic
 ip nhrp network-id 1
ip nhrp holdtime 900
ip nhrp server-only
ip nhrp redirect
 ip summary-address eigrp 100 192.168.0.0 255.255.0.0
ip tcp adjust-mss 1360
tunnel source Loopback0
tunnel mode gre multipoint
 tunnel key 0
 tunnel protection ipsec profile DMVPN_IKEv1

interface Virtual-Template1 type tunnel
ip unnumbered Loopback100
ip mtu 1400
 ip nhrp network-id 2
ip tcp adjust-mss 1360
```

```
 tunnel protection ipsec profile default
```

Sul lato hub, l'associazione tra il profilo IKE e il profilo IPsec si verifica a livello di profilo, a differenza della configurazione spoke, in cui viene completata tramite il comando **tunnel protection**. Entrambi gli approcci sono metodi validi per completare l'associazione.

Èimportante notare che gli ID di rete NHRP (Next Hop Resolution Protocol) sono diversi per DMVPN e FlexVPN nel cloud. Nella maggior parte dei casi, non è consigliabile creare un singolo dominio in entrambi i framework.

La chiave del tunnel differenzia i tunnel DMVPN e FlexVPN a livello GRE per raggiungere lo stesso obiettivo menzionato nella sezione **Configurazione spoke**.

La configurazione di routing sull'hub è di base. Il dispositivo hub mantiene due relazioni con qualsiasi spoke specificato, una che utilizza EIGRP e una che utilizza BGP. La configurazione BGP utilizza l'intervallo di ascolto per evitare una configurazione lunga per spoke.

Gli indirizzi di riepilogo vengono introdotti due volte. La configurazione EIGRP invia un riepilogo utilizzando la configurazione **tunnel0** (indirizzo di riepilogo IP EIGRP 100) e il BGP introduce un riepilogo utilizzando l'indirizzo di aggregazione. I riepiloghi sono necessari per garantire il reindirizzamento NHRP e per semplificare gli aggiornamenti del routing. È possibile inviare un reindirizzamento NHRP (simile a un reindirizzamento ICMP (Internet Control Message Protocol) che indica se esiste un hop migliore per una determinata destinazione, che consente di stabilire un tunnel spoke-to-spoke. Questi riepiloghi vengono utilizzati anche per ridurre al minimo la quantità di aggiornamenti del routing inviati tra l'hub e il relativo ciascun raggio, che consente una migliore scalabilità delle impostazioni.

```
router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.0.0 0.0.255.255
passive-interface default
no passive-interface Tunnel0

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
```

Verifica

La verifica di questo esempio di configurazione è divisa in più sezioni.

Controlli pre-migrazione

Poiché sia DMVPN/EIGRP che FlexVPN/BGP funzionano contemporaneamente, è necessario verificare che Spoke mantenga una relazione su IPsec sia con IKEv1 che con IKEv2 e che i prefissi appropriati vengano appresi tramite EIGRP e BGP.

Nell'esempio, **Spoke1** mostra che vengono gestite due sessioni con il router hub; una utilizza IKEv1/**Tunnel0**, l'altra IKEv2/**Tunnel1**.

Nota: Per ogni tunnel vengono gestite due associazioni di sicurezza IPsec (una in entrata e una in uscita).

```
Spoke1#show cry sess
Crypto session current status

Interface: Tunnel0
Profile: DMVPN_IKEv1
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 0
IKEv1 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
 Active SAs: 2, origin: crypto map

Interface: Tunnel1
Profile: Flex_IKEv2
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 1
 IKEv2 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
Active SAs: 2, origin: crypto map
```

Quando si controllano i protocolli di routing, è necessario verificare che sia stato formato un router adiacente e che siano stati appresi i prefissi corretti. Questa operazione viene innanzitutto verificata con il protocollo EIGRP. Verificare che l'hub sia visibile come router adiacente e che l'indirizzo 192.168.0.0/16 (riepilogo) sia stato ricavato dall'hub:

```
Spoke1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.0.0.1 Tu0 10 00:04:02 7 1398 0 13

Spoke1#show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status

P 192.168.101.0/24, 1 successors, FD is 281600
via Connected, Ethernet1/0
P 192.168.0.0/16, 1 successors, FD is 26880000
via 10.0.0.1 (26880000/256), Tunnel0
P 10.0.0.0/24, 1 successors, FD is 26880000
via Connected, Tunnel0
```

Verificare quindi il BGP:

```
Spoke1#show bgp summary
(...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 13 11 3 0 0 00:06:56 1
Spoke1#show bgp
BGP table version is 3, 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
r>i 192.168.0.0/16 10.1.1.1 0 100 0 i
*> 192.168.101.0 0.0.0.0 0 32768 i
```

L'output mostra che l'indirizzo IP FlexVPN dell'hub (10.1.1.1) è un router adiacente tramite il quale il spoke riceve un prefisso (192.168.0.0/16). Inoltre, il BGP informa l'amministratore che si è verificato un errore RIB (Routing Information Base) per il prefisso 192.168.0.0/16. Questo errore si verifica perché esiste una route migliore per il prefisso già esistente nella tabella di routing. Questo percorso è stato creato da EIGRP e può essere confermato selezionando la tabella di routing.

```
Spoke1#show ip route 192.168.0.0 255.255.0.0
Routing entry for 192.168.0.0/16, supernet
 Known via "eigrp 100", distance 90, metric 26880000, type internal
Redistributing via eigrp 100
Last update from 10.0.0.1 on Tunnel0, 00:10:07 ago
Routing Descriptor Blocks:
* 10.0.0.1, from 10.0.0.1, 00:10:07 ago, via Tunnel0
Route metric is 26880000, traffic share count is 1
Total delay is 50000 microseconds, minimum bandwidth is 100 Kbit
Reliability 255/255, minimum MTU 1400 bytes
Loading 1/255, Hops 1
```

Migrazione

Nella sezione precedente è stato verificato che IPsec e i protocolli di routing siano configurati e funzionino come previsto. Uno dei modi più semplici per eseguire la migrazione da DMVPN a FlexVPN sullo stesso dispositivo è modificare la distanza amministrativa (AD). In questo esempio, il BGP (iBGP) interno ha un AD di 200, mentre l'EIGRP ha un AD di 90.

Affinché il traffico fluisca correttamente attraverso FlexVPN, il BGP deve avere un AD migliore. In questo esempio, l'AD EIGRP viene modificato in 230 e 240 rispettivamente per le route interne ed esterne. Ciò rende BGP AD (di 200) più preferibile per il prefisso 192.168.0.0/16.

Un altro metodo utilizzato per ottenere questo risultato è ridurre BGP AD. Tuttavia, il protocollo eseguito dopo la migrazione ha valori non predefiniti che possono influire su altre parti della distribuzione.

Nell'esempio, il comando debug ip routing viene usato per verificare il funzionamento di Spoke.

> **Nota:** Se le informazioni di questa sezione vengono utilizzate in una rete di produzione, evitare di utilizzare i comandi di debug e basarsi sui comandi show elencati nella sezione successiva. Inoltre, il processo EIGRP spoke deve ristabilire le adiacenze con l'hub.

```
Spoke1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Spoke1(config)#router eigrp 100
Spoke1(config-router)# distance eigrp 230 240
Spoke1(config-router)#^Z
Spoke1#
*Oct 9 12:12:34.207: %SYS-5-CONFIG_I: Configured from console by console
```

```
*Oct 9 12:12:43.648: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1
 (Tunnel0) is down: route configuration changed

*Oct 9 12:12:43.648: RT: delete route to 192.168.0.0 via 10.0.0.1,
 eigrp metric [90/26880000]
*Oct 9 12:12:43.648: RT: no routes to 192.168.0.0, delayed flush
*Oct 9 12:12:43.648: RT: delete network route to 192.168.0.0/16
*Oct 9 12:12:43.650: RT: updating bgp 192.168.0.0/16 (0x0) :
via 10.1.1.1

*Oct 9 12:12:43.650: RT: add 192.168.0.0/16 via 10.1.1.1, bgp metric [200/0]
Spoke1#
*Oct 9 12:12:45.750: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1
 (Tunnel0) is up: new adjacency
```

In questo output è possibile notare tre azioni importanti:

- Il raggio nota che l'Active Directory è cambiata e disattiva l'adiacenza.
- Nella tabella di routing, il prefisso EIGRP viene mantenuto e viene introdotto il BGP.
- L'adiacenza all'hub sull'EIGRP torna online.

La modifica di Active Directory in un dispositivo influisce solo sul percorso dal dispositivo alle altre reti; non influisce sulla modalità di esecuzione del routing da parte degli altri router. Ad esempio, dopo aver aumentato la distanza EIGRP su **Spoke1** (e aver utilizzato FlexVPN sul cloud per instradare il traffico), l'hub mantiene gli AD configurati (predefiniti). Ciò significa che utilizza DMVPN per indirizzare il traffico a **Spoke1**.

In alcuni scenari, ciò può causare problemi, ad esempio quando i firewall prevedono traffico di ritorno sulla stessa interfaccia. È pertanto consigliabile modificare l'Active Directory su tutti gli spoke prima di modificarlo nell'hub. La migrazione del traffico da parte di FlexVPN viene completata solo al termine di questa operazione.

Migrazione da EIGRP a EIGRP

Una migrazione da DMVPN a FlexVPN con solo EIGRP non viene trattata in modo approfondito in questo documento; tuttavia, viene qui menzionato per completezza.

Èpossibile aggiungere sia DMVPN che EIGRP alla stessa istanza di routing di EIGRP Autonomous System (AS). Con questa impostazione, l'adiacenza di routing viene stabilita su entrambi i tipi di cloud. Ciò può causare il bilanciamento del carico, che in genere non è consigliato.

Per assicurarsi che sia stato scelto FlexVPN o DMVPN, un amministratore può assegnare valori di **ritardo** diversi per ogni interfaccia. Tuttavia, è importante ricordare che non è possibile modificare le interfacce dei modelli virtuali mentre sono presenti le interfacce di accesso virtuale corrispondenti.

Controlli successivi alla migrazione

Analogamente al processo utilizzato nella sezione **Controlli pre-migrazione**, è necessario verificare l'IPsec e il protocollo di routing.

Verificare innanzitutto il protocollo IPsec:

```
Spoke1#show crypto session
Crypto session current status

Interface: Tunnel0
Profile: DMVPN_IKEv1
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 0
IKEv1 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
 Active SAs: 2, origin: crypto map

Interface: Tunnel1
Profile: Flex_IKEv2
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 1
IKEv2 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
Active SAs: 2, origin: crypto map
```

Come in precedenza, vengono visualizzate due sessioni, entrambe con due SA IPsec attive.

Sul spoke, il percorso aggregato (**192.168.0.0/16**) punta dall'hub ed è appreso tramite BGP.

```
Spoke1#show ip route 192.168.0.0 255.255.0.0
Routing entry for 192.168.0.0/16, supernet
Known via "bgp 65001", distance 200, metric 0, type internal
Last update from 10.1.1.1 00:14:07 ago
Routing Descriptor Blocks:
* 10.1.1.1, from 10.1.1.1, 00:14:07 ago
Route metric is 0, traffic share count is 1
AS Hops 0
MPLS label: none
```

Analogamente, la LAN spoke con prefisso sull'hub deve essere nota tramite EIGRP. In questo esempio, viene controllata la subnet LAN **spoke2**:

```
Hub#show ip route 192.168.102.0 255.255.255.0
Routing entry for 192.168.102.0/24
 Known via "bgp 65001", distance 200, metric 0, type internal
Last update from 10.1.1.106 00:04:35 ago
Routing Descriptor Blocks:
* 10.1.1.106, from 10.1.1.106, 00:04:35 ago
Route metric is 0, traffic share count is 1
AS Hops 0
MPLS label: none

Hub#show ip cef 192.168.102.100
192.168.102.0/24
nexthop 10.1.1.106 Virtual-Access2
```

Nell'output, il percorso di inoltro viene aggiornato correttamente e punta all'esterno di un'interfaccia di accesso virtuale.

Ulteriori considerazioni

In questa sezione vengono descritte alcune aree di importanza aggiuntive rilevanti per questo

esempio di configurazione.

Tunnel spoke-to-spoke esistenti

Con una migrazione da EIGRP a BGP, i tunnel spoke-to-spoke non sono influenzati, in quanto la commutazione di collegamento è ancora in funzione. La commutazione di collegamento sullo spoke inserisce una route NHRP più specifica con AD di 250.

Di seguito è riportato un esempio di tale percorso:

```
Spoke1#show ip route 192.168.102.100
Routing entry for 192.168.102.0/24
Known via "nhrp", distance 250, metric 1
Last update from 10.1.1.106 on Virtual-Access1, 00:00:42 ago
Routing Descriptor Blocks:
* 10.1.1.106, from 10.1.1.106, 00:00:42 ago, via Virtual-Access1
Route metric is 1, traffic share count is 1
```

Comunicazione tra spoke migrati e non migrati

Se uno spoke già presente su un FlexVPN/BGP desidera comunicare con un dispositivo per cui il processo di migrazione non è iniziato, il traffico scorre sempre sull'hub.

Questo è il processo che si verifica:

1. Lo spoke esegue una ricerca route per la destinazione, che punta attraverso una route di riepilogo annunciata dall'hub.
2. Il pacchetto viene inviato all'hub.
3. L'hub riceve il pacchetto ed esegue una ricerca del percorso per la destinazione, che punta all'esterno di un'altra interfaccia che fa parte di un dominio NHRP diverso.

   Nota: L'ID di rete NHRP nella configurazione hub precedente è diverso per FlexVPN e DMVPN.

Anche se gli ID di rete NHRP sono unificati, potrebbe verificarsi un problema quando il spoke migrato instrada oggetti sulla rete FlexVPN. inclusa la direttiva utilizzata per configurare la commutazione dei collegamenti. Lo spoke non migrato tenta di eseguire oggetti sulla rete DMVPN, con un obiettivo specifico di eseguire la commutazione dei collegamenti.

Risoluzione dei problemi

In questa sezione vengono descritte le due categorie utilizzate in genere per risolvere i problemi relativi alla migrazione.

Problemi con i tentativi di stabilire i tunnel

Se la negoziazione IKE non riesce, completare i seguenti passaggi:

1. Verificare lo stato corrente con questi comandi:

   show crypto isakmp sa: questo comando rivela la quantità, l'origine e la destinazione di una sessione IKEv1.**show crypto ipsec sa**: questo comando rivela l'attività delle associazioni di protezione IPsec.**Nota:** A differenza di IKEv1, in questo output il valore Gruppo Diffie-Hellman (DH) PFS (Perfect Forward Secrecy) viene visualizzato come **PFS (Y/N): N, gruppo DH: nessuna** durante la prima negoziazione nelle gallerie; tuttavia, dopo una nuova chiave, verranno visualizzati i valori corretti. Non si tratta di un bug, anche se il comportamento è descritto in CSCug67056. La differenza tra IKEv1 e IKEv2 è che in quest'ultimo caso le associazioni di protezione figlio vengono create come parte dello scambio **AUTH**. Il gruppo DH configurato nella mappa crittografica viene utilizzato solo durante una reimpostazione della chiave. Per questo motivo, viene visualizzato **PFS (S/N): N, gruppo DH: nessuna fino alla prima reimpostazione della chiave.** Con IKEv1, il comportamento è diverso in quanto la creazione dell'associazione di protezione figlio viene eseguita durante la modalità rapida e il messaggio **CREATE_CHILD_SA** include disposizioni per il trasferimento del payload di scambio chiave che specifica i parametri DH per derivare un nuovo segreto condiviso.**show crypto ikev2 sa** - Questo comando restituisce un output simile a ISAKMP ma specifico di IKEv2.**show crypto session** - Questo comando restituisce l'output di riepilogo delle sessioni di crittografia del dispositivo.**show crypto socket** - Questo comando mostra lo stato dei crypto-socket.**show crypto map** - Questo comando mostra il mapping dei profili IKE e IPsec alle interfacce.**show ip nhrp** - Questo comando restituisce le informazioni NHRP dal dispositivo. Ciò è utile per le associazioni spoke-to-spoke nelle impostazioni FlexVPN e per le associazioni spoke-to-hub nelle impostazioni DMVPN.
2. Per eseguire il debug della configurazione del tunnel, usare questi comandi:

   debug crypto ikev2debug crypto isakmpdebug crypto ipsecdebug crypto kmi

Problemi di propagazione route

Di seguito sono riportati alcuni comandi utili che è possibile utilizzare per risolvere i problemi relativi a EIGRP e alla topologia:

- **show bgp summary**: utilizzare questo comando per verificare i router adiacenti connessi e i relativi stati.
- **show ip eigrp neighbors**: utilizzare questo comando per visualizzare i router adiacenti connessi tramite EIGRP.
- **show bgp** - Utilizzare questo comando per verificare i prefissi appresi sul protocollo BGP.
- **show ip eigrp topology**: utilizzare questo comando per visualizzare i prefissi appresi tramite EIGRP.

Èimportante sapere che un prefisso appreso è diverso da un prefisso installato nella tabella di routing. Per ulteriori informazioni su questo argomento, fare riferimento all'articolo Route Selection in Cisco Router Cisco o al manuale Routing TCP/IP Cisco Press.

Avvertenze note

Sull'ASR1K esiste una limitazione simile alla gestione del tunnel GRE. Questa condizione viene rilevata con l'ID bug Cisco CSCue00443. Al momento, la limitazione ha una correzione pianificata nel software Cisco IOS XE versione 3.12.

Monitorare il bug se si desidera ricevere una notifica quando la correzione diventa disponibile.