Migrazione di un disco rigido da DMVPN a FlexVPN sugli stessi dispositivi

Sommario

Introduzione

Questo documento offre informazioni su come eseguire la migrazione da una rete DMVPN esistente a FlexVPN sugli stessi dispositivi.

Le configurazioni di entrambi i framework coesisteranno sui dispositivi.

In questo documento viene mostrato solo lo scenario più comune: DMVPN che utilizza una chiave già condivisa per l'autenticazione ed EIGRP come protocollo di routing.

Questo documento dimostra la migrazione a BGP (protocollo di routing consigliato) e a un protocollo EIGRP meno desiderabile.

Prerequisiti

Requisiti

In questo documento si presume che il lettore conosca i concetti di base di DMVPN e FlexVPN.

Componenti usati

Non tutti i componenti software e hardware supportano IKEv2. Per ulteriori informazioni, fare riferimento a Cisco Feature Navigator. Le versioni software da utilizzare sono:

- ISR - 15.2(4)M1 o versione successiva
- ASR1k - 3.6.2 release 15.2(2)S2 o successiva

Tra i vantaggi della piattaforma e del software più recenti vi è la possibilità di utilizzare la crittografia di nuova generazione, ad esempio AES GCM per la crittografia in IPsec. Questa condizione viene discussa nella RFC 4106.

AES GCM consente di raggiungere una velocità di crittografia molto più elevata su alcuni componenti hardware.

Per ulteriori raccomandazioni sull'utilizzo e la migrazione della crittografia di nuova generazione, fare riferimento a:

http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Procedura di migrazione

Attualmente, il modo consigliato per migrare da DMVPN a FlexVPN è che i due framework non funzionino contemporaneamente.

Questa limitazione verrà rimossa a causa delle nuove funzionalità di migrazione introdotte nella versione ASR 3.10, rilevate in più richieste di miglioramenti sul lato Cisco, incluso CSCuc08066. Tali funzionalità saranno disponibili a fine giugno 2013.

Una migrazione in cui entrambi i framework coesistono e operano contemporaneamente sugli stessi dispositivi viene definita migrazione soft, che indica un impatto minimo e un failover senza problemi da un framework all'altro.

Una migrazione in cui la configurazione di entrambi i framework coesiste, ma non funziona contemporaneamente viene definita migrazione hardware. Ciò significa che il passaggio da un framework all'altro comporta una mancanza di comunicazione sulla VPN, anche se minima.

Migrazione hardware sugli stessi dispositivi

In questo documento viene descritta la migrazione da una rete DMVPN esistente a una nuova rete FlexVPN sugli stessi dispositivi.

Questa migrazione richiede che entrambi i framework non funzionino contemporaneamente sui dispositivi, essenzialmente richiedendo che la funzionalità DMVPN sia disabilitata a tutti i livelli prima di abilitare FlexVPN.

Finché la nuova funzionalità di migrazione non sarà disponibile, per eseguire migrazioni utilizzando gli stessi dispositivi è necessario:

1. Verificare la connettività su DMVPN.
2. Aggiungere la configurazione FlexVPN e arrestare le interfacce tunnel e modello virtuale appartenenti alla nuova configurazione.
3. (Durante un intervento di manutenzione) Chiudere tutte le interfacce del tunnel DMVPN su tutti i spoke e gli hub prima di passare al punto 4.
4. Riavviare le interfacce del tunnel FlexVPN.
5. Verificare la connettività spoke-hub.
6. Verificare la connettività spoke-to-spoke.
7. *Se la verifica di cui ai punti 5 o 6 non è stata eseguita correttamente, tornare a DMVPN chiudendo l'interfaccia FlexVPN e rimuovendo le interfacce DMVPN.*
8. *Verificare la comunicazione spoke-hub.*
9. *Verifica la comunicazione spoke.*

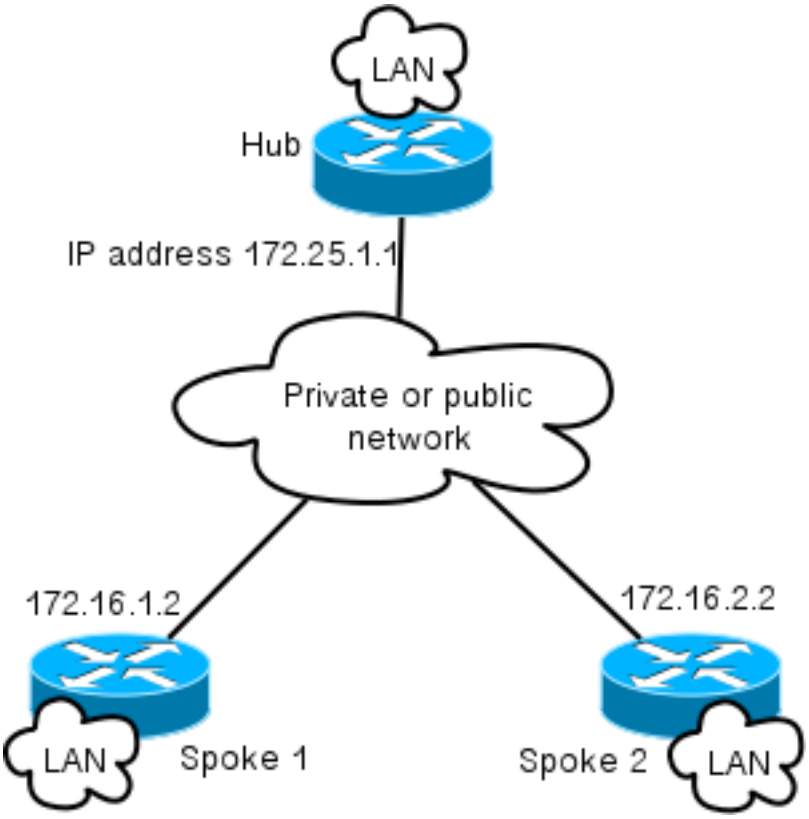
Approccio personalizzato

Se, a causa della complessità della rete o del routing, l'approccio non è quello ottimale, avviare una discussione con il rappresentante Cisco prima di procedere alla migrazione. La persona migliore per discutere di un processo di migrazione personalizzato è il tecnico di sistema o il tecnico dell'assistenza.

Topologia della rete

Topologia della rete di trasporto

Il diagramma mostra una topologia di connessioni tipica degli host su Internet. In questo documento, l'indirizzo IP di loopback0 (172.25.1.1) dell'hub viene utilizzato per terminare la sessione IPsec.

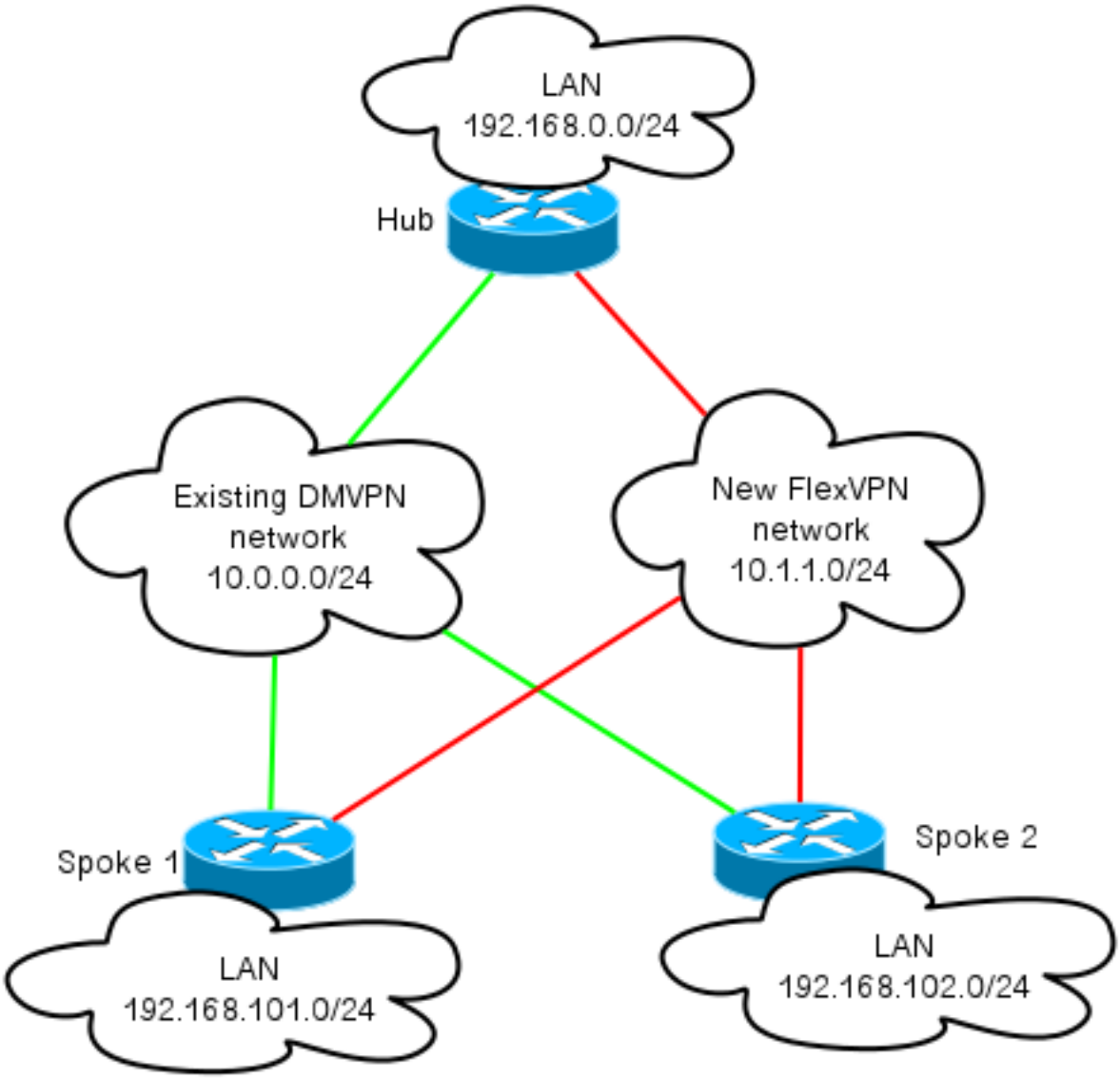


Sovrapponi topologia di rete

Il diagramma della topologia mostra due cloud separati utilizzati per la sovrapposizione: Connessioni DMVPN (green connections) e FlexVPN.

I prefissi Local Area Network vengono visualizzati per i lati corrispondenti.

La subnet 10.1.1.0/24 non rappresenta una subnet effettiva in termini di indirizzamento dell'interfaccia, ma piuttosto un blocco di spazio IP dedicato al cloud FlexVPN. Le motivazioni alla base di sono descritte più avanti nella sezione Configurazione FlexVPN.



Configurazione

Configurazione DMVPN

Questa sezione contiene la configurazione di base di Hub e Spoke DMVPN.

Chiave già condivisa (PSK) utilizzata per l'autenticazione IKEv1.

Una volta stabilito il protocollo IPsec, la registrazione NHRP viene eseguita da spoke a hub, in modo che l'hub possa apprendere dinamicamente l'indirizzamento NBMA degli spoke.

Quando NHRP esegue la registrazione su spoke e hub, l'adiacenza di routing può stabilire e route scambiate. Nell'esempio, il protocollo EIGRP viene usato come protocollo di routing di base per la rete di sovrapposizione.

Configurazione Spoke DMVPN

Questa è una configurazione di base di DMVPN con autenticazione a chiave già condivisa e EIGRP come protocollo di routing.

```
crypto isakmp policy 10
  encr aes
  authentication pre-share
crypto isakmp key cisco address 0.0.0.0
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
interface Tunnel0
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 protection ipsec profile DMVPN_IKEv1
router eigrp 100
 network 10.0.0.0 0.0.0.255
 network 192.168.102.0
 passive-interface default
 no passive-interface Tunnel0
```

Configurazione DMVPN hub

Nella configurazione hub il tunnel viene originato da loopback0 con un indirizzo IP di 172.25.1.1.

Il resto è una distribuzione standard di hub DMVPN con EIGRP come protocollo di routing.

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
crypto isakmp key cisco 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
 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 protection ipsec profile DMVPN_IKEv1
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
```

Configurazione FlexVPN

FlexVPN si basa sulle stesse tecnologie fondamentali:

- IPSec: A differenza dell'impostazione predefinita in DMVPN, IKEv2 viene utilizzato al posto di IKEv1 per negoziare le associazioni di protezione IPSec. IKEv2 offre miglioramenti rispetto a IKEv1, a partire dalla resilienza fino al numero di messaggi necessari per stabilire un canale dati protetto.
- GRE : A differenza di DMVPN, vengono utilizzate interfacce point-to-point statiche e dinamiche e non solo su interfacce GRE multipoint statiche. Questa configurazione consente una maggiore flessibilità, in particolare per il comportamento per spoke/per hub.
- NHRP: In FlexVPN NHRP viene utilizzato principalmente per stabilire la comunicazione spoke. I raggi non vengono registrati nell'hub.
- Instradamento: Poiché gli spoke non eseguono la registrazione NHRP all'hub, è necessario fare affidamento su altri meccanismi per garantire che hub e spoke possano comunicare in modo bidirezionale. Analogamente a DMVPN, è possibile utilizzare protocolli di routing dinamico. Tuttavia, FlexVPN consente di utilizzare IPsec per introdurre informazioni di routing. Per impostazione predefinita, il valore /32 viene introdotto come percorso per l'indirizzo IP sull'altro lato del tunnel e consente la comunicazione diretta da spoke a hub.

Nella migrazione da DMVPN a FlexVPN, i due framework non funzionano contemporaneamente sugli stessi dispositivi. Si consiglia tuttavia di tenerli separati.

Separarli su più livelli:

- NHRP: utilizzare un ID di rete NHRP diverso (consigliato).
- Instradamento: utilizzare processi di instradamento separati (scelta consigliata).
- La separazione VRF - VRF consente una maggiore flessibilità, ma non verrà discussa in questa sezione (opzionale).

Configurazione Spoke FlexVPN

Una delle differenze nella configurazione spoke di FlexVPN rispetto a DMVPN, è che potenzialmente si hanno due interfacce.

Ènecessario un tunnel per la comunicazione spoke-hub e un tunnel opzionale per i tunnel spoke-spoke. Se si sceglie di non utilizzare il tunneling spoke dinamico e si preferisce che tutto passi attraverso il dispositivo hub, è possibile rimuovere l'interfaccia del modello virtuale e rimuovere il collegamento NHRP per la commutazione dall'interfaccia del tunnel.

Notare anche che l'interfaccia del tunnel statico ha un indirizzo IP ricevuto in base alla negoziazione. In questo modo, l'hub fornisce all'IP dell'interfaccia del tunnel la funzionalità spoke dinamica senza la necessità di creare indirizzi statici nel cloud FlexVPN.

```
aaa new-model
aaa authorization network default local
```

```
aaa session-id common

crypto ikev2 profile Flex_IKEv2
 match identity remote fqdn domain cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 aaa authorization group cert list default default
 virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

Cisco consiglia di utilizzare AES GCM nell'hardware che lo supporta.

```
crypto ipsec transform-set IKEv2 esp-gcm
    mode transport
crypto ipsec profile default
 set ikev2-profile Flex_IKEv2
! set transform-set IKEv2
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
 shutdown
 tunnel source Ethernet0/0
 tunnel destination 172.25.1.1
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
interface Virtual-Template1 type tunnel
 ip unnumbered Tunnel1
 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
```

PKI è la modalità consigliata per eseguire l'autenticazione su larga scala in IKEv2.

Tuttavia, è possibile continuare a utilizzare una chiave già condivisa se si è consapevoli dei relativi limiti.

Di seguito è riportato un esempio di configurazione con "cisco" come PSK:

```
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
```

Configurazione hub FlexVPN

In genere, un hub termina solo i tunnel spoke-to-hub dinamici. Ecco perché nella configurazione

dell'hub non è presente un'interfaccia tunnel statica per FlexVPN, ma viene utilizzata un'interfaccia modello virtuale. Verrà generata un'interfaccia di accesso virtuale per ogni connessione.

Notare che sul lato hub è necessario indicare gli indirizzi del pool da assegnare agli spoke.

Gli indirizzi di questo pool verranno aggiunti in seguito nella tabella di routing come route /32 per ogni spoke.

```
aaa new-model
aaa authorization network default local
aaa session-id common
crypto ikev2 authorization policy default
 pool FlexSpokes
crypto ikev2 profile Flex_IKEv2
 match identity remote fqdn domain cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 aaa authorization group cert list default default
 virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

Cisco consiglia di utilizzare AES GCM nell'hardware che lo supporta.

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

Nella configurazione riportata di seguito, l'operazione AES GCM è stata commentata.

```
crypto ipsec profile default
 set ikev2-profile Flex_IKEv2
! set transform-set IKEv2
interface Loopback0
 description DMVPN termination
 ip address 172.25.1.1 255.255.255.255
interface Loopback100
 ip address 10.1.1.1 255.255.255.255
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback100
 ip nhrp network-id 2
 ip nhrp redirect
 shutdown
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

Con l'autenticazione in IKEv2, lo stesso principio si applica all'hub e allo spoke.

Per garantire scalabilità e flessibilità, utilizzare i certificati. Tuttavia, è possibile riutilizzare per PSK la stessa configurazione di on spoke.

Nota: IKEv2 offre flessibilità in termini di autenticazione. Un lato può autenticarsi utilizzando PSK mentre l'altro RSA-SIG.

Migrazione del traffico

Migrazione a BGP come protocollo di routing di overlay [consigliato]

BGP è un protocollo di routing basato sullo scambio unicast. Per via delle sue caratteristiche è stato il protocollo di scalabilità migliore nelle reti DMVPN.

Nell'esempio viene utilizzato iBGP.

Configurazione Spoke BGP

La migrazione del raggio è costituita da due parti. Abilitazione di BGP come routing dinamico.

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

Dopo l'accensione del router BGP adiacente (vedere la configurazione BGP hub in questa sezione della migrazione) e l'apprendimento di nuovi prefissi su BGP, è possibile spostare il traffico dal cloud DMVPN esistente al nuovo cloud FlexVPN.

Configurazione BGP hub

Nell'hub per evitare di mantenere la configurazione di prossimità per ogni spoke separatamente, vengono configurati i listener dinamici.

In questa configurazione, BGP non avvierà nuove connessioni, ma accetterà la connessione dal pool di indirizzi IP fornito. In questo caso il pool è 10.1.1.0/24, ovvero tutti gli indirizzi nel nuovo cloud FlexVPN.

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

Migrazione del traffico a FlexVPN

Come accennato in precedenza, la migrazione deve essere eseguita arrestando la funzionalità DMVPN e attivando FlexVPN.

Questa procedura garantisce un impatto minimo.

1. Su tutti i raggi:
   ```
   interface tunnel 0
      shut
   ```
2. Nell'hub:
   ```
   interface tunnel 0
     shut
   ```
   A questo punto verificare che non vi siano sessioni IKEv1 stabilite per l'hub da spoke.Èpossibile verificare questa condizione controllando l'output del comando **show crypto isakmp sa** e monitorando i messaggi syslog generati dalla sessione di registrazione

crittografica.Una volta confermata la conferma, puoi iniziare a utilizzare FlexVPN.

3. Continua sull'hub:
```
interface Virtual-template 1
 no shut
```
4. Raggi:
```
interface tunnel 1
   no shut
```

Fasi di verifica

Stabilità IPSec

Il modo migliore per valutare la stabilità di IPSec è monitorare i sylog con questo comando di configurazione abilitato:

```
crypto logging session
```

Se le sessioni sono attive o inattive, è possibile che si tratti di un problema a livello di IKEv2/FlexVPN che deve essere risolto prima di poter iniziare la migrazione.

Informazioni BGP popolate

Se IPsec è stabile, verificare che la tabella BGP sia popolata con le voci dagli spoke (sull'hub) e dal summary from hub (sugli spoke).

Nel caso di BGP, è possibile visualizzare questa condizione eseguendo:

```
show bgp
! or
show bgp ipv4 unicast
! or
show ip bgp summary
```

Esempio di informazioni corrette dall'hub:

```
Hub#show bgp
BGP router identifier 172.25.1.1, local AS number 65001
(...omitted...)
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
*10.1.1.101 4 65001 83 82 13 0 0 01:10:46 1
*10.1.1.102 4 65001 7 7 13 0 0 00:00:44 1
```

Èpossibile notare che l'hub ha appreso che 1 prefisso da ciascuno dei raggi ed entrambi i raggi sono dinamici (contrassegnati da un asterisco (*)).

Esempio di informazioni simili da spoke:

```
Spoke1#show ip bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
(...omitted...)
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 11 11 6 0 0 00:03:43 1
```

Spoke ha ricevuto un prefisso dall'hub. Nel caso di questa impostazione, questo prefisso dovrebbe essere il riepilogo annunciato sull'hub.

Migrazione a nuovi tunnel tramite EIGRP

EIGRP è una scelta popolare nelle reti DMVPN grazie alla sua installazione relativamente semplice e alla rapida convergenza.

Tuttavia, avrà una scalabilità peggiore di BGP e non offre molti dei meccanismi avanzati che possono essere utilizzati da BGP immediatamente.

In questa sezione viene descritto uno dei modi per passare a FlexVPN utilizzando un nuovo processo EIGRP.

Configurazione spoke aggiornata

Nell'esempio, viene aggiunto un nuovo AS con un processo EIGRP separato.

```
router eigrp 200
 network 10.1.1.0 0.0.0.255
 network 192.168.101.0
 passive-interface default
 no passive-interface Tunnel1
```

Nota: evitare di stabilire l'adiacenza del protocollo di routing sui tunnel spoke, in modo da rendere solo l'interfaccia del tunnel1 (spoke to hub) non passiva.

Configurazione hub aggiornata

Analogamente, negli hub, DMVPN dovrebbe rimanere il modo preferito per scambiare il traffico. Tuttavia, FlexVPN dovrebbe annunciare e imparare già gli stessi prefissi.

```
router eigrp 200
 network 10.1.1.0 0.0.0.255
```

Ci sono due modi per fornire un riassunto verso il raggio.

- Ridistribuzione di una route statica che punta a null0 (opzione preferita).
  ```
  ip route 192.168.0.0 255.255.0.0 null 0
  ip access-list standard EIGRP_SUMMARY
   permit 192.168.0.0 0.0.255.255
  router eigrp 200
   distribute-list EIGRP_SUMMARY out Virtual-Template1
   redistribute static metric 1500 10 10 1 1500
  ```
  Questa opzione consente di controllare il riepilogo e la ridistribuzione senza modificare la configurazione VT dell'hub.
- In alternativa, è possibile impostare un indirizzo di riepilogo di tipo DMVPN in Virtual-template. Questa configurazione non è consigliata a causa dell'elaborazione interna e della replica di tale riepilogo in ogni accesso virtuale. Di seguito è riportato un esempio di riferimento:
  ```
  interface Virtual-Template1 type tunnel
   ip summary-address eigrp 200 172.16.1.0 255.255.255.0
   ip summary-address eigrp 200 192.168.0.0 255.255.0.0
  ```

```
delay 2000
```

Migrazione del traffico a FlexVPN

La migrazione deve essere eseguita arrestando la funzionalità DMVPN e attivando FlexVPN.

La seguente procedura garantisce un impatto minimo.

1. Su tutti i raggi:
   ```
   interface tunnel 0
      shut
   ```
2. Nell'hub:
   ```
   interface tunnel 0
     shut
   ```
   A questo punto verificare che non vi siano sessioni IKEv1 stabilite per l'hub da spoke.Èpossibile verificare questa condizione controllando l'output del comando **show crypto isakmp sa** e monitorando i messaggi syslog generati dalla sessione di registrazione crittografica.Una volta confermata la conferma, puoi iniziare a utilizzare FlexVPN.
3. Continua sull'hub:
   ```
   interface Virtual-template 1
    no shut
   ```
4. Su tutti i raggi:
   ```
   interface tunnel 1
      no shut
   ```

Fasi di verifica

Stabilità IPSec

Come nel caso del BGP, è necessario valutare se IPsec è stabile. Il modo migliore per farlo è monitorare i sylog con questo comando di configurazione abilitato:

```
crypto logging session
```

Se le sessioni sono attive o inattive, è possibile che si tratti di un problema a livello di IKEv2/FlexVPN che deve essere risolto prima di poter iniziare la migrazione.

Informazioni EIGRP nella tabella della topologia

Verificare che la tabella della topologia EIGRP sia popolata con voci LAN spoke sull'hub e summary sugli spoke. È possibile verificare questa condizione eseguendo questo comando su hub e spoke.

```
show ip eigrp topology
```

Esempio di output corretto da spoke:

```
Spoke1#sh 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
(...omitted as output related to DMVPN cloud ...)
EIGRP-IPv4 Topology Table for AS(200)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status

P 10.1.1.1/32, 1 successors, FD is 26112000
 via Rstatic (26112000/0)


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 26114560
 via 10.1.1.1 (26114560/1709056), Tunnel1


P 10.1.1.107/32, 1 successors, FD is 26112000
 via Connected, Tunnel1
```

Si noterà che spoke conosce la propria subnet LAN (in corsivo) e i relativi riepiloghi (in **grassetto**).

Esempio di output corretto dall'hub.

```
Hub#sh ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(172.25.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status
(...omitted, related to DMVPN...)
EIGRP-IPv4 Topology Table for AS(200)/ID(172.25.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status

P 10.1.1.1/32, 1 successors, FD is 128256
 via Connected, Loopback100


P 192.168.101.0/24, 1 successors, FD is 1561600 via 10.1.1.107 (1561600/281600), Virtual-Access1
P 192.168.0.0/16, 1 successors, FD is 1709056
 via Rstatic (1709056/0)

P 10.1.1.107/32, 1 successors, FD is 1709056
 via Rstatic (1709056/0)


P 10.1.1.106/32, 1 successors, FD is 1709056
 via Rstatic (1709056/0)


P 0.0.0.0/0, 1 successors, FD is 1709056
 via Rstatic (1709056/0)

P 192.168.102.0/24, 1 successors, FD is 1561600 via 10.1.1.106 (1561600/281600), Virtual-Access2
```

Si noti che l'hub è a conoscenza delle subnet LAN degli spoke (in corsivo), del prefisso di riepilogo che sta pubblicizzando (in **grassetto**) e dell'indirizzo IP assegnato di ogni spoke tramite negoziazione.

Ulteriori considerazioni

Tunnel spoke-to-spoke esistenti

Poiché l'arresto dell'interfaccia del tunnel DMVPN provoca la rimozione delle voci NHRP, i tunnel spoke esistenti verranno eliminati.

Cancellazione di voci NHRP

Come accennato in precedenza, un hub FlexVPN non si basa sul processo di registrazione NHRP da spoke per sapere come instradare il traffico indietro. Tuttavia, i tunnel spoke dinamici si basano su voci NHRP.

In DMVPN, dove la cancellazione di NHRP sull'hub potrebbe avere causato problemi di connettività di breve durata.

In FlexVPN, la cancellazione di NHRP sugli spoke causerà la disattivazione della sessione IPsec di FlexVPN, correlata ai tunnel spoke. Quando si cancella NHRP nessun hub avrà effetto sulla sessione FlexVPN.

Ciò è dovuto al fatto che in FlexVPN, per impostazione predefinita:

- I raggi non vengono registrati negli hub.
- Gli hub funzionano solo come redirector NHRP e non installano voci NHRP.
- Le voci di scelta rapida NHRP vengono installate su spoke per tunnel spoke e sono dinamiche.

Avvertenze note

Il traffico di sintesi vocale potrebbe essere influenzato da CSCub07382.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems