Migrazione da DMVPN a FlexVPN su un hub diverso

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Procedura di migrazione
Migrazione completa tra due hub diversi
Approccio personalizzato
Topologia della rete
Topologia della rete di trasporto
Sovrapponi topologia di rete
Configurazione
Configurazione DMVPN
Configurazione Spoke DMVPN
Configurazione Hub DMVPN
Configurazione FlexVPN
Configurazione Spoke FlexVPN
Configurazione hub FlexVPN
Migrazione del traffico
Eseguire la migrazione a BGP come protocollo di routing della sovrimpressione [consigliato]
Configurazione Spoke BGP
Configurazione BGP hub
Migrazione del traffico a BGP/FlexVPN
Migrazione ai nuovi tunnel con EIGRP
Configurazione spoke aggiornata
Configurazione hub FlexVPN aggiornata
DMVPN Hub - Configurazione BGP aggiornata
Hub FlexVPN - Configurazione BGP aggiornata
Migrazione del traffico a FlexVPN
Fasi di verifica
Ulteriori considerazioni
Tunnel spoke-to-spoke già esistenti
Cancella voci NHRP
Avvertenze note
Informazioni correlate

Introduzione

In questo documento viene illustrato come eseguire la migrazione da una rete DMVPN (Dynamic Multipoint VPN) esistente a FlexVPN su diversi dispositivi hub. Le configurazioni per entrambi i framework coesistono sui dispositivi. In questo documento viene mostrato solo lo scenario più comune: DMVPN con la chiave già condivisa per l'autenticazione e il protocollo EIGRP (Enhanced Interior Gateway Routing Protocol) come protocollo di routing. In questo documento viene illustrata la migrazione al Border Gateway Protocol (BGP), il protocollo di routing consigliato, e il meno desiderabile protocollo EIGRP.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- DMVPN
- FlexVPN

Componenti usati

> **Nota:** Non tutti i componenti software e hardware supportano Internet Key Exchange versione 2 (IKEv2). Fare riferimento a Cisco Feature Navigator per ulteriori informazioni.

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

- Cisco Integrated Service Router (ISR) versione 15.2(4)M1 o successive
- Cisco Aggregation Services Router serie 1000 (ASR1K) 3.6.2 release 15.2(2)S2 o successive

Uno dei vantaggi di una piattaforma e di un software più recenti è la possibilità di utilizzare la crittografia di nuova generazione, ad esempio AES (Advanced Encryption Standard) Galois/Counter Mode (GCM) per la crittografia in IPSec (Internet Protocol Security), come indicato in RFC (Request for Comments) 4106. AES GCM consente di raggiungere una velocità di crittografia molto più elevata su alcuni componenti hardware. Per ulteriori informazioni sui consigli di Cisco relativi all'utilizzo della crittografia di nuova generazione e alla migrazione a tale crittografia, fare riferimento all'articolo sulla crittografia di nuova generazione.

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.

Procedura di migrazione

Al momento, il metodo 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 da introdurre nell'ASR 3.10, rilevate nelle richieste di miglioramenti multipli sul lato Cisco, che includono l'ID bug Cisco CSCuc08066. Queste 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 le configurazioni di entrambi i framework coesistono, ma non funzionano contemporaneamente viene definita **migrazione rigida**. Ciò significa che il passaggio da un framework all'altro implica una mancanza di comunicazione sulla VPN, anche se minima.

Migrazione completa tra due hub diversi

In questo documento viene descritta la migrazione dall'hub DMVPN attualmente utilizzato a un nuovo hub FlexVPN. Questa migrazione consente l'intercomunicazione tra spoke già migrati a FlexVPN e quelli ancora in esecuzione su DMVPN e può essere eseguita in più fasi, su ciascuno spoke separatamente.

A condizione che le informazioni di routing siano popolate correttamente, la comunicazione tra i spoke migrati e non migrati dovrebbe rimanere possibile. Tuttavia, è possibile osservare una latenza aggiuntiva perché i spoke migrati e non migrati non creano reciprocamente tunnel spoke-to-spoke. Allo stesso tempo, i spoke migrati dovrebbero essere in grado di stabilire tunnel spoke-to-spoke diretti tra loro. Lo stesso vale per i raggi non migrati.

Finché non sarà disponibile questa nuova funzionalità di migrazione, completare i seguenti passaggi per eseguire le migrazioni con un hub diverso da DMVPN e FlexVPN:

1. Verificare la connettività su DMVPN.
2. Aggiungere la configurazione FlexVPN e arrestare il tunnel che appartiene alla nuova configurazione.
3. (Durante un intervento di manutenzione) Su ciascun spoke, uno per uno, arrestare il tunnel DMVPN.
4. Nello stesso spoke del passo 3, sbloccare le interfacce del tunnel FlexVPN.
5. Verificare la connettività spoke-to-hub.
6. Verificare la connettività spoke-to-spoke all'interno di FlexVPN.
7. Verificare la connettività spoke-to-spoke con DMVPN da FlexVPN.
8. Ripetere i passaggi da 3 a 7 per ogni raggio separatamente.
9. In caso di problemi con le verifiche descritte nei passaggi 5, 6 o 7, chiudere l'interfaccia FlexVPN e sbloccare le interfacce DMVPN per tornare a DMVPN.
10. Verificare la comunicazione spoke-to-hub sulla DMVPN di backup.
11. Verificare la comunicazione spoke sulla DMVPN di backup.

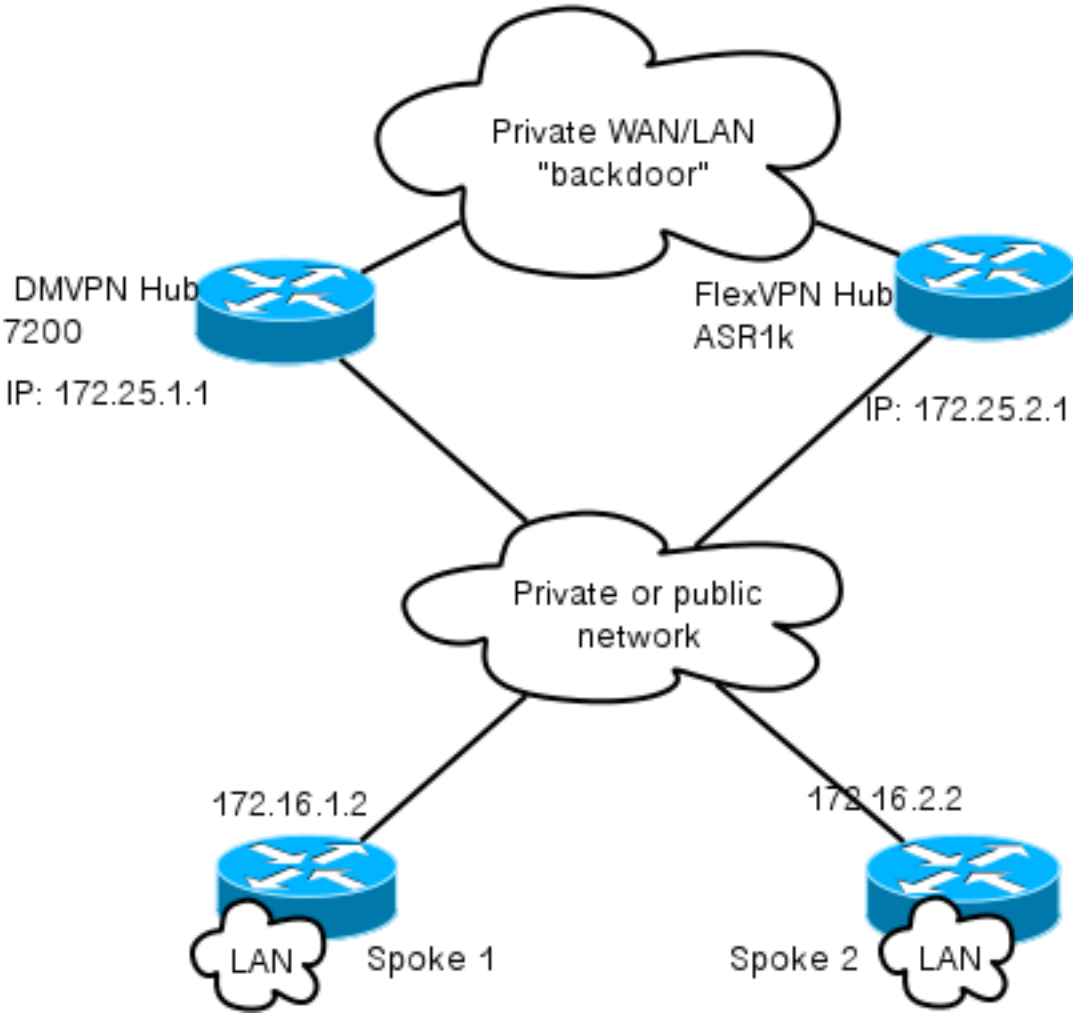
Approccio personalizzato

Se l'approccio precedente non è la soluzione migliore per la tua azienda a causa di complessità di rete o routing, avvia una discussione con il tuo rappresentante Cisco prima di procedere alla migrazione. La persona migliore con cui discutere di un processo di migrazione personalizzato è il tecnico di sistema o il tecnico dei servizi avanzati.

Topologia della rete

Topologia della rete di trasporto

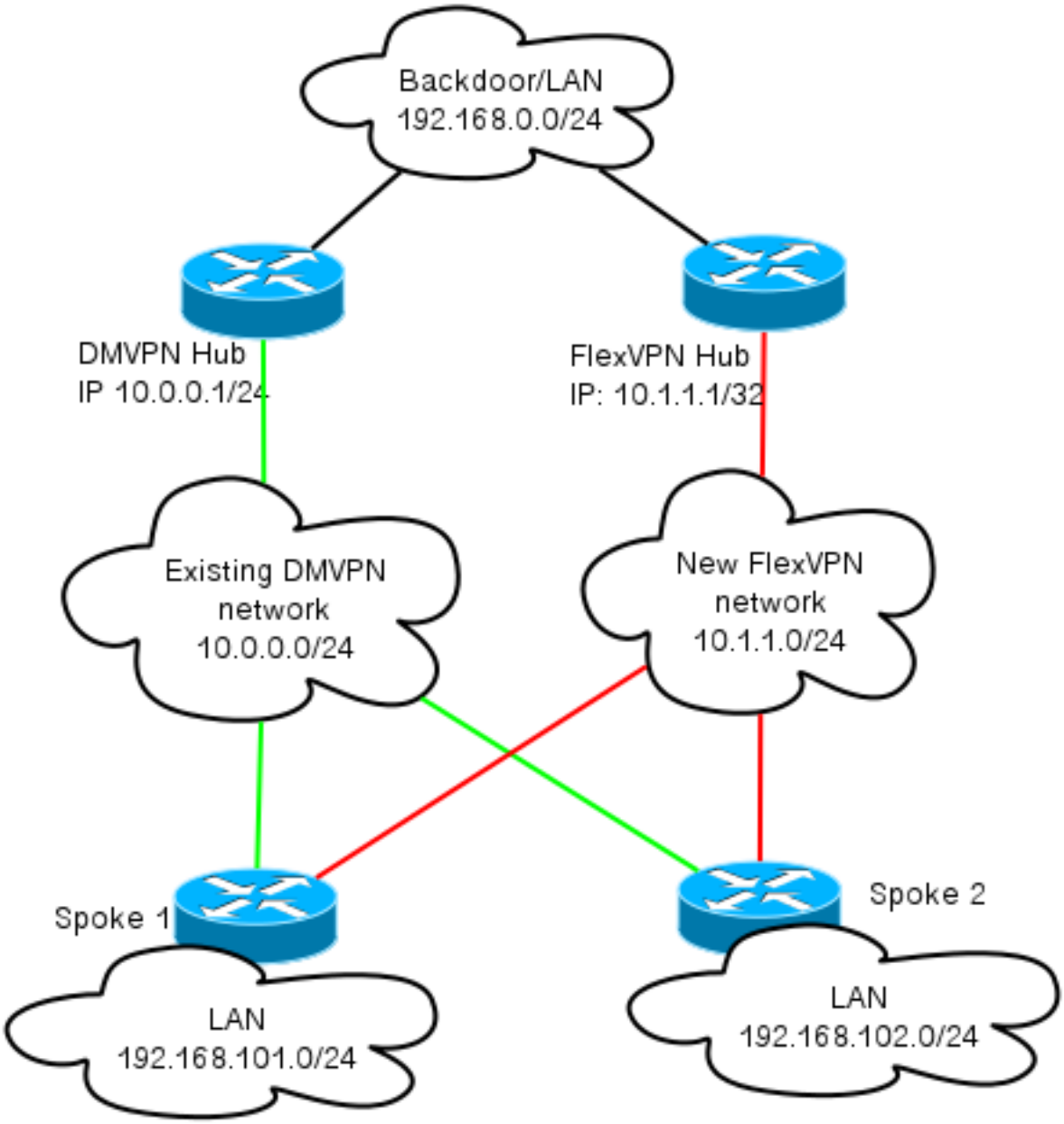
Il diagramma mostra la topologia di connessione tipica degli host su Internet. Per terminare la sessione IPsec DMVPN, viene usato l'indirizzo IP **loopback0** (**172.25.1.1**) dell'hub. L'indirizzo IP sul nuovo hub (**172.25.2.1**) viene utilizzato per FlexVPN.



Si noti il collegamento tra i due hub. Questo collegamento è cruciale per consentire la connettività tra i cloud FlexVPN e DMVPN durante la migrazione. Consente agli spoke già migrati a FlexVPN di comunicare con le reti DMVPN e viceversa.

Sovrapponi topologia di rete

Il diagramma della topologia mostra due cloud separati utilizzati per la sovrapposizione: DMVPN (connessioni verdi) e FlexVPN (connessioni rosse). I prefissi LAN vengono visualizzati per i siti corrispondenti. La subnet **10.1.1.0/24** non rappresenta una subnet effettiva in termini di indirizzamento dell'interfaccia, ma rappresenta un blocco di spazio IP dedicato al cloud FlexVPN. Le motivazioni alla base di questa operazione sono discusse più avanti nella sezione **Configurazione FlexVPN**.



Configurazione

In questa sezione vengono descritte le configurazioni di DMVPN e FlexVPN.

Configurazione DMVPN

In questa sezione viene descritta la configurazione di base per l'hub e lo spoke DMVPN.

La chiave già condivisa (PSK) viene utilizzata per l'autenticazione IKEv1. Una volta stabilito il protocollo IPsec, viene eseguita la registrazione del protocollo NHRP (Next Hop Resolution Protocol) da spoke a hub in modo che l'hub possa apprendere dinamicamente l'indirizzamento NBMA (Nonbroadcast Multiaccess) degli spoke.

Quando NHRP esegue la registrazione sul spoke e sull'hub, l'adiacenza di instradamento può essere stabilita e le route possono essere scambiate. Nell'esempio, il protocollo EIGRP viene usato come protocollo di routing di base per la rete di sovrapposizione.

Configurazione Spoke DMVPN

Qui è possibile trovare un esempio di configurazione di base di DMVPN con autenticazione PSK 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 Hub DMVPN

Nella configurazione hub, il tunnel viene originato da **loopback0** con indirizzo IP **172.25.1.1**. Il resto è una distribuzione standard di un 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 sicurezza (SA) di IPSec. IKEv2 offre miglioramenti rispetto a IKEv1, ad esempio la resilienza e il 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 un'interfaccia GRE multipoint statica. 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 basarsi su altri meccanismi per assicurarsi che l'hub e gli 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, viene introdotto il percorso as **/32** per l'indirizzo IP sull'altro lato del tunnel, che consente la comunicazione diretta spoke-to-hub.

In una migrazione rigida 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).

- Routing e inoltro virtuale (VRF) - La separazione VRF consente una maggiore flessibilità, ma non viene discussa in questa sede (opzionale).

Configurazione Spoke FlexVPN

Una delle differenze nella configurazione spoke di FlexVPN rispetto a DMVPN è che potenzialmente si hanno due interfacce. Sono necessari un tunnel per la comunicazione spoke-to-hub e un tunnel opzionale per i tunnel spoke-to-spoke. Se si sceglie di non utilizzare il tunneling spoke-to-spoke dinamico e si preferisce che tutto passi attraverso il dispositivo hub, è possibile rimuovere l'interfaccia del modello virtuale e rimuovere il passaggio rapido NHRP dall'interfaccia del tunnel.

Si noti che l'interfaccia del tunnel statico riceve un indirizzo IP in base alla negoziazione. Questo consente all'hub di fornire dinamicamente l'indirizzo IP dell'interfaccia del tunnel allo spoke 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
local identity fqdn spoke.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
```

> **Nota:** Per impostazione predefinita, l'identità locale viene impostata in modo da utilizzare l'indirizzo IP. Pertanto, anche l'istruzione match corrispondente nel peer deve corrispondere in base all'indirizzo. Se il requisito deve corrispondere in base al nome distinto (DN) nel certificato, la corrispondenza deve essere eseguita utilizzando una mappa dei certificati.

Cisco consiglia di utilizzare AES GCM con l'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 172.25.2.1
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
```

Infrastruttura a chiave pubblica (PKI, Public Key Infrastructure) è il metodo consigliato per eseguire l'autenticazione su larga scala in IKEv2. È tuttavia possibile utilizzare PSK purché se ne conoscano i limiti.

Di seguito è riportata una configurazione di esempio che utilizza **cisco** come chiave pubblica (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
virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

Configurazione hub FlexVPN

In genere, un hub termina solo i tunnel spoke-to-hub dinamici. Ecco perché non si trova un'interfaccia tunnel statica per FlexVPN nella configurazione hub. Viene invece utilizzata un'interfaccia di modello virtuale.

> **Nota:** Sul lato hub è necessario indicare gli indirizzi del pool da assegnare agli spoke.

Gli indirizzi di questo pool vengono aggiunti successivamente 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
local identity fqdn hub.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 con l'hardware che lo supporta.

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

Nota: In questa configurazione, 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 172.25.2.1 255.255.255.255
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
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 utilizzata per Spoke.

Nota: IKEv2 offre flessibilità in termini di autenticazione. Un lato può autenticarsi con PSK mentre l'altro usa la firma Rivest-Shamir-Adleman (RSA-SIG).

Se il requisito è l'utilizzo di chiavi già condivise per l'autenticazione, le modifiche alla configurazione sono simili a quelle descritte qui per il router spoke.

Connessione BGP inter-hub

Verificare che gli hub sappiano dove si trovano determinati prefissi. Questa operazione diventa sempre più importante in quanto alcuni spoke sono stati migrati a FlexVPN, mentre altri rimangono su DMVPN.

Di seguito è riportata la connessione BGP tra hub basata sulla configurazione dell'hub DMVPN:

```
router bgp 65001
network 192.168.0.0
neighbor 192.168.0.2 remote-as 65001
```

Migrazione del traffico

Eseguire la migrazione a BGP come protocollo di routing della sovrimpressione [consigliato]

BGP è un protocollo di routing basato sullo scambio unicast. Grazie alle sue caratteristiche, è il protocollo di scalabilità migliore nelle reti DMVPN.

Nell'esempio viene utilizzato il protocollo BGP (iBGP) interno.

Configurazione Spoke BGP

La migrazione del raggio è costituita da due parti. Innanzitutto, abilitare 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 sezione successiva) e l'apprendimento di nuovi prefissi su BGP, è possibile instradare il traffico dal cloud DMVPN corrente a un nuovo cloud FlexVPN.

Configurazione BGP hub

Hub FlexVPN - Configurazione BGP completa

Sull'hub, per evitare di mantenere separata la configurazione di prossimità per ogni spoke, configurare i listener dinamici. In questa configurazione, BGP non avvia nuove connessioni, ma accetta connessioni dal pool di indirizzi IP fornito. In questo caso, il pool indicato è **10.1.1.0/24**, ovvero tutti gli indirizzi del nuovo cloud FlexVPN.

Due punti da notare:

- L'hub FlexVPN annuncia prefissi specifici all'hub DMVPN; viene quindi utilizzata la mappa di rimozione.
- Annunciare la subnet FlexVPN di **10.1.1.0/24** alla tabella di routing o accertarsi che l'hub DMVPN veda l'hub FlexVPN come hop successivo.

Il documento illustra quest 'ultimo approccio.

```
access-list 1 permit any
route-map ALL permit 10
match ip address 1

route-map SET_NEXT_HOP permit 10
set ip next-hop 192.168.0.2

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

neighbor 192.168.0.1 remote-as 65001
neighbor 192.168.0.1 route-reflector-client
neighbor 192.168.0.1 unsuppress-map ALL
neighbor 192.168.0.1 route-map SET_NEXT_HOP out
```

Hub DMVPN - Configurazione completa BGP ed EIGRP

La configurazione sull'hub DMVPN è di base, in quanto riceve solo prefissi specifici dall'hub FlexVPN e annuncia i prefissi che apprende da EIGRP.

```
router bgp 65001
bgp log-neighbor-changes
redistribute eigrp 100
neighbor 192.168.0.2 remote-as 65001
```

Migrazione del traffico a BGP/FlexVPN

Come descritto in precedenza, per eseguire la migrazione è necessario arrestare la funzionalità DMVPN e attivare FlexVPN.

Questa procedura garantisce un impatto minimo:

1. In ogni raggio, separatamente, immettere quanto segue:

   ```
   interface tunnel 0
    shut
   ```

   A questo punto, verificare che non vi siano sessioni IKEv1 stabilite per questo spoke. Per verificare questa condizione, controllare l'output del comando **show crypto isakmp sa** e monitorare i messaggi syslog generati dal comando **crypto logging session**. Una volta confermato, è possibile procedere per visualizzare FlexVPN.

2. Nello stesso raggio, immetti questo:

   ```
   interface tunnel 1
     no shut
   ```

Fasi di verifica

Stabilità IPSec

Il modo migliore per valutare la stabilità di IPSec è monitorare i sylog con il comando di configurazione **crypto logging session** abilitato. Se vengono rilevate sessioni attive e non attive, è possibile che si tratti di un problema a livello IKEv2/FlexVPN che deve essere corretto prima di poter avviare la migrazione.

Informazioni BGP popolate

Se IPsec è stabile, verificare che la tabella BGP sia popolata con le voci degli spoke (sull'hub) e il riepilogo dall'hub (sugli spoke). Nel caso di BGP, ciò può essere visualizzato con questi comandi:

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

Di seguito è riportato un esempio di informazioni corrette provenienti dall'hub FlexVPN:

```
BGP router identifier 172.25.2.1, local AS number 65001
(...omitted...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
*10.1.1.100 4 65001 112 123 16 0 0 01:35:58 1
192.168.0.1 4 65001 97 99 16 0 0 01:24:12 4
```

L'output mostra che l'hub ha appreso un prefisso da ciascuno dei raggi ed entrambi i raggi sono dinamici e contrassegnati da un asterisco (*). Mostra inoltre che viene ricevuto un totale di quattro prefissi dalla connessione tra hub.

Di seguito è riportato un esempio di informazioni simili tratte da the spoke:

```
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 120 109 57 0 0 01:33:23 2
```

Spoke ha ricevuto due prefissi dall'hub. Nel caso di questa configurazione, un prefisso dovrebbe essere il riepilogo annunciato sull'hub FlexVPN. L'altro è la rete DMVPN 10.0.0.0/24 ridistribuita sulla DMVPN spoke in BGP.

Migrazione ai nuovi tunnel con EIGRP

EIGRP è una scelta popolare nelle reti DMVPN grazie alla sua installazione relativamente semplice e alla rapida convergenza. Tuttavia, ha una scalabilità peggiore di BGP e non offre molti meccanismi avanzati che possono essere utilizzati da BGP immediatamente. La sezione successiva descrive uno dei modi per passare a FlexVPN con un nuovo processo EIGRP.

Configurazione spoke aggiornata

Viene aggiunto un nuovo sistema autonomo (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: È meglio non stabilire l'adiacenza del protocollo di routing sui tunnel spoke. Pertanto,

impostare solo l'interfaccia di **tunnel1** (spoke-to-hub) in modo non passivo.

Configurazione hub FlexVPN aggiornata

Analogamente, per l'hub FlexVPN, preparare il protocollo di routing nell'appliance ASA appropriata, corrispondente a quello configurato sugli spoke.

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

Esistono due metodi per fornire un riepilogo verso il raggio.

- Ridistribuire una route statica che punta a **null0** (opzione preferita).

```
ip route 192.168.0.0 255.255.0.0 null 0
ip route 10.1.1.0 255.255.255.0 null 0

ip prefix-list EIGRP_SUMMARY_ONLY seq 5 permit 192.168.0.0/16
ip prefix-list EIGRP_SUMMARY_ONLY seq 10 permit 10.1.1.0/24

route-map EIGRP_SUMMARY permit 20
match ip address prefix-list EIGRP_SUMMARY_ONLY

router eigrp 200
distribute-list route-map EIGRP_SUMMARY out Virtual-Template1
redistribute static metric 1500 10 10 1 1500 route-map EIGRP_SUMMARY
```

Questa opzione consente il controllo del riepilogo e della ridistribuzione senza modifiche alla configurazione della tecnologia di virtualizzazione (VT) dell'hub. Questa operazione è importante perché la configurazione della VT dell'hub non può essere modificata se è associato un accesso virtuale attivo.

- Impostare un indirizzo di riepilogo di tipo DMVPN in un modello virtuale.

Questa configurazione *non* è *consigliata*, a causa dell'elaborazione interna e della replica di tale riepilogo in ogni accesso virtuale. Qui è mostrato come riferimento.

```
interface Virtual-Template1 type tunnel
 ip summary-address eigrp 200 192.168.0.0 255.255.0.0
```

Un altro aspetto da considerare è lo scambio di routing tra hub. A tale scopo, è possibile ridistribuire le istanze EIGRP su iBGP.

DMVPN Hub - Configurazione BGP aggiornata

La configurazione rimane di base. È necessario ridistribuire prefissi specifici da EIGRP a BGP:

```
router bgp 65001

redistribute eigrp 100

neighbor 192.168.0.2 remote-as 65001
```

Hub FlexVPN - Configurazione BGP aggiornata

Analogamente all'hub DMVPN, in FlexVPN è necessario ridistribuire i prefissi del nuovo processo EIGRP in BGP:

```
router bgp 65001

 redistribute eigrp 200 redistribute static

 neighbor 192.168.0.1 remote-as 65001
```

Migrazione del traffico a FlexVPN

Per eseguire la migrazione, è necessario arrestare la funzionalità DMVPN e attivare FlexVPN su ogni spoke, uno alla volta. Questa procedura garantisce un impatto minimo:

1. In ogni raggio, separatamente, immettere quanto segue:

   ```
   interface tunnel 0
    shut
   ```

   A questo punto, verificare che non vi siano sessioni IKEv1 stabilite su questo spoke. Per verificare questa condizione, controllare l'output del comando **show crypto isakmp sa** e monitorare i messaggi syslog generati dal comando **crypto logging session**. Una volta confermato, è possibile procedere per visualizzare FlexVPN.
2. Nello stesso raggio, immetti questo:

   ```
   interface tunnel 1
     no shut
   ```

Fasi di verifica

Stabilità IPSec

Come nel caso di BGP, è necessario valutare se IPsec è stabile. Il modo migliore per farlo è monitorare i sylog con il comando di configurazione **crypto logging session** abilitato. Se le sessioni diventano attive e inattive, è possibile che si sia verificato un problema a livello 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 riepilogo sugli spoke. È possibile verificare questa condizione se si immette questo comando negli

hub e negli spoke:

show ip eigrp [AS_NUMBER] topology

Di seguito è riportato un esempio dell'output del raggio:

```
Spoke1#show ip eigrp 200 topology
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)
via 10.1.1.1 (26240000/128256), Tunnel1

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 (26114560/2562560), Tunnel1

P 10.1.1.100/32, 1 successors, FD is 26112000
via Connected, Tunnel1

P 10.1.1.0/24, 1 successors, FD is 26114560
via 10.1.1.1 (26114560/2562560), Tunnel1
```

L'output mostra che il spoke conosce la propria subnet LAN (in *corsivo*) e i relativi riepiloghi (in **grassetto**).

Di seguito è riportato un esempio di output dell'hub:

```
hub2# show ip eigrp 200 topology
EIGRP-IPv4 Topology Table for AS(200)/ID(172.25.2.1)
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, Loopback200

P 192.168.101.0/24, 1 successors, FD is 26905600
via 10.1.1.100 (26905600/281600), Virtual-Access1

P 192.168.0.0/16, 1 successors, FD is 2562560
via Rstatic (2562560/0)

P 10.1.1.0/24, 1 successors, FD is 2562560
via Rstatic (2562560/0)
```

L'output mostra che l'hub è a conoscenza delle subnet LAN degli spoke (in *corsivo*), del prefisso di riepilogo pubblicizzato (in **grassetto**) e dell'indirizzo IP assegnato a ciascun spoke tramite negoziazione.

Ulteriori considerazioni

Tunnel spoke-to-spoke già esistenti

Poiché la chiusura dell'interfaccia del tunnel DMVPN determina la rimozione delle voci NHRP, i tunnel spoke già esistenti verranno eliminati.

Cancella voci NHRP

Un hub FlexVPN non si basa sul processo di registrazione NHRP dallo spoke per sapere come instradare il traffico indietro. Tuttavia, i tunnel spoke dinamici si basano su voci NHRP.

In DMVPN, se NHRP sull'hub viene cancellato, possono verificarsi problemi di connettività di breve durata. In FlexVPN, se si cancella NHRP sugli spoke, la sessione IPsec di FlexVPN, relativa ai tunnel spoke-to-spoke, verrà terminata. La cancellazione di NHRP sull'hub non ha alcun effetto sulla sessione FlexVPN.

Infatti, 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 spoke potrebbe essere influenzato dall'ID bug Cisco CSCub07382.

Informazioni correlate

- Esempio di configurazione della migrazione soft da DMVPN a FlexVPN
- Documentazione e supporto tecnico – Cisco Systems