Configurazione e verifica della soluzione FlexVPN

Sommario

Introduzione

Questo documento descrive l'ambiente Flex Virtual Private Network, ne introduce le funzionalità e spiega come configurare ciascuna topologia FlexVPN.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco IOS e Cisco IOS XE
- IKE (Internet Key Exchange) versione 2
- IPsec (Internet Protocol Security)
- FlexVPN

Componenti usati

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

- Cisco IOS XE Amsterdam-17.3.6

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

FlexVPN è una soluzione VPN versatile e completa fornita da Cisco, progettata per offrire un framework unificato per vari tipi di connessioni VPN. Basato sul protocollo IKEv2 (Internet Key Exchange versione 2), FlexVPN è progettato per semplificare la configurazione, la gestione e l'installazione della VPN, utilizzando un insieme coerente di strumenti; gli stessi comandi e passaggi di configurazione si applicano a diversi tipi di VPN (site-to-site, accesso remoto e così via). Questa coerenza consente di ridurre gli errori e rende il processo di installazione più intuitivo.

IKEV2 E IKEV1

FlexVPN sfrutta la tecnologia IKEv2, che supporta algoritmi di crittografia moderni, ad esempio AES (Advanced Encryption Standard) e SHA-256 (Secure Hash Algorithm). Questi algoritmi forniscono una crittografia efficace e l'integrità dei dati, proteggendo i dati trasmessi sulla VPN dall'intercettazione o dalla manomissione.

IKEv2 offre più metodi di autenticazione rispetto a IKEv1. Oltre alla chiave già condivisa (PSK) e ai tipi di autenticazione ibrida e basata su certificati, IKEv2 consente al risponditore di utilizzare il protocollo EAP (Extensible Authentication Protocol) per l'autenticazione del client.

In FlexVPN, EAP viene utilizzato per l'autenticazione del client, il router funge da relay, passando messaggi EAP tra il client e il server EAP backend, in genere un server RADIUS. FlexVPN supporta vari metodi EAP, tra cui EAP-TLS, EAP-PEAP, EAP-PSK e altri, per proteggere il processo di autenticazione.

Nella tabella vengono illustrate le differenze tra le funzioni IKEv1 e IKEv2:

	IKEv2	IKEv1
Messaggi di definizione del	4 messaggi	6 messaggio

protocollo		
Supporto EAP	Sì (2 messaggi aggiuntivi)	No
Negoziazione per le associazioni di sicurezza	2 messaggi aggiuntivi	3 messaggio aggiuntivo
Esecuzione su UDP 500/4500	Sì	Sì
NAT Traversal (NAT-T)	Sì	Sì
Funzioni di ritrasmissione e riconoscimento	Sì	Sì
Protezione dell'identità, meccanismo di protezione DoS e PFS (Perfect Forward Secrecy)	Sì	Sì
Supporto dei dispositivi di crittografia di nuova generazione	Sì	No

Scalabilità

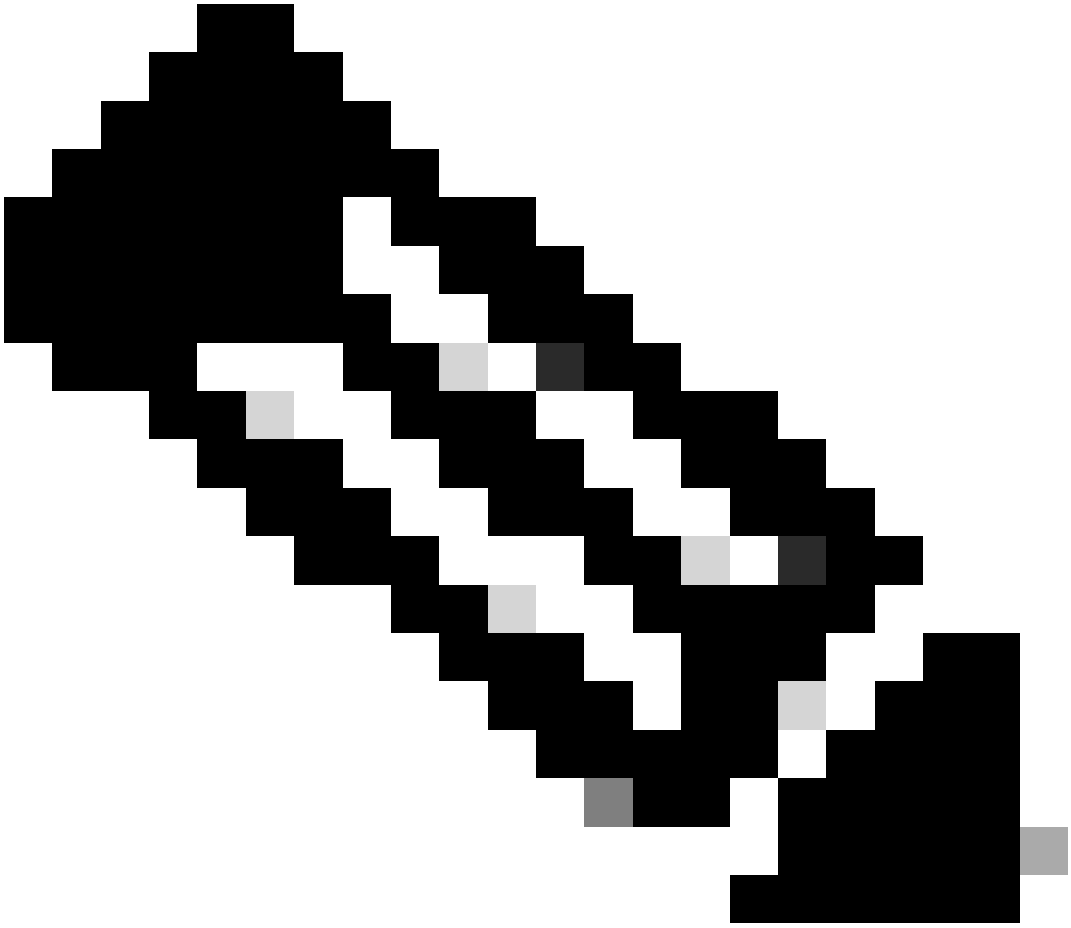
FlexVPN può essere facilmente espansa dalle reti dei piccoli uffici a quelle delle grandi aziende. Questa caratteristica la rende la scelta ideale per le organizzazioni con un numero significativo di utenti remoti che richiedono un accesso alla rete sicuro e affidabile.

Caratteristiche principali

- Configurazione dinamica e tunnel on-demand:
  - Connessione FlexVPN avviata. Il sistema genera un'interfaccia di accesso virtuale basata su un modello preconfigurato. Questa interfaccia funge da endpoint del tunnel per la durata della connessione. Quando il tunnel non è più necessario, l'interfaccia di accesso virtuale viene disattivata, liberando risorse di sistema.

- Flessibilità nell'implementazione:
  - Modello hub e spoke: Un hub centrale si connette a più filiali. FlexVPN semplifica la configurazione di queste connessioni con un unico framework, rendendolo ideale per reti di grandi dimensioni.
  - Topologie Mesh completa e Mesh parziale: Tutti i siti possono comunicare direttamente senza passare attraverso un hub centrale, riducendo i ritardi e migliorando le prestazioni.

- Alta disponibilità e ridondanza:
  - Hub ridondanti: Supporto di più hub per il backup. In caso di guasto di un hub, le filiali possono connettersi a un altro hub, garantendo una connettività continua.
  - Bilanciamento del carico: In questo modo le connessioni VPN vengono distribuite su più dispositivi per evitare il sovraccarico di un singolo dispositivo, fondamentale per mantenere le prestazioni in installazioni di grandi dimensioni.



Nota: Nella guida successiva vengono fornite ulteriori informazioni sulla configurazione per il bilanciamento del carico per la connessione Hub.

Configurazione del servizio di bilanciamento del carico IKEv2

- Autenticazione e autorizzazione scalabili:
  - Integrazione AAA: Funziona con server AAA come Cisco ISE o RADIUS per la gestione centralizzata di credenziali e policy utente, essenziali per l'utilizzo su larga scala.
  - PKI e certificati: Supporta l'infrastruttura a chiave pubblica (PKI) e i certificati digitali per un'autenticazione sicura, più scalabile rispetto all'utilizzo della chiave precondivisa, soprattutto in ambienti di grandi dimensioni.

Routing

La funzionalità di routing di FlexVPN è progettata per migliorare la scalabilità e per gestire in modo efficiente più connessioni VPN e consentire un modo dinamico per indirizzare il traffico a ognuna

di esse. I successivi componenti e meccanismi chiave che rendono il routing FlexVPN efficiente:

- Interfaccia modello virtuale: Questo è un modello di configurazione che include tutte le impostazioni necessarie per una connessione VPN, ad esempio l'assegnazione dell'indirizzo IP, l'origine del tunnel e le impostazioni IPsec. In questa interfaccia viene configurato il comando per`ip unnumbered`prendere in prestito un indirizzo IP, in genere da un loopback anziché configurare un indirizzo IP specifico come origine del tunnel. In questo modo, lo stesso modello può essere utilizzato da ciascun spoke, consentendo a ciascun spoke di utilizzare il proprio indirizzo IP di origine.

- Interfaccia di accesso virtuale: Si tratta di interfacce create in modo dinamico che ereditano le relative impostazioni dall'interfaccia del modello virtuale. Ogni volta che viene stabilita una nuova connessione VPN, viene creata una nuova interfaccia di accesso virtuale basata sul modello virtuale. Ciò significa che ogni sessione VPN ha la propria interfaccia unica, che semplifica la gestione e la scalabilità.

- Protocolli di routing dinamico: Funziona con protocolli di routing come OSPF, EIGRP e BGP su tunnel VPN. In questo modo le informazioni di routing vengono aggiornate automaticamente, un aspetto importante per le reti grandi e dinamiche.

- IKEv2 annuncia le route consentendo al server FlexVPN di eseguire il push degli attributi di rete al client, che installa le route sull'interfaccia del tunnel. Il client comunica inoltre le proprie reti al server durante lo scambio della modalità di configurazione, abilitando gli aggiornamenti del percorso su entrambe le estremità.

- NHRP (Next Hop Resolution Protocol) è un protocollo di risoluzione degli indirizzi dinamico utilizzato nelle topologie Hub e Spoke per mappare gli indirizzi IP pubblici agli endpoint VPN privati. Consente agli spoke di rilevare altri IP spoke per la comunicazione diretta.

Criteri di autorizzazione

È possibile configurare un criterio di autorizzazione IKEv2 per FlexVPN per controllare vari aspetti della connessione VPN. Un criterio di autorizzazione IKEv2 definisce il criterio di autorizzazione locale e contiene gli attributi locale e/o remoto:

- Gli attributi locali, come il routing e l'inoltro VPN (VRF) e il criterio QOS, vengono applicati localmente.
- Gli attributi remoti, ad esempio i percorsi, vengono inviati al peer tramite la modalità di configurazione.
- Utilizzare il comando crypto ikev2 authorization policy per definire il criterio locale.
- I criteri di autorizzazione IKEv2 vengono richiamati dal profilo IKEv2 tramite il comando AAA authorization.

In questa tabella viene fornita una panoramica dei parametri chiave che è possibile configurare nel criterio di autorizzazione IKEv2.

Parametro	Descrizione
AAA	Integrazione con i server AAA per la convalida

	delle credenziali utente, l'autorizzazione di accesso e l'utilizzo dell'account. Il criterio può specificare se la convalida viene eseguita localmente sul router o in remoto, ad esempio tramite un server RADIUS.
Configurazione client	Invia le impostazioni di configurazione al client, ad esempio i valori di timeout di inattività, i valori keepalive, l'assegnazione di server DNS e WINS e così via.
Configurazione specifica del client	Consente configurazioni diverse per client diversi in base all'identità o all'appartenenza ai gruppi.
Set route	Questa configurazione consente al traffico di passare attraverso il tunnel VPN. In questo modo viene eseguito il routing injection inviato al client VPN al completamento della connessione.

FlexVPN rispetto ad altre tecnologie

FlexVPN offre una gamma di vantaggi che la rendono una scelta interessante per gli ambienti di rete moderni. Fornendo un framework unificato, FlexVPN semplifica la configurazione e la gestione, migliora la sicurezza, supporta la scalabilità, garantisce l'interoperabilità e riduce la complessità.

	Mappa crittografica	DMVPN	FlexVPN
Routing dinamico	No	Sì	Sì
Spoke-to-Spoke dinamico diretto	No	Sì	Sì
VPN ad accesso remoto	Sì	No	Sì
Push di configurazione	No	No	Sì
Configurazione peer	No	No	Sì
Qos Peer-peer	No	Sì	Sì
Integrazione server AAA	No	No	Sì

Esempio di rete

FlexVPN consente la creazione di tunnel tra i dispositivi, stabilendo la comunicazione tra l'hub e gli spoke. Consente inoltre la creazione di tunnel per la comunicazione diretta tra gli spoke e la connessione per gli utenti VPN ad accesso remoto, come mostrato nel diagramma.

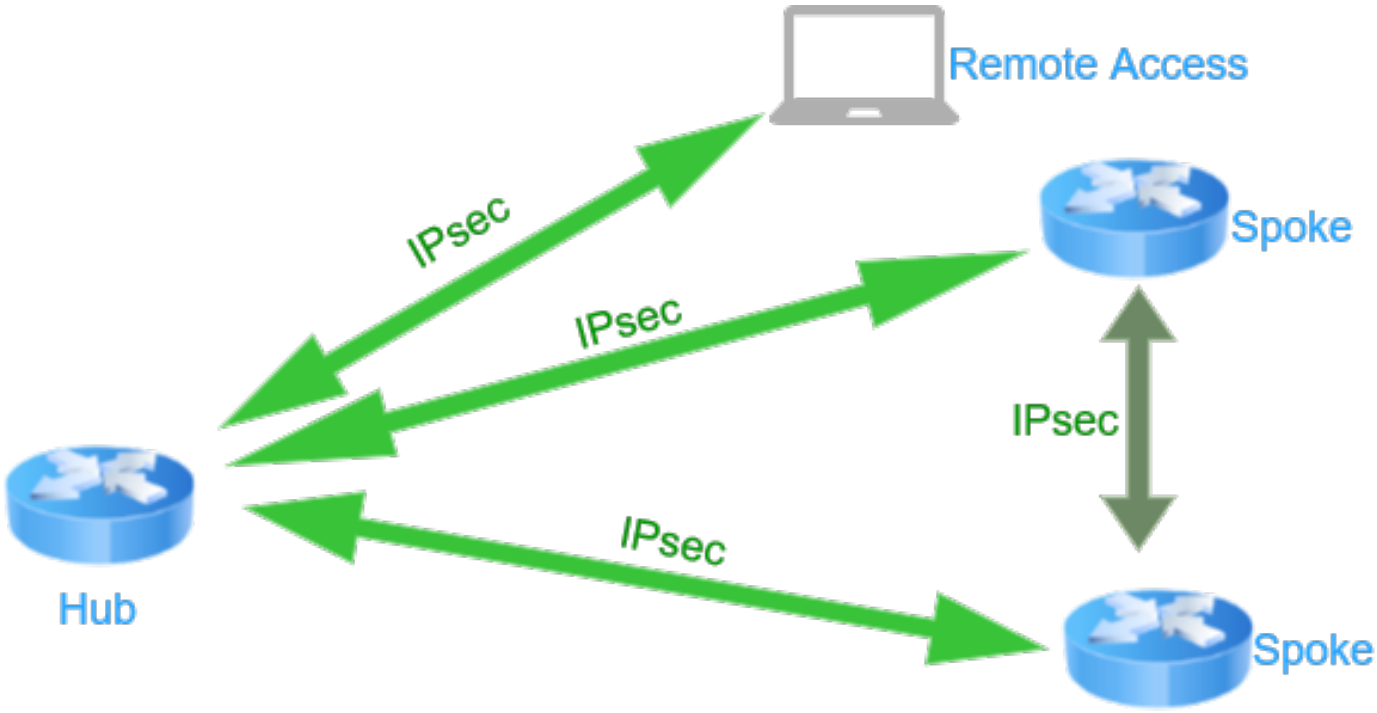
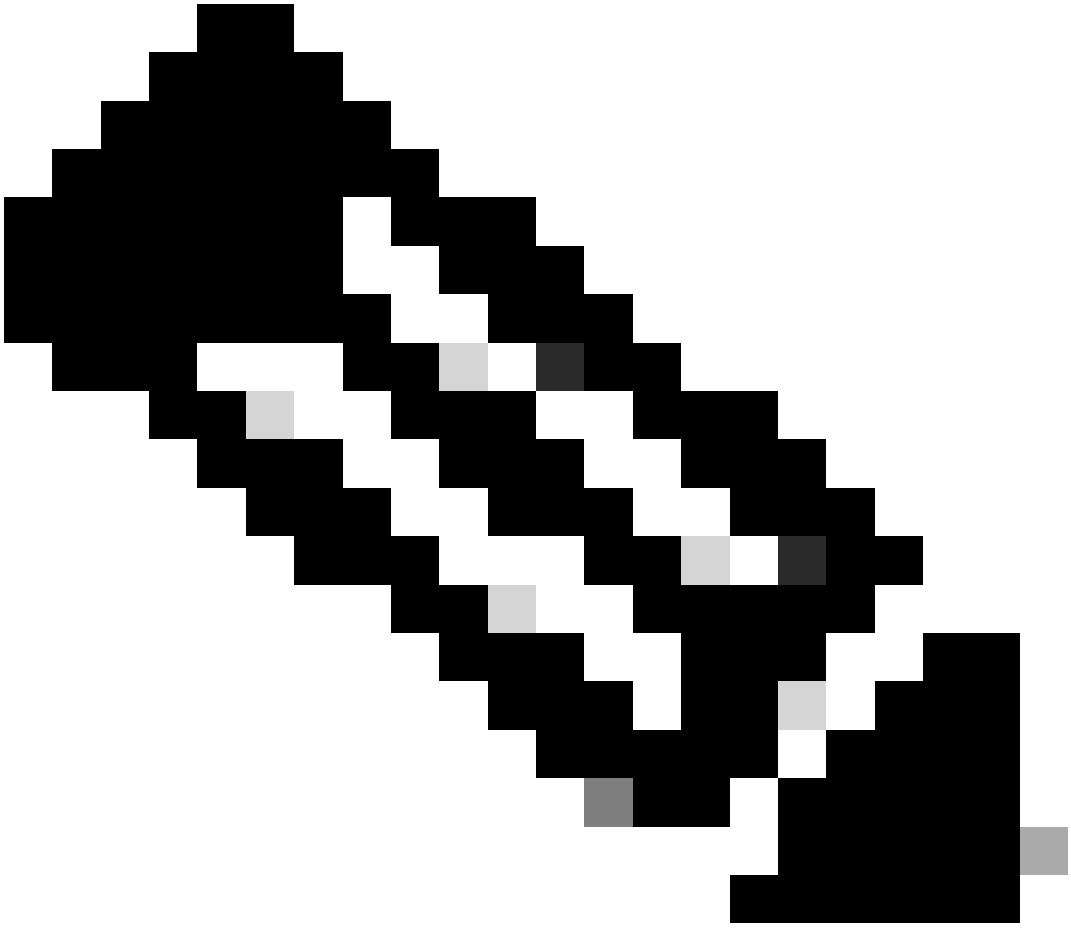


Diagramma FlexVPN



Nota: La configurazione della VPN ad accesso remoto non è illustrata in questa guida. Per i dettagli relativi alla configurazione, consultare la guida:

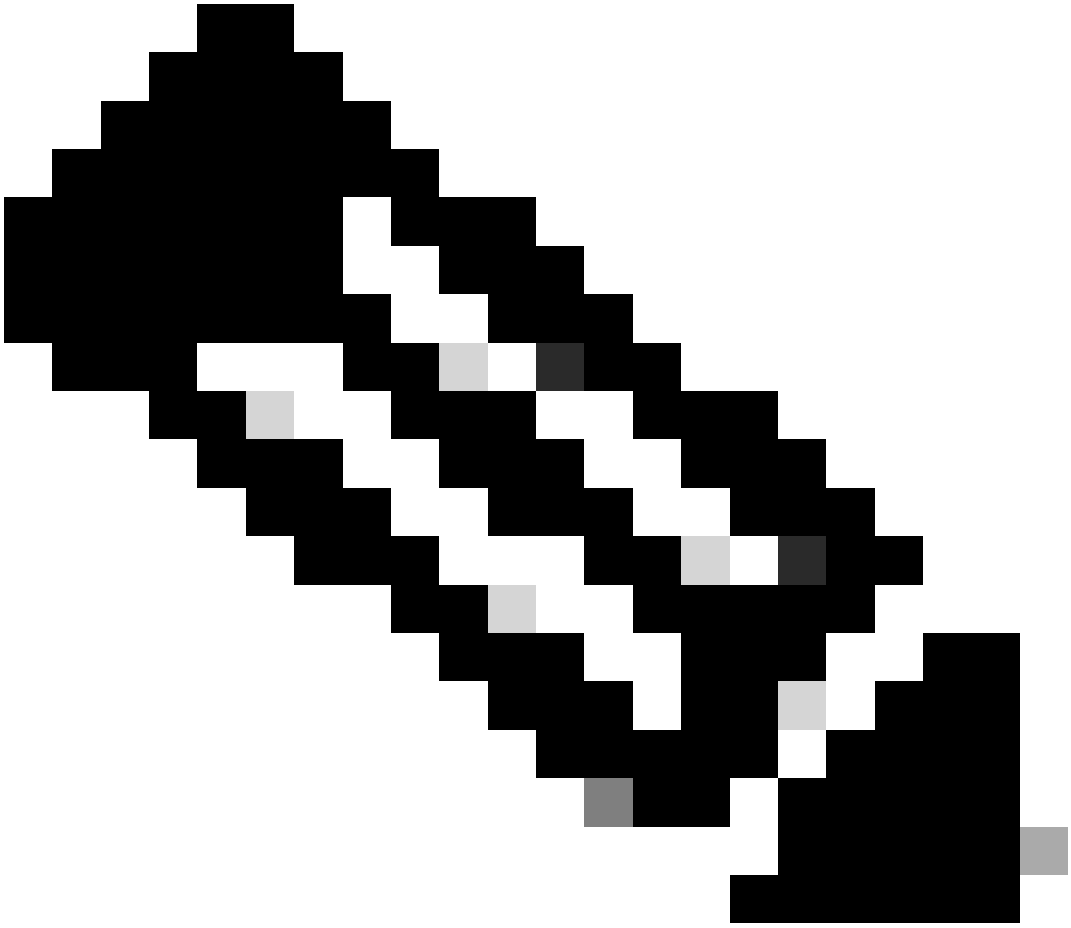
Configurazione dell'headend FlexVPN per l'accesso remoto AnyConnect IKEv2 del client sicuro con il database degli utenti locali

Configurazione

FlexVPN è caratterizzata dalla semplicità della sua configurazione. Questa semplicità è evidente nei blocchi di configurazione coerenti utilizzati per vari tipi di VPN. FlexVPN fornisce blocchi di configurazione semplici, generalmente applicabili, con configurazioni opzionali o passaggi aggiuntivi disponibili a seconda delle caratteristiche o dei requisiti specifici della topologia:

- Proposta IKEv2: Definisce gli algoritmi utilizzati nella negoziazione dell'associazione di sicurezza (SA, Security Association) IKEv2. Dopo la creazione, allegare la proposta a un criterio IKEv2 in modo che venga selezionata durante la negoziazione.

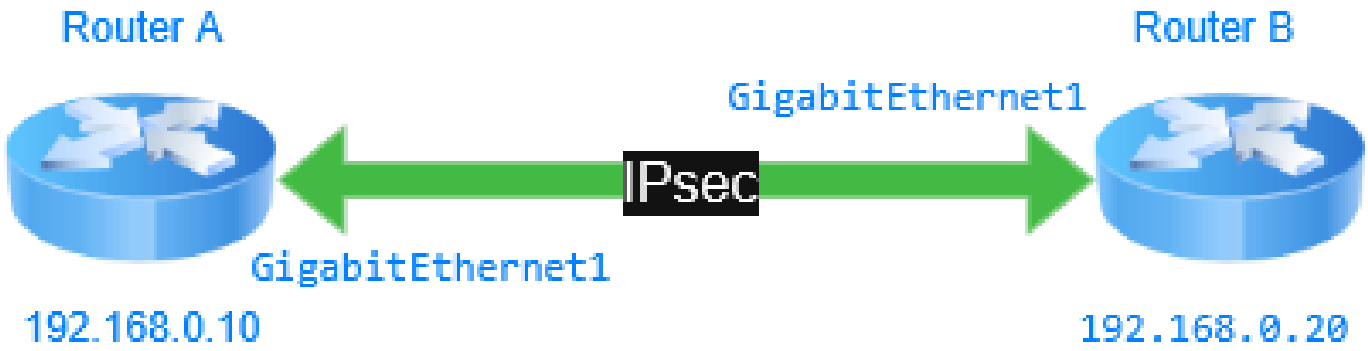
- Criteri IKEv2: Collega la proposta a un'istanza VRF (Virtual Routing and Forwarding) o a un indirizzo IP locale. Collegamento di criterio alla proposta IKEv2.
- Keyring IKEv2: Specifica le chiavi già condivise (PSK), che possono essere asimmetriche se utilizzate per l'autenticazione peer.
- Trustpoint (facoltativo): Configura gli attributi di identità e Autorità di certificazione (CA) per l'autenticazione peer quando si utilizza l'infrastruttura a chiave pubblica (PKI) come metodo di autenticazione.
- Integrazione AAA (opzionale): FlexVPN integra come metodo di autenticazione i server AAA, ad esempio Cisco ISE (Identity Services Engine) o RADIUS.
- Profilo IKEv2: Archivia i parametri non negoziabili dell'associazione di sicurezza IKE, ad esempio l'indirizzo peer VPN e i metodi di autenticazione. Poiché non esiste un profilo IKEv2 predefinito, è necessario configurarne uno e collegarlo a un profilo IPsec sull'iniziatore. Se si utilizza l'autenticazione PSK, il profilo IKEv2 fa riferimento al keyring IKEv2. Se si utilizza l'autenticazione PKI o il metodo di autenticazione AAA, fare riferimento a questa sezione.
- Set di trasformazioni IPSec: Specifica una combinazione di algoritmi accettabile per l'associazione di protezione IPSec.
- Profilo IPSec: Consolida le impostazioni di FlexVPN in un unico profilo che può essere applicato a un'interfaccia. Questo profilo fa riferimento al set di trasformazioni IPSec e al profilo IKEv2.



Nota: Gli esempi di configurazione utilizzano chiavi già condivise per fornire una dimostrazione immediata della configurazione e della semplicità di FlexVPN. Mentre le chiavi già condivise possono essere utilizzate per semplificare l'installazione e le topologie di piccole dimensioni, i metodi AAA o PKI sono più adatti per le topologie di grandi dimensioni.

Configurazione FlexVPN da sito a sito

La topologia da sito a sito di FlexVPN è progettata per le connessioni VPN dirette tra due siti. Ogni sito è dotato di un'interfaccia tunnel che stabilisce un canale sicuro attraverso il quale può passare il traffico. La configurazione spiega come stabilire una connessione VPN diretta tra due siti, come mostrato nel diagramma.



Diagramma_sito

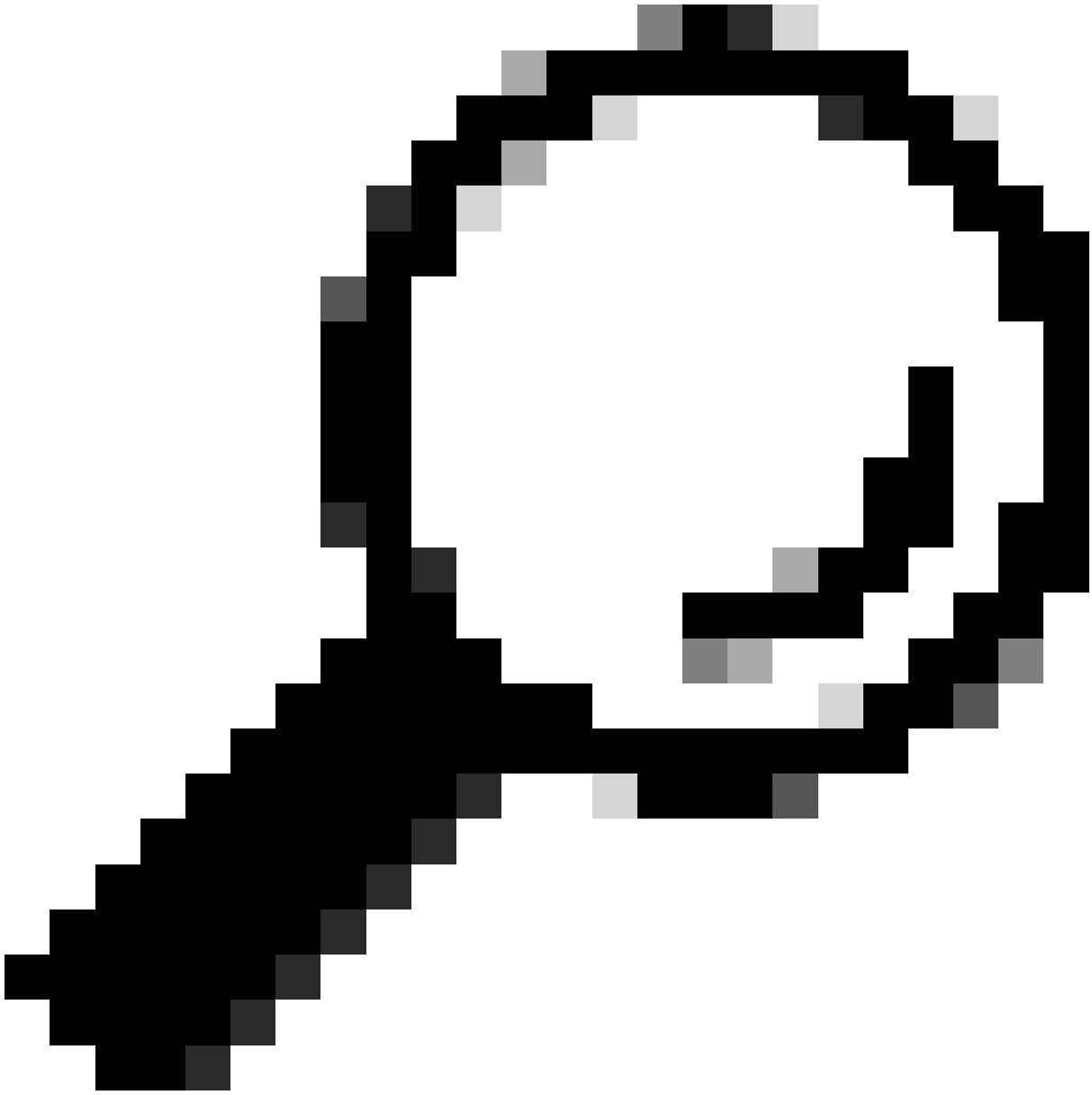
Passaggio 1: Configurazione router A

r. Definire la proposta e il criterio IKEv2.

b. Configurare un keyring e immettere un nome Pre-Shared Key utilizzato per autenticare il peer.

c. Creare un IKEv2 profile e assegnare il keyringfile.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 192.168.0.20
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
crypto ikev2 profile FLEXVPN_PROFILE
match identity remote address 192.168.0.20
authentication remote pre-share
authentication local pre-share
keyring local FLEXVPN_KEYRING
lifetime 86400
dpd 10 2 on-demand
!
```



Suggerimento: Questa **IKEv2 Smart Defaults** funzione riduce al minimo la configurazioneFlexVPNin quanto copre la maggior parte degli use case. È possibile eseguire la personalizzazione in base **IKEv2 Smart Defaults** a scenari di utilizzo specifici, sebbene Cisco non consigli questa procedura.

d. Creare un Transport Set e definire gli algoritmi di crittografia e hash utilizzati per proteggere i dati.

e. Creare un **IPsec profile**file.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
```

```
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

f. Configurare l'interfaccia del tunnel.

```
!
interface Tunnel0
 ip address 10.1.120.10 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.20
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
 ip address 192.168.0.10 255.255.255.0
!
```

g. Configurare il routing dinamico per annunciare l'interfaccia del tunnel. In seguito, può annunciare altre reti che devono passare attraverso il tunnel.

```
router eigrp 100
 no auto-summary
 network 10.1.120.0 0.0.0.255
```

Passaggio 2: Configurazione router B

r. Definire la proposta e il criterio IKEv2.

b. Configurare un keyring elemento e immettere un Pre-Shared Key elemento utilizzato per autenticare il peer.

c. Creare un IKEv2 profile e assegnare il keyringfile.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 192.168.0.10
pre-shared-key local cisco123
pre-shared-key remote cisco123
```

```
!
crypto ikev2 profile FLEXVPN_PROFILE
match identity remote address 192.168.0.10
authentication remote pre-share
authentication local pre-share
keyring local FLEXVPN_KEYRING
lifetime 86400
dpd 10 2 on-demand
!
```

d. Creare un Transport Set e definire gli algoritmi di crittografia e hash utilizzati per proteggere i dati.

e. Creare un IPsec profile e assegnare il profilo IKEv2 e il set di trasformazioni creati in precedenza.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

f. Configurare il Tunnel interfacefile.

```
!
interface Tunnel0
 ip address 10.1.120.20 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
 ip address 192.168.0.20 255.255.255.0
!
```

g. Configurare il routing dinamico per annunciare l'interfaccia del tunnel. In seguito, può annunciare altre reti che devono passare attraverso il tunnel.

```
router eigrp 100
 no auto-summary
 network 10.1.120.0 0.0.0.255
```

Verifica

- Usare il comando show ip interface brief per esaminare lo stato dell'interfaccia del tunnel e verificare che il tunnel sia in stato attivo/attivo.

<#root>

```
RouterB#
```

show ip interface brief

```
Interface              IP-Address      OK?   Method    Status   Protocol
GigabitEthernet1       192.168.0.20    YES   NVRAM     up       up
Tunnel0                10.1.120.11     YES   manual
```

up

```
 up
```

1. Per verificare che la connessione protetta tra i router sia stata stabilita, usare il comando show crypto ikev2 sa.

<#root>

```
RouterB#
```

show crypto ikev2 sa

```
IPv4 Crypto IKEv2 SA

Tunnel-id  Local                Remote               fvrf/ivrf   Status
2          192.168.0.20/500     192.168.0.10/500     none/none
```

READY

```
    Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
```

Life/Active Time: 86400/3139 sec

```
IPv6 Crypto IKEv2 SA
```

- Utilizzare il comando show crypto ipsec sa per confermare che il traffico è crittografato e che sta passando attraverso il tunnel, verificando che i contatori encaps e decaps siano in aumento.

<#root>

```
RouterB#
```

show crypto ipsec sa

```
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.168.0.20

   protected vrf: (none)
   local ident (addr/mask/prot/port): (192.168.0.20/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.0.10/255.255.255.255/47/0)
   current_peer 192.168.0.10 port 500
     PERMIT, flags={origin_is_acl,}


#pkts encaps: 669, #pkts encrypt: 669, #pkts digest: 669




#pkts decaps: 668, #pkts decrypt: 668, #pkts verify: 668


    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

      local crypto endpt.: 192.168.0.20, remote crypto endpt.: 192.168.0.10
      plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
      current outbound spi: 0x93DCB8AE(2480715950)
      PFS (Y/N): N, DH group: none

      inbound esp sas:


spi: 0x89C141EB(2311143915)


         transform: esp-256-aes esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 5578, flow_id: CSR:3578, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0


sa timing: remaining key lifetime (k/sec): (4607913/520)


         IV size: 16 bytes
         replay detection support: Y


Status: ACTIVE(ACTIVE)



      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:


spi: 0x93DCB8AE(2480715950)


         transform: esp-256-aes esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 5577, flow_id: CSR:3577, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0
```

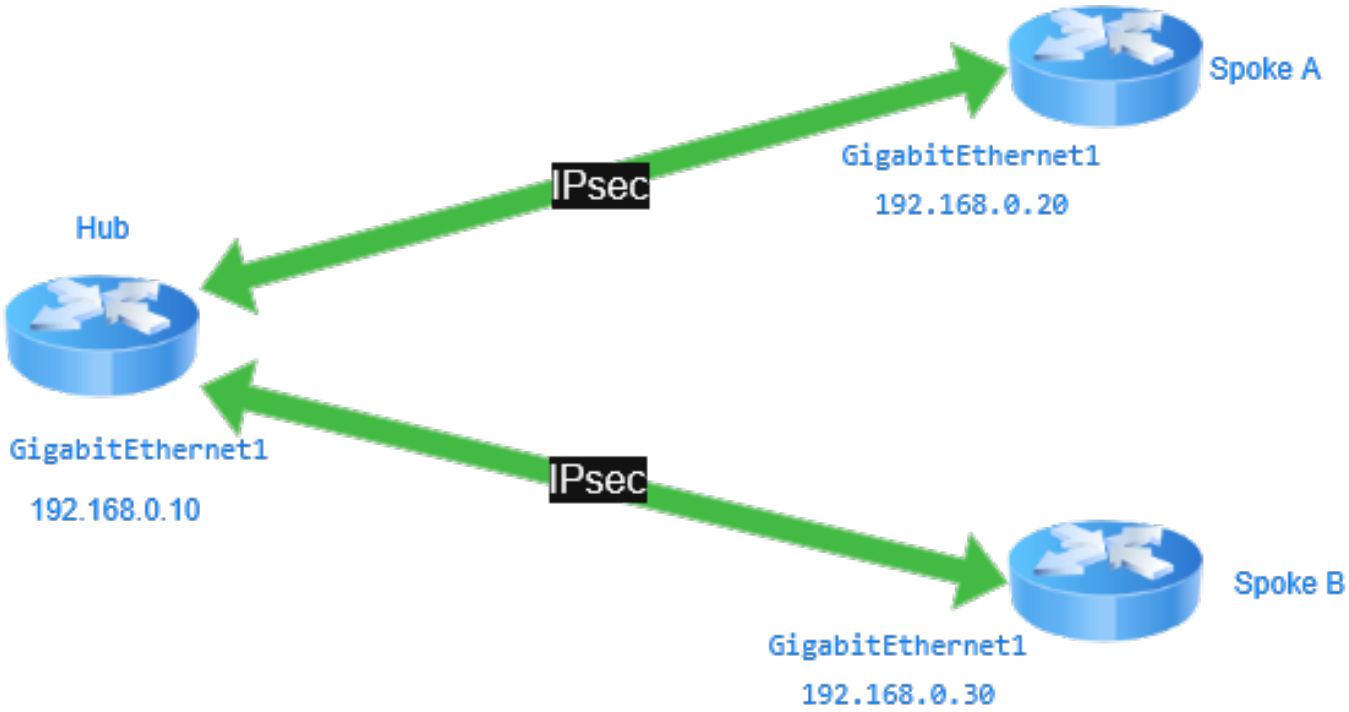
```
sa timing: remaining key lifetime (k/sec): (4607991/3137)

         IV size: 16 bytes
         replay detection support: Y

Status: ACTIVE(ACTIVE)


      outbound ah sas:

      outbound pcp sas:
```

- Per verificare che l'adiacenza EIGRP sia stabilita con l'altro sito, usare il comando show ip eigrp neighbors.

```
RouterB#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface              Hold  Uptime     SRTT    RTO    Q   Seq
                                                   (sec)            (ms)          Cnt  Num
0   10.1.120.10             Tu0                     13   00:51:26    3      1470   0   2
```

FlexVPN Hub-and-Spoke

Nella topologia hub e spoke, più router spoke si connettono a un router hub centrale. Questa configurazione è ottimale per gli scenari in cui gli spoke comunicano principalmente con l'hub. In FlexVPN, i tunnel dinamici possono essere configurati per migliorare l'efficienza delle comunicazioni. L'hub utilizza il routing IKEv2 per distribuire le route ai router spoke, garantendo una connettività ininterrotta. Come indicato nel diagramma, la configurazione spiega la connessione VPN tra un hub e spoke e come l'hub è configurato per stabilire una connessione dinamica con più spoke ed è in grado di aggiungere altri spoke.



Diagramma_Hub_and_Spoke

Passaggio 1: Configurazione hub

r. Definire la proposta e il criterio IKEv2.

b. Configurare un keyring file e immettere un file Pre-Shared Key da utilizzare per autenticare gli spoke.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. Abilitare i servizi AAA sul router hub, quindi definire un elenco di autorizzazioni di rete denominatoFlexAuthche specifichi i criteri dalla configurazione del dispositivo locale.

```
!
aaa new-model
```

```
 aaa authorization network FlexAuth local
!
```

d. Definire unIP address poolnomeFlexPoolcontenente gli indirizzi da 10.1.1.2 a 10.1.1.254. Questo pool viene utilizzato per assegnare automaticamente un indirizzo IP all'interfaccia tunnel degli spoke.

```
!
ip local pool FlexPool 10.1.1.2 10.1.1.254
!
```

e. Definire un elenco degli accessi IP standard con nomeFlexTraffice che consenta la rete 10.10.1.0/24. Questo ACL definisce le reti sottoposte a push negli spoke FlexVPN per raggiungerli attraverso il tunnel.

```
!
ip access-list standard FlexTraffic
 permit 10.10.1.0 0.0.0.255
!
```

Nell'elenco degli accessi e nel pool di indirizzi IP sono presenti riferimenti a **IKEv2 Authorization Policy**.

```
!
crypto ikev2 authorization policy HUBPolicy
 pool FlexPool
 route set interface
 route set access-list FlexTraffic
!
```

f. Creare un gruppo di IKEv2 profileautorizzazioni, assegnare il gruppo di autorizzazioni keyring e AAA.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth HUBPolicy
 virtual-template 1
!
```

g. Creare un Transport Setfile, definire gli algoritmi di crittografia e hash utilizzati per proteggere i dati.

h. Creare un IPsec profilefile, assegnare il file IKEv2 profile e Transport Set creato in precedenza.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

i. Configurare il **virtual-template 1** as **type tunnel**file. Fare riferimento all'interfaccia comeIP unnumbered addressinterfaccia e applicare **IPsec profile**

```
!
interface virtual-template 1 type tunnel
 ip unnumbered loopback1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
!
```

Passaggio 2: Configurazione Spoke

r. Definire la proposta e il criterio IKEv2.

b. Configurare un keyring e immettere una chiave già condivisa utilizzata per l'autenticazione all'hub.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. Abilitare i servizi AAA sul router hub, quindi definire un elenco di autorizzazioni di rete denominato **FlexAuth** che specifichi i criteri dalla configurazione del dispositivo locale. Quindi, configurare il criterio di configurazione della modalità per eseguire il push dell'indirizzo IP e dei percorsi allo spoke FlexVPN.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. Definire un elenco degli accessi IP standard di nome **FlexTraffic** 10.20.2.0/24. Questo ACL definisce le reti condivise da questo spoke per il passaggio attraverso il tunnel.

```
!
ip access-list standard FlexTraffic
 permit 10.20.2.0 0.0.0.255
!
```

L'elenco degli accessi viene assegnato nella **IKEv2 Authorization Policy**directory.

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

e. Creare un gruppo di IKEv2 profileautorizzazioni, assegnare il gruppo di autorizzazioni keyring e AAA.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
!
```

f. Creare un set di trasporto e definire gli algoritmi di crittografia e hash utilizzati per proteggere i dati.

g. Creare un profilo IPSec, assegnare il profilo IKEv2 e il set di trasporto creati in precedenza.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

h. Configurare l'interfaccia tunnel con la proprietà dell'indirizzo IP negoziato, ottenuta dal pool configurato nell'hub.

```
!
interface tunnel 0
 ip address negotiated
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.20 255.255.255.0
!
```

Verifica

Utilizzare il comando show ip interface brief per esaminare lo stato del tunnel, del modello virtuale e dell'accesso virtuale:

- Nell'hub, lo stato di Virtual-Template è normale. Per ogni spoke viene creato un accesso virtuale che stabilisce una connessione con l'hub e mostra uno stato attivo/attivo.
- Nello spoke, l'interfaccia del tunnel ha ricevuto un indirizzo IP e mostra uno stato attivo/attivo.

<#root>

```
FlexVPN_HUB#
```

show ip interface brief

```
Interface              IP-Address      OK? Method Status           Protocol
GigabitEthernet1       192.168.0.10    YES NVRAM  up               up
GigabitEthernet2       10.10.1.10      YES manual up               up
Loopback1              10.1.1.1        YES manual up               up
```

Virtual-Access1 10.1.1.1 YES unset up up

```
 <<<<<<< This Virtual-Access has been created and is up/up
Virtual-Template1      10.1.1.1        YES unset  up
```

```
FlexVPN_Spoke#
show ip interface brief
Interface              IP-Address      OK? Method  Status            Protocol
GigabitEthernet1       192.168.0.20    YES NVRAM   up                up
GigabitEthernet2       10.20.2.20      YES manual  up                up
Tunnel0                10.1.1.8        YES manual  up                up <<<<<<
The tunnel interface received an IP address from pool defined
```

- Per verificare che la connessione protetta tra l'hub e il spoke sia stata stabilita, usare il comando show crypto ikev2 sa.

<#root>

```
FlexVPN_HUB#
show crypto ikev2 sa
 IPv4 Crypto IKEv2 SA
Tunnel-id Local                 Remote                fvrf/ivrf                Status
1         192.168.0.10/500      192.168.0.20/500      none/none
READY
 Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
 Life/Active Time: 86400/587 sec
 IPv6 Crypto IKEv2 SA
```

- Utilizzare il comando show crypto ipsec sa per confermare che il traffico è crittografato e che sta passando attraverso il tunnel, verificando che i contatori encaps e decaps siano in aumento.

<#root>

```
FlexVPN_HUB#
show crypto ipsec sa
interface: Virtual-Access1
    Crypto map tag: Virtual-Access1-head-0, local addr 192.168.0.10
```

```
   protected vrf: (none)
   local ident (addr/mask/prot/port): (192.168.0.10/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.0.20/255.255.255.255/47/0)
   current_peer 192.168.0.20 port 500
     PERMIT, flags={origin_is_acl,}

    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10



    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10


    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.0.10, remote crypto endpt.: 192.168.0.20
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
     current outbound spi: 0xAFC2F841(2948790337)
     PFS (Y/N): N, DH group: none

     inbound esp sas:


spi: 0x7E780336(2121794358)


        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 5581, flow_id: CSR:3581, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-h


sa timing: remaining key lifetime (k/sec): (4607998/3010)


        IV size: 16 bytes
        replay detection support: Y


Status: ACTIVE(ACTIVE)



      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:


spi: 0xAFC2F841(2948790337)


         transform: esp-256-aes esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 5582, flow_id: CSR:3582, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-


sa timing: remaining key lifetime (k/sec): (4607998/3010)


         IV size: 16 bytes
```

```
         replay detection support: Y

Status: ACTIVE(ACTIVE)


      outbound ah sas:

      outbound pcp sas:
```

- Utilizzare il comando show ip route per verificare che le route siano state spostate sul spoke:
  - Il route per 10.1.1.1/32 è stato sottoposto a push tramite i payload di configurazione IKEv2 a causa dell'istruzione route set interface nella configurazione HUB.
  - Il route per 10.10.1.0/24 è stato sottoposto a push tramite i payload di configurazione IKEv2 a causa dell'istruzione FlexTraffic dell'elenco di accesso del set di route nella configurazione HUB.

<#root>

```
FlexVPN_Spoke#show ip route
<<< Omitted >>>

Gateway of last resort is 192.168.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.0.1
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

S        10.1.1.1/32 is directly connected, Tunnel0   <<<<<<<


C        10.1.1.8/32 is directly connected, Tunnel0

S        10.10.1.0/24 is directly connected, Tunnel0  <<<<<<<


C        10.20.2.20/32 is directly connected, GigabitEthernet2
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet1
L        192.168.0.20/32 is directly connected, GigabitEthernet1
```

- Utilizzare il comando ping per verificare la connettività alle reti annunciate.

<#root>

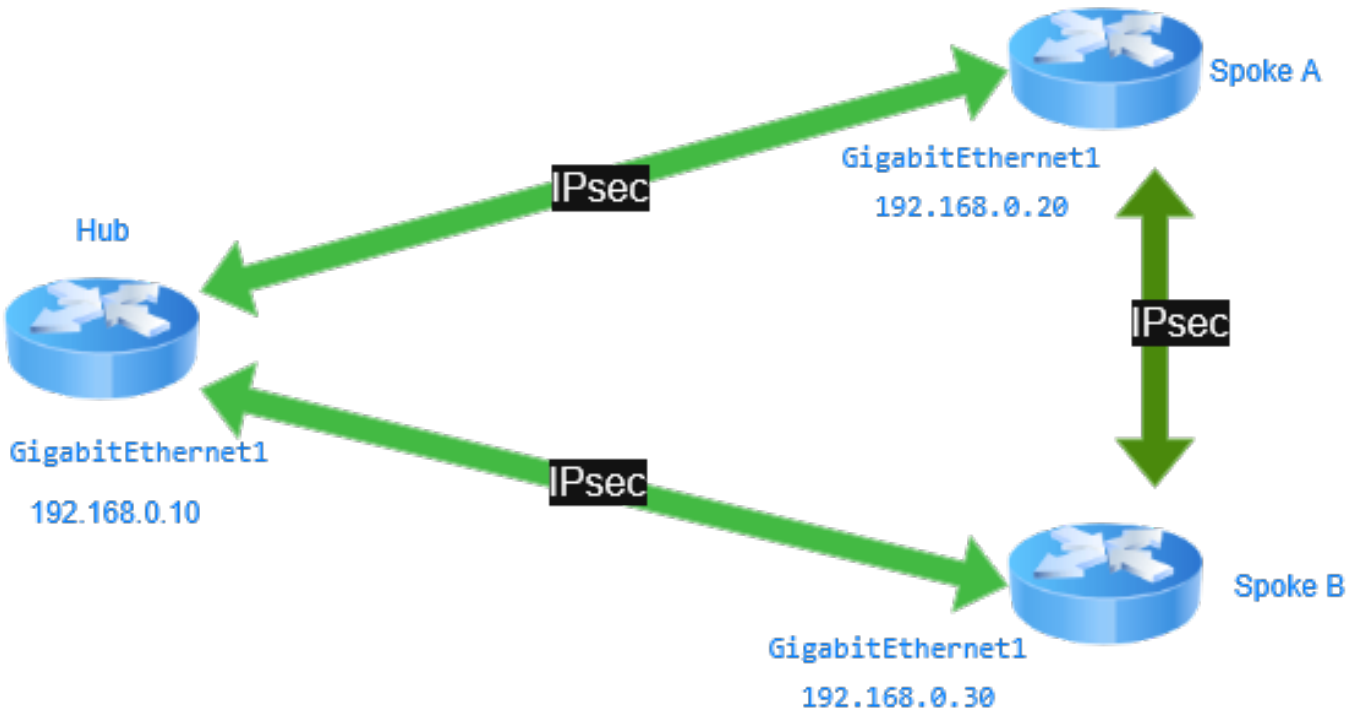
```
FlexVPN_HUB#

ping 10.20.2.20

Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.20.2.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms



FlexVPN_Spoke#

ping 10.10.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Spoke to Spoke FlexVPN

FlexVPN in una topologia Hub e Spoke con connettività Spoke-to-Spoke consente una comunicazione VPN dinamica, scalabile e sicura. L'hub funge da punto di controllo centralizzato in cui NHRP consente agli spoke di eseguire query sull'hub per altri indirizzi IP spoke, consentendo tunnel IPsec spoke diretti per una comunicazione efficiente e una latenza ridotta.

Sull'hub, il **ip nhrp redirect** comando viene utilizzato per notificare ai spoke che la comunicazione diretta spoke è possibile, ottimizzando il flusso del traffico bypassando l'hub per il traffico del piano dati. Sugli spoke, il **ip nhrp shortcut** comando consente loro di stabilire dinamicamente tunnel diretti con altri spoke dopo aver ricevuto il reindirizzamento dall'hub. Il diagramma fa riferimento al traffico tra Hub e Spoke e alla comunicazione Spoke-to-Spoke.



Spoke_to_Spoke_Diagram

Passaggio 1: Configurazione hub

r. Definire criteri e profili IKEv2.

b. Configurare un keyring file e immettere un file Pre-Shared Key da utilizzare per autenticare gli spoke.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. Abilitare i servizi AAA sul router hub, definire un elenco di autorizzazioni di rete denominato **FlexAuth** che specifichi i criteri dalla configurazione del dispositivo locale, quindi configurare i criteri di configurazione della modalità per eseguire il push dell'indirizzo IP e dei percorsi allo spoke FlexVPN.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. Definire unIP address poolnome **FlexPool**, contenente gli indirizzi da 10.1.1.2 a 10.1.1.254. Questo pool viene utilizzato per assegnare automaticamente un indirizzo IP all'interfaccia tunnel degli spoke.

```
!
ip local pool FlexPool 10.1.1.2 10.1.1.254
!
```

e. Definire un elenco degli accessi IP standard denominatoFlexTraffice che consenta la rete 10.0.0.0/8. Questo ACL definisce le reti inviate agli spoke FlexVPN, incluse le reti di altri spoke connessi all'hub, in modo che gli spoke sappiano che tali reti sono raggiunte prima attraverso l'hub.

```
!
ip access-list standard FlexTraffic
 permit 10.0.0.0 0.255.255.255
!
```

L'elenco degli accessi e i IP address pool nomi vengono assegnati in **IKEv2 Authorization Policy**.

```
!
crypto ikev2 authorization policy HUBPolicy
 pool FlexPool
 route set interface
 route set access-list FlexTraffic
!
```

f. Creare un IKEv2 profilegruppo, assegnare il gruppo di autorizzazioni keyring e AAA.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth HUBPolicy
 virtual-template 1
!
```

g. Creare un Transport Set e definire gli algoritmi di crittografia e hash utilizzati per proteggere i dati.

h. Creare un IPsec profilefile, assegnare il file IKEv2 profile e Transport Set creato in precedenza.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

i. Configurare il **virtual-template 1** as **type tunnel**file. Fare riferimento all'interfaccia come **IP unnumbered address** e applicare la **IPsec profile**.

Il **ip nhrp redirect** comando è configurato in Virtual-Template per informare gli spoke di stabilire una

connessione diretta con altri spoke per raggiungere le loro reti.

```
!
interface virtual-template 1 type tunnel
 ip unnumbered loopback1
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
!
```

Passaggio 2: Configurazione Spoke A

r. Definire criteri e profili IKEv2.

b. Configurare un keyring file e immettere un file Pre-Shared Key da utilizzare per autenticare gli spoke.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. Abilitare i servizi AAA sul router hub, quindi definire un elenco di autorizzazioni di rete denominato **FlexAuth** che specifichi i criteri dalla configurazione del dispositivo locale. Quindi, configurare il criterio di configurazione della modalità per eseguire il push dell'indirizzo IP e dei percorsi allo spoke FlexVPN.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. Definire un elenco degli accessi IP standard con nome **FlexTraffic** e che consenta la rete

10.20.2.0/24. Questo ACL definisce le reti condivise da questo spoke da passare attraverso il tunnel.

```
!
ip access-list standard FlexTraffic
 permit 10.20.2.0 0.0.0.255
!
```

L'elenco degli accessi viene assegnato nella **IKEv2 Authorization Policy.**

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

e. Creare un gruppo di IKEv2 profileautorizzazioni, assegnare il gruppo di autorizzazioni keyring e AAA.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
 virtual-template 1
!
```

f. Creare un Transport Set e definire gli algoritmi di crittografia e hash utilizzati per proteggere i dati.

g. Creare un profilo IPSec, assegnare il profilo IKEv2 e il set di trasporto creati in precedenza.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

h. Configurare l'interfaccia del tunnel e il modello virtuale. Specificare **Virtual-Template1** i valori dVTI

creati per supportare **NHRP shortcuts**l'interfaccia. Inoltre, impostaretunnel0come indirizzo senza numero invirtual-template.

Il **ip nhrp shortcut** comando viene configurato sugli spoke per consentire loro di stabilire in modo dinamico tunnel diretti ad altri spoke basati sui messaggi di reindirizzamento NHRP provenienti dall'hub.

```
!
interface tunnel 0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface virtual-template 1 type tunnel
 ip unnumbered tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.20 255.255.255.0
!
```

Passaggio 3: Configurazione Spoke B

r. Definire criteri e profili IKEv2.

b. Configurare un keyring file e immettere un file Pre-Shared Key da utilizzare per autenticare gli spoke.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. Abilitare i servizi AAA sul router hub, definire un elenco di autorizzazioni di rete denominato

FlexAuth che specifichi i criteri dalla configurazione del dispositivo locale, quindi configurare i criteri di configurazione della modalità per eseguire il push dell'indirizzo IP e dei percorsi allo spoke FlexVPN.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. Definire l'elenco degli accessi IP standard con nome **FlexTraffic** e che consente alla rete di passare attraverso il tunnel 10.30.3.0/24. Questo ACL definisce le reti condivise da questo spoke.

```
!
ip access-list standard FlexTraffic
 permit 10.30.3.0 0.0.0.255
!
```

Nell'elenco degli accessi IKEv2 Authorization Policy.

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

e. Creare un gruppo di IKEv2 profileautorizzazioni, assegnare il gruppo di autorizzazioni keyring e AAA.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
 virtual-template 1
!
```

f. Creare un Transport Set e definire gli algoritmi di crittografia e hash utilizzati per proteggere i dati.

g. Creare un IPsec profilefile, assegnare il file IKEv2 profile e il file Transport Set creato in precedenza.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

h. Configurare la tunnel interface e virtual template. Specificare **Virtual-Template1** per i dVTI creati per il supporto NHRP shortcuts. Inoltre, impostaretunnel0come indirizzo senza numero invirtual-template.

Il **ip nhrp shortcut** comando viene configurato sugli spoke per consentire loro di stabilire in modo dinamico tunnel diretti ad altri spoke basati sui messaggi di reindirizzamento NHRP provenienti dall'hub.

```
!
interface tunnel 0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface virtual-template 1 type tunnel
 ip unnumbered tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.30 255.255.255.0
!
```

Verifica

Utilizzare il comando show ip interface brief per esaminare lo stato del tunnel, del modello virtuale e dell'accesso virtuale. Ora, è una connessione diretta spoke-to-spoke:

- Nei spoke, lo stato di Virtual-Template è normale. Viene creato un accesso virtuale per la connessione nello stato attivo/attivo.

<#root>

FlexVPN_Spoke#

show ip interface brief

```
Interface                  IP-Address      OK?  Method  Status                Protocol
GigabitEthernet1           192.168.0.30    YES  NVRAM   up                    up
GigabitEthernet2           10.20.2.20      YES  manual  up                    up

Tunnel0                    10.1.1.12       YES  manual  up                    up


Virtual-Access1            10.1.1.12       YES  unset   up                    up

Virtual-Template1          10.1.1.12       YES  unset   up                    down
```

- Per verificare che la connessione protetta tra ciascun dispositivo sia stata stabilita, usare il comando show crypto ikev2 sa.
- Utilizzare il comando show crypto ipsec sa per confermare che il traffico è crittografato e che sta passando attraverso il tunnel, verificando che i contatori encaps e decaps siano in aumento.
- Utilizzare il comando show ip nhrp per verificare il reindirizzamento del traffico tra gli spoke.

<#root>

```
FlexVPN_Spoke#

show ip nhrp


10.1.1.10/32 via 10.1.1.10
   Virtual-Access1 created 00:00:13, expire 00:09:46
   Type:

dynamic

, Flags: router nhop rib nho
   NBMA address: 192.168.0.30

10.30.3.0/24 via 10.1.1.10


   Virtual-Access1 created 00:00:13, expire 00:09:46
   Type:

dynamic

, Flags: router rib nho
   NBMA address: 192.168.0.30
```

Utilizzare il comando show ip route per verificare che le route siano state spostate nel spoke:

- Le due route associate all'interfaccia Virtual-Access1 sono nuove e associate ai collegamenti NHRP.
- Il carattere % indica un override dell'hop successivo.

<#root>

```
FlexVPN_Spoke#sh ip route
<<<< Omitted >>>>
```

```
Gateway of last resort is 192.168.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.0.1
      10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
S        10.0.0.0/8 is directly connected, Tunnel0
S        10.1.1.1/32 is directly connected, Tunnel0

S  %     10.1.1.10/32 is directly connected, Virtual-Access1


C        10.1.1.12/32 is directly connected, Tunnel0
C        10.20.2.20/32 is directly connected, GigabitEthernet2

S  %     10.30.3.0/24 is directly connected, Virtual-Access1


      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet1
L        192.168.0.30/32 is directly connected, GigabitEthernet1
```

- Utilizzare il comando ping per verificare la connettività alle reti annunciate.

<#root>

```
FlexVPN_Spoke#

ping 10.30.3.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.30.3.30, timeout is 2 seconds:

.!!!!


Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione. Utilizzare questi comandi per eseguire il debug del processo di negoziazione del tunnel:

debug crypto interface

debug crypto ikev2
debug crypto ikev2 client flexvpn
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ikev2 packet

debug crypto ipsec
debug crypto ipsec error
debug crypto ipsec message
debug crypto ipsec states

I debug NHRP possono essere di aiuto nella risoluzione dei problemi delle connessioni spoke.

```
debug nhrp
debug nhrp detail
debug nhrp event
debug nhrp error
debug nhrp packet
debug nhrp routing
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).