FlexVPN: Esempio di configurazione di IPv6 in una distribuzione Hub e Spoke

Sommario

Introduzione

Questo documento descrive una configurazione comune che utilizza una distribuzione spoke e hub Cisco IOS® FlexVPN in un ambiente IPv6. Vengono illustrati i concetti trattati in [FlexVPN: Configurazione di base da LAN a LAN IPv6](#).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco IOS FlexVPN
- Protocolli di routing

Componenti usati

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

- Cisco Integrated Services Router generazione 2 (ISR G2)
- Software Cisco IOS versione 15.3 (o versione 15.4T per tunnel spoke dinamici con IPv6)

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.

Configurazione

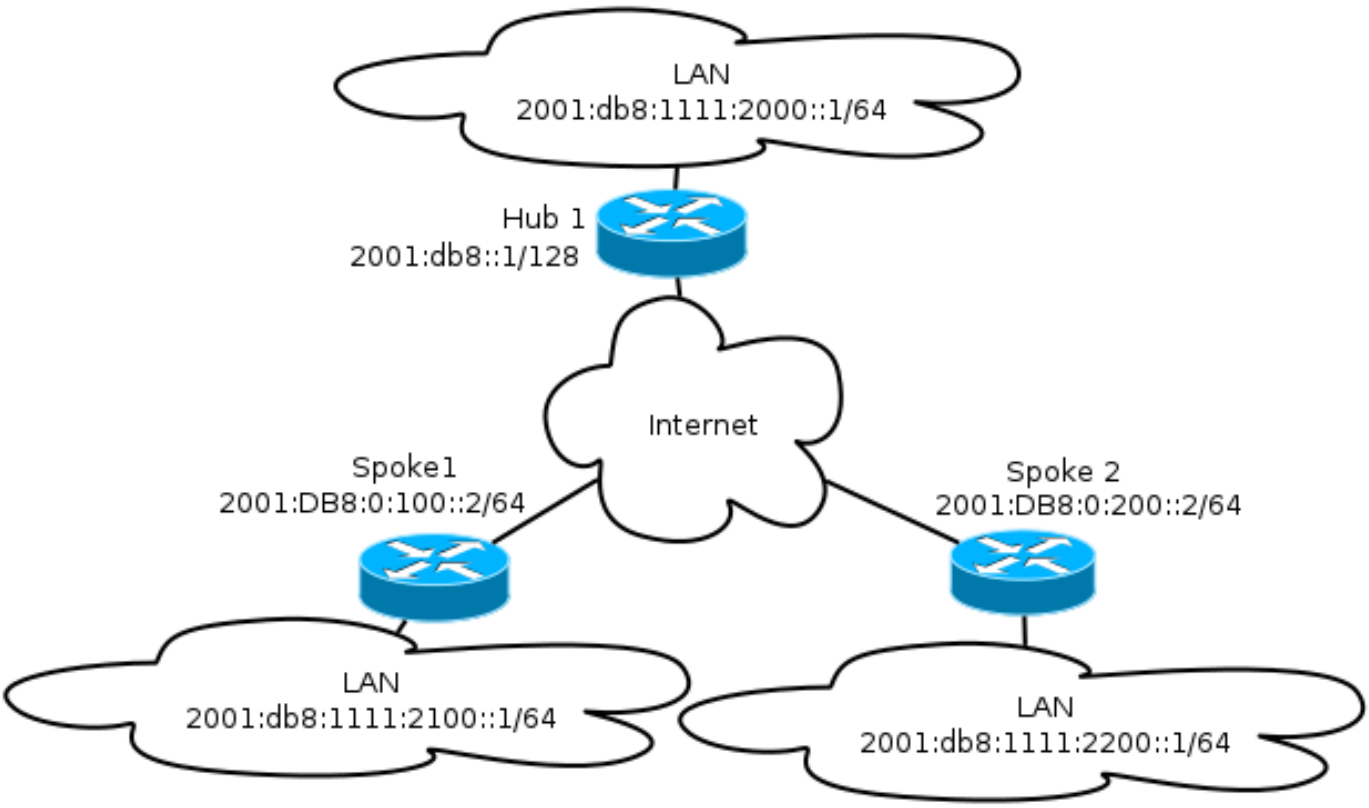
> **Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Mentre in questo esempio di configurazione e nel diagramma di rete viene utilizzato IPv6 come rete di trasporto, nelle distribuzioni FlexVPN viene in genere utilizzato GRE (Generic Routing Encapsulation). L'utilizzo di GRE anziché di IPsec consente agli amministratori di eseguire IPv4, IPv6 o entrambi negli stessi tunnel, indipendentemente dalla rete di trasporto.

Esempio di rete

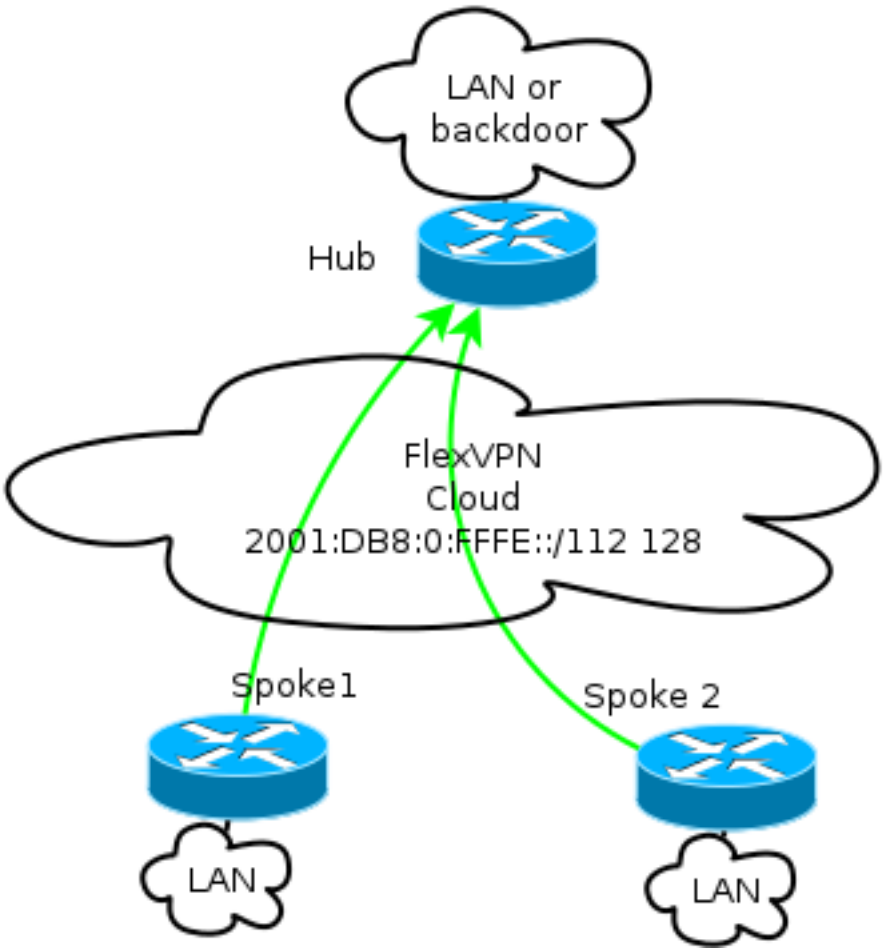
Transport Network

Questo è un diagramma della rete di trasporto utilizzata nell'esempio:



Sovrapponi rete

Questo è un diagramma della topologia di rete sovrapposta di base utilizzata nell'esempio:



Ogni spoke viene assegnato da un pool di indirizzi di /112, ma riceve un indirizzo /128. Pertanto, la notazione '/112 128' viene utilizzata nella configurazione del pool IPv6 dell'hub.

Configurazioni

Questa configurazione mostra una sovrapposizione IPv4 e IPv6 che funziona su una backbone IPv6.

Rispetto agli esempi che utilizzano IPv4 come backbone, si noti che è necessario utilizzare il comando **tunnel mode** per modificare il nodo e supportare il trasporto IPv6.

La funzionalità del tunnel spoke su IPv6 verrà introdotta nel software Cisco IOS versione 15.4T, che non è ancora disponibile.

Protocolli di routing

Cisco consiglia di utilizzare il protocollo iBGP (Internal Border Gateway Protocol) per il peering tra spoke e hub per installazioni di grandi dimensioni, in quanto iBGP è il protocollo di routing più scalabile.

L'intervallo di ascolto Border Gateway Protocol (BGP) non supporta l'intervallo IPv6, ma semplifica l'utilizzo con un trasporto IPv4. Sebbene sia possibile utilizzare BGP in un ambiente di questo tipo, questa configurazione illustra un esempio di base ed è stato quindi scelto il protocollo EIGRP (Enhanced Interior Gateway Routing Protocol).

Configurazione hub

Rispetto agli esempi precedenti, questa configurazione include l'utilizzo di nuovi protocolli di trasporto.

Per configurare l'hub, l'amministratore deve:

- Abilita routing unicast.
- Eseguire il provisioning del routing di trasporto.
- Eseguire il provisioning di un nuovo pool di indirizzi IPv6 da assegnare in modo dinamico. Il pool è 2001:DB8:0:FFFE::/112; 16 bit consente di indirizzare 65.535 dispositivi.
- Abilitare IPv6 per la configurazione NHRP (Next Hop Resolution Protocol) per consentire IPv6 nella sovrapposizione.
- Account per l'indirizzamento IPv6 nel keyring e profilo nella configurazione crittografica.

In questo esempio, l'hub annuncia un riepilogo EIGRP a tutti i raggi.

Cisco sconsiglia di utilizzare un indirizzo di riepilogo sull'interfaccia Virtual-Template nell'implementazione di FlexVPN; tuttavia, in una DMVPN (Dynamic Multipoint VPN), questa non è solo una procedura comune, ma è anche considerata una best practice. Vedere Migrazione FlexVPN: Spostamento hardware da DMVPN a FlexVPN sugli stessi dispositivi: Configurazione hub aggiornata per i dettagli.

```
ipv6 unicast-routing
ipv6 cef

ip local pool FlexSpokes 10.1.1.176 10.1.1.254
ipv6 local pool FlexSpokesv6 2001:DB8:0:FFFE::/112 128

crypto ikev2 authorization policy default
 ipv6 pool FlexSpokesv6
pool FlexSpokes
route set interface
crypto ikev2 keyring Flex_key
peer ALL
address ::/0
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile Flex_IKEv2
match identity remote address ::/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

interface Virtual-Template1 type tunnel
```

```
ip unnumbered Loopback100
ip mtu 1400
ip nhrp network-id 2
ip nhrp redirect
ip tcp adjust-mss 1360
ipv6 mtu 1400
ipv6 tcp adjust-mss 1358
 ipv6 unnumbered Loopback100
ipv6 enable
ipv6 eigrp 65001
 ipv6 nhrp network-id 2
 ipv6 nhrp redirect
 tunnel mode gre ipv6
tunnel protection ipsec profile default

interface Ethernet1/0
description LAN subnet
ip address 192.168.0.1 255.255.255.0
ipv6 address 2001:DB8:1111:2000::1/64
ipv6 enable
ipv6 eigrp 65001

interface Loopback0
ip address 172.25.1.1 255.255.255.255
ipv6 address 2001:DB8::1/128
ipv6 enable

ip route 192.168.0.0 255.255.0.0 Null0
ipv6 route 2001:DB8:1111::/48 Null0

ip prefix-list EIGRP_SUMMARY_ONLY seq 5 permit 192.168.0.0/16
ipv6 prefix-list EIGRP_SUMMARY_v6 seq 5 permit 2001:DB8:1111::/48

router eigrp 65001
 distribute-list prefix EIGRP_SUMMARY_ONLY out Virtual-Template1
 network 10.1.1.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
 redistribute static metric 1500 10 10 1 1500

ipv6 router eigrp 65001
 distribute-list prefix-list EIGRP_SUMMARY_v6 out Virtual-Template1
 redistribute static metric 1500 10 10 1 1500
```

Configurazione spoke

Come nella configurazione hub, l'amministratore deve eseguire il provisioning degli indirizzi IPv6, abilitare il routing IPv6 e aggiungere la configurazione NHRP e di crittografia.

Èpossibile utilizzare il protocollo EIGRP e altri protocolli di routing per il peer spoke-to-spoke. In uno scenario tipico, tuttavia, i protocolli non sono necessari e possono influire sulla scalabilità e la stabilità.

Nell'esempio, la configurazione di routing mantiene solo l'adiacenza EIGRP tra lo spoke e l'hub, e l'unica interfaccia non passiva è l'interfaccia Tunnel1:

```
ipv6 unicast-routing
ipv6 cef

crypto logging session
```

```
crypto ikev2 authorization policy default
route set interface
crypto ikev2 keyring Flex_key
peer ALL
address ::/0
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile Flex_IKEv2
match identity remote address ::/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

interface Tunnel1
description FlexVPN tunnel
ip address negotiated
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
delay 1000
ipv6 mtu 1400
ipv6 tcp adjust-mss 1358
ipv6 address negotiated
 ipv6 enable
 ipv6 nhrp network-id 2
 ipv6 nhrp shortcut virtual-template 1
 ipv6 nhrp redirect
tunnel source Ethernet0/0
 tunnel mode gre ipv6
tunnel destination 2001:DB8::1
tunnel protection ipsec profile default

interface Virtual-Template1 type tunnel
ip unnumbered Ethernet1/0
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
delay 1000
ipv6 mtu 1400
ipv6 tcp adjust-mss 1358
 ipv6 unnumbered Ethernet1/0
ipv6 enable
 ipv6 nhrp network-id 2
 ipv6 nhrp shortcut virtual-template 1
 ipv6 nhrp redirect
tunnel mode gre ipv6
tunnel protection ipsec profile default
```

Quando si creano voci del protocollo di routing su un spoke, attenersi alle seguenti raccomandazioni:

1. Consentire al protocollo di routing di stabilire una relazione tramite la connessione (in questo caso, l'interfaccia Tunnel1) all'hub. Generalmente non è consigliabile stabilire l'adiacenza di

instradamento tra i raggi, in quanto ciò aumenta in modo significativo la complessità nella maggior parte dei casi.

2. Annunciare solo le subnet LAN locali e abilitare il protocollo di routing su un indirizzo IP assegnato dall'hub. Prestare attenzione a non pubblicizzare una subnet di grandi dimensioni perché potrebbe influire sulla comunicazione tra persone.

Questo esempio riflette entrambe le raccomandazioni per l'EIGRP su Spoke1:

```
router eigrp 65001
 network 10.1.1.0 0.0.0.255
 network 192.168.101.0 0.0.0.255
 passive-interface default
 no passive-interface Tunnel1

ipv6 router eigrp 65001
 passive-interface default
 no passive-interface Tunnel1
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

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

Sessione spoke-to-hub

Una sessione configurata correttamente tra dispositivi spoke e hub dispone di una sessione IKEv2 (Internet Key Exchange versione 2) attiva e di un protocollo di routing in grado di stabilire l'adiacenza. Nell'esempio, il protocollo di routing è EIGRP, quindi sono disponibili due comandi EIGRP:

- **show crypto ikev2 sa**
- **show ipv6 eigrp 65001 neighbors**
- **show ip eigrp 6501 neighbors**

```
Spoke1#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

 IPv6 Crypto IKEv2  SA

Tunnel-id    fvrf/ivrf              Status
1          none/none            READY
Local  2001:DB8:0:100::2/500
Remote  2001:DB8::1/500
     Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
     Life/Active Time: 86400/1945 sec
```

```
Spoke1#sh ipv6 eigrp 65001 neighbor
EIGRP-IPv6 Neighbors for AS(65001)
H   Address                 Interface          Hold Uptime   SRTT   RTO  Q  Seq
                                              (sec)         (ms)       Cnt Num
0   Link-local address:     Tu1                  14 00:32:29   72  1470  0  10
   FE80::A8BB:CCFF:FE00:6600

Spoke1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(65001)
H   Address                 Interface          Hold Uptime   SRTT   RTO  Q  Seq
                                              (sec)         (ms)       Cnt Num
0   10.1.1.1                Tu1                  11 00:21:05   11  1398  0  26
```

Nell'IPv4, EIGRP utilizza un indirizzo IP assegnato al peer; nell'esempio precedente, questo indirizzo IP è l'indirizzo 10.1.1.1.

IPv6 utilizza un indirizzo locale del collegamento; in questo esempio, l'hub è FE80::A8BB:CCFF:FE00:6600. Per verificare che l'hub sia raggiungibile tramite l'IP locale al collegamento, usare il comando **ping**:

```
Spoke1#ping FE80::A8BB:CCFF:FE00:6600
Output Interface: tunnel1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::A8BB:CCFF:FE00:6600, timeout is
2 seconds:
Packet sent with a source address of FE80::A8BB:CCFF:FE00:6400%Tunnel1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/5 ms
```

Sessione spoke

Le sessioni oratorie vengono visualizzate dinamicamente su richiesta. Utilizzare un semplice comando **ping** per avviare una sessione:

```
Spoke1#ping  2001:DB8:1111:2200::100 source e1/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:1111:2200::100, timeout is 2 seconds:
Packet sent with a source address of 2001:DB8:1111:2100::1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/8/10 ms
```

Per confermare la connettività spoke diretta, l'amministratore deve:

- Verificare che una sessione spoke dinamica attivi una nuova interfaccia di accesso virtuale:

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed
state to up
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is UP.
Peer 2001:DB8:0:200::2:500       Id: 2001:DB8:0:200::2
```

- Verificare lo stato della sessione IKEv2:

```
Spoke1#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

 IPv6 Crypto IKEv2  SA
```

```
Tunnel-id    fvrf/ivrf              Status
1          none/none            READY
Local  2001:DB8:0:100::2/500
Remote  2001:DB8::1/500
     Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK,
Auth verify: PSK
     Life/Active Time: 86400/3275 sec

Tunnel-id    fvrf/ivrf              Status
2          none/none            READY
Local  2001:DB8:0:100::2/500
Remote  2001:DB8:0:200::2/500
     Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK,
Auth verify: PSK
     Life/Active Time: 86400/665 sec
```

Sono disponibili due sessioni: uno spoke-to-hub e uno spoke-to-spoke.

- Verifica NHRP:

```
Spoke1#show ipv6 nhrp
2001:DB8:0:FFFE::/128 via 2001:DB8:0:FFFE::
Virtual-Access1 created 00:00:10, expire 01:59:49
Type: dynamic, Flags: router nhop rib nho
NBMA address: 2001:DB8:0:200::2
2001:DB8:1111:2200::/64 via 2001:DB8:0:FFFE::
Virtual-Access1 created 00:00:10, expire 01:59:49
Type: dynamic, Flags: router rib nho
NBMA address: 2001:DB8:0:200::2
```

L'output mostra che 2001:DB8:111:2200::/64 (la LAN per Spoke2) è disponibile tramite 2001:DB8:0:FFFE:, ovvero l'indirizzo IPv6 negoziato nell'interfaccia Tunnel1 per Spoke2. L'interfaccia Tunnel1 è disponibile tramite l'indirizzo multiaccesso non broadcast (NBMA) di 2001:db8:0:200::2, ovvero l'indirizzo IPv6 assegnato staticamente a Spoke2.

- Verificare che il traffico stia passando attraverso l'interfaccia:

```
Spoke1#sh crypto ipsec sa peer 2001:DB8:0:200::2

interface: Virtual-Access1
   Crypto map tag: Virtual-Access1-head-0, local addr 2001:DB8:0:100::2

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (2001:DB8:0:100::2/128/47/0)
  remote ident (addr/mask/prot/port): (2001:DB8:0:200::2/128/47/0)
  current_peer 2001:DB8:0:200::2 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 196, #pkts encrypt: 196, #pkts digest: 196
   #pkts decaps: 195, #pkts decrypt: 195, #pkts verify: 195
(...)
```

- Verificare il percorso di routing e le impostazioni CEF:

```
Spoke1#show ipv6 route
(...)
D   2001:DB8:1111:2200::/64 [90/27161600]
    via 2001:DB8:0:FFFE::, Virtual-Access1 [Shortcut]
    via FE80::A8BB:CCFF:FE00:6600, Tunnel1
(...)
```

```
Spoke1#show ipv6 cef 2001:DB8:1111:2200::
2001:DB8:1111:2200::/64
 nexthop 2001:DB8:0:FFFE:: Virtual-Access
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

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

I seguenti comandi di debug consentono di risolvere i problemi:

- FlexVPN/IKEv2 e IPsec: **debug crypto ipsecdebug crypto ikev2 [pacchetto|interno]**
- NHRP (relatore):
  - **debug nhrp pack**
  - **debug nhrp extension**
  - **debug nhrp cache**
  - **debug nhrp route**

Per ulteriori informazioni su questi comandi, consultare la lista dei comandi principali di Cisco IOS, tutte le versioni.