Configurazione di Secure Overlay con gli annunci delle route BGP

Sommario

Introduzione

Questo documento descrive come configurare la sovrapposizione sicura e gli annunci eBGP su NFVIS per la gestione esclusiva del traffico vBranch.

Componenti usati

Le informazioni di questo documento si basano sui seguenti componenti hardware e software:

- ENCS5412 con NFVIS 4.7.1
- Catalyst 8000v con Cisco IOS® XE 17.09.03a

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.

Annuncio route BGP

La funzione NFVIS BGP funziona con la funzione secure overlay per imparare le route dal router adiacente BGP su un tunnel di overlay sicuro. I percorsi o le subnet appresi vengono aggiunti alla tabella di routing NFVIS per il tunnel sicuro, che rende i percorsi accessibili attraverso il tunnel. Poiché Secure Overlay consente di imparare solo una singola route privata dal tunnel; la configurazione di BGP consente di superare questo limite stabilendo un'adiacenza tramite il tunnel crittografato e inserendo le route esportate nella tabella di routing NFVIS vpnv4 e viceversa.

Esempio di configurazione

Diagramma topologico

L'obiettivo di questa configurazione è quello di raggiungere l'indirizzo IP di gestione di NFVIS dal c8000v. Una volta stabilito il tunnel, è possibile annunciare più route dalle subnet private-vrf utilizzando gli annunci delle route eBGP.

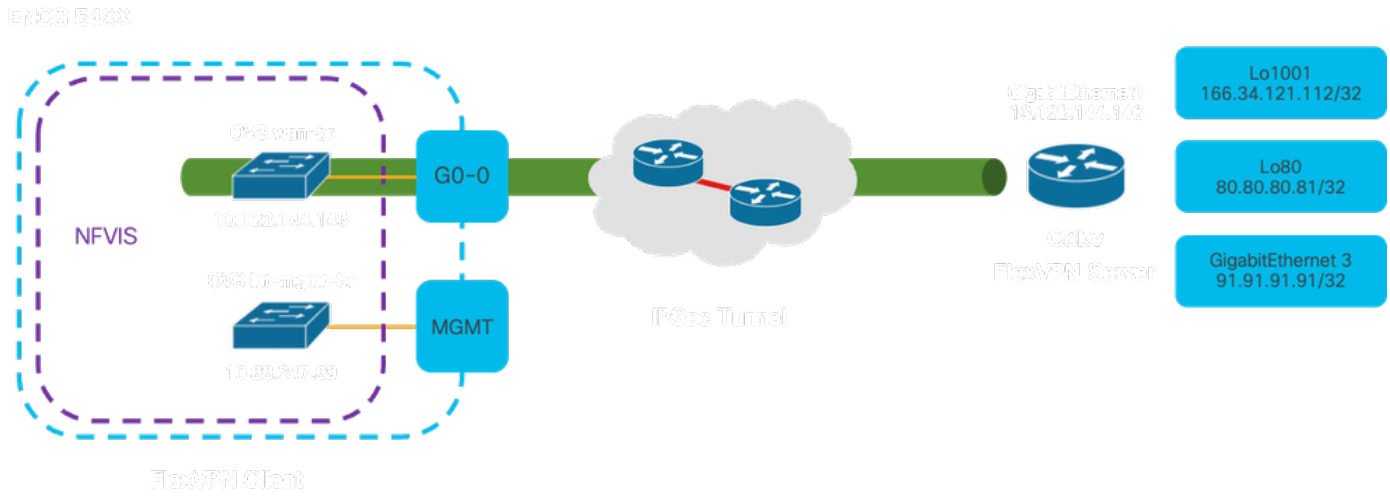


Figura 1. Diagramma topologico per l'esempio preparato in questo articolo

Configurazione iniziale

Configurare l'indirizzo IP pertinente sul server FlexVPN (tutto in modalità di configurazione globale)

```
vrf definition private-vrf
 rd 65000:7
 address-family ipv4
 exit-address-family

vrf definition public-vrf
 address-family ipv4
 exit-address-family

interface GigabitEthernet1
 description Public-Facing Interface
 vrf forwarding public-vrf
 ip address 10.88.247.84 255.255.255.224

interface Loopback1001
 description Tunnel Loopback
 vrf forwarding private-vrf
 ip address 166.34.121.112 255.255.255.255

interface Loopback80
 description Route Announced Loopback
 vrf forwarding private-vrf
 ip address 81.81.81.1 255.255.255.255

interface GigabitEthernet3
 description Route Announced Physical Interface
 vrf forwarding private-vrf
 ip address 91.91.91.1 255.255.255.0
```

Per NFVIS, configurare l'interfaccia WAN e MGMT di conseguenza

```
system settings mgmt ip address 192.168.1.1 255.255.255.0
system settings wan ip address 10.88.247.89 255.255.255.224
system settings default-gw 10.88.247.65
system settings ip-receive-acl 0.0.0.0/0
 service  [ ssh https netconf scpd ]
 action   accept
 priority 10
!
```

Configurazione del server FlexVPN sul router Catalyst 8000v

1. Creare una proposta IKEv2

Specifica i protocolli e gli algoritmi di sicurezza che due endpoint VPN devono utilizzare durante la fase iniziale (fase 1) che prevede la creazione di un canale di comunicazione sicuro. Lo scopo della proposta IKEv2 è quello di delineare i parametri per l'autenticazione, la crittografia, l'integrità

e lo scambio di chiavi, assicurando in tal modo che entrambi gli endpoint concordino una serie comune di misure di sicurezza prima di scambiarsi dati sensibili.

```
crypto ikev2 proposal uCPE-proposal
 encryption aes-cbc-256
 integrity sha512
 group 16 14
```

Dove:

encryption <algoritmo>	La proposta include gli algoritmi di crittografia (come AES o 3DES) che la VPN deve utilizzare per proteggere i dati. La crittografia impedisce agli intercettatori di leggere il traffico che attraversa il tunnel VPN.
integrità <hash>	Specifica gli algoritmi (ad esempio SHA-512) utilizzati per garantire l'integrità e l'autenticità dei messaggi scambiati durante la negoziazione IKEv2. In questo modo si evitano manomissioni e attacchi di tipo replay.

2. Creare un criterio IKEv2 e associarlo alla proposta.

Si tratta di un set di configurazione che determina i parametri per la fase iniziale (fase 1) della creazione di una connessione VPN IPsec. Si concentra principalmente sul modo in cui gli endpoint VPN si autenticano a vicenda e stabiliscono un canale di comunicazione sicuro per la configurazione della VPN.

```
crypto ikev2 policy uCPE-policy
 match fvrf public-vrf
 proposal uCPE-proposal
```

3. Configurare il criterio di autorizzazione IKEv2

IKEv2 è un protocollo utilizzato per configurare una sessione protetta tra due endpoint in una rete e i criteri di autorizzazione sono un insieme di regole che determina le risorse e i servizi a cui un client VPN può accedere una volta stabilito il tunnel VPN.

```
crypto ikev2 authorization policy uCPE-author-pol
 pfs
 route set interface Loopback1001
```

Dove:

pfs	Perfect Forward Secrecy (PFS) è una funzione che migliora la sicurezza di una

	connessione VPN garantendo che ogni nuova chiave di crittografia sia protetta in modo indipendente, anche se le chiavi precedenti sono compromesse.
route set interface <nome-interfaccia>	Quando una sessione VPN viene stabilita correttamente, le route definite nel criterio di autorizzazione IKEv2 vengono aggiunte automaticamente alla tabella di routing dei dispositivi. In questo modo, il traffico destinato alle reti specificate nel set di route viene indirizzato correttamente tramite il tunnel VPN.

4. Creare un profilo IKEv2

Un criterio IKEv2 (Internet Key Exchange versione 2) è un insieme di regole o parametri utilizzati durante la fase IKEv2 della creazione di un tunnel VPN IPsec (Internet Protocol Security). IKEv2 è un protocollo che facilita lo scambio sicuro di chiavi e la negoziazione di associazioni di protezione (SA, Security Association) tra due parti che desiderano comunicare in modo sicuro su una rete non attendibile, ad esempio Internet. Il criterio IKEv2 definisce le modalità di esecuzione della negoziazione, specificando vari parametri di sicurezza che devono essere concordati da entrambe le parti per stabilire un canale di comunicazione protetto e crittografato.

Il profilo IKEv2 DEVE avere:

- Metodo di autenticazione locale e remota.
- Identità o certificato di corrispondenza oppure corrispondenza di qualsiasi istruzione.

```
crypto ikev2 profile uCPE-profile
 description uCPE profile
 match fvrf public-vrf
 match identity remote any
 authentication remote pre-share key ciscociscocisco123
 authentication local pre-share key ciscociscocisco123
 dpd 60 2 on-demand
 aaa authorization group psk list default uCPE-author-pol local
 virtual-template 1 mode auto
```

Dove:

match fvrf public-vrf	Rendere un profilo compatibile con vrf.
corrispondenza identità remota qualsiasi	Misura per il riconoscimento della validità di una sessione in ingresso, in questo caso chiunque.
chiave di autenticazione pre-condivisione remota ciscocisco123	Specifica che il peer remoto deve essere autenticato utilizzando chiavi già condivise.
chiave di autenticazione pre-condivisione locale ciscocisco123	Specifica che il dispositivo (locale) deve eseguire l'autenticazione utilizzando chiavi già condivise.
dpd 60.2 su richiesta	Dead Peer Detection; se non viene ricevuto alcun pacchetto nel corso di un minuto (60 secondi), inviare 2 pacchetti dpd entro questo intervallo di 60 secondi.

gruppo di autorizzazioni aaa elenco psk uCPE-author-pol predefinito locale	Assegnazione route.
virtual-template modalità 1 auto	Eseguire l'associazione a un modello virtuale.

5. Creare un set di trasformazioni IPSec

Definisce un insieme di protocolli e algoritmi di sicurezza da applicare al traffico di dati che passa attraverso il tunnel IPsec. In sostanza, il set di trasformazioni specifica come i dati devono essere crittografati e autenticati, garantendo una trasmissione sicura tra gli endpoint VPN. La modalità tunnel configura il tunnel IPsec in modo da incapsulare l'intero pacchetto IP per il trasporto sicuro sulla rete.

```
crypto ipsec transform-set tset_aes_256_sha512 esp-aes 256 esp-sha512-hmac
 mode tunnel
```

Dove:

set transform-set <nome-set-trasformazioni>	Specifica gli algoritmi di crittografia e integrità (ad esempio, AES per la crittografia e SHA per l'integrità) che devono essere utilizzati per proteggere il flusso di dati attraverso il tunnel VPN.
set ikev2-profile <nome-profilo-ikev2>	Definisce i parametri per la negoziazione delle associazioni di protezione (SA) nella fase 1 dell'installazione della VPN, inclusi gli algoritmi di crittografia, gli algoritmi hash, i metodi di autenticazione e il gruppo Diffie-Hellman.
set pfs <gruppo>	Impostazione facoltativa che, se abilitata, assicura che ogni nuova chiave di crittografia non sia correlata a nessuna chiave precedente, migliorando la protezione.

6. Rimuovere il profilo IPSec predefinito

La rimozione del profilo IPSec predefinito è una procedura adottata per diversi motivi correlati alla protezione, alla personalizzazione e alla chiarezza del sistema. Il profilo IPSec predefinito non può soddisfare i criteri o i requisiti di protezione specifici della rete. La sua rimozione garantisce che nessun tunnel VPN utilizzi inavvertitamente impostazioni non ottimali o non sicure, riducendo il rischio di vulnerabilità.

Ogni rete ha requisiti di sicurezza univoci, inclusi algoritmi di crittografia e hashing specifici, lunghezze delle chiavi e metodi di autenticazione. La rimozione del profilo predefinito favorisce la creazione di profili personalizzati in base a queste esigenze specifiche, garantendo la migliore protezione e prestazioni possibili.

```
no crypto ipsec profile default
```

7. Creare un profilo IPSec e associarlo a un set di trasformazioni e al profilo IKEv2.

Un profilo IPsec (Internet Protocol Security) è un'entità di configurazione che incapsula le impostazioni e i criteri utilizzati per stabilire e gestire i tunnel VPN IPsec. Funge da modello che può essere applicato a più connessioni VPN, standardizzando i parametri di sicurezza e semplificando la gestione di comunicazioni sicure attraverso una rete.

```
crypto ipsec profile uCPE-ips-prof
 set security-association lifetime seconds 28800
 set security-association idle-time 1800
 set transform-set tset_aes_256_sha512
 set pfs group14
 set ikev2-profile uCPE-profile
```

8. Creare un modello virtuale

L'interfaccia Virtual-Template funge da modello dinamico per le interfacce di accesso virtuale, offrendo un modo scalabile ed efficiente per gestire le connessioni VPN. che consente la creazione dinamica di istanze di interfacce di accesso virtuale. Quando viene avviata una nuova sessione VPN, il dispositivo crea un'interfaccia di accesso virtuale in base alla configurazione specificata nel modello virtuale. Questo processo supporta un numero elevato di client e siti remoti tramite l'allocazione dinamica delle risorse in base alle esigenze, senza la necessità di interfacce fisiche preconfigurate per ogni connessione.

Utilizzando i modelli virtuali, le distribuzioni FlexVPN possono essere scalate in modo efficiente man mano che vengono stabilite nuove connessioni, senza la necessità di configurare manualmente ogni singola sessione.

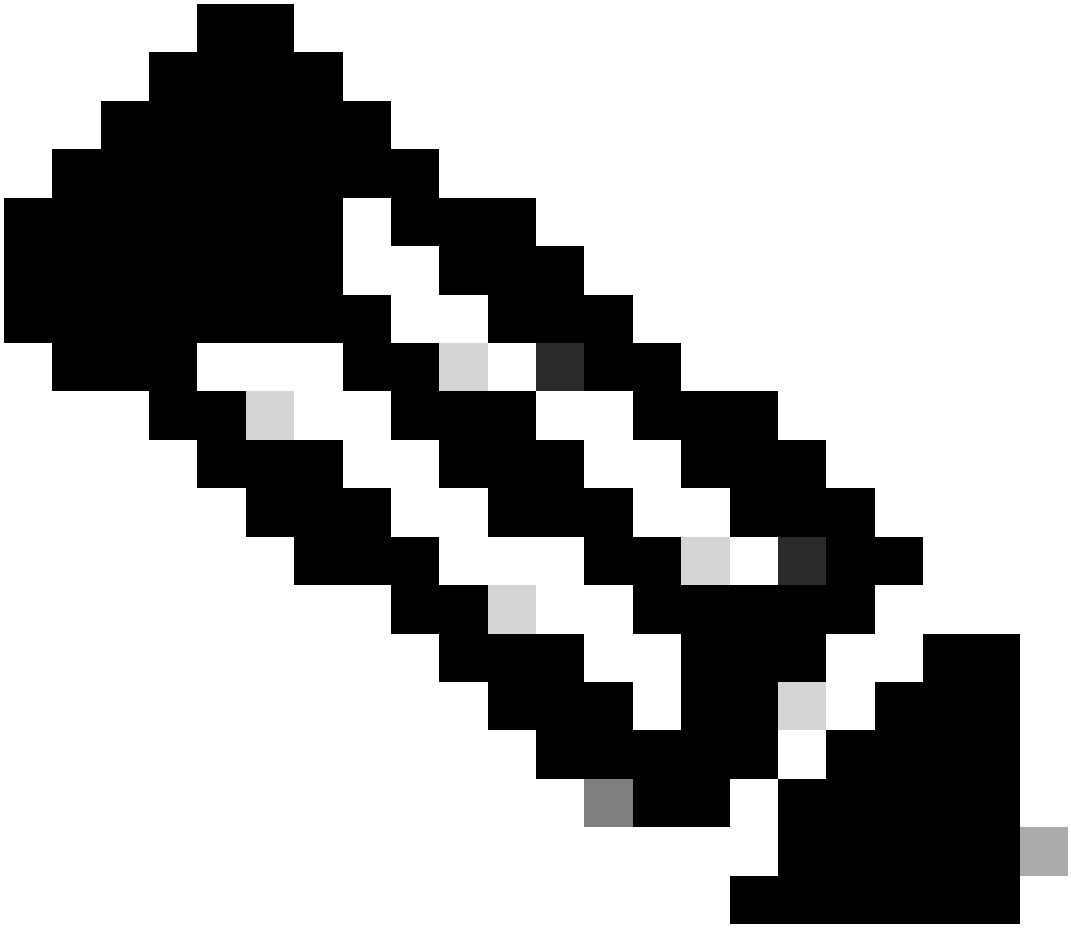
```
interface Virtual-Template1 type tunnel
 vrf forwarding private-vrf
 ip unnumbered Loopback1001
 ip mtu 1400
 ip tcp adjust-mss 1380
 tunnel mode ipsec ipv4
 tunnel vrf public-vrf
 tunnel protection ipsec profile uCPE-ips-prof
```

Configurazione minima NFVIS Secure Overlay

Configurare l'istanza secure-overlay

```
secure-overlay myconn local-bridge wan-br local-system-ip-addr 10.122.144.146 local-system-ip-subnet 10
```

```
 ike-cipher aes256-sha512-modp4096 esp-cipher aes256-sha512-modp4096
 psk local-psk ciscociscocisco123 remote-psk ciscociscocisco123
 commit
```



> Nota: quando si configura l'annuncio della route BGP su un tunnel IPSec, accertarsi di configurare la sovrimpressione sicura in modo che utilizzi un indirizzo IP virtuale (non originato da un'interfaccia fisica o da un bridge OVS) per l'indirizzo IP del tunnel locale. Nell'esempio precedente, sono riportati i comandi di indirizzamento virtuale modificati: local-system-ip-addr 10.122.144.146 local-system-ip-subnet 10.122.144.128/27

Verifica stato sovrapposizione

```
show secure-overlay
secure-overlay myconn
 state                          up
 active-local-bridge            wan-br
```

```
 selected-local-bridge           wan-br
 active-local-system-ip-addr     10.122.144.146
 active-remote-interface-ip-addr 10.88.247.84
 active-remote-system-ip-addr    166.34.121.112
 active-remote-system-ip-subnet  166.34.121.112/32
 active-remote-id                10.88.247.84
```

Configurazione dell'annuncio della route BGP per il server FlexVPN

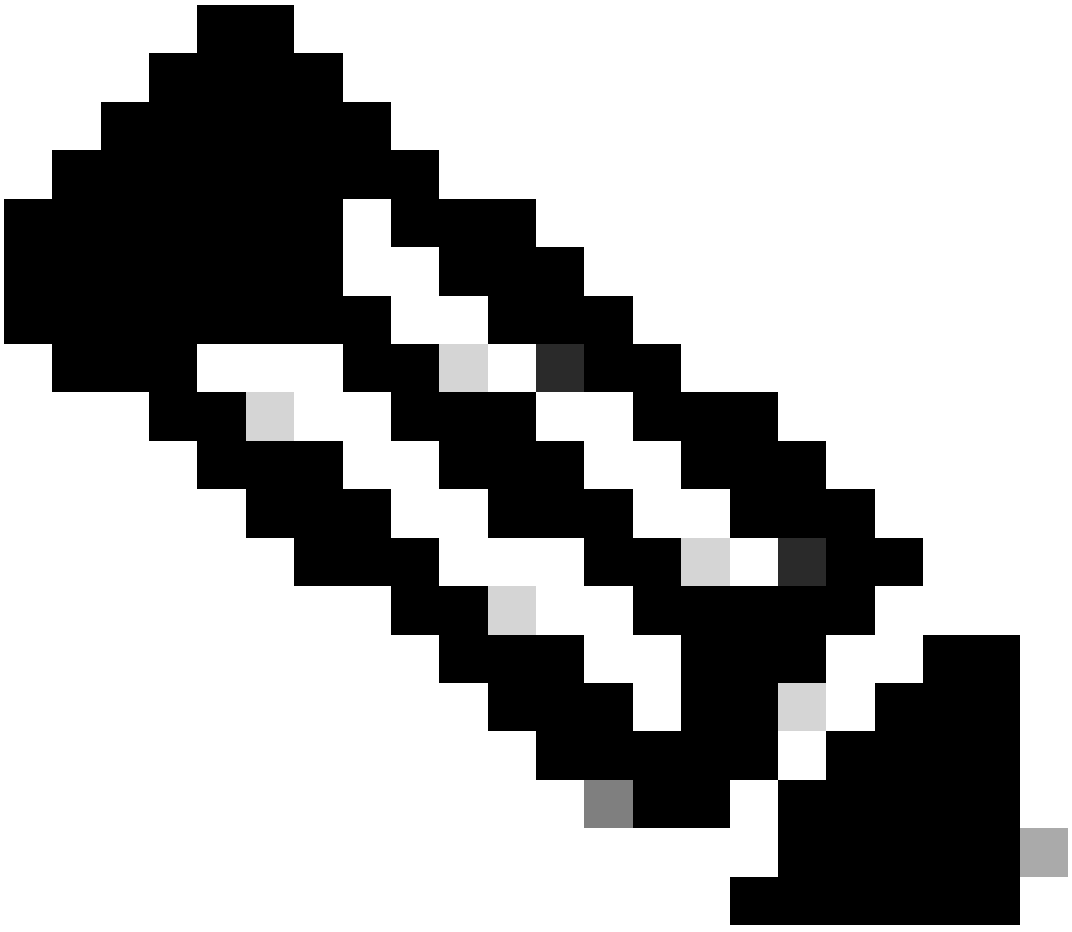
Questa configurazione deve utilizzare eBGP per i peer, in cui la subnet dell'indirizzo di origine (indirizzo IP virtuale per l'IP del tunnel locale) dal lato NFVIS deve essere aggiunta all'intervallo di ascolto.

```
router bgp 65000
 bgp router-id 166.34.121.112
 bgp always-compare-med
 bgp log-neighbor-changes
 bgp deterministic-med
 bgp listen range 10.122.144.0/24 peer-group uCPEs
 bgp listen limit 255
 no bgp default ipv4-unicast
 address-family ipv4 vrf private-vrf
  redistribute connected
  redistribute static
  neighbor uCPEs peer-group
  neighbor uCPEs remote-as 200
  neighbor uCPEs ebgp-multihop 10
  neighbor uCPEs timers 610 1835
 exit-address-family
```

Dove:

bgp always-compare-med	Configura il router in modo che confronti sempre l'attributo MED (Multi-Exit Discriminator) per tutte le route, indipendentemente dalla AS di origine.
bgp log-neighbor-changes	Abilita la registrazione degli eventi correlati alle modifiche nelle relazioni dei nodi adiacenti BGP.
bgp deterministic-med	Assicura il confronto del MED per i percorsi dai vicini in diversi sistemi autonomi.
intervallo di ascolto bgp <rete>/<maschera> gruppo peer <nome-gruppo-peer>	Abilita l'individuazione dinamica dei router adiacenti all'interno dell'intervallo IP specificato (rete/maschera) e assegna i router adiacenti individuati al nome del gruppo peer. Ciò semplifica la configurazione applicando impostazioni comuni a tutti i peer del gruppo.
limite di ascolto bgp 255	Imposta su 255 il numero massimo di router adiacenti BGP dinamici che possono essere accettati nell'intervallo di ascolto.
no bgp default ipv4-unicast	Disabilita l'invio automatico delle informazioni di routing unicast IPv4 ai router BGP adiacenti, richiedendo una configurazione

	esplicita per abilitare questa funzionalità.
ridistribuisci connesso	Ridistribuisce le route dalle reti connesse direttamente in BGP (subnet private dal server FlexVPN che appartengono al private-vrf)
ridistribuisci statico	Ridistribuisce le route statiche in BGP.
router adiacente uCPE ebgp-multihop 10	Consente alle connessioni EBGP (External BGP) con i peer nel gruppo di peer di estendersi fino a 10 hop, utile per il collegamento di dispositivi non direttamente adiacenti.
timer cupe router adiacenti <keep-alive> <hold-down>	Imposta i timer keepalive e hold-down BGP per i vicini rispettivamente nel gruppo peer (610 secondi e 1835 secondi per l'esempio).



Nota: è possibile configurare un elenco di prefissi in uscita per controllare gli annunci delle route adiacenti nel gruppo peer: prefisso adiacente-elenco in uscita

Configurazione BGP su NFVIS

Avvia il processo BGP con le impostazioni di vicinato eBGP

```
router bgp 200
 router-id 10.122.144.146
 neighbor 166.34.121.112 remote-as 65000
 commit
```

Revisione BGP

Questo output rivela le condizioni di una sessione BGP come segnalato dal daemon di routing Internet del BIRD. Questo software di routing è responsabile della gestione delle route IP e dell'adozione di decisioni relative alla direzione. In base alle informazioni fornite, è chiaro che la sessione BGP è in uno stato "Stabilito", a indicare il completamento corretto del processo di peering BGP, e che la sessione è attualmente attiva. È stata completata l'importazione di quattro cicli di lavorazione ed è stato rilevato che è possibile importare un limite massimo di 15 cicli di lavorazione.

```
nfvis# support show bgp
BIRD 1.6.8 ready.
name     proto    table    state  since       info
bgp_166_34_121_112 BGP      bgp_table_166_34_121_112 up     09:54:14    Established
  Preference:     100
  Input filter:   ACCEPT
  Output filter:  ACCEPT
  Import limit:   15
    Action:       disable
  Routes:         4 imported, 0 exported, 8 preferred
  Route change stats:     received   rejected   filtered    ignored   accepted
    Import updates:              4          0          0          0          4
    Import withdraws:            0          0        ---          0          0
    Export updates:              4          4          0        ---          0
    Export withdraws:            0        ---        ---        ---          0
  BGP state:          Established
    Neighbor address: 166.34.121.112
    Neighbor AS:      65000
    Neighbor ID:      166.34.121.112
    Neighbor caps:    refresh enhanced-refresh AS4
    Session:          external multihop AS4
    Source address:   10.122.144.146
    Route limit:      4/15
    Hold timer:       191/240
    Keepalive timer:  38/80
```

Verificare che le subnet private del server FlexVPN siano state annunciate tramite BGP

Quando si configura l'annuncio della route BGP, l'unica combinazione configurabile di famiglia di indirizzi o trasmissione è ipv4 unicast per IPSec. Per visualizzare lo stato BGP, la famiglia di indirizzi o la trasmissione configurabile per IPSec è vpnv4 unicast.

```
nfvis# show bgp vpnv4 unicast
Family Transmission Router ID       Local AS Number
vpnv4  unicast      10.122.144.146  200
```

Il comando show bgp vpnv4 unicast route consente di recuperare informazioni sulle route unicast VPNv4 note al processo BGP.

```
nfvis# show bgp vpnv4 unicast route
Network            Next-Hop        Metric LocPrf Path
81.81.81.1/32      166.34.121.112  0      100    65000 ?
91.91.91.0/24      166.34.121.112  0      100    65000 ?
10.122.144.128/27  166.34.121.112  0      100    65000 ?
166.34.121.112/32  166.34.121.112  0      100    65000 ?
```

Per il server VPN headend, è possibile generare una panoramica della configurazione BGP e dello stato operativo per valutare rapidamente lo stato e la configurazione delle sessioni BGP.

```
c8000v# show ip bgp summary
Number of dynamically created neighbors in vrf private-vrf: 1/(100 max)
Total dynamically created neighbors: 1/(255 max), Subnet ranges: 1
```

Inoltre, è possibile visualizzare informazioni dettagliate sulle voci della tabella di routing VPNv4 (VPN over IPv4) gestite da BGP, deve includere attributi specifici di ciascuna route VPNv4, come il prefisso delle route, l'indirizzo IP dell'hop successivo, il numero AS di origine e vari attributi BGP, come la preferenza locale, MED (Multi-Exit Discriminator) e i valori della community.

```
c8000v# show ip bgp vpnv4 all
BGP table version is 5, local router ID is 166.34.121.112
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 65000:7 (default for vrf private-vrf)
 *>   10.122.144.128/27
                      0.0.0.0                  0         32768 ?
 *>   81.81.81.1/32    0.0.0.0                  0         32768 ?
 *>   91.91.91.0/24    0.0.0.0                  0         32768 ?
 *>   166.34.121.112/32
                      0.0.0.0                  0         32768 ?
```

Risoluzione dei problemi

NFVIS (client FlexVPN)

File di log NFVIS

È possibile visualizzare tutti i log degli errori e di inizializzazione per le fasi IPsec dal file di log charon.log NFVIS:

```
nfvis# show log charon.log
Feb  5 07:55:36.771 00[JOB] spawning 16 worker threads
Feb  5 07:55:36.786 05[CFG] received stroke: add connection 'myconn'
Feb  5 07:55:36.786 05[CFG] added configuration 'myconn'
Feb  5 07:55:36.787 06[CFG] received stroke: initiate 'myconn'
Feb  5 07:55:36.787 06[IKE] <myconn|1> initiating IKE_SA myconn[1] to 10.88.247.84
Feb  5 07:55:36.899 06[ENC] <myconn|1> generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_
Feb  5 07:55:36.899 06[NET] <myconn|1> sending packet: from 10.88.247.89[500] to 10.88.247.84[500] (741
Feb  5 07:55:37.122 09[NET] <myconn|1> received packet: from 10.88.247.84[500] to 10.88.247.89[500] (80
Feb  5 07:55:37.122 09[ENC] <myconn|1> parsed IKE_SA_INIT response 0 [ SA KE No V V V V N(NATD_S_IP) N(
Feb  5 07:55:37.122 09[IKE] <myconn|1> received Cisco Delete Reason vendor ID
Feb  5 07:55:37.122 09[ENC] <myconn|1> received unknown vendor ID: 43:49:53:43:4f:56:50:4e:2d:52:45:56:
Feb  5 07:55:37.122 09[ENC] <myconn|1> received unknown vendor ID: 43:49:53:43:4f:2d:44:59:4e:41:4d:49:
Feb  5 07:55:37.122 09[IKE] <myconn|1> received Cisco FlexVPN Supported vendor ID
Feb  5 07:55:37.122 09[CFG] <myconn|1> selected proposal: IKE:AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SH
Feb  5 07:55:37.235 09[IKE] <myconn|1> cert payload ANY not supported - ignored
Feb  5 07:55:37.235 09[IKE] <myconn|1> authentication of '10.88.247.89' (myself) with pre-shared key
Feb  5 07:55:37.235 09[IKE] <myconn|1> establishing CHILD_SA myconn{1}
Feb  5 07:55:37.236 09[ENC] <myconn|1> generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) IDr AUTH SA
Feb  5 07:55:37.236 09[NET] <myconn|1> sending packet: from 10.88.247.89[4500] to 10.88.247.84[4500] (4
Feb  5 07:55:37.322 10[NET] <myconn|1> received packet: from 10.88.247.84[4500] to 10.88.247.89[4500] (
Feb  5 07:55:37.322 10[ENC] <myconn|1> parsed IKE_AUTH response 1 [ V IDr AUTH SA TSi TSr N(SET_WINSIZE
Feb  5 07:55:37.323 10[IKE] <myconn|1> authentication of '10.88.247.84' with pre-shared key successful
Feb  5 07:55:37.323 10[IKE] <myconn|1> IKE_SA myconn[1] established between 10.88.247.89[10.88.247.89].
Feb  5 07:55:37.323 10[IKE] <myconn|1> scheduling rekeying in 86190s
Feb  5 07:55:37.323 10[IKE] <myconn|1> maximum IKE_SA lifetime 86370s
Feb  5 07:55:37.323 10[IKE] <myconn|1> received ESP_TFC_PADDING_NOT_SUPPORTED, not using ESPv3 TFC padd
Feb  5 07:55:37.323 10[CFG] <myconn|1> selected proposal: ESP:AES_CBC_256/HMAC_SHA2_512_256/NO_EXT_SEQ
Feb  5 07:55:37.323 10[IKE] <myconn|1> CHILD_SA myconn{1} established with SPIs cfc15900_i 49f5e23c_o a
Feb  5 07:55:37.342 11[NET] <myconn|1> received packet: from 10.88.247.84[4500] to 10.88.247.89[4500] (
Feb  5 07:55:37.342 11[ENC] <myconn|1> parsed INFORMATIONAL request 0 [ CPS(SUBNET VER U_PFS) ]
Feb  5 07:55:37.342 11[IKE] <myconn|1> Processing informational configuration payload CONFIGURATION
Feb  5 07:55:37.342 11[IKE] <myconn|1> Processing information configuration payload of type CFG_SET
Feb  5 07:55:37.342 11[IKE] <myconn|1> Processing attribute INTERNAL_IP4_SUBNET
Feb  5 07:55:37.342 11[ENC] <myconn|1> generating INFORMATIONAL response 0 [ ]
Feb  5 07:55:37.342 11[NET] <myconn|1> sending packet: from 10.88.247.89[4500] to 10.88.247.84[4500] (9
```

Route iniettate strongSwan del kernel interno

Su Linux, strongswan (implementazione IPsec multipiattaforma utilizzata da NFVIS) installa le route (incluse le route unicast BGP VPNv4) nella tabella di routing 220 per impostazione predefinita e richiede quindi che il kernel supporti il routing basato su policy.

```
nfvis# support show route 220
10.122.144.128/27 dev ipsec0 proto bird scope link
81.81.81.1 dev ipsec0 proto bird scope link
91.91.91.0/24 dev ipsec0 proto bird scope link
166.34.121.112 dev ipsec0 scope link
```

Verifica stato interfaccia IPsec0

Per ulteriori informazioni sull'interfaccia virtuale ipsec0, usare il comando ifconfig

```
nfvis# support show ifconfig ipsec0
ipsec0: flags=209<UP,POINTOPOINT,RUNNING,NOARP>  mtu 9196
        inet 10.122.144.146  netmask 255.255.255.255  destination 10.122.144.146
        tunnel   txqueuelen 1000  (IPIP Tunnel)
        RX packets 5105  bytes 388266 (379.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5105  bytes 389269 (380.1 KiB)
        TX errors 1  dropped 0 overruns 0  carrier 1  collisions 0
```

Headend (server FlexVPN)

Esamina compilazione SA IPsec tra peer

Nell'output seguente, il tunnel crittografato viene generato tra 10.88.247.84 tramite l'interfaccia Virtual-Access1 e 10.88.247.89 per il traffico tra le reti 0.0.0.0/0 e 10.122.144.128/27; due SA Encapsulating Security Payload (ESP) generate in entrata e in uscita.

```
c8000v# show crypto ipsec sa

interface: Virtual-Access1
    Crypto map tag: Virtual-Access1-head-0, local addr 10.88.247.84

   protected vrf: private-vrf
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (10.122.144.128/255.255.255.224/0/0)
   current_peer 10.88.247.89 port 4500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 218, #pkts encrypt: 218, #pkts digest: 218
    #pkts decaps: 218, #pkts decrypt: 218, #pkts verify: 218
    #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.: 10.88.247.84, remote crypto endpt.: 10.88.247.89
     plaintext mtu 1422, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
     current outbound spi: 0xC91BCDE0(3374042592)
     PFS (Y/N): Y, DH group: group16
```

```
     inbound esp sas:
      spi: 0xB80E6942(3087952194)
        transform: esp-256-aes esp-sha512-hmac ,
        in use settings ={Tunnel, }
        conn id: 2123, flow_id: CSR:123, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-he
         sa timing: remaining key lifetime (k/sec): (4607969/27078)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xC91BCDE0(3374042592)
        transform: esp-256-aes esp-sha512-hmac ,
        in use settings ={Tunnel, }
        conn id: 2124, flow_id: CSR:124, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-he
         sa timing: remaining key lifetime (k/sec): (4607983/27078)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

Visualizza sessioni di crittografia attive

L'output per il comando show crypto session detail deve fornire dettagli completi su ciascuna sessione crittografica attiva, inclusi il tipo di VPN (ad esempio, da sito a sito o accesso remoto), gli algoritmi di crittografia e hash in uso e le associazioni di sicurezza (SA) per il traffico in entrata e in uscita. Inoltre, visualizza le statistiche sul traffico crittografato e decrittografato, ad esempio il numero di pacchetti e byte. Questa opzione può essere utile per monitorare la quantità di dati protetti dalla VPN e per risolvere i problemi di velocità di trasmissione.

```
c8000v# show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP VPN

Interface: Virtual-Access1
Profile: uCPE-profile
Uptime: 11:39:46
Session status: UP-ACTIVE
Peer: 10.88.247.89 port 4500 fvrf: public-vrf ivrf: private-vrf
      Desc: uCPE profile
      Phase1_id: 10.88.247.89
  Session ID: 1235
  IKEv2 SA: local 10.88.247.84/4500 remote 10.88.247.89/4500 Active
```

```
        Capabilities:D connid:2 lifetime:12:20:14
IPSEC FLOW: permit ip   0.0.0.0/0.0.0.0 10.122.144.128/255.255.255.224
      Active SAs: 2, origin: crypto map
      Inbound:  #pkts dec'ed 296 drop 0 life (KB/Sec) 4607958/7 hours, 20 mins
      Outbound: #pkts enc'ed 296 drop 0 life (KB/Sec) 4607977/7 hours, 20 mins
```

Reimposta connessioni VPN

I comandi clear crypto vengono usati per reimpostare manualmente le connessioni VPN o per cancellare le associazioni di sicurezza (SA) senza dover riavviare l'intero dispositivo.

- clear crypto ikev2 consente di cancellare le associazioni di sicurezza IKEv2 (SA IKEv2).
- se si deseleziona la sessione crittografica, le associazioni di protezione IKEv1 (isakmp)/IKEv2 e IPSec verranno cancellate.
- se si deseleziona sa crittografica, verranno deselezionate solo le SA IPSec.
- deselezionare crypto ipsec sa per eliminare le associazioni di protezione IPSec attive.

Esegui debug per ulteriore risoluzione dei problemi

I debug IKEv2 possono aiutare a identificare e risolvere gli errori sul dispositivo headend (c8000v) che possono verificarsi durante il processo di negoziazione IKEv2 e le connessioni dei client FlexVPN, ad esempio i problemi relativi alla creazione della sessione VPN, all'applicazione dei criteri o a eventuali errori specifici del client.

```
c8000v# terminal no monitor
c8000v(config)# logging buffer 1000000
c8000v(config)# logging buffered debugging
c8000v# debug crypto ikev2 error
c8000v# debug crypto ikev2 internal
c8000v# debug crypto ikev2 client flexvpn
```

Articoli e documentazione correlati

Sovrapposizione sicura e configurazione con IP singolo

Supporto BGP su NFVIS

Comandi Secure Overlay e BGP

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).