使用BGP路由通告配置安全覆蓋

目錄

簡介

本文檔介紹如何在NFVIS上為專用vBranch流量管理配置安全覆蓋和eBGP通告。

採用元件

本檔案中的資訊是根據以下硬體和軟體元件而定：

- 運行NFVIS 4.7.1的ENCS5412
- 執行Cisco IOS® XE 17.09.03a的Catalyst 8000v

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

BGP路由宣告

NFVIS BGP功能與安全重疊功能搭配使用，可透過安全重疊通道從BGP鄰居得知路由。這些獲知的路由或子網將增加到安全隧道的NFVIS路由表中，這樣就可以透過隧道訪問路由。由於安全覆蓋只允許從隧道獲取1條單獨的私有路由；配置BGP可以透過加密隧道建立鄰接關係並將導出的路由注入NFVIS vpnv4路由表（反之亦然）來克服此限制。

組態範例

拓撲圖表

此配置的目標是從c8000v到達NFVIS的管理IP地址。 一旦隧道建立，就可以使用eBGP路由通告從專用vrf子網通告更多路由。

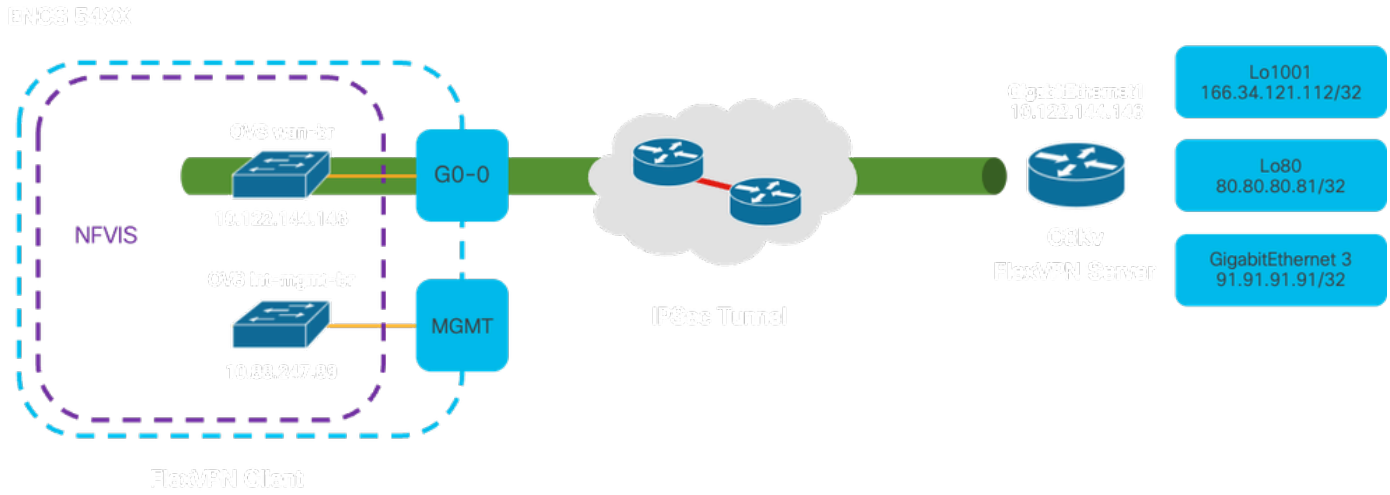


圖1. 針對本文準備的示例的拓撲圖

初始設定

在FlexVPN伺服器上配置相關IP編址（全部在全局配置模式下）

```
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
```

對於NFVIS，請相應地配置WAN和管理介面

```
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
!
```

Catalyst 8000v路由器上的FlexVPN伺服器配置

1. 建立IKEv2方案

它指定了兩個VPN端點在建立安全通訊通道的初始階段（第1階段）必須使用的安全協定和演算法。IKEv2方案的目的是概述身份驗證、加密、完整性和金鑰交換的引數，從而確保兩端在交換任何敏感資料之前商定一組通用的安全措施。

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

其中：

encryption <algorithm>	該提議包括VPN必須用來保護資料的加密演算法（如AES或3DES）。加密可防止竊聽者讀取透過VPN隧道的流量。

integrity <hash>	它指定了用於確保在IKEv2協商期間交換的消息的完整性和真實性的演算法（例如SHA-512）。這可以防止篡改和重新執行攻擊。

2. 建立IKEv2策略並將其與建議關聯。

它是用於指定建立IPSec VPN連線的初始階段（第1階段）的引數的配置集。 它主要關注VPN端點如何相互驗證以及如何為VPN設定建立安全通訊通道。

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

3. 配置IKEv2授權策略

IKEv2協定用於在網路上的兩個端點之間設定安全會話，授權策略是一組規則，用於確定VPN客戶端在建立VPN隧道後允許訪問哪些資源和服務。

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

其中：

pfs	完全正向保密(PFS)功能透過確保每個新加密金鑰獨立安全來增強VPN連線的安全性，即使以前的金鑰受到威脅。
route set interface <interface-name>	成功建立VPN會話後，IKEv2授權策略中定義的路由將自動增加到裝置路由表中。這可確保透過VPN隧道正確路由發往路由集中指定網路的流量。

4. 建立IKEv2配置檔案

IKEv2（網際網路金鑰交換版本2）策略是在建立IPsec（網際網路協定安全）VPN隧道的IKEv2階段期間使用的一組規則或引數。IKEv2是一種協定，它有助於希望透過不受信任的網路（例如internet）進行安全通訊的兩方之間金鑰的安全交換和安全關聯(SA)的協商。IKEv2策略定義必須如何進行此協商，指定雙方必須同意的各種安全引數，以建立安全且加密的通訊通道。

IKEv2配置檔案必須具有：

- 一種本地和遠端身份驗證方法。
- 匹配身份或匹配證書或匹配任何語句。

```
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
```

其中：

match fvrf public-vrf	讓設定檔vrf感知。
match identity remote any	辨識傳入會話的有效措施；在這種情況下，為任何人。
身份驗證遠端預共用金鑰 ciscociscocisco123	指定遠端對等體必須使用預共用金鑰進行身份驗證。
身份驗證本地預共用金鑰 ciscociscocisco123	指定此裝置（本地）必須使用預共用金鑰進行身份驗證。
dpd 60 2點播	失效對等體檢測；如果在60秒內沒有收到資料包，請在此60秒間隔內傳送2個dpd資料包。
aaa authorization group psk list default uCPE-author-pol local	路由分配。
virtual-template 1 mode auto	繫結到虛擬模板。

5. 建立IPsec轉換集

它定義了一組必須應用於透過IPSec隧道的資料流量的安全協定和演算法。實際上，轉換集指定了資料必須如何加密和驗證，從而確保VPN端點之間的安全傳輸。隧道模式將IPSec隧道配置為封裝整個IP資料包，以便在網路上進行安全傳輸。

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

其中：

set transform-set <transform-set-name>	指定必須用來保護流經VPN隧道的資料的加密和完整性演算法（例如：AES用於加密，SHA用於完整性）。
set ikev2-profile <ikev2-profile-name>	定義VPN設定第1階段中安全關聯(SA)協商的引數，包括加密演算法、雜湊演算法、身份驗證方法和Diffie-Hellman組。
set pfs <group>	一個可選設定，如果啟用，可確保每個新加密金鑰與之前的任何金鑰無關，從而增強安全性。

6. 刪除預設IPSec配置檔案

出於與安全、自定義和系統清晰性相關的幾個原因，採用刪除預設IPsec配置檔案的做法。 預設IPSec配置檔案無法滿足您的網路的特定安全策略或要求。刪除它可確保任何VPN隧道都不會不慎使用次優或不安全的設定，從而降低漏洞風險。

每個網路都有獨特的安全要求，包括特定的加密和雜湊演算法、金鑰長度以及身份驗證方法。移除預設設定檔會鼓勵您建立符合這些特定需求的自訂設定檔，以確保儘可能最佳的保護和效能。

```
no crypto ipsec profile default
```

7. 建立IPsec配置檔案並將其與轉換集和IKEv2配置檔案關聯。

IPsec （Internet協定安全）配置檔案是一個配置實體，它封裝了用於建立和管理IPsec VPN隧道的設定和策略。它可以作為一個模板，應用於多個VPN連線，使安全引數標準化，並簡化對網路中安全通訊的管理。

```
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. 建立虛擬模板

Virtual-Template介面充當虛擬訪問介面的動態模板，為管理VPN連線提供了一種可擴展且有效的方法。它允許虛擬訪問介面的動態例項化。當新的VPN會話啟動時，裝置會根據虛擬模板中指定的配置建立虛擬訪問介面。此過程透過根據需要動態分配資源來支援大量遠端客戶端和站點，而無需為每個連線預配置物理介面。

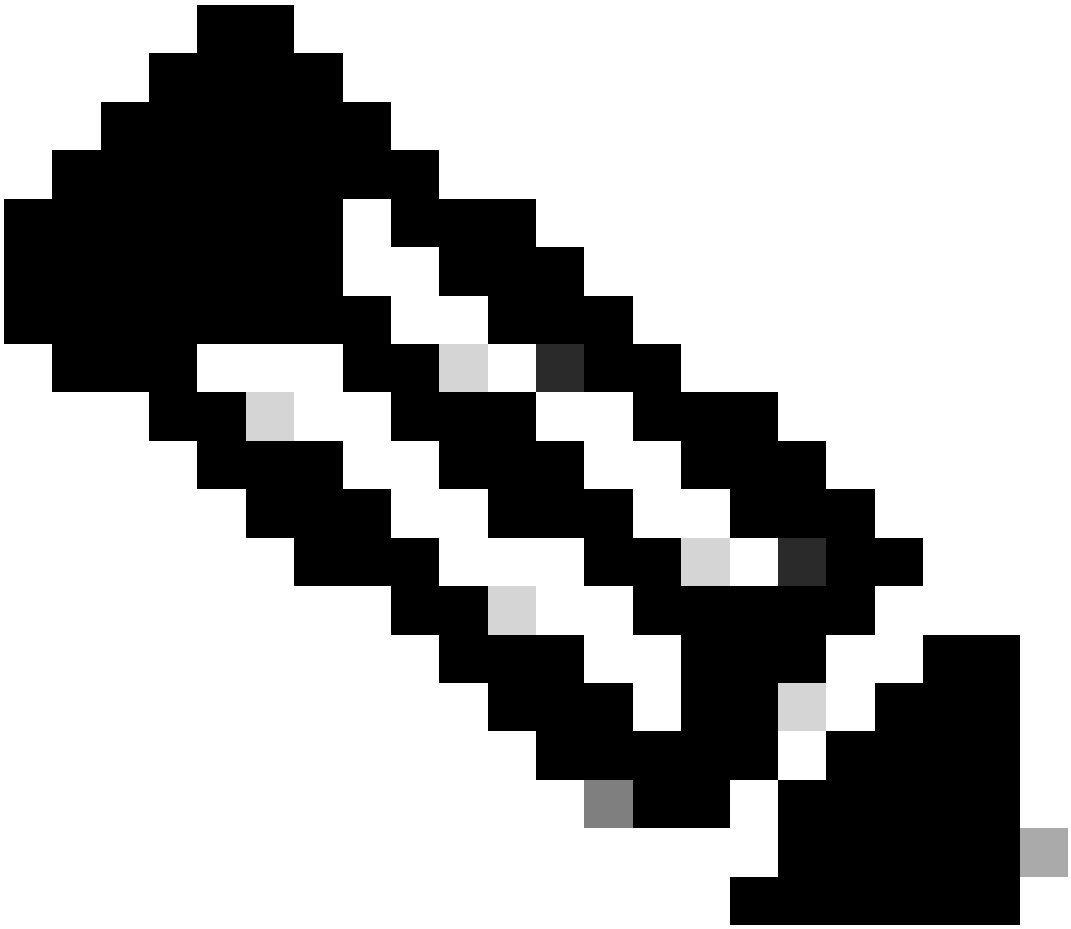
透過使用虛擬模板，FlexVPN部署可以在建立新連線時有效擴展，而無需手動配置每個會話。

```
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
```

NFVIS安全覆蓋最小配置

配置安全覆蓋例項

```
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
```



注意：當配置透過IPSec隧道的BGP路由通告時，請確保將安全重疊配置為使用本地隧道IP地址的虛擬IP地址（不是來自物理介面或OVS網橋）。對於上述示例，虛擬編址命令已更改：local-system-ip-addr 10.122.144.146 local-system-ip-subnet 10.122.144.128/27

檢視覆蓋狀態

```
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
```

FlexVPN伺服器的BGP路由通告配置

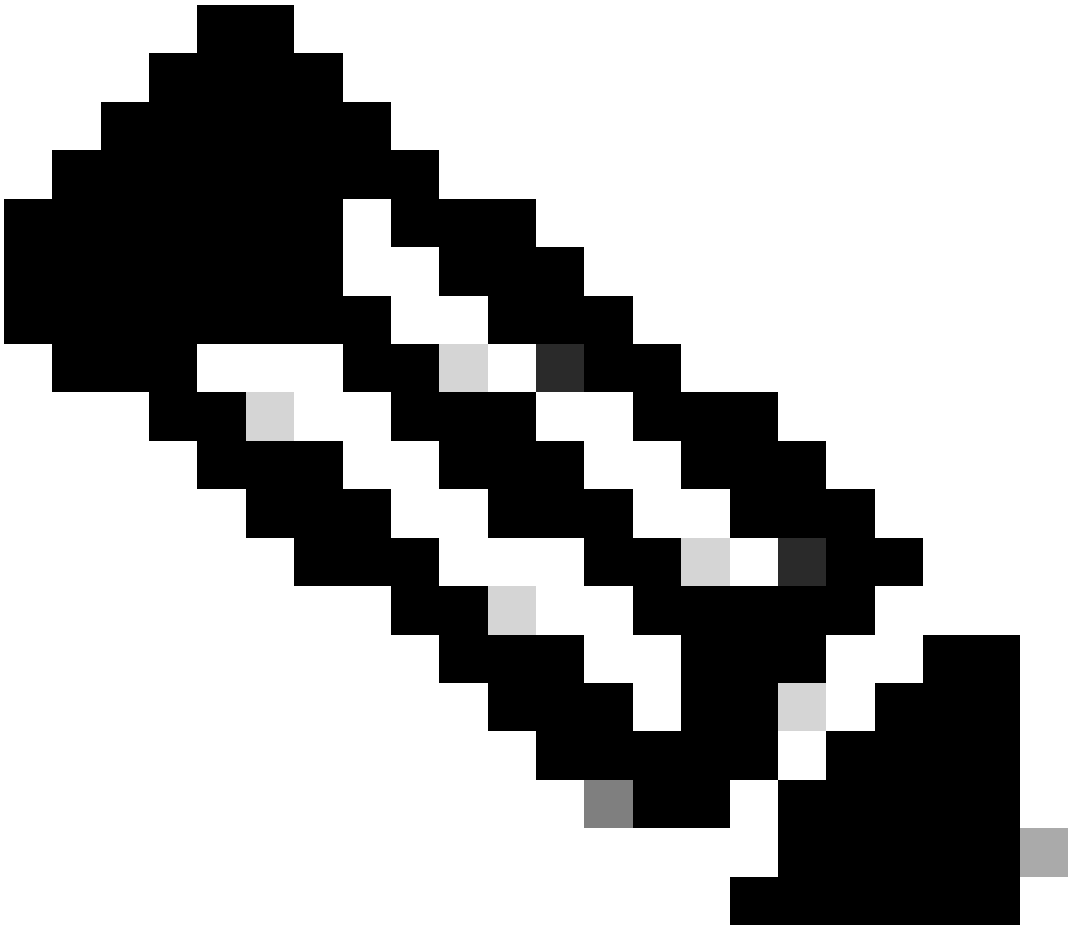
此設定必須為對等體使用eBGP，其中必須將NFVIS端的源地址（本地隧道IP的虛擬IP地址）子網增加到偵聽範圍。

```
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
```

其中：

bgp always-compare-med	將路由器配置為始終比較所有路由的MED（多出口識別符號）屬性，而不考慮其來源AS。
bgp log-neighbor-changes	啟用與BGP鄰居關係更改相關的事件記錄。
bgp deterministic-med	確保比較來自不同自治系統中鄰居的路徑的MED。
bgp listen range <network>/<mask> peer-group <peer-group-name>	啟用指定IP範圍（網路/掩碼）內的動態鄰居發現，並將發現的鄰居分配給對等體組名稱。這透過將通用設定應用於組中的所有對等體來簡化配置。
bgp偵聽限制255	將偵聽範圍內可以接受的動態BGP鄰居最大數量設定為255。
no bgp default ipv4-unicast	停用向BGP鄰居自動傳送IPv4單播路由資訊，需要顯式配置才能啟用此功能。
已連線再分配	將來自直連網路的路由重分配到BGP（來自屬於private-vrf的

	FlexVPN伺服器的專用子網）
redistribute static	將靜態路由重分配到BGP中。
鄰居uCPE ebgp-multihop 10	允許與對等組中的對等體的EBGP （外部BGP）連線跨越最多10跳，這對於連線不直接相鄰的裝置很有用。
neighbor uCPEs timers <keep-alive> <hold-down>	為對等體組中的鄰居設定BGP keepalive和抑制計時器（例如，610秒和1835秒）。



注意：可以配置出站字首清單以控制對等體組中的鄰居路由通告：neighbor prefix-list out

NFVIS上的BGP配置

使用eBGP鄰居關係設定啟動BGP進程

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

BGP稽核

此輸出顯示BIRD Internet路由守護進程報告的BGP會話情況。此路由軟體負責處理IP路由並決定其方向。根據提供的資訊，它表明BGP會話處於「已建立」狀態，這表明BGP對等進程已成功完成，並且會話當前處於活動狀態。它已成功導入了四條路由，並指出可導入的路由上限為15條。

```
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
```

確保透過BGP通告FlexVPN伺服器的專用子網

配置BGP路由通告時，唯一可配置的地址系列或傳輸組合是ipv4 unicastfor IPSec。要檢視BGP狀態，IPSec的可配置地址系列或傳輸是vpnv4 unicast。

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

使用show bgp vpnv4 unicast route命令，您可以檢索有關BGP進程已知的VPNv4單播路由的資訊。

```
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 ?
```

對於頭端VPN伺服器，可以生成BGP配置和運行狀態的概述，以快速評估BGP會話的運行狀況和配置。

```
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
```

此外，可以顯示由BGP管理的VPNv4 (VPN over IPv4)路由表條目的詳細資訊，它必須包括每個VPNv4路由的特定屬性，如路由字首、下一跳IP地址、始發AS編號和各種BGP屬性，如本地優先順序、MED（多出口識別符號）和社群值。

```
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 ?
```

疑難排解

NFVIS（FlexVPN客戶端）

NFVIS記錄檔

您可以從NFVIS charon.log日誌檔案檢視IPSec階段的所有初始化和錯誤日誌：

```
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_SHA
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
```

內部核心強天鵝注入路由

在Linux上，預設情況下，strongswan（NFVIS使用的多平台IPsec實現）將路由（包括BGP VPNv4單播路由）安裝到路由表220中，因此需要核心支援基於策略的路由。

```
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
```

檢視IPsec0介面狀態

您可以使用ifconfig來獲取有關ipsec0虛擬介面的更多詳細資訊

```
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
```

頭端（FlexVPN伺服器）

檢視對等體之間的IPsec SA構建

從以下輸出中，透過Virtual-Access1介面在10.88.247.84與10.88.247.89之間構建加密隧道，用於傳輸網路0.0.0.0/0與10.122.144.128/27之間的流量；兩個封裝安全有效載荷(ESP)SA構建入局和出局。

```
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:
```

顯示活動加密（加密）會話

show crypto session detail的輸出必須提供有關每個活動加密會話的全面詳細資訊，包括VPN型別（如站點到站點或遠端訪問）、使用的加密和雜湊演算法，以及入站和出站流量的安全關聯(SA)。因為它還顯示有關加密和解密流量的統計資訊，例如資料包數和位元組數；這對於監控VPN保護的資料量和排除吞吐量問題非常有用。

```
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
```

重置VPN連線

clear cryptocommands用於手動重置VPN連線，或清除安全關聯(SA)而不需要重新啟動整個裝置。

- clear crypto ikev2 將清除IKEv2安全關聯(IKEv2 SA)。
- clear crypto session將清除IKEv1 (isakmp)/IKEv2和IPSec SA。
- clear crypto sa將僅清除IPSec SA。
- clear crypto ipsec sa將刪除活動的IPSec安全關聯。

執行調試以進行其他故障排除

IKEv2調試可以幫助標識和排除前端裝置(c8000v)上在IKEv2協商過程和FlexVPN客戶端連線期間可能發生的錯誤，如建立VPN會話的問題、策略應用的問題或任何客戶端特定的錯誤。

```
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
```

相關文章和文檔

安全重疊和單一IP配置

NFVIS上的BGP支援

安全覆蓋和BGP命令

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。