# Configuración de la Superposición Segura con Anuncios de Ruta BGP

## Contenido



## Introducción

Este documento describe cómo configurar la superposición segura y los anuncios eBGP en NFVIS para la gestión exclusiva del tráfico vBranch.

# Componentes Utilizados

La información de este documento se basa en estos componentes de hardware y software:

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Anuncio de ruta BGP

La función NFVIS BGP funciona con la función de superposición segura para aprender rutas del vecino BGP sobre un túnel de superposición seguro. Estas rutas o subredes aprendidas se agregan a la tabla de ruteo NFVIS para el túnel seguro, lo que hace que las rutas sean accesibles a través del túnel. Dado que la superposición segura solo permite aprender una única ruta privada del túnel, la configuración de BGP permite superar esta limitación estableciendo la adyacencia a través del túnel cifrado e inyectando rutas exportadas en la tabla de routing NFVIS vpnv4 y viceversa.

# Ejemplo de configuración

## Diagrama de topología

El objetivo de esta configuración es alcanzar la dirección IP de administración de NFVIS desde el c8000v. Una vez establecido el túnel, es posible anunciar más rutas desde las subredes de vrf privado mediante anuncios de ruta eBGP.

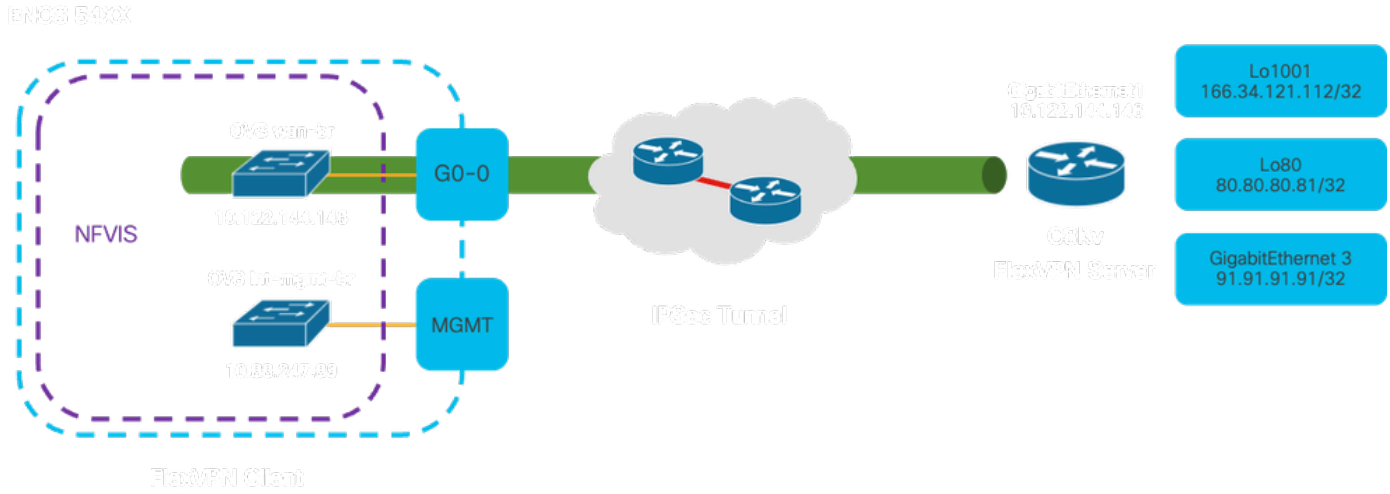



Figura 1. Diagrama de topología para el ejemplo preparado en este artículo

## Configuración inicial

Configure el direccionamiento IP relevante en el servidor FlexVPN (todo ello en el modo de configuración global)

```
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
```

Para NFVIS, configure la WAN y la interfaz de administración según corresponda

```
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
!
```

## Configuración del servidor FlexVPN en el router Catalyst 8000v

1. Crear una propuesta IKEv2

Especifica los protocolos y algoritmos de seguridad que deben utilizar dos terminales VPN durante la fase inicial (fase 1) del establecimiento de un canal de comunicación seguro. El objetivo de la propuesta IKEv2 es describir los parámetros de autenticación, cifrado, integridad e

intercambio de claves, garantizando así que ambos terminales acuerden un conjunto común de medidas de seguridad antes de intercambiar datos confidenciales.

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

Where:

| | |
|---|---|
| encryption <algorithm> | La propuesta incluye los algoritmos de cifrado (como AES o 3DES) que la VPN debe utilizar para proteger los datos. El cifrado impide que los intrusos puedan leer el tráfico que pasa a través del túnel VPN. |
| Integrity <hash> | Especifica los algoritmos (como SHA-512) utilizados para garantizar la integridad y autenticidad de los mensajes intercambiados durante la negociación IKEv2. Esto evita la manipulación y los ataques de repetición. |

2. Cree una política IKEv2 y asóciela a la propuesta.

Se trata de un conjunto de configuración que establece los parámetros para la fase inicial (fase 1) del establecimiento de una conexión VPN IPsec. Se centra principalmente en cómo los terminales VPN se autentican entre sí y establecen un canal de comunicación seguro para la configuración de VPN.

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

3. Configure la política de autorización de IKEv2

IKEv2 es un protocolo que se utiliza para configurar una sesión segura entre dos terminales de una red y la política de autorización es un conjunto de reglas que determina a qué recursos y servicios puede acceder un cliente VPN una vez establecido el túnel VPN.

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

Where:

| | |
|---|---|
| pfs | Perfect Forward Secrecy (Confidencialidad directa perfecta, PFS) es una función |

| | |
|---|---|
| | que mejora la seguridad de una conexión VPN al garantizar que cada nueva clave de cifrado sea segura de forma independiente, incluso si las claves anteriores están en peligro. |
| route set interface <interface-name> | Cuando una sesión VPN se establece correctamente, las rutas definidas en la política de autorización IKEv2 se agregan automáticamente a la tabla de routing de dispositivos. Esto garantiza que el tráfico destinado a las redes especificadas en el conjunto de rutas se enrute correctamente a través del túnel VPN. |

4. Crear un perfil IKEv2

Una directiva IKEv2 (Intercambio de claves de Internet versión 2) es un conjunto de reglas o parámetros que se utilizan durante la fase IKEv2 de establecimiento de un túnel VPN IPsec (seguridad de protocolo de Internet). IKEv2 es un protocolo que facilita el intercambio seguro de claves y la negociación de asociaciones de seguridad (SA) entre dos partes que desean comunicarse de forma segura a través de una red no fiable, como Internet. La política IKEv2 define cómo debe tener lugar esta negociación, especificando varios parámetros de seguridad que ambas partes deben acordar para establecer un canal de comunicación seguro y cifrado.

El perfil IKEv2 DEBE tener:

- Método de autenticación local y remoto.
- Una identidad de coincidencia o un certificado de coincidencia o una sentencia de coincidencia.

```
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
```

Where:

| | |
|---|---|
| match fvrf public-vrf | Haga un perfil que reconozca vrf. |
| match identity remote any | Medida para reconocer una sesión entrante como válida; en este caso, cualquiera. |
| clave precompartida remota de autenticación ciscociscocisco123 | Especifica que el par remoto debe autenticarse mediante claves previamente compartidas. |
| clave local previamente compartida de autenticación ciscociscocisco123 | Especifica que este dispositivo (local) debe autenticarse mediante claves previamente compartidas. |
| dpd 60 2 a demanda | Detección de puntos inactivos; si no se recibió ningún paquete en |

| | |
|---|---|
| | un intervalo de 60 segundos, envíe 2 paquetes dpd en este intervalo de 60 segundos. |
| aaa authorization group psk list default uCPE-author-pol local | Asignación de ruta. |
| virtual-template 1 mode auto | Enlazar a una plantilla virtual. |

5. Crear un conjunto de transformación IPsec

Define un conjunto de protocolos y algoritmos de seguridad que se deben aplicar al tráfico de datos que pasa a través del túnel IPsec. Básicamente, el conjunto de transformación especifica cómo se deben cifrar y autenticar los datos, lo que garantiza una transmisión segura entre los terminales VPN. El modo de túnel configura el túnel IPsec para encapsular el paquete IP completo para el transporte seguro a través de la red.

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

Where:

| | |
|---|---|
| set transform-set <transform-set-name> | Especifica los algoritmos de cifrado e integridad (ejemplo: AES para cifrado y SHA para integridad) que se deben utilizar para proteger los datos que fluyen a través del túnel VPN. |
| set ikev2-profile <ikev2-profile-name> | Define los parámetros para la negociación de las asociaciones de seguridad (SA) en la fase 1 de la configuración VPN, incluidos los algoritmos de cifrado, los algoritmos hash, los métodos de autenticación y el grupo Diffie-Hellman. |
| set pfs <group> | Parámetro opcional que, si está habilitado, garantiza que cada nueva clave de cifrado no está relacionada con ninguna clave anterior, lo que mejora la seguridad. |

6. Eliminar perfil IPsec predeterminado

La eliminación del perfil IPsec predeterminado es una práctica que se sigue por varios motivos relacionados con la seguridad, la personalización y la claridad del sistema. El perfil IPsec predeterminado no puede cumplir las directivas o los requisitos de seguridad específicos de la red. Su eliminación garantiza que ningún túnel VPN utilice inadvertidamente una configuración no óptima o insegura, lo que reduce el riesgo de vulnerabilidades.

Cada red tiene unos requisitos de seguridad únicos, incluidos algoritmos específicos de cifrado y hash, longitudes de clave y métodos de autenticación. La eliminación del perfil predeterminado fomenta la creación de perfiles personalizados adaptados a estas necesidades específicas, lo que garantiza la mejor protección y rendimiento posibles.

```
no crypto ipsec profile default
```

7. Cree un perfil IPsec y asócielo a un conjunto de transformación y al perfil IKEv2.

Un perfil IPsec (seguridad de protocolo de Internet) es una entidad de configuración que encapsula la configuración y las directivas utilizadas para establecer y administrar túneles VPN IPsec. Sirve como plantilla que se puede aplicar a varias conexiones VPN, estandarizando los parámetros de seguridad y simplificando la gestión de la comunicación segura a través de una red.

```
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. Crear una plantilla virtual

La interfaz de plantilla virtual actúa como una plantilla dinámica para interfaces de acceso virtual, proporcionando una forma escalable y eficiente de administrar conexiones VPN. Permite la instanciación dinámica de interfaces de acceso virtual. Cuando se inicia una nueva sesión VPN, el dispositivo crea una interfaz de acceso virtual basada en la configuración especificada en la plantilla virtual. Este proceso admite un gran número de clientes y sitios remotos mediante la asignación dinámica de recursos según sea necesario sin necesidad de interfaces físicas preconfiguradas para cada conexión.

Mediante el uso de plantillas virtuales, las implementaciones de FlexVPN pueden ampliarse de forma eficaz a medida que se establecen nuevas conexiones, sin necesidad de configurar manualmente cada sesión individual.

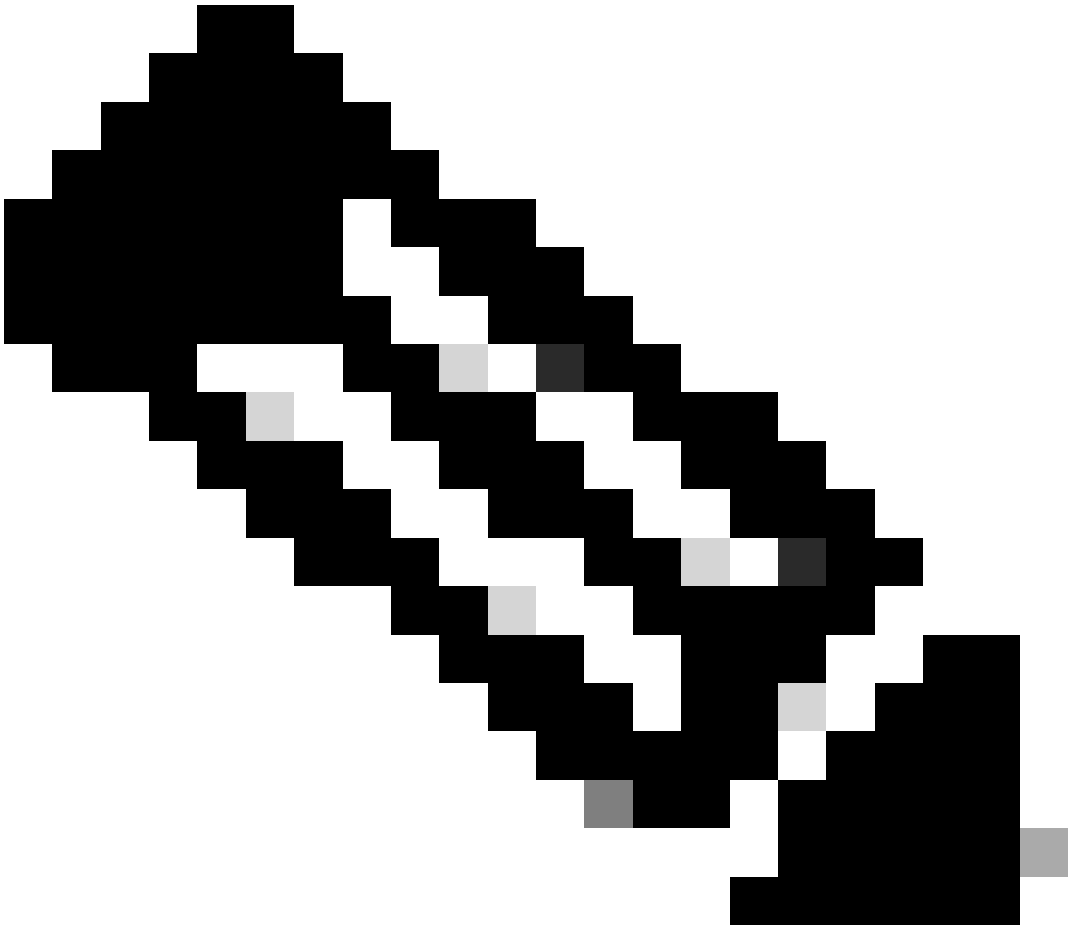
```
interface Virtual-Template1 type tunnel
 vrf forwarding private-vrf
 ip unnumbered Loopback1001
 ip mtu 1400
 ip tcp adjust-mss 1380
 tunnel mode ipsec ipv4
 tunnel vrf public-vrf
 tunnel protection ipsec profile uCPE-ips-prof
```

## Configuración mínima de NFVIS Secure Overlay

Configuración de la instancia de superposición segura

```
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: Al configurar el anuncio de ruta BGP en un túnel IPSec, asegúrese de configurar la superposición segura para utilizar una dirección IP virtual (no originada en una interfaz física o un puente OVS) para la dirección IP del túnel local. Para el ejemplo anterior, estos son los comandos de direccionamiento virtual cambiados: local-system-ip-addr 10.122.144.146 local-system-ip-subnet 10.122.144.128/27

---

Revisar estado de superposición

```
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
```

## Configuración del anuncio de ruta BGP para el servidor FlexVPN

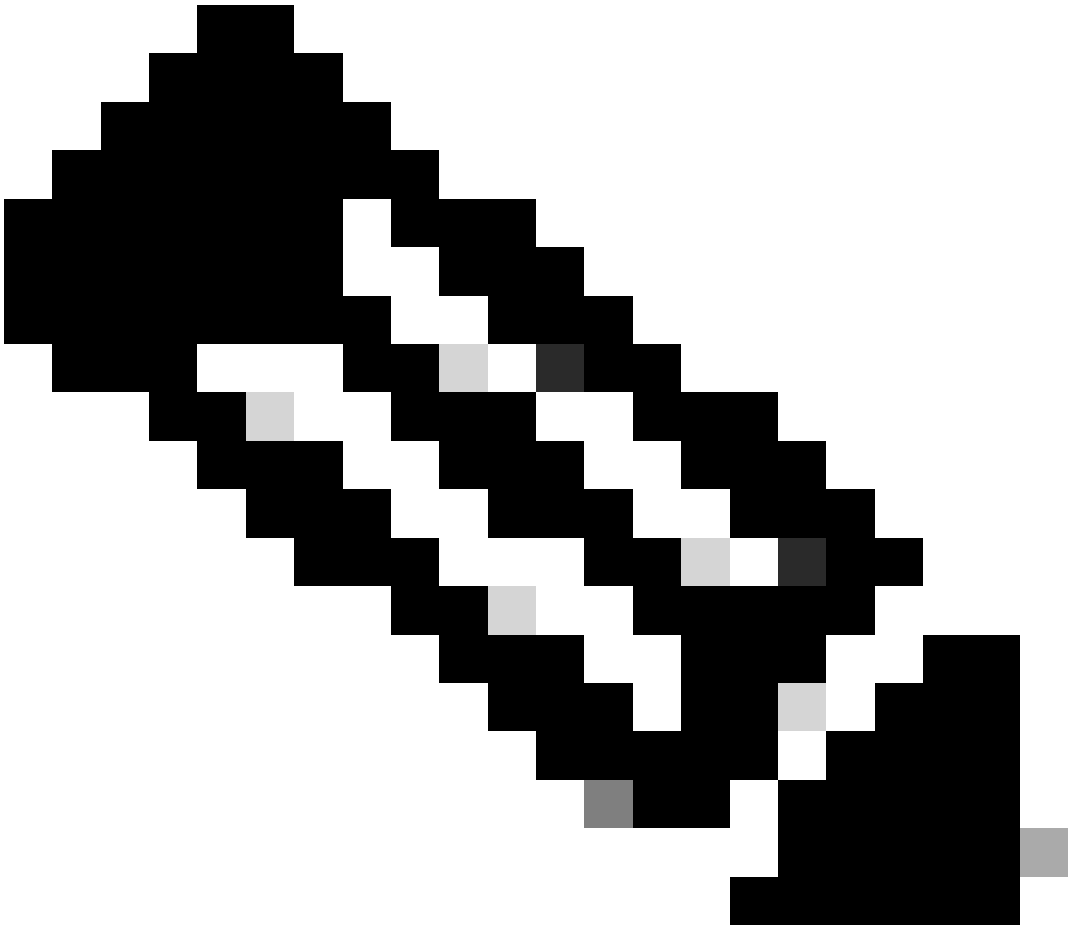
Esta configuración debe utilizar eBGP para los pares, donde la dirección de origen (dirección IP virtual para la IP del túnel local) subred del lado NFVIS debe agregarse al rango de escucha.

```
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
```

Where:

| | |
|---|---|
| bgp always-compare-med | Configura el router para comparar siempre el atributo MED (Multi-Exit Discriminator) para todas las rutas, independientemente de su AS de origen. |
| bgp log-neighbor-changes | Habilita el registro de eventos relacionados con cambios en las relaciones de vecinos BGP. |
| bgp deterministic-med | Asegura la comparación del MED para trayectos de vecinos en diferentes sistemas autónomos. |
| bgp listen range <network>/<mask> peer-group <peer-group-name> | Habilita la detección de vecinos dinámicos dentro del rango de IP especificado (red/máscara) y asigna los vecinos detectados al nombre del grupo de pares. Esto simplifica la configuración al aplicar la configuración común a todos los peers del grupo. |
| bgp listen limit 255 | Establece el número máximo de vecinos BGP dinámicos que se pueden aceptar dentro del rango de escucha en 255. |
| no bgp default ipv4-unicast | Inhabilita el envío automático de información de ruteo unicast IPv4 a los vecinos BGP, lo que requiere una configuración |

| | |
|---|---|
| | explícita para habilitar esto. |
| redistribute connected | Redistribuye rutas de redes conectadas directamente en BGP (subredes privadas del servidor FlexVPN que pertenecen al vrf privado) |
| redistribute static | Redistribuye las rutas estáticas en BGP. |
| neighbor uCPEs ebgp-multihop 10 | Permite que las conexiones EBGP (BGP externo) con peers en el grupo de peers abarquen hasta 10 saltos, útil para conectar dispositivos no adyacentes directamente. |
| neighbor uCPEs timers <keep-alive> <hold-down> | Establece los temporizadores keepalive y hold-down BGP para los vecinos en el grupo de peers respectivamente (610 segundos y 1835 segundos para el ejemplo). |



Nota: Se puede configurar una lista de prefijos salientes para controlar los anuncios de ruta de vecino en el grupo de peers: neighbor prefix-list out

## Configuración de BGP en NFVIS

Iniciar el proceso BGP con la configuración de vecindad eBGP

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

Revisión de BGP

Este resultado revela la condición de una sesión BGP según lo informado por el daemon de ruteo de Internet BIRD. Este software de ruteo es responsable de manejar las rutas IP y tomar decisiones con respecto a su dirección. A partir de la información proporcionada, queda claro que la sesión de BGP se encuentra en un estado "Establecido", lo que indica que el proceso de peering de BGP se ha completado con éxito y que la sesión está actualmente activa. Ha importado correctamente cuatro rutas y ha observado que hay un límite superior de 15 rutas que se pueden importar.

```
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
```

Asegúrese de que las subredes privadas del servidor FlexVPN se anunciaron a través de BGP

Al configurar el anuncio de ruta BGP, la única combinación configurable de familia de direcciones o transmisión es ipv4 unicast para IPSec. Para ver el estado de BGP, la familia de direcciones o transmisión configurable para IPSec es unicast vpnv4.

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

Con el comando show bgp vpnv4 unicast route, puede recuperar información sobre las rutas unicast VPNv4 conocidas para el proceso 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 ?
```

Para el servidor VPN de cabecera, se puede generar una descripción general de la configuración BGP y del estado operativo para evaluar rápidamente el estado y la configuración de las sesiones 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
```

Además, se puede mostrar información detallada acerca de las entradas de la tabla de ruteo VPNv4 (VPN sobre IPv4) administradas por BGP; debe incluir atributos específicos de cada ruta VPNv4, como el prefijo de rutas, la dirección IP del siguiente salto, el número de AS de origen y varios atributos BGP como la preferencia local, MED (Multi-Exit Discriminator) y valores de comunidad.

```
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 ?
```

# Resolución de problemas

## NFVIS (cliente FlexVPN)

### Archivos de registro NFVIS

Puede ver todos los registros de inicialización y errores de las fases de IPsec desde el archivo de registro charon.log de 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_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
```

### Rutas inyectadas de Strongswan del núcleo interno

En Linux, strongSwan (implementación IPsec multiplataforma utilizada por NFVIS) instala rutas (incluidas rutas unicast BGP VPNv4) en la tabla de ruteo 220 de forma predeterminada y, por lo

tanto, requiere que el núcleo admita el ruteo basado en políticas.

```
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
```

Revisar el estado de la interfaz IPsec0

Puede obtener más detalles sobre la interfaz virtual ipsec0 con el uso de 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
```

## Cabecera (servidor FlexVPN)

Revisar compilación de SAs IPsec entre pares

A partir de la siguiente salida, el túnel cifrado se crea entre 10.88.247.84 a través de la interfaz Virtual-Access1 y 10.88.247.89 para el tráfico que va entre las redes 0.0.0.0/0 y 10.122.144.128/27; dos SA de carga de seguridad de encapsulación (ESP) integradas de forma entrante y saliente.

```
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:
```

Mostrar sesiones de cifrado activas (cifrado)

El resultado de show crypto session detail debe proporcionar detalles completos sobre cada sesión crypto activa, incluyendo el tipo de VPN (como sitio a sitio o acceso remoto), los algoritmos de cifrado y hash en uso, y las asociaciones de seguridad (SA) para el tráfico entrante y saliente. Dado que también muestra estadísticas sobre el tráfico cifrado y descifrado, como el número de paquetes y bytes, puede resultar útil para supervisar la cantidad de datos que protege la VPN y para solucionar problemas de rendimiento.

```
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
```

Restablecer conexiones VPN

Los comandos clear crypto se utilizan para restablecer manualmente las conexiones VPN o borrar las asociaciones de seguridad (SA) sin necesidad de reiniciar todo el dispositivo.

- clear crypto ikev2 borraría las asociaciones de seguridad IKEv2 (IKEv2 SAs).
- clear crypto session borraría IKEv1 (isakmp)/IKEv2 e IPSec SA.
- clear crypto sa borraría solamente las SAs IPSec.
- clear crypto ipsec sa eliminaría las asociaciones de seguridad IPSec activas.

Realizar depuraciones para resolución de problemas adicional

Los debugs de IKEv2 pueden ayudar a identificar y solucionar los errores en el dispositivo de cabecera (c8000v) que pueden ocurrir durante el proceso de negociación de IKEv2 y las conexiones del cliente FlexVPN, como los problemas con el establecimiento de la sesión VPN, la aplicación de políticas o cualquier error específico del cliente.

```
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
```

## Artículos y documentación relacionados

Superposición segura y configuración de IP única

Soporte BGP en NFVIS

Comandos Secure Overlay y BGP

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).