Configurar sobreposição segura com anúncios de rota BGP

Contents

Introdução

Este documento descreve como configurar a sobreposição segura e anúncios eBGP em NFVIS para gerenciamento de tráfego vBranch exclusivo.

Componentes Utilizados

As informações neste documento são baseadas nestes componentes de hardware e software:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Anúncio de rota BGP

O recurso NFVIS BGP funciona com o recurso de sobreposição segura para aprender rotas do vizinho BGP sobre um túnel de sobreposição segura. Essas rotas ou sub-redes aprendidas são adicionadas à tabela de roteamento NFVIS para o túnel seguro, o que torna as rotas acessíveis pelo túnel. Como o Secure Overlay permite apenas que uma única rota privada seja aprendida do túnel, a configuração do BGP permite superar essa limitação estabelecendo adjacência através do túnel criptografado e injetando rotas exportadas na tabela de roteamento NFVIS vpnv4 e vice-versa.

Exemplo de configuração

Diagrama de topologia

O objetivo dessa configuração é alcançar o endereço IP de gerenciamento de NFVIS a partir do c8000v. Uma vez que o túnel é estabelecido, é possível anunciar mais rotas das sub-redes vrf privadas usando anúncios de rota eBGP.

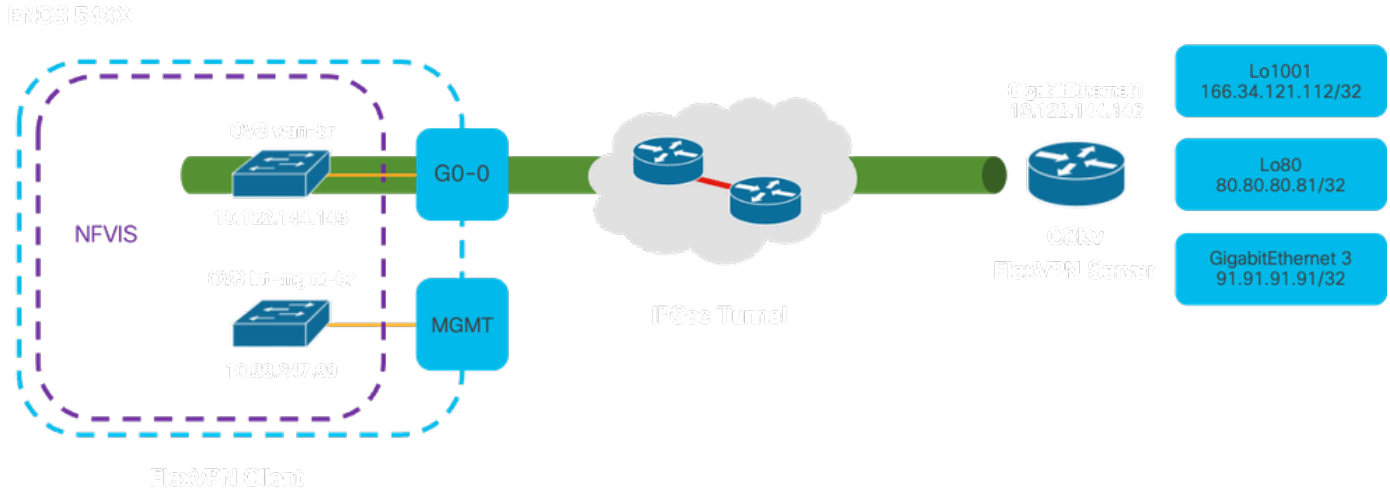


Figura 1. Diagrama de Topologia para o Exemplo preparado neste artigo

Configuração inicial

Configure o endereçamento IP relevante no servidor FlexVPN (tudo no modo de configuração 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 a interface WAN e de GERENCIAMENTO de acordo

```
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
!
```

Configuração do servidor FlexVPN no roteador Catalyst 8000v

1. Criar uma Proposta IKEv2

Ele especifica os protocolos e algoritmos de segurança que dois endpoints VPN devem usar durante a fase inicial (Fase 1) do estabelecimento de um canal de comunicação seguro. O objetivo da proposta IKEv2 é delinear os parâmetros para autenticação, criptografia, integridade e

troca de chave, garantindo assim que ambos os endpoints concordem com um conjunto comum de medidas de segurança antes de trocar quaisquer dados confidenciais.

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

Where:

encryption <algorithm>	A proposta inclui os algoritmos de criptografia (como AES ou 3DES) que a VPN deve usar para proteger os dados. A criptografia impede que bisbilhoteiros leiam o tráfego que passa pelo túnel VPN.
Integridade <hash>	Especifica os algoritmos (como SHA-512) usados para garantir a integridade e a autenticidade das mensagens trocadas durante a negociação de IKEv2. Isso evita adulterações e ataques de repetição.

2. Crie uma Política IKEv2 e Associe-a à Proposta.

É um conjunto de configurações que determina os parâmetros para a fase inicial (fase 1) de estabelecimento de uma conexão VPN IPsec. Ele se concentra principalmente em como os endpoints VPN se autenticam e estabelecem um canal de comunicação seguro para a configuração da VPN.

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

3. Configurar a Política de Autorização IKEv2

O IKEv2 é um protocolo usado para configurar uma sessão segura entre dois pontos finais em uma rede, e a política de autorização é um conjunto de regras que determina quais recursos e serviços um cliente VPN tem permissão para acessar depois que o túnel VPN é estabelecido.

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

Where:

pfs	O PFS (Perfect Forward Secrecy) é um recurso que aumenta a segurança de

	uma conexão VPN, garantindo que cada nova chave de criptografia seja protegida de forma independente, mesmo que as chaves anteriores sejam comprometidas.
route set interface <interface-name>	Quando uma sessão VPN é estabelecida com êxito, as rotas definidas na política de autorização de IKEv2 são automaticamente adicionadas à tabela de roteamento do dispositivo. Isso garante que o tráfego destinado às redes especificadas no conjunto de rotas seja roteado corretamente através do túnel VPN.

4. Criar um Perfil IKEv2

Uma política IKEv2 (Internet Key Exchange versão 2) é um conjunto de regras ou parâmetros usados durante a fase IKEv2 do estabelecimento de um túnel VPN IPsec (Internet Protocol Security). O IKEv2 é um protocolo que facilita a troca segura de chaves e a negociação de associações de segurança (SAs) entre duas partes que desejam se comunicar com segurança através de uma rede não confiável, como a Internet. A política IKEv2 define como essa negociação deve ocorrer, especificando vários parâmetros de segurança que ambas as partes devem concordar para estabelecer um canal de comunicação seguro e criptografado.

O perfil IKEv2 DEVE ter:

- Um método de autenticação local e remoto.
- Uma identidade de correspondência ou um certificado de correspondência ou qualquer instrução correspondente.

```
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	Crie um perfil com reconhecimento de vrf.
match identity remote any	Medida para reconhecer uma sessão de entrada como válida; nesse caso, qualquer pessoa.
chave pré-compartilhamento remota de autenticação ciscocisco123	Especifica que o par remoto deve ser autenticado usando chaves pré-compartilhadas.
chave pré-compartilhamento local de autenticação ciscocisco123	Especifica que este dispositivo (local) deve se autenticar usando chaves pré-compartilhadas.

dpd 60 2 sob demanda	Dead Peer Detection; se nenhum pacote foi recebido durante um minuto (60 segundos), envie 2 pacotes dpd dentro desse intervalo de 60 segundos.
aaa authorization group psk list default uCPE-author-pol local	Atribuição de rota.
virtual-template 1 mode auto	Vincular a um modelo virtual.

5. Criar um Conjunto de Transformação IPsec

Ele define um conjunto de protocolos e algoritmos de segurança que devem ser aplicados ao tráfego de dados que passa pelo túnel IPsec. Essencialmente, o conjunto de transformação especifica como os dados devem ser criptografados e autenticados, garantindo uma transmissão segura entre os pontos terminais da VPN. O modo de túnel configura o túnel IPsec para encapsular todo o pacote IP para transporte seguro através da rede.

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

Where:

set transform-set <transform-set-name>	Especifica os algoritmos de criptografia e integridade (Exemplo: AES para criptografia e SHA para integridade) que devem ser usados para proteger o fluxo de dados pelo túnel VPN.
set ikev2-profile <ikev2-profile-name>	Define os parâmetros para a negociação das associações de segurança (SAs) na fase 1 da configuração da VPN, incluindo algoritmos de criptografia, algoritmos de hash, métodos de autenticação e o grupo Diffie-Hellman.
set pfs <group>	Uma configuração opcional que, se habilitada, garante que cada nova chave de criptografia não esteja relacionada a nenhuma chave anterior, aumentando a segurança.

6. Remover Perfil IPsec Padrão

A remoção do perfil IPsec padrão é uma prática adotada por vários motivos relacionados à segurança, personalização e clareza do sistema. O perfil IPsec padrão não pode atender às políticas de segurança específicas ou aos requisitos da sua rede. A sua remoção garante que nenhum túnel VPN use inadvertidamente configurações inadequadas ou inseguras, reduzindo o risco de vulnerabilidades.

Cada rede tem requisitos de segurança exclusivos, incluindo algoritmos específicos de criptografia e hash, tamanhos de chave e métodos de autenticação. A remoção do perfil padrão incentiva a criação de perfis personalizados adaptados a essas necessidades específicas, garantindo a melhor proteção e desempenho possíveis.

```
no crypto ipsec profile default
```

7. Crie um perfil IPsec e associe-o a um conjunto de transformação e ao perfil IKEv2.

Um perfil IPsec (Internet Protocol Security) é uma entidade de configuração que encapsula as configurações e políticas usadas para estabelecer e gerenciar túneis VPN IPsec. Ele serve como um modelo que pode ser aplicado a várias conexões VPN, padronizando parâmetros de segurança e simplificando o gerenciamento de comunicação segura em uma rede.

```
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. Criar um Modelo Virtual

A interface Virtual-Template atua como um modelo dinâmico para interfaces de acesso virtual, fornecendo uma maneira escalável e eficiente de gerenciar conexões VPN. Ele permite a instanciação dinâmica de interfaces de acesso virtual. Quando uma nova sessão VPN é iniciada, o dispositivo cria uma interface de Acesso Virtual com base na configuração especificada no Modelo Virtual. Esse processo suporta um grande número de clientes remotos e locais, alocando dinamicamente recursos conforme necessário, sem a necessidade de interfaces físicas pré-configuradas para cada conexão.

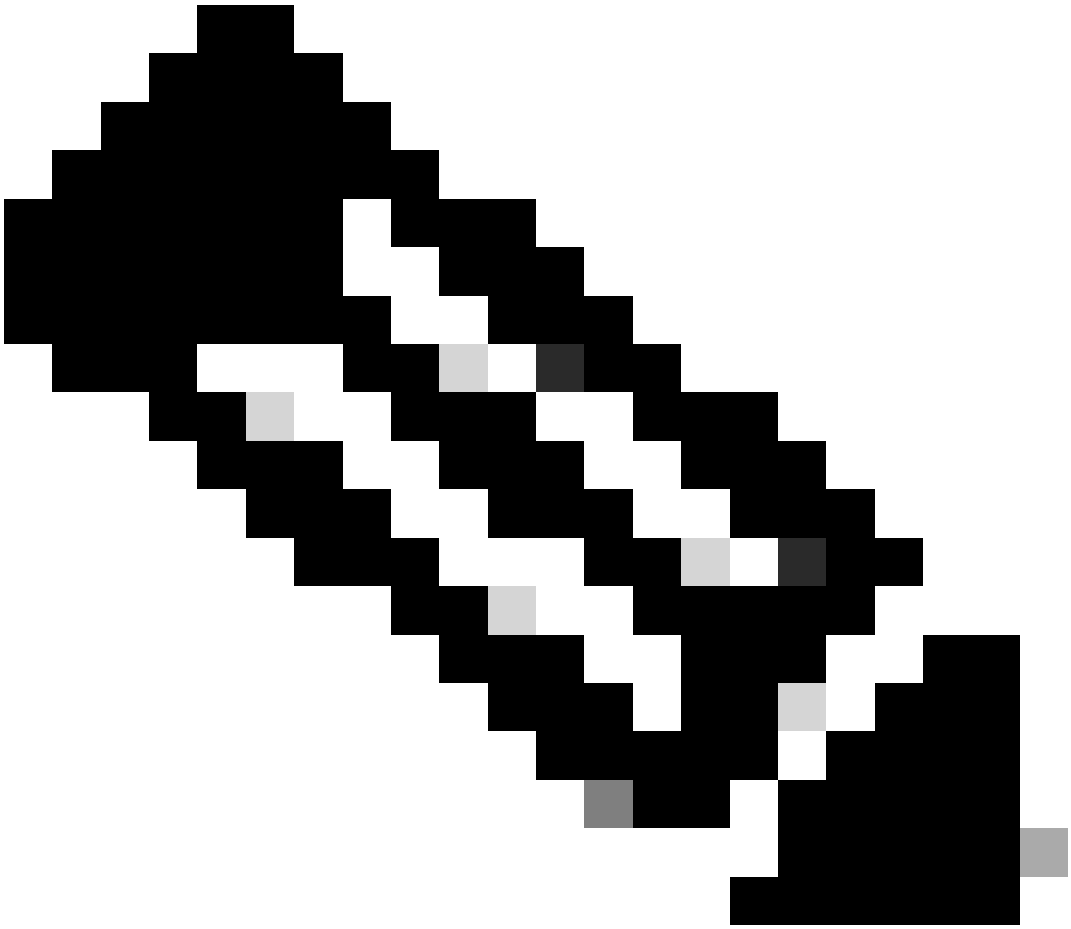
Com o uso de modelos virtuais, as implantações do FlexVPN podem ser dimensionadas com eficiência à medida que novas conexões são estabelecidas, sem a necessidade de configuração manual de cada sessão individual.

```
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
```

Configuração mínima de sobreposição segura NFVIS

Configurar a instância de sobreposição 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
```



Observação: ao configurar o anúncio de rota BGP sobre um túnel IPSec, certifique-se de configurar a sobreposição segura para usar um endereço IP virtual (não originado de uma interface física ou ponte OVS) para o endereço IP do túnel local. Para o exemplo acima, estes são os comandos de endereçamento virtual alterados: local-system-ip-addr 10.122.144.146 local-system-ip-subnet 10.122.144.128/27

Revisar Status de Sobreposição

```
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
```

Configuração de anúncio de rota BGP para o servidor FlexVPN

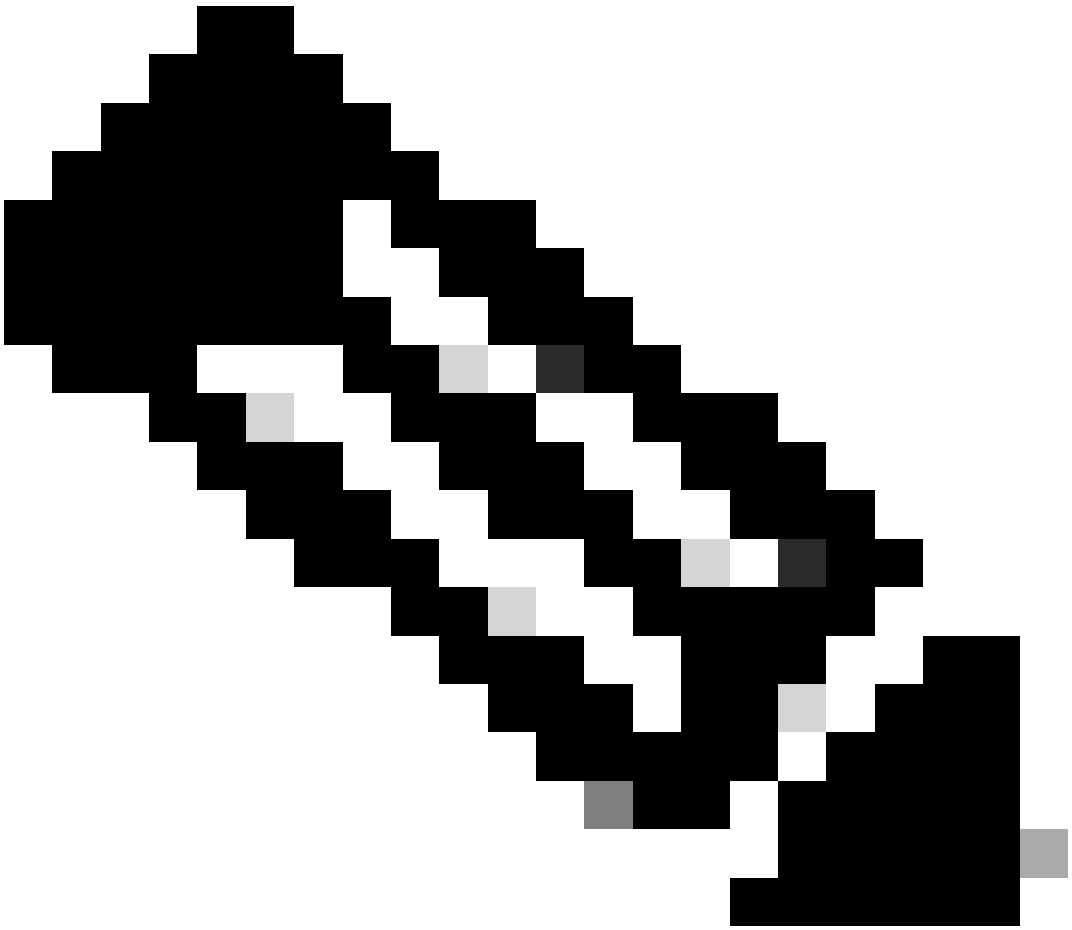
Esta configuração deve usar o eBGP para os peers, onde o endereço de origem (endereço IP virtual para o IP do túnel local) da sub-rede do lado NFVIS deve ser adicionado ao intervalo de escuta.

```
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 o roteador para sempre comparar o atributo MED (Multi-Exit Discriminator) para todas as rotas, independentemente de seu AS de origem.
bgp log-neighbor-changes	Habilita o log de eventos relacionados a alterações nas relações de vizinhança BGP.
bgp deterministic-med	Garante a comparação do MED para caminhos de vizinhos em diferentes sistemas autônomos.
bgp listen range <network>/<mask> peer-group <peer-group-name>	Habilita a descoberta dinâmica de vizinhos dentro do intervalo de IP especificado (rede/máscara) e atribui vizinhos descobertos ao nome do grupo de peer. Isso simplifica a configuração aplicando configurações comuns a todos os pares no grupo.
bgp listen limit 255	Define o número máximo de vizinhos BGP dinâmicos que podem ser aceitos dentro do intervalo de escuta como 255.
no bgp default ipv4-unicast	Desabilita o envio automático de informações de roteamento

	unicast IPv4 para vizinhos BGP, exigindo configuração explícita para habilitar isso.
redistribute connected	Redistribui rotas de redes conectadas diretamente no BGP (sub-redes privadas do servidor FlexVPN que pertencem ao vrf privado)
redistribute static	Redistribui rotas estáticas no BGP.
neighbor uCPEs ebgp-multihop 10	Permite conexões EBGP (BGP Externo) com pares no grupo de pares para abranger até 10 saltos, útil para conectar dispositivos não adjacentes diretamente.
neighbor uCPEs timers <keep-alive> <hold-down>	Define os temporizadores keepalive e hold-down do BGP para vizinhos no grupo de peer respectivamente (610 segundos e 1835 segundos para o exemplo).



Observação: uma lista de prefixos de saída pode ser configurada para controlar anúncios de rotas de vizinhos no grupo de pares: neighbor prefix-list out

Configuração de BGP em NFVIS

Inicie o processo BGP com as configurações de vizinhança do eBGP

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

Revisão de BGP

Essa saída revela a condição de uma sessão BGP conforme relatada pelo daemon de roteamento de Internet BIRD. Esse software de roteamento é responsável por manipular rotas IP e tomar decisões relacionadas à direção. A partir das informações fornecidas, fica claro que a sessão BGP está em um estado "Estabelecido", indicando a conclusão bem-sucedida do processo de peering BGP, e a sessão está atualmente ativa. Ela importou com êxito quatro rotas e observou que há um limite máximo de 15 rotas que podem ser importadas.

```
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
```

Assegure-se de que as sub-redes privadas do servidor FlexVPN foram anunciadas através do BGP

Ao configurar o anúncio de rota BGP, a única combinação configurável de família de endereços ou transmissão é ipv4 unicast para IPSec. Para visualizar o status do BGP, a família de endereços configurável ou transmissão para IPSec é unicast vpnv4.

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

Com o comando show bgp vpnv4 unicast route, você pode recuperar informações sobre as rotas unicast VPNv4 conhecidas pelo 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 ?
```

Para o servidor VPN headend, uma visão geral da configuração do BGP e do estado operacional pode ser gerada para avaliar rapidamente a integridade e a configuração das sessões de 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
```

Além disso, informações detalhadas sobre as entradas da tabela de roteamento de VPNv4 (VPN sobre IPv4) gerenciadas pelo BGP podem ser exibidas, elas devem incluir atributos específicos de cada rota de VPNv4, como o prefixo de rotas, o endereço IP do próximo salto, o número AS de origem e vários atributos de BGP, como preferência local, MED (Multi-Exit Discriminator) e valores de comunidade.

```
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 ?
```

Troubleshooting

NFVIS (FlexVPN Client)

Arquivos de log NFVIS

Você pode exibir todos os logs de inicialização e de erro das fases do IPsec no arquivo de log charon.log do 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
```

Rotas injetadas strongswan de kernel interno

No Linux, o strongswan (implementação de IPsec multiplataforma usada pelo NFVIS) instala rotas (incluindo rotas unicast BGP VPNv4) na tabela de roteamento 220 por padrão e, portanto, requer o kernel para suportar o roteamento baseado em política.

```
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 o status da interface IPsec0

Você pode obter mais detalhes sobre a interface virtual ipsec0 com o 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
```

Central (servidor FlexVPN)

Revisar SAs IPsec Criadas Entre Pares

A partir da saída abaixo, o túnel criptografado é construído entre 10.88.247.84 através da interface Virtual-Access1 e 10.88.247.89 para o tráfego que vai entre as redes 0.0.0.0/0 e 10.122.144.128/27; duas SAs ESP (Encapsulating Security Payload) construídas dentro e fora.

```
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:
```

Exibir sessões de criptografia ativas

A saída do comando show crypto session detail deve fornecer detalhes abrangentes sobre cada sessão de criptografia ativa, incluindo o tipo de VPN (como acesso de site a site ou remoto), os algoritmos de criptografia e hash em uso e as associações de segurança (SAs) para tráfego de entrada e saída. Como ele também exibe estatísticas sobre o tráfego criptografado e descriptografado, como o número de pacotes e bytes; isso pode ser útil para monitorar a quantidade de dados protegidos pela VPN e para solucionar problemas de throughput.

```
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
```

Redefinir Conexões VPN

Os comandos clear cryptosão usados para redefinir manualmente conexões VPN ou limpar associações de segurança (SAs) sem precisar reinicializar o dispositivo inteiro.

- clear crypto ikev2 limparia associações de segurança IKEv2 (SAs IKEv2).
- clear crypto session limparia IKEv1 (isakmp)/IKEv2 e IPSec SAs.
- clear crypto sa limparia somente as SAs de IPSec.
- clear crypto ipsec sa excluiria as associações de segurança IPSec ativas.

Executar depurações para solução de problemas adicional

As depurações de IKEv2 podem ajudar a identificar e solucionar erros no dispositivo headend (c8000v) que podem ocorrer durante o processo de negociação de IKEv2 e conexões de cliente FlexVPN, como problemas com o estabelecimento da sessão VPN, aplicação de política ou qualquer erro específico do 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
```

Artigos e documentação relacionados

Sobreposição segura e configuração de IP único

Suporte de BGP em NFVIS

Sobreposição segura e comandos BGP

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.