# Konfigurieren von sicherem Overlay mit BGP-Routenankündigungen

## Inhalt



## Einleitung

In diesem Dokument wird beschrieben, wie sichere Overlay- und eBGP-Ankündigungen auf NFVIS für die exklusive Verwaltung des vBranch-Datenverkehrs konfiguriert werden.

# Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Hardware- und Softwarekomponenten:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Ankündigung der BGP-Route

Die NFVIS BGP-Funktion arbeitet mit der Funktion für sicheres Overlay zusammen, um Routen vom BGP-Nachbarn über einen sicheren Overlay-Tunnel abzurufen. Diese übergebenen Routen oder Subnetze werden der NFVIS-Routing-Tabelle für den sicheren Tunnel hinzugefügt, wodurch die Routen über den Tunnel zugänglich sind. Da Secure Overlay nur das Abrufen einer einzelnen privaten Route aus dem Tunnel zulässt, ermöglicht die Konfiguration von BGP das Überwinden dieser Einschränkung, indem Adjacency über den verschlüsselten Tunnel eingerichtet und exportierte Routen in die NFVIS-Routing-Tabelle "vpnv4" und umgekehrt eingespeist werden.

# Konfigurationsbeispiel

## Topologiediagramm

Ziel dieser Konfiguration ist es, die Management-IP-Adresse von NFVIS aus dem c8000v zu erreichen. Sobald der Tunnel eingerichtet ist, können mithilfe von eBGP-Routenankündigungen weitere Routen aus den Private-VRF-Subnetzen angekündigt werden.

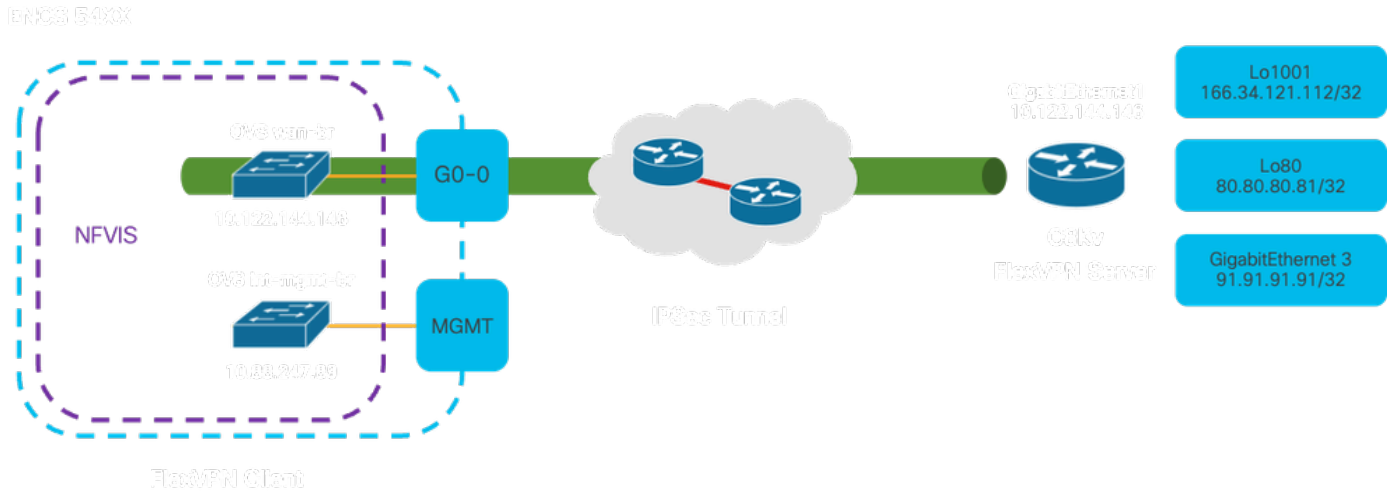



Abbildung 1. Topologiediagramm für das auf diesem Artikel vorbereitete Beispiel

## Ersteinrichtung

Konfigurieren der relevanten IP-Adressierung auf dem FlexVPN-Server (alle im globalen Konfigurationsmodus)

```
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
```

Konfigurieren Sie für NFVIS die WAN- und MGMT-Schnittstelle entsprechend.

```
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
!
```

## FlexVPN-Serverkonfiguration auf dem Catalyst 8000v-Router

1. Erstellen eines IKEv2-Angebots

Sie spezifiziert die Sicherheitsprotokolle und -algorithmen, die zwei VPN-Endpunkte in der Anfangsphase (Phase 1) des Aufbaus eines sicheren Kommunikationskanals verwenden müssen. Der Zweck des IKEv2-Vorschlags besteht darin, die Parameter für Authentifizierung, Verschlüsselung, Integrität und Schlüsselaustausch zu skizzieren und so sicherzustellen, dass sich beide Endpunkte vor dem Austausch vertraulicher Daten auf gemeinsame Sicherheitsmaßnahmen einigen.

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

Dabei gilt:

| | |
|---|---|
| encryption <Algorithmus> | Der Vorschlag enthält die Verschlüsselungsalgorithmen (wie AES oder 3DES), die das VPN zum Schutz der Daten verwenden muss. Die Verschlüsselung verhindert, dass Abhörer den Datenverkehr, der durch den VPN-Tunnel fließt, lesen können. |
| Integrität <Hash> | Es legt die Algorithmen (z. B. SHA-512) fest, die verwendet werden, um die Integrität und Authentizität der Nachrichten sicherzustellen, die während der IKEv2-Aushandlung ausgetauscht werden. Dadurch werden Manipulationen und Wiederholungen von Angriffen verhindert. |

2. Erstellen Sie eine IKEv2-Richtlinie, und ordnen Sie sie dem Angebot zu.

Es handelt sich um einen Konfigurationssatz, der die Parameter für die Anfangsphase (Phase 1) des Aufbaus einer IPsec-VPN-Verbindung vorgibt. Der Schwerpunkt liegt dabei auf der gegenseitigen Authentifizierung der VPN-Endpunkte und der Einrichtung eines sicheren Kommunikationskanals für die VPN-Einrichtung.

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

3. Konfigurieren der IKEv2-Autorisierungsrichtlinie

IKEv2 ist ein Protokoll zum Einrichten einer sicheren Sitzung zwischen zwei Endpunkten in einem Netzwerk. Die Autorisierungsrichtlinie besteht aus einem Satz von Regeln, die festlegen, auf welche Ressourcen und Services ein VPN-Client zugreifen darf, sobald der VPN-Tunnel eingerichtet ist.

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

Dabei gilt:

| | |
|---|---|
| Pfs | Perfect Forward Secrecy (PFS) ist eine Funktion, die die Sicherheit einer VPN-Verbindung erhöht, indem sichergestellt wird, dass jeder neue Verschlüsselungsschlüssel unabhängig sicher ist, auch wenn vorherige Schlüssel kompromittiert wurden. |
| route set interface <Schnittstellenname> | Wenn eine VPN-Sitzung erfolgreich hergestellt wurde, werden die in der IKEv2-Autorisierungsrichtlinie definierten Routen automatisch zur Routing-Tabelle des Geräts hinzugefügt. Dadurch wird sichergestellt, dass der Datenverkehr, der für die im Routensatz angegebenen Netzwerke bestimmt ist, ordnungsgemäß durch den VPN-Tunnel geleitet wird. |

4. IKEv2-Profil erstellen

Eine IKEv2-Richtlinie (Internet Key Exchange Version 2) ist ein Satz von Regeln oder Parametern, die während der IKEv2-Phase zum Einrichten eines IPsec-VPN-Tunnels (Internet Protocol Security) verwendet werden. IKEv2 ist ein Protokoll, das den sicheren Austausch von Schlüsseln und die Aushandlung von Sicherheitszuordnungen (Security Associations, SAs) zwischen zwei Parteien ermöglicht, die sicher über ein nicht vertrauenswürdiges Netzwerk wie das Internet kommunizieren möchten. Die IKEv2-Richtlinie legt fest, wie diese Aushandlung stattfinden soll. Sie legt verschiedene Sicherheitsparameter fest, auf die sich beide Parteien einigen müssen, um einen sicheren und verschlüsselten Kommunikationskanal einzurichten.

IKEv2-Profil MUSS folgende Merkmale aufweisen:

- Eine lokale und eine Remote-Authentifizierungsmethode.
- Eine Übereinstimmungsidentität, ein Übereinstimmungszertifikat oder eine beliebige Anweisung.

```
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
```

Dabei gilt:

| | |
|---|---|
| Übereinstimmung mit öffentlichem VRF | Profil VRF-fähig machen. |

| | |
|---|---|
| Übereinstimmung Identität Remote any | Ermitteln Sie, ob eine eingehende Sitzung gültig ist. In diesem Fall jeder. |
| Authentifizierung, Remote, Pre-Share-Schlüssel CiscoCiscoCisco123 | Gibt an, dass der Remote-Peer mithilfe von vorinstallierten Schlüsseln authentifiziert werden muss. |
| Authentifizierung, lokaler Pre-Share-Schlüssel CiscoCiscoCisco123 | Gibt an, dass dieses Gerät (lokal) mithilfe von vorinstallierten Schlüsseln authentifiziert werden muss. |
| dpd 60 2 On-Demand | Dead Peer Detection: Wenn über eine Minute (60 Sekunden) keine Pakete empfangen wurden, senden Sie innerhalb dieses 60-Sekunden-Intervalls 2 dpd-Pakete. |
| aaa, Autorisierungsgruppe PSK-Liste Standard uCPE-author-pol lokal | Routenzuweisung. |
| Virtual-Template 1 Modus automatisch | An eine virtuelle Vorlage binden. |

5. IPsec-Transformationssatz erstellen

Sie definiert eine Reihe von Sicherheitsprotokollen und -algorithmen, die auf den Datenverkehr angewendet werden müssen, der durch den IPsec-Tunnel läuft. Im Wesentlichen legt der Transformationssatz fest, wie die Daten verschlüsselt und authentifiziert werden müssen, um eine sichere Übertragung zwischen VPN-Endpunkten zu gewährleisten. Im Tunnelmodus wird der IPsec-Tunnel so konfiguriert, dass das gesamte IP-Paket gekapselt wird, um einen sicheren Transport im Netzwerk zu gewährleisten.

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

Dabei gilt:

| | |
|---|---|
| set transform-set <Transformationssatzname> | Gibt die Verschlüsselungs- und Integritätsalgorithmen an (Beispiel: AES für Verschlüsselung und SHA für Integrität), die zum Schutz der Daten verwendet werden müssen, die durch den VPN-Tunnel fließen. |
| set ikev2-profile <ikev2-Profilname> | Definiert die Parameter für die Aushandlung der Sicherheitszuordnungen (Security Associations, SAs) in Phase 1 der VPN-Konfiguration, einschließlich Verschlüsselungsalgorithmen, Hash-Algorithmen, Authentifizierungsmethoden und der Diffie-Hellman-Gruppe. |
| set pfs <Gruppe> | Eine optionale Einstellung, die bei Aktivierung sicherstellt, dass jeder neue Verschlüsselungsschlüssel unabhängig von einem vorherigen Schlüssel ist, wodurch die Sicherheit erhöht wird. |

6. Standard-IPsec-Profil entfernen

Das Entfernen des Standard-IPsec-Profils wird aus verschiedenen Gründen im Zusammenhang mit Sicherheit, Anpassung und Systemübersichtlichkeit durchgeführt. Das Standard-IPsec-Profil kann die spezifischen Sicherheitsrichtlinien oder Anforderungen Ihres Netzwerks nicht erfüllen. Durch das Entfernen wird sichergestellt, dass keine VPN-Tunnel versehentlich suboptimale oder unsichere Einstellungen verwenden, wodurch das Risiko von Schwachstellen verringert wird.

Jedes Netzwerk stellt spezielle Sicherheitsanforderungen, z. B. spezielle Verschlüsselungs- und Hashing-Algorithmen, Schlüssellängen und Authentifizierungsverfahren. Das Entfernen des Standardprofils fördert die Erstellung individueller Profile, die auf diese spezifischen Anforderungen zugeschnitten sind, und gewährleistet bestmöglichen Schutz und optimale Leistung.

```
no crypto ipsec profile default
```

7. Erstellen Sie ein IPsec-Profil, und ordnen Sie es einem Transformationssatz und dem IKEv2-Profil zu.

Ein IPsec-Profil (Internet Protocol Security) ist eine Konfigurationseinheit, die die Einstellungen und Richtlinien für die Einrichtung und Verwaltung von IPsec-VPN-Tunneln kapselt. Es dient als Vorlage, die auf mehrere VPN-Verbindungen angewendet werden kann, wodurch Sicherheitsparameter standardisiert und die Verwaltung sicherer Kommunikation im Netzwerk vereinfacht werden.

```
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. Erstellen einer virtuellen Vorlage

Die Virtual-Template-Schnittstelle fungiert als dynamische Vorlage für virtuelle Zugriffsschnittstellen und bietet eine skalierbare und effiziente Möglichkeit zum Verwalten von VPN-Verbindungen. Es ermöglicht die dynamische Instanziierung von Virtual-Access-Schnittstellen. Wenn eine neue VPN-Sitzung initiiert wird, erstellt das Gerät eine Virtual-Access-Schnittstelle auf Grundlage der in der Virtual-Template angegebenen Konfiguration. Dieser Prozess unterstützt eine große Anzahl von Remote-Clients und Standorten, indem Ressourcen bei Bedarf dynamisch zugewiesen werden, ohne dass für jede Verbindung vorkonfigurierte physische Schnittstellen erforderlich sind.

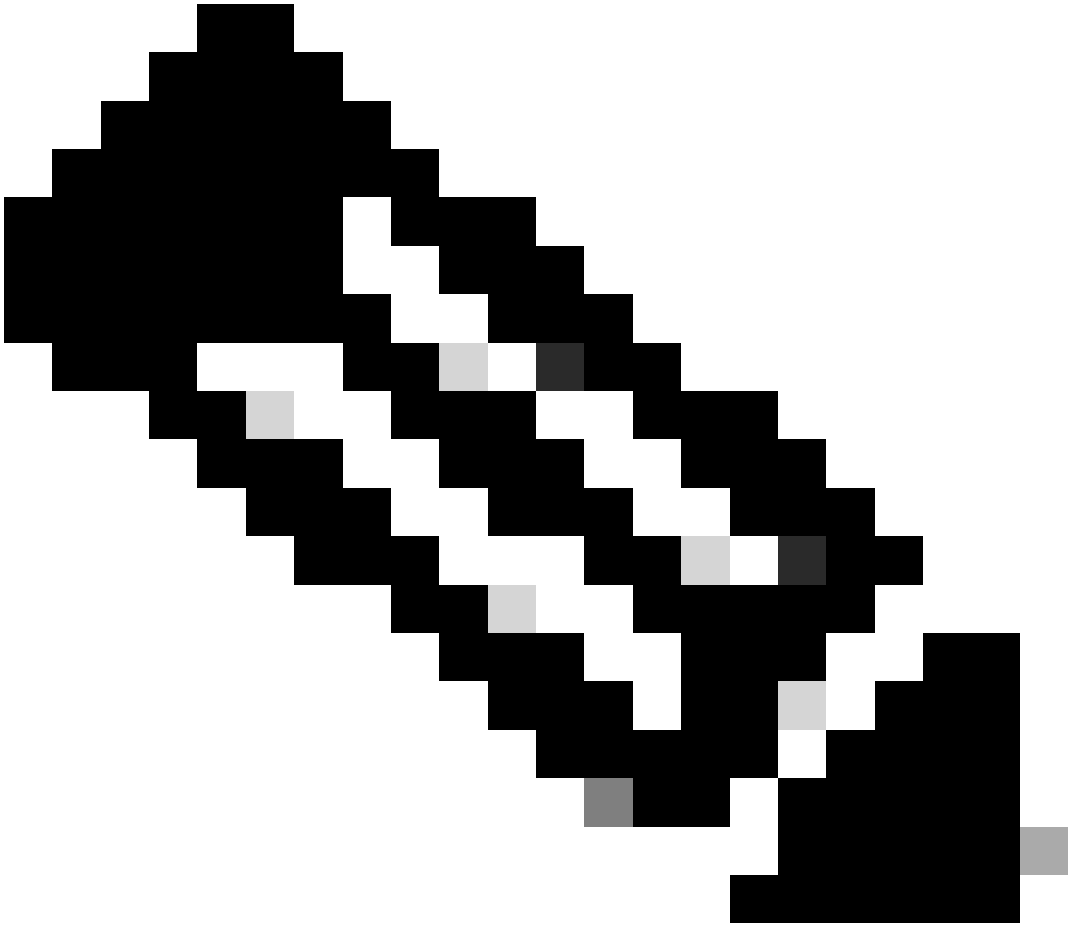
Durch die Verwendung virtueller Vorlagen können FlexVPN-Bereitstellungen effizient skaliert werden, wenn neue Verbindungen hergestellt werden, ohne dass jede einzelne Sitzung manuell konfiguriert werden muss.

```
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
```

## Minimale NFVIS Secure Overlay-Konfiguration

### Konfigurieren der Secure-Overlay-Instanz

```
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
```



Hinweis: Wenn Sie die Ankündigung der BGP-Route über einen IPSec-Tunnel konfigurieren, stellen Sie sicher, dass Sie das sichere Overlay so konfigurieren, dass es eine virtuelle IP-Adresse (die nicht von einer physischen Schnittstelle oder einer OVS-Bridge stammt) für die IP-Adresse des lokalen Tunnels verwendet. Im obigen Beispiel wurden die virtuellen Adressierungsbefehle geändert: local-system-ip-addr 10.122.144.146 local-system-ip-subnet 10.122.144.128/27

Overlay-Status überprüfen

```
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
```

## Konfiguration der BGP-Routenankündigung für den FlexVPN-Server

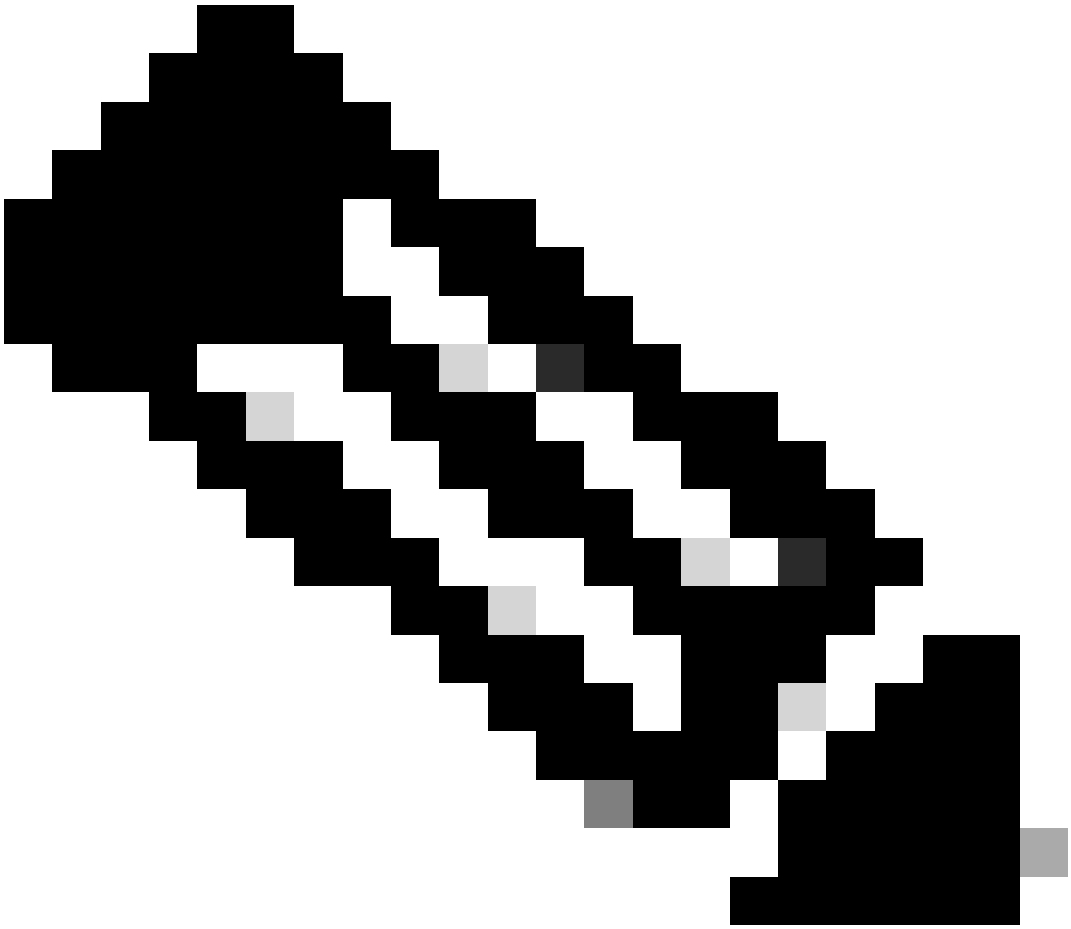
Bei dieser Konfiguration muss eBGP für die Peerings verwendet werden, wobei die Quelladresse (virtuelle IP-Adresse für die lokale Tunnel-IP) des Subnetzes von der NFVIS-Seite zum Listen-Bereich hinzugefügt werden muss.

```
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
```

Dabei gilt:

| | |
|---|---|
| bgp always-compare-med | Konfiguriert den Router so, dass er das MED-Attribut (Multi-Exit Discriminator) für alle Routen unabhängig von ihrem Ursprungs-AS immer vergleicht. |
| bgp log-neighbor-änderungen | Ermöglicht die Protokollierung von Ereignissen, die mit Änderungen in BGP-Nachbarbeziehungen zusammenhängen. |
| bgp deterministisch-med | Stellt den Vergleich der MED für Pfade von Nachbarn in verschiedenen autonomen Systemen sicher. |
| bgp listen range <Netzwerk>/<Maske> peer-group <Name der Peer-Gruppe> | Aktiviert die dynamische Nachbarerkennung innerhalb des angegebenen IP-Bereichs (Netzwerk/Maske) und weist erkannte Nachbarn dem Namen der Peer-Gruppe zu. Dies vereinfacht die Konfiguration, da allgemeine Einstellungen auf alle Peers in der Gruppe angewendet werden. |
| BGP-Abhörgrenze 255 | Legt die maximale Anzahl dynamischer BGP-Nachbarn, die im Listen-Bereich akzeptiert werden können, auf 255 fest. |
| kein BGP-Standard "ipv4-unicast" | Deaktiviert das automatische Senden von IPv4-Unicast-Routing-Informationen an BGP-Nachbarn, wozu eine explizite Konfiguration erforderlich ist. |
| verbunden umverteilen | Verteilt Routen aus direkt verbundenen Netzwerken über BGP (private Subnetze des FlexVPN-Servers, die zum privaten VRF |

| | |
|---|---|
| | gehören) |
| statisch verteilen | Verteilt statische Routen über das BGP |
| neighbor uCPEs ebgp-multihop 10 | Ermöglicht EBGP-(externes BGP)-Verbindungen mit Peers in der Peer-Gruppe für bis zu 10 Hops und eignet sich zum Verbinden von Geräten, die nicht direkt benachbart sind. |
| Neighbor uCPEs-Timer <Keep-Alive> <Hold-Down> | Legt die BGP Keepalive- und Hold-Down-Timer für Nachbarn in der Peer-Gruppe fest (im Beispiel 610 Sekunden und 1835 Sekunden). |



Hinweis: Eine ausgehende Präfixliste kann so konfiguriert werden, dass sie Nachbar-Routenankündigungen in der Peer-Gruppe steuert: Nachbar-Präfixliste ausgehend

## BGP-Konfiguration auf NFVIS

Starten des BGP-Prozesses mit den eBGP-Nachbarschaftseinstellungen

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

BGP-Prüfung

Diese Ausgabe zeigt den Zustand einer BGP-Sitzung an, wie vom BIRD Internet Routing Daemon berichtet. Diese Routing-Software ist für die Verarbeitung von IP-Routen und die Entscheidungsfindung hinsichtlich ihrer Richtung zuständig. Aus den bereitgestellten Informationen geht hervor, dass sich die BGP-Sitzung im Status "Established" befindet, was auf den erfolgreichen Abschluss des BGP-Peering-Prozesses hinweist, und dass die Sitzung derzeit aktiv ist. Vier Routen wurden erfolgreich importiert, und es wurde festgestellt, dass maximal 15 Routen importiert werden können.

```
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
```

Stellen Sie sicher, dass die privaten Subnetze des FlexVPN-Servers über BGP angekündigt wurden.

Beim Konfigurieren der BGP-Routenankündigung ist die einzige konfigurierbare Adressfamilie oder Übertragungskombination ipv4-unicastfür IPSec. Um den BGP-Status anzuzeigen, kann die Adressfamilie oder die Übertragung für IPSec als vpnv4-Unicast konfiguriert werden.

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

Mit dem Befehl show bgp vpnv4 unicast route können Sie Informationen zu den VPNv4-Unicast-Routen abrufen, die dem BGP-Prozess bekannt sind.

```
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 ?
```

Für den Head-End-VPN-Server kann ein Überblick über die BGP-Konfiguration und den Betriebsstatus generiert werden, um Status und Konfiguration von BGP-Sitzungen schnell zu bewerten.

```
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
```

Darüber hinaus können detaillierte Informationen zu den vom BGP verwalteten Einträgen der VPNv4-Routing-Tabelle (VPN over IPv4) angezeigt werden. Diese müssen spezifische Attribute jeder VPNv4-Route enthalten, z. B. das Routen-Präfix, die Next-Hop-IP-Adresse, die ursprüngliche AS-Nummer sowie verschiedene BGP-Attribute wie lokale Präferenz, MED (Multi-Exit Discriminator) und Community-Werte.

```
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 ?
```

# Fehlerbehebung

## NFVIS (FlexVPN-Client)

### NFVIS-Protokolldateien

Sie können alle Initialisierungs- und Fehlerprotokolle für die IPsec-Phasen aus der Protokolldatei NFVIS charon.log anzeigen:

```
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
```

### Interner Kernel führt Routen mit Strongswan ein

Unter Linux installiert strongswan (von NFVIS verwendete Multiplattform-IPsec-Implementierung) Routen (einschließlich BGP VPNv4-Unicast-Routen) standardmäßig in Routing-Tabelle 220 und erfordert daher, dass der Kernel richtlinienbasiertes Routing unterstützt.

```
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
```

Überprüfung des IPsec0-Schnittstellenstatus

Weitere Details über die virtuelle ipsec0-Schnittstelle erhalten Sie mit 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 (FlexVPN-Server)

Überprüfung von IPsec-SAs, die zwischen Peers erstellt wurden

Aus der folgenden Ausgabe wird der verschlüsselte Tunnel zwischen 10.88.247.84 über die Virtual-Access1-Schnittstelle und 10.88.247.89 für den Datenverkehr zwischen den Netzwerken 0.0.0.0/0 und 10.122.144.128/27 erstellt; zwei Encapsulating Security Payload (ESP)SAs wurden eingehend und ausgehend integriert.

```
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:
```

Aktive Verschlüsselungssitzungen anzeigen

Die Ausgabe für show crypto session detail muss umfassende Details zu jeder aktiven Crypto-Sitzung enthalten, einschließlich des VPN-Typs (z. B. Site-to-Site- oder Remote-Zugriff), der verwendeten Verschlüsselungs- und Hash-Algorithmen und der Sicherheitszuordnungen (Security Associations, SAs) für eingehenden und ausgehenden Datenverkehr. Es zeigt auch Statistiken über den verschlüsselten und entschlüsselten Datenverkehr an, z. B. die Anzahl der Pakete und Bytes. Dies kann zur Überwachung der Datenmenge, die durch das VPN gesichert wird, und zur Behebung von Durchsatzproblemen nützlich sein.

```
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
```

Zurücksetzen von VPN-Verbindungen

Mit den Befehlen clear cryptography werden VPN-Verbindungen oder Sicherheitszuordnungen manuell zurückgesetzt, ohne dass das gesamte Gerät neu gestartet werden muss.

- clear crypto ikev2 löscht IKEv2-Sicherheitszuordnungen (IKEv2-SAs).
- clear crypto session would clear IKEv1 (isakmp)/IKEv2 and IPSec SAs.
- clear crypto sa löscht nur die IPSec-SAs.
- clear crypto ipsec sa löscht die aktiven IPSec-Sicherheitszuordnungen.

Debuggen für zusätzliche Fehlerbehebung

IKEv2-Debugs können bei der Identifizierung und Fehlerbehebung von Fehlern am Headend (c8000v) helfen, die während des IKEv2-Aushandlungsprozesses und der FlexVPN-Clientverbindungen auftreten können, z. B. Probleme beim Aufbau der VPN-Sitzung, bei der Richtlinienanwendung oder Client-spezifische Fehler.

```
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
```

## Verwandte Artikel und Dokumentation

Sichere Overlay- und Single-IP-Konfiguration

BGP-Unterstützung auf NFVIS

Sichere Overlay- und BGP-Befehle

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.