# BGPルートアナウンスメントを使用したセキュアオーバーレイの設定

## 内容



## はじめに

このドキュメントでは、vBranchトラフィックを排他的に管理するために、NFVISでセキュアなオーバーレイとeBGPアナウンスを設定する方法について説明します。

# 使用するコンポーネント

このドキュメントの情報は、次のハードウェアおよびソフトウェア コンポーネントに基づくものです。

- NFVIS 4.7.1を実行するENCS5412
- Cisco IOS® XE 17.09.03aを実行するCatalyst 8000v

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## BGPルートアナウンス

NFVIS BGP機能は、セキュアオーバーレイ機能と連携して、セキュアオーバーレイトンネル経由でBGPネイバーからルートを学習します。これらの学習したルートまたはサブネットは、セキュアトンネルのNFVISルーティングテーブルに追加されます。これにより、トンネルを介してルートにアクセスできるようになります。セキュアオーバーレイでは、トンネルから学習できるプライベートルートは1つだけです。BGPを設定すると、暗号化されたトンネルを介して隣接関係を確立し、エクスポートされたルートをNFVIS vpnv4ルーティングテーブルに挿入したり、その逆を行ったりすることで、この制限を克服できます。

# 設定例

## トポロジ ダイアグラム

この設定の目標は、c8000vからNFVISの管理IPアドレスに到達することです。 トンネルが確立されると、eBGPルートアナウンスメントを使用して、private-vrfサブネットからより多くのルートをアドバタイズできるようになります。

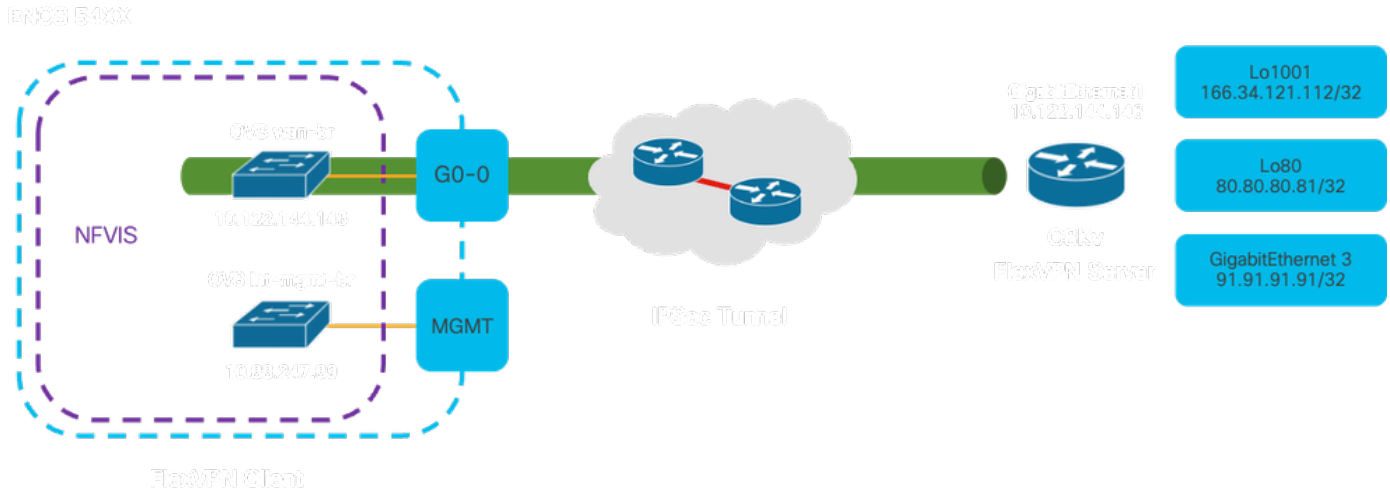



図 1. この文書に用意されている例のトポロジ図

## 初期設定

FlexVPNサーバで関連するIPアドレスを設定します（すべてグローバルコンフィギュレーションモード内）

```
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
```

NFVISについては、WANと管理インターフェイスを適宜設定します

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

## Catalyst 8000vルータでのFlexVPNサーバの設定

1. IKEv2プロポーザルの作成

2つのVPNエンドポイントがセキュア通信チャネルを確立する最初のフェーズ（フェーズ1）で使用する必要があるセキュリティプロトコルとアルゴリズムを指定します。IKEv2プロポーザルの目的は、認証、暗号化、整合性、およびキー交換のパラメータの概要を示すことにより、機密データを交換する前に、両方のエンドポイントが共通のセキュリティ対策のセットに合意するようにすることです。

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

場所：

| | |
|---|---|
| encryption <アルゴリズム> | 提案には、VPNがデータを保護するために使用する必要がある暗号化アルゴリズム（AESや3DESなど）が含まれます。暗号化により、盗聴者がVPNトンネルを通過するトラフィックを読み取ることができなくなります。 |
| integrity <ハッシュ> | IKEv2ネゴシエーション中に交換されるメッセージの整合性と信頼性を保証するために使用されるアルゴリズム（SHA-512など）を指定します。これにより、改ざんやリプレイアタックを防止できます。 |

2. IKEv2ポリシーを作成し、プロポーザルに関連付けます。

これは、IPSec VPN接続を確立する最初のフェーズ（フェーズ1）のパラメータを指定する設定セットです。 主に、VPNエンドポイントが相互に認証し合い、VPNセットアップ用のセキュアな通信チャネルを確立する方法に焦点を当てています。

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

3. IKEv2許可ポリシーの設定

IKEv2は、ネットワーク上の2つのエンドポイント間にセキュアなセッションを設定するために使用されるプロトコルで、認可ポリシーは、VPNトンネルが確立された後にVPNクライアントがアクセスできるリソースとサービスを決定する一連のルールです。

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

場所：

| | |
|---|---|
| pfs | Perfect Forward Secrecy（PFS；完全転送秘密）は、前のキーが侵害された場合でも、新しい各暗号化キーが独立して安全であることを保証することによって、VPN接続のセキュリティを強化する機能です。 |
| ルートセットインターフェイス | VPNセッションが正常に確立されると、IKEv2許可ポリシーで定義されているルートが自動的にデバイスのルーティングテーブルに追加されます。これにより、ルートセットで指定されたネットワーク宛てのトラフィックがVPNトンネルを通じて正しくルーティングされるようになります。 |

4. IKEv2プロファイルの作成

IKEv2(インターネットキーエクスチェンジ(IKE)バージョン2)ポリシーは、IPsec（インターネットプロトコルセキュリティ）VPNトンネルを確立するIKEv2フェーズで使用される一連のルールまたはパラメータです。IKEv2は、インターネットなどの信頼できないネットワーク経由で安全に通信を行おうとする2者間での、鍵の安全な交換とセキュリティアソシエーション(SA)のネゴシエーションを容易にするプロトコルです。IKEv2ポリシーは、このネゴシエーションの実行方法を定義し、セキュアで暗号化された通信チャネルを確立するために両当事者が合意する必要のあるさまざまなセキュリティパラメータを指定します。

IKEv2プロファイルには次のものが必要です。

- ローカルおよびリモートの認証方式。
- 一致するID、一致する証明書、または一致するステートメント。

```
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
```

場所：

| | |
|---|---|
| match fvrf public-vrf | プロファイルをvrf対応にします。 |
| match identity remote any（任意のアイデンティティの照合） | 着信セッションを有効なセッションとして認識する手段。この場合は「誰でも」です。 |
| 認証リモート事前共有キーciscociscocisco123 | 事前共有キーを使用してリモートピアを認証する必要があることを指定します。 |
| 認証ローカル事前共有キーciscociscocisco123 | このデバイス（ローカル）が事前共有キーを使用して認証する必要があることを指定します。 |
| dpd 60 2オンデマンド | Dead Peer Detection（デッドピア検出）：最小間隔（60秒）でパ |

| | |
|---|---|
| | ケットが受信されなかった場合、この60秒以内に2つのdpdパケットを送信します。 |
| aaa authorization group psk list default uCPE-author-pol local | ルート割り当て。 |
| virtual-template 1モードauto | 仮想テンプレートにバインドします。 |

5. IPSecトランスフォームセットの作成

IPSecトンネルを通過するデータトラフィックに適用する必要がある一連のセキュリティプロトコルとアルゴリズムを定義する基本的に、トランスフォームセットはデータの暗号化および認証方法を指定し、VPNエンドポイント間の安全な伝送を保証します。トンネルモードは、ネットワークを介した安全な転送のためにIPパケット全体をカプセル化するようにIPsecトンネルを設定します。

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

場所：

| | |
|---|---|
| set transform-set <トランスフォームセット名> | VPNトンネルを通過するデータフローを保護するために使用する必要がある暗号化アルゴリズムと整合性アルゴリズム（例：暗号化にAES、整合性にSHA）を指定します。 |
| set ikev2-profile <ikev2-profile-name> | 暗号化アルゴリズム、ハッシュアルゴリズム、認証方法、Diffie-Hellmanグループなど、VPNセットアップのフェーズ1のセキュリティアソシエーション(SA)のネゴシエーションのパラメーターを定義します。 |
| set pfs <グループ> | オプションの設定で、有効にすると、新しい暗号化キーが以前のキーと関連付けられなくなり、セキュリティが強化されます。 |

6. デフォルトのIPsecプロファイルの削除

デフォルトのIPsecプロファイルを削除することは、セキュリティ、カスタマイズ、およびシステムの明確さに関連するいくつかの理由で採用されている方法です。 デフォルトのIPsecプロファイルは、ネットワークの特定のセキュリティポリシーまたは要件を満たすことができません。これを削除することで、VPNトンネルが誤って最適ではない設定や安全でない設定を使用することがなくなり、脆弱性のリスクが軽減されます。

各ネットワークには、特定の暗号化アルゴリズムとハッシュアルゴリズム、キーの長さ、認証方法など、固有のセキュリティ要件があります。デフォルトプロファイルを削除すると、これらの特定のニーズに合わせたカスタムプロファイルの作成が促進され、可能な限り最高の保護とパフォーマンスが確保されます。

```
no crypto ipsec profile default
```

7. IPsecプロファイルを作成し、トランスフォームセットおよびIKEv2プロファイルに関連付けます。

IPsec（インターネットプロトコルセキュリティ）プロファイルは、IPsec VPNトンネルを確立して管理するために使用される設定とポリシーをカプセル化する構成エンティティです。これは、複数のVPN接続に適用できるテンプレートとして機能し、セキュリティパラメータを標準化して、ネットワーク上の安全な通信の管理を簡素化します。

```
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. 仮想テンプレートの作成

バーチャルテンプレートインターフェイスは、バーチャルアクセスインターフェイスのダイナミックテンプレートとして機能し、スケーラブルで効率的なVPN接続の管理方法を提供します。仮想アクセスインターフェイスの動的なインスタンス化が可能になる新しいVPNセッションが開始されると、デバイスはバーチャルテンプレートで指定された設定に基づいてバーチャルアクセスインターフェイスを作成します。このプロセスは、各接続に対して事前に設定された物理インターフェイスを必要とせずに、必要に応じてリソースを動的に割り当てることにより、多数のリモートクライアントおよびサイトをサポートします。

仮想テンプレートを使用することで、FlexVPNの導入は、新しい接続が確立されるたびに効率的に拡張でき、個々のセッションを手動で設定する必要はありません。

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

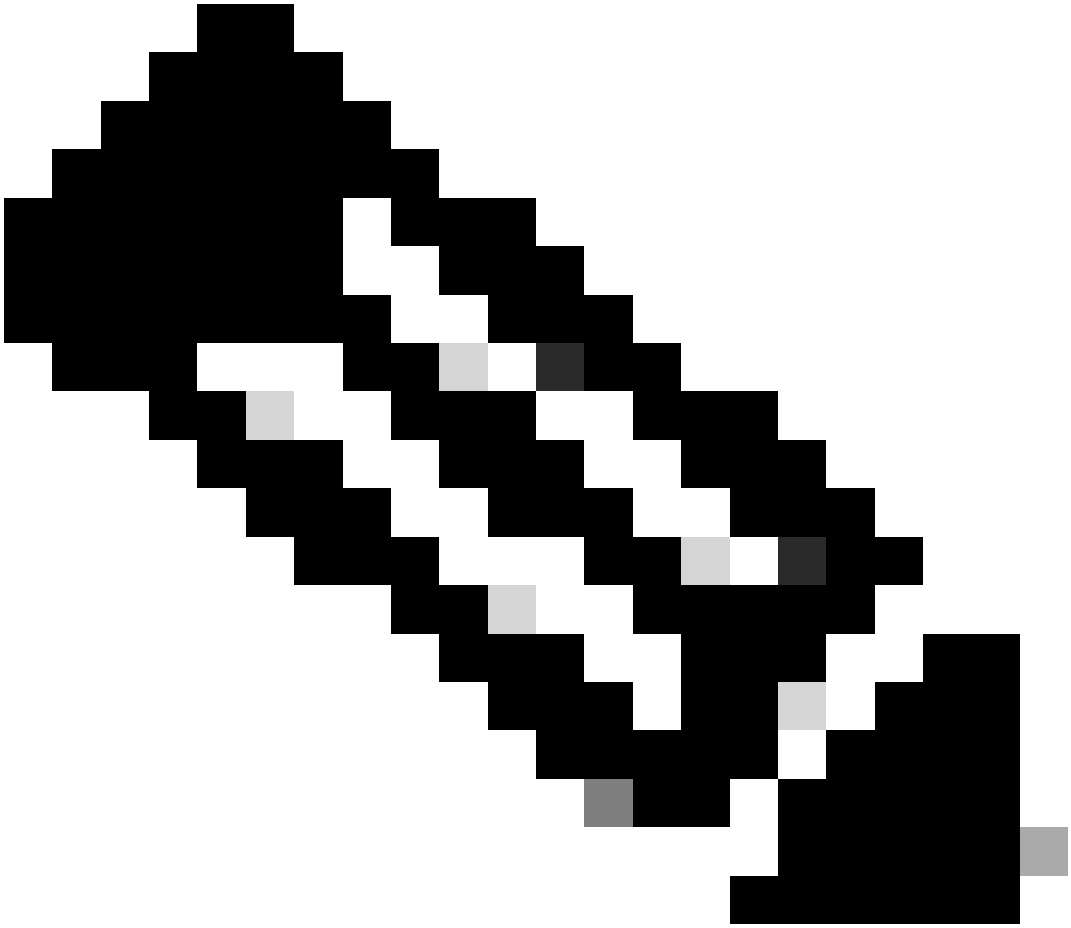
## NFVISセキュアオーバーレイの最小構成

### セキュアオーバーレイインスタンスの設定

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

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

---



注：IPSecトンネルを介したBGPルートアナウンスを設定する場合は、ローカルトンネルIPアドレスに（物理インターフェイスまたはOVSブリッジから送信されたものではなく）仮想IPアドレスを使用するようにセキュアオーバーレイが設定されていることを確認してください。上記の例では、仮想アドレッシングコマンドlocal-system-ip-addr 10.122.144.146 local-system-ip-subnet 10.122.144.128/27が変更されています。

---

## オーバーレイステータスの確認

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

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

## FlexVPNサーバのBGPルートアナウンスの設定

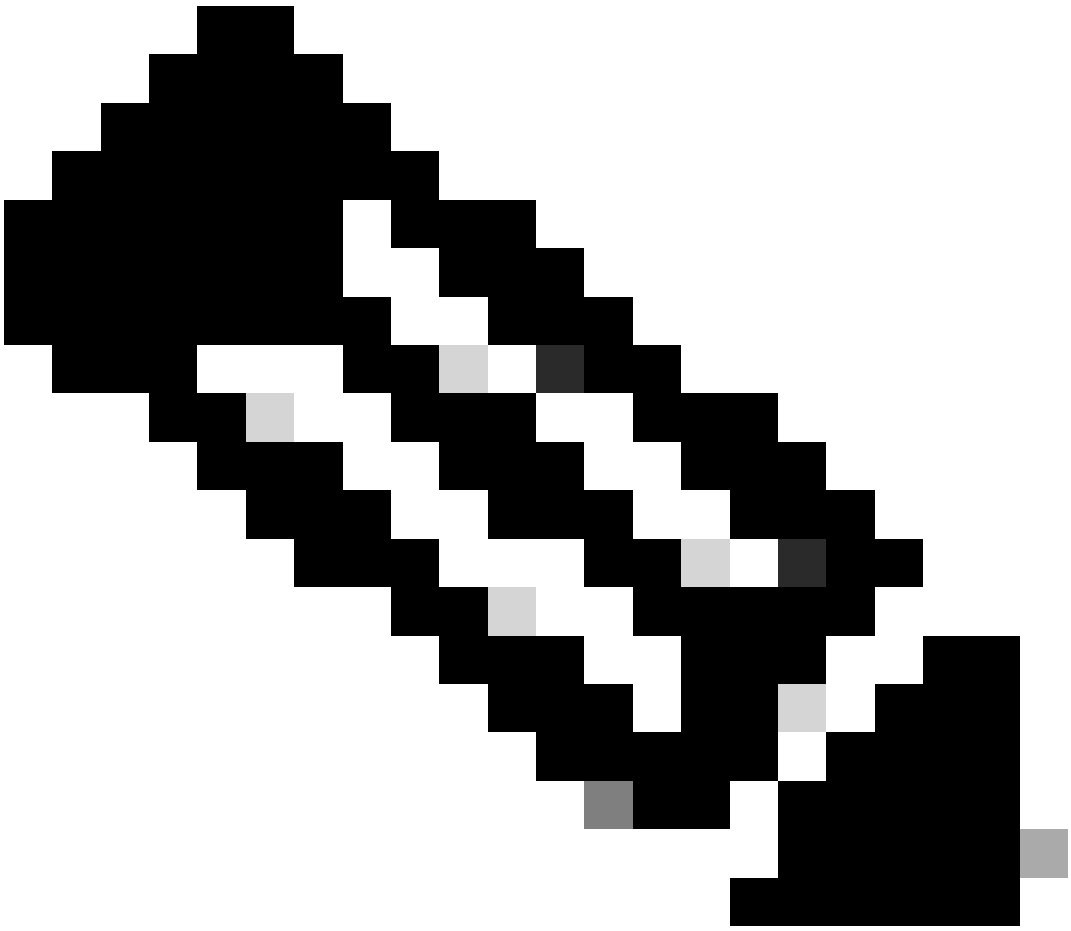
この設定では、ピアリングにeBGPを使用する必要があります。そこでは、NFVIS側からの送信元アドレス（ローカルトンネルIPの仮想IPアドレス）サブネットをリッスン範囲に追加する必要があります。

```
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
```

場所：

| | |
|---|---|
| bgp always-compare-med | 発信元ASに関係なく、すべてのルートのMED(Multi-Exit Discriminator)アトリビュートを常に比較するようにルータを設定します。 |
| bgp log-neighbor-changes | BGPネイバー関係の変更に関連するイベントの口ギングを有効にします。 |
| bgp確定med | 異なる自律システムのネイバーからのパスについて、MEDを比較します。 |
| bgp listen range <ネットワーク>/<マスク> peer-group <ピアグループ名> | 指定したIP範囲（ネットワーク/マスク）内でダイナミックなネイバー探索を有効にし、検出されたネイバーをピアグループ名に割り当てます。これにより、グループ内のすべてのピアに共通の設定が適用されるため、設定が簡素化されます。 |
| BGPリッスン制限255 | リッスン範囲内で受け入れ可能なダイナミックBGPネイバーの最大数を255に設定します。 |
| no bgp default ipv4-unicast | BGPネイバーへのIPv4ユニキャストルーティング情報の自動送信を無効にします。これを有効にするには、明示的な設定が必要です。 |

| | |
|---|---|
| redistribute connected | 直接接続されたネットワークからのルートをBGPに再配布します（private-vrfに属するFlexVPNサーバからのプライベートサブネット）。 |
| redistribute static | スタティックルートをBGPに再配布します。 |
| neighbor uCPEs ebgp-multihop 10 | ピアグループ内のピアとのEBGP（外部BGP）接続を最大10ホップに広げることができ、直接隣接していないデバイスの接続に役立ちます。 |
| neighbor uCPEs timers <keep-alive> <hold-down> | ピアグループ内のネイバーのBGPキープアライブタイマーとホールドダウンタイマーをそれぞれ設定します（例では610秒と1835秒）。 |



注：発信プレフィックスリストは、ピアグループ内のネイバールートアドバタイズメントを制御するように設定できます。neighbor prefix-list out

## NFVISでのBGPの設定

eBGPネイバーシップ設定でBGPプロセスを開始します

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

BGPレビュー

この出力は、BIRDインターネットルーティングデーモン(IRD)によって報告されたBGPセッションの状態を示しています。このルーティングソフトウェアは、IPルートを処理し、その方向に関する決定を行います。提示された情報から、BGPセッションが「Established」状態であることが明らかになります。これは、BGPピアリングプロセスが正常に完了し、セッションが現在アクティブであることを示しています。4つのルートが正常にインポートされました。インポートできるルートの上限は15個です。

```
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
```

FlexVPNサーバからのプライベートサブネットがBGP経由でアドバタイズされたことを確認します。

BGPルートのアナウンスを設定している場合、設定可能なアドレスファミリまたは伝送の組み合わせは、IPSecのipv4 ユニキャストだけです。BGPステータスを表示するために設定可能なIPSecのアドレスファミリまたは送信は、vpnv4ユニキャストです。

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

show bgp vpnv4 unicast routeコマンドを使用すると、BGPプロセスで認識されているVPNv4ユニキャストルートに関する情報を取得できます。

```
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 ?
```

ヘッドエンドVPNサーバでは、BGP設定と動作状態の概要を生成して、BGPセッションの健全性と設定をすばやく評価できます。

```
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
```

また、BGPによって管理されるVPNv4(VPN over IPv4)ルーティングテーブルエントリに関する詳細情報を表示できます。この情報には、各VPNv4ルートの特定の属性(ルートプレフィックス、ネクストホップIPアドレス、送信元AS番号、およびlocal preference、MED(Multi-Exit Discriminator)、コミュニティ値などのさまざまなBGP属性など)を含める必要があります。

```
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 ?
```

# トラブルシューティング

## NFVIS（FlexVPNクライアント）

### NFVISログファイル

NFVIS charon.logログファイルから、IPSecフェーズのすべての初期化ログとエラーログを表示できます。

```
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
```

### 内部カーネルstrongswan挿入ルート

Linuxでは、strongswan（NFVISが使用するマルチプラットフォームIPsec実装）はデフォルトでルート（BGP VPNv4ユニキャストルートを含む）をルーティングテーブル220にインストールするため、カーネルはポリシーベースルーティングをサポートする必要があります。

```
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
```

### IPsec0インターフェイスのステータスの確認

ipsec0仮想インターフェイスの詳細を確認するには、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
```

## ヘッドエンド（FlexVPNサーバ）

### ピア間のIPSec SA構築の確認

次の出力では、ネットワーク0.0.0.0/0と10.122.144.128/27の間を行き来するトラフィックに対して、Virtual-Access1インターフェイスを介した10.88.247.84と10.88.247.89の間で暗号化トンネルが構築されています。インバウンドとアウトバウンドで構築された2つのEncapsulating Security Payload(ESP)SAです。

```
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:
```

## アクティブな暗号化セッションの表示

show crypto session detailの出力には、VPNのタイプ（サイト間やリモートアクセスなど）、使用中の暗号化とハッシュアルゴリズム、着信トラフィックと発信トラフィックのセキュリティアソシエーション(SA)など、各アクティブな暗号化セッションに関する包括的な詳細が示される必要があります。また、パケット数やバイト数など、暗号化および復号化されたトラフィックに関する統計情報も表示されるため、VPNによって保護されているデータ量を監視したり、スループットの問題をトラブルシューティングしたりする場合に役立ちます。

```
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
```

VPN接続のリセット

clear暗号コマンドを使用すると、VPN接続を手動でリセットしたり、デバイス全体をリブートせずにセキュリティアソシエーション(SA)をクリアしたりできます。

- clear crypto ikev2は、IKEv2セキュリティアソシエーション(IKEv2 SA)をクリアします。
- clear crypto sessionは、IKEv1(isakmp)/IKEv2およびIPSec SAをクリアします。
- clear crypto saはIPSec SAだけをクリアします。
- clear crypto ipsec saは、アクティブなIPSecセキュリティアソシエーションを削除します。

追加のトラブルシューティングのためのデバッグの実行

IKEv2デバッグは、IKEv2ネゴシエーションプロセスとFlexVPNクライアントの接続中に発生する可能性があるヘッドエンドデバイス(c8000v)のエラー（VPNセッションの確立の問題、ポリシーの適用、クライアント固有のエラーなど）の特定とトラブルシューティングに役立ちます。

```
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
```

## 関連記事およびドキュメント

セキュアオーバーレイと単一IP設定

NFVISでのBGPサポート

セキュアオーバーレイおよびBGPコマンド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。