

BGP 경로 알림으로 보안 오버레이 구성

목차

[소개](#)

[사용되는 구성 요소](#)

[BGP 경로 알림](#)

[컨피그레이션 예시](#)

[토폴로지 다이어그램](#)

[초기 설정](#)

[Catalyst 8000v 라우터의 FlexVPN 서버 구성](#)

- [1. IKEv2 제안서 생성](#)
- [2. IKEv2 정책을 생성하고 제안서에 연결합니다.](#)
- [3. IKEv2 권한 부여 정책 구성](#)
- [4. IKEv2 프로파일 생성](#)
- [5. IPsec 변형 집합 만들기](#)
- [6. 기본 IPsec 프로파일 제거](#)
- [7. IPsec 프로파일을 생성하고 변형 집합 및 IKEv2 프로파일과 연결합니다.](#)
- [8. 가상 템플릿 생성](#)

[NFVIS 보안 오버레이 최소 컨피그레이션](#)

[오버레이 상태 검토](#)

[FlexVPN 서버에 대한 BGP 경로 알림 컨피그레이션](#)

[NFVIS의 BGP 컨피그레이션](#)

[BGP 검토](#)

[FlexVPN Server의 사설 서브넷이 BGP를 통해 알려졌는지 확인합니다.](#)

[문제 해결](#)

[NFVIS\(FlexVPN 클라이언트\)](#)

[NFVIS 로그 파일](#)

[내부 커널 스트롬스완 주입 경로](#)

[IPsec0 인터페이스 상태 검토](#)

[Head-End\(FlexVPN 서버\)](#)

[피어 간의 IPsec SA 빌드 검토](#)

[활성 암호화\(암호화\) 세션 표시](#)

[VPN 연결 재설정](#)

[추가 트러블슈팅을 위해 디버깅 수행](#)

[관련 문서 및 문서](#)

소개

이 문서에서는 독립적인 vBranch 트래픽 관리를 위해 NFVIS에서 보안 오버레이 및 eBGP 공지를 구성하는 방법에 대해 설명합니다.

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 구성 요소를 기반으로 합니다.

- NFVIS 4.7.1을 실행하는 ENCS5412
- Cisco IOS® XE 17.09.03a를 실행하는 Catalyst 8000v

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

BGP 경로 알림

NFVIS BGP 기능은 보안 오버레이 기능과 함께 작동하여 보안 오버레이 터널을 통해 BGP 인접 디바이스에서 경로를 학습합니다. 이러한 학습된 경로 또는 서브넷은 보안 터널의 NFVIS 라우팅 테이블에 추가되어 터널을 통해 경로에 액세스할 수 있게 합니다. Secure Overlay에서는 터널에서 학습할 단일 개인 경로 하나만 허용하므로, BGP를 구성하면 암호화된 터널을 통해 인접성을 설정하고 내보낸 경로를 NFVIS vpnv4 라우팅 테이블에 삽입하여 이러한 제한을 극복할 수 있습니다.

컨피그레이션 예시

토폴로지 다이어그램

이 컨피그레이션의 목적은 c8000v에서 NFVIS의 관리 IP 주소에 연결하는 것입니다. 터널이 설정되면 eBGP 경로 공지를 사용하여 private-vrf 서브넷에서 더 많은 경로를 광고할 수 있습니다.

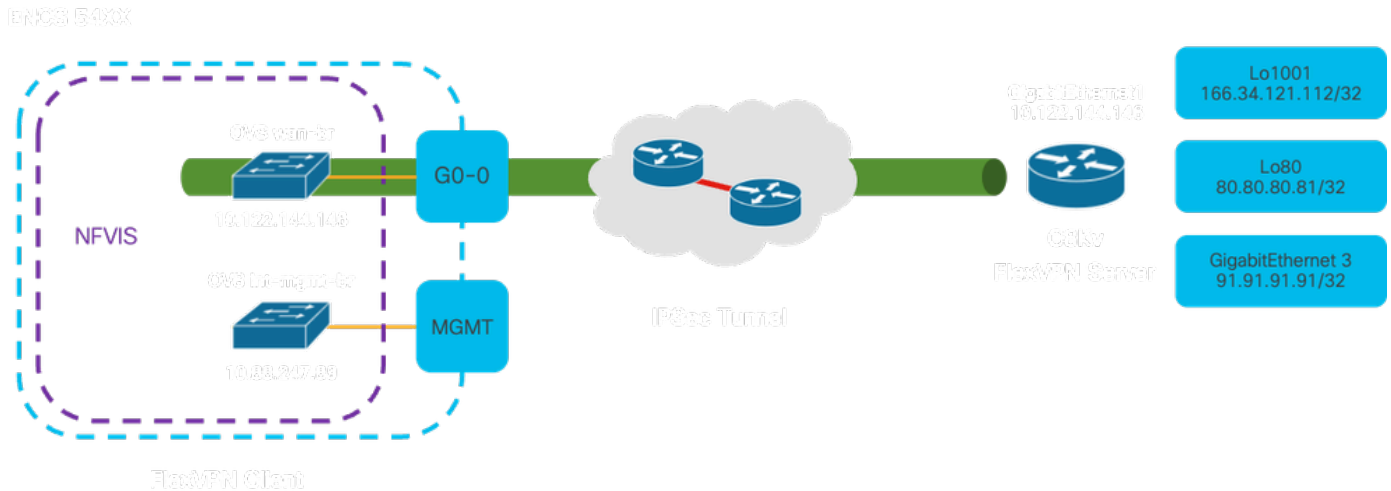


그림 1. 이 문서에서 준비한 예제의 토폴로지 다이어그램

초기 설정

FlexVPN Server에서 관련 IP 주소 지정 구성(모두 전역 컨피그레이션 모드 내)

```
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

```

NFVIS의 경우 WAN 및 관리 인터페이스를 적절하게 구성합니다

```

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 scp ]
action accept
priority 10
!

```

Catalyst 8000v 라우터의 FlexVPN 서버 구성

1. IKEv2 제안서 생성

보안 통신 채널 설정의 초기 단계(1단계) 동안 두 VPN 엔드포인트가 사용해야 하는 보안 프로토콜과 알고리즘을 지정합니다. IKEv2 제안의 목적은 인증, 암호화, 무결성 및 키 교환을 위한 매개변수를 개략적으로 설명하는 것이므로 민감한 데이터를 교환하기 전에 두 엔드포인트가 공통된 보안 조치 집합에 동의하도록 하는 것입니다.

```

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

```

여기서 각 항목은 다음을 나타냅니다.

암호화 <알고리즘>	제안서에는 VPN에서 데이터를 보호하기 위해 사용해야 하는 암호화 알고리즘(예: AES 또는 3DES)이 포함되어 있습니다. 암호화는 도청자가 VPN 터널을 통과하는 트래픽을 읽을 수 없게 합니다.
무결성 <해시>	IKEv2 협상 중에 교환되는 메시지의 무결성 및 신뢰성을 보장하는 데 사용되는 알고리즘(예: SHA-512)을 지정합니다. 이렇게 하면 위조 및 반복 공격을 방지할 수 있습니다.

2. IKEv2 정책을 생성하고 제안서에 연결합니다.

IPsec VPN 연결 설정의 초기 단계(1단계)에 대한 매개변수를 지정하는 컨피그레이션 세트입니다. 주로 VPN 엔드포인트가 서로를 인증하고 VPN 설정을 위한 보안 통신 채널을 설정하는 방법에 중점을 둡니다.

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

3. IKEv2 권한 부여 정책 구성

IKEv2는 네트워크의 두 엔드포인트 간에 보안 세션을 설정하는 데 사용되는 프로토콜이며, 권한 부여 정책은 VPN 터널이 설정되면 VPN 클라이언트에서 액세스할 수 있는 리소스와 서비스를 결정하는 규칙 집합입니다.

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

여기서 각 항목은 다음을 나타냅니다.

pfs	PFS(Perfect Forward Secrecy)는 이전 키가 손상된 경우에도 각각의 새 암호화 키가 독립적으로 보호되도록 하여 VPN 연결의 보안을 강화하는 기능입니다.
route set interface <interface-name>	VPN 세션이 성공적으로 설정되면 IKEv2 권한 부여 정책에 정의된 경로가 자동으로 디바이스 라우팅 테이블에 추가됩니다. 이렇게 하면 경로 집합에 지정된 네트워크로 향하는 트래픽이 VPN 터널을 통해 올바르게 라우팅됩니다.

4. IKEv2 프로파일 생성

IKEv2(Internet Key Exchange 버전 2) 정책은 IPsec(Internet Protocol Security) VPN 터널을 설정하는 IKEv2 단계에서 사용되는 규칙 또는 매개변수 집합입니다. IKEv2는 인터넷과 같은 신뢰할 수 없

는 네트워크를 통해 안전하게 통신하려는 두 당사자 간에 키를 안전하게 교환하고 SA(Security Association)를 협상할 수 있게 해주는 프로토콜입니다. IKEv2 정책은 보안 및 암호화된 통신 채널을 설정하기 위해 양 당사자가 동의해야 하는 다양한 보안 매개변수를 지정하여 이 협상이 발생하는 방식을 정의합니다.

IKEv2 프로파일에는 다음이 있어야 합니다.

- 로컬 및 원격 인증 방법입니다.
- 일치 ID 또는 일치 인증서 또는 일치 명령문.

```
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
```

여기서 각 항목은 다음을 나타냅니다.

fvrf public-vrf 일치	프로필을 vrf 인식(vrf-aware)으로 만듭니다.
id 원격 일치	수신 세션을 유효한 것으로 인식하기 위한 측정값입니다. 이 경우 모든 사람이 해당됩니다.
인증 원격 사전 공유 키 ciscocisco123	사전 공유 키를 사용하여 원격 피어를 인증하도록 지정합니다.
인증 로컬 사전 공유 키 ciscocisco123	이 디바이스(로컬)가 사전 공유 키를 사용하여 인증하도록 지정합니다.
dpd 60 2 on-demand	Dead Peer Detection(데드 피어 탐지). minutec(60초)을 통해 수신된 패킷이 없는 경우 이 60초 간격 내에 2개의 dpd 패킷을 전송합니다.
aaa authorization group psk list default uCPE-author-pol local	경로 지정.
가상 템플릿 1 모드 자동	가상 템플릿에 바인딩합니다.

5. IPsec 변형 집합 만들기

IPsec 터널을 통과하는 데이터 트래픽에 적용해야 하는 보안 프로토콜 및 알고리즘 집합을 정의합니다. 기본적으로 변형 집합은 VPN 엔드포인트 간의 안전한 전송을 보장하면서 데이터를 암호화 및 인증하는 방법을 지정합니다. 터널 모드는 네트워크 전반에 안전한 전송을 위해 전체 IP 패킷을 캡슐화하도록 IPsec 터널을 구성합니다.

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

```
mode tunnel
```

여기서 각 항목은 다음을 나타냅니다.

set transform-set <transform-set-name>	VPN 터널을 통해 흐르는 데이터를 보호하는 데 사용해야 하는 암호화 및 무결성 알고리즘(예: 암호화의 경우 AES, 무결성의 경우 SHA)을 지정합니다.
ikev2-profile <ikev2-profile-name> 설정	암호화 알고리즘, 해시 알고리즘, 인증 방법 및 Diffie-Hellman 그룹을 포함하여 VPN 설정의 1단계에서 SA(Security Association) 협상에 대한 매개변수를 정의합니다.
pfs <group> 설정	활성화할 경우 각 새 암호화 키가 이전 키와 관련이 없도록 하여 보안을 강화하는 선택적 설정입니다.

6. 기본 IPsec 프로파일 제거

기본 IPsec 프로파일을 제거하는 방법은 보안, 사용자 지정 및 시스템 명확성과 관련된 몇 가지 이유로 채택된 방식입니다. 기본 IPsec 프로파일은 네트워크의 특정보안 정책 또는 요구 사항을 충족하지 못합니다. 이를 제거하면 어떤 VPN 터널에서도 최적화되지 않거나 안전하지 않은 설정을 무심코 사용하지 않으므로 취약성의 위험이 줄어듭니다.

각 네트워크에는 특정 암호화 및 해싱 알고리즘, 키 길이, 인증 방법 등 고유한 보안 요구 사항이 있습니다. 기본 프로파일을 제거하면 이러한 특정 요구 사항에 부합하는 맞춤형 프로파일을 생성할 수 있으므로 최상의 보호 및 성능을 보장할 수 있습니다.

```
no crypto ipsec profile default
```

7. IPsec 프로파일을 생성하고 변형 집합 및 IKEv2 프로파일과 연결합니다.

IPsec(Internet Protocol Security) 프로파일은 IPsec VPN 터널을 설정하고 관리하는 데 사용되는 설정과 정책을 캡슐화하는 구성 엔터티입니다. 여러 VPN 연결에 적용할 수 있는 템플릿 역할을 하며 보안 매개변수를 표준화하고 네트워크 전반의 보안 통신 관리를 단순화합니다.

```
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. 가상 템플릿 생성

Virtual-Template 인터페이스는 가상 액세스 인터페이스의 동적 템플릿 역할을 하여 VPN 연결을 관리하기 위한 확장 가능하고 효율적인 방법을 제공합니다. 이를 통해 가상 액세스 인터페이스의 동적 인스턴스화가 가능합니다. 새 VPN 세션이 시작되면 디바이스에서 Virtual-Template에 지정된 컨피그레이션을 기반으로 Virtual-Access 인터페이스를 생성합니다. 이 프로세스는 각 연결에 대해 미리 구성된 물리적 인터페이스를 사용할 필요 없이 필요에 따라 리소스를 동적으로 할당하여 다수의 원격 클라이언트 및 사이트를 지원합니다.

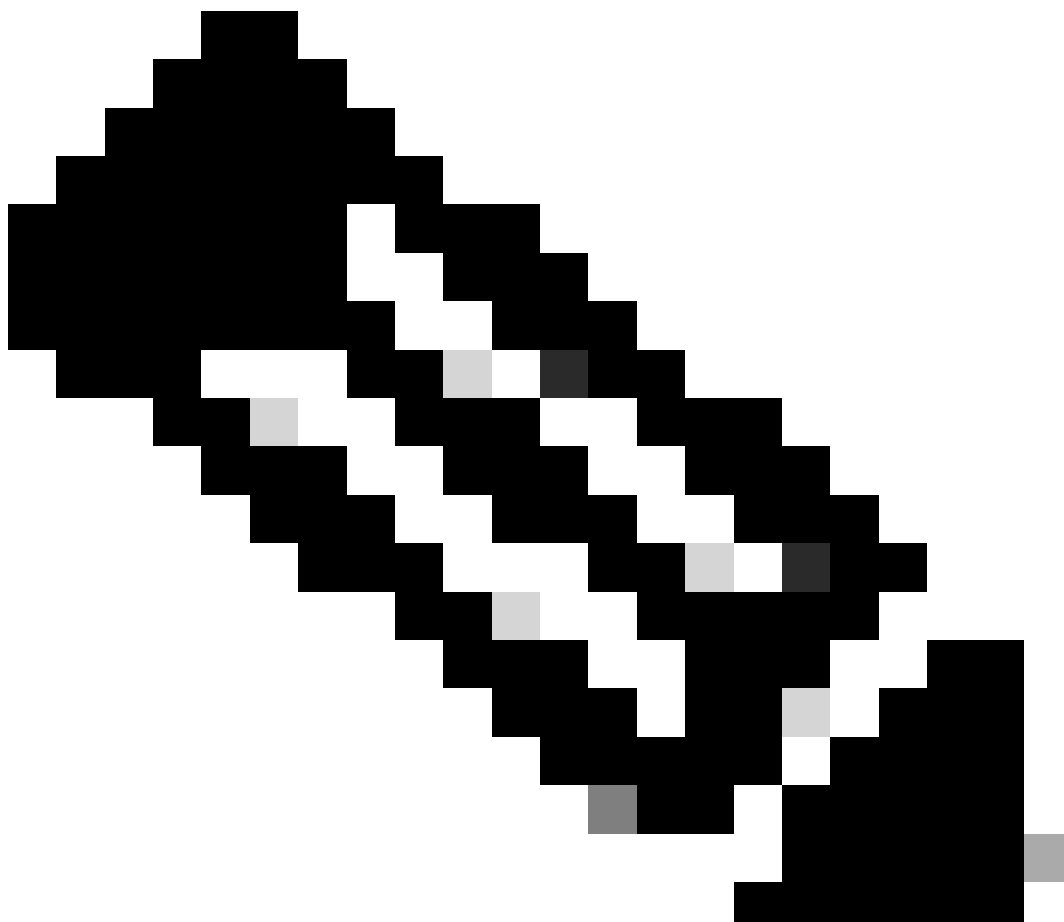
FlexVPN 구축은 가상 템플릿을 사용하여 각 개별 세션의 수동 컨피그레이션 없이 새로운 연결이 설정되는 대로 효율적으로 확장할 수 있습니다.

```
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 보안 오버레이 최소 컨피그레이션

보안 오버레이 인스턴스 구성

```
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
```



참고: IPSec 터널을 통해 BGP 경로 알리를 구성할 때 로컬 터널 IP 주소에 대해 가상 IP 주소(물리적 인터페이스 또는 OVS 브리지에서 소싱되지 않음)를 사용하도록 보안 오버레이를 구성해야 합니다. 위의 예에서 변경된 가상 주소 지정 명령입니다. local-system-ip-addr 10.122.144.146 local-system-ip-subnet 10.122.144.128/27

오버레이 상태 검토

```
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 서버에 대한 BGP 경로 알림 컨피그레이션

이 설정에서는 피어링에 eBGP를 사용해야 합니다. 여기서 NFVIS 측의 소스 주소(로컬 터널 IP의 가상 IP 주소) 서브넷을 수신 대기 범위에 추가해야 합니다.

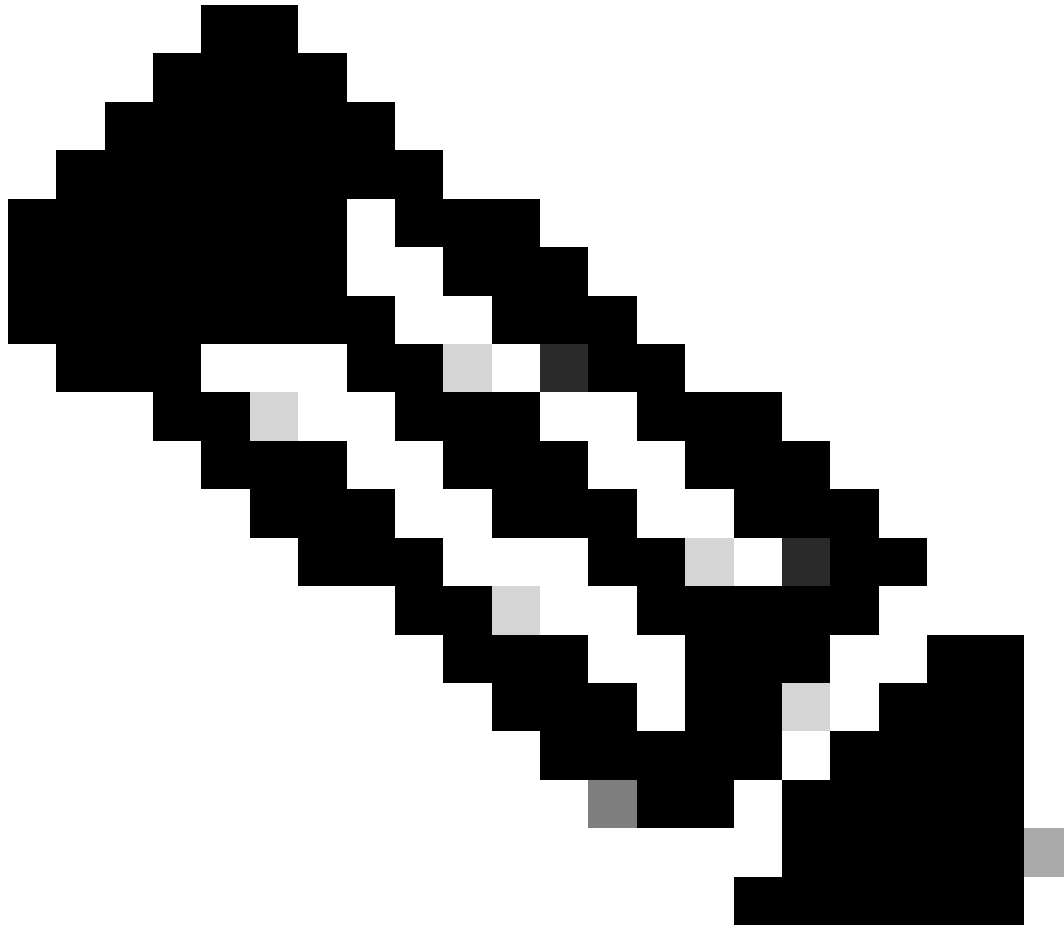
```
router bgp 65000
  bgp router-id 166.34.121.112
  bgp always-compare-med
  bgp log-neighbor-changes
  bgp deterministic-med
  bgp listen range 10.122.144.0/24 peer-group uCPEs
  bgp listen limit 255
  no bgp default ipv4-unicast
  address-family ipv4 vrf private-vrf
    redistribute connected
    redistribute static
  neighbor uCPEs peer-group
  neighbor uCPEs remote-as 200
  neighbor uCPEs ebgp-multihop 10
  neighbor uCPEs timers 610 1835
  exit-address-family
```

여기서 각 항목은 다음을 나타냅니다.

bgp always-compare-med	원래 AS와 상관없이 모든 경로에 대해 항상 MED(Multi-Exit Discriminator) 특성을 비교하도록 라우터를 구성합니다.
bgp 로그 인접 디바이스 변경	BGP 네이버 관계의 변경과 관련된 이벤트에 대한 로깅을 활성화합니다.
bgp 결정적-med	서로 다른 자율 시스템의 네이버에서 오는 경로에 대한 MED의 비교를 보장합니다.
bgp 수신 범위 <네트워크>/<마스크> peer-group <peer-group-name>	지정된 IP 범위(네트워크/마스크) 내에서 동적 인접 디바이스 검색을 활성화하고, 검색된 인접 디바이스를 피어 그룹 이름에 할당합니다. 이렇게 하면 그룹의 모든 피어에 공통 설정을 적용하여 컨피그레이션을 간소화할 수 있습니다.
bgp 수신 제한 255	수신 범위 내에서 수락할 수 있는 동적 BGP 인접 디바이스의 최대 수를 255로 설정합니다.
bgp 기본 ipv4 유니캐스트 없음	BGP 인접 디바이스에 대한 IPv4 유니캐스트 라우팅 정보의 자동 전송을 비활성화합니다. 이를 활성화하려면 명시적 컨피그레이션이 필요합니다.
재배포 연결됨	직접 연결된 네트워크에서 BGP(private-vrf에 속하는 FlexVPN 서버의 사설 서브넷)로 경로를 재배포합니다.
고정 재배포	고정 경로를 BGP로 재배포합니다.
인접 uCPE ebgp-multihop 10	피어 그룹의 피어와의 EBGP(External BGP) 연결이 최대 10홉까지 확장되도록 허용합니다. 이는 직접 인접하지 않은 디바이스를 연결하는 데 유용합니다.
네이버 uCPE 타이머 <keep-	피어 그룹의 네이버에 대한 BGP keepalive 및 hold-down 타이머를

alive> <hold-down>

각각 설정합니다(예제의 경우 610초 및 1835초).



참고: 피어 그룹에서 네이버 경로 알림을 제어하도록 아웃바운드 접두사 목록을 구성할 수 있습니다. 네이버 접두사 목록 출력

NFVIS의 BGP 컨피그레이션

eBGP 인접 디바이스 설정으로 BGP 프로세스 시작

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

BGP 검토

이 출력은 BIRD Internet Routing Daemon에서 보고한 BGP 세션의 상태를 나타냅니다. 이 라우팅 소프트웨어는 IP 경로를 처리하고 그 방향에 대한 결정을 내리는 역할을 담당합니다. 제공된 정보에서 BGP 세션이 "Established(설정됨)" 상태임을 나타내어 BGP 피어링 프로세스가 성공적으로 완료되었으며 세션이 현재 활성 상태임을 나타냅니다. 4개 노선을 성공적으로 수입했으며, 수입 가능한 노선은 15개로 상한이 있다고 언급했다.

```

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 Server의 사설 서브넷이 BGP를 통해 알려졌는지 확인합니다.

BGP 경로 공지를 구성할 때 구성 가능한 주소 패밀리 또는 전송 조합은 ipv4 unicastfor IPsec뿐입니다. BGP 상태를 보려면 IPsec에 대한 구성 가능한 주소군 또는 전송이 vpnv4 유니캐스트입니다.

```

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

```

show bgp vpnv4 unicast route 명령을 사용하면 BGP 프로세스에 알려진 VPNv4 유니캐스트 경로에 대한 정보를 검색할 수 있습니다.

```

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 ?
```

헤드엔드 VPN 서버의 경우 BGP 세션의 상태 및 컨피그레이션을 신속하게 평가하기 위해 BGP 컨피그레이션 및 작동 상태에 대한 개요를 생성할 수 있습니다.

```
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
```

또한 BGP에서 관리하는 VPNv4(VPN over IPv4) 라우팅 테이블 항목에 대한 자세한 정보를 표시할 수 있습니다. 여기에는 경로 접두사, next-hop IP 주소, 원래 AS 번호, 로컬 기본 설정, MED(Multi-Exit Discriminator), 커뮤니티 값 등의 다양한 BGP 특성과 같은 각 VPNv4 경로의 특정 특성이 포함되어야 합니다.

```
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	?

문제 해결

NFVIS(FlexVPN 클라이언트)

NFVIS 로그 파일

NFVIS charon.log 로그 파일에서 IPsec 단계에 대한 모든 초기화 및 오류 로그를 볼 수 있습니다.

```
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 successfu
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

```

내부 커널 스트롱스완 주입 경로

Linux에서는 strongswan(NFVIS에서 사용하는 멀티플랫폼 IPsec 구현)이 라우팅 테이블(220)에 경로(BGP VPNv4 유니캐스트 경로 포함)를 기본적으로 설치하므로 커널이 정책 기반 라우팅을 지원해야 합니다.

```

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 인터페이스 상태 검토

ifconfig를 사용하여 ipsec0 가상 인터페이스에 대한 자세한 내용을 확인할 수 있습니다

```

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
```

Head-End(FlexVPN 서버)

피어 간의 IPsec SA 빌드 검토

아래의 출력에서 암호화된 터널은 Virtual-Access1 인터페이스를 통해 10.88.247.84와 0.0.0.0/0과 10.122.144.128/27 네트워크 간에 이동하는 트래픽에 대해 10.88.247.89 사이에 구축됩니다. 즉, 인바운드와 아웃바운드에 2개의 ESP(Encapsulating Security Payload)SA가 구축됩니다.

```
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-head-0
    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 pcg sas:

활성 암호화(암호화) 세션 표시

show crypto session detail의 출력은 VPN 유형(사이트 간 또는 원격 액세스 등), 사용 중인 암호화 및 해싱 알고리즘, 인바운드 및 아웃바운드 트래픽 모두에 대한 SA(Security Association)를 비롯한 각 활성 암호화 세션에 대한 포괄적인 세부 정보를 제공해야 합니다. 또한 암호화된 트래픽과 해독된 트래픽에 대한 통계(예: 패킷 및 바이트 수)를 표시하므로, VPN에서 보호하는 데이터 양을 모니터링하고 처리량 문제를 해결하는 데 유용할 수 있습니다.

```
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 연결 재설정

clear cryptocommands는 전체 디바이스를 재부팅할 필요 없이 VPN 연결을 수동으로 재설정하거나 SA(Security Association)를 지우는 데 사용됩니다.

- clear crypto ikev2는 IKEv2 보안 연결(IKEv2 SA)을 지웁니다.
- clear crypto session은 IKEv1(isakmp)/IKEv2 및 IPSec SA를 지웁니다.

- clear crypto sa는 IPsec SA만 지웁니다.
- crypto ipsec sa를 지우면 활성 IPsec 보안 연결이 삭제됩니다.

추가 트러블슈팅을 위해 디버깅 수행

IKEv2 디버그는 VPN 세션, 정책 애플리케이션 또는 클라이언트별 오류 설정 문제와 같이 IKEv2 협상 프로세스 및 FlexVPN 클라이언트 연결 중에 발생할 수 있는 헤드엔드 디바이스(c8000v)의 오류를 식별하고 트러블슈팅하는 데 도움이 될 수 있습니다.

```
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
```

관련 문서 및 문서

[보안 오버레이 및 단일 IP 컨피그레이션](#)

[NFVIS의 BGP 지원](#)

[Secure Overlay 및 BGP 명령](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.