使用BGP路由通告配置安全重叠

目录

简介

本文档介绍如何在NFVIS上为专用vBranch流量管理配置安全重叠和eBGP通告。

使用的组件

本文档中的信息基于以下硬件和软件组件：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

BGP路由通告

NFVIS BGP功能与安全重叠功能配合使用，通过安全重叠隧道从BGP邻居获知路由。这些获取的路由或子网会添加到安全隧道的NFVIS路由表中，从而可通过隧道访问路由。由于安全重叠仅允许从隧道获取1个私有路由；配置BGP可以通过加密隧道建立邻接并将导出的路由注入NFVIS vpnv4路由表（反之亦然）来克服此限制。

配置示例

拓扑图

此配置的目标是从c8000v访问NFVIS的管理IP地址。 一旦隧道建立，就可以使用eBGP路由通告从专用vrf子网通告更多路由。

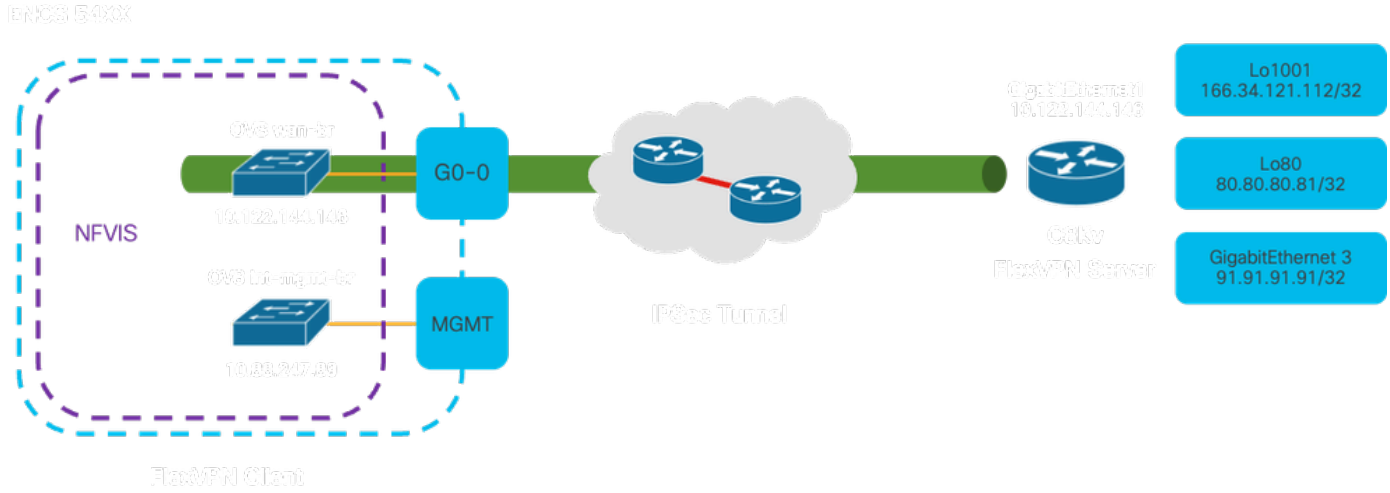


图 1. 针对本文准备的示例的拓扑图

初始设置

在FlexVPN服务器上配置相关IP编址（均在全局配置模式下）

```
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
```

对于NFVIS，请相应地配置WAN和管理接口

```
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路由器上的FlexVPN服务器配置

1. 创建IKEv2方案

它指定了两个VPN终端在建立安全通信信道的初始阶段（第1阶段）必须使用的安全协议和算法。IKEv2提议的目的是概述身份验证、加密、完整性和密钥交换的参数，从而确保两个终端在交换任何敏感数据之前同意一组通用的安全措施。

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

其中：

encryption <algorithm>	该方案包括VPN必须用来保护数据的加密算法（如AES或3DES）。加密可防止窃听者读取通过VPN隧道的流量。

integrity <hash>	它指定了用于确保IKEv2协商期间所交换消息的完整性和真实性的算法（例如SHA-512）。这可以防止篡改和重播攻击。

2. 创建IKEv2策略并将其与建议关联。

它是一个配置集，规定了建立IPsec VPN连接的初始阶段（第1阶段）的参数。 它主要关注VPN终端如何相互进行身份验证以及如何为VPN设置建立安全通信信道。

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

3. 配置IKEv2授权策略

IKEv2协议用于在网络上的两个终端之间设置安全会话，授权策略是一组规则，用于确定在建立VPN隧道后允许VPN客户端访问哪些资源和服务。

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

其中：

pfs	完全转发保密(PFS)功能通过确保每个新加密密钥独立安全（即使之前的密钥已泄露）来增强VPN连接的安全性。
route set interface <接口名称>	成功建立VPN会话后，IKEv2授权策略中定义的路由将自动添加到设备路由表中。这可确保通过VPN隧道正确路由发往路由集中指定网络的流量。

4. 创建IKEv2配置文件

IKEv2（Internet密钥交换版本2）策略是在建立IPsec（Internet协议安全）VPN隧道的IKEv2阶段使用的一组规则或参数。IKEv2协议可促进希望通过不受信任的网络（例如internet）进行安全通信的两方之间的密钥安全交换和安全关联(SA)协商。IKEv2策略定义如何进行此协商，指定双方必须同意的各种安全参数，以建立安全加密的通信信道。

IKEv2配置文件必须具有：

- 本地和远程身份验证方法。
- 匹配身份或匹配证书或match any语句。

```
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
```

其中：

match fvrf public-vrf	使配置文件具有vrf感知能力。
match identity remote any	识别传入会话的有效措施；在这种情况下，识别任何人。
authentication remote pre-share key ciscociscocisco123	指定必须使用预共享密钥对远程对等设备进行身份验证。
authentication local pre-share key ciscociscocisco123	指定此设备（本地）必须使用预共享密钥进行身份验证。
dpd 60 2点播	失效对等体检测；如果在一分钟（60秒）内没有收到数据包，请在此60秒间隔内发送2个dpd数据包。
aaa authorization group psk list default uCPE-author-pol local	路由分配。
virtual-template 1 mode auto	绑定到虚拟模板。

5. 创建IPsec转换集

它定义了一组必须应用于通过IPsec隧道的数据流量的安全协议和算法。实质上，转换集指定如何加密和验证数据，确保VPN终端之间的安全传输。隧道模式将IPsec隧道配置为封装整个IP数据包，以便在网络中实现安全传输。

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

其中：

set transform-set <transform-set-name>	指定必须用于保护通过VPN隧道的数据的加密和完整性算法（例如：AES用于加密，SHA用于完整性）。
set ikev2-profile <ikev2-profile-name>	定义VPN设置第1阶段中安全关联(SA)协商的参数，包括加密算法、哈希算法、身份验证方法和Diffie-Hellman组。
set pfs <group>	一个可选设置，如果启用，该设置可确保每个新加密密钥与之前的任何密钥无关，从而增强安全性。

6. 删除默认IPsec配置文件

出于与安全、自定义和系统清晰性相关的多个原因，采用删除默认IPsec配置文件是一种做法。 默认IPsec配置文件无法满足网络的特定安全策略或要求。删除它可确保没有任何VPN隧道无意中使用次优或不安全的设置，从而降低漏洞风险。

每个网络都有独特的安全要求，包括特定的加密和散列算法、密钥长度和身份验证方法。删除默认配置文件可鼓励创建符合这些特定需求的自定义配置文件，确保提供最佳保护和性能。

```
no crypto ipsec profile default
```

7. 创建IPsec配置文件并将其与转换集和IKEv2配置文件关联。

IPsec（Internet协议安全）配置文件是一个配置实体，封装用于建立和管理IPsec VPN隧道的设置和策略。它可以作为一个模板应用于多个VPN连接，标准化安全参数并简化对网络中安全通信的管理。

```
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. 创建虚拟模板

Virtual-Template接口充当虚拟访问接口的动态模板，为管理VPN连接提供了一种可扩展且有效的方法。它允许虚拟访问接口的动态实例化。当新的VPN会话启动时，设备会根据虚拟模板中指定的配置创建虚拟访问接口。此过程通过根据需要动态分配资源来支持大量远程客户端和站点，而无需为每个连接预配置物理接口。

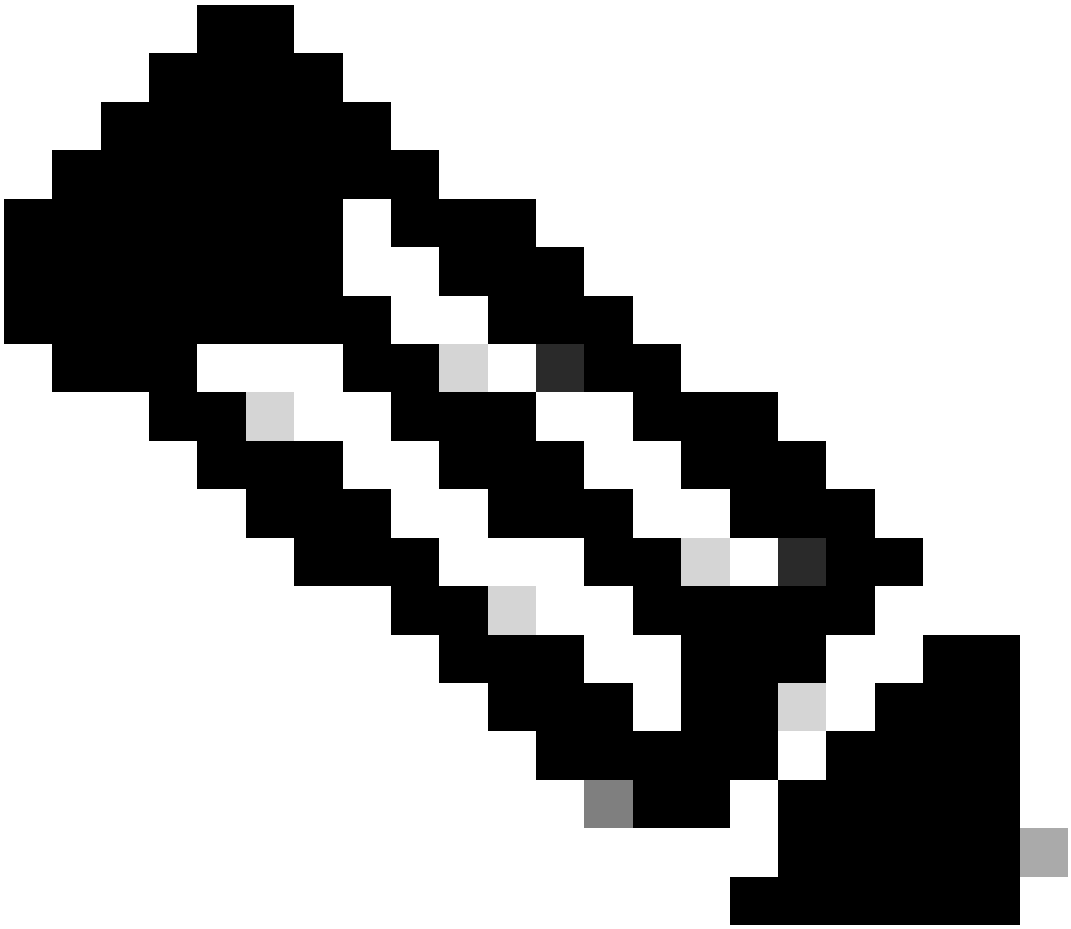
通过使用虚拟模板，FlexVPN部署可以在建立新连接时有效扩展，而无需手动配置每个会话。

```
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安全覆盖最低配置

配置安全重叠实例

```
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
```



注意：在IPSec隧道上配置BGP路由通告时，请确保将安全重叠配置为使用本地隧道IP地址的虚拟IP地址（不是来自物理接口或OVS网桥）。对于以上示例，虚拟编址命令已更改：local-system-ip-addr 10.122.144.146 local-system-ip-subnet 10.122.144.128/27

查看覆盖状态

```
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服务器的BGP路由通告配置

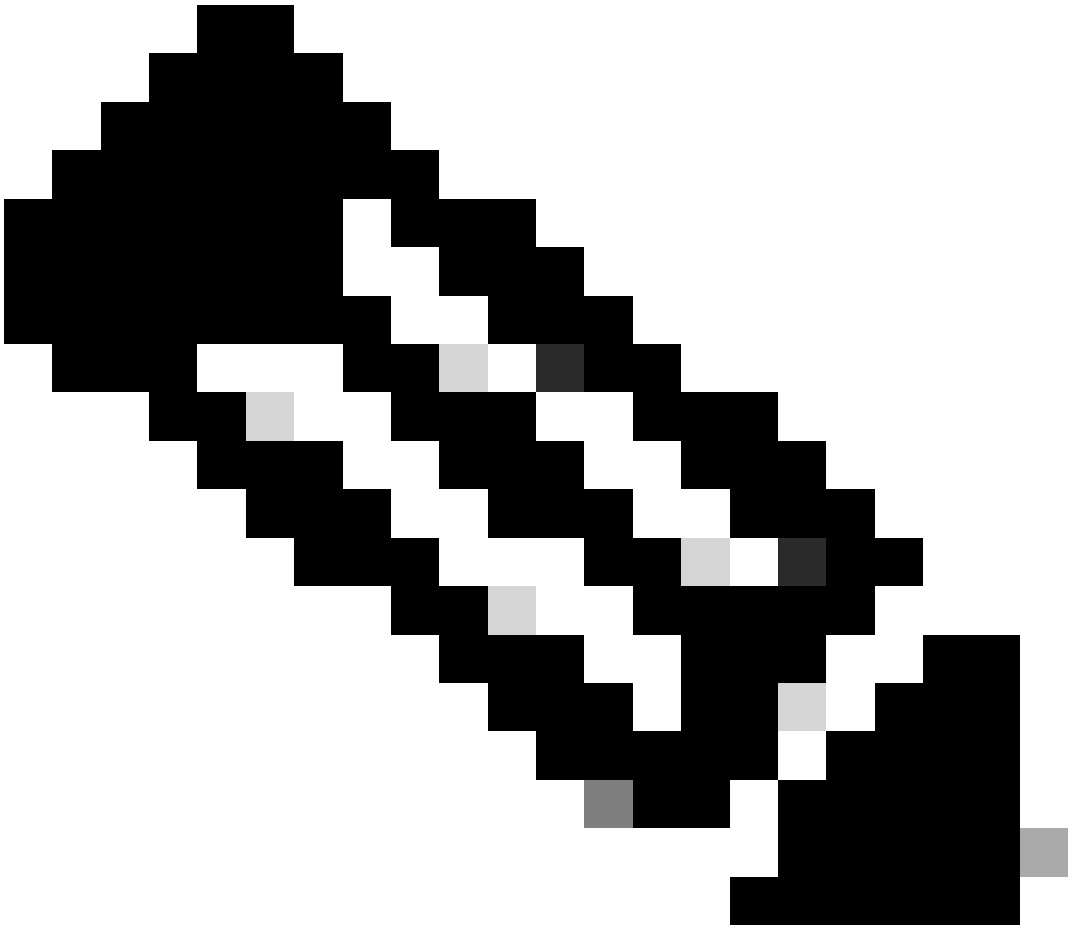
此设置必须为对等体使用eBGP，其中必须将NFVIS端的源地址（本地隧道IP的虚拟IP地址）子网添加到侦听范围。

```
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
```

其中：

bgp always-compare-med	将路由器配置为始终比较所有路由的MED（多出口标识符）属性，而不考虑其来源AS。
bgp log-neighbor-changes	启用与BGP邻居关系更改相关的事件的日志记录。
bgp deterministic-med	确保对不同自治系统中邻居的路径的MED进行比较。
bgp listen range <network>/<mask> peer-group <peer-group-name>	在指定的IP范围（网络/掩码）内启用动态邻居发现，并将发现的邻居分配给对等体组名称。这通过将通用设置应用于组中的所有对等体，简化了配置。
bgp listen limit 255	将侦听范围内可接受的动态BGP邻居的最大数量设置为255。
no bgp default ipv4-unicast	禁止向BGP邻居自动发送IPv4单播路由信息，需要显式配置才能启用此功能。
redistribute connected	将来自直连网络的路由重分布到BGP（来自属于专用vrf的

	FlexVPN服务器的专用子网）中
redistribute static	将静态路由重分布到BGP中。
neighbor uCPEs ebgp-multihop 10	允许与对等体组中的对等体的EBGP（外部BGP）连接跨接最多10跳，这对于连接不直接邻接的设备非常有用。
neighbor uCPEs timers <keep-alive> <hold-down>	为对等组中的邻居分别设置BGP保持连接和抑制计时器（示例为610秒和1835秒）。



注意：出站前缀列表可以配置为控制对等体组中的邻居路由通告：neighbor prefix-list out

NFVIS上的BGP配置

使用eBGP邻居关系设置启动BGP进程

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

BGP评审

此输出显示BIRD Internet路由守护程序报告的BGP会话情况。此路由软件负责处理IP路由并做出有关其方向的决策。根据给出的信息，表明BGP会话处于“Established”状态，表示BGP对等过程已成功完成，并且会话当前处于活动状态。它已成功导入了四条路由，并指出可导入的路由的上限为15条。

```
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
```

确保通过BGP通告FlexVPN服务器的专用子网

配置BGP路由通告时，唯一可配置的地址系列或传输组合是ipv4 unicastfor IPSec。要查看BGP状态，IPSec的可配置地址系列或传输是vpnv4单播。

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

使用show bgp vpnv4 unicast route命令，您可以检索有关BGP进程已知的VPNv4单播路由的信息。

```
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 ?
```

对于头端VPN服务器，可以生成BGP配置和运行状态的概述，以快速评估BGP会话的运行状况和配置。

```
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
```

此外，还可以显示由BGP管理的VPNv4 (VPN over IPv4)路由表条目的详细信息，它必须包括每个VPNv4路由的特定属性，如路由前缀、下一跳IP地址、始发AS编号和各种BGP属性(如本地优先级、MED（多出口标识符）和社区值)。

```
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 ?
```

故障排除

NFVIS（FlexVPN客户端）

NFVIS日志文件

您可以从NFVIS charon.log日志文件查看IPsec阶段的所有初始化和错误日志：

```
nfvis# show log charon.log
Feb  5 07:55:36.771 00[JOB] spawning 16 worker threads
Feb  5 07:55:36.786 05[CFG] received stroke: add connection 'myconn'
```

```
Feb  5 07:55:36.786 05[CFG] added configuration 'myconn'
Feb  5 07:55:36.787 06[CFG] received stroke: initiate 'myconn'
Feb  5 07:55:36.787 06[IKE] <myconn|1> initiating IKE_SA myconn[1] to 10.88.247.84
Feb  5 07:55:36.899 06[ENC] <myconn|1> generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_
Feb  5 07:55:36.899 06[NET] <myconn|1> sending packet: from 10.88.247.89[500] to 10.88.247.84[500] (741
Feb  5 07:55:37.122 09[NET] <myconn|1> received packet: from 10.88.247.84[500] to 10.88.247.89[500] (80
Feb  5 07:55:37.122 09[ENC] <myconn|1> parsed IKE_SA_INIT response 0 [ SA KE No V V V V N(NATD_S_IP) N(
Feb  5 07:55:37.122 09[IKE] <myconn|1> received Cisco Delete Reason vendor ID
Feb  5 07:55:37.122 09[ENC] <myconn|1> received unknown vendor ID: 43:49:53:43:4f:56:50:4e:2d:52:45:56:
Feb  5 07:55:37.122 09[ENC] <myconn|1> received unknown vendor ID: 43:49:53:43:4f:2d:44:59:4e:41:4d:49:
Feb  5 07:55:37.122 09[IKE] <myconn|1> received Cisco FlexVPN Supported vendor ID
Feb  5 07:55:37.122 09[CFG] <myconn|1> selected proposal: IKE:AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SHA
Feb  5 07:55:37.235 09[IKE] <myconn|1> cert payload ANY not supported - ignored
Feb  5 07:55:37.235 09[IKE] <myconn|1> authentication of '10.88.247.89' (myself) with pre-shared key
Feb  5 07:55:37.235 09[IKE] <myconn|1> establishing CHILD_SA myconn{1}
Feb  5 07:55:37.236 09[ENC] <myconn|1> generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) IDr AUTH SA
Feb  5 07:55:37.236 09[NET] <myconn|1> sending packet: from 10.88.247.89[4500] to 10.88.247.84[4500] (4
Feb  5 07:55:37.322 10[NET] <myconn|1> received packet: from 10.88.247.84[4500] to 10.88.247.89[4500] (
Feb  5 07:55:37.322 10[ENC] <myconn|1> parsed IKE_AUTH response 1 [ V IDr AUTH SA TSi TSr N(SET_WINSIZE
Feb  5 07:55:37.323 10[IKE] <myconn|1> authentication of '10.88.247.84' with pre-shared key successful
Feb  5 07:55:37.323 10[IKE] <myconn|1> IKE_SA myconn[1] established between 10.88.247.89[10.88.247.89].
Feb  5 07:55:37.323 10[IKE] <myconn|1> scheduling rekeying in 86190s
Feb  5 07:55:37.323 10[IKE] <myconn|1> maximum IKE_SA lifetime 86370s
Feb  5 07:55:37.323 10[IKE] <myconn|1> received ESP_TFC_PADDING_NOT_SUPPORTED, not using ESPv3 TFC padd
Feb  5 07:55:37.323 10[CFG] <myconn|1> selected proposal: ESP:AES_CBC_256/HMAC_SHA2_512_256/NO_EXT_SEQ
Feb  5 07:55:37.323 10[IKE] <myconn|1> CHILD_SA myconn{1} established with SPIs cfc15900_i 49f5e23c_o a
Feb  5 07:55:37.342 11[NET] <myconn|1> received packet: from 10.88.247.84[4500] to 10.88.247.89[4500] (
Feb  5 07:55:37.342 11[ENC] <myconn|1> parsed INFORMATIONAL request 0 [ CPS(SUBNET VER U_PFS) ]
Feb  5 07:55:37.342 11[IKE] <myconn|1> Processing informational configuration payload CONFIGURATION
Feb  5 07:55:37.342 11[IKE] <myconn|1> Processing information configuration payload of type CFG_SET
Feb  5 07:55:37.342 11[IKE] <myconn|1> Processing attribute INTERNAL_IP4_SUBNET
Feb  5 07:55:37.342 11[ENC] <myconn|1> generating INFORMATIONAL response 0 [ ]
Feb  5 07:55:37.342 11[NET] <myconn|1> sending packet: from 10.88.247.89[4500] to 10.88.247.84[4500] (9
```

内部Kernel strongswan注入路由

在Linux上，默认情况下，strongswan（NFVIS使用的多平台IPsec实施）将路由（包括BGP VPNv4单播路由）安装到路由表220中，因此需要内核支持基于策略的路由。

```
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
```

检查IPsec0接口状态

通过使用ifconfig，您可以获得有关ipsec0虚拟接口的更多详细信息

```
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
```

头端（FlexVPN服务器）

检查对等体之间的IPsec SA构建

从以下输出中，通过Virtual-Access1接口在10.88.247.84和10.88.247.89之间建立加密隧道，用于传输网络0.0.0.0/0和10.122.144.128/27之间的流量；两个封装安全负载(ESP)SA构建入站和出站。

```
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:
```

显示活动加密（加密）会话

show crypto session detail的输出必须提供有关每个活动加密会话的全面详细信息，包括VPN类型（如站点到站点或远程访问）、使用的加密和散列算法，以及入站和出站流量的安全关联(SA)。因为它还会显示有关加密和解密流量的统计信息，例如数据包数和字节数；这对于监控VPN保护的数据量和排除吞吐量问题非常有用。

```
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
```

重置VPN连接

clear cryptocommand用于手动重置VPN连接，或清除安全关联(SA)，而无需重新启动整个设备。

- clear crypto ikev2 将清除IKEv2安全关联(IKEv2 SA)。
- clear crypto session将清除IKEv1 (isakmp)/IKEv2和IPSec SA。
- clear crypto sa将仅清除IPSec SA。
- clear crypto ipsec sa将删除活动的IPSec安全关联。

执行调试以进行其他故障排除

IKEv2调试可以帮助识别前端设备(c8000v)上在IKEv2协商进程和FlexVPN客户端连接期间可能发生的错误（例如建立VPN会话的问题、策略应用或任何客户端特定的错误）并进行故障排除。

```
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
```

相关文章和文档

安全重叠和单一IP配置

NFVIS上的BGP支持

安全覆盖和BGP命令

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。