تكوين تغشية آمنة باستخدام إعلانات مسار BGP

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين تغشية آمنة وإعلانات eBGP على NFVIs لإدارة حركة مرور البيانات الخاصة ببروتوكول vBranch.

المكونات المستخدمة

أسست المعلومة في هذا وثيقة على هذا جهاز وبرمجية مكون:

- ENCS5412 الذي يشغل NFVIs 4.7.1
- مادة حفازة 8000v ريكض cisco IOS® XE 17.09.03a

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

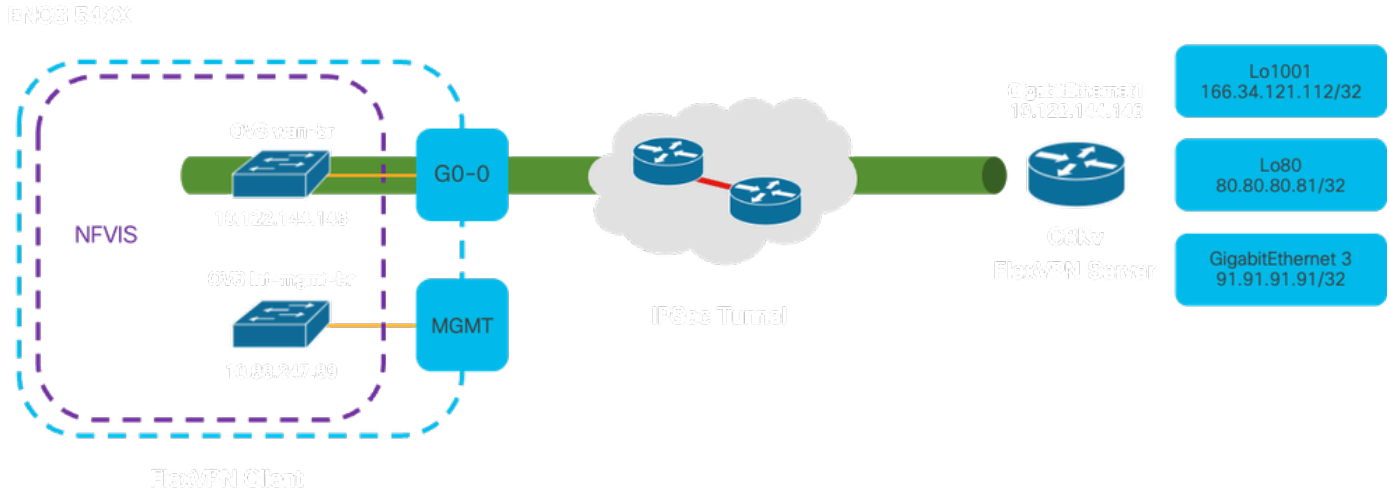
إعلان مسار BGP

تعمل ميزة NFVIs BGP مع ميزة التغشية الآمنة للتعرف على المسارات من جوار BGP عبر نفق تغشية آمن. تتم إضافة المسارات أو الشبكات الفرعية المتعلمة هذه إلى جدول توجيه NFVI للنفق الآمن، مما يجعل المسارات قابلة للوصول إليها عبر النفق. ونظرا لأن التغشية الآمنة تسمح فقط بتعلم مسار خاص واحد من النفق، فإن تكوين بروتوكول BGP يمكن التغلب على هذا التحديد من خلال إنشاء تجاور من خلال النفق المشفر وإدخال المسارات المصدرة إلى جدول توجيه NFVIs VPNV4 والعكس.

مثال التكوين

مخطط الطوبولوجيا

الهدف لهذا التكوين هو الوصول إلى عنوان IP الخاص بإدارة NFVIs من c8000v. وبمجرد إنشاء النفق، من الممكن الإعلان عن مزيد من المسارات من الشبكات الفرعية الخاصة-VRF باستخدام إعلانات مسار بروتوكول eBGP.



شكل 1. مخطط مخطط المخطط للمثال الذي تم إعداده على هذه المقالة

الإعداد الأولي

تكوين عنونة IP ذات الصلة على خادم FlexVPN (جميعها داخل وضع التكوين العام)

```
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
```

باللنسبة لوجهات NFVIs، قم بتكوين واجهة WAN و MGMT وفقا لذلك

```
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
!
```

تكوين خادم FlexVPN على موجه Catalyst 8000v

1. إنشاء مقترح IKEv2

وهو يحدد بروتوكولات المصادقة وخوارزميات التشفير التي يجب أن تستخدمها نقطتا نهاية الشبكة الخاصة الظاهرية (VPN) أثناء المرحلة الأولى (المرحلة 1) من إنشاء قناة اتصال آمنة. والغرض من اقتراح IKEv2 هو تحديد البارامترات الخاصة بالتصديق والتشفير والنزاهة وتبادل المفاتيح، وبالتالي ضمان إتفاق نقطتي النهاية على مجموعة مشتركة من تدابير الأمان قبل تبادل أي بيانات حساسة.

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

حيث:

<خوارزمية التشفير>	ويتضمن المقترح خوارزميات التشفير (مثل AES أو 3DES) التي يجب أن تستخدمها الشبكة الخاصة الظاهرية (VPN) لحماية البيانات. يمنع التشفير متلقي الصوت من القدرة على قراءة حركة مرور البيانات التي تمر عبر نفق VPN.
<hash> التكامل	وهو يحدد الخوارزميات (مثل SHA-512) المستخدمة لضمان سلامة وأصالة الرسائل المتبادلة أثناء التفاوض بشأن IKEv2. وهذا يمنع التلاعب والهجمات المتكررة.

2. إنشاء سياسة IKEv2 وإقرانها بالاقتراح.

إنها مجموعة تكوين تملي معلمات المرحلة الأولية (المرحلة 1) لإنشاء اتصال VPN لـ IPsec. وهو يركز بشكل أساسي على كيفية مصادقة نظائر الشبكة الخاصة الظاهرية (VPN) بعضها البعض وإنشاء قناة اتصال آمنة لإعداد الشبكة الخاصة الظاهرية (VPN).

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

3. تكوين نهج تخويل IKEv2

IKEv2 هو بروتوكول يستخدم لإعداد جلسة عمل آمنة بين نقطتي نهاية على شبكة، ونهج التخويل هو مجموعة من القواعد التي تحدد المواردوالخدمات التي يسمح لعميل VPN بالوصول إليها بمجرد إنشاء نفق VPN.

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

حيث:

ملفات PFS	السرية التامة لإعادة التوجيه (PFS) هي ميزة تعمل على تحسين أمان اتصال الشبكة الخاصة الظاهرية (VPN) من خلال ضمان أمان كل مفتاح تشفير جديد بشكل مستقل، حتى إذا تم أختراق المفاتيح السابقة.
واجهة مجموعة المسارات <interface-	عند إنشاء جلسة عمل الشبكة الخاصة الظاهرية (VPN) بنجاح، تتم إضافة المسارات المحددة في سياسة تفويض IKEv2 تلقائيا إلى جدول توجيه الجهاز. وهذا يضمن توجيه حركة المرور الموجهة للشبكات المحددة في مجموعة

name>	المسارات بشكل صحيح من خلال نفق VPN.

4. إنشاء ملف تعريف IKEv2

سياسة IKEv2 (Internet Key Exchange version 2) هي مجموعة من القواعد أو المعلمات المستخدمة أثناء مرحلة IKEv2 لإنشاء نفق VPN (أمان بروتوكول الإنترنت) لـ IPsec. IKEv2 بين بروتوكول يسمح التبادل الآمن للمفاتيح والتفاوض حول اقترانات الأمان (SAs) وهو طرفين يرغبان في الاتصال بشكل آمن عبر شبكة غير موثوق بها، مثل الإنترنت. تحدد سياسة IKEv2 كيفية إجراء هذا التفاوض، وتحدد معلمات أمان مختلفة يجب أن يتفق عليها الطرفان لإنشاء قناة اتصال آمنة ومشفرة.

يجب أن يحتوي ملف تعريف IKEv2 على:

- أسلوب مصادقة محلي وعن بعد.
- هوية مطابقة أو شهادة مطابقة أو مطابقة أي كشف.

```
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
```

حيث:

تطابق FVRF عام-VRF	عمل ملف تعريف مع مراعاة VRF.
مطابقة الهوية عن بعد أي	إجراء للتعرف على جلسة العمل الواردة كجلسة صالحة، وفي هذه الحالة، أي شخص.
مصادقة مفتاح المشاركة المسبقة عن بعد Cisco123	تحديد أنه يجب مصادقة النظير البعيد باستخدام مفاتيح مشتركة مسبقا.
المصادقة المحلية لمشاركة مفتاح Cisco123	تحديد وجوب مصادقة هذا الجهاز (المحلي) باستخدام مفاتيح مشتركة مسبقا.
DPD 60 2 حسب الطلب	اكتشاف النظير الميت؛ إذا لم يتم إستلام أي حزم خلال دقيقة (60 ثانية)، فعليك إرسال حزمتين DPD هذه خلال الفترة الزمنية التي تبلغ 60 ثانية.
قائمة AAA للتخويل ASK الخاصة بقائمة uCPE-author-pol الافتراضية المحلية	تعيين المسار.
وضع Virtual-Template 1 التلقائي	الربط بقالب ظاهري.

5. إنشاء مجموعة تحويل IPsec

وهو يحدد مجموعة من بروتوكولات الأمان والخوارزميات التي يجب تطبيقها على حركة مرور البيانات عبر نفق IPsec. وفي الأساس، تحدد مجموعة التحويل كيفية تشفير البيانات ومصادقتها، مما يضمن الإرسال الآمن بين نقاط نهاية VPN. يقوم وضع النفق بتكوين نفق IPsec لتضمين حزمة IP بالكامل للنقل الآمن عبر الشبكة.

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

حيث:

ضبط مجموعة تحويل <transform-set-name>	تحديد خوارزميات التشفير والتكامل (على سبيل المثال: AES للتشفير و SHA للنزاهة) التي يجب إستخدامها لحماية البيانات المتدفقة عبر نفق VPN.
set ikev2-profile <ikev2-profile-name>	يحدد معلمات التفاوض على اقترانات الأمان (SAs) في المرحلة الأولى من إعداد الشبكة الخاصة الظاهرية (VPN)، بما في ذلك خوارزميات التشفير وخوارزميات التجزئة وأساليب المصادقة ومجموعة Diffie-Hellman.
ضبط ملفات PFS <مجموعة>	الإعداد الاختياري الذي يضمن، في حالة تمكينه، عدم إرتباط كل مفتاح تشفير جديد بأي مفتاح سابق، مما يعزز الأمان.

6. إزالة ملف تعريف IPsec الافتراضي

إزالة ملف تعريف IPsec الافتراضي هي ممارسة معتمدة لعدة أسباب تتعلق بالأمان والتخصيص ووضوح النظام. لا يمكن أن يفي ملف تعريف IPsec الافتراضي بسياسات الأمان أو متطلبات الأمان المحددة لشبكتك. كما تضمن إزالتها أن جميع أنفاق الشبكة الخاصة الظاهرية (VPN) تستخدم دون قصد إعدادات دون المستوى الأمثل أو غير آمنة، مما يقلل من مخاطر نقاط الضعف.

ولكل شبكة متطلبات أمان فريدة، بما في ذلك التشفير المحدد وخوارزميات التجزئة وطول المفاتيح وطرق المصادقة. تشجع إزالة التوصيف الافتراضي على إنشاء توصيفات مخصصة مخصصة مخصصة مخصصة لهذه الاحتياجات وتضمن أفضل حماية وأداء ممكن.

```
no crypto ipsec profile default
```

7. قم بإنشاء ملف تعريف IPsec وربطه بمجموعة تحويل وملف تعريف IKEv2.

ملف تعريف IPsec (أمان بروتوكول الإنترنت) هو كيان تكوين يتضمن الإعدادات والسياسات الخاصة بإنشاء أنفاق VPN IPsec وإدارتها. وهو يعمل كقالب يمكن تطبيقه على المستخدمة لإنشاء أنفاق VPN IPsec وإدارتها. وهو يعمل كقالب يمكن تطبيقه على إتصالات متعددة للشبكات الخاصة الظاهرية (VPN)، مما يعمل على توحيد معلمات الأمان

وتبسيط إدارة الاتصال الآمن عبر الشبكة.

```
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. إنشاء قالب ظاهري

تعمل واجهة القالب الظاهري كقالب ديناميكي لواجهات الوصول الظاهرية، مما يوفر طريقة قابلة للتطوير وفعالة لإدارة إتصالات VPN. وهو يسمح بالتمثيل الديناميكي لواجهات Virtual-Access. عند بدء جلسة عمل VPN جديدة، يقوم الجهاز بإنشاء واجهة وصول ظاهري استنادا إلى التكوين المحدد في القالب الظاهري. تدعم هذه العملية عددا كبيرا من العملاء والمواقع البعيدة من خلال التخصيص الديناميكي للموارد حسب الحاجة دون الحاجة إلى واجهات مادية تم تكوينها مسبقا لكل اتصال.

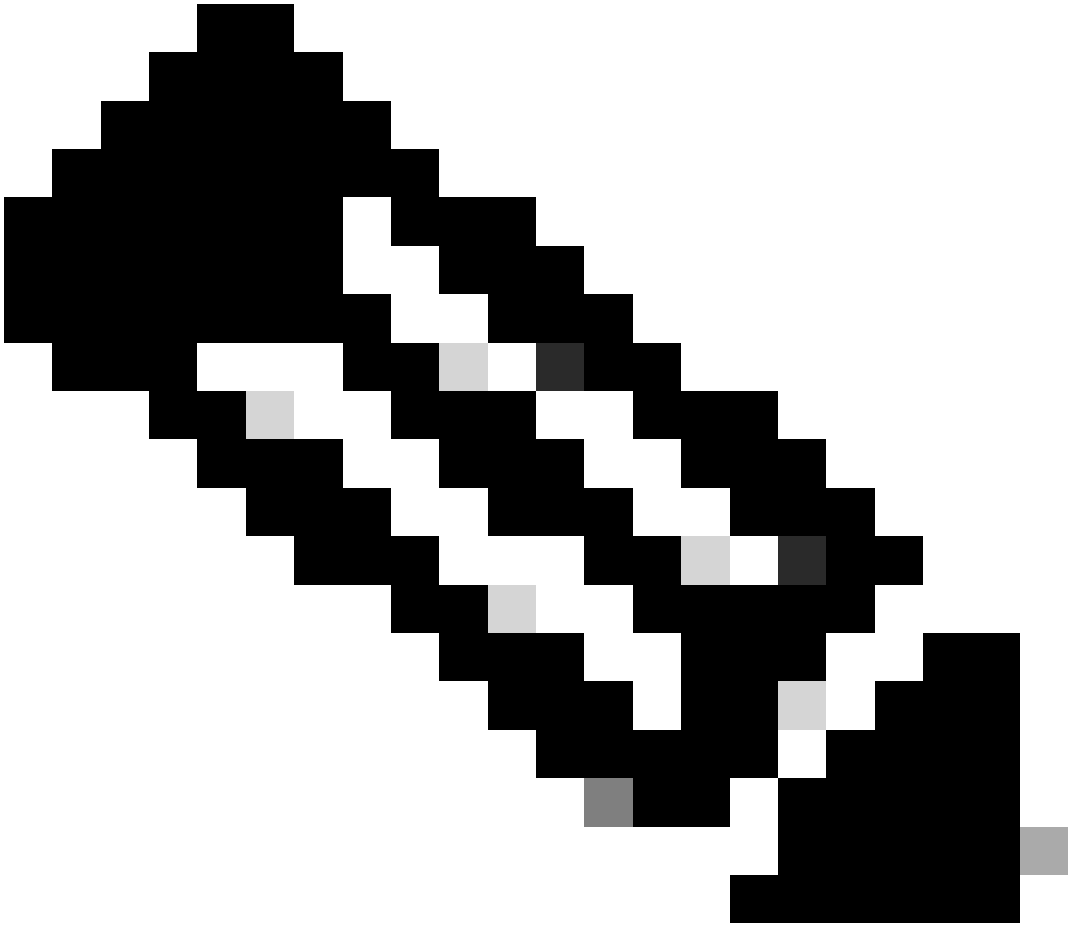
من خلال إستخدام Virtual-Templates، يمكن تطوير عمليات نشر FlexVPN بكفاءة مع إنشاء إتصالات جديدة، دون الحاجة إلى التهيئة اليدوية لكل جلسة عمل فردية.

```
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
```

الحد الأدنى للتكوين الآمن لتضمين NFVIs

تكوين مثيل Secure-overlay

```
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
```



ملاحظة: عند تكوين إعلان مسار BGP عبر نفق IPSec، تأكد من تكوين التغشية لعنوان IP (OS جسر أو وحدة مادية أو جهاز مصدرها من ليس) ظاهري IP عنوان استخدام على الآمنة. على سبيل المثال أعلاه، هذه هي أوامر العنونة الظاهرية التي تم تغييرها: local-system-ip-addr 10.122.144.146 local-system-ip-subnet 10.122.144.128/27

مراجعة حالة التغشية

```
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
```

تكوين إعلان مسار BGP لخادم FlexVPN

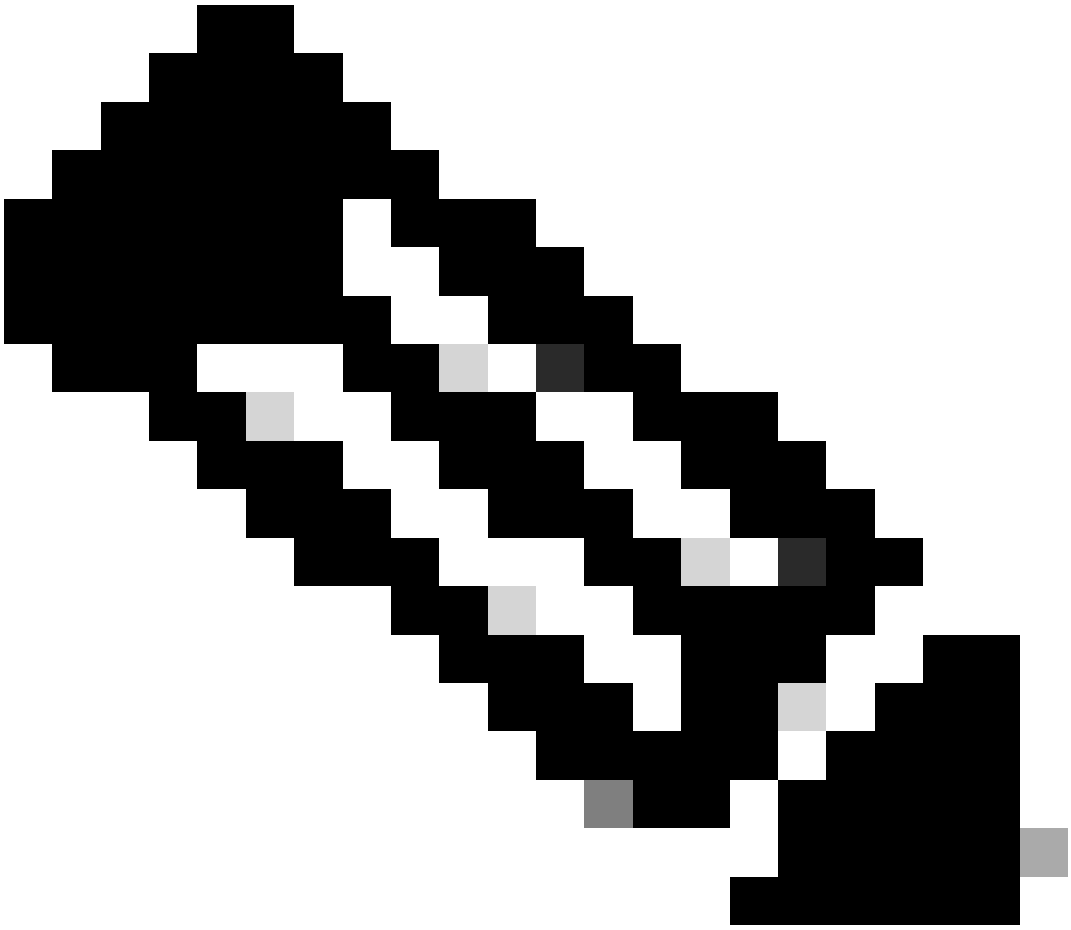
يجب أن يستخدم هذه الإعداد eBGP للعلامات، حيث يجب إضافة عنوان المصدر (عنوان IP الظاهري للشبكة الفرعية للنفق المحلي IP) من جانب NFVIs إلى نطاق الاستماع.

```
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
```

حيث:

BGP Always-compare-med	يقوم بتكوين الموجه لمقارنة سمة MED (مميز متعدد المنافذ) دائما لجميع المسارات، بغض النظر عن مصدرها AS.
BGP log-neighbor-changes	تمكين التسجيل للأحداث المتعلقة بالتغييرات في علاقات جوار BGP.
BGP المحدد-Med	تضمن مقارنة الموارد الكيميائية للمسارات القادمة من الدول المجاورة في أنظمة تحكم ذاتي مختلفة.
نطاق إستماع BGP <network>/<mask> مجموعة نظير <peer-group-name>	تمكين اكتشاف المجاور الديناميكي ضمن نطاق IP المحدد (الشبكة/القناع) وتعيين الجيران المكتشفين لمس مجموعة النظير. يعمل هذا على تبسيط التكوين من خلال تطبيق الإعدادات المشتركة على جميع النظراء في المجموعة.
حد الاستماع ل BGP 255	تعيين الحد الأقصى لعدد جيران BGP الديناميكية التي يمكن قبولها ضمن نطاق الإصغاء إلى 255.
ال يوجد بروتوكول BGP افتراضي بروتوكول IPv4-unicast	تعطيل الإرسال التلقائي لمعلومات توجيه البث الأحادي IPv4 إلى جيران BGP، يتطلب تكوين صريح لتمكين هذا.
إعادة توزيع متصل	يعيد توزيع المسارات من الشبكات المتصلة مباشرة إلى BGP (الشبكات الفرعية الخاصة من خادم FlexVPN الذي ينتمي إلى Private-VRF)
إعادة توزيع ثابت	إعادة توزيع المسارات الثابتة إلى بروتوكول BGP.
neighbor uCPEs eBGP-multihop 10	يسمح لاتصالات EBGP (BGP الخارجي) مع النظراء في مجموعة النظير بتفسحة بين دعامتين حتى 10 نقلات، مفيدة لتوصيل الأجهزة غير المتقابلة مباشرة.

وحدات توقيت CPE المجاورة <Keep-Alive> <Hold-Down>	تعيين مؤقتات BGP keepalive ومؤقتات التعليق للجيران في واجهة مجموعة النظير (610 ثانية و 1835 ثانية للمثال).



ملاحظة: يمكن تكوين قائمة البادئات الصادرة للتحكم في إعلانات المسار المجاور في مجموعة النظير: خروج قائمة البادئات المجاورة

تكوين BGP على NFVIs

بدء عملية BGP باستخدام إعدادات جوار eBGP

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

مراجعة BGP

يكشف هذا المخرج حالة جلسة BGP كما تم الإبلاغ عنها من قبل برنامج توجيه إنترنت الطوير. يكون برنامج التوجيه هذا مسؤولا عن معالجة مسارات IP واتخاذ القرارات المتعلقة باتجاهها. ومن المعلومات المقدمة، يتضح أن جلسة بروتوكول بوابة الحدود (BGP) في حالة "قائمة"، مما يشير إلى إتمام عملية تزجيء بروتوكول بوابة الحدود (BGP) بنجاح، وأن الجلسة نشطة حاليا. وقد استوردت بنجاح أربعة مسارات، والحظت أن هناك حدا أقصى قدره 15 طريقا يمكن إستيرادها.

```
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
```

التأكد من الإعلان عن الشبكات الفرعية الخاصة من خادم FlexVPN من خلال BGP

عند تكوين إعلان مسار BGP، تكون مجموعة العناوين أو مجموعات الإرسال الوحيدة القابلة للتكوين هي IPv4 unicastfor IPSec. لعرض حالة BGP، تكون مجموعة العناوين أو الإرسال القابلة للتكوين ل IPSec هي البث الأحادي VPNV4.

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

باستخدام الأمر show bgp vpnv4 unicast route، يمكنك إستردادا المعلومات حول مسارات البث الأحادي ل VPNv4 المعروفة لعملية BGP.

```
nfvis# show bgp vpnv4 unicast route
Network            Next-Hop        Metric LocPrf Path
81.81.81.1/32      166.34.121.112  0      100    65000 ?
91.91.91.0/24      166.34.121.112  0      100    65000 ?
10.122.144.128/27  166.34.121.112  0      100    65000 ?
166.34.121.112/32  166.34.121.112  0      100    65000 ?
```

بالنسبة لخادم شبكة VPN الطرفي الرئيسي، يمكن إنشاء نظرة عامة على تكوين BGP وحالة التشغيل لتقييم صحة جلسات BGP وتكوينها بسرعة.

```
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
```

وبالإضافة إلى ذلك، يمكن عرض معلومات تفصيلية حول إدخالات جدول توجيه VPNv4 (VPN عبر IPv4) التي تتم إدارتها بواسطة BGP. ويجب أن تتضمن سمات محددة لكل مسار VPNv4، مثل بادئة المسارات وعنوان IP للخطوة التالية والرقم المنشأ AS وسمات BGP المختلفة مثل التفضيل المحلي و MED (مميز متعدد المخرج) وقيم المجتمع.

```
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 ?
```

استكشاف الأخطاء وإصلاحها

NFVIs (عميل FlexVPN)

ملفات سجل NFVIs

يمكنك عرض جميع سجلات التهيئة والخطأ للمراحل IPsec من ملف سجل NFVIs charon.log:

```
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
```

مسارات حقن البجعة الداخلية ل Kernel

في نظام التشغيل Linux، يقوم تقنية SWAN (تنفيذ IPsec متعدد الأنظمة الذي يتم إستخدامه من قبل NFVIs) بتثبيت المسارات (بما في ذلك مسارات البث الأحادي BGP المستخدمة لتوجيه 220 بشكل افتراضي، وبالتالي يتطلب أن يقوم kernel بدعم VPNv4) في جدول التوجيه القائم على السياسة.

```
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
```

مراجعة حالة واجهة IPsec0

يمكنك الحصول على مزيد من التفاصيل حول الواجهة الظاهرية IPSec0 باستخدام 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
```

طرف رئيسي (خادم FlexVPN)

مراجعة بناء IPsec SAs بين الأقران

من إرتباط الإخراج، يتم إنشاء النفق المشفر بين 10.88.247.84 من خلال واجهة Virtual-Access1 و 0.0.0.0/0 تتنقل بين الشبكات لحركة المرور التي تنتقل بين 10.88.247.89 و 10.122.144.128/27؛ ومحمولة أمان التضمين (ESP)SAs تم إنشاؤها في الداخل والخارج.

```
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:
```

عرض جلسات عمل التشفير النشطة (التشفير)

يجب أن يوفر إخراج تفاصيل جلسة عمل show crypto تفاصيل شاملة حول كل جلسة VPN (مثل الوصول من موقع إلى موقع أو من بعد)، بما في ذلك عنوان شبكة نشطة، تشفير، ارتباطات الأمان (SAs) لكل من حركة المرور المستخدمة، وخوارزميات التشفير والتجزئة قيد الاستخدام. كما يعرض إحصائيات حول حركة المرور المشفرة والتي تم فك تشفيرها، والواردة والصادرة. يمكن أن يكون هذا مفيدا لمراقبة مقدار البيانات التي يتم تأمينها بواسطة الشبكة الخاصة الظاهرية (VPN) والاستكشاف أخطاء سعة المعالجة وإصلاحها.

```
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
```

إعادة ضبط إتصالات VPN

يتم إستخدام أوامر التشفير الواضحة لإعادة ضبط إتصالات VPN يدوياً، أو مسح اقترانات الأمان (SAs) دون الحاجة إلى إعادة تمهيد الجهاز بالكامل.

- مسح crypto ikev2 من شأنه مسح اقترانات أمان IKEv2 (IKEv2 SAs).
- جلسة تشفير واضحة من شأنها مسح IKEv1 (isakmp)/IKEv2 و IPSec SAs.
- لن تقوم ميزة التشفير الواضح بمسح IPSec SAs فقط.
- سيؤدي مسح تشفير IPsec إلى حذف اقترانات أمان IPSec النشطة.

إجراء تصحيح الأخطاء لمزيد من أستكشاف الأخطاء وإصلاحها

يمكن أن يساعد تصحيح أخطاء IKEv2 في تحديد أخطاء الجهاز الطرفي الرئيسي (c8000v) التي يمكن أن تحدث أثناء عملية التفاوض مع IKEv2 واتصالات عميل FlexVPN واستكشاف أخطائها وإصلاحها، مثل المشاكل المتعلقة بإنشاء جلسة عمل VPN أو تطبيق السياسة أو أي أخطاء خاصة بالعميل.

```
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
```

المقالات والوثائق ذات الصلة

تغشية آمنة وتكوين IP أحادي

دعم BGP على NFVIs

BGP و آلمنة التغشية وأوامر

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).