مثال تكوين الوصول عن بعد الموردس إلى FlexVPN الخاص بـ VRF

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
التكوين
مخطط الشبكة
تكوين خادم FlexVPN
تكوين ملف تعريف مستخدم RADIUS
التحقق من الصحة
واجهة الوصول الظاهري المشتقة
جلسات عمل التشفير
استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يزود هذا وثيقة عينة تشكيل ل VPN تحشد وإعادة توجيه (VRF)-aware FlexVPN في سيناريو الوصول عن بعد. يستخدم التكوين موجه Cisco IOS® كجهاز تجميع النفق مع عملاء AnyConnect للوصول عن بعد.

المتطلبات الأساسية

المتطلبات

في مثال التكوين هذا، يتم إنهاء إتصالات VPN على جهاز Multiprotocol Label Switching (MPLS) Provider Edge (PE) حيث تكون نقطة نهاية النفق في شبكة VPN MPLS (الجهة [FVRF] VRF]). بعد فك تشفير حركة مرور البيانات المشفرة، تتم إعادة توجيه حركة مرور النص الواضح إلى شبكة VPN MPLS أخرى (VRF الداخلي [IVRF]).

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- موجه خدمات التجميع من Cisco ASR 1000 Series مع (15.2(4)S1 (IOS-XE3.7.1 كخادم FlexVPN
- Cisco AnyConnect Secure Mobility Client و Cisco AnyConnect VPN Client، الإصدار 3.1
- خادم RADIUS Microsoft Network Policy Server (NPS)

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 مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

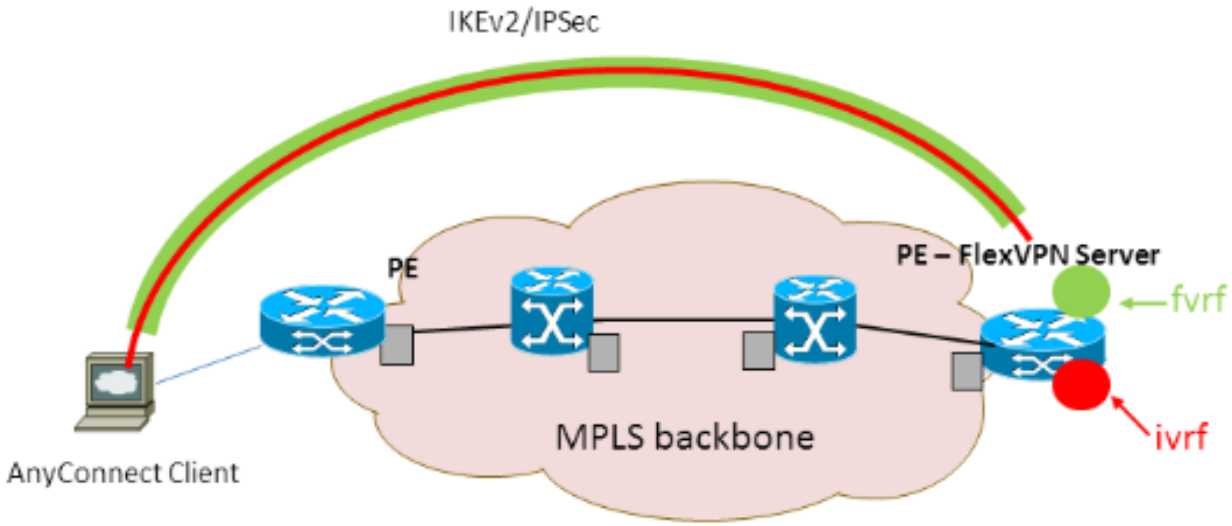
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

مخطط الشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



تكوين خادم FlexVPN

هذا مثال على تكوين خادم FlexVPN:

```
hostname ASR1K
!
aaa new-model
!
!
aaa group server radius lab-AD
server-private 172.18.124.30 key Cisco123
!
aaa authentication login default local
aaa authentication login AC group lab-AD
aaa authorization network AC local
!
aaa session-id common
```

```
!
ip vrf fvrf
rd 2:2
route-target export 2:2
route-target import 2:2
!
ip vrf ivrf
rd 1:1
route-target export 1:1
route-target import 1:1
!
!
crypto pki trustpoint AC
enrollment mode ra
enrollment url http://lab-ca:80/certsrv/mscep/mscep.dll
fqdn asr1k.labdomain.cisco.com
subject-name cn=asr1k.labdomain.cisco.com
revocation-check crl
rsakeypair AC
!
!
crypto pki certificate chain AC
certificate 433D7311000100000259
certificate ca 52DD978E9680C1A24812470E79B8FB02
!
!
crypto ikev2 authorization policy default
pool flexvpn-pool
def-domain cisco.com
route set interface
!
crypto ikev2 authorization policy AC
pool AC
dns 10.7.7.129
netmask 255.255.255.0
banner ^CCC Welcome ^C
def-domain example.com
!
crypto ikev2 proposal AC
encryption aes-cbc-256
integrity sha1
group 5
!
crypto ikev2 policy AC
match fvrf fvrf
proposal AC
!
!
crypto ikev2 profile AC
match fvrf fvrf
match identity remote key-id cisco.com
identity local dn
authentication remote eap query-identity
authentication local rsa-sig
pki trustpoint AC
dpd 60 2 on-demand
aaa authentication eap AC
aaa authorization group eap list AC AC
virtual-template 40
!
!
crypto ipsec transform-set AC esp-aes 256 esp-sha-hmac
mode tunnel
!
```

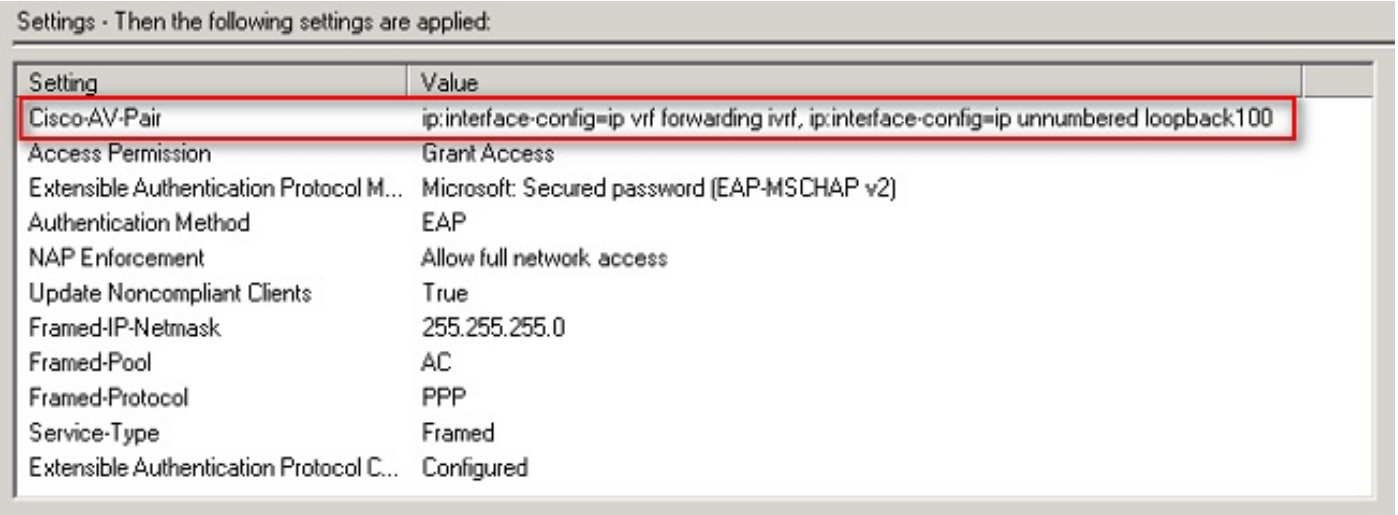
```
crypto ipsec profile AC
  set transform-set AC
  set ikev2-profile AC
!
!
interface Loopback0
 description BGP source interface
 ip address 10.5.5.5 255.255.255.255
!
interface Loopback99
 description VPN termination point in the FVRF
 ip vrf forwarding fvrf
 ip address 7.7.7.7 255.255.255.255
!
interface Loopback100
 description loopback interface in the IVRF
 ip vrf forwarding ivrf
 ip address 6.6.6.6 255.255.255.255
!
interface GigabitEthernet0/0/1
 description MPLS IP interface facing the MPLS core
 ip address 20.11.11.2 255.255.255.0
 negotiation auto
 mpls ip
 cdp enable
!
!
!
interface Virtual-Template40 type tunnel
 no ip address
 tunnel mode ipsec ipv4
 tunnel vrf fvrf
 tunnel protection ipsec profile AC
!
router bgp 2
 bgp log-neighbor-changes
  redistribute connected
  redistribute static
 neighbor 10.2.2.2 remote-as 2
 neighbor 10.2.2.2 update-source Loopback0
 !
 address-family vpnv4
  neighbor 10.2.2.2 activate
  neighbor 10.2.2.2 send-community extended
  exit-address-family
 !
 address-family ipv4 vrf fvrf
  redistribute connected
  redistribute static
  exit-address-family
 !
 address-family ipv4 vrf ivrf
  redistribute connected
  redistribute static
  exit-address-family
 !
ip local pool AC 192.168.1.100 192.168.1.150
```

تكوين ملف تعريف مستخدم RADIUS

يكون تكوين المفتاح المستخدم لملف تعريف RADIUS هو زوجا قيمة السمة (VSA) (AV) الخاصين بالمورد من Cisco اللذان يضعان واجهة الوصول الظاهري التي تم إنشاؤها ديناميكيا في IVRF ويمكن IP على واجهة الوصول الظاهرية التي تم إنشاؤها ديناميكيا:

```
ip:interface-config=ip unnumbered loopback100
ip:interface-config=ip vrf forwarding ivrf
```

في Microsoft NPS، يكون التكوين في إعدادات "نهج الشبكة" كما هو موضح في هذا المثال:



تحذير: يجب أن يأتي الأمر **ip vrf forwarding** قبل الأمر **ip unnumber**. إذا تم نسخ واجهة الوصول الظاهرية من القالب الظاهري، وتم تطبيق الأمر **ip vrf forwarding** بعد ذلك، فسيتم إزالة أي تكوين IP من واجهة الوصول الظاهري. على الرغم من إنشاء النفق، فإن تجاور CEF لواجهة نقطة إلى نقطة (P2P) غير مكتمل. هذا مثال على الأمر **show** neighbors بنتائج غير كاملة:

```
ASR1k#show adjacency virtual-access 1
Protocol Interface                 Address
(IP      Virtual-Access1           point2point(6) (incomplete
```

إذا لم يكتمل تجاور CEF، يتم إسقاط جميع حركة مرور VPN الصادرة.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح. تحقق من واجهة الوصول الظاهري المشتقة، ثم تحقق من إعدادات IVRF و FVRF.

واجهة الوصول الظاهري المشتقة

تحقق من نسخ واجهة الوصول الظاهرية التي تم إنشاؤها بشكل صحيح من واجهة القالب الظاهري ومن أنها قامت بتطبيق كافة سمات كل مستخدم التي تم تنزيلها من خادم RADIUS:

```
ASR1K#sh derived-config interface virtual-access 1
Building configuration...Derived configuration : 250 bytes
!
interface Virtual-Access1
 ip vrf forwarding ivrf
 ip unnumbered Loopback100
 tunnel source 7.7.7.7
 tunnel mode ipsec ipv4
 tunnel destination 8.8.8.10
 tunnel vrf fvrf
 tunnel protection ipsec profile AC
 no tunnel protection ipsec initiate
```

```
end
```

جلسات عمل التشفير

تحقق من إعدادات IVRF و FVRF باستخدام مخرجات مستوى التحكم هذه.

هذا مثال على المخرجات من أمر التفاصيل **show crypto sessiond**:

```
ASR1K#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

Interface: Virtual-Access1
Uptime: 00:23:19
Session status: UP-ACTIVE
Peer: 8.8.8.10 port 57966 fvrf: fvrf ivrf: ivrf
Phase1_id: cisco.com
(Desc: (none
IKEv2 SA: local 7.7.7.7/4500 remote 8.8.8.10/57966 Active
Capabilities:(none) connid:1 lifetime:23:36:41
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 192.168.1.103
Active SAs: 2, origin: crypto map
Inbound:  #pkts dec'ed 95 drop 0 life (KB/Sec) 4607990/2200
Outbound: #pkts enc'ed 44 drop 0 life (KB/Sec) 4607997/2200
```

هذا مثال على المخرج من الأمر **show crypto IKEv2 session detail**:

```
ASR1K#show crypto ikev2 sess detail
IPv4 Crypto IKEv2 Session

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
fvrf/ivrf            READY        8.8.8.10/57966          7.7.7.7/4500         1
Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:5, Auth sign: RSA, Auth verify: EAP
Life/Active Time: 86400/1298 sec
CE id: 1004, Session-id: 4
Status Description: Negotiation done
Local spi: EE87373C2C2643CA       Remote spi: F80C8A4CB4143091
Local id: cn=asr1k.labdomain.cisco.com,hostname=asr1k.labdomain.cisco.com
Remote id: cisco.com
Remote EAP id: user1
Local req msg id:  1              Remote req msg id:  43
Local next msg id: 1              Remote next msg id: 43
Local req queued:  1              Remote req queued:  43
Local window:      5              Remote window:      1
DPD configured for 60 seconds, retry 2
NAT-T is detected  outside
Cisco Trust Security SGT is disabled
Assigned host addr: 192.168.1.103
Initiator of SA : No
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
remote selector 192.168.1.103/0 - 192.168.1.103/65535
ESP spi in/out: 0x88F2A69E/0x19FD0823
AH spi in/out: 0x0/0x0
CPI in/out: 0x0/0x0
Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

```
IPv6 Crypto IKEv2 Session

#ASR1K
```

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems

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).