الترحيل من EzVPN-NEM+ القديم إلى FlexVPN على نفس الخادم

المحتويات

المقدمة

يصف هذا المستند عملية الترحيل من EzVPN إلى FlexVPN. FlexVPN هو حل الشبكة الخاصة الظاهرية (VPN) الموحد الجديد الذي توفره Cisco. تعمل شبكة FlexVPN على تحقيق أقصى إستفادة من بروتوكول IKEv2 وتجمع بين إمكانية الوصول عن بعد والوصول من موقع إلى موقع والوصول والمخاطبة وعمليات النشر الجزئية للشبكة الخاصة الظاهرية (VPN) للشبكة العنكبوتية. باستخدام التقنيات القديمة مثل شبكة EzVPN، تشجعك Cisco بشدة على الترحيل إلى FlexVPN من أجل الاستفادة من الإمكانات الثرية بالميزات الخاصة بها.

يفحص هذا المستند نشر EzVPN موجود الذي يتكون من عملاء أجهزة EzVPN القديمة التي تقوم بإنهاء الأنفاق الموجودة على جهاز الاستقبال والبث الخاص ب EzVPN المستند إلى خريطة التشفير القديمة. الهدف هو الترحيل من هذا التكوين لدعم FlexVPN مع المتطلبات التالية:

- سيستمر العملاء المتوارثون الحاليون في العمل بسلاسة تامة دون إجراء أي تغييرات على التهيئة. وهذا يسمح بترحيل هؤلاء العملاء على مراحل إلى FlexVPN بمرور الوقت.
- يجب أن يدعم جهاز وحدة الاستقبال والبث في نفس الوقت إنهاء عملاء FlexVPN الجدد.

يتم إستخدام مكوني تكوين IPsec الأساسيين للمساعدة في تحقيق أهداف الترحيل هذه: تحديدا، IKEv2 وواجهات النفق الظاهرية (VTI). وتناقش هذه الأهداف بإيجاز في هذه الوثيقة.

مستندات أخرى في هذه السلسلة

- دليل نشر FlexVPN: AnyConnect إلى وحدة الاستقبال والبث عبر IPsec باستخدام IKEv2 والشهادات

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الاصطلاحات

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

IKEv1 مقابل IKEv2

تستند FlexVPN إلى بروتوكول IKEv2، وهو بروتوكول إدارة المفاتيح من الجيل التالي القائم على بروتوكول RFC 4306، وتحسين بروتوكول IKEv1. لا يتوافق FlexVPN مع التقنيات التي تدعم IKEv1 فقط (على سبيل المثال، EzVPN). هذا أحد الاعتبارات الأساسية عند الترحيل من EzVPN إلى FlexVPN. للحصول على مقدمة للبروتوكول حول IKEv2 والمقارنة مع IKEv1، راجع الإصدار 2 من IKE نظرة سريعة.

خريطة التشفير مقابل واجهات النفق الظاهرية

واجهة النفق الظاهرية (VTI) هي طريقة تكوين جديدة تستخدم لكل من تكوينات خادم VPN والعميل. VTI:

- إستبدال خرائط التشفير الديناميكية، والتي تعتبر الآن تكوينا قديما.
- يدعم اتصال IPsec النفقي الأصلي.
- لا يتطلب تعيين ثابت لجلسة عمل IPsec إلى واجهة مادية؛ لذلك، يوفر مرونة لإرسال حركة مرور مشفرة واستقبالها على أي واجهة مادية (على سبيل المثال، مسارات متعددة).
- تم نسخ الحد الأدنى من التكوين كوصول ظاهري حسب الطلب من واجهة القالب الظاهري.
- يتم تشفير/فك تشفير حركة مرور البيانات عند إعادة التوجيه إلى/من واجهة النفق وتتم إدارتها بواسطة جدول توجيه IP (وبالتالي، تقوم بدور مهم في عملية التشفير).
- يمكن تطبيق الميزات على حزم النصوص غير المشفرة على واجهة VTI، أو الحزم المشفرة على الواجهة المادية.

النوعان المتاحان من VTIs يتوفر:

- ساكن إستاتيكي (sVTI) — تحتوي واجهة النفق الظاهرية الثابتة على مصدر النفق الثابت والوجهة ويتم إستخدامها عادة في سيناريو نشر من موقع إلى موقع. هنا مثال من sVTI تشكيل:

```
interface Tunnel2
 ip address negotiated
tunnel source Ethernet0/1
 tunnel mode ipsec ipv4
```

```
tunnel destination 172.16.0.2
tunnel protection ipsec profile testflex
```

- Dynamic (dVTI) — يمكن إستخدام واجهة نفق ظاهري ديناميكي لإنهاء أنفاق IPsec الديناميكية التي ليس لها وجهة نفق ثابت. عند نجاح تفاوض النفق، سيتم نسخ واجهات الوصول الظاهري من قالب ظاهري وسترث جميع ميزات L3 على هذا القالب الظاهري. هنا مثال من dVTI تشكيل:

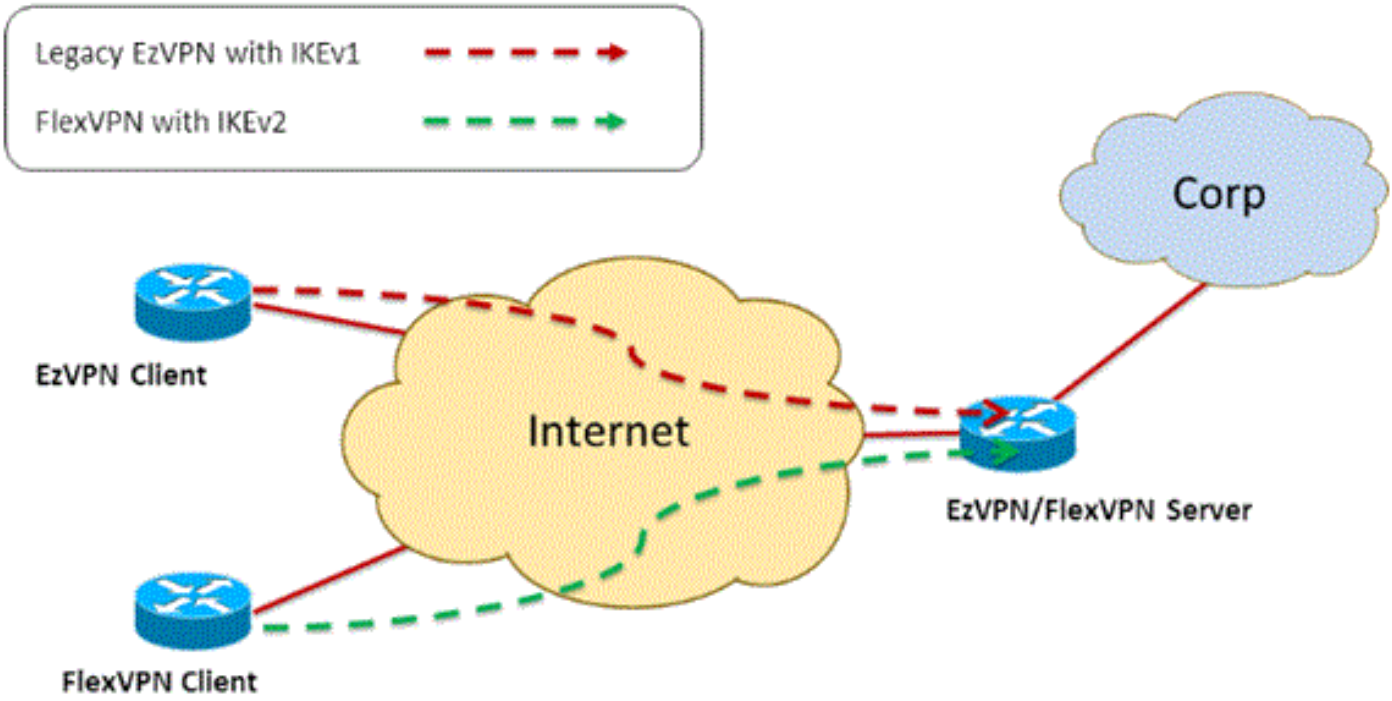
```
interface Virtual-Template1 type tunnel
ip unnumbered Ethernet0/1
tunnel mode ipsec ipv4
tunnel protection ipsec profile testflex
```

أحلت هذا وثيقة ل كثير معلومة على dVTI:

- تكوين شبكة VPN سهلة من Cisco باستخدام واجهة النفق الظاهرية الديناميكية (DVTI) لبروتوكول IPSec
- قيود واجهة النفق الظاهري ل IPsec
- تكوين دعم Multi-SA لواجهات النفق الظاهرية الديناميكية باستخدام IKEv1

لكي يتعايش عملاء EzVPN و FlexVPN، يجب عليك أولا ترحيل خادم EzVPN من تكوين خريطة التشفير القديم إلى تكوين dVTI. وتشرح الأقسام التالية بالتفصيل الخطوات اللازمة.

مخطط الشبكة



التكوين الحالي مع عميل وضع EzVPN القديم الذي يحمل اسم NEM+

تكوين العميل

فيما يلي تكوين موجه عميل EzVPN نموذجي. في هذا التكوين، يتم إستخدام وضع Network Extension Plus (NEM+)، والذي يؤدي إلى إنشاء أزواج SA متعددة لكل من واجهات LAN الداخلية بالإضافة إلى تكوين وضع عنوان IP المعين للعميل.

```
crypto ipsec client ezvpn legacy-client
connect manual
group Group-One key cisco123
```

```
                                                mode network-plus
                                                peer 192.168.1.10
                                      username client1 password client1
                                                xauth userid mode local
                                                                      !
                                                interface Ethernet0/0
                                        description EzVPN WAN interface
                                    ip address 192.168.2.101 255.255.255.0
                                   crypto ipsec client ezvpn legacy-client
                                                                      !
                                                interface Ethernet1/0
                                     description EzVPN LAN inside interface
                                        ip address 172.16.1.1 255.255.255.0
                    crypto ipsec client ezvpn legacy-client inside
```

تكوين الخادم

على خادم EzVPN، يتم إستخدام تكوين خريطة تشفير قديمة كتكوين أساسي قبل الترحيل.

```
                                                aaa new-model
                                                                      !
                                  aaa authentication login client-xauth local
                                aaa authorization network ezvpn-author local
                                                                      !
                                      username client1 password 0 client1
                                                                      !
                                                crypto isakmp policy 10
                                                               encr aes
                                            authentication pre-share
                                                                group 2
                                                                      !
                    crypto isakmp client configuration group Group-One
                                                        key cisco123
                                                 pool Group-One-Pool
                                                acl split-tunnel-acl
                                   crypto isakmp profile Group-One-Profile
                                         match identity group Group-One
                                  client authentication list client-xauth
                                   isakmp authorization list ezvpn-author
                                     client configuration address respond
                                                                      !
                crypto ipsec transform-set aes-sha esp-aes esp-sha-hmac
                                                                      !
                                    crypto dynamic-map client-dynamic-map 1
                                                set transform-set aes-sha
                                                            reverse-route
                                                                      !
        crypto map client-map 1 ipsec-isakmp dynamic client-dynamic-map
                                                                      !
                                                interface Ethernet0/0
                                     description EzVPN server WAN interface
                                      ip address 192.168.1.10 255.255.255.0
                                                crypto map client-map
                                                                      !
                    ip local pool Group-One-Pool 10.1.1.100 10.1.1.200
                                                                      !
                                   ip access-list extended split-tunnel-acl
                                            remark EzVPN split tunnel ACL
                                        permit ip 172.16.0.0 0.0.0.255 any
```

ترحيل الخادم إلى FlexVPN

كما هو موضح في الأقسام السابقة، تستخدم FlexVPN الإصدار IKEv2 كبروتوكول مستوى التحكم ولا يتوافق مع الإصدارات السابقة من حل EzVPN القائم على بروتوكول IKEv1. ونتيجة لذلك، تتمثل الفكرة العامة لهذا الترحيل في تكوين خادم EzVPN الموجود بطريقة تسمح بالتعايش بين كل من EzVPN (IKEv1) و FlexVPN (IKEv2) القديم. ومن أجل تحقيق هذا الهدف، يمكنك إستخدام نهج الترحيل المكون من خطوتين:

1. نقل تكوين EzVPN القديم على وحدة الاستقبال والبث من تكوين مستند إلى خريطة تشفير إلى dVTI.
2. أضفت ال FlexVPN تشكيل، أي يكون أيضا يؤسس على dVTI.

نقل خريطة التشفير القديمة إلى dVTI

تغييرات تكوين الخادم

يتضمن خادم EzVPN الذي تم تكوينه باستخدام خريطة التشفير على الواجهة المادية العديد من القيود عندما يتعلق الأمر بدعم الميزات ومرونتها. إذا كانت لديك شبكة EzVPN، فإن Cisco تشجعك بشدة على إستخدام dVTI بدلا من ذلك. كخطوة أولى للترحيل إلى تكوين مشترك بين EzVPN و FlexVPN، يجب عليك تغييره إلى تكوين dVTI. وسيوفر ذلك فصل IKEv1 و IKEv2 بين واجهات القوالب الظاهرية المختلفة لاستيعاب كلا النوعين من العملاء.

ملاحظة: لدعم امتداد الشبكة بالإضافة إلى وضع عملية EzVPN على عملاء EzVPN، يجب أن يتلقى موجه وحدة الاستقبال والبث دعم لميزة Multi SA على dVTI. وهذا يسمح بحماية تدفقات IP المتعددة بواسطة النفق، والذي يكون مطلوبا لوحدة الاستقبال والبث لتشفير حركة مرور البيانات إلى الشبكة الداخلية لعميل EzVPN، بالإضافة إلى عنوان IP الذي تم تعيينه للعميل من خلال تكوين وضع IKEv1. لمزيد من المعلومات حول دعم Multi SA على dVTI باستخدام IKEv1، ارجع إلى دعم Multi-SA لواجهات النفق الظاهرية الديناميكية ل IKEv1.

أكمل الخطوات التالية لتنفيذ تغيير التكوين على الخادم:

الخطوة 1— قم بإزالة خريطة التشفير من واجهة الخروج المادي التي تنهي أنفاق عميل EzVPN:

```
interface Ethernet0/0
ip address 192.168.1.10 255.255.255.0
no crypto map client-map
```

الخطوة 2— قم بإنشاء واجهة قالب ظاهري يتم من خلالها نسخ واجهات الوصول الظاهرية بمجرد إنشاء الأنفاق:

```
interface Virtual-Template1 type tunnel
ip unnumbered Ethernet1/0
tunnel mode ipsec ipv4
tunnel protection ipsec profile legacy-profile
```

الخطوة 3- أربط واجهة القالب الظاهري هذه التي تم إنشاؤها حديثا بملف تعريف ISAKMP لمجموعة EzVPN التي تم تكوينها:

```
crypto isakmp profile Group-One-Profile
match identity group Group-One
client authentication list client-xauth
isakmp authorization list ezvpn-author
client configuration address initiate
client configuration address respond
virtual-template 1
```

بمجرد إجراء تغييرات التكوين الواردة أعلاه، تحقق من إستمرار عملاء EzVPN الحاليين في العمل. ومع ذلك، يتم

الآن إنهاء أنفاقها على واجهة وصول افتراضية تم إنشاؤها ديناميكيا. يمكن التحقق من هذا الإجراء باستخدام أمر **show crypto session** كما في هذا المثال:

```
PE-EzVPN-Server#show crypto session
Crypto session current status
Interface: Virtual-Access1
Username: client1
Profile: Group-One-Profile
Group: Group-One
Assigned address: 10.1.1.101
Session status: UP-ACTIVE
Peer: 192.168.2.101 port 500
IKEv1 SA: local 192.168.1.10/500 remote 192.168.2.101/500 Active
IPSEC FLOW: permit ip 172.16.0.0/255.255.255.0 host 10.1.1.101
Active SAs: 2, origin: crypto map
IPSEC FLOW: permit ip 172.16.0.0/255.255.255.0 172.16.1.0/255.255.255.0
Active SAs: 2, origin: crypto map
```

إضافة تكوين FlexVPN إلى الخادم

يستخدم هذا المثال RSA-SIG (أي مرجع الشهادة) على كل من عميل FlexVPN والخادم. يفترض التكوين الموجود في هذا القسم أن الخادم قام بالفعل بمصادقة وتسجيل نفسه مع خادم CA بنجاح.

الخطوة 1—التحقق من التكوين الافتراضي الذكي ل IKEv2.

مع IKEv2، يمكنك الآن الاستفادة من ميزة "الافتراضية الذكية" التي تم تقديمها في T(1)15.2. ويتم إستخدامها لتبسيط تكوين FlexVPN. فيما يلي بعض التكوينات الافتراضية:

نهج تخويل IKEv2 الافتراضي:

```
VPN-Server#show crypto ikev2 authorization policy default
IKEv2 Authorization Policy : default
route set interface
route accept any tag : 1 distance : 1
```

مقترح IKEv2 الافتراضي:

```
VPN-Server#show crypto ikev2 proposal default
IKEv2 proposal: default
Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
Integrity : SHA512 SHA384 SHA256 SHA96 MD596
PRF : SHA512 SHA384 SHA256 SHA1 MD5
DH Group : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
```

نهج IKEv2 الافتراضي:

```
VPN-Server#show crypto ikev2 policy default
IKEv2 policy : default
Match fvrf : any
Match address local : any
Proposal : default
```

ملف تعريف IPsec الافتراضي:

```
VPN-Server#show crypto ipsec profile default
```

```
IPSEC profile default
Security association lifetime: 4608000 kilobytes/3600 seconds
Responder-Only (Y/N): N
PFS (Y/N): N
}=Transform sets
, { default: { esp-aes esp-sha-hmac
{
```

مجموعة تحويل IPsec الافتراضية:

```
VPN-Server#show crypto ipsec transform default
{ esp-aes esp-sha-hmac }
,{ ,will negotiate = { Transport
```

أحلت ل كثير معلومة على ال IKEv2 Smart تقصير سمة، IKEv2 Smart Default (يسجل زبون فقط).

الخطوة 2- قم بتعديل سياسة تفويض IKEv2 الافتراضية وأضف ملف تعريف IKEv2 الافتراضي لعملاء FlexVPN.

سيتطابق ملف تعريف IKEv2 الذي تم إنشاؤه هنا مع معرف نظير استنادا إلى اسم المجال cisco.com، وسيتم إنشاء واجهات الوصول الظاهرية التي تم إنشاؤها للعملاء من القالب الظاهري 2. لاحظ أيضا أن سياسة التخويل تحدد تجمع عناوين IP المستخدم لتعيين عناوين IP النظيرة بالإضافة إلى المسارات التي سيتم تبادلها عبر وضع تكوين IKEv2:

```
crypto ikev2 authorization policy default
pool flexvpn-pool
def-domain cisco.com
route set interface
route set access-list 1
!
crypto ikev2 profile default
match identity remote fqdn domain cisco.com
identity local fqdn VPN-Server.cisco.com
authentication remote pre-share
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint flex-trustpoint
aaa authorization group cert list default default
virtual-template 2
```

الخطوة 3- قم بإنشاء واجهة القالب الظاهري المستخدمة لعملاء FlexVPN:

```
interface Virtual-Template2 type tunnel
ip unnumbered Ethernet1/0
tunnel protection ipsec profile default
```

تكوين عميل FlexVPN

```
crypto ikev2 authorization policy default
route set interface
route set access-list 1
!
crypto ikev2 profile default
match identity remote fqdn domain cisco.com
identity local fqdn Client2.cisco.com
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint flex-trustpoint
aaa authorization group cert list default default
```

```
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel destination 192.168.1.10
 tunnel protection ipsec profile default
```

إكمال التكوين

إكمال تكوين الخادم المختلط

```
hostname VPN-Server
!
!
aaa new-model
!
aaa authentication login client-xauth local
aaa authorization network default local
aaa authorization network ezvpn-author local
!
!
no ip domain lookup
ip domain name cisco.com
ip host ca-server 192.168.2.1
!
crypto pki trustpoint flex-trustpoint
 enrollment url http://ca-server:80
 serial-number
 ip-address none
 fingerprint 08CBB1E948A6D9571965B5EE58FBB726
 subject-name cn=vpn-server.cisco.com, OU=Flex, O=cisco
 revocation-check crl
 rsakeypair flex-key-pair 1024
!
!
crypto pki certificate chain flex-trustpoint
 certificate 07
 certificate ca 01
username client1 password 0 client1
username cisco password 0 cisco
!
crypto ikev2 authorization policy default
 pool flexvpn-pool
 def-domain cisco.com
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn VPN-Server.cisco.com
 authentication remote pre-share
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
 virtual-template 2
!
```

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto isakmp client configuration group Group-One
 key cisco123
 pool Group-One-Pool
 acl split-tunnel-acl
 save-password
crypto isakmp profile Group-One-Profile
   match identity group Group-One
   client authentication list client-xauth
   isakmp authorization list ezvpn-author
   client configuration address initiate
   client configuration address respond
   virtual-template 1
!
crypto ipsec transform-set aes-sha esp-aes esp-sha-hmac
!
crypto ipsec profile default
 set ikev2-profile default
!
crypto ipsec profile legacy-profile
 set transform-set aes-sha
!
crypto dynamic-map client-dynamic-map 1
 set transform-set aes-sha
 reverse-route
!
crypto map client-map 1 ipsec-isakmp dynamic client-dynamic-map
!
interface Ethernet0/0
 description WAN
 ip address 192.168.1.10 255.255.255.0
!
interface Ethernet1/0
 description LAN
 ip address 172.16.0.1 255.255.255.0
!
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet1/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile legacy-profile
!
interface Virtual-Template2 type tunnel
 ip unnumbered Ethernet1/0
 tunnel protection ipsec profile default
!
ip local pool Group-One-Pool 10.1.1.100 10.1.1.200
ip local pool flexvpn-pool 10.1.1.201 10.1.1.250
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1
!
ip access-list extended split-tunnel-acl
 remark EzVPN split tunnel ACL
 permit ip 172.16.0.0 0.0.0.255 any
!
access-list 1 permit 172.16.0.0 0.0.0.255
```

تكوين عميل IKEv1 EzVPN الكامل

```
hostname Client1
!
crypto ipsec client ezvpn legacy-client
 connect manual
 group Group-One key cisco123
 mode network-extension
 peer 192.168.1.10
 username client1 password client1
 xauth userid mode local
!
interface Ethernet0/0
 description WAN
 ip address 192.168.2.101 255.255.255.0
 crypto ipsec client ezvpn legacy-client
!
interface Ethernet1/0
 description LAN
 ip address 172.16.1.1 255.255.255.0
 crypto ipsec client ezvpn legacy-client inside
!
ip route 0.0.0.0 0.0.0.0 192.168.2.1
```

تکوین عمیل IKEv2 FlexVPN کامل

```
hostname Client2
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization network default local
!
!
no ip domain lookup
ip domain name cisco.com
ip host ca-server 192.168.2.1
!
crypto pki trustpoint flex-trustpoint
 redundancy
 enrollment url http://ca-server:80
 serial-number
 ip-address none
 fingerprint 08CBB1E948A6D9571965B5EE58FBB726
 subject-name cn=Client2.cisco.com, OU=Flex, O=cisco
 revocation-check crl
 rsakeypair flex-key-pair 1024
!
!
crypto pki certificate chain flex-trustpoint
 certificate 06
 certificate ca 01
!
!
crypto ikev2 authorization policy default
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Client2.cisco.com
```

```
 authentication remote rsa-sig
 authentication local rsa-sig
pki trustpoint flex-trustpoint
aaa authorization group cert list default default
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel destination 192.168.1.10
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 description WAN
 ip address 192.168.2.102 255.255.255.0
!
interface Ethernet1/0
 description LAN
 ip address 172.16.2.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.2.1
!
access-list 1 permit 172.16.2.0 0.0.0.255
```

التحقق من التكوين

فيما يلي بعض الأوامر المستخدمة للتحقق من عمليات EzVPN/FlexVPN على موجه:

```
show crypto session

show crypto session detail

show crypto isakmp sa

show crypto ikev2 sa

show crypto ipsec sa detail

(show crypto ipsec client ez (for legacy clients

show crypto socket

show crypto map
```

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).