الترحيل من مثال تكوين EZvpn القديم إلى EzVPN المحسن

المحتويات

المقدمة

يصف هذا وثيقة كيف أن يشكل VPN سهل (EzVPN) حيث يتحدث 1 يستعمل يحسن EZvpn in order to ربطت إلى الصرة، بينما يتحدث 2 يستعمل القديم EzVPN in order to ربطت إلى ال نفسه صرة. تم تكوين الصرة ل EzVPN المحسن. يكمن الفرق بين شبكة EzVPN المحسنة وشبكة EzVPN القديمة في إستخدام واجهات النفق الظاهرية الديناميكية (dVTIs) في الأولى وخرائط التشفير في الأخيرة. Cisco dVTI طريقة يمكن إستخدامها من قبل العملاء مع Cisco EzVPN لكل من الخادم والتكوين عن بعد. توفر الأنفاق واجهة وصول افتراضية منفصلة حسب الطلب لكل اتصال EZvpn. يتم نسخ تكوين واجهات الوصول الظاهرية من تكوين قالب ظاهري، يتضمن تكوين IPsec وأي ميزة برنامج Cisco IOS®التي تم تكوينها على واجهة القالب الظاهري، مثل QoS أو NetFlow أو قوائم التحكم في الوصول (ACLs).

باستخدام بروتوكولات IPsec dVTIs و Cisco EzVPN، يمكن للمستخدمين توفير اتصال آمن للغاية لشبكات VPN الخاصة بالوصول عن بعد التي يمكن دمجها مع Cisco AVVID (بنية الصوت والفيديو والبيانات المدمجة) لتوفير الصوت والفيديو والبيانات المتقاربة عبر شبكات IP.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة من EzVPN.

المكونات المستخدمة

أسست المعلومة في هذا وثيقة على cisco ios صيغة 15.4(2)T.

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.

معلومات أساسية

يوفر Cisco EzVPN مع تكوين dVTI واجهة قابلة للتوجيه لإرسال حركة مرور البيانات بشكل انتقائي إلى وجهات مختلفة، مثل مركز EzVPN، أو نظير مختلف من موقع إلى موقع، أو الإنترنت. لا يتطلب تكوين IPsec dVTI تعيين ثابت لجلسات عمل IPsec إلى واجهة مادية. وهذا يسمح للمرونة بإرسال حركة مرور مشفرة واستقبالها على أي واجهة مادية، مثل حالة المسارات المتعددة. يتم تشفير حركة مرور البيانات عند إعادة توجيهها من واجهة النفق أو إليها.

تتم إعادة توجيه حركة المرور إلى واجهة النفق أو منها بموجب جدول توجيه IP. يتم التعرف بشكل ديناميكي على المسارات أثناء تكوين وضع تبادل مفتاح الإنترنت (IKE) ويتم إدراجها في جدول التوجيه الذي يشير إلى dVTI. يمكن إستخدام توجيه IP الديناميكي لنشر المسارات عبر شبكة VPN. يؤدي إستخدام توجيه IP لإعادة توجيه حركة مرور البيانات إلى التشفير إلى تبسيط تكوين VPN ل IPsec عند مقارنته باستخدام قوائم التحكم في الوصول مع خريطة التشفير في تكوين IPsec الأصلي.

في الإصدارات الأقدم من الإصدار 12.4(2)T من Cisco IOS، في انتقال النفق لأعلى/النفق لأسفل، كان يجب تحليل السمات التي تم دفعها أثناء تكوين الوضع وتطبيقها. عندما نتج عن هذه السمات تطبيق التكوينات على الواجهة، تعين تجاوز التكوين الموجود. باستخدام ميزة دعم تقنية dVTI، يمكن تطبيق تكوين النفق لأعلى على الواجهات المنفصلة، مما يجعل من السهل دعم ميزات منفصلة في وقت النفق. يمكن فصل الميزات التي يتم تطبيقها على حركة المرور

(قبل التشفير) التي تنتقل إلى النفق عن الميزات التي يتم تطبيقها على حركة المرور التي لا تمر عبر النفق (على سبيل المثال، حركة مرور النفق المنقسم وحركة المرور التي تترك الجهاز عندما لا يكون النفق قيد التشغيل).

عندما يكون تفاوض EzVPN ناجحا، يتم تغيير حالة بروتوكول الخط لواجهة الوصول الظاهري إلى up. عند تعطل نفق EzVPN بسبب انتهاء صلاحية اقتران الأمان أو حذفه، تتغير حالة بروتوكول الخط لواجهة الوصول الظاهري إلى أسفل.

تعمل جداول التوجيه كمحددين لحركة مرور البيانات في تكوين واجهة افتراضية ل EzVPN - أي، أن تستبدل المسارات قائمة الوصول على خريطة التشفير. في تكوين واجهة افتراضية، يقوم EzVPN بالتفاوض على اقتران أمان IPsec واحد إذا تم تكوين خادم EzVPN باستخدام dVTI ل IPsec. يتم إنشاء اقتران الأمان الأحادي هذا بغض النظر عن وضع EzVPN الذي تم تكوينه.

بعد إنشاء اقتران الأمان، تتم إضافة الموجهات التي تشير إلى واجهة الوصول الظاهرية إلى حركة المرور المباشرة إلى شبكة الشركة. كما تضيف EzVPN مسارا إلى مركز VPN حتى يتم توجيه الحزم التي تغلف IPsec إلى شبكة الشركة. تتم إضافة المسار الافتراضي الذي يشير إلى واجهة الوصول الظاهري في حالة وضع عدم التقسيم. عندما "يدفع" خادم EzVPN النفق المقسم، تصبح الشبكة الفرعية للنفق المقسم الوجهة التي تتم إضافة المسارات التي تشير إلى الوصول الظاهري إليها. وفي كلتا الحالتين، إذا لم يكن النظير (مركز VPN) متصلا مباشرة، فإن EzVPN يضيف مسارا إلى النظير.

ملاحظة: تشتمل معظم الموجهات التي تشغل برنامج عميل Cisco EzVPN على مسار افتراضي تم تكوينه. يجب أن يحتوي المسار الافتراضي الذي تم تكوينه على قيمة مترية أكبر من 1 نظرا لأن EzVPN يضيف مسارا افتراضيا يحتوي على قيمة مترية مقدارها 1. يشير المسار إلى واجهة الوصول الظاهرية حتى يتم توجيه حركة مرور البيانات بالكامل إلى شبكة الشركة عندما لا يقوم مركز التركيز "بدفع" سمة النفق المقسم.

يمكن إستخدام جودة الخدمة (QoS) لتحسين أداء التطبيقات المختلفة عبر الشبكة. في هذا التكوين، يتم إستخدام تنظيم حركة مرور البيانات بين الموقعين للحد من المبلغ الإجمالي لحركة مرور البيانات التي يجب إرسالها بين المواقع. وبالإضافة إلى ذلك، يمكن لتكوين جودة الخدمة دعم أي مزيج من ميزات جودة الخدمة المقدمة في برنامج Cisco IOS، لدعم أي من تطبيقات الصوت أو الفيديو أو البيانات.

ملاحظة: مخصص تكوين جودة الخدمة في هذا الدليل للعرض فقط. من المتوقع أن تكون نتائج قابلية توسع VTI مماثلة لتضمين التوجيه العام (GRE) من نقطة إلى نقطة (P2P) عبر IPsec. لاعتبارات القياس والأداء، اتصل بممثل Cisco الخاص بك. للحصول على معلومات إضافية، راجع تكوين واجهة نفق ظاهري باستخدام أمان IP.

الفوائد

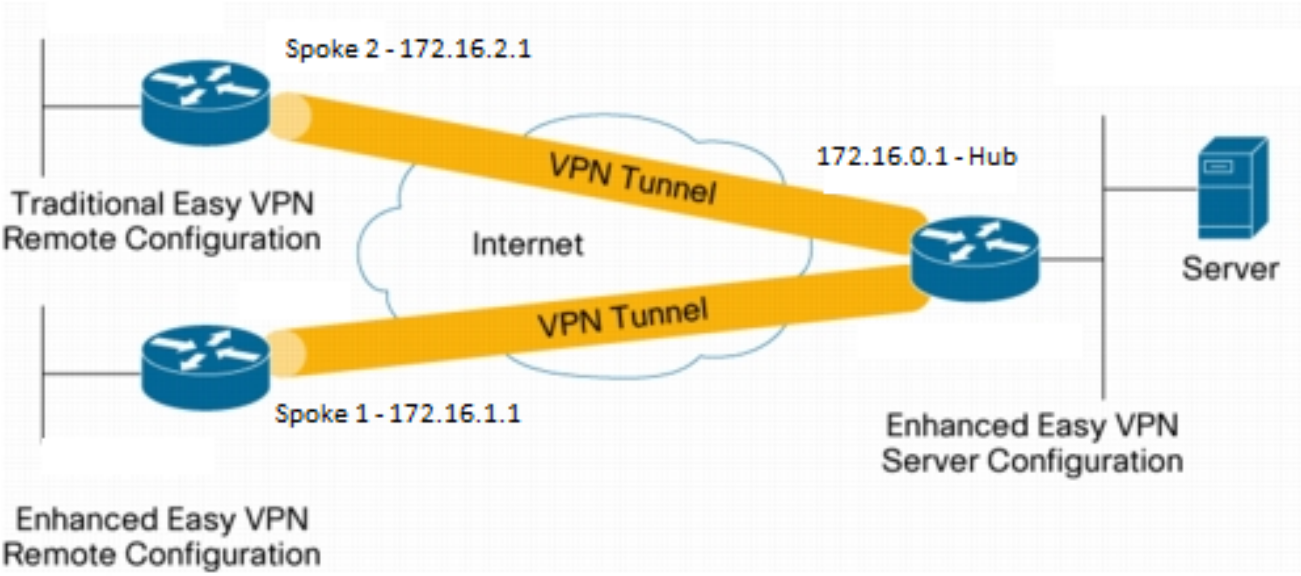
- **تعمل على تبسيط الإدارة**
يمكن للعملاء إستخدام القالب الظاهري Cisco IOS لنسخ واجهات الوصول الافتراضية الجديدة ل IPsec، عند الطلب، والتي تعمل على تبسيط تعقيد تكوين VPN وترجمتها إلى تكاليف أقل. وبالإضافة إلى ذلك، يمكن لتطبيقات الإدارة الحالية مراقبة الواجهات المنفصلة لمختلف المواقع لأغراض الرصد.
- **يوفر واجهة قابلة للتوجيه**
يمكن ل Cisco IPsec VTIs دعم جميع أنواع بروتوكولات توجيه IP. ويمكن للعملاء إستخدام هذه الإمكانات لتوصيل بيئات المكاتب الأكبر حجما، مثل المكاتب الفرعية.
- **يحسن القياس**
تستخدم IPsec VTIs اقترانات أمان فردية لكل موقع، والتي تغطي أنواعا مختلفة من حركة المرور، مما يتيح إمكانية التطوير المحسنة.
- **يوفر المرونة في تحديد الميزات**
VTI ل IPsec هي عملية كبسلة داخل الواجهة الخاصة بها. يوفر هذا مرونة في تحديد ميزات حركة مرور النص

الواضح على VTIs ل IPsec ويحدد ميزات حركة المرور المشفرة على الواجهات المادية.

التكوين

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

الرسم التخطيطي للشبكة



ملخص التكوين

تكوين الموزع

```
hostname Hub
!
no aaa new-model
!
no ip domain lookup
!
username test-user privilege 15 password 0 cisco123
!
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto isakmp client configuration group En-Ezvpn
```

```
 key test-En-Ezvpn
crypto isakmp profile En-EzVpn-Isakmp-Profile
 match identity group En-Ezvpn
 isakmp authorization list default
 client configuration address respond
 virtual-template 1
!
!
crypto ipsec transform-set VPN-TS esp-aes esp-sha-hmac
 mode tunnel
!
crypto ipsec profile En-EzVpn-Ipsec-Profile
 set transform-set VPN-TS
 set isakmp-profile En-EzVpn-Isakmp-Profile
!
!
interface Loopback0
 description Router-ID
 ip address 10.0.0.1 255.255.255.255
!
interface Loopback1
 description inside-network
 ip address 192.168.0.1 255.255.255.255
!
interface Ethernet0/0
 description WAN-Link
 ip address 172.16.0.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile En-EzVpn-Ipsec-Profile
!
router eigrp 1
 network 10.0.0.1 0.0.0.0
 network 192.168.0.1 0.0.0.0
 network 192.168.1.1 0.0.0.0
!
ip route 0.0.0.0 0.0.0.0 172.16.0.100
!
end
```

تحدث 1 (تحسين تكوين EZvpn)

```
hostname Spoke1
!
no aaa new-model
!
interface Loopback0
 description Router-ID
 ip address 10.0.1.1 255.255.255.255
 crypto ipsec client ezvpn En-EzVpn inside
!
interface Loopback1
 description Inside-network
 ip address 192.168.1.1 255.255.255.255
!
interface Ethernet0/0
 description WAN-Link
```

```
 ip address 172.16.1.1 255.255.255.0
 crypto ipsec client ezvpn En-EzVpn
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel mode ipsec ipv4
!
router eigrp 1
 network 10.0.1.1 0.0.0.0
 network 192.168.1.1 0.0.0.0
!
ip route 0.0.0.0 0.0.0.0 172.16.1.100
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto ipsec client ezvpn En-EzVpn
 connect auto
 group En-Ezvpn key test-En-Ezvpn
 mode network-extension
 peer 172.16.0.1
 virtual-interface 1
!
end
```

تحذير: يلزم تعريف القالب الظاهري قبل إدخال تكوين العميل. بدون قالب ظاهري حالي بنفس الرقم، لن يقبل الموجه أمر **الواجهة الظاهرية 1**.

تحدث 2 (Legacy EZvpn) تشكيل

```
hostname Spoke2
!
no aaa new-model
!
no ip domain lookup
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto ipsec client ezvpn Leg-Ezvpn
 connect auto
 group En-Ezvpn key test-En-Ezvpn
 mode network-extension
 peer 172.16.0.1
 xauth userid mode interactive
!
!
interface Loopback0
 ip address 10.0.2.1 255.255.255.255
 crypto ipsec client ezvpn Leg-Ezvpn inside
!
interface Loopback1
 ip address 192.168.2.1 255.255.255.255
```

```
!
interface Ethernet0/0
 ip address 172.16.2.1 255.255.255.0
 crypto ipsec client ezvpn Leg-Ezvpn
!
ip route 0.0.0.0 0.0.0.0 172.16.2.100
!
end
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر **show**.

محور التكلم 1

المرحلة الأولى

```
Hub#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
                  IPv4 Crypto ISAKMP SA

.C-id  Local           Remote          I-VRF  Status Encr Hash   Auth DH Lifetime Cap

   ACTIVE aes  sha    psk  2  23:54:53 C            172.16.2.1      172.16.0.1  1006
                                                Engine-id:Conn-id =  SW:6

   ACTIVE aes  sha    psk  2  23:02:14 C            172.16.1.1      172.16.0.1  1005
                                                Engine-id:Conn-id =  SW:5

                  IPv6 Crypto ISAKMP SA
```

المرحلة الثانية

الوكلاء هنا هم لأي/أي مما يعني أن أي حركة مرور تخرج Virtual Access 1 سيتم تشفيرها وإرسالها إلى 172.16.1.1.

```
Hub#show crypto ipsec sa peer 172.16.1.1 detail

interface: Virtual-Access1
Crypto map tag: Virtual-Access1-head-0, local addr 172.16.0.1

(protected vrf: (none
(local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
(remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
current_peer 172.16.1.1 port 500
{,PERMIT, flags={origin_is_acl
```

```
                pkts encaps: 776, #pkts encrypt: 776, #pkts digest: 776#
                pkts decaps: 771, #pkts decrypt: 771, #pkts verify: 771#
                            pkts compressed: 0, #pkts decompressed: 0#
                        pkts not compressed: 0, #pkts compr. failed: 0#
                    pkts not decompressed: 0, #pkts decompress failed: 0#
                            pkts no sa (send) 0, #pkts invalid sa (rcv) 0#
                pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0#
                      pkts invalid prot (recv) 0, #pkts verify failed: 0#
                pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0#
            pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0#
                                        pkts replay failed (rcv): 0##
                            pkts tagged (send): 0, #pkts untagged (rcv): 0#
                    pkts not tagged (send): 0, #pkts not untagged (rcv): 0#
                pkts internal err (send): 0, #pkts internal err (recv) 0#

         local crypto endpt.: 172.16.0.1, remote crypto endpt.: 172.16.1.1
      plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
                                (current outbound spi: 0x9159A91E(2438572318
                                        PFS (Y/N): N, DH group: none

                                                          :inbound esp sas
                                                 (spi: 0xB82853D4(3089650644
                                        , transform: esp-aes esp-sha-hmac
                                              { ,in use settings ={Tunnel
    :conn id: 13, flow_id: SW:13, sibling_flags 80000040, crypto map
                                                    Virtual-Access1-head-0
            (sa timing: remaining key lifetime (k/sec): (4342983/3529
                                                  IV size: 16 bytes
                                            replay detection support: Y
                                                 (Status: ACTIVE(ACTIVE

                                                           :inbound ah sas

                                                          :inbound pcp sas

                                                         :outbound esp sas
                                                 (spi: 0x9159A91E(2438572318
                                        , transform: esp-aes esp-sha-hmac
                                              { ,in use settings ={Tunnel
    :conn id: 14, flow_id: SW:14, sibling_flags 80000040, crypto map
                                                    Virtual-Access1-head-0
            (sa timing: remaining key lifetime (k/sec): (4342983/3529
                                                  IV size: 16 bytes
                                            replay detection support: Y
                                                 (Status: ACTIVE(ACTIVE

                                                           :outbound ah sas

                                                          :outbound pcp sas
```

EIGRP

```
                                                    Hub#show ip eigrp neighbors
                                                  (EIGRP-IPv4 Neighbors for AS(1
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
 sec)         (ms)       Cnt Num)
  Vi1                        13 00:59:28   31  1398  0  3             172.16.1.1   0
```

ملاحظة: لا يشكل الكلام 2 إدخالا نظرا لأنه من غير الممكن تكوين نظير بروتوكول توجيه العبارة الداخلي المحسن (EIGRP) بدون واجهة قابلة للتوجيه. هذه إحدى مميزات إستخدام VTIs في الكلام.

حادثتم 1

المرحلة الأولى

```
Spoke1#show cry is sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal
T - cTCP encapsulation, X - IKE Extended Authentication
psk - Preshared key, rsig - RSA signature
renc - RSA encryption
IPv4 Crypto ISAKMP SA

.C-id  Local           Remote          I-VRF  Status Encr Hash   Auth DH Lifetime Cap

   ACTIVE aes  sha    psk  2  22:57:07 C            172.16.0.1      172.16.1.1  1005
Engine-id:Conn-id =  SW:5

IPv6 Crypto ISAKMP SA
```

المرحلة الثانية

```
Spoke1#show crypto ipsec sa detail

interface: Virtual-Access1
Crypto map tag: Virtual-Access1-head-0, local addr 172.16.1.1

(protected vrf: (none
(local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
(remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
current_peer 172.16.0.1 port 500
{,PERMIT, flags={origin_is_acl
pkts encaps: 821, #pkts encrypt: 821, #pkts digest: 821#
pkts decaps: 826, #pkts decrypt: 826, #pkts verify: 826#
pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 0, #pkts compr. failed: 0#
pkts not decompressed: 0, #pkts decompress failed: 0#
pkts no sa (send) 0, #pkts invalid sa (rcv) 0#
pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0#
pkts invalid prot (recv) 0, #pkts verify failed: 0#
pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0#
pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0#
pkts replay failed (rcv): 0##
pkts tagged (send): 0, #pkts untagged (rcv): 0#
pkts not tagged (send): 0, #pkts not untagged (rcv): 0#
pkts internal err (send): 0, #pkts internal err (recv) 0#

local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.0.1
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
(current outbound spi: 0xB82853D4(3089650644
PFS (Y/N): N, DH group: none

:inbound esp sas
(spi: 0x9159A91E(2438572318
, transform: esp-aes esp-sha-hmac
{ ,in use settings ={Tunnel
:conn id: 11, flow_id: SW:11, sibling_flags 80004040, crypto map
Virtual-Access1-head-0
```

```
(sa timing: remaining key lifetime (k/sec): (4354968/3290
                                                IV size: 16 bytes
                                        replay detection support: Y
                                             (Status: ACTIVE(ACTIVE

                                                      :inbound ah sas

                                                     :inbound pcp sas

                                                    :outbound esp sas
                                               (spi: 0xB82853D4(3089650644
                                      , transform: esp-aes esp-sha-hmac
                                           { ,in use settings ={Tunnel
:conn id: 12, flow_id: SW:12, sibling_flags 80004040, crypto map
                                                    Virtual-Access1-head-0
(sa timing: remaining key lifetime (k/sec): (4354968/3290
                                                IV size: 16 bytes
                                        replay detection support: Y
                                             (Status: ACTIVE(ACTIVE

                                                      :outbound ah sas

                                                     :outbound pcp sas
```

EzVPN

```
Spoke1#show crypto ipsec client ezvpn
Easy VPN Remote Phase: 8

                                        Tunnel name : En-EzVpn
                                    Inside interface list: Loopback0
(Outside interface: Virtual-Access1 (bound to Ethernet0/0
                                    Current State: IPSEC_ACTIVE
                                         Last Event: SOCKET_UP
                                    Save Password: Disallowed
                                Current EzVPN Peer: 172.16.0.1
```

التوجيه - EIGRP

في 2 Talk تكون الوكلاء على درجة أن أي حركة مرور تخرج واجهة الوصول الظاهرية سيتم تشفيرها. طالما هناك مسار يشير إلى واجهة شبكة، فسيتم تشفير حركة مرور البيانات:

```
Spoke1#ping 192.168.0.1 source loopback 1
                                        .Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds
                                Packet sent with a source address of 192.168.1.1
                                                                        !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/6 ms

                                Spoke1#ping 192.168.0.1 source loopback 0
                                        .Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds
                                Packet sent with a source address of 10.0.1.1
                                                                        !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms

                                                        Spoke1# sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
                D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
                N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
                        E1 - OSPF external type 1, E2 - OSPF external type 2
          i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
            o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
                                                    a - application route
                                  replicated route, % - next hop override - +

                          Gateway of last resort is 172.16.1.100 to network 0.0.0.0

                                                S*    0.0.0.0/0 [1/0] via 172.16.1.100
                                    via 0.0.0.0, Virtual-Access1 [1/0]
                                                  is subnetted, 2 subnets 10.0.0.0/32
          D        10.0.0.1 [90/27008000] via 10.0.0.1, 01:16:15, Virtual-Access1
                                       C        10.0.1.1 is directly connected, Loopback0
                        is variably subnetted, 3 subnets, 2 masks 172.16.0.0/16
                                          S        172.16.0.1/32 [1/0] via 172.16.1.100
                             C        172.16.1.0/24 is directly connected, Ethernet0/0
                             L        172.16.1.1/32 is directly connected, Ethernet0/0
                                           is subnetted, 1 subnets 192.168.0.0/32
        D        192.168.0.1 [90/27008000] via 10.0.0.1, 01:16:15, Virtual-Access1
                                    is subnetted, 1 subnets 192.168.1.0/32
                                C        192.168.1.1 is directly connected, Loopback1
                                                                        Spoke1#
```

محور التخاطب 2 النفق

المرحلة الأولى

```
                                                                Hub#show crypto isakmp sa det
                                        Codes: C - IKE configuration mode, D - Dead Peer Detection
                                                        K - Keepalives, N - NAT-traversal
                                    T - cTCP encapsulation, X - IKE Extended Authentication
                                                    psk - Preshared key, rsig - RSA signature
                                                                renc - RSA encryption
                                                                      IPv4 Crypto ISAKMP SA

.C-id  Local           Remote          I-VRF  Status Encr Hash   Auth DH Lifetime Cap

   ACTIVE aes  sha    psk  2  23:54:53 C            172.16.2.1      172.16.0.1  1006
                                                     Engine-id:Conn-id =  SW:6

   ACTIVE aes  sha    psk  2  23:02:14 C            172.16.1.1      172.16.0.1  1005
                                                     Engine-id:Conn-id =  SW:5

                                                                      IPv6 Crypto ISAKMP SA
```

المرحلة الثانية

لا يتم إستخدام قائمة التحكم في الوصول (ACL) للنفق المنقسم ضمن تكوين العميل على الموزع في هذا المثال. لذلك تكون الوكلاء الذين يتم تكوينهم على الشبكة ذات الإتجاه الخاص ب EzVPN "داخلي" على الشبكة التي يتم التحدث بها إلى أي شبكة. أساسا، على لوحة الوصل، أي حركة مرور موجهة إلى واحدة من الشبكات "الداخلية" على ال يتحدث سيتم تشفيرها وإرسالها إلى 172.16.2.1.

```
Hub#show crypto ipsec sa  peer 172.16.2.1 detail
```

```
                                                interface: Virtual-Access2
        Crypto map tag: Virtual-Access2-head-0, local addr 172.16.0.1

                                                (protected vrf: (none
              (local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
          (remote ident (addr/mask/prot/port): (10.0.2.1/255.255.255.255/0/0
                                        current_peer 172.16.2.1 port 500
                                         {,PERMIT, flags={origin_is_acl
                    pkts encaps: 15, #pkts encrypt: 15, #pkts digest: 15#
                    pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15#
                               pkts compressed: 0, #pkts decompressed: 0#
                          pkts not compressed: 0, #pkts compr. failed: 0#
                    pkts not decompressed: 0, #pkts decompress failed: 0#
                           pkts no sa (send) 0, #pkts invalid sa (rcv) 0#
                pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0#
                      pkts invalid prot (recv) 0, #pkts verify failed: 0#
             pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0#
          pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0#
                                         pkts replay failed (rcv): 0##
                              pkts tagged (send): 0, #pkts untagged (rcv): 0#
                       pkts not tagged (send): 0, #pkts not untagged (rcv): 0#
                    pkts internal err (send): 0, #pkts internal err (recv) 0#

         local crypto endpt.: 172.16.0.1, remote crypto endpt.: 172.16.2.1
      plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
                                  (current outbound spi: 0x166CAC10(376220688
                                               PFS (Y/N): N, DH group: none

                                                         :inbound esp sas
                                                  (spi: 0x8525868A(2233829002
                                       , transform: esp-aes esp-sha-hmac
                                                  { ,in use settings ={Tunnel
       :conn id: 11, flow_id: SW:11, sibling_flags 80000040, crypto map
                                                        Virtual-Access2-head-0
              (sa timing: remaining key lifetime (k/sec): (4217845/1850
                                                      IV size: 16 bytes
                                           replay detection support: Y
                                                (Status: ACTIVE(ACTIVE

                                                          :inbound ah sas

                                                         :inbound pcp sas

                                                        :outbound esp sas
                                                   (spi: 0x166CAC10(376220688
                                       , transform: esp-aes esp-sha-hmac
                                                  { ,in use settings ={Tunnel
       :conn id: 12, flow_id: SW:12, sibling_flags 80000040, crypto map
                                                        Virtual-Access2-head-0
              (sa timing: remaining key lifetime (k/sec): (4217845/1850
                                                      IV size: 16 bytes
                                           replay detection support: Y
                                                (Status: ACTIVE(ACTIVE

                                                          :outbound ah sas

                                                         :outbound pcp sas
```

نطق 2

المرحلة الأولى

```
Spoke2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
QM_IDLE           1001 ACTIVE      172.16.2.1      172.16.0.1

IPv6 Crypto ISAKMP SA
```

المرحلة الثانية

```
Spoke2#show crypto ipsec sa detail

interface: Ethernet0/0
    Crypto map tag: Ethernet0/0-head-0, local addr 172.16.2.1

(protected vrf: (none
  (local  ident (addr/mask/prot/port): (10.0.2.1/255.255.255.255/0/0
  (remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
current_peer 172.16.0.1 port 500
{,PERMIT, flags={origin_is_acl
  pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5#
  pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5#
  pkts compressed: 0, #pkts decompressed: 0#
  pkts not compressed: 0, #pkts compr. failed: 0#
  pkts not decompressed: 0, #pkts decompress failed: 0#
  pkts no sa (send) 0, #pkts invalid sa (rcv) 0#
  pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0#
  pkts invalid prot (recv) 0, #pkts verify failed: 0#
  pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0#
  pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0#
  pkts replay failed (rcv): 0##
  pkts tagged (send): 0, #pkts untagged (rcv): 0#
  pkts not tagged (send): 0, #pkts not untagged (rcv): 0#
  pkts internal err (send): 0, #pkts internal err (recv) 0#

    local crypto endpt.: 172.16.2.1, remote crypto endpt.: 172.16.0.1
  plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
(current outbound spi: 0x8525868A(2233829002
PFS (Y/N): N, DH group: none

:inbound esp sas
(spi: 0x166CAC10(376220688
, transform: esp-aes esp-sha-hmac
{ ,in use settings ={Tunnel
:conn id: 1, flow_id: SW:1, sibling_flags 80004040, crypto map
Ethernet0/0-head-0
(sa timing: remaining key lifetime (k/sec): (4336232/2830
IV size: 16 bytes
replay detection support: Y
(Status: ACTIVE(ACTIVE

:inbound ah sas

:inbound pcp sas

:outbound esp sas
(spi: 0x8525868A(2233829002
, transform: esp-aes esp-sha-hmac
```

```
{ ,in use settings ={Tunnel
:conn id: 2, flow_id: SW:2, sibling_flags 80004040, crypto map
                                                Ethernet0/0-head-0
(sa timing: remaining key lifetime (k/sec): (4336232/2830
                                                IV size: 16 bytes
                                        replay detection support: Y
                                             (Status: ACTIVE(ACTIVE

                                                :outbound ah sas

                                               :outbound pcp sas
```

EzVPN

```
Spoke2#show crypto ipsec client ezvpn
Easy VPN Remote Phase: 8

Tunnel name : Leg-Ezvpn
Inside interface list: Loopback0
Outside interface: Ethernet0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Save Password: Disallowed
Current EzVPN Peer: 172.16.0.1
```

التوجيه - ثابت

بخلاف Talk 1، يجب أن يكون للمحادثة 2 مسارات ثابتة أو إستخدام حقن المسار العكسي (RRI) لحقن المسارات لإعلام حركة المرور التي يجب تشفيرها وما لا يجب تشفيرها. في هذا المثال، يتم تشفير حركة المرور التي يتم الحصول عليها من Loopback 0 فقط وفقا للوكيل والتوجيه.

```
Spoke2#ping 192.168.0.1 source loopback 1
.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds
Packet sent with a source address of 192.168.2.1
.....
(Success rate is 0 percent (0/5

Spoke2#ping 192.168.0.1 source loopback 0
.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds
Packet sent with a source address of 10.0.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/7 ms

Spoke2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
a - application route
+ - replicated route, % - next hop override

Gateway of last resort is 172.16.2.100 to network 0.0.0.0
```

```
S*    0.0.0.0/0 [1/0] via 172.16.2.100
                  is subnetted, 1 subnets 10.0.0.0/32
C        10.0.2.1 is directly connected, Loopback0
is variably subnetted, 2 subnets, 2 masks 172.16.0.0/16
C        172.16.2.0/24 is directly connected, Ethernet0/0
L        172.16.2.1/32 is directly connected, Ethernet0/0
                  is subnetted, 1 subnets 192.168.2.0/32
C        192.168.2.1 is directly connected, Loopback1
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

تلميح: غالبا ما لا تظهر الأنفاق في EzVPN بعد تغييرات التكوين. لن تعمل المرحلة الأولى والمرحلة الثانية من التطهير على زيادة الأنفاق في هذه الحالة. في معظم الحالات، أدخل الأمر **clear crypto ipSec client ezVPN <group-name>** في **المقطع** لإظهار النفق.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

أوامر الموجهات

- **debug crypto ipSec** - يعرض مفاوضات IPsec للمرحلة 2.
- **debug crypto isakmp** - يعرض مفاوضات ISAKMP للمرحلة 1.

الأوامر التي تم التحدث عنها

- **debug crypto ipSec** - يعرض مفاوضات IPsec للمرحلة 2.
- **debug crypto isakmp** - يعرض مفاوضات ISAKMP للمرحلة 1.
- **debug crypto ipSec client ezVPN** - يعرض تصحيح أخطاء EzVPN.

معلومات ذات صلة

- صفحة دعم IPsec
- جهاز تحكم VPN سهل من Cisco
- خادم سهل للشبكة الخاصة الظاهرية (VPN)
- واجهة النفق الظاهري IPsec
- تكوين أمان شبكة IPsec
- تكوين بروتوكول أمان Internet Key Exchange
- 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).