تكوين IPSec باستخدام EIGRP و IPX باستخدام اتصال GRE النفقي

المحتويات

المقدمة

لا يمكن لتكوينات IPSec العادية نقل بروتوكولات التوجيه مثل بروتوكول توجيه العبارة الداخلي المحسن (EIGRP) وفتح أقصر مسار أولا (OSPF) أو حركة مرور غير خاصة ب IP مثل تبادل حزم الشبكة البينية (IPX) و AppleTalk وما إلى ذلك. يوضح هذا المستند كيفية التوجيه بين الشبكات المختلفة باستخدام بروتوكول توجيه وحركة مرور غير خاصة ب IP باستخدام IPSec. يستخدم هذا الأسلوب تضمين التوجيه العام (GRE) كطريقة لتحقيق ذلك.

المتطلبات الأساسية

المتطلبات

قبل أن تحاول إجراء هذا التكوين، فتأكد من استيفاء المتطلبات التالية:

- تأكد من عمل النفق قبل تطبيق خرائط التشفير.
- يجب أن تحتوي قائمة وصول التشفير على GRE كبروتوكول للسماح: access-list 101 allowed gre host <tunnel_source> y.y.y = <tunnel_destination> x.x.x.x host y.y.y x.x
- أستخدم عناوين IP الاسترجاع لتحديد نظائر مفتاح الإنترنت (IKE) ومصدر النفق ووجهة النفق لتحسين التوفر.
- لمناقشة المشكلات المحتملة المتعلقة بوحدة الإرسال القصوى (MTU)، ارجع إلى ضبط IP MTU و TCP MSS و PMTUD على Windows و Sun Systems.

المكونات المستخدمة

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

- برنامج IOS® الإصدارات 12.1.8 و 12.2.1 من Cisco

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

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

التكوين

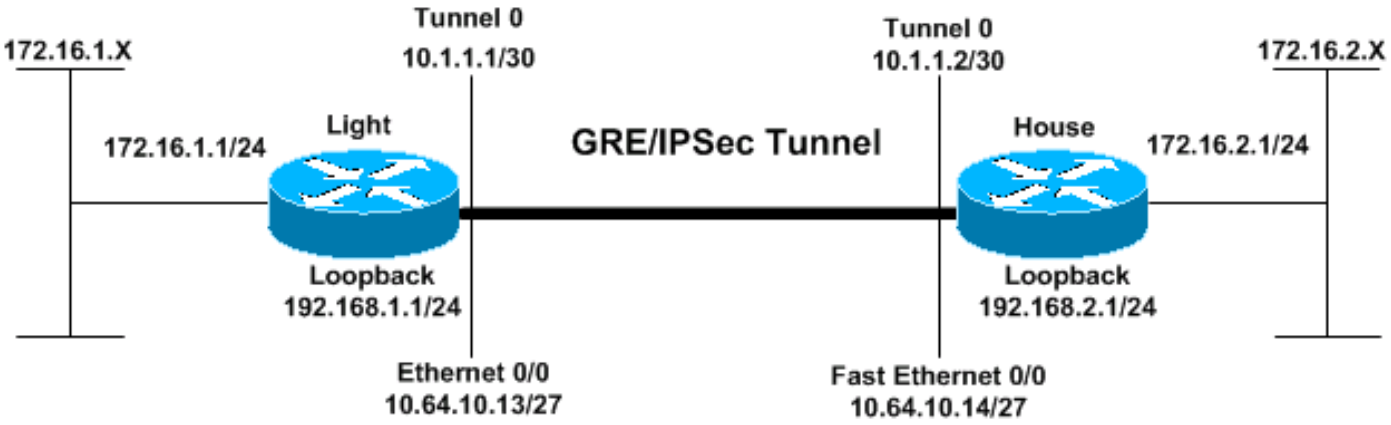
في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط).

ملاحظة تكوين IOS: باستخدام برنامج Cisco IOS الإصدار 12.2T(13) والرموز الأحدث (رموز t-train الأعلى ترقما، وبرنامج Cisco IOS Software الإصدار 12.3 والرموز الأحدث) لا يلزم تطبيق "خريطة التشفير" ل IPSec التي تم تكوينها إلا على الواجهة المادية. لم يعد مطلوبا لتطبيقه على واجهة نفق GRE. لا يزال وجود "خريطة التشفير" على الواجهة المادية وواجهة النفق عند إستخدام برنامج Cisco IOS الإصدار 12.2.1T(13) والرموز الأحدث يعمل. ومع ذلك، يوصى بشدة بتطبيقه فقط على الواجهة المادية.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في هذا الرسم التخطيطي.



التكوينات

- ضوء
- بيت

ضوء

```
:Current configuration
!
version 12.2
```

```
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Light
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
!
no ip finger
!
no ip dhcp-client network-discovery
ipx routing 00e0.b06a.40fc
!
IKE policies. crypto isakmp policy 25 ---!
hash md5
authentication pre-share
crypto isakmp key cisco123 address 192.168.2.1
!
IPSec policies. crypto ipsec transform-set WWW esp- ---!
des esp-md5-hmac
mode transport
!
crypto map GRE local-address Loopback0
crypto map GRE 50 ipsec-isakmp
set peer 192.168.2.1
set transform-set WWW
What to encrypt? match address 101 ---!
!
call rsvp-sync
!
fax interface-type modem
mta receive maximum-recipients 0
!
interface Loopback0
ip address 192.168.1.1 255.255.255.0
!
interface Tunnel0
ip address 10.1.1.1 255.255.255.252
ip mtu 1440
ipx network CC
tunnel source Loopback0
tunnel destination 192.168.2.1
crypto map GRE
!
interface FastEthernet0/0
ip address 10.64.10.13 255.255.255.224
no ip route-cache
no ip mroute-cache
duplex auto
speed auto
crypto map GRE
!
interface FastEthernet0/1
ip address 172.16.1.1 255.255.255.0
duplex auto
speed auto
ipx network AA
!
router eigrp 10
network 10.1.1.0 0.0.0.3
```

```
network 172.16.1.0 0.0.0.255
network 192.168.1.0
no auto-summary
no eigrp log-neighbor-changes
!
ip kerberos source-interface any
ip classless
ip route 192.168.2.0 255.255.255.0 10.64.10.14
ip http server
!
What to encrypt? access-list 101 permit gre host ---!
192.168.1.1 host 192.168.2.1
!
dial-peer cor custom
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end

!#Light
```

بيت

```
:Current configuration
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname House
!
ip subnet-zero
!
ipx routing 00e0.b06a.4114
!
IKE policies. crypto isakmp policy 25 ---!
hash md5
authentication pre-share
crypto isakmp key cisco123 address 192.168.1.1
!
IPSec policies. crypto ipsec transform-set WWW esp- ---!
des esp-md5-hmac
mode transport
!
crypto map GRE local-address Loopback0
crypto map GRE 50 ipsec-isakmp
set peer 192.168.1.1
set transform-set WWW
What to encrypt? match address 101 ---!
!
!
interface Loopback0
ip address 192.168.2.1 255.255.255.0
!
interface Tunnel0
ip address 10.1.1.2 255.255.255.252
ip mtu 1440
ipx network CC
tunnel source Loopback0
```

```
tunnel destination 192.168.1.1
crypto map GRE
!
interface FastEthernet0/0
ip address 10.64.10.14 255.255.255.224
no ip route-cache
no ip mroute-cache
duplex auto
speed auto
crypto map GRE
!
interface FastEthernet0/1
ip address 172.16.2.1 255.255.255.0
duplex auto
speed auto
ipx network BB
!
interface FastEthernet4/0
no ip address
shutdown
duplex auto
speed auto
!
router eigrp 10
network 10.1.1.0 0.0.0.3
network 172.16.2.0 0.0.0.255
network 192.168.2.0
no auto-summary
no eigrp log-neighbor-changes
!
ip classless
ip route 192.168.1.0 255.255.255.0 10.64.10.13
ip http server
What to encrypt? access-list 101 permit gre host ---!
192.168.2.1 host 192.168.1.1
!
line con 0
line aux 0
line vty 0 4
login
!
end

#House
```

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

- **show crypto engine connections active**—يعرض الحزم المشفرة وغير المشفرة بين أقران IPSec.
- **show crypto isakmp sa**—يعرض اقترانات أمان المرحلة 1.
- **show crypto ipSec sa**—يعرض اقترانات أمان المرحلة 2.
- **show ipx route [network] [default] [detail]**—يعرض محتويات جدول توجيه IPX.

إظهار إخراج الأمر مع زيادة الأنفاق

```
Light#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
i - IS-IS, 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

                                Gateway of last resort is not set

                           is subnetted, 2 subnets 172.16.0.0/24
                C       172.16.1.0 is directly connected, FastEthernet0/1
             D       172.16.2.0 [90/297246976] via 10.1.1.2, 00:00:31, Tunnel0
                     is variably subnetted, 2 subnets, 2 masks 10.0.0.0/8
                        C       10.1.1.0/30 is directly connected, Tunnel0
                  C       10.64.10.0/27 is directly connected, FastEthernet0/0
                        C    192.168.1.0/24 is directly connected, Loopback0
                              S    192.168.2.0/24 [1/0] via 10.64.10.14
                                                        Light#ping
                                                    :[Protocol [ip
                                            Target IP address: 172.16.2.1
                                                    :[Repeat count [5
                                                :[Datagram size [100
                                              :[Timeout in seconds [2
                                             Extended commands [n]: y
                                    Source address or interface: 172.16.1.1
                                                    :[Type of service [0
                                          :[Set DF bit in IP header? [no
                                              :[Validate reply data? [no
                                                  :[Data pattern [0xABCD
                                 :[Loose, Strict, Record, Timestamp, Verbose[none
                                                 :[Sweep range of sizes [n
                                          .Type escape sequence to abort
                   :Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds
                                                                    !!!!!
                  Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
                                                                  #Light

                                                        House#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
i - IS-IS, 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

                                Gateway of last resort is not set

                           is subnetted, 2 subnets 172.16.0.0/24
             D       172.16.1.0 [90/297246976] via 10.1.1.1, 00:00:36, Tunnel0
                C       172.16.2.0 is directly connected, FastEthernet0/1
                     is variably subnetted, 2 subnets, 2 masks 10.0.0.0/8
                        C       10.1.1.0/30 is directly connected, Tunnel0
                  C       10.64.10.0/27 is directly connected, FastEthernet0/0
                              S    192.168.1.0/24 [1/0] via 10.64.10.13
                        C    192.168.2.0/24 is directly connected, Loopback0
                                                        House#ping
                                                    :[Protocol [ip
                                            Target IP address: 172.16.1.1
                                                    :[Repeat count [5
```

```
                                                  :[Datagram size [100
                                                :[Timeout in seconds [2
                                               Extended commands [n]: y
                                    Source address or interface: 172.16.2.1
                                                  :[Type of service [0
                                           :[Set DF bit in IP header? [no
                                              :[Validate reply data? [no
                                                 :[Data pattern [0xABCD
                                  :[Loose, Strict, Record, Timestamp, Verbose[none
                                                :[Sweep range of sizes [n
                                              .Type escape sequence to abort
                    :Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds
                                                                      !!!!!
                        Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

                                                  Light#show ipx route
                    Codes: C - Connected primary network,    c - Connected secondary network
                    S - Static, F - Floating static, L - Local (internal), W - IPXWAN
                            R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
                                        s - seconds, u - uses, U - Per-user static

                             .Total IPX routes. Up to 1 parallel paths and 16 hops allowed 3

                                                    .No default route known

                                               C         AA (NOVELL-ETHER),  Fa0/1
                                                 C         CC (TUNNEL),        Tu0
                                  R         BB [151/01] via       CC.00e0.b06a.4114,   17s, Tu0

                                                  House#show ipx route
                    Codes: C - Connected primary network,    c - Connected secondary network
                    S - Static, F - Floating static, L - Local (internal), W - IPXWAN
                            R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
                                        s - seconds, u - uses, U - Per-user static

                             .Total IPX routes. Up to 1 parallel paths and 16 hops allowed 3

                                                    .No default route known

                                               C         BB (NOVELL-ETHER),  Fa0/1
                                                 C         CC (TUNNEL),        Tu0
                                  R         AA [151/01] via       CC.00e0.b06a.40fc,   59s, Tu0

                                               Light#ping ipx BB.0004.9af2.8261

                                                .Type escape sequence to abort
                :Sending 5, 100-byte IPX Novell Echoes to BB.0004.9af2.8261, timeout is 2 second
                                                                      !!!!!
                        Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

                                               House#ping ipx AA.0004.9af2.8181

                                                .Type escape sequence to abort
                :Sending 5, 100-byte IPX Novell Echoes to AA.0004.9af2.8181, timeout is 2 second
                                                                      !!!!!
                        Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

                                                  Light#show crypto isa sa
                              dst           src          state        conn-id   slot
                               QM_IDLE           1       0    192.168.1.1    192.168.2.1
                               QM_IDLE           2       0    192.168.2.1    192.168.1.1

                                                  House#show crypto isa sa
                              dst           src          state        conn-id   slot
```

```
                      QM_IDLE           1       0    192.168.2.1    192.168.1.1
                      QM_IDLE           2       0    192.168.1.1    192.168.2.1
```

Light#**show crypto engine connections active**

```
ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
none>          <none>          set    HMAC_MD5+DES_56_CB        0        0> 1
none>          <none>          set    HMAC_MD5+DES_56_CB        0        0> 2
FastEthernet0/0 10.64.10.13     set    HMAC_MD5+DES_56_CB        0      161 2000
FastEthernet0/0 10.64.10.13     set    HMAC_MD5+DES_56_CB      161        0 2001
FastEthernet0/0 10.64.10.13     set    HMAC_MD5+DES_56_CB        0        0 2002
FastEthernet0/0 10.64.10.13     set    HMAC_MD5+DES_56_CB        0        0 2003
FastEthernet0/0 10.64.10.13     set    HMAC_MD5+DES_56_CB        0        0 2004
FastEthernet0/0 10.64.10.13     set    HMAC_MD5+DES_56_CB        0        0 2005
```

House#**show crypto engine connections active**

```
ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
none>          <none>          set    HMAC_MD5+DES_56_CB        0        0> 1
none>          <none>          set    HMAC_MD5+DES_56_CB        0        0> 2
FastEthernet0/0 10.64.10.14     set    HMAC_MD5+DES_56_CB        0      159 2000
FastEthernet0/0 10.64.10.14     set    HMAC_MD5+DES_56_CB      159        0 2001
FastEthernet0/0 10.64.10.14     set    HMAC_MD5+DES_56_CB        0        0 2002
FastEthernet0/0 10.64.10.14     set    HMAC_MD5+DES_56_CB        0        0 2003
FastEthernet0/0 10.64.10.14     set    HMAC_MD5+DES_56_CB        0        0 2004
FastEthernet0/0 10.64.10.14     set    HMAC_MD5+DES_56_CB        0        0 2005
```

House#**show crypto ipsec sa detail**

```
                                                interface: Tunnel0
                                Crypto map tag: GRE, local addr. 192.168.2.1

      (local  ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/47/0
      (remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/47/0
                                                current_peer: 192.168.1.1
                             {,PERMIT, flags={origin_is_acl,transport_parent
                      pkts encaps: 192, #pkts encrypt: 192, #pkts digest 192#
                      pkts decaps: 190, #pkts decrypt: 190, #pkts verify 190#
                                  pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0#
                               pkts no sa (send) 12, #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 internal err (send): 0, #pkts internal err (recv) 0#

       local crypto endpt.: 192.168.2.1, remote crypto endpt.: 192.168.1.1
                                            path mtu 1514, media mtu 1514
                                          current outbound spi: 1FA721CA

                                                        :inbound esp sas
                                                  (spi: 0xEE52531(249898289
                                       , transform: esp-des esp-md5-hmac
                                          { ,in use settings ={Transport
                     slot: 0, conn id: 2000, flow_id: 1, crypto map: GRE
            (sa timing: remaining key lifetime (k/sec): (4607961/2797
                                                     IV size: 8 bytes
                                            replay detection support: Y
                                                  (spi: 0xFEE24F3(267265267
                                       , transform: esp-des esp-md5-hmac
                                          { ,in use settings ={Transport
```

```
                        slot: 0, conn id: 2002, flow_id: 3, crypto map: GRE
                  (sa timing: remaining key lifetime (k/sec): (4608000/2826
                                                    IV size: 8 bytes
                                          replay detection support: Y
                                             (spi: 0x19240817(421791767
                                    , transform: esp-des esp-md5-hmac
                                       { ,in use settings ={Transport
                        slot: 0, conn id: 2004, flow_id: 5, crypto map: GRE
                  (sa timing: remaining key lifetime (k/sec): (4608000/2759
                                                    IV size: 8 bytes
                                          replay detection support: Y

                                                      :inbound ah sas

                                                     :inbound pcp sas

                                                    :outbound esp sas
                                               (spi: 0x1FA721CA(531046858
                                    , transform: esp-des esp-md5-hmac
                                       { ,in use settings ={Transport
                        slot: 0, conn id: 2001, flow_id: 2, crypto map: GRE
                  (sa timing: remaining key lifetime (k/sec): (4607972/2797
                                                    IV size: 8 bytes
                                          replay detection support: Y
                                             (spi: 0x12B10EB0(313593520
                                    , transform: esp-des esp-md5-hmac
                                       { ,in use settings ={Transport
                        slot: 0, conn id: 2003, flow_id: 4, crypto map: GRE
                  (sa timing: remaining key lifetime (k/sec): (4608000/2826
                                                    IV size: 8 bytes
                                          replay detection support: Y
                                             (spi: 0x1A700242(443548226
                                    , transform: esp-des esp-md5-hmac
                                       { ,in use settings ={Transport
                        slot: 0, conn id: 2005, flow_id: 6, crypto map: GRE
                  (sa timing: remaining key lifetime (k/sec): (4608000/2759
                                                    IV size: 8 bytes
                                          replay detection support: Y

                                                      :outbound ah sas

                                                     :outbound pcp sas


          (local  ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/0/0
          (remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0
                                                  current_peer: 192.168.1.1
                                           {,PERMIT, flags={transport_parent
                               pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0#
                               pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0#
                                     pkts compressed: 0, #pkts decompressed: 0#
  pkts not compressed: 0, #pkts compr. failed: 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 internal err (send): 0, #pkts internal err (recv) 0#

          local crypto endpt.: 192.168.2.1, remote crypto endpt.: 192.168.1.1
                                           path mtu 1514, media mtu 1514
                                                  current outbound spi: 0
```

```
                                                        :inbound esp sas

                                                         :inbound ah sas

                                                        :inbound pcp sas

                                                       :outbound esp sas

                                                        :outbound ah sas

                                                       :outbound pcp sas


                                                  interface: FastEthernet0/0
                                     Crypto map tag: GRE, local addr. 192.168.2.1

            (local  ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/47/0
            (remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/47/0
                                                  current_peer: 192.168.1.1
                                  {,PERMIT, flags={origin_is_acl,transport_parent
                           pkts encaps: 193, #pkts encrypt: 193, #pkts digest 193#
                           pkts decaps: 192, #pkts decrypt: 192, #pkts verify 192#
                                        pkts compressed: 0, #pkts decompressed: 0#
     pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0#
                                  pkts no sa (send) 12, #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 internal err (send): 0, #pkts internal err (recv) 0#

             local crypto endpt.: 192.168.2.1, remote crypto endpt.: 192.168.1.1
                                            path mtu 1514, media mtu 1514
                                          current outbound spi: 1FA721CA

                                                        :inbound esp sas
                                                  (spi: 0xEE52531(249898289
                                       , transform: esp-des esp-md5-hmac
                                          { ,in use settings ={Transport
                            slot: 0, conn id: 2000, flow_id: 1, crypto map: GRE
                     (sa timing: remaining key lifetime (k/sec): (4607961/2789
                                                       IV size: 8 bytes
                                          replay detection support: Y
                                              (spi: 0xFEE24F3(267265267
                                       , transform: esp-des esp-md5-hmac
                                          { ,in use settings ={Transport
                            slot: 0, conn id: 2002, flow_id: 3, crypto map: GRE
                     (sa timing: remaining key lifetime (k/sec): (4608000/2817
                                                       IV size: 8 bytes
                                          replay detection support: Y
                                             (spi: 0x19240817(421791767
                                       , transform: esp-des esp-md5-hmac
                                          { ,in use settings ={Transport
                            slot: 0, conn id: 2004, flow_id: 5, crypto map: GRE
                     (sa timing: remaining key lifetime (k/sec): (4608000/2750
                                                       IV size: 8 bytes
                                          replay detection support: Y

                                                         :inbound ah sas

                                                        :inbound pcp sas
```

```
                                                    :outbound esp sas
                                                (spi: 0x1FA721CA(531046858
                                        , transform: esp-des esp-md5-hmac
                                           { ,in use settings ={Transport
                  slot: 0, conn id: 2001, flow_id: 2, crypto map: GRE
            (sa timing: remaining key lifetime (k/sec): (4607972/2789
                                                    IV size: 8 bytes
                                         replay detection support: Y
                                           (spi: 0x12B10EB0(313593520
                                        , transform: esp-des esp-md5-hmac
                                           { ,in use settings ={Transport
                  slot: 0, conn id: 2003, flow_id: 4, crypto map: GRE
            (sa timing: remaining key lifetime (k/sec): (4608000/2817
                                                    IV size: 8 bytes
                                         replay detection support: Y
                                           (spi: 0x1A700242(443548226
                                        , transform: esp-des esp-md5-hmac
                                           { ,in use settings ={Transport
                  slot: 0, conn id: 2005, flow_id: 6, crypto map: GRE
            (sa timing: remaining key lifetime (k/sec): (4608000/2750
                                                    IV size: 8 bytes
                                         replay detection support: Y

                                                     :outbound ah sas

                                                    :outbound pcp sas


        (local  ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/0/0
        (remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0
                                                 current_peer: 192.168.1.1
                                       {,PERMIT, flags={transport_parent
                            pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0#
                            pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0#
                                    pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 0, #pkts compr. failed: 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 internal err (send): 0, #pkts internal err (recv) 0#

        local crypto endpt.: 192.168.2.1, remote crypto endpt.: 192.168.1.1
                                         path mtu 1514, media mtu 1514
                                         current outbound spi: 0

                                                    :inbound esp sas

                                                     :inbound ah sas

                                                    :inbound pcp sas

                                                   :outbound esp sas

                                                    :outbound ah sas

                                                   :outbound pcp sas
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

ملاحظة: قبل إصدار أوامر **debug**، راجع المعلومات المهمة في أوامر تصحيح الأخطاء.

- **debug crypto isakmp**—يعرض الأخطاء أثناء المرحلة 1.
- **debug crypto ipSec**—يعرض الأخطاء أثناء المرحلة 2.
- **debug crypto engine**—يعرض معلومات من محرك التشفير.
- **debug ip *بروتوكول التوجيه*** —يعرض معلومات حول حركات توجيه بروتوكول التوجيه لديك.
- **معرف اتصال التشفير الواضح *[slot | RSM | vip]*** —ينهي جلسة مشفرة قيد التقدم حاليا. تنتهي عادة جلسات العمل المشفرة عند انتهاء مهلة جلسة العمل. أستخدم الأمر **show crypto cisco connections** لمعرفة قيمة معرف الاتصال.
- مسح **التشفير** isakmp—يعمل على مسح اقترانات أمان المرحلة الأولى.
- **مسح التشفير sa**—يمحو اقترانات أمان المرحلة 2.

معلومات ذات صلة

- صفحة دعم IPSec
- مقدمة عن تشفير أمان IP (IPSec)
- تكوين أمان شبكة IPSec
- تكوين بروتوكول أمان Internet Key Exchange
- أداة بحث الأوامر (للعملاء **المسجلين فقط**)
- الدعم الفني - 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).