مثال على تكوين VPN على ASA مع السيناريوهات المتداخلة

المحتويات

[المقدمة]
[المتطلبات الأساسية]
[المتطلبات]
[المكونات المستخدمة]
[معلومات أساسية]
[الترجمة على كل من نقاط نهاية VPN]
[ASA 1]
[إنشاء الكائنات اللازمة للشبكات الفرعية قيد الاستخدام]
[تكوين عبارة NAT]
[تكوين قائمة التحكم في الوصول إلى التشفير باستخدام الشبكات الفرعية التي تمت ترجمتها]
[تكوين التشفير ذي الصلة]
[ASA 2]
[إنشاء الكائنات اللازمة للشبكات الفرعية قيد الاستخدام]
[تكوين عبارة NAT]
[تكوين قائمة التحكم في الوصول إلى التشفير باستخدام الشبكات الفرعية التي تمت ترجمتها]
[تكوين التشفير ذي الصلة]
[التحقق من الصحة]
[ASA 1]
[ASA 2]
[الموزع والمتكلم مع أفرع متداخلة]
[ASA1]
[إنشاء الكائنات اللازمة للشبكات الفرعية قيد الاستخدام]
[إنشاء جمل يدوية لترجمة:]
[تكوين قائمة التحكم في الوصول إلى التشفير باستخدام الشبكات الفرعية التي تمت ترجمتها]
[تكوين التشفير ذي الصلة]
[ASA2 (متكلم 1)]
[تكوين قائمة التحكم في الوصول (ACL) للتشفير الذي يذهب إلى الشبكة الفرعية المترجمة (10.20.20.0 /24)]
[تكوين التشفير ذي الصلة]
[R1 (TALK2)]
[قم بتكوين قائمة التحكم في الوصول (ACL) للتشفير الانتقال إلى الشبكة الفرعية المترجمة (10.30.30.0 /24)]
[تكوين التشفير ذي الصلة]
[التحقق من الصحة]
[ASA 1]
[ASA2 (متكلم 1)]

R1 (TALK2)
استكشاف الأخطاء وإصلاحها
مسح القارنات المأمنية
رجاع تشكيل nat
أوامر استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يصف هذا وثيقة الـ steps يستعمل أن يتجرم الـ VPN حركة مرور أن يسافر عبر lan إلى LAN (L2L) IPsec نفق بين إثنان أمن مهايئ (ASA) في سيناريو متداخل وأيضا ترجمة عنوان أيسر (PAT) حركة مرور الإنترنت.

المتطلبات الأساسية

المتطلبات

تأكد من تكوين جهاز الأمان القابل للتكيف من Cisco باستخدام عنوان IP على الواجهات، ومن توفر إمكانية الاتصال الأساسية قبل المتابعة بمثال التكوين هذا.

المكونات المستخدمة

أسست المعلومة في هذا وثيقة على هذه برمجية صيغة:

- برنامج أجهزة الأمان المعدلة Cisco Adaptive Security Appliance، الإصدار 8.3 والإصدارات الأحدث.

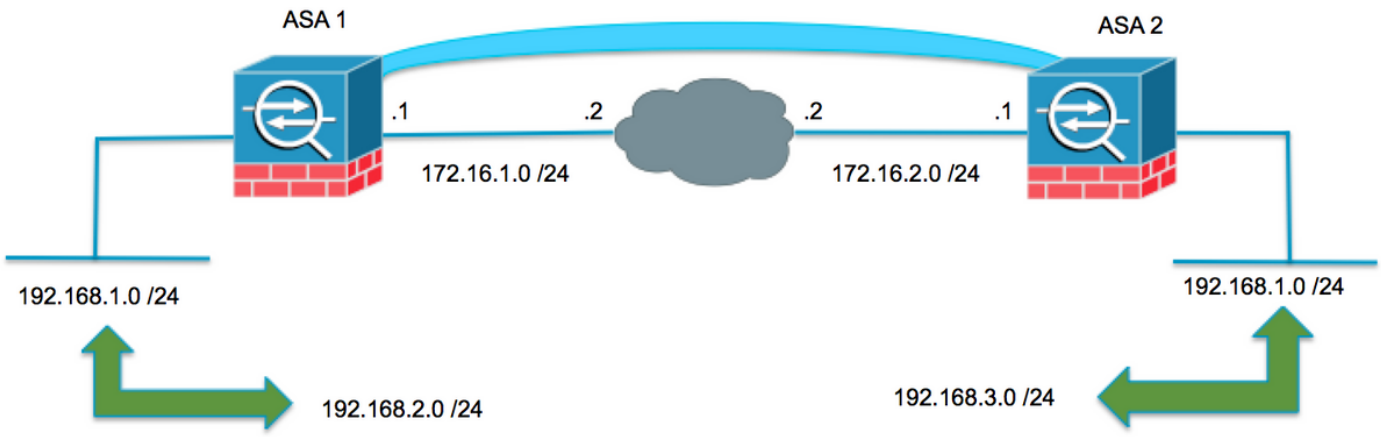
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يوجد خلف كل جهاز شبكة خاصة محمية. في السيناريوهات المتداخلة، الحد الاتصال عبر شبكة VPN أبدا لأن الحزم الا تغادر الشبكة الفرعية المحلية أبدا منذ إرسال حركة المرور إلى عنوان IP الخاص بنفس الشبكة الفرعية. يمكن تحقيق ذلك مع ترجمة عنوان الشبكة (NAT) كما هو موضح في الأقسام التالية.

الترجمة على كل من نقاط نهاية VPN

عندما تتداخل شبكات VPN المحمية ويمكن تعديل التكوين على الكل نقطتي النهاية، ويمكن إستخدام NAT لترجمة الشبكة المحلية إلى شبكة فرعية مختلفة عند الانتقال إلى الشبكة الفرعية المترجمة عن بعد.



ASA 1

إنشاء الكائنات اللازمة للشبكات الفرعية قيد الاستخدام

```
object network LOCAL
 subnet 192.168.1.0 255.255.255.0
object network XLATED-LOCAL
 subnet 192.168.2.0 255.255.255.0
object network XLATED-REMOTE
 subnet 192.168.3.0 255.255.255.0
```

تكوين عبارة NAT

إنشاء عبارة يدوية لترجمة الشبكة المحلية إلى شبكة فرعية مختلفة فقط عند الانتقال إلى الشبكة الفرعية البعيدة (مترجمة أيضا)

```
nat (inside,outside) source static LOCAL XLATED-LOCAL destination static XLATED-REMOTE XLATED-
REMOTE
```

تكوين قائمة التحكم في الوصول إلى التشفير باستخدام الشبكات الفرعية التي تمت ترجمتها

```
access-list VPN-TRAFFIC extended permit ip object XLATED-LOCAL object XLATED-REMOTE Rele
```

تكوين التشفير ذي الصلة

```
crypto ikev1 enable outside
crypto ikev1 policy 1
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400

crypto ipsec ikev1 transform-set AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-TRAFFIC
crypto map MYMAP 10 set peer 172.16.2.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
```

```
crypto map MYMAP interface outside

tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
 ikev1 pre-shared-key secure_PSK
```

ASA 2

إنشاء الكائنات اللازمة للشبكات الفرعية قيد الاستخدام

```
object network LOCAL
 subnet 192.168.1.0 255.255.255.0
object network XLATED-LOCAL
 subnet 192.168.3.0 255.255.255.0
object network XLATED-REMOTE
 subnet 192.168.2.0 255.255.255.0
```

تكوين عبارة NAT

إنشاء عبارة يدوية لترجمة الشبكة المحلية إلى شبكة فرعية مختلفة فقط عند الانتقال إلى الشبكة الفرعية البعيدة (مترجمة أيضا)

```
nat (inside,outside) source static LOCAL XLATED-LOCAL destination static XLATED-REMOTE XLATED-
REMOTE
```

تكوين قائمة التحكم في الوصول إلى التشفير باستخدام الشبكات الفرعية التي تمت ترجمتها

```
access-list VPN-TRAFFIC extended permit ip object XLATED-LOCAL object XLATED-REMOTE Rele
```

تكوين التشفير ذي الصلة

```
crypto ikev1 enable outside
crypto ikev1 policy 1
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400

crypto ipsec ikev1 transform-set AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-TRAFFIC
crypto map MYMAP 10 set peer 172.16.1.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside

tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
 ikev1 pre-shared-key secure_PSK
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

ASA 1

```
ASA1(config)# sh cry isa sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 172.16.2.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs

ASA1(config)# show crypto ipsec sa
interface: outside
    Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.1.1

      access-list VPN-TRAFFIC extended permit ip 192.168.2.0 255.255.255.0 192.168.3.0
255.255.255.0
      local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      current_peer: 172.16.2.1


      #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
      #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0
      path mtu 1500, ipsec overhead 74(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: F90C149A
      current inbound spi : 6CE656C7

    inbound esp sas:
      spi: 0x6CE656C7 (1827034823)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 16384, crypto-map: MYMAP
         sa timing: remaining key lifetime (kB/sec): (3914999/28768)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x000003FF
    outbound esp sas:
      spi: 0xF90C149A (4178318490)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 16384, crypto-map: MYMAP
         sa timing: remaining key lifetime (kB/sec): (3914999/28768)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

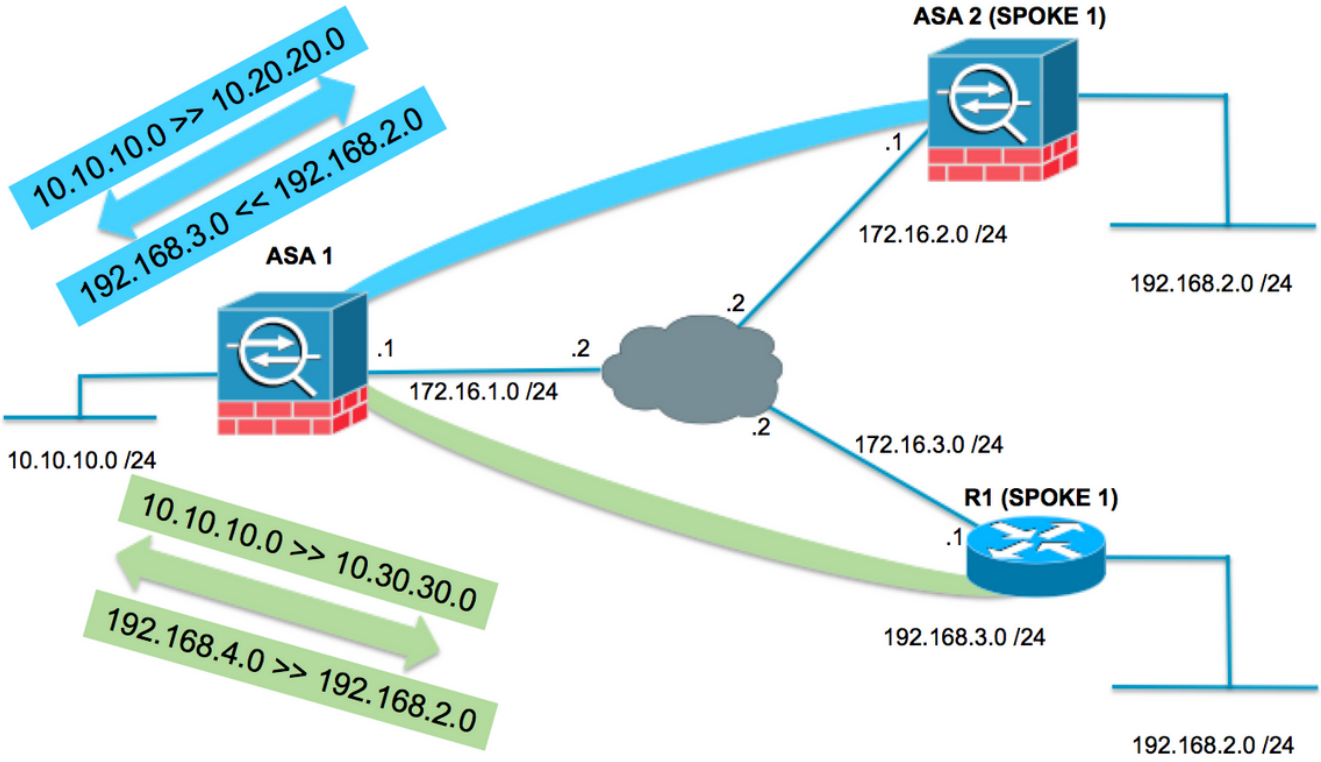
ASA 2

```
ASA2(config)# show crypto isa sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 172.16.1.1
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs

ASA2(config)# show crypto ipsec sa
interface: outside
    Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.2.1

      access-list VPN-TRAFFIC extended permit ip 192.168.3.0 255.255.255.0 192.168.2.0
255.255.255.0
      local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
      current_peer: 172.16.1.1


      #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
      #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
      path mtu 1500, ipsec overhead 74(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 6CE656C7
      current inbound spi : F90C149A

    inbound esp sas:
      spi: 0xF90C149A (4178318490)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 12288, crypto-map: MYMAP
         sa timing: remaining key lifetime (kB/sec): (4373999/28684)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x000003FF
    outbound esp sas:
      spi: 0x6CE656C7 (1827034823)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 12288, crypto-map: MYMAP
         sa timing: remaining key lifetime (kB/sec): (4373999/28683)
```

```
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
 0x00000000 0x00000001
```

الموزع والمتكلم مع أفرع متداخلة

في المخطط التالي، يحتوي كل الخادمين على الشبكة الفرعية نفسها التي يلزم حمايتها عبر نفق IPsec باتجاه الصرة. لتسهيل الإدارة على القارن ال nat تشكيل أن يحل ال يتداخل مشكلة أنجزت على الصرة فقط.



ASA1

إنشاء الكائنات اللازمة للشبكات الفرعية قيد الاستخدام

```
object network LOCAL
 subnet 10.10.10.0 255.255.255.0
object network SPOKES-NETWORK
 subnet 192.168.2.0 255.255.255.0
object network LOCAL-XLATE-TO-SPOKE1
 subnet 10.20.20.0 255.255.255.0
object network LOCAL-XLATE-TO-SPOKE2
 subnet 10.30.30.0 255.255.255.0
object network REMOTE-XLATE-SPOKE1
 subnet 192.168.3.0 255.255.255.0
object network REMOTE-XLATE-SPOKE2
 subnet 192.168.4.0 255.255.255.0
```

إنشاء جمل يدوية لترجمة:

- الشبكة المحلية من 10.10.10.0 /24 إلى 10.20.20.0 /24 عند الانتقال إلى TALK1 (192.168.2.0 /24).
- شبكة TALK1 من 192.168.2.0 /24 إلى 192.168.3.0 /24 عند الوصول إلى 10.20.20.0 /24.
- الشبكة المحلية من 10.10.10.0 /24 إلى 10.30.30.0 /24 عند الانتقال إلى TALK3 (192.168.2.0 /24).
- شبكة TALK2 من 192.168.2.0 /24 إلى 192.168.4.0 /24 عند اتصالك إلى 10.30.30.0 /24.

```
nat (inside,outside) source static LOCAL LOCAL-XLATE-SPOKE1 destination static REMOTE-XLATE-
SPOKE1 SPOKES-NETWORK
nat (inside,outside) source static LOCAL LOCAL-XLATE-SPOKE2 destination static REMOTE-XLATE-
SPOKE2 SPOKES-NETWORK
```

تكوين قائمة التحكم في الوصول إلى التشفير باستخدام الشبكات الفرعية التي تمت ترجمتها

```
access-list VPN-to-SPOKE1 extended permit ip object LOCAL-XLATE-SPOKE1 object SPOKES-NETWORKS
access-list VPN-to-SPOKE2 extended permit ip object LOCAL-XLATE-SPOKE2 object SPOKES-NETWORKS
```

تكوين التشفير ذي الصلة

```
crypto ikev1 enable outside
crypto ikev1 policy 1
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400

crypto ipsec ikev1 transform-set AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-to-SPOKE1
crypto map MYMAP 10 set peer 172.16.2.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP 20 match address VPN-to-SPOKE2
crypto map MYMAP 20 set peer 172.16.3.1
crypto map MYMAP 20 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside

tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
 ikev1 pre-shared-key secure_PSK
tunnel-group 172.16.3.1 type ipsec-l2l
tunnel-group 172.16.3.1 ipsec-attributes
 ikev1 pre-shared-key secure_PSK
```

ASA2 (تكلم 1)

تكوين قائمة التحكم في الوصول (ACL) للتشفير الذي يذهب إلى الشبكة الفرعية المترجمة (10.20.20.0 /24)

```
access-list VPN-TRAFFIC extended permit ip 192.168.2.0 255.255.255.0 10.20.20.0 255.255.255.0
```

تكوين التشفير ذي الصلة

```
crypto ikev1 enable outside
```

```
crypto ikev1 policy 1
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400

crypto ipsec ikev1 transform-set esp-aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map MYMAP 10 match address VPN-TRAFFIC
crypto map MYMAP 10 set peer 172.16.1.1
crypto map MYMAP 10 set ikev1 transform-set AES256-SHA
crypto map MYMAP interface outside

tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
 ikev1 pre-shared-key secure_PSK
```

R1 (TALK2)

قم بتكوين قائمة التحكم في الوصول (ACL) للتشفير الانتقال إلى الشبكة الفرعية المترجمة (10.30.30.0 /24)

```
ip access-list extended VPN-TRAFFIC
 permit ip 192.168.2.0 0.0.0.255 10.30.30.0 0.0.0.255
```

تكوين التشفير ذي الصلة

```
crypto isakmp policy 1
 encr aes 256
 authentication pre-share
 group 2

crypto isakmp key secure_PSK address 172.16.1.1

crypto ipsec transform-set AES256-SHA esp-aes 256 esp-sha-hmac
 mode tunnel

crypto map MYMAP 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set AES256-SHA
 match address VPN-TRAFFIC

interface GigabitEthernet0/1
 ip address 172.16.3.1 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 crypto map MYMAP
```

التحقق من الصحة

ASA 1

```
ASA1(config)# show crypto isakmp sa

IKEv1 SAs:
```

```
   Active SA: 2
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 2

1   IKE Peer: 172.16.3.1
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE
2   IKE Peer: 172.16.2.1
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs

ASA1(config)# show crypto ipsec sa
interface: outside
    Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.1.1

      access-list VPN-to-SPOKE1 extended permit ip 10.20.20.0 255.255.255.0 192.168.2.0
255.255.255.0
      local ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
      current_peer: 172.16.2.1


      #pkts encaps: 10, #pkts encrypt: 9, #pkts digest: 10
      #pkts decaps: 10, #pkts decrypt: 9, #pkts verify: 10
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0
      path mtu 1500, ipsec overhead 74(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 79384296
      current inbound spi : 2189BF7A

    inbound esp sas:
      spi: 0x2189BF7A (562675578)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 12288, crypto-map: MYMAP
         sa timing: remaining key lifetime (kB/sec): (3914999/28618)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x000003FF
    outbound esp sas:
      spi: 0x79384296 (2033730198)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 12288, crypto-map: MYMAP
         sa timing: remaining key lifetime (kB/sec): (3914999/28618)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001

    Crypto map tag: MYMAP, seq num: 20, local addr: 172.16.1.1
```

```
      access-list VPN-to-SPOKE2 extended permit ip 10.30.30.0 255.255.255.0 192.168.2.0
255.255.255.0
      local ident (addr/mask/prot/port): (10.30.30.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
      current_peer: 172.16.3.1


      #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
      #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.3.1/0
      path mtu 1500, ipsec overhead 74(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 65FDF4F5
      current inbound spi : 05B7155D

    inbound esp sas:
      spi: 0x05B7155D (95884637)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 8192, crypto-map: MYMAP
         sa timing: remaining key lifetime (kB/sec): (3914999/2883)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x0000001F
    outbound esp sas:
      spi: 0x65FDF4F5 (1711142133)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 8192, crypto-map: MYMAP
         sa timing: remaining key lifetime (kB/sec): (3914999/2883)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

ASA2 (مكلت 1)

```
ASA2(config)# show crypto isakmp sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 172.16.1.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
```

```
ASA2(config)# show crypto ipsec sa
interface: outside
    Crypto map tag: MYMAP, seq num: 10, local addr: 172.16.2.1

      access-list VPN-TRAFFIC extended permit ip 192.168.2.0 255.255.255.0 10.20.20.0
255.255.255.0
      local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
      current_peer: 172.16.1.1


      #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
      #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
      path mtu 1500, ipsec overhead 74(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 2189BF7A
      current inbound spi : 79384296

    inbound esp sas:
      spi: 0x79384296 (2033730198)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 8192, crypto-map: MYMAP
         sa timing: remaining key lifetime (kB/sec): (4373999/28494)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x000003FF
    outbound esp sas:
      spi: 0x2189BF7A (562675578)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 8192, crypto-map: MYMAP
         sa timing: remaining key lifetime (kB/sec): (4373999/28494)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

R1 (TALK2)

```
R31show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.16.1.1      172.16.3.1      QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA

R1#show crypto ipsec sa

interface: GigabitEthernet0/1
    Crypto map tag: MYMAP, local addr 172.16.3.1
```

```
protected vrf: (none)
local  ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.30.30.0/255.255.255.0/0/0)
current_peer 172.16.1.1 port 500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
 #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0

  local crypto endpt.: 172.16.3.1, remote crypto endpt.: 172.16.1.1
  plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
  current outbound spi: 0x5B7155D(95884637)
  PFS (Y/N): N, DH group: none

  inbound esp sas:
   spi: 0x65FDF4F5(1711142133)
     transform: esp-256-aes esp-sha-hmac ,
     in use settings ={Tunnel, }
     conn id: 1, flow_id: SW:1, sibling_flags 80004040, crypto map: MYMAP
     sa timing: remaining key lifetime (k/sec): (4188495/2652)
     IV size: 16 bytes
     replay detection support: Y
     Status: ACTIVE(ACTIVE)

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0x5B7155D(95884637)
     transform: esp-256-aes esp-sha-hmac ,
     in use settings ={Tunnel, }
     conn id: 2, flow_id: SW:2, sibling_flags 80004040, crypto map: MYMAP
     sa timing: remaining key lifetime (k/sec): (4188495/2652)
     IV size: 16 bytes
     replay detection support: Y
     Status: ACTIVE(ACTIVE)

  outbound ah sas:

  outbound pcp sas:
```

استكشاف الأخطاء وإصلاحها

يوفر هذه القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

مسح القترانات الأمنية

عند أستكشاف أخطاء SA وإصلاحها، تأكد من مسح رسائل SA الموجودة بعد إجراء تغيير. في الوضع ذي الامتيازات ل PIX، أستخدم الأوامر التالية:

- **مسح تشفير IPsec** - يحذف شبكات IPsec النشطة.
- **مسح التشفير isakmp sa** - يحذف شبكات IKE النشطة.

راجعت تشكيل nat

- **عرض تفاصيل nat** - يعرض تكوين NAT مع توسيع الكائن (الكائنات) / مجموعة (مجموعات) الكائنات

أوامر استكشاف الأخطاء وإصلاحها

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

دعم Cisco CLI Analyzer (من Cisco) (للعملاء المسجلين فقط) أوامر show معينة. استخدم Cisco CLI Analyzer (من Cisco) لعرض تحليل لمُخرَج الأمر show.

> **ملاحظة**: ارجع إلى معلومات مهمة حول أوامر تصحيح الأخطاء واستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر تصحيح الأخطاء واستخدامها قبل أن تستخدم أوامر debug.

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

معلومات ذات صلة

- دشرم لكيل تشكيل nat
- حلول أستكشاف أخطاء الشبكة الخاصة الظاهرية (VPN) عبر بروتوكول IPsec للوصول عن بعد و L2L الأكثر شيوعا
- مفاوضة IPSec/بروتوكولات IKE
- 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).