# تكوين IPSec بين ثلاثة موجهات باستخدام العناوين الخاصة

## المحتويات



## المقدمة

يصف هذا وثيقة تشكيل كامل الربط مع ثلاثة مسحاج تخديد أن يستعمل عنوان خاص. يوضح المثال هذه الميزات:

- حمولة أمان التضمين (ESP) - معيار تشفير البيانات (DES) فقط
- المفاتيح المشتركة مسبقا
- الشبكات الخاصة خلف كل موجه: 192.168.1.0 و 192.168.2.0 و 192.168.3.0
- تكوين سياسة ISAKMP وخريطة التشفير
- تم تحديد حركة مرور النفق باستخدام أوامر **access-list** و**route-map**. بالإضافة إلى ترجمة عنوان المنفذ (PAT)، يمكن تطبيق خرائط المسار على ترجمة عنوان الشبكة (NAT) الثابتة من واحد إلى واحد على برنامج Cisco IOS® الإصدار T2(4)12.2 والإصدارات الأحدث. أحلت ل كثير معلومة nat - قدرة أن يستعمل ممر خرائط مع ساكن إستاتيكي ترجمة سمة نظرة عامة.

**ملاحظة:** تخضع تكنولوجيا التشفير لضوابط التصدير. من مسؤوليتك معرفة القانون المتعلق بتصدير تقنية التشفير. إذا كانت لديك أية أسئلة تتعلق بالتحكم في التصدير، فيرجى إرسال بريد إلكتروني إلى موقع export@cisco.com.

## المتطلبات الأساسية

### المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

### المكونات المستخدمة

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

- برنامج IOS الإصدار 12.3(7)T من Cisco
- تم تكوين موجهات Cisco باستخدام IPSec.

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.

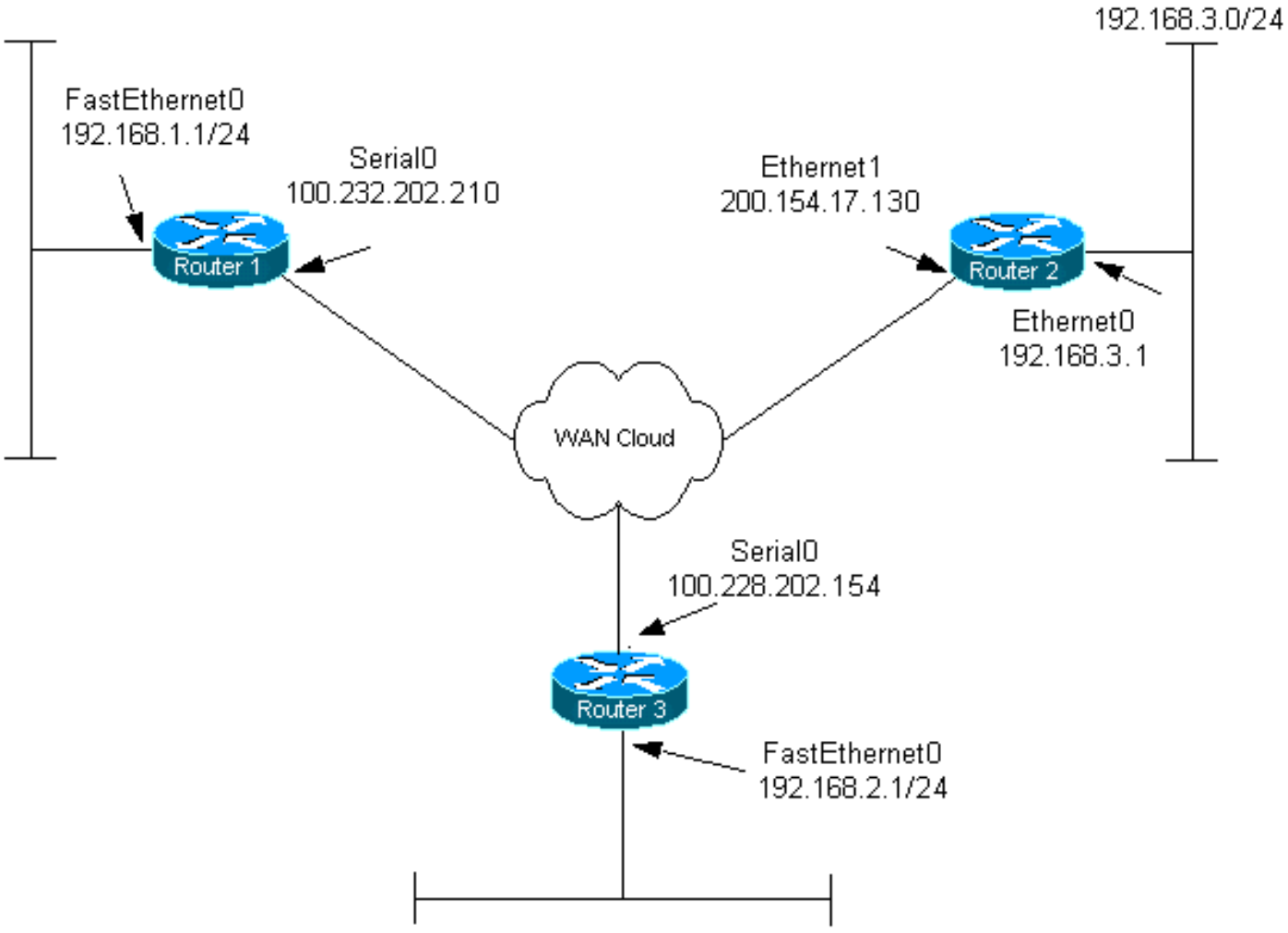
# التكوين

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).

## الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



## التكوينات

يستخدم هذا المستند التكوينات التالية:

- الموجه 1
- الموجه 2
- الموجه 3

**الموجه 1**

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router1
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!

Configure Internet Key Exchange (IKE) policy and !- ---!
-- pre-shared keys for each peer. !--- IKE policy
defined for peers. crypto isakmp policy 4
authentication pre-share

Pre-shared keys for different peers. crypto isakmp ---!
key xxxxxx1234 address 100.228.202.154
crypto isakmp key xxxxxx1234 address 200.154.17.130
!
!

IPSec policies: crypto ipsec transform-set encrypt- ---!
des esp-des
!
!
crypto map combined local-address Serial0

Set the peer, transform-set and encryption traffic ---!
for tunnel peers. crypto map combined 20 ipsec-isakmp
set peer 100.228.202.154
set transform-set encrypt-des
match address 106
crypto map combined 30 ipsec-isakmp
set peer 200.154.17.130
set transform-set encrypt-des
match address 105
!
!
```

```
interface Serial0
 ip address 100.232.202.210 255.255.255.252
 ip nat outside
 serial restart-delay 0

 Apply the crypto map to the interface. crypto map ---!
combined
!
interface FastEthernet0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.232.202.209
no ip http server
no ip http secure-server
!

Define traffic for NAT. ip nat inside source route- ---!
map nonat interface Serial0 overload

 Access control list (ACL) that shows traffic to ---!
 encrypt over the tunnel. access-list 105 permit ip
192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
access-list 106 permit ip 192.168.1.0 0.0.0.255
192.168.2.0 0.0.0.255

 ACL to avoid the traffic through NAT over the ---!
tunnel. access-list 150 deny ip 192.168.1.0 0.0.0.255
192.168.2.0 0.0.0.255
access-list 150 deny ip 192.168.1.0 0.0.0.255
192.168.3.0 0.0.0.255

ACL to perform NAT on the traffic that does not go ---!
 over the tunnel. access-list 150 permit ip 192.168.1.0
0.0.0.255 any

Do not perform NAT on the IPSec traffic. route-map ---!
nonat permit 10
 match ip address 150
!
control-plane
!
!
 line con 0
 line aux 0
line vty 0 4
!
!
end
```

**الموجه 2**

```
:Current configuration
!
version 12.3
service timestamps debug datetime msec
 service timestamps log datetime msec
 no service password-encryption
!
 hostname router2
!
boot-start-marker
```

```
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!

Configure IKE policy and pre-shared keys for each ---!
peer. !--- IKE policy defined for peers. crypto isakmp
policy 4
authentication pre-share

Pre-shared keys for different peers. crypto isakmp ---!
key xxxxxx1234 address  100.228.202.154
crypto isakmp key xxxxxx1234 address  100.232.202.210
!
!


IPSec policies. crypto ipsec transform-set encrypt- ---!
des esp-des
!
!
crypto map combined local-address Ethernet1

Set the peer, transform-set and encryption traffic ---!
for tunnel peers. crypto map combined 7 ipsec-isakmp
set peer 100.232.202.210
set transform-set encrypt-des
match address 105

crypto map combined 8 ipsec-isakmp
set peer 100.228.202.154
set transform-set encrypt-des
match address 106
!
!
!
interface Ethernet0
ip address 192.168.3.1 255.255.255.0
ip nat inside
!
interface Ethernet1
ip address 200.154.17.130 255.255.255.224
ip nat outside

Apply the crypto map to the interface. crypto map ---!
combined
!
ip classless
ip route 0.0.0.0 0.0.0.0 200.154.17.129
no ip http server
no ip http secure-server
!

Define traffic for NAT. ip nat inside source route- ---!
map nonat interface Ethernet1 overload

ACL shows traffic to encrypt over the tunnel. ---!
access-list 105 permit ip 192.168.3.0 0.0.0.255
```

```
                                        192.168.1.0 0.0.0.255
                  access-list 106 permit ip 192.168.3.0 0.0.0.255
                                        192.168.2.0 0.0.0.255

     ACL to avoid the traffic through NAT over the ---!
  tunnel. access-list 150 deny ip 192.168.3.0 0.0.0.255
                                        192.168.1.0 0.0.0.255
                  access-list 150 deny ip 192.168.3.0 0.0.0.255
                                        192.168.2.0 0.0.0.255

 ACL to perform NAT on the traffic that does not go ---!
       over the tunnel. access-list 150 permit ip any any

 Do not perform NAT on the IPSec traffic. route-map ---!
                                              nonat permit 10
                                            match ip address 150
                                                           !
                                                           !
                                                           !
                                                 control-plane
                                                           !
                                                           !
                                                   line con 0
                                                   line aux 0
                                                 line vty 0 4
                                                           !
                                                           !
                                                         end
```

## تكوين الموجه 3

```
                                                 :Current configuration
                                                           !
                                                      version 12.3
                                  service timestamps debug datetime msec
                                    service timestamps log datetime msec
                                          no service password-encryption
                                                           !
                                                   hostname router3
                                                           !
                                                  boot-start-marker
                                                    boot-end-marker
                                                           !
                                                           !
                                                clock timezone EST 0
                                                    no aaa new-model
                                                      ip subnet-zero
                                                           !
                                                           !
                                               ip audit po max-events 100
                                               no ftp-server write-enable
                                                           !

  Configure IKE policy and pre-shared keys for each ---!
  peer. !--- IKE policy defined for peers. crypto isakmp
                                                        policy 4
                                                 authentication pre-share


 Pre-shared keys for different peers. crypto isakmp ---!
                                        key xxxxxx1234 address 100.232.202.210
                     crypto isakmp key xxxxxx1234 address 200.154.17.130
                                                           !
```

```
                                                                    !

IPSec policies: crypto ipsec transform-set encrypt- ---!
                                                        des esp-des
                                                                    !
                                                                    !


 Set the peer, transform-set and encryption traffic ---!
     for tunnel peers. crypto map combined local-address
                                                        Serial0
                          crypto map combined 7 ipsec-isakmp
                                  set peer 100.232.202.210
                             set transform-set encrypt-des
                                    match address 106
                          crypto map combined 8 ipsec-isakmp
                                  set peer 200.154.17.130
                             set transform-set encrypt-des
                                    match address 105
                                                                    !
                                                                    !
                                               interface Serial0
               ip address 100.228.202.154 255.255.255.252
                                                ip nat outside
                                    serial restart-delay 0

  Apply the crypto map to the interface. crypto map ---!
                                                        combined
                                                                    !
                                    interface FastEthernet0
                     ip address 192.168.2.1 255.255.255.0
                                                 ip nat inside
                                                                    !
                                                   ip classless
                   ip route 0.0.0.0 0.0.0.0 100.228.202.153
                                                no ip http server
                                    no ip http secure-server
                                                                    !

Define traffic for NAT. ip nat inside source route- ---!
                                map nonat interface Serial0 overload

 ACL that shows traffic to encrypt over the tunnel. ---!
            access-list 105 permit ip 192.168.2.0 0.0.0.255
                                      192.168.3.0 0.0.0.255
            access-list 106 permit ip 192.168.2.0 0.0.0.255
                                      192.168.1.0 0.0.0.255

      ACL to avoid the traffic through NAT over the ---!
   tunnel. access-list 150 deny ip 192.168.2.0 0.0.0.255
                                      192.168.3.0 0.0.0.255
             access-list 150 deny ip 192.168.2.0 0.0.0.255
                                      192.168.1.0 0.0.0.255

 ACL to perform NAT on the traffic that does not go ---!
  over the tunnel. access-list 150 permit ip 192.168.2.0
                                                0.0.0.255 any

 Do not perform NAT on the IPSec traffic. route-map ---!
                                                nonat permit 10
                                     match ip address 150
                                                                    !
                                                                    !
                                                                    !
                                                   control-plane
```

```
!
!
line con 0
line aux 0
line vty 0 4
 login
!
!
end
```

## 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 جميع اقترانات أمان IKE الحالية (SAs) في نظير.
- **show crypto ipSec**— يعرض الإعدادات المستخدمة من قبل IPSec) SAs) الحالية.

## 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 **تصحيح الأخطاء**، يرجى الاطلاع على المعلومات المهمة في أوامر تصحيح الأخطاء.

**ملاحظة:** يجب تشغيل عمليات تصحيح الأخطاء التالية على كل من موجهات IPSec (الأقران). يجب إجراء مسح SAs على كلا النظيرين.

- **debug crypto isakmp**—يعرض الأخطاء أثناء المرحلة 1.
- **debug crypto ipSec**—يعرض الأخطاء أثناء المرحلة 2.
- **debug crypto engine**—يعرض معلومات من محرك التشفير.
- **مسح معرف *اتصال* التشفير** ***[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**—يمحو المرحلة 1 من SAs.
- **مسح التشفير sa**—يمسح المرحلة 2 SAs.

## معلومات ذات صلة

- صفحة دعم IPSec
- 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).