توجيه السياسة وتأثيره على حزم ESP و Cisco IOS باستخدام ISAKMP

المحتويات

المقدمة

يصف هذا وثيقة الأثر من سياسة baser تحشد (PBR) و PBR محلي عندما يطبق إلى يغلف أمن حمولة (ESP) وإنترنت أمن اقتران ومفتاح إدارة بروتوكول (ISAKMP) عندما يستعمل أنت cisco ios®.

تمت المساهمة بواسطة مايكل جاركارز، مهندس TAC من Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة أساسية بالمواضيع التالية:

- IOS من Cisco
- تكوين VPN على Cisco IOS

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الإصدار x.15 من Cisco IOS.

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

معلومات أساسية

قبل إنشاء نفق IPsec، يقوم الموجه ببدء تبادل ISAKMP. بما أن هذه الحزم يتم إنشاؤها بواسطة الموجه، فإن الحزم يتم معالجتها كحركة مرور تم إنشاؤها محليا ويتم تطبيق أي قرارات PBR محلية. بالإضافة إلى ذلك، يتم إعتبار أي حزم يتم إنشاؤها بواسطة الموجه (بروتوكول توجيه العبارة الداخلي المحسن (EIGRP)، أو بروتوكول تحليل الخطوة التالية (NHRP)، أو إختبارات اتصال بروتوكول العبارة الحدودية (BGP)، أو بروتوكول رسائل التحكم في الإنترنت (ICMP)) كحركة مرور تم إنشاؤها محليا ويتم تطبيق قرار PBR المحلي.

لا تعتبر حركة المرور التي تتم إعادة توجيهها بواسطة الموجه وإرسالها عبر النفق، والذي يسمى حركة مرور النقل، حركة مرور تم إنشاؤها محليا، ويجب تطبيق أي سياسة توجيه مرغوبة على واجهة الدخول إلى الموجه.

إن الآثار التي يخلفها هذا على حركة المرور التي تجتاز النفق هي أن حركة المرور التي تم إنشاؤها محليا تتبع PBR، ولكن حركة مرور النقل لا. توضح هذه المقالة عواقب هذا الاختلاف في السلوك.

بالنسبة لحركة مرور النقل التي تحتاج إلى تضمين ESP، لا حاجة إلى وجود أي إدخالات توجيه لأن PBR يحدد واجهة الخروج للحزمة قبل تضمين ESP وبعده. لحركة المرور التي تم إنشاؤها محليا والتي يلزم تغليف ESP، من الضروري أن يكون هناك إدخالات توجيه، لأن PBR المحلي يحدد واجهة مخرج الحزمة فقط قبل التضمين ويحدد التوجيه واجهة الخروج للحزمة ما بعد التضمين.

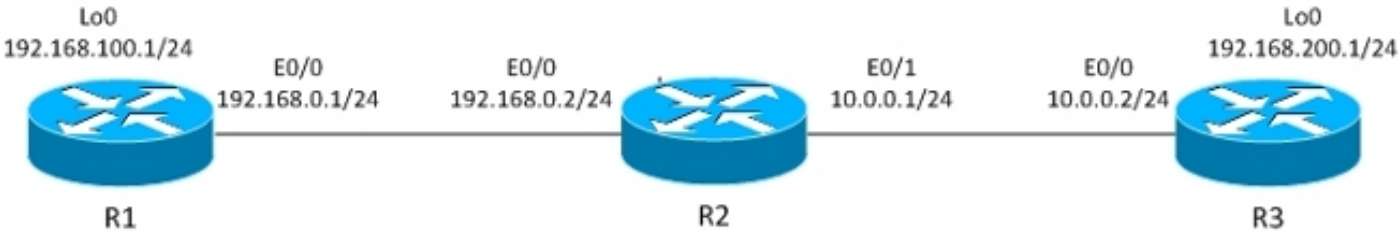
يحتوي هذا المستند على مثال تكوين نموذجي حيث يتم إستخدام موجه واحد مزود بارتباطين من ISP. ويتم إستخدام إرتباط واحد للوصول إلى الإنترنت، بينما يستخدم الثاني لشبكة VPN. في حالة فشل أي إرتباط، يتم إعادة توجيه حركة المرور باستخدام إرتباط مختلف لمزود خدمة الإنترنت (ISP). وتعرض أيضا الاشراك.

يرجى ملاحظة أنه يتم تنفيذ PBR في إعادة التوجيه السريع من Cisco (CEF)، في حين يتم تحويل PBR المحلي للعملية.

حركة المرور التي تم إنشاؤها محليا على الموجه

يصف هذا القسم سلوك حركة المرور التي بدأت من الموجه (R)1. يتم تضمين حركة المرور هذه بواسطة ESP بواسطة R1.

طوبولوجيا



يتم إنشاء نفق IPsec LAN-to-LAN بين R1 و R3.

تقع حركة المرور المثيرة للاهتمام بين 192.168.100.1) Lo0 R1) و 192.168.200.1) Lo0 R3).

يحتوي الموجه R3 على مسار افتراضي إلى R2.

لا يحتوي R1 على إدخالات توجيه، ولكنه يحتوي على شبكات متصلة مباشرة فقط.

التكوين

يحتوي R1 على PBR محلي لجميع حركات المرور:

```
interface Loopback0
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/0
 ip address 192.168.0.1 255.255.255.0
 crypto map CM

track 10 ip sla 10
ip sla 10
 icmp-echo 192.168.0.2 source-ip 192.168.0.1

route-map LOCALPBR permit 10
 set ip next-hop verify-availability 192.168.0.2 1 track 10
ip local policy route-map LOCALPBR
```

تصحيح الأخطاء

يتم إرسال جميع حركة المرور التي تم إنشاؤها محليا على R1 إلى R2 عندما تكون قيد التشغيل.

للتحقق من ما يحدث عند إظهار النفق، قم بإرسال حركة المرور المثيرة للاهتمام من الموجه نفسه:

```
R1#debug ip packet
R1#ping 192.168.200.1 source lo0
```

تحذير: قد يؤدي الأمر **debug ip packet** إلى إنشاء كمية كبيرة من تصحيح الأخطاء ويكون له تأثير كبير على إستخدام وحدة المعالجة المركزية. إستعملوها بحذر.

يسمح هذا تصحيح الأخطاء أيضا باستخدام قائمة الوصول للحد من مقدار حركة المرور التي تمت معالجتها بواسطة تصحيح الأخطاء. يعرض الأمر **debug ip packet** حركة مرور البيانات التي يتم تحويلها للعملية فقط.

فيما يلي تصحيح الأخطاء على R1:

```
IP: s=192.168.100.1 (local), d=192.168.200.1 (Ethernet0/0), len 100, local
feature, Policy Routing(3), rtype 2, forus FALSE, sendself FALSE, mtu 0, fwdchk
FALSE
IP: s=192.168.100.1 (local), d=192.168.200.1 (Ethernet0/0), len 100, sending
,IP: s=192.168.100.1, d=192.168.200.1, pak EF6E8F28 consumed in output feature
packet consumed, IPSec output classification(30), rtype 2, forus FALSE, sendself
FALSE, mtu 0, fwdchk FALSE
IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 192, local feature, Policy
Routing(3), rtype 2, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 192, sending
,IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 192, output feature
,IPSec output classification(30), rtype 2, forus FALSE, sendself FALSE, mtu 0
fwdchk FALSE
,IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 192, output feature
,IPSec: to crypto engine(64), rtype 2, forus FALSE, sendself FALSE, mtu 0
fwdchk FALSE
,IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 192, output feature
,Post-encryption output features(65), rtype 2, forus FALSE, sendself FALSE, mtu 0
fwdchk FALSE
,IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 192, post-encap feature
rtype 2, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE ,(1)
,IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 192, post-encap feature
FastEther Channel(3), rtype 2, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 192, sending full packet
```

وإليكم ما يحدث:

حركة المرور المثيرة للاهتمام (192.168.100.1 < 192.168.200.1) مطابقة ل PBR المحلي، ويتم تحديد واجهة المخرج (E0/0). يؤدي هذا الإجراء إلى تشغيل رمز التشفير لبدء ISAKMP. كما يتم توجيه هذه الحزمة بواسطة PBR المحلي، والذي يحدد واجهة المخرج (E0/0). يتم إرسال حركة مرور ISAKMP، ويتم التفاوض بشأن النفق

ماذا يحدث عند إختبار الاتصال مرة أخرى؟

```
R1#show crypto session
Crypto session current status

Interface: Ethernet0/0
Session status: UP-ACTIVE
Peer: 10.0.0.2 port 500
IKEv1 SA: local 192.168.0.1/500 remote 10.0.0.2/500 Active
IPSEC FLOW: permit ip host 192.168.100.1 host 192.168.200.1
Active SAs: 2, origin: crypto map

R1#ping 192.168.200.1 source lo0 repeat 1

IP: s=192.168.100.1 (local), d=192.168.200.1 (Ethernet0/0), len 100, local
,feature, Policy Routing(3), rtype 2, forus FALSE, sendself FALSE, mtu 0
fwdchk FALSE
IP: s=192.168.100.1 (local), d=192.168.200.1 (Ethernet0/0), len 100, sending
IP: s=192.168.100.1 (local), d=192.168.200.1 (Ethernet0/0), len 100, output
,feature, IPSec output classification(30), rtype 2, forus FALSE, sendself FALSE
mtu 0, fwdchk FALSE
,IP: s=192.168.100.1, d=192.168.200.1, pak EEB40198 consumed in output feature
packet consumed, IPSec: to crypto engine(64), rtype 2, forus FALSE, sendself
FALSE, mtu 0, fwdchk FALSE
,IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 172, output feature
,IPSec output classification(30), rtype 1, forus FALSE, sendself FALSE, mtu 0
fwdchk FALSE
```

```
,IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 172, output feature
    ,IPSec: to crypto engine(64), rtype 1, forus FALSE, sendself FALSE, mtu 0
                                                                fwdchk FALSE
,IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 172, output feature
   ,Post-encryption output features(65), rtype 1, forus FALSE, sendself FALSE
                                                        mtu 0, fwdchk FALSE
    ,IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), g=10.0.0.2, len 172
                                                                    forward
     IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 172, post-encap
      feature, (1), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
     IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 172, post-encap
  ,feature, FastEther Channel(3), rtype 0, forus FALSE, sendself FALSE, mtu 0
                                                                fwdchk FALSE
  IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 172, encapsulation
                                                                    .failed
                                                (Success rate is 0 percent (0/1
```

وإليكم ما يحدث:

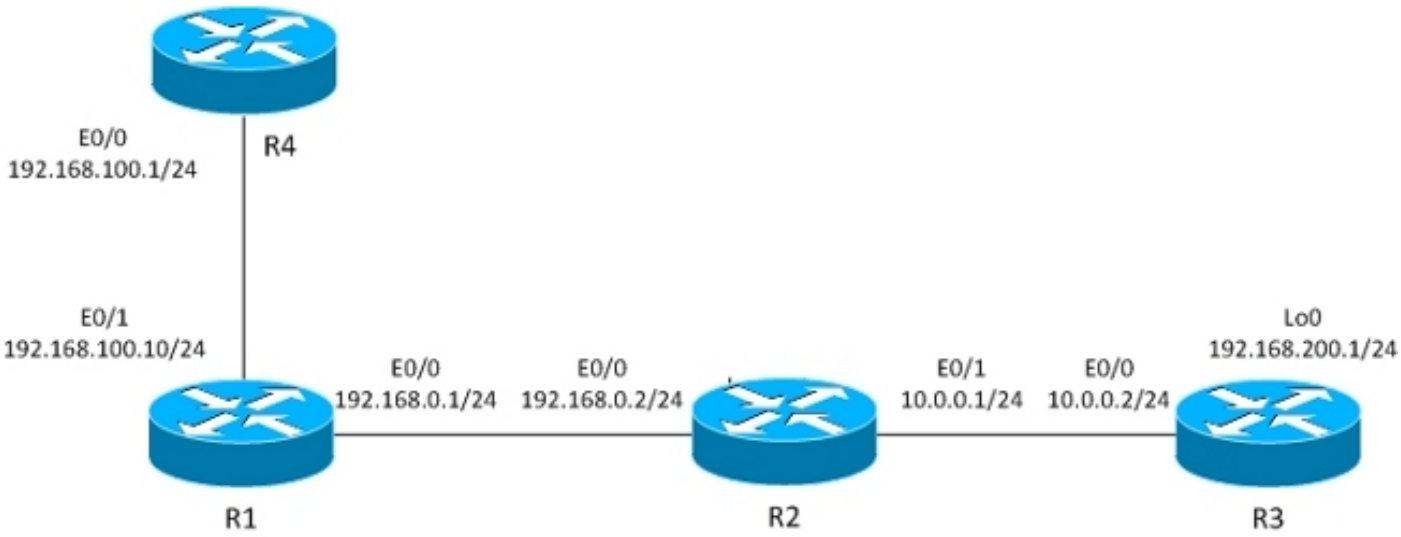
يتم توجيه حركة المرور المهمة التي تم إنشاؤها محليا، 192.168.100.1 > 192.168.200.1، محليا وفقا للسياسة، ويتم تحديد واجهة الخروج (E0/0). يتم إستهلاك الحزمة من قبل ميزة إخراج IPsec على E0/0 ويتم تضمينها. يتم التحقق من الحزمة المغلفة (من 192.168.0.1 إلى 10.0.0.2) للتوجيه لتحديد واجهة المخرج، ولكن لا يوجد شيء في جداول التوجيه الخاصة ب R1، وهو سبب فشل عملية التضمين.

في هذا السيناريو، يكون النفق قيد التشغيل، ولكن لا يتم إرسال حركة المرور لأنه، بعد تضمين ESP، يتحقق Cisco IOS من جداول التوجيه لتحديد واجهة المخرج.

حركة مرور بيانات العبور من خلال الموجه

يصف هذا القسم سلوك حركة مرور النقل التي تأتي من خلال الموجه، والذي يكون ESP مضمن بواسطة ذلك الموجه.

طوبولوجيا



تم إنشاء نفق L2L بين R1 و R3.

تقع حركة المرور المثيرة للاهتمام بين 192.168.100.1) R4) و 192.168.200.1) lo0 R3).

يحتوي الموجه R3 على مسار افتراضي إلى R2.

يحتوي الموجه R4 على مسار افتراضي إلى R1.

لا يحتوي R1 على توجيه.

التكوين

يتم تعديل المخطط السابق لعرض التدفق عندما يستقبل الموجه الحزم للتشفير (حركة مرور النقل بدلا من حركة المرور التي تم إنشاؤها محليا).

في الوقت الحالي، يتم توجيه حركة المرور المفيدة المستلمة من R4 نحو السياسة على R1 (بواسطة PBR على E0/1)، كما يوجد توجيه سياسة محلي لجميع حركات المرور:

```
interface Ethernet0/1
ip address 192.168.100.10 255.255.255.0
ip policy route-map PBR

route-map LOCALPBR permit 10
set ip next-hop verify-availability 192.168.0.2 1 track 10
!
route-map PBR permit 10
set ip next-hop verify-availability 192.168.0.2 1 track 10

ip local policy route-map LOCALPBR
```

تصحيح الأخطاء

للتحقق من ما يحدث عند إظهار النفق على R1 (بعد أن تتلقى حركة المرور المثيرة للاهتمام من R4)، أدخل:

```
R1#debug ip packet

R4#ping 192.168.200.1
```

فيما يلي تصحيح الأخطاء على R1:

```
,IP: s=192.168.100.1 (Ethernet0/1), d=192.168.200.1 (Ethernet0/0), len 100
,input feature, Policy Routing(68), rtype 2, forus FALSE, sendself FALSE, mtu 0
fwdchk FALSE
,IP: s=192.168.100.1 (Ethernet0/1), d=192.168.200.1 (Ethernet0/0), len 100
,input feature, MCI Check(73), rtype 2, forus FALSE, sendself FALSE, mtu 0
fwdchk FALSE
,IP: s=192.168.100.1, d=192.168.200.1, pak EEB4A9D8 consumed in output feature
,packet consumed, IPSec output classification(30), rtype 2, forus FALSE
sendself FALSE, mtu 0, fwdchk FALSE
,IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 192, local feature
Policy Routing(3), rtype 2, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 192, sending
,IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 192, output feature
,IPSec output classification(30), rtype 2, forus FALSE, sendself FALSE, mtu 0
fwdchk FALSE
,IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 192, output feature
,IPSec: to crypto engine(64), rtype 2, forus FALSE, sendself FALSE, mtu 0
fwdchk FALSE
,IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 192, output feature
,Post-encryption output features(65), rtype 2, forus FALSE, sendself FALSE
mtu 0, fwdchk FALSE
```

```
IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 192, post-encap
 feature, (1), rtype 2, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 192, post-encap
,feature, FastEther Channel(3), rtype 2, forus FALSE, sendself FALSE, mtu 0
                                                              fwdchk FALSE
IP: s=192.168.0.1 (local), d=10.0.0.2 (Ethernet0/0), len 192, sending full
                                                                    packet
```

وإليكم ما يحدث:

تضرب حركة المرور المهمة PBR على E0/0 وتثير رمز التشفير لإرسال حزمة ISAKMP. أن ISAKMP وجهت ربط محلي سياسة، ومخرج قارن عينت ب PBR محلي. تم بناء نفق.

فيما يلي إختبار اتصال آخر من R4 إلى 192.168.200.1:

```
R4#ping 192.168.200.1
```

فيما يلي تصحيح الأخطاء على R1:

```
,IP: s=192.168.100.1 (Ethernet0/1), d=192.168.200.1 (Ethernet0/0), len 100
,input feature, Policy Routing(68), rtype 2, forus FALSE, sendself FALSE, mtu 0
                                                              fwdchk FALSE
,IP: s=192.168.100.1 (Ethernet0/1), d=192.168.200.1 (Ethernet0/0), len 100
,input feature, MCI Check(73), rtype 2, forus FALSE, sendself FALSE, mtu 0
                                                              fwdchk FALSE
,IP: s=192.168.100.1 (Ethernet0/1), d=192.168.200.1 (Ethernet0/0), len 100
output feature, IPSec output classification(30), rtype 2, forus FALSE, sendself
                                                    FALSE, mtu 0, fwdchk FALSE
,IP: s=192.168.100.1, d=192.168.200.1, pak EF722068 consumed in output feature
  packet consumed, IPSec: to crypto engine(64), rtype 2, forus FALSE, sendself
                                                    FALSE, mtu 0, fwdchk FALSE
IP: s=192.168.0.1 (Ethernet0/1), d=10.0.0.2 (Ethernet0/0), len 172, input
,feature, Policy Routing(68), rtype 2, forus FALSE, sendself FALSE, mtu 0
                                                              fwdchk FALSE
IP: s=192.168.0.1 (Ethernet0/1), d=10.0.0.2 (Ethernet0/0), len 172, input
     ,feature, MCI Check(73), rtype 2, forus FALSE, sendself FALSE, mtu 0
                                                              fwdchk FALSE
IP: s=192.168.0.1 (Ethernet0/1), d=10.0.0.2 (Ethernet0/0), len 172, output
,feature, IPSec output classification(30), rtype 2, forus FALSE, sendself FALSE
                                                        mtu 0, fwdchk FALSE
IP: s=192.168.0.1 (Ethernet0/1), d=10.0.0.2 (Ethernet0/0), len 172, output
,feature, IPSec: to crypto engine(64), rtype 2, forus FALSE, sendself FALSE
                                                        mtu 0, fwdchk FALSE
IP: s=192.168.0.1 (Ethernet0/1), d=10.0.0.2 (Ethernet0/0), len 172, output
feature, Post-encryption output features(65), rtype 2, forus FALSE, sendself
                                                    FALSE, mtu 0, fwdchk FALSE
IP: s=192.168.0.1 (Ethernet0/1), d=10.0.0.2 (Ethernet0/0), g=192.168.0.2, len
                                                          forward ,172
IP: s=192.168.0.1 (Ethernet0/1), d=10.0.0.2 (Ethernet0/0), len 172, post-encap
 feature, (1), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
IP: s=192.168.0.1 (Ethernet0/1), d=10.0.0.2 (Ethernet0/0), len 172, post-encap
,feature, FastEther Channel(3), rtype 0, forus FALSE, sendself FALSE, mtu 0
                                                              fwdchk FALSE
,IP: s=192.168.0.1 (Ethernet0/1), d=10.0.0.2 (Ethernet0/0), len 172
                                                    sending full packet
```

وإليكم ما يحدث:

تضرب حركة المرور المهمة PBR على E0/0، وأن PBR يحدد واجهة المخرج (E0/0). في E0/0، يتم إستهلاك الحزمة من قبل IPSec وتغليفها. بعد التحقق من الحزمة التي يتم تغليفها مقابل قاعدة PBR نفسها وتحديد واجهة المخرج، يتم إرسال الحزمة واستقبالها بشكل صحيح.

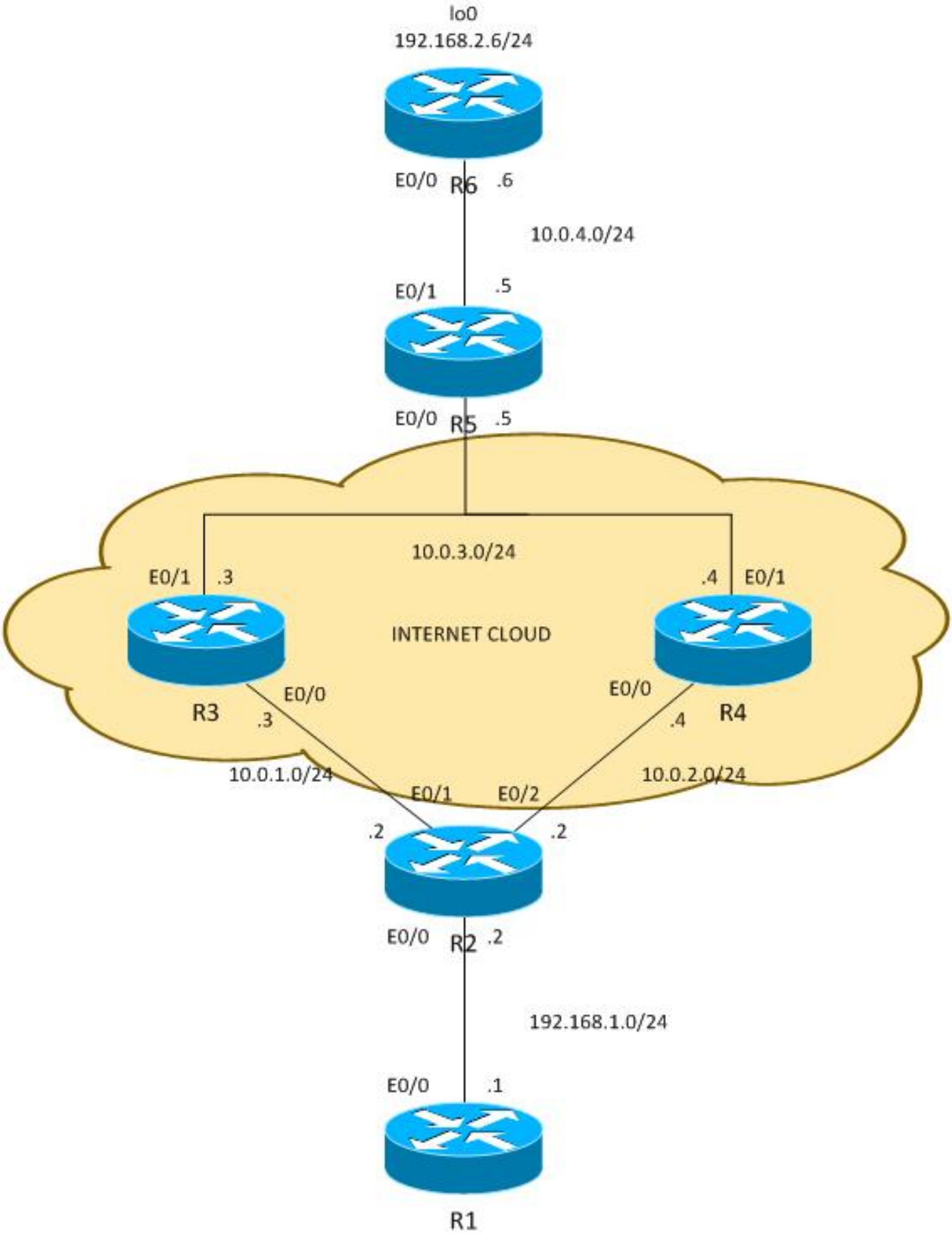
ملخص لاختلافات السلوك

بالنسبة لحركة المرور التي تم إنشاؤها محليا، يتم تحديد واجهة الخروج لحركة المرور غير المدمجة (ISAKMP) بواسطة PBR المحلية. لحركة المرور التي تم إنشاؤها محليا، يتم تحديد واجهة الخروج لحركة المرور بعد التضمين (ESP) بواسطة جداول التوجيه (لم يتم تحديد PBR المحلي). لحركة مرور النقل، يتم تحديد واجهة الخروج لحركة مرور ما بعد التضمين (ESP) بواسطة واجهة PBR (مرتين، قبل وبعد التضمين).

مثال على التكوين

هذا مثال تكوين عملي يعرض المشاكل التي قد تواجهها مع PBR و PBR المحلي مع VPN. يحتوي CE) R2) على إرتباطات ISP. كما يحتوي الموجه R6 أيضا على CE وارتباط ISP واحد. يتم إستخدام الارتباط الأول من R2 إلى R3 كمسار افتراضي للملقم R2. ويتم إستخدام الارتباط الثاني إلى R4 فقط لحركة مرور شبكات VPN إلى R6. في حال أي فشل لارتباط ISP، تتم إعادة توجيه حركة مرور البيانات إلى الارتباط الآخر.

طوبولوجيا



التكوين

تتم حماية حركة المرور بين 24/192.168.1.0 و 24/192.168.2.0. يتم إستخدام أقصر مسار أولا (OSPF) في سحابة الإنترنت للإعلان عن عناوين 8/10.0.0.0، التي يتم معالجتها كعناوين عامة يتم تعيينها من قبل ISP إلى

العميل. في العالم الحقيقي، يتم إستخدام بروتوكول BGP بدلا من OSPF.

يعتمد التكوين في R2 و R6 على خريطة التشفير. في R2، يتم إستخدام PBR على E0/0 لتوجيه حركة مرور VPN إلى R4 إذا كانت فوق:

```
route-map PBR permit 10
 match ip address cmap
set ip next-hop verify-availability 10.0.2.4 1 track 20

ip access-list extended cmap
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

crypto map cmap 10 ipsec-isakmp
 set peer 10.0.4.6
set transform-set TS
 match address cmap

interface Ethernet0/0
ip address 192.168.1.2 255.255.255.0
 ip nat inside
ip virtual-reassembly in
ip policy route-map PBR
```

هنا ترون أن PBR المحلي ليس ضروريا. تقوم الواجهة PBR بتوجيه حركة مرور مثيرة إلى 10.0.2.4. وهذا يؤدي إلى تشغيل رمز التشفير لبدء ISAKMP من الواجهة الصحيحة (الارتباط إلى R4)، حتى عندما يكون التوجيه إلى نقاط النظير البعيدة من خلال R3.

في R6، يتم إستخدام نظامين للشبكة الخاصة الظاهرية (VPN):

```
crypto map cmap 10 ipsec-isakmp
set peer 10.0.2.2             !primary
 set peer 10.0.1.2
set transform-set TS
 match address cmap
```

يستخدم R2 إتفاقية مستوى خدمة IP (SLA) من أجل إختبار اتصال R3 و R4. المسار الافتراضي هو R3. في حالة فشل R3، فإنه يختار R4:

```
ip sla 10
 icmp-echo 10.0.1.3
ip sla schedule 10 life forever start-time now
ip sla 20
 icmp-echo 10.0.2.4
ip sla schedule 20 life forever start-time now

track 10 ip sla 10
track 20 ip sla 20

ip route 0.0.0.0 0.0.0.0 10.0.1.3 track 10
ip route 0.0.0.0 0.0.0.0 10.0.2.4 100
```

كما يتيح R2 الوصول إلى الإنترنت لجميع المستخدمين الداخليين. لتحقيق التكرار في الحالة التي تم فيها إيقاف ISP إلى R3، يلزم وجود خريطة مسار. هو أيسر عنوان ترجمة (ضرب) داخل حركة مرور إلى مخرج قارن مختلف (ضرب إلى E0/1 قارن عندما R3 يكون up و التقصير ممر نقاط إلى R3، و ضرب أن يواجه E0/2 عندما R3 يكون أسفل و R4 استعملت كمسار افتراضي).

```
ip access-list extended pat
deny   ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

```
 deny   udp any any eq isakmp
 deny   udp any eq isakmp any
           permit ip any any

      route-map RMAP2 permit 10
          match ip address pat
    match interface Ethernet0/2
                                !
      route-map RMAP1 permit 10
          match ip address pat
    match interface Ethernet0/1

ip nat inside source route-map RMAP1 interface Ethernet0/1 overload
ip nat inside source route-map RMAP2 interface Ethernet0/2 overload

                      interface Ethernet0/0
 ip address 192.168.1.2 255.255.255.0
                           ip nat inside
                 ip virtual-reassembly in
                  ip policy route-map PBR

                      interface Ethernet0/1
   ip address 10.0.1.2 255.255.255.0
                          ip nat outside
                 ip virtual-reassembly in
                          crypto map cmap

                      interface Ethernet0/2
   ip address 10.0.2.2 255.255.255.0
                          ip nat outside
                 ip virtual-reassembly in
                          crypto map cmap
```

يلزم إستثناء حركة مرور شبكات VPN من الترجمة كما هو الحال مع بروتوكول ISAKMP. إن لا استثنيت حركة مرور ISAKMP من الترجمة، هو ضرب إلى القارن خارجي أن يذهب إلى R3:

```
                                R2#show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
udp 10.0.1.2:500       10.0.2.2:500       10.0.4.6:500       10.0.4.6:500

  Jun  8 09:09:37.779: IP: s=10.0.2.2 (local), d=10.0.4.6, len 196, local*
 feature, NAT(2), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
   ,(Jun  8 09:09:37.779: IP: s=10.0.2.2 (local), d=10.0.4.6 (Ethernet0/1*
                                                          len 196, sending
,Jun  8 09:09:37.779: IP: s=10.0.1.2 (local), d=10.0.4.6 (Ethernet0/1), len 196*
    output feature, Post-routing NAT Outside(24), rtype 1, forus FALSE, sendself
                                                  FALSE, mtu 0, fwdchk FALSE
,Jun  8 09:09:37.779: IP: s=10.0.1.2 (local), d=10.0.4.6 (Ethernet0/1), len 196*
    ,output feature, Common Flow Table(27), rtype 1, forus FALSE, sendself FALSE
                                                      mtu 0, fwdchk FALSE
,Jun  8 09:09:37.779: IP: s=10.0.1.2 (local), d=10.0.4.6 (Ethernet0/1), len 196*
  ,output feature, Stateful Inspection(28), rtype 1, forus FALSE, sendself FALSE
                                                      mtu 0, fwdchk FALSE
,Jun  8 09:09:37.779: IP: s=10.0.1.2 (local), d=10.0.4.6 (Ethernet0/1), len 196*
 output feature, IPSec output classification(34), rtype 1, forus FALSE, sendself
                                                  FALSE, mtu 0, fwdchk FALSE
,Jun  8 09:09:37.779: IP: s=10.0.1.2 (local), d=10.0.4.6 (Ethernet0/1), len 196*
 ,output feature, NAT ALG proxy(59), rtype 1, forus FALSE, sendself FALSE, mtu 0
                                                      fwdchk FALSE
,Jun  8 09:09:37.779: IP: s=10.0.1.2 (local), d=10.0.4.6 (Ethernet0/1), len 196*
,output feature, IPSec: to crypto engine(75), rtype 1, forus FALSE, sendself FALSE
                                                      mtu 0, fwdchk FALSE
,Jun  8 09:09:37.779: IP: s=10.0.1.2 (local), d=10.0.4.6 (Ethernet0/1), len 196*
```

```
output feature, Post-encryption output features(76), rtype 1, forus FALSE, sendself
                                                                FALSE, mtu 0, fwdchk FALSE
   ,Jun  8 09:09:37.779: IP: s=10.0.1.2 (local), d=10.0.4.6 (Ethernet0/1), len 196*
    ,pre-encap feature, IPSec Output Encap(1), rtype 1, forus FALSE, sendself FALSE
                                                             mtu 0, fwdchk FALSE
   ,Jun  8 09:09:37.779: IP: s=10.0.1.2 (local), d=10.0.4.6 (Ethernet0/1), len 196*
,pre-encap feature, Crypto Engine(3), rtype 1, forus FALSE, sendself FALSE, mtu 0
                                                                   fwdchk FALSE
   ,Jun  8 09:09:37.779: IP: s=10.0.1.2 (local), d=10.0.4.6 (Ethernet0/1), len 196*
                                                             sending full packet
```

إختبار

باستخدام هذا التكوين، هناك تكرار كامل. تستخدم الشبكة الخاصة الظاهرية (VPN) الارتباط R4، ويتم توجيه باقي حركة مرور البيانات مع R3. في حالة فشل R4، يتم إنشاء حركة مرور VPN باستخدام الارتباط R3 (لا تتطابق خريطة المسار ل PBR ويتم إستخدام التوجيه الافتراضي).

قبل أن يتعطل ISP إلى R4، يرى R6 حركة مرور من النظير 10.0.2.2:

```
R6#show crypto session
Crypto session current status

Interface: Ethernet0/0
Session status: UP-ACTIVE
Peer: 10.0.2.2 port 500
  IKEv1 SA: local 10.0.4.6/500 remote 10.0.2.2/500 Active
  IPSEC FLOW: permit ip 192.168.2.0/255.255.255.0 192.168.1.0/255.255.255.0
        Active SAs: 2, origin: crypto map
```

بعد أن يستخدم ISP R2 إلى R3 لحركة مرور VPN، يرى R6 حركة مرور من النظير 10.0.1.2:

```
R6#show crypto session
Crypto session current status

Interface: Ethernet0/0
Session status: UP-ACTIVE
Peer: 10.0.1.2 port 500
  IKEv1 SA: local 10.0.4.6/500 remote 10.0.1.2/500 Active
  IPSEC FLOW: permit ip 192.168.2.0/255.255.255.0 192.168.1.0/255.255.255.0
        Active SAs: 2, origin: crypto map
```

أما بالنسبة للسيناريو المعاكس، فعندما ينقطع الارتباط بالخادم طراز R3، فإن كل شيء لا يزال يعمل على ما يرام. لا تزال حركة مرور VPN تستخدم الارتباط إلى R4. أنجزت شبكة عنوان ترجمة (nat) ل 24/192.168.1.0 أن ضرب in order to انتسبت العنوان خارجي. قبل انخفاض R3، توجد ترجمة إلى 10.0.1.2:

```
R2#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
    icmp 10.0.1.2:1        192.168.1.1:1      10.0.4.6:1         10.0.4.6:1
```

بعد تنزيل R3، لا تزال هناك الترجمة القديمة إلى جانب الترجمة الجديدة (إلى 10.0.2.2) التي تستخدم الارتباط باتجاه R4:

```
R2#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
    icmp 10.0.2.2:0        192.168.1.1:0      10.0.4.6:0         10.0.4.6:0
    icmp 10.0.1.2:1        192.168.1.1:1      10.0.4.6:1         10.0.4.6:1
```

مزالق

إذا كان كل شيء على ما يرام، فأين العثرات؟ إنها في التفاصيل.

حركة المرور التي تم إنشاؤها محليا

هنا سيناريو يحتاج إلى بدء حركة مرور VPN من R2 نفسه. يتطلب هذا السيناريو تكوين PBR المحلي على R2 لإجبار R2 على إرسال حركة مرور ISAKMP عبر R4 والتسبب في إرتفاع النفق. ولكن يتم تحديد واجهة الخروج باستخدام جداول التوجيه، مع الإشارة الافتراضية إلى R3، ويتم إرسال الحزمة إلى R3، بدلا من R4، والتي يتم إستخدامها للنقل لشبكة VPN. دخلت in order to دققت أن،:

```
ip access-list extended isakmp
 permit udp any any eq isakmp
 permit udp any eq isakmp any
          permit icmp any any

route-map LOCAL-PBR permit 10
     match ip address isakmp
set ip next-hop verify-availability 10.0.2.4 1 track 20

ip local policy route-map LOCAL-PBR
```

في هذا المثال، يتم فرض بروتوكول رسائل التحكم في الإنترنت (ICMP) الذي يتم إنشاؤه محليا عبر R4. وبدون ذلك، تتم معالجة حركة المرور التي تم إنشاؤها محليا من 192.168.1.2 إلى 192.168.2.5 باستخدام جداول التوجيه ويتم إنشاء نفق مع R3.

ماذا يحدث بعد تطبيق هذا التكوين؟ يتم وضع حزمة ICMP من 192.168.1.2 إلى 192.168.2.5 باتجاه R4، ويبدأ نفق مع الارتباط ب R4. تم إعداد النفق:

```
R2#ping 192.168.2.6 source e0/0 repeat 10
.Type escape sequence to abort
:Sending 10, 100-byte ICMP Echos to 192.168.2.6, timeout is 2 seconds
Packet sent with a source address of 192.168.1.2
!!!!!!!!!.
Success rate is 90 percent (9/10), round-trip min/avg/max = 4/4/5 ms

R2#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Ethernet0/1
Session status: DOWN
(Peer: 10.0.4.6 port 500 fvrf: (none) ivrf: (none
(Desc: (none
(Phase1_id: (none
IPSEC FLOW: permit ip 192.168.1.0/255.255.255.0 192.168.2.0/255.255.255.0
Active SAs: 0, origin: crypto map
Inbound:  #pkts dec"ed 0 drop 0 life (KB/Sec) 0/0
Outbound: #pkts enc"ed 0 drop 0 life (KB/Sec) 0/0
```

```
                                        Interface: Ethernet0/2
                                             Uptime: 00:00:06
                                    Session status: UP-ACTIVE
                          (Peer: 10.0.4.6 port 500 fvrf: (none) ivrf: (none
                                           Phase1_id: 10.0.4.6
                                                  (Desc: (none
                    IKEv1 SA: local 10.0.2.2/500 remote 10.0.4.6/500 Active
                  Capabilities:(none) connid:1009 lifetime:23:59:53
                  IKEv1 SA: local 10.0.2.2/500 remote 10.0.4.6/500 Inactive
                        Capabilities:(none) connid:1008 lifetime:0
IPSEC FLOW: permit ip 192.168.1.0/255.255.255.0 192.168.2.0/255.255.255.0
                                       Active SAs: 2, origin: crypto map
           Inbound:  #pkts dec"ed 9 drop 0 life (KB/Sec) 4298956/3593
           Outbound: #pkts enc"ed 9 drop 0 life (KB/Sec) 4298956/3593
```

يبدو أن كل شيء يعمل بشكل صحيح. يتم إرسال حركة المرور بالارتباط الصحيح E0/2 تجاه R4. توضح حتى R6 أنه يتم تلقي حركة المرور من 10.2.2.2، وهو عنوان IP الخاص برابط R4:

```
R6#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
   X - IKE Extended Authentication, F - IKE Fragmentation

                                        Interface: Ethernet0/0
                                             Uptime: 14:50:38
                                    Session status: UP-ACTIVE
                          (Peer: 10.0.2.2 port 500 fvrf: (none) ivrf: (none
                                           Phase1_id: 10.0.2.2
                                                  (Desc: (none
                    IKEv1 SA: local 10.0.4.6/500 remote 10.0.2.2/500 Active
                  Capabilities:(none) connid:1009 lifetime:23:57:13
IPSEC FLOW: permit ip 192.168.2.0/255.255.255.0 192.168.1.0/255.255.255.0
                                       Active SAs: 2, origin: crypto map
           Inbound:  #pkts dec"ed 1034 drop 0 life (KB/Sec) 4360587/3433
           Outbound: #pkts enc"ed 1029 drop 0 life (KB/Sec) 4360587/3433
```

ولكن في الواقع، يوجد **توجيه غير متناظر لحزم ESP** هنا. يتم إرسال حزم ESP مع 10.0.2.2 كمصدر، ولكن يتم وضعها على الارتباط باتجاه R3. يتم إرجاع إستجابة مشفرة من خلال R4. يمكن التحقق من هذا الإجراء من خلال عدادات التحقق من R3 و R4:

عدادات R3 ل E0/0 قبل إرسال 100 حزمة:

```
R3#show int e0/0 | i pack
  minute input rate 0 bits/sec, 0 packets/sec 5
  minute output rate 0 bits/sec, 0 packets/sec 5
    packets input, 145041 bytes, 0 no buffer 739
  input packets with dribble condition detected 0
  packets output, 243709 bytes, 0 underruns 1918
```

ونفس العدادات، بعد إرسال 100 حزمة:

```
R3#show int e0/0 | i pack
  minute input rate 0 bits/sec, 0 packets/sec 5
  minute output rate 0 bits/sec, 0 packets/sec 5
    packets input, 163241 bytes, 0 no buffer 839
```

```
input packets with dribble condition detected 0
packets output, 243859 bytes, 0 underruns 1920
```

زاد عدد الحزم الواردة بمقدار 100 (على الارتباط باتجاه R2)، ولكن الحزم الصادرة زادت بمقدار 2 فقط. لذلك لا يرى R3 إلا صدى ICMP المشفر.

تظهر الاستجابة على R4، قبل إرسال 100 حزمة:

```
R4#show int e0/0 | i packet
    minute input rate 0 bits/sec, 0 packets/sec 5
  minute output rate 1000 bits/sec, 1 packets/sec 5
    packets input, 150793 bytes, 0 no buffer 793
  input packets with dribble condition detected 0
  packets output, 209111 bytes, 0 underruns 1751
```

بعد إرسال 100 حزمة:

```
R4#show int e0/0 | i packet
    minute input rate 0 bits/sec, 0 packets/sec 5
  minute output rate 0 bits/sec, 0 packets/sec 5
    packets input, 150793 bytes, 0 no buffer 793
  input packets with dribble condition detected 0
  packets output, 227461 bytes, 0 underruns 1853
```

زاد عدد الحزم المرسلة نحو R2 بمقدار 102 (رد ICMP المشفر)، بينما زادت الحزم المستلمة بمقدار 0. لذلك لا يرى R4 إلا رد ICMP المشفر. وبالطبع، يؤكد التقاط الحزمة هذا.

لماذا يحدث هذا؟ الجواب هو في الجزء الاول من المقالة.

وفيما يلي تدفق حزم ICMP هذه:

1. يتم وضع ICMP من 192.168.1.2 إلى 192.168.2.6 على E0/2 (الوصلة نحو R4) بسبب PBR المحلي.
2. يتم بناء جلسة عمل ISAKMP باستخدام 10.0.2.2 ويتم وضعها على إرتباط E0/2 كما هو متوقع.
3. بالنسبة لحزم ICMP بعد التضمين، يحتاج الموجه إلى تحديد واجهة المخرج، والتي يتم إجراؤها باستخدام جداول التوجيه التي تشير إلى R3. هذا هو السبب في إرسال الحزمة المشفرة مع المصدر 10.0.2.2 (الرابط نحو R4) عبر R3.
4. يتلقى R6 حزمة ESP من 10.0.2.2، والتي تتماشى مع جلسة ISAKMP، وتفك تشفير الحزمة، وترسل إستجابة ESP إلى 10.0.2.2.
5. بسبب التوجيه، يرسل R5 إستجابة إلى 10.0.2.2 عبر R4.
6. يستلمه R2 ويفك تشفيرها، ويتم قبول الحزمة.

ولهذا السبب من المهم توخي المزيد من الحذر في حركة المرور التي يتم إنشاؤها محليا.

في العديد من الشبكات، يتم إستخدام إعادة توجيه المسار العكسي للبث الأحادي (uRPF) ويمكن إسقاط حركة المرور المستمدة من 10.0.2.2 على E0/0 من R3. في هذه الحالة، إختبار الاتصال لا يعمل.

هل من حل لهذه المشكلة؟ من الممكن إجبار الموجه على التعامل مع حركة المرور التي تم إنشاؤها محليا على أنها حركة مرور عابرة. ولهذا السبب، تحتاج PBR المحلية إلى توجيه حركة المرور إلى واجهة إسترجاع وهمية يتم توجيهها منها مثل حركة مرور النقل.

وهذا غير مستحسن.

ملاحظة: من المهم أن تكون حذرا عندما تستخدم NAT مع PBR (راجع القسم السابق حول حركة مرور ISKMP في قائمة وصول PAT).

مثال التكوين بدون PBR

وهناك أيضا حل آخر لا يخلو من التسوية. باستخدام نفس الطبولوجيا كالمثال السابق، من الممكن استيفاء جميع المتطلبات بدون إستخدام PBR أو PBR المحلي. بالنسبة إلى هذا المسرح، يتم إستخدام التوجيه فقط. تتم إضافة إدخال توجيه إضافي واحد فقط على R2، ويتم إزالة جميع تكوينات PBR/PBR المحلية:

```
ip route 192.168.2.0 255.255.255.0 10.0.2.4 track 20
```

بشكل إجمالي، يحتوي R2 على تكوين التوجيه هذا:

```
ip route 0.0.0.0 0.0.0.0 10.0.1.3 track 10
ip route 0.0.0.0 0.0.0.0 10.0.2.4 100
ip route 192.168.2.0 255.255.255.0 10.0.2.4 track 20
```

يكون إدخال التوجيه الأول عبارة عن توجيه افتراضي نحو R3، عندما يكون الارتباط إلى R3 قيد التشغيل. ويمثل إدخال التوجيه الثاني المسار الافتراضي للنسخ الاحتياطي تجاه R4، عند تعطل الارتباط إلى R3. ويقرر الإدخال الثالث الطريقة التي يتم بها إرسال حركة المرور إلى شبكة VPN البعيدة، وفقا لحالة الارتباط R4 (إذا كان إرتباط R4 قيد التشغيل، فسيتم إرسال حركة مرور البيانات إلى شبكة VPN البعيدة عبر R4). مع هذا التكوين، لا توجد حاجة لتوجيه السياسة.

ما هو العائق؟ لم يعد هناك أي تحكم متعدد المستويات باستخدام PBR. لا يمكن تحديد عنوان المصدر. في هذه الحالة، يتم إرسال حركة المرور إلى 24/192.168.2.0 نحو R4 عندما تكون قيد التشغيل، بغض النظر عن المصدر. وفي المثال السابق، كان ذلك خاضعا للرقابة من جانب PBR والمصدر المحدد: 24/192.168.1.0 محدد.

ما هو السيناريو الذي يعتبر هذا الحل بسيطا للغاية؟ لشبكات LAN متعددة (خلف R2). عندما تحتاج بعض هذه الشبكات إلى الوصول إلى 24/192.168.2.0 بطريقة آمنة (مشفرة) وغيرها من الطرق غير الآمنة (غير مشفرة)، فإن حركة مرور البيانات من الشبكات غير الآمنة لا تزال توضع على واجهة E0/2 ل R2 ولا تصل إلى خريطة التشفير. لذلك يتم إرسالها دون تشفير عبر إرتباط إلى R4 (وكان المتطلب الأساسي هو إستخدام R4 فقط لحركة المرور المشفرة).

هذا النوع من السيناريو ومتطلباته نادرة، ولهذا السبب يتم إستخدام هذا الحل بشكل متكرر إلى حد ما.

ملخص

قد يكون إستخدام مميزات PBR و PBR المحلية بالإضافة إلى شبكات VPN و NAT معقدا ويتطلب فهما متعمقا لتدفق الحزمة.

بالنسبة لسيناريوهات مثل السيناريوهات المقدمة هنا، يوصى باستخدام موجهين منفصلين - كل موجه مع إرتباط ISP واحد. في حالة فشل ISP، يمكن إعادة توجيه حركة المرور بسهولة. ولا توجد حاجة إلى عمليات إعادة البناء وإعادة البناء، والتصميم العام أبسط بكثير.

هناك أيضا حل توفيقي لا يتطلب إستخدام PBR، ولكنه يستخدم التوجيه العائم الثابت بدلا من ذلك.

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems
- IOS 15.3 M&T- 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).