فهم توجيه السياسات

المحتويات

المقدمة

يوفر التوجيه القائم على السياسة أداة لإعادة توجيه حزم البيانات وتوجيهها استنادا إلى السياسات التي يحددها مسؤولو الشبكة. وفي الواقع، فإنها طريقة لاتخاذ قرارات بروتوكول التوجيه الخاصة بالسياسة وتجاوز هذا الأمر. يتضمن التوجيه القائم على السياسة آلية لتطبيق السياسات بشكل انتقائي استنادا إلى قائمة الوصول أو حجم الحزمة أو معايير أخرى. يمكن أن تتضمن الإجراءات المتخذة حزم التوجيه على المسارات المعرفة من قبل المستخدم، وتعيين الأولوية ونوع وحدات بت الخدمة، وما إلى ذلك.

في هذا المستند، يتم إستخدام جدار حماية لترجمة 8/10.0.0.0 العناوين الخاصة إلى عناوين قابلة للتوجيه عبر الإنترنت تنتمي إلى الشبكة الفرعية 24/172.16.255.0. راجع الرسم التخطيطي أدناه للحصول على شرح مرئي.

راجع التوجيه المستند إلى السياسة للحصول على مزيد من المعلومات.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقيد هذا وثيقة إلى أي جهاز خاص أو برمجية صيغة.

تستند المعلومات الموضحة في هذا المستند إلى إصدارات البرامج والمكونات المادية أدناه.

- برنامج IOS® الإصدار 12.3(3) من Cisco
- الموجّهات من السلسلة 2500 من Cisco

تم إنشاء المعلومات المُقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير

المحتمل لأي أمر قبل استخدامه.

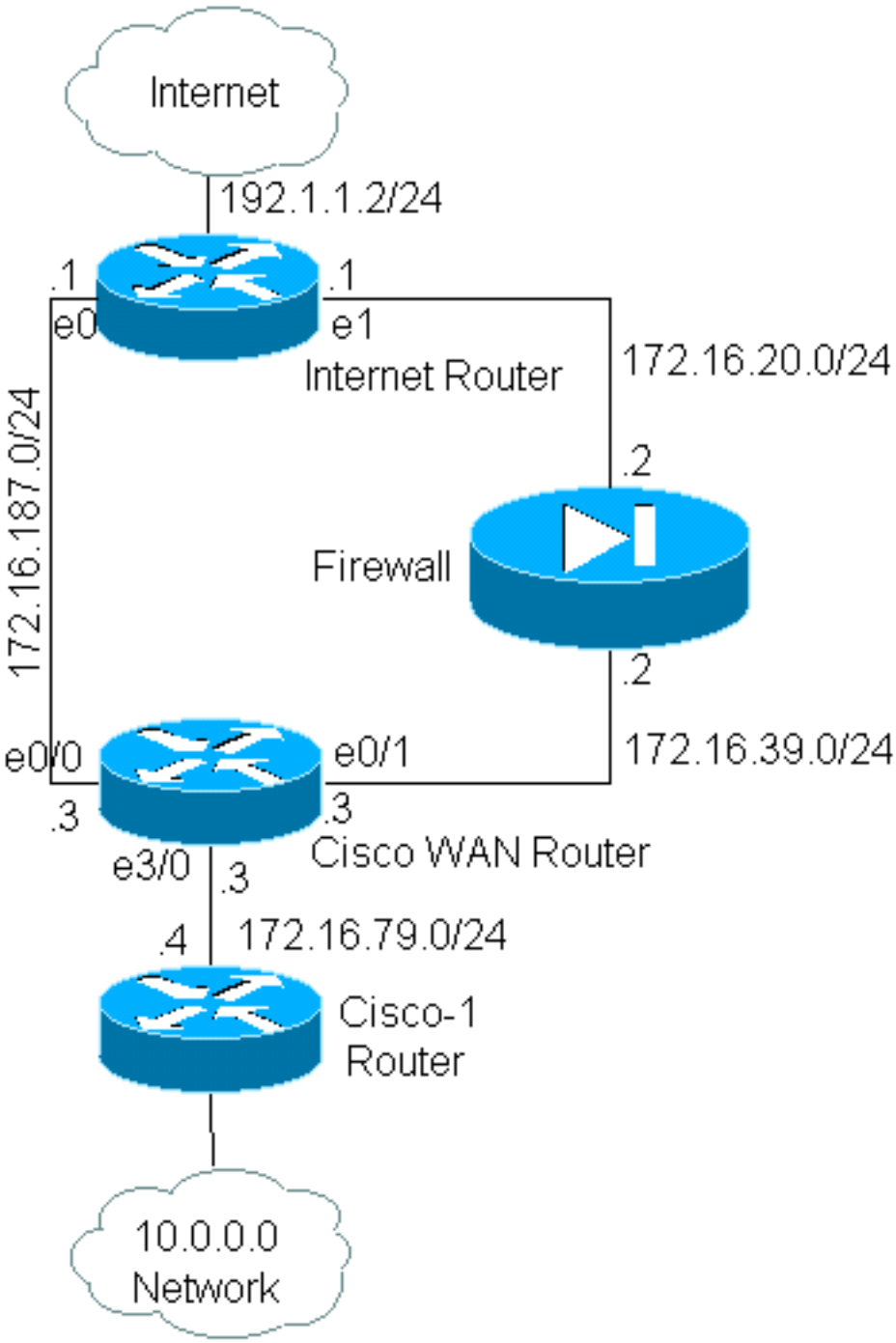
الاصطلاحات

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

التكوينات

في هذا المثال، مع التوجيه العادي، ستأخذ جميع الحزم من 8/10.0.0.0 شبكة إلى الإنترنت المسار من خلال واجهة إيثرنت 0/0 لموجه Cisco WAN (عبر الشبكة الفرعية 24/172.16.187.0) لأنه أفضل مسار بأقل القياسات. باستخدام التوجيه المستند إلى السياسة، نريد أن تأخذ هذه الحزم المسار من خلال جدار الحماية إلى الإنترنت، ويجب تجاوز سلوك التوجيه العادي عن طريق تكوين توجيه السياسة. يترجم جدار الحماية جميع الحزم من 8/10.0.0.0 إلى الإنترنت، وهو على الرغم من ذلك غير ضروري لتوجيه السياسة للعمل.

الرسم التخطيطي للشبكة



تكوين جدار الحماية

تم تضمين تكوين جدار الحماية أدناه لتوفير صورة كاملة. ومع ذلك، فإنه ليس جزءا من مشكلة توجيه السياسة الموضحة في هذا المستند. يمكن بسهولة إستبدال جدار الحماية في هذا المثال بجهاز PIX أو جهاز جدار حماية آخر.

```
!
ip nat pool net-10 172.16.255.1 172.16.255.254 prefix-length 24
ip nat inside source list 1 pool net-10
!
interface Ethernet0
ip address 172.16.20.2 255.255.255.0
ip nat outside
!
interface Ethernet1
ip address 172.16.39.2 255.255.255.0
```

```
 ip nat inside
 !
 router eigrp 1
 redistribute static
 network 172.16.0.0
 default-metric 10000 100 255 1 1500
 !
 ip route 172.16.255.0 255.255.255.0 Null0
 access-list 1 permit 10.0.0.0 0.255.255.255
 !
 end
```

راجع أوامر عنونة خدمات IP للحصول على مزيد من المعلومات حول الأوامر ذات الصلة **ip nat**

في هذا المثال، يقوم موجه Cisco WAN بتشغيل توجيه السياسات لضمان إرسال حزم IP التي تنشأ من الشبكة 8/10.0.0.0 من خلال جدار الحماية. يحتوي التكوين أدناه على بيان قائمة الوصول التي ترسل الحزم التي تنشأ من شبكة 8/10.0.0.0 إلى جدار الحماية.

تكوين Cisco_WAN_Router

```
 !
 interface Ethernet0/0
 ip address 172.16.187.3 255.255.255.0
 no ip directed-broadcast
 !
 interface Ethernet0/1
 ip address 172.16.39.3 255.255.255.0
 no ip directed-broadcast
 !
 interface Ethernet3/0
 ip address 172.16.79.3 255.255.255.0
 no ip directed-broadcast
 ip policy route-map net-10
 !
 router eigrp 1
 network 172.16.0.0
 !

access-list 111 permit ip 10.0.0.0 0.255.255.255 any
 !
 route-map net-10 permit 10
 match ip address 111
 set interface Ethernet0/1
 !
 route-map net-10 permit 20
 !
 end
```

ارجع إلى وثائق أمر route-map للحصول على مزيد من المعلومات حول الأوامر ذات الصلة **route-map**.

ملاحظة: لا يدعم PBR الكلمة الأساسية **log** في **access-list**. إذا تم تكوين الكلمة الأساسية **log**، فإنها لا تظهر أي عمليات وصول.

تكوين موجه Cisco-1

```
 !
 version 12.3

 !
```

```
interface Ethernet0

 Interface connecting to 10.0.0.0 network ip address 10.1.1.1 255.0.0.0 ! interface Ethernet1 --!
!-- Interface connecting to Cisco_Wan_Router ip address 172.16.79.4 255.255.255.0 ! router eigrp
1 network 10.0.0.0 network 172.16.0.0 no auto-summary ! !---Output Suppressed
```

تكوين لموجه إنترنت

```
!
version 12.3

!
interface Ethernet1

 Interface connecting to Firewall ip address 172.16.20.1 255.255.255.0 interface Serial0 !--- --!
    Interface connecting to Internet ip address 192.1.1.2 255.255.255.0 clockrate 64000 no fair-
        queue ! interface Ethernet0 !--- Interface connecting to Cisco_Wan_Router ip address
172.16.187.1 255.255.255.0 ! ! router eigrp 1 redistribute static !--- Redistributing the static
       default route for other routers to reach Internet network 172.16.0.0 no auto-summary ! ip
    classless ip route 0.0.0.0 0.0.0.0 192.1.1.1 !-- Static default route pointing to the router
                                                connected to Internet !---Output Suppressed
```

في إختبار هذا المثال، تم إرسال إختبار اتصال من 10.1.1.1 على موجه Cisco-1، باستخدام **الأمر الموسع ping**، إلى مضيف على الإنترنت. في هذا المثال، تم إستخدام 192.1.1.1 كعنوان الوجهة. لرؤية ما يحدث على موجه الإنترنت، تم إيقاف تشغيل التحويل السريع أثناء إستخدام الأمر **debug ip packet 101 detail**.

تحذير: يمكن أن يؤدي إستخدام الأمر **debug ip packet detail** على موجه الإنتاج إلى إستخدام وحدة المعالجة المركزية (CPU) بشكل كبير، مما يمكن أن يؤدي إلى انخفاض حاد في الأداء أو انقطاع في الشبكة. ننصحك بقراءة قسم إستخدام أمر تصحيح الأخطاء بعناية في فهم أوامر إختبار الاتصال و traceroute قبل أن تستخدم أوامر debug.

ملاحظة: يتم إستخدام **تصريح قائمة الوصول 101 ل ICMP أي** عبارة لتصفية إخراج **حزمة IP debug**. بدون قائمة الوصول هذه، يمكن أن يعمل الأمر **debug ip packet** على إنشاء الكثير من المخرجات على وحدة التحكم التي يتم قفل الموجه بها. أستخدم قوائم التحكم في الوصول (ACL) الموسعة عند تكوين PBR. إذا لم يتم تكوين أي قائمة تحكم في الوصول (ACL) من أجل إنشاء معايير المطابقة، فإنها ينتج عنها أن يتم توجيه جميع حركة المرور وفقا للسياسة.

```
:Results of ping from Cisco_1 to 192.1.1.1/internet taken from Internet_Router
Packet never makes it to Internet_Router

Cisco_1# ping
:[Protocol [ip
Target IP address: 192.1.1.1
:[Repeat count [5
:[Datagram size [100
:[Timeout in seconds [2
Extended commands [n]: y
Source address or interface: 10.1.1.1
:[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 192.1.1.1, timeout is 2 seconds
Packet sent with a source address of 10.1.1.1
.....
(Success rate is 0 percent (0/5
```

كما ترى، لم تصل الحزمة أبدا إلى موجه الإنترنت. تظهر أوامر تصحيح الأخطاء أدناه، والمأخوذة من موجه Cisco WAN، سبب حدوث ذلك.

```
:Debug commands run from Cisco_WAN_Router
"debug ip policy"
Mar  1 00:43:08.367: IP: s=10.1.1.1 (Ethernet3/0), d=192.1.1.1, len 100, policy match*
Mar  1 00:43:08.367: IP: route map net-10, item 10, permit*
Packet with source address belonging to 10.0.0.0/8 network !--- is matched by route-map ---!
"net-10" statement 10. *Mar 1 00:43:08.367: IP: s=10.1.1.1 (Ethernet3/0), d=192.1.1.1
(Ethernet0/1), len 100, policy routed *Mar 1 00:43:08.367: Ethernet3/0 to Ethernet0/1 192.1.1.1
!--- matched packets previously are forwarded out of interface !--- ethernet 0/1 by the set
.command
```

تطابق الحزمة مع إدخال النهج 10 في خريطة نهج net-10، كما هو متوقع. لماذا لم تصل الحزمة إلى موجه الإنترنت؟

```
"debug arp"
Mar  1 00:06:09.619: IP ARP: creating incomplete entry for IP address: 192.1.1.1 interface*
Ethernet0/1
,Mar  1 00:06:09.619: IP ARP: sent req src 172.16.39.3 00b0.64cb.eab1*
dst 192.1.1.1 0000.0000.0000 Ethernet0/1
Mar  1 00:06:09.635: IP ARP rep filtered src 192.1.1.1 0010.7b81.0b19, dst 172.16.39.3*
00b0.64cb.eab1 wrong cable, interface Ethernet0/1

Cisco_Wan_Router# show arp
  Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.39.3             -   00b0.64cb.eab1  ARPA   Ethernet0/1
Internet  172.16.39.2             3   0010.7b81.0b19  ARPA   Ethernet0/1
Internet  192.1.1.1                 0   Incomplete      ARPA
```

يعرض إخراج **debug arp** هذا. يحاول موجه Cisco WAN القيام بما تم توجيهه إليه ويحاول وضع الحزم مباشرة على واجهة الإيثرنت 1/0. يتطلب هذا أن يرسل الموجه طلب بروتوكول تحليل العنوان (ARP) لعنوان الوجهة 192.1.1.1، والذي يدرك الموجه أنه ليس على هذه الواجهة، وبالتالي فإن إدخال ARP لهذا العنوان هو "غير مكتمل"، كما هو موضح بواسطة الأمر **show arp**. يقع عملية كبسلة بعد ذلك لأن الموجه غير قادر على وضع الحزمة على السلك بدون إدخال ARP.

من خلال تحديد جدار الحماية على أنه الخطوة التالية، يمكننا منع هذه المشكلة وعمل خريطة المسار كما هو مطلوب:

```
:Config changed on Cisco_WAN_Router
!
route-map net-10 permit 10
match ip address 111
set ip next-hop 172.16.39.2
!
```

باستخدام الأمر **debug ip packet 101 detail** نفسه على موجه الإنترنت، نرى الآن أن الحزمة تأخذ المسار الصحيح. كما يمكننا أن نرى أن الحزمة قد تمت ترجمتها إلى 172.16.255.1 بواسطة جدار الحماية، وأن الجهاز الذي يتم سحبه، 192.1.1.1، قد رد:

```
Cisco_1# ping
:[Protocol [ip
Target IP address: 192.1.1.1
:[Repeat count [5
:[Datagram size [100
:[Timeout in seconds [2
Extended commands [n]: y
Source address or interface: 10.1.1.1
```

```
:[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 192.1.1.1, timeout is 2 seconds
Packet sent with a source address of 10.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/70/76 ms

:Results of ping from Cisco_1 to 192.1.1.1/internet taken from Internet_Router
#Internet_Router
Mar  1 00:06:11.619: IP: s=172.16.255.1 (Ethernet1), d=192.1.1.1 (Serial0), g=192.1.1.1, len*
100, forward
Mar  1 00:06:11.619:     ICMP type=8, code=0*
 Packets sourced from 10.1.1.1 are getting translated to 172.16.255.1 by !--- the Firewall ---!
before it reaches the Internet_Router. *Mar 1 00:06:11.619: *Mar 1 00:06:11.619: IP: s=192.1.1.1
(Serial0), d=172.16.255.1 (Ethernet1), g=172.16.20.2, len 100, forward *Mar 1 00:06:11.619: ICMP
    type=0, code=0 !--- Packets returning from Internet arrive with the destination !--- address
:172.16.255.1 before it reaches the Firewall. *Mar 1 00:06:11.619
```

يظهر الأمر **debug ip policy** على موجه WAN من Cisco أنه تم إعادة توجيه الحزمة إلى جدار الحماية، 172.16.39.2:

يتم تشغيل أوامر تصحيح الأخطاء من Cisco_WAN_Router

```
"debug ip policy"
Mar  1 00:06:11.619: s=10.1.1.1 (Ethernet3/0), d=192.1.1.1, len 100, policy match*
Mar  1 00:06:11.619: IP: route map net-10, item 20, permit*
Mar  1 00:06:11.619: s=10.1.1.1 (Ethernet3/0), d=192.1.1.1 (Ethernet0/1), len 100, policy*
routed
Mar  1 00:06:11.619: Ethernet3/0 to Ethernet0/1 172.16.39.2*
```

التوجيه المستند إلى السياسة لحركة المرور المشفرة

قم بإعادة توجيه حركة المرور التي تم فك تشفيرها إلى واجهة إسترجاع لتوجيه حركة المرور المشفرة استنادا إلى توجيه السياسة ثم قم ب PBR على تلك الواجهة. إذا تم تمرير حركة المرور التي تم تشفيرها عبر نفق VPN، `ip cef` على الواجهة، وإنهاء نفق VPN.

معلومات ذات صلة

- صفحة دعم توجيه IP
- صفحة دعم ترجمة عناوين الشبكة (NAT)
- أدوات الدعم التقني والموارد
- التوجيه القائم على السياسة
- تقنيات IOS من Cisco
- 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).