سلوك قائمة التحكم في الوصول (ACL) في PBR على Nexus 7K يحتوي على كل من معلومات L3 و L4

المحتويات

المقدمة

يصف هذا المستند سلوك التوجيه المستند إلى السياسة (PBR) على محولات Nexus عند التصفية استنادا إلى معلومات الطبقة 3 (L3) والطبقة 4 (L4).

معلومات أساسية

إذا قمت بإضافة تسلسل في PBR لمطابقة معلومات L4 معينة، حيث إن أحد المميزات N7K تقوم بإنشاء إدخالات لإدخال التحكم في الوصول (ACEs) ويتم إنشاء إدخال إدخال التحكم في الوصول (ACE) للجزء التلقائي لمطابقة معلومات L3 المحددة في تسلسل المطابقة. في حالة الحزم المجزأة، تحتوي الحزمة الأولى المعروفة باسم الجزء الأولي على رأس L4 وتطابق بشكل صحيح في قائمة التحكم في الوصول (ACL). ومع ذلك، لا تحتوي الأجزاء التالية المعروفة باسم الأجزاء غير الأولية على أي معلومات حول L4، وبالتالي إذا كان الجزء L3 من إدخال قائمة التحكم في الوصول (ACL) مطابقا، فيتم السماح بالجزء غير الأولي. لذلك ينبغي توخي أقصى درجات الحذر أثناء تصفية حركة المرور استنادا إلى معلومات المستوى 4، حيث إن الأجزاء غير الأولية قد يتم توجيهها بشكل غير صحيح في غياب معلومات المستوى 4.

طوبولوجيا

يتم توصيل موجه شبكة LAN ب Nexus على الواجهة E2.1، VLAN 700. يتمثل المتطلب في إعادة توجيه حركة مرور البيانات التي تطابق بروتوكول إدارة الشبكة البسيط (SNMP) وشبكة الويب وما إلى ذلك إلى أداة التحسين وجميع حركات المرور الأخرى مباشرة من أجل واجهة E2/2 نحو جدار الحماية. يتم تكوين PBR على واجهة المحول الظاهرية (SVI) VLAN700 على جهاز Nexus. يتم توفير التكوين لنفس الإجراء هنا. يقوم التسلسل 70 في خريطة المسار

بإعادة توجيه جميع حركات المرور الأخرى إلى جدار الحماية. هناك متطلب جديد أن كل حركة المرور مع UDP ميناء 920x تحتاج أن تمر عبر المحسن، لذا تسلسل 50 أضفت في خريطة المسار.

راجع هنا كيفية إستجابة PBR للحزم المجزأة وغير المجزأة التي تصل في التسلسل 50 وتطابق كل من معلومات L3 و L4.

هنا التشكيل على Nexus قارن VLAN700 أن يعيد الحركة مرور أن يأتي على E2/1:

```
interface Vlan700

 no shutdown

 mtu 9000

 vrf member ABC

 no ip redirects

 ip address 10.11.25.25/28

 ip policy route-map In_to_Out


Nexus# show route-map In_to_Out

route-map In_to_Out, permit, sequence 3

 Match clauses:

   ip address (access-lists): Toolbar

 Set clauses:

   ip next-hop 10.3.22.13

route-map In_to_Out, permit, sequence 5

 Match clauses:

   ip address (access-lists): Internet

 Set clauses:

   ip next-hop 10.11.25.19

route-map In_to_Out, permit, sequence 7

 Match clauses:

   ip address (access-lists): Web

 Set clauses:

   ip next-hop 10.11.25.19

route-map In_to_Out, permit, sequence 10

 Match clauses:

   ip address (access-lists): In_to_Out_Internet
```

```
 Set clauses:
   ip next-hop 10.11.25.23
route-map In_to_Out, permit, sequence 30
 Match clauses:
   ip address (access-lists): In_to_Out_www
 Set clauses:
   ip next-hop 10.11.25.23
route-map In_to_Out, permit, sequence 35
 Match clauses:
   ip address (access-lists): In_to_Out_https
 Set clauses:
   ip next-hop 10.11.25.23
route-map In_to_Out, permit, sequence 40
 Match clauses:
   ip address (access-lists): In_to_Out_8080
 Set clauses:
   ip next-hop 10.11.25.23
route-map In_to_Out, permit, sequence 50
 Match clauses:
   ip address (access-lists): UDP_Traffic
 Set clauses:
   ip next-hop 10.11.25.23 >>>>>>>>>>>>>>>>>>>> Towards Optimizer
route-map In_to_Out, permit, sequence 70
 Match clauses:
   ip address (access-lists): To_Firewall
 Set clauses:
    ip next-hop . 10.22.45.63 >>>>>>>>>>>>>>>> Towards Firewall


Nexus# show ip access-lists UDP_Traffic
IP access list UDP_Traffic
10 permit udp any any eq 9201
20 permit udp any any eq 9202
```

```
30 permit udp any any eq 9203



Nexus# sh ip access-lists To_Firewall

IP access list To_Firewall

       10 permit ip any any
```

بمجرد تكوين التوجيه المستند إلى السياسة على SVI، يقوم Nexus بإنشاء إدخال في الأجهزة ل نفسه. دعونا الآن ننظر في برمجة الأجهزة ل PBR على الوحدة 2 من Nexus:

```
Nexus# show system internal access-list vlan 700 input entries detail module 2

Flags: F - Fragment entry  E - Port Expansion

      D - DSCP Expansion  M - ACL Expansion

      T - Cross Feature Merge Expansion

INSTANCE 0x0

---------------

 Tcam 1 resource usage:

 ----------------------

 Label_b = 0x201

  Bank 0

  ------

    IPv4 Class

      Policies: PBR(GGSN_Toolbar)

      Netflow profile: 0

      Netflow deny profile: 0

      Entries:

        [Index] Entry [Stats]

        ---------------------

 [0019:000f:000f] prec 1 permit-routed ip 0.0.0.0/0 224.0.0.0/4   [0]

 [002d:0024:0024] prec 1 redirect(0x5d)-routed tcp 1.1.22.80/28 0.0.0.0/0 eq 80 flow-label 80
[0]

 [002e:0025:0025] prec 1 redirect(0x5d)-routed tcp 1.1.22.80/28 0.0.0.0/0 fragment   [0]

 [002f:0026:0026] prec 1 redirect(0x5d)-routed tcp 1.1.22.80/28 0.0.0.0/0 eq 8080 flow-label
8080  [0]

 [0030:0027:0027] prec 1 redirect(0x5d)-routed tcp 1.1.22.80/28 0.0.0.0/0 fragment   [0]

 [0031:0028:0028] prec 1 redirect(0x5d)-routed tcp 1.1.22.48/28 0.0.0.0/0 eq 80 flow-label 80
[0]
```

```
 [0032:0029:0029] prec 1 redirect(0x5d)-routed tcp 1.1.22.48/28 0.0.0.0/0 fragment   [0]

 [0033:002a:002a] prec 1 redirect(0x5d)-routed tcp 1.1.22.48/28 0.0.0.0/0 eq 8080 flow-label
8080  [0]

 [0034:002b:002b] prec 1 redirect(0x5d)-routed tcp 1.1.22.48/28 0.0.0.0/0 fragment   [0]

 [0035:002c:002c] prec 1 permit-routed ip 1.1.22.24/29 0.0.0.0/0   [0]

 [0036:002d:002d] prec 1 permit-routed ip 1.1.22.32/28 0.0.0.0/0   [0]

 [0037:002e:002e] prec 1 permit-routed ip 1.1.22.64/28 0.0.0.0/0   [0]

 [0038:002f:002f] prec 1 permit-routed ip 1.1.22.80/28 0.0.0.0/0   [0]

 [003d:0033:0033] prec 1 permit-routed ip 1.1.22.96/28 0.0.0.0/0   [0]

 [003e:0034:0034] prec 1 permit-routed tcp 0.0.0.0/0 196.11.146.149/32 eq 25 flow-label 25  [0]

 [0059:004f:004f] prec 1 permit-routed tcp 0.0.0.0/0 196.11.146.149/32 fragment   [0]

 [005a:0050:0050] prec 1 redirect(0x5e)-routed ip 1.1.22.16/29 0.0.0.0/0   [0]

 [005b:0051:0051] prec 1 redirect(0x5e)-routed tcp 0.0.0.0/0 0.0.0.0/0 eq 80 flow-label 80  [0]

 [005c:0052:0052] prec 1 redirect(0x5e)-routed tcp 0.0.0.0/0 0.0.0.0/0 fragment   [0]

 [005d:0053:0053] prec 1 redirect(0x5e)-routed tcp 0.0.0.0/0 0.0.0.0/0 eq 443 flow-label 443
[0]

 [005e:0054:0054] prec 1 redirect(0x5e)-routed tcp 0.0.0.0/0 0.0.0.0/0 fragment   [0]

 [005f:0055:0055] prec 1 redirect(0x5e)-routed tcp 0.0.0.0/0 0.0.0.0/0 eq 8080 flow-label 8080
[0]

 [0060:0056:0056] prec 1 redirect(0x5e)-routed tcp 0.0.0.0/0 0.0.0.0/0 fragment   [0]

********************Sequence 50 is to match the traffic for UDP ports
9201/9202/9203**********************

 [0061:0057:0057] prec 1 redirect(0x5e)-routed udp 0.0.0.0/0 0.0.0.0/0 eq 9201 flow-label 9201
[0]

 [0062:0058:0058] prec 1 redirect(0x5e)-routed udp 0.0.0.0/0 0.0.0.0/0 fragment   [0]

 [0063:0059:0059] prec 1 redirect(0x5e)-routed udp 0.0.0.0/0 0.0.0.0/0 eq 9202 flow-label 9202
[0]

 [0064:005a:005a] prec 1 redirect(0x5e)-routed udp 0.0.0.0/0 0.0.0.0/0 fragment   [0]

 [0065:005b:005b] prec 1 redirect(0x5e)-routed udp 0.0.0.0/0 0.0.0.0/0 eq 9203 flow-label 9203
[0]

 [0066:005c:005c] prec 1 redirect(0x5e)-routed udp 0.0.0.0/0 0.0.0.0/0 fragment   [0]

********************Sequence 70 is to send all other traffic to Firewall**********************

 [0067:005d:005d] prec 1 permit-routed ip 0.0.0.0/0 0.0.0.0/0   [23]

 [0068:005e:005e] prec 1 permit-routed ip 0.0.0.0/0 0.0.0.0/0   [0]
```

أنت ترى أن بالإضافة إلى إدخال قائمة الوصول التي تطابق **UDP 0.0.0.0/0 0.0.0.0/0 eq 9201**، هناك إدخال آخر يطابق الأجزاء **udp 0.0.0.0/0 0.0.0.0/0 عزج** ولكن هذا الإدخال لا يحتوي على أي

معلومات عن منفذ UDP. هذا إدخال مكافئ لأي إدخال آخر يطابق حزمة UDP، لذلك فإن الحزم لمنافذ UDP الأخرى يتم مطابقتها أيضا في هذا التسلسل الذي تم إنشاؤه بواسطة الجهاز.

حالة الاختبار 1: بدء حركة المرور من موجه الشبكة المحلية (LAN) نحو جدار الحماية

- كانت الحزمة التي تصل إلى nexus غير مجزأة وبالتالي تطابقت حركة المرور كما هو متوقع في PBR.
- تمت إعادة توجيهها بشكل صحيح إلى جدار الحماية ويمكن رؤيتها في عمليات تصحيح الأخطاء التي يتم تشغيلها على جدار الحماية.

UDP packet -port 500

*Mar 26 04:07:48.959: IP: s=1.1.1.1 (**GigabitEthernet0/0**), d=3.3.3.3, len 28, rcvd 4 -à **Traffic entering from Nexus interface**

*Mar 26 04:07:48.959: UDP src=500, dst=500

TCP packet - port 80

*Mar 26 04:07:48.671: IP: s=1.1.1.1 (**GigabitEthernet0/1**), d=3.3.3.3, len 40, rcvd 4 -à **Traffic entering from Optimizer interface**

*Mar 26 04:07:48.671: TCP src=1720, dst=80, seq=0, ack=0, win=0

UDP packet -port 9201

*Mar 27 09:30:19.879: IP: s=1.1.1.1 (**GigabitEthernet0/1**), d=3.3.3.3, len 28, input feature à **Traffic entering from Optimizer interface**

*Mar 27 09:30:19.879: UDP src=6000, dst=9201, MCI Check(80), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE

حالة الاختبار 2: حركة المرور التي بدأت عبر ملف sniffer من موجه LAN إلى جدار الحماية باستخدام UDP 500

حركة المرور التي تحتوي على جزأين في ملف sniffer الذي تم إنشاؤه هنا:

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	18:40:45.015197	1.1.1.1	3.3.3.3	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=061e)
2	18:40:45.015288	1.1.1.1	3.3.3.3	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=061e)

1. الأجزاء الأولية مع خريطة المسار:

- يعرف الجزء الأول ذو **الإزاحة = 0** باسم الجزء الأولي ويحتوي على رأس UDP في الحزمة.
- بما أن حركة المرور لـ UDP 500، فإنه يتم مضاهاتها في التسلسل 70 للسماح **ip any.**

```
prec 1 permit-routed ip 0.0.0.0/0 0.0.0.0/0   [23]
```

- ذلك يتم توجيه الحزمة الأولى نفسها التي تحتوي على كل من معلومات الطبقة 3 والطبقة 4 بشكل صحيح.

2. حزم الأجزاء غير الأولية مع خريطة المسار:

- يعرف الجزء الثاني ذو **إزاحة ≠ 0** بالجزء غير الأولي والذي يحتوي على أي رأس UDP. هي حزمة IP خالصة مع نوع البروتوكول UDP (17).
- بما أنه لا توجد معلومات عن الطبقة الرابعة، فإنها تطابق في التسلسل 70: **يتم توجيه IP 0.0.0.0/0 0.0.0.0/0.**
- ومع ذلك، في التسلسل 50، هناك قاعدة وصول تطابق حركة مرور منفذ UDP 920x. يقوم الجهاز بإنشاء إدخال تلقائي للسماح بأجزاء UDP التي تطابق معلومات الطبقة 3 المحددة.
- لذلك، كل حزمة مجزأة لأي معلومات من الطبقة 3 باستخدام بروتوكول UDP يتم مطابقتها في التسلسل 50.

```
prec 1 redirect(0x5e)-routed udp 0.0.0.0/0 0.0.0.0/0 eq 9201 flow-label 9201  [0]

prec 1 redirect(0x5e)-routed udp 0.0.0.0/0 0.0.0.0/0 fragment [23]
>>>>>>>>>>>>>>>>>>>>
```

- بهذه الطريقة، هناك جزء يتم توجيهه بشكل صحيح وآخر يتم توجيهه عبر تسلسل خاطئ.
- يتم تعديل الجزء الثاني من أجل جعل **الإزاحة = 0**، ويتم مطابقته في التسلسل 70 كما هو متوقع.
- وهذا سلوك متوقع عند تلقي أجزاء الطبقة الرابعة.
- والقصد من إنشاء مدخل إضافي للسماح بالأجزاء هو السماح باستلام الأجزاء غير الأولية دون معلومات من الطبقة الرابعة.
- في الحالة، كانت حركة المرور لـ UDP 9201 ولم يكن هناك إدخال للسماح بالأجزاء. ثم تطابق الجزء الثاني في التسلسل 70 للسماح **بـ ip any** وبالتالي يتم توجيهه بشكل خاطئ.

```
Nexus# sh route-map In_to_Out pbr-statistics

route-map In_to_Out, permit, sequence 3

 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 5

 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 7

 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 10

 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 30
```

```
 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 35

 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 40

 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 50 ----------> 2nd Fragment for UDP 500 is matched here

 Policy routing matches: 4397 packets

route-map In_to_Out, permit, sequence 70----------> 1st Fragment for UDP 500 is matched here

 Policy routing matches: 4397 packets
```

- يتم إنشاء تسلسل آخر 45 للسماح بحركة المرور ل UDP 500 والملاحظة أن كل الجزأين متطابقان في التسلسل 45.
- تمت مطابقة الجزء الأولي بسبب معلومات رأس UDP والمطابقة غير الأولية في سطر التسلسل 45 للتسلسل الأجزاء.

```
Nexus# sh route-map In_to_Out pbr-statistics

route-map In_to_Out, permit, sequence 3

 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 5

 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 7

 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 10

 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 30

 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 35

 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 40

 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 45----------> Both fragments matched here

 Policy routing matches: 213 packets

route-map In_to_Out, permit, sequence 50
```

```
 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 70

 Policy routing matches: 0 packets


Default routing: 0 packets
```

قائمة الوصول للتسلسل 45:

```
Nexus# sh ip access-lists udptraffic

IP access list udptraffic

permit udp any any eq isakmp
```

3. الآن لنرى كيف تتصرف الأجزاء الرئيسية مع قائمة التحكم في الوصول (ACL) وخريطة المسار

- يتم تطبيق التسلسل 5 للسماح بأي منفذ UDP عشوائي 56 على قائمة التحكم في الوصول (ACL) الخاصة بالمنفذ.

```
Nexus# sh ip access-lists TEST_UDP


IP access list TEST_UDP

statistics per-entry

 5 permit udp any any eq 56 [match=0]

 10 permit udp any any eq isakmp [match=0]

 20 permit ip any any [match=0]
```

- بدأ تدفق حركة مرور مع حزمة مجزأة غير أولية والحظ أنها متطابقة في التسلسل 5. على الرغم من أن الحزمة ل UDP 500، فإنها تطابق في التسلسل 5 للسماح UDP 56.

```
Nexus# sh ip access-lists TEST_UDP


IP access list TEST_UDP

statistics per-entry

 5 permit udp any any eq 56 [match=56]

 10 permit udp any any eq isakmp [match=0]

 20 permit ip any any [match=0]
```

- يتم رفض الأجزاء على قائمة التحكم في الوصول (ACL) الخاصة بالمنفذ ويالحظ أنه ال يتم مطابقة الحزم في قائمة التحكم في الوصول (ACL) الخاصة بالقوائم غير الأولية التي تم إنشاؤها تلقائيا حيث تتم مطابقة الحزمة في الواقع في **إدخال UDP أي أجزاء**

بواسطة النظام الأساسي.

```
NEXUS# sh ip access-lists TEST_UDP


IP access list TEST_UDP

       statistics per-entry

        fragments deny-all

       5 permit udp any any eq 56 [match=0]

        10 permit udp any any eq isakmp [match=0]

        20 permit ip any any [match=0]


 [0014:000a:000a] prec 3 permit udp 0.0.0.0/0 0.0.0.0/0 eq 56 flow-label 56  [0]-> Here we are now not seeing any entry to allow UDP fragments

 [0015:000b:000b] prec 3 permit udp 0.0.0.0/0 0.0.0.0/0 eq 500 flow-label 500  [0]

 [0016:000c:000c] prec 3 permit ip 0.0.0.0/0 0.0.0.0/0   [0]

 [0017:000d:000d] prec 3 deny ip 0.0.0.0/0 0.0.0.0/0 fragment   [100]>> Getting matched in fragments deny statement

 [001e:0014:0014] prec 3 deny ip 0.0.0.0/0 0.0.0.0/0   [0]
```

- تم رفض الأجزاء في قائمة التحكم في الوصول (ACL) الإشكالية في PBR، ومع ذلك لم يعد هذا إلى 70 و 50 التسلسل من كل في تطابق ترتيب لازالت ما مزحلاو لحال اذه لمعي سلوك البرمجة لقائمة الوصول وخريطة المسار.

```
           NEXUS# sh ip access-lists UDP_Traffic

       IP access list UDP_Traffic

       statistics per-entry

        fragments deny-all

       10 permit udp any any eq 9201

        20 permit udp any any eq 9202

        30 permit udp any any eq 9203


[0061:0057:0057] prec 1 redirect(0x5e)-routed udp 0.0.0.0/0 0.0.0.0/0 eq 9201 flow-label 9201 [0]

[0062:0058:0058] prec 1 redirect(0x5e)-routed udp 0.0.0.0/0 0.0.0.0/0 fragment    [8027]

 [0063:0059:0059] prec 1 redirect(0x5e)-routed udp 0.0.0.0/0 0.0.0.0/0 eq 9202 flow-label 9202 [0]
```

```
 [0064:005a:005a] prec 1 redirect(0x5e)-routed udp 0.0.0.0/0 0.0.0.0/0 fragment    [0]

 [0065:005b:005b] prec 1 redirect(0x5e)-routed udp 0.0.0.0/0 0.0.0.0/0 eq 9203 flow-label 9203
[0]

 [0066:005c:005c] prec 1 redirect(0x5e)-routed udp 0.0.0.0/0 0.0.0.0/0 fragment    [0]

  [0067:005d:005d] prec 1 permit-routed ip 0.0.0.0/0 0.0.0.0/0   [8027]

 [0068:005e:005e] prec 1 permit-routed ip 0.0.0.0/0 0.0.0.0/0   [0]
```

- إخراج عند تطبيق رفض الأجزاء على كل من قائمة التحكم في الوصول (ACL) الخاصة بالمنفذ وقائمة التحكم في الوصول (ACL) الخاصة ببروتوكول PBR:

```
[0061:0057:0057] prec 1 redirect(0x5e)-routed udp 0.0.0.0/0 0.0.0.0/0 eq 9201 flow-label 9201
[0]

[0062:0058:0058] prec 1 redirect(0x5e)-routed udp 0.0.0.0/0 0.0.0.0/0 fragment    [8027] ---
> Once the fragments are denied in port CAL, we observed non-initial packets to be getting
dropped (See the mismatch in number of packets between UDP and IP counter)

 [0063:0059:0059] prec 1 redirect(0x5e)-routed udp 0.0.0.0/0 0.0.0.0/0 eq 9202 flow-label 9202
[0]

 [0064:005a:005a] prec 1 redirect(0x5e)-routed udp 0.0.0.0/0 0.0.0.0/0 fragment    [0]

 [0065:005b:005b] prec 1 redirect(0x5e)-routed udp 0.0.0.0/0 0.0.0.0/0 eq 9203 flow-label 9203
[0]

 [0066:005c:005c] prec 1 redirect(0x5e)-routed udp 0.0.0.0/0 0.0.0.0/0 fragment    [0]

  [0067:005d:005d] prec 1 permit-routed ip 0.0.0.0/0 0.0.0.0/0   [8214]

 [0068:005e:005e] prec 1 permit-routed ip 0.0.0.0/0 0.0.0.0/0   [0]



VDC-1 Ethernet2/1 :

 ====================

INSTANCE 0x0

---------------

 Tcam 0 resource usage:

 ----------------------

 Label_a = 0x200

  Bank 0

  ------

    IPv4 Class

      Policies: PACL(TEST_UDP)

       Netflow profile: 0
```

```
      Netflow deny profile: 0

      Entries:

         [Index] Entry [Stats]

        ---------------------

 [0014:000a:000a] prec 3 permit udp 0.0.0.0/0 0.0.0.0/0 eq 56 flow-label 56  [8027]

 [0015:000b:000b] prec 3 permit udp 0.0.0.0/0 0.0.0.0/0 eq 500 flow-label 500  [8214]

 [0016:000c:000c] prec 3 permit ip 0.0.0.0/0 0.0.0.0/0   [0]

 [0017:000d:000d] prec 3 deny ip 0.0.0.0/0 0.0.0.0/0 fragment   [100]

 [001e:0014:0014] prec 3 deny ip 0.0.0.0/0 0.0.0.0/0   [0]
```

هناك العديد من الطرق الممكنة للتغلب على هذه المشكلة أو الحد من الحزم المجزأة باستخدام معلومات L4:

- يمكن نسخ خريطة المسار للسماح بمعلومات محددة عن L3 لمنافذ UDP معينة.

في التكوين الحالي، إذا تم ذكر معلومات مصدر L3 والوجهة، فسيتم توجيه الحزمة غير الأولية استنادا إلى هذه المعلومات المحددة. ومع ذلك، يكون هذا مفيدا فقط عندما لا يكون هناك تسلسل آخر قبل أن يطابق نفس معلومات L3.

```
Nexus# show ip access-lists UDP_Traffic

IP access list UDP_Traffic

10 permit udp host 1.1.1.1 host 3.3.3.3 eq 9201
20 permit udp any any eq 9202

30 permit udp any any eq 9203
```

- يمكن التحقق من المسار من المصدر إلى الوجهة للتحقق من وحدة الحد الأقصى للنقل (MTU) حتى لا يتم تجزئة الحزمة.

- إن الحل البديل لتطبيق تسلسل آخر يسمح لـ UDP أعلى التسلسل الإشكالي بالعمل، ومع ذلك، فإن السلوك هو نفسه كما تم شرحه سابقا عندما تم تطبيق التسلسل 45

```
Nexus# sh route-map In_to_Out pbr-statistics

route-map In_to_Out, permit, sequence 3

 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 5

 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 7

 Policy routing matches: 0 packets
```

```
route-map In_to_Out, permit, sequence 10

 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 30

 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 35

 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 40

 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 45----------> Both fragments matched here

 Policy routing matches: 213 packets

route-map In_to_Out, permit, sequence 50

 Policy routing matches: 0 packets

route-map In_to_Out, permit, sequence 70

 Policy routing matches: 0 packets
```

قائمة الوصول للتسلسل 45:

```
Nexus# sh ip access-lists udptraffic
```

حركة مرور بيانات قائمة الوصول إلى IP:

```
permit udp any any eq isakmp
```

خطأ المستند: CSCve05428 N7K خطأ المستند || قائمة التحكم في الوصول (ACL) في PBR التي تحتوي على معلومات كل من المستويين الثالث والرابع.

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).