Comportamento di ACL in PBR su Nexus 7K contenente informazioni L3 e L4

Sommario

Introduzione

Questo documento descrive il comportamento di Policy-Based Routing (PBR) sugli switch Nexus quando si applica un filtro basato sulle informazioni di layer 3 (L3) e layer 4 (L4).

Premesse

Se si aggiunge una sequenza in PBR in modo che corrisponda a informazioni L4 specifiche, la funzione N7K crea voci per le voci di controllo di accesso (ACE, Access Control Entry) e viene creata automaticamente una voce ACE del frammento che corrisponde alle informazioni L3 specificate nella sequenza di corrispondenza. In caso di pacchetti frammentati, il primo pacchetto, noto come frammento iniziale, contiene l'intestazione L4 e ha una corrispondenza corretta nell'elenco di controllo di accesso (ACL). Tuttavia, poiché i frammenti successivi, noti come frammenti non iniziali, non contengono informazioni L4, se la parte L3 della voce ACL corrisponde, il frammento non iniziale è autorizzato. Pertanto, occorre procedere con la massima attenzione e filtrare il traffico in base alle informazioni L4, in quanto i frammenti non iniziali potrebbero essere instradati erroneamente in assenza di informazioni L4.

Topologia

Il router LAN è collegato a Nexus sull'interfaccia E2.1, Vlan 700. Il requisito è reindirizzare il traffico che corrisponde al protocollo SNMP (Simple Network Management Protocol), Web ecc. verso Optimizer e tutto il resto del traffico direttamente in modo da interfacciare E2/2 al firewall. Il PBR è configurato sulla switch Virtual Interface (SVI) Vlan700 sul dispositivo Nexus. La sequenza 70 nella mappa dei percorsi inoltra tutto il traffico al firewall. È stato introdotto un nuovo requisito in base al quale tutto il traffico con porta UDP 920x deve passare attraverso l'optimizer, in quanto questa sequenza 50 viene aggiunta nella route-map.

Ecco come il PBR risponde ai pacchetti frammentati e non frammentati che colpiscono nella sequenza 50 e corrispondono sia alle informazioni L3 che L4.

Di seguito è riportata la configurazione sull'interfaccia Nexus Vlan700 per reindirizzare il traffico proveniente dall'interfaccia 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
```

Una volta configurato il routing basato su policy sulla SVI, Nexus crea una voce nell'hardware per lo stesso scopo. Esaminiamo ora la programmazione hardware per il PBR sul modulo 2 di 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]
```

Oltre alla voce dell'elenco degli accessi che corrisponde al valore **udp 0.0.0.0/0 0.0.0.0/0 eq 9201,** esiste un'altra voce che corrisponde al **frammento udp 0.0.0.0/0 0.0.0.0/0** ma tale voce non contiene informazioni sulla porta UDP. Poiché questa voce è equivalente a qualsiasi altra che corrisponde al pacchetto UDP, i pacchetti delle altre porte UDP vengono associati nella sequenza

generata dall'hardware.

Test case 1: Traffico avviato da router LAN verso il firewall

- Il pacchetto che raggiunge il Nexus non è stato frammentato e quindi il traffico corrisponde a quello previsto nel PBR.
- Èstato reindirizzato correttamente al firewall e può essere visualizzato nei debug eseguiti sul firewall.

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
```

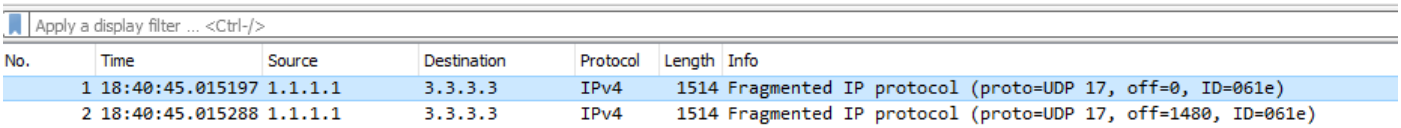
UDP packet -port 9201

```
*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
```

Test case 2: Traffico avviato tramite file sniffer da un router LAN al firewall con UDP 500

Traffico con due frammenti nel file Sniffer generato qui:



1. Frammenti iniziali con route-map:

- Il primo frammento con **Offset = 0** è noto come frammento iniziale e contiene l'intestazione UDP nel pacchetto.
- Poiché il traffico è per UDP 500, viene abbinato nella sequenza 70 per consentire **ip any.**

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

- In questo modo, il primo pacchetto che contiene informazioni sia sul layer 3 che sul layer 4 viene indirizzato correttamente.

2. Pacchetti non iniziali con route-map:

- Il secondo frammento con **Offset ≠ 0** è noto come frammento non iniziale e non contiene alcuna intestazione UDP. È un pacchetto puramente IP con protocollo di tipo UDP (17).
- Poiché non esistono informazioni sul layer 4, la sequenza di corrispondenza è 70: **ip con routing di autorizzazione 0.0.0.0/0 0.0.0.0/0.**
- Tuttavia, nella sequenza 50, è presente un elenco degli accessi che corrisponde al traffico della porta UDP 920x. L'hardware crea automaticamente una voce per consentire ai frammenti UDP che corrispondono alle informazioni specificate sul layer 3.
- Pertanto, tutti i pacchetti frammentati per qualsiasi informazione di layer 3 con protocollo UDP corrispondenti nella sequenza 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]
>>>>>>>>>>>>>>>>>>>>
```

- In questo modo, un frammento viene indirizzato correttamente e un altro tramite la sequenza errata.
- Il secondo frammento viene modificato in modo da ottenere un **offset = 0** e viene associato alla sequenza 70 come previsto.
- Questo è il comportamento previsto quando si ricevono i frammenti di layer 4.
- Lo scopo della creazione di una voce aggiuntiva per consentire i frammenti è permettere i frammenti non iniziali ricevuti senza informazioni sul layer 4.
- In questo caso, il traffico era per UDP 9201 e non era disponibile una voce che consentisse di selezionare i frammenti. Quindi, il secondo frammento avrebbe dovuto corrispondere alla sequenza 70 per permettere l'**ip any** e quindi essere indirizzato erroneamente.

```
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
```

- Viene creata un'altra sequenza 45 per autorizzare il traffico per UDP 500 e osservare che entrambi i frammenti corrispondono alla sequenza 45.
- Il frammento iniziale corrisponde a causa delle informazioni dell'intestazione UDP e non corrisponde inizialmente alla riga dei frammenti della sequenza 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


Default routing: 0 packets
```

Elenco degli accessi per la sequenza 45:

```
Nexus# sh ip access-lists udptraffic

IP access list udptraffic

permit udp any any eq isakmp
```

3. Ora vediamo come si comportano le parole chiave fragments con ACL e Route-Map

- La sequenza 5 viene applicata per autorizzare qualsiasi porta UDP 56 casuale sull'ACL della porta.

```
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]
```

- Èstato avviato un flusso di traffico con un pacchetto non iniziale frammentato che ha rilevato corrispondere nella sequenza 5. Anche se il pacchetto è per UDP 500, corrisponde nella sequenza 5 per consentire 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]
```

- I frammenti vengono rifiutati sull'ACL della porta e si noti che nessun pacchetto viene abbinato nell'ACL per operazioni non iniziali, in quanto il pacchetto viene effettivamente abbinato nella voce **udp a qualsiasi frammento** creato automaticamente dalla piattaforma.

```
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]
```

- Sono stati rifiutati i frammenti nell'ACL con problemi in PBR, ma la soluzione non è riuscita e i pacchetti continuano a corrispondere nella sequenza 50 e 70. Ciò è dovuto al comportamento di programmazione dell'elenco degli accessi e della route-map.

```
          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]
```

- Restituisce un output quando i frammenti vengono negati sia sull'ACL della porta sia sull'ACL del 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]
```

Per risolvere questo problema o limitare i pacchetti frammentati con informazioni L4, è possibile procedere in diversi modi:

- La route-map può essere modificata in modo da consentire informazioni L3 specifiche per determinate porte UDP.

Nella configurazione corrente, se si menzionano le informazioni L3 di origine e destinazione, il pacchetto non iniziale viene instradato in base a quelle informazioni specifiche. Tuttavia, questo è utile solo quando non c'è un'altra sequenza prima che corrisponda alle stesse informazioni 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
```

- Èpossibile verificare il percorso dall'origine alla destinazione per controllare l'MTU in modo che il pacchetto non venga frammentato.
- La soluzione per applicare un'altra sequenza consente il funzionamento di UDP al di sopra della sequenza problematica. Tuttavia, il comportamento è lo stesso descritto in precedenza all'applicazione della sequenza 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
```

Elenco degli accessi per la sequenza 45:

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

Traffico udp elenco accessi IP:

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

Bug documento: CSCve05428 N7K Doc bug || ACL in PBR che contiene sia informazioni L3 che L4.