Policy Based Routing (PBR)

PBR är ett verktyg för att göra routing-beslut baserad på en policy. Routern kommer då vid matchning ta beslut enligt en konfigurerad policy istället för via routing-tabell/FIB. Policyn konfigureras via en route-map som sedan appliceras på inkommande interface.

image.png

PBR är en bra teknik att använda i en VXLAN/EVPN-fabric (troligtivis i en Nexus-miljö, om Cisco) för att låta en brandvägg sköta policy-beslut inom en VRF mellan VLAN. PBR-konfiguration måste då tilldelas samtliga SVI:er inom en VRF. Det kan vara en bra idé att undanta tung trafik, ex. lagring, från PBRn för att inte överlasta brandväggen.

Konfiguration

Följande val finns i en route-map för beslut:

Kommando	Kommentar
set ip next-hop *ip-address* set ipv6 next-hop *ipv6-address*	Bestäm next hop. Måste vara direktanslutet.
set ip default next-hop *ip-address* set ipv6 default next-hop *ipv6-address*	Samma som ovan, men försöker först att routa enligt RIB, och om ingen träff finns så används PBR. Default-routen i RIB ignoreras.
set interface *interface*	Bestämmer next hop interface. Bör enbart användas för P2P interface.
set default interface *interface*	Samma som ovan men enligt samma logik som set ip default next-hop.
set ip df *0/1*	Sätter don't fragment biten till 1 eller 2. Stöds enbart för IPv4.
set ip precedence *number* | *name*	Sätter IP precedence bit. 0-7 eller text-namn.
set ipv6 precedence *number*	Sätt IPv6 precedence bit 0-7.
set ip tos *number* | *name*	Sätt ToS bit enligt decimalvärden eller ASCII namn. Stöds enbart för IPv4.

Exempelkonfiguration IPv4

```
route-map PBR-IPv4 permit 10
 match ip address prefix-list PBR-FILTER
 set ip next-hop

interface Vlan 10
 ip policy route-map
```

Debug

Debug kan man göra med `debug ip policy`. Exempel på debug-output:

```
.Aug 25 14:02:30: SW2: IP: s=172.13.37.35 (Vlan1337), d=172.16.1.17, len 52, FIB policy match
.Aug 25 14:02:30: SW2: IP: s=172.13.37.35 (Vlan1337), d=172.16.1.17, len 52, PBR Counted
.Aug 25 14:02:30: SW2: IP: s=172.13.37.35 (Vlan1337), d=172.16.1.17, g=192.168.18.18, len 52, FIB policy routed
```

Här syns då source IP, source VLAN, destinations-IP samt om PBR sker med ny destination `g=`.

Local PBR

Local PBR används för trafik som initieras från routern själv. Sätts med ett global kommando, `ip local policy route-map ROUTE_MAP_NAMN`. Verifiering med `show ip local policy`.

Problem, lärdomar

På en Catalyst C6807-XL plattform på mjukvara 15.5(1)SY12 så användes objekt-grupper för att identifiera de nät som ska PBRas. En ACL användes för att PBRa trafik som kommer från adresser i objektgruppen till adresser i objektgruppen.

Jobbet gick dåligt och konfigurationen behövde backas. Att uppdatera objektgruppen löste ingenting. Att ta bort ip policy från SVI eller att ta bort och lägga till route-map löste ingenting. Hela

ACLen behövdes tas bort och läggas till på nytt för att felet skulle lösas.

I samma plattform så såg det ut enligt följande:

Första raden i ACL var "any till specifikt nät" och andr araden var "specifikt nät till any". Det borde ha undantagit nätet från PBR.
I tredje raden används objektgrupp som source och destination. En större nätmask täckte nätverket som var med i rad 1 och 2 i objektgruppen.
Rimligtvis borde det ha gjort att nätverket specifiserat i rad 1 och 2 inte PBRades, men det gjorde det.

Jag fick bygga om till att använda ACL som match och route-maps som inte gör någon åtgärd för att lösa felet. Exempelkonf:

```
ip access-list extended NOT_PBR_IPv4
 permit ip 172.13.37.0 0.0.15.255 any
 permit ip any 172.13.37.0 0.0.15.255

route-map PBR_IPv4 permit 5
 match ip address NOT_PBR_IPv4
! Ingen åtgärd sker här och matchning slutar

route-map PBR_IPv4 permit 10
 match ip address PBR_IPv4
 set ip next-hop 192.168.18.18
```

Det gick att bekräfta via debug ip policy:

```
.Aug 26 13:09:23: SW2: IP: s=192.13.37.193 (Vlan11), d=172.13.37.99, len 1500, FIB policy match
.Aug 26 13:09:23: SW2: IP: s=192.13.37.193 (Vlan11), d=172.13.37.99, len 1500, PBR Counted
.Aug 26 13:09:23: SW2: IP: s=192.13.37.193 (Vlan11), d=172.13.37.99, len 1500, FIB policy rejected - normal forwarding
```

Revision #6
Created 26 April 2025 11:59:12 by Jehrlander
Updated 26 August 2026 13:21:31 by Jehrlander