PBR, Policy Based Routing

I Cisco NX-OS kan man inte använda sig av "deny" statements i en ACL för att undanta trafik från PBR.

Istället får man använda sig av route-map logik, där man först har en accesslista som matchar ett entry som inte utför någonting. Sedan en annan ACL som matchar korrekt där man utför PBR.

Ska man använda PBR i en VXLAN/EVPN-fabric får man tänka till, så att man inte skapar routingloopar. Ett alternativ är att direktansluta destinationen till samtliga löv, exempelvis en brandvägg.

Ett annat är att ha ett servicelöv utan loopar, kanske är svårt med vPC dock.

Erfarenheter

Vid tillägg av nytt SVI i ett VXLAN-EVPN nätverk med PBR på slaget så PBRades inte trafiken. `ip policy route-map NAMN` var applicerat på interfacet och ACL som hänvisades av route-map matchade nätet. Det krävdes en shut/no shut på SVIt för att PBRn skulle fungera.

Det här var i September 2026 på NX-OS version 10.5(4).

Revision #3
Created 5 December 2025 13:55:49 by Jehrlander
Updated 2 September 2026 13:03:58 by Jehrlander