



# ポリシーベース リダイレクトの設定

この章は、次の内容で構成されています。

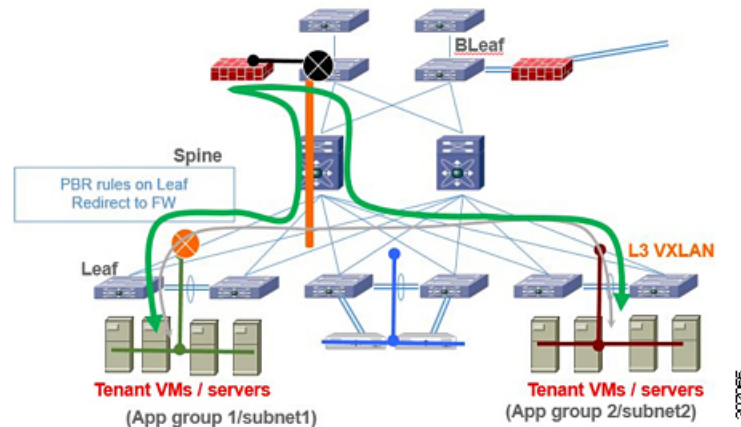
- [ポリシーベースのリダイレクトについて \(1 ページ\)](#)
- [ポリシーベースのリダイレクトの注意事項と制約事項 \(2 ページ\)](#)
- [ポリシーベース リダイレクト機能のイネーブル化 \(3 ページ\)](#)
- [ルート ポリシーの設定 \(3 ページ\)](#)
- [ポリシーベース リダイレクトの設定の確認 \(5 ページ\)](#)
- [ポリシーベース リダイレクトの設定例 \(5 ページ\)](#)

## ポリシーベースのリダイレクトについて

ポリシーベースのリダイレクト (PBR) は、ルーティング テーブル ルックアップをバイパスし、VXLAN 経由で到達可能なネクスト ホップ IP にトラフィックをリダイレクトするメカニズムを提供します。この機能により、ファイアウォールやロード バランサなどのレイヤ 4-レイヤ 7 デバイスへのサービス リダイレクションが可能になります。

PBR では、トラフィックの転送先を指定するルールを使用してルート マップを設定します。ルート マップは、テナント側の SVI に適用され、ホスト側のインターフェイスからファブリック経由で到達可能なネクスト ホップへのトラフィックに影響を与えます。

トラフィックがオーバーレイから VTEP に着信し、別のネクスト ホップにリダイレクトする必要があるシナリオでは、L3VNI SVI に面するファブリックに PBR ポリシーを適用する必要があります。



前の図では、アプリケーショングループ1とアプリケーショングループ2間の通信は、デフォルトでテナント VRF のVLAN 間/VNIルーティングを介して行われます。アプリケーショングループ1からアプリケーショングループ2へのトラフィックがファイアウォールを通過する必要があるという要件がある場合、PBR ポリシーを使用してトラフィックをリダイレクトできます。次の設定スニペットは、トラフィックフローをリダイレクトするために必要な設定を提供します。

PBRの詳細については、「[NX-OSでのPBR](#)」を参照してください。

## ポリシーベースのリダイレクトの注意事項と制約事項

PBR over VXLAN には、次の注意事項と制限事項が適用されます。

- 次のプラットフォームは、PBR over VXLAN をサポートしています。
  - Cisco Nexus 9332C および 9364C プラットフォーム スイッチ
  - Cisco Nexus 9300-EX プラットフォーム スイッチ
  - Cisco Nexus 9300-FX/FX2/FX3 プラットフォーム スイッチ
  - -EX/FX ラインカードを備えた Cisco Nexus 9504 および 9508 プラットフォーム スイッチ
- PBR over VXLAN は、IP SLA、VTEP ECMP、および `set {ip | ipv6} next-hop ip-address` コマンドの `load-share` キーワードをサポートしていません。

# ポリシーベース リダイレクト機能のイネーブル化

## 始める前に

ルート ポリシーを設定するには、あらかじめポリシーベース リダイレクト機能をイネーブル化しておく必要があります。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>[no] feature pbr</b> 例： switch(config)# <b>feature pbr</b>	ポリシーベース ルーティング機能をイネーブルにします。
ステップ 3	(任意) <b>show feature</b> 例： switch(config)# <b>show feature</b>	有効および無効にされた機能を表示します。
ステップ 4	(任意) <b>copy running-config startup-config</b> 例： switch(config)# <b>copy running-config startup-config</b>	この設定変更を保存します。

# ルート ポリシーの設定

ポリシーベースルーティングでルートマップを使用すると、着信インターフェイスにルーティング ポリシーを割り当てることができます。Cisco NX-OS はネクスト ホップおよびインターフェイスを検出するときに、パケットをルーティングします。



(注) スイッチには、IPv4 トラフィック用の RAACL TCAM リージョンがデフォルトで用意されています。

## 始める前に

ポリシーベース ルーティング ポリシーを適用するには、あらかじめ RACL TCAM リージョンを (TCAM カービングを使用して) 設定する必要があります。詳細については『Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.2(x)』の「Configuring ACL TCAM Region Sizes」の項を参照してください。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b>	グローバル設定モードを開始します。
ステップ 2	<b>interface type slot/port</b> 例： switch(config)# <b>interface ethernet 1/2</b>	インターフェイス設定モードを開始します。
ステップ 3	<b>{ip   ipv6} policy route-map map-name</b> 例： switch(config-inf)# <b>ip policy route-map Testmap</b>	IPv4 または IPv6 ポリシーベース ルーティング用のルートマップをインターフェイスに割り当てます。
ステップ 4	<b>route-map map-name [permit   deny] [seq]</b> 例： switch(config-inf)# <b>route-map Testmap</b>	ルートマップを作成するか、または既存のルートマップに対応するルートマップ設定モードを開始します。ルートマップのエントリを順序付けるには、 <i>seq</i> を使用します。
ステップ 5	<b>match {ip   ipv6} address access-list-name name [name...]</b> 例： switch(config-route-map)# <b>match ip address access-list-name ACL1</b>	1 つまたは複数の IPv4 または IPv6 アクセスコントロールリスト (ACL) に対して IPv4 または IPv6 アドレスを照合します。このコマンドはポリシーベースルーティング用であり、ルートフィルタリングまたは再配布では無視されません。
ステップ 6	<b>set ip next-hop address1</b> 例： switch(config-route-map)# <b>set ip next-hop 192.0.2.1</b>	ポリシーベース ルーティング用の IPv4 ネクストホップアドレスを設定します。
ステップ 7	<b>set ipv6 next-hop address1</b> 例： switch(config-route-map)# <b>set ipv6 next-hop 2001:0DB8::1</b>	ポリシーベース ルーティング用の IPv6 ネクストホップアドレスを設定します。

	コマンドまたはアクション	目的
ステップ 8	(任意) <b>set interface null0</b> 例： switch(config-route-map)# <b>set interface null0</b>	ルーティングに使用するインターフェイスを設定します。パケットをドロップするには <b>null0</b> インターフェイスを使用します。
ステップ 9	(任意) <b>copy running-config startup-config</b> 例： switch(config-route-map)# <b>copy running-config startup-config</b>	この設定変更を保存します。

## ポリシーベース リダイレクトの設定の確認

ポリシーベース リダイレクト設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
<b>show [ip   ipv6] policy [name]</b>	IPv4 または IPv6 ポリシーに関する情報を表示します。
<b>show route-map [name] pbr-statistics</b>	ポリシー統計情報を表示します。

**route-map map-name pbr-statistics** コマンドを使用してポリシーを有効にします。**clear route-map map-name pbr-statistics** コマンドを使用してこれらのポリシーをクリアします。

## ポリシーベース リダイレクトの設定例

サービス VTEP を除くすべてのテナント VTEP で次の設定を実行します。

```
feature pbr

ipv6 access-list IPV6_App_group_1
10 permit ipv6 any 2001:10:1:1::0/64

ip access-list IPV4_App_group_1
10 permit ip any 10.1.1.0/24

ipv6 access-list IPV6_App_group_2
10 permit ipv6 any 2001:20:1:1::0/64

ip access-list IPV4_App_group_2
10 permit ip any 20.1.1.0/24

route-map IPV6_PBR_Appgroup1 permit 10
  match ipv6 address IPV6_App_group_2
  set ipv6 next-hop 2001:100:1:1::20 (next hop is that of the firewall)

route-map IPV4_PBR_Appgroup1 permit 10
```

```

match ip address IPV4_App_group_2
set ip next-hop 10.100.1.20 (next hop is that of the firewall)

route-map IPV6_PBR_Appgroup2 permit 10
match ipv6 address IPV6_App_group1
set ipv6 next-hop 2001:100:1:1::20 (next hop is that of the firewall)

route-map IPV4_PBR_Appgroup2 permit 10
match ip address IPV4_App_group_1
set ip next-hop 10.100.1.20 (next hop is that of the firewall)

interface Vlan10
! tenant SVI appgroup 1
vrf member appgroup
ip address 10.1.1.1/24
no ip redirect
ipv6 address 2001:10:1:1::1/64
no ipv6 redirects
fabric forwarding mode anycast-gateway
ip policy route-map IPV4_PBR_Appgroup1
ipv6 policy route-map IPV6_PBR_Appgroup1
interface Vlan20
! tenant SVI appgroup 2
vrf member appgroup
ip address 20.1.1.1/24
no ip redirect
ipv6 address 2001:20:1:1::1/64
no ipv6 redirects
fabric forwarding mode anycast-gateway
ip policy route-map IPV4_PBR_Appgroup2
ipv6 policy route-map IPV6_PBR_Appgroup2

On the service VTEP, the PBR policy is applied on the tenant VRF SVI. This ensures the
traffic post decapsulation will be redirected to firewall.
feature pbr

ipv6 access-list IPV6_App_group_1
10 permit ipv6 any 2001:10:1:1::0/64

ip access-list IPV4_App_group_1
10 permit ip any 10.1.1.0/24

ipv6 access-list IPV6_App_group_2
10 permit ipv6 any 2001:20:1:1::0/64

ip access-list IPV4_App_group_2
10 permit ip any 20.1.1.0/24

route-map IPV6_PBR_Appgroup1 permit 10
match ipv6 address IPV6_App_group_2
set ipv6 next-hop 2001:100:1:1::20 (next hop is that of the firewall)

route-map IPV6_PBR_Appgroup permit 20
match ipv6 address IPV6_App_group1
set ipv6 next-hop 2001:100:1:1::20 (next hop is that of the firewall)

route-map IPV4_PBR_Appgroup permit 10
match ip address IPV4_App_group_2
set ip next-hop 10.100.1.20 (next hop is that of the firewall)

route-map IPV4_PBR_Appgroup permit 20
match ip address IPV4_App_group_1
set ip next-hop 10.100.1.20 (next hop is that of the firewall)

```

```
interface vlan1000
!L3VNI SVI for Tenant VRF
vrf member appgroup
ip forward
ipv6 forward
ipv6 ipv6 address use-link-local-only
ip policy route-map IPV4_PBR_Appgroup
ipv6 policy route-map IPV6_PBR_Appgroup
```

