



# 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。

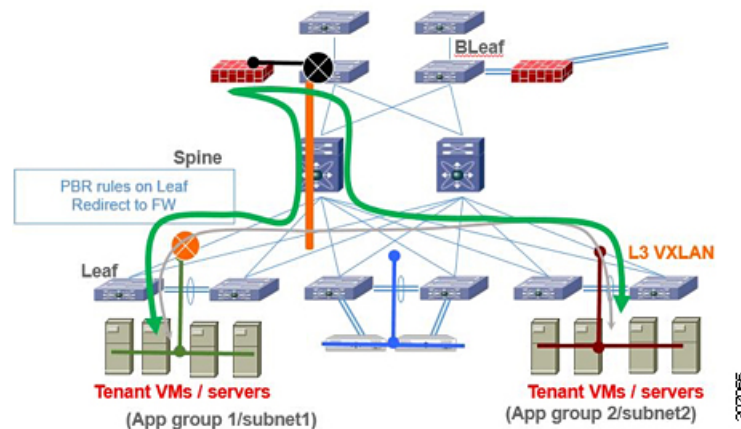
- [ポリシーベースのリダイレクトについて \(1 ページ\)](#)
- [ポリシーベースのリダイレクトの注意事項と制約事項 \(2 ページ\)](#)
- [ポリシーベース リダイレクト機能のイネーブル化 \(3 ページ\)](#)
- [ルート ポリシーの設定 \(3 ページ\)](#)
- [ポリシーベース リダイレクトの設定の確認 \(5 ページ\)](#)
- [ポリシーベース リダイレクトの設定例 \(5 ページ\)](#)

## 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
  - Cisco Nexus 9300-GX 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
- Cisco NX-OS リリース 10.2(3)F 以降、VXLAN 経由の SRv6 は Cisco Nexus 9300-GX2 プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.2(3) 以降、VXLAN PBR 機能は、すべての TOR スイッチの VXLANv6 でサポートされます。
- 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。

## 手順の概要

1. **configure terminal**
2. **[no] feature pbr**
3. (任意) **show feature**
4. (任意) **copy running-config startup-config**

## 手順の詳細

	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 RACL 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。

### 手順の概要

1. **configure terminal**
2. **interface** *type slot/port*
3. **{ip | ipv6} policy route-map** *map-name*
4. **route-map** *map-name* [**permit** | **deny**] [*seq*]
5. **match {ip | ipv6} address access-list-name** *name* [*name...*]
6. **set ip next-hop** *address1*
7. **set ipv6 next-hop** *address1*
8. (任意) **set interface null0**
9. (任意) **copy running-config startup-config**

### 手順の詳細

	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>interface</b> <i>type slot/port</i> 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</b> <i>map-name</i> 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</b> <i>map-name</i> [ <b>permit</b>   <b>deny</b> ] [ <i>seq</i> ] 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。

	コマンドまたはアクション	目的
ステップ 5	<b>match {ip   ipv6} address access-list-name name [name...]</b> 例： <pre>switch(config-route-map)# match ip address access-list-name ACL1</pre>	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す。
ステップ 6	<b>set ip next-hop address1</b> 例： <pre>switch(config-route-map)# set ip next-hop 192.0.2.1</pre>	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： <pre>switch(config-route-map)# set ipv6 next-hop 2001:0DB8::1</pre>	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。
ステップ 8	(任意) <b>set interface null0</b> 例： <pre>switch(config-route-map)# set interface null0</pre>	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： <pre>switch(config-route-map)# copy running-config startup-config</pre>	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
```





## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。