



## VXLAN ACL の構成

この章は、次の内容で構成されています。

- [アクセスコントロールリストについて \(1 ページ\)](#)
- [VXLAN ACL の注意事項と制約事項 \(4 ページ\)](#)
- [VXLANトンネルカプセル化スイッチ \(4 ページ\)](#)
- [VXLANトンネルカプセル化解除スイッチ \(9 ページ\)](#)

## アクセスコントロールリストについて

表 1: Cisco Nexus 92300YC、92160YC-X、93120TX、9332PQ、および 9348GC-FXP スイッチで VXLAN トラフィックに使用できる ACL オプション

| シナリオ | ACL の方向 | ACL タイプ | VTEP タイプ | ポートタイプ | フローの方向   | トラフィックタイプ                             | サポート対象 |
|------|---------|---------|----------|--------|--|---------------------------------------|--------|
| 1    | 入力      | PAACL   | 入力 VTEP  | L2 ポート | ネットワークにアクセス<br>[GROUP :<br>encap<br>direction] | ネイティブ L2 トラフィック<br>[GROUP :<br>inner] | YES    |
| 2    |         | VACL    | 入力 VTEP  | VLAN   | ネットワークにアクセス<br>[GROUP :<br>encap<br>direction] | ネイティブ L2 トラフィック<br>[GROUP :<br>inner] | YES    |

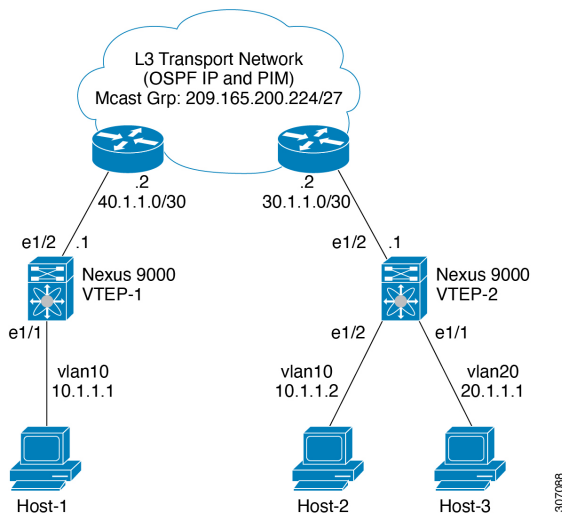
| シナリオ | ACL の方向 | ACL タイプ | VTEP タイプ | ポートタイプ               | フローの方向                                   | トラフィックタイプ                          | サポート対象 |
|------|---------|---------|----------|----------------------|--|------------------------------------|--------|
| 3    | 入力      | RACL    | 入力 VTEP  | テナント L3 SVI          | ネットワークにアクセス<br>[GROUP : encap direction] | ネイティブ L3 トラフィック<br>[GROUP : inner] | YES    |
| 4    | 出力      | RACL    | 入力 VTEP  | アプリケーション L3/L3-POSVI | ネットワークにアクセス<br>[GROUP : encap direction] | VXLAN encap<br>[GROUP : outer]     | NO     |
| 5    | 入力      | RACL    | 出力 VTEP  | アプリケーション L3/L3-POSVI | ネットワークにアクセス<br>[GROUP : decap direction] | VXLAN encap<br>[GROUP : outer]     | NO     |
| 6    | 出力      | PACL    | 出力 VTEP  | L2 ポート               | ネットワークにアクセス<br>[GROUP : decap direction] | ネイティブ L2 トラフィック<br>[GROUP : inner] | NO     |
| 7a   |         | VACL    | 出力 VTEP  | VLAN                 | ネットワークにアクセス<br>[GROUP : decap direction] | ネイティブ L2 トラフィック<br>[GROUP : inner] | YES    |
| 7b   |         | VACL    | 出力 VTEP  | 宛先 VLAN              | ネットワークにアクセス<br>[GROUP : decap direction] | ネイティブ L3 トラフィック<br>[GROUP : inner] | YES    |

| シナリオ | ACL の方向 | ACL タイプ | VTEP タイプ | ポートタイプ      | フローの方向                                   | トラフィックタイプ                               | サポート対象 |
|------|---------|---------|----------|-------------|--|---|--------|
| 8    | 出力      | RACL    | 出力 VTEP  | テナント L3 SVI | ネットワークにアクセス<br>[GROUP : decap direction] | Post-decap L3 トラフィック<br>[GROUP : inner] | YES    |

VXLAN の ACL 実装は、通常の IP トラフィックと同じです。ホストトラフィックは、カプセル化スイッチで入力方向にカプセル化されません。ACL の分類は内部ペイロードに基づいているため、VXLAN カプセル化解除トラフィックでのカプセル化トラフィックの実装は少し異なります。VXLAN でサポートされている ACL のシナリオについては、次のトピックで説明します。また、カプセル化とカプセル化解除の両方のスイッチでサポートされていないケースについても説明します。

前の表に記載されているすべてのシナリオは、次のホストの詳細で説明されています。

図 1: VXLAN Encap スwitch のポート ACL



- Host-1: 10.1.1.1/24 VLAN-10
- Host-2: 10.1.1.2/24 VLAN-10
- Host-3: 20.1.1.1/24 VLAN-20
- ケース1 : VLAN-10 の Host-1 と Host-2 の間を流れるレイヤ 2 トラフィック/L2 VNI。
- ケース2 : VLAN-10 および VLAN-20 上の Host-1 と Host-3 の間を流れるレイヤ 3 トラフィック/L3 VNI。

## VXLAN ACL の注意事項と制約事項

VXLAN には、次の注意事項と制限事項があります。

- 着信 VLAN-10 およびアップリンク ポート (eth1/2) の SVI 上のルータ ACL (RACL) は、出力方向の外部または内部ヘッダーを持つカプセル化された VXLAN トラフィックのフィルタリングをサポートしません。この制限は、レイヤ 3 ポート チャンネルアップリンク インターフェイスにも適用されます。
- SVI およびレイヤ 3 アップリンク ポートのルータ ACL (RACL) は、入力方向の外部または内部ヘッダーを持つカプセル化された VXLAN トラフィックをフィルタリングするためにサポートされていません。この制限は、レイヤ 3 ポート チャンネルアップリンク インターフェイスにも適用されます。
- ポート ACL (PACL) は、ホストが接続されているレイヤ 2 ポートには適用できません。Cisco NX-OS は、出力方向の PACL をサポートしていません。

## VXLAN トンネル カプセル化 スイッチ

### 入力のアクセス ポートのポート ACL

カプセル化スイッチでホストが接続されているレイヤ 2 トランクまたはアクセスポートにポート ACL (PACL) を適用できます。ネットワークへのアクセスからの着信トラフィックは通常の IP トラフィックであるため、レイヤ 2 ポートに適用されている ACL は、非 VXLAN 環境の IP トラフィックと同様にフィルタリングできます。

**ing-ifacl** TCAM リージョンは、次のように分割する必要があります。

#### 手順の概要

1. **configure terminal**
2. **hardware access-list tcam region ing-ifacl 256**
3. **ip access-list name**
4. *sequence-number* **permit ip source-address destination-address**
5. **exit**
6. **interface ethernet slot/port**
7. **ip port access-group pacl-name in**
8. **switchport**
9. **switchport mode trunk**
10. **switchport trunk allowed vlan vlan-list**
11. **no shutdown**

## 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><br>例：<br>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>hardware access-list tcam region ing-ifacl 256</b><br>例：<br>switch(config)# <b>hardware access-list tcam region ing-ifacl 256</b>         | <b>ing-ifacl</b> TCAM リージョンに UDF を接続します。これは IPv4 または IPv6 ポート ACL に適用されます。  |
| ステップ 3 | <b>ip access-list name</b><br>例：<br>switch(config)# <b>ip access list PACL_On_Host_Port</b>  | IPv4 ACL を作成し、IP ACL コンフィギュレーション モードを開始します。name 引数は 64 文字以内で指定します。  |
| ステップ 4 | <b>sequence-number permit ip source-address destination-address</b><br>例：<br>switch(config-acl)# <b>10 permit ip 10.1.1.1/32 10.1.1.2/32</b> | 条件に一致する IPv4 トラフィックを許可または拒否する、ACL のルールを作成します。<br><br><i>source-address destination-address</i> 引数には、IP アドレスとネットワーク ワイルドカード、IP アドレスと可変長サブネット マスク、ホストアドレス、または任意のアドレスを指定する <b>any</b> があります。 |
| ステップ 5 | <b>exit</b><br>例：<br>switch(config-acl)# <b>exit</b>   | IP ACL 設定モードを終了します。   |
| ステップ 6 | <b>interface ethernet slot/port</b><br>例：<br>switch(config)# <b>interface ethernet1/1</b>  | インターフェイス設定モードを開始します。  |
| ステップ 7 | <b>ip port access-group pacl-name in</b><br>例：<br>switch(config-if)# <b>ip port access-group PACL_On_Host_Port in</b>                        | インターフェイスにレイヤ 2 PACL を適用します。ポート ACL では、インバウンドフィルタリングだけがサポートされています。1つのインターフェイスに1つのポート ACL を適用できます。  |
| ステップ 8 | <b>switchport</b><br>例：<br>switch(config-if)# <b>switchport</b>  | そのインターフェイスを、レイヤ2インターフェイスとして設定します。   |
| ステップ 9 | <b>switchport mode trunk</b><br>例：<br>switch(config-if)# <b>switchport mode trunk</b>  | インターフェイスをレイヤ 2 トランク ポートとして設定します。  |

|         | コマンドまたはアクション   | 目的  |
|---------|--|---|
| ステップ 10 | <b>switchport trunk allowed vlan <i>vlan-list</i></b><br>例：<br><pre>switch(config-if)# switchport trunk allowed vlan 10,20</pre> | トランク インターフェイスの許可 VLAN を設定します。デフォルトでは、トランク インターフェイス上のすべての VLAN（1 ～ 3967 および 4048 ～ 4094）が許可されます。VLAN 3968 ～ 4047 は、内部で使用するデフォルトで予約されている VLAN です。 |
| ステップ 11 | <b>no shutdown</b><br>例：<br><pre>switch(config-if)# no shutdown</pre>  | <b>shutdown</b> コマンドを無効にします。  |

## サーバ VLAN の VLAN ACL

VLAN ACL (VACL) は、ホストが接続されている着信 VLAN-10 に適用できます。ネットワークへのアクセスからの着信トラフィックは通常の IP トラフィックであるため、VLAN-10 に適用されている ACL は、非 VXLAN 環境の IP トラフィックと同様にフィルタリングできます。VACL の詳細については、[アクセス コントロール リストについて \(1 ページ\)](#) を参照してください。

### 手順の概要

1. **configure terminal**
2. **ip access-list *name***
3. ***sequence-number* permit ip *source-address* *destination-address***
4. **vlan access-map *map-name* [*sequence-number*]**
5. **match ip address *ip-access-list***
6. **action forward**
7. **vlan access-map *name***

### 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><br>例：<br><pre>switch# configure terminal</pre>                                 | グローバル構成モードを開始します。   |
| ステップ 2 | <b>ip access-list <i>name</i></b><br>例：<br><pre>switch(config)# ip access list Vacl_On_Source_VLAN</pre> | IPv4 ACL を作成し、IP ACL コンフィギュレーションモードを開始します。 <i>name</i> 引数は 64 文字以内で指定します。 |
| ステップ 3 | <b><i>sequence-number</i> permit ip <i>source-address</i> <i>destination-address</i></b><br>例：           | 条件に一致する IPv4 トラフィックを許可または拒否する、ACL のルールを作成します。                             |

|        | コマンドまたはアクション   | 目的  |
|--------|--|---|
|        | <code>switch(config-acl)# 10 permit ip 10.1.1.1 10.1.1.2</code>  | <code>source-address destination-address</code> 引数には、IP アドレスとネットワークワイルドカード、IP アドレスと可変長サブネットマスク、ホストアドレス、または任意のアドレスを指定する <b>any</b> があります。  |
| ステップ 4 | <b>vlan access-map map-name [sequence-number]</b><br>例：<br><code>switch(config-acl)# vlan access-map<br/>Vacl_on_Source_Vlan 10</code> | 指定した VLAN アクセス マップの VLAN アクセス マップ コンフィギュレーション モードを開始します。VLAN アクセス マップが存在しない場合は、デバイスによって作成されます。<br><br>シーケンス番号を指定しなかった場合、デバイスによって新しいエントリが作成され、このシーケンス番号はアクセスマップの最後のシーケンス番号よりも 10 大きい番号となります。 |
| ステップ 5 | <b>match ip address ip-access-list</b><br>例：<br><code>switch(config-acl)# match ip address<br/>Vacl_on_Source_Vlan</code>              | アクセス マップ エントリに ACL を指定します。  |
| ステップ 6 | <b>action forward</b><br>例：<br><code>switch(config-acl)# action forward</code>   | ACL に一致したトラフィックにデバイスが適用する処理を指定します。  |
| ステップ 7 | <b>vlan access-map name</b><br>例：<br><code>switch(config-acl)# vlan access map<br/>Vacl_on_Source_Vlan</code>                          | 指定した VLAN アクセス マップの VLAN アクセス マップ コンフィギュレーション モードを開始します。  |

## 入力の SVI のルーテッド ACL

入力方向のルータ ACL (RACL) は、カプセル化スイッチに接続するホストの着信 VLAN-10 の SVI に適用できます。ネットワークへのアクセスからの着信トラフィックは通常の IP トラフィックであるため、SVI 10 に適用されている ACL は、非 VXLAN 環境の IP トラフィックと同様にフィルタリングできます。

**ing-racl** TCAM リージョンは、次のように分割する必要があります。

### 手順の概要

1. **configure terminal**
2. **hardware access-list tcam region ing-ifacl 256**
3. **ip access-list name**
4. *sequence-number* **permit ip source-address destination-address**
5. **exit**

6. **interface ethernet slot/port**
7. **no shutdown**
8. **ip access-group pacl-name in**
9. **vrf member vxlan-number**
10. **no ip redirects**
11. **ip address ip-address**
12. **no ipv6 redirects**
13. **fabric forwarding mode anycast-gateway**

## 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><br>例：<br>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>hardware access-list tcam region ing-ifacl 256</b><br>例：<br>switch(config)# <b>hardware access-list tcam region ing-ifacl 256</b>                | <b>ing-racl</b> TCAM リージョンに UDF を接続します。これは IPv4 または IPv6 ポート ACL に適用されます。  |
| ステップ 3 | <b>ip access-list name</b><br>例：<br>switch(config)# <b>ip access list PACL_On_Host_Port</b>   | IPv4 ACL を作成し、IP ACL コンフィギュレーション モードを開始します。name 引数は 64 文字以内で指定します。   |
| ステップ 4 | <i>sequence-number</i> <b>permit ip source-address destination-address</b><br>例：<br>switch(config-acl)# <b>10 permit ip 10.1.1.1/32 10.1.1.2/32</b> | 条件に一致する IPv4 トラフィックを許可または拒否する、ACL のルールを作成します。<br><br><i>source-address destination-address</i> 引数には、IP アドレスとネットワーク ワイルドカード、IP アドレスと可変長サブネットマスク、ホストアドレス、または任意のアドレスを指定する <b>any</b> などがあります。 |
| ステップ 5 | <b>exit</b><br>例：<br>switch(config-acl)# <b>exit</b>  | IP ACL 設定モードを終了します。  |
| ステップ 6 | <b>interface ethernet slot/port</b><br>例：<br>switch(config)# <b>interface ethernet1/1</b>   | インターフェイス設定モードを開始します。   |
| ステップ 7 | <b>no shutdown</b><br>例：<br>switch(config-if)# <b>no shutdown</b>   | <b>shutdown</b> コマンドを無効にします。   |



|         | コマンドまたはアクション   | 目的   |
|---------|--|--|
| ステップ 8  | <b>ip access-group</b> <i>pacl-name</i> <i>in</i><br>例：<br>switch(config-if)# <b>ip port access-group</b><br><b>Racl_On_Source_Vlan_SVI in</b> | インターフェイスにレイヤ 2 PACL を適用します。ポート ACL では、インバウンドフィルタリングだけがサポートされています。1つのインターフェイスに1つのポート ACL を適用できます。 |
| ステップ 9  | <b>vrf member</b> <i>vxlan-number</i><br>例：<br>switch(config-if)# <b>vrf member Cust-A</b>   | ホストの SVI を設定します。   |
| ステップ 10 | <b>no ip redirects</b><br>例：<br>switch(config-if)# <b>no ip redirects</b>  | デバイスがリダイレクトを送信しないようにします。   |
| ステップ 11 | <b>ip address</b> <i>ip-address</i><br>例：<br>switch(config-if)# <b>ip address 10.1.1.10</b>  | このインターフェイスの IP アドレスを設定します。   |
| ステップ 12 | <b>no ipv6 redirects</b><br>例：<br>switch(config-if)# <b>no ipv6 redirects</b>  | ICMP のリダイレクトメッセージが BFD 対応インターフェイスでディセーブルであることを確認します。   |
| ステップ 13 | <b>fabric forwarding mode anycast-gateway</b><br>例：<br>switch(config-if)# <b>fabric forwarding mode</b><br><b>anycast-gateway</b>              | エニーキャスト ゲートウェイ転送モードを構成します。   |

## 出力のアップリンクのルーテッド ACL

着信 VLAN-10 の SVI およびアップリンク ポート (eth1/2) の RAACL は、出力方向の外部または内部ヘッダーを持つカプセル化された VXLAN トラフィックをフィルタリングするためにサポートされていません。この制限は、レイヤ 3 ポート チャネルアップリンク インターフェイスにも適用されます。

## VXLAN トンネル カプセル化解除スイッチ

### 入力 of アップリンクのルーテッド ACL

SVI およびレイヤ 3 アップリンク ポートの RAACL は、入力方向の外部または内部ヘッダーを持つカプセル化された VXLAN トラフィックをフィルタリングするためにサポートされていません。この制限は、レイヤ 3 ポート チャネルアップリンク インターフェイスにも適用されません。

## 出力のアクセス ポートのポート ACL

ホストが接続されているレイヤ 2 ポートに PACL を適用しないでください。Cisco Nexus 9000 シリーズ スイッチは、出力方向の PACL をサポートしていません。

## レイヤ 2 VNI トラフィックの VLAN ACL

レイヤ 2 VNI トラフィックが Host-1 から Host-2 に流れている場合、VLAN ACL (VACL) を VLAN-10 に適用して内部ヘッダーでフィルタリングできます。VACL の詳細については、[アクセス コントロール リストについて \(1 ページ\)](#) を参照してください。

VACL TCAM リージョンは、次のように分割する必要があります。

### 手順の概要

1. **configure terminal**
2. **hardware access-list tcam region vACL 256**
3. **ip access-list name**
4. **statistics per-entry**
5. *sequence-number* **permit ip** *source-address destination-address*
6. *sequence-number* **permit protocol** *source-address destination-address*
7. **exit**
8. **vlan access-map map-name [sequence-number]**
9. **match ip address list-name**

### 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><br>例：<br>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>hardware access-list tcam region vACL 256</b><br>例：<br>switch(config)# <b>hardware access-list tcam region vACL 256</b> | ACL TCAM リージョン サイズを変更します。   |
| ステップ 3 | <b>ip access-list name</b><br>例：<br>switch(config)# <b>ip access list VXLAN-L2-VNI</b>                                     | IPv4 ACL を作成し、IP ACL コンフィギュレーションモードを開始します。name 引数は 64 文字以内で指定します。 |
| ステップ 4 | <b>statistics per-entry</b><br>例：<br>switch(config-acl)# <b>statistics per-entry</b>                                       | その VACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。                  |

|        | コマンドまたはアクション   | 目的   |
|--------|--|--|
| ステップ 5 | <p><i>sequence-number permit ip source-address destination-address</i></p> <p>例 :</p> <pre>switch(config-acl)# 10 permit ip 10.1.1.1/32 10.1.1.2/32</pre>        | <p>条件に一致する IPv4 トラフィックを許可または拒否する、ACL のルールを作成します。</p> <p><i>source-address destination-address</i> 引数には、IP アドレスとネットワークワイルドカード、IP アドレスと可変長サブネットマスク、ホストアドレス、または任意のアドレスを指定する <b>any</b> があります。</p>     |
| ステップ 6 | <p><i>sequence-number permit protocol source-address destination-address</i></p> <p>例 :</p> <pre>switch(config-acl)# 20 permit tcp 10.1.1.2/32 10.1.1.1/32</pre> | <p>条件に一致する IPv4 トラフィックを許可または拒否する、ACL のルールを作成します。</p> <p><i>source-address destination-address</i> 引数には、IP アドレスとネットワークワイルドカード、IP アドレスと可変長サブネットマスク、ホストアドレス、または任意のアドレスを指定する <b>any</b> があります。</p>     |
| ステップ 7 | <p><b>exit</b></p> <p>例 :</p> <pre>switch(config-acl)# exit</pre>  | ACL 設定モードを終了します。   |
| ステップ 8 | <p><b>vlan access-map map-name [sequence-number]</b></p> <p>例 :</p> <pre>switch(config)# vlan access-map VXLAN-L2-VNI 10</pre>                                   | <p>指定した VLAN アクセス マップの VLAN アクセス マップ コンフィギュレーション モードを開始します。VLAN アクセス マップが存在しない場合は、デバイスによって作成されます。</p> <p>シーケンス番号を指定しなかった場合、デバイスによって新しいエントリが作成され、このシーケンス番号はアクセスマップの最後のシーケンス番号よりも 10 大きい番号となります。</p> |
| ステップ 9 | <p><b>match ip address list-name</b></p> <p>例 :</p> <pre>switch(config-access-map)# match ip VXLAN-L2-VNI</pre>  | IP リスト名を設定します。   |

## レイヤ3 VNI トラフィックのVLAN ACL

VLAN ACL (VACL) は、レイヤ3 VNI トラフィックがホスト1からホスト3に流れている場合に、内部ヘッダーでフィルタリングするために宛先VLAN20に適用できます。これは、レイヤ3 トラフィックのVACLがシステムの出力で考慮されるため、前のケースとは若干異なります。キーワード **output** は、レイヤ3 VNI トラフィックの VACL エントリをダンプするときに使用する必要があります。VACL の詳細については、[アクセス コントロール リストについて \(1 ページ\)](#) を参照してください。

VACL TCAM リージョンは、次のようにカービングする必要があります。

## 手順の概要

1. **configure terminal**
2. **hardware access-list tcam region vacl 256**
3. **ip access-list name**
4. **statistics per-entry**
5. *sequence-number* **permit ip** *source-address destination-address*
6. *sequence-number* **permit protocol** *source-address destination-address*
7. **vlan access-map map-name [sequence-number]**
8. **action forward**

## 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><br>例：<br>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>hardware access-list tcam region vacl 256</b><br>例：<br>switch(config)# <b>hardware access-list tcam region vacl 256</b>  | ACL TCAM リージョン サイズを変更します。   |
| ステップ 3 | <b>ip access-list name</b><br>例：<br>switch(config)# <b>ip access list VXLAN-L3-VNI</b>  | IPv4 ACL を作成し、IP ACL コンフィギュレーションモードを開始します。name 引数は 64 文字以内で指定します。   |
| ステップ 4 | <b>statistics per-entry</b><br>例：<br>switch(config)# <b>statistics per-entry</b>  | その VACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。  |
| ステップ 5 | <i>sequence-number</i> <b>permit ip</b> <i>source-address destination-address</i><br>例：<br>switch(config-acl)# <b>10 permit ip 10.1.1.1/32 20.1.1.1/32</b>        | 条件に一致する IPv4 トラフィックを許可または拒否する、ACL のルールを作成します。<br><br><i>source-address destination-address</i> 引数には、IP アドレスとネットワークワイルドカード、IP アドレスと可変長サブネットマスク、ホストアドレス、または任意のアドレスを指定する <b>any</b> があります。 |
| ステップ 6 | <i>sequence-number</i> <b>permit protocol</b> <i>source-address destination-address</i><br>例：<br>switch(config-acl)# <b>20 permit tcp 20.1.1.1/32 10.1.1.1/32</b> | 特定の HTTP メソッドをサーバにリダイレクトするように ACL を設定します。   |
| ステップ 7 | <b>vlan access-map map-name [sequence-number]</b><br>例：   | 指定した VLAN アクセス マップの VLAN アクセス マップ コンフィギュレーション モードを開始しま  |

|        | コマンドまたはアクション   | 目的   |
|--------|--|--|
|        | switch(config-acl)# <b>vlan access-map VXLAN-L3-VNI 10</b>                   | す。VLAN アクセスマップが存在しない場合は、デバイスによって作成されます。<br><br>シーケンス番号を指定しなかった場合、デバイスによって新しいエントリが作成され、このシーケンス番号はアクセスマップの最後のシーケンス番号よりも 10 大きい番号となります。 |
| ステップ 8 | <b>action forward</b><br><br>例：<br>switch(config-acl)# <b>action forward</b> | ACL に一致したトラフィックにデバイスが適用する処理を指定します。   |

## 出力の SVI のルーテッド ACL

出力方向のルータ ACL (RACL) は、Host-3 がデキャップスイッチで接続されている宛先 VLAN-20 の SVI に適用して、ネットワークからアクセスへのトラフィックフローの内部ヘッダーでフィルタリングできます。これは通常のカプセル化解除された IP トラフィック ポストです。SVI 20 に適用されている ACL は、非 VXLAN 環境内の IP トラフィックの場合と同様にフィルタリングできます。ACL の詳細については、[アクセスコントロールリストについて \(1 ページ\)](#) を参照してください。

egr-racl TCAM リージョンは、次のように切り分ける必要があります。

### 手順の概要

1. **configure terminal**
2. **hardware access-list tcam region egr-racl 256**
3. **ip access-list name**
4. *sequence-number* **permit ip source-address destination-address**
5. **interface vlan vlan-id**
6. **no shutdown**
7. **ip access-group access-list out**
8. **vrf member vxlan-number**
9. **no ip redirects**
10. **ip address ip-address/length**
11. **no ipv6 redirects**
12. **fabric forwarding mode anycast-gateway**

### 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><br><br>例：<br>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。 |

|         | コマンドまたはアクション  | 目的   |
|---------|---|--|
| ステップ 2  | <b>hardware access-list tcam region egr-racl 256</b><br>例：<br>switch(config)# <b>hardware access-list tcam region egr-racl 256</b>                  | ACL TCAM リージョン サイズを変更します。  |
| ステップ 3  | <b>ip access-list name</b><br>例：<br>switch(config)# <b>ip access-list Racl_on_Source_Vlan_SVI</b>   | IPv4 ACL を作成し、IP ACL コンフィギュレーション モードを開始します。name 引数は 64 文字以内で指定します。   |
| ステップ 4  | <i>sequence-number</i> <b>permit ip source-address destination-address</b><br>例：<br>switch(config-acl)# <b>10 permit ip 10.1.1.1/32 20.1.1.1/32</b> | 条件に一致する IPv4 トラフィックを許可または拒否する、ACL のルールを作成します。<br><br><i>source-address destination-address</i> 引数には、IP アドレスとネットワーク ワイルドカード、IP アドレスと可変長サブネットマスク、ホストアドレス、または任意のアドレスを指定する <b>any</b> があります。 |
| ステップ 5  | <b>interface vlan vlan-id</b><br>例：<br>switch(config-acl)# <b>interface vlan vlan20</b>   | インターフェイス コンフィギュレーション モードを開始します。vlan-id は、DHCP サーバ IP アドレスを設定する VLAN の ID です。   |
| ステップ 6  | <b>no shutdown</b><br>例：<br>switch(config-if)# <b>no shutdown</b>   | shutdown コマンドを使用してください。  |
| ステップ 7  | <b>ip access-group access-list out</b><br>例：<br>switch(config-if)# <b>ip access-group Racl_On_Detination_Vlan_SVI out</b>                           | IPv4 ACL または IPv6 ACL を、指定方向のトラフィックのレイヤ 3 インターフェイスに適用します。各方向にルータ ACL を 1 つ適用できます。  |
| ステップ 8  | <b>vrf member vxlan-number</b><br>例：<br>switch(config-if)# <b>vrf member Cust-A</b>   | ホストの SVI を設定します。   |
| ステップ 9  | <b>no ip redirects</b><br>例：<br>switch(config-if)# <b>no ip redirects</b>   | デバイスがリダイレクトを送信しないようにします。   |
| ステップ 10 | <b>ip address ip-address/length</b><br>例：<br>switch(config-if)# <b>ip address 20.1.1.10/24</b>  | このインターフェイスの IP 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 11 | <b>no ipv6 redirects</b><br>例 :<br>switch(config-if)# <b>no ipv6 redirects</b>   | ICMP のリダイレクトメッセージが BFD 対応インターフェイスでディセーブルであることを確認します。 |
| ステップ 12 | <b>fabric forwarding mode anycast-gateway</b><br>例 :<br>switch(config-if)# <b>fabric forwarding mode anycast-gateway</b> | エニーキャスト ゲートウェイ転送モードを構成します。                           |





## 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。