ACL の設定

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

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	PACL	入力 VTEP	L2 ポート	ネットワークにアクセス [GROUP : encap direction]	ネイティブ L2 トラフィック [GROUP : inner]	YES
2		VACL	入力 VTEP	VLAN	ネットワークにアクセス [GROUP : encap direction]	ネイティブ L2 トラフィック [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
3	入力	RACL	入力 VTEP	テナント L3 SVI	ネットワークにアクセス [GROUP：encap direction]	ネイティブ L3 トラフィック [GROUP：inner]	YES
4	出力	RACL	入力 VTEP	アップリンク L3/L3-PO/SVI	ネットワークにアクセス [GROUP：encap direction]	VXLAN encap [GROUP：outer]	NO
5	入力	RACL	出力 VTEP	アップリンク L3/L3-PO/SVI	ネットワークにアクセス [GROUP：decap direction]	VXLAN encap [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 [GROUP：decap direction]	ネイティブ L2 トラフィック [GROUP：inner]	NO
7a		VACL	出力 VTEP	VLAN	ネットワークにアクセス [GROUP：decap direction]	ネイティブ L2 トラフィック [GROUP：inner]	YES
7b		VACL	出力 VTEP	宛先 VLAN	ネットワークにアクセス [GROUP：decap direction]	ネイティブ L3 トラフィック [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 [GROUP：decap direction]	Post-decap L3 トラフィック [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。

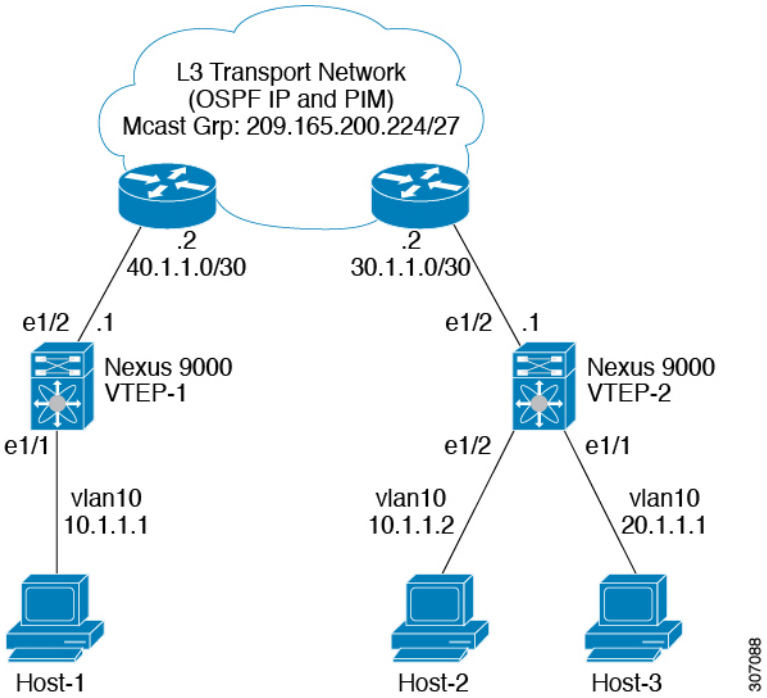
- Host-1: 10.1.1.1/24 VLAN-10
- Host-2: 10.1.1.2/24 VLAN-10
- Host-3: 20.1.1.1/24 VLAN-20
- ケース1：VLAN-10 の Host-1 と Host-2 の間を流れるレイヤ 2 トラフィック/L2 VNI。
- ケース2：VLAN-10 および VLAN-20 上の Host-1 と Host-3 の間を流れるレイヤ 3 トラフィック/L3 VNI。

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。

図 *1 : VXLAN Encap* スイッチのポート *ACL*



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

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	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	**hardware access-list tcam region ing-ifacl 256** 例：	**ing-ifacl** 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。

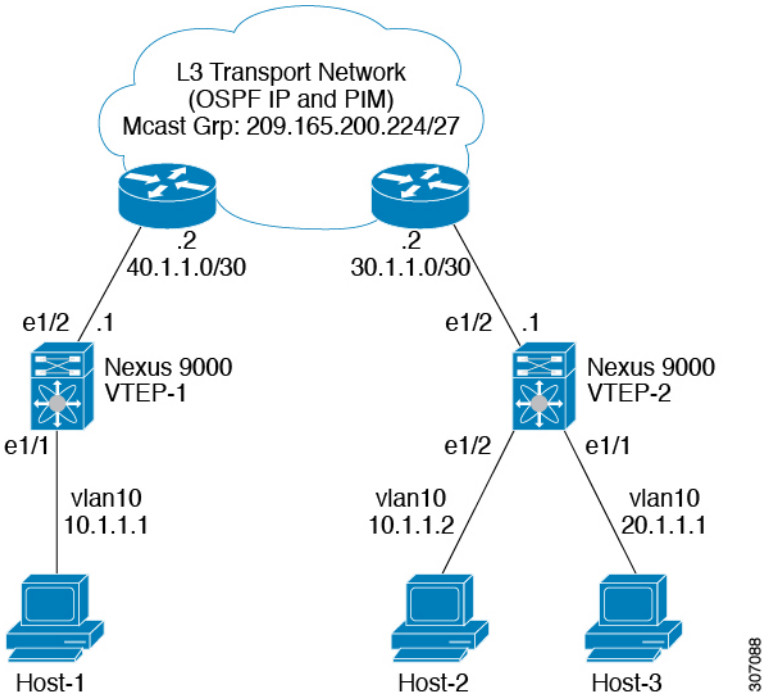
	コマンドまたはアクション	目的
	`switch(config)# hardware access-list tcam region ing-ifacl 256`	
ステップ 3	**ip access-list** *name* 例： `switch(config)# ip access list PACL_On_Host_Port`	IPv4 ACL を作成し、IP ACL コンフィギュレーション モードを開始します。name 引数は 64 文字以内で指定します。
ステップ 4	*sequence-number* **permit ip** *source-address destination-address* 例： `switch(config-acl)# 10 permit ip 10.1.1.1/32 10.1.1.2/32`	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。 *source-address destination-address* 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 **any** などがあります。
ステップ 5	**exit** 例： `switch(config-acl)# exit`	IP ACL 設定モードを終了します。
ステップ 6	**interface ethernet** *slot/port* 例： `switch(config)# interface ethernet1/1`	インターフェイス設定モードを開始します。
ステップ 7	**ip port access-group** *pacl-name***in** 例： `switch(config-if)# ip port access-group PACL_On_Host_Port in`	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	**switchport** 例： `switch(config-if)# switchport`	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	**switchport mode trunk** 例： `switch(config-if)# switchport mode trunk`	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。
ステップ 10	**switchport trunk allowed vlan** *vlan-list* 例：	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

	コマンドまたはアクション	目的
	`switch(config-if)# switchport trunk allowed clan 10,20`	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	**no shutdown** 例： `switch(config-if)# no shutdown`	**shutdown** 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。

図 *2 : VXLAN Encap* スイッチの *VLAN ACL*



手順

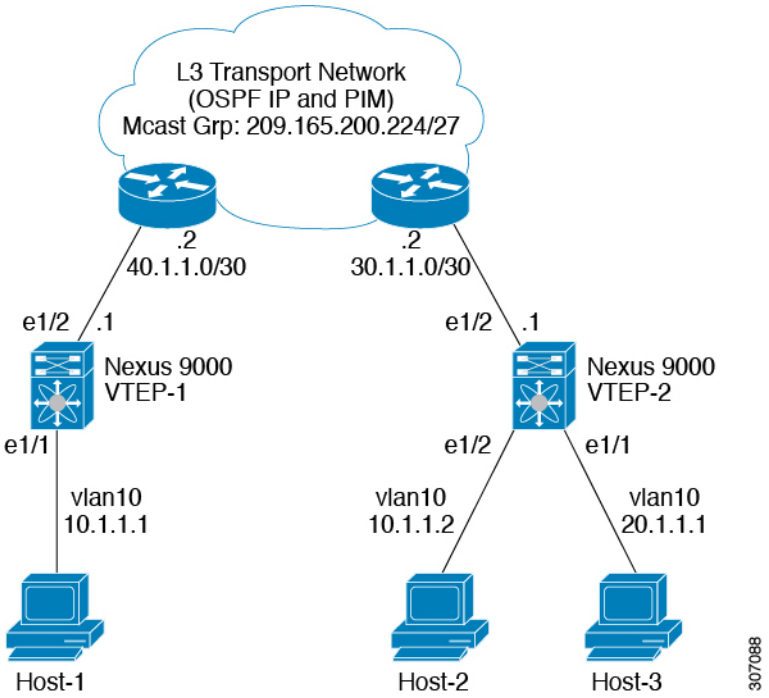
	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**ip access-list** *name* 例： `switch(config)# ip access list Vacl_On_Source_VLAN`	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 3	*sequence-number* **permit ip** *source-address destination-address* 例： `switch(config-acl)# 10 permit ip 10.1.1.1 10.1.1.2`	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。 *source-address destination-address* 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 **any** などがあります。
ステップ 4	**vlan access-map** *map-name* **[***sequence-number***]** 例： `switch(config-acl)# vlan access-map Vacl_on_Source_Vlan 10`	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。 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	**match ip address** *ip-access-list* 例： `switch(config-acl)# match ip address Vacl_on_Source_Vlan`	アクセス マップ エントリに ACL を指定します。
ステップ 6	**action forward** 例： `switch(config-acl)# action forward`	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	**vlan access-map** *name* 例： `switch(config-acl)# vlan access map Vacl_on_Source_Vlan`	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。

図 *3 : VXLAN Encap* スイッチでの入力の *SVI* でのルーテッド *ACL*



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

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	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	**hardware access-list tcam region ing-ifacl 256** 例： `switch(config)# hardware access-list tcam region ing-ifacl 256`	**ing-racl** 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。

	コマンドまたはアクション	目的
ステップ 3	**ip access-list** *name* 例： `switch(config)# ip access list PACL_On_Host_Port`	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	*sequence-number* **permit ip** *source-address destination-address* 例： `switch(config-acl)# 10 permit ip 10.1.1.1/32 10.1.1.2/32`	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。 *source-address destination-address* 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 **any** などがあります。
ステップ 5	**exit** 例： `switch(config-acl)# exit`	IP ACL 設定モードを終了します。
ステップ 6	**interface ethernet** *slot/port* 例： `switch(config)# interface ethernet1/1`	インターフェイス設定モードを開始します。
ステップ 7	**no shutdown** 例： `switch(config-if)# no shutdown`	**shutdown** コマンドを無効にします。
ステップ 8	**ip access-group** *pacl-name***in** 例： `switch(config-if)# ip port access-group Racl_On_Source_Vlan_SVI in`	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	**vrf member** *vxlan-number* 例： `switch(config-if)# vrf member Cust-A`	ホストの SVI を設定します。
ステップ 10	**no ip redirects** 例： `switch(config-if)# no ip redirects`	デバイスがリダイレクトを送信しないようにします。

	コマンドまたはアクション	目的
ステップ 11	**ip address** *ip-address* 例： `switch(config-if)# ip address 10.1.1.10`	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	**no ipv6 redirects** 例： `switch(config-if)# no ipv6 redirects`	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	**fabric forwarding mode anycast-gateway** 例： `switch(config-if)# fabric forwarding mode anycast-gateway`	エニーキャスト ゲートウェイ転送モードを設定します。

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 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

入力の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 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 チャネル アップリンク インターフェイスにも適用されます。

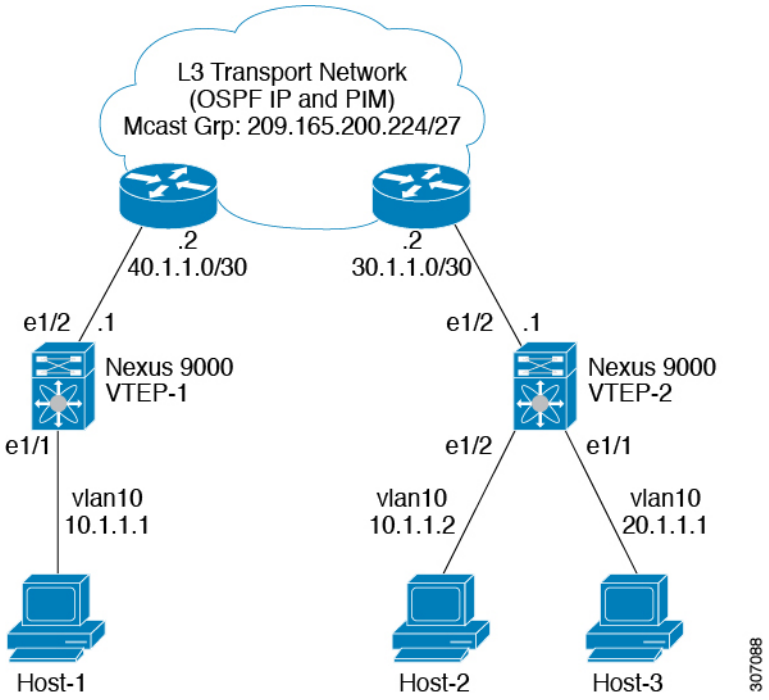
出力のアクセス ポートのポート ACL

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。

図 *4 : VXLAN Decap* スイッチのレイヤ *2 VNI* の *VLAN ACL*



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

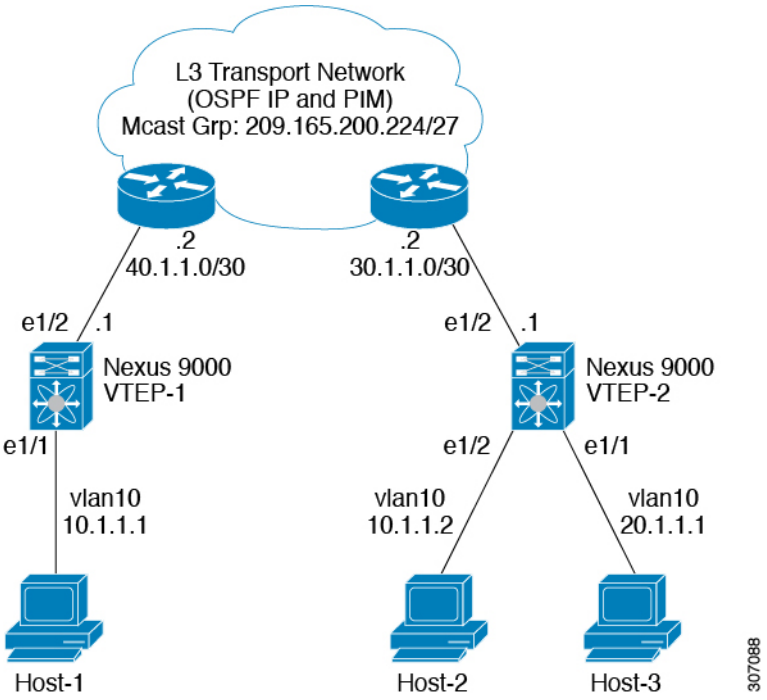
	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**hardware access-list tcam region vacl 256** 例： `switch(config)# hardware access-list tcam region vacl 256`	ACL TCAM リージョン サイズを変更します。
ステップ 3	**ip access-list** *name* 例： `switch(config)# ip access list VXLAN-L2-VNI`	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	**statistics per-entry** 例： `switch(config-acl)# statistics per-entry`	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	*sequence-number* **permit ip** *source-address destination-address* 例： `switch(config-acl)# 10 permit ip 10.1.1.1/32 10.1.1.2/32`	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。 *source-address destination-address* 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 **any** などがあります。
ステップ 6	*sequence-number* **permit** *protocol source-address destination-address* 例： `switch(config-acl)# 20 permit tcp 10.1.1.2/32 10.1.1.1/32`	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。 *source-address destination-address* 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 **any** などがあります。
ステップ 7	**exit** 例： `switch(config-acl)# exit`	ACL 設定モードを終了します。
ステップ 8	**vlan access-map** *map-name* **[***sequence-number***]** 例： `switch(config)# vlan access-map VXLAN-L2-VNI 10`	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。 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 9	**match ip address** *list-name* 例： `switch(config-access-map)# match ip VXLAN-L2-VNI`	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VLAN 20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。

図 *5 : VXLAN Decap* スイッチのレイヤ *3 VNI* の *VLAN ACL*



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

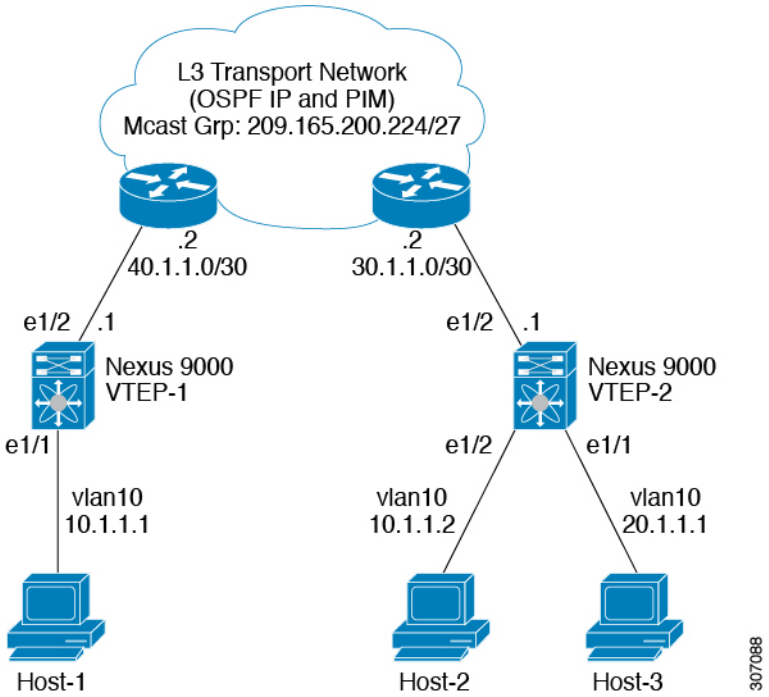
	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**hardware access-list tcam region vacl 256** 例： `switch(config)# hardware access-list tcam region vacl 256`	ACL TCAM リージョン サイズを変更します。

	コマンドまたはアクション	目的
ステップ 3	**ip access-list** *name* 例： `switch(config)# ip access list VXLAN-L3-VNI`	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	**statistics per-entry** 例： `switch(config)# statistics per-entry`	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	*sequence-number* **permit ip** *source-address destination-address* 例： `switch(config-acl)# 10 permit ip 10.1.1.1/32 20.1.1.1/32`	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。 *source-address destination-address* 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 **any** などがあります。
ステップ 6	*sequence-number* **permit** *protocol source-address destination-address* 例： `switch(config-acl)# 20 permit tcp 20.1.1.1/32 10.1.1.1/32`	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	**vlan access-map** *map-name* **[***sequence-number***]** 例： `switch(config-acl)# vlan access-map VXLAN-L3-VNI 10`	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。 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	**action forward** 例： `switch(config-acl)# action forward`	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。

図 *6 : VXLAN* デキャップ スイッチでの出力の *SVI* でのルーテッド *ACL*



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

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	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	**hardware access-list tcam region egr-racl 256** 例： `switch(config)# hardware access-list tcam region egr-racl 256`	ACL TCAM リージョン サイズを変更します。

	コマンドまたはアクション	目的
ステップ 3	**ip access-list** *name* 例： `switch(config)# ip access-list Racl_on_Source_Vlan_SVI`	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	*sequence-number* **permit ip** *source-address destination-address* 例： `switch(config-acl)# 10 permit ip 10.1.1.1/32 20.1.1.1/32`	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。 *source-address destination-address* 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 **any** などがあります。
ステップ 5	**interface vlan** *vlan-id* 例： `switch(config-acl)# interface vlan vlan20`	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	**no shutdown** 例： `switch(config-if)# no shutdown`	shutdown コマンドを使用してください。
ステップ 7	**ip access-group** *access-list* **out** 例： `switch(config-if)# ip access-group Racl_On_Detination_Vlan_SVI out`	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	**vrf member** *vxlan-number* 例： `switch(config-if)# vrf member Cust-A`	ホストの SVI を設定します。
ステップ 9	**no ip redirects** 例： `switch(config-if)# no ip redirects`	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	**ip address** *ip-address/length* 例： `switch(config-if)# ip address 20.1.1.10/24`	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	**no ipv6 redirects** 例： `switch(config-if)# no ipv6 redirects`	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	**fabric forwarding mode anycast-gateway** 例： `switch(config-if)# fabric forwarding mode anycast-gateway`	エニーキャスト ゲートウェイ転送モードを設定します。