VLAN ACL の設定

この章では、Cisco NX-OS デバイスの VLAN ACL（アクセス リスト）の設定方法を説明します。

この章は、次の項で構成されています。

VLAN ACL について

VLAN ACL（VACL）は、MAC ACL または IP ACL の適用例の 1 つです。VACL を設定し、VLAN との間でルーティングされるかまたは VLAN 内でブリッジングされるすべてのパケットに適用できます。VACL は、セキュリティ パケット フィルタリングおよび特定の物理インターフェイスへのトラフィックのリダイレクトだけを目的としたものです。VACL は方向（入力または出力）で定義されることはありません。

VLAN アクセス マップとエントリ

VACL は、アクセス マップを使用して、1 つまたは複数のマップ エントリを順序化したリストを収容します。各マップ エントリは、IP または MAC ACL を処理に関連付けます。各エントリにはシーケンス番号が付き、これに基づいてエントリの優先度を管理できます。

デバイスがパケットに VACL を適用する際、パケットを許可する ACL を含む最初のアクセス マップ エントリで設定されている処理を適用します。

VACL とアクション

アクセス マップ コンフィギュレーション モードでは、action コマンドを使用して、次のいずれかのアクションを指定します。

Forward

デバイスの通常の動作によって決定された宛先にトラフィックを送信します。

Redirect

1 つまたは複数の指定インターフェイスにトラフィックをリダイレクトします。

Drop

トラフィックをドロップします。ドロップを処理として指定する場合、ドロップされたパケットのログをデバイスが記録するよう指定することもできます。

VACL の統計情報

VACL の各ルールのグローバル統計が維持されます。VACL を複数の VLAN に適用した場合、保持されるルール統計情報は、そのVACLが適用されている各インターフェイス上で一致（ヒット）したパケットの総数になります。

（注） インターフェイスレベルの VACL 統計はサポートされていません。

設定する VLAN アクセス マップごとに、その VACL の統計情報を維持するかどうかを指定できます。この機能を使用すると、VACLによってフィルタリングされたトラフィックのモニタが必要かどうかに応じて、あるいは VLAN アクセスマップの設定のトラブルシューティングが必要かどうかに応じて、VACL 統計をオンまたはオフにできます。

VACL に対する Session Manager のサポート

Session Manager は VACL の設定をサポートしています。この機能によって、ACL の設定を確認し、設定を実行コンフィギュレーションにコミットする前に、その設定が必要とするリソースが利用可能かどうかを確認できます。Session Manager の詳細については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』を参照してください。

VACL の前提条件

VACL の前提条件は次のとおりです。

- VACL に使用する IP ACL または MAC ACL が存在し、必要な方法でトラフィックをフィルタリングするように設定されていることを確認します。

VACL の注意事項と制約事項

VACL の設定に関する注意事項は次のとおりです。

- ACLは、セッション マネージャを使用して設定することを推奨します。この機能によって、ACL の設定を確認し、設定を実行コンフィギュレーションにコミットする前に、その設定が必要とするリソースが利用可能かどうかを確認できます。Session Manager の詳細については、『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』を参照してください。
- 適用する ACL エントリが多すぎると、設定が拒否される可能性があります。
- SPAN 宛先ポートへの VACL リダイレクトはサポートされません。
- VACL のロギングはサポートされません。
- TCAM リソースは、VACL を複数の VLAN で適用する場合、共有されません。
- Cisco Nexus 9200 および 9300-EX シリーズスイッチは、VACL リダイレクトオプションをサポートしています。1 つの物理インターフェイスまたはポートチャネルインターフェイスへのリダイレクトが許可されます。
- VACL は、N9K-X9636C-R、N9K-X9636C-RX、および N9K-X9636Q-R ライン カードを搭載した Cisco Nexus 9500 Series スイッチではサポートされていません。
- VACL では deny 文はサポートされていません。その代わりに、permit 文と「drop」アクションを組み合わせると、同様の結果を得ることができます。
- VACL を「redirect」オプションを使用して設定する場合、リダイレクトインターフェイスとして定義するインターフェイスは、この VACL の適用先である VLAN のメンバーとして設定する必要があります。リダイレクションを機能させるには、この VLAN がこのインターフェイス上でフォワーディング状態になっている必要があります。これらの条件が満たされない場合、スイッチは VACL とマッチしたパケットをドロップします。
- VACL カウンタをクリアするには、アクティブな VLAN フィルタが設定されていることを確認する必要があります。

VXLAN の VACL には、次のガイドラインが適用されます。

- アクセスからネットワーク方向（レイヤ 2 からレイヤ 3 のカプセル化パス）の VXLAN VLAN に適用される VACL は、内部ペイロードでサポートされます。
- VACL をアクセス側で使用して、オーバーレイ ネットワークに進入するトラフィックをフィルタ処理して除外することを推奨します。
- カプセル化解除された VXLAN トラフィックでの出力 VACL は、サポートされません。

VACL のデフォルト設定

次の表に、VACL パラメータのデフォルト設定値を示します。

***Table 1: VACL* のデフォルト パラメータ**

パラメータ	デフォルト
VACL	デフォルトでは IP ACL は存在しません。
ACL ルール	すべての ACL に暗黙のルールが適用されます。

VACL の設定

VACL の作成または VACL エントリの追加

VACL エントリを新規作成したり、既存の VACL にエントリを追加できます。どちらの場合も、作成した VACL エントリが、1 つまたは複数の ACL を一致トラフィックに適用される処理と関連付ける VLAN アクセス マップ エントリとなります。

Before you begin

VACL に使用する ACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		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	**vlan access-map** *map-name* [*sequence-number*]
	Example:
	`switch(config)# vlan access-map acl-mac-map`
	`switch(config-access-map)#`
		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。

	Command or Action	Purpose

ステップ 3	次のいずれかのコマンドを入力します。
	• **match** {**ip** | **ipv6**} **address** *ip-access-list*
	• **match mac address** *mac-access-list*
	Example:
	`switch(config-access-map)# match mac address acl-ip-lab`
	Example:
	`switch(config-access-map)# match mac address acl-mac-01`
		アクセス マップ エントリに ACL を指定します。

ステップ 4	**action** {**drop** | **forward** | **redirect**}
	Example:
	`switch(config-access-map)# action forward`
	Example:
	`switch(config-access-map)# vlan access-map vacl1`
	`switch(config-access-map)# action redirect e1/1`
	`switch(config-access-map)# action redirect po100`
		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。
		action コマンドは、**drop**、**forward**、および **redirect** オプションをサポートします。

ステップ 5	(Optional) [**no**] **statistics per-entry** **Example:** `switch(config-access-map)# 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。 **no** オプションを使用すると、デバイスはその VACL のグローバル統計の維持を停止します。
ステップ 6	(Optional) **show running-config aclmgr** **Example:** `switch(config-access-map)# show running-config aclmgr`	ACL の設定を表示します。
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `switch(config-access-map)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VACL または VACL エントリの削除

VACL を削除できます。これにより、VLAN アクセス マップも削除されます。

また、VACL から単一の VLAN アクセス マップ エントリを削除することもできます。

Before you begin

その VACL が VLAN に適用されているかどうかを確認します。削除できるのは、現在適用されている VACL です。VACL を削除しても、その VACL が適用されていた VLAN の設定は影響を受けません。デバイスは削除された VACL を空であると見なします。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		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	**no vlan access-map** *map-name* [*sequence-number*] **Example:** `switch(config)# no vlan access-map acl-mac-map 10`	指定したアクセス マップの VLAN アクセス マップの設定を削除します。*sequence-number* 引数を指定して、VACL に複数のエントリが含まれる場合、このコマンドにより指定したエントリだけが削除されます。
ステップ 3	(Optional) **show running-config aclmgr** **Example:** `switch(config)# show running-config aclmgr`	ACL の設定を表示します。
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VACL の VLAN への適用

VACL を VLAN に適用できます。

Before you begin

VACL を適用する際には、その VACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:**	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。

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	

ステップ 2	[**no**] **vlan filter** *map-name* **vlan-list** *list*
	Example:
	`switch(config)# vlan filter acl-mac-map vlan-list 1-20,26-30`
	`switch(config)#`
		指定したリストによって、VACL を VLANに適用します。**no** を使用すると、VACL の適用が解除されます。

ステップ 3	(Optional) **show running-config aclmgr** **Example:** `switch(config)# show running-config aclmgr`	ACL の設定を表示します。
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VACL 設定の確認

VACL 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show running-config aclmgr [**all**]	VACL-related の設定も含めて、ACL の設定を表示します。 **Note** このコマンドは、実行コンフィギュレーションのユーザ設定 ACL を表示します。**all** オプションを使用すると、実行コンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。
show startup-config aclmgr [**all**]	ACL のスタートアップ コンフィギュレーションを表示します。 **Note** このコマンドは、スタートアップ コンフィギュレーションのユーザ設定 ACL を表示します。**all** オプションを使用すると、スタートアップ コンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。
show vlan filter	VLAN に適用されている VACL の情報を表示します。
show vlan access-map	VLAN アクセス マップに関する情報を表示します。

VACL 統計情報のモニタリングとクリア

VACL の統計情報をモニタまたはクリアを行うには、次の表に示すコマンドのいずれかを使用します。

コマンド	目的
show vlan access-list	VACL の設定を表示します。VLAN アクセス マップに **statistics per-entry** コマンドが含まれている場合は、**show vlan access-list** コマンドの出力に、各ルールと一致したパケットの数が含まれます。
clear vlan access-list counters	VACL の統計情報をクリアします。

VACL の設定例

次の例では、acl-mac-01 という名前の MAC ACL で許可されたトラフィックを転送する VACL を設定し、その VACL を VLAN 50 ～ 82 に適用します。

```
conf t
vlan access-map acl-mac-map
  match mac address acl-mac-01
  action forward
vlan filter acl-mac-map vlan-list 50-82
```

VACL に関する追加情報

関連資料

関連項目	マニュアル タイトル
QoS の設定	『*Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide*』