



V コマンド

この章では、V で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

vlan access-map

新規の VLAN アクセス マップを作成したり、既存の VLAN アクセス マップを設定したりするには、**vlan access-map** コマンドを使用します。VLAN アクセス マップを削除するには、このコマンドの **no** 形式を使用します。

vlan access-map *map-name*

no vlan access-map *map-name*

構文の説明

<i>map-name</i>	作成または設定する VLAN アクセス マップ名。名前では最大 64 文字までの英数字を使用でき、大文字と小文字が区別されます。
-----------------	--

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

各 VLAN アクセス マップには、1 つの **match** コマンドと 1 つの **action** コマンドを含めることができます。

例

次に、vlan-map-01 という名前で VLAN アクセス マップを作成して、そのマップに ip-acl-01 という名前の IPv4 ACL を割り当て、スイッチが ACL に一致するパケットを転送するよう指定し、マップに一致するトラフィックの統計情報をイネーブルにする例を示します。

```
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# statistics
```

関連コマンド

コマンド	説明
action	VLAN アクセス マップにトラフィック フィルタリングのアクションを指定します。
match	VLAN アクセス マップにトラフィック フィルタリングの ACL を指定します。
show vlan access-map	すべての VLAN アクセス マップまたは 1 つの VLAN アクセス マップを表示します。
show vlan filter	VLAN アクセス マップが適用されている方法に関する情報を表示します。
vlan filter	1 つ以上の VLAN に VLAN アクセス マップを適用します。

vlan filter

VLAN アクセス マップを 1 つ以上の VLAN に適用するには、**vlan filter** コマンドを使用します。VLAN アクセス マップの適用を解除するには、このコマンドの **no** 形式を使用します。

vlan filter *map-name* **vlan-list** *VLAN-list*

no vlan filter *map-name* [**vlan-list** *VLAN-list*]

構文の説明	
<i>map-name</i>	作成または設定する VLAN アクセス マップ名
vlan-list <i>VLAN-list</i>	VLAN アクセス マップがトラフィックをフィルタリングする 1 つ以上の VLAN の ID を指定します。 ハイフン (-) を使用して、VLAN ID の範囲の開始 ID と終了 ID を区別します (たとえば、70-100)。 カンマ (,) を使用して、各 VLAN ID および VLAN ID の範囲を区別します (たとえば、20,70-100,142)。 (注) このコマンドの no 形式を使用する場合、 <i>VLAN-list</i> 引数を省略できます。この引数を省略する場合、スイッチはアクセス マップが適用されているすべての VLAN からアクセス マップを削除します。

コマンド デフォルト なし

コマンド モード グローバル コンフィギュレーション モード

コマンド履歴	リリース	変更内容
	4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン 1 つ以上の VLAN に VLAN アクセス マップを適用できます。VLAN に適用できるのは、1 つの VLAN アクセス マップだけです。このコマンドの **no** 形式を使用すると、アクセス マップを適用したときに指定したすべてまたは一部の VLAN リストから VLAN アクセス マップの適用を解除できます。適用されたすべての VLAN からアクセス マップの適用を解除する場合、*VLAN-list* 引数を省略できます。現在適用されている VLAN のサブセットからアクセス マップの適用を解除する場合、*VLAN-list* 引数を使用して、アクセス マップを削除する必要がある VLAN を指定します。

例 次に、vlan-map-01 という名前の VLAN アクセス マップを VLAN 20 ~ 45 に適用する例を示します。

```
switch(config)# vlan filter vlan-map-01 20-45
```

関連コマンド

コマンド	説明
action	VLAN アクセス マップにトラフィック フィルタリングのアクションを指定します。
match	VLAN アクセス マップにトラフィック フィルタリングの ACL を指定します。
show vlan access-map	すべての VLAN アクセス マップまたは 1 つの VLAN アクセス マップを表示します。
show vlan filter	VLAN アクセス マップが適用されている方法に関する情報を表示します。
vlan access-map	VLAN アクセス マップを設定します。

vlan policy deny

ユーザ ロールの VLAN ポリシー コンフィギュレーション モードを開始するには、**vlan policy deny** コマンドを使用します。ユーザ ロールのデフォルトの VLAN ポリシーに戻すには、このコマンドの **no** 形式を使用します。

vlan policy deny

no vlan policy deny

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンドデフォルト

すべての VLAN

コマンドモード

ユーザ ロール コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、ユーザ ロールの VLAN ポリシー コンフィギュレーション モードを開始する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)#
```

次に、ユーザ ロールのデフォルトの VLAN ポリシーに戻す例を示します。

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# no vlan policy deny
```

関連コマンド

コマンド	説明
role name	ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールの情報を表示します。

vrf policy deny

ユーザの Virtual Forwarding and Routing (VRF; 仮想ルーティングおよび転送) インスタンス ポリシーへの拒否アクセスを設定するには、**vrf policy deny** コマンドを使用します。ユーザ ロールのデフォルトの VRF ポリシー設定に戻すには、このコマンドの **no** 形式を使用します。

vrf policy deny

no vrf policy deny

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

ユーザ ロール コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、ユーザ ロールの VRF ポリシー コンフィギュレーション モードを開始する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)#
```

次に、ユーザ ロールのデフォルトの VRF ポリシーに戻す例を示します。

```
switch(config)# role name MyRole
switch(config-role)# no vrf policy deny
```

関連コマンド

コマンド	説明
role name	ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールの情報を表示します。

vsan policy deny

ユーザ ロールの VSAN ポリシーへの拒否アクセスを設定するには、**vsan policy deny** コマンドを使用します。ユーザ ロールのデフォルトの VSAN ポリシー設定に戻すには、このコマンドの **no** 形式を使用します。

vsan policy deny

no vsan policy deny

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンドデフォルト

なし

コマンドモード

ユーザ ロール コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

VSAN ポリシーへのアクセスを許可するには、**permit vsan** コマンドを使用します。

例

次に、ユーザ ロールの VSAN ポリシーへのアクセスを拒否する方法の例を示します。

```
switch(config)# role name MyRole
switch(config-role)# vsan policy deny
switch(config-role-vsan)#
```

次に、ユーザ ロールのデフォルトの VSAN ポリシー設定に戻す例を示します。

```
switch(config)# role name MyRole
switch(config-role)# vsan policy deny
switch(config-role-vsan)# no vsan policy deny
switch(config-role)#
```

関連コマンド

コマンド	説明
permit vsan	ユーザの VSAN ポリシーへの許可アクセスを設定します。
role name	ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールの情報を表示します。

