ポート セキュリティ

この章は、次の項で構成されています。

ポート セキュリティと ACI について

ポート セキュリティ機能は、ポートごとに取得される MAC アドレスの数を制限することによって、不明な MAC アドレスでフラッディングしないように ACI ファブリックを保護します。ポート セキュリティ機能のサポートは、物理ポート、ポート チャネル、および仮想ポート チャネルで使用できます。

ポート セキュリティに関するガイドラインと制約事項

次のようなガイドラインと制約事項があります。

- ポート セキュリティは、ポートごとに使用できます。
- ポートセキュリティは、物理ポート、ポートチャネル、および仮想ポートチャネル（vPC）でサポートされています。
- スタティック MAC アドレスとダイナミック MAC アドレスがサポートされています。
- セキュアなポートからセキュアでないポートへと、セキュアでないポートからセキュアなポートへの MAC アドレスの移動がサポートされています。
- MAC アドレスの制限は、MAC アドレスにのみ適用され、MAC と IP によるアドレスには実行されません。

- ポート セキュリティは、ファブリック エクステンダ（FEX）ではサポートされていません。

ポート レベルでのポート セキュリティ

APICでは、ユーザがスイッチポートのポートセキュリティを設定できます。ポート上でMACが制限の最大設定値を超過すると、超過したMACアドレスからすべてのトラフィックが転送されます。次の属性がサポートされます。

- **ポート セキュリティのタイムアウト** ：現在サポートされているタイムアウト値値は、60 ~ 3600 秒の範囲でサポートされています。
- **違反行為**：違反行為は保護モードで使用できます。保護モードでは、MAC の取得が無効になるため、MAC アドレスは CAM テーブルに追加されません。Mac ラーニングが設定されているタイムアウト値の後に再度有効になります。
- **最大エンドポイント** ：現在のサポートされている最大のエンドポイント設定値は、0 ～ 12000 の範囲でサポートされています。最大エンドポイント値が 0 の場合、そのポートではポート セキュリティ ポリシーが無効になります。

APIC GUI を使用したポート セキュリティの設定

手順

ステップ 1 メニュー バーで [ファブリック アクセス ポリシー（**Fabric** > **Access Policies**）] をクリックし、[ナビゲーション（**Navigation**）] ペインで [ポリシー インターフェイス ポート セキュリティ（**Policies** > **Interface** > **Port Security**）] を展開します。

ステップ 2 **[ポート セキュリティ]** 右クリックして、**[ポート セキュリティ ポリシーの作成]** をクリックします。

ステップ 3 **[ポート セキュリティ ポリシーの作成]** ダイアログ ボックスで、次の操作を実行します。

a) [Name] フィールドにポリシーの名前を入力します。
b) **[ポート セキュリティのタイムアウト]** フィールドに、インターフェイスの MAC ラーニングを再度有効にする前に、タイムアウトの値を選択します。
c) **[最大エンドポイント]** フィールドに、インターフェイスで学習可能なエンドポイントの最大数の希望値を選択します。
d) **[違反アクション]** フィールドで、使用可能なオプションは **[保護]** です。[Submit] をクリックします。ポート セキュリティ ポリシーが作成されます。

ステップ 4 （注）
リーフ スイッチのインターフェイスを設定するときに、使用可能なポート セキュリティ ポリシーのリストからポート セキュリティ ポリシーを選択することができます。

[ナビゲーション] ペインで、**[ファブリック]**>**[インベントリ]**>**[トポロジ]** をクリックし、目的のリーフ スイッチに移動します。インターフェイスを設定する適切なポートを選択し、ポート セキュリティ ポリシー ドロップダウン リストから関連付けに必要なポート セキュリティ ポリシーを選択します。
これで、ポート上のポート セキュリティの設定を完了します。

REST API を使用して、ポート セキュリティの設定

手順

ポート セキュリティを設定します。

例：

```
<polUni>
 <infraInfra>

   <l2PortSecurityPol name="testL2PortSecurityPol" maximum="10" violation=”protect” timeout=“300"/>


    <infraNodeP name="test">
        <infraLeafS name="test" type="range">
            <infraNodeBlk name="test" from_="101" to_="102"/>
        </infraLeafS>
        <infraRsAccPortP tDn="uni/infra/accportprof-test"/>
    </infraNodeP>

            <infraAccPortP name="test">
        <infraHPortS name="pselc" type="range">
           <infraPortBlk name="blk"
                                fromCard="1" toCard="1" fromPort="20" toPort="22">
                  </infraPortBlk>
            <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-testPortG" />
         </infraHPortS>
            </infraAccPortP>

            <infraFuncP>
            <infraAccPortGrp name="testPortG">
                <infraRsL2PortSecurityPol tnL2PortSecurityPolName="testL2PortSecurityPol"/>
                <infraRsAttEntP tDn="uni/infra/attentp-test" />
            </infraAccPortGrp>
            </infraFuncP>

    <infraAttEntityP name="test">
        <infraRsDomP tDn="uni/phys-mininet"/>
    </infraAttEntityP>
 </infraInfra>
</polUni>
```

CLI を使用したポート セキュリティの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	コンフィギュレーション モードに入ります。
ステップ 2	**leaf** *node-id* 例： `apic1(config)# leaf 101`	設定するリーフを指定します。
ステップ 3	**interface** *type-or-range* 例： `apic1(config-leaf)# interface eth 1/2-4`	設定するインターフェイスまたはインターフェイスの範囲を指定します。
ステップ 4	[**no**] **switchport port-security maximum** *number-of-addresses* 例： `apic1(config-leaf-if)# switchport port-security maximum 1`	インターフェイスのセキュア MAC アドレスの最大数を設定します。範囲は 0 ～ 12000 アドレスです。デフォルトは 1 アドレスです。
ステップ 5	[**no**] **switchport port-security violation protect** 例： `apic1(config-leaf-if)# switchport port-security violation protect`	セキュリティ違反が検出された場合に実行するアクションを設定します。**protect** アクションは、十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、不明な送信元アドレスのパケットをドロップします。
ステップ 6	[**no**] **switchport port-security timeout** 例： `apic1(config-leaf-if)# switchport port-security timeout 300`	インターフェイスのタイムアウト値を設定します。範囲は 60 ～ 3600 です。デフォルトは 60 秒です。

例

次に、イーサネットインターフェイスでポートセキュリティを設定する方法を示します。

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface eth 1/2
apic1(config-leaf-if)# switchport port-security maximum 10
apic1(config-leaf-if)# switchport port-security violation protect
```

```
apic1(config-leaf-if)# switchport port-security timeout 300
```

次に、ポート チャネルでポート セキュリティを設定する例を示します。

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface port-channel po2
apic1(config-leaf-if)# switchport port-security maximum 10
apic1(config-leaf-if)# switchport port-security violation protect
apic1(config-leaf-if)# switchport port-security timeout 300
```

次に、仮想ポートチャネル（VPC）でポートセキュリティを設定する例を示します。

```
apic1# configure
apic1(config)# vpc domain explicit 1 leaf 101 102
apic1(config-vpc)# exit
apic1(config)# template port-channel po4
apic1(config-if)# exit
apic1(config)# leaf 101-102
apic1(config-leaf)# interface eth 1/11-12
apic1(config-leaf-if)# channel-group po4 vpc
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)# vpc context leaf 101 102
apic1(config-vpc)# interface vpc po4
apic1(config-vpc-if)# switchport port-security maximum 10
apic1(config-vpc-if)# switchport port-security violation protect
apic1(config-leaf-if)# switchport port-security timeout 300
```

ポート セキュリティおよびラーニング動作

非 vPC ポートまたはポート チャネルでは、新しいエンドポイントに対して学習イベントが発生し、新しい学習が許可されているか確認する検証が行われます。対応するインターフェイスに設定されていない、または無効なポート セキュリティ ポリシーが存在する場合、エンドポイント ラーニング動作はサポートされているものから変更されません。ポリシーが有効になっており制限に到達している場合、現在のサポートされているアクションは次の通りです。

- エンドポイントを学習し、ドロップ アクションのハードウェアにインストールします。
- サイレントに学習を破棄します。

制限に到達していない場合、エンドポイントが学習され、この新しいエンドポイントが発生したため制限に達しているかどうか確認する検証が行われます。制限に到達しており、学習の無効化アクションが設定されている場合、インターフェイス上のハードウェアでラーニングが無効になります（物理インターフェイスまたはポートチャネルまたはvPC）。制限に到達しており、学習の無効化アクションが設定されていない場合、エンドポイントはドロップアクションでハードウェアにインストールされます。このようなエンドポイントは、他のエンドポイントのように通常期限切れです。

初めて制限に達したとき、ポート セキュリティ ポリシー オブジェクトの動作状態がそれを反映して更新されます。スタティック ルールは、ユーザーに警告ができるように、障害の発生と定義されます。制限に到達すると、Syslog も発生します。

vPCの場合、MAC 制限に到達するとピア リーフ スイッチにも通知されるため、ラーニングがピアで無効になる可能性があります。vPC ピアはいつでも再起動でき、vPC レッグが動作不能になるか再起動できるため、この状態はピアと調和して vPC ピアはこの状態に同期されません。同期しない場合は、1 個のレッグでラーニングが有効になり、他のレッグで無効になる状況が発生する可能性があります。

デフォルトでは、制限に到達してラーニングが無効になると、60 秒のデフォルト タイムアウト値の後、自動的に再度有効になります。

保護モード

保護モードはセキュリティ違反を発生している以上に増やさないようにします。MAC の制限がポートで設定されている最大値を超えると、超過したMACアドレスからすべてのトラフィックはドロップされ、さらにラーニングが無効になります。

Visore を使用したポート セキュリティのインストールの確認

手順

ステップ 1 Cisco APIC で、Visore の l2PortSecurityPol クラスのクエリを実行して、ポート セキュリティ ポリシーのインストールを確認します。

ステップ 2 リーフ スイッチで、Visore で l2PortSecurityPolDef のクエリを実行して、具体的なオブジェクトがインターフェイスに存在することを確認します。
ポート セキュリティが Cisco APIC およびリーフ スイッチにインストールされていることを確認したら、Cisco NX-OS CLI を使用して、ポート セキュリティがハードウェアにプログラムされていることを確認します。

Cisco NX-OS CLI を使用したハードウェア ポート セキュリティ設置の確認

手順

ステップ 1 次のように、スイッチ インターフェイスのポート セキュリティ ステータスを表示します。

例：

```
switch# show system internal epm interface ethernet 1/35 det
name : Ethernet1/35 ::: if index : 0x1a022000 ::: state : UP
vPC : No ::: EPT : 0x0
MAC Limit : 8 ::: Learn Disable : No ::: PortSecurity Action : Protect
VLANs : 4-23
Endpoint count : 5
Active Endpoint count : 5

switch# show system internal epm interface port-channel 1 det

name : port-channel1 ::: if index : 0x16000000 ::: state : UP
vPC : No ::: EPT : 0x0
MAC Limit : 6 ::: Learn Disable : No ::: PortSecurity Action : Protect
VLANs :
Endpoint count : 0
Active Endpoint count : 0
Number of member ports : 1
Interface : Ethernet1/34    /0x1a021000
::::
```

ステップ 2 次のように、モジュール インターフェイスのポート セキュリティ ステータスを表示します。

例：

```
module-1# show system internal epmc interface ethernet 1/35 det
if index : 0x1a022000 ::: name : Ethernet1/35 ::: tun_ip = 0.0.0.0
MAC limit : 8 ::: is_learn_disable : No ::: MAC limit action: Protect
pc if index : 0 ::: name :
is_vpc_fc FALSE  ::: num_mem_ports : 0
 interface state : up
Endpoint count : 5
EPT : 0


module-1# show system internal epmc interface port-channel 1 det
if index : 0x16000000 ::: name : port-channel1 ::: tun_ip = 0.0.0.0
MAC limit :  6 ::: is_learn_disable : No ::: MAC limit action: Protect
pc if index : 0 ::: name :
is_vpc_fc FALSE  ::: num_mem_ports : 1
 interface state : up
Endpoint count : 0
EPT : 0
::::
```

ステップ 3 次のように、リーフ スイッチのポート セキュリティ ステータスを表示します。

例：

```
swtb15-leaf2# show system internal epm interface ethernet 1/35 det

name : Ethernet1/35 ::: if index : 0x1a022000 ::: state : UP
vPC : No ::: EPT : 0x0
MAC Limit : 5 ::: Learn Disable : Yes ::: PortSecurity Action : Protect
VLANs : 4-23
Endpoint count : 5
Active Endpoint count : 5
::::
```

ステップ 4 モジュール インターフェイスの MAC 制限を次のように確認します。

例：

```
module-1# show system internal eltmc info interface port-channel1 | grep mac_limit
   mac_limit_reached:              0   :::       mac_limit:              8
port_sec_feature_set:              1   ::: mac_limit_action:              1
```

例：

```
module-1# show system internal eltmc info interface ethernet 1/35 | grep mac_limit
   mac_limit_reached:              0   :::       mac_limit:              8
port_sec_feature_set:              1   ::: mac_limit_action:              1
```

ステップ 5 モジュールのポート セキュリティ ステータスを表示し、次のように MAC 制限を確認します。

例：

```
module-1#  show system internal epmc interface ethernet 1/35 det
if index : 0x1a022000 ::: name : Ethernet1/35 ::: tun_ip = 0.0.0.0
MAC limit : 5 ::: is_learn_disable : Yes ::: MAC limit action: Protect
pc if index : 0 ::: name :
is_vpc_fc FALSE  ::: num_mem_ports : 0
 interface state : up
Endpoint count : 5
EPT : 0
::::
```

例：

```
module-1# show system internal eltmc info interface ethernet 1/35 | grep mac_limit
   mac_limit_reached:              1   :::       mac_limit:              5
port_sec_feature_set:              1   ::: mac_limit_action:              1
module-1# exit
```

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。