



コントロール プレーンのトラフィック

- [コントロール プレーン ポリシングについて \(1 ページ\)](#)
- [CoPP プレフィルタについて \(10 ページ\)](#)

コントロール プレーン ポリシングについて

コントロール プレーン ポリシング (CoPP) はコントロールプレーンを保護し、ネットワークの安定性、到達可能性、およびパケット配信を保証します。

この機能により、コントロールプロセッサに到達可能な各プロトコルに対して、パラメータの仕様でポリサーを使用したレート制限が可能になります。ポリシングは、ルータまたはレイヤ 3 スイッチの IP アドレスのいずれかを宛先とするすべてのトラフィックに適用されます。ネットワーク デバイスへの一般的な攻撃ベクトルは、過剰なトラフィックがデバイスインターフェイスに転送されるサービス妨害 (DoS) 攻撃です。

Cisco Application Centric Infrastructure (ACI) リーフおよびスパインスイッチ NX-OS は、DoS 攻撃がパフォーマンスに影響しないようにするために CoPP を提供します。このような攻撃は誤って、または悪意を持って実行される場合があります。通常は Cisco ACI リーフおよびスパインスイッチ CPU または CPU 自体のスーパーバイザモジュールに宛てられた大量のトラフィックが含まれます。

Cisco ACI リーフおよびスパインスイッチ スイッチのスーパーバイザモジュールは、管理対象のトラフィックを次の 2 つの機能コンポーネント (プレーン) に分類します。

- **データプレーン** : すべてのデータトラフィックを処理します。NX-OS デバイスの基本的な機能は、インターフェイス間でパケットを転送することです。スイッチ自身に向けられたものでないパケットは、中継パケットと呼ばれます。データプレーンで処理されるのはこれらのパケットです。
- **コントロールプレーン** : ルーティングプロトコルのすべての制御トラフィックを処理します。ボーダー ゲートウェイ プロトコル (BGP) や Open Shortest Path First (OSPF) プロトコルなどのルーティングプロトコルは、デバイス間で制御パケットを送信します。これらのパケットはルータのアドレスを宛先とし、コントロール プレーン パケットと呼ばれます。

Cisco ACI リーフスイッチおよびスパインスイッチのスーパーバイザモジュールにはコントロールプレーンがあり、ネットワークの操作に重要です。スーパーバイザモジュールの動作が途絶したり、スーパーバイザモジュールが攻撃されたりすると、重大なネットワークの停止につながります。たとえば、スーパーバイザに過剰なトラフィックが加わると、スーパーバイザモジュールが過負荷になり、Cisco ACI ファブリック全体のパフォーマンスが低下する可能性があります。別の例としては、Cisco ACI リーフスイッチおよびスパインスイッチのスーパーバイザモジュールに対する DoS 攻撃は、コントロールプレーンに対して非常に高速に IP トラフィックストリームを生成することがあります。これにより、コントロールプレーンでは、これらのパケットを処理するために大量の時間を費やしてしまい、本来のトラフィックを処理できなくなります。

次に、DoS 攻撃の例を示します。

- インターネット制御メッセージプロトコル (ICMP) エコー要求
- IP フラグメント
- TCP SYN フラッディング

これらの攻撃によりデバイスのパフォーマンスが影響を受け、次のようなマイナスの結果をもたらします。

- サービス品質の低下（音声、ビデオ、または重要なアプリケーショントラフィックの低下など）
- ルートプロセッサまたはスイッチプロセッサの高い CPU 使用率
- ルーティングプロトコルのアップデートまたはキープアライブの消失によるルートフラップ
- メモリやバッファなどのプロセッサリソースの枯渇
- 着信パケットの無差別のドロップ



- (注) Cisco ACI リーフスイッチとスパインスイッチは、デフォルトで、デフォルト設定の CoPP によって保護されます。この機能では、顧客のニーズに基づいてノードのグループにパラメータを調整できます。

コントロールプレーン保護

コントロールプレーンを保護するため、Cisco ACI リーフスイッチおよびスパインスイッチで実行されている Cisco NX-OS はコントロールプレーンのさまざまなパケットを異なるクラスに分離します。クラスの識別が終わると、Cisco NX-OS デバイスはパケットをポリシングします。これにより、スーパーバイザモジュールに過剰な負担がかからないようになります。

コントロールプレーンのパケットタイプ:

コントロールプレーンには、次のような異なるタイプのパケットが到達します。

- **受信パケット**：ルーターの宛先アドレスを持つパケット。宛先アドレスには、レイヤ2アドレス（ルータ MAC アドレスなど）やレイヤ3アドレス（ルータ インターフェイスの IP アドレスなど）があります。これらのパケットには、ルータアップデートとキープアライブメッセージも含まれます。ルータが使用するマルチキャスト アドレス宛てに送信されるマルチキャストパケットも、このカテゴリに入ります。
- **例外パケット**：スーパーバイザモジュールによる特殊な処理を必要とするパケット。たとえば、宛先アドレスが Forwarding Information Base (FIB) に存在せず、結果としてミスとなった場合は、スーパーバイザモジュールが送信側に到達不能パケットを返し、DDOS 攻撃からスーパーバイザモジュールを保護します。IP オプションを含む IP パケットは、スーパーバイザによってドロップされます。
- **リダイレクトパケット**：スーパーバイザモジュールにリダイレクトされるパケット。ダイナミックホストコンフィギュレーションプロトコル (DHCP) スヌーピングやダイナミックアドレス解決プロトコル (ARP) インスペクションなどの機能は、パケットをスーパーバイザモジュールにリダイレクトします。
- **収集パケット**：宛先 IP アドレスのレイヤ2 MAC アドレスが FIB に存在していない場合は、スーパーバイザモジュールがパケットを受信し、ARP 要求をそのホストに送信します。

これらのさまざまなパケットは、コントロールプレーンへの悪意ある攻撃に利用され、Cisco ACI ファブリックに過剰な負荷をかける可能性があります。CoPP は、これらのパケットを異なるクラスに分類し、これらのパケットを Cisco ACI リーフスイッチおよびスパインスイッチのスーパーバイザが受信する速度を個別に制御するメカニズムを提供します。

CoPP の分類：

効果的に保護するために、Cisco ACI リーフスイッチおよびスパインスイッチ NX-OS は、スーパーバイザモジュールに到達するパケットを分類して、パケットタイプに基づいた異なるレート制御ポリシーを適用できるようにします。たとえば、Hello メッセージなどのプロトコルパケットには厳格度を緩和し、IP オプションがセットされているためにスーパーバイザモジュールに送信されるパケットには厳格度を強化することが考えられます。

利用可能なプロトコル：

- ACLLOG
- ARP
- BGP
- CDP
- COOP
- DHCP
- EIGRP
- ICMP
- IGMP

- ISIS
- LACP
- LLDP
- MCP
- ND
- OSPF
- PERMIT LOG
- PIM
- STP
- TRACEROUTE
- Infra ARP
- IFC Other
- IFC SPAN
- IFC
- グリーニング
- Tor-Glean

プロトコルごとに、毎秒のパケット数（PPS）でレートとバーストを指定できます。レートとバーストの詳細については、「レート制御メカニズム」を参照してください。

レート制御メカニズム：

パケットの分類が終わると、Cisco ACI リーフおよびスパインスイッチ NX-OS デバイスにはスーパーバイザモジュールに到達するパケットのレートを制御するメカニズムがあります。

ポリシングには、次のパラメータを設定できます。

- 認定情報レート（CIR）：1秒あたりのパケット数（PPS）で指定される、必要な帯域幅。
- 認定バースト（BC）：パケット数で指定され、特定の時間枠内に CIR を超えるが、スケジューリングに影響を与えないトラフィックバーストのサイズ。

デフォルトのポリシング ポリシー：

Cisco ACI リーフスイッチおよびスパインスイッチが最初に起動するとき、異なるプロトコル用に事前定義された CoPP パラメータは、シスコで行ったテストに基づいています。

CoPP の注意事項と制約事項

CoPP に関する注意事項と制約事項は次のとおりです。

- 最初にデフォルト CoPP ポリシーを使用し、後で、データセンターおよびアプリケーションの要件に基づいて CoPP ポリシーを変更することをお勧めします。
- CoPP のカスタマイズは継続的なプロセスです。CoPP を設定するときには、特定の環境で使用されるプロトコルや機能に加えて、サーバ環境に必要なスーパーバイザ機能を考慮する必要があります。これらのプロトコルや機能が変更されたら、CoPP を変更する必要があります。
- CoPP を継続的にモニタすることを推奨します。ドロップが発生した場合は、CoPP がトラフィックを誤ってドロップしたのか、または誤動作や攻撃に応答してドロップしたのかを判定してください。いずれの場合も、状況を分析し、CoPP ポリシーを変更する必要性を評価します。
- CoPP ポリシーによって、ルーティング プロトコルなどのクリティカルなトラフィック、またはデバイスへのインタラクティブなアクセスがフィルタリングされないように注意してください。このトラフィックをフィルタリングすると、Cisco ACI リーフ/スパインへのリモートアクセスが禁止され、コンソール接続が必要となる場合があります。
- CoPP プレフィルタ エントリを誤って設定しないでください。CoPP プレフィルタ エントリは、マルチポッド設定、リモート リーフ スイッチ、および Cisco ACI マルチサイト展開への接続に影響を与える可能性があります。
- APIC UI を使用して、CoPP パラメータを調整することができます。
- プロトコルごとの各インターフェイスはリーフ スイッチでのみサポートされています。
- プロトコルごとの各インターフェイスで FEX ポートはサポートされていません。
- プロトコルごとの各インターフェイスでサポートされているプロトコルは、ARP、ICMP、CDP、LLDP、LACP、BGP、STP、BFD、および OSPF です。
- プロトコルごとの各インターフェイスの最大の TCAM エントリは 256 です。しきい値を超過すると、障害が発生します。

APIC GUI を使用した CoPP の設定

手順

- ステップ 1 メニュー バーで、[ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)] の順にクリックします。
- ステップ 2 [ナビゲーション (Navigation)] ペインで、右クリックして[ポリシー (Policies)] > [スイッチ (Switch)] > [CoPP リーフ (CoPP Leaf)] を選択し、[CoPP リーフレベルポリシーの作成 (Create CoPP Leaf Level Policy)] を選択します。
- ステップ 3 [CoPP リーフレベルポリシーの作成 (Create CoPP Leaf Level Policy)] ダイアログで、次のサブステップを実行します。
 - a) [名前 (Name)] フィールドに、ポリシー名を入力します。

- b) [プロファイルのタイプ (Type of Profile)] フィールドで、プロファイルのタイプを選択します。

(注)

各プロトコルを個別に設定する場合、[CoPP にはカスタム値がある (CoPP has custom values)] を選択します。プロファイルタイプを選択しなかった場合、デフォルト値が適用されます。

- c) [送信 (Submit)] をクリックします。`

ステップ 4 [ナビゲーション (Navigation)] ペインで、右クリックして[スイッチ (Switches)] > [リーフスイッチ (Leaf Switches)] > [ポリシーグループ (Policy Groups)] を選択し、[アクセススイッチポリシーグループの作成 (Create Access Switch Policy Group)] を選択します。

ステップ 5 [アクセススイッチポリシーグループの作成 (Create Access Switch Policy Group)] ダイアログボックスで、次のサブステップを実行します。

- [名前 (Name)] フィールドに、ポリシー名を入力します。
- [CoPP リーフポリシー (CoPP Leaf Policy)] フィールドで、以前に作成したポリシーを選択します。
- [送信 (Submit)] をクリックします。`

ステップ 6 [ナビゲーション (Navigation)] ペインで、右クリックして[スイッチ (Switches)] > [リーフスイッチ (Leaf Switches)] > [プロファイル (Profiles)] を選択し、[リーフプロファイルの作成 (Create Leaf Profile)] を選択します。

ステップ 7 [リーフプロファイルの作成 (Create Leaf Profile)] ダイアログで、次のサブステップを実行します。

- [名前 (Name)] フィールドに、プロファイルの名前を入力します。
- [リーフセクタ (Leaf Selectors)] テーブルで、[+] をクリックし、[名前 (Name)] フィールドにリーフセクタの名前を入力し、[ブロック (Blocks)] フィールドでスイッチを選択し、[ポリシーグループ (Policy Group)] で前に選択したポリシーグループを選択し、[更新 (Update)] をクリックします。
- [次へ (Next)]、それから [終了 (Finish)] をクリックして、CoPP 構成を完了します。

Cisco NX-OS CLI を使用した CoPP の設定

手順

ステップ 1 CoPP リーフ プロファイルを設定します。

例 :

```
# configure copp Leaf Profile
apic1(config)# policy-map type control-plane-leaf leafProfile
apic1(config-pmap-copp-leaf)# profile-type custom
apic1(config-pmap-copp-leaf)# set arpRate 786
# create a policy group to be applied on leaves
apic1(config)# template leaf-policy-group coppForLeaves
apic1(config-leaf-policy-group)# copp-aggr leafProfile
apic1(config-leaf-policy-group)# exit
# apply the leaves policy group on leaves
apic1(config)# leaf-profile applyCopp
apic1(config-leaf-profile)# leaf-group applyCopp
```

```
apicl(config-leaf-group)# leaf 101-102
apicl(config-leaf-group)# leaf-policy-group coppForLeaves
```

ステップ2 CoPP スパイン プロファイルを設定します。

例：

```
# configure copp Spine Profile
apicl(config)# policy-map type control-plane-spine spineProfile
apicl(config-pmap-copp-spine)# profile-type custom
apicl(config-pmap-copp-spine)# set arpRate 786
# create a policy group to be applied on spines
apicl(config)# template leaf-policy-group coppForSpines
apicl(config-spine-policy-group)# copp-aggr spineProfile
apicl(config-spine-policy-group)# exit
# apply the spine policy group on spines
apicl(config)# spine-profile applyCopp
apicl(config-spine-profile)# spine-group applyCopp
apicl(config-spine-group)# spine 201-202
apicl(config-spine-group)# spine-policy-group coppForSpines
```

REST API を使用した CoPP の設定

手順

ステップ1 CoPP リーフ プロファイルを設定します。

例：

```
<!-- api/node/mo/uni/.xml -->
<infraInfra>
  <coppLeafProfile type="custom" name="mycustom">                                <!-- define copp leaf profile
-->
    <coppLeafGen1CustomValues bgpBurst="150" bgpRate="300"/>
    </coppLeafProfile>
    <infraNodeP name="leafCopp">
      <infraLeafS name="leafs" type="range">
        <infraNodeBlk name="leaf1" from_="101" to_="101"/>
        <infraNodeBlk name="leaf3" from_="103" to_="103"/>
        <infraRsAccNodePGrp tDn="uni/infra/funcprof/accnodepgrp-myLeafCopp"/>
      </infraLeafS>
    </infraNodeP>
    <infraFuncP>
      <infraAccNodePGrp name="myLeafCopp">
        <infraRsLeafCoppProfile tnCoppLeafProfileName="mycustom"/>    <!-- bind copp leaf policy to
leaf </infraAccNodePGrp>                                              profile -->
      </infraFuncP>
    </infraInfra>
```

ステップ2 CoPP スパイン プロファイルを設定します。

例：

```
<!-- api/node/mo/uni/.xml -->
<infraInfra>
  <coppSpineProfile type="custom" name="mycustomSpine">                    <!-- define copp leaf profile
-->
```

```

    <coppSpineGenlCustomValues bgpBurst="150" bgpRate="300"/>
  </coppSpineProfile>
  <infraSpineP name="spineCopp">
    <infraSpineS name="spines" type="range">
      <infraNodeBlk name="spine1" from="104" to="104"/>
      <infraRsSpineAccNodePGrp tDn="uni/infra/funcprof/spaccnodepgrp-mySpineCopp"/>
    </infraSpineS>
  </infraSpineP>
  <infraFuncP>
    <infraSpineAccNodePGrp name="mySpineCopp">
      <infraRsSpineCoppProfile tnCoppSpineProfileName="mycustomSpine"/> <!-- bind copp spine policy
to
    </infraSpineAccNodePGrp>
    </infraFuncP>
  </infraInfra>

```

GUI を使用した CoPP 統計情報の表示

CoPP の調整を適切に行うには、指定のモードの指定のプロトコルでドロップ/許可されたパケット数を知る必要があります。次の手順を使用して、GUI で情報を表示できます。

手順

メニュー バーで、[ファブリック]>[インベントリ]>[ポッド]/[番号]>[ノード]/[名前]>[コントロールプレーンの統計情報]>[デフォルト] の順にクリックして、クラスのリストから選択し、統計情報の表示形式を設定します。

CoPP によって許可またはドロップされたパケット数に関する統計情報を収集することができます。

APIC GUI を使用したプロトコル CoPP ポリシーごとの各インターフェイスの設定

手順

ステップ 1 メニュー バーで、[ファブリック]>[外部アクセス ポリシー] をクリックします。

ステップ 2 [ナビゲーション] ペインで、[ポリシー]>[インターフェイス]>[CoPP インターフェイス] を展開して、[プロトコル CoPP ポリシーごとの各インターフェイスの作成] ダイアログ ボックスを右クリックして、[プロトコル CoPP ポリシーごとの各インターフェイスの作成] ダイアログ ボックスの次のアクションを実行します。

a) [名前] フィールドでポリシー名を追加します。

- b) [CoPP ポリシー プロトコル] 表を展開し、プロトコル名、タイプ、レート、バースト情報を入力します。[更新] と [送信] をクリックします。

ステップ 3 [ナビゲーション] ペインで、[インターフェイス]>[リーフ インターフェイス]>[ポリシー グループ]>[リーフ アクセス ポート ポリシー グループの作成] を展開して、[リーフ アクセス ポート ポリシー グループの作成] ダイアログ ボックスを右クリックして、[リーフ アクセス ポート ポリシー グループの作成] ダイアログ ボックスの次のアクションを実行します。

- a) [名前] フィールドでポリシー名を追加します。
- b) [COPP リーフ ポリシー] フィールドで、以前に作成されたポリシーを選択します。
- c) [Submit] をクリックします。

ステップ 4 [ナビゲーション] ペインで、[インターフェイス]>[リーフ インターフェイス]>[プロファイル]>[リーフ プロファイル] を展開して、[リーフ インターフェイス プロファイルの作成] ダイアログ ボックスを右クリックして、[リーフ インターフェイス プロファイルの作成] ダイアログ ボックスの次のアクションを実行します。

- a) [名前] フィールドで、プロファイル名を追加します。
- b) [インターフェイス セレクタ] 表を展開し、[名前] および [インターフェイス ID] フィールドにインターフェイス情報を追加して、以前作成した [インターフェイス ポリシー グループ] を選択します。
- c) [Ok] および [送信] をクリックして、プロトコル CoPP ごとの各インターフェイス設定を完了します。

NX-OS スタイル CLI を使用するプロトコル CoPP ポリシーごとのインターフェイスごとの設定

手順

ステップ 1 CoPP クラス マップおよびポリシー マップを定義します。

例 :

```
(config)# policy-map type control-plane-if <name>
(config-pmap-copp)# protocol bgp bps <value>
(config-pmap-copp)# protocol ospf bps <value>
```

ステップ 2 リーフのインターフェイスに設定を適用します。

例 :

```
(config)# leaf 101
(config-leaf)# int eth 1/10
(config-leaf-if)# service-policy type control-plane-if output<name>
```

RESTAPIを使用するプロトコルごとのインターフェイスあたりのCoPPの設定

手順

プロトコルごとにインターフェイスあたりの CoPP を設定します。

例：

```
<polUni>
  <infraInfra>
    <infraNodeP name="default">
      <infraLeafS name="default" type="range">
        <infraNodeBlk name="default" to_="101" from_="101"/>
      </infraLeafS>
      <infraRsAccPortP tDn="uni/infra/accportprof-default"/>
    </infraNodeP>
    <infraAccPortP name="default">
      <infraHPortS name="regularPorts" type="range">
        <infraPortBlk name="blk1" toPort="7" fromPort="1" toCard="1" fromCard="1"/>
        <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-copp"/>
      </infraHPortS>
    </infraAccPortP>

    <infraFuncP>
      <infraAccPortGrp name="copp">
        <infraRsCoppIfPol tnCoppIfPolName="pc"/>
      </infraAccPortGrp>
    </infraFuncP>

    <coppIfPol name = "pc" >
      <coppProtoClassP name = "test" matchProto="lldp,arp" rate="505" burst = "201"/>
      <coppProtoClassP name = "test1" matchProto="bgp" rate="500" burst = "200" />
    </coppIfPol>
  </infraInfra>
</polUni>
```

CoPP プレフィルタについて

Cisco Application Centric Infrastructure (ACI) では、コントロールプレーンポリシング (CoPP) プレフィルタ機能を使用して、CPUに送信される制御パケットをフィルタ処理できます。CoPP プレフィルタは、インフラストラクチャアクセス制御リスト (iACL) と同じです。

この機能を使用する前に、次の重要な点に注意してください。

1. この機能は、インターフェイスごと、または L3Out ごとではなく、リーフスイッチまたはスパインスイッチごとに機能します。
2. この機能は、VRF インスタンス全体で有効になります。つまり、定義するフィルタは VRF インスタンスに固有のものにはなりません。CoPP プレフィルタを有効にし、CoPP

プレフィルタの構成で ICMP トラフィックを明示的に許可しなかった場合、対象のリーフスイッチにおいて、すべての VRF インスタンスのブリッジドメインに送信された ICMP トラフィックはドロップされます。

3. CoPP プレフィルタは許可リストとして構成されます。
4. この機能は、最初のフィルタリングルールを入力するとアクティブになります。つまり、フィルタリングルールが設定されていない場合は、すべてが許可されます。最初のルールを入力するとすぐに、フィルタリングルールで許可したトラフィック以外はすべてドロップされるようになります。これは、許可リストに追加しない限り、すべての IPv4/IPv6 コントロールプレーントラフィックがデフォルトで拒否されることを意味します。
5. フィルタ構成では、プロトコル/DIP/ SIP/Protocol/L4 ポート/L4 ポート範囲を入力できます。トラフィックの送信元と宛先の IP アドレスを入力できます。
6. 暗黙的に許可されていないアンダーレイプロトコルも許可する必要があります。たとえば、BGP は許可する必要があります。許可しないと、リーフまたはスパインスイッチへのインフラ BGP セッションがダウンします。別の例として、リモートリーフスイッチでこの機能を有効にする場合は、リモートリーフの到達可能性のために OSPF を許可する必要があります。
7. ポイント 6 のため、単一の POD のリーフまたはスパインスイッチで CoPP プレフィルタを構成する場合は、BGP および DHCP トラフィックが許可されていることを確認する必要があります。スパインスイッチが IPN/ISN にも接続されている場合は、OSPF を許可することを検討する必要があります。
8. ポイント 6 のため、Cisco ACI マルチポッド、Cisco ACI マルチサイトまたは Cisco Nexus Dashboard Orchestrator、GOLF、またはリモートリーフスイッチでは、インフラ接続の許可リストに BGP、DHCP、および OSPF を追加する必要があります。
9. Cisco Application Policy Infrastructure Controller (APIC) トラフィックが自動的に許可されるため、この機能を有効にしても、リーフスイッチがファブリックから切断されることはありません。ただし、許可リストに明示的に BGP を追加しない限り、この機能を有効にすると、リーフスイッチへのインフラ BGP セッションが切断されることに注意してください。
10. COOP トラフィック、vPC コントロールプレーントラフィック、LACP/LLDP/CDP、ARP などのプロトコル、およびネイバー探索パケット (RS/RA/NS/NA) は自動的に許可されます。
11. ICMP、IGMP、およびその他のプロトコルは明示的に許可する必要があります。CoPP プレフィルタを有効にし、サーバがブリッジドメインサブネット IP アドレスに ping できることを確認する際には、ICMP が許可されていることを確認する必要があります。
12. ICMP 応答または要求のみを許可する ICMP サブタイプはサポートされていません。ICMP を有効にすると、両方が有効になります。

サポートされるプラットフォーム

このセクションでは、CoPP プレフィルタ機能のサポートされているプラットフォームを示します。

リーフ スイッチがサポートされています。

- N9K-C93108TC-EX
- N9K-C93108TC-FX
- N9K-C93108YC-FX
- N9K-C93180LC-EX
- N9K-C93180YC-EX
- N9K-C9348GC-FXP

スパイン スイッチがサポートされています。

- N9K-C92300YC
- N9K-C92304QC
- N9K-C9232C
- N9K-C9236C
- N9K-C9272Q
- N9K-C9364C
- N9K C9508 FM 2
- N9K-C9516-FM-E2

制限事項

- イーサネット タイプ IPv4 または IPv6 パケットだけは、出力 TCAM で一致することができます。ARP ND パケットが一致しません。
- 合計 128(ワイドキー) エントリの許可リストに含めることができます。ただし、一部のエントリは、社外秘予約されています。

GUI を使用した CoPP プレフィルタ、ポリシー グループ、プロファイルの設定

Cisco APIC GUI を使用した CoPP プレフィルタの設定

このセクションでは、リーフ レベルとスパイン レベルは、Cisco APIC GUI を使用して、CoPP プレフィルタを設定する方法について説明します。

始める前に

APIC GUI へのアクセス

手順

ステップ 1 [Fabric] > [External Access Policies] をクリックします。

ステップ 2 [Navigation] ペインで、[Policies] > [Switch] をクリックします。

[Navigation] ペインに [CoPP Pre-Filter for Leaf] および [CoPP Pre-Filter for Spine] ノードが表示されます。

ステップ 3 [Navigation] ペインで、次のオプションから選択します。

- [CoPP Pre-Filter for Leaf] – リーフ スイッチの CoPP プレフィルタを作成する場合は、[CoPP Pre-Filter for Leaf] を右クリックして、[Create Profiles for CoPP Pre-Filter To Be Applied At The Leaf Level] を選択します。
- [CoPP Pre-Filter for Spine] – スパイン スイッチの CoPP プレフィルタを作成する場合は、[CoPP Pre-Filter for Spine] を右クリックして、[Create Profiles for CoPP Pre-Filter To Be Applied At The Spine Level] を選択します。

それぞれの CoPP プレフィルタのダイアログが表示されます。

ステップ 4 ダイアログのフィールドに適切な値を入力します。

(注)

ダイアログ ボックスのフィールドの詳細については、ヘルプ アイコンをクリックすると Cisco APIC ヘルプ ファイルが表示されます。

ステップ 5 完了したら、[送信 (Submit)] をクリックします。

次のタスク

ポリシー グループを設定します。

GUI を使用したリーフ ポリシー グループの設定

このセクションでは、ポリシー グループを作成する方法について説明します。

始める前に

Cisco APIC GUI にアクセスします。

手順

ステップ 1 [Fabric] > [External Access Policies] をクリックします。

- ステップ 2** [ナビゲーション] ペインで、[スイッチ]>[リーフ スイッチ] をクリックします。
[ポリシー グループ] ノードが [ナビゲーション] ウィンドウに表示されます。
- ステップ 3** [ナビゲーション] ペインの [ポリシー グループ] で、リーフ ポリシー グループを作成するには、[ポリシー グループ] を右クリックして、[アクセス スイッチ ポリシー グループの作成] をクリックします。
それぞれのポリシー グループ ダイアログが表示されます。
- ステップ 4** ポリシー グループ ダイアログから、[名前] フィールドに名前を入力して、適用するポリシー タイプのドロップダウン矢印をクリックします。選択したポリシー タイプに設定されているポリシーがドロップダウン リストに表示されます。
- (注)
ダイアログ ボックスのフィールドの詳細については、ヘルプ アイコンをクリックすると Cisco APIC ヘルプ ファイルが表示されます。
- ステップ 5** 完了したら、[送信 (Submit)] をクリックします。

次のタスク

プロファイルを設定します。

GUI を使用したリーフ プロファイルの設定

このセクションでは、プロファイルを作成する方法について説明します。

始める前に

設定されているポリシー グループが必要です。

手順

- ステップ 1** [Fabric]>[External Access Policies] をクリックします。
- ステップ 2** [ナビゲーション] ペインで、[スイッチ]>[リーフ スイッチ]>[プロファイル] をクリックします。
[リーフ プロファイル] ノードが [ナビゲーション] ウィンドウに表示されます。
- ステップ 3** [ナビゲーション] ペインの [プロファイル] で、リーフ スイッチのプロファイルを作成するには、[プロファイル] を右クリックして [リーフ プロファイルの作成] を選択します。
個別にプロファイル ダイアログが表示されます。
- ステップ 4** プロファイル ダイアログから [名前] フィールドに名前を入力し、[+] をクリックしてセレクトタ情報を入力します。完了したら、[Update] をクリックします。
[更新] をクリックした後、プロファイル ダイアログに戻ります。
- ステップ 5** [次へ] をクリックして、インターフェイス セレクトタ プロファイル情報を入力します。
- (注)

ダイアログ ボックスのフィールドの詳細については、ヘルプ アイコンをクリックすると Cisco APIC ヘルプ ファイルが表示されます。

ステップ 6 完了したら、[終了] をクリックします。

CLI を使用した CoPP プレフィルタの設定

CLI を使用したリーフ スイッチの CoPP プレフィルタの設定

このセクションでは、CoPP プレフィルタ ポリシーとポリシー グループを設定し、CLI を使用してスイッチ ポリシー グループとスイッチ プロファイルに関連付ける方法を説明します。

手順

ステップ 1 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 Switch(config)# **template control-plane-policing-prefilter-leaf** <name>

リーフ スイッチの CoPP プレフィルタ プロファイルを作成します。

ステップ 3 Switch (config-control-plane-policing-prefilter-leaf)# **permit proto** { **tcp** | **udp** | **eigrp** | **unspecified** | **icmp** | **icmpv6** | **egp** | **igp** | **l2tp** | **ospf** | **pim** }

指定された IP プロトコルを許可します。

ステップ 4 Switch (config-control-plane-policing-prefilter-leaf)#**exit**

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 5 Switch(config)# **template leaf-policy-group** <name>

CoPP プレフィルタ ポリシー グループ リーフ スイッチを作成します。

ステップ 6 Switch(config-leaf-policy-group)# **control-plane-policing-prefilter** <name>

CoPP プレフィルタ ポリシーとリーフ ポリシー グループを関連付けます。

ステップ 7 Switch(config-leaf-policy-group)# **exit** <name>

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 8 Switch(config)# **leaf-profile** <name>

リーフ プロファイルを作成します。

ステップ 9 Switch(config-leaf-profile)# **leaf-group** <name>

リーフ プロファイルとリーフ グループを関連付けます。

ステップ 10 Switch(config-leaf-group)# **leaf-policy-group** <name>

リーフ グループとリーフ ポリシー グループを関連付けます。

CLI を使用したスパイン スイッチの CoPP プレフィルタの設定

このセクションでは、CoPP プレフィルタ ポリシーとポリシー グループを設定し、CLI を使用してスイッチ ポリシー グループとスイッチ プロファイルに関連付ける方法を説明します。

手順

ステップ 1 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 Switch(config)# **template control-plane-policing-prefilter-spine** <name>

スパイン スイッチの CoPP プレフィルタ プロファイルを作成します。

ステップ 3 Switch (config-control-plane-policing-prefilter-spine)# **permit proto** { **tcp** | **udp** | **eigrp** | **unspecified** | **icmp** | **icmpv6** | **egp** | **igp** | **l2tp** | **ospf** | **pim** }

指定された IP プロトコルを許可します。

ステップ 4 Switch (config-control-plane-policing-prefilter-spine)#**exit**

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 5 Switch(config)# **template spine-policy-group** <name>

CoPP プレフィルタ ポリシー グループ スパイン スイッチを作成します。

ステップ 6 Switch(config-spine-policy-group)# **control-plane-policing-prefilter** <name>

CoPP プレフィルタ ポリシーとスパイン ポリシー グループを関連付けます。

ステップ 7 Switch(config-spine-policy-group)# **exit** <name>

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 8 Switch(config)# **spine-profile** <name>

スパイン プロファイルを作成します。

ステップ 9 Switch(config-spine-profile)# **spine-group** <name>

スパイン プロファイルとスパイン グループを関連付けます。

ステップ 10 Switch(config-spine-group)# **spine-policy-group** <name>

スパイン グループとスパイン ポリシー グループを関連付けます。

REST API を使用した CoPP プレフィルタの設定

REST API を使用したリーフスイッチの CoPP プレフィルタ ポリシーの設定

このセクションでは、REST API を使用してリーフスイッチの CoPP プレフィルタ ポリシーを設定する方法について説明します。

手順

ステップ1 許可リストのエントリとともに CoPP プレフィルタのスイッチ ポリシーを作成します。

```
<iacLeafProfile descr="" dn="uni/infra/iacspinep-spine_icmp" name="COPP_PreFilter_BGP_Config "
ownerKey="" ownerTag="">
<iacEntry dstAddr="0.0.0.0/0" dstPortFrom="179" dstPortTo="179" ipProto="tcp" name="bgp" nameAlias=""
srcAddr="0.0.0.0/0" srcPortFrom="179" srcPortTo="179"/>
</iacLeafProfile>
```

ステップ2 CoPP プレフィルタ ポリシーでスイッチ ポリシー グループを作成します。

```
<infraAccNodePGrp descr="" dn="uni/infra/funcprof/accnodepgrp-COPP_PreFilter_BGP_Config "
name="COPP_PreFilter_BGP_Config" nameAlias="" ownerKey="" ownerTag="">
<infraRsIacLeafProfile tnIacLeafProfileName="COPP_PreFilter_BGP_Config"/>
</infraAccNodePGrp>
```

ステップ3 スイッチ プロファイルにスイッチ ポリシー グループを関連付けます。

```
<infraNodeP descr="" dn="uni/infra/nprof-leafP-103" name="leafP-103" nameAlias="" ownerKey=""
ownerTag="">
<infraLeafS descr="" name="103_Sel" nameAlias="" ownerKey="" ownerTag="" type="range">
<infraRsAccNodePGrp tDn="uni/infra/funcprof/accnodepgrp-COPP_PreFilter_BGP_Config"/>
<infraNodeBlk descr="" from_="103" name="nblk1" nameAlias="" to_="103"/>
</infraLeafS>
</infraNodeP>
```

REST API を使用したスパインの CoPP プレフィルタ ポリシーの設定

このセクションでは、REST API を使用してスパインスイッチの CoPP プレフィルタ ポリシーを設定する方法について説明します。

手順

ステップ 1 許可リストのエントリとともに CoPP プレフィルタのスイッチ ポリシーを作成します。

```
<iaclSpineProfile descr="" dn="uni/infra/iaclspine-spine_icmp" name="COPP_PreFilter_OSPF_Config"
ownerKey="" ownerTag="">
<iaclEntry dstAddr="0.0.0.0/0" dstPortFrom="unspecified" dstPortTo="unspecified" ipProto="ospfigp"
name="" nameAlias="" srcAddr="0.0.0.0/0" srcPortFrom="unspecified" srcPortTo="unspecified"/>
</iaclSpineProfile>
```

ステップ 2 CoPP プレフィルタ ポリシーでスイッチ ポリシー グループを作成します。

```
<infraSpineAccNodePGrp descr="" dn="uni/infra/funcprof/spaccnodepgrp-COPP_PreFilter_OSPF_Config"
name="COPP_PreFilter_OSPF_Config" nameAlias="" ownerKey="" ownerTag="">
<infraRsIaclSpineProfile tnIaclSpineProfileName="COPP_PreFilter_OSPF_Config"/>
</infraSpineAccNodePGrp>
```

ステップ 3 スイッチ プロファイルにスイッチ ポリシー グループを関連付けます。

```
<infraSpineP descr="" dn="uni/infra/spprof-204" name="204" nameAlias="" ownerKey="" ownerTag="">
<infraSpineS descr="" name="204" nameAlias="" ownerKey="" ownerTag="" type="range">
<infraRsSpineAccNodePGrp tDn="uni/infra/funcprof/spaccnodepgrp-COPP_PreFilter_OSPF_Config"/>
<infraNodeBlk descr="" from_="204" name="nodeblock1" nameAlias="" to_="204"/>
</infraSpineS>
<infraRsSpAccPortP tDn="uni/infra/spaccportprof-204"/>
</infraSpineP>
```

次のタスク

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。