



SGT および SGACL の IPv6 サポート

- [SGT および SGACL の IPv6 サポートの機能履歴, on page 1](#)
- [SGT および SGACL の IPv6 サポート, on page 2](#)
- [IPv6 動的学習コンポーネント, on page 2](#)
- [IPv6 アドレスから SGT へのマッピングの優先順位, on page 2](#)
- [SGT および SGACL の IPv6 サポートを設定する方法, on page 3](#)
- [SGT および SGACL の IPv6 サポートの確認, on page 8](#)
- [SGT および SGACL の IPv6 サポートの設定例, on page 8](#)

SGT および SGACL の IPv6 サポートの機能履歴

次の表に、このモジュールで説明する機能のリリース情報とプラットフォームサポート情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能名と説明	サポートされるプラットフォーム
Cisco IOS XE 17.18.1	SGT および SGACL の IPv6 サポート: セキュリティグループタグ (SGT) およびセキュリティグループ アクセス コントロール リスト (SGACL) の IPv6 サポートにより、IPv6 アドレスと SGT 間のシームレスなマッピングが可能になります。	Cisco C9610 シリーズ スマート スイッチ

SGT および SGACL の IPv6 サポート

セキュリティグループタグ（SGT）およびセキュリティ グループ アクセス コントロール リスト（SGACL）機能の IPv6 サポートにより、IPv6 アドレスと SGT 間のシームレスなマッピングが可能になります。これらのマッピングされた SGT は、SGACL を介したセキュリティポリシーの適用において重要な役割を果たします。

IPv6 動的学習コンポーネント

IPv6 アドレスの動的学習は、次の 3 つのコアコンポーネントに依存しています。

- スイッチ統合セキュリティ機能（SISF）：

セキュリティ、アドレス割り当て、解決、ネイバー探索、およびイグジットポイント検出を担当するインフラストラクチャ。

- Cisco Enterprise Policy Manager（EPM）：

IPv6 アドレス通知を受信するために SISF に登録します。次に、EPM は Cisco Identity Services Engine（ISE）から取得した IPv6 アドレスと SGT を使用して、IP-SGT バインディングを作成します。

- Cisco TrustSec：

SGT を着信した通信に割り当て、これらのタグに基づいてネットワーク全体にアクセスポリシーを適用することで、デバイスを不正アクセスから保護します。

IPv6 アドレスから SGT へのマッピングの優先順位

IPv6 アドレスから SGT へのマッピングには、以下のように優先順位付けされたいくつかの方法があります（優先順位の低いものから高いものの順に示します）。

1. VLAN：

ICMPv6 ネイバー探索を使用して、SGT-VLAN マッピングを設定された VLAN で SISF によって学習された IPv6 アドレス。

2. CLI を使用して ROMmon ファイルを転送した場合の upgrade コマンドの例：

cts role-based sgt-map グローバル設定コマンドを使用して設定される手動アドレスバインディング（IP-SGT 形式）。

3. レイヤ 3 インターフェイス：

一貫したレイヤ 3 インターフェイス SGT またはアイデンティティ ポート マッピング（IPM）を設定されたインターフェイスを通過する FIB 転送エントリから作成されたバインディング。

4. SXP：

SGT 交換プロトコル（SXP）ピアから学習されたバインディング。

5. ローカル:

EPM およびデバイストラッキング（SISF）によって特定された認証済みホストのバインディング。

6. 内部:

ローカルで設定された IP アドレスとデバイスの SGT 間のバインディング。

SGT および SGACL の IPv6 サポートを設定する方法

このセクションでは、SGT および SGACL の IPv6 サポートを設定する方法について説明します。

IP-SGT バインディング用の IPv6 アドレスの学習

SISF は、IP-SGT バインディングで使用する IPv6 アドレスを学習する機能です。

IP-SGT バインディング用の IPv6 アドレスを学習するには、次のタスクを設定します。

Procedure

Step 1

enable

Example:

```
Device# enable
```

特権 EXEC モードを有効にします。

プロンプトが表示されたらパスワードを入力します。

Step 2

configure terminal

Example:

```
Device# 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。

Step 3

cts role-based sgt-map *host-address/prefix* sgt sgt-value

Example:

```
Device(config)# cts role-based sgt-map 2001::db8::1/64 sgt 120
```

ホストまたは Virtual Routing and Forwarding（VRF）インスタンスの SGT に送信元 IPv6 アドレスを手動でマッピングします。

Step 4

device-tracking policy *policy-name*

Example:

```
Device(config)# device-tracking policy policy1
```

デバイストラッキングを有効にし、デバイストラッキング設定モードを開始します。

Step 5 **tracking enable**

Example:

```
Device(config-device-tracking)# tracking enable
```

ポートでデフォルトのトラッキング ポリシーを上書きします。

Step 6 **end**

Example:

```
Device(config-device-tracking)# end
```

デバイストラッキング設定モードを終了し、特権 EXEC モードに戻ります。

ローカルバインディングを使用した IPv6 IP-SGT バインディングの設定

ローカルバインディングを使用した IPv6 IP-SGT バインディングを設定するには、次のタスクを実行します。

Before you begin

- ローカルバインディングでは、SGT 値は Cisco Identity Services Engine (ISE) からダウンロードされます。詳細については、「シスコ セキュリティ グループ アクセス ポリシーの設定」を参照してください。
- IPv6 アドレスを生成する前に、SISF を有効にして入力しておく必要があります。



Note このタスクでは、Cisco Identity Based Networking Services (IBNS) バージョン 2.0 を使用します。

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

特権 EXEC モードを有効にします。

プロンプトが表示されたらパスワードを入力します。

Step 2 **configure terminal**

Example:

```
Device# 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。

Step 3 **policy-map type control subscriber control-policy-name****Example:**

```
Device(config)# policy-map type control subscriber policy1
```

加入者セッションに対して制御ポリシーを定義し、制御ポリシーマップの設定モードを開始します。

Step 4 **event session-started match-all****Example:**

```
Device(config-event-control-policymap)# event session-started match-all
```

条件が満たされた場合に制御ポリシーのアクションをトリガーするイベントのタイプを指定します。

Step 5 **priority-number class always do-until-failure****Example:**

```
Device(config-class-control-policymap)# 10 class always do-until-failure
```

制御クラスを制御ポリシー内の1つ以上のアクションに関連付けて、アクション制御ポリシーマップの設定モードを開始します。

名前付き制御クラスを最初に設定してから、このクラスを *control-class-name* 引数を使用して指定する必要があります。

Step 6 **action-number authenticate using mab****Example:**

```
Device(config-action-control-policymap)# 10 authenticate using mab
```

指定されたメソッドを使用して、加入者セッションの認証を開始します。

Step 7 **exit****Example:**

```
Device(config-action-control-policymap)# exit
```

アクション制御ポリシーマップ設定モードを終了し、グローバルコンフィギュレーションモードに戻ります。

Step 8 **interface gigabitethernet interface-number****Example:**

```
Device(config)# interface gigabitethernet 1/0/1
```

インターフェイスを設定し、インターフェイス設定モードを開始します。

Step 9 **description interface-description****Example:**

```
Device(config-if)# description downlink to ipv6 clients
```

設定されたインターフェイスについて説明します。

Step 10 **switchport access vlan vlan-id**

Example:

```
Device(config-if)# switchport access vlan 20
```

インターフェイスのアクセスモード特性を設定し、インターフェイスがアクセスモードのときの VLAN を設定します。

Step 11 switchport mode access**Example:**

```
Device(config-if)# switchport mode access
```

トランキングモードをアクセスモードに設定します。

Step 12 device-tracking attach-policy *policy-name***Example:**

```
Device(config-if)# device-tracking attach-policy snoop
```

IPv6 スヌーピング機能にポリシーを適用します。

Step 13 access-session port-control auto**Example:**

```
Device(config-if)# access-session port-control auto
```

ポートの認可状態を設定します。

Step 14 mab eap**Example:**

```
Device(config-if)# mab eap
```

MAC 認証バイパスに Extensible Authentication Protocol (EAP) を使用します。

Step 15 dot1x pae authenticator**Example:**

```
Device(config-if)# dot1x pae authenticator
```

ポートで dot1x 認証を有効にします。

Step 16 service-policy type control subscriber *policy-name***Example:**

```
Device(config-if)# service-policy type control subscriber policy
```

このインターフェイスで発生するセッションに使用されるポリシーマップを指定します。ポリシーマップには、認証と許可のルールが含まれています。

Step 17 end**Example:**

```
Device(config-if)# end
```

インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

Step 18 show cts role-based sgt-map all ipv6**Example:**

```
Device# show cts role-based sgt-map all ipv6
```

アクティブな IPv6 IP-SGT バインディングを表示します。

VLAN を使用した IPv6 IP-SGT バインディングの設定

VLAN では、ネットワーク管理者が特定の VLAN に SGT 値を割り当てます。

VLAN を使用して IPv6 IP-SGT バインディングを設定するには、次のタスクを実行します。

Procedure

Step 1 enable

Example:

```
Device# enable
```

特権 EXEC モードを有効にします。

プロンプトが表示されたらパスワードを入力します。

Step 2 configure terminal

Example:

```
Device# 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。

Step 3 cts role-based sgt-map vlan-list vlan-id sgt sgt-value

Example:

```
Device(config)# cts role-based sgt-map vlan-list 20 sgt 3
```

設定済みの VLAN に SGT 値を割り当てます。

sgt-value: 2 ～ 65519 の範囲で指定する必要があります。

Step 4 end

Example:

```
Device(config)# end
```

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SGT および SGACL の IPv6 サポートの確認

コマンド	説明
show cts role-based sgt-map all	アクティブな IPv4 および IPv6 IP-SGT バインディングを表示します。
show cts role-based sgt-map all ipv6	アクティブな IPv6 IP-SGT バインディングを表示します。

SGT および SGACL の IPv6 サポートの設定例

以下のセクションでは、SGT および SGACL の IPv6 サポートを設定する方法を示します。

例：IP-SGT バインディング用の IPv6 アドレスの学習

次の例は、IP-SGT バインディングの IPv6 アドレスを学習する方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-map 2001::db8::1/64 sgt 120
Device(config)# device-tracking policy policy1
Device(config-device-tracking)# tracking enable
Device(config-device-tracking)# end
```

例：ローカルバインディングを使用した IPv6 IP-SGT バインディングの設定

以下の例では、IBNS バージョン 2.0 を使用します。

```
Device> enable
Device# configure terminal
Device(config)# policy-map type control subscriber policy1
Device(config-event-control-policymap)# event session-started match-all
Device(config-class-control-policymap)# 10 class always do-until-failure
Device(config-action-control-policymap)# 10 authenticate using mab
Device(config-action-control-policymap)# exit
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# description downlink to ipv6 clients
Device(config-if)# switchport access vlan 20
Device(config-if)# switchport mode access
Device(config-if)# device-tracking attach-policy snoop
Device(config-if)# access-session port-control auto
Device(config-if)# mab eap
Device(config-if)# dot1x pae authenticator
Device(config-if)# service-policy type control subscriber policy
Device(config-if)# end
```

例: VLAN を使用した IPv6 IP-SGT バインディングの設定

次に、VLAN を使用した IP-SGT バインディングを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-map vlan-list 20 sgt 3
Device(config)# end
```

例: VLAN を使用した IPv6 IP-SGT バインディングの設定

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。