



Cisco TrustSec VRF 対応 SGT

- [VRF-Aware SXP \(1 ページ\)](#)
- [VRF 対応 SGT および SGACL の IPv6 サポート \(2 ページ\)](#)
- [Cisco TrustSec VRF 対応 SGT の設定方法 \(4 ページ\)](#)
- [Cisco TrustSec VRF 対応 SGT の設定例 \(5 ページ\)](#)
- [ACE ポート範囲 \(5 ページ\)](#)
- [例：ACE ポート範囲のロールベース アクセス リスト コマンド \(6 ページ\)](#)
- [Cisco TrustSec VRF 対応 SGT の機能履歴 \(6 ページ\)](#)

VRF-Aware SXP

仮想ルーティングおよびフォワーディング (VRF) のセキュリティグループタグ (SGT) Exchange Protocol (SXP) の実装は、特定の VRF と SXP 接続をバインドします。Cisco TrustSec を有効にする前に、ネットワーク トポロジがレイヤ 2 またはレイヤ 3 の VPN に対して正しく設定されており、すべての VRF が設定されていることを前提としています。

SXP VRF サポートは、次のようにまとめることができます。

- 1 つの VRF には 1 つの SXP 接続のみをバインドできます。
- 別の VRF が重複する SXP ピアまたは送信元 IP アドレス持つ可能性があります。
- 1 つの VRF で学習 (追加または削除) された IP-SGT マッピングは、同じ VRF ドメインでのみ更新できます。SXP 接続は異なる VRF にバインドされたマッピングを更新できません。SXP 接続が VRF で終了しない場合は、その VRF の IP-SGT マッピングは SXP によって更新されません。
- VRF ごとに複数のアドレス ファミリがサポートされています。そのため、VRF ドメインの 1 つの SXP 接続が IPV4 および IPV6 両方の IP-SGT マッピングを転送できます。
- SXP には VRF あたりの接続数および IP-SGT マッピング数の制限はありません。

VRF 対応 SGT および SGACL の IPv6 サポート

Cisco IOS XE Bengaluru 17.6.x リリース以降では、VRF 対応セキュリティグループタグ (SGT) および SG アクセスコントロールリスト (SGACL) で IPv6 がサポートされています。この機能は、IPv4 の場合と同じ機能を IPv6 に対して拡張します。

SGT および SGACL 機能に対する IPv6 サポートにより、次の機能が有効になります。

- SGT バインディング
 - SGT への IPv6 アドレス間の静的バインディング
 - VLAN から SGT へのバインディング
 - IPv6 アドレスと SGT 間のマッピングの動的学習
- 施行
 - UDP または TCP ポートに基づく IPv6 トラフィックに対する SGACL 適用
 - 上位層プロトコルタイプに基づく IPv6 トラフィックに対する SGACL 適用



-
- (注)
- SGT バインディングは、リンクローカルアドレスではサポートされていません。
 - SGACL はマルチキャストトラフィックには適用されません。
-

IPv6 SGT と SGACL のスケール値は IPv4 と IPv6 の両方で同じであり、ほとんどの CLI コマンドは変更されていません。

IPv6 サポートの詳細については、次の項を参照してください。

- [IPv4 と IPv6 が SGT および SGACL テーブルを共有する方法 \(2 ページ\)](#)
- [SGT および SGACL スケール値 \(3 ページ\)](#)

Cisco.com の Cisco TrustSec コンフィギュレーションガイド、Cisco IOS XE 17 [英語] も参照してください。

IPv4 と IPv6 が SGT および SGACL テーブルを共有する方法

IPv4 と IPv6 は、FPGA で SGT および SGACL テーブルを共有します。次のリストに、共有の管理方法を示します。

- IPv4 または IPv6 を有効にすると、設定に基づいてテーブル全体が使用されます。
- IPv4 と IPv6 を有効にすると、最初の要求を行う機能に基づいてテーブルが共有されます。

- SGT および SGACL テーブルの上限を超えると、適切な syslog が生成されます。
- サポートされていないポリシーを設定すると、適切な syslog が生成されます。

SGT および SGACL スケール値

次の表に、IPv4 と IPv6 のスケール値を示します。

| エントリの種類 | スケール値 | 説明 |
|-------------------------------------|---------|---------------------|
| ホストから SGT | 1024 | ホストから SGT へのバインド |
| サブネットから SGT | 64 | ネットワークから SGT へのバインド |
| SGT X DGT マトリックス | 21 X 21 | SGT から DGT へのマッピング |
| SGACL ポリシーリストサイズ | 15 | 各 SGACL の最大 ACE |
| ロギングカウンタ [31:0] SGT および DGT ペアの数 | 32 | 最大ペア数 |



(注) デフォルトでは、ロギングは 32 の SGT と DGT のペアに対してのみ有効になっています。ただし、ロギングを有効にするペアを指定できます。32 ペアのうち任意のペアに対するロギングを無効にし、異なるペアのロギングを有効にできます。

- ロギングが有効になっている SGT と DGT のペアを表示するには、`show platform hardware cts cell-logging` コマンドを使用します。
- 特定の SGT および DGT ペアのロギングを無効にするには、`no platform cts logging` コマンドを使用します。
- 特定の SGT と DGT のペアのロギングを有効にするには、`platform cts logging` コマンドを使用します。

次のテキストは、`no platform cts logging` コマンドのオプションを示しています。

```
Device> enable
Device#configure terminal
Device(config)#no platform cts logging ?
all Disable logging for all the cells
default default logging list
from Source Group Tag (SGT) for enabling logging
```

Cisco TrustSec VRF 対応 SGT の設定方法

このセクションでは、Cisco TrustSec VRF 対応 SGT の設定方法について説明します。

VRF と SGT のマッピングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **cts role-based sgt-map vrf vrf-name {ip4_netaddress | ipv6_netaddress | host {ip4_address | ip6_address}}** sgt sgt_number
4. **end**

手順の詳細

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 1 | enable 例 : Device> enable | 特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例 : 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。 |
| ステップ 3 | cts role-based sgt-map vrf vrf-name {ip4_netaddress ipv6_netaddress host {ip4_address ip6_address}} sgt sgt_number 例 : Device(config)# cts role-based sgt-map vrf red 10.0.0.3 sgt 23 例 : Device(config)# cts role-based sgt-map vrf VRF_1 2405:201:c::f115 sgt 1201 | 指定された VRF のパケットに SGT を適用します。 IP-SGT バインドは、指定された VRF と、IP アドレスのタイプによって示される IP プロトコルのバージョンに関連付けられた IP-SGT のテーブルに入力されます。 |
| ステップ 4 | end 例 : 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。 |

Cisco TrustSec VRF 対応 SGT の設定例

このセクションでは、Cisco TrustSec VRF 対応 SGT の設定例を示します。

例 : VRF と SGT のマッピングの設定

IPv4 の例 :

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-map vrf VRF_1 22.1.1.1 sgt 1204
Device(config)# end
```

IPv6 の例 :

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-map vrf VRF_1 2405:201:c::f115 sgt 1201
Device(config)# end
```

例 : ロールベース アクセス リスト コマンド

```
Switch(config)# ipv6 access-list role-based acl-name
Switch(config-rb-acl)#?
Role-based Access List configuration commands:
<1-2147483647> Sequence Number
default      Set a command to its defaults
deny         Specify packets to reject
exit         Exit from access-list configuration mode
no           Negate a command or set its defaults
permit      Specify packets to forward
remark      Access list entry comment
Switch(config-rb-acl)#
```

ACE ポート範囲

Cisco IOS XE Bengaluru 17.6.x リリース以降、TrustSec FPGA モジュールは、いくつかのスケールリングの問題に対処するためにポリシー要素のポート範囲オプションをサポートしています。

FPGA モジュールは、TrustSec の一部として IP-to-SGT バインディングと SGACL ポリシーを維持します。Cisco IE3400 スイッチは、各セルで 21 X 21 SGT または DGT ペアと 15 個のポリシーをサポートし、IP プロトコルフィールド、L4 送信元ポート、および L4 宛先ポートを照合します。

ただし、一致基準を指定すると、ユーザアクセス権限を拡張できない場合があります。そのため、TrustSec FPGA モジュールは、各セルでサポートされるポリシーを 15 個に維持することで、各ポリシー要素のポート範囲オプションをサポートします。

この機能強化により、次のリストに示すように複数のルールを組み合わせることができます。

- IP プロトコルフィールドの照合
- L4 送信元開始ポートと終了ポートの照合
- L4 宛先開始ポートと終了ポートの照合

例：ACE ポート範囲のロールベース アクセス リストコマンド

次のコマンドを使用して、送信元ポートと宛先ポートの ACE ポート範囲を設定できます。

```
Switch(config)# ip access-list role-based rbacl
Switch(config-rb-acl)#10 deny tcp dst range ftp-data telnet
Switch(config-rb-acl)#20 permit tcp dst lt 10
Switch(config-rb-acl)#30 deny tcp dst gt 50
```

Cisco TrustSec VRF 対応 SGT 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および関連情報を示します。

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 | 機能説明 |
|--------------------------|--------------------------------------|--|
| Cisco IOS XE リリース 17.6.1 | SGT および SGACL の IPv6 サポートの拡張 | ホストから SGT へのマッピングとバインディング、およびサブネットから SGT へのバインディングを有効にします。 |
| | SGACL 適用に対する IPv6 サポートの拡張 | UDP ポート、TCP ポート、および上位層プロトコルタイプに基づいて、IPv6 トラフィックに SGACL を適用します。 |
| | TrustSec FPGA モジュールでのポート範囲オプションのサポート | オプションは、スケーリングの問題に対処するためにポリシー要素でサポートされています。 |

| リリース | 機能 | 機能説明 |
|--------------------------|---------------------------|--|
| Cisco IOS XE リリース 17.5.1 | Cisco TrustSec VRF 対応 SGT | Cisco TrustSec VRF 対応 SGT 機能は、SGT SXP 接続を特定の VRF インスタンスにバインドします。 |

