Cisco TrustSec コンフィギュレーション ガイド

First Published: 2025-08-25

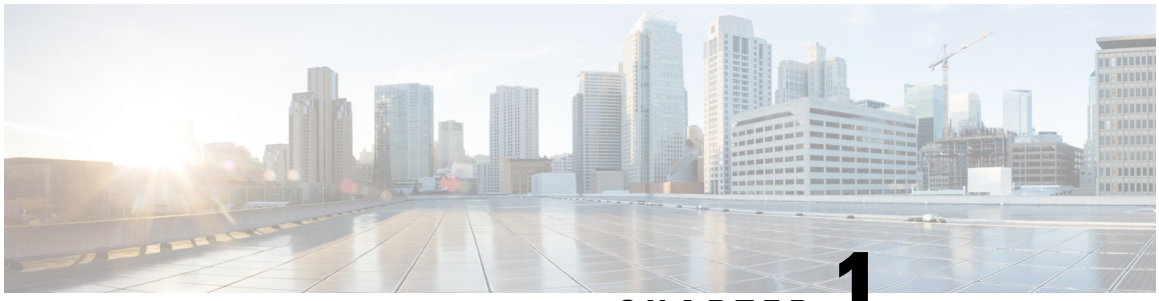
Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

最初にお読みください

サポートされている機能のみが記載されています。プラットフォームでサポートされているすべての機能を確認または明確にするには、Cisco Feature Navigatorにアクセスします。

最初にお読みください

CONTENTS



CHAPTER 1

Cisco TrustSec

Cisco TrustSec の機能の履歴

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 26.1.1	IPv6 用 RADIUS を介した CTS ポリシーサーバーリスト有効化：IPv6 用 RADIUS を介した CTS ポリシーサーバーリスト有効化のサポートが導入されました。	Cisco C9350 シリーズ スマートスイッチ Cisco C9610 シリーズ スマートスイッチ
Cisco IOS XE 26.1.1	IPv6 を介した PAC ダウンロード：IPv6 を介した PAC ダウンロードのサポートが導入されました。	Cisco C9350 シリーズ スマートスイッチ Cisco C9610 シリーズ スマートスイッチ

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	Cisco TrustSec：Cisco TrustSec は、信頼できるネットワークデバイスのドメインを確立することによってセキュアネットワークを構築します。ドメイン内の各デバイスはそのピアによって認証され、デバイス間の通信は、暗号化、メッセージ整合性チェック、データパスリプレイ防止メカニズムを使用して保護されます。	Cisco C9350 シリーズ スマートスイッチ Cisco C9610 シリーズ スマートスイッチ

Cisco TrustSec

Cisco TrustSecは、信頼できるネットワーク デバイスのドメインを確立することによってセキュアネットワークを構築します。ドメイン内の各デバイスはそのピアによって認証され、デバイス間の通信は、暗号化、メッセージ整合性チェック、データパスリプレイ防止メカニズムを使用して保護されます。

Cisco TrustSec の主要コンポーネント

Cisco TrustSec のアーキテクチャには、次の 3 種類の主要コンポーネントが含まれます。

- 認証済みネットワーキング インフラストラクチャ

  Cisco TrustSec ドメインを開始するために最初のデバイス（シードデバイス）が認証サーバーで認証された後、ドメインに追加された新しい各デバイスはドメイン内のピアデバイスにより認証されます。ピアは、ドメインの認証サーバーに対する媒介として動作します。それぞれの新たに認証されたデバイスは認証サーバーによって分類され、アイデンティティ、ロールおよびセキュリティ ポスチャに基づいてセキュリティ グループ番号が割り当てられます。

- セキュリティグループベースのアクセス制御：

  Cisco TrustSec ドメイン内のアクセスポリシーは、トポロジとは無関係で、ネットワークアドレスではなく送信元デバイスおよび宛先デバイスのロール（セキュリティグループ番号で指定）に基づいています。個々のパケットには、送信元のセキュリティ グループ番号のタグが付けられます。

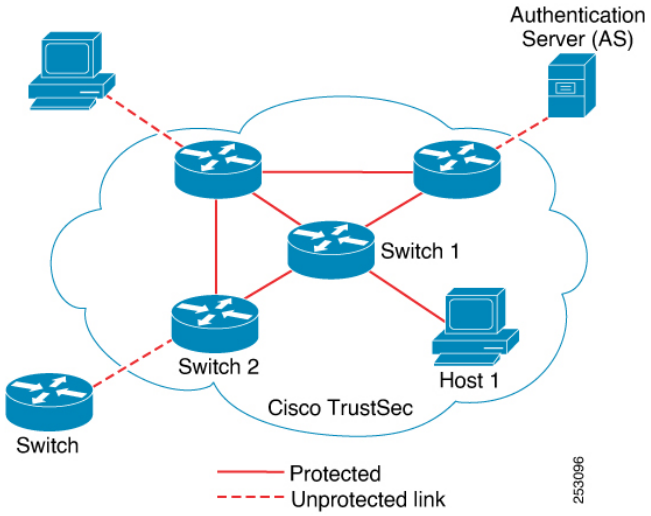
- セキュア通信：

  暗号化対応ハードウェアにより、暗号化、メッセージ整合性チェック、データパスリプレイ保護メカニズムの組み合わせを使用して、ドメイン内のデバイス間の各リンクでの通信を保護できます。

図は、以下を含む Cisco TrustSec ドメインを示しています。

- Cisco TrustSec ドメイン内のエンドポイントデバイスと複数のネットワーキングデバイス
- Cisco TrustSec ドメイン外のエンドポイントデバイスと 1 台のネットワーキングデバイスこれはデバイスが Cisco TrustSec 対応デバイスではないか、デバイスのアクセスが拒否されているためです。
- Cisco TrustSec ドメイン外の認証サーバー認証サーバーは、Cisco Identity Services Engine（Cisco ISE）、または Cisco Secure Access Control System（Cisco ACS）のいずれかを使用できます。

***Figure 1: Cisco TrustSec* ドメイン**



Cisco TrustSec 認証プロセスでのロール

Cisco TrustSec 認証プロセスには、以下のロールがあります。

- Supplicant

  Cisco TrustSec ドメイン内のピアに接続されており、Cisco TrustSec ドメインへのアクセスを試行している非認証デバイス。

- 認証サーバー

  サプリカントのアイデンティティの確認を行い、Cisco TrustSec ドメイン内のサービスへのサプリカントのアクセスを制御するポリシーを割り当てるシステム。

- オーセンティケータ

  すでに Cisco TrustSec ドメインの一部であり、認証サーバーに代わって新しいサプリカントピアを認証する権限のある認証済みデバイス。

認証プロセスのシーケンス

サプリカントとオーセンティケータ間で接続が確立される際、プロセスは通常次の手順に従います。

1. 認証（802.1X）：

   サプリカントのログイン情報は、認証サーバーと、中間デバイスとして機能するオーセンティケータによって検証されます。相互認証がサプリカントとオーセンティケータの間で行われます。

2. Authorization:

   認証サーバーは、サプリカントのアイデンティティに基づいて、接続された両方のピアにセキュリティグループの割り当てやアクセス制御リスト（ACL）などの認証ポリシーを発行します。認証サーバーは、各ピアのアイデンティティを他のサーバーと共有し、適切なポリシーをリンクに適用できるようにします。

これらの手順が正常に完了すると、オーセンティケータはリンクを未認証（ブロッキング）状態から認証済み状態に移行させ、サプリカントはCisco TrustSecドメインに参加できるようになります。

アイデンティティとログイン情報

以下のセクションでは、次の基本要素と、それらがTrustSecデプロイメント内でどのように連携するかについて説明します。

- デバイスアイデンティティ
- デバイスのログイン情報
- ユーザーのログイン情報
- Protected Access Credential（PAC）

デバイス ID

Cisco TrustSecは、IPアドレスまたはMACアドレスの代わりに、割り当てられたデバイス名（デバイスID）を使用して、スイッチを一意に識別します。これらのデバイスIDは、認証時の認証ポリシールックアップとパスワードルックアップに使用されます。

デバイスのクレデンシャル

Cisco TrustSecはパスワードベースのログイン情報をサポートし、相互認証にMSCHAPv2を使用します。

デバイスのログイン情報は、EAP-FAST フェーズ 0（PAC プロビジョニング）交換中に使用されます。後続のリンク起動では、プロビジョニングされた PAC を利用して、EAP-FAST フェーズ 1 および 2 を使用します。

ユーザークレデンシャル

Cisco TrustSec には、エンドポイント装置の特定タイプのユーザークレデンシャルは必要ありません。認証サーバーでサポートされている任意の認証メソッド（Cisco ACS 5.1 の場合は MSCHAPv2、GTC、RSA OTP など）を使用できます。

Protected Access Credential

PAC は、クライアントとサーバーの相互認証のための固有の共有ログイン情報であり、Public Key Infrastructure（PKI）とデジタル証明書が不要になります。

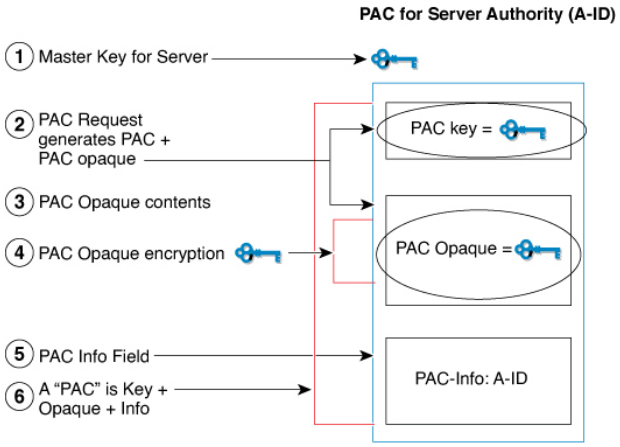
PAC の作成手順

1. サーバーの認証局アイデンティティ（A-ID）では、ローカルマスターキーが保持されます。
2. クライアント（イニシエータ アイデンティティ（I-ID））が PAC を要求すると、サーバーは一意の PAC キーと PAC-Opaque フィールドを生成します。
3. PAC-Opaque フィールドに含まれる PAC キー、I-ID、およびキー有効期間は、マスターキーで暗号化されています。
4. A-ID を含む PAC-Info フィールドが作成されます。
5. PAC は、自動的にクライアントに配布またはインポートされます。

Note サーバーは PAC または PAC キーを保持しないため、ステートレス EAP-FAST サーバーが有効になります。

次の図は、PAC の構造を示しています。PAC は、PAC-Opaque、PAC Key、および PAC-Info フィールドで構成されます。PAC-Info フィールドには A-ID が含まれます。

Figure 2: PAC のプロセスフロー



PAC のプロビジョニング

- Secure RADIUS では、認証中に PAC キーが各デバイスにプロビジョニングされ、共有秘密が導出されます。
- クライアントは、情報を回復し、アイデンティティを検証するためにサーバーが解釈する、PAC-Opaque フィールドを含む追加の RADIUS 属性を送信します。
- EAP-FAST フェーズ 0 は、自動 PAC プロビジョニングに使用されます。

PAC なし認証

PAC なしモードは、通常、デバイスと Identity Services Engine（ISE）間のセキュア通信に必要な Protected Access Credential（PAC）を不要にすることで、Cisco TrustSec ポリシーの展開をシンプルにします。この方法は、複数の ISE ノードがある環境で特に役立ちます。プライマリが使用できなくなった場合、デバイスは PAC を再確立することなく、セカンダリ ISE ノードにシームレスに接続できるため、サービスの中断が削減されます。

利点

AAA PAC なしの認証では、PAC への依存関係が解消されるため、認証プロセスが合理化されます。結果として拡張性が促進され、ユーザー体験が向上します。また、Zero Trust セキュリティの原則に沿った最新の認証アプローチのサポートが可能になります。

PAC なしの認証ワークフロー

1. PAC なしモードでは、デバイスは、Cisco TrustSec ユーザー名、パスワード、および EAP 属性メッセージを含む RADIUS 要求を送信して認証を開始します。
2. ISE は RADIUS アクセスチャレンジで応答し、EAP-FAST セッションを開始します。

3. EAP-FAST セッションが確立されると、ISE は PAC Opaque および PAC 情報を提供します。PAC Opaque には、EAP-FAST サーバーマスターキーを使用して暗号化された PAC キーとユーザーアイデンティティが含まれています。PAC 情報には、サーバーアイデンティティと存続可能時間（TTL）タイマーが含まれています。
4. 次いで PAC Opaque が、ISE への後続の Cisco TrustSec RADIUS 要求のメッセージ オーセンティケータ フィールドに埋め込まれます。これにより、環境データとセキュリティ グループ アクセス コントロール リスト（SGACL）ポリシーをセキュアにダウンロードできるようになります。

Cisco TrustSec のガイドライン

一般的な注意事項

- FIPS モードで Cisco TrustSec はサポートされていません。
- Cisco TrustSec は、IPSG が有効になっている純粋なブリッジングドメインでは設定できません。
- Cisco TrustSec は、セキュリティ アソシエーション プロトコル（SAP）をサポートしていません。

アイデンティティとログイン情報のガイドライン

無効なデバイス ID が指定された場合、Protected Access Credential（PAC）のプロビジョニングが失敗し、ハング状態のままになります。PAC をクリアし、正しいデバイス ID とパスワードを設定した後でも、PAC は失敗します。

回避策として、Cisco Identity Services Engine（ISE）で、PAC が機能するように**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [RADIUS]**メニューの [異常なクライアントの抑制（Suppress Anomalous Clients）] オプションをオフにします。

Cisco TrustSec ログイン情報の設定

このタスクでは、デバイスにデバイス ID、パスワード、および認証メソッドを設定できます。

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 **cts credentials id** *cts-id* **password** *password*

Example:

```
Device# cts credentials id ctsid password abcd
```

EAP-FAST で他の Cisco TrustSec デバイスに対して認証するときにこのデバイスが使用する Cisco TrustSec デバイス ID を設定します。Cisco TrustSec では、ネットワーク内の各デバイスがそれ自体を固有に識別する必要があるためです。

- *cts-id* 引数は、最大 32 文字で大文字と小文字を区別します。
- *password* 引数は、EAP-FAST を使用して他の Cisco TrustSec デバイスで認証するときにこのデバイスが使用するパスワードです。

Step 3 **configure terminal**

Example:

```
Device(config)# 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 4 **aaa new-model**

Example:

```
Device(config)# aaa new-model
```

アクセスコントロールの新しいコマンドおよび機能を有効にします（以前のコマンドを無効にします）。

Step 5 **aaa authentication dot1x default group radius**

Example:

```
Device(config)# aaa authentication dot1x default group radius
```

IEEE 802.1X を実行しているインターフェイスでの認証に RADIUS サーバーを使用することを指定します。

Step 6 **cts authorization list network** *list-name*

Example:

```
Device(config)# cts authorization list network cts-mlist
```

Cisco TrustSec シードデバイスが使用する AAA サーバーのリストを指定します。

Step 7 **aaa authorization network** *list-name* **group radius**

Example:

```
Device(config)# aaa authorization network cts-mlist group radius
```

RADIUS サーバーからのすべてのネットワーク関連サービス要求に、Cisco TrustSec 承認リスト名を指定します。

Step 8 **exit**

Example:

```
Device(config)# exit
```

グローバル コンフィギュレーション モードを終了します。

Step 9 **show cts server-list**

Example:

```
Device# show cts server-list
```

Cisco TrustSec シードデバイスの RADIUS サーバー設定を表示します。

Step 10 **show cts credentials**

Example:

```
Device# show cts credentials
```

Cisco TrustSec（CTS）デバイス ID を表示します。保存されたパスワードは表示されません。

PAC のダウンロード

Cisco TrustSec Protected Access Credential（PAC）のダウンロードは、以下のようなセキュリティプロセスです。

- ISE を使用してネットワークデバイスのセキュアなアイデンティティを確立します。
- RADIUS トランスポート層で EAP-FAST プロトコルを使用します。
- TrustSec 環境データと SGACL ポリシーを取得するための前提条件として機能します。

IPv6 を介した PAC のダウンロード

IPv6 を介した PAC のダウンロードは、以下のようなネットワークトランスポート機能です。

- リテラル IPv6 アドレスを使用して、ポリシーサーバーとの RADIUS セッションを確立します。
- EAP-FAST プロトコルを使用して、IPv6 トランスポートを介して PAC を取得します。
- サーバーアドレスタイプが変更された場合のログイン情報の再取得を自動化します。

この機能により、TrustSec ポリシープレーンが有効になり、IPv6 専用環境またはデュアルスタック環境で動作します。

IPv6 を介した PAC ダウンロード用のポリシーサーバーバージョン

IPv6 を介した PAC のダウンロードは、Cisco IOS XE 26.1.1 リリースからサポートされており、ポリシーサーバー（ISE）バージョン 3.5 以降が必要です。

IPv6 を介した PAC のダウンロードの利点

IPv6 を介した PAC のダウンロードの主な利点は次のとおりです。

- アドレスの柔軟性：ポリシーサーバー識別用のリテラル IPv6 アドレスをサポートします。これにより、デバイスが DNS を介してサーバーの場所を解決できます。
- トランスポートセキュリティ：基盤となるトランスポートを IPv4 から IPv6 に移行する際、EAP-FAST セッションのセキュリティを維持します。
- 動的更新：ユーザーが設定でアドレスタイプを切り替えたときに、PAC 要求を自動的に再トリガーすることで、デバイスとポリシーサーバーの同期が維持されます。

IPv6 を介した PAC ダウンロード用の ISE バージョン

IPv6 を介した PAC のダウンロードは、Cisco IOS XE 26.1.1 リリースからサポートされており、ISE バージョン 3.5 以降が必要です。

PAC ダウンロードの制約事項

PAC ダウンロード用にポリシーサーバーを設定する場合は、以下の制約事項に従います。

- デバイスは、RADIUS サーバー設定のリンクローカル IP アドレスおよび完全修飾ドメイン名（FQDN）をサポートしていません。
- PAC ダウンロードでの IPv4 アドレスタイプと IPv6 アドレスタイプのサポートは、相互に排他的ではありません。デバイスで IPv4 と IPv6 両方のアドレスタイプを設定した場合、いずれかの設定、つまり最新の設定のみが有効になります。
- デバイスは、混合モードのアドレスタイプ（デバイスの送信元アドレスタイプが IPv4 で ISE が IPv6 タイプであるなど）をサポートしていません。

PAC ダウンロード用のポリシーサーバーの設定

ポリシーサーバーへの IPv6 接続を確立し、Cisco TrustSec（CTS）の操作に必要な PAC を取得するには、この手順を使用します。同様に、IPv4 経由の PAC ダウンロードには IPv4 アドレスを使用します。

新しい TrustSec 対応デバイスを設定する場合や、既存のポリシーサーバー接続を IPv6 トランスポートに移行する場合に、このタスクを実行します。

Before you begin

- RADIUS サーバー（ISE）が、IPv6 または IPv4 アドレスを介して到達可能であることを確認します。
- 共有秘密（PAC キー）が使用可能であることを確認します。

Procedure

Step 1 ポリシーサーバーで使用される IPv4 または IPv6 アドレス、認証ポート、およびアカウンティングポートを指定して、RADIUS サーバーを設定します。

Example:

```
Switch(config)#radius server test-server
Switch(config-radius-server)#address ipv6 2001::10 auth-port 1812 acct-port 1813
```

デバイスは、RADIUS サーバーの完全修飾ドメイン名（FQDN）の使用をサポートしていません。

Step 2 RADIUS サーバーの PAC キーを定義します。

Example:

```
Switch(config-radius-server)#pac key testkey123
```

この手順により、デバイスが認証され、PAC 取得用の EAP-FAST セッションを開始できます。

このキーは、ISE サーバーで設定された共有秘密と一致している必要があります。

Step 3 PAC プロビジョニングステータスを監視します。

a) CTS PAC の詳細を確認します。

Example:

```
Switch#show cts pac
AID: 60DABBF8AD435A7B63900EE07E68D2FD
PAC-Info:
  PAC-type = Cisco Trustsec
  AID: 60DABBF8AD435A7B63900EE07E68D2FD
  I-ID: ha_senth_cat9k
  A-ID-Info: Identity Services Engine
  Credential Lifetime: 16:17:20 UTC Mon Feb 24 2025
PAC-Opaque: 000200B800030001000...705E
Refresh timer is set for 12w4d
Switch#
```

b) CTS プロビジョニングキューの詳細を確認します。

Example:

```
Switch#show cts provisioning queue
Server: 2001:420:54FF:4::400:11, Type: Radius, Provisioned: YES
AID: 3ec5d7e02bde9fd04c453918a5e2d3b4
```

デバイスは、ポリシーサーバーとのセキュアなセッションを確立し、IPv4 または IPv6 トランスポートを介して PAC を取得しました。これにより、後続の TrustSec ポリシーのダウンロードが可能になります。

Cisco TrustSec 環境データ

環境データは、Cisco TrustSec 機能を補足する運用データで構成されます。デバイスから Cisco ISE への環境データ要求は、次のデータで構成されます。

- デバイス名：デバイスの名前を指定します。
- デバイス機能：追加データを指定します。

Cisco ISE からデバイスへの環境データ応答は、次のデータで構成されます。

- デバイスのセキュリティグループタグ（SGT）：デバイス名に基づいて Cisco ISE から取得されます。
- サーバーリスト：Cisco ISE で指定された Cisco TrustSec サーバーのリストを表示します。
- SG-Name テーブル：SGT とデバイス名の間のマッピングを表示します。SGT は数字で表示され、デバイス名はテキスト形式で表示されます。
- リフレッシュ時間：環境データがリフレッシュされる時間を示します。

Note

- Cisco TrustSec 環境のデータ更新の一環として、最後に受信したサーバーが削除され、新しく受信したサーバーがサーバーリストに追加されます。更新後、サーバーリストの統計がゼロから再開され、サーバーのステータスが [Inactive] に設定されます。また、IP アドレスの状態が [Reachable] に設定されます。次に、デバイスは、後続のポリシー要求と応答に基づいてサーバーの統計とステータスを更新します。
- Cisco IOS XE Bengaluru 17.4.1 以降では、VRF を認識するように自動テスターを設定できます。**automate-tester** コマンドで **vrf** キーワードを使用すると、デフォルト以外の VRF の自動テスト機能を有効化します。

  VRF 対応の自動テスターを機能させるには、**global config ipv4/ipv6 source interface***interface-name* **vrf***vrf-name* コマンドを設定する必要があります。

IPv6 用 RADIUS を介した CTS ポリシーサーバーリストの有効化

Cisco IOS XE リリース 26.1.1 以降、ISE は、IPv4 アドレスに加えて、PSN の IPv6 アドレスを環境データの一部としてデバイスにプッシュします。デバイスは、SGACL ポリシーをダウンロードすると、これらの PSN IPv6 アドレスを使用して ISE に到達します。

このリリースより前は、環境データの一部として受信される ISE からのサーバーリスト IP は、IPv4 タイプのみでした。

SGACL ポリシーをダウンロードするためのサーバーの選択とフェールオーバーロジック

デバイスは、ISE から IPv4 アドレスと IPv6 アドレスの両方を含むサーバーリストを受信すると、特定の選択ルールおよびフェールオーバーのルールに従います。

- デバイスは、ラウンドロビンフェールオーバーメソッドを使用してアクティブなサーバーを選択します。
- リスト内のプライマリサーバーが到達不能になった場合、デバイスは、シーケンス内の次に使用可能なサーバーへの接続を自動的に試行します。
- デバイスは通常、SGACL ポリシーダウンロード用に設定された送信元インターフェイス アドレス タイプと一致するサーバーアドレスタイプを優先します。

RADIUS を介した CTS ポリシーサーバーリスト有効化の制約事項

デバイスは、混合モードのアドレスタイプ（デバイスの送信元アドレスタイプが IPv4 で ISE が IPv6 タイプであるなど）をサポートしていません。

IPv6 用の CTS ポリシーサーバーリスト有効化の確認

デバイスへの環境データのダウンロードの一環として、IPv6 サーバーリストを ISE から受信するかどうかを確認するには、この手順を使用します。

Procedure

ISE サーバーからデバイスにダウンロードされた環境データの詳細を確認します。

Example:

```
Switch# show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Service Info Table:
Local Device SGT:
  SGT tag = 2-48:TrustSec_Devices
Server List Info:
Installed list: CTSServerList1-0003, 3 server(s):
 *Server: 2001:420:54FF:4::400:11, port 1812, A-ID 1695AF86D38B22DC7C9500408E2DD35D
          Status = DEAD
          auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs

 *Server: 2001:420:54FF:4::400:12, port 1812, A-ID 1695AF86D38B22DC7C9500408E2DD35D
          Status = ALIVE
          auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs

 *Server: 2001:420:54FF:4::400:13, port 1812, A-ID 1695AF86D38B22DC7C9500408E2DD35D
          Status = DEAD
          auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Security Group Name Table:
```

```
    0-48:Unknown
    2-48:TrustSec_Devices
    3-62:Network_Services
    4-56:Employees
    5-48:Contractors
    6-49:Guests
    7-48:Production_Users
    8-49:Developers
    9-49:Auditors
    10-48:Point_of_Sale_Systems
    11-48:Production_Servers
    12-0177:Development_Servers
    13-48:Test_Servers
    14-56:PCI_Servers
    15-48:BYOD
    16-01:sgt_101
Environment Data Lifetime = 86400 secs
Last update time = 05:26:38 UTC Tue Jul 1 2025
Env-data expires in   0:23:52:36 (dd:hr:mm:sec)
Env-data refreshes in 0:23:52:36 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
Retry_timer (60 secs) is not running
Switch#
```

セキュリティグループとセキュリティグループタグ

以下のセクションでは、セキュリティグループとセキュリティグループタグについて説明します。

セキュリティ グループ

セキュリティグループは、アクセスコントロールポリシーを共有するユーザー、エンドポイントデバイス、およびリソースのコレクションです。Cisco ISE または Cisco Secure ACS では、これらのグループは管理者が定義します。新しいユーザーおよびデバイスが Cisco TrustSec（CTS）ドメインに参加すると、認証サーバーは、これらを適切なセキュリティグループに自動的に割り当てます。各グループは、Cisco TrustSec ドメイン内でグローバルに認識される一意の 16 ビットセキュリティグループ番号を指定されます。セキュリティグループの総数は、認証済みのネットワークエンティティの数によって決定されます。管理者がこれらのグループ番号を手動で設定する必要はありません。

セキュリティグループタグとパケットタギング

デバイスが認証されると、Cisco TrustSec は、そのデバイスから発信されるすべてのパケットにセキュリティグループタグ（SGT）をタグ付けします。このタグには、デバイスに割り当てられたセキュリティグループ番号が含まれており、Cisco TrustSec ヘッダー内のネットワーク全域をパケットとともに移動します。SGT は、企業のネットワーク全体における送信元のアクセス権限を定義する単一のラベルとして機能します。

送信元および宛先グループタグ

SGTは、パケットの送信元のセキュリティグループを表すため、送信元SGTと呼ばれることがよくあります。パケットを受信するデバイスは、宛先セキュリティグループと呼ばれるセキュリティグループにも割り当てられます。わかりやすくするため、これを宛先グループタグ（DGT）と呼ぶことができますが、Cisco TrustSecパケット自体には宛先デバイスのセキュリティグループ番号が含まれていません。

送信元セキュリティグループタグの決定

パケットがCisco TrustSecドメインに入る際、入力ポイントのネットワークデバイスは送信元SGTを識別する必要があります。これにより、TrustSec環境への転送の前にパケットに適切にタグ付けすることができます。同様に出力デバイスは、セキュリティ グループ アクセス コントロール リスト（SGACL）を適用するために、パケットのSGTを特定する必要があります。

ネットワークデバイスがパケットのSGTを特定するいくつかの方法があります。

1. 認証サーバーからのポリシー取得

   Cisco TrustSec認証プロセス後、ネットワークデバイスは認証サーバーからポリシー情報を取得します。この情報には、ピアデバイスが信頼できるかどうかが含まれます。ピアデバイスが信頼できない場合、認証サーバーはSGTを提供します。ネットワークデバイスは、SGTをそのピアから受信したすべてのパケットに適用します。

2. パケットに含まれるSGT

   パケットが信頼できるピアデバイスから受信された場合、パケットにはすでにSGTが付与されています。この状況は、特定のパケットのCisco TrustSecドメインにおける最初のエントリポイントではないデバイスに当てはまります。

3. アイデンティティ ポート マッピング（IPM）

   アイデンティティ ポート マッピングを使用して、ネットワーク管理者は、ピアデバイスに接続されているリンクにアイデンティティを手動で割り当てることができます。その後ネットワークデバイスは、SGTおよび信頼ステータスを含むポリシー情報を認証サーバーに要求します。

4. 送信元IPアドレスルックアップ

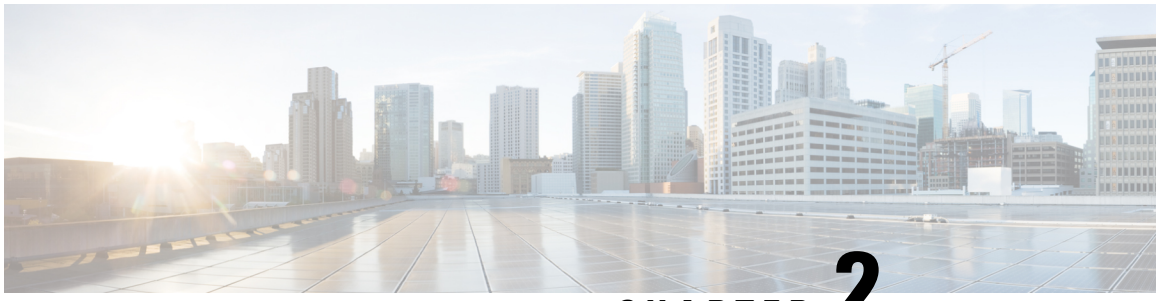
   特定のシナリオでは、送信元IPアドレスに基づいてパケットにSGTを割り当てるようにポリシーを設定できます。SGT交換プロトコル（SXP）を使用して、IPアドレスとSGT間のマッピングテーブルに自動的に入力することもできます。

宛先セキュリティグループタグの決定

Cisco TrustSecドメインの出力ネットワークデバイスは、SGACLを適用するための宛先セキュリティグループ（DGT）の識別を担当します。パケットの宛先セキュリティグループを決定するため、ネットワークデバイスは、パケットの送信元セキュリティグループを決定するために使用さ

れるのと同じ方法を使用します（宛先グループ番号はパケットのタグに含まれていないため、パケットのタグからのグループ番号の取得を除く）。

特定のシナリオでは、入力デバイスまたはその他の中間ネットワークデバイスが宛先グループ情報にアクセスできることがあります。その場合、出力点だけではなく、該当するデバイスでもSGACL を適用できます。



CHAPTER 2

セキュリティグループ ACL

SGACL 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 26.2.1ea	SGACL：セキュリティ グループ アクセス コントロール リスト（SGACL）機能のサポートが導入されました。	Cisco C9550 シリーズ スマート スイッチ

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	SGACL：セキュリティ グループ アクセス コントロール リスト（SGACL）を使用すると、管理者は、割り当てられたセキュリティグループとアクセスしているリソースに基づいて、ユーザーが実行できる操作を制御するポリシーを適用できます。	Cisco C9350 シリーズ スマート スイッチ Cisco C9610 シリーズ スマート スイッチ

セキュリティグループ ACL

セキュリティ グループ アクセス コントロール リスト（SGACL）を使用すると、管理者は、割り当てられたセキュリティグループとアクセスしているリソースに基づいて、ユーザーが実行できる操作を制御するポリシーを適用できます。

SGACL は、従来の IP アドレスとフィルタではなく、セキュリティグループタグに依存するステートレスなアクセス制御メカニズムを提供します。

SGACL ポリシーをプロビジョニングする主な方法には、以下の 3 つがあります。

- 静的ポリシープロビジョニング：

  管理者は **cts role-based permission** コマンドを使用して SGACL ポリシーを手動で定義します。

- 動的ポリシープロビジョニング：

  SGACL ポリシーは、Cisco Identity Services Engine（ISE）ポリシー管理機能によって一元的に管理および設定されます。

- 認可変更（CoA）：

  Cisco ISE で SGACL ポリシーが更新されると、新しいポリシーは CoA を介して TrustSec デバイスにプッシュされます。デバイスのデータプレーンでは、CoA パケットに新しいポリシーが適用されます。その後、さらなるポリシー適用のためにコントロールプレーンに転送されます。

SGACL ポリシーを使用したロールベースのアクセス制御

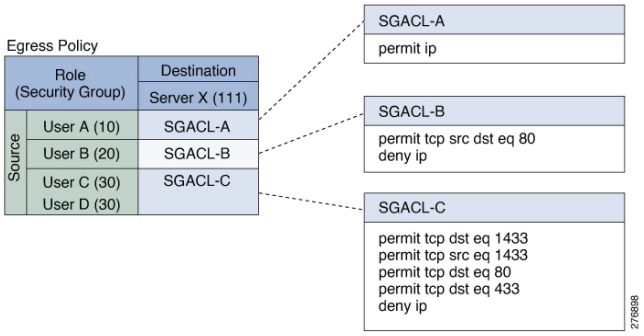
SGACL を使用すると、割り当てられたセキュリティグループとアクセスするリソースに基づいて、ユーザーが実行できるアクションを正確に制御できます。

Cisco TrustSec ドメイン内で、ポリシーの適用は権限マトリックスを使用して管理されます。一方の軸には送信元セキュリティグループ番号が、もう一方の軸には宛先セキュリティグループ番号が表示されます。マトリックスの各セルでは、SGACL の順序付きリストが保持され、特定の送信

元セキュリティグループから特定の宛先セキュリティグループに移動するパケットに適用される権限が指定されます。

次の図に、3 つの定義済みのユーザーロールと 1 つの定義済み宛先リソースを含むシンプルなドメインの Cisco TrustSec 許可マトリックスの例を示します。ユーザーの役割に基づいて宛先サーバーへのアクセスを 3 つの SGACL ポリシーで制御します。

***Figure 3: SGACL* ポリシー マトリクスの例**



Cisco TrustSec での SGACL の利点

ユーザーとデバイスをセキュリティグループに割り当て、セキュリティグループ間でのアクセスを制御することにより、Cisco TrustSec は、ロールベースのトポロジに依存しないアクセス制御を実現します。IP アドレスに依存する従来のアクセス制御リスト（ACL）とは異なり、SGACL はデバイスアイデンティティを使用します。これは、デバイスがネットワーク内の任意の場所で IP アドレスを移動または変更することができ、ロールと権限が同じである限り、セキュリティポリシーは変更されないことを意味します。新しいユーザーまたはデバイスが追加された場合、適切なセキュリティグループに割り当てるだけで、グループの権限がすぐに継承されます。

シンプルなポリシー管理とリソースの効率

SGACL は、アクセス コントロール エントリ（ACE）の数と複雑さを抑制することにより、アクセス制御を合理化します。ACE の総数は、個別の権限数によって決定されますが、これは通常、従来の IP ベースの ACL よりも大幅に少なくなります。このロールベースのアプローチにより、継続的なメンテナンスがシンプル化されるだけでなく、ネットワークデバイスで TCAM などのハードウェアリソースをより効率的に使用できます。Cisco TrustSec は、最大 5,000 の SGACL ポリシーをサポートします。

Cisco TrustSec でのデバイス認証とリンク認可

デバイス認証が終了すると、サプリカントとオーセンティケータの両方が認証サーバーからセキュリティポリシー情報を受信します。2 台のデバイスは、リンク認可を実行し、Cisco TrustSec デバイス ID に基づいて、該当するリンクセキュリティポリシーを適用します。

リンクの認証メソッドは、802.1X 認証または手動認証に設定できます。

- 802.1X 認証：

各デバイスは、認証サーバーによって提供されたデバイス ID を使用します。

- 手動認証：

  デバイス ID を各ピアに手動で割り当てる必要があります。

認証サーバーは以下のポリシー属性を提供します。

- Cisco TrustSec 信頼：

  ピアデバイスによるパケットへのセキュリティグループタグ（SGT）の挿入を信頼するかどうかを指定します。

- ピア SGT：

  ピアが属しているセキュリティグループを識別します。ピアが信頼されていない場合は、デバイスから受信したすべてのパケットにこの SGT がタグ付けされます。ピアの SGT に関連付けられた SGACL が存在するかどうか不明な場合、デバイスが認証サーバーに追加の要求を送信して、必要な SGACL を取得することがあります。

- 認可の有効期限：

  承認とポリシーが有効である秒数を示します。デバイスは、期限切れになる前にポリシーと認可を更新する必要があります。キャッシュされた認証およびポリシーデータは、有効期限が切れていない場合、リブート後に再利用できます。

Note Cisco TrustSec デバイスは、認証サーバーからピアの適切なポリシーを取得できない場合に備えて、最小限のデフォルト アクセス ポリシーをサポートする必要があります。

SGACL レイヤ 2 適用

レイヤ 2 での適用は、インターフェイスまたは VLAN に SGACL ポリシーを適用し、パケットに含まれる SGT に基づいて通信をフィルタリングすることによって行われます。適用すると、同じレイヤ 2 ドメイン内でのセグメンテーションと制御が可能になります。

ルーテッドおよびスイッチド トラフィックでの SGACL の強制

SGACL の強制は IP トラフィックだけに適用されますが、強制はルーティングまたはスイッチングされるトラフィックに適用できます。

- ルーティングされた通信：

  SGACL の適用は IP 通信にのみ適用され、出力スイッチ（たとえば、ディストリビューション スイッチやルーテッドポートを備えたアクセススイッチ）によって実行されます。グローバルに有効にすると、レイヤ 3 インターフェイス（SVI を除く）で自動的に実行されます。

- スイッチされた通信：

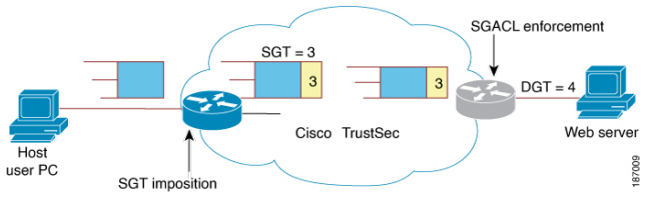
適用は、ルーティングされていない単一のスイッチングドメイン内の通信に対して行われます。VLAN 内でスイッチングされるパケットまたは VLAN に関連付けられた SVI に転送されるパケットに適用できます。ただし、VLAN ごとに明示的に有効化する必要があります。

Cisco TrustSec での入力タギングおよび出力適用

Cisco TrustSec では、入力タギングと出力適用の組み合わせによって、アクセス制御が適用されます。通信が Cisco TrustSec ドメインに到達すると、入力デバイスは、送信元のセキュリティグループ番号を識別する SGT を使用してパケットにタグを付けます。通信が TrustSec ドメインを通過する間、この SGT はそのまま保持されます。出力ポイントで、出力デバイスは、送信元 SGT と宛先のセキュリティグループ番号（宛先グループタグまたは DGT とも呼ばれます）の両方を評価します。この情報を使用して、出力デバイスは SGACL ポリシーマトリックスを参照し、通信に適したアクセスポリシーを決定して適用できます。

Cisco TrustSec ドメインでは、次の図のように SGT の割り当てと SGACL の適用が実行されます。

Figure 4: Cisco TrustSec* ドメインの *SGT* と *SGACL



SGT および SGACL が適用されたパケットフローは、次のように動作します。

1. ホスト PC は Web サーバーにパケットを送信します。PC と Web サーバーは Cisco TrustSec ドメインのメンバーではありませんが、パケットのパスは Cisco TrustSec ネットワークを通過します。
2. Cisco TrustSec の入力デバイスは、パケットを受信し、認証サーバーによりホスト PC に割り当てられたとおり、セキュリティグループ番号 3 の SGT を追加します。
3. Cisco TrustSec 出力デバイスは、パケットを検査し、送信元グループ 3（ホスト PC）から宛先グループ 4（Web サーバー）への通信を制御する SGACL ポリシーを適用します。グループ 4 は、認証サーバーによって Web サーバーに割り当てられたセキュリティグループです。
4. SGACL が通信を許可すると、Cisco TrustSec 出力スイッチはパケットから SGT を削除して、Web サーバーに転送します。

SGACL ロギング

Cisco TrustSec における SGACL ロギングでは、SGACL に一致する通信に関する詳細情報が記録されます。SGACL ロギングが有効になっている場合、デバイスは以下の情報をログに記録します。

- 送信元および宛先セキュリティグループタグ（SGT）

- SGACL ポリシーの名前
- パケットのプロトコルタイプ
- パケットで実行されるアクション

ロギングオプションは個々の ACE に適用できるため、それらの ACE に一致するパケットのみがログに記録されます。log キーワードをトリガーする最初のパケットは、syslog メッセージを生成します。その後、5 分ごとにログメッセージが報告されます。同じ ACE が同じ特性を持つ別のパケットをログに記録すると、デバイスの一致カウンタの数が増分され、その情報が次のレポートに含められます。

ロギングを有効にするには、SGACL 設定で ACE 定義の前に **log** キーワードを使用します。たとえば、**permit ip log** のようになります。

SGACL ロギングが有効の場合、デバイスからクライアントへの ICMP 要求メッセージは、IPv4 および IPv6 プロトコルについては記録されません。ただし、クライアントからデバイスへの ICMP 応答メッセージがログに記録されます。

次に、送信元と宛先の SGT、ACE の一致（許可または拒否アクション）、およびプロトコル、つまり TCP、UDP、IGMP、および ICMP 情報を表示するサンプルログを示します。

```
*Jun 2 08:58:06.489: %C4K_IOSINTF-6-SGACLHIT: list deny_udp_src_port_log-30 Denied
udp 24.0.0.23(100) -> 28.0.0.91(100), SGT8 DGT 12
```

SGACL ロギングおよびメッセージ制御

デバイスは、標準 IP アクセスリストまたは SGACL によって許可または拒否されたパケットに関するログメッセージを生成できます。パケットが SGACL エントリと一致するたびに、情報メッセージがコンソールに送信されます。コンソールに表示されるメッセージの量は、syslog の出力を制御する **logging console** コマンドを使用して管理します。

SGACL ロギングは、はるかに高いロギングレートを可能にする NetFlow ハードウェアを使用するように拡張されました。

最初のパケットが SGACL エントリをトリガーすると、フローが作成され、NetFlow タイムアウトに基づいてロギングが実行されます。タイムアウト時間は、非アクティブなフローの場合は 30 秒、アクティブなフローの場合は 1 分です。この最初の期間の後、後続のパケットはカウントされて集約され、5 分ごとにロギングメッセージが生成されます。

各ログメッセージには、次の内容が含まれます。

- アクセスリスト番号
- パケットが許可されたか、拒否されたか
- 送信元 IP アドレスと宛先 IP アドレス
- 入力インターフェイス
- 過去 5 分間に同じ送信元から許可または拒否されたパケットの数

SGACL セル統計情報

SGACL セル統計情報では、SGACL ポリシーの適用に関する詳細な可視性が提供されます。適用マトリックスは、送信元 SGT と宛先 SGT のペア別に編成され、各セルはそれらのグループ間で適用される権限を表します。管理者は、各 SGT ペアの SGACL によって許可または拒否されたパケットを示すセルごとの統計情報を表示できます。

show cts role-based counters コマンドを使用して表示できる既存の「セルごとの」SGACL 統計情報に加えて、**show ip access-list** *sgacl_name* コマンドを使用して ACE 統計情報も表示できます。これについて追加設定は必要ありません。

次に、**showipaccess-list** コマンドを使用して ACE カウントを表示する例を示します。

```
Device# show ip access-control deny_udp_src_port_log-30
Role-based IP access list deny_udp_src_port_log-30 (downloaded)
10 deny udp src eq 100 log (283 matches)
20 permit ip log (50 matches)
```

SGACL モニター モード

SGACL モニターモードは、Cisco TrustSec のデプロイメント前フェーズ用に設計されており、管理者は、セキュリティポリシーを適用せずにセキュリティポリシーをテストできます。このモードは、実際の適用が開始される前に、ポリシーが想定どおりに動作することを確認するのに役立ちます。ポリシーが意図されたとおりに機能しない場合、モニターモードで問題を簡単に特定して修正できます。これにより、適用が有効になる前に、不正アクセスの拒否などのセキュリティ要件が満たされます。

モニタリングは、SGT-DGT（送信元グループタグと接続先グループタグ）ペアレベルで動作します。SGACL モニターモードが有効になっている場合、ポリシー内の拒否アクションは、デバイスのラインカードで許可として扱われます。これにより、SGACL カウンタとロギングによりポリシーの動作への可視性が提供され、適用がアクティブな場合に通信がどのように処理されるかが示されます。モニター対象のすべての通信が許可されるため、テストフェーズの間にサービスが中断されることはありません。

SGACL の制約事項

次の制約事項がすべてのスイッチに適用されます。

- ハードウェアの制限により、Cisco TrustSec SGACL はハードウェアのパント（CPUバウンド）トラフィックに適用できません。ソフトウェアでの SGACL の適用は、スイッチ仮想インターフェイス（SVI）、レイヤ 2 およびレイヤ 3 の Location Identifier Separation Protocol（LISP）、およびループバック インターフェイスの CPU バウンド通信ではバイパスされます。
- SGACL ポリシーを設定する際に、IP バージョンを IPv4 または IPv6 から 非依存（IPv4 と IPv6 の両方に適用）に変更した場合（逆も同様）、IPv4 と IPv6 に対応する SGACL ポリシーは管理 VRF インターフェイスを介して完全にダウンロードされません。

- SGACL ポリシーを設定する際に、既存の IP バージョンを他のバージョン（IPv4 または IPv6 または 非依存）に変更した場合（逆も同様）、RADIUS を使用して Cisco Identity Services Engine（ISE）からの認可変更（CoA）を実行できません。代わりに、SSH を使用して **cts refresh policy** コマンドを実行し、手動でポリシーを更新します。
- **deny all** をデフォルトアクションとする SGT 許可モデルを使用する場合、デバイスのリロード後に Cisco TrustSec ポリシーが ISE サーバーから部分的にダウンロードされることがあります。

  これを回避するには、デバイスで静的ポリシーを定義します。deny all オプションが適用されている場合でも、静的ポリシーは通信を許可します。これにより、デバイスは ISE サーバーからポリシーをダウンロードし、定義された静的ポリシーを上書きできます。デバイス SGT では、グローバル コンフィギュレーション モードで次のコマンドを設定します。

  - **cts role-based permissions from** *sgt_num* **to unknown**
  - **cts role-based permissions from unknown to** *sgt_num*

次の制約事項が Cisco C9610 シリーズ スマートスイッチに適用されます。

- 同じ ACL のセットを通常の SGACL セル権限と SGACL デフォルト権限の両方に使用することはできません。代わりに、デフォルトの権限に固有の ACL のセットを使用します。

SGACL の設定方法

以下のセクションでは、SGACL に関する設定情報を提供します。

SGACL ポリシーの設定プロセス

SGACL ポリシーを設定してイネーブルにするには、次の手順を実行します。

Procedure

Step 1 SGACL ポリシーの設定は、主に Cisco Identity Services Engine（ISE）のポリシー管理機能によって実行する必要があります。

SGACL ポリシー設定のダウンロードに Cisco ISE での AAA を使用しない場合は、SGACL のマッピングとポリシーを手動で設定できます。

Note
Cisco ISE からダイナミックにダウンロードされた SGACL ポリシーは、競合のローカル定義されたポリシーよりも優先されます。

Step 2 ルーテッドポートの出力トラフィックに対する SGACL ポリシーの適用を有効にするには、「SGACL ポリシーの適用のグローバルな有効化」セクションに記載されているように、SGACL ポリシー適用を有効にします。

Step 3 VLAN 内のスイッチングされたトラフィック、または VLAN に関連付けられた SVI に転送されるトラフィックに対して SGACL ポリシーの適用を有効にするには、「VLAN に対する SGACL ポリシーの適用の有効化」セクションの説明に従って、特定の VLAN に対して SGACL ポリシーの適用を有効にします。

SGACL ポリシー適用のグローバルな有効化

Cisco TrustSec をイネーブルにしたルーテッド インターフェイスで SGACL ポリシーの強制をグローバルにイネーブルにする必要があります。

ルーテッド インターフェイスの SGACL ポリシーの強制をイネーブルにするには、次の作業を行います。

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 enforcement**

Example:

```
Device(config)# cts role-based enforcement
```

ルーテッド インターフェイスで Cisco TrustSec SGACL ポリシーの強制を有効にします。

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。

インターフェイスごとの SGACL ポリシー適用の有効化

Cisco TrustSec をイネーブルにしたルーテッド インターフェイスで SGACL ポリシーの強制をグローバルにイネーブルにする必要があります。

ルーテッド インターフェイスの SGACL ポリシーの強制をイネーブルにするには、次の作業を行います。

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 **interface** *type slot/port*

Example:

```
Device(config)# interface gigabitethernet 6/2
```

インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

Step 4 **cts role-based enforcement**

Example:

```
Device(config-if)# cts role-based enforcement
```

ルーテッド インターフェイスで Cisco TrustSec SGACL ポリシーの強制をイネーブルにします。

Step 5 **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 6 **show platform software fed [switch] [active | standby] sgacl port**

Example:

```
Device#show platform software fed switch active sgacl port |  i Port|6/2
```

（オプション）インターフェイスでの Cisco TrustSec SGACL ポリシー適用のステータスを表示します。

VLAN での SGACL ポリシー適用の有効化

VLAN 内のスイッチングされたトラフィック、または VLAN に関連付けられた SVI に転送されるトラフィックに対してアクセス コントロールを適用するには、特定の VLAN に対して SGACL ポリシーの強制をイネーブルにする必要があります。

VLAN または VLAN リスト内で、SGACL ポリシーの強制をイネーブルにするには、次の作業を行います。

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 enforcement vlan-list** *vlan-list*

Example:

```
Device(config)# cts role-based enforcement vlan-list 31-35,41
```

VLAN または VLAN リストで Cisco TrustSec SGACL ポリシーの強制をイネーブルにします。

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。

ネットワークデバイスでの Cisco TrustSec ステータスの確認

ネットワークデバイスで Cisco TrustSec のステータスを確認するには、次の手順を実行します。

Procedure

Step 1 インターフェイスで Cisco TrustSec（CTS）ロールベース適用ステータスを確認します。

Example:

```
Device#show platform software fed switch active sgacl port |  i Port|1/0/23

Port            Status     Port-SGT  Trust  Propagate  IngressCache EgressCache
Te1/0/23       Enabled         0     No      No          No          No
```

インターフェイスでロールベース適用設定を削除すると、出力の `Status` フィールドには `Disabled` と表示されます。

Step 2 インターフェイスでの静的 SGT、MACsec 暗号化、または SGT インラインタギングに関連した CTS 設定のステータスを確認します。

Example:

この例では、静的 SGT がインターフェイス Te1/0/12 で設定されています。

```
interface TenGigabitEthernet1/0/12
 description lan interface
 switchport mode trunk
 cts manual
  policy static sgt 8000 trusted
```

show cts interface コマンドの出力には、そのインターフェイスについて `CTS is enabled` と表示されます。

```
Device#show cts interface te1/0/12
Global Dot1x feature is Disabled
Interface TenGigabitEthernet1/0/12:
    CTS is enabled.
```

この例では、インターフェイス Te1/0/23 には、静的 SGT、MACsec 暗号化、または SGT に関連した設定がありません。そのため、インターフェイスでロールベースの適用が有効になっていても、コマンド出力に `CTS is disabled` と表示されます。

```
Device#show cts interface te1/0/23
Global Dot1x feature is Disabled
Interface TenGigabitEthernet1/0/23:
    CTS is disabled.

    L3 IPM:   disabled.
```

この動作はインターフェイス VLAN でも同じです。この例では、VLAN 1035 でロールベースの適用が有効になっています。それでも、**show cts interface vlan 1035** コマンド出力には `CTS is disabled` と表示されます。

```
Device#show run | i cts role-based enforcement
cts role-based sgt-map vlan-list 1044 sgt 8
cts role-based sgt-map vlan-list 1035 sgt 13
cts role-based enforcement
cts role-based enforcement vlan-list 1030,1032,1035,1044-1045,2047

Device#show cts interface vlan 1035
Global Dot1x feature is Disabled
Interface Vlan1035:
    CTS is disabled.
```

```
    L3 IPM:   disabled.
```

Note
show cts interface コマンド出力では、CTS ロールベースの適用がインターフェイスでアクティブになっているかどうかが示されません。

ロールベースの適用がグローバル、インターフェイスレベル、VLAN レベル、またはこれらすべてのレベルで有効になっている場合でも、**show cts interface** <> コマンドの出力には、これらのいずれかに関連した設定がインターフェイスレベルで設定されている場合にのみ、`CTS is enabled` と表示されます。

- 静的 SGT
- MACSec 暗号化
- SGT インライン タギング

Step 3 CTS が有効になっているインターフェイスの概要を表示します。

Example:

この例では、インターフェイス Te1/0/23 で **role-based enforcement** が有効になっていても、コマンド出力にそのインターフェイスは表示されません。

```
Device#show cts interface summary
CTS Interfaces
---------------------
Interface                       Mode    IFC-state dot1x-role peer-id    IFC-cache
Critical-Authentication
------------------------------------------------------------------------------
Te1/0/1                         MANUAL  OPEN      unknown    unknown    invalid  Invalid
Te1/0/12                        MANUAL  OPEN      unknown    unknown    invalid  Invalid
```

静的 SGT、MACsec 暗号化、または SGT インライン タギングに関連した設定がインターフェイスに存在する場合、**show cts interface** コマンドの出力にその特定のインターフェイスも一覧表示されます。

```
interface TenGigabitEthernet1/0/23
 description lan interface
 switchport mode trunk
 cts manual
  policy static sgt 8000 trusted--->static sgt configuration

Device#show cts interface summary
CTS Interfaces
---------------------
Interface                       Mode    IFC-state dot1x-role peer-id    IFC-cache
Critical-Authentication
------------------------------------------------------------------------------
Te1/0/1                         MANUAL  OPEN      unknown    unknown    invalid  Invalid
Te1/0/12                        MANUAL  OPEN      unknown    unknown    invalid  Invalid
Te1/0/23                        MANUAL  OPEN      unknown    unknown    invalid  Invalid
```

SGACL モニターモードの設定

SGACL モニターモードを設定するには、次の手順を実行します。

Before you begin

SGACL モニターモードを設定する前に、次の点を確認してください。

- Cisco TrustSec が有効になっている。
- カウンタが有効になっている。

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 monitor all**

Example:

```
Device(config)# cts role-based monitor all
```

グローバルモニターモードを有効にします。

Step 4 **cts role-based monitor permissions from** {*sgt_num*} **to** {*dgt_num*} [**ipv4** | **ipv6**]

Example:

```
Device(config)# cts role-based permissions from 2 to 3 ipv4
```

IPv4 または IPv6 ロールベースアクセス制御リスト（RBACL）のモニターモードを有効にします。

- *sgt_num*：セキュリティグループタグ
- *dgt_num*：宛先グループタグ

Step 5 **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。

SGACL ポリシーの手動設定

送信元グループタグ（SGT）と宛先グループタグ（DGT）の範囲に適用されるロールベースのアクセス制御リスト（ACL）は、出力トラフィックに適用される Cisco TrustSec ポリシーである SGACL になります。SGACL ポリシーを設定するための推奨されるアプローチは、Cisco Identity Services Engine（ISE）のポリシー管理機能を使用する方法です。

ローカル（手動）設定では、ロールベース ACL を作成し、それを SGT の特定の範囲にバインドできます。この機能により、デバイスで直接アクセス コントロール ポリシーを定義して適用できます。

Note Cisco ISE から動的にダウンロードされた SGACL ポリシーは、手動で設定されたポリシーと競合する場合、それを上書きします。

IPv4 SGACL ポリシーの設定と適用

IPv4 SGACL ポリシーを設定して適用するには、次の手順を実行します。

Before you begin

SGACL および RBACL を設定する場合、名前付きアクセスコントロールリスト（ACL）はアルファベットで始まる必要があります。

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 **ip access-list role-based** *rbacl-name*

Example:

```
Device(config)# ip access-list role-based allow_webtraff
```

RBACL を作成して、ロールベース ACL コンフィギュレーション モードを開始します。

Step 4 {[*sequence-number*] | **default** | **permit** | **deny** | **remark**}

Example:

```
Device(config-rb-acl)# 10 permit tcp dst allowed in extended named access list eq 80 dst
eq 20
```

RBACL のアクセス コントロール エントリ（ACE）を指定します。

拡張名前付きアクセス リスト コンフィギュレーション モードで使用可能なコマンドおよびオプションの大部分を、送信元および宛先フィールドを省略して使用できます。

次の ACE キーワードはサポートされていません。

- reflect
- evaluate
- time-range

Step 5 **exit**

Example:

```
Device(config-rb-acl)# exit
```

RBACL を作成して、ロールベース ACL コンフィギュレーション モードを開始します。

Step 6 **ip access-list role-based** *rbacl-name*

Example:

```
Device(config)# ip access-list role-based allow_webtraff
```

ロールベース ACL コンフィギュレーション 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 7 **cts role-based permissions** {**default** | [**from** { *sgt_num* | **unknown**} **to** {*dgt_num* | **unknown**}] {*rbacls* **ipv4** *rbacls*}

Example:

```
Device(config)# cts role-based permissions from 55 to 66 allow_webtraff
```

SGT と DGT を RBACL にバインドします。この設定は、Cisco ISE で設定された権限マトリックスにデータを入力することに似ています。

- **default**：デフォルトの権限リスト。
- *sgt_num*：0 ～ 65,519。送信元グループタグ。
- *dgt_num*：0 ～ 65,519。宛先グループタグ。
- **unknown**：SGACL がセキュリティグループ（送信元または宛先）を特定できないパケットに適用されます。
- **ipv4**：RBACL が IPv4 であることを示します。

- *rbacls*：RBACL の名前。

Step 8 **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。

IPv6 SGACL ポリシーの設定

IPv6 SGACL ポリシーを手動で設定するには、次の作業を行います。

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 **ipv6 access-list role-based** *sgacl-name*

Example:

```
Device(config)# ipv6 access-list role-based sgaclname
```

名前付き IPv6 SGACL を作成して、IPv6 ロールベース ACL コンフィギュレーション モードを開始します。

Step 4 {**permit** | **deny**} *protocol* [**dest-option** | **dest-option-type** {*doh-number* | *doh-type*}] [**dscp** *cp-value*] [**flow-label** *fl-value*] [**mobility** | **mobility-type** {*mh-number* | *mh-type*}] [**routing** | **routing-type** *routing-number*] [**fragments**] [**log** | **log-input**] [**sequence** *seqno*]

Example:

```
Device(config-ipv6rb-acl)# permit 33 dest-option dscp af11
```

RBACL のアクセス コントロール エントリ（ACE）を指定します。

拡張名前付きアクセス リスト コンフィギュレーション モードで使用可能なコマンドおよびオプションの大部分を、送信元および宛先フィールドを省略して使用できます。

次の ACE キーワードはサポートされていません。

- **reflect**
- **evaluate**
- **time-range**

Step 5 **end**

Example:

```
Device(config-ipv6rb-acl)# end
```

IPv6 ロールベース ACL 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。

手動での SGACL ポリシーの適用

手動で SGACL ポリシーを適用するには、次の作業を行います。

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 permissions default** [**ipv4** | **ipv6**] [*sgacl-name1* [*sgacl-name2* [*sgacl-name3* ...]]]

Example:

```
Device(config)# cts role-based permissions default MYDEFAULTSGACL
```

デフォルト SGACL を指定します。デフォルト ポリシーは明示的なポリシーが送信元と宛先セキュリティグループの間にない場合に適用されます。

Step 4 **cts role-based permissions from** {*source-sgt* | **unknown**} to {*dest-sgt* | **unknown**} [**ipv4** | **ipv6**] *sgacl-name1* [*sgacl-name2* [*sgacl-name3* ...]]]

Example:

```
Device(config)# cts role-based permissions from 3 to 5 SRB3 SRB5
```

SGT および DGT に適用する SGACL を指定します。

- *source-sgt*：範囲は 1 ー 65533 です。
- *dest-sgt*：範囲は 1 ー 65533 です。
- **from**：送信元 SGT を指定します。
- **to**：宛先セキュリティグループを指定します。
- **unknown**：SGACL がセキュリティグループ（送信元または宛先）を特定できないパケットに適用されます。

Note

- デフォルトでは、SGACL は IPv4 であると見なされます。
- ACS から動的にダウンロードされた SGACL ポリシーは、競合の手動ポリシーよりも優先されます。

Step 5 **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。

SGACL ポリシーの更新

SGACL ポリシーを更新するには、次のタスクを実行します。

Procedure

	Command or Action	Purpose
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	**cts refresh policy** {**peer** [*peer-id*] | **sgt** [*sgt_number* | **default** | **unknown**]} **Example:** `Device# cts refresh policy peer my_cisco_ise`	認証サーバーからの SGACL ポリシーの即時リフレッシュを実行します。 • *peer-id* が指定される場合、指定されたピア接続に関連するポリシーだけがリフレッシュされます。 すべてのピアポリシーを更新するには、ID を指定しないで [Enter] を押します。

	Command or Action	Purpose
		• SGT 番号が指定されている場合、その SGT に関連するポリシーだけがリフレッシュされます。 • すべての SGT ポリシーをリフレッシュするには、SGT 番号を指定せずに [Enter] を押します。 • デフォルトポリシーを更新するには、**default** を選択します。 • 不明ポリシーを更新するには、**unknown** を選択します。
Step 3	**exit** **Example:** `Device# exit`	特権 EXEC モードを終了します。

SGACL ポリシーのモニタリングと表示

コマンド	説明
show cts interface	インターフェイスでの静的SGT、MACsec暗号化、またはSGTインライン タギングに関連した CTS 設定のステータスを表示します。
show cts role-based counters [ipv4 | ipv6]	IPv4 および IPv6 イベントのすべての SGACL 適用の統計情報を表示します。
show cts role-based permissions	RBACL 設定に対する権限を表示します。

コマンド	説明
show cts role-based permissions from {*source-sgt* | unknown} to {*dest-sgt* | unknown}] [ipv4 | ipv6 | details]	SGACL ポリシーとペアごとのモニターモード機能に関する詳細を表示します。 *SGT-DGT* ペアに対してセルごとのモニターモードが有効になっている場合、コマンド出力が表示されます。 • キーワードを使用または省略して、許可マトリクスの全部または一部を表示できます。 • from キーワードを省略すると、権限マトリックスの列が表示されます。 • to キーワードを省略すると、権限マトリックスの行が表示されます。 • from および to キーワードを省略すると、権限マトリックス全体が表示されます。 • from および to キーワードが指定されている場合、権限マトリックスから 1 つのセルが表示され、details キーワードを使用できます。details が入力されると、1 つのセルの SGACL の ACE が表示されます。
show ip access-lists {*rbacls* | ipv4 *rbacls*}	すべての RBACL または指定された RBACL の ACE を表示します。
show cts role-based permissions default [ipv4 | ipv6 | details]	デフォルトポリシーの SGACL のリストを表示します。
show platform software fed [switch] [active | standby] sgacl port	インターフェイスでの Cisco TrustSec SGACL ポリシー適用のステータスを表示します。

セキュリティグループ ACL ポリシーの設定例

次のセクションでは、さまざまな SGACL ポリシーの設定例を示します。

例：SGACL ポリシー適用のグローバルな有効化

次に、 SGACL ポリシーの適用をグローバルに有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# cts role-based enforcement
```

例：インターフェイスごとの SGACL ポリシー適用の有効化

次に、インターフェイスごとに SGACL ポリシーの適用を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/2
Device(config-if)# cts role-based enforcement
Device(config-if)# end
```

例：VLAN に対する SGACL ポリシー適用の有効化

次に、VLAN 上で SGACL ポリシーの適用を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# cts role-based enforcement vlan-list 31-35,41
Device(config)# exit
```

例：SGACL モニターモードの設定

次に、SGACL モニターモードを設定する例を示します。

```
Device# configure terminal
Device(config)# cts role-based monitor enable
Device(config)# cts role-based permissions from 2 to 3 ipv4
Device# show cts role-based permissions from 2 to 3 ipv4

IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
        denytcpudpicmp-10
        Deny IP-00

Device# show cts role-based permissions from 2 to 3 ipv4 details

IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
        denytcpudpicmp-10
        Deny IP-00
Details:
Role-based IP access list denytcpudpicmp-10 (downloaded)
        10 deny tcp
        20 deny udp
        30 deny icmp
Role-based IP access list Permit IP-00 (downloaded)
        10 permit ip

Device# show cts role-based counters ipv4

Role-based IPv4 counters
From     To     SW-Denied  HW-Denied  SW-Permitt  HW_Permitt  SW-Monitor  HW-Monitor
*         *     0          0          8           18962       0           0
2         3     0          0          0           0           0           341057
```

例：SGACL ポリシーの手動設定

```
Device# configure terminal
Device(config)# ip access role allow_webtraff
```

```
Device(config-rb-acl)# 10 permit tcp dst eq 80
Device(config-rb-acl)# 20 permit tcp dst eq 443
Device(config-rb-acl)# 30 permit icmp
Device(config-rb-acl)# 40 deny ip
Device(config-rb-acl)# exit
Device(config)# cts role-based permissions from 55 to 66 allow_webtraff
Device# show ip access allow_webtraff

Role-based IP access list allow_webtraff
    10 permit tcp dst eq www
    20 permit tcp dst eq 443
    30 permit icmp
    40 deny ip
Device# show show cts role-based permissions from 50 to 70
```

例：SGACL の手動適用

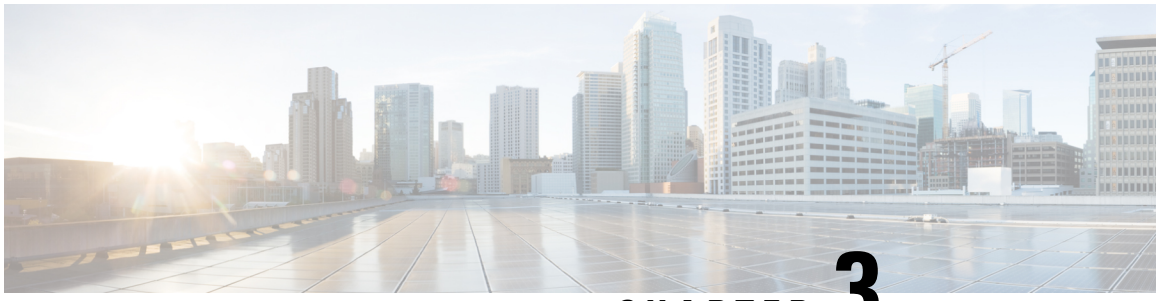
次に、SGACL ポリシーを手動で適用する例を示します。

```
Device# configure terminal
Device(config)# cts role-based permissions default MYDEFAULTSGACL
Device(config)# cts role-based permissions from 3 to 5 SRB3 SRB5
Device(config)# exit
```

例：SGACL ポリシーの表示

次に、セキュリティ グループ 3 から送信されたトラフィックの SGACL ポリシーの許可マトリクスの内容を表示する例を示します。

```
Device# show cts role-based permissions from 3

Role-based permissions from group 3 to group 5:
        SRB3
        SRB5
Role-based permissions from group 3 to group 7:
        SRB4
```



CHAPTER 3

SGT 交換プロトコル

SXP 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 26.1.1	SGT交換プロトコルの高可用性（HA）：SGT 交換プロトコルの高可用性（HA）サポートが導入されました。	Cisco C9350 シリーズ スマートスイッチ Cisco C9610 シリーズ スマートスイッチ
Cisco IOS XE 26.1.1	IPv6 を介した SGT 交換プロトコル：IPv6 を介した SGT 交換プロトコルのサポートが導入されました。	Cisco C9350 シリーズ スマートスイッチ Cisco C9610 シリーズ スマートスイッチ
Cisco IOS XE 17.18.1	SGT 交換プロトコル：SGT 交換プロトコル（SXP）を使用すると、シスコのグループベースポリシー（GBP）ハードウェアタギングをネイティブにサポートしないネットワークデバイス間でセキュリティグループタグを伝達できます。	Cisco C9350 シリーズ スマートスイッチ Cisco C9610 シリーズ スマートスイッチ

SGT 交換プロトコル

セキュリティグループタグ（SGT）交換プロトコルを使用すると、シスコ グループベース ポリシー（GBP）ハードウェアタギングのサポートがないネットワークデバイスにセキュリティグループ SGT を伝達できます。このプロトコルを使用すると、組織は、ハードウェアが直接サポートされていないデバイスも含めて、ネットワーク全体にセキュリティ グループ タギング機能を拡張できます。

IPv6 を介した SGT 交換プロトコル

IPv6 を介した SGT 交換プロトコルは、以下の特長を備えたセキュア トランスポート メカニズムです。

- SXP ピア間の通信に IPv6 アドレスを使用します。
- IPv6 インフラストラクチャでのセキュリティグループタグ（SGT）の伝達を容易にします。
- スピーカー、リスナー、またはその両方を含むさまざまなデバイスロールをサポートします。

SGT 交換プロトコルの高可用性（HA）

デバイスは、アクティブデバイスとスタンバイデバイス間の SXP データベースにおける、IP セキュリティグループタグ（SGT）バインディングのステートフルな同期に対する高可用性（HA）のサポートを提供します。

シスコ グループベース ポリシー

シスコ グループベース ポリシーでは、信頼できるデバイスで構成されるセキュアなネットワークドメインが作成されます。このドメインでは、各デバイスはそのピアによって認証されます。該当するドメイン内の通信は、暗号化、メッセージ整合性チェック、データパスリプレイ防止メカニズムを使用して保護されます。

ネットワーク内で SGT が使用される仕組み

デバイスまたはユーザーが認証されると、SXP（セキュリティグループタグ交換プロトコル）は、取得されたログイン情報を使用して、ネットワークに入ってくるパケットをセキュリティグループ（SG）に分類します。パケットは入ってくる時点でタグ付けされるため、パケットがデータパスを通過する際に、アクセス制御などのポリシー適用対象として識別できます。SGT によって、エンドポイントデバイスとネットワーク インフラストラクチャは、割り当てられたタグに基づいて通信をフィルタ処理および制御できます。さらに、静的ポート識別を使用して、特定のポートに接続されているエンドポイントの SGT 値を決定できます。

SGT 割り当てのメカニズム

SGT は、以下のさまざまなシナリオで、ポートレベルでパケットに割り当てることができます。

- 信頼できるポートでの SGT 付きパケット

  SGT タグ付きのパケットが信頼できるポートに到達すると、そのタグは送信元 SGT として受け入れられます。

- 信頼できないポートでの SGT 付きパケット

  タグ付けされたパケットが信頼できないポート経由で着信した場合、パケットは無視され、送信元 SGT はポートの設定に従って設定されます。

- SGT のないパケット

  パケットに SGT がない場合、送信元 SGT はポートで設定されたものとして設定されます。

SGT 割り当てメソッド

セキュリティグループタグは、次のようなさまざまなエンドポイントアドミッションコントロール（EAC）メソッドを使用して割り当てることができます。

- 802.1X ポートベースの認証
- MAC 認証バイパス（MAB）
- Web 認証

サポートされている SGT 割り当てメソッド

ネットワークで SGT を割り当てるには、次のメソッドがサポートされています。

- エンドポイント アドミッション コントロール（EAC）

  802.1X、MAB、および Web 認証が含まれます。

- VLAN から SGT へのマッピング

  IP デバイストラッキングによって VLAN 内で学習された IP アドレスに静的 SGT を割り当てます。これは優先順位の低い分類方法です。

- SXP リスナー

  SGT 交換プロトコルを使用して他のデバイスから SGT 情報を受信します。

- IP SGT

  IP アドレスに基づいて SGT を割り当てます。

- サブネット SGT

  IP サブネットに基づいて SGT を割り当てます。

- ポート SGT

  ポートレベルで SGT を割り当てます。

- SGT のキャッシング

  効率化のため、以前に割り当てられた SGT を保存して再利用します。

エンドポイント認証と SGT の関連付け

エンドポイント認証中に、アクセスデバイスは、DHCP スヌーピングや IP デバイストラッキングなどの方法を使用して、エンドポイントの IP アドレスを SGT に関連付けます。その後このバインディングは、SXP を介してハードウェア対応の出力デバイスに伝達され、送信元 IP から SGT へのバインディングのテーブルが保持されます。出力インターフェイスでは、これらのデバイス

はセキュリティ グループ アクセス コントロール リスト（SGACL）を使用してセキュリティポリシーを適用します。

セキュリティグループタグ伝達での SXP のロール

SXP は制御プロトコルとして機能し、認証ポイントからアップストリーム ネットワーク デバイスに、IP から SGT へのバインディング情報を伝達します。このプロセスにより、スイッチ、ルータ、ファイアウォールのセキュリティサービスは、アクセスデバイスからのアイデンティティ情報を確実に学習し利用することができます。SXP は、パケットタギング機能がないネットワークセグメントで特に重要です。

SXP プロトコルの詳細

SXP はトランスポートプロトコルとして TCP を使用します。具体的には、接続の開始に TCP ポート 64999 を使用します。SXP では、認証と完全性を目的として次の方式が採用されています。

- Message Digest 5（MD5）
- TCP 認証オプション（TCP-AO）

このプロトコルでは、次の 2 つの運用ロールが定義されています。

- スピーカー：接続を開始します。
- リスナー：接続を受信します。

SXP バージョン 5

SXP バージョン 5 を使用すると、Virtual Routing and Forwarding（VRF）を使用する環境での SGT 伝達の拡張性と柔軟性が向上します。以前のバージョンでは、VRF の数を増やすと、その分 SXP 接続と IP-SGT マッピングが増加します。SXP バージョン 5 では、単一の接続を使用して、指定された SXP ピア間での SXP マッピングのエクスポートおよびインポートを可能にすることで、この制約に対処します。

SXP バージョン 5 マッピング

SXP バージョン 5 マッピングは、以下のように動作します。

- マッピングのエクスポート：

  SXP スピーカー側では、SXP バージョン 5 は、バインディング送信元タイプまたは関連した VRF に基づいて、特定の IP-SGT バインディングをエクスポートできます。

- マッピングのインポート：

SXP リスナー側では、SXP バージョン 5 は、関連マッピングを指定された VRF にインポートします。

SXP 動作モード

設定に従って、リモートピアデバイスにエクスポートする VRF 関連 IP-SGT バインディングを指定できます。SXP バージョン 5 をサポートする 2 台のデバイス間で SXP 接続が確立されると、接続は SXP バージョン 5 モードで動作します。いずれかのデバイスが以前のバージョンのみをサポートしている場合、デフォルトの接続は、共通にサポートされる最も古いバージョンになります。

IP-SGT バインディングをピアデバイスにエクスポートする VRF または VRF テーブルのリストを制御するには、**cts sxp** グローバル設定コマンドを使用します。

SXP 設定のガイドライン

- Cisco SGT Exchange Protocol（SXP）ネットワークを確立する必要があります。このネットワークには次の前提条件があります。
  - 既存のデバイスでシスコ グループベース ポリシー機能を使用するには、シスコ グループベース ポリシー セキュリティ ライセンスを購入していることを確認します。デバイスを発注済みでシスコ グループベース ポリシー機能が必要な場合は、発送前に、このライセンスがデバイスにプリインストールされていることを確認します。
  - シスコ グループベース ポリシー機能。発送前に、このライセンスがデバイスにプリインストールされていることを確認します。
  - シスコのグループベースポリシー SXP ソフトウェアをすべてのネットワークデバイス上で実行すること。
  - すべてのネットワークデバイス間が接続されていること。
- シスコのグループベースポリシー 交換プロトコルは論理インターフェイスでサポートされておらず、物理インターフェイスだけでサポートされています。
- Dynamic Host Control Protocol（DHCP）スヌーピングが有効になっている場合、DHCP パケットに対するシスコ グループベース ポリシーの適用は、適用ポリシーによって渡されます。
- ピア接続設定が存在する場合、SXP グループのピアリストの変更はサポートされません。
- グループ内のいずれかのピアに SXP 接続設定がある場合、スピーカーまたはリスナーエクスポートインポート グループの下にあるエクスポートリストまたはインポートリストの変更は許可されません。エクスポート インポート グループの設定を変更するには、対応するピア SXP 接続の設定を削除する必要があります。また、**no cts sxp enable** コマンドを使用して SXP をシャットダウンすることもできます。

- 単一のピアを複数のエクスポートインポートグループの下に同じ方向に設定することはできません。つまり、ピアは、スピーカーエクスポートインポートグループとリスナー エクスポート インポート グループの一部になることはできますが、同時に 2 つ目のスピーカーグループまたはリスナーグループの一部になることはできません。
- グローバル エクスポート インポート グループ設定と、ピア エクスポート インポート グループごとの設定は、相互に排他的です。

IPv6 を介した SGT 交換プロトコルの制約事項

IPv6 を介した SGT 交換プロトコル（SXP）には、以下の制約事項があります。

- 送信元デバイスとピアデバイスを同じアドレスタイプ（IPv6）に設定します。デバイスは、IPv4 と IPv6 のアドレスタイプが混在する接続をサポートしていません。
- すべての SXP 設定でリテラル IPv6 アドレスを使用します。デバイスは SXP 接続で完全修飾ドメイン名（FQDN）をサポートしていません。
- 適切なデバイスが識別されるように、SXP ネットワーク内のノード ID として一意の 4 バイト IPv4 アドレスを使用します。

SXP の設定方法

以下のセクションでは、SXP の設定方法に関する情報を提供します。

デバイス SGT の手動設定

通常のシスコのグループベースポリシー操作では、認証サーバーがデバイスから発信されるパケット用に、そのデバイスに SGT を割り当てます。認証サーバーにアクセスできない場合は、使用する SGT を手動で設定できますが、認証サーバーから割り当てられた SGT のほうが、手動で割り当てた SGT よりも優先されます。

デバイスの SGT を手動で設定するには、次の作業を行います。

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 sgt** *tag*

Example:

```
Device(config)# cts sgt tag
```

デバイスから送信されるパケットの SGT を設定します。

tag：tag 引数は 10 進形式です。範囲は 1 ～ 65533 です。

Step 4 **exit**

Example:

```
Device(config)# exit
```

設定モードを終了します。

SXP ピア接続の設定

両方のデバイスで SXP ピア接続を設定する必要があります。一方のデバイスがスピーカーであり、もう一方のデバイスがリスナーです。または、両方のデバイスでスピーカーとリスナーの両方を設定することもできます。パスワード保護を使用している場合は、必ず両エンドに同じパスワードを使用してください。

Note デフォルトの SXP 送信元 IP アドレスが設定されておらず、かつ接続の SXP 送信元アドレスが指定されていない場合、シスコのグループベース ポリシー ソフトウェアは既存のローカル IP アドレスから SXP 送信元 IP アドレスを抽出します。SXP 送信元アドレスは、デバイスから開始される各 TCP 接続ごとに異なる場合があります。

SXP ピア接続を設定するには、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 sxp connection peer** *peer-ipv4-addr* [**source** *src-ipv4-addr*] **password** {**default** | **none**} **mode** {**local** | **peer**} {**speaker** | **listener**} {**vrf** *vrf-name*}

Example:

```
Device(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

SXP アドレス接続を設定します。

オプションの **source** キーワードには発信元デバイスの IPv4 アドレスを指定します。アドレスが指定されていない場合、接続は、デフォルトの送信元アドレス（設定されている場合）、またはポートのアドレスを使用します。

password キーワードには、SXP で接続に使用するパスワードを指定します。次のオプションがあります。

- **default**：**cts sxp default password** コマンドを使用して設定したデフォルトの SXP パスワードを使用します。
- **none**：パスワードを使用しません。

mode キーワードでは、リモートピアデバイスのロールを指定します。

- **local**：指定したモードでは、ローカルデバイスを参照します。
- **peer**：指定したモードでは、ピアデバイスを参照します。
- **speaker**：デフォルト。このデバイスが接続の際にスピーカーになります。
- **listener**：このデバイスが接続の際にリスナーになります。

オプションの **vrf** キーワードでは、ピアに対する VRF を指定します。デフォルトはデフォルト VRF です。

Step 4 **exit**

Example:

```
Device(config)# exit
```

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。

Step 5 **show cts sxp connections**

Example:

```
Device# show cts sxp connections
```

（任意）SXP 接続情報を表示します。

デフォルトの SXP パスワードの設定

デフォルトでは、SXP は接続のセットアップ時にパスワードを使用しません。

デフォルト SXP パスワードを設定するには、次の作業を行います。

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 sxp default password** [**0** | **6** | **7**] *passeword*

Example:

```
Device(config)# cts sxp default password 0 hello
```

SXP のデフォルト パスワードを設定します。

以下を入力できます。

- クリアテキストのパスワード（**0** を使用するか、オプションなしで指定）
- 暗号化されたパスワード（**6** または **7** オプションを使用）

パスワードの最大長は 32 文字です。

Step 4 **exit**

Example:

```
Device(config)# exit
```

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。

デフォルトの SXP 送信元 IP アドレスの設定

SXP は送信元 IP アドレスが指定されないと、新規の TCP 接続すべてにデフォルトの送信元 IP アドレスを使用します。デフォルト SXP 送信元 IP アドレスを設定しても、既存の TCP 接続には影響しません。

デフォルト SXP 送信元 IP アドレスを設定するには、次の作業を行います。

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 sxp default source-ip** *src-ip-addr*

Example:

```
Device(config)# cts sxp default source-ip 10.0.1.2
```

SXP のデフォルトの送信元 IP アドレスを設定します。

Step 4 **exit**

Example:

```
Device(config)# exit
```

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。

SXP 復帰期間の変更

ピアが SXP 接続を終了すると、内部ホールドダウン タイマーが開始されます。内部ホールドダウン タイマーが終了する前にピアが再接続すると、SXP 復帰期間タイマーが開始されます。SXP 復帰期間タイマーがアクティブな間、シスコのグループベース ポリシー ソフトウェアは前回の接続で学習した SGT マッピング エントリを保持し、無効なエントリを削除します。

SXP 復帰期間を 0 秒に設定すると、タイマーがディセーブルになり、前回の接続のすべてのエントリが削除されます。

SXP の復帰期間を変更するには、次の作業を行います。

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 sxp reconciliation period** *seconds*

Example:

```
Device(config)# cts sxp reconciliation period 360
```

SXP 復帰タイマーを変更します。

seconds：値の範囲は 0 ～ 64000 です。デフォルト値は 120 秒（2 分）です。

Step 4 **exit**

Example:

```
Device(config)# exit
```

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。

SXP 再試行期間の変更

SXP リトライ期間によって、シスコのグループベース ポリシー ソフトウェアが SXP 接続を再試行する頻度が決まります。SXP 接続が正常に確立されなかった場合、Cisco グループベース ポリシー ソフトウェアは SXP リトライ期間タイマーの終了後に、新たな接続の確立を試行します。SXP 再試行期間を 0 秒に設定するとタイマーは無効になり、接続は再試行されません。

SXP のリトライ期間を変更するには、次の作業を行います。

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 sxp retry period** *vlan-list*

Example:

```
Device(config)# cts sxp retry period 360
```

SXP リトライ タイマーを変更します。

seconds：値の範囲は 0 ～ 64000 です。デフォルト値は 120 秒（2 分）です。

Step 4 **exit**

Example:

```
Device(config)# exit
```

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。

SXP で学習された IP アドレスから SGT へのマッピングの変更をキャプチャするための syslog の作成

グローバル コンフィギュレーション モードで **cts sxp log binding-changes** コマンドを設定すると、IP アドレスから SGT へのバインディングの変更（追加、削除、変更）が発生するたびに SXP の syslog（sev 5 syslog）が生成されます。

これらの変更は SXP 接続で学習されて伝播されます。デフォルトは **no cts sxp log binding-changes** です。

バインディングの変更のロギングをイネーブルにするには、次の作業を実行します。

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 sxp log binding-changes**

Example:

```
Device(config)# cts sxp log binding-changes
```

IP と SGT のバインドの変更のロギングを有効にします。

Step 4 **exit**

Example:

```
Device(config)# exit
```

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。

SXP エクスポートリストの設定

SXP エクスポートリストを設定するには、このタスクを実行します。

Note エクスポートリストの設定は、SXP グループに関連付けられている場合は削除できません。削除するには、まず SXP 接続を無効化する必要があります。

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 sxp export-list** *export_list_name*

Example:

```
Device(config)# cts sxp export-list export_list_1
```

SXP エクスポートリストを設定し、エクスポートリスト設定モードを開始します。

Step 4 **binding-source-type** {**all** | **caching** | **cli** | **l3if** | **lisp-local-host** | **lisp-remote-host** | **local** | **omp** | **vlan**}

Example:

```
Device(config-export-list)# binding-source-type all
```

（任意）ピアにエクスポートする、対応する送信元タイプのバインディングを設定します。

- **all**：すべてのバインディングをエクスポートします。
- **caching**：キャッシュされているバインディングをピアにエクスポートします。
- **cli**：CLI バインディングをピアにエクスポートします。
- **l3if**：L3IF バインディングをピアにエクスポートします。
- **lisp-local-host**：LISP ローカルバインディングをピアにエクスポートします。
- **lisp-remote-host**：LISP リモートバインディングをピアにエクスポートします。
- **local**：ローカルバインディングをピアにエクスポートします。
- **omp**：OMP バインディングをピアにエクスポートします。
- **vlan**：VLAN バインディングをピアにエクスポートします。

Step 5 **vrf** {*instance_name* | **Default-vrf** | **all**}

Example:

```
Device(config-export-list)# vrf all
```

（任意）バインディングをインポートするために使用される VRF を設定します。

- *instance_name*：VPN ルーティングおよび転送インスタンス名を指定します。
- **Default-vrf**：デフォルトの VRF バインディングをエクスポートします。
- **all**：すべての IP-SGT バインディングをエクスポートします。

Note
vrf と **vrf** *instance_name* 設定は相互に排他的です。

Step 6 **end**

Example:

```
Device(config-export-list)# end
```

エクスポートリスト設定モードを終了し、特権 EXEC モードに戻ります。

SXP インポートリストの設定

SXP インポートリストを設定するには、次の作業を行います。

Note インポートリスト設定は、SXP グループに関連付けられている場合は削除できません。インポートリスト設定を削除するには、まず対応する SXP 接続を無効化する必要があります。

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 sxp import-list** *import_list_name*

Example:

```
Device(config)# cts sxp import-list import_list_1
```

SXP インポートリストを設定し、インポートリスト設定モードを開始します。

Step 4 **vlan-list**

Example:

```
Device(config-import-list)# vlan-list
```

（任意）受信したバインディング更新の VLAN に基づいて、インポート VRF を設定します。

Note
更新で受信した VLAN に対する VRF マッピングがデバイスにない場合、受信したバインディングはデフォルトの VRF テーブルに追加されます。

Step 5 **vrf** {*instance_name* | **Default-vrf**}}

Example:

```
Device(config-import-list)# vrf vrf_1
```

（任意）バインディングをインポートするために使用される VRF を設定します。

- *instance_name*：VPN ルーティングおよび転送インスタンス名を指定します。
- **Default-vrf**：デフォルトの VPN ルーティングおよび転送インスタンスを設定します。

Note

vrf *instance_name* と **vlan-list** の設定は相互に排他的です。

Step 6 **end**

Example:

```
Device(config-import-list)# end
```

エクスポートリスト設定モードを終了し、特権 EXEC モードに戻ります。

SXP エクスポート インポート グループの設定

エクスポート インポート グループは、グループの SXP バインディングのエクスポートまたはインポートを制御するスピーカーグループまたはリスナーグループとして定義されます。

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 sxp export-import-group** {**listener** | **speaker**} {**global** | *list_name*}

Example:

```
Device(config)# cts sxp export-import-group listener group_1
```

SXP エクスポート インポート グループを設定し、エクスポート インポート グループ コンフィギュレーション モードを開始します。

- **global**：SXP リスナー グローバル インポートグループまたは SXP スピーカー グローバル エクスポートグループのいずれかを設定します。グローバルスピーカーまたはリスナー エクスポート インポート グループは、デバイスで設定されているすべての SXP 接続に適用されます。
- *list_name*：デフォルトの VPN ルーティングおよび転送インスタンス名を指定します。

Step 4 **import-list** *list_name*

Example:

```
Device(config-export-import-group)# import-list import_1
```

（任意）エクスポート/インポートグループに適用されるインポートリスト名を指定します。

空のインポートリストまたはエクスポートリストは、それぞれリスナーまたはスピーカーのエクスポート インポート グループにアタッチできません。

Step 5 **export-list** *list_name*

Example:

```
Device(config-export-import-group)# export-list export_1
```

（オプション）エクスポート インポート グループに適用するエクスポートリスト名を指定します。

空のインポートリストまたはエクスポートリストは、それぞれリスナーまたはスピーカーのエクスポート インポート グループにアタッチできません。

Step 6 **peer** *address_name*

Example:

```
Device(config-export-import-group)# peer 1.1.1.1 2.2.2.2
```

（任意）エクスポート/インポート グループに適用されるピアのリストを設定します。最大 8 つのピアを設定できます。

Step 7 **end**

Example:

```
Device(config-export-import-group)# end
```

エクスポート インポート グループ設定モードを終了し、特権 EXEC モードに戻ります。

IPv6 を介した SGT 交換プロトコルの設定

IPv6 アドレッシングを使用してピア間で SGT 交換プロトコル（SXP）接続を確立し、セキュリティグループタグ（SGT）を伝達するには、次の手順を使用します。

TrustSec インフラストラクチャでは、IPv6 トランスポート層を介して通信する SXP ピアが必要な場合があります。この設定は、SGT から IP へのマッピングを交換する必要がある IPv6 専用またはデュアルスタック環境のデバイスに必要です。

Before you begin

- IPv6 ユニキャストルーティングをデバイスで有効にします。
- ピアデバイスが IPv6 ネットワークを介して到達可能であることを確認します。

Procedure

Step 1 SXP 接続用のデフォルトの送信元 IP アドレスを設定します。

Example:

```
Switch(config)#cts sxp default source-ipv6 2001:db8:1:1::1
```

この手順では、デバイスが SXP ピアに対して自身を識別するために使用するプライマリ IPv6 アドレスを確立します。このアドレスは、デバイスによって開始されたすべての SXP セッションのデフォルトのローカル識別子として機能します。

Step 2 特定のピアへの SXP 接続を設定します。

Example:

```
Switch(config)#cts sxp connection peer 2001:db8:2:2::2 password default mode local both
```

この手順では、トランスポート層接続を開始し、SXP 交換でのデバイスのロールを定義します。このコマンドは、ピアの IPv6 アドレス、スピーカー、リスナー、またはその両方などの接続モード、およびパスワードや VRF インスタンスなどのセキュリティパラメータを定義します。

Step 3 一意の 4 バイトの IPv4 アドレスを使用して、SXP ノード識別子を設定します。

Example:

```
Switch(config)#cts sxp node-id ipv4 192.168.0.1
```

この手順により、TrustSec ドメイン内のデバイスに一意のアイデンティティが付与されます。適切なデバイスが識別されるように、ノード ID は、SXP ネットワーク内の一意の 4 バイト IPv4 アドレスである必要があります。

Step 4 SXP エクスポート インポート グループを作成します。

Example:

```
Switch(config)#cts sxp export-import-group GROUP_V6
```

この手順では、複数のピアにまたがるマッピングポリシーを管理するための論理コンテナを作成します。エクスポート インポート グループは、ピアのセットに関する SGT から IP へのマッピングの伝達を管理および分類するために使用されます。

Step 5 エクスポート インポート グループにピア IPv6 アドレスを割り当てます。

Example:

```
Switch(config-sxp-cluster)#peer 2001:db8:2:2::2
```

この手順には、グループのマッピング交換プロセスで指定されたピアが含まれます。この関連付けにより、特定のピアが、グループに対して定義されているエクスポートおよびインポートのルールに従うようになります。

デバイスは設定された IPv6 ピアと SXP セッションを確立し、SGT から IP へのマッピングが IPv6 トランスポートでの伝達を開始します。

SGT 交換プロトコル接続の確認

Table 1:

コマンド	説明
show cts sxp connections	SXP ステータスと接続に関する詳細情報を表示します。
show cts sxp connections [brief]	SXP ステータスと接続に関する要約情報を表示します。
show cts sxp export-list	特定のエクスポートリスト名またはすべてのエクスポートリストに関連付けられている VRF のリストを表示します。
show cts sxp import-list	特定のインポートリスト名またはすべてのインポートリストに関連付けられている VRF のリストを表示します。
show cts sxp export-import-group [detailed]	特定のエクスポート/インポートグループに適用されるエクスポートリストまたはインポートリストと、このエクスポート/インポートグループの一部であるピアのリストを表示します。

SXP の設定例

以下のセクションでは、SXP の設定例を紹介します。

例：シスコ グループベース ポリシー SXP および SXP ピア接続の有効化

以下に、SXP を有効にし、デバイス A（スピーカー）とデバイス B（リスナー）間に SXP ピア接続を設定する方法の例を示します。

```
Device# configure terminal
Device(config)# cts sxp enable
Device(config)# cts sxp default password Cisco123
Device(config)# cts sxp default source-ip 10.10.1.1
Device(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

以下に、デバイス B（リスナー）とデバイス A（スピーカー）間に SXP ピア接続を設定する方法の例を示します。

```
Device# configure terminal
Device(config)# cts sxp enable
Device(config)# cts sxp default password Cisco123
Device(config)# cts sxp default source-ip 10.20.2.2
Device(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

例：デフォルトの SXP パスワードと送信元 IP アドレスの設定

次に、デフォルトの SXP パスワードとの送信元 IP アドレスを設定する例を示します。

```
Device# configure terminal
Device(config)# cts sxp default password Cisco123
Device(config)# cts sxp default source-ip 10.20.2.2
Device(config)# end
```

例：SGT 交換プロトコル接続の確認

次に、**show cts sxp connections** コマンドの出力例を示します。

```
Device# show cts sxp connections

SXP                   : Enabled
Default Password      : Set
Default Source IP     : 10.10.1.1
Connection retry open period: 10 secs
Reconcile period      : 120 secs
Retry open timer is not running
------------------------------------------
Peer IP               : 10.20.2.2
Source IP             : 10.10.1.1
Conn status           : On
Conn Version          : 2
Connection mode       : SXP Listener
Connection inst#      : 1
TCP conn fd           : 1
TCP conn password     : default SXP password
Duration since last state change: 0:00:21:25 (dd:hr:mm:sec)
Total num of SXP Connections = 1
```

次に、**show cts sxp connections brief** コマンドの出力例を示します。

```
Device# show cts sxp connections brief

SXP                   : Enabled
Default Password      : Set
Default Source IP     : Not Set
Connection retry open period: 120 secs
Reconcile period      : 120 secs
Retry open timer is not running
```

```
------------------------------------------------------------------------------
Peer_IP          Source_IP          Conn Status    Duration
------------------------------------------------------------------------------
10.1.3.1         10.1.3.2           On             6:00:09:13 (dd:hr:mm:sec)
Total num of SXP Connections = 1
```

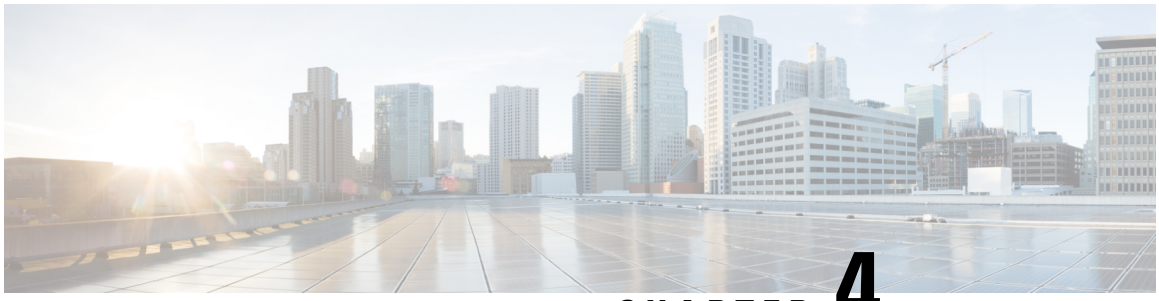
次に、特定のエクスポートリストまたはデバイスで設定されているすべてのエクスポートリストに関連付けられた VRF のリストを表示する **show cts sxp export-list** コマンドのサンプル出力を示します。

```
Device# show cts sxp export-list export_list_1

   Export-list-name: export_list_1
   vrf red_vrf
   vrf blue_vrf

Device# show cts sxp export-list

   Export-list-name: export_list_1
       vrf red_vrf
       vrf blue_vrf
       vrf green_vrf
   Export-list-name: export_list_2
       vrf all
```

特定のエクスポート/インポートグループに適用されるエクスポートリストまたはインポートリストと、このエクスポート/インポートグループの一部であるピアのリストを表示します。**show cts sxp export-import-groupshow cts sxp export-import-group** コマンドは、デバイスに設定されているすべてのエクスポートおよびインポート グループの詳細も一覧表示します。**detailed** キーワードを使用して、エクスポートリストまたはインポートリストの内容を、エクスポートリストまたはインポートリスト名、ピアのリストとともに表示します。**global** キーワードは、グローバルなリスナーとスピーカーの詳細のみを表示します。

```
Device# show cts sxp export-import-group speaker group_1

   Export-import-group: group_1
   Export-list-name: export_list_1
   Peer-list: 1.1.1.1, 2.2.2.2, 3.3.3.3

Device# show cts sxp export-import-group listener

Global Listener export-import-group: Not configured

   Export-import-group: group_1
   Export-list-name:  export_list_1
   Peer-list: 1.1.1.1, 2.2.2.2, 3.3.3.3

   Export-import-group: group_2
   Import-list-name: import_list_1
   Peer-list: 4.4.4.4, 5.5.5.5, 6.6.6.6


Device# show cts sxp export-import-group speaker group_1 detailed

    Export-import-group: group_1
    Export-list-name: export_list_1
    Export-list-content:
       vrf Red_vrf
       vrf Blue_vrf
    Peer-list: 1.1.1.1, 2.2.2.2, 3.3.3.3
```

```
Device# show cts sxp export-import-group listener detailed

    Global Listener export-import-group: Not configured

    Export-import-group: group_1
    Import-list-name: import_list_1
    Import-list-content:
       vlan-list
    Peer-list: 1.1.1.1, 2.2.2.2, 3.3.3.3

Device# show cts sxp export-import-group global

   Global Listener export-import-list Name: group_1
   Global Speaker export-import-list Name: group_2
```



CHAPTER 4

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

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

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

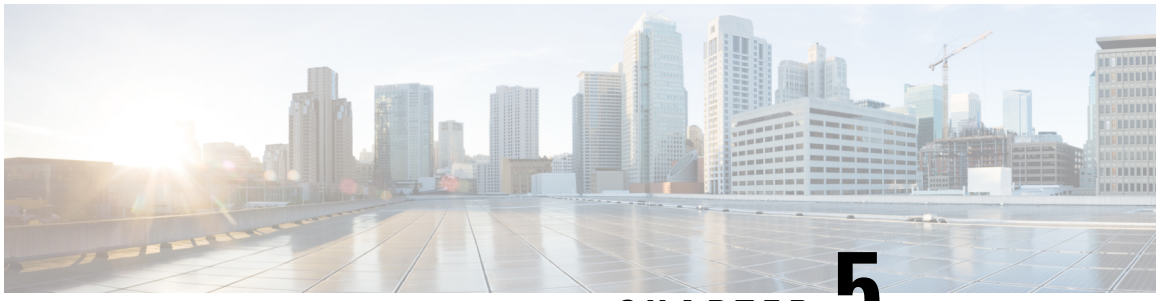
以下の例では、IBNS バージョン 2.0 を使用します。

```
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
```



CHAPTER 5

TrustSec セキュリティグループ名のダウンロード

TrustSec セキュリティグループ名のダウンロード機能の履歴

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	TrustSec セキュリティグループ名のダウンロード： TrustSec セキュリティグループ名ダウンロード機能は、ネットワーク アクセス デバイスが、SGT 番号と SGACL ポリシーだけでなく、関連する SGT 名も受信できるようにすることで、SGT ポリシーを強化します。	Cisco C9610 シリーズ スマートスイッチ

TrustSec セキュリティグループ名のダウンロード

TrustSec セキュリティグループ名のダウンロード

TrustSec セキュリティグループ名ダウンロード機能は、ネットワーク アクセス デバイスが、SGT 番号とセキュリティ グループ アクセス コントロール リスト（SGACL）ポリシーだけでなく、関連する SGT 名も受信できるようにすることで、セキュリティグループタグ（SGT）ポリシーを強化します。

レイヤ 3 論理インターフェイスへの SGT のマッピング

この機能により、基盤となる物理インターフェイスに関係なく、次のレイヤ 3 インターフェイスのいずれかの通信に SGT を直接マッピングできます。

- ルーテッド ポート
- スイッチ仮想インターフェイス（SVI または VLAN インターフェイス）
- レイヤ 2 ポートのレイヤ 3 サブインターフェイス
- トンネル インターフェイス

cts role-based sgt-map interface グローバル設定コマンドを使用すると、特定の SGT 番号またはセキュリティグループ名を指定できます。セキュリティグループ名とその SGT の関連付けは、Cisco Identity Services Engine（ISE）または Cisco Access Control Server（ACS）から動的に取得されます。

TrustSec セキュリティグループ名のダウンロードの設定

TrustSec セキュリティグループ名のダウンロードを設定するには、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 interface** *type slot/port* [**security-group** *name* | **sgt** *number*]

Example:

```
Device(config)# cts role-based sgt-map interface gigabitEthernet 1/1 sgt 77
```

SGT は指定されたインターフェイスへの入力トラフィックに適用されます。

- **interface** *type slot/port*：使用可能なインターフェイスのリストを表示します。
- **security-group** *name*：セキュリティグループ名から SGT へのペアリングは Cisco ISE または Cisco ACS で設定されます。
- **sgt** *number*：SGT 番号を指定します。範囲は 0 ～ 65,535 です。

Step 4 **exit**

Example:

```
Device(config)# exit
```

グローバル コンフィギュレーション モードを終了します。

Step 5 **show cts role-based sgt-map all**

Example:

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

入力トラフィックに指定された SGT がタグ付けされたことを確認します。

例：TrustSec セキュリティグループ名のダウンロードの設定

次の例は、入力インターフェイスへの SGT のダウンロード設定を示します。

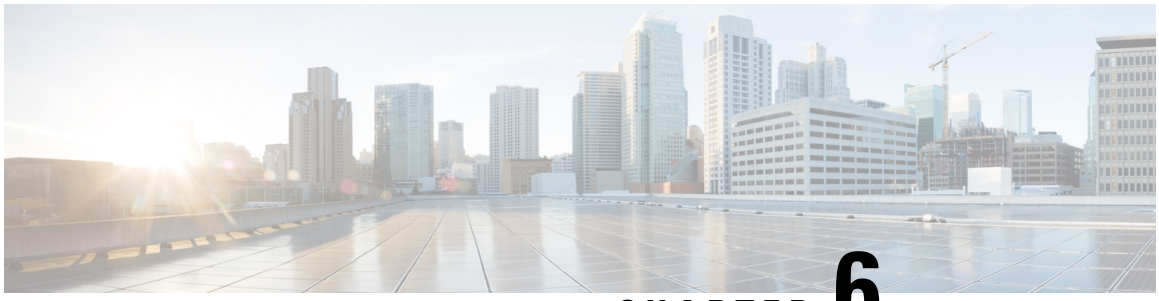
```
Device# config terminal
Device(config)# cts role-based sgt-map interface gigabitEthernet 6/3 sgt 3
Device (config)# exit
```

例：TrustSec セキュリティグループ名ダウンロード設定の確認

次の例は、**show cts role-based sgt-map all** コマンドのサンプル出力を示しています。

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

IP Address              SGT     Source

========================================
```

```
15.1.1.15               4       INTERNAL

17.1.1.0/24             3       L3IF

21.1.1.2                4       INTERNAL

31.1.1.0/24             3       L3IF

31.1.1.2                4       INTERNAL

43.1.1.0/24             3       L3IF

49.1.1.0/24             3       L3IF

50.1.1.0/24             3       L3IF

50.1.1.2                4       INTERNAL

51.1.1.1                4       INTERNAL

52.1.1.0/24             3       L3IF

81.1.1.1                5       CLI

102.1.1.1               4       INTERNAL

105.1.1.1               3       L3IF

111.1.1.1               4       INTERNAL

IP-SGT Active Bindings Summary

============================================

Total number of CLI      bindings = 1

Total number of L3IF     bindings = 7

Total number of INTERNAL bindings = 7

Total number of active   bindings = 15
```



CHAPTER 6

レイヤ 2 SGT インポジションと転送

レイヤ 2 SGT インポジションと転送の機能履歴

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	レイヤ2SGTインポジションと転送： レイヤ2SGTインポジションと転送を使用すると、スイッチ上のインターフェイスを Cisco TrustSec 用に手動で設定することが可能になり、スイッチが SGT をネットワークパケットに挿入できるようになります。	Cisco C9610 シリーズ スマートスイッチ

レイヤ 2 SGT インポジションと転送

レイヤ 2 SGT インポジションと転送機能を使用すると、スイッチ上のインターフェイスを Cisco TrustSec 用に手動で設定することが可能になり、スイッチが SGT をネットワークパケットに挿入できるようになります。SGT は Cisco TrustSec ヘッダーでネットワーク全体に伝送されるため、

インフラストラクチャ全体での一貫したセキュリティ グループ ポリシーの適用が可能になります。

レイヤ 2 SGT インポジションと転送を設定するためのガイドライン

L2 SGT インポジションと転送の機能を導入する前に、次の前提条件で Cisco TrustSec ネットワークを確立する必要があります。

- すべてのネットワーク デバイス間が接続されていること。
- Cisco Secure Access Control System（ACS）5.1 が、Cisco Trustsec -SXP ライセンスで動作していること
- ディレクトリ、DHCP、DNS、認証局、および NTP サーバーがネットワーク内で機能すること。
- ルータごとに、それぞれ異なる retry open timer コマンドの値を設定してください。

SGT 処理の設定方法：L2 SGT インポジションと転送

以下のセクションでは、SGT 処理：L2 SGT インポジションと転送に関する設定情報を提供します。

インターフェイスでのレイヤ 2 SGT のインポジションと転送の有効化

次のタスクを実行して、Cisco TrustSec のデバイス上のインターフェイスを手動で有効化します。これによりデバイスは、ネットワーク全体で伝達するパケットに SGT を追加し、静的認証ポリシーを導入できます。

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 **interface** {**GigabitEthernet** *port* | **Vlan** *number*}

Example:

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

CTS SGT の認証と転送が有効なインターフェイスを開始します。

Step 4 **cts manual**

Example:

```
Device(config-if)# cts manual
```

CTS SGT 認証と転送のインターフェイスを有効化し、CTS 手動インターフェイス コンフィギュレーション モードを開始します。

Step 5 **policy static sgt** *tag* [**trusted**]

Example:

```
Device(config-if-cts-manual)# policy static sgt 100 trusted
```

SGT の信頼性を定義するタグ付きパケットを使用して、CTS セキュリティ グループのスタティック認証ポリシーを設定します。

Step 6 **end**

Example:

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

CTS 手動インターフェイス構成モードを終了し、特権 EXEC モードを開始します。

Step 7 **show cts interface** [**GigabitEthernet** *port* | **Vlan** *number* | **brief** | **summary**]

Example:

```
Device# show cts interface brief
```

インターフェイスの CTS 設定の統計情報を表示します。

インターフェイスでの CTS SGT 伝達の無効化

ピアデバイスが SGT を受信できない場合、次の手順を実行して、インスタンス内のインターフェイスで CTS SGT 伝達を無効化します。

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 **interface** {**GigabitEthernet** *port* | **Vlan** *number*}

Example:

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

CTS SGT の認証と転送が有効なインターフェイスを開始します。

Step 4 **cts manual**

Example:

```
Device(config-if)# cts manual
```

CTS SGT の承認と転送用のインターフェイスを有効化します。

CTS 手動インターフェイス コンフィギュレーション モードは、CTS パラメーターを設定できる場合に開始されます。

Step 5 **no propagate sgt**

Example:

```
Device(config-if-cts-manual)# no propagate sgt
```

ピア デバイスが SGT を受信できない状況では、インターフェイスの CTS SGT 伝達を無効化します。

Note
CTS SGT 伝達はデフォルトで有効化されています。ピアデバイスで CTS SGT 伝達を再度オンにする必要がある場合、**propagate sgt** コマンドを使用できます。

no propagate sgt コマンドが入力されると、SGT タグは L2 ヘッダーに追加されなくなります。

Step 6 **end**

Example:

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

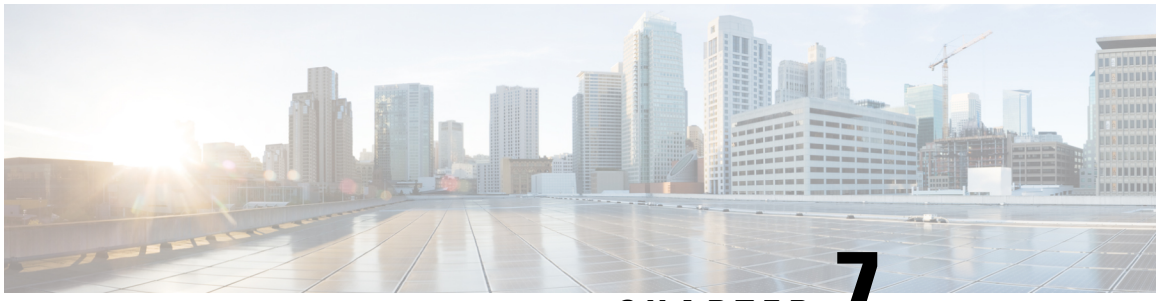
CTS 手動インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

Step 7 **show cts interface** [**GigabitEthernet** *port* | **Vlan** *number* | **brief** | **summary**]

Example:

```
Device# show cts interface brief
```

インターフェイスでCTS SGT 伝達が無効化されていることを確認するため、CTS 設定の統計情報を表示します。



CHAPTER 7

SGT インライン タギング

SGT インラインタギングの機能の履歴

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 26.1.1	SGT インライン タギング機能が Cisco C9610 シリーズ スマートスイッチでも使用できるようになりました。	Cisco C9610 シリーズ スマートスイッチ

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 インライン タギング： SGT インライン タギングにより、Cisco TrustSec はセキュリティグループのアイデンティティ情報をイーサネットフレーム内で直接伝達できます。これにより、ネットワークデバイスは、送信元のセキュリティ グループ メンバーシップに基づいてセキュリティポリシーを効率的に適用できます。	Cisco C9350 シリーズ スマート スイッチ

レイヤ 2 SGT インポジション

Cisco TrustSec 対応デバイスは、MAC（レイヤ 2）レベルで組み込まれた SGT を持つパケットを送受信するためのハードウェアサポートを提供します。レイヤ 2（L2）SGT インポジションと呼ばれるこの機能により、イーサネットインターフェイスはSGTをパケットに直接挿入できます。挿入後、パケットは隣接するイーサネットデバイスに転送されます。SGT-over-Ethernet メソッドでは、ホップバイホップでの SGT のクリアテキスト伝達が可能で、コントロール プレーン オーバーヘッドを追加することなく、拡張可能で効率的なアイデンティティのタギングが実現します。

SXPv4 での SGT の処理

SGT 交換プロトコルバージョン4（SXPv4）を備えた Cisco TrustSec ソリューションは、メタデータベースの L2-SGT をサポートします。パケットが TrustSec 対応インターフェイスに入ると、デバイスは、SXP を介して動的に、または設定によって静的に構築された IP-SGT マッピングデータベースを参照して、送信元 IP アドレスに基づいて正しい SGT を決定します。その後この SGT はパケットに挿入され、TrustSec ドメイン全体に配信されます。

SGACL を使用した SGT の処理

ネットワークの出力エッジで、パケットの接続先のグループが決定され、アクセス制御を適用できます。セキュリティ グループ アクセス コントロール リスト（SGACL）は、異なるセキュリティグループ間の通信を許可または制限するかどうかを定義します。各パケットのポリシー適用は、送信元と宛先のセキュリティグループタグによって決まります。

SGT の伝達とユースケース

- 信頼できるインターフェイスの伝達：信頼できるインターフェイスから受信された SGT は、ネットワーク全体に伝達され、アイデンティティベースのファイアウォールの分類に使用できます。
- IPSec の統合：IPSec を使用する場合、適切な SGT タギングのために、パケットで受信された SGT を IPSec と共有できます。

パケットの SGT の決定

Cisco TrustSec ドメインの入力側にあるデバイスがパケットを受信する際、適切な SGT を決定してパケットにタグ付けする必要があります。この操作は、主に次の 2 つの方法で実行できます。

- TrustSec ヘッダーの SGT フィールド：

  パケットが信頼できるピアデバイスから到着した場合、Cisco TrustSec ヘッダーの SGT フィールドは正確であると見なされます。

- 送信元 IP による SGT ルックアップ：

  管理者は、手動でポリシーを設定するか、または SXP プロトコルを利用して IP から SGT へのマッピングテーブルを取り込み、送信元 IP アドレスに基づいて SGT を割り当てることができます。

NAT 対応デバイスでの SGT インライン タギング

このセクションでは、入力ポートと出力ポートの両方でネットワークアドレス変換（NAT）が有効化されているプライマリデバイスからセカンダリデバイスに流れるパケットの SGT 値の決定方法と適用方法について説明します。

Note フローに含まれるすべてのポートは、両方のデバイスで Cisco TrustSec（CTS）の手動および信頼できるモードを設定している必要があります。

インライン タギングが有効で、CLI を介して SGT タグが変更されていない

- プライマリデバイスでは、Cisco TrustSec はパケットの最初の送信元 IP に対応する SGT タグを適用します。
- NAT 変換後、NAT IP は同じ SGT タグに関連付けられます。
- セカンダリデバイスでは、Cisco TrustSec は送信元 IP（SGT タグで表される）に基づいて SGT タグを適用します。

例

送信元 IP 192.0.2.5 および SGT タグ 133 を指定されたパケットがプライマリデバイスに到達したとします。

- Cisco TrustSec は、プライマリデバイスで SGT タグ 133 を適用します。
- NAT 後、パケットの IP は 198.51.100.10 に変更されます。ただし、SGT タグ 133 でタグ付けされたままになります。
- セカンダリデバイスは、IP 198.51.100.10 および SGT 133 のパケットを受信し、SGT 133 に基づいて TrustSec ポリシーを適用します。

インラインタギングが有効で、CLI を介して SGT タグが変更された

- プライマリデバイスでは、Cisco TrustSec はパケットの最初の送信元 IP に基づいて SGT タグを適用します。
- SGT タグは CLI を介して変更できますが、NAT IP は最初の送信元 IP の SGT でタグ付けされたままになります。
- セカンダリデバイスでは、TrustSec はパケットの最初の送信元 IP に対応する SGT タグに従ってポリシーを適用します。

例

送信元 IP 192.0.2.5 および SGT タグ 133 を指定されたパケットがプライマリデバイスに到達したとします。

- SGT タグは CLI を介して 200 に変更されますが、NAT 後（IP は 198.51.100.10 に変更）、パケットは SGT 133 でタグ付けされたままになります。
- セカンダリデバイスは、IP 198.51.100.10 および SGT 133 のパケットを受信し、SGT 133 に基づいて TrustSec ポリシーを適用します。

インライン タギングが無効で、SGT は SXP プロトコル経由で学習され、CLI を介して変更された

- プライマリデバイスでは、TrustSec は最初の送信元 IP に基づいて SGT タグを適用します。
- NAT 後の IP の SGT は、CLI を介して定義され、プライマリデバイスで学習されます。
- セカンダリデバイスでは、ダイレクト TrustSec リンクがない場合、IP から SGT へのバインディングは SXP プロトコルを介して学習され、TrustSec は NAT IP に関連付けられた SGT に基づいて適用されます。

例

送信元 IP 192.0.2.5 および SGT タグ 133 を指定されたパケットがプライマリデバイスに到達したとします。

- NAT 後、送信元 IP は 198.51.100.10 になり、この IP の SGT は CLI を介して 200 に設定されます。

- TrustSec は、プライマリデバイスで SGT 133 を適用します。
- セカンダリデバイスでは、IP から SGT へのバインディング（198.51.100.10—200）は SXP を介して学習され、TrustSec は SGT 200 を使用して適用されます。

IPv6 マルチキャスト通信による SGT インライン タギング

レイヤ 2 インライン タギングは、マルチキャストパケットがユニキャスト IPv6 送信元アドレスから発信されている場合、IPv6 マルチキャスト通信でもサポートされます。

SGT インラインタギングの制約事項

一般的な制約事項

Cisco Catalyst 9000 シリーズ スマートスイッチでの SGT インライン タギングには、以下の制約事項があります。

- Q-in-Q VLAN タギングは、Cisco TrustSec ヘッダーではサポートされていません。
- Flexible NetFlow、ポリシーベースルーティング（PBR）、および Quality of Service（QoS）SGT 機能はサポートされていません。

Cisco C9350 シリーズ スマートスイッチに固有の制約事項

一般的な制約事項とは別に、Cisco C9350 シリーズ スマートスイッチでの SGT インライン タギングには、以下の制約事項も適用されます。

- 出力インターフェイス用にシステムで生成されたパケットは、Cisco TrustSec 対応インターフェイスにおいて Cisco TrustSec タグ付きでは送信されません。
- VLAN ベースの SGT 割り当ておよび VLAN ベースの適用はサポートされていません。

SGT インライン タギングの設定

SGT インライン タギ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 **interface** {**gigabitethernet port** | **vlan** *number*}

Example:

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

Cisco TrustSec SGT 認証と転送が有効化されるようにインターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

Step 4 **cts manual**

Example:

```
Device(config-if)# cts manual
```

インターフェイスで Cisco TrustSec SGT 認証と転送を有効化し、Cisco TrustSec 手動インターフェイス コンフィギュレーション モードを開始します。

Step 5 **propagate sgt**

Example:

```
Device(config-if-cts-manual)# propagate sgt
```

インターフェイスでの Cisco TrustSec SGT 伝達を有効化します。

Note
このコマンドは、ピア デバイスで SGT over Ethernet パケットを受信できる状況（つまり、ピア デバイスが Cisco Ethertype CMD 0x8909 フレーム形式をサポートする場合）で使用します。

Step 6 **policy static sgt** *tag* [**trusted**]

Example:

```
Device(config-if-cts-manual)# policy static sgt 77 trusted
```

インターフェイスでスタティック SGT 入力ポリシーを設定し、インターフェイスで受信する SGT の信頼性を定義します。

Note
trusted キーワードは、そのインターフェイスが Cisco TrustSec に信頼されていることを示します。このインターフェイス上のイーサネットパケット内で受信した SGT 値は信頼され、デバイスによって任意の SG 認識型ポリシーの適用または出力タギングに使用されます。

Step 7 **end**

Example:

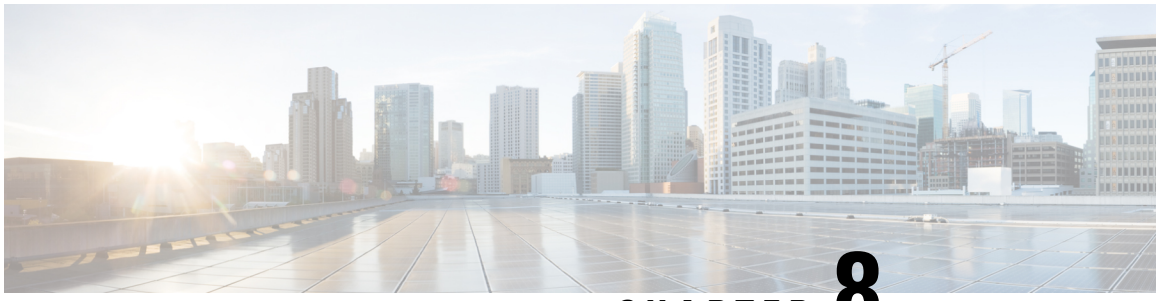
```
Device(config-if-cts-manual)# end
```

Cisco TrustSec 手動インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

例：SGT 静的インライン タギングの設定

この例では、デバイスのインターフェイスで L2-SGT タギングまたはインポジションを有効にして、インターフェイスが Cisco TrustSec に信頼されるかどうかを定義する方法を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# cts manual
Device(config-if-cts-manual)# propagate sgt
Device(config-if-cts-manual)# policy static sgt 77 trusted
```



CHAPTER 8

SGACL ハイ アベイラビリティ

SGACL ハイアベイラビリティの機能履歴

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	SGACL 高可用性（HA）： Cisco TrustSec セキュリティ グループ アクセス コントロール リスト（SGACL）は、Cisco StackWise 技術を備えたスイッチでの高可用性（HA）をサポートしています。	Cisco C9350 シリーズ スマート スイッチ Cisco C9610 シリーズ スマート スイッチ

Cisco TrustSec SGACL のハイ アベイラビリティ

Cisco TrustSec セキュリティ グループ アクセス コントロール リスト（SGACL）は、Cisco StackWise 技術を備えたスイッチでの高可用性（HA）をサポートしています。StackWise はステートフルな冗長性を提供するため、フェールオーバーイベント中にもスイッチスタックがアクセス コントロール エントリ（ACE）を適用して処理できます。

スイッチスタックでの高可用性（HA）操作

スイッチスタック内で、スタックマネージャは、最も高い優先順位を持つスイッチをアクティブスイッチに指定し、次に優先順位が高いスイッチをスタンバイスイッチに割り当てます。ステートフル スイッチオーバーの際、自動か CLI からの実行かに関係なく、スタンバイスイッチがアクティブになり、次の順位のスイッチがスタンバイロールを引き継ぎます。

運用データは、システムのブートアップ中、運用データの変更時（認可変更（CoA）など）、または運用データの更新中に、アクティブスイッチからスタンバイスイッチに同期されます。

ハイ アベイラビリティ セットアップでのデバイスの展開

高可用性（HA）セットアップでデバイスをデプロイする場合は、次の手順を実行します。

1. 高可用性（HA）セットアップに参加するすべてのデバイスから既存のログイン情報を削除します。
2. スタックの電源を投入し、デバイスロール（アクティブ、スタンバイ、およびメンバースイッチ）を割り当てます。
3. アクティブデバイスで、**cts credentials id** *id* **password** *password* コマンドを使用してログイン情報を設定します。

データの同期およびスイッチオーバーのプロセス

ステートフル スイッチオーバーが発生すると、新たにアクティブになったスイッチは、必要な運用データを要求してダウンロードします。環境データ（ENV データ）とロールベースアクセス制御リスト（RBACL）は、更新時間が完了した後にのみ更新されます。

次に、アクティブスイッチにダウンロードされるさまざまなタイプの運用データを示します。

運用データ	説明
環境データ（**ENV データ**）	更新または初期化中に RBACL 情報を取得するための優先サーバーリストが含まれています。
Protected Access Credential（**PAC**）	スイッチとオーセンティケータ間の一意の共有秘密で、セキュアトンネリングを介した Extensible Authentication Protocol Flexible Authentication（EAP-FAST）を保護するために使用されます。
ロールベースのポリシー（**RBACL** または **SGACL**）	スイッチ上のすべてのセキュリティグループタグ（SGT）マッピングのポリシーを定義する可変長リスト。

Note デバイス ID とパスワードの詳細で構成される Cisco TrustSec クレデンシャルは、アクティブスイッチでコマンドとして実行されます。

Cisco TrustSec SGACL 高可用性（HA）の確認

Cisco TrustSec SGACL 高可用性構成を確認するには、アクティブスイッチとスタンバイスイッチの両方で **show cts role-based permissions** コマンドを実行します。コマンドの出力は、両方のスイッチで同じである必要があります。

次に、アクティブスイッチでの **show cts role-based permissions** コマンドの出力例を示します。

```
Device# show cts role-based permissions

IPv4 Role-based permissions default (monitored):
        default_sgacl-01
        Deny IP-00
IPv4 Role-based permissions from group 10:SGT_10 to group 15:SGT_15:
        SGACL_3-01
IPv4 Role-based permissions from group 14:SGT_14 to group 15:SGT_15:
        multple_ace-14
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

次に、スタンバイスイッチでの **show cts role-based permissions** コマンドの出力例を示します。

```
Device-stby# show cts role-based permissions

IPv4 Role-based permissions default (monitored):
        default_sgacl-01
        Deny IP-00
IPv4 Role-based permissions from group 10:SGT_10 to group 15:SGT_15:
        SGACL_3-01
IPv4 Role-based permissions from group 14:SGT_14 to group 15:SGT_15:
        multple_ace-14
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

ステートフル スイッチオーバー後、アクティブスイッチで次のコマンドを実行して機能を確認します。

次に、**show cts pacs** コマンドの出力例を示します。

```
Device# show cts pacs

AID: A3B6D4D8353F102346786CF220FF151C
PAC-Info:
    PAC-type = Cisco Trustsec
    AID: A3B6D4D8353F102346786CF220FF151C
    I-ID: CTS_ED_21
    A-ID-Info: Identity Services Engine
    Credential Lifetime: 17:22:32 IST Mon Mar 14 2016
PAC-Opaque:
000200B800030001000400010A3B6D4D8353F102346786CF220FF151C0006009C00030100E044B2650D8351FD06
F23623C470511E00000001356DEA96C00093A80538898D40F633C368B053200D4C9D2422A7FEB4837EA9DBB89D1
```

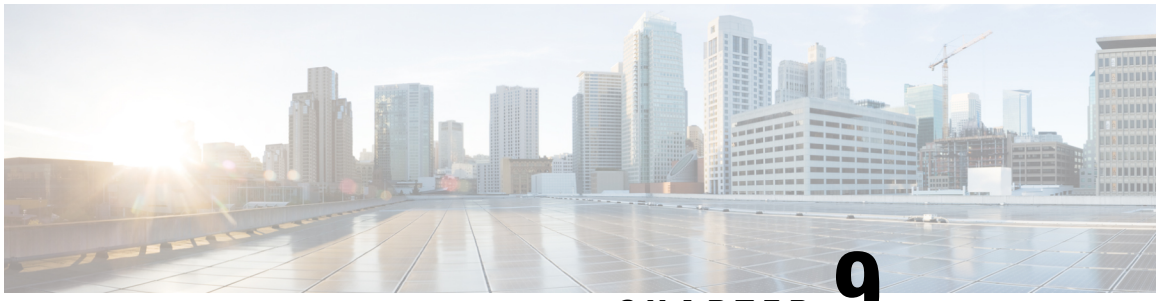
```
E51DA4E7B184E66D3D5F2839C11E5FB386936BB85250C61CA0116FDD9A184C6E96593EEAF5C39BE08140AFBB19
4EE701A0056600CFF5B12C02DD7ECEAA3CCC8170263669C483BD208052A46C31E39199830F794676842ADEECBB
A30FC4A5A0DEDA93
Refresh timer is set for 01:00:05
```

次に、**show cts environment-data** コマンドの出力例を示します。

```
Device# show cts environment-data

CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 0:Unknown
Server List Info:
Installed list: CTSServerList1-000D, 1 server(s):
  *Server: 10.78.105.47, port 1812, A-ID A3B6D4D8353F102346786CF220FF151C
  Status = ALIVE
  auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
0001-45 :
  0-00:Unknown
  2-ba:SGT_2
  3-00:SGT_3
  4-00:SGT_4
  5-00:SGT_5
  6-00:SGT_6
  7-00:SGT_7
  8-00:SGT_8
  9-00:SGT_9
  10-16:SGT_10
!
!
!
Environment Data Lifetime = 3600 secs
Last update time = 14:32:53 IST Mon Mar 14 2016
Env-data expires in 0:00:10:04 (dd:hr:mm:sec)
Env-data refreshes in 0:00:10:04 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
```

次に、ステートフル スイッチオーバー後の **show cts role-based permissions** コマンドの出力例を示します。

```
Device# show cts role-based permissions

IPv4 Role-based permissions default:
        default_sgacl-01
        Deny IP-00
IPv4 Role-based permissions from group 10:SGT_10 to group 15:SGT_15:
        SGACL_3-01
IPv4 Role-based permissions from group 14:SGT_14 to group 15:SGT_15:
        multple_ace-14
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```



CHAPTER 9

双方向 SXP サポート

双方向 SXP 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	双方向 SXP サポート： 双方向 SXP をサポートすることで、ピアはスピーカーとリスナーの両方として動作し、SXP バインドが単一の接続で双方向にフローできるようになります。	Cisco C9350 シリーズ スマートスイッチ Cisco C9610 シリーズ スマートスイッチ

Cisco TrustSec および SXP ロール

Cisco TrustSec は、デバイスが相互に認証されるセキュアなネットワークドメインを確立します。このシステムの中で、データを発信しているデバイスを「スピーカー」、受信しているデバイスを「リスナー」と呼びます。

双方向 SXP サポート

双方向 SXP をサポートすることで、ピアはスピーカーとリスナーの両方として動作し、SXP バインドが単一の接続で双方向にフローできるようになります。このセットアップに必要な IP アドレスのペアは 1 つだけであり、リスナーが接続を開始し、スピーカーが接続を受け入れます。

SXPv4 ループ検出

SXP バージョン 4 では、ループ検出のサポートが維持されているため、ネットワーク内の古いバインディングを防ぐことができます。

双方向 SXP サポートの設定

双方向 SXP サポートを設定するには、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。

パスワードを入力します（要求された場合）。

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 sxp enable**

Example:

```
Device(config)# cts sxp enable
```

Cisco TrustSec セキュリティグループタグ（SGT）交換プロトコルバージョン 4（SXPv4）を有効にします。

Step 4 **cts sxp default password** *password*

Example:

```
Device(config)# cts sxp default password Cisco123
```

（オプション）Cisco TrustSec SGT SXP のデフォルト パスワードを指定します。

Step 5 **cts sxp default source-ip** *ipv4-address*

Example:

```
Device(config)# cts sxp default source-ip 10.20.2.2
```

（オプション）Cisco TrustSec SGT SXP 送信元 IPv4 アドレスを設定します。

Step 6 **cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} **both** [**vrf** *vrf-name*]

Example:

```
Device(config)# cts sxp connection peer 10.20.2.2 password default mode local both
```

双方向 SXP 設定用の Cisco TrustSec SXP ピア アドレス接続を設定します。

- **both** キーワードは、双方向 SXP 設定を設定します。
- **source** キーワードには発信元デバイスの IPv4 アドレスを指定します。接続アドレスが指定されていない場合、デフォルトの送信元アドレス（設定されている場合）、またはポートのアドレスを使用します。
- **password** キーワードには、Cisco TrustSec SXP で接続に使用するパスワードを指定します。次のオプションがあります。
  - **default**：cts sxp default password コマンドを使用して設定したデフォルトの Cisco TrustSec SXP パスワードを使用します。
  - **none**：パスワードは使用されません。
- **mode** キーワードでは、リモートピアデバイスのロールを指定します。
  - **local**：指定したモードでは、ローカルデバイスを参照します。
  - **peer**：指定したモードでは、ピアデバイスを参照します。
  - **both**：双方向 SXP 接続のスピーカーとリスナーの両方の動作をするようにデバイスを指定します。
- **optional** vrf キーワードでは、ピアに対する VRF を指定します。デフォルトはデフォルト VRF です。

Step 7 **cts sxp speaker** *hold-time minimum-period*

Example:

```
Device(config)# cts sxp speaker hold-time 950
```

（オプション）Cisco TrustSec SGT SXPv4 用のスピーカー ネットワーク デバイスのグローバル ホールド時間（秒単位）を設定します。

有効な範囲は 1 ～ 65534 です。デフォルトは 120 です。

Step 8 **cts sxp listener hold-time** *minimum-period maximum-period*

Example:

```
Device(config)# cts sxp listener hold-time 750 1500
```

（オプション）Cisco TrustSec SGT SXPv4 用のリスナー ネットワーク デバイスのグローバル ホールド時間（秒単位）を設定します。

有効な範囲は 1 ～ 65534 です。デフォルトは 90 ～180 です。

Note
maximum-period 値は、minimum-period の値以上である必要があります。

Step 9 **exit**

Example:

```
Device(config)# exit
```

グローバル コンフィギュレーション モードを終了します。

Step 10 **show cts sxp** {**connections** | **sgt-map**} [**brief** | **vrf** *vrf-name*]

Example:

```
Device# show cts sxp connections
```

Cisco TrustSec 交換プロトコル（SXP）のステータスと接続を表示します。

双方向 SXP サポートの設定例

以下のセクションでは、双方向 SXP サポートの設定例を紹介します。

例：双方向 SXP サポートの設定

次の例は、双方向 CTS-SXP を有効化し、Device_A 上の SXP ピア接続が Device_B に接続するように設定する方法を示しています。

```
Device-A> enable
Device-A# configure terminal
Device-A(config)# cts sxp enable
Device-A(config)# cts sxp default password Cisco123
Device-A(config)# cts sxp default source-ip 10.10.1.1
Device-A(config)# cts sxp connection peer 10.20.2.2 password default mode local both
Device-A(config)# exit
```

次の例は、Device_B 上の双方向 CTS-SXP ピア接続が Device_A に接続するように設定する方法を示しています。

```
Device-B> enable
Device-B# configure terminal
Device-B(config)# cts sxp enable
Device-B(config)# cts sxp default password Password123
Device-B(config)# cts sxp default source-ip 10.20.2.2
Device-B(config)# cts sxp connection peer 10.10.1.1 password default mode local both
Device-B(config)# exit
```

例：双方向 SXP サポートの確認

次に、**show cts sxp connections** コマンドの出力例を示します。

```
Device# show cts sxp connections

        SXP : Enabled
        Highest Version Supported: 4
        Default Password : Set
        Default Source IP: Not Set
        Connection retry open period: 120 secs
        Reconcile period: 120 secs
        Retry open timer is running
        ------------------------------------------------
        Peer IP : 2.0.0.2
        Source IP : 1.0.0.2
        Conn status : On (Speaker) :: On (Listener)
        Conn version : 4
        Local mode : Both
        Connection inst# : 1
        TCP conn fd : 1(Speaker) 3(Listener)
        TCP conn password: default SXP password
        Duration since last state change: 1:03:38:03 (dd:hr:mm:sec) :: 0:00:00:46
(dd:hr:mm:sec)
```

次に、**show cts sxp connections brief** コマンドの出力例を示します。

```
        Device# show cts sxp connection brief

        SXP : Enabled
        Highest Version Supported: 4
        Default Password : Set
        Default Source IP: Not Set
        Connection retry open period: 120 secs
        Reconcile period: 120 secs
        Retry open timer is running
        ------------------------------------------------------
        Peer_IP Source_IP Conn Status Duration
        ------------------------------------------------------
        2.0.0.2 1.0.0.2 On(Speaker)::On(Listener) 0:00:37:17 (dd:hr:mm:sec)::0:00:37:19
(dd:hr:mm:sec)
```

次のテーブルに、接続ステータス出力のさまざまなシナリオを示します。

Node1	Node2	接続ステータスについての Node1 CLI 出力	接続ステータスについての Node2 CLI 出力
両方	両方	オン（スピーカー） オン（リスナー）	オン（リスナー） オン（スピーカー）

Node1	Node2	接続ステータスについての Node1 CLI 出力	接続ステータスについての Node2 CLI 出力
スピーカー	リスナー	オン	点灯
リスナー	スピーカー	オン	点灯

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。