



SGT 交換プロトコル

- [SXP の機能履歴, on page 1](#)
- [SGT 交換プロトコル, on page 2](#)
- [シスコ グループベース ポリシー, on page 3](#)
- [ネットワーク内で SGT が使用される仕組み, on page 3](#)
- [SGT 割り当てのメカニズム, on page 3](#)
- [SGT 割り当てメソッド, on page 4](#)
- [エンドポイント認証と SGT の関連付け, on page 4](#)
- [セキュリティグループタグ伝達での SXP のロール, on page 5](#)
- [SXP プロトコルの詳細, on page 5](#)
- [SXP バージョン 5, on page 5](#)
- [SXP 設定のガイドライン, on page 6](#)
- [IPv6 を介した SGT 交換プロトコルの制約事項, on page 7](#)
- [SXP の設定方法, on page 7](#)
- [IPv6 を介した SGT 交換プロトコルの設定, on page 18](#)
- [SGT 交換プロトコル接続の確認, on page 20](#)
- [SXP の設定例, on page 20](#)

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) ハードウェアタグging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) ハードウェアタグging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グging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] password

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グGING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-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
```

例: SGT 交換プロトコル接続の確認

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。