Cisco TrustSec SGT Exchange Protocol IPv4

Cisco TrustSec（CTS）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ます。ドメイン内のデバイス間リンクでの通信は、暗号化、メッセージ整合性検査、データパス リプレイ防止メカニズムを組み合わせたセキュリティで保護されます。

セキュリティ グループ タグ（SGT）交換プロトコル（SXP）は、CTS をサポートする複数のプロトコルの 1 つであり、本書では CTS-SXP と呼びます。CTS-SXP は、パケットのタグ付け機能がないネットワーク デバイス全体に IP-to-SGT バインドの情報を伝播する、制御プロトコルです。CTS-SXP は、ネットワーク上のアップストリーム デバイスへの認証ポイントから SGT バインドへの IP を渡します。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 デバイスから学習したアイデンティティ情報を伝えることができます。

Cisco TrustSec SGT Exchange Protocol IPv4 の制約事項

- IOS 機能の Cisco TrustSec サポートは、第 2 世代 Cisco サービス統合型ルータ（ISR G2）のみでサポートされています。
- CTS-SXP は物理インターフェイスだけでサポートされ、論理インターフェイスでサポートされません。
- CTS-SXP 検証は、IPv6 をサポートしていません。
- ルータにデフォルトのパスワードが実装されている場合、そのルータでの接続は、デフォルト パスワードを使用するようにパスワードを設定する必要があります。デフォルトのパスワードが設定されていない場合、そのルータでの接続はパスワード設定を使用しないよ

うに設定してください。パスワードオプションの設定は導入ネットワーク全体で一貫している必要があります。

Cisco TrustSec SGT Exchange Protocol IPv4 に関する情報

セキュリティ グループ タギング

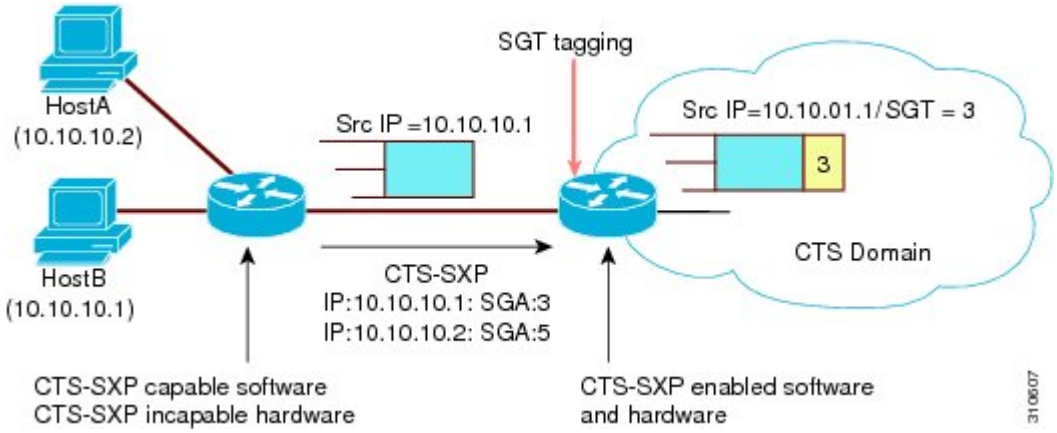
CTS-SXP は、認証時に取得したデバイスおよびユーザの識別情報を使用して、ネットワークに進入するパケットをセキュリティ グループ（SG）で分類します。このパケット分類は、CTS-SXP ネットワークへの入力時にパケットにタグ付けされることにより維持されます。タグによってパケットはデータ パス全体を通じて正しく識別され、セキュリティおよびその他のポリシー基準が適用されます。セキュリティ グループ タグ（SGT）によってエンドポイント デバイスはトラフィックをフィルタリングできるので、ネットワークへのアクセス コントロール ポリシーの適用が可能になります。

CTS-SXP によるレガシー アクセス ネットワークへの SGT の伝播

パケットへの SGT のタグ付けには、ハードウェアによるサポートが必要です。CTS 認証に参加できが、SGT でパケットをタグ付けするハードウェア機能を持たないデバイスが、ネットワーク内にある場合があります。ただし、CTS-SXP を使用する場合は、これらのデバイスが、IP と SGT のマッピングを CTS 対応ハードウェアがある CTS ピア デバイスに渡すことができます。

通常、CTS-SXP は CTS ドメイン エッジの入力アクセス レイヤ デバイスと CTS ドメイン内のディストリビューション レイヤ デバイス間で動作します。アクセス レイヤ デバイスは入力パケットの適切な SGT を判断するために、外部送信元デバイスの CTS 認証を実行します。アクセス レイヤ デバイスは IP デバイス トラッキングおよび（任意で）DHCP スヌーピングを使用して送信元デバイスの IP アドレスを学習し、その後 CTS-SXP を使用して送信元デバイスの IP アドレスおよび SGT を、ディストリビューション スイッチに渡します。CTS 対応のハードウェアを備えたディストリビューション スイッチは、この IP と SGT のマッピング情報を使用して、パケットに適切にタグを付け、セキュリティ グループ アクセス コントロール リスト（SGACL）ポリシーを強制します。次の図を参照してください。SGACL は、SGT とポリシーを関連付けます。ポリシーは、SGT タグ付けされたトラフィックが CTS ドメインから出力されると適用されます。

図 *1 : CTS-SXP* による *SGT* 情報の伝達方法



CTS ハードウェア サポート対象外のピアと CTS ハードウェア サポート対象のピア間の CTS-SXP 接続は、手動で設定する必要があります。CTS-CSXP 接続を設定する場合は、次の作業を実行する必要があります。

- CTS-SXP のデータの整合性と認証が必要な場合、同じ CTS-SXP パスワードを両方のピア デバイスで設定できます。CTS-SXP パスワードは各ピア接続に対して明示的に指定することも、デバイスに対してグローバルに設定することもできます。CTS-SXP パスワードは必須ではありませんが、推奨します。
- CTS-SXP 接続の各ピアは、CTS-SXP スピーカーまたは CTS-SXP リスナーとして設定する必要があります。スピーカー デバイスはリスナー デバイスに IP-to-SGT 情報を渡します。
- 各ピアの関係に使用する送信元 IP アドレスを指定できます。または、特定の送信元 IP アドレスが設定されていないピア接続に対して、デフォルトの送信元 IP アドレスを設定できます。送信元 IP アドレスが指定されていないと、デバイスはピアへの接続のインターフェイス IP アドレスを使用します。

CTS-SXP では複数のホップを許可します。つまり、CTS ハードウェア サポート対象外デバイスのピアが CTS ハードウェア サポートの対象外でもある場合、2 番目のピアはハードウェア対応ピアに到達するまで IP と SGT のマッピング情報の伝播を継続して、3 番目のピアへの CTS-SXP 接続を設定できます。デバイスは 1 つの CTS-SXP 接続では CTS-SXP リスナーとして、別の CTS-SXP 接続では CTS-SXP スピーカーとして設定できます。

CTS デバイスは TCP キープアライブ メカニズムを使用して、CTS-SXP ピアとの接続を維持します。ピア接続を確立または回復するために、デバイスは設定可能な再試行期間を使用して接続が成功するか、接続が設定から削除されるまで接続の確立を繰り返し試行します。

VRF-Aware CTS-SXP

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

CTS-SXP VRF サポートは、次のようにまとめることができます。

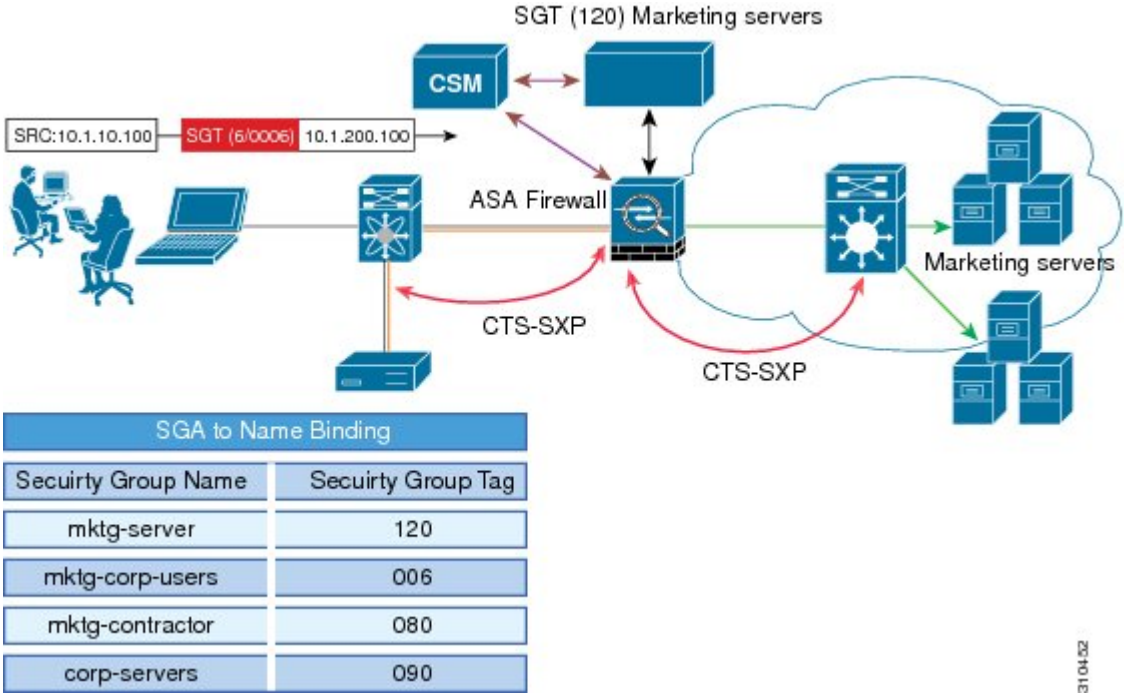
- 1 つの VRF には 1 つの CTS-SXP 接続のみをバインドできます。
- 別の VRF が重複する CTS-SXP ピアまたは送信元 IP アドレス持つ可能性があります。
- 1 つの VRF で学習（追加または削除）された IP と SGT のマッピングは、同じ VRF ドメインでのみ更新できます。CTS-SXP 接続は異なる VRF にバインドされたマッピングを更新できません。SXP 接続が VRF で終了しない場合は、その VRF の IP-SGT マッピングは SXP によって更新されません。
- CTS-SXP 検証は、送信元 IPv6 アドレスを使用した接続の確立をサポートしていません。ただし、VRF ドメイン内の 1 つの CTS-SXP 接続を IPv4 と IPv6 両方の IP と SGT のマッピングに転送できる場合は、VRF あたりで複数のアドレス ファミリがサポートされます。
- CTS-SXP には VRF あたりの接続数および IP と SGT のマッピング数に制限はありません。

セキュリティ グループ アクセスのゾーンベース ポリシー ファイアウォール

CTS-SXP は、セキュリティ グループ アクセス（SGA）ゾーンベース ポリシー ファイアウォール（ZBPF）を使用することで、ネットワーク デバイスの導入をネットワークのさらに別の場所へ拡張します。CTS-SXP は、次の図に示すとおり、ネットワーク全体に存在するプライマリ通信パスからアイデンティティ情報を学習するインラインデバイスを通じたアイデンティティ分散に使用されます。

セキュリティ グループ タグ（SGT）は、強制ポリシーを適用するため、SGA ZBPF によって使用されます。IP と SGT のマッピング情報は、CTS-SXP から学習します。パケットを受信すると、パケット内の送信元と宛先の IP アドレスは、送信元と宛先のタグを派生させるために使用されます。アイデンティティ ファイアウォールは、属性の 1 つに SGT がある、設定されたポリシーに基づいて、受信した IP パケットにポリシーを適用します。

図 *2 :* ネットワーク全体の *CTS-SXP SGA ZBPF* 分散パス



Cisco TrustSec SGT Exchange Protocol IPv4 の設定方法

CTS-SXP の有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp enable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	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。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**cts sxp enable** 例： `Device(config)# cts sxp enable`	設定された任意のピア接続に対して CTS-SXP 接続を有効化します。 （注） ピア接続が設定されていることを確認します。ピア接続が設定されていない場合、CTS-SXP 接続はそれらとは確立できません。

CTS-SXP ピア接続の設定

CTS-SXP ピア接続を両方のデバイスで設定する必要があります。一方のデバイスはスピーカーで、他方のデバイスはリスナーになります。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。

（注） デフォルトの CTS-SXP 送信元 IP アドレスが設定されていない場合に、接続の CTS-SXP 送信元アドレスを設定しないと、Cisco TrustSec ソフトウェアは既存のローカル IP アドレスから CTS-SXP 送信元 IP アドレスを抽出します。CTS-SXP 送信元 IP アドレスは、ルータから開始される TCP 接続ごとに異なる場合があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} [[**listener** | **speaker**] [**vrf** *vrf-name*]]
4. **exit**
5. **show cts sxp** {**connections** | **sgt-map**} [**brief** | **vrf** *vrf-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	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。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} [[**listener** | **speaker**] [**vrf** *vrf-name*]] 例： `Device(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker`	CTS-SXP ピア アドレス接続を設定します。 **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、CTS-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 CTS-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**：指定したモードはローカルデバイスを参照します。 • **peer**：指定したモードはピアデバイスを参照します。 • **listener**：このデバイスが接続の際にリスナーになります。 • **speaker**：接続の際にこのデバイスがスピーカーになります。これはデフォルトです。 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。
ステップ 4	**exit** 例： `Device# 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。
ステップ 5	**show cts sxp** {**connections** | **sgt-map**} [**brief** | **vrf** *vrf-name*] 例： `Device# show cts sxp connections`	（オプション）CTS-SXP のステータスと接続を表示します。

デフォルトの CTS-SXP パスワードの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp default password** [**0** | **6** | **7**] *password*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts sxp default password** [**0** | **6** | **7**] *password* 例： `Device(config)# cts sxp default password Cisco123`	CTS-SXP のデフォルト パスワードを設定します。クリアテキストパスワード（**0**を使用するかオプションなし）または暗号化パスワード（**6** または **7** オプションを使用）を入力できます。パスワードの最大長は 32 文字です。 （注） デフォルトでは、CTS-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。
ステップ 4	**exit** 例： `Device# 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 CTS-SXP 送信元 IP アドレスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp default source-ip** *src-ip-addr*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts sxp default source-ip** *src-ip-addr* 例： `Device(config)# cts sxp default source-ip 10.20.2.2`	CTS-SXP デフォルトの送信元 IP アドレスを設定します。これは、送信元IPアドレスが指定されていないすべての新しい TCP 接続に使用されます。 （注） デフォルトの CTS-SXP 送信元 IP アドレスが設定されている場合も、既存の TCP 接続には影響しません。
ステップ 4	**exit** 例： `Device# 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。

CTS-SXP の復帰期間の設定

ピアが CTS-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、CTS-SXP 復帰期間タイマーが開始されます。CTS-SXP 復帰期間タイマーがアクティブな間、CTS 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。デフォルト値は 120 秒（2 分）です。CTS-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。

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp reconciliation period** *seconds*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts sxp reconciliation period** *seconds* 例： `Device(config)# cts sxp reconciliation period 150`	CTS-SXP 復帰タイマーを秒単位で設定します。範囲は 0 ～ 64000 です。デフォルトは 120 です。
ステップ 4	**exit** 例： `Device# 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 モードを開始します。

CTS-SXP 再試行期間の設定

CTS-SXP 再試行期間によって、CTS ソフトウェアが CTS-SXP 接続を再試行する頻度が決まります。CTS-SXP 接続が正常に確立されなかった場合、CTS ソフトウェアは CTS-SXP 再試行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。デフォルト値は2分です。CTS-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。

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp retry period** *seconds*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts sxp retry period** *seconds* 例： `Device(config)# cts sxp retry period 160`	CTS-SXP 再試行タイマーを秒単位で設定します。範囲は 0 ～ 64000 です。デフォルトは 120 です。
ステップ 4	**exit** 例： `Device# 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。

IP と SGT のマッピング変更をキャプチャする Syslog の作成

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp log binding-changes**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts sxp log binding-changes** 例： `Device(config)# cts sxp log binding-changes`	IP と SGT バインド変更のロギングを有効にすると、IP と SGT バインディングの変更（追加、削除、変更）が発生するたびに CTS-SXP の syslog （sev 5 syslog）が生成されます。これらの変更は CTS-SXP 接続で学習されて伝播されます。

	コマンドまたはアクション	目的
		（注） このロギング機能は、デフォルトではディセーブルになっています。
ステップ 4	**exit** 例： `Device# 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。

セキュリティ グループ アクセスのゾーンベース ポリシー ファイアウォールのクラス マップの設定

このタスクを実行して、セキュリティ グループ アクセス（SGA）ゾーンベース ポリシー ファイアウォールのネットワーク トラフィックを分類するためのクラス マップを設定します。

（注） 少なくとも 1 つの手順を実行する必要があります。

ゾーンベース ファイアウォール ポリシーは、フィルタリングにセキュリティ グループ タグの ID を使用します。ゾーンベース ファイアウォール ポリシーでは、ポリシーと一致するのは、セッションを作成した最初のパケットのみです。このフローの後続パケットは、設定されたポリシー内のフィルタと一致しませんが、セッションとは直接一致します。後続パケットに関連する統計情報は、検査アクションの一部として表示されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **object-group security** *name*
4. **security-group tag-id** *sgt-id*
5. **group-object** *name*
6. **description** *text*
7. **exit**
8. **class-map type inspect** [**match-any** | **match-all**] *class-map-name*
9. **match group-object security source** *name*
10. **match group-object security destination** *name*
11. **end**
12. **show object-group** [*name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**object-group security** *name* 例： `Device(config)# object-group security myobject1a`	オブジェクト グループを作成して、特定のユーザまたはエンドポイントから受信するトラフィックを特定し、オブジェクトグループのアイデンティティ モードに入ります。
ステップ 4	**security-group tag-id** *sgt-id* 例： `Device(config-object-group)# security-group tag-id 120`	SGT ID 番号を使用して、セキュリティ グループのメンバーシップを指定します。この番号は 1 ～ 65535 ですこのコマンドを使用すると、複数のセキュリティ グループを指定できます。
ステップ 5	**group-object** *name* 例： `Device(config-object-group)# group-object admin`	（オプション）ネストされた参照を、ユーザ グループのタイプに指定します。このコマンドを使用すると、複数のネストされたユーザ グループを指定できます。
ステップ 6	**description** *text* 例： `Device(config-object-group)# description my sgtinfo`	（オプション）セキュリティ グループに関する情報を定義します。
ステップ 7	**exit** 例： `Device(config-object-group)# exit`	オブジェクトグループ アイデンティティ モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 8	**class-map type inspect** [**match-any** | **match-all**] *class-map-name* 例： `Device(config)# class-map type inspect match-any myclass1`	レイヤ 3 またはレイヤ 4 の検査タイプ クラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 9	**match group-object security source** *name* 例： `Device(config-cmap)# match group-object security source myobject1`	セキュリティ グループ内のユーザからのトラフィックと一致させます。
ステップ 10	**match group-object security destination** *name* 例： `Device(config-cmap)# match group-object security destination myobject1`	セキュリティ グループ内のユーザのトラフィックと一致させます。
ステップ 11	**end** 例： `Device(config-cmap)# end`	クラスマップ 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。
ステップ 12	**show object-group** [*name*] 例： `Device# show object-group admin`	（オプション）すべてのユーザ グループのコンテンツを表示します。オプションとして、*name* 引数を使用すると、単一グループの情報が表示されます。

セキュリティ グループ アクセスのゾーンベース ポリシー ファイアウォールのポリシー マップの作成

このタスクを実行して、ゾーン ペアに接続する、セキュリティ グループ アクセス（SGA）ゾーンベース ポリシー ファイアウォールのポリシー マップを作成します。また、このタスクは、セキュリティ ゾーンに属するインターフェイス上で、セキュリティ グループ タグ（SGT）交換プロトコル（SXP）またはL2タグ付きトラフィックと動作するよう、アイデンティティ ファイアウォール（IDFW）を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *policy-map-name*
4. **class type inspect** *class-name*
5. **inspect**
6. **exit**
7. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
8. **service-policy type inspect** *policy-map-name*
9. **end**
10. **interface** *type number*
11. **zone-member security** *zone-name*

12. **cts manual**
13. **no propagate sgt**
14. **policy static sgt** *tag* [**trusted**]
15. **exit**
16. **show policy-map type inspect zone-pair session**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect z1z2-policy`	レイヤ 3 またはレイヤ 4 の検査タイプ ポリシーマップを作成します。 • ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class type inspect** *class-name* 例： `Device(config-pmap)# class type inspect cmap-1`	アクションを実行する対象のトラフィック（クラス）を指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 5	**inspect** 例： `Device(config-pmap-c)# inspect`	パケット インスペクションを有効化します。
ステップ 6	**exit** 例： `Device(config-pmap-c)# exit`	ポリシーマップ クラス 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 モードを開始します。
ステップ 7	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security z1z2 source z1 destination z2`	ゾーン ペアを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。

	コマンドまたはアクション	目的
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone)# service-policy type inspect z1z2-policy2`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 9	**end** 例： `Device(config-sec-zone)# end`	セキュリティ ゾーン 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 モードを開始します。
ステップ 10	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/1/1`	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。
ステップ 11	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security Inside`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 （注） インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（ルータ宛のトラフィックまたはルータ発信のトラフィックを除く）は、デフォルトでドロップされます。トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 12	**cts manual** 例： `Device(config-if)# cts manual`	Cisco TrustSec Security（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。
ステップ 13	**no propagate sgt** 例： `Device(config-if-cts-manual)# no propagate sgt`	CTS インターフェイスで レイヤ 2 の SGT 伝達を無効化します。

	コマンドまたはアクション	目的
ステップ 14	**policy static sgt** *tag* [**trusted**] 例： `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。
ステップ 15	**exit** 例： `Device(config-if)# exit`	セキュリティ ゾーン 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。
ステップ 16	**show policy-map type inspect zone-pair session** 例： `Device# show policy-map type inspect zone-pair session`	（オプション）指定されたゾーン ペアのポリシー マップアプリケーションが原因で作成された、Cisco IOS ステートフル パケット インスペクション セッションを表示します。 （注） クラスマップ フィールドの下に表示される情報は、接続開始トラフィックのみに属するトラフィックのトラフィック レート（ビット/秒）です。接続セットアップ レートが非常に高く、レートが計算される複数のインターバルにわたって高い接続セットアップ レートが持続する場合を除き、接続に関する意味のあるデータは表示されません。

例：

次の出力例は、**show policy-map type inspect zone-pair session** コマンドによって表示される、指定されたゾーンペアのポリシーマップ アプリケーションが原因で作成された、Cisco IOS ステートフル パケット インスペクション セッションに関する情報を示します。

```
Device# show policy-map type inspect zone-pair session

Zone-pair: in-out
 Service-policy inspect : test

   Class-map: test (match-any)
     Match: group-object security source sgt
     Inspect
       Established Sessions
        Session 113EF68C (192.2.2.1:8)=>(198.51.100.252:153) icmp SIS_OPEN
         Created 00:00:02, Last heard 00:00:02
         Bytes sent (initiator:responder) [360:360]


   Class-map: class-default (match-any)
```

```
Match: any
Drop (default action)
  310 packets, 37380 bytes
```

Cisco TrustSec SGT Exchange Protocol IPv4 の設定例

例：CTS-SXP ピア接続のイネーブル化と設定

次に、CTS-SXP をイネーブルにし、Device_A（スピーカー）で Device_B（リスナー）への SXP ピア接続を設定する例を示します。

```
Device# 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 speaker
```

次に、Device_B（リスナー）で Device_A（スピーカー）への CTS-SXP ピア接続を設定する例を示します。

```
Device# configure terminal
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Cisco123
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 listener
```

次に、CTS-SXP 接続を表示する **show cts sxp connections** コマンドの出力例を示します。

```
Device_B# 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
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
```

例：セキュリティ グループ アクセスのゾーンベース ポリシー ファイアウォールの設定

次の例は、SGA ゾーンベース ポリシー ファイアウォールのクラス マップとポリシー マップの設定を示します。

```
Device(config)# object-group security myobject1
Device(config-object-group)# security-group tag-id 1
Device(config-object-group)# exit
Device(config)# object-group security myobject2
Device(config-object-group)# security-group tag-id 2
Device(config-object-group)# exit
Device(config)# object-group security myobject3
Device(config-object-group)# security-group tag-id 3
Device(config-object-group)# exit
Device(config)# object-group security myobject4
Device(config-object-group)# security-group tag-id 4
Device(config-object-group)# exit

Device(config)# class-map type inspect match-any myclass1
Device(config-cmap)# match group-object security source myobject1
Device(config-cmap)# exit
Device(config)# class-map type inspect match-any myclass2
Device(config-cmap)# match group-object security source myobject2
Device(config-cmap)# exit
Device(config)# class-map type inspect match-any myclass3
Device(config-cmap)# match group-object security source myobject3
Device(config-cmap)# exit
Device(config)# class-map type inspect match-any myclass4
Device(config-cmap)# match group-object security source myobject4
Device(config-cmap)# exit

Device(config)# policy-map type inspect InsideOutside
Device(config-pmap)# class type inspect myclass1
Device(config-pmap-c)# pass
Device(config-pmap-c)# exit
Device(config-pmap)# class type inspect myclass2
Device(config-pmap-c)# drop log
Device(config-pmap-c)# exit

Device(config)# policy-map type inspect OutsideInside
Device(config-pmap)# class type inspect myclass3
Device(config-pmap-c)# pass
Device(config-pmap-c)# exit
Device(config-pmap)# class type inspect myclass4
Device(config-pmap-c)# drop
Device(config-pmap-c)# exit

Device(config)# zone-pair security Inside
Device(config-sec-zone)# description Firewall Inside Zone
Device(config-sec-zone)# exit

Device(config)# zone-pair security Outside
Device(config-sec-zone)# description Firewall Outside Zone
Device(config-sec-zone)# exit

Device(config)# zone-pair security InsideOutside source Inside destination Outside
Device(config-sec-zone)# description Firewall ZonePair Inside Outside
Device(config-sec-zone)# service-policy type inspect InsideOutside
```

```
Device(config-sec-zone)# exit

Device(config)# zone-pair security OutsideInside source Outside destination Inside
Device(config-sec-zone)# description Firewall ZonePair Outside Inside
Device(config-sec-zone)# service-policy type inspect OutsideInside
Device(config-sec-zone)# exit

Device(config)# interface Gigabit 0/1/1
Device(config-if)# zone-member security Inside
Device(config-if)# exit
```

TrustSec SGT の処理：L2 SGT のインポジションと転送に関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	『Cisco IOS Security Command Reference: Commands A to C』
	『Cisco IOS Security Command Reference: Commands D to L』
	『Cisco IOS Security Command Reference: Commands M to R』
	『Cisco IOS Security Command Reference: Commands S to Z』
Cisco TrustSec スイッチ	『Cisco TrustSec スイッチ コンフィギュレーション ガイド』

MIB

MIB	MIB のリンク
CISCO-TRUSTSEC-SXP-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco TrustSec SGT Exchange Protocol IPv4 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : Cisco TrustSec SGT Exchange Protocol IPv4* の機能情報

機能名	リリース	機能情報
Cisco TrustSec SGT Exchange Protocol IPv4		セキュリティ グループ タグ（SGT）交換プロトコル（SXP）は、CTS をサポートする複数のプロトコルの 1 つであり、本書では CTS-SXP と呼びます。CTS-SXP は、パケットのタグ付け機能がないネットワーク デバイス全体に IP-to-SGT バインドの情報を伝播する、制御プロトコルです。CTS-SXP は、ネットワーク上のアップストリーム デバイスへの認証ポイントから SGT バインドへの IP を渡します。これにより、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 デバイスから学習したアイデンティティ情報を伝えることができます。 次のコマンドが導入または変更されました。**cts sxp enable, cts sxp connection peer**、**show cts sxp**、**cts sxp default source-ip, cts sxp reconciliation period, cts sxp retry period, cts sxp log binding-changes**。

機能名	リリース	機能情報
TrustSec SG Firewall Enforcement IPv4		この機能は、CTS-SXP がセキュリティ グループ アクセス（SGA）ゾーンベース ポリシー ファイアウォール（ZBPF）を通じてネットワーク デバイスを拡張するのを支援します。 次のコマンドが導入または変更されました。**group-object**、**match group-object security**、**object-group security**、**policy static sgt**、および **security-group**。

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。