『Cisco TrustSec スイッチ コンフィギュレーションガイド』

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

有効な Cisco IOS XE リリース 3.7.0E（Catalyst スイッチング用）および Cisco IOS XE リリース 3.17S（アクセスおよびエッジ ルーティング用）の 2 つのリリースは、コンバージド リリースの 1 つのバージョンに進化（マージ）しました。これは、1 つのリリースでスイッチングおよびルーティング ポートフォリオにおいて幅広いアクセスおよびエッジ製品をカバーします。

（注） 技術構成ガイドの機能情報の表に、機能の導入時期を記載しています。他のプラットフォームがその機能をサポートした時期については、記載があるものも、ないものもあります。特定の機能が使用しているプラットフォームでサポートされているかどうかを判断するには、製品のランディング ページに掲載された技術構成ガイドを参照してください。技術構成ガイドが製品のランディング ページに表示されると、その機能が該当のプラットフォームでサポートされているかどうかが示されます。

第 2 章

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。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモ

ジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

Cisco TrustSec SGT Exchange Protocol IPv4 の前提条件

SXP を実装する前に、CTS-SXP ネットワークを確立する必要があります。CTS-SXP ネットワークには次の前提条件があります。

- Cisco TrustSec の機能を既存のルータで使用するには、Cisco TrustSec のセキュリティ ライセンスを購入していること。ルータを発注済みで Cisco TrustSec の機能が必要な場合は、発送前に、このライセンスが使用するルータにプリインストールされていること。
- すべてのネットワーク デバイスで CTS-SXP ソフトウェアを実行していること。
- 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。
- 認証には Cisco Identity Services Engine 1.0 が必要です。認証には Secure Access Control Server（ACS）Express Appliance サーバも使用できますが、CTS ではすべての ACS 機能がサポートされていません。ACS 5.1 が CTS-SXP ライセンスで動作していること。
- 異なるルータ上の異なる値に、**retryopentimer** コマンドが設定されていること。

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。

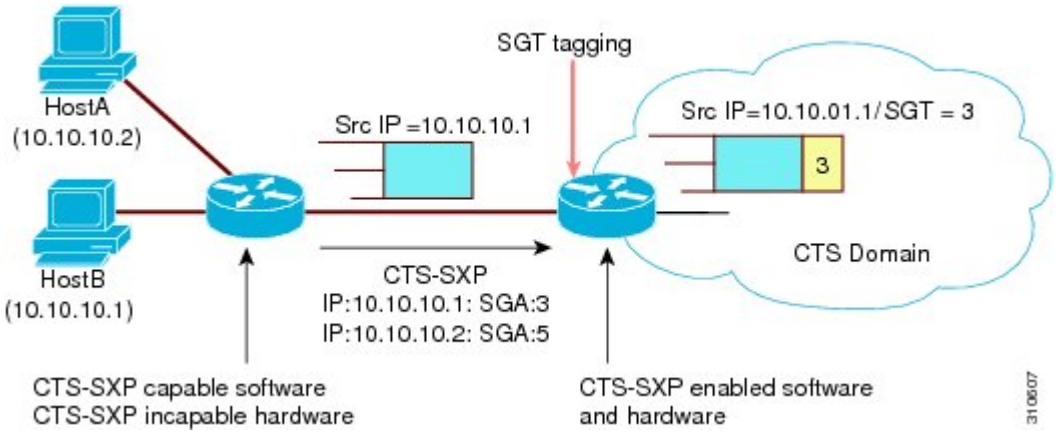
CTS-SXP によるレガシー アクセス ネットワークへの SGT の伝播

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。

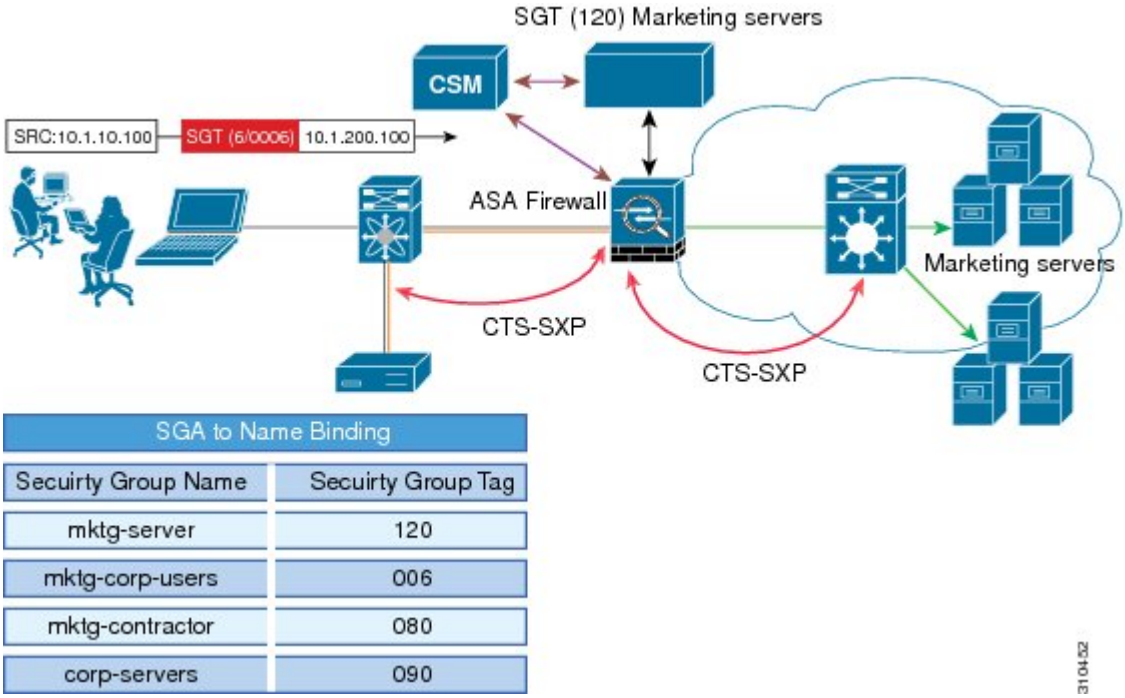
セキュリティ グループ アクセスのゾーンベース ポリシー ファイアウォール

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. イネーブル化
2. **configure terminal**
3. **ctssxpenable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Device> enable`	• 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	**ctssxpenable** 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. イネーブル化
2. **configureterminal**
3. **ctssxpconnectionpeer***ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} [[**listener** | **speaker**] [**vrf***vrf-name*]]
4. **exit**
5. **showctssxp** {**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	**イネーブル化** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**ctssxpconnectionpeer***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。

	コマンドまたはアクション	目的
ステップ 5	**showctssxp** {**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. イネーブル化
2. **configureterminal**
3. **ctssxpdefaultpassword**[**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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**ctssxpdefaultpassword**[**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。

	コマンドまたはアクション	目的
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. イネーブル化
2. **configureterminal**
3. **ctssxpdefaultsource-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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**ctssxpdefaultsource-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。

	コマンドまたはアクション	目的
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. イネーブル化
2. **configureterminal**
3. **ctssxpreconciliationperiod***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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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。

	コマンドまたはアクション	目的
ステップ 3	**ctssxpreconciliationperiod***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. イネーブル化
2. **configureterminal**
3. **ctssxpretryperiod***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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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。

	コマンドまたはアクション	目的
ステップ 3	**ctssxpretryperiod***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. イネーブル化
2. **configureterminal**
3. **ctssxplogbinding-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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**ctssxplogbinding-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. イネーブル化
2. **configureterminal**
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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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。

	コマンドまたはアクション	目的
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。
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. イネーブル化
2. **configureterminal**
3. **policy-maptypeinspect***policy-map-name*
4. **classtypeinspect***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***typenumber*
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	イネーブル化 例： `Device> enable`	特権EXECモードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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-maptypeinspect***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	**classtypeinspect***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。

	コマンドまたはアクション	目的
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。
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***typenumber* 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。

	コマンドまたはアクション	目的
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。
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。

	コマンドまたはアクション	目的
		（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
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

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
★枠で囲まれた Technical Assistance の場合★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：**ctssxpenable**、**ctssxpconnectionpeer**、**showctssxp**、**ctssxpdefaultsource-ip**、**ctssxpreconciliationperiod**、**ctssxpretryperiod**、**ctssxplogbinding-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**、**security-group**。

第 3 章

TrustSec SGTの処理：L2 SGTのインポジションと転送

初版：2011年7月25日

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。

TrustSec SGT の処理：L2 SGT のインポジションと転送の機能により、ルータのインターフェイスは CTS を手動で有効化できるようになるため、ルータはセキュリティ グループ タグ（SGT）を、CTS ヘッダー内でネットワーク全体に運ばれるパケットに挿入できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

TrustSec SGT の処理：L2 SGT のインポジションと転送の前提条件

TrustSec SGT の処理：L2 SGT インポジションと転送の機能を実装する前に、次の前提条件で CTS 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、CTS-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 サーバがネットワーク内で機能すること。
- 異なるルータ上の異なる値に、**retryopentimer** コマンドが設定されていること。

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

セキュリティ グループおよび SGT

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、エンドポイント デバイス、およびリソースのグループです。セキュリティ グループは管理者が ACS で定義します。新しいユーザおよびデバイスが Cisco TrustSec（CTS）ドメインに追加されると、認証サーバは、適切なセキュリティ グループにこれらの新しいエンティティを割り当てます。CTS は各セキュリティ グループに、その範囲が CTS ドメイン内でグローバルな一意のセキュリティ グループ番号（16 ビット）を割り当てます。ルータ内のセキュリティ グループの数は、認証されたネットワーク エンティティの数に制限されます。セキュリティ グループ番号は、手動で設定する必要はありません。

デバイスが認証されると、CTS はそのデバイスから発信されるすべてのパケットに、デバイスのセキュリティ グループ番号が含まれている SGT をタグ付けします。タグ付けされたパケットはネットワークを通じて CTS ヘッダーで SGT を運びます。SGT は CTS ドメイン全体で送信元の許可を特定する単一ラベルです。SGT には送信元のセキュリティ グループが含まれるため、送信元として特定されます。宛先デバイスには、宛先グループ タグ（DGT）が割り当てられます。

（注） CTS パケット タグには、宛先デバイスのセキュリティ グループ番号は含まれません。

TrustSec SGT の処理：L2 SGT のインポジションと転送の設定方法

TrustSec SGT の処理：インターフェイスでの L2 SGT のインポジションと転送の手動による有効化

次の手順を実行して、Cisco TrustSec（CTS）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播するパケット内のセキュリティ グループ タグ（SGT）を追加し、スタティック認証ポリシーを実装できます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface** {**GigabitEthernet***port* | **Vlan***number*}
4. **cts manual**
5. **policy static sgt** *tag* [**trusted**]
6. **end**
7. **show cts interface** [**GigabitEthernet***port* | **Vlan***number* | **brief** | **summary**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**interface** {**GigabitEthernet***port* | **Vlan***number*} 例： `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。

	コマンドまたはアクション	目的
ステップ 4	**cts manual** 例： `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。
ステップ 5	**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 6	**end** 例： `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。
ステップ 7	**show cts interface** [**GigabitEthernet***port* | **Vlan***number* | **brief** | **summary**] 例： `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。

例：

次は、**show cts interface brief** コマンドの出力例です。

Cisco ASR 1000 シリーズ アグリゲーション サービス ルータとシスコ クラウド サービス ルータ 1000V シリーズ

```
Device# show cts interface brief

Global Dot1x feature is Disabled
 Interface GigabitEthernet0/1/0:
     CTS is enabled, mode:    MANUAL
     IFC state:               OPEN
     Interface Active for 00:00:40.386
     Authentication Status:   NOT APPLICABLE
         Peer identity:       "unknown"
         Peer's advertised capabilities: ""
     Authorization Status:    NOT APPLICABLE
     SAP Status:              NOT APPLICABLE
     Propagate SGT:           Enabled
     Cache Info:
         Cache applied to link : NONE
```

『Cisco 4400 Series Integrated Services Routers』

```
Device# show cts interface brief

Interface GigabitEthernet0/1/0
    CTS is enabled, mode:     MANUAL
      Propagate SGT:          Enabled
      Static Ingress SGT Policy:
        Peer SGT:             100
        Peer SGT assignment:  Trusted
```

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。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface** {**GigabitEthernet***port* | **Vlan***number*}
4. **cts manual**
5. **no propagate sgt**
6. **end**
7. **show cts interface** [**GigabitEthernet***port* | **Vlan***number* | **brief** | **summary**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**interface** {**GigabitEthernet***port* | **Vlan***number*} 例： `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。
ステップ 4	**cts manual** 例： `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。

	コマンドまたはアクション	目的
ステップ 5	**no propagate sgt** 例： `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。 （注） 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** コマンドが開始されると、SGT タグは L2 ヘッダーに追加できなくなります。
ステップ 6	**end** 例： `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。

ステップ 7	**show cts interface** [**GigabitEthernet***port* | **Vlan***number* | **brief** | **summary**]
	
	例：
	
	`Device# show cts interface brief`
	`Global Dot1x feature is Disabled`
	`Interface GigabitEthernet0:`
	`  CTS is enabled, mode:  MANUAL`
	`  IFC state:  OPEN`
	`  Authentication Status:  NOT APPLICABLE`
	
	`  Peer identity:  "unknown"`
	`  Peer's advertised capabilities: ""`
	
	`  Authorization Status:  NOT APPLICABLE`
	
	`  SAP Status:  NOT APPLICABLE`
	
	`  Propagate SGT:  Disabled`
	`  Cache Info:`
	`  Cache applied to link : NONE`
		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。

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
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

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
★枠で囲まれた Technical Assistance の場合★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

TrustSec SGT の処理：L2 SGT のインポジションと転送の機能情報

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 *2*：*TrustSec SGT* の処理：*L2 SGT* のインポジションと転送の機能情報

機能名	リリース	機能情報
TrustSec SGT の処理：L2 SGT のインポジションと転送		この機能により、ルータのインターフェイスは CTS を手動で有効化できるようになるため、ルータはセキュリティ グループ タグ（SGT）を、CTS ヘッダー内でネットワーク全体に運ばれるパケットに挿入できます。 次のコマンドが導入または変更されました：**cts manual**、**policy static sgt**、**propagate sgt**、**show cts interface**。

第 4 章

SXPv4 を使用した Cisco TrustSec

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 つです。CTS SXP バージョン 4（SXPv4）は、ネットワークの古いバインディングを防ぐため、ループ検出メカニズムを追加することで、SXP の機能を強化しました。さらに、SXPv4 を使用した Cisco TrustSec は、SGT インライン タギングをサポートしているため、クリアテキスト（暗号化されていない）イーサネット パケットに組み込まれた SGT の伝達が可能になります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

SXPv4 を使用した Cisco TrustSec に関する情報

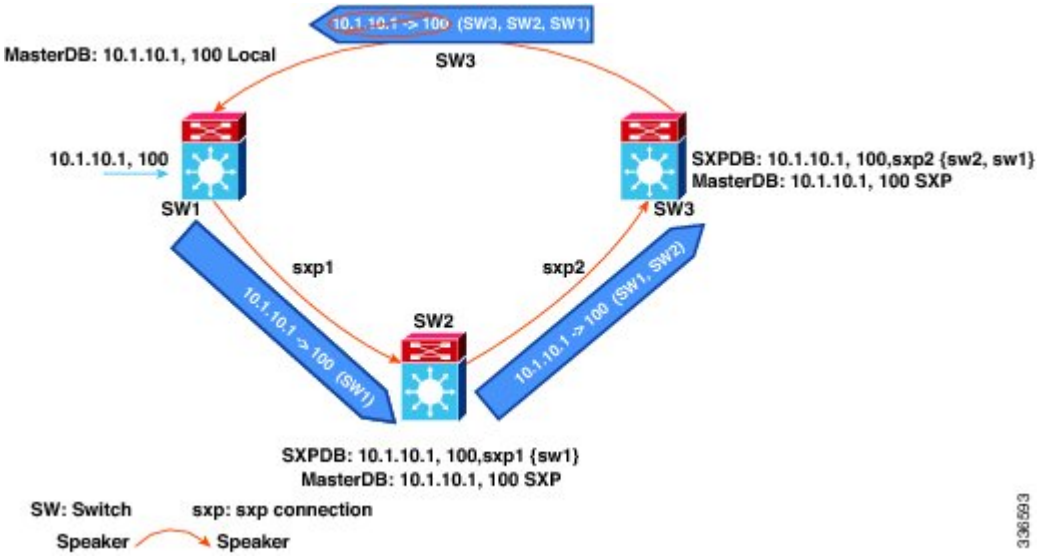
SXPv4 を使用した Cisco TrustSec の概要

Cisco TrustSec（CTS）セキュリティ グループ タグ（SGT）交換プロトコル（SXP）（CTS-SXP）は、ネットワーク デバイス間で IP アドレスとセキュリティ グループ タグ（SGT）のバインド情報を伝播する制御プロトコルです。SGT 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。

SXP 接続は有効化できます。1 つのスイッチによって SXP 接続に転送されるバインドは、別の SXP 接続から受信できるため、SXP 接続がループします。ただし、SXP ループ トポロジは、ネットワーク内の古いバインドになる可能性があります。SXPv4 に組み込まれたループの検出と防止メカニズムは、SXP ノード間にループがある場合は必ず古いバインドの問題を解決します。

ループ防止は、バインドの伝播（追加/削除）時に SXP 伝播パス情報を追加することで実現されます。伝播パス情報は、バインドが順次移動するネットワーク デバイスを（それらのノード ID によって）記録します。ループした SXP 接続があるネットワーク内で関係するすべてのノードでは、正常に動作するため、SXPv4 を実行する必要があります。ループ検出は、SXPv4 の必須機能です。

図 *3*：*SXPv4* ループ検出



上記の図では、3 つのネットワーク デバイス、SW1、SW2、SW3 があります。また、3 つの SXP 接続、SXP1、SXP2、SXP3 があり、合わせて SXP 接続ループを作成しています。バインド（10.1.10.1, 100）は、ローカル認証を通じて SW1 から学習されました。このバインドは、SW1 によってパス情報（つまり、バインドの転送元である SW1）とともに SW2 にエクスポートされました。

バインドを受信すると、SW2 はそれを SW3 にエクスポートし、再度パス情報（SW2、SW1）を先頭に追加します。同様に、SW3 はこのバインドにパス情報である SW3、SW2、SW1 を付けて SW1 に転送します。SW1 がこのバインドを受信すると、パス情報がチェックされます。自身のパス属性が受信したバインド更新内にある場合、伝播ループが検出されます。このバインドは廃棄され、SXP バインド データベースには保存されません。

バインドが SW1 から削除されると（たとえば、ユーザがログオフすると）、バインド検出イベントが送信されます。削除イベントは、上記と同じパスをたどります。これが SW1 に到達しても、そのようなバインドは SW1 バインド データベースには存在しないため、何の対応も行われません。

ループ検出は、バインドがバインドデータベースに追加される前に SXP によって受信されると実行されます。

SXP ノード ID

SXP ノード ID は、ネットワーク内の個別デバイスを特定するために使用されます。ノード ID は、ユーザが設定できる 4 オクテットの整数です。ユーザが設定しない場合、SXP は、EIGRP がそのノード ID を生成するのと同じ方法で、デフォルトの VRF ドメイン内で最高の IPv4 アドレスを使用してノード ID 自体を選択します。ノード ID は、SXP ループ検出を有効化するために SXP 接続が横断するネットワーク内で一意である必要があります。

SXP ループ検出メカニズムは、ピア シーケンス属性内でのその固有ノード ID の検出に基づいて、バインド伝播パケットを破棄します。ループ検出実行中の SXP ネットワーク内でノード ID を変更すると、SXP ループ検出機能が破損する可能性があるため、取り扱いには注意が必要です。

元のノード ID と関連付けされたバインドは、新しいノード ID を設定する前に、すべての SXP ノードから削除する必要があります。これは、ノード ID を変更するネットワーク デバイスで SXP 機能を無効化することで実行できます。

（注） SXP 機能を無効化すると、デバイス上のすべての SXP 接続がダウンします。

ノード ID を変更する前に、パス属性内に特定のノード ID を指定して伝播される SXP バインドが削除されるまで待機します。

（注） syslog は、ノード ID を変更すると生成されます。

SXPv4 とのキープアライブおよびホールド時間ネゴシエーション

SXP はTCP ベースのキープアライブ メカニズムを使用して、接続が存続しているかどうかを判断します。SXPv4 は、接続損失をさらに予想しやすくしてタイムリーに検出するため、プロトコル内のオプションのネゴシエーション済みキープアライブ メカニズムを追加します。

SXP 接続は、SXP スピーカーから SXP リスナーに送信されるほぼすべてのプロトコル メッセージと非対称です（open/open_resp メッセージ エラーメッセージを除く）。SXP リスナーは、接続から学習したすべてのバインド情報を含め、大量になる可能性のあるボリュームの状態を接続単位で維持できます。したがって、キープアライブ メカニズムを持ち、リスナーがスピーカーとの接続損失を検出できるようにすることは有意義です。

このメカニズムは、2 つのタイマーに基づきます。

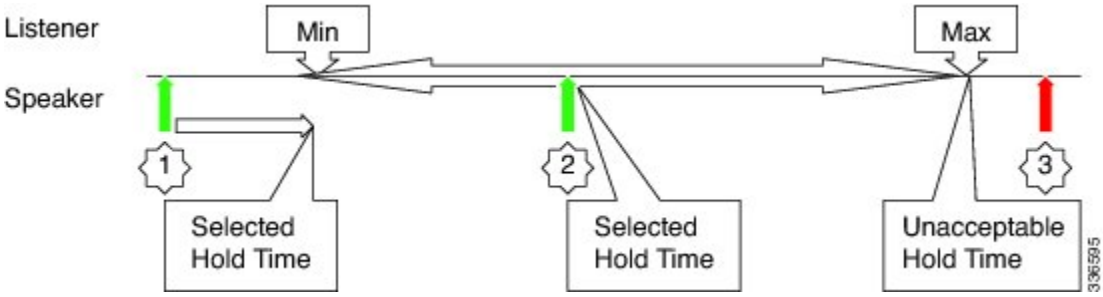
- ホールド タイマー：リスナーが使用して、スピーカーからの連続したキープアライブ/更新メッセージなしで、経過時間を検出します。
- キープアライブ タイマー：スピーカーが使用して、更新メッセージによって他の情報がエクスポートされないインターバル期間にキープアライブ メッセージのディスパッチをトリガーします。

キープアライブ メカニズムのホールド時間は、接続設定時の open/open_resp 交換中にネゴシエートされる場合があります。ネゴシエーション中は次の問題が重要になります。

- リスナーは、ローカル設定されたホールド時間を望ましい範囲内にするか、デフォルトの 90 ～ 180 秒にすることができます。値 0xFFFF..0xFFFF は、キープアライブ メカニズムが使用されていないことを示します。
- スピーカーは、ローカル設定されたホールド時間を最小許容にするか、デフォルトの 120 秒にすることができます。これは、スピーカーが接続を維持するためのキープアライブ メッセージを送信する最短期間です。ホールド時間の期間を短くすると、スピーカーがサポートできるレートよりも速いキープアライブ レートにする必要があります。
- 値 0xFFFF は、キープアライブ メカニズムが使用されていないことを示します。
- ネゴシエーションは、スピーカーの最小許容ホールド時間がリスナー望ましいホールド時間よりも小さいか、その範囲内にある場合は成功します。一方の端でキープアライブ メカニズムがオフになった場合、ネゴシエーションを成功させるには、他の端でもオフにする必要があります。
- ネゴシエーションは、スピーカーの最小許容ホールド時間がリスナーのホールド時間の上限よりも大きいと失敗します。
- 正常なネゴシエーションのために選択するホールド時間は、スピーカーの最小許容ホールド時間の最大値であり、リスナーのホールド範囲の下限になります。

- 異なるキープアライブ時間がローカルで設定されていない限り、スピーカーは、キープアライブ時間を選択したホールド時間の 1/3 とデフォルトで計算します。

図 *4*：ホールド時間ネゴシエーション プロセス



上記の図は、ホールド時間ネゴシエーション プロセスを示します。リスナーおよびスピーカーのロールの詳細は、以下のとおりです。

リスナーが開始する接続

- リスナーには、ホールド時間に設定された範囲に設定された最小値および最大値を持つ、オープン メッセージのホールド時間属性が含まれる場合があります。0xFFFF0 に設定された最小値のみを持つホールド時間属性は、スピーカーにキープアライブ メカニズムが使用されていないことを示します。
- オープン メッセージを受信したスピーカーは、次のように対応します。
  - ホールド時間属性がないか、0xFFFF0 に設定された最小値を含む場合、スピーカーはそのキープアライブ時間を、キープアライブ メカニズムが無効であることを示す 0xFFFF0 に設定します。
  - 受信したホールド時間属性に有効な範囲が含まれている場合、スピーカーには、ホールド時間属性を次のように最小値に設定した open_resp メッセージを含む必要があります。
    - スピーカーがキープアライブ メカニズムをサポートしないか、メカニズムはサポートされているがローカル設定によって無効な場合は 0xFFFF0 に設定します。これにより、キープアライブ時間は 0xFFFF0 に設定されます。koreha
    - スピーカーの最小許容ホールド時間値が、指定された範囲の上限よりも大きい場合、スピーカーは、サブコードを「Unacceptable hold-time」に設定したオープン エラー メッセージを送信し、接続を終了する必要があります。それ以外の場合、スピーカーは選択したホールド時間を、その最小許容ホールド時間値の最小値であり指定されたホールド時間範囲の下限に設定します。
    - スピーカーは、そのキープアライブ時間の新しい値を、選択したホールド時間の 1/3 として計算します。
    - スピーカーは、ホールド時間属性の最小ホールド時間値を選択したホールド時間に設定します。

- スピーカーから open_resp メッセージを受信したリスナーは、ホールド時間属性を検索します。
  - ホールド時間属性が存在し、最小ホールド時間値 0xFFFF0 が含まれている場合、スピーカーはそのホールド時間値を、キープアライブ メカニズムが使用されていないことを示す 0xFFFF0 に設定します。
  - 最小ホールド時間値がリスナーが指定する範囲内にある場合、リスナーはそのホールド時間を、open_resp メッセージ内で受信した選択した値に設定します。
  - 最小ホールド時間値が指定された範囲外の場合、リスナーはサブコードが「Unacceptable hold-time」に設定されたオープン エラー メッセージを送信し、接続を終了します。

スピーカーが開始する接続

- スピーカーには、最小値をその最小受容ホールド期間に設定した、オープン メッセージにホールド時間属性が含まれる場合があります。0xFFFF0 の最小値のみを持つホールド時間属性は、リスナーにキープアライブ メカニズムが使用されていないことを示します。
- オープン メッセージを受信したリスナーは、次のように対応します。
  - ホールド時間属性がないか、0xFFFF0 に設定された最小値を含む場合、リスナーはそのホールド時間を、キープアライブ メカニズムが無効であることを示す 0xFFFF0 に設定します。
  - 受信したホールド時間属性に有効な値が含まれている場合、スピーカーには、ホールド時間属性を次のように最小値に設定した open_resp メッセージを含む必要があります。
    - リスナーがキープアライブ メカニズムをサポートしないか、メカニズムはサポートされているがローカル設定によって無効な場合は 0xFFFF0 に設定します。これにより、キープアライブ時間は 0xFFFF0 に設定されます。
    - 受信したホールド時間値が、リスナーの設定されたホールド時間範囲の上限よりも大きい場合、スピーカーは、サブコードを「Unacceptable hold-time」に設定したオープン エラー メッセージを送信し、接続を終了する必要があります。
    - 受信したホールド時間値が、リスナーの設定されたホールド時間範囲内にある場合、リスナーはそれを選択したホールド時間として設定します。
    - 受信したホールド時間値が、リスナーの設定されたホールド時間範囲の下限よりも小さい場合、リスナーは選択したホールド時間を、そのホールド時間範囲の下限に設定します。
    - リスナーは、ホールド時間属性の最小ホールド時間値を選択したホールド時間に設定します。

- リスナーから open_resp メッセージを受信したスピーカーは、ホールド時間属性を検索します。

- ホールド時間属性が存在し、最小ホールド時間値 0xFFFF0 が含まれている場合、スピーカーはそのホールド時間値を、キープアライブ メカニズムが使用されていないことを示す 0xFFFF0 に設定します。
- 受信したホールド時間値がスピーカーの最小受容ホールド時間よりも大きいか等しい場合、スピーカーは、キープアライブ時間の新しい値を受信したホールド時間の 1/3 として計算します。
- 受信したホールド時間値が最小受容値よりも小さい場合、スピーカーは、サブコードを「Unacceptable hold-time」に設定したオープン エラー メッセージを送信して接続を終了する必要があります。

SGT インライン タギング

CTS ドメイン内の各セキュリティ グループは、「セキュリティ グループ タグ」（SGT）と呼ばれる一意の 16 ビット タグが割り当てられます。SGT はネットワーク全体で送信元の権限を示す単一ラベルです。これは、ネットワーク ホップ間で順番に伝搬され、任意の中間デバイス（スイッチ、ルータ）はこれによってアイデンティティ タグに基づいたポリシーを適用できます。

CTS 対応デバイスには、MAC（L2）レイヤ内に組み込まれた SGT を持つパケットを送受信できる、ハードウェア機能が組み込まれています。この機能は、「L2-SGT インポジション」と呼ばれます。これにより、デバイスのイーサネット インターフェイスで L2-SGT インポジションを有効にできるため、そのデバイスはネクスト ホップ イーサネット ネイバーに運ばれるパケット内に SGT を挿入できるようになります。SGT-over-Ethernet は、クリアテキスト（非暗号化）イーサネット パケットに組み込まれた SGT のホップバイホップの伝達方式です。インライン アイデンティティ伝達はスケーラブルで、ほぼラインレートのパフォーマンスを提供し、コントロール プレーンのオーバーヘッドを防ぎます。

SXPv4 機能を備えた Cisco TrustSec は、CTS メタ データ（CMD）ベースの L2-SGT をサポートします。パケットが CTS 対応インターフェイスに入力されると、IP-SGT マッピング データベース（SXP によって構築されたダイナミック エントリや設定コマンドによって構築されたスタティック エントリがある）が分析され、パケットの送信元 IP アドレスに対応する SGT が学習されます。この SGT はパケットに挿入され、CTS ヘッダー内でネットワーク全体に運ばれます。

このタグは、送信元のグループを表しているので、送信元グループ タグ（SGT）としても参照されます。ネットワークの出力エッジでは、パケットの宛先に割り当てられたグループが既知になります。この時点で、アクセス制御を適用できます。CTS を使用すると、セキュリティ グループ アクセス コントロール リスト（SGACL）と呼ばれるアクセス コントロール ポリシーがセキュリティ グループ間で定義されます。任意のパケットから見れば、これは単純にセキュリティ グループから送信され、別のセキュリティ グループに送信されています。

SXPv4 を使用した Cisco TrustSec の設定方法

ネットワーク デバイス上の SXPv4 プロトコルのホールド時間の設定

ホールド時間はネットワーク デバイスでグローバルに設定でき、これはデバイス上で設定されたすべての SXP 接続に適用されます。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **cts sxp listener hold-time***minimum-period maximum-period*
4. **cts sxp speaker hold-time** *minimum-period*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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 listener hold-time***minimum-period maximum-period* 例： `Device(config)# cts sxp listener hold-time 750 1500`	リスナー デバイス用の最小および最大受容ホールド時間を秒単位で設定します。有効な範囲は 1 ～ 65534 です。リスナー用のデフォルト ホールド時間の範囲は 90 ～ 180 秒です。 （注） *maximum-period* 値は、*minimum-period* 値よりも大きいか等しくする必要があります。
ステップ 4	**cts sxp speaker hold-time** *minimum-period* 例： `Device(config)# cts sxp speaker hold-time 950`	スピーカー デバイス用の最小受容ホールド時間を秒単位で設定します。有効な範囲は 1 ～ 65534 です。スピーカー用のデフォルト ホールド時間は 120 秒です。

接続ごとの SXPv4 プロトコルのホールド時間の設定

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。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ctssxpconnectionpeer***ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} [[**listener** | **speaker**] [**hold-time** *minimum-period maximum-period*] [**vrf***vrf-name*]]
4. **exit**
5. **showctssxp** {**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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# 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	**ctssxpconnectionpeer***ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} [[**listener** | **speaker**] [**hold-time** *minimum-period maximum-period*] [**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。

	コマンドまたはアクション	目的
		• **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。 **hold-time** キーワードでは、スピーカーまたはリスナー デバイスのホールド時間の長さを指定できます。 （注） **hold-time** *maximum-period* 値は、次のキーワード（**peer speaker** および **local listener**）を使用する場合のみ必要です。その他のインスタンスでは、**hold-time** *minimum-period* 値のみが必要です。 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(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。
ステップ 5	**showctssxp** {**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。

ネットワーク デバイスのノード ID の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cts sxp node-id** {*sxp-node-id* | **interface** *interface-type* | *ipv4-address*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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 node-id** {*sxp-node-id* | **interface** *interface-type* | *ipv4-address*} 例： `Device(config)# cts sxp node-id 172.16.1.3`	ネットワーク デバイスのノード ID を設定します。

SGT インライン タギングの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface** {**gigabitethernet** *port* | **vlan***number*}
4. **cts manual**
5. **propagate sgt**
6. **policy static sgt** *tag* [**trusted**]
7. **end**
8. **show cts interface brief**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Device> enable`	• 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	**interface** {**gigabitethernet** *port* | **vlan***number*} 例： `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。
ステップ 4	**cts manual** 例： `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 モードを開始します。
ステップ 5	**propagate sgt** 例： `Device(config-if-cts-manual)# propagate sgt`	インターフェイスでの CTS SGT 伝達を無効化します。 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ない状況（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しない場合）で使用します。
ステップ 6	**policy static sgt** *tag* [**trusted**] 例： `Device(config-if-cts-manual)# policy static sgt 77`	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。 （注） **trusted** キーワードは、そのインターフェイスが CTS 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。
ステップ 7	**end** 例： `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。

	コマンドまたはアクション	目的

ステップ 8	**show cts interface brief**
	
	例：
	
	`Device# show cts interface brief`
	
	`Interface GigabitEthernet0/0`
	`  CTS is enabled, mode:  MANUAL`
	`  Propagate SGT:  Enabled`
	`  Peer SGT assignment:  Trusted`
	
	`Interface GigabitEthernet0/1`
	`  CTS is enabled, mode:  MANUAL`
	`  Propagate SGT:  Disabled`
	`  Peer SGT assignment:  Untrusted`
	
	`Interface GigabitEthernet0/3`
	`  CTS is disabled.`
		インターフェイスの CTS 設定の統計情報を表示します。

SXPv4 を使用した Cisco TrustSec の設定例

例：SXPv4 を使用した Cisco TrustSec の設定

ネットワーク デバイス上の SXPv4 プロトコルのホールド時間の設定

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

接続ごとの SXPv4 プロトコルのホールド時間の設定

```
Device(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
hold-time 500
```

ネットワーク デバイスのノード ID の設定

```
Device(config)# cts sxp node-id 172.16.1.3
```

SXPv4 を使用した Cisco TrustSec の確認

デバイス上の SXP 接続の表示

```
Device# show cts sxp connection

 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 not running
---------------------------------------------
Peer IP          : 2.2.2.1
Source IP        : 2.2.2.2
Conn status      : On
Conn version     : 4
Conn capability  : IPv4-IPv6-Subnet
Conn hold time   : 0 seconds
Local mode       : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: default SXP password
Duration since last state change: 32:00:41:31 (dd:hr:mm:sec)


Total num of SXP Connections = 1
```

現在の CST-SGT マップ データベースの表示

SXPv4 では、SXP ノード ID が表示されます。

```
Device# show cts sxp sgt-map

SXP Node ID(generated):0x02020202(2.2.2.2)
IP-SGT Mappings as follows:
IPv4,SGT: <2.2.2.0/29 , 29>
source  : SXP;
Peer IP : 2.2.2.1;
Ins Num : 1;
Status  : Active;
Seq Num : 3
Peer Seq: 0B0B0B02,
IPv4,SGT: <12.12.133.1 , 12>
source  : SXP;
Peer IP : 2.2.2.1;
Ins Num : 1;
Status  : Active;
Seq Num : 5
Peer Seq: 0B0B0B02,
Total number of IP-SGT Mappings: 2
```

例：SGT 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 CTS 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 0
Device(config-if)# cts manual
Device(config-if-cts-manual)# propagate sgt
Device(config-if-cts-manual)# policy static sgt 77 trusted
```

SXPv4 を使用した Cisco TrustSec 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
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
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』

MIB

MIB	MIB のリンク
CISCO-TRUSTSEC-SXP-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、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
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

SXPv4 を使用した Cisco TrustSec 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 *3*：*SXPv4* を使用した *Cisco TrustSec* の機能情報

機能名	リリース	機能情報
SXPv4 を使用した Cisco TrustSec	Cisco IOS XE Release 3.9S	CTS SXP バージョン 4（SXPv4）は、ネットワークの古いバインディングを防ぐため、ループ検出および防止メカニズムを追加することで、SXP の機能を強化しました。さらに、SXPv4 を使用した Cisco TrustSec は、SGT インラインタギングをサポートしているため、クリア テキスト（暗号化されていない）イーサネットパケットに組み込まれた SGT の伝達が可能になります。 この機能は、Cisco IOS XE リリース 3.9S で、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 次のコマンドが導入されました。 **cts sxp listener hold-time**、**cts sxp node-id**、**cts sxp speaker hold-time**。

第 5 章

双方向 SXP サポートの有効化

双方向 SXP サポート機能は、セキュリティ グループ タグ（SGT）交換プロトコル（SXP）バインドのサポートを追加することで、SXP バージョン 4 を使用した Cisco TrustSec の機能を強化します。このバインドは、単一の接続でスピーカーとリスナーどちらの方向へも伝播できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

双方向 SXP サポートの前提条件

- Cisco TrustSec がデバイス上に設定されていること。詳細については、『*Cisco TrustSec Configuration Guide*』の「Cisco TrustSec Support for IOS」の章を参照してください。

双方向 SXP サポートの制約事項

- 接続のそれぞれの端のピアは、**both** キーワードを使用して双方向接続として設定する必要があります。一方の端を **both** キーワードを使用した双方向接続として設定し、他方の端をスピーカーまたはリスナーとして設定（単方向接続）するのは、誤った設定です。

双方向 SXP サポートに関する情報

双方向 SXP サポートの概要

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ます。データを生成するピアはスピーカーで、対応するピアはリスナーになります。

双方向セキュリティ グループ タグ（SGT）交換プロトコル（SXP）の設定をサポートすることで、ピアはスピーカーとリスナーのどちらとしても動作し、単一の接続を使用する双方向の SXP バインドを伝播できるようになります。

双方向 SXP の設定は、IP アドレスのペア 1 組と管理されます。いずれかの端で、SXP 接続を開始するのはリスナーのみであり、スピーカーは着信接続を受け入れます。

図 *5*：双方向 *SXP* 接続

さらに、SXP バージョン 4（SXPv4）は、引き続きループ検出メカニズムをサポートしています（ネットワークの古いバインディングを防ぐため）。

双方向 SXP サポートを有効化する方法

双方向 SXP サポートの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ctssxpenable**
4. **ctssxpdefaultpassword**
5. **ctssxpdefaultsource-ip**
6. **cts sxp connection peer***ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} **both** [**vrf***vrf-name*]
7. **cts sxpspeakerhold-time***minimum-period*
8. **cts sxplistenerhold-time***minimum-periodmaximum-period*
9. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**ctssxpenable** 例： `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）をネットワーク デバイスで有効にします。
ステップ 4	**ctssxpdefaultpassword** 例： `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。

	コマンドまたはアクション	目的
ステップ 5	**ctssxpdefaultsource-ip** 例： `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。
ステップ 6	**cts sxp connection peer***ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} **both** [**vrf***vrf-name*] 例： `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。 • **both**：デバイスが双方向 SXP 接続のスピーカーとリスナー両方であることを指定します。 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。
ステップ 7	**cts sxpspeakerhold-time***minimum-period* 例： `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。

	コマンドまたはアクション	目的
ステップ 8	**cts sxplistenerhold-time***minimum-periodmaximum-period* 例： `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。 （注） *maximum-period* 値は、*minimum-period* 値よりも大きいか等しくする必要があります。
ステップ 9	**exit** 例： `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。

双方向 SXP サポート設定の確認

手順の概要

1. イネーブル化
2. **showctssxp** {**connections** | **sgt-map**} [**brief** | **vrf***vrf-name*]

手順の詳細

ステップ 1 イネーブル化

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 **showctssxp** {**connections** | **sgt-map**} [**brief** | **vrf***vrf-name*]

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。

例：

```
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)


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。

表 *4*：接続ステータスの出力シナリオ

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（スピーカー） オン（リスナー）
スピーカー	リスナー	オン	オン
リスナー	スピーカー	オン	オン

双方向 SXP サポートの設定例

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 に接続するよう設定する方法を示します。

```
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
```

双方向 SXP サポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
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』

関連項目	マニュアル タイトル
Cisco TrustSec の設定	『*Cisco TrustSec Configuration Guide*』の「Cisco TrustSec Support for IOS」の章

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

双方向 SXP サポートの機能情報

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 *5*：双方向 *SXP* サポートの機能情報

機能名	リリース	機能情報
双方向 SXP サポート		双方向 SXP サポート機能は、セキュリティ グループ タグ（SGT）交換プロトコル（SXP）バインドのサポートを追加することで、SXP バージョン 4 を使用した Cisco TrustSec の機能を強化します。このバインドは、単一の接続でスピーカーとリスナーどちらの方向へも伝播できます。 次のコマンドが導入または変更されました：**cts sxp connection peer**。

第 6 章

Cisco TrustSec インターフェイスと SGT のマッピング

Cisco TrustSec インターフェイスと SGT のマッピング機能は、レイヤ 3 入力インターフェイス上のすべてのトラフィックを、セキュリティ グループ タグ（SGT）にバインドします。このマッピングを実装すると、Cisco TrustSec では、SGT を使用してさまざまな論理レイヤ 3 入力インターフェイスからトラフィックを分離できるようになります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

Cisco TrustSec インターフェイスと SGT のマッピングに関する情報

インターフェイスと SGT のマッピング

インターフェイスとセキュリティ グループ タグ（SGT）間のマッピングを使用して、基盤となる物理インターフェイスに関わらず、SGT を次の論理レイヤ 3 入力インターフェイスいずれかのトラフィックにマッピングします。

- レイヤ 3（ルーテッド）イーサネット インターフェイス
- レイヤ 3（ルーテッド）イーサネット 802.1Q サブインターフェイス
- トンネル インターフェイス

設定された SGT タグは、レイヤ 3 入力インターフェイスのすべてのトラフィックに割り当てられ、インライン タギングとポリシーの適用に使用できます。

バインディング送信元プライオリティ

Cisco TrustSec は完全優先方式で IP-SGT（IP アドレスからセキュリティ グループ タグへ）バインディング ソース間の競合を解決します。現在の優先順位の適用順序は、最小から最大まで、次のとおりです。

1. CLI：**cts role-based sgt-map sgt** コマンドを使用して設定されたバインド。
2. L3IF：一貫した L3IF-SGT（レイヤ 3 インターフェイスから SGT へ）マッピングやアイデンティティ ポート マッピングを使用する 1 つ以上のインターフェイスを通るパスを持つ FIB 転送エントリが原因で追加されたバインド。
3. SXP：SXP（SGT Exchange Protocol）ピアから学習されたバインド。
4. INTERNAL：ローカルで設定された IP アドレスとデバイス独自の SGT 間のバインド。

Cisco TrustSec インターフェイスと SGT のマッピングの設定方法

レイヤ 3 インターフェイスと SGT のマッピングの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***typeslot/port*
4. **cts role-based sgt-map sgt***sgt-number*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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	**interface***typeslot/port* 例： `Device(config)# interface gigabitEthernet 0/0`	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 4	**cts role-based sgt-map sgt***sgt-number* 例： `Device(config-if)# cts role-based sgt-map 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。 • *sgt-number*：セキュリティ グループ タグ（SGT）番号を指定します。有効値は 2 ～ 65519 です。
ステップ 5	**end** 例： `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。

レイヤ 3 インターフェイスと SGT のマッピングの確認

手順の概要

1. イネーブル化
2. **show cts role-based sgt-map all**

手順の詳細

ステップ 1 イネーブル化

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 **show cts role-based sgt-map all**

レイヤ 3 インターフェイスの入力トラフィックに対するセキュリティ グループ タグ（SGT）マッピングを表示します。

例：

次は、**show cts role-based sgt-map all** コマンドからの出力例です。Cisco TrustSec インターフェイス と SGT のマッピング機能が実装されると、入力インターフェイスのトラフィックは、レイヤ 3 インターフェイス（L3IF）によって適切にタグ付けされます。この出力では、IP アドレスからセキュリティ グループ タグ（IP-SGT）バインディング ソースの優先方式を表示します（IP-SGT バインディング ソースの優先度について、詳細は「バインディング送信元プライオリティ」の項を参照）。

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

IP Address              SGT     Source
=========================================
192.0.2.1               4       INTERNAL
192.0.2.5/24            3       L3IF
192.0.2.10/8            3       L3IF
192.0.2.20              5       CLI
198.51.100.1            4       INTERNAL
IP-SGT Active Bindings Summary
=========================================
Total number of CLI      bindings = 1
Total number of L3IF     bindings = 2
Total number of INTERNAL bindings = 2
Total number of active   bindings = 5
```

Cisco TrustSec インターフェイスと SGT のマッピングの設定例

例：レイヤ 3 インターフェイスと SGT のマッピングの設定

次の例は、レイヤ 3 入力インターフェイスへのセキュリティ グループ タグ（SGT）のマッピング設定を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet 0/0
Device(config-if)# cts role-based sgt-map sgt 77
Device(config-if)# end
```

Cisco TrustSec インターフェイスと SGT のマッピングに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
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 と SXP の設定	『Cisco TrustSec スイッチ コンフィギュレーション ガイド』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ 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 インターフェイスと SGT のマッピングの機能情報

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 *6*：*Cisco TrustSec* インターフェイスと *SGT* のマッピングの機能情報

機能名	リリース	機能情報
Cisco TrustSec インターフェイスと SGT のマッピング		Cisco TrustSec インターフェイスと SGT のマッピング機能は、レイヤ 3 入力インターフェイス上のすべてのトラフィックを、セキュリティ グループ タグ（SGT）にバインドします。このマッピングを実装すると、Cisco TrustSec では、SGT を使用してさまざまな論理レイヤ 3 入力インターフェイスからトラフィックを分離できるようになります。 次のコマンドが導入または変更されました：**cts role-based sgt-map sgt**。

第 7 章

Cisco TrustSec サブネットと SGT のマッピング

サブネットとセキュリティ グループ タグ（SGT）のマッピングは、指定したサブネット内のすべてのホストアドレスに SGT をバインドします。このマッピングが実行されると、Cisco TrustSec により、指定のサブネットに属する送信元 IP アドレスを持つ任意の着信パケットに SGT が課せられます。

第 8 章

Cisco TrustSec フィールドの Flexible NetFlow エクスポート

Cisco TrustSec フィールドの Flexible NetFlow エクスポートでは、Flexible Netflow（FNF）フローレコード内の Cisco TrustSec フィールドをサポートし、Cisco TrustSec 導入の標準から外れた動作のモニタ、トラブルシューティング、および特定を支援します。

このモジュールでは、Cisco TrustSec と FNF のインタラクションについてと、NetFlow バージョン 9 フロー レコードの Cisco TrustSec フィールドを設定しエクスポートする方法を説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

Cisco TrustSec フィールドの Flexible NetFlow エクスポートの制約事項

- Flexible Netflow（FNF）レコードでエクスポートされるセキュリティ グループ タグ（SGT）値は、次のシナリオではゼロになります。
  - パケットは、信頼されたインターフェイスから、ゼロの SGT 値とともに受信します。
  - パケットは SGT なしで受信します。
  - IP-SGT ルックアップ中に SGT が検出されません。

Cisco TrustSec フィールドの Flexible NetFlow エクスポートに関する情報

Flexible NetFlow の Cisco TrustSec フィールド

Flexible Netflow（FNF）フロー レコード内の Cisco TrustSec フィールド、送信元セキュリティ グループ タグ（SGT）および宛先セキュリティ グループ タグ（DGT）は、管理者によるフローとアイデンティティ情報の関連付けに役立ちます。ネットワーク エンジニアは、これにより、顧客のネットワーク リソースおよびアプリケーション リソースの利用について詳しく理解できます。この情報を使用して、潜在的なセキュリティやポリシーの違反を検出して解決するために、アクセスおよびアプリケーション リソースを効率的に計画して割り当てることができます。

Cisco TrustSec フィールドは入力/出力 FNF、ユニキャスト/マルチキャスト トラフィックでサポートされています。

次のテーブルに、Cisco TrustSec 用の NetFlow V9 の企業固有フィールド タイプを示します。これは、Cisco TrustSec の送信元/宛先ソース グループ タグの FNF テンプレートで使用されます。

ID	説明
CTS_SRC_GROUP_TAG	Cisco Trusted Security 送信元グループ タグ
CTS_DST_GROUP_TAG	Cisco Trusted Security 宛先グループ タグ

FNF フロー レコードで既存の一致するフィールドに加えて、Cisco TrustSec フィールドが設定されます。次の設定を使用して、Cisco TrustSec フロー オブジェクトをキー フィールドまたは非キー フィールドとして FNF フロー レコードに追加し、パケット用の送信元と宛先のセキュリティ グループ タグを設定します。

- **match flow cts {source | destination} group-tag** コマンドは、キー フィールドとして Cisco TrustSec フィールドを指定するため、フロー レコード以下で設定されます。キー フィールドはフローを差別化するものです。各フローのキー フィールドには、一連の一意の値が設定されています。フロー レコードにキー フィールドが含まれていない場合は、フロー モニタで使用することができません。
- **collect flow cts {source | destination} group-tag** コマンドは、非キー フィールドとして Cisco TrustSec フィールドを指定するため、フロー レコード以下で設定されます。非キー フィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。

フロー レコードは、フロー モニタ下で設定され、フロー モニタはインターフェイスに適用されます。FNF データをエクスポートするには、フローエクスポータを設定し、フローモニタ以下に追加する必要があります。

Cisco TrustSec フィールドの Flexible NetFlow エクスポートの設定方法

フロー レコードのキー フィールドとしての Cisco TrustSec フィールドの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **flow record***record-name*
4. **match** {**ipv4** | **ipv6**} **protocol**
5. **match** {**ipv4** | **ipv6**} **source address**
6. **match** {**ipv4** | **ipv6**} **destination address**
7. **match transport source-port**
8. **match transport destination-port**
9. **match flow direction**
10. **match flow cts source group-tag**
11. **match flow cts destination group-tag**
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**flow record***record-name* 例： `Device(config)# flow record cts-record-ipv4`	Flexible Netflow（FNF）フロー レコードを作成するか、または既存の FNF フロー レコードを変更して、Flexible NetFlow フロー レコード 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	**match {ipv4 | ipv6} protocol** 例： `Device(config-flow-record)# match ipv4 protocol`	（オプション）フロー レコードのキー フィールドとして IPv4 プロトコルまたは IPv6 プロトコルを設定します。
ステップ 5	**match {ipv4 | ipv6} source address** 例： `Device(config-flow-record)# match ipv4 source address`	（オプション）IPv4 または IPv6 送信元アドレスをフローレコードのキー フィールドとして設定します。
ステップ 6	**match {ipv4 | ipv6} destination address** 例： `Device(config-flow-record)# match ipv4 destination address`	（オプション）IPv4 または IPv6 接続先アドレスをフローレコードのキー フィールドとして設定します。
ステップ 7	**match transport source-port** 例： `Device(config-flow-record)# match transport source-port`	（オプション）フロー レコードのキー フィールドとして、トランスポート送信元ポートを設定します。

	コマンドまたはアクション	目的
ステップ 8	**match transport destination-port** 例： `Device(config-flow-record)# match transport destination-port`	（オプション）フロー レコードのキー フィールドとして、トランスポート宛先ポートを設定します。
ステップ 9	**match flow direction** 例： `Device(config-flow-record)# match flow direction`	（オプション）フローがモニタされる方向をキーフィールドとして設定します。
ステップ 10	**match flow cts source group-tag** 例： `Device(config-flow-record)# match flow cts source group-tag`	FNF フロー レコード内の Cisco TrustSec 送信元セキュリティ グループ タグ（SGT）をキー フィールドとして設定します。
ステップ 11	**match flow cts destination group-tag** 例： `Device(config-flow-record)# match flow cts destination group-tag`	FNF フロー レコード内の Cisco TrustSec 宛先セキュリティ グループ タグ（DGT）をキー フィールドとして設定します。
ステップ 12	**end** 例： `Device(config-flow-record)# end`	Flexible NetFlow フロー レコード コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

フロー レコードの非キー フィールドとしての Cisco TrustSec フィールドの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **flow record***record-name*
4. **match** {**ipv4** | **ipv6**} **protocol**
5. **match** {**ipv4** | **ipv6**} **source address**
6. **match** {**ipv4** | **ipv6**} **destination address**
7. **match transport source-port**
8. **match transport destination-port**
9. **collect flow direction**
10. **collect flow cts source group-tag**
11. **collect flow cts destination group-tag**
12. **collect counter packets**
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**flow record***record-name* 例： `Device(config)# flow record cts-record-ipv4`	Flexible Netflow（FNF）フロー レコードを作成するか、または既存の FNF フロー レコードを変更して、Flexible NetFlow フロー レコード 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 4	**match {ipv4 | ipv6} protocol** 例： `Device(config-flow-record)# match ipv4 protocol`	（オプション）フロー レコードのキー フィールドとして IPv4 プロトコルまたは IPv6 プロトコルを設定します。
ステップ 5	**match {ipv4 | ipv6} source address** 例： `Device(config-flow-record)# match ipv4 source address`	（オプション）IPv4 または IPv6 送信元アドレスをフローレコードのキー フィールドとして設定します。
ステップ 6	**match {ipv4 | ipv6} destination address** 例： `Device(config-flow-record)# match ipv4 destination address`	（オプション）IPv4 または IPv6 接続先アドレスをフローレコードのキー フィールドとして設定します。
ステップ 7	**match transport source-port** 例： `Device(config-flow-record)# match transport source-port`	（オプション）フロー レコードのキー フィールドとして、トランスポート送信元ポートを設定します。
ステップ 8	**match transport destination-port** 例： `Device(config-flow-record)# match transport destination-port`	（オプション）フロー レコードのキー フィールドとして、トランスポート宛先ポートを設定します。
ステップ 9	**collect flow direction** 例： `Device(config-flow-record)# collect flow direction`	（オプション）フロー方向を非キーフィールドとして設定し、フローがモニタされた方向の収集を有効化します。
ステップ 10	**collect flow cts source group-tag** 例： `Device(config-flow-record)# collect flow cts source group-tag`	FNF フロー レコード内の Cisco TrustSec 送信元セキュリティ グループ タグ（SGT）を非キー フィールドとして設定します。

	コマンドまたはアクション	目的
ステップ 11	**collect flow cts destination group-tag** 例： `Device(config-flow-record)# collect flow cts destination group-tag`	FNF フロー レコード内の Cisco TrustSec 宛先セキュリティ グループ タグ（DGT）を非キー フィールドとして設定します。
ステップ 12	**collect counter packets** 例： `Device(config-flow-record)# collect counter packets`	（オプション）フローで確認されるパケット数を非キーフィールドとして設定し、フローから合計パケット数を収集します。
ステップ 13	**end** 例： `Device(config-flow-record)# end`	Flexible NetFlow フロー レコード コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

フロー エクスポータの設定

フローエクスポータごとに、1つ宛先のみがサポートされます。複数の宛先にデータをエクスポートする場合は、複数のフロー エクスポータを設定してフロー モニタに割り当てる必要があります。

はじめる前に

フロー レコードを作成していることを確認します。詳細については、「フロー レコードの非キーフィールドとしての Cisco TrustSec フィールドの設定」の項および「フロー レコードの非キーフィールドとしての Cisco TrustSec フィールドの設定」の項を参照してください。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **flow exporter***exporter-name*
4. **destination** {*ip-address* | *hostname*} [**vrf***vrf-name*]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**flow exporter***exporter-name* 例： `Device(config)# flow exporter EXPORTER-1`	フローエクスポータを作成するか、または既存のフローエクスポータを変更して、Flexible NetFlow フローエクスポータ 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	**destination** {*ip-address* | *hostname*} [**vrf***vrf-name*] 例： `Device(config-flow-exporter)# destination 172.16.10.2`	エクスポータの宛先システムの IP アドレスまたはホスト名を指定します。
ステップ 5	**end** 例： `Device(config-flow-exporter)# end`	Flexible NetFlow フロー エクスポータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

フロー モニタの設定

はじめる前に

フローエクスポータをデータエクスポート用のフローモニタに追加するには、フローエクスポータを作成していることを確認します。詳細については、「フローエクスポータの設定」の項を参照してください。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **flow monitor***monitor-name*
4. **record***record-name*
5. **exporter***exporter-name*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**flow monitor***monitor-name* 例： `Device(config)# flow monitor FLOW-MONITOR-1`	フロー モニタを作成するか、または既存のフロー モニタを変更して、Flexible NetFlow フロー モニタ 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	**record***record-name* 例： `Device(config-flow-monitor)# record FLOW-RECORD-1`	フロー モニタのレコードを指定します。
ステップ 5	**exporter***exporter-name* 例： `Device(config-flow-monitor)# exporter EXPORTER-1`	フロー モニタのエクスポータを指定します。
ステップ 6	**end** 例： `Device(config-flow-monitor)# end`	Flexible NetFlow フロー モニタ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

インターフェイスへのフロー モニタの適用

フローモニタをアクティベートするには、フローモニタを1つ以上のインターフェイスに適用する必要があります。

はじめる前に

フローモニタを作成していることを確認します。詳細については、「フローモニタの設定」の項を参照してください。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***type number*
4. {**ip** | **ipv6**} **flow monitor***monitor-name* {**input** | **output**}
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**interface***type number* 例： `Device(config)# interface ethernet 0/0`	インターフェイスを指定し、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。

	コマンドまたはアクション	目的
ステップ 4	{**ip** | **ipv6**} **flow monitor***monitor-name* {**input** | **output**} 例： `Device (config-if)# ip flow monitor FLOW-MONITOR-1 input`	作成済みのフローモニタを、トラフィックの分析対象となるインターフェイスに割り当てることで、そのフローモニタをアクティブにします。
ステップ 5	**end** 例： `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。

Cisco TrustSec フィールドの Flexible NetFlow エクスポートの確認

手順の概要

1. イネーブル化
2. **show flow record***record-name*
3. **show flow exporter***exporter-name*
4. **show flow monitor***monitor-name*
5. **show flow monitor***monitor-name***cache**
6. **show flow interface***type number*

手順の詳細

ステップ 1 イネーブル化

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 **show flow record***record-name*

指定した Flexible Netflow（FNF）フロー レコードの詳細を表示します。

例：

```
Device> show flow record cts-recordipv4

flow record cts-recordipv4:
  Description:        User defined
  No. of users:       1
  Total field space:  30 bytes
  Fields:
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    match interface input
    match interface output
    match flow direction
    match flow cts source group-tag
    match flow cts destination group-tag
    collect counter packets
```

ステップ 3 **show flow exporter***exporter-name*

指定した FNF フロー エクスポータの現在のステータスを表示します。

例：

```
Device> show flow exporter EXPORTER-1

Flow Exporter EXPORTER-1:
  Description:              User defined
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 100.100.100.1
    Source IP address:      3.3.3.2
    Transport Protocol:     UDP
    Destination Port:       2055
    Source Port:            65252
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Used
```

ステップ 4 **show flow monitor***monitor-name*

指定した FNF フロー モニタのステータスと統計情報を表示します。

例：

```
Device> show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:       User defined
  Flow Record:       cts-recordipv4
  Flow Exporter:     EXPORTER-1
  Cache:
    Type:                 normal (Platform cache)
    Status:               allocated
    Size:                 200000 entries
    Inactive Timeout:     60 secs
    Active Timeout:       1800 secs
    Update Timeout:       1800 secs
    Synchronized Timeout: 600 secs
```

```
    Trans end aging:      off
```

ステップ 5 **show flow monitor***monitor-name***cache**

指定した FNF フロー モニタ キャッシュのコンテンツを表示します。

例：

```
Device> show flow monitor FLOW-MONITOR-1 cache

  Cache type:                                Normal
  Cache size:                                4096
  Current entries:                           2
  High Watermark:                            2

  Flows added:                               6
  Flows aged:                                4
    - Active timeout      (1800 secs)        0
    - Inactive timeout    (15 secs)          4
    - Event aged                             0
    - Watermark aged                         0
    - Emergency aged                         0

  IPV4 SOURCE ADDRESS:                       10.1.0.1
  IPV4 DESTINATION ADDRESS:                  172.16.2.0
  TRNS SOURCE PORT:                          58817
  TRNS DESTINATION PORT:                     23
  FLOW DIRECTION:                            Input
  IP PROTOCOL:                               6
  SOURCE GROUP TAG:                          100
  DESTINATION GROUP TAG:                     200
  counter packets:                           10

  IPV4 SOURCE ADDRESS:                       172.16.2.0
  IPV4 DESTINATION ADDRESS:                  10.1.0.1
  TRNS SOURCE PORT:                          23
  TRNS DESTINATION PORT:                     58817
  FLOW DIRECTION:                            Output
  IP PROTOCOL:                               6
  SOURCE GROUP TAG:                          200
  DESTINATION GROUP TAG:                     100
  counter packets:                           8
```

ステップ 6 **show flow interface***type number*

指定したインターフェイスに適用される FNF フロー モニタの詳細を表示します。フロー モニタがインターフェイスに適用されない場合、出力は空になります。

例：

```
Device>  show flow interface GigabitEthernet0/0/3

Interface GigabitEthernet0/0/3
  FNF:  monitor:          FLOW-MONITOR-1
        direction:        Input
        traffic(ip):      on
  FNF:  monitor:          FLOW-MONITOR-1
        direction:        Output
        traffic(ip):      on
```

Cisco TrustSec フィールドの Flexible NetFlow エクスポートの設定例

例：フロー レコードのキー フィールドとしての Cisco TrustSec フィールドの設定

次の例は、Cisco TrustSec フロー オブジェクトを、IPv4 Flexible NetFlow フロー レコードのキー フィールドとして設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# flow record cts-record-ipv4
Device(config-flow-record)# match ipv4 protocol
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# match transport destination-port
Device(config-flow-record)# match flow direction
Device(config-flow-record)# match flow cts source group-tag
Device(config-flow-record)# match flow cts destination group-tag
Device(config-flow-record)# end
```

例：フローレコードの非キーフィールドとしてのCiscoTrustSecフィールドの設定

次の例は、Cisco TrustSec フロー オブジェクトを、IPv4 Flexible NetFlow フロー レコードの非キー フィールドとして設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# flow record cts-record-ipv4
Device(config-flow-record)# match ipv4 protocol
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# match transport destination-port
Device(config-flow-record)# collect flow direction
Device(config-flow-record)# collect flow cts source group-tag
Device(config-flow-record)# collect flow cts destination group-tag
Device(config-flow-record)# collect counter packets
Device(config-flow-record)# end
```

例：フロー エクスポータの設定

```
Device> enable
Device# configure terminal
Device(config)# flow exporter EXPORTER-1
```

```
Device(config-flow-exporter)# destination 172.16.10.2
Device(config-flow-exporter)# end
```

例：フロー モニタの設定

```
Device> enable
Device# configure terminal
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# record FLOW-RECORD-1
Device(config-flow-monitor)# exporter EXPORTER-1
Device(config-flow-monitor)# end
```

例：インターフェイス上のフロー モニタの適用

次の例は、トラフィックを分析するインターフェイスにIPv4フローモニタを適用することで、このフローモニタをアクティベートする方法を示します。IPv6フローモニタをアクティベートするには、**ip** キーワードを **ipv6** キーワードと置き換えます。

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 0/0
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# end
```

Cisco TrustSec フィールドの Flexible NetFlow エクスポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
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』

関連項目	マニュアル タイトル
Flexible NetFlow でのデータ エクスポート	『*Flexible Netflow Configuration Guide*』パブリケーションの「Flexible NetFlow Output Features on Data Export」の章
Flexible NetFlow のフロー レコードとフロー モニタ	『*Flexible Netflow Configuration Guide*』パブリケーションの「Customizing Flexible NetFlow Flow Records and Flow Monitors」の章

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ 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 フィールドの Flexible NetFlow エクスポートの機能情報

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 *7*：***Cisco TrustSec*** フィールドの ***Flexible NetFlow*** エクスポートの機能情報

機能名	リリース	機能情報
Cisco TrustSec フィールドの Flexible NetFlow エクスポート		Cisco TrustSec フィールドの Flexible NetFlow エクスポートでは、Flexible Netflow（FNF）フロー レコード内の Cisco TrustSec フィールドをサポートし、Cisco TrustSec 導入の標準から外れた動作のモニタ、トラブルシューティング、および特定を支援します。 この機能によって次のコマンドが導入されました：**match flow cts {source | destination} group-tag** および **collect flow cts {source | destination} group-tag**。

第 9 章

Cisco TrustSec SGT キャッシング

Cisco TrustSec SGT キャッシング 機能は、セキュリティ グループ タグ（SGT）の移動性を柔軟にする Cisco TrustSec の機能を強化します。この機能は、IP-SGT バインドを特定し、対応する SGT をキャッシュすることで、通常のディープ パケット インスペクションを処理するすべてのネットワーク サービスを通じて、またパケットが該当する SGT で再度タグ付けされるサービス出力ポイントにおいて、ネットワーク パケットを転送します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

Cisco TrustSec SGT キャッシング の制約事項

グローバルなセキュリティ グループ タグ（SGT）キャッシング設定と、インターフェイス固有の入力設定は相互に排他的です。次のシナリオでは、SGTキャッシングをグローバルおよびインターフェイス上の両方で構成しようとした場合に、警告メッセージが表示されます。

- **cts role-based sgt-cache ingress** コマンドをインターフェイス設定モードで使用して、インターフェイスが SGT キャッシングを有効にし、**cts role-based sgt-caching** コマンドを使用してグローバル設定を試行した場合、この例が示すような警告メッセージが表示されます。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet0/0
Device(config-if)# cts role-based sgt-cache ingress
Device(config-if)# exit
Device(config)# cts role-based sgt-caching

There is at least one interface that has ingress sgt caching configured. Please remove
 all interface ingress sgt caching configuration(s) before attempting global enable.
```

- **cts role-based sgt-caching** コマンドを使用してグローバル設定を有効化し、インターフェイス設定モードで **cts role-based sgt-cache ingress** コマンドを使用してインターフェイス設定を試行した場合、次の例が示すような警告メッセージが表示されます。

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-caching
Device(config)# interface gigabitEthernet0/0
Device(config-if)# cts role-based sgt-cache ingress

Note that ingress sgt caching is already active on this interface due to global
sgt-caching enable.
```

Cisco TrustSec SGT キャッシングの詳細

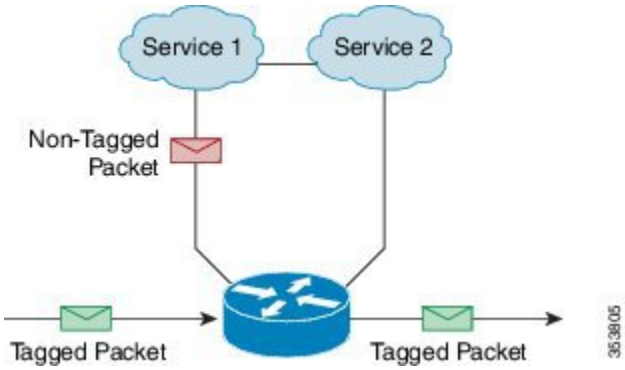
SGT キャッシングを使用した SGT の特定と再適用

Cisco TrustSec は、セキュリティ グループ タグ（SGT）キャッシングを使用して、SGT でタグ付けされたトラフィックを、SGT を認識していないサービスを通じても渡すことができるようにします。SGTを伝播できないサービスには、WANの高速化または最適化、侵入防御システム（IPS）、およびアップストリーム ファイアウォールがあります。

ワンアーム モードでは、SGT でタグ付けされたパケットはデバイス（タグがキャッシュされた場所）に入力され、サービスにリダイレクトされます。そのサービスが完了した後、パケットはデバイスに戻されるか、別のデバイスにリダイレクトされます（図を参照）。このようなシナリオでは、次のようになります。

1. Cisco TrustSec SGT キャッシング 機能により、デバイスは、着信パケットからの IP-SGT バインド情報を特定し、この情報をキャッシュします。
2. デバイスは、SGT を伝播できないサービスにパケットをリダイレクトします。
3. サービスが完了した後、パケットはデバイスに返されます。
4. サービスの出力ポイントで、適切な SGT がパケットに再適用されます。
5. サービスからデバイスに返されたパケットには、ロールベースの強制が適用されます。
6. SGT のパケットは、他の Cisco TrustSec 対応デバイスのダウンストリームに転送されます。

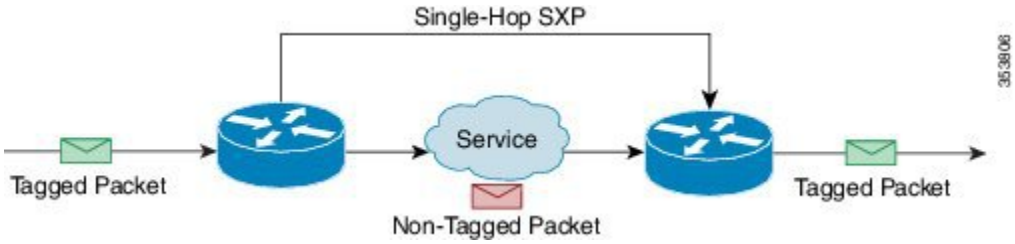
図 *6*：ワンアーム モードでの *SGT* キャッシング



特定のインスタンスでは、Bump-In-The-Wire（BITW）トポロジに導入されるサービスがあります。このようなシナリオでは、次のようになります。

1. サービスを通過するパケットはデバイスに返されません。
2. シングルホップ SGT Exchange Protocol（SXP）を使用して、IP-SGT バインドを特定し、特定されたバインドをエクスポートします。
3. ネットワーク内のアップストリーム デバイスは、SXP を通じて IP-SGT バインドを特定し、適切なタグを再適用するか、それらを SGT ベース強制に使用します。出力キャッシング中、元のネットワーク アドレス移動（NAT）前の送信元 IP アドレスは、特定された IP-SGT バインド情報の一部としてキャッシュされます。
4. 300 秒間トラフィックを受信しない IP-SGT バインドは、キャッシュから削除されます。

図 *7*：*Bump-In-The-Wire*（*BITW*）トポロジでの *SGT* キャッシング



Cisco TrustSec SGT キャッシング の設定方法

SGT キャッシングのグローバル設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **cts role-based sgt-caching**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts role-based sgt-caching** 例： `Device(config)# cts role-based sgt-caching`	すべてのインターフェイスに対して、入力方向の SGT キャッシングを有効化します。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

インターフェイスでの SGT キャッシシングの設定

インターフェイスが Virtual Routing and Forwarding（VRF）ネットワーク上に設定された場合、そのインターフェイス上で特定された IP-SGT バインドは特定の VRF 以下に追加されます。（対応する VRF 上で特定されたバインドを表示するには、**show cts role-based sgt-map vrf***vrf-name***all** コマンドを使用します。）

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***type slot/port*
4. **cts role-based sgt-cache** [**ingress** | **egress**]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**interface***type slot/port* 例： `Device(config)# interface gigabitEthernet 0/1/0`	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 4	**cts role-based sgt-cache** [**ingress** | **egress**] 例： `Device(config-if)# cts role-based sgt-cache ingress`	特定のインターフェイスで SGT キャッシングを設定します。 • ingress：特定のインターフェイスを開始するトラフィック（インバウンド トラフィック）に対して SGT キャッシングを有効化します。 • egress：特定のインターフェイスを終了するトラフィック（アウトバウンド トラフィック）に対して SGT キャッシングを有効化します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `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。

Cisco TrustSec SGT キャッシング の確認

手順の概要

1. イネーブル化
2. **show cts**
3. **show cts interface**
4. **show cts interface brief**
5. **show cts role-based sgt-map all ipv4**
6. **show cts role-based sgt-map vrf**

手順の詳細

ステップ 1 イネーブル化

特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 show cts

Cisco TrustSec 接続とグローバル SGT キャッシングのステータスを表示します。

例：

```
Device# show cts

Global Dot1x feature: Disabled
CTS device identity: ""
CTS caching support: disabled
CTS sgt-caching global: Enabled
Number of CTS interfaces in DOT1X mode:  0,    MANUAL mode: 0
Number of CTS interfaces in LAYER3 TrustSec mode: 0
Number of CTS interfaces in corresponding IFC state
  INIT            state:  0
  AUTHENTICATING  state:  0
```

```
  AUTHORIZING     state:  0
  SAP_NEGOTIATING state:  0
  OPEN            state:  0
  HELD            state:  0
  DISCONNECTING   state:  0
  INVALID         state:  0
CTS events statistics:
  authentication success: 0
  authentication reject : 0
  authentication failure: 0
  authentication logoff : 0
  authentication no resp: 0
  authorization success : 0
  authorization failure : 0
  sap success           : 0
  sap failure           : 0
  port auth failure     : 0
```

ステップ 3 **show cts interface**

モード詳細（入力または出力）を使用した、インターフェイスと SGT キャッシング情報についての Cisco TrustSec 設定の統計情報を表示します。

例：

```
Device# show cts interface GigabitEthernet0/1

Interface GigabitEthernet0/1
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is enabled, mode:     MANUAL
      Propagate SGT:          Enabled
      Static Ingress SGT Policy:
        Peer SGT:             200
        Peer SGT assignment:  Trusted

    L2-SGT Statistics
        Pkts In                     : 16298041
        Pkts (policy SGT assigned)  : 0
        Pkts Out                    : 5
        Pkts Drop (malformed packet): 0
        Pkts Drop (invalid SGT)     : 0
```

ステップ 4 **show cts interface brief**

すべてのインターフェイスについて、モード詳細（入力または出力）を使用して SGT キャッシング情報を表示します。

例：

```
Device# show cts interface brief

Interface GigabitEthernet0/0
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is disabled

Interface GigabitEthernet0/1
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is enabled, mode:     MANUAL
      Propagate SGT:          Enabled
      Static Ingress SGT Policy:
        Peer SGT:             200
```

```
        Peer SGT assignment:  Trusted

Interface GigabitEthernet0/2
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is enabled, mode:     MANUAL
      Propagate SGT:          Enabled
      Static Ingress SGT Policy:
        Peer SGT:             0
        Peer SGT assignment:  Untrusted

Interface GigabitEthernet0/3
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is disabled

Interface Backplane-GigabitEthernet0/4
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is disabled

Interface RG-AR-IF-INPUT1
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is disabled
```

ステップ 5 **show cts role-based sgt-map all ipv4**

すべての SGT-IPv4 バインドを表示します。

例：

```
Device# show cts role-based sgt-map all ipv4

Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
192.0.2.1                50      CACHED
192.0.2.2                50      CACHED
192.0.2.3                50      CACHED
192.0.2.4                50      CACHED
192.0.2.5                3900    INTERNAL
192.0.2.6                3900    INTERNAL
192.0.2.7                3900    INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of CACHED   bindings = 20
Total number of INTERNAL bindings = 3
Total number of active   bindings = 23
```

ステップ 6 **show cts role-based sgt-map vrf**

特定の Virtual Routing and Forwarding（VRF）インターフェイスに対する SGT-IP バインドをすべて表示します。

例：

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

%IPv6 protocol is not enabled in VRF RED
Active IPv4-SGT Bindings Information
```

```
IP Address              SGT     Source
============================================
192.0.2.1                50      CACHED
192.0.2.2                2007    CACHED
192.0.2.3                50      CACHED
192.0.2.4                50      CACHED
```

Cisco TrustSec SGT キャッシング の設定例

例：SGT キャッシングのグローバル設定

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-caching
Device(config)# end
```

例：インターフェイスの SGT キャッシシングの設定

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet 0/1/0
Device(config-if)# cts role-based sgt-cache ingress
Device(config-if)# end
```

例：インターフェイスでの SGT キャッシシングの無効化

次の例は、キャッシングがグローバルに有効だがインターフェイスでは無効な場合に、インターフェイスで SGT キャッシングを無効化し、インターフェイスの SGT キャッシングの状態を表示する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-caching
Device(config)# interface gigabitEthernet 0/1
Device(config-if)# no cts role-based sgt-cache ingress
Device(config-if)# end
Device# show cts interface GigabitEthernet0/1

Interface GigabitEthernet0/1
    CTS sgt-caching Ingress:  Disabled
    CTS sgt-caching Egress :  Disabled
    CTS is enabled, mode:     MANUAL
      Propagate SGT:          Enabled
      Static Ingress SGT Policy:
        Peer SGT:             200
        Peer SGT assignment:  Trusted
```

```
L2-SGT Statistics
    Pkts In                      : 200890684
    Pkts (policy SGT assigned)   : 0
    Pkts Out                     : 14
    Pkts Drop (malformed packet): 0
    Pkts Drop (invalid SGT)      : 0
```

Cisco TrustSec SGT キャッシング 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
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS 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 の設定	『*Cisco TrustSec Configuration Guide*』の「Cisco TrustSec Support for IOS」の章
Cisco TrustSec の概要	『Overview of TrustSec』
Cisco TrustSec ソリューション	『Cisco TrustSec Security Solution』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ 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 キャッシング 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 *8*：*Cisco TrustSec SGT* キャッシング の機能情報

機能名	リリース	機能情報
Cisco TrustSec SGT キャッシング		Cisco TrustSec SGT キャッシング 機能は、セキュリティ グループ タグ（SGT）の移動性を柔軟にする Cisco TrustSec の機能を強化します。この機能は、IP-SGT バインドを特定し、対応する SGT をキャッシュすることで、通常のディープパケット インスペクションを処理するすべてのネットワーク サービスを通じて、またパケットが該当する SGT で再度タグ付けされるサービス出力ポイントにおいて、ネットワーク パケットを転送します。 次のコマンドが導入または変更されました：**cts role-based sgt-caching**、**cts role-based sgt-cache** [**ingress** | **egress**]。

第 10 章

CTS SGACL のサポート

CTS SGACL のサポート機能は、IP アドレスではなく、セキュリティ アソシエーションまたはセキュリティ グループ タグ値に基づいたステートレスのアクセス制御メカニズムを提供します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

CTS SGACL サポートの前提条件

CTS SGACL サポートについては、Protected Access Credential（PAC）と環境データのダウンロードが、ダイナミック SGACL のデバイスで設定されていること。

CTS SGACL サポートの制約事項

- プラットフォームあたりでサポートされている TrustSec 機能のリストおよび IOS リリースの最小要件については、次の URL の Cisco TrustSec プラットフォーム サポート マトリックス [英語] を参照してください。 http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html
- SGACL の適用は、管理インターフェイスではサポートされていません。
- ダイナミック SGACL のダウンロード サイズは、6 KB に制限されています。
- Port-Channel インターフェイスの SGACL 適用は検証されていません。
- VRF aware SGT 設定では、Cisco IOS XE Denali 16.3 は、VRF 管理インターフェイスではありませんが、ISE 通信をサポートしています。管理インターフェイスを通じた ISE 通信はサポートされていません。
- 6 KB の拡張制限は、ダイナミック SGACL のみです。スタティック SGACL は、500*500 マトリックスのような高い拡張性をサポートできます。

CTS SGACL サポートに関する情報

CTS SGACL のサポート

セキュリティ グループ アクセス コントロール リスト（SGACL）はポリシーの適用です。これによって管理者は、セキュリティ グループの割り当てと宛先リソースに基づいてユーザが実行する操作を制御できます。Cisco TrustSec ドメイン内のポリシーの適用は、軸の 1 つが送信元セキュリティ グループ番号、もう 1 つの軸が宛先セキュリティ グループ番号である、アクセス許可マトリックスで表示されます。マトリックス内の各セルには、SGACL の番号付きリストが含まれます。ここでは、送信元セキュリティ グループに属し宛先セキュリティ グループに属する宛先 IP を持つ、IP から送信されるパケットに適用される必要があるアクセス権限を指定します。

SGACL は、IP アドレスではなく、セキュリティ アソシエーションまたはセキュリティ グループ タグ値に基づいたステートレスのアクセス制御メカニズムを提供し、一致クラスに基づいてトラフィックをフィルタリングします。SGACL ポリシーをプロビジョニングするには、次の 3 つの方法があります。

- スタティック ポリシー プロビジョニング：**cts role-based permission** コマンドを使用して、ユーザが SGACL ポリシーを定義します。

- ダイナミック ポリシー プロビジョニング：SGACL ポリシーの設定は、Cisco Secure ACS または Cisco Identity Services Engine の主にポリシー管理機能によって実行する必要があります。後者については『Cisco Identity Services Engine User Guide』を参照してください。
- 認可変更（CoA）：更新されたポリシーは、SGACL ポリシーが ISE で変更され、CoA が CTS デバイスにプッシュされるとダウンロードされます。

CTS SGACL サポートの設定方法

SGACL ポリシーの適用のグローバルな有効化

Cisco TrustSec 対応ルーテッド インターフェイスの SGACL ポリシーの強制を有効化するには、次のタスクを実行します。

```
enable
configure terminal
cts role-based enforcement
```

インターフェイスあたりの SGACL ポリシーの適用の有効化

cts role-based enforcement コマンドを使用すると、SGACL のグローバルな適用を有効にして、特定のインターフェイスでは無効にすることができます。また、SGACL の適用は、グローバルで有効化しなくても、特定のインターフェイスで有効化できます。

インターフェイスでの SGACL ポリシーの適用を有効化するには、次のタスクを実行します。

```
enable
configure terminal
interface GigabitEthernet 0/1/1
cts role-based enforcement
```

SGACL ポリシーの手動設定

SGACL ポリシーを手動で設定するには、次のタスクを実行します。

```
enable
configure terminal
ip access-list role-based allow_webtraff
10 permit tcp dst eq 80
20 permit tcp dst eq 443
cts role-based permissions from 55 to 66 allow_webtraff
end
```

ダウンロードされた SGACL ポリシーのリフレッシュ

ダウンロードされた SGACL ポリシーを更新するには、次のタスクを実行します。

```
enable
cts refresh policy
```

または

```
enable
cts refresh policy sgt 10
```

CTS SGACL サポートの設定例

例：CTS SGACL のサポート

次に、show cts role-based permissions コマンドの出力例を示します。

```
Router# show cts role-based permissions

IPv4 Role-based permissions default:
        default_sgacl-02
        Permit IP-00
IPv4 Role-based permissions from group 55:SGT_55 to group 66:SGT_66 (configured):
        allow_webtraff
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

次に、ダイナミック SGACL にのみ適用される show cts policy sgt コマンドの出力例を示します。

```
Router# show cts policy sgt

CTS SGT Policy
==============
RBACL Monitor All : FALSE
RBACL IP Version Supported: IPv4
SGT: 0-02:Unknown
SGT Policy Flag: 0xc1408801
RBACL Source List: Empty
RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
RBACL Policy Last update time = 20:58:28 IST Wed Jul 13 2016
Policy expires in 0:00:24:05 (dd:hr:mm:sec)
Policy refreshes in 0:00:24:05 (dd:hr:mm:sec)
Cache data applied = NONE

SGT: 65535-46:ANY
SGT Policy Flag: 0x41400001
RBACL Source List:
  Source SGT: 65535-46:ANY-0, Destination SGT: 65535-46:ANY-0
  rbacl_type = 80
  rbacl_index = 1
  name   = default_sgacl-02
  IP protocol version = IPV4
```

```
  refcnt = 1
  flag   = 0x40000000
  stale  = FALSE
  RBACL ACEs:
    permit icmp
    permit ip
  Source SGT: 65535-46:ANY-0, Destination SGT: 65535-46:ANY-0
  rbacl_type = 80
  rbacl_index = 2
  name   = Permit IP-00
  IP protocol version = IPV4
  refcnt = 1
  flag   = 0x40000000
  stale  = FALSE
  RBACL ACEs:
    permit ip
RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
RBACL Policy Last update time = 20:58:28 IST Wed Jul 13 2016
Policy expires in 0:00:24:05 (dd:hr:mm:sec)
Policy refreshes in 0:00:24:05 (dd:hr:mm:sec)
Cache data applied = NONE
```

次に、ダイナミック SGACL にのみ適用される show cts rbacl コマンドの出力例を示します。

```
Router# show cts rbacl

CTS RBACL Policy
================
RBACL IP Version Supported: IPv4 & IPv6
  name   =multple_ace-16
  IP protocol version = IPV4
  refcnt = 4
  flag = 0x40000000
  stale = FALSE
  RBACL ACEs:
      permit icmp
      deny tcp

  name   =default_sgacl-02
  IP protocol version = IPV4
  refcnt = 2
  flag = 0x40000000
  stale = FALSE
  RBACL ACEs:
      permit icmp
      permit ip

  name   =SGACL_256_ACE-71
  IP protocol version = IPV4
```

CTS SGACL サポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

MIB

MIB	MIB のリンク
• CISCO-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、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
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

CTS SGACL サポートの機能情報

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 *9*：***CTS SGACL*** サポートの機能情報

機能名	リリース	機能情報
CTS SGACL のサポート	Cisco IOS Release 16.3	CTS SGACL のサポート機能は、IP アドレスではなく、セキュリティ アソシエーションまたはセキュリティ グループタグ値に基づいたステートレスのアクセス制御メカニズムを提供します。 Cisco IOS リリース 16.3 では、この機能は、シスコアグリゲーション サービス ルータ 1000 シリーズとサービス統合型ルータ 4000 シリーズに導入されました。 この機能によって次のコマンドが導入されました：**cts role-based enforcement**、**ip access-list role-based**、**cts role-based permissions**、**show cts role-based permissions**、**show cts rbacl**。