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 Cisco TrustSec 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、Cisco TrustSec 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。

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

Cisco 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 Cisco Trustsec ネットワークを確立する必要があります。

- すべてのネットワーク デバイス間が接続されていること。
- Cisco Secure Access Control System（ACS）5.1 が、Cisco Trustsec -SXP ライセンスで動作していること。
- ディレクトリ、DHCP、DNS、認証局、およびNTPサーバがネットワーク内で機能すること。
- 異なるルータで異なる値に **retry open timer** コマンドを設定します。

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

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。

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

このセクションでは、L2 SGT のインポジションと転送を設定する例を示します。

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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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 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。 （注） サブインターフェイスで **cts manual** コマンドを有効にするには、Dot1Q タグの追加バイトに対応するように IP MTU サイズを増やす必要があります。これは、Cisco IOS XE リリース 3.17 より前のリリースにのみ適用されます。
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。

	コマンドまたはアクション	目的
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。

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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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。
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。

	コマンドまたはアクション	目的
		（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。

例：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

例：

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

```
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
```

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

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	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 Cisco TrustSec を手動で有効化できるようになるため、ルータは SGT を、Cisco TrustSec 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。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。