SGT インライン タギングの設定

SGT インラインタギングの制約事項

- Cisco TrustSec の手動設定と 802.1x 設定は共存できません。

SGT インラインタギングに関する情報

Cisco TrustSec 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。

Cisco TrustSec 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、レイヤ 2 （L2）-SGT インポジションと呼ばれます。この機能により、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 ネイバーに伝送されるパケット内に 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。

Cisco TrustSec SGT Exchange Protocol V4（SXPv4）機能は、Cisco TrustSec メタデータベースの L2-SGT をサポートします。パケットが Cisco TrustSec 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、Cisco TrustSec 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。Cisco TrustSec 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、SGACL 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。

信頼されるインターフェイスからのパケット内で受信した SGT タグはネットワークに伝播され、アイデンティティ ファイアウォールの分類にも使用されます。IPSec サポートが追加される場合は、受信した SGT タグは SGT タギング用の IPSec と共有されます。

Cisco TrustSec クラウドの入口のネットワーク デバイスは、Cisco TrustSec クラウドにパケットを転送する際に、パケットに SGT をタグ付けできるように、Cisco TrustSec クラウドに入るパケットの SGT を判断する必要があります。パケットの SGT は次の方法で判断できます。

- Cisco TrustSec ヘッダーの SGT フィールド：パケットを信頼されたピアデバイスから受信している場合は、Cisco TrustSec ヘッダーは正しい SGT フィールドを運んでいることを前提としています。この状況は、そのパケットにとって、そのネットワークが Cisco TrustSec クラウド内の最初のネットワークデバイスではない場合に適用されます。
- 送信元 IP アドレスに基づいた SGT ルックアップ：この場合、送信元 IP アドレスに基づいてパケットの SGT を決定するポリシーを、管理者が手動で設定できます。IP アドレスから SGT へのテーブルも、SXP プロトコルによって入力できます。

ユニキャスト送信元 IPv6 アドレスを持つ IPv6 マルチキャストトラフィックに対する L2 インラインタギングがサポートされています。

NAT 対応デバイスでの SGT インラインタギング

次のシナリオでは、入力ポートと出力ポートの両方でネットワークアドレス変換（NAT）が有効化されているプライマリデバイスから、セカンダリデバイスに流れるパケットの SGT の決定方法について説明します。

（注） フローに使用されるすべてのポートには **CTS manual** があり、両方のデバイスで信頼され、設定されている必要があります。

- 両方のデバイス間でインラインタギングが有効化されており、SGT タグが CLI で変更されていない場合：

  この場合、プライマリデバイスでは Cisco TrustSec がパケットの送信元 IP に対応する SGT タグに適用されます。同じ SGT タグが NAT IP にタグ付けされます。セカンダリデバイスでは、パケットの送信元 IP に対応する SGT タグにも Cisco TrustSec が適用されます。

SGT インライン タギングの設定

たとえば、送信元 IP 192.0.2.5 および SGT タグ 133 を持つパケットがプライマリデバイスで受信されます。Cisco TrustSec は、プライマリデバイスの SGT タグ 133 に適用されます。NAT 変換後、パケットの IP は 198.51.100.10 に変更され、SGT タグ 133 にタグ付けされます。セカンダリデバイスでは、パケットは IP アドレス 198.51.100.10 および SGT タグ 133 で受信されます。Cisco TrustSec は、セカンダリデバイスで SGT タグ133を使用して適用されます。

- 両方のデバイス間でインラインタギングが有効になっており、SGTタグがCLIで変更されている場合：

  この場合、プライマリデバイスでは Cisco TrustSec がパケットの送信元 IP に対応する SGT タグに適用されます。SGT タグは CLI によって変更されますが、パケットの送信元 IP に対応する SGT タグは、パケットの NAT IP にタグ付けされます。セカンダリデバイスでは、パケットの送信元 IP に対応する SGT タグにも Cisco TrustSec が適用されます。

  たとえば、送信元 IP 192.0.2.5 および SGT タグ 133 を持つパケットがプライマリデバイスで受信されます。Cisco TrustSec は、プライマリデバイスの SGT タグ 133 に適用されます。SGT タグは CLI で 200 に変更されます。NAT 変換後、パケットの IP は 198.51.100.10 に変更されます。ただし、SGT タグ 133 にタグ付けされます。セカンダリデバイスでは、パケットは IP アドレス 198.51.100.10 および SGT タグ 133 で受信されます。Cisco TrustSec は、セカンダリデバイスで SGT タグ133 に適用されます。

- インラインタギングが無効化されており（SGT がセカンダリデバイスの SXP プロトコルを介して入力されている）、SGT タグが CLI で変更されている場合：

  この場合、プライマリデバイスでは Cisco TrustSec がパケットの送信元 IP に対応する SGT タグに適用されます。NAT 後の IP への SGT は CLI を介して定義され、プライマリデバイスで学習されます。プライマリデバイスとセカンダリデバイス間に Cisco TrustSec の直接リンクが存在せず、IP と SGT のバインディングがセカンダリデバイスの SXP を通じて学習される場合、セカンダリデバイスでは、NAT IP に対応する SGT タグに Cisco TrustSec が適用されます。

  たとえば、送信元 IP 192.0.2.5 および SGT タグ 133 を持つパケットがプライマリデバイスで受信されます。NAT 変換後、送信元 IP は 198.51.100.10 に変更され、SGT は CLI を介して 200 として定義されます。Cisco TrustSec は、プライマリデバイスの SGT タグ 133 に適用されます。セカンダリデバイスでは、IP から SGT へのバインディングが SXP 経由で受信され、セカンダリデバイスの SGT タグ 200 に Cisco TrustSec が適用されます。

SGT インライン タギングの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。

SGT インライン タギングの設定

	コマンドまたはアクション	目的
	`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 1/0/1`	Cisco TrustSec SGT 認証と転送が有効化されるようにインターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**cts manual** 例： `Device(config-if)# cts manual`	インターフェイスで Cisco TrustSec SGT 認証と転送を有効化し、Cisco TrustSec 手動インターフェイス コンフィギュレーション モードを開始します。
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 Cisco TrustSec SGT 伝達を有効化します。 （注） 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 trusted`	インターフェイスでスタティック SGT 入力 ポリシーを設定し、インターフェイスで受信する SGT の信頼性を定義します。

	コマンドまたはアクション	目的
		（注） **trusted** キーワードは、そのインターフェイスが Cisco TrustSec に信頼されていることを示します。このインターフェイス上のイーサネットパケット内で受信した SGT 値は信頼され、デバイスによって任意の SG 認識型ポリシーの適用または出力タギングに使用されます。
ステップ 7	**end** 例： `Device(config-if-cts-manual)# end`	Cisco TrustSec 手動インターフェイス コンフィギュレーションモードを終了し、特権 EXEC モードを開始します。

例：SGT 静的インラインタギングの設定

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

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

SGT インラインタギングの機能の履歴

次の表に、このモジュールで説明する機能のリリース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 Gibraltar 16.11.1	SGT インラインタギング	Cisco TrustSec ドメイン内の各セキュリティグループは、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。

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 [英語] からアクセスします。