セキュリティグループタグのマッピングの設定

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。

SGT のマッピングの制約事項

サブネットと SGT のマッピングの制約事項

- /31 プレフィックスの IPv4 サブ ネットワークを拡張できません。
- サブネットホストアドレスは、**network-map** *bindings* bindings パラメータが、指定したサブネットのサブネットホストの合計数よりも小さいか、bindings が 0 の場合、セキュリティグループタグ（SGT）にバインドできません。
- セキュリティ交換プロトコル（SXP）スピーカーおよびリスナーが SXPv3 以降のバージョンを実行している場合のみ、IPv6 拡張および伝播が実行されます。

デフォルトルートの SGT マッピングの制約事項

- デフォルトルートの設定は、サブネット **/0** でのみ受け入れられます。サブネット /0 なしで host-ip のみを入力すると、次のメッセージが表示されます。

```
Device(config)#cts role-based sgt-map 0.0.0.0 sgt 1000
Default route configuration is not supported for host ip
```

SGT のマッピングに関する情報

このセクションでは、SGT マッピングに関する情報を提供します。

サブネットと SGT のマッピングの概要

サブネットと 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。Cisco TrustSec は着信パケットの送信元 IP アドレスが指定したサブネットに属する場合そのパケットに SGT を適用します。サブネットおよび SGT は、**cts role-based sgt-map** *net_address/prefix* **sgt** *sgt_number* グローバル コンフィギュレーション コマンドを使用して CLI で指定されます。単一のホストは、このコマンドでマップされる可能性があります。

IPv4 ネットワークでは、セキュリティ交換プロトコル（SXP）v3 以降のバージョンは SXPv3 ピアからサブネットの *net_address/prefix* ストリングを受信し、解析できます。SXP の以前のバージョンでは、SXP リスナー ピアにエクスポートする前に、サブネットのプレフィックスをホスト バインドのセットに変換します。

たとえば、IPv4 サブネット 192.0.2.0/24 は次のように拡張されます（ホストアドレスの 3 ビットのみ）。

- ホストアドレス 198.0.2.1 から 198.0.2.7：タグ付けされて SXP ピアに伝播します。
- ネットワークおよびブロードキャストアドレス 198.0.2.0 および 198.0.2.8：タグ付けされず、伝播しません。

SXPv3 がエクスポートできるサブネットバインドの数を制限するには、**cts sxp mapping network-map** グローバル コンフィギュレーション コマンドを使用します。

サブネット バインディングはスタティックで、アクティブ ホストの学習はありません。これらは SGT インポジションおよび SGACL の適用にローカルで使用できます。サブネットと SGT のマッピングによってタグ付けされたパケットは、レイヤ 2 またはレイヤ 3 Cisco TrustSec リンクに伝播できます。

IPv6 ネットワークの場合、SXPv3 は SXPv2 または SXPv1 ピアにサブネット バインディングをエクスポートできません。

VLAN と SGT のマッピングの概要

VLAN と SGT のマッピング機能は、指定した VLAN からのパケットに SGT をバインドします。これは、次のような点で、レガシーネットワークからの Cisco TrustSec 対応ネットワークへの移行を簡素化します。

- レガシーのスイッチ、ワイヤレスコントローラ、アクセスポイント、VPN などの、Cisco TrustSec 対応ではないが VLAN 対応のデバイスをサポートします。

- データセンターのサーバー セグメンテーションなどの、VLAN および VLAN ACL がネットワークを分割するトポロジに対する下位互換性を提供します。

VLAN と SGT のバインドは、**cts role-based sgt-map vlan-list** グローバル コンフィギュレーション コマンドで設定します。

Cisco TrustSec 対応スイッチ上で、スイッチ仮想インターフェイス（SVI）であるゲートウェイが VLAN に割り当てられており、そのスイッチで IP デバイストラッキングが有効になっている場合、Cisco TrustSec は、SVI サブネットにマッピングされている VLAN 上のすべてのアクティブなホストに対して IP と SGT のバインドを作成できます。

アクティブ VLAN のホストの IP-SGT バインディングは SXP リスナーにエクスポートされます。マッピングされた各 VLAN のバインドは VRF に関連付けられた IP-to-SGT テーブルに挿入されます。VLAN は SVI または **cts role-based l2-vrf** コマンドでマッピングされます。

VLAN と SGT のバインドの優先順位は最も低く、SXP または CLI ホスト コンフィギュレーションなどのその他のソースからのバインドを受け取った場合は、無視されます。バインドの優先順位は、「バインド送信元の優先順位」セクションに記載されています。

レイヤ 3 論理インターフェイスと SGT のマッピング（L3IF-SGT マッピング）の概要

L3IF-SGTマッピングは、基盤となる物理インターフェイスに関係なく、次のレイヤ3インターフェイスのいずれかのトラフィックに SGT を直接マッピングできます。

- ルーテッド ポート
- SVI（VLAN インターフェイス）
- レイヤ 2 ポートのレイヤ 3 サブインターフェイス
- トンネル インターフェイス

（SGT アソシエーションが Cisco ISE または Cisco ACS アクセスサーバーから動的に取得される）特定の SGT 番号またはセキュリティグループ名を指定するには、**cts role-based sgt-map interface** グローバル コンフィギュレーション コマンドを使用します。

アイデンティティ ポート マッピング（ctsインターフェイス手動サブモードコンフィギュレーション）および L3IF-SGT が異なる IP と SGT のバインドを必要とする場合、IPM が優先されます。IP と SGT のバインドのその他の競合は、「バインド送信元の優先順位」セクションにリストされている優先順位に従って解決されます。

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 バインドソース間の競合を解決します。たとえば、SGT は **policy** { **dynamic identity** *peer-name* | **static sgt** *tag*} Cisco Trustsec 手動インターフェイス モード コマンド（アイデンティティ ポート マッピング）を使用してインターフェイスに適用

されます。現在の優先順位の適用順序は、最も小さい（1）から最高（7）まで、次のとおりです。

1. VLAN：VLAN-SGT マッピングが設定された VLAN 上のスヌーピングされた ARP パケットから学習されたバインディング。
2. CLI：cts role-based sgt-map グローバル コンフィギュレーション コマンドの IP-SGT 形式を使用して設定されたアドレス バインディング。
3. レイヤ 3 インターフェイス：（L3IF）一貫した L3IF-SGT 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ディング。
4. SXP：SXP ピアから学習されたバインディング。
5. IP_ARP：タグ付けされた ARP パケットが CTS 対応リンクで受信されたときに学習されたバインディング。
6. LOCAL：EPM とデバイス トラッキングによって学習された認証済みホストのバインディング。このタイプのバインディングには、L2 [I]PM が設定されたポートの ARP スヌーピングによって学習された個々のホストも含まれます。
7. 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 間のバインディング。

デフォルトルートの SGT

デフォルトルートのセキュリティグループタグ（SGT）は、デフォルトルートに SGT 番号を割り当てます。

デフォルトルートは、指定されたルートと一致しないルートであるため、ラストリゾートの宛先へのルートです。デフォルトルートは、ルーティングテーブルに明示的にリストされていないネットワークが宛先になっているパケットの転送に使用されます。

SGT のマッピングの設定方法

このセクションでは、SGT マッピングを設定する例を示します。

デバイス SGT の手動設定

通常の Cisco TrustSec 動作では、認証サーバーがデバイスから発信されるパケット用に、そのデバイスに SGT を割り当てます。認証サーバーにアクセスできない場合は、使用する SGT を手動で設定できますが、認証サーバーから割り当てられた SGT のほうが、手動で割り当てた SGT よりも優先されます。

デバイスの SGT を手動で設定するには、次の作業を行います。

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	**cts sgt** *tag* 例： `Device(config)# cts sgt 1234`	Cisco TrustSec の SXP をイネーブルにします。
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、特権 EXEC モードに戻ります。

サブネットと SGT のマッピングの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts sxp mapping network-map** *bindings* 例： `Device(config)# cts sxp mapping network-map 10000`	• サブネットと SGT のマッピングのホスト数の制限を設定します。bindings 引数は、SGT にバインドされ、SXP リスナーにエクスポートできるサブネット IP ホストの最大数を指定します。 • *bindings*：（0 ～ 65,535）デフォルトは 0（実行される拡張なし）です。

	コマンドまたはアクション	目的
ステップ 4	**cts role-based sgt-map** *ipv4_address/prefix* **sgt** *number* 例： `Device(config)# cts role-based sgt-map 10.10.10.10/29 sgt 1234`	（IPv4）CIDR 表記でサブネットを指定します。 • サブネットと SGT のマッピング設定を取り消すには、このコマンドの *no* 形式を使用します。ステップ 2 で指定するバインディングの数は、サブネット上のホスト アドレスの数以上である必要があります（ネットワーク、およびブロードキャスト アドレスを除く）。sgt number キーワードは、指定したサブネットの各ホスト アドレスにバインドするセキュリティ グループ タグを指定します。 • *ipv4_address*：ドット付き 10 進表記で IPv4 ネットワークアドレスを指定します。 • *prefix*：（0 ～ 30）ネットワークアドレス内のビット数を指定します。 • **sgt** *number*：（0 ～ 65,535）セキュリティグループタグ（SGT）番号を指定します。
ステップ 5	**cts role-based sgt-map** *ipv6_address::prefix* **sgt** *number* 例： `Device(config)# cts role-based sgt-map 2020::/64 sgt 1234`	（IPv6）コロン 16 進表記でサブネットを指定します。サブネットと SGT のマッピング設定を取り消すには、このコマンドの *no* 形式を使用します。 ステップ 2 で指定するバインディングの数は、サブネット上のホスト アドレスの数以上である必要があります（ネットワーク、およびブロードキャスト アドレスを除く）。sgt number キーワードは、指定したサブネットの各ホスト アドレスにバインドするセキュリティ グループ タグを指定します。 • *ipv6_address*：コロン 16 進表記で IPv6 ネットワークアドレスを指定します。 • *prefix*：（0 ～ 128）ネットワークアドレス内のビット数を指定します。

	コマンドまたはアクション	目的
		• **sgt** *number*：（0 ～ 65,535）セキュリティグループタグ（SGT）番号を指定します。
ステップ 6	**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、特権 EXEC モードに戻ります。

VLAN と SGT のマッピングの設定

Cisco TrustSec デバイスで VLAN-SGT マッピングを設定するタスクフロー。

- 着信 VLAN の同じ VLAN_ID でデバイス上に VLAN を作成します。
- エンドポイントのクライアントに対して、デフォルトゲートウェイになるようにデバイスの VLAN に SVI を作成します。
- VLAN トラフィックに SGT を適用するようにデバイスを設定します。
- デバイスの IP デバイストラッキングを有効にします。
- VLAN にデバイストラッキングポリシーをアタッチします。

（注） マルチスイッチネットワークでは、SISF ベースのデバイストラッキングにより、機能を実行しているスイッチ間でバインドテーブルエントリを分散できます。これは、ホストがアクセスポートに表示されるスイッチでバインドエントリが作成され、トランクポートを介して表示されるホストに対してエントリが作成されないことを前提としています。マルチスイッチセットアップでこれを行うには、『*Security Configuration Guide*』の「*Configuring SISF-Based Device Tracking*」の章にある「*Configuring a Multi-Switch Network to Stop Creating Binding Entries from a Trunk Port*」の手順に従って、別のポリシーを設定し、トランクポートにアタッチすることを推奨します。

- VLAN と SGT のマッピングがデバイスで発生することを確認します。

手順

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

	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	**vlan** *vlan_id* 例： `Device(config)# vlan 100`	TrustSec 対応ゲートウェイデバイスに VLAN 100 を作成し、VLAN 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	[**no**] **shutdown** 例： `Device(config-vlan)# no shutdown`	VLAN 100 をプロビジョニングします。
ステップ 5	**exit** 例： `Device(config-vlan)# exit`	VLAN 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 モードに戻ります。
ステップ 6	**interface** *type slot/port* 例： `Device(config)# interface vlan 100`	インターフェイス タイプを指定して、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 7	**ip address** *slot/port* 例： `Device(config-if)# ip address 10.1.1.2 255.0.0.0`	VLAN 100 のスイッチ仮想インターフェイス（SVI）を設定します。
ステップ 8	[**no**] **shutdown** 例： `Device(config-if)# no shutdown`	SVI をイネーブルにします。
ステップ 9	**exit** 例： `Device(config-if)# exit`	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、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**cts role-based sgt-map vlan-list** *vlan_id* **sgt** *sgt_number* 例： `Device(config)# cts role-based sgt-map vlan-list 100 sgt 10`	指定した SGT を指定した VLAN を割り当てます。

	コマンドまたはアクション	目的
ステップ 11	**device-tracking policy** *policy-name* 例： `Device(config)# device-tracking policy policy1`	ポリシーを指定し、デバイストラッキングポリシーコンフィギュレーションモードを開始します。
ステップ 12	**tracking enable** 例： `Device(config-device-tracking)# tracking enable`	ポリシー属性のデフォルトのデバイストラッキング設定を上書きします。
ステップ 13	**exit** 例： `Device(config-device-tracking)# exit`	デバイストラッキング ポリシー コンフィギュレーションモードを終了します。続いて、グローバルコンフィギュレーション モードに戻ります。
ステップ 14	**vlan configuration** *vlan_id* 例： `Device(config)# vlan configuration 100`	デバイス トラッキング ポリシーをアタッチする VLAN を指定し、その VLAN のコンフィギュレーション モードを開始します。
ステップ 15	**device-tracking attach-policy** *policy-name* 例： `Device(config-vlan-config)# device-tracking attach-policy policy1`	指定された VLAN にデバイス トラッキング ポリシーをアタッチします。
ステップ 16	**end** 例： `Device(config-vlan-config)# end`	VLAN コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 17	**show cts role-based sgt-map** {*ipv4_netaddr* | *ipv4_netaddr/prefix* | *ipv6_netaddr* | *ipv6_netaddr/prefix* |**all** [**ipv4** |**ipv6**] |**host** { *ipv4__addr* |*ipv6_addr* } |**summary** [**ipv4** |**ipv6**] 例： `Device# show cts role-based sgt-map all`	（任意）VLAN と SGT のマッピングを表示します。
ステップ 18	**show device-tracking policy** *policy-name* 例： `Device# show device-tracking policy policy1`	（任意）現在のポリシー属性を表示します。

L3IF と SGT のマッピングの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts role-based sgt-map interface** *type slot/port* [**security-group** *name* | **sgt** *number*] 例： `Device(config)# cts role-based sgt-map interface gigabitEthernet 1/1 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。 • **interface** *type slot/port*：使用可能なインターフェイスのリストを表示します。 • **security-group** *name*：SGT ペアリングに対するセキュリティグループ名は Cisco ISE または Cisco ACS で設定されています。 • **sgt** *number*：（0 ～ 65,535）。セキュリティグループタグ（SGT）番号を指定します。
ステップ 4	**exit** 例： `Device(config)# exit`	設定モードを終了します。
ステップ 5	**show cts role-based sgt-map all** 例： `Device# cts role-based sgt-map all`	入力トラフィックに指定された SGT がタグ付けされたことを確認します。

ハードウェアキーストアのエミュレート

ハードウェアキーストアが存在しないか使用できない場合は、キーストアのソフトウェアエミュレーションを使用するようにスイッチを設定できます。ソフトウェアキーストアの使用を設定するには、次の作業を行います。

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	**cts keystore emulate** 例： `Device(config)# cts keystore emulate`	ハードウェアキーストアの代わりにキーストアのソフトウェアエミュレーションを使用するようにスイッチを設定します。
ステップ 4	**exit** 例： `Device(config)# exit`	設定モードを終了します。
ステップ 5	**show keystore** 例： `Device# show keystore`	キーストアのステータスと内容を表示します。保存された秘密は表示されません。

デフォルトルートの SGT の設定

始める前に

ip route 0.0.0.0 コマンドを使用して、デバイスにデフォルトルートがすでに作成されていることを確認します。そうでない場合、デフォルトルート（デフォルトルートの SGT に付属）は不明な宛先を取得するため、ラストリゾートの宛先は CPU を指します。

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。

	コマンドまたはアクション	目的

ステップ 3	**cts role-based sgt-map 0.0.0.0/0 sgt** *number*
	例：
	`Device(config)# cts role-based sgt-map 0.0.0.0/0 sgt 3`
		デフォルトルートの SGT 番号を指定します。有効値は 0 ～ 65,519 です。
		（注）
		• **host_address/subnet** は、IPv4 アドレス（0.0.0.0/0）または IPv6 アドレス（0:0::/0）のどちらかです。
		• デフォルトルートの設定は、サブネット **/0** でのみ受け入れられます・サブネット /0 なしで host-ip のみを入力すると、次のメッセージが表示されます。
		`Device(config)#cts role-based sgt-map 0.0.0.0 sgt 1000`
		`Default route configuration is not supported for host ip`

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。

SGT のマッピングの確認

次のセクションでは、SGT マッピングを確認する方法を示します。

サブネットと SGT のマッピングの設定確認

サブネットと SGT のマッピングの設定情報を表示するには、次の show コマンドのいずれかを使用します。

コマンド	目的
show cts sxp connections	SXP スピーカーとリスナーの接続と、動作ステータスを表示します。
show cts sxp sgt-map	SXP リスナーにエクスポートした IP と SGT のバインディングを表示します。

コマンド	目的
show running-config	サブネットと SGT のコンフィギュレーション コマンドが実行コンフィギュレーション ファイル内にあることを確認します。

VLAN と SGT のマッピングの確認

VLAN と SGT の設定情報を表示するには、次の show コマンドを使用します。

表 *1:*

コマンド	目的
show device-tracking policy	デバイストラッキング ポリシーの現在のポリシー属性を表示します。
show cts role-based sgt-map	IP アドレスと SGT のバインドを表示します。

L3IF と SGT のマッピングの確認

L3IF と SGT の設定情報を表示するには、次の show コマンドを使用します。

コマンド	目的
show cts role-based sgt-map all	すべての IP アドレスと SGT のバインドを表示します。

デフォルトルートの SGT の設定確認

デフォルトルートの SGT の設定確認

```
device# show role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
0.0.0.0/0               3       CLI
11.0.0.0/8              11      CLI
11.0.0.10               1110    CLI
11.1.1.1                1111    CLI
21.0.0.2                212     CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 5
Total number of active   bindings = 5
```

SGT のマッピングの設定例

このセクションでは、SGT のマッピングの設定例を示します。

例：デバイス SGT の手動設定

```
Device# configure terminal
Device(config)# cts sgt 1234
Device(config)# exit
```

例：サブネットと SGT のマッピングの設定

次の例は、SXPv3 を実行しているデバイス（Device 1 と Device 2）間の IPv4 サブネットと SGT のマッピングを設定する方法を示します。

1. デバイス間の SXP スピーカー/リスナー ピアリングを設定します。

```
Device1# configure terminal
Device1(config)# cts sxp enable
Device1(config)# cts sxp default source-ip 1.1.1.1
Device1(config)# cts sxp default password 1syzygy1
Device1(config)# cts sxp connection peer 2.2.2.2 password default mode local speaker
```

2. Device 1 の SXP リスナーとして Device 2 を設定します。

```
Device2(config)# cts sxp enable
Device2(config)# cts sxp default source-ip 2.2.2.2
Device2(config)# cts sxp default password 1syzygy1
Device2(config)# cts sxp connection peer 1.1.1.1 password default mode local listener
```

3. Device 2 で、SXP 接続が動作していることを確認してください。

```
Device2# show cts sxp connections brief | include 1.1.1.1
          1.1.1.1                 2.2.2.2          On                 3:22:23:18
 (dd:hr:mm:sec)
```

4. サブネットワークが Device 1 に拡張されるように設定します。

```
Device1(config)# cts sxp mapping network-map 10000
Device1(config)# cts role-based sgt-map 10.10.10.0/30 sgt 101
Device1(config)# cts role-based sgt-map 11.11.11.0/29 sgt 11111
Device1(config)# cts role-based sgt-map 192.168.1.0/28 sgt 65000
```

5. Device 2 で、Device1 からのサブネットと SGT の拡張を確認します。ここには、10.10.10.0/30 サブネットワーク用の拡張が 2 個、11.11.11.0/29 サブネットワーク用の拡張が 6 個、192.168.1.0/28 サブネットワーク用の拡張が 14 個存在する必要があります。

```
Device2# show cts sxp sgt-map brief | include 101|11111|65000
            IPv4,SGT: <10.10.10.1 , 101>
            IPv4,SGT: <10.10.10.2 , 101>
            IPv4,SGT: <11.11.11.1 , 11111>
            IPv4,SGT: <11.11.11.2 , 11111>
            IPv4,SGT: <11.11.11.3 , 11111>
```

```
IPv4,SGT: <11.11.11.4 , 11111>
IPv4,SGT: <11.11.11.5 , 11111>
IPv4,SGT: <11.11.11.6 , 11111>
IPv4,SGT: <192.168.1.1 , 65000>
IPv4,SGT: <192.168.1.2 , 65000>
IPv4,SGT: <192.168.1.3 , 65000>
IPv4,SGT: <192.168.1.4 , 65000>
IPv4,SGT: <192.168.1.5 , 65000>
IPv4,SGT: <192.168.1.6 , 65000>
IPv4,SGT: <192.168.1.7 , 65000>
IPv4,SGT: <192.168.1.8 , 65000>
IPv4,SGT: <192.168.1.9 , 65000>
IPv4,SGT: <192.168.1.10 , 65000>
IPv4,SGT: <192.168.1.11 , 65000>
IPv4,SGT: <192.168.1.12 , 65000>
IPv4,SGT: <192.168.1.13 , 65000>
IPv4,SGT: <192.168.1.14 , 65000>
```

6. Device 1 の拡張数を確認します。

```
Device1# show cts sxp sgt-map
            IP-SGT Mappings expanded:22
            There are no IP-SGT Mappings
```

7. Device 1 と Device 2 の設定を保存し、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。

```
Device1(config)# copy running-config startup-config
Device1(config)# exit
Device2(config)# copy running-config startup-config
Device2(config)# exit
```

例：アクセスリンクを介した1つのホストに対するVLANとSGTのマッピングの設定

次の例では、単一のホストは、アクセスデバイス上の VLAN 100 に接続します。TrustSec デバイスのスイッチ仮想インターフェイスは VLAN 100 のエンドポイントのデフォルトゲートウェイになります（IP アドレス 10.1.1.1）。TrustSec デバイスは VLAN 100 からのパケットにセキュリティグループタグ（SGT）10 を適用します。

1. アクセスデバイス上に VLAN 100 を作成します。

```
access_device# configure terminal
access_device(config)# vlan 100
access_device(config-vlan)# no shutdown
access_device(config-vlan)# exit
access_device(config)#
```

2. アクセスリンクとして TrustSec デバイスのインターフェイスを設定します。エンドポイントのアクセス ポートの設定は、この例では省略されます。

```
access_device(config)# interface gigabitEthernet 6/3
access_device(config-if)# switchport
access_device(config-if)# switchport mode access
access_device(config-if)# switchport access vlan 100
```

3. TrustSec デバイスに VLAN 100 を作成します。

```
TS_device(config)# vlan 100
TS_device(config-vlan)# no shutdown
TS_device(config-vlan)# end
TS_device#
```

4. 着信 VLAN 100 のゲートウェイとして SVI を作成します。

```
TS_device(config)# interface vlan 100
TS_device(config-if)# ip address 10.1.1.2 255.0.0.0
TS_device(config-if)# no shutdown
TS_device(config-if)# end
TS_device(config)#
```

5. VLAN 100 のホストにセキュリティ グループ タグ（SGT）10 を割り当てます。

```
TS_device(config)# cts role-based sgt-map vlan 100 sgt 10
```

6. TrustSec デバイスの IP デバイストラッキングを有効にします。それが動作していることを確認します。

```
TS_device(config)# ip device tracking
TS_device# show ip device tracking all

IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 100
--------------------------------------------------------------------
  IP Address     MAC Address   Vlan   Interface          STATE
--------------------------------------------------------------------
Total number interfaces enabled: 1
Vlan100
```

7. （任意）エンドポイントからデフォルトゲートウェイを ping します（この例では、ホスト IP アドレス 10.1.1.1）。SGT 10 が VLAN 100 のホストにマッピングされていることを確認します。

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

Active IP-SGT Bindings Information

IP Address          SGT          Source
============================================

10.1.1.1            10            VLAN

IP-SGT Active Bindings Summary
============================================
Total number of VLAN bindings = 1
Total number of CLI bindings = 0
Total number of active bindings = 1
```

例：入力ポートでの L3IF と SGT のマッピングの設定

次の例では、デバイスラインカードのレイヤ3インターフェイスで、すべての入力トラフィックにSGT3がタグ付けされるように設定します。接続されたサブネットのプレフィックスがすでにわかっています。

1. インターフェイスを設定します。

```
Device# configure terminal
Device(config)# interface gigabitEthernet 6/3 sgt 3
Device(config)# exit
```

2. インターフェイスに着信するトラフィックが適切にタグ付けされることを確認します。

```
Device# show cts role-based sgt-map all
IP Address          SGT             Source
========================================
15.1.1.15           4               INTERNAL
17.1.1.0/24         3               L3IF
21.1.1.2            4               INTERNAL
31.1.1.0/24         3               L3IF
31.1.1.2            4               INTERNAL
43.1.1.0/24         3               L3IF
49.1.1.0/24         3               L3IF
50.1.1.0/24         3               L3IF
50.1.1.2            4               INTERNAL
51.1.1.1            4               INTERNAL
52.1.1.0/24         3               L3IF
81.1.1.1            5               CLI
102.1.1.1           4               INTERNAL
105.1.1.1           3               L3IF
111.1.1.1           4               INTERNAL
IP-SGT Active Bindings Summary
========================================
Total number of CLI      bindings = 1
Total number of L3IF     bindings = 7
Total number of INTERNAL bindings = 7
Total number of active   bindings = 15
```

例：ハードウェアキーストアのエミュレート

次に、ソフトウェアキーストアの使用を設定および確認する例を示します。

```
Device# configure terminal
Device(config)# cts keystore emulate
Device(config)# exit
Device#show keystore
No hardware keystore present, using software emulation.
Keystore contains the following records (S=Simple Secret, P=PAC, R=RSA):
Index    Type     Name
-----    ----     ----
0         S       CTS-password
1         P       ECF05BB8DFAD854E8376DEA4EF6171CF
```

例：デバイスルートの SGT の設定

```
Device# configure terminal
Device(config)# cts role-based sgt-map 0.0.0.0/0 sgt 3
Device(config)# exit
```

セキュリティグループタグのマッピングの機能履歴

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 Everest 16.5.1a	セキュリティグループタグのマッピング	サブネットと 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。
Cisco IOS XE Gibraltar 16.11.1	デフォルトルート SGT の分類	デフォルトルート SGT は、指定されたルートと一致しないルートに SGT タグ番号を割り当てます。

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 [英語] からアクセスします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。