Cisco TrustSec 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。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。

Cisco TrustSec の制約事項

- 無効なデバイス ID が指定された場合、Protected Access Credential（PAC）のプロビジョニングが失敗し、ハング状態のままになります。PAC をクリアし、正しいデバイス ID とパスワードを設定した後でも、PAC は失敗します。

  回避策として、Cisco Identity Services Engine（ISE）で、PAC が機能するように、[Administration] > [System] > [Settings] > [Protocols] > [Radius] メニューの [Suppress Anomalous Clients] オプションをオフにします。

Cisco TrustSec のアーキテクチャに関する情報

Cisco TrustSec のセキュリティ アーキテクチャは、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。Cisco TrustSec は、ネットワークに入るようにセキュリティ グループ（SG）がパケットを分類するために認証中に取得したデバイスおよびユーザ クレデンシャルを使用します。このパケット分類は、Cisco TrustSec 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。このタグはセキュリティ グループ タグ（SGT）と呼ばれ、エンドポイント デバイスはこの SGT に基づいて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。

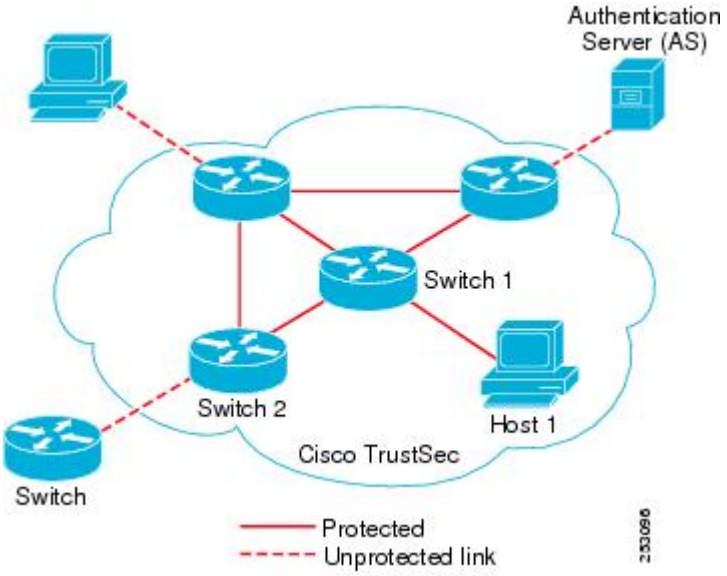
（注） Cisco TrustSec IEEE 802.1X リンクは、Cisco IOS XE Denali、Cisco IOS XE Everest、および Cisco IOS XE Fuji リリースでサポートされているプラットフォームではサポートされていないため、オーセンティケータのみがサポートされます。サプリカントはサポートされていません。

Cisco TrustSec のアーキテクチャは、3 種類の主要コンポーネントで構成されています。

- 認証されたネットワーキング インフラストラクチャ：Cisco TrustSec ドメインを開始するために最初のデバイス（シードデバイス）が認証サーバで認証した後に、ドメインに追加された新しい各デバイスはドメイン内のピア デバイスにより認証されます。ピアは、ドメインの認証サーバに対する媒介として動作します。それぞれの新たに認証されたデバイスは認証サーバによって分類され、アイデンティティ、ロールおよびセキュリティ ポスチャに基づいてセキュリティ グループ番号が割り当てられます。
- セキュリティ グループ ベースのアクセス コントロール：Cisco TrustSec ドメイン内のアクセス ポリシーは、トポロジとは無関係で、ネットワーク アドレスではなく送信元デバイスおよび宛先デバイスのロール（セキュリティ グループ番号で指定）に基づいています。個々のパケットには、送信元のセキュリティ グループ番号のタグが付けられます。
- セキュアな通信：暗号化対応ハードウェアでは、暗号化、メッセージ整合性検査、データパス リプレイ保護メカニズムの組み合わせを使用してドメイン内のデバイス間の各リンクの通信を保護できます。

次の図に、Cisco TrustSec ドメインの例を示します。この例では、Cisco TrustSec ドメイン内に、ネットワーク接続されたデバイスが数台とエンドポイント装置が 1 台あります。エンドポイント装置 1 台とネットワーク接続デバイス 1 台がドメインの外部にあるのは、これらが Cisco TrustSec 対応デバイスでないか、またはアクセスを拒否されたためです。認証サーバは、Cisco TrustSec ドメインの外部にあると見なされます。これは、Cisco Identities Service Engine（Cisco ISE）、または Cisco Secure Access Control System（Cisco ACS）です。

図 *1 : Cisco TrustSec* ネットワーク ドメインの例



Cisco TrustSec 認証プロセスの各参加者は、次のいずれかの役割を果たします。

- サプリカント：Cisco TrustSec ドメインへの参加を試行している、Cisco TrustSec ドメイン内のピアに接続されている認証されないデバイス。
- 認証サーバ：サプリカントのアイデンティティを確認し、Cisco TrustSec ドメイン内のサービスへのサプリカントのアクセスを決定するポリシーを発行します。
- オーセンティケータ：すでに Cisco TrustSec ドメインの一部であり、認証サーバに代わって新しいピアサプリカントを認証できる認証済みデバイス。

サプリカントとオーセンティケータの間のリンクの初回の確立時には、通常は次の一連のイベントが発生します。

1. 認証（802.1X）：サプリカントは認証サーバによって認証され、オーセンティケータが仲介として機能します。相互認証は、2 つのピア（サプリカントとオーセンティケータ）間で実行されます。
2. 認可：サプリカントのアイデンティティ情報に基づいて、認証サーバは、リンクされた各ピアにセキュリティグループの割り当てや ACL などの認可ポリシーを提供します。認証サーバは各ピアのアイデンティティを相互に提供し、各ピアはリンクに適切なポリシーを適用します。
3. セキュリティアソシエーションプロトコル（SAP）ネゴシエーション：リンクの両側で暗号化がサポートされている場合、サプリカントとオーセンティケータはセキュリティアソシエーション（SA）を確立するために必要なパラメータをネゴシエートします。

3 つのステップがすべて完了すると、オーセンティケータはリンクの状態を無許可（ブロッキング）状態から許可状態に変更し、サプリカントは Cisco TrustSec ドメインのメンバになります。

Cisco TrustSec では、入力タギングと出力フィルタリングを使用して、スケーラブルな方法でアクセス コントロール ポリシーを適用します。ドメインに入るパケットは、送信元デバイスに割り当てられたセキュリティグループ番号を含むセキュリティグループタグ（SGT）でタグ付けされます。このパケット分類は、Cisco TrustSec ドメイン内のデータ パスに沿ってセキュリティ、およびその他のポリシーの基準を適用するために維持されます。データ パスの最後の Cisco TrustSec デバイス（エンドポイントまたはネットワークの出力ポイント）は、Cisco TrustSec 送信元デバイスのセキュリティ グループおよび最終の Cisco TrustSec デバイスのセキュリティ グループに基づいてアクセス コントロール ポリシーを適用します。ネットワーク アドレスに基づいた以前のアクセス コントロール リストとは異なり、Cisco TrustSec アクセス コントロール ポリシーは、セキュリティ グループ アクセス コントロール リスト（SGACL）と呼ばれるロール ベース アクセス コントロール リスト（RBACL）形式です。

（注） 入力とは、宛先へのパス上のパケットが最初の Cisco TrustSec 対応デバイスに入るパケットを指します。出力とは、パス上の最後の Cisco TrustSec 対応デバイスを出るパケットを指します。

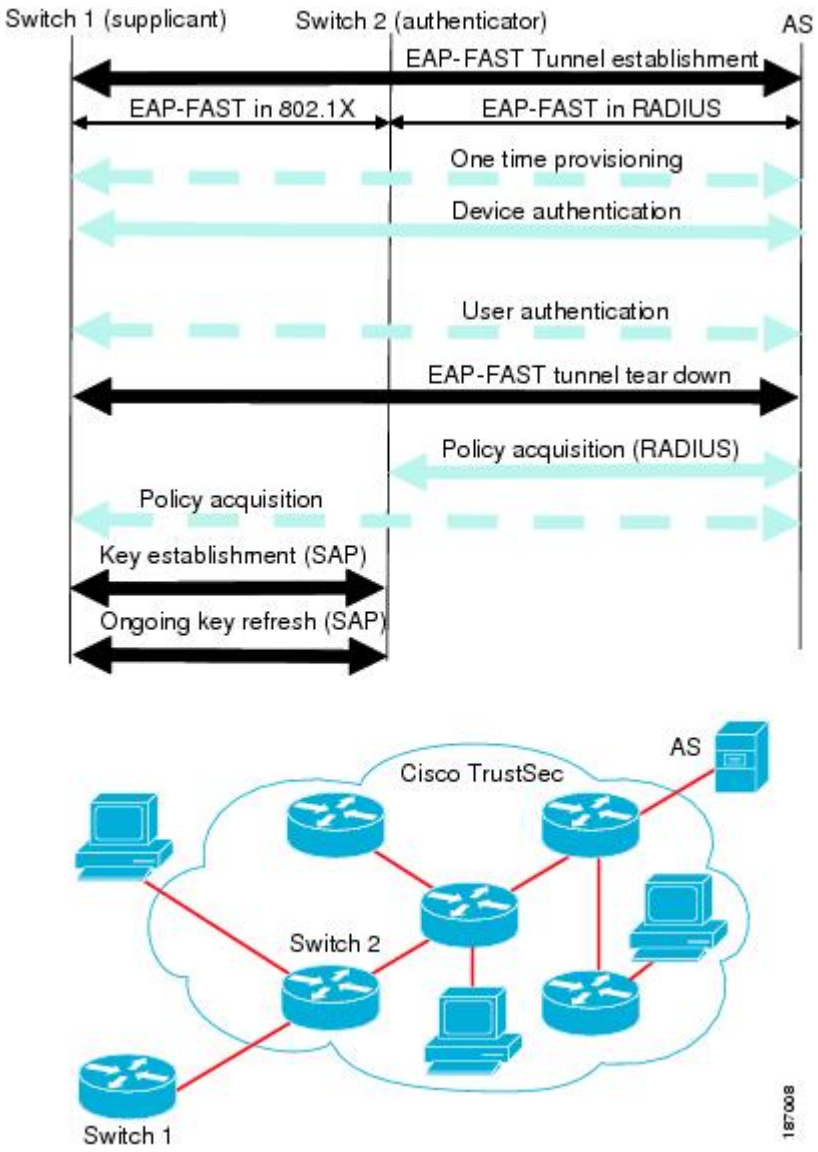
認証

Cisco TrustSec と認証

ネットワーク デバイス アドミッション コントロール（NDAC）を使用して、Cisco TrustSec は、デバイスがネットワークに参加できるようにする前にデバイスを認証します。NDAC は、Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）方式としての Extensible Authentication Protocol Flexible Authentication via Secure Tunnel（EAP-FAST）とともに、802.1X 認証を使用して、認証を実行します。EAP-FAST カンバセーションによって、チェーンを使用した EAP-FAST トンネル内で他の EAP 方式の交換が可能になります。この方法では、管理者は Microsoft Challenge Handshake Authentication Protocol Version 2（MSCHAPv2）のような従来型のユーザ認証方式を使用しながら、EAP-FAST トンネルが提供するセキュリティも利用できます。EAP-FAST 交換中に、認証サーバは認証サーバとの将来のセキュアな通信に使用される共有キーおよび暗号化されたトークンが含まれる一意の保護されたアクセス クレデンシャル（PAC）を作成し、サプリカントに配信します。

次の図に、EAP-FAST トンネルおよび Cisco TrustSec で使用する内部方式を示します。

図 *2 : Cisco TrustSec* の認証



EAP-FAST への Cisco TrustSec の機能拡張

Cisco TrustSec に EAP-FAST を実装することにより、次の機能拡張が実現しました。

- オーセンティケータの認証：オーセンティケータと認証サーバの間の共有キーを得るために PAC を使用するようにオーセンティケータに求めることにより、オーセンティケータのアイデンティティをセキュアに判断します。また、この機能により、オーセンティケータが使用できるすべての IP アドレスに関して認証サーバに RADIUS 共有キーを設定する手間が省けます。
- ピアのアイデンティティを各デバイスに通知：認証交換の完了までに、認証サーバはサプリカントとオーセンティケータの両方を識別します。認証サーバは、保護された EAP-FAST

終端で追加の type-length-value（TLV）パラメータを使用して、オーセンティケータのアイデンティティと、そのオーセンティケータが Cisco TrustSec に対応しているかどうかをサプリカントに伝えます。認証サーバはさらに、Access- Accept メッセージの RADIUS 属性を使用して、サプリカントのアイデンティティおよびそのサプリカントが Cisco TrustSec に対応しているかどうかをオーセンティケータに伝えます。各デバイスは、ピアのアイデンティティを認識しているため、認証サーバに追加の RADIUS Access-Requests を送信し、リンクに適用されるポリシーを取得できます。

802.1X ロールの選択

802.1X では、オーセンティケータに認証サーバとの IP 接続が必要です。オーセンティケータは RADIUS over UDP/IP を使用してサプリカントとオーセンティケータの認証交換をリレーする必要があるためです。PC などのエンドポイント装置はネットワークへの接続時にサプリカントとして機能することになります。ただし、2 つのネットワーク デバイス間の Cisco TrustSec 接続の場合、各ネットワーク デバイスの 802.1X ロールが他方のネットワーク デバイスに即座に認識されない場合もあります。

隣接する 2 つのスイッチにオーセンティケータとサプリカントのロールを手動で設定する代わりに、Cisco TrustSec はロール選択アルゴリズムを実行し、オーセンティケータとして機能するスイッチとサプリカントとして機能するスイッチを自動的に判断します。ロール選択アルゴリズムは、RADIUS サーバに IP で到達可能なスイッチにオーセンティケータロールを割り当てます。どちらのスイッチもオーセンティケータとサプリカントの両方のステートマシンを起動します。あるスイッチが、ピアに RADIUS サーバへのアクセス権があることを検出すると、そのデバイスは自身のオーセンティケータ ステート マシンを終了し、サプリカントのロールを引き受けます。両方のスイッチが RADIUS サーバにアクセスできる場合、RADIUS サーバから最初に応答を受信したスイッチがオーセンティケータになり、もう 1 つのスイッチがサプリカントになります。

Cisco TrustSec 認証の概要

Cisco TrustSec 認証プロセスが完了するまでに、認証サーバは次の処理を行います。

- サプリカントとオーセンティケータのアイデンティティの検証
- サプリカントがエンドポイント装置の場合はユーザの認証

Cisco TrustSec 認証プロセスの完了時には、オーセンティケータおよびサプリカントの両方が次の情報を取得しています。

- ピアのデバイス ID
- ピアの Cisco TrustSec 機能についての情報
- SAP に使用されるキー

デバイス ID

Cisco TrustSec はデバイスの ID として IP アドレスも MAC アドレスも使用しません。その代わり、各 Cisco TrustSec 対応スイッチに、Cisco TrustSec ドメインで一意に識別できる名前（デバイス ID）を手動で割り当てる必要があります。このデバイス ID は次の操作に使用されます。

- 認証ポリシーの検索
- 認証時におけるデータベース内のパスワードの検索

デバイスのクレデンシャル

Cisco TrustSec はパスワードベースのクレデンシャルをサポートしています。Cisco TrustSec はパスワードでサプリカントを認証し、相互認証を提供するために MSCHAPv2 を使用します。

認証サーバはこれらのクレデンシャルを EAP-FAST フェーズ 0（プロビジョニング）の交換（サプリカントで PAC がプロビジョニングされる）中にサプリカントの相互認証に使用します。Cisco TrustSec は PAC の期限が切れるまで、EAP-FAST フェーズ 0 の交換は再実行しません。その後のリンク起動時には、EAP-FAST フェーズ 1 とフェーズ 2 の交換だけを実行します。EAP-FAST フェーズ 1 交換では、認証サーバとサプリカントの相互認証に PAC を使用します。Cisco TrustSec がデバイスのクレデンシャルを使用するのは、PAC プロビジョニング（または再プロビジョニング）段階だけです。

サプリカントが最初に Cisco TrustSec ドメインに加入する際に、認証サーバはサプリカントを認証し、PAC を使用してサプリカントに共有キー、および暗号化されたトークンをプッシュします。認証サーバとサプリカントは、その後の EAP-FAST フェーズ 0 交換の相互認証にこのキーとトークンを使用します。

ユーザ クレデンシャル

Cisco TrustSec には、エンドポイント装置の特定タイプのユーザ クレデンシャルは必要ありません。認証サーバでサポートされるユーザ認証方式を任意に選択して、対応するクレデンシャルを使用できます。たとえば、Cisco Secure Access Control System（ACS）バージョン 5.1 は、MSCHAPv2、汎用トークンカード（GTC）、または RSA ワンタイムパスワード（OTP）をサポートしています。

セキュリティ グループ ベースのアクセス コントロール

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 Cisco ISE または Cisco Secure ACS の管理者が定義します。新しいユーザおよびデバイスが Cisco TrustSec 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。Cisco TrustSec は各セキュリティグループに一意の 16 ビットのセキュリティグループ番号を割り当てます。番号の範囲はCisco TrustSec ドメイン内でグローバルです。スイッチ内のセキュリティ 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 グループ番号を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、Cisco TrustSec 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セキュリティ グループ タグ（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 Cisco TrustSec ヘッダーで SGT を運びます。SGT は全社内の送信元の許可を特定する単一ラベルです。

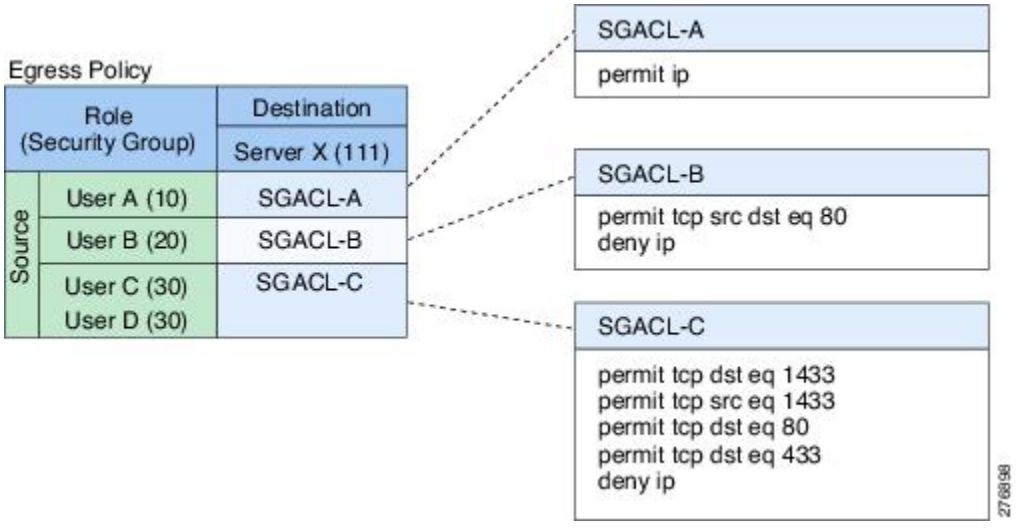
SGT には、送信元のセキュリティ グループが含まれているため、タグは送信元 SGT と呼ばれることもあります。宛先デバイスもまたセキュリティグループ（宛先 SG）に割り当てられるため、便宜上、このセキュリティグループを接続先グループタグ（DGT）と呼ぶこともあります。ただし、実際の Cisco TrustSec パケットタグには、宛先デバイスのセキュリティグループ番号は含まれていません。

SGACL ポリシー

セキュリティ グループ アクセス コントロール リスト（SGACL）を使用して、ユーザと宛先リソースのセキュリティグループの割り当てに基づいて、ユーザが実行でき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、許可マトリックスで表示されます。マトリクスの本体の各セルには送信元セキュリティ グループから宛先セキュリティ グループ宛てに送信されるパケットに適用される必要がある許可を指定する SGACL の順序リストを含めることができます。

次の図に、3 つの定義済みのユーザロールと 1 つの定義済み宛先リソースを含むシンプルなドメインの Cisco TrustSec 許可マトリックスの例を示します。ユーザの役割に基づいて宛先サーバへのアクセスを 3 つの SGACL ポリシーで制御します。

図 *3: SGACL* ポリシー マトリクスの例



ネットワーク内のユーザとデバイスをセキュリティグループに割り当て、セキュリティグループ間でアクセス制御を適用することにより、Cisco TrustSec はネットワーク内でロールベースのトポロジに依存しないアクセス制御を実現します。SGACL は従来の ACL とは異なり、IP アドレスではなくデバイス アイデンティティに基づいてアクセス コントロール ポリシーを定義するため、ネットワーク デバイスはネットワーク全体を移動し、IP アドレスを変更することができます。ロールと許可が同じであれば、ネットワーク トポロジが変更されてもセキュリティ ポリシーには影響しません。ユーザがスイッチに追加されたら、適切なセキュリティグループにユーザを割り当てるだけで、ユーザはただちにそのグループの許可を受信します。

（注） SGACL ポリシーは、スイッチからエンドホストデバイスに生成されるトラフィックではなく、2 つのホストデバイス間で生成されるトラフィックに適用されます。

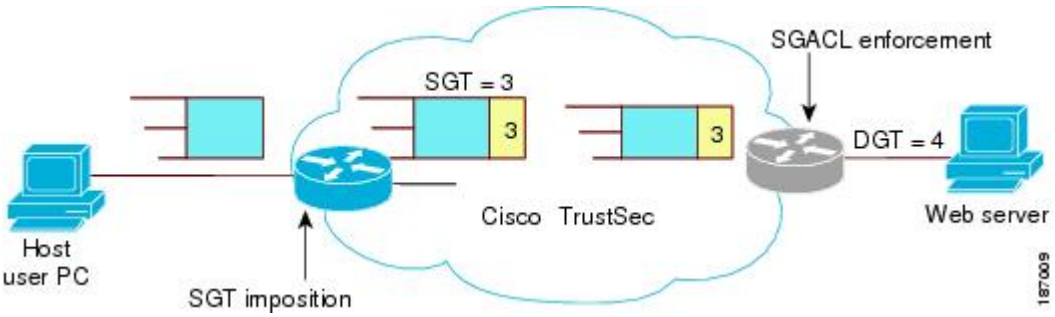
ロール ベースの許可を使用すると ACL のサイズが大幅に節約され、メンテナンス作業も簡単になります。Cisco TrustSec によって、設定されているアクセス コントロール エントリ（ACE）の数は、指定されている許可の数によって決定されるため、ACE の数は従来の IP ネットワークでよりもずっと小さくなります。Cisco TrustSec での SGACL の使用は、従来の ACL と比較して TCAM リソースをより効率的に使用します。

入力タギングおよび出力の強制

Cisco TrustSec アクセス コントロールは、入力タギングと出力の適用を使用して実装されます。Cisco TrustSec ドメインの入力点では、送信元からのトラフィックは、送信元エンティティのセキュリティグループ番号を含む SGT でタグ付けされます。SGT は、ドメイン全体にわたってトラフィックと合わせて伝播されます。Cisco TrustSec ドメインの出力ポイントで、出力デバイスは送信元 SGT および宛先エンティティのセキュリティ グループ番号（宛先 SG、または DGT）を使用して、SGACL ポリシー マトリクスから適用するアクセス ポリシーを決定します。

Cisco TrustSec ドメインでは、次の図のように SGT の割り当てと SGACL の適用が実行されます。

図 *4 : Cisco TrustSec* ドメインの *SGT* と *SGACL*



1. ホスト PC は Web サーバにパケットを送信します。PC と Web サーバは Cisco TrustSec ドメインのメンバではありませんが、パケットのデータパスには Cisco TrustSec ドメインが含まれています。

2. Cisco TrustSec の入力スイッチは、ホスト PC の認証サーバにより割り当てられたセキュリティ グループ番号である、セキュリティ グループ番号 3 の SGT を追加するようにパケットを変更します。
3. Cisco TrustSec 出力スイッチは、Web サーバの認証サーバによって割り当てられたセキュリティ グループ番号である、送信元グループ 3 と宛先グループ 4 に適用する SGACL ポリシーを適用します。
4. SGACL がパケットを転送するように許可している場合は、Cisco TrustSec 出力スイッチは SGT を削除するようにパケットを変更し、Web サーバにパケットを転送します。

送信元セキュリティ グループの判断

Cisco TrustSec ドメインの入口のネットワークデバイスは、Cisco TrustSec ドメイン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 ドメインに入るパケットの SGT を判断する必要があります。出力のネットワーク デバイスは、SGACL を適用するために、パケットの SGT を判断する必要があります。

ネットワーク デバイスは、次のいずれかの方法でパケットの SGT を判断できます。

- ポリシー取得時に送信元の SGT を取得する：Cisco TrustSec 認証フェーズ後、ネットワーク デバイスは、ピア デバイスが信頼できるかどうかを示すポリシー情報を、認証サーバから取得します。ピア デバイスが信頼できない場合、認証サーバはそのピア デバイスから着信するすべてのパケットに適用する SGT も提供します。
- パケットの送信元 SGT を取得する：パケットが信頼できるピア デバイスから送信される場合、パケットは、SGT を伝送します。これは、そのパケットにとって、そのネットワーク デバイスが Cisco TrustSec ドメイン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。
- 送信元アイデンティティに基づいて送信元 SGT を検索する：アイデンティティ ポート マッピング（IPM）を使用すると、接続されているピア アイデンティティのリンクを手動で設定できます。ネットワーク デバイスは、SGT および信頼状態を含むポリシー情報を認証サーバに要求します。
- 送信元 IP アドレスに基づいて送信元 SGT を検索する：場合によっては、送信元 IP アドレスに基づいてパケットの SGT を判断するようにパケットを手動で設定できます。SGT Exchange Protocol（SXP）も、IP-address-to-SGT マッピング テーブルに値を格納できます。

宛先セキュリティ グループの判断

Cisco TrustSec ドメインの出力のネットワーク デバイスは、SGACL を適用する宛先グループ（DGT）を決定します。ネットワーク デバイスは、パケットの送信元セキュリティ グループを決定するために使用されるのと同じ方法（パケットのタグからのグループ番号の取得を除く）を使用して宛先セキュリティ グループを決定します。宛先セキュリティ グループ番号はパケットのタグに含まれません。

場合によっては、入口のデバイスまたは出口以外のその他のデバイスが、使用できる宛先グループの情報を持っていることもあります。このような場合、SGACL は出力デバイスではなくこれらのデバイスに適用されます。

ルーテッドおよびスイッチド トラフィックでの SGACL の強制

SGACL の強制は IP トラフィックだけに適用されますが、強制はルーティングまたはスイッチングされるトラフィックに適用できます。

ルーテッドトラフィックの場合、SGACL の適用は、宛先ホストに接続されたルーテッドポートを持つ出力スイッチ（通常はディストリビューション スイッチまたはアクセススイッチ）によって実行されます。SGACL の適用をグローバルに有効にすると、SVI インターフェイスを除くすべてのレイヤ 3 インターフェイスで適用が自動的に有効になります。

スイッチングされるトラフィックの場合は、SGACL の強制はルーティング機能のない単一スイッチング ドメイン内のトラフィック フローで実行されます。2 台の直接接続されたサーバ間のサーバ間トラフィックのデータセンター アクセス スイッチ上で実行された SGACL の強制が、その例です。この例では、通常、サーバ間のトラフィックはスイッチングされます。SGACL の強制は、VLAN 内でスイッチングされるパケットまたは VLAN に関連付けられた SVI に転送されるパケットに適用できます。ただし実行は VLAN ごとに明示的にイネーブルにする必要があります。

SGACL ロギングと ACE 統計情報

SGACL でロギングが有効になっている場合、スイッチは次の情報を記録します。

- 送信元セキュリティグループタグ（SGT）および宛先 SGT
- SGACL ポリシー名
- パケットプロトコルタイプ
- パケットで実行されるアクション

ログオプションは個々の ACE に適用され、ACE に一致するパケットがログに記録されます。log キーワードで記録された最初のパケットは、syslog メッセージを生成します。後続のログメッセージは 5 分間隔で生成および報告されます。ロギング対応 ACE が別のパケット（ログメッセージを生成したパケットと同一の特性を持つ）と一致する場合、一致したパケットの数が増加（カウンタ）し、レポートされます。

ロギングを有効にするには、SGACL 構成の ACE 定義の前に **log** キーワードを使用します。たとえば、**permit ip log** のようになります。

次に、送信元と宛先の SGT、ACE の一致（許可または拒否アクション）、およびプロトコル、つまり TCP、UDP、IGMP、および ICMP 情報を表示するサンプルログを示します。

```
*Jun 2 08:58:06.489: %C4K_IOSINTF-6-SGACLHIT: list deny_udp_src_port_log-30 Denied
udp 24.0.0.23(100) -> 28.0.0.91(100), SGT8 DGT 12
```

show cts role-based counters コマンドを使用して表示できる既存の「セルごとの」SGACL 統計情報に加えて、**show ip access-list** *sgacl_name* コマンドを使用して ACE 統計情報も表示できます。これについて追加設定は必要ありません。

次に、show ip access-list コマンドを使用して ACE カウントを表示する例を示します。

```
Switch# show ip access-control deny_udp_src_port_log-30

Role-based IP access list deny_udp_src_port_log-30 (downloaded)
10 deny udp src eq 100 log (283 matches)
20 permit ip log (50 matches)
```

（注） 着信トラフィックがセルに一致するが、セルの SGACL に一致しない場合、トラフィックは許可され、セルの HW-許可のカウンタが増加します。

次に、セルの SGACL の動作例を示します。

SGACL ポリシーは「deny icmp echo」で 5 ー 18 に設定され、TCP ヘッダーで 5 ー 18 の着信トラフィックがあります。セルが 5 ー 18 に一致するが、トラフィックが icmp と一致しない場合、トラフィックは許可され、セル 5 ー 18 の HW-許可カウンタが増加します。

```
Switch# show cts role-based permissions from 5 to 18

IPv4 Role-based permissions from group 5:sgt_5_Contractors to group
18:sgt_18_data_user2:sgacl_5_18-01
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

Switch# show ip access-lists sgacl_5_18-01
Role-based IP access list sgacl_5_18-01 (downloaded)
10 deny icmp echo log (1 match)

Switch# show cts role-based counters from 5 to 18
Role-based IPv4 counters
From   To   SW-Denied   HW-Denied   SW-Permitt   HW-Permitt   SW-Monitor   HW-Monitor
  5    18       0           0            0        1673202          0            0
```

SGACL モニタ モード

Cisco TrustSec の事前導入段階で、管理者は、モニタモードを使用して、ポリシーが意図したとおりに機能することを確認するために、セキュリティポリシーを適用しない状態でテストします。セキュリティポリシーが意図したとおり機能しない場合には、モニタモードが、その問題を識別するための便利なメカニズムと、SGACL の適用を有効にする前にポリシーを修正する機会を提供します。これにより、管理者は、ポリシーを適用する前にポリシーアクションの結果をより可視的に確認でき、対象のポリシーがセキュリティ要件を満たしている（ユーザが認証されなければリソースへのアクセスは拒否される）ことを確認できます。

モニタリング機能は、SGT-DGT ペア レベルで提供されます。SGACL モニタ モード機能を有効にすると、拒否アクションがラインカード上の ACL 許可として実装されます。これにより、SGACL カウンタおよびロギングでは、接続が SGACL ポリシーによりどう処理されているか

を表示できます。すべてのモニタ対象トラフィックが許可されるため、SGACL モニタモードでは、SGACL によるサービスの中断はありません。

許可とポリシーの取得

デバイス認証が終了すると、サプリカントとオーセンティケータの両方が認証サーバからセキュリティ ポリシーを取得します。2 つのピアは、リンク認可を実行し、Cisco TrustSec デバイス ID に基づいてリンク セキュリティ ポリシーを相互に適用します。リンクの認証方式は、802.1X または手動認証に設定できます。リンクのセキュリティが 802.1X である場合、各ピアは認証サーバから受信したデバイス ID を使用します。リンクのセキュリティが手動の場合、ピア デバイス ID を割り当てる必要があります。

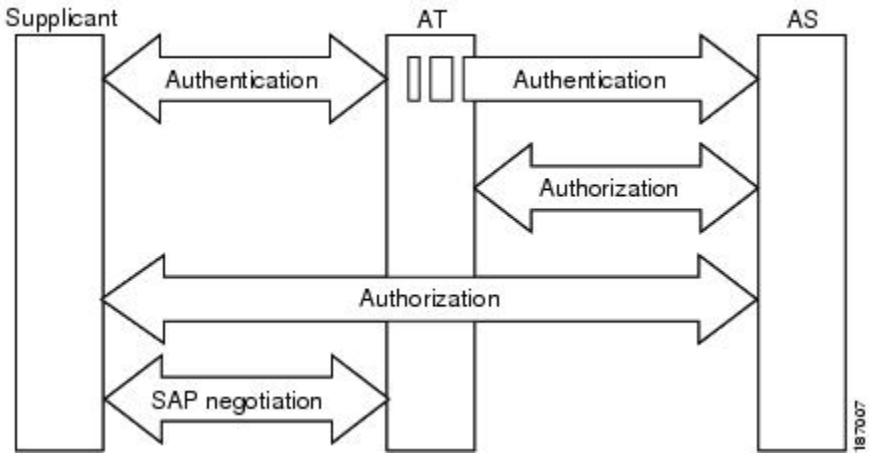
認証サーバは次の属性を返します。

- Cisco TrustSec の信頼状態：パケットに SGT を付けるにあたり、ピア デバイスが信用できるかどうかを示します。
- ピア SGT：ピアが属しているセキュリティ グループを示します。ピアが信頼できない場合は、ピアから受信したすべてのパケットにこの SGT がタグ付けされます。SGACL がピアの SGT に関連付けられているかどうかデバイスが認識できない場合、デバイスは認証サーバに追加要求を送信して SGACL をダウンロードする場合もあります。
- 許可期限：ポリシーの期限が切れるまでの秒数を示します。Cisco TrustSec デバイスはポリシーと許可を期限が切れる前にリフレッシュする必要があります。デバイスはデータの有効期限が切れていなければ認証およびポリシーデータをキャッシュし、リブート後に再利用できます。

（注） Cisco TrustSec デバイスは、認証サーバからピアの適切なポリシーを取得できない場合に備えて、最小限のデフォルト アクセス ポリシーをサポートする必要があります。

次の図に、NDAC および SAP ネゴシエーションプロセスを示します。

図 *5: NDAC* および *SAP* ネゴシエーション



環境データのダウンロード

Cisco TrustSec 環境データは、Cisco TrustSec ノードとしてのデバイスの機能を支援するひとまとまりの情報またはポリシーです。デバイスは、Cisco TrustSec ドメインに最初に加入する際に、認証サーバから環境データを取得しますが、一部のデータをデバイスに手動で設定することもできます。たとえば、Cisco TrustSec のシード デバイスには認証サーバの情報を設定する必要がありますが、この情報は、デバイスが認証サーバから取得するサーバ リストを使用して、後から追加することができます。

デバイスは、期限前に Cisco TrustSec 環境データをリフレッシュする必要があります。また、このデータの有効期限が切れていなければ、環境データをキャッシュし、リブート後に再利用することもできます。

デバイスは RADIUS を使用して、認証サーバから次の環境データを取得します。

- サーバリスト：クライアントがその後の RADIUS 要求に使用できるサーバのリスト（認証および許可の両方）PAC のリフレッシュは、これらのサーバを介して行われます。
- デバイス SG：そのデバイス自体が属しているセキュリティグループ
- 有効期間：Cisco TrustSec デバイスが環境データをリフレッシュする頻度を左右する期間

RADIUS リレー機能

802.1X 認証プロセスで Cisco TrustSec オーセンティケータのロールを引き受けるスイッチは、認証サーバへの IP 接続を通じて、UDP/IP での RADIUS メッセージの交換により、スイッチが認証サーバからポリシーと許可を取得できるようにします。サプリカントデバイスは認証サーバとの IP 接続がなくてもかまいません。サプリカントに認証サーバとの IP 接続がない場合、

Cisco TrustSec はオーセンティケータをサプリカントの RADIUS リレーとして機能させることができます。

サプリカントは、RADIUS サーバの IP アドレスと UDP ポートを持つオーセンティケータに特別な EAPOL メッセージを送信し、RADIUS 要求を完了します。オーセンティケータは、受信した EAPOL メッセージから RADIUS 要求を抽出し、これを UDP/IP を通じて認証サーバに送信します。認証サーバから RADIUS 応答が返ると、オーセンティケータはメッセージを EAPOL フレームにカプセル化して、サプリカントに転送します。

リンク セキュリティ

リンクの両側で 802.1AE Media Access Control Security（MACsec）をサポートしている場合、セキュリティ アソシエーション プロトコル（SAP）ネゴシエーションが実行されます。サプリカントとオーセンティケータの間で EAPOL-Key が交換され、暗号スイートのネゴシエーション、セキュリティ パラメータの交換、およびキーの管理が実行されます。これら 3 つの作業が正常に完了すると、セキュリティ アソシエーション（SA）が確立します。

ソフトウェア バージョン、暗号ライセンス、およびリンク ハードウェア サポートに応じて、SAP ネゴシエーションは次の動作モードの 1 つを使用できます。

- Galois/Counter Mode（GCM）：認証および暗号化ありを指定します
- GCM 認証（GMAC）：認証あり、暗号化なしを指定します
- カプセル化なし：カプセル化なし（クリア テキスト）を指定します
- ヌル：カプセル化あり、認証なし、暗号化なしを指定します

カプセル化なしを除くすべてのモードで、Cisco TrustSec 対応のハードウェアが必要です。

Cisco TrustSec ネットワークでの Cisco TrustSec 非対応デバイスおよびネットワークの使用

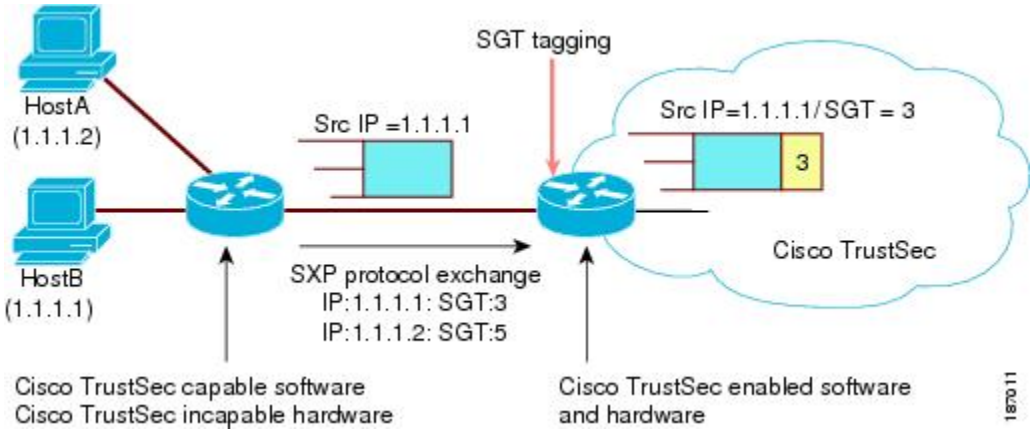
SXP によるレガシー アクセス ネットワークへの SGT の伝播

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。Cisco TrustSec 認証に参加する機能があっても、パケットに SGT をタグ付けするハードウェア機能がないデバイスがネットワークにある場合があります。SGT 交換プロトコル（SXP）を使用して、これらのデバイスは、Cisco TrustSec 対応のハードウェアを搭載している Cisco TrustSec ピア デバイスに IP アドレスと SGT のマッピングを渡すことができます。

通常、SXP は Cisco TrustSec ドメイン エッジの入力アクセス レイヤ デバイスと Cisco TrustSec 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 Cisco TrustSec 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 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。Cisco TrustSec 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、SGACL ポリシーを強制します。

図 *6 : SXP* プロトコルによる *SGT* 情報の伝播



Cisco TrustSec ハードウェア サポート対象外のピアと Cisco TrustSec ハードウェア サポート対象のピア間の SXP 接続は、手動で設定する必要があります。SXP 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。

- SXP データの整合性と認証が必要になる場合は、ピア デバイスの両方に同じ SXP パスワードを設定する必要があります。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。SXP パスワードは必須ではありませんが、使用することを推奨します。
- 各ピアを SXP 接続に SXP スピーカーまたは 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。
- 送信元 IP アドレスを指定して各ピアの関係付けに使用したり、特定の送信元 IP アドレスを設定していないピア接続に対してデフォルトの送信元 IP アドレスを設定したりすることができます。送信元 IP アドレスを指定しない場合、デバイスはピアへの接続のインターフェイスの IP アドレスを使用します。

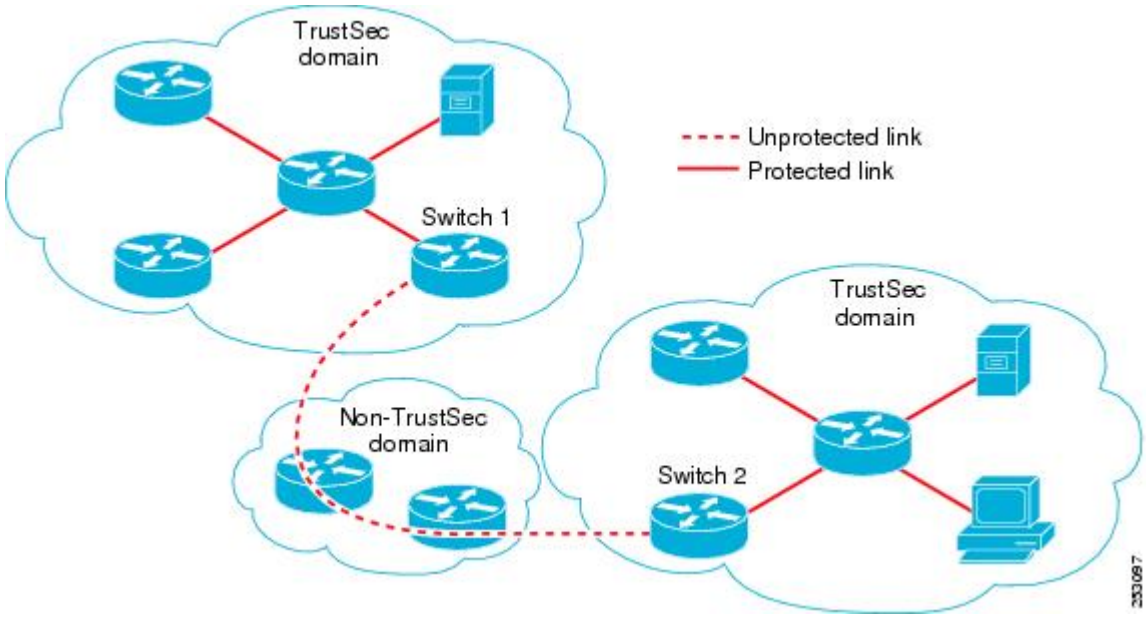
SXP は複数のホップを許可します。つまり、Cisco TrustSec ハードウェア サポート対象外デバイスのピアが Cisco TrustSec ハードウェア サポートの対象外でもある場合、2 番目のピアはハードウェア対応ピアに到達するまで IP と SGT のマッピング情報の伝播を継続して、3 番目のピアへの SXP 接続を設定できます。デバイスは 1 つの SXP 接続では SXP リスナーとして、別の SXP 接続では SXP スピーカーとして設定できます。

Cisco TrustSec デバイスは TCP キープアライブ メカニズムを使用して、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。

非 TrustSec 領域のスパニングのためのレイヤ 3 SGT トランスポート

パケットが非 TrustSec を宛先として Cisco TrustSec ドメインを離れると、出力 Cisco TrustSec デバイスは外部ネットワークにパケットを転送する前に Cisco TrustSec ヘッダーおよび SGT を削除します。ただし、次の図に示すように、パケットが別の Cisco TrustSec ドメインへのパス上にある非 TrustSec ドメインを通過するだけの場合、Cisco TrustSec レイヤ 3 SGT トランスポート機能を使用して SGT を維持できます。この機能では、出力 Cisco TrustSec デバイスは、SGT のコピーを含む ESP ヘッダーを使用してパケットをカプセル化します。カプセル化されたパケットが次の Cisco TrustSec ドメインに到達すると、入力 Cisco TrustSec デバイスは ESP カプセル化を解除して、SGT のパケットを伝播します。

図 *7*: 非 *TrustSec* ドメインのスパニング



Cisco TrustSec レイヤ 3 SGT トランスポートをサポートするために、Cisco TrustSec 入力または出力レイヤ 3 ゲートウェイとして機能するすべてのデバイスは、リモート Cisco TrustSec ドメインの適格なサブネットと、それらの領域内の除外されたサブネットを一覧表示するトラフィック ポリシー データベースを維持する必要があります。Cisco Secure ACS から自動的にダウンロードできない場合、デバイスごとにこのデータベースを手動で設定できます。

デバイスは 1 つのポートからレイヤ 3 SGT トランスポートデータを送信し、別のポートでレイヤ 3 SGT トランスポートデータを受信できますが、入力および出力ポートの両方が Cisco TrustSec 対応のハードウェアであることが必要です。

（注） Cisco TrustSec はレイヤ 3 SGT トランスポートのカプセル化パケットを暗号化しません。非 TrustSec ドメインを通過するパケットを保護するために、IPsec などの他の保護方式を設定できます。

Cisco TrustSec 非対応スイッチングモジュールの Cisco TrustSec リフレクタ

Cisco TrustSec ドメインのシスコデバイスには、次のいずれかのタイプのスイッチングモジュールが含まれている場合があります。

- Cisco TrustSec 対応：ハードウェアは SGT の挿入および伝播をサポートします。
- Cisco TrustSec-Aware：ハードウェアは SGT の挿入および伝播をサポートしませんが、ハードウェアはパケットの送信元および宛先 SGT を特定するために検索を実行できます。
- Cisco TrustSec 非対応：ハードウェアは SGT の挿入および伝播をサポートせず、ハードウェア検索で SGT を特定することもできません。

スイッチに Cisco TrustSec 対応のスーパーバイザエンジンが含まれる場合は、同じスイッチ内のレガシー Cisco TrustSec 非対応スイッチングモジュールに対応するために、Cisco TrustSec リフレクタ機能を使用できます。Cisco TrustSec リフレクタは SPAN を使用して Cisco TrustSec 非対応スイッチングモジュールからのトラフィックを、SGT の割り当ておよび挿入のためにスーパーバイザエンジンにリフレクトします。

2 つの相互に排他的なモード（入力および出力）は、Cisco TrustSec リフレクタでサポートされます。デフォルトはいずれのリフレクタもイネーブルでないピュア モードです。Cisco TrustSec 入力のリフレクタは、ディストリビューション スイッチに対向しているアクセススイッチで設定され、Cisco TrustSec 出力のリフレクタはディストリビューション スイッチで設定されます。

入力のリフレクタ

Cisco TrustSec 入力のリフレクタは、Cisco TrustSec 非対応スイッチングモジュールが Cisco TrustSec ドメインのエッジにあり、Cisco TrustSec 対応のスーパバイザエンジンのアップリンク ポートが Cisco TrustSec 対応ディストリビューションに接続している、アクセススイッチで導入されます。

Cisco TrustSec 入力のリフレクタの設定を受け入れるには、次の条件を満たす必要があります。

- スーパーバイザ エンジンが Cisco TrustSec 対応でなければなりません。
- Cisco TrustSec 非対応 DFC は、すべて電源がオフにする必要があります。
- Cisco TrustSec 出力のリフレクタはスイッチ上に設定しないでください。

- Cisco TrustSec 入力リフレクタをディセーブルにする前に、Cisco TrustSec 非対応スイッチング モジュールの電力を切る必要があります。

出力のリフレクタ

Cisco TrustSec 出力のリフレクタは Cisco TrustSec 非対応スイッチングモジュールがアクセススイッチに対向するレイヤ 3 のアップリンクを使用して、ディストリビューション スイッチに実装されます。Cisco TrustSec 出力のリフレクタはレイヤ 3 のアップリンクだけでサポートされ、レイヤ 2 インターフェイス、SVI、サブインターフェイス、またはトンネルではサポートされないので、NAT トラフィックではサポートされません。

Cisco TrustSec 出力のリフレクタの設定を受け入れるには、次の条件を満たす必要があります。

- スーパーバイザ エンジンまたは DFC のスイッチング モジュールが Cisco TrustSec 対応である必要があります。
- Cisco TrustSec は、スーパーバイザ エンジンのアップリンク ポートまたは Cisco TrustSec 対応 DFC スイッチング モジュールの非ルーテッド インターフェイスでイネーブルにしないでください。
- Cisco TrustSec 出力リフレクタをディセーブルにする前に、Cisco TrustSec 非対応スイッチング モジュールの電力を切る必要があります。
- Cisco TrustSec 入力のリフレクタはスイッチ上に設定しないでください。

VRF-Aware SXP

仮想ルーティングおよびフォワーディング（VRF）の SXP の実装は、特定の VRF と SXP 接続をバインドします。Cisco TrustSec をイネーブルにする前に、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。

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 SXP 接続のみをバインドできます。
- 別の VRF が重複する 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-SGT マッピングは、同じ VRF ドメインでのみ更新できます。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。
- VRF ごとに複数のアドレス ファミリがサポートされています。そのため、VRF ドメインの 1 つの SXP 接続が IPV4 および IPV6 両方の IP-SGT マッピングを転送できます。
- SXP には VRF あたりの接続数および IP-SGT マッピング数の制限はありません。

レイヤ 2 VRF-Aware SXP および VRF の割り当て

VRF からレイヤ 2 VLAN への割り当ては、**cts role-based l2-vrf vrf-name vlan-list** グローバル コンフィギュレーション コマンドで指定されます。VLAN は VLAN 上に IP アドレスが設定されたスイッチ仮想インターフェイス（SVI）がない限り、レイヤ 2 VLAN と見なされます。VLAN の SVI に IP アドレスが設定されると、VLAN はレイヤ 3 VLAN になります。

cts role-based l2-vrf コマンドで設定された VRF 割り当ては、VLAN がレイヤ 2 VLAN として維持されている間はアクティブです。VRF の割り当てがアクティブな間に、学習した IP-SGT バインディングも VRF と IP プロトコルバージョンに関連付けられた転送情報ベース（FIB）テーブルに追加されます。VLAN の SVI がアクティブになると、VRF から VLAN への割り当てが非アクティブになり、VLAN で学習したすべてのバインドが SVI の VRF に関連付けられた FIB テーブルに移動されます。

VRF から VLAN への割り当ては、割り当てが非アクティブになっても保持されます。SVI が削除された、または SVI の IP アドレスの設定が解除された場合に再アクティブ化されます。再アクティブ化された場合、IP-SGT バインドは、SVI の FIB に関連付けられた FIB テーブルから、**cts role-based l2-vrf** コマンドによって割り当てられた VRF に関連付けられた FIB テーブルに戻されます。

Cisco TrustSec の概要の機能情報

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* の概要の機能情報

機能名	リリース	機能情報
Cisco TrustSec の概要	Cisco IOS XE Denali 16.1.1	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。