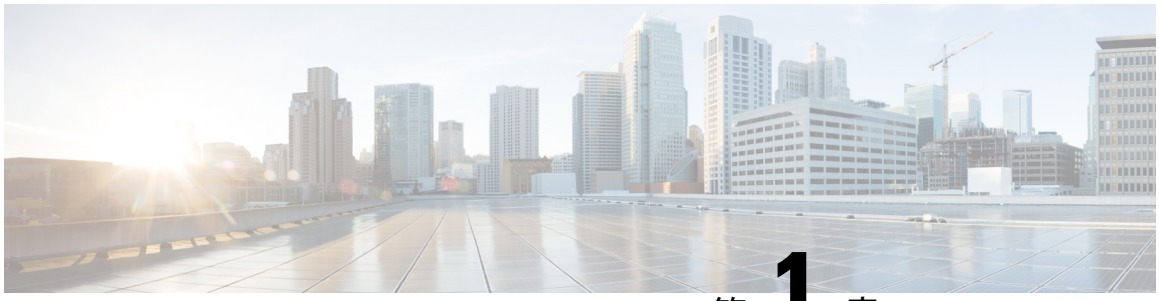
Cisco IOS XE Gibraltar 16.12.x（Catalyst 3650 スイッチ）Cisco TrustSec コンフィギュレーション ガイド

初版：2019 年 7 月 31 日

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

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。

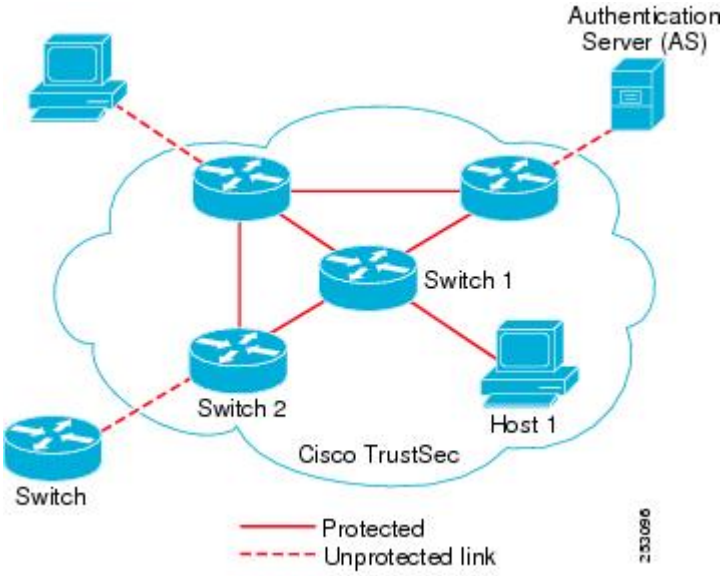
（注） Cisco TrustSec IEEE 802.1X リンクは、Cisco IOS XE Denali、Cisco IOS XE Everest、および Cisco IOS XE Fuji リリースでサポートされているプラットフォームではサポートされていないため、オーセンティケータのみがサポートされます。サプリカントはサポートされていません。

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。

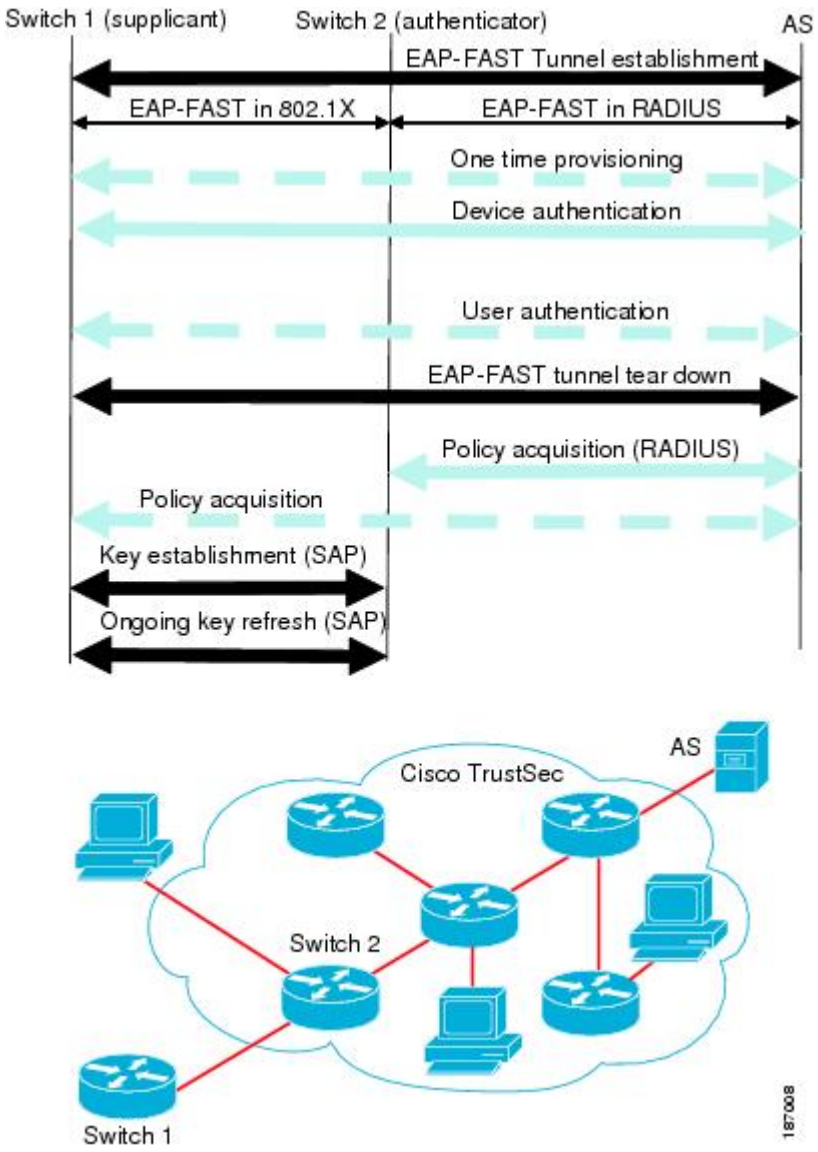
認証

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。

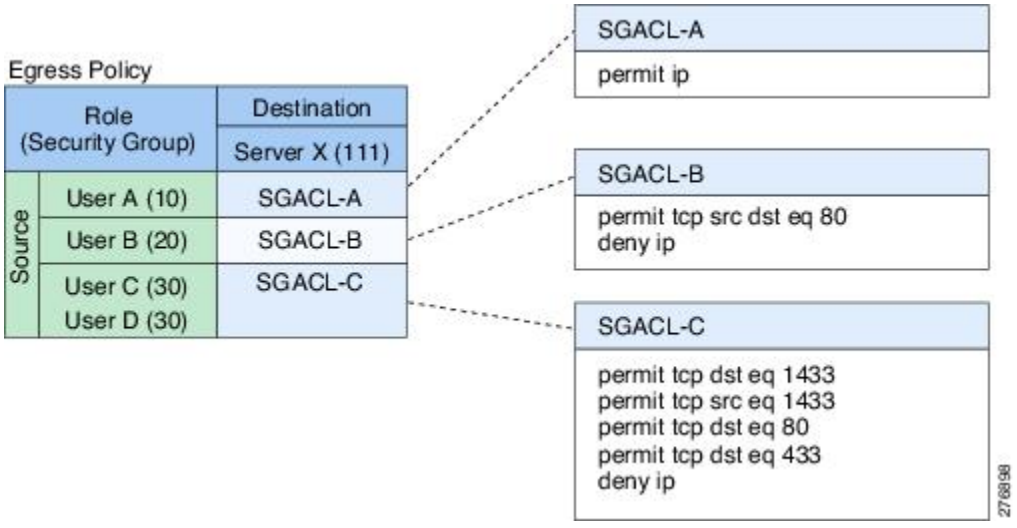
SGT には、送信元のセキュリティ グループが含まれているため、タグは送信元 SGT と呼ばれることもあります。宛先デバイスもまたセキュリティグループ（宛先 SG）に割り当てられるため、便宜上、このセキュリティグループを接続先グループタグ（DGT）と呼ぶこともあります。ただし、実際の Cisco TrustSec パケットタグには、宛先デバイスのセキュリティグループ番号は含まれていません。

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。

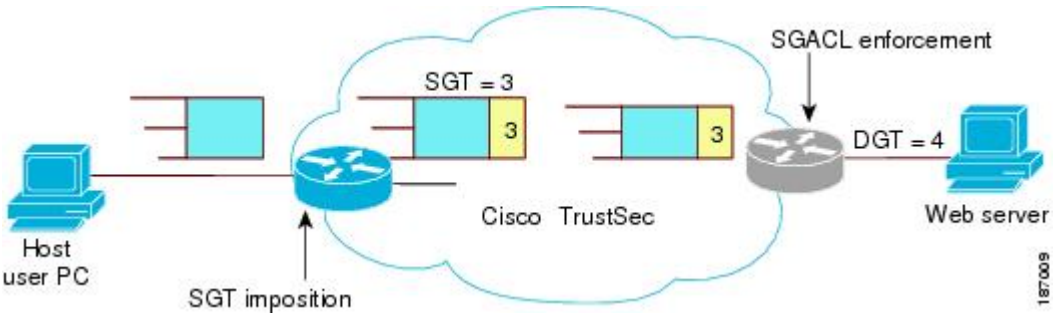
ロール ベースの許可を使用すると ACL のサイズが大幅に節約され、メンテナンス作業も簡単になります。Cisco TrustSec によって、設定されているアクセス コントロール エントリ（ACE）の数は、指定されている許可の数によって決定されるため、ACE の数は従来の IP ネットワークでよりもずっと小さくなります。Cisco TrustSec での SGACL の使用は、従来の ACL と比較して TCAM リソースをより効率的に使用します。

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。

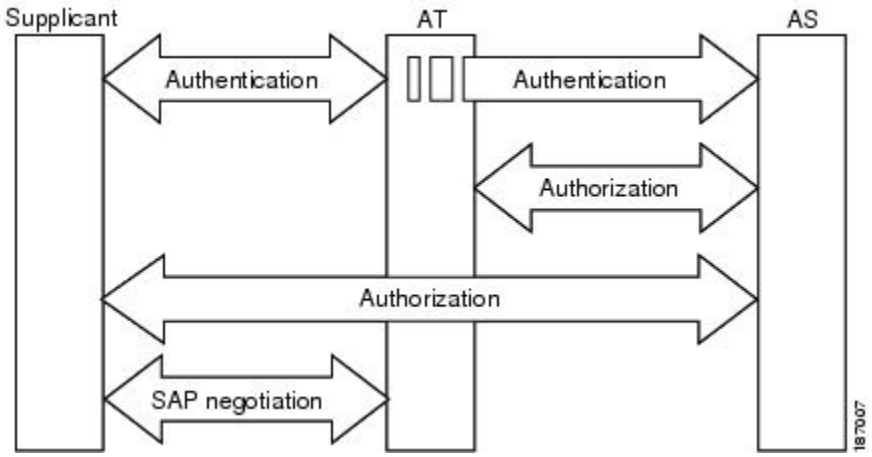
認証サーバは次の属性を返します。

- 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

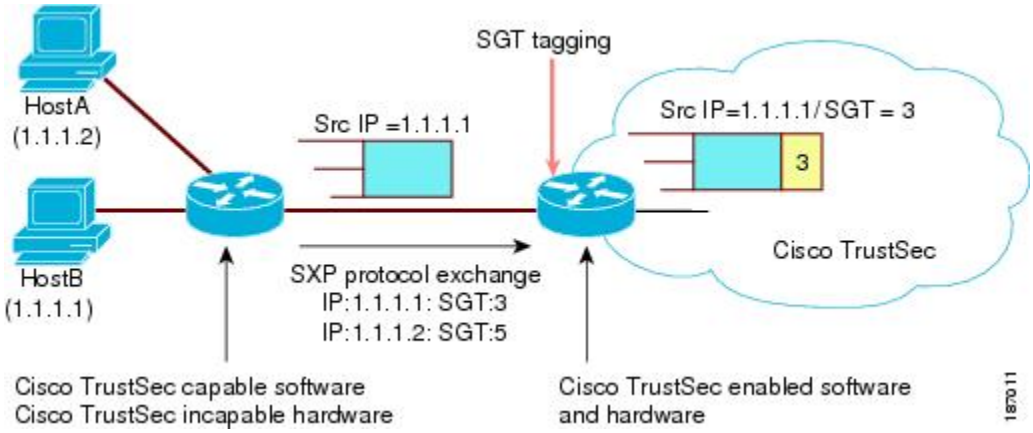
SXP によるレガシー アクセス ネットワークへの SGT の伝播

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。

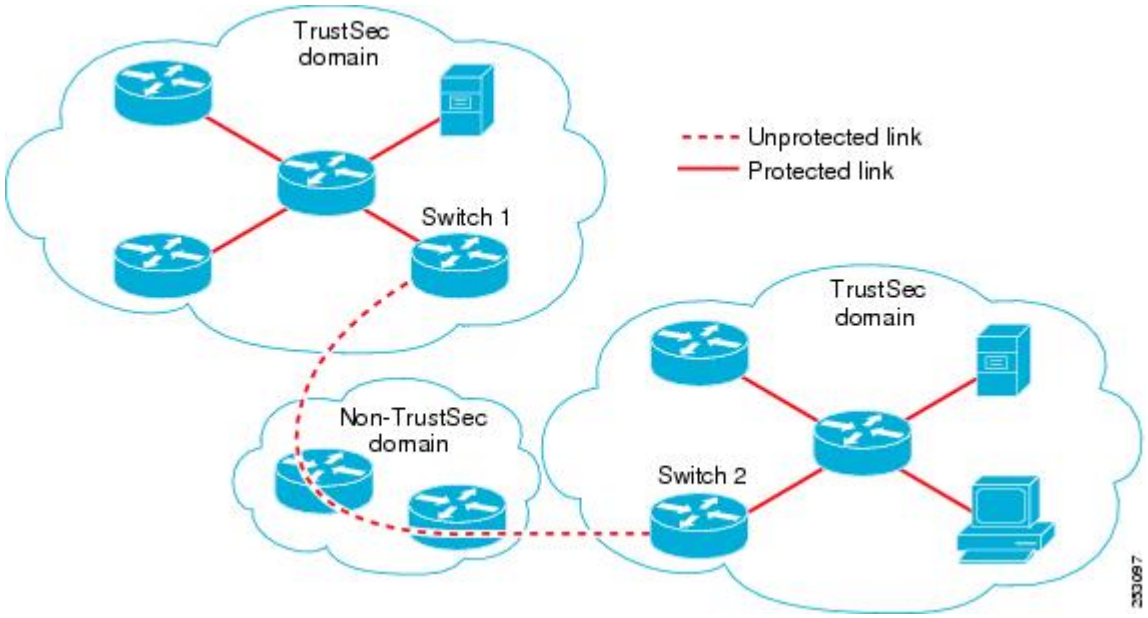
SXP は複数のホップを許可します。つまり、Cisco TrustSec ハードウェア サポート対象外デバイスのピアが Cisco TrustSec ハードウェア サポートの対象外でもある場合、2 番目のピアはハードウェア対応ピアに到達するまで IP と SGT のマッピング情報の伝播を継続して、3 番目のピアへの SXP 接続を設定できます。デバイスは 1 つの SXP 接続では SXP リスナーとして、別の SXP 接続では SXP スピーカーとして設定できます。

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。

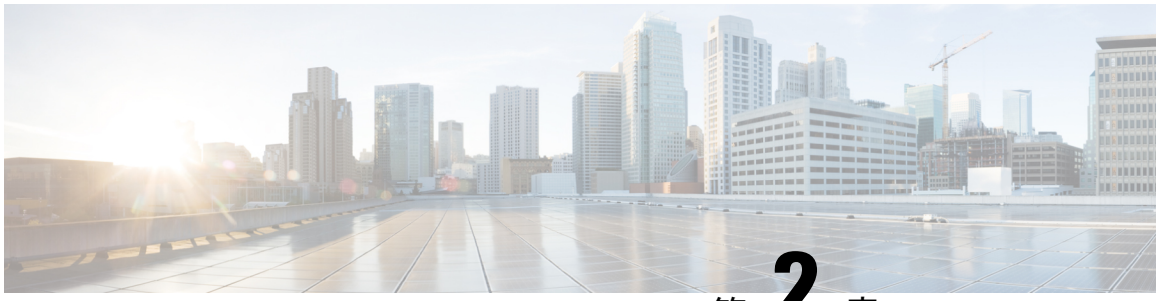
Cisco TrustSec の概要の機能情報

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。



第 2 章

アイデンティティ、接続および SGT の設定

アイデンティティと接続の設定

このモジュールでは、次の機能について説明します。

- Cisco TrustSec シード デバイスのクレデンシャル、AAA 設定
- Cisco TrustSec 非シード デバイスのクレデンシャル、AAA 設定
- アップリンクポートでの 802.1X モードの Cisco TrustSec 認証と Macsec
- アップリンクポートでの手動モードの Cisco TrustSec と MACsec
- インターフェイスの SAP キーの再生成

アイデンティティと接続の設定方法

Cisco TrustSec シード デバイスのクレデンシャル、AAA 設定

認証サーバに直接接続されているか、または接続は間接でも TrustSec ドメインを開始する最初のデバイスである Cisco TrustSec 対応デバイスは、シード デバイスと呼ばれます。他の Cisco TrustSec ネットワーク デバイスは非シード デバイスです。

（注）

- Cisco Identity Services Engine（Cisco ISE）または Cisco Secure Access Control Server（Cisco ACS）にも、デバイスの Cisco TrustSec クレデンシャルを設定する必要があります。
- **cts authorization list** コマンドは、Cisco Identity Services Engine（ISE）から Cisco TrustSec 環境データと SGACL ポリシーをダウンロードするように設定する必要があります。

Cisco TrustSec ドメインを開始できるように、シードスイッチで NDAC および AAA をイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**cts credentials id** *device-id* **password** *password* 例： `Device# cts credentials id Switch1 password Cisco123`	EAP-FAST を使用して他の Cisco TrustSec デバイスで認証するときにこのスイッチが使用する Cisco TrustSec デバイス ID およびパスワードを指定します。*device-id* 引数は、最大 32 文字で大文字と小文字を区別します。
ステップ 2	**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 3	**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 4	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 5	**aaa authentication dot1x default group radius** 例： `Device(config)# aaa authentication dot1x default group radius`	RADIUS として 802.1X ポート ベース認証方式を指定します。
ステップ 6	**aaa authorization network** *mlist* **group radius** 例： `Device(config)# aaa authorization network mlist group radius`	ネットワーク関連のすべてのサービス要求に対して RADIUS 認証を使用するようにスイッチを設定します。 • *mlist*：Cisco TrustSec AAA サーバ グループ。
ステップ 7	**cts authorization list** *mlist* 例： `Device(config)# cts authorization list mlist`	Cisco TrustSec の AAA サーバ グループを指定します。非シード デバイスはオーセンティケータからサーバ リストを取得します。

	コマンドまたはアクション	目的
ステップ 8	**aaa accounting dot1x default start-stop group radius** 例： `Device(config)# aaa accounting dot1x default start-stop group radius`	RADIUS を使用して 802.1X アカウンティングをイネーブルにします。
ステップ 9	**radius-server host** *ip-addr* **auth-port 1812 acct-port 1813 pac key** *secret* 例： `Device(config)# radius-server host 10.20.3.1 auth-port 1812 acct-port 1813 pac key AbCe1234`	RADIUS 認証サーバのホスト アドレス、サービス ポートおよび暗号キーを指定します。 • *ip-addr*：認証サーバの IP アドレス。 • *secret*：認証サーバによって共有される暗号キー。
ステップ 10	**radius-server vsa send authentication** 例： `Device(config)# radius-server vsa send authentication`	認証段階でスイッチによって生成される RADIUS Access-Request 内のベンダー固有属性（VSA）を認識して使用するようにスイッチを設定します。
ステップ 11	**dot1x system-auth-control** 例： `Device(config)# dot1x system-auth-control`	802.1x ポートベースの認証をグローバルにイネーブルにします。
ステップ 12	**exit** 例： `Device(config)# exit`	設定モードを終了します。

Cisco TrustSec 非シード デバイスのクレデンシャル、AAA 設定

（注） Cisco Identity Services Engine または Cisco Secure ACS にも、スイッチの Cisco TrustSec クレデンシャルを設定する必要があります。

Cisco TrustSec ドメインに参加できるように、非シードスイッチで NDAC および AAA をイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**cts credentials id** *device-id* **password** *password* 例： `Device# cts credentials id device-id password password`	EAP-FAST を使用して他の Cisco TrustSec デバイスで認証するときにこのスイッチが使用する Cisco TrustSec デバイス ID およびパスワードを指定します。*device-id* 引数は、最大 32 文字で大文字と小文字を区別します。
ステップ 2	**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 3	**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 4	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 5	**aaa authentication dot1x default group radius** 例： `Device(config)# aaa authentication dot1x default group radius`	RADIUS として 802.1X ポート ベース認証方式を指定します。
ステップ 6	**aaa authorization network** *mlist* **group radius** 例： `Device(config)# aaa authorization network mlist group radius`	ネットワーク関連のすべてのサービス要求に対して RADIUS 認証を使用するようにスイッチを設定します。 • *mlist*：Cisco TrustSec の AAA サーバグループを指定します。
ステップ 7	**aaa accounting dot1x default start-stop group radius** 例： `Device(config)# aaa accounting dot1x default start-stop group radius`	RADIUS を使用して 802.1X アカウンティングをイネーブルにします。
ステップ 8	**radius-server vsa send authentication** 例： `Device(config)# radius-server vsa send authentication`	認証段階でスイッチによって生成される RADIUS Access-Request 内のベンダー固有属性（VSA）を認識して使用するようにスイッチを設定します。

	コマンドまたはアクション	目的
ステップ 9	**dot1x system-auth-control** 例： `Device(config)# dot1x system-auth-control`	802.1x ポートベースの認証をグローバルにイネーブルにします。
ステップ 10	**exit** 例： `Device(config)# exit`	設定モードを終了します。

アップリンクポートでの手動モードの Cisco TrustSec と MACsec の設定

（注） Cisco Catalyst 9400 シリーズ スイッチ は MACsec をサポートしていません。

インターフェイス上で Cisco TrustSec を手動で設定できます。接続の両側のインターフェイスに手動で設定する必要があります。認証は行われません。ポリシーは静的に設定することも、サーバのデバイスアイデンティティを指定して認証サーバから動的にダウンロードすることもできます。

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** *type slot/port* 例： `Device(config)# interface gi 2/1`	アップリンク インターフェイスのインターフェイス 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`	Cisco TrustSec 手動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	[**no**] **sap pmk** *key* [**mode-list** *mode1* [*mode2* [*mode3* [*mode4*]]]] 例：	（任意）SAP のペアワイズマスターキー（PMK）と動作モードを設定します。Cisco TrustSec の手動モードでは、

	コマンドまたはアクション	目的
	`Device(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm null no-encap`	SAP はデフォルトでディセーブルになっています。 • *key*：文字数が偶数個で最大 32 文字の 16 進値。 SAP 動作の mode オプションは次のとおりです。 • **gcm**：認証あり、暗号化あり • **gmac**：認証あり、暗号化なし • **no-encap**：カプセル化なし • **null**：カプセル化あり、認証なし、暗号化なし （注） MACsec with SAP は、Catalyst 3K スイッチではサポートされていません。 （注） インターフェイスで SGT 挿入またはデータリンク暗号化を使用できない場合は、デフォルトおよび唯一使用可能な SAP 動作モードは no-encap です。
ステップ 6	[**no**] **policy dynamic identity** *peer-name* 例： `Device(config-if-cts-manual)# policy dynamic identity my_cisco_ise_id`	（任意）ピアのアイデンティティに基づいた認可サーバからの認可ポリシーの動的ダウンロードを許可するようにアイデンティティ ポート マッピング（IPM）を設定します。この作業の次に記載されている追加の使用上の注意を参照してください。 • *peer-name*：ピアデバイスの Cisco TrustSec デバイス ID。ピア名では、大文字と小文字が区別されます。

	コマンドまたはアクション	目的
		（注） Cisco TrustSec クレデンシャルが設定されていることを確認します（Cisco TrustSec シード デバイスのクレデンシャル、AAA 設定 （21 ページ）を参照）
ステップ 7	[**no**] **policy static sgt** *tag* **[trusted]** 例： `Device(config-if-cts-manual)# policy static sgt 111`	（任意）スタティック許可ポリシーを設定します。この作業の次に記載されている追加の使用上の注意を参照してください。 • *tag*：10 進表記の SGT。指定できる範囲は 1 ～ 65533 です。 • **trusted**：この SGT を使用するインターフェイスの入力トラフィックのタグを上書きしてはいけないことを示します。
ステップ 8	**[no] propagate sgt** 例： `Device(config-if-cts-manual)# propagate sgt`	（任意）このコマンドの no 形式は、ピアが SGT を処理できない場合に使用されます。**no propagate sgt** コマンドを使用すると、インターフェイスからピアに SGT が送信されなくなります。
ステップ 9	**exit** 例： `Device(config-if-cts-manual)# exit`	Cisco TrustSec 手動インターフェイス コンフィギュレーション モードを終了します。
ステップ 10	**shutdown** 例： `Device(config-if)# shutdown`	インターフェイスをディセーブルにします。
ステップ 11	**no shutdown** 例： `Device(config-if)# no shutdown`	インターフェイスをイネーブルにして、インターフェイスの Cisco TrustSec 認証をイネーブルにします。
ステップ 12	**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 モードを終了します。

例

インターフェイスの SAP キーの再生成

暗号キーを手動で更新する機能は、多くの場合、ネットワーク アドミニストレーションのセキュリティ要件の一部です。SAP キー リフレッシュは通常、ネットワーク イベントおよび設定不可能な内部タイマーの組み合わせによりトリガーされ、自動的に行われます。

手順

	コマンドまたはアクション	目的
ステップ 1	**cts rekey interface** *type slot/port* 例： `Device# cts rekey int gig 1/1`	MACsec リンクで SAP キーの再ネゴシエーションを強制します。

追加認証サーバ関連のパラメータの設定

スイッチと Cisco TrustSec サーバ間の相互対話を設定するには、次の作業を 1 つまたは複数行います。

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 server deadtime** *seconds* 例： `Device(config)# cts server deadtime 20`	（任意）いったん停止中としてマークされたグループ内のサーバを、どのくらいの期間、サービス用に選択してはいけないかを指定します。デフォルトは 20 秒です。指定できる範囲は 1 ～ 864000 です。
ステップ 4	**cts server load-balance method least-outstanding** [**batch-size** *transactions*] [**ignore-preferred-server**] 例：	（任意）Cisco TrustSec プライベート サーバ グループに RADIUS ロード バランシングをイネーブルにし、最も未処理のトランザクションが少ないサーバを選択します。デフォルトでは、ロード バ

	コマンドまたはアクション	目的
	`Device(config)# cts server load-balance method least-outstanding batch-size 50 ignore-preferred-server`	ランシングは適用されません。デフォルトの transactions は 25 です。 **ignore-preferred-server** キーワードは、セッション全体を通じて同じサーバを使用しないようにスイッチに指示します。
ステップ 5	**cts server test** {*server-IP-address* | **all**} { **deadtime** *seconds* | **enable** | **idle-time** *seconds* } 例： `Device(config)# cts server test 10.15.20.102 idle-time 120`	（任意）指定されたサーバまたはダイナミック サーバ リスト内のすべてのサーバに対してサーバ存続性テストを設定します。デフォルトでは、テストはすべてのサーバに対してイネーブルになっています。デフォルトの **idle-time** は 60 秒で、範囲は 1 ～ 14400 です。
ステップ 6	**exit** 例： `Device(config)# exit`	設定モードを終了します。
ステップ 7	**show cts server-list** 例： `Device# show cts server-list`	Cisco TrustSec サーバのリストのステータスおよび設定の詳細を表示します。

アイデンティティと接続の設定例

例：非シードデバイスの設定

伝播 SGT がデフォルトではないアクセス VLAN の Catalyst 3850/3650 の例：

```
switch(config-if)# switchport access vlan 222
switch(config-if)# switchport mode access
switch(config-if)# authentication port-control auto
switch(config-if)# dot1x pae authenticator
switch(config-if)# cts dot1x
switch(config-if)# propagate sgt
```

例：アップリンクポートでの手動モードと MACsec の設定

手動モードでの Catalyst 3650 および 3850 Cisco TrustSec インターフェイスの設定：

```
Device# configure terminal
Device(config)# interface gig 1/0/5
Device(config-if)# cts manual
Device(config-if-cts-manual)# policy dynamic identity my_cisco_ise_id
Device(config-if-cts-manual)# exit
Device(config-if)# shutdown
```

```
Device(config-if)# no shutdown
Device(config-if)# end
```

例：追加認証サーバ関連のパラメータの設定

スイッチと Cisco TrustSec サーバ間の相互対話を設定するには、次の作業を 1 つまたは複数行います。

次に、サーバ設定を設定して Cisco TrustSec サーバ リストを表示する例を示します。

```
Device# configure terminal
Device(config)# cts server load-balance method least-outstanding batch-size 50
ignore-preferred-server
Device(config)# cts server test all deadtime 20
Device(config)# cts server test all enable
Device(config)# exit
Device#show cts server-list
CTS Server Radius Load Balance = ENABLED
    Method   = least-outstandin
    Batch size = 50
    Ignore preferred server
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)

Preferred list, 1 server(s):
*Server: 10.15.20.102, port 1812, A-ID 87B3503255C4384485BB808DC24C6F55
               Status = ALIVE
               auto-test = TRUE, idle-time = 120 mins, deadtime = 20 secs
Installed list: SL1-1E6E6AE57D4E2A9B320D1844C68BA291, 3 server(s):
  *Server: 10.15.20.102, port 1812, A-ID 87B3503255C4384485BB808DC24C6F55
               Status = ALIVE
               auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
  *Server: 10.15.20.101, port 1812, A-ID 255C438487B3503485BBC6F55808DC24
               Status = ALIVE
               auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
Installed list: SL2-1E6E6AE57D4E2A9B320D1844C68BA293, 3 server(s):
  *Server: 10.0.0.1, port 1812, A-ID 04758B1F05D8C1439F27F9509E07CFB6.
               Status = ALIVE
               auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
  *Server: 10.0.0.2, port 1812, A-ID 04758B1F05D8C1439F27F9509E07CFB6.
               Status = DEAD
               auto-test = TRUE, idle-time = 60 mins, deadtime = 20 sec
```

Cisco TrustSec インターフェイス設定の確認

Cisco TrustSec 関連のインターフェイスの設定を表示するには、を使用します。 **show cts interface**

Cisco 3850 TrustSec インターフェイスクエリ：

```
Device> show cts interface gigabitethernet 1/0/6

Global Dot1x feature is Disabled
Interface GigabitEthernet1/0/6:
    CTS is enabled, mode:    MANUAL
    IFC state:               INIT
    Authentication Status:   NOT APPLICABLE
```

```
        Peer identity:       "unknown"
        Peer's advertised capabilities: ""
    Authorization Status:    NOT APPLICABLE
    SAP Status:              NOT APPLICABLE
    Propagate SGT:           Enabled
    Cache Info:
        Expiration            : N/A
        Cache applied to link : NONE

Statistics:
        authc success:              0
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                0
        sap fail:                   0
        authz success:              0
        authz fail:                 0
        port auth fail:             0

L3 IPM:     disabled.
```

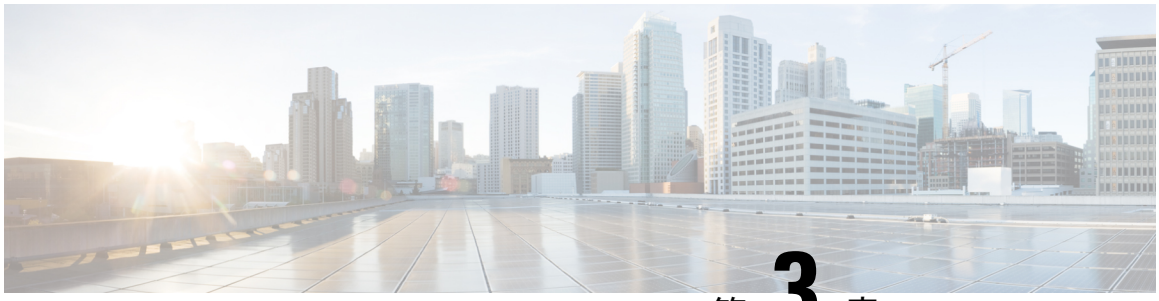
アイデンティティ、接続、SGT の機能情報

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:* アイデンティティ、接続、*SGT* の機能情報

機能名	リリース	機能情報
アイデンティティ、接続および SGT	Cisco IOS XE Denali 16.1.1	この機能が導入されました。



第 3 章

セキュリティグループACLポリシーの設定

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。

セキュリティ グループ アクセス コントロール リスト（SGACL）の制約事項

Cisco Catalyst 3650 シリーズ スイッチおよび Cisco Catalyst 3850 シリーズ スイッチには、次の制限が適用されます。

- ハードウェアの制限により、CTS SGACL はハードウェアのパント（CPU バウンド）トラフィックに適用できません。

SGACL ポリシーの設定方法

このセクションでは、さまざまな SGACL ポリシー設定について説明します。

SGACL ポリシーの設定プロセス

Cisco TrustSec のセキュリティグループ ACL（SGACL）ポリシーを設定してイネーブルにするには、次の手順を実行します。

1. SGACL ポリシーの設定は、Cisco Secure Access Control Server（ACS）または Cisco Identity Services Engine（ISE）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。

   SGACL ポリシーの設定のダウンロードに Cisco Secure ACS または Cisco ISE 上の AAA を使用しない場合は、SGACL のマッピングとポリシーを手動で設定できます。

（注） Cisco Secure ACS または Cisco ISE からダイナミックにダウンロードされた SGACL ポリシーは、競合のローカル定義されたポリシーよりも優先されます。

2. ルーテッドポートの出力トラフィックに対する SGACL ポリシーの適用を有効にするには、「SGACL ポリシーの適用のグローバルな有効化」セクションに記載されているように、SGACL ポリシー適用を有効にします。
3. VLAN 内のスイッチングされたトラフィック、または VLAN に関連付けられた SVI に転送されるトラフィックに対して SGACL ポリシーの適用を有効にするには、「VLAN に対する SGACL ポリシーの適用の有効化」セクションの説明に従って、特定の VLAN に対して SGACL ポリシーの適用を有効にします。

SGACL ポリシーの適用のグローバルな有効化

Cisco TrustSec をイネーブルにしたルーテッド インターフェイスで SGACL ポリシーの強制をグローバルにイネーブルにする必要があります。

ルーテッドインターフェイスの SGACL ポリシーの強制をイネーブルにするには、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。

	コマンドまたはアクション	目的
ステップ 3	**cts role-based enforcement** 例： `Device(config)# cts role-based enforcement`	ルーテッド インターフェイスで Cisco TrustSec SGACL ポリシーの強制をイネーブルにします。

インターフェイスあたりの SGACL ポリシーの適用の有効化

まず、Cisco TrustSec を有効にしたルーテッドインターフェイスで SGACL ポリシーの適用をグローバルに有効にする必要があります。この機能はポート チャネル インターフェイスではサポートされません。

レイヤ 3 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	**interface** *type slot/port* 例： `Device(config)# interface gigabitethernet 6/2`	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 enforcement** 例： `Device(config-if)# cts role-based enforcement`	ルーテッド インターフェイスで Cisco TrustSec SGACL ポリシーの強制をイネーブルにします。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show cts interface** 例： `Device# show cts interface`	インターフェイスごとの Cisco TrustSec ステートおよび統計情報を表示します。

VLAN に対する SGACL ポリシーの強制のイネーブル化

VLAN 内のスイッチングされたトラフィック、または VLAN に関連付けられた SVI に転送されるトラフィックに対してアクセス コントロールを適用するには、特定の VLAN に対して SGACL ポリシーの強制をイネーブルにする必要があります。

VLAN または VLAN リスト内で、SGACL ポリシーの強制をイネーブルにするには、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 role-based enforcement vlan-list** *vlan-list* 例： `Device(config)# cts role-based enforcement vlan-list 31-35,41`	VLAN または VLAN リストで Cisco TrustSec SGACL ポリシーの強制をイネーブルにします。

SGACL モニタ モードの設定

SGACL モニタモードを設定する前に、次の点を確認してください。

- Cisco TrustSec が有効になっている。
- カウンタが有効になっている。

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 monitor enable** 例： `Device(config)# cts role-based monitor enable`	デバイスレベルのモニタモードをイネーブルにします。 • デフォルトでは、デバイスレベルのモニタモードは有効になっています。デバイスモニタモードが無効な場合でも、モニタモード情報はISEからダウンロードされますが、この設定がオンになるまでデバイスに適用されません。
ステップ 4	**cts role-based monitor permissions from** {*sgt_num*} **to** {*dgt_num*} [**ipv4** | **ipv6**] 例： `Device(config)# cts role-based permissions from 2 to 3 ipv4`	IPv4/IPv6 ロール ベースアクセス制御リスト（RBACL）（セキュリティグループタグ（SGT）：接続先グループタグ（DGT）ペア）のモニタモードを有効にします。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show cts role-based monitor permissions from** {*sgt_num*} **to** {*dgt_num*} [**ipv4** | **ipv6**] [**details**] 例： `Device# show cts role-based permissions from 2 to 3 ipv4 details`	SGACL ポリシーとペアごとのモニタモード機能に関する詳細を表示します。<SGT-DGT> ペアでセルごとのモニタモードが有効になっている場合、コマンド出力にはモニタ対象が表示されます。
ステップ 7	**show cts role-based counters** [**ipv4** | **ipv6**] 例： `Device# show cts role-based counters ipv4`	IPv4 および IPv6 イベントのすべての SGACL 適用の統計情報を表示します。

SGACL ポリシーの手動設定

SGT と DGT の範囲にバインドされたロールベースアクセス制御リストは、出力トラフィックに適用される Cisco TrustSec ポリシーである SGACL を形成します。SGACL ポリシーの設定は、Cisco ISE または Cisco Secure ACS のポリシー管理機能を使用して行うのが最適です。手動で（ローカルに）SGACL ポリシーを設定するには、次の手順を実行します。

1. ロールベース ACL を設定します。
2. ロールベース ACL を SGT の範囲にバインドします。

（注） Cisco ISE または Cisco ACS からダイナミックにダウンロードされた SGACL ポリシーは、競合の手動設定されたポリシーよりも優先されます。

IPv4 SGACL ポリシーの手動設定と適用

（注） SGACL およびロールベース アクセス コントロール リスト（RBACL）を設定する場合、名前付きアクセスコントロールリスト（ACL）はアルファベットで始まる必要があります。

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	**ip access-list role-based** *rbacl-name* 例： `Device(config)# ip access-list role-based allow_webtraff`	ロールベースの ACL を作成して、ロールベース ACL 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	{ [*sequence-number*] | **default** | **permit** | **deny** | **remark**} 例： `Device(config-rb-acl)# 10 permit tcp dst eq 80 dst eq 20`	RBACL のアクセス コントロール エントリ（ACE）を指定します。 拡張名前付きアクセス リスト コンフィギュレーション モードで使用可能なコマンドおよびオプションの大部分を、送信元および宛先フィールドを省略して使用できます。 Enter キーを押して ACE を完了し、次の手順を開始します。 次の ACE コマンドまたはキーワードはサポートされていません。 • **reflect** • **evaluate**

	コマンドまたはアクション	目的
		• **time-range**
ステップ 5	**exit** 例： `Device(config-rb-acl)# exit`	ロールベース ACL 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	**cts role-based permissions {default** | **[from** {*sgt_num* | **unknown**} **to** {*dgt_num* | **unknown** }] {*rbacls* | **ipv4** *rbacls*} 例： `Device(config)# cts role-based permissions from 55 to 66 allow_webtraff`	SGT と DGT を RBACL にバインドします。この設定は、Cisco ISE または Cisco Secure ACS で設定された許可マトリックスにデータを入力することに似ています。 • Default：デフォルトの権限リスト • *sgt_num*：0 ー 65,519。送信元グループタグ。 • *dgt_num*：0 ー 65,519 接続先グループタグ。 • unknown：SGACL がセキュリティグループ（送信元または宛先）を特定できないパケットに適用されます。 • ipv4：次の RBACL が IPv4 であることを示します。 • *rbacls*：RBACL の名前
ステップ 7	**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。
ステップ 8	**show cts role-based permissions** 例： `Device# show cts role-based permissions`	RBACL 設定に対する権限を表示します。
ステップ 9	**show ip access-lists** {*rbacls* | **ipv4** *rbacls*} 例： `Device# show ip access-lists allow_webtraff`	すべての RBACL または指定された RBACL の ACE を表示します。

IPv6 ポリシーの設定

IPv6 SGACL ポリシーを手動で設定するには、次の作業を行います。

（注） IPv6 SGACL は、Cisco IOS XE Everest 16.8.1 ではサポートされていません。

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	**ipv6 access-list role-based** *sgacl-name* 例： `Device(config)# ipv6 access-list role-based sgaclname`	名前付き IPv6 SGACL を作成して、IPv6 ロールベース ACL 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	{**permit** | **deny** } *protocol* [**dest-option** | **dest-option-type** {*doh-number* | *doh-type*}] [**dscp** *cp-value*] [**flow-label** *fl-value*] [**mobility** | **mobility-type** {*mh-number* | *mh-type*}] [**routing** | **routing-type** *routing-number*] [**fragments**] [**log** | **log-input**] [**sequence** *seqno*]	RBACL のアクセス コントロール エントリ（ACE）を指定します。 拡張名前付きアクセス リスト コンフィギュレーション モードで使用可能なコマンドおよびオプションの大部分を、送信元および宛先フィールドを省略して使用できます。 次の ACE コマンドまたはキーワードはサポートされていません。 • **reflect** • **evaluate** • **time-range**
ステップ 5	**end** 例： `Device(config-ipv6rb-acl)# end`	IPv6 ロールベース ACL 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。

手動で SGACL ポリシーを適用する方法

手動で SGACL ポリシーを適用するには、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 role-based permissions default** [**ipv4** | **ipv6**] *sgacl-name1* [*sgacl-name2* [*sgacl-name3 ...*]]] 例： `Device(config)# cts role-based permissions default MYDEFAULTSGACL`	デフォルト SGACL を指定します。デフォルト ポリシーは明示的なポリシーが送信元と宛先セキュリティ グループの間にない場合に適用されます。
ステップ 4	**cts role-based permissions from** {*source-sgt* | **unknown**} **to** {*dest-sgt* | **unknown**} [**ipv4** | **ipv6**] *sgacl-name1* [*sgacl-name2* [*sgacl-name3 ...*]]] 例： `Device(config)# cts role-based permissions from 3 to 5 SRB3 SRB5`	送信元セキュリティ グループ（SGT）と宛先セキュリティ グループ（DGT）に適用する SGACL を指定します。source-sgt と dest-sgt の値範囲は 1 ～ 65533 です。デフォルトでは、SGACL は IPv4 であると見なされます。 • **from**：送信元 SGT を指定します。 • **to**：宛先セキュリティグループを指定します。 • **unknown**：SGACL がセキュリティ グループ（送信元または宛先）を特定できないパケットに適用されます。 （注） ACS から動的にダウンロードされた SGACL ポリシーは、競合の手動ポリシーよりも優先されます。

SGACL ポリシーの表示

Cisco TrustSec デバイス クレデンシャルと AAA の設定後、認証サーバからダウンロードされたか、または手動で設定された Cisco TrustSec SGACL ポリシーを検証できます。Cisco TrustSec は、インターフェイスに対する認証および許可、SXP、または IP アドレスおよび SGT の手動マッピングによって新しい SGT を学習すると、SGACL ポリシーをダウンロードします。

キーワードを使用して、許可マトリクスの全部または一部を表示できます。

- **from** キーワードを省略すると、許可マトリックスのカラムが表示されます。
- **to** キーワードを省略すると、許可マトリックスの行が表示されます。
- **from** および **to** キーワードを省略すると、許可マトリックス全体が表示されます。
- **from** および **to** キーワードが指定されている場合、許可マトリックスから 1 つのセルが表示され、**details** キーワードを使用できます。**details** が入力された場合、1 つのセルの SGACL の ACE が表示されます。

SGACL ポリシーの許可マトリクスの内容を表示するには、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	**show cts role-based permissions default** [**ipv4** | **ipv6** | **details**] 例： `Device(config)# show cts role-based permissions default MYDEFAULTSGACL`	デフォルト ポリシーの SGACL のリストを表示します。
ステップ 3	**show cts role-based permissions from** {*source-sgt* | **unknown**} **to** {*dest-sgt* | **unknown**}] [**ipv4** | **ipv6** | **details**] 例： `Device(config)# show cts role-based permissions from 3`	送信元セキュリティ グループ（SGT）と宛先セキュリティ グループ（DGT）に適用する SGACL を指定します。source-sgt と dest-sgt の値範囲は 1 ～ 65533 です。デフォルトでは、SGACL は IPv4 であると見なされます。 • **from**：送信元 SGT を指定します。 • **to**：宛先セキュリティグループを指定します。 • **unknown**：SGACL がセキュリティグループ（送信元または宛先）を特

	コマンドまたはアクション	目的
		定できないパケットに適用されます。 （注） ACS から動的にダウンロードされた SGACL ポリシーは、競合の手動ポリシーよりも優先されます。

ダウンロードされた SGACL ポリシーのリフレッシュ

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 refresh policy** {**peer** [*peer-id*] | **sgt** [*sgt_number* | **default** | **unknown**]} 例： `Device(config)# cts refresh policy peer my_cisco_ise`	認証サーバからの SGACL ポリシーの即時リフレッシュを実行します。 • *peer-id* が指定される場合、指定されたピア接続に関連するポリシーだけがリフレッシュされます。すべてのピア ポリシーを更新するには、ID を指定しないで Enter を押します。 • SGT 番号が指定されている場合、その SGT に関連するポリシーだけがリフレッシュされます。すべてのセキュリティ グループ タグ ポリシーをリフレッシュするには、SGT 番号を指定せずに Enter を押します。デフォルトポリシーをリフレッシュするには、default を選択します。不明なポリシーをリフレッシュするには、unknown を選択します。

SGACL ポリシーの設定例

次のセクションでは、さまざまな SGACK ポリシーの設定例を示します。

例：SGACL ポリシーの適用のグローバルな有効化

```
Device# configure terminal
Device(config)# cts role-based enforcement
```

例：インターフェイスあたりの SGACL ポリシーの適用の有効化

```
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/2
Device(config-if)# cts role-based enforcement
Device(config-if)# end
```

例：VLAN に対する SGACL ポリシーの適用の有効化

```
Device# configure terminal
Device(config)# cts role-based enforcement vlan-list 31-35,41
Device(config)# exit
```

例：SGACL モニタモードの設定

```
Device# configure terminal
Device(config)# cts role-based monitor enable
Device(config)# cts role-based permissions from 2 to 3 ipv4
Device# show cts role-based permissions from 2 to 3 ipv4

IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
        denytcpudpicmp-10
        Deny IP-00

Device# show cts role-based permissions from 2 to 3 ipv4 details

IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
        denytcpudpicmp-10
        Deny IP-00
Details:
Role-based IP access list denytcpudpicmp-10 (downloaded)
        10 deny tcp
        20 deny udp
        30 deny icmp
Role-based IP access list Permit IP-00 (downloaded)
        10 permit ip

Device# show cts role-based counters ipv4

Role-based IPv4 counters
```

```
From     To     SW-Denied  HW-Denied  SW-Permitt  HW_Permitt  SW-Monitor  HW-Monitor
*         *     0          0          8           18962       0           0
2         3     0          0          0           0           0           341057
```

例：SGACL ポリシーの手動設定

```
Device# configure terminal
Device(config)# ip access role allow_webtraff
Device(config-rb-acl)# 10 permit tcp dst eq 80
Device(config-rb-acl)# 20 permit tcp dst eq 443
Device(config-rb-acl)# 30 permit icmp
Device(config-rb-acl)# 40 deny ip
Device(config-rb-acl)# exit
Device(config)# cts role-based permissions from 55 to 66 allow_webtraff
Device# show ip access allow_webtraff

Role-based IP access list allow_webtraff
    10 permit tcp dst eq www
    20 permit tcp dst eq 443
    30 permit icmp
    40 deny ip
Device# show show cts role-based permissions from 50 to 70
```

例：SGACL の手動適用

```
Device# configure terminal
Device(config)# cts role-based permissions default MYDEFAULTSGACL
Device(config)# cts role-based permissions from 3 to 5 SRB3 SRB5
Device(config)# exit
```

例：SGACL ポリシーの表示

次に、セキュリティ グループ 3 から送信されたトラフィックの SGACL ポリシーの許可マトリクスの内容を表示する例を示します。

```
Device# show cts role-based permissions from 3

Role-based permissions from group 3 to group 5:
        SRB3
        SRB5
Role-based permissions from group 3 to group 7:
        SRB4
```

SGACL ポリシーの機能情報

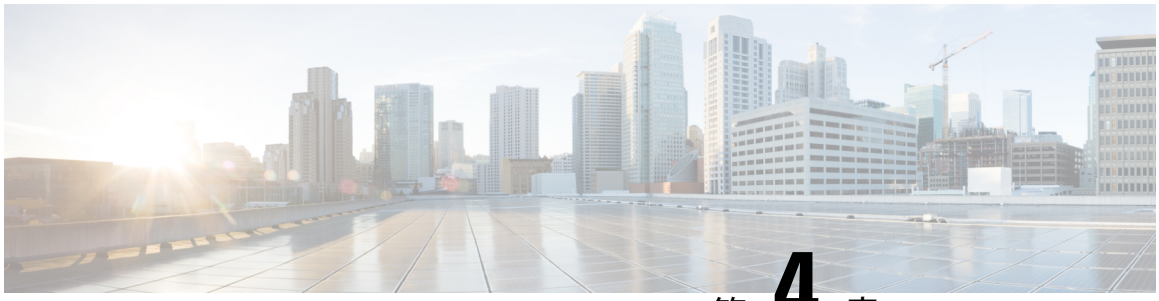
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

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 : SGACL* ポリシーの機能情報

機能名	リリース	機能情報
SGACL ポリシー	Cisco IOS XE Denali 16.1.1	この機能が導入されました。



第 4 章

Cisco TrustSec SGACL のハイ アベイラビリティ

Cisco TrustSec 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、Cisco StackWise 技術をサポートしているスイッチでのハイアベイラビリティ機能をサポートしています。この技術によってステートフルな冗長性が提供され、スイッチスタックはアクセス制御エントリを強制し、処理できます。

Cisco TrustSec SGACL のハイアベイラビリティの前提条件

このマニュアルでは、次のことを前提としています。

- Cisco TrustSec およびセキュリティ グループ アクセス コントロール リスト（SGACL）構成を理解している。
- デバイスは、スタックとして機能するように設定されている。
- スタック内のすべてのデバイスが同一バージョンの Cisco IOS XE ソフトウェアを実行している。

Cisco TrustSec SGACL のハイアベイラビリティの制約事項

- アクティブスイッチとスタンバイスイッチの両方で同時に障害が発生した場合、SGACL のステートフル スイッチオーバーは行われません。

Cisco TrustSec SGACL のハイアベイラビリティに関する情報

Cisco TrustSec 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、Cisco StackWise 技術をサポートしているスイッチでのハイアベイラビリティ機能をサポートしています。この技術によってステートフルな冗長性が提供され、スイッチスタックはアクセス制御エントリを強制し、処理できます。

この機能を有効にする Cisco TrustSec 固有の設定はありません。これは、Cisco IOS XE Denali 16.2.1 以降のリリースでサポートされます。

高可用性の概要

スイッチスタックでは、スタックマネージャが最も高い優先順位を持つスイッチをアクティブスイッチとして割り当て、次に高い優先順位を持つスイッチをスタンバイスイッチとして割り当てます。自動またはCLIベースのステートフルスイッチオーバー中は、スタンバイスイッチがアクティブスイッチになり、次に優先順位の高いスイッチがスタンバイスイッチになります。

運用データは、初期のシステムブートアップ、運用データの変更（認可変更（CoA）とも呼ばれる）、または運用データのリフレッシュ時に、アクティブスイッチからスタンバイスイッチに同期されます。

ステートフルスイッチオーバー中に、新たにアクティブになったスイッチは、運用データを要求してダウンロードします。環境データ（ENV-data）とロールベース アクセス コントロール リスト（RBACL）は、リフレッシュ時間が完了するまで更新されません。

次の運用データがアクティブスイッチにダウンロードされます。

- 環境データ（ENV-data）：リフレッシュ時または初期化時に RBACL 情報を取得するための優先サーバリストで構成される可変長フィールド。
- Protected Access Credential（PAC）：Authentication Protocol Flexible Authentication via the Secure Tunneling（EAP-FAST）のトンネルを保護するために、スイッチとオーセンティケータ間で相互に一意に共有される共有秘密。
- ロールベースのポリシー（RBACL またはSGACL）：スイッチ上のすべてのセキュリティグループタグ（SGT）マッピングのポリシー定義で構成される可変長ロールベースのポリシーリスト。

（注） デバイス ID とパスワードの詳細で構成される Cisco TrustSec クレデンシャルは、アクティブスイッチでコマンドとして実行されます。

Cisco TrustSec SGACL のハイアベイラビリティの確認

Cisco TrustSec SGACL ハイアベイラビリティ設定を確認するには、アクティブスイッチとスタンバイスイッチの両方で **show cts role-based permissions** コマンドを実行します。コマンドの出力は、両方のスイッチで同じである必要があります。

次に、アクティブスイッチでの **show cts role-based permissions** コマンドの出力例を示します。

```
Device# show cts role-based permissions

IPv4 Role-based permissions default (monitored):
        default_sgacl-01
        Deny IP-00
IPv4 Role-based permissions from group 10:SGT_10 to group 15:SGT_15:
        SGACL_3-01
IPv4 Role-based permissions from group 14:SGT_14 to group 15:SGT_15:
        multple_ace-14
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

次に、スタンバイスイッチでの show cts role-based permissions コマンドの出力例を示します。

```
Device-stby# show cts role-based permissions

IPv4 Role-based permissions default (monitored):
        default_sgacl-01
        Deny IP-00
IPv4 Role-based permissions from group 10:SGT_10 to group 15:SGT_15:
        SGACL_3-01
IPv4 Role-based permissions from group 14:SGT_14 to group 15:SGT_15:
        multple_ace-14
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

ステートフルスイッチオーバー後、アクティブスイッチで次のコマンドを実行して機能を確認します。

次に、**show cts pacs** コマンドの出力例を示します。

```
Device# show cts pacs

AID: A3B6D4D8353F102346786CF220FF151C
PAC-Info:
    PAC-type = Cisco Trustsec
    AID: A3B6D4D8353F102346786CF220FF151C
    I-ID: CTS_ED_21
    A-ID-Info: Identity Services Engine
    Credential Lifetime: 17:22:32 IST Mon Mar 14 2016
PAC-Opaque:
000200B80003000100040010A3B6D4D8353F102346786CF220FF151C0006009C00030100E044B2650D8351FD06
F23623C470511E0000001356DEA96C00093A80538898D40F633C368B053200D4C9D2422A7FEB4837EA9DBB89D1
E51DA4E7B184E66D3D5F2839C11E5FB386936BB85250C61CA0116FDD9A184C6E96593EEAF5C39BE08140AFBB19
4EE701A0056600CFF5B12C02DD7ECEAA3CCC8170263669C483BD208052A46C31E39199830F794676842ADEECBB
A30FC4A5A0DEDA93
Refresh timer is set for 01:00:05
```

次に、**show cts environment-data** コマンドの出力例を示します。

```
Device# show cts environment-data

CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 0:Unknown
Server List Info:
Installed list: CTSServerList1-000D, 1 server(s):
  *Server: 10.78.105.47, port 1812, A-ID A3B6D4D8353F102346786CF220FF151C
  Status = ALIVE
  auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
0001-45 :
  0-00:Unknown
  2-ba:SGT_2
  3-00:SGT_3
  4-00:SGT_4
  5-00:SGT_5
  6-00:SGT_6
  7-00:SGT_7
  8-00:SGT_8
  9-00:SGT_9
  10-16:SGT_10
!
!
!
Environment Data Lifetime = 3600 secs
Last update time = 14:32:53 IST Mon Mar 14 2016
Env-data expires in 0:00:10:04 (dd:hr:mm:sec)
Env-data refreshes in 0:00:10:04 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
```

次に、ステートフル スイッチオーバー後の **show cts role-based permissions** コマンドの出力例を示します。

```
Device# show cts role-based permissions

IPv4 Role-based permissions default:
        default_sgacl-01
        Deny IP-00
IPv4 Role-based permissions from group 10:SGT_10 to group 15:SGT_15:
        SGACL_3-01
IPv4 Role-based permissions from group 14:SGT_14 to group 15:SGT_15:
        multple_ace-14
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

Cisco TrustSec SGACL のハイアベイラビリティの設定に関するその他の関連資料

関連資料

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

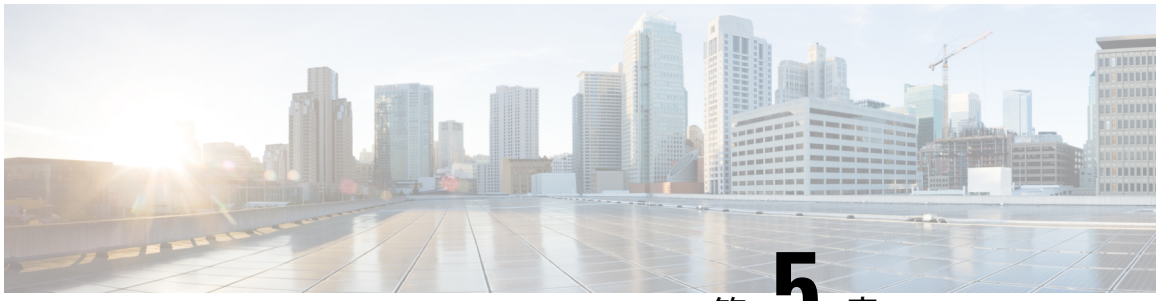
SGACL のハイアベイラビリティの機能情報

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 *4 : Cisco TrustSec SGACL* のハイアベイラビリティの機能情報

機能名	リリース	機能情報
Cisco TrustSec SGACL のハイ アベイラビリティ	Cisco IOS XE Denali 16.2.1	Cisco TrustSec 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、スイッチスタックマネージャで利用可能なハイアベイラビリティ機能をサポートしています。 この機能を有効にする Cisco TrustSec 固有の設定はありません。この機能は、スタック マネージャ アーキテクチャを備えた、Cisco IOS XE Denali 16.2.1 以降のリリースを使用するスイッチでのみ使用できます。



第 5 章

SGT 交換プロトコルの設定

SGT 交換プロトコル（SXP）を使用すると、Cisco TrustSec のハードウェアサポートがないネットワークデバイスにセキュリティグループタグ（SGT）を伝播できます。このモジュールでは、ネットワークのスイッチに Cisco TrustSec SXP を設定する方法について説明します。

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。

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 Cisco TrustSec-SXP と呼びます。Cisco TrustSec-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 と SGT のバインドの情報を伝播する、制御プロトコルです。Cisco TrustSec-SXP は、IP と SGT のバインドをネットワーク上の認証ポイントからアップストリームデバイスへ渡します。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。

SGT 交換プロトコルの前提条件

SXP を導入する前に、Cisco TrustSec-SGT Over Exchange Protocol （SXP）ネットワークを確立する必要があります。この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。

- Cisco TrustSec ソフトウェアをすべてのネットワークデバイス上で実行すること。
- 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、Cisco TrustSec ではすべての ACS 機能がサポートされているわけではありません。ACS 5.1 が Cisco TrustSec-SXP ライセンスで動作していること。
- 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。

SGT 交換プロトコルの制約事項

Cisco TrustSec 交換プロトコルは物理インターフェイスだけでサポートされおり、論理インターフェイスではサポートされていません。

- Cisco IOS XE Everest 16.6.4 以降のリリースでは、ダイナミックホスト制御プロトコル（DHCP）スヌーピングが有効になっている場合、DHCP パケットに対する Cisco TrustSec の適用は、適用ポリシーによってバイパスされます。

SGT 交換プロトコルに関する情報

SGT 交換プロトコルの概要

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。

セキュリティグループタグ（SGT）交換プロトコル（SXP）は、Cisco TrustSec をサポートする複数のプロトコルの 1 つです。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 のバインドの情報を伝播する、制御プロトコルです。Cisco TrustSec は、出力インターフェイスでパケットをフィルタリングします。エンドポイント認証では、Cisco TrustSec ドメイン（エンドポイントの IP アドレス）にアクセスするホストはダイナミックホスト制御プロトコル（DHCP）スヌーピングおよびIPデバイストラッキングによってアクセスデバイスで SGT に関連付けられます。アクセスデバイスは、Cisco TrustSec ハードウェア対応出力のデバイスに、SXP経由でそのアソシエーションまたはバインドを送信します。これらのデバイスは、送信元の IP と SGT のバインドのテーブルを維持します。パケットは、セキュリティ グループ アクセス コントロール リスト（SGACL）を適用することにより、Cisco TrustSec ハードウェア対応デバイスによって出力インターフェイスでフィルタリングされます。SXP は、IP と SGT のバインドをネットワーク上の認証ポイントからアップストリームデバイスへ渡します。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。

SGT は、次のエンドポイント アドミッション コントロール（EAC）アクセス方式のいずれかを使用して割り当てることができます。

- 802.1X ポートベースの認証
- MAC 認証バイパス（MAB）
- Web 認証

SXP は、トランスポートプロトコルとして TCP を使用し、接続の開始に TCP ポート 64999 を使用します。SXP は、認証と完全性チェックに Message Digest 5（MD5）を使用します。これには定義されたロールが2つあります。そのロールとは、スピーカー（イニシエータ）とリスナー（レシーバ）です。

セキュリティ グループ タギング

セキュリティグループタグは、一意のロールに割り当てられる一意の 16 ビットタグです。送信元ユーザ、デバイス、またはエンティティの特権を表し、Cisco TrustSec ドメインの入力でタグ付けされます。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、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。静的ポート ID は、ポートに接続された特定のエンドポイントの SGT 値をルックアップするために使用されます。

SGT の割り当て

パケットのセキュリティグループタグ（SGT）は、パケットが Cisco TrustSec リンクでタグ付けされたとき、または単一のエンドポイントがポートで認証されたときに、ポートレベルで割り当てることができます。着信パケットの SGT は、次の方法で決定されます。

- SGTでタグ付けされたパケットが信頼ポートに着信すると、パケットのタグはパケットの SGT と見なされます。
- パケットが SGT でタグ付けされているが、信頼できないポートに着信した場合、パケットの SGT は無視され、ピア SGT がポートに設定されます。
- パケットに SGT がない場合、ピア SGT はポートに設定されます。

SGT を割り当てるための次の方法がサポートされています。

- IPM（dot1x、MAB、Web 認証）
- VLAN と VLAN と SGT のマッピングは、認証方式がすでに IP アドレスを割り当てられた認証済みエントリに SGT を提供する際に確立されます。スイッチプロセスは、エンドポイントセッションをモニタし、IP と SGT のバインドの変更または削除を検出します。

• SXP（SGT 交換プロトコル）リスナー

SGT 交換プロトコルの設定方法

デバイス SGT の手動設定

通常の Cisco TrustSec 動作では、認証サーバ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	**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 2	**cts sgt** *tag* 例： `Device(config)# cts sgt tag`	デバイスから送信されるパケットの SGT を設定します。tag 引数は 10 進表記です。指定できる範囲は 1 ～ 65533 です。
ステップ 3	**exit** 例： `Device(config)# exit`	設定モードを終了します。

SXP ピア接続の設定

両方のデバイスで SXP ピア接続を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 SXP 送信元 IP アドレスが設定されておらず、かつ接続の SXP 送信元アドレスが指定されていない場合、Cisco TrustSec ソフトウェアは既存のローカル IP アドレスから SXP 送信元 IP アドレスを抽出します。SXP 送信元アドレスは、スイッチから開始される TCP 接続ごとに異なる場合があります。

SXP ピア接続を設定するには、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 sxp connection peer** *peer-ipv4-addr*[**source** *src-ipv4-addr*] **password** {**default | none**} **mode** {**local | peer**} {**speaker | listener**} { **vrf** *vrf-name*} 例： `Device(config)# cts sxp connection peer 10.10.1.1 password default mode local listener`	SXP アドレス接続を設定します。 オプションの **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。アドレスが指定されていない場合、接続は、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、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 SXP パスワードを使用します。 • **none**：パスワードを使用しないでください。 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。 • **speaker**：デフォルトこのデバイスが接続の際にスピーカーになります。 • **listener**：このデバイスが接続の際にリスナーになります。

	コマンドまたはアクション	目的
		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、特権 EXEC モードに戻ります
ステップ 5	**show cts sxp connections** 例： `Device# show cts sxp connections`	（任意）SXP 接続情報を表示します。

デフォルトの SXP パスワードの設定

デフォルトでは、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。

デフォルト SXP パスワードを設定するには、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 sxp default password** [**0** | **6** | **7**] *password* 例： `Device(config)# cts sxp default password 0 hello`	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。
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

デフォルトの SXP 送信元 IP アドレスの設定

SXP は送信元 IP アドレスが指定されないと、新規の TCP 接続すべてにデフォルトの送信元 IP アドレスを使用します。デフォルト SXP 送信元 IP アドレスを設定しても、既存の TCP 接続には影響しません。

デフォルト SXP 送信元 IP アドレスを設定するには、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 sxp default source-ip** *src-ip-addr* 例： `Device(config)# cts sxp default source-ip 10.0.1.2`	SXP のデフォルトの送信元 IP アドレスを設定します。
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。

SXP の復帰期間の変更

ピアが 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、SXP 復帰期間タイマーが開始されます。SXP 復帰期間タイマーがアクティブな間、Cisco TrustSec 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。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。

SXP の復帰期間を変更するには、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：	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	**cts sxp reconciliation period** *seconds* 例： `Device(config)# cts sxp reconciliation period 360`	SXP復帰タイマーを変更します。デフォルト値は 120 秒（2 分）です。範囲は 0 ～ 64000 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、特権 EXEC モードに戻ります。

SXP リトライ期間の変更

SXP リトライ期間によって、Cisco TrustSec ソフトウェアが SXP 接続を再試行する頻度が決まります。SXP 接続が正常に確立されなかった場合、Cisco TrustSec ソフトウェアは SXP リトライ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 120 秒です。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。

SXP のリトライ期間を変更するには、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 sxp retry period** *seconds* 例： `Device(config)# cts sxp retry period 360`	SXP リトライ タイマーを変更します。デフォルト値は 120 秒（2 分）です。範囲は 0 ～ 64000 です。

	コマンドまたはアクション	目的
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。

SXP で学習された IP アドレスと SGT マッピングの変更をキャプチャするための syslog の作成方法

グローバル コンフィギュレーション モードで **cts sxp log binding-changes** コマンドを設定すると、IP アドレスと SGT バインドの変更（追加、削除、変更）が発生するたびに SXP の syslog（sev 5 syslog）が生成されます。これらの変更は SXP 接続で学習されて伝播されます。デフォルトは、**no cts sxp log binding-changes** です。

バインディングの変更のロギングをイネーブルにするには、次の作業を実行します。

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	**cts sxp log binding-changes** 例： `Device(config)# cts sxp log binding-changes`	IP と SGT のバインドの変更のロギングを有効にします。
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。

SGT 交換プロトコルの設定例

例：Cisco TrustSec SXP および SXP ピア接続の有効化

以下に、SXP を有効にし、スイッチ A（スピーカー）とスイッチ B（リスナー）間に SXP ピア接続を設定する方法の例を示します。

```
Device# configure terminal
Device(config)# cts sxp enable
Device(config)# cts sxp default password Cisco123
Device(config)# cts sxp default source-ip 10.10.1.1
Device(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

以下に、スイッチ B（リスナー）とスイッチ A（スピーカー）間に SXP ピア接続を設定する方法の例を示します。

```
Device# configure terminal
Device(config)# cts sxp enable
Device(config)# cts sxp default password Cisco123
Device(config)# cts sxp default source-ip 10.20.2.2
Device(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

例：デフォルトの SXP パスワードと送信元 IP アドレスの設定

次に、デフォルトのSXPパスワードとの送信元IPアドレスを設定する例を示します。

```
Device# configure terminal
Device(config)# cts sxp default password Cisco123
Device(config)# cts sxp default source-ip 10.20.2.2
Device(config)# end
```

SGT 交換プロトコルの接続の確認

SXP 接続を表示するには、次の作業を行います。

コマンド	目的
show cts sxp connections	SXP ステータスと接続に関する詳細情報を表示します。
show cts sxp connections [brief]	SXP ステータスと接続に関する要約情報を表示します。

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

```
Switch# 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
Conn Version             : 2
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
```

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

```
Switch# show cts sxp connections brief

SXP                      : Enabled
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          Source_IP          Conn Status    Duration
-------------------------------------------------------------------------------
10.1.3.1         10.1.3.2           On             6:00:09:13 (dd:hr:mm:sec)
Total num of SXP Connections = 1
```

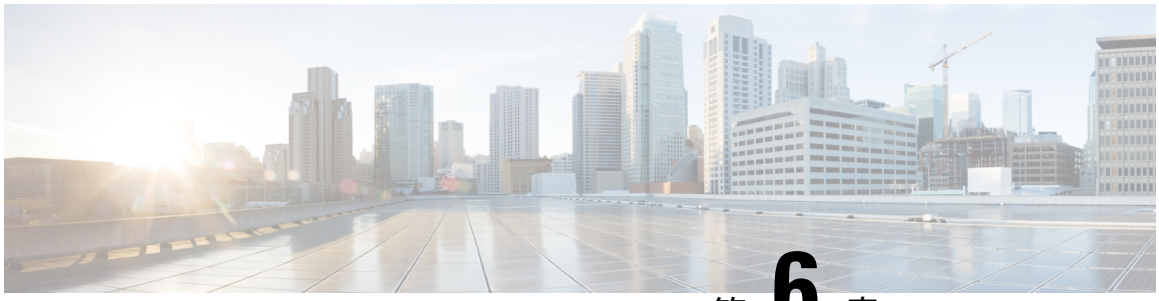
SGT 交換プロトコルの機能情報

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 : SGT* 交換プロトコルの機能情報

機能名	リリース	機能情報
SGT 交換プロトコル	Cisco IOS XE Denali 16.1.1	SGT 交換プロトコル（SXP）は、Cisco TrustSec のハードウェアサポートがないネットワークデバイスにセキュリティ グループタグ（SGT）を伝播します。



第 6 章

Cisco TrustSec VRF 対応 SGT

Cisco TrustSec VRF 対応 SGT 機能は、特定の Virtual Route Forwarding（VRF）インスタンスとセキュリティグループタグ（SGT）の交換プロトコル（SXP）接続をバインドします。

Cisco TrustSec VRF 対応 SGT に関する情報

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。

VRF 対応 SGT の設定方法

VRF とレイヤ 2 VLAN の割り当ての設定

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	**interface** *type number* 例： `Device(config)# interface vlan 101`	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	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding vrf-intf`	VRFインスタンスまたは仮想ネットワークをインターフェイスまたはサブインターフェイスに関連付けます。 （注） 管理インターフェイスで VRF を設定しないでください。
ステップ 5	**exit** 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、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	**cts role-based l2-vrf vrf1 vlan-list 20** 例： `Device(config)# cts role-based l2-vrf vrf1 vlan-list 20`	レイヤ 2 VLAN の VRF インスタンスを選択します。
ステップ 7	**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。

VRF 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 vrf vrf-name** {**ip4_netaddress** | *ipv6_netaddress* | **host** {*ip4_address* | *ip6_address*}} **sgt** *sgt_number* 例： `Device(config)# cts role-based sgt-map vrf red 10.0.0.3 sgt 23`	指定された VRF のパケットに SGT を適用します。 IP-SGT バインドは、指定された VRF と、IP アドレスのタイプによって示される IP プロトコルのバージョンに関連付けられた IP-SGT のテーブルに入力されます。
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。

Cisco TrustSec VRF 対応 SGT の設定例

例：VRF とレイヤ 2 VLAN の割り当ての設定

```
Device> enable
Device# configure terminal
Device(config)# interface vlan 101
Device(config-if)# vrf forwarding vrf-intf
Device(config-if)# exit
Device(config)# cts role-based l2-vrf vrf1 vlan-list 20
Device(config)# end
```

例：VRF とレイヤ 2 VLAN の割り当ての設定

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-map vrf red 23.1.1.2 sgt 23
Device(config)# end
```

Cisco TrustSec VRF-Aware SGT の設定に関するその他の関連資料

関連資料

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、および機能セットに関する MIB を検索およびダウンロードするには、http://www.cisco.com/go/mibs にある Cisco MIB Locator を使用してください。

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。	https://www.cisco.com/c/en/us/support/index.html

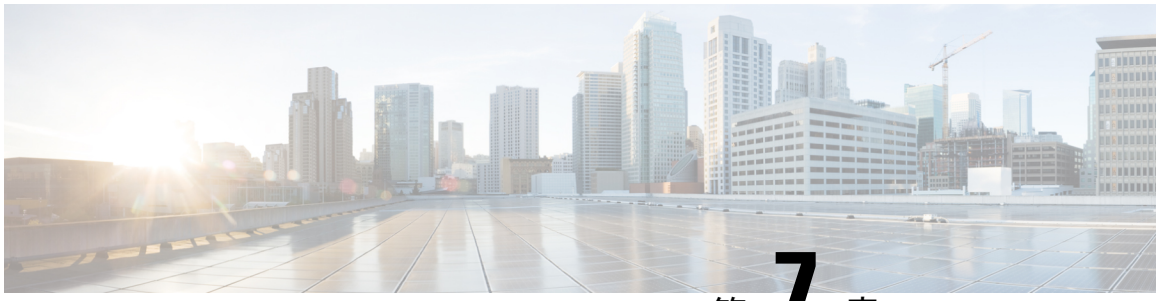
Cisco TrustSec VRF 対応 SGT の機能情報

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 VRF* 対応 *SGT* の機能情報

機能名	リリース	機能情報
Cisco TrustSec VRF 対応 SGT	Cisco IOS XE Denali 16.1.1	Cisco TrustSec VRF 対応 SGT 機能は、特定の Virtual Route Forwarding（VRF）インスタンスとセキュリティグループタグ（SGT）の交換プロトコル（SXP）接続をバインドします。



第 7 章

IP プレフィックスと SGT ベースの SXP フィルタリング

セキュリティグループタグ（SGT）交換プロトコル（SXP）は、Cisco TrustSec をサポートする複数のプロトコルの 1 つです。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。SXP は、IP と SGT のバインドをネットワーク上の認証ポイントからアップストリームデバイスへ渡します。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ユーザアイデンティティ情報を伝えることができます。

IP プレフィックスと SGT ベースの SXP フィルタリング機能を使用すると、IP と SGT のバインドをエクスポートまたはインポートするときにフィルタリングできます。このフィルタリングは、IP プレフィックス、SGT、またはその両方の組み合わせに基づいて実行できます。

IP プレフィックスとセキュリティグループタグ（SGT）ベースのセキュリティ交換プロトコル（SXP）フィルタリングの制約事項

- アクティブデバイスとスタンバイデバイス間のセキュリティ交換プロトコル（SXP）データベースでの、IP セキュリティグループタグ（SGT）バインドのステートフルな同期のハイアベイラビリティのサポートはありません。

- 既存の接続に適用されたフィルタは、エクスポートまたはインポートされた後続のバインドでのみ有効になります。フィルタは、フィルタを適用する前にエクスポートまたはインポートされたバインドには適用されません。
- Virtual Route Forwarding（VRF）固有のフィルタリングはサポートされておらず、ピア IP に指定されたフィルタはデバイス上のすべての VRF に適用されます。
- フィルタルールの SGT 値は、単一の SGT 番号のリストになります。SGT の範囲はサポートされていません。

IP プレフィックスと SGT ベースの SXP フィルタリングに関する情報

概要

IP プレフィックスと SGT ベースの SXP フィルタリング機能を使用すると、IP と SGT のバインドをエクスポートまたはインポートするときにフィルタリングできます。このフィルタリングは、IP プレフィックス、SGT、またはその両方の組み合わせに基づいて実行できます。

セキュリティグループタグ（SGT）交換プロトコル（SXP）は、Cisco TrustSec をサポートする複数のプロトコルの 1 つです。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。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ユーザアイデンティティ情報を伝えることができます。

IP-to-SGT フィルタリングにより、システムは対象のバインドだけを選択的にインポートまたはエクスポートできます。SXP 接続では、バインドのエクスポートまたはインポート中に発生するフィルタリングに基づいて、スピーカーまたはリスナーのどちらかとして機能するデバイスにフィルタを設定できます。

双方向 SXP 接続の場合、スピーカーまたはリスナーのフィルタが設定されているかどうかに基づいて、どちらかの方向にフィルタが適用されます。ピアがスピーカーとリスナーの両方のフィルタグループの一部である場合、フィルタリングは両方向に適用されます。

フィルタは、ピアツーピアベースまたはグローバルに適用できます（すべての SXP 接続に適用可能）。どちらの場合も、フィルタはスピーカーまたはリスナーに適用できます。

フィルタ ルール

デバイスに適用する必要があるフィルタは、一連のフィルタルールを使用して作成されます。各フィルタルールは、特定の SGT 値や IP プレフィックス値を持つバインドに対して実行するアクションを指定します。各バインドは、フィルタルールで指定された値と照合されます。一致が見つかった場合は、フィルタルールで指定された対応するアクションが適用されます。選択したバインドに適用できるアクションは、許可アクションまたは拒否アクションです。IP-SGT

バインドのエクスポートまたはインポート中に、スピーカーまたはリスナーでフィルタが有効になっている場合、バインドはフィルタルールに基づいてフィルタリングされます。

フィルタリストのバインドにルールが指定されていない場合は、フィルタリストに設定されているキャッチオールルールが実行されます。キャッチオールルールがない場合、対応するバインドは暗黙的に拒否されます。

SXP フィルタリングのタイプ

IP-SGT バインドは、次のいずれかの方法でフィルタリングされます。

- SGT ベースのフィルタリング：SGT 値に基づいて SXP 接続の IP-SGT バインドをフィルタリングします。
- IP プレフィックスベースのフィルタリング：IP プレフィックス値に基づいて SXP 接続の IP-SGT バインドをフィルタリングします。
- SGT および IP プレフィックスベースのフィルタリング：SGT 値と IP プレフィックス値に基づいて SXP 接続の IP-SGT バインドをフィルタリングします。

フィルタルールは、各 IP-SGT バインドに適用されます。

IP プレフィックスと SGT ベースの SXP フィルタリングの設定方法

SXP フィルタリストの設定

このステップでは、ルールセットを保持するフィルタリストを作成します。これらのルールは、許可されたバインドを検証し、拒否されたバインドをブロックすることによって、IP-SGT バインドをフィルタリングします。各ルールは、SGT、IP プレフィックス、または SGT と IP プレフィックスの両方の組み合わせに基づいて設定できます。

フィルタリストに特定の IP-SGT バインドと一致するルールがない場合、デフォルトまたはキャッチオールルールが定義されていない限り、バインドは暗黙的に拒否されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**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**	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 sxp filter-list** *filter-name*	Cisco TrustSec フィルタリストを設定し、フィルタリスト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	*sequence-number* **permit ipv4** *ip-address/prefix* **deny sgt** *sgt-value*	フィルタリストのルールを設定します。
ステップ 5	**exit**	フィルタリストコンフィギュレーションモードを終了して、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 6	**cts sxp filter-list** *filter-name*	Cisco TrustSec フィルタリストを設定し、フィルタリスト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	[*sequence-number*] **deny sgt** *sgt-value* **permit ipv6** *ipv6-address/prefix*	フィルタリストのルールを設定します。
ステップ 8	**exit**	フィルタリストコンフィギュレーションモードを終了して、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 9	**cts sxp filter-list** *filter-name*	Cisco TrustSec フィルタリストを設定し、フィルタリスト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	[*sequence-number*] **permit ipv6** *ipv6-address/prefix* **permit** *sgt-value* **permit**	フィルタリストのルールを設定します。
ステップ 11	**end**	フィルタリスト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。

SXP フィルタグループの設定

このステップでは、ピアセットを 1 つのグループにまとめ、そのグループにフィルタリストを適用します。フィルタグループは、スピーカーグループまたはリスナーグループとして定義できます。すべてのスピーカーまたはすべてのリスナーに同じフィルタリストを適用するには、グローバルスピーカーのフィルタグループまたはグローバルリスナーのフィルタグループを作成します。

（注） フィルタグループに適用できるフィルタリストは 1 つだけです。

手順

	コマンドまたはアクション	目的
ステップ 1	**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**	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 filter-group listener** *listener-name*	SXP フィルタグループのリスナーを設定し、フィルタグループ 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	**filter** *filter-list-name*	フィルタリストのルールを設定します。
ステップ 5	**peer** *ipv4-address*	ピアの IP アドレスを設定します。
ステップ 6	**exit**	フィルタグループ コンフィギュレーションモードを終了して、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 7	**cts sxp filter-group speaker** *speaker-name*	複数の VLAN アクセス ポートで音声 VLAN を設定します。
ステップ 8	**filter** *filter-list-name*	フィルタリスト名を設定します。
ステップ 9	**peer** *ipv4-address*	ピアの IP アドレスを設定します。
ステップ 10	**end**	フィルタグループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

グローバルリスナーまたはグローバルスピーカーのフィルタグループの設定

グローバルリスナーとグローバルスピーカーのフィルタグループを設定すると、リスナーモードまたはスピーカーモードのすべての SXP 接続のボックス全体にフィルタが適用されます。

フィルタグループにフィルタリストを追加すると、ボックスに現在設定されているフィルタリストのセットがヘルプストリングとして表示されます。

（注） **peer** コマンドは、グローバルリスナーとグローバルスピーカーのフィルタグループでは使用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	**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**	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 filter-group listener global** *filter-list-name*	グローバルリスナーのフィルタグループを設定します。
ステップ 4	**cts sxp filter-group speaker global** *filter-list-name*	グローバルスピーカーのフィルタグループを設定します。
ステップ 5	**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。

SXP フィルタリングの有効化

SXP フィルタリストとフィルタグループを設定したら、フィルタリングを有効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**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**	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 sxp filter enable**	インターフェイスにソース テンプレートを設定します。
ステップ 4	**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。
ステップ 5	**show cts sxp filter-list** *filter_name*	デバイスに設定されているフィルタリストを、各フィルタリストのフィルタルールとともに表示します。

デフォルトルールまたはキャッチオールルールの設定

デフォルトまたはキャッチオールルールは、フィルタリスト内のどのルールとも一致しない IP-SGT バインドに適用されます。デフォルトルールが指定されていない場合、これらの IP-SGT バインドは拒否されます。

対応するフィルタリストのフィルタリスト コンフィギュレーション モードで、デフォルトまたはキャッチオールルールを定義します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	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**	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 filter-list** *filter-name*	Cisco TrustSec フィルタリストを設定し、フィルタリスト 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	**permit ipv4** *ip-address/prefix*	条件が一致した場合にアクセスを許可します。
ステップ 5	**deny ipv6** *ipv6-address/prefix*	条件に一致する場合、アクセスを拒否します。
ステップ 6	**permit sgt all**	すべての SGT に対応するバインドを許可します。

	コマンドまたはアクション	目的
ステップ 7	**end**	フィルタリスト 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 プレフィックスと SGT ベースの SXP フィルタリングの設定例

例：SXP フィルタリストの設定

```
Device> enable
Device# configure terminal
Device(config)# cts sxp filter-list filter1
Device(config-filter-list)# permit ipv4 10.1.1.0/24 deny sgt 3 4
Device(config-filter-list)# exit
Device(config)# cts sxp filter-list filter2
Device(config-filter-list)# permit sgt all
Device(config-filter-list)# exit
Device(config)# cts sxp filter-list filter3
Device(config-filter-list)# deny ipv6 2001:db8::1/64 permit sgt 67
Device(config-filter-list)# end
```

例：SXP フィルタグループの設定

```
Device> enable
Device# configure terminal
Device(config)# cts sxp filter-group listener group1
Device(config-filter-group)# filter filter1
Device(config-filter-group)# peer 172.16.0.1 192.168.0.1
Device(config-filter-group)# exit
Device(config)# cts sxp filter-group listener global group2
Device(config)# end
```

例：SXP フィルタリングの有効化

```
Device> enable
Device# configure terminal
Device(config)# cts sxp filter-enable
Device(config)# end
```

例：デフォルトルールまたはキャッチオールルールの設定

次に、すべての IPv4 および IPv6 アドレスに対応するバインドを許可するデフォルトのプレフィックスルールを作成する例を示します。

```
Device(config)# cts sxp filter-list filter1
Device(config-filter-list)# permit ipv4 10.0.0.0/0
Device(config-filter-list)# deny ipv6 2001:db8::1/0
```

次に、すべての SGT に対応するバインドを許可するデフォルトの SGT ルールを作成する例を示します。

```
Device(config)# cts sxp filter-list filter_1
Device(config-filter-list)# permit sgt all
```

IP プレフィックスと SGT ベースの SXP フィルタリングの確認

設定を確認するには、次のコマンドを使用します。

debug cts sxp filter events コマンドは、フィルタリストおよびフィルタグループの作成、削除、更新に関連するイベントをログに記録するために使用されます。このコマンドは、フィルタリングプロセスの一致アクションに関連するイベントをキャプチャするためにも使用されます。

```
Device# debug cts sxp filter events
```

次に、SXP スピーカーのフィルタグループを表示する **show cts sxp filter-group speaker** コマンドの出力例を示します。

```
Device# show cts sxp filter-group speaker group1
   Filter-group: group1
   Filter-name: filter1
   Peer-list: 172.16.0.1 192.168.0.1
```

次に、SXP スピーカーのリスナーグループを表示する **show cts sxp filter-group listener** コマンドの出力例を示します。

```
Device# show cts sxp filter-group listener

Global Listener Filter: Not configured
   Filter-group: group1
   Filter-name: filter1
   Peer-list: 172.16.0.1 192.168.0.1
   Filter-group: group2
   Filter-name: filter1
   Peer-list: 192.0.2.1, 198.51.100.1, 203.0.113.1
```

次に、SXP スピーカーのフィルタグループに関する詳細情報を表示する **show cts sxp filter-group speaker detailed** コマンドの出力例を示します。

```
Device# show cts sxp filter-group speaker group1 detailed

   Filter-group: group1
   Filter-name: filter1
   Filter-rules:
      10 deny sgt 30
      20 deny prefix 10.1.0.0/16
      30 permit sgt 60-100
   Peer-list: 172.16.0.1 192.168.0.1
```

次に、設定されたすべてのフィルタグループに関する情報を表示する **show cts sxp filter-group** コマンドの出力例を示します。

```
Device# show cts sxp filter-group

Global Listener Filter: Not configured

Global Speaker Filter: Not configured

Listener Group:
   Filter-group: group1
   Filter-name: filter1
   Peer-list: 172.16.0.1 192.168.0.1
   Filter-group: group2
   Filter-name: filter1
   Peer-list: 192.0.2.1, 198.51.100.1, 203.0.113.1

Speaker Group:
   Filter-group: group3
   Filter-name: filter1
   Peer-list: 172.16.0.1 192.168.0.13
   Filter-group: group2
   Filter-name: filter1
   Peer-list: 192.0.2.1, 198.51.100.1, 203.0.113.1
```

次に、設定されたすべての SXP フィルタグループに関する詳細情報を表示する **show sxp filter-group detailed** コマンドの出力例を示します。

```
Device# show cts sxp filter-group detailed

Global Listener Filter: Configured
   Filter-name: global1
   Filter-rules:
      10 deny 192.168.0.13/32
      20 deny sgt 100-200

Global Speaker Filter: Configured
   Filter-name: global2
   Filter-rules:
      10 deny 192.168.0.13/32
      20 deny sgt 100-200

Listener Group:
   Filter-group: group1
   Filter-name: filter1
   Filter-rules:
```

```
      10 deny sgt 30
      20 deny prefix 172.16.0.0/16
      30 permit sgt 60-100
   Peer-list: 172.16.0.1, 192.168.0.13

   Filter-group: group2
   Filter-name: filter1
   Filter-rules:
      10 deny sgt 30
      20 deny prefix 172.16.0.0/16
      30 permit sgt 60-100
   Peer-list: 192.0.2.1, 198.51.100.1, 203.0.113.1

Speaker Group
   Filter-group: group3
   Filter-name: filter1
   Filter-rules:
      10 deny sgt 30
      20 deny prefix 172.16.0.0/16
      30 permit sgt 60-100
   Peer-list: 10.10.10.1, 172.16.0.1, 192.168.0.13

   Filter-group: group2
   Filter-name: filter1
   Filter-rules:
      10 deny sgt 30
      20 deny prefix 172.16.0.0/16
      30 permit sgt 60-100
   Peer-list: 192.0.2.1, 198.51.100.1, 203.0.113.1
```

SXP フィルタリングの syslog メッセージ

SXP フィルタリングの syslog メッセージは、フィルタリングに関連するさまざまなイベントを示すために生成されます。

フィルタルールの syslog メッセージ

単一のフィルタに設定できるルールの最大数は 128 です。単一のフィルタに設定されているフィルタルールの数が制限の 20% 増加するたびに、次のメッセージが生成されます。

```
CTS SXP filter rules exceed %[ ] threshold. Reached count of [count] out of [max] in
filter [filter-name].
```

単一のフィルタに設定されているルールの数が、フィルタリストに許可されているルールの最大数の 95% に達すると、次のメッセージが生成されます。

```
CTS SXP filter rules exceed [ ] threshold. Reached count of [count] out of [max] in
filter [filter-name].
```

次のメッセージは、単一のフィルタで設定されたルールの数が許可されたルールの最大数に達し、それ以上ルールを追加できない場合に生成されます。

```
Reached maximum filter rules. Could not add new rule in filter [filter-name]
```

フィルタリストの syslog メッセージ

設定できるフィルタリストの最大数は256です。設定されているフィルタリストの数がこの制限の 20% 増加するたびに、次のメッセージが生成されます。

```
CTS SXP filter rules exceed %[ ] threshold. Reached count of [count] out of [max] in
filter [filter-name].
```

設定されているフィルタリストの数が、許可されたフィルタリストの最大数の 95% に達すると、次のメッセージが生成されます。

```
CTS SXP filter rules exceed %[ ] threshold. Reached count of [count] out of [max]
```

次のメッセージは、設定されているフィルタリストの数が許可されたフィルタリストの最大数に達し、それ以上フィルタリストを追加できない場合に生成されます。

```
Reached maximum filter count. Could not add new filter
```

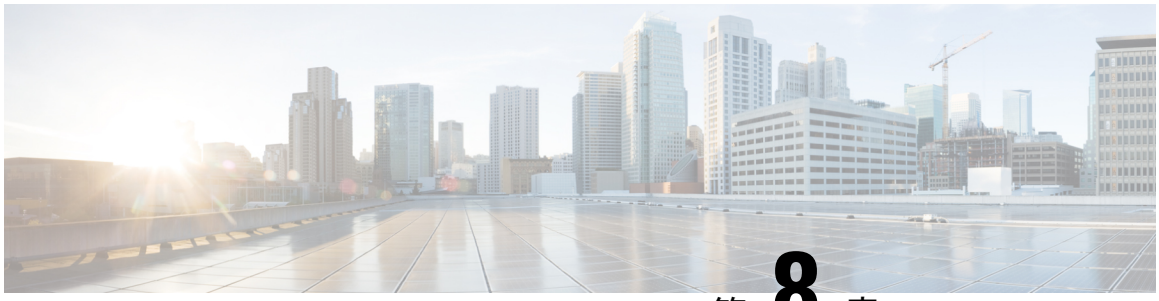
IP プレフィックスと SGT ベースの SXP フィルタリングの機能情報

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 *7: IP* プレフィックスと *SGT* ベースの *SXP* フィルタリングの機能情報

機能名	リリース	機能情報
IP プレフィックスと SGT ベースの SXP フィルタリング	Cisco IOS XE Denali 16.1.1	IP プレフィックスと SGT ベースの SXP フィルタリング機能は、高い IP-SGT バインドの拡張性の問題を解決するためのフィルタリングメカニズムを提供します。 次のコマンドが導入されました：**debug cts sxp filter events**、**cts sxp filter-list**、**cts sxp filter-group**、**cts sxp filter-enable**、**show cts sxp filter-group**、**show cts sxp filter-list**



第 8 章

エンドポイントアドミッションコントロールの設定

このモジュールでは、TrustSec ネットワークでの認証および許可のためのエンドポイント アドミッション コントロール（EAC）のアクセス方式について説明します。

エンドポイント アドミッション コントロールの概要

TrustSec ネットワークでは、パケットはネットワークへの入力ではなく出力でフィルタリングされます。TrustSec エンドポイント認証では、TrustSec ドメイン（エンドポイントの IP アドレス）にアクセスするホストは DHCP スヌーピングおよび IP デバイス トラッキングによってアクセス デバイスでセキュリティ グループ タグ（SGT）に関連付けられます。アクセスデバイスは、継続的に更新される送信元 IP と SGT のバインディングテーブルを維持する TrustSec ハードウェア対応出力のデバイスに、SXP 経由でそのアソシエーション（バインド）を送信します。パケットは、セキュリティグループ ACLS（SGACL）を適用することにより、TrustSec ハードウェア対応デバイスで出力フィルタリングされます。

認証および許可のためのエンドポイント アドミッション コントロール（EAC）アクセス方式には、次のものがあります。

- 802.1X ポートベースの認証
- MAC 認証バイパス（MAB）

- Web 認証（WebAuth）

すべてのポートベース認証は、authentication コマンドでイネーブルにできます。各アクセス方式はポート単位で個別に設定する必要があります。複数の認証モードが設定され、アクティブ方式が失敗すると柔軟な認証シーケンスおよびフェールオーバー機能により管理者は、フェールオーバーおよびフォールバック シーケンスを指定することができます。802.1X ホスト モードは、802.1X ポートごとに接続できるエンドポイントのホスト数を決定します。

例：802.1X 認証の設定

次に、ギガビット イーサネット ポートでの基本的な 802.1x の設定例を示します。

```
Device> enable
Device# configure terminal
Device(config)# dot1x system-auth-control
Device(config)# interface GigabitEthernet2/1
Device(config-if)# authentication port-control auto
Device(config-if)# dot1x pae authenticator
```

例：MAC 認証バイパスの設定

MAC 認証バイパス（MAB）は 802.1X 対応ではないホストまたはクライアントが 802.1X をイネーブルにしたネットワークに参加できるようにします。MAB をイネーブルにする前に、802.1X 認証をイネーブルにする必要はありません。

次の例では、Catalyst スイッチでの基本的な MAB 設定の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet2/1
Device(config-if)# authentication port-control auto
Device(config-if)# mab
```

MAB 認証の設定の詳細については、アクセススイッチのコンフィギュレーション ガイドを参照してください。

例：Web 認証プロキシの設定

Web 認証プロキシ（WebAuth）は、ユーザが Web ブラウザを使用して、アクセス デバイスの Cisco IOS Web サーバ経由で Cisco Secure ACS にログイン クレデンシャルを送信できるようにするものです。WebAuth は独立してイネーブルにできます。これは、802.1X または MAB の設定は必要ではありません。

次の例では、ギガビット イーサネット ポートでの基本的な WebAuth 設定の例を示します。

```
Device(config)# ip http server
Device(config)# ip access-list extended POLICY
Device(config-ext-nacl)# permit udp any any eq bootps
Device(config-ext-nacl)# permit udp any any eq domain
Device(config)# ip admission name HTTP proxy http
Device(config)# fallback profile FALLBACK_PROFILE
Device(config-fallback-profile)# ip access-group POLICY in
Device(config-fallback-profile)# ip admission HTTP
Device(config)# interface GigabitEthernet2/1
Device(config-if)# authentication port-control auto
Device(config-if)# authentication fallback FALLBACK_PROFILE6500(config-if)#ip access-group
POLICY in
```

例：柔軟な認証シーケンスおよびフェールオーバーコンフィギュレーション

フレキシブル認証シーケンス（FAS）を使用すると、802.1X、MAB、および WebAuth 認証方式用にアクセスポートを設定でき、1 つ以上の認証方式が使用できない場合にフォールバックシーケンスを指定できます。デフォルトのフェールオーバーシーケンスは次のとおりです。

- 802.1X ポートベースの認証
- MAC 認証バイパス
- Web 認証

レイヤ 2 認証はレイヤ 3 の認証前に常に実行されます。つまり、802.1X と MAB は WebAuth の前に実行される必要があります。

次の例では、MAB、dot1X および WebAuth の順で認証シーケンスを指定します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet 2/1
Device(config-if)# authentication order mab dot1x webauth
Device(config-if)# ^Z
```

FAS の詳細については、『Flexible Authentication Order, Priority, and Failed Authentication』を参照してください。

802.1X ホスト モード

ポート単位で 4 種類の分類モードを設定できます。

- Single Host：1 個の MAC アドレスを持つインターフェイス ベースのセッション
- Multi Host：ポートごとに複数の MAC アドレスを持つインターフェイス ベースのセッション
- Multi Domain：MAC + ドメイン（VLAN）セッション

• Multi Auth：ポートごとに複数の MAC アドレスを持つ MAC ベースのセッション

認証前オープン アクセス

認証前オープンアクセス機能は、ポートの認証の実行前に、クライアントとデバイスがネットワーク アクセスを取得できるようにするものです。このプロセスが主に、PXE がタイムアウトする前にデバイスがネットワークにアクセスし、サプリカントが含まれる可能性のあるブート可能イメージをダウンロードする必要がある PXE のブートのシナリオで必要です。

例：DHCP スヌーピングおよび SGT の割り当て

認証プロセス後は、デバイス認証が発生します（たとえば、ダイナミック VLAN 割り当て、ACL プログラミングなど）。TrustSec ネットワークの場合、セキュリティ グループ タグ（SGT）は Cisco ACS のユーザ コンフィギュレーションごとに割り当てられます。SGT はそのエンドポイントから DHCP スヌーピングおよび IP デバイス トラッキング インフラストラクチャを使用して送信されたトラフィックにバインドされます。

次の例では、アクセス スイッチで DHCP スヌーピングおよび IP デバイス トラッキングをイネーブルにします。

```
Device> enable
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ip dhcp snooping
Device(config)# ip dhcp snooping vlan 10
Device(config)# no ip dhcp snooping information option
Device(config)# ip device tracking
```

エンドポイントアドミッションコントロールの機能情報

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 :* エンドポイント アドミッション コントロールの機能情報

機能名	リリース	機能情報
エンドポイント アドミッション コントロール	Cisco IOS XE Denali 16.1.1	TrustSec ネットワークでは、パケットはネットワークへの入力ではなく出力でフィルタリングされます。TrustSec エンドポイント認証では、TrustSec ドメイン（エンドポイントの IP アドレス）にアクセスするホストは DHCP スヌーピングおよび IP デバイス トラッキングによってアクセスデバイスでセキュリティ グループ タグ（SGT）に関連付けられます。