# ASA および Cisco TrustSec

この章では、ASA に Cisco TrustSec を実装する方法について説明します。



## Cisco TrustSec について

従来、ファイアウォールなどのセキュリティ機能は、事前定義されている IP アドレス、サブネット、およびプロトコルに基づいてアクセス コントロールを実行していました。しかし、企業のボーダレス ネットワークへの移行に伴い、ユーザと組織の接続に使用されるテクノロジーおよびデータとネットワークを保護するためのセキュリティ要件が大幅に向上しています。エンドポイントは、ますます遊動的となり、ユーザは通常さまざまなエンドポイント（ラップトップとデスクトップ、スマートフォン、タブレットなど）を使用します。つまり、ユーザ属性とエンドポイント属性の組み合わせにより、ファイアウォール機能または専用ファイアウォールを持つスイッチやルータなどの実行デバイスがアクセス コントロール判断のために信頼して使用できる既存の 6 タプル ベースのルール以外の主要な特性が提供されます。

その結果、お客様のネットワーク全体、ネットワークのアクセス レイヤ、分散レイヤ、コア レイヤ、およびデータセンターのセキュリティを有効にするためには、エンドポイント属性またはクライアント アイデンティティ属性のアベイラビリティと伝搬がますます重要な要件となります。

Cisco TrustSec は、既存の ID 認証インフラストラクチャを基盤とするアクセス コントロールです。ネットワーク デバイス間のデータ機密性保持を目的としており、セキュリティ アクセス サービスを 1 つのプラットフォーム上で統合します。Cisco TrustSec 機能では、実行デバイスはユーザ属性とエンドポイント属性の組み合わせを使用して、ロールベースおよびアイデンティティベースのアクセス コントロールを決定します。この情報のアベイラビリティおよび伝搬によって、ネットワークのアクセス レイヤ、分散レイヤ、およびコア レイヤでのネットワーク全体におけるセキュリティが有効になります。

ご使用の環境に Cisco TrustSec を実装する利点は、次のとおりです。

- デバイスからの適切でより安全なアクセスにより、拡大する複雑なモバイル ワークフォースを提供します。
- 有線または無線ネットワークへの接続元を包括的に確認できるため、セキュリティ リスクが低減されます。
- 物理またはクラウドベースの IT リソースにアクセスするネットワーク ユーザのアクティビティに対する非常に優れた制御が実現されます。
- 中央集中化、非常にセキュアなアクセスポリシー管理、およびスケーラブルな実行メカニズムにより、総所有コストが削減されます。
- 詳細については、次の URL を参照してください。

| 参照先 | 説明 |
|---|---|
| http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html | 企業向けの Cisco TrustSec システムおよびアーキテクチャが説明されています。 |
| http://www.cisco.com/en/us/solutions/enterprise/design-zone-security/landing_DesignZone_TrustSec.html | コンポーネントの設計ガイドへのリンクなど、Cisco TrustSec ソリューションを企業に導入する場合の手順が紹介されています。 |
| http://www.cisco.com/en/us/solutions/collateral/enterprise-networks/trustsec/solution_overview_c22-591177.pdf | Cisco TrustSec ソリューションを ASA、スイッチ、ワイヤレス LAN（WLAN）コントローラ、およびルータと共に使用する場合の概要が紹介されています。 |
| http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html | Cisco TrustSec プラットフォームのサポート一覧が掲載されています。Cisco TrustSec ソリューションをサポートしているシスコ製品を確認できます。 |

# Cisco TrustSec の SGT および SXP サポートについて

Cisco TrustSec 機能では、セキュリティ グループ アクセスは、トポロジ認識ネットワークをロールベースのネットワークに変換するため、ロールベース アクセス コントロール（RBAC）に基づいて実施されるエンドツーエンドポリシーがイネーブルになります。認証時に取得されたデバイスおよびユーザ クレデンシャルは、パケットをセキュリティ グループごとに分類するために使用されます。Cisco TrustSec クラウドに着信するすべてのパケットは、セキュリティ グループ タグ（SGT）でタグ付けされます。タギングは、信頼できる中継がパケットの送信元のアイデンティティを識別し、データ パスでセキュリティ ポリシーを適用するのに役立ちます。SGT は、SGT を使用してセキュリティ グループ ACL を定義する場合に、ドメイン全体の特権レベルを示すことができます。

SGT は、RADIUS ベンダー固有属性で発生する IEEE 802.1X 認証、Web 認証、または MAC 認証バイパス（MAB）を使用してデバイスに割り当てられます。SGT は、特定の IP アドレスまたはスイッチ インターフェイスにスタティックに割り当てることができます。SGT は、認証の成功後にスイッチまたはアクセス ポイントにダイナミックに渡されます。

セキュリティ グループ交換プロトコル（SXP）は、SGT およびセキュリティ グループ ACL をサポートしているハードウェアに対する SGT 対応ハードウェア サポートがないネットワーク デバイスに IP-to-SGT マッピング データベースを伝搬できるよう Cisco TrustSec 向けに開発されたプロトコルです。コントロール プレーン プロトコルの SXP は、IP-SGT マッピングを認証ポイント（レガシー アクセス レイヤ スイッチなど）からネットワークのアップストリーム デバイスに渡します。

SXP 接続はポイントツーポイントであり、基礎となる転送プロトコルとして TCP を使用します。SXP は接続を開始するために既知の TCP ポート番号 64999 を使用します。また、SXP 接続は、送信元および宛先 IP アドレスによって一意に識別されます。

# Cisco TrustSec 機能のロール

アイデンティティおよびポリシーベースのアクセス実施を提供するために、Cisco TrustSec 機能には、次のロールがあります。

- アクセス要求側（AR）：アクセス要求側は、ネットワークの保護されたリソースへのアクセスを要求するエンドポイント デバイスです。これらのデバイスはアーキテクチャのプライマリ対象であり、そのアクセス権限はアイデンティティ クレデンシャルによって異なります。

  アクセス要求側には、PC、ラップトップ、携帯電話、プリンタ、カメラ、MACsec 対応 IP フォンなどのエンドポイント デバイスが含まれます。

- ポリシー デシジョン ポイント（PDP）：ポリシー デシジョン ポイントはアクセス コントロール判断を行います。PDP は 802.1x、MAB、Web 認証などの機能を提供します。PDP は VLAN、DACL および Security Group Access（SGACL/SXP/SGT）による許可および適用をサポートします。

  Cisco TrustSec 機能では、Cisco Identity Services Engine（ISE）が PDP として機能します。Cisco ISE はアイデンティティおよびアクセス コントロール ポリシーの機能を提供します。

- ポリシー情報ポイント（PIP）：ポリシー情報ポイントは、ポリシー デシジョン ポイントに外部情報（たとえば、評価、場所、および LDAP 属性）を提供する送信元です。

  ポリシー情報ポイントには、Session Directory、IPS センサー、Communication Manager などのデバイスが含まれます。

- ポリシー管理ポイント（PAP）：ポリシー管理ポイントはポリシーを定義し、許可システムに挿入します。PAP はアイデンティティ リポジトリとしても動作し、Cisco TrustSec タグからユーザ アイデンティティへのマッピングと、Cisco TrustSec タグからサーバ リソースへのマッピングを行います。

  Cisco TrustSec 機能では、Cisco Secure Access Control System（802.1x および SGT サポートと統合されたポリシー サーバ）が PAP として機能します。

- ポリシー エンフォースメント ポイント（PEP）：ポリシー エンフォースメント ポイントは、各 AR の PDP による決定（ポリシー ルールおよびアクション）を実行するエンティティです。PEPデバイスは、ネットワーク全体に存在するプライマリ通信パスを介してアイデンティティ情報を学習します。PEPデバイスは、エンドポイントエージェント、許可サーバ、ピア実行デバイス、ネットワーク フローなど、さまざまな送信元から各ARのアイデンティティ属性を学習します。同様に、PEPデバイスはSXPを使用して、ネットワーク全体で相互信頼できるピア デバイスに IP-SGT マッピングを伝搬します。

  ポリシー エンフォースメント ポイントには、Catalyst Switches、ルータ、ファイアウォール（具体的にはASA）、サーバ、VPNデバイス、SANデバイスなどのネットワーク デバイスが含まれます。

Cisco ASA は、アイデンティティ アーキテクチャの中で PEP の役割を果たします。SXP を使用して、ASAは、認証ポイントから直接アイデンティティ情報を学習し、その情報を使用してアイデンティティベースのポリシーを適用します。

# セキュリティ グループ ポリシーの適用

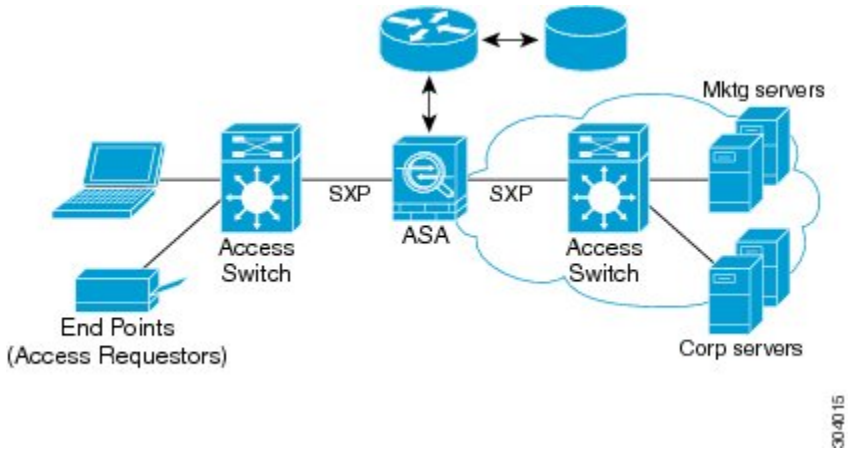
セキュリティ ポリシーの適用はセキュリティ グループの名前に基づきます。エンドポイントデバイスは、データセンターのリソースへのアクセスを試行します。ファイアウォールで設定された従来の IP ベースのポリシーと比較して、アイデンティティベースのポリシーは、ユーザおよびデバイス アイデンティティに基づいて設定されます。たとえば、mktg-contractor が mktg-server にアクセスできるとします。mktg-corp-user は、mktg-server および corp-server にアクセスできます。

このタイプの導入には次のような利点があります。

- ユーザ グループとリソースが1つのオブジェクト（SGT）を使用して定義されます（簡易ポリシー管理）。
- ユーザ アイデンティティとリソース アイデンティティは、Cisco TrustSec 対応スイッチ インフラストラクチャ全体で保持されます。

次の図に、セキュリティ グループの名前ベースのポリシー適用のための展開を示します。

図 *1:* セキュリティ グループ名に基づくポリシー適用の導入




Cisco TrustSec を実装すると、サーバのセグメンテーションをサポートするセキュリティ ポリシーを設定できます。また、Cisco TrustSec の実装には次のような特徴があります。

- 簡易ポリシー管理用に、サーバのプールに SGT を割り当てることができます。
- SGT 情報は、Cisco TrustSec 対応スイッチのインフラストラクチャ内に保持されます。
- ASA は、Cisco TrustSec ドメイン全体にポリシーを適用するために IP-SGT マッピングを利用できます。
- サーバの 802.1x 許可が必須であるため、導入を簡略化できます。

# ASA によるセキュリティ グループベースのポリシーの適用

（注） ユーザベースのセキュリティポリシーおよびセキュリティ グループベースのポリシーは、ASA で共存できます。セキュリティポリシーでは、ネットワーク属性、ユーザベースの属性、およびセキュリティ グループベースの属性の任意の組み合わせを設定できます。

Cisco TrustSec と連携するように ASA を設定するには、ISE から Protected Access Credential（PAC）ファイルをインポートする必要があります。

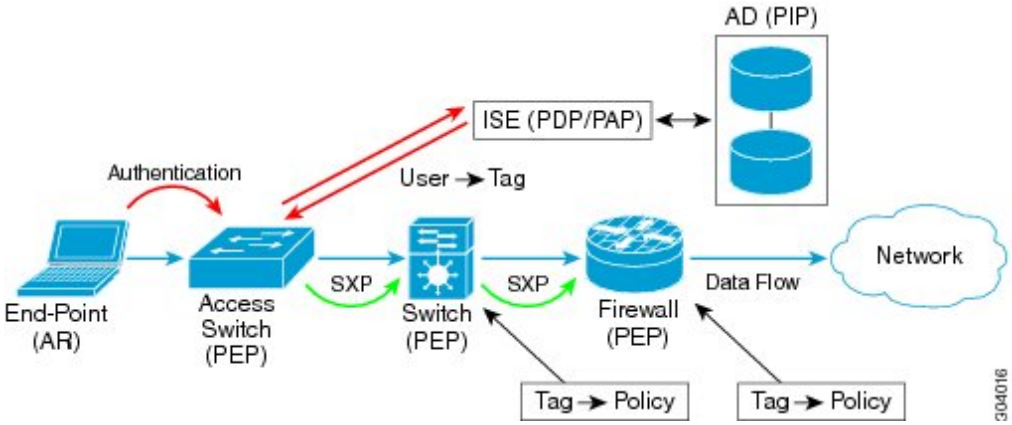
PAC ファイルを ASA にインポートすると、ISE との安全な通信チャネルが確立されます。チャネルが確立されると、ASA は、ISE を使用して PAC セキュア RADIUS トランザクションを開始し、Cisco TrustSec 環境データをダウンロードします（具体的には、セキュリティ グループ テーブル）。セキュリティ グループ テーブルによって、SGT がセキュリティ グループ名にマッピングされます。セキュリティ グループの名前は ISE 上で作成され、セキュリティ グループをわかりやすい名前で識別できるようになります。

ASA は、最初にセキュリティ グループ テーブルをダウンロードするときに、テーブル内のすべてのエントリを順を追って調べ、そこで設定されているセキュリティポリシーに含まれるすべてのセキュリティ グループの名前を解決します。次に、ASA は、それらのセキュリティ ポ

リシーをローカルでアクティブ化します。ASA がセキュリティ グループの名前を解決できない場合、不明なセキュリティ グループ名に対して syslog メッセージを生成します。

次の図に、セキュリティ ポリシーが Cisco TrustSec で適用される仕組みを示します。

**図 *2:* セキュリティ ポリシーの適用**




1. エンドポイント デバイスは、アクセス レイヤ デバイスに直接アクセスするか、またはリモート アクセスを介してアクセスし、Cisco TrustSec で認証します。
2. アクセス レイヤ デバイスは 802.1X や Web 認証などの認証方式を使用して ISE のエンドポイント デバイスを認証します。エンドポイント デバイスは、ロールおよびグループ メンバーシップ情報を渡して、デバイスを適切なセキュリティ グループに分類します。
3. アクセス レイヤ デバイスは SXP を使用して、アップストリーム デバイスに IP-SGT マッピングを伝搬します。
4. ASA はパケットを受信すると、SXP から渡された IP-SGT マッピングを使用して、送信元および宛先 IP アドレスの SGT を調べます。

   マッピングが新規の場合、ASA はそのマッピングをローカル IP-SGT マネージャ データベースに記録します。コントロール プレーンで実行される IP-SGT マネージャ データベースは、各 IPv4 または IPv6 アドレスの IP-SGT マッピングを追跡します。データベースでは、マッピングが学習された送信元が記録されます。SXP 接続のピア IP アドレスがマッピングの送信元として使用されます。各 IP-SGT にマップされたエントリには、送信元が複数存在する可能性があります。

   ASA が送信者として設定されている場合、ASA は SXP ピアに IP-SGT マッピング エントリをすべて送信します。
5. ASA で SGT またはセキュリティ グループの名前を使用してセキュリティ ポリシーが設定されている場合、ASA はそのポリシーを適用します。（ASA では、SGT またはセキュリティ グループの名前を含むセキュリティ ポリシーを作成できます。セキュリティ グループの名前に基づいてポリシーを適用するには、ASA はセキュリティ グループ テーブルで SGT にセキュリティ グループの名前をマッピングする必要があります）。

   ASA がセキュリティ グループ テーブルでセキュリティ グループの名前を見つけることができず、その名前がセキュリティ ポリシーに含まれている場合、ASA は、セキュリティ

グループの名前を不明と見なし、syslogメッセージを生成します。ISEからのセキュリティ グループ テーブルの更新とセキュリティ グループの名前の学習後、ASA はセキュリティ グループの名前がわかっていることを示す syslog メッセージを生成します。

# セキュリティ グループに対する変更が ISE に及ぼす影響

ASA は、ISE から最新のテーブルをダウンロードして、セキュリティ グループ テーブルを定期的に更新します。セキュリティ グループは、ダウンロードの合間にISEで変更できます。これらの変更は、セキュリティ グループ テーブルが更新されるまで、ASAには反映されません。

ヒント ISE のポリシー設定の変更は、メンテナンス時間中にスケジュールすることをお勧めします。さらに、セキュリティ グループの変更を確実に行うには、ASA でセキュリティ グループ テーブルを手動で更新します。

このようにポリシー設定の変更を行うことで、セキュリティグループの名前を解決し、セキュリティ ポリシーを即座にアクティブ化できる可能性が最大限に高まります。

セキュリティ グループ テーブルは、環境データのタイマーが期限切れになると自動的に更新されます。セキュリティ グループ テーブルの更新は、オンデマンドでトリガーすることも可能です。

ISE でセキュリティ グループを変更する場合、ASA がセキュリティ グループ テーブルを更新するときに次のイベントが発生します。

- セキュリティ グループの名前を使用して設定されたセキュリティ グループ ポリシーだけは、セキュリティ グループ テーブルを通じて解決する必要があります。セキュリティ グループ タグを含むポリシーは、常にアクティブになります。
- セキュリティ グループ テーブルが初めて利用できるようになったときに、セキュリティグループの名前を含むすべてのポリシーが確認され、セキュリティグループの名前が解決され、ポリシーがアクティブ化されます。また、タグ付きのすべてのポリシーが確認されます。不明なタグの場合は syslog が生成されます。
- セキュリティ グループ テーブルの期限が切れていても、そのテーブルをクリアするか、新しいテーブルを使用できるようになるまで、最後にダウンロードしたセキュリティ グループ テーブルに従って引き続きポリシーが適用されます。
- ASA で解決済みのセキュリティ グループの名前が不明になると、セキュリティ ポリシーが非アクティブ化されます。ただし、ASA の実行コンフィギュレーションではセキュリティ ポリシーが保持されます。
- PAP で既存のセキュリティ グループが削除されると、既知のセキュリティ グループ タグが不明になる可能性がありますが、ASA のポリシー ステータスは変化しません。既知のセキュリティグループの名前は未解決になる可能性があり、その場合、ポリシーは非アクティブになります。セキュリティグループの名前が再利用される場合、新しいタグを使用してポリシーが再コンパイルされます。

- PAP で新しいセキュリティ グループが追加されると、不明なセキュリティ グループ タグが既知になる可能性があり、syslog メッセージが生成されます。ただし、ポリシー ステータスは変化しません。不明なセキュリティ グループの名前が解決される可能性があり、その場合、関連付けられているポリシーがアクティブ化されます。
- PAP でタグの名前が変更された場合、タグを使用して設定されたポリシーによって新しい名前が表示されます。ポリシー ステータスは変化しません。セキュリティ グループの名前を使用して設定されたポリシーは、新しいタグ値を使用して再コンパイルされます。

# ASA での送信者および受信者のロール

ASA では、SXP の他のネットワーク デバイスとの間の IP-SGT マッピング エントリの送受信がサポートされます。SXP を使用すると、セキュリティ デバイスとファイアウォールが、ハードウェアをアップグレードまたは変更する必要なく、アクセス スイッチからのアイデンティティ情報を学習できます。また、SXP を使用して、アップストリーム デバイス（データセンター デバイスなど）からの IP-SGT マッピング エントリをダウンストリーム デバイスに渡すこともできます。ASA は、アップストリームおよびダウンストリームの両方向から情報を受信できます。

ASA での SXP ピアへの SXP 接続を設定する場合は、アイデンティティ情報を交換できるように、ASA を送信者または受信者として指定する必要があります。

- 送信者モード：ASA で収集されたアクティブな IP-SGT マッピング エントリをすべてポリシー適用のためアップストリーム デバイスに転送できるように ASA を設定します。
- 受信者モード：ダウンストリーム デバイス（SGT 対応スイッチ）からの IP-SGT マッピング エントリを受信し、ポリシー定義作成のためにこの情報を使用できるように ASA を設定します。

SXP 接続の一方の端が送信者として設定されている場合、もう一方の端は受信者として設定する必要があります。逆の場合も同様です。SXP 接続の両端の両方のデバイスに同じロール（両方とも送信者または両方とも受信者）が設定されている場合、SXP 接続が失敗し、ASA は syslog メッセージを生成します。

SXP 接続が複数ある場合でも、IP-SGT マッピング データベースからダウンロードされた IP-SGT マッピング エントリを学習できます。ASA で SXP ピアへの SXP 接続が確立されると、受信者が送信者から IP-SGT マッピング データベース全体をダウンロードします。この後に行われる変更はすべて、新しいデバイスがネットワークに接続されたときにのみ送信されます。このため、SXP の情報が流れる速さは、エンドホストがネットワーク認証を行う速さに比例します。

SXP 接続を通じて学習された IP-SGT マッピング エントリは、SXP IP-SGT マッピング データベースで管理されます。同じマッピング エントリが異なる SXP 接続を介して学習される場合もあります。マッピング データベースは、学習した各マッピング エントリのコピーを 1 つ保持します。同じ IP-SGT マッピング値の複数のマッピング エントリは、マッピングを学習した接続のピア IP アドレスによって識別されます。SXP は IP-SGT マネージャに対して、新しいマッピングが初めて学習された場合にはマッピング エントリを追加するように、SXP データベース内の最後のコピーが削除された場合にはマッピングエントリを削除するように要求します。

SXP 接続が送信者として設定されている場合は必ず、SXP は IP-SGT マネージャに対して、デバイスで収集したすべてのマッピングエントリをピアに転送するよう要求します。新しいマッピングがローカルで学習されると、IP-SGT マネージャは SXP に対して、送信者として設定されている接続を介してそのマッピングを転送するよう要求します。

ASA を SXP 接続の送信者および受信者の両方として設定すると、SXP ループが発生する可能性があります。つまり、SXP データが最初にそのデータを送信した SXP ピアで受信される可能性があります。

# ISE への ASA の登録

ASA が PAC ファイルを正常にインポートするには、ISE の認識された Cisco TrustSec ネットワーク デバイスとして ASA を設定する必要があります。ISE に ASA を登録するには、次の手順を実行します。

**手順**

**ステップ 1** ISE にログインします。

**ステップ 2** [Administration] > [Network Devices] > [Network Devices] を選択します。

**ステップ 3** [Add] をクリックします。

**ステップ 4** ASA の IP アドレスを入力します。

**ステップ 5** ISE がユーザ認証用に使用されている場合、[Authentication Settings] 領域に共有秘密を入力します。

ASA で AAA サーバを設定する場合は、ISE でここで作成した共有秘密を指定します。ASA の AAA サーバはこの共有秘密を使用して、ISE と通信します。

**ステップ 6** ASA のデバイス名、デバイス ID、パスワード、およびダウンロード間隔を指定します。これらのタスクの実行方法については、ISE のマニュアルを参照してください。

# ISE でのセキュリティ グループの作成

ISE と通信するように ASA を設定する場合は、AAA サーバを指定します。AAA サーバを ASA で設定する場合は、サーバ グループを指定する必要があります。セキュリティ グループは、RADIUS プロトコルを使用するように設定する必要があります。ISE でセキュリティ グループを作成するには、次の手順を実行します。

**手順**

**ステップ 1** ISE にログインします。

**ステップ 2** [Policy] > [Policy Elements] > [Results] > [Security Group Access] > [Security Group] を選択します。

**ステップ 3** ASAのセキュリティ グループを追加します。（セキュリティ グループは、グローバルであり、ASA に固有ではありません）。

ISE は、タグを使用して [Security Groups] でエントリを作成します。

**ステップ 4** [Security Group Access] 領域で、ASA のデバイス ID クレデンシャルおよびパスワードを設定します。

# PAC ファイルの生成

PAC ファイルを生成するには、次の手順を実行します。

（注） PAC ファイルには、ASA および ISE がその間で発生する RADIUS トランザクションを保護できる共有キーが含まれています。このため、必ずこのキーを安全にASAに保存してください。

**手順**

**ステップ 1** ISE にログインします。

**ステップ 2** [Administration] > [Network Resources] > [Network Devices] を選択します。

**ステップ 3** デバイスのリストから ASA を選択します。

**ステップ 4** [Security Group Access (SGA)] で、[Generate PAC] をクリックします。

**ステップ 5** PAC ファイルを暗号化するには、パスワードを入力します。

PAC ファイルを暗号化するために入力するパスワード（または暗号キー）は、デバイス クレデンシャルの一部として ISE で設定したパスワードとは関係ありません。

ISE はPACファイルを生成します。ASAは、フラッシュ、またはTFTP、FTP、HTTP、HTTPS、SMB を介してリモート サーバから PAC ファイルをインポートできます。（PAC ファイルは、インポート前に ASA フラッシュに配置されている必要はありません）。

# Cisco TrustSec のガイドライン

ここでは、Cisco TrustSec を設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

### フェールオーバー

- アクティブ/アクティブおよびアクティブ/スタンバイ コンフィギュレーションの両方で ASA のセキュリティ グループベースのポリシーを設定できます。

- ASA がフェールオーバー設定の一部である場合、プライマリ ASA デバイスに PAC ファイルをインポートする必要があります。また、プライマリ デバイスで環境データを更新する必要もあります。
- ASA は、ハイ アベイラビリティ（HA）用に設定された ISE と通信できます。
- ASA では複数の ISE サーバを設定できます。最初のサーバが到達不能の場合、引き続き 2 番目以降のサーバに接続を試みます。ただし、サーバ リストが Cisco TrustSec 環境データの一部としてダウンロードされた場合、そのリストは無視されます。
- ISE からダウンロードされた PAC ファイルが ASA で期限切れとなり、ASA が更新されたセキュリティ グループ テーブルをダウンロードできない場合、ASA が更新されたテーブルをダウンロードするまで、最後にダウンロードされたセキュリティ グループ テーブルに基づいてセキュリティ ポリシーを適用し続けます。

### クラスタ

- ASA がクラスタリング設定の一部である場合、マスター ユニットに PAC ファイルをインポートする必要があります。
- ASA がクラスタリング設定の一部である場合、マスター ユニットで環境データを更新する必要があります。

### IPv6

ASA は、IPv6 と IPv6 対応ネットワーク デバイス用に SXP をサポートします。AAA サーバは IPv4 アドレスを使用する必要があります。

### レイヤ 2 SGT インポジション

- 物理インターフェイス、サブインターフェイス、EtherChannel インターフェイス、および冗長インターフェイスでのみサポートされます。
- 論理インターフェイスまたは仮想インターフェイス（BVI など）ではサポートされません。
- SAP ネゴシエーションおよび MACsec を使用したリンク暗号化はサポートされていません。
- フェールオーバー リンクではサポートされません。
- クラスタ制御リンクではサポートされません。
- SGT が変更されても、ASA は既存のフローを再分類しません。以前の SGT に基づいて行われたポリシーに関する決定が、フローのライフサイクルにわたって適用され続けます。ただし、ASA は、パケットが以前の SGT に基づいて分類されたフローに属していても、SGT の変更内容を出力パケットに即座に反映できます。
- ASA 5585-X のハードウェア アーキテクチャは、通常のパケットのロード バランシングを最適な方法で行えるように設計されていますが、レイヤ 2 セキュリティ グループのタギン

グ インポジションでタグ付けされたインライン パケットに適したアーキテクチャではありません。ASA 5585-X では、タグ付けされた着信インライン タグ付きパケットを処理する際に、パフォーマンスが大きく低下することがあります。この問題は、ASA 5585-X のタグなしパケットだけでなく、他の ASA プラットフォームのタグ付きインライン パケットでも発生しません。回避策の 1 つは、タグ付きインライン パケットが ASA 5585-X に最小限しか送信されないようにアクセス ポリシーを調整することです。こうすることで、タグ付けされたポリシーの適用をスイッチで行えるようになります。ASA 5585-X において、タグ付きパケットを受信する必要なく、IP アドレスをセキュリティ グループ タグにマッピングできるように SXP を使用する方法も回避策になります。

- ASASM は、レイヤ 2 セキュリティ グループのタギング インポジションをサポートしていません。

### その他のガイドライン

- ASA は、SXP バージョン 3 をサポートしています。ASA は、さまざまな SXP 対応ネットワーク デバイスの SXP バージョンをネゴシエートします。
- SXP 調整タイマーの期限が切れたときにセキュリティ グループ テーブルを更新するように ASA を設定できます。セキュリティ グループ テーブルはオンデマンドでダウンロードできます。ASA のセキュリティ グループ テーブルが ISE から更新された場合、この変更が適切なセキュリティ ポリシーに反映されます。
- Cisco TrustSec は、シングル コンテキスト モードおよびマルチ コンテキスト モード（システム コンテキスト モードを除く）で Smart Call Home 機能をサポートしています。
- ASA は、単一の Cisco TrustSec ドメインでのみ相互運用するように設定できます。
- ASA は、デバイスの SGT 名のマッピングのスタティック コンフィギュレーションをサポートしていません。
- NAT は SXP メッセージでサポートされません。
- SXP はネットワークのエンフォースメント ポイントに IP-SGT マッピングを伝搬します。アクセス レイヤ スイッチがエンフォースメント ポイントと異なる NAT ドメインに属している場合、アップロードする IP-SGT マップは無効であり、実行デバイスに対する IP-SGT マッピング データベース検索から有効な結果を得ることはできません。その結果、ASA は実行デバイスにセキュリティ グループ対応セキュリティ ポリシーを適用できません。
- SXP 接続に使用する ASA にデフォルト パスワードを設定するか、またはパスワードを使用しないようにします。ただし、接続固有パスワードは SXP ピアではサポートされません。設定されたデフォルト SXP パスワードは導入ネットワーク全体で一貫している必要があります。接続固有パスワードを設定すると、接続が失敗する可能性があり、警告メッセージが表示されます。デフォルトパスワードを使用して接続を設定しても設定されていない場合、結果はパスワードなしで接続を構成した場合と同じです。
- ASA を SXP 送信者または受信者、あるいはその両方として設定できます。ただし、SXP 接続のループは、デバイスにピアへの双方向の接続がある場合、またはデバイスがデバイスの単方向に接続されたチェーンの一部である場合に発生します。（ASA は、データセン

ターのアクセス レイヤからのリソースの IP-SGT マッピングを学習できます。ASA は、これらのタグをダウンストリーム デバイスに伝搬する必要がある場合があります）。SXP 接続ループによって、SXP メッセージ転送の予期しない動作が発生する可能性があります。ASA が送信者および受信者として設定されている場合、SXP 接続ループが発生し、SXP データが最初にそのデータを送信したピアで受信される可能性があります。

- ASA のローカル IP アドレスを変更する場合は、すべての SXP ピアでピア リストが更新されていることを確認する必要があります。さらに、SXP ピアがその IP アドレスを変更する場合は、変更が ASA に反映されていることを確認する必要があります。
- 自動 PAC ファイル プロビジョニングはサポートされません。ASA 管理者は、ISE 管理インターフェイスの PAC ファイルを要求し、それを ASA にインポートする必要があります。
- PAC ファイルには有効期限があります。現在の PAC ファイルが期限切れになる前に更新された PAC ファイルをインポートする必要があります。そうしないと、ASA は環境データの更新を取得できません。ISE からダウンロードされた PAC ファイルが ASA で期限切れとなり、ASA が更新されたセキュリティ グループ テーブルをダウンロードできない場合、ASA が更新されたテーブルをダウンロードするまで、最後にダウンロードされたセキュリティ グループ テーブルに基づいてセキュリティ ポリシーを適用し続けます。
- セキュリティ グループが ISE で変更された（名前変更、削除など）場合、ASA は、変更されたセキュリティ グループに関連付けられた SGT またはセキュリティ グループ名を含む ASA セキュリティ ポリシーのステータスを変更しません。ただし、ASA は、それらのセキュリティ ポリシーが変更されたことを示す syslog メッセージを生成します。
- マルチキャスト タイプは ISE 1.0 ではサポートされていません。
- SXP 接続は、次の例に示すように、ASA によって相互接続された 2 つの SXP ピア間で初期化状態のままとなります。

```
(SXP peer A) - - - - (ASA) - - - (SXP peer B)
```

したがって、Cisco TrustSec と統合するように ASA を設定する場合は、SXP 接続を設定するために、ASA で、no-NAT、no-SEQ-RAND、MD5-AUTHENTICATION TCP オプションをイネーブルにする必要があります。SXP ピア間の SXP ポート TCP 64999 宛てのトラフィックに対して TCP 状態バイパス ポリシーを作成します。そして、適切なインターフェイスにポリシーを適用します。

たとえば、次のコマンド セットは、TCP 状態バイパス ポリシーの ASA の設定方法を示しています。

```
access-list SXP-MD5-ACL extended permit tcp host peerA host peerB eq 64999
access-list SXP-MD5-ACL extended permit tcp host peerB host peerA eq 64999

tcp-map SXP-MD5-OPTION-ALLOW
 tcp-options range 19 19 allow

class-map SXP-MD5-CLASSMAP
 match access-list SXP-MD5-ACL
```

```
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
class SXP-MD5-CLASSMAP
  set connection random-sequence-number disable
  set connection advanced-options SXP-MD5-OPTION-ALLOW
  set connection advanced-options tcp-state-bypass
service-policy global_policy global
```

# Cisco TrustSec と統合するための ASA の設定

Cisco TrustSec と統合するように ASA を設定するには、次のタスクを実行します。

### 始める前に

Cisco TrustSec と統合するように ASA を設定する前に、ISE で次のタスクを実行する必要があります。

- ISE への ASA の登録 （9 ページ）
- ISE でのセキュリティ グループの作成 （9 ページ）
- PAC ファイルの生成 （10 ページ）

### 手順

**ステップ 1** Cisco TrustSec と統合するための AAA サーバの設定 （14 ページ）

**ステップ 2** PAC ファイルのインポート （15 ページ）

**ステップ 3** Security Exchange Protocol の設定 （17 ページ）

このタスクでは、SXP のデフォルト値を有効にし、設定します。

**ステップ 4** SXP 接続のピアの追加 （18 ページ）

**ステップ 5** 環境データの更新 （19 ページ）

必要に応じてこれを実行してください。

**ステップ 6** セキュリティ ポリシーの設定 （20 ページ）

**ステップ 7** レイヤ 2 セキュリティ グループのタギング インポジションの設定 （21 ページ）

# Cisco TrustSec と統合するための AAA サーバの設定

ここでは、Cisco TrustSec の AAA サーバを統合する方法について説明します。ASA で ISE と通信するように AAA サーバ グループを設定するには、次の手順を実行します。

### 始める前に

- 参照先のサーバ グループは、RADIUS プロトコルを使用するように設定する必要があります。ASA に非 RADIUS サーバ グループを追加すると、設定は失敗します。
- ISE もユーザ認証に使用する場合は、ISE に ASA を登録したときに ISE で入力した共有秘密を取得します。この情報については、ISE 管理者に問い合わせてください。

### 手順

**ステップ 1** [Configuration] > [Firewall] > [Identity By TrustSec] を選択します。

**ステップ 2** ASA にサーバ グループを追加するには、[Manage] をクリックします。

[Configure AAA Server Group] ダイアログボックスが表示されます。

**ステップ 3** ASA 用 ISE で作成したセキュリティ グループの名前を入力します。

ここで指定するサーバ グループ名は、ASA 用 ISE で作成したセキュリティ グループの名前と一致している必要があります。2 つのグループ名が一致しない場合、ASA は ISE と通信できません。この情報については、ISE 管理者に問い合わせてください。

**ステップ 4** [Protocol] ドロップダウンリストから [RADIUS] を選択します。

[AAA Server Group] ダイアログボックスの残りのフィールドの入力については、一般的な操作の設定ガイドの RADIUS の章を参照してください。

**ステップ 5** [OK] をクリックします。

**ステップ 6** グループにサーバを追加するには、作成した AAA サーバ グループを選択し、[Servers in the Selected Group] 領域で [Add] をクリックします。

[Add AAA Server] ダイアログボックスが表示されます。

**ステップ 7** ISE サーバが配置されているネットワーク インターフェイスを選択します。

**ステップ 8** ISE サーバの IP アドレスを入力します。

[AAA Server] ダイアログボックスの残りのフィールドの入力については、一般的な操作の設定ガイドの RADIUS の章を参照してください。

**ステップ 9** [OK] をクリックします。

**ステップ 10** [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

# PAC ファイルのインポート

ここでは、PAC ファイルをインポートする方法について説明します。

### 始める前に

- ASA が PAC ファイルを生成するには、ISE の認識された Cisco TrustSec ネットワーク デバイスとして ASA を設定する必要があります。
- ISE での PAC ファイルの生成時に PAC ファイルを暗号化するために使用されたパスワードを取得します。ASA は、PAC ファイルをインポートし、復号化する場合にこのパスワードが必要となります。
- ASA は、ISE で生成された PAC ファイルにアクセスする必要があります。ASA は、フラッシュ、または TFTP、FTP、HTTP、HTTPS、SMB を介してリモート サーバから PAC ファイルをインポートできます。（PAC ファイルは、インポート前に ASA フラッシュに配置されている必要はありません）。
- ASA のサーバ グループを設定します。

PAC ファイルをインポートするには、次の手順を実行します。

### 手順

**ステップ 1** [Configuration] > [Firewall] > [Identity By TrustSec] を選択します。

**ステップ 2** [Enable Security Exchange Protocol] チェック ボックスをオンにして、SXP をイネーブルにします。

**ステップ 3** [Import PAC] をクリックして [Import PAC] ダイアログボックスを表示します。

**ステップ 4** 次の形式の 1 つを使用して PAC ファイルのパスとファイル名を入力します。

- **disk0**：disk0 のパスおよびファイル名
- **disk1**：disk1 のパスおよびファイル名
- **flash**：フラッシュのパスおよびファイル名
- **ftp**：FTP のパスおよびファイル名
- **http**：HTTP のパスおよびファイル名
- **https**：HTTPS のパスおよびファイル名
- **smb**：SMB のパスおよびファイル名
- **tftp**：TFTP のパスおよびファイル名

### マルチ モード

- **http**：HTTP のパスおよびファイル名
- **https**：HTTPS のパスおよびファイル名
- **smb**：SMB のパスおよびファイル名
- **tftp**：TFTP のパスおよびファイル名

**ステップ 5** PAC ファイルの暗号化に使用されるパスワードを入力します。このパスワードは、デバイス クレデンシャルの一部として ISE で設定したパスワードとは関係ありません。

**ステップ 6** 確認のためにパスワードを再入力します。

**ステップ 7** [Import] をクリックします。

**ステップ 8** [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

PAC ファイルをインポートする場合、ファイルは ASCII 16 進形式に変換され、非インタラクティブ モードで ASA に送信されます。

# Security Exchange Protocol の設定

Cisco TrustSec を使用するように Security Exchange Protocol（SXP）を有効にして設定する必要があります。

### 始める前に

少なくとも 1 つのインターフェイスを UP/UP ステートにする必要があります。すべてのインターフェイスがダウンした状態で SXP がイネーブルになっている場合、ASA では、SXP が動作していない、あるいは SXP をイネーブルにできなかったことを示すメッセージは表示されません。show running-config コマンドを入力して設定を確認すると、コマンドの出力に次のメッセージが表示されます。

```
"WARNING: SXP configuration in process, please wait for a few moments and try again."
```

### 手順

**ステップ 1** **[Configuration]** > **[Firewall]** > **[Identity By TrustSec]** を選択します。

**ステップ 2** [Enable Security Exchange Protocol] チェック ボックスをオンにして、SXP をイネーブルにします。SXP は、デフォルトで、ディセーブルに設定されています。

**ステップ 3** （任意。推奨されません）SXP接続のデフォルトのローカル IP アドレスを入力します。IP アドレスは、IPv4 または IPv6 アドレスを使用できます。

（注） ピア IP アドレスが到達可能な発信インターフェイスの IP アドレスとして、ASA が SXP 接続のローカル IP アドレスを指定します。設定されたローカル アドレスがインターフェイスの IP アドレスと異なる場合、ASA は SXP ピアに接続できず、syslog メッセージを生成します。SXP接続のデフォルトの送信元IPアドレスを設定せずに、ASA が route/ARP 検索を実行して SXP 接続の送信元 IP アドレスを決定できるようにすることを推奨します。

**ステップ 4** （任意）SXP ピアでの TCP MD5 認証のデフォルト パスワードを入力します。デフォルトでは、SXP 接続にパスワードは設定されていません。

デフォルトのパスワードを使用するように SXP 接続ピアを設定した場合、または設定した場合にのみ、デフォルトのパスワードを設定します。パスワードには、最大 80 文字を指定できます。これは暗号化されません。

**ステップ 5** （任意）ASA 試行間の時間間隔を変更し、[Retry Timer] フィールドで SXP ピア間の新しい SXP 接続を設定します。

ASA は、成功した接続が確立されるまで接続を試み続け、失敗した試行後、再度試行するまでに再試行間隔の間待機します。再試行期間には 0 ～ 64000 秒の値を指定できます。デフォルトは 120 秒です。0 秒を指定すると、ASA は SXP ピアへの接続を試行しません。

再試行タイマーは、SXP ピア デバイスとは異なる値に設定することを推奨します。

**ステップ 6** （任意）調整タイマーの値を変更します。

SXP ピアが SXP 接続を終了すると、ASA はホールド ダウン タイマーを開始します。ホールド ダウン タイマーの実行中に SXP ピアが接続されると、ASA は調整タイマーを開始します。次に、ASA は、SXP マッピング データベースを更新して、最新のマッピングを学習します。

調整タイマーの期限が切れると、ASA は、SXP マッピング データベースをスキャンして、古いマッピング エントリ（前回の接続セッションで学習されたエントリ）を識別します。ASA は、これらの接続を廃止としてマークします。調整タイマーが期限切れになると、ASA は、SXP マッピング データベースから廃止エントリを削除します。

調整期間には 1 ～ 64000 秒の値を指定できます。デフォルトは 120 秒です。

**ステップ 7** （任意）[Network Map] で、SXPv2 以下を使用するピアへのスピーカーとして機能する場合の IPv4 サブネット拡張の深さを設定します。

ピアが SXPv2 以下を使用する場合、ピアはサブネット バインディングへの SGT を理解できません。ASA は、個々のホスト バインディングに IPv4 サブネット バインディングを拡張できます（IPv6 バインディングは拡張されません）。このコマンドでは、サブネット バインディングから生成できるホスト バインディングの最大数が指定されます。

最大数には 0 ～ 65535 を指定できます。デフォルトは 0 で、サブネット バインディングがホスト バインディングに拡張されないことを意味します。

**ステップ 8** [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

# SXP 接続のピアの追加

SXP 接続のピアを追加するには、次の手順を実行します。

**手順**

**ステップ 1** **[Configuration] > [Firewall] > [Identity By TrustSec]** を選択します。

**ステップ 2** [Add] をクリックして、[Add Connection] ダイアログボックスを表示します。

**ステップ 3** SXP ピアの IPv4 アドレスまたは IPv6 アドレスを入力します。ピア IP アドレスは、ASA 発信インターフェイスからアクセスできる必要があります。

**ステップ 4** 次の値の 1 つを選択し、SXP 接続に認証キーを使用するかどうかを指定します。

- [Default]：SXP 接続用に設定されたデフォルト パスワードを使用します。
- [None]：SXP 接続にパスワードを使用しません。

**ステップ 5** （任意）次の値の 1 つを選択し、SXP 接続のモードを指定します。

- [Local]：ローカル SXP デバイスを使用します。
- [Peer]：ピア SXP デバイスを使用します。

**ステップ 6** SXP 接続で、ASA が送信者または受信者のいずれとして機能するかを指定します。

- [Speaker]：ASA は IP-SGT マッピングをアップストリーム デバイスに転送できます。
- [Listener]：ASA はダウンストリーム デバイスから IP-SGT マッピングを受信できます。

**ステップ 7** （オプション）[Advanced] をクリックして、SXP 接続のローカル IPv4 または IPv6 アドレスを入力します。

ASA は、ルート ルックアップを使用して正しいインターフェイスを決定します。アドレスを指定する場合は、発信インターフェイスのルート ルックアップ インターフェイス アドレスと一致する必要があります。SXP 接続の送信元 IP アドレスを設定せずに、ASA が route/ARP 検索を実行して SXP 接続の送信元 IP アドレスを決定できるようにすることを推奨します。

**ステップ 8** [OK] をクリックします。

**ステップ 9** [Apply] をクリックして設定を実行コンフィギュレーションに保存します。

# 環境データの更新

ASA は、ISE からセキュリティ グループ タグ（SGT）名テーブルなどの環境データをダウンロードします。ASA で次のタスクを完了すると、ASA は、ISE から取得した環境データを自動的にリフレッシュします。

- ISE と通信するように AAA サーバを設定します。
- ISE から PAC ファイルをインポートします。
- Cisco TrustSec 環境データを取得するために ASA で使用する AAA サーバ グループを識別します。

通常、ISE からの環境データを手動でリフレッシュする必要はありません。ただし、セキュリティ グループが ISE で変更されることがあります。ASA セキュリティ グループ テーブルのデータをリフレッシュするまで、これらの変更は ASA に反映されません。そのため、ASA の

データをリフレッシュして、ISE でのセキュリティ グループの変更が確実に ASA に反映されるようにします。

（注） メンテナンス時間中に ISE のポリシー設定および ASA での手動データ リフレッシュをスケジュールすることを推奨します。このようにポリシー設定の変更を処理すると、セキュリティ グループ名が解決される可能性が最大化され、セキュリティ ポリシーが ASA で即時にアクティブ化されます。

環境データを更新するには、次の手順を実行します。

**手順**

**ステップ 1** [Configuration] > [Firewall] > [Identity By TrustSec] を選択します。

**ステップ 2** [Server Group Setup] 領域で **[Refresh Environment]** > **[Data]** をクリックします。

ASA は、ISE からの Cisco TrustSec 環境データをリフレッシュし、設定されたデフォルト値に調整タイマーをリセットします。

# セキュリティ ポリシーの設定

Cisco TrustSec ポリシーは、多くの ASA 機能に組み込むことができます。拡張 ACL を使用する機能（この章でサポート対象外としてリストされている機能を除く）で Cisco TrustSec を使用できます。拡張 ACL に、従来のネットワークベースのパラメータとともにセキュリティ グループ引数を追加できます。

- アクセス ルールを設定するには、アクセス ルールの設定 を参照してください。その他の拡張 ACL については、拡張 ACL の設定 を参照してください。
- ACL で使用できるセキュリティ グループ オブジェクト グループを設定する方法については、セキュリティ グループ オブジェクト グループの設定を参照してください。

たとえば、アクセスルールは、ネットワーク情報を使用してインターフェイスのトラフィックを許可または拒否します。Cisco TrustSec では、セキュリティ グループに基づいてアクセスを制御できます。たとえば、sample_securitygroup1 10.0.0.0 255.0.0.0 のアクセス ルールを作成できます。これは、セキュリティ グループがサブネット 10.0.0.0/8 上のどの IP アドレスを持っていてもよいことを意味します。

セキュリティ グループの名前（サーバ、ユーザ、管理対象外デバイスなど）、ユーザベース属性、および従来の IP アドレスベースのオブジェクト（IP アドレス、Active Directory オブジェクト、およびFQDN）の組み合わせに基づいてセキュリティ ポリシーを設定できます。セキュリティ グループ メンバーシップはロールを超えて拡張し、デバイスと場所属性を含めることができます。また、セキュリティ グループ メンバーシップは、ユーザ グループ メンバーシップに依存しません。

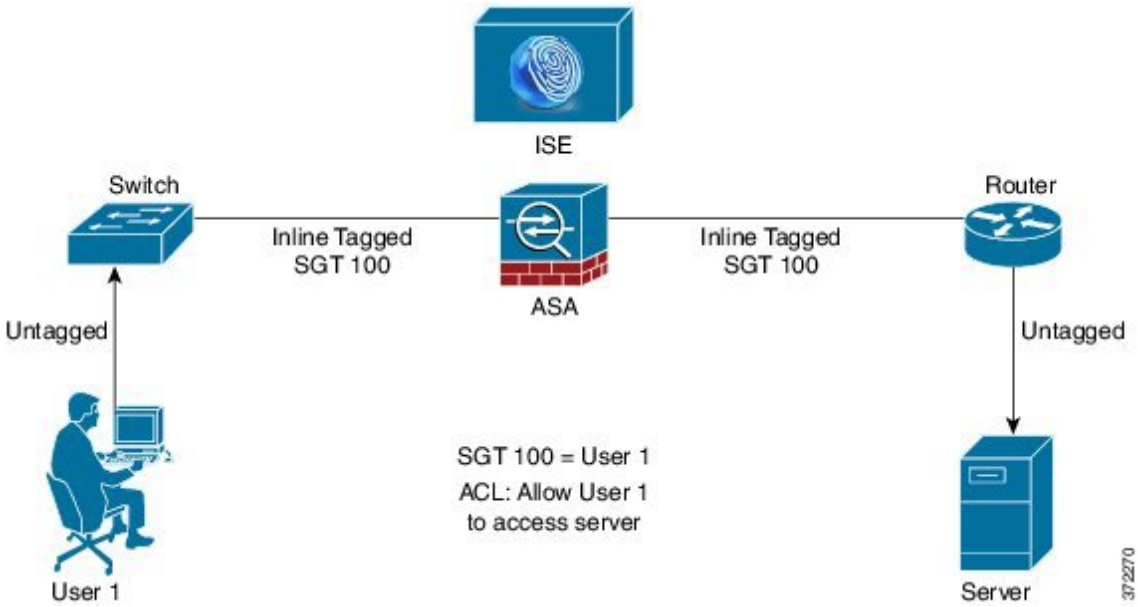
# レイヤ 2 セキュリティ グループのタギング インポジションの設定

Cisco TrustSec は、各ネットワーク ユーザおよびリソースの特定と認証を行い、セキュリティ グループ タグ（SGT）と呼ばれる 16 ビットの番号を割り当てます。この ID は、ネットワーク ホップ間で順番に伝搬されます。これにより、ASA、スイッチ、ルータなどの任意の中間デバイスで、この ID タグに基づいてポリシーを適用できます。

SGT とイーサネット タギング（レイヤ 2 SGT インポジションとも呼ばれる）を利用すると、ASA でシスコ独自のイーサネット フレーミング（EtherType 0x8909）を使用して、イーサネット インターフェイスでセキュリティ グループ タグを送受信できます。これにより、送信元のセキュリティ グループ タグをプレーン テキストのイーサネット フレームに挿入できます。ASA は、インターフェイスごとの手動設定に基づいて、発信パケットにセキュリティ グループ タグを挿入し、着信パケットのセキュリティ グループ タグを処理します。この機能を使用することで、ネットワーク デバイス間におけるエンドポイント ID の伝搬をインラインかつホップバイホップで実行できます。また、各ホップ間でシームレスなレイヤ 2 SGT インポジションを実現できます。

次の図 に、レイヤ 2 SGT インポジションの一般的な例を示します。

**図 *3 :* レイヤ *2 SGT* インポジション**




## 使用シナリオ

次の表で、この機能を設定した場合の入力トラフィックの予期される動作について説明します。

表 *1:* 入力トラフィック

| インターフェイス コンフィギュレーション | タグ付きの受信パケット | タグのない受信パケット |
|---|---|---|
| コマンドが発行されない。 | パケットがドロップされる。 | SGT 値が IP-SGT マネージャから取得される。 |
| cts manual コマンドが発行される。 | SGT 値が IP-SGT マネージャから取得される。 | SGT 値が IP-SGT マネージャから取得される。 |
| **cts manual** コマンドと **policy static sgt** *sgt_number* コマンドが両方とも発行される。 | SGT 値が **policy static sgt** *sgt_number* コマンドで取得される。 | SGT 値が **policy static sgt** *sgt_number* コマンドで取得される。 |
| **cts manual** コマンドと **policy static sgt** *sgt_number* **trusted** コマンドが両方とも発行される。 | SGT 値がパケットのインライン SGT から取得される。 | SGT 値が **policy static sgt** *sgt_number* コマンドで取得される。 |

（注） IP-SGT マネージャと一致する IP-SGT マッピングが存在しない場合、予約されている SGT 値（「不明」を表す「0x0」）が使用されます。

次の表で、この機能を設定した場合の出力トラフィックの予期される動作について説明します。

表 *2:* 出力トラフィック

| インターフェイス コンフィギュレーション | 送信パケットのタグの有無 |
|---|---|
| コマンドが発行されない。 | タグなし |
| cts manual コマンドが発行される。 | タグ付き |
| cts manual コマンドと propagate sgt コマンドが両方とも発行される。 | タグ付き |
| cts manual コマンドと no propagate sgt コマンドが両方とも発行される。 | タグなし |

次の表で、この機能を設定した場合の to-the-box トラフィックと from-the-box トラフィックの予期される動作について説明します。

表 *3 : to-the-box* トラフィックと *from-the-box* トラフィック

| インターフェイス コンフィギュレーション | 受信パケットのタグの有無 |
|---|---|
| to-the-box トラフィック用の入力インターフェイスで、コマンドが発行されない。 | パケットがドロップされる。 |
| to-the-box トラフィック用の入力インターフェイスで、cts manual コマンドが発行される。 | パケットは受け入れられるが、ポリシーの適用や SGT の伝搬は行われない。 |
| **cts manual** コマンドが発行されない。または、from-the-box トラフィック用の出力インターフェイスで、**cts manual** コマンドと **no propagate sgt** コマンドが両方とも発行される。 | タグなしパケットは送信されるが、ポリシーの適用は行われない。SGT 値が IP-SGT マネージャから取得される。 |
| cts manual コマンドが発行される。または、from-the-box トラフィック用の出力インターフェイスで、cts manual コマンドと propagate sgt コマンドが両方とも発行される。 | タグ付きパケットが送信される。SGT 値が IP-SGT マネージャから取得される。 |

（注） IP-SGT マネージャと一致する IP-SGT マッピングが存在しない場合、予約されている SGT 値（「不明」を表す「0x0」）が使用されます。

## インターフェイスでのセキュリティ グループ タグの設定

インターフェイスでセキュリティ グループ タグを設定するには、次の手順を実行します。

### 手順

**ステップ 1** 次のいずれかのオプションを選択します。

- **[Configuration] > [Device Setup]** > **[Interfaces]** > [Add Interface] > [Advanced]
- **[Configuration] > [Device Setup]** > **[Interfaces] > [Add Redundant Interface] > [Advanced]**
- **[Configuration] > [Device Setup]** > **[Interfaces] > [Add Ethernet Interface] > [Advanced]**

**ステップ 2** [Enable secure group tagging for Cisco TrustSec] チェック ボックスをオンにします。

**ステップ 3** [Tag egress packets with service group tags] チェック ボックスをオンにします。

**ステップ 4** [Add a static secure group tag to all ingress packets] チェック ボックスをオンにします。

**ステップ 5** セキュリティ グループ タグの番号を入力します。有効な値の範囲は 2 ～ 65519 です。

**ステップ 6** [This is a trusted interface.Do not override existing secure group tags] チェック ボックスをオンにします。

**ステップ 7** [OK] をクリックして設定内容を保存します。

## IP-SGT バインディングの手動設定

IP-SGT バインディングを手動で設定するには、次の手順を実行します。

**手順**

**ステップ 1** **[Configuration]** > **[Firewall Identity by TrustSec]** を選択します。

**ステップ 2** [SGT Map Setup] 領域で [Add] をクリックするか、または SGT マップを選択して [Edit] をクリックします。

**ステップ 3** [SGT Map] ダイアログボックスで、SGT マップの IP アドレスと SGT 値を該当するフィールドに入力します。

2 ～ 65519 の SGT 番号を指定できます。

ネットワークを SGT にマップするには、[Prefix] チェックボックスをオンにして、サブネットまたは IPv6 プレフィックスを入力します。たとえば、10.100.10.0/24 をマッピングするには 24 と入力します。

**ステップ 4** [OK]、[Apply] の順にクリックし、設定を保存します。

# Cisco TrustSec に対する AnyConnect VPN のサポート

ASA は、VPN セッションのセキュリティ グループ タギングをサポートしています。外部 AAA サーバを使用するか、または、ローカル ユーザか VPN グループ ポリシーのセキュリティ グループ タグを設定することで、セキュリティ グループ タグ（SGT）を VPN セッションに割り当てることができます。さらに、レイヤ 2 イーサネット経由で、Cisco TrustSec システムを介してこのタグを伝搬することができます。AAA サーバが SGT を提供できない場合には、セキュリティ グループ タグをグループ ポリシーで利用したり、ローカル ユーザが利用したりすることができます。

次は、VPN ユーザに SGT を割り当てるための一般的なプロセスです。

1. ユーザは、ISE サーバを含む AAA サーバ グループを使用しているリモート アクセス VPN に接続します。
2. ASA が ISE に AAA 情報を要求します。この情報に SGT が含まれている場合があります。ASA は、ユーザのトンネル トラフィックに対する IP アドレスの割り当ても行います。
3. ASA が AAA 情報を使用してユーザを認証し、トンネルを作成します。
4. ASA が AAA 情報から取得した SGT と割り当て済みの IP アドレスを使用して、レイヤ 2 ヘッダー内に SGT を追加します。

5. SGT を含むパケットが Cisco TrustSec ネットワーク内の次のピア デバイスに渡されます。

AAA サーバの属性に、VPN ユーザに割り当てるための SGT が含まれていない場合、ASA はグループ ポリシーの SGT を使用します。グループ ポリシーに SGT が含まれていない場合は、タグ 0x0 が割り当てられます。

（注） また、ISE 認可変更（CoA）を使用してポリシーの適用に ISE を使用することもできます。ポリシーの適用を設定する方法については、VPN の設定ガイドを参照してください。

# リモート アクセス VPN グループ ポリシーおよびローカル ユーザへの SGT の追加

リモート アクセス VPN グループ ポリシーまたはローカル ユーザ データベースで定義されたユーザの VPN ポリシーで SGT 属性を設定するには、次の手順を実行します。

グループ ポリシーまたはローカル ユーザ用のデフォルト SGT はありません。

**手順**

**ステップ 1** リモート アクセス VPN グループ ポリシーで SGT を設定するには、次の手順を実行します。

a) **[Configuration]** > **[Remote Access VPN]** > **[Network (Client) Access]** > **[Group Policies]** の順に選択します。
b) [General] タブをクリックし、[More Options] をクリックします。
c) [Security Group Tag (STG)] フィールドに 2 ～ 65519 の範囲の値を入力します。

   SGT を設定しない場合は、[None] を選択することもできます。

d) [OK] をクリックします。

**ステップ 2** ローカル データベースでユーザ用の SGT を設定するには、次の手順を実行します。

a) **[Configuration]** > **[Remote Access VPN]** > **[AAA/Local Users]** > **[Local Users]** の順に選択します。
b) ユーザを選択して [Edit] をクリックします。
c) [VPN Policy] をクリックします。
d) [Security Group Tag (STG)] フィールドに 2 ～ 65519 の範囲の値を入力します。

   SGT を設定しない場合は、[None] を選択することもできます。

e) [OK] をクリックします。

# Cisco TrustSec のモニタリング

Cisco TrustSec の監視については、次の画面を参照してください。

- [Monitoring] > [Properties] > [Identity By TrustSec] > [SXP Connections]

  Cisco TrustSec インフラストラクチャおよび SXP コマンドの設定済みのデフォルト値を表示します。

- [Monitoring] > [Properties] > [Connections]

  セキュリティ グループ テーブル値、セキュリティ グループの名前、IP アドレスでデータが表示されるように、IP アドレス セキュリティ グループのテーブル マップ エントリをフィルタリングします。

- [Monitoring] > [Properties] > [Identity By TrustSec] > [Environment Data]

  ASA のセキュリティ グループ テーブルに含まれる Cisco TrustSec 環境情報を表示します。

- [Monitoring] > [Properties] > [Identity By TrustSec] > [IP Mapping]

  セキュリティ グループ テーブル値、セキュリティ グループの名前、IP アドレスでデータが表示されるように、IP アドレス セキュリティ グループのテーブル マップ エントリをフィルタリングします。選択したセキュリティ グループ オブジェクトが ACL で使用されている場所、もしくは別のセキュリティ グループ オブジェクトにネストされている場所を表示するには、[Where Used] をクリックします。

- [Monitoring] > [Properties] > [Identity By TrustSec] > [PAC]

  ISE から ASA にインポートされた PAC ファイルに関する情報を表示し、PAC ファイルの有効期限が切れた場合、または期限切れの 30 日以内になった場合には、警告メッセージが含まれます。

# Cisco TrustSec の履歴

表 *4 : Cisco TrustSec* の履歴

| 機能名 | プラットフォーム リリース | 説明 |
|---|---|---|
| Cisco TrustSec | 9.0(1) | Cisco TrustSec は、既存の ID 認識型インフラストラクチャを基盤とするアクセス コントロールです。ネットワーク デバイス間のデータ機密性保持を目的としており、セキュリティ アクセス サービスを 1 つのプラットフォーム上で統合します。Cisco TrustSec 機能では、実行デバイスはユーザ属性とエンドポイント属性の組み合わせを使用して、ロールベースおよびアイデンティティベースのアクセス コントロールを決定します。<br><br>このリリースでは、ASA に Cisco TrustSec が統合されており、セキュリティ グループに基づいてポリシーが適用されます。Cisco TrustSec ドメイン内のアクセス ポリシーは、トポロジには依存しません。ネットワーク IP アドレスではなく、送信元および宛先のデバイスのロールに基づいています。<br><br>ASA は、セキュリティ グループに基づくその他のタイプのポリシー（アプリケーション インスペクションなど）に対しても Cisco TrustSec を活用できます。たとえば、設定するクラス マップの中に、セキュリティ グループに基づくアクセス ポリシーを入れることができます。<br><br>次の画面が導入または変更されました。<br><br>[Configuration] > [Firewall] > [Identity By TrustSec Configuration] > [Firewall] > [Objects] > [Security Groups Object Groups Configuration] > [Firewall] > [Access Rules] > [Add Access Rules Monitoring] > [Properties] > [Identity By Tag] |
| レイヤ 2 セキュリティ グループのタグ インポジション | 9.3(1) | セキュリティ グループ タギングをイーサネット タギングと組み合わせて使用して、ポリシーを適用できるようになりました。SGT とイーサネット タギング（レイヤ 2 SGT インポジションとも呼ばれる）を利用すると、ASA でシスコ独自のイーサネット フレーミング（EtherType 0x8909）を使用して、イーサネット インターフェイスでセキュリティ グループ タグを送受信できます。これにより、送信元のセキュリティ グループ タグをプレーン テキストのイーサネット フレームに挿入できます。<br><br>次の画面が変更されました。<br><br>[Configuration] > [Device Setup] > [Interfaces] > [Add Interface] > [Advanced Configuration] > [Device Setup] > [Interfaces] > [Add Redundant Interface] > [Advanced Configuration] > [Device Setup] > [Add Ethernet Interface] > [Advanced] |

| 機能名 | プラットフォーム リリース | 説明 |
| --- | --- | --- |
| Security Exchange Protocol（SXP）バージョン 3 の Cisco TrustSec サポート。 | 9.6(1) | ASA の Cisco Trustsec は、ホスト バインディングよりも効率的な SGT とサブネット間のバインディングを可能にする SXPv3 を実装するようになりました。<br><br>**[Configuration]** > **[Firewall]** > **[Identity By TrustSec]** と [SGT Map Setup] ダイアログボックスが変更されました。 |