



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](#) (1 ページ)
- [Cisco TrustSec のガイドライン](#) (10 ページ)
- [Cisco TrustSec と統合するための ASA の設定](#) (14 ページ)
- [Cisco TrustSec の例](#) (29 ページ)
- [Cisco TrustSec に対する AnyConnect VPN のサポート](#) (29 ページ)
- [Cisco TrustSec のモニタリング](#) (31 ページ)
- [Cisco TrustSec の履歴](#) (33 ページ)

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可用性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。この情報の可用性および伝

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/c/en/us/td/topics/signosau/rdg/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/c/en/us/td/docs/enterprise-networks/tdn/ocw/229177.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/matix.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。タグging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

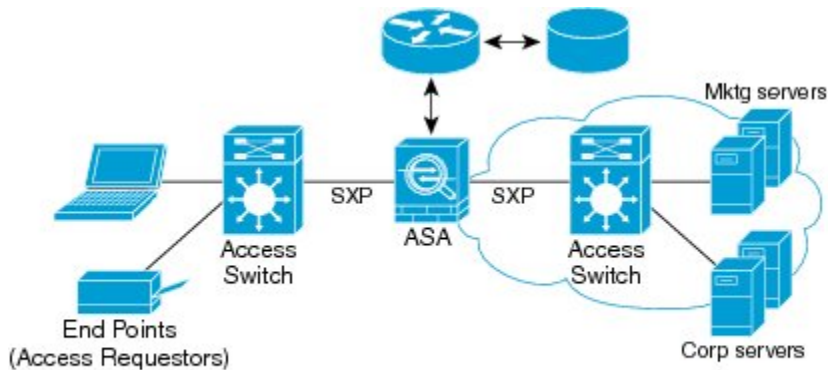
セキュリティ ポリシーの適用はセキュリティ グループの名前に基づきます。エンドポイント デバイスは、データセンターのリソースへのアクセスを試行します。ファイアウォールで設定された従来の IP ベースのポリシーと比較して、アイデンティティベースのポリシーは、ユーザおよびデバイス アイデンティティに基づいて設定されます。たとえば、mktg-contractor が mktg-server にアクセスできるとします。mktg-corp-user は、mktg-server および corp-server にアクセスできます。

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



30-4015

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。

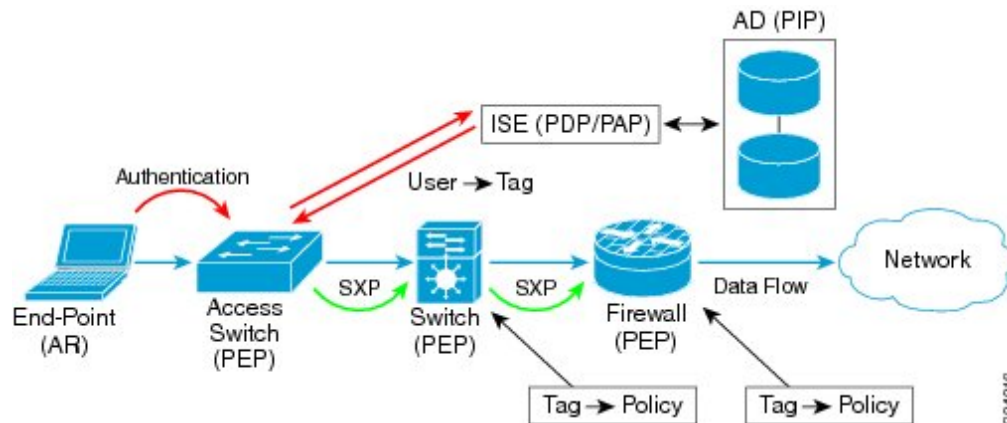
PAC ファイルを ASA にインポートすると、ISE との安全な通信チャネルが確立されます。チャネルが確立されると、ASA は、ISE を使用して PAC セキュア RADIUS トランザクションを開始し、Cisco TrustSec 環境データをダウンロードします (具体的には、セキュリティグループテーブル)。セキュリティグループテーブルによって、SGT がセキュリティグループ名にマッピングされます。セキュリティグループの名前は ISE 上で作成され、セキュリティグループをわかりやすい名前でも識別できるようになります。

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ーを順を追って調べ、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。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が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 \(16 ページ\)](#)

ステップ 3 [Security Exchange Protocol の設定 \(18 ページ\)](#)

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 \(21 ページ\)](#)

ステップ 5 [環境データの更新 \(22 ページ\)](#)

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 \(23 ページ\)](#)

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 \(24 ページ\)](#)

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 AAA サーバグループを作成し、ISE サーバと通信するように ASA の AAA サーバパラメータを設定します。

aaa-server server-tag protocol radius

例：

```
ciscoasa(config)# aaa-server ISEserver protocol radius
```

server-tag 引数には、サーバグループ名を指定します。

ステップ 2 AAA サーバグループ コンフィギュレーション モードを終了します。

exit

例：

```
ciscoasa(config-aaa-server-group)# exit
```

ステップ 3 AAA サーバを AAA サーバグループの一部として設定し、ホスト固有の接続データを設定します。

```
ciscoasa(config)# aaa-server server-tag(interface-name) host server-ip
```

例：

```
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
```

interface-name 引数には、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指定します。このパラメータにはカッコが必要です。*server-tag* 引数は、AAA サーバグループの名前です。*server-ip* 引数には、ISE サーバの IP アドレスを指定します。

ステップ 4 ISE サーバで ASA の認証に使用されるサーバ秘密値を指定します。

key key

例：

```
ciscoasa(config-aaa-server-host)# key myexclusivekey
```

key 引数は、最大 127 文字の英数字キーワードです。

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入力します。

ステップ 5 AAA サーバホスト コンフィギュレーション モードを終了します。

exit

例：

```
ciscoasa(config-aaa-server-host)# exit
```

ステップ 6 環境データ取得のために Cisco TrustSec によって使用される AAA サーバグループを識別します。

cts server-group *AAA-server-group-name*

例：

```
ciscoasa(config)# cts server-group ISEserver
```

AAA-server-group-name 引数は、ステップ 1 で *server-tag* 引数に指定した AAA サーバグループの名前です。

(注) ASA では、サーバグループの 1 つのインスタンスだけを Cisco TrustSec 用に設定できます。

次に、Cisco TrustSec との統合のために ISE サーバと通信するように ASA を設定する例を示します。

```
ciscoasa(config)#aaa-server ISEserver protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
ciscoasa(config-aaa-server-host)# key myexclusivemumblekey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# cts server-group ISEserver
```

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

Cisco TrustSec PAC ファイルをインポートします。

cts import-pac*filepath password value*

例 :

```
ciscoasa(config)# cts import-pac disk0:/xyz.pac password IDFW-pac99
```

value 引数には、PAC ファイルの暗号化に使用するパスワードを指定します。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。
filepath 引数には、次のオプションのいずれか 1 つを入力します。

シングル モード

- **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

次に、PAC ファイルを ASA にインポートする例を示します。

```
ciscoasa(config)# cts import pac disk0:/pac123.pac password hideme
PAC file successfully imported
```

次に、端末を使用して PAC ファイルを ASA にインポートする例を示します。

```
ciscoasa(config)# cts import-pac terminal password A98752a551
Enter the PAC file data in ASCII hex format
End with the word "quit" on a line by itself.
ciscoasa(exec_pac_hex)# 01002904050000010000000000000000
ciscoasa(exec_pac_hex)# 00000000000000011111111111111111
ciscoasa(exec_pac_hex)# 11111111111111112222222222222222
ciscoasa(exec_pac_hex)# 222222222222222276d7d64b6be4804b
ciscoasa(exec_pac_hex)# 0b4fdca3aeee11950ecd0e47c34157e5
ciscoasa(exec_pac_hex)# 25f4964ed75835cde0adb7e198e0bcdb
ciscoasa(exec_pac_hex)# 6aa8e363b0e4f9b4ac241be9ab576d0b
ciscoasa(exec_pac_hex)# a1fcd34e5dd05dbe1312cbfea072fdb9
ciscoasa(exec_pac_hex)# ee356fb61fe987d2d8f0ac3ef0467627
ciscoasa(exec_pac_hex)# 7f8b137da2b840e16da520468b039bae
ciscoasa(exec_pac_hex)# 36a4d844acc85cdefd7cb2cc58787590
ciscoasa(exec_pac_hex)# ef123882a69b6c37bdbc9320e403024f
ciscoasa(exec_pac_hex)# 354d42f404ec2d67ef3606575014584b
ciscoasa(exec_pac_hex)# 2796e65ccd6e6c8d14d92448a8b24f6e
ciscoasa(exec_pac_hex)# 47015a21f4f66cf6129d352bdfd4520f
ciscoasa(exec_pac_hex)# 3f0c6f340a80715df4498956efe15dec
ciscoasa(exec_pac_hex)# c08bb9a58cb6cb83ac91a3c40ce61de0
ciscoasa(exec_pac_hex)# 284b743e52fd68e848685e2d78c33633
ciscoasa(exec_pac_hex)# f2b4c5824138fc7bac9d9b83ac58ff9f
ciscoasa(exec_pac_hex)# 1dbc84c416322f1f3c5951cf2132994a
ciscoasa(exec_pac_hex)# a7cf20409df1d0d6621eba2b3af83252
ciscoasa(exec_pac_hex)# 70d0130650122bdb13a83b2dae55533a
ciscoasa(exec_pac_hex)# 4a394f21b441e164
ciscoasa(exec_pac_hex)# quit
PAC Imported Successfully
ciscoasa(config)#
```

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 ASA で 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。

```
cts sxp enable
```

例 :

```
ciscoasa(config)# cts sxp enable
```

ステップ 2 (任意。推奨されません) SXP 接続のデフォルトの送信元 IP アドレスを設定します。

```
cts sxp default source-ip ipaddress
```

例 :

```
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
```

ipaddress 引数は、IPv4 または IPv6 アドレスです。

SXP 接続のデフォルトの送信元 IP アドレスを設定する場合は、ASA 発信インターフェイスと同じアドレスを指定する必要があります。送信元 IP アドレスが発信インターフェイスのアドレスと一致しない場合、SXP 接続は失敗します。

SXP 接続の送信元 IP アドレスが設定されていない場合、ASA は、route/ARP 検索を実行して、SXP 接続用の発信インターフェイスを判別します。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 3 (任意) SXP ピアでの TCP MD5 認証のデフォルト パスワードを設定します。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。

```
cts sxp default password [0 | 8] password
```

例 :

```
ciscoasa(config)# cts sxp default password 8 IDFW-TrustSec-99
```

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。

パスワードの長さは復号レベルによって異なります。指定しない場合、デフォルトは 0 になります。

- **0** : 暗号化されていないクリアテキスト。パスワードには、最大 80 文字を指定できます。
- **8** : 暗号化テキスト。パスワードには、最大 162 文字を指定できます。

ステップ 4 (任意) ASA が SXP ピア間での新しい SXP 接続の設定を試行する時間間隔を指定します。

cts sxp retry period *timervalue*

例 :

```
ciscoasa(config)# cts sxp retry period 60
```

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 5 (任意) 調整タイマーの値を指定します。

cts sxp reconciliation period *timervalue*

例 :

```
ciscoasa(config)# cts sxp reconciliation period 60
```

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 6 (任意) SXP ピアが SXP 接続を終了した後にピアから学習した IP-SGT マッピングに削除ホールドダウンタイマーを設定します。

cts sxp delete-hold-down period *timervalue*

タイマーの値は、SXP 接続の切断から学習した IP-SGT マッピングが削除されるまで保持する秒数を 120 ~ 64000 の範囲で指定します。

例 :

```
ciscoasa(config)# cts sxp delete-hold-down period 240
```

各 SXP 接続が削除ホールドダウンタイマーに関連付けられます。このタイマーは、リスナー側の SXP 接続が切断されたときにトリガーされます。この SXP 接続から学習した IP-SGT マッピングはすぐには削除されません。その代わりに、削除ホールドダウンタイマーの有効期限が切れるまで保持されます。このタイマーの有効期限が切れると、マッピングが削除されます。

ステップ 7 (任意) 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。

cts sxp mapping network-map maximum_hosts

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せん (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。

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

SXP ピアへの SXP 接続を設定します。

```
cts sxp connection peer peer_ip_address [source source_ip_address] password {default | none} [mode {local | peer}] {speaker | listener}
```

例 :

```
ciscoasa(config)# cts sxp connection peer 192.168.1.100 password default mode peer speaker
```

SXP 接続は IP アドレスごとに設定されます。単一デバイスのペアは複数の SXP 接続に対応できます。

peer_ip_address 引数は、SXP ピアの IPv4 または IPv6 アドレスです。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。

source_ip_address 引数は、SXP 接続のローカル IPv4 または IPv6 アドレスです。送信元 IP アドレスは ASA 発信インターフェイスと同じである必要があります。そうでなければ、接続が失敗します。

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。

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。

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。

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。

次に、ASA で SXP ピアを設定する例を示します。

```
ciscoasa(config)# cts sxp connection peer 192.168.1.100 password default
mode peer speaker
ciscoasa(config)# cts sxp connection peer 192.168.1.101 password default
mode peer speaker
```

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リング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

ISE からの環境データを更新し、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。

```
cts refresh environment-data
```

例：

```
ciscoasa(config)# cts refresh environment-data
```

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。

- 拡張 ACL を設定するには、[セキュリティ グループ ベースの照合 \(Cisco TrustSec\) に使用する拡張 ACE の追加](#) 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シップは、ユーザグループメンバシップに依存しません。

次に、ローカルで定義されたセキュリティオブジェクトグループを使用する ACL を作成する例を示します。

```
object-group security objgrp-it-admin
  security-group name it-admin-sg-name
  security-group tag 1
object-group security objgrp-hr-admin
  security-group name hr-admin-sg-name // single sg_name
  group-object it-admin // locally defined object-group as nested object
object-group security objgrp-hr-servers
  security-group name hr-servers-sg-name
object-group security objgrp-hr-network
  security-group tag 2
access-list hr-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers
```

前の例で設定した ACL をアクティブにするには、アクセスグループまたはモジュラポリシーフレームワークを設定します。

その他の例：

```
!match src hr-admin-sg-name from any network to dst host 172.23.59.53
access-list idw-acl permit ip security-group name hr-admin-sg-name any host 172.23.59.53

!match src hr-admin-sg-name from host 10.1.1.1 to dst any
access-list idfw-acl permit ip security-group name hr-admin-sg-name host 10.1.1.1 any

!match src tag 22 from any network to dst hr-servers-sg-name any network
access-list idfw-acl permit ip security-group tag 22 any security-group
name hr-servers-sg-name any

!match src user mary from any host to dst hr-servers-sg-name any network
access-list idfw-acl permit ip user CSCCO\mary any security-group
name hr-servers-sg-name any

!match src objgrp-hr-admin from any network to dst objgrp-hr-servers any network
access-list idfw-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers any

!match src user Jack from objgrp-hr-network and ip subnet 10.1.1.0/24
! to dst objgrp-hr-servers any network
access-list idfw-acl permit ip user CSCCO\Jack object-group-security
objgrp-hr-network 10.1.1.0 255.255.255.0 object-group-security objgrp-hr-servers any

!match src user Tom from security-group mktg any google.com
object network net-google
fqdn google.com
access-list sgacl permit ip sec name mktg any object net-google

! If user Tom or object_group security objgrp-hr-admin needs to be matched,
! multiple ACEs can be defined as follows:
access-list idfw-acl2 permit ip user CSCCO\Tom 10.1.1.0 255.255.255.0
    object-group-security objgrp-hr-servers any
access-list idfw-acl2 permit ip object-group-security objgrp-hr-admin
    10.1.1.0 255.255.255.0 object-group-security objgrp-hr-servers any
```

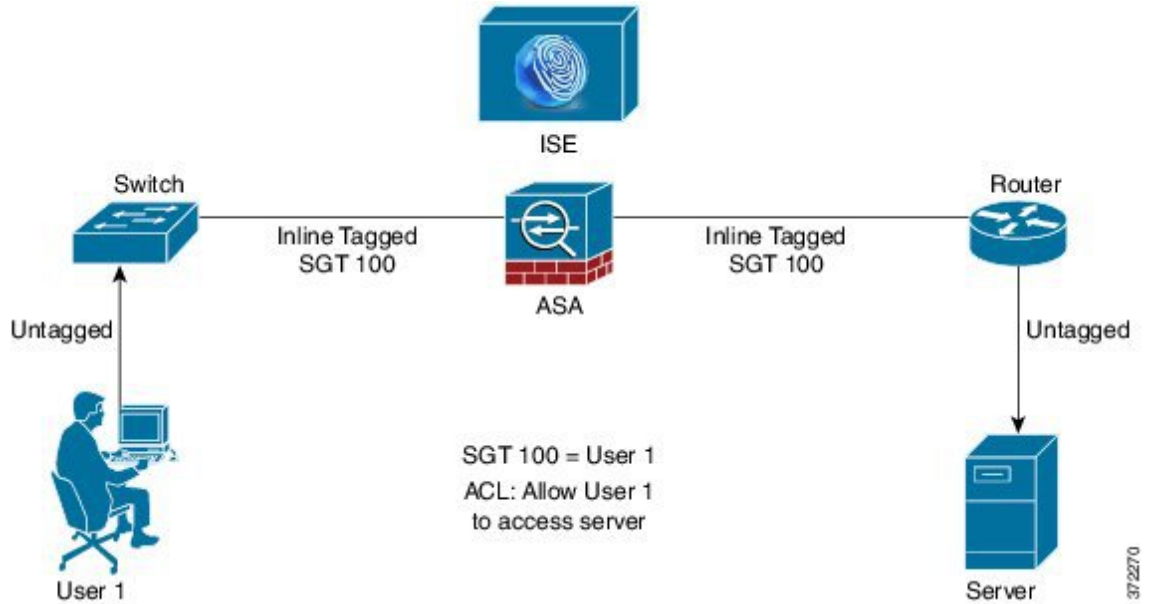
レイヤ2セキュリティグループのタギングインポジションの設定

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



37/2270

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: 入カトラフィック

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。
<code>cts manual</code> 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。
<code>cts manual</code> コマンドと <code>policy static sgt sgt_number</code> コマンドが両方とも発行される。	SGT 値が <code>policy static sgt sgt_number</code> コマンドで取得される。	SGT 値が <code>policy static sgt sgt_number</code> コマンドで取得される。
<code>cts manual</code> コマンドと <code>policy static sgt sgt_number trusted</code> 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 <code>policy static sgt sgt_number</code> 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: 出カトラフィック

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** インターフェイスを指定し、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。

interface id

例 :

```
ciscoasa(config)# interface gigabitethernet 0/0
```

- ステップ 2** レイヤ2SGTインポジションをイネーブルにし、CTS手動インターフェイスコンフィギュレーションモードを開始します。

cts manual

例 :

```
ciscoasa(config-if)# cts manual
```

- ステップ 3** インターフェイスでのセキュリティグループタグの伝播をイネーブルにします。伝播はデフォルトでイネーブルになっています。

propagate sgt

例 :

```
ciscoasa(config-if-cts-manual)# propagate sgt
```

- ステップ 4** 手動で設定された CTS リンクにポリシーを適用します。

policy static sgt sgt_number [trusted]

例 :

```
ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

static キーワードで、リンクの着信トラフィックに適用する SGT ポリシーを指定します。

sgt キーワードと *sgt_number* 引数には、ピアからの着信トラフィックに適用する SGT 値を指定します。有効な値の範囲は 2 ~ 65519 です。

trusted キーワードは、コマンドで SGT が指定されたインターフェイスの入力トラフィックでは、SGT を上書きしてはいけないことを示します。デフォルトは **untrusted** です。

次に、レイヤ2SGTインポジション用のインターフェイスをイネーブルにし、インターフェイスが信頼できるかどうかを定義する例を示します。

```
ciscoasa(config)# interface gi0/0
```

```
ciscoasa(config-if)# cts manual
ciscoasa(config-if-cts-manual)# propagate sgt
ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

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

IP-SGT バインディングを手動で設定します。

```
cts role-based sgt-map {IPv4_addr[/mask] | IPv6_addr[/prefix]} sgt sgt_value
```

例：

```
ciscoasa(config)# cts role-based sgt-map 10.2.1.2 sgt 50
```

IPv4 または IPv6 ホスト アドレスを指定できます。また、10.100.10.0/24 のようなサブネットマスクまたはプレフィックス値 (IPv6 の場合) を含めることで、ネットワーク アドレスを指定することもできます。sgt_value は SGT 番号で、2 ~ 65519 の範囲です。

トラブルシューティングのヒント

特定のセッションが許可または拒否された理由、使用されている SGT 値 (パケットの SGT 値、IP-SGT マネージャから取得した SGT 値、またはインターフェイスで設定した **policy static sgt** コマンドで取得した SGT 値)、および適用されたセキュリティグループベースのセキュリティポリシーを確認するには、**packet-tracer** コマンドを使用します。

次に、**packet-tracer** コマンドの出力例を示します。この出力から、セキュリティグループタグと IP アドレスの対応付けがわかります。

```
ciscoasa# packet-tracer input inside tcp inline-tag 100
security-group name alpha 30 security-group tag 31 300
Mapping security-group 30:alpha to IP address 10.1.1.2.
Mapping security-group 31:bravo to IP address 192.168.1.2.

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 192.168.1.0 255.255.255.0 outside...
-----More-----
```

特定の SGT 値を指定するかどうかにかかわらず、Cisco CMD パケット (EtherType 0x8909) のみをキャプチャするには、**capture capture-name type inline-tag tag** コマンドを使用します。

次に、SGT 値を指定した場合の **show capture** コマンドの出力例を示します。

```
ciscoasa# show capture my-inside-capture
1: 11:34:42.931012 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
2: 11:34:42.931470 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply
3: 11:34:43.932553 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
4: 11.34.43.933164 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply
```

Cisco TrustSec の例

次に、Cisco TrustSec を使用するように ASA を設定する方法の例を示します。

```
// Import an encrypted CTS PAC file
cts import-pac asa.pac password Cisco
// Configure ISE for environment data download
aaa-server cts-server-list protocol radius
aaa-server cts-server-list host 10.1.1.100 cisco123
cts server-group cts-server-list
// Configure SXP peers
cts sxp enable
cts sxp connection peer 192.168.1.100 password default mode peer speaker
//Configure security-group based policies
object-group security objgrp-it-admin
  security-group name it-admin-sg-name
  security-group tag 1
object-group security objgrp-hr-admin
security-group name hr-admin-sg-name
group-object it-admin
object-group security objgrp-hr-servers
security-group name hr-servers-sg-name
access-list hr-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers
//Configure security group tagging plus Ethernet tagging
interface gi0/1
  cts manual
  propagate sgt
  policy static sgt 100 trusted
  cts role-based sgt-map 10.1.1.100 sgt 50
```

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グging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、ローカルユーザが 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) グループポリシー コンフィギュレーションモードを開始します。

group-policy name

例 :

```
ciscoasa(config)# group policy Grpolicy1
```

- b) グループポリシー用の SGT を設定します。

security-group-tag {none | value sgt}

value を使用してタグを設定する場合、タグは 2 ~ 65519 の範囲で指定できます。SGT を設定しない場合は **none** を指定します。

例 :

```
ciscoasa(config-group-policy)# security-group-tag value 101
```

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) 必要に応じて、ユーザを作成します。

```
username name {nopassword | password password [encrypted]} [privilege priv_level]}
```

例 :

```
ciscoasa(config)# username newuser password changeme encrypted privilege 15
```

- b) ユーザ名コンフィギュレーションモードを開始します。

```
username name attributes
```

例 :

```
asa3(config)# username newuser attributes
asa3(config-username)#
```

- c) ユーザ用の SGT を設定します。

```
security-group-tag {none | value sgt}
```

value を使用してタグを設定する場合、タグは 2 ~ 65519 の範囲で指定できます。SGT を設定しない場合は **none** を指定します。

例 :

```
ciscoasa(config-username)# security-group-tag value 101
```

Cisco TrustSec のモニタリング

Cisco TrustSec の監視については、次のコマンドを参照してください。

- **show running-config cts**
- **show running-config [all] cts role-based [sgt-map]**
このコマンドは、ユーザ定義の IP-SGT バインディングテーブルエントリを表示します。
- **show cts sxp connections**
このコマンドでは、マルチ コンテキスト モードが使用されると、特定のユーザ コンテキストの ASA の SXP 接続が表示されます。
- **show conn security-group**

すべての SXP 接続のデータを表示します。

- **show cts 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。

- **show cts sgt-map**

制御パスの IP アドレス セキュリティ グループ テーブル マネージャ エントリを表示します。

- **show asp table cts sgt-map**

このコマンドは、データ パスに保持されている IP アドレス セキュリティ グループのテーブル マップ データベースから IP アドレス セキュリティ グループのテーブル マップ エントリを表示します。

- **show cts 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)	<p>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。</p> <p>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。</p> <p>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。</p> <p>access-list extended、cts sxp enable、cts server-group、cts sxp default、cts sxp retry period、cts sxp reconciliation period、cts sxp connection peer、cts import-pac、cts refresh environment-data、object-group security、security-group、show running-config cts、show running-config object-group、clear configure cts、clear configure object-group、show cts pac、show cts environment-data、show cts environment-data sg-table、show cts sxp connections、show object-group、show configure security-group、clear cts environment-data、debug cts、packet-tracer の各コマンドが導入または変更されました。</p>

機能名	プラットフォーム リリース	説明
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)	<p>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。</p> <p>cts manual、policy static sgt、propagate sgt、cts role-based sgt-map、show cts sgt-map、packet-tracer、capture、show capture、show asp drop、show asp table classify、show running-config all、clear configure all、および write memory の各コマンドが導入または変更されました。</p>
Security Exchange Protocol (SXP) バージョン 3 の Cisco TrustSec サポート。	9.6(1)	<p>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。</p> <p>cts sxp mapping network-map、cts role-based sgt-map、show cts sgt-map、show cts sxp sgt-map、show asp table cts sgt-map の各コマンドが導入または変更されました。</p>
Trustsec SXP 接続の設定可能な削除ホールドダウン タイマー	9.8(3)	<p>デフォルトの SXP 接続ホールドダウン タイマーは 120 秒です。このタイマーを 120 ~ 64000 秒に設定できるようになりました。</p> <p>新規/変更されたコマンド：cts sxp delete-hold-down period、show cts sxp connection brief、show cts sxp connections</p>