CHAPTER 34

Cisco TrustSec と統合するための ASA の設定

この章の内容は、次のとおりです。

Cisco TrustSec と統合された ASA に関する情報

この項では、次のトピックについて取り上げます。

Cisco TrustSec の概要

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、コンピュータのネットワークにおける、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などでのセキュリティ ソリューションをイネーブルにするために、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 ソリューションです。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 ソリューションでは、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 ソリューションが可能となります。

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。

Cisco TrustSec の詳細については、http://www.cisco.com/go/trustsec を参照してください。

Cisco TrustSec の SGT および SXP サポートについて

Cisco TrustSec ソリューションでは、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（RBACL）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 は接続を開始するときに既知の 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 ソリューションのロール

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 ソリューションには、次の機能があります。

- **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のデバイスです。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 ソリューションでは、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、ユーザ アイデンティティ マッピングおよびサーバ リソース マッピングに Cisco TrustSec タグを提供することによって、アイデンティティ リポジトリとして機能します。

  Cisco TrustSec ソリューションでは、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。

ASA は、アイデンティティ アーキテクチャで 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、こ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。

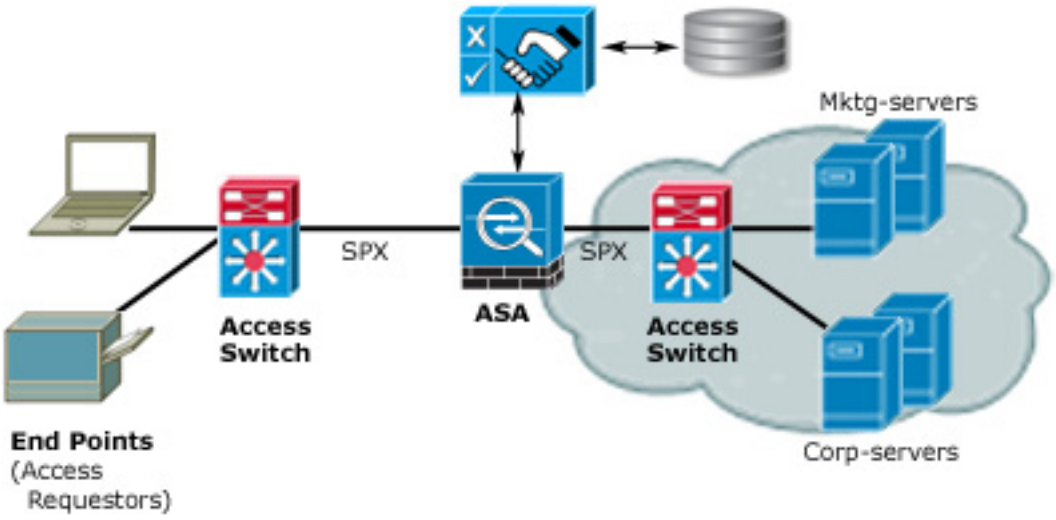
セキュリティ グループ ポリシーの適用

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。

このタイプの導入の利点を次に示します。

- 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。

図 34-1　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、サーバの分割をサポートするセキュリティ ポリシーを設定できます。

- 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。ネットワークの組み合わせでは、ユーザベースの属性とセキュリティグループ ベースの属性をセキュリティ ポリシーで設定できます。ユーザベースのセキュリティ ポリシーの設定については、第 33 章「アイデンティティ ファイアウォールの設定」を参照してください。

ASA を Cisco TrustSec で機能するように設定する一環として、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。「Protected Access Credential（PAC）ファイルのインポート」（P.34-13）。

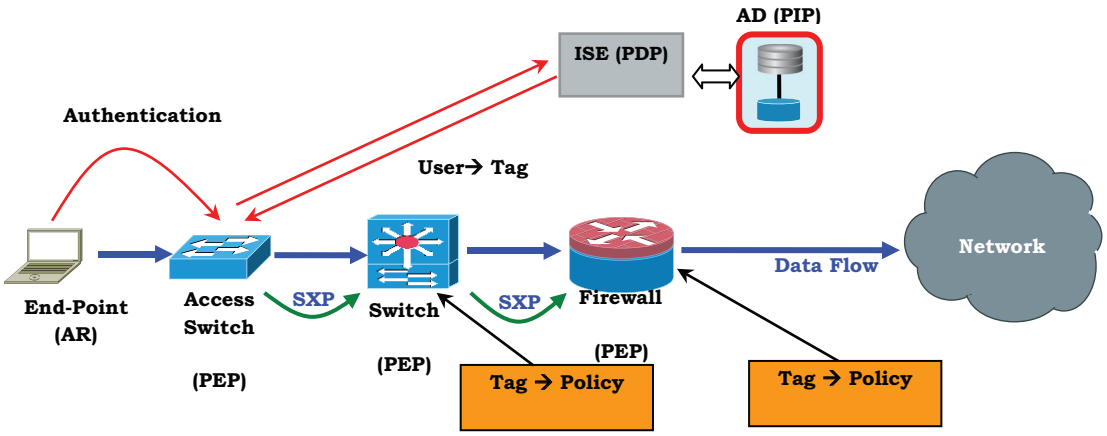
PAC ファイルを ASA にインポートすると、ISE との安全な通信チャネルが確立されます。チャネルが確立されると、ASA は、ISE を使用して PAC セキュア RADIUS トランザクションを開始し、Cisco TrustSec 環境データをダウンロードします。具体的には、ASA は、セキュリティ グループ テーブルを

ダウンロードします。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、ASA 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 は、セキュリティ グループの名前を解決できない場合、未知のセキュリティ グループ名に関するシステム ログ 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 34-2　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 がパケットを受信します。SXP によって渡された IP-SGT マッピングを使用して、ASA は SGT で送信元および宛先 IP アドレスを検索します。

   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 マッピングには、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 マッピングを送信します。「ASA での送信者および受信者のロール」（P.34-6）を参照してください。
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、システム ログ メッセージを生成します。ASA が ISE からセキュリティ グループ テーブルをリフレッシュした後にこの名前が既知になった場合、ASA は、セキュリティ グループの名前が既知であることを示すシステム ログ メッセージを生成します。

ASA での送信者および受信者のロール

では、SXP の他のネットワーク デバイスとの間の IP-SGT マッピングの送受信がサポートされます。ASASXP 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 マッピングを受信し、ポリシー定義の作成で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 はシステム ログ メッセージを生成します。

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。ASA

での SXP の設定の一部として、SXP 調整タイマーを設定します。ASASXP 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。受信者デバイスとして指定された SXP ピアのみが接続を終了できます。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、IP-SGT 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。

ASA-Cisco TrustSec 統合の機能

ASA は、アイデンティティベースのファイアウォール機能の一部として Cisco TrustSec を利用します。Cisco TrustSec と ASA を統合すると、次の主要な機能が提供されます。

柔軟性

- 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。

  「ASA での送信者および受信者のロール」（P.34-6）を参照してください。
- 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。
- 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。ASASXP バージョン ネゴシエーションによって、バージョンのスタティック コンフィギュレーションが不要になります。

- 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 テーブルをリフレッシュするように 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。
- ASA では、送信元フィールドまたは宛先フィールド、あるいはその両方のセキュリティ グループの名前に基づくセキュリティ ポリシーがサポートされます。セキュリティ グループ、IP アドレス、Active Directory グループ/ユーザ名、および FQDN の組み合わせに基づいて ASA のセキュリティ ポリシーを設定できます。

可用性

- 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 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。
- 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 は、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。

拡張性

ASA では、次の数の IP-SGT マッピング エントリがサポートされます。

表 34-1　IP-SGT マッピングの許容数

ASA プラットフォーム	IP-SGT マッピング エントリの数
5505	250
5510	1000
5520	2500
5540	5000
5550	7500
5580-20	10,000
5580-40	20,000
5585-X（SSP-10）	18,750
5585-X（SSP-20）	25,000
5585-X（SSP-40）	50,000
5585-X（SSP-60）	100,000

ASA では、次の数の SXP 接続がサポートされます。

表 34-2　SXP 接続

ASA プラットフォーム	SXP TCP 接続の数
5505	10
5510	25
5520	50
5540	100
5550	150

表 34-2　SXP 接続 （続き）

ASA プラットフォーム	SXP TCP 接続の数
5580-20	250
5580-40	500
5585-X（SSP-10）	150
5585-X（SSP-20）	250
5585-X（SSP-40）	500
5585-X（SSP-60）	1000

Cisco TrustSec と ASA を統合した場合のライセンス要件

モデル	ライセンス要件
すべてのモデル	基本ライセンス

Cisco TrustSec と ASA を統合するための前提条件

Cisco TrustSec と統合するように ASA を設定する前に、次の前提条件を満たす必要があります。

- ISE に ASA を登録します。
- ISE で ASA のセキュリティ グループを作成します。
- ASA にインポートする PAC ファイルを ISE で生成します。

ASA の ISE への登録

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。

1. ISE にログインします。
2. [Administration] > [Network Devices] > [Network Devices] を選択します。
3. [Add] をクリックします。
4. ASA の IP アドレスを入力します。
5. ISE が Cisco TrustSec ソリューションでユーザ認証に使用されている場合は、[Authentication Settings] エリア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。
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。これらのタスクを実行する方法の詳細については、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。

1. ISE にログインします。
2. [Policy] > [Policy Elements] > [Results] > [Security Group Access] > [Security Group] を選択します。
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。
4. [Security Group Access] セクションで、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 ファイルについては、「Protected Access Credential（PAC）ファイルのインポート」（P.34-13）を参照してください。

PAC ファイルを生成する前に、ISE に ASA を登録する必要があります。

1. ISE にログインします。
2. [Administration] > [Network Resources] > [Network Devices] を選択します。
3. デバイスのリストから、ASA デバイスを選択します。
4. [Security Group Access (SGA)] で、[Generate PAC] をクリックします。
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、または SMB を介してリモート サーバから PAC をインポートできます （PAC 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）。

注意事項と制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。

クラスタリングのガイドライン

クラスタリング設定のマスター デバイスだけでサポートされます。

ハイ アベイラビリティのガイドライン

設定によってサーバのリストをサポートします。最初のサーバが到達不能の場合、ASA は、リストの 2 番目以降のサーバに順番に接続を試みます。ただし、Cisco TrustSec 環境データの一部としてダウンロードされたサーバ リストは無視されます。

制限事項

- 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 スイッチが適用ポイントと異なる NAT ドメインに属する場合、アップロードする IP-SGT マップは無効であり、実行デバイスでの IP-SGT マッピング データベース検索は有効な結果を得ることができません。したがって、ASA は、実行デバイスのセキュリティ グループの認識セキュリティ ポリシーを適用できません。
- Cisco TrustSec と統合するように ASA を設定する場合は、ASA のデフォルトのパスワードを設定して、SXP 接続に使用するか、またはパスワードを使用しないように選択できます。ただし、接続固有のパスワードは 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で一貫している必要があります。
- 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-DGT 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。同様に、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 ファイルについては、「PAC ファイルの生成」（P.34-9）および 「Protected Access Credential（PAC）ファイルのインポート」（P.34-13）を参照してください。
- 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。
- 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システム ログ メッセージを生成します。

  ISE の変更を反映するために、ASA でセキュリティ グループ テーブルを手動で更新する方法については、「環境データのリフレッシュ」（P.34-20）を参照してください。
- 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 ピア A）- - - - - -（ASA）-（SXP ピア 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、ASA で、非 NAT、非 SEQ-RAND、および 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。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 TCP 状態バイパス ポリシーの設定例に示すように ASA を設定します。

```
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

ここでは、次の内容について説明します。

Cisco TrustSec と統合するための ASA の設定のタスク フロー

前提条件

Cisco TrustSec と統合するように ASA を設定する前に、次の前提条件を満たす必要があります。

- ISE に ASA を登録します。
- ASA にインポートする PAC ファイルを ISE で生成します。

詳細については、「Cisco TrustSec と ASA を統合するための前提条件」（P.34-8）を参照してください。

ASA でのタスク フロー

Cisco TrustSec と統合するように ASA を設定するには、次の作業を実行します。

ステップ 1　AAA サーバを設定します。

「Cisco TrustSec と統合するための AAA サーバの設定」（P.34-12）を参照してください。

ステップ 2　ISE から PAC ファイルをインポートします。

「Protected Access Credential（PAC）ファイルのインポート」（P.34-13）を参照してください。

ステップ 3　SXP のデフォルト値をイネーブルにし、設定します。

「Security Exchange Protocol（SXP）の設定」（P.34-15）を参照してください。

ステップ 4　Cisco TrustSec アーキテクチャの SXP 接続ピアを追加します。

「SXP 接続のピアの追加」（P.34-18）を参照してください。

ステップ 5　必要に応じて、Cisco TrustSec と統合された ASA の環境データをリフレッシュします。

「環境データのリフレッシュ」（P.34-20）を参照してください。

ステップ 6　セキュリティ ポリシーを設定します。

「セキュリティ ポリシーの設定」（P.34-21）を参照してください。

Cisco TrustSec と統合するための AAA サーバの設定

Cisco TrustSec と統合するための ASA の設定の一環として、ISE と通信できるように ASA を設定する必要があります。

詳細については、「AAA サーバ グループの設定」（P.32-11）も参照してください。

前提条件

- 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、機能の設定は失敗します。
- 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。この情報が不明な場合は、ISE 管理者にお問い合わせください。

ASA で ISE の 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。

	コマンド	目的

ステップ 1	`hostname(config)# aaa-server server-tag protocol radius`
	Example:
	`hostname(config)# aaa-server ISEserver protocol radius`
		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。
		server-tag はサーバ グループ名を指定します。
		詳細については、「ISE でのセキュリティ グループの作成」（P.34-8）を参照してください。

ステップ 2	`hostname(config-aaa-server-group)# exit`	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。

	コマンド	目的
ステップ 3	hostname(config)# **aaa-server** *server-tag* (*interface-name*) **host** *server-ip* **Example:** hostname(config)# aaa-server ISEserver (inside) host 192.0.2.1	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。 (*interface-name*) 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* 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。 *server-ip* は、ISE サーバの IP アドレスを指定します。
ステップ 4	hostname(config-aaa-server-host)# **key** *key* **Example:** hostname(config-aaa-server-host)# key myexclusivemumblekey	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* 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。 詳細については、「ASA の ISE への登録」（P.34-8）を参照してください。
ステップ 5	hostname(config-aaa-server-host)# **exit**	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。
ステップ 6	hostname(config)# **cts server-group** *AAA-server-group-name* **Example:** hostname(config)# cts server-group ISEserver	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。 *AAA-server-group-name* 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。 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。

例

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。

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

Protected Access Credential（PAC）ファイルのインポート

PAC ファイルを ASA にインポートすると、ISE との接続が確立されます。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、ASA は、セキュリティ グループ テーブルをダウンロードします。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。

具体的には、チャネルは RADIUS トランザクションの前には確立されません。ASA は、認証用の PAC を使用して ISE の RADIUS トランザクションを開始します。

ヒント　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。このキーは、その機密性により、ASA に安全に保存する必要があります。

ファイルの正常なインポート後に、ASA は、ISE で設定されたデバイスのパスワードを要求せずに、ISE から Cisco TrustSec 環境データをダウンロードします。

前提条件

- 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。ASA は、任意の PAC ファイルをインポートできますが、PAC ファイルは、正しく設定された ISE によって生成された場合にのみ ASA で動作します。「ASA の ISE への登録」（P.34-8）を参照してください。
- 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。
- ISE で生成された PAC ファイルにアクセスします。ASA は、フラッシュ、または TFTP、FTP、HTTP、HTTPS、または SMB を介してリモート サーバから PAC をインポートできます （PAC 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。

制約事項

- ASA が HA 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。
- ASA がクラスタリング設定の一部である場合、マスター デバイスに PAC をインポートする必要があります。

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。

	コマンド	目的
ステップ 1	hostname(config)# **cts import-pac** *filepath* **password** *value* **Example:** hostname(config)# cts import-pac disk0:/xyz.pac password IDFW-pac99	Cisco TrustSec PAC ファイルをインポートします。 *filepath* には、次の **EXEC** モード コマンドおよび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 *value* 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。

例

次に、PAC ファイルを ASA にインポートする例を示します。

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

Security Exchange Protocol（SXP）の設定

Security Exchange Protocol（SXP）の設定では、ASA のプロトコルをイネーブルにし、次の SXP のデフォルト値を設定します。

- SXP 接続の送信元 IP アドレス
- SXP ピア間の認証パスワード
- SXP 接続の再試行間隔
- Cisco TrustSec SXP 調整期間

SXP を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`hostname(config)# cts sxp enable`	必要に応じて、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。 マルチ コンテキスト モードでは、SXP のイネーブル化はユーザ コンテキストで実行されます。
ステップ 2	`hostname(config)# cts sxp default source-ip` *ipaddress* **Example:** `hostname(config)# cts sxp default source-ip 192.168.1.100`	SXP 接続のデフォルトの送信元 IP アドレスを設定します。 *ipaddress* 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。すべての SXP 接続用のデフォルトの送信元 IP アドレスの設定については、「SXP 接続のピアの追加」（P.34-18）を参照してください。
ステップ 3	`hostname(config)# cts sxp default password [0 | 8]` *password* **Example:** `hostname(config)# cts sxp default password 8 IDFW-TrustSec-99`	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。 パスワードの暗号化レベルの設定は任意です。暗号化レベルを設定する場合、設定できるレベルは 1 つのみです。 • レベル 0：暗号化されていないクリア テキスト • レベル 8：暗号化テキスト *password* は 162 文字までの暗号化された文字列または 80 文字までの ASCII キー ストリングを指定します。

	コマンド	目的
ステップ 4	hostname(config)# **cts sxp retry period** *timervalue* **Example:** hostname(config)# cts sxp retry period 60	ASA が SXP ピア間での新しい SXP 接続の設定を試行するデフォルトの時間間隔を指定します。ASA は、成功した接続が確立されるまで接続を試み続けます。 ASA で確立されていない SXP 接続が存在する限り、再試行タイマーがトリガーされます。 *timervalue* は 0 ～ 64000 秒の範囲の秒数です。 0 秒を指定すると、タイマーの期限が切れず、ASA は SXP ピアへの接続を試行しません。 デフォルトでは、*timervalue* は 120 秒です。 再試行タイマーが期限切れになると、ASA は接続データベースを順に検索し、データベースに切断されているか、または「保留中」状態の接続が含まれている場合、ASA は、再試行タイマーを再開します。 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	hostname(config)# **cts sxp reconciliation period** *timervalue* **Example:** hostname(config)# cts sxp reconciliation period 60	デフォルトの調整タイマーの値を指定します。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。 *timervalue* は 1 ～ 64000 秒の範囲の秒数です。 デフォルトでは、*timervalue* は 120 秒です。 0 を指定すると調整タイマーが開始されないため、このタイマーには 0 を指定できません。調整タイマーを実行できないようにすると、未定義の時間の古いエントリが維持され、ポリシーの適用の結果が予期せぬものとなります。

例

次に、SXP のデフォルト値を設定する例を示します。

```
hostname(config)# cts sxp enable
hostname(config)# cts sxp default source-ip 192.168.1.100
hostname(config)# cts sxp default password 8 ********
hostname(config)# cts sxp retry period 60
hostname(config)# cts sxp reconcile period 60
```

SXP 接続のピアの追加

ピア間の 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 接続のピアを追加するには、次の手順を実行します。

	コマンド	目的
ステップ 1	hostname(config)# **cts sxp enable**	必要に応じて、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。
ステップ 2	hostname(config)# **cts sxp connection peer** *peer_ip_address* [**source** *source_ip_address*] **password** {**default**|**none**} [**mode** {**local**|**peer**}] {**speaker**|**listener**} **Example:** hostname(config)# cts sxp connection peer 192.168.1.100 password default mode peer speaker	SXP ピアへの SXP 接続を設定します。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。 **ピア IP アドレス（必須）** *peer_ip_address* 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。 **送信元 IP アドレス（任意）** *source_ip_address* 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。 **パスワード（必須）** 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。「Security Exchange Protocol（SXP）の設定」（P.34-15）を参照してください。 • **none**：SXP 接続にパスワードを使用しません。 **モード（任意）** 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。 **ロール（必須）** 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。「ASA での送信者および受信者のロール」（P.34-6）を参照してください。 • **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。

例

次に、ASA で SXP ピアを設定する例を示します。

```
hostname(config)# cts sxp enable
hostname(config)# cts sxp connection peer 192.168.1.100 password default mode peer speaker
hostname(config)# cts sxp connection peer 192.168.1.101 password default mode peer
hostname(config)# no cts sxp connection peer 192.168.1.100
hostname(config)# cts sxp connection peer 192.168.1.100 source 192.168.1.1 password default mode peer speaker
hostname(config)# no cts sxp connection peer 192.168.1.100 source 192.168.1.1 password default mode peer
speaker
```

環境データのリフレッシュ

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。これらの変更は、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 ASA には反映されません。ASA でデータをリフレッシュして、ISE 上で作成されたセキュリティ グループが ASA に反映されるようにします。

ヒント　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。

前提条件

Cisco TrustSec の変更が ASA に適用されるように、ASA は、ISE の認識された Cisco TrustSec ネットワークとして設定される必要があり、ASA は PAC ファイルを正常にインポートする必要があります。

制約事項

- ASA が HA 設定の一部である場合、プライマリ ASA デバイスで環境データをリフレッシュ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 デバイスで環境データをリフレッシュする必要があります。

環境データのリフレッシュ

ASA で、次のコマンドを入力します。

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

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

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 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るようになりました。

- 拡張 ACL を設定するには、第 19 章「拡張アクセス コントロール リストの追加」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には、「ローカル ユーザ グループの設定」（P.17-11）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。TrustSec を使用して、セキュリティ グループに基づいてアクセスを制御できるようになりました。ファイアウォール コンフィギュレーション ガイドの Chapter 6, “Configuring Access Rules,” を参照してください。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。

例

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
```

上記で設定される ACL は、アクセス グループまたは MPF を設定することによってアクティブ化できます。

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 CSCO\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 CSCO\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 CSCO\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
```

設定例

次に、ASA と Cisco TrustSec の完全な統合を実行するための設定例を示します。

```
// 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
```

Cisco TrustSec と統合された ASA のモニタリング

ここでは、次の内容について説明します。

ASA の Cisco TrustSec 設定の表示

構文：

show running-config cts

説明：

Cisco TrustSec SXP インフラストラクチャおよび SXP コマンドの設定済みデフォルト値を表示するには、**show running-config cts** コマンドを指定します。

出力：

次に、基本的な Cisco TrustSec の設定例を示します。

```
hostname# show running-config cts
!
cts server-group ctsgroup
!
cts sxp enable
cts sxp connection peer 192.16.1.1 password none mode speaker
```

次に、デフォルトの設定を含む Cisco TrustSec の設定例を示します。

```
hostname# show running-config all cts
!
cts server-group ctsgroup
!
no cts sxp enable
no cts sxp default password
cts sxp retry period 120
cts sxp reconcile period 120
```

SXP 接続のモニタリング

構文：

show cts sxp connections [**peer** *peer_addr*] [**local** *local_addr*] [**ipv4**|**ipv6**] [**status** {**on**|**off**|**delete-hold-down**|**pending-on**}] [**mode** {**speaker**|**listener**}] [**brief**]

説明：

どの SXP 接続が稼働中であるかを確認するには、このコマンドを使用します。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。

peer *peer_addr*	一致したピア IP アドレスとの接続だけが表示されます。
local *local_addr*	一致したローカル IP アドレスとの接続だけが表示されます。
ipv4	IPv4 接続だけが表示されます。
ipv6	IPv6 接続だけが表示されます。
status	一致したステータスの接続だけが表示されます。

mode　　一致したモードの接続だけが表示されます。

brief　　接続の要約だけが表示されます。

または **security-group** キーワードを指定した **show connection** コマンドを使用して、SXP 接続情報を表示することもできます。

```
show connection [security-group [tag <sgt#> | name <sg_name>]...]
```

この **show connection** コマンドは、**security-group** キーワードが含まれている場合に SXP 接続のデータを表示します。特定の接続に関する情報を表示するには、接続元および宛先の両方の SGT 値またはセキュリティ グループ名を指定する **security-group** キーワードを含めます。ASA は、特定の SGT 値またはセキュリティ グループ名と一致する接続を表示します。

送信元および宛先 SGT 値または送信元および宛先セキュリティ グループ名を指定せずに **security-group** キーワードを指定すると、ASA は、すべての SXP 接続のデータを表示します。

ASA は、接続データを *security_group_name* (*SGT_value*) の形式で表示するか、またはセキュリティ グループ名が不明な場合は単に *SGT_value* として表示します。

（注） スタブ接続が低速パスを通過しないため、セキュリティ グループ データはスタブ接続には使用できません。スタブ接続には、接続の所有者にパケットを転送するために必要な情報だけが保持されます。

単一のセキュリティ グループの名前を指定して、クラスタ内のすべての接続を表示できます。たとえば、次の例では、クラスタのすべてのユニットのセキュリティ グループ mktg に一致する接続が表示されます。

```
hostname# show cluster conn security-group name mktg
...
```

出力

次に、ASA でイネーブルになっている SXP 接続のサマリー例を示します。

```
hostname# show cts sxp connection brief
SXP                : Enabled
Highest version    : 2
Default password   : Set
Default local IP   : Not Set
Reconcile period   : 120 secs
Retry open period : 10 secs
Retry open timer   : Not Running
Total number of SXP connections : 2
-------------------------------------------------------------------------------
Peer IP          Local IP         Conn Status       Duration (dd:hr:mm:sec)
-------------------------------------------------------------------------------
2.2.2.1          2.2.2.2          On                0:00:02:14
3.3.3.1          3.3.3.2          On                0:00:02:14
-------------------------------------------------------------------------------------------------
Peer IP                    Local IP                   Conn Status       Duration
(dd:hr:mm:sec)
-------------------------------------------------------------------------------------------------
1234::A8BB:CCFF:FE00:1101  1234::A8BB:CCFF:FE00:2202  On 0:00:02:14
```

次に、ASA でイネーブルになっている各 SXP 接続の詳細情報の例を示します。

```
hostname# show cts sxp connections
SXP                : Enabled
```

```
Highest version   : 2
Default password  : Set
Default local IP  : Not Set
Reconcile period  : 120 secs
Retry open period : 10 secs
Retry open timer  : Not Running
Total number of SXP connections : 2
------------------------------------------------------------
Peer IP           : 2.2.2.1
Local IP          : 2.2.2.2
Conn status       : Delete Hold Down
Local mode        : Listener
Ins number        : 3
TCP conn password : Set
Delete hold down timer : Running
Reconciliation timer   : Not Running
Duration since last state change: 0:00:00:16 (dd:hr:mm:sec)
------------------------------------------------------------
Peer IP           : 3.3.3.1
Local IP          : 3.3.3.2
Conn status       : On
Local mode        : Listener
Ins number        : 2
TCP conn password : Default
Delete hold down timer : Not Running
Reconciliation timer   : Not Running
Duration since last state change: 0:00:05:49 (dd:hr:mm:sec)
```

次に、すべての SXP 接続のデータの表示例を示します。

```
hostname# show connection security-group
100 in use, 90 most used
TCP inside (security-group mktg(3)) 10.1.1.1:2000 outside (security-group 111)
172.23.59.53:21, idle 0:00:00, bytes 10, flags ...
TCP inside (security-group mktg(3)) 10.1.1.1:2010 outside (security-group 222)
172.23.59.53:21, idle 0:00:00, bytes 10, flags ...
...
```

次に、送信元および宛先の特定の SGT 値と一致する SXP 接続の表示例を示します。

```
hostname# show connection security-group tag 3 security-group tag 111
1 in use
TCP inside (security-group mktg(3)) 10.1.1.1:2000 outside (security-group 111)
172.23.59.53:21, idle 0:00:00, bytes 10, flags ...
```

環境データのモニタリング

構文：

show cts sxp connections security-group-table [**sgt** *value* | **name** *name-value*]

説明：

このコマンドは、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。この情報には、有効期間およびセキュリティ グループ名テーブルが含まれます。セキュリティ グループ テーブルには、PAC ファイルをインポートするときに ISE のデータが移入されます。

SGT またはセキュリティ グループの名前を指定して、表示する特定のテーブル エントリを選択できます。セキュリティ グループには、1 つの名前が割り当てられています。同じ名前は単一の SGT にしか関連付けることができません。

sgt *value*	特定の SGT 値と一致するセキュリティ グループ名の環境データを表示します。*value* は 1 ～ 65533 の数値です。
name *name-value*	指定するセキュリティ グループ名の環境データを表示します。*name-value* は 32 バイトの大文字と小文字が区別される文字列です。

SGT または名前を指定しない場合、ASA は、セキュリティ グループ テーブルに含まれるすべての環境データを表示します。

エントリに「reserved」が含まれている場合は、予約された範囲から SGT が割り当てられています。

出力：

次に、ASA が PAC ファイルをインポートできない場合に表示される環境データの例を示します。

```
hostname# show cts environment-data
CTS Environment Data
====================
Status:                    Expired
Last download attempt:     Failed
Retry_timer (60 secs) is running
```

次に、ASA が PAC ファイルを正常にインポートした場合に表示される環境データの例を示します。

```
hostname# show cts environment-data
CTS Environment Data
====================
Status:                    Active
Last download attempt:     Successful
Environment Data Lifetime: 1036800 secs
Last update time:          16:43:39 EDT May 5 2011
Env-data expires in        11:01:18:27 (dd:hr:mm:sec)
Env-data refreshes in      11:01:08:27 (dd:hr:mm:sec)
```

次に、セキュリティ グループ テーブルに含まれている環境データの例を示します。

```
hostname# show cts environment-data sg-table
Valid until: 04:16:29 EST Feb 16 2012
Total number of entries: 4
Number of entries shown: 4

SG Name     SG Tag  Type
-------     -------------
Marketing   1       unicast
Engineering123      unicast (reserved)
Finance     44      multicast
Payroll     54321   multicast (reserved)
```

Cisco TrustSec IP-SGT マッピングのモニタリング

ここでは、Cisco TrustSec IP-SGT マッピングのモニタリングに関する次の項目について説明します。

- 「コントロール プレーンの IP-SGT マネージャ エントリの表示」（P.34-27）
- 「SXP によって学習された IP-SGT マッピングの表示」（P.34-28）
- 「データパスの IP-SGT マッピング データベースの表示」（P.34-29）

コントロール プレーンの IP-SGT マネージャ エントリの表示

構文：

show cts sgt-map [**address** *ip_address*|[**ipv4**|**ipv6**]] [**sgt** *value*] [**name** *sg_name*] [**brief**|**detail**]

説明：
このコマンドは、SXP から統合されたアクティブ IP-SGT マッピングを表示します。SGT 値が指定されたセキュリティ グループ名（カッコを含む）などの詳細を表示するには、**detail** キーワードを含めます。セキュリティ グループの名前が使用できない場合、SGT 値だけがカッコなしで表示されます。

address *ip_address*	指定した IPv4 または IPv6 アドレスと一致する IP-SGT マッピングを表示します。
ipv4 | **ipv6**	IPv4 または IPv6 マッピングを表示します。デフォルトでは、IPv4 マッピングだけが表示されます。
sgt *value*	指定した SGT と一致する IP-SGT マッピングを表示します。
name *sg_name*	指定したセキュリティ グループ名と一致する IP-SGT マッピングを表示します。
brief	サマリーを表示します。
detail	セキュリティ グループの名前などの詳細を表示します。

出力：

次に、IPv6 アドレスを持つ IP-SGT マッピングの例を示します。

```
hostname# show cts sgt-map ipv6
Active IP-SGT Bindings Information

IP Address                                SGT     Source
============================================================
3330::1                                   17      SXP
FE80::A8BB:CCFF:FE00:110                  17      SXP

IP-SGT Active Bindings Summary
============================================
Total number of SXP    bindings = 2
Total number of active   bindings = 2
```

次に、IPv6 アドレスを持つ IP-SGT マッピングに関する、セキュリティ グループの名前を含む詳細情報の例を示します。

```
hostname# show cts sgt-map ipv6 detail
Active IP-SGT Bindings Information

IP Address                 Security Group                          Source
============================================================================
3330::1                     2345                                    SXP
1280::A8BB:CCFF:FE00:110    Security Tech Business Unit(12345)      SXP

IP-SGT Active Bindings Summary
===================================
Total number of SXP    bindings = 2
Total number of active bindings = 2
```

次に、IPv6 アドレスを持つ IP-SGT マッピングのサマリーの例を示します。

```
hostname# show cts sgt-map ipv6 brief
Active IP-SGT Bindings Information

IP-SGT Active Bindings Summary
==================================
Total number of SXP    bindings = 2
Total number of active bindings = 2
```

次に、特定のサブネット内に含まれる IP-SGT マッピングを表示する例を示します。

```
hostname# show cts sgt-map address 10.10.10.5 mask 255.255.255.255

Active IP-SGT Bindings Information

IP Address              SGT     Source
============================================================
10.10.10.5              1234    SXP

IP-SGT Active Bindings Summary
==========================================
Total number of SXP    bindings = 1
Total number of active   bindings = 1
```

SXP によって学習された IP-SGT マッピングの表示

構文：

show cts sxp sgt-map [**peer** *peer_addr*] [**sgt** *value*] [**address** *ipv4_addr* [**netmask** *mask*]|**address** *ipv6_addr*[*/prefix*]|**ipv4**|**ipv6**] [**brief**|**detail**]

説明：

このコマンドは、特定のユーザ コンテキストの SXP モジュールの現在の IP-SGT マッピング データベースを表示します。

SGT 値が指定されたセキュリティ グループ名（カッコを含む）などの詳細を表示するには、**detail** キーワードを含めます。セキュリティ グループの名前が使用できない場合、SGT 値だけがカッコなしで表示されます。

（注） **show cts sgt-map** コマンドは、制御パスの IP-SGT マネージャ エントリを表示します。一方、**show cts sxp sgt-map** コマンドは、インスタンス番号、ピア IP アドレスなど、より詳細な情報を表示します。

peer *peer_addr*	IP-SGT マッピングの *ipv4_addr* ピア IP アドレスだけを表示します。
sgt *value*	IP-SGT マッピングの *ipv4_addr* SGT だけを表示します。
address *ipv4_addr* [**netmask** *mask*]	指定の IPv4 アドレスまたはサブネットに含まれる IP-SGT マッピングだけを表示します。
address *ipv6_addr*[*/prefix*]	指定の IPv6 アドレスまたはサブネットに含まれる IP-SGT マッピングだけが表示されます。

brief　サマリーだけを表示します。

detail　セキュリティ グループの名前などの詳細を表示します。

出力：

次に、エントリがアクティブであるかどうかを含め、IP-SGT マッピング データベースの各 IP-SGT マッピング エントリに関する詳細情報の例を示します。エントリはセキュリティ ポリシーまたはセキュリティ グループ オブジェクトで使用されるときにアクティブになります。

```
hostname# show cts sxp sgt-map detail
Total number of IP-SGT mappings : 3

SGT        : STBU(7)
IPv4       : 2.2.2.1
Peer IP    : 2.2.2.1
Ins Num    : 1
Status     : Active

SGT        : STBU(7)
IPv4       : 2.2.2.0
Peer IP    : 3.3.3.1
Ins Num    : 1
Status     : Inactive

SGT        : 6
IPv6       : 1234::A8BB:CCFF:FE00:110
Peer IP    : 2.2.2.1
Ins Num    : 1
Status     : Active
```

次に、IP-SGT マッピング データベースからのマッピング情報のサマリーの例を示します。

```
hostname# show cts sxp sgt-map brief
Total number of IP-SGT mappings : 3
SGT, IPv4: 7, 2.2.2.1
SGT, IPv4: 7, 3.3.3.0
SGT, IPv6: 7, FE80::A8BB:CCFF:FE00:110
```

データパスの IP-SGT マッピング データベースの表示

構文：

show asp table cts sgt-map [**address** *ipv4_addr*|**address** *ipv6_addr*|**ipv4**|**ipv6**|**sgt** *value*]

説明：

このコマンドは、データパスに維持される IP-SGT マッピング データベースからの IP-SGT マッピングを表示します。IP アドレスが指定されていない場合、データパスの IP-SGT マッピング データベースのすべてのエントリが表示されます。IP アドレスには、正確なアドレスまたはサブネット ベースの IP アドレスを指定できます。

address *ipv4_addr*　指定した IPv4 アドレスの IP-SGT マッピングを表示します。

address *ipv6_addr*　指定した IPv6 アドレスの IP-SGT マッピングを表示します。

ipv4　IPv4 アドレスを持つすべての IP-SGT マッピングを表示します。

ipv6　IPv6 アドレスを持つすべての IP-SGT マッピングを表示します。

sgt *value*	指定した SGT 値の IP-SGT マッピングを表示します。
default	IPv4 アドレスを持つ IP-SGT マッピングを表示します。

出力：

次に、ASP テーブルのすべての IP-SGT マッピング エントリの例を示します。

```
hostname# show asp table cts sgt-map
IP Address                      SGT
======================================
10.10.10.5                      1234
55.67.89.12                     05
56.34.0.0                       338
192.4.4.4                       345
```

次に、特定の IP アドレスの ASP テーブルの IP-SGT マップ情報の例を示します。

```
hostname# show asp table cts sgt-map address 10.10.10.5
IP Address                      SGT
======================================
10.10.10.5                      1234
```

次に、すべての IPv6 アドレスの ASP テーブルの IP-SGT マップ情報の例を示します。

```
hostname# show asp table cts sgt-map ipv6
IP Address                      SGT
======================================
FE80::A8BB:CCFF:FE00:110        17
FE80::A8BB:CCFF:FE00:120        18
```

次に、特定の SGT 値の ASP テーブルの IP-SGT マップ情報の例を示します。

```
hostname# show asp table cts sgt-map sgt 17
IP Address                      SGT
======================================
FE80::A8BB:CCFF:FE00:110        17
```

PAC ファイルのモニタリング

構文：

```
show cts pac
```

説明：

このコマンドは、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ます。

ASA は、PAC ファイルの期限が切れるか、または PAC ファイルが期限切れの 30 日以内になった場合に、表示の最後に警告メッセージを表示します。

```
WARNING: The pac will expire in less than 10 days
WARNING: The pac expired at Apr 30 2011 21:03:49 and needs to be refreshed
```

出力：

```
hostname# show cts pacs
  AID: CAFECAFECAFECAFECAFECAFECAFECAFE
  PAC-Info:
```

```
    Valid until: Apr 06 2002 01:00:31 UTC
    AID: CAFECAFECAFECAFECAFECAFECAFECAFE
    I-ID: someASA
    A-ID-Info: "Cisco Policy Manager"
    PAC-type = Cisco trustsec
PAC-Opaque:
000200820001000400010DEADBEEFDEADBEEF11111111111111110006005400000000158EDE58522C8698794F2F2
4F2623F8D26D78414DE33B102E6E93EDE53B8EFF0061FC14C1E1CCF14A04F69DAC79FE9F1BCD514893AC87B0AD
B476D2CB9CBF75788C5B8C3AE89E5322E4A124D4CB6A616B306E1DDD38CCE3E634E64E17BBD31957B0579DBC
```

ASA-Cisco TrustSec 統合の機能履歴

表 34-3 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 34-3　ASA-Cisco TrustSec 統合の機能履歴

機能名	プラットフォーム リリース	機能情報
Cisco TrustSec の統合	9.0(1)	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 ソリューションです。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 ソリューションでは、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。 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 ソリューションを活用できます。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。 **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**、**show object-group**、**show conn security-group**、**clear cts**、**debug cts** の各コマンドが導入または変更されました。