Trustsec ファイアウォールポリシーの管理

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ー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。

Cisco ASA に Cisco TrustSec が統合され、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。

（注） バージョン 4.21 以降、Cisco Security Manager では、すべてのアグリゲーション サービス ルータ、統合サービスルータ、埋め込み型サービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体が終了します。

セキュリティグループ認識は複数の既存のファイアウォールルールに組み込まれます。固有の TrustSec ファイアウォールポリシーはありません。この章では、TrustSec ファイアウォールポリシーと、セキュリティグループ認識をサポートするさまざまなポリシーに TrustSec ファイアウォールポリシーを実装する方法について説明します。

この章は次のトピックで構成されています。

TrustSec ファイアウォールポリシーの概要

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、ユーザー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で、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のセキュリティソリューションを有効にするために、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可用性と伝達がますます重要な要件となっています。

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ー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。

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 ユーザー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。

ここでは、次の内容について説明します。

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（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ー 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 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制御を判断します。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）、サーバー、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。

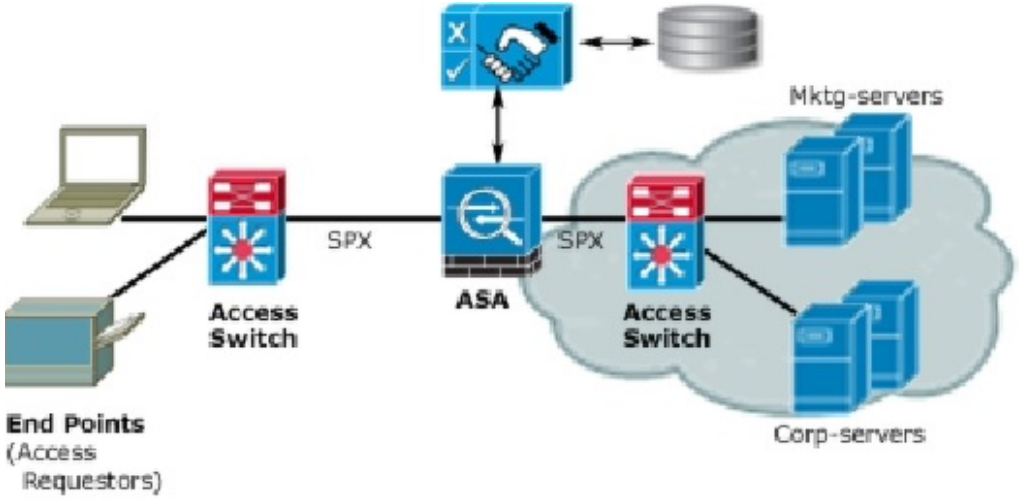
セキュリティ グループ ポリシーの適用

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。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、ユーザーおよびデバイス 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。

- ユーザー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 *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、サーバー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、サーバーのプールに 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。
- サーバーの 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） ユーザー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、ユーザーベースの属性、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。

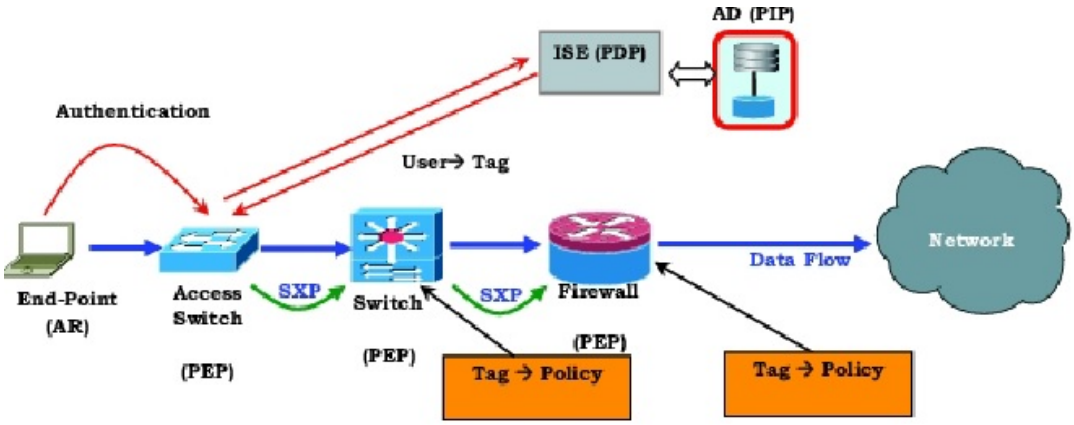
（注） バージョン 4.23 以降、Cisco Security Manager は、ACL および AAA ポリシーでの ISE サーバーからの 20 を超えるセキュリティグループタグ（SGT）の取得をサポートしています。[SGT] フィールドおよび[ユーザー（User）]フィールドの検索テキストボックスで下線を使用することにより、下線が含まれているユーザー名を検索する手間を減らすこともできます。

（注） Cisco Identity Services Engine の詳細については、http://www.cisco.com/en/US/products/ps11640/index.htmlを参照してください。

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 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、ADSA は SXP ピアに IP-SGT マッピングを送信します。 送信者および受信者のロールについて （7 ページ）を参照してください。

- 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。

送信者および受信者のロールについて

セキュリティグループ交換プロトコル（SXP）では、他のネットワークデバイスとの間でIP-SGTマッピングを送受信するために使用されます。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 マッピングをダウンストリーム デバイスに渡すこともできます。

SXP ピアへの SXP 接続を設定する場合は、その接続について、アイデンティティ情報を交換できるように、デバイス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：アクティブな IP-SGT マッピングをポリシー適用のためにすべてアップストリームデバイスに転送できるように、デバイスを設定します。
- 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、デバイスを設定します。

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、デバイスはシステムログメッセージを生成します。

デバイスを 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。

SXP の設定の一部として、SXP 調整タイマーを設定します。SXP ピアが SXP 接続を終了すると、デバイス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、デバイスは調整タイマーを開始します。次に、デバイスは、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 と Cisco TrustSec 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 を登録する。
- ISE で ASA のセキュリティグループを作成する。
- ASA にインポートする PAC ファイルを ISE で生成する。

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。

1. ISE にログインします。
2. [管理（Administration）] > [ネットワークデバイス（Network Devices）] > [ネットワークデバイス（Network Devices）] の順に選択します。
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 サーバーを設定する場合は、ISE でここで作成した共有秘密を指定します。ASA の AAA サーバー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 サーバーを指定します。AAA サーバーを ASA で設定する場合は、サーバー 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. [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [セキュリティグループアクセス（Security Group Access）] > [セキュリティグループ（Security Groups）] 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. [セキュリティグループアクセス（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 の生成

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. [管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワークデバイス（Network Devices）] の順に選択します。
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、SMB を介してリモートサーバーから 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）。

TrustSec ファイアウォールポリシーの構成

セキュリティグループ認識は複数の既存のファイアウォールルールに組み込まれます。固有の TrustSec ファイアウォールポリシーはありません。また、サポートするツールが更新され、TrustSec ファイアウォールポリシーで機能するようになりました。たとえば、[検索と置換（Find and Replace）] ツールを使用して、特定のセキュリティグループを含むルールを検索できます。

この項では、セキュリティグループ認識をファイアウォールポリシーに統合するためのさまざまな手順について説明します。

ここでは、次の内容について説明します。

- Cisco TrustSec サービスの設定 （10 ページ）
- セキュリティ グループ オブジェクトの作成 （19 ページ）
- ポリシーでのセキュリティグループの選択 （21 ページ）
- TrustSec ベースのファイアウォールルールの設定 （22 ページ）

Cisco TrustSec サービスの設定

この手順では、Cisco Security Manager および必要なセキュリティデバイスで Cisco TrustSec の有効化と設定の方法について説明します。

はじめる前に

Cisco TrustSec と統合するために ASA を設定する前に、 ASA と Cisco TrustSec を統合するための前提条件 （8 ページ）で説明されている前提条件を満たす必要があります。

Cisco TrustSec を設定するには、次のタスクを実行します。

ステップ 1 Cisco Security Manager と Cisco Identity Services Engine（ISE）間の通信を設定します。[ISE設定（ISE Settings）] ページを参照してください。

（注） Cisco Security Manager は、セキュリティグループの名前とタグを取得して解決するために、1 つの ISE アプライアンス/サーバーとの通信のみサポートします。

ステップ 2 Security Exchange Protocol（SXP）を有効にしてデフォルト値を設定します。 Cisco TrustSec の SGT および SXP サポートについて （2 ページ）を参照してください。

ステップ 3 Cisco TrustSec アーキテクチャの SXP 接続ピアを追加します。 SXP 接続ピアの定義 （15 ページ）を参照してください。

ステップ 4 （ASA 9.3.1 以降のデバイスのみ）セキュリティ グループ タギング オプションを設定します。[Add Interface]/[Edit Interface] ダイアログボックス - [Advanced] タブ（ASA/PIX 7.0 以降）を参照してください。

ステップ 5 （ASA 9.3.1 以降のデバイスのみ）VPN セッションのセキュリティ グループ タギングを設定します。ASA グループ ポリシーの SSL VPN フル クライアント設定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。 TrustSec ベースのファイアウォールルールの設定 （22 ページ）を参照してください

ステップ 7 TrustSec ファイアウォールシステムを監視します。 TrustSec ファイアウォールポリシーのモニタリング （23 ページ） を参照してください。

Security Exchange Protocol（SXP）の設定

[SXP 設定（SXP Settings）] ページを使用して、セキュリティデバイスで Security Exchange Protocol（SXP）を有効にし、デバイスの SXP 設定を行います。

（注） 特定のデバイスタイプのポリシービューまたはデバイスビューからそのページにアクセスするかどうかにかかわらず、すべての設定は [SXP 設定（SXP Settings）] ページで使用できます。特定のデバイスでサポートされていない設定を行うと、検証警告を受信し、そのデバイスでサポートされていない CLI は生成されません。

ナビゲーション パス

- （デバイスビュー）セキュリティデバイスを選択し、ポリシーセレクタから [TrustSec] > [SXP設定（SXP Settings）] を選択します。
- (ポリシービュー) ポリシーセレクターから [TrustSec] > [SXP設定（SXP Settings）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- ASA と Cisco TrustSec を統合するための前提条件 （8 ページ）
- SXP 接続ピアの定義 （15 ページ）

フィールド リファレンス

表 *1 : [SXP*設定（*SXP Settings***）*]* ページ**

要素	説明
SGT 交換プロトコル（SXP）の有効化	デバイスでセキュリティ交換プロトコルを有効にするかどうか。デフォルトではディセーブルになっています。
再試行タイマー	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。0～64000 秒の範囲で、再試行タイマー値を秒数で入力します。0 秒を指定すると、タイマーの期限が切れず、デバイスは SXP ピアへの接続を試行しません。デフォルトでは、タイマー値は 120 秒です。 デバイスは、接続に成功するまで、新しい SXP ピアへの接続の試みを続けます。 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。 再試行タイマーが期限切れになると、デバイスは接続データベースを順に検索し、データベースにオフまたは「保留中」状態の接続が含まれている場合、 デバイスは再試行タイマーを再開します。

要素	説明
調整タイマー	調整タイマー値（1 ～ 64000 秒の範囲）。デフォルトでは、タイマー値は 120 秒です。 SXP ピアが SXP 接続を終了すると、セキュリティデバイス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 ピアが再接続されると、デバイスは調整タイマーを開始します。次に、デバイスは 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、デバイスは、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。デバイスは、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、デバイスは 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。 （注） 復帰期間を 0 秒に設定すると、タイマーが無効になり、前回の接続のすべてのエントリが削除されます。
ネットワーク マップ	ネットワークマップ引数は、SGT にバインドされ、SXP リスナーにエクスポートできる、0 ～ 65,535 のサブネット IP ホストの最大数を指定します。デフォルトは 0（実行される拡張なし）です。
Server Group Name （IOS-XE には適用されません）	デバイス用 ISE で作成したセキュリティグループの名前を入力または選択します。 （注） サーバーグループを選択する場合、AAA サーバーグループを追加することもできます。 ここで指定するサーバーグループ名は、デバイス用 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。これら 2 つのグループ名が一致しない場合、デバイスは ISE と通信できません。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。
CTS サーバー設定（IOS/IOS-XE のみ）	
ログバインディング変更	IP から SGT へのバインディング変更のロギングを有効にすると、IP から SGT へのバインディング変更（追加、削除、変更）が発生するたびに SXP の syslog（sev 5 syslog）が生成されるかどうか。これらの変更は SXP 接続で学習されて伝播されます。このロギング機能は、デフォルトではディセーブルになっています。

要素	説明
キャッシングの有効化 キャッシュ NV ストレージ （IOS-XE には適用されません）	DRAM および NVRAM への TrustSec 許可および環境データ情報のキャッシュを有効にするかどうか。 DRAM キャッシュの更新を不揮発性ストレージに書き込み、デバイスの起動時に DRAM キャッシュが不揮発性ストレージから最初に読み込まれるようにするには、[キャッシュNVストレージ（Cache NV Storage）] リストから目的のファイルシステムを選択します。次のオプションがあります。 • flash • flash0 • flash1 • flash2 • disk0 • disk1 • disk2
CTS SGT 番号	1 ～ 65533 の番号を入力して、このデバイスのセキュリティグループタグ（SGT）番号を手動で割り当てます。
サーバーのデッドタイム （IOS-XE には適用されません）	いったん停止中としてマークされたグループ内のサーバを、どのくらいの期間、サービス用に選択してはいけないかを指定します。デフォルトは 20 秒です。指定できる範囲は 1 ～ 864000 です。

要素	説明
ロード バランシング（Load Balance） （IOS-XE には適用されません）	RADIUS サーバーグループのロードバランシングを設定するかどうか。ロードバランスが有効になっている場合、次のオプションを指定できます。 バッチサイズ：バッチごとに割り当てられるトランザクションの数。デフォルトの transactions は 25 です。 （注） バッチ サイズを変更すると、CPU の負荷やネットワークのスループットに影響する可能性があります。バッチ サイズが大きくなるほど、CPUの負荷が減少し、ネットワークのスループットが増加します。ただし、バッチ サイズが大きくても、使用可能なすべてのサーバー リソースが使い果たされることはありません。バッチ サイズが小さくなるほど、CPUの負荷が増加し、ネットワークのスループットが減少します。デフォルト バッチ サイズの 25 の使用を推奨します。これは、CPU の負荷に悪影響を及ぼさない、高スループットに最適化されているためです。 優先サーバを無視：セッション全体を通じて同じサーバーを使用しないようにデバイスに指示します。
SGT ロールベース マップテーブル （ASA 9.3(1)+、IOS15.2(2)T+、および IOS-XE3.5.x（15.2(1)S）+ のみ）	SGT ロールベースマップテーブルを使用して、セキュリティグループタグ（SGT）番号を個々の IP アドレスまたはホストオブジェクトに手動でマッピングします。 次を実行できます。 • エントリを追加するには、[行の追加（+）（Add Row(+)] ボタンをクリックし、[接続ピアの追加（Add Connection Peer）] ダイアログボックスに入力します。 [SGTロールの追加/編集（Add/Edit SGT Role）] ダイアログボックス （14 ページ）を参照してください。 • エントリを編集するには、エントリを選択し、[行の編集（鉛筆）（Edit Row (pencil)）] ボタンをクリックします。 • エントリを削除するには、エントリを選択し、[行の削除（ゴミ箱）（Delete Row (trash can)）] ボタンをクリックします。

[SGTロールの追加/編集（Add/Edit SGT Role）] ダイアログボックス

[SGTロールの追加/編集（Add/Edit SGT Role）] ダイアログボックスを使用して、セキュリティグループタグ（SGT）番号を個々の IP アドレスまたはホストオブジェクトに手動でマッピングします。

ナビゲーション パス

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから [TrustSec] > [SXP設定（SXP Settings）] を選択します。
  - エントリを追加するには、[SGTロールベースマップ（SGT Rolebased Map）] テーブルの下にある [行の追加（+）（Add Row (+)）] ボタンをクリックします。
  - エントリを編集するには、エントリを選択し、[SGTロールベースマップ（SGT Rolebased Map）] テーブルの下にある [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。
- (ポリシービュー) ポリシーセレクターから [TrustSec] > [SXP設定（SXP Settings）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。
  - エントリを追加するには、[SGTロールベースマップ（SGT Rolebased Map）] テーブルの下にある [行の追加（+）（Add Row (+)）] ボタンをクリックします。
  - エントリを編集するには、エントリを選択し、[SGTロールベースマップ（SGT Rolebased Map）] テーブルの下にある [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。

関連項目

- 送信者および受信者のロールについて （7 ページ）
- ASA と Cisco TrustSec を統合するための前提条件 （8 ページ）

フィールド リファレンス

表 *2 : [SGT*ロールの追加/編集（*Add/Edit SGT Role***）*]* ダイアログボックス**

要素	説明
IPアドレス	セキュリティグループタグ（SGT）番号を手動で割り当てるホストの IPv4 アドレス。 ホストオブジェクトの IP アドレスまたは名前を入力できます。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成できます。
CTS SGT 番号	指定したホスト/IP アドレスに割り当てるセキュリティグループタグ（SGT）番号。ASA 9.3(1)+ で有効なセキュリティタグ番号は 2 ～ 65519 です。

SXP 接続ピアの定義

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。ピア間の SXP 接続はポイントツーポイントであり、基礎となるトランスポート プロトコルとして TCP を使用します。

関連項目

- ASA と Cisco TrustSec を統合するための前提条件 （8 ページ）
- 送信者および受信者のロールについて （7 ページ）
- Security Exchange Protocol（SXP）の設定 （10 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから [TrustSec（TrustSec）] > [SXP接続ピア（SXP Connection Peers）] を選択します。
- (ポリシー ビュー) ポリシー セレクターから [TrustSec] > [SXP 接続ピア] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 [デフォルトソース（Default Source）] フィールドに、SXP 接続のデフォルトローカル IP アドレスを入力します。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力できます。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成できます。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、デバイスが 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発信インターフェイスの IP アドレスと異なる場合、デバイスは SXP ピアに接続できず、システムログメッセージを生成します。

ステップ 3 [デフォルトパスワード（Default password）] と [確認（Confirm）] に、SXP ピアによる TCP MD5 認証用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。

パスワードは、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 ストリングとして指定できます。

ステップ 4 SXP ピアの設定：

次を実行できます。

- エントリを追加するには、[行の追加（+）（Add Row(+)] ボタンをクリックし、[接続ピアの追加（Add Connection Peer）] ダイアログボックスに入力します。[接続ピアの追加（Add Connection Peer）]/[接続ピアの編集（Edit Connection Peer）] ダイアログボックス （17 ページ）を参照してください。
- エントリを編集するには、エントリを選択し、[行の編集（鉛筆）（Edit Row (pencil)）] ボタンをクリックします。
- エントリを削除するには、エントリを選択し、[行の削除（ゴミ箱）（Delete Row (trash can)）] ボタンをクリックします。

ステップ 5 [保存（Save）] をクリックして変更を保存します。

[接続ピアの追加（Add Connection Peer）]/[接続ピアの編集（Edit Connection Peer）] ダイアログボックス

[接続ピアの追加（Add Connection Peer）]/[接続ピアの編集（Edit Connection Peer）] ダイアログボックスを使用して、SXP 接続の設定を定義します。

（注） ポリシービューまたは特定のデバイスタイプのデバイスビューのどちらから [接続ピアの追加/編集（Add/Edit Connection Peer）] ダイアログボックスにアクセスしても、このダイアログボックスですべての設定を使用できます。特定のデバイスでサポートされていない設定を行うと、検証警告を受信し、そのデバイスでサポートされていない CLI は生成されません。

ナビゲーション パス

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから [TrustSec（TrustSec）] > [SXP接続ピア（SXP Connection Peers）] を選択します。
  - エントリを追加するには、[行の追加（Add Row）]（+）ボタンをクリックします。
  - エントリを編集するには、エントリを選択し、[行の編集（鉛筆）（Edit Row (pencil)）] ボタンをクリックします。
- (ポリシー ビュー) ポリシー セレクターから [TrustSec] > [SXP 接続ピア] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。
  - エントリを追加するには、[行の追加（Add Row）]（+）ボタンをクリックします。
  - エントリを編集するには、エントリを選択し、[行の編集（鉛筆）（Edit Row (pencil)）] ボタンをクリックします。

関連項目

- 送信者および受信者のロールについて （7 ページ）
- ASA と Cisco TrustSec を統合するための前提条件 （8 ページ）

フィールド リファレンス

表 3 : [接続ピアの追加（Add Connection Peer）] ダイアログボックス

要素	説明
ピア IP アドレス（Peer IP Address）	SXP ピアの IPv4 アドレスまたは IPv6 アドレス。ピア IP アドレスは、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。 ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力できます。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成できます。
送信元 IP アドレス	（任意）SXP 接続のローカル IPv4 または IPv6 アドレス。送信元 IP アドレスの指定は任意ですが、選択することにより設定ミスを防ぐことができます。 ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力できます。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成できます。 （注） 送信元 IP アドレスとピア IP アドレスを同じアドレスで設定することはできません。また、一方のフィールドで IPv4 アドレスを使用し、もう一方のフィールドで IPv6 アドレスを使用することはできません。
パスワード	SXP 接続に認証キーを使用するかどうかを指定します。次の値から選択します。 • 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。 SXP 接続ピアの定義 （15 ページ）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（Mode）]	SXP 接続のモード。次の値から選択します。 • 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。

要素	説明
ロール	SXP接続で、デバイスがスピーカまたはリスナーのいずれとして機能するかを指定します。 • [リスナー（Listener）]：デバイス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。 • [スピーカ（Speaker）]： デバイスは 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。 送信者および受信者のロールについて （7 ページ）を参照してください。
最小保留時間（Hold Time (Min)） IOS および IOS-XE のみに適用	スピーカーまたはリスナーデバイスの最小保留時間（秒単位）。
最大保留時間（Hold Time Max） IOS および IOS-XE のみに適用	スピーカーまたはリスナーデバイスの最大保留時間（秒単位）。hold-time maximum-period 値は、peer speaker と local listener オプションを組み合わせて使用する場合のみ必要です。その他のインスタンスでは、hold-time minimum-period 値のみが必要です。

セキュリティ グループ オブジェクトの作成

作成したセキュリティ グループ オブジェクト グループは、Cisco TrustSec をサポートする機能で使用できます。そのグループを拡張 ACL に入れると、たとえばアクセス ルールで使用できるようになります。

Cisco TrustSec と統合されているときは、セキュリティデバイスは Cisco Identity Services Engine（ISE）からセキュリティグループの情報をダウンロードします。ISE はアイデンティティ リポジトリとしても動作し、Cisco TrustSec タグからユーザー アイデンティティへのマッピングと、Cisco TrustSec タグからサーバー リソースへのマッピングを行います。セキュリティ グループ アクセス リストのプロビジョニングおよび管理は、中央集中型で ISE 上で行います。

ただし、デバイスには、グローバルには定義されていない、ローカライズされたネットワーク リソースが存在することがあり、そのようなリソースにはローカル セキュリティ グループとローカライズされたセキュリティポリシーが必要です。ローカルセキュリティ グループには、ISEからダウンロードされた、ネストされたセキュリティ グループを含めることができます。セキュリティデバイスは、ローカルと中央のセキュリティグループを統合します。

デバイス上でローカル セキュリティ グループを作成するには、ローカル セキュリティ オブジェクト グループを作成します。1 つのローカル セキュリティ オブジェクト グループに、1 つ以上のネストされたセキュリティ オブジェクト グループまたはセキュリティ ID またはセキュリティ グループ名を入れることができます。ユーザーは、デバイス上に存在しない新しいセキュリティ ID またはセキュリティグループ名を作成することもできます。

作成したセキュリティ オブジェクト グループは、ネットワークリソースへのアクセスを制御するために使用できます。セキュリティ オブジェクト グループを、アクセス グループやサービス ポリシーの一部として使用できます。

ヒント

- これらのオブジェクトの使用は、ASA 9.0(1) 以降でのみサポートされます。
- これらのオブジェクトの使用を有効にするには、デバイスで TrustSec ポリシーを設定する必要があります。
- このオブジェクトタイプを使用するポリシー、またはオブジェクトを定義するときに、セキュリティ グループ オブジェクトを作成できます。詳細については、ポリシーでのセキュリティグループの選択 （21 ページ）を参照してください。

関連項目

- ポリシーでのセキュリティグループの選択 （21 ページ）
- ポリシー オブジェクトの作成

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます（Policy Object Managerを参照）。

ステップ 2 オブジェクトタイプセレクタから [セキュリティグループ（Security Group）] を選択します。

ステップ 3 作業領域を右クリックして [新規オブジェクト（New Object）] を選択し、[セキュリティグループの追加（Add Security Group）] ダイアログボックスを開きます。

ステップ 4 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

ステップ 5 [グループ内のメンバー（Members in Group）] リストにアイテムを追加したり、このリストからアイテムを削除したりして、オブジェクトに定義されているユーザーとユーザーグループを識別します。

リストに入力するには、次のいずれかの組み合わせを実行します。

- [利用可能なセキュリティグループ（Available Security Group）] で、既存のオブジェクトを選択し、リスト間の [追加>>（Add >>）] ボタンをクリックします。
- [名前/タグの検索（Search name/tag）] で、[ISE設定（ISE Settings）] の管理オプションで設定済みの ISE サーバーからセキュリティグループを選択します。名前またはタグを選択する前に、設定を行う必要があります（[ISE設定（ISE Settings）] ページを参照）。

セキュリティグループを検索するには、検索文字列を入力します。次に、[検索（Search）] をクリックして一致する文字列を検索します。文字列がセキュリティグループ名のどこかにある場合、名前は一致したと見なされます。

セキュリティグループを追加するには、リストで選択し、リスト間にある [追加>>（Add >>）] ボタンをクリックします。

- [カンマ区切りで入力（名前またはタグ）（Type in comma separated (Name or Tag)）] で、最初に作成するエントリのタイプ（名前またはタグ）を選択します。有効なセキュリティグループ名またはタグ番号を入力し、リスト間の [追加>>（Add >>）] ボタンをクリックします。複数の名前やタグはカンマで

区切ります。名前やタグはメンバーリストに別々の行として追加されます。複数の名前やタグを追加する場合は、カンマの前後にスペースを追加しないでください。

有効なセキュリティタグ番号は、ASA 9.3 以降の場合は 0 ～ 65533、ASA のバージョンが 9.3 未満の場合は 1 ～ 65533 です。

- オブジェクトから項目を削除するには、[メンバー（Members）] リストで項目を選択し、リスト間にある [<<削除（<< Remove）] ボタンをクリックします。

（注） バージョン 4.21 以降、Cisco Security Manager では、すべてのアグリゲーション サービス ルータ、統合サービスルータ、埋め込み型サービスルータ、およびCisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体が終了します。

ステップ 6 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。カテゴリ オブジェクトの使用を参照してください。

ステップ 7 （任意）[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択して、このオブジェクトのプロパティを個々のデバイスで再定義できるようにします。ポリシー オブジェクトの上書きの許可を参照してください。

ステップ 8 [OK] をクリックしてオブジェクトを保存します。

ポリシーでのセキュリティグループの選択

セキュリティグループの指定を許可するポリシーまたはポリシーオブジェクトで、直接または TrustSec セキュリティ グループオブジェクトを選択して、[セキュリティグループ（Security Groups）] フィールドの横にある [選択（Select）] ボタンをクリックして情報を入力できます。

[セキュリティグループセレクタ（Security Group Selector）] ダイアログボックスで [グループ内のメンバー（Members in Group）] リストに入力することにより、[セキュリティグループ（Security Groups）] フィールドの内容を定義できます。リストに入力するには、次のいずれかの組み合わせを実行します。

- [利用可能なセキュリティグループ（Available Security Group）] で、既存のオブジェクトを選択し、リスト間の [追加>>（Add >>）] ボタンをクリックします。目的のオブジェクトが存在しない場合は、リストの下にある [追加（Add）]（+）ボタンをクリックして新しいオブジェクトを作成できます。オブジェクトを選択し [編集（Edit）]（鉛筆）ボタンをクリックして、オブジェクトを変更するか、内容を確認できます。
- [名前/タグの検索（Search name/tag）] で、[ISE設定（ISE Settings）] の管理オプションで設定済みの ISE サーバーからセキュリティグループを選択します。名前またはタグを選択する前に、設定を行う必要があります（[ISE設定（ISE Settings）] ページを参照）。

セキュリティグループを検索するには、検索文字列を入力します。次に、[検索（Search）] をクリックして一致する文字列を検索します。文字列がセキュリティグループ名のどこかにある場合、名前は一致したと見なされます。

セキュリティグループを追加するには、リストで選択し、リスト間にある [追加>>（Add>>）] ボタンをクリックします。

- [カンマ区切りで入力（名前またはタグ）（Type in comma separated (Name or Tag)）] で、最初に作成するエントリのタイプ（名前またはタグ）を選択します。有効なセキュリティグループ名またはタグ番号を入力し、リスト間の [追加>>（Add >>）] ボタンをクリックします。複数の名前やタグはカンマで区切ります。名前やタグはメンバーリストに別々の行として追加されます。複数の名前やタグを追加する場合は、カンマの前後にスペースを追加しないでください。

有効なセキュリティタグ番号は、ASA 9.3 以降の場合は 0 ～ 65533、ASA のバージョンが 9.3 未満の場合は 1 ～ 65533 です。

- オブジェクトから項目を削除するには、[メンバー（Members）] リストで項目を選択し、リスト間にある [<<削除（<< Remove）] ボタンをクリックします。

TrustSec ベースのファイアウォールルールの設定

セキュリティグループ認識は、ファイアウォールサービスを提供するために使用される ACL 内のアクセス コントロール エントリまたはルールと統合されます。この機能は ACL と統合されるため、セキュリティグループ認識をファイアウォール ポリシーに追加する方法は、すべてのタイプのファイアウォールポリシーで同じになります。この項では、セキュリティグループ認識を既存のポリシーに取り込む一般的な方法を説明し、セキュリティグループをサポートするポリシーごとの設定について、詳細な情報を提供します。

セキュリティグループをサポートするファイアウォール ポリシー

ASA 9.0.1 以降でのみ、次のポリシータイプのセキュリティグループを設定できます。

- AAA ルール：[ファイアウォール（Firewall）] > [AAA ルール（AAA Rules）] を選択します。ASA、PIX、および FWSM デバイスの AAA ルールの設定を参照してください。
- アクセスルール：**[ファイアウォール（Firewall）] > [アクセスルール（Access Rules）]**を選択します。アクセス ルールの設定を参照してください。
- インスペクションルール：[ファイアウォール（Firewall）] > [インスペクションルール（Inspection Rules）] を選択します。インスペクション ルールの設定を参照してください。
- 拡張 ACL ポリシー オブジェクトを使用するポリシー：複数のファイアウォール ポリシーが拡張 ACL ポリシー オブジェクトを使用して、ルール テーブルを直接ポリシーに取り込む代わりにトラフィック照合基準を定義できます。セキュリティグループ指定を組み込むために拡張 ACL ポリシー オブジェクトを設定できます（拡張アクセス コントロール リスト オブジェクトの作成を参照）。これらの拡張 ACL オブジェクトは、次のポリシーで使用できます。
  - ボットネット トラフィック フィルタ ルール：[ファイアウォール（Firewall）] > [ボットネット トラフィック フィルタ ルール（Botnet Traffic Filter Rules）] を選択します。ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル

化を参照してください。セキュリティグループは、イネーブルルールおよびドロップルールのトラフィック分類の一部として使用できます。

- IPS ルール、QoS ルール、および接続ルール（サービスポリシールール）：[プラットフォーム（Platform）] > [サービスポリシールール（Service Policy Rules）] > [IPS、QoS、および接続ルール（IPS, QoS, and Connection Rules）]を選択します。[サービスポリシールール（Service Policy Rules）] ページを参照してください。

このポリシーのトラフィック照合基準は、トラフィック フロー ポリシー オブジェクトに組み込まれる拡張 ACL ポリシー オブジェクトに基づいて行われます。セキュリティグループのトラフィック分類を組み込むトラフィック フロー オブジェクトに、ACL を指定するオプションをいずれか選択する必要があります。詳細については、トラフィック フロー オブジェクトの設定を参照してください。

IOS 15.2(2)T 以降および IOS-XE 3.5.x(15.2(1)S) 以降を実行しているデバイスでは、ゾーンベースのファイアウォールルールにセキュリティグループを設定できます **([ファイアウォール（Firewall）] > [ゾーンベースのファイアウォールルール（ Zone Based Firewall Rules）])**。詳細については、ゾーンベースのファイアウォールルールの追加を参照してください。

TrustSec ファイアウォールポリシーのモニタリング

イベントビューアを使用して、他のタイプのポリシーやイベントと同じ方法で TrustSec ファイアウォールポリシーをモニタリングできます。次に、アイデンティティ ポリシーを効率的に監視するためのヒントをいくつか示します。Event Viewer 使用の一般情報については、イベントの表示を参照してください。

- 特に Cisco TrustSec に関連する syslog メッセージには、766001 ～ 766020、766201 ～ 766205、766251 ～ 766254、および 766301 ～ 766313 の各グループがあります。これらのメッセージの説明については、http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html [英語] で、ご使用の ASA ソフトウェアバージョンの syslog メッセージを参照してください。
- イベントビューアには、TrustSec 情報を表示する次の列があります。[TrustSecセキュリティグループ名（TrustSec Security Group Name）]、[TrustSecセキュリティグループタグ（TrustSec Security Group Tag）]、[SXP接続ソースIP（SXP Connection Source IP）]、[SXP接続失敗理由（SXP Connection Failure Reason）]、[SXPピアIP（SXP Peer IP）]、[SXPピア接続失敗理由（SXP Peer Connection Failure Reason）]。
- [イベントタイプ（Event Type）] にフィルタを作成し、[すべてのファイアウォールイベント（All Firewall Events）] > [TrustSecイベント（TrustSec Events）] フォルダを選択することで、すべてのアイデンティティ関連の syslog メッセージをフィルタリングできます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。