CHAPTER 39

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

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 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（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 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 TrsutSec 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。

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

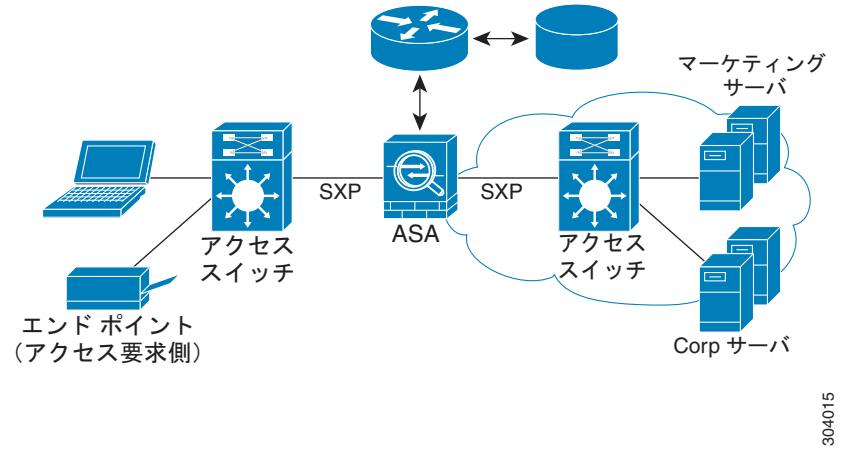
セキュリティ ポリシーの適用はセキュリティ グループの名前に基づきます。エンドポイント デバイスは、データセンターのリソースへのアクセスを試行します。ファイアウォールで設定された従来の IP ベースのポリシーと比較して、アイデンティティベースのポリシーは、ユーザおよびデバイス アイデンティティに基づいて設定されます。たとえば、mktg-contractor が mktg-server にアクセスできるとします。mktg-corp-user は、mktg-server および corp-server にアクセスできます。

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 39-1 は、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 39-1　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 38 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。

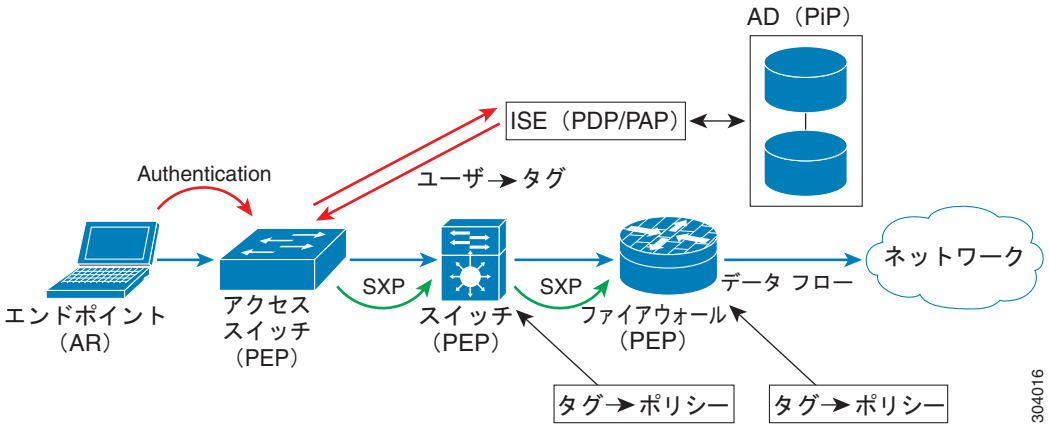
ASA を Cisco TrustSec で機能するように設定する一環として、ISE から Protected Access Credential（PAC）ファイルをインポートする必要があります。詳細については、「Protected Access Credential（PAC）ファイルのインポート」（P.39-13）を参照してください。

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

ASA は、最初にセキュリティ グループ テーブルをダウンロードするときに、テーブル内のすべてのエントリを順を追って調べ、そこで設定されているセキュリティ ポリシーに含まれるすべてのセキュリティ グループの名前を解決します。次に、ASA は、それらのセキュリティ ポリシーをローカルでアクティブ化します。ASA がセキュリティ グループの名前を解決できない場合、不明なセキュリティ グループ名に対して syslog メッセージを生成します。

図 39-2 は、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 39-2　セキュリティ ポリシーの適用



1. エンドポイント デバイスは、アクセス レイヤ デバイスに直接アクセスするか、またはリモート アクセスを介してアクセスし、Cisco TrustSec で認証します。
2. アクセス レイヤ デバイスは 802.1X や Web 認証などの認証方式を使用して ISE のエンドポイント デバイスを認証します。エンドポイント デバイスは、ロールおよびグループ メンバーシップ情報を渡して、デバイスを適切なセキュリティ グループに分類します。
3. アクセス レイヤ デバイスは SXP を使用して、アップストリーム デバイスに IP-SGT マッピングを伝搬します。
4. ASA 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 エントリを送信します。詳細については、「ASA での送信者および受信者のロール」（P.39-6）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、syslog メッセージを生成します。ISE からの ASA 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。

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。

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。

 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.39-6）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 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 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

表 39-1 は ASA がサポートする IP-SGT マッピング エントリ数を示します。

表 39-1　IP-SGT マッピングの許容数

ASA モデル	IP-SGT マッピング エントリ数
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

表 39-2 は ASA がサポートする SXP 接続数を示します。

表 39-2　SXP 接続

ASA モデル	SXP TCP 接続の数
5505	10
5510	25
5520	50
5540	100
5550	150
5580-20	250
5580-40	500
5585-X（SSP-10）	150

表 39-2　SXP 接続 （続き）

ASA モデル	SXP TCP 接続の数
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、次のタスクを実行する必要があります。

- 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 機能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.39-13）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 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）。

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。

フェールオーバーのガイドライン

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。アクセス層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、接続は失敗し、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。
- SXP 接続のループは、デバイスにピアへの双方向の接続がある場合またはデバイスがデバイスの単方向に接続されたチェーンの一部である場合に発生します （ASA は、データセンターのアクセス レイヤからのリソースの IP-SGT マッピングを学習できます。ASA はこれらのタグをダウンストリーム デバイスに伝搬する必要がある場合があります）。SXP 接続ループによって、SXP メッセージ転送の予期しない動作が発生する可能性があります。ASA が送信者および受信者として設定されている場合、SXP 接続ループが発生し、SXP データが最初にそのデータを送信したピアで受信される可能性があります。
- ASA のローカル IP アドレスを変更する場合は、すべての SXP ピアでピア リストが更新されていることを確認する必要があります。さらに、SXP ピアがその IP アドレスを変更する場合は、変更が ASA に反映されていることを確認する必要があります。
- 自動 PAC ファイル プロビジョニングはサポートされません。ASA 管理者は、ISE 管理インターフェイスの PAC ファイルを要求し、それを ASA にインポートする必要があります。PAC ファイルについては、「PAC ファイルの生成」（P.39-9）と「Protected Access Credential（PAC）ファイルのインポート」（P.39-13）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 syslog メッセージを生成します。

  ISE の変更を含めるために、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.39-16）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、SXP 接続を設定するために、ASA で、no-NAT、no-SEQ-RAND、MD5-AUTHENTICATION TCP オプションをイネーブルにする必要があります。SXP ピア間の SXP ポート TCP 64999 宛てのトラフィックに対して TCP 状態バイパス ポリシーを作成します。そして、適切なインターフェイスにポリシーを適用します。

たとえば、次のコマンド セットは、TCP ステート バイパスのポリシーの 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

この項では、次のトピックについて取り上げます。

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、次のタスクを完了する必要があります。

- 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.39-8）を参照してください。

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.39-12）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.39-13）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.39-14）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.39-15）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.39-16）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.39-17）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。

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、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。

Cisco TrustSec との統合のために ISE と通信するように ASA を設定するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Configuration] > [Firewall] > [Identity By TrustSec] の順に選択します。

ステップ 2　ASA にサーバ グループを追加するには、[Manage in the Server Group Setup] 領域で [Manage] をクリックします。[Configure AAA Server Group] ダイアログボックスが表示されます。

ステップ 3　[AAA Server Group] フィールドに、ASA 用 ISE で作成したセキュリティ グループの名前を入力します。

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

ステップ 4　[Protocol] ドロップダウン リストで、[RADIUS] を選択します。

[AAA Server Group] ダイアログボックスの残りのフィールドの完了については、「RADIUS サーバ グループの設定」（P.34-16）を参照してください。

ステップ 5　[OK] をクリックします。ASA が、[AAA Server Group] のリストに、グループを追加します。

ステップ 6　グループにサーバを追加するには、作成した AAA サーバ グループを選択し、[Selected Group] 領域（ペイン下部）の [Server] で [Add] をクリックします。[Add AAA Server] ダイアログボックスが表示されます。

ステップ 7　[Interface Name] フィールドで、ISE サーバが存在するネットワーク インターフェイスを選択します。

ステップ 8　[Server Name or IP Address] フィールドに、ISE サーバの IP アドレスを入力します。

[AAA Server] ダイアログボックスの残りのフィールドの完了については、「グループへの RADIUS サーバの追加」（P.34-18）を参照してください。

ステップ 9　[OK] をクリックします。ASA が、AAA サーバのリストに ISE サーバを追加します。

ステップ 10　[Apply] をクリックして、Cisco TrustSec と連動させるため、ISE サーバとサーバ グループの追加を保存します。

変更内容が実行コンフィギュレーションに保存されます。

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、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。

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 ファイルを使用して 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。

PAC ファイルをインポートする場合、ファイルは ASCII 16 進形式に変換され、非インタラクティブ モードで ASA に送信されます。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。詳細については、「ASA の ISE への登録」（P.39-8）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、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。

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 ファイルをインポートする必要があります。

PAC ファイルをインポートするには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Configuration] > [Firewall] > [Identity By TrustSec] の順に選択します。

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

ステップ 3　[Server Group Setup] 領域で、[Import PAC] をクリックします。[Import PAC] ダイアログボックスが表示されます。

ステップ 4　[Filename] フィールドで、次の形式の 1 つを使用して PAC ファイルのパスとファイル名を入力します。

- disk0：disk0 のパスおよびファイル名
- disk1：disk1 のパスおよびファイル名
- flash：フラッシュのパスおよびファイル名

ステップ 5　[Password] フィールドに、PAC ファイルを暗号化するためのパスワードを入力します。このパスワードは、デバイス クレデンシャルの一部として ISE で設定したパスワードとは関係ありません。

ステップ 6　確認のために [Confirm Password] フィールドにもう一度パスワードを入力します。

ステップ 7　[Import] をクリックします。[Identity By TrustSec] ペインが再表示されます。

ステップ 8　[Apply] をクリックして、変更内容を保存します。

変更内容が実行コンフィギュレーションに保存されます。

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

Cisco TrustSec と ASA の統合のためのデフォルト設定を設定するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Configuration] > [Firewall] > [Identity By TrustSec] の順に選択します。

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

マルチ コンテキスト モードで、ユーザ コンテキストの SXP をイネーブルにします。

ステップ 3　[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。IP アドレスは、IPv4 または IPv6 アドレスを使用できます。

（注）　ピア IP アドレスが到達可能な発信インターフェイスの IP アドレスとして、ASA が SXP 接続のローカル IP アドレスを指定します。設定されたローカル アドレスがインターフェイスの IP アドレスと異なる場合、ASA は SXP ピアに接続できず、syslog メッセージを生成します。

ステップ 4　[Default password] フィールドに、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 文字の暗号化された文字列または 80 文字の ASCII キー ストリングとして指定できます。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

ステップ 5　[Retry Timer] フィールドで、ASA 試行間のデフォルトの時間間隔を入力し、SXP ピア間の新しい SXP 接続を設定します。

ASA は、接続に成功するまで、新しい SXP ピアへの接続を試みます。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。

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、ASA 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。

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。

ステップ 6　[Reconcile Timer] フィールドに、デフォルト リコンサイル タイマーを入力します。

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。

1 ～ 64000 秒の範囲で、リコンサイル タイマー値を秒数で入力します。デフォルトでは、タイマー値は 120 秒です。

（注）　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 秒を指定できません。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。

ステップ 7　[Apply] をクリックして、デフォルト設定内容を保存します。

変更内容が実行コンフィギュレーションに保存されます。

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。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Configuration] > [Firewall] > [Identity By TrustSec] の順に選択します。

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

ステップ 3　[Add] をクリックします。[Add Connection] ダイアログボックスが表示されます。

ステップ 4　[Peer IP Address] フィールドに、SXP ピアの IPv4 アドレスまたは IPv6 アドレスを入力します。ピア IP アドレスは、ASA 発信インターフェイスからアクセスできる必要があります。

ステップ 5　（任意）[Source IP Address] フィールドに、SXP 接続のローカル IPv4 または IPv6 アドレスを入力します。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。

ステップ 6　[Password] ドロップダウン リストから、次の値の 1 つを選択し、SXP 接続に認証キーを使用するかどうかを指定します。

- Default：SXP 接続用に設定されたデフォルト パスワードを使用します。

  「Security Exchange Protocol（SXP）の設定」（P.39-14）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。

ステップ 7　（任意）[Mode] ドロップダウン リストから、次の値の 1 つを選択し、SXP 接続のモードを指定します。

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

ステップ 8　[Role] ドロップダウン リストから、SXP 接続のスピーカーまたはリスナーのどちらとして ASA 動作するを指定します。

- 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。

「ASA での送信者および受信者のロール」（P.39-6）を参照してください。

ステップ 9　[OK] をクリックします。ピアが、[COnnection Peers] リストに表示されます。

ステップ 10　[Apply] をクリックして設定値を保存します。

変更内容が実行コンフィギュレーションに保存されます。

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。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。

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。

環境データをリフレッシュするには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Configuration] > [Firewall] > [Identity By TrustSec]

コマンド	目的
cts refresh environment-data **例：** `hostname(config)# cts refresh environment-data`	ISE からの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。

の順に選択します。

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

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

セキュリティ ポリシーの設定

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。

- アクセスルールを設定するのは、Chapter 46, “Configuring Access Rules.”
- 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.20-8）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 46, “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。

Cisco TrustSec と統合された ASA のモニタリング

ASA の Cisco TrustSec をモニタするには、ASDM の次のパスの 1 本を選択します。

パス	目的
[Monitoring] > [Properties] > [Identity By TrustSec] > [SXP Connections]	Cisco TrustSec インフラストラクチャおよび SXP コマンドの設定デフォルト値が表示されます。
	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。
[Monitoring] > [Properties] > [Connections]	すべての SXP 接続のデータを表示します。セキュリティ グループ テーブル値、セキュリティ グループの名前、IP アドレスでデータが表示されるように IP アドレス セキュリティ グループのテーブル マップ エントリにフィルタに掛けます。
[Monitoring] > [Properties] > [Identity By TrustSec] > **[Environment Data]**	ASA のセキュリティ グループ テーブルに含まれる Cisco TrustSec 環境情報を表示します。
	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。
[Monitoring] > [Properties] > [Identity By TrustSec] > [IP Mapping]	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。セキュリティ グループ テーブル値、セキュリティ グループの名前、IP アドレスでデータが表示されるように IP アドレス セキュリティ グループのテーブル マップ エントリにフィルタに掛けます。 **ヒント** [Where Used] をクリックして、選択したセキュリティ グループ オブジェクトが ACL で使用されている場所、もしくはセキュリティ グループ オブジェクトにネストされている場所を表示します。
[Monitoring] > [Properties] > [Identity By TrustSec] > [PAC]	ISE から ASA にインポートされた PAC ファイルに関する情報を表示します。PAC ファイルの有効期限が切れた場合、または有効期限切れ 30 日以前を過ぎると警告メッセージが表示されます。

Cisco TrustSec 統合の ASA 機能履歴

表 39-3 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。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 39-3　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 機能を活用できます。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。 次の画面が導入または変更されました。 [Configuration] > [Firewall] > [Identity By TrustSec] [Configuration] > [Firewall] > [Objects] > [Security Groups Object Groups] [Configuration] > [Firewall] > [Access Rules] > [Add Access Rules] [Monitoring] > [Properties] > [Identity By Tag]。