Cisco TrustSec

Cisco TrustSec の機能の履歴

次の表に、このモジュールで説明する機能のリリース情報とプラットフォームサポート情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能名と説明	サポートされるプラットフォーム
Cisco IOS XE 26.1.1	IPv6 用 RADIUS を介した CTS ポリシーサーバーリスト有効化：IPv6 用 RADIUS を介した CTS ポリシーサーバーリスト有効化のサポートが導入されました。	Cisco C9350 シリーズ スマートスイッチ Cisco C9610 シリーズ スマートスイッチ
Cisco IOS XE 26.1.1	IPv6 を介した PAC ダウンロード：IPv6 を介した PAC ダウンロードのサポートが導入されました。	Cisco C9350 シリーズ スマートスイッチ Cisco C9610 シリーズ スマートスイッチ

リリース	機能名と説明	サポートされるプラットフォーム
Cisco IOS XE 17.18.1	Cisco TrustSec：Cisco TrustSec は、信頼できるネットワークデバイスのドメインを確立することによってセキュアネットワークを構築します。ドメイン内の各デバイスはそのピアによって認証され、デバイス間の通信は、暗号化、メッセージ整合性チェック、データパスリプレイ防止メカニズムを使用して保護されます。	Cisco C9350 シリーズ スマートスイッチ Cisco C9610 シリーズ スマートスイッチ

Cisco TrustSec

Cisco TrustSecは、信頼できるネットワークデバイスのドメインを確立することによってセキュアネットワークを構築します。ドメイン内の各デバイスはそのピアによって認証され、デバイス間の通信は、暗号化、メッセージ整合性チェック、データパスリプレイ防止メカニズムを使用して保護されます。

Cisco TrustSec の主要コンポーネント

Cisco TrustSec のアーキテクチャには、次の 3 種類の主要コンポーネントが含まれます。

- 認証済みネットワーキング インフラストラクチャ

  Cisco TrustSec ドメインを開始するために最初のデバイス（シードデバイス）が認証サーバーで認証された後、ドメインに追加された新しい各デバイスはドメイン内のピアデバイスにより認証されます。ピアは、ドメインの認証サーバーに対する媒介として動作します。それぞれの新たに認証されたデバイスは認証サーバーによって分類され、アイデンティティ、ロールおよびセキュリティ ポスチャに基づいてセキュリティ グループ番号が割り当てられます。

- セキュリティグループベースのアクセス制御：

  Cisco TrustSec ドメイン内のアクセスポリシーは、トポロジとは無関係で、ネットワークアドレスではなく送信元デバイスおよび宛先デバイスのロール（セキュリティグループ番号で指定）に基づいています。個々のパケットには、送信元のセキュリティ グループ番号のタグが付けられます。

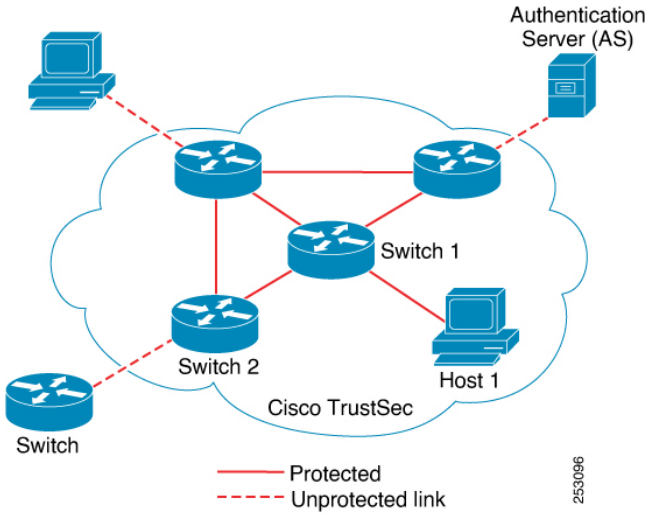
- セキュア通信：

  暗号化対応ハードウェアにより、暗号化、メッセージ整合性チェック、データパスリプレイ保護メカニズムの組み合わせを使用して、ドメイン内のデバイス間の各リンクでの通信を保護できます。

図は、以下を含む Cisco TrustSec ドメインを示しています。

- Cisco TrustSec ドメイン内のエンドポイントデバイスと複数のネットワーキングデバイス
- Cisco TrustSec ドメイン外のエンドポイントデバイスと 1 台のネットワーキングデバイスこれはデバイスが Cisco TrustSec 対応デバイスではないか、デバイスのアクセスが拒否されているためです。
- Cisco TrustSec ドメイン外の認証サーバー認証サーバーは、Cisco Identity Services Engine（Cisco ISE）、または Cisco Secure Access Control System（Cisco ACS）のいずれかを使用できます。

***Figure 1: Cisco TrustSec* ドメイン**



Cisco TrustSec 認証プロセスでのロール

Cisco TrustSec 認証プロセスには、以下のロールがあります。

- Supplicant

  Cisco TrustSec ドメイン内のピアに接続されており、Cisco TrustSec ドメインへのアクセスを試行している非認証デバイス。

- 認証サーバー

  サプリカントのアイデンティティの確認を行い、Cisco TrustSec ドメイン内のサービスへのサプリカントのアクセスを制御するポリシーを割り当てるシステム。

- オーセンティケータ

  すでに Cisco TrustSec ドメインの一部であり、認証サーバーに代わって新しいサプリカントピアを認証する権限のある認証済みデバイス。

認証プロセスのシーケンス

サプリカントとオーセンティケータ間で接続が確立される際、プロセスは通常次の手順に従います。

1. 認証（802.1X）：

   サプリカントのログイン情報は、認証サーバーと、中間デバイスとして機能するオーセンティケータによって検証されます。相互認証がサプリカントとオーセンティケータの間で行われます。

2. Authorization:

   認証サーバーは、サプリカントのアイデンティティに基づいて、接続された両方のピアにセキュリティグループの割り当てやアクセス制御リスト（ACL）などの認証ポリシーを発行します。認証サーバーは、各ピアのアイデンティティを他のサーバーと共有し、適切なポリシーをリンクに適用できるようにします。

これらの手順が正常に完了すると、オーセンティケータはリンクを未認証（ブロッキング）状態から認証済み状態に移行させ、サプリカントはCisco TrustSec ドメインに参加できるようになります。

アイデンティティとログイン情報

以下のセクションでは、次の基本要素と、それらが TrustSec デプロイメント内でどのように連携するかについて説明します。

- デバイスアイデンティティ
- デバイスのログイン情報
- ユーザーのログイン情報
- Protected Access Credential（PAC）

デバイス ID

Cisco TrustSec は、IP アドレスまたは MAC アドレスの代わりに、割り当てられたデバイス名（デバイス ID）を使用して、スイッチを一意に識別します。これらのデバイス ID は、認証時の認証ポリシールックアップとパスワードルックアップに使用されます。

デバイスのクレデンシャル

Cisco TrustSec はパスワードベースのログイン情報をサポートし、相互認証に MSCHAPv2 を使用します。

デバイスのログイン情報は、EAP-FAST フェーズ 0（PAC プロビジョニング）交換中に使用されます。後続のリンク起動では、プロビジョニングされた PAC を利用して、EAP-FAST フェーズ 1 および 2 を使用します。

ユーザークレデンシャル

Cisco TrustSec には、エンドポイント装置の特定タイプのユーザークレデンシャルは必要ありません。認証サーバーでサポートされている任意の認証メソッド（Cisco ACS 5.1 の場合は MSCHAPv2、GTC、RSA OTP など）を使用できます。

Protected Access Credential

PAC は、クライアントとサーバーの相互認証のための固有の共有ログイン情報であり、Public Key Infrastructure（PKI）とデジタル証明書が不要になります。

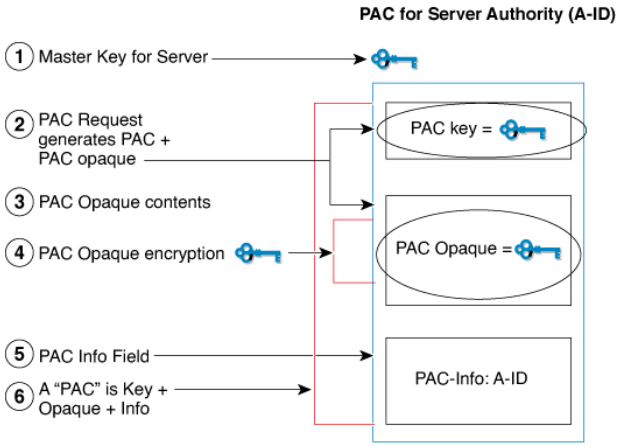
PAC の作成手順

1. サーバーの認証局アイデンティティ（A-ID）では、ローカルマスターキーが保持されます。
2. クライアント（イニシエータ アイデンティティ（I-ID））が PAC を要求すると、サーバーは一意の PAC キーと PAC-Opaque フィールドを生成します。
3. PAC-Opaque フィールドに含まれる PAC キー、I-ID、およびキー有効期間は、マスターキーで暗号化されています。
4. A-ID を含む PAC-Info フィールドが作成されます。
5. PAC は、自動的にクライアントに配布またはインポートされます。

Note サーバーは PAC または PAC キーを保持しないため、ステートレス EAP-FAST サーバーが有効になります。

次の図は、PAC の構造を示しています。PAC は、PAC-Opaque、PAC Key、および PAC-Info フィールドで構成されます。PAC-Info フィールドには A-ID が含まれます。

Figure 2: PAC のプロセスフロー



PAC のプロビジョニング

- Secure RADIUS では、認証中に PAC キーが各デバイスにプロビジョニングされ、共有秘密が導出されます。
- クライアントは、情報を回復し、アイデンティティを検証するためにサーバーが解釈する、PAC-Opaque フィールドを含む追加の RADIUS 属性を送信します。
- EAP-FAST フェーズ 0 は、自動 PAC プロビジョニングに使用されます。

PAC なし認証

PAC なしモードは、通常、デバイスと Identity Services Engine（ISE）間のセキュア通信に必要な Protected Access Credential（PAC）を不要にすることで、Cisco TrustSec ポリシーの展開をシンプルにします。この方法は、複数の ISE ノードがある環境で特に役立ちます。プライマリが使用できなくなった場合、デバイスは PAC を再確立することなく、セカンダリ ISE ノードにシームレスに接続できるため、サービスの中断が削減されます。

利点

AAA PAC なしの認証では、PAC への依存関係が解消されるため、認証プロセスが合理化されます。結果として拡張性が促進され、ユーザー体験が向上します。また、Zero Trust セキュリティの原則に沿った最新の認証アプローチのサポートが可能になります。

PAC なしの認証ワークフロー

1. PAC なしモードでは、デバイスは、Cisco TrustSec ユーザー名、パスワード、および EAP 属性メッセージを含む RADIUS 要求を送信して認証を開始します。
2. ISE は RADIUS アクセスチャレンジで応答し、EAP-FAST セッションを開始します。

3. EAP-FAST セッションが確立されると、ISE は PAC Opaque および PAC 情報を提供します。PAC Opaque には、EAP-FAST サーバーマスターキーを使用して暗号化された PAC キーとユーザーアイデンティティが含まれています。PAC 情報には、サーバーアイデンティティと存続可能時間（TTL）タイマーが含まれています。
4. 次いで PAC Opaque が、ISE への後続の Cisco TrustSec RADIUS 要求のメッセージ オーセンティケータ フィールドに埋め込まれます。これにより、環境データとセキュリティ グループ アクセス コントロール リスト（SGACL）ポリシーをセキュアにダウンロードできるようになります。

Cisco TrustSec のガイドライン

一般的な注意事項

- FIPS モードで Cisco TrustSec はサポートされていません。
- Cisco TrustSec は、IPSG が有効になっている純粋なブリッジングドメインでは設定できません。
- Cisco TrustSec は、セキュリティ アソシエーション プロトコル（SAP）をサポートしていません。

アイデンティティとログイン情報のガイドライン

無効なデバイス ID が指定された場合、Protected Access Credential（PAC）のプロビジョニングが失敗し、ハング状態のままになります。PAC をクリアし、正しいデバイス ID とパスワードを設定した後でも、PAC は失敗します。

回避策として、Cisco Identity Services Engine（ISE）で、PAC が機能するように**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [RADIUS]**メニューの [異常なクライアントの抑制（Suppress Anomalous Clients）] オプションをオフにします。

Cisco TrustSec ログイン情報の設定

このタスクでは、デバイスにデバイス ID、パスワード、および認証メソッドを設定できます。

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

特権 EXEC モードを有効にします。

プロンプトが表示されたらパスワードを入力します。

Step 2 **cts credentials id** *cts-id* **password** *password*

Example:

```
Device# cts credentials id ctsid password abcd
```

EAP-FAST で他の Cisco TrustSec デバイスに対して認証するときにこのデバイスが使用する Cisco TrustSec デバイス ID を設定します。Cisco TrustSec では、ネットワーク内の各デバイスがそれ自体を固有に識別する必要があるためです。

- *cts-id* 引数は、最大 32 文字で大文字と小文字を区別します。
- *password* 引数は、EAP-FAST を使用して他の Cisco TrustSec デバイスで認証するときにこのデバイスが使用するパスワードです。

Step 3 **configure terminal**

Example:

```
Device(config)# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

Step 4 **aaa new-model**

Example:

```
Device(config)# aaa new-model
```

アクセスコントロールの新しいコマンドおよび機能を有効にします（以前のコマンドを無効にします）。

Step 5 **aaa authentication dot1x default group radius**

Example:

```
Device(config)# aaa authentication dot1x default group radius
```

IEEE 802.1X を実行しているインターフェイスでの認証に RADIUS サーバーを使用することを指定します。

Step 6 **cts authorization list network** *list-name*

Example:

```
Device(config)# cts authorization list network cts-mlist
```

Cisco TrustSec シードデバイスが使用する AAA サーバーのリストを指定します。

Step 7 **aaa authorization network** *list-name* **group radius**

Example:

```
Device(config)# aaa authorization network cts-mlist group radius
```

RADIUS サーバーからのすべてのネットワーク関連サービス要求に、Cisco TrustSec 承認リスト名を指定します。

Step 8 **exit**

Example:

```
Device(config)# exit
```

グローバル コンフィギュレーション モードを終了します。

Step 9 **show cts server-list**

Example:

```
Device# show cts server-list
```

Cisco TrustSec シードデバイスの RADIUS サーバー設定を表示します。

Step 10 **show cts credentials**

Example:

```
Device# show cts credentials
```

Cisco TrustSec（CTS）デバイス ID を表示します。保存されたパスワードは表示されません。

PAC のダウンロード

Cisco TrustSec Protected Access Credential（PAC）のダウンロードは、以下のようなセキュリティプロセスです。

- ISE を使用してネットワークデバイスのセキュアなアイデンティティを確立します。
- RADIUS トランスポート層で EAP-FAST プロトコルを使用します。
- TrustSec 環境データと SGACL ポリシーを取得するための前提条件として機能します。

IPv6 を介した PAC のダウンロード

IPv6 を介した PAC のダウンロードは、以下のようなネットワークトランスポート機能です。

- リテラル IPv6 アドレスを使用して、ポリシーサーバーとの RADIUS セッションを確立します。
- EAP-FAST プロトコルを使用して、IPv6 トランスポートを介して PAC を取得します。
- サーバーアドレスタイプが変更された場合のログイン情報の再取得を自動化します。

この機能により、TrustSec ポリシープレーンが有効になり、IPv6 専用環境またはデュアルスタック環境で動作します。

IPv6 を介した PAC ダウンロード用のポリシーサーバーバージョン

IPv6 を介した PAC のダウンロードは、Cisco IOS XE 26.1.1 リリースからサポートされており、ポリシーサーバー（ISE）バージョン 3.5 以降が必要です。

IPv6 を介した PAC のダウンロードの利点

IPv6 を介した PAC のダウンロードの主な利点は次のとおりです。

- アドレスの柔軟性：ポリシーサーバー識別用のリテラル IPv6 アドレスをサポートします。これにより、デバイスが DNS を介してサーバーの場所を解決できます。
- トランスポートセキュリティ：基盤となるトランスポートを IPv4 から IPv6 に移行する際、EAP-FAST セッションのセキュリティを維持します。
- 動的更新：ユーザーが設定でアドレスタイプを切り替えたときに、PAC 要求を自動的に再トリガーすることで、デバイスとポリシーサーバーの同期が維持されます。

IPv6 を介した PAC ダウンロード用の ISE バージョン

IPv6 を介した PAC のダウンロードは、Cisco IOS XE 26.1.1 リリースからサポートされており、ISE バージョン 3.5 以降が必要です。

PAC ダウンロードの制約事項

PAC ダウンロード用にポリシーサーバーを設定する場合は、以下の制約事項に従います。

- デバイスは、RADIUS サーバー設定のリンクローカル IP アドレスおよび完全修飾ドメイン名（FQDN）をサポートしていません。
- PAC ダウンロードでの IPv4 アドレスタイプと IPv6 アドレスタイプのサポートは、相互に排他的ではありません。デバイスで IPv4 と IPv6 両方のアドレスタイプを設定した場合、いずれかの設定、つまり最新の設定のみが有効になります。
- デバイスは、混合モードのアドレスタイプ（デバイスの送信元アドレスタイプが IPv4 で ISE が IPv6 タイプであるなど）をサポートしていません。

PAC ダウンロード用のポリシーサーバーの設定

ポリシーサーバーへの IPv6 接続を確立し、Cisco TrustSec（CTS）の操作に必要な PAC を取得するには、この手順を使用します。同様に、IPv4 経由の PAC ダウンロードには IPv4 アドレスを使用します。

新しい TrustSec 対応デバイスを設定する場合や、既存のポリシーサーバー接続を IPv6 トランスポートに移行する場合に、このタスクを実行します。

Before you begin

- RADIUS サーバー（ISE）が、IPv6 または IPv4 アドレスを介して到達可能であることを確認します。
- 共有秘密（PAC キー）が使用可能であることを確認します。

Procedure

Step 1 ポリシーサーバーで使用される IPv4 または IPv6 アドレス、認証ポート、およびアカウンティングポートを指定して、RADIUS サーバーを設定します。

Example:

```
Switch(config)#radius server test-server
Switch(config-radius-server)#address ipv6 2001::10 auth-port 1812 acct-port 1813
```

デバイスは、RADIUS サーバーの完全修飾ドメイン名（FQDN）の使用をサポートしていません。

Step 2 RADIUS サーバーの PAC キーを定義します。

Example:

```
Switch(config-radius-server)#pac key testkey123
```

この手順により、デバイスが認証され、PAC 取得用の EAP-FAST セッションを開始できます。

このキーは、ISE サーバーで設定された共有秘密と一致している必要があります。

Step 3 PAC プロビジョニングステータスを監視します。

a) CTS PAC の詳細を確認します。

Example:

```
Switch#show cts pac
AID: 60DABBF8AD435A7B63900EE07E68D2FD
PAC-Info:
  PAC-type = Cisco Trustsec
  AID: 60DABBF8AD435A7B63900EE07E68D2FD
  I-ID: ha_senth_cat9k
  A-ID-Info: Identity Services Engine
  Credential Lifetime: 16:17:20 UTC Mon Feb 24 2025
PAC-Opaque: 000200B800030001000...705E
Refresh timer is set for 12w4d
Switch#
```

b) CTS プロビジョニングキューの詳細を確認します。

Example:

```
Switch#show cts provisioning queue
Server: 2001:420:54FF:4::400:11, Type: Radius, Provisioned: YES
AID: 3ec5d7e02bde9fd04c453918a5e2d3b4
```

デバイスは、ポリシーサーバーとのセキュアなセッションを確立し、IPv4 または IPv6 トランスポートを介して PAC を取得しました。これにより、後続の TrustSec ポリシーのダウンロードが可能になります。

Cisco TrustSec 環境データ

環境データは、Cisco TrustSec 機能を補足する運用データで構成されます。デバイスから Cisco ISE への環境データ要求は、次のデータで構成されます。

- デバイス名：デバイスの名前を指定します。
- デバイス機能：追加データを指定します。

Cisco ISE からデバイスへの環境データ応答は、次のデータで構成されます。

- デバイスのセキュリティグループタグ（SGT）：デバイス名に基づいて Cisco ISE から取得されます。
- サーバーリスト：Cisco ISE で指定された Cisco TrustSec サーバーのリストを表示します。
- SG-Name テーブル：SGT とデバイス名の間のマッピングを表示します。SGT は数字で表示され、デバイス名はテキスト形式で表示されます。
- リフレッシュ時間：環境データがリフレッシュされる時間を示します。

Note

- Cisco TrustSec 環境のデータ更新の一環として、最後に受信したサーバーが削除され、新しく受信したサーバーがサーバーリストに追加されます。更新後、サーバーリストの統計がゼロから再開され、サーバーのステータスが [Inactive] に設定されます。また、IP アドレスの状態が [Reachable] に設定されます。次に、デバイスは、後続のポリシー要求と応答に基づいてサーバーの統計とステータスを更新します。
- Cisco IOS XE Bengaluru 17.4.1 以降では、VRF を認識するように自動テスターを設定できます。**automate-tester** コマンドで **vrf** キーワードを使用すると、デフォルト以外の VRF の自動テスト機能を有効化します。

  VRF 対応の自動テスターを機能させるには、**global config ipv4/ipv6 source interface***interface-name* **vrf***vrf-name* コマンドを設定する必要があります。

IPv6 用 RADIUS を介した CTS ポリシーサーバーリストの有効化

Cisco IOS XE リリース 26.1.1 以降、ISE は、IPv4 アドレスに加えて、PSN の IPv6 アドレスを環境データの一部としてデバイスにプッシュします。デバイスは、SGACL ポリシーをダウンロードすると、これらの PSN IPv6 アドレスを使用して ISE に到達します。

このリリースより前は、環境データの一部として受信される ISE からのサーバーリスト IP は、IPv4 タイプのみでした。

SGACL ポリシーをダウンロードするためのサーバーの選択とフェールオーバーロジック

デバイスは、ISE から IPv4 アドレスと IPv6 アドレスの両方を含むサーバーリストを受信すると、特定の選択ルールおよびフェールオーバーのルールに従います。

- デバイスは、ラウンドロビンフェールオーバーメソッドを使用してアクティブなサーバーを選択します。
- リスト内のプライマリサーバーが到達不能になった場合、デバイスは、シーケンス内の次に使用可能なサーバーへの接続を自動的に試行します。
- デバイスは通常、SGACL ポリシーダウンロード用に設定された送信元インターフェイス アドレス タイプと一致するサーバーアドレスタイプを優先します。

RADIUS を介した CTS ポリシーサーバーリスト有効化の制約事項

デバイスは、混合モードのアドレスタイプ（デバイスの送信元アドレスタイプが IPv4 で ISE が IPv6 タイプであるなど）をサポートしていません。

IPv6 用の CTS ポリシーサーバーリスト有効化の確認

デバイスへの環境データのダウンロードの一環として、IPv6 サーバーリストを ISE から受信するかどうかを確認するには、この手順を使用します。

Procedure

ISE サーバーからデバイスにダウンロードされた環境データの詳細を確認します。

Example:

```
Switch# show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Service Info Table:
Local Device SGT:
  SGT tag = 2-48:TrustSec_Devices
Server List Info:
Installed list: CTSServerList1-0003, 3 server(s):
 *Server: 2001:420:54FF:4::400:11, port 1812, A-ID 1695AF86D38B22DC7C9500408E2DD35D
          Status = DEAD
          auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs

 *Server: 2001:420:54FF:4::400:12, port 1812, A-ID 1695AF86D38B22DC7C9500408E2DD35D
          Status = ALIVE
          auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs

 *Server: 2001:420:54FF:4::400:13, port 1812, A-ID 1695AF86D38B22DC7C9500408E2DD35D
          Status = DEAD
          auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Security Group Name Table:
```

```
    0-48:Unknown
    2-48:TrustSec_Devices
    3-62:Network_Services
    4-56:Employees
    5-48:Contractors
    6-49:Guests
    7-48:Production_Users
    8-49:Developers
    9-49:Auditors
    10-48:Point_of_Sale_Systems
    11-48:Production_Servers
    12-0177:Development_Servers
    13-48:Test_Servers
    14-56:PCI_Servers
    15-48:BYOD
    16-01:sgt_101
Environment Data Lifetime = 86400 secs
Last update time = 05:26:38 UTC Tue Jul 1 2025
Env-data expires in   0:23:52:36 (dd:hr:mm:sec)
Env-data refreshes in 0:23:52:36 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
Retry_timer (60 secs) is not running
Switch#
```

セキュリティグループとセキュリティグループタグ

以下のセクションでは、セキュリティグループとセキュリティグループタグについて説明します。

セキュリティ グループ

セキュリティグループは、アクセスコントロールポリシーを共有するユーザー、エンドポイントデバイス、およびリソースのコレクションです。Cisco ISE または Cisco Secure ACS では、これらのグループは管理者が定義します。新しいユーザーおよびデバイスが Cisco TrustSec（CTS）ドメインに参加すると、認証サーバーは、これらを適切なセキュリティグループに自動的に割り当てます。各グループは、Cisco TrustSec ドメイン内でグローバルに認識される一意の 16 ビットセキュリティグループ番号を指定されます。セキュリティグループの総数は、認証済みのネットワークエンティティの数によって決定されます。管理者がこれらのグループ番号を手動で設定する必要はありません。

セキュリティグループタグとパケットタギング

デバイスが認証されると、Cisco TrustSec は、そのデバイスから発信されるすべてのパケットにセキュリティグループタグ（SGT）をタグ付けします。このタグには、デバイスに割り当てられたセキュリティグループ番号が含まれており、Cisco TrustSec ヘッダー内のネットワーク全域をパケットとともに移動します。SGT は、企業のネットワーク全体における送信元のアクセス権限を定義する単一のラベルとして機能します。

送信元および宛先グループタグ

SGTは、パケットの送信元のセキュリティグループを表すため、送信元SGTと呼ばれることがよくあります。パケットを受信するデバイスは、宛先セキュリティグループと呼ばれるセキュリティグループにも割り当てられます。わかりやすくするため、これを宛先グループタグ（DGT）と呼ぶことができますが、Cisco TrustSecパケット自体には宛先デバイスのセキュリティグループ番号が含まれていません。

送信元セキュリティグループタグの決定

パケットがCisco TrustSecドメインに入る際、入力ポイントのネットワークデバイスは送信元SGTを識別する必要があります。これにより、TrustSec環境への転送の前にパケットに適切にタグ付けすることができます。同様に出力デバイスは、セキュリティ グループ アクセス コントロール リスト（SGACL）を適用するために、パケットのSGTを特定する必要があります。

ネットワークデバイスがパケットのSGTを特定するいくつかの方法があります。

1. 認証サーバーからのポリシー取得

   Cisco TrustSec認証プロセス後、ネットワークデバイスは認証サーバーからポリシー情報を取得します。この情報には、ピアデバイスが信頼できるかどうかが含まれます。ピアデバイスが信頼できない場合、認証サーバーはSGTを提供します。ネットワークデバイスは、SGTをそのピアから受信したすべてのパケットに適用します。

2. パケットに含まれるSGT

   パケットが信頼できるピアデバイスから受信された場合、パケットにはすでにSGTが付与されています。この状況は、特定のパケットのCisco TrustSecドメインにおける最初のエントリポイントではないデバイスに当てはまります。

3. アイデンティティ ポート マッピング（IPM）

   アイデンティティ ポート マッピングを使用して、ネットワーク管理者は、ピアデバイスに接続されているリンクにアイデンティティを手動で割り当てることができます。その後ネットワークデバイスは、SGTおよび信頼ステータスを含むポリシー情報を認証サーバーに要求します。

4. 送信元IPアドレスルックアップ

   特定のシナリオでは、送信元IPアドレスに基づいてパケットにSGTを割り当てるようにポリシーを設定できます。SGT交換プロトコル（SXP）を使用して、IPアドレスとSGT間のマッピングテーブルに自動的に入力することもできます。

宛先セキュリティグループタグの決定

Cisco TrustSecドメインの出力ネットワークデバイスは、SGACLを適用するための宛先セキュリティグループ（DGT）の識別を担当します。パケットの宛先セキュリティグループを決定するため、ネットワークデバイスは、パケットの送信元セキュリティグループを決定するために使用さ

れるのと同じ方法を使用します（宛先グループ番号はパケットのタグに含まれていないため、パケットのタグからのグループ番号の取得を除く）。

特定のシナリオでは、入力デバイスまたはその他の中間ネットワークデバイスが宛先グループ情報にアクセスできることがあります。その場合、出力点だけではなく、該当するデバイスでもSGACL を適用できます。

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。