Cisco TrustSec の概要

Cisco TrustSec は、論理グループ権限を示すためにタグを使用します。このタグは、セキュリティグループタグ（SGT）と呼ばれ、アクセスポリシーで使用されます。SGT は、シスコのスイッチ、ルータ、およびファイアウォールでトラフィックを適用するために使用されます。Cisco TrustSec は、分類、伝達、および適用の 3 つのフェーズで定義されます。

ユーザーとデバイスがネットワークに接続すると、ネットワークは、特定のセキュリティグループを割り当てます。このプロセスは「分類」と呼ばれます。分類は、認証の結果に基づいて行うことも、SGT を IP、VLAN、またはポートプロファイルに関連付けることによって行うこともできます。

ユーザートラフィックが分類されると、SGT は、分類が行われた場所から適用アクションが呼び出される場所に伝達されます。このプロセスは「伝播」と呼ばれます。Cisco TrustSec には、インラインタギングと SXP の 2 つの SGT 伝達方式があります。

インラインタタギングの場合、SGT は、イーサネットフレームに組み込まれます。イーサネットフレーム内に SGT を埋め込む機能には、特定のハードウェアサポートが必要です。そのため、ハードウェアサポートのないネットワークデバイスは、SXP（SGT 交換プロトコル）と呼ばれるプロトコルを使用します。SXP は、SGT から IP アドレスへのマッピングを共有するために使用されます。これにより、SGT 伝達がパス内の次のデバイスに対して続行されます。

最終的に、適用デバイスが、タグ情報に基づいてトラフィックを制御します。シスコのファイアウォール、ルータ、またはスイッチを TrustSec の適用ポイントとすることができます。適用デバイスは送信元 SGT を取得し、それを宛先 SGT と照合して、トラフィックを許可するか拒否するかを決定します。適用デバイスがシスコのファイアウォールである場合、そのデバイスは、単一のファイアウォールルールで同じ送信元 SGT を使用して、ステートフル ファイアウォール処理と IPS ディープ パケット インスペクションも許可します。

（注） Cisco TrustSec 機能は、Cisco 1000 シリーズ サービス統合型ルータのスイッチポートではサポートされません。

（注） CTS 適用が有効になっている場合、デバイスは、ISE からポリシーをダウンロードしようとします。これには、RADIUS サーバーが設定されている必要があります。RADIUS サーバーが設定されていないと、ポリシーをダウンロードできず、Syslog ファイルにエラーが記録されます。

分類と適用の詳細については、『Cisco TrustSec Quick Start Configuration Guide』を参照してください。

- SGT インライン タギング （2 ページ）
- Protected Access Credential（PAC） （3 ページ）
- PAC Provisioning （4 ページ）
- ハイ アベイラビリティ セットアップでのデバイスの展開 （4 ページ）
- CTS ログイン情報 （5 ページ）
- SGT インライン タギングの設定 （5 ページ）
- CTS ログイン情報の設定 （7 ページ）
- 例：SGT インライン タギングの設定 （8 ページ）

SGT インライン タギング

CTS ドメイン内の各セキュリティグループは、「スケーラブルグループタグ」（SGT）と呼ばれる一意の 16 ビットタグが割り当てられます。SGT はネットワーク全体で送信元の権限を示す単一ラベルです。これは、ネットワーク ホップ間で順番に伝搬され、任意の中間デバイス（スイッチ、ルータ）はこれによってアイデンティティ タグに基づいたポリシーを適用できます。

CTS 対応デバイスには、MAC（L2）レイヤ内に組み込まれた SGT を持つパケットを送受信できる、ハードウェア機能が組み込まれています。この機能は、「L2-SGT インポジション」と呼ばれます。これにより、デバイスのイーサネット インターフェイスで L2-SGT インポジションを有効にできるため、そのデバイスはネクスト ホップ イーサネット ネイバーに運ばれるパケット内に SGT を挿入できるようになります。SGT-over-Ethernet は、クリアテキスト（非暗号化）イーサネット パケットに組み込まれた SGT のホップバイホップの伝達方式です。インライン アイデンティティ伝達はスケーラブルで、ほぼラインレートのパフォーマンスを提供し、コントロール プレーンのオーバーヘッドを防ぎます。

SXPv4 機能を備えた Cisco TrustSec は、CTS メタ データ（CMD）ベースの L2-SGT をサポートします。パケットが CTS 対応インターフェイスに入力されると、IP-SGT マッピング データベース（SXP によって構築されたダイナミック エントリや設定コマンドによって構築されたスタティック エントリがある）が分析され、パケットの送信元 IP アドレスに対応する SGT が学習されます。この SGT はパケットに挿入され、CTS ヘッダー内でネットワーク全体に運ばれます。

このタグは、送信元のグループを表しているので、送信元グループ タグ（SGT）としても参照されます。ネットワークの出力エッジでは、パケットの宛先に割り当てられたグループが既知になります。この時点で、アクセス制御を適用できます。CTS を使用すると、セキュリティ

グループアクセス コントロール リスト（SGACL）と呼ばれるアクセス コントロール ポリシーがセキュリティ グループ間で定義されます。任意のパケットから見れば、これは単純にセキュリティ グループから送信され、別のセキュリティ グループに送信されています。

Protected Access Credential（PAC）

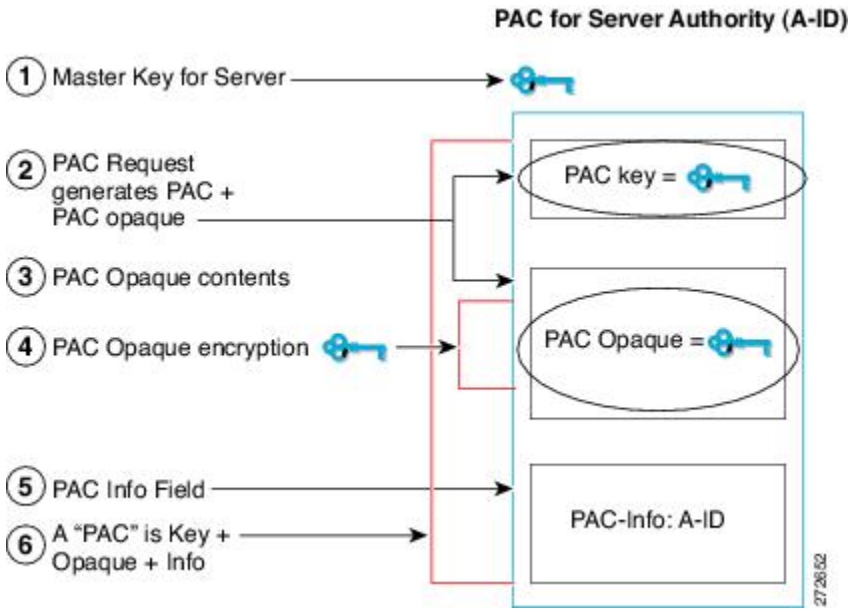
PACは、クライアントとサーバーの相互認証に使用される一意の共有ログイン情報です。これは、特定のクライアントユーザー名およびサーバー権限識別子（A-ID）に関連付けられます。PAC により、Public Key Infrastructure（PKI）およびデジタル証明書が不要になります。

PAC は次の手順で作成します。

1. サーバー A-ID は、サーバーのみが知っているローカルキー（マスターキー）を保持します。
2. クライアント（この文脈ではイニシエータ アイデンティティ（I-ID）と呼ばれる）がサーバーに PAC を要求すると、サーバーはこのクライアントに対してランダムに一意の PAC キーと PAC-Opaque フィールドを生成します。
3. PAC-Opaque フィールドには、ランダムに生成された PAC キーと、I-ID やキーの有効期間などの他の情報が含まれます。
4. PAC-Opaque フィールドの PAC キー、I-ID、およびライフタイムは、マスターキーで暗号化されます。
5. A-ID を含む PAC-Info フィールドが作成されます。
6. PAC は、クライアントに自動的に配布またはインポートされます。

（注） サーバーは PAC または PAC キーを保持しないため、EAP-FAST サーバーはステートレスになります。

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。



PAC Provisioning

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。RADIUS ACS は各デバイスの PAC キーを保存しないため、クライアントは、PAC-Opaque フィールドを含む追加の RADIUS 属性も送信する必要があります。PAC-Opaque フィールドは可変長のフィールドであり、サーバーだけが解釈して、必要な情報を回復し、ピアのアイデンティティと認証を検証することができます。たとえば、PAC-Opaque フィールドには PAC キーと PAC のピアアイデンティティが含まれていることがあります。

PAC-Opaque フィールドの形式と内容は、発行元の PAC サーバーによって異なります。RADIUS サーバーは、PAC-Opaque フィールドから PAC キーを取得し、クライアントと同じ方法で共有秘密を導出します。Secure RADIUS は、共有秘密の導出方法のみを変更し、その使用方法は変更しません。

EAP-FAST フェーズ 0 は、PAC を使用してクライアントを自動的にプロビジョニングするために使用されます。

ハイアベイラビリティセットアップでのデバイスの展開

HA セットアップでデバイスを展開する場合は、次の手順を実行します。

1. HA セットアップに含まれるすべてのデバイスのログイン情報をクリアします。
2. スタックセットアップを起動し、デバイスロール（アクティブ、スタンバイ、およびメンバー）を確立します。
3. アクティブデバイスのログイン情報を設定します。ログイン情報を設定するには、**cts credentials id** *id* **password** *password* コマンドを使用します。

（注） 既存のスタックに新しいデバイスを追加する場合は、新しいデバイスのログイン情報をクリアしてから、既存のスタックセットアップに追加してください。

CTS ログイン情報

CTS では、ネットワーク内の各デバイスがそれ自体を一意に識別する必要があります。TrustSec ネットワーク デバイス アドミッション コントロール（NDAC）認証で使用する場合は、**cts credentials** コマンドを使用して、別の Cisco TrustSec デバイスでの認証時や、EAP-FAST を使用した PAC（Protected Access Credentials）のプロビジョニングのために、このデバイスが使用する Cisco TrustSec デバイス ID およびパスワードを指定します。CTS のクレデンシャル情報は startup-config ではなくキーストアに保存されているため、CTS のクレデンシャルの状態取得は不揮発性生成（NVGEN）プロセスでは実行されません。これらのクレデンシャルは、キーストアで保存され、running-config を保存する必要性がなくなります。CTS デバイス ID を表示するには、**show cts credentials** コマンドを使用します。保存されたパスワードは表示されません。

デバイス ID またはパスワードを変更するには、コマンドを再入力します。キーストアをクリアするには、**clear cts credentials** コマンドを使用します。

（注） CTS デバイス ID が変更された場合、Protected Access Credential（PAC）は古いデバイス ID に関連付けられており、新しいアイデンティティに対しては有効でないため、すべての PAC はキーストアから消去されます。

SGT インライン タギングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** {**gigabitethernet** *port* | **vlan** *number*}
4. **cts manual**
5. **policy static sgt** *tag* [**trusted**]
6. **end**
7. **show cts interface brief**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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。
ステップ 3	**interface** {**gigabitethernet** *port* | **vlan** *number*} 例： `Device(config)# interface gigabitethernet 0`	CTS SGT の認証と転送が有効なインターフェイスを開始します。
ステップ 4	**cts manual** 例： `Device(config-if)# cts manual`	CTS SGT の承認と転送用のインターフェイスを有効化します。CTS 手動インターフェイス コンフィギュレーション モードを開始します。 （注） サブインターフェイスを使用している場合は、**config-if** モード（親インターフェイス）ではなく **config-subif** モード（サブインターフェイス）で **cts manual** コマンドを設定します。
ステップ 5	**policy static sgt** *tag* [**trusted**] 例： `Device(config-if-cts-manual)# policy static sgt 77`	インターフェイスでスタティック SGT 入力ポリシーを設定し、インターフェイスで受信する SGT の信頼性を定義します。 （注） **trusted** キーワードは、そのインターフェイスが CTS に信頼されていることを示します。このインターフェイス上のイーサネット パケット内で受信した SGT 値は信頼され、デバイスによって任意の SG 認識型ポリシーの適用または出力タギングに使用されます。
ステップ 6	**end** 例： `Device(config-if-cts-manual)# end`	CTS 手動インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 7	**show cts interface brief** 例：	インターフェイスの CTS 設定の統計情報を表示します。

	コマンドまたはアクション	目的

	`Device# show cts interface brief`
	
	`Interface GigabitEthernet0/0`
	`CTS is enabled, mode: MANUAL`
	`Propagate SGT: Enabled`
	`Peer SGT assignment: Trusted`
	
	`Interface GigabitEthernet0/1`
	`CTS is enabled, mode: MANUAL`
	`Propagate SGT: Disabled`
	`Peer SGT assignment: Untrusted`
	
	`Interface GigabitEthernet0/3`
	`CTS is disabled.`	

CTS ログイン情報の設定

手順の概要

1. **enable**
2. **cts credentials id** *cts-id* **password** *cts-pwd*
3. **show cts credentials**
4. **show keystore**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**cts credentials id** *cts-id* **password** *cts-pwd* 例： `Device# cts credentials id atlas password cisco123`	EAP-FAST を使用して他の Cisco TrustSec（CTS）デバイスで認証するときにこのデバイスが使用する CTS デバイス ID およびパスワードを指定します。
ステップ 3	**show cts credentials** 例： `Device# show cts credentials`	Cisco TrustSec（CTS）デバイス ID を表示します。
ステップ 4	**show keystore** 例： `**Note that the following is the sample output of the command till Cisco IOS XE Everest release`	ソフトウェアまたはハードウェア暗号化キーストアの内容を表示します。

	コマンドまたはアクション	目的
	16.5.** Device# **show keystore** Using software keystore emulation. Keystore contains the following records (S=Simple Secret, P=PAC, R=RSA): Index Type Name ----- ---- ---- 0 S CTS-password 1 P 57366898EEF9D71A6E33C3628CE7EEDE 例： ****Note that the following is the sample output of the command from Cisco IOS XE Everest release 16.6 and above. The Protected Access Credentials (PAC) information is not displayed.**** Device# **show keystore** Using software keystore emulation. Keystore contains the following records (S=Simple Secret, P=PAC, R=RSA): Index Type Name ----- ---- ---- 0 S CTS-password	

例：SGT インライン タギングの設定

この例では、デバイスのインターフェイスで L2-SGT タギングまたはインポジションを有効にして、インターフェイスが CTS に信頼されるかどうかを定義する方法を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet 0
Device(config-if)# cts manual
Device(config-if-cts-manual)# propagate sgt
Device(config-if-cts-manual)# policy static sgt 77 trusted
```

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。