セキュリティグループ ACL

SGACL の機能履歴

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 26.2.1ea	SGACL：セキュリティ グループ アクセス コントロール リスト（SGACL）機能のサポートが導入されました。	Cisco C9550 シリーズ スマート スイッチ

セキュリティグループ ACL

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	SGACL：セキュリティ グループ アクセス コントロール リスト（SGACL）を使用すると、管理者は、割り当てられたセキュリティグループとアクセスしているリソースに基づいて、ユーザーが実行できる操作を制御するポリシーを適用できます。	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

セキュリティグループ ACL

セキュリティ グループ アクセス コントロール リスト（SGACL）を使用すると、管理者は、割り当てられたセキュリティグループとアクセスしているリソースに基づいて、ユーザーが実行できる操作を制御するポリシーを適用できます。

SGACLは、従来のIPアドレスとフィルタではなく、セキュリティグループタグに依存するステートレスなアクセス制御メカニズムを提供します。

SGACL ポリシーをプロビジョニングする主な方法には、以下の 3 つがあります。

- 静的ポリシープロビジョニング：

  管理者は**cts role-based permission** コマンドを使用してSGACLポリシーを手動で定義します。

- 動的ポリシープロビジョニング：

  SGACL ポリシーは、Cisco Identity Services Engine（ISE）ポリシー管理機能によって一元的に管理および設定されます。

- 認可変更（CoA）：

  Cisco ISE で SGACL ポリシーが更新されると、新しいポリシーはCoA を介して TrustSec デバイスにプッシュされます。デバイスのデータプレーンでは、CoA パケットに新しいポリシーが適用されます。その後、さらなるポリシー適用のためにコントロールプレーンに転送されます。

SGACL ポリシーを使用したロールベースのアクセス制御

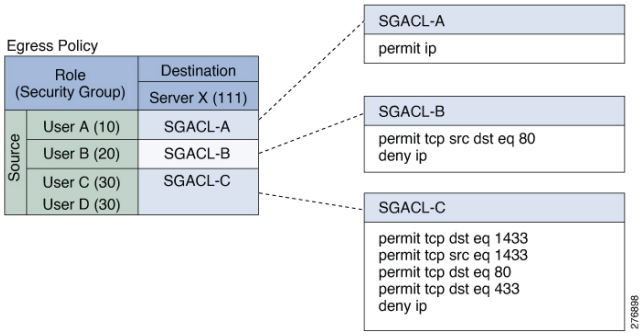
SGACL を使用すると、割り当てられたセキュリティグループとアクセスするリソースに基づいて、ユーザーが実行できるアクションを正確に制御できます。

Cisco TrustSec ドメイン内で、ポリシーの適用は権限マトリックスを使用して管理されます。一方の軸には送信元セキュリティグループ番号が、もう一方の軸には宛先セキュリティグループ番号が表示されます。マトリックスの各セルでは、SGACLの順序付きリストが保持され、特定の送信

元セキュリティグループから特定の宛先セキュリティグループに移動するパケットに適用される権限が指定されます。

次の図に、3 つの定義済みのユーザーロールと 1 つの定義済み宛先リソースを含むシンプルなドメインの Cisco TrustSec 許可マトリックスの例を示します。ユーザーの役割に基づいて宛先サーバーへのアクセスを 3 つの SGACL ポリシーで制御します。

***Figure 1: SGACL* ポリシー マトリクスの例**



Cisco TrustSec での SGACL の利点

ユーザーとデバイスをセキュリティグループに割り当て、セキュリティグループ間でのアクセスを制御することにより、Cisco TrustSec は、ロールベースのトポロジに依存しないアクセス制御を実現します。IP アドレスに依存する従来のアクセス制御リスト（ACL）とは異なり、SGACL はデバイスアイデンティティを使用します。これは、デバイスがネットワーク内の任意の場所で IP アドレスを移動または変更することができ、ロールと権限が同じである限り、セキュリティポリシーは変更されないことを意味します。新しいユーザーまたはデバイスが追加された場合、適切なセキュリティグループに割り当てるだけで、グループの権限がすぐに継承されます。

シンプルなポリシー管理とリソースの効率

SGACL は、アクセス コントロール エントリ（ACE）の数と複雑さを抑制することにより、アクセス制御を合理化します。ACE の総数は、個別の権限数によって決定されますが、これは通常、従来の IP ベースの ACL よりも大幅に少なくなります。このロールベースのアプローチにより、継続的なメンテナンスがシンプル化されるだけでなく、ネットワークデバイスで TCAM などのハードウェアリソースをより効率的に使用できます。Cisco TrustSec は、最大 5,000 の SGACL ポリシーをサポートします。

Cisco TrustSec でのデバイス認証とリンク認可

デバイス認証が終了すると、サプリカントとオーセンティケータの両方が認証サーバーからセキュリティポリシー情報を受信します。2 台のデバイスは、リンク認可を実行し、Cisco TrustSec デバイス ID に基づいて、該当するリンクセキュリティポリシーを適用します。

リンクの認証メソッドは、802.1X 認証または手動認証に設定できます。

- 802.1X 認証：

各デバイスは、認証サーバーによって提供されたデバイス ID を使用します。

- 手動認証：

  デバイス ID を各ピアに手動で割り当てる必要があります。

認証サーバーは以下のポリシー属性を提供します。

- Cisco TrustSec 信頼：

  ピアデバイスによるパケットへのセキュリティグループタグ（SGT）の挿入を信頼するかどうかを指定します。

- ピア SGT：

  ピアが属しているセキュリティグループを識別します。ピアが信頼されていない場合は、デバイスから受信したすべてのパケットにこの SGT がタグ付けされます。ピアの SGT に関連付けられた SGACL が存在するかどうか不明な場合、デバイスが認証サーバーに追加の要求を送信して、必要な SGACL を取得することがあります。

- 認可の有効期限：

  承認とポリシーが有効である秒数を示します。デバイスは、期限切れになる前にポリシーと認可を更新する必要があります。キャッシュされた認証およびポリシーデータは、有効期限が切れていない場合、リブート後に再利用できます。

Note Cisco TrustSec デバイスは、認証サーバーからピアの適切なポリシーを取得できない場合に備えて、最小限のデフォルト アクセス ポリシーをサポートする必要があります。

SGACL レイヤ 2 適用

レイヤ 2 での適用は、インターフェイスまたは VLAN に SGACL ポリシーを適用し、パケットに含まれる SGT に基づいて通信をフィルタリングすることによって行われます。適用すると、同じレイヤ 2 ドメイン内でのセグメンテーションと制御が可能になります。

ルーテッドおよびスイッチド トラフィックでの SGACL の強制

SGACL の強制は IP トラフィックだけに適用されますが、強制はルーティングまたはスイッチングされるトラフィックに適用できます。

- ルーティングされた通信：

  SGACL の適用は IP 通信にのみ適用され、出力スイッチ（たとえば、ディストリビューション スイッチやルーテッドポートを備えたアクセススイッチ）によって実行されます。グローバルに有効にすると、レイヤ 3 インターフェイス（SVI を除く）で自動的に実行されます。

- スイッチされた通信：

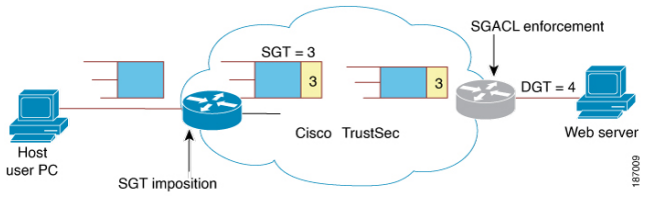
適用は、ルーティングされていない単一のスイッチングドメイン内の通信に対して行われます。VLAN 内でスイッチングされるパケットまたは VLAN に関連付けられた SVI に転送されるパケットに適用できます。ただし、VLAN ごとに明示的に有効化する必要があります。

Cisco TrustSec での入力タギングおよび出力適用

Cisco TrustSec では、入力タギングと出力適用の組み合わせによって、アクセス制御が適用されます。通信が Cisco TrustSec ドメインに到達すると、入力デバイスは、送信元のセキュリティグループ番号を識別する SGT を使用してパケットにタグを付けます。通信が TrustSec ドメインを通過する間、この SGT はそのまま保持されます。出力ポイントで、出力デバイスは、送信元 SGT と宛先のセキュリティグループ番号（宛先グループタグまたは DGT とも呼ばれます）の両方を評価します。この情報を使用して、出力デバイスは SGACL ポリシーマトリックスを参照し、通信に適したアクセスポリシーを決定して適用できます。

Cisco TrustSec ドメインでは、次の図のように SGT の割り当てと SGACL の適用が実行されます。

Figure 2: Cisco TrustSec* ドメインの *SGT* と *SGACL



SGT および SGACL が適用されたパケットフローは、次のように動作します。

1. ホスト PC は Web サーバーにパケットを送信します。PC と Web サーバーは Cisco TrustSec ドメインのメンバーではありませんが、パケットのパスは Cisco TrustSec ネットワークを通過します。
2. Cisco TrustSec の入力デバイスは、パケットを受信し、認証サーバーによりホスト PC に割り当てられたとおり、セキュリティグループ番号 3 の SGT を追加します。
3. Cisco TrustSec 出力デバイスは、パケットを検査し、送信元グループ 3（ホスト PC）から宛先グループ 4（Web サーバー）への通信を制御する SGACL ポリシーを適用します。グループ 4 は、認証サーバーによって Web サーバーに割り当てられたセキュリティグループです。
4. SGACL が通信を許可すると、Cisco TrustSec 出力スイッチはパケットから SGT を削除して、Web サーバーに転送します。

SGACL ロギング

Cisco TrustSec における SGACL ロギングでは、SGACL に一致する通信に関する詳細情報が記録されます。SGACL ロギングが有効になっている場合、デバイスは以下の情報をログに記録します。

- 送信元および宛先セキュリティグループタグ（SGT）

- SGACL ポリシーの名前
- パケットのプロトコルタイプ
- パケットで実行されるアクション

ロギングオプションは個々の ACE に適用できるため、それらの ACE に一致するパケットのみがログに記録されます。log キーワードをトリガーする最初のパケットは、syslog メッセージを生成します。その後、5 分ごとにログメッセージが報告されます。同じ ACE が同じ特性を持つ別のパケットをログに記録すると、デバイスの一致カウンタの数が増分され、その情報が次のレポートに含められます。

ロギングを有効にするには、SGACL 設定で ACE 定義の前に **log** キーワードを使用します。たとえば、**permit ip log** のようになります。

SGACL ロギングが有効の場合、デバイスからクライアントへの ICMP 要求メッセージは、IPv4 および IPv6 プロトコルについては記録されません。ただし、クライアントからデバイスへの ICMP 応答メッセージがログに記録されます。

次に、送信元と宛先の SGT、ACE の一致（許可または拒否アクション）、およびプロトコル、つまり TCP、UDP、IGMP、および ICMP 情報を表示するサンプルログを示します。

```
*Jun 2 08:58:06.489: %C4K_IOSINTF-6-SGACLHIT: list deny_udp_src_port_log-30 Denied
udp 24.0.0.23(100) -> 28.0.0.91(100), SGT8 DGT 12
```

SGACL ロギングおよびメッセージ制御

デバイスは、標準 IP アクセスリストまたは SGACL によって許可または拒否されたパケットに関するログメッセージを生成できます。パケットが SGACL エントリと一致するたびに、情報メッセージがコンソールに送信されます。コンソールに表示されるメッセージの量は、syslog の出力を制御する **logging console** コマンドを使用して管理します。

SGACL ロギングは、はるかに高いロギングレートを可能にする NetFlow ハードウェアを使用するように拡張されました。

最初のパケットが SGACL エントリをトリガーすると、フローが作成され、NetFlow タイムアウトに基づいてロギングが実行されます。タイムアウト時間は、非アクティブなフローの場合は 30 秒、アクティブなフローの場合は 1 分です。この最初の期間の後、後続のパケットはカウントされて集約され、5 分ごとにロギングメッセージが生成されます。

各ログメッセージには、次の内容が含まれます。

- アクセスリスト番号
- パケットが許可されたか、拒否されたか
- 送信元 IP アドレスと宛先 IP アドレス
- 入力インターフェイス
- 過去 5 分間に同じ送信元から許可または拒否されたパケットの数

SGACL セル統計情報

SGACL セル統計情報では、SGACL ポリシーの適用に関する詳細な可視性が提供されます。適用マトリックスは、送信元 SGT と宛先 SGT のペア別に編成され、各セルはそれらのグループ間で適用される権限を表します。管理者は、各 SGT ペアの SGACL によって許可または拒否されたパケットを示すセルごとの統計情報を表示できます。

show cts role-based counters コマンドを使用して表示できる既存の「セルごとの」SGACL 統計情報に加えて、**show ip access-list** *sgacl_name* コマンドを使用して ACE 統計情報も表示できます。これについて追加設定は必要ありません。

次に、**showipaccess-list** コマンドを使用して ACE カウントを表示する例を示します。

```
Device# show ip access-control deny_udp_src_port_log-30
Role-based IP access list deny_udp_src_port_log-30 (downloaded)
10 deny udp src eq 100 log (283 matches)
20 permit ip log (50 matches)
```

SGACL モニター モード

SGACL モニターモードは、Cisco TrustSec のデプロイメント前フェーズ用に設計されており、管理者は、セキュリティポリシーを適用せずにセキュリティポリシーをテストできます。このモードは、実際の適用が開始される前に、ポリシーが想定どおりに動作することを確認するのに役立ちます。ポリシーが意図されたとおりに機能しない場合、モニターモードで問題を簡単に特定して修正できます。これにより、適用が有効になる前に、不正アクセスの拒否などのセキュリティ要件が満たされます。

モニタリングは、SGT-DGT（送信元グループタグと接続先グループタグ）ペアレベルで動作します。SGACL モニターモードが有効になっている場合、ポリシー内の拒否アクションは、デバイスのラインカードで許可として扱われます。これにより、SGACL カウンタとロギングによりポリシーの動作への可視性が提供され、適用がアクティブな場合に通信がどのように処理されるかが示されます。モニター対象のすべての通信が許可されるため、テストフェーズの間にサービスが中断されることはありません。

SGACL の制約事項

次の制約事項がすべてのスイッチに適用されます。

- ハードウェアの制限により、Cisco TrustSec SGACL はハードウェアのパント（CPUバウンド）トラフィックに適用できません。ソフトウェアでの SGACL の適用は、スイッチ仮想インターフェイス（SVI）、レイヤ 2 およびレイヤ 3 の Location Identifier Separation Protocol（LISP）、およびループバック インターフェイスの CPU バウンド通信ではバイパスされます。
- SGACL ポリシーを設定する際に、IP バージョンを IPv4 または IPv6 から 非依存（IPv4 と IPv6 の両方に適用）に変更した場合（逆も同様）、IPv4 と IPv6 に対応する SGACL ポリシーは管理 VRF インターフェイスを介して完全にダウンロードされません。

- SGACL ポリシーを設定する際に、既存の IP バージョンを他のバージョン（IPv4 または IPv6 または 非依存）に変更した場合（逆も同様）、RADIUS を使用して Cisco Identity Services Engine（ISE）からの認可変更（CoA）を実行できません。代わりに、SSH を使用して **cts refresh policy** コマンドを実行し、手動でポリシーを更新します。
- **deny all** をデフォルトアクションとする SGT 許可モデルを使用する場合、デバイスのリロード後に Cisco TrustSec ポリシーが ISE サーバーから部分的にダウンロードされることがあります。

  これを回避するには、デバイスで静的ポリシーを定義します。deny all オプションが適用されている場合でも、静的ポリシーは通信を許可します。これにより、デバイスは ISE サーバーからポリシーをダウンロードし、定義された静的ポリシーを上書きできます。デバイス SGT では、グローバル コンフィギュレーション モードで次のコマンドを設定します。

  - **cts role-based permissions from** *sgt_num* **to unknown**
  - **cts role-based permissions from unknown to** *sgt_num*

次の制約事項が Cisco C9610 シリーズ スマートスイッチに適用されます。

- 同じ ACL のセットを通常の SGACL セル権限と SGACL デフォルト権限の両方に使用することはできません。代わりに、デフォルトの権限に固有の ACL のセットを使用します。

SGACL の設定方法

以下のセクションでは、SGACL に関する設定情報を提供します。

SGACL ポリシーの設定プロセス

SGACL ポリシーを設定してイネーブルにするには、次の手順を実行します。

Procedure

Step 1 SGACL ポリシーの設定は、主に Cisco Identity Services Engine（ISE）のポリシー管理機能によって実行する必要があります。

SGACL ポリシー設定のダウンロードに Cisco ISE での AAA を使用しない場合は、SGACL のマッピングとポリシーを手動で設定できます。

Note
Cisco ISE からダイナミックにダウンロードされた SGACL ポリシーは、競合のローカル定義されたポリシーよりも優先されます。

Step 2 ルーテッドポートの出力トラフィックに対する SGACL ポリシーの適用を有効にするには、「SGACL ポリシーの適用のグローバルな有効化」セクションに記載されているように、SGACL ポリシー適用を有効にします。

Step 3 VLAN 内のスイッチングされたトラフィック、または VLAN に関連付けられた SVI に転送されるトラフィックに対して SGACL ポリシーの適用を有効にするには、「VLAN に対する SGACL ポリシーの適用の有効化」セクションの説明に従って、特定の VLAN に対して SGACL ポリシーの適用を有効にします。

SGACL ポリシー適用のグローバルな有効化

Cisco TrustSec をイネーブルにしたルーテッド インターフェイスで SGACL ポリシーの強制をグローバルにイネーブルにする必要があります。

ルーテッド インターフェイスの SGACL ポリシーの強制をイネーブルにするには、次の作業を行います。

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 **configure terminal**

Example:

```
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。

Step 3 **cts role-based enforcement**

Example:

```
Device(config)# cts role-based enforcement
```

ルーテッド インターフェイスで Cisco TrustSec SGACL ポリシーの強制を有効にします。

Step 4 **end**

Example:

```
Device(config)# end
```

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

インターフェイスごとの SGACL ポリシー適用の有効化

Cisco TrustSec をイネーブルにしたルーテッド インターフェイスで SGACL ポリシーの強制をグローバルにイネーブルにする必要があります。

ルーテッド インターフェイスの SGACL ポリシーの強制をイネーブルにするには、次の作業を行います。

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 **configure terminal**

Example:

```
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。

Step 3 **interface** *type slot/port*

Example:

```
Device(config)# interface gigabitethernet 6/2
```

インターフェイスを設定し、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。

Step 4 **cts role-based enforcement**

Example:

```
Device(config-if)# cts role-based enforcement
```

ルーテッド インターフェイスで Cisco TrustSec SGACL ポリシーの強制をイネーブルにします。

Step 5 **end**

Example:

```
Device(config-if)# end
```

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 モードに戻ります。

Step 6 **show platform software fed [switch] [active | standby] sgacl port**

Example:

```
Device#show platform software fed switch active sgacl port |  i Port|6/2
```

（オプション）インターフェイスでの Cisco TrustSec SGACL ポリシー適用のステータスを表示します。

VLAN での SGACL ポリシー適用の有効化

VLAN 内のスイッチングされたトラフィック、または VLAN に関連付けられた SVI に転送されるトラフィックに対してアクセス コントロールを適用するには、特定の VLAN に対して SGACL ポリシーの強制をイネーブルにする必要があります。

VLAN または VLAN リスト内で、SGACL ポリシーの強制をイネーブルにするには、次の作業を行います。

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 **configure terminal**

Example:

```
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。

Step 3 **cts role-based enforcement vlan-list** *vlan-list*

Example:

```
Device(config)# cts role-based enforcement vlan-list 31-35,41
```

VLAN または VLAN リストで Cisco TrustSec SGACL ポリシーの強制をイネーブルにします。

Step 4 **end**

Example:

```
Device(config)# end
```

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ネットワークデバイスでの Cisco TrustSec ステータスの確認

ネットワークデバイスで Cisco TrustSec のステータスを確認するには、次の手順を実行します。

Procedure

Step 1 インターフェイスで Cisco TrustSec（CTS）ロールベース適用ステータスを確認します。

Example:

```
Device#show platform software fed switch active sgacl port |  i Port|1/0/23

Port            Status     Port-SGT  Trust  Propagate  IngressCache EgressCache
Te1/0/23       Enabled         0     No      No          No          No
```

インターフェイスでロールベース適用設定を削除すると、出力の `Status` フィールドには `Disabled` と表示されます。

Step 2 インターフェイスでの静的 SGT、MACsec 暗号化、または SGT インラインタギングに関連した CTS 設定のステータスを確認します。

Example:

この例では、静的 SGT がインターフェイス Te1/0/12 で設定されています。

```
interface TenGigabitEthernet1/0/12
 description lan interface
 switchport mode trunk
 cts manual
  policy static sgt 8000 trusted
```

show cts interface コマンドの出力には、そのインターフェイスについて `CTS is enabled` と表示されます。

```
Device#show cts interface te1/0/12
Global Dot1x feature is Disabled
Interface TenGigabitEthernet1/0/12:
    CTS is enabled.
```

この例では、インターフェイス Te1/0/23 には、静的 SGT、MACsec 暗号化、または SGT に関連した設定がありません。そのため、インターフェイスでロールベースの適用が有効になっていても、コマンド出力に `CTS is disabled` と表示されます。

```
Device#show cts interface te1/0/23
Global Dot1x feature is Disabled
Interface TenGigabitEthernet1/0/23:
    CTS is disabled.

    L3 IPM:   disabled.
```

この動作はインターフェイス VLAN でも同じです。この例では、VLAN 1035 でロールベースの適用が有効になっています。それでも、**show cts interface vlan 1035** コマンド出力には `CTS is disabled` と表示されます。

```
Device#show run | i cts role-based enforcement
cts role-based sgt-map vlan-list 1044 sgt 8
cts role-based sgt-map vlan-list 1035 sgt 13
cts role-based enforcement
cts role-based enforcement vlan-list 1030,1032,1035,1044-1045,2047

Device#show cts interface vlan 1035
Global Dot1x feature is Disabled
Interface Vlan1035:
    CTS is disabled.
```

```
    L3 IPM:   disabled.
```

Note
show cts interface コマンド出力では、CTS ロールベースの適用がインターフェイスでアクティブになっているかどうかが示されません。

ロールベースの適用がグローバル、インターフェイスレベル、VLAN レベル、またはこれらすべてのレベルで有効になっている場合でも、**show cts interface** <> コマンドの出力には、これらのいずれかに関連した設定がインターフェイスレベルで設定されている場合にのみ、`CTS is enabled` と表示されます。

- 静的 SGT
- MACSec 暗号化
- SGT インライン タギング

Step 3 CTS が有効になっているインターフェイスの概要を表示します。

Example:

この例では、インターフェイス Te1/0/23 で **role-based enforcement** が有効になっていても、コマンド出力にそのインターフェイスは表示されません。

```
Device#show cts interface summary
CTS Interfaces
---------------------
Interface                       Mode    IFC-state dot1x-role peer-id    IFC-cache
Critical-Authentication
------------------------------------------------------------------------------
Te1/0/1                         MANUAL  OPEN      unknown    unknown    invalid  Invalid
Te1/0/12                        MANUAL  OPEN      unknown    unknown    invalid  Invalid
```

静的 SGT、MACsec 暗号化、または SGT インライン タギングに関連した設定がインターフェイスに存在する場合、**show cts interface** コマンドの出力にその特定のインターフェイスも一覧表示されます。

```
interface TenGigabitEthernet1/0/23
 description lan interface
 switchport mode trunk
 cts manual
  policy static sgt 8000 trusted--->static sgt configuration

Device#show cts interface summary
CTS Interfaces
---------------------
Interface                       Mode    IFC-state dot1x-role peer-id    IFC-cache
Critical-Authentication
------------------------------------------------------------------------------
Te1/0/1                         MANUAL  OPEN      unknown    unknown    invalid  Invalid
Te1/0/12                        MANUAL  OPEN      unknown    unknown    invalid  Invalid
Te1/0/23                        MANUAL  OPEN      unknown    unknown    invalid  Invalid
```

SGACL モニターモードの設定

SGACL モニターモードを設定するには、次の手順を実行します。

Before you begin

SGACL モニターモードを設定する前に、次の点を確認してください。

- Cisco TrustSec が有効になっている。
- カウンタが有効になっている。

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 **configure terminal**

Example:

```
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。

Step 3 **cts role-based monitor all**

Example:

```
Device(config)# cts role-based monitor all
```

グローバルモニターモードを有効にします。

Step 4 **cts role-based monitor permissions from** {*sgt_num*} **to** {*dgt_num*} [**ipv4** | **ipv6**]

Example:

```
Device(config)# cts role-based permissions from 2 to 3 ipv4
```

IPv4 または IPv6 ロールベースアクセス制御リスト（RBACL）のモニターモードを有効にします。

- *sgt_num*：セキュリティグループタグ
- *dgt_num*：宛先グループタグ

Step 5 **end**

Example:

```
Device(config)# end
```

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SGACL ポリシーの手動設定

送信元グループタグ（SGT）と宛先グループタグ（DGT）の範囲に適用されるロールベースのアクセス制御リスト（ACL）は、出力トラフィックに適用される Cisco TrustSec ポリシーである SGACL になります。SGACL ポリシーを設定するための推奨されるアプローチは、Cisco Identity Services Engine（ISE）のポリシー管理機能を使用する方法です。

ローカル（手動）設定では、ロールベース ACL を作成し、それを SGT の特定の範囲にバインドできます。この機能により、デバイスで直接アクセスコントロールポリシーを定義して適用できます。

Note Cisco ISE から動的にダウンロードされた SGACL ポリシーは、手動で設定されたポリシーと競合する場合、それを上書きします。

IPv4 SGACL ポリシーの設定と適用

IPv4 SGACL ポリシーを設定して適用するには、次の手順を実行します。

Before you begin

SGACL および RBACL を設定する場合、名前付きアクセスコントロールリスト（ACL）はアルファベットで始まる必要があります。

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 **configure terminal**

Example:

```
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。

Step 3 **ip access-list role-based** *rbacl-name*

Example:

```
Device(config)# ip access-list role-based allow_webtraff
```

RBACL を作成して、ロールベース ACL コンフィギュレーション モードを開始します。

Step 4 {[*sequence-number*] | **default** | **permit** | **deny** | **remark**}

Example:

```
Device(config-rb-acl)# 10 permit tcp dst allowed in extended named access list eq 80 dst
eq 20
```

RBACL のアクセス コントロール エントリ（ACE）を指定します。

拡張名前付きアクセス リスト コンフィギュレーション モードで使用可能なコマンドおよびオプションの大部分を、送信元および宛先フィールドを省略して使用できます。

次の ACE キーワードはサポートされていません。

- reflect
- evaluate
- time-range

Step 5 **exit**

Example:

```
Device(config-rb-acl)# exit
```

RBACL を作成して、ロールベース ACL コンフィギュレーション モードを開始します。

Step 6 **ip access-list role-based** *rbacl-name*

Example:

```
Device(config)# ip access-list role-based allow_webtraff
```

ロールベース ACL コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

Step 7 **cts role-based permissions** {**default** | [**from** { *sgt_num* | **unknown**} **to** {*dgt_num* | **unknown**}] {*rbacls* **ipv4** *rbacls*}

Example:

```
Device(config)# cts role-based permissions from 55 to 66 allow_webtraff
```

SGT と DGT を RBACL にバインドします。この設定は、Cisco ISE で設定された権限マトリックスにデータを入力することに似ています。

- **default**：デフォルトの権限リスト。
- *sgt_num*：0 ～ 65,519。送信元グループタグ。
- *dgt_num*：0 ～ 65,519。宛先グループタグ。
- **unknown**：SGACL がセキュリティグループ（送信元または宛先）を特定できないパケットに適用されます。
- **ipv4**：RBACL が IPv4 であることを示します。

• *rbacls*：RBACL の名前。

Step 8 **end**

Example:

```
Device(config)# end
```

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPv6 SGACL ポリシーの設定

IPv6 SGACL ポリシーを手動で設定するには、次の作業を行います。

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 **configure terminal**

Example:

```
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。

Step 3 **ipv6 access-list role-based** *sgacl-name*

Example:

```
Device(config)# ipv6 access-list role-based sgaclname
```

名前付き IPv6 SGACL を作成して、IPv6 ロールベース ACL コンフィギュレーション モードを開始します。

Step 4 {**permit** | **deny**} *protocol* [**dest-option** | **dest-option-type** {*doh-number* | *doh-type*}] [**dscp** *cp-value*] [**flow-label** *fl-value*] [**mobility** | **mobility-type** {*mh-number* | *mh-type*}] [**routing** | **routing-type** *routing-number*] [**fragments**] [**log** | **log-input**] [**sequence** *seqno*]

Example:

```
Device(config-ipv6rb-acl)# permit 33 dest-option dscp af11
```

RBACL のアクセス コントロール エントリ（ACE）を指定します。

拡張名前付きアクセス リスト コンフィギュレーション モードで使用可能なコマンドおよびオプションの大部分を、送信元および宛先フィールドを省略して使用できます。

次の ACE キーワードはサポートされていません。

- **reflect**
- **evaluate**
- **time-range**

Step 5 **end**

Example:

```
Device(config-ipv6rb-acl)# end
```

IPv6 ロールベース ACL コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

手動での SGACL ポリシーの適用

手動で SGACL ポリシーを適用するには、次の作業を行います。

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 **configure terminal**

Example:

```
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。

Step 3 **cts role-based permissions default** [**ipv4** | **ipv6**] [*sgacl-name1* [*sgacl-name2* [*sgacl-name3* ...]]]

Example:

```
Device(config)# cts role-based permissions default MYDEFAULTSGACL
```

デフォルト SGACL を指定します。デフォルト ポリシーは明示的なポリシーが送信元と宛先セキュリティグループの間にない場合に適用されます。

Step 4 **cts role-based permissions from** {*source-sgt* | **unknown**} to {*dest-sgt* | **unknown**} [**ipv4** | **ipv6**] *sgacl-name1* [*sgacl-name2* [*sgacl-name3* ...]]]

Example:

```
Device(config)# cts role-based permissions from 3 to 5 SRB3 SRB5
```

SGT および DGT に適用する SGACL を指定します。

- *source-sgt*：範囲は 1 ー 65533 です。
- *dest-sgt*：範囲は 1 ー 65533 です。
- **from**：送信元 SGT を指定します。
- **to**：宛先セキュリティグループを指定します。
- **unknown**：SGACL がセキュリティグループ（送信元または宛先）を特定できないパケットに適用されます。

Note

- デフォルトでは、SGACL は IPv4 であると見なされます。
- ACS から動的にダウンロードされた SGACL ポリシーは、競合の手動ポリシーよりも優先されます。

Step 5 **end**

Example:

```
Device(config)# end
```

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SGACL ポリシーの更新

SGACL ポリシーを更新するには、次のタスクを実行します。

Procedure

	Command or Action	Purpose
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 refresh policy** {**peer** [*peer-id*] | **sgt** [*sgt_number* | **default** | **unknown**]} **Example:** `Device# cts refresh policy peer my_cisco_ise`	認証サーバーからの SGACL ポリシーの即時リフレッシュを実行します。 • *peer-id* が指定される場合、指定されたピア接続に関連するポリシーだけがリフレッシュされます。 すべてのピアポリシーを更新するには、ID を指定しないで [Enter] を押します。

	Command or Action	Purpose
		• SGT 番号が指定されている場合、その SGT に関連するポリシーだけがリフレッシュされます。 • すべての SGT ポリシーをリフレッシュするには、SGT 番号を指定せずに [Enter] を押します。 • デフォルトポリシーを更新するには、**default** を選択します。 • 不明ポリシーを更新するには、**unknown** を選択します。
Step 3	**exit** **Example:** `Device# exit`	特権 EXEC モードを終了します。

SGACL ポリシーのモニタリングと表示

コマンド	説明
show cts interface	インターフェイスでの静的SGT、MACsec暗号化、またはSGTインライン タギングに関連した CTS 設定のステータスを表示します。
show cts role-based counters [ipv4 | ipv6]	IPv4 および IPv6 イベントのすべての SGACL 適用の統計情報を表示します。
show cts role-based permissions	RBACL 設定に対する権限を表示します。

コマンド	説明
show cts role-based permissions from {*source-sgt* | unknown} to {*dest-sgt* | unknown}] [ipv4 | ipv6 | details]	SGACL ポリシーとペアごとのモニターモード機能に関する詳細を表示します。 *SGT-DGT* ペアに対してセルごとのモニターモードが有効になっている場合、コマンド出力が表示されます。 • キーワードを使用または省略して、許可マトリクスの全部または一部を表示できます。 • from キーワードを省略すると、権限マトリックスの列が表示されます。 • to キーワードを省略すると、権限マトリックスの行が表示されます。 • from および to キーワードを省略すると、権限マトリックス全体が表示されます。 • from および to キーワードが指定されている場合、権限マトリックスから 1 つのセルが表示され、details キーワードを使用できます。details が入力されると、1 つのセルの SGACL の ACE が表示されます。
show ip access-lists {*rbacls* | ipv4 *rbacls*}	すべての RBACL または指定された RBACL の ACE を表示します。
show cts role-based permissions default [ipv4 | ipv6 | details]	デフォルトポリシーの SGACL のリストを表示します。
show platform software fed [switch] [active | standby] sgacl port	インターフェイスでの Cisco TrustSec SGACL ポリシー適用のステータスを表示します。

セキュリティグループ ACL ポリシーの設定例

次のセクションでは、さまざまな SGACL ポリシーの設定例を示します。

例：SGACL ポリシー適用のグローバルな有効化

次に、 SGACL ポリシーの適用をグローバルに有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# cts role-based enforcement
```

例：インターフェイスごとの SGACL ポリシー適用の有効化

次に、インターフェイスごとに SGACL ポリシーの適用を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/2
Device(config-if)# cts role-based enforcement
Device(config-if)# end
```

例：VLAN に対する SGACL ポリシー適用の有効化

次に、VLAN 上で SGACL ポリシーの適用を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# cts role-based enforcement vlan-list 31-35,41
Device(config)# exit
```

例：SGACL モニターモードの設定

次に、SGACL モニターモードを設定する例を示します。

```
Device# configure terminal
Device(config)# cts role-based monitor enable
Device(config)# cts role-based permissions from 2 to 3 ipv4
Device# show cts role-based permissions from 2 to 3 ipv4

IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
        denytcpudpicmp-10
        Deny IP-00

Device# show cts role-based permissions from 2 to 3 ipv4 details

IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
        denytcpudpicmp-10
        Deny IP-00
Details:
Role-based IP access list denytcpudpicmp-10 (downloaded)
        10 deny tcp
        20 deny udp
        30 deny icmp
Role-based IP access list Permit IP-00 (downloaded)
        10 permit ip

Device# show cts role-based counters ipv4

Role-based IPv4 counters
From     To     SW-Denied  HW-Denied  SW-Permitt  HW_Permitt  SW-Monitor  HW-Monitor
*         *     0          0          8           18962       0           0
2         3     0          0          0           0           0           341057
```

例：SGACL ポリシーの手動設定

```
Device# configure terminal
Device(config)# ip access role allow_webtraff
```

```
Device(config-rb-acl)# 10 permit tcp dst eq 80
Device(config-rb-acl)# 20 permit tcp dst eq 443
Device(config-rb-acl)# 30 permit icmp
Device(config-rb-acl)# 40 deny ip
Device(config-rb-acl)# exit
Device(config)# cts role-based permissions from 55 to 66 allow_webtraff
Device# show ip access allow_webtraff

Role-based IP access list allow_webtraff
    10 permit tcp dst eq www
    20 permit tcp dst eq 443
    30 permit icmp
    40 deny ip
Device# show show cts role-based permissions from 50 to 70
```

例：SGACL の手動適用

次に、SGACL ポリシーを手動で適用する例を示します。

```
Device# configure terminal
Device(config)# cts role-based permissions default MYDEFAULTSGACL
Device(config)# cts role-based permissions from 3 to 5 SRB3 SRB5
Device(config)# exit
```

例：SGACL ポリシーの表示

次に、セキュリティ グループ 3 から送信されたトラフィックの SGACL ポリシーの許可マトリクスの内容を表示する例を示します。

```
Device# show cts role-based permissions from 3

Role-based permissions from group 3 to group 5:
        SRB3
        SRB5
Role-based permissions from group 3 to group 7:
        SRB4
```

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。