セキュリティグループACLポリシーの設定

セキュリティ グループ アクセス コントロール リスト（SGACL）を使用して、ユーザーと宛先リソースのセキュリティ グループの割り当てに基づいて、ユーザーが実行できる操作を制御できます。Cisco TrustSec ドメイン内のポリシーの適用は、軸の 1 つが送信元セキュリティ グループ番号、もう 1 つの軸が宛先セキュリティグループ番号である、許可マトリックスで表示されます。マトリクスの本体の各セルには送信元セキュリティ グループから宛先セキュリティ グループ宛てに送信されるパケットに適用される必要がある許可を指定する SGACL の順序リストを含めることができます。

SGACL ポリシーの設定の制約事項

- 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、SVI、レイヤ 2 とレイヤ 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 バウンドトラフィック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）を実行しないでください。代わりに、SSH を使用して **cts refresh policy** コマンドを実行し、手動でポリシーをリフレッシュします。
- デフォルトのアクションを **deny all** とした SGT 許可リスト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、静的ポリシーはトラフィックを許可します。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*>

SGACL ポリシーの設定方法

このセクションでは、さまざまな SGACL ポリシー設定について説明します。

SGACL ポリシーの設定プロセス

Cisco TrustSec のセキュリティグループ ACL（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。

1. SGACL ポリシーの設定は、Cisco Secure Access Control Server（ACS）または Cisco Identity Services Engine（ISE）の主にポリシー管理機能によって実行する必要があります。

   SGACL ポリシーの設定のダウンロードに Cisco Secure ACS または Cisco ISE 上の 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。

（注） Cisco Secure ACS または 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。

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。
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 ポリシーの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。

手順

	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	**cts role-based enforcement** 例： `Device(config)# cts role-based enforcement`	ルーテッド インターフェイスで Cisco TrustSec SGACL ポリシーの強制をイネーブルにします。
ステップ 4	**end** 例： `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。

インターフェイスあたりの SGACL ポリシーの適用の有効化

まず、Cisco TrustSec を有効にしたルーテッドインターフェイスで SGACL ポリシーの適用をグローバルに有効にする必要があります。この機能はポート チャネル インターフェイスではサポートされません。

レイヤ 3 インターフェイスでの SGACL ポリシーの適用を有効化するには、次の作業を行います。

手順

	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** *type slot/port* 例： `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。

	コマンドまたはアクション	目的
ステップ 4	**cts role-based enforcement** 例： `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。
ステップ 5	**end** 例： `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。
ステップ 6	**show cts interface** 例： `Device# show cts interface`	（任意）インターフェイスごとの Cisco TrustSec ステートおよび統計情報を表示します。

VLAN に対する SGACL ポリシーの強制のイネーブル化

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。

手順

	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	**cts role-based enforcement vlan-list** *vlan-list* 例： `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。
ステップ 4	**end** 例： `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 モニター モードの設定

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。

手順

	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	**cts role-based monitor all** 例： `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。
ステップ 4	**cts role-based monitor permissions from** {*sgt_num*} **to** {*dgt_num*} [**ipv4** | **ipv6**] 例： `Device(config)# cts role-based permissions from 2 to 3 ipv4`	IPv4/IPv6 ロール ベース アクセス コントロール リスト（RBACL）（セキュリティグループタグ（SGT）：接続先グループタグ（DGT）ペア）のモニターモードを有効にします。
ステップ 5	**end** 例： `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。
ステップ 6	**show cts role-based permissions from** {*sgt_num*} **to** {*dgt_num*} [**ipv4** | **ipv6**] [**details**] 例： `Device# show cts role-based permissions from 2 to 3 ipv4 details`	（任意）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> ペアでセルごとのモニターモードが有効になっている場合、コマンド出力にはモニター対象が表示されます。
ステップ 7	**show cts role-based counters** [**ipv4** | **ipv6**] 例： `Device# show cts role-based counters ipv4`	（任意）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。

SGACL ポリシーの手動設定

SGT と DGT の範囲にバインドされたロールベース アクセス コントロール リストは、出力トラフィックに適用される Cisco TrustSec ポリシーである SGACL を形成します。SGACL ポリシーの設定は、Cisco ISE または Cisco Secure ACS のポリシー管理機能を使用して行うのが最適です。SGACL ポリシーを手動で（つまりローカルに）設定するには、ロールベース ACL を設定し、ロールベース ACL を SGT の範囲にバインドします。

（注） Cisco ISE または Cisco ACS からダイナミックにダウンロードされた SGACL ポリシーは、競合の手動設定されたポリシーよりも優先されます。

IPv4 SGACL ポリシーの設定と適用

（注） SGACL およびロールベース アクセス コントロール リスト（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。

手順

	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	**ip access-list role-based** *rbacl-name* 例： `Device(config)# ip access-list role-based allow_webtraff`	ロールベースの ACL 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。
ステップ 4	{[*sequence-number*] | **default** | **permit** | **deny** | **remark**} 例： `Device(config-rb-acl)# 10 permit tcp dst 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。

	コマンドまたはアクション	目的
		Enter キーを押して ACE を完了し、次の手順を開始します。 次の ACE コマンドまたはキーワードはサポートされていません。 • **reflect** • **evaluate** • **time-range**
ステップ 5	**exit** 例： `Device(config-rb-acl)# exit`	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。
ステップ 6	**cts role-based permissions {default** | **[from** {*sgt_num* | **unknown**} **to** {*dgt_num* | **unknown** }] {*rbacls* | **ipv4** *rbacls*} 例： `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 または Cisco Secure ACS で設定された許可マトリックスにデータを入力することに似ています。 • デフォルト：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。接続先グループタグ。 • 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：次の RBACL が IPv4 であることを示します。 • *rbacls*：RBACL の名前
ステップ 7	**end** 例： `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。
ステップ 8	**show cts role-based permissions** 例：	（任意）RBACL 設定に対する権限を表示します。

	コマンドまたはアクション	目的
	`Device# show cts role-based permissions`	
ステップ 9	**show ip access-lists** {*rbacls* | **ipv4** *rbacls*} 例： `Device# show ip access-lists allow_webtraff`	（任意）すべてのRBACLまたは指定された RBACL の ACE を表示します。

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。

手順

	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	**ipv6 access-list role-based** *sgacl-name* 例： `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。
ステップ 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*] 例： `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 コマンドまたはキーワードはサポートされていません。 • **reflect** • **evaluate** • **time-range**

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `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 SGACL ポリシーを適用する方法

手動で SGACL ポリシーを適用するには、次の作業を行います。

手順

	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	**cts role-based permissions default** [**ipv4** | **ipv6**] *sgacl-name1* [*sgacl-name2* [*sgacl-name3 ...*]]] 例： `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。
ステップ 4	**cts role-based permissions from** {*source-sgt* | **unknown**} **to** {*dest-sgt* | **unknown**} [**ipv4** | **ipv6**] *sgacl-name1* [*sgacl-name2* [*sgacl-name3 ...*]]] 例： `Device(config)# cts role-based permissions from 3 to 5 SRB3 SRB5`	送信元セキュリティ グループ（SGT）と宛先セキュリティグループ（DGT）に適用する SGACL を指定します。source-sgt と dest-sgt の値範囲は 1 ～ 65533 です。デフォルトでは、SGACL は IPv4 であると見なされます。 • **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。

	コマンドまたはアクション	目的
		（注） 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。
ステップ 5	**end** 例： `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 ポリシーの表示

Cisco TrustSec デバイス クレデンシャルと AAA の設定後、認証サーバーからダウンロードされたか、または手動で設定された Cisco TrustSec SGACL ポリシーを検証できます。Cisco TrustSec は、インターフェイスに対する認証および許可、SXP、または IP アドレスおよび SGT の手動マッピングによって新しい SGT を学習すると、SGACL ポリシーをダウンロードします。

キーワードを使用して、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、許可マトリックスのカラムが表示されます。
- **to** キーワードを省略すると、許可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、許可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、許可マトリックスから 1 つのセルが表示され、**details** キーワードを使用できます。**details** が入力された場合、1 つのセルの SGACL の ACE が表示されます。

SGACL ポリシーの許可マトリクスの内容を表示するには、次の作業を行います。

手順

	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	**show cts role-based permissions default** [**ipv4** | **ipv6** | **details**] 例： `Device# show cts role-based permissions default MYDEFAULTSGACL`	デフォルト ポリシーの SGACL のリストを表示します。

	コマンドまたはアクション	目的
ステップ 3	**show cts role-based permissions from** {*source-sgt* | **unknown**} **to** {*dest-sgt* | **unknown**}] [**ipv4** | **ipv6** | **details**] 例： `Device# show cts role-based permissions from 3`	送信元セキュリティ グループ（SGT）と宛先セキュリティグループ（DGT）に適用する SGACL を指定します。source-sgt と dest-sgt の値範囲は 1 ～ 65533 です。デフォルトでは、SGACL は IPv4 であると見なされます。 • **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。 （注） 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。
ステップ 4	**exit** 例： `Device# exit`	特権 EXEC モードを終了します。

ダウンロードされた SGACL ポリシーのリフレッシュ

手順

	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 refresh policy** {**peer** [*peer-id*] | **sgt** [*sgt_number* | **default** | **unknown**]} 例： `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、

	コマンドまたはアクション	目的
		ID を指定しないで Enter を押します。 • 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。すべてのセキュリティ グループ タグ 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リフレッシュするには、default を選択します。不明なポリシーをリフレッシュするには、unknown を選択します。
ステップ 3	**exit** 例： `Device# exit`	特権 EXEC モードを終了します。

SGACL ポリシーの設定例

次のセクションでは、さまざまな SGACK ポリシーの設定例を示します。

例：SGACL ポリシーの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：インターフェイスあたりの SGACL ポリシーの適用の有効化

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 ポリシーの適用の有効化

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> enable
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

次に、SGACL ポリシーを手動で設定する例を示します。

```
Device> enable
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 cts role-based permissions from 2 to 5

Role-based permissions from group 2 to group 5:
srb2
srb5
```

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> enable
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> enable
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
```

セキュリティグループ ACL ポリシーの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

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	機能情報
Cisco IOS XE Everest 16.5.1a	セキュリティグループ ACL ポリシー	SGACL を使用して、ユーザーと宛先リソースのセキュリティグループの割り当てに基づいて、ユーザーが実行できる操作を制御できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。

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。