

セキュリティグループタグ（SGT）ベースのアクセスコントロール

- SGACL 経由のユーザーアクセスコントロール （2 ページ）
- ISE 統合向け SGACL の仕組み （4 ページ）
- UPF でのセカンダリ ISE サーバーの統合 （6 ページ）
- ISE 統合向け SGACL 構成 （10 ページ）
- モニタリングおよびトラブルシューティング （15 ページ）

SGACL 経由のユーザーアクセスコントロール

表 *1:* 機能の履歴

機能名	リリース情報	説明
セキュリティグループタグ（SGT）ベースのアクセス コントロール リスト（SGACL）によるユーザー アクセス制御	2024.03.0	UPF は、ダウンリンクパケットへの SGACL の適用のための Cisco ISE 統合をサポートしています。SGACL とは、セキュリティ グループ メンバーの承認を制御および管理するアクセス制御リスト（ACL）です。 UPF は、接続先 SGT（D-SGT）に基づく API クエリ経由で ISE から SGACL マトリックスをフェッチします。D-SGT は、SMF から Sx または N4 インターフェイス経由で受信されます。次に、UPF は、ダウンリンクパケットの D-SGT と送信元 SGT（S-SGT）マッピングに基づいて SGACL を適用します。したがって、Cisco ISE からのポリシーの適用が有効になります。 **デフォルト設定**：無効：有効にするには設定が必要。
UPF での Cisco Identity Services Engine（ISE）統合向けセキュリティグループタグ（SGT）	2023.03	UPF は、SMF から受信した SGT を処理するための ISE 統合をサポートしています。SMF は、RADIUS サーバーから SGT を受信します。次に、SMF は Session Establishment 要求中に、Sx または N4 インターフェイス経由で UPF に SGT を送信します。 SGT は、Cisco ISE または SMF の静的ポリシーに従って作成されます。UPF では、アップリンクパケットの Cisco Meta Data（CMD）ヘッダーに SGT を挿入する必要があります。 **デフォルト設定**：該当なし

セキュリティグループタグ（SGT）は、信頼されたネットワーク内における通信の送信元の権限を指定します。TrustSec または ISE にセキュリティグループを追加すると、セキュリティ グループ アクセスは、自動で SGT を生成します。Cisco ISE は、集中管理型ポリシーエンジンとして、他のシスコのパケットコア要素に対して統合されたポリシー管理体験を提供します。

S-SGT は 16 ビット値で、レイヤ 2 イーサネットフレームの [Cisco Meta Data（CMD）] フィールドで送信されます。CMDヘッダーは、「.1Q」タグの後に挿入されます（ある場合）。「.1Q」タグがない場合、CMD は MAC 送信元アドレスの直後に続きます。

ISE 統合で SGT をサポートするには：

- SMF は、ISE サーバーから D-SGT を受信します。
- SMF は N4 拡張機能を使用して UPF に対して D-SGT を更新します。
- UPF はパケットを識別し、D-SGT と S-SGT の組み合わせを N6 DL パケットに適用します。

セキュリティ グループ アクセス コントロール リスト（SGACL）とは、セキュリティ グループ メンバーの承認を制御および管理するアクセス制御リスト（ACL）です。SGACL は、セキュリティ グループ タグ マトリックス（SGT マトリックス）で表される SGACL ポリシーを作成します。

SGT マトリックスは、権限マトリックスとも呼ばれ、TrustSec ドメインの SGACL ポリシーを表します。このマトリックスは、セキュリティグループ番号と接続先セキュリティグループ番号で構成され、2 つのエンドポイントの通信方法を示します。適用可能なポリシーは、Permit と Deny です。SGT マトリックスと SGACL の内容は、REST API を使用して ISE サーバーからダウンロードされます。

UPF は、N6 インターフェイス経由で送信されるアップリンクパケットの D-SGT 値を挿入します。UPF は、N6 インターフェイス経由でダウンリンクパケットの S-SGT 値を受信します。この S-SGT 値は、マトリックスルックアップに使用され、N3 インターフェイスを介した発信ダウンリンクパケットの送信中に削除されます。

接続先 SGT（D-SGT）と送信元 SGT（S-SGT）間のマッピングに基づいて、ポリシーは UPF で適用され、適切な SGACL がダウンリンクパケットに適用されます。

UPF は、次の SGT 値によるダウンリンクパケットの SGACL 適用に向けて ISE 統合をサポートしています。

- 接続先 SGT（D-SGT）：UPF は、N4 インターフェイス経由のサブスクライバセッションごとに、Session Establishment 要求の SMF からこの値を受信します。SMF は、RADIUS Access Accept メッセージで ISE から D-SGT を受信します。この機能では、SMF は N4 インターフェイスの proprietary IE で SGT を UPF に送信する必要があります。
- 送信元 SGT（S-SGT）：ダウンリンクパケットの CMDヘッダーで受信します。ワイヤレス LAN コントローラ（WLC）またはアクセススイッチは、この値を挿入します。

（注）

- SMF は、Access Accept メッセージで ISE から D-SGT を受信します。この機能では、SMF は N4 インターフェイスの proprietary IE で SGT を UPF に送信する必要があります。
- SGACL 経由でユーザー アクセス コントロールが有効になっている場合、サブスクライバ セッションが D-SGT を受信すると、SGACL がダウンリンクパケットに適用されます。この場合、APN ACL は、これらのサブスクライバセッションには適用されません。
- SGACL 経由でユーザー アクセス コントロールを有効にしない場合、または UPD が、N4 Session Establishment 要求中に D-SGT を受信しない場合、APN ACL は、既存の構成に従って適用されます。

ISE サーバープロファイルは、**ise-server-profile** *profile_name* CLI コマンドを使用して定義でき、ISE サーバープロファイルは、**associate ise-server-profile name** *server_profile_name* CLI コマンドを使用して、UPF を関連付けることができます。

ISE 統合向け SGACL の仕組み

この項では、ISE 統合用の SGACL の仕組みについて説明します。

- SMF は RADIUS 経由で ISE から対応する SGT 値をフェッチし、N4 インターフェイスで UPF に送信します。
- 各 UPF は、ISE サーバーでネットワークアクセスデバイス（NAD）として登録されます。
- UPF は、REST API を使用して ISE サーバーから SGT マトリックスおよび対応する SGACL をダウンロードします。UPF は、D-SGT から S-SGT へのマッピングに基づいて、フローに対して SGACL を適用します。
- 非リアルタイムの更新は、UPF からの定期的またはトリガ ベースのプルを通じて利用できます。
- セッションリカバリと ICSR ベースのリカバリでは、D-SGT 値をチェックポイント指定する必要があります。

通話フロー

次の図は、SGT フェッチと SGACL 適用のコールフローを示しています。

ステップ	説明
1	SMF は、N4 Session Establishment 要求を UPF に送信します。この要求の一部として、UPF は SMF から D-SGT 値を受信します。
2	UPF は、N4 Session Establishment 応答を SMF に送信します。

ステップ	説明
3	特定の D-SGT の最初のセッションの場合、UPF は ISE サーバーに REST API要求を送信して D-SGT 列の値をフェッチします。
4	ISE は、REST API 応答を UPF に送信します。この応答には、D-SGT に対してマッピングされた S-SGT 値と、SGACL 名を含む SGACL マトリックス情報と更新タイマーが含まれます。 SGT マトリックスセルエントリと SGACL は UPF に保存されます。各 D-SGT 列には、ISE で設定された更新タイマーがあります。
5	UPF は、REST API 要求を ISE サーバーに送信して、必要な SGACL をフェッチします。 ISE は、SGACL 定義を使用して、REST API 応答を UPF に送信します。
6	N3 はアップリンク（UL）データを UPF に送信します。
7	UPF はイーサネットヘッダーに D-SGT を追加し、UL データを N6 インターフェイスに送信します。
8	N6 はダウンリンク（DL）データを N3 インターフェイスに送信します。
9	UPF は D-SGT と S-SGT のマッピングをチェックし、SGACL を適用します。
10	UPF は、SGT を使用せずに DL データを N3 インターフェイスに転送します。

制限事項

この機能には、次の既知の制限事項があります。

- PFCP Session Establishment 要求は、N4 インターフェイス経由で D-SGT 値に送信されます。D-SGT は変更できませんが、S-SGT は変更できます。
- ACL は特定の SGT ペアの組み合わせに対してスタックできるため、SGACL は特定の SGT ペアに対して受信した ACL の順序に従って適用されます。
- 推奨されるマトリックスの組み合わせの最大数は、150 D-SGT 列 × 150 S-SGT 行で、デフォルトの SGACL を含む 255 の異なる SGACL があります。
- 1 つのセルに含まれる SGACL の最大数は 16 に制限されています。
- UPF は、一度に 1 つのデフォルト SGACL のみを保存できます。したがって、デフォルトの SGACL が変更されると、更新された SGACL 情報のみが UPF に保存されます。

UPF でのセカンダリ ISE サーバーの統合

表 *2:* 機能の履歴

機能名	リリース情報	説明
UPF でのセカンダリ ISE サーバーのサポート	2025.03.0	

機能名	リリース情報	説明
		この機能により、ネットワークオペレータは UPF でセカンダリ ISE サーバーを統合できます。 セカンダリ ISE サーバー統合は、プライマリ ISE サーバーがダウンしたときに SGACL のシームレスな適用を保証する障害メカニズムを提供します。 **コマンドの拡張**： • **[secondary-server { ipv4_address** *ipv4_address* **| ipv6-address** *ipv6_address* **}]**：この CLI は、セカンダリサーバー IP アドレスを構成します。 • **[secondary username** *user_name* **password** *password* **]**：この CLI は、セカンダリユーザー名とパスワードを構成します。 • **[secondary-certificate** *certificate_path* **]**：この CLI は、セカンダリ証明書パスを構成します。 • **[secondary-ca-certificate** *ca_certificate_path* **]**：この CLI は、セカンダリ CA 証明書を構成します。 • **[secondary-key** *key_path* **]**：この CLI は、セカンダリキーパスを構成します。 **導入されたコマンド**： • **max-retransmissions** *max_retrans_count*：この CLI は、最大再試行回数を構成します。 • **retransmission-timeout** *timeout_duration*：この CLI は、は再送信タイムアウト

機能名	リリース情報	説明
		を構成します。 • **backoff-period** *backoff_duration*：この CLI は、バックオフ期間を構成します。 **デフォルト設定**：無効：有効にするには構成が必要です

ISE サーバーは、UPF にポリシーを適用します。ただし、ISE サーバーに到達できないまたは ISE サーバーが停止しているなど、ISE サーバーでのサービス障害が原因で、UPF はポリシーを更新またはリフレッシュできない場合があります。

セカンダリ ISE サーバーを統合すると、UPF はポリシーの動作状態を維持し、シームレスなポリシーの適用を保証できます。

セカンダリ ISE サーバー統合の仕組み

process_workflow

これらの段階は、UPF でのセカンダリ ISE サーバーサポートのプロセスの概要です。

1. UPF は、プライマリ ISE サーバーを「アクティブ」としてマークします。アクティブなプライマリ ISE サーバーは、すべての REST API 要求を受信します。
2. UPF がプライマリ ISE サーバーとの接続を試行したが、プライマリ ISE サーバーが応答しない場合、UPF は設定された再送信回数と再送信タイムアウトに従って再接続を試行します。
3. 再接続の試行が失敗した場合、UPF は現在の「アクティブ」サーバーを「非アクティブ」としてマークします。次に、UPF は、構成に従って、セカンダリ ISE サーバーを「アクティブ」としてマークします。セカンダリ ISE サーバーを設定するには、「セカンダリ ISE サーバープロファイルを構成する」項を参照してください。

   ネットワークオペレータは、CLI を使用してアクティブな ISE サーバーを手動で選択できます。

   手動設定の詳細については、「アクティブな ISE サーバーに手動で切り替える」項を参照してください。
4. 現在「アクティブ」とマークされているサーバーは、同じ REST API 要求の受信を開始します。
5. ISE サーバーからポリシーをまだ受信していない場合、UPF は、デフォルトのポリシーまたはポリシー使用不可処理を適用します。

6. UPF は、サーバーを「アクティブ」としてマークする前に、セカンダリ ISE サーバーが最近「非アクティブ」とマークされていないことを確認します。両方のサーバーに到達不能な場合に UPF がループする問題を防ぎます。

   プライマリ ISE サーバーで障害を検出した後、UPF がセカンダリ ISE サーバーでも障害を検出した場合、またはその逆の場合、UPF は代替サーバーへの再試行を行わないはずです。これにより、UPF がループ内の ISE サーバーに到達するのを防ぎます。

   UPF は、構成されたバックオフ期間を使用してこの動作を制御します。

バックオフ期間

プライマリ ISE サーバーからセカンダリ ISE サーバーに、またはその逆に切り替えている間、両方のサーバーが到達不能な場合、UPF はループ状態になります。これを回避するために、UPF がプライマリまたはセカンダリ ISE サーバーとの接続を試行する前に、バックオフ期間が待機期間として使用されます。

バックオフ期間は、継続的な再試行による過剰なネットワーク通信とリソースの消費を防ぎます。

バックオフ期間は、ISE サーバープロファイルで設定できます。

セカンダリ ISE サーバー統合の制限事項

次に、UPF でのセカンダリ ISE サーバー統合の既知の制限事項を示します。

- ISE サーバーのエラーは、次回の REST API コールでのみ検出されます。
- プライマリまたはセカンダリ ISE サーバーの正常性に対するアクティブなモニタリングはありません。
- フェールオーバー中の REST API の場合、追加される遅延には、障害検出時間（再送信試行に基づく）およびアクティブな ISE サーバーからの接続時間または応答時間が含まれます。
- 認証の失敗によって、セカンダリ ISE サーバーへのスイッチオーバーがトリガーことは想定されていません。
- 関連する REST API 間でスイッチオーバーが発生する可能性があるため、プライマリ ISE サーバーとセカンダリ ISE サーバー間での SGT または SGACL のデータベース同期を前提としています。
- UPF は、ピアサーバー間のデータベースバージョンの不一致を検出しません。
- 定期的な更新または CLI がトリガーした更新は、以前にフェッチされたポリシーと同期していることを前提に、現在のアクティブなサーバーで実行されます。
- アクティブな ISE サーバーへのスイッチオーバーが発生すると、UPF は既存の SGACL またはポリシーを再学習しません。

再学習により遅延が増えるため、すべてのフローをオンボーディングする必要があるため、スループットに影響します。

ISE 統合向け SGACL 構成

この項では、ISE 統合向け SGACL を構成する手順について説明します。

API Manager を有効にする

API Manager は、REST API 経由で API 要求と応答の統合を可能にする機能です。

（注） API マネージャの有効化は、SGACL 統合の前提条件です。

手順

ステップ 1 構成モードを開始します。

ステップ 2 **require apimgr** コマンドを入力します。

例：

```
config
   require apimgr
end
```

この CLI コマンドは、新しいプロシージャを生成する起動構成の一部です。

次のタスク

1. ISE サーバープロファイルを構成する
2. ISE サーバープロファイルを関連付ける

ISE サーバープロファイルを構成する

次の手順では、ISE サーバープロファイルを設定します。

始める前に

ISE サーバープロファイルを設定する前に、API マネージャを有効にする必要があります。API マネージャの設定の詳細については、「API マネージャを有効にする」項を参照してください。

手順

ステップ 1 CLI **[no] ise-server-profile** *profile-name* を使用して、コンテキスト EPC モードで ISE サーバープロファイルのインスタンスを作成します。

例：

```
[local]UPF1(config)# context EPC
[local]UPF1(config-ctx)# ise-server-profile ise_1
[local]UPF1(config-ctx)#
```

ステップ 2 CLI **bind { ipv4-address** *ipv4_address* **| ipv6-address** *ipv6_address***}** を使用して、バインド IPv4 および IPv6 アドレスを指定します。

例：

```
[local]UPF1(config-ctx)# bind ipv4-address 192.0.2.1
[local]UPF1(config-ctx)#
```

ステップ 3 CLI **server { ipv4-address** *ipv4_address* **| ipv6-address** *ipv6_address* **} [secondary-server { ipv4-address** *ipv4_address* **| ipv6-address** *ipv6_address* **}]** を使用して、プライマリ ISE サーバーとセカンダリ ISE サーバーを構成します。

例：

```
[local]UPF1(config-ctx)# server ipv4-address 192.0.2.254 secondary-server ipv4-address
 198.51.100.1
```

ステップ 4 CLI **username** *user_name* **encrypted | password** *password* **[secondary username** *user_name* **password** *password* **]** を使用してプライマリ ISE サーバーとセカンダリ ISE サーバーのユーザー名とパスワードを構成します。

例：

```
[local]UPF1(config-ctx)# username ise1 password cisco1
cisco2secondary username ise2 password  cisco2
[local]UPF1(config-ctx)#
```

（注） show configuration 出力では、パスワードは暗号化された形式で表示されます。

ステップ 5 プライマリおよびセカンダリ ISE サーバーの証明書、CA 証明書、およびキーを構成します。

a) CLI **certificate** *certificate_path* **[secondary-certificate** *certificate_path* **]** を使用して、証明書を構成します。

例：

```
[local]UPF1(config-ctx)# certificate /root/certificate/client/client.cert.pem
secondary-certificate /root/certificate/client/client2.cert.pem
[local]UPF1(config-ctx)#
```

b) CLI **ca-certificate** *ca_certificate_path* および **[secondary-ca-certificate** *ca_certificate_path* **]** を使用して CA 証明書を構成します。

例：

```
[local]UPF1(config-ctx)# ca-certificate /root/certificate/ca.cert.pem
secondary-ca-certificate /root/certificate/ca.cert2.pem
[local]UPF1(config-ctx)#
```

c) CLI **key** *key_path* **[secondary-key** *key_path* **]** を使用して、キーを構成します。

例：

```
[local]UPF1(config-ctx)# key /root/certificate/client/client.key.pem
secondary-key /root/certificate/client/client2.key.pem
[local]UPF1(config-ctx)#
```

ステップ 6 CLI **policy-unavailable-treatment [drop | pass]** GACL マトリックスが具体的な D-SGT に対して使用できない場合の通信処理を指定します。

例：

```
[local]UPF1(config-ctx)# policy-unavailable-treatment drop
[local]UPF1(config-ctx)#
```

ステップ 7 最大再送信回数、再送信タイムアウト、およびバックオフ期間を設定します。

a) CLI **max-retransmissions** *max_retrans_count* を使用して、サーバーが応答しない場合の最大再送信回数を構成します。

例：

```
[local]UPF1(config-ctx)# max-retransmissions 6
[local]UPF1(config-ctx)#
```

CLI **max-retransmissions** *max_retrans_count* は、最大再試行回数を 0 ～ 15 の範囲で構成します。デフォルト値は 3 です。

b) CLI **retransmission-timeout** *timeout_duration* を使用して再送信タイムアウトを構成します。

例：

```
[local]UPF1(config-ctx)# retransmission-timeout 4000
[local]UPF1(config-ctx)#
```

retransmission-timeout *timeout_duration* 要求を ISE サーバーに再送信する前にタイムアウト期間を 1 ～ 300 秒の間で構成します。デフォルト値は 3 秒です。

c) CLI **backoff-period** *backoff_duration* を使用して、バックオフ期間を構成します。現在の構成モードを保存して終了します。

例：

```
[local]UPF1(config-ctx)# backoff-period 400
[local]UPF1(config-ctx)# exit
```

CLI **backoff-period** *backoff_duration* は、ISE サーバー y への再試行が保留される期間を構成します。デフォルト値は、200 秒です。

次のタスク

ISE サーバープロファイルを設定したら、それを既存のユーザープレーンサービスに関連付ける必要があります。詳細については、「ISE サーバープロファイルを関連付ける」項を参照してください。

アクティブな ISE サーバーに手動で切り替える

次の手順では、現在アクティブな ISE サーバーに手動で切り替えることができます。

始める前に

現在アクティブな ISE サーバーに手動で切り替える前に、ISE サーバープロファイルでセカンダリ ISE サーバーを構成します。「ISE サーバープロファイルを構成する」 項を参照してください。

手順

実行モードで、コマンド **select ise-server { primary | secondary}** を実行し、手動でアクティブな ISE SNMP に切り替えます。

例：

```
[local]laas-si-setup# select ise-server secondary
```

- 手動切り替え後、UPF は、古いあアクティブ ISE サーバーからの未処理の REST API レスポンスを受信し、UPF はそれらを処理します。
- 保留中のすべての再試行は、ISE サーバーに適用されます。このサーバーは、再試行リクエストを受信します。
- コマンド **select** は、隠しキーワードです。

ISE サーバープロファイルを関連付ける

定義されると、ISE サーバープロファイルは、既存の UPF サービス構成と関連付けられます。

始める前に

ISE サーバープロファイルを構成する

手順

ステップ 1 ユーザープレーンサービス構成モードを開始します。

ステップ 2 定義された ISE サーバープロファイルを、既存の UPF サービス構成と関連付けます。

例：

```
user-plane-service UPlane1
      associate ise-server-profile name ise_1
  #exit
```

D-SGT 列を更新する

各 D-SGT 列には、ISE で設定された更新タイマーがあります。更新タイマーの構成に基づいて、または UPF CLI トリガー経由で、D-SGT 列の値が REST API クエリ経由で ISE サーバーから再度取得されます。ISE からの API レスポンスに基づいて、SGT マトリックスまたは SGACL のバージョンが変更された場合、UPF はそれぞれのマトリックスセルまたは SGACL 情報をローカルで更新します。必要に応じて、更新後に対応する SGACL がダウンロードされます。

始める前に

1. ISE サーバープロファイルを構成する
2. ISE サーバープロファイルを関連付ける

手順

ステップ 1 Exec モードを開始します。

ステップ 2 **refresh-sgt-column** *d_sgt* コマンドを入力して、ISE サーバーから列の値をフェッチして、D-SGT 列の更新をトリガーします。

例：

```
refresh-sgt-column d-sgt
```

（注） CLI はすぐに返されますが、バックグラウンドでのポリシーのダウンロードには時間がかかるため、更新の完了にも時間がかかる場合があります。

以下は、**refresh-sgt-column** *d_sgt* CLI コマンドの出力例で、*d_sgt* 値は、*65535* に設定されます。

```
refresh-sgt-column 65535
```

モニタリングおよびトラブルシューティング

SGACL と SGT 統合を確認する

この項では、SGACL と SGT の統合機能に関する show コマンドとその出力について説明します。

show subscribers user-plane-only full callid *callid_value*

この CLI コマンドの出力が強化され、UPF の ISE 統合の D-SGT 関連情報を表示する **SGT Value** フィールドと SGACL 経由でユーザーアクセスコントロール関連の情報を表示する **SGACL match stats** フィールドが追加されました。

```
show subscribers user-plane-only full callid 00004e3a
   Local SEID      : [0x0004000000000003] 1125899906842627
  Remote SEID     : [0x00000436b7616206] 4633051357702
  State           : Connected

....

  input pkts: 20                                  output pkts: 16
  input bytes: 9246                               output bytes: 11248
  input bytes dropped: 0                          output bytes dropped: 5624
  input pkts dropped: 0                           output pkts dropped: 8

....

  SGT Value: 0x001a

....

QoS-Group Statistics:
QGR Name            Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
  FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
------------------- ---------- ---------- ---------- ---------- ---------- --------------
  -------------------  -----------------

SGACL Match stats:
ACL Name              Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Pkts dropped
--------------------- ---------- ---------- ---------- ---------- -------------
ACL2611                       4       1432          0          0             2
ACL2612                       4       4112          0          0             2
ACL2621                       8       5704          0          0             4
....

Total subscribers matching specified criteria: 1
```

show subscribers user-plane-only callid *callid_value* flows full

この CLI コマンドの出力は、SGACL 経由のユーザー アクセス コントロール関連の情報を表示する **Uplink SGT**、**Downlink SGT** および **Matched SGACL** フィールドで拡張されています。

```
show subscribers user-plane-only callid 00004e21 flows full
  Callid: 00004e21
  Interface Type: Sxab
  IP address: n/a
```

```
  Flow ID: 1:1
  Uplink pkts: 1                    Downlink pkts: 1
  Uplink bytes: 1040                Downlink bytes: 40
…
  Downlink Sfp Id: NA
  Uplink SGT: 0xA1
  Downlink SGT: 0xB5
  Matched SGACL: ACL_123
```

show user-plane-service sgt-column summary

この CLI コマンドの出力には、UPF で使用可能なすべての D-SGT 値とISE サーバーから受信した更新タイマーの概要が表示されます。

次の出力例では、**D-SGT Columns fetched** および **D-SGT Version** フィールドの D-SGT 値を示しています。

```
show user-plane-service sgt-column summary
 D-SGT Columns fetched:
 D-SGT      Version
 ---------------------------------------
 65535         0
   7           0
 Total D-SGT column(s) found: 2
```

show user-plane-service sgt-column dsgt

この CLI コマンドの出力は、D-SGT クエリ中に ISE から受信した D-SGT および S-SGT ごとの SGACL マトリックスの概要を表示します。

以下の出力例では、**D-SGT**、**Refresh TimeS-SGT**、**SGACL Name**、**Version** および **Total SGT column(s) found** フィールドを示しています。

```
show user-plane-service sgt-column dsgt 26

    D-SGT: 26            Refresh Time: 86400
    S-SGT: 1
    SGACL Name           Version
    ---------------------------------------
    ACL2611                              0
    ACL2612                              0

    S-SGT: 2
    SGACL Name                      Version
    ---------------------------------------
    ACL2621                              0

  Total SGT column(s) found: 1
```

show user-plane-service sgacl name

このCLIコマンドの出力には、SGACLクエリ中にISEから受信した具体的なSGACL定義ルール行を表示します。

```
show user-plane-service sgacl name AACL2
 SGACL Name: AACL2
```

```
permit ip
Total SGACL(s) found: 1
```

show user-plane-service statistics sgacl all

この CLI コマンドの出力には、SGACL に従ったパケット一致統計が表示されます。

```
show user-plane-service statistics sgacl all

ACL Name              Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Pkts dropped
--------------------- ---------- ---------- ---------- ---------- -------------
SGACL1-REFRESH2          6           1156       0          0          2
SGACL1-REFRESH1         13           9344       0          0          6
Allow All                0              0       0          0          0

Total SGACL(s) : 3
```

show user-plane-service statistics drop-counter

この CLI コマンドの出力は、SGACL アプリケーションが原因でドロップされたパケットを表示するように拡張されています。

```
show user-plane-service statistics drop-counter
Packet Drop Data Statistics:
        ------------------------------------------------
...
        FastPath Misc Drops:
            Overload Protection:                    0
            Invalid Client:                         0
            Stream ID 0:                            0
            Invalid Stream ID:                      0
        OHR Mismatch Packet Drops:                  0
       SGACL Packet Drops:                        8
        SGACL No Policy Packet Drops:              2
        No Default SGT cell Packet Drops:          0
```

（注）

- **No Default SGT cell Packet Drops** は、廃止されたカウンタです。既存の設計では、デフォルトの ACL が使用できない場合にのみパケットを通過させることができます。
- ISE server REST API 要求および応答の統計がサポートされています。

show apimgr statistics ise-server

show apimgr statistics ise-server には、ISE サーバー統計の状態が表示されます。

```
[local]qvpc-si# show apimgr statistics ise-server

Ise-Server Connection Statistics:

Server: 10.10.10.30           Current state: Active
Last Inactive Time:          0000:00:00:00:00:00
Request sent:                          5
Response Success:                      4
Response Fail:                         1

Server: 10.10.10.40           Current state: Inactive
```

```
Last Inactive Time:             2025:01:16:12:30:11
Request sent:                          0
Response Success:                      0
Response Fail:                         0
```

SNMP トラップ

UPF た、別の ISE サーバーに切り替わるたびに、トラップ **ISEServerSwitchoverOccured** が生成されます。

OAM のサポート

バルク統計情報

SGACL 機能によるユーザー アクセス コントロールでは、次の新しいバルク統計がサポートされています。

スキーマ：**UPF**	
統計	**説明**
downlink-total-pkts-sgacl-matched	SGACL と一致したダウンリンクパケットの総数
downlink-total-bytes-sgacl-matched	SGACL と一致したダウンリンクバイトの総数
downlink-total-pkts-sgacl-dropped	SGACL との一致が原因でドロップしたダウンリンクパケットの総数
downlink-total-bytes-sgacl-dropped	SGACL との一致が原因でドロップされたダウンリンクバイトの総数

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。

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。