

APN ACL のサポート

この章では、次のトピックについて取り上げます。

- 機能の概要と変更履歴, on page 1
- 機能説明, on page 2
- IP ソース違反, on page 5
- ゲート制御, on page 6

機能の概要と変更履歴

要約データ

Table 1: 要約データ

該当製品または機能エリア	5G-UPF
該当するプラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効：常時オン
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

更新履歴

Table 2: マニュアルの変更履歴

改訂の詳細	リリース
ゲートウェイ制御機能が拡張され、ダイナミックルールの PDRごとに追加の QER を介して有効/無効としてゲート状態が表示できるようになりました。	2024.01.1
選択的なサブスクライバセッションに通信分類とポリシーの適用を適用するために設定可能なメカニズムが導入されました。	2021.01.0
最初の導入。	2020.02.0

機能説明

IPアクセスリスト（一般にアクセス制御リスト（ACL）と呼ばれる）は、システムに出入りするパケットのフローを制御します。この構成はコンテキストごとに設定され、「ルール」（ACL ルール）または、フィルタ条件に一致するパケットに適用するアクションを制御するフィルタで構成されます。構成が完了すると、ACL を個々のサブスクライバに適用できます。IPv4 と IPv6 のアクセスルートに個別の ACL を作成できます。

次に、ACL の 2 つの重要な側面を示します。

- ルール
- ルールの順序

ルール

単一の ACL は、1 つ以上の ACL ルールで構成されます。各ルールは、パケットが特定の基準に一致した場合に、特定のアクションを実行するように設定されたフィルタです。

各ルールは、指定された基準にパケットが一致した場合に、実行するアクションを指定します。この項では、システムでサポートされているルールアクションと基準について説明します。

アクション

ACLは、指定された基準に一致するパケットに対して、次のいずれかのアクションを実行できるように指定します。

- **Permit**：パケットが受け入れられ、分類とポリシーの適用のために処理されます。
- **Deny**：パケットは拒否されます。

- **Redirect CSS**：許可アクションと同じ動作をします。

注：

- UPF では、Redirect CSS の代わりに Permit オプションを使用することを推奨します。機能的には、UPF では、両方のオプションは同じです。Redirect CSS オプションのサポートは、後方互換性のみを目的としており、後方互換性関連シナリオでのみ使用する必要があります。
- ルールなしで構成されている設定済み ACL は、「deny any」ルールを示します。これは、空の ACL のデフォルトの動作です。
- UPF では、ACL が APN に関連付けられていない場合、コールは起動します。デフォルトでは、通信は、分類およびポリシー適用のために処理されます。UPF 以外のアーキテクチャの場合、Redirect CSS が必須であるため、コールは失敗します。
- 特定の通信に対して ACL で Deny オプションのみが指定されている場合、残りの通信を通過させるには、その通信に対して Permit オプションを明示的に指定する必要があります。
- 特定の通信に対して ACL で Permit オプションのみが指定されている場合、残りの通信を通過させるには、その通信に対して Permit を明示的に指定する必要があります。
- Router Advertisement/Router Solicitation（RA/RS）パケットは、ACL の候補です。したがって、IPv6 ACL を指定する際には注意が必要です。
- ACL の構成変更は、既存のコールではなく、新しいコールに適用されます。

基準

各 ACL は、パケットの比較基準を指定する 1 つまたは複数のルールで構成されます。

サポートされる基準は次のとおりです。

- **Any**：すべてのパケットをフィルタ処理します。
- **Host**：送信元ホストの IP アドレスに基づいてパケットをフィルタ処理します。
- **ICMP**：Internet Control Message Protocol（ICMP）のパケットをフィルタ処理します。
- **IP**：Internet Protocol（IP）パケットをフィルタ処理します。
- **Source IP Address**：1 つ以上の送信元 IP アドレスに基づいてパケットをフィルタ処理します。
- **TCP**：Transport Control Protocol（TCP）パケットをフィルタ処理します。
- **UDP**：User Datagram Protocol （UDP）パケットをフィルタ処理します。

上記の基準それぞれについては、以降の項で詳述します。

- **Any**：すべてのパケットにルールが適用されます。
- **Host**：IP アドレスによって決定される特定のホストにルールが適用されます。

- **ICMP**：特定の Internet Control Message Protocol（ICMP）パケット、タイプ、またはコードにルールが適用されます。ICMP のタイプとコードの定義については、*www.iana.org*（RFC 3232）を参照してください。
- **IP**：特定のIP パケットまたはフラグメントにルールが適用されます。
- **Source IP Address**：特定の送信元アドレスまたは送信元アドレスのグループから発信される特定のパケットにルールが適用されます。
- **TCP**：任意の TCP 通信にルールが適用され、送信元/接続先の IP アドレス、特定のポート番号、またはポート番号のグループの任意の組み合わせでフィルタ処理されます。TCP ポート番号の定義については、*www.iana.org* を参照してください。
- **UDP**：任意の UDP 通信にルールが適用され、送信元/接続先の IP アドレス、特定のポート番号、またはポート番号のグループの任意の組み合わせでフィルタ処理されます。UDP ポート番号の定義については、*www.iana.org*を参照してください。

ルールの順序

複数のルールで 1 つの ACL を構成できます。各パケットは、一致が見つかるまで、各 ACL ルールを入力した順序で比較されます。一致が特定されると、後続のすべてのルールは無視されます。

制限事項

UPF の APN ACL 機能の既知の制限を次に示します。

- ACL のアドレス再指定オプションは、サポートされていません。
- コンテキストおよびネクストホップのリダイレクト ACL は、サポートされていません。
- ログオプションは、ACL ではサポートされていません。
- ACL ドロップ（IPv4 のみ）の APN レベルのバルク統計は、サポートされています。

ACL の設定

ACL を APN 経由で個々のサブスクライバに適用するには、次の構成を使用します。

```
configure
  context dest_context_name [ -noconfirm ]
    { ip | ipv6 } access-list acl_list_name
      { permit | deny | redirect }acl
      end
configure
  apn apn_name
    { ip | ipv6 } access-group acl_list_name [ in | out ]
    end
```

（注）

- 適用する ACL は、APN の接続先コンテキスト内にある必要があります（APN が設定されているコンテキストとは異なる場合があります）。
- **in** キーワードも **out** キーワードも指定しなかった場合、ACL はインバウンドとアウトバウンドのすべてのパケットに適用されます。
- 各 APN に対して 4 つのアクセスグループを適用できます。次に例を示します。

  ip access-group acl_list_name_1 in

  ip access-group acl_list_name_2 out

  ipv6 access-group acl_list_name_3 in

  ipv6 access-group acl_list_name_4 out

ACL 構成を確認する

Exec モードで次の CLI コマンドを使用して、ACL リストが適切に適用されたかどうかと、ACL が原因で削除されたパケットをチェックします。

- **show subscriber user-plane-only full all**
- **show subscribers user-plane-only full callid** *call_id*
- **show user-plane-service pdn-instance statistics** *name*

IP ソース違反

送信元検証では、受信パケットの送信元アドレスがセッション中のサブスクライバの IP アドレスと一致する必要があります。これにより、ハンドオフのシナリオでユーザーが 2 つのゲートウェイ間を何度も行き来する際に問題が発生するのを防ぐよう、ネットワークを構成できます。

UPF が送信元 IP アドレス違反のあるサブスクライバパケットを受信すると、システムは IP 送信元違反ドロップ制限カウンタをインクリメントし、IP 送信元違反期間のタイマーを開始します。IP 送信元違反期間中に不正な送信元アドレスで受信された後続の各パケットにより、ドロップ制限カウンタがインクリメントされます。たとえば、ドロップ制限を 10 に設定すると、10 の送信元違反が発生するとコールはドロップされます。検出期間タイマーは、このプロセス全体でカウントし続けます。

ユーザープレーン APN 構成で、以下を構成する必要があります。

```
ip source-violation { ignore | check [ drop-limit limit ] } [
exclude-from-accounting ]
```

Note IP source violation CLI コマンドの詳細については、「*CLI*（コマンドライン インターフェイス）のリファレンス」を参照してください。

ゲート制御

Table 3: 機能の履歴

機能名	リリース情報	説明
追加の QER を使用したゲート制御	2024.01.1	このリリースでは、UPF でサポートされる PDR あたりの QER の数が 2 から 3 に増えています。 すべてのルールとフィルタは、PDR経由でUPFに送信されます。SMFは、デフォルトのQFI/ベアラーにインストールされたダイナミックルールに対して追加のQERを送信します。Gate Status IE は、ゲートが開いているか閉じているかを示します。 **デフォルト設定**： 該当なし

UPF のゲート制御は、サービスデータフローに属する IP パケットまたは、検出されtあアプリケーションの通信の転送を有効または無効にし、目的のエンドポイントにパススルーします。「3GPP TS 23.203、subclause 4.3.2」を参照してください。

SMF は、サービスデータフローまたは検出するアプリケーションの通信向けに PDR に関連付けられている QER を作成して UPF でゲート状態を制御します。Gate Status IE に関連付けられている QER は、サービスデプロイフローまたは検出されたアプリケーション通信が、転送可能か（ゲートが開いているか）、またはアップリンクやダウンリンク方向で破棄されるか（ゲートウェイが閉じているか）を示します。

デフォルト PDR の 2 つの QER は、デフォルト QFI/ベアラーのダイナミックルールの PDR に関連付けられます。したがって、SMF は、その他の QER を作成し、デフォルトの QFI/ベアラーのダイナミックルールに関する GATE 状態を表示します。その他の QER は、ダイナミックルールの PDR に関連付けられます。したがって、UPF は、PDR アソシエーションごとに最大 3 つの QER をサポートします。

UPF は、PDR の PDI の Source Interface IE または FAR の接続先 Interface IE ごとに UL と DL のフローを識別します。UPF は、それに応じて、UL と DL ゲーティングを適用します。

SMF は、QER の Gate Status IE にある [ゲート（Gate）] フィールドを [クローズ（CLOSED）] に設定することで、PDR で受信したパケットを博するように UPF にリクエストします。

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。

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。