IP ソース違反

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • SAEGW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *P-GW Administration Guide* • *Command Line Interface Reference*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.28

機能説明

P-GW は、コントロールプレーンでのパケット送信元の検証をサポートします。コントロールプレーンからの設定がユーザープレーンにプッシュされ、その情報に基づいて、ユーザープレーンが送信元違反パケットに対処します。

送信元の検証は、パケットスプーフィングが疑われる場合や、ネットワーク内でのパケットの回送およびラベル付けの確認に有効です。送信元検証では、受信パケットの送信元アドレスが、セッション中にサブスクライバに静的または動的に割り当てられた IP アドレスと一致する必要があります。

StarOS 21.28.0 以降のリリースでは、APN コンフィギュレーション モードの一部である **ip source-violation** コマンドを使用して、IPv4 および IPv6 アドレスの IP 送信元違反の動作を追跡します。

IP ソース違反の設定

特定の APN に対するパケット送信元の検証を有効または無効にするには、次の設定を使用します。

```
configure
   context context_name
      apn apn_name
         ip source-violation { ignore | check [ drop-limit limit ] [
exclude-from-accounting ][ drop-count-timeout time-interval ] }[
traffic-type { ipv4 | ipv6 } ]
         default ip source-violation
         end
```

注：

- **default**：サブスクライバから受信した送信元アドレスの違反チェックを有効にします。セッションが削除される前にサブスクライバから受信できる無効パケットのドロップ制限数は 10 です。
- **ignore**：APN の送信元アドレスチェックを無効にします。
- **check [drop-limit** *limit* **]**：デフォルトは [Enabled] で、limit は 10 です。

  サブスクライバから受信した送信元アドレスの違反チェックを有効にします。drop-limit を設定して、セッションが削除される前にサブスクライバから受信できる無効なパケット数に対する制限を設定できます。

  limit：0 ～ 10000 の任意の整数値に設定できます。値 0 は、すべての無効なパケットが廃棄され、セッションはシステムによって削除されないことを示します。
- **exclude-from-accounting**：アカウンティングレコード用に生成された統計情報から、IP ソース違反で識別されたパケットを除外します。

- **check [drop-count-timeout time-interval]**：**drop-count-timeout** を使用すると、違反ドロップ数の更新タイマーの時間間隔を設定できます。これによりドロップカウンタ値を更新する時間間隔が指定されます。時間間隔は分単位で指定する必要があります。デフォルト値は 120 秒（2 分）です。
- **check [traffic-type { ipv4 | ipv6 }]**：パケットトラフィックのタイプを IPv4 または ipv6 で指定します。デフォルトでは、設定は IPv4 と IPv6 の両方に共通です。CLI が「traffic-type」で設定されている場合、その traffic-type の「ip source violation」CLI は、「traffic-type」なしで設定された CLI よりも優先されます。

（注） ドロップ制限とタイマーの値がゼロの場合でも、違反カウントは増分します。セッションは削除されませんが、違反したパケットはドロップされます。

モニタリングおよびトラブルシューティング

この項では、IP ソース違反機能のモニタリングと障害対応について説明します

コマンドと出力の表示

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

show subscribers full all

IPv4 および IPv6 のカウンタ違反に関連するすべての統計を個別に表示します。

表 *1 : show subscribers full all* コマンド出力の説明

フィールド	説明
ipv6 source violations	IPv6 送信元検証違反の数。
ipv6 source violations no acct	検出されたが統計に含まれていない IPv6 送信元検証違反。
ipv6 source violations ignored	検出されたが、無視された IPv6 送信元検証違反。
ipv6 source violations active	アクティブな IPv6 送信元検証違反の合計数。

show apn name *apn_name*

IPv4 および IPv6 のカウンタ違反に関連するすべての統計を個別に表示します。

表 *2 : show apn name apn_name* コマンド出力の説明

フィールド	説明
ipv4 source violations	IPv4 送信元検証違反の数。
drop limit	IPv4 送信元検証違反のドロップ制限の数。
ipv4 source violations no acct	検出されたが統計に含まれていない IPv4 送信元検証違反。
ipv6 source violations	IPv6 送信元検証違反の数。
drop limi	IPv6 送信元検証違反のドロップ制限の数。
ipv6 source violations no acct	検出されたが統計に含まれていない IPv6 送信元検証違反。

show apn statistics name *apn_name*

IPv4 および IPv6 のカウンタ違反に関連するすべての統計を個別に表示します。

表 *3 : show apn statistics name apn_name* コマンド出力の説明

フィールド	説明
IPv4 src violations	IPv4 送信元検証違反の数。
IPv4 src violations no acct	検出されたが統計に含まれていない IPv4 送信元検証違反。
IPv4 src violations ignored	検出されたが、無視された IPv4 送信元検証違反。
ipv6 src violations	IPv6 送信元検証違反の数。
ipv6 src violations no acct	検出されたが統計に含まれていない IPv6 送信元検証違反。
IPv6 src violations ignored	検出されたが、無視された IPv6 送信元検証違反。

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。