



GPRS トンネリング プロトコル サポート

General Packet Radio Service (GPRS) トンネリングプロトコルバージョン2 (GTPv2) は、2G および 3G モバイル ネットワークで使用される GPRS トンネリングプロトコルを変更して拡張する、第3世代パートナーシッププロジェクト (3GPP) の技術仕様 (TS) 29.274 で導入されました。GTPv2 は、GTP アプリケーションインスペクションと制御 (AIC) ポリシーを拡張して、加入者データにセキュリティを提供します。

このモジュールでは、ゾーンベースのポリシー ファイアウォール上に GTPv2 を設定する方法について説明します。

- [機能情報の確認, 1 ページ](#)
- [GPRS トンネリング プロトコル サポートの制約事項, 2 ページ](#)
- [GPRS トンネリング プロトコル サポートについて, 2 ページ](#)
- [GPRS トンネリング プロトコル サポートの設定方法, 6 ページ](#)
- [GPRS トンネリング プロトコル サポートの設定例, 12 ページ](#)
- [GPRS トンネリング プロトコル サポートの追加情報, 12 ページ](#)
- [GPRS トンネリング プロトコルバージョン2 サポートの機能情報, 13 ページ](#)

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の注意事項と機能情報については、[Bug Search Tool](#) およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

GPRS トンネリング プロトコル サポートの制約事項

- レイヤ 7 クラス マップの **match** ステートメントの数の制限は 64 です。
- レイヤ 7 ポリシー マップのクラス（デフォルト クラスを含む）の数の制限は 255 です。
- 正規表現（**regex**）パラメータ マップのパターン スtring の文字数の制限は 245 です。
- データ パスは、最大 512 の正規表現をサポートします。
- **match** コマンドで統計情報は使用できません。統計情報は、クラスの packets および bytes でだけ使用可能です。
- 3GPP 技術仕様 29.274 リリース 8 および 9 は、GPRS トンネリング プロトコル バージョン 2（GTPv2）と互換性はありません。

GPRS トンネリング プロトコル サポートについて

GTPv2 の概要

進化したパケットサービス（GTP または eGTP）とも呼ばれる General Packet Radio Service（GPRS）トンネリング プロトコル バージョン 2（GTPv2）は、2G および 3G モバイル ネットワーク で使用される GPRS トンネリング プロトコル から変更 および 拡張 されました。GTPv2 には、コントロール プレーン プロトコル（GTPv2-C）と ユーザ プレーン プロトコル（GTPv2-U）という 2 つの種類があります。GTPv2 は、Evolved Packet Core（EPC）ネットワークでの Serving Gateway（SGW）と Packet Data Network（PDN）ゲートウェイ（PGW）間の制御 シグナリング に主に使用されます。

第 3 世代 パートナリシップ プロジェクト（3GPP）は、第 3 世代（3G）モバイル システム 用の グローバル に受け入れ可能な仕様を開発しました。GPRS は、既存の Global System for Mobile Communication（GSM）ネットワークに統合され、企業 ネットワーク および インターネット への 常時接続 パケット 交換 データ サービス を提供します。

GTPv0 および GTPv1 の詳細については、『セキュリティ コンフィギュレーション ガイド：ゾーンベース ポリシー ファイアウォール』の「GPRS トンネリング プロトコル サポートの設定」の章を参照してください。

図 1：GTPv2-C ヘッダーの一般的な形式

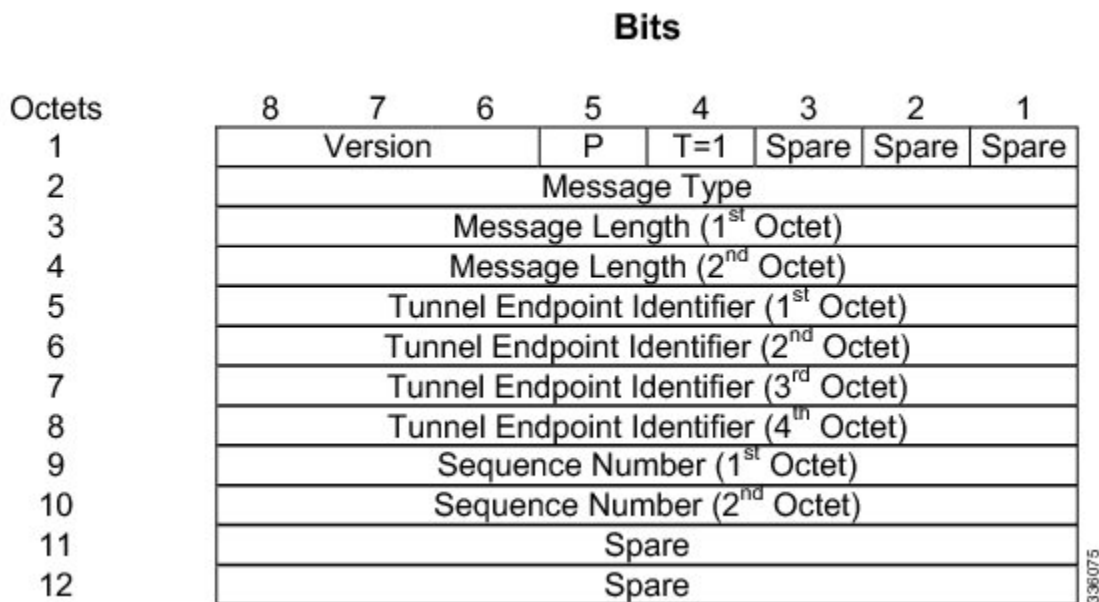
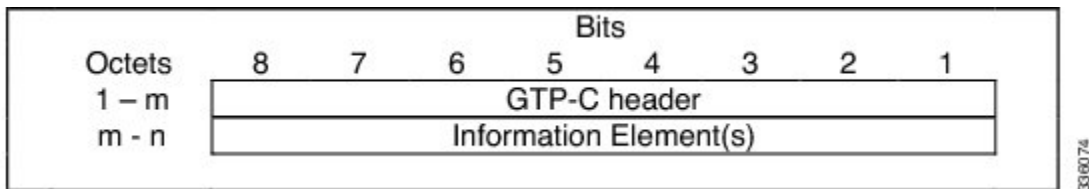


図 2：エコーおよびサポートされないバージョンのメッセージの GTPv2-C ヘッダー形式



EPC 固有のインターフェイスの GTPv2-C ヘッダーの使用は、下のように定義されています。

オクテット 1：

- オクテット 1 は、10 進数の 2（「010」）に設定されているバージョン（ビット 8～6）を表します。
- 「T」フラグ（ビット 4）が 1 に設定されている場合、トンネルエンドポイント識別子（TEID）フィールドは、オクテット 5～8 の Length フィールドのすぐ後に続きます。
- 「P」フラグ（ピギーバック サポート）はサポートされません。

オクテット 2：

- オクテット 2 は、Message Type フィールドを表します。このフィールドは GTPv2-C メッセージタイプ値をサポートします。

オクテット 3 ～ 4 :

- オクテット 3 および 4 は **Length** フィールドを表します。これは、GTPv2-C ヘッダーの必須部分（最初の 4 オクテット）を除くオクテットのメッセージの長さです。

オクテット 5 ～ 8 :

- オクテット 5 ～ 8 は、「T」フラグが最初のオクテットに設定されている場合は、**Tunnel Identifier** フィールドを表します。

オクテット 9 ～ 10 :

- オクテット 9 および 10 は、TEID が存在する場合、**Sequence Number** フィールドを表します。TEID フィールドが存在しない場合、**Sequence Number** フィールドはオクテット 5 と 6 に含まれます。

オクテット 11 ～ 12 :

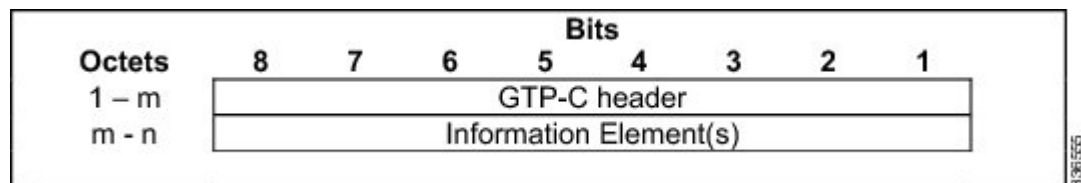
- オクテット 11 および 12 は、**Sequence Number** フィールドの後に続く 2 つのスペア オクテットです。



(注) 次のメッセージを除き、他のすべての GTPv2-C メッセージには、そのヘッダーに TEID が含まれます。

- Echo Request
- エコー応答
- サポートされないバージョンを示す

図 3: コントロール プレーンの GTPv2 メッセージの一般的な形式



ステートフル インспекション

ダイナミック パケット フィルタリングとも呼ばれるステートフル インспекションは、パケットのヘッダー内の情報に基づいてそのパケットを検査し、ファイアウォールが接続されている各接続を追跡および検証します。ステートフル インспекション中、ファイアウォールは、特定のポートへの接続要求を受信するまでポートを閉じます。

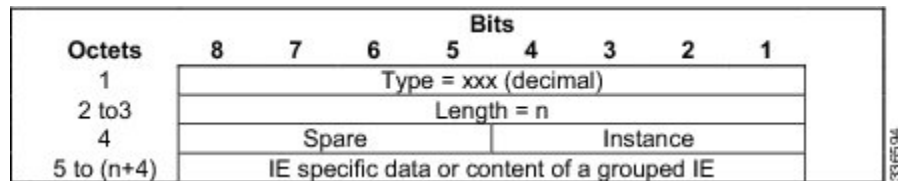
グローバルデータベースは、GTPv2 トラフィックのステートフルインスペクションのために GTP アプリケーション インスペクションと制御（AIC）ポリシーに構築されます。GTPv2 メッセージがゾーンベース ファイアウォールを通過する場合、GTP AIC ポリシーはパケット データ プロトコル（PDP）コンテキスト データベースに基づいてメッセージを検査します。レイヤ 7 インスペクションが必要なパケット（パケットのペイロードの検査または変更が必要）は、コントロールプレーンに渡されます。

情報要素

GTP ヘッダーには、情報要素（IE）と呼ばれるいくつかのオプションフィールドが含まれます。IE は、GTP プロトコル データ ユニット（PDU）に存在する場合があります。IE は、メッセージ ヘッダーに含まれる場合があります。

IE は、IE のタイプおよびインスタンスの値で識別されます。IE のタイプおよびインスタンス値の組み合わせが、メッセージ内の IE を一意に識別します。グループ化された IE には複数の IE が含まれ、4 オクテットの IE ヘッダーがあります。グループ化された IE 内の各 IE にも 4 オクテットの IE ヘッダーがあります。GTPv2 の IE の形式は、TLIV（タイプ、長さ、インスタンス、値）符号化です。グループ化された IE の長さの値は、組み込まれた IE の合計の長さです。

図 4: GTPv2-C メッセージ内の情報要素（IE）の一般的な形式



オクテット 1:

オクテット 1 は、IE Type フィールドを表します。IE Type フィールドは、GTPv2-C IE タイプの値をサポートします。

オクテット 2 ～ 3:

オクテット 2 および 3 は、Type および Length フィールドを除く IE の長さを表します。

オクテット 4:

オクテット 4 は、IE のインスタンス番号（ビット 4 ～ 1）を表します。

オクテット 5 ～ n:

オクテット 5 ～ n は、IE に含まれている実際のデータを表します。

GPRS トンネリング プロトコル サポートの設定方法

GPRS トンネリング プロトコル サポートの設定

GPRS トンネリング プロトコル バージョン 2 (GTPv2) は、ポリシーおよびクラス マップのゾーンベース ファイアウォール構造を使用して設定されます。GTPv2 および GTPv1 プロトコルは同じ宛先ポートを共有するため、レイヤ 4 クラス マップは、GTPv2 および GTPv1 を分類できません。レイヤ 7 クラス マップで分類されます。

GPRS トンネリング プロトコル サポートのパラメータ マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type regex *parameter-map-name***
4. **pattern *expression***
5. **exit**
6. **parameter-map type inspect-global gtp**
7. **gtpv2 {request-queue *elements* | tunnel-limit *tunnels*}**
8. **end**

手順の詳細

	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 モードをイネーブルにします。 • 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	parameter-map type regex <i>parameter-map-name</i> 例 : Device(config)# parameter-map type regex PARAM-REG	特定のトラフィック パターンに一致させるための正規表現 パラメータ マップ タイプを設定し、パラメータ マップ タイプ 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	pattern expression 例 : Device(config-profile)# pattern apn.cisco.com	ローカル URL フィルタリングで許可またはブロックされるドメイン、URL キーワード、または URL メタ文字のリストを指定する一致パターンを設定します。
ステップ 5	exit 例 : Device(config-profile)# exit	パラメータ マップ タイプ 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	parameter-map type inspect-global gtp 例 : Device(config)# parameter-map type inspect-global gtp	接続しきい値、タイムアウト、および inspect アクションに関連するその他のパラメータの検査タイプ パラメータ マップを設定し、パラメータ マップ タイプ コンフィギュレーション モードを開始します。
ステップ 7	gtpv2 {request-queue elements tunnel-limit tunnels} 例 : Device(config-profile)# gtpv2 request-queue 429496	GTP のインスペクション パラメータを設定します。
ステップ 8	end 例 : Device(config-profile)# end	パラメータマップタイプ検査モードを終了し、特権EXECモードに戻ります。

例 : GPRS トンネリング プロトコル サポートのパラメータ マップ

次に、**show parameter-map type** コマンドの出力例を示します。

```
Device# show parameter-map type inspect-global gtp
```

```
parameter-map type inspect-global gtp
  gtp request-queue 40000 (default)
  gtp tunnel-limit 40000 (default)
  gtp pdp-context timeout 300 (default)
  gtp request-queue timeout 60 (default)
  permit-error Disable (default)
  gtpv2 request-queue 429496729
  gtpv2 tunnel-limit 42949672
```

GPRS トンネリング プロトコル サポートのクラス マップおよびポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect** *protocol-name* {**match-any** | **match-all**} *class-map-name*
4. **match** {**apn regex** *parameter-name* | {**mcc country-code mnc network-code** | **message-length msisdn regex** *parameter-name* | **version number**}
5. **exit**
6. **policy-map type inspect** *protocol-name* *policy-map-name*
7. **class type inspect** *protocol-name* *class-map-name*
8. **inspect**
9. **service-policy** *protocol-name* **policy-map**
10. **end**

手順の詳細

	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 モードをイネーブルにします。 • 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	class-map type inspect <i>protocol-name</i> { match-any match-all } <i>class-map-name</i> 例 : Device(config)# class-map type inspect gtpv1 match-any gtpv2-cl7-1	レイヤ 7（アプリケーション固有）検査タイプクラス マップを作成し、クラスマップ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	match { apn regex <i>parameter-name</i> { mcc country-code mnc network-code message-length msisdn regex <i>parameter-name</i> version number } 例 : Device(config-cmap)# match version 2	GTP の検査タイプクラス マップ用の分類基準を設定します。

	コマンドまたはアクション	目的
ステップ 5	exit 例 : Device(config-cmap)# exit	クラス マップ 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	policy-map type inspect protocol-name policy-map-name 例 : Device(config)# policy-map type inspect gtpv1 gtpv2-POLICY-MAP	レイヤ 7 (プロトコル固有) 検査タイプポリシーマップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 7	class type inspect protocol-name class-map-name 例 : Device(config-pmap)# class type inspect gtpv1 gtpv2-cl7-1	アクションを実行する対象のトラフィック (クラス) を指定し、ポリシーマップクラス コンフィギュレーション モードを開始します。
ステップ 8	inspect 例 : Device(config-pmap-c)# inspect	ステートフル パケット インスペクションをイネーブルにします。
ステップ 9	service-policy protocol-name policy-map 例 : Device(config-pmap-c)# service-policy gtpv1 gtpv2-POLICY-MAP	レイヤ 7 ポリシー マップをトップレベルのレイヤ 3 またはレイヤ 4 ポリシー マップに付加します。
ステップ 10	end 例 : Device(config-pmap-c)# end	ポリシーマップクラス 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。

GPRS トンネリング プロトコル サポートのゾーンおよびゾーン ペアの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security {zone-name | default}**
4. **exit**
5. **zone-pair security zone-pair-name source {source-zone-name | self | default} destination {destination-zone-name | self | default}**
6. **service-policy type inspect policy-map-name**
7. **exit**
8. **interface type number**
9. **zone-member security zone-name**
10. **end**

手順の詳細

	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 モードをイネーブルにします。 • 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	zone security {zone-name default} 例 : Device(config)# zone security z1 Device(config)# zone security z2	インターフェイスを割り当てることのできるセキュリティゾーンを作成し、セキュリティ ゾーンコンフィギュレーションモードを開始します。 (注) セキュリティ ゾーン ペアを作成するには、インターフェイスを割り当てる2つのセキュリティゾーン (z1 と z2) を設定する必要があります。
ステップ 4	exit 例 : Device(config-sec-zone)# exit	セキュリティ ゾーン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。

	コマンドまたはアクション	目的
ステップ 5	zone-pair security <i>zone-pair-name</i> source { <i>source-zone-name</i> self default } destination { <i>destination-zone-name</i> self default } 例 : Device(config)# zone-pair security clt2srv1 source z1 destination z2	セキュリティ ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。 (注) ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 6	service-policy type inspect <i>policy-map-name</i> 例 : Device(config-sec-zone-pair)# service-policy type inspect gtpv2-POLICY-MAP	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 (注) セキュリティ ゾーンのペア間でポリシーが設定されていない場合、トラフィックはデフォルトでドロップされます。
ステップ 7	exit 例 : Device(config-sec-zone-pair)# exit	セキュリティ ゾーンペア 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 8	interface type number 例 : Device(config)# interface gigabitethernet 0/0/0	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 モードに戻ります。
ステップ 9	zone-member security zone-name 例 : Device(config-if)# zone-member security z1	インターフェイスを指定したセキュリティゾーンに割り当てます。 (注) インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（デバイス宛のトラフィックまたはデバイス発信のトラフィックを除く）は、デフォルトでドロップされます。トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 10	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。

GPRS トンネリング プロトコル サポートの設定例

例：GPRS トンネリング プロトコル サポートの設定

次に、GTPv2 サポートを設定する例を示します。

```

Device> enable
Device# configure terminal
Device(config)# parameter-map type regex PARAM-REG
Device(config-profile)# pattern apn.cisco.com
Device(config-profile)# exit
Device(config)# parameter-map type inspect-global
Device(config-profile)# gtpv2 tunnel-limit 100
Device(config-profile)# exit
Device(config)# class-map type inspect gtpv1 match-any gtpv2-cl7-1
Device(config-cmap)# match version 2
Device(config-cmap)# exit
Device(config)# policy-map type inspect gtpv1 gtpv2-POLICY-MAP
Device(config-pmap)# class type inspect gtpv1 gtpv2-cl7-1
Device(config-pmap-c)# inspect
Device(config-pmap-c)# service-policy gtpv1 gtpv2-POLICY-MAP
Device(config-pmap)# end

```

例：GPRS トンネリング プロトコル サポートのゾーンおよびゾーン ペアの設定

次に、GTPv2 にゾーンおよびゾーン ペアを設定する例を示します。

```

Device> enable
Device# configure terminal
Device(config)# zone security z1
Device(config-sec-zone)# exit
Device(config)# zone-pair security clt2srv1 source z1 destination z2
Device(config-sec-zone-pair)# service-policy type inspect gtpv2-POLICY-MAP
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# ip address 5.0.0.1 255.255.255.0
Device(config-if)# zone-member security z1
Device(config-if)# exit
Device(config)# interface gigabitethernet0/0/2
Device(config-if)# ip address 4.0.0.1 255.255.255.0
Device(config-if)# zone-member security z2
Device(config)# end

```

GPRS トンネリング プロトコル サポートの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	『Security Command Reference: Commands A to C』 『Security Command Reference: Commands D to L』 『Security Command Reference: Commands M to R』 『Security Command Reference: Commands S to Z』
セキュリティ 設定	『Security Configuration Guide: Zone-Based Policy Firewall』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

GPRS トンネリング プロトコル バージョン 2 サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 1: GPRS トンネリング プロトコル バージョン 2 サポートの機能情報

機能名	リリース	機能情報
GTPv2 Support	Cisco IOS XE Release 3.9S	GTPv2 サポート機能は、第3世代パートナーシッププロジェクト (3GPP) TS 29.274 によって導入され、2G および 3G モバイル ネットワークで使用される GPRS トンネリング プロトコルを変更および拡張します。GTPv2 は、GTP アプリケーション インспекション と制御 (AIC) ポリシーを拡張して、加入者データにセキュリティを提供します。 このモジュールでは、ゾーンベースのポリシー ファイアウォール上に GTPv2 を設定する方法について説明します。 次のコマンドが、新たに導入または変更されました。 show parameter-map type inspect-global、zone-pair security。