フローあたりの同時パケットの設定可能数

ゾーンベース ポリシー ファイアウォールでは、フローあたりの同時パケットの数は 25 に制限されており、この制限を超えるパケットはドロップされます。この制限に達したためにパケットのドロップが発生すると、ネットワークのパフォーマンスに影響します。フローあたりの設定可能な同時パケット数機能では、フローあたりの同時パケットの数を 25 ～ 100 の範囲で設定できます。

このモジュールではこの機能について概説し、この機能を設定する方法を説明します。

フローあたりの同期パケットの設定可能数に関する制約事項

- TCP ウィンドウ スケール オプションが設定されている場合、ファイアウォールはフローあたりの多すぎる TCP パケットを同時に処理できないため、設定された制限を超えたパケットはドロップされます。TCP ウィンドウ スケール オプションが有効になっている場合は、使用可能な最大ウィンドウ サイズが 1 GB になります。

  標準の TCP ウィンドウ サイズは 2～65,535 バイトの間です。TCP ペイロード サイズが 655 バイト未満の場合は、1 つの TCP ウィンドウに属しているすべての TCP パケットを 100 個の同時パケットに含めることができないため、パケット ドロップが発生する可能性があります。パケット ドロップを回避するには、TCP ペイロード サイズを大きくするか、TCP ウィンドウ サイズを小さくすることをお勧めします。

- 各プラットフォームで利用可能な総スレッド数は有効なライセンス レベルによって異なります。設定されたフローあたりの同時パケット数が利用可能なハードウェア スレッド数を超えている場合は、同時パケット数の設定が無効になります。

フローあたりの同時パケットの設定可能数に関する情報

設定可能なフローごとの同時パケット数の概要

フローごとの同時パケット数は設定可能であるため、フローごとにネットワークに入ることができる同時パケット数を増やすことができます。フローごとの同時パケット数は、25から100まで増加させることができます。デフォルトの同時パケット数は25です。

マルチスレッド環境では、ゾーンベース ポリシー ファイアウォールが単一のトラフィック フローで複数のパケットを同時に受信する場合があります。ファイアウォールがパケットの処理中に使用するロックのタイプには、フロー ロックとソフトウェア ロックの2つがあります。フロー ロックでは、同じフローに属するパケットが正しい順序で処理されるようになります。通常のソフトウェア ロックは、クリティカルセクションまたは共通データ構造（メモリなど）に対して、複数の Power Processing Element（PPE）スレッドが同時に読み取りや書き込みを試行する際に使用されます。

フローごとの同時パケット数が大きいと、スレッドがロックを要求して取得するまでの時間が大幅に長くなります。この遅延は、リソースの再利用やとハートビート処理などといったタイムクリティカルなインフラストラクチャに悪影響を与えます。遅延を制御するために、同時パケットの数は25に制限され、25を超えるパケットはドロップされていました。

ただし、パケットのドロップはシステムパフォーマンスに多大な影響を与えます。パケットのドロップを最小限に抑えるために、設定可能なフローごとの同時パケット数の機能が導入されました。フローごとの同時パケット数をデフォルトの25から最大100までに変更して設定できます。

フローごとの同時パケット数を変更するには、**parameter-map type inspect** *parameter-map-name* コマンドまたは **parameter-map type inspect global** コマンドの後に **session packet** コマンドを続けて設定する必要があります。**parameter-map type inspect** *parameter-map-name* コマンドで設定された制限は、**parameter-map type inspect global** コマンドで設定された制限より優先されます。

ファイアウォールは、Session Initiation Protocol（SIP）トランクのトラフィックを単一のセッションと見なします。ただし、SIP トランクのトラフィックには、さまざまなユーザのアプリケーション層ゲートウェイ（ALG）フローが多数含まれます。SIP トランクのトラフィックのスループットが他のトラフィックに比べて高いと、同時パケット数の制限によってパケットがドロップされて、ユーザのコールが終了される可能性があります。

フローあたりの同時パケット数の設定方法

フローあたりの同時パケットのクラス マップとポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect** {**match-any** | **match-all**} *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **policy-map type inspect** *policy-map-name*
7. **class type inspect** *class-map-name*
8. **inspect**
9. **exit**
10. **class class-default**
11. **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 モードを有効にします。
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。 • パスワードを入力します（要求された場合）。
ステップ 3	**class-map type inspect** {**match-any** | **match-all**} *class-map-name* 例： `Device(config)# class-map type inspect match-any cmap-protocols`	検査タイプ クラス マップを作成して、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 protocol** *protocol-name* 例： `Device(config-cmap)# match protocol tcp`	指定されたプロトコルを基づくクラス マップの一致基準を設定します。

	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 モードを終了して、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** *policy-map-name* 例： `Device(config)# policy-map type inspect policy1`	検査タイプ ポリシー マップを作成して、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** *class-map-name* 例： `Device(config-pmap)# class type inspect cmap-protocols`	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	**exit** 例： `Device(config-pmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション モードを終了して、ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 10	**class class-default** 例： `Device(config-pmap)# class class-default`	デフォルト クラスのポリシーを設定または変更します。
ステップ 11	**end** 例： `Device(config-pmap)# end`	ポリシー マップ 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。

フローあたりの同時パケット数の設定

parameter-map type inspect コマンドまたは **parameter-map type inspect global** コマンドのいずれかを設定した後で、フローあたりの同時パケットの数を設定できます。**parameter-map type inspect** コマンドで設定されたフローあたりの同時パケット数は、**parameter-map type inspect global** コマンドで設定された数を上書きします。

フローあたりの同時パケットの数を設定するには、**session packet** コマンドを設定する必要があります。

（注） ステップ 3 と 4 またはステップ 6 と 7 のどちらかを設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** *parameter-map-name*
4. **session packet** *number-of-simultaneous-packets*
5. **exit**
6. **parameter-map type inspect global**
7. **session packet** *number-of-simultaneous-packets*
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 モードを有効にします。
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。 • パスワードを入力します（要求された場合）。
ステップ 3	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect param1`	（オプション）接続しきい値、タイムアウト、および検査アクションに関連するその他のパラメータを設定する、検査タイプ パラメータ マップを定義します。また、parameter-map タイプ検査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	**session packet** *number-of-simultaneous-packets* 例： `Device(config-profile)# session packet 55`	（オプション）セッションごとに設定可能な同時トラフィック パケットの数を設定します。 • *number-of-simultaneous-packets* 引数の有効値は 25 ～ 55 です。
ステップ 5	**exit** 例： `Device(config-profile)# exit`	パラメータマップ タイプ検査コンフィギュレーション モードを終了して、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** 例： `Device(config)# parameter-map type inspect global`	（オプション）グローバル検査パラメータ マップを定義して、parameter-map タイプ検査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	**session packet** *number-of-simultaneous-packets* 例： `Device(config-profile)# session packet 35`	（オプション）セッションごとに設定可能な同時トラフィック パケットの数を設定します。 • *number-of-simultaneous-packets* 引数の有効値は 25 ～ 55 です。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

フローあたりの同時パケットのゾーンの設定

この作業では、セキュリティ ゾーン、ゾーン ペアを設定し、ゾーン メンバーとしてインターフェイスを割り当てる方法を示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *security-zone*
4. **exit**
5. **zone security** *security-zone*
6. **exit**
7. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **zone-member security** *zone-name*
12. **exit**
13. **interface** *type number*
14. **zone-member security** *zone-name*
15. **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。

	コマンドまたはアクション	目的
ステップ 3	**zone security** *security-zone* 例： `Device(config)# zone security z1`	インターフェイスを割り当てることが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。 • 送信元ゾーンと宛先ゾーンという、ゾーン ペアを作成するための 2 つのセキュリティ ゾーンが必要です。
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。
ステップ 5	**zone security** *security-zone* 例： `Device(config)# zone security z2`	インターフェイスを割り当てることが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。 • 送信元ゾーンと宛先ゾーンという、ゾーン ペアを作成するための 2 つのセキュリティ ゾーンが必要です。
ステップ 6	**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。
ステップ 7	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security zp-security source z1 destination z2`	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。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect policy1`	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。 • ゾーンのペア間でポリシーが設定されない場合、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 9	**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 10	**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 モードを開始します。

	コマンドまたはアクション	目的
ステップ 11	**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。 • 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、そのインターフェイスを通して送受信されるすべてのトラフィックは、デフォルトでドロップされます（ただしデバイス宛のトラフィックとデバイス発のトラフィックを除く）。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 12	**exit** 例： `Device(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 13	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/3`	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。
ステップ 14	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security z2`	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。
ステップ 15	**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。

フローあたりの同時パケットの設定可能数の設定例

例：フローあたりの同時パケットのクラス マップとポリシー マップの設定

```
Device# configure terminal
Device(config)# class-map type inspect match-any cmap-protocols
Device(config-cmap)# match protocol tcp
Device(config-cmap)# exit
Device(config)# policy-map type inspect policy1
Device(config-pmap)# class type inspect cmap-protocols
Device(config-pmap-c)# inspect
```

```
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap)# end
```

例：フローあたりの同時パケット数の設定

parameter-map type inspect コマンドまたは **parameter-map type inspect global** コマンドのいずれかを設定した後で、フローあたりの同時パケットの数を設定できます。**parameter-map type inspect** コマンドで設定されたフローあたりの同時パケット数は、**parameter-map type inspect global** コマンドで設定された数を上書きします。

```
Device# configure terminal
Device(config)# parameter-map type inspect param1
Device(config-profile)# session packet 55
Device(config-profile)# exit
Device(config)# parameter-map type inspect global
Device(config-profile)# session packet 35
Device(config-profile)# end
```

例：フローあたりの同時パケットのゾーンの設定

```
Device# configure terminal
Device(config)# zone security z1
Device(config-sec-zone)# exit
Device(config)# zone security z2
Device(config-sec-zone)# exit
Device(config)# zone-pair security zp-security source z1 destination z2
Device(config-sec-zone-pair)# service-policy type inspect policy1
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# zone-member security z1
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/0/3
Device(config-if)# zone-member security z2
Device(config-if)# end
```

フローあたりの同時パケットの設定可能数に関する追加情報

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
ファイアウォール コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

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

フローあたりの同時パケットの設定可能数に関する機能情報

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:* フローあたりの同時パケットの設定可能数に関する機能情報

機能名	リリース	機能情報
フローあたりの同時パケットの設定可能数	Cisco IOS XE リリース 3.11S	ゾーンベース ポリシー ファイアウォールでは、フローあたりの同時パケット数が 25 に制限され、その制限を超えたパケットはドロップされました。上限に達したことによるパケットのドロップは、ネットワーク パフォーマンスに影響します。フローあたりの設定可能な同時パケット数機能では、フローあたりの同時パケットの数を 25 ～ 100 の範囲で設定できます。 Cisco IOS XE リリース 3.11S では、この機能が Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ、Cisco 4400 シリーズ サービス統合型ルータ、およびシスコ クラウド サービス ルータ 1000V シリーズで導入されました。 次のコマンドが導入または変更されました。**session packet**、**show parameter-map type inspect**、**show platform hardware qfp feature firewall datapath scb**、**show platform hardware qfp feature firewall zone-pair**、および **show platform software firewall parameter-map**。

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。