ファイアウォール リソース管理の設定

ファイアウォール リソース管理機能は、ルータで設定される VPN ルーティングおよび転送（VRF）セッションとグローバル ファイアウォール セッションの数を制限します。

ファイアウォールリソース管理の設定に関する制約事項

- グローバル レベルまたは VRF レベルのセッション制限を設定した後、その制限値を下回るセッション制限を再設定すると、新しいセッションは追加されなくなります。ただし、現在のセッションはドロップされません。

ファイアウォール リソース管理の設定について

ファイアウォール リソース管理

リソース管理では、デバイス上の共有リソースの利用レベルが制限されます。デバイス上の共有リソースには次のものがあります。

- 帯域幅
- 接続状態
- メモリ使用率（テーブル単位）
- セッションまたはコールの数
- Packets per second（1 秒あたりのパケット数）

- Ternary content addressable memory（TCAM）エントリ

ファイアウォール リソース管理機能は、ゾーンベースのファイアウォール リソース管理をクラス レベルから VRF レベルおよびグローバル レベルに拡張します。クラス レベルのリソース管理は、クラス レベルでファイアウォール セッションのリソースを保護します。たとえば、最大セッション制限、セッション レート制限、不完全セッション制限などのパラメータは、ファイアウォール リソース（チャンク メモリなど）を保護し、これらのリソースが単一クラスによって使い果たされないようにします。

複数の Virtual Routing and Forwarding（VRF）インスタンスが同じポリシーを共有する場合、1 つの VRF インスタンスからのファイアウォール セッション設定要求によって総セッション数が最大制限に達する可能性があります。1 つの VRF がデバイス上で最大量のリソースを消費すると、他の VRF インスタンスがデバイス リソースを共有することが難しくなります。VRF ファイアウォール セッションの数を制限するには、ファイアウォール リソース管理機能を使用できます。

グローバル レベルでは、ファイアウォール リソース管理機能により、グローバル ルーティング ドメインでのファイアウォール セッションによるリソースの使用を制限できます。

VRF 対応 Cisco IOS XE ファイアウォール

サービス プロバイダー（SP）または大企業のエッジ ルータで VRF 対応 Cisco IOS XE ファイアウォールが設定されている場合は、Cisco IOS XE ファイアウォール機能が VPN ルーティングおよび転送（VRF）インターフェイスに適用されます。SP は中小企業市場にマネージドサービスを提供しています。

VRF 対応 Cisco IOS XE ファイアウォールは、さまざまなプロトコルの VRF-Lite（別名 Multi-VRF CE）と Application Inspection and Control（AIC）をサポートします。

VRF 対応ファイアウォールは、さまざまなプロトコルの VRF-Lite（別名 Multi-VRF CE）と Application Inspection and Control（AIC）をサポートします。

（注） Cisco IOS XE リリースは、コンテキストベースのアクセス コントロール（CBAC）ファイアウォールをサポートしません。

ファイアウォール セッション

セッション定義

Virtual Routing and Forwarding（VRF）レベルでは、ファイアウォール リソース管理機能により、各 VRF インスタンスのファイアウォール セッション数が追跡されます。グローバル レベルでは、ファイアウォール リソース管理機能により、デバイス レベルではなくグローバル ルーティング ドメインでのファイアウォール セッションの合計数が追跡されます。VRF とグローバル レベルの両方では、セッション数はオープン セッションとハーフオープン セッションと

不正確なファイアウォール セッション データベース内のセッションの合計です。まだ確立状態に達していない TCP セッションは、ハーフオープン セッションと呼ばれます。

ファイアウォールには 2 つのセッション データベースがあります。1 つはセッション データベースで、もう 1 つは不正確なセッションデータベースです。セッションデータベースには、5 つのタプル（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびプロトコル）のセッションが含まれます。タプルは、要素の番号付きリストです。不正確なセッションデータベースには、5 つ未満のタプル（欠落した IP アドレス、ポート番号など）のセッションが含まれます。

次の規則は、セッション制限の設定に適用されます。

- クラスレベル セッションの上限は、グローバルの制限を超える可能性があります。
- クラスレベル セッションの上限は、関連する VRF セッションの最大値を超える可能性があります。
- VRF 制限値の合計は、グローバルなコンテキストを含め、ハードコーディングされたセッションの制限を超える可能性があります。

セッション レート

セッション レートは、セッションが特定の時間間隔で確立されるレートです。最大および最小セッション レート制限を定義できます。セッション レートが指定された最大レートを超えると、ファイアウォールは新しいセッションのセットアップ要求を拒否し始めます。

リソース管理の観点から最大および最小セッション レート制限を設定すると、多数のファイアウォール セッションのセットアップ要求が受信された場合に、Cisco Packet Processor が過負荷になることを防ぐのに役立ちます。

未完了またはハーフオープン セッション

未完了セッションはハーフオープンセッションです。未完了セッションで使用されるリソースがカウントされ、未完了セッション数の増加は最大セッション数制限を設定することにより制限されます。

ファイアウォール リソース管理セッション

ファイアウォール リソース管理セッションには次のルールが適用されます。

- デフォルトでは、オープン セッションまたはハーフオープン セッションのセッション制限は無制限です。
- オープン セッションまたはハーフオープン セッションは、パラメータで制限され、個別にカウントされます。
- オープン セッションの数またはハーフオープン セッションの数には、Internet Control Message Protocol（ICMP）、TCP、または UDP セッションが含まれます。
- オープン セッションの数とレートを制限できます。

• ハーフオープン セッションではセッションの数だけを制限できます。

ファイアウォール リソース管理の設定方法

ファイアウォール リソース管理の設定

（注） グローバル パラメータ マップは、ルータ レベルではなく、グローバル ルーティング ドメインで有効になります。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-vrf** *vrf-pmap-name*
4. **session total** *number*
5. **tcp syn-flood limit** *number*
6. **exit**
7. **parameter-map type inspect-global**
8. **vrf** *vrf-name* **inspect** *parameter-map-name*
9. **exit**
10. **parameter-map type inspect-vrf vrf-default**
11. **session total** *number*
12. **tcp syn-flood limit** *number*
13. **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。
ステップ 3	**parameter-map type inspect-vrf** *vrf-pmap-name* 例： `Device(config)# parameter-map type inspect-vrf vrf1-pmap`	VRF 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 タイプ検査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	**session total** *number* 例： `Device(config-profile)# session total 1000`	セッションの総数を設定します。
ステップ 5	**tcp syn-flood limit** *number* 例： `Device(config-profile)# tcp syn-flood limit 2000`	新しい SYN パケットの同期（SYN）Cookie 処理をトリガーする TCP ハーフ オープン セッションの数を制限します。
ステップ 6	**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、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 7	**parameter-map type inspect-global** 例： `Device(config)# parameter-map type inspect-global`	グローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 8	**vrf** *vrf-name* **inspect** *parameter-map-name* 例： `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	VRF をパラメータ マップにバインドします。
ステップ 9	**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、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 10	**parameter-map type inspect-vrf vrf-default** 例： `Device(config)# parameter-map type inspect-vrf vrf-default`	デフォルトの VRF 検査タイプ パラメータ マップを設定します。
ステップ 11	**session total** *number* 例： `Device(config-profile)# session total 6000`	セッションの総数を設定します。 • VRF 検査タイプパラメータマップ用およびグローバルパラメータマップ用に **session total** コマンドを設定できます。VRF 検査タイプパラメータマップ用に **session total** コマンドを設定する場合、VRF 検査タイプパラメータマップにセッションが関連付けられます。グローバルパラメータマップ用に **session total** コマンドを設定する場合、このコマンドはグローバル ルーティング ドメインに適用されます。

	コマンドまたはアクション	目的
ステップ 12	**tcp syn-flood limit** *number* 例： `Device(config-profile)# tcp syn-flood limit 7000`	新しいSYNパケットのSYN Cookie処理をトリガーするTCPハーフ オープン セッションの数を制限します。
ステップ 13	**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、特権 EXEC モードを開始します。

ファイアウォール リソース管理の設定例

例：ファイアウォール リソース管理の設定

```
Device# configure terminal
Device(config)# parameter-map type inspect-vrf vrf1-pmap
Device(config-profile)# session total 1000
Device(config-profile)# tcp syn-flood limit 2000
Device(config-profile)# exit
Device(config)# parameter-map type inspect-global
Device(config-profile)# vrf vrf1 inspect pmap1
Device(config-profile)# exit
Device(config)# parameter-map type inspect-vrf vrf-default
Device(config-profile)# session total 6000
Device(config-profile)# tcp syn-flood limit 7000
Device(config-profile)# end
```

その他の参考資料

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 Commands List, All Releases』
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』
VRF 対応ファイアウォール	「VRF 対応 Cisco IOS XE ファイアウォール」モジュール

関連項目	マニュアル タイトル
ゾーンベース ポリシー ファイアウォール	「ゾーンベース ポリシー ファイアウォール」モジュール

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ファイアウォール リソース管理の設定に関する機能情報

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:* ファイアウォール リソース管理の設定に関する機能情報

機能名	リリース	機能情報
ファイアウォール リソース管理	Cisco IOS XE リリース 3.3S	ファイアウォール リソース管理機能は、ルータで設定される VPN ルーティングおよび転送（VRF）セッションとグローバル ファイアウォール セッションの数を制限します。 次のコマンドが導入または変更されました。**parameter-map type inspect-vrf**。

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。