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。

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。

ファイアウォール リソース管理の設定の制約事項

- 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、セッション制限を再設定すると、グローバル レベルまたはVRF レベルのセッション制限が最初に設定されたセッショ

ン数よりも低い場合、新しいセッションは追加されません。ただし、既存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

リソース管理は、デバイス上の共有リソースの利用レベルを制限します。 デバイス上の共有リソースは次のとおりです。

- 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数
- 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。

複数の仮想ルーティングおよび転送（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 がデバイス上のリソースの最大量を消費すると、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ために、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-Aware Cisco IOS XE ファイアウォール

VRF-Aware Cisco IOS XE ファイアウォールは、ファイアウォールがサービス プロバイダー（SP）または大企業のエッジ ルータに設定されている場合、VPN ルーティングおよび転送（VRF）インターフェイスに Cisco IOS XE ファイアウォール機能を適用します。 SP は中小企業の市場向けにマネージド サービスを提供します。

VRF-Aware Cisco IOS XE ファイアウォールは、VRF-lite（Multi-VRF CE とも呼ばれる）および各種プロトコルでのアプリケーション インスペクションと制御（AIC）をサポートします。

VRF 認識ファイアウォールは、VRF-lite（Multi-VRF CE とも呼ばれる）および各種プロトコルでのアプリケーション インスペクションと制御（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 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

仮想ルーティングおよび転送（VRF）レベルで、ファイアウォール リソース管理機能は、各 VRF インスタンスのファイアウォール セッションの数を追跡します。 グローバル レベルでは、ファイアウォール リソース管理は、デバイス レベルではなくグローバル ルーティング ドメインで総ファイアウォール セッション数を追跡します。 VRF レベルとグローバル レベルの両方で、セッション数は、開かれたセッション、ハーフ オープン セッション、および明確でないファイアウォール セッション データベース内のセッションの合計です。 確立状態にまだ到達していない 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（セッション データベースおよび明確でないセッション データベース）があります。 セッション データベースには、5 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、要素の順序付きリストです。 明確でないセッション データベースには、5 タプルよりも少ない（IP アドレスやポート番号などが欠落している）セッションが含まれます。

次のルールが、セッション制限の設定に適用されます:

- クラス レベルのセッション制限は、グローバル制限を超えることができます。
- クラス レベルのセッション制限は、関連付けられた VRF セッションの最大値を超えることができます。
- グローバル コンテキストを含む VRF 制限の合計は、ハードコーディングされたセッション制限を超えることができます。

セッション レート

セッション レートは、特定の時間間隔でセッションが確立されるレートです。 最大および最小のセッション 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設定要求を拒否するようになります。

リソース管理の観点から、最大および最小のセッション レート制限を設定すると、Cisco Packet Processor が多数のファイアウォール セッション設定要求を受信して過負荷状態になるのを防ぐことができます。

不完全なセッションまたはハーフ オープン セッション

不完全なセッションは、ハーフ オープン セッションです。 最大セッション制限を設定することで、不完全なセッションが使用するリソースがカウントされ、不完全なセッション数の増加が制限されます。

ファイアウォール リソース管理セッション

次のルールが、ファイアウォール リソース管理セッションに適用されます。

- デフォルトでは、開かれた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。
- 開かれた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。
- 開かれたセッション数またはハーフ オープン セッション数には、インターネット制御メッセージ プロトコル（ICMP）、TCP、または UDP セッションが含まれます。
- 開かれた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 セッションの数のみを制限できます。

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 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。
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 セッション数を制限します。

	コマンドまたはアクション	目的
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`	パラメータ マップに VRF をバインドします。
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。 • **session total** コマンドを VRF 検査タイプ パラメータ マップおよびグローバル パラメータ マップに設定できます。 VRF 検査タイプ パラメータ マップに **session total** コマンドを設定した場合、セッションは VRF 検査タイプ パラメータ マップに関連付けられます。 **session total** コマンドがグローバル パラメータ マップに設定された場合、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。
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 セッション数を制限します。

	コマンドまたはアクション	目的
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
```

その他の関連資料

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』

関連項目	マニュアル タイトル
VRF 認識ファイアウォール	「VRF-Aware Cisco IOS XE Firewall」モジュール
ゾーンベース ポリシー ファイアウォール	「Zone-Based Policy Firewall」モジュール

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 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*：ファイアウォール リソース管理の設定の機能情報

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 Release 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**。