ゾーンベース ポリシー ファイアウォールのネストされたクラス マップ サポート

ゾーンベース ポリシー ファイアウォールのネストされたクラス マップ サポート機能では、複数のトラフィック クラス（ネストされたクラス マップまたは階層型クラス マップとも呼ばれます）を単一のトラフィック クラスとして設定する機能を Cisco IOS XE ファイアウォールに提供します。 パケットが複数の一致条件を満たす場合、単一のトラフィック ポリシーに関連付けることができる複数のクラス マップを設定できます。 Cisco IOS XE ファイアウォールは、クラス マップ階層を 3 つのレベルまでサポートします。

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。

ゾーンベースポリシーファイアウォールのネストされたクラス マップ サポートの前提条件

ネストされたクラス マップを設定する前に、モジュラ Quality of Service（QoS）CLI（MQC）を十分に理解している必要があります。

ゾーンベースポリシーファイアウォールのネストされたクラス マップ サポートについて

ネストされたクラス マップ

Cisco IOS XE Release 3.5S 以降のリリースでは、複数のトラフィック クラス（ネストされたクラス マップまたは階層型クラスマップとも呼ばれます）を単一のトラフィック クラスとして設定できます。パケットが複数の一致条件を満たす場合、単一のトラフィック ポリシーに関連付けることができる複数のクラス マップを設定できます。 クラス マップのネストを **match class-map** コマンドにより実現できます。 1 つのトラフィック クラスで match-any 特性と match-all 特性を組み合わせる唯一の方法は、**class-map** コマンドを使用することです。

class-map コマンドの match-all キーワードと match-any キーワード

トラフィック クラスを作成するには、**class-map** コマンドを **match-all** キーワードと **match-any** キーワードを使用して設定する必要があります。 トラフィック クラスで複数の一致条件が設定されている場合にのみ、**match-all** キーワードと **match-any** キーワードを指定する必要があります。次のルールは、**match-all** キーワードおよび **match-any** キーワードに適用されます。

- 指定したトラフィック クラスにパケットを配置するために、トラフィック クラスのすべての一致条件が満たされる必要がある場合は、**match-all** キーワードを使用します。
- 指定したトラフィック クラスにパケットを配置するために、トラフィック クラスの一致条件の 1 つだけが満たされる必要がある場合は、**match-any** キーワードを使用します。
- **match-all** キーワードまたは **match-any** キーワードを指定しない場合、トラフィック クラスは **match-all** キーワードと一致する方法で動作します。

ゾーンベース ポリシー ファイアウォール コンフィギュレーションでは、次の条件が満たされた場合にネストされたクラス マップをサポートします。

- 階層の個々のクラス マップには複数の **match class-map** コマンド リファレンスが含まれます。
- 階層の個々のクラスマップには、**match class-map** コマンド以外の一致ルールが含まれます。

ゾーンベースポリシーファイアウォールのネストされたクラス マップ サポートの設定方法

ネストされた Two-Layer クラス マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **class-map match-any** *class-map-name*
7. **match protocol** *protocol-name*
8. **exit**
9. **class-map match-any** *class-map-name*
10. **match class-map** *class-map-name*
11. **match class-map** *class-map-name*
12. **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： `Router> 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： `Router# 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	**class-map match-any** *class-map-name* 例： `Router(config)# class-map match-any child1`	レイヤ 3 またはレイヤ 4 のクラス 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 protocol** *protocol-name* 例： `Router(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。
ステップ 5	**exit** 例： `Router(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 モードを開始します。
ステップ 6	**class-map match-any** *class-map-name* 例： `Router(config)# class-map match-any child2`	レイヤ 3 またはレイヤ 4 のクラス 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 7	**match protocol** *protocol-name* 例： `Router(config-cmap)# match protocol udp`	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。
ステップ 8	**exit** 例： `Router(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 モードを開始します。
ステップ 9	**class-map match-any** *class-map-name* 例： `Router(config)# class-map match-any parent`	レイヤ 3 またはレイヤ 4 のクラス 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 10	**match class-map** *class-map-name* 例： `Router(config-cmap)# match class-map child1`	トラフィック クラスを分類ポリシーとして設定します。
ステップ 11	**match class-map** *class-map-name* 例： `Router(config-cmap)# match class-map child2`	トラフィック クラスを分類ポリシーとして設定します。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： `Router(config-cmap)# end`	クラス マップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ネストされたクラス マップのポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *policy-map-name*
4. **class-type inspect** *class-map-name*
5. **inspect**
6. **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： `Router> 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： `Router# 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	**policy-map type inspect** *policy-map-name* 例： `Router(config)# policy-map type inspect pmap`	レイヤ 3 またはレイヤ 4 の検査タイプ 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 4	**class-type inspect** *class-map-name* 例： `Router(config-pmap)# class-type inspect parent`	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。

	コマンドまたはアクション	目的
ステップ 5	**inspect** 例： `Router(config-pmap-c)# inspect`	Cisco IOS XE 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 6	**end** 例： `Router(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 モードを開始します。

ゾーン ペアへのポリシー マップの付加

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *zone-name*
4. **exit**
5. **zone security** *zone-name*
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** *zone-name* **destination** [*zone-name*]]
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **zone-member security** *zone-name*
12. **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： `Router> 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： `Router# 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** *zone-name* 例： `Router(config)# zone security source-zone`	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。
ステップ 4	**exit** 例： `Router(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 モードを開始します。
ステップ 5	**zone security** *zone-name* 例： `Router(config)# zone security destination-zone`	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。
ステップ 6	**exit** 例： `Router(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 モードを開始します。
ステップ 7	**zone-pair security** *zone-pair-name* [**source** *zone-name* **destination** [*zone-name*]] 例： `Router(config)# zone-pair security secure-zone source source-zone destination destination-zone`	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。 • 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 8	**service-policy type inspect** *policy-map-name* 例： `Router(config-sec-zone-pair)# service-policy type inspect pmap`	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） 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： `Router(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 モードを開始します。
ステップ 10	**interface** *type number* 例： `Router(config)# interface gigabitethernet 0/0/1`	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： `Router(config-if)# zone-member security source-zone`	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、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（ルータ宛のトラフィックまたはルータ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 12	**end** 例： `Router(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 モードを開始します。

ゾーンベースポリシーファイアウォールのネストされたクラス マップ サポートの設定例

例：ネストされた Two-Layer クラス マップの設定

```
Router# configure terminal
Router(config)# class-map match-any child1
Router(config-cmap)# match protocol tcp
Router(config-cmap)# exit
Router(config)# class-map match-any child2
Router(config-cmap)# match protocol udp
Router(config-cmap)# exit
Router(config)# class-map match-any parent
Router(config-cmap)# match class-map child1
Router(config-cmap)# match class-map child2
Router(config-cmap)# end
```

例：ネストされたクラス マップのポリシー マップの設定

```
Router# configure terminal
Router(config)# policy-map type inspect pmap
Router(config-pmap)# class-type inspect parent
Router(config-pmap-c)# inspect
```

```
Router(config-pmap-c)# end
```

例：ゾーン ペアへのポリシー マップの付加

```
Router# configure terminal
Router(config)# zone security source-zone
Router(config-sec-zone)# exit
Router(config)# zone security destination-zone
Router(config-sec-zone)# exit
Router(config)# zone-pair security secure-zone source source-zone destination destination-zone
Router(config-sec-zone-pair)# service-policy type inspect pmap
Router(config-sec-zone-pair)# exit
Router(config)# interface gigabitethernet 0/0/1
Router(config-if)# zone-member security source-zone
Router(config-if)# end
```

ゾーンベースポリシーファイアウォールのネストされたクラス マップ 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』
セキュリティ 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』
ゾーンベース ポリシー ファイアウォール	『*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

ゾーンベースポリシーファイアウォールのネストされたクラス マップ 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*：ゾーンベース ポリシー ファイアウォールのネストされたクラス マップ サポートの機能情報

機能名	リリース	機能情報
ゾーンベース ポリシー ファイアウォールのネストされたクラス マップ サポート	Cisco IOS XE Release 3.5S	ゾーンベース ポリシー ファイアウォールのネストされたクラス マップ サポート機能では、複数のトラフィック クラス（ネストされたクラス マップまたは階層型クラス マップとも呼ばれます）を単一のトラフィック クラスとして設定する機能を Cisco IOS XE ファイアウォールに提供します。 パケットが複数の一致条件を満たす場合、単一のトラフィック ポリシーに関連付けることができる複数のクラス マップを設定できます。