ゾーンベース ポリシー ファイアウォールに対する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 ファイアウォールに対するネストされたクラス マップ サポート機能は、Cisco IOS XE ファイアウォールに単一のトラフィック クラスとして複数のトラフィック クラスを設定する機能（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る）を提供します。パケットが複数の一致基準を満たしている場合は、単一のトラフィック ポリシーに関連付けることが可能な複数のクラス マップを設定できます。Cisco IOS XE ファイアウォールは、最大 3 レベルのクラス マップ階層をサポートします。

ゾーンベース ポリシー ファイアウォールに対するネストされたクラス マップ サポートに関する前提条件

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）に精通しておく必要があります。

ゾーンベース ポリシー ファイアウォールに対するネストされたクラス マップ サポートに関する情報

ネストされたクラス マップ

Cisco IOS XE リリース 3.5S 以降のリリースでは、複数のトラフィック クラスを単一のトラフィック クラスとして設定できます（これらのトラフィック クラスは、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）。パケットが複数の一致基準を満たしている場合は、単一のトラフィック ポリシーに関連付けることが可能な複数のクラス マップを設定できます。クラスマップをネストするには、**match class-map** コマンドを設定します。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、**match-all** および **match-any** キーワードを指定した **class-map** コマンドを設定する必要があります。**match-all** キーワードと **match-any** キーワードの指定が必要になるのは、トラフィッククラスで複数の一致基準を設定する場合だけです。**match-all** および **match-any** キーワードには次のルールが適用されます。

- 指定したトラフィッククラスにパケットを分類するために、そのパケットがトラフィック クラス内のすべての一致基準に一致する必要がある場合、**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分類するために、そのパケットがトラフィック クラス内のいずれかの一致基準にのみ一致する必要がある場合、**match-any** キーワードを使用します。
- **match-all** キーワードと **match-any** キーワードのどちらも指定しないと、トラフィッククラスは **match-all** キーワードを指定した場合と同じように動作します。

ゾーンベース ポリシー ファイアウォールの設定は、次の条件が満たされる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で複数の **match class-map** コマンドが参照されている場合。
- 階層の個々のクラスマップに **match class-map** コマンド以外の一致ルールが含まれている場合。

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

2 レイヤ ネスト 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： `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	**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。

	コマンドまたはアクション	目的
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。
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 マップ用のポリシー 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： `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。
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 マップのアタッチ

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： `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	**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 モードを終了して、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 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。
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 ファイアウォールに対するネストされたクラス マップ サポートの設定例

例：2 レイヤ ネストされたクラス 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 マップのアタッチ

```
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 ファイアウォールに対するネストされたクラス マップ サポートに関する追加情報

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』
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
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

ゾーンベース ポリシー ファイアウォールに対するネストされたクラス マップ サポートに関する機能情報

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:* ゾーンベース ポリシー ファイアウォールに対するネストされたクラス マップ サポートに関する機能情報

機能名	リリース	機能情報
ゾーンベース ポリシー ファイアウォールに対するネストされたクラス マップ サポート	Cisco IOS XE リリース 3.5S	ゾーンベース ポリシー ファイアウォールに対するネストされたクラス マップ サポート機能は、Cisco IOS XE ファイアウォールに単一のトラフィック クラスとして複数のトラフィック クラスを設定する機能（ネストされたクラス マップまたは階層型クラス マップとも呼ばれる）を提供します。パケットが複数の一致基準を満たしている場合は、単一のトラフィック ポリシーに関連付けることが可能な複数のクラス マップを設定できます。

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。