ゾーンのポリシーの管理

Detector モジュールでは、ラーニング プロセスを使用してゾーン トラフィックの特性に合ったポリシーを作成することに加えて、ゾーンの設定のポリシーを変更できます。この章では、ゾーンの設定の異常検出機能を手動で微調整する方法について説明します。

この章は、次の項で構成されています。

ゾーンのポリシーの表示

ゾーンの設定のポリシーを表示するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Configuration > Policy** を選択します。Policies 画面が表示されます（図 8-1 および表 8-1 を参照）。

ステップ 3　GUARD_ ゾーン テンプレートを使用してゾーンを作成した場合は、ポリシーのリストの上に **View Detector/View Guard** トグル ボタンが表示されます。使用するポリシー ビューを選択します。

- Detector モジュールが使用するポリシーを表示するには、**View Detector** をクリックします。
- Cisco Anomaly Guard Module が使用するポリシーを表示するには、**View Guard** をクリックします。

ステップ 4　（オプション）画面フィルタを設定するには、Policies 画面の **Set screen filter** をクリックします。Policy Filter ウィンドウが表示されます。

ステップ 5　使用する画面フィルタを設定します。表 8-1 に、Policy Filter ウィンドウに表示される画面フィルタ パラメータの説明を示します。目的の表示パラメータを、対応するドロップダウン リストから選択します。複数のフィルタ パラメータを変更するときは、Policy Filter ウィンドウの一番上のパラメータから開始して、下方向に順に変更していきます。フィルタ パラメータを 1 つ変更すると、そのパラメータの下にあるすべてのパラメータが、デフォルト設定に自動的にリセットされます。

表 8-1　ポリシーのフィルタ パラメータ

パラメータ	表示する項目
Policy template	選択したポリシー テンプレートに基づいて作成されたポリシー。
Service	選択したサービスのために作成されたポリシー。
Protection level	選択した保護レベルを持つポリシー。
Type	選択したパケット タイプを持つポリシー。
Policy	選択した名前を持つポリシー。
State	選択した動作状態になっているポリシー。
Action	選択したアクションを使用して設定されているポリシー。
Policies	動作中の現在の設定のポリシー、またはスナップショット（使用可能な場合）のポリシー。

図 8-1 に、Policy 画面の例を示します。

図 8-1　ポリシー テーブル

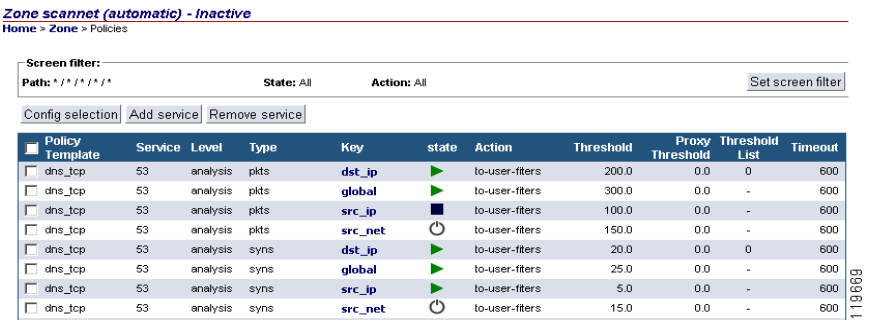

表 8-2 に、ポリシー テーブルに含まれているフィールドの説明を示します。

表 8-2　ポリシー テーブルに含まれているフィールドの説明

フィールド	説明
Policy Template	ポリシーの構築に Detector モジュールが使用したポリシー テンプレート。
Service	トラフィック フローに含まれていて、ポリシーが監視しているサービス。サービスは、アプリケーション ポートまたはプロトコルのいずれかです。サービスを追加すると、ラーニング プロセス中に Detector モジュールがゾーンに対して作成したポリシーの設定をさらに適切なものに調整できます。P.8-19 の「サービスの追加または削除」を参照してください。 Detector モジュールは、同じポリシー テンプレートから作成された他のサービスと特に一致しないすべてのトラフィックに対して **any** というサービス値を表示します。
Level	ポリシーがトラフィック フローに適用する異常検出のレベル。Detector モジュールでは常に **analysis** です。

表 8-2　ポリシー テーブルに含まれているフィールドの説明（続き）

フィールド	説明
Type	トラフィック フローの、パケットまたは接続のタイプ。 パケット タイプの値は、次のいずれかです。 • **auth_pkts**：TCP ハンドシェイクまたは UDP 認証を受けたパケット。 • **auth_tcp_pkts**：TCP　ハンドシェイクを受けたパケット。 • **auth_udp_pkts**：UDP 認証を受けたパケット。 • **in_nodata_conns**：接続でデータ転送が発生していない、ゾーンへの着信接続（データ ペイロードを含んでいないパケット）。 • **in_conns**：ゾーンへの着信接続。 • **in_pkts**：ゾーンに着信する DNS クエリー パケット。 • **in_unauth_pkts**：ゾーンに着信する未認証の DNS クエリー。 • **out_pkts**：ゾーンに着信する DNS 応答パケット。 • **reqs**：データ ペイロードを含んだ要求パケット。 • **syns**：同期パケット。つまり、TCP SYN フラグの付いたパケット。 • **syn_by_fin**：SYN フラグ付きパケットと FIN フラグ付きパケット。SYN フラグの付いたパケット数と FIN フラグの付いたパケット数の比率を確認します。 • **unauth_pkts**：TCP　ハンドシェイクを受けていないパケット。 • **pkts**：同じ検出レベルになっている他のいずれのカテゴリにも該当しない、すべてのパケット タイプ。 • **non_estb_conns**：確立されていない接続。失敗したゾーン着信接続。要求に対する応答がなかった TCP 接続要求（SYN パケット）。

表 8-2　ポリシー テーブルに含まれているフィールドの説明（続き）

フィールド	説明
Key	ポリシーの集約に使用されたトラフィック特性。キー名をダブルクリックすると詳細が表示されます。 キー名の値は、次のいずれかです。 • **dst_ip**：ゾーンの IP アドレスが宛先となっているトラフィック。 • **dst_ip_ratio**：特定の IP アドレスが宛先となっている SYN フラグ付きパケットと FIN フラグ付きパケットの比率。 • **dst_port_ratio**：特定のポートが宛先となっている SYN フラグ付きパケットと FIN フラグ付きパケットの比率。 • **global**：他のポリシー セクションによって定義された、すべてのトラフィック フローの合計。 • **src_ip**：送信元 IP アドレスに基づいて集計された、ゾーンが宛先となっているトラフィック。 • **dst_port**：ゾーンの特定のポートが宛先となっているトラフィック。 • **protocol**：プロトコルに基づいて集計された、ゾーンが宛先となっているトラフィック。 • **src_ip_many_dst_ips**：IP スキャニングに使用されるキー。単一の IP からゾーンの多数の IP アドレスに送信されるトラフィックです。 • **src_ip_many_ports**：ポート スキャニングに使用されるキー。単一の IP からゾーンの多数のポートに送信されるトラフィックです。 • **scanners**：特定の宛先ポート上でゾーンの宛先 IP アドレスをスキャンする送信元 IP アドレスのヒストグラム。

表 8-2　ポリシー テーブルに含まれているフィールドの説明（続き）

フィールド	説明
State	ポリシーの動作状態。ポリシーは、次のいずれかの状態で動作します。 ▶ アクティブ：Detector モジュールは、トラフィック フローにポリシーを適用します。トラフィック フローがポリシーのしきい値を超過すると、ポリシーがアクションを実行します。 ■ 非アクティブ：Detector モジュールは、トラフィック フローにポリシーを適用します。トラフィック フローがポリシーのしきい値を超過しても、ポリシーはアクションを実行しません。 ⏻ ディセーブル：Detector モジュールは、トラフィック フローにポリシーを適用しません。
Action	ポリシーに割り当てられているアクション。トラフィック フローがポリシーのしきい値を超過すると、ポリシーがこのアクションを実行します。詳細については、「ポリシーのパラメータの変更」の項を参照してください。
Threshold	ポリシーのしきい値となるトラフィック レート。トラフィック フローがポリシーのこのしきい値を超過すると、ポリシーは割り当てられているアクションを実行します。ポリシーのしきい値は、ユーザが手動で設定することも、ラーニング プロセスのしきい値調整フェーズで Detector モジュールが設定するように指定することもできます。
Timeout	割り当てられているアクションをポリシーがトラフィック フローに適用する最短期間。タイムアウト値は **never** に設定することができます。

表 8-2　ポリシー テーブルに含まれているフィールドの説明（続き）

フィールド	説明
Fixed	ポリシーのしきい値の動作ステータス。チェック マークは、このしきい値が固定値であり、ラーニング プロセスのしきい値調整フェーズ実行中に変更できないことを示します。**x** は、しきい値が固定でないことを示します。つまり、Detector モジュールがしきい値調整プロセスの実行中にポリシーのしきい値を変更できることを意味します。
Learning Multiplier	Detector モジュールがしきい値調整フェーズの結果を受け入れるときにしきい値に掛ける係数。

ポリシーのパラメータの変更

この項の手順では、ポリシーのパラメータを変更する方法について説明します。ゾーンのポリシーは、Detector モジュールでゾーンのトラフィックについてラーニングや異常の分析を実行していない場合にのみ変更できます。WBM では、ポリシーのパラメータを変更する手順が 2 つ用意されています。1 つは単一のポリシーを変更する手順で、もう 1 つは、複数のポリシーに同じパラメータ変更を同時に適用する手順です。表 8-3 に、それぞれの手順で変更できるポリシー パラメータのリストを示します。

表 8-3　ポリシーの変更手順

	手順	
ポリシーのパラメータ	単一のポリシーの変更	複数のポリシーの同時変更
(Operating) State	X	X
Action	X	X
Threshold	X	
Threshold multiplier		X
Timeout	X	X
Learning parameters: • Set as fixed • Learning multiplier	X	X

（注）　ポリシーのパラメータに加えた変更内容は、パラメータの変更後にポリシー構築フェーズを実行すると失われます。ユーザがポリシー構築フェーズの結果を受け入れると、Detector モジュールはゾーン設定の現在のポリシーを削除して、新しいポリシーに置き換えます。

注意　ポリシーの状態を**非アクティブ**または**ディセーブル**に設定すると、ゾーンのトラフィック異常を検出する Detector モジュールの機能に支障をきたす恐れがあります。ポリシーをディセーブルにすると、ディセーブルにしたポリシーが管理していたトラフィックは、イネーブルになっているポリシーが管理するようになります。ポリシーをディセーブルにした後にゾーンの異常検出をアクティブにする場合は、しきい値調整フェーズを事前に実行して、イネーブルになっているポリシーのしきい値をアップデートする必要があります。

この項では、次の手順について説明します。

- 単一のポリシーの変更
- 複数のポリシーの同時変更

単一のポリシーの変更

単一のポリシーのパラメータを変更するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Configuration > Policy** を選択します。Policies 画面が表示されます。

ステップ 3　GUARD ゾーン テンプレートを使用してゾーンを作成した場合は、ポリシーのリストの上に **View Detector/View Guard** トグル ボタンが表示されます。使用するポリシー ビューを選択します。

- Detector モジュールが使用するポリシーを変更するには、**View Detector** をクリックします。
- Cisco Anomaly Guard Module が使用するポリシーを変更するには、**View Guard** をクリックします。

ステップ 4　目的のポリシーのキーをクリックします。Policy details 画面が表示されます。

ステップ 5　Learning parameters テーブルの下にある **Configure** をクリックします。Config Policy 画面が表示され、パラメータの現在の値が示されます。

ステップ 6　目的のポリシー パラメータを設定し直します。表 8-4 に、Zone Policies Parameter Form の設定済みポリシー パラメータの説明を示します。

表 8-4　Zone Policies Parameter Form

パラメータ	説明
State	ポリシーの状態。指定可能な値は、次のいずれかです。 • **active**：Detector モジュールは、ポリシーをトラフィックに適用します。トラフィックがポリシーのしきい値を超過すると、ポリシーは割り当てられているアクションを実行します。 • **inactive**：Detector モジュールは、ポリシーをトラフィックに適用します。ただし、トラフィックがポリシーのしきい値を超過しても、ポリシーは割り当てられているアクションを実行しません。 • **disabled**：Detector モジュールは、ポリシーをトラフィックに適用しません。
Action	トラフィックがポリシーのしきい値を超過したときに、ポリシーが実行するアクション。ポリシーのアクションをドロップダウン リストから選択します。 • **notify**：ポリシーは、ユーザに対して通知します。 • **remote_activation**：ポリシーは Cisco Anomaly Guard Module をアクティブにします。Cisco Anomaly Guard Module は、ゾーンのトラフィックを自身に宛先変更し、ゾーンの保護プロセスを管理します。システム管理者は、Detector モジュールがアクティブにする Cisco Anomaly Guard Module を CLI を使用して定義し、リモート Guard リストを設定します。

表 8-4　Zone Policies Parameter Form（続き）

パラメータ	説明
Threshold	ポリシーのしきい値となるトラフィック レート。トラフィックがこのしきい値を超過すると、ポリシーはゾーンを保護するためのアクションを実行します。しきい値は、次のポリシーを除いてパケット / 秒（pps）単位で測定されます。 • **tcp_connections**：接続数で測定されます。 • **tcp_ratio**：比率で測定されます。
Timeout	ポリシーがアクションを適用する最短期間。タイムアウト値を秒単位で入力します。
Learning parameters	ポリシーに関連するしきい値調整フェーズの結果を Detector モジュールが受け入れる方法。しきい値調整フェーズの結果を Detector モジュールが変更なしで受け入れるようにするには、Learning parameters チェックボックスをオフのままにします。 Learning parameters チェックボックスをオンにして、次のいずれかのオプションを選択します。 • **Set as fixed** : Detector モジュールは、ポリシーの現在のしきい値を固定値として定義します。Detector モジュールは、しきい値調整フェーズの結果を受け入れるとき、このポリシーのしきい値を変更しません。 • **Learning multiplier**: Detector モジュールは、ここにユーザが入力する値をポリシーの現在のしきい値に掛けます。Detector モジュールは、この乗数を将来のしきい値調整フェーズの結果にも適用します。ポリシーのしきい値を増減するための係数を入力します。

複数のポリシーの同時変更

複数のゾーンのポリシーに同じパラメータ変更を適用するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Configuration > Policy** を選択します。Policies 画面が表示されます。

ステップ 3　GUARD ゾーン テンプレートを使用してゾーンを作成した場合は、ポリシーのリストの上に **View Detector**/**View Guard** トグル ボタンが表示されます。使用するポリシー ビューを選択します。

- Detector モジュールが使用するポリシーを変更するには、**View Detector** をクリックします。
- Cisco Anomaly Guard Module が使用するポリシーを変更するには、**View Guard** をクリックします。

ステップ 4　設定し直すポリシーの隣にあるチェックボックスをオンにして、**Config Selection** をクリックします。Zone Policies Parameter Form が表示されます。複数のポリシーを選択すると、値の異なるポリシー パラメータについて **multiple** の値が表示されます。

ステップ 5　目的のポリシー パラメータを変更します。表 8-5 に、Zone Policies Parameter Form に含まれている設定可能なポリシー パラメータの説明を示します。

表 8-5　Zone Policies Parameter Form

パラメータ	説明
State	ポリシーの動作状態。動作状態をドロップダウン リストから選択します。 • **active**：Detector モジュールは、ポリシーをトラフィックに適用します。トラフィック フローがいずれかのポリシーのしきい値を超過すると、そのポリシーは、割り当てられているアクションを実行します。 • **inactive**：Detector モジュールは、ポリシーをトラフィックに適用します。ただし、トラフィック フローがポリシーのしきい値を超過しても、ポリシーは割り当てられているアクションを実行しません。 • **disabled**：Detector モジュールは、ポリシーをトラフィックに適用しません。
Action	トラフィック フローがポリシーのしきい値を超過したときに、ポリシーが実行するアクション。ポリシーのアクションをドロップダウン リストから選択します。 • **notify**：トラフィックがポリシーのしきい値を超過すると、ポリシーはユーザに対して通知します。 • **remote_activation**：ポリシーは Cisco Anomaly Guard Module をアクティブにします。Cisco Anomaly Guard Module は、ゾーンのトラフィックを自身に宛先変更し、ゾーンの保護プロセスを管理します。システム管理者は、Detector モジュールがアクティブにする Cisco Anomaly Guard Module を CLI を使用して定義し、リモート Guard リストを設定します。
Threshold multiplier	ポリシーのしきい値を増減するための係数。ポリシーのしきい値がゾーンのトラフィックに対して適切でないときに、しきい値を増減する係数を入力します。

表 8-5　Zone Policies Parameter Form（続き）

パラメータ	説明
Timeout	ポリシーがアクションをトラフィック フローに適用する最短期間。タイムアウト値を秒単位で入力します。
Learning parameters	選択したポリシーに関連するしきい値調整フェーズの結果を Detector モジュールが受け入れる方法。しきい値調整フェーズの結果を Detector モジュールが変更なしで受け入れるようにするには、Learning parameters チェックボックスをオフのままにします。 Learning parameters チェックボックスをオンにして、次のいずれかのオプションを選択します。 • **Set as fixed** : Detector モジュールは、選択したポリシーの現在のしきい値を固定値として設定します。Detector モジュールは、しきい値調整フェーズの結果を受け入れるとき、これらのポリシーのしきい値を変更しません。 • **Learning multiplier**：Detector モジュールは、ここにユーザが入力する値をポリシーの現在のしきい値に掛けます。Detector モジュールは、この乗数を将来のしきい値調整フェーズの結果にも適用します。ポリシーのしきい値を増減するための係数を入力します。

ステップ 6　次のいずれかのオプションを選択します。

- **OK**：設定情報を保存します。Zone Policies Parameter Form が閉じて Policies 画面が表示され、変更のあったポリシーの設定がすべて示されます。
- **Clear**：Zone Policies Parameter Form の情報をデフォルト値に戻します。
- **Cancel**：ポリシーのパラメータを変更せずに Zone Policies Parameter Form を終了します。

IP アドレスとしきい値の追加または削除

トラフィック量が多い既知の送信元または宛先の IP アドレスでトラフィックが増加する場合、Detector モジュールによる誤った攻撃検出を回避するために、当該 IP アドレスに関連付けられているトラフィックのしきい値をポリシーに設定できます。次のネットワーク事情が当てはまる場合に、IP アドレスとしきい値をポリシーに追加します。

- 送信元 IP アドレスからのトラフィック量が多い：通常の状態で、ゾーンが特定の送信元 IP アドレスから大量のトラフィックを受信する場合、その送信元 IP アドレスから発信されるトラフィックに適用されるしきい値をポリシーに設定できます。
- 宛先 IP アドレスへのトラフィック量が多い：ゾーンに複数の IP アドレスを定義しており、通常の状態で、ゾーンの複数のセクションが大量のトラフィックを受信する場合は、そのゾーン内の宛先 IP アドレスをターゲットとするトラフィックに適用されるしきい値をポリシーに設定できます。

WBM で IP しきい値を設定できる対象は、次のような特性を持つポリシーのみです。

- Key のタイプが **src_ip**（送信元 IP アドレス）で、Action のタイプが **drop** のポリシー。
- Key のタイプが **dst_ip**（宛先 IP アドレス）で、Action のタイプが **to-user**、**strong**、**notify**、または **drop** のポリシー。

ポリシーごとに、IP アドレスとしきい値を 5 つまで設定できます。

ここでは、次の手順について説明します。

- IP アドレスとしきい値の追加
- IP アドレスとしきい値の削除

IP アドレスとしきい値の追加

IP アドレスとしきい値を使用してポリシーを設定するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Configuration > Policy** を選択します。Policies 画面が表示されます。

ステップ 3　GUARD ゾーン テンプレートを使用してゾーンを作成した場合は、ポリシーのリストの上に **View Detector/View Guard** トグル ボタンが表示されます。使用するポリシー ビューを選択します。

- Detector モジュールが使用するポリシーに IP アドレスとしきい値を設定するには、**View Detector** をクリックします。
- Cisco Anomaly Guard Module が使用するポリシーに IP アドレスとしきい値を設定するには、**View Guard** をクリックします。

ステップ 4　目的のポリシーの（Key カラムの下にある）Key タイプをクリックします。Policy details 画面が表示されます。

ステップ 5　Threshold list テーブルの下にある **Add** をクリックします。Add threshold entry 画面が表示されます。

ステップ 6　送信元または宛先の IP アドレスとしきい値を定義します。表 8-6 に、Threshold IP Entry Form のパラメータの説明を示します。

表 8-6　Threshold IP Entry Form

パラメータ	説明
IP	IP アドレス。送信元または宛先の IP アドレスを入力します。
Threshold	IP アドレスのしきい値。トラフィックがこのしきい値を超過すると、ポリシーは設定されているアクションを実行します。しきい値は、次のタイプのポリシーを除いてパケット / 秒（pps）単位で入力します。 • **tcp_connections**：測定の単位は接続数です。 • **tcp_ratio**：測定の単位は比率です。

ステップ 7　次のいずれかのオプションを選択します。

- **OK**：ポリシーの設定とゾーンの設定に、ポリシーの IP アドレス情報を保存します。Threshold IP Entry Form が閉じて Policy details 画面が表示され、変更のあったポリシーの設定がすべて示されます。
- **Clear**：Threshold IP Entry Form に追加した情報をすべて消去します。
- **Cancel**：ポリシーの設定を変更せずに Threshold IP Entry Form を終了します。

IP アドレスとしきい値の削除

ポリシーの IP アドレスとしきい値を削除するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Configuration > Policy** を選択します。Policies 画面が表示されます。

ステップ 3　GUARD ゾーン テンプレートを使用してゾーンを作成した場合は、ポリシーのリストの上に **View Detector**/**View Guard** トグル ボタンが表示されます。使用するポリシー ビューを選択します。

- Detector モジュールが使用するポリシーから IP アドレスとしきい値を削除するには、**View Detector** をクリックします。
- Cisco Anomaly Guard Module が使用するポリシーから IP アドレスとしきい値を削除するには、**View Guard** をクリックします。

ステップ 4　目的のポリシーの Key パラメータをクリックします。Policy details 画面が表示されます。

ステップ 5　Threshold list テーブルから削除する IP リストのチェックボックスをオンにします。

ステップ 6　Threshold list テーブルの下にある **Delete** をクリックします。変更されたポリシーの設定情報が、ポリシーの設定とゾーンの設定に保存されます。

サービスの追加または削除

Detector モジュールがポリシー構築フェーズで検出しなかったサービスをゾーンの設定に手動で追加できます。サービスを追加すると、Detector モジュールは、そのサービスに対してユーザが選択するポリシー テンプレートに基づいて、サービスの新しいポリシーを作成します。次のポリシー テンプレートに新しいサービスを追加できます。

- http
- other protocols
- tcp_services
- udp_services

http、tcp_services、および udp_services については、追加するサービスをポート番号で指定します。other_protocols については、追加するサービスをプロトコル番号で指定します。

GUARD_ ゾーン テンプレートを使用して作成したゾーンの設定に対してサービスを追加または削除する場合、Detector モジュールは、Detector モジュールと Cisco Anomaly Guard Module のポリシーの設定にサービスの変更を加えます。

ゾーンの設定に対してサービスを追加または削除すると、Detector モジュールは、そのゾーンを未調整としてマークします。ゾーンが未調整であるため、Detect and Learn をアクティブにしても、ユーザが次のいずれかのアクションを実行するまで Detector モジュールはゾーンの異常を検出できません。

- ラーニング　プロセスのしきい値調整フェーズを実行して、その結果を受け入れる（第 7 章「ゾーンのトラフィックのラーニング」の「しきい値調整フェーズの開始」の項を参照）。
- ゾーンを調整済みとしてマークする（第 7 章「ゾーンのトラフィックのラーニング」の「ゾーンのポリシーに対する調整済みまたは未調整のマーク付け」の項を参照）。

この項では、次の手順について説明します。

- サービスの追加
- サービスの削除

サービスの追加

サービスをポリシーのタイプに追加するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　次のいずれかの方法で、Add Service プロセスを開始します。

- ゾーンのメイン メニューの **Configuration > Add Service** を選択します。
- ゾーンのメイン メニューの **Configuration > Policy** を選択し、Policies 画面の **Add service** をクリックします。GUARD ゾーン テンプレートを使用してゾーンを作成した場合は、現在 Detector モジュールと Cisco Anomaly Guard Module のどちらのポリシー設定が表示されているかに関係なく、Detector モジュールは両方のポリシー設定にサービスの変更を加えます。
- ゾーンのメイン メニューの **Configuration > Policy templates** を選択し、Policies Templates 画面の **Add service** をクリックします。

  Add service step 1 画面が表示されます。

ステップ 3　Policy Template リストからポリシー テンプレートを選択し、**Next** をクリックします（ポリシー テンプレートのタイプの詳細については、第 6 章「ポリシー テンプレートの設定」の「ポリシー テンプレートのタイプ」の項を参照）。Add service step 2 画面の Add Service Form が表示されます。

ステップ 4　新しいサービスを Add Service Form に入力します。

ステップ 5　次のいずれかのオプションを選択します。

- **OK**：サービスのための新しいポリシーをゾーンの設定に追加します。Policies 画面が表示されます。追加されたサービスのポリシーが表示され、Detector モジュールはゾーンを未調整としてマークします。
- **Clear**：Add Service Form の情報を消去します。

- **Cancel**：新しいサービスをゾーンの設定に追加せずに Add Service Form を終了します。

ステップ 6　（オプション）サービスを追加した後にゾーンの設定を未調整から調整済みに変更するには、次のいずれかの操作を実行します。

- ラーニング　プロセスのしきい値調整フェーズを実行して、フェーズの結果を受け入れる（第 7 章「ゾーンのトラフィックのラーニング」の「しきい値調整フェーズの開始」の項を参照）。
- ゾーンを調整済みとしてマークする（第 7 章「ゾーンのトラフィックのラーニング」の「ゾーンのポリシーに対する調整済みまたは未調整のマーク付け」の項を参照）。

新しいサービスのポリシーは、デフォルトのしきい値を使用して設定されます。各ポリシーのしきい値を手動で定義することもできますが、しきい値調整フェーズを実行して、ポリシーをゾーンのトラフィックに合せて調整することをお勧めします（第 7 章「ゾーンのトラフィックのラーニング」の「しきい値調整フェーズの開始」の項を参照）。

サービスの削除

ポリシーのタイプに関連する特定のサービスを削除できます。Detector モジュールは、ユーザが選択するポリシー テンプレートから作成されたすべてのポリシーを削除します。

注意　サービスを削除すると、削除されたトラフィック サービスに Detector モジュールのポリシーが関連付けられなくなるため、ゾーンの保護に支障をきたす恐れがあります。

サービスをポリシーから削除するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　次のいずれかの方法で、Remove Service プロセスを開始します。

- ゾーンのメイン メニューの **Configuration > Add Service** を選択します。
- ゾーンのメイン メニューの **Configuration > Policy** を選択し、Policies 画面の **Remove service** をクリックします。GUARD_ ゾーン テンプレートを使用してゾーンを作成した場合は、現在 Detector モジュールと Cisco Anomaly Guard Module のどちらのポリシー設定が表示されているかに関係なく、Detector モジュールは両方のポリシー設定にサービスの変更を加えます。
- ゾーンのメイン メニューの **Configuration > Policy templates** を選択し、Policies Templates 画面の **Remove service** をクリックします。

  Remove service 画面が表示されます。

ステップ 3　リストから削除するサービスを選択し、**Delete** をクリックします。削除の確認画面が表示されます。

ステップ 4　次のいずれかのオプションを選択します。

- **OK**：選択したサービスをゾーンの設定から削除します。Policies 画面が表示され、Detector モジュールはゾーンを未調整としてマークします。
- **Cancel**：選択したサービスをゾーンの設定から削除せずに Remove Service Form を終了します。

ステップ 5　（オプション）サービスを削除した後にゾーンの設定を未調整から調整済みに変更するには、次のいずれかの操作を実行します。

- ラーニング プロセスのしきい値調整フェーズを実行して、フェーズの結果を受け入れる（第 7 章「ゾーンのトラフィックのラーニング」の「しきい値調整フェーズの開始」の項を参照）。
- ゾーンを調整済みとしてマークする（第 7 章「ゾーンのトラフィックのラーニング」の「ゾーンのポリシーに対する調整済みまたは未調整のマーク付け」の項を参照）。