CHAPTER 8

ゾーンのポリシーの管理

Detector モジュールでは、ゾーンの設定のポリシーを変更することができます。この章では、ゾーンの設定の保護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
- ポリシーのパラメータの変更
- IP アドレスとしきい値の設定
- サービスの追加または削除
- ゾーンのポリシーのバックアップ

ゾーンのポリシーの表示

ゾーン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 > Policies > View** を選択します。Policies 画面が表示されます。

ステップ 3　（オプション）表示したいポリシー、または設定するポリシーだけが表示されるように、画面フィルタを設定します。画面フィルタを設定するには、次の手順を実行します。

a. **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。

b. 使用する画面フィルタを設定し、**OK** をクリックします。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には、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。

（注）　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	選択したキーを持つポリシー。
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	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。

指定した基準を満たす、ポリシーのリストの一部が表示されます。選択したパス、状態、およびアクションの詳細が Screen Filter フレームに表示されます。

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	Detector モジュールがポリシーの構築に使用したポリシー テンプレート。各ポリシー テンプレートは、Detector モジュールが特定の DDoS 攻撃の検出で必要とする特性を処理します。
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、ポート番号またはプロトコル番号のいずれかです。P.8-17 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。
Type	Detector モジュールが監視するパケット 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 認証のいずれかが実行されたパケット。 • **auth_tcp_pkts**：TCP ハンドシェイクが実行されたパケット。 • **auth_udp_pkts**：UDP 認証が実行されたパケット。 • **in_nodata_conns**：ゾーンへの着信接続のうち、接続時にデータ転送が行われない（データ ペイロードのないパケット）もの。 • **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。

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 （続き）	• **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）。 • **num_sources** : Detector モジュールのスプーフィング防止機能で認証された、ゾーンが宛先となっている TCP 送信元 IP アドレスのパケット。 • **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（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。Detector モジュールは、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** : 同じ保護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。

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**：同一のポートで多数のゾーン IP アドレスをプローブする 1 つの IP アドレスからのトラフィック。このキーは IP スキャニングに使用されます。 • **src_ip_many_ports**：ゾーンの宛先 IP アドレスで多数のポートをプローブする 1 つの IP アドレスからのトラフィック。このキーはポート スキャニングに使用されます。 • **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。 デフォルトでは、しきい値はオンデマンドの保護に適した値に設定されています。
Timeout	ポリシーがトラフィック フローにその割り当てられたアクションを適用するまでの最短時間。

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、このしきい値が固定値ではないことを示し、Detector モジュールがしきい値調整プロセス中にポリシーのしきい値を変更する可能性があ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。ゾーンのポリシーを変更できるのは、Detector モジュールがゾーンのトラフィックをラーニングしていないとき、またはゾーンのトラフィックで異常を検出していないときのみです。1 つのポリシーのパラメータを変更することも、一度に複数のポリシーのパラメータを変更することもできます。

（注） ポリシーのパラメータを変更した後にポリシー構築フェーズを実行すると、パラメータに行った変更が失われることがあります。これは、ポリシー構築フェーズの結果を受け入れた場合に、Detector モジュールが現在のゾーン ポリシーを新しいポリシーで置き換えるためです。

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 > Policies > View** を選択します。Policies 画面が表示されます。

ステップ 3　次のいずれかの方法で、設定するポリシーを選択します。

- 1 つのポリシーを設定するには、設定対象のポリシーの Key をクリックします（Policy details 画面が表示されます）。次に、Learning parameters テーブルの下にある **Configure** をクリックします。Zone Policy Form が表示されます。
- 複数のポリシーを設定するには、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、**Config Selection** をクリックします。Zone Policy Parameter Form が表示されます。

  ポリシー セクションの **Multiple** という値は、選択したすべてのポリシーに、そのポリシーセクションと同じ値を持つポリシーがないことを指定します。

ステップ 4　ポリシー パラメータを設定し直して、OK をクリックします。

ポリシー パラメータのフィールドをブランクのままにしておくと、Detector モジュールは選択したポリシーのパラメータの値を変更しません。

表 8-3 に、Zone Policy Form および Zone Policy Parameter Form のポリシー パラメータの説明を示します。

表 8-3　Zone Policy Parameter Form および Zone Policy Form

パラメータ	説明
State	ポリシーの状態。使用可能な値は、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。 ⚠ **注意**　ポリシーの状態を **inactive** または **disabled** に設定すると、ゾーンの保護に支障をきたす恐れがあります。ポリシーの状態を **disabled** に設定すると、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ゾーン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 Detector モジュールでゾーン保護を実行する場合は、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。

表 8-3　Zone Policy Parameter Form および Zone Policy Form（続き）

パラメータ	説明
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**：ポリシーからユーザに通知します。 • **remote_activation**：ポリシーによって Cisco Anomaly Guard Module がアクティブになります。ゾーンのトラフィックはポリシー自身に宛先変更され、ゾーンの保護プロセスを管理します。Detector モジュールがアクティブにする Cisco Anomaly Guard Module を定義するには、CLI を使用してリモート Guard リストを設定します。
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、ポリシーはアクションを実行してゾーンを保護します。 このしきい値は、単一のポリシーに対してだけ設定できます。 しきい値は、次のポリシー テンプレートから構築されたポリシーを除いて pps 単位で測定されます。 • num_soruces：しきい値は、IP アドレスまたはポートの数で測定されます。 • tcp_connections：しきい値は、接続の数で測定されます。 • tcp_ratio：しきい値は、比率値で測定されます。

表 8-3　Zone Policy Parameter Form および Zone Policy Form（続き）

パラメータ	説明
Threshold multiplier	ポリシーのしきい値を増減するための係数。 しきい値係数は、グループ化されたポリシーに対してだけ設定できます。 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。 **（注）** 新しい値を固定値として設定しない場合、その値は後続のしきい値調整フェーズで変更されることがあります。
Timeout	ポリシーがアクションを適用するために作成する動的フィルタの最短時間。タイムアウト値を秒単位で入力します。
Learning parameters	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、ポリシーのしきい値を変更する方法。 ラーニング パラメータを設定するには、Learning parameters チェックボックスをオンにします。次のラーニング パラメータが設定できます。 • **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、後続のしきい値調整フェーズの結果を受け入れる前に、ラーニングしたしきい値に、指定された係数を乗算して新しいポリシーのしきい値を計算します。Detector モジュールは、設定したしきい値の選択方法を使用して、しきい値調整フェーズの結果を受け入れます。ポリシーのしきい値を掛ける正の実数（浮動小数点数 2 桁）を入力します。1 未満の数字を入力するとポリシーのしきい値が減少します。

IP アドレスとしきい値の設定

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。

IP しきい値は、次のようなポリシーに対してだけ設定できます。

- トラフィック特性が宛先 IP （dst_ip）のポリシー。
- トラフィック特性が送信元 IP アドレス（src_ip）で、デフォルトのポリシー アクションが drop のポリシー。デフォルトのポリシー アクションとは、新しいゾーンを作成したときに Detector モジュールがそのポリシーに割り当てるアクションです。このようなポリシーに対しては、ポリシーのアクションを変更しても、しきい値のリストを設定できます。

ポリシーごとに IP アドレスとしきい値を 10 種類まで設定できます。

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

ポリシーに IP アドレスとしきい値を追加するには、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　ゾーンのメイン メニューの **Configuration > Policies > View** を選択します。Policies 画面が表示されます。

ステップ 3　設定するポリシーの Key タイプ（Key カラムの下にある）をクリックします。Policy details 画面が表示されます。

ステップ 4　Threshold list テーブルの下にある **Add** をクリックします。Add Threshold IP Entry 画面が表示されます。

ステップ 5　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 8-4 に、Threshold IP Entry Form のパラメータの説明を示します。

表 8-4　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 6　次のいずれかのオプションを選択します。

- **OK**：ゾーン設定にポリシーの 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 > Policies > View** を選択します。Policies 画面が表示されます。

ステップ 3　ポリシーの Key パラメータをクリックして、ポリシーの IP アドレスとしきい値を削除します。Policy details 画面が表示されます。

ステップ 4　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 5　**Delete** をクリックします。変更されたポリシーの設定情報が Detector モジュールに保存されます。

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（アプリケーション ポートまたはプロトコル）をゾーン設定に手動で追加できます。異常検出が個々のニーズに対して最適になるように、ゾーンのメイン サービスに特定のポリシーを定義することをお勧めします。

注意　パフォーマンスが低下する場合があるため、複数のポリシーに同一サービス（ポート番号）を追加しないでください。

ゾーンのポリシー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のポリシー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 トラフィック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 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）。
- ゾーンのポリシーを調整済みとしてマークする（第 7 章「ゾーン 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

特定のポリシー テンプレートから作成されたすべてのポリシーにサービスを追加できます。新しいサービスはポリシー構築フェーズ中に検出されたサービスに追加され、デフォルト値で定義されます。しきい値は手動で定義できますが、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、ゾーン トラフィックに対してポリシーを調整することをお勧めします。

次のポリシー テンプレートから作成されたポリシーに、新しいサービスを追加できます。

- tcp_services、udp_services、tcp_services_ns、worm_tcp
  サービスをポート番号で指定します。
- other_protocols
  サービスをプロトコル番号で指定します。

（注） サービスを追加してポリシー構築フェーズをアクティブにすると、新しいサービスは手動で追加したサービスを上書きする場合があります。

ポリシー構築を再び実行しない場合、次の状況ではサービスを手動で追加する必要があります。

- 新しいアプリケーションまたはサービスがゾーン　ネットワークに追加された。
- ポリシー構築フェーズのアクティブな期間が短かったため、すべてのネットワーク サービスが反映されていない（たとえば、週 1 回または夜間のみアクティブとなる既知のアプリケーションまたはサービスがある場合）。

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　ゾーンのメイン メニューの **Configuration > PolicyTemplates > Add Service** を選択します。

次のいずれかのアクションを実行して Add Service 画面に移動することもできます。

- ゾーンのメイン メニューの **Configuration > Policies > View** を選択し、Policies 画面で **Add service** をクリックします。
- ゾーンのメイン メニューの **Configuration > Policy templates > View** を選択し、Policies Templates 画面で **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 リストでポリシー テンプレートを選択し、**Next** をクリックします。Add Service Step 2 フォームが表示されます。

ポリシー テンプレート 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 テンプレートの使用」の項を参照してください。

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。Detector モジュールはゾーン ポリシーを未調整としてマークします。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。
- **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）新しいポリシーのしきい値を定義します。しきい値は手動で定義できますが、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、ゾーン トラフィックに対してポリシーを調整することをお勧めします。詳細については、第 7 章「ゾーン 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」の項を参照してください。

ゾーン ポリシーは、ラーニング プロセスのしきい値調整フェーズを実行しなくても調整済みとしてマークできます。第 7 章「ゾーン 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」の項を参照してください。

サービスの削除

すべてのポリシー テンプレートから特定のサービスを削除できます。Detector モジュールは、特定のポリシー テンプレートから作成されたすべてのポリシーからサービスを削除します。

注意　サービスを削除すると、Detector　モジュールのポリシーはそのサービスのトラフィックを監視できなくなり、ゾーンの異常検出に支障をきたす恐れがあります。

次のポリシー テンプレートからサービスを削除できます。

- tcp_services、udp_services、tcp_services_ns、worm_tcp
  サービスをポート番号で指定します。
- other_protocols
  サービスをプロトコル番号で指定します。

ラーニング プロセスのポリシー構築フェーズをアクティブにしない場合、次の状況ではサービスを手動で削除する必要があります。

- アプリケーションまたはサービスがネットワークから削除された。
- イネーブルにはしないが（ネットワーク環境では一般的でないため）アプリケーションまたはサービスが、ポリシー構築フェーズ中に識別された。

（注）　サービスを削除してポリシー構築フェーズをアクティブにすると、同じサービスが再び追加される場合があります。

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　ゾーンのメイン メニューの **Configuration > Policy Templates > Remove service** を選択します。Remove Service 画面が表示されます。

次のいずれかのアクションを実行して Remove Service 画面に移動することもできます。

- ゾーンのメイン メニューの **Configuration > Policies > View** を選択し、Policies 画面で **Remove service** をクリックします。
- ゾーンのメイン メニューの **Configuration > Policy templates > View** を選択し、Policies Templates 画面で **Remove service** をクリックします。

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。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 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 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）。

ゾーンのポリシーのバックアップ

スナップショット機能を使用すると、現在のゾーン ポリシーをいつでもバックアップできます。

ゾーンのポリシーをバックアップするには、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、ラーニング フェーズに現在入っていない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 **Learning > Snapshot** を選択します。Create Snapshot 画面が表示されます。

ステップ 3　スナップショットの名前を Snapshot name フィールドに入力し、**OK** をクリックします。Detector モジュールが、ゾーンのポリシーを保存してスナップショットに連続 ID 番号を割り当てます。