ゾーンのポリシーの管理

Detector 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追加または削除
- サービスの追加または削除

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 > Policies > View** 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　（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。

表 8-1　ポリシーのフィルタ パラメータ（続き）

パラメータ	表示する項目
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。

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。

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

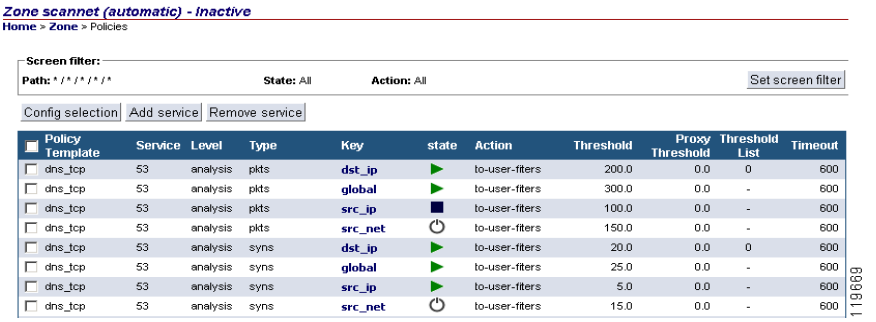

表 8-2 に、ポリシー テーブルに含まれているフィールドの説明を示します。

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	Detector 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 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.8-15 の「サービスの追加または削除」を参照してください。 Detector では、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のサービスの値に **any** が表示されます。
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 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	Detector 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。 • **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 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。 • **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 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 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 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、手動で設定するか、Detector によってラーニング プロセスのしきい値調整フェーズで設定することができます。
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。
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 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。

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
Learning Multiplier	Detector 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 がゾーンのトラフィックをラーニングしていないとき、またはゾーンを保護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 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、目的のポリシーの 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　目的のポリシー 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 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 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 8-3　Zone Policies Parameter Form

パラメータ	説明
State	ポリシーの状態。表示される値は、次のいずれかです。 • **active**：Detector はトラフィックにポリシーを適用します。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たアクションを実行します。 • **inactive**：Detector はトラフィックにポリシーを適用します。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たアクションを実行しません。 • **disabled**：Detector はトラフィックにポリシーを適用しません。 **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、ゾーンの保護に支障をきたす恐れがあります。ポリシーの状態を**ディセーブル**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 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 Policies Parameter 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**：しきい値を超過したときに通知します。 • **remote_activation**：Cisco Guard をアクティブにします。Cisco Guard はゾーンのトラフィックを自身に誘導し、ゾーンの保護プロセスを管理します。Detector がアクティブにする Cisco Guard 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。
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。

表 8-3　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	ポリシーに関係するしきい値調整フェーズの結果を Detector が受け入れる方法。Detector に、しきい値調整フェーズの結果を変更せずにそのまま受け入れさせるには、Learning Parameters チェックボックスをオフのままにしておきます。 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 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。しきい値調整フェーズの結果を受け入れるときに、Detector はこのポリシーのしきい値を変更しません。 • **Learning multiplier**：Detector は、ここに入力する値をポリシーの現在のしきい値に掛けます。また、Detector は、後続のしきい値調整フェーズの結果にも乗数を適用します。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。

IP アドレスとしきい値の追加または削除

特定の送信元または宛先 IP アドレスとの間に大量のトラフィックがあることがわかっている場合に、Detector が誤って攻撃を検出しないようにするために、その IP アドレスに関連するトラフィック用のしきい値をポリシーに設定することができます。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 アドレスからの大量のトラフィック：ゾーンが通常特定の送信元 IP アドレスから大量のトラフィックを受信する場合は、その送信元 IP アドレスからのトラフィックに適用されるしきい値をポリシーに設定します。
- 宛先 IP アドレスへの大量のトラフィック：ゾーンに複数の IP アドレスが定義され、ゾーンの複数のセクションが通常大量のトラフィックを受信する場合は、そのゾーン内の IP アドレスを宛先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

ポリシーの IP アドレスとしきい値を設定するには、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 > Policies> View** 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 で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 Guard で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 8-4 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 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 > Policies> View** 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 で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 Guard で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 がポリシー構築フェーズで検出しなかったサービスを手動でゾーンの設定に追加することができます。サービスを追加すると、Detector はそのサービス用に選択したポリシー テンプレートを使用して、そのサービス用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 テンプレートで作成したゾーンの設定でサービスを追加または削除すると、Detector と Cisco Guard のポリシーの設定でサービスが変更されます。

ゾーンの設定でサービスを追加または削除すると、Detector は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、次のアクションを実行するまで Detector でゾーンの異常を検出することはできません。

- 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

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 > Policy Templates > Add Service** を選択します。
- 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。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 と Cisco Guard のどちらのポリシーの設定が表示されているかに関係なく、両方のポリシーの設定でサービスが変更されます。
- 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 テンプレートの使用」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 画面に追加されたサービスのポリシーが表示され、Detector 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 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）。

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 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 は、選択したポリシー 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、Detector のポリシーが削除されたトラフィック サービスに関連付けられなくなるため、ゾーンの異常の検出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 > Policy Templates > Remove Service** を選択します。
- 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。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 と Cisco Guard のどちらのポリシーの設定が表示されているかに関係なく、両方のポリシーの設定でサービスが変更されます。
- 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 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）。