ゾーンのポリシーの管理

Guard 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

ゾーン 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 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。

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

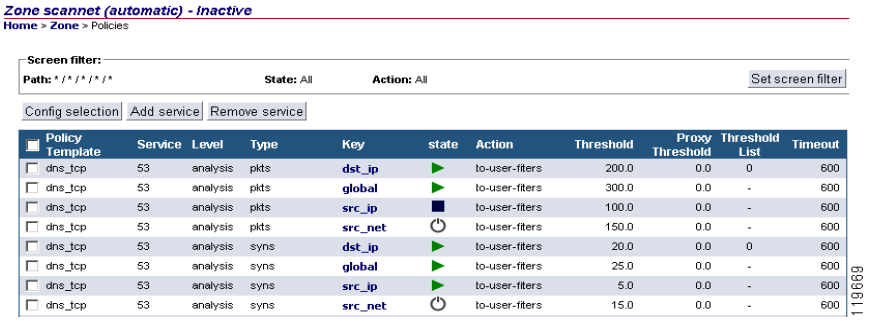

表 8-2 に、ポリシー テーブルに含まれているフィールドの説明を示します。

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	Guard 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、Guard が特定の DDoS 攻撃からの保護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.8-16 の「サービスの追加または削除」を参照してください。 Guard 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、サービスの値 **any** を表示します。
Level	ポリシーがトラフィック フローに適用する保護レベル。 次の 3 つの保護レベルがあります。 • Analysis • Basic • Strong

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	Guard 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。 • **num_sources**：ゾーンが宛先となっていて、Guard のスプーフィング防止機能によって認証された TCP 送信元 IP アドレスがあるパケット。 • **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。Guard 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。
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：Guard は、ポリシーをトラフィック フローに適用します。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：Guard は、ポリシーをトラフィック フローに適用します。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：Guard は、ポリシーをトラフィック フローに適用しません。

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
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、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中に Guard に設定させることもできます。 デフォルトでは、しきい値はオンデマンド保護に適した値に設定されています。
Proxy Threshold	HTTP プロキシ クライアントのしきい値。プロキシしきい値は、プロキシを介して HTTP でゾーンに接続するクライアントのトラフィック レートを定義します。CLI を使用して、プロキシしきい値を設定します。
Threshold List	特定のポリシーのしきい値リストのエントリ数。ダッシュ（-）は、ポリシーのしきい値リストを設定できないことを示します。
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。タイムアウトになると、Guard はポリシーによって作成された動的フィルタを非アクティブにするかどうかを決定します。タイムアウト値は、**never** に設定できます。
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、Guard 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	Guard 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、Guard 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、Guard 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、Guard 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 にあるポリシー 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** : Guard は、ポリシーをトラフィックに適用します。ポリシーは、トラフィックがポリシーのしきい値を超過すると、割り当てられているアクションを実行します。 • **inactive** : Guard はポリシーをトラフィックに適用しますが、ポリシーは、トラフィックがポリシーのしきい値を超過しても、割り当てられているアクションを実行しません。 • **disabled** : Guard 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**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 Guard 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。 ポリシーが定義している保護が強化されるように、ポリシー アクションを設定します。たとえば、分析の保護モジュールを持つポリシーに対して、ポリシー アクションを to-user-filters に設定します。あるいは、強化の保護モジュールを持つポリシーに対して、ポリシー アクションを filter/drop に設定します。ポリシーが定義している保護レベルが低下するようなポリシー アクションは設定しないでください。たとえば、基本または強化の保護モジュールを持つポリシーに対して、ポリシー アクションを to-user-filters に設定しないでください。 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。 • **block-unauthenticated**：スプーフィング防止機能によって認証されなかったトラフィック（事前のハンドシェイクがない ACK など）をブロックするフィルタを追加します。 このポリシー アクションは、パケット タイプが in_unauth_pkts および unauth_pkts のポリシーに対してだけ設定してください。 • **to-user-filters**：トラフィックをユーザ フィルタに転送するフィルタを追加します。 このポリシー アクションは、分析の保護レベルを持つポリシーに対して設定してください。 • **filter/strong**：トラフィック フローに強化保護レベルを適用するフィルタを追加します。 このポリシー アクションは、分析および基本の保護レベルを持つポリシーに対して設定してください。このポリシー アクションは、トラフィック特性が src_ip の TCP（着信）ポリシーに対してだけ使用し、トラフィック特性が global のポリシーに対しては使用しないことをお勧めします。そのようにしないと、ロード バランサまたは ACL[1] を使用してトラフィックを管理しているネットワークで、ネットワークの問題が発生する場合があります。

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

パラメータ	説明
Action（*続き*）	• **filter/drop** : Guard に特定のトラフィックをドロップするように指示するフィルタを追加します。 このポリシー アクションは、Guard がスプーフィング防止機能を適用した後にトラフィックを監視するポリシー（基本および強化の保護レベルを持つポリシー）に対して設定してください。分析の保護レベルを持つポリシーに対してこのポリシー アクションを使用することはお勧めしません。そのようにすると、Guard はスプーフィングを利用した攻撃を軽減するときに、すべての Guard フィルタを消費する場合があります。 • **redirect/zombie** : すべてのユーザ フィルタの認証を拡張し、リダイレクト アクションを備えるフィルタを追加します。 このポリシー アクションは、tcp_connections/any/basic/num_sources/global ポリシーだけに適用されます。
Threshold	ポリシーのしきい値となるトラフィック レート。トラフィックがしきい値を超過すると、ポリシーはゾーンを保護する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。

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生成した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	Guard が、しきい値調整フェーズの結果を受け入れ、ポリシー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 パラメータを設定できます。 • **Set as fixed** : Guard 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。Guard は、しきい値調整フェーズの結果を受け入れるときに、ポリシーのこのしきい値を変更しません。 • **Learning multiplier** : Guard 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、指定された係数をラーニングしたしきい値に乗算して新しいポリシーしきい値を計算します。Guard は、設定されている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。ポリシーしきい値に掛ける正の実数値（小数点以下 2 桁の浮動小数点数）を入力してください。ポリシーしきい値を小さくするには、1 未満の数値を入力します。

1. ACL = Access Control List（アクセス コントロール リスト）

IP アドレスとしきい値の設定

大量のトラフィックが発生することが分かっている送信元 IP アドレスまたは宛先 IP アドレスでトラフィックが増加したときに、Guard が誤って攻撃を検出することを避けるには、その IP アドレスに関連するトラフィックのしきい値をポリシーで設定します。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。

- 大量のトラフィックが発生する送信元 IP アドレス：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日常的に受信するときは、その送信元 IP アドレスからのトラフィックに Guard が適用するしきい値をポリシーで設定できます。
- 大量のトラフィックが発生する宛先 IP アドレス：ゾーンに複数の IP アドレスを定義していて、ゾーンの特定のセクションが大量のトラフィックを日常的に受信するときは、ゾーン内部のその宛先 IP アドレスをターゲットとするトラフィックに Guard が適用するしきい値をポリシーで設定できます。

IP しきい値は、次の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 アクションがドロップのポリシー。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 Guard によってポリシーに適用されるアクションです。ポリシー アクションを変更した場合でも、このようなポリシーのしきい値リストを設定できます。

ポリシーごとに最大 10 個の IP アドレスとしきい値を設定できます。

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　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 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**：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　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 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　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

ポリシー構築フェーズ中に Guard が検出しなかったサービスは、ゾーンの設定に手動で追加することができます。サービスを追加すると、Guard はそのサービス用にシステム管理者が選択したポリシー テンプレートに基づいて、そのサービスのため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
- tcp_services_ns
- udp_services

http、tcp_services、tcp_services_ns、および udp_services の場合、追加するサービスはポート番号を指定します。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。

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、Guard 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、次のいずれかの操作を実行するまでは、Protect and Learn を有効にしても Guard はゾーンを保護できません。

- 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。
- 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　ポリシー テンプレートを Policy Template リストから選択し、**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」の項を参照してください。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、追加したサービスのポリシーが示されます。Guard 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。Guard は、選択するポリシー テンプレートから作成されたポリシーをすべて削除します。

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 Guard のポリシーが関連付けられなくなるため、ゾーン保護に支障をきたす場合があります。

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　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。
- 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、Guard 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）。