



ゾーンのポリシーの管理

この章では、Cisco Guard (Guard) で、ゾーン設定のポリシーを変更する方法、およびゾーン設定の保護機能を手動で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。

- [ゾーンのポリシーについて](#)
- [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](#)

ゾーンのポリシーについて

ゾーンのポリシーによって、Guard は、ゾーンのトラフィック フローの統計分析を行うことができます。ポリシーは、ポリシーのタイプに応じて、トラフィックで次のいずれかのトラフィック特性を監視します。

- **トラフィック レート**：パケット / 秒単位またはパケット / 時単位で測定した、トラフィックのレート。パケット / 時単位でトラフィックを監視するポリシー (PPH ポリシー) は、ゾーントラフィックで、何時間または何日も続くことのある低レート ゾンビ攻撃を監視するために使用されます。PPH ポリシーの詳細については、「[ポリシーのパラメータの変更](#)」の項を参照してください。



(注) PPH ポリシーは、6.1 ソフトウェア リリースで作成するゾーン設定だけに含まれます。以前のソフトウェア バージョンで作成したゾーンには、PPH ポリシーが含まれません。

- **接続**：同時接続の数。
- **パケットの比率**：あるパケット タイプと別のパケット タイプの比率。

トラフィック フローがポリシーのしきい値を超えると、ゾーンのポリシーはそのフローを悪意のあるもの、または異常なものであると見なします。その時点で、ポリシーは、フィルタを動的に作成して (動的フィルタ)、攻撃の重大度に応じてトラフィック フローを保護します。ポリシーのしきい値、およびポリシーが異常を検出したときに実行するアクションを設定できます。

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。ゾーンのマイン メニューが表示されます。
- ステップ 2** ゾーンのマイン 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) 表示または設定の対象のポリシーだけが表示されるように、次の方法で画面フィルタを設定します。

- 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。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るため、一番上から開始する必要があります。

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。

- ステップ 4** (オプション) 1 つのポリシーだけの詳細を表示する場合、またはポリシー設定を変更する場合は、目的のポリシーの Key タイプをクリックします。Policy Details 画面が表示されます。ポリシー設定の変更については、「[ポリシーのパラメータの変更](#)」の項を参照してください。

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

Zone scannet (automatic) - inactive
Home > Zone > Policies

Screen filter:
Path: ^ / * / * / * / * State: All Action: All Set screen filter

Config selection Add service Remove service

Policy Template	Service	Level	Type	Key	state	Action	Threshold	Proxy Threshold	Threshold List	Timeout
<input type="checkbox"/> dns_tcp	53	analysis	pmts	dst_ip	▶	to-user-filters	200.0	0.0	0	600
<input type="checkbox"/> dns_tcp	53	analysis	pmts	global	▶	to-user-filters	300.0	0.0	-	600
<input type="checkbox"/> dns_tcp	53	analysis	pmts	src_ip	■	to-user-filters	100.0	0.0	-	600
<input type="checkbox"/> dns_tcp	53	analysis	pmts	src_net	⏻	to-user-filters	150.0	0.0	-	600
<input type="checkbox"/> dns_tcp	53	analysis	syns	dst_ip	▶	to-user-filters	20.0	0.0	0	600
<input type="checkbox"/> dns_tcp	53	analysis	syns	global	▶	to-user-filters	25.0	0.0	-	600
<input type="checkbox"/> dns_tcp	53	analysis	syns	src_ip	▶	to-user-filters	5.0	0.0	-	600
<input type="checkbox"/> dns_tcp	53	analysis	syns	src_net	⏻	to-user-filters	15.0	0.0	-	600

118683

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 Distributed Denial of Service (DDoS; 分散型サービス拒絶) 攻撃からの保護で必要とする特定のトラフィック特性に関連しています。
Service	<p>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。詳細については、「サービスの追加または削除」の項を参照してください。</p> <p>Guard 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について、サービスの値が <i>any</i> と表示されます。</p>
Level	<p>ポリシーがトラフィック フローに適用する保護レベル。</p> <p>次の 3 つの保護レベルがあります。</p> <ul style="list-style-type: none"> • 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	<p>Guard が監視するパケット タイプ。</p> <p>パケット タイプの値は次のとおりです。</p> <ul style="list-style-type: none"> 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 Domain Name System (DNS; ドメイン ネーム システム) 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。 reqs_pph : データ ペイロードを含んだ要求パケット (パケット / 時単位)。このパケット タイプのポリシーは、ゾーン トラフィックの低レート ゾンビ攻撃を監視するために設計されています。新しいゾーンの作成時は、デフォルトで PPH ポリシーがディセーブル状態に設定されています。これは、PPH ポリシーにより、ゾーンが使用するメモリ量が増加したり、Guard のパフォーマンスに影響が及んだりする可能性があるためです。ゾーンの PPH ポリシーをイネーブルにするには、ポリシーの状態をアクティブに変更する必要があります (「ポリシーのパラメータの変更」の項を参照)。 syns : 同期パケット (TCP SYN フラグの付いたパケット)。 syns_pph : 同期パケット (TCP SYN フラグの付いたパケット (パケット / 時単位))。このパケット タイプのポリシーは、ゾーン トラフィックの低レート ゾンビ攻撃を監視するために設計されています。新しいゾーンの作成時は、デフォルトで PPH ポリシーがディセーブル状態に設定されています。これは、PPH ポリシーにより、ゾーンが使用するメモリ量が増加したり、Guard のパフォーマンスに影響が及んだりする可能性があるためです。ゾーンの PPH ポリシーをイネーブルにするには、ポリシーの状態をアクティブに変更する必要があります (「ポリシーのパラメータの変更」の項を参照)。 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	<p>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。</p> <p>キー名の値は次のとおりです。</p> <ul style="list-style-type: none"> • 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 スキャン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 スキャンングに使用されます。
State	<p>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。</p> <ul style="list-style-type: none"> ▶ 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 フローに適用しません。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。
Action	<p>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。</p>
Threshold	<p>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で Guard が設定することもできます。</p> <p>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。</p>
Proxy Threshold	<p>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。</p>
Threshold List	<p>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。</p>

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
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。
Detection Time	PPH ポリシーがパケット レートの平均値を計算する期間を定義するパラメータ。PPH ポリシーは、ゾーン トラフィックの低レート ゾンビ攻撃を監視し、パケット / 秒単位ではなくパケット / 時単位でトラフィック レートを測定するポリシーです (「 ゾーンのポリシーについて 」の項を参照)。

ポリシーのパラメータの変更

この項では、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。ゾーンポリシーを変更できるのは、Guard がゾーントラフィックのラーニングまたはゾーンの保護を実行していない場合のみです。1つのポリシーのパラメータを変更することも、複数のポリシーのパラメータを同時に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** タイプをクリックします (Policy Details 画面が表示されます)。次に、Learning Parameters テーブルの下にある **Config** 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、そのポリシーセクションに含まれている値が、選択したすべてのポリシーで同一とは限らないことを示します。
- 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空白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	<p>ポリシーの状態。表示される値は次のいずれかです。</p> <ul style="list-style-type: none"> • active : Guard がポリシーをトラフィックに適用し、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 : Guard がポリシーをトラフィックに適用しますが、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 : Guard はポリシーをトラフィックに適用しません。 <p> 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。</p>
Action	<p>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。</p> <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • notify : トラフィックがポリシーの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 バランサまたはアクセス コントロール リスト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)	<ul style="list-style-type: none"> 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。使用した場合、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可能性があります。 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	<p>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。</p> <p>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。</p> <p>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 packets per second (pps; パケット / 秒) 単位で測定されます。</p> <ul style="list-style-type: none"> num_soruces : 測定の単位は、IP アドレスまたはポートの数です。 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。
Threshold multiplier	<p>ポリシーのしきい値を増減するための係数。</p> <p>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。</p> <p>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。</p> <p> (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。</p>
Timeout	<p>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。</p>
Detection Time	<p>(PPH ポリシーのみ) PPH ポリシーがパケット レートの平均値を計算する期間。デフォルトは1時間ですが、悪意のあるトラフィックと正当なトラフィックを識別するために長いサンプリング期間が必要な場合は、検出時間を長くすることができます。たとえば、1時間の期間中に正当なユーザと攻撃者が同じ数のパケットを送信することがあります。ただし、2時間の期間では、正当なユーザがトラフィックの送信を停止してトラフィック レートが低くなる一方、執拗な攻撃者のトラフィック レートは高いままであることがあります。PPH ポリシーの詳細については、「ゾーンのポリシーについて」の項を参照してください。</p> <p>検出時間は、時間単位で定義します。1～48の値を入力します。デフォルトは1です。</p>

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

パラメータ	説明
Learning parameters	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • Set as fixed : 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場合、Guard はこのポリシーのしきい値を変更しません。 • Learning multiplier : 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。

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。

- 送信元 IP アドレスからのトラフィック量が多い：通常の状態では、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、通常の状態では、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 アドレス (`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。

この項は、次の内容で構成されています。

- [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 アドレスのトラフィックしきい値。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。 <ul style="list-style-type: none"> 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 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、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 (アプリケーション ポートまたはプロトコル) をゾーンの設定に手動で追加できます。ゾーンに最適な保護にするために、ゾーンの主要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

ネットワークのパフォーマンスを低下させる恐れがあるため、複数のポリシーに同じサービス (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関してサービスを追加または削除すると、Guard はゾーンのポリシーを未調整としてマークします。ゾーンが未調整のため、Protect and Learn をアクティブにしても、次のアクションのいずれかが実行されるまで Guard で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)。

この項は、次の内容で構成されています。

- 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。Guard は、ポリシー構築フェーズ中に検出したサービスに新しいサービスを追加し、新しいサービスにデフォルトのしきい値を設定します。しきい値を手動で定義することもできますが、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、ポリシーをゾーントラフィックに合せて調整することをお勧めします。

新しいサービスを追加できるのは、次のポリシー テンプレートから作成されたポリシーです。

- tcp_services、udp_services、tcp_services_ns
このサービスは、ポート番号を表します。
- other_protocols
このサービスは、プロトコル番号を表します。



(注)

サービスを追加した後でポリシー構築フェーズをアクティブにすると、新しいサービスによって、手動で追加したサービスが上書きされる場合があります。

次の理由で、サービスを手動で追加する必要があることがあります。

- 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が、サービスをゾーン設定に追加するためにポリシー構築フェーズをアクティブにしたくない。
- すべてのネットワーク サービスを検出するだけの十分な時間、ポリシー構築フェーズを実行しなかった。たとえば、1 週間に 1 回だけまたは夜の間だけアクティブであるアプリケーションまたはサービスがあることが分かっているが、そのときにポリシー構築フェーズをアクティブにしていない場合があります。

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 リストからポリシー テンプレートを**Next** をクリックします。Add Service Step 2 画面が表示されます。
- ポリシー テンプレートのタイプについては、[第 6 章「ポリシー テンプレートの設定」](#)の「[ポリシー テンプレートについて](#)」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。Guard 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。しきい値を手動で定義することもできますが、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、ポリシーをゾーン トラフィックに合せて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。
-

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、ゾーンのポリシーを調整済みとしてマークできます。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「[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

任意のポリシー テンプレートの特定のサービスを削除できます。Guard 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、そのサービスを削除します。



注意

サービスを削除すると、ゾーンのポリシーはそのサービスのトラフィックを監視できません。そのため、ゾーン保護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`
このサービスは、ポート番号を表します。
- `other_protocols`
このサービスは、プロトコル番号です。

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は、次の理由でサービスを手動で削除する必要があることがあります。

- 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。
- ポリシー構築フェーズ中にアプリケーションまたはサービスが識別されたが、ネットワーク環境でそのアプリケーションまたはサービスが一般的でないためイネーブルにしたいくない。



(注)

サービスを削除した後でポリシー構築フェーズをアクティブにすると、Guard が同じサービスを再度追加する場合があります。

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** 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 画面で **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。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) 次のいずれかの操作を実行して、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して、現在のゾーンポリシーのバックアップを作成できます。

ゾーン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 画面が表示されません。
 - 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。Guard はゾーンポリシーを保存し、スナップショットに連続した ID 番号を割り当てます。
-