ゾーン トラフィックのラーニング

この章では、Detector のラーニング プロセスを使用して、ゾーンのトラフィック特性を分析し、Detector がゾーン異常検出に使用するポリシーを作成および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。

ラーニング プロセスについて

ラーニング プロセスは、ネットワーク上で攻撃が発生していないときに、正常なトラフィック パターンのベースラインを作成します。Detector は、このベースラインを、ゾーン トラフィックの異常を検出するための参照ポイントとして使用します。このような参照ポイントは、*ポリシー*と呼ばれます。

ラーニング プロセス中に、Detector はポリシーを作成し、作成した各ポリシーのしきい値を調整します。Detector がゾーンのトラフィックをラーニングしている間、システム管理者はラーニング プロセスを監視して、ラーニング プロセスの結果を受け入れるか拒否するかを決定できます。

この項は、ラーニング プロセスに関する次の情報で構成されています。

ラーニング プロセスのフェーズについて

ラーニング プロセスは、次の 2 つのフェーズで構成され、それぞれを Detector で個別に実行します。

1. ポリシー構築フェーズ : Detector がポリシー テンプレートを使用してゾーン ポリシーを作成します。各ポリシーは、デフォルトのしきい値とアクションで設定されます。トラフィックが通過することにより、Detector はゾーンが使用している主要サービスの検出が可能になります。新しいポリシーは、既存のポリシーを上書きします。

   ポリシー テンプレートは、ポリシーを構築するための Detector ツールです。これらのテンプレートは、Detector が作成するゾーン ポリシーのタイプを定義します。ポリシー テンプレートは、Detector が詳細に監視するサービスの最大数、および Detector による新しいポリシーの作成をトリガーする最小しきい値も定義します。ゾーン ポリシーを構築するための規則を変更するには、ポリシー構築フェーズを開始する前に、ポリシー テンプレートのパラメータを変更する必要があります。

- しきい値調整フェーズ：Detector がゾーン ポリシーのしきい値を調整します。ポリシーのしきい値は、通常のトラフィックがポリシーのアクションをアクティブにすることなく Detector を通過できる値に設定されます。ゾーンを保護しているとき、Detector はゾーンのポリシーをトラフィック フローに適用し、ポリシーのしきい値を超過した場合は Detector がポリシーのアクションで動的フィルタを作成します。

ポリシー構築フェーズとしきい値調整フェーズを使用するタイミングおよび方法については、次に示す 2 つの例外があります。

- ポリシー構築フェーズは、Guard_Link ゾーン テンプレートおよび Detector_Link ゾーン テンプレートを使用して作成するゾーンに対しては実行できません。
- ゾーンの設定に worm_tcp ポリシー テンプレートが含まれる場合、Detector はしきい値調整フェーズを使用してワーム ポリシーを構築し、作成する各ポリシーのしきい値を調整します。

ラーニング プロセスを実行するには、スイッチにポート ミラーリングを設定するか、光スプリッタを使用して Detector をルータに接続する必要があります。

Detector のスナップショット機能を使用すると、どちらのラーニング フェーズでも、ラーニング プロセスの任意の時点で現在の結果を保存できます。ラーニング プロセスのスナップショットを取得すると、スナップショットの時点までに Detector で作成されたポリシー情報を表示することができます。ラーニング フェーズの結果をスナップショットに保存しても、ゾーンの設定には影響しません。ラーニング プロセスのスナップショットは、必要に応じていくつでも取得できます。ゾーンの設定は、スナップショットに保存したポリシー情報を使用していつでもアップデートできます。スナップショット機能の使用の詳細については、「ラーニング プロセスのスナップショットの管理」の項を参照してください。

検出およびラーニング機能について

Detector がラーニング プロセスのポリシー構築フェーズの実行を終えたら、Detect and Learn 機能をアクティブにできます。この機能を使用すると、Detector でしきい値調整フェーズ（Learn）を実行しながら、同時にトラフィックの異常を探索（Detect）することができます。Detector は、攻撃を検出するとラーニング プロセスを一時停止します。攻撃が終了すると、Detector はラーニング プロセスを再開します。検出およびラーニング機能を使用すると、Detector は、ゾーン トラフィックの異常を検出したり、ゾーンのトラフィック特性に基づいてポリシーのしきい値を常にアップデートすることが可能になるため、Detector が悪意のあるトラフィックのしきい値をラーニングすることが防止されます。

ラーニング プロセスの結果の管理

ポリシー構築フェーズまたはしきい値調整フェーズを停止したとき、そのフェーズの結果を受け入れるか拒否するかを決定できます。結果を受け入れてラーニング フェーズを継続することもできます。Detector は、ラーニング プロセスの実行中はゾーンの設定のポリシーを変更しません。Detector がゾーンの設定をアップデートし、新しいポリシーやポリシーのしきい値を使用して動作を開始するのは、ユーザがラーニング フェーズの結果を受け入れた後だけです。

ラーニング プロセスの実行

この項の手順では、ラーニング プロセスの 2 つのフェーズ、ポリシー構築フェーズとしきい値調整フェーズを開始および停止する方法について説明します。ラーニング プロセスは、ゾーン異常検出を次の方法で最適化するために使用します。

- 選択したゾーン テンプレートのデフォルト ポリシーとポリシーしきい値を使用して設定した、新しいゾーンのポリシーを微調整する。
- ゾーンのトラフィック　パターンが変化したときに、ゾーンの既存の設定をアップデートする。

ラーニング プロセスの結果を正確なものにし、通常時のゾーン トラフィックに適合した設定結果を得るためには、ゾーンのトラフィックが次の条件を満たしたときにラーニング プロセスをアクティブにします。

- ゾーンのトラフィックが通常である（攻撃を受けていない）：この条件により、Detector が DDoS 攻撃のトラフィックの特性に従ってゾーンのポリシーを構築および調整しないことが保証されます。ゾーンが攻撃を受けているときにラーニング プロセスを開始した場合、Detector は攻撃のトラフィック パターンをラーニングして、そのラーニング結果を以後の参照基準として保存します。この結果、Detector が以後の攻撃を通常のトラフィック状態と見なすことがあるため、攻撃を検出できなくなる可能性が生じます。
- ゾーンのトラフィックのボリュームがピークに達している：この条件により、Detector はポリシーのしきい値を通常のトラフィックのピーク時に相当する値に設定することができ、Detector は、通常のトラフィックのピーク時の状態を攻撃として認識することがなくなります。

この項では、次の手順について説明します。

ポリシー構築フェーズの開始

ポリシー構築フェーズは、新しいゾーンを作成した後、または新しいサービス ポリシーを使用してゾーンの設定をアップデートする必要があるときに使用します。ポリシー構築フェーズを実行した後は、しきい値調整フェーズを実行して各ポリシーのしきい値を微調整します。

（注） ポリシー構築フェーズは、Guard_Link ゾーン テンプレートまたは Detector_Link ゾーン テンプレートのいずれかを使用して作成したゾーンに対しては実行できません。

ポリシー構築フェーズを開始するには、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 **Learning > Construct Policies** を選択します。Detector は、トラフィック フローで使用されているサービスに関するゾーン トラフィックのコピーの分析を開始し、検出する各サービスに関連するポリシーを作成します。

Policy Templates 画面が表示されます。

ゾーンのステータス アイコンがラーニング  に変更されます。

ステップ 3　（オプション）ポリシー構築フェーズの任意の時点で、**Learning > Snapshot** を選択してこのフェーズの現在の結果と提案されているポリシーを保存し、確認します。スナップショット機能の使用の詳細については、「ラーニング プロセスのスナップショットの管理」の項を参照してください。

（注）　ゾーンの設定に worm_tcp ポリシー テンプレートを使用する場合、Detector はしきい値調整フェーズを使用してワーム ポリシーを構築し、作成する各ポリシーのしきい値を調整します（「しきい値調整フェーズの開始」の項を参照）。

Detector が通常のゾーン トラフィックの正確な状態を取得し、分析できるように、ポリシー構築フェーズは 2 時間以実行してから停止することをお勧めします。

ポリシー構築フェーズの現在の結果の受け入れ

ラーニング プロセスの結果を受け入れた後も Detector によるゾーンのトラフィック特性のラーニングを継続するには、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 **Learning > Accept** を選択します。Detector はゾーンの設定の現在のポリシーをすべて削除し、提案されたゾーンのポリシーに置き換えます。Detector はポリシー構築フェーズを停止せず、ゾーンのサービスのラーニングを続行します。

ポリシー構築フェーズの停止

ポリシー構築フェーズを停止するには、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 **Learning > Stop Learning** を選択します。Stop Learning ウィンドウが表示されます。

ステップ 3　次のいずれかのオプションを選択します。

- **Reject**：提案されたゾーン ポリシーを拒否します。
- **Accept**：提案されたゾーン ポリシーを受け入れます。

ステップ 4　次のいずれかのオプションを選択します。

- **OK**：このオプションを選択した場合の結果は、ポリシー構築フェーズの結果を受け入れるか、拒否するかによって次のように異なります。
  - **Reject** を選択した場合、Detector は提案されたゾーン ポリシーをすべて削除します。ゾーンの設定は一切変更されません。
  - **Accept** を選択した場合、Detector は、ゾーンの設定の現在のポリシーを、提案されたゾーン ポリシーで置き換え、ポリシー構築フェーズを終了します。
- **Clear**：Stop Learning ウィンドウの設定をデフォルトに戻します。
- **Cancel**：Stop Learning ウィンドウを閉じて、ポリシー構築フェーズを続行します。

ポリシー構築フェーズの結果を受け入れてから、しきい値調整フェーズをアクティブにします。しきい値調整フェーズを実行すると、受け入れたポリシーのしきい値が、ゾーンのトラフィック フローの特性に基づいて設定されます。ポリシーは、しきい値調整フェーズを実行するまでは工場出荷時のデフォルトしきい値を使用して設定されます。

しきい値調整フェーズの開始

ポリシー構築フェーズの実行後、またはゾーンのポリシーのしきい値をアップデートする必要があるときは、しきい値調整フェーズを使用します。

（注）　ゾーンの設定に worm_tcp ポリシー テンプレートが含まれる場合、Detector はしきい値調整フェーズを使用してワーム ポリシーを構築し、作成する各ポリシーのしきい値を調整します。

しきい値調整フェーズを開始するには、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 **Learning > Tune Threshold** を選択します。Detector は、ゾーンのトラフィックの分析を開始し、ゾーンのポリシーのしきい値をトラフィック フローの特性に合せて調整します。

ゾーンのステータス ラーニング アイコン  が、作業領域内の、ナビゲーション パネルのゾーン名の隣に表示されます。

しきい値調整フェーズは、少なくとも 24 時間実行してから終了することをお勧めします。

ステップ 3　（オプション）しきい値調整フェーズの任意の時点で、ゾーンのメイン メニューの **Learning > Snapshot** を選択して、このフェーズの現在の結果と提案されているしきい値を保存し、確認します。スナップショット オプションの使用の詳細については、「ラーニング プロセスのスナップショットの管理」の項を参照してください。

Detector が通常のゾーン トラフィックの正確な状態を取得し、分析できるように、しきい値調整フェーズは 24 時間以実行してから停止することをお勧めします。

しきい値調整フェーズの現在の結果の受け入れ

しきい値調整フェーズの現在の結果を受け入れて、Detector がしきい値調整フェーズを継続できるようにするには、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 **Learning > Accept** を選択します。Accept Thresholds ウィンドウが表示されます。

ステップ 3　使用するしきい値の選択方法を定義します。表 7-1 に、Accept Thresholds ウィンドウに表示されるパラメータの説明を示します。

表 7-1　しきい値の選択方法

パラメータ	説明
Threshold selection method	受け入れるしきい値を選択する方法。ドロップダウン リストから、次のいずれかのオプションを選択します。 • **Accept new thresholds** : Detector は、ラーニング プロセスの結果をゾーンの設定に保存します。 • **Accept max. thresholds** : Detector は、ポリシーの現在のしきい値をラーニングしたしきい値と比較し、値の大きい方をゾーンの設定に保存します。これがデフォルトの方法です。 • **Accept weighted thresholds** : Detector は、次の公式に基づいて、保存するポリシーのしきい値を計算します。 新しいしきい値 =（ラーニングしたしきい値 * 重み + 現在のしきい値 *（100 - 重み））/ 100 Weight フィールドに重み値を入力します。 • **Keep current thresholds** : Detector は、ラーニング プロセスの提案されたしきい値をすべて拒否し、ポリシーが現在のしきい値を保持します。
Weight	Detector が新しいしきい値の計算に使用する重みを定義します。このオプションがアクティブになるのは、しきい値の選択方法として **Accept weighted thresholds** を選択したときのみです。次の式に、Detector が使用する重み値を入力します。 新しいしきい値 =（ラーニングしたしきい値 * 重み + 現在のしきい値 *（100 - 重み））/ 100

ステップ 4　次のいずれかのオプションを選択します。

- **OK**：Detector　は、ゾーンの設定のポリシーをしきい値調整フェーズの現在の結果でアップデートして、しきい値調整フェーズを継続します。
- **Clear**：Accept Thresholds ウィンドウの設定をデフォルトに戻します。
- **Cancel**：Accept Thresholds ウィンドウを閉じて、しきい値調整フェーズを続行します。

しきい値調整フェーズの停止

しきい値調整フェーズの現在の結果を受け入れるか拒否して、しきい値調整フェーズを停止するには、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 **Learning > Stop Learning** を選択します。Stop Learning ウィンドウが表示されます。

ステップ 3　Stop Learning ウィンドウで、次のいずれかのオプションを選択します。

- **Reject**：しきい値調整フェーズの現在の結果を無視します。
- **Accept**：しきい値調整フェーズの現在の結果をゾーンの設定に使用します。使用するしきい値の選択方法を定義します。

表 7-2 に、しきい値の選択方法のパラメータの説明を示します。

表 7-2　しきい値の選択方法

パラメータ	説明
Threshold selection method	受け入れるしきい値を選択する方法。ドロップダウン リストから、次のいずれかのオプションを選択します。 • **Accept new thresholds**：Detector は、ラーニング プロセスの結果をゾーンの設定に保存します。 • **Accept max. thresholds**：Detector は、ポリシーの現在のしきい値をラーニングしたしきい値と比較し、値の大きい方をゾーンの設定に保存します。これがデフォルトの方法です。 • **Accept weighted thresholds**：Detector は、次の公式に基づいて、保存するポリシーのしきい値を計算します。 新しいしきい値 =(ラーニングしたしきい値 * 重み + 現在のしきい値 *（100 - 重み））/ 100 Weight フィールドに重み値を入力します。 • **Keep current thresholds**：Detector は、ラーニング プロセスの提案されたしきい値をすべて拒否し、ポリシーが現在のしきい値を保持します。
Weight	Detector が新しいしきい値の計算に使用する重みを定義します。このオプションがアクティブになるのは、しきい値の選択方法として **Accept weighted thresholds** を選択したときのみです。次の式に、Detector が使用する重み値を入力します。 新しいしきい値 =（ラーニングしたしきい値 * 重み + 現在のしきい値 *（100 - 重み））/ 100

ステップ 4　次のいずれかのオプションを選択します。

- **OK**：Detector は、ゾーンの設定のポリシーをしきい値調整フェーズの現在の結果でアップデートして、しきい値調整フェーズを停止します。
- **Clear**：Stop Learning ウィンドウの設定をデフォルトに戻します。
- **Cancel**：Stop Learning ウィンドウを閉じて、しきい値調整フェーズを続行します。

Detect and Learn を使用したラーニング プロセスの実行

この項の手順では、Detect and Learn 操作の管理方法について説明します。Detect and Learn 操作では、Detector はゾーンのトラフィックの異常を分析しながら、ゾーンのトラフィックをラーニングしてポリシーのしきい値を調整します。Detect and Learn をアクティブにする前に、Detector でいつどのようにラーニング プロセスの結果を受け入れるかを設定することができます。Detector は、ゾーンに対する攻撃を検出するとラーニング プロセスを一時停止し、攻撃が終了するとラーニング プロセスを再開します。

この項では、次の手順について説明します。

自動ラーニングのパラメータの設定

自動ラーニングのパラメータを設定すると、Detect and Learn をアクティブにした場合に、Detector がいつどのようにラーニング プロセス（しきい値調整フェーズ）の現在の結果を自動的に受け入れるかを制御できます。

自動ラーニングのパラメータを設定するには、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> Learning Parameters** を選択します。Learning parameters 画面が表示されます。

ステップ 3　**Config** をクリックします。Config learning parameters 画面が表示されます。

ステップ 4　自動ラーニングのパラメータを定義します。

表 7-3 に、ラーニングのパラメータの説明を示します。

表 7-3　ラーニングのパラメータ

パラメータ	説明
Zone is tuned	ゾーンのポリシーを調整済みまたは未調整としてマークします。このオプションを選択すると、ポリシーが調整済みとしてマークされ、Detector でそのポリシーをすぐにゾーンの異常の検出に使用することができます。このオプションの選択を解除すると、ポリシーが未調整としてマークされ、Detector でゾーンの異常を検出する前にしきい値調整フェーズの結果の受け入れが必要になります。詳細については、「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。
Set periodic learning	自動ラーニング プロセスをイネーブルにします。このオプションを選択する場合は、次のラーニング パラメータを設定します。 • Learning cycle：Detector がラーニング プロセスの結果を保存する頻度を定義します。保存の間隔は、週、日、時間、および分単位で定義します。0 ～ 1,000 までの整数を各時間フィールドに入力します。 • Learning results：Detector がラーニング プロセスの結果を保存する方法を定義します。次のいずれかの方法を選択します。 — **Automatic accept**：Detector が提案するラーニング プロセス（ポリシーのしきい値）の結果を、指定した間隔でゾーンの設定に受け入れます。Detector は新しく提案されたゾーン ポリシーを受け入れた後で、ゾーン ポリシーのスナップショットを保存します。 — **Snapshot only**：ラーニング プロセスのスナップショット（ポリシーのしきい値）を指定した間隔で保存します。Detector は新しいポリシーを受け入れず、ゾーンの設定のポリシーのしきい値を変更しません。

表 7-3　ラーニングのパラメータ（続き）

パラメータ	説明
Threshold selection method	受け入れるしきい値を選択する方法。ドロップダウン リストから、次のいずれかのオプションを選択します。 • **Accept new thresholds**：ラーニング プロセスの結果をゾーンの設定に保存します。 • **Accept max. thresholds**：ポリシーの現在のしきい値をラーニングしたしきい値と比較し、値の大きい方をゾーンの設定に保存します。これがデフォルトの方法です。 • **Accept weighted thresholds**：次の公式に基づいて、保存するポリシーのしきい値を計算します。 新しいしきい値 =（ラーニングしたしきい値 * 重み + 現在のしきい値 *（100 - 重み））/ 100 Weight フィールドに重み値を入力します。
Weight	Detector が新しいしきい値の計算に使用する重みを定義します。このオプションがアクティブになるのは、しきい値の選択方法として **Accept weighted thresholds** を選択したときのみです。次の式に、Detector が使用する重み値を入力します。 新しいしきい値 =（ラーニングしたしきい値 * 重み + 現在のしきい値 *（100 - 重み））/ 100

ステップ 5　次のいずれかのオプションを選択します。

- **OK**：Detector は、自動ラーニングのパラメータをゾーンの設定に保存します。
- **Clear**：Learning Parameters フォームの設定をデフォルトに戻します。
- **Cancel**：Config learning parameters 画面を閉じます。

Detect and Learn のアクティブ化

Detect and Learn をアクティブにすると、Detector でゾーンのトラフィックをラーニングしてポリシーのしきい値を調整しながら、ゾーン トラフィックの異常を検出することができます。Detect and Learn をアクティブにする前に、ゾーンのポリシーが調整済みまたは未調整のどちらとしてマークされているかを確認する必要があります。これは、ゾーンのポリシーの調整状態によって Detector の動作が異なるためです。Detect and Learn をアクティブにするときにポリシーが調整済みとしてマークされている場合、Detector は攻撃を検出し、ゾーンのトラフィックをラーニングします。Detect and Learn をアクティブにするときにゾーンのポリシーが未調整としてマークされている場合、Detector は、ゾーンのポリシーのしきい値が一度受け入れられるまで次のように動作します。

- Detector は、ゾーン トラフィックに含まれている攻撃を検出しません。
- Detector は、しきい値の選択方法 Accept new thresholds をアクティブにします（「自動ラーニングのパラメータの設定」を参照）。

ポリシーを調整済みまたは未調整としてマークする方法の詳細については、「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。

Detect and Learn をアクティブにするには、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　**Detect and Learn** をクリックします。

ラーニング プロセスのしきい値調整フェーズ（ゾーンのメイン メニューの **Learning > Tune Thresholds** を選択）とゾーン異常検出（**Detect** をクリック）の両方をアクティブにすることもできます。この順序は重要ではありません。

次の処理が実行されます。

- Detector が、トラフィック異常についてトラフィック フローの分析を開始します。
- Detector はラーニング プロセスのしきい値調整フェーズを開始します。

ナビゲーション ペインの Under Detection ゾーン リストにゾーン名が追加され、Recent Events テーブルには、検出されるゾーンの詳細なリストとともに、検出開始のイベント タイプが表示されます。

Detect and Learn の非アクティブ化

Detector で Detect and Learn を非アクティブにするときには、異常検出とラーニングの両方か、またはこの 2 つの動作のいずれかのみを非アクティブにすることができます。

Detect and Learn を非アクティブにするには、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、検出実行中のゾーンを選択します。ゾーンのメイン メニューとゾーンのステータス画面が表示されます。

ステップ 2　次のいずれかの方法で、Detect and Learn を非アクティブにします。

- ゾーンのステータス画面の **Deactivate** をクリックします。
- ゾーンのメイン メニューの **Detection > Deactivate** を選択します。

Deactivate ウィンドウが表示されます。

ステップ 3　必要なアクションの隣にあるチェックボックスをオンにします。次のアクションをいずれかまたは両方選択します。

- **Stop Detection**：異常の検出を停止します。
- **Stop Learning**：しきい値調整フェーズを停止します。次のいずれかのオプションを選択します。
  - **Reject**：しきい値調整フェーズの現在の結果を無視します。
  - **Accept**：しきい値調整フェーズの現在の結果をゾーンの設定に保存します。使用するしきい値の選択方法を定義します。

表 7-4 に、しきい値の選択方法のパラメータの説明を示します。

表 7-4　しきい値の選択方法

パラメータ	説明
Threshold selection method	受け入れるしきい値を選択するために Detector が使用する方法を定義します。ドロップダウン リストから、次のいずれかのオプションを選択します。 • **Accept new thresholds** : ラーニング プロセスの結果をゾーンの設定に保存します。 • **Accept max. thresholds** : ポリシーの現在のしきい値をラーニングしたしきい値と比較し、値の大きい方をゾーンの設定に保存します。これがデフォルトの方法です。 • **Accept weighted thresholds** : 次の公式に基づいて、保存するポリシーのしきい値を計算します。 新しいしきい値 =(ラーニングしたしきい値 * 重み + 現在のしきい値 *（100 - 重み））/ 100 Weight フィールドに重み値を入力します。 • **Accept current** : ラーニング プロセスの提案されたしきい値を拒否します。ポリシーがしきい値調整フェーズ前の値を保持します。
Weight	Detector が新しいしきい値の計算に使用する重みを定義します。このオプションがアクティブになるのは、しきい値の選択方法として **Accept weighted thresholds** を選択したときのみです。次の式に、Detector が使用する重み値を入力します。 新しいしきい値 =（ラーニングしたしきい値 * 重み + 現在のしきい値 *（100 - 重み））/ 100

異常の検出とラーニングの両方を非アクティブにする場合、ナビゲーション ペインの Detected Zones リストからゾーン名が削除され、Recent Events テーブルには、検出されないゾーンの詳細なリストとともに、保護停止のイベント タイプが表示されます。

ゾーンのステータス アイコンが、検出  からスタンバイ  に変更されます。

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

Detector は、次の条件によってゾーンのポリシーが調整済みまたは未調整であると見なします。

- 未調整：次のいずれかの操作を実行した場合、Detector はゾーン ポリシーを未調整としてマークします。
  - 新しいゾーンを作成する。
  - ゾーンに関するポリシー構築フェーズの結果を受け入れる。
  - ゾーンのポリシーにサービスを追加するか、ゾーンのポリシーからサービスを削除する。
- 調整済み：Detector は、しきい値調整フェーズの結果を受け入れると、ゾーンを調整済みとしてマークします。この時点では、しきい値はゾーンのトラフィック特性に合せて個別に調整されています。

ゾーンに対して Protect and Learn をアクティブにするときは、ゾーンの調整状態を把握しておくことが重要です。Detect and Learn をアクティブにするときにゾーンの調整状態が未調整の場合、Detector は、しきい値調整フェーズの結果を一度受け入れるまで、ゾーンに対する攻撃を検出しません。Detector は、自動ラーニングのパラメータに基づいて、しきい値調整フェーズの結果を受け入れることができます（「自動ラーニングのパラメータの設定」を参照）。または、管理者が手動で結果を受け入れることもできます。Detector は、Threshold selection method の設定にかかわらず、しきい値調整フェーズの最初の結果を受け入れるときに Accept new thresholds 設定を使用します。これ以降は、Detector はシステム管理者が選択したしきい値の選択方法を使用します。

ゾーンの調整状態は手動で変更できます。次のいずれかの条件に当てはまるときは、状態を調整済みに変更することを検討してください。

- トラフィック特性が似ている既存ゾーンの設定をコピーしてゾーンを作成した。
- ポリシーのすべてのしきい値を手動で設定した。

次のいずれかの条件に当てはまるときは、ゾーンの調整状態を未調整に変更することを検討してください。

- ゾーンのネットワークが大幅に変更された。
- ゾーンの IP アドレスまたはサブネットが変更された。
- トラフィックのピーク時に保護およびラーニング機能を開始していない（ピーク時のトラフィックを Detector が攻撃と見なさないようにするため）。

ゾーンを未調整としてマークすると、Detector は現在のポリシーのしきい値に関連付けられず、これらのしきい値を超過してもゾーンに対する攻撃を検出しません。

ゾーンを調整済みまたは未調整としてマークするには、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> Learning Parameters** を選択します。Learning parameters 画面が表示されます。

ステップ 3　**Config** をクリックします。Config learning parameters 画面が表示されます。

ステップ 4　Learning Parameters フォームから、次のいずれかのオプションを選択します。

- ゾーン ポリシーを調整済みとしてマークするには、**Zone is tuned** チェックボックスをオンにします。これにより、Detector はポリシーを調整済みとしてマークし、すぐにそのポリシーをゾーン トラフィックの異常の検出に使用できるようになります。
- ゾーン ポリシーを未調整としてマークするには、**Zone is tuned** チェックボックスをオフにします。これにより、Detector はポリシーを未調整としてマークし、Detector はそのポリシーをゾーン トラフィックの異常の検出に使用する前に、しきい値調整フェーズの結果を受け入れるように求めます。

ステップ 5　次のいずれかのオプションを選択します。

- **OK**：Detector が、調整状態の設定をゾーンの設定に保存します。
- **Clear**：Detector が変更内容を廃棄し、フォームに現在の設定が表示されます。
- **Cancel**：Config learning parameters 画面を閉じます。

Learning Parameter フォームのオプションの詳細については、「自動ラーニングのパラメータの設定」の項を参照してください。

ラーニング プロセスのスナップショットの管理

Detector のスナップショット機能を使用すると、ゾーンのポリシー情報を保存できます。これによって、ポリシーを表示して比較することが可能になります。スナップショット機能を使用して、次の操作を実行することができます。

- ラーニング プロセスの現在の結果を表示する。
- スナップショットのポリシー情報をゾーンの設定に保存する。
- ポリシーのスナップショットの結果を、他のスナップショットまたはゾーンの設定と比較する（「2 つのゾーンまたはスナップショットのポリシーの設定の比較」の項を参照）。
- ゾーンの設定に含まれている、ゾーンの現在のポリシーをバックアップする。

ラーニング プロセスの任意の段階で、現在のラーニング パラメータ（サービス、しきい値、およびその他のポリシー関連データ）のスナップショットを保存できます。Detector は、スナップショット情報を記録し、スナップショットに連続した ID 番号を割り当てながら、現在のラーニング フェーズの実行を継続します。

この項では、次の手順について説明します。

ラーニング プロセスの結果のスナップショット取得

ラーニング プロセス（ポリシー構築またはしきい値調整）の現在の結果のスナップショットを取得するには、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る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ます。

Threshold selection method ドロップダウン リストから、ポリシーのしきい値を受け入れるために Detector が使用するしきい値の選択方法を選択します。

- **Accept new thresholds** : ラーニング プロセスの結果をゾーンの設定に保存します。
- **Accept max. thresholds** : ポリシーの現在のしきい値をラーニングしたしきい値と比較し、値の大きい方をゾーンの設定に保存します。これがデフォルトの方法です。
- **Accept weighted thresholds** : 次の公式に基づいて、保存するポリシーのしきい値を計算します。

  新しいしきい値 = （ラーニングしたしきい値 * 重み + 現在のしきい値 * （100 - 重み））/ 100

  Weight フィールドに重み値を入力します。
- **Accept current** : ラーニング プロセスの提案されたしきい値を拒否します。ポリシーがしきい値調整フェーズ前の値を保持します。

ステップ 4　**Accept weighted thresholds** というしきい値調整方法を選択した場合は、しきい値の計算に Detector が使用する重み値を Weight フィールドに入力します。

ステップ 5　**OK** をクリックしてスナップショットを保存します。Detector 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。

現在のゾーン設定ポリシーのスナップショット取得

ゾーン トラフィックがラーニングされていない（ゾーンがスタンバイ モードであるか、ゾーン検出がイネーブルになっている）ゾーンのスナップショットを取得すると、Detector はゾーンの設定の現在のポリシー情報が含まれたスナップショットを作成します。このタイプのスナップショットは、ゾーンのポリシーのバックアップを作成するために、または比較の対象として使用することができます。

ゾーンの設定のポリシーのスナップショットを作成するには、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 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。

スナップショットの結果の表示と使用

スナップショットの結果を使用して、ポリシーを表示します。次の作業を実行できます。

- スナップショットのポリシーを修正する。
- ゾーン ポリシーをスナップショットからゾーンの設定にコピーする。
- 2 つのゾーン スナップショットのラーニング パラメータを比較してラーニング プロセスの結果を確認し、ポリシー、サービス、およびしきい値の相違点をトレースする（詳細については、この章の「2 つのゾーンまたはスナップショットのポリシーの設定の比較」の項を参照）。

スナップショットの結果を表示および使用するには、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、ラーニング フェーズに現在入っている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 List** を選択します。スナップショットのリストが表示され、各スナップショットの ID 番号と名前が、スナップショットの取得日時とともに示されます。

ステップ 3　スナップショットを表示するには、テーブル内のスナップショット フィールドのいずれかをクリックします。Policies 画面が表示され、スナップショットの時点で Detector が記録したポリシーが示されます。

ステップ 4　次の操作のいずれかまたはすべてを実行して、スナップショット ポリシーを設定します。

- 1　つまたは複数のポリシーのパラメータを設定し直すには、**Configure Selection** をクリックします。詳細については、第 8 章「ゾーンのポリシーの管理」の「ポリシーのパラメータの変更」の項を参照してください。
- サービスをポリシーに追加するには、**Add service** をクリックします。詳細については、第 8 章「ゾーンのポリシーの管理」の「サービスの追加」の項を参照してください。
- サービスをポリシーから削除するには、**Remove service** をクリックします。詳細については、第 8 章「ゾーンのポリシーの管理」の「サービスの削除」の項を参照してください。

ステップ 5　**Accept Thresholds** をクリックして、スナップショットのポリシーをゾーンの設定に保存します。

スナップショットの削除

古いスナップショットを削除すると、ディスク スペースを解放できます。

スナップショットを削除するには、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、ラーニング フェーズに現在入っている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 List** を選択します。スナップショットのリストが表示され、各スナップショットの ID 番号と名前が、スナップショットの取得日時とともに示されます。

ステップ 3　削除するスナップショットの ID 番号の隣にあるチェックボックスをオンにするか、ヘッダー行にあるチェックボックスをオンにしてすべてのスナップショットを選択し、**Delete** をクリックします。

Detector により、選択したスナップショットが Snapshot リストから削除されます。

2 つのゾーンまたはスナップショットのポリシーの設定の比較

2 つのゾーン、2 つのスナップショット、またはゾーンとスナップショットの間で、ポリシーの設定を比較することができます。Detector は、ポリシーの設定のサービス、ポリシー、およびポリシーのしきい値の違いをトレースします。2 つのゾーンまたはスナップショットのポリシー設定を比較しながら、ポリシー設定のアトリビュートを比較元のゾーンまたはスナップショットから削除したり、そこに追加したりできます。比較元のゾーンまたはスナップショットの設定を修正することにより、ラーニングしたポリシー アトリビュートを選択的に受け入れることができます。

この項では、次の手順について説明します。

ポリシーの設定の相違点の表示

2 つのゾーンまたはスナップショットのポリシーを比較して相違点を表示するには、次の手順を実行します。

ステップ 1　次のいずれかの方法で、ポリシーの比較プロセスを開始します。

- Detector の要約のメイン メニューの **Zones > Compare Zone policies** を選択します。
- ゾーンのメイン メニューの **Configuration > Policies > Compare Policies** を選択します。Policies Comparison クエリーが表示されます。

ステップ 2　比較元を定義し、ゾーンまたはスナップショットを比較します。

比較元ゾーンとは、設定を変更できるゾーンです。比較先ゾーンとは、サービスまたはポリシーのコピー元にできるゾーンです。

表 7-5 に、Policies Comparison クエリーのパラメータの説明を示します。

表 7-5　ポリシー比較のパラメータ

パラメータ 1	パラメータ 2	説明
Base Zone	Zone	ゾーンまたはスナップショットの名前。ゾーンの設定を変更するには、そのゾーンを比較元ゾーンとして選択します。比較元となるゾーンをドロップダウン リストから選択します。
	Policy Configuration	選択した比較元ゾーンのポリシーの設定。デフォルト値は、ゾーンの現在のポリシーの設定です。ドロップダウン リストからゾーン ポリシーのスナップショットを選択できます。
Compared Zone	Zone	比較元ゾーンとの比較の対象になるゾーンまたはスナップショットの名前。比較先ゾーンの設定を修正することはできません。比較先となるゾーンをドロップダウン リストから選択します。
	Policy Configuration	選択した比較先ゾーンのポリシーの設定。デフォルト値は、ゾーンの現在のポリシーの設定です。ドロップダウン リストからゾーン ポリシーのスナップショットを選択できます。
Minimal difference		比較元ゾーンと比較先ゾーンにおけるポリシーの設定の相違点の割合。Detector は、2 つのゾーンを比較し、指定された値より大きいポリシーしきい値の相違点だけを表示します。デフォルトの割合は 100% です。この割合では、Detector は 2 つのゾーン間のすべての相違点を表示します。

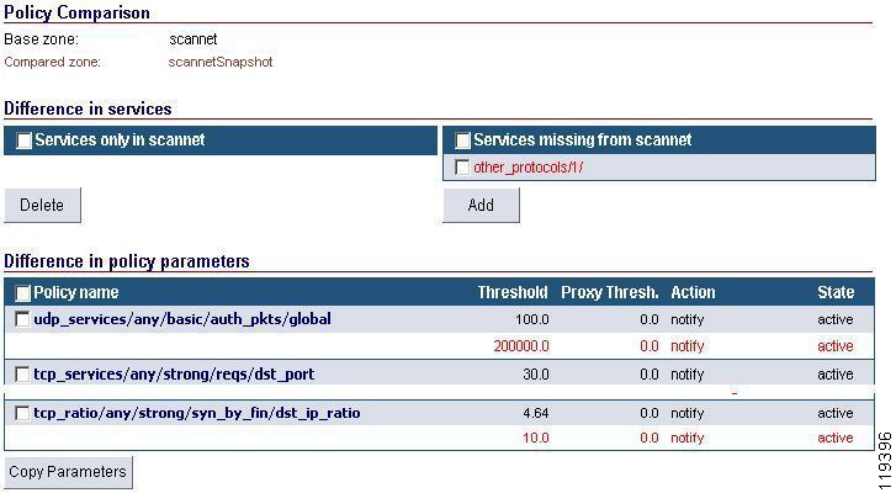
ステップ 3　次のいずれかのオプションを選択します。

- **OK**：2 つのゾーンのポリシーの設定を比較します。Policy Comparison 画面が表示され、サービスとポリシー パラメータの相違点が示されます（図 7-1 を参照）。

- **Cancel**：ゾーンのポリシーを比較せずに Policies Comparison クエリーを終了します。

図 7-1 に、ポリシー比較テーブルの例を示します。比較元のゾーンにのみ存在するポリシー設定アトリビュートは黒色で表示され、比較先のゾーンにのみ存在するアトリビュートは赤色で表示されます。

図 7-1　　ポリシー比較テーブル



Policy Comparison 画面は、次の 2 つのセクションに分かれています。

- **Difference in services**：このセクションの 2 つのテーブルには、次の情報が表示されます。
  - 比較元ゾーンのポリシーにのみ存在するサービス。
  - 比較元ゾーンに存在しないサービス。このリストに含まれているサービスは、比較先のゾーンにのみ定義されているサービスです。

（注）　Detector により、チェックボックスは、表示されたサービスの中で比較元ゾーンへの追加または削除が可能なものの横にのみ表示されます。タイプが **any** のサービスなど、表示されている一部のサービスはゾーン固有のサービスではないため、追加および削除できません。

- **Difference in policy parameters**：ポリシーの動作パラメータ（state、action、threshold、proxy-threshold）の相違点が表示されます。このテーブルの各セクションは、1 つのポリシーの中で見つかった相違点を示しています。各セクションの最初の行は、比較元ゾーンのパラメータを示します。各セクションの 2 行目は、比較先ゾーンのパラメータを示します。

比較元ゾーンからのサービスの削除

比較元ゾーンの設定からサービスを削除するには、次の手順を実行します。

ステップ 1　Services only in *ゾーン名*テーブルで、比較元ゾーンの設定から削除するサービスの隣にあるチェックボックスをオンにします。すべてのテーブル エントリを選択するには、テーブルのヘッダーにあるチェックボックスをオンにします。

ステップ 2　**Delete** をクリックします。Detector が、サービスを比較元ゾーンの設定から削除します。

比較元ゾーンへのサービスの追加

比較元ゾーンの設定にサービスを追加するには、次の手順を実行します。

ステップ 1　Services missing from *ゾーン名*テーブルで、比較元ゾーンの設定に追加するサービスの隣にあるチェックボックスをオンにします。すべてのテーブル エントリを選択するには、テーブルのヘッダーにあるチェックボックスをオンにします。

ステップ 2　**Add** をクリックします。Detector により、選択したサービスが比較元ゾーンのポリシーの設定に追加されます。

比較元ゾーンへのポリシー パラメータのコピー

ポリシーのパラメータを比較先ゾーンから比較元ゾーンにコピーするには、次の手順を実行します。

ステップ 1　Difference in policy parameters テーブルで、比較元ゾーンにコピーするポリシーの隣にあるチェックボックスをオンにします。比較元ゾーンのポリシーは黒色で示されます。比較先ゾーンのポリシーは赤色で示されます。すべてのテーブル エントリを選択するには、テーブルのヘッダーにあるチェックボックスをオンにします。

ステップ 2　**Copy Parameters** をクリックします。選択したポリシーが Detector によって比較先ゾーンから比較元ゾーンのポリシーの設定にコピーされます。選択したポリシーがテーブルから削除されます。