



ゾーントラフィックの ラーニング

この章では、Detector モジュール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 モジュール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の実行](#)
- [Detect and Learn を使用したラーニングプロセスの実行](#)
- [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](#)
- [ラーニングプロセスのスナップショットの管理](#)
- [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](#)

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 モジュールは、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 モジュール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 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、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](#)
- [Detect and Learn 機能について](#)
- [ラーニング プロセスの結果の管理](#)

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、Detector モジュールでユーザが個別に実行する次の2つのフェーズで構成されています。

1. **ポリシー構築フェーズ**: Detector モジュールがポリシー 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 モジュール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 モジュール ツールです。これらのテンプレートは、Detector モジュールが作成するゾーン 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 モジュールが詳細に監視するサービスの最大数、および Detector モジュール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** モジュール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** モジュールを通過できる値に設定されています。ゾーンを保護しているとき、**Detector** モジュール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** モジュールがポリシーのアクションで動的フィルタを作成します。

Detector モジュールがラーニングプロセスを使用する方法には、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** 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ている場合、**Detector** モジュールは、ワームポリシーを作成するとき、および作成する各ポリシーのしきい値を調整するときに、しきい値調整フェーズを使用します。

ラーニングプロセスを発生させるには、ゾーンに送信されたトラフィックをキャプチャし、そのコピーを **Detector** モジュールに送信するようにスイッチを設定する必要があります。

Detector モジュールのスナップショット機能を使用すれば、ラーニングプロセスのどちらのラーニングフェーズであっても、いつでも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ことにより、**Detector** モジュールがそのスナップショットの時点までに作成したポリシー情報を表示できます。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、この章で後述する「[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。

Detect and Learn 機能について

Detector モジュールがラーニングプロセスのポリシー構築フェーズを実行した後に、Detect and Learn 機能をアクティブにすることができます。Detect and Learn 機能により、Detector モジュールは、しきい値調整フェーズを実行 (Learn) しながら、同時にトラフィックの異常を検出 (Detect) できます。Detector モジュールは、ゾーンで攻撃を検出すると、ラーニングプロセスを一時停止します。Detector モジュールは、攻撃の終了を判断した後、ラーニングプロセスを再開します。Protect and Learn 機能を使用すると、Detector モジュールはゾーントラフィックの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 モジュール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を防止します。

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。ラーニングプロセス中、Detector モジュールはゾーン設定のポリシーを変更しません。ユーザがラーニングフェーズの結果を受け入れた場合のみ、Detector モジュールはゾーン設定をアップデートし、新しいポリシーまたはポリシーしきい値による動作を開始します。

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 トラフィックが通常状態である（攻撃を受けていない）：この場合、**Detector** モジュールが **DDoS** 攻撃のトラフィックの特性に基づい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** モジュール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** モジュール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 トラフィックの量がピークに達している：この場合、**Detector** モジュールは、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し、通常のトラフィックのピークが攻撃として認識されないようにすることができます。

この項では、次の手順について説明します。

- [ポリシー構築フェーズの開始](#)
- [ポリシー構築フェーズの現在の結果の受け入れ](#)
- [ポリシー構築フェーズの停止](#)
- [しきい値調整フェーズの開始](#)
- [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停止](#)

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 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
モジュールは、トラフィック フローで使用されているサービスに対するゾーン
トラフィックのコピーの分析を開始し、検出するサービスのポリシーを作成しま
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](#)」を参照してください。



(注)

ゾーンの設定で worm_tcp ポリシー テンプレートを使用している場合、Detector
モジュールは、ワーム ポリシーを作成するとき、および作成する各ポリシーの
しきい値を調整するときに、しきい値調整フェーズを使用します（「[しきい値調](#)

[整フェーズの開始](#)」の項を参照)。

Detector モジュールが十分時間を費やして、通常のゾーントラフィックの正確な状態を受信し、分析できるように、ポリシー構築フェーズは少なくとも2時間実行した後で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 モジュール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 モジュールは、ゾーン設定の現在のポリシーをすべて削除し、提案されたゾーンポリシーに置き換えます。Detector モジュールは、ポリシー構築フェーズを停止せず、ゾーン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。

■ ラーニングプロセスの実行

- **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** モジュール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** モジュールは、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の **Accept** 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。

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 モジュールは、ゾーントラフィックの分析を開始し、トラフィックフローの特性に合わせてゾーンポリシーのしきい値を調整します。

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 モジュールが十分時間を費やして、通常のゾーントラフィックの正確な状態を受信し、分析できるように、しきい値調整フェーズは少なくとも 24 時間実行した後で終了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 モジュール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	<p>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。</p> <ul style="list-style-type: none"> • Accept new thresholds : Detector モジュールは、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 モジュールは、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 モジュールは、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。 $\text{新しいしきい値} = (\text{ラーニングしたしきい値} * \text{重み} + \text{現在のしきい値} * (100 - \text{重み})) / 100$ Weight フィールドに重み値を入力します。 • Keep current thresholds : Detector モジュールは、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	<p>Detector モジュール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 モジュールが使用する重み値を入力します。</p> $\text{新しいしきい値} = (\text{ラーニングしたしきい値} * \text{重み} + \text{現在のしきい値} * (100 - \text{重み})) / 100$

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 モジュールは、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、ポリシー構築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	<p>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。</p> <ul style="list-style-type: none"> • Accept new thresholds : Detector モジュールは、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 モジュールは、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 モジュールは、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。 $\text{新しいしきい値} = (\text{ラーニングしたしきい値} * \text{重み} + \text{現在のしきい値} * (100 - \text{重み})) / 100$ Weight フィールドに重み値を入力します。 • Keep current thresholds : Detector モジュールは、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	<p>Detector モジュール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 モジュールが使用する重み値を入力します。</p> $\text{新しいしきい値} = (\text{ラーニングしたしきい値} * \text{重み} + \text{現在のしきい値} * (100 - \text{重み})) / 100$

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 モジュールは、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 動作の管理方法について説明します。Detect and Learn 動作では、Detector モジュールはゾーントラフィックに異常がないかを検出しながら、ゾーントラフィックをラーニングしてポリシー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 モジュールがラーニングプロセスの結果を受け入れるタイミングと方法を設定できます。Detector モジュールは、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](#)
- [Detect and Learn のアクティブ化](#)
- [Detect and Learn の非アクティブ化](#)

自動ラーニングのパラメータの設定

自動ラーニングパラメータを設定することにより、Detect and Learn をアクティブにする場合に、Detector モジュールが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タイミングと方法を制御できます。

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 モジュールは、ゾーントラフィックの異常を検出するためにそのポリシーをすぐに使用できます。このオプションを選択解除すると、ポリシーが未調整としてマークされ、ユーザは Detector モジュールがゾーントラフィックの異常を検出する前に、しきい値調整フェーズの結果を受け入れる必要があります。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	<p>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。</p> <ul style="list-style-type: none"> • Learning cycle : Detector モジュール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 モジュール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。 <ul style="list-style-type: none"> – Automatic accept : 指定した間隔で、Detector モジュールが提案するラーニングプロセスの結果（ポリシーのしきい値）を受け入れます。Detector モジュール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 モジュールは新しいポリシーを受け入れず、ゾーン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	<p>受け入れるしきい値を選択するために Detector モジュール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。</p> <ul style="list-style-type: none"> • 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	<p>Detector モジュール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 モジュールが使用する重み値を入力します。</p> <p>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</p>

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** モジュールは、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 モジュールは、ゾーントラフィックをラーニングして、ポリシーしきい値を調整する一方で、ゾーントラフィックの異常を検出できます。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 モジュール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 モジュールは攻撃を検出し、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 モジュールは、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 モジュールは、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 モジュールは、しきい値の選択方法 **Accept new thresholds** をアクティブにします (P.7-14 の「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 モジュールがトラフィックフローの分析を開始して、トラフィックの異常を検出します。

■ Detect and Learn を使用したラーニング プロセスの実行

- **Detector** モジュールがラーニング 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** リストにゾーン名が追加され、**Recent Events** テーブルには、検出が実行されてい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

Detect and Learn を非アクティブにする場合、Detector モジュールでは、ゾーンの異常検出とラーニングの両方、またはこの 2 つの動作のいずれかだけ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** : ゾーンの異常検出を停止します。
- **Stop Learning** : ラーニング プロセスの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	<p>受け入れるしきい値を選択するために Detector モジュール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。</p> <ul style="list-style-type: none"> • 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。 $\text{新しいしきい値} = (\text{ラーニングしたしきい値} * \text{重み} + \text{現在のしきい値} * (100 - \text{重み})) / 100$ 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	<p>Detector モジュール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 モジュールが使用する重み値を入力します。</p> $\text{新しいしきい値} = (\text{ラーニングしたしきい値} * \text{重み} + \text{現在のしきい値} * (100 - \text{重み})) / 100$

■ Detect and Learn を使用したラーニング プロセスの実行

ナビゲーション ペインの Protected Zones リストからゾーン名が削除され、Recent Events テーブルには、検出が停止されているゾーンの詳細なリストとともに、検出停止のイベント 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 モジュールは、次の条件に応じて、ゾーン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 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 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、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わせて個別に調整されています。

ゾーンに対して Detect 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 モジュールは、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 モジュールは、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](#)」の項を参照）。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 モジュールは、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 モジュール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。

■ 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

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 モジュール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 モジュールは現在のポリシーのしきい値を監視できず、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。チェックボックスがオンにされると、Detector モジュール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。チェックボックスがオフにされると、Detector モジュールはポリシーを未調整としてマークし、Detector モジュールはそのポリシーをゾーントラフィックの異常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 モジュールが、調整状態の設定をゾーンの設定に保存します。
 - **Clear** : Detector モジュール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 モジュール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 モジュールは、スナップショットの情報を記録し、スナップショットに連続した ID 番号を割り当てながら、ラーニングフェーズを続行します。

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](#)
- [現在のゾーンのポリシーのスナップショット取得](#)
- [スナップショットの表示](#)
- [スナップショットのポリシーの設定の修正](#)
- [スナップショットの削除](#)

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 モジュール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 モジュール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 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。

現在のゾーンの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、ゾーンの異常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 モジュール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 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。
-

スナップショットの表示

スナップショットを表示すると、ゾーンのラーニング結果を包括的に把握できます。

スナップショットの結果を表示するには、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 **Learning > Snapshot List** を選択します。Snapshot List テーブルが表示されます。

表 7-5 に、Snapshot List テーブルに含まれているフィールドの説明を示します。

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 モジュールが記録したポリシーが示されます。

表 7-5 Snapshot List テーブルのフィールドの説明

パラメータ	説明
ID	スナップショットの識別番号。
Name	スナップショットの名前。Detector モジュールは、自動的に取得された名前のないスナップショットを表示（自動）します。
Creation Time	スナップショットを取得した日時。
Snapshot Type	スナップショットの取得に使用された方法。次の種類のいずれかです。 <ul style="list-style-type: none">• Manual : ユーザのアクションでスナップショットが開始された。• Periodic : Detector モジュールによって、スナップショットはラーニング パラメータの設定に基づいて自動で取得された（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）。• Automatic : Detector モジュールによって、ラーニングプロセスがアクティブになった時点で自動的にスナップショットが取得された。このスナップショットは、ゾーンが攻撃を受けるなど、ただちに必要になった場合にバックアップとして使用できます。

表 7-5 Snapshot List テーブルのフィールドの説明 (続き)

パラメータ	説明
Operation	<p>スナップショットが取得されたときのゾーンの動作モードです。動作モードは次のいずれかです。</p> <ul style="list-style-type: none"> • Threshold Tuning : ラーニング プロセスのしきい値調整フェーズ。 • Policy Construction : ラーニング プロセスのポリシー構築フェーズ。 • N/A : ゾーンはラーニング プロセスを実行していません。
Accept Method	<p>しきい値を受け入れるために使用された方法。次の方法のいずれかです。</p> <ul style="list-style-type: none"> • Accept new thresholds : 新しいしきい値を受け入れます。 • 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。 • Accept weighted thresholds : 新しいしきい値、現在のしきい値、および定義した重み値に基づいてポリシーのしきい値を計算して保存します。 • Accept current : 現在のしきい値を変更せずに保存します。

スナップショットのポリシーの設定の修正

スナップショットを使用すると、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ポリシーの設定を修正するには、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 > Snapshot List** を選択します。Snapshot List テーブルが表示されます。
 - ステップ 3** テーブル内でスナップショットのフィールドのいずれかをクリックして、設定するスナップショットを表示します。Policies 画面が表示され、スナップショットの時点で **Detector** モジュールが記録したポリシーが示されます。
 - ステップ 4** 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。
 - ステップ 5** (オプション) 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。
 - ステップ 6** (オプション) 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 7** **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。

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 モジュールは、ポリシーの設定のサービス、ポリシー、およびポリシーしきい値の相違点をトレースします。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](#)
- [比較元ゾーンからのサービスの削除](#)
- [比較元ゾーンへのサービスの追加](#)
- [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 モジュール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 クエリー画面が表示されます。

■ 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

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 7-6 に、Policies Comparison クエリーのパラメータの説明を示します。

表 7-6 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 モジュールは、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。デフォルトのパーセンテージは100%で、Detector モジュールはいずれかのポリシーしきい値が他の値の少なくとも2倍以上のポリシーだけを表示します。

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

Base zone: scannet
Compared zone: scannetSnapshot

Difference in services

Services only in scannet	Services missing from scannet
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/> other_protocols/1/

Delete Add

Difference in policy parameters

Policy name	Threshold	Proxy Thresh.	Action	State
<input type="checkbox"/> udp_services/any/basic/auth_pkts/global	100.0	0.0	notify	active
<input type="checkbox"/>	200000.0	0.0	notify	active
<input type="checkbox"/> tcp_services/any/strong/reqs/dst_port	30.0	0.0	notify	active
<input type="checkbox"/>	4.64	0.0	notify	active
<input type="checkbox"/> tcp_ratio/any/strong/syn_by_fin/dst_ip_ratio	10.0	0.0	notify	active

Copy Parameters

113396

■ 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

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 モジュールは、サービスのうち、比較元ゾーンに対する追加または削除が可能なサービスの隣にのみチェックボックスを表示します。タイプが **any** のサービスなど、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 モジュールによってサービスが比較元ゾーンの設定から削除されます。
-

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。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** モジュール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。
-

■ 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