CHAPTER 7

ゾーン トラフィックのラーニング

この章では、Cisco Traffic Anomaly Detector Module（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、ゾーン異常の検出に Detector モジュールが使用するポリシーを作成および調整する方法について説明します。

ここでは、Detector モジュールの付属製品である Cisco Guard（Guard）について説明します。Guard は Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃を検出および軽減するデバイスです。攻撃トラフィックをドロップし、正当なトラフィックをネットワークに再注入することで、トラフィックがゾーンを通過するときにゾーン トラフィックをクリーニングします。Detector モジュールは、ゾーンが攻撃を受けていると判断したときに、Guard の攻撃軽減サービスをアクティブにすることができます。また、Detector モジュールはゾーンの設定を Guard と同期させることもできます。Guard の詳細については、『*Cisco Anomaly Guard Module Configuration Guide*』または『*Cisco Guard Configuration Guide*』を参照してください。

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、正常なゾーン トラフィック パターンのベースラインを作成します。ベースラインの参照ポイントは、ゾーンのポリシーです。ゾーンのポリシーによって、Detector モジュールは、ゾーン トラフィックに異常が存在する状況を特定できます。

ラーニング プロセスを使用すると、次の方法でゾーン異常の検出を最適化できます。

- ゾーン トラフィックのサービスに基づいてポリシーを作成する。
- ゾーン テンプレートのデフォルトの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しきい値を調整する。
- 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 プロセスは、トラフィックのピーク時、およびゾーンに対する攻撃が存在しないと確信できるときにアクティブにします。ラーニング プロセス中、Detector モジュールは、トラフィック サービスに基づいてゾーンのポリシーを構築し、トラフィック レートに基づいて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 プロセスの現在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、次の内容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ています。

- **ポリシー構築フェーズ**：Detector モジュールがゾーン トラフィックを分析して、ゾーンが使用するサービスを特定します。その後、Detector モジュールは、各サービス用のポリシー テンプレートを使用して、ゾーンのポリシーを作成します。ポリシー テンプレートによって、新しいポリシーのそれぞれに割り当てられるデフォルトのしきい値とポリシー アクションが決まります。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、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。ポリシー テンプレートの変更については、第 6 章「ポリシー テンプレートの設定」を参照してください。

  （注）　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。

- **しきい値調整フェーズ**：Detector モジュールがゾーン ポリシーのトラフィック レートしきい値を調整します。このしきい値は、通常のトラフィックが、ポリシー アクションをアクティブにすることなく Detector モジュールが分析できる値に設定されます。ゾーン トラフィックの異常を検出しているとき、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、トラフィックが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。

（注）　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、ポリシーの構築、およびしきい値の調整のどちらにも、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。

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。Detect and Learn がアクティブである場合、Detector モジュールは、通常のゾーン 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 プロセスを停止して、悪意のあるトラフィックのしきい値をラーニングしないよう防止します。

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、そのラーニング 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。現在の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 モジュールは、ラーニング プロセスのどちらのフェーズ中も、ラーニング フェーズの結果が受け入れられるまで、ゾーン設定のポリシーを変更しません。受け入れられた時点で、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で動作を開始します。

また、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 フェーズであっても、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では、現在のゾーン設定に影響を及ぼすことなく、スナップショットの時点までに Detector モジュールが作成したポリシー情報を保存および表示できます。スナップショットは必要に応じていくつでも取得でき、スナップショットに保存したポリシー情報を使用して、ゾーンの設定をいつでもアップデートできます。スナップショットを使用する方法の詳細については、「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。

ラーニング プロセスの実行

この項では、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のベースラインとして保存します。この場合、Detector モジュールが以降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　トラフィックがピーク量にある：Detector　モジュールはポリシーのしきい値を通常のピーク量のトラフィックに適した値に設定できるため、Detector モジュールでは通常のピーク量のトラフィック状態が攻撃と見なされないことが保証されます。

この項は、次の内容で構成されています。

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アクティブにできます。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 時間実行した後で終了することをお勧めします。

（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。

（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）。

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アクティブにして各ポリシーしきい値を調整します。

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 メニューで **Learning > Construct Policies** を選択します。

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。

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。Detector モジュールは、ポリシー構築フェーズの結果が受け入れられるまで、ゾーン設定の現在のポリシーを新しいポリシーで置き換えません（「ポリシー構築フェーズの現在の結果の受け入れ」の項を参照）。

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。スナップショットを保存しても、現在のゾーン設定は変更されません。スナップショットを使用する方法の詳細については、「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。

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 メニューで **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に、引き続きゾーンのサービスをラーニングします。

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 メニューで **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 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た後で、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 レートに合せて個別に設定されます。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。詳細については、「しきい値調整フェーズの開始」の項を参照してください。

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アクティブにできます。

（注） Detector モジュールが十分な時間をかけて通常のゾーン トラフィックを正確に受信および分析できるようにするには、少なくとも 24 時間実行した後でしきい値調整フェーズを終了することをお勧めします。

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 メニューで **Learning > Tune Threshold** を選択します。

ラーニングを示すゾーンのステータス 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。

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 フローの特性に合せて、ゾーン ポリシーのしきい値を調整します。Detector モジュールは、しきい値調整フェーズの結果が受け入れられるまで、ゾーン設定に対する変更を保存しません（「しきい値調整フェーズの現在の結果の受け入れ」の項を参照）。

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しきい値を保存し、確認します。スナップショットを保存しても、現在のゾーン設定は変更されません。

スナップショット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。

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 メニューで **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：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とラーニングしたしきい値とを比較し、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。 • Keep current thresholds：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ます。ポリシーは、現在のしきい値を保持します。
Weight	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。このオプションは、Accept weighted thresholds という方法を選択した場合にだけアクティブになります。次の式に、Detector モジュールが使用する重み値を入力します。 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　モジュールは、しきい値調整フェーズの現在の結果でゾーン設定のポリシーをアップデートし、しきい値調整フェーズを続行します。
- **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 メニューで **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：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とラーニングしたしきい値とを比較し、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。 • Keep current thresholds：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ます。ポリシーは、現在のしきい値を保持します。
Weight	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。このオプションは、Accept weighted thresholds という方法を選択した場合にだけアクティブになります。次の式に、Detector モジュールが使用する重み値を入力します。 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　モジュールは、しきい値調整フェーズの現在の結果でゾーン設定のポリシーをアップデートし、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

この項では、Detect and Learn 動作を管理する方法について説明します。この動作状態では、Detector モジュールはゾーン トラフィックの異常を検出すると同時に、ゾーン 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。Detector モジュールは、ゾーンで攻撃を検出すると、ラーニング プロセスを停止します。

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。

この項は、次の内容で構成されています。

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ときにラーニング プロセス（しきい値調整フェーズ）の現在の結果を Detector モジュールが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 メニューで、**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 ポリシーを次のようにマークします。 • 調整済み：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。 • 未調整：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	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 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 ～ 1000 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。 — Automatic accept：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、指定した間隔で受け入れます。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、ゾーン設定内のポリシーのしきい値を変更しません。
Threshold selection method	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。 • 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とラーニングしたしきい値とを比較し、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 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。このオプションは、Accept weighted thresholds という方法を選択した場合にだけアクティブになります。次の式に、Detector モジュールが使用する重み値を入力します。 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 モジュールは自動ラーニングのパラメータをゾーン設定に保存します。
- **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初めて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（「自動ラーニングのパラメータの設定」の項を参照）。

ゾーンのポリシーしきい値が初めて受け入れられた後、Detector モジュールはポリシーを調整済みとしてマークします。その結果、ゾーン トラフィックをラーニングしながら攻撃を検出できるようになります。

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 メニューで **Learning > Tune Thresholds** を選択）とゾーン異常の検出（**Detect** をクリック）を個々にアクティブにすることもできます。これら 2 つの動作をアクティブにする順序は問いません。

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。
- Detector モジュールは、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 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、検出動作とラーニング動作のいずれかまたは両方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 メニューで **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。次のアクションのいずれかまたは両方を選択します。

- **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	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。 • 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とラーニングしたしきい値とを比較し、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。ポリシーは、しきい値調整フェーズ前の値を保持します。
Weight	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。このオプションは、Accept weighted thresholds という方法を選択した場合にだけアクティブになります。次の式に、Detector モジュールが使用する重み値を入力します。 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

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、*検出されないゾーン*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

ゾーン ポリシーの調整状態は、ポリシーのしきい値に関連します。Detector モジュールは、次の条件に応じて、ゾーン ポリシーを調整済みまたは未調整と見なします。

- 未調整：ゾーンのポリシーしきい値が、ゾーン トラフィックに適した値に設定されていない可能性があります。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：ゾーンのポリシーしきい値が、ゾーン　トラフィックに適した値に設定されています。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が未調整状態の場合、Detector モジュールは、しきい値調整フェーズの結果を初めて受け入れるまで、ゾーンに対する攻撃を検出できません。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、しきい値の選択方法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。
- すべてのポリシー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 Detect and Learn 機能を開始していないが、ピーク時のトラフィックを Detector モジュールがゾーンへの攻撃と見なさないよう防止する必要がある。

ゾーンを未調整としてマークすると、Detector モジュールは、トラフィックのポリシーしきい値違反を監視しないため、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 メニューで、**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。Detector モジュールがポリシーを調整済みとしてマークし、ただちにポリシーを使用してゾーン トラフィックの異常を検出できます。
- 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。Detector モジュールがポリシーを未調整としてマークします。この場合、Detector モジュールがポリシーを使用してゾーン トラフィックの異常を検出できるようにするには、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。

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 モジュールは調整状態の設定をゾーン設定に保存します。
- **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、次のタスク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、スナップショット情報を記録すると同時に、ラーニング フェーズを継続します。Detector モジュールがラーニング プロセスを実行していないときにスナップショットを保存して、現在のゾーン ポリシーのコピーを作成することもできます。

この項は、次の内容で構成されています。

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 メニューで **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。

ステップ 4　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とラーニングしたしきい値とを比較し、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。ポリシーは、しきい値調整フェーズ前の値を保持します。

ステップ 5　Accept weighted thresholds という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 6　**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。

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 メニューで **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。

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 メニューで **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　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て、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。

表 7-5　Snapshot List テーブルに含まれているフィールドの説明

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。自動的に取得された名前のないスナップショットの場合、Detector モジュールは (automatic) と表示します。
Creation Time	スナップショットが取得された日時。
Snapshot Type	スナップショットの取得に使用された方法。スナップショットのタイプは、次のとおりです。 • Manual：手動で取得された。 • Periodic：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の設定」の項を参照）に基づいて、Detector モジュールによって自動的に取得された。 • Automatic：ラーニング プロセスがアクティブになったときに Detector モジュールによって自動的に取得された。このスナップショットは、ゾーンが攻撃を受けている場合にバックアップとして使用できます。
Operation	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。動作モードは、次のいずれかです。 • 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：ラーニング プロセスのフェーズではありません。
Accept Method	しきい値の受け入れに使用された方法。この方法は、次のいずれかです。 • 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とラーニングしたしきい値とを比較し、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に基づいて、保存するポリシーのしきい値を計算します。 • 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して、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変更する。
- 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（「2 つのゾーンまたはスナップショットのポリシー設定の比較」の項を参照）。

スナップショットのポリシーを設定するには、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 メニューで **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　（オプション）**Configure Selection** をクリックして、1 つまたは複数のポリシーのパラメータを設定し直します。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）**Add service** をクリックして、サービスをポリシーに追加します。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）**Remove service** をクリックして、サービスをポリシーから削除します。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 メニューで **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 モジュールが、選択したスナップショットを Snapshot リストから削除します。

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、ポリシー設定サービス、ポリシー、およびポリシーのしきい値の相違点をトレースします。ポリシーの設定を比較する場合は、1 つのゾーンまたはスナップショットを*比較元ゾーン*として選択し、別のゾーンまたはスナップショットを*比較先ゾーン*として選択します。ポリシー設定のアトリビュートを比較元ゾーンから削除したり、そこに追加したりできます。比較元ゾーンの設定を変更することにより、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。

この項は、次の内容で構成されています。

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 モジュールの要約のメイン メニューで **Zones > Compare Zone policies** を選択します。
- ゾーンのメイン メニューで **Configuration > Policies > Compare Policies** を選択します。

Policies Comparison Query 画面が表示されます。

ステップ 2　比較元ゾーンと比較先ゾーンを定義します。

表 7-6 に、Policies Comparison Query 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。

表 7-6　ポリシー比較のパラメータ（続き）

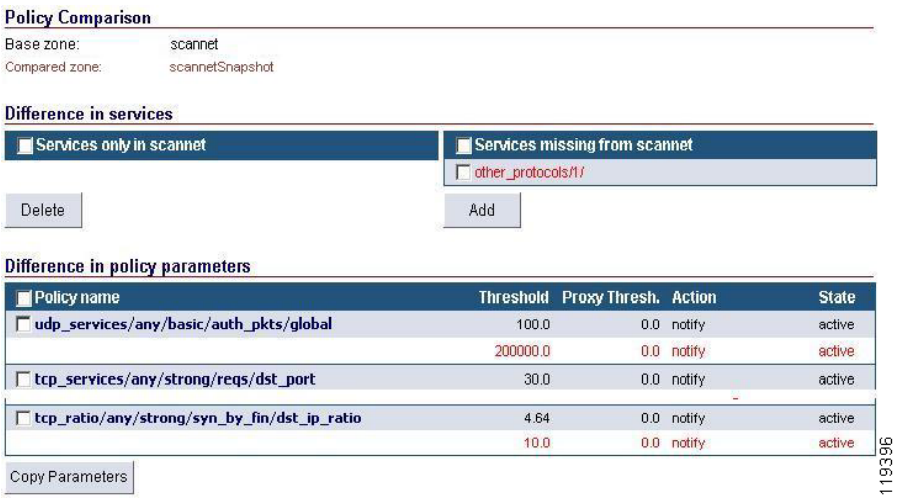
パラメータ 1	パラメータ 2	説明
Compared Zone	Zone	比較元ゾーンとの比較の対象になるゾーンまたはスナップショットの名前。比較先ゾーンの設定を変更することはできません。比較先となるゾーンをドロップダウン リストから選択します。
	Policy Configuration	選択した比較先ゾーンのポリシーの設定。デフォルト値は、ゾーンの現在のポリシーの設定です。ドロップダウン リストからゾーン ポリシーのスナップショットを選択できます。
Minimal difference		比較元ゾーンと比較先ゾーンにおけるポリシーの設定の相違点の割合。Detector モジュールは、2 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。デフォルトの割合は 100% です。この場合、Detector モジュールは、一方のしきい値が他方のしきい値よりも 2 倍以上大きい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、比較元ゾーンに追加できるサービスと、比較元ゾーンから削除できる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、追加または削除できません。

- Difference in policy parameters：ポリシーの動作パラメータ（state、action、threshold、proxy-threshold）の相違点を表示します。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 モジュールが、選択されたサービスを比較元ゾーンのポリシー設定に追加します。

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表示され、比較先ゾーンのポリシーは赤色で表示されます。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。