CHAPTER 8

ゾーン トラフィックの特性のラーニング

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 トラフィックの特性を分析し、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、ネットワーク上で現在攻撃が発生していないときに、通常のトラフィック 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 トラフィック内における異常の存在を検出するための参照ポイントとして使用します。これらの参照ポイントを*ポリシー*といいます。

ポリシーを構築する最初のラーニング プロセスが終了したら、ラーニング プロセスとゾーン異常検出を同時にアクティブにできます。Detector モジュールは、ポリシーのしきい値を調整するとともに、トラフィックに異常がないかどうかについて、ポリシーのしきい値を監視します。このプロセスでは、Detector モジュールがゾーンのトラフィック特性に応じてポリシーのしきい値を常にアップデートしながら、ゾーン トラフィックの異常を検出でき、Detector モジュールで悪意のあるトラフィックのしきい値がラーニングされません。

ラーニング プロセスを実行するには、ゾーンに送信されるトラフィックをキャプチャし、そのコピーを Detector モジュールに渡すようにスイッチを設定する必要があります。詳細については、P.2-6 の「トラフィックをキャプチャするためのトラフィックの送信元の設定」を参照してください。

複数のゾーンに対して同時に **learning** 関連のコマンドを入力できます。これには、グローバル モードで、ワイルドカードにアスタリスク（*）を使用してコマンドを発行します。たとえば、すべてのゾーンについてポリシー構築フェーズを開始する場合は、グローバル モードで **learning policy-construction *** コマンドを入力します。*scan* で始まる名前を持つ Detector モジュールのすべてのゾーン（scannet や scanserver など）のポリシー構築フェーズの結果を受け入れるには、グローバル モードで **no learning** *scan**** **accept** コマンドを入力します。

この項では、次のトピックについて取り上げます。

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 : Detector モジュールはポリシー テンプレートを使用してゾーン ポリシーを作成します。トラフィックは Detector モジュールを通過し、ゾーンによって使用される主なサービスを検出できます。既存のポリシーが新しいポリシーで上書きされます。

  ポリシー テンプレートは、Detector モジュールのポリシー構築用ツールです。このテンプレートは、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。また、ポリシー テンプレートは、Detector モジュールが厳密に監視するサービスの最大数と、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 テンプレート パラメータを変更してから、ポリシー構築フェーズを開始する必要があります。詳細については、第 7 章「ポリシー テンプレートとポリシーの設定」を参照してください。

  GUARD_LINK ゾーン テンプレートまたは DETECTOR_LINK ゾーン テンプレートを使用して作成されたゾーンに対してポリシー構築フェーズを実行することはできません。

- しきい値調整 : Detector モジュールは、ゾーン サービスのトラフィック レートに合せて、ポリシー構築フェーズ中に構築されたポリシーを調整します。トラフィックは Detector モジュールを通過し、ゾーン ポリシーの構築中に検出されたサービスのしきい値を調整できます。既存のしきい値が新しいしきい値で上書きされます。

  しきい値調整フェーズとゾーン異常検出を同時にアクティブにすると（検出およびラーニング機能）、Detector モジュールで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できます。Detector モジュールが常にゾーン ポリシーを調整するように設定し、Detector モジュールがポリシーのしきい値を更新するときの間隔を定義することができます。

Detector モジュールは、ゾーンのトラフィックの特性をラーニングして、ゾーンのトラフィックを比較するベースラインを作成し、悪意の攻撃となる可能性のある異常をすべてトレースします。Detector モジュールは、ラーニング プロセスの間は、現在のゾーン ポリシーを変更しません。ラーニング フェーズの結果の 1 つを受け入れると決めたときに限り、ポリシーを更新します。ポリシーが作成された後は、ポリシーを追加または削除できます。また、しきい値、サービス、タイムアウト、アクションなどのポリシー パラメータを変更することもできます。

Detector モジュールは、ポリシー構築フェーズ中ではなく、しきい値調整フェーズ中にワーム ポリシーの新しいサービスをラーニングします。そのため、しきい値調整フェーズ中に、ワーム ポリシーに追加された新しいサービス（ポート）が表示される場合があります。

ラーニング プロセスの結果の確認

ラーニング プロセス中のどの段階でも、任意のラーニング フェーズの現在の結果を保存して、後で **snapshot** コマンドを使用して確認できます。ラーニング プロセスのスナップショットを保存することで、スナップショットのポイントまでに Detector モジュールが作成したポリシー情報を表示し、ラーニング プロセスの結果を受け入れるかどうかを判断できます。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、ゾーン設定には影響はありません。スナップショット内のポリシー情報を使用してゾーン設定をアップデートできます。

検出およびラーニング機能について

ポリシーを構築する最初のラーニング プロセスが終了したら、ラーニング プロセスをアクティブにし、検出およびラーニング機能を使用して、同時にゾーン異常検出をイネーブルにできます。Detector モジュールは、ポリシーのしきい値を調整するとともに、トラフィックに異常がないかどうかについて、ポリシーのしきい値を監視します。検出およびラーニング機能により、ポリシーのしきい値をゾーンのトラフィック特性に基づいて常にアップデートしながら、Detector モジュールでゾーン トラフィックの異常検出を実行できるようになるため、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がなくなります。

保護およびラーニング機能をアクティブにする前に、ラーニング パラメータを設定することで、Detector モジュールがラーニング プロセスの結果をいつ、どのように受け入れるかを設定できます。

詳細については、P.8-20 の「ゾーンのポリシーのしきい値調整とゾーン異常検出のイネーブル化の同時実行」を参照してください。

ゾーンのラーニング プロセスの結果と Cisco Anomaly Guard Module の同期

Detector モジュールは、ゾーン上で攻撃を検出すると、ラーニング プロセスを停止し、関連付けられているすべての Guard をアクティブ化してゾーンを保護します。その後、攻撃が終了すると、ゾーン トラフィックのラーニングを再開します。このプロセスにより、トラフィックに対するゾーンのポリシーのしきい値を継続的に調整できる一方で、ゾーンのトラフィックが常に Guard モジュールに宛先変更されることがなくなります。Detector モジュールがゾーンのトラフィックを常にラーニングして、ゾーンのポリシーで Guard モジュールをアップデートするように設定できます。

ラーニング プロセスの結果を Guard モジュールと同期させるには、次の作業を実施する必要があります。

1. Guard モジュールを Detector モジュール上のリモート Guard リストに追加して、通信方法を Secure Sockets Layer（SSL）として定義します。P.9-8 の「リモート Guard リストを使用したリモート Guard のアクティブ化」を参照してください。
2. Guard モジュールとの SSL 通信チャネルを確立します。P.4-29 の「SSL 通信チャネルの設定」を参照してください。
3. Detector モジュール上で Guard ゾーン テンプレートを使用してゾーンを作成します。P.5-7 の「ゾーン テンプレートからの新しいゾーンの作成」を参照してください。
4. ゾーンの検出およびラーニング機能をアクティブにします。P.8-20 の「ゾーンのポリシーのしきい値調整とゾーン異常検出のイネーブル化の同時実行」を参照してください。

ゾーン設定を Guard モジュールと手動で同期させることも、ゾーン設定を自動的に Guard モジュールと同期させるように Detector モジュールを設定することもできます。詳細については、P.5-15 の「Detector モジュールの Guard とのゾーン設定の同期」を参照してください。

ポリシーの構築

ポリシー構築フェーズは、新しいゾーンを作成した後や、ゾーン設定が新しいサービス ポリシーを使用してアップデートを行う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、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調整します。

ポリシー構築フェーズでは、Detector モジュールはポリシー テンプレートを使用してゾーン ポリシーを作成します。トラフィックが Detector モジュールを通過し、ゾーンによって使用される主なサービス（ポートとプロトコル）を検出できます。ポリシー構築の規則を設定することもできます。たとえば、Detector モジュールで特定のタイプのポリシーが作成されないようにするには、関連するポリシー テンプレートをディセーブルにします。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 テンプレート パラメータを変更してから、ポリシー構築フェーズを開始する必要があります。詳細については、P.7-5 の「ポリシー テンプレートについて」を参照してください。

Detector モジュールは、ポリシー パラメータ（タイムアウト、アクション、およびしきい値）のデフォルト値を設定します。動作パラメータのデフォルト値の設定方法については、第 7 章「ポリシー テンプレートとポリシーの設定」を参照してください。

このフェーズで Detector モジュールが作成する新しいポリシーは、既存のポリシーに置き換えられます。

（注） 帯域幅限定リンク ゾーン テンプレート（DETECTOR_LINK_128K、DETECTOR_LINK_1M、DETECTOR_LINK_4M、GUARD_LINK_512K、および GUARD_LINK_128K、GUARD_LINK_1M、GUARD_LINK_4M、GUARD_LINK_512K）に基づくゾーンに対しては、ポリシー構築フェーズを実行できません。

ポリシー構築フェーズをアクティブ化する前に、ゾーン上に攻撃がないことを確認してください。これによって、Detector モジュールが、Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃のトラフィック特性に基づいてポリシーを構築することを回避できます。Detector モジュールが DDoS 攻撃のトラフィック特性をラーニングし、攻撃の結果をベースラインとして保存できるようにすると、攻撃を通常のトラフィックの状態と見なすため、Detector モジュールはその後に発生する攻撃を検出できなくなる場合があります。

ゾーン ポリシーを構築するには、次の手順を実行します。

ステップ 1　ゾーン設定モードで次のコマンドを入力することで、ポリシー構築フェーズを実行できます。

```
learning policy-construction
```

ステップ 2　Detector　モジュールがゾーンのトラフィックのコピーを受信していることを確認してください。

ポリシー構築またはしきい値調整を開始してから少なくとも 10 秒待ってから、**show rates** コマンドを発行します。*Received traffic* レートの値がゼロより大きいことを確認します。値がゼロの場合は、Detector モジュールがゾーンのトラフィックのコピーを受信していないことを示します。トラフィックの送信元が、トラフィックのキャプチャについて設定されていることを確認します。詳細については、P.2-6 の「トラフィックをキャプチャするためのトラフィックの送信元の設定」を参照してください。

ステップ 3　（オプション）Detector モジュールが構築中のポリシーを表示します。

ポリシー構築フェーズの任意の段階で **snapshot** コマンドを使用して、ラーニング パラメータ（サービス、しきい値、およびポリシー関連のその他のデータ）のスナップショットを保存しておいて、後で確認することができます。単一のスナップショットを保存するか、定期的なスナップショットを（指定した間隔で）保存することができます。

詳細については、P.7-44 の「ポリシー設定のバックアップ」を参照してください。

ステップ 4　（オプション）ポリシー構築フェーズを長期間実行する場合、ポリシー構築フェーズを停止しなくても、Detector モジュールによって提案されたポリシーを受け入れることができます。ポリシーを 1 回受け入れるか、提案されたポリシーを Detector モジュールが指定された間隔で自動的に受け入れるように定義できます。これでゾーンが最新のポリシーを持つだけでなく、継続してゾーンのトラフィックをラーニングすることを保証できます。

Detector モジュールによって提案されたポリシーを受け入れ、ポリシー構築フェーズを継続するには、次のコマンドを使用します。

```
learning accept
```

Detector モジュールによって提案されたポリシーを指定した間隔で自動的に受け入れるには、次のコマンドを入力します。

learning-params periodic-action auto-accept *learn_params_days learn_params_hours learn_params_minutes*

詳細については、P.8-15 の「ラーニング パラメータの設定」を参照してください。

定期的なアクションを終了するには、**no learning-params periodic-action** コマンドを使用します。

ステップ 5　十分に時間をおいてからポリシー構築フェーズを終了し、新しく構築されたポリシーの取り扱いを決定します。

（注）　ゾーンが使用する主なサービス（ポートおよびプロトコル）を Detector モジュールが検出するための十分な時間を確保するために、ポリシー構築フェーズを少なくとも 2 時間継続することをお勧めします。

次のアクションのいずれかを行うことができます。

- 提案されたポリシーの受け入れ：Detector モジュールによって提案されたポリシーを受け入れるには、ゾーン設定モードで次のコマンドを入力します。

  ```
  no learning accept
  ```

Detector モジュールは、以前にラーニングしたポリシーとしきい値を消去します。

新しく構築されたポリシーを受け入れた後は、手動でポリシーを追加または削除できます。詳細については、第 7 章「ポリシー テンプレートとポリシーの設定」を参照してください。

- 提案されたポリシーの拒否：Detector　モジュールによって提案されたポリシーを拒否するには、ゾーン設定モードで次のコマンドを入力します。

  no learning reject

  Detector モジュールはプロセスを停止し、ラーニングした新しいポリシーを保存しません。ゾーンのポリシーは、Detector モジュールがラーニング プロセスを開始する前か、ポリシー構築フェーズの結果を最後に受け入れる前のポリシーになります。

次の例は、ポリシー構築フェーズを開始し、提案されたポリシーを 12 時間間隔で受け入れる方法を示しています。さらに、ポリシー構築フェーズを停止し、提案されたポリシーを受け入れる方法も示しています。

```
user@DETECTOR-conf-zone-scannet# learning policy-construction
user@DETECTOR-conf-zone-scannet# learning-params periodic-action
auto-accept 0 12 0
user@DETECTOR-conf-zone-scannet# no learning accept
```

ポリシーしきい値の調整

しきい値調整フェーズでは、Detector モジュールがゾーンのトラフィックを分析し、ポリシー構築フェーズで構築されたポリシーのしきい値を定義します。

Detector モジュールが、最後に受け入れられたポリシーしきい値を監視してトラフィックの異常を探しながら、ゾーンのトラフィックをラーニングするように設定できます。Detector モジュールは、ゾーンに対する攻撃を検出した後、しきい値調整フェーズを停止しますが、ゾーン異常検出を継続することで、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がなくなります。

攻撃が終了すると、Detector モジュールはラーニング プロセスを再開します。

ポリシーのしきい値を調整するには、次の手順を実行します。

ステップ 1　ゾーン設定モードで次のコマンドを入力することで、しきい値調整フェーズを実行できます。

```
detect learning
```

（注）　検出およびラーニング機能をイネーブルにすること、つまり、しきい値調整フェーズをアクティブにすると同時に Detector モジュールがゾーンを異常検出するように設定することをお勧めします。

すでにゾーン異常検出またはラーニング プロセスのしきい値調整フェーズをアクティブにしている場合、**learning threshold-tuning** コマンドと **detect** コマンド（順序は問いません）の両方を入力して、検出およびラーニング機能をアクティブにします。

Detector モジュールは、ゾーンに対する攻撃を検出した場合はしきい値調整フェーズを停止しますが、ゾーン検出は継続します。

（注）　ゾーン宛てのトラフィックが通常の量のときに、検出およびラーニング機能をアクティブにした場合、Detector モジュールは、ピーク時のトラフィックを攻撃と見なす可能性があります。このような場合は、次のいずれかを行うことができます。

- ゾーン設定モードで **learning-params threshold-tuned** コマンドを入力することで、ゾーン ポリシーしきい値の状態を未調整に設定できます。詳細については、P.8-18 の「ポリシーに対する調整済みのマーク付け」を参照してください。
- ゾーン設定モードで **no detect** コマンドを入力して、ゾーン異常検出を非アクティブにし、ゾーン ポリシーしきい値を継続してラーニングします。

ゾーン異常検出としきい値調整フェーズを同時に非アクティブにするには、ゾーン設定モードで **deactivate** コマンドを使用します。

しきい値調整フェーズだけをアクティブにするには、**learning threshold-tuning** コマンドを使用します。

ステップ 2　Detector　モジュールがゾーンのトラフィックのコピーを受信していることを確認してください。

ポリシー構築フェーズまたはしきい値調整フェーズを開始してから少なくとも 10 秒待ってから、**show rates** コマンドを発行します。*Received traffic* レートの値がゼロより大きいことを確認します。値がゼロの場合は、Detector モジュールがゾーンのトラフィックのコピーを受信していないことを示します。トラフィックの送信元が、トラフィックのキャプチャについて設定されていることを確認します。詳細については、P.2-6 の「トラフィックをキャプチャするためのトラフィックの送信元の設定」を参照してください。

ステップ 3　（オプション）Detector モジュールが調整中のゾーン ポリシーを表示します。

しきい値調整フェーズの任意の段階で、**snapshot** コマンドを使用して、ラーニング パラメータ（サービス、しきい値、およびポリシー関連のその他のデータ）のスナップショットを保存できます。後でスナップショットを確認することや、

ラーニング パラメータを別のスナップショットと比較することができます。単一のスナップショットを保存するか、定期的なスナップショットを（指定した間隔で）保存することができます。

詳細については、P.7-44 の「ポリシー設定のバックアップ」を参照してください。

ステップ 4　ポリシーを受け入れます。

Detector モジュールが提案したゾーン ポリシーを受け入れ、しきい値の調整フェーズを継続するか、または Detector モジュールが自動的に提案したポリシーを指定した間隔で受け入れることを定義することで、ゾーンが最新のポリシーを持ち、ゾーンのトラフィックのラーニングを継続することが保証されます。

Detector モジュールによって提案されたポリシーを受け入れ、しきい値調整フェーズを継続するには、次のコマンドを使用します。

```
learning accept [threshold-selection {new-thresholds | max-thresholds
| weighted weight}]
```

threshold-selection の引数とキーワードについては、表 8-2 を参照してください。

Detector モジュールによって提案されたポリシーを指定した間隔で自動的に受け入れるには、次のコマンドを入力します。

```
learning-params periodic-action auto-accept learn_params_days
learn_params_hours learn_params_minutes
```

詳細については、P.8-15 の「ラーニング パラメータの設定」を参照してください。

定期的なアクションを終了するには、**no learning-params periodic-action** コマンドを使用します。

ステップ 5　十分な時間が経過してから、しきい値調整フェーズを終了し、新しく調整されたポリシーの処理方法を決定します。

（注）　しきい値調整フェーズをトラフィックのピーク時（1 日で最も忙しい部分）に、少なくとも 24 時間実行して、Detector モジュールがポリシーしきい値を正しく調整するために十分な時間を確保することをお勧めします。

（注） 検出機能とラーニング機能をイネーブルにし、しきい値調整フェーズを継続することをお勧めします。

次のアクションのいずれかを行うことができます。

- 提案されたポリシーの受け入れ：Detector モジュールによって提案されたポリシーのしきい値を受け入れるには、ゾーン設定モードで次のコマンドを入力します。

  no learning accept [**threshold-selection** {**new-thresholds** | **max-thresholds** | **weighted** *weight*}]

  threshold-selection の引数とキーワードについては、表 8-2 を参照してください。

  Detector モジュールは、以前にラーニングしたしきい値を消去します。

  新しく調整されたポリシーを受け入れた後は、手動でポリシーのパラメータを変更することができます。詳細については、第 7 章「ポリシー テンプレートとポリシーの設定」を参照してください。

- 提案されたポリシーの拒否：Detector　モジュールによって提案されたポリシーのしきい値を拒否するには、ゾーン設定モードで次のコマンドを入力します。

  no learning reject

  Detector モジュールはしきい値の調整を停止して、前のしきい値の状態に戻します。そのプロセスの結果、新しく構築されたゾーン ポリシーには、以前のトラフィック特性に基づいて取得したしきい値が使用される場合があります。

（注） 後でしきい値調整フェーズをイネーブルにするか、またはそのしきい値を手動で設定することをお勧めします。

次の例は、しきい値調整フェーズを開始し、提案されたポリシーを 1 時間間隔で受け入れる方法を示しています。Detector モジュールは、次に、しきい値調整フェーズを停止し、しきい値が現在の値よりも大きい場合に、提案されたポリシーを受け入れます（max-thresholds 方式）。

```
user@DETECTOR-conf-zone-scannet# learning threshold-tuning
user@DETECTOR-conf-zone-scannet# learning-params periodic-action
auto-accept 0 1 0
user@DETECTOR-conf-zone-scannet# no learning accept
threshold-selection max-thresholds
```

ラーニングの結果を表示するには、**show policies statistics** コマンドを使用します。詳細については、P.7-39 の「ポリシーの表示」を参照してください。

ラーニングしたしきい値を確認した後は、結果の一部を変更できます。この変更がその後のしきい値調整フェーズで上書きされないようにするには、次のタスクのいずれかを実行します。

- ポリシーのしきい値を固定値として設定する：Detector モジュールは新しいしきい値を無視し、現在のしきい値を保持します。詳細については、P.7-25 の「固定値としてのしきい値の設定」を参照してください。
- ポリシーの固定乗数を設定する：Detector モジュールが新しいポリシーのしきい値を計算する場合は、ラーニングしたしきい値に指定の乗数を掛け、その結果にしきい値選択方式を適用します。詳細については、P.7-26 の「しきい値の乗数の設定」を参照してください。

ラーニング パラメータの設定

ラーニング パラメータを使用すると、Detector モジュールで実行できるラーニング関連のアクションを設定し、指定したポリシーを Detector モジュールで処理する方法を定義できます。次のパラメータを定義できます。

- periodic-action：自動的にゾーン　ポリシーを受け入れ、指定した間隔でゾーン ポリシーのスナップショットを保存するように Detector モジュールを設定します。
- threshold-tuned：ゾーンのポリシーに調整済みのマークを付けます。ゾーンのポリシーが調整済みとしてマークされていない場合、Detector モジュールはゾーンに対する攻撃を検出しません。
- threshold-selection：Detector　モジュールがしきい値調整フェーズの結果を受け入れて新しいポリシーのしきい値を生成するときに使用される、デフォルトの方式を設定します。
- fixed-threshold：ポリシーのしきい値を固定値として設定するため、Detector モジュールは後続のしきい値調整フェーズで、ポリシーしきい値の値を変更しません。
- threshold-multiplier：ポリシーのしきい値の固定乗数を設定するので、Detector モジュールは後続のしきい値調製フェーズで新しいポリシーしきい値を計算します。

ラーニング パラメータの設定を表示するには、ゾーン設定モードで **show learning-params** コマンドを使用します。

この項では、次のトピックについて取り上げます。

- 定期的なアクションの設定
- しきい値選択方式の設定
- ポリシーに対する調整済みのマーク付け

定期的なアクションの設定

指定した間隔で次のいずれかのアクションを実行するように Detector モジュールを設定します。

- ゾーン　ポリシーを自動的に受け入れ、ポリシーのスナップショットを保存する
- ゾーン ポリシーのスナップショットだけを保存する

スナップショットの詳細については、P.7-39 の「ポリシーの監視」を参照してください。

Detector モジュールが実行する定期的なアクションを設定するには、ゾーン設定モードで次のコマンドを入力します。

learning-params periodic-action {**auto-accept** | **snapshot-only**}
learn_params_days learn_params_hours learn_params_minutes

表 8-1 に、**learning-params** コマンドの引数とキーワードを示します。

表 8-1　learning-params periodic-action コマンドの引数とキーワード

パラメータ	説明
auto-accept	Detector モジュールによって提案されたポリシーを、指定され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	指定された間隔でポリシーのスナップショットを保存します。Detector モジュールは新しいポリシーを受け入れず、ポリシーのしきい値を変更しません。
learn_params_days	間隔（日単位）。0 ～ 1000 の整数を入力します。
learn_params_hours	間隔（時間単位）。0 ～ 1000 の整数を入力します。
learn_params_minutes	間隔（分単位）。0 ～ 1000 の整数を入力します。

間隔の値は、*learn_params_days* 値、*learn_params_hours* 値、および *learn_params_minutes* 値の合計となります。

次の例は、Detector モジュールがポリシーを 1 時間間隔で受け入れるように設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# learning-params periodic-action
auto-accept 0 1 0
```

しきい値選択方式の設定

しきい値調整フェーズ中に、Detector モジュールが新しいしきい値の生成に使用するデフォルトの方式を設定できます。しきい値調整フェーズの結果を手動で受け入れることも、しきい値調整フェーズの結果を特定の間隔で Detector モジュールが自動的に受け入れるように設定することもできます。

しきい値選択方式を設定するには、ゾーン設定モードで次のコマンドを使用します。

learning-params threshold-selection {**new-thresholds** | **max-thresholds** | **weighted** *weight*}

表 8-2 に、**learning-params threshold-selection** コマンドの引数とキーワードを示します。

表 8-2　learning-params threshold-selection コマンドの引数とキーワード

パラメータ	説明
new-thresholds	ラーニング プロセスの結果をゾーン設定に保存します。
max-thresholds	現在のポリシーのしきい値をラーニングされたしきい値と比較し、値の大きい方をゾーン設定に保存します。 この方式がデフォルトです。
weighted *weight*	次の数式に基づいて、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

次の例は、ラーニングされたしきい値が現在のポリシーのしきい値よりも大きい場合に、提案されたポリシーを Detector モジュールが受け入れるように設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# learning-params threshold-selection
max-thresholds
```

ポリシーに対する調整済みのマーク付け

Detector モジュールは、ポリシーしきい値が調整されているかどうかを定義するポリシーしきい値の状態にマークを付け、保護およびラーニング機能をイネーブルにするときにこのステータスに関連付けます。ポリシーのしきい値のステータスは、ポリシーのしきい値を超過したときに、Detector モジュールでゾーンに対する攻撃と見なすかどうかを示します。

新しいゾーンが作成されるとき、または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た後に、Detector モジュールはゾーンのポリシーのしきい値を未調整としてマークします。ゾーン テンプレートのデフォルトのしきい値は、ゾーンのトラフィックに異常を発見した場合に Detector モジュールがスプーフィング防止機能をすぐにアクティブにするように調整されています。保護およびラーニング機能をイネーブルにしている場合、現在のゾーン トラフィックが現在のポリシーしきい値よりも高いと、ラーニング プロセスは停止します。この状況を防ぐために、ゾーン ポリシーが調整されていなければ、検出およびラーニング機能をイネーブルにした場合、ゾーン ポリシーしきい値が受け入れられるまで Detector モジュールはゾーン トラフィックにおける攻撃を検出しません。

ゾーンのポリシーが未調整である場合、Detector モジュールは、新しいポリシーを受け入れるときに、しきい値選択方式 accept-new をアクティブにして、以前のしきい値を無視します。Detector モジュールがそのゾーンに関するラーニング プロセスのしきい値調整フェーズの結果を受け入れるときに、accept-new 以外のしきい値選択方式を使用すると、ポリシーのしきい値の集合が不適切になる場合があります。しきい値の選択方式の詳細については、P.8-17 の「しきい値選択方式の設定」を参照してください。

Detector モジュールは、次の場合にゾーンの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場合
- ポリシー構築フェーズの結果を受け入れた場合
- ゾーン ポリシーに対してサービスの削除または新しいサービスの追加を行った場合

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た後に、ゾーンのポリシーを調整済みとしてマークします。

ユーザは、ゾーン ポリシーの設定を変更できます。ゾーン ポリシーに調整済みのマークを付けるには、ゾーン設定モードで次のコマンドを使用します。

learning-params threshold-tuned

ゾーン ポリシーに未調整のマークを付けるには、このコマンドの **no** 形式を使用します。

次のどちらかの場合は、ゾーン ポリシーのステータスを調整済みに変更することもできます。

- 新しいゾーンが既存のゾーンまたはスナップショットから複製されており、両方のゾーンのトラフィック特性が似ている場合
- ポリシーのしきい値をすべて手動で設定した場合

次のどちらかの場合は、ゾーン ポリシーのステータスを未調整に変更することもできます。

- ゾーンのネットワークに重要な変更を加えた場合
- ゾーンの IP アドレスまたはサブネットを変更した場合
- トラフィックのピーク時の間、検出およびラーニング機能を開始していない場合。ゾーン ポリシーのステータスを未調整に変更し、Detector モジュールがピーク時のトラフィックを攻撃として識別しないようにします。

ゾーン ポリシーが未調整としてマークされている場合、Detector モジュールは現在のポリシーしきい値を監視しません。また、ポリシーしきい値が超過してもゾーンへの攻撃を検出しません。

注意　ゾーンに対する攻撃がある場合は、ゾーン　ポリシーのステータスを未調整に変更しないでください。これは、ステータスを変更すると Detector モジュールで攻撃が検出されなくなり、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ためです。

次の例は、ゾーン ポリシーのステータスに調整済みのマークを付ける方法を示しています。

```
user@DETECTOR-conf-zone-scannet# learning-params threshold-tuned
```

ゾーンのポリシーのしきい値調整とゾーン異常検出のイネーブル化の同時実行

検出およびラーニング機能を使用することで、ラーニング プロセスのアクティブ化とゾーン異常検出のイネーブル化を同時に実行できます。Detector モジュールは、ポリシーのしきい値を調整し、同時にトラフィックの異常についてポリシーのしきい値を監視します。検出およびラーニング機能により、ポリシーのしきい値をゾーンのトラフィック特性に基づいて常にアップデートしながら、Detector モジュールでゾーン トラフィックの異常を検出できるようになります。検出およびラーニング機能を使用すると、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回避できます。

（注） 保護およびラーニング機能をアクティブ化する前に、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て、ゾーン ポリシーを構築する必要があります。

新しいゾーンを作成する場合、ゾーン ポリシーからサービスを追加または削除するか、ポリシー構築フェーズの結果を受け入れることで、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。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の結果を受け入れた後にだけ、ゾーンのポリシーを調整済みとしてマークします。しきい値調整フェーズの結果を手動で受け入れることも、**learning-params** コマンドを使用して、Detector モジュールが自動的に受け入れるように設定することもできます。

ラーニング プロセスとゾーン検出が同時にイネーブルになっており、ゾーン ポリシーのステータスが未調整の場合、ゾーン ポリシーのしきい値が受け入れられるまで、Detector モジュールは次のように機能します。

- Detector モジュールはゾーン トラフィックの攻撃を検出しない。
- Detector モジュールは、しきい値選択方式 accept-new をアクティブにする（P.8-17 の「しきい値選択方式の設定」を参照）。

Detector モジュールは、ゾーンに対する攻撃を識別すると、ラーニング プロセスを停止します。Detector モジュールは、Guard をアクティブにしてゾーンを保護した場合、Guard モジュールを定期的にポーリングします。Detector モジュールは、Guard モジュールがゾーンの保護を非アクティブにしたことを識別すると、他のトラフィック異常が存在しないことを確認してから、検出およびラーニング機能を再度アクティブにします。このオプションを使用できるのは、SSL 通信チャネルを設定した場合のみです。

保護およびラーニング機能をアクティブにする前に、Detector モジュールがラーニング プロセスの結果をいつ、どのように受け入れるかを設定できます。詳細については、P.8-15 の「ラーニング パラメータの設定」を参照してください。

ラーニング プロセスとゾーン異常検出を同時にアクティブにするには、**detect learning** コマンドを使用するか、**learning threshold-tuning** コマンドと **detect** コマンドを順番に入力します（順序は問いません）。

詳細については、P.8-10 の「ポリシーしきい値の調整」および第 9 章「ゾーンのトラフィックの異常の検出」を参照してください。

スナップショットを使用したラーニング プロセスの結果の確認

ラーニング プロセス中の任意の段階でラーニング パラメータ（サービス、しきい値、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して、後で確認できます。2 つのゾーンのラーニング パラメータまたはスナップショットを比較して、ラーニング プロセスの結果を確認し、ポリシー、サービス、およびしきい値の違いをトレースできます。

ラーニング プロセス中、数時間ごとにスナップショットを保存することをお勧めします。ラーニング プロセス中に攻撃が発生した場合は、スナップショット ポリシーをゾーンに使用できます。スナップショットは、手動で撮ることも、指定した間隔で Detector モジュールが自動的に撮るように設定することもできます。Detector モジュール は、スナップショットをゾーンごとに 100 個まで保存します。以前のスナップショットは新しいスナップショットに置き換えられます。

スナップショットからゾーン ポリシーをコピーすることで、必要に応じて、以前のラーニングの結果に基づいてゾーンを設定できます。

この項では、次のトピックについて取り上げます。

- スナップショットの作成
- ラーニングの結果の比較
- スナップショットの表示
- スナップショットの削除
- ゾーン設定へのポリシーのコピー

スナップショットの作成

ゾーンのラーニング パラメータの単一スナップショットを保存することができます。または、指定した間隔で Detector モジュールが自動的にスナップショットを撮るように設定できます。Detector モジュールは、スナップショットが撮られている間も、ラーニング プロセスを続行します。

Detector モジュールが指定した間隔で自動的にスナップショットを撮るように設定する方法の詳細については、P.8-15 の「定期的なアクションの設定」を参照してください。

ゾーンのラーニング パラメータのスナップショットを 1 つ保存するには、ゾーン設定モードで次のコマンドを使用します。

snapshot [**threshold-selection** {**new-thresholds** | **max-thresholds** | **cur-thresholds** | **weighted** *calc-weight*}]

表 8-3 に、**snapshot** コマンドの引数とキーワードを示します。

表 8-3　snapshot コマンドの引数とキーワード

パラメータ	説明
threshold-selection	（オプション）Detector モジュールがスナップショットのしきい値計算に使用する方式を設定します。デフォルトでは、Detector モジュールは **learning-params threshold-selection** コマンドで定義されたゾーンしきい値選択方式を使用します。ゾーンのデフォルトのしきい値選択方式は、**max-thresholds** です。
new-thresholds	ラーニング プロセスの結果をゾーン設定に保存します。
max-thresholds	現在のポリシーのしきい値をラーニングされたしきい値と比較し、値の大きい方をゾーン設定に保存します。 これがデフォルトの方式です。
cur-thresholds	ラーニング プロセスの新しいしきい値を無視して、現在のポリシーのしきい値をスナップショットに保存します。この方式は、バックアップの目的で使用できます。

表 8-3　snapshot コマンドの引数とキーワード（続き）

パラメータ	説明
weighted *calc-weight*	次の数式に基づいて、保存するポリシーのしきい値を計算します。 しきい値 =(新しいしきい値 * *計算された重み* + 現在のしきい値 *（100 - *計算された重み*)) / 100

snapshot コマンドを使用すると、ゾーンのラーニング プロセスの結果が保存されます。この結果には、ゾーンのポリシー、サービス、およびしきい値が含まれます。スナップショットのパラメータを確認するか、2 つのスナップショットを比較するか、またはスナップショットのパラメータを新しいゾーンにコピーし終わったら、スナップショットを削除できます。

snapshot threshold-selection cur-thresholds コマンドを使用すると、現在のゾーンポリシーをバックアップできます。

次の例は、ポリシーの現在のしきい値とラーニング プロセスの新しいしきい値のうちで最も大きい値をしきい値として持つスナップショットを作成する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# snapshot threshold-selection
max-thresholds
```

グローバル モードでスナップショットを 1 つ保存するには、**snapshot** *zone-name* [**threshold-selection** {**new-thresholds** | **max-thresholds** | **cur-thresholds** | **weighted** *weight*}] コマンドを使用します。

ラーニングの結果の比較

2 つのスナップショットまたはゾーンのラーニングの結果を比較して、ポリシー、サービス、およびしきい値の違いをトレースできます。

この項では、次のトピックについて取り上げます。

- スナップショットの比較
- ゾーンの比較

スナップショットの比較

2 つのスナップショットを比較するには、ゾーン設定モードで次のコマンドを使用します。

diff snapshots *snapshot-id1 snapshot-id2* [*percent*]

表 8-4 に、**diff** コマンドの引数を示します。

表 8-4　diff コマンドの引数

パラメータ	説明
snapshot-id1	最初に比較するスナップショットの ID。ゾーンのスナップショットのリストを表示するには、**show snapshots** コマンドを使用します。
snapshot-id2	2 番目に比較するスナップショットの ID。ゾーンのスナップショットのリストを表示するには、**show snapshots** コマンドを使用します。
percent	（オプション）違いの割合。Detector モジュールは、2 つのスナップショットを比較して、指定した値よりも大きいポリシーしきい値の違いだけを表示します。デフォルトのパーセンテージは 100% で、Detector モジュールは 2 つのスナップショットにおける相違をすべて表示します。

次の例は、ゾーンのスナップショットの表示方法と、最新の 2 つのスナップショットを比較する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show snapshots
ID    Time
1     Feb 10 10:32:04
2     Feb 10 10:49:12
3     Feb 10 11:01:50
user@DETECTOR-conf-zone-scannet# diff 2 3
```

グローバル モードでスナップショットを比較するには、**diff** *zone-name* **snapshots** *snapshot-id1 snapshot-id2* [*percent*] コマンドを使用します。

ゾーンの比較

2 つのゾーンのラーニング パラメータを比較するには、グローバル モードまたは設定モードで次のコマンドを使用します。

diff *zone-name1 zone-name2* [*percent*]

表 8-5 に、**diff** コマンドの引数を示します。

表 8-5　diff コマンドの引数

パラメータ	説明
zone-name1	比較対象のラーニング パラメータを持つ最初のゾーンの名前。
zone-name2	比較対象のラーニング パラメータを持つ 2 番目のゾーンの名前。
percent	（オプション）違いの割合。Detector モジュールは、2 つのゾーンを比較して、指定した値よりも大きいポリシーしきい値の違いだけを表示します。デフォルトのパーセンテージは 100% で、Detector モジュールは 2 つのゾーンにおける相違をすべて表示します。

次の例は、2 つのゾーンのラーニング パラメータの比較方法を示しています。

```
user@DETECTOR# diff scannet scannet-mailserver
```

スナップショットの表示

ゾーンのスナップショットまたはスナップショット パラメータのリストを表示し、ゾーンのラーニングの結果を包括的に把握するには、次のコマンドを入力します。

show snapshots [*snapshot-id* [**policies** *policy-path*]]

表 8-6 に、**show snapshots** コマンドのキーワードと引数を示します。

表 8-6　show snapshots コマンドの引数とキーワード

パラメータ	説明
snapshot-id	（オプション）表示するスナップショットの ID。ポリシーを指定しない場合、デフォルトでは、ゾーンのスナップショットすべてのリストが表示されます。スナップショット ID を表示するには、このコマンドを引数なしで使用します。
policies *policy-path*	（オプション）表示対象のポリシーのグループを指定します。詳細については、P.7-2 の「ポリシー パスの使用」を参照してください。

グローバル モードでスナップショットを比較するには、**show zone** *zone-name* **snapshots** [*snapshot-id* [**policies** *policy-path*]] コマンドを使用します。

次の例は、ゾーンのスナップショットのリストを表示する方法と、スナップショット 2 の dns_tcp に関連するポリシーを表示する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show snapshots
ID    Time
1     Feb 10 10:32:04
2     Feb 10 10:49:12
user@DETECTOR-conf-zone-scannet# show snapshots 2 policies dns_tcp
```

show zone *zone-name* **snapshots** *snapshot-id* **policies** *policy-path* コマンドの出力のフィールドは、**show policies** コマンドの出力のフィールドと同じです。詳細については、P.7-39 の「ポリシーの表示」を参照してください。

表 8-7 に、**show snapshots** コマンド出力のフィールドを示します。

表 8-7　show snapshots コマンド出力のフィールドの説明

フィールド	説明
ID	スナップショット ID。
Time	スナップショットが取得された日付と時刻。

スナップショットの削除

古いスナップショットを削除して、空きディスク スペースを得ることができます。

スナップショットを削除するには、ゾーン設定モードで次のコマンドを使用します。

no snapshot *snapshot-id*

snapshot-id 引数には、既存のスナップショットの ID を指定します。すべてのゾーンのスナップショットを削除するには、アスタリスク（*）を入力します。スナップショットの詳細を表示するには、**show snapshots** コマンドを使用します。

次の例では、すべてのゾーンのスナップショットを削除する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# no snapshot *
```

ゾーン設定へのポリシーのコピー

ポリシーの全体の設定または部分的な設定を現在のゾーンにコピーできます。

次の情報をコピーできます。

- サービスのコピー：ソース ゾーンからゾーンにサービスをコピーできます。この操作により、これらのサービスの検出にポリシー構築フェーズを適用することなく、ゾーン ポリシーを設定できます。サービスをゾーンにコピーするには、まず、そのゾーンが同様のトラフィック パターンを持つことを確認します。
- ポリシー パラメータの コピー：ゾーン ポリシー パラメータをゾーンのスナップショットのポリシー パラメータに置き換えることができます。この操作により、以前のラーニングの結果に戻すことができます。Detector モジュールは、既存ポリシーのパラメータだけをコピーします。

ゾーンのポリシーをコピーするには、ゾーン設定モードで次のコマンドを使用します。

copy-policies {*snapshot-id* | *src-zone-name* [*service-path*]}

表 8-8 に、**copy-policies** コマンドの引数とキーワードを示します。

表 8-8　copy-policies コマンドの引数とキーワード

パラメータ	説明
snapshot-id	ポリシーのコピー元のスナップショットの ID。スナップショットの ID を表示するには、**show snapshots** コマンドを使用します。
src-zone-name	サービス ポリシーのコピー元のゾーン名。
service-path	（オプション）コピー元のサービス。サービス パスの形式は、次のいずれかです。 • policy-template：ポリシー テンプレートに関連するすべてのポリシーをコピーします。 • policy-template/service-num：ポリシー テンプレートおよび指定のサービスに関連するすべてのポリシーをコピーします。 デフォルトでは、すべてのポリシーとサービスがコピーされます。

次の例は、ポリシー テンプレート tcp_connections に関連するすべてのサービスを、ゾーン webnet から現在のゾーン scannet にコピーする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# copy-policies webnet tcp_connections/
```

次の例は、ゾーンのスナップショットのリストを表示し、次に ID が 2 のスナップショットからポリシーをコピーする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show snapshots
ID   Time
1    Feb 10 10:32:04
2    Feb 10 10:49:12
user@DETECTOR-conf-zone-scannet# copy-policies 2
```

ゾーン ポリシーのバックアップ

現在のゾーン ポリシーは、**snapshot threshold-selection cur-thresholds** コマンドを使用していつでもバックアップできます。

次の例は、現在のゾーン ポリシーのバックアップ方法を示しています。

```
user@DETECTOR-conf-zone-scannet# snapshot threshold-selection
cur-thresholds
```