CHAPTER 7

ゾーン トラフィックのラーニング

この章では、Cisco Guard（Guard）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、Guard がゾーン保護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 プロセスの実行
- Protect 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、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、Guard 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、次の方法でゾーン保護を最適化できます。

- 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、Guard 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。Guard 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
- 保護およびラーニング機能について
- 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、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**：Guard 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、Guard 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、Guard 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、Guard が詳細に監視するサービスの最大数、および Guard 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 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**：Guard 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 Guard 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、Guard 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、Guard がポリシーのアクションで動的フィルタを作成します。

ゾーンのトラフィック特性をラーニングするには、ゾーンのトラフィックを Guard に宛先変更する必要があります。外部デバイスを使用して、ラーニング プロセスを開始する前にトラフィックの宛先変更を設定するか、ゾーンのトラフィックを Guard に手動で宛先変更する必要があります。Guard の CLI を使用してルーティング設定を設定することで、トラフィックの宛先変更を設定できます。詳細については、『*Guard Configuration Guide*』を参照してください。

保護およびラーニング機能について

Guard 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は、保護およびラーニング機能をアクティブにできます。この機能を使用すると、しきい値調整フェーズ（Learn）を実行しながら、同時に Guard でトラフィックの異常を検出（Protect）することができます。Protect and Learn がアクティブである場合、Guard 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。Guard 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、攻撃からのゾーンの保護を開始します。攻撃が終了したことを確認すると、Guard はラーニング プロセスを再開します。

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。Guard 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、Guard 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、Guard 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 Guard 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の状態にある（攻撃を受けていない）：Guard では DDoS 攻撃のトラフィック特性に応じてゾーン ポリシーが構築および調整され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、Guard 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、Guard 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：Guard 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、Guard 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アクティブにできます。Guard 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 2 時間実行した後でポリシー構築フェーズを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、いずれかの Guard_Link ゾーン テンプレート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 メニューの **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。

Guard が、宛先変更されたゾーン トラフィックの分析を開始して、トラフィック フローのサービスを検出し、検出したサービスのポリシーを作成します。Guard 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。

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 Guard 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。

Guard は、ゾーンの設定の現在のポリシーをすべて削除して、提案されたゾーン ポリシーで置き換えます。Guard 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、Guard 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、Guard 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） Guard 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 メニューの **Learning > Tune Threshold** を選択します。

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。

Guard 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。Guard 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 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。

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、Guard 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：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	Guard 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、Guard 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**：Guard　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継続します。

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：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	Guard 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、Guard 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**：Guard　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。

Protect and Learn を使用したラーニング プロセスの実行

この項では、Protect 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、Guard 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。Guard は、ゾーンに対する攻撃を検出してその攻撃を軽減している間、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、Guard はラーニング プロセスを再開し、引き続きトラフィックの異常を監視します。

Protect and Learn をアクティブにする前に、Guard 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
- Protect and Learn のアクティブ化
- Protect 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

自動ラーニングのパラメータを設定すると、Protect 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 Guard 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 ポリシーを次のようにマークします。 • 調整済み：ポリシーを調整済みとしてマークするには、このオプションを選択します。調整済みの場合、Guard はただちにポリシーを使用してゾーンを保護することができます。 • 未調整：ポリシーを未調整としてマークするには、このオプションを選択解除します。未調整の場合、Guard がゾーンを保護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。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。

表 7-3　ラーニングのパラメータ（続き）

パラメータ	説明
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 : Guard 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できます。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 : ラーニング プロセスの結果を Guard が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 : Guard 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。Guard 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。Guard 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。
Threshold selection method	受け入れるしきい値を選択するために Guard 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	Guard 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、Guard 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**：Guard 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。

Protect and Learn のアクティブ化

Protect 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 Guard の動作が異なるためです。Protect 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、Guard はすぐに攻撃を検出できると同時に、ゾーンのトラフィックをラーニングできます。Protect 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、Guard 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。

- Guard 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。
- Guard は、Accept new thresholds という方法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、Guard 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。

Protect 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　**Protect 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）とゾーン保護（**Protect** 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。

- Guard は、ゾーン トラフィックを自身に宛先変更し、異常についてトラフィック フローの分析を開始します。正当なトラフィックは、その目的の宛先へと転送されるネットワークに再び注入されます。悪意のあるトラフィックは Guard によってフィルタリングされ、ドロップされます。
- Guard 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 Protected Zones リストにゾーン名が追加され、Recent Events テーブルには、*保護されるゾーン*の詳細なリストとともに、*保護開始*のイベント タイプが表示されます。

Protect and Learn の非アクティブ化

Protect and Learn を非アクティブにする場合、Guard では、保護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。

Protect 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、保護されている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、Protect 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 **Protection > 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 Protection**：ゾーン保護を停止します。
- **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できます。

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 Guard 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	Guard 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、Guard 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

ゾーン保護とラーニングの両方を非アクティブにした場合、Guard はゾーン トラフィックの自身への宛先変更を停止します。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、*保護されないゾーン* 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、保護  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

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。Guard 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、Guard はゾーン ポリシーを未調整としてマークします。
  - 新しいゾーンを作成する。
  - 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。Guard 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必要があります。Protect and Learn をアクティブにするときにゾーンが未調整の場合、Guard 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。Guard 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。Guard 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、Guard 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保護およびラーニング機能を開始していないが、ピーク時のトラフィックを Guard が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、Guard 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。Guard 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を保護できます。
- 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。Guard がポリシーを未調整としてマークします。この場合、Guard がポリシーを使用してゾーンを保護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**：Guard は調整済みの設定をゾーン設定に保存します。
- **Clear**：Guard 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 Form 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

スナップショットを使用すると、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。スナップショットにより、次の作業を実行できます。

- 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。Guard 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。Guard 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
- 現在のゾーン 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変更
- 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。

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 Guard 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 Guard 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。Guard はゾーン ポリシーを保存し、スナップショットに連続した ID 番号を割り当てます。

現在のゾーン 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、Guard 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。Guard はゾーン ポリシーを保存し、スナップショットに連続した ID 番号を割り当てます。

スナップショットの表示

スナップショットを表示して、ゾーンのラーニングの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　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 Guard 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、名前のないスナップショットの場合、Guard 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、Guard 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 Guard 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：ゾーンがラーニング プロセスを実行していません。
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変更

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 Guard 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。

Guard 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。Guard 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
- 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。

- Guard 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 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。
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。

表 7-6　ポリシー比較のパラメータ（続き）

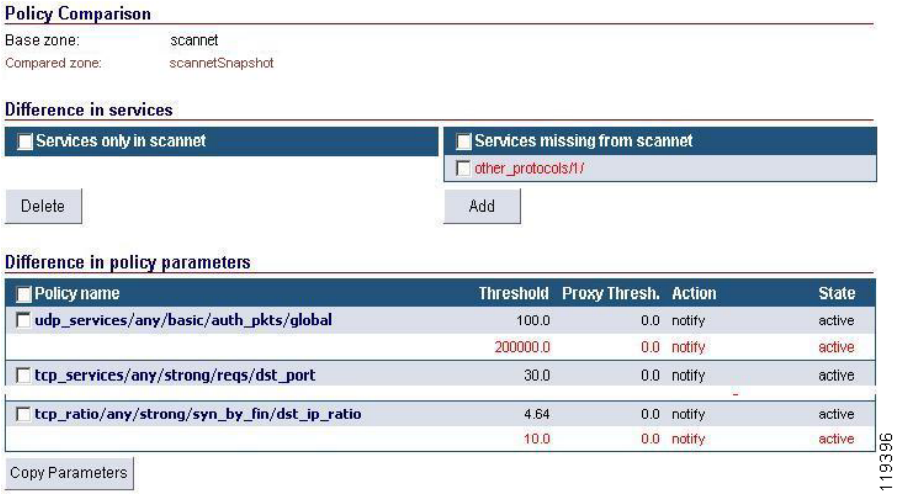
パラメータ 1	パラメータ 2	説明
Minimal difference		比較元ゾーンと比較先ゾーンにおけるポリシーの設定の相違点の割合。Guard は、2 つのゾーンを比較し、指定された値より大きいポリシーしきい値の相違点だけを表示します。デフォルトの割合は 100% です。この場合、Guard は、一方のしきい値が他方のしきい値よりも 2 倍以上大きいポリシーだけを表示します。

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） Guard 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。Guard 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。Guard 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 Guard 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。