ゾーンのトラフィックのラーニング

この章では、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を分析し、ゾーンの設定の保護機能を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 プロセスの概要

ラーニング プロセスでは、Guard はゾーンのトラフィックを分析し、検出されたトラフィック フロー サービスに基づいてゾーン固有のポリシーのセットを作成することができます。ラーニング プロセス中に、Guard は作成する各ポリシーのしきい値も調整します。ポリシーのしきい値は、ゾーンを保護するときに Guard が使用する参照ポイントです。このしきい値によって、トラフィック レートが通常の量をいつ超過し、ゾーンに対する攻撃を示唆するようになったかが判断されます。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 プロセスの結果を受け入れるか拒否するかを決定します。ラーニング プロセスの結果を受け入れると、Guard はポリシーの情報をゾーンの設定に保存して、ゾーンの設定の以前のポリシーをすべて削除します。ラーニング プロセスの結果を拒否すると、Guard はラーニング プロセスの結果を削除して、ゾーンの設定に含まれている既存のポリシーを引き続き使用します。

この項は、ラーニング プロセスに関する次の情報で構成されています。

- ラーニング プロセスのフェーズ
- Protect and Learn 機能
- ラーニング プロセスの結果の受け入れまたは拒否

ラーニング プロセスのフェーズ

ラーニング プロセスは、Guard 上で個別に実行する次の 2 つのフェーズで構成されます。

- ポリシー構築フェーズ：このフェーズでは、Guard が、トラフィック フローで検出したサービスに基づいてポリシーを作成します。各ポリシーには、Guard がトラフィックの異常を検出したときに実行するアクションが設定されます。ポリシー テンプレートは、ポリシーを作成するときに Guard が従うガイドラインを提供します。たとえば、ポリシー構築フェーズ中に Guard がテンプレートから作成できるポリシーの数について、ポリシー テンプレートで制限することができます。また、Guard がポリシー テンプレートから作成する各ポリシーのデフォルトしきい値も、ポリシー テンプレートで設定します。

- しきい値調整フェーズ：このフェーズでは、Guard がゾーンの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 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、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を実行します。

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。

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 のルーティング設定を使用して、ゾーンの宛先変更を設定してください。Guard のルーティング設定は、CLI でのみ設定できます。詳細については、『*Cisco Guard Configuration Guide*』を参照してください。

どちらのラーニング フェーズでも、ラーニング プロセスの任意の時点で Guard のスナップショット機能を使用して現在の結果を保存することができます。ラーニング プロセスのスナップショットを取得すると、そのスナップショットの時点までに Guard が作成したポリシーの情報を確認できます。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。また、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アップデートすることもできます。スナップショット機能の使用の詳細については、この章の「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。

Protect and Learn 機能

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、Protect and Learn 機能をアクティブにできます。この機能を使用すると、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。Guard は、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。保護およびラーニングの動作状態では、ポリシーのしきい値を通常時のゾーンのトラフィック特性に従って常にアップデートしながら、Guard でゾーンを保護できるようになり、Guard 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がなくなります。

ラーニング プロセスの結果の受け入れまたは拒否

ポリシー構築フェーズまたはしきい値調整フェーズの結果は、フェーズの実行中またはフェーズを停止したときに、受け入れまたは拒否できます。ラーニング プロセス中に、Guard がゾーンの設定のポリシーを変更することはありません。Guard がゾーンの設定をアップデートし、新しいポリシーまたはポリシーのしきい値を使用して動作を開始するのは、システム管理者がラーニング フェーズの結果を受け入れた後のみです。

ラーニング プロセスの実行

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

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

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

- ゾーンのトラフィックが通常の状態である（攻撃を受けていない）：Guard が、DDoS 攻撃のトラフィック特性に従ってゾーンのポリシーを作成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、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基準として保存します。この結果、Guard 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ります。
- ゾーンのトラフィックがピーク量に達している：Guard が、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適合した値に設定できるようになります。また、Guard が通常のトラフィックのピーク時の状態を攻撃と見なさないことが保証されます。

この項では、次の手順について説明します。

ポリシー構築フェーズの開始

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

（注）　ポリシー構築フェーズは、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。次の処理が実行されます。

- 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 フローで使用されているサービスを検出し、検出したサービスに関連する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（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。

Guard が十分な時間をかけて、通常時のゾーン トラフィックが正確に表現されているトラフィックを受信し、分析できるようにするには、ポリシー構築フェーズを少なくとも 2 時間実行してから停止することをお勧めします。

ポリシー構築フェーズの停止

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　ポリシー構築フェーズの現在の結果を受け入れるか拒否するには、次のいずれかのオプションを使用します。

- ゾーンのメイン メニューの **Learning > Accept** を選択して、ラーニング フェーズの結果を受け入れます。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、ゾーンのサービスを引き続きラーニングします。
- 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。次のいずれかのオプションを選択して、ステップ 3 に進みます。
  - **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 3　このステップが必要になるのは、ステップ 2 で **Learning > Stop Learning** を選択した場合のみです。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。ポリシー構築フェーズは終了します。
- **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。

しきい値調整フェーズをアクティブにするのは、ポリシー構築フェーズの結果を受け入れた後にすることをお勧めします。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。次の処理が実行されます。

- Guard がゾーンのトラフィックの分析を開始して、ゾーンのポリシーのしきい値をトラフィック フローの特性に合せて調整します。
- ゾーンのステータス ラーニング アイコン  が、作業領域内の、ナビゲーション パネルのゾーン名の隣に表示されます。

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

ステップ 3　（オプション）しきい値調整フェーズの任意の時点で、**Learning > Snapshot** を選択してこのフェーズの現在の結果（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。

Guard が十分な時間をかけて、通常時のゾーン トラフィックが正確に表現されているトラフィックを受信し、分析できるようにするには、しきい値調整フェーズを少なくとも 24 時間実行してから終了することをお勧めします。

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** : Guard 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** : Guard 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** : Guard は、次の公式に基づいて、保存するポリシーのしきい値を計算します。 新しいしきい値 = (ラーニングしたしきい値 * 重み + 現在のしきい値 * (100 - 重み)) / 100 重み値は、システム管理者が定義します。 • **Keep current thresholds** : Guard 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、ポリシーがしきい値調整フェーズ前の値を保持します。

表 7-1　しきい値の選択方法（続き）

パラメータ	説明
weight	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、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、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。使用するしきい値選択方法を定義します。表 7-2 に、しきい値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	• **Accept new thresholds** : Guard 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** : Guard 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式です。 • **Accept weighted thresholds** : Guard は、次の公式に基づいて、保存するポリシーのしきい値を計算します。 新しいしきい値 = (ラーニングしたしきい値 * 重み + 現在のしきい値 * (100 - 重み)) / 100 重み値は、システム管理者が定義します。 • **Keep current thresholds** : Guard 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、ポリシーがしきい値調整フェーズ前の値を保持します。
weight	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、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、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。

Protect 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、Protect and Learn の動作を管理する方法について説明します。Protect and Learn では、Guard でゾーンのトラフィックをラーニングしてポリシーのしきい値調整を実行しながら、ゾーンを保護することができます。Protect and Learn をアクティブにする前に、ラーニング プロセスの結果を Guard が受け入れるタイミングと方法を設定できます。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、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 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 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場合に、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 > 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 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。ポリシーを調整済みとしてマークし、Guard がポリシーを使用してすぐにゾーンを保護できるようにするには、このオプションをオンにします。ポリシーを未調整としてマークし、システム管理者がしきい値調整フェーズの結果を受け入れた後にのみ Guard がゾーンを保護できるようにするには、このオプションをオフにします。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 : 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 : Guard 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** : 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、指定した間隔でゾーンの設定に受け入れます。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。

表 7-3　ラーニングのパラメータ（続き）

パラメータ	説明
Threshold selection method	受け入れるしきい値を選択する方法。ドロップダウン リストから、次のいずれかのオプションを選択します。 • **Accept new thresholds** : Guard 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** : Guard 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** : Guard は、次の公式に基づいて、保存するポリシーのしきい値を計算します。 新しいしきい値 = (ラーニングしたしきい値 * 重み + 現在のしきい値 * (100 - 重み)) / 100 重み値は、システム管理者が定義します。 • **Keep current thresholds** : Guard 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、ポリシーがしきい値調整フェーズ前の値を保持します。
weight	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、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。

Protect and Learn のアクティブ化

Protect and Learn をアクティブにすると、Guard でゾーンのトラフィックをラーニングしてポリシーのしきい値調整を実行しながら、ゾーンを保護することができます。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 は攻撃を検出し、ゾーンのトラフィックをラーニングすることができます。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 は次のように動作します。

- Guard 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、ゾーンのトラフィックに含まれている攻撃を検出しません。
- Guard は、しきい値選択方法 Accept new thresholds だけをアクティブにします（P.7-12 の「自動ラーニング 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。

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。

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。
- ゾーンの名前が、ナビゲーション ペインの Protected Zones リストに追加されます。

- ゾーンのステータス アイコンが、スタンバイ  から保護  に変更されます。
- Recent Events テーブルに、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ときは、Guard でゾーン保護とラーニングの両方を非アクティブにすることも、2 つの動作のいずれか一方のみを非アクティブにすることもできます。

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。次のアクションをいずれかまたは両方選択します。

- **Stop Protection**：ゾーン保護を停止します。
- **Stop Learning**：しきい値調整フェーズを停止します。次のいずれかのオプションを選択します。
  - **Reject**：しきい値調整フェーズの現在の結果を無視します。
  - **Accept**：しきい値調整フェーズの現在の結果をゾーンの設定に使用します。使用するしきい値選択方法を定義します。表 7-4 に、しきい値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	• **Accept new thresholds** : Guard 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** : Guard 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** : Guard は、次の公式に基づいて、保存するポリシーのしきい値を計算します。 新しいしきい値 = (ラーニングしたしきい値 * 重み + 現在のしきい値 * (100 - 重み)) / 100 重み値は、システム管理者が定義します。 • **Keep current thresholds** : Guard 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、ポリシーがしきい値調整フェーズ前の値を保持します。
weight	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、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

ゾーンの保護とラーニングを両方とも非アクティブにすると、次の処理が実行されます。

- Guard が、ゾーン トラフィックの自身への宛先変更を停止します。
- ゾーンの名前が、ナビゲーション ペインの Protected Zones リストから削除されます。
- 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。
- Recent Events テーブルに、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。

ゾーンのポリシーに対する調整済みまたは未調整のマーク付け

Guard は、ゾーンのポリシーを次の条件に基づいて調整済みまたは未調整と判断します。

- 未調整 : Guard は、ゾーンの設定でゾーン テンプレートのデフォルトのポリシーのしきい値が使用されている場合、ゾーンを*未調整*としてマークします。次のいずれかの操作を実行すると、ゾーンの設定にはデフォルトのポリシーのしきい値が使用されます。
  - 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 : 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ことが重要です。Protect 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*である場合、Guard は、自動ラーニングのパラメータに従ってしきい値調整フェーズの結果を受け入れるまで、ゾーンに対する攻撃を検出できません（「自動ラーニング パラメータの設定」の項を参照）。自動ラーニングのしきい値選択方法を *Accept new thresholds* 以外に設定している場合、Guard は *Accept new thresholds* 設定を使用してしきい値調整フェーズの最初の結果を受け入れます。これ以降は、Guard はシステム管理者が選択したしきい値選択方法を使用します。

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

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

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

- ゾーンのネットワークが大幅に変更された。

- ゾーンの IP アドレスまたはサブネットが変更された。
- （ピーク時のトラフィックを Guard が攻撃と見なさないようにするために）トラフィックのピーク時に検出およびラーニングの動作状態を開始していない。

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

ゾーンを調整済みまたは未調整としてマークするには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Configuration > 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。

- **Zone is tuned をオンにする**：Guard は、ポリシーを調整済みとしてマークし、ポリシーを使用してすぐにゾーンを保護できます。
- **Zone is tuned をオフにする**：Guard は、ポリシーを未調整としてマークし、システム管理者がしきい値調整フェーズの結果を受け入れた後にのみ、Guard が保護およびラーニング モードでゾーン保護をアクティブにできるようにします。

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 が、調整状態の設定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。

Learning Parameter Form のオプションの詳細については、「自動ラーニング 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

Guard 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確認およびポリシー比較のために保存できます。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。Guard は、スナップショット情報を記録してスナップショットに連続 ID 番号を割り当て、現在のラーニング フェーズの実行を継続します。

この項では、次の手順について説明します。

ラーニング プロセスの現在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。Guard 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。

ゾーン設定ポリシーのスナップショット取得

ゾーン トラフィックがラーニングされていない（ゾーンがスタンバイ モードまたは保護モードのいずれかになっている）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。Guard が、ゾーンの設定に含まれているポリシーをスナップショットに保存し、スナップショットに連続 ID 番号を割り当てます。

スナップショットの結果の表示、変更、または保存

スナップショットの結果を表示、変更、またはゾーンの設定に保存するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインで、ラーニング フェーズに現在入っているゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Learning > Snapshot List** を選択します。スナップショットのリストが表示され、各スナップショットの ID 番号が、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　表示するスナップショットの ID 番号または日付を選択します。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）スナップショットの Policies 画面で、次のいずれかのオプションを選択します。

- **Configure Selection**：1 つまたはそれ以上のポリシーのパラメータを再設定します（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）。
- **Add service** または **Remove service**：スナップショットの時点で検出されたサービスのリストに対して、サービスを追加または削除します（第 8 章「ゾーンのポリシーの管理」の「サービスの追加」または「サービスの削除」の項を参照）。
- **Accept Thresholds**：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

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します。

ステップ 4　**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。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。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を比較するときは、次の操作を実行できます。

- 比較の詳細度を定義する。
- ポリシーの設定のアトリビュートを削除または追加して、比較した 2 つのゾーンを互いに類似させる。
- ラーニングしたポリシーのアトリビュートについて、一部を選択して受け入れる。

この項では、次の手順について説明します。

ポリシーの設定の相違点の表示

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

ステップ 1　次のいずれかの方法で、ポリシーの比較プロセスを開始します。

- 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 > Compare Policies** を選択します。

Policies Comparison クエリーの画面が表示されます。

ステップ 2　比較元および比較先となるゾーンまたはスナップショットを定義します。表 7-5 に、Policies Comparison クエリーのパラメータの説明を示します。

表 7-5　ポリシー比較のパラメータ

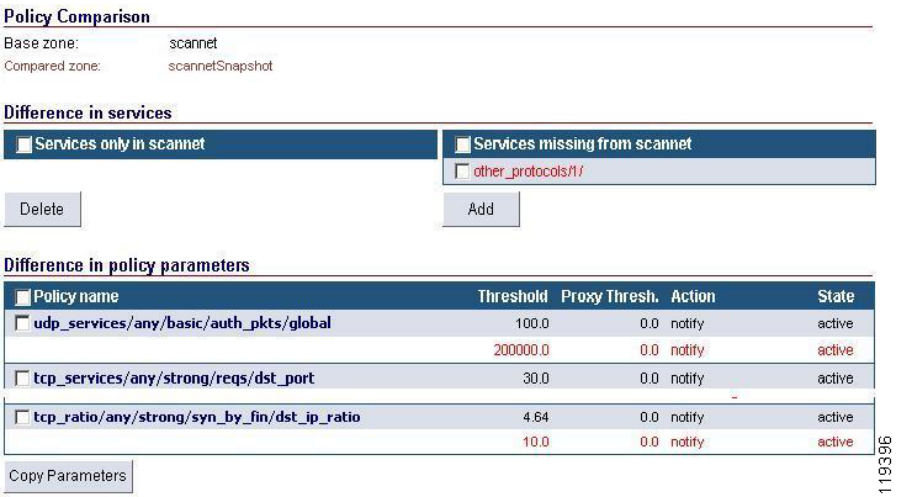
パラメータ 1	パラメータ 2	説明
Base Zone	Zone	ゾーンまたはスナップショットの名前。比較されている 2 つのゾーンのポリシーの設定に見つかった相違点を修正するために、設定を変更する必要がある場合は、比較元のゾーンに変更を加えます。比較元となるゾーンをドロップダウン リストから選択します。
	Policy Configuration	選択した比較元ゾーンのポリシーの設定。デフォルト値は、ゾーンの設定の現在のポリシーの設定です。ただし、スナップショットを使用できる場合はスナップショットもドロップダウン リストに表示されます。比較元となるゾーンのポリシーの設定をドロップダウン リストから選択します。
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、ゾーンの設定の現在のポリシーの設定です。ただし、スナップショットを使用できる場合はスナップショットもドロップダウン リストに表示されます。ポリシーの設定をドロップダウン リストから選択します。
Minimal difference		比較元のゾーンと比較先のゾーンで、ポリシーの設定が異なっている割合。Guard は、相違点がここに定義した割合を超えているパラメータをすべてトレースします。デフォルトでは、Guard は比較対象ゾーンのすべての違いをトレースします（100%）。相違点のパーセンテージ値を入力します。

ステップ 3　次のいずれかのオプションを選択します。

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

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

図 7-1　ポリシー比較テーブル



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

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

- **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。

（注）　Guard がチェックボックスを表示するのは、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のみです。タイプが **any** のサービスなど、表示されている一部のサービスはゾーン固有のサービスではないため、追加および削除できません。

比較元ゾーンのサービスの削除

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、選択したサービスを比較元ゾーンのポリシー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、選択したサービスを比較元ゾーンのポリシーの設定に追加します。

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。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。Guard が、選択したポリシーを比較先ゾーン（赤色）から比較元ゾーン（黒色）のポリシーの設定にコピーして、選択したポリシーをテーブルから削除します。