ゾーンの設定

この章では、Cisco Guard（Guard）上でゾーンを作成し、管理する方法について説明します。これらの手順は、ゾーン保護をイネーブルにするために必要です。

この章には、次の項があります。

概要

ゾーンは、Guard で DDoS 攻撃からの保護の対象となるネットワーク要素です。ゾーンは、ネットワーク サーバ、クライアント、ルータ、ネットワーク リンク、サブネット、ネットワーク全体、個々のインターネット ユーザ、企業、インターネット サービス プロバイダー（ISP）、またはこれらを組み合せたものを包含できます。Guard は、ゾーンのネットワーク アドレスの範囲が重なっていなければ、複数のゾーンを同時に保護できます。

ゾーンには、名前を割り当て、この名前を使用してゾーンを参照します。

ゾーンの設定処理には、次のタスクがあります。

- ゾーンの作成：ゾーンを作成し、ゾーン名、説明、およびネットワーク IP アドレスなど、ゾーンのアトリビュートを設定します。詳細については、P.5-3 の「ゾーンの作成」を参照してください。
- ゾーン フィルタの設定：さまざまなゾーン フィルタを設定します。ゾーン フィルタは、ゾーンのトラフィックを必要な保護レベルに誘導し、Guard で特定のトラフィック フローを処理する方法を定義します。詳細については、第 6 章「ゾーンのフィルタの設定」を参照してください。
- ゾーンのトラフィック特性のラーニング：ゾーンの保護ポリシーを作成します。このポリシーは、Guard で特定のトラフィック フローを分析して、トラフィック フローがポリシーのしきい値を超過した場合にアクションを実行できるようにします。ポリシーは、ポリシー構築およびしきい値調整という 2 つのフェーズで構成されるラーニング プロセスの中で構築されます。詳細については、P.5-13 の「ゾーン トラフィックの特性のラーニング」を参照してください。

ゾーンの作成

ゾーンを作成し、ゾーンのアトリビュートを設定します。ゾーンのアトリビュートは、ゾーン名、ゾーンの説明、ゾーンのネットワーク アドレス、ゾーンの動作定義、およびネットワーク定義で構成されています。

新しいゾーンを作成するときには、既存のゾーンをテンプレートとして使用するか、またはシステム定義のゾーン テンプレートからゾーンを作成することができます。ゾーン テンプレートには、ゾーンの初期ポリシーおよびフィルタ設定が定義されています。

新しいゾーンには、オンデマンド保護用に調整されたデフォルト ポリシーが割り当てられます。ただし、ゾーンをすぐに保護する必要がない場合は、Guard でゾーンのトラフィック特性をラーニングすることをお勧めします。詳細については、P.5-43 の「オンデマンド保護のイネーブル化」を参照してください。または、ゾーンの設定とゾーンのポリシーを Detector からコピーすることもできます。

新しいゾーンは、次の 3 つの方法で作成できます。

- 新しいゾーンの作成：システム定義のゾーン テンプレートから新しいゾーンを作成します。この方式は、デフォルトのポリシーおよびフィルタを使用して新しいゾーンを作成する場合に使用します。

  新しいゾーンを作成したら、ゾーンの特性を設定する必要があります。
- ゾーンの複製：既存のゾーンからゾーンを作成します。この方式は、新しいゾーンに既存のゾーンと同様のトラフィック パターンを割り当てる場合に使用します。
- ゾーンの設定の Detector からのコピー：この方式は、Detector とのゾーンの設定の同期をイネーブルにする場合に使用します。P.5-29 の「Guard のゾーンの設定と Detector の同期」を参照してください。

  この操作は、Cisco Traffic Anomaly Detector からのみ開始できます。詳細については、『*Cisco Traffic Anomaly Detector Configuration Guide*』を参照してください。

ゾーンの設定の設定値を変更する方法については、P.5-9 の「ゾーンのアトリビュートの設定」を参照してください。

新しいゾーンの作成

システム定義のゾーン テンプレートから新しいゾーンを作成するには、次のコマンドのいずれかを入力します。

- **zone** *new-zone-name* [*template-name*] [**interactive**]：Guard は、新しいゾーンを作成します。*template-name* 引数を挿入しない場合、新しいゾーンは GUARD_DEFAULT ゾーン テンプレートから作成されます。
- **zone** *zone-name* [*template-name*] [**interactive**]：Guard は、既存のゾーンを削除して、同じ名前で新しいゾーンを作成します。

システム定義のゾーン テンプレートを使用する場合、Guard は、ゾーンのすべてのアトリビュートにデフォルト設定を適用します。これらのデフォルト ポリシーの設定は、オンデマンド保護用に調整されます。

コマンドが正常に実行されると、Guard は新しいゾーンの設定モードに入ります。

ゾーン テンプレートを指定せずに既存のゾーンの名前を入力すると、Guard は指定したゾーンの設定モードに入ります。

表 5-1 に、**zone** コマンドの引数とキーワードを示します。

表 5-1　zone コマンドの引数とキーワード

パラメータ	説明
new-zone-name	新しいゾーンの名前。名前は、1 ～ 63 文字の英数字の文字列です。この文字列は英字で始まる必要があり、アンダースコアを含むことができますが、スペースを含むことはできません。
zone-name	既存のゾーンの名前。
template-name	(オプション) ゾーンの設定を定義するゾーン テンプレート。デフォルトでは、GUARD_DEFAULT ゾーン テンプレートを使用してゾーンが作成されます。 詳細については、表 5-2 を参照してください。

表 5-1　zone コマンドの引数とキーワード（続き）

パラメータ	説明
interactive	Guard がゾーン保護をインタラクティブ方式で実行するように設定します。ポリシーが作成する動的フィルタは、推奨事項として表示されます。各動的フィルタをアクティブにするかどうかを決定する必要があります。詳細については、第 8 章「インタラクティブ保護モード」を参照してください。

表 5-2 に、ゾーン テンプレートを示します。

表 5-2　ゾーン テンプレート

テンプレート	説明
GUARD_DEFAULT	デフォルトのゾーン テンプレート。Guard は、パケットの送信元 IP アドレスを Guard の TCP プロキシ IP アドレスに変更することがあります。このゾーン テンプレートは、該当のゾーン ネットワークの着信 IP アドレスに基づく IP ベースのアクセス リスト（ACL）、アクセス ポリシー、またはロード バランシング ポリシーを使用しない場合に使用することができます。
GUARD_TCP_NO_PROXY	TCP プロキシを使用しないゾーン用に設計されたゾーン テンプレート。このゾーン テンプレートは、ゾーンが IP アドレスに従って管理される場合（Internet Relay Chat（IRC; インターネット リレー チャット）サーバ タイプのゾーンなど）や、ゾーンで実行されているサービスのタイプが不明な場合に使用することができます。

表 5-2　ゾーン テンプレート（続き）

テンプレート	説明
帯域幅限定リンク テンプレート	帯域幅のわかっているゾーンに応じてセグメント化された大規模なサブネットのオンデマンド保護用に設計されたゾーン テンプレート。これらのゾーンについては、**activation-extent ip-address-only** コマンドを使用して、攻撃されているサブネットまたは範囲に基づいてゾーン保護をアクティブにすることをお勧めします。このようなゾーンは、protect-ip-state が dst-ip-by-name となっている Detector で定義することを推奨します。 ポリシーのしきい値は、ゾーン宛てのトラフィックのレートが指定したレートを超過した場合に、ゾーンに対する攻撃を Guard が識別できるように調整されています。 帯域幅限定リンク ゾーン テンプレートは、128 Kb、1 Mb、4 Mb、および 512 Kb のリンクをそれぞれ対象とした次のものが用意されています。 **GUARD_LINK_128K** **GUARD_LINK_1M** **GUARD_LINK_4M** **GUARD_LINK_512K** これらのテンプレートから作成されたゾーンに対してポリシー構築を実行することはできません。

次の例は、新しいゾーンを作成する方法を示しています。

```
user@GUARD-conf# zone scannet interactive
user@GUARD-conf-zone-scannet#
```

ゾーンを削除するには、**no zone** コマンドを使用します。ゾーンを削除するときは、ゾーン名の末尾に、ワイルドカード文字としてアスタリスク（*）を使用できます。ワイルドカードを使用すると、同じプレフィクスを持つ複数のゾーンを 1 つのコマンドで削除できます。

ゾーン テンプレートを表示するには、グローバル モードまたは設定モードで **show templates** コマンドを使用します。ゾーン テンプレートのデフォルト ポリシーを表示するには、グローバル モードまたは設定モードで **show templates** *template-name* **policies** コマンドを使用します。

ゾーンの複製

既存のゾーンに基づいて、新しいゾーンを作成することができます。既存のゾーンを新しいゾーンのテンプレートとして使用すると、既存のゾーンのプロパティすべてが、新しく定義したゾーンにコピーされます。スナップショットを指定すると、ゾーン ポリシーはスナップショットからコピーされます。

ゾーンを複製するには、次のコマンドのいずれかを入力します。

- **zone** *new-zone-name* **copy-from-this** [*snapshot-id*]: このコマンドは、現在のゾーンの設定を使用して新しいゾーンを作成するときに、ゾーン設定モードで使用します。
- **zone** *new-zone-name* **copy-from** *zone-name* [*snapshot-id*]：このコマンドは、特定のゾーンの設定を使用して新しいゾーンを作成するときに、設定モードで使用します。

表 5-3 で、**zone** コマンドの引数について説明します。

表 5-3　zone コマンドの引数

パラメータ	説明
new-zone-name	新しいゾーンの名前。名前は、1 ～ 63 文字の英数字の文字列です。この文字列は英字で始まる必要があり、アンダースコアを含むことができますが、スペースを含むことはできません。
zone-name	既存のゾーンの名前。
snapshot-id	既存のスナップショットの ID。詳細については、P.7-41 の「スナップショットの表示」を参照してください。

次の例は、現在のゾーンに関連して新しいゾーンを作成する方法を示しています。

```
user@GUARD-conf-zone-scannet# zone mailserver copy-from-this
user@GUARD-conf-zone-mailserver#
```

コマンドが正常に実行されると、Guard は新しいゾーンの設定モードに入ります。

新しいゾーンのポリシーには、未調整のマークが付けられます。ラーニング プロセスのしきい値調整フェーズを実行して、ポリシーのしきい値をゾーンのトラフィックに合せて調整する方法をお勧めします。新しいゾーンのトラフィック特性が、元になるゾーンのトラフィック特性と同じか、よく似ていれば、ポリシーのしきい値に調整済みのマークを付けることができます。詳細については、P.5-26 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。

新しいゾーンのアクティベーション インターフェイスは、ソース ゾーンの設定に関係なく zone-name-only に設定されます。詳細については、P.5-37 の「アクティベーション方式の設定」を参照してください。

ゾーンのアトリビュートの設定

ゾーンを作成したら、ゾーンのアトリビュートを設定できます。

ゾーンのアトリビュートを設定するには、次の手順を実行します。

ステップ 1　ゾーン設定モードに入ります。すでにゾーン設定モードになっている場合、このステップは省略してください。

ゾーン設定モードに入るには、次のコマンドのいずれかを入力します。

- **conf** *zone-name*：グローバル モードから
- **zone** *zone-name*：設定モードまたはゾーン設定モードから

zone-name 引数には、既存のゾーンの名前を指定します。

ステップ 2　ゾーンの IP アドレスを定義します。Guard でゾーンのトラフィックをラーニングしてゾーンを保護できるようにするには、IP アドレスを定義する必要があります。

ゾーンの IP アドレスを設定するには、次のコマンドを入力します。

ip address *ip-addr* [*ip-mask*]

表 5-4 に、**ip address** コマンドの引数を示します。

表 5-4　ip address コマンドの引数

パラメータ	説明
ip-addr	ゾーンの IP アドレス。ゾーンは、サブネットでもかまいません。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.100.1）。
ip-mask	（オプション）IP サブネット マスク。サブネット マスクをドット区切り 10 進表記で入力します（たとえば 255.255.255.0）。デフォルトのサブネット マスクは、255.255.255.255 です。

ゾーン保護をアクティブにするには、IP アドレスを少なくとも 1 つ定義する必要があります。ゾーンの IP アドレスおよびサブセットはいつでも追加できます。

ゾーンの IP アドレスまたはサブセットを変更する場合は、次のタスクのいずれかを実行します。

- 新しい　IP　アドレスまたはサブネットが新しいサービスで構成され、そのサービスがゾーンのネットワークで定義されたことがない場合は、ゾーン保護をアクティブにする前にポリシー構築フェーズをアクティブにするか、サービスを手動で追加します。詳細については、P.5-16 の「ポリシーの構築」および P.7-14 の「サービスの追加」を参照してください。
- ゾーンが保護およびラーニング状態にある場合は、**no learning-params threshold-tuned** コマンドを使用して、ゾーン ポリシーに未調整のマークを付けます。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 Guard で攻撃が検出されなくなり、Guard 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。詳細については、P.5-26 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。
- ゾーンが保護およびラーニングの動作状態になく、保護およびラーニングの動作状態をアクティブにする予定がない場合は、しきい値調整フェーズをアクティブにしてから、ゾーン保護をアクティブにします。P.5-19 の「しきい値の調整」を参照してください。

ステップ 3　（オプション）Guard がゾーンに再び注入するトラフィックの帯域幅を、ゾーンで処理できると考えられるトラフィック レートに従って制限します。

次のコマンドを入力します。

rate-limit {**no-limit** | *rate burst-size rate-units*}

帯域幅の値は、ゾーンへの送信で測定された最大の帯域幅に設定することをお勧めします。この値が不明な場合は、デフォルトの帯域幅の値（無制限）のままにします。

表 5-5 に、**rate limit** コマンドの引数を示します。

表 5-5　rate limit コマンドの引数

パラメータ	説明
no-limit	ゾーンが無制限のレート リミットで定義されるよう指定します。
rate	ゾーンに通すことのできるトラフィック量を指定する、64 より大きな整数。単位は、*rate-units* 引数で指定されます。レートリミットは、最大でバーストリミットの 10 倍まで指定可能です。
burst	ゾーンに通すことのできるトラフィックの最大ピーク量を指定する、64 より大きな整数。単位は、*rate-units* 引数で指定されるレートの単位に応じて、ビット、キロビット、キロパケット、メガビット、またはパケットになります。バーストリミットは、最大でレートリミットの 8 倍まで指定可能です。
rate-units	レートの単位。次の単位があります。 • **bps**：ビット / 秒 • **kbps**：キロビット / 秒 • **kpps**：キロパケット / 秒 • **mbps**：メガビット / 秒 • **pps**：パケット / 秒

ステップ 4　（オプション）識別の目的で、ゾーンの説明を追加します。次のコマンドを入力します。

```
description string
```

文字列の長さは最大 80 文字です。

ゾーンの説明を変更するには、ゾーンの説明を再入力します。前の説明は新しい説明で上書きされます。

ステップ 5　新しく設定されたゾーンの設定を表示します。ゾーン設定モードで **show running-config** コマンドを使用します。

設定情報は、Guard を現在の設定値で設定するために実行される CLI コマンドで構成されています。詳細については、特定のコマンド エントリを参照してください。

次の例は、新しいゾーンを作成し、ゾーンのアトリビュートを設定する方法を示しています。

```
user@GUARD-conf# zone scannet
user@GUARD-conf-zone-scannet# ip address 192.168.100.34 255.255.255.252
user@GUARD-conf-zone-scannet# rate-limit 1000 2300 pps
user@GUARD-conf-zone-scannet# description Demonstration zone
```

ゾーン トラフィックの特性のラーニング

この項では、Guard 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、Guard がゾーン保護に使用するポリシーを作成および微調整する方法について説明します。

この項では、次のトピックについて取り上げます。

ラーニング プロセスの概要

ラーニング プロセスでは、Guard が通常のゾーン トラフィックの特性をラーニングします。Guard は、ラーニング プロセスの結果を使用してゾーン保護用のポリシーを作成します。これらのポリシーは、ゾーンのトラフィック フローの処理方法を Guard に指示します。

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 プロセスとゾーン保護を同時にアクティブにできます。Guard 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。

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。

詳細については、第 4 章「トラフィックの宛先変更の設定」を参照してください。

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。

1. ポリシー構築 : Guard 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。トラフィックが透過的に Guard を通過し、Guard は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、Guard のポリシー構築用ツールです。このテンプレートは、Guard が作成するゾーン ポリシーのタイプを定義します。また、ポリシー テンプレートは、Guard が厳密に監視するサービスの最大数と、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指針となる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します。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。

2. しきい値の調整 : Guard はゾーンのサービスのトラフィック レートに合せてポリシーを調整します。トラフィックが透過的に Guard を通過し、Guard はゾーン 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保護を同時にアクティブにすると（保護およびラーニング モード）、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を防止できます。Guard が常にポリシーを調整するように設定し、Guard 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。

（注）　Guard を保護およびラーニング モードでアクティブにすると、ゾーンのトラフィックが常に Guard に誘導されます。

Guard 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基準とし、悪意の攻撃となる可能性のあるあらゆる異常をトレースします。Guard は、ラーニング プロセス中は、現在のゾーン ポリシーを変更しません。Guard がポリシーを更新するのは、ラーニング フェーズのいずれかの段階における結果を受け入れるように指定した場合のみです。

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。

snapshot threshold-selection cur-thresholds コマンドを使用すると、現在のゾーン ポリシーをいつでもバックアップできます。詳細については、P.7-38 の「スナップショットの作成」を参照してください。

（注）　ラーニング プロセス中に Guard がパケットをドロップするのは、パケットに含まれている、送信元 IP アドレス、プロトコル番号、UDP 送信元ポートまたは宛先ポート、TCP 送信元ポートまたは宛先ポートのいずれかのフィールドが 0 である場合のみです。

ラーニング プロセスが完了する前にゾーンに対する攻撃があった場合、次の条件のいずれかに該当するときは、オンデマンド保護を使用してゾーンを保護します。

- ゾーンがラーニング プロセスの実行中である。
- Guard が保護およびラーニング モードになっているが、ゾーンのトラフィック特性をラーニングしていない。
- ゾーンのトラフィックを表さないと考えられるポリシーのしきい値を受け入れている。

詳細については、P.5-43 の「オンデマンド保護のイネーブル化」を参照してください。

複数のゾーンに対して同時に**ラーニング**関連のコマンドを発行できます。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 Guard 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。

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

Cisco Traffic Anomaly Detector（Detector）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 をアップデートするように設定できます。

Detector 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、Guard をアクティブにしてゾーンを保護します。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、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 に宛先変更されることがなくなります。

ラーニング プロセスの結果を Detector 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 を Detector のリモート Guard SSL リストのいずれかに追加します。
2. Detector との SSL 通信チャネルを確立します（P.3-24 の「SSL 通信チャネルの設定」を参照）。
3. Detector 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。

ゾーンの設定を Detector と同期させることや、Detector がゾーンの設定を Detector と自動的に同期させるように設定することができます。詳細については、P.5-29 の「Guard のゾーンの設定と Detector の同期」を参照してください。

このオプションを設定できるのは、Detector 上のみです。詳細については、『*Cisco Traffic Anomaly Detector Configuration Guide*』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では、Guard 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。トラフィックが透過的に Guard を通過し、Guard は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。ポリシー構築の指針となる規則を設定することもできます。たとえば、Guard 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します。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。

Guard 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 Guard が作成する新しいポリシーは、既存のポリシーを上書きします。

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

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　ポリシー構築フェーズを開始します。ゾーン設定モードで次のコマンドを入力します。

```
learning policy-construction
```

ヒント　Guard　がゾーンのトラフィックの宛先変更を実行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 details** 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、宛先変更に問題があることを示しています。

ステップ 2　（オプション）Guard 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.7-37 の「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」を参照してください。

ステップ 3　（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、Guard 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 Guard 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。このようにすると、ゾーンが最新のポリシーを持つと同時に、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。

Guard 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、次のコマンドを入力します。

```
learning accept
```

Guard 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.5-23 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 4　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。

ポリシー構築フェーズを終了する前に、少なくとも 2 時間はこのフェーズを続けることを推奨します。

次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**：Guard 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
  ```

  Guard 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**：Guard 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
  ```

Guard 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、ラーニング プロセスを開始する前のままになるか、ポリシー構築フェーズの結果を最後に受け入れる前のままになります。

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。例では、次に、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ます。

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

しきい値の調整

しきい値調整フェーズでは、Guard 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。

Guard 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。Guard は、ゾーンに対する攻撃を検出するとしきい値調整フェーズを停止しますが、ゾーン保護は継続します。この結果、Guard では悪意のあるトラフィックのしきい値がラーニングされなくなります。

攻撃が終了すると、Guard はラーニング プロセスを再開します。Guard は、攻撃の終了後、protection-end-timer によって定義された期間（ただし 10 分未満）待機してからラーニング プロセスを再度アクティブにします。詳細については、P.5-41 の「保護の無活動タイムアウトの設定」を参照してください。

（注）　しきい値調整フェーズは、トラフィックのピーク時（最も忙しい日）に、少なくとも 24 時間実行することを推奨します。

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　しきい値調整フェーズを開始します。

保護およびラーニング モードを開始すること、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 Guard がゾーンを保護するように設定することをお勧めします。ゾーン設定モードで次のコマンドを入力します。

```
protect learning
```

または、learning threshold-tuning コマンドと **protect** コマンドを順番に発行します（順序は問いません）。

ヒント　Guard　がゾーンのトラフィックの宛先変更を実行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 details** 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、宛先変更に問題があることを示しています。

Guard 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、ゾーン保護は継続します。

（注）　ゾーン宛てのトラフィックが通常の量のときに保護およびラーニング　モードを開始した場合、Guard 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。

- ポリシーのしきい値の状態を未調整に設定する。ゾーン設定モードで **learning-params threshold-tuned** コマンドを使用します。詳細については、P.5-26 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。
- ゾーン保護を非アクティブにし、継続してポリシーのしきい値をラーニングする。ゾーン設定モードで **no protect** コマンドを使用します。

ゾーン保護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　（オプション）Guard が調整中の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、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.7-37 の「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」を参照してください。

ステップ 3　Guard 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 Guard 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。このようにすると、ゾーンが最新のポリシーを持つと同時に、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。

Guard 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、次のコマンドを入力します。

```
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 5-7 を参照してください。

Guard 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.5-23 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 4　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。

ただし、Guard がゾーンのトラフィックを常に宛先変更している場合は、ゾーンを保護およびラーニング モードのままにして、しきい値調整フェーズを終了しない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**：Guard 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 5-7 を参照してください。

  Guard 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**：Guard 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

  この場合、Guard はしきい値調整フェーズを停止し、しきい値調整フェーズを開始する前のしきい値の状態に戻ります。その結果、新しく構築されたポリシーには、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。

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。例では、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@GUARD-conf-zone-scannet# learning threshold-tuning
user@GUARD-conf-zone-scannet# learning-params periodic-action auto-accept 0 1 0
user@GUARD-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.7-33 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、次のアクション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：Guard 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.7-24 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：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.7-25 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、Guard で実行できるラーニング関連のアクションと、指定したポリシーを Guard で処理する方法を設定できます。次のパラメータを定義できます。

- **periodic-action**：Guard が、ポリシーのスナップショットを保存してポリシーを自動的に受け入れるように設定できます。または、Guard がポリシーのスナップショットの保存だけを指定した間隔で実行するように設定できます。P.5-24 の「定期的なアクションの設定」を参照してください。
- **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、Guard はゾーンに対する攻撃を検出しません。P.5-26 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。
- **threshold-selection**：Guard 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。P.5-25 の「しきい値選択方式の設定」を参照してください。
- **fixed-threshold**：ポリシーのしきい値を固定値として設定します。Guard は、以後のしきい値調整フェーズでポリシーのしきい値を変更しません。P.7-24 の「固定値としてのしきい値の設定」を参照してください。

- **threshold-multiplier**：ポリシーのしきい値の固定乗数を設定します。Guard は、以後のしきい値調整フェーズで、現在のポリシーのしきい値、ラーニングしたしきい値、および固定乗数に基づいてポリシーのしきい値を計算します。P.7-25 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。

定期的なアクションの設定

Guard が、ポリシーのスナップショットを保存してポリシーを自動的に受け入れるように設定できます。または、Guard がポリシーのスナップショットの保存だけを指定した間隔で実行するように設定できます。スナップショットの詳細については、P.7-33 の「ポリシーの監視」を参照してください。

定期的なアクションを設定するには、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 5-6 で、**learning-params** コマンドの引数とキーワードについて説明します。

表 5-6　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	Guard 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。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	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。Guard 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*、*learn_params_hours*、および *learn_params_minutes* の合計となります。

次の例は、Guard 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@GUARD-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新しいポリシーのしきい値が受け入れられた後に、Guard 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 Guard が自動的に受け入れるように設定することもできます。

次のコマンドを入力します。

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

表 5-7 で、**learning-params threshold-selection** コマンドの引数とキーワードについて説明します。

表 5-7　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	Guard は、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	Guard は、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。
weighted *weight*	Guard は、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

この例は、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 Guard が受け入れるように設定する方法を示しています。

```
user@GUARD-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

Guard は、ポリシーのしきい値のステータス、つまりポリシーのしきい値が調整済みであるかどうかをマークします。保護およびラーニング モードのときは、このステータスに関連付けられます。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、Guard 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、Guard 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 Guard がスプーフィング防止メカニズムをすぐにアクティブにするように調整されています。Guard が保護およびラーニング モードの場合は、これによってラーニング プロセスが停止する可能性があります。このような状況を避けるため、Guard は、保護およびラーニング モードになっている場合にゾーンのポリシーが調整済みでないときは（つまり、ゾーンのポリシーが一度受け入れられるまでは）、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。

ゾーンのポリシーが未調整である場合、Guard は、しきい値選択方式 accept-new だけをアクティブにします（P.5-25 の「しきい値選択方式の設定」を参照）。Guard は、新しいしきい値を受け入れるときに以前のしきい値を無視します。これは、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るためです。

Guard 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

Guard 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入力します。

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してもかまいません。

- 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

次のいずれかの場合は、ゾーン ポリシーのステータスを未調整に変更してもかまいません。

- 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
- （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保護およびラーニング モードを開始していない場合

Guard は、現在のポリシーのしきい値に関連せず、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。

（注）　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 Guard で攻撃が検出されなくなり、Guard 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@GUARD-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保護のイネーブル化の同時実行

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、同時にゾーン保護をイネーブルにすることができます。Guard 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。この状態では、ポリシーのしきい値を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。

新しいゾーンを作成するとき、ゾーンのポリシーに対してサービスを追加または削除するとき、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、Guard 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。Guard がゾーンのポリシーを調整済みとしてマークするのは、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のみです。

ラーニング プロセスとゾーン保護を同時にイネーブルにする場合、ゾーンが調整済みでないときは、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、しきい値選択方式 accept-new だけをアクティブにします（P.5-25 の「しきい値選択方式の設定」を参照）。

Guard 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が、ゾーン保護は継続します。攻撃が終了すると、Guard は保護およびラーニングの動作状態に戻ります。

ラーニング プロセスとゾーン保護を同時にアクティブにするには、**protect learning** コマンドを使用するか、**learning threshold-tuning** コマンドと **protect** 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.5-19 の「しきい値の調整」および P.5-33 の「ゾーンの保護」を参照してください。

Guard のゾーンの設定と Detector の同期

ゾーンの設定とポリシーを Detector のゾーンと同期させることができます。Detector は、ゾーンの設定全体をコピーします。同期を使用すると、ゾーンを一度設定するだけで、Guard と Detector の両方で同じ設定とポリシーを維持できます。

Detector と Guard との通信には、認証と暗号化を提供する Secure Socket Layer（SSL）プロトコルが必要です。ゾーンを同期させる前に、SSL 通信接続チャネルを設定する必要があります。詳細については、P.3-23 の「Cisco Traffic Anomaly Detector との通信のイネーブル化」を参照してください。

Detector では、ゾーンのトラフィック特性を常にラーニングしてゾーンのポリシーを最新の状態に維持する一方で、ゾーンのトラフィックを常に Guard に宛先変更しなくても済むように設定できます。

同期のためのゾーンを作成して、ゾーンを Detector から同期させる必要があります。詳細については、『*Cisco Traffic Anomaly Detector Configuration Guide*』参照してください。

この項では、次のトピックについて取り上げます。

設定のガイドライン

Guard と Detector の間でゾーンを同期させる場合は、次のガイドラインを使用してください。

- Guard と Detector の間でゾーンを同期させるには、Guard と Detector の両方に適合したゾーン テンプレート（GUARD ゾーン テンプレート）を使用して、Detector 上に新しいゾーンを作成する必要があります。
- ゾーンのポリシーを適切に同期させるには、Guard（トラフィックを宛先変更しているとき）と Detector の両方に向かって同じタイプのトラフィックが流れるようにする必要があります。それ以外の場合は、ゾーンのグローバルポリシーが高すぎるか、または低すぎるため、スプーフィングを利用した DDoS 攻撃から適切に保護されることを保証できません。

- Detector を中央の設定ポイントとして使用します。Detector 上にゾーンを作成して、Detector の設定のバックアップを保守します。ゾーンの設定は、Detector から Guard にコピーします。
- デバイスを物理的に変更する場合や、Detector と Guard が通信に使用するインターフェイスの IP アドレスを変更する場合は、Detector と Guard が安全な通信に使用する SSL 証明書を再生成する必要があります。
- Guard 上でゾーンの設定を確認します。アクティベーション範囲が **ip-address-only** で、アクティベーション方式が **zone-name-only** でない場合は、**protection-end-timer** コマンドを使用して、ゾーンに対する攻撃が終了したことを Guard が識別するためのタイマーを設定することをお勧めします。**protection-end-timer** の値が **forever** の場合、Guard は、ゾーンに対する攻撃が終了したことを識別せず、特定の IP アドレスを保護するために作成したサブゾーンを削除しません。

サンプル シナリオ

次の設定プロセスの例は、同期を使用して、現在のトラフィック特性に応じてゾーンが保護されることを保証する方法を示しています。

1. GUARD ゾーン テンプレートのいずれかを使用して、Detector 上で新しいゾーンを作成および設定します。

   Guard では、ゾーン設定モードの **show** コマンドの出力に含まれているゾーン ID フィールドの隣にある *(Guard/Detector)* を表示して、これらのゾーンを識別します。
2. Detector 上で、ゾーンの SSL リモート Guard リストまたはデフォルトの SSL リモート Guard リストに Guard を追加します。
3. Detector がゾーンのポリシーを構築するように設定します。**learning policy-construction** コマンドを使用します。
4. Detector が、トラフィックの異常を検出しながら、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を調整するように設定します。**detect learning** コマンドを使用します。
5. ラーニングするポリシーのしきい値を Detector が 24 時間ごとに受け入れるように設定します。これにより、ゾーンのポリシーが、変化するトラフィック パターンで更新されることが保証されます。

6. ラーニングした新しいポリシーのしきい値を受け入れるたびに、Detector がゾーンの設定を Guard と同期させるように設定します。この設定により、Detector がゾーンのポリシーをラーニングする限り、Guard 上のゾーンのポリシーがアップデートされることが保証されます。
7. Guard をアクティブにしてゾーンを保護する前に、Detector がゾーンの設定を Guard 上の設定と同期させるように設定します。この設定により、Guard がゾーンを保護するときに、Guard 上のゾーンが最新の設定とポリシーを保持することが保証されます。
8. Detector は、ゾーンに対する攻撃を検出すると、次の処理を実行します。
   - Guard　上のゾーンの設定が、最新のものであることを確認する。Guard 上のゾーンの設定が Detector 上のゾーンの設定と同じものでない場合、Detector はゾーンの設定を同期させます。
   - Guard をアクティブにしてゾーンを保護する（Guard がゾーン保護をアクティブにします）。
   - ゾーンのラーニング プロセスを停止し、ゾーン トラフィックの異常の検出を継続する。この結果、Detector では悪意のあるトラフィックのしきい値がラーニングされなくなります。

   攻撃が進行中でも、Guard 上でゾーンのポリシーを変更できます。

   Detector は、Guard を常にポーリングします。攻撃が終了すると、Guard はゾーン保護を非アクティブにします。Detector は、Guard がゾーン保護を非アクティブにしたことを識別すると、追加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の動作状態を再度アクティブにします。
9. ゾーンのポリシーを攻撃の特性に合せて調整するために、Guard 上でゾーンのポリシーを手動で変更した場合は、Detector をその新しいポリシーに同期させることができます。このことは、ゾーン トラフィックによって、特定のポリシーのしきい値を固定値として設定することや、ポリシーのしきい値の固定乗数を設定することが必要になった場合に重要になります。このようにすると、Detector が以後のしきい値調整フェーズでポリシーのしきい値に正しく関連し、Guard のポリシーが正しいしきい値で更新されることが保証されます。

   詳細については、P.7-24 の「固定値としてのしきい値の設定」および P.7-25 の「しきい値の乗数の設定」を参照してください。

   この操作は、Detector からのみ実行できます。詳細については、『*Cisco Traffic Anomaly Detector Configuration Guide*』を参照してください。

ゾーン設定のオフラインでの同期

ゾーンの設定は、Guard と Detector の間に安全な通信チャネルを確立できない場合でも同期させることができます。次のいずれかの場合は、ゾーン設定をオフラインで同期させることが必要になる場合があります。

- Guard が Detector にアクセスできない場合
- Detector が Guard にアクセスできない場合
- Detector が、Network Address Translation（NAT; ネットワーク アドレス変換）デバイス経由で Guard と通信する場合

ゾーンの設定をオフラインで同期させるには、まずゾーンの設定を Detector から FTP サーバまたはセキュア FTP （SFTP）サーバにエクスポートして、次にゾーンの設定を Guard に手動でインポートする必要があります。

Guard と Detector の間に安全な通信チャネルがないため、Detector がゾーンのトラフィックの異常を検出したときは、Guard を手動でアクティブにしてゾーンを保護する必要があります。

詳細については、P.5-33 の「ゾーンの保護」を参照してください。

Guard がゾーンの設定を同期できるようにするには、Detector 上で、GUARD ゾーン テンプレートのいずれかを使用してゾーンを作成する必要があります。

ゾーンの設定をオフラインで同期させるには、次の手順を実行します。

ステップ 1　ゾーン設定をソース デバイスからエクスポートします。

copy zone *zone-name* **running-config ftp** コマンドを使用します。P.11-2 の「設定のエクスポート」を参照してください。

ステップ 2　ゾーンの設定を FTP または SFTP サーバからターゲット デバイスにインポートします。**copy ftp running-config** コマンドまたは **copy sftp running-config** コマンドを使用します。

ゾーン設定をインポートする前に、ゾーンを非アクティブにすることをお勧めします。詳細については、P.11-4 の「設定のインポートとアップデート」を参照してください。

ゾーンの保護

ゾーン保護をアクティブにする前に、Guard でゾーンのトラフィック パターンをラーニングすることをお勧めします。ラーニング プロセスにより、Guard で各ゾーンのトラフィック パターンをラーニングし、ゾーン トラフィックの統計分析に従って推奨のしきい値のセットを作成することができます。または、ポリシーを含むゾーンの設定を Cisco Traffic Anomaly Detector（Detector）から同期させることもできます。ゾーンの IP アドレス範囲が重なっていなければ、複数のゾーンを同時に保護できます。

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。

詳細については、第 4 章「トラフィックの宛先変更の設定」を参照してください。

ゾーンが攻撃を受けていない間は、Guard を 保護およびラーニング モードでアクティブにすることができます。Guard は、ゾーンのトラフィックを常に宛先変更し、ポリシーのしきい値を調整します。詳細については、P.5-13 の「ゾーン トラフィックの特性のラーニング」を参照してください。

次の保護特性を定義できます。

- **動作モード**：Guard　がゾーン保護手段を自動的に適用するか、インタラクティブ方式で適用するかを定義します。
- **アクティベーション方式**：ゾーンをアクティブにするときに、ゾーン名、ゾーンのアドレス範囲、または受信トラフィックのいずれに従うかを定義します。アクティベーション方式を設定することは、ゾーン保護が外部デバイス（Detector など）によってアクティブにされる場合は重要です。
- **アクティベーション範囲**：ゾーン保護を、ゾーンのアドレス範囲全体についてアクティブにするか、ゾーン内の特定の IP アドレスに限定してアクティブにするかを定義します。アクティベーション範囲は、外部デバイスによってゾーン保護がアクティブにされたゾーンだけに適用されます。
- **保護の終了のタイムアウト**：Guard がゾーン保護を終了するまでのタイムアウトを定義します。

この項では、次のトピックについて取り上げます。

- 保護の動作モードの定義
- アクティベーション方式の設定
- アクティベーション範囲の設定
- 保護の無活動タイムアウトの設定

ゾーン保護のアクティブ化

外部（Cisco Traffic Anomaly Detector やその他の手段）から攻撃の兆候が示されてから Guard を設定してゾーンを保護することも、ゾーンの設定後すぐにゾーンを保護するように Guard に指示することもできます。Guard は、ゾーンを保護するときにゾーンのトラフィックを Guard に宛先変更し、保護ポリシーを適用します。

Guard がゾーンのトラフィック特性をラーニングし終わる前にゾーンが攻撃を受けた場合は、オンデマンドの保護を使用してゾーンを保護してください。新しいゾーンに対する Guard のデフォルトのしきい値を使用すると、効果的なオンデマンド保護を実行できます。詳細については、P.5-43 の「オンデマンド保護のイネーブル化」を参照してください。

（注）　Guard　が受信したトラフィックに従ってゾーン保護をアクティブにするように設定する場合は、ゾーンのトラフィックを手動で Guard に宛先変更する必要があります。

ゾーン保護は、次の方法のいずれかでアクティブにできます。

- ゾーン全体の保護。ゾーン設定モードで次のコマンドを入力します。

  protect [**learning**]

  learning キーワードは、Guard がゾーンを保護してポリシーのしきい値を調整するように設定します。詳細については、P.5-19 の「しきい値の調整」を参照してください。

  次の例を参考にしてください。

  ```
  user@GUARD-conf-zone-scannet# protect
  ```

- ゾーンのアドレス範囲の一部である、IP が特定されたゾーンの保護。この場合は、Guard により、新しいゾーンが作成されます。新しいゾーンの名前は、元になるゾーンの最初の 30 文字と、アンダースコアで連結された特定の IP アドレスで構成されます。同じ名前のゾーンがすでに存在する場合、Guard は同じ名前の別のゾーンを作成せず、既存のゾーンに対する保護をアクティブにします。

  IP が特定されたゾーンについてゾーン保護をアクティブにするには、グローバル モードで次のコマンドを入力します。

  protect *zone-name ip-address-general*

  zone-name 引数には、特定のゾーンの名前を指定し、*ip-address-general* 引数には、ゾーンのアドレス範囲内の特定の IP アドレスを指定します。IP アドレスをドット区切り 10 進表記で入力します。たとえば、192.168.5.6 です。

  このゾーンを削除するには、**zone** コマンドの no 形を使用します。

  次の例を参考にしてください。

  ```
  user@GUARD# protect scannet 192.168.5.6
  creating zone scannet_192.168.5.6
  user@GUARD#
  ```

- 特定の IP アドレスの保護。グローバル モードで次のコマンドを入力します。

  protect *ip-address-general* [*subnet-mask*]

  ip-address-general 引数には、ゾーンのアドレス範囲内にある特定の IP アドレスを指定します。IP アドレスをドット区切り 10 進表記で入力します。たとえば、192.168.5.6 です。Guard は、IP アドレス アクティベーション方式に従ってゾーン保護をアクティブにします。詳細については、P.5-39 の「アクティベーション範囲の設定」を参照してください。

複数のゾーンに対して同時に**保護**関連のコマンドを発行できます。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ゾーン保護を停止する場合は、グローバル モードで **no protect *** コマンドを入力します。名前が *scan* で始まるゾーン（scannet や scanserver など）すべてについてゾーン保護を停止する場合は、グローバル モードで **no protect** *scan** コマンドを入力します。

ヒント　Guard がゾーンのトラフィックを受信していることを確認してください。ゾーン保護をアクティブにしてから少なくとも 10 秒待って、**show rates** コマンドを発行します。レートのうち少なくとも 1 つの値がゼロより大きいことを確認します。すべてのレートの値がゼロの場合は、宛先変更に問題があることを示しています。

ゾーン保護の非アクティブ化

ゾーンに対する攻撃がなく、ゾーンのトラフィック異常の検出を他のソースに依存しているときは、ゾーン保護を非アクティブにして、Guard へのトラフィックの宛先変更を終了することができます。

ゾーン保護を非アクティブにするには、ゾーン設定モードで次のコマンドのいずれかを入力します。

- **no protect**：ゾーン保護を終了します。ゾーンが保護およびラーニング モードの場合、Guard はポリシーのしきい値のラーニングを継続します。
- **deactivate**：ゾーン保護と、ラーニング プロセスのしきい値調整フェーズの両方を終了します。

保護の動作モードの定義

Guard の保護は、次の 2 つの動作モードにおいてアクティブにできます。

- 自動保護モード：動的フィルタはユーザの操作なしでアクティブになります。これはデフォルトの動作モードです。
- インタラクティブ保護モード：動的フィルタは、インタラクティブ モードにおいて手動でアクティブになります。動的フィルタは推奨事項としてグループ化され、ユーザの決定を待ちます。ユーザは、これらの推奨事項を確認して、どの推奨事項を受け入れるか、無視するか、自動アクティベーションに切り替えるかを決定できます。

詳細については、第 8 章「インタラクティブ保護モード」を参照してください。

アクティベーション方式の設定

アクティベーション方式は、外部からの攻撃の兆候を受信したときに、ゾーン保護をアクティブにするゾーンを Guard がどのように識別するかを定義します。この兆候には、外部デバイス（Cisco Traffic Anomaly Detector など）からのコマンドや、ゾーンを宛先とするトラフィック（パケット）があります。

Guard は、次のアクティベーション方式をサポートします。

- **ゾーン名**：Guard は、ゾーン名に基づいてゾーン保護をアクティブにします。ゾーン保護をアクティブにする外部からの兆候には、ゾーン名が含まれている必要があります。これはデフォルトのアクティベーション方式です。
- **IP アドレス**：Guard は、宛先変更されたトラフィックから抽出する情報に基づいて、ゾーン保護をアクティブにします。Guard は、ゾーンの一部である IP アドレスまたはサブネットで構成された外部からの攻撃の兆候を受信した場合に、ゾーン保護をアクティブにします。Guard はゾーンのデータベースをスキャンし、受信 IP アドレスまたはサブネットを含むアドレス範囲を持つゾーンをアクティブにします。受信 IP アドレスを含むアドレス範囲を持つ複数のゾーンが設定されている場合、Guard は、プレフィックスが最も長く一致するゾーンをアクティブにします。つまり、受信 IP アドレスを含むアドレス範囲が最も限定的なゾーンがアクティブになります。受信 IP アドレスまたはサブネットは、ゾーンの IP アドレス範囲に完全に含まれている必要があります。

注意　IP アドレスまたはパケットのアクティベーション方式を使用して、同じアドレス範囲を持つ複数のゾーンを設定しないでください。

- **パケット（トラフィック）**：Guard は、ゾーン宛てのトラフィックを受信したときにゾーン保護をアクティブにします。Guard はゾーンのデータベースをスキャンし、受信パケットの IP アドレスを含むアドレス範囲を持つゾーンをアクティブにします。受信パケットの IP アドレスを含むアドレス範囲を持つ複数のゾーンが設定されている場合、Guard は、プレフィックスが最も長く一致するゾーンをアクティブにします。つまり、受信パケット IP アドレスを含むアドレス範囲が最も限定的なゾーンがアクティブになります。受信 IP アドレスまたはサブネットは、ゾーンの IP アドレス範囲に完全に含まれている必要があります。

Guard がゾーン保護をアクティブにするのは、単一 IP アドレス宛ての受信トラフィックのレートが、アクティベーションの詳細度よりも高い場合のみです。アクティベーションの詳細度はグローバルに定義され、すべてのゾーンに適用されます。

ゾーン保護をアクティブにするのに必要な最小パケット レートを変更するには、設定モードで次のコマンドを入力します。

protect-packet activation-sensitivity *min-rate*

min-rate 引数には、Guard がゾーンに対してゾーン保護をアクティブにする原因となる、単一のゾーン宛先 IP アドレス宛ての最小パケットレートを定義します。デフォルトは 0 pps です。

（注）　アクティベーション範囲がパケットである場合や、Guard でゾーンのトラフィックを監視できない場合は、外部デバイスを使用して、ゾーンのトラフィックを手動で Guard に宛先変更する必要があります。

- **IP アドレスまたはパケット**：Guard は、ゾーンを宛先とするトラフィック（パケット）を受信した場合、またはゾーンのアドレス範囲の一部である IP アドレスまたはサブネットで構成される外部からの攻撃の兆候を受信した場合に、ゾーン保護をアクティブにします。詳細については、上記の箇条書きの **IP アドレス**と**パケット（トラフィック）**の項を参照してください。

アクティベーション方式が **zone-name-only** でない場合、Guard は、ゾーンのアクティベーション範囲に従って、ゾーン全体または指定された IP アドレス範囲をアクティブにします（P.5-39 の「アクティベーション範囲の設定」を参照）。

アクティベーション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入力します。

activation-interface {**packet** | **ip-address** | **packet-or-ip-address** | **zone-name-only**}

デフォルトは zone-name-only です。ゾーンを複製する場合（P.5-7 の「ゾーンの複製」を参照）、アクティベーション インターフェイスは、ソース ゾーンの設定にかかわらずデフォルトに設定されます。

（注）　アクティベーション範囲が **ip-address-only** で（P.5-39 の「アクティベーション範囲の設定」を参照）、アクティベーション方式が **zone-name-only** でない場合は、**protection-end-timer** コマンドを使用して、ゾーンに対する攻撃が終了したことを Guard が識別するためのタイマーを設定することをお勧めします（P.5-41 の「保護の無活動タイムアウトの設定」を参照）。**protection-end-timer** の値が **forever** の場合、Guard は、ゾーンに対する攻撃が終了したことを識別せず、特定の IP アドレスを保護するために作成したサブゾーンを削除しません。

受信 IP アドレスまたはパケットが他のどのゾーンの一部でもない場合に備えて、保護のための Guard のデフォルト ゾーンを作成することができます。そのようなゾーンを定義できるのは、ネットワークが同種であるために、同じゾーン テンプレートを使用できる場合のみです。そのゾーンに対してラーニング プロセスを実行することはできません。IP アドレスが 0.0.0.0 で、サブネットが 0.0.0.0 のゾーンを作成します。アクティベーション範囲を ip-address として定義します（P.5-39 の「アクティベーション範囲の設定」を参照）。

ゾーンのアクティベーション方式を表示するには、**show running-config** コマンドを使用します。

アクティベーション範囲の設定

アクティベーション範囲は、Guard が外部からの攻撃の兆候を受信した場合に、ゾーン全体またはゾーンの一部に対してゾーン保護をアクティブにするかどうかを定義します。この兆候には、外部デバイス（Cisco Traffic Anomaly Detector など）からのコマンドや、ゾーンを宛先とするトラフィック（パケット）があります。

Guard は、次のアクティベーション範囲をサポートします。

- **ゾーン全体**：ゾーン全体についてゾーン保護をアクティブにします。Guard は、ゾーンを宛先とするトラフィックを受信した場合、またはゾーンの一部である IP アドレスまたはサブネットで構成される外部からの攻撃の兆候を受信した場合に、ゾーン保護をアクティブにします。
- **IP アドレスのみ**：指定した IP アドレスまたはサブネットに限定してゾーン保護をアクティブにします。Guard は、ゾーンを宛先とするトラフィックを受信した場合、またはゾーンの一部である IP アドレスまたはサブネットで

構成される外部からの攻撃の兆候を受信した場合、新しいゾーン（サブゾーン）を作成します。これはデフォルトのアクティベーション範囲です。詳細については、P.5-40 の「サブゾーンについて」を参照してください。

アクティベーション範囲を設定するには、ゾーン設定モードで次のコマンドを入力します。

activation-extent {**entire-zone** | **ip-address-only**}

デフォルトは ip-address-only です。

ゾーンのアクティベーション範囲を表示するには、**show running-config** コマンドを使用します。

サブゾーンについて

ゾーンの一部（ソース ゾーンのすべての IP アドレス範囲を含まないゾーン）に対してゾーン保護をアクティブにした場合、Guard はサブゾーンを作成します。サブゾーンの IP アドレス範囲は、ソース ゾーンのアドレス範囲に含まれます。

サブゾーンの設定は、IP アドレスと名前を除いて、ソース ゾーンの設定と同じです。サブゾーンの名前は、ソース ゾーン名の最初の 30 文字と、アンダースコアで連結された IP アドレスおよびサブネットで構成されます。サブゾーンが単一の IP アドレスで構成される場合、サブネットは追加されません。たとえば、ソース ゾーンの名前が *scannet* で、アドレス範囲 *10.10.10.0* とサブネット *255.255.255.0* を持つとき、Guard が IP アドレス *10.10.10.192* の内部範囲およびサブネット *255.255.255.252* に対してゾーン保護をアクティブにする場合、サブゾーンの名前は *scannet_10.10.10.192_255.255.255.252* となります。

サブゾーンの IP アドレスおよびサブネットは、Guard が外部からの攻撃の兆候で受信したもの、または Guard がゾーン保護をアクティブにする原因となったパケットの IP アドレスです。

サブゾーンに対するゾーン保護が終了すると、Guard はサブゾーンを消去しますが、サブゾーンのログおよび攻撃レポートは消去しません。サブゾーンのゾーン保護を終了する方法は、通常のゾーンのゾーン保護を終了する方法と同じで、アクティベーション方式と保護の終了のタイムアウトに従います。

Guard がサブゾーンを消去した後にサブゾーンのログおよびレポートを表示するには、次のコマンドを使用します。

- **show log** *sub-zone-name*：詳細については、P.10-2 の「Guard の設定の表示」を参照
- **show reports** *sub-zone-name* [*report-id* | **current**] [**details**]：詳細については、P.9-14 の「攻撃レポートの表示」を参照

サブゾーンのリストを表示するには、コマンドを入力し、Tab キーを押します。

保護の無活動タイムアウトの設定

Guard は、ゾーンに対する攻撃が終了したことを識別したときに、保護およびラーニング モードをアクティブまたは非アクティブにできます。Guard は、ゾーンを保護している場合、ゾーンが攻撃を受けなくなった時点でゾーン保護を終了します。Guard は、保護およびラーニング モードである場合、攻撃が検出されるとラーニング プロセスを非アクティブにし、ゾーンが攻撃を受けなくなった時点でラーニング プロセスを再開します。

Guard は、ゾーンに対する攻撃が終了したかどうかを無活動タイムアウトに従って確認します。このタイムアウトは、数秒から無限まで定義できます。

無活動タイムアウトを定義するには、次のコマンドを入力します。

protection-end-timer {*time-seconds* | **forever**}

表 5-8 に、**protection-end-timer** コマンドの引数とキーワードを示します。

表 5-8　protection-end-timer コマンドの引数とキーワード

パラメータ	説明
time-seconds	タイムアウト（秒単位）。61 以上の整数を入力します。
forever	無限のタイムアウト。

デフォルトは **forever** です。デフォルト値を変更しない場合は、ゾーン保護を手動で非アクティブにする必要があります。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# protection-end-timer 300
```

Guard は、動的フィルタの無活動およびドロップされたトラフィックに基づいて無活動を測定します。事前定義された期間中に、使用中になった動的フィルタがなく、次の両方の条件に該当している場合、Guard はゾーンに対する攻撃が終了したものと見なします。

- 新しい動的フィルタが追加されていない：動的フィルタを削除するタイミングを Guard がどのように決定するかについては、P.6-36 の「動的フィルタの非アクティブ化」を参照してください。
- ドロップされているゾーン トラフィックのレートが、定義済みのしきい値よりも低い：Guard は、保護メカニズム（動的フィルタ、フレックス コンテンツ フィルタ、レート リミッタ モジュール）が攻撃の一部と見なしたゾーン パケットをドロップします。ドロップされるパケットは、ゾーンの Dropped カウンタを使用してカウントされます（詳細については、P.10-4 の「ゾーンのカウンタの表示」を参照）。デフォルトのしきい値は 1 pps です。ドロップ カウンタのしきい値を変更するには、ゾーン設定モードで次のコマンドを入力します。

  attack-detection zone-malicious-rate *threshold*

  threshold 引数には、ドロップされるゾーン パケットの最小レートを定義します。レートがこのしきい値より低くなった場合、Guard はゾーン保護を終了することがあります。

ゾーンのアクティベーション方式が **Packet** である場合、Guard はゾーンを非アクティブにする前に、受信したトラフィックに基づいて無活動をチェックします。Guard が保護を非アクティブにするのは、上の条件に該当し、ゾーン宛てのパケットをまったく受信しなかった場合のみです。

オンデマンド保護のイネーブル化

ゾーンが攻撃にさらされている場合など、緊急を要する場合には、ラーニング プロセスを実行せずにゾーンを保護することができます。システム定義のゾーン テンプレートには、ラーニング プロセスが完了していないゾーンの保護に適した定義済みの保護ポリシーとユーザ フィルタが含まれています。これらのゾーン 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 Guard がスプーフィング防止メカニズムをすぐにアクティブにするように調整されています。

Guard はゾーンのトラフィック パターンについての知識を持たないため、送信元 IP アドレスをブロック（ドロップ）するために使用されるしきい値は、比較的高い値に設定されています。つまり、オンデマンド保護では、スプーフィングを利用しない攻撃を軽減する場合にはユーザの介入が必要になります。ゾーンの正当なトラフィックと悪意のあるトラフィックのレートを監視して、Guard の軽減アクションを確認する必要があります。

次のいずれかの場合は、ゾーンに対してオンデマンド保護が必要になる場合があります。

- ゾーンがラーニング プロセスの実行中である。
- Guard が保護およびラーニング モードになっているが、ゾーンのトラフィック特性をラーニングしていない。
- ゾーンのトラフィックを表さないと考えられるポリシーのしきい値を受け入れている。

オンデマンド保護を開始するには、次の手順を実行します。

ステップ 1　新しいゾーンを作成します。次のコマンドを入力します。

```
zone new-zone-name [template-name] [interactive]
```

詳細については、P.5-4 の「新しいゾーンの作成」を参照してください。

ステップ 2　ゾーンの IP アドレスを定義します。次のコマンドを入力します。

```
ip address ip-addr [ip-mask]
```

詳細については、P.5-9 の「ゾーンのアトリビュートの設定」を参照してください。

ステップ 3　ゾーン保護をアクティブにします。次のコマンドを入力します。

```
protect
```

詳細については、P.5-33 の「ゾーンの保護」を参照してください。

ステップ 4　ゾーンのトラフィック パターンを分析します。詳細については、第 12 章「Guard による軽減の分析」を参照してください。