ゾーンの設定

この章では、Cisco Traffic Anomaly Detector Module（Detector モジュール）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、ゾーン検出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、Detector モジュールで DDoS 攻撃の監視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。Detector モジュールは、DDoS 攻撃を発見すると、リモートの Guard を自動的にアクティブにしてゾーンを攻撃から保護するか、手動で Guard をアクティブにするようにユーザに通知することができます。Detector モジュールでは、ゾーンのネットワーク アドレス範囲が互いに重複していない場合に限り、複数のゾーンのトラフィックを同時に分析できます。

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 トラフィックを必要な検出レベルに誘導し、Detector モジュールが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：ゾーンの検出ポリシーを作成します。このポリシーにより、Detector モジュールは、特定のトラフィック フローを分析し、そのトラフィック 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.5-12 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。

新しいゾーンは、次の 2 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。

ゾーンの設定内容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**]：Detector モジュールによって新しいゾーンが作成されます。*template-name* 引数を挿入しない場合、新しいゾーンは DETECTOR_DEFAULT ゾーン テンプレートから作成されます。
- **zone** *zone-name* [*template-name*] [**interactive**]：Detector モジュールによって既存のゾーンが削除され、同じ名前で新しいゾーンが作成されます。

システム定義のゾーン テンプレートを使用する場合、Detector モジュールによって、すべてのゾーン アトリビュートにデフォルト設定が適用されます。

コマンドが正常に実行されると、Detector モジュール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、Detector モジュールは、指定したゾーンの設定モードに入ります。

表 5-1 で、**zone** コマンドの引数とキーワードについて説明します。

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、DETECTOR_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。
interactive	インタラクティブにゾーン検出を実行するように Detector モジュールを設定します。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「インタラクティブ検出モード」を参照してください。

Detector モジュールには、次のプレフィックスを持つ 2 つのゾーン テンプレート セットが含まれています。

- DETECTOR_ : Detector モジュール専用に設計されたゾーン テンプレート。ゾーン設定を Cisco Anomaly Guard Module と共有しない場合は、DETECTOR_ バージョンのゾーン テンプレートを選択します。
- GUARD_ : Detector モジュールと Cisco Anomaly Guard Module 用に設計されたゾーン テンプレート。ゾーン設定を Cisco Anomaly Guard Module と同期させる場合は、GUARD_ バージョンのゾーン テンプレートを選択します。

  これらのテンプレートから作成されたゾーンを設定する方法の詳細については、P.5-32 の「同期用のゾーンの設定」を参照してください。

表 5-2 で、ゾーン テンプレートについて説明します。

表 5-2　ゾーン テンプレート

テンプレート	説明
DETECTOR_DEFAULT	デフォルトのゾーン テンプレート。このゾーン テンプレートを使用してゾーンを作成した場合、ゾーンに対する TCP ワーム攻撃は検出できません。
DETECTOR_WORM	ゾーンに対する TCP ワーム攻撃の検出が可能になるゾーン テンプレート。
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検出用に設計されたゾーン テンプレート。これらのゾーン テンプレートによって定義されたゾーンに対しては、ラーニング プロセスを行わずにゾーン検出をアクティブにすることができます。このようなゾーンは、protect-ip state を dst-ip-by-name にして定義することをお勧めします。詳細については、P.5-53 の「Guard 保護のアクティベーション方式の設定」を参照してください。 ゾーンへのトラフィック レートが指定のレートを超えると Detector モジュールがゾーンに対する攻撃を識別するように、ポリシーのしきい値が調整されます。 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。 **DETECTOR_LINK_128K** **DETECTOR_LINK_1M** **DETECTOR_LINK_4M** **DETECTOR_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。

表 5-2　ゾーン テンプレート（続き）

テンプレート	説明
Guard ゾーン テンプレート	Guard モジュールとのゾーン設定の同期をイネーブルにするために設計されたゾーン テンプレート。これらのテンプレートから作成されたゾーンに Detector モジュールと Guard モジュールの両方のアトリビュートを設定して、ゾーン設定を Guard モジュールにコピーできます。Guard ゾーン テンプレートは次のとおりです。 • **GUARD_DEFAULT**：Guard モジュールのデフォルトのゾーン テンプレート。 • **GUARD_LINK** テンプレート：帯域幅のわかっているゾーン用に設計されたテンプレート。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 **GUARD_LINK_128K**、**GUARD_LINK_1M**、**GUARD_LINK_4M**、および **GUARD_LINK_512K** が用意されています。 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。GUARD_LINK ゾーン テンプレートから作成されたゾーンに対しては、しきい値調整フェーズを実行せずにゾーン検出をアクティブにすることができます。このようなゾーンは、protect-ip-state を dst-ip-by-name にして定義することをお勧めします。 • **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テンプレート。このテンプレートは、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。

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@DETECTOR-conf# zone scannet interactive
user@DETECTOR-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.7-44 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@DETECTOR-conf-zone-scannet# zone mailserver copy-from-this
user@DETECTOR-conf-zone-mailserver#
```

コマンドが正常に実行されると、Detector モジュール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.5-25 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 モードから入力
- **zone** *zone-name*：設定モードまたはゾーン設定モードから入力

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。Detector モジュールでゾーン トラフィックのラーニングとゾーンの検出をイネーブルにするには、ゾーンの 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 で、**ip address** コマンドの引数について説明します。

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。

ゾーン検出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ていない場合は、ゾーン検出をアクティブにする前にポリシー構築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.5-15 の「ポリシーの構築」および P.7-15 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 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。詳細については、P.5-25 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。
- ゾーンが検出およびラーニングの動作状態になく、検出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、ゾーン検出をアクティブにします。P.5-18 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）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 4　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、Detector モジュール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@DETECTOR-conf# zone scannet
user@DETECTOR-conf-zone-scannet# ip address 192.168.100.34
255.255.255.252
user@DETECTOR-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、Detector モジュールのラーニング プロセスを使用して、ゾーンのトラフィック特性を分析し、Detector がゾーンの検出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、Detector 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。Detector モジュールは、ラーニング プロセスの結果を使用して、ゾーン検出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 Detector 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同時に、ポリシーのしきい値を監視してトラフィック異常がないか調べます。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.2-5 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。

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：Detector 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 Detector を通過し、Detector 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、Detector のポリシー構築用ツールです。このテンプレートは、Detector 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 が厳密に監視するサービスの最大数と、Detector 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：Detector 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 Detector を通過し、Detector はゾーン ポリシー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検出を同時にアクティブにして（検出およびラーニング モード）、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ないようにすることができます。Detector が常にポリシーを調整するように設定し、Detector 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 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。Detector 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。Detector 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.7-40 の「スナップショットの作成」を参照してください。

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。したがって、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。

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 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。

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

ゾーン トラフィックを常にラーニングし、ゾーン ポリシーで Cisco Anomaly Guard Module（Guard モジュール）をアップデートするように、Detector モジュールを設定できます。

Detector モジュールは、ゾーンに対する攻撃を検出すると、ラーニング プロセスを停止し、Guard モジュール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、ゾーンのポリシーしきい値を継続的に調整できる一方で、ゾーン トラフィックを常に Guard モジュールに宛先変更することを回避できます。

ラーニング プロセスの結果と Guard モジュールを同期させるには、次のタスクを実行する必要があります。

1. Guard モジュールを Detector モジュールのリモート Guard SSL リストのいずれかに追加する（P.5-45 の「リモート Guard のアクティブ化」を参照）
2. Guard モジュールとの SSL 通信チャネルを確立する（P.4-24 の「SSL 通信チャネルの設定」を参照）
3. GUARD ゾーン テンプレートを使用して、Detector モジュールにゾーンを作成する（P.5-3 の「新しいゾーンの作成」を参照）

ゾーン設定を Guard モジュールと同期させることも、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.5-28 の「Detector モジュールと Guard モジュール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では、Detector 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 Detector を通過し、Detector 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。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、Detector 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。

Detector 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を設定する方法については、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 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（DETECTOR_LINK_128K、DETECTOR_LINK_1M、DETECTOR_LINK_4M、GUARD_LINK_512K、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　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.2-5 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 2　（オプション）Detector　モジュールが構築している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.7-40 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、Detector 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 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。

Detector 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
```

Detector 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.5-22 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**：Detector 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 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 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 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@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
```

しきい値の調整

しきい値調整フェーズでは、Detector 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。

最後に受け入れたポリシーしきい値を監視してトラフィック異常がないか調べながらゾーン トラフィックをラーニングするように Detector モジュールを設定できます。Detector モジュールは、ゾーンに対する攻撃を検出すると、しきい値調整フェーズを停止しますが、ゾーンの検出は続行します。この結果、Detector モジュール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。

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

（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。

検出およびラーニング 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 Detector がゾーンを検出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。

```
detect learning
```

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

ヒント　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.2-5 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。

Detector モジュールは、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、ゾーンの検出は続行します。

（注）　ゾーンへのトラフィックが中程度のときに検出およびラーニング　モードを開始した場合、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。

- 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.5-25 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。
- ゾーン検出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 detect** コマンドを使用します。

ゾーン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　（オプション）Detector モジュールが調整している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.7-40 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　Detector 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 Detector 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。

Detector 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 5-6 を参照してください。

Detector 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.5-22 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。

ゾーンを検出およびラーニング 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**：Detector 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 5-6 を参照してください。

  Detector 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 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、Detector 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@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.7-36 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：Detector 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：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 パラメータでは、Detector モジュールが実行できるラーニング関連のアクション、および Detector モジュールが指定のポリシーを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**：指定した間隔で、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 Detector モジュールを設定することも、ポリシーのスナップショットの保存だけを行うように Detector モジュールを設定することもできます。P.5-23 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。ゾーンのポリシーに調整済みのマークが付いていない場合、Detector モジュールは、ゾーンに対する攻撃を検出しません。P.5-25 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**：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た後に、新しいポリシーしきい値の生成に使用するデフォルトの方式を設定します。P.5-24 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。Detector モジュールは、将来のしきい値調整フェーズでポリシーしきい値を変更しません。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。
- **threshold-multiplier**：ポリシーのしきい値の固定乗数を設定します。Detector モジュールは、現在のポリシーしきい値、ラーニングされたしきい値、および固定乗数に基づいて、将来のしきい値調整フェーズでポリシーしきい値を計算します。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

指定した間隔で、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 Detector モジュールを設定することも、ポリシーのスナップショットの保存だけを行うように Detector モジュールを設定することもできます。スナップショットの詳細については、P.7-36 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 5-5 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 5-5　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 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 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 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、*1 時間*ごとにポリシーを受け入れるように Detector モジュールを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新しいポリシーしきい値が受け入れられた後に、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、指定した間隔でしきい値調整フェーズの結果を自動的に受け入れるように Detector モジュールを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 5-6 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 5-6　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	Detector モジュールは、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	Detector モジュールは、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*	Detector モジュールは、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

次の例は、ラーニングされたしきい値が現在のポリシーしきい値よりも大きい場合に、提案されたポリシーを受け入れるように Detector モジュールを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、ポリシーしきい値のステータスのマーク、つまりポリシーしきい値が調整済みであるかどうかのマークを付けます。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。ポリシーしきい値のステータスは、ポリシーしきい値の超過が発生した場合に Detector モジュールがゾーンに対する攻撃を識別するかどうかを示します。

新しいゾーンが作成される場合、またはゾーンのポリシー構築フェーズの結果を受け入れた後、Detector モジュールは、ゾーンのポリシーしきい値に未調整のマークを付けます。ゾーン テンプレートのデフォルトのしきい値は、Detector モジュールがゾーン トラフィックに異常を発見した場合に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。このため、Detector モジュールが保護およびラーニング モードである場合、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に、Detector モジュールは、保護およびラーニング モードであり、ゾーン ポリシーが未調整である場合（つまり、ゾーンのポリシーしきい値が一度受け入れられるまで）、ゾーン トラフィック内の攻撃を検出しません。

ゾーン ポリシーが未調整である場合、Detector モジュールは、accept-new しきい値選択方式だけをアクティブにします（P.5-24 の「しきい値選択方式の設定」を参照）。Detector モジュールは、新しいしきい値を受け入れる場合、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。

Detector モジュールは、次のような場合、ゾーン ポリシーに未調整のマークを付けます。

- 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、ゾーン ポリシーに調整済みのマークを付けます。

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

ゾーンの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
- トラフィックのピーク時に検出およびラーニング　モードを開始しなかった場合（Detector モジュールがピーク時のトラフィックを攻撃と見なすことを防ぐため）

Detector モジュールは、現在のポリシーしきい値に関連付けされず、そのしきい値が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 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
```

ゾーンのポリシーしきい値調整とゾーン検出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、同時にゾーン検出をイネーブルにすることができます。Detector モジュールは、ポリシーのしきい値を調整すると同時に、ポリシーのしきい値を監視してトラフィック異常がないか調べます。この状態では、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。

新しいゾーンを作成する場合、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場合、あるいはゾーンのポリシー構築フェーズの結果を受け入れた後、Detector モジュールは、ゾーンのポリシーしきい値に未調整のマークを付けます。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、ゾーンのポリシーに調整済みのマークを付けます。

ラーニング プロセスとゾーン検出を同時にイネーブルにし、ゾーンのポリシーが未調整の場合、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 トラフィック内の攻撃を検出しない（ゾーンのポリシーしきい値が一度受け入れられるまで）
- Detector モジュールは、accept-new しきい値選択方式だけをアクティブにする（P.5-24 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、Cisco Anomaly Guard Module（Guard モジュール）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ます。次に、検出およびラーニング モードを再度アクティブにします。Detector モジュールは、Guard モジュールをアクティブにしなかった場合、攻撃が終了すると検出およびラーニング モード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。

ラーニング プロセスとゾーン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.5-18 の「しきい値の調整」および P.5-50 の「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。

Detector モジュールと Guard モジュールのゾーン設定の同期

ゾーンの設定およびポリシーを Guard モジュールのゾーンと同期させることができます。Detector モジュールは、完全なゾーン設定をコピーします。このようにして、一度ゾーンを設定し、Detector モジュールと Guard モジュールの両方で同じ設定およびポリシーを保持できます。

Detector モジュールと Guard モジュールの間の通信には、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.4-23 の「Cisco Anomaly Guard Module との通信のイネーブル化」を参照してください。

ゾーンのポリシーを最新に保つためにゾーンのトラフィック特性を常にラーニングする一方で、ゾーン トラフィックを常に Guard モジュールに宛先変更することを回避するように Detector モジュールを設定できます。

この項では、次のトピックについて取り上げます。

設定のガイドライン

Guard モジュールと Detector モジュールの間でゾーンを同期させるには、次のガイドラインを使用します。

- Guard モジュールと Detector モジュールの間でゾーンを同期させるには、Guard モジュールと Detector モジュールの両方に適したゾーン テンプレート（GUARD ゾーン テンプレート）を使用して、Detector モジュール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正しく同期させることを保証するため、Guard モジュールがトラフィックを宛先変更するときに、Guard モジュールと Detector モジュールの両方に同じタイプのトラフィックが流れることを保証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。
- 中央の設定ポイントとして Detector モジュールを使用します。Detector モジュールでゾーンを設定し、Detector モジュールの設定のバックアップを保持します。Detector モジュールから Guard モジュールにゾーン設定をコピーします。
- デバイスを物理的に変更する場合、または Detector モジュールと Guard モジュール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 モジュールと Guard モジュール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 モジュール上のゾーン設定を確認します。アクティベーション範囲が **ip-address-only** であり、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、Detector モジュールがゾーンに対する攻撃の終了を識別するために使用する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、Detector モジュールは、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。

シナリオ例

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 モジュールで新しいゾーンを作成および設定します。

   Detector モジュールは、ゾーン設定モードの **show** コマンドの出力で、ゾーン ID フィールドの隣に *(Guard/Detector)* と表示することにより、このようなゾーンを識別します。

   詳細については、P.5-3 の「新しいゾーンの作成」を参照してください。

2. Detector モジュールで、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 モジュールを追加します。

   詳細については、P.5-47 の「デフォルトのリモート Guard リストの設定」および P.5-48 の「ゾーンのリモート Guard リストの設定」を参照してください。

3. ゾーンのポリシーを構築するように Detector モジュールを設定します。**learning policy-construction** コマンドを使用します。

4. トラフィック異常を検出する一方で、ゾーン トラフィックをラーニングし、ポリシーのしきい値を調整するように Detector モジュールを設定します。**detect learning** コマンドを使用します。

   詳細については、P.5-50 の「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。

5. ラーニングしたポリシーのしきい値を 24 時間ごとに受け入れるように Detector モジュールを設定します。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。

   learning-params periodic-action auto-accept コマンドを使用します。

   詳細については、P.5-23 の「定期的なアクションの設定」を参照してください。

6. ラーニングしたばかりの新しいポリシーしきい値を受け入れるたびにゾーン設定を Guard モジュールと同期させるように Detector モジュールを設定します。このように設定することによって、Detector モジュールがゾーンのポリシーをラーニングする限り、Guard モジュール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。

   learning-params sync コマンドを使用します。

   詳細については、P.5-34 の「ゾーンの自動的な同期とエクスポート パラメータの設定」を参照してください。

7. Guard モジュールをアクティブにしてゾーンを保護する前に、ゾーン設定を Guard モジュール上の設定と同期させるように Detector モジュールを設定します。このように設定することによって、Guard モジュールがゾーンを保護するときに、Guard モジュール上のゾーンが最新の設定とポリシーを持つことが保証されます。

   learning-params sync コマンドを使用します。

   詳細については、P.5-34 の「ゾーンの自動的な同期とエクスポート パラメータの設定」を参照してください。

8. Detector モジュールは、ゾーンに対する攻撃を検出すると、次のアクションを実行します。

   - Guard　モジュール上のゾーン設定が最新であることを確認する。Guard モジュール上のゾーン設定が Detector モジュール上のゾーン設定と同じでない場合、Detector モジュールはゾーン設定を同期させます。
   - Guard モジュールをアクティブにしてゾーンを保護する（Guard モジュール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 モジュール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 モジュールは、定期的に Guard モジュールをポーリングします。攻撃が終了すると、Guard モジュールはゾーン保護を非アクティブにします。Detector モジュールは、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、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の動作状態を再度アクティブにします。

9. Guard モジュール上のゾーンのポリシーを手動で変更し、攻撃の特性に合せてゾーンのポリシーを調整した場合は、これまでとは反対に Detector モジュール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 モジュール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 モジュール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.7-25 の「固定値としてのしきい値の設定」および P.7-26 の「しきい値の乗数の設定」を参照してください。

ゾーンの設定およびポリシーを Guard モジュールに同期させるには、次のアクションを実行します。

- **deactivate** コマンドを使用して、ゾーンを非アクティブにする。
- **sync** コマンドを入力して、Detector モジュールのゾーン設定を Guard モジュールに同期させる。
- **detect** コマンドを使用して、ゾーン検出を再度アクティブにする。

詳細については、P.5-36 の「Detector モジュールに対するゾーン設定の同期」および P.5-50 の「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。

同期用のゾーンの設定

Guard モジュールと Detector モジュールの間でゾーンを同期させるには、GUARD ゾーン テンプレートを使用して、Detector モジュールに新しいゾーンを作成する必要があります。Guard モジュールと Detector モジュールの両方で、このテンプレートから作成されたゾーンを設定できます。

新しいゾーンには、Guard モジュール用と Detector モジュール用の 2 つの定義セットがあります。ゾーンの特性は、次の設定モードで設定できます。

- ゾーン設定モード：リモート Guard など、Detector モジュールに固有の定義を設定します。ゾーン設定モードに入るには、設定モードで **zone** コマンドを使用します。コマンド プロンプトでの表示は、次のようになります。

  ```
  user@DETECTOR-conf-zone-scannet#
  ```

- Guard 設定モード：ユーザ フィルタなど、Guard モジュールに固有の定義を設定します。guard 設定モードに入るには、ゾーン設定モードで **guard-conf** コマンドを使用します。コマンド プロンプトでの表示は、次のようになります。

  ```
  user@DETECTOR-conf-zone-scannet(guard)#
  ```

- ゾーン設定モードまたは guard 設定モード：IP アドレスなど、Guard モジュールと Detector モジュールの両方に共通の定義を設定します。

  Guard モジュールと Detector モジュールの両方に共通の設定を変更する場合、その変更は両方の定義セットに適用されます。たとえば、ゾーン設定モードでゾーンの IP アドレスを変更する場合、Guard モジュールのゾーン定義でも新しい IP アドレスに変更されます。guard 設定モードで Guard モジュールの新しいゾーン定義を表示できます。guard 設定モードでポリシーの動作状態を変更する場合、Detector モジュールのゾーン定義でもその動作状態が変更されます。

ゾーンを作成し、その同期について設定するには、次の手順を実行します。

ステップ 1　Guard ゾーン テンプレートのいずれかを使用して、Detector モジュールに新しいゾーンを作成します。

P.5-3 の「新しいゾーンの作成」を参照してください。

Detector モジュールは、**show** コマンドの出力で、ゾーン ID フィールドの隣に *(Guard/Detector)* と表示することにより、このようなゾーンを識別します。

ステップ 2　ゾーンの特性を設定します。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　Guard モジュールに固有の特性を設定するには、guard 設定モードに入ります。次のいずれかのコマンドを入力します。

- **guard-conf**：ゾーン設定モードから入力
- **configure** *zone-name* **guard-conf**：グローバル モードから入力
- **zone** *zone-name* **guard-conf**：設定モードから入力

zone-name 引数には、既存のゾーンの名前を指定します。

Detector モジュールが guard 設定モードに入ります。CLI プロンプトでは、モードを示すため、カッコで囲まれた guard という単語（guard）がプロンプトに追加されます。

次の例は、guard 設定モードに入る方法を示しています。

```
user@DETECTOR-conf-zone-scannet# guard-conf
user@DETECTOR-conf-zone-scannet(guard)#
```

guard 設定モードでは、ユーザ フィルタ、フィルタ終了、ポリシー アクションまたはフィルタ アクションの drop など、Guard モジュールに固有のすべてのゾーン特性を設定できます。詳細については、『*Cisco Anomaly Guard Module Configuration Guide*』を参照してください。

ゾーンの自動的な同期とエクスポート パラメータの設定

ゾーン設定をリモート Guard と自動的に同期させるように、またはゾーン設定を自動的に FTP サーバまたは SFTP サーバにエクスポートするように Detector モジュールを設定できます。

Detector モジュールは、次のアクションを実行します。

- Detector モジュールは、ゾーンの設定を、ゾーンのリモート Guard リストにあるすべてのリモート Guard と同期させます。ゾーンのリモート Guard リストが空の場合、Detector モジュールはゾーンの設定を、Detector モジュールのデフォルトのリモート Guard リストに定義されているリモート Guard と同期させます。1 つのリモート Guard との同期に失敗すると、Detector モジュールはリスト内の次のリモート Guard から続行します。

  ゾーンのリモート Guard リストと Detector モジュールのデフォルトのリモート Guard リストが両方とも空の場合、Detector モジュールはゾーンの設定を同期化しません。

  Guard モジュール上に同じ名前のゾーンが存在する場合、既存の設定は新しい設定によって上書きされます。

- しきい値調整フェーズの結果が受け入れられる場合、Detector モジュールは、ゾーンの FTP サーバ リストに記載されているすべての FTP サーバまたは SFTP サーバにゾーン設定をエクスポートします。リストが空の場合、Detector モジュールはデフォルトの FTP リストを参照します。詳細については、P.5-39 の「ゾーン設定の自動エクスポート」を参照してください。

  ゾーンの FTP サーバ リストと Detector モジュールのデフォルトの FTP サーバ リストが両方とも空の場合、Detector モジュールはゾーンの設定をエクスポートしません。

ゾーンの設定の自動的な同期とエクスポートをイネーブルにするには、ゾーン設定モードで次のコマンドを入力します。

learning-params sync {**accept** | **remote-activate**}

表 5-7 で、**learning-params sync** コマンドのキーワードについて説明します。

表 5-7　learning-params sync コマンドのキーワード

パラメータ	説明
accept	ラーニング プロセスのしきい値調整フェーズの結果が受け入れられるたびに、ゾーンの設定を同期化およびエクスポートします。
remote-activate	ゾーンの設定を同期させてから、リモート Guard をアクティブにします。リモート Guard 上の設定が最新でない場合にだけ、Detector モジュールはゾーン設定を同期させます。 Detector モジュールは、ゾーン設定を FTP サーバにも SFTP サーバにもエクスポートしません。

次の例は、ラーニング プロセスのしきい値調整フェーズの結果が受け入れられるたびに、ゾーンの設定を自動的に同期化およびエクスポートする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# learning-params sync accept
```

自動的な同期とエクスポートをディセーブルにするには、**no learning-params sync** コマンドを使用します。

ゾーン設定の自動的な同期

ゾーン設定をリモート Guard と自動的に同期させるように Detector モジュールを設定できます。Detector モジュールは、ゾーン設定を Guard モジュールにコピーします。Guard モジュール上に同じ名前のゾーンが存在する場合、既存の設定は新しい設定によって上書きされます。

Detector モジュールは、ゾーンの設定を、ゾーンのリモート Guard リストにあるすべてのリモート Guard と同期させます。ゾーンのリモート Guard リストが空の場合、Detector モジュールはゾーンの設定を、Detector モジュールのデフォルトのリモート Guard リストに定義されているリモート Guard と同期させます。1 つのリモート Guard との同期に失敗すると、Detector モジュールはリスト内の次のリモート Guard から続行します。

ゾーンのリモート Guard リストと Detector モジュールのデフォルトのリモート Guard リストが両方とも空の場合、Detector モジュールはゾーンの設定を同期化しません。

Detector モジュールがいつゾーン設定を同期させるかを定義するには、**learning-params sync** コマンドを使用します。詳細については、P.5-34 の「ゾーンの自動的な同期とエクスポート パラメータの設定」を参照してください。

Detector モジュールに対するゾーン設定の同期

Guard モジュールから Detector モジュールにゾーン設定をコピーすることにより、Guard モジュール上のゾーン設定と Detector モジュール上のゾーン設定を同期させることができます。これは、攻撃の特性に合せてゾーン ポリシーを調整するために Guard モジュール上のゾーン ポリシーを手動で変更し、その変更で Detector モジュールをアップデートして、将来の DDoS 攻撃の正しい検出を保証する場合、または将来 Guard モジュール上のゾーン設定を Detector モジュールに同期させるときに Guard モジュール上のゾーン設定が保持されることを保証する場合に必要となることがあります。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（P.7-25 の「固定値としてのしきい値の設定」を参照）、ポリシーのしきい値の固定乗数を設定すること（P.7-26 の「しきい値の乗数の設定」を参照）が必要になった場合に特に当てはまります。このようにすると、Detector モジュール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 モジュール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。

Detector モジュールは、Guard モジュールからゾーンの設定をコピーします。既存の設定が新しい設定で上書きされます。

Detector モジュールからゾーンの設定およびポリシーを同期させるには、次の手順を実行します。

ステップ 1　ゾーンが現在アクティブになっている場合は、ゾーン設定モードで **deactivate** コマンドを使用して、ゾーンを非アクティブにします。

ステップ 2　Detector モジュールのゾーン設定を Guard モジュールに同期させます。グローバル モードで次のコマンドを入力します。

```
sync zone zone-name remote-guard-address local
```

表 5-8 で、**sync zone** コマンドの引数について説明します。

表 5-8　sync zone コマンドの引数とキーワード

パラメータ	説明
zone-name	既存のゾーンの名前。
remote-guard-address	ゾーンの設定を、指定されたリモート Guard と同期させます。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 192.168.100.1）。

ステップ 3　同期プロセスを開始する前にゾーンがアクティブになっていた場合は、ゾーンを再度アクティブにします。ゾーン設定モードで **detect** コマンド（P.5-50 の「ゾーンのトラフィックの異常の検出」を参照）または **learning** コマンド（P.5-12 の「ゾーン トラフィックの特性のラーニング」を参照）を使用します。

次の例は、ゾーン *scannet* を非アクティブにし、Detector モジュールのゾーン設定を IP アドレス *192.168.55.10* の Guard モジュールに同期させる方法を示しています。次に、ゾーンを再度アクティブにする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# deactivate
user@DETECTOR-conf-zone-scannet# end
user@DETECTOR# sync zone scannet 192.168.55.10 local
user@DETECTOR# conf scannet
user@DETECTOR-conf-zone-scannet# detect learning
```

Detector モジュールからのゾーン設定の同期

ゾーンの設定およびポリシーを Guard モジュールのゾーンと同期させることができます。このようにして、Detector モジュールで一度ゾーンを設定し、ゾーンのトラフィック特性を常にラーニングする一方で、Detector モジュールと Guard モジュールの両方で同じ設定およびポリシーを保持し、ゾーン トラフィックを常に Guard モジュールに宛先変更することを回避できます。

Detector モジュールは、ゾーンの設定を Guard モジュールにコピーします。Guard モジュール上に同じ名前のゾーンが存在する場合、既存の設定は新しい設定によって上書きされます。このようにして、Guard モジュールがアクティブになってゾーンを保護するときに、Guard モジュール上のゾーンが最新のポリシーを持つことを保証できます。

（注）　同期プロセスを開始する前に、Guard モジュールでゾーンを非アクティブにする必要があります。

Detector モジュールからゾーンの設定およびポリシーを同期させるには、グローバル モードで次のコマンドを入力します。

sync zone *zone-name* **local** {**remote-guards** | *remote-guard-address*}

表 5-9 で、**sync zone** コマンドの引数とキーワードについて説明します。

表 5-9　sync zone コマンドの引数とキーワード

パラメータ	説明
zone-name	既存のゾーンの名前。
remote-guards	ゾーンの設定を、ゾーンのリモート Guard リストにあるすべてのリモート Guard と同期させます。ゾーンのリモート Guard リストが空の場合は、ゾーンの設定を、Detector のデフォルトのリモート Guard リストに定義されているリモート Guard と同期させます。
remote-guard-address	ゾーンの設定を、指定されたリモート Guard と同期させます。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 192.168.100.1）。

次の例は、ゾーンの設定を、ゾーンのリモート Guard リストにあるすべてのリモート Guard と同期させる方法を示しています。

```
user@DETECTOR# sync zone scannet local remote-guards
```

ゾーン設定の自動エクスポート

ゾーン設定を FTP サーバまたは SFTP サーバに自動的にエクスポートするように Detector モジュールを設定できます。ラーニング プロセスのしきい値調整フェーズの結果が受け入れられるたびに、Detector モジュールはゾーンの設定をエクスポートします。

ゾーンの設定を自動的にエクスポートするには、FTP または SFTP サーバを設定する必要があります。FTP または SFTP サーバは、次のリストに設定できます。

- ゾーンの FTP サーバ リスト：Detector モジュールがゾーン設定をエクスポートする先の FTP サーバまたは SFTP サーバのリスト。
- Detector モジュールのデフォルトの FTP サーバ リスト：FTP サーバまたは SFTP サーバのデフォルトのリスト。ゾーンの FTP サーバ リストが空の場合、Detector は、このリスト上のサーバにゾーンの設定をエクスポートします。

ゾーン設定を FTP サーバまたは SFTP サーバに自動的にエクスポートするように Detector モジュールを設定するには、次の手順を実行します。

ステップ 1　FTP サーバを定義します。設定モードで、次のいずれかのコマンドを入力します。

- **ftp-server** *ftp-server-name description* **ftp** *server remote-path login password*：FTP サーバを定義します。
- **ftp-server** *ftp-server-name description* **sftp** *server remote-path login*：SFTP サーバを定義します。

  Detector モジュールが SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.4-37 の「SFTP 接続用の鍵の設定」を参照してください。

表 5-10 で、**ftp-server** コマンドの引数について説明します。

表 5-10　ftp-server コマンドの引数とキーワード

パラメータ	説明
ftp	FTP サーバを定義します。
sftp	SFTP サーバを定義します。
ftp-server-name	FTP または SFTP サーバの名前。1 ～ 63 文字の英数字の文字列を入力します。文字列にはアンダースコアを含めることができますが、スペースを含めることはできません。
description	FTP または SFTP サーバを説明する文字列。文字列の長さは最大 80 文字です。
server	FTP または SFTP サーバの IP アドレス。
remote-path	ファイルの完全な名前。パスを指定しない場合、サーバはユーザのホーム ディレクトリにファイルを保存します。
login	FTP または SFTP サーバのログイン名。
password	リモート FTP サーバのパスワード。 このオプションは、FTP サーバ専用です。Detector モジュールは、公開鍵を使用して、SFTP サーバを認証します。

次の例は、FTP サーバを定義する方法を示しています。

```
user@DETECTOR-conf# ftp-server MyFTP-Server Description ftp 10.0.0.191
/root/ConfigFiles <user> <password>
```

（注）　Detector モジュールが特定の FTP サーバまたは SFTP サーバにゾーン設定を自動的にエクスポートできるようにするには、Detector モジュールのデフォルトの FTP サーバ リストまたはゾーンの FTP サーバ リストにそのサーバを設定する必要があります。

ステップ 2　（オプション）FTP または SFTP サーバをゾーンの FTP サーバ リストに追加します。

FTP または SFTP サーバをゾーンの FTP サーバ リストに追加するには、ゾーン設定モードで次のコマンドを入力します。

ftp-server *ftp-server-name*

ftp-server-name 引数には、FTP または SFTP サーバの名前を指定します。

次の例は、FTP サーバをゾーンの FTP サーバ リストに追加する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# ftp-server default MyFTP-Server
```

リストから FTP サーバを削除するには、コマンドの **no** 形を使用します。

ステップ 3　（オプション）FTP または SFTP サーバを Detector モジュールのデフォルトの FTP サーバ リストに追加します。

Detector モジュールは、ゾーンの FTP サーバ リストに記載されている FTP サーバにゾーン設定をエクスポートします。リストが空の場合、Detector モジュールはデフォルトの FTP リストを参照します。

FTP または SFTP サーバを Detector モジュールのデフォルトの FTP サーバ リストに追加するには、設定モードで次のコマンドを入力します。

ftp-server default *ftp-server-name*

ftp-server-name 引数には、FTP または SFTP サーバの名前を指定します。

次の例は、FTP サーバを Detector モジュールのデフォルトの FTP サーバ リストに追加する方法を示しています。

```
user@DETECTOR-conf# ftp-server default MyFTP-Server
```

リストから FTP サーバを削除するには、コマンドの **no** 形を使用します。

ステップ 4　（オプション）ラーニング プロセスのしきい値調整フェーズの結果が受け入れられるたびに、ゾーン設定を FTP サーバまたは SFTP サーバに自動的にエクスポートするように Detector モジュールを設定します。**learning-params sync accept** コマンドを使用します。詳細については、P.5-39 の「ゾーン設定の自動エクスポート」を参照してください。

ゾーン設定の手動エクスポート

Detector モジュールをアクティブにして、FTP サーバまたは SFTP サーバにゾーン設定をエクスポートできます。Detector モジュールは、ゾーンの設定のうち、Guard モジュールにゾーンを設定するために必要な部分をエクスポートします。

グローバル モードで次のコマンドのいずれかを入力します。

- **copy zone** *zone-name* **guard-running-config ftp** *server remote-path* [*login password*]]：ゾーンの設定を FTP サーバにエクスポートします。
- **copy zone** *zone-name* **guard-running-config sftp** *server remote-path login*：ゾーンの設定を SFTP サーバにエクスポートします。

  Detector モジュールが SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.4-37 の「SFTP 接続用の鍵の設定」を参照してください。

表 5-11 で、**copy guard-running-config** コマンドの引数について説明します。

表 5-11　copy guard-running-config コマンドの引数とキーワード

パラメータ	説明
ftp	ゾーンの設定を FTP サーバにエクスポートします。
sftp	ゾーンの設定を SFTP サーバにエクスポートします。
zone-name	既存のゾーンの名前。Detector モジュールは、Guard モジュールに適用される、指定されたゾーン設定の一部をエクスポートします。
server	FTP または SFTP サーバの IP アドレス。
remote-path	ファイルの完全な名前。パスを指定しない場合、サーバはユーザのホーム ディレクトリにファイルを保存します。

表 5-11　copy guard-running-config コマンドの引数とキーワード（続き）

パラメータ	説明
login	FTP または SFTP サーバのログイン名。 FTP の場合、この引数はオプションです。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。パスワードを入力しない場合、Detector モジュールによって入力するよう要求されます。 このオプションは、FTP サーバ専用です。SFTP サーバは、Detector モジュールの公開鍵を使用して、Detector モジュールを認証します。

次の例は、ゾーンの設定を FTP サーバにエクスポートする方法を示しています。

```
user@DETECTOR-conf# copy zone scannet guard-running-config ftp
10.0.0.191 /root/ConfigFiles/scannet.txt <user> <password>
```

ゾーン設定のオフラインでの同期

Guard モジュールと Detector モジュールの間に安全な通信チャネルが確立できない場合でも、ゾーン設定を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 モジュールが Detector モジュールにアクセスできない場合
- Detector モジュールが Guard モジュールにアクセスできない場合
- Detector モジュールが Network Address Translation（NAT; ネットワーク アドレス変換）デバイスを介して Guard モジュールと通信する場合

ゾーン設定をオフラインで同期させるには、まず Detector モジュールから FTP サーバまたは Secure FTP（SFTP）サーバにゾーン設定をエクスポートしてから、ゾーン設定を Guard モジュールに手動でインポートする必要があります。

Guard モジュールと Detector モジュールの間に安全な通信チャネルが存在しないため、Detector モジュールによってゾーン トラフィック内で異常が検出された場合は、Guard モジュール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。

Detector モジュールがゾーン設定を同期できるようにするには、次のタスクを実行する必要があります。

- GUARD ゾーン テンプレートのいずれかを使用して、Detector モジュールにゾーンを作成する。P.5-3 の「新しいゾーンの作成」を参照してください。
- 設定を SFTP サーバにエクスポートするために、Detector モジュールが SFTP 通信に使用する SSH 鍵を設定する。P.4-37 の「SFTP 接続用の鍵の設定」を参照してください。

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。

ゾーン設定は、次の 2 つの方法でエクスポートできます。

- 自動：特定の状態が発生すると必ずゾーン設定をエクスポートするように Detector モジュールを設定します（P.5-39 の「ゾーン設定の自動エクスポート」を参照）。
- 一度：Detector モジュールをアクティブにして、ゾーン設定のエクスポートを開始します（P.5-42 の「ゾーン設定の手動エクスポート」を参照）。

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。

リモート Guard のアクティブ化

Detector モジュールは、ゾーンのトラフィックの異常を検出すると、そのイベントをログに記録するか（*通知*として知られるアクション）、ゾーンを保護するためのアクションを開始する Guard モジュール（リモート Guard）をアクティブにします。

Detector モジュールは、ゾーンを保護するためにアクティブにされる Guard モジュールのリストを保持します。このリストは、リモート Guard リストと呼ばれます。また、Detector モジュールは、リモート Guard リスト上の Guard モジュールとゾーン設定を同期させることもできます。Detector モジュールは、次の 4 つのタイプのリモート Guard リストを保持します。

1. ゾーン固有の SSL リモート Guard リスト：Detector モジュールは、SSL 通信チャネルを使用して、SSL リモート Guard リスト内の Guard モジュールと通信します。Detector モジュールは、Guard モジュールをアクティブにして、ゾーンを保護し、ゾーン設定を同期させることができます。
2. ゾーン固有の SSH リモート Guard リスト：Detector モジュールは、SSH 通信チャネルを使用して、SSH リモート Guard リスト内の Guard モジュールと通信します。Detector モジュールは、Guard モジュールをアクティブにして、ゾーンの保護だけを行います。
3. デフォルトの SSL リモート Guard リスト：Detector モジュールは、SSL 通信チャネルを使用して、SSL リモート Guard リスト内の Guard モジュールと通信します。ゾーンの SSL リモート Guard リストが空の場合、Detector は、デフォルトの SSL リモート Guard リストにある Guard をアクティブにし、ゾーンの設定を同期させます。
4. デフォルトの SSH リモート Guard リスト：Detector モジュールは、SSH 通信チャネルを使用して、SSH リモート Guard リスト内の Guard モジュールと通信します。ゾーンの SSH リモート Guard リストが空の場合、Detector は、デフォルトの SSH リモート Guard リストにある Guard をアクティブにします。

複数のリモート Guard リストに Guard モジュールを設定できます。

次の各項では、リモートの Guard を設定し、アクティブにする方法について説明します。

設定のガイドライン

リモート Guard のアクティベーションと、ゾーン情報の同期をイネーブルにするには、次のタスクを実行する必要があります。

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

（注）　SSH 通信チャネルだけを使用してリモート Guard をアクティブにする必要がある場合は、Guard モジュールと Detector モジュールの両方にゾーンを作成してください。GUARD ゾーン テンプレートと DETECTOR ゾーン テンプレートのいずれかを使用して、Detector モジュールにゾーンを作成できます。ゾーン名は同一である必要があります。ただし、**protect-ip-state** コマンドを使用して、リモート Guard の Guard 保護のアクティベーション形態を **dst-ip-by-ip** に設定した場合を除きます。

P.5-3 の「新しいゾーンの作成」を参照してください。

2. Detector モジュールで、ゾーンのリモート Guard リストまたはデフォルトのリモート Guard リストにリモート Guard の IP アドレスを追加します。
   - ゾーンのリモート Guard リスト：そのゾーンの保護用に Detector モジュールによってアクティブにされるリモート Guard のリスト。詳細については、P.5-48 の「ゾーンのリモート Guard リストの設定」を参照してください。
   - Detector のデフォルト リスト：リモート Guard のデフォルト リスト。ゾーンのリモート Guard リストが空の場合、Detector はこれらの Guard をアクティブにします。詳細については、「デフォルトのリモート Guard リストの設定」を参照してください。
3. リモート Guard との通信チャネルを設定します（詳細については、P.4-23 の「Cisco Anomaly Guard Module との通信のイネーブル化」を参照）。
4. （オプション）Detector モジュールと Guard モジュールのゾーンを同期させます。ゾーンの設定を同期化できるのは、SSL 通信チャネルを使用する場合のみです。
5. アクティベーションのタイプを決定するために、ゾーンの Guard 保護の形態（protect-ip-state）を設定します。詳細については、P.5-53 の「Guard 保護のアクティベーション方式の設定」を参照してください。

デフォルトのリモート Guard リストの設定

ゾーン固有のリモート Guard リストが空の場合、Detector モジュールはデフォルトのリモート Guard リストをアクティブにします。Detector モジュールには、次の 2 つのタイプのデフォルト リモート Guard リストがあります。

1. デフォルトの SSL リモート Guard リスト : Detector モジュールは、SSL 通信チャネルを使用して、SSL リモート Guard リスト内の Guard モジュールと通信します。ゾーンの SSL リモート Guard リストが空の場合、Detector は、デフォルトの SSL リモート Guard リストにある Guard をアクティブにし、ゾーンの設定を同期させます。
2. デフォルトの SSH リモート Guard リスト : Detector モジュールは、SSH 通信チャネルを使用して、SSH リモート Guard リスト内の Guard モジュールと通信します。ゾーンの SSH リモート Guard リストが空の場合、Detector は、デフォルトの SSH リモート Guard リストにある Guard をアクティブにします。

Detector モジュールにおいて、リモート Guard リストのいずれかにリモート Guard が少なくとも 1 つ含まれていることを確認します（リモート Guard リストは、デフォルトの SSL リモート Guard リスト、デフォルトの SSH リモート Guard リスト、ゾーンの SSL リモート Guard リスト、またはゾーンの SSH リモート Guard リスト）。どのリモート Guard リストにもリモート Guard が定義されていない場合、Detector モジュールはログ ファイルにイベントを記録します。

デフォルトのリモート Guard リストに Guard を追加するには、設定モードで次のコマンドのいずれかを入力します。

- **remote-guard ssh** *remote-guard-address* [*description*]
- **remote-guard ssl** *remote-guard-address* [*description*]

表 5-12 で、**remote-guard** コマンドの引数について説明します。

表 5-12　remote-guard コマンドの引数

パラメータ	説明
ssh	デフォルトの SSH リモート Guard リストにリモート Guard を追加します。
ssl	デフォルトの SSL リモート Guard リストにリモート Guard を追加します。

表 5-12　remote-guard コマンドの引数（続き）

パラメータ	説明
remote-guard-address	リモートの Guard の IP アドレス。
description	（オプション）リモートの Guard の説明。説明は、最大 63 文字です。

次の例は、デフォルトの SSL リモート Guard リストにリモート Guard を追加する方法を示しています。

```
user@DETECTOR-conf# remote-guard ssl 192.168.100.33
```

注意　リモート Guard リストを変更する場合は、Detector モジュールがリモート Guard との通信チャネルに使用する SSL 証明書を再生成する必要があります。詳細については、P.4-28 の「SSL 証明書の再生成」を参照してください。

リモート Guard のデフォルト リストを表示するには、**show detector** コマンドを使用します。

ゾーンのリモート Guard リストの設定

Detector モジュールは、ゾーンのトラフィックの異常を検出すると、そのイベントをログに記録するか（*通知*として知られるアクション）、ゾーンを保護するためのアクションを開始するリモートの Guard をアクティブにします。Detector モジュールには、次の 2 つのタイプのゾーン リモート Guard リストがあります。

1. ゾーンの SSL リモート Guard リスト : Detector モジュールは、SSL 通信チャネルを使用して、SSL リモート Guard リスト内の Guard モジュールと通信します。
2. ゾーンの SSH リモート Guard リスト : Detector モジュールは、SSH 通信チャネルを使用して、SSH リモート Guard リスト内の Guard モジュールと通信します。

Detector モジュールは、両方のゾーン リモート Guard リストに記載されているリモート Guard をアクティブにします。リストが空の場合、Detector モジュールは、対応するデフォルトのリモート Guard リストも参照します。

Detector モジュールにおいて、リモート Guard リストのいずれかにリモート Guard が少なくとも 1 つ含まれていることを確認します（リモート Guard リストは、デフォルトの SSL リモート Guard リスト、デフォルトの SSH リモート Guard リスト、ゾーンの SSL リモート Guard リスト、またはゾーンの SSH リモート Guard リスト）。どのリモート Guard リストにもリモート Guard が定義されていない場合、Detector モジュールはログ ファイルにイベントを記録します。

注意　リモート Guard リストを変更する場合は、リモート Guard との通信チャネルを確立する必要があります。詳細については、P.4-23 の「Cisco Anomaly Guard Module との通信のイネーブル化」を参照してください。

ゾーンのリモート Guard リストに Guard を追加するには、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。

- **remote-guard ssh** *remote-guard-address* [*description*]
- **remote-guard ssl** *remote-guard-address* [*description*]

表 5-13 で、**remote-guard** コマンドの引数について説明します。

表 5-13　remote-guard コマンドの引数

パラメータ	説明
ssh	ゾーンの SSH リモート Guard リストにリモート Guard を追加します。
ssl	ゾーンの SSL リモート Guard リストにリモート Guard を追加します。
remote-guard-address	リモート Guard の IP アドレス。
description	（オプション）リモートの Guard の説明。説明は、最大 63 文字です。

次の例を参考にしてください。

```
user@DETECTOR-conf-zone-scannet# remote-guard ssl 192.168.100.33
```

（注）　ゾーンのリモート Guard リストを表示するには、**show zone** コマンドを使用します。

ゾーンのトラフィックの異常の検出

ゾーンの異常検出をアクティブにすると、Detector モジュールは、受信するゾーン トラフィックのコピーを監視します。トラフィック異常がポリシーしきい値を超える（攻撃を示す）ことによってポリシー アクションをトリガーすると、Detector は、通知を送信するか、または Cisco Anomaly Guard Module（Guard モジュール）をアクティブにしてゾーンを保護します。

ゾーンの異常検出をアクティブにする前に、Detector モジュールにゾーンのトラフィック パターンを学習させます。ラーニング プロセスにより、Detector モジュール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。

ゾーンが攻撃されていない場合は、**learning policy-construction** コマンドを使用して Detector モジュールにゾーンのポリシーを構築させてから、検出およびラーニング モードで Detector モジュールをアクティブにすることをお勧めします。Detector モジュールは、ゾーン トラフィックをラーニングすると同時に、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異常がないか調べます。Detector モジュールは、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 トラフィック内の異常の検出は続行します。この結果、Detector モジュール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。P.5-27 の「ゾーンのポリシーしきい値調整とゾーン検出イネーブル化の同時実行」を参照してください。

Guard モジュールをアクティブにしてゾーンを保護する前に、Detector モジュール上のゾーン設定と Guard モジュール上のゾーン設定を同期させることができます。詳細については、P.5-28 の「Detector モジュールと Guard モジュールのゾーン設定の同期」および P.5-45 の「リモート Guard のアクティブ化」を参照してください。

ゾーン検出をアクティブにする前に、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.2-5 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。

ヒント　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.2-5 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。

次の検出特性を定義できます。

- **動作モード**：Detector モジュールがゾーンを保護する手段を自動的に適用するか、インタラクティブに適用するかを定義します。
- **Guard 保護アクティベーション方式**：Detector モジュールがゾーンを保護するためにリモート Guard のアクティブ化に使用する方式を定義します。Detector モジュールは、リモート Guard をアクティブにしてゾーン全体の一部である特定のゾーン（たとえば、保護されたネットワーク環境の一部である特定のサーバ）を保護することも、リモート Guard をアクティブにしてゾーン全体を保護することもできます。

この項では、次のトピックについて取り上げます。

ゾーン検出のアクティブ化

ゾーン検出を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を入力します。

detect [**learning**]

learning キーワードでは、ゾーン トラフィック内の異常を検出すると同時に、ポリシーのしきい値を調整するように Detector モジュールが設定されます。詳細については、P.5-18 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@DETECTOR-conf-zone-scannet# detect
```

ゾーン検出の非アクティブ化

ゾーン検出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 detect :** ゾーン検出を終了します。ゾーンが検出およびラーニング モードである場合、Detector モジュールはポリシーのしきい値のラーニングを続行します。
- **deactivate :** ゾーン検出と、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。

検出動作モードの定義

Detector 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。

- **自動検出モード**：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。
- **インタラクティブ検出モード**：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「インタラクティブ検出モード」を参照してください。

Guard 保護のアクティベーション方式の設定

Guard 保護アクティベーション方式は、Cisco Anomaly Guard Module（Guard モジュール）がゾーン保護をアクティブにする方法を定義します。この方式は、ゾーンの保護要件に、より正確に焦点を当て、Guard モジュールのリソースを節約することを目的としたものです。アクティベーション方式は、ゾーン全体の一部である特定のゾーン（保護されたネットワーク環境内の特定のサーバなど）のゾーン保護をアクティブにするものから、ゾーン全体のゾーン保護をアクティブにするものまであります。

Detector モジュールは、次の Guard 保護のアクティベーション方式をサポートします。

- **entire-zone**：Detector モジュールは、ゾーン宛てのトラフィック内で異常を検出すると必ず、Guard モジュールをアクティブにしてゾーン全体を保護します。この方式では、Guard モジュールが保護するアクティブなゾーンの数が減るため、Guard モジュールのリソースが節約されます。ゾーン全体が関連性のあるサブゾーンで構成されている場合には、この方法を推奨します。
- **dst-ip-by-name**：Detector モジュールは、特定の IP アドレス宛てのトラフィック異常がトレースされると、Guard モジュールをアクティブにしてその IP アドレスを保護します。ゾーン全体が関連性のないサブゾーンで構成されている場合には、この方法を推奨します。このように定義すると、Guard モジュールをアクティブにして攻撃の対象となる IP アドレスを保護できる一方で、ゾーン全体のトラフィックを Guard モジュールに宛先変更することを回避できます。Detector モジュールは、トラフィック異常を特定の IP アドレスに関連付けることができない場合、Guard モジュールをアクティブにしないため、ゾーンが保護されません。
- **dst-ip-by-ip**：Detector モジュールは、特定の IP アドレス宛てのトラフィック異常がトレースされると、Guard モジュールをアクティブにしてその IP アドレスを保護します。IP アドレスは、Guard モジュールに定義されているいずれかのゾーンのアドレス範囲内である必要があります。ただし、Detector モジュール上のゾーン名が、Guard モジュール上のゾーン名と一致する必要はありません。これは、Guard モジュールで **protect** *ip-address* コマンドを使用するのと同じです。Detector モジュール上のゾーン名が Guard モジュール上のゾーン名と一致しない場合、またはゾーン全体が関連性のないサブゾーンで構成されている場合は、この方法をお勧めします。

（注） Guard モジュールが攻撃対象の IP アドレスだけのゾーン保護をアクティブにするようにするには、Guard　モジュールでゾーンに **ip-address-only** というアクティベーション範囲が定義されていることを確認してください。このように定義すると、Guard モジュールをアクティブにして攻撃の対象となる IP アドレスを保護できる一方で、ゾーン全体のトラフィックを Guard モジュールに宛先変更することを回避できます。

- **policy-type** : Detector モジュールは、Guard モジュールをアクティブにし、リモート アクティベーションの原因となったポリシーに応じて、ゾーン全体を保護するか、またはゾーン内の特定の IP アドレスを保護します。特定の IP アドレス宛てのトラフィック異常がトレースされた場合（たとえば、リモート アクティベーションの原因となったポリシーのトラフィック特性が dst_ip である場合）、Detector モジュールは Guard モジュールをアクティブにしてその IP アドレスを保護します。トラフィック異常を特定の IP アドレスと関連付けることができない場合（たとえば、リモート アクティベーションの原因となったポリシーのトラフィック特性が global である場合）、Detector モジュールは Guard モジュールをアクティブにしてゾーン全体を保護します。

  ゾーン全体が関連性の高いサブゾーンで構成されている場合には、この方法を推奨します。この方法では、攻撃対象となったゾーンがゾーン全体に損害を与える状況を避けることができます。

Guard 保護アクティベーション方式をアクティブにするには、関係するゾーンの設定モードで次のコマンドを入力します。

protect-ip-state {**entire-zone | dst-ip-by-name | dst-ip-ip** | **policy-type**}

次の例を参考にしてください。

```
user@DETECTOR-conf-zone-scannet# protect-ip-state entire-zone
```