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。

この章は、次の項で構成されています。

- 概要
- ゾーン テンプレートの使用
- 新しいゾーンの作成
- ゾーンのアトリビュートの設定
- ゾーンの IP アドレス範囲の設定
- Detector モジュールの Cisco Anomaly Guard Module とのゾーン設定の同期

概要

ゾーンとは、Detector モジュールが Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃を監視するために使用するネットワーク要素のことです。ゾーンは、次の要素を任意に組み合せたものです。

- ネットワークサーバ、クライアント、またはルータ
- ネットワーク リンクまたはサブネット、またはネットワーク全体
- 個々のインターネット ユーザまたは企業
- インターネット サービス プロバイダー（ISP）

Detector モジュールは、DDoS 攻撃を発見すると、Cisco Anomaly Guard Module（Guard モジュール）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 モジュール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、ゾーン名とゾーンの説明を設定できる。詳細については、P.5-6 の「新しいゾーンの作成」を参照してください。
- ゾーン ネットワーク定義の設定：ネットワークの IP アドレスやサブネット マスクなどを含む、ゾーン ネットワーク定義を設定できる。詳細については、P.5-10 の「ゾーンのアトリビュートの設定」を参照してください。
- ゾーン フィルタの設定：ゾーン フィルタを設定できる。ゾーン フィルタは、ゾーンのトラフィックに必要な検出レベルを適用し、Detector モジュール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　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。このポリシーは、Detector モジュール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。Detector モジュールは、ポリシー構築フェーズおよびしきい値調整フェーズの 2 つのフェーズで構成されるラーニング プロセスの中でポリシーを構築します。詳細については、第 8 章「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 テンプレートの使用

ゾーン テンプレートとは、ゾーンのデフォルト設定を定義したものです。

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 Guard モジュール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 Guard モジュール用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。ゾーン設定を Guard モジュール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.5-16 の「同期用のゾーンの設定」を参照してください。

表 5-1 に、ゾーン テンプレートを示します。

表 5-1　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 VoIP[1] サーバを保護することができます。 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。DETECTOR_WORM ゾーン テンプレートから作成されたゾーンには、worm_tcp ポリシー テンプレートから作成されたポリシーが含まれています（詳細については、P.7-34 の「ワーム ポリシーについて」を参照）。

表 5-1　ゾーン テンプレート（続き）

テンプレート	説明
DETECTOR_LINK 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。Detector モジュールが、攻撃されている IP アドレスまたはサブネットのみに対する Guard モジュール上のゾーン保護をアクティブにするようにするには、**protect-ip-state dst-ip-by-name** コマンドを使用します。**protect-ip-state** コマンドの詳細については、P.9-4 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。 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は、ラーニング プロセスのポリシー構築フェーズを実行することはできません。
GUARD_DEFAULT	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ゾーン テンプレート。テンプレートは、128Kb、1Mb、4Mb、および 512Kb のリンクを対象とした GUARD_LINK_128K、GUARD_LINK_1M、GUARD_LINK_4M、GUARD_LINK_512K が用意されています。

表 5-1　ゾーン テンプレート（続き）

テンプレート	説明
GUARD_LINK テンプレート（*続き*）	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。 このようなゾーンを定義する際は、**protect-ip-state** コマンドを使用した **dst-ip-by-name** による Guard 保護アクティベーション方式（特定の IP アドレス宛てのゾーン トラフィック異常が検出されると Detector モジュールが Guard モジュールをアクティブにしてその IP アドレスを保護する）を使用することをお勧めします。詳細については、P.9-4 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。
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。ゾーンが IP アドレスに基づいて制御されている場合（IRC[2] サーバタイプのゾーンなど）、または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、このゾーン テンプレートを使用できます。
GUARD_VOIP	SIP[3] over UDP を使用して VoIP セッションを確立し、セッション確立後に RTP/RTCP[4] を使用して音声データを SIP エンド ポイント間で伝送する VoIP サーバが含まれているゾーン用に設計されたテンプレート。 Detector モジュールは、GUARD_SIP ポリシーから作成された VoIP トラフィックを処理するためのポリシーを GUARD_VOIP ゾーン テンプレートからユーザが作成したゾーンに追加します。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。

1. VoIP = Voice over IP
2. IRC = Internet Relay Chat（インターネット リレー チャット）
3. SIP = Session Initiation Protocol
4. RTP/RTCP = Real-Time Transport Protocol/Real-Time Control Protocol

新しいゾーンの作成

ゾーンを作成し、ゾーン名、説明、ネットワーク アドレス、動作定義、ネットワーク定義を設定することができます。

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 アトリビュート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。

ゾーン設定の設定値を変更する方法については、P.5-10 の「ゾーンのアトリビュートの設定」を参照してください。

ゾーン テンプレートからの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使用します。

- **zone** *new-zone-name* [*template-name*] [**interactive**]：新しいゾーンを作成します。*template-name* 引数を入力しなかった場合、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**]：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と、Detector モジュールは、すべてのゾーン アトリビュートにデフォルト設定を適用します。

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 5-2 に、**zone** コマンドの引数とキーワードを示します。

表 5-2　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。 ゾーン テンプレートは次のいずれかになります。 • GUARD_DEFAULT • GUARD_LINK_128K • GUARD_LINK_1M • GUARD_LINK_4M • GUARD_LINK_512K • GUARD_TCP_NO_PROXY • DETECTOR_DEFAULT • DETECTOR_LINK_128K • DETECTOR_LINK_1M • DETECTOR_LINK_4M • DETECTOR_LINK_512K • DETECTOR_WORM 詳細については、表 5-1 を参照してください。

表 5-2　zone コマンドの引数とキーワード（続き）

パラメータ	説明
interactive	（オプション）Detector モジュールがゾーン異常検出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 10 章「インタラクティブ検出モードの使用方法」を参照してください。

次の例は、新しいゾーンを作成し、インタラクティブ検出モードに設定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、同じプレフィッ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。

既存のゾーンの複製による新しいゾーンの作成

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使用します。

- **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、指定されたゾーン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 に、**zone** コマンドの引数とキーワードを示します。

表 5-3　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める必要があります。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。
copy-from-this	現在のゾーンの設定をコピーして、新しいゾーンを作成します。
copy-from	指定されたゾーンの設定をコピーして、新しいゾーンを作成します。
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.8-27 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、現在のゾーンから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.8-18 の「ポリシーに対する調整済みのマーク付け」を参照してください。

ゾーン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使用します。

- **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。

（注）　**aaa authorization commands zone-completion tacacs+** コマンドを使用すると、**zone** コマンドにおけるゾーン名のタブ補完をディセーブルにすることができます。詳細については、P.4-18 の「ゾーン名のタブ補完のディセーブル化」を参照してください。

ステップ 2　**ip address** コマンドを使用して、ゾーンの IP アドレス を定義します。Detector モジュールがゾーン トラフィックをラーニングしてゾーンを検出できるようにするには、除外されない IP アドレスを少なくとも 1 つ定義する必要があります。

詳細については、P.5-12 の「ゾーンの IP アドレス範囲の設定」を参照してください。

ステップ 3　（オプション）ゾーン設定モードで次のコマンドを入力して、識別用の説明をゾーンに追加します。

```
description string
```

文字列の長さは最大 80 文字です。式にスペースを使用する場合は、式を引用符（" "）で囲みます。

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　ゾーン設定モードで **show running-config** コマンドを入力して、新しく設定したゾーンの設定を表示します。

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 アトリビュートを設定する方法を示しています。ゾーンの IP アドレス範囲は 192.168.100.32/27 に設定されていますが、IP アドレス 192.168.100.50 はこのゾーンの IP アドレス範囲から除外されています。

```
user@DETECTOR-conf# zone scannet
user@DETECTOR-conf-zone-scannet# ip address 192.168.100.32
255.255.255.224
user@DETECTOR-conf-zone-scannet# ip address exclude 192.168.100.50
user@DETECTOR-conf-zone-scannet# description Demonstration zone
user@DETECTOR-conf-zone-scannet# show running-config
```

ゾーンの IP アドレス範囲の設定

ゾーン異常検出をアクティブにする前に、除外されない IP アドレスを少なくとも 1 つ定義する必要がありますが、IP アドレスの IP アドレス範囲への追加や、IP アドレス範囲からの削除はいつでもできます。大規模なサブネットを設定し、特定の IP アドレスがゾーンの IP アドレス範囲に含まれないようにそのサブネットからを除外することができます。

ゾーンの IP アドレスを設定するには、ゾーン設定モードで次のコマンドを使用します。

ip address [**exclude**] *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 コマンドの引数とキーワード

パラメータ	説明
exclude	IP アドレスをゾーンの IP アドレス範囲から除外します。
ip-addr	IP address.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）。 デフォルトで、IP アドレスをゾーンの IP アドレス範囲から除外します。 この IP アドレスはサブネット マスクに一致している必要があります。クラス A、クラス B、またはクラス C のサブネット マスクを入力した場合、IP アドレスのホスト ビットは 0 である必要があります。
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。

次の例は、ゾーンの IP アドレス範囲を 192.168.100.32/27 に設定し、IP アドレス 192.168.100.50 をゾーンの IP アドレス範囲から除外する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# ip address 192.168.100.32
255.255.255.224
user@DETECTOR-conf-zone-scannet# ip address exclude 192.168.100.50
```

ゾーンの IP アドレス範囲を変更する場合は、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.8-6 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。
- 検出およびラーニング機能をイネーブルにしている場合、**no learning-params threshold-tuned** コマンドを使用して、ゾーン ポリシーに未調整マークを付けます。ゾーン上で攻撃が行われている場合は、ゾーン ポリシーの状態を未調整に変更しないでください。ゾーン ポリシーの状態を変更すると、Detector モジュールは攻撃を検出できなくなり、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原因になります。詳細については、P.8-18 の「ポリシーに対する調整済みのマーク付け」を参照してください。
- 検出およびラーニング機能を使用していない場合は、ゾーン異常検出をアクティブにする前に、しきい値調整フェーズをアクティブにする必要があります。P.8-10 の「ポリシーしきい値の調整」を参照してください。

ゾーンの IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

IP アドレスの除外を削除するには、**no ip address exclude** コマンドを使用します。

ゾーンの IP アドレスをすべて削除して IP アドレスを除外するには、**no ip address *** コマンドを使用します。

Detector モジュールの Cisco Anomaly Guard Module と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、ゾーン設定全体を Guard モジュールにコピーします。このプロセスにより、ゾーンを一度設定するだけで、Detector モジュールと Guard モジュールの両方で同じ設定とポリシーを維持できます。

Detector モジュールと Guard モジュールとの通信には、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.4-26 の「Cisco Anomaly Guard Module との通信の確立」を参照してください。

Detector モジュールが常にゾーン トラフィック特性をラーニングし、ゾーン ポリシーを最新状態に保ち、ゾーン トラフィックが絶え間なく Guard モジュールに宛先変更されるのを避けるように設定できます。

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
- 同期用のゾーンの設定
- 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
- ゾーン設定の自動的な同期
- Detector モジュールとのゾーン設定の同期化
- Detector モジュールからのゾーン設定の同期
- ゾーン設定のオフラインでの同期
- ゾーン設定の自動エクスポート
- ゾーン設定の手動エクスポート
- サンプル シナリオ

設定のガイドライン

Guard モジュールと Detector モジュールとの間でゾーンを同期させるには、次のガイドラインに従います。

- 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 モジュール上に新しいゾーンを作成します。

  詳細については、表 5-1 を参照してください。
- ゾーン ポリシーを正しく同期させるには、Guard モジュール（トラフィックを宛先変更しているとき）と Detector モジュール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。そうしないと、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 攻撃から正しく保護されません。
- Detector モジュールを中央設定ポイントとして使用します。これは、新しいゾーンは Detector モジュール上にのみ作成でき、Detector モジュールの設定ファイルには Detector モジュールのゾーンと Guard モジュールのゾーンの設定が含まれるためです。Detector モジュール上にゾーンを設定し、Detector モジュールの設定のバックアップを保守します。ゾーン設定は、Detector モジュールから Guard モジュールにコピーします。
- デバイスを交換する場合や、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、アクティベーション方式が **zone-name-only** でない場合は、Detector モジュールがゾーンに対する攻撃が終了したことを確認するために使用するタイマーを、**protection-end-timer** コマンドで設定することをお勧めします。**protection-end-timer** の値を **forever** に設定すると、攻撃が終了しても Detector モジュールはゾーン保護を終了せず、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も削除しません。

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新しいゾーンを Detector モジュールに作成する必要があります。これは、Guard ゾーン テンプレートで作成された新しいゾーンには、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るた

めです。ゾーン テンプレートの詳細については、表 5-1 を参照してください。

ゾーンは、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 プロンプトは次のようになっています。

  ```
  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 プロンプトは次のようになっています。

  ```
  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。

Detector モジュールは、ゾーン設定モードでの **show** コマンドの出力において、ゾーン ID フィールドの隣に (Guard/Detector) を表示します。

P.5-6 の「ゾーン テンプレートからの新しいゾーンの作成」を参照してください。

ステップ 2　ゾーンの特性を設定します。

P.5-10 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、次のいずれかのコマンドを入力して guard 設定モードに入ります。

- **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属性を設定できます。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ネットワーク 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 リストに定義されてい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、既存の設定を新しい設定で置き換えます。

- 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、ゾーンのリモート サーバ リストに記載されているすべてのネットワーク 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リモート リストを検索します。詳細については、P.5-25 の「ゾーン設定の自動エクスポート」を参照してください。

  ゾーンのリモート サーバ リストと Detector モジュールのデフォルトのリモート 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使用します。

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

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

表 5-5　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、ゾーン設定をネットワーク サーバに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.5-17 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 モジュールとのゾーン設定の同期化

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。ゾーン ポリシーを攻撃の特性に合せて調整するために Guard モジュールのゾーン 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いる場合は、Guard モジュールのゾーン設定を Detector モジュールに同期させる必要が生じる場合があります。次の 2 点が保証されるように、特定のポリシーのしきい値を固定値として設定したり、ポリシーのしきい値の固定乗数を設定することができます。

- Detector モジュールが正しいポリシーしきい値を持ち、将来の DDoS 攻撃を適切に検出できる。
- Detector モジュールから将来ゾーン設定を同期化したときに正しいゾーン設定が Guard モジュールで維持される。これは、Detector モジュールが継続してゾーン トラフィックの特性をラーニングする場合に必要になることがあります。

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。

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。

Guard モジュールからゾーン設定およびポリシーを Detector モジュールに同期させるには、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。次のいずれかのコマンドを入力します。

- **sync zone** *zone-name remote-guard-address* **local**（グローバル モードで入力）
- **sync** *remote-guard-address* **local**（ゾーン設定モードで入力）

表 5-6 で、**sync** コマンドの引数について説明します。

表 5-6　sync コマンドの引数とキーワード

パラメータ	説明
zone	指定のゾーンの設定を同期させます。
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）。
local	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。

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、ゾーン設定モードで **detect** コマンドまたは **learning** コマンドを使用してゾーンを再度アクティブにします。

詳細については、第 9 章「ゾーンのトラフィックの異常の検出」および P.5-14 の「Detector モジュールの Cisco Anomaly Guard Module とのゾーン設定の同期」を参照してください。

次の例は、ゾーン scannet を非アクティブにし、Guard モジュールのゾーン設定を IP アドレス 192.168.55.10 の Detector 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# sync 192.168.55.10 local
user@DETECTOR-conf-zone-scannet# detect learning
```

Detector モジュールからのゾーン設定の同期

Guard モジュールがゾーン保護をアクティブにしたときに Guard モジュールのゾーン設定とポリシーが必ずアップデートされるように、ゾーン設定とポリシーを Guard モジュールのゾーンと同期させることができます。このプロセスによって、Detector モジュールでゾーンを一度設定し、継続的にゾーン トラフィックの特定をラーニングしたり、さらに、Guard モジュールで同一のゾーン設定とポリシーを保持することでゾーン 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。

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。

（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、次のいずれかのコマンドを使用します。

- **sync zone** *zone-name* **local** {**remote-guards** | *remote-guard-address-to*}
  （グローバル モードで入力）
- **sync local** {**remote-guards** | *remote-guard-address-to*}
  （ゾーン設定モードで入力）

表 5-7 に、**sync** コマンドの引数とキーワードを示します。

表 5-7　sync コマンドの引数とキーワード

パラメータ	説明
zone	指定のゾーンの設定を同期させます。
zone-name	既存のゾーンの名前。
local	Detector モジュールのゾーンの設定とポリシーを Guard モジュールに同期させます。

表 5-7　sync コマンドの引数とキーワード（続き）

パラメータ	説明
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-to	リモート Guard の Ip アドレス。Detector モジュールは、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
```

次の例は、ゾーンの設定を IP アドレスが 192.168.100.5 のリモート Guard と同期させる方法を示しています。

```
user@DETECTOR-conf-zone-scannet# sync local 192.168.100.5
```

ゾーン設定のオフラインでの同期

Detector モジュールのゾーン設定と Guard モジュール のゾーン設定は、同期させることができます。これは、Detector モジュールと Guard モジュールの間で安全な通信チャネルを確立できない場合でも可能です。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）デバイス経由で Guard モジュールと通信する場合。

Detector モジュールのゾーン設定を Guard モジュールのゾーン設定とオフラインで同期させるには、FTP、Secure FTP（SFTP）、または Secure Copy（SCP）を使用して、まずゾーン設定を Detector モジュールからネットワーク サーバにエクスポートし、次にそのゾーン設定を手動で Guard モジュールにインポートします。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ないため、Detector モジュールがゾーン トラフィックの異常を検出したときは、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.5-6 の「ゾーン テンプレートからの新しいゾーンの作成」を参照）。
- 設定を SFTP または SCP を使用してネットワーク 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.4-40 の「SFTP 接続および SCP 接続用の鍵の設定」参照）。

Detector モジュールのゾーン設定と Guard モジュールのゾーン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　次のいずれかの方法で、ソース デバイス（Guard モジュールまたは Detector モジュール）のゾーン設定をエクスポートします

- 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。詳細については、P.5-25 の「ゾーン設定の自動エクスポート」を参照してください。
- 手動：次のいずれかのコマンドをグローバル モードで入力してゾーン設定をエクスポートします。
  - **copy zone** *zone-name* **guard-running-config ftp** *server remote-path* [*login password*]]
  - **copy zone** *zone-name* **guard-running-config** {**sftp** | **scp**} *server remote-path login*

  詳細については、P.5-27 の「ゾーン設定の手動エクスポート」を参照してください。

ステップ 2　グローバル　モードで次のコマンドを入力して、ネットワーク　サーバからターゲット デバイスにゾーン設定をインポートします。

（注）　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します。

- **copy ftp running-config** *server full-file-name* [*login* [*password*]]
- **copy** {**sftp** | **scp**} **running-config** *server full-file-name login*
- **copy** *file-server-name* **running-config** *source-file-name*

詳細については、P.13-7 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。

ゾーン設定の自動エクスポート

Detector モジュールがゾーン設定をネットワーク サーバへ自動的にエクスポートするように設定できます。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が受け入れられるたびに、ゾーンの設定をエクスポートします（しきい値調整フェーズの結果がいつ受け入れられるかの詳細については、P.8-16 の「定期的なアクションの設定」を参照してください）。

ゾーン設定を自動的にエクスポートするには、ネットワーク サーバを設定する必要があります。ネットワーク サーバには、FTP、Secure FTP（SFTP）、Secure Copy（SCP）が設定できます。ネットワーク サーバは、次のリストに設定できます。

- ゾーンのリモート 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ネットワーク サーバのリスト。
- Detector モジュールデフォルトのリモート サーバ リスト：ネットワーク サーバのデフォルト リスト。ゾーンのリモート 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。

ゾーン設定をネットワーク 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　**file-server** コマンドを入力してネットワーク サーバを定義します。

SFTP または SCP を使用してネットワーク サーバを設定する場合は、Detector モジュールが SFTP 通信および SCP 通信で使用する SSH 鍵を設定する必要があります。

詳細については、P.13-10 の「ファイルを自動的にエクスポートする方法」を参照してください。

（注）　Detector モジュールが特定のネットワーク 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リモート サーバ リストまたはゾーンのリモート 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）ゾーン設定モードで次のコマンドを入力して、ネットワーク サーバをゾーンのリモート サーバ リストに追加します。

```
export sync-config file-server-name
```

file-server-name 引数には、ネットワーク サーバの名前を指定します。**file-server** コマンドを使用してネットワーク サーバを設定する必要があります。

リモート サーバ リストからネットワーク 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）ゾーン設定モードで次のコマンドを入力して、ネットワーク サーバを Detector モジュールのデフォルトのリモート サーバ リストに追加します。

```
export sync-config file-server-name
```

file-server-name 引数には、ネットワーク サーバの名前を指定します。**file-server** コマンドを使用してネットワーク サーバを設定する必要があります。

リモート サーバ リストからネットワーク 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　**learning-params sync accept** コマンドを入力して、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、ゾーン設定をネットワーク 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。

詳細については、P.5-17 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。

次の例は、ゾーンのリモート サーバ リストにネットワーク サーバを追加する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# export sync-config Corp-FTP-Server
```

Detector モジュールがゾーン設定をエクスポートするために使用するネットワーク サーバのデフォルトのリストを表示するには、設定モードで **show sync-config file-servers** コマンドを使用します。

リモート サーバ リストを表示するには、ゾーン設定モードで **show sync-config file-servers** コマンドを使用します。

ゾーン設定の手動エクスポート

ゾーン設定をネットワーク サーバにエクスポートすることができます。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。

ゾーンの設定をネットワーク サーバにエクスポートするには、グローバル モードで次のいずれかのコマンドを使用します。

- **copy zone** *zone-name* **guard-running-config ftp** *server full-file-name* [*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** | **scp**} *server full-file-name login*（SFTP または SCP を使用してゾーンの設定をネットワーク サーバにエクスポートします）。

- **copy zone** *zone-name* **guard-running-config** *file-server-name dest-file-name*（ゾーンの設定をネットワーク サーバにエクスポートします）。
- **copy zone** *zone-name* **guard-running-config ***（ゾーン ファイル サーバ リストおよびデフォルトのファイル サーバ リストに定義されているネットワーク サーバにゾーンの設定をエクスポートします）。

SFTP および SCP は安全な通信を SSH に依存しているので、**sftp** オプションまたは **scp** オプションを使用して **copy** コマンドを入力する前に Detector モジュールが使用する鍵を設定していない場合、Detector モジュールはパスワードの入力を求めます。Detector モジュールがセキュアな通信のために使用する鍵を設定する方法の詳細については、P.4-40 の「SFTP 接続および SCP 接続用の鍵の設定」を参照してください。

表 5-8 で、**copy guard-running-config** コマンドの引数について説明します。

表 5-8　copy guard-running-config コマンドの引数とキーワード

パラメータ	説明
zone *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。
guard-running-config	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だけをエクスポートします。
ftp	FTP を使用しているネットワーク サーバにゾーンの設定をエクスポートします。
sftp	SFTP を使用しているネットワーク サーバにゾーンの設定をエクスポートします。
scp	SCP を使用しているネットワーク サーバにゾーンの設定をエクスポートします。
server	ネットワーク サーバの IP アドレス。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 192.168.10.2）。
full-file-name	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 5-8　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	サーバのログイン名。 *login* 引数は、FTP サーバを定義する場合のオプションです。ログイン名を入力しなかった場合、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パスワードを要求されます。
file-server-name	設定ファイルをエクスポートするネットワーク サーバの名前。**file-server** コマンドを使用してネットワーク サーバを設定する必要があります。 SFTP または SCP を使用してネットワーク サーバを設定する場合は、Detector モジュールが SFTP 通信および SCP 通信で使用する SSH 鍵を設定する必要があります。 詳細については、P.13-2 の「ファイル サーバの設定」を参照してください。
destination-file-name	リモート サーバ上の設定ファイルの名前。Detector モジュールは、**file-server** コマンドを入力してネットワーク サーバに対して定義したディレクトリの宛先ファイル名を使用してネットワーク サーバ上に設定ファイルを保存します。
*	ゾーン設定のうち、ゾーンのリモート サーバ リストおよびデフォルトのリモート サーバ リストに定義されている、すべてのネットワーク サーバに Guard モジュールのゾーンを設定するために必要な部分のみをエクスポートします（詳細については、P.5-25 の「ゾーン設定の自動エクスポート」を参照してください）。

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>
```

サンプル シナリオ

次のサンプル シナリオは、Detector モジュールのゾーン設定を Detector モジュールのゾーン設定と同期させて、ゾーンを保護し、ゾーン トラフィック特性のラーニングを続行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 モジュール上に新しいゾーンを作成および設定します。

   Detector モジュールは、ゾーン設定モードでの **show** コマンドの出力において、ゾーン ID フィールドの隣に (Guard/Detector) を表示します。

   詳細については、P.5-6 の「ゾーン テンプレートからの新しいゾーンの作成」を参照してください。

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.9-11 の「デフォルトのリモート Guard リストの設定」および P.9-12 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. **learning policy-construction** コマンドを入力して、Detector モジュールがゾーン ポリシーを構築するように設定します。

4. **detect learning** コマンドを入力して、Detector モジュールがトラフィックの異常を検出しながら、ゾーン トラフィックをラーニングしてポリシーしきい値を調整するように設定します。

   詳細については、第 9 章「ゾーンのトラフィックの異常の検出」を参照してください。

5. **learning-params periodic-action auto-accept** コマンドを使用して、Detector モジュールが 24 時間ごとにポリシーしきい値を受け入れ、次々に変化するトラフィック パターンに合せてゾーン ポリシーを最新のものにするように設定します。

   詳細については、P.8-16 の「定期的なアクションの設定」を参照してください。

6. Detector モジュールが、新しくラーニングしたポリシーの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設定し、Detector モジュールが新しいゾーン ポリシーのしきい値をラーニングした場合に、Guard モジュールのゾーン ポリシーも必ず更新されるようにします。

   learning-params sync コマンドを使用して、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。詳細については、P.5-17 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 モジュールによるゾーン保護をアクティブにする前に、Detector モジュールのゾーン設定を Guard モジュールのゾーン設定と同期させるように設定し、Guard モジュールがゾーン保護をアクティブにした場合に、Guard モジュール上のゾーン設定とポリシーが必ず更新されるようにします。

   learning-params sync コマンドを使用します。

   詳細については、P.5-17 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、次の処理を実行します。

   - Guard モジュール のゾーン設定が更新されていることを確認する。Guard モジュールのゾーン設定が Detector モジュールのゾーン設定と同じものでない場合、Detector モジュールはゾーン設定を Guard モジュールと同期させます。
   - 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する）。
   - ゾーンのラーニング プロセスを停止するが、ゾーン トラフィックの異常の検出は続行し、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しないようにする。

   攻撃が進行中でも、Guard モジュール上でゾーン ポリシーを変更できます。

   Detector モジュールは、Guard モジュールを常にポーリングします。Detector モジュールが、Guard モジュールがゾーン保護を非アクティブにしたことを確認し（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する）、トラフィックの異常がなくなったことを確認すると、Detector モジュールはゾーンの異常検出とラーニング プロセスを非アクティブにします。

9. ゾーン ポリシーを攻撃の特性に合せて調整するために Guard モジュールのゾーン ポリシーを手動で変更した場合、その新しいポリシーを Detector モジュールに同期させることができます。特定のポリシーしきい値を固定値として設定することや、ポリシーしきい値の固定乗数を設定することがゾーントラフィックに必要になった場合に、この処理が重要になります。ゾーン設定を Detector モジュールと同期させることにより、Detector モジュールが正しいポリシーしきい値を持ち、将来のしきい値調整フェーズでしきい値を正しく計算し、正しいしきい値を持つ Guard モジュールポリシーが更新されます。

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

   詳細については、P.5-20 の「Detector モジュールとのゾーン設定の同期化」および第 9 章「ゾーンのトラフィックの異常の検出」を参照してください。