CHAPTER 5

ゾーンの設定

この章では、Cisco Traffic Anomaly Detector モジュール（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。

この章には、Detector モジュールの関連製品である Cisco Guard（Guard）についての記述があります。Guard は、DDoS 攻撃（分散型サービス拒絶攻撃）を検出して軽減するデバイスです。Guard は、ゾーン トラフィックが通過する際に攻撃トラフィックをドロップして正常なトラフィックをネットワークに戻し、ゾーン トラフィックをクリーンにします。Detector モジュールは、ゾーンが攻撃を受けていると判断したときに、Guard の攻撃軽減サービスをアクティブにできます。また、Detector モジュールは Guard とゾーン設定を同期させることができます。Guard の詳細については、『*Cisco Anomaly Guard Module Configuration Guide*』または『*Cisco Guard Configuration Guide*』を参照してください。

この章は、次の項で構成されています。

ゾーンについて

ゾーンとは、Detector モジュールが DDoS 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、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、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：ゾーン名とゾーンの説明を定義することにより、ゾーンを作成できる。詳細については、P.5-5 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する。詳細については、P.5-8 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できる。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。
- 異常検出オプションの定義：Detector モジュールがゾーン異常検出を実行する方法を定義できる。詳細については、第 9 章「ゾーン トラフィック異常の検出」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 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 の両方のアトリビュートを設定して、ゾーン設定を Guard 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。

  GUARD_ テンプレートを使用して作成するゾーンの設定方法の詳細については、P.5-12 の「同期のためのゾーン作成」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 ワーム攻撃を Detector モジュールが検出できるようにするゾーン 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.7-23 の「ワーム ポリシーについて」を参照）。
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。

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	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。128 Kb、1 Mb、4 Mb、および 512 Kb のリンクを対象とした次のテンプレート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。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 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。

1. VoIP = Voice over IP
2. IRC = Internet Relay Chat

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、または事前定義されたゾーン テンプレートを使用して、ゾーンを作成できます。使用するゾーン 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。

- 事前定義されたゾーン テンプレートの使用 : テンプレートから、デフォルトのポリシーおよびフィルタで新しいゾーンを作成します。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。
- 既存のゾーンのゾーン テンプレートとしての使用 : 既存のゾーンと同じ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します。この方式は、新しいゾーンに既存のゾーンのトラフィック パタ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.5-8 の「ゾーンのアトリビュートの設定」を参照してください。

この項では、次のトピックについて取り上げます。

ゾーン テンプレートからの新しいゾーンの作成

ゾーン テンプレートを使用して新しいゾーンを作成する場合は、ゾーン テンプレートによって、事前定義されたポリシーおよびポリシーしきい値のセットが新しいゾーン設定に提供されます。

テンプレートを使用して新しいゾーンを作成するには、設定モードで次のコマンドを使用します。

zone *zone-name* [*template-name*] [**interactive**]

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
zone-name	ゾーンの名前。次のいずれかのタイプのゾーン名を入力します。 • 新しいゾーン名：1 ～ 63 文字の英数字の文字列を入力します。この名前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。 • 既存のゾーン名：既存のゾーンの名前を入力すると、現在のゾーン設定が削除され、指定したゾーン テンプレートの設定アトリビュートを使用して、同じゾーン名で新しいゾーンが作成されます。
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。新しいゾーン名を入力して、ゾーン テンプレートを指定しない場合、Detector モジュールは DETECTOR_DEFAULT テンプレートを使用してゾーンを作成します（ゾーン テンプレートの詳細については、P.5-3 の「ゾーン テンプレートの使用」を参照）。 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、設定を何も変更せずに、既存のゾーンのゾーン設定モードに入ります。 使用可能なゾーン テンプレートのリストについては、表 5-1 を参照してください。
interactive	（オプション）インタラクティブ検出モードでゾーン異常検出を実行するように Detector モジュールを設定します。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。

zone コマンドを入力すると、Detector モジュールは新しいゾーンの設定モードに入ります。

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

既存のゾーンのコピーを作成することにより、新しいゾーンを作成できます。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、ソース ゾーンのプロパティすべてが、新しいゾーンにコピーされます。ゾーンのスナップショットをソース ゾーンとして指定すると、ゾーン ポリシーがスナップショットからコピーされます。

ゾーンのコピーを作成するには、次のコマンドのいずれかを使用します。

- **zone** *new-zone-name* **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	（オプション）既存のスナップショットの ID。詳細については、P.8-17 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#
```

zone コマンドを入力すると、Detector モジュールは新しいゾーンの設定モードに入ります。Detector モジュールは、新しいゾーンのポリシーを未調整（ゾーン固有の値に調整されていない）としてマークします。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（P.8-8 の「しきい値調整フェーズのアクティブ化」を参照）。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（P.8-12 の「ポリシーに対する調整済みのマーク付け」を参照）。

ゾーンのアトリビュートの設定

ゾーンの IP アドレスやゾーンの説明などのゾーン設定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*：このコマンドは、グローバル モードで使用します。
- **zone** *zone-name*：このコマンドは、設定モードまたはゾーン設定モードで使用します。

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.4-13 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　ゾーンの IP アドレスを定義するには、次のコマンドを入力します。

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

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.5-9 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 文字の英数字です。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　（オプション）ゾーン設定モードで **show running-config** コマンドを入力し、新しく設定したゾーン設定を表示して確認します。

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てから、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** コマンドの引数とキーワードを示します。

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	（オプション）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 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 192.168.100.1）。 デフォルトでは、IP アドレスはゾーンの IP アドレス範囲に含まれます。 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した場合は、次のいずれかまたは両方のタスクを実行して、ゾーン設定ポリシーおよびポリシーしきい値をアップデートします。

- 新しいサービスの定義：ゾーン ネットワークで定義されていないサービスが新しい IP アドレスまたはサブネット上にある場合は、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.8-5 の「ポリシー構築フェーズのアクティブ化」および P.7-10 の「サービスの追加」を参照してください。
- ポリシーしきい値の調整：次のいずれかの方法を使用して、変更したアドレス範囲に合せてポリシーしきい値を調整します。

- 検出およびラーニング機能：検出およびラーニング機能をイネーブルにする場合、**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。

注意　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.8-14 の「検出およびラーニング機能のイネーブル化」および P.8-12 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。

- しきい値調整フェーズ：検出およびラーニング機能を使用しない場合は、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.8-8 の「しきい値調整フェーズのアクティブ化」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。

除外される IP アドレスを削除するには、**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。

Guard モジュール とのゾーン設定の同期

同期プロセスにより、Detector モジュールと、Detector モジュールに関連付けた Guard の両方で、ゾーン設定のコピーを保持できます。同期プロセスを使用して、リモート サーバ上で Detector モジュールのゾーン設定のコピーを保持することもできます。

同期プロセスは、Detector モジュールのみから実行し、次の操作を行うことができます。

- Detector モジュールから Guard への同期：Detector モジュールがゾーン設定を自分自身から Detector モジュールのリモート Guard リストに定義されている Guard にコピーします。リモート Guard リストの詳細については、P.9-6 の「ゾーンを保護するためのリモート Guard のアクティブ化」を参照してください。このオプションでは、Detector モジュールと Guard が Secure Sockets Layer（SSL）通信チャネルを使用してオンラインで相互に通信できるように、Detector と Guard を設定する必要があります（P.4-18 の「Guard との通信の確立」を参照）。
- Guard から Detector モジュールへの同期：Detector モジュールがゾーン設定を Guard から自分自身にコピーします。この処理により、Detector モジュール上でゾーン設定に対して行った変更で、Guard のゾーン設定をアップデートできます。このオプションでは、Detector モジュールと Guard が Secure Sockets Layer（SSL）通信チャネルを使用してオンラインで相互に通信できるように、Detector と Guard を設定する必要があります（P.4-18 の「Guard との通信の確立」を参照）。
- Detector モジュールからリモート サーバへのエクスポート：Detector モジュールがゾーン設定を自分自身からネットワーク サーバにエクスポートします。

手動でゾーン設定を同期させることも、次のタスクを自動的に実行するように Detector モジュールを設定することもできます。

- しきい値調整フェーズの結果を受け入れた後に、Guard またはリモート サーバとゾーン設定を同期させる。
- Guard をアクティブにしてゾーン保護を行う前に、Guard とゾーン設定を同期させる。

同期プロセスを使用すると、Detector モジュールでゾーンを作成、設定、および変更してから、同じゾーン情報で Guard をアップデートできます。また、同期プロセスにより、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、自分自身と Guard の両方でゾーン ポリシーを最新の状態に保つことができます。Detector モジュールが Guard のためにラーニングを実行できるようにすると、ゾーン トラフィックを Guard に宛先変更する必要がなくなります。

この項では、次のトピックについて取り上げます。

同期のための設定ガイドラインについて

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

- 両方のデバイス タイプの設定パラメータを含むいずれかの 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（使用可能なゾーン テンプレートの詳細については、表 5-1 を参照）。
- ゾーン ポリシーを正しく同期させるには、Guard 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（同じトラフィック レートやプロトコルなど）が流れるようにする必要があります。
- Detector モジュールと Guard の間の通信が可能になるように SSL 通信接続チャネルを設定します（P.4-18 の「Guard との通信の確立」を参照）。
- デバイスを交換した場合、または Detector モジュールと Guard が通信に使用するインターフェイスの IP アドレスを変更した場合は、Detector モジュールと Guard が安全な通信に使用する SSL 証明書を再生成します（P.4-20 の「SSL 証明書の再生成」を参照）。
- Guard 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。

同期のためのゾーン作成

Detector モジュールと Guard との間でゾーン設定を同期させるには、いずれかの Guard ゾーン テンプレートを使用して Detector モジュール上でゾーンを作成する必要があります。Guard ゾーン テンプレートには、Guard 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 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。

いずれかの Guard ゾーン テンプレートを使用してゾーンを作成する場合は、次の設定モードでゾーンを設定します。

- ゾーン設定モード：リモート Guard の定義など、Detector モジュールに固有のゾーン アトリビュートを設定します。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。ゾーン設定のコマンド 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 に固有のゾーン アトリビュートを設定します。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。guard 設定モードのコマンド 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 と Detector モジュールの両方に共通の定義を設定します。

  Guard と Detector モジュールの両方に共通のゾーン アトリビュートを変更する場合、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 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 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.5-5 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）。

Guard ゾーン テンプレートを使用して新しいゾーンを作成する場合、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。

ステップ 2　ゾーン アトリビュートを設定します（P.5-8 の「ゾーンのアトリビュートの設定」を参照）。

ステップ 3　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、Guard に固有の特性を設定します。

- **guard-conf**：このコマンドは、ゾーン設定モードで使用します。
- **configure** *zone-name* **guard-conf**：このコマンドは、グローバル モードで使用します。
- **zone** *zone-name* **guard-conf**：このコマンドは、設定モードで使用します。

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 に固有のすべてのゾーン アトリビュートを設定できます。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

Detector モジュールを設定して、次のタスクを自動的に実行できます。

- 次の場合に、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リモート Guard と同期します。
  - 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。
  - Detector モジュールがゾーンを保護するために Guard をアクティブ化する前。

  ゾーンのリモート Guard リストでガードを何も定義していない場合、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 と同期します。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上の次のリモート 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。
- 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る場合、ゾーンのリモート サーバ リストで定義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。ゾーンのリモート サーバ リストが空の場合、Detector モジュールは、Detector モジュールの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.5-18 の「ゾーン設定のネットワーク サーバへ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設定をエクスポートしません。

ゾーン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	ゾーン設定をリモート Guard と同期させ、Detector モジュールがラーニング プロセスのしきい値調整フェーズの結果を受け入れるたびに、ゾーン設定をリモート サーバにエクスポートします。
remote-activate	Guard をアクティブにしてゾーンを保護する前に、ゾーン設定をリモート Guard と同期します。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します。 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、Detector モジュールがラーニング 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
```

自動的な同期およびエクスポート機能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。

Guard から Detector モジュールへのゾーン設定の同期

Detector モジュールによって、ゾーン設定を Guard から Detector モジュールにコピーすることができます。ゾーンがすでに Detector モジュールに存在する場合、既存の設定が Guard の新しい設定で上書きされます。

攻撃の特性に合せて調整するために Guard 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 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 Guard に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 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.7-17 の「固定値としてのしきい値の設定」および P.7-17 の「しきい値の乗数の設定」を参照してください。

Guard からゾーン設定を Detector モジュールに同期させるには、Detector モジュールで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　次のいずれかのコマンドを入力して、Detector モジュールのゾーン設定を Guard に同期します。

- **sync zone** *zone-name remote-guard-address* **local**：このコマンドは、グローバル モードで使用します。
- **sync** *remote-guard-address* **local**：このコマンドは、ゾーン設定モードで使用します。

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	指定のゾーン設定を同期します。
zone-name	既存のゾーンの名前。
remote-guard-address	リモート Guard 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 192.168.100.1）。
local	Detector モジュールのゾーン設定を Guard に同期します。

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 トラフィック異常の検出」および P.5-11 の「Guard モジュール 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 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 Guard へのゾーン設定の同期

Guard がゾーン保護をアクティブにしたときに Guard 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、Detector モジュールのゾーン設定を Guard 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 トラフィックの特性をラーニングしたり、さらに、Guard 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 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 にコピーします。Guard 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）　ゾーンの同期プロセスを開始する前に、Guard　が現在ゾーンを保護していないことを確認します。ゾーン保護を非アクティブにしてからゾーン設定を同期します。

次のいずれかのコマンドを入力して、Detector モジュールからゾーン設定およびポリシーを同期します。

- **sync zone** *zone-name* **local** {**remote-guards** | *remote-guard-address-to*}：このコマンドは、グローバル モードで使用します。
- **sync local** {**remote-guards** | *remote-guard-address-to*}：このコマンドは、ゾーン設定モードで使用します。

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	指定のゾーン設定を同期します。
zone-name	既存のゾーンの名前。
local	Detector モジュールのゾーン設定とポリシーを Guard に同期します。
remote-guards	ゾーン設定を、ゾーンのリモート Guard リストにあるすべてのリモート Guard と同期します。ゾーンのリモート Guard リストが空の場合は、ゾーン設定を、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 と同期します。
remote-guard-address-to	リモート Guard の IP アドレス。Detector モジュールは、ゾーン設定を指定されたリモート Guard と同期します。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 192.168.100.1）。

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

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

次の例は、ゾーン設定を IP アドレスが 192.168.100.5 のリモート Guard と同期す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

この項に示すオフラインでの同期手順を使用して、Detector モジュールのゾーン設定を Guard に同期することができます。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。

- この 2 つのデバイス間で安全な通信チャネルを確立できない場合（Guard と Detector モジュールが相互に通信できない）。
- 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 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、FTP、SFTP、または 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ネットワーク サーバから Guard にインポートします。

Detector モジュールのゾーンと Guard 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　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.5-5 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）。

ステップ 2　次のいずれかの方法で、Detector モジュールから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（P.5-18 の「ゾーン設定のネットワーク サーバへの自動エクスポート」を参照）。
- 手動：グローバル モードで次のいずれかのコマンドを入力して、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*

  copy zone コマンドの引数とキーワードの説明については、表 5-9（P.5-20）を参照してください。詳細については、P.5-19 の「ゾーン設定のネットワーク サーバへの手動エクスポート」を参照してください。

ステップ 3　Guard から、グローバル モードで次のいずれかのコマンドを入力して、ネットワーク サーバからゾーン設定をインポートします。

（注）　Guard が現在ゾーンを保護している場合は、ゾーンを非アクティブにしてからゾーン設定をインポートします。

- **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*

表 5-8 に、**copy** コマンドの引数とキーワードを示します。

表 5-8　copy コマンドの引数

パラメータ	説明
running-config	実行設定を指定します。
ftp	FTP を指定します。
sftp	SFTP を指定します。
scp	SCP を指定します。
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 ディレクトリでファイルを検索します。
login	（オプション）サーバのログイン名。*login* 引数は、FTP サーバを定義するときは省略可能です。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パスワードを要求されます。

表 5-8　copy コマンドの引数（続き）

パラメータ	説明
file-server-name	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。
source-file-name	ファイルの名前。

詳細については、P.13-5 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。

（注）　Guard と Detector の間に安全な通信チャネルが存在しない場合は、ゾーン設定をオフラインで同期させた後、Detector がゾーン トラフィックの異常を検出したときに、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。

ゾーン設定のネットワーク サーバへ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、ゾーン設定をエクスポートします（ラーニング プロセスのしきい値調整フェーズの結果がいつ受け入れられるかの詳細については、P.8-11 の「定期的なアクションの設定」を参照）。

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 サーバを定義する必要があります。ネットワーク サーバには、FTP、SFTP、または SCP が定義できます。ネットワーク サーバは、次のリストに定義できます。

- 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 モジュールの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　設定モードで、**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（詳細についてはP.13-2 の「ファイル サーバの設定」を参照）。

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（P.4-27 の「SFTP 接続および SCP 接続用の鍵の設定」を参照）。

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、ステップ 1 で指定したネットワーク サーバの名前を指定します。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** 形式を使用します。

ステップ 3　（オプション）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、ステップ 1 で指定したネットワーク サーバの名前を指定します。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** 形式を使用します。

ステップ 4　ゾーン設定モードで **learning-params sync accept** コマンドを入力して、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.5-13 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。

ゾーンのリモート 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。

ゾーン設定のネットワーク サーバへの手動エクスポート

ゾーン設定をネットワーク サーバに手動でエクスポートすることができます。

グローバル モードで次のいずれかのコマンドを入力して、ゾーン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 ftp** *server full-file-name* [*login password*] : ゾーン設定を 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 サーバにゾーン設定をエクスポートします。

表 5-9 に、**copy guard-running-config** コマンドの引数を示します。

表 5-9　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を指定します。
guard-running-config	Guard モジュール上でゾーンを設定するために必要な、ゾーン設定の一部をエクスポートします。
ftp	FTP を指定します。
sftp	SFTP を指定します。
scp	SCP を指定します。
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。
login	（オプション）サーバのログイン名。*login* 引数は、FTP サーバを定義するときは省略可能です。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.5-18 の「ゾーン設定のネットワーク サーバへの自動エクスポート」を参照してください。

SFTP および SCP はセキュアな通信を SSH に依存しているので、**sftp** 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 モジュールで使用する鍵を設定していない場合、Detector モジュールによってパスワードの入力が求められます。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.4-27 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。

次の例は、ゾーン設定を 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>
```

サンプル同期シナリオ

次のサンプル シナリオは、Detector モジュールのゾーン設定を Guard のゾーン設定と同期させて、Detector モジュールがゾーン トラフィック特性をラーニングする一方でゾーンを保護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。Guard ゾーン テンプレートを使用して新しいゾーンを作成する場合、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.5-5 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 Guard を追加します。

   詳細については、P.9-8 の「デフォルトのリモート Guard リストの設定」および P.9-9 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 トラフィックをラーニングしながら、ゾーン ポリシーを構築できるようにします（P.8-5 の「ポリシー構築フェーズのアクティブ化」を参照）。

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できるようにします（P.8-14 の「検出およびラーニング機能のイネーブル化」を参照）。

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.8-11 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 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 のゾーン ポリシーも必ずアップデート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 Detector モジュールと同期させるように Guard を設定します。詳細については、P.5-13 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 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 のゾーン設定と同期させるように設定し、Guard がゾーン保護をアクティブにした場合に、Guard 上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.5-13 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　のゾーン設定がアップデートされていることを確認する。Guard　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 と同期します。
   - 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する）。
   - ゾーンのラーニング プロセスを停止し、Detector 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。Detector モジュールは、引き続きゾーン トラフィックの異常を探します。

   攻撃が進行中でも、Guard 上でゾーン ポリシーを変更できます。

Detector モジュールは、Guard を常にポーリングします。Detector モジュールが、Guard 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 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 プロセスを再度アクティブにします。

8. 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 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 ポリシーがアップデートされます。

   詳細については、P.7-17 の「固定値としてのしきい値の設定」および P.7-17 の「しきい値の乗数の設定」を参照してください。

   Guard 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、Detector モジュールから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 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.5-14 の「Guard から Detector モジュールへのゾーン設定の同期」および第 9 章「ゾーン トラフィック異常の検出」を参照してください。