ゾーンの設定

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

この章は、次の項で構成されています。

ゾーンについて

ゾーンとは、Guard が Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃からの保護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）

Guard モジュールは、ゾーンのネットワーク アドレスの範囲が重なっていなければ、複数のゾーンを同時に保護できます。

ゾーンに名前を割り当て、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.6-5 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できる。詳細については、P.6-10 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保護レベルを適用し、Guard 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 7 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：ゾーンの保護ポリシーを作成します。このポリシーは、Guard 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。Guard 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 9 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。

表 6-1 に、ゾーン テンプレートを示します。

表 6-1　ゾーン テンプレート

テンプレート	説明
GUARD_DEFAULT	デフォルトのゾーン テンプレート。Guard モジュールは、パケットの送信元 IP アドレスを Guard モジュールの TCP プロキシ IP アドレスに変更する場合があります。ゾーン ネットワークの着信 IP アドレスに基づく ACL[1]、アクセス ポリシー、またはロードバランシング ポリシーを使用していない場合に、このゾーン テンプレートを使用できます。
GUARD_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オンデマンド保護用に設計されたゾーン テンプレート。ゾーン保護要件にいっそうの重点を置き、Guard モジュールのリソースをより節約できるようにするため、これらのゾーンでのゾーン保護は、攻撃されているアドレス範囲でのみアクティブにすることをお勧めします。Guard モジュールで使用される方式を設定し、攻撃されているサブネットまたは範囲に対するゾーン保護を **activation-extent ip-address-only** コマンドによってアクティブにします。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でのみ、Guard モジュール上のゾーン保護をアクティブにできるようにするには、Detector モジュールで **protect-ip-state dst-ip-by-name** コマンドを使用します。

表 6-1　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*）	帯域幅限定リンク ゾーン テンプレートは、128 Kb、1 Mb、4 Mb、および 512 Kb のリンクをそれぞれ対象とした次のものが用意されています。 • GUARD_LINK_128K • GUARD_LINK_1M • GUARD_LINK_4M • GUARD_LINK_512K これらのテンプレートから作成されたゾーンに対しては、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_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[5] 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。 GUARD_VOIP ゾーン テンプレートから作成されたゾーンには、sip_udp ポリシー テンプレートから作成された VoIP トラフィックを処理するための特殊なポリシーが含まれています（詳細については、P.8-5 の「ポリシー テンプレートについてとその設定」を参照）。

1. ACL = Access Control List（アクセス コントロール リスト）
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
5. VoIP = Voice over IP

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。

新しいゾーンには、オンデマンド保護用に調整されたデフォルト ポリシーが割り当てられます。ただし、ゾーンをすぐに保護する必要がない場合は、Guard モジュールにゾーンのトラフィック特性をラーニングさせることをお勧めします。詳細については、P.10-3 の「オンデマンド保護のアクティブ化」を参照してください。または、ゾーンの設定とゾーンのポリシーを Cisco Traffic Anomaly Detector Module（Detector モジュール）からコピーすることもできます。

新しいゾーンは、次の 3 つの方法で作成できます。

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

  新しいゾーンを作成したら、ゾーン 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。
- Detector　モジュールからのゾーン設定のコピー：この方式は、Detector　モジュールとのゾーン設定の同期をイネーブルにする場合に使用します。P.6-15 の「Guard モジュールの Cisco Traffic Anomaly Detector Module とのゾーン設定の同期」を参照してください。

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

ゾーン設定の設定値を変更する方法については、P.6-10 の「ゾーンのアトリビュートの設定」を参照してください。

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
- 既存のゾーンの複製による新しいゾーンの作成

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 GUARD_DEFAULT ゾーン テンプレートから作成されます。
- **zone** *zone-name* [*template-name*] [**interactive**] : 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、Guard 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。これらのデフォルト ポリシーの設定は、オンデマンド保護用に調整されます。

コマンドが正常に実行されると、Guard 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しないで既存のゾーンの名前を入力すると、Guard モジュールは指定されたゾーンの設定モードに入ります。

表 6-2 に、**zone** コマンドの引数とキーワードを示します。

表 6-2　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。

表 6-2　zone コマンドの引数とキーワード（続き）

パラメータ	説明
template-name	（オプション）ゾーンの設定を定義するゾーン テンプレート。デフォルトでは、GUARD_DEFAULT ゾーン テンプレートを使用してゾーンが作成されます。 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 • GUARD_VOIP ゾーン テンプレートの詳細については、P.6-3 の「ゾーン テンプレートの使用」を参照してください。
interactive	（オプション）Guard モジュールがゾーン保護をインタラクティブ方式で実行するように設定します。ポリシーが作成する動的フィルタは、推奨事項として表示されます。各動的フィルタをアクティブにするかどうかを決定する必要があります。詳細については、第 11 章「インタラクティブ保護モードの使用方法」を参照してください。

次の例は、新しいゾーンを作成し、インタラクティブ保護モードに設定する方法を示しています。

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

ゾーンを削除するには、**no zone** コマンドを使用します。ゾーンを削除するときは、ゾーン名の末尾に、ワイルドカード文字としてアスタリスク（*）を使用できます。ワイルドカードを使用すると、同じプレフィ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 6-3 に、**zone** コマンドの引数とキーワードを示します。

表 6-3　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。

表 6-3　zone コマンドの引数とキーワード（続き）

パラメータ	説明
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.9-27 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@GUARD-conf-zone-scannet# zone mailserver copy-from-this
user@GUARD-conf-zone-mailserver#
```

コマンドが正常に実行されると、Guard 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.9-19 の「ポリシーに対する調整済みのマーク付け」を参照してください。

新しいゾーンのアクティベーション インターフェイスは、ソース ゾーンの設定に関係なく zone-name-only に設定されます。詳細については、P.10-5 の「保護アクティベーション方式の設定」を参照してください。

ゾーンのアトリビュートの設定

ゾーンを作成したら、ゾーンのアトリビュートを設定できます。

ゾーンのアトリビュートを設定するには、次の手順を実行します。

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

ゾーン設定モードに入るには、次のコマンドのいずれかを使用します。

- **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.4-20 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。Guard 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保護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.6-13 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、Guard モジュールがゾーンに戻すトラフィックの帯域幅を、ゾーンで処理可能と考えられるトラフィック レートに応じて制限します。

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

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

表 6-4 に、**rate limit** コマンドの引数とキーワードを示します。

表 6-4　rate limit コマンドの引数とキーワード

パラメータ	説明
no-limit	レート リミットなしでゾーンを定義します。
rate	ゾーンに渡すことのできるトラフィック量を指定する、64 より大きな整数。単位は、*rate-units* 引数で指定されます。レート リミットは、最大でバースト リミットの 10 倍まで指定可能です。
burst	ゾーンに渡すことのできるトラフィックの最大ピーク量を指定する、64 より大きな整数。単位は、*rate-units* 引数で指定されるレートの単位に応じて、ビット、キロビット、キロパケット、メガビット、またはパケットになります。*burst* リミットは、最大で *rate* リミットの 8 倍まで指定可能です。
rate-units	レートの単位。単位は次のとおりです。 • **bps**：ビット / 秒 • **kbps**：キロビット / 秒 • **kpps**：キロパケット / 秒 • **mbps**：メガビット / 秒 • **pps**：パケット / 秒

ステップ 4　（オプション）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 5　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、Guard 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@GUARD-conf# zone scannet
user@GUARD-conf-zone-scannet# ip address 192.168.100.32
255.255.255.224
user@GUARD-conf-zone-scannet# ip address exclude 192.168.100.50
user@GUARD-conf-zone-scannet# rate-limit 1000 2300 pps
user@GUARD-conf-zone-scannet# description Demonstration zone
user@GUARD-conf-zone-scannet# show running-config
```

ゾーンの IP アドレス範囲の設定

ゾーン保護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 6-5 に、**ip address** コマンドの引数とキーワードを示します。

表 6-5　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@GUARD-conf-zone-scannet# ip address 192.168.100.32
255.255.255.224
user@GUARD-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たことがない場合は、ゾーン保護をアクティブにする前にポリシー構築フェーズをアクティブにするか、サービスを手動で追加します。詳細については、P.9-7 の「ポリシーの構築」および P.8-15 の「サービスの追加」を参照してください。
- 保護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、Guard モジュールは攻撃を検出できなくなり、Guard 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.9-19 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。
- 保護およびラーニング機能を使用していない場合は、ゾーン保護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.9-11 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。

Guard モジュールの Cisco Traffic Anomaly Detector Module とのゾーン設定の同期

ゾーン設定（ゾーン ポリシーやフィルタを含む）を Detector 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、Guard モジュールと Detector 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.4-27 の「Cisco Traffic Anomaly Detector 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。

同期のためのゾーンを作成して、ゾーンを Detector モジュールから同期させる必要があります。詳細については、『*Cisco Trafiic Anomaly Detector Module Configuration Guide*』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。

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。

- 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。このように設定しないと、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、Detector モジュールおよびすべての関連付けられた Guard デバイスの中央設定ポイントとして使用します。Detector モジュールには、Detector モジュールおよび Guard デバイスとして使用可能なゾーン テンプレートが含まれています。Detector モジュールでゾーン設定を作成してから、Detector モジュールに関連付けるすべての Guard デバイスにその設定をコピーできます。
- 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、Guard 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 Guard 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。

  詳細については、P.10-5 の「保護アクティベーション方式の設定」、P.10-10 の「保護アクティベーション範囲の設定」、および P.10-14 の「保護の無活動タイムアウトの設定」を参照してください。

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。

詳細については、第 10 章「ゾーンの保護」を参照してください。

Guard モジュールがゾーン設定を同期できるようにするには、Guard ゾーン テンプレートのいずれかを使用して、Detector モジュール上にゾーンを作成する必要があります。

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　グローバル モードで次のコマンドを入力して、ゾーン設定をソース デバイス（Guard モジュールまたは Detector モジュール）からエクスポートします。

```
copy zone zone-name running-config ftp
```

P.14-4 の「設定のエクスポート」を参照してください。

ステップ 2　**deactivate** コマンドを使用して、ゾーンを非アクティブにします。

詳細については、P.10-19 の「ゾーン保護の非アクティブ化」を参照してください。

ステップ 3　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。

- **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.14-6 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。

サンプル シナリオ

次のサンプル シナリオは、Detector モジュールでゾーン トラフィック特性のラーニングを続行させながら、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同期させて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。

   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。

2. Detector モジュール上で、ゾーンの SSL リモート Guard リストまたはデフォルトの SSL リモート Guard リストに Guard モジュールを追加します。

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。

5. 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。

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て、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する場合に、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。

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 Detector モジュールを設定して、Guard モジュールがゾーン保護をアクティブにする場合に、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。

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。

（注） この処理は、Detector モジュールのみから実行できます。詳細については、『*Cisco Trafiic Anomaly Detector Module Configuration Guide*』を参照してください。

詳細については、P.8-26 の「固定値としてのしきい値の設定」および P.8-27 の「しきい値の乗数の設定」を参照してください。