CHAPTER 6

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。

この章には、Guard モジュールの関連製品である Cisco Detector（Detector）についての記述があります。Detector は、DDoS 攻撃（分散型サービス拒絶攻撃）を検出するデバイスです。Detector は、ゾーン トラフィックのコピーを分析します。Detector は、ゾーンが攻撃を受けていると判断したときに、Guard モジュールの攻撃軽減サービスをアクティブにできます。また、Detector は Guard モジュールとゾーン設定を同期させることができます。Detector の詳細については、『*Cisco Traffic Anomaly Detector Module Configuration Guide*』および『*Cisco Traffic Anomaly Detector 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、Guard モジュールが DDoS 攻撃から保護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）

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.6-4 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.6-7 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。
- ゾーン保護オプションの定義：アクティベーション範囲や、保護の動作モードなど、ゾーン保護オプションを定義できる。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。

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。攻撃されている IP アドレスまたはサブネットに対してのみ Guard モジュールでのゾーン保護を Detector がアクティブにできるようにするには、Detector で **protect-ip-state dst-ip-by-name** コマンドを使用します。 帯域幅限定リンク ゾーン テンプレートは、128 Kb、1 Mb、4 Mb、および 512 Kb のリンクをそれぞれ対象とした次のものが用意されています。 • GUARD_LINK_128K • GUARD_LINK_1M • GUARD_LINK_4M • GUARD_LINK_512K これらのテンプレートから作成されたゾーンに対しては、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	VoIP[3] 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。VoIP サーバは、SIP[4] 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[5] を使用して音声データを SIP エンド ポイント間で伝送します。 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.8-3 の「ポリシー テンプレートとその設定について」を参照）。

1. ACL = Access Control List
2. IRC = Internet Relay Chat
3. VoIP = Voice over IP
4. SIP = Session Initiation Protocol
5. 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 3 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。デフォルトのポリシーは、オンデマンド保護用に調整されています。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。

  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 : 既存のゾーンをゾーン テンプレートとして使用して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。
- Detector からのゾーン設定のコピー : 同期プロセスを使用して、Detector に作成したゾーン設定を Guard モジュールにコピーします。P.6-10 の「Guard モジュールの Detector とのゾーン設定の同期」を参照してください。

  同期プロセスは、Detector から開始する必要があります。詳細については、『*Cisco Traffic 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.6-7 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。事前定義されたポリシー設定は、オンデマンド保護用に調整されています（P.10-3 の「オンデマンド保護のアクティブ化」を参照）。

事前定義されたゾーン 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 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
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、Guard　モジュールは GUARD_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.6-3 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、Guard 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6-1 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保護を実行するように Guard モジュールを設定します。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。

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

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 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。
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.9-17 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@GUARD-conf-zone-scannet# zone mailserver copy-from-this
user@GUARD-conf-zone-mailserver#
```

zone コマンドを入力すると、Guard モジュールは新しいゾーンの設定モードに入ります。Guard 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.9-8 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.9-12 の「ポリシーに対する調整済みのマーク付け」を参照）。

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

次のゾーン設定アトリビュートを設定できます。

- ゾーンの IP アドレス
- Guard モジュールがネットワークに戻すトラフィックの帯域幅
- ゾーンの説明

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 モードで使用）
- **zone** *zone-name*（設定モードまたはゾーン設定モードで使用）

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]
```

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.6-9 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）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設定します。
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。

表 6-4　rate limit コマンドの引数とキーワード（続き）

パラメータ	説明
burst-size	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）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　（オプション）**show running-config** コマンドを入力し、新しく設定したゾーンの設定を表示して確認します。

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。ただし、ゾーン IP アドレス範囲への IP アドレスの追加や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 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	（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@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：ゾーン設定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.9-5 の「ポリシー構築フェーズのアクティブ化」および P.8-10 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。
  - 保護およびラーニング機能：保護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　ゾーンが攻撃を受けている間は、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。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.9-14 の「保護およびラーニング機能のイネーブル化」および P.9-12 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：保護およびラーニング機能を使用しない場合は、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.9-8 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 アドレスと除外される IP アドレスをすべて削除するには、**no ip address *** コマンドを使用します。

Guard モジュールの Detector とのゾーン設定の同期

同期プロセスにより、Detector と、Detector に関連付けた Guard モジュールの両方で、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 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 のみから実行し、次の操作を行うことができます。

- Detector から Guard モジュールへの同期：Detector がゾーン設定を自分自身から Detector のリモート Guard モジュール リストに定義されている Guard モジュールにコピーします。このオプションでは、Detector と Guard モジュールが 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「Detector との通信の確立」を参照）。
- Guard モジュールから Detector への同期：Detector がゾーン設定を Guard モジュールから自分自身にコピーします。この処理により、Guard モジュール上でゾーン設定に対して行った変更で、Detector 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 と Guard モジュールが 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「Detector との通信の確立」を参照）。
- Detector からリモート サーバへのエクスポート：Detector 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 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 モジュールまたはリモート サーバとゾーン設定を同期させる。
- Guard モジュールをアクティブにしてゾーン保護を行う前に、Guard モジュール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 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 モジュールをアップデートできます。また、同期プロセスにより、Detector 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 モジュールの両方でゾーン ポリシーを最新の状態に保つことができます。Detector が Guard モジュール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 モジュールに宛先変更する必要がなくなります。

（注）　同期プロセスを使用するには、同期のためのゾーンを作成し、そのゾーンを Detector から同期させる必要があります。この項では、Detector と Guard モジュールの間でオフラインでゾーン設定を同期させる方法だけを説明します。他の同期オプションを使用する方法については、『*Cisco Traffic Anomaly Detector Module Configuration Guide*』または『*Cisco Traffic 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 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。

- 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 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 モジュールと Detector 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）が送信されるようにする必要があります。
- Guard モジュールと Detector 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「Detector 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 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 アドレスを変更した場合は、Detector と Guard モジュールが安全な通信に使用する SSL 証明書を再生成します（P.4-20 の「SSL 証明書の再生成」を参照）。
- 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.10-8 の「保護アクティベーション範囲の設定」、および P.10-10 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 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 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 モジュールと Detector が相互に通信できない場合。
- Detector が、Network Address Translation（NAT; ネットワーク アドレス変換）デバイス経由で Guard モジュールと通信する場合。

Detector 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 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 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 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）。

Detector 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、Guard ゾーン テンプレートのいずれかを使用して、Detector 上にゾーンを作成する必要があります。Detector の設定の詳細については、『*Cisco Traffic Anomaly Detector Module Configuration Guide*』、および『*Cisco Traffic Anomaly Detector Configuration Guide*』を参照してください。

Detector 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、Detector からゾーン設定をエクスポートします。

- 自動：特定の状態が発生した場合は必ずゾーン設定をエクスポートするように Detector を設定します。
- 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*

表 6-6 に、**copy guard-running-config** コマンドの引数を示します。

表 6-6　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）。
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	（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 によってパスワードを要求されます。

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.10-13 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 Guard モジュール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*

表 6-7 に、**copy** コマンドの引数とキーワードを示します。

表 6-7　copy コマンドの引数とキーワード

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 ディレクトリからファイルをコピーします。
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、Guard モジュールによってパスワードを要求されます。
file-server-name	ファイル転送サーバ名を表す固有な文字列。
source-file-name	ファイルの名前。

詳細については、P.14-5 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。

同期のサンプル シナリオ

次のサンプル シナリオは、Detector でゾーン トラフィック特性をラーニングしている間に、Detector のゾーン設定を Guard モジュールのゾーン設定と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 上に新しいゾーンを作成および設定します。

   Detector では、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)」と表示されます。

2. Detector 上で、ゾーンの SSL リモート Guard リストまたはデフォルトの SSL リモート Guard リストに Guard 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 がゾーン ポリシーを構築できるようにします。

4. **detect learning** コマンドを入力して、Detector 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。

5. Detector 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 ポリシーをアップデートするように設定します。

6. Detector　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 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 ポリシーも必ずアップデート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、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 を設定し、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アップデートされるようにします。

   Detector は、ゾーンに対する攻撃を検出すると、次の処理を実行します。

   - Guard モジュール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 モジュールのゾーン設定が Detector のゾーン設定と同じものでない場合、Detector 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 は、引き続きトラフィックの異常を探します。

   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 は、Guard モジュールを常にポーリングします。Detector 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 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 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 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 と同期させることにより、Detector 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、正しいしきい値により Guard モジュール ポリシーがアップデートされるようになります。

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

詳細については、P.8-17 の「固定値としてのしきい値の設定」および P.8-18 の「しきい値の乗数の設定」を参照してください。