CHAPTER 10

ゾーンの保護

この章では、Cisco Anomaly Guard Module（Guard モジュール）の設定およびアクティブ化の方法について説明します。

（注） ゾーンの IP アドレス範囲が重なっていない限り、Guard モジュールは複数のゾーンを同時に保護できます。

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。

ゾーン保護の要件とオプションについて

ゾーン保護をアクティブにする前に、次の要件と推奨事項を確認してください。

- トラフィックの宛先変更の設定：トラフィックの宛先変更を設定する必要があります。トラフィックの宛先変更を設定すると、Guard モジュールは、ゾーン トラフィックを通常のネットワーク パスからハイジャックして分析し、攻撃を軽減した後、正当なトラフィックだけをネットワークに戻せるようになります。詳細については、第 5 章「トラフィックの宛先変更の設定」を参照してください。
- ゾーン設定のアップデート：Guard モジュールが通常のトラフィック状態と攻撃トラフィックの違いを正確に認識できるように、次のいずれかの方式を使用して、ゾーン設定を常に最新の状態にしておくことをお勧めします。
  - ラーニング プロセス：Guard モジュールでは、ゾーンのトラフィック特性に基づいて、一連のゾーン固有のポリシーおよびポリシーのしきい値が作成されます。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。
  - ゾーンの同期：Detector は、Guard モジュールのゾーン トラフィックをラーニングし、ゾーン設定を Guard モジュールと同期させます（自動または手動）。詳細については、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。
- 保護およびラーニング機能のアクティブ化：Guard モジュールでは、ラーニング プロセスのしきい値調整フェーズの実行中に、ゾーン トラフィックの異常（攻撃）が監視されます。Guard モジュールで攻撃が検出された場合、しきい値調整フェーズは攻撃が軽減されるまで一時停止されます。

（注）　保護およびラーニングのオプションは、ゾーンが攻撃を受けていないと確信できるときにのみアクティブにします。

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」を参照してください。

- 保護特性の定義：次のオプションの保護特性を設定できます。
  - 動作モード：Guard モジュールがゾーン保護を実行する方法を設定して、Guard モジュールがゾーン保護手段を自動的に適用するか、またはインタラクティブな方式で適用するかを定義します（P.10-4 の「ゾーン保護の動作モードの設定」を参照）。
  - アクティベーション方式：ゾーン名、ゾーンのアドレス範囲、または受信トラフィックのいずれに基づいて、ゾーンをアクティブにするかを定義します（P.10-5 の「保護アクティベーション方式の設定」を参照）。ゾーン保護が Detector のような外部デバイスによってアクティブにされる場合は、アクティベーション方式を設定する必要があります。
  - アクティベーション範囲：ゾーン保護を、ゾーンのアドレス範囲全体についてアクティブにするか、ゾーン内の特定の IP アドレスに限定してアクティブにするかを定義します（P.10-8 の「保護アクティベーション範囲の設定」を参照）。アクティベーション範囲は、ゾーン保護が Detector などの外部デバイスによってアクティブにされる場合に限り、ゾーンに適用されます。
  - 保護の終了のタイムアウト：Guard モジュールがゾーン保護を終了するまでのタイムアウトを定義します（P.10-10 の「保護の無活動タイムアウトの設定」を参照）。

オンデマンド保護のアクティブ化

オンデマンド保護は、定義済みのゾーン テンプレートの 1 つを使用して、Guard モジュールがゾーン トラフィックの特性をラーニングする前に発生したゾーン攻撃を軽減する動作です。それぞれのポリシー テンプレートには、一連の定義済みのポリシーとフィルタが含まれていて、即時にゾーン保護を実行できます。これらのゾーン ポリシーのデフォルトのしきい値は、ゾーンのトラフィックに異常を発見した場合に Guard モジュールがスプーフィング防止機能をすぐにアクティブにするように調整されています。

送信元 IP アドレスをブロック（ドロップ）するために使用されるデフォルトのしきい値は、高い値に設定されています。このしきい値はゾーン トラフィック向けに特別に調整されていないため、非スプーフィング攻撃の場合、オンデマンド保護にはユーザによる軽減プロセスの監視が必要になります。正当なゾーンのレート、悪意のあるトラフィックのレート、および Guard モジュールの軽減アクションを監視する必要があります。

ゾーンに対する攻撃があり、次のいずれかの条件に当てはまる場合は、ゾーンのオンデマンド保護が必要になる場合があります。

- Guard モジュールがゾーン トラフィックのラーニング中である。
- 保護およびラーニング機能がイネーブルになっているが、Guard モジュールにゾーン トラフィックをラーニングする時間がなかった。
- ゾーン設定の現在のポリシーのしきい値が、通常のゾーン トラフィックを正確に表していない。

オンデマンド保護をアクティブにするには、次の手順を実行します。

ステップ 1　次のコマンドを入力して新しいゾーンを作成します。

```
zone new-zone-name [template-name] [interactive]
```

詳細については、P.6-5 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。

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 ip-addr [ip-mask]
```

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。

ステップ 3　次のコマンドを入力してゾーン保護をアクティブにします。

```
protect
```

詳細については、P.10-11 の「ゾーン保護のアクティブ化」を参照してください。

ステップ 4　ゾーンのトラフィック パターンを分析します。詳細については、第 15 章「Guard モジュールによる軽減の分析」を参照してください。

ゾーン保護の動作モードの設定

ゾーンの攻撃中、Guard では、攻撃をどのように軽減するかを決定する動的フィルタが作成されます。それぞれの動的フィルタに関連付けられた軽減アクションを自動的に実行するか、または提案されたアクションを実行するかどうかをユーザが決定するのを待つように、Guard を設定できます。軽減アクションの実行を制御するには、次のいずれかのモードでゾーン保護が実行されるように Guard を設定します。

- 自動保護モード：Guard で動的フィルタが作成されるとすぐにフィルタのアクションが実行されます。この動作モードはデフォルトです。
- インタラクティブ保護モード：Guard の動的フィルタは*推奨事項*として保存されます。ユーザは推奨事項のリストを確認して、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の対象にするかを決定します。

ゾーン設定モードで **show** コマンドを使用して、ゾーンの現在の動作モードを表示します。

インタラクティブ保護モード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。

interactive

インタラクティブ保護モードをディセーブルにして、自動保護モードを使用するには、ゾーン設定モードで次のコマンドを使用します。

no interactive

次のインタラクティブ保護動作の詳細については、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。

- 新しいゾーンを作成する際のインタラクティブ保護モードのイネーブル化
- 保護の推奨事項の管理
- 自動保護モードへの切り替えが必要なタイミングの判断

保護アクティベーション方式の設定

保護アクティベーション方式では、Guard モジュールが外部からの攻撃の兆候を受信したときに、ゾーンが保護を必要とするかどうかを判定する方法を定義します。この兆候には、外部デバイス（Detector など）からのコマンドや、パケット IP アドレスによって決定されるゾーンを宛先とするトラフィックがあります。

次のいずれかの方式を使用して保護をアクティブにするように Guard モジュールを設定できます。

- IP アドレス：ゾーンの一部である IP アドレスまたはサブネットで構成された Detector などの外部デバイスからコマンドを受信した場合に、ゾーン保護をアクティブにします。
- パケット：ゾーン宛のトラフィックを受信したときにゾーン保護をアクティブにします。
- パケットまたは IP アドレス：ゾーンを宛先とするトラフィック（パケット）を受信した場合、またはゾーンのアドレス範囲の一部である IP アドレスまたはサブネットで構成される Detector などの外部デバイスからのコマンドを受信した場合に、ゾーン保護をアクティブにします。
- ゾーン名のみ：ゾーン名に基づいてゾーン保護をアクティブにします。

パケットか、**パケットまたは IP アドレス**の保護アクティベーション方式でゾーンを設定する場合は、次の作業を実行します。

- 外部デバイスを使用して、ゾーンのトラフィックを手動で　Guard　モジュールに宛先変更し、Guard でゾーンのトラフィックを監視できるようにします。
- 同一のアドレス範囲に複数のゾーンを設定しないでください。複数のゾーンを設定すると、ゾーン保護が正しく機能しない場合があります。
- （オプション）**protect-packet activation-sensitivity** コマンドを入力して、Guard モジュールがゾーン保護をアクティブにするために必要な最小受信トラフィック レートを設定します（詳細については、P.10-7 の「ゾーン保護をアクティブにする詳細度の設定」を参照）。

保護アクティベーション方式がゾーン名のみ以外の場合、Guard モジュールは、ゾーンのアクティベーション範囲に従って、ゾーン全体または指定された IP アドレス範囲をアクティブにします。ゾーン名のみの場合、Guard モジュールはゾーン全体をアクティブにします（P.10-8 の「保護アクティベーション範囲の設定」を参照）。

保護アクティベーション方式を設定するには、ゾーン設定モードで次のコマンドを使用します。

activation-interface {**ip-address** | **packet** [**divert**] | **packet-or-ip-address** [**divert**] | **zone-name-only**}

デフォルトは **zone-name-only** です。既存のゾーンを複製してゾーンを作成する場合、複製元になったゾーンの設定に関わらず、保護アクティベーション方式は **zone-name-only** に設定されます。P.6-6 の「既存のゾーンの複製による新しいゾーンの作成」を参照してください。

表 10-1 に、**activation-interface** コマンドのキーワードを示します。

表 10-1　activation-interface コマンドのキーワード

パラメータ	説明
ip-address	ゾーンの一部である IP アドレスまたはサブネットで構成された Detector などの外部デバイスからコマンドを受信した場合に、ゾーン保護をアクティブにします。Guard モジュールはゾーンのデータベースをスキャンし、受信 IP アドレスまたはサブネットを含むアドレス範囲を持つゾーンをアクティブにします。受信 IP アドレスを含むアドレス範囲を持つ複数のゾーンが設定されている場合、Guard モジュールは、プレフィックスが最も長く一致するゾーン（受信 IP アドレスを含むアドレス範囲が最も限定的なゾーン）をアクティブにします。受信 IP アドレスまたはサブネットは、ゾーンの IP アドレス範囲に完全に含まれている必要があります。

表 10-1　activation-interface コマンドのキーワード（続き）

パラメータ	説明
packet	パケット IP アドレスによって決定されるゾーン宛のトラフィックを受信したときにゾーン保護をアクティブにします。Guard モジュールはゾーンのデータベースをスキャンし、受信パケットの IP アドレスを含むアドレス範囲を持つゾーンをアクティブにします。受信パケット IP アドレスを含むアドレス範囲を持つ複数のゾーンが設定されている場合、Guard モジュールは、プレフィックスが最も長く一致するゾーン（受信 IP アドレスを含むアドレス範囲が最も限定的なゾーン）をアクティブにします。受信 IP アドレスまたはサブネットは、ゾーンの IP アドレス範囲に完全に含まれている必要があります。 （注）　**パケット**の保護アクティベーション方式でゾーンを設定する場合、Guard モジュールはアクティブなゾーンが宛先になっていないトラフィックを処理する方法を変更します。そのトラフィックへの注入を設定した場合、Guard モジュールはトラフィックをドロップする代わりに転送します。
divert	（オプション）パケットを受信したときにゾーン保護をアクティブにするように Guard モジュールを設定する場合に、Guard モジュールがスーパーバイザ エンジンに RHI[1] 通知を送信できるようにします。**divert** キーワードは、BGP 通知を隣接ルータに発行して Guard モジュールへのトラフィックの宛先変更を開始することによって、Detector アプライアンスがアップストリームの Guard モジュールをアクティブにするときに使用します。パケットを受信すると Guard モジュールはゾーン保護をアクティブにし、RHI 通知を発行してトラフィックの宛先変更が継続されるようにします。攻撃の期間中にトラフィックの宛先変更を維持する責任は Guard モジュールに移行します。これは、Guard モジュールの攻撃軽減プロセスの結果として Detector が攻撃を感知できなくなると、ルータに対する BGP 通知の発行を停止するからです。 詳細については、『*Cisco Traffic Anomaly Detector Module Configuration Guide*』を参照してください。
packet-or-ip-address	ゾーンを宛先とするトラフィック（パケット）を受信した場合、またはゾーンのアドレス範囲の一部である IP アドレスまたはサブネットで構成される Detector などの外部デバイスからのコマンドを受信した場合に、ゾーン保護をアクティブにします。詳細については、この表の ip-address および packet の保護アクティベーション方式を参照してください。
zone-name-only	ゾーン名に基づいてゾーン保護をアクティブにします。Guard モジュールは、Guard モジュールが Detector などの外部デバイスから受信するコマンドで呼び出されるゾーンのゾーン保護をアクティブにします。このアクティベーション方式はデフォルトです。

1. RHI = Route Health Injection

次の例は、保護アクティベーション方式を設定する方法を示しています。これによって、ゾーンの IP アドレス範囲内のパケットを受信すると、Guard モジュールは保護をアクティブにします。

```
user@GUARD-conf-zone-scannet# activation-interface packet
```

（注）　アクティベーション範囲が **ip-address-only** で（P.10-8 の「保護アクティベーション範囲の設定」を参照）、保護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、ゾーンに対する攻撃が終了したことを Guard モジュールが識別するためのタイマーを設定することをお勧めします（P.10-10 の「保護の無活動タイムアウトの設定」を参照）。**protection-end-timer forever** コマンドを入力した場合、Guard モジュールは、攻撃が終了したときに、ゾーン保護を終了しません。また、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。

受信 IP アドレスまたはパケットが他のどのゾーンの一部でもない場合に備えて、保護のための Guard モジュールのデフォルト ゾーンを作成することができます。デフォルトのゾーンを定義できるのは、ネットワークが同種であるために、同じゾーン テンプレートを使用できる場合だけです。デフォルトのゾーンでラーニング プロセスを実行することはできません。次の必須パラメータを使用して、デフォルトのゾーンを作成します。

- 次の 2 つの IP アドレスを使用して、デフォルトのゾーンを設定します。
  - 0.0.0.0 128.0.0.0
  - 128.0.0.0 128.0.0.0
- アクティベーション範囲を ip-address として定義します（P.10-8 の「保護アクティベーション範囲の設定」を参照）。ゾーンのアクティベーション方式を表示するには、ゾーン設定モードで **show running-config** コマンドを使用します。

ゾーン保護をアクティブにする詳細度の設定

単一 IP アドレスへのトラフィック レートに基づいて、Guard モジュールがゾーン保護をアクティブにするタイミングを決定するアクティベーション詳細度のパラメータを設定できます。単一 IP アドレスへの受信トラフィック レートが、ユーザが定義したアクティベーションの詳細度よりも高い場合に限り、Guard モジュールはゾーン保護をアクティブにします。このアクティベーション詳細度のパラメータは、保護アクティベーション方式（P.10-5 の「保護アクティベーション方式の設定」を参照）が「**パケット**」か「**パケットまたは IP アドレス**」に設定されたすべてのゾーンに適用されます。

ゾーン保護をアクティブにするのに必要な最小パケット レートを定義するには、設定モードで次のコマンドを使用します。

protect-packet activation-sensitivity *min-rate*

min-rate 引数には、Guard モジュールがゾーン保護をアクティブにする原因となる、単一のゾーン宛先 IP アドレス宛ての最小パケット レートを定義します。デフォルトは 0 パケット / 秒（pps）です。

次の例は、アクティベーション詳細度を 10 pps に設定する方法を示しています。

```
user@GUARD-conf# protect-packet activation-sensitivity 10
```

保護アクティベーション範囲の設定

保護アクティベーション範囲は、Guard モジュールが外部からの攻撃の兆候を受信した場合に、ゾーン全体に対してゾーン保護をアクティブにするか、またはゾーンの一部に対してゾーン保護をアクティブにするかを定義します。この兆候には、外部デバイス（Detector など）からのコマンドや、パケット IP アドレスによって決定されるゾーンを宛先とするトラフィックがあります。

Guard モジュールは、次のアクティベーション範囲の方式をサポートします。

- ゾーン全体 : ゾーン全体についてゾーン保護をアクティブにします。Guard モジュールは、ゾーンを宛先とするトラフィックを受信した場合、またはゾーンの一部である IP アドレスまたはサブネットで構成される外部からの攻撃の兆候を受信した場合に、ゾーン保護をアクティブにします。
- IP アドレスのみ : 指定した IP アドレスまたはサブネットに限定してゾーン保護をアクティブにします。Guard モジュールがゾーンを宛先とするトラフィックを受信した場合、またはゾーンの一部である IP アドレスまたはサブネットで構成される Detector などの外部デバイスからのコマンドを受信した場合、Guard モジュールは新しいゾーン（サブゾーン）を作成します。このアクティベーション範囲はデフォルトです。詳細については、P.10-9 の「サブゾーンについて」を参照してください。

アクティベーション範囲を設定するには、ゾーン設定モードで次のコマンドを使用します。

activation-extent {**entire-zone** | **ip-address-only**}

表 10-2 に、**activation-extent** コマンドのキーワードを示します。

表 10-2　activation-extent コマンドのキーワード

パラメータ	説明
entire-zone	ゾーン全体のゾーン保護をアクティブにします。
ip-address-only	指定した IP アドレスまたはサブネットに限定してゾーン保護をアクティブにします。このアクティベーション範囲はデフォルトです。

次の例は、**activation-extent** コマンドを使用して、ゾーン全体のゾーン保護のアクティベーション範囲を設定する方法を示しています。

```
user@GUARD-conf-zone-scannet# activation-extent entire-zone
```

ゾーンのアクティベーション範囲を表示するには、**show running-config** コマンドを使用します。

サブゾーンについて

ゾーンの一部（ソース ゾーンのすべての IP アドレス範囲を含まないゾーン）に対してゾーン保護をアクティブにした場合、Guard モジュールはサブゾーンを作成します。サブゾーンの IP アドレス範囲は、ソース ゾーンのアドレス範囲に含まれます。

サブゾーンの設定は、IP アドレスとゾーン名が異なること以外は、ソース ゾーンの設定と同様です。サブゾーンの名前は、ソース ゾーン名の最初の 30 文字と、アンダースコアで連結された IP アドレスおよびサブネットで構成されます。サブゾーンが単一の IP アドレスで構成される場合、サブネットは追加されません。たとえば、ソース ゾーンの名前が *scannet* で、アドレス範囲 *10.10.10.0* とサブネット *255.255.255.0* を持つ場合に、Guard モジュールが IP アドレス *10.10.10.192* の内部範囲およびサブネット *255.255.255.252* に対してゾーン保護をアクティブにすると、サブゾーンの名前は *scannet_10.10.10.192_255.255.255.252* となります。

サブゾーンの IP アドレスおよびサブネットは、Guard モジュールが外部コマンドとともに受信したもの、または Guard モジュールがゾーン保護をアクティブにする原因となったパケットの IP アドレスです。

ゾーン保護を終了すると、Guard モジュールはサブゾーンを削除します。Guard モジュールは、設定したソース ゾーンのアクティベーション方式と保護の終了のタイムアウトに従って、サブゾーンのゾーン保護を終了します。**no protect** コマンドまたは **deactivate** コマンドを使用してゾーン保護を手動で終了する場合、Guard モジュールはサブゾーンを削除しません。

（注）　**protection-end-timer forever** コマンドを使用して、Guard モジュールがゾーン上の攻撃が終了したタイミングの判断に使用するタイマーを設定する場合、Guard モジュールは攻撃が終了したときにゾーン保護を終了せず、サブゾーンを削除しません。

Guard モジュールがサブゾーンを削除しても、サブゾーンのログと攻撃レポートは消去されません。Guard モジュールがサブゾーンを削除した後にサブゾーンのログおよびレポートを表示するには、次のコマンドを使用します。

- **show log** *sub-zone-name*：詳細については、P.13-3 の「Guard モジュールの設定の表示」を参照してください。
- **show reports** *sub-zone-name* [*report-id* | **current**] [**details**]：詳細については、P.12-10 の「攻撃レポートの表示」を参照してください。

Guard モジュールでゾーンから作成されたサブゾーンのリストは、**show log** コマンドまたは **show reports** コマンドを、サブゾーン名を指定せずに入力することで表示できます。

次の例は、Guard モジュールによって消去されたサブゾーンのログを表示する方法を示しています。

```
user@GUARD-conf-zone-scannet# show logs scannet_10.10.10.192
```

保護の無活動タイムアウトの設定

無活動のまま一定の期間が経過した場合に、ゾーン保護が自動的に停止されるように Guard モジュールを設定できます。Guard モジュールは、動的フィルタの無活動およびドロップされたトラフィックに基づいて無活動の期間を測定します。指定された期間中に、使用中になった動的フィルタがなく、次の両方の条件に該当している場合、Guard モジュールはゾーンに対する攻撃が終了したものと見なします。

- 新しい動的フィルタが追加されていない：動的フィルタを削除するタイミングを Guard モジュールがどのように決定するかについては、P.7-25 の「動的フィルタの非アクティブ化」を参照してください。
- ドロップされるゾーン トラフィックのレートが定義されているしきい値よりも低い：Guard モジュールは、動的フィルタ、ユーザ フィルタ、およびフレックスコンテンツ フィルタが攻撃の一部として識別するゾーン パケットをドロップします。また Guard モジュールは、**rate-limit** コマンドが使用されるときに、ゾーンに対して定義されたレート リミットを超過したトラフィックをドロップします。Guard モジュールはゾーンの Dropped カウンタを使用してドロップするパケットをカウントします（詳細については、P.13-5 の「カウンタを使用したトラフィックの分析」を参照）。デフォルトのしきい値は 1 パケット / 秒です。ドロップ カウンタのしきい値を変更するには、ゾーン設定モードで次のコマンドを入力します。

  attack-detection zone-malicious-rate *threshold*

  threshold 引数には、ドロップされるゾーン パケットの最小レートを定義します。レートがこのしきい値より低くなった場合、Guard モジュールはゾーン保護を終了することがあります。レートがこのしきい値を超えた場合、Guard モジュールはゾーンへの攻撃を識別し、攻撃レポートを作成します。

ゾーンのアクティベーション方式が **packet** である場合、Guard モジュールはゾーンを非アクティブにする前に、受信したトラフィックに基づいて無活動をチェックします。Guard モジュールが保護を非アクティブにするのは、前の条件が当てはまり、ゾーンへのパケットが受信されなかった場合のみです。

無活動タイムアウトを指定するには、ゾーン設定モードで次のコマンドを使用します。

protection-end-timer {*time-seconds* | **forever**}

表 10-3 に、**protection-end-timer** コマンドの引数とキーワードを示します。

表 10-3　protection-end-timer コマンドの引数とキーワード

パラメータ	説明
time-seconds	タイムアウト（秒単位）。61 以上の整数を入力します。
forever	無限のタイムアウトを設定します。

デフォルトは **forever** です。デフォルト値を変更しない場合は、ゾーン保護を手動で非アクティブにする必要があります。

次の例は、保護の無活動タイムアウトを設定する方法を示しています。

```
user@GUARD-conf-zone-scannet# protection-end-timer 300
```

ゾーン保護のアクティブ化

外部デバイス（Detector など）からコマンドを受信したときにゾーン保護をアクティブにするように Guard モジュールを設定できますが、ゾーンを設定してからも、必要なときにゾーン保護を手動でアクティブにすることができます。Guard モジュールでゾーンのトラフィック特性をラーニングし終わる前にゾーンが攻撃中になった場合は、オンデマンド保護を使用してゾーンを保護します。新しいゾーンに対する Guard モジュールのデフォルトのしきい値を使用すると、効果的なオンデマンド保護を実行できます。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。

（注）　**activation-interface packet** コマンドによりアクティベーション範囲を **packet** に設定している場合は、外部デバイスを使用して、ゾーンのトラフィックを手動で Guard モジュールに宛先変更する必要があります。この設定を行わないと、Guard モジュールはゾーンのトラフィックを監視できません（P.10-8 の「保護アクティベーション範囲の設定」を参照）。

ゾーン保護をアクティブにした後、Guard モジュールがゾーンのトラフィックを受信していることを確認できます。それには、ゾーン保護をアクティブにしてから少なくとも 10 秒待ってから、**show rates** コマンドを入力します。レートのうち少なくとも 1 つの値がゼロより大きいことを確認します。すべてのレートの値がゼロの場合は、宛先変更に問題があることを示しています。詳細については、P.15-2 の「トラフィックの宛先変更問題の認識」を参照してください。

ゾーン保護は、次の項で説明するように、ゾーン全体またはゾーンの一部だけに対してアクティブにすることができます。

- ゾーン全体の保護
- ゾーンのアドレス範囲の部分である IP ゾーンの保護
- ゾーン名が未知の場合の IP アドレスの保護

ゾーン全体の保護

ゾーン設定モードで次のコマンドを入力することにより、ゾーン全体を保護できます。

protect [**learning**]

オプションの **learning** キーワードは、保護およびラーニング機能（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」を参照）によって、Guard モジュールがゾーンを保護してポリシーのしきい値を調整できるようにします。

次の例は、ゾーン保護をアクティブにする方法を示しています。

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

ゾーンのアドレス範囲の部分である IP ゾーンの保護

ゾーンのアドレス範囲の一部である、IP が特定されたゾーンを保護できます。この場合、Guard モジュールは新しいゾーンを作成します。新しいゾーンの名前は、元になるゾーンの最初の 30 文字と、アンダースコアで連結された特定の IP アドレスで構成されます。同じ名前のゾーンがすでに存在する場合、Guard モジュールは同じ名前の別のゾーンを作成せず、既存のゾーンに対するゾーン保護をアクティブにします。

IP が特定されたゾーンについてゾーン保護をアクティブにするには、グローバル モードで次のコマンドを使用します。

protect *zone-name ip-address-general*

表 10-4 に、**protect** コマンドの引数を示します。

表 10-4　ゾーン設定モードの protect コマンドの引数

パラメータ	説明
zone-name	ゾーンの名前。
ip-address-general	ゾーン アドレス範囲内の特定の 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、192.168.5.6 を入力します。

このゾーンを削除するには、**zone** コマンドの **no** 形式を使用します。

次の例は、ゾーン scannet の IP アドレス範囲に含まれている IP アドレス 192.168.5.6 のゾーン保護をアクティブにする方法を示しています。

```
user@GUARD# protect scannet 192.168.5.6
creating zone scannet_192.168.5.6
user@GUARD#
```

ゾーン名が未知の場合の IP アドレスの保護

グローバル モードで次のコマンドを入力することにより、ゾーンの名前がわからない場合でも、ゾーンの IP アドレス範囲に含まれる特定の IP アドレスを保護できます。

protect *ip-address-general* [*subnet-mask*]

表 10-5 に、**protect** コマンドの引数を示します。

表 10-5　グローバル モードの protect コマンドの引数

パラメータ	説明
ip-address-general	ゾーンのアドレス範囲内の特定の 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、192.168.5.6 を入力します。
subnet-mask	（オプション）ゾーン保護をアクティブにするサブネット マスク。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、255.255.255.252 と入力します。

Guard モジュールは、IP アドレス アクティベーション方式に基づいて、その IP アドレスを含む IP アドレス範囲を持つゾーンに対するゾーン保護をアクティブにします。詳細については、P.10-8 の「保護アクティベーション範囲の設定」を参照してください。

次の例は、IP アドレス 192.168.5.6 のゾーン保護をアクティブにする方法を示しています。

```
user@GUARD# protect 192.168.5.6
```

（注）　複数のゾーンに対して同時に **protect** 関連のコマンドを入力できます。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入力します。たとえば、すべてのゾーンについてゾーン保護をアクティブにする場合は、グローバル モードで **protect *** コマンドを入力します。名前が *scan* で始まるゾーン（scannet や scanserver など）すべてについてゾーン保護をアクティブにする場合は、グローバル モードで **protect** *scan** コマンドを入力します。

ゾーン保護の非アクティブ化

ゾーンに対する攻撃がなく、ゾーンのトラフィック異常の検出を他のソースに依存しているときは、ゾーン保護を非アクティブにして、Guard モジュールへのトラフィックの宛先変更を終了することができます。

ゾーン保護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使用します。

- **no　protect**：ゾーン保護を終了します。保護およびラーニング機能をイネーブルにした状態で **no protect** コマンドを入力すると、Guard モジュールはポリシーのしきい値のラーニングを継続します。

（注）　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入力することにより、複数のゾーンに対して同時に **protect** 関連のコマンドを入力できます。たとえば、すべてのゾーンについてゾーン保護を停止する場合は、グローバル モードで **no protect *** コマンドを入力します。名前が *scan* で始まるゾーン（scannet や scanserver など）すべてについてゾーン保護を停止する場合は、グローバル モードで **no protect** *scan**** コマンドを入力します。

- **deactivate**：ゾーン保護と、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。

次の例は、ゾーン保護およびラーニング プロセスを非アクティブにする方法を示しています。

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