CHAPTER 5

ゾーンの設定

この章では、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、Guard を設定してゾーンを保護するために必要です。

この章には、次の主要な項があります。

概要

ゾーンの設定処理には、次の手順があります。

ステップ 1　基本的なゾーン設定：基本設定には、ゾーンの作成のほか、ゾーンの名前と説明、ゾーンのネットワーク アドレスと動作の定義、およびゾーンの帯域幅をはじめとする基本的なネットワーク特性の設定があります。詳細については、P.5-4 の「基本的なゾーン設定」を参照してください。

ステップ 2　宛先変更の設定：ターゲット ホスト（ゾーン）を保護するには、そのホストへのトラフィックが宛先変更され、Guard に送られる必要があります。宛先変更は、Guard のルーティング設定を通じてグローバルに設定されます。グローバルな宛先変更の設定が新しいゾーンの設定に対応していることを確認する必要があります。この手順には、トラフィックの転送方式の設定も含まれます。詳細については、付録 A「宛先変更の設定」を参照してください。

ステップ 3　ゾーンのトラフィックのラーニングとポリシーの調整：保護ポリシーを作成します。ポリシーは、特定のトラフィック フローを測定し、しきい値超過の結果としてそのフローに対してアクションを実行するメカニズムです。Guard では、テンプレートを使用して、2 つのフェーズのゾーン トラフィック ラーニング プロセスの中で保護ポリシーを作成します。また、オンデマンドの保護を使用することもできます。詳細については、P.5-11 の「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。

ステップ 4　Guard のフィルタの設定：さまざまなゾーン フィルタを設定します。フィルタは、宛先変更されたトラフィックを必要な保護モジュールに誘導するメカニズムです。ユーザは、フィルタを設定して、カスタマイズされたトラフィック誘導や DDoS 攻撃の防止メカニズムをさまざまに設計することができます。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。

ステップ 5　ゾーンの保護：ゾーンのトラフィックの特性をラーニングすると、Guard はゾーンの保護を開始できる状態になります。外部（Detector やその他の手段）から攻撃の兆候が示されてから Guard を設定してゾーンを保護することも、ゾーンの設定後すぐにゾーンを保護するように Guard に指示することもできます。ゾーンの保護プロセスの間、Guard はゾーンのトラフィックの宛先を変更し、保護ポリシーを適用します。詳細については、P.5-17 の「ゾーンの保護」を参照してください。

基本的なゾーン設定

新しいゾーンを作成するときには、システム定義のテンプレートに基づいてゾーンを作成するか、既存のゾーンをテンプレートとして使用することができます。テンプレートには、ゾーンの初期設定が定義されています。この設定は、オンデマンドの保護（ラーニングが実行されていないゾーンの保護）に使用されます。詳細については、P.5-20 の「オンデマンド保護」を参照してください。

新しいゾーンを作成し、その基本特性を設定するには、次の手順を実行します。

ステップ 1　システム定義のテンプレートに基づいて新しいゾーンを作成します。P.5-7 の「ゾーンの作成」を参照してください。

または

既存のゾーンに基づいてゾーンを作成します。P.5-10 の「ゾーンの複製」を参照してください。

（注）　既存のゾーンの設定を変更するには、ゾーン設定モードに入ります。**zone** *zone-name* コマンドを使用してください。

ステップ 2　ゾーンの IP アドレスを定義します。Guard でトラフィックのラーニングと保護を可能にするには、この定義が必要です。

最初に定義する場合、ゾーンの IP アドレスは、ゾーンが 保護モードでないときに挿入する必要があります。ただし、ゾーンのサブネットや追加の IP アドレスは、ゾーンが保護モードでも追加できます。

IP アドレスを追加するには、次のコマンドを複数回入力します。各ゾーンに 100 個まで IP エントリ（特定の IP アドレスまたはサブネット）を追加できます。

次のように入力します。

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

表 5-1 に、**ip address** コマンドの引数を示します。

表 5-1　ip address コマンドの引数

パラメータ	説明
ip-addr	ゾーンの IP アドレス。ゾーンは、サブネットでもかまいません。
ip-mask	（オプション）IP マスク。デフォルトのサブネット マスクは、255.255.255.255 です。

ステップ 3　ゾーンが処理できるトラフィックの量に応じて、ゾーンに通すことのできる帯域幅を定義します（オプション）。

（注）　この帯域幅の値には、該当のゾーンへ流入する測定された最大の帯域幅を設定することを推奨します。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。

次のように入力します。

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

表 5-2 に、**rate limit** コマンドの引数を示します。

表 5-2　rate limit コマンドの引数

パラメータ	説明
no-limit	ゾーンは、無制限のレート リミットで定義されます。
rate	ゾーンに通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* パラメータで指定されます。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 5-2　rate limit コマンドの引数（続き）

パラメータ	説明
burst	ゾーンに通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* パラメータ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。バースト リミットは、最大でレート リミットの 8 倍まで指定可能です。
units	レートの単位。次の単位があります。 • **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）識別の目的で、ゾーンの説明を追加します。次のように入力します。

description *string*

文字列の長さは最大 80 文字です。

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。

次の例を参考にしてください。

```
admin@GUARD-conf-zone-scannet# ip address 192.168.100.34
255.255.255.252
admin@GUARD-conf-zone-scannet# rate-limit 1000 2300 pps
admin@GUARD-conf-zone-scannet# description This zone is used for
demonstration purposes
```

（注）　新しく設定されたゾーンの設定ファイルを表示するには、ゾーンのプロンプトで **show running-config** コマンドを使用します。

ゾーンの作成

システム定義のテンプレートに基づいてゾーンを作成するには、次のように入力します。

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

このコマンドを実行すると、Guard は新しいゾーンの設定モードに入ります。既存のゾーンの名前を入力すると、Guard はそのゾーンの設定モードに入ります。

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、最大 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。
template	（オプション）ゾーンの設定を定義するテンプレート。デフォルトでは、Guard の 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。 詳細については、表 5-4 を参照してください。
interactive	新しいゾーンの動作モードをインタラクティブ モードに設定します。このモードでは、ポリシーによって生成される動的フィルタが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 8 章「インタラクティブ推奨モード」を参照してください。

表 5-4 に、Guard のゾーン テンプレートを示します。

表 5-4　Guard のゾーン テンプレート

テンプレート	説明
DEFAULT	Guard のデフォルトのゾーン テンプレート。Guard では、TCP プロキシのスプーフィング防止メカニズムでこのテンプレートを使用します。このメカニズムにより、パケットの送信元 IP アドレスが Guard の TCP プロキシ アドレスに変更されます。このテンプレートは、該当のゾーン ネットワークの着信 IP アドレスに基づく ACL（IP ベースのアクセス リスト）、アクセス ポリシー、またはロード バランシング ポリシーを使用しない場合に使用することができます。
TCP_NO_PROXY	このテンプレートは、TCP プロキシを使用しないゾーン用に設計されています。このテンプレートは、ゾーンが IP アドレスに従って管理される場合（Internet Relay Chat（IRC; インターネット リレー チャット）サーバ タイプのゾーンなど）や、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使用することができます。
帯域幅限定リンク 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テンプレート。このようなゾーンの保護は、攻撃されているサブネットまたは範囲に対して実行されます。このようなゾーンは、protect-ip-state が only-dest-ip となっている Detector で定義することを推奨します。 128K、1M、4M、および 512K の各リンクに対して、それぞれ次の帯域幅限定リンク テンプレートを使用できます。 **LINK_128K** **LINK_1M** **LINK_4M** **LINK_512K** （注）　これらのテンプレートに対しては、ポリシー構築のためのラーニングを実行することはできません。

（注）　ゾーン テンプレートを表示するには、**show templates** コマンドを使用します。テンプレートのデフォルト ポリシーを表示するには、**show templates** *template-name* **policies** コマンドを使用します。

次の例を参考にしてください。

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

ゾーンの複製

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。

ゾーンを複製するには、次のいずれかを実行します。

- 設定プロンプトで次のように入力します。

  zone *new-zone-name* **copy-from** *base-zone-name*

  引数 *base-zone-name* には、新しいゾーンのテンプレートとして使用するゾーンの名前を指定します。

  次の例を参考にしてください。

  ```
  admin@GUARD-conf#zone scanserver copy-from scannet
  admin@GUARD-conf-zone-scanserver#
  ```

または

- 関連するゾーンのプロンプトで次のように入力します。

  zone *new-zone-name* **copy-from-this**

  現在のゾーンから新しいゾーンに設定がコピーされます。

  次の例を参考にしてください。

  ```
  admin@GUARD-conf-zone-scannet# zone mailserver copy-from-this
  admin@GUARD-conf-zone-mailserver#
  ```

引数 *new-zone-name* には、新しいゾーンの名前を指定します。ゾーン名は、最大 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。

このコマンドを実行すると、Guard は新しいゾーンの設定モードに入ります。

ゾーン トラフィックの特性のラーニング

ラーニング フェーズでは、Guard はゾーンのトラフィックの特性をラーニングします。結果は、保護のポリシーに変換されます。これらのポリシーは、Guard の保護システムに対して、ゾーンのトラフィック フローにどのように注意を向けるかを指示します。Guard のラーニング フェーズは、通常のゾーン トラフィックの宛先を変更して Guard に送る、Guard のトラフィック宛先変更メカニズムで始まります。

（注）　ラーニング プロセスを開始する前に、宛先変更を設定する必要があります。Guard のルーティング設定を使用して、ゾーンの宛先変更を設定してください。詳細については、第 4 章「ゾーン トラフィックの宛先変更」を参照してください。

ポリシー テンプレートは、Guard のポリシー構築用ツールです。ポリシー テンプレートは、トラフィックの特性に従って、作成するゾーン ポリシーのタイプを定義します。また、ポリシー テンプレートは、与えられたガイド パラメータに従って、各サービス ポリシーの最大サービス数と最小しきい値も定義します（詳細については、第 7 章「ポリシー テンプレートとポリシーの設定」を参照）。

（注）　ラーニング フェーズが完了する前にゾーンが攻撃され、Guard がまだ保護ポリシーを適用していない場合は、ラーニングを打ち切り、同じ IP アドレスの新しいゾーンを定義して（P.5-7 の「ゾーンの作成」を参照）、新しいゾーンをオンデマンド保護に使用します。詳細については、P.5-20 の「オンデマンド保護」を参照してください。

ラーニング プロセスは、次の 2 つのフェーズで構成され、これらのフェーズで Guard はゾーンのトラフィックをラーニングし、特定の特性に対応します。

1. **ポリシーの構築**：このフェーズでは、Guard はポリシー テンプレートを使用してゾーン ポリシーを作成します。トラフィックが透過的に Guard を通過し、Guard はゾーンによって使用される主なサービスを検出できます。

2. **しきい値の調整**: このフェーズでは、Guard はゾーンのサービスのトラフィック レートに合わせてポリシーを調整します。トラフィックが透過的に Guard を通過し、Guard はゾーン ポリシーの構築中に検出されたサービスのしきい値を調整できます。

（注）　ラーニング プロセスの間、パケットの次のいずれかのフィールドがゼロに等しい場合、Guard はそのパケットをドロップします。

- 送信元 IP アドレス
- プロトコル番号
- UDP 送信元または宛先ポート
- TCP 送信元または宛先ポート

Guard は、ゾーンのトラフィックの特性をラーニングして、ゾーンのトラフィックを比較する基準とし、悪意の攻撃となる可能性のあるあらゆる異常をトレースします。

ポリシーの作成後は、ポリシーを追加または削除したり、しきい値、サービス、タイムアウト、アクションなどのポリシーのパラメータを変更することができます。

ポリシーが実行するアクションは、単なる通知から、Guard のさまざまな保護メカニズムへのトラフィックの誘導や悪意のあるトラフィックのドロップに及びます。

ポリシーの構築

このフェーズでは、Guard はポリシー テンプレートを使用してゾーン ポリシーを作成します。トラフィックが透過的に Guard を通過し、Guard はゾーンによって使用される主なサービスを検出できます。ポリシー構築の指針となるルールを設定することもできます。詳細については、第 7 章「ポリシー テンプレートとポリシーの設定」を参照してください。

（注）　帯域幅限定リンク　テンプレート（LINK_128K、LINK_1M、LINK_4M、および LINK_512K）に基づいたゾーンに対しては、ポリシー構築を実行することはできません。

ゾーン ポリシーを構築するには、次の手順を実行します。

ステップ 1　次のように入力します。

```
learning policy-construction
```

ヒント　Guard がゾーンのトラフィックの宛先変更を実行していることを確認してください。ポリシー構築フェーズを開始してから少なくとも 10 秒待ってから、**show rates details** コマンドを発行します。*Received traffic* レートの値がゼロより大きいことを確認します。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。

ステップ 2　十分な時間が経過してからポリシー構築フェーズを終了し、新しく構築されたポリシーの処理方法を決定します。

（注）　次のフェーズに進む前に、少なくとも 2 時間はポリシー構築フェーズを続けることを推奨します。

詳細については、次の項、「ポリシー構築フェーズの終了」を参照してください。

次の例を参考にしてください。

```
admin@GUARD-conf-zone-scannet# learning policy-construction
```

ワンポイント・アドバイス

複数のゾーンに対して同時にポリシー ラーニング コマンドを発行することができます。これには、グローバル プロンプトで、ワイルドカードにアスタリスク（*）を使用してコマンドを発行します。たとえば、すべてのゾーンについてポリシーの構築を開始する場合は、グローバル プロンプトで **learning policy-construction *** と入力します。*scan* で始まる名前を持つ Guard のすべてのゾーン（scannet や scanserver など）のポリシー構築フェーズの結果を受け入れるには、グローバル プロンプトで **no learning** *scan** **accept** と入力します。

ポリシー構築フェーズの終了

ポリシー構築フェーズを終了するには、3 つの方法があります。

- **提案されたポリシーの受け入れ**：Guard で提案されたポリシーを受け入れるには、関連するゾーンのプロンプトで次のように入力します。

  ```
  no learning accept
  ```

  Guard は、以前にラーニングしたポリシーとしきい値を消去します。

  新しく構築されたポリシーを受け入れた後は、手動でポリシーを追加または削除したり、ポリシーのパラメータを変更することができます。詳細については、第 7 章「ポリシー テンプレートとポリシーの設定」を参照してください。

- **提案されたポリシーの拒否**：Guard で提案されたポリシーを拒否するには、関連するゾーンのプロンプトで次のように入力します。

  ```
  no learning reject
  ```

  この場合、Guard はプロセスを停止し、ラーニングしたすべてのデータを消去します。その結果、Guard はデフォルトの設定に戻る（新しいゾーンの場合）か、このラーニング フェーズの前のゾーンのトラフィック設定に戻ります。

- **提案されたポリシーの表示**：決定の前に、ラーニング プロセスの結果を表示することができます。詳細については、P.7-28 の「スナップショットの作成とポリシーの比較」を参照してください。

次の例を参考にしてください。

```
admin@GUARD-conf-zone-scannet# no learning accept
```

しきい値の調整

この段階では、Guard はゾーンのトラフィックをさらに分析し、前のフェーズで構築したポリシーのしきい値を定義します。Guard は、ポリシーの動作パラメータ（Timeout および Action）のデフォルト値を設定します。動作パラメータの値の設定方法については、第 7 章「ポリシー テンプレートとポリシーの設定」を参照してください。

ポリシーのしきい値を調整するには、次の手順を実行します。

ステップ 1　関連するゾーンのプロンプトで次のように入力します。

```
learning threshold-tuning
```

ステップ 2　十分な時間が経過してから、しきい値調整フェーズを終了し、新しく構築されたポリシーの処理方法を決定します。

（注）　しきい値調整フェーズは、トラフィックのピーク時（最も忙しい日）に、少なくとも 24 時間実行することを推奨します。

詳細については、次の項、「しきい値調整フェーズの終了」を参照してください。

次の例を参考にしてください。

```
admin@GUARD-conf-zone-scannet# learning threshold-tuning
```

ワンポイント・アドバイス

複数のゾーンに対して同時にポリシー　ラーニング　コマンドを発行することができます。これには、グローバル プロンプトで、ワイルドカードにアスタリスク（*）を使用してコマンドを発行します。たとえば、すべてのゾーンについてしきい値の調整を開始する場合は、グローバル プロンプトで **learning threshold-tuning *** と入力します。*scan* で始まる名前を持つ Guard のすべてのゾーン（scannet や scanserver など）のポリシー構築フェーズの結果を受け入れるには、グローバル プロンプトで **no learning** *scan** **accept** と入力します。

ラーニングの結果を表示するには、**show policies statistics** コマンドを使用します。

詳細については、P.7-31 の「ポリシーの表示」を参照してください。

しきい値調整フェーズの終了

しきい値調整フェーズを終了するには、3 つの方法があります。

- **提案されたポリシーの受け入れ**：Guard で提案されたポリシーを受け入れるには、関連するゾーンのプロンプトで次のように入力します。

  ```
  no learning accept
  ```

  Guard は、以前にラーニングしたしきい値を消去します。

  新しく構築されたポリシーを受け入れた後は、手動でポリシーのパラメータを変更することができます。詳細については、第 7 章「ポリシー テンプレートとポリシーの設定」を参照してください。

- **提案されたポリシーの拒否**：Guard　で提案されたしきい値を拒否するには、関連するゾーンのプロンプトで次のように入力します。

  ```
  no learning reject
  ```

  この場合、Guard はしきい値調整フェーズを停止し、ポリシー構築フェーズの結果と以前のしきい値の状態に戻ります。その結果、新しく構築されたポリシーは、オンデマンドの保護用に調整されたしきい値か、過去のトラフィック特性に従って取得されたしきい値を持つ状況になります。

- **提案されたポリシーの表示**：決定の前に、ラーニング　プロセスの結果を表示することができます。詳細については、P.7-28 の「スナップショットの作成とポリシーの比較」を参照してください。

次の例を参考にしてください。

```
admin@GUARD-conf-zone-scannet# no learning accept
```

ゾーンの保護

Guard の保護をアクティブにする前に、Guard でゾーンのトラフィック パターンをラーニングすることを推奨します。ラーニング プロセスにより、Guard で各ゾーンのトラフィック パターンをラーニングし、トラフィックの統計分析に従って推奨のしきい値のセットを作成することができます。

（注）　ラーニング フェーズが完了する前にゾーンが攻撃され、Guard が保護ポリシーを適用していない場合のために、Guard には*オンデマンド*の保護が用意されています。新しいゾーンに対する Guard 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.5-20 の「オンデマンド保護」を参照してください。

Guard の保護は、次の 2 つの動作モードでアクティブにできます。

- **自動保護モード**：動的フィルタはユーザの操作なしでアクティブになります。
- **インタラクティブ保護モード**：動的フィルタは、インタラクティブ　モードにおいて手動でアクティブになります。詳細については、第 8 章「インタラクティブ推奨モード」を参照してください。

外部（Detector やその他の手段）から攻撃の兆候が示されてから Guard を設定してゾーンを保護することも、ゾーンの設定後すぐにゾーンを保護するように Guard に指示することもできます。ゾーンの保護プロセスの間、Guard はゾーンのトラフィックを宛先変更し、保護ポリシーを適用します。

保護の終了は、動的フィルタの無活動タイムアウトに従って定義できます。詳細については、P.5-19 の「保護の終了の定義」を参照してください。

ゾーンの保護では、次のいずれかの方法を選択できます。

- ゾーン全体の保護。

  関連するゾーンのプロンプトで次のように入力します。

  protect

または

- 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の保護。この場合は、新しいゾーンが作成されます。新しいゾーンの名前は、基になるゾーンの最初の 30 文字、下線、および特定の 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 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保護をアクティブにします。

  次のように入力します。

  protect *zone-name ip-addr*

  引数 *zone-name* には、特定のゾーンの名前を指定し、引数 *ip-addr* には、ゾーンのアドレス範囲内の特定の IP アドレスを指定します。

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

次の例を参考にしてください。

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

ヒント　Guard がゾーンのトラフィックの宛先変更を実行していることを確認してください。少なくとも 10 秒待ってから、**show rates** コマンドを発行します。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。

保護の終了の定義

保護の終了は、動的フィルタの無活動タイムアウトに従って定義できます。事前に定義された期間に、使用される動的フィルタがなく、新しい動的フィルタが追加されない場合、Guard はゾーンに対する攻撃が終了したものと見なし、保護を終了します（Guard が動的フィルタを削除するタイミングを決定する方法については、P.6-24 の「動的フィルタの非アクティブ化」を参照してください）。このタイムアウトは、数秒から無限まで定義できます。

次のように入力します。

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

表 5-5 に、protection-end-timer コマンドの引数とキーワードを示します。

表 5-5　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	保護のタイムアウト（秒単位）を指定する、60 より大きな整数。
forever	無限のタイムアウト。

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

オンデマンド保護

ゾーンが攻撃にさらされている場合など、緊急を要する場合には、ラーニングを実行せずにゾーンを保護することができます。システム定義のゾーン テンプレートには、ラーニング プロセスが完了していないゾーンの保護に適した定義済みの保護ポリシーとユーザ フィルタが含まれています。これらのテンプレートのデフォルトのしきい値は、Guard がゾーンのトラフィックに異常を発見した場合に Guard のスプーフィング防止メカニズムがすぐにアクティブになるように調整されています。

Guard はゾーンのトラフィック パターンについての知識を持たないため、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しきい値は、比較的高い値に設定されています。つまり、オンデマンド保護では、スプーフィングを利用しない攻撃を軽減する場合にはユーザの介入が必要になります。ゾーンの正当なトラフィックと悪意のあるトラフィックのレートを監視して、Guard の軽減アクションを確認する必要があります。

オンデマンド保護を開始するには、次の手順を実行します。

ステップ 1　新しいゾーンを作成します。次のように入力します。

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

詳細については、P.5-7 の「ゾーンの作成」を参照してください。

ステップ 2　保護をアクティブにします。次のように入力します。

protect

詳細については、P.5-17 の「ゾーンの保護」を参照してください。

ステップ 3　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、P.11-2 の「ゾーンのトラフィック パターンの分析」を参照してください。

ゾーンのトラフィックの分析

ゾーンのステータスや、ゾーンの各種レートまたはカウンタの概要を表示することができます。

ゾーンのカウンタの表示

ゾーンのトラフィックの分析には、次のコマンドを使用できます。

- **show rates :** Malicious カウンタと Legitimate カウンタの平均トラフィック レートを表示します。
- **show rates details :** すべての Guard のカウンタの平均トラフィック レートを表示します。
- **show rates history :** Malicious カウンタおよび Legitimate カウンタの平均トラフィック レートを、過去 24 時間にわたり 1 分ごとに表示します。
- **show counters**：Guard の Malicious カウンタと Legitimate カウンタを表示します。
- **show counters details**：すべての Guard のカウンタを表示します。
- **show counters history**：過去の Malicious カウンタおよび Legitimate カウンタの値を 1 分ごとに表示します。

レートの単位は、ビット / 秒（bps）およびパケット / 秒（pps）です。

（注）　ゾーンのレートは、ゾーンがラーニング中または保護モードの場合にのみ使用可能です。

Guard は、トラフィックの合計を測定し、平均のトラフィック レートを計算します。値が **cleared** のレートは、ゾーンが保護されていなかった時間を示します。

カウンタの単位はパケットおよびキロビットです。カウンタは、保護の開始時にゼロにリセットされます。

表 5-6 に、Guard のカウンタを示します。

表 5-6　Guard のカウンタ

カウンタ	説明
Malicious	ゾーンを宛先とする悪意のあるトラフィック。悪意のあるトラフィックは、ドロップされたパケットとスプーフィングされたパケット（ゾンビ パケットも含む）の合計です。
Legitimate	Guard によってゾーンに転送された正当なトラフィック。
Received	Guard が受信し、処理したパケット。受信されたパケットは、正当なトラフィックと悪意のあるトラフィックの合計です。
Forwarded	Guard によってゾーンに転送された正当なトラフィック。
Dropped	Guard によって攻撃の一部であると判断され、ドロップされたパケット。
Replied	スプーフィング防止およびゾンビ防止メカニズムの一部として、信頼できるトラフィックと悪意のあるトラフィックのどちらに属するかを確認するために開始クライアントに対して応答が送信されたパケット。
Spoofed	Guard によってスプーフィングされたパケットと判断され、ゾーンに転送されなかったパケット。スプーフィングされたパケットは、応答が送信されたパケット（詳細については上の「Replied カウンタ」を参照）のうち、それに対する応答が受信されなかったものです。スプーフィングされたパケットのカウンタには、ゾンビ パケットも含まれます。
Invalid zone	Guard で保護されたどのゾーンも宛先としない、宛先変更されたトラフィック。

次の例を参考にしてください。

```
admin@GUARD-conf-zone-scannet# show rates
```

ゾーンのステータスの表示

特定のゾーンの概要を表示して、そのゾーンの全般的な状況と現在のステータスを知ることができます。ゾーンの概要を表示するには、**show** コマンドを使用します。概要には、次の情報が含まれます。

- **ゾーンのステータス**：ゾーンが現在保護されているか、ラーニング　フェーズのいずれかにあるか、または非アクティブであるかを示します。
- **ゾーンの基本設定**：動作モード（自動またはインタラクティブ）、しきい値とタイマー、IP アドレスなど、ゾーンの基本的な設定を示します。詳細については、P.5-4 の「基本的なゾーン設定」を参照してください。
- **ゾーンのフィルタ**：フレックス　フィルタの設定も含めて、動的フィルタおよびユーザ フィルタの設定数を示します。ゾーンがインタラクティブ モードの場合、概要には推奨事項の数が表示されます。詳細については、P.6-7 の「フレックス フィルタの設定」および P.6-14 の「ユーザ フィルタの設定」を参照してください。
- **ゾーンのトラフィック　レート**：ゾーンの正当なトラフィックと悪意あるトラフィックのレートを表示します。詳細については、P.5-21 の「ゾーンのカウンタの表示」を参照してください。

次の例を参考にしてください。

```
admin@GUARD-conf-zone-scannet# show
```