ゾーンの作成と設定

この章では、Cisco Traffic Anomaly Detector Module（Detector モジュール）のゾーンを作成し、管理する方法について説明します。

この章は、次の項で構成されています。

ゾーンの概要

ゾーンは、Detector モジュールが Distributed Denial of Service（DDoS: 分散型サービス拒絶）攻撃の監視の対象とするネットワーク要素です。ゾーンは、次の要素の組み合せのいずれかです。

- ネットワーク サーバ、ネットワーク クライアント、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）

DDoS 攻撃を感知すると、Detector モジュールでは、Cisco Anomaly Guard Module（Guard モジュール）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、ユーザに対して Guard モジュールを手動で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い限り、複数のゾーンのトラフィックを同時に分析できます。

ゾーンには名前を付け、ゾーンを指すときはその名前を使用します。

ゾーンの設定には、次のアトリビュートが含まれます。

- ゾーンの説明：ゾーンの名前と説明を定義します。
- ゾーンのネットワーク定義：ゾーンのネットワーク IP アドレスとサブネット マスクを含んだ、ゾーンのネットワーク アトリビュートを定義します。
- ポリシー　テンプレート：ユーザがラーニング　プロセスを実行するときに Detector モジュールが作成するポリシーのタイプを定義します。
- ポリシー：ゾーンのトラフィックを分析し、Detector モジュールがゾーン トラフィックで異常を感知したときにアクションを実行します。ゾーン ポリシーは、ゾーン テンプレートから作成されたデフォルトのポリシー、または Detector モジュールがラーニング プロセス中に作成したゾーン固有のポリシーのいずれかです。
- ゾーン フィルタ：必要な保護レベルにゾーンのトラフィックを誘導し、Detector モジュールによる特定のトラフィック フローの処理方法を定義します。

次の方法により、ゾーンを作成することができます。

- 定義済みのゾーン　テンプレートを使用する：システムで定義されたゾーン テンプレートから新しいゾーンを作成できます。この方法は、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。デフォルトのポリシーを持つゾーンは、オンデマンドの保護で使用できます。

  新しいゾーンを作成後、ゾーン アトリビュートを設定する必要があります。
- 既存のゾーンをテンプレートとして使用する：既存のゾーンからゾーンを作成できます。この方法は、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。

Guard ゾーンの設定

Guard ゾーン テンプレートを使用して、Cisco Anomaly Guard Module （Guard モジュール）をゾーン設定と同期させて、ゾーンを作成できます。ゾーンは Guard ゾーン テンプレートから作成され、2 つの定義セットがあります。1 つは Detector モジュール 用で、もう 1 つは Guard モジュール用です。ゾーン設定には、Guard モジュールにだけ影響する追加のパラメータが含まれています。

この項は、次の内容で構成されています。

Guard ゾーンの設定の表示

ゾーン設定の 2 つの定義セットである Detector モジュール用の定義と Guard モジュール用の定義は、どちらも表示できます。画面の最上部に表示されるトグル フィルタを使用して、2 つの定義セットの表示を切り替えることができます。

Detector モジュールのゾーン設定を表示するには、**View Guard** をクリックします。トグル ボタンにより **View Detector** が表示され、Detector モジュールの設定が表示されていることを示します。

Guard モジュールのゾーン設定を表示するには、**View Detector** をクリックします。トグル ボタンにより **View Guard** が表示され、Guard モジュールの設定が表示されていることを示します。

保護特性の設定

Guard モジュールによるゾーン保護のアクティブ化の方法を定義できます。設定でアクティブにしたゾーン保護を有効にするには、事前にゾーン設定と Guard モジュールとを同期化する必要があります。次の保護特性を定義できます。

- 動作モード：Guard モジュールのゾーン保護の方法を設定したり、Guard モジュールが自動またはインタラクティブのどちらでゾーンを保護するかを決定する基準を定義したりできます。

- 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、または受信したトラフィックに基づいてゾーンをアクティブにするかどうかを定義できます。Detector モジュールのゾーン保護が Guard モジュールをアクティブにする場合は、アクティベーション方式を定義する必要があります。詳細については、「保護のアクティベーション方式」を参照してください。
- アクティベーション範囲：ゾーン全体のアドレス範囲またはゾーン内の特定の IP アドレスに対してゾーン保護をアクティブにするかどうかを定義できます。Detector モジュールのゾーン保護が Guard モジュールをアクティブにする場合は、アクティベーション方式を定義する必要があります。アクティベーション範囲は、Detector モジュールなどの外部デバイスに限りゾーン保護がアクティブ化されるゾーンに適用されます。詳細については、「ゾーンの保護の範囲」の項を参照してください。
- 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タイムアウトを定義できます。

保護のアクティベーション方式

保護のアクティベーション方式により、外部からの攻撃の兆候を受信した場合に、Guard モジュールがゾーン保護をアクティブにするゾーンを特定する方法が決まります。この兆候には、外部デバイス（Detector モジュールなど）からのコマンドや、ゾーンを宛先とするトラフィック（パケット）があります。

Guard モジュールは、保護をアクティブにする方法として、次のものを使用できます。

- 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 モジュール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：ゾーンが宛先となっているトラフィックを受信した場合に、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 モジュール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。
- 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。

パケットまたは IP アドレスの保護アクティベーション方式を指定してゾーンを設定する場合、次のようになります。

- 外部デバイスを使用して手動でゾーン トラフィックを Guard モジュールに宛先変更する必要があります。宛先を変更しないと、ゾーン トラフィックを Guard モジュールで監視できません。
- CLI コマンドの **protect-packet activation-sensitivity** コマンドを使用して、Guard モジュールがゾーン保護のアクティブ化に必要な最小受信トラフィック レートを設定できます。Guard モジュール CLI を使用したアクティベーションの詳細度に限り設定できます。

  詳細については、『*Cisco Traffic Anomaly Detector Module Configuration Guide*』を参照してください。
- 同じ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、ゾーン保護が正常に機能しない場合があります。

ゾーンの保護の範囲

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どうかを定義します。この兆候には、外部デバイス（Detector モジュールなど）からのコマンドや、ゾーンを宛先とするトラフィック（パケット）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をサポートします。

- ゾーン全体 : ゾーン全体の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、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のみ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 モジュールなどの外部デバイスから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がデフォルトです。

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できます。

新しいゾーンを作成する場合は、既存のゾーンをテンプレートとして使用するか、またはシステムで定義されたゾーン テンプレートからゾーンを作成できます。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。

新しいゾーンは、次の 2 つの方法で作成できます。

- 新しいゾーンの作成：システムで定義されたゾーン　テンプレートから新しいゾーンを作成します。この方法は、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後、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。この方法は、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。

ゾーンの設定内容を変更する方法については、「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 テンプレートからのゾーンの作成

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には、次の手順を実行します。

ステップ 1　ナビゲーション ペインの **Detector Summary** をクリックします。Detector の要約メニューが表示されます。

ステップ 2　Detector のメイン メニューの **Zones > Create Zone** を選択します。Zone Form が表示されます。

Zone Form を表示するには、**Zones > Zone list** を選択後 **Add** をクリックするか、ゾーンのメイン メニューから **Main > Create Zone** を選択します。

ステップ 3　ゾーンを定義します。表 4-1 に、Zone Form のフィールドの説明を示します。

表 4-1　Zone Configuration Form のフィールド

フィールド	説明
Name	新しいゾーンの名前。1 ～ 63 文字の英数字文字列の名前にします。文字列は英数字で始まる必要があります。アンダースコアを含むことはできますが、スペースを含むことはできません。
Description	ゾーンについて説明するテキスト。1 ～ 80 文字の英数字文字列を入力します。
Operation mode	Detector モジュールのゾーンの保護方法を定義します。動作モードは次のいずれかです。 • **Automatic**：Detector モジュールは、攻撃の進行中に作成する動的フィルタのすべてを自動的にアクティブにします。 • **Interactive :** Detector モジュールはポリシーで作成される動的フィルタを推奨事項として表示します。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。 ゾーンの動作モードの詳細については、第 9 章「異常の検出のアクティブ化」の「Detector モジュールが実行するゾーンの異常検出方法の設定」の項を参照してください。
Zone Template	ゾーンの設定で使用されるポリシーを定義するゾーン テンプレート。Detector モジュールには、次のプレフィクスを持つ 2 セットのゾーン テンプレートがあります。 • DETECTOR_ : Detector モジュールでのみ使用するために設計されたゾーン テンプレート。Guard モジュールとゾーン設定を共有させない場合は、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 モジュールで使用するため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で作成された、Detector モジュールと Guard モジュールの両方のゾーンのアトリビュートを設定できます。このゾーン設定は Guard モジュールにコピーできます。Guard モジュール とゾーン設定を同期させる予定の場合は、GUARD_ バージョンのゾーン テンプレートを選択します。

表 4-1　Zone Configuration Form のフィールド（続き）

フィールド	説明
Zone Template（続き）	次のいずれかのゾーン テンプレートを選択します。 • **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する場合、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 ワーム攻撃を検出できるようにするためのゾーン テンプレート。GUARD_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。 • **DETECTOR_LINK** テンプレート：ゾーンが既知の帯域幅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 プロセスを実行することなく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、攻撃を受けた IP アドレスまたはサブネットだけを対象に 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** パラメータを **Only Dst IP** に設定します。詳細については、この表の **Protect-IP State** パラメータの説明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。 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。

表 4-1　Zone Configuration Form のフィールド（続き）

フィールド	説明
Zone Template（続き）	• **GUARD_DEFAULT**：Guard モジュールの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。このゾーン 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、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。 • **GUARD_LINK** テンプレート：既知の帯域幅の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 の各リンク用に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は、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することなくゾーン検出をアクティブにすることができます。 Detector モジュールが攻撃を受けた IP アドレスまたはサブネットだけに対する 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** パラメータを **Only Dst IP** に設定します。詳細については、この表の **Protect-IP State** パラメータの説明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。IRC[2] サーバタイプのゾーンなど、ゾーンが IP アドレスに基づいて制御されている場合や、ゾーン上で実行されているサービスのタイプが不明な場合、このゾーン テンプレートを使用できます。
Protect-IP state	Detector モジュールがリモート Cisco Anomaly Guard Module をアクティブにするのに使用する Guard の保護方式。ここで選択する Guard の保護方式により、Cisco Anomaly Guard Module が特定のゾーン保護の要件に集中するようにして、Cisco Anomaly Guard Module のリソースを節約できます。

表 4-1　Zone Configuration Form のフィールド（続き）

フィールド	説明
Protect-IP state（続き）	状態を Protect-IP state ドロップダウン リストから選択します。 • **Entire Zone :** ゾーン トラフィックの異常を検出すると、Guard モジュールをアクティブにして、ゾーン全体を保護します。この方法を使用すると、Guard モジュールが保護するアクティブなゾーンの数が減るため、Guard モジュールのリソースは節約されます。ゾーンが関連したサブゾーンで構成されている場合に、この方法をお勧めします。 • **Only Dst IP**：特定の IP アドレスを宛先とするゾーン トラフィックの異常を検出すると、Guard モジュールをアクティブにして、その IP アドレスを保護します。Guard モジュールをアクティブにして攻撃の対象となる IP アドレスを保護できる一方で、ゾーン全体のトラフィックを Guard モジュールに宛先変更することを回避できます。Detector モジュールは、トラフィックの異常を特定の IP アドレスと関連付けることができない場合、ゾーンを保護するために Guard モジュールをアクティブにしません。ゾーンが関連性のないサブゾーンで構成されている場合に、この方法をお勧めします。 • **Policy type :** Guard モジュールをアクティブにしてゾーン全体を保護、またはゾーンのアドレス範囲にある特定の IP アドレスを保護します。これは、Detector モジュールが Guard モジュールをアクティブにする要因となったポリシーに基づいて実行されます。Detector モジュールは、特定の IP アドレスを宛先とするゾーン トラフィックの異常を検出すると、Guard モジュールをアクティブにしてその IP アドレスを保護します（たとえば、リモート アクティベーションの要因となったポリシーのトラフィック特性が dst_ip である場合）。Detector モジュールは、トラフィックの異常を特定の IP アドレスと関連付けることができない場合、ゾーン全体を保護するために Guard モジュールをアクティブにします（たとえば、リモート アクティベーションの要因となったポリシーのトラフィック特性が global である場合）。 ゾーンが関連したサブゾーンで構成されている場合に、この方法をお勧めします。この方法によって、攻撃対象となったゾーンがゾーン全体に損害を与える事態を避けることができます。

表 4-1　Zone Configuration Form のフィールド（続き）

フィールド	説明
Protect-IP state（続き）	• **Only Dst IP by address**：特定の IP アドレスを宛先とするゾーン トラフィックの異常を検出すると、Guard モジュールをアクティブにして、その IP アドレスを保護します。この IP アドレスは、Guard モジュールに定義されているいずれかのゾーンのアドレス範囲に存在する必要があります。ただし、Detector モジュールのゾーン名が Guard モジュールのゾーン名と同じである必要はありません。protect-IP state の Only Dst IP by address は、Guard モジュールのメイン メニューの **Main > Protect IP** を選択して実行できる、ゾーン名が不明な場合の IP アドレスの保護と同じ設定です。Detector モジュールのゾーン名が Guard モジュールのゾーン名と異なる場合、またはゾーンが関連性のないサブゾーンで構成されている場合には、この方法を推奨します。 Guard モジュールが、攻撃を受けた IP アドレスだけを対象にゾーン保護をアクティブにすること、およびゾーン全体のトラフィックを自身に宛先変更しないようにするには、Guard モジュールでゾーンのアクティベーション範囲が IP Address only として定義されていることを確認してください。
IP address	ゾーンの IP アドレス。ゾーンを作成後、IP アドレスの変更または別の IP アドレスの追加ができます。詳細については、「ゾーンの IP アドレス範囲の設定」の項を参照してください。
Mask	ゾーンのアドレス マスク。アドレス マスクを Mask ドロップダウン リストから選択します。ゾーンを作成後、アドレス マスクを変更できます。詳細については、「ゾーンの IP アドレス範囲の設定」の項を参照してください。

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

ステップ 4　**OK** をクリックして、新しいゾーンを保存します。ゾーンの全般ビュー画面が表示され、ゾーンの設定情報が示されます。

ゾーンを作成後、ゾーン設定の変更および、Activation のパラメータ、Packet Dump のパラメータなど、追加のゾーン アトリビュートを設定できます。詳細については、「ゾーンのアトリビュートの設定」の項を参照してください。

既存のゾーンからのゾーンの作成

既存のゾーンをテンプレートとして使用して新しいゾーンを作成するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインで、ゾーン テンプレートとして使用するゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Main > Save as** を選択します。Zone Save as 画面が表示されます。

ステップ 3　新しいゾーンの名前を定義します。Name テキスト フィールドに、ゾーン名を 1 ～ 63 文字の英数字文字列で入力します。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。

ステップ 4　**OK** をクリックして新しいゾーンを保存します。ゾーンの全般ビュー画面が表示されます。

ゾーンのアトリビュートの設定

ゾーンを作成後、ゾーンのアトリビュートの設定、または既存のゾーン設定の変更ができます。

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　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Configuration > General** を選択します。ゾーンの全般ビューが表示されます。

ステップ 3　最初のテーブルの下にある **Config** をクリックします。Config Zone 画面が表示されます。Config 画面には次のセクションがあります。

- General Details（このセクションに見出しはありません）
- Packet Dump のパラメータ

Guard ゾーン テンプレートからゾーンを作成する場合、Config 画面には追加のセクションが 2 つあります。

- Attack Detection/Termination のパラメータ
- Activation のパラメータ

ステップ 4　(オプション）ゾーンの General Details を設定します。表 4-2 に、このセクションのフィールドの説明を示します。各フィールドの詳細については、表 4-1 を参照してください。

表 4-2　General Details のパラメータ

フィールド	説明
Description	ゾーンについて説明するテキスト。1 ～ 80 文字の英数字文字列を入力します。
Operation mode	Detector モジュールのゾーン保護方法を定義します。次のいずれかの動作モードがあります。 • **Automatic** : Detector モジュールは作成するすべての動的フィルタを自動的にアクティブにします。 • **Interactive :** Detector モジュールはポリシーで作成される動的フィルタを推奨事項として表示します。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。
Protect-IP state	Detector モジュールがリモート Cisco Anomaly Guard Module をアクティブにするのに使用する Guard の保護方式。ここで選択する Guard の保護方式により、Cisco Anomaly Guard Module が特定のゾーン保護の要件に集中するようにして、Cisco Anomaly Guard Module のリソースを節約できます。

表 4-2　General Details のパラメータ（続き）

フィールド	説明
	Protect-IP state には、次のいずれかを指定できます。 • Entire Zone : ゾーン トラフィックの異常を検出すると、Guard モジュールをアクティブにして、ゾーン全体を保護します。 • Policy type : Guard モジュールをアクティブにしてゾーン全体を保護、またはゾーンのアドレス範囲にある特定の IP アドレスを保護します。これは、Detector モジュールが Guard モジュールをアクティブにする要因となったポリシーに基づいて実行されます。 • dst-ip-name : 特定の IP アドレスを宛先とするゾーン トラフィックの異常を検出すると、Guard モジュールをアクティブにして、その IP アドレスを保護します。 • dst-ip-by-ip : 特定の IP アドレスを宛先とするゾーン トラフィックの異常を検出すると、Guard モジュールをアクティブにして、その IP アドレスを保護します。この IP アドレスは、Guard モジュールに定義されているいずれかのゾーンのアドレス範囲に存在する必要があります。
Max. Rate	Guard モジュールがネットワークに再び注入できるトラフィックの量。最大レートの整数を入力し、ドロップダウン リストから測定単位を選択します。帯域幅の最大値が不明な場合は、Max. Rate フィールドおよび Burst フィールドをブランクのままにして、ドロップダウン リストから無制限の単位（**unlimit**）を選択します。 このフィールドは Guard モジュールの設定にだけ適用され、Detector モジュールには影響しません。

表 4-2　General Details のパラメータ（続き）

フィールド	説明
Burst	Guard モジュールが許可されています。バースト サイズ レートの整数を入力します。最大レート（Max. Rate）の測定単位です。 このフィールドは Guard モジュールの設定にのみ適用され、Detector モジュールには影響しません。

ステップ 5　（オプション）Attack Detection/Termination のパラメータを設定します。表 4-3 に、General Details セクションの説明を示します。これらのパラメータは、Guard モジュールの設定にだけ適用され、Detector モジュールには影響しません。

表 4-3　Attack Detection/Termination のパラメータ

フィールド	説明
Malicious-rate detection threshold	ドロップされるゾーン パケットの最小レート。
Protection-end Timer	ゾーンが攻撃されていない場合の、ゾーン保護を終了するための非アクティブ タイムアウト。1 秒以上の値を入力します。無期限にすることもできます。
Filter-rate termination threshold	このしきい値は、Malicious-rate termination threshold とともに使用して、動的フィルタを非アクティブにできるタイミングを指定します。このしきい値は、パケット / 秒（pps）単位で定義します。
Malicious-rate termination threshold	このしきい値は Filter-rate termination threshold とともに使用して、が動的フィルタを非アクティブにできるタイミングを指定します。このしきい値は、パケット / 秒（pps）単位で定義します。

ステップ 6　Activation のパラメータを設定します。これらのパラメータは、Guard モジュールの設定にだけ適用され、Detector モジュールには影響しません。表 4-4 に、Activation のパラメータのフィールドの説明を示します。

表 4-4　Activation のパラメータ

フィールド	説明
Activation interface	保護のアクティベーション方式。次のアクティベーション方式があります。 • **ゾーン名**：これがデフォルトのアクティベーション方式です。 ゾーン名によるアクティベーション方式を設定するには、両方のチェックボックスをオフにします。 **By packet**：パケットによるアクティベーション方式を設定するには、**By packet** チェックボックスをオンにします。 • **By IP address**： パケットによるアクティベーション方式を設定するには、**By IP address** チェックボックスをオンにします。 • **By IP Address or By Packet**：詳細については、この項の「By IP address」および「By packet」の説明を参照してください。 IP アドレス、またはパケットによるアクティベーション方式を設定するには、**By IP address** チェックボックスと **By packet** チェックボックスの両方をオンにします。 パケットまたは IP アドレスによるに保護アクティベーションを設定している場合は、ゾーンが攻撃を受けたときに、トラフィックの宛先を手動で Guard モジュールに変更する必要があります。 詳細については、「保護のアクティベーション方式」の項を参照してください。

表 4-4　Activation のパラメータ（続き）

フィールド	説明
Activation extent	Guard モジュールが外部からの攻撃の兆候を受信してゾーン保護をアクティブにする場合に、ゾーン全体またはゾーンの一部のどちらに対して Guard モジュールがゾーン保護をアクティブにするかを定義します。アクティベーションの範囲は、次のいずれかです。 • **IP address only**：ゾーン内部の指定した IP アドレスまたはサブネットだけ、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がデフォルトです。 • **Entire zone**：ゾーン全体の保護をアクティブにします。 アクティベーション範囲のオプションの詳細については、「ゾーンの保護の範囲」の項を参照してください。

ステップ 7　（オプション）Packet Dump のパラメータを設定して、自動パケット ダンプ キャプチャをイネーブルにします。パケット ダンプ キャプチャの使用方法の詳細については、第 11 章「ネットワーク トラフィックの監視と攻撃シグニチャの抽出」を参照してください。

表 4-5 に、Packet Dump のパラメータのフィールドの説明を示します。

表 4-5　Packet Dump のパラメータ

フィールド	説明
Auto Packet Dump	次のいずれかのオプションの隣にあるチェックボックスをオンにします。 • On：自動パケット ダンプをイネーブルにする • Off：自動パケット　ダンプをディセーブルにする（デフォルト設定）
Max. disk space	Detector モジュールが自動パケットダンプに使用するディスク スペースの最大容量（MB）を入力します。 このフィールドは Cisco Traffic Anomaly Detector にだけ適用され、Cisco Traffic Anomaly Detector Module には影響しません。

ステップ 8　**OK** をクリックして、ゾーンの設定を保存します。

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、除外しない IP アドレスを少なくとも 1 つ設定する必要がありますが、ゾーンの IP アドレス範囲に対する IP アドレスの追加または削除は、いつでも可能です。

この項は、次の内容で構成されています。

ゾーンの IP アドレス範囲への IP アドレスの追加

大きなサブネットを設定してから、そのサブネットから特定の IP アドレスを除外することで、それらがゾーンの IP アドレス範囲に入らないように設定できます。

ゾーンの設定に IP アドレスを追加するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Configuration > General** を選択します。ゾーンの全般ビューが表示されます。

ステップ 3　2 番目のテーブルの下にある **Add** をクリックします。

Add Zone IP 画面が表示されます。

ステップ 4　次の IP アドレス情報を入力します。

- IP Address：ゾーンの IP アドレス。IP アドレスをドット付き 10 進表記で入力します（たとえば、192.168.100.32）。

- IP Mask：ゾーンの IP アドレス マスク。サブネット マスクをドット付き 10 進表記で入力します（たとえば、255.255.255.224）。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 5　（オプション）ゾーンの IP アドレス範囲から IP アドレスを除外するには、**Exclude** チェックボックスをオンにします。

ステップ 6　**OK** をクリックして、ゾーンの設定を保存します。ゾーンの全般ビュー画面が表示されます。

ステップ 7　ゾーン ポリシーをアップデートします。詳細については、「ゾーン ポリシーのアップデート」の項を参照してください。

ゾーンの IP アドレス範囲からの IP アドレスの削除

ゾーンの IP アドレス範囲から IP アドレスを削除するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインでゾーンを選択します。ゾーンのメイン メニューが表示されます。

ステップ 2　ゾーンのメイン メニューの **Configuration > General** を選択します。ゾーンの全般ビューが表示されます。

ステップ 3　削除する各 IP アドレスの隣にあるチェックボックスをオンにし、**Delete** をクリックします。

ステップ 4　ゾーン ポリシーをアップデートします。詳細については、「ゾーン ポリシーのアップデート」の項を参照してください。

ゾーン ポリシーのアップデート

ゾーンの IP アドレス、またはサブネットを変更する場合は、次のいずれかの作業を実施します。

- 新しい IP アドレス、またはサブネットが、ゾーンのネットワークに定義されていなかった新しいサービスで構成されている場合は、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、次の項を参照してください。
  - 第 7 章「ゾーン トラフィックのラーニング」の「ポリシー構築フェーズの停止」
  - 第 8 章「ゾーンのポリシーの管理」の「サービスの追加」
- ゾーン保護とラーニング プロセスがイネーブルの場合は、ゾーン ポリシーを未調整としてマークします。ゾーンに対する攻撃がある場合は、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。これは、ステータスを変更すると Detector モジュールで攻撃が検出されなくなり、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ためです。詳細については、第 7 章「ゾーン トラフィックのラーニング」の「ゾーンのポリシーに対する調整済みまたは未調整のマーク付け」の項を参照してください。
- ゾーン保護とラーニング　プロセスをイネーブルにしなかった状態で、ゾーン保護とラーニング プロセスをアクティブにする予定もない場合は、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します。詳細については、第 7 章「ゾーン トラフィックのラーニング」の「しきい値調整フェーズの開始」の項を参照してください。

ゾーンの削除

1 つ、またはそれ以上のゾーンを削除するには、次の手順を実行します。

ステップ 1　ナビゲーション ペインで **Detector Summary** をクリックする。Detector の要約メニューが表示されます。

ステップ 2　Detector モジュールのメイン メニューの **Zones > Zone list** を選択します。Zone list 画面が表示されます。

ステップ 3　削除する各ゾーンの隣にあるチェックボックスをオンにし、**Delete** をクリックします。表示されているゾーンをすべて削除するには、ヘッダーの（Zone の隣にある）チェックボックスをオンにし、**Delete** をクリックします。Validation Form が表示されます。

ステップ 4　**OK** をクリックして、ゾーンを削除します。