CHAPTER 4

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。

ここでは、Detector モジュールの付属製品である Cisco Guard（Guard）について説明します。Guard は Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃を検出および軽減するデバイスです。攻撃トラフィックをドロップし、正当なトラフィックをネットワークに再注入することで、トラフィックがゾーンを通過するときにゾーン トラフィックをクリーニングします。Detector モジュールは、ゾーンが攻撃を受けていると判断したときに、Guard の攻撃軽減サービスをアクティブにすることができます。また、Detector モジュールはゾーンの設定を Guard と同期させることもできます。Guard の詳細については、『*Cisco Anomaly Guard Module Configuration Guide*』または『*Cisco Guard 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
- Guard ゾーンの設定
- ゾーンの作成
- ゾーンの IP アドレス範囲の設定
- ゾーン設定の表示と変更
- ゾーンの削除

ゾーンについて

ゾーンは、Detector モジュールによって DDoS 攻撃を監視する対象として定義するネットワーク要素です。ゾーンは、次の要素の任意の組み合せです。

- 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、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、Guard 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、Guard を手動でアクティブにするようユーザ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ければ、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：ラーニング プロセスの実行時に 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：ゾーンのトラフィックを必要な保護レベルに誘導し、Detector 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。

次のいずれかの方法を使用して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：システム定義のゾーン テンプレートのいずれかを使用して新しいゾーンを作成します。システム定義のゾーン テンプレートは、ゾーンにデフォルトのポリシーおよびフィルタのセットを設定します。

  新しいゾーンを作成したら、そのゾーンの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：既存のゾーンをコピーしてゾーンを作成します。新しいゾーンが既存のゾーンと類似のトラフィック パターンを持つ場合は、この方法を使用します。

Guard ゾーンの設定

Guard ゾーン テンプレートを使用して、Guard をゾーン設定と同期させて、ゾーンを作成できます。Guard ゾーン テンプレートを使用して作成されたゾーンには、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 用です。ゾーン設定には、Guard にだけ影響を与え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
- 保護特性について
- 保護のアクティベーション方式について
- ゾーン保護の範囲について

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 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、次のように 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 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。

保護特性について

Guard 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 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 のゾーン保護の方法を設定できます。Guard がゾーン保護の措置を自動的に適用するか、インタラクティブな方法で適用するかを定義できます。インタラクティブな方法では、Guard が適用する保護措置をユーザが決定する必要があります。
- 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のどれに基づいてゾーンをアクティブにするかを定義できます。詳細については、「保護のアクティベーション方式について」の項を参照してください。
- アクティベーション範囲：ゾーンのアドレス範囲全体またはゾーン内の特定の IP アドレスのみのどちらに対してゾーン保護をアクティブにするかを定義できます。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よって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、「ゾーン保護の範囲について」の項を参照してください。
- 保護の終了のタイムアウト：Guard 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について

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、ゾーン保護をアクティブにする対象のゾーンを Guard が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 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。

パケットによる保護アクティベーション方式、あるいはパケットまたは IP アドレスによる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、次の規則が適用されます。

- 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 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 で監視できません。
- CLI で **protect-packet activation-sensitivity** コマンドを使用して、Guard 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。アクティベーションの詳細度は、Guard の CLI を使用してのみ設定できます。

  詳細については、『*Cisco Guard Configuration Guide*』または『*Cisco Anomaly Guard 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。

ゾーン保護の範囲について

アクティベーション範囲は、Guard 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のどちら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 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 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 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 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 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、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。

ゾーンの作成

ゾーンを作成し、ゾーンの名前、説明、ネットワーク アドレス、動作定義、およびネットワーク アドレスを設定することができます。

新しいゾーンは、次の 2 つの方法で作成できます。

- 定義済みのゾーン テンプレートを使用する：定義済みのゾーン テンプレートを使用して新しいゾーンを作成できます。デフォルトのポリシーとフィルタでゾーンを新しく作成するには、この方法を使用します。

（注）　発生率の低いゾンビ攻撃監視用の PPH ポリシーを含むゾーン テンプレートを使用してゾーンを作成する場合、PPH ポリシーはデフォルトでディセーブル状態に設定されます。これは、PPH ポリシーによりゾーンで使用されるメモリの量が増えたり、Guard モジュールのパフォーマンスに影響を与えたりするおそれがあるからです。ゾーンの PPH ポリシーをイネーブルにするには、ポリシーの状態をアクティブに変更する必要があります（第 8 章「ゾーンのポリシーの管理」の「ポリシーのパラメータの変更」の項を参照）。

- 既存のゾーン設定をテンプレートとして使用する：既存のゾーンを複製して新しいゾーンを作成できます。新しいゾーンが既存のゾーンと類似のトラフィック パターンを持つ場合は、この方法を使用します。

ゾーンの設定内容を変更する方法については、「ゾーンの IP アドレス範囲の設定」を参照してください。

この項は、次の内容で構成されています。

- ゾーン テンプレートからのゾーンの作成
- 既存のゾーンからのゾーンの作成

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 メニューで **Zones > Create Zone** を選択します。Zone Definition Form が表示されます。

Zone Definition Form は、**Zones > Zone list** を選択して **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** を選択することによっても表示できます。

ステップ 3　ゾーン設定パラメータの最初のセットを定義します。表 4-1 に、Zone Definition Form の各フィールドの説明を示します。

表 4-1　Zone Definition Form のフィールド

フィールド	説明
Name	新しいゾーンの名前。名前は 1 ～ 63 文字の英数字文字列です。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めることができますが、スペースを含めることはできません。
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。
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、次のプレフィックスを持つ 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のゾーン テンプレート。Guard 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 で使用するためのゾーン テンプレート。これらのテンプレートで作成されたゾーンについて、Detector モジュールと Guard の両方のアトリビュートを設定できます。このゾーン設定は Guard にコピーできます。Guard 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。 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 Voice-over-IP サーバを保護できます。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 : Detector モジュールがゾーンに対する 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。DETECTOR_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を Detector モジュールが検出できるようにするためのゾーン 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。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 Detector モジュールが Guard 上のゾーン保護をアクティブにできるよう設定するには、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、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。 DETECTOR_LINK_128K、DETECTOR_LINK_1M、DETECTOR_LINK_4M、および DETECTOR_LINK_512K これらのテンプレートから作成されたゾーンでは、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（第 7 章「ゾーン トラフィックのラーニング」の「ラーニング プロセスについて」の項を参照）。

表 4-1　Zone Definition Form のフィールド（続き）

フィールド	説明
Zone Template（続き）	• GUARD_DEFAULT：Guard のデフォルトのゾーン テンプレート。Guard は、パケットの送信元 IP アドレスを、Guard の TCP プロキシ IP アドレスに変更することがあります。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 アドレスに基づくアクセス コントロール 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できます。 • GUARD_VOIP：Voice over IP（VoIP）サーバが含まれているゾーン用に設計されたゾーン テンプレート。このサーバは、Session Initiation Protocol（SIP）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 Real-time Transport Protocol/Real-time Control Protocol（RTP/RTCP）を使用して SIP エンドポイント間のボイス データを送信するものです。 GUARD_VOIP ゾーン テンプレートから作成されたゾーンには、VoIP トラフィックを処理するための、sip_udp ポリシー テンプレートから生成された特定のポリシーが含まれています。 • GUARD_LINK　テンプレート：既知の帯域幅のゾーン用のゾーン 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、および 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。 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 Detector モジュールが Guard 上のゾーン保護をアクティブにできるよう設定するには、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、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のゾーン テンプレート。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、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。
Operation mode	Detector モジュールがゾーン保護を実行するモード。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を、すべて自動的にアクティブにします。 • Interactive：Detector モジュールは、ポリシーが推奨事項として作成する動的フィルタを表示します。各動的フィルタをアクティブにするかどうかをユーザが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「自動検出モードまたはインタラクティブ検出モードのアクティブ化」の項を参照してください。
IP address	ゾーンの IP アドレス。ゾーンを作成した後で、IP アドレスの変更や IP アドレスの追加ができます（「ゾーンの IP アドレス範囲の設定」の項を参照）。

表 4-1　Zone Definition Form のフィールド（続き）

フィールド	説明
IP 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。ゾーンを作成した後で、アドレス マスクを変更できます（「ゾーンの IP アドレス範囲の設定」の項を参照）。
IP List	追加の IP アドレス。ゾーンの IP アドレスのリストを作成します。リストはスペース区切りで、ドット付き 10 進表記です（a.b.c.d/x の形式を使用。x はサブネット マスク）。

ステップ 4　**OK** をクリックします。Zone Configuration Form に、ゾーン設定パラメータの 2 つ目のセットが表示されます。このフォームには、前のステップで選択したゾーン テンプレートに関連付けられているデフォルトのパラメータ値が含まれています。

ステップ 5　ゾーン設定パラメータの 2 つ目のセットを定義します。表 4-2 に、Zone Configuration Form の各フィールドの説明を示します。

表 4-2　Zone Configuration Form のフィールド

フィールド	説明
一般的なパラメータ	
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 モジュールがゾーン保護を実行するモード。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を、すべて自動的にアクティブにします。 • Interactive：Detector モジュールは、ポリシーが推奨事項として作成する動的フィルタを表示します。各動的フィルタをアクティブにするかどうかをユーザが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「自動検出モードまたはインタラクティブ検出モードのアクティブ化」の項を参照してください。

表 4-2　Zone Configuration Form のフィールド（続き）

フィールド	説明
Protect-IP state	Detector モジュールがリモート Guard モジュールをアクティブにするために使用する Guard の保護方式。ここで選択する Guard の保護方式により、特定のゾーン保護の要件に Guard を集中させることで、Guard のリソースを節約できます。 Protect-IP state ドロップダウン リストには次の状態があります。 • Entire Zone : ゾーン トラフィックの異常が検出されると、Guard 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 が保護するアクティブなゾーンの数が減るため、Guard のリソースは節約されます。関連性のあるサブゾーンでゾーンが構成されている場合、この方法を使用することをお勧めします。 • 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が検出されると、Guard をアクティブにして、その IP アドレスを保護します。Guard 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 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。 関連性のないサブゾーンでゾーンが構成されている場合、この方法を使用することをお勧めします。 • Policy type : Guard をアクティブにして、ゾーン全体、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 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 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 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）。 関連性のあるサブゾーンでゾーンが構成されている場合、この方法を使用することをお勧めします。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 4-2　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が検出されると、Guard 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 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。Only Dst IP by address を選択することは、Guard のメイン メニューで **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です。Detector モジュールのゾーン名が Guard のゾーン名と異なる場合、または関連性のないサブゾーンでゾーンが構成されている場合、この方法を推奨します。 Guard 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し、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 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。
Rate	（GUARD_ テンプレートのみ）Guard がネットワークに再び注入できるトラフィックの量。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します。帯域幅の最大値が不明な場合は、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。 最大レートの整数を入力し、ドロップダウン リストから次のいずれかの測定単位を選択します。 • unlimit：Guard がネットワークに再び注入するトラフィックのレートを制限しない場合は、このデフォルト設定を使用します。unlimit を選択した場合、最大レート値を入力しないでください。 • mbps：メガビット / 秒 • kbps：キロビット / 秒 • bps：ビット / 秒 • kpp：キロパケット / 秒 • pps：パケット / 秒
Burst	（GUARD_ テンプレートのみ）Guard がゾーンに転送できる最大のトラフィック ピーク。バースト サイズ レートの整数を入力します。単位は、ビット、キロビット、キロパケット、メガビット、およびパケットです。各単位は、レート（Rate）で測定単位に指定したレート単位に対応します。
攻撃検出 / 終了のパラメータ（GUARD_ テンプレートのみ）	
Protection-end Timer	ゾーンに攻撃がない場合に Guard がゾーン保護を終了するために使用する非アクティビティ タイムアウト。Guard は、動的フィルタの非アクティビティとドロップされたトラフィックに基づいて非アクティビティを測定します。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。

表 4-2　Zone Configuration Form のフィールド（続き）

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。レートがこのしきい値より低くなった場合、Guard 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 は、ゾーンに対する攻撃と見なし、攻撃レポートを作成します。 Malicious-rate detection threshold のデフォルトは、10 パケット / 秒（pps）です。
Filter-rate termination threshold	Guard 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するしきい値。Malicious-rate termination threshold とともに使用します。このしきい値は、パケット / 秒（pps）単位で定義します。詳細については、第 9 章「異常の検出のアクティブ化」の「動的フィルタの管理」の項を参照してください。
Filter-rate-pph termination threshold	Guard 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するしきい値。Malicious-rate termination threshold とともに使用します。このしきい値は、パケット / 時間（pph）単位で定義します。詳細については、第 9 章「異常の検出のアクティブ化」の「動的フィルタの管理」の項を参照してください。
Malicious-rate termination threshold	Guard 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するしきい値。Filter-rate termination threshold とともに使用します。このしきい値は、パケット / 秒（pps）単位で定義します。詳細については、第 9 章「異常の検出のアクティブ化」の「動的フィルタの管理」の項を参照してください。

表 4-2　Zone Configuration Form のフィールド（続き）

フィールド	説明
アクティベーションのパラメータ（GUARD_ テンプレートのみ）	
Activation interface	保護のアクティベーション方式。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する対象のゾーンを Guard が特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、ゾーン（パケット）を宛先とするトラフィックがあります。アクティベーション方式は、次のいずれかです。 • Zone name：ゾーン名に基づいてゾーン保護をアクティブにします。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：ゾーンが宛先となっている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 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。受信パケットの IP アドレスを含むアドレス範囲を持つゾーンが複数設定されている場合、Guard 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）パケットによる保護アクティベーション方式をゾーンに設定すると、Guard はアクティブなゾーンを宛先としないトラフィックの処理方法を変更します。これに該当するトラフィックの注入を設定した場合、Guard はそのトラフィックをドロップせずに転送します。 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：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します。Guard 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ゾーンが複数設定されている場合、Guard 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。 IP アドレス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。

表 4-2　Zone Configuration Form のフィールド（続き）

フィールド	説明
Activation interface（続き）	• By IP Address or By Packet：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 アドレスやサブネットで構成される外部デバイス（Detector など）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。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。 （注）保護アクティベーションを By Packet または By IP Address or By Packet に設定した場合は、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 に変更する必要があります。Activation interface のオプションの詳細については、「保護のアクティベーション方式について」の項を参照してください。
Activation extent	Guard 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のどちら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。アクティベーション範囲は、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に対してのみ、保護をアクティブにします。これがデフォルトのアクティベーション範囲設定です。 • Entire zone：ゾーン全体の保護をアクティブにします。 Activation extent のオプションの詳細については、「ゾーン保護の範囲について」の項を参照してください。
パケット ダンプのパラメータ	
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します。 • Off：自動パケット ダンプをディセーブルにします（デフォルト設定）。
Max. disk space	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をメガバイト単位で入力します。 このフィールドは Cisco Guard（アプライアンス）だけに適用され、Cisco Traffic Anomaly Detector Module には影響しません。

ステップ 6　**OK** をクリックして新しいゾーンを保存します。

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、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 メニューで **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める必要があります。アンダースコアを含めることができますが、スペースを含めることはできません。

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 IP アドレス範囲の設定

ゾーンの異常の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
- 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 ポリシーのアップデート

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、その後に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 メニューで **Configuration > General** を選択します。ゾーンの全般ビュー画面が表示されます。

ステップ 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）**Exclude** チェックボックスをオンにして、ゾーンの IP アドレス範囲から IP アドレスを除外します。

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 メニューで **Configuration > General** を選択します。ゾーンの全般ビュー画面が表示されます。

ステップ 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 Detector モジュールがポリシー構築フェーズを実行できるようにするか、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。
  - ポリシー構築フェーズの開始（P.7-4）
  - サービスの追加（P.8-12）
- 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、「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。
- **Detect and Learn** の選択によってゾーンの異常検出とラーニングのプロセスをイネーブルにしていない状態で、この 2 つの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、「しきい値調整フェーズの開始」の項を参照してください。

ゾーン設定の表示と変更

ゾーン設定のパラメータ設定は、いつでも表示して現在の設定を確認したり、必要に応じて変更したりできます。

ゾーン設定の現在のパラメータ設定を表示するには、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 メニューで **Configuration > General** を選択します。General Configuration ビュー画面が表示され、ゾーン設定のパラメータ設定値が表示されます。

表 4-3 に、General Configuration 領域に表示される情報の説明を示します。

表 4-3　General Configuration の情報

項目	説明
ゾーンの基本情報	
Name	ゾーンに割り当てた名前
Description	ゾーンを識別するための説明。
Operation mode	ゾーンに設定された動作モード（自動またはインタラクティブ）。
Zone template	ゾーンの作成に使用されたテンプレート。
Rate	(GUARD_ テンプレートのみ) Guard がネットワークに再び注入できるトラフィックの量。
Burst	(GUARD_ テンプレートのみ) Guard がゾーンに転送できる最大のトラフィック ピーク。
攻撃検出 / 終了のパラメータ（GUARD_ テンプレートのみ）	
Protection-end timer	ゾーンに攻撃がない場合に Guard がゾーン保護を終了するために使用する非アクティビティ タイムアウト。
Malicious-rate detection threshold	ドロップされるゾーン パケットの最小レート。
Filter-rate termination threshold	トラフィック レートをパケット / 秒単位で測定するポリシーによって作成された動的フィルタを Guard が非アクティブにできるタイミングを指定するしきい値（パケット / 秒単位で定義）。Malicious-rate termination threshold とともに使用します。
Filter-rate-pph termination threshold	トラフィック レートをパケット / 時間単位で測定するポリシーによって作成された動的フィルタを Guard が非アクティブにできるタイミングを指定するしきい値（パケット / 時間単位で定義）。Filter-rate termination threshold とともに使用します。
Malicious-rate termination threshold	Guard 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するしきい値。Filter-rate termination threshold とともに使用します。

表 4-3　General Configuration の情報（続き）

項目	説明
アクティベーションのパラメータ（GUARD_ テンプレートのみ）	
Activation interface	保護のアクティベーション方式。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する対象のゾーンを Guard が特定する方法を定義します。
Activation extent	Guard がゾーン保護をアクティブにする対象である外部からの攻撃の兆候を受信した場合に、Guard がゾーン保護の対象とする範囲（ゾーン全体またはゾーンの一部）。
パケット ダンプのパラメータ	
Auto Packet Dump	自動パケット ダンプ キャプチャ機能の状態（オンまたはオフ）。
Max. disk space	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（メガバイト単位）。

表 4-4 に、IP address テーブルに表示される情報の説明を示します。

表 4-4　ゾーンの IP アドレス

項目	説明
IP	ゾーンの IP アドレス。
Mask	ゾーンの IP アドレス マスク。
Type	ゾーンの IP アドレス範囲に含める、または範囲から除外する IP アドレス（regular または excluded）。

ゾーンの設定を変更するには、次の機能ボタンのいずれかを選択します。

- Config : 一般的な設定パラメータを変更します。Zone Configuration Form が表示されます。ゾーン設定関連の編集可能な各フィールドについては、「ゾーン テンプレートからのゾーンの作成」の項の表 4-2 を参照してください。
- Add : ゾーンの設定に IP アドレスを追加します。Zone IP Form が表示されます。IP アドレス関連の編集可能な各フィールドについては、「ゾーンの IP アドレス範囲への IP アドレスの追加」の項を参照してください。
- Delete : ゾーンの設定から IP アドレスを削除します。ゾーンの設定からの IP アドレスの削除については、「ゾーンの IP アドレス範囲からの IP アドレスの削除」の項を参照してください。

ゾーンの削除

1 つまたは複数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** を選択します。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 メニューで **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（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 フォームが表示されます。

ステップ 4　**OK** をクリックしてゾーンを削除します。