CHAPTER 4

ゾーンの作成と設定

この章では、Cisco Guard（Guard）上にゾーンを作成し、管理する方法について説明します。

ここでは、Guard の付属製品である Cisco Traffic Anomaly Detector（Detector）について説明します。Detector は Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃検出デバイスで、ゾーンの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 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 はゾーンの設定を Guard と同期させることもできます。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

ゾーンは、Guard によって DDoS 攻撃から保護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）

Guard 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 Guard 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、Guard がゾーンのトラフィックに異常があることを検出したときにアクションを実行します。ゾーン ポリシーには、ゾーン テンプレートに含まれているデフォルトのポリシーと、ラーニング プロセス中に Guard が作成したゾーン固有のポリシーがあります。
- 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、Guard　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できます。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。デフォルトのポリシーを持つゾーンは、オンデマンド保護に使用できます。

  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：既存のゾーンから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。
- Detector からゾーンの設定をコピーする：Detector とのゾーンの設定の同期をイネーブルにできます。この操作は、CLI を使用し、Detector 側からだけ開始できます。詳細については、『*Guard Configuration Guide*』を参照してください。

ゾーン保護のアクティベーション方式と保護範囲のオプションについて

ゾーンの設定を定義するときに、Guard がゾーン保護を自動的にアクティブにするためのトリガー、つまり、*アクティベーション方式*を定義できます。また、Guard が保護する範囲の大きさも定義できます。たとえば、ゾーン全体や、ゾーンの IP アドレス範囲内の特定の IP アドレスのみを Guard で保護することができます。

この項は、次の内容で構成されています。

保護のアクティベーション方式について

Guard は、ゾーン名に基づいて、または宛先変更されたトラフィックから抽出する情報に基づいて、ゾーン保護をアクティブにできます。

保護をアクティブにする方式として、次のものを使用できます。

- 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。保護がアクティブになるには、外部から示される攻撃の兆候にゾーン名が含まれている必要があります。これが、Guard がゾーン保護のアクティベーションに使用するデフォルトの方式です。
- 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。Guard はゾーンのデータベースをスキャンして、対象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を含むアドレス範囲を持つゾーンが対象です。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）を選択して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。
- パケット：データベース内のゾーンのパケットを受信した場合に、ゾーン保護をアクティブにします。パケットを受信すると、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。
- IP アドレスまたはパケット：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。詳細については、上記のパケットおよび IP アドレスの説明を参照してください。

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 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。

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：ゾーン内部の、指定された IP アドレスまたはサブネットのみ、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、サブゾーンと呼ばれる新しいゾーンを作成します（「サブゾーンについて」の項を参照）。これが、アクティベーション範囲パラメータのデフォルト設定です。

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）に対して保護をアクティブにする場合、Guard 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ています。

サブゾーンの設定は、IP アドレスと名前を除いて、ソース ゾーンの設定と同じです。サブゾーンの名前は、ソース ゾーンの名前の最初の 30 文字、IP アドレス、およびサブネットで構成され、名前、IP アドレス、およびサブネットは、アンダースコアで連結されています。サブゾーンが単一の IP アドレスで構成されている場合には、サブネットは付加されません。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 を持つとき、Guard 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 に対して保護モードをアクティブにする場合、サブゾーンの名前は scannet_10.10.10.192_255.255.255.252 となります。

Guard は、外部からの攻撃の兆候のあるサブゾーンの IP アドレスおよびサブネット、または Guard がゾーンの保護をアクティブにする原因となったパケットの IP アドレスを受信します。

サブゾーンのゾーン保護が終了すると、Guard はサブゾーンを消去しますが、サブゾーンの攻撃レポートは消去しません。Guard は、ソース ゾーンに対して設定されているアクティベーション方式、および保護の終了のタイムアウトに基づいて、サブゾーンのゾーン保護を終了します。

Guard が消去したサブゾーンの攻撃レポートを表示するには、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 メニューの **Diagnostics > Attack Reports > Attack Summary** を選択します。Attacks summary 画面が表示され、サブゾーンの攻撃レポートの要約がサブゾーンのレポート テーブルに表示されます。

ステップ 3　攻撃レポートの詳細を表示するには、サブゾーンのレポート テーブルに表示されている攻撃のいずれかのフィールドをクリックします。

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、定義済みのゾーン テンプレートのいずれかを使用することができます。ゾーン テンプレートは、ゾーンの初期ポリシーおよびフィルタ設定を定義します。

新しいゾーンはデフォルトのポリシーを持ち、これらをオンデマンド保護用に調整できます。ただし、ゾーンの保護が緊急に必要でなければ、Guard でゾーンのトラフィックの特性をラーニングできるようにすることをお勧めします。詳細については、第 9 章「ゾーン保護のアクティブ化」の「オンデマンド保護のアクティブ化」の項を参照してください。または、Detector からゾーンの設定とゾーン ポリシーをコピーすることもできます。

ゾーンは、次の 3 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。
- Detector からゾーンの設定をコピーする：Detector とのゾーンの設定の同期をイネーブルにします。

  この操作は、CLI を使用し、Detector 側からだけ開始できます。詳細については、『*Cisco Traffic Anomaly Detector Configuration Guide*』または『*Cisco Traffic Anomaly Detector Module Configuration Guide*』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

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 **Guard Summary** をクリックします。Guard の要約メニューが表示されます。

ステップ 2　Guard のメイン メニューの **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 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。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	ゾーンの設定でポリシーを定義するゾーン テンプレート。Template ドロップダウン リストから、次のいずれかのオプションを選択します。 • GUARD_DEFAULT：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します。 • GUARD_TCP_NO_PROXY：TCP　プロキシを使用しないゾーン用のテンプレート。このテンプレートは、インターネット リレー チャット サーバ タイプ 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に使用します。 • 帯域幅限定リンクテンプレート：既知の帯域幅を持つ複数のゾーンに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のゾーン テンプレート。ゾーン保護が必要な場所により的確に集中し、Guard のリソースを節約するために、攻撃対象のアドレス範囲に対応するゾーンに対してのみゾーン保護をアクティブにする必要があります。リソースを定義するときに、protect-ip state を **only-dest-ip** にしてゾーンを定義することをお勧めします。128 Kbps、1 Mbps、4 Mbps、および 512 Kbps 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。しきい値調整フェーズは実行できます（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 Configuration Form のフィールド（続き）

フィールド	説明
Zone Template （続き）	（注）　これらのゾーンについては、ステップ 4 で activation-extent パラメータを **IP address only** に設定して、攻撃されているサブネットまたは範囲に基づいてゾーン保護をアクティブにすることをお勧めします。 • 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。
Operation mode	Guard 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：Guard 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：Guard 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「ゾーン保護のアクティブ化」の「自動保護モードまたはインタラクティブ保護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）。
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	Guard 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：Guard 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：Guard 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「ゾーン保護のアクティブ化」の「自動保護モードまたはインタラクティブ保護モードのアクティブ化」の項を参照してください。
Rate	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 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	
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。
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。

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

フィールド	説明
Filter-rate termination threshold	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。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「ゾーン保護のアクティブ化」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	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。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「ゾーン保護のアクティブ化」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	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。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「ゾーン保護のアクティブ化」の「動的フィルタの管理」の項を参照してください。
アクティベーションのパラメータ	
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ときに、ゾーン保護をアクティブにするゾーンを Guard がどのように識別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、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。

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：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。 • 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 Guard 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

ゾーン保護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。Zone IP Form 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 メニューの **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。
  - ポリシー構築フェーズの開始（P.7-4）
  - サービスの追加（P.8-13）
- ゾーンが攻撃を受けていない状態で、**Protect and Learn** を選択してゾーン保護とラーニングのプロセスをイネーブルにしている場合は、ゾーン ポリシーを未調整としてマークします。ゾーンが攻撃を受けているときにゾーン ポリシーを未調整としてマークすると、Guard は攻撃を検出しなくなります。その結果、Guard は悪意のあるトラフィックのしきい値をラーニングします。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。
- **Protect and Learn** の選択によってゾーン保護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 つのプロセスを同時に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 メニューの **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 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 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	
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	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。Filter-rate termination threshold とともに使用します。
アクティベーションのパラメータ	
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ときに、ゾーン保護をアクティブにするゾーンを Guard がどのように識別するかを定義します。
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）。

表 4-3　General Configuration の情報（続き）

項目	説明
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 **Guard Summary** を選択します。Guard の要約メニューが表示されます。

ステップ 2　Guard 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（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。