CHAPTER 4

ゾーンの作成と設定

この章では、Detector 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 で DDoS 攻撃の監視の対象となるネットワーク要素です。次のいずれかまたはすべてのネットワーク オブジェクトを表現するゾーンを作成できます。

- 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 は Cisco 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、ユーザに対して Cisco Guard 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 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監視できます。新しいゾーンを作成するときは、次のアトリビュートを含んだゾーン設定を作成します。

- 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 が作成するポリシーのタイプを定義します。各ゾーン テンプレートには、一連のポリシー テンプレートが含まれています。
- ポリシー：ゾーンのトラフィックを分析し、ゾーンが異常なトラフィックを受信したときにアクションを実行します。各ゾーンの設定は、それぞれ独自のポリシー セットで構成されています。これらのポリシーは、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、またはラーニング プロセス実行中に作成されたゾーン固有のポリシーのいずれかです。ゾーンのトラフィックがいずれかのポリシーのしきい値を超過すると、攻撃と見なされ、そのポリシーはアクションを実行します。ポリシーのアクションは、通知の送信から、ゾーンを DDoS 攻撃から保護するための Cisco Guard のアクティブ化に及びます。

- ゾーン　フィルタ：ゾーンのトラフィックを必要とされる保護レベルに誘導し、Detector 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。ゾーン フィルタを使用すると、特定のトラフィック フローをカウントしたり、Detector の異常検出機能をバイパスすることができます。デフォルトのフィルタ設定を変更してカスタマイズしたゾーン フィルタの設定を作成し、そのフィルタで Detector がトラフィック フローに適用する異常検出機能を決定することもできます。

次の方法により、ゾーンを作成することができます。

- Detector または Cisco Guard の定義済みのゾーン テンプレートを使用する：Detector または Guard のゾーン テンプレートのいずれかの設定に基づいて、ゾーンを作成します。Guard のゾーン テンプレートを使用すると、Detector と Cisco Guard の間でゾーンの設定情報を同期させることができます。ゾーンを同期させるための手動と自動の機能は、CLI を使用して設定します（詳細については、『*Cisco Traffic Anomaly Detector Configuration Guide*』を参照）。

  Detector のゾーン テンプレートは、Detector でのみ使用します。Detector のゾーン テンプレートは、ゾーンの設定情報の同期が不要な場合に使用します。

  各ゾーン テンプレートには、Detector が監視するネットワーク サービスを定義する、あらかじめ定義された一連のポリシーがあります。また、ゾーンのテンプレートには、Detector がラーニング プロセスの実行中にゾーンのトラフィックの分析や検出するサービスに対するポリシーの作成に使用する、一連のポリシー テンプレートも含まれています。Detector がラーニング プロセスの実行中に作成する新規の各ポリシーは、対応するポリシー テンプレートの規則を使用して構築されます。
- 既存のゾーンをテンプレートとして使用する：既存のゾーンのポリシーとポリシーのしきい値を含んでいる、既存のゾーン設定に基づいて新しいゾーンを作成します。新しいゾーンのトラフィック特性が既存のゾーンと一致している場合は、新しいゾーンに対してラーニング プロセスを実行する必要はありません。2 つのゾーンでトラフィックの特性が異なる場合は、新しいゾーンでラーニング プロセスを実行して、Detector が新しいゾーンのトラフィックを分析し、そのゾーンの設定に対して必要に応じてポリシーを変更できるようにする必要があります。

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

ゾーンを同期させるために GUARD_ ゾーン テンプレートを使用してゾーンの設定を定義する場合は、Cisco Guard がゾーンの保護を自動的にアクティブにするために使用するトリガーである、アクティベーション方式を定義することができます。また、Cisco Guard で保護する領域の範囲も定義できます。たとえば、Cisco Guard は、ゾーン全体を保護することも、ゾーン内の特定の領域を保護することもできます。

この項は、次の情報で構成されています。

保護のアクティベーション方式

Cisco Guard では、ゾーン名か、または宛先変更で Guard に送信されたトラフィックから抽出した情報に基づいて、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。

- ゾーン名：Cisco Guard は、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、Cisco Guard がゾーン保護をアクティブにするために使用するデフォルトの方式です。
- IP アドレス：Cisco Guard 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。Cisco 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複数のゾーンが設定されている場合、Cisco Guard は、プレフィックスが最も長く一致するゾーンをアクティブにすることを選択します。つまり、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がアクティブになります。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：Cisco Guard は、データベースにある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。Cisco Guard は、パケットを受信すると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複数のゾーンが設定されている場合、Cisco Guard は、プレフィックスが最も長く一致するゾーンをアクティブにします。つまり、受信したパケットの IP アドレスが含まれていて、アドレス範囲が最も詳細に特定されるゾーンです。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。

ゾーンの保護の範囲

アクティベーション範囲は、Cisco 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に対して保護モード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 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。

Cisco 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。Cisco 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：ゾーン内部の指定した 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。Cisco 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（次の「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）に対して保護モードをアクティブにした場合、Cisco 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、Cisco 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。サブゾーンの IP アドレスおよびサブネットは、Cisco Guard が外部からの攻撃の兆候で受信したもの、または Cisco Guard が保護モード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。

サブゾーンの保護モードが終了すると、Cisco Guard はサブゾーンを消去します。サブゾーンの保護モードは、通常のゾーンの保護モードを終了するときと同様に、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終了します。

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　次のいずれかの方法で、Create Zone 画面を表示します。

- ナビゲーション ペインで **Detector Summary** をクリックして Detector の要約メニューを表示し、次のいずれかのメニュー オプションを選択します。
  - **Zones > Create Zone** を選択する
  - **Zones > Zone list** を選択し、Zone list 画面で **Add** をクリックする
- ナビゲーション ペインで任意のゾーンをクリックしてゾーンのメイン メニューを表示し、そのメニューから **Main > Create Zone** を選択します。

ステップ 2　表 4-1 の説明に従って、ゾーンの設定のパラメータを設定します。

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。先頭を英字にして、1 ～ 63 文字の英数字文字列を入力します。文字列にアンダースコア（_）を含めることはできますが、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。
Operation mode	攻撃中に Detector で実行される異常検出のモード。Operation mode ドロップダウン リストから、次のいずれかを選択します。 • **Automatic** : Detector は攻撃中に動的フィルタを作成し、それらをすべて自動的にアクティブにします。 • **Interactive :** 攻撃中に作成され、Detector の推奨事項として提案される動的フィルタを受け入れるか無視するかをユーザが決定します。 ゾーンの検出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 がゾーンの異常の検出を実行する方法の設定」の項を参照してください。

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

フィールド	説明
Zone Template	ゾーンの設定で使用されるデフォルト ポリシーを定義するゾーン テンプレート。Detector 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 専用のゾーン テンプレート。ゾーンの設定を Cisco Guard と同期させない場合は、DETECTOR_ の方のゾーン テンプレートを選択します。 • **GUARD_** : Detector と Cisco Guard で使用するためのゾーン テンプレート。CLI を使用してゾーンの設定を Cisco Guard と同期させる予定がある場合は、GUARD_ の方のゾーン テンプレートを選択します（『*Cisco Traffic Anomaly Detector Configuration Guide*』を参照）。 Template ドロップダウン リストから、次のいずれかを選択します。 • **DETECTOR_DEFAULT** : Detector のデフォルトのゾーン テンプレート。 • **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_DEFAULT**: Cisco Guard のデフォルトのゾーン テンプレート。Cisco Guard は、パケットの送信元 IP アドレスを Cisco Guard 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。 • **GUARD_TCP_NO_PROXY** : Cisco Guard が TCP プロキシとして動作しないようにするゾーン用のゾーン 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（IRC）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運用されている場合に使用できます。

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

フィールド	説明
Zone Template（続き）	• **GUARD_VOIP**：Session Initiation Protocol（SIP）over UDP を使用して Voice over IP（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 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。 • **帯域幅限定リンク　テンプレート**：小規模なカスタマー（ゾーン）による大規模なネットワークに関係するアプリケーションを主な対象として、特定のサーバまたはサービスではなく、リンクに対する攻撃を検出するために設計されたゾーン テンプレート。リンク テンプレートをこの目的で使用するには、ゾーンを既知の帯域幅ごとにセグメント化できる必要があります。リンク テンプレートを使用して新しいゾーンを作成するときは、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。（表の Protect-IP state 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 K、1 M、4 M、および 512 K の各リンク用が用意されています。 － **DETECTOR_LINK_128K** － **DETECTOR_LINK_1M** － **DETECTOR_LINK_4M** － **DETECTOR_LINK_512K** － **GUARD_LINK_128K** － **GUARD_LINK_1M** － **GUARD_LINK_4M** － **GUARD_LINK_512K** リンク テンプレートで作成されるポリシーは、ゾーンでオンデマンドの保護が必要になった場合に使用できるように設定されます。

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）	リンク テンプレートを使用するときは、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。ただし、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 プロセスの実行」の項を参照）。 これらのゾーンについては、攻撃されているサブネットまたは範囲に基づいて Cisco Guard で保護モードをアクティブにすることをお勧めします。これには、ステップ 5 で activation-extent パラメータを **IP address only** に設定します。
Protect-IP state	Detector がリモートの Cisco Guard をアクティブにするために使用する Guard 保護方式。ここで選択する Guard 保護方式により、Cisco Guard が特定のゾーン保護要件に集中するようにして、Cisco Guard のリソースを節約することができます。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 トラフィックで異常を検出したら、Cisco Guard をアクティブにしてゾーン全体を保護します。この方式は、Cisco Guard が保護するアクティブ ゾーンの数を削減するので、Cisco Guard リソースを節約します。ゾーンが関連するサブゾーンから構成されている場合、この方法をお勧めします。 • **Only Dst IP**：ゾーン トラフィックで異常が検出され、特定の IP アドレスが宛先になっていた場合、Cisco Guard をアクティブにして特定の IP アドレスを保護します。Cisco 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ますが、ゾーン全体のトラフィックを Cisco Guard に宛先変更することを回避できます。Detector が特定の IP アドレスで異常が発生したトラフィックに関連付けられない場合、ゾーンを保護するために、Detector module をアクティブ化しません。ゾーンが関連性のないサブゾーンから構成されている場合、この方法をお勧めします。

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）	• **Policy type**：Detector が Cisco Guard をアクティブ化するために使用するポリシーに従って、Cisco Guard をアクティブにしてゾーン全体を保護するか、ゾーン アドレス範囲内の特定の IP アドレスを保護します。Detector は、Cisco Guard をアクティブにして、特定の IP アドレスが宛先となっているゾーン トラフィックで異常を検出した場合、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原因であるポリシーが dst_ip のトラフィックの特性を持つ場合）。Detector がトラフィックの異常を特定の IP アドレスに関連付けられない場合、Cisco Guard をアクティブ化して、ゾーン全体を保護します（たとえば、リモート アクティベーションの原因となったポリシーがグローバルなトラフィックの特性を持つ場合）。 ゾーンが関連するサブゾーンで構成されていて、対象となるゾーンがゾーン全体に損失を発生させるような状況を避けたい場合は、この方法をお勧めします。 • **Only Dst IP by address**：ゾーン トラフィックで異常が検出され、特定の IP アドレスが宛先になっていた場合、Cisco Guard をアクティブにして特定の IP アドレスを保護します。この IP アドレスは、該当の Cisco Guard で定義されたゾーンのいずれかのアドレス範囲内にある必要があります。ただし、Detector でのゾーン名は Cisco Guard でのゾーン名と同じである必要はありません。Cisco Guard メイン メニューで **Main > Protect IP** を選択することにより、Only Dst IP by address protect-IP 状態は、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 でのゾーン名が Cisco Guard でのゾーン名と同じでない場合や、ゾーン全体が関連性のないサブゾーンで構成されている場合は、この方法をお勧めします。 **（注）** Detector module が攻撃を受けた IP アドレスだけに対するゾーン保護をアクティブにして、ゾーン トラフィックの自身への宛先変更を停止していることを確認するには、ゾーンが IP アドレスのみのアクティベーション範囲を持つ Cisco Guard で定義されていることを確かめます。

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

フィールド	説明
IP address	ゾーンの IP アドレス。
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。

ステップ 3　次のいずれかのオプションを選択します。

- **OK**：新しいゾーン設定を保存します。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。

  （オプション）全般ビュー画面に表示される Attack Detection/Termination、Activation、および Packet Dump のパラメータを設定するには、**Config** をクリックして Config 画面を表示し、次のステップに進みます。

  - Attack Detection/Termination のパラメータを設定する場合は、ステップ 4（GUARD_ ゾーン テンプレートのみ）
  - Activation のパラメータを設定する場合は、ステップ 5（GUARD_ ゾーン テンプレートのみ）
  - Packet Dump のパラメータを設定する場合は、ステップ 6
- **Clear**：フォームの情報をデフォルト値に戻し、追加した情報をすべて消去します。
- **Cancel**：情報を保存せずに Create Zone 画面を終了します。Zone List 画面が表示されます。

ステップ 4　（オプション）GUARD_ ゾーン テンプレートを使用して作成するゾーンの Attack Detection/Termination のパラメータを設定します。この設定は、Cisco Guard のゾーンだけに影響を与えます。表 4-3 では、attack detection と termination パラメータについて説明します。

表 4-2　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。レートがこのしきい値より低くなった場合、Cisco Guard がゾーンの保護モード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、Cisco 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。Cisco Guard は、保護メカニズム（動的フィルタ、フレックスコンテンツ フィルタ、およびレート リミッタ）が攻撃の一部として識別したゾーン パケットをドロップします。ドロップされるパケットは、ゾーンの Dropped カウンタを使用してカウントされます。Malicious-rate detection threshold のデフォルトは、10 パケット / 秒（pps）です。
Protection-end timer	Cisco Guard が保護モードを終了できる時刻。Cisco Guard は、自身が作成する動的フィルタをチェックすることで、攻撃が終了したかどうかを確認します。使用中になっている動的フィルタがなく、事前定義されている期間内に新しい動的フィルタが作成されなかった場合、Cisco Guard は保護モードを非アクティブにします。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。
Filter-rate termination threshold	このしきい値は、Malicious-rate termination threshold とともに使用して、Cisco 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、Cisco 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 5　（オプション）GUARD_ ゾーン テンプレートを使用して作成するゾーンのアクティベーション範囲を設定します。この設定は、Cisco Guard のゾーンだけに影響を与えます。表 4-3 の説明に従ってパラメータを設定します。

表 4-3　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。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 Cisco Guard がどのように識別するかを定義します。Cisco Guard は、次のアクティベーション方式をサポートします。 • **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。ゾーン保護をアクティブにするコマンドにゾーン名が含まれている必要があります。 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**：Cisco Guard は、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。Cisco 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、Cisco 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。 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**：Cisco Guard 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。Cisco 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、Cisco 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。

表 4-3　Activation のパラメータ

フィールド	説明
Activation interface（続き）	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**：Cisco Guard は、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。
Activation extent	外部からの攻撃の兆候を受信した場合に、Cisco Guard が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。 次のいずれかのオプションを選択します。 • **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。

ステップ 6　（オプション）表 4-4 の説明に従って、Packet Dump 領域のパラメータを設定します。

表 4-4　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	Detector で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 単位）を入力します。

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　次のいずれかのオプションを選択します。

- **OK**：新しいゾーン設定を保存します。ゾーンの全般ビュー画面が表示されます。
- **Clear**：フォームの情報をデフォルト値に戻し、追加した情報をすべて消去します。
- **Cancel**：情報を保存せずに Zone Save as 画面を終了します。ゾーンの全般ビュー画面が表示されます。

ゾーンの設定の変更

ゾーンの設定のパラメータを変更するには、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。

ステップ 4　目的のゾーン パラメータを変更します（パラメータについては、表 4-1 を参照）。

ステップ 5　次のいずれかのオプションを選択します。

- **OK**：新しいゾーン設定を保存します。ゾーンの全般ビュー画面が表示されます。
- **Clear**：フォームの情報をデフォルト値に戻し、追加した情報をすべて消去します。
- **Cancel**：情報を保存せずに Zone Save as 画面を終了します。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。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。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、192.168.100.50）。

ステップ 6　次のいずれかのオプションを選択します。

- **OK**：新しいゾーン設定を保存します。ゾーンの全般ビュー画面が表示されます。

- **Cancel**：情報を保存せずに Add Zone IP 画面を終了します。ゾーンの全般ビュー画面が表示されます。

ゾーンの IP アドレス範囲から IP アドレスを削除するには、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て、**Delete** をクリックします。

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、ゾーンで検出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、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開始」の項、または第 8 章「ゾーンのポリシーの管理」の「サービスの追加または削除」の項を参照してください。
- ゾーン検出とラーニング 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 で攻撃が検出されなくなり、Detector 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。
- ゾーン検出とラーニング　プロセスをイネーブルにしていない状態で、ゾーン検出とラーニング プロセスをイネーブルにする予定もない場合は、ゾーン検出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 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、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。削除の確認画面が表示されます。

ステップ 4　次のいずれかのオプションを選択します。

- **OK**：ゾーンを削除して Zone list 画面を表示します。
- **Cancel**：ゾーンの削除要求を無視して Zone list 画面を表示します。