CHAPTER 9

ゾーン トラフィック異常の検出

この章では、Cisco Traffic Anomaly Detector モジュール（Detector モジュール）を設定してトラフィックの異常を検出する方法について説明します。

この章には、Detector モジュールの関連製品である Cisco Guard（Guard）についての記述があります。Guard は、DDoS 攻撃（分散型サービス拒絶攻撃）を検出して軽減するデバイスです。Guard は、ゾーン トラフィックが通過する際に攻撃トラフィックをドロップして正常なトラフィックをネットワークに戻し、ゾーン トラフィックをクリーンにします。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できます。また、Detector モジュールは Guard とゾーン設定を同期させることができます。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。

ゾーン異常検出について

ゾーン異常検出とは、Detector モジュールがゾーンのトラフィックのコピーを積極的に監視し、ゾーンでの DDoS 攻撃の兆候がないかを調べることです。ポリシーしきい値を超える（攻撃を示す）ことによってトラフィック異常がポリシー アクションをトリガーすると、Detector モジュールは、次のいずれかのタスクを実行します。

- Detector モジュールのリモート Guard リストで定義している Guard をアクティブにし、攻撃を軽減する。
- ユーザに通知を送信する。

異常検出をアクティブにする前に、次の要件と推奨事項を確認してください。

- スイッチでのポート ミラーリングの設定、または光スプリッタによる Detector モジュールとルータの接続：分析のためにゾーン トラフィックのコピーを Detector モジュールに提供するには、これらのいずれかの方式を使用する必要があります。
- ラーニング プロセスの実行：Detector モジュールに対して、通常のトラフィック特性に基づいたゾーン固有のポリシーおよびポリシーしきい値のセットの作成を許可することをお勧めします。ラーニング プロセスを実行するには、次の手順を実行することをお勧めします。
  1. ポリシー構築フェーズをアクティブ化する：Detector モジュールは、ゾーン トラフィックで検出するサービスに基づいてポリシーのセットを作成します。詳細については、P.8-5 の「ポリシー構築フェーズのアクティブ化」を参照してください。
  2. 検出およびラーニング機能をアクティブにする：Detector モジュールは、最後に受け入れられたポリシーしきい値を使用してトラフィックの異常を監視しながら、ラーニング プロセスのしきい値調整フェーズを実行します。Detector モジュールは、ゾーンに対する攻撃を検出した場合はしきい値調整フェーズを停止しますが、ゾーン トラフィックの異常検出は継続します。詳細については、P.8-14 の「検出およびラーニング機能のイネーブル化」を参照してください。

  （注）　検出およびラーニングのオプションは、ゾーンが攻撃を受けていないと確信できるときにのみアクティブにします。

- ゾーン設定と Guard との同期：Guard を Detector モジュールと関連付けてゾーン保護を行うと、Detector モジュール上のゾーン設定を Guard 上のゾーン設定と同期させることができます。詳細については、P.5-11 の「Guard モジュール とのゾーン設定の同期」および P.9-6 の「ゾーンを保護するためのリモート Guard のアクティブ化」を参照してください。
- 異常検出特性の定義：次のオプションの異常検出特性を設定できます。
  - 動作モード：Detector モジュールがゾーン異常検出を実行する方法を定義します（Detector モジュールによってゾーン トラフィックの異常を自動的に検出するか、または Detector モジュールが実行するアクションを決定するインタラクティブ方式で検出するか）。詳細については、P.9-3 の「Detector モジュールがゾーン異常検出を行う方法の設定」を参照してください。
  - Guard 保護アクティベーション方式：Detector モジュールがゾーンを保護するためにリモート Guard をアクティブにする方法を定義します。Detector モジュールは、リモート Guard をアクティブにしてゾーン全体の一部である特定のゾーン（たとえば、保護されたネットワーク環境の一部である特定のサーバ）を保護することも、リモート Guard をアクティブにしてゾーン全体を保護することもできます。

ヒント　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** コマンドを入力して、Detector モジュールがゾーンのトラフィックのコピーを受信していることを確認できます。*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、Detector モジュールがゾーンのトラフィックのコピーを受信していないことを示します。スイッチでのポートミラーリングの設定を確認するか、または光スプリッタで Detector モジュールとルータとの接続を確認します。

Detector モジュールがゾーン異常検出を行う方法の設定

ゾーンの攻撃中、Detector モジュールでは、攻撃中に Detector モジュールが実行するアクションを決定する動的フィルタが作成されます。それぞれの動的フィルタに関連付けられたアクションを自動的に実行するか、または提案されたアクションを実行するかどうかをユーザが決定するのを待つように、Detector モジュールを設定できます。動的フィルタのアクションの実行を制御するには、次のいずれかのモードで異常検出が実行されるように Detector モジュールを設定します。

- 自動検出モード：Detector モジュールで動的フィルタが作成されるとすぐにフィルタのアクションが実行されます。この動作モードはデフォルトです。
- インタラクティブ検出モード：Detector モジュールの動的フィルタは*推奨事項*として保存されます。ユーザは推奨事項のリストを確認して、どの推奨事項を受け入れるか、無視するか、自動アクティベーションの対象にするかを決定します。

ゾーン設定モードで **show** コマンドを使用して、ゾーンの現在の動作モードを表示します。

インタラクティブ検出モードをイネーブルにするには、ゾーン設定モードで次のコマンドを使用します。

interactive

インタラクティブ検出モードをディセーブルにして、自動検出モードを使用するには、ゾーン設定モードで次のコマンドを使用します。

no interactive

次のインタラクティブ保護動作の詳細については、第 10 章「インタラクティブ検出モードの使用方法」を参照してください。

- 新しいゾーンを作成する際のインタラクティブ保護モードのイネーブル化
- 保護の推奨事項の管理
- 自動保護モードへの切り替えが必要なタイミングの判断

Guard 保護のアクティベーション方式の設定

Guard 保護のアクティベーション方式は、Detector と関連付けられているリモート Guard がゾーン保護をアクティブにする方法を定義します。このアクティベーション方式は、ゾーンの保護要件に焦点を当て、Guard モジュールのリソースを節約するものです。

Guard 保護アクティベーション方式をアクティブにするには、ゾーンの設定モードで次のコマンドを入力します。

protect-ip-state {**entire-zone | dst-ip-by-name | dst-ip-by-ip | policy-type**}

Guard 保護アクティベーション方式は次のとおりです。

- **entire-zone** : Guard モジュールをアクティブにし、ゾーン トラフィックに異常が検出されるとゾーン全体を保護します。この方式では、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が節約されます。ゾーンが関連性のあるサブゾーンで構成されている場合にこの方式を使用します。
- **dst-ip-by-name** : Guard モジュールをアクティブにし、特定の IP アドレス宛てのゾーン トラフィックに異常が検出された場合に、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、攻撃対象の IP アドレスを保護しながら、ゾーン全体のトラフィックが Guard モジュールに宛先変更されるのを回避できます。Detector モジュールは、トラフィック異常を特定の IP アドレスに関連付けることができない場合、Guard モジュールをアクティブにしないため、ゾーンが保護されません。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式を使用します。
- **dst-ip-by-ip** : Guard モジュールをアクティブにし、特定の IP アドレス宛てのゾーン トラフィックに異常が検出された場合に、その IP アドレスを保護します。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内である必要があります。ただし、Detector モジュール上のゾーン名が、Guard モジュール上のゾーン名と一致する必要はありません。**dst-ip-by-ip** Guard 保護アクティベーション方式は、Guard モジュール上で **protect** *ip-address* コマンドを使用した場合と同じ結果になります。Detector モジュール上のゾーン名が Guard モジュール上のゾーン名と一致しない場合、または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にこの方式を使用します。

（注）　確実に Guard モジュールが攻撃対象の IP アドレスに対してだけ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がそれ自身に宛先変更されるのを回避するには、アクティベーション範囲が **ip-address-only** になるように Guard モジュール上でゾーンを定義します。

- **policy-type** : Guard モジュールをアクティブにし、Detector モジュールが Guard モジュールをアクティブにする原因となったポリシーに応じて、ゾーン全体を保護するか、またはゾーン内の特定の IP アドレスを保護します。特定の IP アドレス宛てのゾーン トラフィックで異常が検出された場合（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のトラフィック特性が **dst_ip** である場合）、Detector モジュールは 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。トラフィック異常を特定の IP アドレスと関連付けることができない場合（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のトラフィック特性が global である場合）、Detector モジュールは 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。ゾーンが関連するサブゾーンから構成されており、攻撃対象のサブゾーンの状況によってゾーン全体がダメージを受けるのを防止できる場合に、この方式を使用します。

次の例は、Guard 保護アクティベーション方式を設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# protect-ip-state entire-zone
```

ゾーン異常検出のアクティブ化

ゾーン異常検出をアクティブにするには、ゾーン設定モードで次のコマンドを入力します。

detect [**learning**]

オプションの **learning** キーワードは、検出およびラーニング機能（詳細については、P.8-14 の「検出およびラーニング機能のイネーブル化」を参照）によって、Detector モジュールがゾーン トラフィックの異常を検出してゾーン ポリシーのしきい値を調整できるようにします。

次の例は、ゾーン scannet の異常検出を非アクティブにする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# detect
```

ゾーン異常検出の非アクティブ化

ゾーン異常検出を非アクティブにするには、ゾーン設定モードで次のコマンドのいずれかを使用します。

- **no detect**：ゾーン異常検出を終了します。**no detect** コマンドに入るときに検出およびラーニング機能をイネーブルにしている場合、Detector モジュールはゾーン異常検出を終了しますが、ラーニング プロセスのポリシーしきい値フェーズは継続します（詳細については P.8-14 の「検出およびラーニング機能のイネーブル化」を参照）。
- **deactivate**：ゾーン異常検出と、ラーニング　プロセスのしきい値調整フェーズの両方を終了します。

ゾーンを保護するためのリモート Guard のアクティブ化

Detector モジュールは、ゾーン トラフィックの異常を検出すると動的フィルタを作成します。このフィルタは、Detector モジュールと関連付けている Guard モジュールをアクティブにできます。Guard モジュールを Detector モジュールと関連付けていない場合は、動的フィルタは Detector モジュールに対して、イベントだけを記録するよう指示します。

Detector モジュールを使用して、リモート Guard を次の方法のいずれかでアクティブにできます。

- リモート Guard リストの使用：Secure Sockets Layer（SSL）を使用してリモート アクティベーションとゾーン同期をイネーブルにするか、または SSH を使用してリモート アクティベーションだけをイネーブルにします。
- オフラインでのアクティブ化：ゾーンで攻撃が発生したときに通知を発行するように Detector モジュールを設定します。
- 手動でのアクティブ化:リモート Guard をアクティブにするための動的フィルタを作成します。

Detector モジュールは、Guard のダウンストリームに配置します。進行中の攻撃がない場合、Detector モジュールは、保護されたゾーン宛てのすべてのインバウンド トラフィックを監視します。攻撃を受けている間に、Guard が被害を軽減するために攻撃対象のゾーンからのトラフィックを宛先変更した場合は、Detector モジュールは Guard からそのゾーンに転送された正当なトラフィックを監視します。

この項では、次のトピックについて取り上げます。

リモート Guard リストを使用したリモート Guard のアクティブ化

ゾーンを保護するためにアクティブにする Guard のリスト（リモート Guard リストとも呼ばれる）で、Detector モジュールを設定することができます。Detector モジュールは、次の 2 つのタイプのリモート Guard リストを保持します。

- ゾーンのリモート Guard リスト：Detector モジュールは、このゾーン固有のリストで Guard をアクティブにし、ゾーンを保護します。場合によっては、ゾーン設定を Guard と同期します。
- デフォルトのリモート Guard リスト：ゾーンのリモート Guard リストが空であるか、または SSL とセキュア シェルのどちらの通信方式も含まれていない場合にだけ、Detector がデフォルト リストを検索します。

（注）　リモート Guard リストに Guard を追加する場合は、リモート Guard との通信チャネルを確立する必要があります。詳細については、P.4-18 の「Guard との通信の確立」を参照してください。

各リモート Guard リストは 2 つの通信方式をサポートしています。

- SSL：Detector モジュールは、SSL を使用して Guard と通信します。Detector モジュールは、Guard をアクティブにして、ゾーンを保護し、ゾーン設定とリモート Guard を同期できます。

  Detector モジュールは、Guard をアクティブにしてゾーンを保護する前に、ゾーン設定をリモート Guard リストの Guard と同期できます。詳細については、P.5-11 の「Guard モジュール とのゾーン設定の同期」を参照してください。
- Secure Shell（SSH）：Detector モジュールは、SSH を使用して Guard と通信します。Detector モジュールは、Guard をアクティブにしてゾーンを保護できますが、ゾーン設定を Guard と同期できません。

Detector モジュールは、同じ通信方式の Guard モジュールがゾーンのリモート Guard リストに定義されていない場合にだけ、デフォルトのリモート Guard リストの Guard モジュールをアクティブにします。

注意　リモート Guard リストを変更する場合は、Detector モジュールがリモート Guard との通信チャネルに使用する SSL 証明書を再生成する必要があります。再生成しないと、通信に失敗します。詳細については、P.4-20 の「SSL 証明書の再生成」を参照してください。

Detector モジュールのリモート Guard リストのいずれか（デフォルトのリモート Guard リスト、またはゾーンのリモート Guard リスト）に少なくとも 1 つは Guard が定義されていることを確認してください。どのリモート Guard リストにもリモート Guard が定義されていない場合、Detector モジュールはログ ファイルにイベントを記録します。

この項では、次のトピックについて取り上げます。

- リモート Guard のアクティブ化およびゾーン設定の同期
- デフォルトのリモート Guard リストの設定
- ゾーンのリモート Guard リストの設定

リモート Guard のアクティブ化およびゾーン設定の同期

リモート Guard をアクティブにしゾーン設定を同期するには、次の手順を実行します。

ステップ 1　Guard 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および設定します。

P.5-5 の「新しいゾーンの作成」を参照してください。

ステップ 2　リモート Guard IP アドレスを次のいずれかのリストに追加します。

- ゾーンのリモート Guard リスト：そのゾーンの保護用に Detector モジュールによってアクティブにされるリモート Guard のリスト。

  詳細については、P.9-9 の「ゾーンのリモート Guard リストの設定」を参照してください。
- Detector のデフォルト リモート Guard リスト：リモート Guard のデフォルト リスト。ゾーンのリモート Guard リストが空の場合、Detector モジュールはこれらのリモート Guard をアクティブにします。

  詳細については、P.9-8 の「デフォルトのリモート Guard リストの設定」を参照してください。

ステップ 3　リモート Guard との通信チャネルを設定します。

詳細については、P.4-18 の「Guard との通信の確立」を参照してください。

ステップ 4　ゾーン Guard 保護形態（**protect-ip-state**）を設定し、Detector モジュールがリモート Guard をアクティブにするために使用する方式を決定します。

詳細については、P.9-4 の「Guard 保護のアクティベーション方式の設定」を参照してください。

ステップ 5　次のいずれかの方法で、リモート Guard 上に新しいゾーンを作成します。

- SSL を使用して、Detector モジュールのゾーン設定を Guard に同期させる。

  詳細については、P.5-11 の「Guard モジュール とのゾーン設定の同期」を参照してください。
- リモート Guard 上に新しいゾーンを作成する。**protect-ip-state dst-ip-by-ip** コマンドを使用して、攻撃対象の IP アドレスのみに基づいて Guard 上の保護をアクティブにするように Detector モジュールを設定していない限り、Guard 上のゾーン名は Detector モジュール上のゾーン名と一致している必要があります。

  protect-ip-state コマンドの詳細については、P.9-4 の「Guard 保護のアクティベーション方式の設定」を参照してください。

ステップ 6　リモート Guard 内で **protection-end-timer** コマンドを使用して、リモート Guard がゾーン保護を終了するために使用するタイマーを設定します。protection-end-timer の値が **forever** の場合、リモート Guard は攻撃が終了してもゾーン保護を終了しません。

デフォルトのリモート Guard リストの設定

Detector モジュールは、次の両方の条件が当てはまる場合に、デフォルトのリモート Guard リスト内のリモート Guard をアクティブにします。

- ゾーンのリモート Guard リストが空であるか、または SSL および SSH の両方の通信方式を持つ Guard モジュールが含まれていない。
- デフォルトのリストのリモート Guard に、ゾーン固有のリモート Guard リストに定義されていない通信方式が設定されている。

Detector モジュールは、同じ通信方式のすべてのリモート Guard をアクティブにします。

デフォルトのリモート Guard リストに Guard を追加するには、設定モードで次のコマンドを入力します。

remote-guard {**ssh** | **ssl**} *remote-guard-address* [*description*]

表 9-1 に、**remote-guard** コマンドの引数とキーワードを示します。

表 9-1　remote-guard コマンドの引数とキーワード

パラメータ	説明
ssh	SSH 通信方式を指定します。
ssl	SSL 通信方式を指定します。
remote-guard-address	リモート Guard の IP アドレス。
description	（オプション）リモート Guard の説明。説明は、最大 63 文字の英数字です。

次の例は、SSL 通信方式を使用してデフォルトのリモート Guard リストにリモート Guard を追加する方法を示しています。

```
user@DETECTOR-conf# remote-guard ssl 192.168.100.33
```

リモート Guard のデフォルトのリストを表示するには、グローバル モードまたは設定モードで **show remote-guards** コマンドを使用します。

ゾーンのリモート Guard リストの設定

Detector モジュールは、ゾーンのリモート Guard リストで定義しているすべてのリモート Guard をアクティブにします。

ゾーンのリモート Guard リストに Guard を追加するには、ゾーン設定モードで次のコマンドを入力します。

remote-guard {**ssh** | **ssl**} *remote-guard-address* [*description*]

表 9-2 に、**remote-guard** コマンドの引数とキーワードを示します。

表 9-2　remote-guard コマンドの引数

パラメータ	説明
ssh	SSH 通信方式を指定します。
ssl	SSL 通信方式を指定します。
remote-guard-address	リモート Guard の IP アドレス。
description	（オプション）リモート Guard の説明。説明は、最大 63 文字の英数字です。

次の例は、SSL 通信方式を使用してゾーンのリモート Guard リストに Guard を追加する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# remote-guard ssl 192.168.100.33
```

ゾーンのリモート Guard リストを表示するには、ゾーン設定モードで **show remote-guards** コマンドを使用します。

リモート Guard のオフラインでのアクティブ化

Detector モジュールは、ゾーン トラフィックに異常を検出すると、イベントをログに記録し、場合によっては Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップを生成します（P.4-29 の「SNMP トラップのイネーブル化」を参照）。その後、手動で Guard をアクティブにし、ゾーンを保護することができます。

Guard をオフラインでアクティブにするには、次の手順を実行します。

ステップ 1　Detector モジュールと Guard の両方にゾーンを設定するか、またはゾーン設定をオフラインで同期します。

詳細については、P.5-12 の「同期のためのゾーン作成」を参照してください。

ステップ 2　（ オプション）リモート Guard 内で **protection-end-timer** コマンドを使用して、リモート Guard がゾーン保護を終了するために使用するタイマーを設定します。protection-end-timer の値を **forever** に設定すると、リモート Guard は攻撃が終了してもゾーン保護を終了しません。

ステップ 3　**protect** コマンドを使用して、Cisco Anomaly Guard モジュール上のゾーンをアクティブにします。

手動でのリモート Guard のアクティブ化

Detector モジュールがゾーン トラフィックに異常を検出する前であっても、Detector モジュールからリモート Guard を手動でアクティブにしてゾーンを保護することができます。

リモート Guard を手動でアクティブにするには、Detector モジュールで次の手順を実行します。

ステップ 1　ゾーン リモート Guard リストまたはデフォルトのリモート Guard リストにリモート Guard を追加します。

詳細については、P.9-6 の「リモート Guard リストを使用したリモート Guard のアクティブ化」を参照してください。

ステップ 2　**dynamic-filter remote-activate** コマンドを入力して動的フィルタを作成します。

詳細については、P.6-17 の「動的フィルタの追加」を参照してください。