ゾーンのトラフィックの異常の検出

この章では、Cisco Traffic Anomaly Detector Module（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と、Cisco Anomaly Guard Module をアクティブにしてゾーンを保護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。

概要

ゾーンの異常検出をアクティブにすると、Detector モジュールは、受信するゾーン トラフィックのコピーを監視します。トラフィック異常がポリシーしきい値を超える（攻撃を示す）ことによってポリシー アクションをトリガーすると、Detector は、Guard モジュールが定義されている場合は Guard モジュールをアクティブにしてゾーンを保護するか、または、通知を送信します。

ゾーン異常検出をアクティブにする前に、Detector モジュールにラーニング プロセスを使用してゾーン トラフィックのパターンを学習させることができます。ラーニング プロセスを使用すると、Detector モジュールはゾーンのトラフィック パターンを学習して、ゾーン トラフィックの統計分析に従い一連の推奨しきい値を作成できます。

ゾーンが攻撃されていない場合は、**learning policy-construction** コマンドを使用して Detector モジュールにゾーンのポリシーを構築させてから、検出およびラーニング機能をイネーブルにすることをお勧めします。Detector モジュールは、ゾーン トラフィックをラーニングすると同時に、最後に受け入れられたポリシーしきい値を監視してトラフィック異常がないか調べます。Detector モジュールは、ゾーンで攻撃を検出すると、しきい値調整フェーズを停止しますが、Detector モジュールでの悪意あるトラフィックのしきい値のラーニングを回避するためにゾーン トラフィックの異常検出は継続します。P.8-21 の「ゾーンのポリシーのしきい値調整とゾーン異常検出のイネーブル化の同時実行」を参照してください。

Guard モジュールをアクティブにしてゾーンを保護する前に、Detector モジュール上のゾーン設定と Guard モジュール上のゾーン設定を同期させることができます。詳細については、P.5-14 の「Detector モジュールの Cisco Anomaly Guard Module とのゾーン設定の同期」および P.9-7 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。

ゾーン異常検出をアクティブにする前に、ゾーンに送信されるトラフィックをキャプチャし、そのコピーを Detector モジュールに渡すようにスイッチを設定する必要があります。詳細については、P.2-5 の「トラフィックをキャプチャするためのトラフィックの送信元の設定」を参照してください。

ヒント　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してください。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。トラフィックの送信元が、トラフィックのキャプチャについて設定されていることを確認します。詳細については、P.2-5 の「トラフィックをキャプチャするためのトラフィックの送信元の設定」を参照してください。

次の異常検出特性を定義できます。

- 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、またはインタラクティブ方式で検出するかを定義します）。
- 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 のアクティブ化に使用する方式を定義します。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。

Detector モジュールがゾーン異常検出を行う方法の設定

動作モードによって、異常検出がイネーブルな場合に Detector モジュールがどのように動的フィルタをアクティブにするかが決まります。

ゾーン異常検出は、次の 2 つの動作モードにおいてアクティブにできます。

- 自動検出モード：動的フィルタはユーザの操作なしでアクティブになります。これはデフォルトの動作モードです。
- インタラクティブ検出モード：動的フィルタは、インタラクティブ　モードにおいて手動でアクティブになります。動的フィルタは推奨されるグループに分けられています。それらを確認し、どれを受け入れるか、無視するか、または自動アクティブ化するかを決定できます。

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。

Guard 保護のアクティベーション方式の設定

Guard 保護アクティベーション方式は、リモート Guard として定義されている Cisco Anomaly Guard Module（Guard モジュール）がゾーン保護をアクティブにする方法を定義します。この方式は、ゾーンの保護要件に、より正確に焦点を当て、Guard モジュールのリソースを節約することを目的としたものです。アクティベーション方式は、ゾーン全体の一部である特定のゾーン（保護されたネットワーク環境内の特定のサーバなど）のゾーン保護をアクティブにするものから、ゾーン全体のゾーン保護をアクティブにするものまであります。

Detector モジュールは、次の Guard 保護のアクティベーション方式をサポートします。

- **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は、この方法を推奨します。
- **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は、この方法を推奨します。
- **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は、この方法をお勧めします。

（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、activation-extent **ip-address-only** コマンドを使用して 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。

  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回避できるように、ゾーンが関連するサブゾーンから構成されている場合は、この方式をお勧めします。

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**}

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**]

learning キーワードでは、ゾーン トラフィック内の異常を検出すると同時に、ゾーン ポリシーのしきい値を調整するように Detector モジュールが設定されます。詳細については、P.8-21 の「ゾーンのポリシーのしきい値調整とゾーン異常検出のイネーブル化の同時実行」を参照してください。

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。Detector モジュールは、ゾーン トラフィックの異常検出とラーニングの実行中である場合には、ゾーン ポリシーのしきい値のラーニングを継続します。
- **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、動的フィルタと呼ばれる新しいフィルタを作成します。このフィルタは、ゾーンを保護するためにアクションを初期化する Cisco Anomaly Guard Module をアクティブにするか、またはリモート Guard が定義されていない場合はログを記録します。

リモート Guard は、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: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。

論理的に、Detector モジュールは Cisco Anomaly Guard Module のダウンストリームに配置されます。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、Cisco Anomaly Guard Module 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

Detector モジュールは、ゾーンを保護するためにアクティブにされる Guard モジュールのリストを維持しています。このリストは、リモート Guard リストと呼ばれます。複数のリモート Guard リストに Guard モジュールを設定できます。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。

- ゾーン固有のリモート Guard リスト：Detector モジュールは Guard モジュールをアクティブにし、ゾーンを保護します。場合によっては、ゾーン設定を Guard モジュールと同期します。
- 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 Cisco Anomaly Guard Module 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.4-26 の「Cisco Anomaly Guard Module 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 モジュールと通信します。Detector は、リモート 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 モジュール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 モジュールと同期できます。詳細については、P.5-14 の「Detector モジュールの Cisco Anomaly Guard Module とのゾーン設定の同期」を参照してください。
- SSH：Detector モジュールは、SSH を使用して Guard モジュールと通信します。Detector は、リモート Guard をアクティブにしてゾーンを保護できますが、ゾーン設定をリモート 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.4-29 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 Cisco Anomaly Guard Module 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.5-6 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.9-12 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.9-11 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.4-26 の「Cisco Anomaly Guard Module 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 モジュールに同期させます。

  詳細については、P.5-14 の「Detector モジュールの Cisco Anomaly Guard Module 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します。**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 モジュール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かぎり、Guard モジュール上のゾーン名は 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。

- ゾーン固有のリモート 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	リモート Guard の通信方式を SSH に設定します。
ssl	リモート Guard の通信方式を SSL に設定します。
remote-guard-address	リモートの Guard の IP アドレス。
description	（オプション）リモートの Guard の説明。説明は、最大 63 文字です。

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 リストに記載され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	リモート Guard の通信方式を SSH に設定します。
ssl	リモート Guard の通信方式を SSL に設定します。
remote-guard-address	リモート Guard の IP アドレス。
description	（オプション）リモートの Guard の説明。説明は、最大 63 文字です。

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 SNMP トラップを生成します。その後、手動で Cisco Anomaly Guard Module をアクティブにし、ゾーンを保護することができます。詳細については、P.4-42 の「SNMP トラップのイネーブル化」を参照してください。

Cisco Anomaly Guard Module 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 Cisco Anomaly Guard Module 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.5-16 の「同期用のゾーンの設定」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 Module 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、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、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.9-7 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.6-25 の「動的フィルタの追加」を参照してください。