製品概要

この章では、Cisco Traffic Anomaly Detector Module（Detector モジュール）の概要、コンポーネント、および動作のしくみ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。

Cisco Traffic Anomaly Detector Module について

Detector モジュールは、Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃の兆候がないかを継続的に調べる受動的な監視デバイスで、監視の対象となるのは、サーバ、ファイアウォール インターフェイス、またはルータ インターフェイスなどの保護対象の宛先（ゾーンとして参照される）です。Detector モジュールは、Cisco Anomaly Guard モジュールまたはアプライアンス（Guard）との併用に最も適していますが、単独でも DDoS 検出および警告コンポーネントとして運用できます。

Detector モジュールは、次のいずれかの製品にインストールできます。

- Catalyst 6500 シリーズ スイッチ
- Cisco 7600 シリーズ ルータ

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。

Detector モジュールは、保護対象ゾーン（複数も可）を宛先とするすべての着信トラフィックのコピーを分析して、現在のトラフィックと動作のしきい値のセット（ゾーン ポリシー）とを比較し、異常なトラフィックの動作を検出します。Detector モジュールが潜在的な攻撃と見なされる異常な動作を見つけると、Detector モジュールは、Detector モジュールをアクティブにしてこれらの攻撃を軽減することができます。

Detector モジュールでは、次の機能を使用してトラフィックを監視します。

- ゾーンのトラフィックをラーニングし、その特性に合せて自身をチューニングし、Detector モジュールにしきい値とポリシーに基づいた参照とインストラクションを提供する、アルゴリズム ベースのシステム。
- Detector モジュールをリモートでアクティブにしてゾーン（複数も可）を保護状態に置くか、または Detector モジュールの syslog にトラフィックの異常を記録するシステム。

これらの機能を使用することにより、Detector モジュールは、バックグラウンドに控えた状態で検出の役割を果たすことができます。

DDos について

DDoS 攻撃は、正当なユーザが特定のコンピュータまたはネットワーク リソースにアクセスできないようにします。このような攻撃は、個人が悪意のある要求をターゲットに送信してネットワーク サービスの質を低下させ、サーバやネットワーク デバイスのネットワーク サービスを妨害し、不要なトラフィックでネットワーク リンクを飽和状態にすることで発生します。

DDoS 攻撃は、悪意のあるユーザがインターネット上で数百、数千台ものホスト（ゾンビ）を操作し、トロイの木馬を仕掛けることにより発生します。トロイの木馬とは、無害なアプリケーションを装った複製しないプログラムで、ユーザが予想もしない有害なアクションを起こすものです。トロイの木馬は、攻撃者により、いつ、どのように組織的攻撃を開始するかの指示をマスター サーバ コントローラから受けます。ゾンビは、保護されたサーバのネットワーク リソースを偽のサービス要求によって使用不能にする自動化スクリプトを実行します。このような攻撃には、Web サーバに偽のホームページ要求を大量に送信して正当なユーザがアクセスできないようにしたり、Domain Name System（DNS; ドメイン ネーム システム）サーバのアベイラビリティと正確性を低下させようとしたりするものなどがあります。多くの場合、ゾンビは個人によって開始されますが、実際に攻撃用コードを実行しているコンピュータは、複数の組織によって管理される複数の自律システム上に分散しており、その数は何十万にも及ぶ可能性があります。このような分散攻撃は、一般的なゾーンで使用される低い帯域幅では処理できない大量のトラフィックを発生させます。ゾーンの詳細については、P.1-4 の「ゾーンについて」を参照してください。

ゾーンについて

ゾーンは、次のいずれかの要素です。

- ネットワーク サーバ、クライアント、またはルータ
- 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）
- 上記の要素の任意の組み合せ

Detector モジュールは、DDoS 攻撃を発見すると、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、手動で Guard をアクティブにするようにユーザに通知することができます。

Detector モジュールでは、ゾーンのネットワーク アドレス範囲が互いに重複していない場合に複数のゾーンのトラフィックを同時に分析できます。

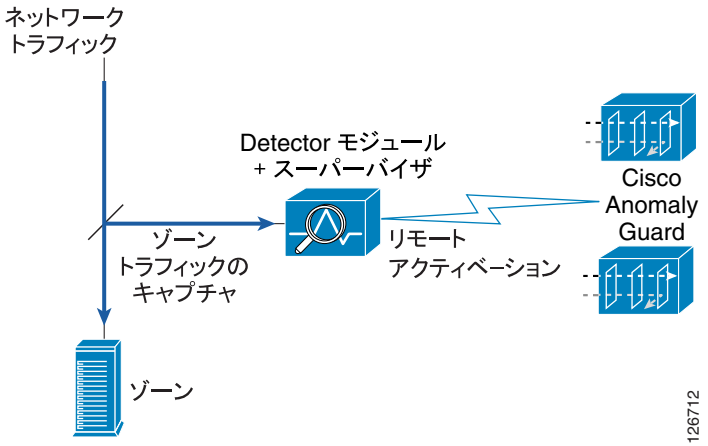
ゾーンを定義するときに、Detector モジュールがゾーンの異常検出に使用するネットワーク アドレスとポリシーを設定します。ゾーンに名前を割り当てて、この名前を使用してゾーンを参照します。

Detector モジュールの動作のしくみについて

Detector モジュールは、近づく DDoS 攻撃の新たな兆候がないか、トラフィックを分析します。トラフィックの異常を検出すると、Detector モジュールはそのイベントを自身の syslog に記録するか、自身と関連付けられた Guard をアクティブにします。Guard は、新たに発生する DDoS 攻撃を軽減してゾーンを保護します。図 1-1 に、検出の動作を示します。

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。

図 1-1　Cisco Traffic Anomaly Detector Module の動作



Detector モジュールは、ゾーン トラフィックの特性をラーニングしてゾーン トラフィックの比較基準とし、悪意のある攻撃になりうるあらゆる異常をトレースします。

この項では、次のトピックについて取り上げます。

ラーニング プロセスについて

ラーニング プロセスを使用すると、Detector モジュールが、通常のゾーン トラフィック パターンを解析して、ゾーンでのトラフィックの異常や攻撃を検出するためのポリシーを作成できるようになります。

ラーニング プロセスは、次の 2 つのフェーズで構成されています。

- ポリシー構築フェーズ : Detector モジュールがゾーン ポリシーを作成します。ポリシー テンプレートは、Detector モジュールがゾーン ポリシーの構築に使用する規則を提供します。トラフィックが透過的に Detector モジュールを通過することにより、ゾーンが使用する主なサービスを検出できます。
- しきい値調整フェーズ : Detector モジュールがゾーン サービスのトラフィック レートに合せてゾーン ポリシーを調整します。トラフィックが透過的に Detector モジュールを通過することにより、Detector モジュールはポリシー構築フェーズ中に検出されたサービスのしきい値を調整できます。

ゾーン ポリシーについて

ゾーン ポリシーは Detector モジュールの構成要素で、悪意のあるものになりうる異常をトレースするために、Detector モジュールがゾーン トラフィックを比較する基準になります。トラフィック フローがポリシーしきい値を超えると、Detector モジュールはこれを異常または悪意のあるトラフィックとして認識し、フィルタ セット（動的フィルタ）を動的に設定し、攻撃の重大度に応じて適切な検出レベルをこのトラフィック フローに適用します。

トラフィックのラーニングの詳細については、第 5 章「ゾーンの設定」を参照してください。ゾーン ポリシーの詳細については、第 7 章「ポリシー テンプレートとポリシーの設定」を参照してください。

Detector モジュールによるゾーン異常検出のしくみについて

Detector モジュールの保護は、次の方法でアクティブにできます。

- 自動保護モード：Detector モジュールが、作成した動的フィルタを自動的にアクティブにします。
- インタラクティブ保護モード：Detector モジュールが、作成した動的フィルタのキューを作成し、それらのフィルタを推奨されるアクションとしてグループ化します。ユーザは、これらの推奨事項を確認して、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に切り替えるかを決定します。

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。

検出およびラーニング機能について

しきい値調整フェーズとゾーン検出を同時にアクティブにして（検出およびラーニング機能）、Detector モジュールがゾーン ポリシーのしきい値をラーニングすると同時に、ゾーン ポリシーのしきい値でトラフィックの異常がないかを監視するようにできます。Detector モジュールは、攻撃を検出するとラーニング プロセスを停止しますが、ゾーン検出は継続します。このプロセスにより、Detector モジュールでは悪意のあるトラフィックのしきい値がラーニングされなくなります。攻撃が終了すると、Detector モジュールはラーニング プロセスを再開します。詳細については、P.8-20 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。

攻撃レポートについて

Detector モジュールはゾーンごとの攻撃レポートを提供し、ゾーン ステータスが表示できるようになっています。攻撃レポートでは、最初の動的フィルタの生成から保護の終了まで、攻撃の詳細な情報が提供されます。詳細については、第 11 章「攻撃レポートの使用方法」を参照してください。

異常検出プロセスについて

Detector モジュールは、ゾーンのトラフィックを必要な検出レベルに誘導するために、3 種類のフィルタを使用します。これらのフィルタを設定して、Detector モジュールがトラフィックの異常検出で使用する、トラフィックの方向や機能をカスタマイズすることができます。

Detector モジュールでは、次のタイプのフィルタが使用されます。

- バイパス フィルタ : Detector モジュールが特定のトラフィック フローを処理しないようにします。
- フレックスコンテンツ フィルタ : 指定されたパケット フローをカウントします。フレックスコンテンツ フィルタには、IP ヘッダーと TCP ヘッダー内のフィールドに応じたフィルタリングや、コンテンツ バイト数に応じたフィルタリングなど、非常に柔軟なフィルタリング機能があります。
- 動的フィルタ : 分析検出レベルをトラフィック フローに適用します。Detector モジュールは、トラフィック フローの分析結果として動的フィルタを作成します。動的フィルタは、Detector モジュールの syslog にイベントを記録するか、ゾーンを保護するために Guard をアクティブにします。動的フィルタは有効期間が限定されており、攻撃が終了すると削除されます。

Detector モジュールは、トラフィックの統計分析を行って、ポリシー（これによって異常がないかゾーン トラフィックを監視する）とフィルタ システムとの間の調整を行います。

1 Gbps および 2 Gbps 帯域幅オプションについて

Detector モジュールは、1 ギガビット / 秒（Gbps）と 2 Gbps という 2 つの帯域幅パフォーマンス レベルで動作できます。Detector モジュールにロードされるソフトウェア イメージが、モジュールとスーパーバイザ エンジンの間にある 3 つの物理インターフェイスを Detector モジュールが使用する方法を制御して、動作帯域幅を決めます。インストールされたソフトウェア イメージは、次の方法でインターフェイスを制御します。

- 6.0 ソフトウェア イメージ：このソフトウェア イメージのスループットは 1 Gbps で、1 つのインターフェイス ポートを介して、データ トラフィックをスーパーバイザ エンジンと Detector モジュール間で移動できます。2 番目のインターフェイス ポートは、アウトオブバンド管理トラフィックを転送し、関連付けられている Guard デバイスをアクティブにする場合に使用します。3 番目のインターフェイス ポートは使用されません。
- 6.0-XG ソフトウェア イメージ：このソフトウェア イメージのスループットは 2 Gbps で、データ トラフィックを転送するためのインターフェイス ポートのうち、2 つをイネーブルにします。3 番目のインターフェイスは、アウトオブバンド管理トラフィックの転送と Guard デバイスのアクティブ化のための専用インターフェイスです。XG ソフトウェア イメージを使用するには、Detector モジュールにソフトウェア ライセンスが必要です。

（注） ソフトウェア イメージがインストールされている Detector モジュールを注文することも、6.0 ソフトウェア イメージ（1 Gbps 動作）を 6.0-XG ソフトウェア イメージ（2 Gbps 動作）にアップグレードすることもできます。6.0-XG ソフトウェア イメージが事前にインストールされている Detector モジュールを注文する場合には、Detector モジュールをセットアップするときにライセンスをインストールする必要があります（P.13-30 の「1 Gbps から 2 Gbps への帯域幅パフォーマンスのアップグレード」を参照）。

表 1-1 に、Detector モジュールの物理インターフェイスとスーパーバイザ ポート間の相関を示します。この表では、2 Gbps 動作用のソフトウェア イメージをインストールした後にデータ トラフィック変更用の CLI インターフェイス指定子がどのように変更されるかも示します。

表 1-1　スーパーバイザ エンジン ポートと相関する Detector モジュール インターフェイス

スーパーバイザ エンジン ポート	Detector モジュール 1 Gbps 動作		Detector モジュール 2 Gbps 動作	
	インターフェイス	トラフィック タイプ	インターフェイス	トラフィック タイプ
ポート 1	giga2	データ	giga1	データ
ポート 2	不使用	-	giga2	データ
ポート 3	mng	管理および Guard のアクティベーション	mng	管理および Guard のアクティベーション

1 Gbps 動作と 2 Gbps 動作の間では、スーパーバイザ エンジンでのソース データ トラフィック VLAN の定義方法が次のように異なります。

- 1 Gbps 動作：ポート 1 でのみデータ トラフィック VLAN を定義します。
- 2 Gbps 動作：ポート 1 と 2 でデータ トラフィック VLAN を定義します。各ポートで異なる VLAN を定義します。