CHAPTER 1

製品概要

この章では、Cisco Traffic Anomaly Detector モジュール（Detector モジュール）の概要について説明します。概要には、Detector モジュールの主要コンポーネントについての説明、および悪意のある攻撃トラフィックを検出してネットワーク要素を保護するための主要コンポーネントの連携方法についての説明などが含まれます。

この章は、次の項で構成されています。

Detector モジュールについて

Detector モジュールは、ネットワーク トラフィックのコピーを監視し、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ます。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ネットワーク要素（つまり *ゾーン*）です。

Detector モジュールは、次のいずれかのシスコ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

ポート ミラーリング、または光ファイバ回線スプリッタを使用して、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またはルータを設定します。

Detector モジュールは、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が、Detector モジュールの関連製品である Cisco Guard（Guard）との併用に最も適しています。

（注） Guard は、DDoS 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。

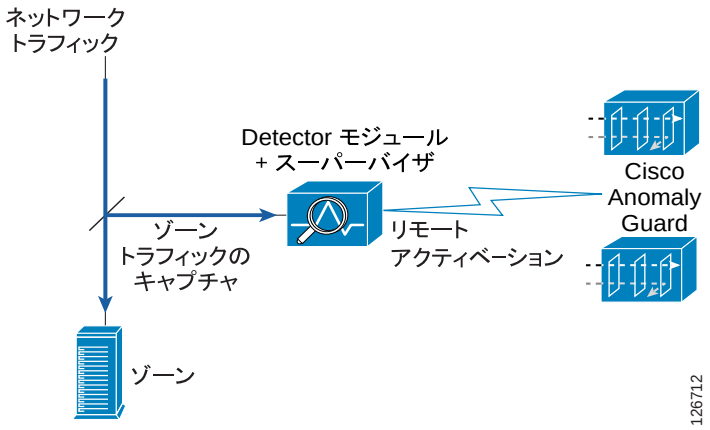
Detector モジュールは一連のゾーン ポリシーを使用して、すべてのインバウンド ゾーン トラフィックのコピーを分析します。Detector モジュールはゾーン ポリシーにより、ゾーンへの攻撃を示すトラフィック異常を識別できます。Detector モジュールはトラフィックの異常を識別すると、syslog メッセージを発行して攻撃を通知したり、Guard をアクティブにして攻撃を軽減したりすることができます。

Detector モジュールでは、次のタスクを実行できます。

- トラフィックのラーニング：アルゴリズムに基づくプロセスを使用して、通常のゾーン　トラフィックの特性（サービスおよびトラフィック レート）をラーニングします。Detector モジュールは、ラーニング プロセス中、デフォルトのゾーン トラフィック ポリシーおよびポリシーしきい値を通常のゾーン トラフィックの特性に合うように変更します。トラフィック ポリシーおよびしきい値は、ゾーン トラフィックが正常か異常（ゾーンに対する攻撃の可能性）かを判別するために Detector モジュールが使用する参照ポイントを定義します。
- トラフィックの異常検出：通常のトラフィック特性に基づいて、ゾーンのトラフィックの異常を検出します。

図 1-1 に、ネットワークでの適用例を示します。ここで、Detector モジュールは、分析のためにネットワーク トラフィックのコピーを受信します。

図 1-1　Cisco Traffic Anomaly Detector モジュールの動作



DDos 攻撃について

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。

この項では、次のトピックについて取り上げます。

スプーフィング攻撃について

スプーフィング攻撃は DDoS 攻撃の一種で、パケットのヘッダーに送信元デバイスの実際の IP アドレスではない IP アドレスが含まれます。スプーフィングされたパケットの送信元 IP アドレスは、ランダムである場合も、特定の限定されたアドレスを持つ場合もあります。スプーフィング攻撃は、ターゲット サイトのリンクおよびサーバ リソースを飽和状態にします。コンピュータ ハッカーは、1 つのデバイスからでも、大量のスプーフィング攻撃を簡単に生成できます。

非スプーフィング攻撃について

非スプーフィング攻撃（クライアント攻撃）は、ほとんどの場合実際の TCP 接続による TCP ベースの攻撃で、ネットワーク リンクやオペレーティング システムではなく、サーバ上でアプリケーション レベルを利用不能にすることができます。

多数のクライアント（ゾンビ）からのクライアント攻撃は、個々のクライアントが異常を作り出さなくても、サーバ アプリケーションを利用不能にすることができます。ゾンビ プログラムは、ターゲット サイトにアクセスする正当なブラウザのふりをしようとします。

ゾーン、ゾーン ポリシー、およびラーニング プロセスについて

この項では、Detector モジュールのゾーンとは何か、ゾーン ポリシーがトラフィック異常を検出する方法、および Detector モジュールがゾーンのトラフィック特性をラーニングする方法について説明します。

この項では、次のトピックについて取り上げます。

ゾーンについて

Detector モジュールがトラフィックの異常を監視するゾーンは、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

新しいゾーンを作成する場合は、ゾーンに名前を割り当て、ネットワーク アドレスを設定します。ゾーン トラフィックの異常を検出するデフォルトのポリシーおよびポリシーしきい値のセットが Detector モジュールによりゾーンに設定されます。

Detector モジュールは、ゾーンのネットワーク アドレス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 ポリシーについて

Detector モジュールは、ゾーン設定に関連付けられているポリシーによって、ゾーン トラフィックの異常を検出できます。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。

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。

ラーニング プロセスについて

Detector モジュールは、ラーニング プロセスにより、通常のゾーン トラフィックを分析し、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を作成できます。このため、Detector モジュールはゾーン トラフィックの異常をより正確に検出できるようになります。

ラーニング プロセスにより、デフォルトのゾーン ポリシー セットを置き換えることができます。また、現在のゾーン ポリシー セットが現在の正常なトラフィック サービスとトラフィック量を認識するように正しく設定されていない可能性がある場合、そのポリシー セットをアップデートすることもできます。ポリシーしきい値が、現在の正常なトラフィック量に比べて大きすぎる値に設定されていると、Detector モジュールがトラフィック異常（攻撃）を検出できない可能性があります。ポリシーしきい値が小さすぎると、Detector モジュールが正常なトラフィックを攻撃トラフィックと取り違えてしまう可能性があります。

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：ゾーン トラフィックが使用する主なサービスのゾーン ポリシーを作成します。ゾーン ポリシーを作成する場合、Detector モジュールは、各ゾーン設定に含まれるポリシー テンプレートによって設定された規則に従います。
- しきい値調整フェーズ：ゾーン ポリシーのしきい値を、ゾーン サービスの通常のトラフィック レートを認識するための適切な値に調整します。

ラーニング プロセスの詳細については、第 8 章「ゾーン トラフィックの特性のラーニング」を参照してください。

異常検出プロセスについて

この項では、Detector モジュールでのゾーン トラフィック異常の検出方法、および攻撃レポートの生成方法について説明します。

この項では、次のトピックについて取り上げます。

トラフィック フィルタについて

Detector モジュールは、3 種類のトラフィック フィルタを使用して、必要な検出レベルをゾーン トラフィックに適用します。これらのフィルタは、トラフィック フローをカスタマイズし、DDoS 検出操作を制御するように設定できます。

Detector モジュールでは、次のタイプのトラフィック 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 フローに DDoS 検出措置を適用しないようにします。
- フレックスコンテンツ フィルタ : 指定されたトラフィック フローをカウントします。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、およびコンテンツ バイト数に応じたフィルタリングを実行します。
- 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。分析プロセス中に Detector モジュールが異常を検出すると、動的フィルタは Detector モジュールに対して、syslog にイベントを記録するか、ゾーンを保護するために Guard をアクティブにするよう指示します。

Detector モジュールは、ゾーン トラフィックの異常を監視するゾーン ポリシーの動作とゾーン フィルタを調整します。

フィルタの詳細については、第 6 章「ゾーンのフィルタの設定」を参照してください。

各種の異常検出モードについて

Detector モジュールの異常検出動作は、次の方法でアクティブにできます。

- 自動検出モード : 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。
- インタラクティブ検出モード : 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。

インタラクティブ検出モードの詳細については、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。

検出およびラーニング機能について

ラーニング プロセスのしきい値調整フェーズとゾーン異常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）、新しいゾーン ポリシーのしきい値のラーニングと、現在のしきい値を使用したトラフィック異常の監視を Detector モジュールが同時に行うようにできます。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、トラフィック異常の監視は継続します。このプロセスにより、Detector モジュールでは、攻撃中に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。

検出およびラーニング機能の詳細については、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。

攻撃レポートについて

Detector モジュールは、各ゾーンの攻撃レポートを提供します。攻撃レポートでは、最初の動的フィルタの生成から異常検出の終了まで、ゾーンのステータス情報と攻撃の詳細な情報が提供されます。

攻撃レポートの詳細については、第 11 章「攻撃レポートの使用方法」を参照してください。

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、シスコがこのソフトウェア イメージに必要なライセンスのインストールを行います。6.0-XG ソフトウェア イメージのアップグレードの詳細については、P.13-20 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」を参照してください。

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

次の項目では、1 Gbps 動作と 2 Gbps 動作の VLAN インターフェイス設定の違いについて説明しています。

- 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。